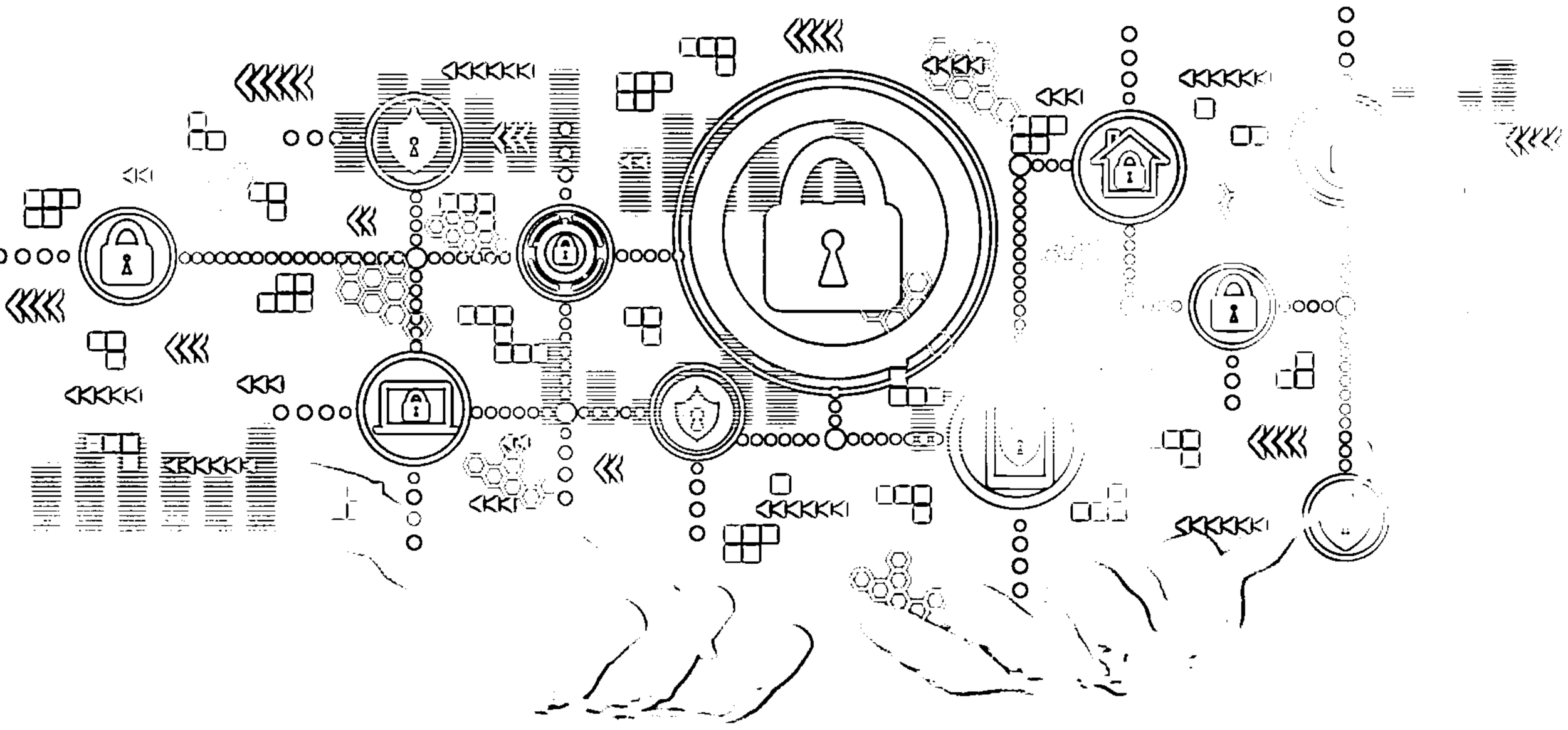
EC-Council



C|EH
Certified Ethical Hacker

Ethical Hacking and Countermeasures v11

Professional Series

EC-COUNCIL OFFICIAL CURRICULA

Ethical Hacking and Countermeasures

Version 11

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

NOTICE TO THE READER

Foreword

Since you are reading this CEHv11 courseware, you most likely realize the importance of information systems security. However, we would like to put forth our motive behind compiling a resource such as this one and what you can gain from this course.

You might find yourself asking what sets this course apart from the others out there. The truth is that no single courseware can address all the issues of information security in a detailed manner. Moreover, the rate at which exploits, tools, and methods are being discovered by the security community makes it difficult for one program to cover all the necessary facets of information security. This doesn't mean that this course is inadequate in any way as we have worked to cover all major domains in such a manner that the reader will be able to appreciate the way security has evolved over time as well as gain insight in to the fundamental workings relevant to each domain. It is a blend of academic and practical wisdom supplemented with tools that the reader can readily access in order to obtain a hands-on experience.

The emphasis throughout the courseware is on gaining practical know-how, which explains the stress on free and accessible tools. You will read about some of the most widespread attacks seen, the popular tools used by attackers, and how attacks have been carried out using ordinary resources.

You may also want to know what to expect once you have completed the course. This courseware is a resource material. Any penetration tester can tell you that there is no one straight methodology or sequence of steps that you can follow while auditing a client site. There is no one template that will meet all your needs. Your testing strategy will vary with the client, the basic information about the system or situation, and the resources at your disposal. However, for each stage you choose – be it enumeration, firewall, penetration of other domains - you will find something in this courseware that you can definitely use.

Finally, this is not the end! This courseware is to be considered a constant work-in-progress because we will be adding value to this courseware over time. You may find some aspects extremely detailed, while others may have less detail. We are constantly asking ourselves if the content helps explain the core point of the lesson, and we constant calibrate our material with that in mind. We would love to hear your viewpoints and suggestions so please send us your feedback to help in our quest to constantly improve our courseware.

About the EC-Council CEH Program

If you want to stop hackers from invading your network, first you've got to invade their minds.

Computers around the world are systematically being victimized by rampant hacking. This hacking is not only widespread, but is being executed so flawlessly that the attackers compromise a system, steal everything of value and completely erase their tracks.

The goal of the ethical hacker is to help the organization take preemptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits. This philosophy stems from the proven practice of trying to catch a thief, by thinking like a thief. As technology advances and organization depend on technology increasingly, information assets have evolved into critical components of survival.

If hacking involves creativity and thinking 'out-of-the-box', then vulnerability testing and security audits will not ensure the security proofing of an organization. To ensure that organizations have adequately protected their information assets, they must adopt the approach of 'defense in depth'. In other words, they must penetrate their networks and assess the security posture for vulnerabilities and exposure.

The Ethical Hacker is an individual who is usually employed with the organization and who can be trusted to undertake an attempt to penetrate networks and/or computer systems using the same methods as a Hacker. Hacking is a felony in some countries. When it is done by request and under a contract between an Ethical Hacker and an organization, it is legal. The most important point is that an Ethical Hacker has authorization to probe the target.

The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

To achieve the Certified Ethical Hacker Certification, you must pass the CEH exam 312-50.

Please visit **https://www.eccouncil.org/programs/certified-ethical-hacker-ceh** for more information.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. It is considered as the benchmark for many government entities and major corporations around the globe.

EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

Other EC-Council Programs

Security Awareness: Certified Secure Computer User

C|SCU
Certified | Secure Computer User

The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

Network Defense: Certified Network Defender

C|ND
Certified | Network Defender

Students enrolled in the Certified Network Defender course will gain a detailed understanding of network defense and develop their hands-on expertise to perform in real-life network defense situations. They will gain the depth of technical knowledge required to actively design a secure network within your organization. This course provides a fundamental understanding of the true nature of data transfer, network technologies, and software technologies so that students may understand how networks operate, how automation software behaves, and how to analyze networks and their defense.

Students will learn how to protect, detect, and respond to the network attacks as well as learning about network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. Students will also learn the intricacies of network traffic signature, analysis, and vulnerability scanning, which will help in designing improved network security policies and successful incident response plans. These skills will help organizations foster resiliency and operational continuity during attacks.

Penetration Testing: Certified Penetration Testing Professional

CPENT certification requires you to demonstrate the application of advanced penetration testing techniques such as advanced Windows attacks, IOT systems attacks, advanced binaries exploitation, exploits writing, bypassing a filtered network, Operational Technology (OT) pen testing, accessing hidden networks with pivoting and double pivoting, privilege escalation, and evading defense mechanisms.

EC-Council's CPENT standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective of the CPENT is to ensure that each professional follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry.

Unlike a normal security certification, the CPENT credential provides an assurance that security professionals possess skills to analyze the security posture of a network exhaustively and recommend corrective measures authoritatively. For many years EC-Council has been certifying IT Security Professionals around the globe to ensure these professionals are proficient in network security defense mechanisms. EC-Council's credentials vouch for their professionalism and expertise thereby making these professionals more sought after by organizations and consulting firms globally.

Computer Forensics: Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

Incident Handling: EC-Council Certified Incident Handler

E|CIH™ EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe. It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

Management: Certified Chief Information Security Officer

C|CISO Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

Application Security: Certified Application Security Engineer

C|ASE .NET Certified Application Security Engineer

C|ASE JAVA Certified Application Security Engineer

The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally.It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Incident Handling: Certified Threat Intelligence Analyst

C|TIA
Certified | Threat Intelligence Analyst

Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

In the ever-changing threat landscape, C|TIA is an essential Threat Intelligence training program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level Threat Intelligence training programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

Incident Handling: Certified SOC Analyst

C|SA™
Certified | SOC Analyst

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

CEH Exam Information

CEH Exam Details	
Exam Title	**Certified Ethical Hacker (CEH)**
Exam Code	**312-50**
Availability	**EC-Council Exam Portal** (please visit **https://www.eccexam.com**) **VUE** (please visit **https://home.pearsonvue.com/eccouncil**)
Duration	**4 Hours**
Questions	**125**
Passing Score	Please refer **https://cert.eccouncil.org/faq.html**

Please visit **https://cert.eccouncil.org/certified-ethical-hacker.html** for more information.

Table of Contents

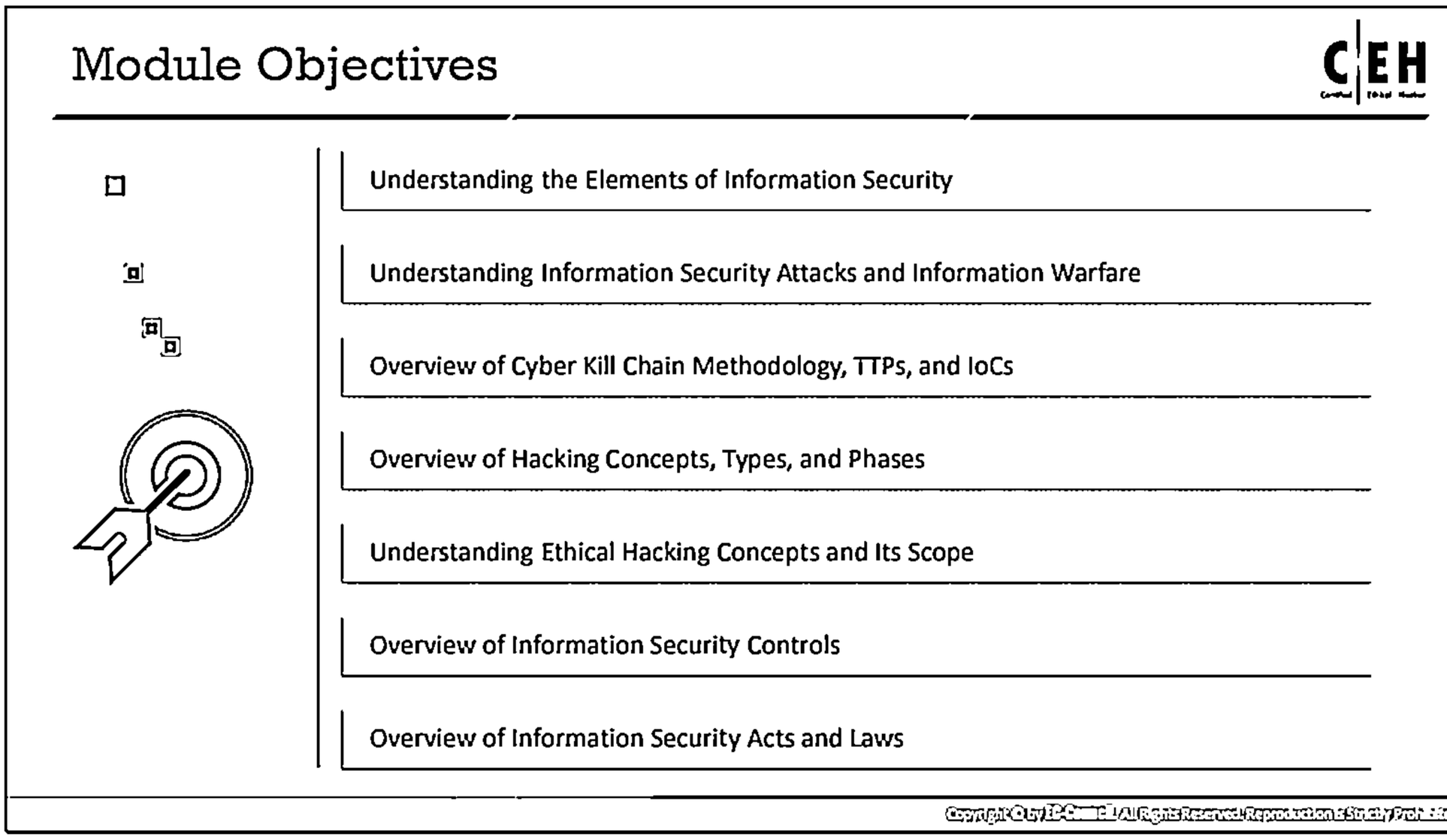
ETHICAL HACKING

ETHICAL HACKING

C|EH™

Certified Ethical Hacker

Module 01:
Introduction to Ethical Hacking



Module Objectives

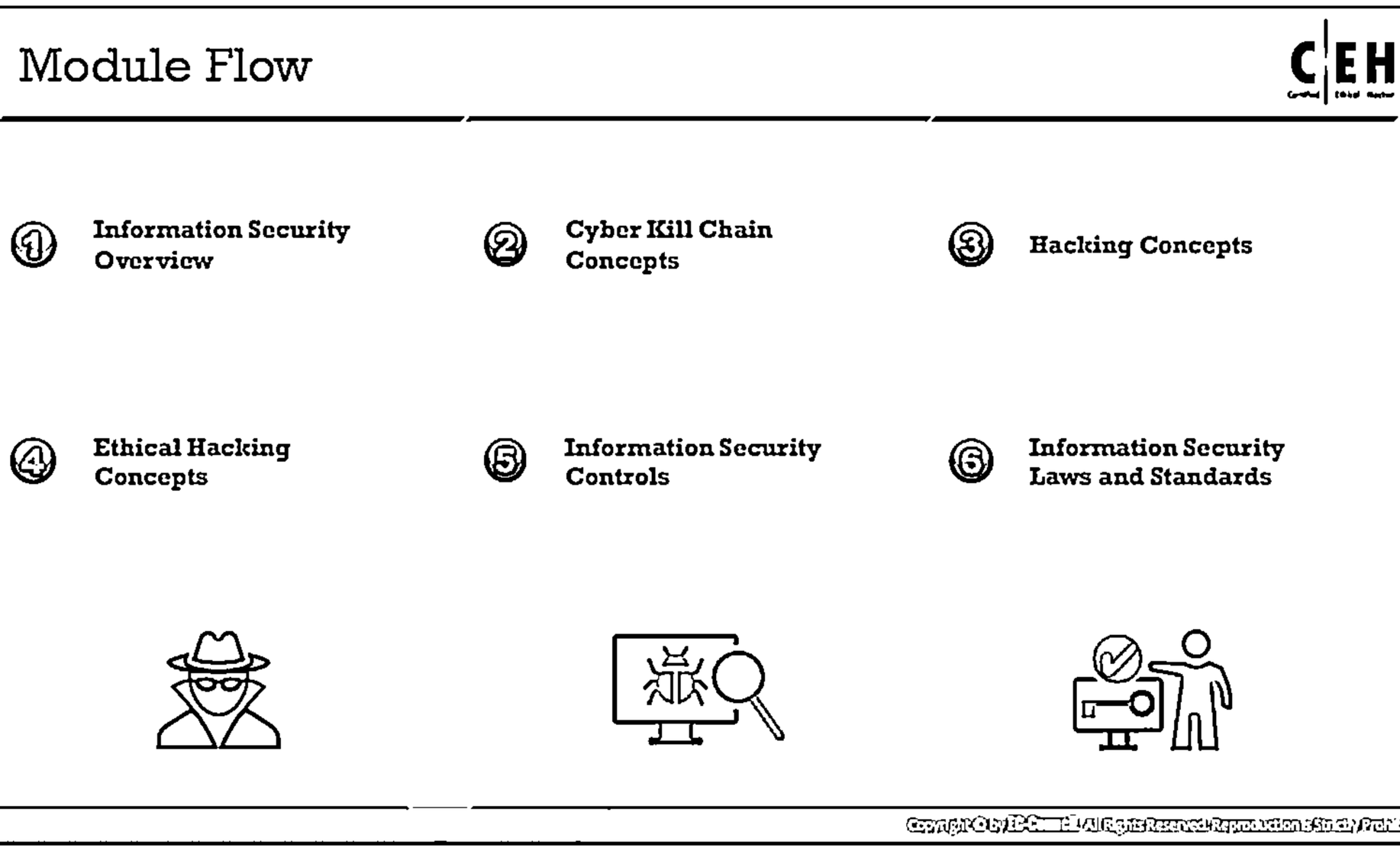
Attackers break into systems for various reasons and purposes. Therefore, it is important to understand how malicious hackers attack and exploit systems and the probable reasons behind those attacks. As Sun Tzu states in the Art of War, "If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat." System administrators and security professionals must guard their infrastructure against exploits by knowing the enemy—the malicious hacker(s)—who seeks to use the same infrastructure for illegal activities.

This module starts with an overview of the current security scenario and emerging threat vectors. It provides insight into the different elements of information security. Later, the module discusses hacking and ethical hacking concepts and ends with a brief discussion on information security controls and information security laws and acts.

At the end of this module, you will be able to:

- Describe the elements of information security
- Explain information security attacks and information warfare
- Describe cyber kill chain methodology, TTPs, and IoCs
- Describe hacking concepts, types, and phases
- Explain ethical hacking concepts and scope
- Understand information security controls (defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI/ML)
- Know about the information security acts and laws

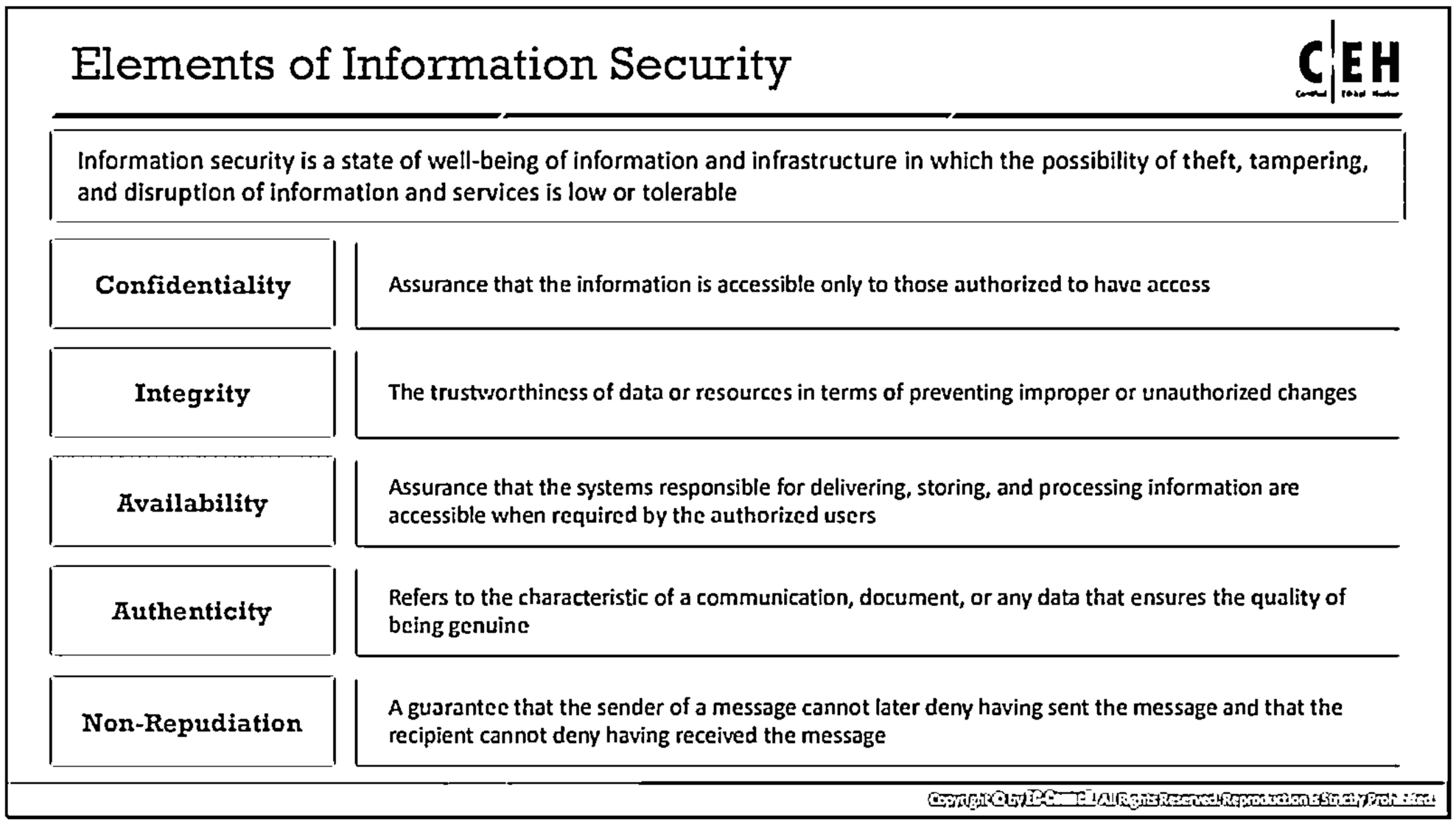
Module Flow



Information Security Overview

Information security refers to the protection or safeguarding of information and information systems that use, store, and transmit information from unauthorized access, disclosure, alteration, and destruction. Information is a critical asset that organizations must secure. If sensitive information falls into the wrong hands, then the respective organization may suffer huge losses in terms of finances, brand reputation, customers, or in other ways. To provide an understanding of how to secure such critical information resources, this module starts with an overview of information security.

This section introduces the elements of information security, classification of attacks, and information warfare.



Elements of Information Security

Information security is "the state of the well-being of information and infrastructure in which the possibility of theft, tampering, or disruption of information and services is kept low or tolerable." It relies on five major elements: confidentiality, integrity, availability, authenticity, and non-repudiation.

- **Confidentiality**

  Confidentiality is the assurance that the information is accessible only to authorized. Confidentiality breaches may occur due to improper data handling or a hacking attempt. Confidentiality controls include data classification, data encryption, and proper disposal of equipment (such as DVDs, USB drives, and Blu-ray discs).

- **Integrity**

  Integrity is the trustworthiness of data or resources in the prevention of improper and unauthorized changes—the assurance that information is sufficiently accurate for its purpose. Measures to maintain data integrity may include a checksum (a number produced by a mathematical function to verify that a given block of data is not changed) and access control (which ensures that only authorized people can update, add, or delete data).

- **Availability**

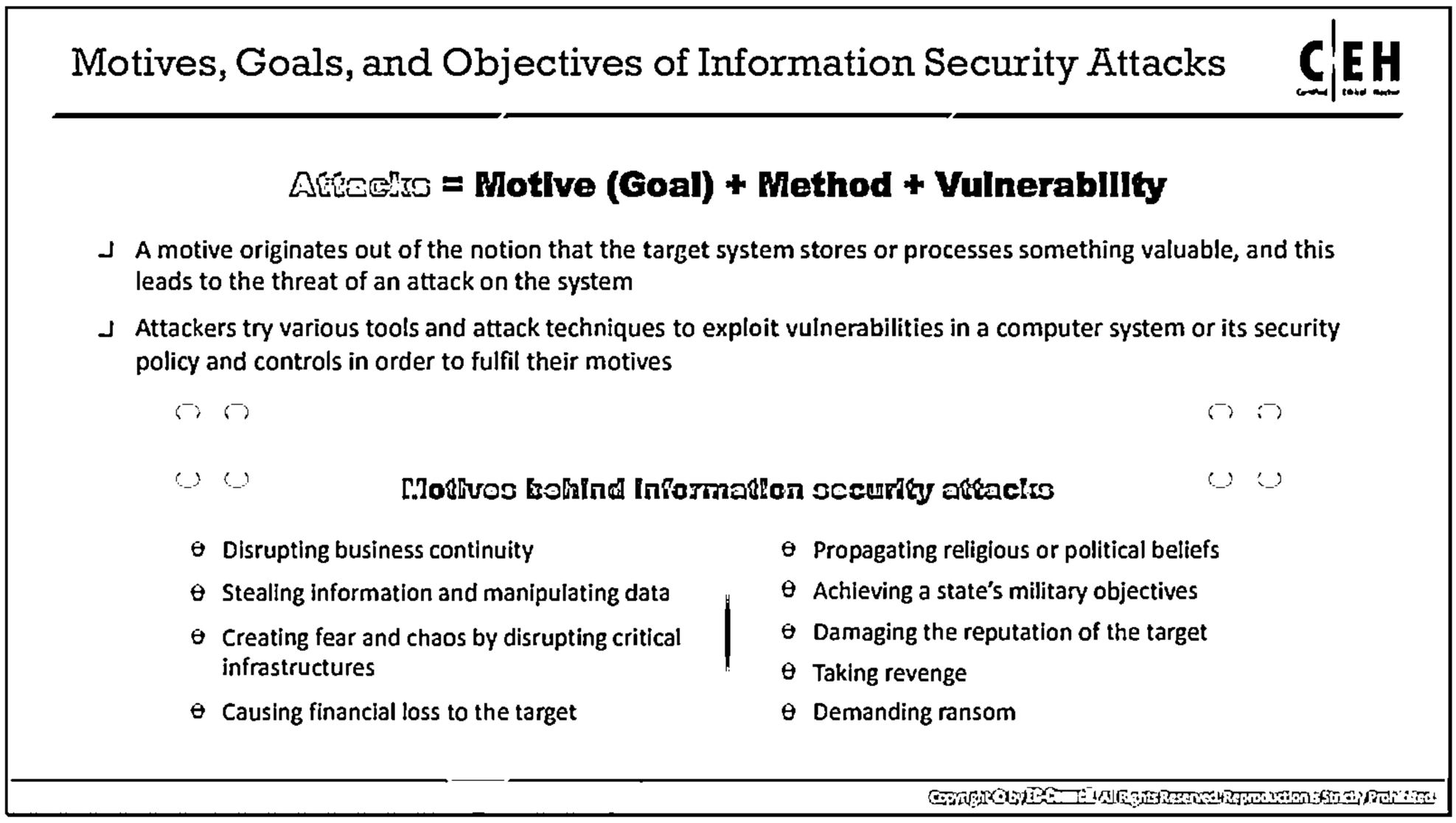
  Availability is the assurance that the systems responsible for delivering, storing, and processing information are accessible when required by authorized users. Measures to maintain data availability can include disk arrays for redundant systems and clustered machines, antivirus software to combat malware, and distributed denial-of-service (DDoS) prevention systems.

- **Authenticity**

  Authenticity refers to the characteristic of communication, documents, or any data that ensures the quality of being genuine or uncorrupted. The major role of authentication is to confirm that a user is genuine. Controls such as biometrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, and documents.

- **Non-Repudiation**

  Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Individuals and organizations use digital signatures to ensure non-repudiation.



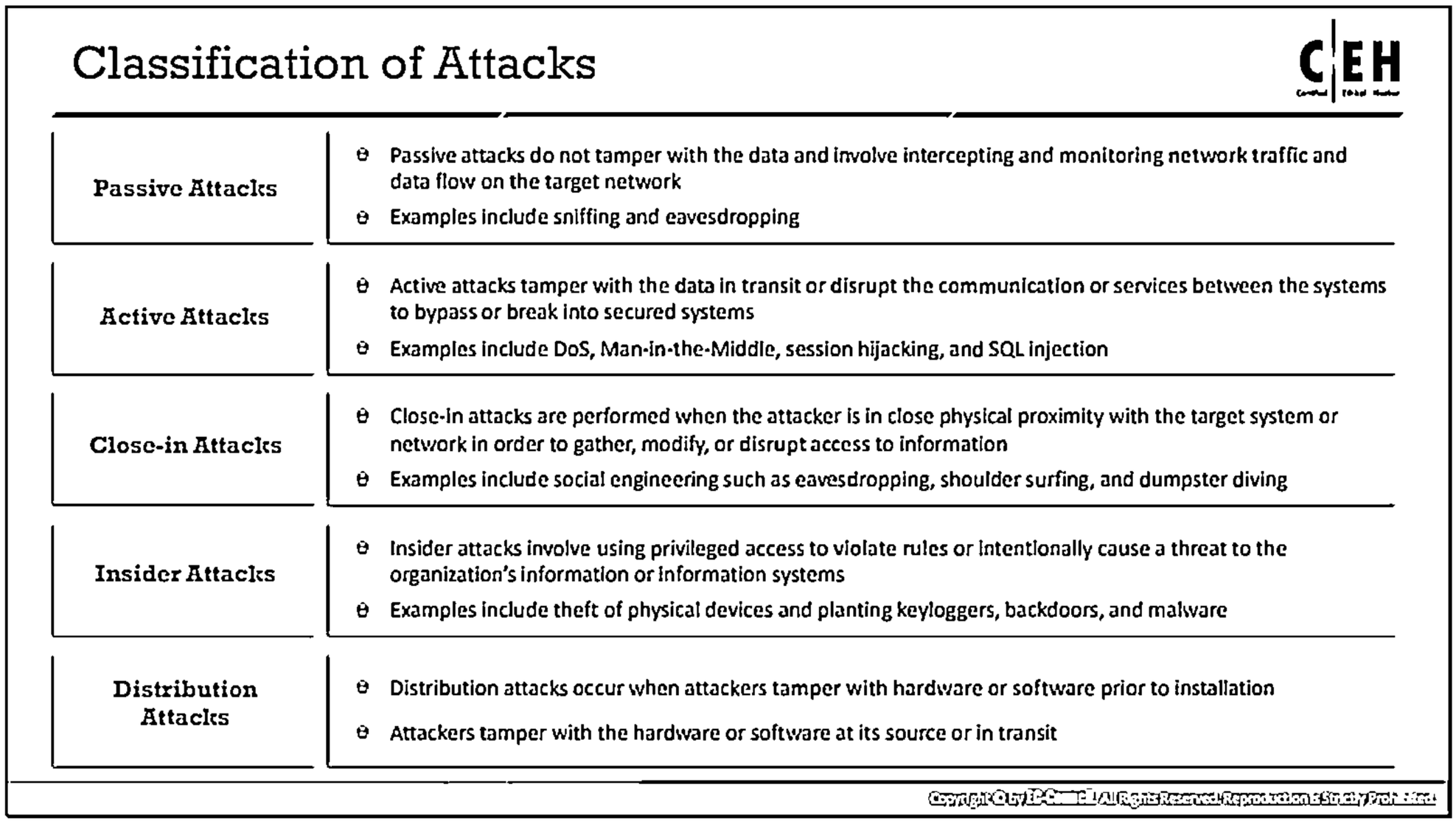
Motives, Goals, and Objectives of Information Security Attacks

Attackers generally have motives (goals), and objectives behind their information security attacks. A motive originates out of the notion that a target system stores or processes something valuable, which leads to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization's business operations, to steal valuable information for the sake of curiosity, or even to exact revenge. Therefore, these motives or goals depend on the attacker's state of mind, their reason for carrying out such an activity, as well as their resources and capabilities. Once the attacker determines their goal, they can employ various tools, attack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls.

Attacks = Motive (Goal) + Method + Vulnerability

Motives behind information security attacks

- Disrupt business continuity
- Perform information theft
- Manipulating data
- Create fear and chaos by disrupting critical infrastructures
- Bring financial loss to the target
- Propagate religious or political beliefs
- Achieve a state's military objectives
- Damage the reputation of the target
- Take revenge
- Demand ransom



Classification of Attacks

According to IATF, security attacks are classified into five categories: passive, active, close-in, insider, and distribution.

- **Passive Attacks**

  Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data. Attackers perform reconnaissance on network activities using sniffers. These attacks are very difficult to detect as the attacker has no active interaction with the target system or network. Passive attacks allow attackers to capture the data or files being transmitted in the network without the consent of the user. For example, an attacker can obtain information such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks.

  Examples of passive attacks:

  - Footprinting
  - Sniffing and eavesdropping
  - Network traffic analysis
  - Decryption of weakly encrypted traffic

- **Active Attacks**

  Active attacks tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems. Attackers launch attacks on the target system or network by sending traffic actively that can be detected. These

attacks are performed on the target network to exploit the information in transit. They penetrate or infect the target's internal network and gain access to a remote system to compromise the internal network.

Examples of active attacks:

- Denial-of-service (DoS) attack
- Bypassing protection mechanisms
- Malware attacks (such as viruses, worms, ransomware)
- Modification of information
- Spoofing attacks
- Replay attacks
- Password-based attacks
- Session hijacking
- Man-in-the-Middle attack
- DNS and ARP poisoning
- Compromised-key attack
- Firewall and IDS attack
- Profiling
- Arbitrary code execution
- Privilege escalation
- Backdoor access
- Cryptography attacks
- SQL injection
- XSS attacks
- Directory traversal attacks
- Exploitation of application and OS software

- **Close-in Attacks**

  Close-in attacks are performed when the attacker is in close physical proximity with the target system or network. The main goal of performing this type of attack is to gather or modify information or disrupt its access. For example, an attacker might shoulder surf user credentials. Attackers gain close proximity through surreptitious entry, open access, or both.

  Examples of close-in attacks:

  - Social engineering (Eavesdropping, shoulder surfing, dumpster diving, and other methods)

- **Insider Attacks**

  Insider attacks are performed by trusted persons who have physical access to the critical assets of the target. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. They misuse the organization's assets to directly affect the confidentiality, integrity, and availability of information systems. These attacks impact the organization's business operations, reputation, and profit. It is difficult to figure out an insider attack

  Examples of insider attacks:

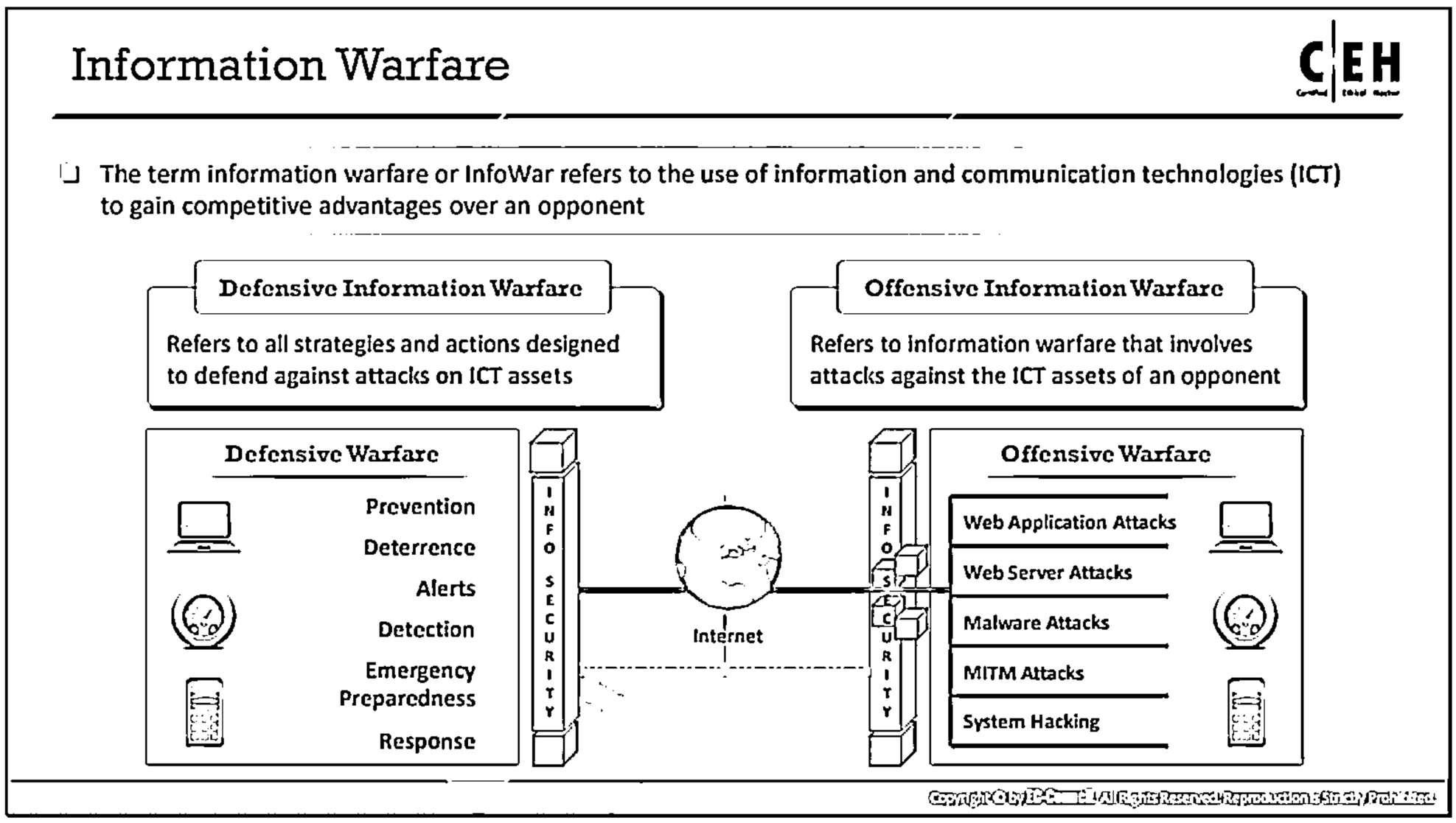
  - Eavesdropping and wiretapping

- Theft of physical devices
- Social engineering
- Data theft and spoliation
- Pod slurping
- Planting keyloggers, backdoors, or malware

- **Distribution Attacks**

  Distribution attacks occur when attackers tamper with hardware or software prior to installation. Attackers tamper the hardware or software at its source or when it is in transit. Examples of distribution attacks include backdoors created by software or hardware vendors at the time of manufacture. Attackers leverage these backdoors to gain unauthorized access to the target information, systems, or network.

  - Modification of software or hardware during production
  - Modification of software or hardware during distribution



Information Warfare

Source: *http://www.iwar.org.uk*

The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) for competitive advantages over an opponent. Examples of information warfare weapons include viruses, worms, Trojan horses, logic bombs, trap doors, nanomachines and microbes, electronic jamming, and penetration exploits and tools.

Martin Libicki divided information warfare into the following categories:

- **Command and control warfare (C2 warfare)**: In the computer security industry, C2 warfare refers to the impact an attacker possesses over a compromised system or network that they control.
- **Intelligence-based warfare**: Intelligence-based warfare is a sensor-based technology that directly corrupts technological systems. According to Libicki, "intelligence-based warfare" is warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace.
- **Electronic warfare**: According to Libicki, electronic warfare uses radio-electronic and cryptographic techniques to degrade communication. Radio electronic techniques attack the physical means of sending information, whereas cryptographic techniques use bits and bytes to disrupt the means of sending information.
- **Psychological warfare**: Psychological warfare is the use of various techniques such as propaganda and terror to demoralize one's adversary in an attempt to succeed in battle.
- **Hacker warfare**: According to Libicki, the purpose of this type of warfare can vary from the shutdown of systems, data errors, theft of information, theft of services, system

monitoring, false messaging, and access to data. Hackers generally use viruses, logic bombs, Trojan horses, and sniffers to perform these attacks.

- **Economic warfare**: Libicki notes that economic information warfare can affect the economy of a business or nation by blocking the flow of information. This could be especially devastating to organizations that do a lot of business in the digital world.
- **Cyberwarfare**: Libicki defines cyber warfare as the use of information systems against the virtual personas of individuals or groups. It is the broadest of all information warfare. It includes information terrorism, semantic attacks (similar to Hacker warfare, but instead of harming a system, it takes over the system while maintaining the perception that it is operating correctly), and simula-warfare (simulated war, for example, acquiring weapons for mere demonstration rather than actual use).

Each form of information warfare mentioned above consists of both defensive and offensive strategies.

- **Defensive Information Warfare**: Involves all strategies and actions to defend against attacks on ICT assets.
- **Offensive Information Warfare**: Involves attacks against the ICT assets of an opponent.

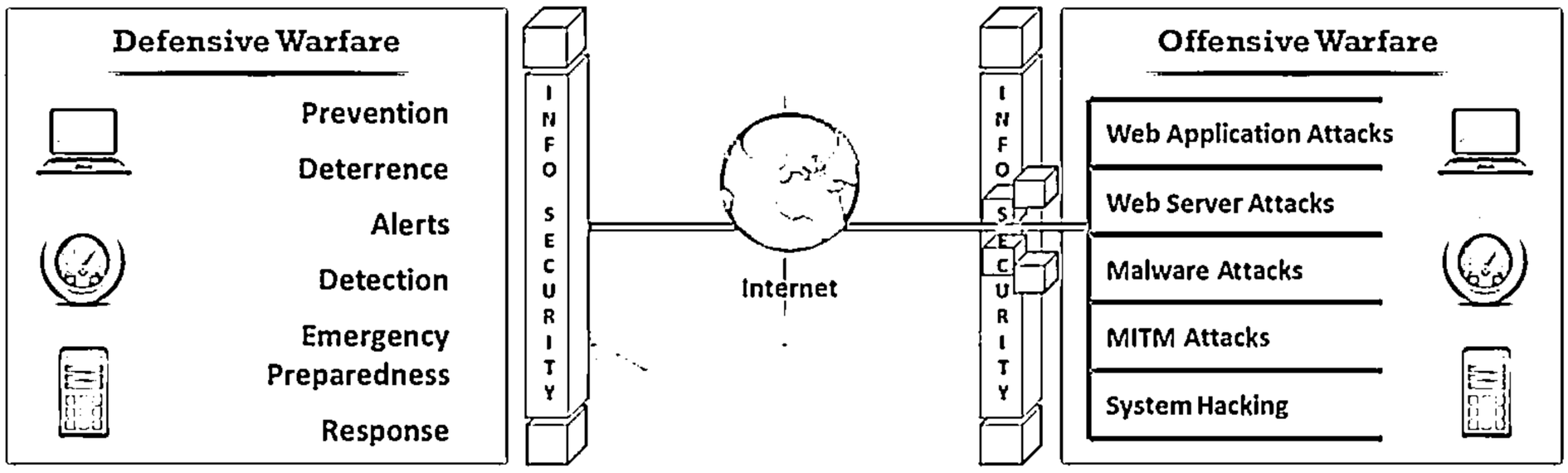
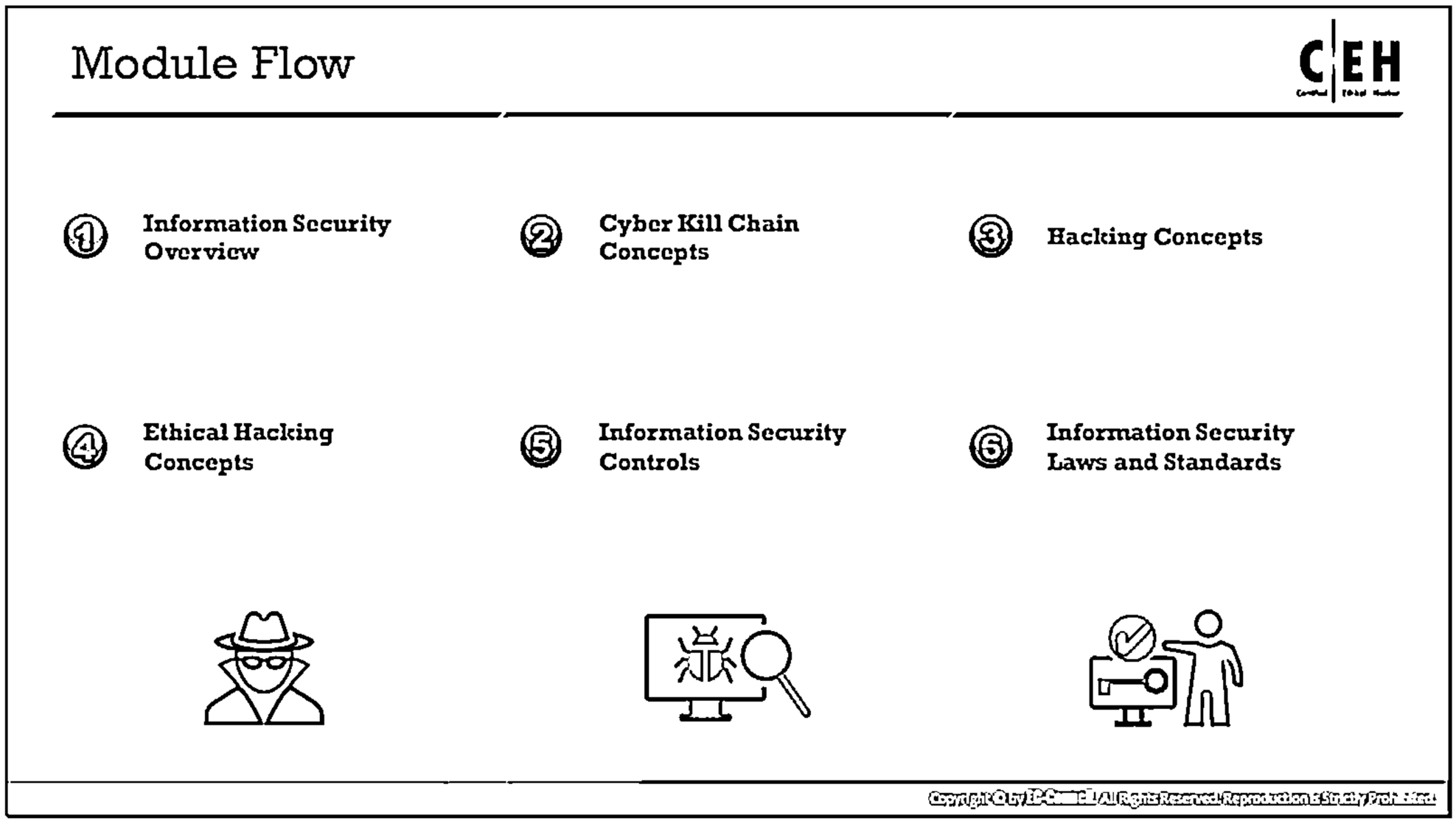


Figure 1.1: Block Diagram of Information Warfare



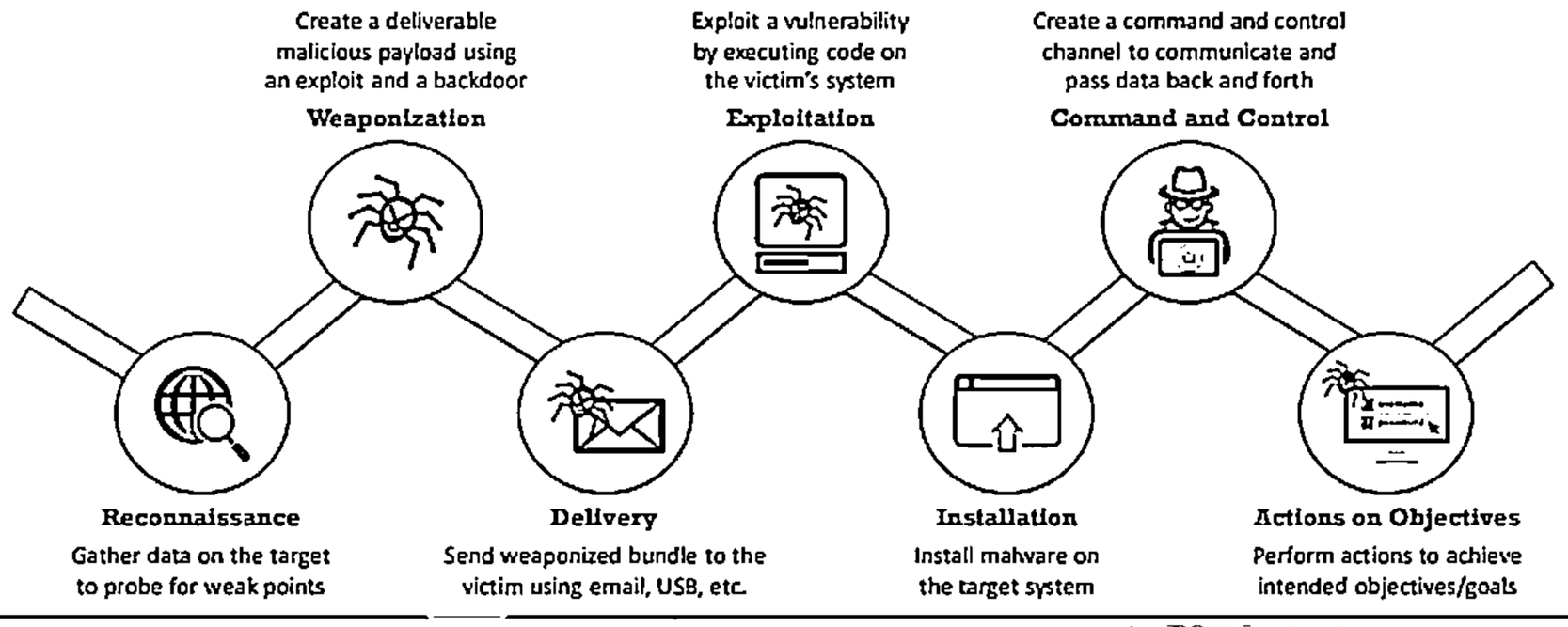
Cyber Kill Chain Concepts

The cyber kill chain is an efficient and effective way of illustrating how an adversary can attack the target organization. This model helps organizations understand the various possible threats at every stage of an attack and the necessary countermeasures to defend against such attacks. Also, this model provides security professionals with a clear insight into the attack strategy used by the adversary so that different levels of security controls can be implemented to protect the IT infrastructure of the organization.

This section discusses the cyber kill chain methodology, common TTPs used by adversaries, behavioral identification of adversaries, and Indicators of Compromise (IoCs).

Cyber Kill Chain Methodology

- The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities
- It provides greater insight into attack phases, which helps security professionals to understand the adversary's tactics, techniques, and procedures beforehand



Cyber Kill Chain Methodology

The cyber kill chain methodology is a component of intelligence-driven defense for the identification and prevention of malicious intrusion activities. This methodology helps security professionals in identifying the steps that adversaries follow in order to accomplish their goals.

The cyber kill chain is a framework developed for securing cyberspace based on the concept of military kill chains. This method aims to actively enhance intrusion detection and response. The cyber kill chain is equipped with a seven-phase protection mechanism to mitigate and reduce cyber threats.

According to Lockheed Martin, cyberattacks might occur in seven different phases, from reconnaissance to the final accomplishment of the objective. An understanding of cyber kill chain methodology helps security professionals to leverage security controls at different stages of an attack and helps them to prevent the attack before it succeeds. It also provides greater insight into the attack phases, which helps in understanding the adversary's TTPs beforehand.

Discussed below are various phases included in cyber kill chain methodology:

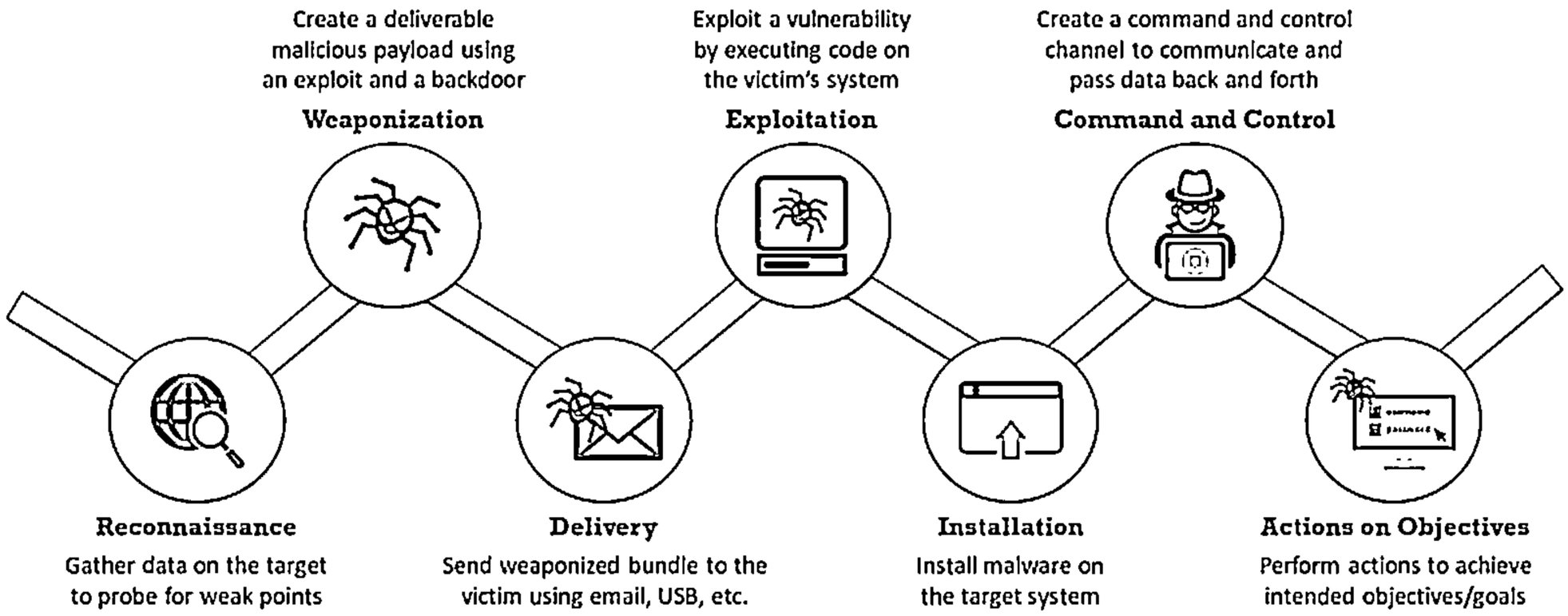


Figure 1.2: Cyber kill chain methodology

- **Reconnaissance**

  An adversary performs reconnaissance to collect as much information about the target as possible to probe for weak points before actually attacking. They look for information such as publicly available information on the Internet, network information, system information, and the organizational information of the target. By conducting reconnaissance across different network levels, the adversary can gain information such as network blocks, specific IP addresses, and employee details. The adversary may use automated tools such as open ports and services, vulnerabilities in applications, and login credentials, to obtain information. Such information can help the adversary in gaining backdoor access to the target network.

  Activities of the adversary include the following:

  - Gathering information about the target organization by searching the Internet or through social engineering
  - Performing analysis of various online activities and publicly available information
  - Gathering information from social networking sites and web services
  - Obtaining information about websites visited
  - Monitoring and analyzing the target organization's website
  - Performing Whois, DNS, and network footprinting
  - Performing scanning to identify open ports and services

- **Weaponization**

  The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware

weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary.

The following are the activities of the adversary:

- Identifying appropriate malware payload based on the analysis
- Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability
- Creating a phishing email campaign
- Leveraging exploit kits and botnets

- **Delivery**

  The previous stage included creating a weapon. Its payload is transmitted to the intended victim(s) as an email attachment, via a malicious link on websites, or through a vulnerable web application or USB drive. Delivery is a key stage that measures the effectiveness of the defense strategies implemented by the target organization based on whether the intrusion attempt of the adversary is blocked or not.

  The following are the activities of the adversary:

  - Sending phishing emails to employees of the target organization
  - Distributing USB drives containing malicious payload to employees of the target organization
  - Performing attacks such as watering hole on the compromised website
  - Implementing various hacking tools against the operating systems, applications, and servers of the target organization

- **Exploitation**

  After the weapon is transmitted to the intended victim, exploitation triggers the adversary's malicious code to exploit a vulnerability in the operating system, application, or server on a target system. At this stage, the organization may face threats such as authentication and authorization attacks, arbitrary code execution, physical security threats, and security misconfiguration.

  Activities of the adversary include the following:

  - Exploiting software or hardware vulnerabilities to gain remote access to the target system

- **Installation**

  The adversary downloads and installs more malicious software on the target system to maintain access to the target network for an extended period. They may use the weapon to install a backdoor to gain remote access. After the injection of the malicious code on one target system, the adversary gains the capability to spread the infection to other end systems in the network. Also, the adversary tries to hide the presence of malicious activities from security controls like firewalls using various techniques such as encryption.

  The following are the activities of the adversary:

  - Downloading and installing malicious software such as backdoors
  - Gaining remote access to the target system
  - Leveraging various methods to keep backdoor hidden and running
  - Maintaining access to the target system

- **Command and Control**

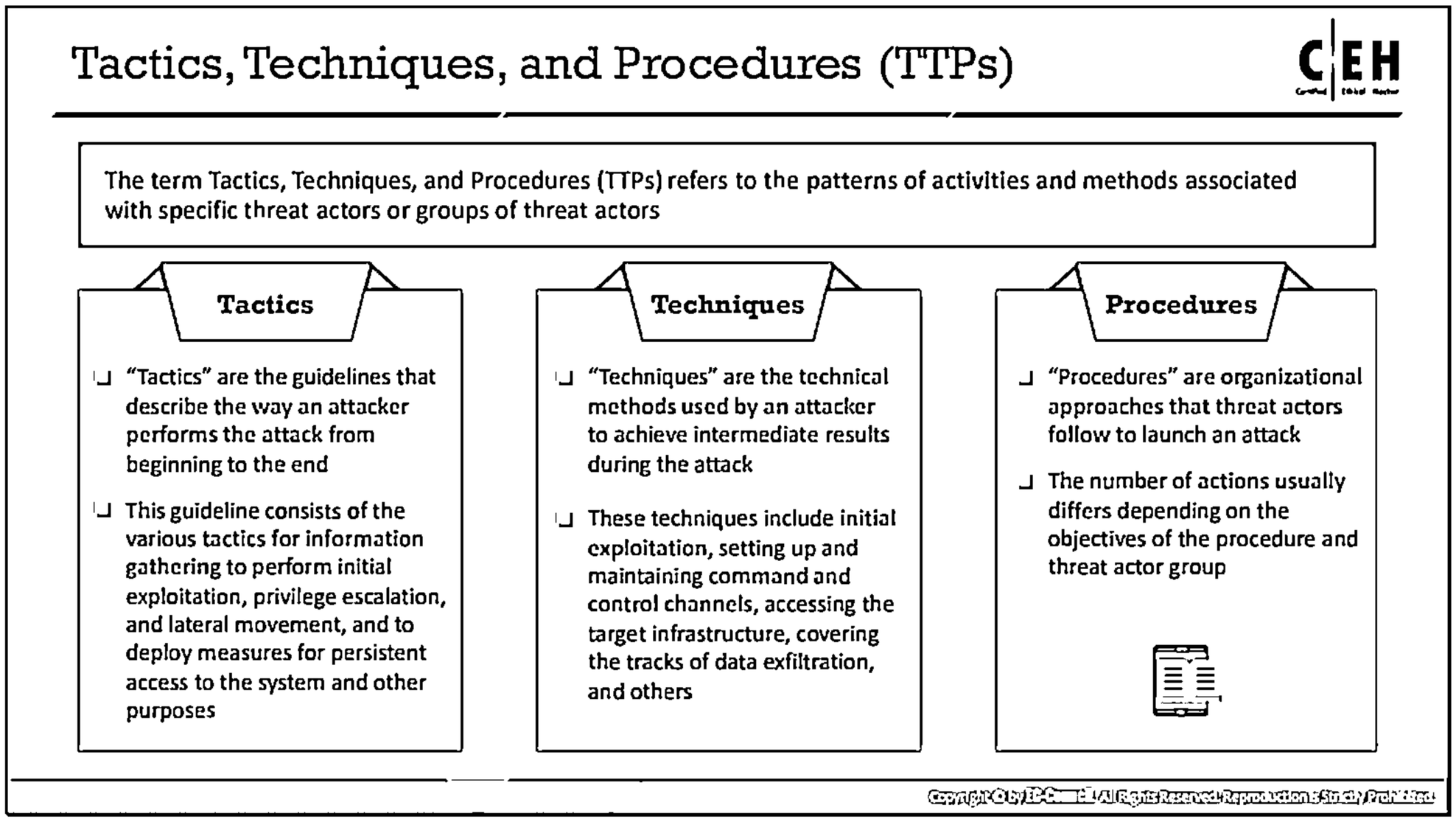
  The adversary creates a command and control channel, which establishes two-way communication between the victim's system and adversary-controlled server to communicate and pass data back and forth. The adversaries implement techniques such as encryption to hide the presence of such channels. Using this channel, the adversary performs remote exploitation on the target system or network.

  The following are the activities of the adversary:

  - Establishing a two-way communication channel between the victim's system and the adversary-controlled server
  - Leveraging channels such as web traffic, email communication, and DNS messages.
  - Applying privilege escalation techniques
  - Hiding any evidence of compromise using techniques such as encryption

- **Actions on Objectives**

  The adversary controls the victim's system from a remote location and finally accomplishes their intended goals. The adversary gains access to confidential data, disrupts the services or network, or destroys the operational capability of the target by gaining access to its network and compromising more systems. Also, the adversary may use this as a launching point to perform other attacks.



Tactics, Techniques, and Procedures (TTPs)

The terms "tactics, techniques, and procedures" refer to the patterns of activities and methods associated with specific threat actors or groups of threat actors. TTPs are helpful in analyzing threats and profiling threat actors and can further be used to strengthen the security infrastructure of an organization. The word "tactics" is defined as a guideline that describes the way an attacker performs their attack from beginning to end. The word "techniques" is defined as the technical methods used by an attacker to achieve intermediate results during their attack. Finally, the word "procedures" is defined as the organizational approach followed by the threat actors to launch their attack. In order to understand and defend against the threat actors, it is important to understand the TTPs used by adversaries. Understanding the tactics of an attacker helps to predict and detect evolving threats in the early stages. Understanding the techniques used by attackers helps to identify vulnerabilities and implement defensive measures in advance. Lastly, analyzing the procedures used by the attackers helps to identify what the attacker is looking for within the target organization's infrastructure.

Organizations should understand TTPs to protect their network against threat actors and upcoming attacks. TTPs enable the organizations to stop attacks at the initial stage, thereby protecting the network against massive damages.

- **Tactics**

  Tactics describe the way the threat actor operates during different phases of an attack. It consists of the various tactics used to gather information for the initial exploitation, perform privilege escalation and lateral movement, and deploy measures for persistence access to the system. Generally, APT groups depend on a certain set of unchanging tactics, but in some cases, they adapt to different circumstances and alter

the way they perform their attacks. Therefore, the difficulty of detecting and attributing the attack campaign depends on the tactics used to perform the attack.

An organization can profile threat actors based on tactics they use; this consists of the way they gather information about a target, the methods they follow for initial compromise, and the number of entry points they use while attempting to enter the target network.

For example, to obtain information, some threat actors depend solely on information available on the Internet, whereas others might perform social engineering or use connections in intermediate organizations. Once information such as the email addresses of employees of the target organization is gathered, the threat actors either choose to approach the target one by one or as a group. Furthermore, the attackers' designed payload can stay constant from the beginning to the end of the attack or may be changed based on the targeted individual. Therefore, to understand the threat actors better, tactics used in the early stages of an attack must be analyzed properly.

Another method of analyzing the APT groups is inspecting the infrastructure and tools used to perform their attack. For example, consider establishing a command and control channel on the servers controlled by the attacker. These C&C servers may be located within a specific geographical location or may spread across the Internet and can be static or can change dynamically. It is also important to analyze the tools used to perform the attack. This includes analyzing the exploits and tools used by various APT groups. In such a scenario, a sophisticated threat actor may exploit many zero-day vulnerabilities by using adapted tools and obfuscation methods. However, this might be difficult as less-sophisticated threat actors generally depend on publicly known vulnerabilities and open-source tools. Identifying this type of tactic helps in profiling the APT groups and building defensive measures in advance.

In some cases, understanding the tactics used in the last stages of an attack helps in profiling the threat actor. Also, the methods used to cover the tracks help the target organization understand attack campaigns. Analyzing the tactics used by the attackers helps in creating an initial profile by understanding different phases of an APT life cycle. This profile helps in performing further analysis of the techniques and procedures used by the attackers. An attacker may continually change the TTPs used, so it is important to constantly review and update the tactics used by the APT groups.

- **Techniques**

  To launch an attack successfully, threat actors use several techniques during its execution. These techniques include initial exploitation, setting up and maintaining command and control channels, accessing the target infrastructure, and covering the tracks of data exfiltration. The techniques followed by the threat actor to conduct an attack might vary, but they are mostly similar and can be used for profiling. Therefore, understanding the techniques used in the different phases of an attack is essential to analyzing the threat groups effectively.

Techniques can also be analyzed at each stage of the threat life cycle. Therefore, the techniques at the initial stage mainly describe the tools used for information gathering and initial exploitation. The techniques used in this stage need not necessarily have a technical aspect. For example, in social engineering, certain non-technical software tools are used as an effective way of gathering information. An attacker can use such tools to obtain the email addresses of target organization employees through publicly available resources.

In the same manner, purely human-based social engineering can be used to perform the initial exploitation. For example, consider a scenario where the victim is tricked via a phone call to reveal their login credentials for accessing the target organization's internal network. These techniques are used in the initial phase of an attack to gather information about the target and break the first line of defense.

Techniques used in the middle stages of an attack mostly depend on technical tools for initially escalating privileges on systems that are compromised or performing lateral movements within the target organization's network. At this stage of an attack, the attackers use various exploits or misuse configuration vulnerabilities on the target system. They may also exploit network design flaws to gain access to other systems in the network. In all of these cases, either exploits or a collection of tools allows the attacker to perform a successful attack. In this scenario, the term "technique" is the set of tools and the way they are used to obtain intermediate results during an attack campaign.

The techniques in the last stage of an attack can have both technical and nontechnical aspects. In such a scenario, the techniques used for data-stealing are usually based on network technology and encryption. For example, the threat actor encrypts the stolen files, transfers them through the established command and control channel, and copies them to their own system. After successfully executing the attack and transferring the files, the attacker follows certain purely technical techniques to cover their tracks. They use automated software tools to clear logs files to evade detection.

After aggregating the techniques used in all the stages of an attack, the organization can use the information to profile the threat actors. In order to make an accurate attribution of threat actors, the organization must observe all the techniques used by its adversaries.

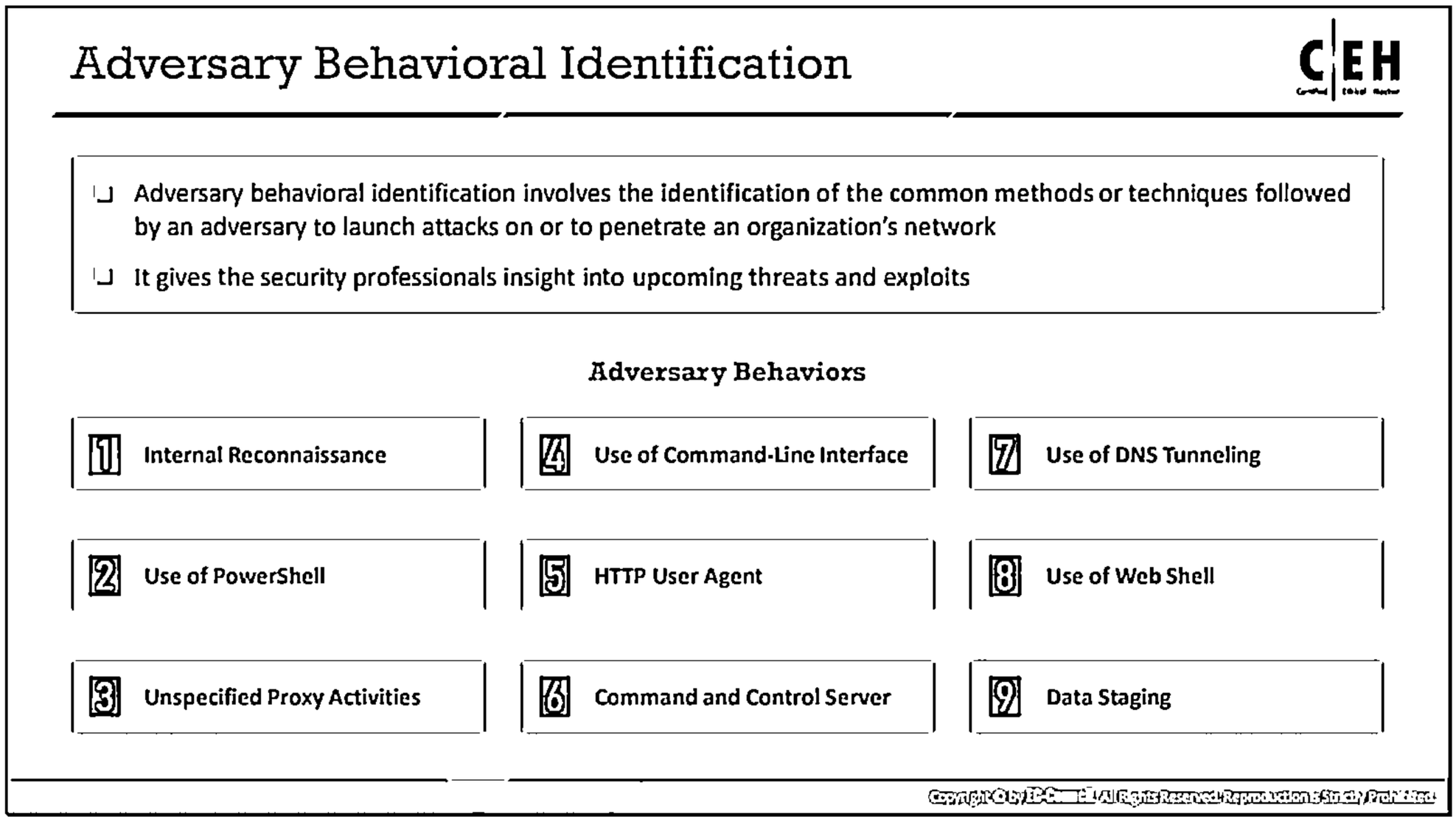
- **Procedures**

  "Procedures" involve a sequence of actions performed by the threat actors to execute different steps of an attack life cycle. The number of actions usually differs depending upon the objectives of the procedure and the APT group. An advanced threat actor uses advanced procedures that consist of more actions than a normal procedure to achieve the same intermediate result. This is done mainly to increase the success rate of an attack and decrease the probability of detection by security mechanisms.

  For example, in a basic procedure of information gathering, an actor collects information about the target organization; identifies key targets, employees; collects

their contact details, identifies vulnerable systems and potential entry points to the target network, and documents all the collected information. The further actions of an adversary depend on the tactics used. These actions include extensive research and repeated information gathering to collect in-depth and up-to-date information on the target individuals via social networking sites. This information can assist threat actors in performing spear phishing, monitoring security controls to identify zero-day exploits in the target systems, and other tasks. For example, a threat actor using a more detailed procedure executes the malware payload. At the time of execution, the malicious code decrypts itself, evades security monitoring controls, deploys persistence, and establishes a command and control channel for communicating with the victim system. This type of procedure is common for malware, where different threat actors may implement the same feature, and hence it is useful in forensic investigations.

An understanding and proper analysis of the procedures followed by certain threat actors during an attack helps organizations profile threat actors. In the initial stage of an attack, such as during information gathering, observing the procedure of an APT group is difficult. However, the later stages of an attack can leave trails that may be used to understand the procedures the attacker followed.



Adversary Behavioral Identification

Adversary behavioral identification involves the identification of the common methods or techniques followed by an adversary to launch attacks to penetrate an organization's network. It gives security professionals insight into upcoming threats and exploits. It helps them plan network security infrastructure and adapt a range of security procedures as prevention against various cyberattacks.

Given below are some of the behaviors of an adversary that can be used to enhance the detection capabilities of security devices:

- **Internal Reconnaissance**

  Once the adversary is inside the target network, they follow various techniques and methods to carry out internal reconnaissance. This includes the enumeration of systems, hosts, processes, the execution of various commands to find out information such as the local user context and system configuration, hostname, IP addresses, active remote systems, and programs running on the target systems. Security professionals can monitor the activities of an adversary by checking for unusual commands executed in the Batch scripts and PowerShell and by using packet capturing tools.

- **Use of PowerShell**

  PowerShell can be used by an adversary as a tool for automating data exfiltration and launching further attacks. To identify the misuse of PowerShell in the network, security professionals can check PowerShell's transcript logs or Windows Event logs. The user agent string and IP addresses can also be used to identify malicious hosts who try to exfiltrate data.

- **Unspecified Proxy Activities**

  An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains. Using this data feed, the security professionals can also find any malicious files downloaded and the unsolicited communication with the outside network based on the domains.

- **Use of Command-Line Interface**

  On gaining access to the target system, an adversary can make use of the command-line interface to interact with the target system, browse the files, read file content, modify file content, create new accounts, connect to the remote system, and download and install malicious code. Security professionals can identify this behavior of an adversary by checking the logs for process ID, processes having arbitrary letters and numbers, and malicious files downloaded from the Internet.

- **HTTP User Agent**

  In HTTP-based communication, the server identifies the connected HTTP client using the user agent field. An adversary modifies the content of the HTTP user agent field to communicate with the compromised system and to carry further attacks. Therefore, security professionals can identify this attack at an initial stage by checking the content of the user agent field.

- **Command and Control Server**

  Adversaries use command and control servers to communicate remotely with compromised systems through an encrypted session. Using this encrypted channel, the adversary can steal data, delete data, and launch further attacks. Security professionals can detect compromised hosts or networks by identifying the presence of a command and control server by tracking network traffic for outbound connection attempts, unwanted open ports, and other anomalies.

- **Use of DNS Tunneling**

  Adversaries use DNS tunneling to obfuscate malicious traffic in the legitimate traffic carried by common protocols used in the network. Using DNS tunneling, an adversary can also communicate with the command and control server, bypass security controls, and perform data exfiltration. Security professionals can identify DNS tunneling by analyzing malicious DNS requests, DNS payload, unspecified domains, and the destination of DNS requests.

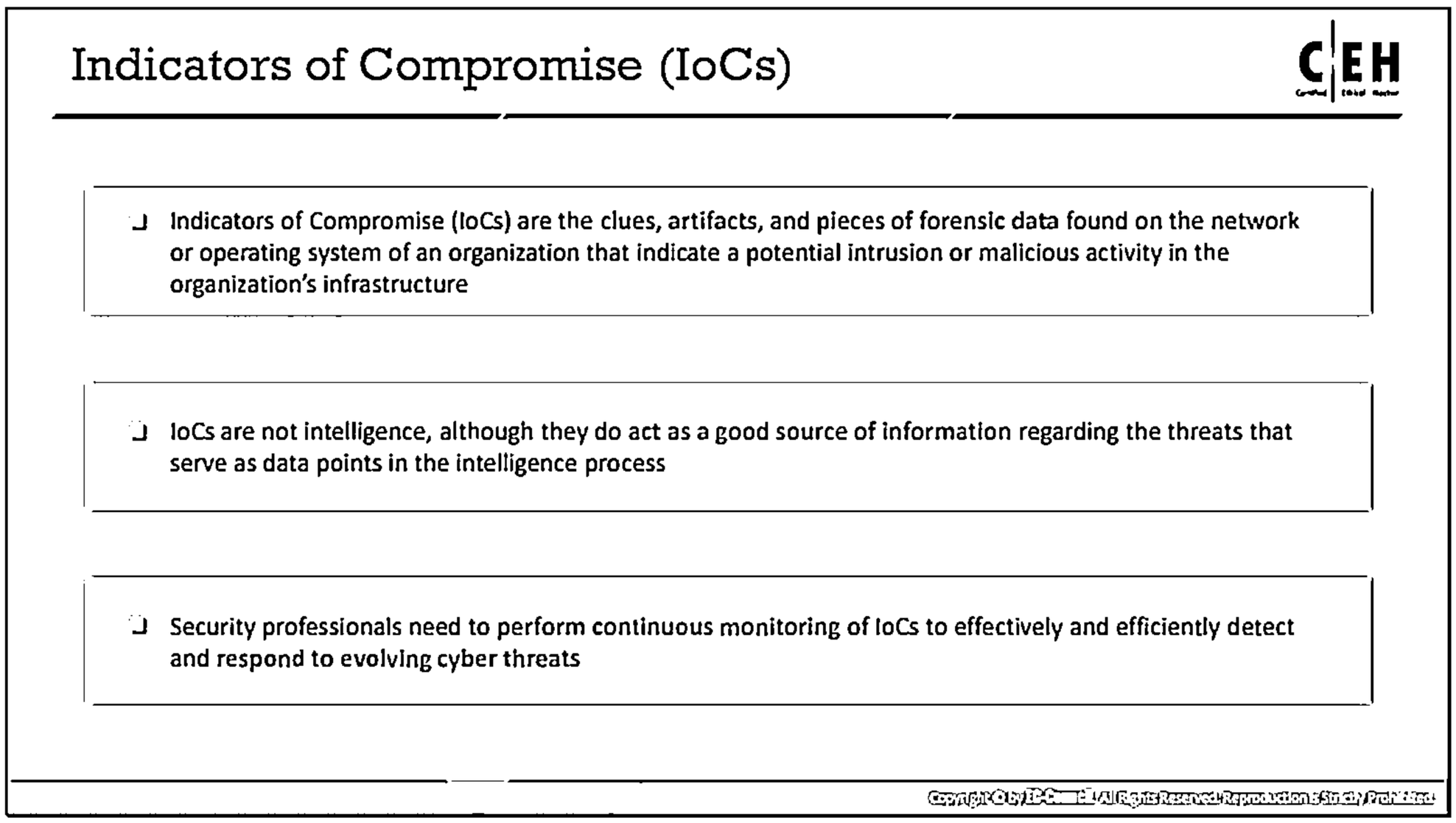
- **Use of Web Shell**

  An adversary uses a web shell to manipulate the web server by creating a shell within a website; it allows an adversary to gain remote access to the functionalities of a server. Using a web shell, an adversary performs various tasks such as data exfiltration, file transfers, and file uploads. Security professionals can identify the web shell running in

the network by analyzing server access, error logs, suspicious strings that indicate encoding, user agent strings, and through other methods.

- **Data Staging**

  After successful penetration into a target's network, the adversary uses data staging techniques to collect and combine as much data as possible. The types of data collected by an adversary include sensitive data about the employees and customers, the business tactics of an organization, financial information, and network infrastructure information. Once collected, the adversary can either exfiltrate or destroy the data. Security professionals can detect data staging by monitoring network traffic for malicious file transfers, file integrity monitoring, and event logs.

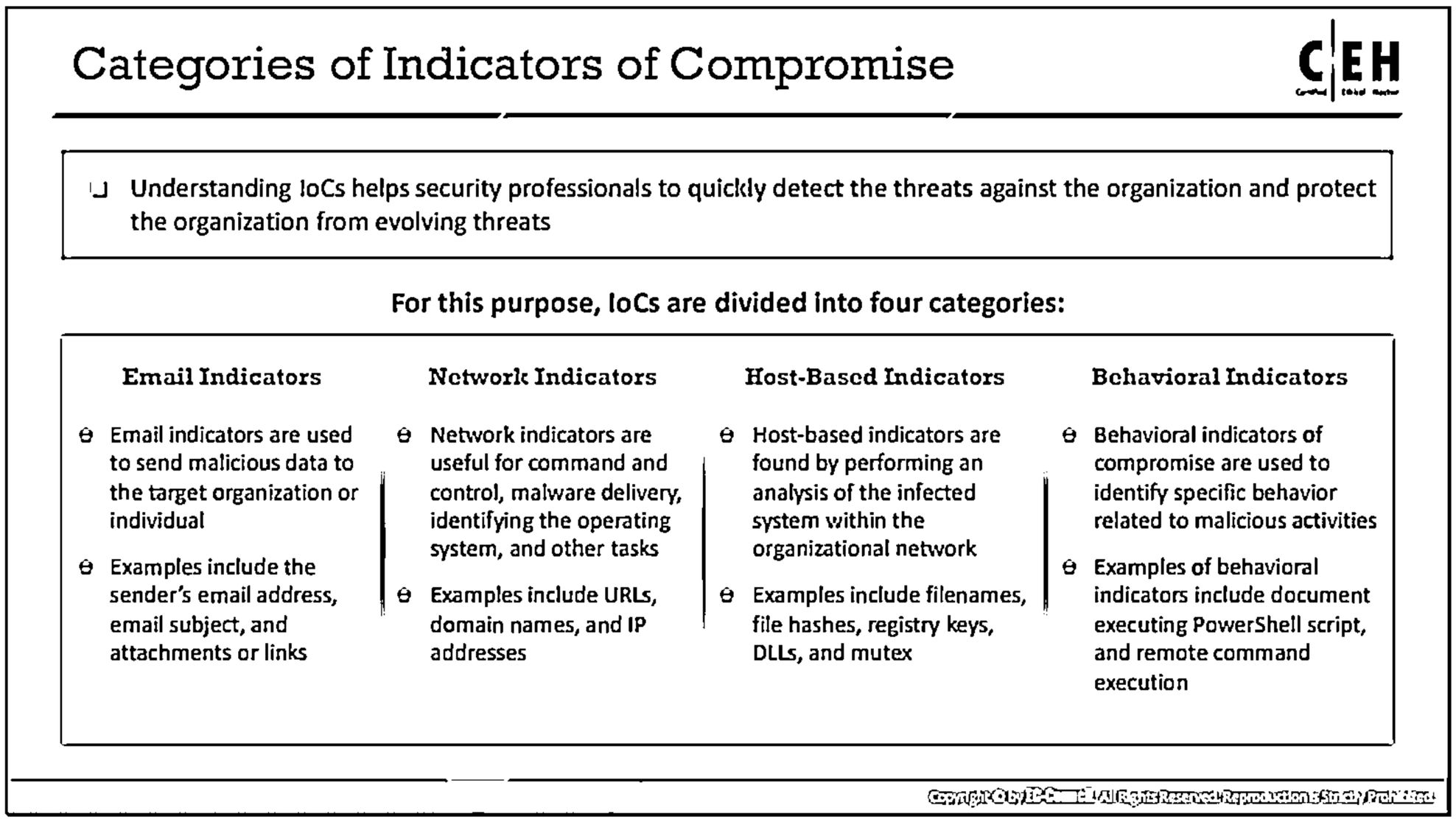


Indicators of Compromise (IoCs)

Cyber threats are continuously evolving with the newer TTPs adapted based on the vulnerabilities of the target organization. Security professionals must perform continuous monitoring of IoCs to effectively and efficiently detect and respond to evolving cyber threats. Indicators of Compromise are the clues, artifacts, and pieces of forensic data that are found on a network or operating system of an organization that indicate a potential intrusion or malicious activity in the organization's infrastructure.

However, IoCs are not intelligence; rather, IoCs act as a good source of information about threats that serve as data points in the intelligence process. Actionable threat intelligence extracted from IoCs helps organizations enhance incident-handling strategies. Cybersecurity professionals use various automated tools to monitor IoCs to detect and prevent various security breaches to the organization. Monitoring IoCs also helps security teams enhance the security controls and policies of the organization to detect and block suspicious traffic to thwart further attacks. To overcome the threats associated with IoCs, some organizations like STIX and TAXII have developed standardized reports that contain condensed data related to attacks and shared it with others to leverage the incident response.

An IoC is an atomic indicator, computed indicator, or behavioral indicator. It is the information regarding suspicious or malicious activities that is collected from various security establishments in a network's infrastructure. Atomic indicators are those that cannot be segmented into smaller parts, and whose meaning is not changed in the context of an intrusion. Examples of atomic indicators are IP addresses and email addresses. Computed indicators are obtained from the data extracted from a security incident. Examples of computed indicators are hash values and regular expressions. Behavioral indicators refer to a grouping of both atomic and computed indicators, combined on the basis of some logic.



Categories of Indicators of Compromise

The cybersecurity professionals must have proper knowledge about various possible threat actors and their tactics related to cyber threats, mostly called Indicators of Compromise (IoCs). This understanding of IoCs helps security professionals quickly detect the threats entering the organization and protect the organization from evolving threats. For this purpose, IoCs are divided into four categories:

- **Email Indicators**

  Attackers usually prefer email services to send malicious data to the target organization or individual. Such socially engineered emails are preferred due to their ease of use and comparative anonymity. Examples of email indicators include the sender's email address, email subject, and attachments or links.

- **Network Indicators**

  Network indicators are useful for command and control, malware delivery, and identifying details about the operating system, browser type, and other computer-specific information. Examples of network indicators include URLs, domain names, and IP addresses.

- **Host-Based Indicators**

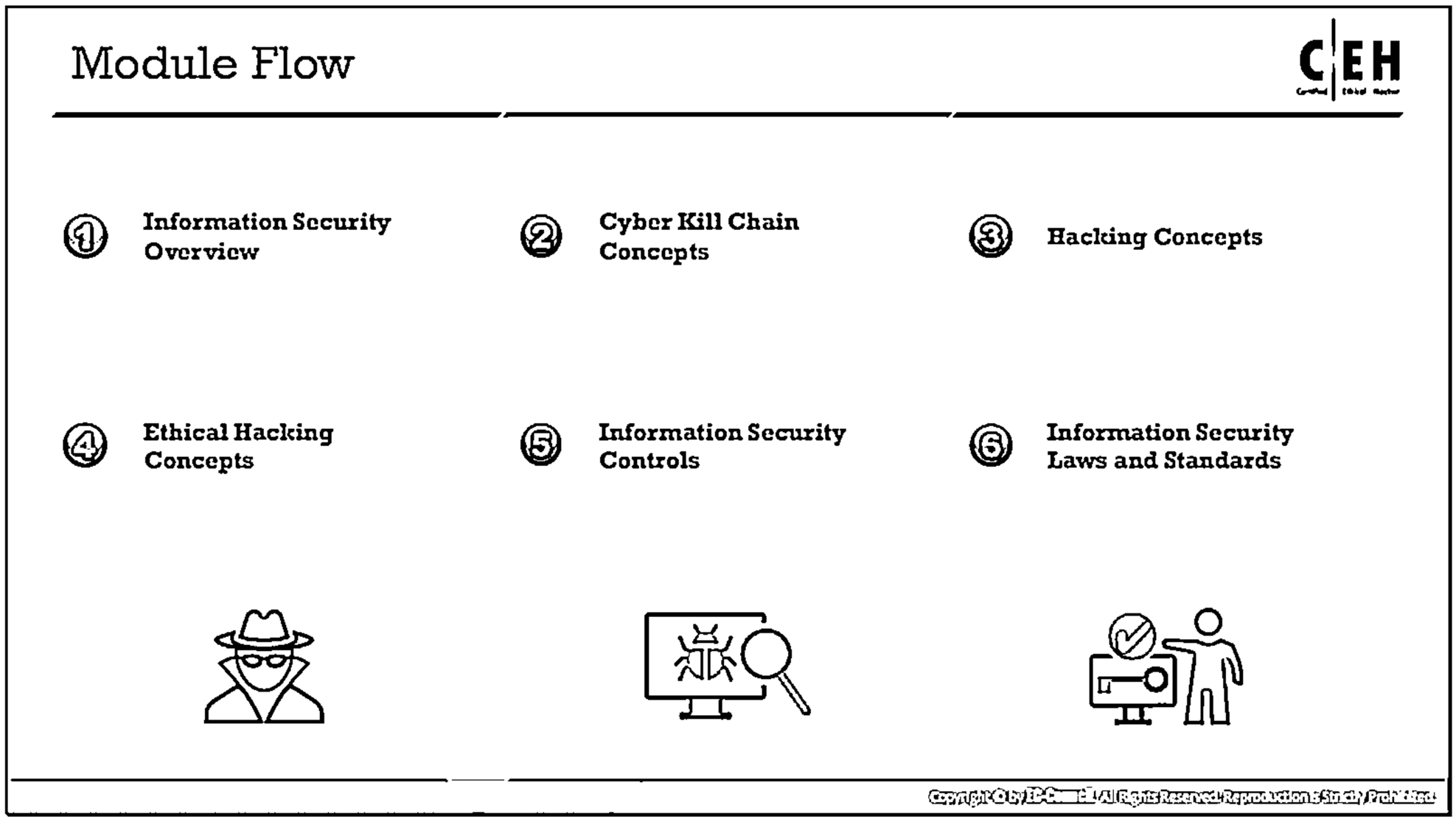
  Host-based indicators are found by performing an analysis of the infected system within the organizational network. Examples of host-based indicators include filenames, file hashes, registry keys, DLLs, and mutex.

- **Behavioral Indicators**

  Generally, typical IoCs are useful for identifying indications of intrusion, such as malicious IP addresses, virus signatures, MD5 hash, and domain names. Behavioral IoCs are used to identify specific behavior related to malicious activities such as code injection into the memory or running the scripts of an application. Well-defined behaviors enable broad protection to block all current and future malicious activities. These indicators are useful to identify when legitimate system services are used for abnormal or unexpected activities. Examples of behavioral indicators include document executing PowerShell script, and remote command execution.

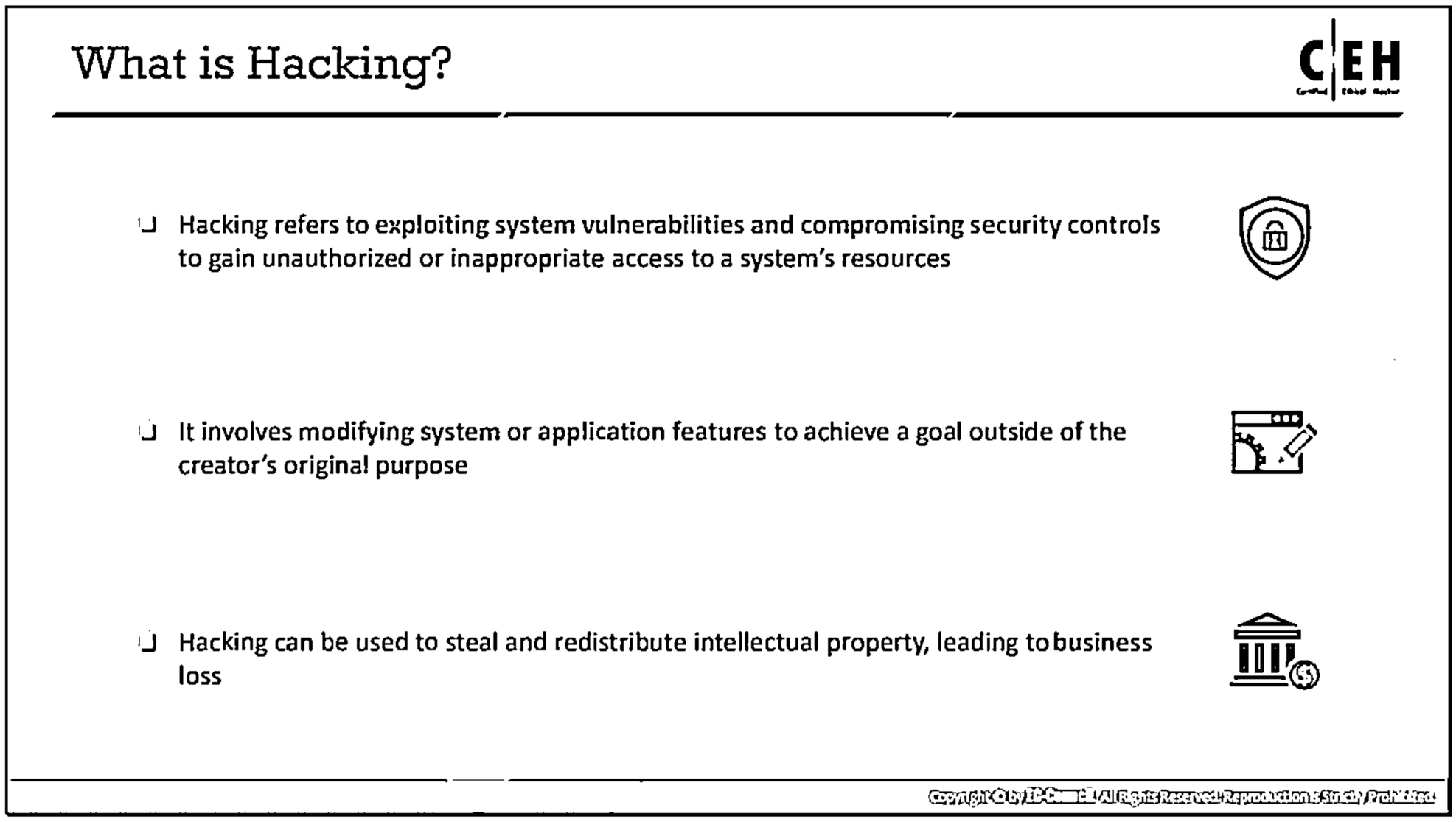
Listed below are some of the key Indicators of Compromise (IoCs):

- Unusual outbound network traffic
- Unusual activity through a privileged user account
- Geographical anomalies
- Multiple login failures
- Increased database read volume
- Large HTML response size
- Multiple requests for the same file
- Mismatched port-application traffic
- Suspicious registry or system file changes
- Unusual DNS requests
- Unexpected patching of systems
- Signs of Distributed Denial-of-Service (DDoS) activity
- Bundles of data in the wrong places
- Web traffic with superhuman behavior



Hacking Concepts

This section deals with basic concepts of hacking: what is hacking, who is a hacker, and hacker classes—the five distinct hacking phases that one should be familiar with before proceeding with ethical hacking methodology.



What is Hacking?

Hacking in the field of computer security refers to exploiting system vulnerabilities and compromising security controls to gain unauthorized or inappropriate access to system resources. It involves a modifying system or application features to achieve a goal outside its creator's original purpose. Hacking can be done to steal, pilfer, or redistribute intellectual property, thus leading to business loss.

Hacking on computer networks is generally done using scripts or other network programming. Network hacking techniques include creating viruses and worms, performing denial-of-service (DoS) attacks, establishing unauthorized remote access connections to a device using trojans or backdoors, creating botnets, packet sniffing, phishing, and password cracking. The motive behind hacking could be to steal critical information or services, for thrill, intellectual challenge, curiosity, experiment, knowledge, financial gain, prestige, power, peer recognition, vengeance and vindictiveness, among other reasons.

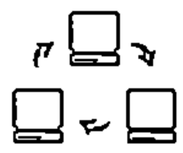
Who is a Hacker?

01

An intelligent individual with excellent computer skills who can create and explore computer software and hardware

02

For some hackers, hacking is a hobby to see how many computers or networks they can compromise



03

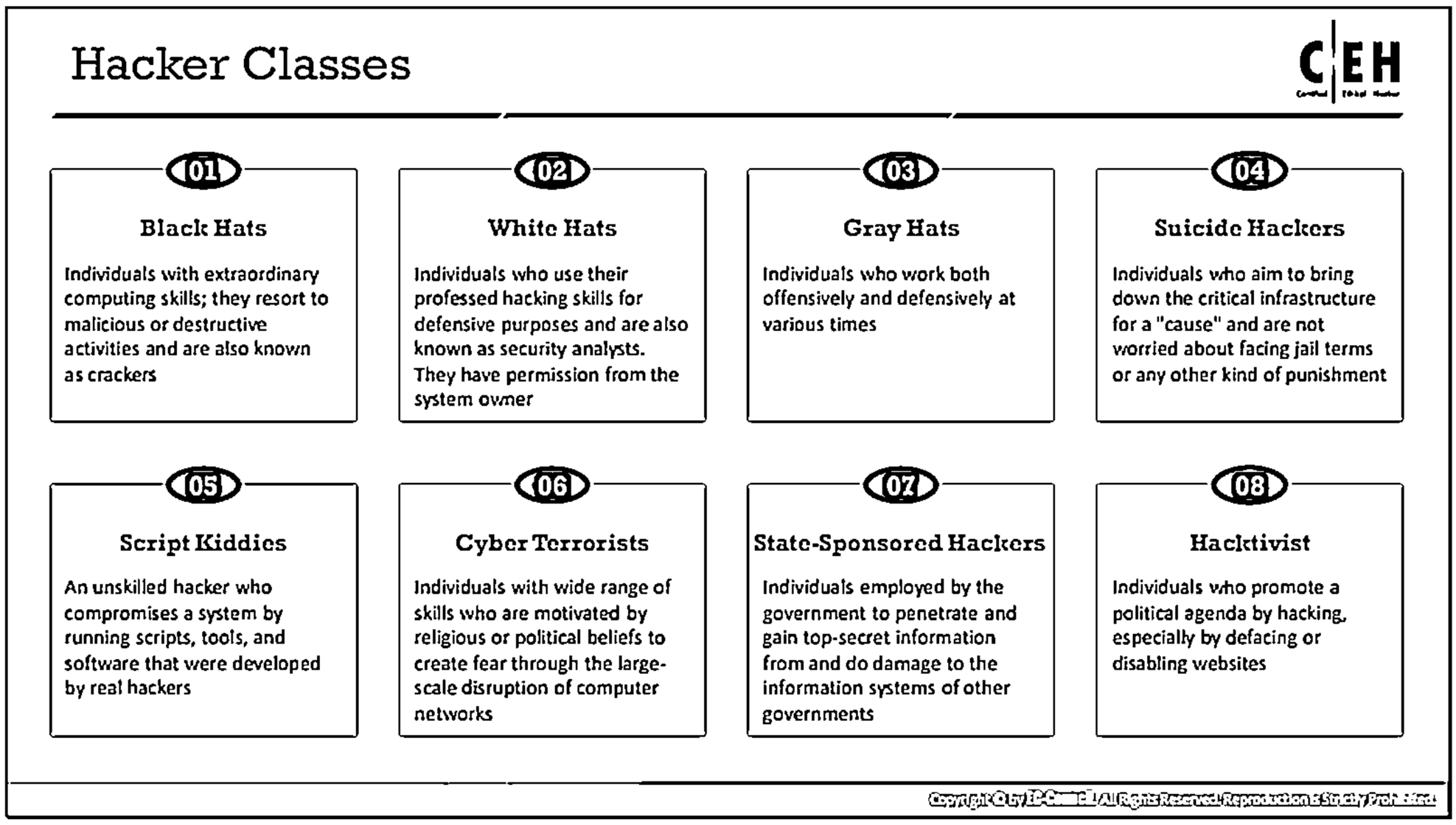
Some hackers' intentions can either be to gain knowledge or to probe and do illegal things

Some hack with malicious intent such as to steal business data, credit card information, social security numbers, email passwords, and other sensitive data

Who is a Hacker?

A hacker is a person who breaks into a system or network without authorization to destroy, steal sensitive data, or perform malicious attacks. A hacker is an intelligent individual with excellent computer skills, along with the ability to create and explore the computer's software and hardware. Usually, a hacker is a skilled engineer or programmer with enough knowledge to discover vulnerabilities in a target system. They generally have subject expertise and enjoy learning the details of various programming languages and computer systems.

For some hackers, hacking is a hobby to see how many computers or networks they can compromise. Their intention can either be to gain knowledge or to poke around to do illegal things. Some hack with malicious intent behind their escapades, like stealing business data, credit card information, social security numbers, and email passwords.



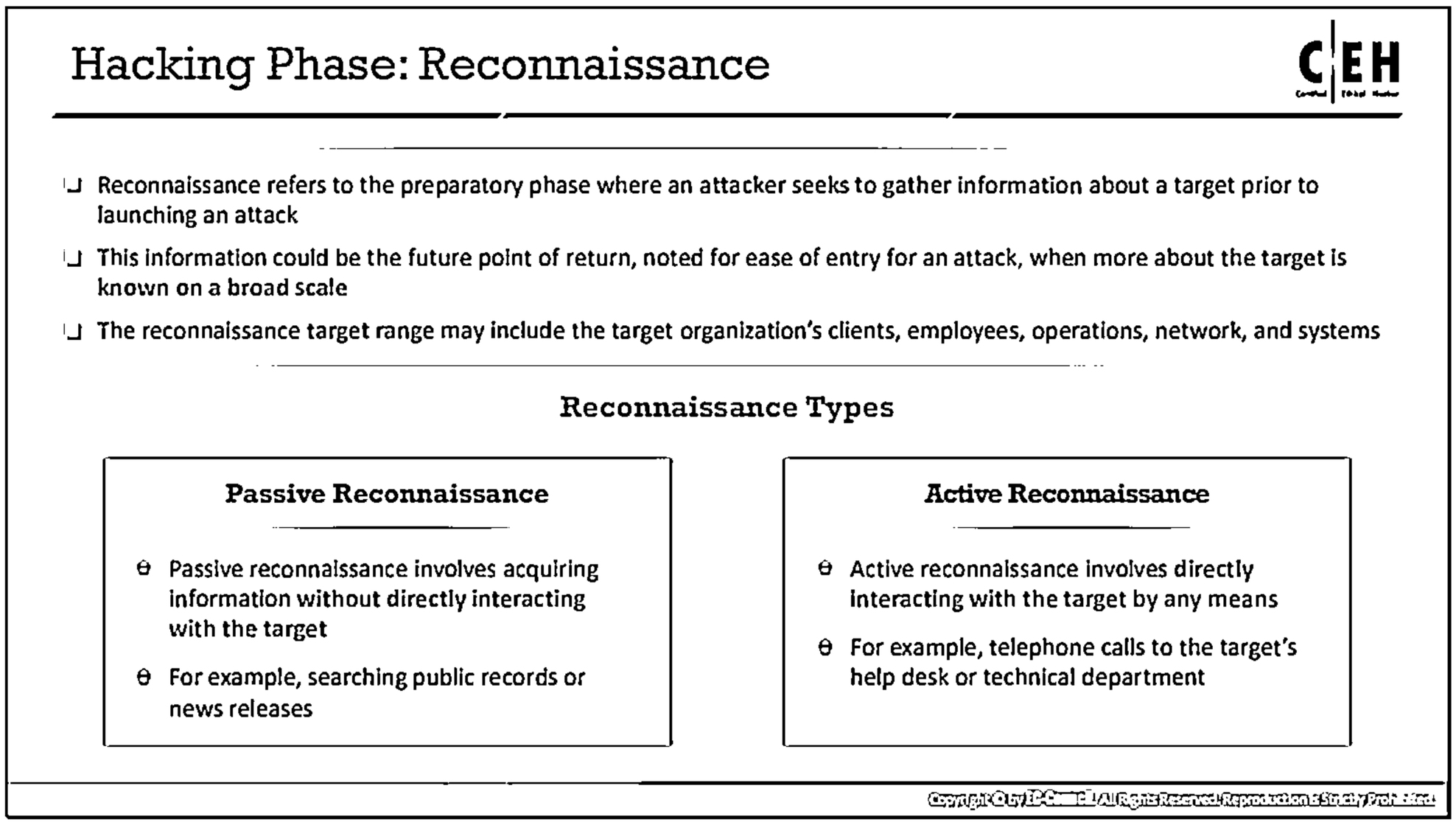
Hacker Classes

Hackers usually fall into one of the following categories, according to their activities:

- **Black Hats**: Black hats are individuals who use their extraordinary computing skills for illegal or malicious purposes. This category of hacker is often involved in criminal activities. They are also known as crackers.
- **White Hats**: White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner.
- **Gray Hats**: Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure.
- **Suicide Hackers**: Suicide hackers are individuals who aim to bring down critical infrastructure for a “cause” and are not worried about facing jail terms or any other kind of punishment. Suicide hackers are similar to suicide bombers who sacrifice their life for an attack and are thus not concerned with the consequences of their actions.
- **Script Kiddies**: Script kiddies are unskilled hackers who compromise systems by running scripts, tools, and software developed by real hackers. They usually focus on the quantity rather than the quality of the attacks that they initiate.

- **Cyber Terrorists**: Cyber terrorists are individuals with a wide range of skills, motivated by religious or political beliefs, to create fear of large-scale disruption of computer networks.
- **State-Sponsored Hackers**: State-sponsored hackers are individuals employed by the government to penetrate, gain top-secret information from, and damage the information systems of other governments.
- **Hacktivist**: Hacktivism is when hackers break into government or corporate computer systems as an act of protest. Hacktivists use hacking to increase awareness of their social or political agendas, as well as to boost their own reputations in both the online and offline arenas. They are individuals who use hacking to promote a political agenda, especially by defacing or disabling websites.

  Common hacktivist targets include government agencies, multinational corporations, and any other entity that they perceive as a threat. Irrespective of the hacktivists' intentions, the gaining of unauthorized access is a crime.



Hacking Phases

In general, there are five phases of hacking:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Clearing Tracks

Hacking Phase: Reconnaissance

Reconnaissance refers to the preparatory phase in which an attacker gathers as much information as possible about the target prior to launching the attack. In this phase, the attacker draws on competitive intelligence to learn more about the target. It could be the future point of return, noted for ease of entry for an attack when more about the target is known on a broad scale. The reconnaissance target range may include the target organization's clients, employees, operations, network, and systems.

This phase allows attackers to plan the attack. It may take some time as the attacker gathers as much information as possible. Part of this reconnaissance may involve social engineering. A social engineer is a person who convinces people to reveal information such as unlisted phone numbers, passwords, and other sensitive information. For instance, the hacker could call the target's Internet service provider and, using personal information previously obtained, convince the customer service representative that the hacker is actually the target, and in doing so, obtain even more information about the target.

Another reconnaissance technique is dumpster diving. Dumpster diving is, simply enough, looking through an organization's trash for any discarded sensitive information. Attackers can use the Internet to obtain information such as employees' contact information, business partners, technologies currently in use, and other critical business knowledge. Dumpster diving may even provide attackers with even more sensitive information, such as usernames, passwords, credit card statements, bank statements, ATM receipts, Social Security numbers, private telephone numbers, checking account numbers, or other sensitive data.

Searching for the target company's web site in the Internet's Whois database can easily provide hackers with the company's IP addresses, domain names, and contact information.

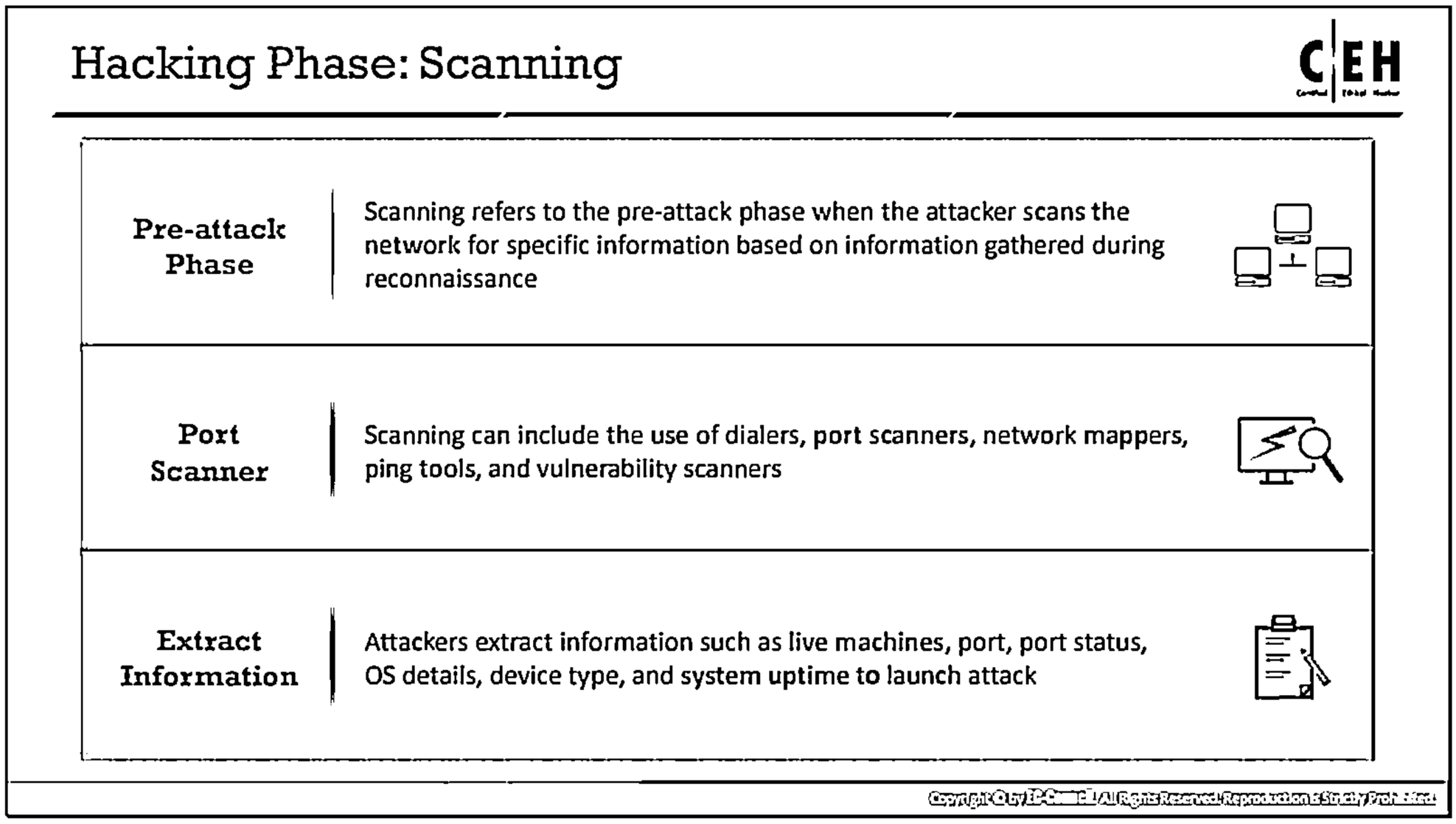
Reconnaissance Types

Reconnaissance techniques are broadly categorized into active and passive.

When an attacker is using passive reconnaissance techniques, they do not interact with the target directly. Instead, the attacker relies on publicly available information, news releases, or other no-contact methods.

Active reconnaissance techniques, on the other hand, involve direct interactions with the target system by using tools to detect open ports, accessible hosts, router locations, network mapping, details of operating systems, and applications. Attackers use active reconnaissance when there is a low probability of the detection of these activities. For example, they may make telephone calls to the help desk or technical department.

As an ethical hacker, it is important to be able to distinguish among the various reconnaissance methods and advocate preventive measures in the light of potential threats. Companies, on their part, must address security as an integral part of their business and operational strategies, and be equipped with the proper policies and procedures to check for potential vulnerabilities.



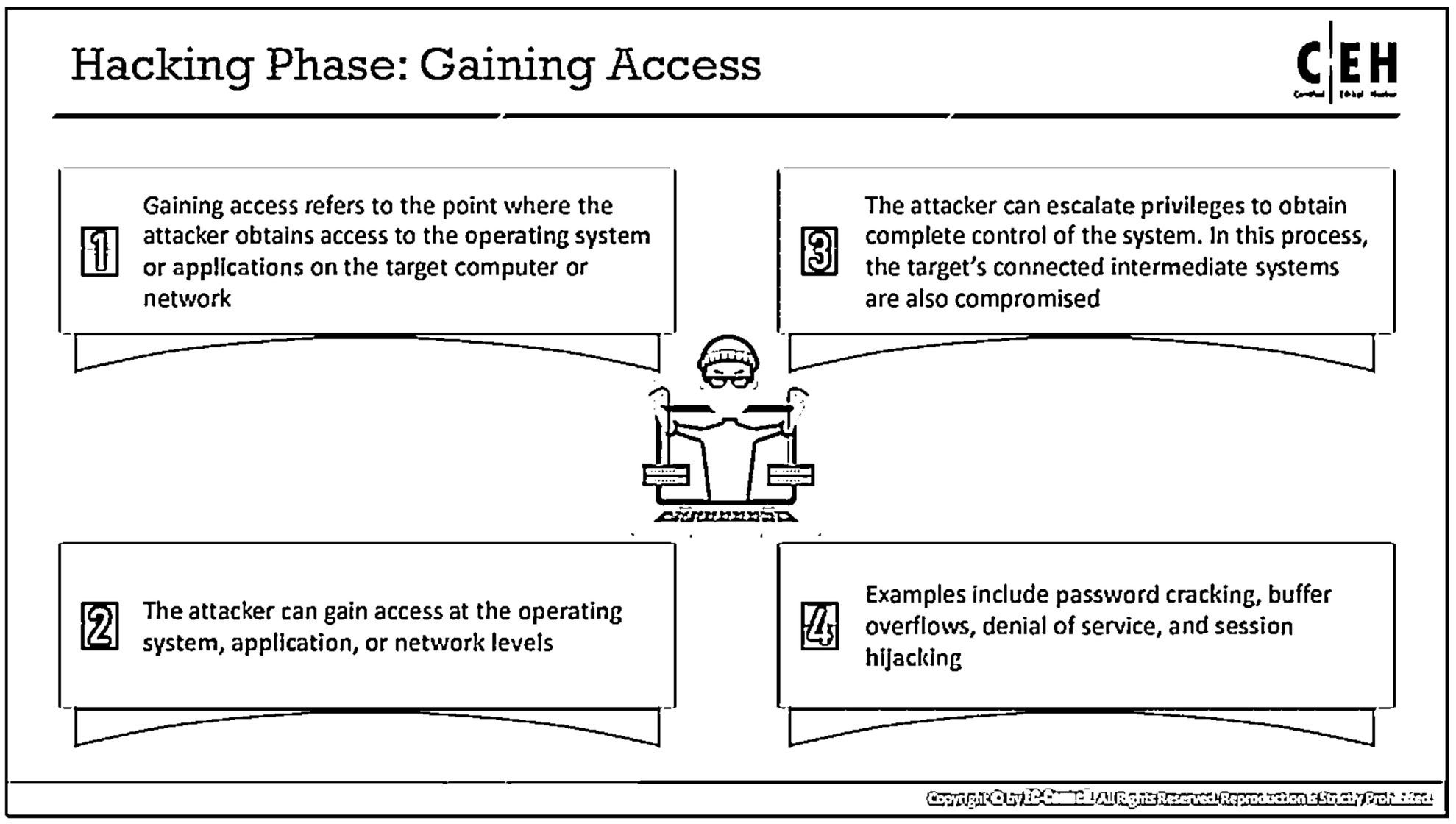
Hacking Phase: Scanning

Scanning is the phase immediately preceding the attack. Here, the attacker uses the details gathered during reconnaissance to scan the network for specific information. Scanning is a logical extension of active reconnaissance, and in fact, some experts do not differentiate scanning from active reconnaissance. There is a slight difference, however, in that scanning involves more in-depth probing on the part of the attacker. Often the reconnaissance and scanning phases overlap, and it is not always possible to separate the two. An attacker can gather critical network information such as the mapping of systems, routers, and firewalls by using simple tools such as the standard Windows utility Traceroute. Alternatively, they can use tools such as Cheops to add additional information to Traceroute's results.

Scanning can include the use of dialers, port scanners, network mappers, ping tools, vulnerability scanners, or other tools. Attackers extract information such as live machines, port, port status, OS details, device type, and system uptime to launch an attack.

Port scanners detect listening ports to find information about the nature of services running on the target machine. The primary defense technique against port scanners is shutting down services that are not required and implementing appropriate port filtering. However, attackers can still use tools to determine the rules implemented by the port filtering.

The most commonly used tools are vulnerability scanners, which can search for thousands of known vulnerabilities on a target network. This gives the attacker an advantage because he or she only has to find a single means of entry, while the systems professional has to secure as much vulnerability as possible by applying patches. Organizations that use intrusion detection systems still have to remain vigilant because attackers can and will use evasion techniques wherever possible.

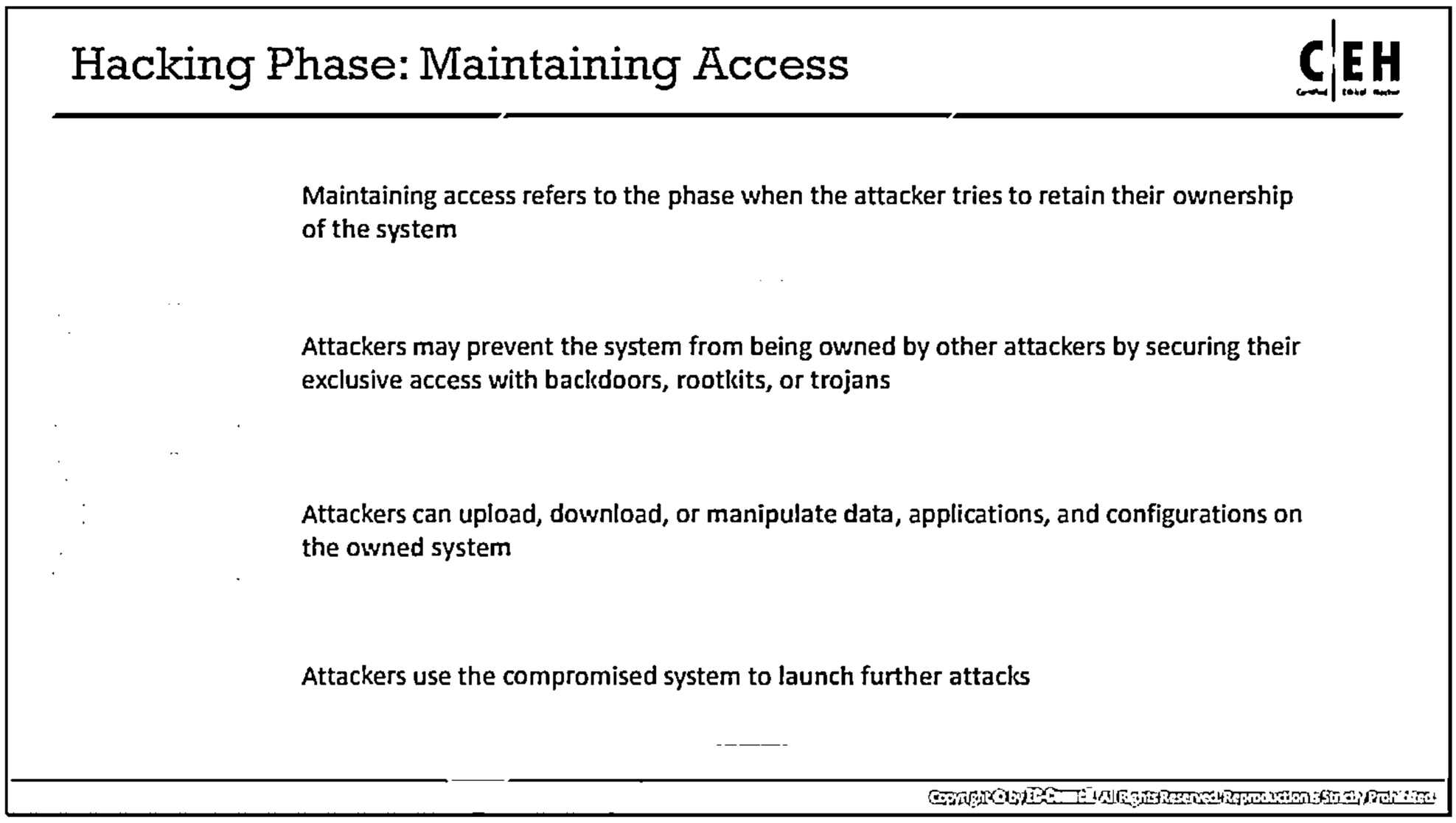


Hacking Phase: Gaining Access

This is the phase in which real hacking occurs. Attackers use vulnerabilities identified during the reconnaissance and scanning phases to gain access to the target system and network. Gaining access refers to the point where the attacker obtains access to the operating system or to applications on the computer or network. The attacker can gain access to the operating system, application, or network level. Even though attackers can cause plenty of damage without gaining any access to the system, the impact of unauthorized access is catastrophic. For instance, external denial-of-service attacks can either exhaust resources or stop services from running on the target system. Ending processes can stop a service, using a logic bomb or time bomb, or even reconfigure and crash the system. Furthermore, attackers can exhaust system and network resources by consuming all outgoing communication links.

Attackers gain access to the target system locally (offline), over a LAN, or the Internet. Examples include password cracking, stack-based buffer overflows, denial-of-service, and session hijacking. Using a technique called spoofing to exploit the system by pretending to be a legitimate user or different system, attackers can send a data packet containing a bug to the target system in order to exploit a vulnerability. Packet flooding also breaks the availability of essential services. Smurf attacks attempt to cause users on a network to flood each other with data, making it appear as if everyone is attacking each other, and leaving the hacker anonymous.

A hacker's chances of gaining access to a target system depend on several factors such as the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained. Once an attacker gains access to the target system, they then try to escalate privileges in order to take complete control. In the process, they also compromise the intermediate systems that are connected to it.

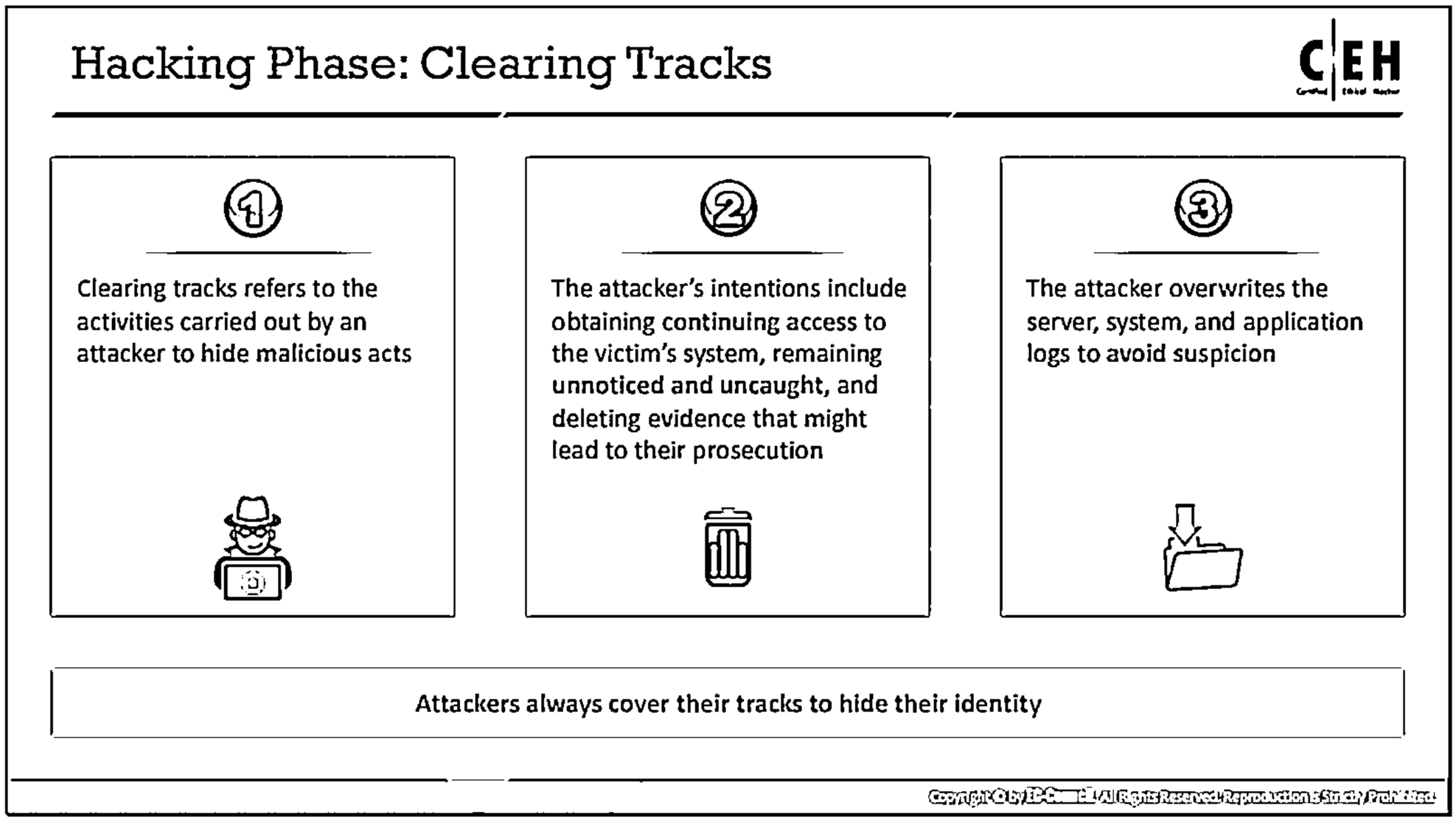


Hacking Phase: Maintaining Access

Maintaining access refers to the phase when the attacker tries to retain his or her ownership of the system. Once an attacker gains access to the target system with admin or root-level privileges (thus owning the system), they can use both the system and its resources at will. The attacker can either use the system as a launchpad to scan and exploit other systems or to keep a low profile and continue their exploitation. Both of these actions can cause a great amount of damage. For instance, the hacker could implement a sniffer to capture all network traffic, including Telnet and FTP (file transfer protocol) sessions with other systems, and then transmit that data wherever they please.

Attackers who choose to remain undetected remove evidence of their entry and install a backdoor or a trojan to gain repeat access. They can also install rootkits at the kernel level to gain full administrative access to the target computer. Rootkits gain access at the operating system level, while trojans gain access at the application level. Both rootkits and trojans require users to install them locally. In Windows systems, most trojans install themselves as a service and run as part of the local system with administrative access.

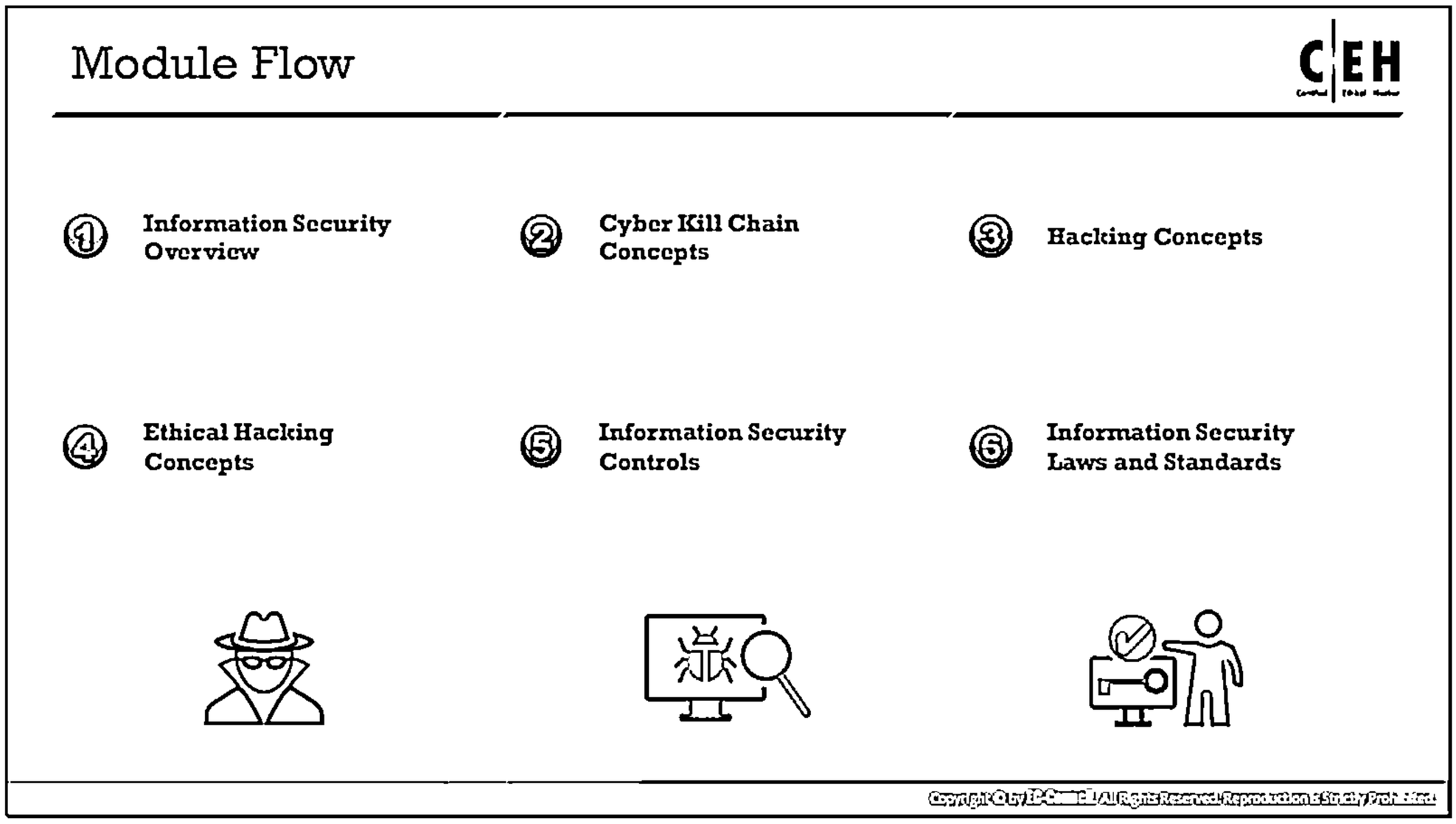
Attackers can upload, download, or manipulate data, applications, and configurations on the owned system and can also use trojans to transfer usernames, passwords, and any other information stored on the system. They can maintain control over the system for a long time by closing up vulnerabilities to prevent other hackers from taking control of them, and sometimes, in the process, render some degree of protection to the system from other attacks. Attackers use the compromised system to launch further attacks.



Hacking Phase: Clearing Tracks

For obvious reasons, such as avoiding legal trouble and maintaining access, attackers will usually attempt to erase all evidence of their actions. Clearing tracks refers to the activities carried out by an attacker to hide malicious acts. The attacker's intentions include continuing access to the victim's system, remaining unnoticed and uncaught, and deleting evidence that might lead to their own prosecution. They use utilities such as PsTools (*https://docs.microsoft.com*), Netcat, or trojans to erase their footprints from the system's log files. Once the trojans are in place, the attacker has most likely gained total control of the system and can execute scripts in the trojan or rootkit to replace the critical system and log files to hide their presence in the system. Attackers always cover their tracks to hide their identity.

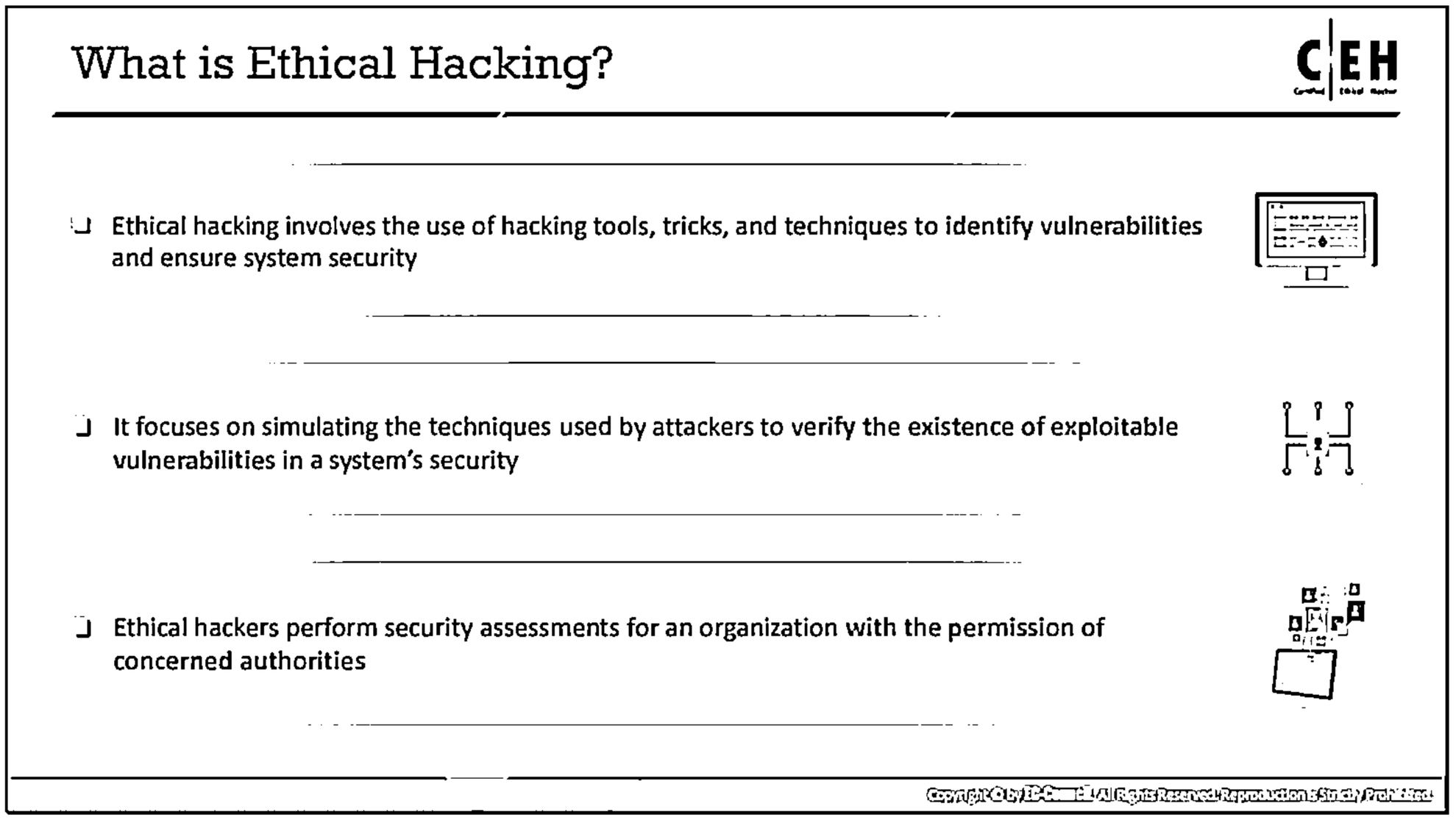
Other techniques include steganography and tunneling. Steganography is the process of hiding data in other data, for instance, in image and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Attackers can use even a small amount of extra space in the data packet's TCP and IP headers to hide information. An attacker can use the compromised system to launch new attacks against other systems or as a means of reaching another system on the network undetected. Thus, this phase of the attack can turn into another attack's reconnaissance phase. System administrators can deploy host-based IDS (intrusion detection systems) and antivirus software in order to detect trojans and other seemingly compromised files and directories. An ethical hacker must be aware of the tools and techniques that attackers deploy so that they can advocate and implement the countermeasures detailed in subsequent modules.



Ethical Hacking Concepts

An ethical hacker follows processes similar to those of a malicious hacker. The steps to gain and maintain access to a computer system are similar irrespective of the hacker's intentions.

This section provides an overview of ethical hacking, why ethical hacking is necessary, the scope and limitations of ethical hacking, and the skills of an ethical hacker.



What is Ethical Hacking?

Ethical hacking is the practice of employing computer and network skills in order to assist organizations in testing their network security for possible loopholes and vulnerabilities. White Hats (also known as security analysts or ethical hackers) are the individuals or experts who perform ethical hacking. Nowadays, most organizations (such as private companies, universities, and government organizations) are hiring White Hats to assist them in enhancing their cybersecurity. They perform hacking in ethical ways, with the permission of the network or system owner and without the intention to cause harm. Ethical hackers report all vulnerabilities to the system and network owner for remediation, thereby increasing the security of an organization's information system. Ethical hacking involves the use of hacking tools, tricks, and techniques typically used by an attacker to verify the existence of exploitable vulnerabilities in system security.

Today, the term hacking is closely associated with illegal and unethical activities. There is continuing debate as to whether hacking can be ethical or not, given the fact that unauthorized access to any system is a crime. Consider the following definitions:

- The noun "hacker" refers to a person who enjoys learning the details of computer systems and stretching their capabilities.
- The verb "to hack" describes the rapid development of new programs or the reverse engineering of existing software to make it better or more efficient in new and innovative ways.
- The terms "cracker" and "attacker" refer to persons who employ their hacking skills for offensive purposes.

- The term "ethical hacker" refers to security professionals who employ their hacking skills for defensive purposes.

Most companies employ IT professionals to audit their systems for known vulnerabilities. Although this is a beneficial practice, crackers are usually more interested in using newer, lesser-known vulnerabilities, and so these by-the-numbers system audits do not suffice. A company needs someone who can think like a cracker, keep up with the newest vulnerabilities and exploits, and recognize potential vulnerabilities where others cannot. This is the role of the ethical hacker.

Ethical hackers usually employ the same tools and techniques as hackers, with the important exception that they do not damage the system. They evaluate system security, update the administrators regarding any discovered vulnerabilities, and recommend procedures for patching those vulnerabilities.

The important distinction between ethical hackers and crackers is consent. Crackers attempt to gain unauthorized access to systems, while ethical hackers are always completely open and transparent about what they are doing and how they are doing it. Ethical hacking is, therefore, always legal.

Why Ethical Hacking is Necessary

To beat a hacker, you need to think like one!

Ethical hacking is necessary as it allows for counter attacks against malicious hackers through anticipating the methods used to break into the system

Reasons why organizations recruit ethical hackers

- To prevent hackers from gaining access to the organization's information systems
- To provide adequate preventive measures in order to avoid security breaches
- To uncover vulnerabilities in systems and explore their potential as a security risk
- To help safeguard customer data
- To analyze and strengthen an organization's security posture, including policies, network protection infrastructure, and end-user practices
- To enhance security awareness at all levels in a business

Why Ethical Hacking is Necessary (Cont'd)

Ethical Hackers Try to Answer the Following Questions

1. What can an intruder see on the target system? (Reconnaissance and Scanning phases)
2. What can an intruder do with that information? (Gaining Access and Maintaining Access phases)
3. Does anyone at the target organization notice the intruders' attempts or successes? (Reconnaissance and Covering Tracks phases)
4. Are all components of the information system adequately protected, updated, and patched?
5. How much time, effort, and money are required to obtain adequate protection?
6. Are the information security measures in compliance with legal and industry standards?

Why Ethical Hacking is Necessary

As technology is growing at a faster pace, so is the growth in the risks associated with it. To beat a hacker, it is necessary to think like one!

Ethical hacking is necessary as it allows to counter attacks from malicious hackers by anticipating methods used by them to break into a system. Ethical hacking helps to predict various possible vulnerabilities well in advance and rectify them without incurring any kind of

outside attack. As hacking involves creative thinking, vulnerability testing, and security audits alone cannot ensure that the network is secure. To achieve security, organizations must implement a "defense-in-depth" strategy by penetrating their networks to estimate and expose vulnerabilities.

Reasons why organizations recruit ethical hackers

- To prevent hackers from gaining access to the organization's information systems
- To uncover vulnerabilities in systems and explore their potential as a risk
- To analyze and strengthen an organization's security posture, including policies, network protection infrastructure, and end-user practices
- To provide adequate preventive measures in order to avoid security breaches
- To help safeguard the customer data
- To enhance security awareness at all levels in a business

An ethical hacker's evaluation of a client's information system security seeks to answer three basic questions:

1. **What can an attacker see on the target system?**

   Normal security checks by system administrators will often overlook vulnerabilities. The ethical hacker has to think about what an attacker might see during the reconnaissance and scanning phases of an attack.

2. **What can an intruder do with that information?**

   The ethical hacker must discern the intent and purpose behind attacks to determine appropriate countermeasures. During the gaining-access and maintaining-access phases of an attack, the ethical hacker needs to be one step ahead of the hacker in order to provide adequate protection.

3. **Are the attackers' attempts being noticed on the target systems?**

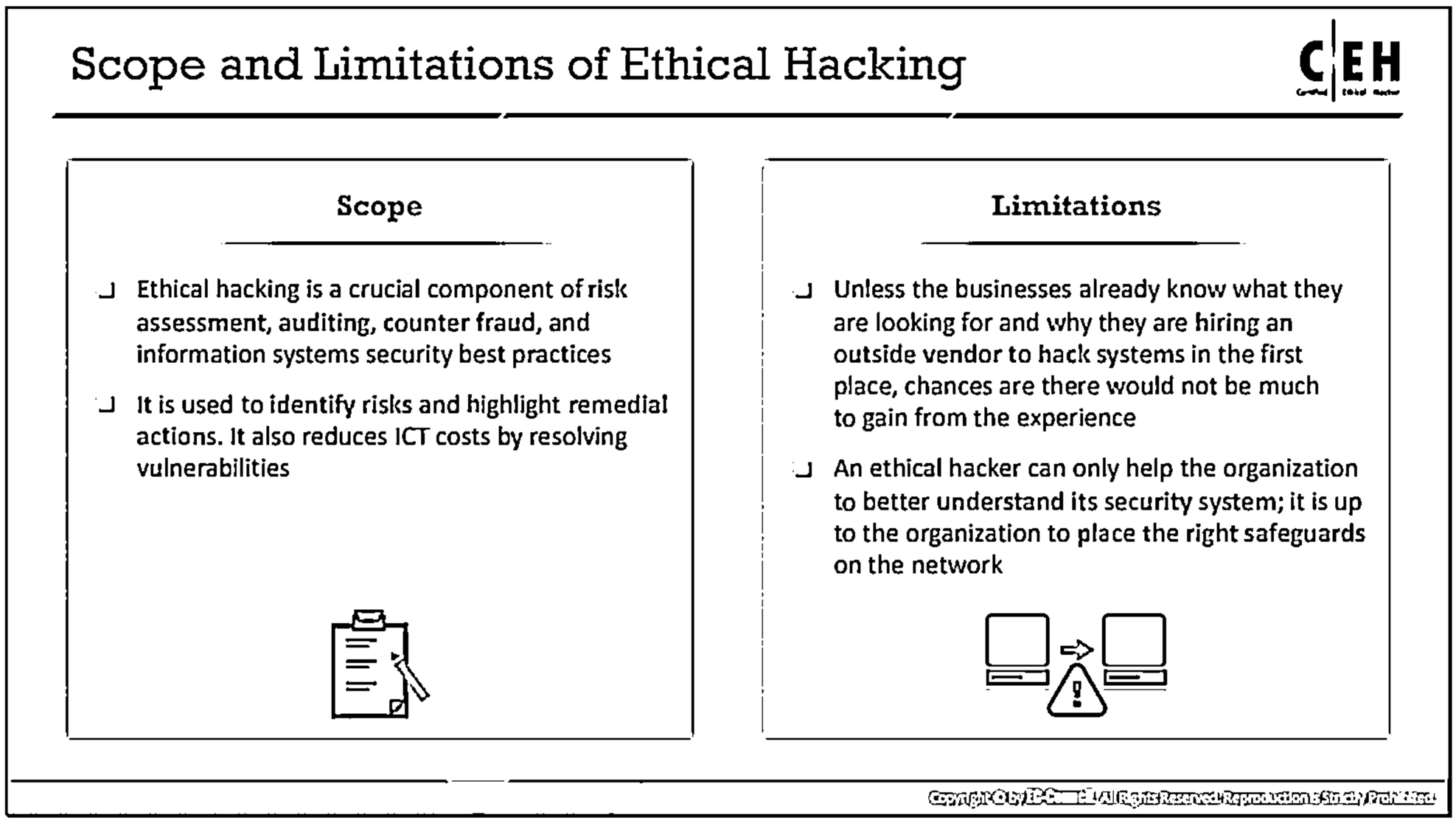
   Sometimes attackers will try to breach a system for days, weeks, or even months. Other times they will gain access but will wait before doing anything damaging. Instead, they will take the time to assess the potential use of exposed information. During the reconnaissance and covering tracks phases, the ethical hacker should notice and stop the attack.

After carrying out attacks, hackers may clear their tracks by modifying log files and creating backdoors, or by deploying trojans. Ethical hackers must investigate whether such activities have been recorded and what preventive measures have been taken. This not only provides them with an assessment of the attacker's proficiency but also gives them insight into the existing security measures of the system being evaluated. The entire process of ethical hacking and subsequent patching of discovered vulnerabilities depends on questions such as:

- What is the organization trying to protect?
- Against whom or what are they trying to protect it?

- Are all the components of the information system adequately protected, updated, and patched?
- How much time, effort, and money is the client willing to invest to gain adequate protection?
- Do the information security measures comply with industry and legal standards?

Sometimes, in order to save on resources or prevent further discovery, the client might decide to end the evaluation after the first vulnerability is found; therefore, it is important that the ethical hacker and the client work out a suitable framework for investigation beforehand. The client must be convinced of the importance of these security exercises through concise descriptions of what is happening and what is at stake. The ethical hacker must also remember to convey to the client that it is never possible to guard systems completely, but that they can always be improved.



Scope and Limitations of Ethical Hacking

Security experts broadly categorize computer crimes into two categories: crimes facilitated by a computer and those in which the computer is the target.

Ethical hacking is a structured and organized security assessment, usually as part of a penetration test or security audit, and is a crucial component of risk assessment, auditing, counter fraud, and information systems security best practices. It is used to identify risks and highlight remedial actions. It is also used to reduce Information and Communications Technology (ICT) costs by resolving vulnerabilities.

Ethical hackers determine the scope of the security assessment according to the client's security concerns. Many ethical hackers are members of a "Tiger Team." A tiger team works together to perform a full-scale test covering all aspects of the network, as well as physical and system intrusion.

An ethical hacker should know the penalties of unauthorized hacking into a system. No ethical hacking activities associated with a network-penetration test or security audit should begin before receiving a signed legal document giving the ethical hacker express permission to perform the hacking activities from the target organization. Ethical hackers must be judicious with their hacking skills and recognize the consequences of misusing those skills.

The ethical hacker must follow certain rules to fulfill their ethical and moral obligations. They must do the following:

- Gain authorization from the client and have a signed contract giving the tester permission to perform the test.
- Maintain confidentiality when performing the test and follow a Nondisclosure Agreement (NDA) with the client for the confidential information disclosed during the

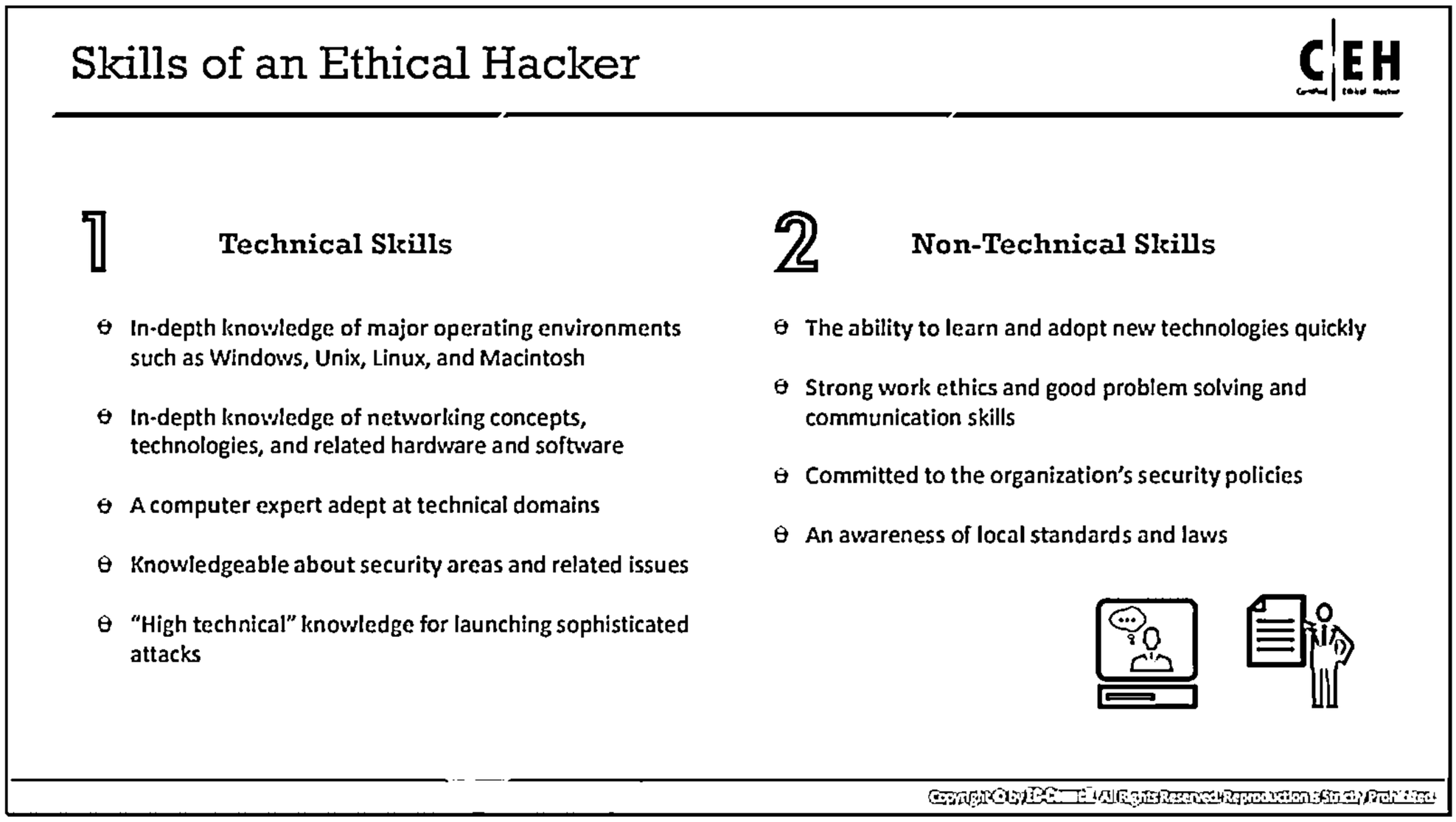
test. The information gathered might contain sensitive information, and the ethical hacker must not disclose any information about the test or the confidential company data to a third party.

- Perform the test up to but not beyond the agreed-upon limits. For example, ethical hackers should perform DoS attacks only if they have previously agreed upon this with the client. Loss of revenue, goodwill, and worse consequences could befall an organization whose servers or applications are unavailable to customers because of the testing.

The following steps provide a framework for performing a security audit of an organization, which will help in ensuring that the test is organized, efficient, and ethical:

- Talk to the client and discuss the needs to be addressed during the testing
- Prepare and sign NDA documents with the client
- Organize an ethical hacking team and prepare the schedule for testing
- Conduct the test
- Analyze the results of the testing and prepare a report
- Present the report findings to the client

However, there are limitations too. Unless the businesses first know what they are looking for and why they are hiring an outside vendor to hack their systems in the first place, chances are there would not be much to gain from experience. An ethical hacker, thus, can only help the organization to better understand its security system. It is up to the organization to place the right safeguards on the network.

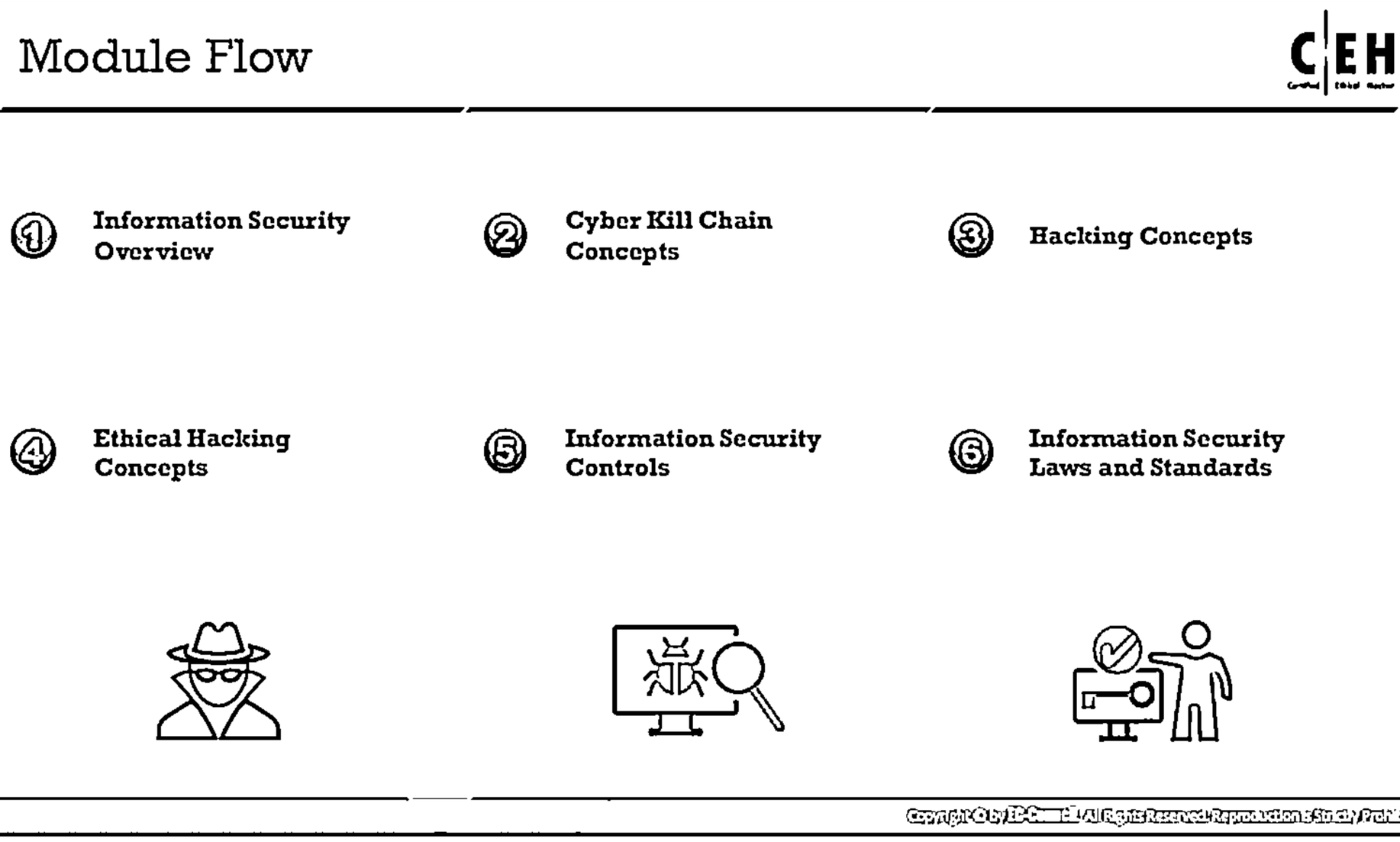


Skills of an Ethical Hacker

It is essential for an ethical hacker to acquire the knowledge and skills to become an expert hacker and to use this knowledge in a lawful manner. The technical and non-technical skills to be a good ethical hacker are discussed below:

- **Technical Skills**
  - In-depth knowledge of major operating environments, such as Windows, Unix, Linux, and Macintosh
  - In-depth knowledge of networking concepts, technologies, and related hardware and software
  - A computer expert adept at technical domains
  - The knowledge of security areas and related issues
  - High technical knowledge of how to launch sophisticated attacks
- **Non-Technical Skills**
  - The ability to quickly learn and adapt new technologies
  - A strong work ethic and good problem solving and communication skills
  - Commitment to an organization's security policies
  - An awareness of local standards and laws

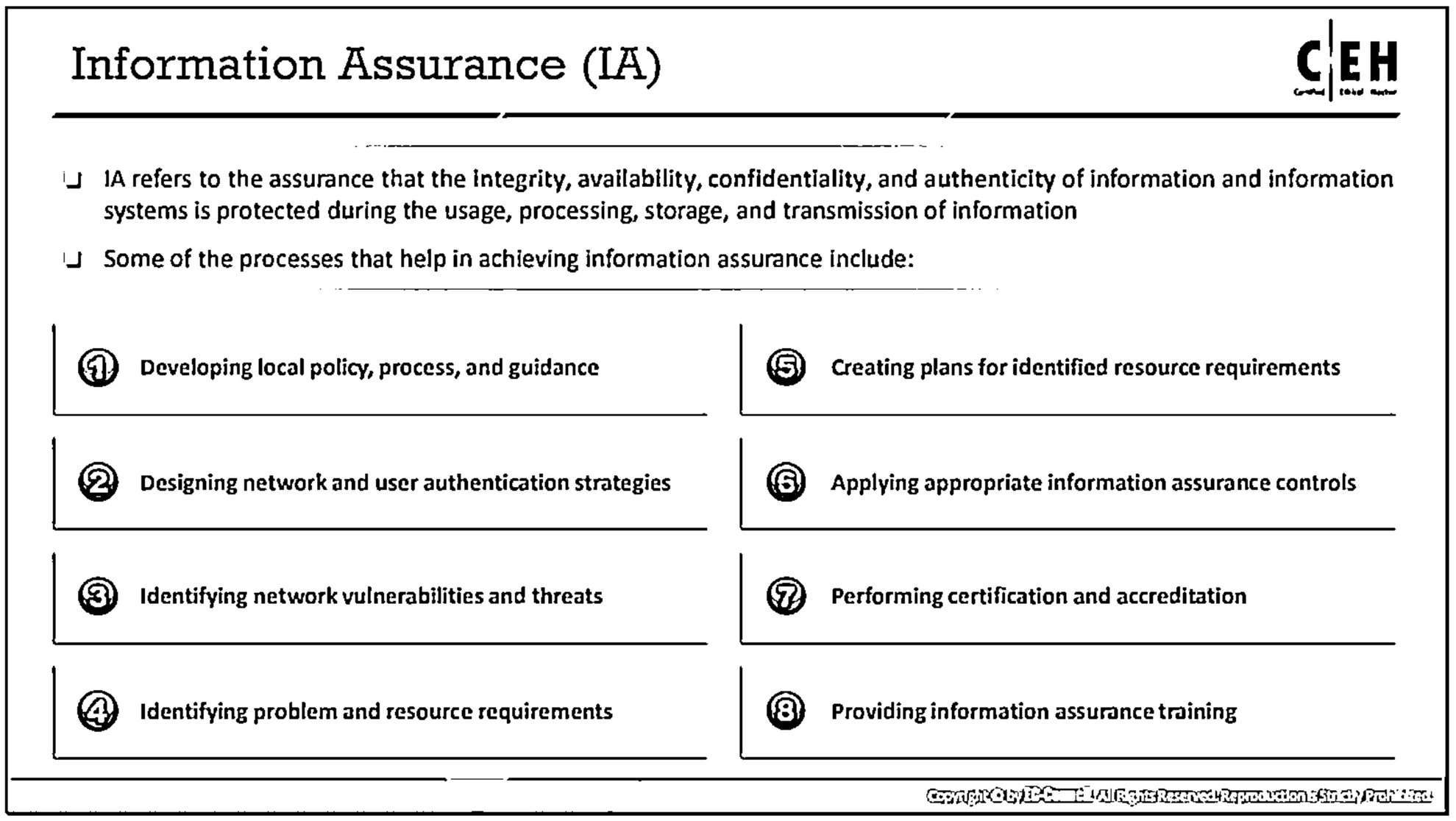
Module Flow



Information Security Controls

Information security controls prevent the occurrence of unwanted events and reduce risk to the organization's information assets. The basic security concepts critical to information on the Internet are confidentiality, integrity, and availability; the concepts related to the persons accessing the information are authentication, authorization, and non-repudiation. Information is the greatest asset of an organization. It must be secured using various policies, creating awareness, employing security mechanisms, or by other means.

This section deals with Information Assurance (IA), defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management, and AI and ML concepts.



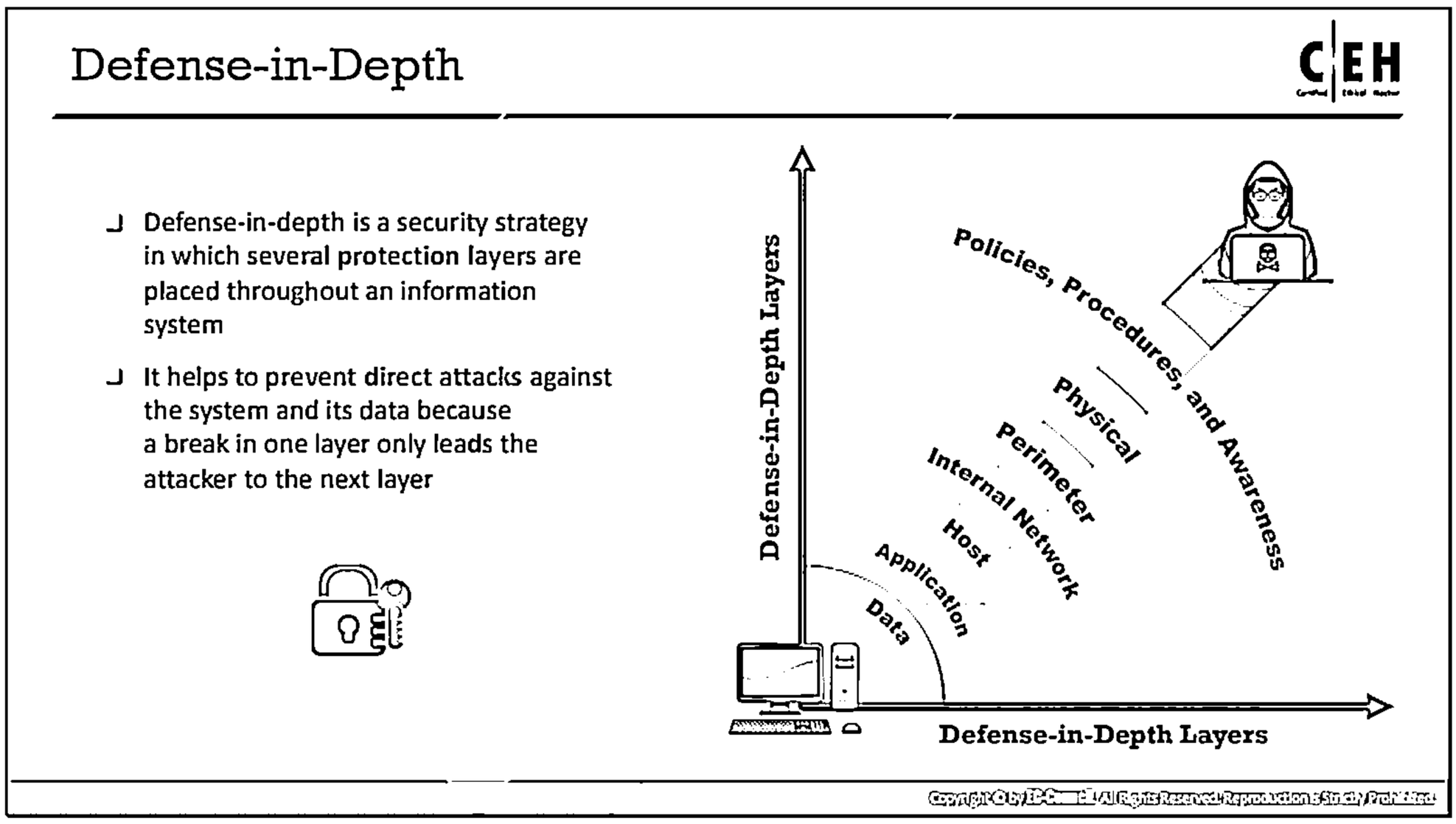
Information Assurance (IA)

IA refers to the assurance of the integrity, availability, confidentiality, and authenticity of information and information systems during the usage, processing, storage, and transmission of information. Security experts accomplish information assurance with the help of physical, technical, and administrative controls. Information Assurance and Information Risk Management (IRM) ensure that only authorized personnel access and use information. This helps in achieving information security and business continuity.

Some of the processes that help in achieving information assurance include:

- Developing local policy, process, and guidance in such a way to maintain the information systems at an optimum security level
- Designing network and user authentication strategy—Designing a secure network ensures the privacy of user records and other information on the network. Implementing an effective user authentication strategy secures the information system's data
- Identifying network vulnerabilities and threats—Vulnerability assessments outline the security posture of the network. Performing vulnerability assessments in search of network vulnerabilities and threats help to take the proper measures to overcome them
- Identifying problems and resource requirements
- Creating a plan for identified resource requirements
- Applying appropriate information assurance controls
- Performing the Certification and Accreditation (C&A) process of information systems helps to trace vulnerabilities, and implement safety measures to nullify them

- Providing information assurance training to all personnel in federal and private organizations brings among them an awareness of information technology



Defense-in-Depth

Defense-in-depth is a security strategy in which security professionals use several protection layers throughout an information system. This strategy uses the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier. Defense-in-depth helps to prevent direct attacks against an information system and its data because a break in one layer only leads the attacker to the next layer. If a hacker gains access to a system, defense-in-depth minimizes any adverse impact and gives administrators and engineers time to deploy new or updated countermeasures to prevent a recurrence of the intrusion.

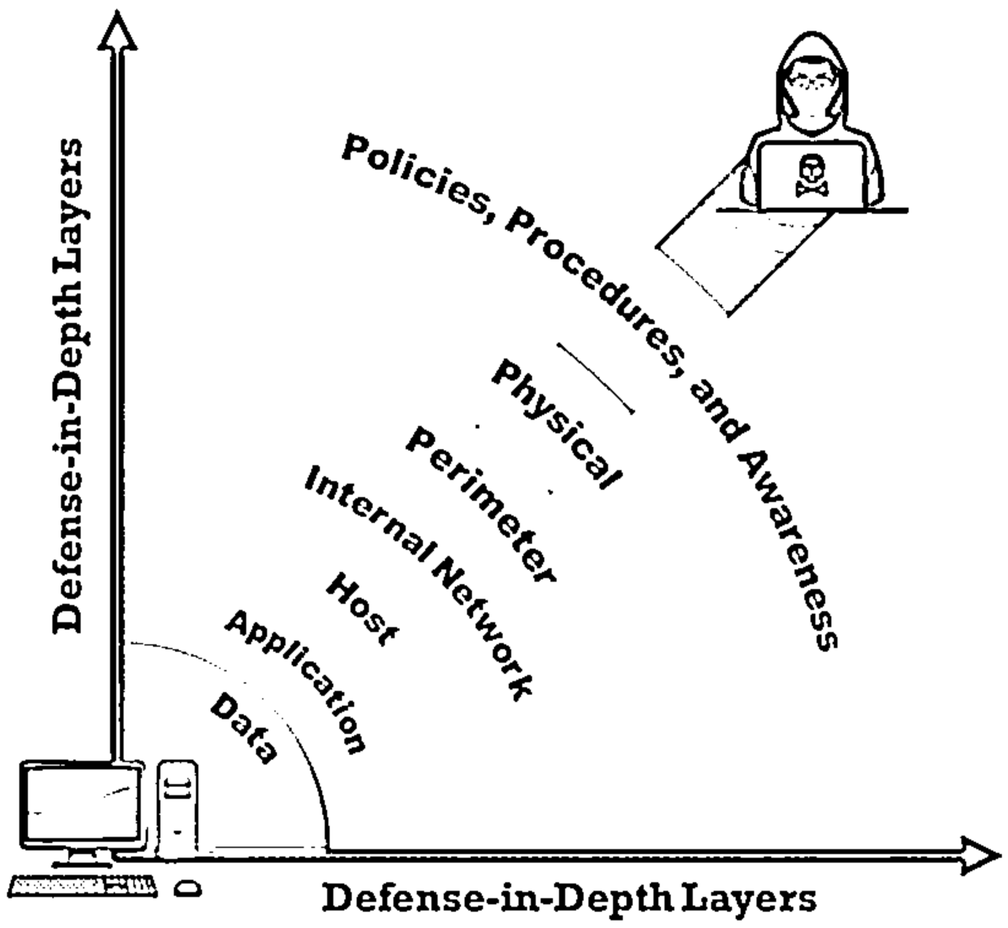


Figure 1.3: Defense in Depth

What is Risk?

- Risk refers to the degree of uncertainty or expectation that an adverse event may cause damage to the system
- Risks are categorized into different levels according to their estimated impact on the system
- A risk matrix is used to scale risk by considering the probability, likelihood, and consequence or impact of the risk

Risk Levels

Risk Level	Action
Extreme or High	➢ Immediate measures should be taken to combat risk ➢ Identify and impose controls to reduce risk to a reasonably low level
Medium	➢ No urgent action is required ➢ Implement controls as soon as possible to reduce risk to a reasonably low level
Low	➢ Take preventive steps to mitigate the effects of risk

Risk Matrix

Probability		Consequences				
		Insignificant	Minor	Moderate	Major	Severe
81 - 100%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

Likelihood

Note: This is an example of a risk matrix. Organizations need to create their own risk matrix based on their business needs

What is Risk?

Risk refers to the degree of uncertainty or expectation of potential damage that an adverse event may cause to the system or its resources, under specified conditions. Alternatively, risk can also be:

- The probability of the occurrence of a threat or an event that will damage, cause loss to, or have other negative impacts on the organization, either from internal or external liabilities.
- The possibility of a threat acting upon an internal or external vulnerability and causing harm to a resource.
- The product of the likelihood that an event will occur and the impact that the event might have on an information technology asset.

The relation between Risk, Threats, Vulnerabilities, and Impact is as follows:

RISK = Threats x Vulnerabilities x Impact

The impact of an event on an information asset is the product of vulnerability in the asset and the asset's value to its stakeholders. IT risk can be expanded to

RISK = Threat × Vulnerability × Asset Value

In fact, the risk is the combination of the following two factors:

- The probability of the occurrence of an adverse event
- The consequence of the adverse event

Risk Level

Risk level is an assessment of the resulted impact on the network. Various methods exist to differentiate the risk levels depending on the risk frequency and severity. One of the common methods used to classify risks is to develop a two-dimensional matrix.

Working out the frequency or probability of an incident happening (likelihood) and its possible consequences is necessary to analyze risks. This is referred to as the level of risk. Risk can be represented and calculated using the following formula:

Level of Risk = Consequence x Likelihood

Risks are categorized into different levels according to their estimated impact on the system. Primarily, there are four risk levels, which include extreme, high, medium, and low levels. Remember that control measures may decrease the level of a risk, but do not always entirely eliminate the risk.

Risk Level	Consequence	Action
Extreme or High	Serious or Imminent danger	➢ Immediate measures are required to combat the risk ➢ Identify and impose controls to reduce the risk to a reasonably low level
Medium	Moderate danger	➢ Immediate action is not required, but action should be implement quickly ➢ Implement controls as soon as possible to reduce the risk to a reasonably low level
Low	Negligible danger	➢ Take preventive steps to mitigate the effects of risk

Table 1.1: Risk Levels

Risk Matrix

The risk matrix scales the risk occurrence or likelihood probability, along with its consequences or impact. It is the graphical representation of risk severity and the extent to which the controls can or will mitigate it. The Risk matrix is one of the simplest processes to use for increased visibility of risk; it contributes to the management's decision-making capability. The risk matrix defines various levels of risk and categorizes them as the product of negative probability and negative severity. Although there are many standard risk matrices, individual organizations must create their own.

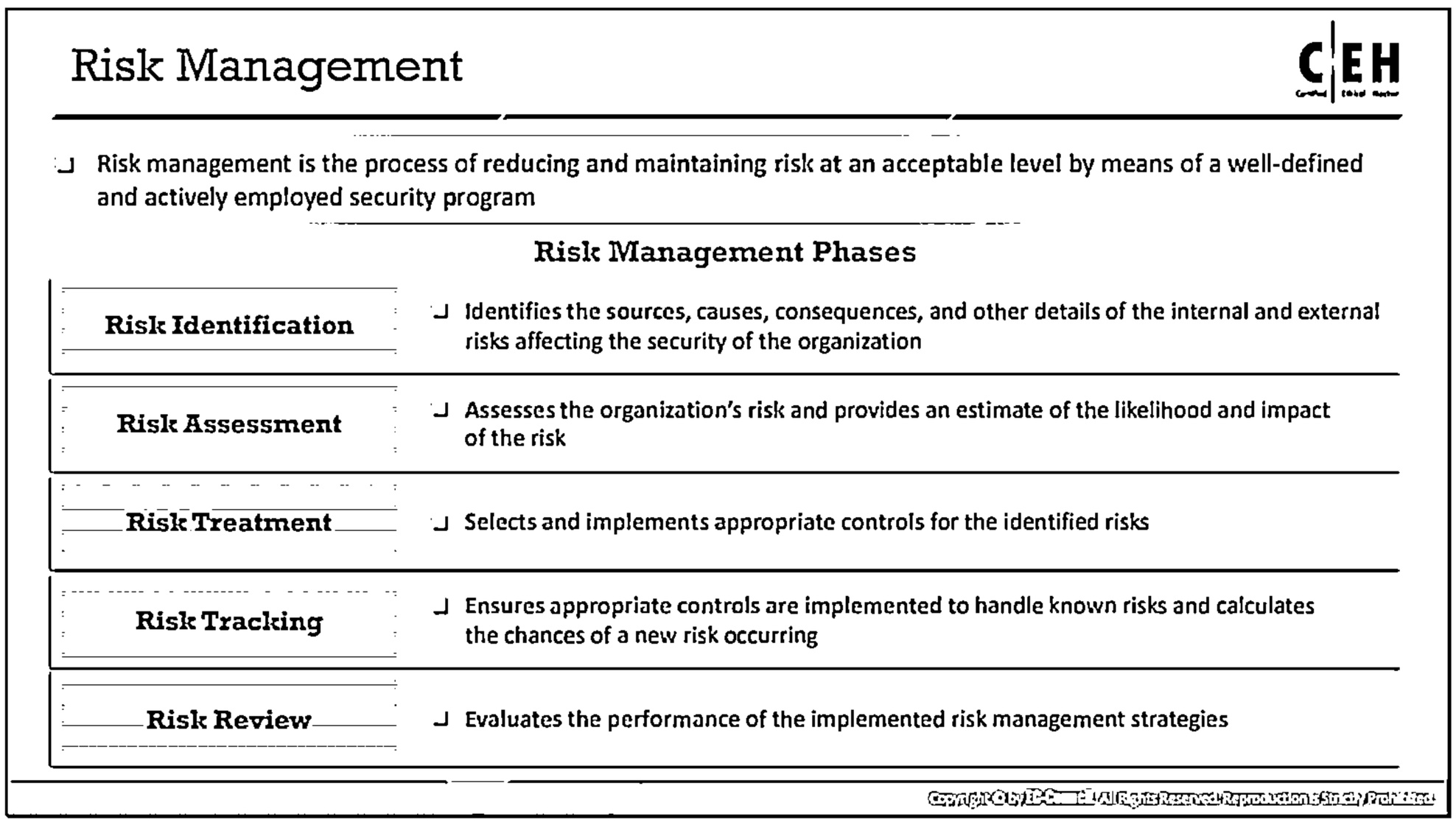
Probability		Consequences				
		Insignificant	Minor	Moderate	Major	Severe
81 - 100%	Very High Probability	Low	Medium	High	Extreme	Extreme
61 - 80%	High Probability	Low	Medium	High	High	Extreme
41 - 60%	Equal Probability	Low	Medium	Medium	High	High
21 - 40%	Low Probability	Low	Low	Medium	Medium	High
1 - 20%	Very Low Probability	Low	Low	Medium	Medium	High

Table 1.2: Risk Matrix

The above table is the graphical representation of a risk matrix, which is used to visualize and compare risks. It differentiates the two levels of risk and is a simple way of analyzing them.

- Likelihood: The chance of the risk occurring
- Consequence: The severity of a risk event that occurs

Note: This is an example of a risk matrix. Organizations must create individual risk matrices based on their business needs.



Risk Management

Risk management is the process of identifying, assessing, responding to, and implementing the activities that control how the organization manages the potential effects of risk. It has a prominent place throughout the security life cycle and is a continuous and ever-increasing complex process. The types of risks vary from organization to organization, but the act of preparing a risk management plan is common to all organizations.

Risk Management Objectives

- Identify potential risks—this is the main objective of risk management
- Identify the impact of risks and help the organization develop better risk management strategies and plans
- Prioritize the risks, depending on the impact or severity of the risk, and use established risk management methods, tools, and techniques to assist in this task
- Understand and analyze the risks and report identified risk events.
- Control the risk and mitigate its effect.
- Create awareness among the security staff and develop strategies and plans for lasting risk management strategies.

Risk management is a continuous process performed by achieving goals at every phase. It helps reduce and maintain risk at an acceptable level utilizing a well-defined and actively employed security program. This process is applied in all stages of the organization, for example, to specific network locations in both strategic and operational contexts.

The four key steps commonly termed as risk management phases are:

- Risk Identification
- Risk Assessment
- Risk Treatment
- Risk Tracking and Review

Every organization should follow the above steps while performing the risk management process.

- **Risk Identification**

  The initial step of the risk management plan. Its main aim is to identify the risks—including the sources, causes, and consequences of the internal and external risks affecting the security of the organization before they cause harm. The risk identification process depends on the skill set of the people, and it differs from one organization to another.

- **Risk Assessment**

  This phase assesses the organization's risks and estimates the likelihood and impact of those risks. Risk assessment is an ongoing iterative process that assigns priorities for risk mitigation and implementation plans, which in turn help to determine the quantitative and qualitative value of risk. Every organization should adopt a risk evaluation process in order to detect, prioritize, and remove risks.

  The risk assessment determines the kind of risks present, their likelihood and severity, and the priorities and plans for risk control. Organizations perform a risk assessment when they identify a hazard but are not able to control it immediately. A risk assessment is followed by a regular update of all information facilities.

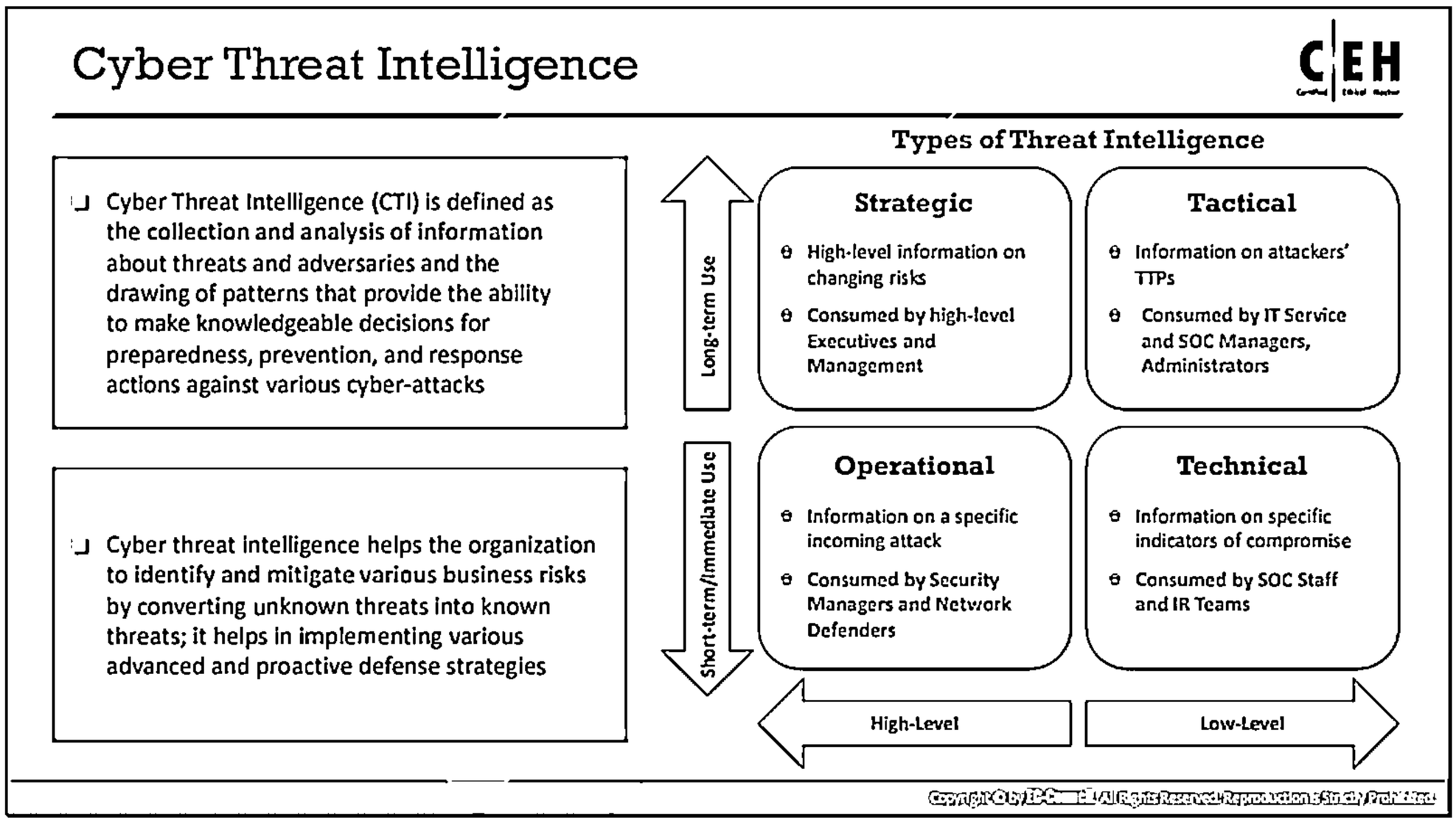
- **Risk Treatment**

  Risk treatment is the process of selecting and implementing appropriate controls on the identified risks in order to modify them. The risk treatment method addresses and treats the risks according to their severity level. Decisions made in this phase are based on the results of a risk assessment. The purpose of this step is to identify treatments for the risks that fall outside the department's risk tolerance and provide an understanding of the level of risk with controls and treatments. It identifies the priority order in which individual risks should be treated, monitored, and reviewed. The following information is needed before treating the risk:

  - The appropriate method of treatment
  - The people responsible for the treatment
  - The costs involved
  - The benefits of treatment
  - The likelihood of success
  - Ways to measure and assess the treatment

- **Risk Tracking and Review**

  An effective risk management plan requires a tracking and review structure to ensure effective identification and assessment of the risks as well as the use of appropriate controls and responses. The tracking and review process should determine the measures and procedures adopted and ensure that the information gathered to perform the assessment was appropriate. The review phase evaluates the performance of the implemented risk management strategies. Performing regular inspections of policies and standards, as well as regularly reviewing them, helps to identify the opportunities for improvement. Further, the monitoring process ensures that there are appropriate controls in place for the organization's activities and that all procedures are understood and followed.



Cyber Threat Intelligence

According to the Oxford dictionary, a threat is defined as "the possibility of a malicious attempt to damage or disrupt a computer network or system." A threat is a potential occurrence of an undesired event that can eventually damage and interrupt the operational and functional activities of an organization. A threat can affect the integrity and availability factors of an organization. The impact of threats is very great and may affect the state of the physical IT assets in an organization. The existence of threats may be accidental, intentional, or due to the impact of some action.

Cyber threat intelligence, usually known as CTI, is the collection and analysis of information about threats and adversaries and the drawing up of patterns that provide an ability to make knowledgeable decisions for preparedness, prevention, and response actions against various cyberattacks. It is the process of recognizing or discovering any "unknown threats" that an organization may face so that necessary defense mechanisms can be applied to avoid such occurrences. It involves collecting, researching, and analyzing trends and technical developments in the field of cyber threats (including cybercrime, hacktivism, and espionage). Any knowledge about threats that results in an organization's planning and decision-making to handle it is a piece of threat Intelligence. The main aim of CTI is to make the organization aware of existing or emerging threats and prepare them to develop a proactive cybersecurity posture in advance of exploitation. This process, where unknown threats are converted into possibly known ones, helps to anticipate the attack before it can happen, and ultimately results in a better and more secure system. Thus, threat Intelligence is useful in achieving secure data sharing and global transactions among organizations.

Threat intelligence processes can be used to identify the risk factors that are responsible for malware attacks, SQL injections, web application attacks, data leaks, phishing, denial-of-service

attack, and other attacks. Such risks, after being filtered out, can be put on a checklist and handled appropriately. Threat intelligence is beneficial for an organization to handle cyber threats with effective planning and execution. Along with a thorough analysis of the threat, CTI also strengthens the organization's defense system, creates awareness about impending risks, and aids in responding against such risks.

Types of Threat Intelligence

Threat intelligence is contextual information that describes threats and guides organizations in making various business decisions. It is extracted from a huge collection of sources and information. It provides operational insight by looking outside the organization and issuing alerts on evolving threats to the organization. For the better management of information that is collected from different sources, it is important to subdivide threat intelligence into different types. This subdivision is performed based on the consumers and goals of the intelligence. From the perspective of consumption, threat intelligence is divided into four different types. They are, namely, strategic, tactical, operational, and technical threat intelligence. These four types differ in terms of data collection, data analysis, and intelligence consumption.

- **Strategic Threat Intelligence**

  Strategic threat intelligence provides high-level information regarding cybersecurity posture, threats, details about the financial impact of various cyber activities, attack trends, and the impact of high-level business decisions. This information is consumed by the high-level executives and management of the organization, such as IT management and CISO. It helps the management to identify current cyber risks, unknown future risks, threat groups, and attribution of breaches. The intelligence obtained provides a risk-based view that mainly focuses on high-level concepts of risks and their probability. It mainly deals with long-term issues and provides real-time alerts for threats to the organization's critical assets, such as IT infrastructure, employees, customers, and applications. This intelligence is used by the management to make strategic business decisions and to analyze their effect. Based on the analysis, the management can allocate sufficient budget and staff to protect critical IT assets and business processes.

  Strategic threat intelligence is generally in the form of a report that mainly focuses on high-level business strategies. Since the characteristic of strategic threat intelligence is preeminent, the data collection also relates to high-level sources and requires highly skilled professionals to extract information. This intelligence is collected from sources such as OSINT, CTI vendors, and ISAOs and ISACs.

  The strategic threat intelligence helps organizations identify any similar past incidents, their intentions, and any attributes that might identify the attacking adversaries, why the organization is within the scope of the attack, major attack trends, and how to reduce the risk level.

  Generally, strategic threat intelligence includes the following information:

  - The financial impact of cyber activity
  - Attribution for intrusions and data breaches

- Threat actors and attack trends
- The threat landscape for various industry sectors
- Statistical information on data breaches, data theft, and malware
- Geopolitical conflicts involving various cyberattacks
- Information on how adversary TTPs change over time
- Industry sectors that might impact due to high-level business decisions

- **Tactical Threat Intelligence**

  Tactical threat intelligence plays a major role in protecting the resources of the organization. It provides information related to the TTPs used by threat actors (attackers) to perform attacks. Tactical threat intelligence is consumed by cybersecurity professionals such as IT service managers, security operations managers, network operations center (NOC) staff, administrators, and architects. It helps the cybersecurity professionals understand how the adversaries are expected to perform their attack on the organization, identify the information leakage from the organization, and assess the technical capabilities and goals of the attackers along with the attack vectors. Using tactical threat intelligence, security personnel develop detection and mitigation strategies beforehand through procedures such as updating security products with identified indicators and patching vulnerable systems.

  The collection sources for tactical threat intelligence include campaign reports, malware, incident reports, attack group reports, and human intelligence, among other information. This intelligence is generally obtained by reading white or technical papers, communicating with other organizations, or purchasing intelligence from third parties. It includes highly technical information on topics such as malware, campaigns, techniques, and tools in the form of forensic reports.

  Tactical threat intelligence provides day-to-day operational support by helping analysts assess various security incidents related to events, investigations, and other activities. It also guides the high-level executives of the organizations in making strategic business decisions.

- **Operational Threat Intelligence**

  Operational threat intelligence provides information about specific threats against the organization. It provides contextual information about security events and incidents that help defenders disclose potential risks, provide greater insight into attacker methodologies, identify past malicious activities, and perform investigations on malicious activity in a more efficient way. It is consumed by security managers or heads of incident response, network defenders, security forensics, and fraud detection teams. It helps organizations to understand the possible threat actors and their intention, capability, and opportunity to attack vulnerable IT assets and the impact of a successful attack. In many cases, only government organizations can collect this type of intelligence. However, doing so helps IR and forensic teams to deploy security assets to

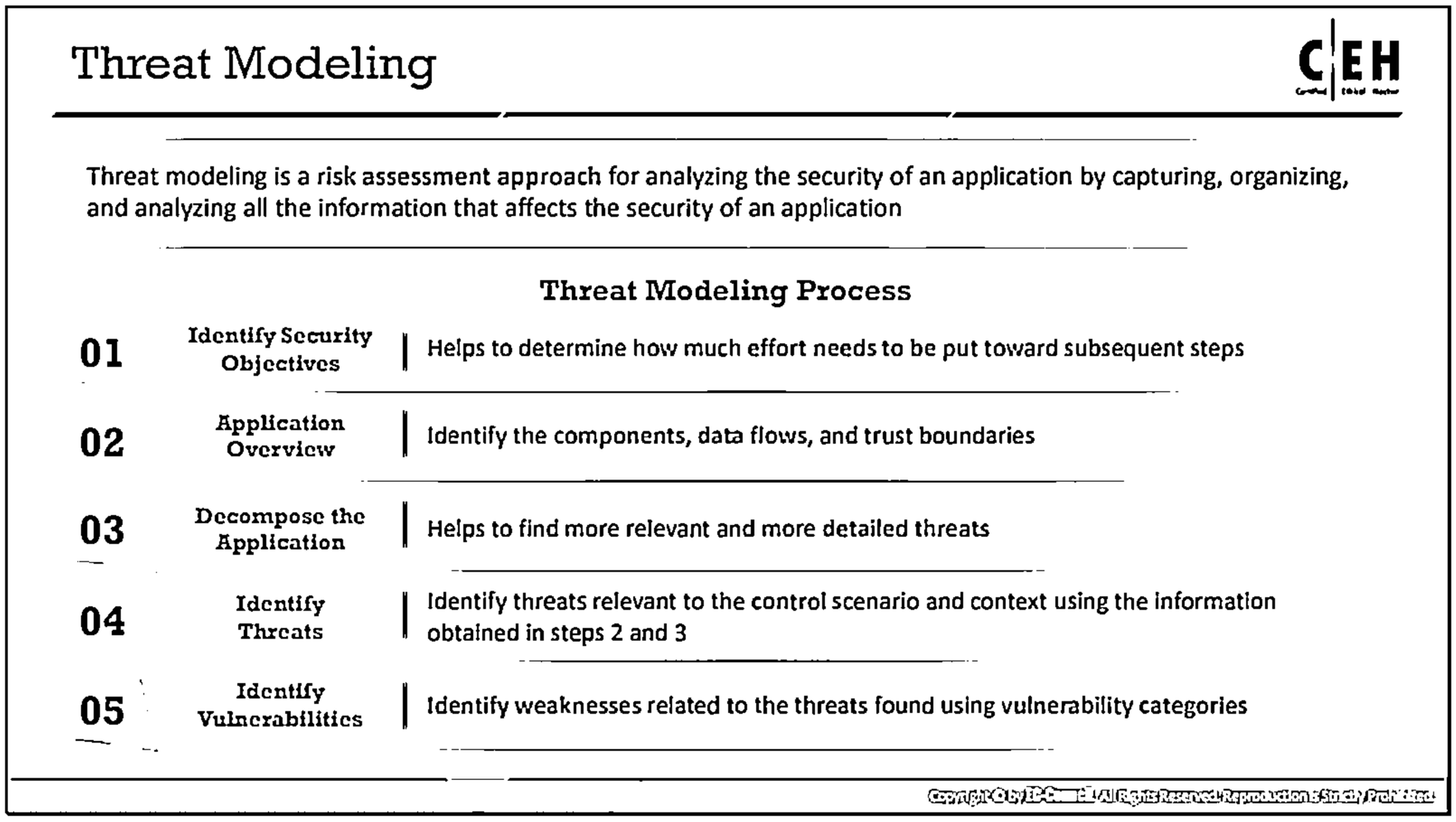
identify and stop upcoming attacks, improve early-stage attack detecting capability, and reduce an attack's damage to IT assets.

Operational threat intelligence is generally collected from sources such as humans, social media, and chat rooms; it may and also be collected from the real-world activities and events that result in cyberattacks. Operational threat intelligence is obtained by analyzing human behavior, threat groups, and by similar means. This information helps to predict future attacks and thus enhances incident response plans and mitigation strategies. Operational threat intelligence generally appears as a report that contains identified malicious activities, recommended courses of action, and warnings of emerging attacks.

- **Technical Threat Intelligence**

  Technical threat intelligence provides information about resources an attacker uses to perform an attack; this includes command and control channels, tools, and other items. It has a shorter lifespan compared to tactical threat intelligence and mainly focuses on a specific IoC. It provides rapid distribution and response to threats. For example, a piece of malware used to perform an attack is tactical threat intelligence, whereas the details related to the specific implementation of the malware come under technical threat intelligence. Other examples of technical threat intelligence include the specific IP addresses and domains used by malicious endpoints, phishing email headers, and hash checksums of malware, among others. Technical threat intelligence is consumed by SOC staff and IR teams.

  The indicators of technical threat intelligence are collected from active campaigns, attacks that are performed on other organizations, or data feeds provided by external third parties. These indicators are generally collected as part of investigations of attacks performed on various organizations. This information helps security professionals add the identified indicators to the defensive systems such as IDS and IPS, firewalls, and endpoint security systems, thereby enhancing the detection mechanisms used to identify the attacks at an early stage. It also helps them identify malicious traffic and IP addresses suspected of spreading malware and spam emails. This intelligence is directly fed into the security devices in digital format to block and identify inbound and outbound malicious traffic entering the organization's network.



Threat Modeling

Threat modeling is a risk assessment approach for analyzing the security of an application by capturing, organizing, and analyzing all the information that affects it. The threat model consists of three major building blocks: understanding the adversary's perspective, characterizing the security of the system, and determining threats. Every application should have a developed and documented threat model that should be revisited as the application evolves and development progresses.

Threat modeling helps to:

- Identify relevant threats to a particular application scenario
- Identify key vulnerabilities in an application's design
- Improve security design

When using this approach, an administrator should keep the following in mind:

- Try not to be rigid about specific steps or implementations; instead, focus on the approach. If any step becomes impassable, go right to step 4 of the threat modeling process and identify the problem.
- Use scenarios to scope the modeling activity.
- Use existing design documents. Use items like documented use cases or use stories, architectural diagrams, data flow diagrams, or other design documentation.
- Start with a whiteboard before capturing information in documents or getting lost in details. It may be helpful to use a digital camera with printing capabilities to document and distribute the information from the whiteboard.

- Use an iterative approach. Add more details and improve the threat model as design and development continue. This will help with becoming familiar with the modeling process and developing the threat model to better examine more possible scenarios.
- Obtain input about the host and network constraints from the system and network administrators. To better understand the end-to-end deployment diagram, obtain as much information as possible about host configurations, firewall policies, allowed protocols and ports, and other relevant details.

The threat modeling process involves five steps:

1. **Identify Security Objectives**

   Security objectives are the goals and constraints related to the application's confidentiality, integrity, and availability. Security-specific objectives guide the threat modeling efforts and help to determine how much effort needs to be put toward subsequent steps. To identify security objectives, administrators should ask the following questions:

   - What data should be protected?
   - Are there any compliance requirements?
   - Are there specific quality-of-service requirements?
   - Are there intangible assets to protect?

2. **Application Overview**

   Identify the components, data flows, and trust boundaries. To draw the end-to-end deployment scenario, the administrator should use a whiteboard. First, they should draw a rough diagram that explains the workings and structure of the application, its subsystems, and its deployment characteristics. The deployment diagram should contain the following:

   - End-to-end deployment topology
   - Logical layers
   - Key components
   - Key services
   - Communication ports and protocols
   - Identities
   - External dependencies

   Identify Roles

   The administrator should identify people and the roles and actions they can perform within the application. For example, are there higher-privileged groups of users? Who can read data? Who can update data? Who can delete data?

Identify Key Usage Scenarios

The administrator should use the application's use cases to determine its objective. Use cases explain how the application is used and misused.

Identify Technologies

The administrator should list the technologies and key features of the software, as well as the following technologies in use:

- Operating systems
- Web server software
- Database server software
- Technologies for presentation, business, and data access layers
- Development languages

Identifying these technologies helps to focus on technology-specific threats.

Identify Application Security Mechanisms

The administrator should identify some key points regarding the following:

- Input and data validation
- Authorization and authentication
- Sensitive data
- Configuration management
- Session management
- Parameter manipulation
- Cryptography
- Exception management
- Auditing and logging

These efforts aim to identify relevant details and to add details where required, or to identify areas that require more.

3. **Decompose the Application**

   In this step, the administrator breaks down the application to identify the trust boundaries, data flows, entry points, and exit points. Doing so makes it considerably easier to find more relevant and more detailed threats and vulnerabilities.

   Identify Trust Boundaries

   Identifying the application's trust boundaries helps the administrator to focus on the relevant areas of the application. It indicates where trust levels change.

   - Identify outer system boundaries

- Identify access control points or key places where access requires extra privileges or role membership
- Identify trust boundaries from a data flow perspective

Identify Data Flows

The administrator should list the application's data input from entry to exit. This helps to understand how the application communicates with outside systems and clients and how the internal components interact. They should pay particular attention to the data flow across trust boundaries and the data validation at the trust boundary entry point. A good approach is to start at the highest level and then deconstruct the application by testing the data flow between different subsystems.

Identify Entry Points

The application's entry point can also serve as an entry point for attacks. All users interact with the application at these entry points. Other internal entry points uncovered by subcomponents over the layers of the application may be present only to support internal communication with other components. The administrator should identify these entry points to determine the methods used by an intruder to get in through them. They should focus on the entry points that allow access to critical functionalities and provide adequate defense for them.

Identify Exit Points

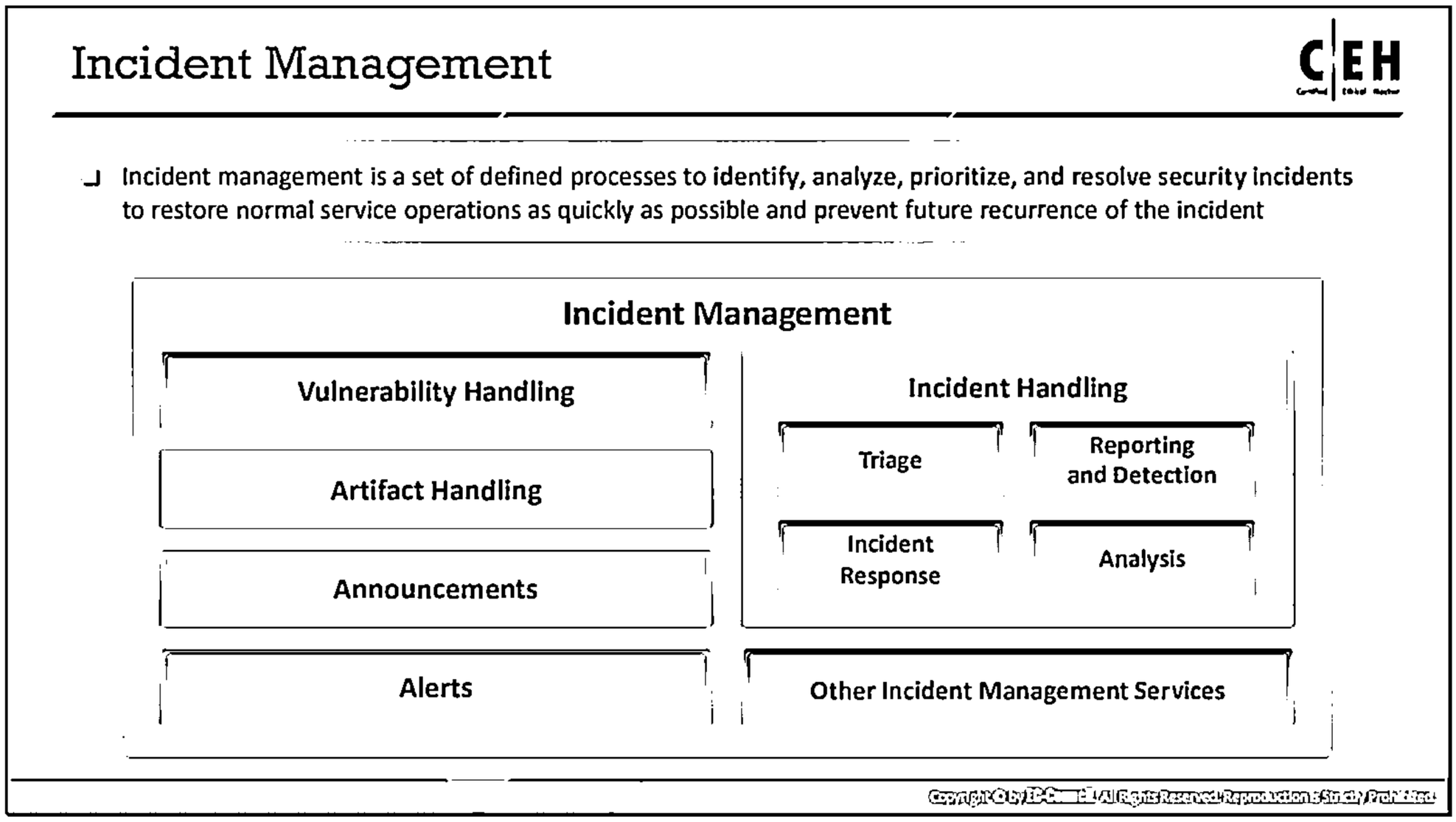
The administrator should also identify the points where the application transfers data to the client or external systems. They should prioritize the exit points at which the application writes data containing client input or data from untrusted sources, such as a shared database.

4. **Identify Threats**

   The administrator should identify threats relevant to the control scenario and context using the information obtained in the application overview and decompose application steps. They should bring members of the development and test teams together to identify potential threats. The team should start with a list of common threats grouped by their application vulnerability category. This step uses a question-driven approach to help identify threats.

5. **Identify Vulnerabilities**

   A vulnerability is a weakness in an application (deployed in an information system) that allows attacker exploitation, thereby leading to security breaches. Security administrators should identify any weaknesses related to the threats found using the vulnerability categories to identifying vulnerabilities and fix them beforehand to keep intruders away.



Incident Management

Incident management is a set of defined processes to identify, analyze, prioritize, and resolve security incidents to restore the system to normal service operations as soon as possible, and prevent recurrence of the incident. It involves not only responding to incidents but also triggering alerts to prevent potential risks and threats. A security administrator must identify software that is open to attacks before someone takes advantage of the vulnerabilities.

Incident management includes the following:

- Vulnerability analysis
- Artifact analysis
- Security awareness training
- Intrusion detection
- Public or technology monitoring

The incident management process is designed to:

- Improve service quality
- Resolve problems proactively
- Reduce the impact of incidents on an organization or its business
- Meet service availability requirements
- Increase staff efficiency and productivity
- Improve user and customer satisfaction
- Assist in handling future incidents

Conducting training sessions to spread awareness among users is an important part of incident management. Such sessions help end-users to recognize suspicious events or incidents easily and report an attacker's behavior to the appropriate authority.

The following people perform incident management activities:

- Human resources personnel take steps to fire employees suspected of harmful computer activities.
- The legal counsel sets the rules and regulations in an organization. These rules can influence the internal security policies and practices of the organization in case an insider or an attacker uses the organization's system for harmful or malicious activities.
- The firewall manager keeps filters in place. These filters are frequently where denial-of-service attacks are made.
- An outsourced service provider repairs systems infected by viruses and malware.

Incident response is one of the functions performed in incident handling. In turn, incident handling is one of the services provided as part of incident management. The following diagram illustrates the relationship between incident response, incident handling, and incident management.

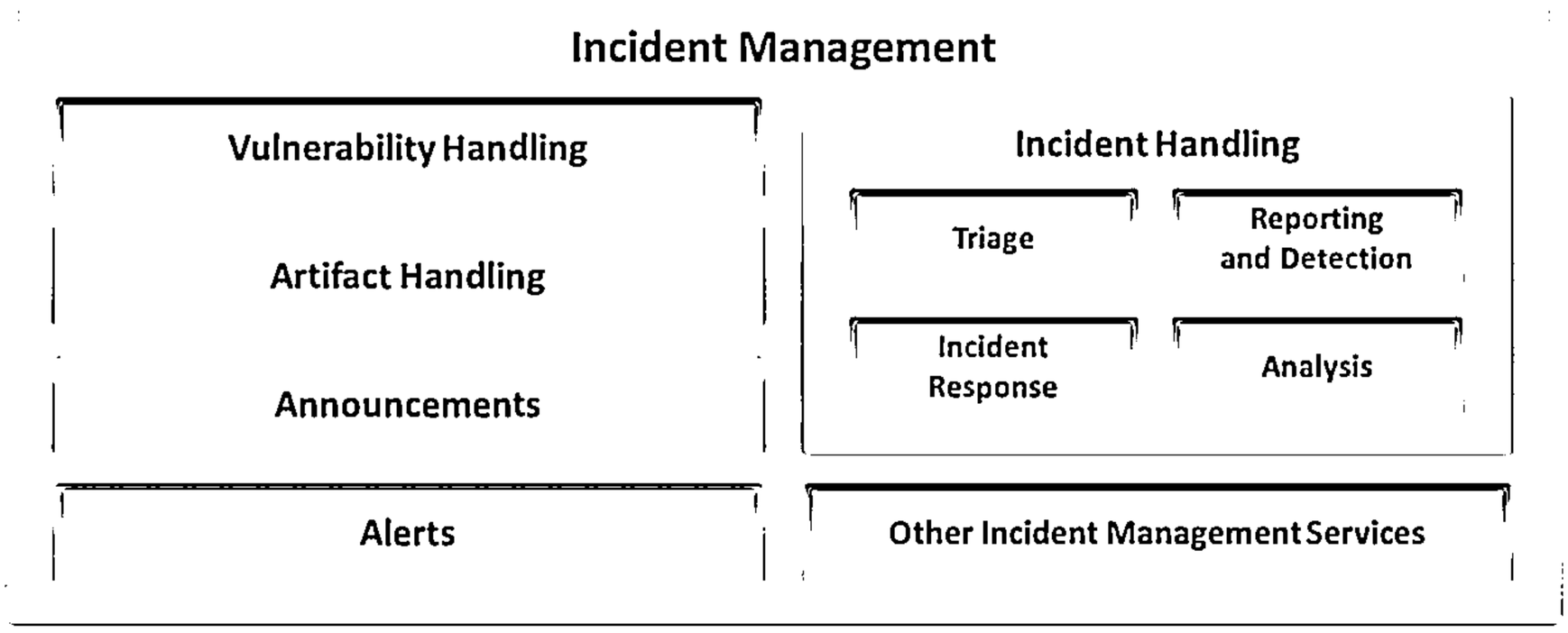
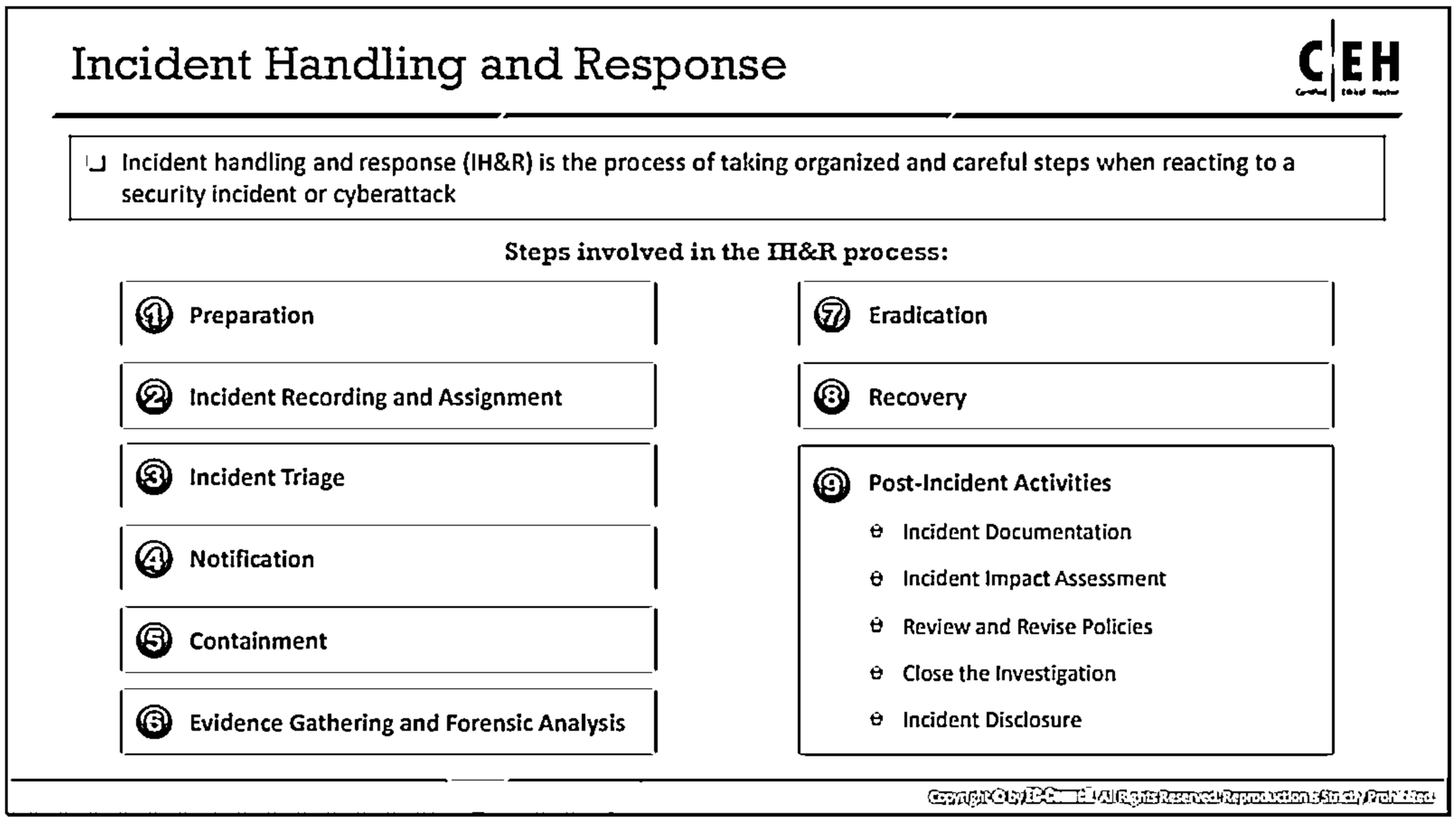


Figure 1.4: Block Diagram of Incident Management



Incident Handling and Response

Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. It is a set of procedures, actions, and measures taken against an unexpected event occurrence. It involves logging, recording, and resolving incidents that take place in the organization. It notes the incident, when it occurred, its impact, and its cause. It is the practice of managing the incident response processes, such as preparation, detection, containment, eradication, and recovery, to overcome the impact of an incident quickly and efficiently. IH&R processes are important to provide a focused approach for restoring normal business operations as quickly as possible after an incident and with a minimal impact on the business.

The IH&R process involves defining user policies, developing protocols, building incident response teams, auditing organizational assets, planning incident response procedures, obtaining management approval, incident reporting, prioritization, and managing response. It also includes establishing proper communication between the individuals responding to an incident and guiding them to detect, analyze, contain, recover, and prevent incidents.

Discussed below are the steps involved in the IH&R process:

- **Step 1: Preparation**

  The preparation phase includes performing an audit of resources and assets to determine the purpose of security and define the rules, policies, and procedures that drive the IH&R process. It also includes building and training an incident response team, defining incident readiness procedures, and gathering required tools as well as training the employees to secure their systems and accounts.

- **Step 2: Incident Recording and Assignment**

  In this phase, the initial reporting and recording of the incident take place. This phase handles identifying an incident and defining proper incident communication plans for the employees and also includes communication methods that involve informing IT support personnel or submitting an appropriate ticket.

- **Step 3: Incident Triage**

  In this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited.

- **Step 4: Notification**

  In the notification phase, the IH&R team informs various stakeholders, including management, third-party vendors, and clients, about the identified incident.

- **Step 5: Containment**

  This phase helps to prevent the spread of infection to other organizational assets, preventing additional damage.

- **Step 6: Evidence Gathering and Forensic Analysis**

  In this phase, the IH&R team accumulates all possible evidence related to the incident and submits it to the forensic department for investigation. Forensic analysis of an incident reveals details such as the method of attack, vulnerabilities exploited, security mechanisms averted, network devices infected, and applications compromised.

- **Step 7: Eradication**

  In the eradication phase, the IH&R team removes or eliminates the root cause of the incident and closes all the attack vectors to prevent similar incidents in the future.

- **Step 8: Recovery**

  After eliminating the causes for the incidents, the IH&R team restores the affected systems, services, resources, and data through recovery. It is the responsibility of the incident response team to ensure that that the incident causes no disruption to the services or business of the organization.

- **Step 9: Post-Incident Activities**

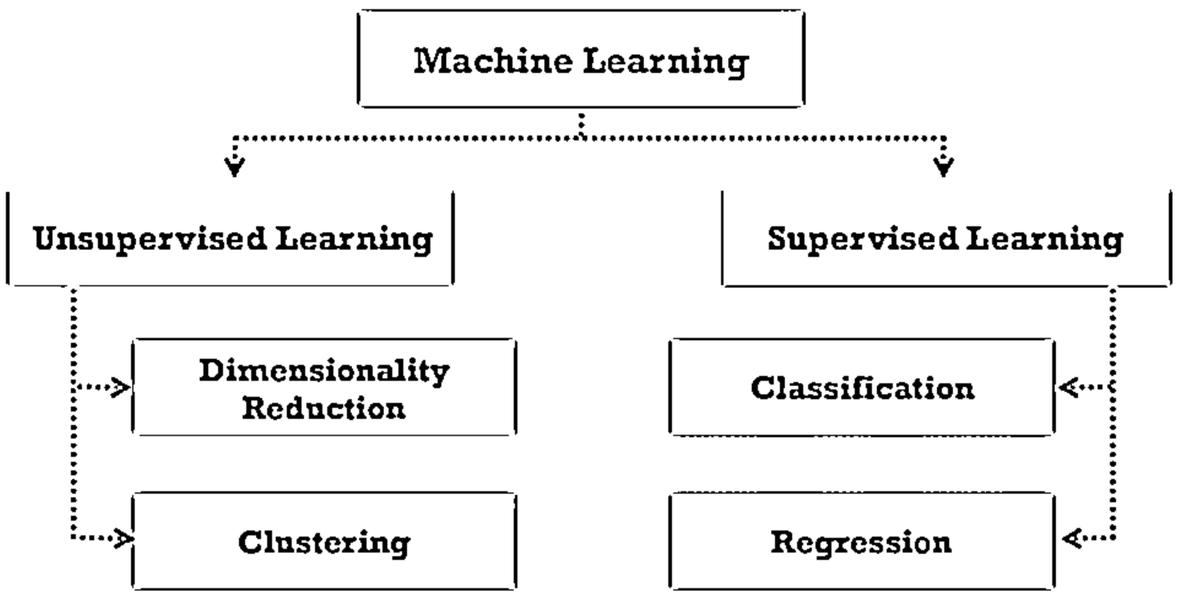
  Once the process is complete, the security incident requires additional review and analysis before closing the matter. Conducting a final review is an important step in the IH&R process that includes:

  - Incident documentation
  - Incident impact assessment
  - Reviewing and revising policies
  - Closing the investigation
  - Incident disclosure

Role of AI and ML in Cyber Security

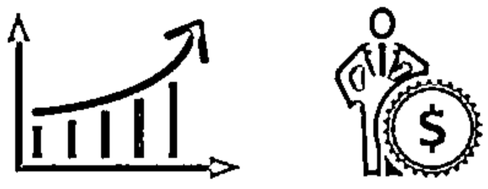
- Machine learning (ML) and artificial intelligence (AI) are now vastly used across various industries and applications due to the increase in computing power, data collection, and storage capabilities
- ML is an unsupervised self-learning system that is used to define what the normal network looks like, along with its devices, and then to backtrack and report any deviations or anomalies in real-time
- AI and ML in cyber security helps in identifying new exploits and weaknesses, which can then be easily analyzed to mitigate further attacks

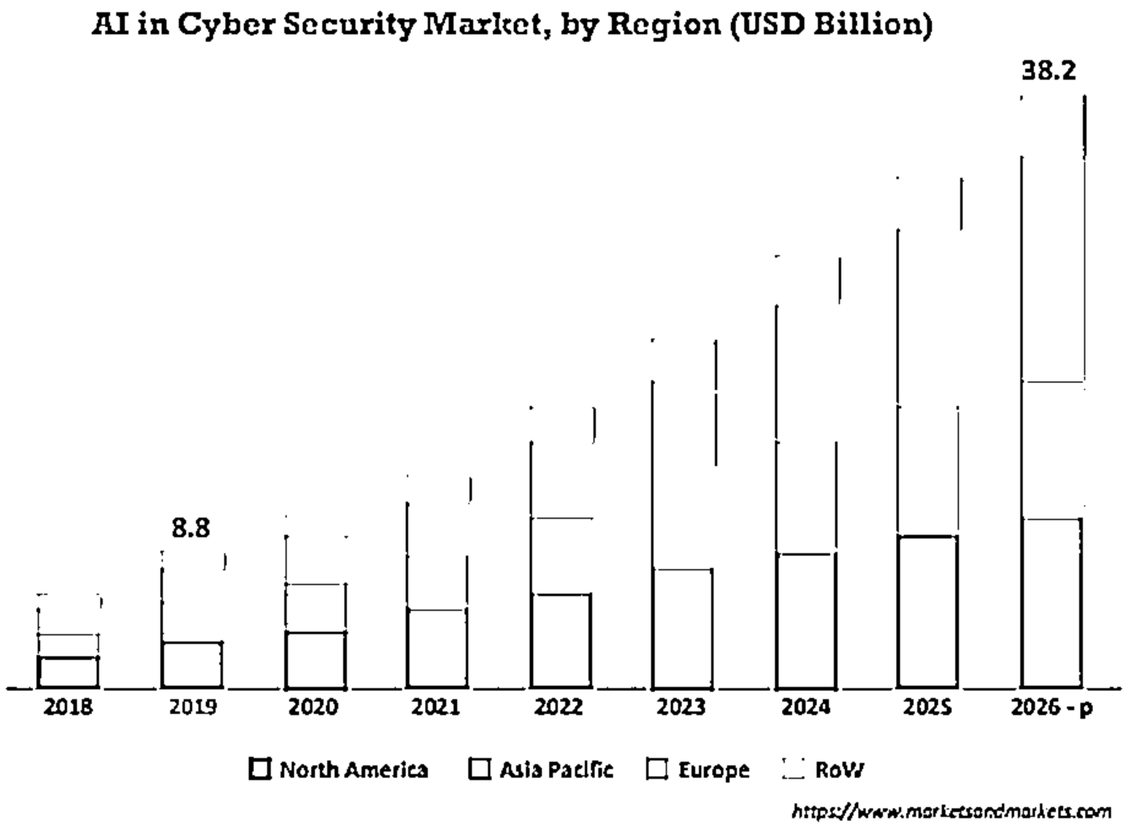
- ML classification techniques:
  - Supervised learning makes use of algorithms that input a set of labeled training data, with the aim of learning the differences between the labels
  - Unsupervised learning makes use of algorithms that input unlabeled training data, with the aim of deducing all categories by itself



Role of AI and ML in Cyber Security (Cont'd)

- The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026

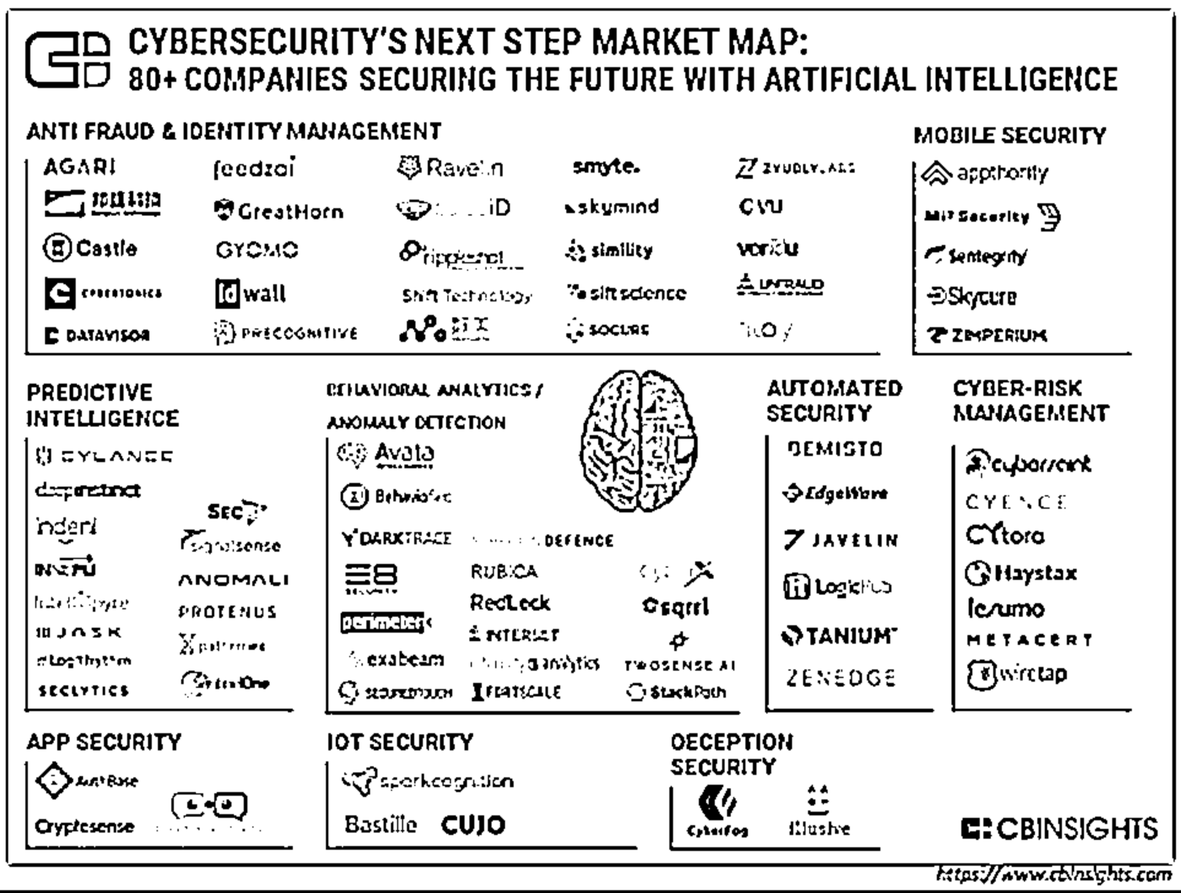




Role of AI and ML in Cyber Security (Cont'd)

According to CB Insights, alongside overall rising investment activity, many cybersecurity companies are emerging to offer novel solutions to cyber threats by leveraging the advantages of AI

Cybersecurity is the fourth most active industry that deals with companies applying AI



Role of AI and ML in Cyber Security

Machine learning (ML) and Artificial Intelligence (AI) are now popularly used across various industries and applications due to the increase in computing power, data collection, and storage capabilities.

Along with technological advancements in AI, such as self-driving cars, language translators, and big data, there is also a rise in threats such as ransomware, botnets, malware, and phishing. Using AI and ML in cybersecurity helps to identify new exploits and weaknesses, which can be easily analyzed to mitigate further attacks. It reduces the pressure on security professionals and alerts them whenever an action is needed.

What are AI and ML?

Artificial Intelligence is the only solution to defend networks against the various attacks that an antivirus scan cannot detect. A huge amount of collected data is fed into the AI, which processes and analyzes it to understand its details and trends.

ML is a branch of artificial intelligence (AI) that gives the systems the ability to self-learn without any explicit programs. This self-learning system is used to define what the normal network, along with its devices, looks like, and then uses this to backtrack and report any deviations or anomalies in real-time.

There are two types of ML classification techniques:

- **Supervised Learning**

  Supervised learning uses algorithms that input a set of labeled training data to attempt to learn the differences between the given labels. Supervised learning is further divided into two subcategories, namely, classification and regression. Classification includes

completely divided classes. Its main task is to define the test sample to identify its class. Regression is used when data classes are not separated, such as when the data is continuous.

- **Unsupervised Learning**

  Unsupervised learning makes use of algorithms that input unlabeled training data to attempt to deduce all the categories without guidance. Unsupervised learning is further divided into two subcategories, namely, clustering and dimensionality reduction. Clustering divides the data into clusters based on their similarities, regardless of class information. Dimensionality reduction is the process of reducing the dimensions (attributes) of data.

Why AI and ML?

Source: *https://www.gartner.com*, *https://www.marketsandmarkets.com*

The security threat landscape continues to evolve not just in scale, but, more importantly, in sophistication. Despite a range of advancements in the industry to safeguard against increasingly bold and intricate threats, organizations have struggled to keep pace with the technologies and techniques employed by attackers.

As companies continue to increase their digital footprints, "identify and diagnose" capabilities are not enough to remediate against this growing fundamental business challenge for organizations of all shapes and sizes. The development of advanced security analytics is an important consideration for organizations looking to implement machine learning to defend against an array of internal and external security threats.

The cyber security market is set to exceed $300 billion by 2024, and the AI-related cyber security market is predicted to reach a value of $38.2 billion by 2026.

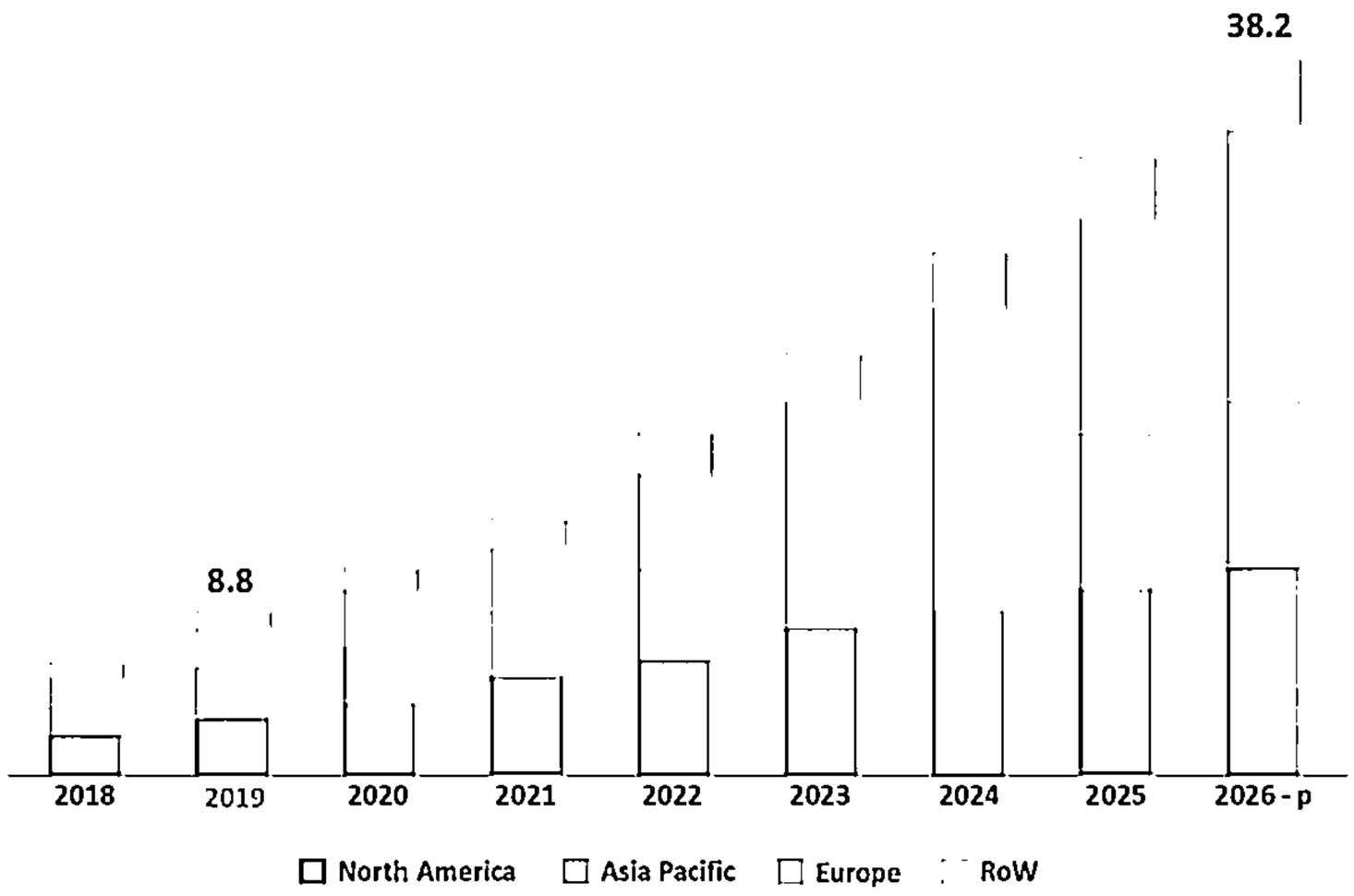


Figure 1.5: AI in Cyber Security Market

AI and ML Application Areas

Source: *https://www.cbinsights.com*

According to CB Insights, alongside overall rising investment activity, many cybersecurity companies are emerging to offer novel solutions to cyber threats by leveraging the advantages of artificial intelligence (AI).

According to CB Insights' AI Deals Tracker, cybersecurity is the fourth most active industry for deals to companies applying AI. As per CB Insights' data, there are over 80 private companies in cybersecurity that are using AI, categorized into the nine main areas in which they operate:

- Anti-fraud and identity management
- Mobile security
- Predictive intelligence
- Behavioral analytics and anomaly detection
- Automated security
- Cyber-risk management
- App security
- IoT security
- Deception security

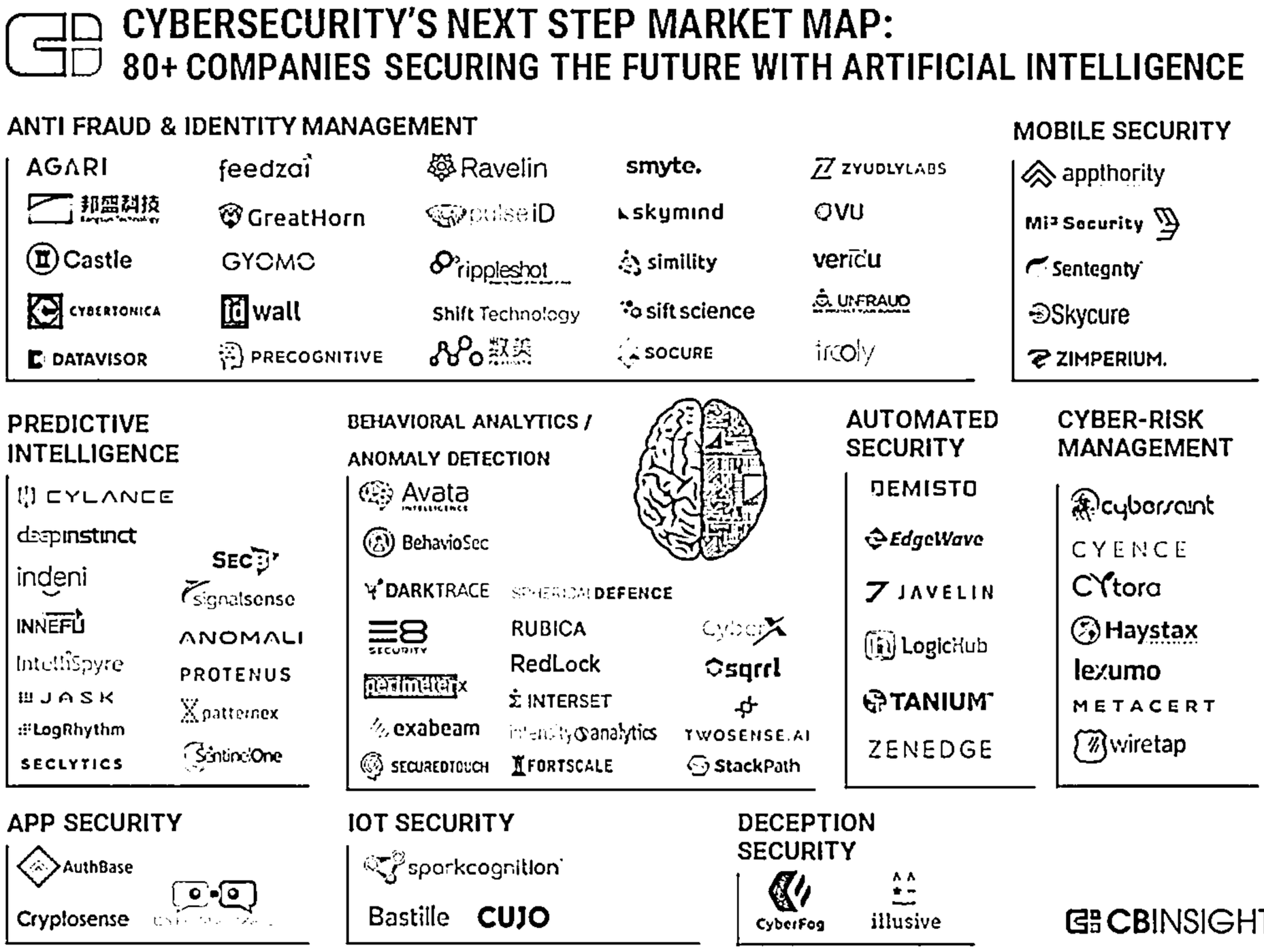
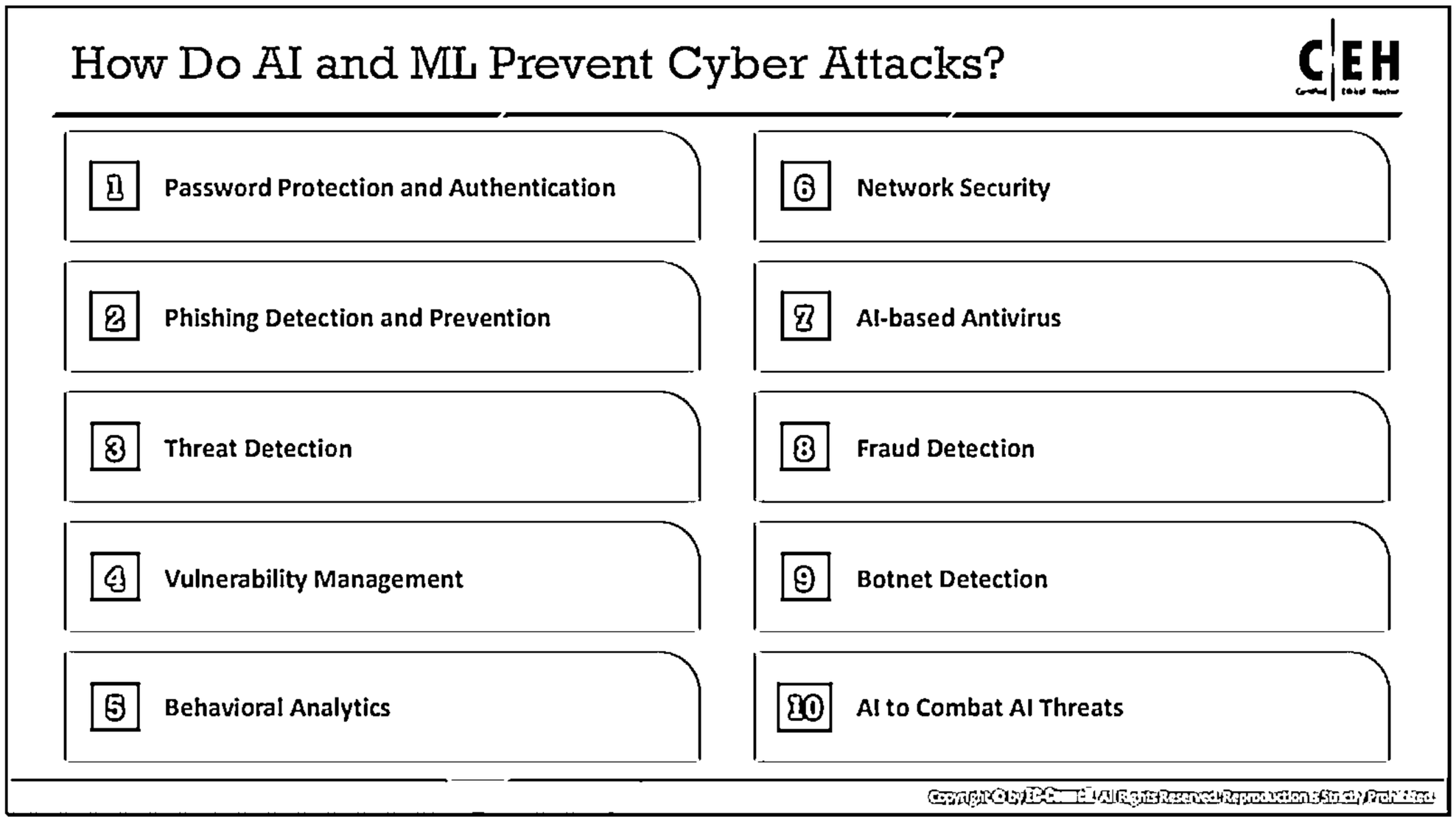


Figure 1.6: Companies using Artificial Intelligence



How Do AI and ML Prevent Cyber Attacks?

Artificial Intelligence (AI), and with it, Machine Learning (ML), is an emerging technology in the field of cybersecurity. It is widely adopted by largescale industries such as automation, IT services, manufacturing, production, and finance. AI plays a crucial role in detecting imminent cyber threats by incorporating machine learning as a subset.

Following are different ways that AI and ML safeguard industries from cybersecurity attacks:

- **Password Protection and Authentication**

  Password credentials play a critical role in preventing illegitimate access to the organization's or user's data. If credentials are compromised, the reputation of the organization or person could be damaged. Sometimes, traditional face detection and other biometric security measures can also be vulnerable to these credential breaches. Programmers use AI to improve biometric validations and face recognition to thwart such attacks. AI provides the latest models for recognizing an individual's face by tracking key correlations and patterns.

- **Phishing Detection and Prevention**

  Phishing is a common method attackers employ to send their payloads via emails. The majority of users cannot figure out which received emails have a malicious attachment or payload. In this case, AI and ML could play a pivotal role in identifying and preventing such phishing attacks. They can scan and identify phishing emails much faster than a human being can. They can also quickly differentiate malicious websites from legitimate websites.

- **Threat Detection**

  Machine learning assists companies in detecting cyber-attacks before systems are compromised. Being a part of AI, machine learning constantly keeps admins notified of imminent cyber threats by carrying out logical data analysis. ML allows systems to run its algorithms upon the data being received, then performs deep learning on the and comprehends the advancements required to ensure the safety of the information systems.

- **Vulnerability Management**

  AI and ML-based systems never allow vulnerability to exist for long; they dynamically scan for all types of vulnerabilities and alert the admins before the system is exploited. They can also provide the attacker's information and the patterns used to perform the attack. These AI- and ML-based systems can also forecast how and when a vulnerability exploitation might occur.

- **Behavioral Analytics**

  Another notable security improvement by artificial intelligence is "Behavioral Analytics." Attackers who have stolen the credentials of a legitimate user can perform malicious activities on the organization's network; such attempts are difficult to detect and thwart. Here, AI with ML generates specific user patterns based on their regular usage. AI software instantly alerts the admin if it detects any suspicious activity or deviation in regular usage.

- **Network Security**

  Two significant factors of network security are generating comprehensive security policies and mapping an enterprise's network topology. Unfortunately, both of these factors are time-consuming. Therefore, administrators are adopting AI to enhance this operation; it can carry out the network traffic analysis and propose efficient security policies by default.

- **AI-based Antivirus**

  Traditional antivirus tools perform file scanning on the organization's networks to check if any signatures match those of known viruses or malware. The issue with this is that antivirus tools must be updated when the user wants to scan for new malware or viruses. Updating is time-consuming, and new deployment often takes a certain amount of time. To overcome these issues, organizations employ AI-based antiviruses, which use anomaly detection to understand programs' behavior. AI-based antivirus detects suspicious program behavior instead of matching signatures for viruses.

- **Fraud Detection**

  AI and ML algorithms carry out anomaly detection to identify payment inconsistencies and fraudulent transactions. They also perform automated pattern discovery across different transactions. ML can easily differentiate between authentic and illegitimate transactions and blocks fraudulent transactions.

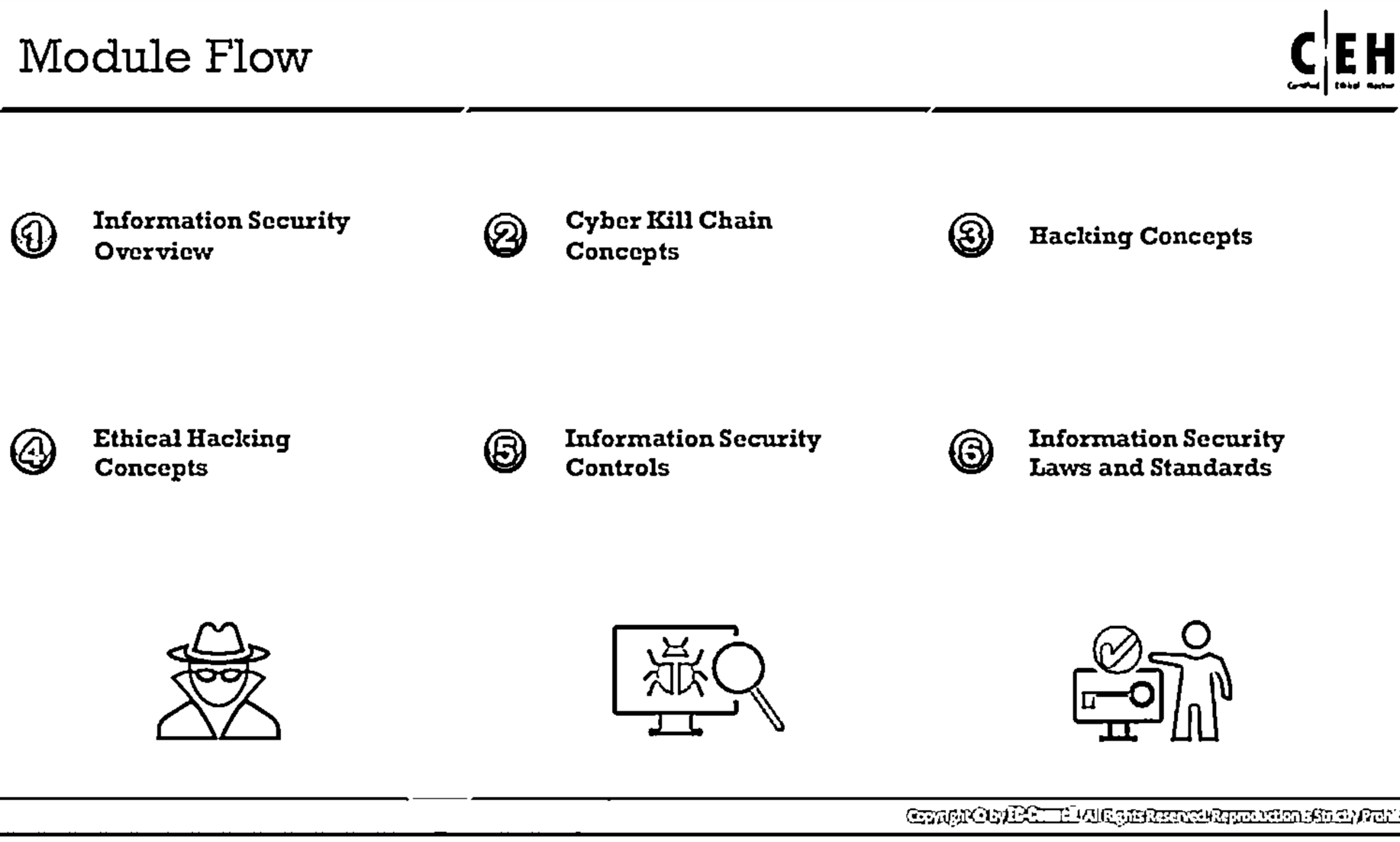
- **Botnet Detection**

  Botnets can bypass the Instruction Detection System (IDS) by leveraging its ineffectiveness in matching signatures. Botnets can be embedded using a highly sophisticated code that makes them untraceable by traditional IDS implementations. Hence, security professionals use AI and ML algorithms that alert about the suspicious behavior of a network and detect unauthorized intrusions.

- **AI to Combat AI Threats**

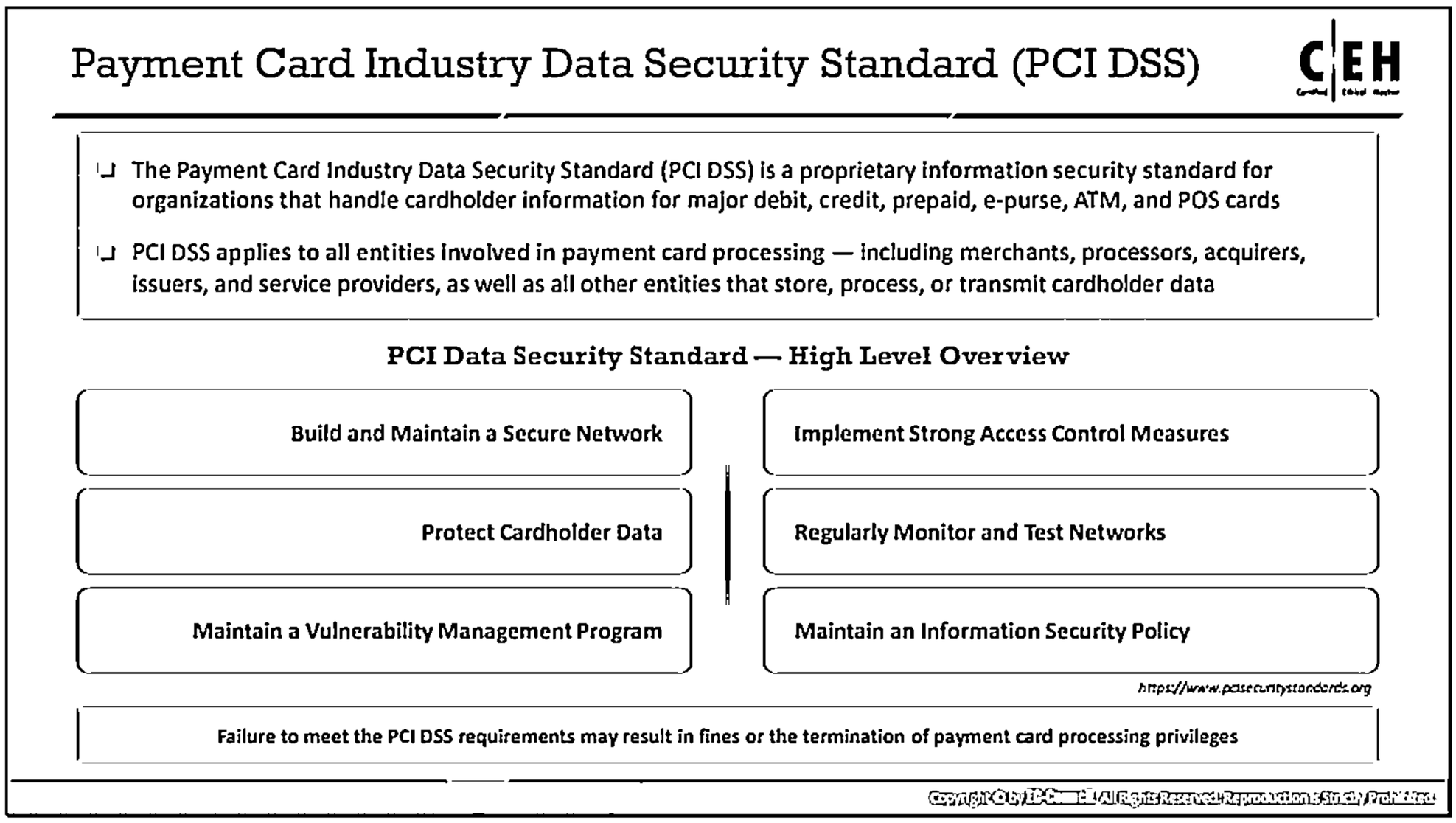
  Attackers can also leverage AI technology to make their way into an organization's network; such cyber threats must be detected immediately. AI software can detect such imminent AI-augmented attacks before the network is compromised.

Module Flow



Information Security Laws and Standards

Laws are a system of rules and guidelines that are enforced by a particular country or community to govern behavior. A Standard is a "document established by consensus and approved by a recognized body that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context." This section deals with the various laws and standards dealing with information security in different countries.



Payment Card Industry Data Security Standard (PCI DSS)

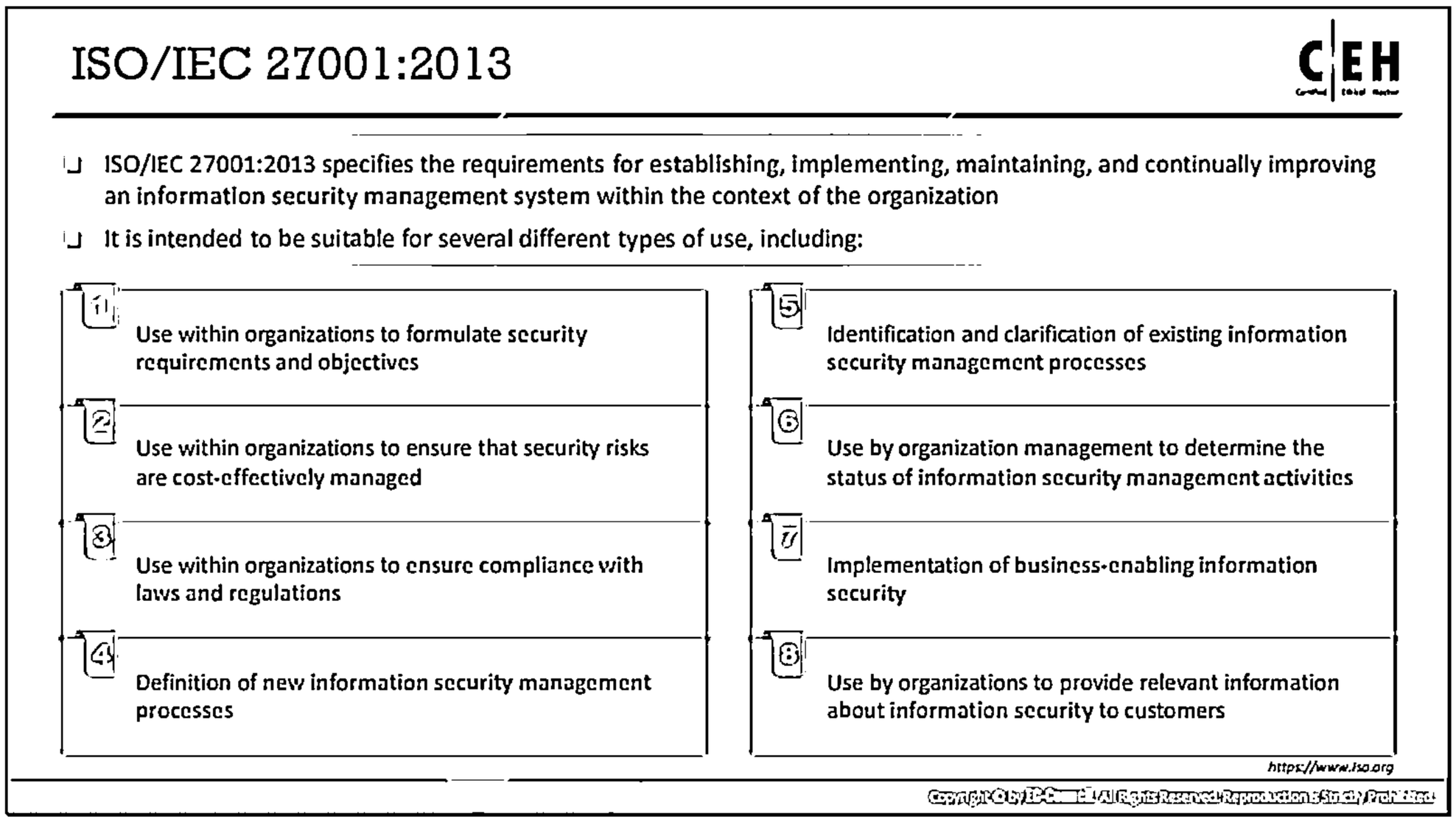
Source: *https://www.pcisecuritystandards.org*

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data. The Payment Card Industry (PCI) Security Standards Council has developed and maintains a high-level overview of PCI DSS requirements.

PCI Data Security Standard - High Level Overview	
Build and Maintain a Secure Network	▪ Install and maintain a firewall configuration to protect cardholder data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored cardholder data ▪ Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software or programs ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to cardholder data by business need to know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security for all personnel

Table 1.3: Table Showing the PCI Data Security Standard—High-Level Overview

Failure to meet PCI DSS requirements may result in fines or the termination of payment-card processing privileges.



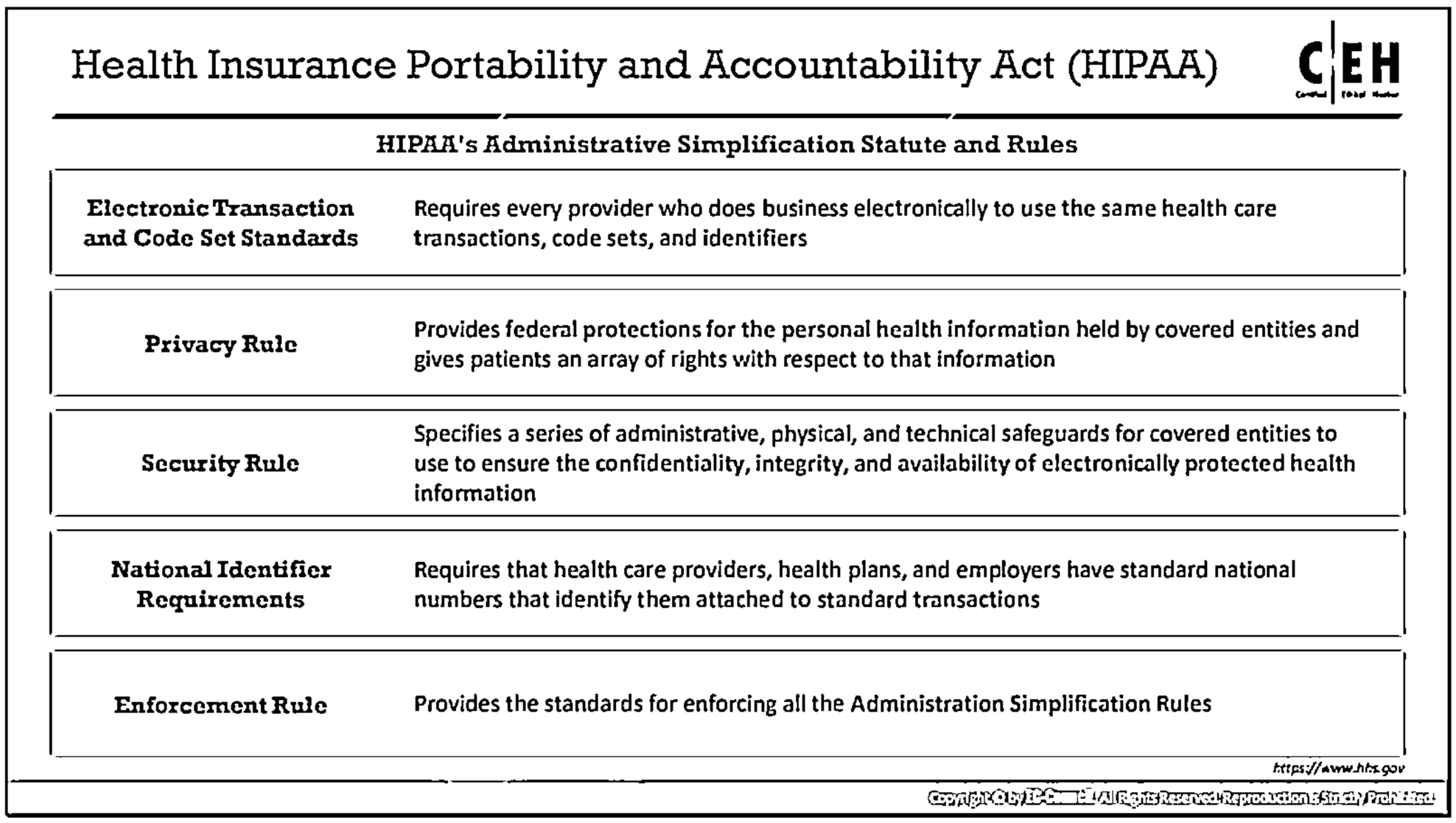
ISO/IEC 27001:2013

Source: *https://www.iso.org*

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of an organization. It includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

The regulation is intended to be suitable for several different uses, including:

- Use within organizations to formulate security requirements and objectives
- Use within organizations as a way to ensure that security risks are cost-effectively managed
- Use within organizations to ensure compliance with laws and regulations
- Defining new information security management processes
- Identifying and clarifying existing information security management processes
- Use by the management of organizations to determine the status of information security management activities
- Implementing business-enabling information security
- Use by organizations to provide relevant information about information security to customers



Health Insurance Portability and Accountability Act (HIPAA)

Source: *https://www.hhs.gov*

The HIPAA Privacy Rule provides federal protections for the individually identifiable health information held by covered entities and their business associates and gives patients an array of rights to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other necessary purposes.

The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to ensure the confidentiality, integrity, and availability of electronically protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transactions and Code Set Standards**

  Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) designated certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for the Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payment. Under HIPAA, if a covered entity electronically conducts one of the adopted transactions, they must use the adopted standard—either from ASC, X12N, or NCPDP (for certain pharmacy

transactions). Covered entities must adhere to the content and format requirements of each transaction. Every provider who does business electronically must use the same health care transactions, code sets, and identifiers.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect people's medical records and other personal health information and applies to health plans, health care clearinghouses, and health care providers that conduct certain health care transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information. It sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients rights over their health information, including the right to examine and obtain a copy of their health records and to request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronically protected health information.

- **Employer Identifier Standard**

  The HIPAA requires that each employer has a standard national number that identifies them on standard transactions.

- **National Provider Identifier Standard (NPI)**

  The National Provider Identifier (NPI) is a HIPAA Administrative Simplification Standard. The NPI is a unique identification number assigned to covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

  The HIPAA Enforcement Rule contains provisions relating to compliance and investigation, as well as the imposition of civil monetary penalties for violations of the HIPAA Administrative Simplification Rules and procedures for hearings.

Sarbanes Oxley Act (SOX)

- Enacted in 2002, the Sarbanes-Oxley Act is designed to protect investors and the public by increasing the accuracy and reliability of corporate disclosures
- The key requirements and provisions of SOX are organized into 11 titles:

Title I	Public Company Accounting Oversight Board (PCAOB) provides independent oversight of public accounting firms providing audit services ("auditors")
Title II	Auditor Independence establishes the standards for external auditor independence, intended to limit conflicts of interest and address new auditor approval requirements, audit partner rotation, and auditor reporting requirements
Title III	Corporate Responsibility mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports
Title IV	Enhanced Financial Disclosures describe enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers
Title V	Analyst Conflicts of Interest consist of measures designed to help restore investor confidence in the reporting of securities analysts
Title VI	Commission Resources and Authority defines practices to restore investor confidence in securities analysts

Sarbanes Oxley Act (SOX) (Cont'd)

Title VII	Studies and Reports includes the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations and enforcement actions, and whether investment banks assisted Enron, Global Crossing, or others to manipulate earnings and obfuscate true financial conditions
Title VIII	Corporate and Criminal Fraud Accountability describes specific criminal penalties for fraud by the manipulation, destruction, or alteration of financial records, or other interference with investigations while providing certain protections for whistle-blowers
Title IX	White Collar Crime Penalty Enhancement increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds the failure to certify corporate financial reports as a criminal offense
Title X	Corporate Tax Returns states that the Chief Executive Officer should sign the company tax return
Title XI	Corporate Fraud Accountability identifies corporate fraud and record tampering as criminal offenses and assigns them specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to temporarily freeze large or unusual payments

https://www.sec.gov

Sarbanes Oxley Act (SOX)

Source: *https://www.sec.gov*

Enacted in 2002, the Sarbanes-Oxley Act aims to protect the public and investors by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization must store records but describes the records that organizations must store and the duration of their storage. The Act mandated several reforms to enhance corporate responsibility, enhance financial disclosures, and combat corporate and accounting fraud.

The key requirements and provisions of SOX are organized into 11 titles:

- **Title I: Public Company Accounting Oversight Board (PCAOB)**

  Title I consists of nine sections and establishes the Public Company Accounting Oversight Board to provide independent oversight of public accounting firms that provide audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- **Title II: Auditor Independence**

  Title II consists of nine sections and establishes standards for external auditor independence to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (such as consulting) for the same clients.

- **Title III: Corporate Responsibility**

  Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction between external auditors and corporate audit committees and specifies the corporate officers' responsibility for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

  Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures, and the stock transactions of corporate officers. It requires internal controls to ensure the accuracy of financial reports and disclosures and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial conditions and specific enhanced reviews of corporate reports by the SEC or its agents.

- **Title V: Analyst Conflicts of Interest**

  Title V consists of only one section that discusses the measures designed to help restore investor confidence in the reporting of securities analysts. It defines the code of conduct for securities analysts and requires that they disclose any knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

  Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines the conditions to bar a person from practicing as a broker, advisor, or dealer.

- **Title VII: Studies and Reports**

  Title VII consists of five sections and requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and to report their findings. The required studies and reports include the effects of the consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

  Title VIII, also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for the manipulation, destruction, or alteration of financial records or interference with investigations, while also providing certain protections for whistle-blowers.

- **Title IX: White-Collar-Crime Penalty Enhancement**

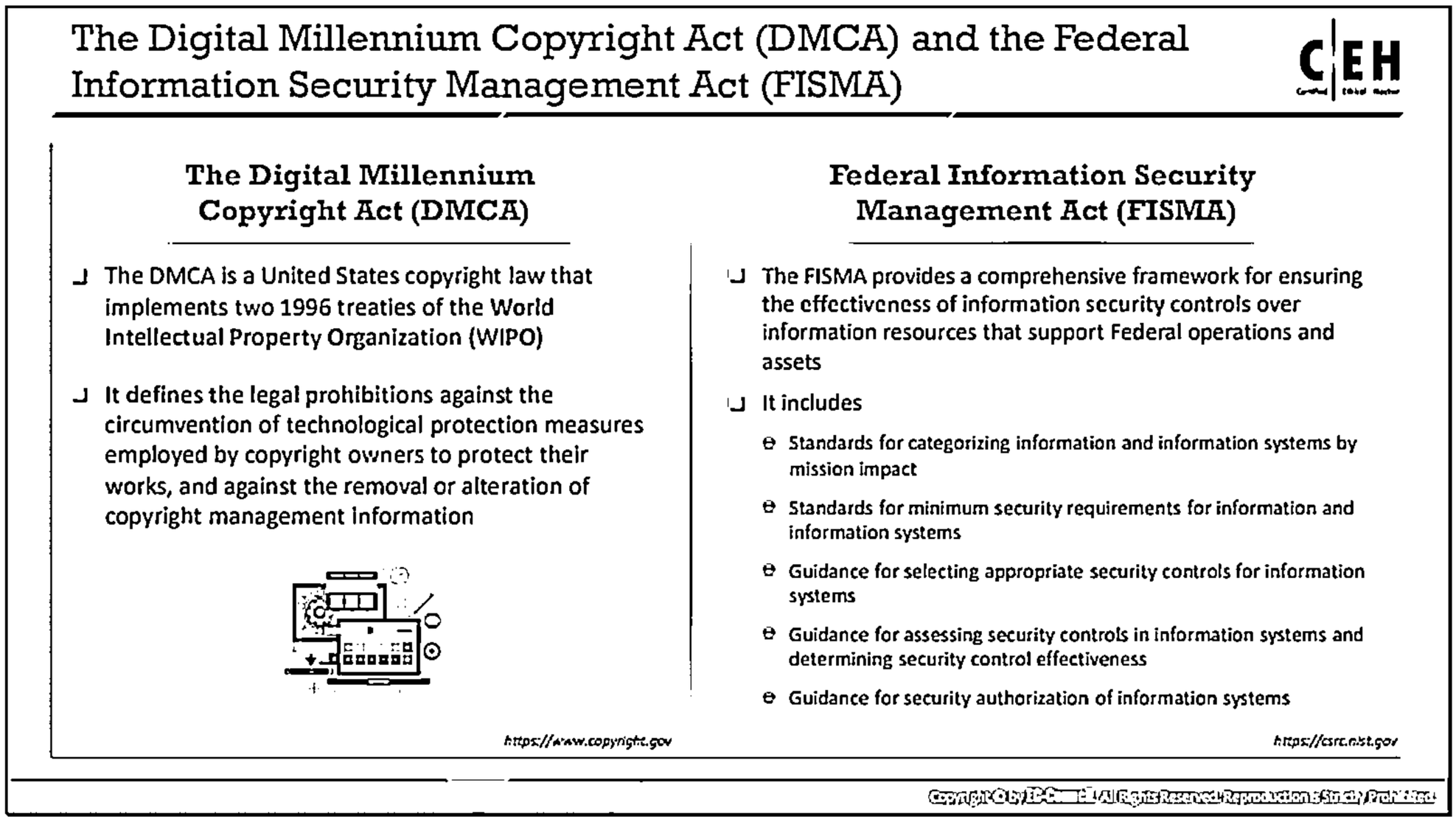
  Title IX, also known as the "White Collar Crime Penalty Enhancement Act of 2002," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

- **Title X: Corporate Tax Returns**

  Title X consists of one section that states that the Chief Executive Officer should sign the company tax return.

- **Title XI: Corporate Fraud Accountability**

  Title XI consists of seven sections. Section 1101 recommends the following name for the title: "Corporate Fraud Accountability Act of 2002." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens penalties. Doing so enables the SEC to temporarily freeze "large" or "unusual" transactions or payments.



The Digital Millennium Copyright Act (DMCA)

Source: *https://www.copyright.gov*

The DMCA is an American copyright law that implements two 1996 treaties from the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. In order to implement US treaty obligations, the DMCA defines legal prohibitions against circumvention of the technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information. The DMCA contains five titles:

- **Title I: WIPO TREATY IMPLEMENTATION**

  Title I implements the WIPO treaties. First, it makes certain technical amendments to US law in order to provide the appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of the technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

- **Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION**

  Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. A service provider bases these limitations on the following four categories of conduct:

  - Transitory communications
  - System caching
  - The user-directed storage of information on systems or networks

- Information location tools

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III: COMPUTER MAINTENANCE OR REPAIR**

Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or to authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV: MISCELLANEOUS PROVISIONS**

Title IV contains six miscellaneous provisions. The first provision announces the Clarification of the Authority of the Copyright Office; the second grants exemption for the making of "ephemeral recordings"; the third promotes study by distance education; the fourth provides an exemption for Nonprofit Libraries and Archives; the fifth allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and, finally, the sixth provision addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations where the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

Title V of the DMCA, entitles the Vessel Hull Design Protection Act (VHDPA). This act creates a new system for protecting the original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

The Federal Information Security Management Act (FISMA)

Source: *https://csrc.nist.gov*

The Federal Information Security Management Act of 2002 was enacted to produce several key security standards and guidelines required by Congressional legislation. The FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or another source. The FISMA framework includes:

- Standards for categorizing information and information systems by mission impact
- Standards for the minimum security requirements for information and information systems
- Guidance for selecting appropriate security controls for information systems

- Guidance for assessing security controls in information systems and determining their effectiveness
- Guidance for the security authorization of information systems

Cyber Law in Different Countries

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Esplonage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net

Cyber Law in Different Countries (Cont'd)

Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

Cyber Law in Different Countries

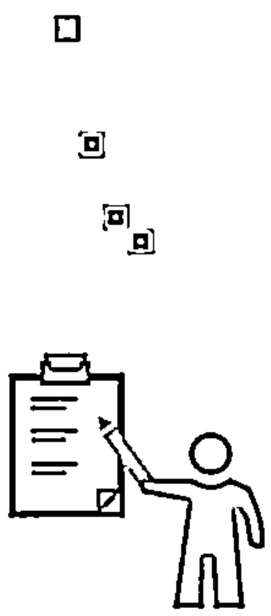
Cyberlaw or Internet law refers to any laws that deal with protecting the Internet and other online communication technologies. Cyberlaw covers topics such as Internet access and usage, privacy, freedom of expression, and jurisdiction. Cyber laws provide an assurance of the integrity, security, privacy, and confidentiality of information in both governmental and private organizations. These laws have become prominent due to the increase in Internet usage around the world. Cyber laws vary by jurisdiction and country, so implementing them is quite challenging. Violating these laws results in punishments ranging from fines to imprisonment.

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	https://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	https://www.uspto.gov
	The Electronic Communications Privacy Act	https://fas.org
	Foreign Intelligence Surveillance Act	https://fas.org
	Protect America Act of 2007	https://www.justice.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.nrotc.navy.mil
	Computer Security Act of 1987	https://csrc.nist.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov

	Computer Fraud and Abuse Act	https://energy.gov
	Federal Identity Theft and Assumption Deterrence Act	https://www.ftc.gov
Australia	The Trade Marks Act 1995	https://www.legislation.gov.au
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	https://www.legislation.gov.uk
	Trademarks Act 1994 (TMA)	
	Computer Misuse Act 1990	
China	Copyright Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	https://www.meity.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	https://www.cybercrimelaw.net
Italy	Penal Code Article 615 ter	https://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	https://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
South Africa	Trademarks Act 194 of 1993	http://www.cipc.co.za
	Copyright Act of 1978	https://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916	https://www.copyright.or.kr
	Industrial Design Protection Act	https://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994	https://www.wipo.int
	Computer Hacking	https://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Hong Kong	Article 139 of the Basic Law	https://www.basiclaw.gov.hk

Table 1.4: Cyber Law in Different Countries

Module Summary



- This module discussed elements of information security, information security attacks, and information warfare
- It discussed cyber kill chain methodology, TTPs, and IoCs in detail
- It also discussed hacking concepts, types, and phases
- This module also covered ethical hacking concepts such as the scope and limitations of ethical hacking, skills, and other pertinent information in detail
- It discussed information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML
- This module ended with a detailed discussion of various information security acts and laws from around the world
- The next module will go into detail about how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about the target of an evaluation before an attack or audit

Module Summary

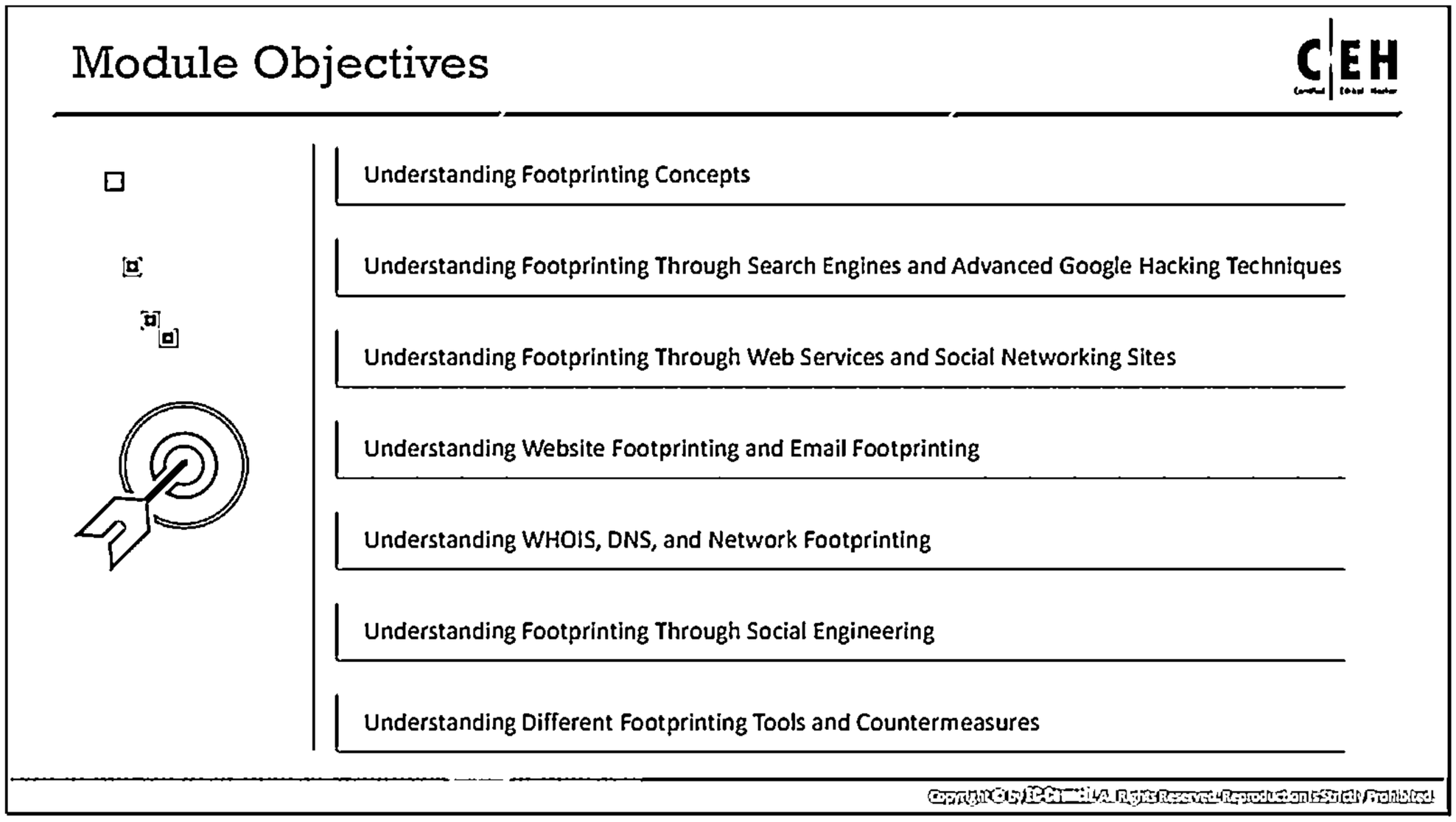
This module has discussed elements of information security, information security attacks, and information warfare. It has covered cyber kill chain methodology, TTPs, and IoCs in detail. It also discussed hacking concepts, types, and phases. This module closely examined ethical hacking concepts such as its scope and limitations and the skills of an ethical hacker. It also covered the topic of information security controls such as defense-in-depth, risk management, cyber threat intelligence, threat modeling, incident management process, and AI and ML. Finally, this module ended with a detailed discussion of various information security acts and laws.

The next module will examine how attackers, as well as ethical hackers and pen testers, perform footprinting to collect information about their target before an attack or audit.

C|EH™

Certified Ethical Hacker

Module 02:
Footprinting and Reconnaissance



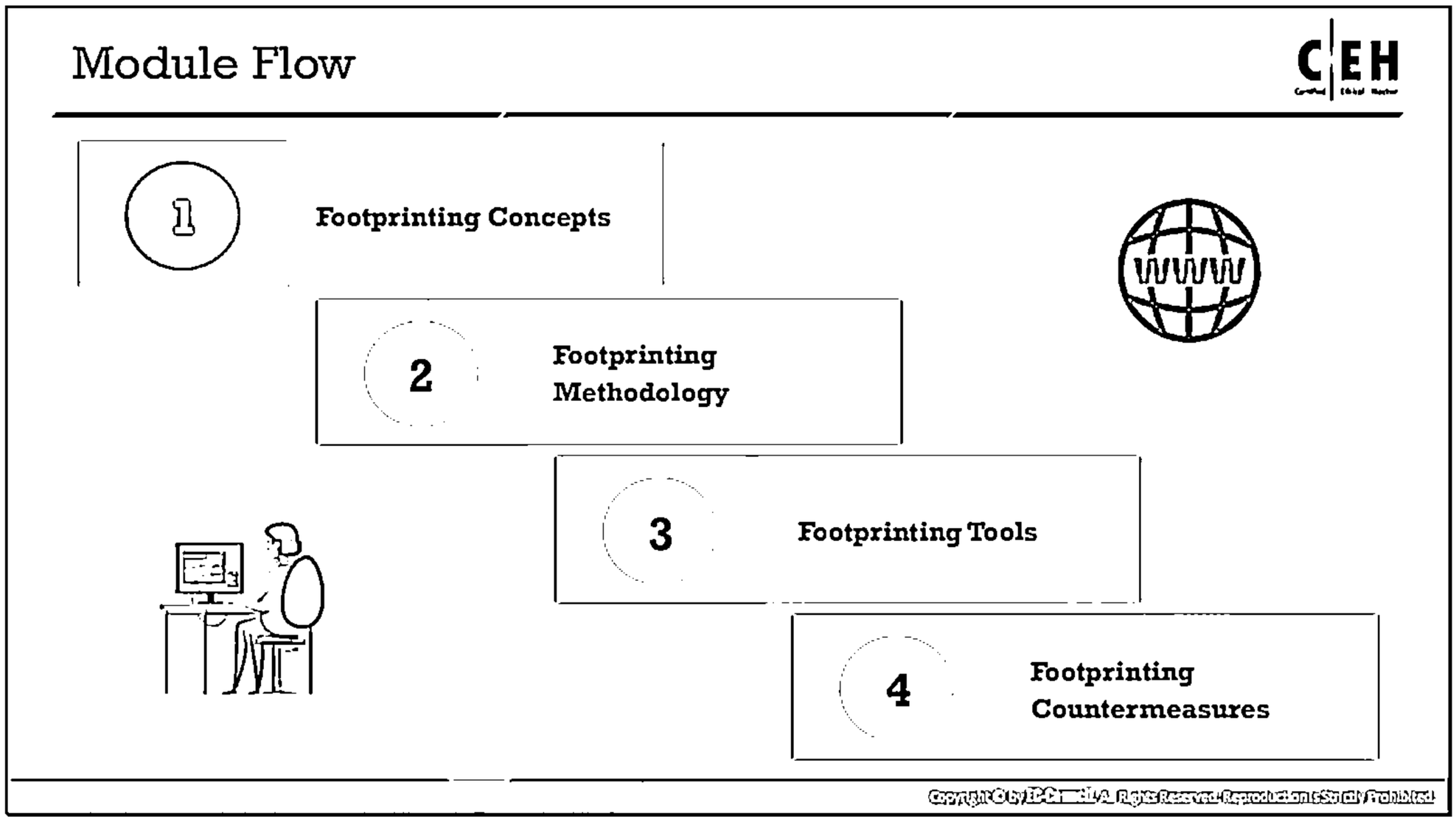
Module Objectives

Footprinting is the first step in the evaluation of the security posture of the IT infrastructure of a target organization. Through footprinting and reconnaissance, one can gather maximum information about a computer system or a network and about any device connected to that network. In other words, footprinting provides a security profile blueprint for an organization and should be undertaken in a methodological manner.

This module starts with an introduction to footprinting concepts and provides insights into the footprinting methodology. The module ends with an overview of footprinting tools and countermeasures.

At the end of this module, you will be able to:

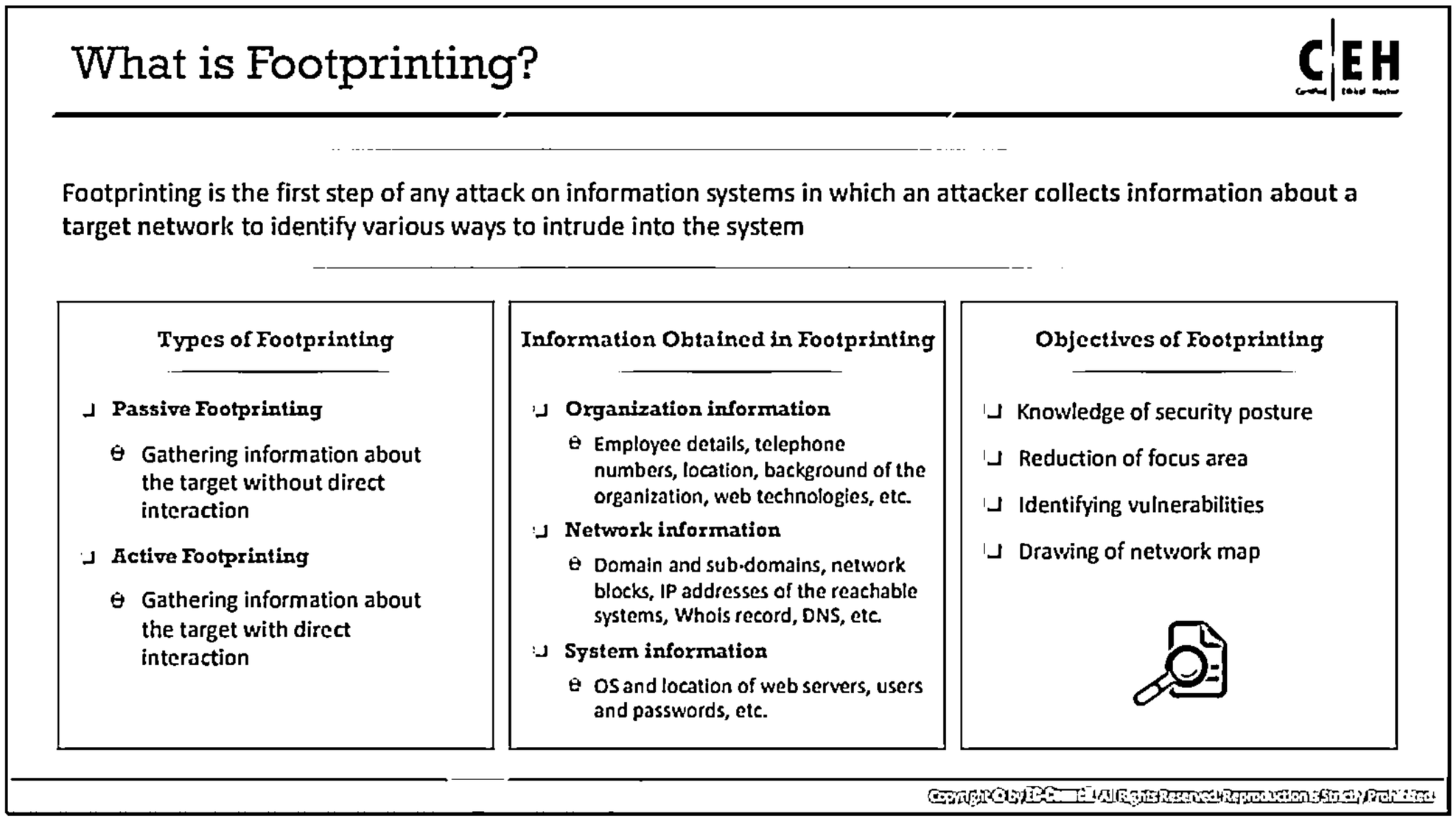
- Describe footprinting concepts
- Perform footprinting through search engines and using advanced Google hacking techniques
- Perform footprinting through web services and social networking sites
- Perform website footprinting and email footprinting
- Perform Whois, DNS, and network footprinting
- Perform footprinting through social engineering
- Use different footprinting tools
- Apply footprinting best practices



Footprinting Concepts

Ethical hacking is legal in nature and conducted to evaluate the security of a target organization's IT infrastructure with their consent. Footprinting, where an attacker tries to gather information about a target, is the first step in ethical hacking. This step acts as a preparatory phase for the attacker, who needs to gather as much information as possible to easily find ways to intrude into the target network.

This section aims to familiarize you with footprinting, why it is necessary, and its objectives.



What is Footprinting?

An essential aspect of footprinting is identifying the level of risk associated with the organization's publicly accessible information. Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using footprinting, you can find a number of opportunities to penetrate and assess the target organization's network.

After you complete the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of the target organization. Here, the term "blueprint" refers to the unique system profile of the target organization acquired by footprinting.

There is no single methodology for footprinting, as information can be traced in a number of ways. However, the activity is important, as you need to gather all the crucial information about the target organization before beginning the hacking phase. For this reason, footprinting needs to be carried out in an organized manner. The information gathered in this step helps in uncovering vulnerabilities existing in the target network and in identifying different ways of exploiting these vulnerabilities.

Types of Footprinting

Footprinting can be categorized into passive footprinting and active footprinting.

- **Passive Footprinting**

  Passive footprinting involves gathering information about the target without direct interaction. It is mainly useful when the information gathering activities are not to be detected by the target. Performing passive footprinting is technically difficult, as active traffic is not sent to the target organization from a host or anonymous hosts or services

over the Internet. We can only collect archived and stored information about the target using search engines, social networking sites, and so on.

Passive footprinting techniques include:

- Finding information through search engines
- Finding the Top-level Domains (TLDs) and sub-domains of a target through web services
- Collecting location information on the target through web services
- Performing people search using social networking sites and people search services
- Gathering financial information about the target through financial services
- Gathering infrastructure details of the target organization through job sites
- Collecting information through deep and dark web footprinting
- Determining the operating systems in use by the target organization
- Performing competitive intelligence
- Monitoring the target using alert services
- Gathering information using groups, forums, blogs, and NNTP Usenet newsgroups
- Collecting information through social engineering on social networking sites
- Extracting information about the target using Internet archives
- Gathering information using business profile sites
- Monitoring website traffic of the target
- Tracking the online reputation of the target

- **Active Footprinting**

  Active footprinting involves gathering information about the target with direct interaction. In active footprinting, the target may recognize the ongoing information gathering process, as we overtly interact with the target network. Active footprinting requires more preparation than passive footprinting, as it may leave traces that may alert the target organization.

  Active footprinting techniques include:

  - Querying published name servers of the target
  - Searching for digital files
  - Extracting website links and gathering wordlists from the target website
  - Extracting metadata of published documents and files
  - Gathering website information using web spidering and mirroring tools
  - Gathering information through email tracking

- Harvesting email lists
- Performing Whois lookup
- Extracting DNS information
- Performing traceroute analysis
- Performing social engineering

Information Obtained in Footprinting

The major objectives of footprinting include collecting the network information, system information, and organizational information of the target. By conducting footprinting across different network levels, you can gain information such as network blocks, specific IP addresses, employee details, and so on. Such information can help attackers in gaining access to sensitive data or performing various attacks on the target network.

- **Organization Information**: Such information about an organization is available from its website. In addition, you can query the target's domain name against the Whois database and obtain valuable information.

  The information collected includes:

  - Employee details (employee names, contact addresses, designations, and work experience)
  - Addresses and mobile/telephone numbers
  - Branch and location details
  - Partners of the organization
  - Web links to other company-related sites
  - Background of the organization
  - Web technologies
  - News articles, press releases, and related documents
  - Legal documents related to the organization
  - Patents and trademarks related to the organization

  Attackers can access organizational information and use such information to identify key personnel and launch social engineering attacks to extract sensitive data about the entity.

- **Network Information**: You can gather network information by performing Whois database analysis, trace routing, and so on.

  The information collected includes:

  - Domain and sub-domains
  - Network blocks
  - Network topology, trusted routers, and firewalls

- IP addresses of the reachable systems
- Whois records
- DNS records and related information

- **System Information**: You can gather system information by performing network footprinting, DNS footprinting, website footprinting, email footprinting, and so on.

  The information collected includes:

  - Web server OS
  - Location of web servers
  - Publicly available email addresses
  - Usernames, passwords, and so on.

Objectives of Footprinting

To build a hacking strategy, attackers need to gather information about the target organization's network. They then use such information to locate the easiest way to break through the organization's security perimeter. As mentioned previously, the footprinting methodology makes it easy to gather information about the target organization; this plays a vital role in the hacking process.

Footprinting helps to

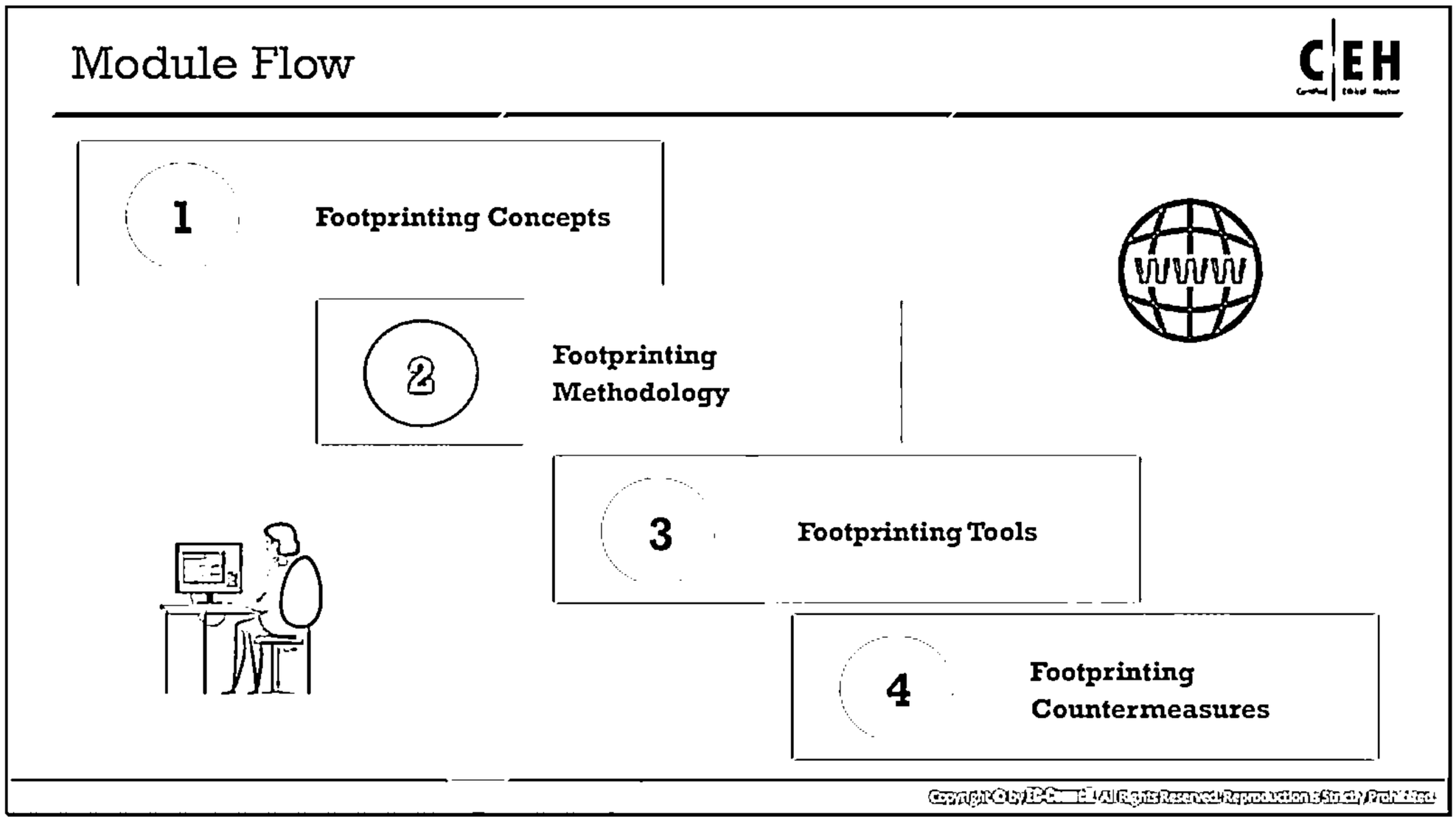
- **Know Security Posture**: Performing footprinting on the target organization gives the complete profile of the organization's security posture. Hackers can then analyze the report to identify loopholes in the security posture of the target organization and build a hacking plan accordingly.
- **Reduce Focus Area**: By using a combination of tools and techniques, attackers can take an unknown entity (for example, XYZ Organization) and reduce it to a specific range of domain names, network blocks, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its security posture.
- **Identify Vulnerabilities**: A detailed footprint provides maximum information about the target organization. It allows the attacker to identify vulnerabilities in the target systems to select appropriate exploits. Attackers can build their own information database about the security weaknesses of the target organization. Such a database can then help in identifying the weakest link in the organization's security perimeter.
- **Draw Network Map**: Combining footprinting techniques with tools such as Tracert allows the attacker to create diagrammatic representations of the target organization’s network presence. Specficially, it allows attackers to draw a map or outline of the target organization’s network infrastructure to know about the actual environment that they are going to break into. A network map will depict the attacker’s understanding of the target's Internet footprint. These network diagrams can guide the attacker in performing an attack.

Footprinting Threats

Attackers perform footprinting as the first step of any attack on information systems. In this phase, attackers attempt to collect valuable system-level information such as account details, operating system and other software versions, server names, database schema details, and so on, which will be useful in the hacking process.

The following are assorted threats made possible through footprinting:

- **Social Engineering**: Without using any intrusion methods, hackers directly and indirectly collect information through persuasion and other means. Hackers gather crucial information from willing employees who are unaware of the hackers' intent.
- **System and Network Attacks**: Footprinting enables an attacker to perform system and network attacks. Thus, attackers can gather information related to the target organization's system configuration, the operating system running on the machine, and so on. Using this information, attackers can find vulnerabilities in the target system and then exploit such vulnerabilities. They can then take control of a target system or the entire network.
- **Information Leakage**: Information leakage poses a threat to any organization. If sensitive information of an entity falls into the hands of attackers, they can mount an attack based on the information or alternatively use it for monetary benefit.
- **Privacy Loss**: Through footprinting, hackers can access the systems and networks of the organization and even escalate the privileges up to admin levels, resulting in the loss of privacy for the organization as a whole and for its individual personnel.
- **Corporate Espionage**: Corporate espionage is a central threat to organizations, as competitors often aim to attempt to secure sensitive data through footprinting. Through this approach, competitors can launch similar products in the market, alter prices, and generally undermine the market position of a target organization.
- **Business Loss**: Footprinting can have a major effect on organizations such as online businesses and other e-commerce websites as well as banking and finance-related businesses. Billions of dollars are lost every year due to malicious attacks by hackers.



Footprinting Methodology

Now that you are familiar with footprinting concepts and potential threats, we will discuss the footprinting methodology. The footprinting methodology is a procedure for collecting information about a target organization from all available sources. It involves gathering information about a target organization, such as URLs, locations, establishment details, number of employees, specific range of domain names, contact information, and other related information. Attackers collect this information from publicly accessible sources such as search engines, social networking sites, Whois databases, and so on. This section discusses the common techniques used to collect information about the target organization from different sources.

Footprinting techniques:

- Footprinting through search engines
- Footprinting through web services
- Footprinting through social networking sites
- Website footprinting
- Email footprinting
- Whois footprinting
- DNS footprinting
- Network footprinting
- Footprinting through social engineering

Footprinting through Search Engines

- Attackers use search engines to extract information about a target, such as employed technology platforms, employee details, login pages, and intranet portals, which help the attacker to perform social engineering and other types of advanced system attacks
- Major search engines:

  Google Bing YAHOO! Ask Aol. Baidu 百度 DuckDuckGo
- Attackers can use advanced search operators available with these search engines and create complex queries to find, filter, and sort specific information about the target
- Search engines are also used to find other sources of publically accessible information resources, e.g., you can type "top job portals" to find major job portals that provide critical information about the target organization

Footprinting through Search Engines

Search engines are the main sources of key information about a target organization. They play a major role in extracting critical details about a target from the Internet. Search engines use automated software, i.e., crawlers, to continuously scan active websites and add the retrieved results in the search engine index that is further stored in a massive database. When a user queries the search engine index, it returns a list of Search Engine Results Pages (SERPs). These results include web pages, videos, images, and many different file types ranked and displayed according to their relevance. Many search engines can extract target organization information such as technology platforms, employee details, login pages, intranet portals, contact information, and so on. The information helps the attacker in performing social engineering and other types of advanced system attacks.

A Google search could reveal submissions to forums by security personnel, disclosing the brands of firewalls or antivirus software used by the target. This information helps the attacker in identifying vulnerabilities in such security controls.

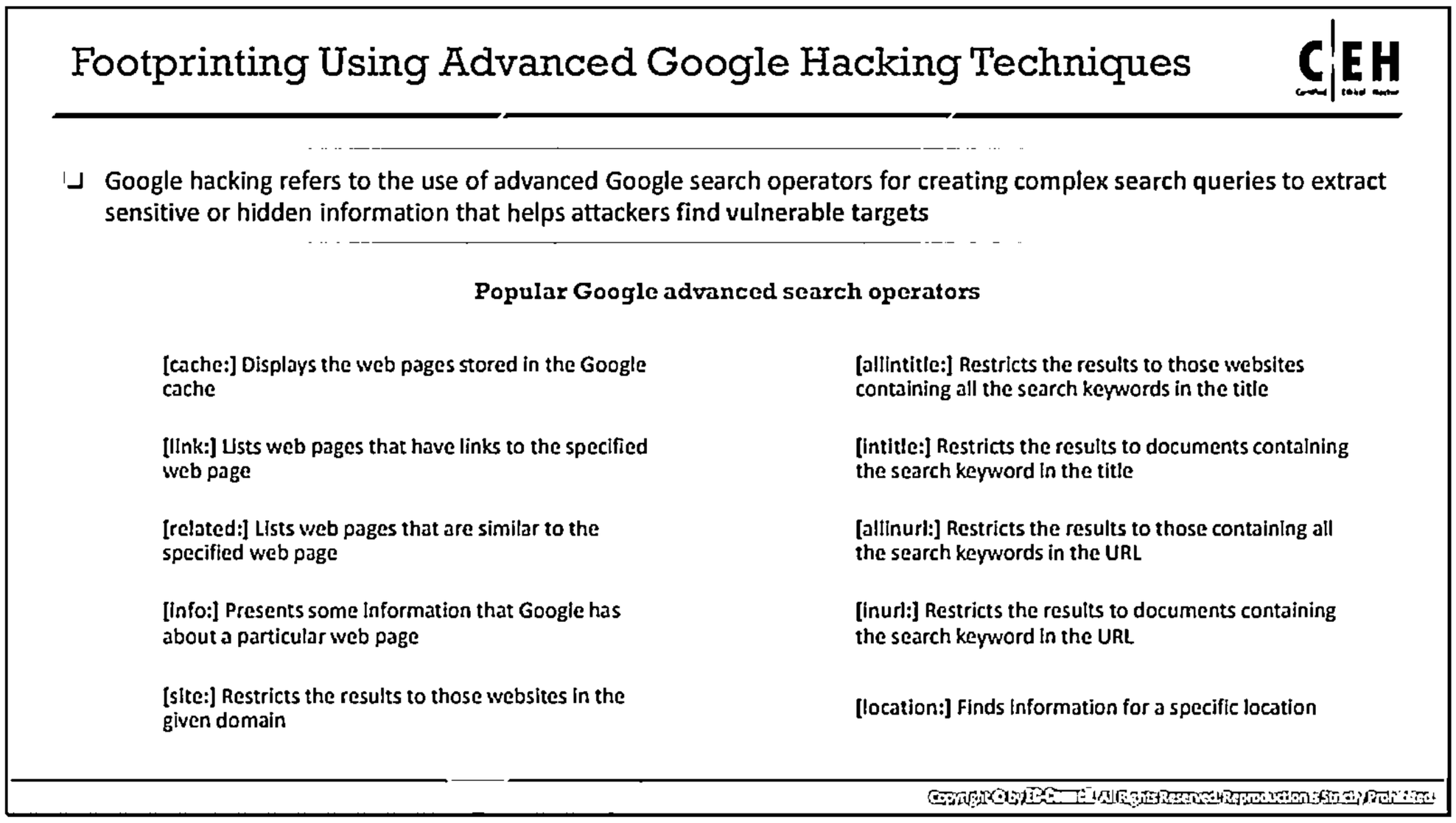
For example, consider an organization, perhaps Microsoft. Type **Microsoft** in the **Search** box of a search engine and press **Enter**; this will display the results containing information about Microsoft. Browsing the results often provides critical information such as physical location, contact addresses, services offered, number of employees, and so on, which may prove to be a valuable source for hacking.

Examples of major search engines include Google, Bing, Yahoo, Ask, Aol, Baidu, WolframAlpha, and DuckDuckGo.

Attackers can use advanced search operators available with these search engines and create complex queries to find, filter, and sort specific information regarding the target. Search engines

are also used to find other sources of publicly accessible information. For example, you can type "top job portals" to find major job portals that provide critical information about the target organization.

As an ethical hacker, if you find any deleted pages/information about your company in SERPs or the search engine cache, you can request the search engine to remove the pages/information from its indexed cache.



Footprinting Using Advanced Google Hacking Techniques

Google hacking refers to the use of advanced Google search operators for creating complex search queries to extract sensitive or hidden information. The accessed information is then used by attackers to find vulnerable targets. Footprinting using advanced Google hacking techniques involves locating specific strings of text within search results using advanced operators in the Google search engine.

Advanced Google hacking refers to the art of creating complex search engine queries. Queries can retrieve valuable data about a target company from Google search results. Through Google hacking, an attacker tries to find websites that are vulnerable to exploitation. Attackers can use the Google Hacking Database (GHDB), a database of queries, to identify sensitive data. Google operators help in finding the required text and avoiding irrelevant data. Using advanced Google operators, attackers can locate specific strings of text such as specific versions of vulnerable web applications. When a query without advanced search operators is specified, Google traces the search terms in any part of the webpage, including the title, text, URL, digital files, and so on. To confine a search, Google offers advanced search operators. These search operators help to narrow down the search query and obtain the most relevant and accurate output.

The syntax to use an advanced search operator is as follows: operator**: search_term**

Note: Do not enter any spaces between the operator and the query.

Some popular Google advanced search operators include:

Source: *http://www.googleguide.com*

- **site:** This operator restricts search results to the specified site or domain.

  For example, the [games site: www.certifiedhacker.com] query gives information on games from the certifiedhacker site.

- **allinurl**: This operator restricts results to only the pages containing all the query terms specified in the URL.

  For example, the [allinurl: google career] query returns only pages containing the words "google" and "career" in the URL.

- **inurl**: This operator restricts the results to only the pages containing the specified word in the URL.

  For example, the [inurl: copy site:www.google.com] query returns only Google pages in which the URL has the word "copy."

- **allintitle**: This operator restricts results to only the pages containing all the query terms specified in the title.

  For example, the [allintitle: detect malware] query returns only pages containing the words "detect" and "malware" in the title.

- **intitle**: This operator restricts results to only the pages containing the specified term in the title.

  For example, the [malware detection intitle:help] query returns only pages that have the term "help" in the title, and the terms "malware" and "detection" anywhere within the page.

- **inanchor**: This operator restricts results to only the pages containing the query terms specified in the anchor text on links to the page.

  For example, the [Anti-virus inanchor:Norton] query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus."

- **allinanchor**: This operator restricts results to only the pages containing all query terms specified in the anchor text on links to the pages.

  For example, the [allinanchor: best cloud service provider] query returns only pages for which the anchor text on links to the pages contains the words "best," "cloud," "service," and "provider."

- **cache**: This operator displays Google's cached version of a web page instead of the current version of the web page.

  For example, [cache:www.eff.org] will show Google's cached version of the Electronic Frontier Foundation home page.

- **link**: This operator searches websites or pages that contain links to the specified website or page.

  For example, [link:www.googleguide.com] finds pages that point to Google Guide's home page.

  Note: According to Google's documentation, "you cannot combine a link: search with a regular keyword search."

Also note that when you combine link: with another advanced operator, Google may not return all the pages that match.

- **related**: This operator displays websites that are similar or related to the URL specified.

  For example, [related:www.microsoft.com] provides the Google search engine results page with websites similar to microsoft.com.

- **info**: This operator finds information for the specified web page.

  For example, [info:gothotel.com] provides information about the national hotel directory GotHotel.com home page.

- **location:** This operator finds information for a specific location.

  For example, [location: 4 seasons restaurant] will give you results based on the term "4 seasons restaurant."

- **Filetype:** This operator allows you to search for results based on a file extension.

  For Example, [jasmine:jpg] will provide jpg files based on jasmine.

What can a Hacker do with Google Hacking?

An attacker can create complex search engine queries to filter large amounts of search results to obtain information related to computer security. The attacker uses Google operators that help locate specific strings of text within the search results. Thus, the attacker can not only detect websites and web servers that are vulnerable to exploitation but also locate private, sensitive information about others, such as credit card numbers, social security numbers, passwords, and so on. Once a vulnerable site is identified, attackers try to launch various possible attacks, such as buffer overflow and SQL injection, which compromise information security.

Examples of sensitive information on public servers that an attacker can extract with the help of Google Hacking Database (GHDB) queries include:

- Error messages that contain sensitive information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data, such as IDS, firewall logs, and configurations
- Advisories and server vulnerabilities
- Software version information
- Web application source code
- Connected IoT devices and their control panels, if unprotected
- Hidden web pages such as intranet and VPN services

Example: Use Google Advance Operator syntax `[intitle:intranet inurl:intranet +intext:"human resources"]` to find sensitive information about a target organization and its employees. Attackers use the gathered information to perform social engineering attacks.

The screenshot below shows a Google search engine results page displaying the results for the query mentioned above.

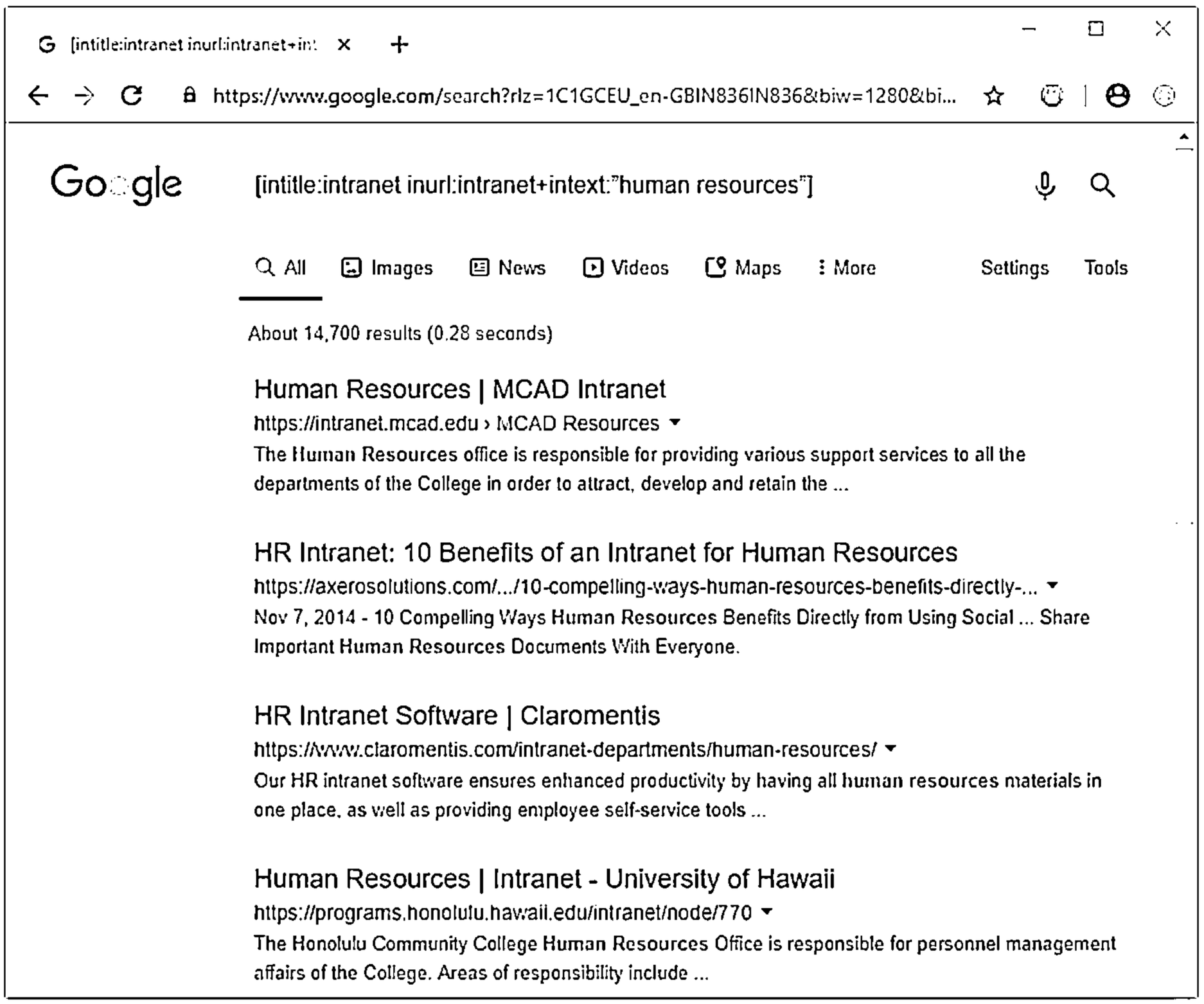
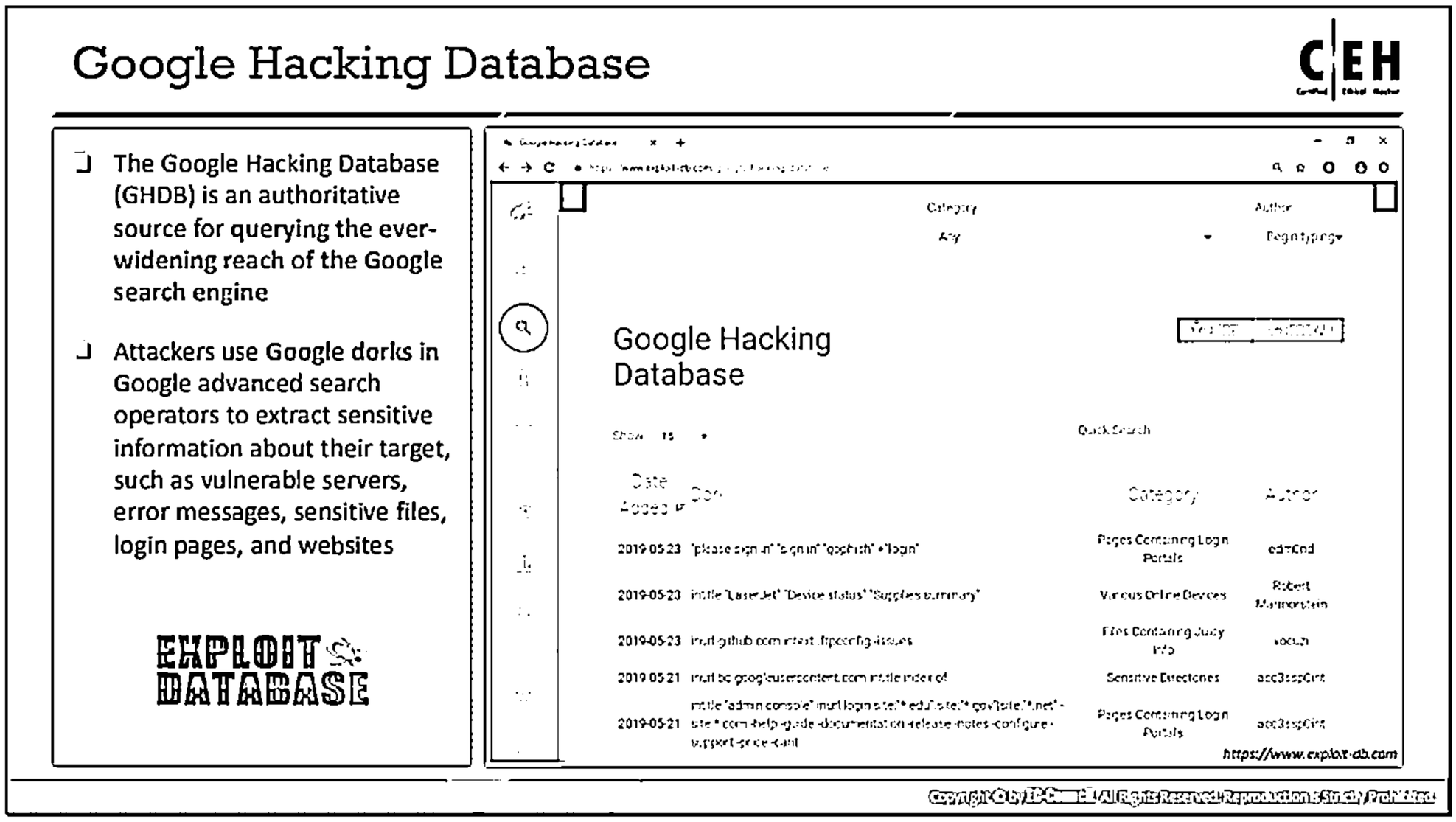


Figure 2.1: Search engine results for given Google Advance Operator syntax



Google Hacking Database

Source: *https://www.exploit-db.com*

The Google Hacking Database (GHDB) is an authoritative source for querying the ever-widening scope of the Google search engine. In the GHDB, you will find search terms for files containing usernames, vulnerable servers, and even files containing passwords. The Exploit Database is a Common Vulnerabilities and Exposures (CVE) compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

Using GHDB dorks, attackers can rapidly identify all the publicly available exploits and vulnerabilities of the target organization's IT infrastructure. Attackers use Google dorks in Google advanced search operators to extract sensitive information about the target, such as vulnerable servers, error messages, sensitive files, login pages, and websites.

Google Hacking Database Categories:

- Footholds
- Files Containing Usernames
- Sensitive Directories
- Web Server Detection
- Vulnerable Files
- Vulnerable Servers
- Error Messages
- Files Containing Juicy Info
- Files Containing Passwords
- Sensitive Online Shopping Info
- Network or Vulnerability Data
- Pages Containing Login Portals
- Various Online Devices
- Advisories and Vulnerabilities

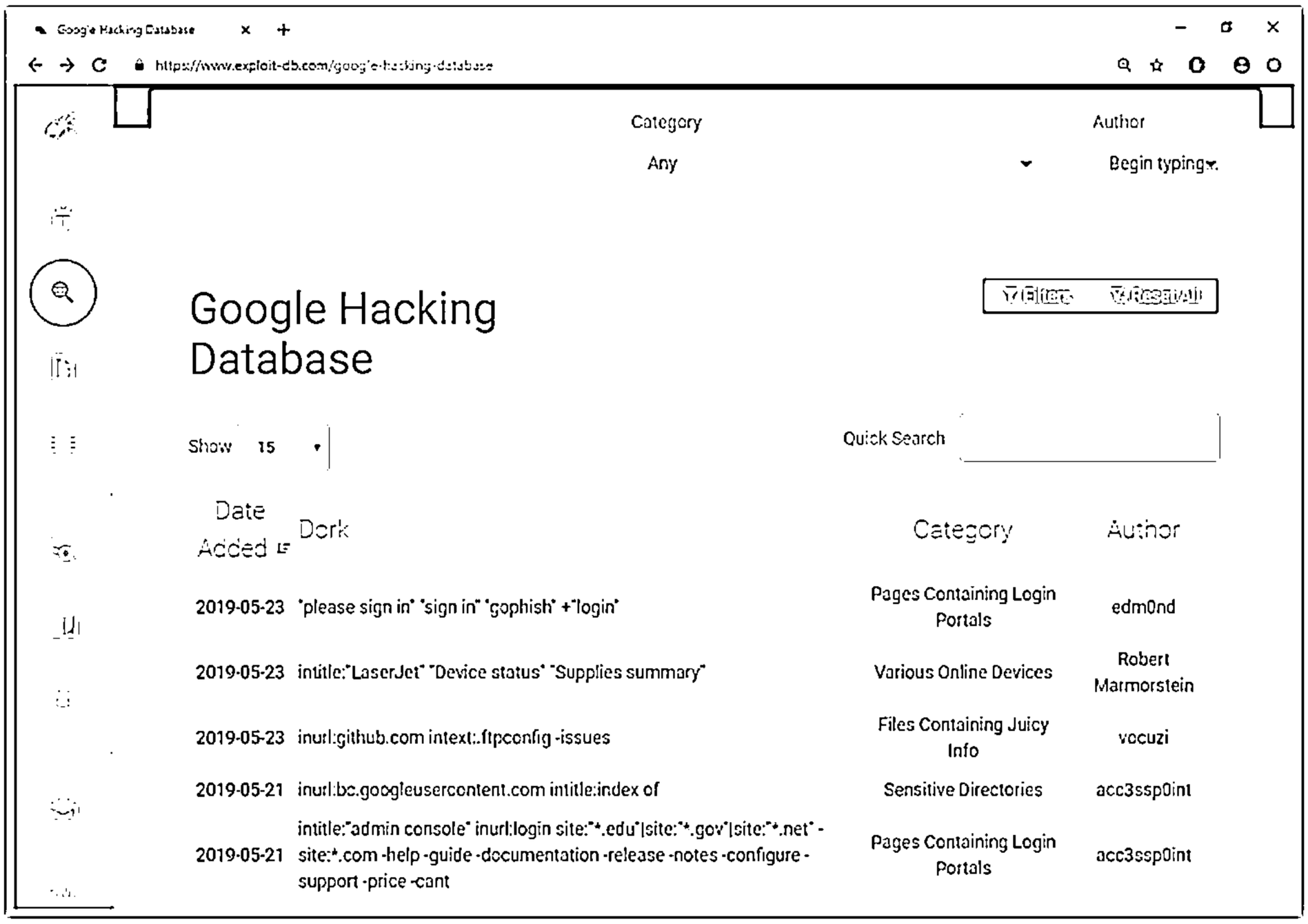


Figure 2.2: Google Hacking Database screenshot

VoIP and VPN Footprinting through Google Hacking Database

Google search queries for VoIP footprinting

Google Dork	Description
intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
inurl:/voice/advanced/ intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
intitle:"D-Link VIP Router" "Welcome"	Pages containing D-Link login portals
intitle:asterisk.management.portal web-access	Look for the Asterisk management portal
intitle:"SPA504G Configuration"	Finds Cisco SPA504G Configuration Utility for IP phones
intitle:asterisk.management.portal web-access	Finds the Asterisk web management portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals
intitle:"Sipura.SPA.Configuration" -.pdf	Finds configuration pages for online VoIP devices

Google search queries for VPN footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with Group Passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted but easily cracked!)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
!Host=*.* intext:enc_UserPassword=* ext:pcf	Looks for profile configuration files (.pcf), which contain user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login
filetype:pcf vpn OR Group	Finds publicly accessible .pcf used by VPN clients

https://www.exploit-db.com

VoIP and VPN Footprinting through Google Hacking Database

Google hacking involves the implementation of advanced operators in the Google search engine to match specific strings of text within the search result. These advanced operators help refine searches to expose sensitive information, vulnerabilities, and passwords. You can use these Google hacking operators or Google dorks for footprinting VoIP and VPN networks. Thus, you can extract information such as pages containing login portals, VoIP login portals, directories with keys of VPN servers, and so on.

The following tables summarize some of the Google hacking operators or Google dorks to obtain specific information related to VoIP and VPN footprinting, respectively.

Google search queries for VoIP footprinting

Google Dork	Description
intitle:"Login Page" intext:"Phone Adapter Configuration Utility"	Pages containing login portals
inurl:/voice/advanced/ intitle:Linksys SPA configuration	Finds the Linksys VoIP router configuration page
intitle:"D-Link VoIP Router" "Welcome"	Pages containing D-Link login portals
intitle:asterisk.management.portal web-access	Looks for the Asterisk management portal
intitle:"SPA504G Configuration"	Finds Cisco SPA504G Configuration Utility for IP phones

intitle:"Sipura.SPA.Configuration" -.pdf	Finds configuration pages for online VoIP devices
intitle:asterisk.management.portal web-access	Finds the Asterisk web management portal
inurl:8080 intitle:"login" intext:"UserLogin" "English"	VoIP login portals

Table 2.1: Google search queries for VoIP footprinting

Google search queries for VPN footprinting

Google Dork	Description
filetype:pcf "cisco" "GroupPwd"	Cisco VPN files with Group Passwords for remote access
"[main]" "enc_GroupPwd=" ext:txt	Finds Cisco VPN client passwords (encrypted but easily cracked)
"Config" intitle:"Index of" intext:vpn	Directory with keys of VPN servers
inurl:/remote/login?lang=en	Finds FortiGate Firewall's SSL-VPN login portal
!Host=*.* intext:enc_UserPassword=* ext:pcf	Looks for profile configuration files (.pcf), which contain user VPN profiles
filetype:rcf inurl:vpn	Finds Sonicwall Global VPN Client files containing sensitive information and login
filetype:pcf vpn OR Group	Finds publicly accessible .pcf used by VPN clients
vpnssl	Retrieves login portals containing vpnssl companies' access
intitle:"SSL VPN Service" + intext:"Your system administrator provided the following information to help understand and remedy the security conditions:"	Finds Cisco asa login web pages

Table 2.2: Google search queries for VPN footprinting

Other Techniques for Footprinting through Search Engines

Gathering Information Using Google Advanced Search and Advanced Image Search

- Attackers can use Google Advanced Search and Advanced Image Search to achieve the same precision as that of using the advanced operators but without typing or remembering the operators
- Using Google's Advanced search option, attackers can find sites that may link back to the target organization's website

Gathering Information using Reverse Image Search

- Reverse image search helps an attacker in tracking the original source and details of images, such as photographs, profile pictures, and memes
- Attackers can use online tools such as Google Image Search, TinEye Reverse Image Search, and Yahoo Image Search to perform reverse image search

Gathering Information from Video Search Engines

- Video search engines such as YouTube, and Google Videos allow attackers to search for a video content related to the target
- Attackers can further analyze the video content to gather hidden information such as time/date and thumbnail of the video
- Using video analysis tools such as YouTube DataViewer, and EZGif, an attacker can reverse and convert video to text formats to extract critical information about the target

Other Techniques for Footprinting through Search Engines (Cont'd)

Gathering Information from Meta Search Engines

- Meta search engines use other search engines (Google, Bing, Ask.com, etc.) to produce their own results from the Internet
- Attackers use meta search engines such as Startpage and MetaGer to gather more detailed information about the target, such as images, videos, blogs, and news articles, from different sources

Gathering Information from FTP Search Engines

- FTP search engines are used to search for files located on the FTP servers
- Attackers use FTP search engines, such as NAPALM FTP Indexer and Global FTP Search Engine, to retrieve critical files and directories about the target that reveal valuable information, such as business strategy, tax documents, and employee's personal records

Gathering Information from IoT Search Engines

- IoT search engines crawl the Internet for IoT devices that are publicly accessible
- Attackers use IoT search engines, such as Shodan, Censys, and Thingful, to gather information about the target IoT devices, such as manufacturer details, geographical location, IP address, hostname, and open ports

Other Techniques for Footprinting through Search Engines

- **Gathering Information Using Google Advanced Search, Advanced Image Search, and Reverse Image Search**

  An attacker cannot always gather information easily from an information-rich site using only a normal search box. A complicated search involves a number of interrelated conditions.

Google's Advanced search feature helps an attacker to perform complex web searching. With **Google Advanced Search** and **Advanced Image Search**, one can search the web more precisely and accurately. You can use these search features to achieve the same precision as that achieved using the advanced operators but without typing or remembering the operators. Using Google's Advanced Search option, you can find sites that may link back to the target organization's website. This helps to extract information such as partners, vendors, clients, and other affiliations of the target website. You can use Google Advanced Image Search to acquire images of the target, its location, employees, and so on.

To perform an advanced search in Google, click **Settings** at the bottom-right of the **Google** home page, and then choose **Advanced search** in the menu or directly type ***https://www.google.com/advanced_search*** in the address bar. Advanced search allows you to specify any number of criteria that the search must match, as this pattern builds on the search box pattern by adding more search options. To do this, you choose a field. Then, enter the string you want to search for in the field's text box and click on the **Advanced Search** button. By default, various values are joined together with "and" (meaning all of them need to match) except for sets, blocks, and formats, which are joined together with "or" (meaning any of them can match).

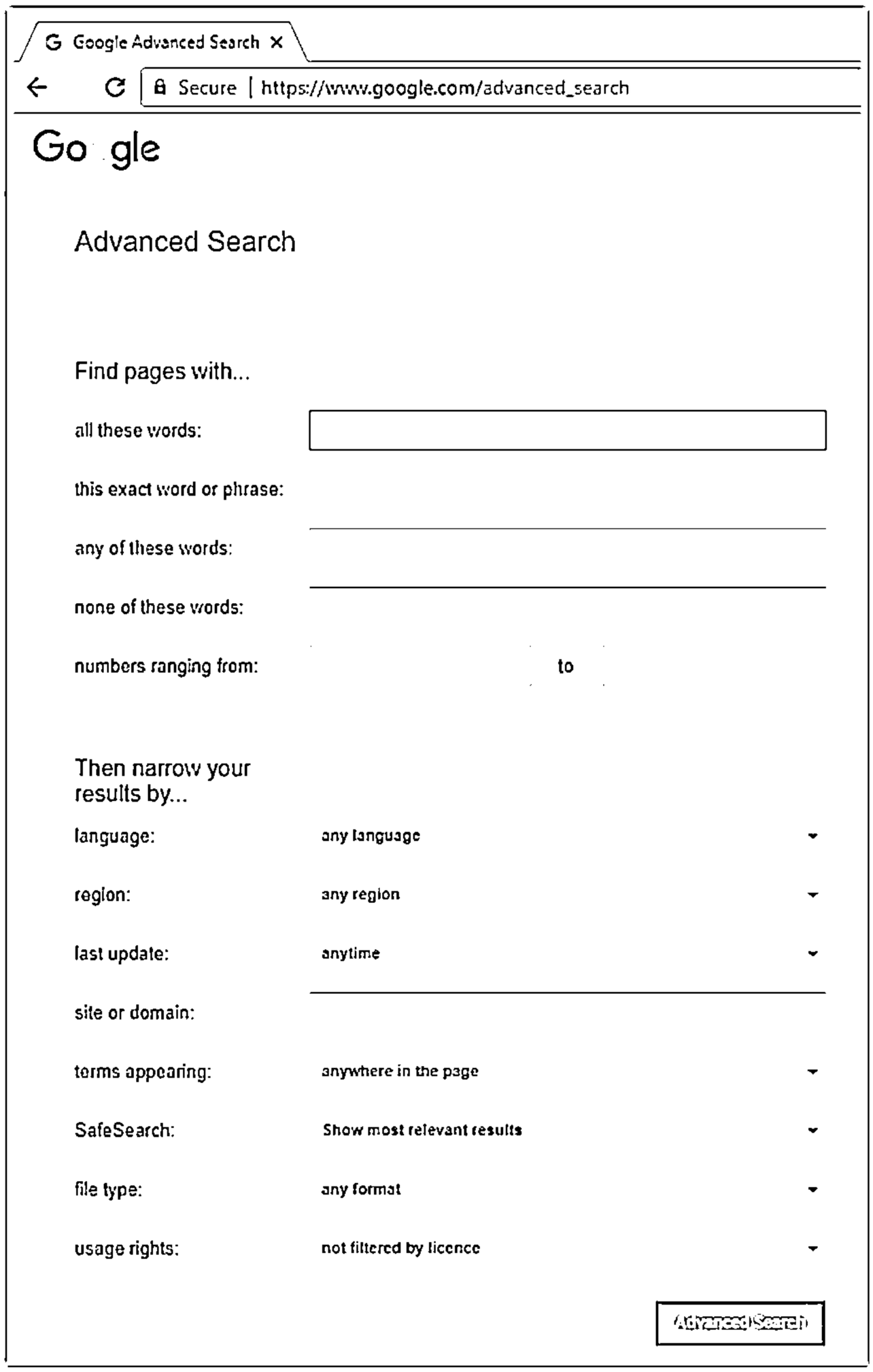


Figure 2.3: Google Advance Search

To perform an advanced image search in Google, type ***https://www.google.com/advanced_image_search*** in the address bar. Advanced image search allows you to tweak your image search in a number of ways. You can search based on image color, domain, file type, size, keyword, and so on. To do this, you choose a field. Then, enter the string you want to search for in the field's text box and click on the **Advanced Search** button.

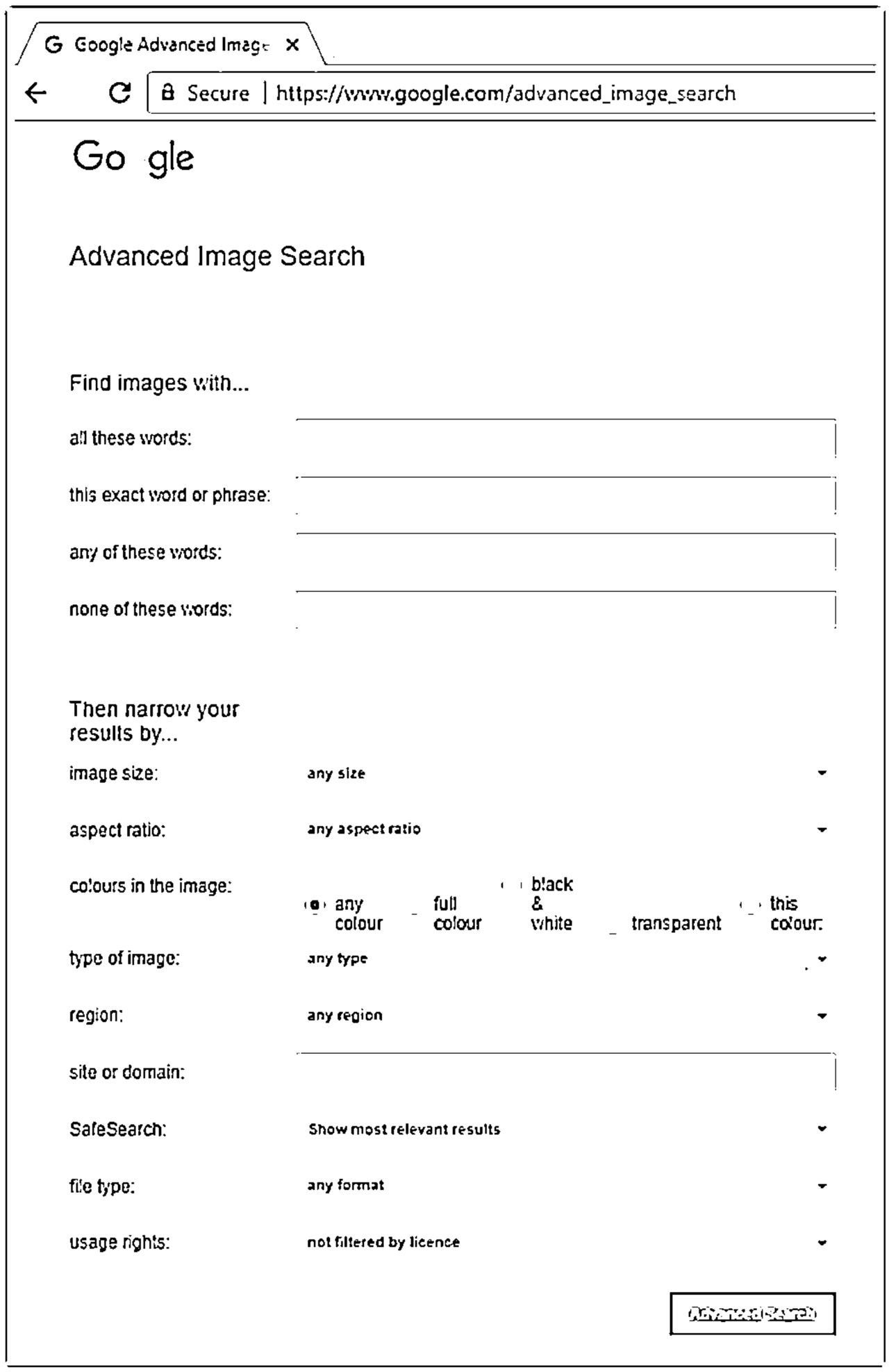


Figure 2.4: Google Advance Image Search

To perform a reverse image search in Google, type ***https://www.google.com/imghp*** in the address bar. Reverse image search allows you to use an image as a search query. You can upload an image or paste the URL of the image in the reverse image search engine. The search engine verifies the search engine index and displays all the online locations of the image in the search results page. The results obtained can help you in tracking the original source and details of the images, such as photographs, profile pictures, and memes.

Attackers use online tools such as Google Image Search, TinEye Reverse Image Search, Yahoo Image Search, and Bing Image Search to perform a reverse image search.

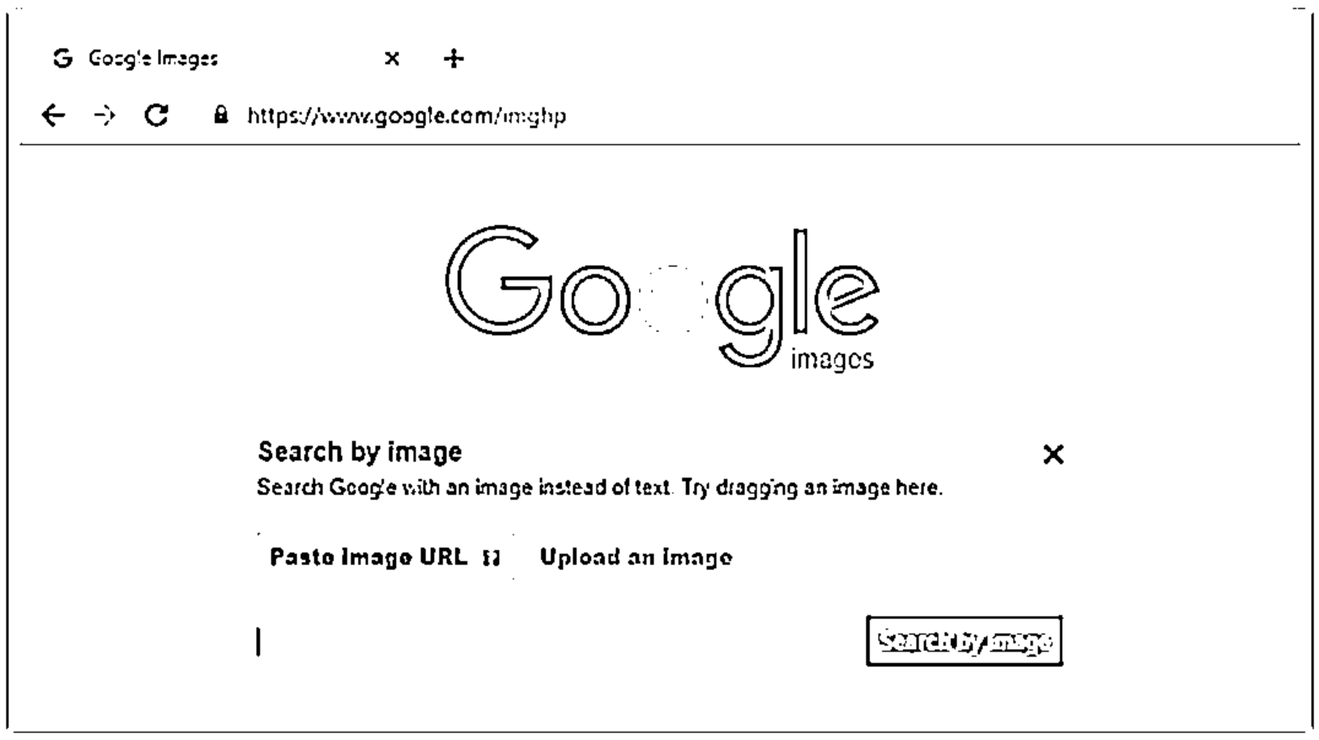


Figure 2.5: Reverse Image Search using Google

- **Gathering Information from Video Search Engines**

  Video search engines are Internet-based search engines that crawl the web for video content. These video search engines either provide the functionality of uploading and hosting video content on their own web servers or parse video content that is hosted externally. The video content obtained from video search engines is of high value, as it can be used for gathering information about the target. Video search engines such as YouTube, Google videos, Yahoo videos, and Bing videos allow attackers to search for video content based on the format type and duration.

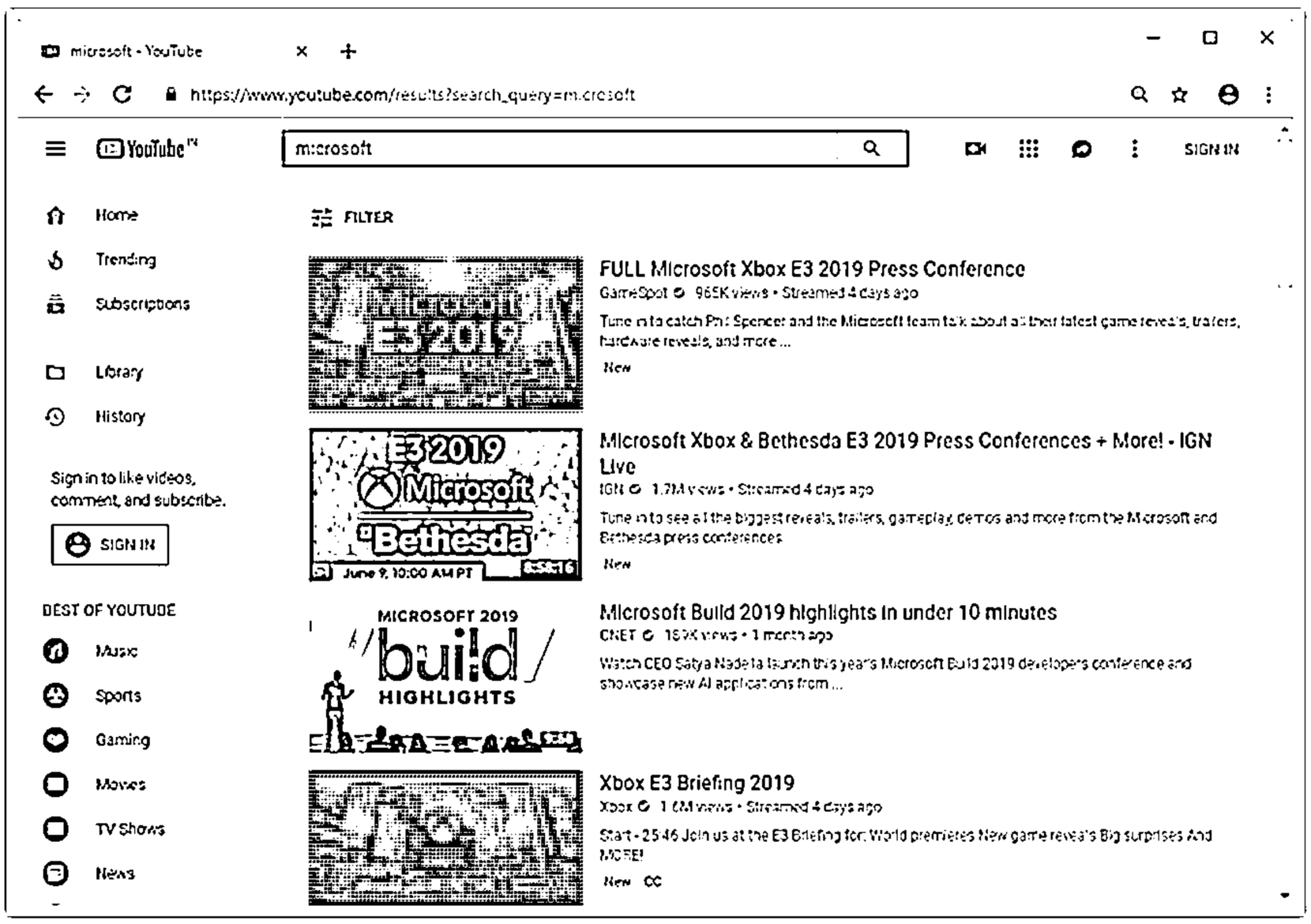


Figure 2.6: Screenshot of YouTube showing search results for Microsoft

After searching for videos related to the target using video search engines, an attacker can further analyze the video content to gather hidden information such as the time/date and thumbnail of the video. Using video analysis tools such as YouTube DataViewer, EZGif, and VideoReverser.com, an attacker can reverse a video or convert a video into text and other formats to extract critical information about the target.

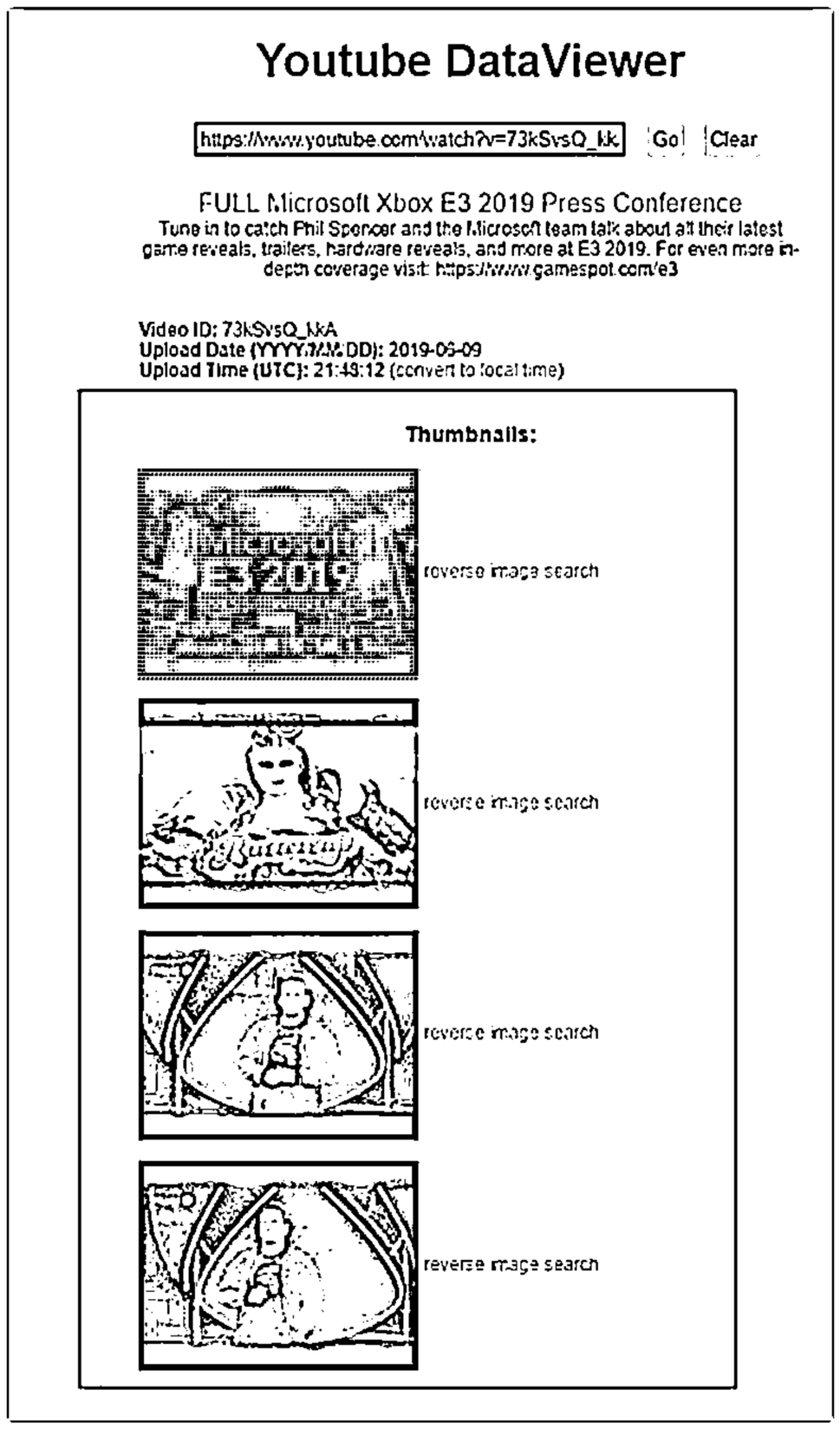


Figure 2.7: Screenshot of YouTube DataViewer showing video analysis result

- **Gathering Information from Meta Search Engines**

  Meta search engines are a different type of search engines that use other search engines (Google, Bing, Ask.com, etc.) to produce their own results from the Internet in a very short time span. These search engines do not have their own search indexes; instead, they take the inputs from the users and simultaneously send out the queries to the third-party search engines to obtain the results. Once sufficient results are gathered, they are ranked according to their relevance and presented to the user through the web interface. Meta search engines also include a functionality whereby identical search results are filtered out so that if the user searches the same query again, then it will not display the same

results twice. A meta search engine is advantageous compared to simple search engines, as it can retrieve more results with the same amount of effort.

Using meta search engines, such as Startpage, MetaGer, and eTools.ch, attackers can send multiple search queries to several search engines simultaneously and gather substantially detailed information such as information from shopping sites (Amazon, eBay, etc.), images, videos, blogs, news, and articles from different sources. Further, meta search engines also provide privacy to the search engine user by hiding the user's IP address.

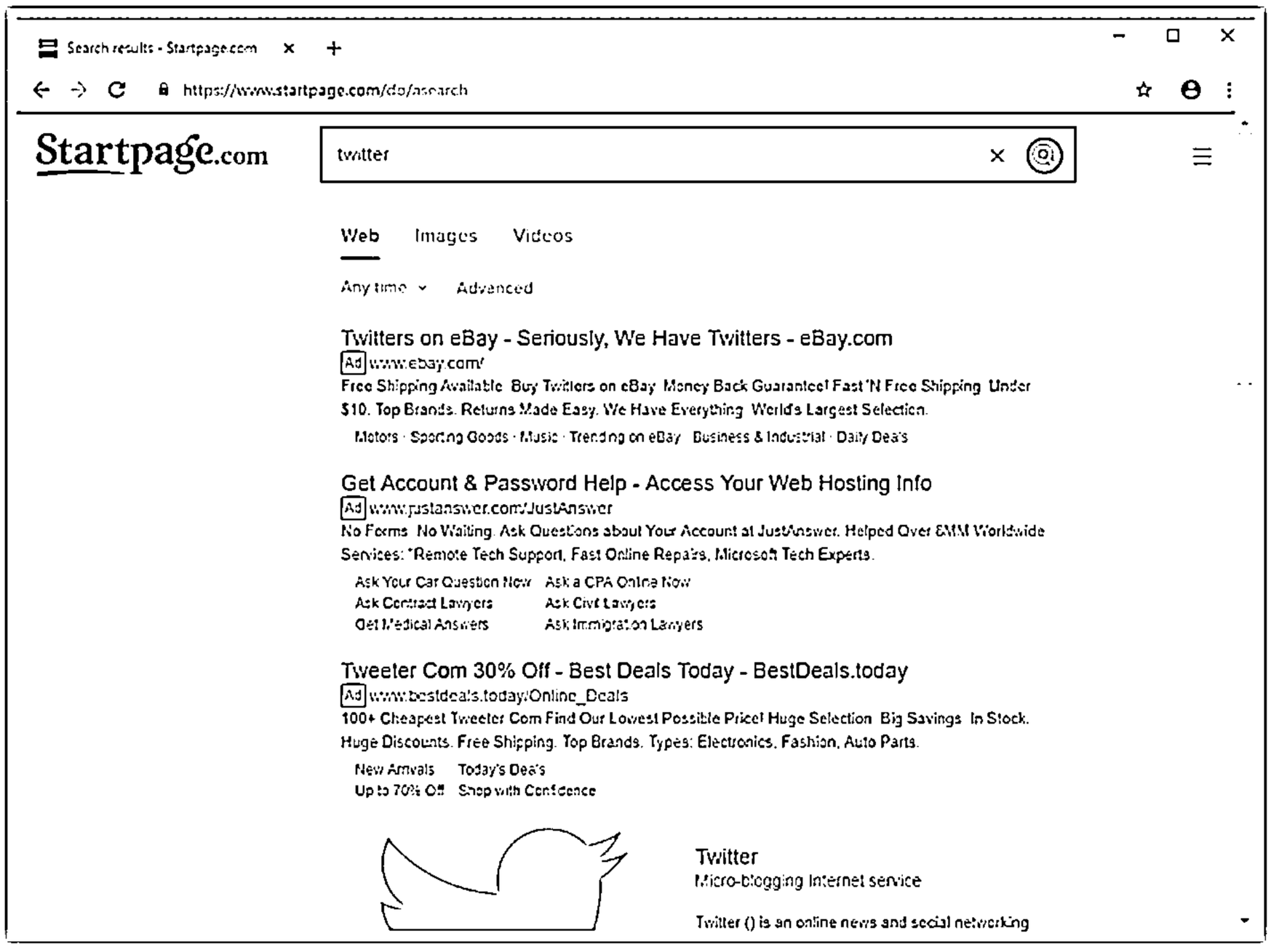


Figure 2.8: Screenshot of Meta Search Engine StartPage.com showing search results for Twitter

- **Gathering Information from FTP Search Engines**

  FTP search engines are used to search for files located on FTP servers that contain valuable information about the target organization. Many industries, institutions, companies, and universities use FTP servers to store large file archives and other software that are shared among their employees. A special client such as FileZilla (*https://filezilla-project.org*) can be used to access the FTP accounts; it also supports functionalities such as uploading, downloading, and renaming files. Although FTP servers are usually protected with passwords, many servers are left unsecured and can be accessed through web browsers directly.

  Using FTP search engines such as NAPALM FTP Indexer, Global FTP Search Engine, and FreewareWeb FTP File Search, attackers can search for critical files and directories

containing valuable information such as business strategies, tax documents, employee's personal records, financial records, licensed software, and other confidential information.

Listed below are some of the important advanced Google search queries to find FTP servers:

Google Dork	Description
inurl:github.com intext:.ftpconfig -issues	Returns SFTP/FTP server credentials on Github
type:mil inurl:ftp ext:pdf | ps	Returns sensitive directories on FTP
intext:pure-ftpd.conf intitle:index of	Returns servers exposing pure-ftpd configuration files
intitle:"Index Of" intext:sftp-config.json	Extracts list of FTP/SFTP passwords from sublime text
inurl:"ftp://www." "Index of /"	Displays various online FTP servers
inurl:~/ftp://193 filetype:(php | txt | html | asp | xml | cnf | sh) ~'/html'	Returns a list of FTP servers by IP address, mostly Windows NT servers with guest login capabilities

Table 2.3: Google search queries to find FTP servers

As shown in the screenshot, attackers can use the NAPALM FTP Indexer online tool to search for critical files and documents related to the target domain.

Figure 2.9: Screenshot of FTP Search Engine NAPALM FTP Indexer showing search results for Microsoft

- **Gathering Information from IoT Search Engines**

  Internet of Things (IoT) search engines crawl the Internet for IoT devices that are publicly accessible. Through a basic search on these search engines, an attacker can gain control of Supervisory Control and Data Acquisition (SCADA) systems, traffic control systems, Internet-connected household appliances, industrial appliances, CCTV cameras, etc. Many of these IoT devices are unsecured, i.e., they are without passwords or they use the default credentials, which can be exploited easily by attackers.

  With the help of IoT search engines such as Shodan, Censys, and Thingful, attackers can obtain information such as the manufacturer details, geographical location, IP address, hostname, and open ports of the target IoT device. Using this information, the attacker can establish a back door to the IoT devices and gain access to them to launch further attacks.

  As shown in the screenshot, attackers can use Shodan to find all the IoT devices of the target organization that are having open ports and services.

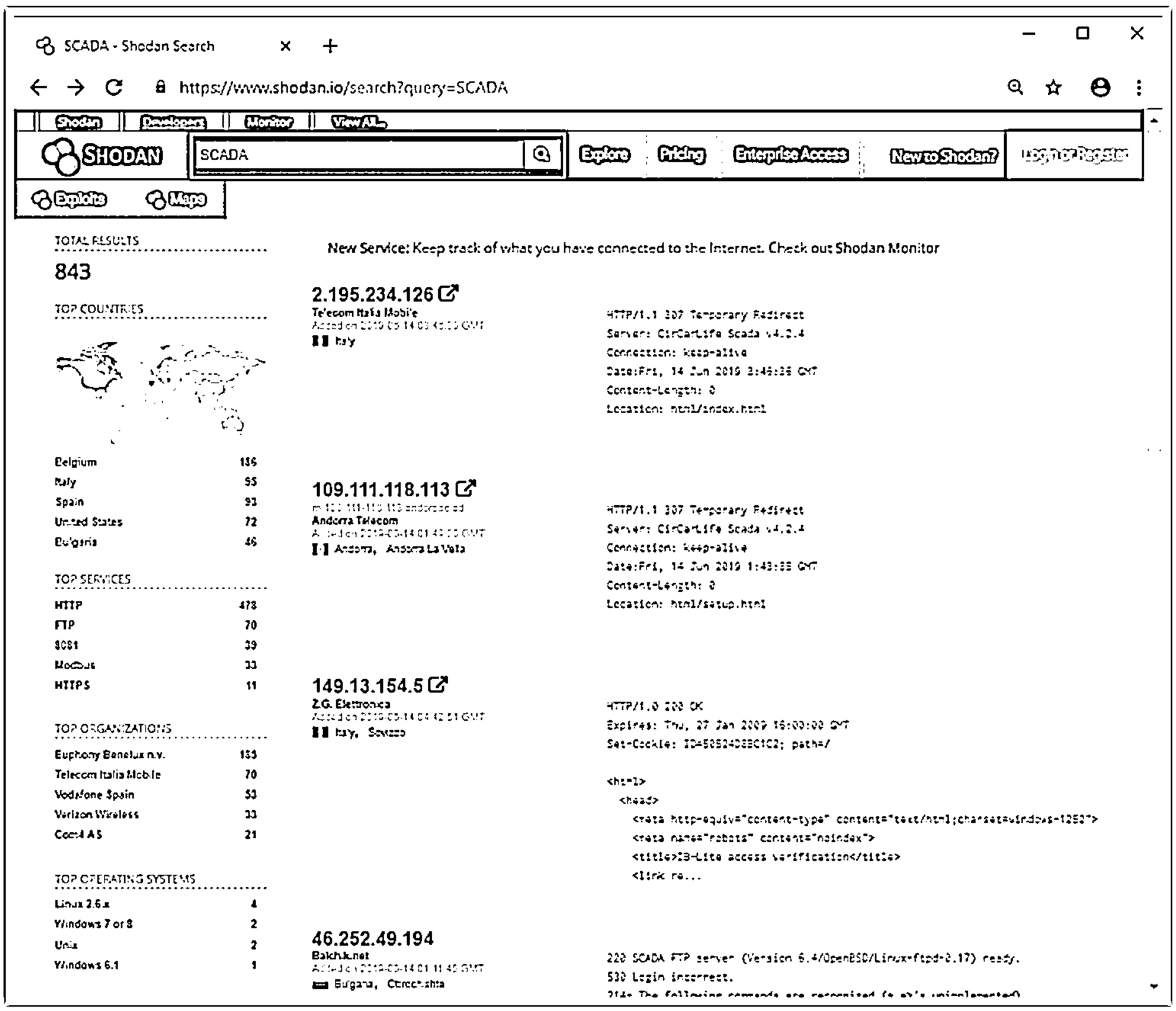


Figure 2.10: Screenshot of Shodan showing search results for SCADA devices

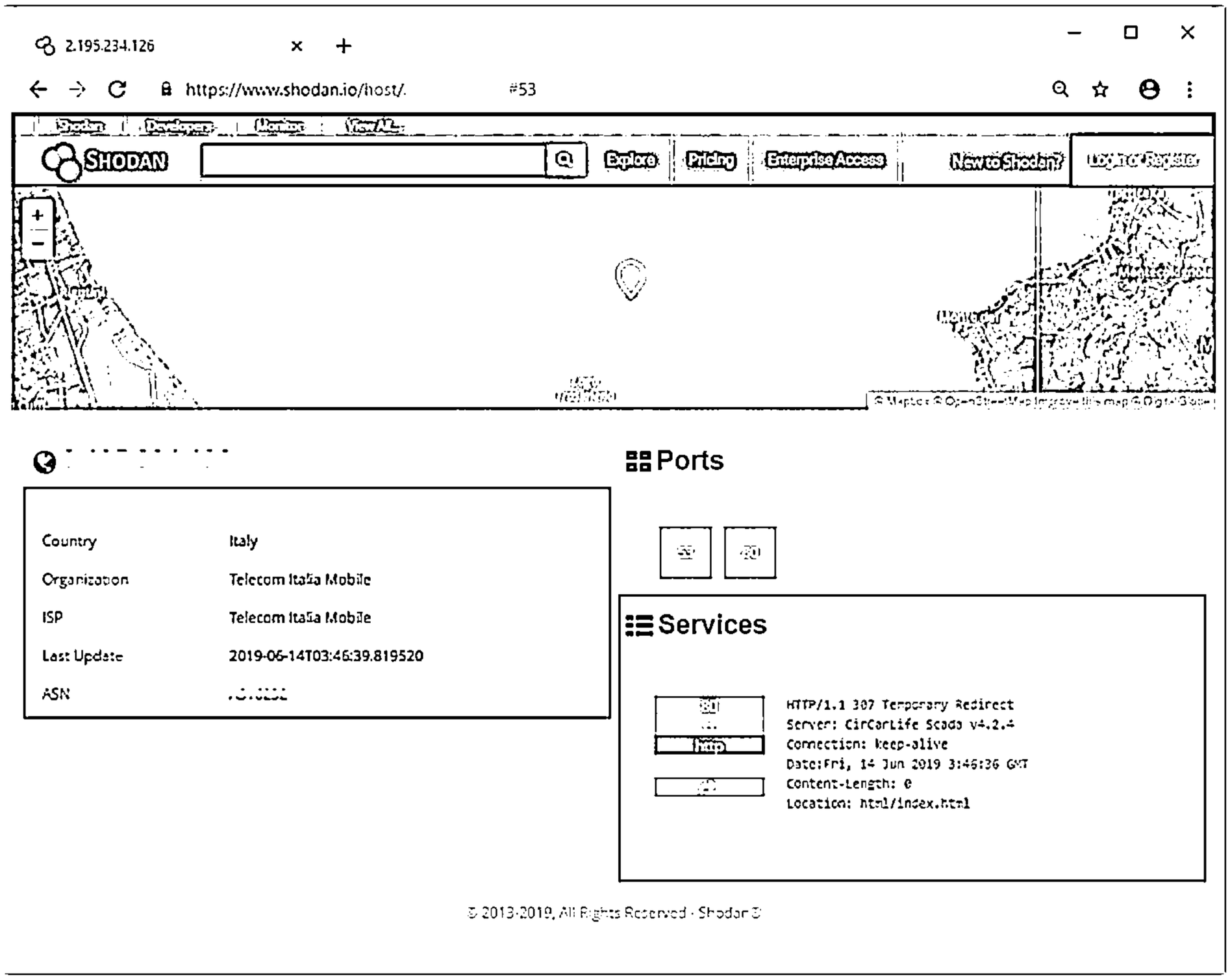
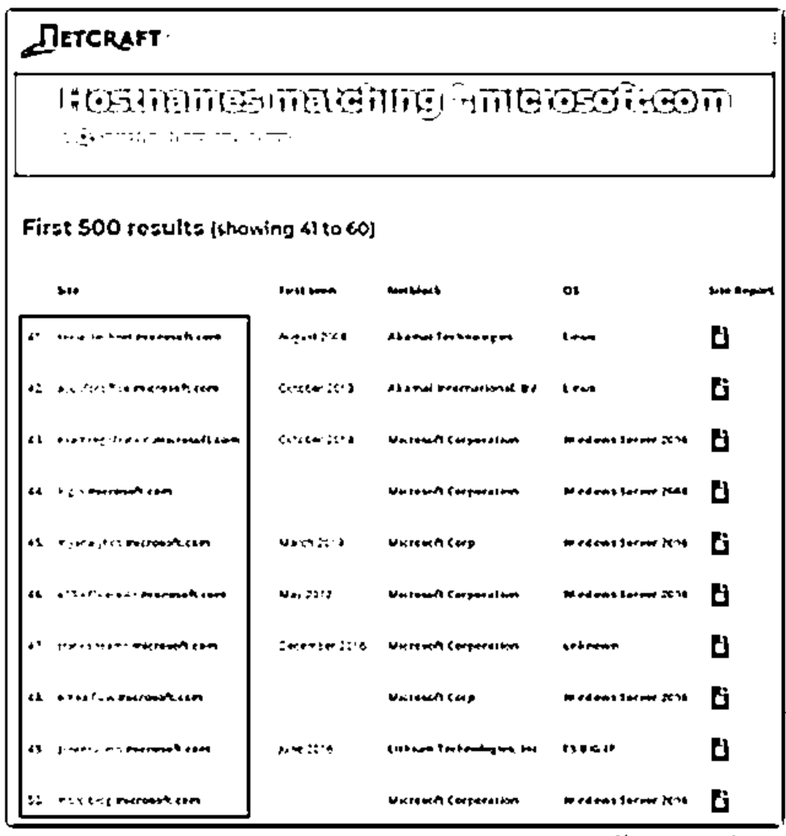


Figure 2.11: Screenshot of Shodan showing open ports and services of a SCADA system

Finding a Company's Top-Level Domains (TLDs) and Sub-domains

- Search for the target company's external URL in a search engine, such as Google and Bing
- Sub-domains provide an insight into different departments and business units in an organization
- You may find a company's sub-domains by trial and error method or using a service such as *https://www.netcraft.com*
- You can use the Sublist3r python script, which enumerates subdomains across multiple sources at once



https://www.netcraft.com

https://github.com

Footprinting through Web Services

Web services such as people search services can provide sensitive information about the target. Internet archives may also provide sensitive information that has been removed from the World Wide Web (WWW). Social networking sites, people search services, alerting services, financial services, and job sites provide information about a target such as infrastructure details, physical location, and employee details. Moreover, groups, forums, and blogs can help attackers in gathering sensitive information about a target, such as public network information, system information, and personal information. Using this information, an attacker may build a hacking strategy to break into the target organization's network and carry out other types of advanced system attacks.

This section aims to familiarize you with finding the target company's top-level domains, sub-domains, and geographical location, performing people search on social networking sites and people search services, gathering information from job sites, financial services, third-party data repositories, performing deep and dark web footprinting, determining the operating system, VOIP and VPN footprinting through Shodan, gathering competitive intelligence, etc.

Finding a Company's Top-Level Domains (TLDs) and Sub-domains

A company's top-level domains (TLDs) and sub-domains can provide a large amount of useful information to an attacker. A public website is designed to show the presence of an organization on the Internet. It is available for free public access. It is designed to attract customers and partners. It may contain information such as organizational history, services and products, and contact information. The target organization's external URL can be located with the help of search engines such as Google and Bing.

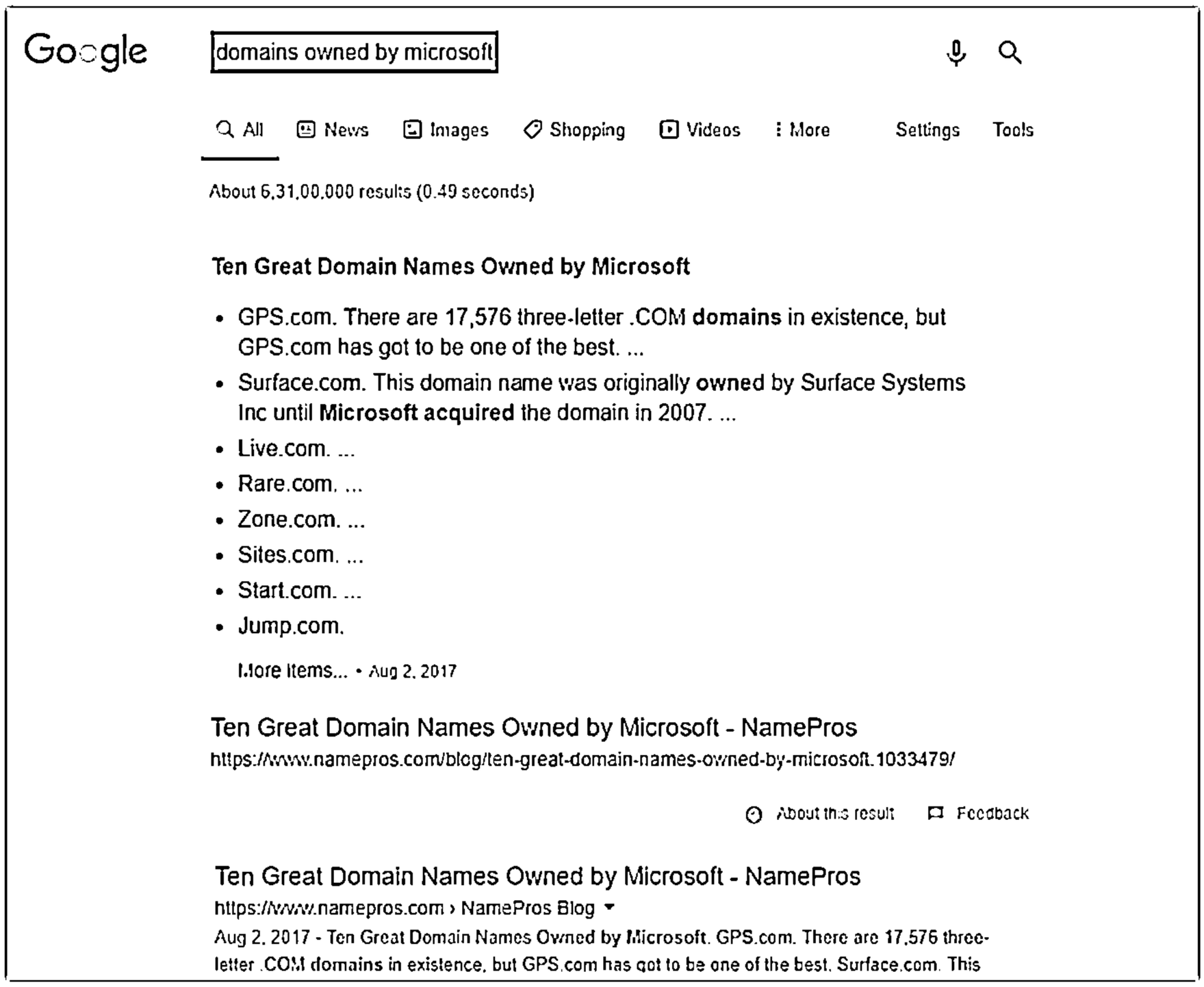


Figure 2.12: Google search engine showing results for given syntax

The sub-domain is available to only a few people. These persons may be employees of an organization or members of a department. In many organizations, website administrators create sub-domains to test new technologies before deploying them on the main website. Generally, these sub-domains are in the testing stage and are insecure; hence, they are more vulnerable to various exploitations. Sub-domains provide insights into the different departments and business units in an organization. Identifying such sub-domains may reveal critical information regarding the target, such as the source code of the website and documents on the webserver. Access restrictions can be applied based on the IP address, domain or subnet, username, and password. The sub-domain helps to access the private functions of an organization. Most organizations use common formats for sub-domains. Therefore, a hacker who knows the external URL of a company can often discover the sub-domain through trial and error, or by using a service such as Netcraft.

You can also use the advanced Google search operator shown below to identify all the sub-domains of the target:

```
site:microsoft.com -inurl:www
```

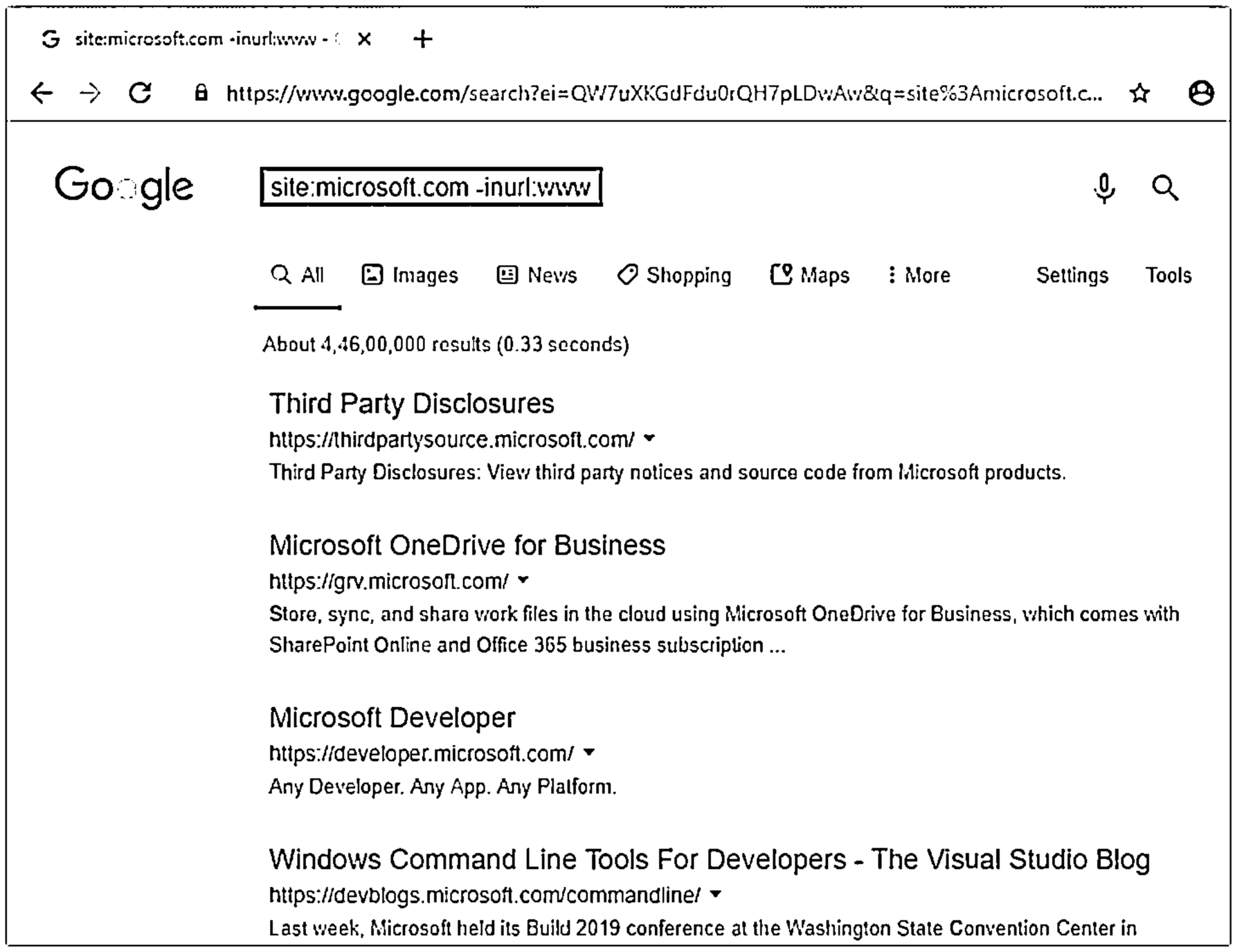


Figure 2.13: Finding sub-domains using Google Advanced Search Operator

Tools to Search Company's Sub-domains

- **Netcraft**

  Source: *https://www.netcraft.com*

  Netcraft provides Internet security services, including anti-fraud and anti-phishing services, application testing, and PCI scanning. They also analyze the market share of web servers, operating systems, hosting providers and SSL certificate authorities, and other parameters of the Internet.

  As shown in the screenshot below, attackers can use Netcraft to obtain all the sub-domains related to the target domain.

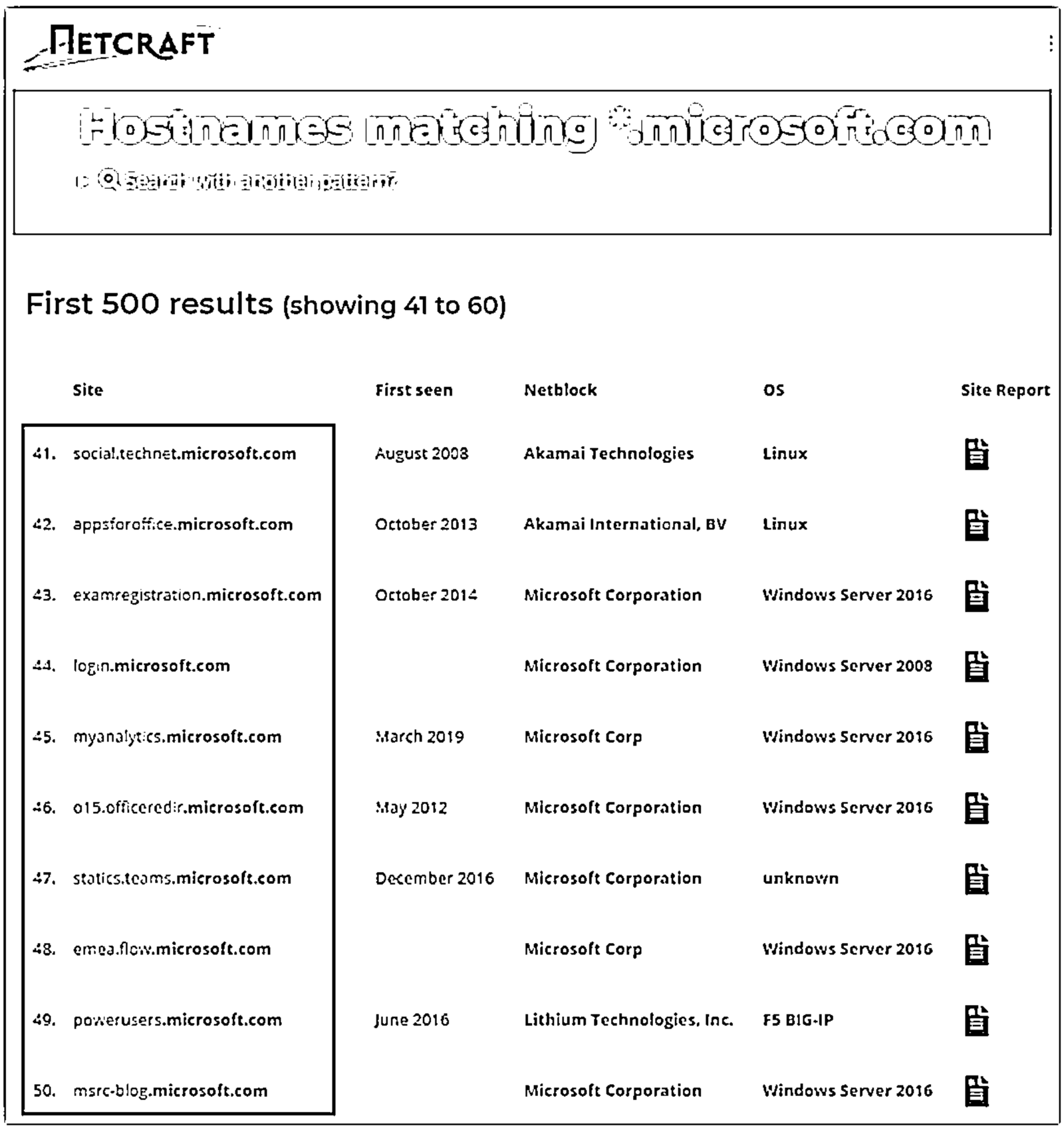


Figure 2.14: Screenshot of Netcraft displaying sub-domains of microsoft.com

- **Sublist3r**

  Source: *https://github.com*

  Sublist3r is a Python script designed to enumerate the subdomains of websites using OSINT. It enables you to enumerate subdomains across multiple sources at once. Further, it helps penetration testers and bug hunters in collecting and gathering subdomains for the domain they are targeting. It enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask. It also enumerates subdomains using Netcraft, VirusTotal, ThreatCrowd, DNSdumpster, and ReverseDNS.

  Syntax:

  ```
  sublist3r [-d DOMAIN] [-b BRUTEFORCE] [-p PORTS] [-v VERBOSE][-t
  THREADS] [-e ENGINES] [-o OUTPUT]
  ```

Short Form	Long Form	Description
-d	--domain	Domain name to enumerate subdomains of
-b	--bruteforce	Enable the subbrute bruteforce module
-p	--ports	Scan the found subdomains against specific TCP ports
-v	--verbose	Enable the verbose mode and display results in real time
-t	--threads	Number of threads to use for subbrute bruteforce
-e	--engines	Specify a comma-separated list of search engines
-o	--output	Save the results to a text file
-h	--help	Show the help message and exit

Table 2.4: Sublist3r options with description

Examples 1:

As shown in the screenshot, Sublist3r helps attackers in enumerating the subdomains of a target company from multiple sources at the same time.

Figure 2.15: Screenshot of Sublist3r displaying sub-domains of google.com

Examples 2:

Sublist3r also helps attackers in enumerating the subdomains of a target company with a specific port open.

As shown in the screenshot, attackers search for subdomains of google.com (-d google.com) using the Bing search engine (-e Bing) with port 80 (-p 80) open.

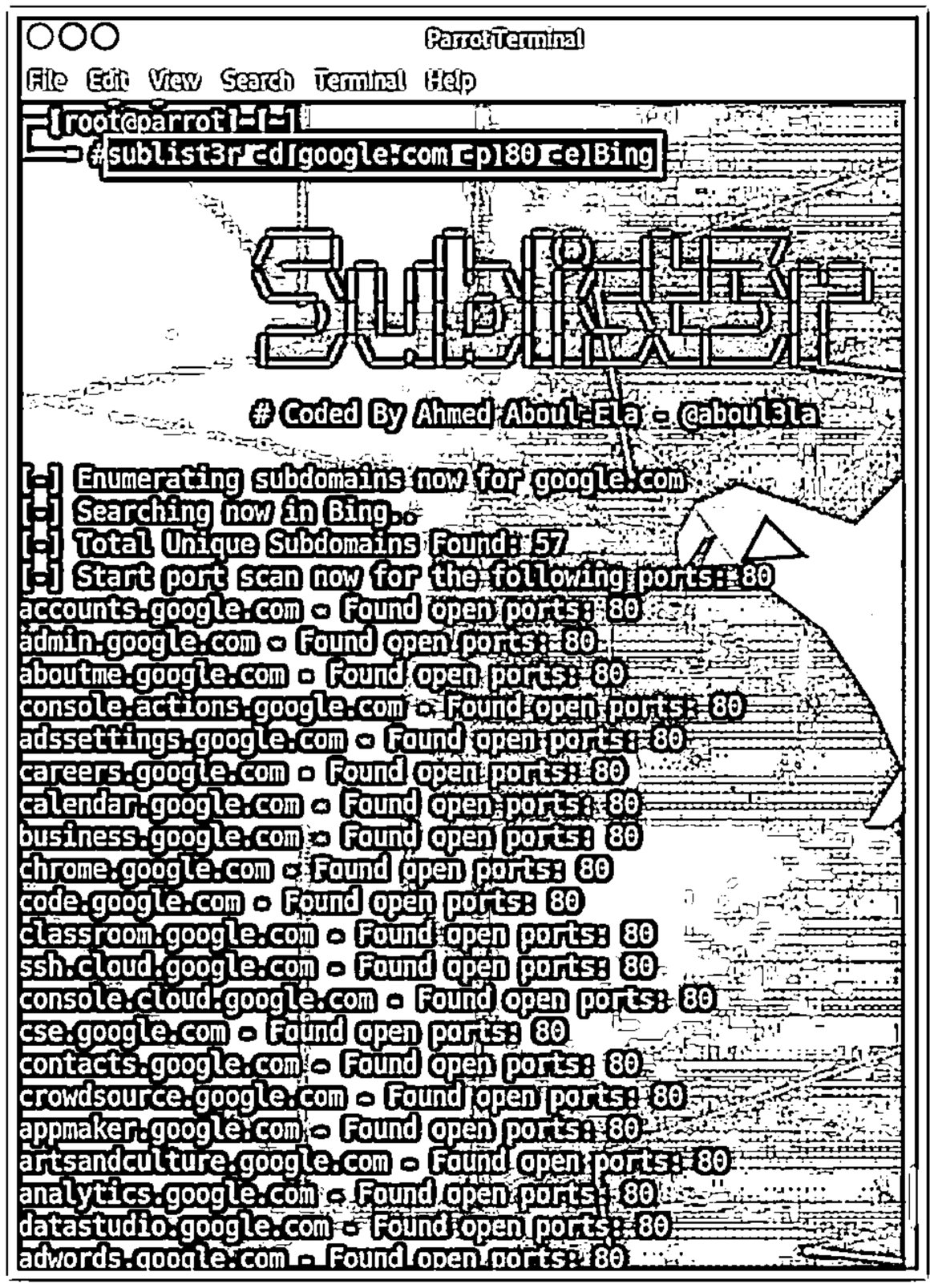


Figure 2.16: Screenshot of Sublist3r displaying sub-domains of google.com with port 80 open

- **Pentest-Tools Find Subdomains**

  Source: *https://pentest-tools.com*

  Pentest-Tools Find Subdomains is an online tool used for discovering subdomains and their IP addresses, including network information and their HTTP servers.

  As shown in the screenshot, attackers search for sub-domains related to microsoft.com to obtain critical information about the target company domain, such as sub-domains, IP addresses, operating systems, servers used, technology used, web platform, and page titles.

Pentest-Tools.com

✓ microsoft.com

DOWNLOAD REPORT

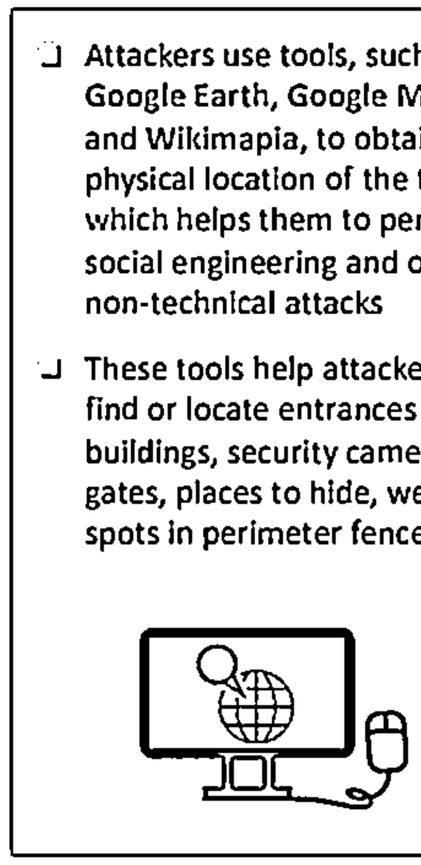
Found 117 subdomains

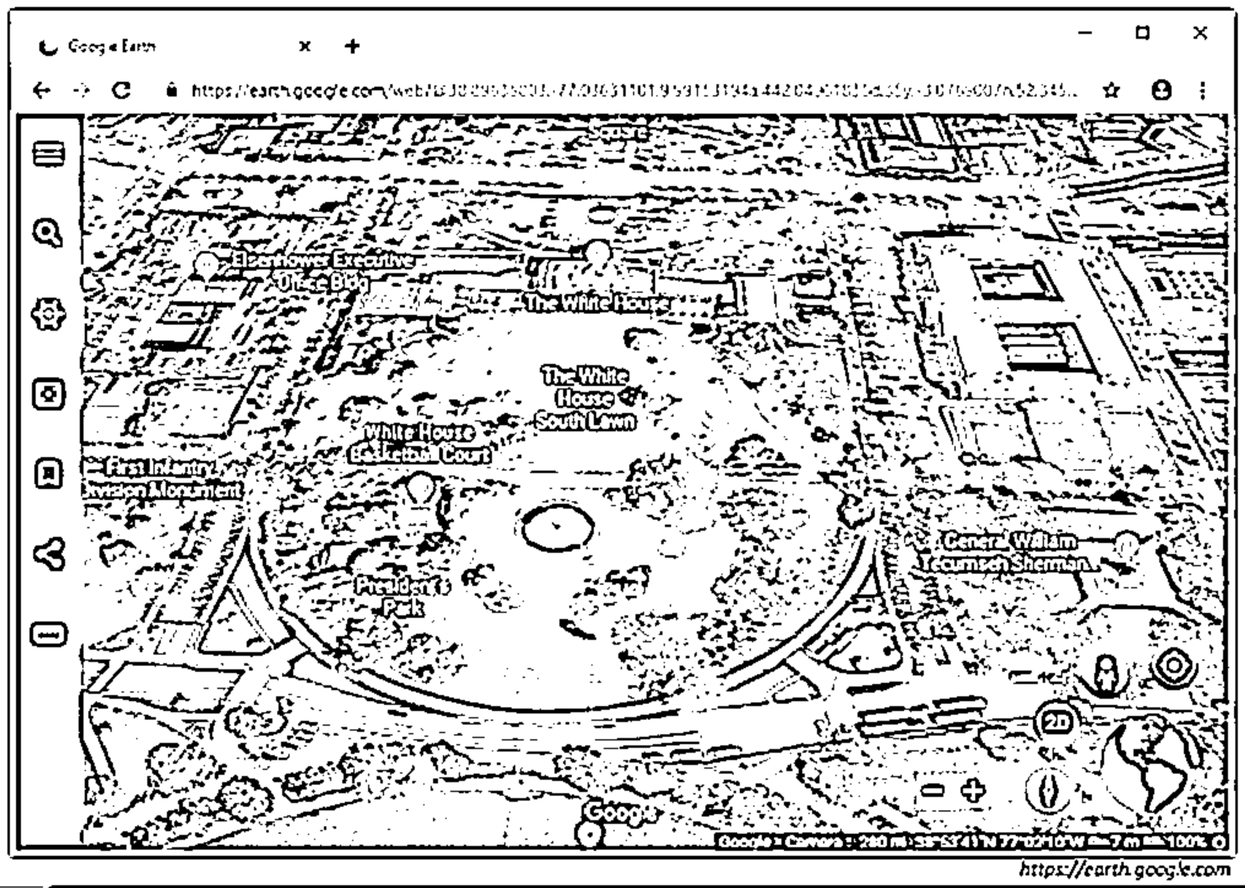
Subdomain	IP address	OS	Server	Technology	Web Platform	Page Title
download.microsoft.com	2.19.60.35	Windows	Microsoft-IIS	ASP.NET		Microsoft Download Center: Windows, Office, Xbox & More
support.microsoft.com	2.19.61.76					
docs.microsoft.com	2.20.37.130					Technical documentation, API, and code examples | Microsoft Docs
codecs.microsoft.com	2.22.146.89		AkamaiGHost			Access Denied
rto.microsoft.com	13.66.244.249	Windows	Microsoft-IIS 10.0	ASP.NET		Your Azure Function App is up and running.
me.microsoft.com	13.68.197.138	Windows	Microsoft-IIS 10.0	ASP.NET 4.0.30319		Home Page - My ASP.NET Application
linux.microsoft.com	13.77.154.182		Apache 2.4.6			Microsoft: Linux Systems Group
online.microsoft.com	13.77.161.179					We are sorry, the page you requested cannot be found
profile.microsoft.com	13.77.200.139	Windows	Microsoft-IIS 10.0	ASP.NET		IIS Windows Server
input.microsoft.com	13.95.64.138					
portal.microsoft.com	13.107.6.156					Sign In to your account

Figure 2.17: Screenshot of Pentest-Tools displaying sub-domains of microsoft.com

Finding the Geographical Location of the Target

- Attackers use tools, such as Google Earth, Google Maps, and Wikimapia, to obtain the physical location of the target, which helps them to perform social engineering and other non-technical attacks
- These tools help attackers to find or locate entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, etc.





Finding the Geographical Location of the Target

Information such as the physical location of an organization plays a vital role in the hacking process. Attackers can obtain this information using footprinting. In addition to the physical location, a hacker can also acquire information such as surrounding public Wi-Fi hotspots that may offer a way to break into the target organization's network.

Attackers with the knowledge of a target organization's location may attempt dumpster diving, surveillance, social engineering, and other non-technical attacks to gather more information. Once the attackers discern the location of the target, they can obtain detailed satellite images of the location using various sources available on the Internet such as Google Earth and Google Maps. The attackers can use this information to gain unauthorized access to buildings, wired and wireless networks, and systems.

Tools for Finding the Geographical Location

The tools for finding the geographical location allow you to find and explore most locations on the earth. They provide information such as images of buildings, as well as their surroundings, including Wi-Fi networks. Tools such as Google Maps even locate entrances of the building, security cameras, and gates. These tools provide interactive maps, outline maps, satellite imagery, and information on how to interact with and create one's own maps. Google Maps, Yahoo Maps, and other tools provide driving directions, traffic conditions, landmarks, and detailed address and contact information.

Attackers may use tools such as Google Earth, Google Maps, and Wikimapia, to find or locate entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, and utility resources such as electricity connections, to measure the distance between different objects, and so on.

- **Google Earth** (*https://earth.google.com*)

  Attackers use the Google Earth tool to find the exact location of a target. Using this tool, attackers can even access 3D images that depict most of the populated Earth's surface with a high resolution. The detail allows attackers to obtain street views, altitude information, and even coordinates.

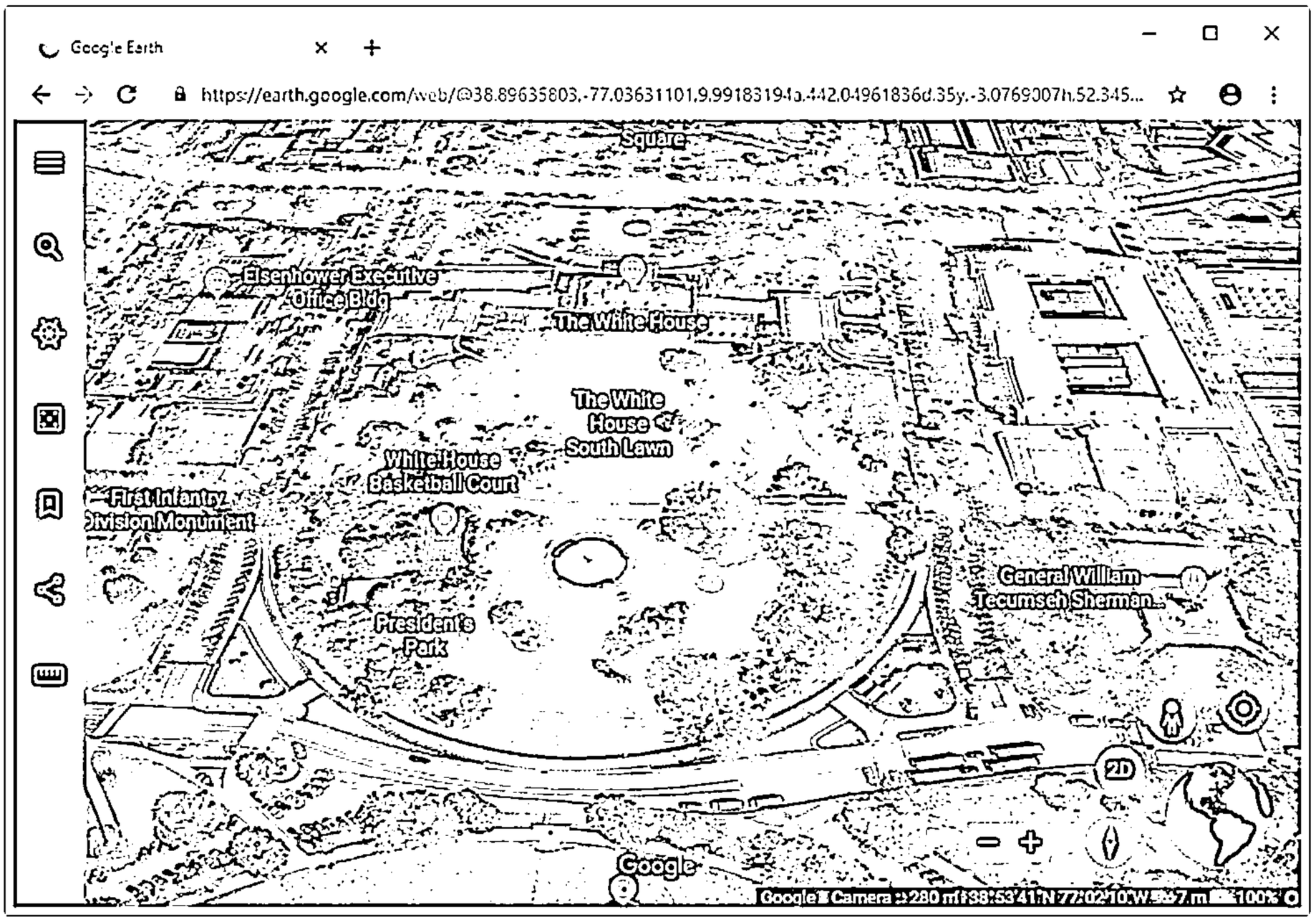
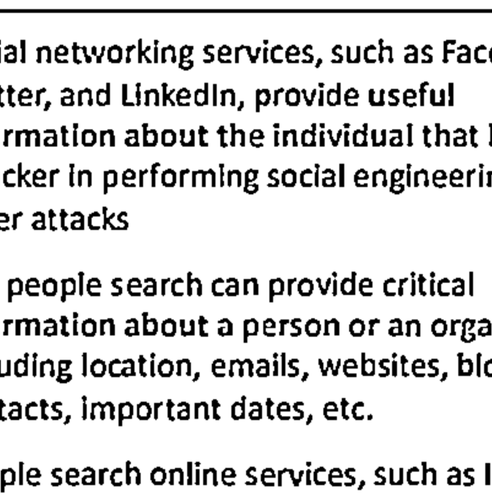
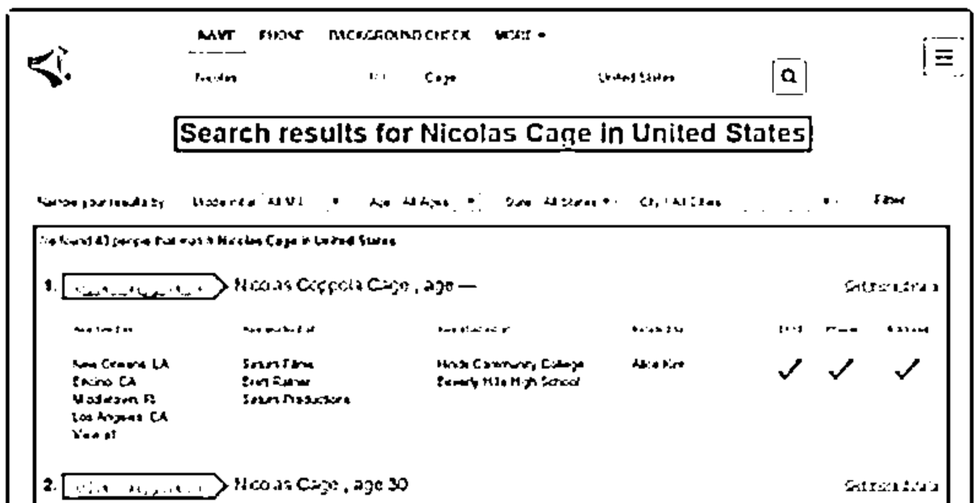


Figure 2.18: Screenshot of Google Earth

People Search on Social Networking Sites and People Search Services

- Social networking services, such as Facebook, Twitter, and LinkedIn, provide useful information about the individual that helps the attacker in performing social engineering and other attacks
- The people search can provide critical information about a person or an organization, including location, emails, websites, blogs, contacts, important dates, etc.
- People search online services, such as Intelius, pipl, BeenVerified, Whitepages, and PeekYou, provide people's names, addresses, contact details, date of birth, photographs, videos, profession, and so on





People Search on Social Networking Sites

Searching for a particular person on a social networking website is fairly easy. Social networking services are online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people. These websites contain information that users provide in their profiles. They help to directly or indirectly relate people to each other through various fields such as common interests, work location, and education.

Social networking sites allow people to share information quickly, as they can update their personal details in real time. Such sites allow users to update facts about upcoming or current events, recent announcements and invitations, and so on. Social networking sites are a great platform for finding people and their related information. Many social networking sites allow visitors to search for people without registering on the site; this makes people searching on social networking sites an easy and anonymous task. A user can search for a person using the name, email, or address. Some sites allow users to check whether an account is active, which then provides information on the status of the person being searched.

Social networking sites such as Facebook, Twitter, LinkedIn, and Instagram allow you to find people by name, keyword, company, school, friends, colleagues, and the people living around them. Searching for people on these sites returns personal information such as name, position, organization name, current location, and educational qualifications. In addition, you can also find professional information such as company or business, current location, phone number, email ID, photos, videos and so on. Social networking sites such as Twitter are used to share advice, news, concerns, opinions, rumors, and facts. Through people searching on social networking services, an attacker can gather critical information that will help them in performing social engineering or other kinds of attacks.

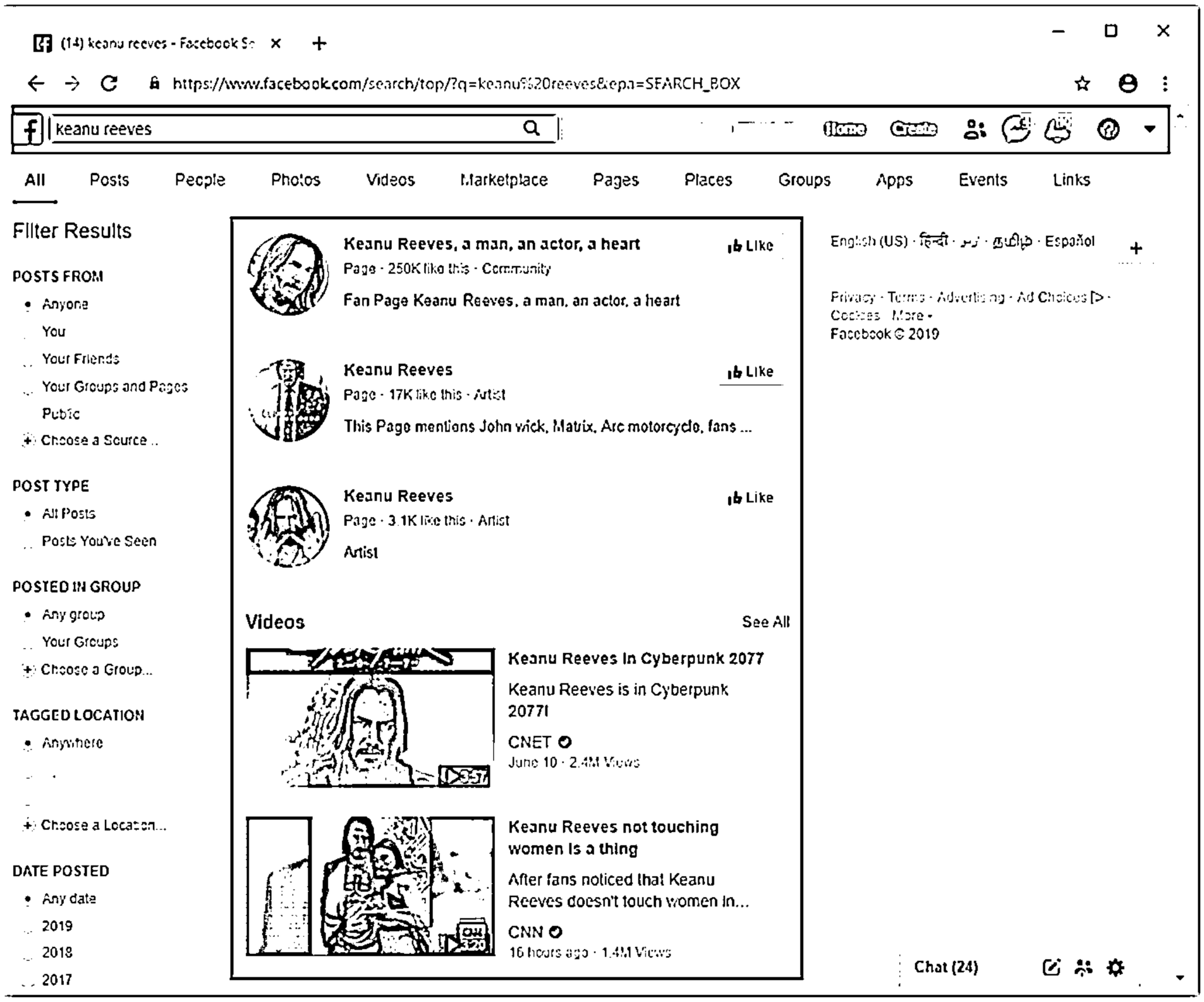


Figure 2.19: Screenshot of Facebook showing search results

People Search on People Search Services

You can use public record websites to find information about email addresses, phone numbers, house addresses, and other information. Many individuals use online people search services to find information about other people. Generally, online people search services such as pipl, Intelius, BeenVerified, Whitepages, and PeekYou provide people's names, addresses, contact details, date of birth, photographs, videos, profession, details about their family and friends, social networking profiles, property information, and optional background on criminal checks. Further, online people search services may often reveal the profession of an individual, businesses owned by a person, upcoming projects and operating environment, websites and blogs, contact numbers, important dates, company email addresses, cell phone numbers, fax numbers, and personal e-mail addresses. Using this information, an attacker can try to obtain bank details, credit card details, past history, and so on. This information proves to be highly beneficial for attackers to launch attacks. There are many available online people search services that help in obtaining information regarding people. Examples of such people search services include Intelius, pipl, and AnyWho.

- **People search service - Intelius**

  Source: *https://www.intelius.com*

  Attackers can use the Intelius people search online service to search for people belonging to the target organization. Using this service, attackers obtain information such as phone numbers, address history, age, date of birth, relatives, previous work history, educational background, and so on.

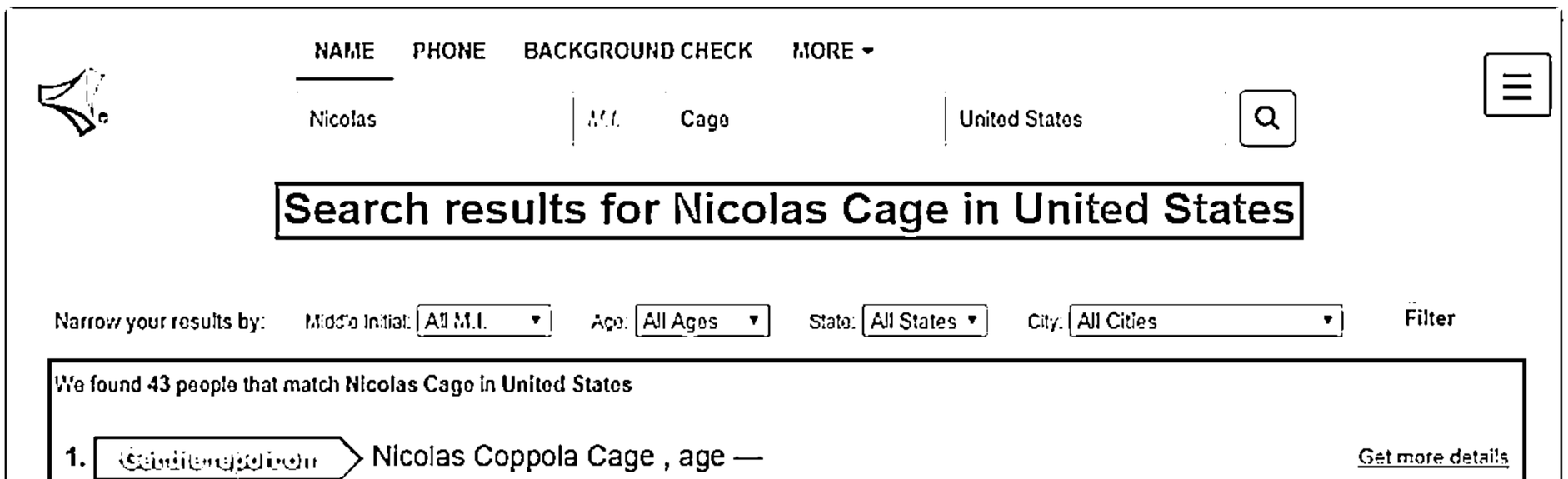
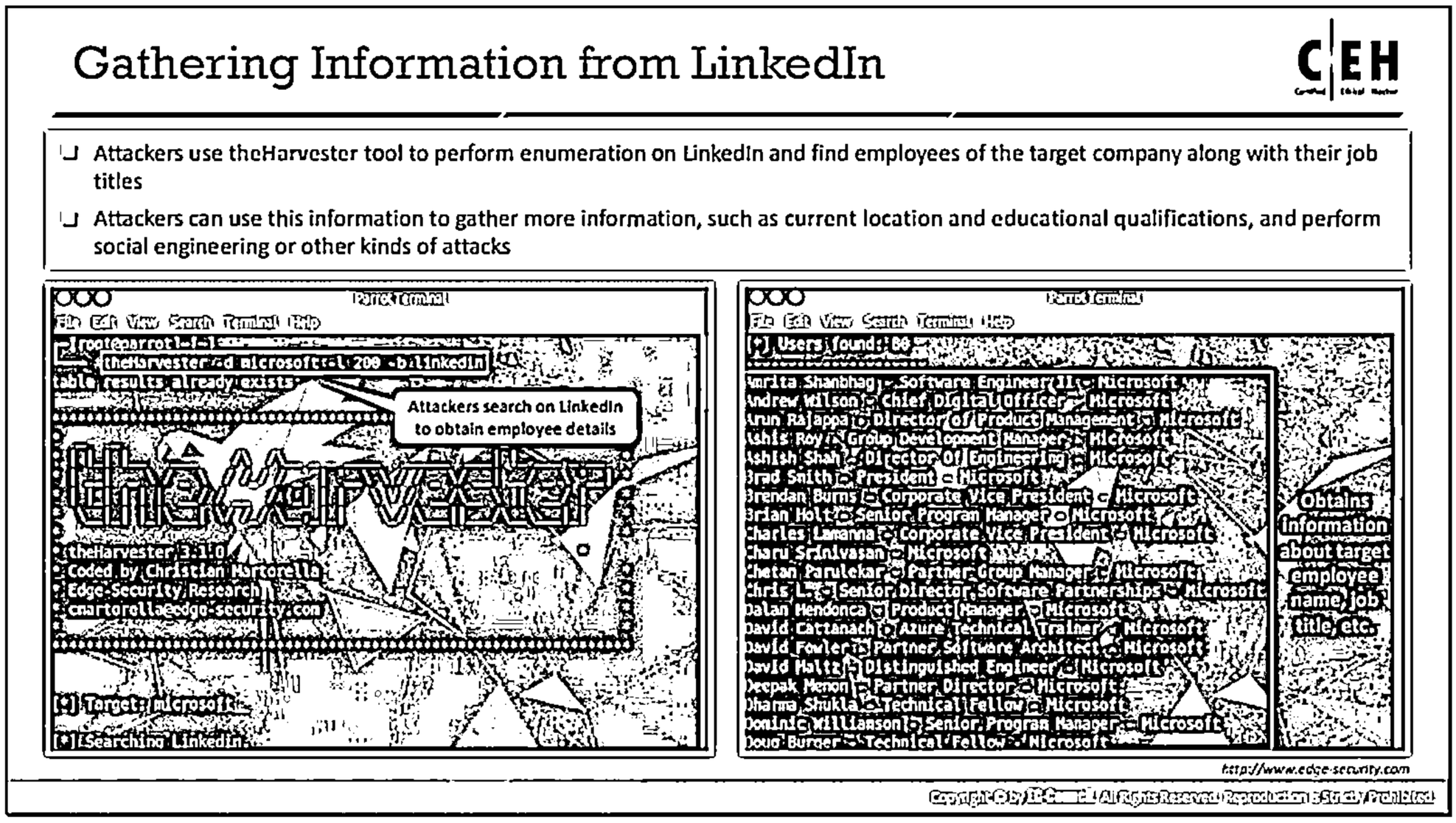


Figure 2.20: Screenshot of Intelius People Search



Gathering Information from LinkedIn

LinkedIn is a social networking website for professionals. It connects the world's human resources to aid productivity and success. The site contains personal information such as name, position, organization name, current location, educational qualifications, and so on. Information gathered from LinkedIn helps an attacker in performing social engineering or other kinds of attacks.

Attackers can use theHarvester tool to gather information from LinkedIn based on the target organization name:

- **theHarvester**

  Source: *http://www.edge-security.com*

  theHarvester is a tool designed to be used in the early stages of a penetration test. It is used for open-source intelligence gathering and helps to determine a company's external threat landscape on the Internet. Attackers use this tool to perform enumeration on the LinkedIn social networking site to find employees of the target company along with their job titles.

  As shown in the screenshot, the attacker uses the following command to enumerate users on LinkedIn:

  ```
  theHarvester -d microsoft -l 200 -b linkedin
  ```

  In the above command, -d specifies the domain or company name to search, -l specifies the number of results to be retrieved, and -b specifies the data source as LinkedIn.

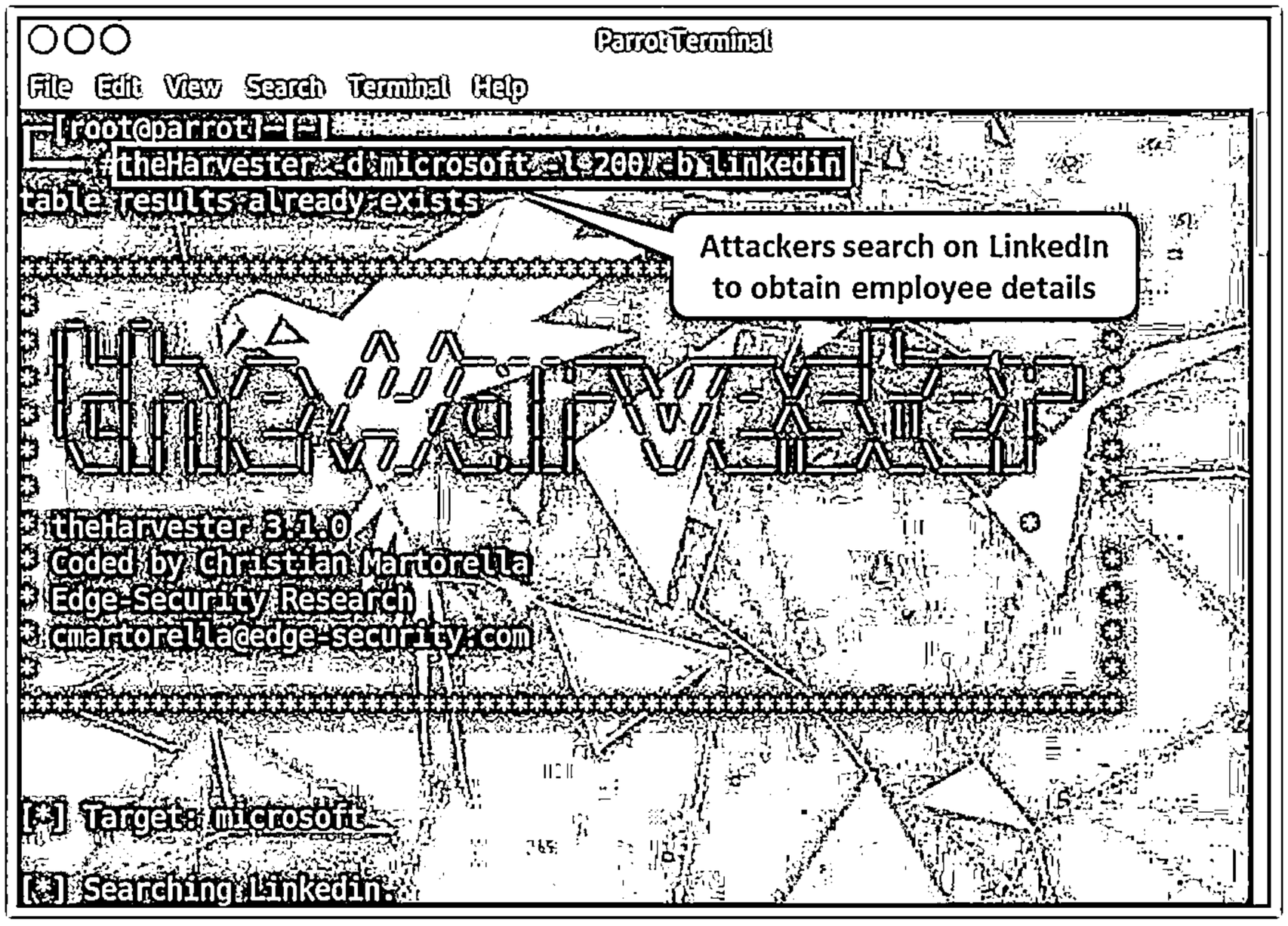


Figure 2.21: Screenshot showing theHarvester command to enumerate users on LinkedIn

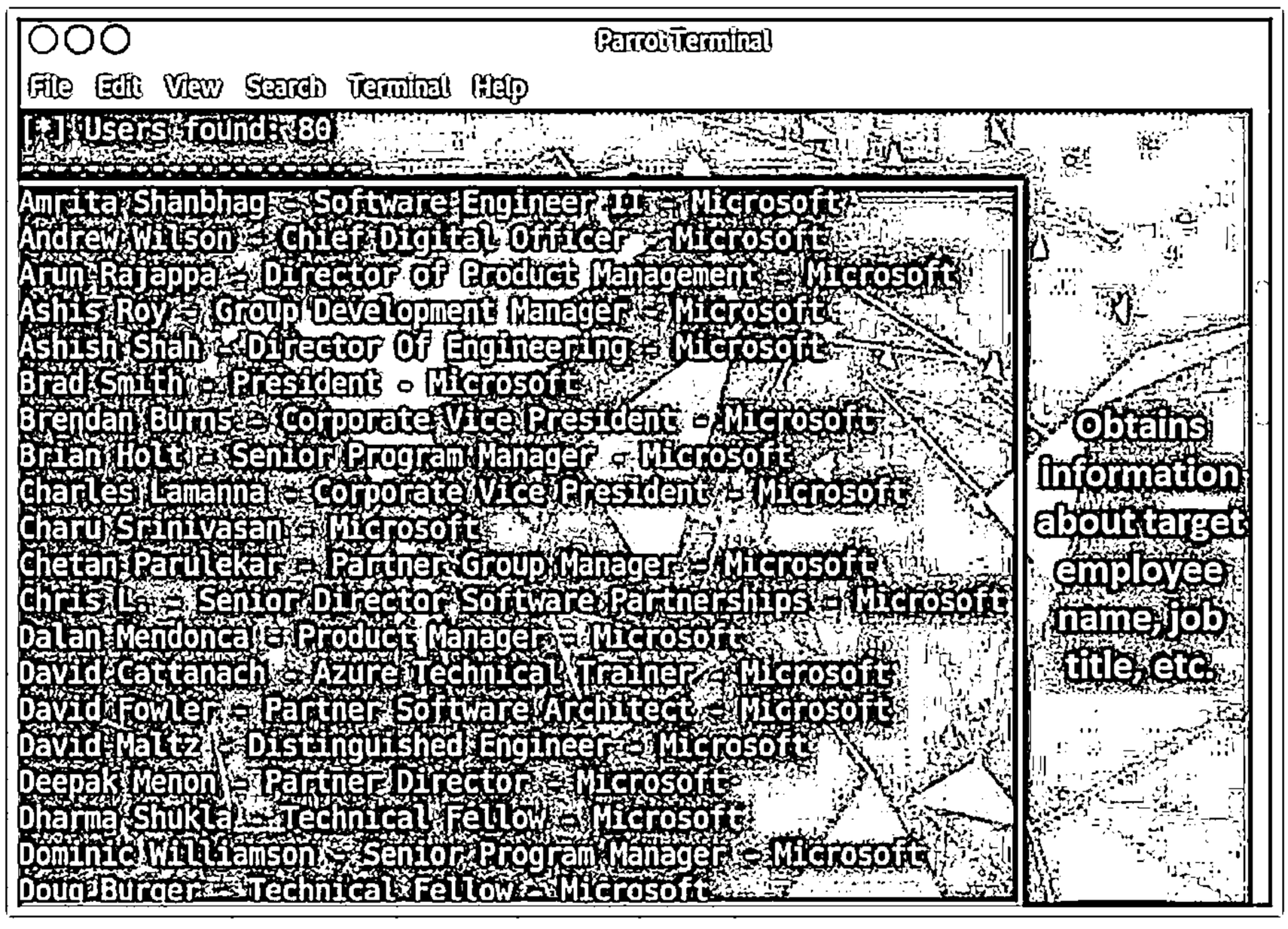
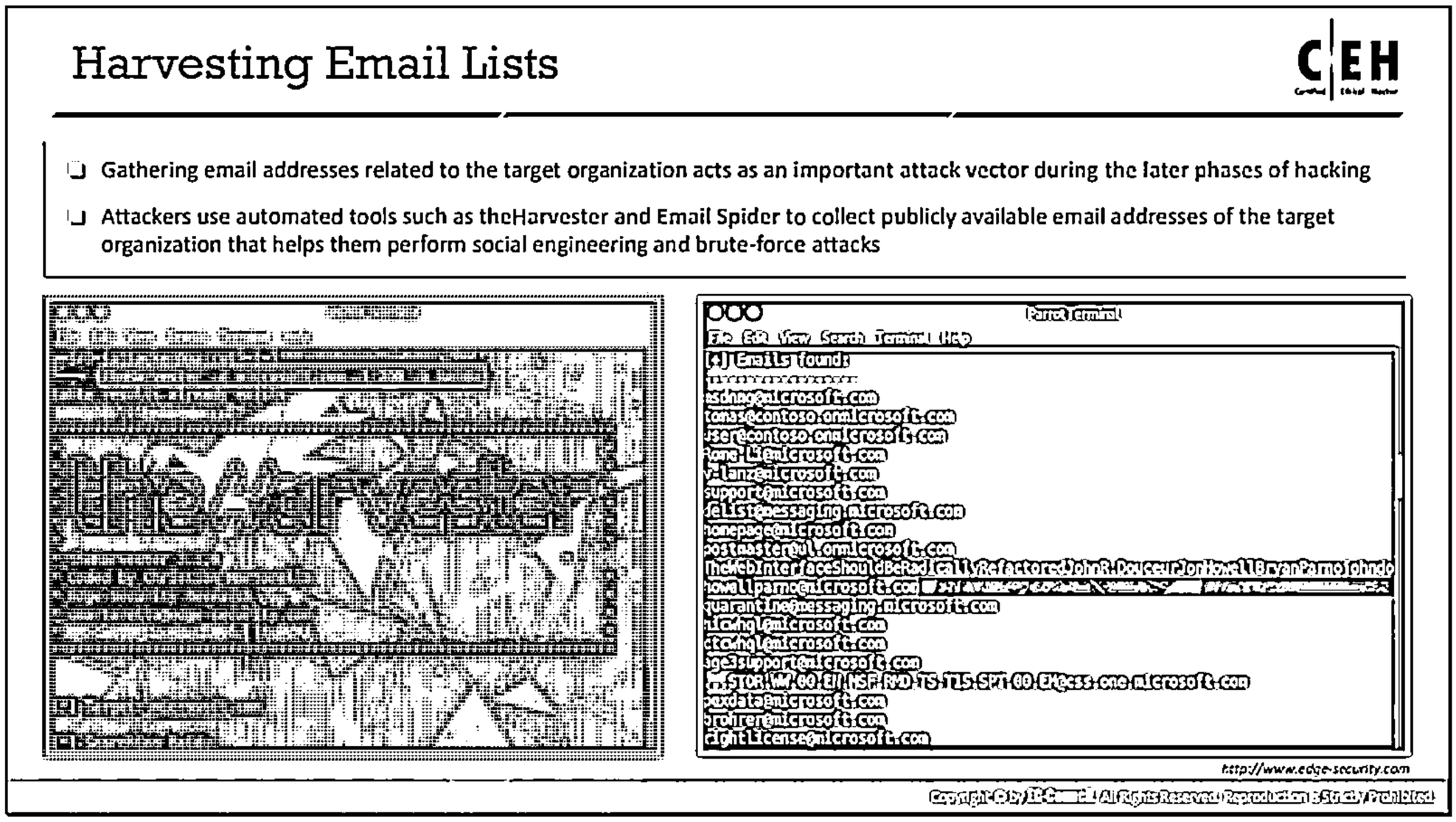


Figure 2.22: Screenshot showing theHarvester search results from LinkedIn



Harvesting Email Lists

Gathering email addresses related to the target organization acts as an important attack vector during the later phases of hacking. Attackers can use automated tools such as theHarvester and Email Spider to collect publicly available email addresses of the employees of the target organization. These tools harvest email lists related to a specified domain using search engines such as Google, Bing, and Baidu. Attackers use these email lists and usernames to perform social engineering and brute force attacks on the target organization.

- **theHarvester**

  Source: *http://www.edge-security.com*

  Attackers use theHarvester tool to extract email addresses related to the target domain. For example, attackers use the following command to extract email addresses of microsoft.com using the Baidu search engine:

  ```
  theharvester -d microsoft.com -l 200 -b baidu
  ```

  In the above command, -d specifies the domain used for harvesting the emails, -l will limit the results to 200, and -b tells theHarvester to extract the results from the Baidu search engine; alternatively, you can use Google, Bing, etc.

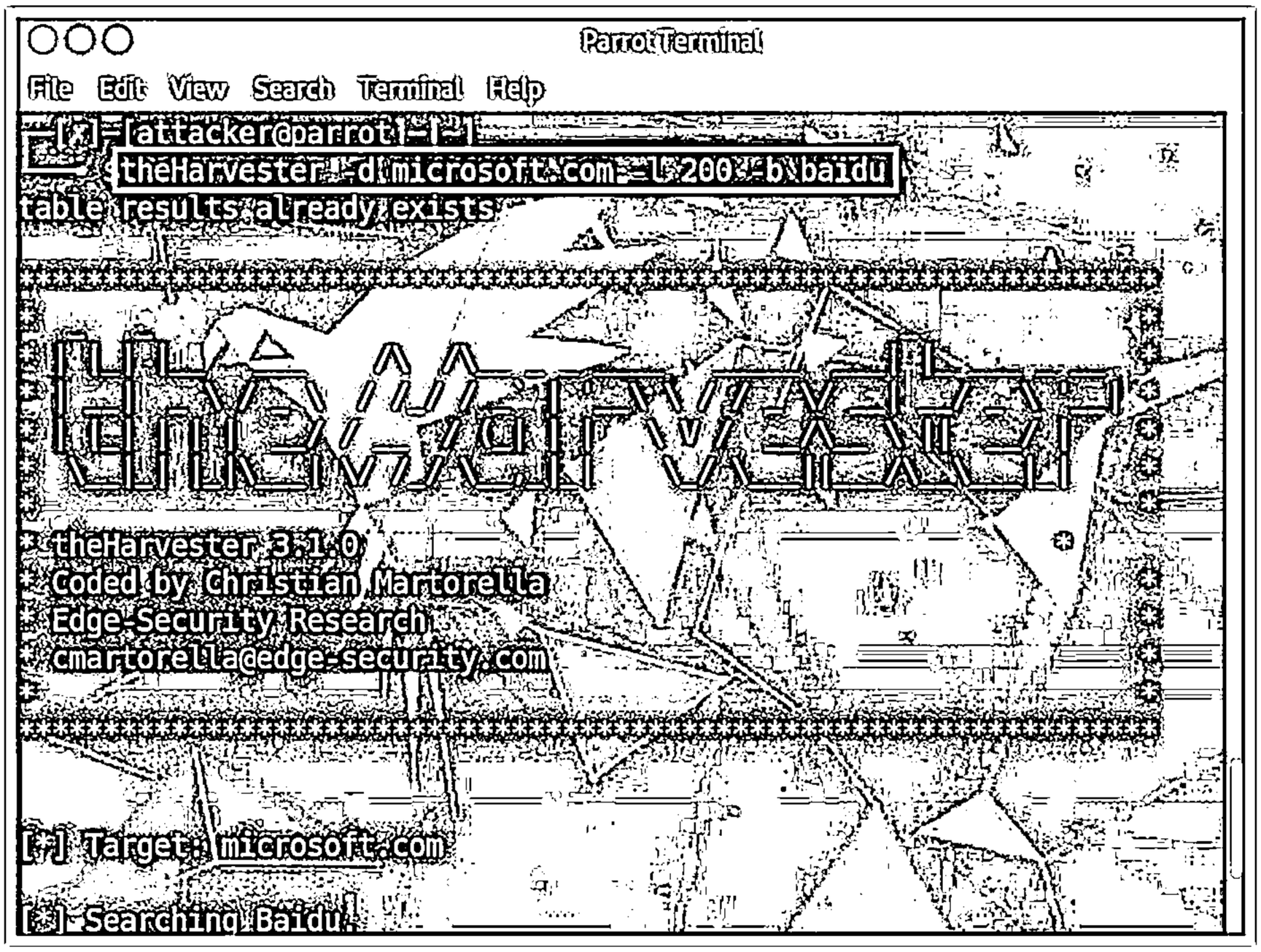


Figure 2.23: Screenshot showing theHarvester command to extract email addresses

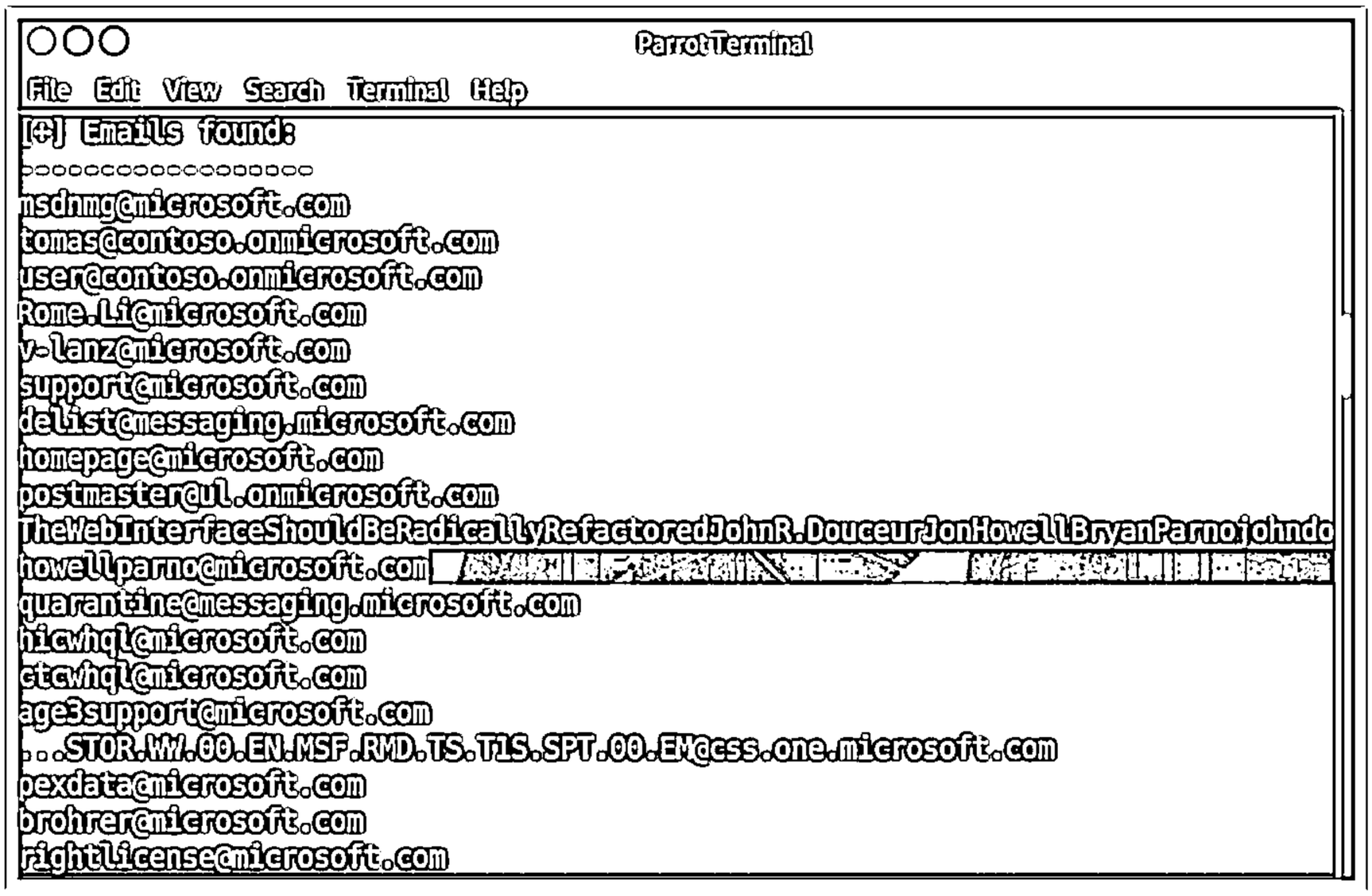
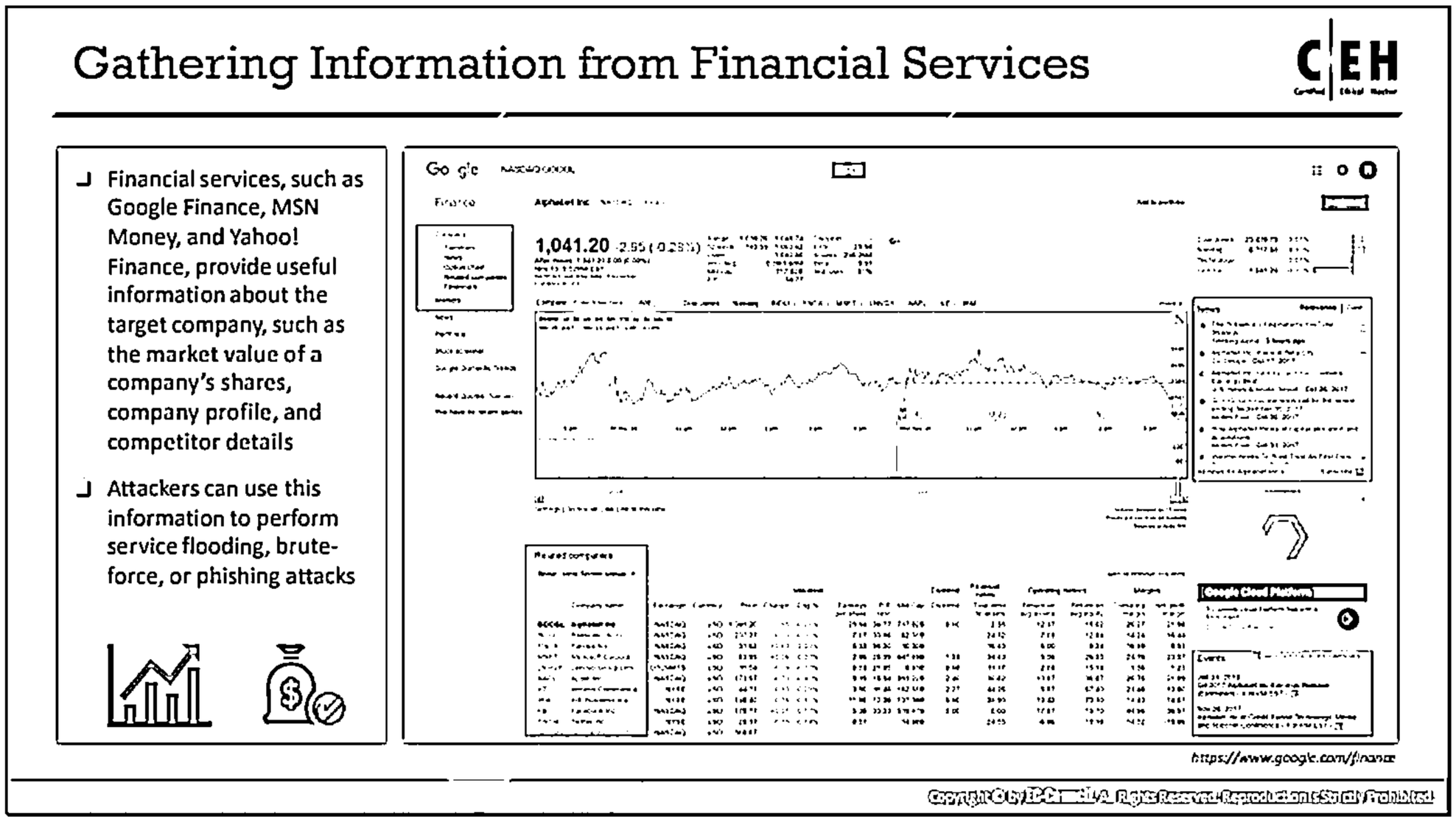


Figure 2.24: Screenshot showing the email list extracted by theHarvester



Gathering Information from Financial Services

Attackers who seek access to personal information or financial information often target financial data such as stock quotes and charts, financial news, and portfolios. Financial services such as Google Finance, MSN Money, Yahoo Finance, and Investing.com can provide a large amount of useful information such as the market value of a company's shares, company profile, competitor details, stock exchange rates, corporate press releases, financial reports along with news, and blog search articles about corporations. The information provided varies from one service to the other. Financial firms rely on web services to perform transactions and grant users access to their accounts. Attackers can obtain sensitive and private information regarding these firms by using malware, exploiting software design flaws, breaking authentication mechanisms, service flooding, and performing brute force attacks and phishing attacks.

- **Google Finance**

  Source: *https://www.google.com/finance*

  The Google finance service features business and enterprise headlines for many corporations, including their financial decisions and major news events. Stock information is also available, as are stock price charts that contain marks for major news events and corporate actions. The site also aggregates Google news and Google blog search articles about each corporation.

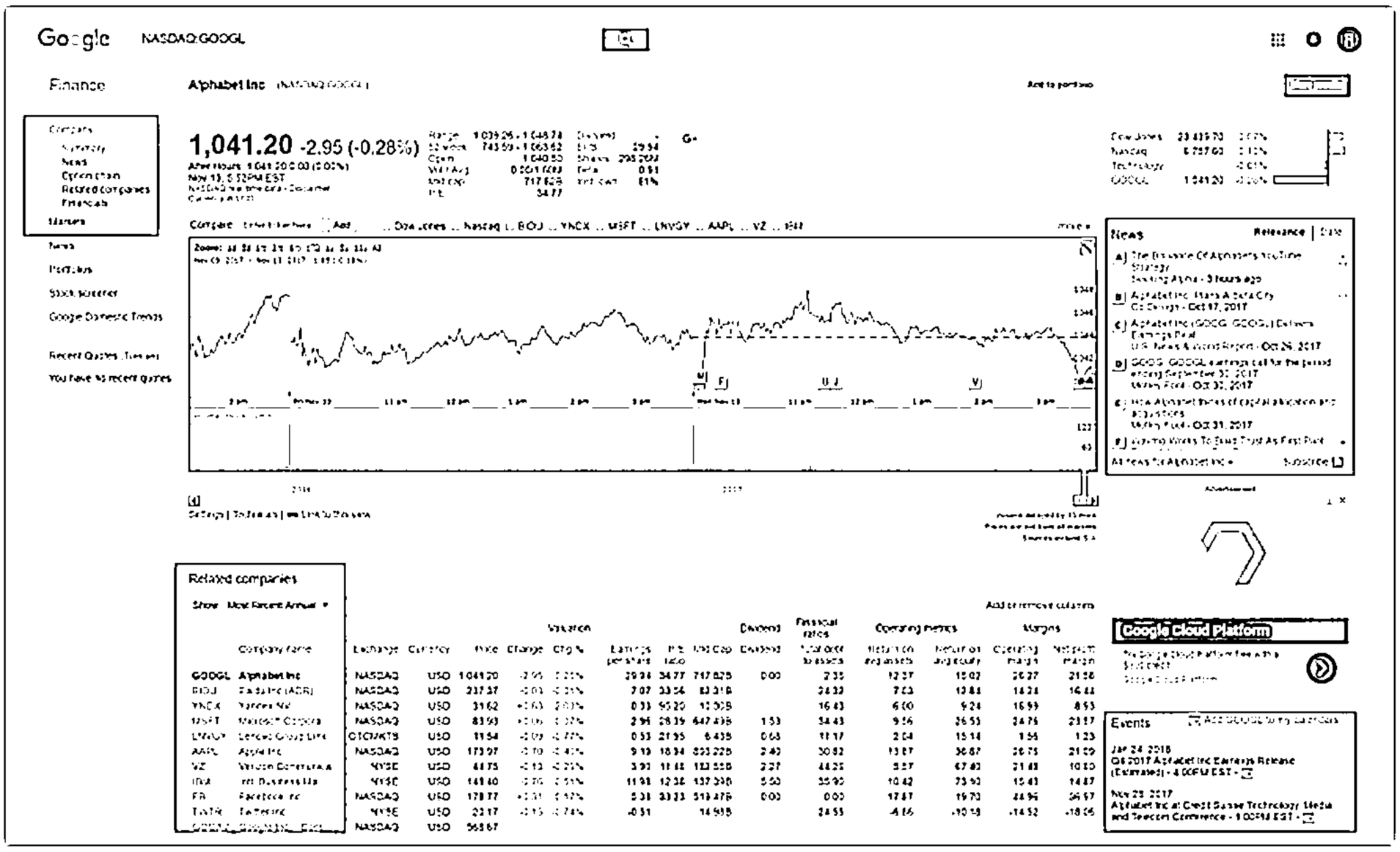
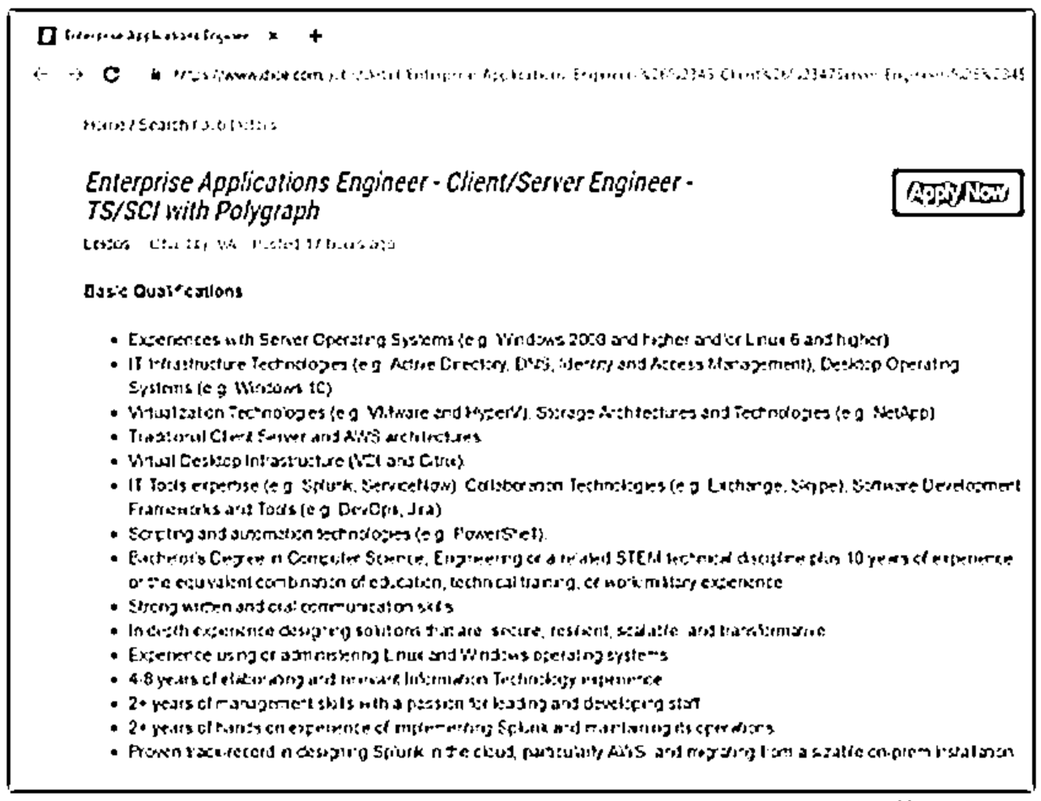


Figure 2.25: Screenshot of Google Finance Service

Footprinting through Job Sites

A company's infrastructure details can be gathered from job postings



Enterprise Application Engineer

https://www.dice.com

Home / Search Jobs / Details

Enterprise Applications Engineer - Client/Server Engineer - TS/SCI with Polygraph

Apply Now

Location: Chantilly, VA Posted: 17 hours ago

Basic Qualifications

- Experiences with Server Operating Systems (e.g. Windows 2008 and higher and/or Linux 6 and higher)
- IT Infrastructure Technologies (e.g. Active Directory, DNS, Identity and Access Management), Desktop Operating Systems (e.g. Windows 10)
- Virtualization Technologies (e.g. VMware and HyperV), Storage Architectures and Technologies (e.g. NetApp)
- Traditional Client Server and AWS architectures
- Virtual Desktop Infrastructure (VDI and Citrix)
- IT Tools expertise (e.g. Splunk, ServiceNow) Collaboration Technologies (e.g. Exchange, Skype), Software Development Frameworks and Tools (e.g. DevOps, Jira)
- Scripting and automation technologies (e.g. PowerShell).
- Bachelor's Degree in Computer Science, Engineering or a related STEM technical discipline plus 10 years of experience or the equivalent combination of education, technical training, or work/military experience
- Strong written and oral communication skills
- In-depth experience designing solutions that are secure, resilient, scalable, and transformative
- Experience using or administering Linux and Windows operating systems
- 4-8 years of elaborating and relevant Information Technology experience
- 2+ years of management skills with a passion for leading and developing staff
- 2+ years of hands on experience of implementing Splunk and maintaining its operations
- Proven track-record in designing Splunk in the cloud, particularly AWS, and migrating from a sizable on-prem installation

https://www.dice.com

Look for these:

- Job requirements
- Employees' profiles
- Hardware information
- Software information

- Attackers use the technical information obtained through job sites, such as Dice, LinkedIn, and Simply Hired, to detect underlying vulnerabilities in the target IT infrastructure

Footprinting through Job Sites

Attackers can gather valuable information about the operating system, software versions, company's infrastructure details, and database schema of an organization through footprinting job sites using different techniques. Many organizations' websites provide recruiting information on a job posting page that, in turn, reveals hardware and software information, network-related information, and technologies used by the company (e.g., firewall, internal server type, OS used, network appliances, and so on.). In addition, the website may have a key employee list with email addresses. Such information may prove to be beneficial for an attacker. For example, if an organization advertises a Network Administrator job, it posts the requirements related to that position.

Further, attackers can go through employee resumes posted on job sites and extract information such as an individual's expertise, educational qualifications, and job history. The job history of an employee can reveal technical information about the target organization. Attackers can use the technical information obtained through job sites such as Dice, LinkedIn, and Simply Hired to detect underlying vulnerabilities in the target IT infrastructure.

Enterprise Applications Engineer ×

https://www.dice.com/jobs/detail/Enterprise-Applications-Engineer-%26%2345-Client%26%2347Server-Engineer-%26%2345

Home / Search / Job Details

Enterprise Applications Engineer - Client/Server Engineer - TS/SCI with Polygraph

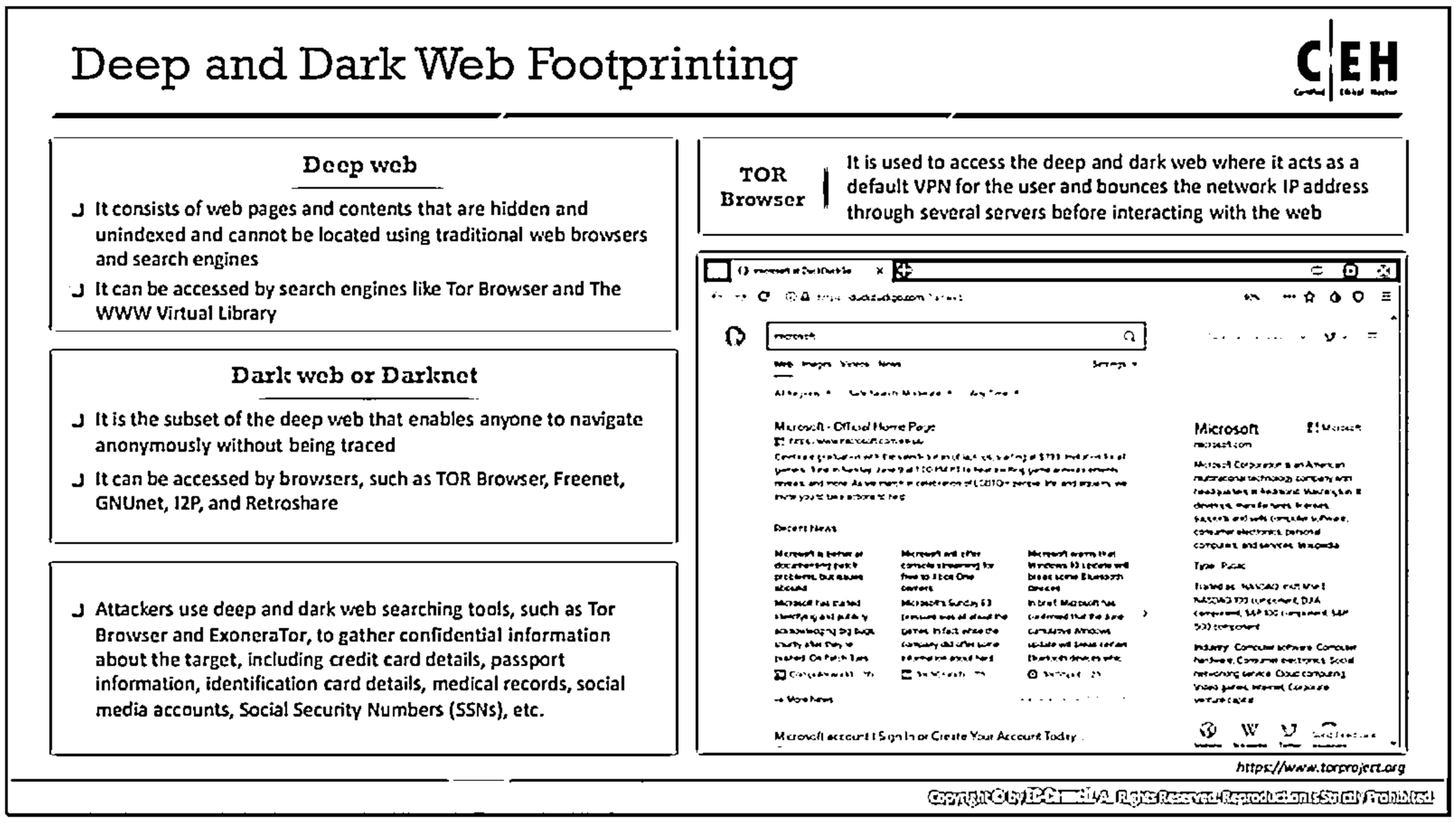
Apply Now

Leidos , Chantilly, VA Posted 17 hours ago

Basic Qualifications

- Experiences with Server Operating Systems (e.g. Windows 2008 and higher and/or Linux 6 and higher).
- IT Infrastructure Technologies (e.g. Active Directory, DNS, Identity and Access Management); Desktop Operating Systems (e.g. Windows 10).
- Virtualization Technologies (e.g. VMware and HyperV); Storage Architectures and Technologies (e.g. NetApp).
- Traditional Client Server and AWS architectures.
- Virtual Desktop Infrastructure (VDI and Citrix).
- IT Tools expertise (e.g. Splunk, ServiceNow); Collaboration Technologies (e.g. Exchange, Skype); Software Development Frameworks and Tools (e.g. DevOps, Jira).
- Scripting and automation technologies (e.g. PowerShell).
- Bachelor's Degree in Computer Science, Engineering or a related STEM technical discipline plus 10 years of experience or the equivalent combination of education, technical training, or work/military experience.
- Strong written and oral communication skills.
- In depth experience designing solutions that are: secure, resilient, scalable, and transformative.
- Experience using or administering Linux and Windows operating systems.
- 4-8 years of elaborating and relevant Information Technology experience.
- 2+ years of management skills with a passion for leading and developing staff.
- 2+ years of hands on experience of implementing Splunk and maintaining its operations.
- Proven track-record in designing Splunk in the cloud, particularly AWS, and migrating from a sizable on-prem installation.

Figure 2.26: Screenshot of job posting showing valuable information



Deep and Dark Web Footprinting

The surface web is the outer layer of the online cyberspace that allows the user to find web pages and content using regular web browsers. Search engines use crawlers that are programmed bots to access and download web pages. The surface web can be accessed by browsers such as Google Chrome, Mozilla Firefox, and Opera.

The deep web is the layer of the online cyberspace that consists of web pages and content that are hidden and unindexed. Such content cannot be located using traditional web browsers and search engines. The size of the deep web is incalculable, and it expands to almost the entire World Wide Web. The deep web does not allow the crawling process of basic search engines. It consists of official government or federal databases and other information linked to various organizations. The deep web can be accessed using search engines such as Tor Browser and the WWW Virtual Library. It can be used for both legal and illegal activities.

The dark web or Darknet is a deeper layer of the online cyberspace, and it is the subset of the deep web that enables anyone to navigate anonymously without being traced. The dark web can be accessed only through specialized tools or darknet browsers. Attackers primarily use the dark web to perform footprinting on the target organization and launch attacks. The dark web can be accessed using search engines such as Tor Browser and ExoneraTor.

Attackers can use deep and dark web searching tools such as Tor Browser, ExoneraTor, and OnionLand Search engine to gather confidential information about the target, such as credit card details, passports information, identification card details, medical records, social media accounts, and Social Security Numbers (SSNs). With the help of this information, they can launch further attacks on the targets.

- **Tor Browser**

  Source: *https://www.torproject.org*

  Tor Browser is used to access the deep and dark web, where it acts as a default VPN for the user and bounces the network IP address through several servers before interacting with the web. Attackers use this browser to access hidden content, unindexed websites, and encrypted databases present in the deep web.

  As shown in the screenshot, by using Tor Browser, attackers can obtain more detailed and hidden information about the target organization.

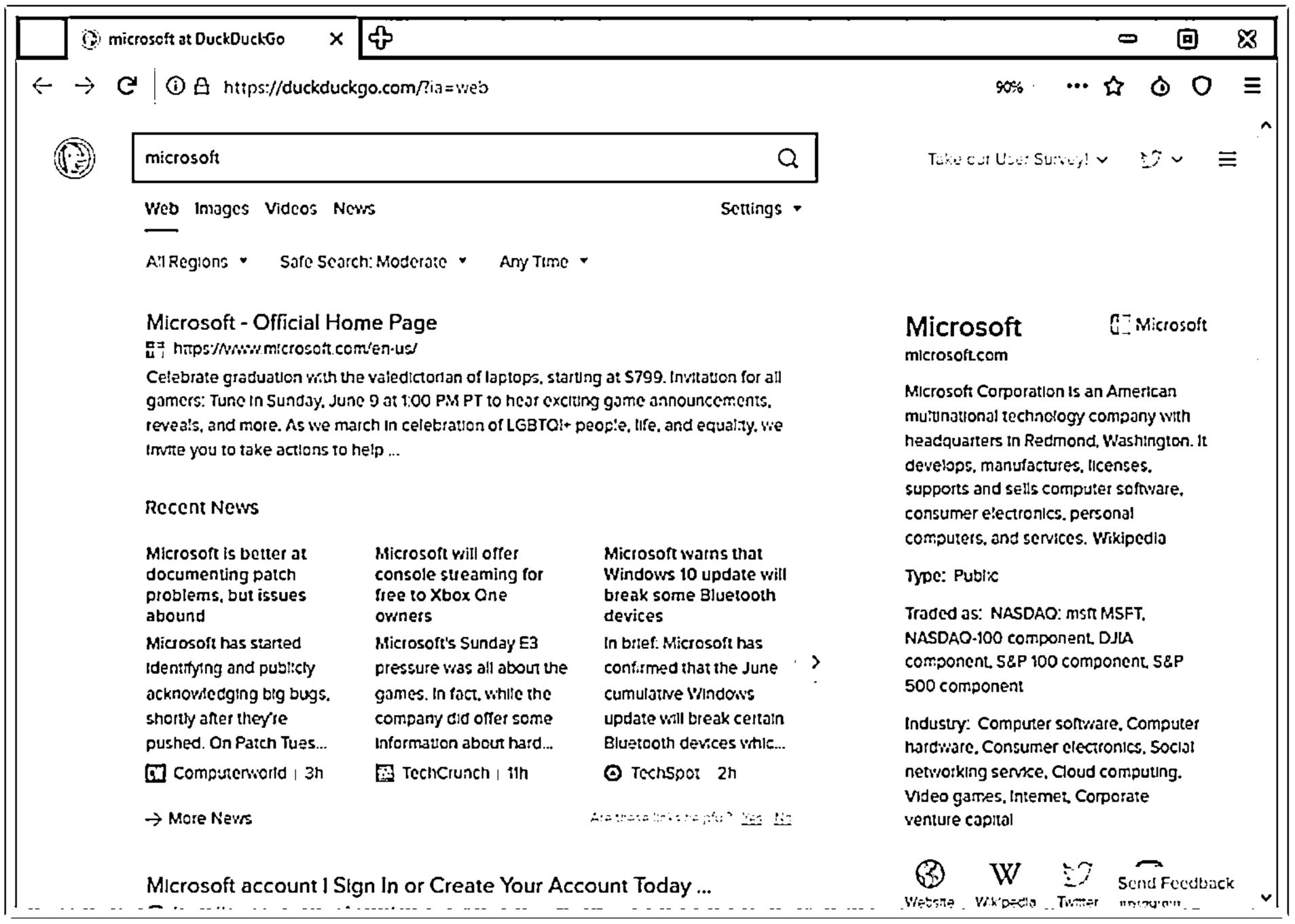
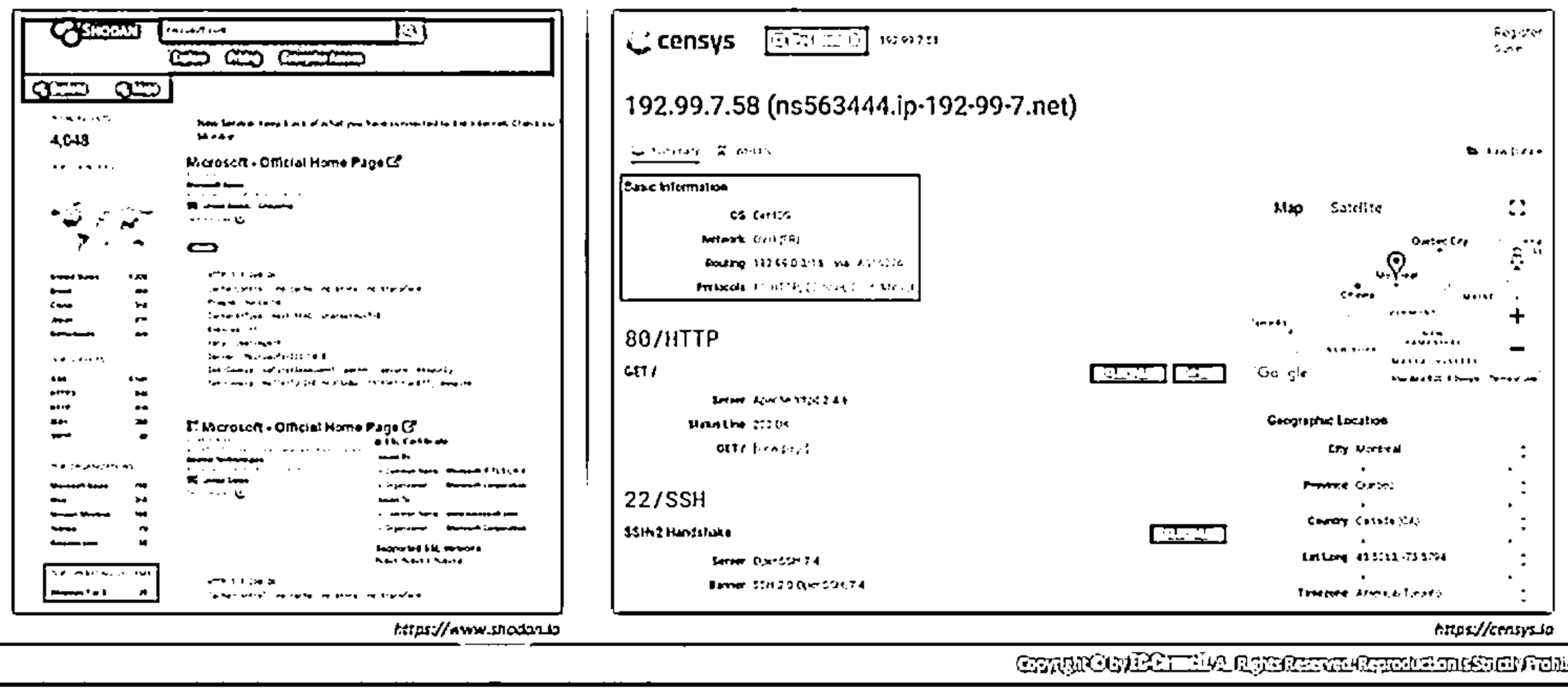


Figure 2.27: Screenshot of Tor Browser

Determining the Operating System

- SHODAN search engine lets you find connected devices (routers, servers, IoT, etc.) using a variety of filters
- Censys search engine provides a full view of every server and device exposed to the Internet



Determining the Operating System

Attackers use various online tools such as Netcraft, Shodan, and Censys to detect the operating system used at the target organization. These tools search the Internet for detecting connected devices such as routers, servers, and IoT devices belonging to the target organization. Using these tools, attackers obtain information such as the city, country, latitude/longitude, hostname, operating system, and IP address of the target organization. Such information further helps attackers in identifying potential vulnerabilities and finding effective exploits to perform various attacks on the target.

- **Netcraft**

  Source: *https://www.netcraft.com*

  The technique of obtaining information about the target network operating system is called OS fingerprinting. Open ***https://www.netcraft.com*** in the browser and type the domain name of the target network in the **What's that site running?** field. Attackers use the Netcraft tool to identify all the sites associated with the target domain along with the operating system running at each site.

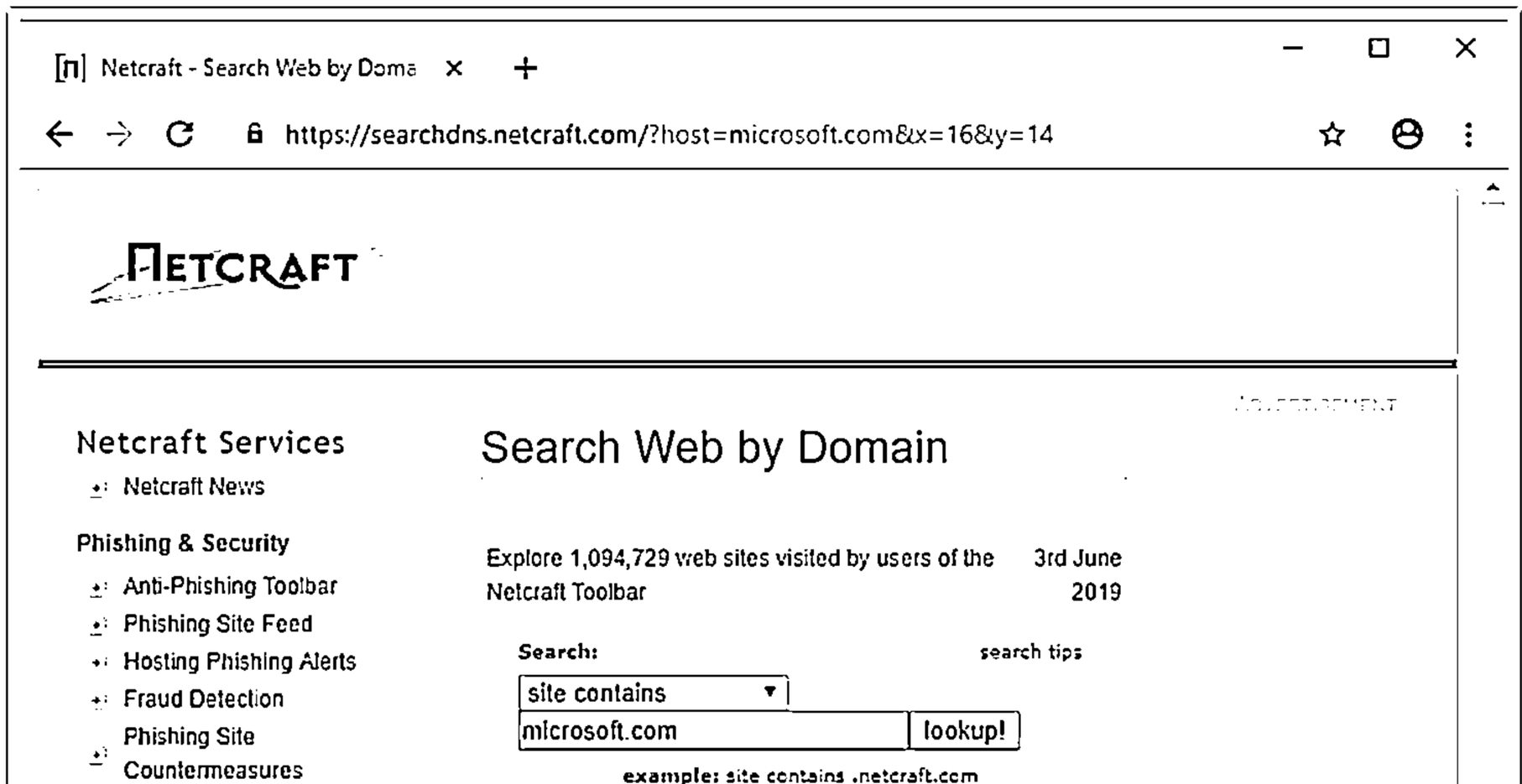


Figure 2.28: Screenshot of Netcraft showing target operating system

- **SHODAN Search Engine**

  Source: *https://www.shodan.io*

  Shodan is a computer search engine that searches the Internet for connected devices (routers, servers, and IoT.). You can use Shodan to discover which devices are connected to the Internet, where they are located, and who is using them.

It helps attackers to keep track of all the devices on the target network that are directly accessible from the Internet. It also allows the attacker to find devices based on the city, country, latitude/longitude, hostname, operating system, and IP address. Further, it helps the attacker to search for known vulnerabilities and exploits across Exploit DB, Metasploit, CVE, OSVDB, and Packetstorm with a single interface.

As shown in the screenshot, attackers use this tool to detect various target devices connected to the Internet along with the operating system used.

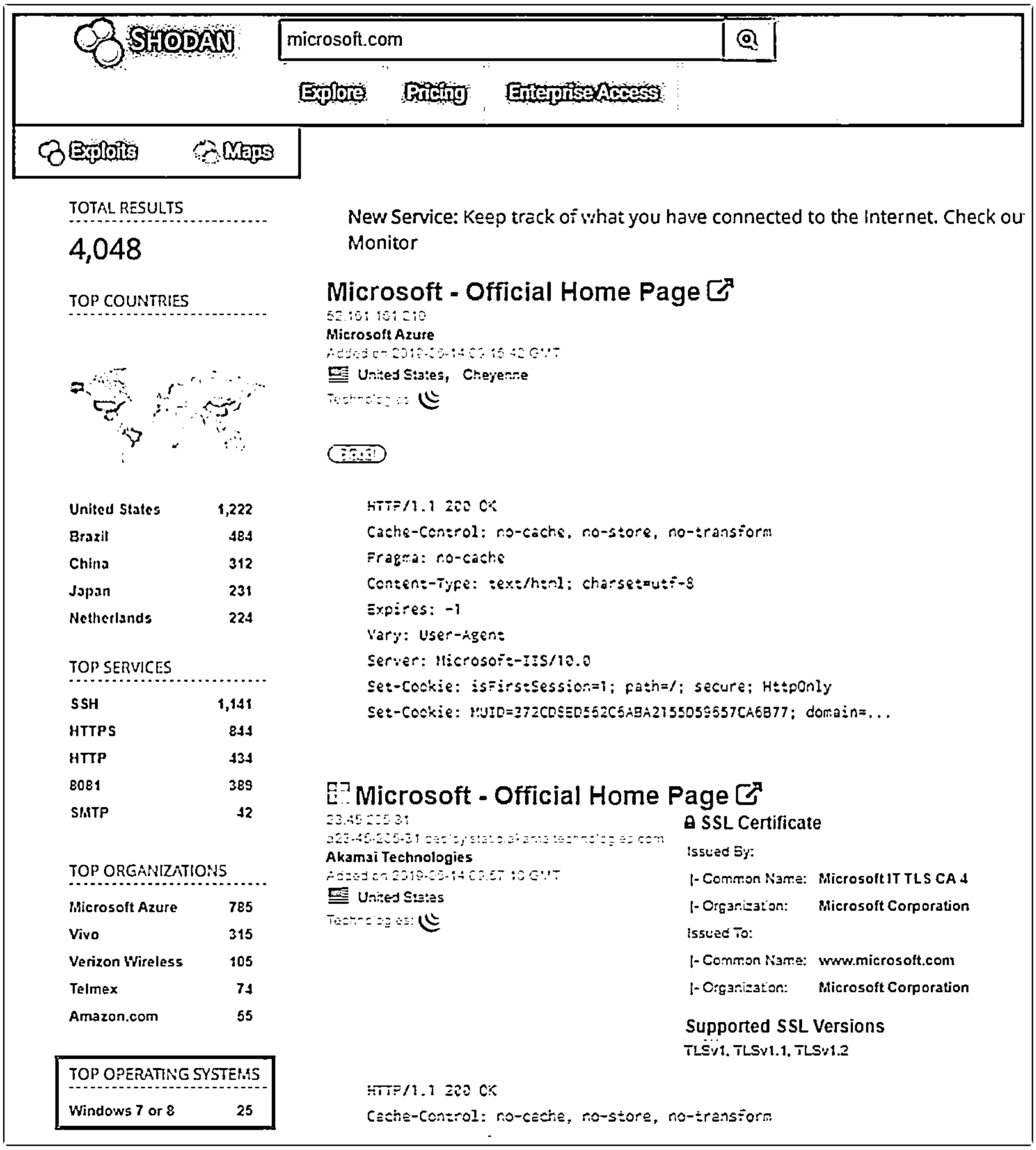


Figure 2.29: Screenshot of SHODAN Search Engine showing target operating system

- **Censys**

  Source*: https://censys.io*

  Censys monitors the infrastructure and discovers unknown assets anywhere on the Internet. It provides a full view of every server and device exposed to the Internet.

  Attackers use this tool to monitor the target IT infrastructure to discover various devices connected to the Internet along with their details such as the operating system used, IP address, protocols used, and geographical location.

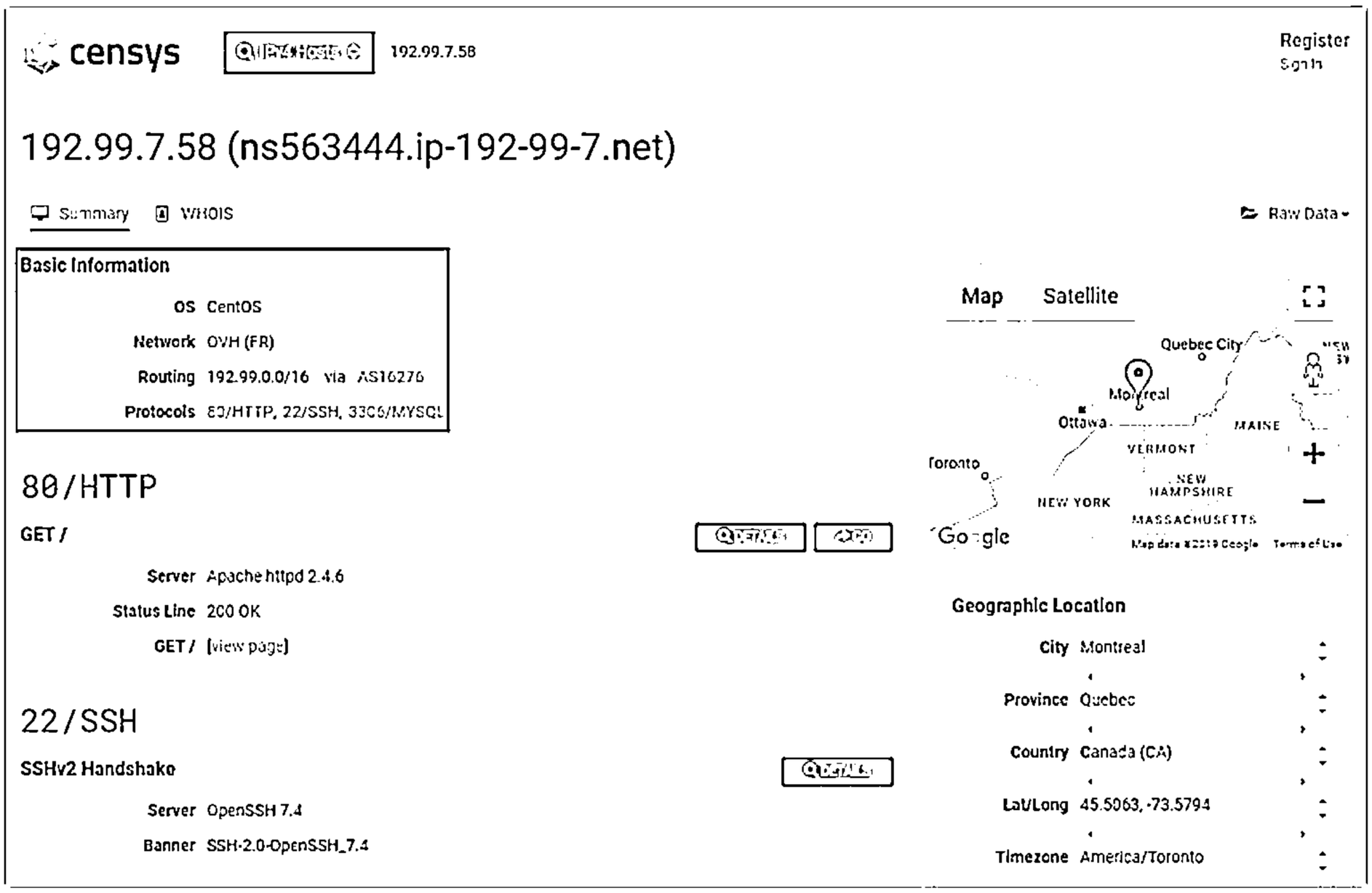
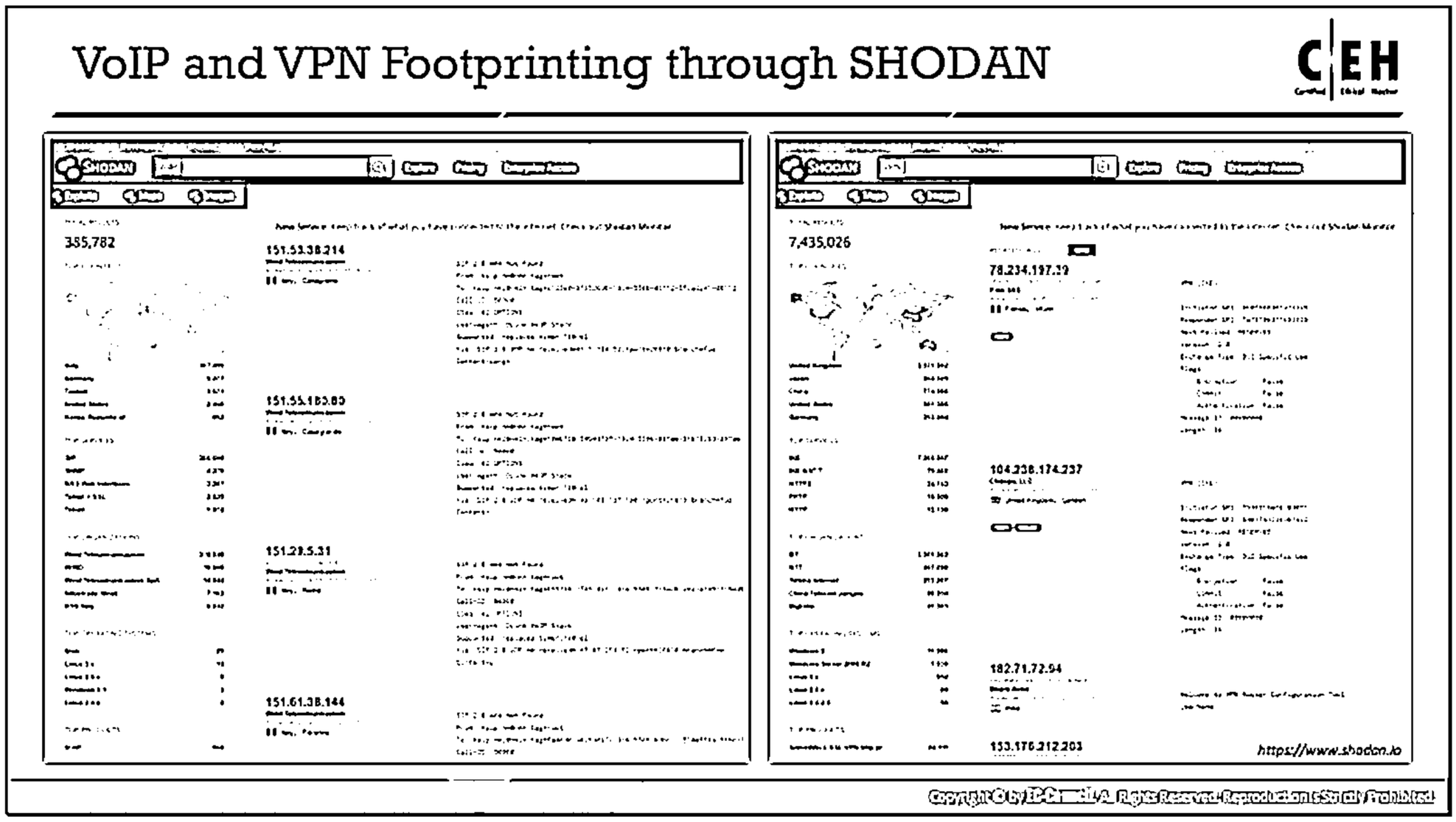


Figure 2.30: Screenshot of Censys Search Engine showing target operating system



VoIP and VPN Footprinting through SHODAN

Source: *https://www.shodan.io*

Shodan is a search engine that enables attackers to perform footprinting at various levels. It is used to detect devices and networks with vulnerabilities. A search in Shodan for VoIP and VPN footprinting can deliver various results, which will help gather VPN- and VoIP-related information. The following screenshots show some of the VPN and VoIP footprinting search results obtained through Shodan:

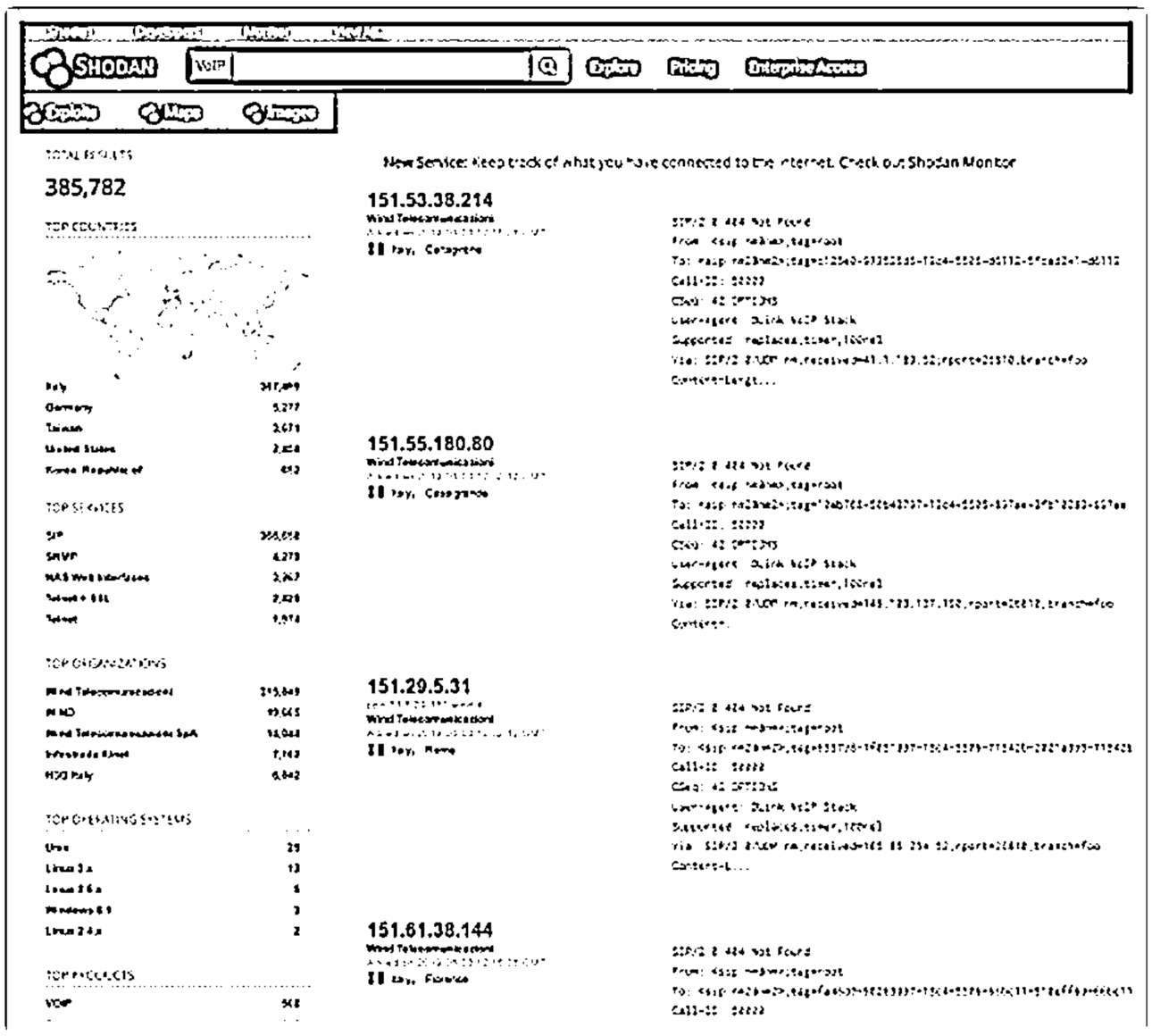


Figure 2.31: Screenshot of SHODAN search engine showing VoIP results

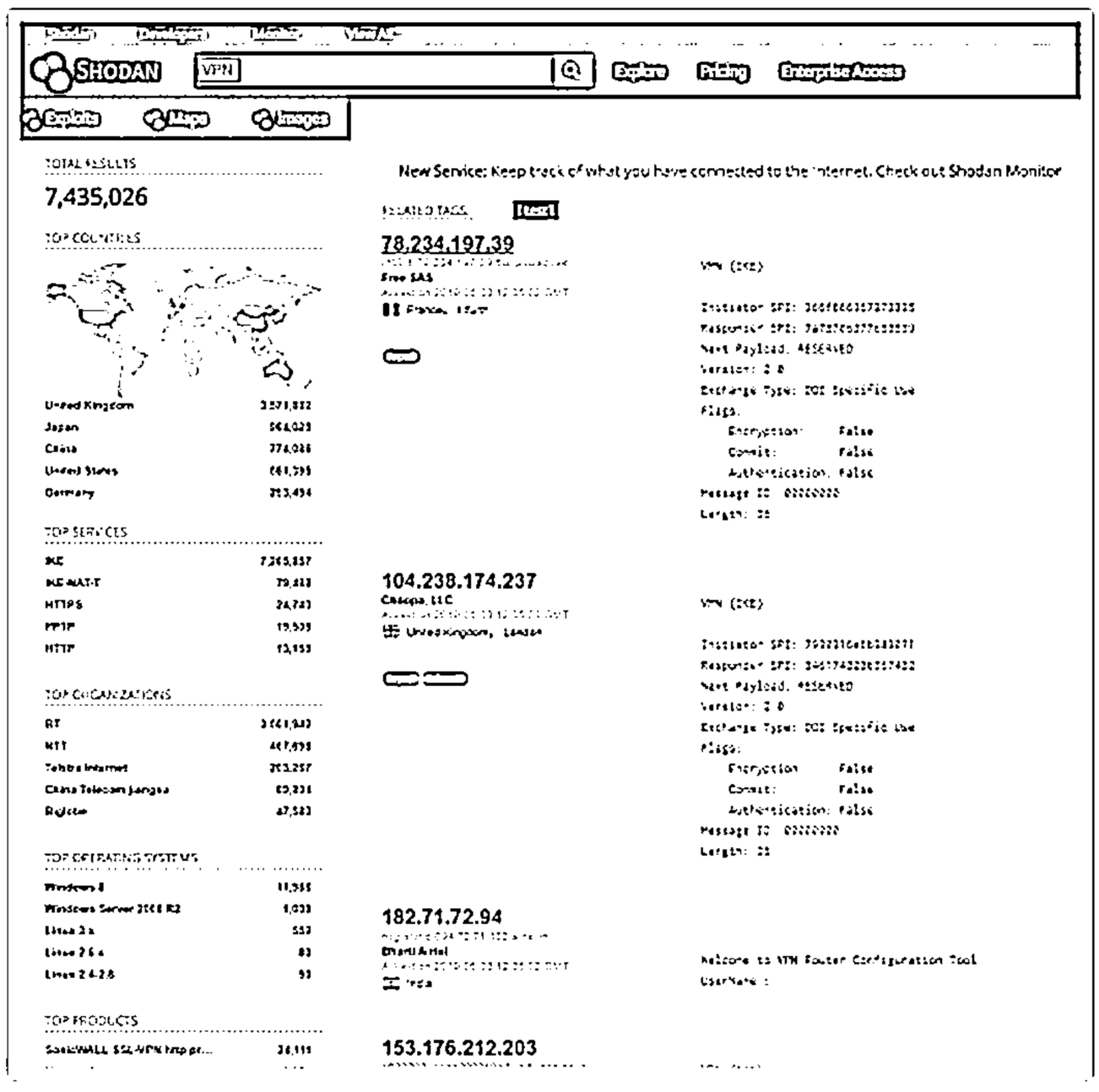


Figure 2.32: Screenshot of SHODAN search engine showing VPN results

Competitive Intelligence Gathering

- Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources, such as the Internet
- Competitive intelligence is non-interfering and subtle in nature

Sources of Competitive Intelligence

1. Company websites and employment ads
2. Search engines, Internet, and online database
3. Press releases and annual reports
4. Trade journals, conferences, and newspapers
5. Patent and trademarks
6. Social engineering employees
7. Product catalogs and retail outlets
8. Analyst and regulatory reports
9. Customer and vendor interviews
10. Agents, distributors, and suppliers

Competitive Intelligence Gathering (Cont'd)

When Did this Company Begin? How Did it Develop?

- Information Resource Sites
  - EDGAR Database
    https://www.sec.gov/edgar.shtml
  - D & B Hoovers
    http://www.hoovers.com
  - LexisNexis
    https://www.lexisnexis.com
  - Business Wire
    http://www.businesswire.com

What Are the Company's Plans?

- Information Resource Sites
  - MarketWatch
    https://www.marketwatch.com
  - The Wall Street Transcript
    https://www.twst.com
  - Alexa
    https://www.olexa.com
  - Euromonitor
    https://www.euromonitor.com

What Expert Opinions Say About the Company?

- Information Resource Sites
  - SEMRush
    https://www.semrush.com
  - AttentionMeter
    http://www.attentionmeter.com
  - ABI/INFORM Global
    https://www.proquest.com
  - SimilarWeb
    https://www.similarweb.com

Competitive Intelligence Gathering

Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet. Competitive intelligence means understanding and learning about other businesses to become as competitive as possible. It is non-interfering and subtle in nature compared to direct intellectual property theft carried out via hacking or industrial espionage. It focuses on the external business

environment. In this method, professionals gather information ethically and legally instead of gathering it secretly.

Competitive intelligence helps in determining:

- What the competitors are doing?
- How competitors are positioning their products and services?
- What customers are saying about competitors' strengths and weaknesses?

Companies carry out competitive intelligence either by employing people to search for information or by utilizing a commercial database service, which involves lower costs. The information that is gathered can help the managers and executives of a company make strategic decisions.

Sources of Competitive Intelligence

Competitive Intelligence gathering can be performed using a direct or indirect approach.

- **Direct Approach**

  The direct approach serves as the primary source for competitive intelligence gathering. Direct approach techniques include gathering information from trade shows, social engineering of employees and customers, and so on.

- **Indirect Approach**

  Through an indirect approach, information about competitors is gathered using online resources. Indirect approach techniques include:

  - Company websites and employment ads
  - Support threads and reviews
  - Search engines, Internet, and online database
  - Social media postings
  - Press releases and annual reports
  - Trade journals, conferences, and newspapers
  - Patent and trademarks
  - Product catalogs and retail outlets
  - Analyst and regulatory reports
  - Customer and vendor interviews
  - Agents, distributors, and suppliers
  - Industry-specific blogs and publications
  - Legal databases, e.g., LexisNexis
  - Business information databases, e.g., Hoover's
  - Online job postings

Competitive Intelligence - When Did this Company Begin? How Did it Develop?

Gathering competitor documents and records helps to improve productivity and profitability, which in turn stimulates the growth of the company. It helps in determining answers to the following:

- **When did it begin?**

  Through competitive intelligence, companies can collect the history of a particular company, such as its establishment date. Sometimes, they gather crucial information that is not often available to others.

- **How did it develop?**

  What are the various strategies that the company uses? Development intelligence can include advertisement strategies, customer relationship management, and so on.

- **Who leads it?**

  This information helps a company learn about the competitor's decision-makers.

- **Where is it located?**

  Competitive intelligence also includes the location of the company and information related to various branches and their operations.

Attackers can use the information gathered through competitive intelligence to build a hacking strategy.

Information Resource Sites

Information resource sites that help to gain competitive intelligence include:

- **EDGAR Database**

  Source: *https://www.sec.gov/edgar.shtml*

  The Electronic Data Gathering, Analysis, and Retrieval system (EDGAR) performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others who are required by law to file with the U.S. Securities and Exchange Commission (SEC). Its primary purpose is to increase the efficiency and fairness of the securities market for the benefit of investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the agency.

- **D&B Hoovers**

  Source: *http://www.hoovers.com*

  D&B Hoovers leverages a commercial database of 120 million business records and analytics to deliver a sales intelligence solution that enables sales and marketing professionals to focus on the right prospects so that they can generate immediate growth for their business.

- **LexisNexis**

  Source: *https://www.lexisnexis.com*

  LexisNexis provides content-enabled workflow solutions designed specifically for professionals in the legal, risk management, corporate, government, law enforcement, accounting, and academic markets. It maintains an electronic database of information related to legal and public records. It enables customers to access documents and records of legal, news, and business sources. It is beneficial for companies and government agencies seeking data analytics supporting compliance, customer acquisition, fraud detection, health outcomes, identity solutions, investigation, receivables management, risk decisioning, and workflow optimization.

- **Business Wire**

  Source: *https://www.businesswire.com*

  Business Wire focuses on press release distribution and regulatory disclosure. This company distributes full-text news releases, photos, and other multimedia content from various organizations across the globe to journalists, news media, financial markets, investors, information website, databases, and general audiences. It has its own patented electronic network through which it releases news.

- **Factiva**

  Source: *https://www.dowjones.com*

  Factiva is a global news database and licensed content provider. It is a business information and research tool that gets information from licensed and free sources and provides capabilities such as searching, alerting, dissemination, and business information management. Factiva products provide access to more than 33,000 sources such as licensed publications, influential websites, blogs, images, and videos. Its resources are made available from nearly every country worldwide in 28 languages, including more than 600 continuously updated newswires.

Competitive Intelligence - What Are the Company's Plans?

Information resource sites that help attackers gain a company's business plans include:

- **MarketWatch**

  Source: *https://www.marketwatch.com*

  MarketWatch tracks the pulse of markets for engaged investors. The site is an innovator in business news, personal finance information, real-time commentary, and investment tools and data, with journalists generating headlines, stories, videos, and market briefs.

- **The Wall Street Transcript**

  Source: *https://www.twst.com*

  The Wall Street Transcript is a website as well as a paid subscription-based publication that publishes industry reports. It expresses the views of money managers and equity

analysts of different industry sectors. The site also publishes interviews with CEOs of companies.

- **Alexa**

  Source: *https://www.alexa.com*

  Alexa is a great tool to dig deep into the analytics of other companies. It allows users to

  - Discover influencer outreach opportunities by uncovering sites that link to their competitors using Competitor Backlink Checker.
  - Benchmark and track their company's performance relative to their competitors using Competitive Intelligence Tools.

- **Euromonitor**

  Source: *https://www.euromonitor.com*

  Euromonitor provides strategy research capabilities for consumer markets. It publishes reports on industries, consumers, and demographics. It provides market research and surveys focused on the organization's needs.

- **Experian**

  Source: *https://www.experian.com*

  Experian provides insights into competitors' search, affiliate, display, and social marketing strategies and metrics to improve marketing campaign results. It allows the user to:

  - Benchmark the effectiveness of existing customer acquisition strategies
  - Determine what is driving competitors' success
  - Use historical consumer data to forecast future trends and quickly respond to changing behaviors
  - Measure website's performance against industry or specific sites

- **SEC Info**

  Source: *http://www.secinfo.com*

  SEC Info offers the U.S. Securities and Exchange Commission (SEC) EDGAR database service on the web, with many links added to SEC documents. It allows searches by name, industry, business, SIC code, area code, accession number, file number, CIK, topic, ZIP code, and so on.

- **The Search Monitor**

  Source: *https://www.thesearchmonitor.com*

  The Search Monitor provides competitive intelligence to monitor brand and trademark use, affiliate compliance, and competitive advertisers on paid search, organic search, local search, social media, mobile, and shopping engines worldwide. It helps interactive agencies, search marketers, and affiliate marketers to track ad rank, ad copy, keyword

reach, click rates and CPCs, monthly ad spending, market share, trademark use, and affiliate activity.

- **USPTO**

  Source: *https://www.uspto.gov*

  The United States Patent and Trademark Office (USPTO) provides information related to patent and trademark registration. It provides general information concerning patents and search options for patents and trademark databases.

Competitive Intelligence - What Expert Opinions Say About the Company?

Information resource sites that help the attacker to obtain expert opinions about the target company include:

- **SEMRush**

  Source: *https://www.semrush.com*

  SEMRush is a competitive keyword research tool. It can provide a list of Google keywords and AdWords for any site, as well as a competitor list in the organic and paid Google search results. It enables an approach for gaining in-depth knowledge about what competitors are advertising and their budget allocation to specific Internet marketing tactics.

- **AttentionMeter**

  Source: *http://www.attentionmeter.com*

  AttentionMeter is a tool for comparing websites (traffic) by using Alexa, Compete, and Technorati. It gives a snapshot of traffic data as well as graphs from Alexa, Compete, and Technorati for the specified websites.

- **ABI/INFORM Global**

  Source: *https://www.proquest.com*

  ABI/INFORM Global is a business database. ABI/INFORM Global offers the latest business and financial information for researchers. With ABI/INFORM Global, users can determine business conditions, management techniques, business trends, management practice and theory, corporate strategy and tactics, and the competitive landscape.

- **SimilarWeb**

  Source: *https://www.similarweb.com*

  SimilarWeb aggregates data from multiple sources to estimate traffic, geography, and referral data for a company's websites and mobile apps. It also provides a panel through a browser extension that allows refining other data sources by anonymously tracking browser activity across millions of browsers worldwide.

Other Techniques for Footprinting through Web Services

Information Gathering Using Business Profile Sites	❑ Business profile sites contain the business information of companies located in a particular region, which includes their contact information and can be viewed by anyone ❑ Attackers use business profile sites, such as opencorporates and Crunchbase, to gather important information about the target organizations, such as their location, addresses, contact information, and employee database
Monitoring Targets Using Alerts	❑ Alerts are content monitoring services that automatically provide up-to-date information based on your preference, usually via email or SMS ❑ Tools, such as Google Alerts and Twitter Alerts, help attackers to track mentions of the organization's name, member names, website, or any people or projects
Tracking Online Reputation of the Target	❑ Online Reputation Management (ORM) is a process of monitoring a company's reputation on the Internet and taking certain measures to minimize the negative search results/reviews and thereby improve its brand reputation ❑ Attackers use ORM tracking tools, such as Trackur and Brand24, to track a company's online reputation, search engine ranking information, email notifications when a company is mentioned online, and social news about the company

Other Techniques for Footprinting through Web Services (Cont'd)

Information Gathering Using Groups, Forums, and Blogs

- Groups, forums, and blogs provide sensitive information about a target, such as public network information, system information, and personal information
- Attackers register with fake profiles in Google groups, Yahoo groups, etc. and try to join the target organization's employee groups, where they share personal and company information

Information Gathering Using NNTP Usenet Newsgroups

- Usenet newsgroup is a repository containing a collection of notes or messages on various subjects and topics that are submitted by the users over the Internet
- Attackers can search the Usenet newsgroups, such as Newshosting and Eweka, to find valuable information about the operating systems, software, web servers, etc. used by the target organization

Other Techniques for Footprinting through Web Services

- **Information Gathering Using Business Profile Sites**

  Finding useful information from corporate websites is a necessary step in the information gathering phase. These business profile sites contain business information of companies located in a particular region with their contact information, which can be viewed by anyone.

Attackers use business profile sites such as opencorporates, Crunchbase, and corporationwiki to gather important information about the target organizations, such as their location, addresses, contact information (such as phone numbers, email addresses), employee database, department names, type of service provided, and type of industry.

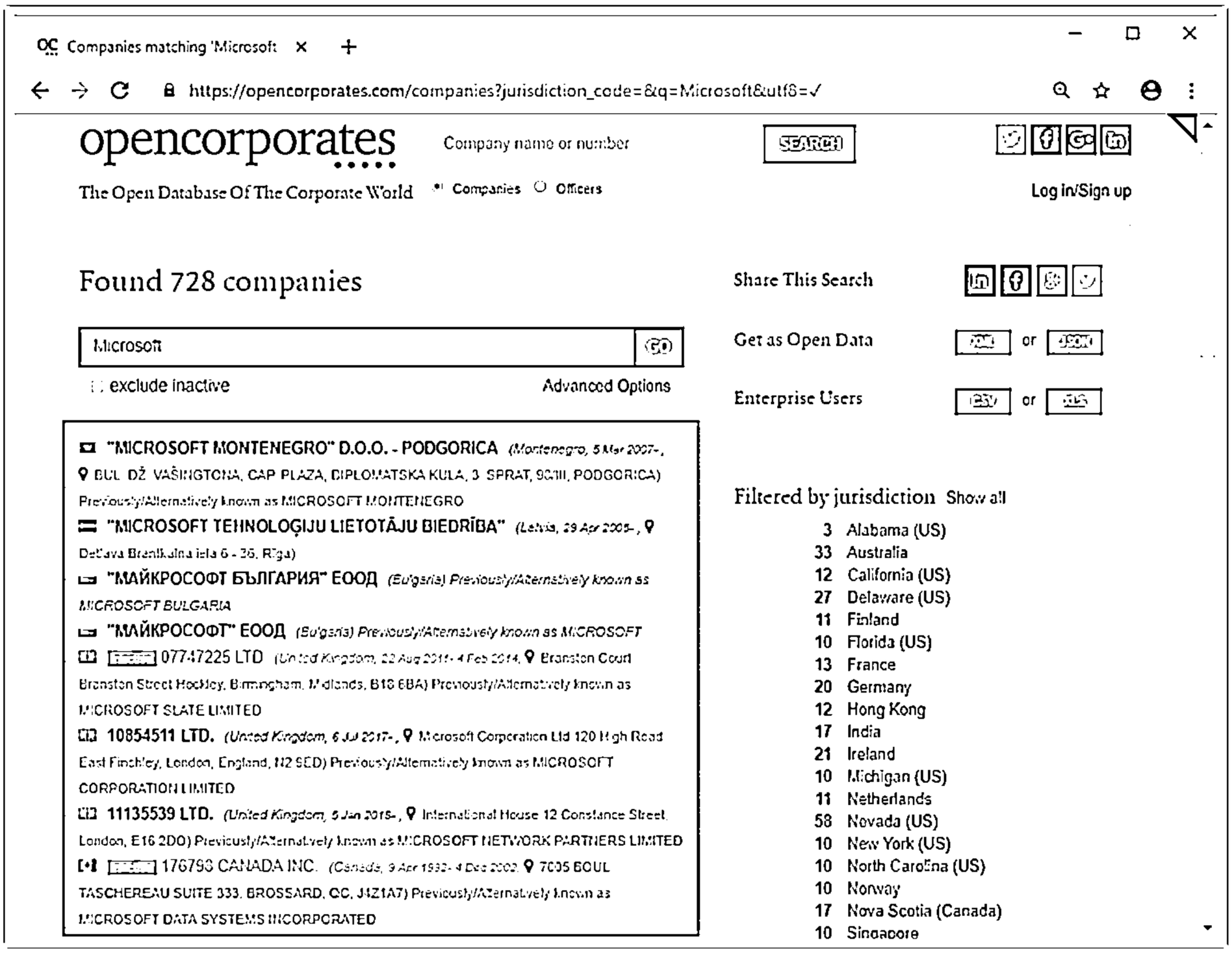


Figure 2.33: Screenshot of opencorporates showing search results of Microsoft

- **Monitoring Targets Using Alerts**

  Alerts are content monitoring services that provide automated, up-to-date information based on user preference, usually via email or SMS. To receive alerts, a user must register on the website and provide either an email address or a phone number. Online alert services automatically notify users when new content from news, blogs, and discussion groups matches a set of search terms selected by the user. These services provide up-to-date information about competitors and the industry. Alerts are sent via email or SMS notifications.

  Tools such as Google Alerts, Twitter Alerts, and Giga Alerts help attackers to track mentions of the organization's name, member names, website, or any people or projects that are important. Attackers can gather updated information about the target periodically from the alert services and use it for further attacks.

- **Google Alerts**

  Source: *https://www.google.com/alerts*

  Google Alerts automatically notifies users when new content from news, websites, blogs, videos, and/or discussion groups matches a set of search terms selected by the user and stored by the Google Alerts service.

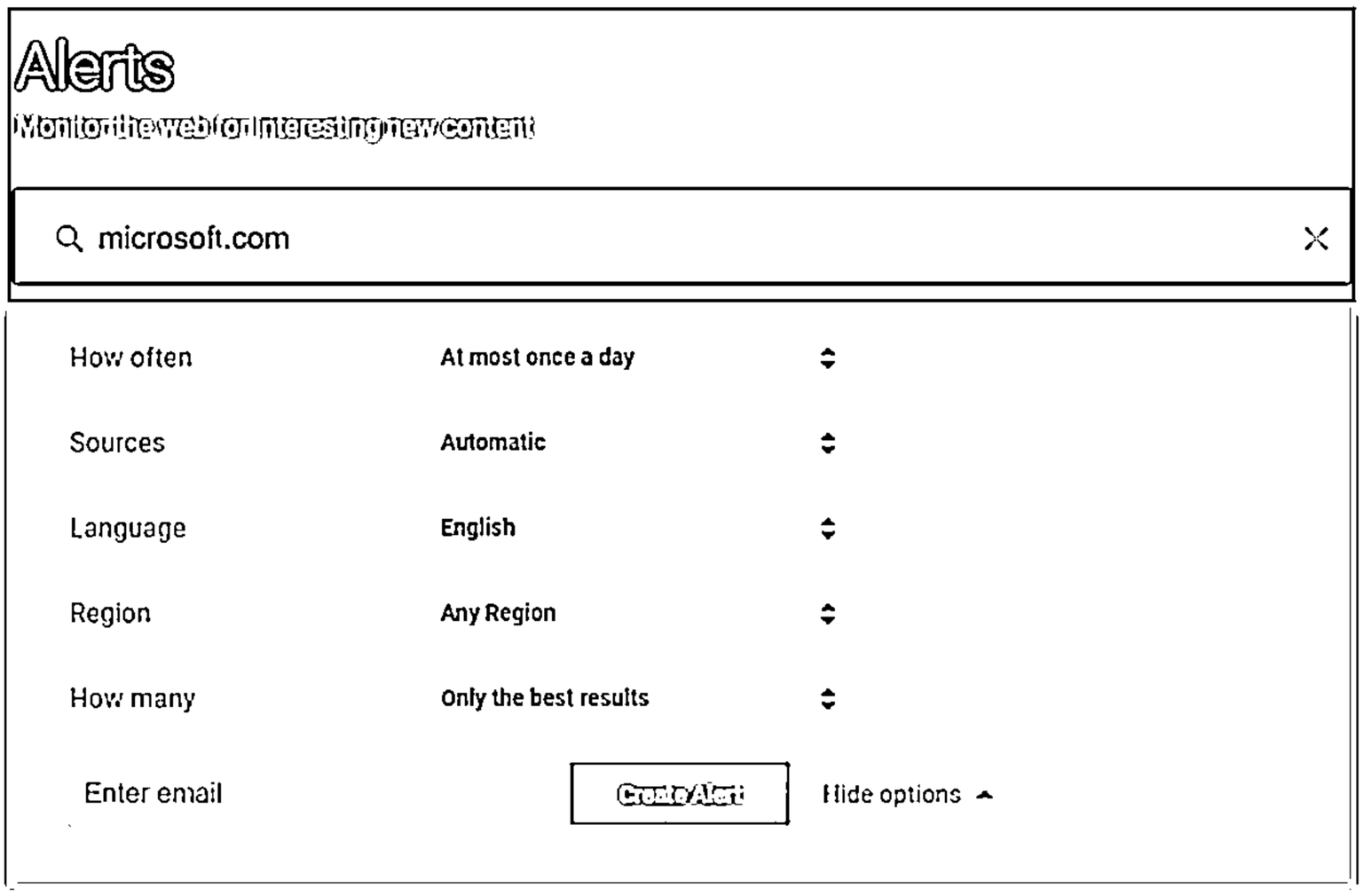


Figure 2.34: Screenshot of Google Alert

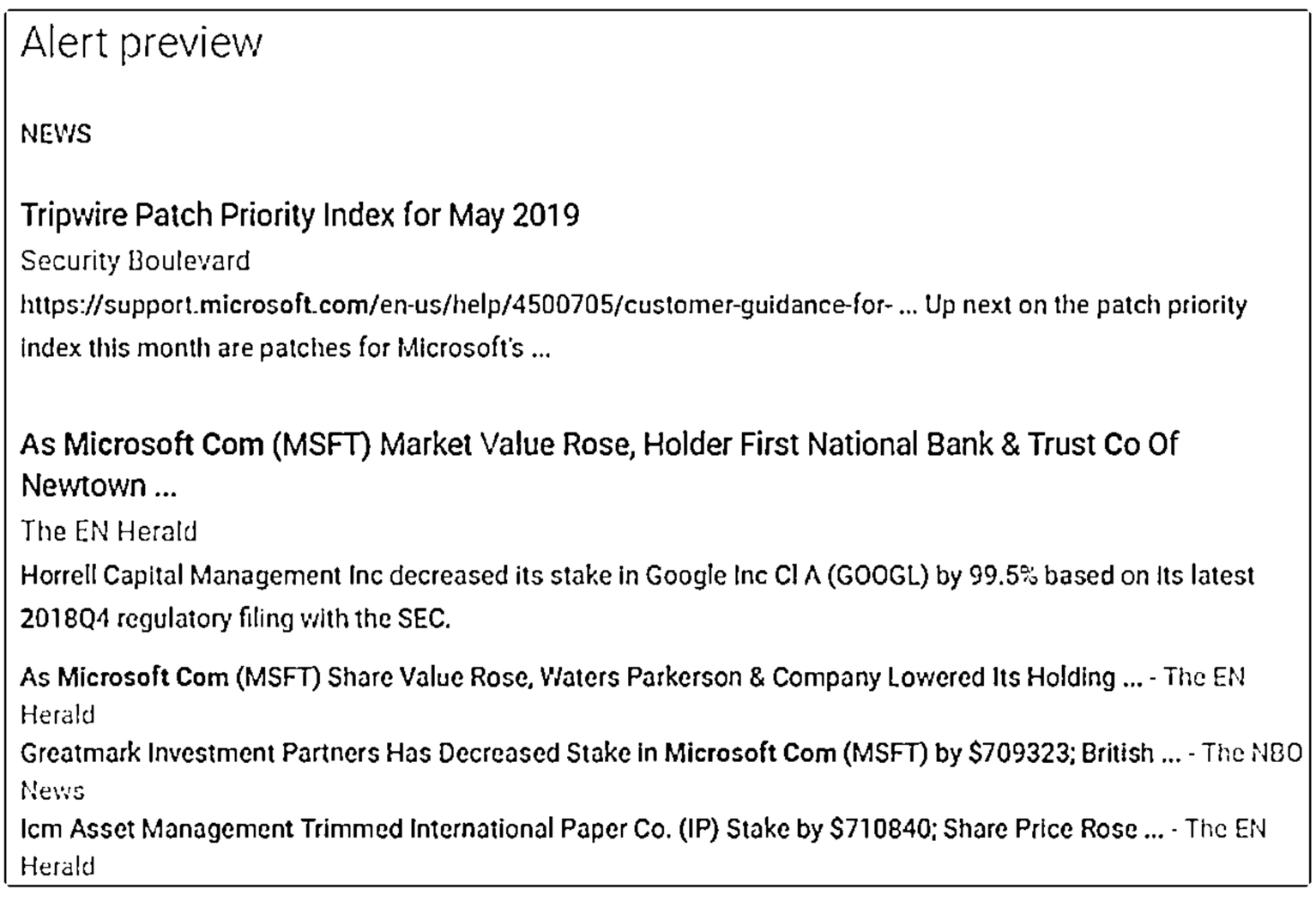


Figure 2.35: Screenshot of Google Alert Preview

- **Tracking Online Reputation of the Target**

  Online Reputation Management (ORM) is a process of monitoring displays when someone searches for your company's reputation on the Internet. ORM then takes measures to minimize negative search results or reviews. The process helps to improve brand reputation.

  Companies often track the public feedback given to them using ORM tracking tools and then take measures to improve their credibility and retain their customers' trust. For positive online reputation management, organizations will often try to be more transparent over the Internet. This transparency may help the attacker to collect genuine information about the target organization.

  Online Reputation Tracking Tools

  Online reputation tracking tools help us to discover what people are saying online about the company's brand in real time across the web, social media, and news. They help in monitoring, measuring, and managing one's reputation online.

  An attacker may use ORM tracking tools to:

  - Track a company's online reputation
  - Collect a company's search engine ranking information
  - Obtain email notifications when a company is mentioned online
  - Track conversations
  - Obtain social news about the target organization

  Mention

  Source: *https://mention.com*

  Mention is an online reputation tracking tool that helps attackers in monitoring the web, social media, forums, and blogs to learn more about the target brand and industry. As shown in the screenshot, this tool helps attackers in tracking online conversations as they happen, wherever they happen. Using Mention, attackers can have live, up-to-date reports delivered to any email address in real time.

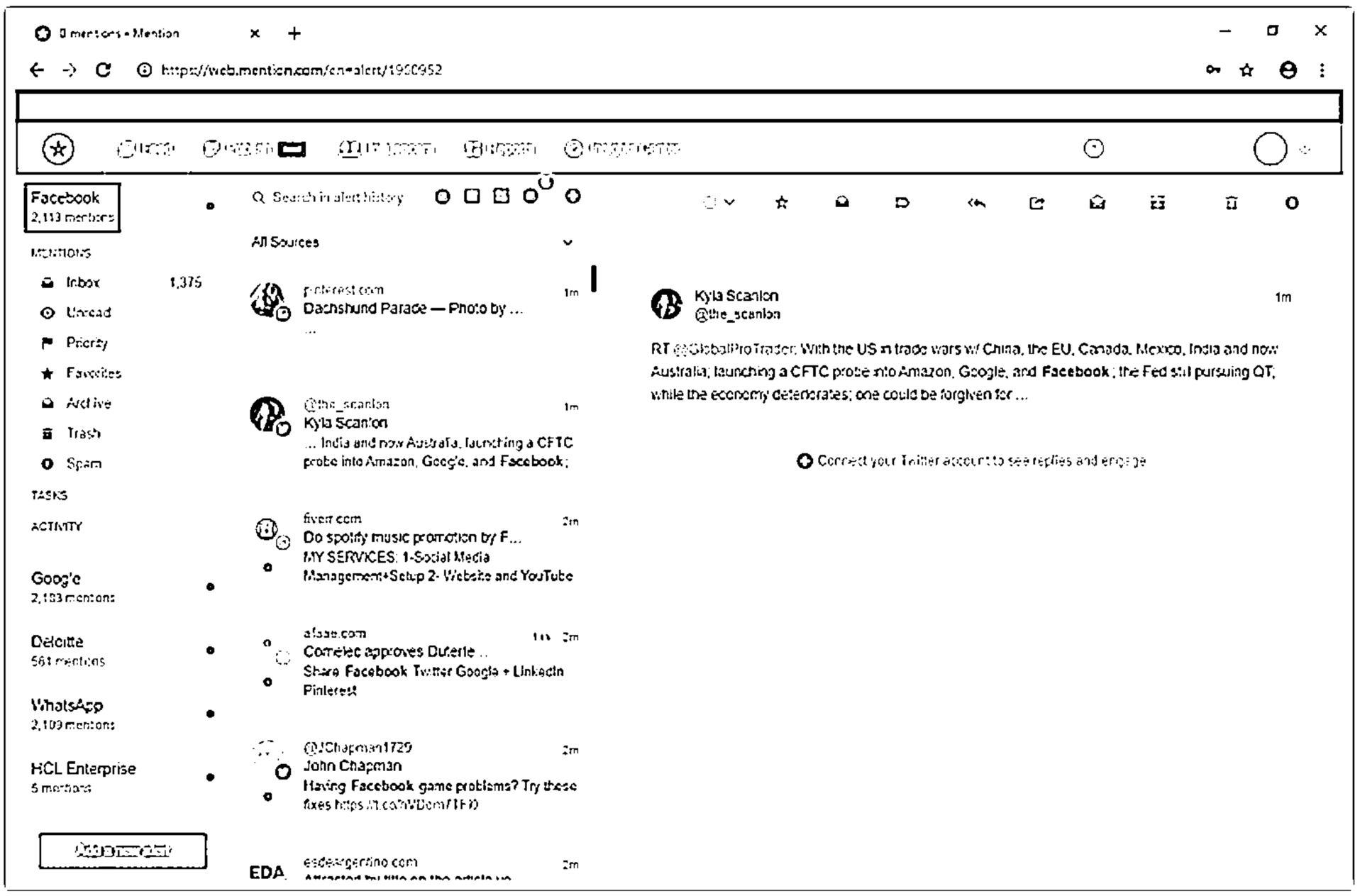


Figure 2.36: Screenshot of Mention

- **Information Gathering Using Groups, Forums, and Blogs**

  Many Internet users use blogs, groups, and forums for knowledge sharing purposes. For this reason, attackers often focus on groups, forums, and blogs to find information about a target organization and its people. Organizations generally fail to monitor the exchange of information that employees reveal to other users in forums, blogs, and group discussions. Attackers see this as an advantage and collect sensitive information about the target, such as public network information, system information, and employee personal information. Attackers can register with fake profiles in Google groups, Yahoo groups, and so on. They try to join the target organization's employee groups, where they can obtain personal and company information. Attackers can also search for information in groups, forums, and blogs by Fully Qualified Domain Names (FQDNs), IP addresses, and usernames.

  Employee information that an attacker can gather from groups, forums, and blogs may include:

  - Full name of the employee
  - Place of work and residence
  - Home telephone, cell number, or office number
  - Personal and organizational email address

- Pictures of the employee residence or work location that include identifiable information
- Pictures of employee awards and rewards or upcoming goals

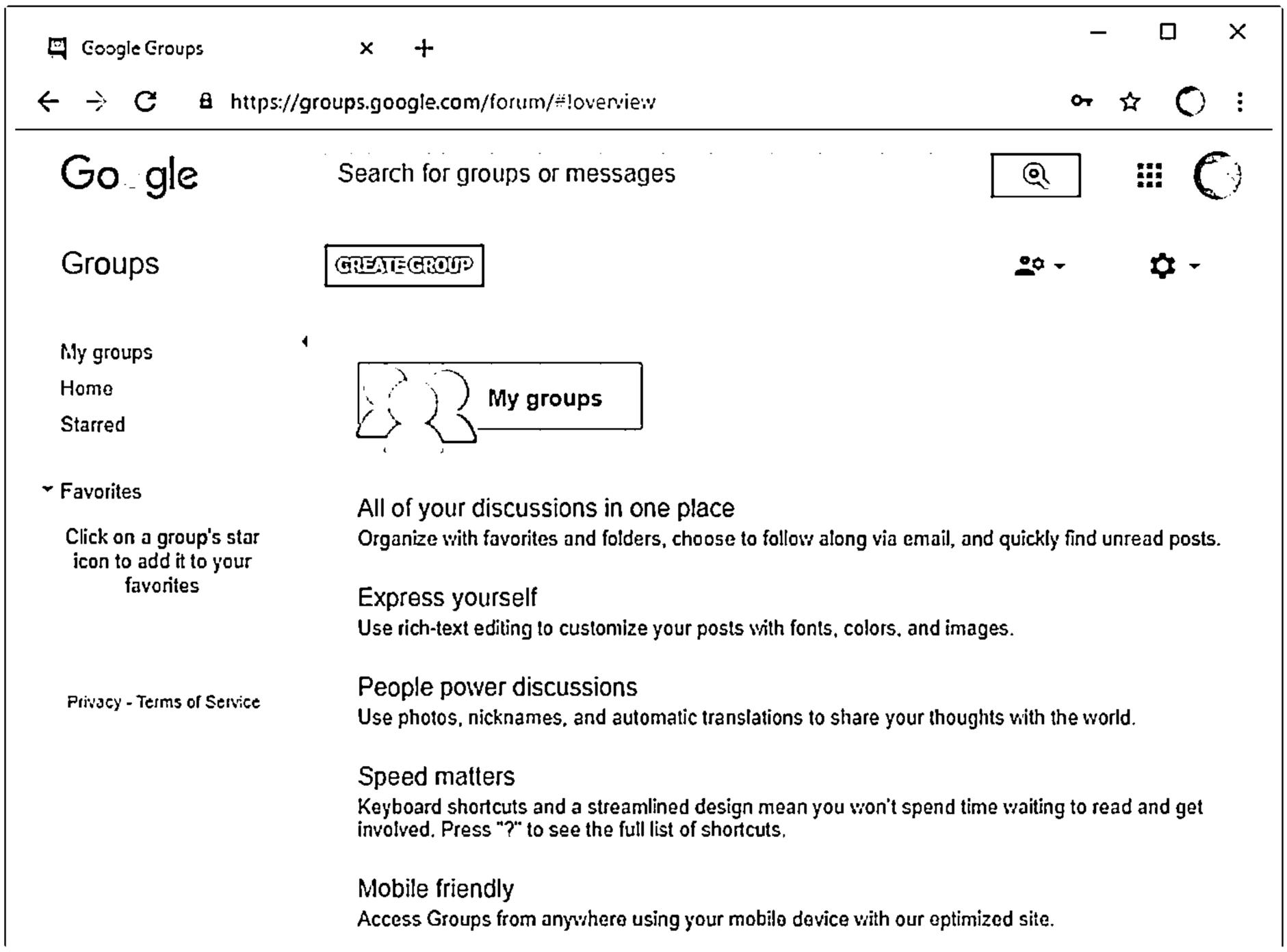


Figure 2.37: Screenshot of Google Groups

- **Information Gathering Using NNTP Usenet Newsgroups**

  Usenet newsgroup is a repository containing a collection of notes or messages on various subjects and topics that are submitted by the users over the Internet. Network News Transfer Protocol (NNTP) is used to relay Usenet news articles from the discussions over the newsgroup. Usenet newsgroups can be a useful source of valuable information about the target. People seek help by posting questions and asking for a solution on Usenet newsgroups. Many professionals use the newsgroups to resolve their technical issues by posting questions on Usenet. To obtain solutions for these issues, sometimes they post more detailed information about the target than needed. Attackers can search Usenet newsgroups or mailing lists such as Newshosting, Eweka, and Supernews to find valuable information about the operating systems, software, web servers, etc., used by the target organization.

For example, from the screenshot given below, you can understand that the target organization is using a Red Hat Linux 6.2 machine that is running Apache web server 1.3.23. This information helps attackers in performing web server and web application attacks.

From: adams@certifiedhacker.com
Subject: Apache Problem
Newsgroups: comp.infosystems.www.servers.unix, comp.os.linux, alt.apache.configuration, comp.lang.java.programmer
Date: 2018-02-27 09:19:28 PST

I am having a problem with Apache reverse proxy not communicating with web applications using HTTP 1.1 keepalive. I am using Apache 1.3.23 on Red Hat Linux 6.2. It is compiled with mod_proxy and mod_ssl.

Any ideas would be greatly appreciated.
Thank you.

---
adams@certifiedhacker.com
Sr. Systems Administrator
certifiedhacker.com

Figure 2.38: Screenshot of sample USENET newsgroup posting

Collecting Information through Social Engineering on Social Networking Sites

- Attackers use social engineering tricks to gather sensitive information from social networking websites
- Attackers create a fake profile and then use the false identity to lure employees into revealing their sensitive information
- Attackers collect information about the employees' interests and tricks them into revealing more information

What Users Do	What Attacker Gets
Maintain profile	Contact info, location, etc.
Connect to friends, chat	Friends list, friends' info, etc.
Share photos and videos	Identity of family members, interests, etc.
Play games, join groups	Interests
Create events	Activities

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Recruitment	Platform/technology
Background check to hire employees	Type of business

Footprinting through Social Networking Sites

While footprinting through social networking sites may seem similar to footprinting through social engineering (which is discussed in greater detail later), there are some differences between the two methods. In footprinting through social engineering, the attacker tricks people into revealing information, whereas in footprinting through social networking sites, the attacker gathers information available on those sites. Attackers can even use social networking sites as a medium to perform social engineering attacks.

This section explains the type of information one can collect from social networking sites using social engineering and how it can be obtained. It aims to familiarize you with locating information from social media sites using various online services and resources.

Collecting Information through Social Engineering on Social Networking Sites

Social networking sites are online services, platforms, or other sites that allow people to connect and to build interpersonal relations. The use of social networking sites is increasing rapidly. Examples of such sites include LinkedIn, Facebook, Instagram, Twitter, Pinterest, YouTube, and so on. Each social networking site has its own purpose and features. One site may connect friends, family and so on, while another helps users to share professional profiles. Social networking sites are open to everyone. Attackers may take advantage of this feature to gather sensitive information from users either by browsing through users' public profiles or by creating a fake profile to pose as a genuine user. On social networking sites, people may post personal information such as date of birth, educational information, employment background, spouse's names, and so on. Organizations often post information such as potential partners, websites, and upcoming news about the company.

For an attacker, social networking sites can be valuable sources of information about the target person or organization. The attacker can only gather the information that is posted by individuals. There are no barriers for attackers to access the public pages of accounts created on social networking sites. To obtain more information about the target, attackers may create fake accounts and use social engineering techniques to lure the victim into revealing more information. For example, the attacker can send a friend request to the target person from a fake account; if the victim accepts the request, then the attacker can access even the restricted pages of the target person on that website.

Information Available on Social Networking Sites

So far, we have discussed *how* an attacker can collect information from social networking sites. Now, we will discuss *what* information an attacker can get from social networking sites.

People usually maintain profiles on social networking sites to provide basic information about themselves and to help create and maintain connections with others. A profile generally contains personal information such as a person's name, contact information (cell phone number, email address), friends' information, information about family members, interests, and activities. People usually connect with friends and chat with them. Attackers can gather sensitive information through these chats. Social networking sites also allow people to share photos and videos. If users fail to set the appropriate privacy settings for their albums, then attackers can see the pictures and videos shared by them. Users may join groups to play games or to share their views and interests. Attackers can collect information about the victim's interests by tracking his or her groups and can then mislead the victim into revealing more information. Users may create events to notify other users about upcoming occasions, from which attackers will come to know about the user's activities.

The activities of users on social networking sites and the respective information that an attacker can collect is summarized in the following table.

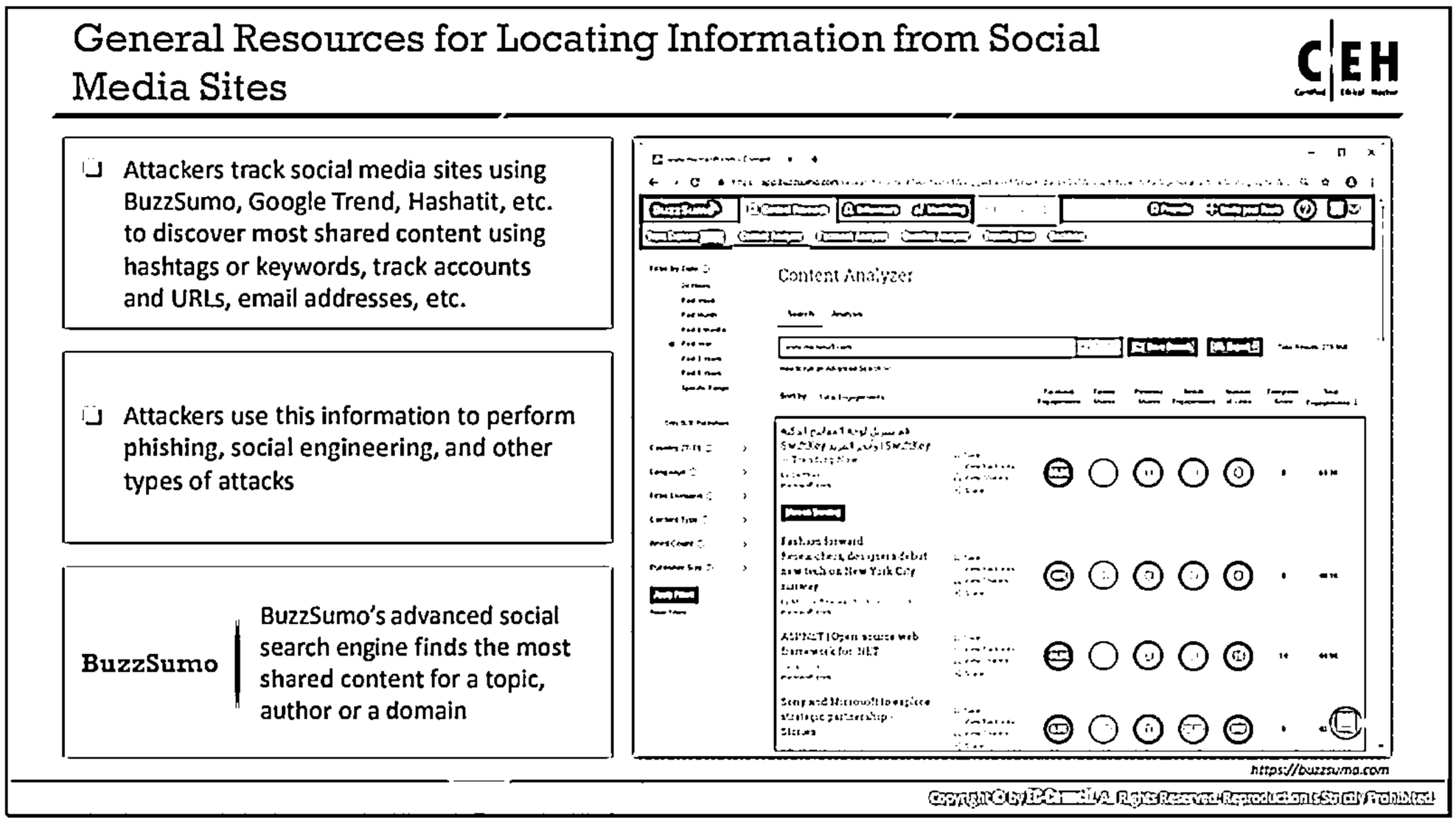
What Users Do	What Attacker Gets
Maintain profile	Contact info, location, and related information
Connect to friends, chat	Friends list, friends' info, and related information
Share photos and videos	Identity of family members, interests, and related information
Play games, join groups	Interests
Create events	Activities

Table 2.5: Activities of users on the social networking sites and the respective information

Like individuals, organizations also use social networking sites to connect with people, promote their products, and gather feedback about their products and services. The activities of an organization on social networking sites and the respective information that an attacker can collect are summarized in the table below.

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Recruitment	Platform/technology information
Background check to hire employees	Type of business

Table 2.6: Activities of the organization on the social networking sites and the respective information



General Resources for Locating Information from Social Media Sites

Several online services and resources are available to gather valuable information about a target from one or more social media sites. These services allow attackers to discover most shared content across social media sites by using hashtags or keywords, track accounts and URLs on various social media sites, obtain a target's email address, etc. This information helps attackers to perform phishing, social engineering, and other types of attacks.

Attackers use tools such as BuzzSumo, Google Trends, Hashatit, and Ubersuggest to locate information on social media sites:

- **BuzzSumo**

  Source: *https://buzzsumo.com*

  BuzzSumo's advanced social search engine finds the most shared content for a topic, author, or domain. It shows the shared activity across all the major social networks including Twitter, Facebook, LinkedIn, Google Plus, and Pinterest.

  As shown in the screenshot, attackers use BuzzSumo to track the most shared content related to the target domain and obtain details such as social media account information, URLs, and email addresses.

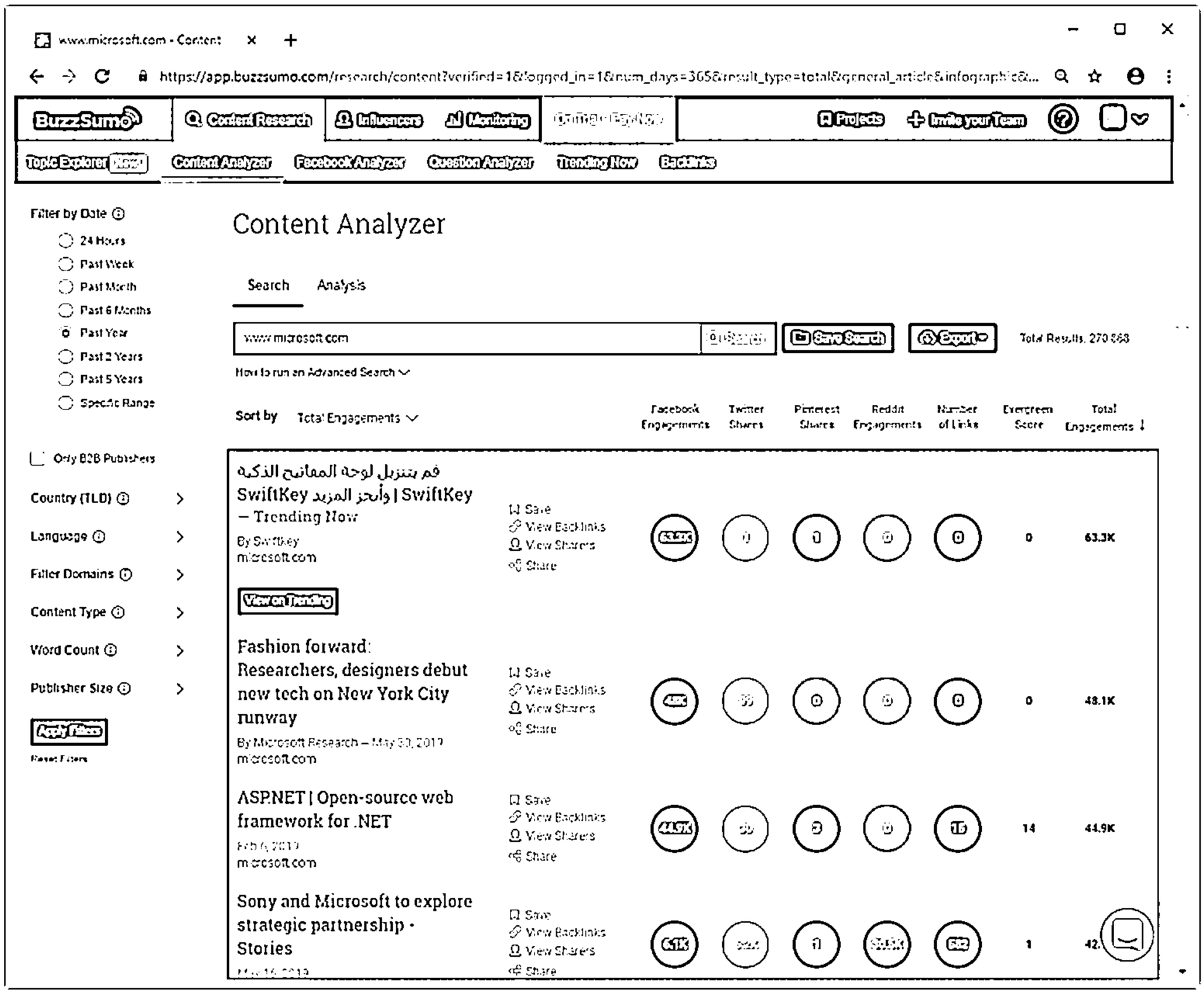
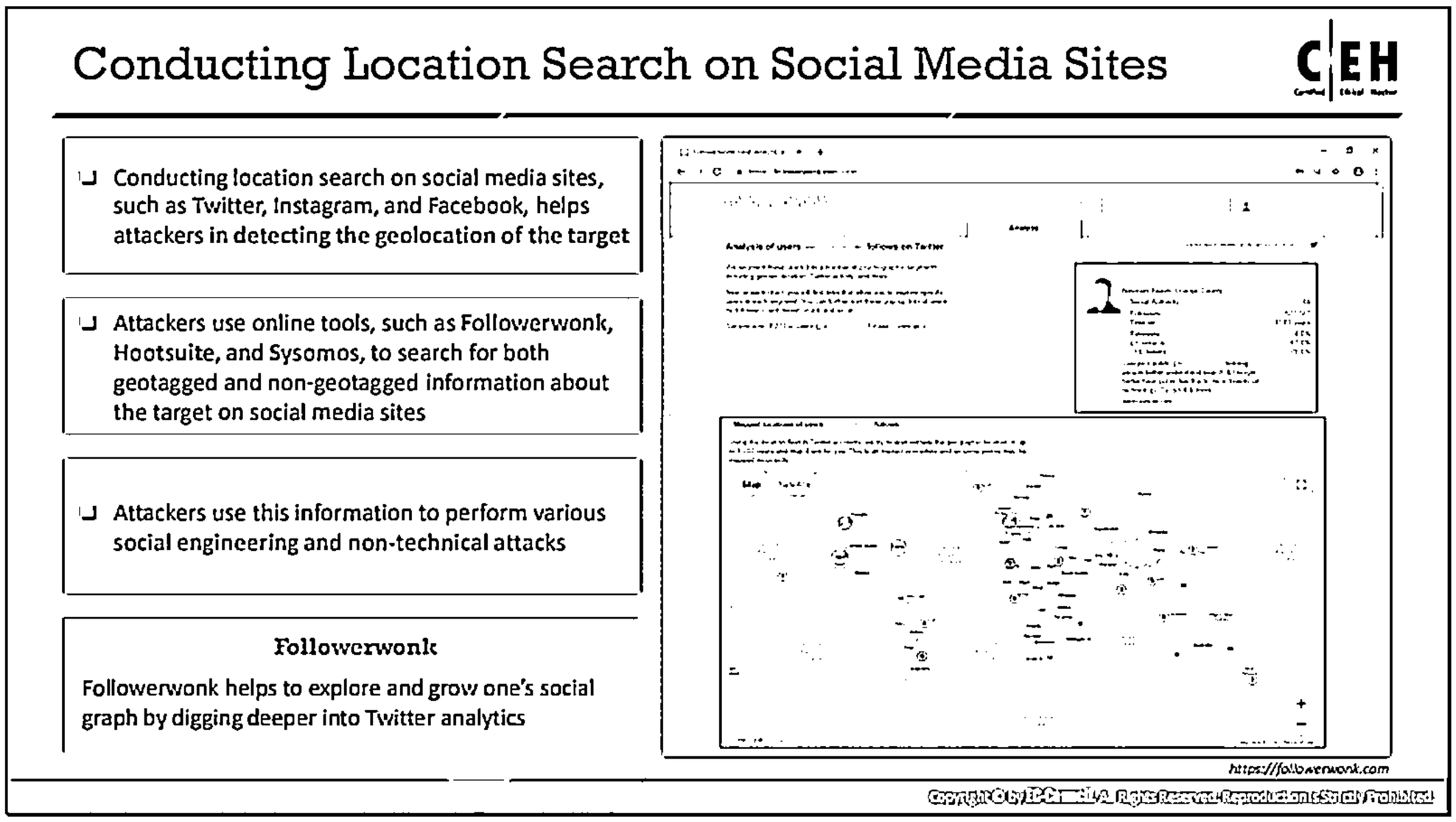


Figure 2.39: Screenshot of BuzzSumo showing the shared content



Conducting Location Search on Social Media Sites

Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on.

- **Followerwonk**

  Source: *https://followerwonk.com*

  Followerwonk helps you explore and grow your social graph: Dig deeper into Twitter analytics: Who are your followers? Where are they located? When do they tweet?

  As shown in the screenshot, attackers use Followerwonk to track the geolocation of the target Twitter users.

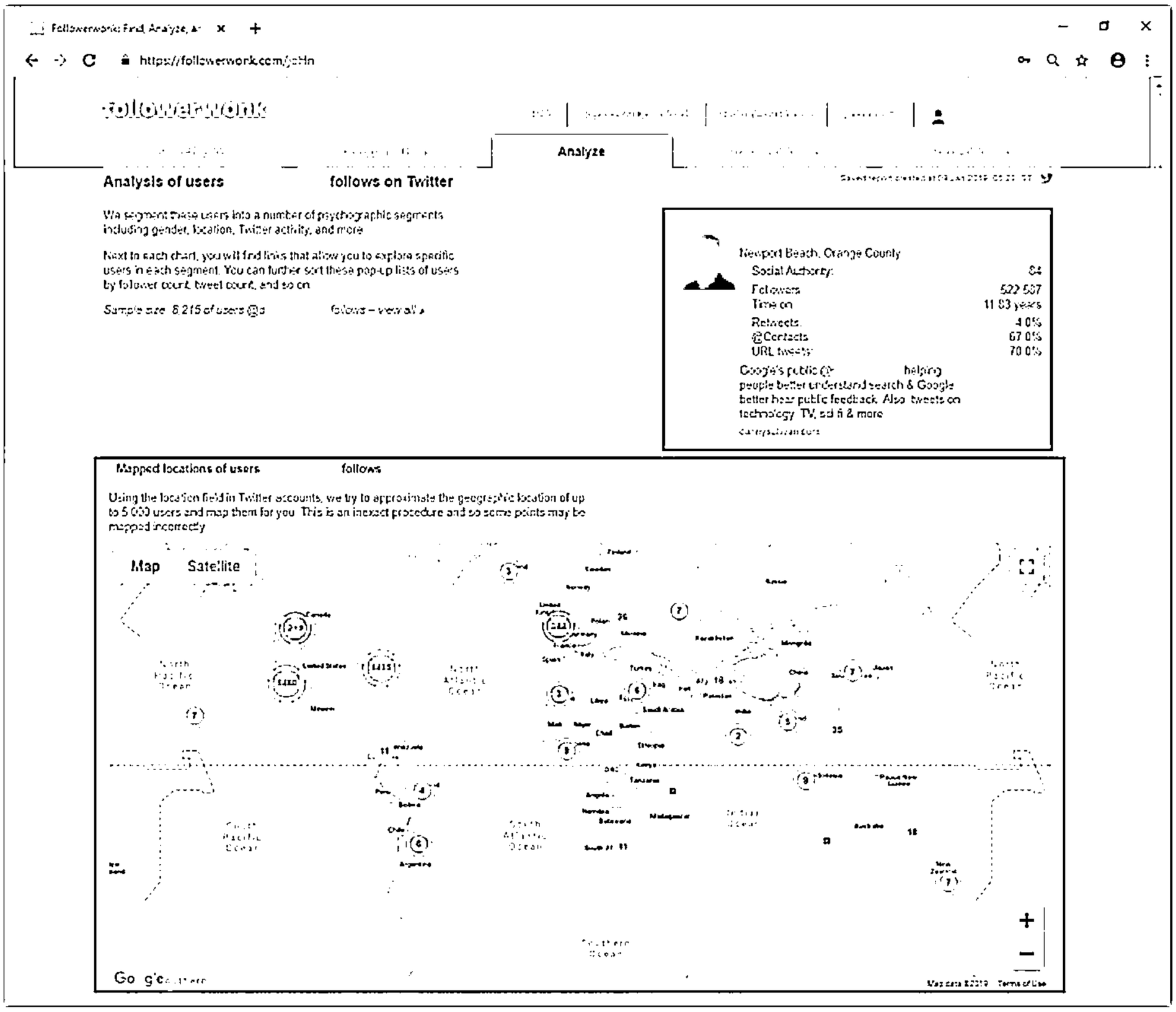
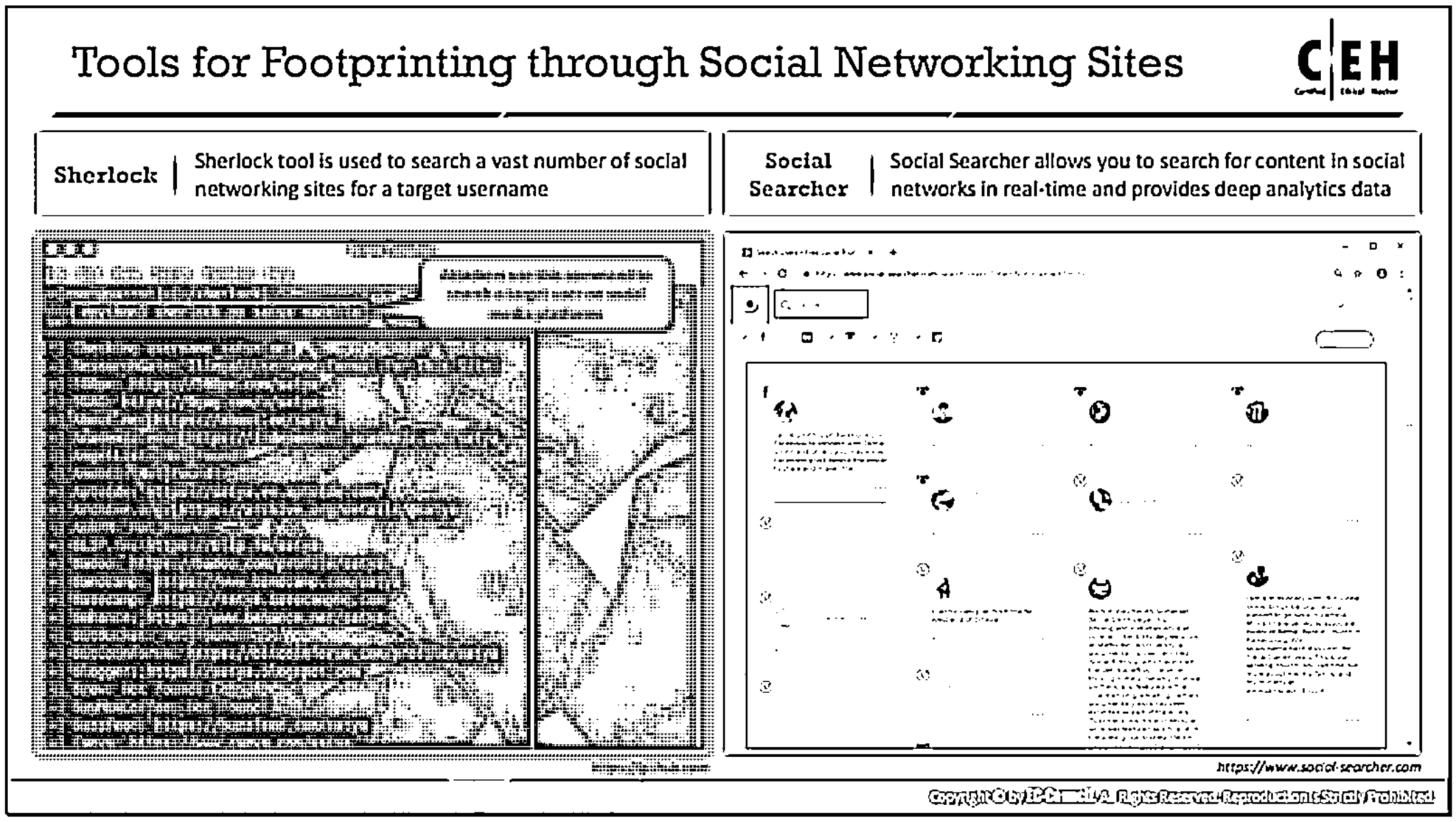


Figure 2.40: Screenshot of Followerwonk showing the geolocation



Tools for Footprinting through Social Networking Sites

Attackers use various tools such Sherlock, Social Searcher, and UserRecon to footprint social networking sites such as Twitter, Instagram, Facebook, and Pinterest to gather sensitive information about the target such as DOB, educational qualification, employment status, name of the relatives, and information about the organization that they are working for, including the business strategy, potential clients, and upcoming project plans.

- **Sherlock**

  Source: *https://github.com*

  As shown in the screenshot, attackers use Sherlock to search a vast number of social networking sites for a target username. This tool helps the attacker to locate the target user on various social networking sites along with the complete URL.

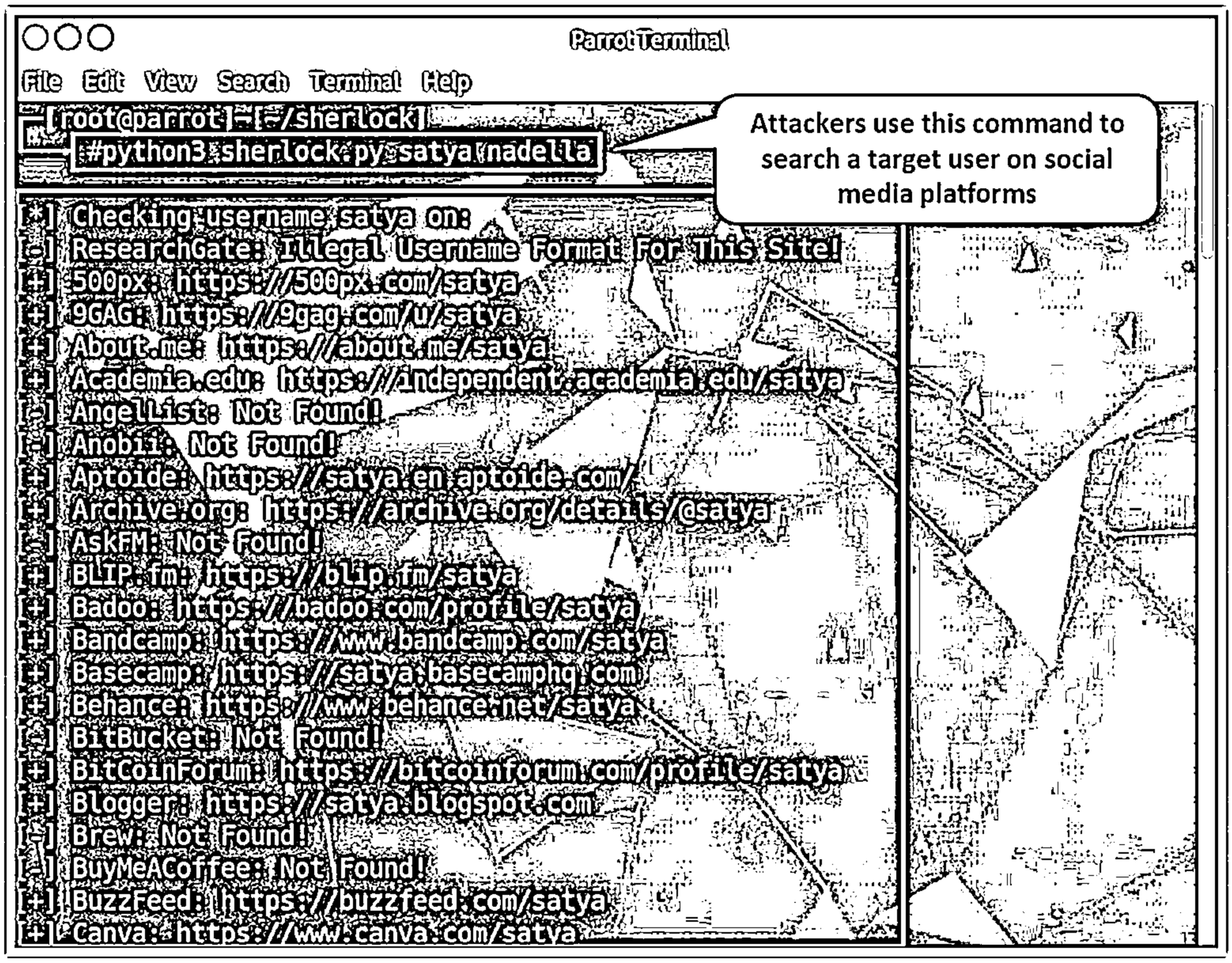


Figure 2.41: Screenshot showing the result of Sherlock tool

- **Social Searcher**

  Source: *https://www.social-searcher.com*

  Social Searcher allows attackers to search for content in social networks in real time and provides deep analytics data. Attackers use this tool to track a target user on various social networking sites and obtain information such as complete URLs to their profiles, their postings, and other personal information.

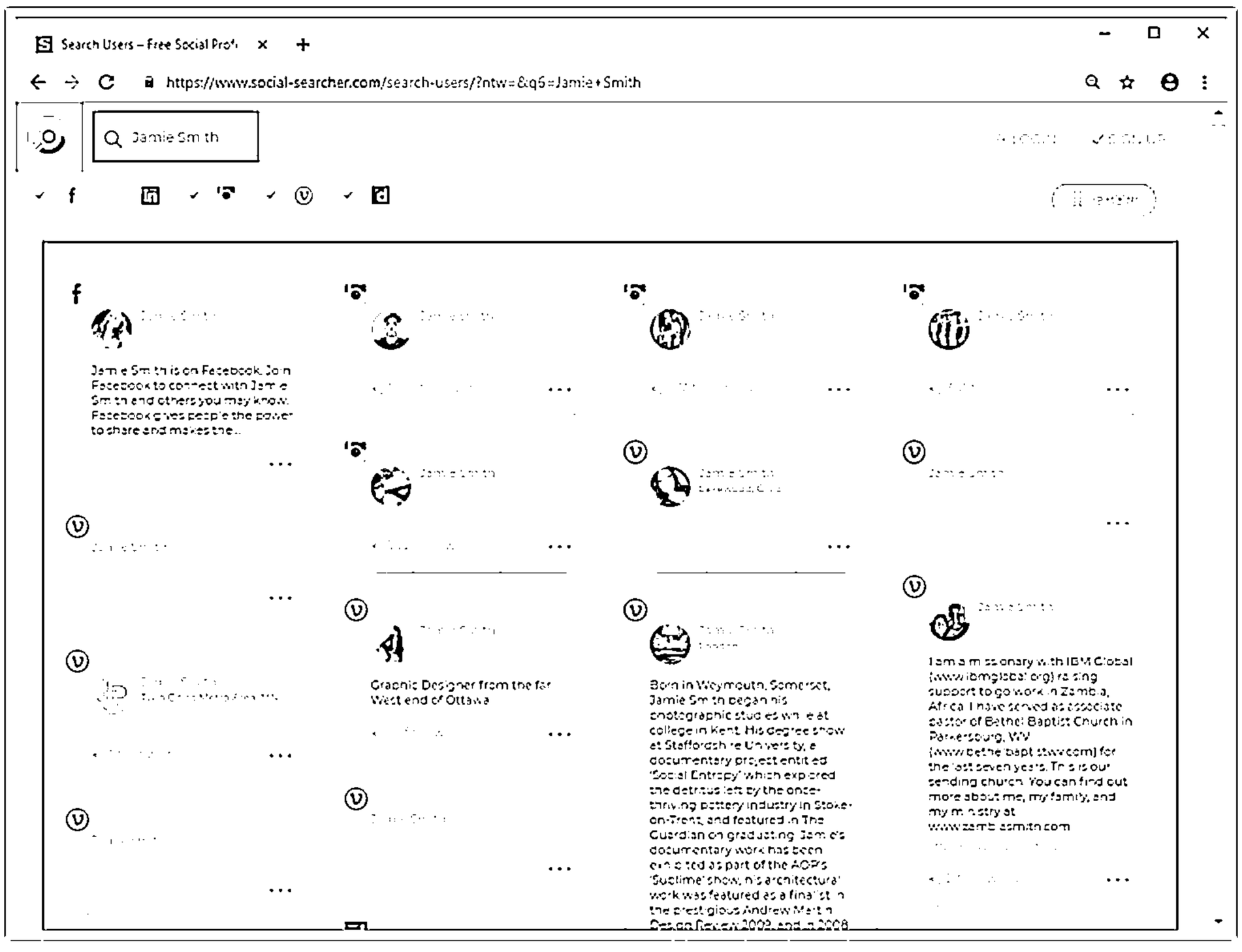


Figure 2.42: Screenshot of Social Searcher showing user content on social networks

Website Footprinting

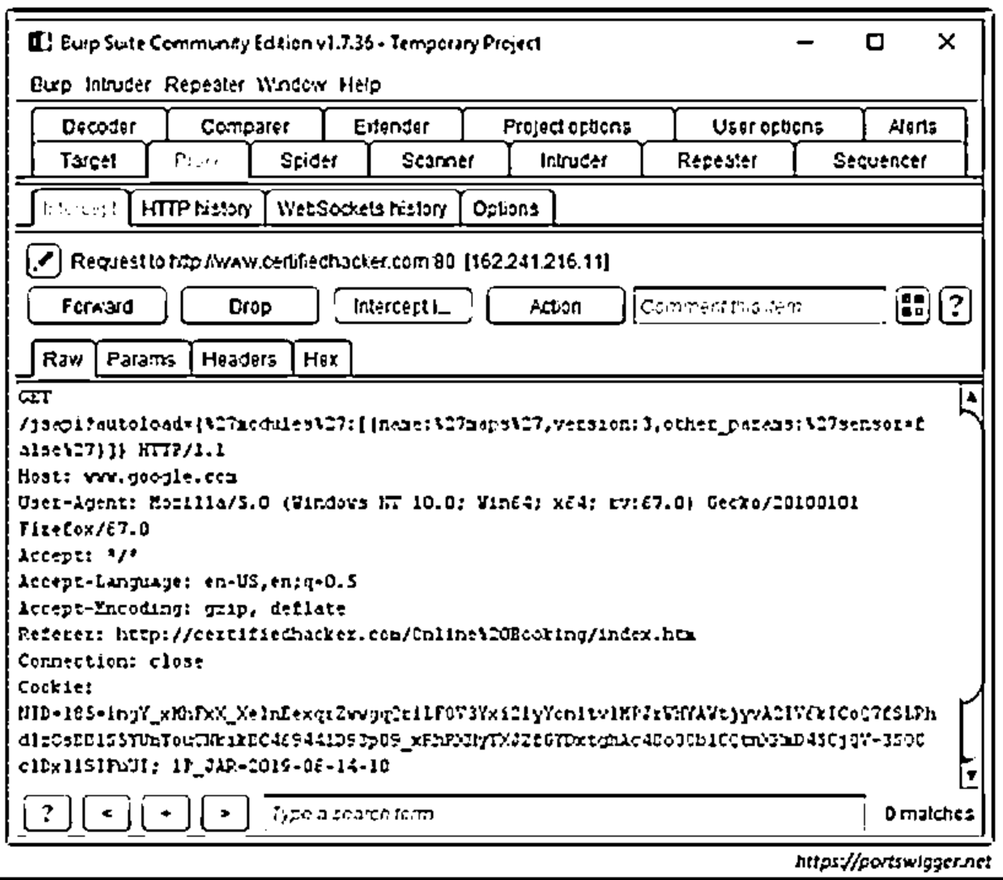
- Website footprinting refers to the monitoring and analysis of the target organization's website for information

Browsing the target website may provide the following information:

- Software used and its version
- Operating system used and its scripting platform
- Sub-directories and parameters
- Filename, path, database field name, or query
- Technologies used
- Contact and CMS details

Attackers use Burp Suite, Zaproxy, Wappalyzer, Website Informer, etc. to view headers that provide the following information:

- Connection status and content-type
- Accept-Ranges and Last-Modified
- X-Powered-By information
- Web server in use and its version



https://portswigger.net

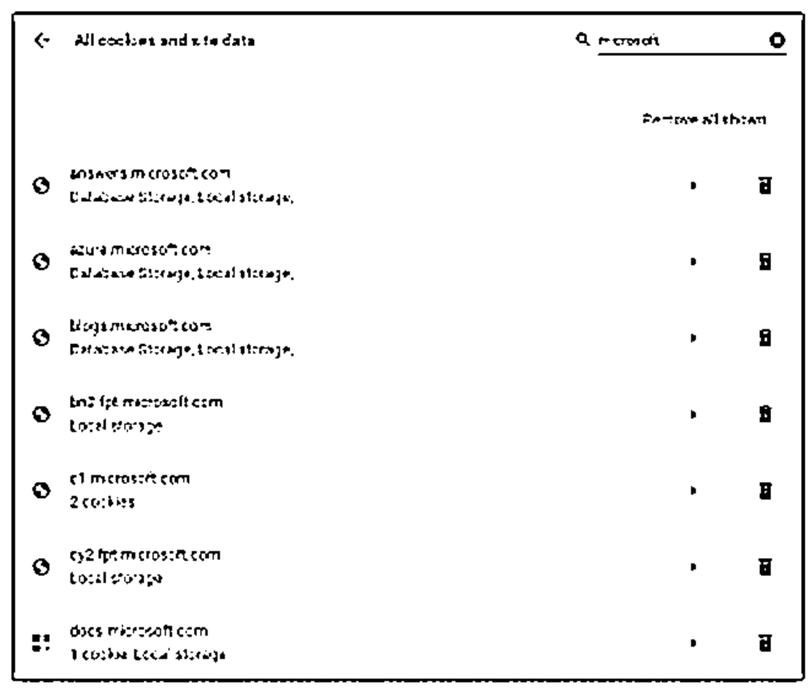
Website Footprinting (Cont'd)

Examining the HTML source code may provide

- Comments present in the source code
- Contact details of the web developer or admin
- File system structure and script type

Examining cookies may provide

- Software in use and its behavior
- Scripting platforms used



Website Footprinting

So far, we have discussed footprinting through search engines, web services, and social networking sites. Hereafter, we will discuss website footprinting. An organization's website is the first place to get sensitive information such as names and contact details of the leaders of the organization, upcoming project details, and so on.

This section covers the website footprinting concept, mirroring websites, extracting website information and links, gathering wordlists, extracting metadata of public documents, and monitoring web updates and website traffic.

Website footprinting refers to monitoring and analyzing a target organization's website for information. An attacker can build a detailed map of a website's structure and architecture without triggering the IDS or arousing the suspicion of any system administrator. Attackers use sophisticated footprinting tools or the basic tools that come with the operating system, such as Telnet, or a browser.

The Netcraft tool can gather website information such as IP address, registered name and address of the domain owner, domain name, host of the site, and OS details. However, the tool may not give all these details for every site. In such cases, the attacker can browse the target website.

Browsing the target website will typically provide the following information:

- **Software used and its version**: An attacker can easily find the software and version in use on an off-the-shelf software-based website.
- **Operating system used**: Usually, the operating system in use can also be determined.
- **Sub-directories and parameters**: Searches can reveal the sub-directories and parameters by making a note of the URLs while browsing the target website.
- **Filename, path, database field name, or query**: The attacker will often carefully analyze anything after a query that looks like a filename, path, database field name, or query to check whether it offers opportunities for SQL injection.
- **Scripting platform**: With the help of script filename extensions such as .php, .asp, or .jsp, one can easily determine the scripting platform that the target website is using.
- **Technologies Used**: By inspecting the URLs of the target website, one can easily determine the technologies (.NET, J2EE, PHP, etc.) used to build that website.
- **Contact details and CMS details**: The contact pages usually offer details such as names, phone numbers, email addresses, and locations of admin or support personnel. An attacker can use these details to perform a social engineering attack. CMS software allows URL rewriting to disguise the script filename extensions if the attacker is willing to devote additional effort toward determining the scripting platform.

Attackers use Burp Suite, Zaproxy, WhatWeb, BuiltWith, Wappalyzer, and Website Informer to view headers that provide:

- Connection status and content type
- Accept-Ranges and Last-Modified information
- X-Powered-By information
- Web server in use and its version

Burp Suite

Source: *https://portswigger.net*

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities.

Burp Proxy allows attackers to intercept all requests and responses between the browser and the target web application and obtain information such as web server used, its version, and web-application-related vulnerabilities.

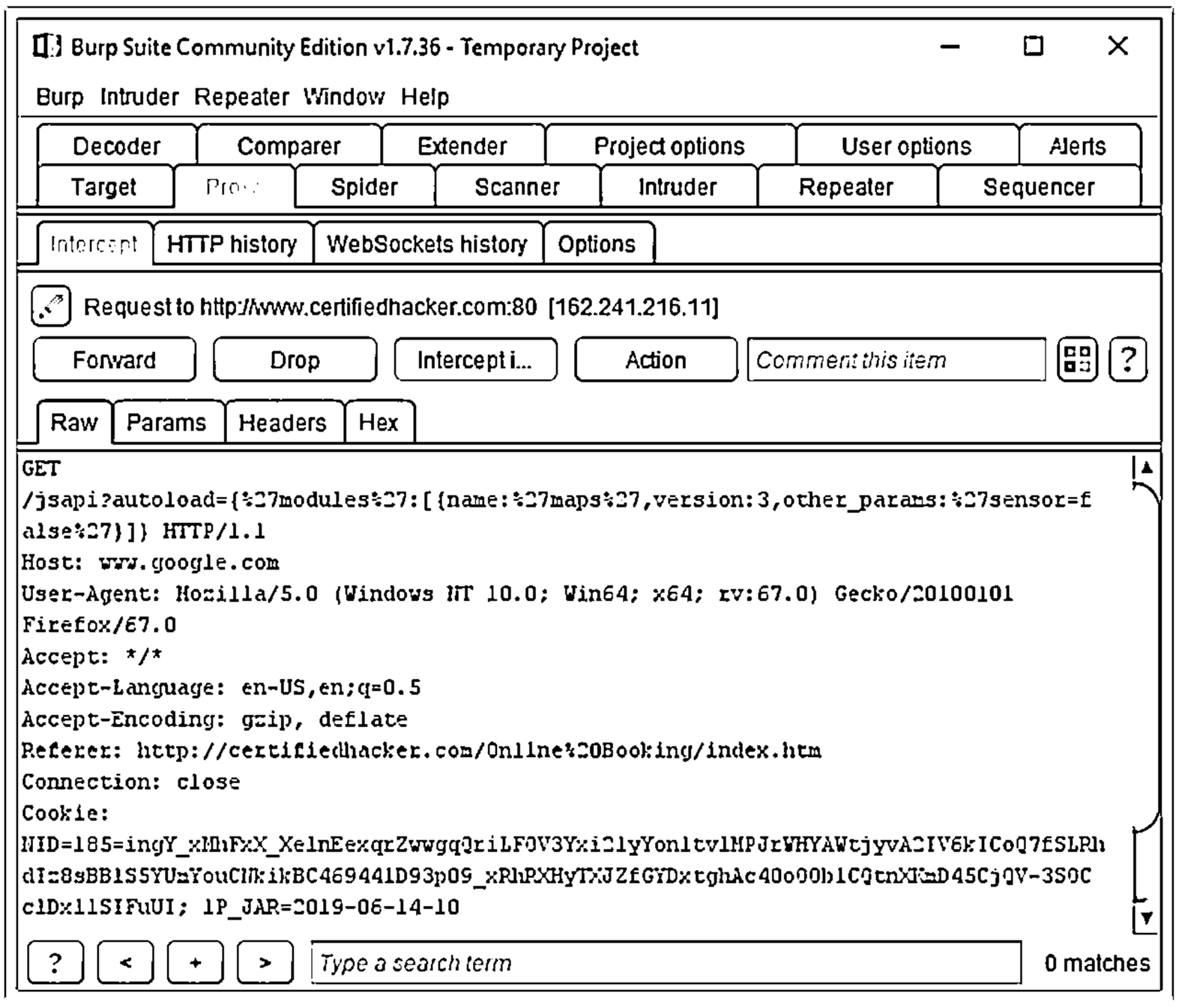


Figure 2.43: Screenshot of Burp Suite

Website footprinting can be performed by examining HTML source code and cookies.

- **Examining the HTML source code**

  Attackers can gather sensitive information by examining the HTML source code and following the comments that are inserted manually or those that the CMS system creates. The comments may provide clues as to what is running in the background. They may even provide contact details of the web developer or administrator.

  Observe all the links and image tags to map the file system structure. This will reveal the existence of hidden directories and files. Enter fake data to determine how the script works. It is sometimes possible to edit the source code.

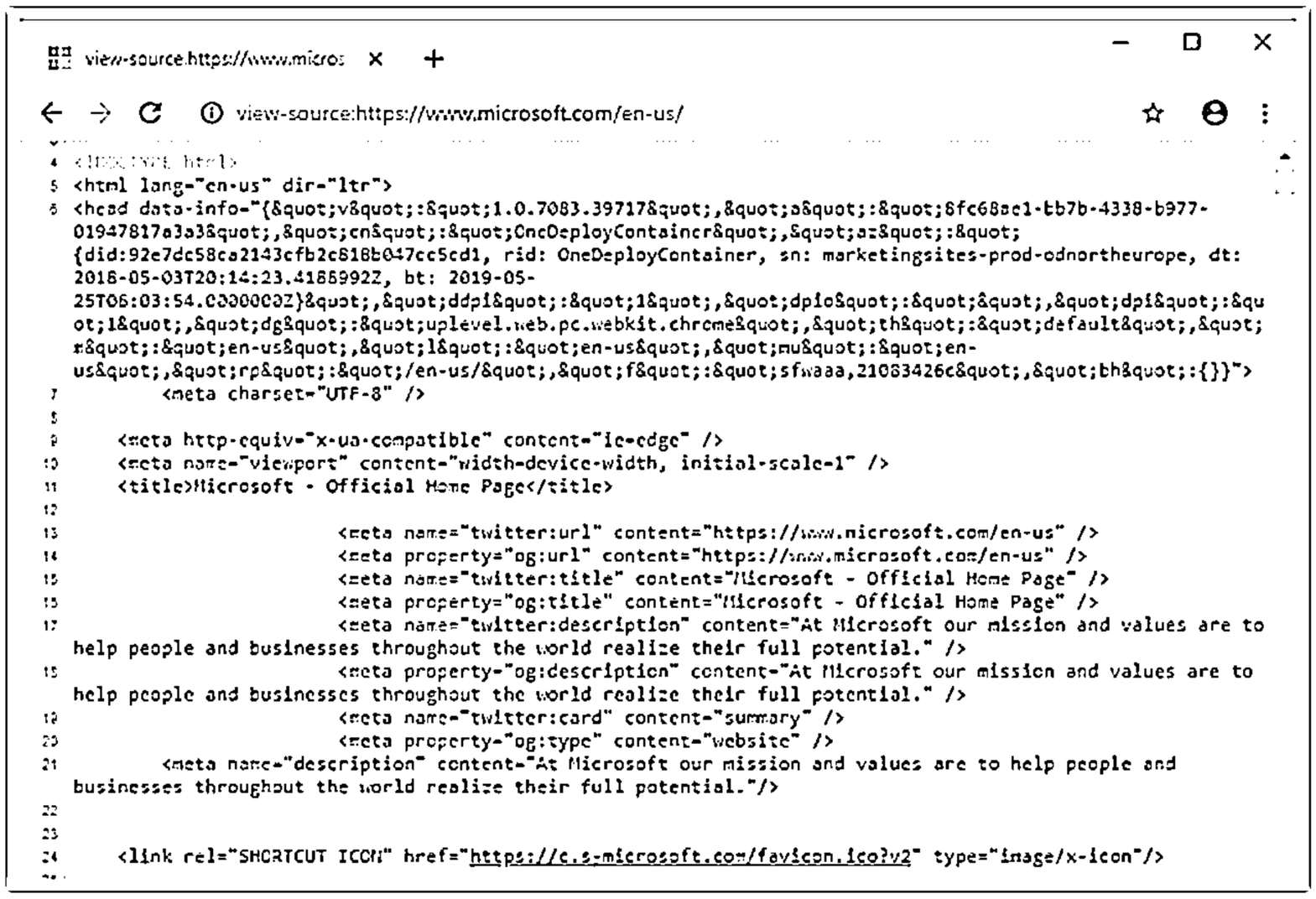


Figure 2.44: Screenshot showing HTML source code

- **Examining Cookies**

  To determine the software running and its behavior, one can examine cookies set by the server. Identify the scripting platforms by observing sessions and other supporting cookies. The information about cookie name, value, and domain size can also be extracted.

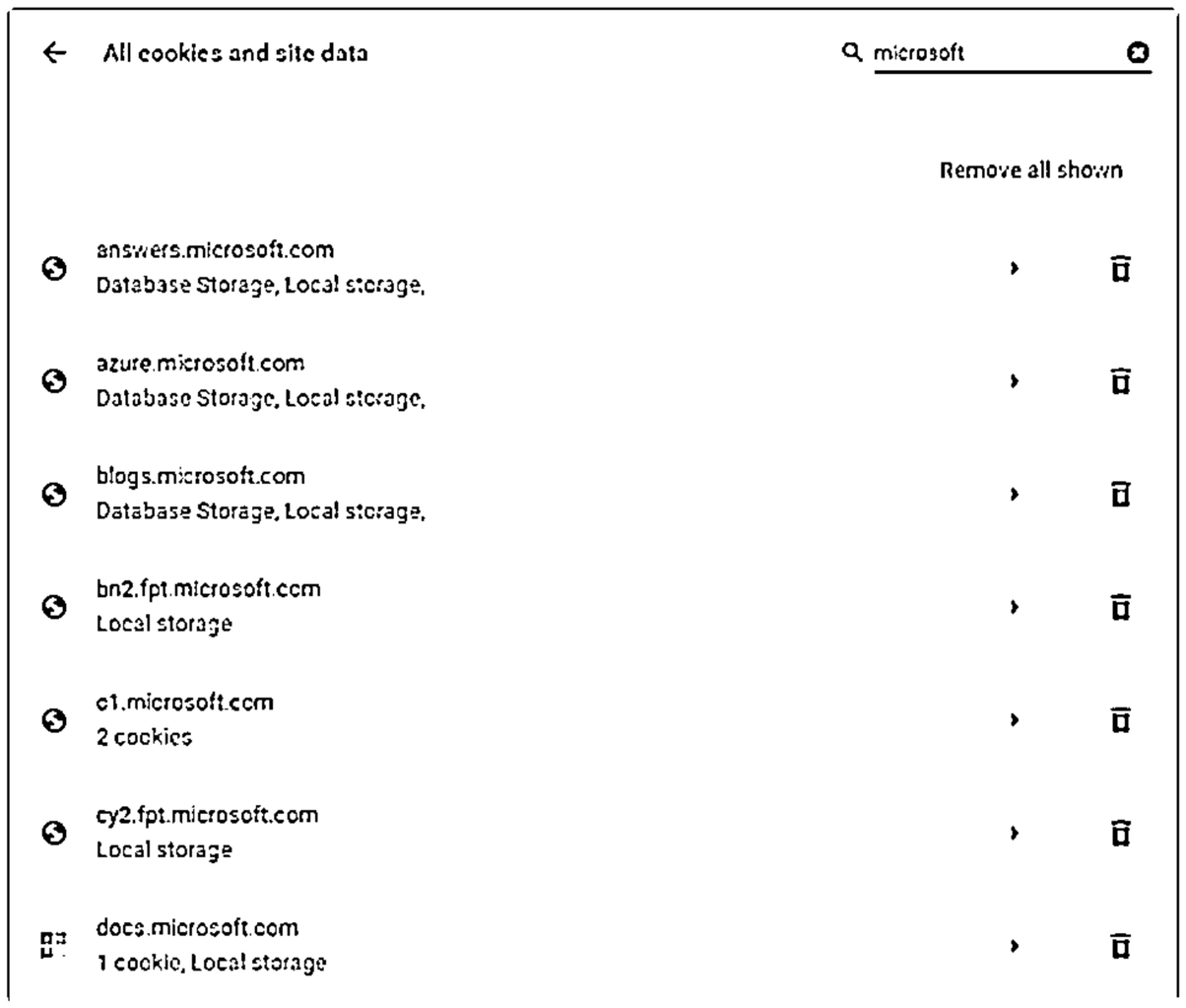
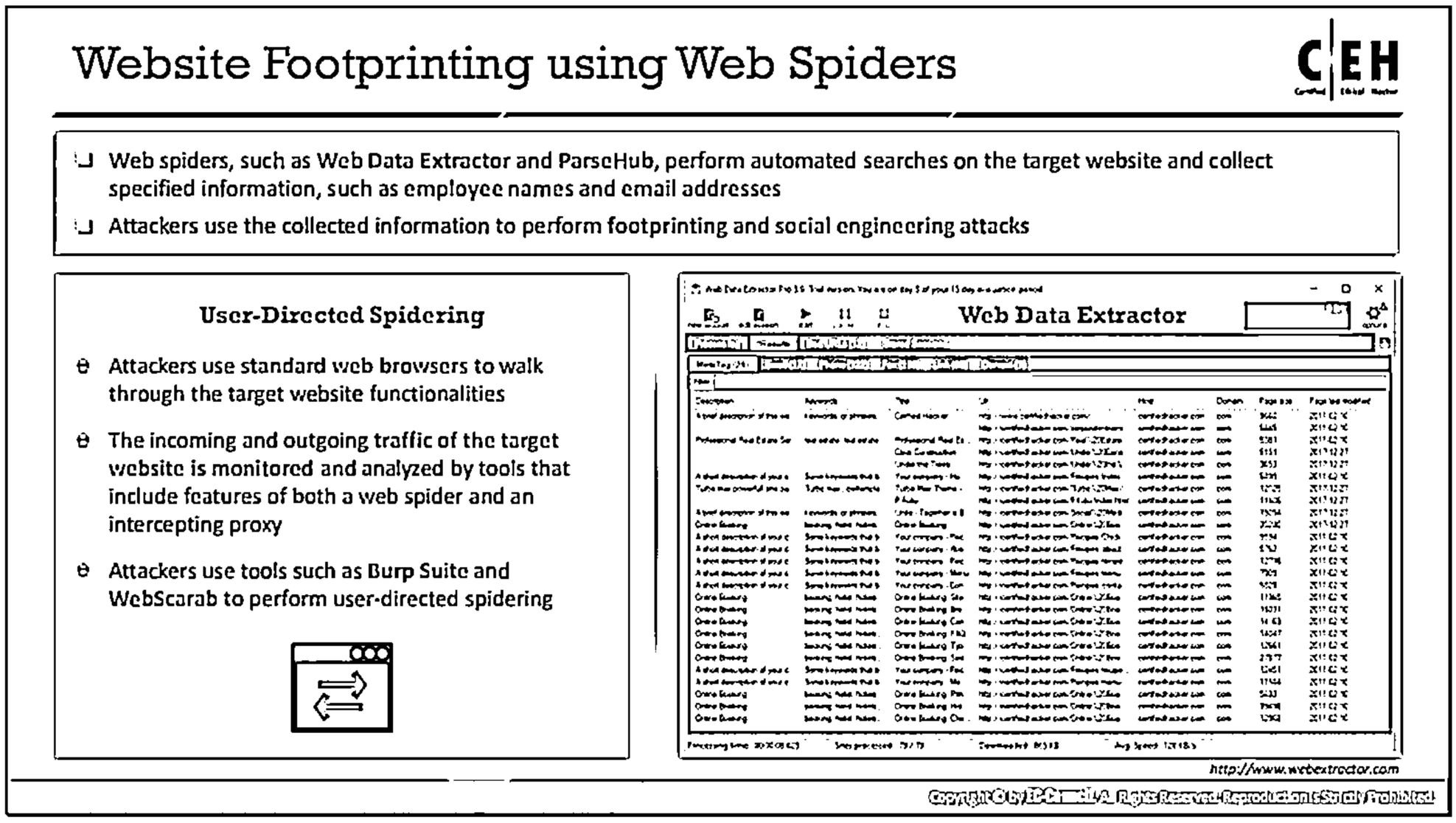


Figure 2.45: Screenshot showing cookies



Website Footprinting using Web Spiders

A web spider (also known as web crawler or web robot) is a program or automated script that browses websites in a methodical manner to collect specific information such as employee names and email addresses. Attackers then use the collected information to perform footprinting and social engineering attacks. Web spidering fails if the target website has the robots.txt file in its root directory with a listing of directories to prevent crawling.

Attackers can uncover all the files and web pages on the target website by simply feeding the web spider with a URL. Then, the web spider sends hundreds of requests to the target website and analyzes the HTML code of all the received responses for identifying additional links. If any new links are found, then the spider adds them to the target list and starts spidering and analyzing the newly discovered links. This method helps attackers to not only detect exploitable web-attack surfaces but also to find all the directories, web pages, and files that make up the target website.

User-Directed Spidering

Attackers, in some cases, use a more sophisticated technique for spidering the target website instead of using automated tools. They use standard web browsers to walk through the target website in an attempt to navigate through all the functionalities provided by the web application. While performing this task, the resulting incoming and outgoing traffic of the website is monitored and analyzed by the tools that include features of both a web spider and an intercepting proxy. Further, these tools create a map of the web application consisting of all the URLs visited by the browser. It also analyzes the responses of the application and updates the map with the discovered content and its functionalities. Attackers use tools such as Burp Suite and WebScarab to perform user-directed spidering.

Web spidering tools such as Web Data Extractor, ParseHub, and SpiderFoot can collect sensitive information from the target website.

- **Web Data Extractor**

  Source: *http://www.webextractor.com*

  Web Data Extractor automatically extracts specific information from web pages. It extracts targeted contact data (email, phone, and fax) from the website, extracts the URL and meta tags (title, description, keyword) for website promotion, searches directory creation, performs web research, and so on.

  As shown in the screenshot, attackers use Web Data Extractor to automatically gather critical information such as lists of meta tags, e-mail addresses, and phone and fax numbers from the target website.

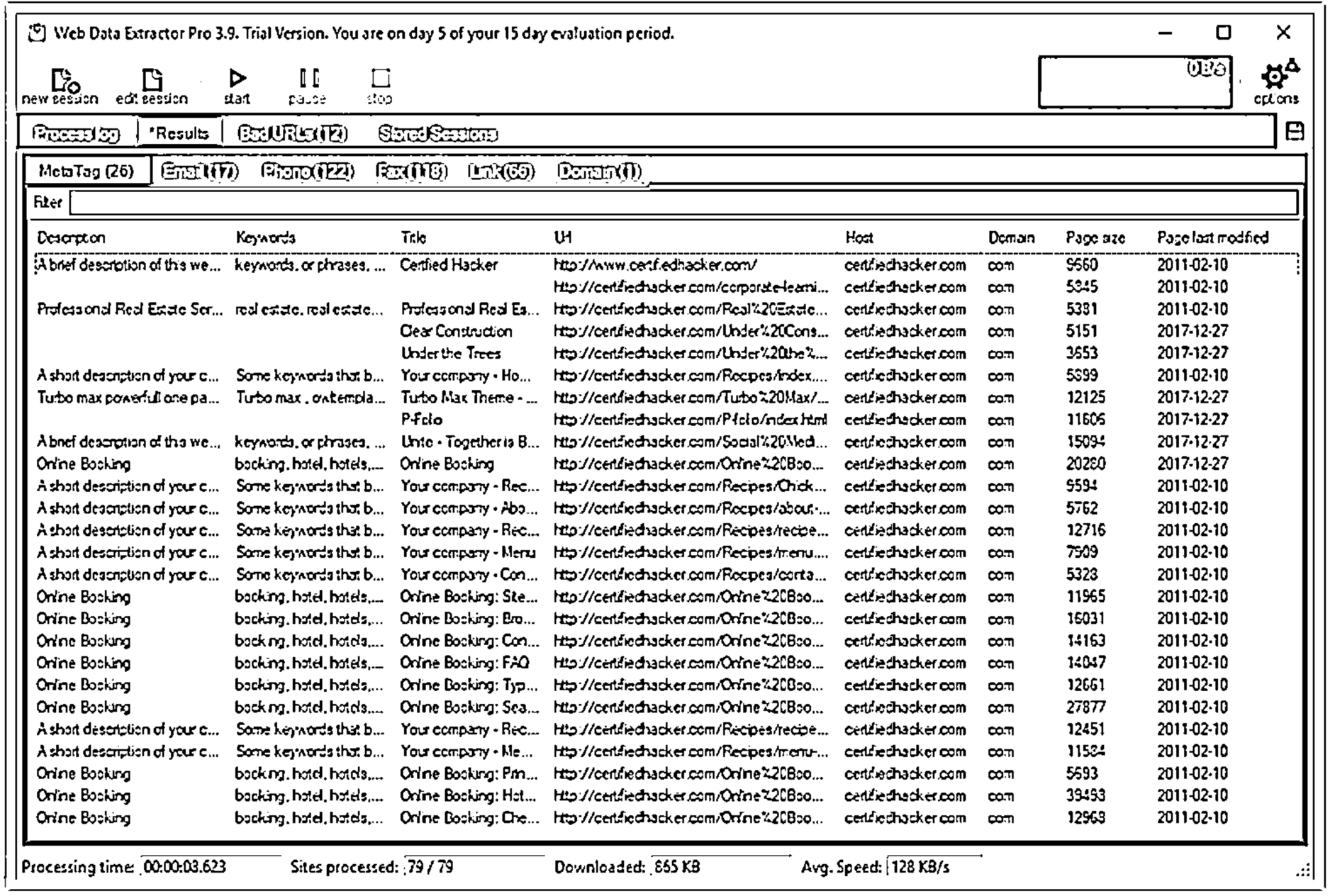
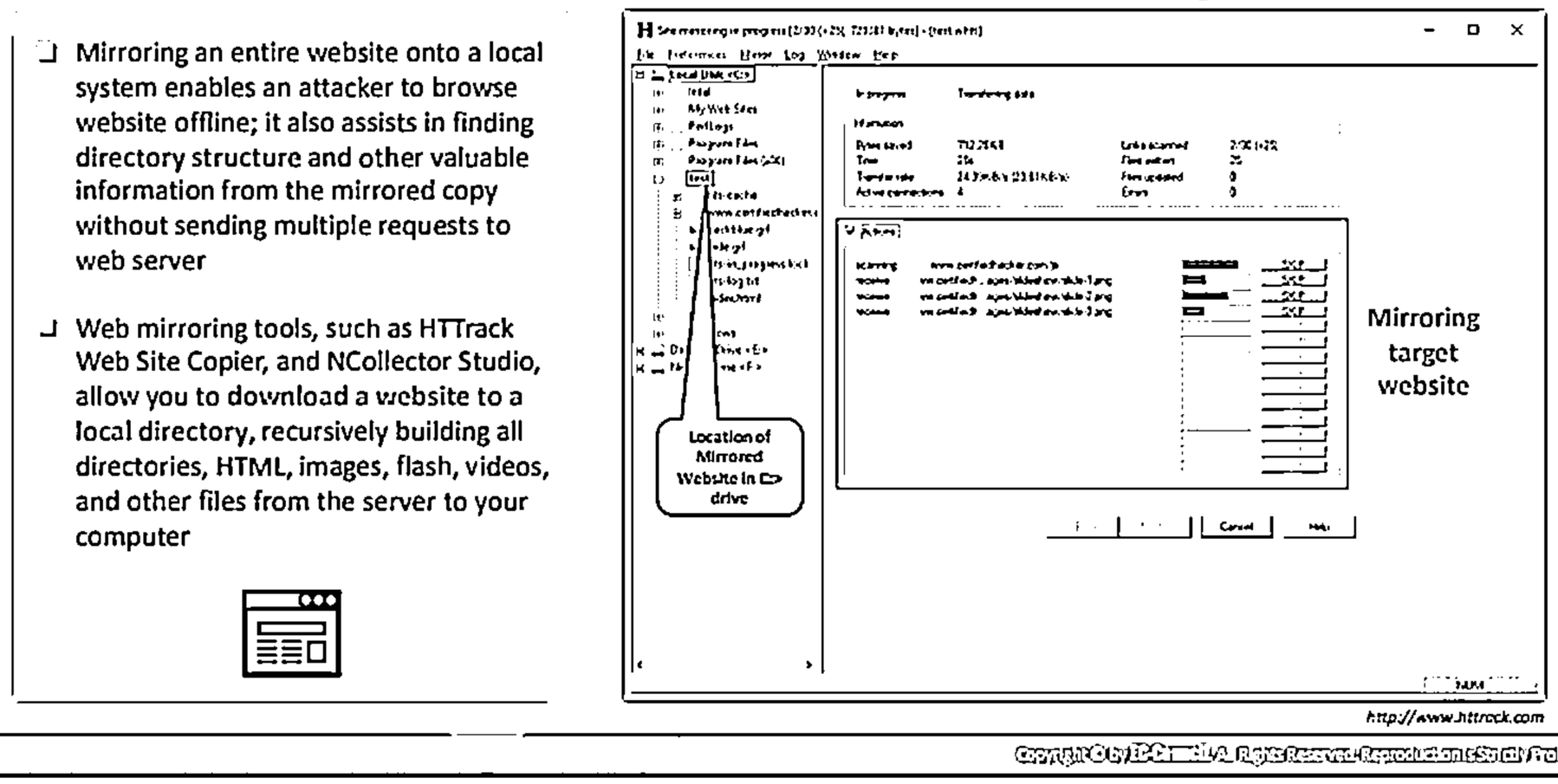


Figure 2.46: Screenshot of Web Data Extractor

Mirroring Entire Website

- Mirroring an entire website onto a local system enables an attacker to browse website offline; it also assists in finding directory structure and other valuable information from the mirrored copy without sending multiple requests to web server
- Web mirroring tools, such as HTTrack Web Site Copier, and NCollector Studio, allow you to download a website to a local directory, recursively building all directories, HTML, images, flash, videos, and other files from the server to your computer



Mirroring Entire Website

Website mirroring is the process of creating a replica or clone of the original website. Users can duplicate websites using mirroring tools such as HTTrack Web Site Copier and NCollector Studio. These tools download a website to a local directory and recursively build all the directories including HTML, images, flash, videos, and other files from the webserver on another computer.

Website mirroring has the following benefits:

- It is helpful for offline site browsing
- It enables an attacker to spend more time in viewing and analyzing the website for vulnerabilities and loopholes
- It helps in finding the directory structure and other valuable information from the mirrored copy without multiple requests to the webserver

Attackers can use this information to perform various web application attacks on the target organization's website.

Website Mirroring Tool: HTTrack Web Site Copier

Source: *http://www.httrack.com*

HTTrack is an offline browser utility. It downloads a website from the Internet to a local directory and recursively builds all the directories including HTML, images, and other files from the web server on another computer.

As shown in the screenshot, attackers use HTTrack to mirror the entire website of the target organization, store it in the local system drive, and browse the local website to identify possible exploits and vulnerabilities.

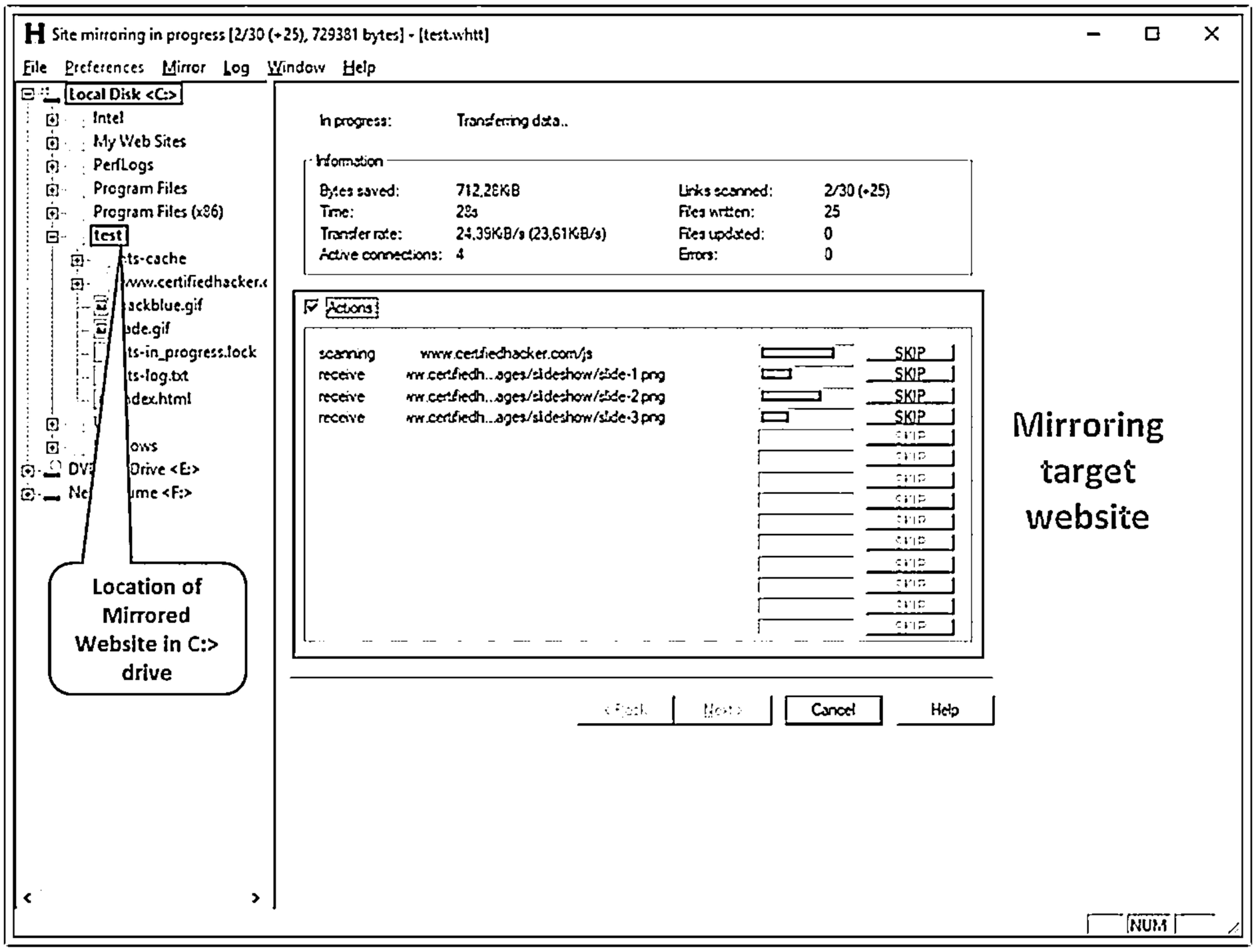
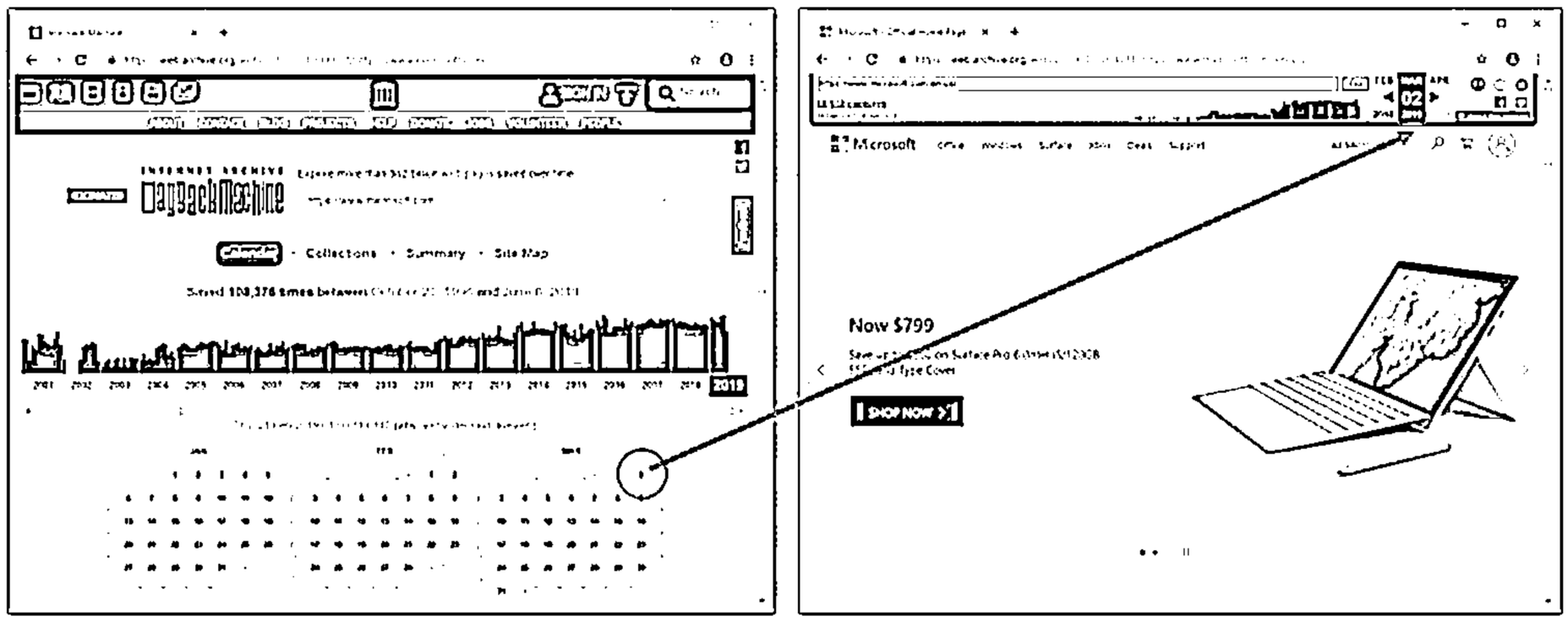


Figure 2.47: Screenshot of HTTrack Web Site Copier

Extracting Website Information from https://archive.org

- Internet Archive's Wayback Machine allows one to visit archived versions of websites



Extracting Website Information from https://archive.org

Source: *https://archive.org*

Archive is an Internet Archive Wayback Machine that explores archived versions of websites. Such exploration allows an attacker to gather information on an organization's web pages since its creation. As the website ***https://archive.org*** keeps track of web pages from the time of their creation, an attacker can retrieve even information removed from the target website, such as web pages, audio files, video files, images, text, and software programs. Attackers use this information to perform phishing and other types of web application attacks on the target organization.

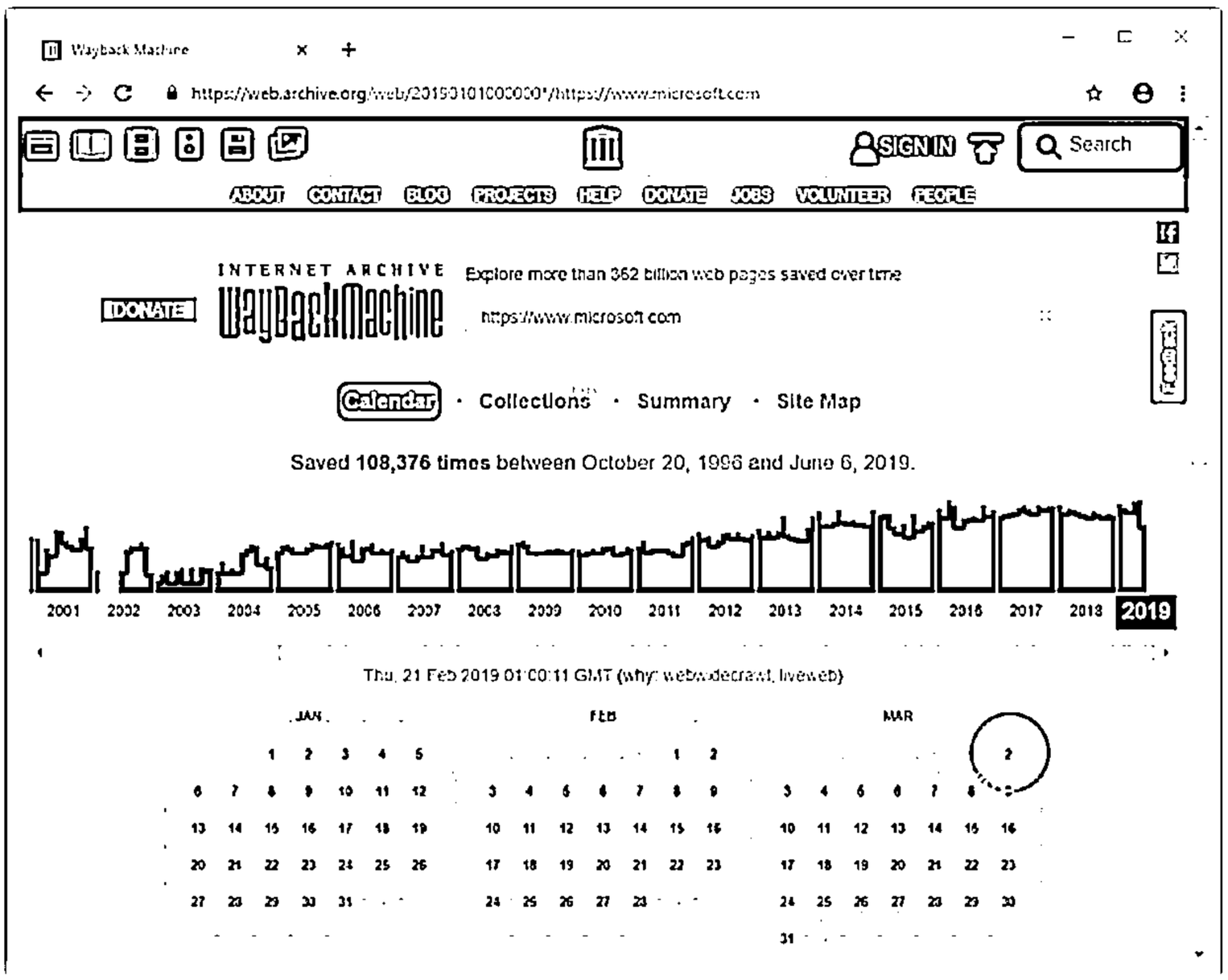


Figure 2.48: Screenshot of Archive showing archived versions of microsoft.com

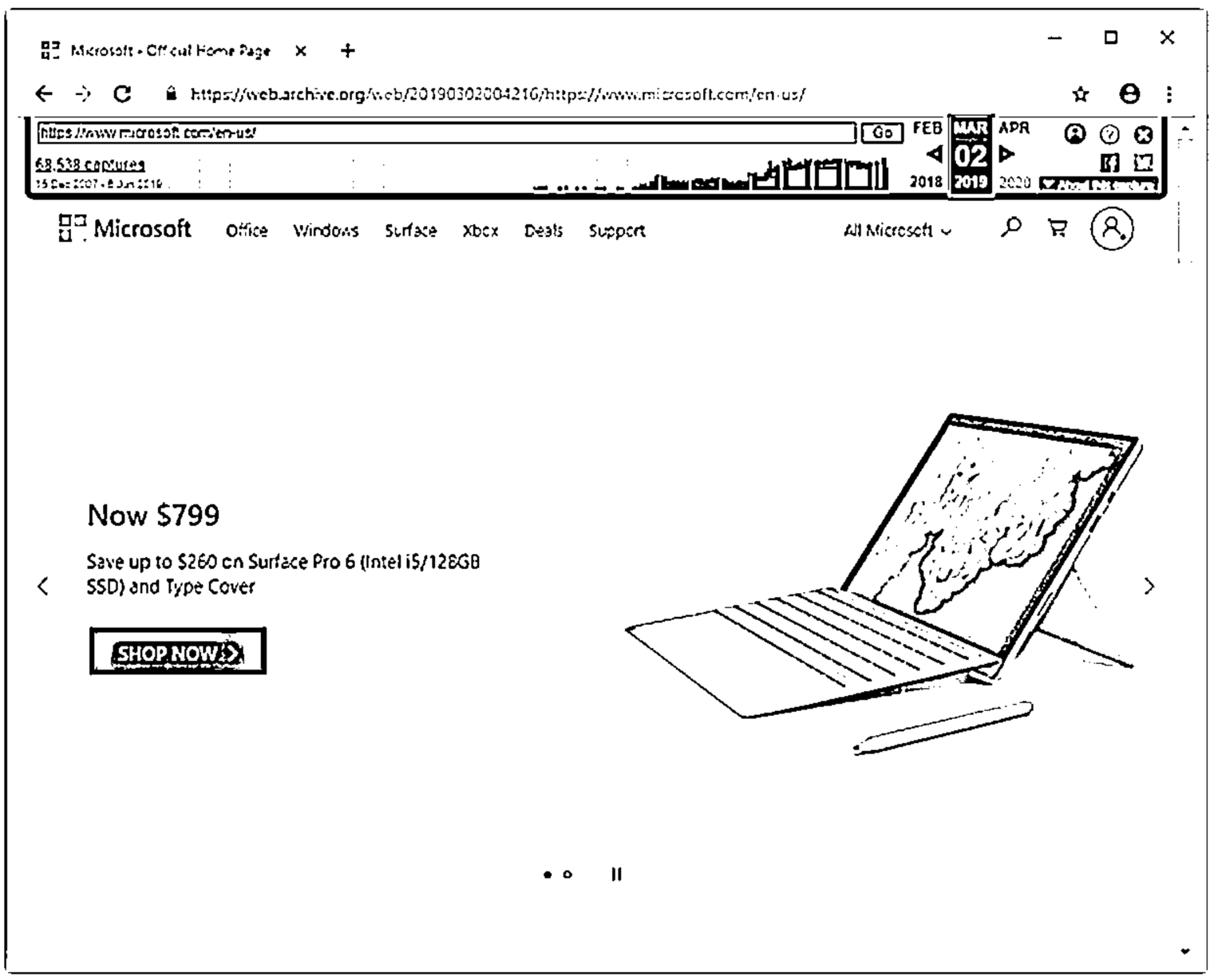
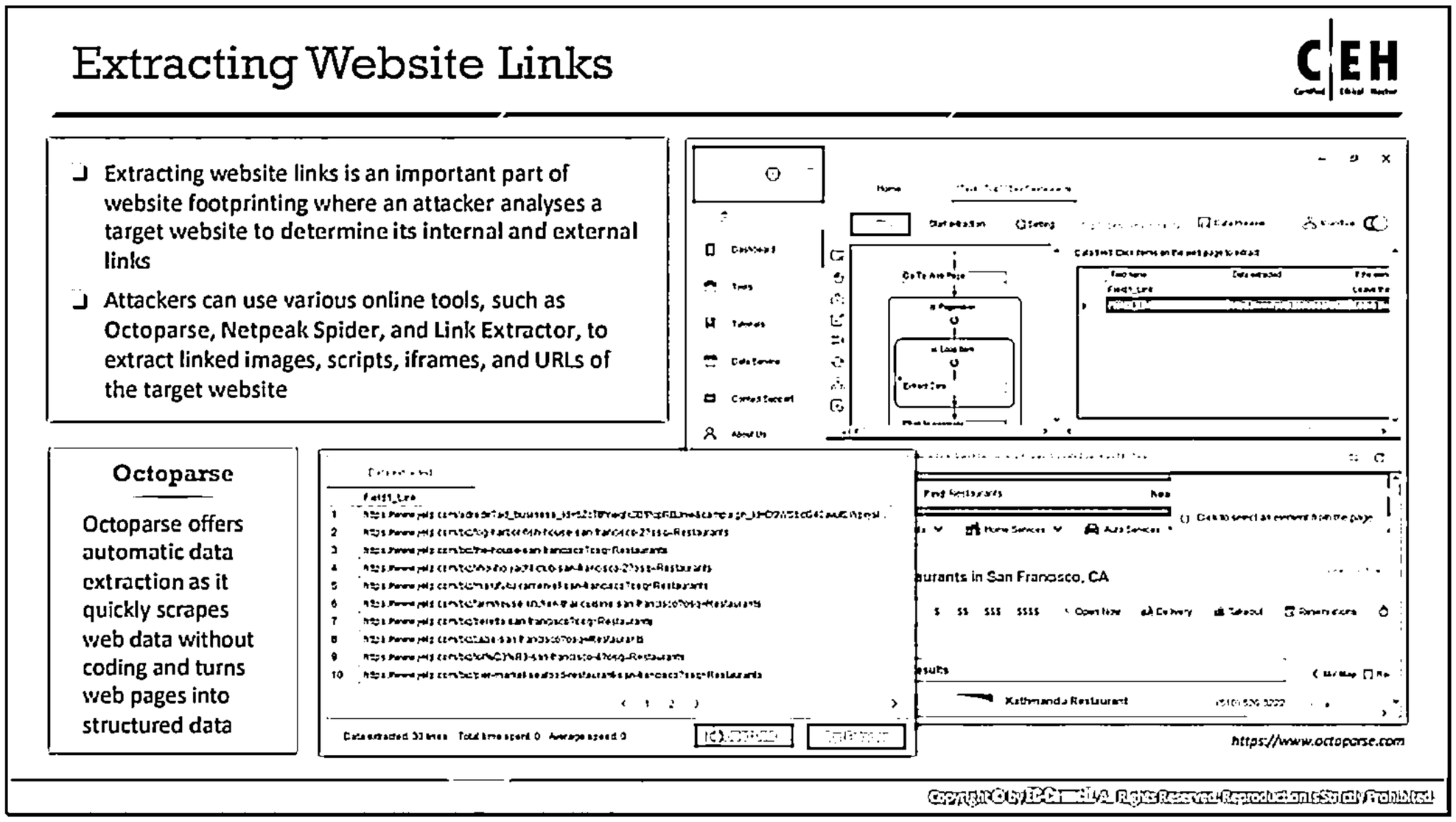


Figure 2.49: Screenshot of Archive showing archived web pages of microsoft.com



Extracting Website Links

Extracting website links is an important part of website footprinting, where an attacker analyzes a target website to determine its internal and external links. Using the gathered information, an attacker can find out the applications, web technologies, and other related websites that are linked to the target website. Further, dumping the obtained links can reveal important connections and extract URLs of other resources such as JavaScript and CSS files. This information helps attackers to identify vulnerabilities in the target website and find ways to exploit the web application.

Attackers can use various online tools or services such as Octoparse, Netpeak Spider, and Link Extractor to extract linked images, scripts, iframes, URLs, etc., of the target website. Using these tools, an attacker can also extract backlinks to a target website, which can provide important and useful information about the target to perform further exploitation.

- **Octoparse**

  Source: *https://www.octoparse.com*

  Octoparse offers automatic data extraction, as it quickly scrapes web data without coding and turns web pages into structured data. As shown in the screenshot, attackers use Octoparse to capture information from webpages, such as text, links, image URLs, or html code.

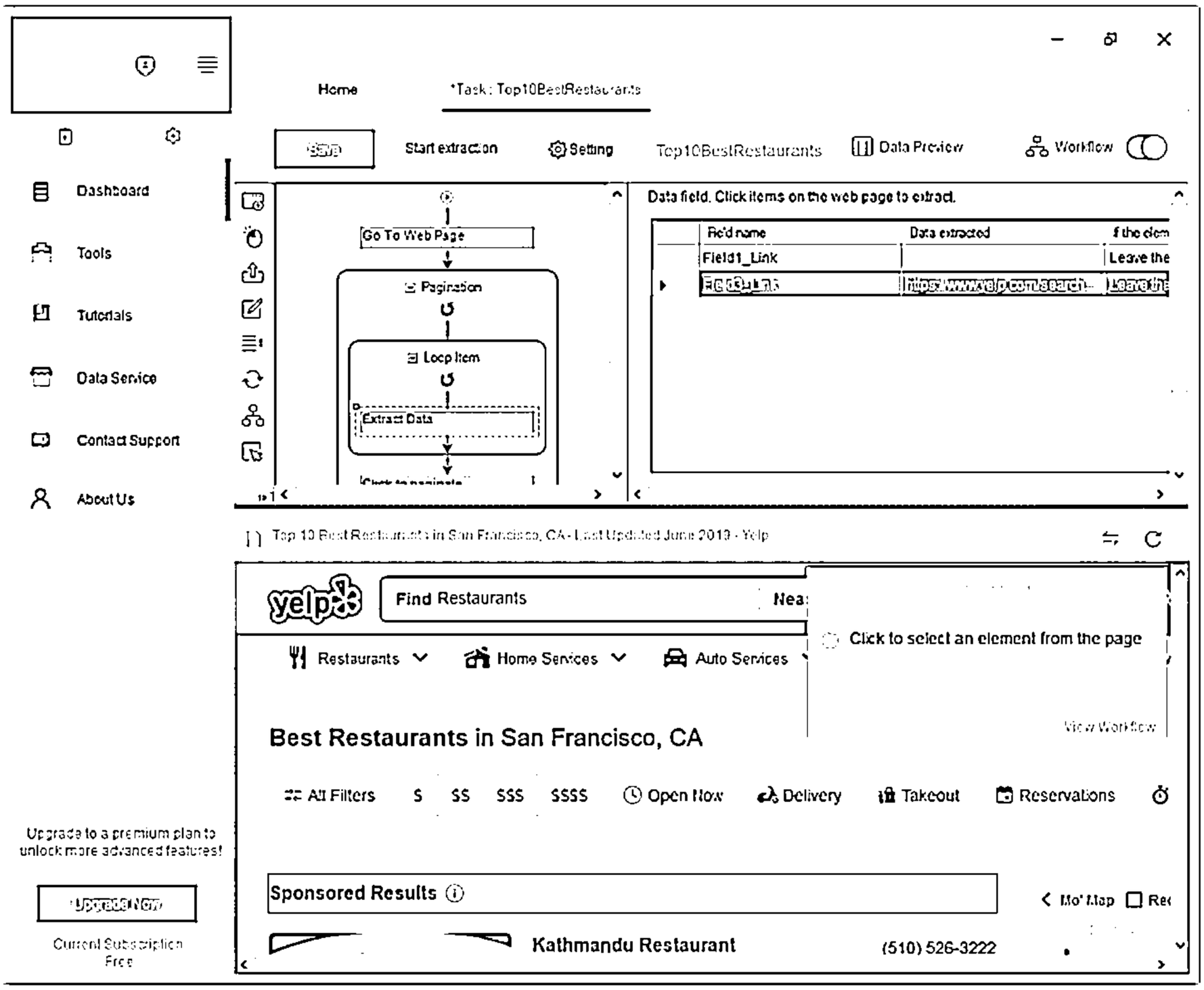


Figure 2.50: Screenshot of Octoparse

	Field1_Link
1	https://www.yelp.com/adredir?ad_business_id=5ZcTtPneqlk3BfPcpRBJnw&campaign_id=D9WSbdG40avufEWpxysl...
2	https://www.yelp.com/biz/fog-harbor-fish-house-san-francisco-2?osq=Restaurants
3	https://www.yelp.com/biz/the-house-san-francisco?osq=Restaurants
4	https://www.yelp.com/biz/ilhoilho-yacht-club-san-francisco-2?osq=Restaurants
5	https://www.yelp.com/biz/marufuku-ramen-sf-san-francisco?osq=Restaurants
6	https://www.yelp.com/biz/farmhouse-kitchen-thai-cuisine-san-francisco?osq=Restaurants
7	https://www.yelp.com/biz/beretta-san-francisco?osq=Restaurants
8	https://www.yelp.com/biz/zazie-san-francisco?osq=Restaurants
9	https://www.yelp.com/biz/lol%C3%B3-san-francisco-4?osq=Restaurants
10	https://www.yelp.com/biz/pier-market-seafood-restaurant-san-francisco?osq=Restaurants

< 1 2 3 >

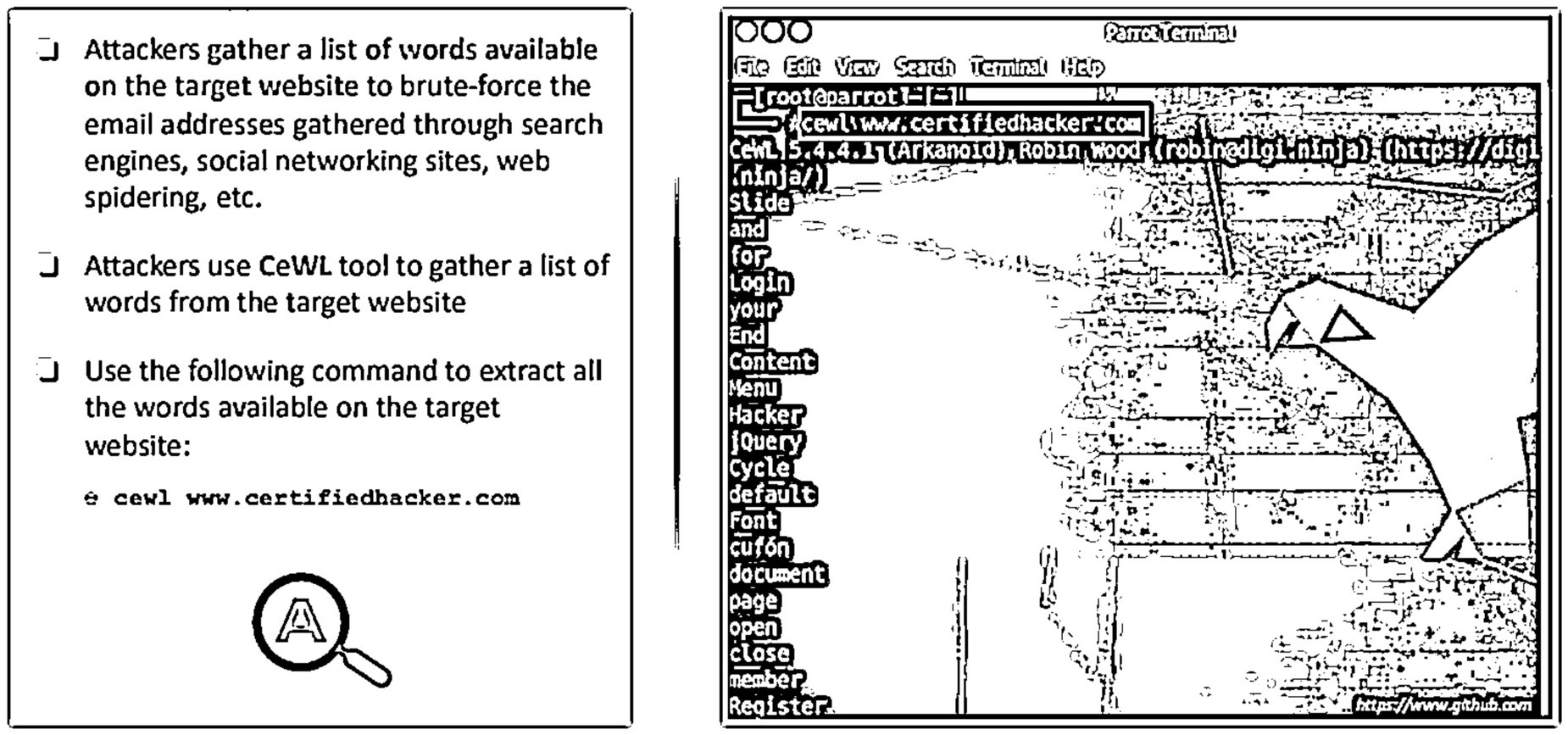
Data extracted: 30 lines Total time spent: 0 Average speed: 0 Export Data Start Extraction

Figure 2.51: Screenshot showing output of Octoparse

Gathering Wordlist from the Target Website

- Attackers gather a list of words available on the target website to brute-force the email addresses gathered through search engines, social networking sites, web spidering, etc.
- Attackers use CeWL tool to gather a list of words from the target website
- Use the following command to extract all the words available on the target website:

```
e cewl www.certifiedhacker.com
```



Gathering Wordlist from the Target Website

The words available on the target website may reveal critical information that helps attackers to perform further exploitation. Attackers gather a list of email addresses related to the target organization using various search engines, social networking sites, web spidering tools, etc. After obtaining these email addresses, an attacker can gather a list of words available on the target website. This information helps the attacker to perform brute-force attacks on the target organization. An attacker uses the CeWL tool to gather a list of words from the target website and perform a brute-force attack on the email addresses gathered earlier.

To run the CeWL tool, issue the following commands:

- **`ruby cewl.rb --help`**

  This command displays various options that a user can use to obtain a list of words from the target website.

- **`cewl www.certifiedhacker.com`**

  This command returns a list of unique words present in the target URL.

- **`cewl --email www.certifiedhacker.com`**

  In this case, the target website is **`www.certifiedhacker.com`**, and the **`'--email'`** option is used to fetch a list of words and email addresses from the target website.

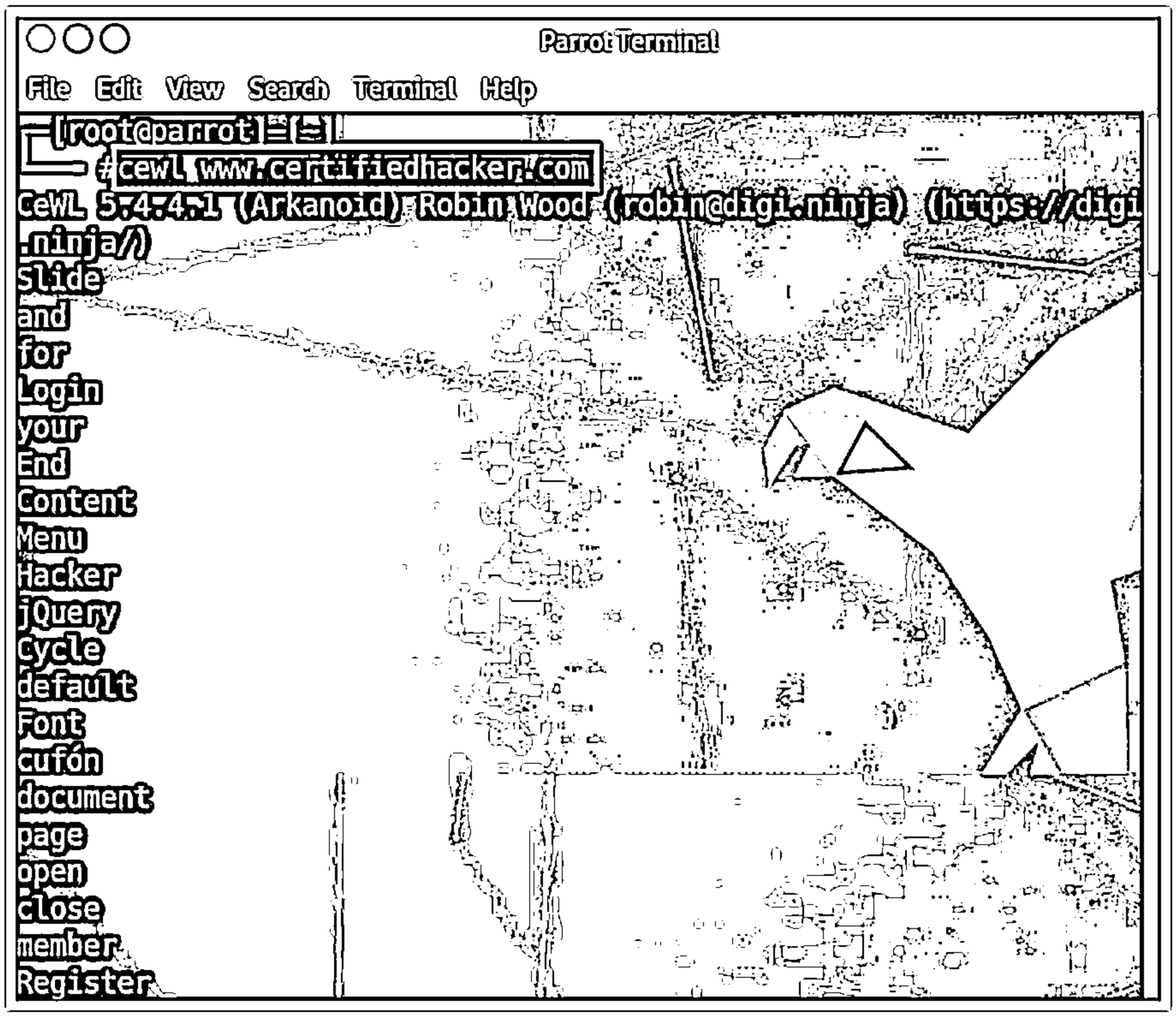
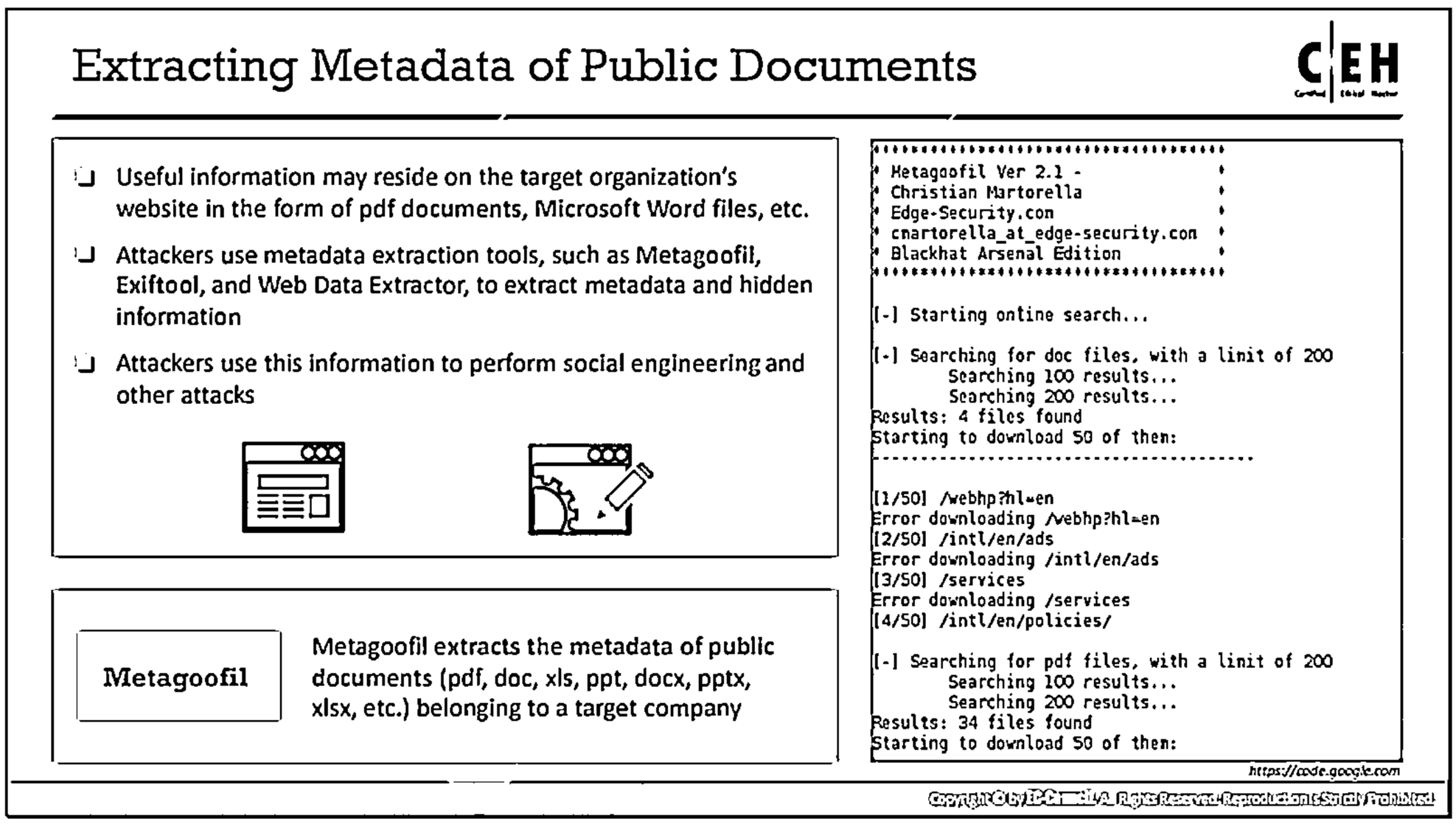


Figure 2.52: Screenshot showing results obtained from CeWL tool



Extracting Metadata of Public Documents

Useful information may reside on the target organization's website in the form of pdf documents, Microsoft Word files, and other files in various formats. Attackers extract valuable data, including metadata and hidden information from such documents. The data mainly contains hidden information about the public documents that can be analyzed to extract information such as the title of the page, description, keywords, creation/modification date and time of the content, and usernames and e-mail addresses of employees of the target organization.

An attacker can misuse this information to perform malicious activities against the target organization by brute-forcing authentication using the usernames and e-mail addresses of employees, or perform social engineering to send malware, which can infect the target system.

Metadata Extraction Tools

Metadata extraction tools such as Metagoofil, Exiftool, and Web Data Extractor automatically extract critical information that includes the usernames of clients, operating systems (exploits are OS-specific), email addresses (possibly for social engineering), list of software (version and type) used, list of servers, document date creation/modification, and authors of the website.

- **Metagoofil**

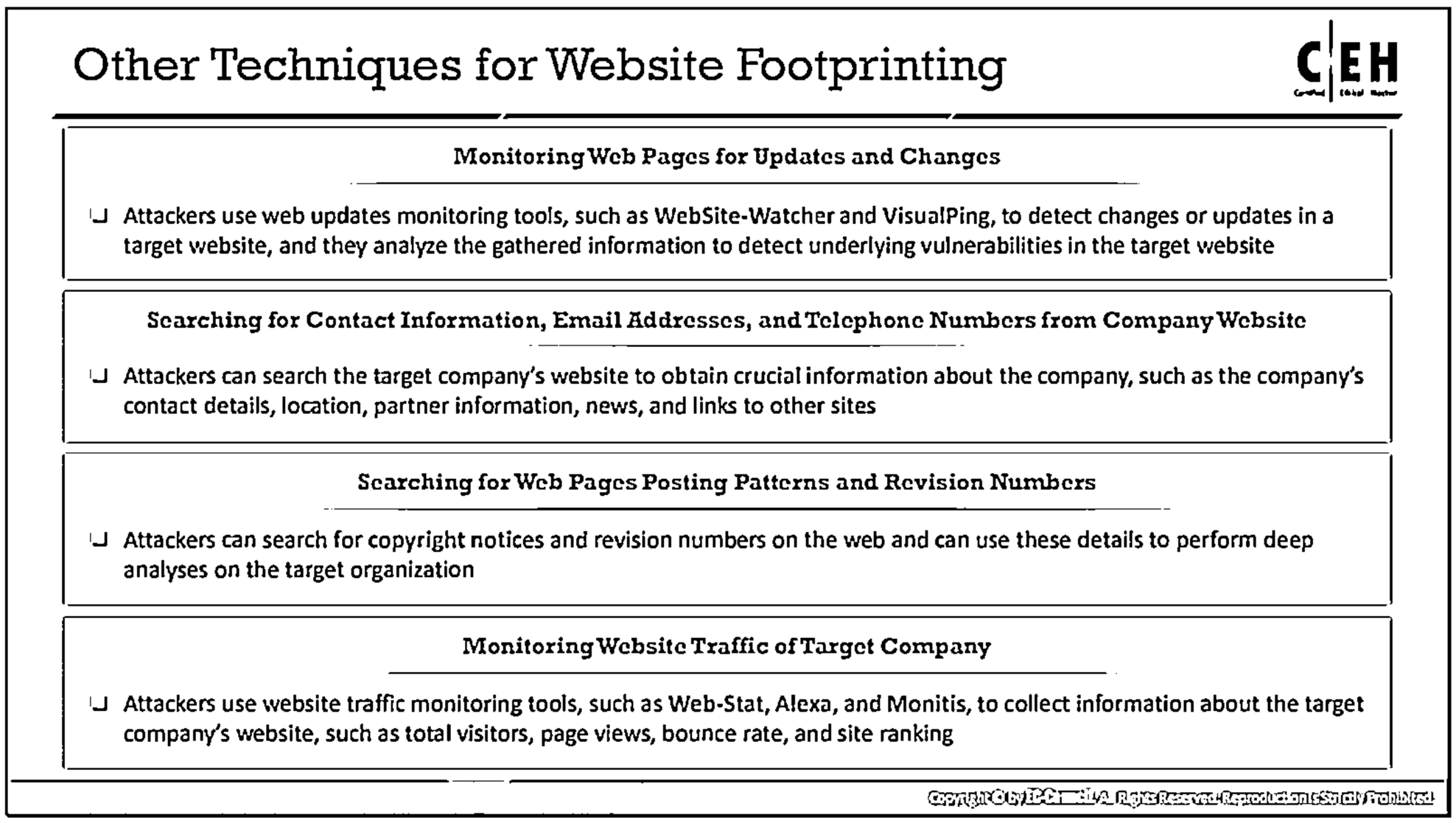
  Source: *https://code.google.com*

  Metagoofil extracts metadata of public documents (pdf, doc, xls, ppt, docx, pptx, and xlsx) belonging to a target company. It performs a Google search to identify and download the documents to the local disk and then extracts the metadata with different libraries such as Hachoir, PdfMiner, and others.

As shown in the screenshot, Metagoofil generates a report with usernames, software versions, and servers or machine names, which helps attackers in the information gathering phase.

```
*****************************************
* Metagoofil Ver 2.1 -                  *
* Christian Martorella                  *
* Edge-Security.com                     *
* cmartorella_at_edge-security.com      *
* Blackhat Arsenal Edition              *
*****************************************

[-] Starting online search...

[-] Searching for doc files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 4 files found
Starting to download 50 of them:
----------------------------------------

[1/50] /webhp?hl=en
Error downloading /webhp?hl=en
[2/50] /intl/en/ads
Error downloading /intl/en/ads
[3/50] /services
Error downloading /services
[4/50] /intl/en/policies/

[-] Searching for pdf files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 34 files found
Starting to download 50 of them:
```

Figure 2.53: Screenshot of Metagoofil



Other Techniques for Website Footprinting

- **Monitoring Web Pages for Updates and Changes**

  Attackers monitor the target website to detect web updates and changes. Monitoring the target website helps attackers to access and identify changes in the login pages, extract password-protected pages, track changes in the software version and driver updates, extract and store images on the modified web pages, and so on. Attackers analyze the gathered information to detect underlying vulnerabilities in the target website, and based on these vulnerabilities, they perform exploitation of the target web application.

  Web Updates Monitoring Tools

  Web updates monitoring tools are capable of detecting any changes or updates on a particular website, and they can send notifications or alerts to interested users through email or SMS.

  - **WebSite-Watcher**

    Source: *https://www.aignes.com*

    WebSite-Watcher helps to track websites for updates and automatic changes. When an update or change occurs, WebSite-Watcher automatically detects and saves the last two versions onto your disk.

    As shown in the screenshot, attackers use WebSite-Watcher to extract the older and newer versions of web pages related to the target website.

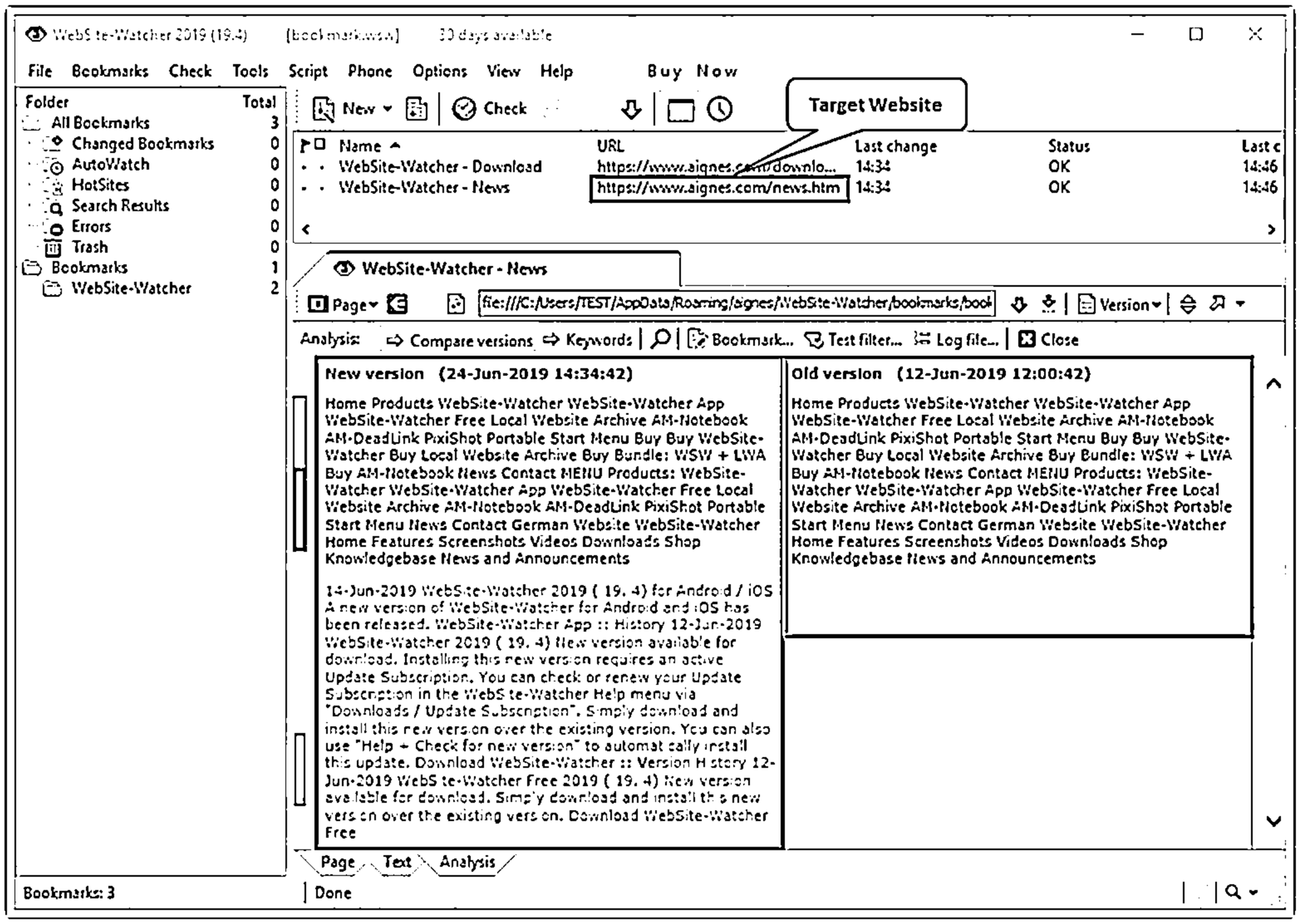


Figure 2.54: Screenshot of WebSite-Watcher

- **Searching for Contact Information, Email Addresses, and Telephone Numbers from Company Website**

  Attackers can search the target company's website to gather crucial information about the company. Generally, organizations use websites to inform the public about what they do, what type of services or products they provide, how to contact them, etc. Attackers can exploit this information to launch further attacks on the target company.

  For example, attackers can search for the following information on the company's website:

  - Company contact names, phone numbers, and email addresses
  - Company locations and branches
  - Partner Information
  - News
  - Links to other sites
  - Product, project, or service data

- **Searching for Web Pages Posting Patterns and Revision Numbers**

  Copyright is a protecting mechanism provided by the law of a country, which grants the creator of an original work exclusive rights for its use and distribution. To restrict third parties from accessing their data freely, most organizations ensure that there is a copyright notice on every single piece of their published work.

  A typical copyright notice contains the following information:

  - The Copyright Symbol
  - The Year of Creation
  - The Name of the Author
  - A Rights Statement

  An attacker can search for copyright notices on the web and use these details to perform a deep analysis of the target organization. Further, attackers can search and note down the revision number of a product. The revision number is a unique string that acts as an identifier for the revision of a given document, and it can be found within the documents of the company.

  Attackers can also search for the document numbers that are assigned to the documents after revision, which can be searched from the Internet and recorded to launch further attacks on the target.

- **Monitoring Website Traffic of Target Company**

  Attackers can monitor a target company's website traffic using tools such as Web-Stat, Alexa, and Monitis to collect valuable information. These tools help to collect information about the target's customer base, which help attackers to disguise themselves as customers and launch social engineering attacks on the target.

  The information collected includes:

  - **Total visitors**: Tools such as Clicky (*https://clicky.com*) find the total number of visitors browsing the target website.
  - **Page views**: Tools such as Opentracker (*https://www.opentracker.net*) monitor the total number of pages viewed by the users along with the timestamps and the status of the user on a particular web page (whether the webpage is still active or closed).
  - **Bounce rate**: Tools such as Google Analytics (*https://analytics.google.com*) measure the bounce rate of the target company's website.
  - **Live visitors map**: Tools such as Web-Stat (*https://www.web-stat.com*) track the geographical location of the users visiting the company's website.
  - **Site ranking**: Tools such as Alexa (*https://www.alexa.com*) track a company's rank on the web.
  - **Audience geography**: Tools such as Alexa track a company's customer locations on the globe.

- **Track Visitors and monitor sales:** Tools such as goingup! (*https://goingup.com*) track visitors, monitor sales, and show conversation rates with the company's website.

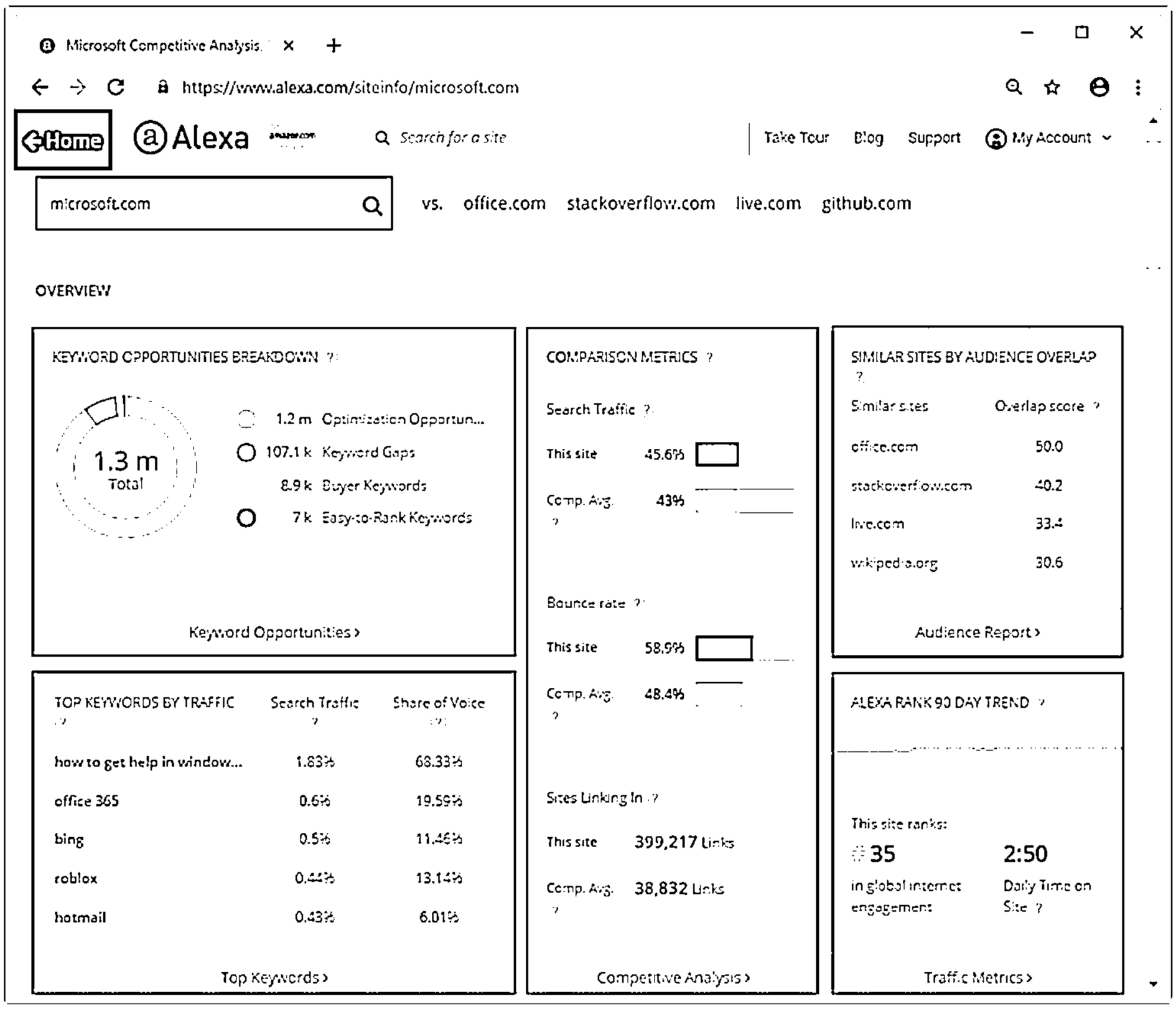


Figure 2.55: Screenshot of Alexa

Tracking Email Communications

- Email tracking is used to monitor the delivery of emails to an intended recipient
- Attackers track emails to gather information about a target recipient, such as IP addresses, geolocation, browser and OS details, to build a hacking strategy and perform social engineering and other such attacks

Collecting Information from Email Header

```
Delivered-To: [redacted]@gmail.com
Received: by 2002:a8a:a99:0:0:0:0:0 with SMTP
        Sun, 9 Jun 2019 21:09:48 -0700 (PDT)
Return-Path: <[redacted]@gmail.com>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
        by mx.google.com with SMTPS id v17sor2[redacted]9.48
        for <[redacted]@gmail.com>
        (Google Transport Security);
        Sun, 09 Jun 2019 21:09:48 -0700 (PDT)
Received-SPF: pass (google.com: domain of [redacted]@gmail.com designates 209.85.220.41 as
permitted sender) client-ip=209.85.220.41;
Authentication-Results: mx.google.com;
        dkim=pass header.i=@gmail.com header.s=20161025 header.b=s6SNavzN;
        spf=pass (google.com: domain of [redacted]@gmail.com designates 209.85.220.41 as
permitted sender) smtp.mailfrom=[redacted]@gmail.com;
        dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=gmail.com
DKIM-Signature: v=1; a=rsa-sha256;
        d=gmail.com; s=20161025;
        h=mime-version:from:date:message-id:subject:to;
        bh=nheQC6dgQ1hKwkCykBx4gYXJWwtRRaK2KrErKhvfCg=;
        b=s6SNavzNMAeeZJZF5r7LGPdGSiUyxSKDxvLIBGHxEcf/pIIqx8XkNR2JGfO[redacted]VXAL
         e763D+SPbKrPS4CPx9hkvdbYhbcVgUZFuEvp3J/fPvIlIT7B1f8jGXHqvvxxQhTH8+/g
         XeIE0g6h98SYL4lvePj819hw1xvjyn8QVRoCgEqkE8JVRfqnNcOxNBa6yoxu0V1JRT0A
         aFdUZSJKJPwbG8gBU5hS+bIrr3no37OYJgL1h/YwkLTx76h7BgDYBzNCyg+ZPA+NvK5K
         3E/vrqeaGvGeZwh6xaS6L/mhf7CIuuxa/skSls1pfsKIeJv1geCAV8Cq134JC292NRn2
         YCxw==
MIME-Version: 1.0
From: [redacted] <[redacted]@gmail.com>
Date: Sun, 09 Jun 2019 21:09:47 -0700
Message-ID: <CA+[redacted]com>
Subject: Check Out Daily News Feed
To: [redacted]@gmail.com
```

The address from which the message was sent

Date and time received by the originator's email servers

Sender's IP address

Sender's mail server

Authentication system used by sender's mail server

Sender's full name

Date and time of message sent

Email Footprinting

So far, we have discussed footprinting through search engines, footprinting using Google, footprinting through social networking sites, and website footprinting. Now, we will discuss email footprinting. This section describes how to track email communications, how to collect information from email headers, and email tracking tools.

Tracking Email Communications

Email tracking monitors the email messages of a particular user. This kind of tracking is possible through digitally time-stamped records that reveal the time and date when the target receives and opens a specific email. Email tracking tools allow an attacker to collect information such as IP addresses, mail servers, and service providers involved in sending the email. Attackers can use this information to build a hacking strategy and to perform social engineering and other attacks. Examples of email tracking tools include eMailTrackerPro, Infoga, and Mailtrack.

Information about the victim gathered using email tracking tools includes:

- **Recipient's System IP address**: Allows tracking of the recipient's IP address
- **Geolocation**: Estimates and displays the location of the recipient on the map and may even calculate the distance from the attacker's location
- **Email Received and Read**: Notifies the attacker when the email is received and read by the recipient
- **Read Duration**: The time spent by the recipient in reading the email sent by the sender
- **Proxy Detection**: Provides information about the type of server used by the recipient
- **Links**: Checks whether the links sent to the recipient through email have been checked

- **Operating System and Browser information**: Reveals information about the operating system and the browser used by the recipient. The attacker can use this information to find loopholes in that version of the operating system and browser to launch further attacks
- **Forward Email**: Determines whether the email sent to the user is forwarded to another person
- **Device Type**: Provides information about the type of device used to open and read the email, e.g., desktop computer, mobile device, or laptop
- **Path Travelled**: Tracks the path through which the email traveled via email transfer agents from source to destination system

Collecting Information from Email Header

An email header contains the details of the sender, routing information, addressing scheme, date, subject, and recipient. Email headers also help attackers to trace the routing path taken by an email before it is delivered to the recipient. Each email header is a useful source of information for an attacker to launch attacks against the target. The process of viewing the email header varies with different email programs.

Commonly used email programs:

- eM Client
- Mailbird Lite
- Hiri
- Mozilla Thunderbird
- Spike
- Claws Mail
- SmarterMail Webmail
- Outlook

The email header contains the following information:

- Sender's mail server
- Date and time of receipt by the originator's email servers
- Authentication system used by the sender's mail server
- Data and time of sending the message
- A unique number assigned by mx.google.com to identify the message
- Sender's full name
- Sender's IP address and address from which the message was sent

The attacker can trace and collect all this information by performing a detailed analysis of the complete email header.

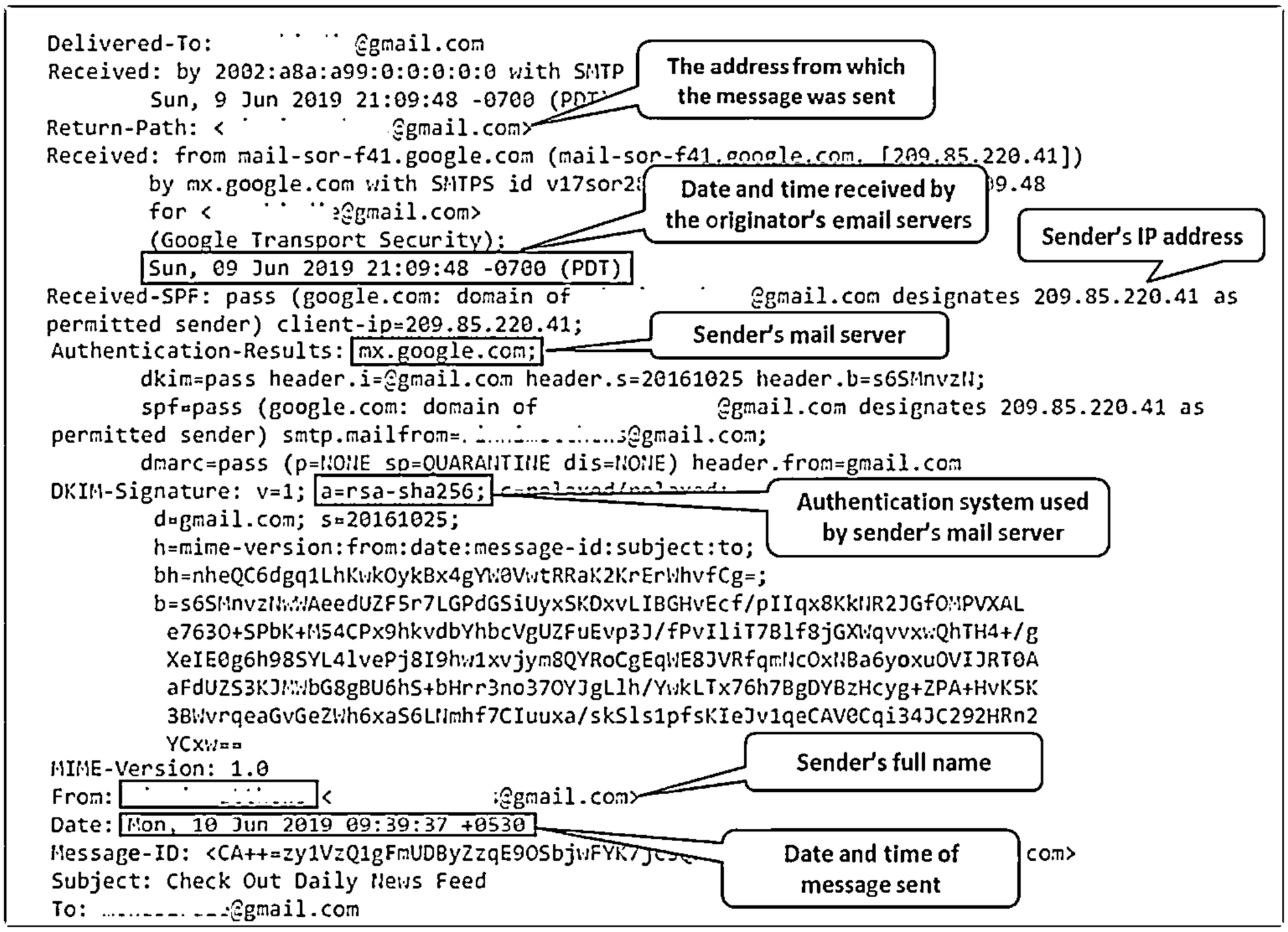
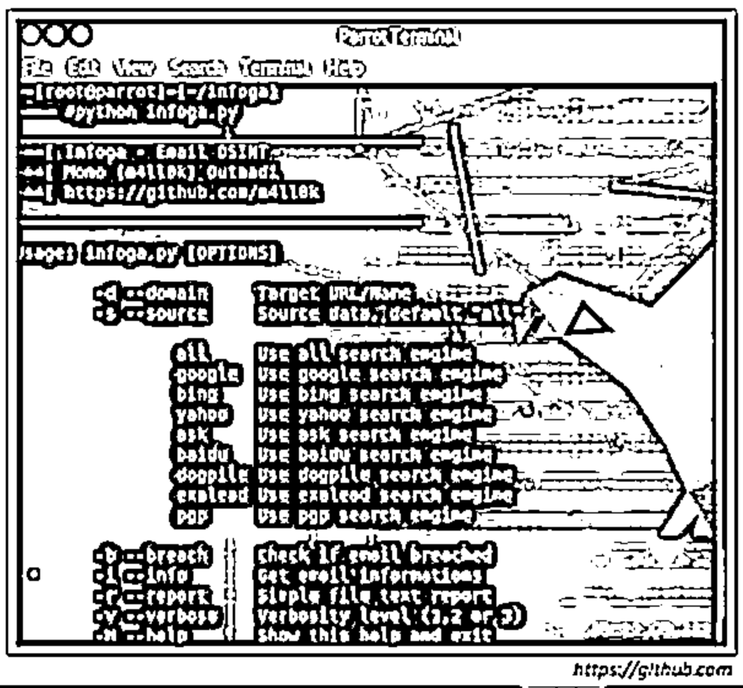
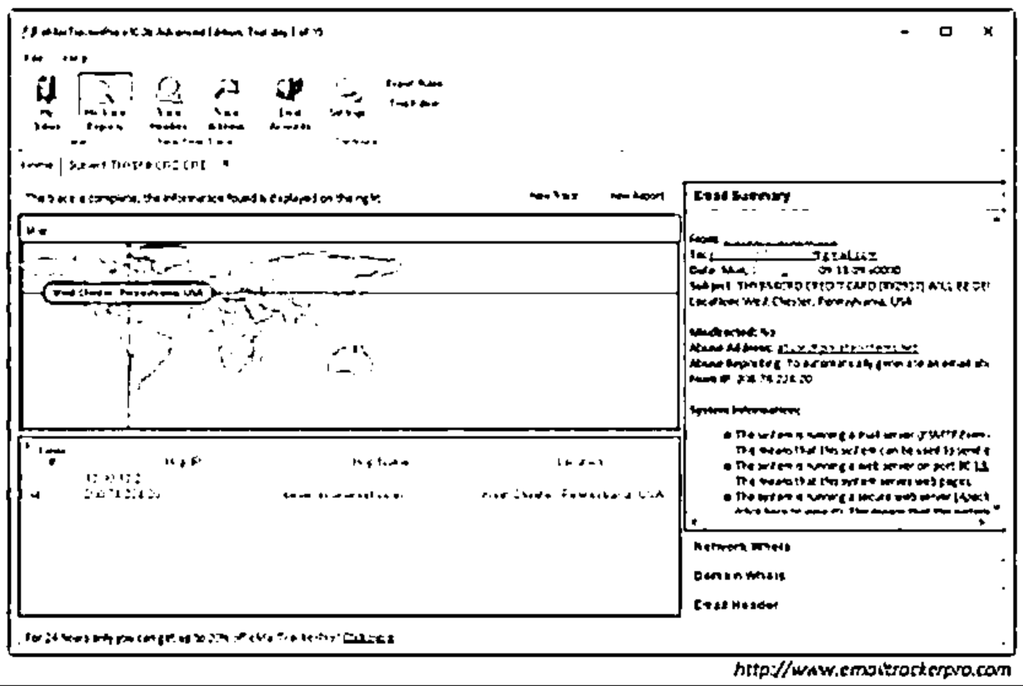


Figure 2.56: Screenshot showing detailed analysis of the email header

Email Tracking Tools

- Email tracking tools, such as eMailTrackerPro, Infoga, Mailtrack, and PoliteMail, allow an attacker to track an email and extract information, such as sender identity, mail server, sender's IP address, and location
- eMailTrackerPro analyzes email headers and reveals information, such as sender's geographical location and IP address





Email Tracking Tools

Email tracking tools allow an attacker to track an email and extract information such as sender identity, mail server, sender's IP address, location, and so on. These tools send notifications automatically when the recipients open the mail and provide status information about whether the email was successfully delivered or not. Attackers use the extracted information to attack the target organization's systems by sending malicious emails.

- **Infoga**

  Source: *https://github.com*

  Infoga is a tool used for gathering email account information (IP, hostname, country, etc.) from different public sources (search engines, pgp key servers, and Shodan), and it checks if an email was leaked using the haveibeenpwned.com API. For example, the command

  ```
  python infoga.py --domain microsoft.com --source all --breach -v
  2 --report ../microsoft.txt
  ```

  will retrieve all the publicly available email addresses related to the domain microsoft.com along with email account information.

  ```
  python infoga.py --info m4ll0k@protonmail.com --breach -v 3 --
  report ../m4ll0k.txt
  ```

  The above command will retrieve email account information for a specified email address.

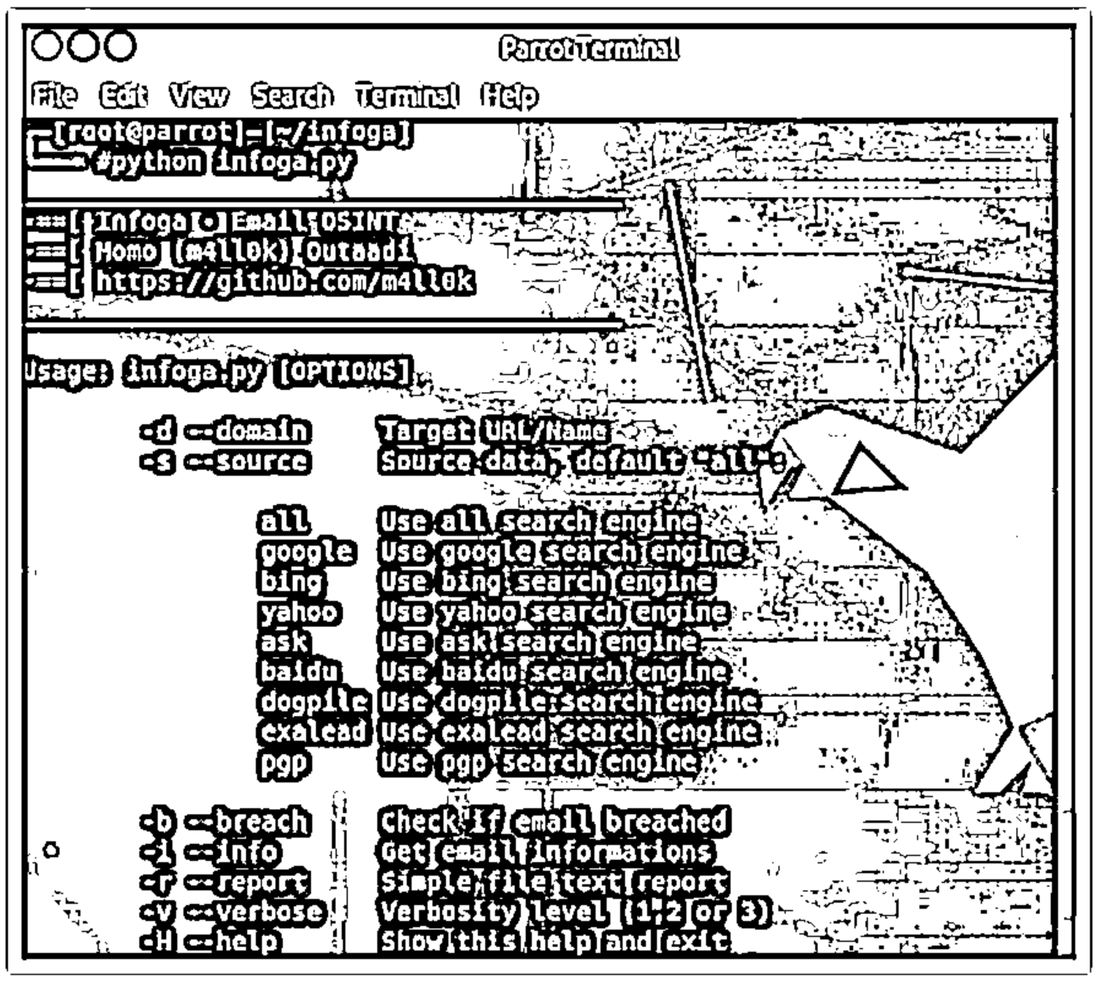


Figure 2.57: Screenshot showing various options of Infoga

- **eMailTrackerPro**

  Source: *http://www.emailtrackerpro.com*

  As shown in the screenshot, attackers use eMailTrackerPro to analyze email headers and extract information such as the sender's geographical location, IP address, and so on. It allows an attacker to review the traces later by saving past traces.

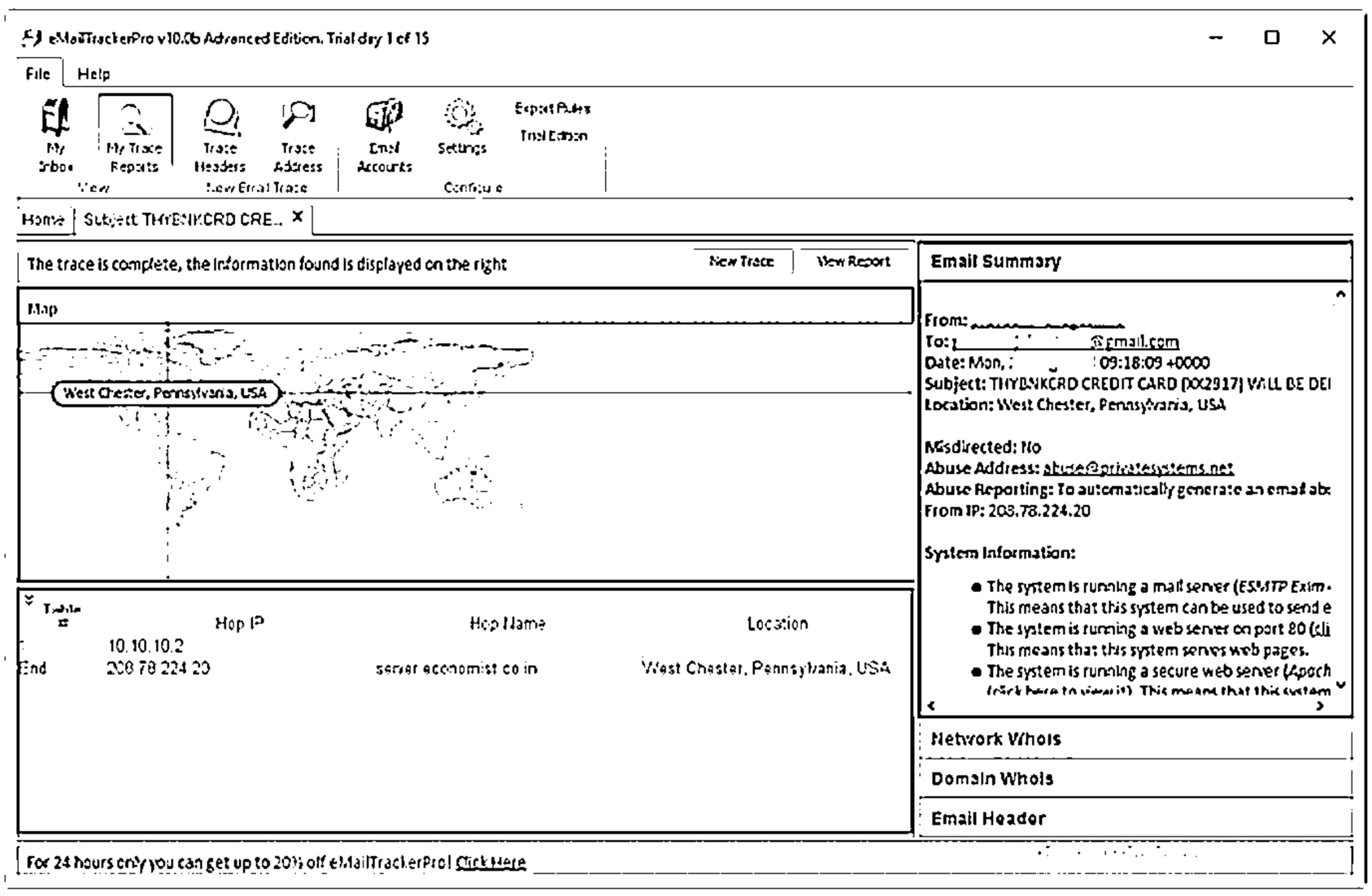


Figure 2.58: Screenshot of eMailTrackerPro

Whois Lookup

Whois databases are maintained by Regional Internet Registries and contain personal information of domain owners

Whois query returns

- Domain name details
- Contact details of domain owners
- Domain name servers
- NetRange
- When a domain was created
- Expiry records
- Last updated record

Information obtained from Whois database assists an attacker to

- Gather personal information that assists in social engineering
- Create a map of the target organization's network
- Obtain internal details of the target network

Regional Internet Registries (RIRs)

ARIN
AFRINIC
RIPE NCC
lacnic
APNIC

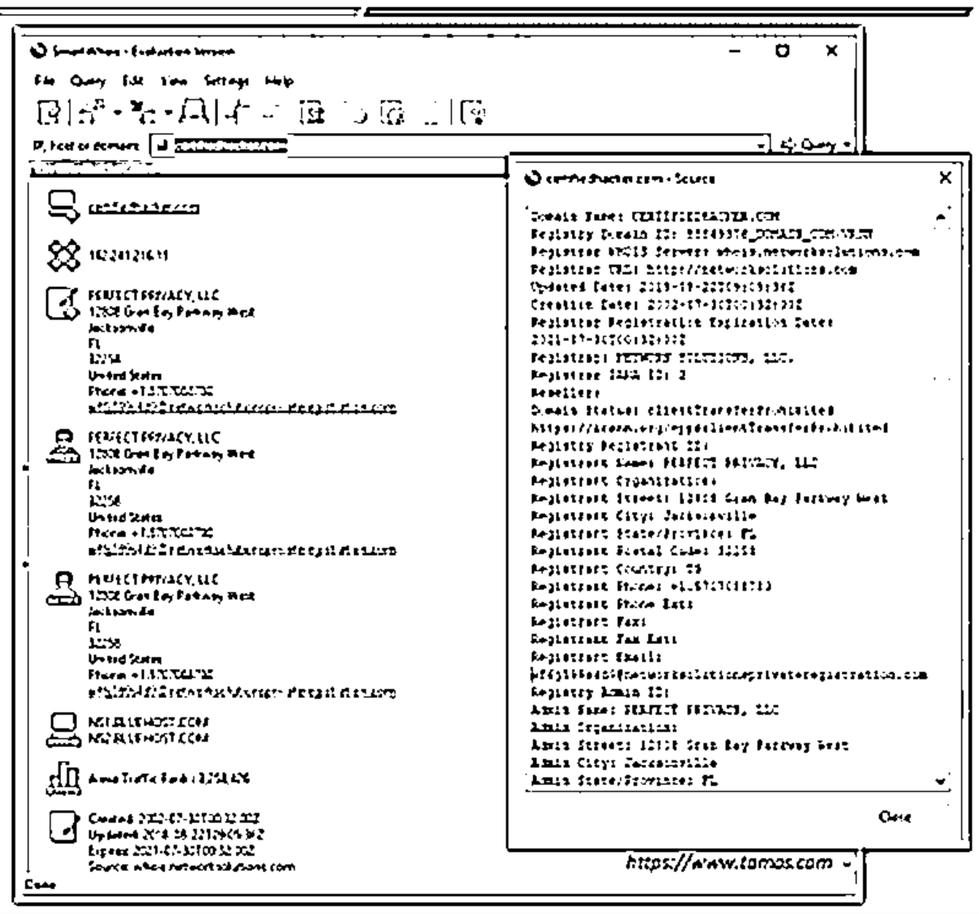
Whois Lookup (Cont'd)

Whois Record for CertifiedHacker.com

Domain Profile

Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	NETWORK SOLUTIONS, LLC, Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com abuse@web.com tel:1.8003337680
Registrar Status	clientTransferProhibited, clientTransferProhibited
Dates	6,160 days old Created on 2002-07-29 Expires on 2021-07-29 Updated on 2018-05-22
Name Servers	NS1.BLUEHOST.COM (has 2,477,906 domains) NS1.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains)
Tech Contact	PERFECT PRIVACY, LLC 12808 Gran Bay Parkway West, Jacksonville, FL, 32258, us tel:1.5707088240
IP Address	162.241.216.11 - 1,025 other sites hosted on this server
IP Location	- Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 13 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 16

http://whois.domaintools.com



Whois Footprinting

Gathering network-related information such as "Whois" information about the target organization is important when planning an attack. In this section, we will discuss Whois footprinting, which helps in gathering domain information such as information regarding the owner of an organization, its registrar, registration details, its name server, and contact information. Whois footprinting focuses on how to perform a Whois lookup, analyze the Whois

lookup results, and find IP geolocation information, as well as the tools used to gather Whois information.

Whois Lookup

Whois is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain Whois databases, which contain the personal information of domain owners. For each resource, the Whois database provides text records with information about the resource itself and relevant information regarding assignees, registrants, and administrative information (creation and expiration dates).

Two types of data models exist to store and lookup Whois information:

- **Thick Whois** - Stores the complete Whois information from all the registrars for a particular set of data.
- **Thin Whois** - Stores only the name of the Whois server of the registrar of a domain, which in turn holds complete details on the data being looked up.

Whois query returns the following information:

- Domain name details
- Contact details of the domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated

An attacker queries a Whois database server to obtain information about the target domain name, contact details of its owner, expiry date, creation date, and so on, and the Whois server responds to the query with the requested information. Using this information, an attacker can create a map of the organization's network, mislead domain owners with social engineering, and then obtain internal details of the network.

Regional Internet Registries (RIRs)

The RIRs include:

- ARIN (American Registry for Internet Numbers) (*https://www.arin.net*)
- AFRINIC (African Network Information Center) (*https://www.afrinic.net*)
- APNIC (Asia Pacific Network Information Center) (*https://www.apnic.net*)
- RIPE (Réseaux IP Européens Network Coordination Centre) (*https://www.ripe.net*)
- LACNIC (Latin American and Caribbean Network Information Center) (*https://www.lacnic.net*)

Whois Lookup Result

Whois services such as *http://whois.domaintools.com* or *https://www.tamos.com* can help to perform Whois lookups. The screenshot shows the result analysis of a Whois lookup obtained with the two above-mentioned Whois services. The services perform Whois lookup by entering the target's domain or IP address. The domaintools.com service provides Whois information such as registrant information, email, administrative contact information, creation and expiry date, and a list of domain servers. SmartWhois, available at *http://www.tamos.com*, gives information about an IP address, hostname, or domain, including information about the country, state or province, city, phone number, fax number, name of the network provider, administrator, and technical support contact information. It also helps in finding the owner of the domain, the owner's contact information, the owner of the IP address block, registered date of the domain, and so on. It supports Internationalized Domain Names (IDNs), which means one can query domain names that use non-English characters. It also supports IPv6 addresses.

Whois Record for CertifiedHacker.com

— Domain Profile

Registrant	PERFECT PRIVACY, LLC
Registrant Country	us
Registrar	NETWORK SOLUTIONS, LLC. Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com abuse@web.com (p) 18003337680
Registrar Status	clientTransferProhibited, clientTransferProhibited
Dates	6,160 days old Created on 2002-07-29 Expires on 2021-07-29 Updated on 2018-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,477,906 domains) NS1.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains) NS2.BLUEHOST.COM (has 2,477,906 domains)
Tech Contact	PERFECT PRIVACY, LLC 12808 Gran Bay Parkway West, Jacksonville, FL, 32258, us wf6j599s4d9@networksolutionsprivateregistration.com (p) 15707088780
IP Address	162.241.216.11 - 1,025 other sites hosted on this server
IP Location	- Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008)
Domain Status	Registered And Active Website
IP History	13 changes on 13 unique IP addresses over 13 years
Registrar History	3 registrars with 2 drops
Hosting History	6 changes on 4 unique name servers over 16 years

Figure 2.59: Screenshot of Whois

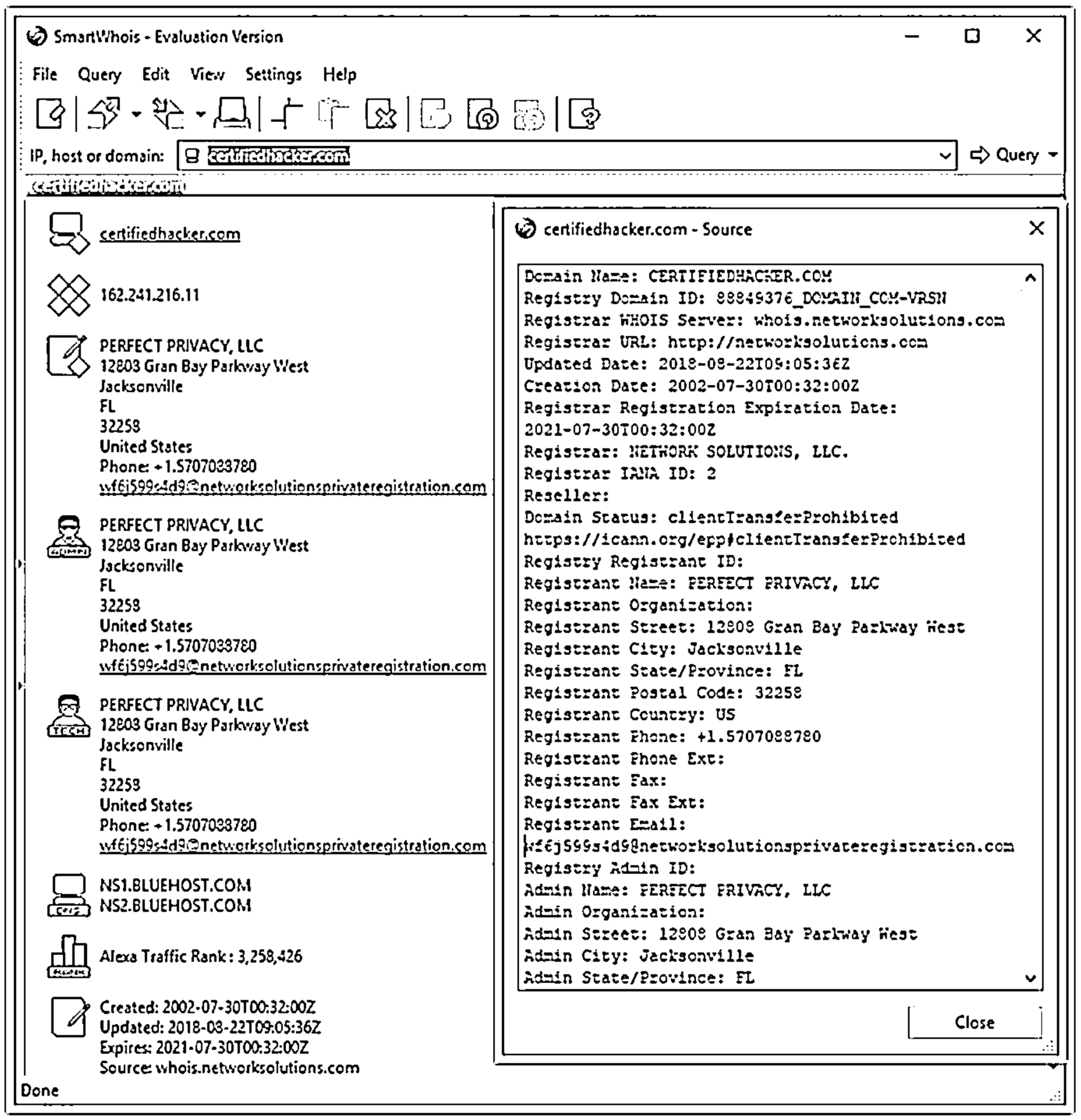
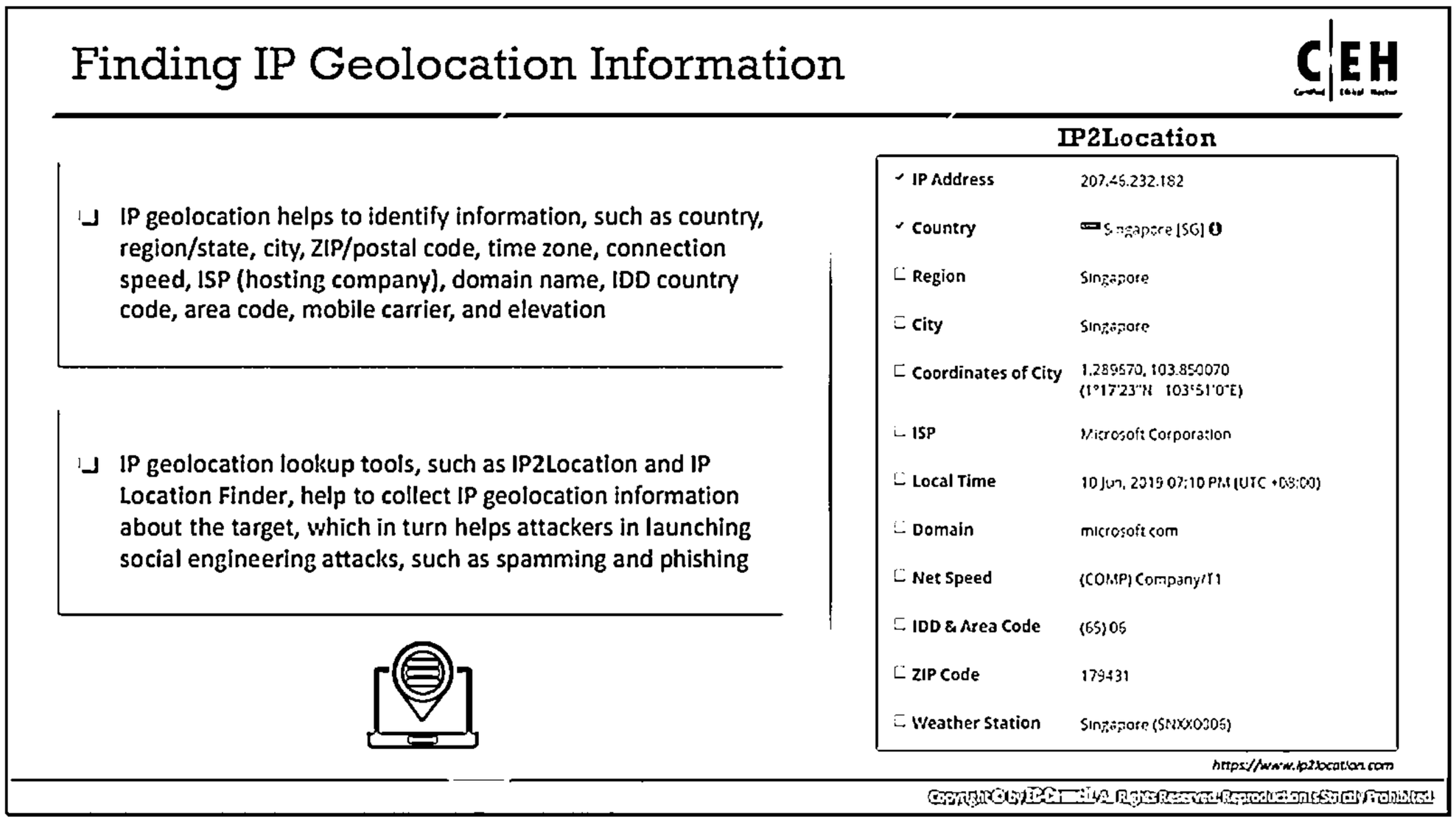


Figure 2.60: Screenshot of SmartWhois

Attackers use Whois lookup tools such as Batch IP Converter, WhoIs Analyzer Pro, and ActiveWhois to extract information such as IP addresses, hostnames or domain names, registrant information, and DNS records, including the country, city, state, phone and fax numbers, network service providers, administrators, and technical support information, for any IP address or domain name.



Finding IP Geolocation Information

IP geolocation helps to obtain information regarding a target such as its country, region/state, city, latitude and longitude of its city, ZIP/postal code, time zone, connection speed, ISP (hosting company), domain name, IDD country code, area code, weather station code and name, mobile carrier, and elevation.

Using the information obtained from IP geolocation, an attacker may attempt to gather more information about a target with the help of social engineering, surveillance, and non-technical attacks such as dumpster diving, hoaxing, or acting as a technical expert. With the help of the information obtained, an attacker can also set up a compromised web server near the victim's location, and if the exact location of the victim is detected, the attacker can perform malicious activities and infect the victim with malware designed for that specific area or gain unauthorized access to the target device or attempt to launch an attack using the target device.

IP geolocation lookup tools such as IP2Location, IP Location Finder, and IP Address Geographical Location Finder help to collect IP geolocation information about the target, which enables attackers to launch social engineering attacks such as spamming and phishing.

IP Geolocation Lookup Tools

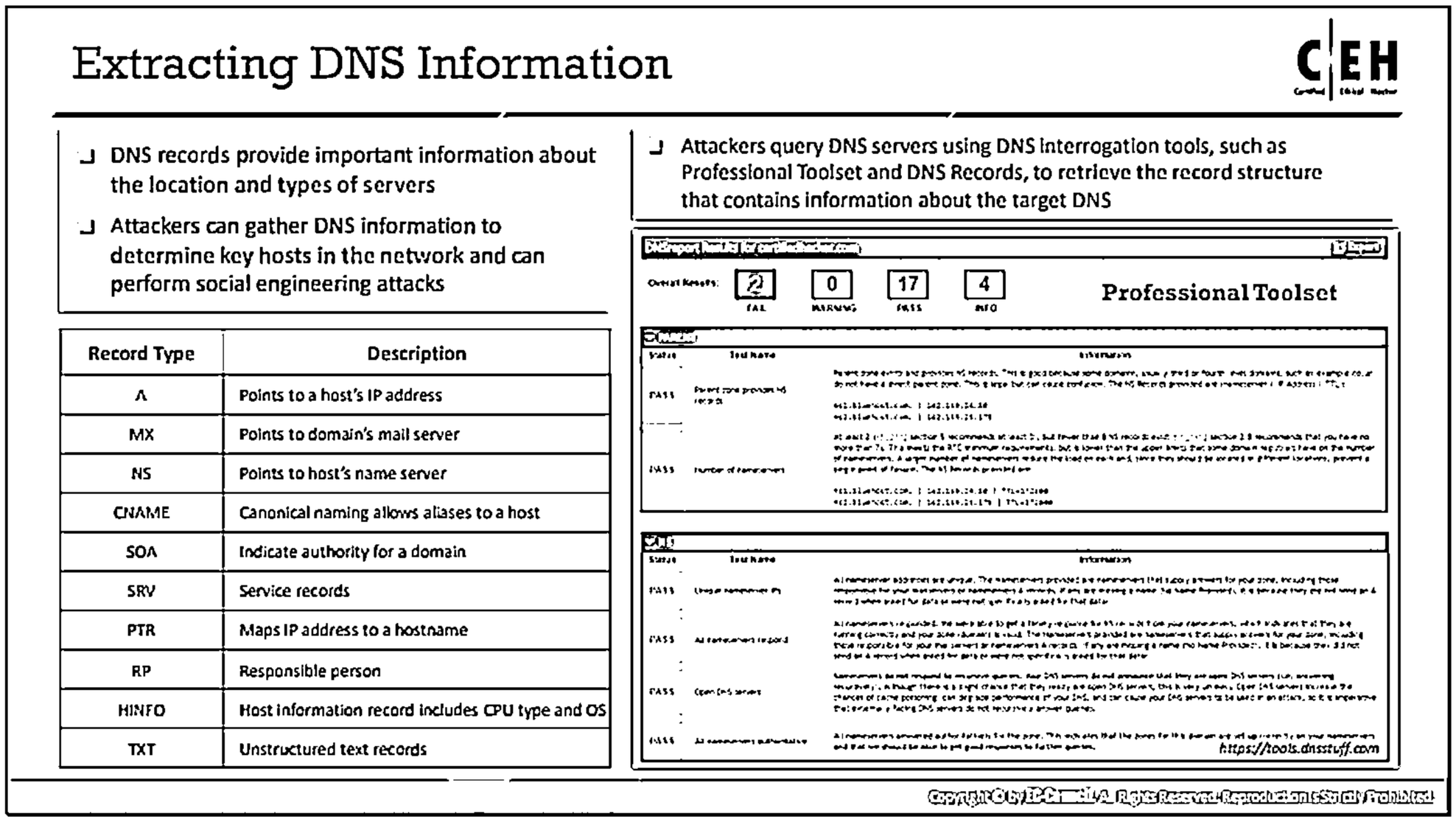
- **IP2Location**

  Source*: https://www.ip2location.com*

  As shown in the screenshot, attackers use IP2Location tool to identify a visitor's geographical location, i.e., country, region, city, latitude and longitude of city, ZIP code, time zone, connection speed, ISP, domain name, IDD country code, area code, weather station code and name, mobile carrier, elevation, and usage type information using a proprietary IP address lookup database and technology.

✓ IP Address	207.46.232.182
✓ Country	Singapore [SG]
☐ Region	Singapore
☐ City	Singapore
☐ Coordinates of City	1.289670, 103.850070 (1°17'23"N 103°51'0"E)
☐ ISP	Microsoft Corporation
☐ Local Time	10 Jun, 2019 07:10 PM (UTC +08:00)
☐ Domain	microsoft.com
☐ Net Speed	(COMP) Company/T1
☐ IDD & Area Code	(65) 06
☐ ZIP Code	179431
☐ Weather Station	Singapore (SNXX0006)

Figure 2.61: Screenshot of IP2Location



DNS Footprinting

After collecting Whois records about the target, the next phase in the footprinting methodology is DNS footprinting. Attackers perform DNS footprinting to gather information about DNS servers, DNS records, and types of servers used by the target organization. This information helps attackers to identify the hosts connected in the target network and perform further exploitation on the target organization.

This section describes how to extract DNS information, perform the reverse DNS lookup, and collect information from DNS zone transfers, as well as DNS interrogation tools.

Extracting DNS Information

DNS footprinting reveals information about DNS zone data. DNS zone data include DNS domain names, computer names, IP addresses, and much more information about a network. An attacker uses DNS information to determine key hosts in the network and then performs social engineering attacks to gather even more information.

DNS footprinting helps in determining the following records about the target DNS:

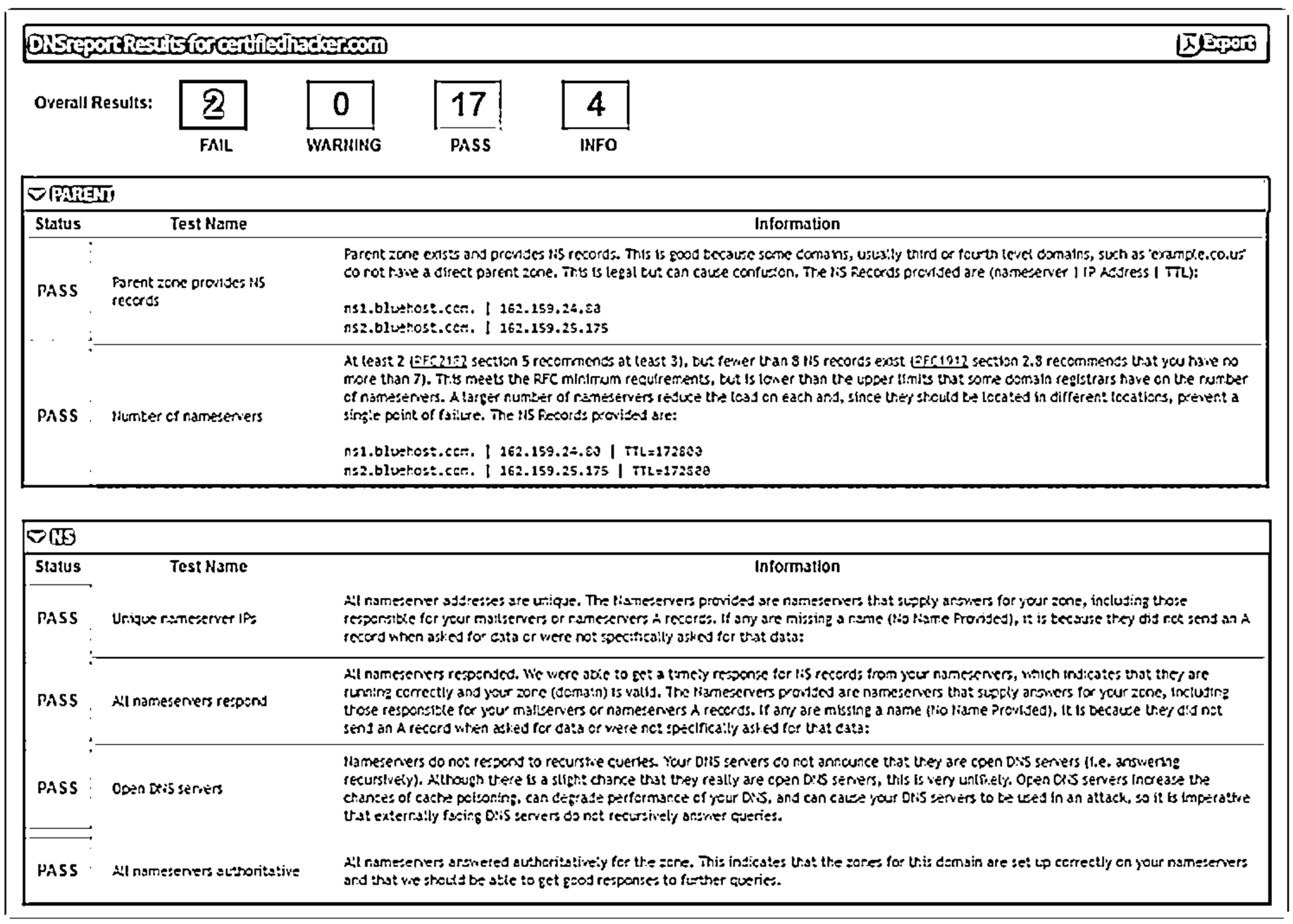
Record Type	Description
A	Points to a host's IP address
MX	Points to domain's mail server
NS	Points to host's name server
CNAME	Canonical naming allows aliases to a host
SOA	Indicate authority for a domain
SRV	Service records

PTR	Maps IP address to a hostname
RP	Responsible person
HINFO	Host information record includes CPU type and OS
TXT	Unstructured text records

Table 2.7: DNS records and their description

DNS interrogation tools such as Professional Toolset (*https://tools.dnsstuff.com)* and DNS Records (*https://network-tools.com*) enable the user to perform DNS footprinting. DNSstuff (Professional Toolset) extracts DNS information about IP addresses, mail server extensions, DNS lookups, Whois lookups, and so on. It can extract a range of IP addresses using an IP routing lookup. If the target network allows unknown, unauthorized users to transfer DNS zone data, then it is easy for an attacker to obtain the information about DNS with the help of the DNS interrogation tool.

When the attacker queries the DNS server using the DNS interrogation tool, the server responds with a record structure that contains information about the target DNS. DNS records provide important information about the location and types of servers.


DNSreport Results for certifiedhacker.com — Export

Overall Results: 2 FAIL | 0 WARNING | 17 PASS | 4 INFO

PARENT

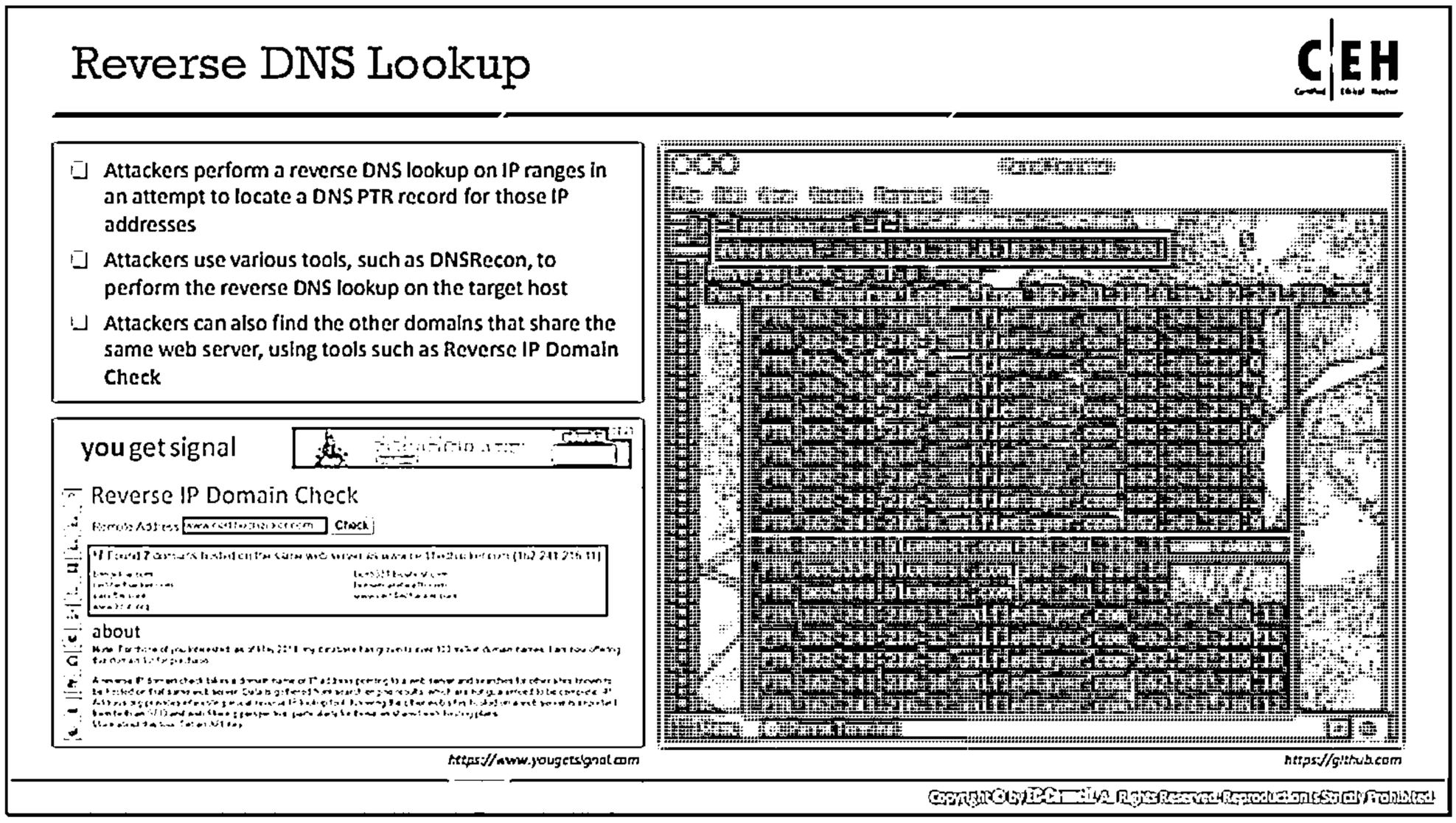
Status	Test Name	Information
PASS	Parent zone provides NS records	Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level domains, such as 'example.co.uk' do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are (nameserver | IP Address | TTL): ns1.bluehost.com. | 162.159.24.80 ns2.bluehost.com. | 162.159.25.175
PASS	Number of nameservers	At least 2 (RFC2182 section 5 recommends at least 3), but fewer than 8 NS records exist (RFC1912 section 2.8 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are: ns1.bluehost.com. | 162.159.24.80 | TTL=172800 ns2.bluehost.com. | 162.159.25.175 | TTL=172800

NS

Status	Test Name	Information
PASS	Unique nameserver IPs	All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:
PASS	All nameservers respond	All nameservers responded. We were able to get a timely response for NS records from your nameservers, which indicates that they are running correctly and your zone (domain) is valid. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:
PASS	Open DNS servers	Nameservers do not respond to recursive queries. Your DNS servers do not announce that they are open DNS servers (i.e. answering recursively). Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open DNS servers increase the chances of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack, so it is imperative that externally facing DNS servers do not recursively answer queries.
PASS	All nameservers authoritative	All nameservers answered authoritatively for the zone. This indicates that the zones for this domain are set up correctly on your nameservers and that we should be able to get good responses to further queries.

Figure 2.62: Screenshot of Professional Toolset

Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records.



Reverse DNS Lookup

DNS lookup is used for finding the IP addresses for a given domain name, and the reverse DNS operation is performed to obtain the domain name of a given IP address. When you are looking for a domain and type the domain name in the browser, the DNS converts that domain name into an IP address and forwards the request for further processing. This conversion of a domain name into an IP address is performed by a record. Attackers perform a reverse DNS lookup on the IP range to locate a DNS PTR record for such IP addresses.

Attackers use various tools such as DNSRecon and Reverse IP Domain Check for performing the reverse DNS lookup on the target host. When we get an IP address or a range of IP addresses, we can use these tools to obtain the domain name.

- **DNSRecon**

  Source: *https://github.com*

  As shown in the screenshot, attackers use the following command to perform a reverse DNS lookup on the target host:

  ```
  dnsrecon -r 162.241.216.0-162.241.216.255
  ```

  In the above command, the -r option specifies the range of IP addresses (first-last) for a reverse lookup by brute force.

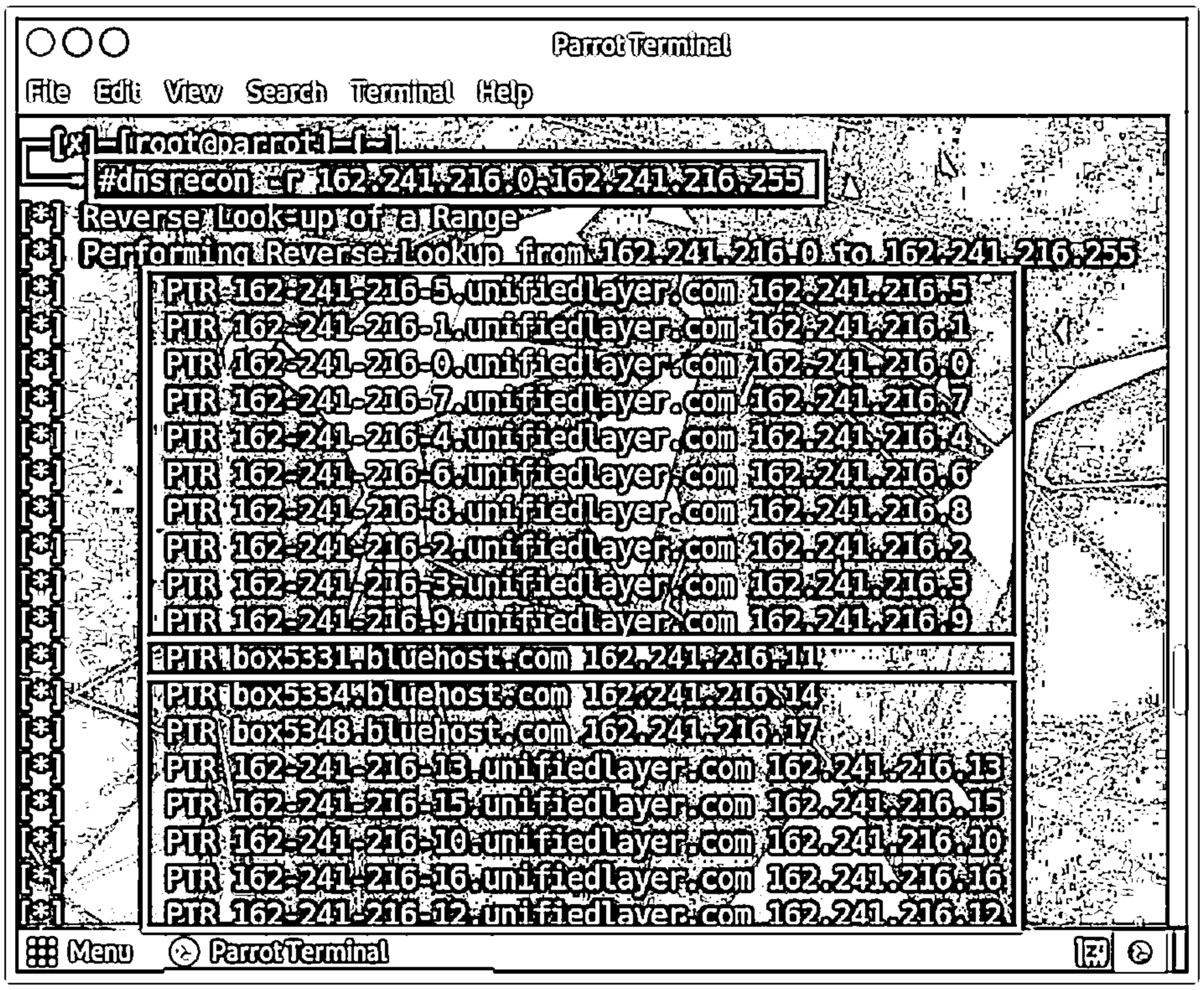


Figure 2.63: Screenshot of DNSRecon showing reverse DNS lookup information

Attackers also find the other domains that share the same web server using tools such as Reverse IP Domain Check. These tools list the possible domains that are hosted on the same web server.

- **Reverse IP Domain Check**

  Source: *https://www.yougetsignal.com*

  As shown in the screenshot, a reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other sites known to be hosted on the same web server.

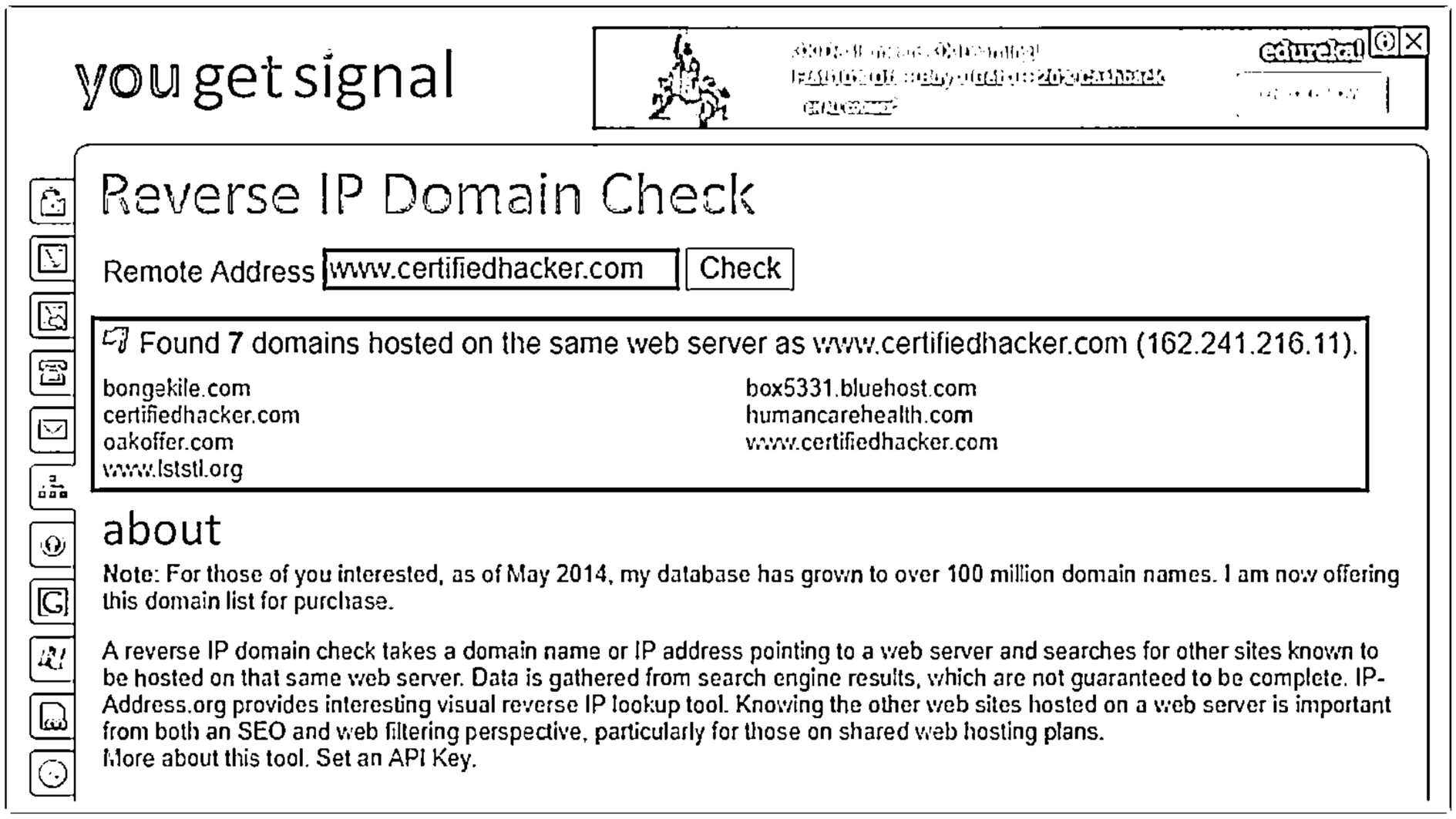
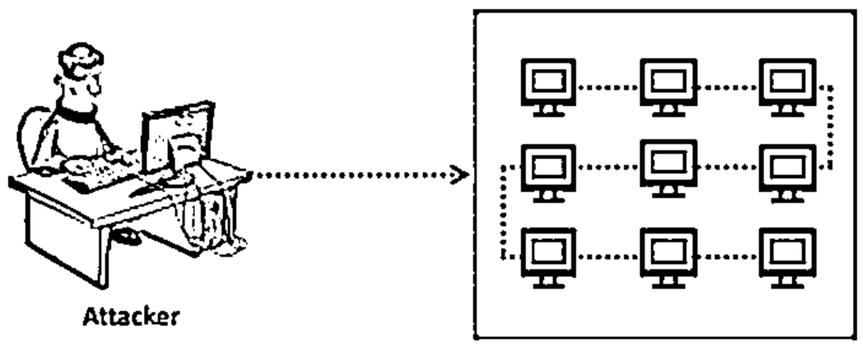
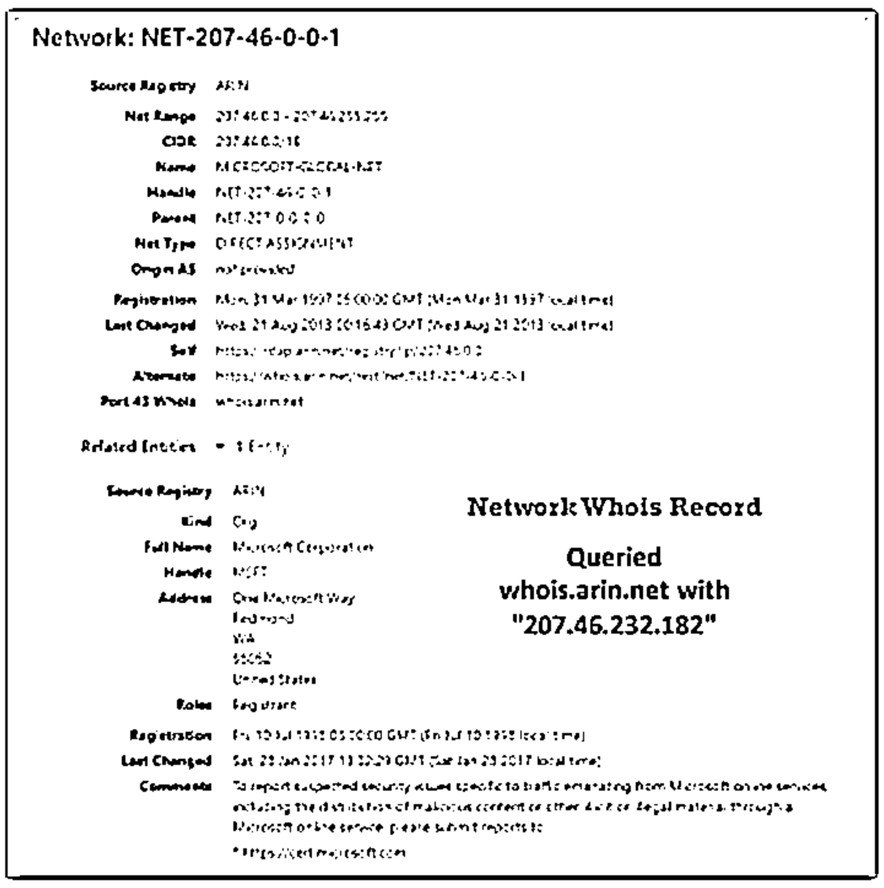


Figure 2.64: Screenshot of Reverse IP Domain Check

Locate the Network Range

- Network range information assists attackers in creating a map of the target network
- One can find the range of IP addresses using ARIN whois database search tool
- One can also find the range of IP addresses and the subnet mask used by the target organization from Regional Internet Registry (RIR)





Network: NET-207-46-0-0-1

Source Registry	ARIN
Net Range	207.46.0.0 - 207.46.255.255
CIDR	207.46.0.0/16
Name	MICROSOFT-GLOBAL-NET
Handle	NET-207-46-0-0-1
Parent	NET-207-0-0-0-0
Net Type	DIRECT ASSIGNMENT
Origin AS	not provided
Registration	Mon, 31 Mar 1997 05:00:00 GMT (Mon Mar 31 1997 local time)
Last Changed	Wed, 21 Aug 2013 20:16:43 GMT (Wed Aug 21 2013 local time)
Self	https://rdap.arin.net/registry/ip/207.46.0.0
Alternate	https://whois.arin.net/rest/net/NET-207-46-0-0-1
Port 43 Whois	whois.arin.net

Related Entities = 1 Entity

Source Registry	ARIN
Kind	Org
Full Name	Microsoft Corporation
Handle	MSFT
Address	One Microsoft Way Redmond WA 98052 United States
Roles	Registrant
Registration	Fri, 10 Jul 1992 04:00:00 GMT (Fri Jul 10 1992 local time)
Last Changed	Sat, 28 Jan 2017 13:32:29 GMT (Sat Jan 28 2017 local time)
Comments	To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illegal or abusive material through a Microsoft online service, please submit reports to: * https://cert.microsoft.com

Network Whois Record

Queried whois.arin.net with "207.46.232.182"

Network Footprinting

The next step after retrieving the DNS information is gathering network-related information. We will now discuss network footprinting, a method of gathering the footprint of the target organization's network. This section describes how to locate the network range, traceroute analysis, and traceroute tools.

Locate the Network Range

One needs to gather basic and important information about the target organization, such as what the organization does, who works there, and what type of work they do to perform network footprinting. The answers to these questions provide information about the internal structure of the target network.

After gathering the information, an attacker can proceed to find the network range of a target system. Detailed information is available from the appropriate regional registry database regarding IP allocation and the nature of the allocation. An attacker can also determine the subnet mask of the domain and trace the route between the system and the target system. Traceroute tools that are widely used include Path Analyzer Pro and VisualRoute.

Obtaining private IP addresses can be useful to attackers. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets: 10.0.0.0–10.255.255.255 (10/8 prefix), 172.16.0.0–172.31.255.255 (172.16/12 prefix), and 192.168.0.0–192.168.255.255 (192.168/16 prefix).

Using the network range, the attacker can get information about how the network is structured and which machines in the networks are alive. Using the network range also helps to identify the network topology, access control device, and OS used in the target network. To find the network range of the target network, one needs to enter the server IP address (that was gathered in Whois

footprinting) in the ARIN Whois database search tool. A user can also visit the ARIN website (*https://www.arin.net/about/welcome/region*) and enter the server IP in the **SEARCH Whois** text box. This gives the network range of the target network. Improperly set up DNS servers offer attackers a good chance of obtaining a list of internal machines on the server. In addition, sometimes, if an attacker traces a route to a machine, it is possible to obtain the internal IP address of the gateway, which can be useful.

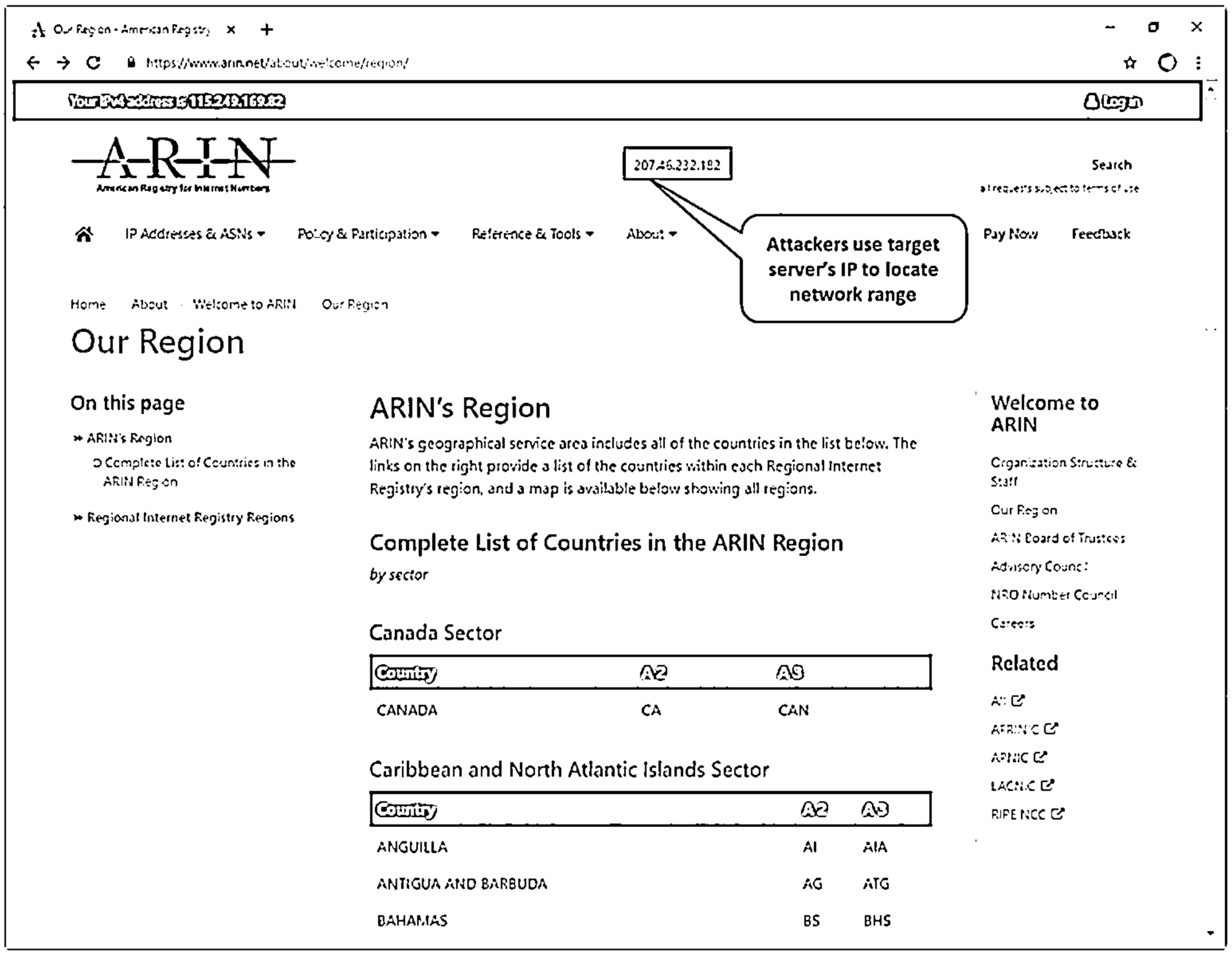


Figure 2.65: Screenshot of ARIN's Region

Network: NET-207-46-0-0-1

Source Registry	ARIN
Net Range	207.46.0.0 - 207.46.255.255
CIDR	207.46.0.0/16
Name	MICROSOFT-GLOBAL-NET
Handle	NET-207-46-0-0-1
Parent	NET-207-0-0-0-0
Net Type	DIRECT ASSIGNMENT
Origin AS	*not provided*
Registration	Mon, 31 Mar 1997 05:00:00 GMT (Mon Mar 31 1997 local time)
Last Changed	Wed, 21 Aug 2013 00:16:49 GMT (Wed Aug 21 2013 local time)
Self	https://rdap.arin.net/registry/ip/207.46.0.0
Alternate	https://whois.arin.net/rest/net/NET-207-46-0-0-1
Port 43 Whois	whois.arin.net

Related Entities ▾ 1 Entity

Source Registry	ARIN
Kind	Org
Full Name	Microsoft Corporation
Handle	MSFT
Address	One Microsoft Way Redmond WA 98052 United States
Roles	Registrant
Registration	Fri, 10 Jul 1998 03:00:00 GMT (Fri Jul 10 1998 local time)
Last Changed	Sat, 28 Jan 2017 13:32:29 GMT (Sat Jan 28 2017 local time)
Comments	To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to: * https://cert.microsoft.com.

Network Whois Record

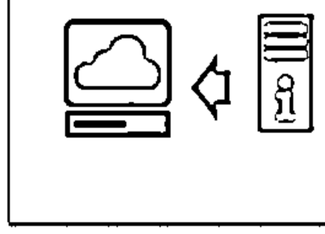
Queried whois.arin.net with "207.46.232.182"

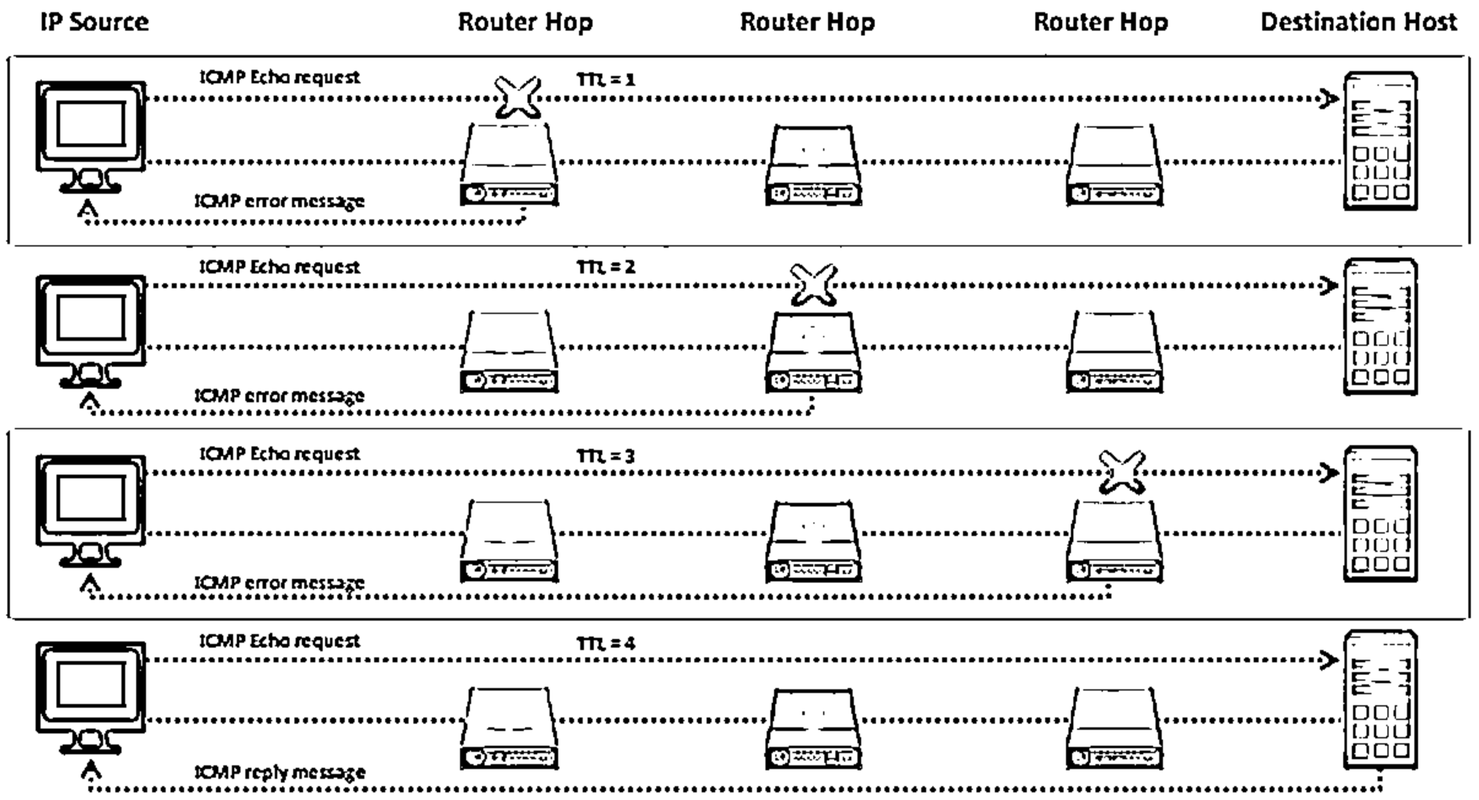
Figure 2.66: Screenshot showing result of ARIN Whois database search result

Attackers typically use more than one tool to obtain network information, as a single tool cannot provide all the required information.

Traceroute

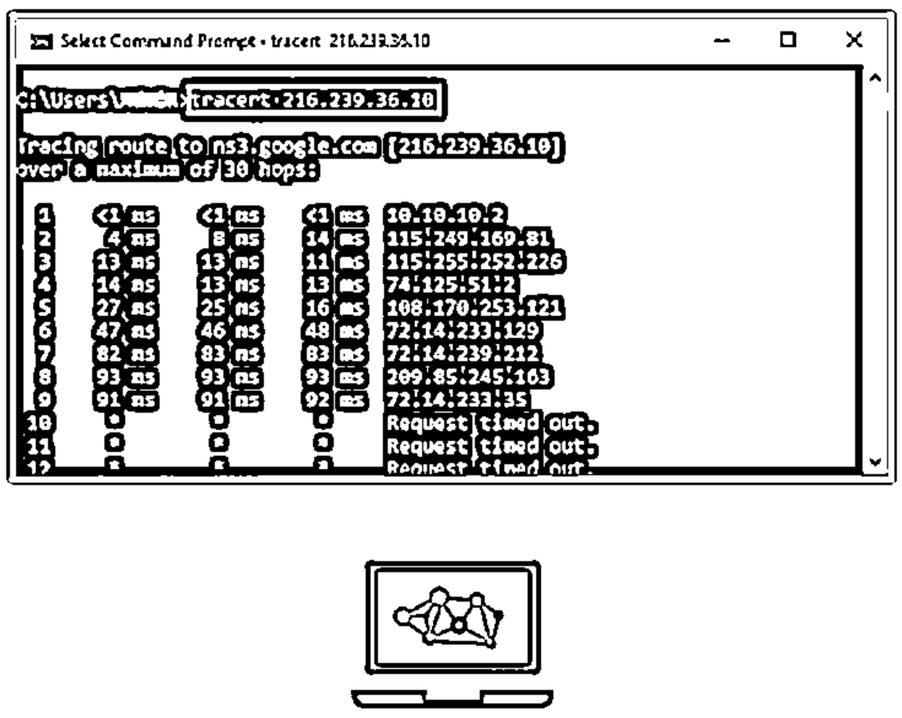
Traceroute programs work on the concept of ICMP protocol and use the TTL field in the header of ICMP packets to discover the routers on the path to a target host



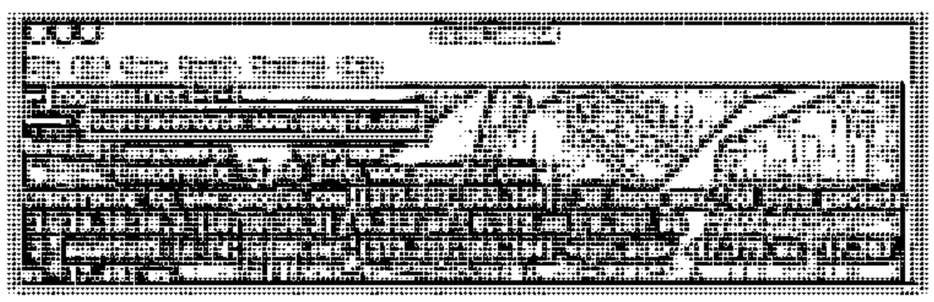


Traceroute (Cont'd)

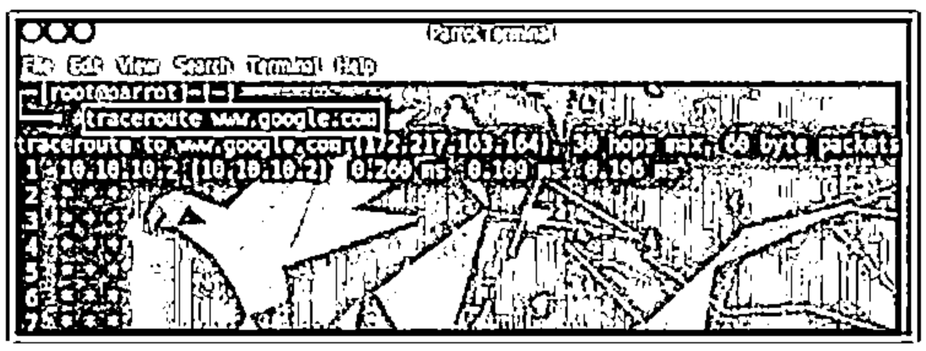
IMCP Traceroute



TCP Traceroute



UDP Traceroute



Traceroute

Finding the route of the target host on the network is necessary to test against man-in-the-middle attacks and other related attacks. Most operating systems come with a Traceroute utility to perform this task. It traces the path or route through which the target host packets travel in the network.

Traceroute uses the ICMP protocol concept and Time to Live (TTL) field of the IP header to find the path of the target host in the network.

The Traceroute utility can detail the path through which IP packets travel between two systems. The utility can trace the number of routers the packets travel through, the round-trip time (duration in transiting between two routers), and, if the routers have DNS entries, the names of the routers and their network affiliation. It can also trace geographic locations. It works by exploiting a feature of the Internet Protocol called TTL. The TTL field indicates the maximum number of routers a packet may traverse. Each router that handles a packet decrements the TTL count field in the ICMP header by one. When the count reaches zero, the router discards the packet and transmits an ICMP error message to the originator of the packet.

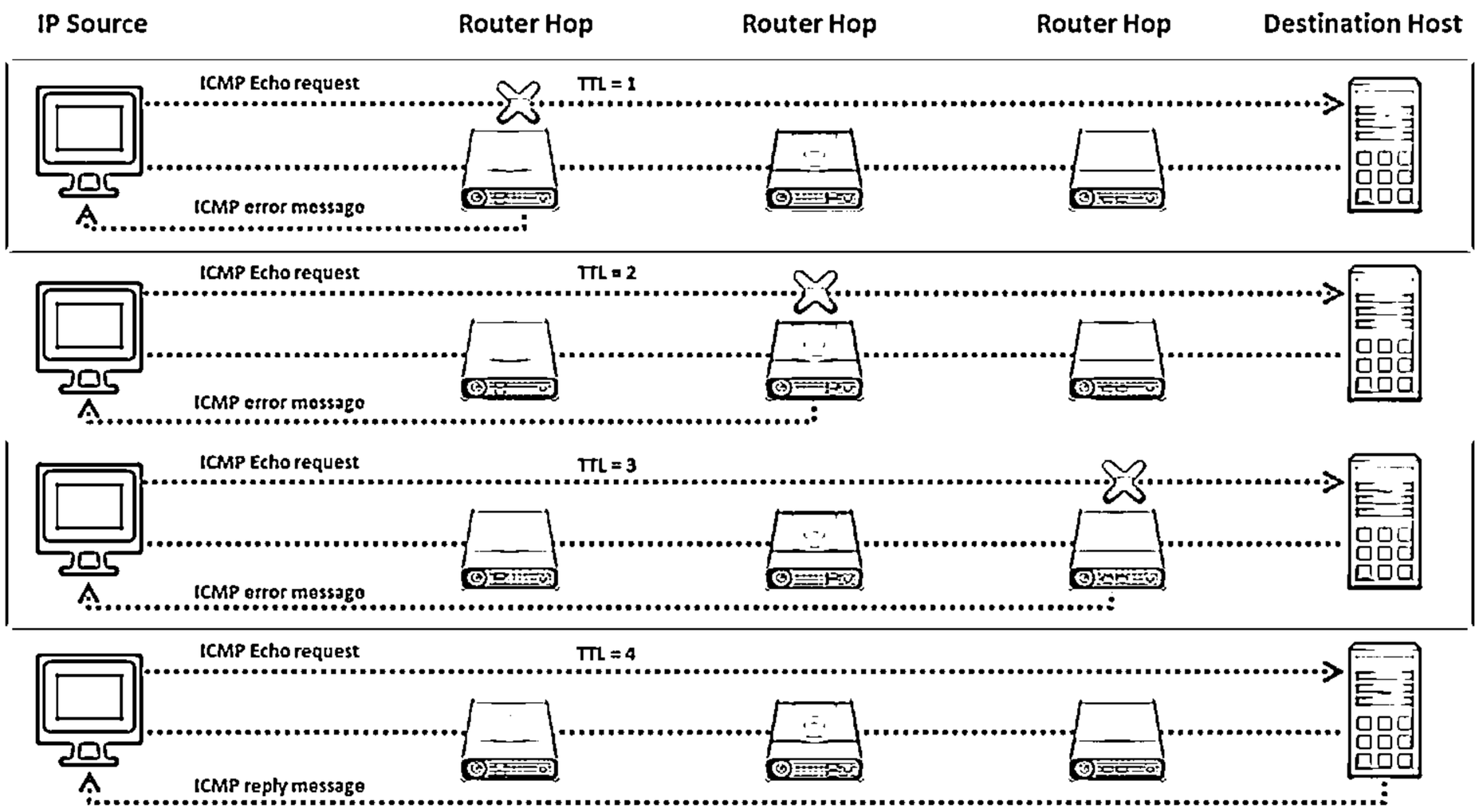


Figure 2.67: Illustration of Traceroute

The utility records the IP address and DNS name of the router and sends out another packet with a TTL value of two. This packet makes it through the first router and then times-out at the next router in the path. This second router also sends an error message back to the originating host. Traceroute continues to do this and records the IP address and name of each router until a packet finally reaches the target host or until it decides that the host is unreachable. In the process, it records the time taken for each packet to make a round trip to each router. Finally, when it reaches the destination, the normal ICMP ping response will be sent back to the sender. The utility helps to reveal the IP addresses of the intermediate hops in the route to the target host from the source.

ICMP Traceroute

Windows operating system by default uses ICMP traceroute. Go to the command prompt and type the **tracert** command along with the destination IP address or domain name as follows:

```
C:\>tracert 216.239.36.10

Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30
hops:
  1   <1 ms     <1 ms     <1 ms   10.10.10.2
  2   20 ms      4 ms      5 ms   1.6.15.234
  3   21 ms     19 ms     21 ms   100.66.8.23
  4   20 ms     19 ms     19 ms   100.68.8.23
  5   23 ms     41 ms     20 ms   72.14.210.200
  6   21 ms     21 ms     23 ms   108.170.248.163
  7   68 ms     67 ms     67 ms   209.85.242.115
  8  102 ms    102 ms    102 ms   209.85.247.194
  9  100 ms    106 ms    122 ms   72.14.239.175
 10  114 ms    119 ms    114 ms   209.85.244.31
 11  114 ms    112 ms    112 ms   209.85.247.118
 12  114 ms    118 ms    115 ms   74.125.253.85
 13  111 ms    112 ms    113 ms   ns3.google.com [216.239.36.10]
Trace complete.
```

TCP Traceroute

Many devices in any network are generally configured to block ICMP traceroute messages. In this scenario, an attacker uses TCP or UDP traceroute, which is also known as Layer 4 traceroute. Go to the terminal in Linux operating system and type the **tcptraceroute** command along with the destination IP address or domain name as follows:

```
tcptraceroute www.google.com
```

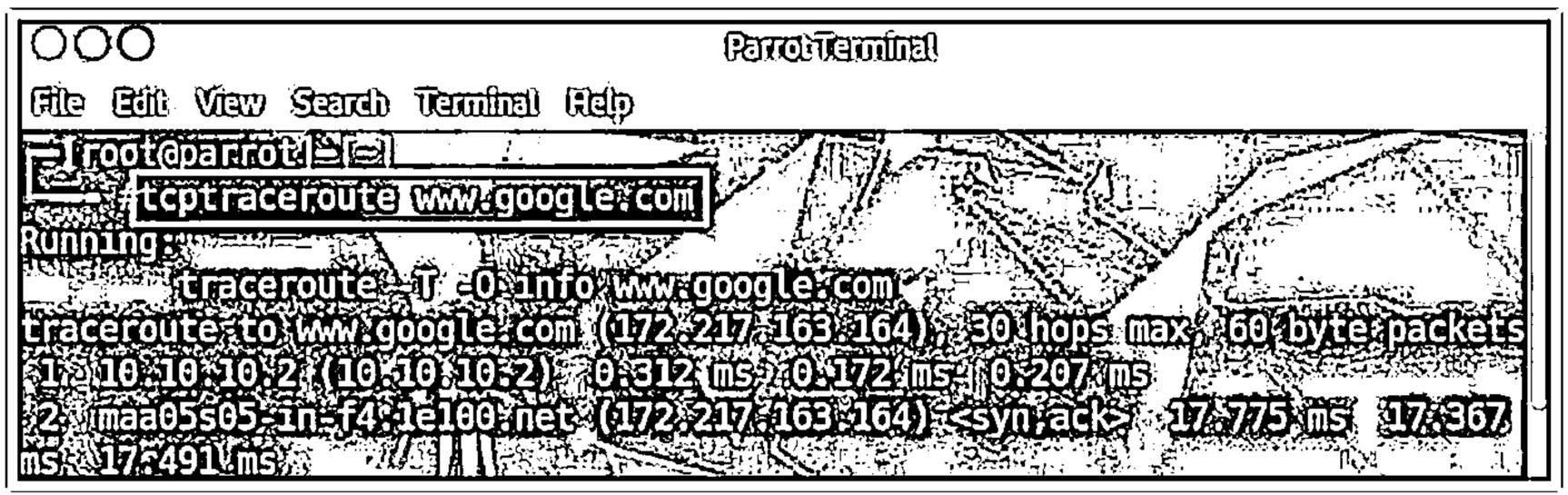


Figure 2.68: Screenshot showing the output of TCP Traceroute

UDP Traceroute

Like Windows, Linux also has a built-in traceroute utility, but it uses the UDP protocol for tracing the route to the destination. Go to the terminal in the Linux operating system and type the **traceroute** command along with the destination IP address or domain name as follows:

```
traceroute www.google.com
```

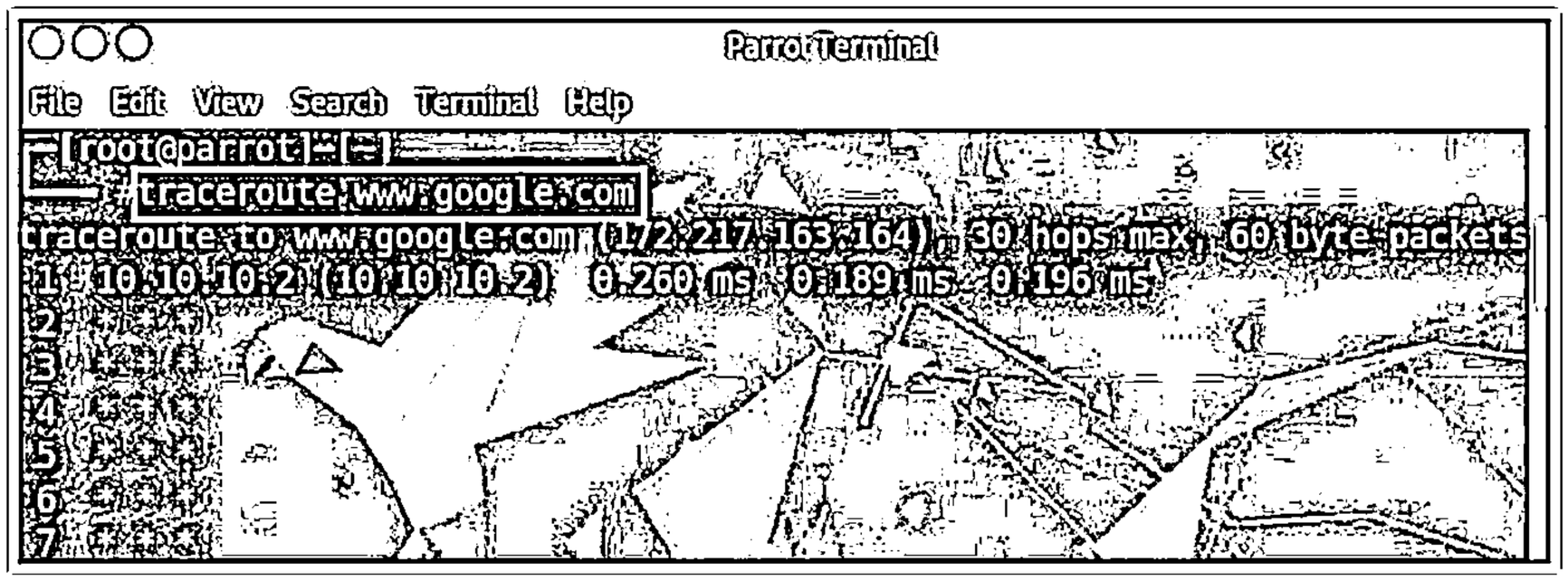
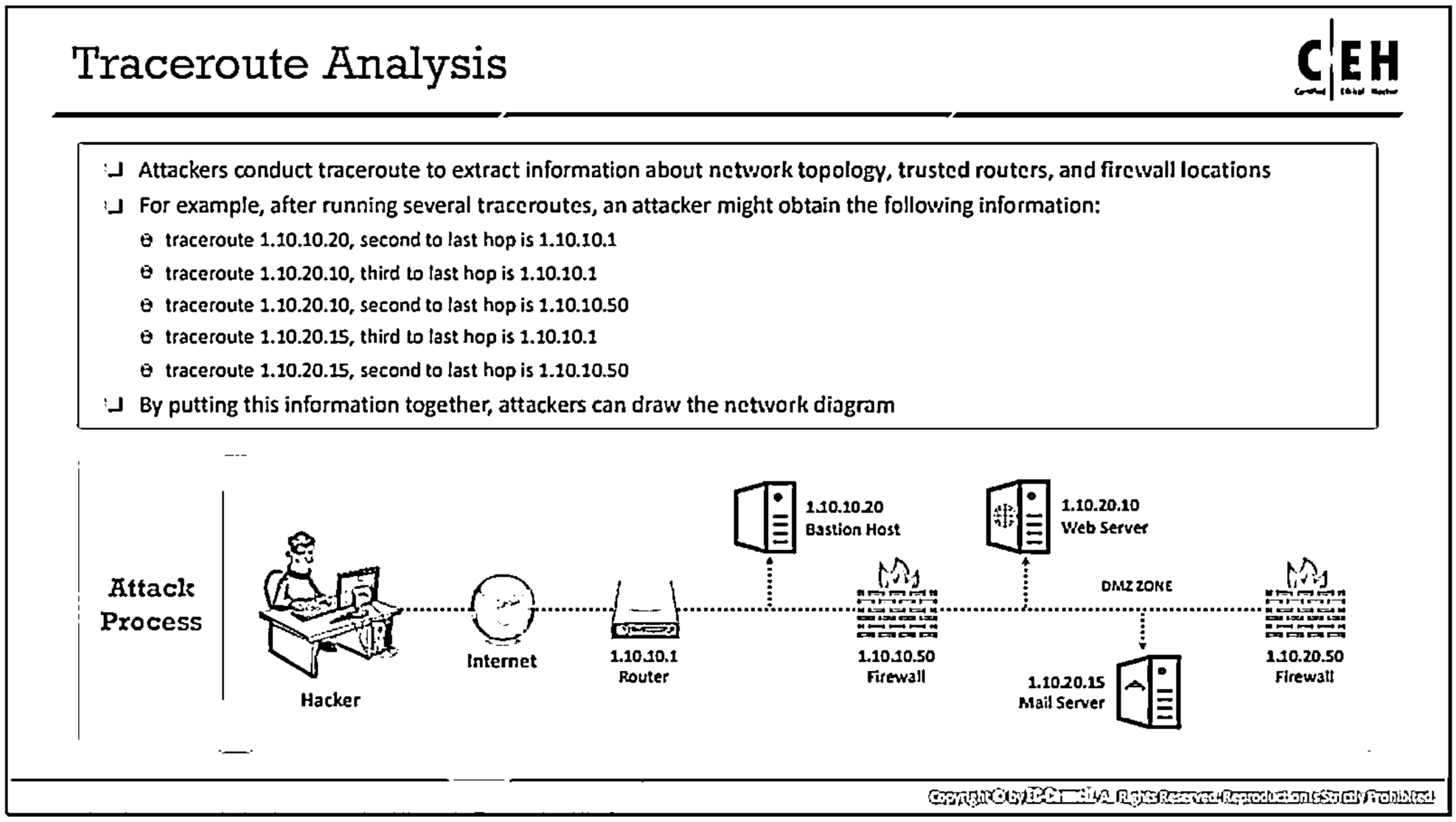


Figure 2.69: Screenshot showing the output of UDP Traceroute



Traceroute Analysis

We have seen how the Traceroute utility helps to find the IP addresses of intermediate devices such as routers and firewalls present between a source and its destination. After running several traceroutes, an attacker will be able to find the location of a hop in the target network. Consider the following traceroute results obtained:

- `traceroute 1.10.10.20, second to last hop is 1.10.10.1`
- `traceroute 1.10.20.10, third to last hop is 1.10.10.1`
- `traceroute 1.10.20.10, second to last hop is 1.10.10.50`
- `traceroute 1.10.20.15, third to last hop is 1.10.10.1`
- `traceroute 1.10.20.15, second to last hop is 1.10.10.50`

By analyzing these results, an attacker can draw the network topology diagram of the target network, as shown below.

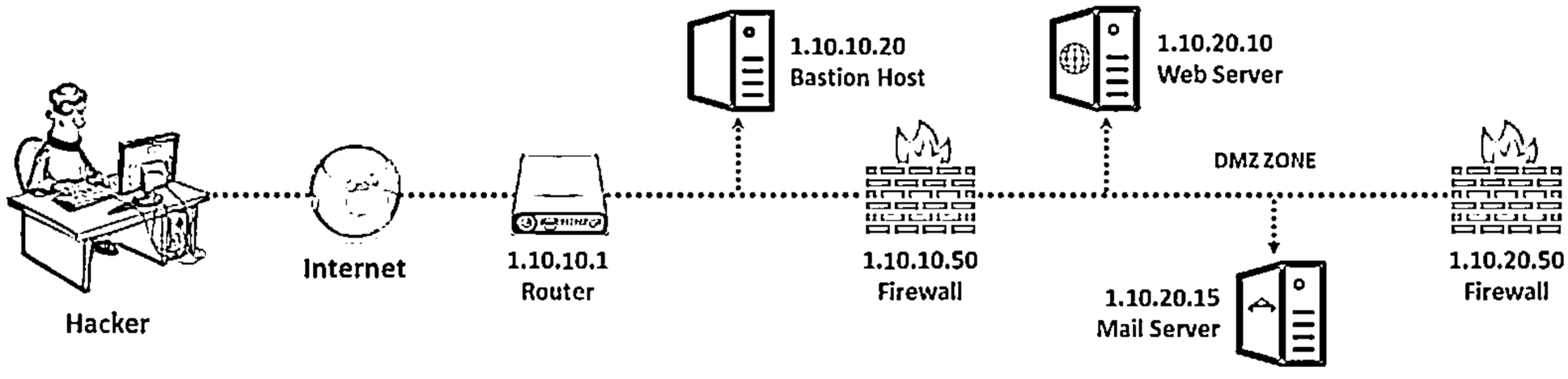
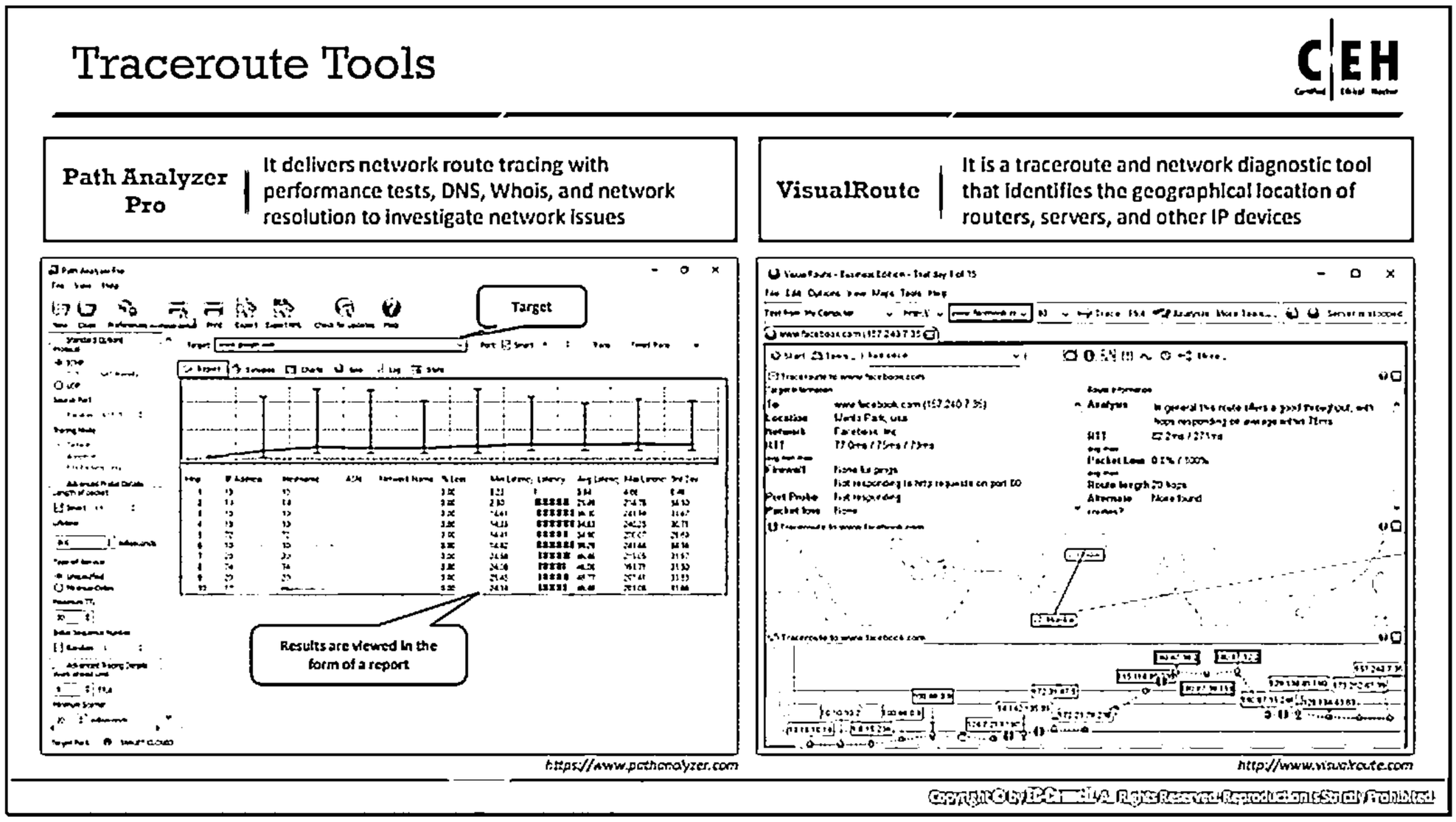


Figure 2.70: Traceroute Analysis



Traceroute Tools

Traceroute tools such as Path Analyzer Pro, VisualRoute, Traceroute NG, and PingPlotter are useful for extracting information about the geographical location of routers, servers, and IP devices in a network. Such tools help us to trace, identify, and monitor the network activity on a world map. Some of the features of these tools are as follows:

- Hop-by-hop traceroutes
- Reverse tracing
- Historical analysis
- Packet loss reporting
- Reverse DNS
- Ping plotting
- Port probing
- Detect network problems
- Performance metrics analysis
- Network performance monitoring
- **Path Analyzer Pro**

  Source: *https://www.pathanalyzer.com*

  Path Analyzer Pro performs network route tracing with performance tests, DNS, Whois, and network resolution to investigate network issues.

  Attackers use Path Analyzer Pro to identify the route from the source to destination target systems graphically. As shown in the screenshot, this tool helps attackers to gather information such as the hop number, its IP address, hostname, ASN, network name, percentage loss, latency, average latency, and standard deviation for each hop in the path.

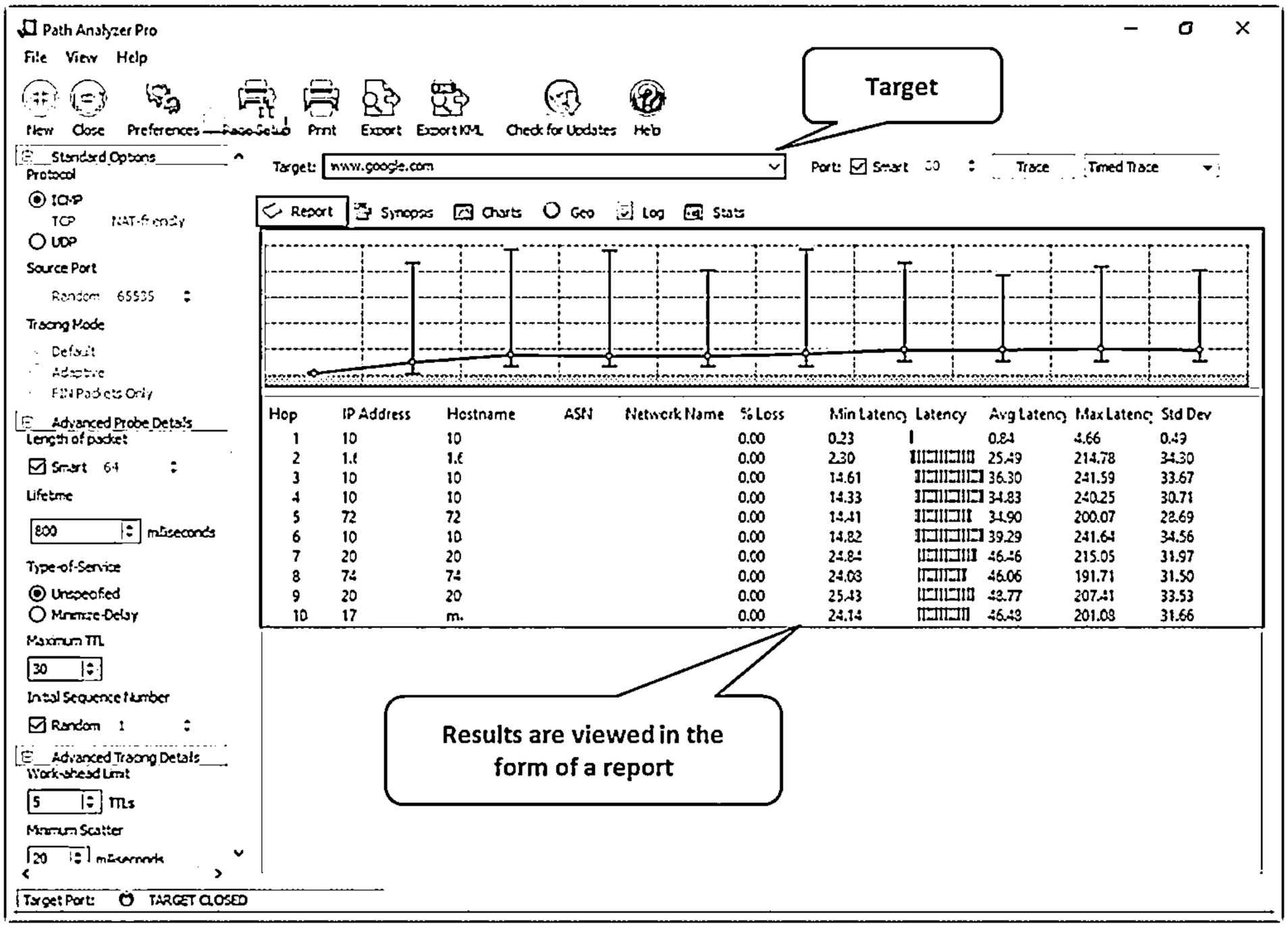


Figure 2.71: Screenshot of Path Analyzer Pro

- **VisualRoute**

  Source: *http://www.visualroute.com*

  VisualRoute is a traceroute and network diagnostic tool. Attackers use VisualRoute to identify the geographical location of routers, servers, and other IP devices in the target network.

  This tool helps attackers in tracking the path between the source and destination systems and obtaining the results in a graphical format. As shown in the screenshot, using VisualRoute tool enables attackers to gather information such as hop number, IP address, node name, and geographical location of each hop in the route.

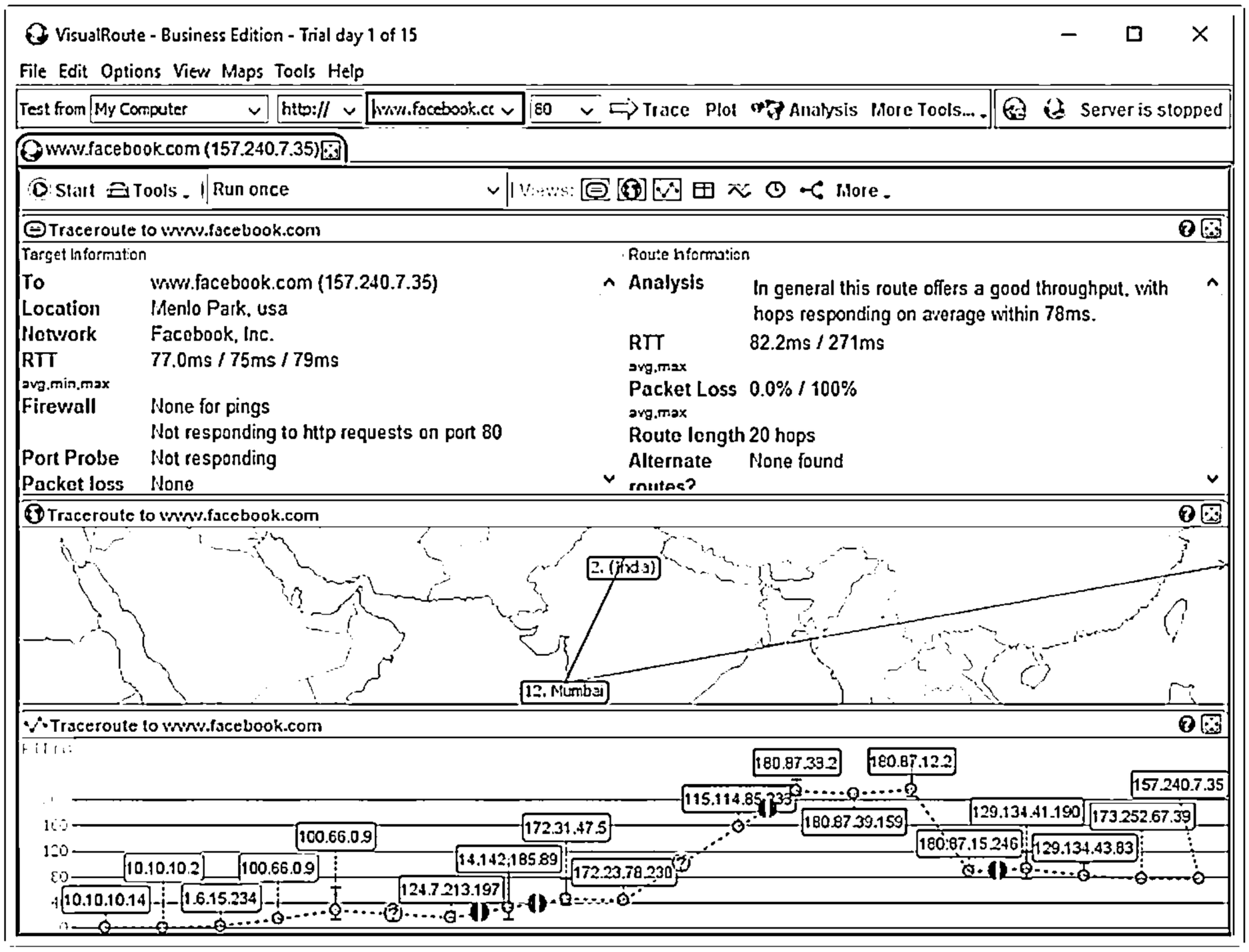
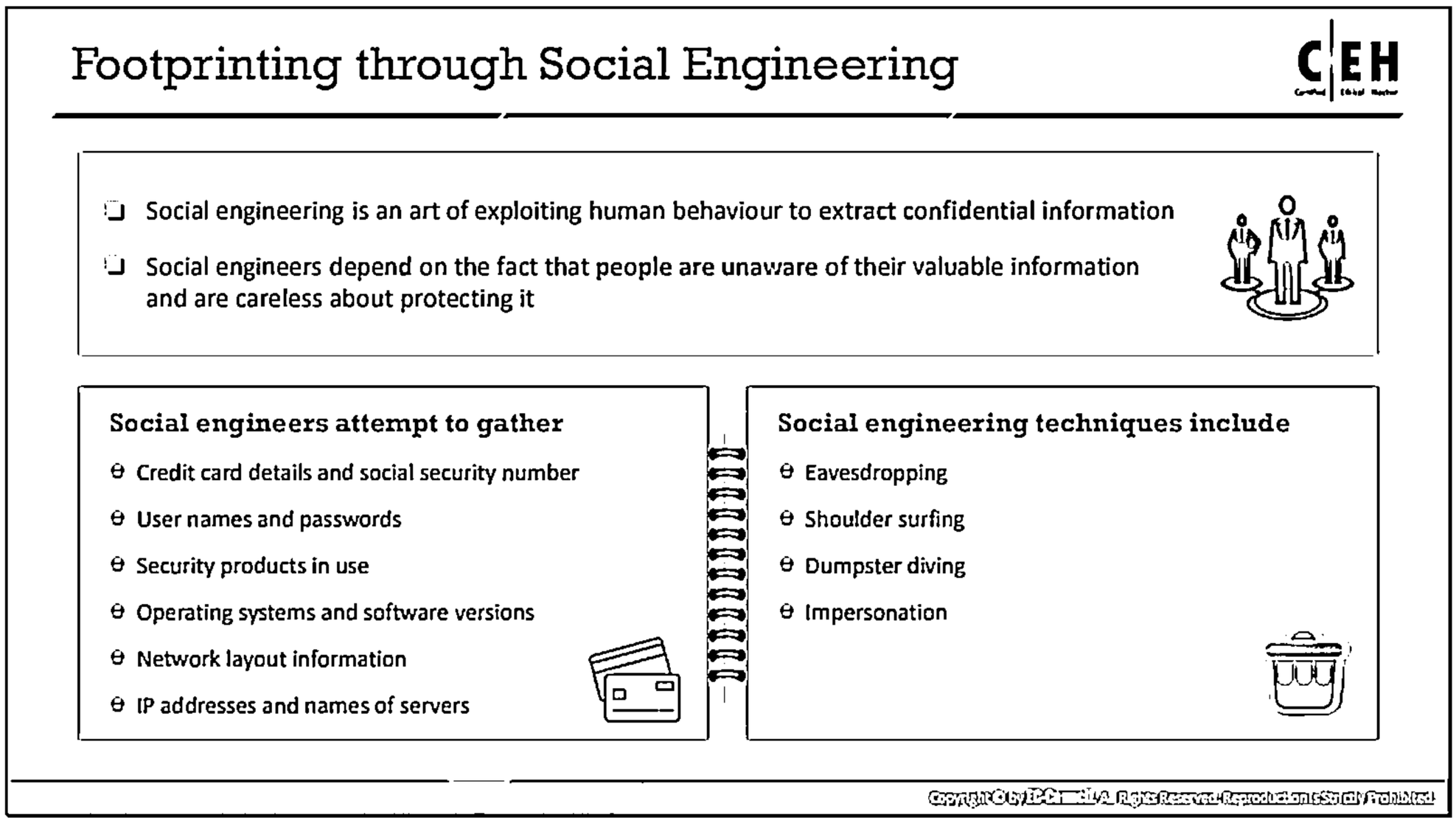


Figure 2.72: Screenshot of VisualRoute



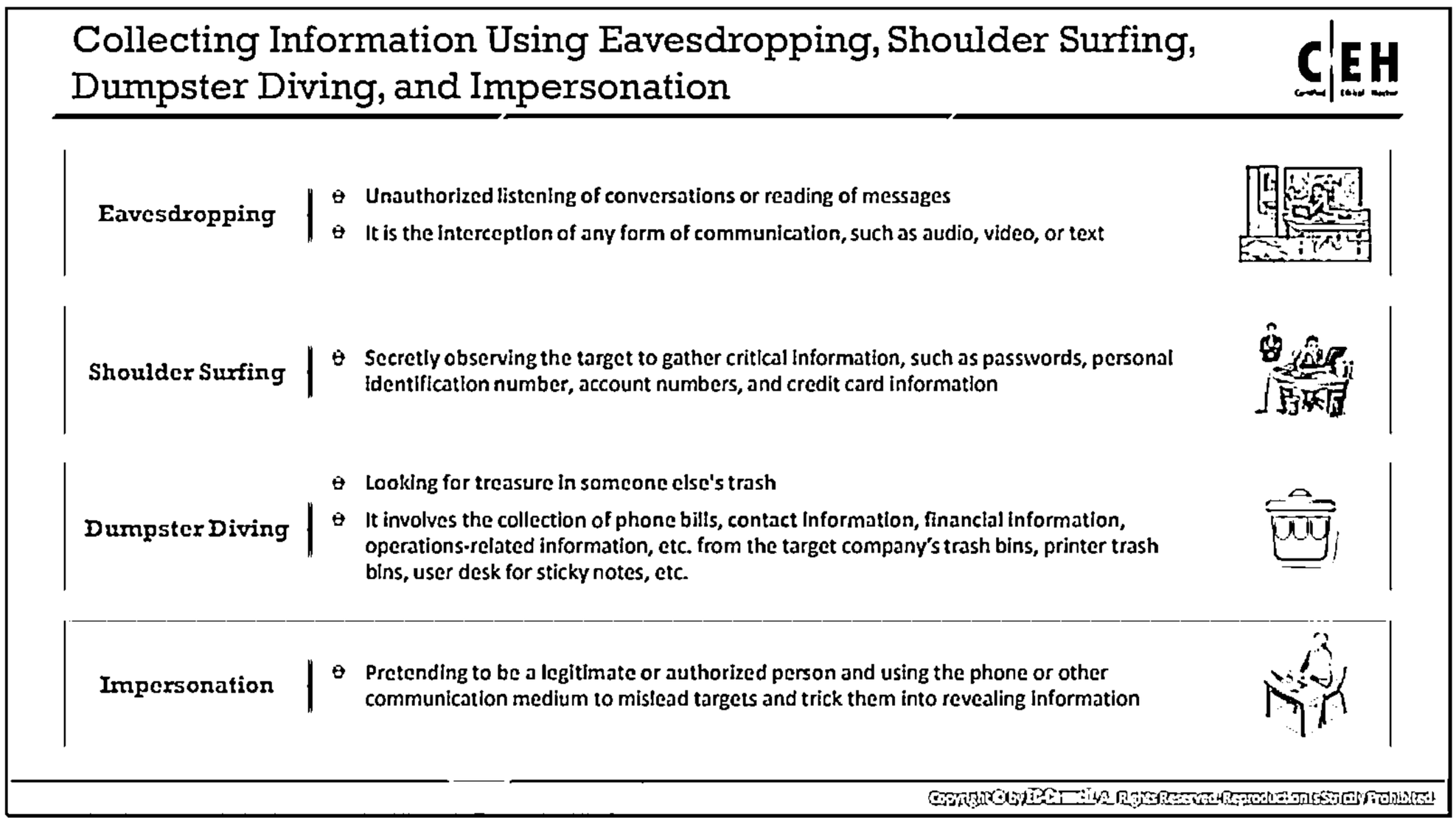
Footprinting through Social Engineering

So far, we have discussed the different techniques for gathering information using online resources or tools. Now, we will discuss footprinting through social engineering, i.e., the art of obtaining information from people by exploiting their weaknesses. This section covers the concept as well as the techniques used to gather information through social engineering.

Social engineering is a non-technical process in which an attacker misleads a person into providing confidential information inadvertently. In other words, the target is unaware of the fact that someone is stealing confidential information. The attacker takes advantage of the gullible nature of people and their willingness to provide confidential information.

To perform social engineering, an attacker first needs to gain the confidence of an authorized user and then mislead that user into revealing confidential information. The goal of social engineering is to obtain the required confidential information and then use that information for malicious purposes such as gaining unauthorized access to the system, identity theft, industrial espionage, network intrusion, fraud, and so on. The information obtained through social engineering may include credit card details, social security numbers, usernames and passwords, other personal information, security products in use, OS and software versions, IP addresses, names of servers, network layout information, and so on.

Social engineering can be performed in many ways, such as eavesdropping, shoulder surfing, dumpster diving, impersonation, tailgating, third-party authorization, piggybacking, reverse social engineering, and so on.



Collecting Information Using Eavesdropping, Shoulder Surfing, Dumpster Diving, and Impersonation

Eavesdropping, shoulder surfing, dumpster diving, and impersonation are social engineering techniques that are widely used to collect information from people.

- **Eavesdropping**

  Eavesdropping is the act of secretly listening to the conversations of people over a phone or video conference without their consent. It also includes reading confidential messages from communication media, such as instant messaging or fax transmissions. It is the act of intercepting communication in any form such as audio, video, or text without the consent of the communicating parties. The attacker gains information by tapping phone conversations or intercepting audio, video, or written communication.

- **Shoulder Surfing**

  Shoulder surfing is a technique whereby attackers secretly observe the target to gain critical information. In the shoulder surfing technique, an attacker stands behind the victim and secretly observes the victim's activities on the computer, such as keystrokes while entering usernames, passwords, and so on. The technique is effective in gaining passwords, personal identification numbers, security codes, account numbers, credit card information, and similar data. Attackers can easily perform shoulder surfing in a crowded place, as it is relatively easy to stand behind and watch the victim without his or her knowledge.

- **Dumpster Diving**

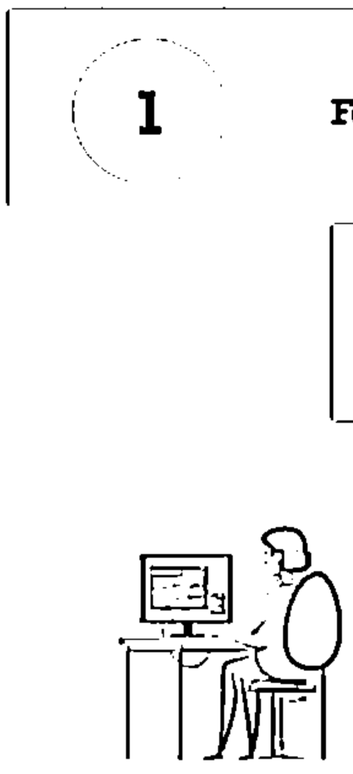
  This uncouth technique, also known as trashing, involves the attacker rummaging for information in garbage bins. The attacker may gain vital information such as phone bills,

contact information, financial information, operations-related information, printouts of source codes, printouts of sensitive information, and so on from the target company's trash bins, printer waste bins, sticky notes at users' desks, and so on. The attacker may also gather account information from ATM trash bins. The information can help the attacker to commit attacks.

- **Impersonation**

  Impersonation is a technique whereby an attacker pretends to be a legitimate or authorized person. Attackers perform impersonation attacks personally or use phones or other communication media to mislead targets and trick them into revealing information. The attacker might impersonate a courier/delivery person, janitor, businessman, client, technician, or he/she may pretend to be a visitor. Using this technique, an attacker gathers sensitive information by scanning terminals for passwords, searching important documents on desks, rummaging bins, and so on. The attacker may even try to overhear confidential conversations and "shoulder surf" to obtain sensitive information.

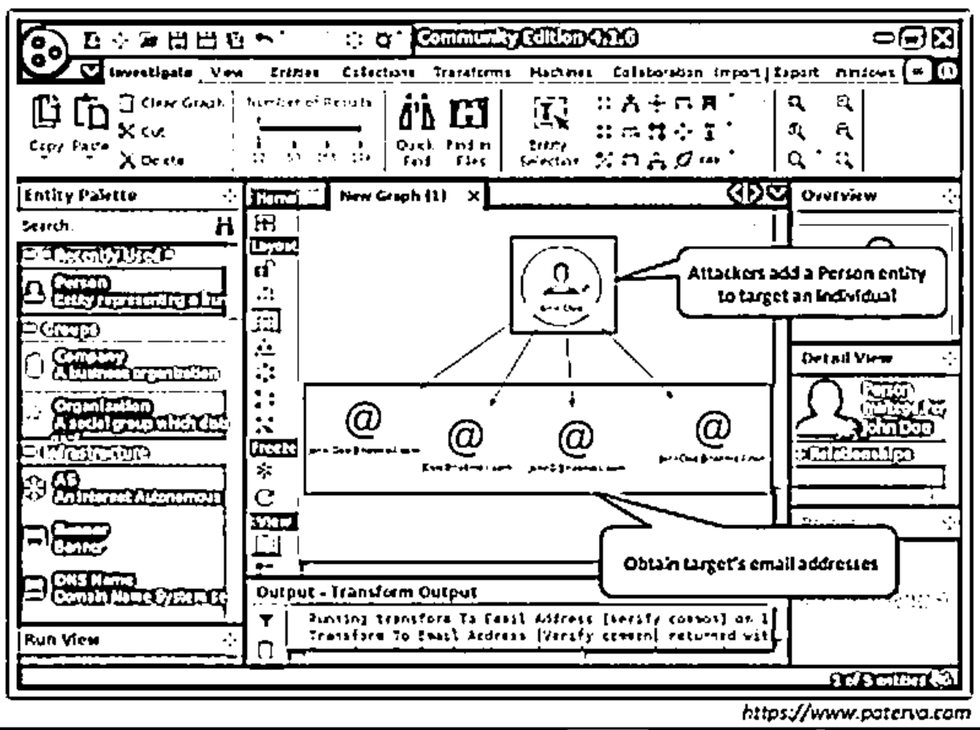
Module Flow



1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures

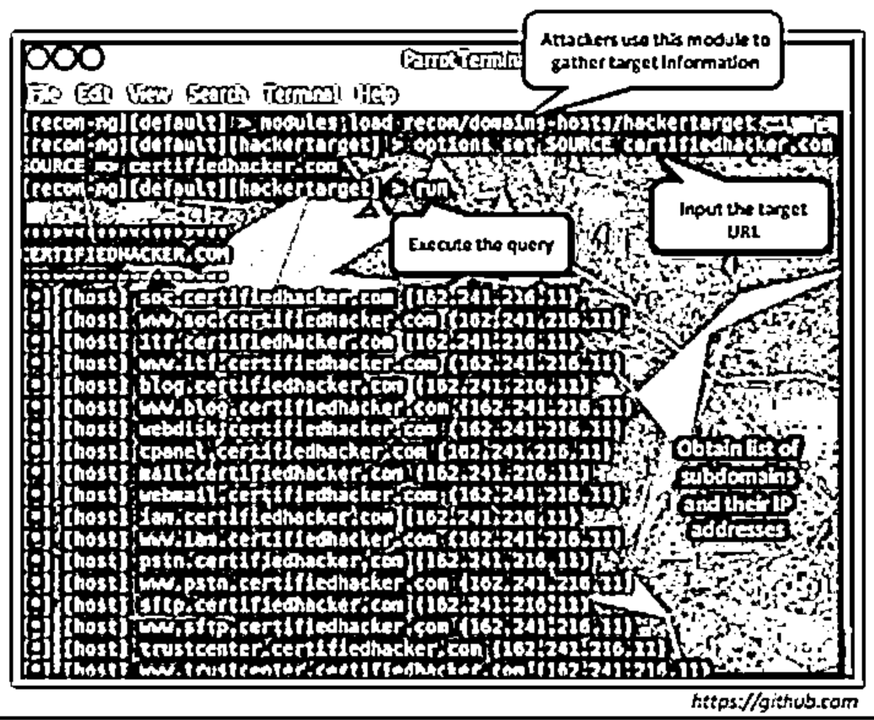
Footprinting Tools: Maltego and Recon-ng

Maltego | Maltego can be used to determine the relationships and real world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.



https://www.paterva.com

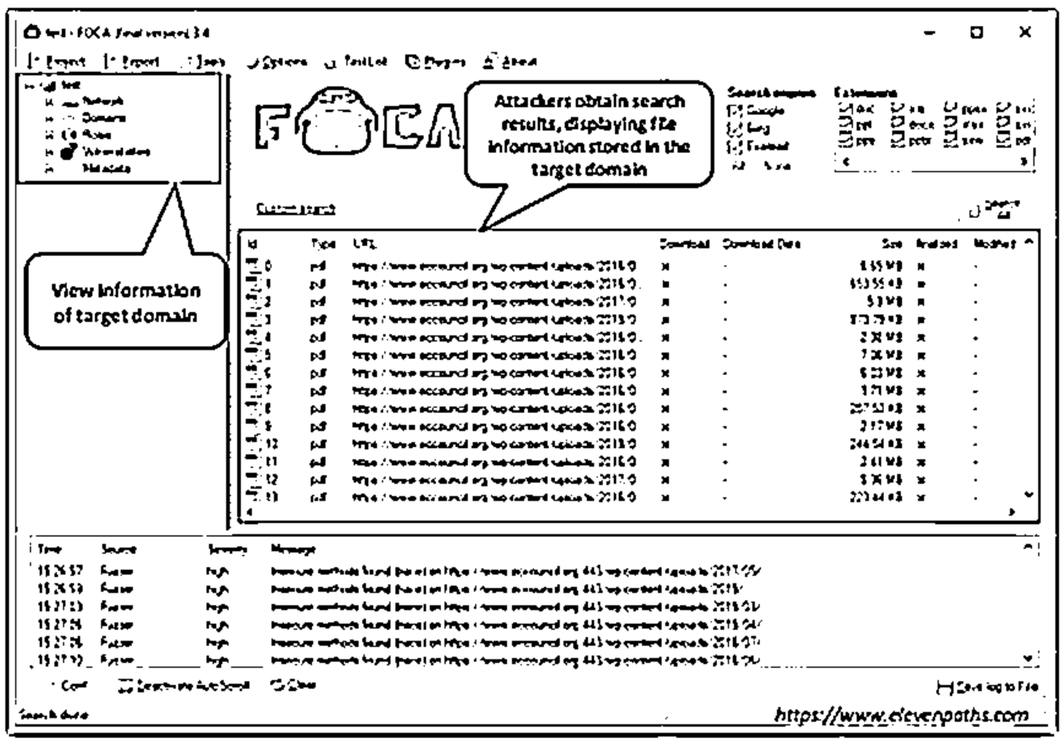
Recon-ng | Recon-ng is a Web Reconnaissance framework with independent modules and database interaction, which provides an environment in which open source, web-based reconnaissance can be conducted



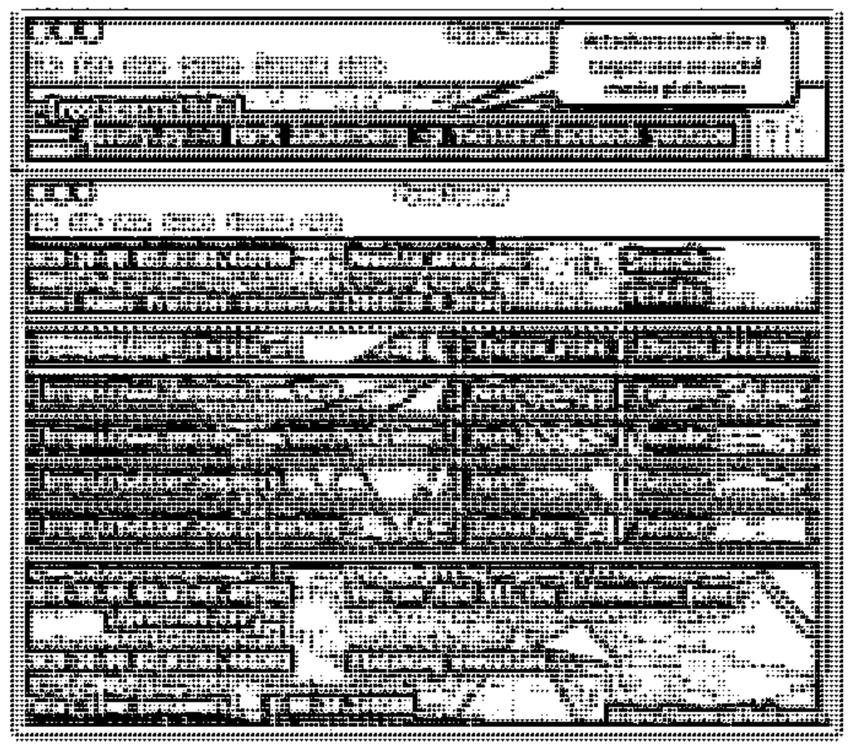
https://github.com

Footprinting Tools: FOCA and OSRFramework

FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents it scans



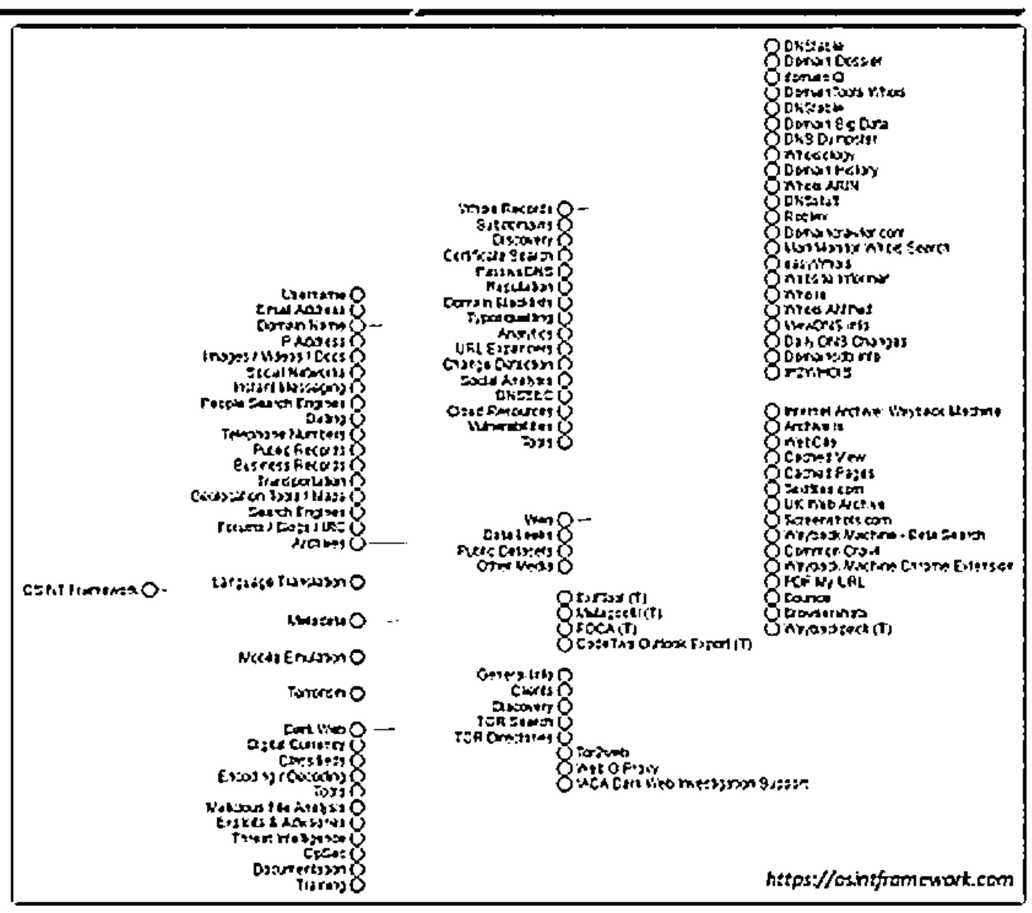
OSRFramework includes applications related to username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, etc.

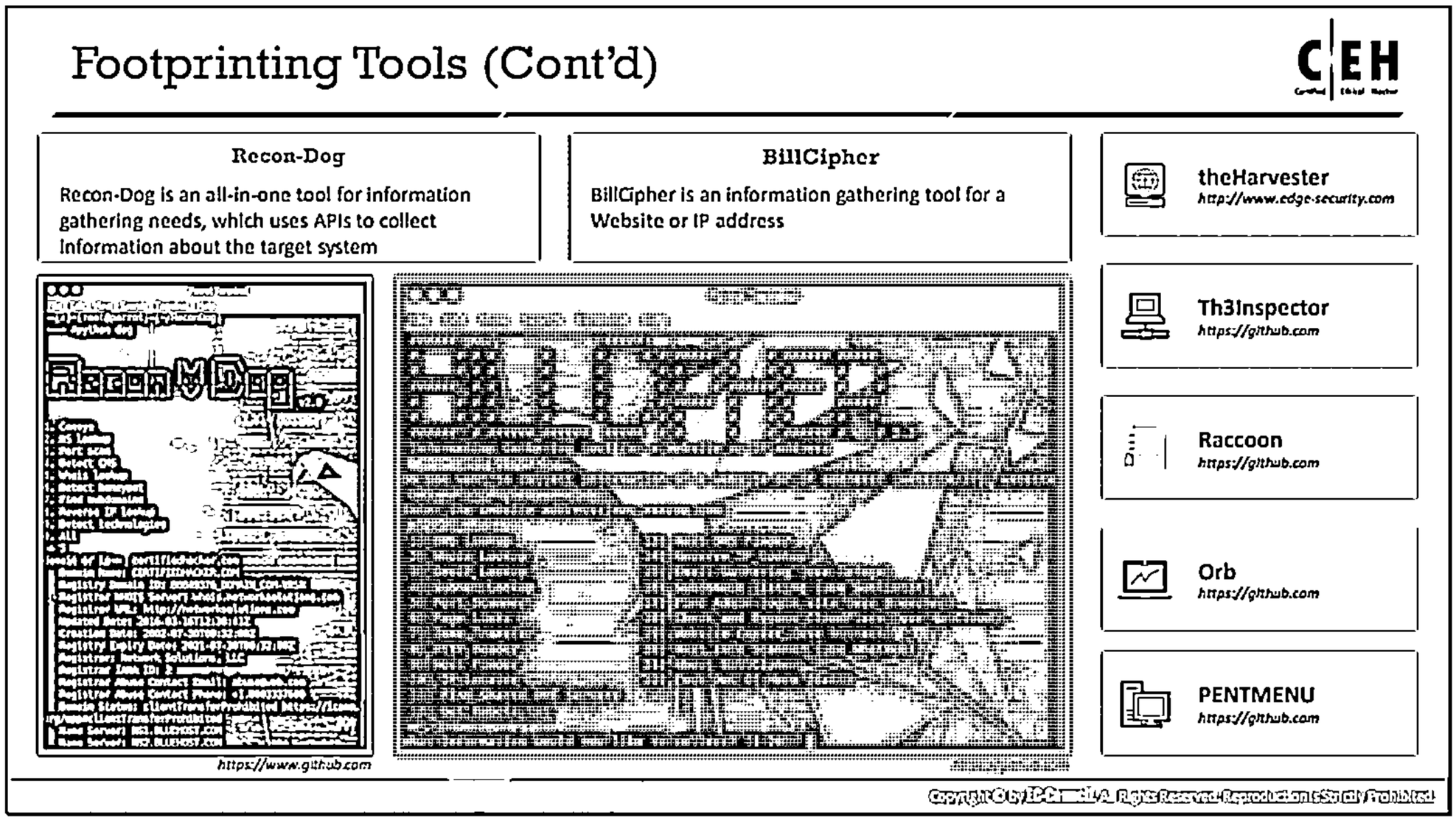


Footprinting Tools: OSINT Framework

OSINT Framework

- OSINT Framework is an open source intelligence gathering framework that is focused on gathering information from free tools or resources
- It provides a simple web interface that lists various OSINT tools arranged by categories and is shown as OSINT tree structure on the web interface
- Tools listed includes the following indicators:
  - (T) - Indicates a link to a tool that must be installed and run locally
  - (D) - Google Dork
  - (R) - Requires registration
  - (M) - Indicates a URL that contains the search term and the URL itself must be edited manually





Footprinting Tools

Various tools help attackers in footprinting. Many organizations offer tools that make information gathering an easy task. This section describes tools intended for obtaining information from various sources.

Footprinting tools are used to collect basic information about target systems to exploit them. Information collected by the footprinting tools includes the target's IP location information, routing information, business information, address, phone number and social security number, details about a source of an email and a file, DNS information, domain information, and so on.

- **Maltego**

  Source: *https://www.paterva.com*

  Maltego is a program that can be used to determine the relationships and real-world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.

  Attackers can use different entities available in the tool to obtain information such as email addresses, a list of phone numbers, and a target's Internet infrastructure (domains, DNS names, Netblocks, IP addresses information).

  As shown in the screenshot, attackers add a **`Person entity`**, rename it with the target's name, and obtain the email addresses associated with the target.

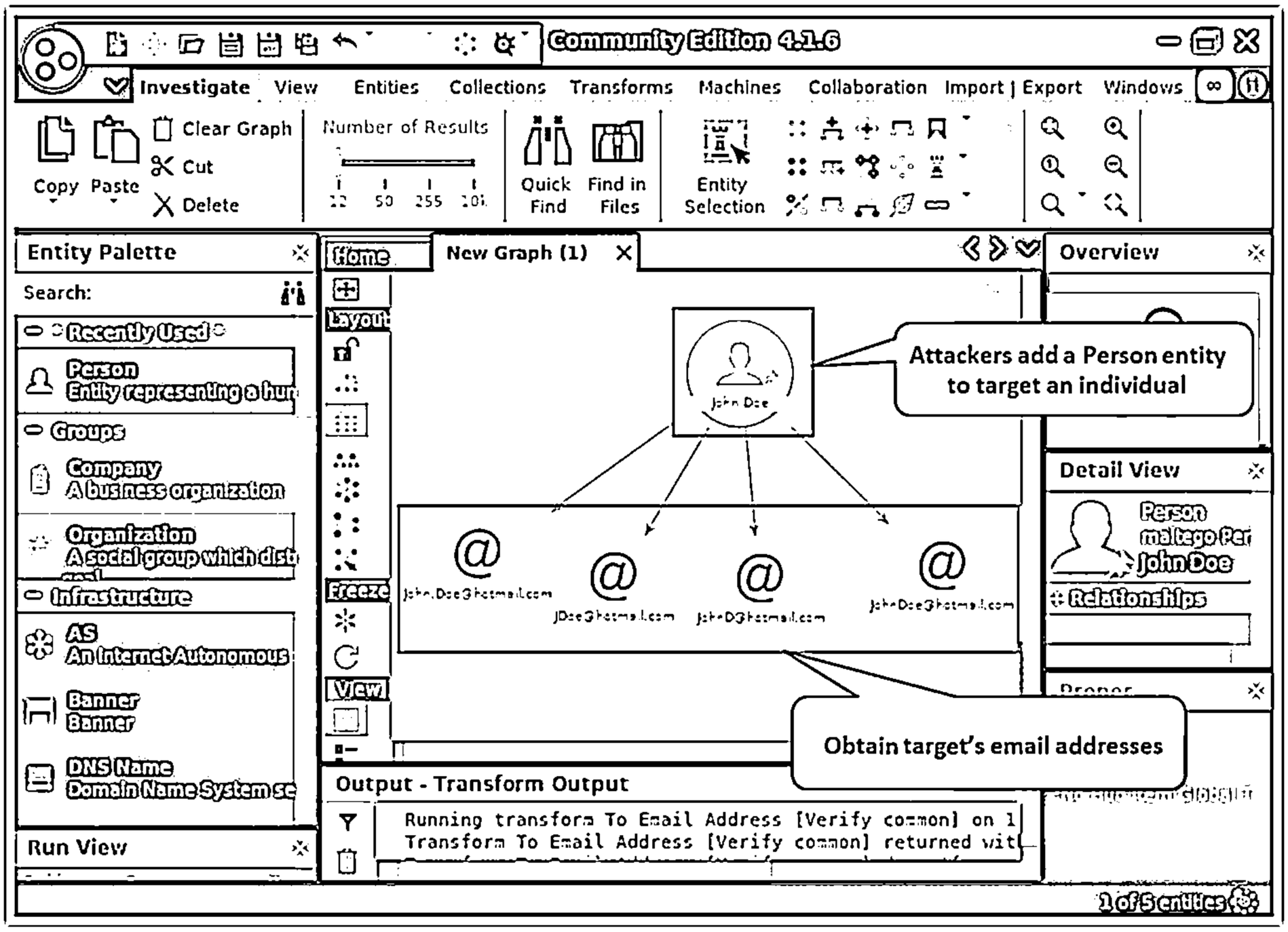


Figure 2.73: Screenshot of Maltego

- **Recon-ng**

  Source: *https://github.com*

  Recon-ng is a web reconnaissance framework with independent modules for database interaction that provides an environment in which open-source web-based reconnaissance can be conducted.

  As shown in the screenshot, attackers use the module **`recon/domains-hosts/hackertarget`** to extract a list of subdomains and IP addresses associated with the target URL.

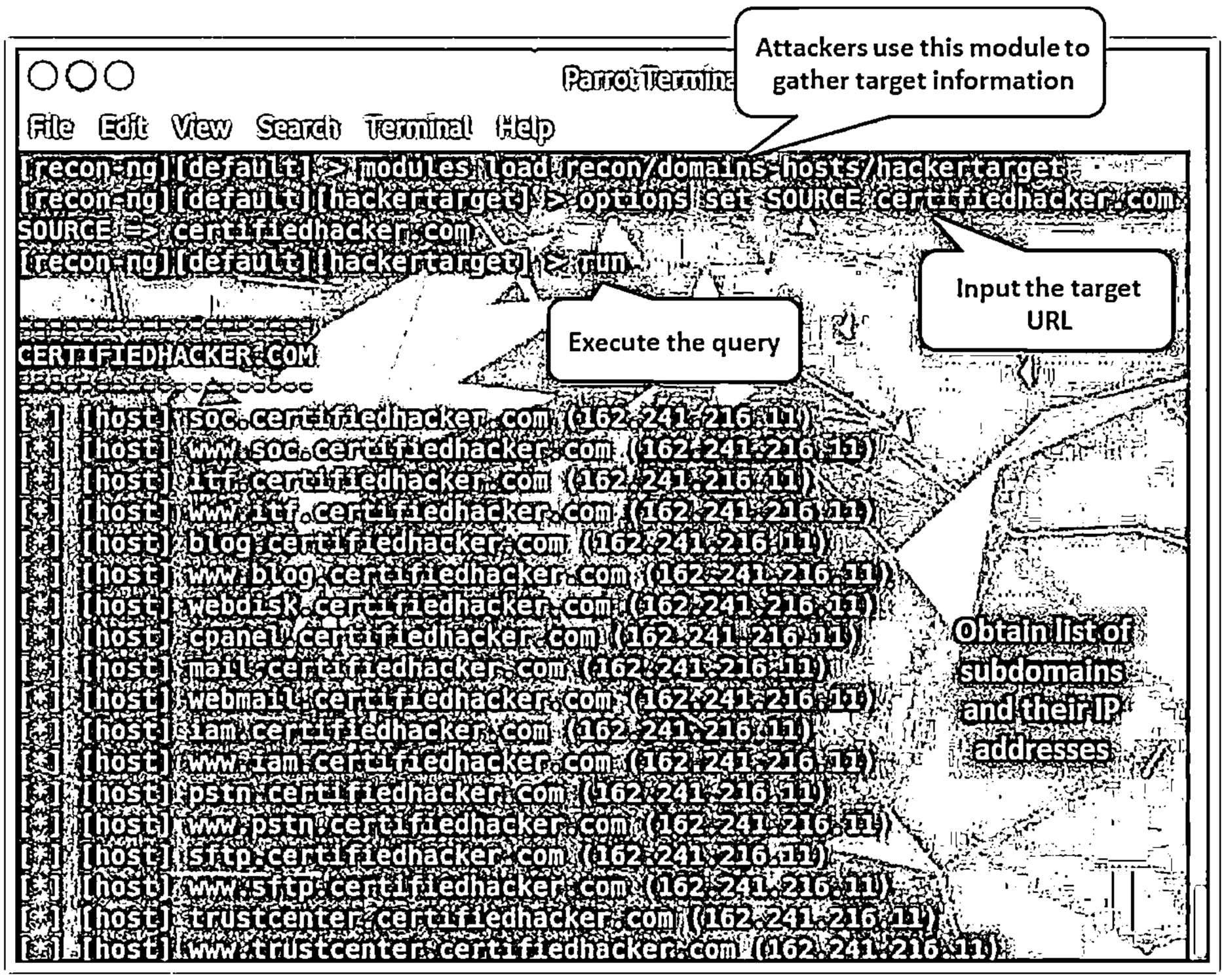


Figure 2.74: Screenshot of recon-ng

- **FOCA**

  Source: *https://www.elevenpaths.com*

  Fingerprinting Organizations with Collected Archives (FOCA) is a tool used mainly to find metadata and hidden information in the documents that its scans. FOCA is capable of scanning and analyzing a wide variety of documents, with the most common ones being Microsoft Office, Open Office, or PDF files.

Features:

- **Web Search** - Searches for hosts and domain names through URLs associated with the main domain. Each link is analyzed to extract information from its new host and domain names.
- **DNS Search** - Checks each domain to ascertain the host names configured in NS, MX, and SPF servers to discover the new host and domain names.
- **IP Resolution** - Resolves each host name by comparison with the DNS to obtain the IP address associated with this server name. To perform this task accurately, the tool performs analysis against the organization's internal DNS.
- **PTR Scanning** - Finds more servers in the same segment of a determined address; IP FOCA executes a PTR log scan.
- **Bing IP** - Launches FOCA, which is a search process for new domain names associated with that IP address for each IP address discovered.
- **Common Names** - Perform dictionary attacks against the DNS.

As shown in the screenshot, attackers search the target domain and obtain the file information stored in it. The extracted files can be viewed on the web browser. Further, the attackers can view additional information such as network domains, roles, vulnerabilities, and metadata of the target domain.

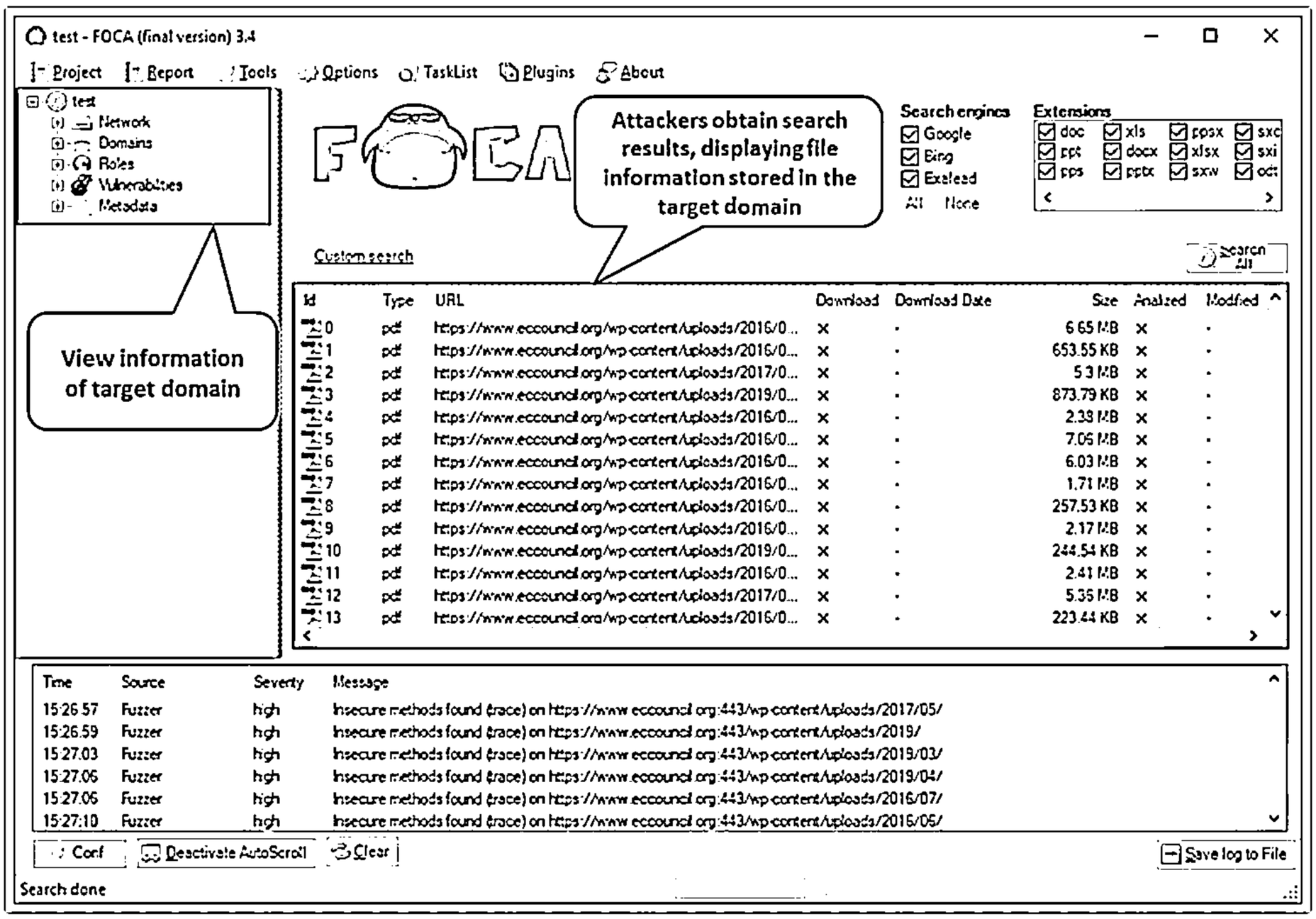


Figure 2.75: Screenshot of FOCA

- **OSRFramework**

  Source: *https://github.com*

  OSRFramework includes applications related to username checking, DNS lookups, information leaks research, deep web search, and regular expression extraction.

  The tools included in the OSRFramework package that attackers can use to gather information on the target are listed below:

  - **usufy.py** - Checks for a user profile on up to 290 different platforms
  - **mailfy.py** - Check for the existence of a given email
  - **searchfy.py** - Performs a query on the platforms in OSRFramework
  - **domainfy.py** - Checks for the existence of domains
  - **phonefy.py** - Checks for the existence of a given series of phones
  - **entify.py** - Uses regular expressions to extract entities

  As shown in the screenshot, attackers use the following command to search for a target user on social media platforms,

  ```
  usufy.py -n Mark Zuckerberg -p twitter facebook youtube
  ```

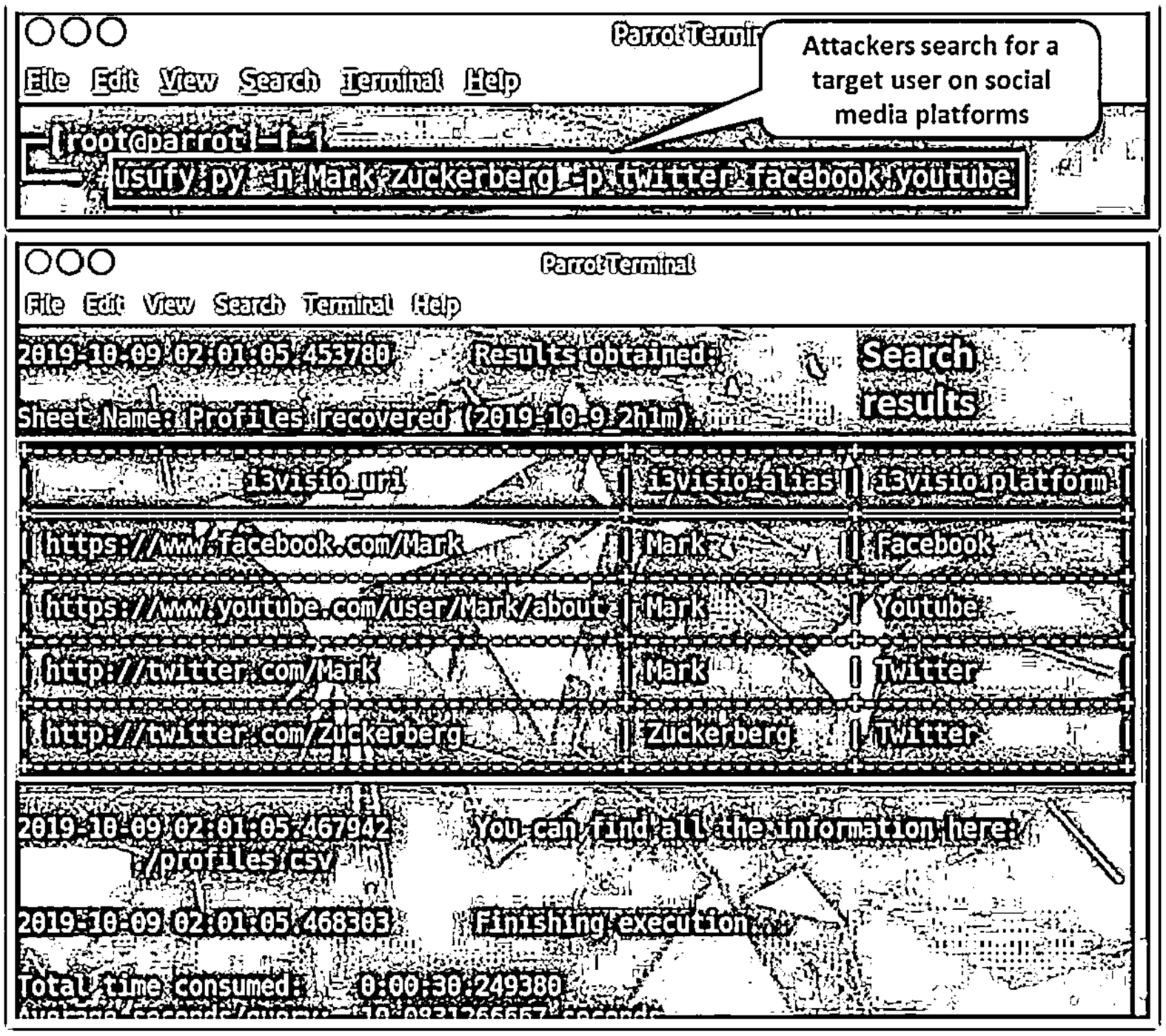


Figure 2.76: Screenshot of OSRFramework

- **OSINT Framework**

  Source: *https://osintframework.com*

  OSINT Framework is an open source intelligence gathering framework that helps security professionals in performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering. It is focused on gathering information from free tools or resources. This framework includes a simple web interface that lists various OSINT tools arranged by category, and it is shown as an OSINT tree structure on the web interface.

  As shown in the screenshot, the tools listed include the following indicators:

  - (T) - Indicates a link to a tool that must be installed and run locally
  - (D) - Google dork
  - (R) - Requires registration
  - (M) - Indicates a URL that contains the search term and the URL itself must be edited manually

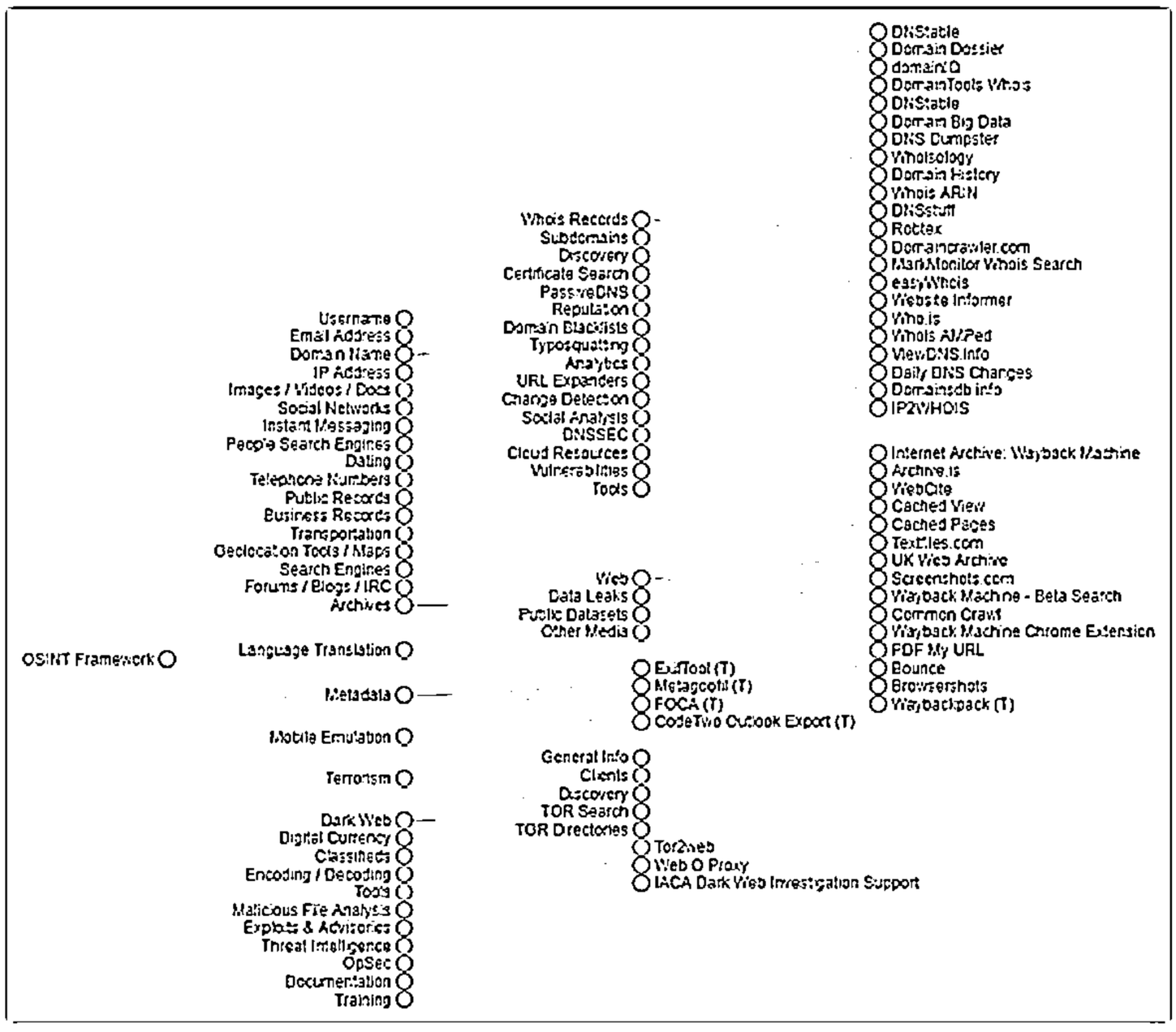


Figure 2.77: Screenshot of OSINT Framework

- **Recon-Dog**

  Source: *https://www.github.com*

  Recon-Dog is an all-in-one tool for all basic information gathering needs. It uses APIs to collect information about the target system.

Features:

- **Censys**: Uses censys.io to gather a massive amount of information about an IP address.
- **NS lookup**: Performs name server lookup
- **Port scan**: Scans most common TCP ports
- **Detect CMS**: Can detect 400+ content management systems
- **Whois lookup**: Performs a Whois lookup
- **Detect honeypot**: Uses shodan.io to check if the target is a honeypot
- **Find subdomains**: Uses findsubdomains.com to find subdomains
- **Reverse IP lookup**: Performs a reverse IP lookup to find domains associated with an IP address
- **Detect technologies**: Uses wappalyzer.com to detect 1000+ technologies
- **All**: Runs all utilities against the target

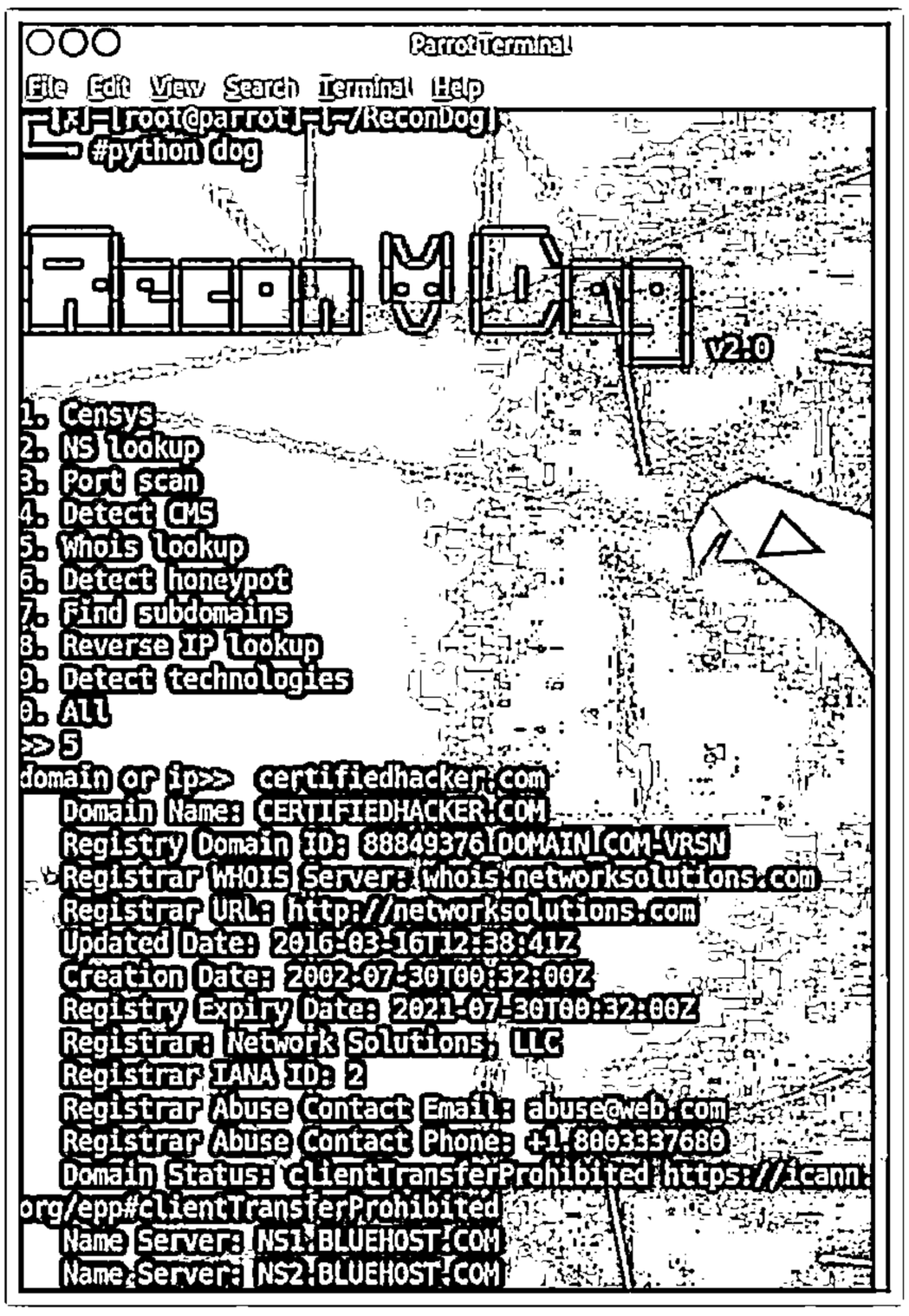


Figure 2.78: Screenshot of Recon-Dog

- **BillCipher**

  Source: *https://www.github.com*

  BillCipher is an information gathering tool for a website or IP address. It can work on any operating system that supports Python 2, Python 3, and Ruby. This tool includes various options such as DNS lookup, Whois lookup, port scanning, zone transfer, host finder, and reverse IP lookup, which help to gather critical information.

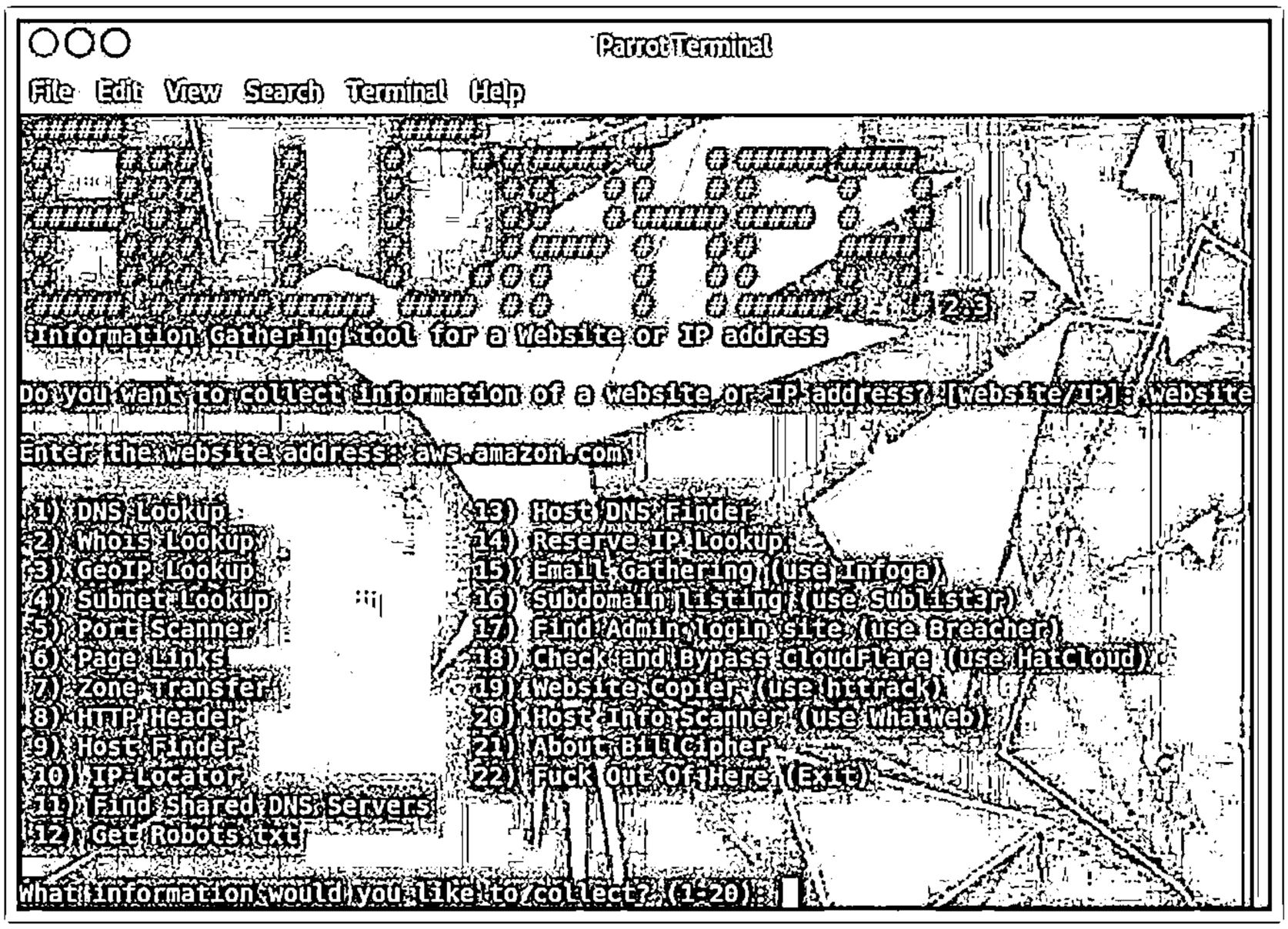
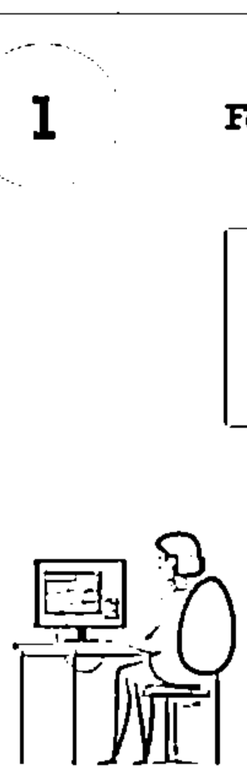


Figure 2.79: Screenshot of BillCipher

Some additional footprinting tools are listed below:

- theHarvester (*http://www.edge-security.com*)
- Th3Inspector (*https://github.com*)
- Raccoon (*https://github.com*)
- Orb (*https://github.com*)
- PENTMENU (*https://github.com*)

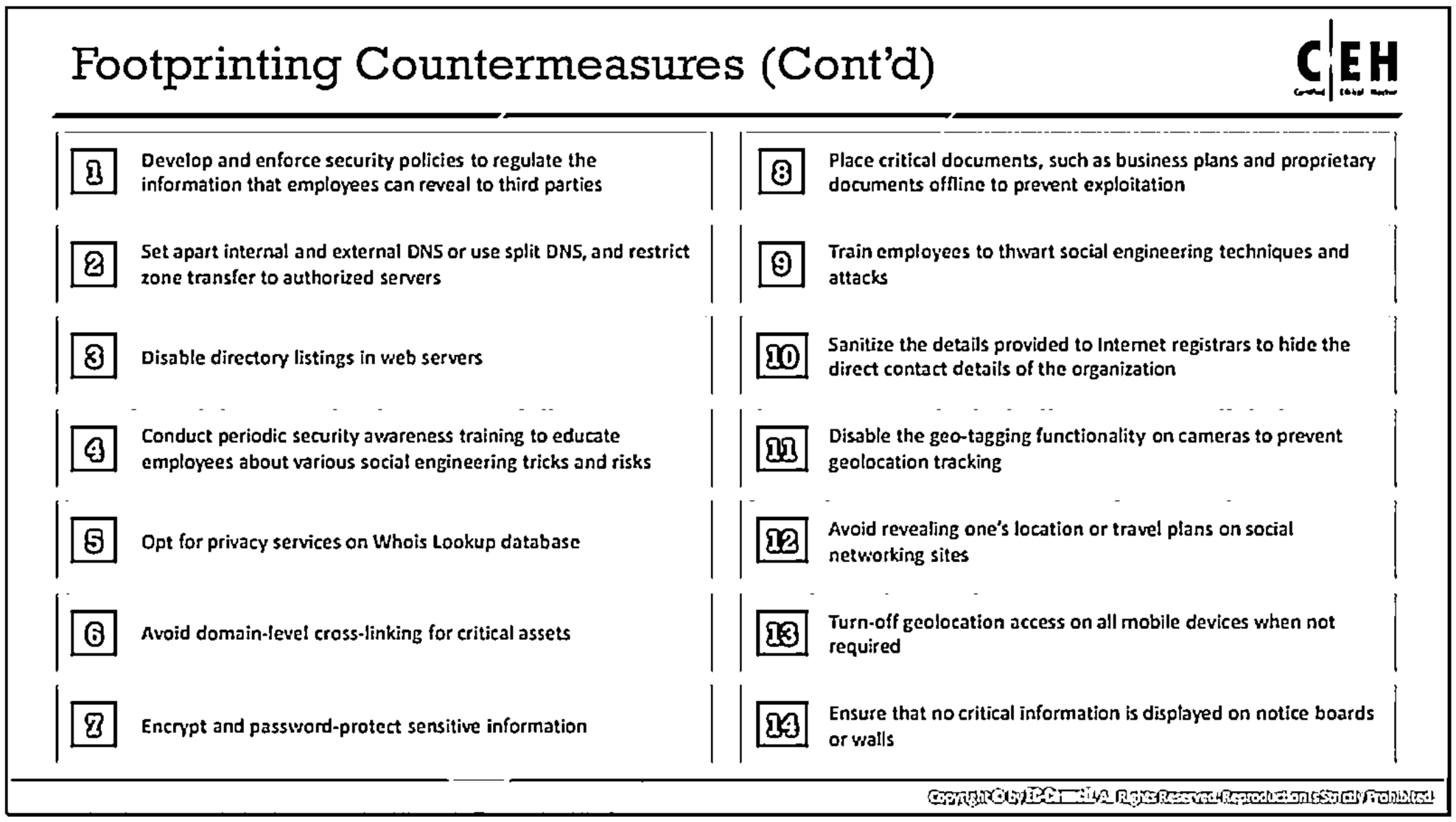
Module Flow



1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures

Footprinting Countermeasures

- Restrict the employees' access to social networking sites from the organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogues, etc.
- Limit the amount of information published on the website/Internet
- Use footprinting techniques to discover and remove any sensitive information publicly available
- Prevent search engines from caching a web page and use anonymous registration services



Footprinting Countermeasures

So far, we have discussed the importance of footprinting, various ways to perform the task, and the tools that help in its execution. Now, we will discuss footprinting countermeasures, i.e., the measures or actions taken to prevent or offset information disclosure.

Some of the footprinting countermeasures are as follows:

- Restrict the employees' access to social networking sites from the organization's network
- Configure web servers to avoid information leakage
- Educate employees to use pseudonyms on blogs, groups, and forums
- Do not reveal critical information in press releases, annual reports, product catalogs, and so on.
- Limit the amount of information that you are publishing on the website/Internet
- Use footprinting techniques to discover and remove any sensitive information publicly available
- Prevent search engines from caching a web page and use anonymous registration services
- Develop and enforce security policies such as information security policy, password policy, and so on, to regulate the information that employees can reveal to third parties
- Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers
- Disable directory listings in the web servers

- Conduct security awareness training periodically to educate employees about various social engineering tricks and risks
- Opt for privacy services on Whois lookup database
- Avoid domain-level cross-linking for critical assets
- Encrypt and password-protect sensitive information
- Do not enable protocols that are not required
- Always use TCP/IP and IPSec filters for defense in depth
- Configure IIS to avoid information disclosure through banner grabbing
- Hide the IP address and the related information by implementing VPN or keeping the server behind a secure proxy
- Request archive.org to delete the history of the website from the archive database
- Keep the domain name profile private
- Place critical documents such as business plans and proprietary documents offline to prevent exploitation
- Train employees to thwart social engineering techniques and attacks
- Sanitize the details provided to the Internet registrars to hide the direct contact details of the organization
- Disable the geo-tagging functionality on cameras to prevent geolocation tracking
- Avoid revealing one's location or travel plans on social networking sites
- Turn-off geolocation access on all mobile devices when not required
- Ensure that no critical information such as strategic plans, product information, and sales projections is displayed on notice boards or walls

Module Summary

- In this module, we have discussed the following:
  - Footprinting concepts and the objectives of footprinting
  - Various footprinting techniques, such as footprinting through search engines, footprinting through web services, and footprinting through social networking sites
  - Website, email, Whois, and DNS footprinting
  - Network footprinting and footprinting through social engineering
  - Some important footprinting tools
  - How organizations can defend against footprinting and reconnaissance activities
- In the next module, we will discuss in detail how attackers, ethical hackers, and pen testers perform network scanning to collect information about a target of evaluation before an attack or audit

Module Summary

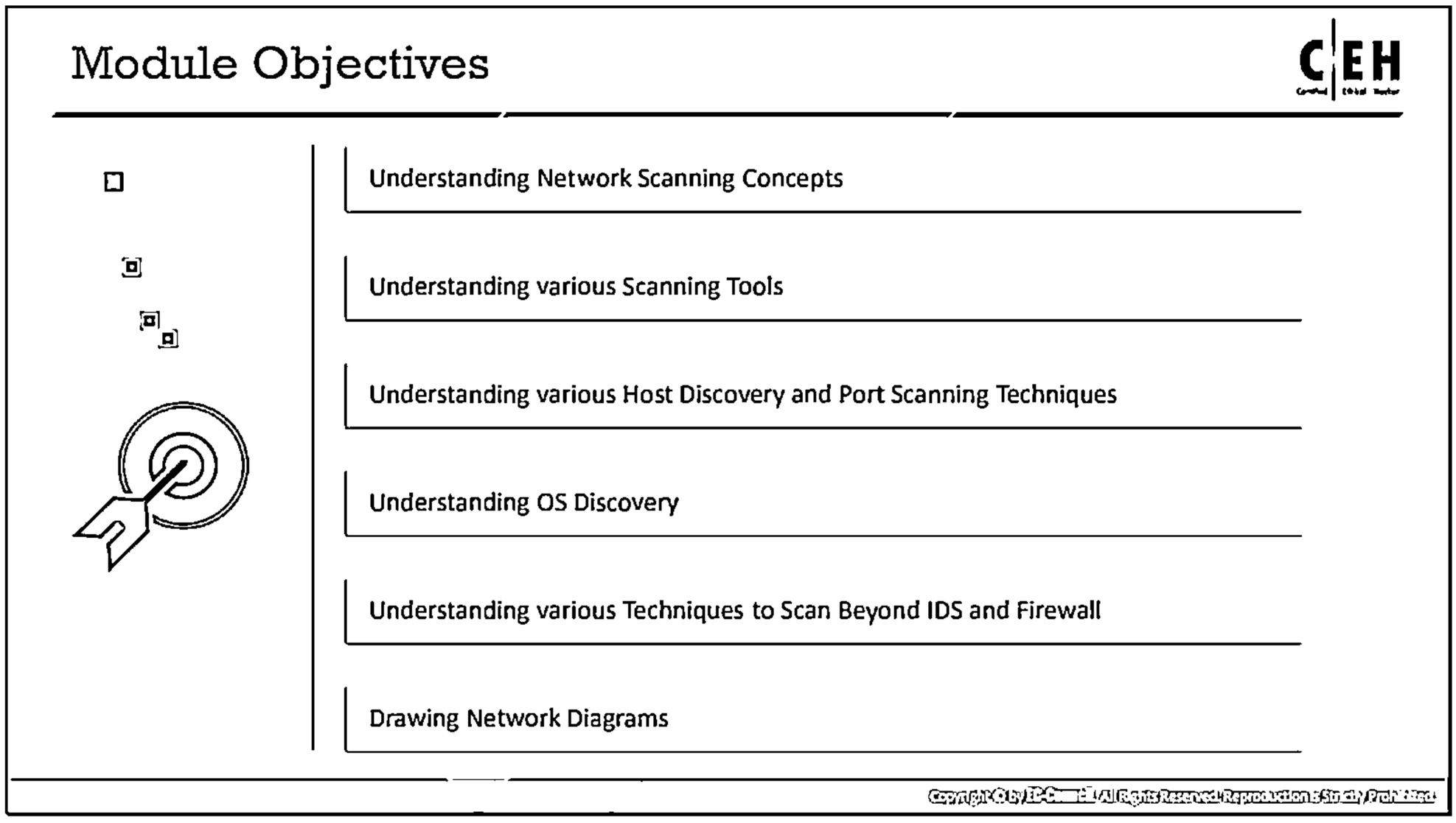
This module presented footprinting concepts along with the objectives of footprinting. It provided a detailed explanation of the various techniques used for footprinting through search engines. Further, it described footprinting through web services and social networking sites. In addition, it discussed website and email footprinting techniques. It also explained Whois and DNS footprinting in detail. Moreover, it described network footprinting along with traceroute analysis. It also explained footprinting through social engineering. Finally, it presented an overview of important footprinting tools. The module ended with a detailed discussion of how organizations can defend themselves against footprinting and reconnaissance activities.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen testers perform network scanning to collect information about a target for evaluation before an attack or audit.

C|EH™

Certified | Ethical Hacker

Module 03:
Scanning Networks



Module Objectives

After identifying the target and performing the initial reconnaissance, as discussed in the Footprinting and Reconnaissance module, attackers begin to search for an entry point into the target system. Attackers should determine whether the target systems are active or inactive to reduce the time spent on scanning. Notably, the scanning itself is not the actual intrusion but an extended form of reconnaissance in which the attacker learns more about his/her target, including information about OSs, services, and any configuration lapses. The information gleaned from such reconnaissance helps the attacker select strategies for attacking the target system or network.

This module starts with an overview of network scanning and provides insights into various host discovery techniques that can be used to check for live and active systems. Furthermore, it discusses various port and service discovery techniques, operating system discovery techniques, and techniques for scanning beyond IDS and firewalls. Finally, it ends with an overview of drawing network diagrams.

At the end of this module, you will be able to:

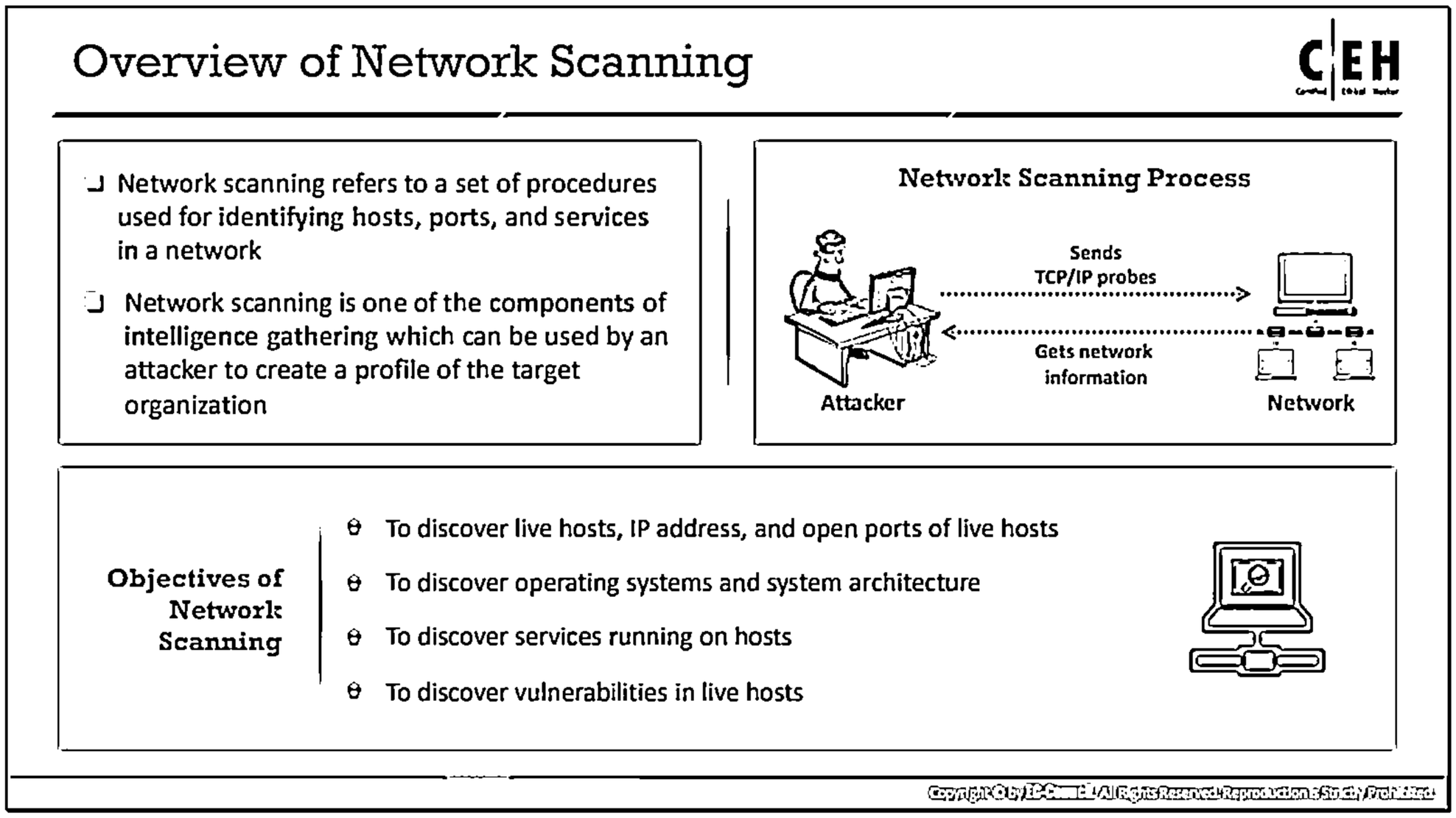
- Describe the network scanning concepts
- Use various scanning tools
- Perform host discovery to check for live systems
- Perform port and service discovery using various scanning techniques
- Scan beyond intrusion detection systems (IDS) and firewalls
- Perform operating system (OS) discovery
- Draw network diagrams using network discovery tools

Module Flow

1. Network Scanning Concepts
2. Scanning Tools
3. Host Discovery
4. Port and Service Discovery
5. OS Discovery (Banner Grabbing/ OS Fingerprinting)
6. Scanning Beyond IDS and Firewall
7. Draw Network Diagrams

Network Scanning Concepts

As already discussed, footprinting is the first phase of hacking, in which the attacker gains primary information about a potential target. He/she then uses this information in the scanning phase to gather more details about the target.



Overview of Network Scanning

Scanning is the process of gathering additional detailed information about the target using highly complex and aggressive reconnaissance techniques. Network scanning refers to a set of procedures used for identifying hosts, ports, and services in a network. Network scanning is also used for discovering active machines in a network and identifying the OS running on the target machine. It is one of the most important phases of intelligence gathering for an attacker, which enables him/her to create a profile of the target organization. In the process of scanning, the attacker tries to gather information, including the specific IP addresses that can be accessed over the network, the target's OS and system architecture, and the ports along with their respective services running on each computer.

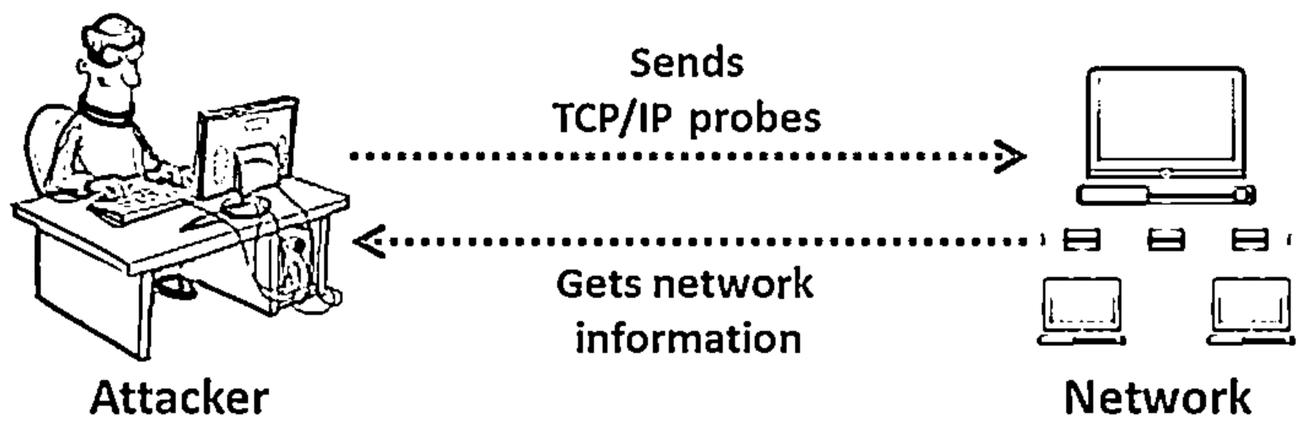


Figure 3.1: Network scanning process

The purpose of scanning is to discover exploitable communications channels, probe as many listeners as possible, and track the ones that are responsive or useful to an attacker's particular needs. In the scanning phase of an attack, the attacker tries to find various ways to intrude into a target system. The attacker also tries to discover more information about the target system to determine the presence of any configuration lapses. The attacker then uses the information obtained to develop an attack strategy.

Types of Scanning

- **Port Scanning** – Lists the open ports and services. Port scanning is the process of checking the services running on the target computer by sending a sequence of messages in an attempt to break in. Port scanning involves connecting to or probing TCP and UDP ports of the target system to determine whether the services are running or are in a listening state. The listening state provides information about the OS and the application currently in use. Sometimes, active services that are listening may allow unauthorized users to misconfigure systems or to run software with vulnerabilities.
- **Network Scanning** – Lists the active hosts and IP addresses. Network scanning is a procedure for identifying active hosts on a network, either to attack them or assess the security of the network.
- **Vulnerability Scanning** – Shows the presence of known weaknesses. Vulnerability scanning is a method for checking whether a system is exploitable by identifying its vulnerabilities. A vulnerability scanner consists of a scanning engine and a catalog. The catalog includes a list of common files with known vulnerabilities and common exploits for a range of servers. A vulnerability scanner may, for example, look for backup files or directory traversal exploits. The scanning engine maintains logic for reading the exploit list, transferring the request to the web server, and analyzing the requests to ensure the safety of the server. These tools generally target vulnerabilities that secure host configurations can fix easily through updated security patches and a clean web document.

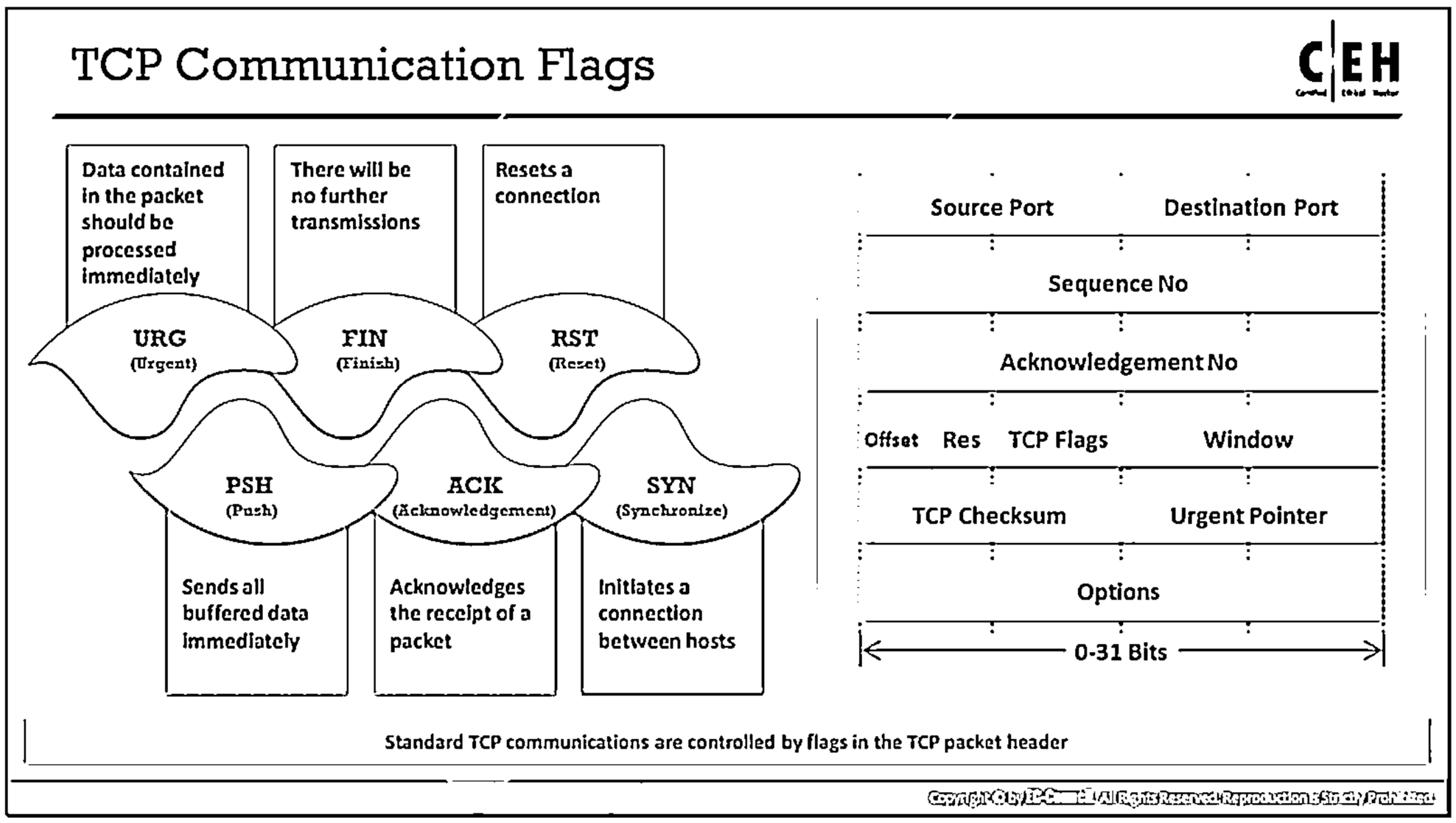
A thief who wants to break into a house looks for access points such as doors and windows. These are usually the house's points of vulnerability, as they are easily accessible. When it comes to computer systems and networks, ports are the doors and windows of a system that an intruder uses to gain access. A general rule for computer systems is that the greater the number of open ports on a system, the more vulnerable is the system. However, there are cases in which a system with fewer open ports than another machine presents a much higher level of vulnerability.

Objectives of Network Scanning

The more the information at hand about a target organization, the higher are the chances of knowing a network's security loopholes, and, consequently, for gaining unauthorized access to it.

Some objectives for scanning a network are as follows:

- Discover the network's live hosts, IP addresses, and open ports of the live hosts. Using the open ports, the attacker will determine the best means of entering into the system.
- Discover the OS and system architecture of the target. This is also known as fingerprinting. An attacker can formulate an attack strategy based on the OS's vulnerabilities.
- Discover the services running/listening on the target system. Doing so gives the attacker an indication of the vulnerabilities (based on the service) that can be exploited for gaining access to the target system.
- Identify specific applications or versions of a particular service.
- Identify vulnerabilities in any of the network systems. This helps an attacker to compromise the target system or network through various exploits.



TCP Communication Flags

The TCP header contains various flags that control the transmission of data across a TCP connection. Six TCP control flags manage the connection between hosts and give instructions to the system. Four of these flags (SYN, ACK, FIN, and RST) govern the establishment, maintenance, and termination of a connection. The other two flags (PSH and URG) provide instructions to the system. The size of each flag is 1 bit. As there are six flags in the TCP Flags section, the size of this section is 6 bits. When a flag value is set to "1," that flag is automatically turned on.

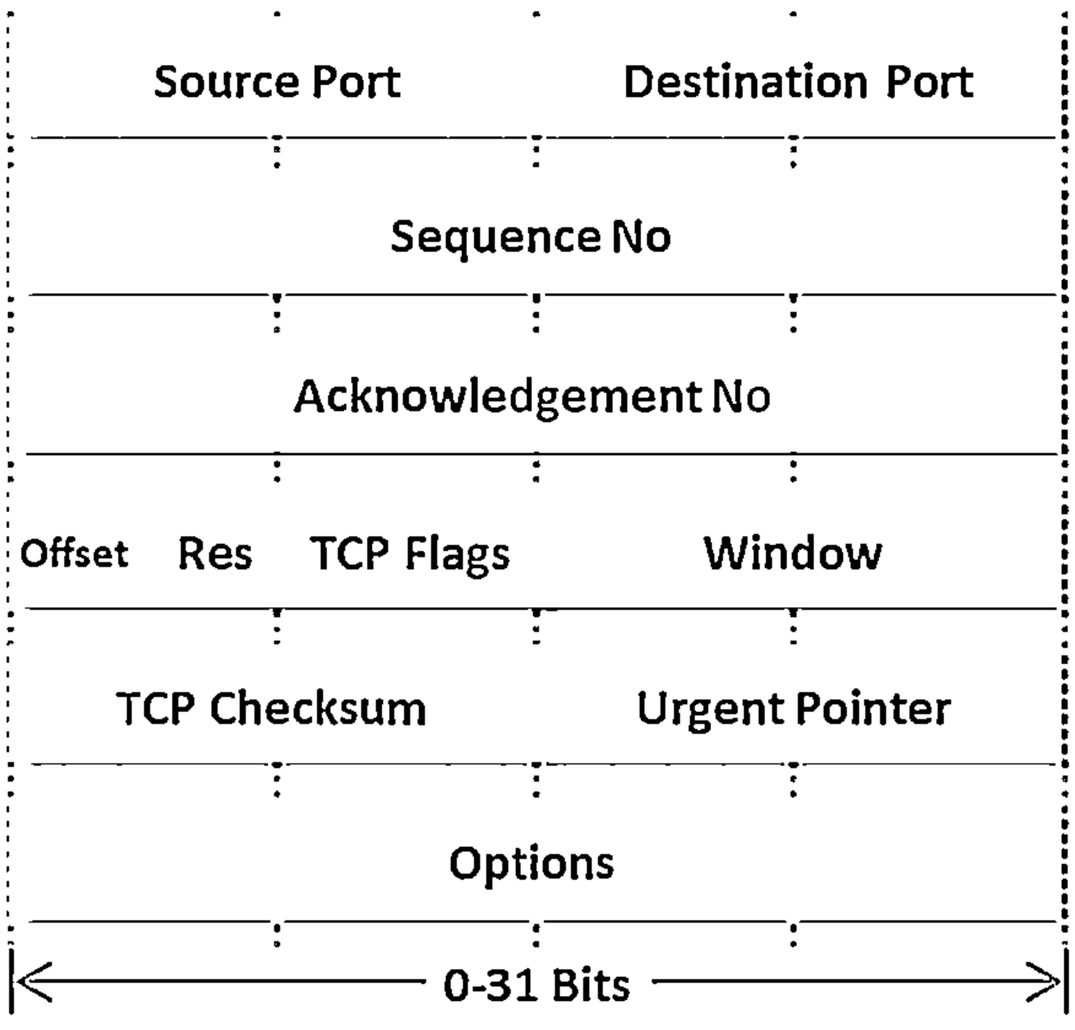


Figure 3.2: TCP header format

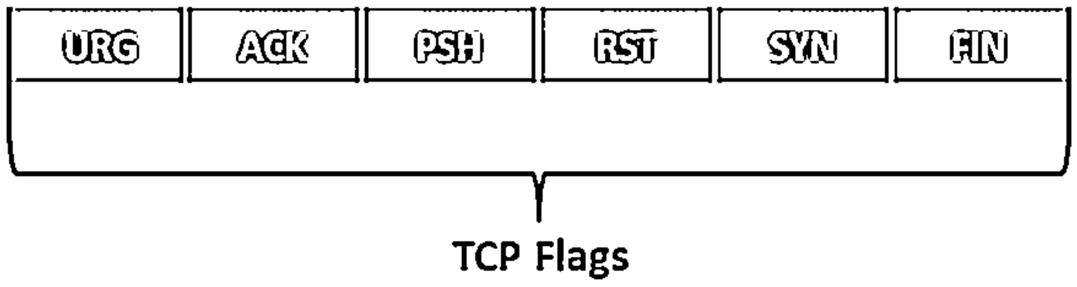
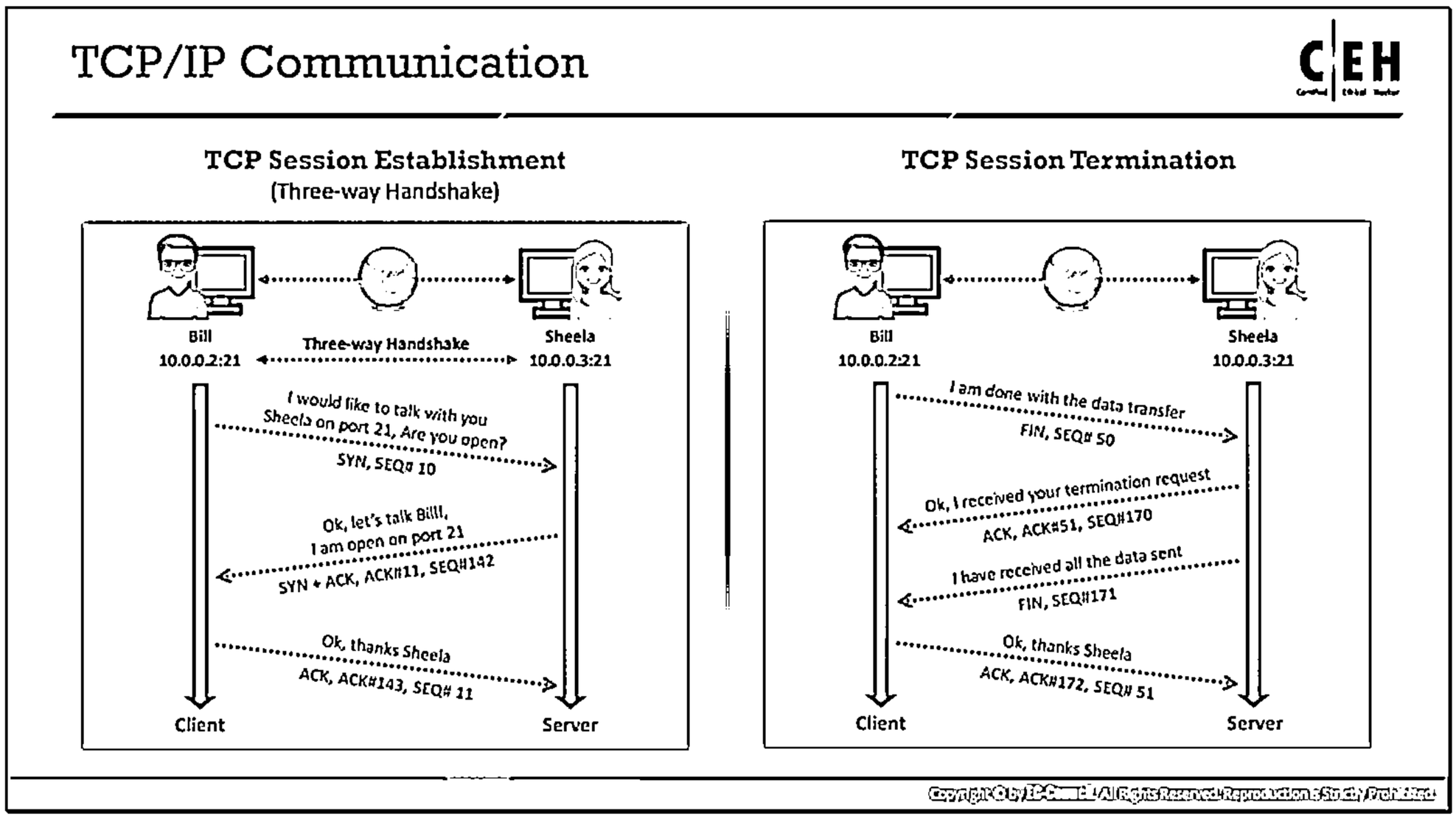


Figure 3.3: TCP communication flags

The following are the TCP communication flags:

- Synchronize or "SYN": It notifies the transmission of a new sequence number. This flag generally represents the establishment of a connection (three-way handshake) between two hosts.
- Acknowledgement or "ACK": It confirms the receipt of the transmission and identifies the next expected sequence number. When the system successfully receives a packet, it sets the value of its flag to "1," thus implying that the receiver should pay attention to it.
- Push or "PSH": When it is set to "1," it indicates that the sender has raised the push operation to the receiver; this implies that the remote system should inform the receiving application about the buffered data coming from the sender. The system raises the PSH flag at the start and end of data transfer and sets it on the last segment of a file to prevent buffer deadlocks.
- Urgent or "URG": It instructs the system to process the data contained in packets as soon as possible. When the system sets the flag to "1," priority is given to processing the urgent data first and all the other data processing is stopped.
- Finish or "FIN": It is set to "1" to announce that no more transmissions will be sent to the remote system and the connection established by the SYN flag is terminated.
- Reset or "RST": When there is an error in the current connection, this flag is set to "1" and the connection is aborted in response to the error. Attackers use this flag to scan hosts and identify open ports.

SYN scanning mainly deals with three flags: SYN, ACK, and RST. You can use these three flags for gathering illegal information from servers during enumeration.



TCP/IP Communication

TCP is connection oriented, i.e., it prioritizes connection establishment before data transfer between applications. This connection between protocols is possible through the three-way handshake.

A TCP session initiates using a three-way handshake mechanism:

- To launch a TCP connection, the source (10.0.0.2:21) sends a SYN packet to the destination (10.0.0.3:21).
- On receiving the SYN packet, the destination responds by sending a SYN/ACK packet back to the source.
- The ACK packet confirms the arrival of the first SYN packet to the source.
- Finally, the source sends an ACK packet for the ACK/SYN packet transmitted by the destination.
- This triggers an "OPEN" connection, thereby allowing communication between the source and destination, which continues until one of them issues a "FIN" or "RST" packet to close the connection.

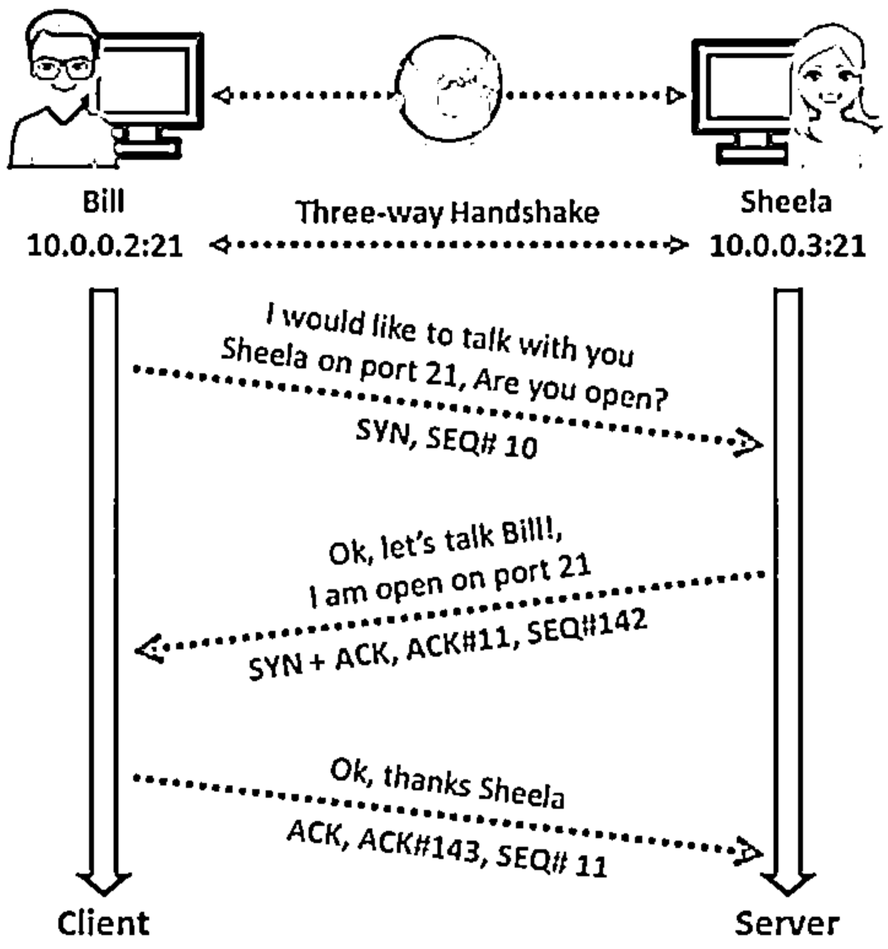


Figure 3.4: TCP session establishment

The TCP protocol maintains stateful connections for all connection-oriented protocols throughout the Internet and works similarly to ordinary telephone communication, in which one picks up a telephone receiver, hears a dial tone, and dials a number that triggers ringing at the other end until someone picks up the receiver and says, "Hello."

The system terminates the established TCP session as follows:

After completing all the data transfers through the established TCP connection, the sender sends the connection termination request to the receiver through a FIN or RST packet. Upon receiving the connection termination request, the receiver acknowledges the termination request by sending an ACK packet to the sender and finally sends its own FIN packet. Then, the system terminates the established connection.

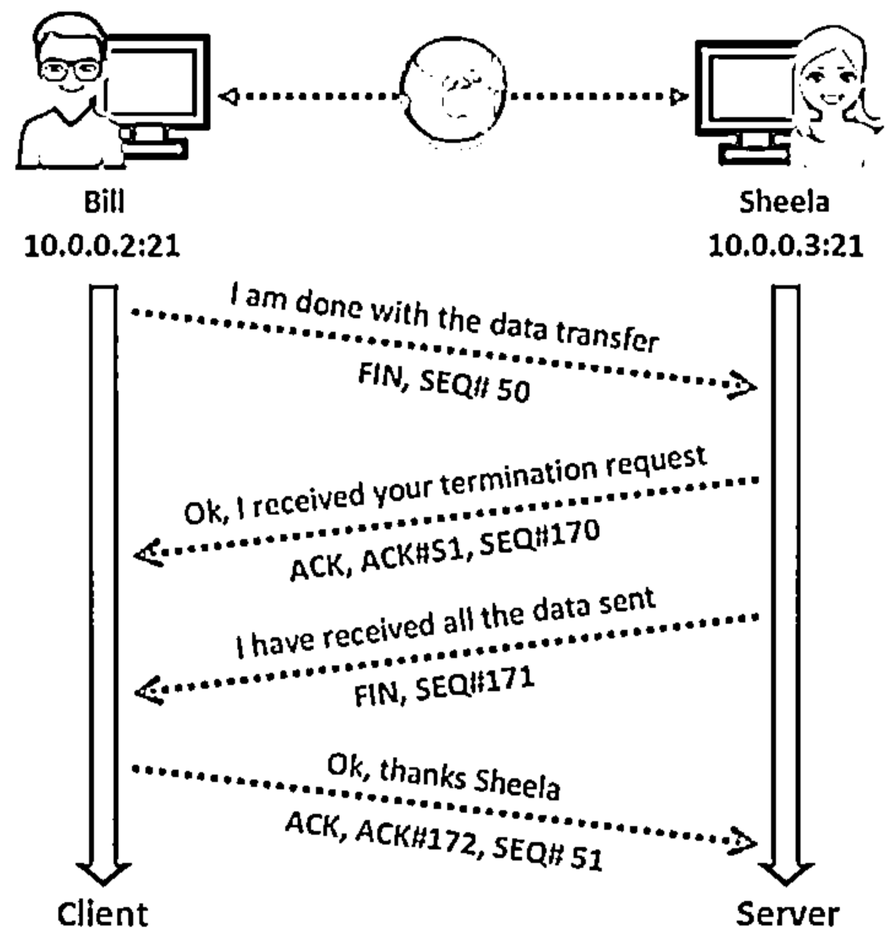


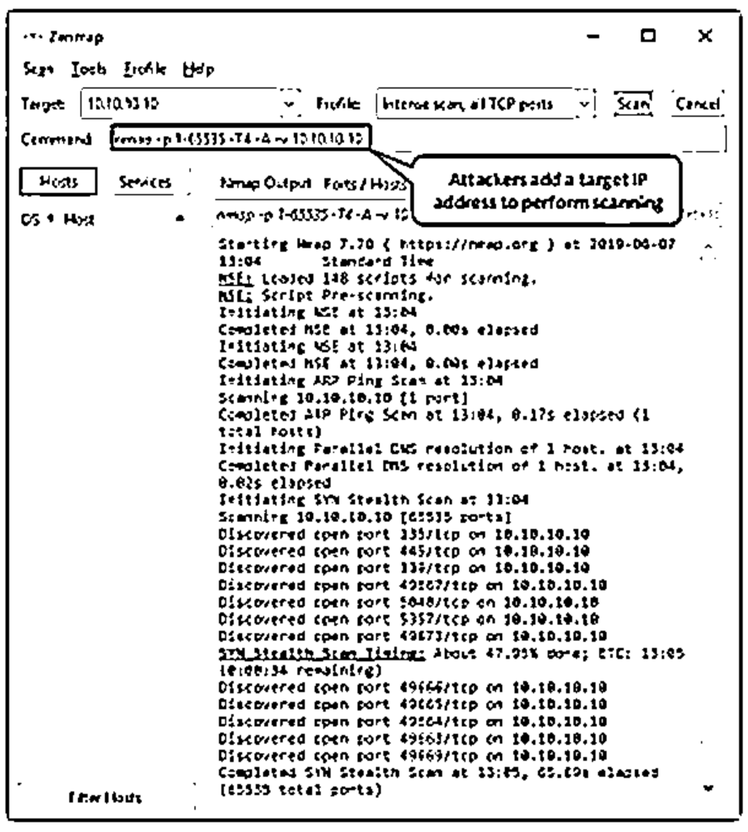
Figure 3.5: TCP session termination

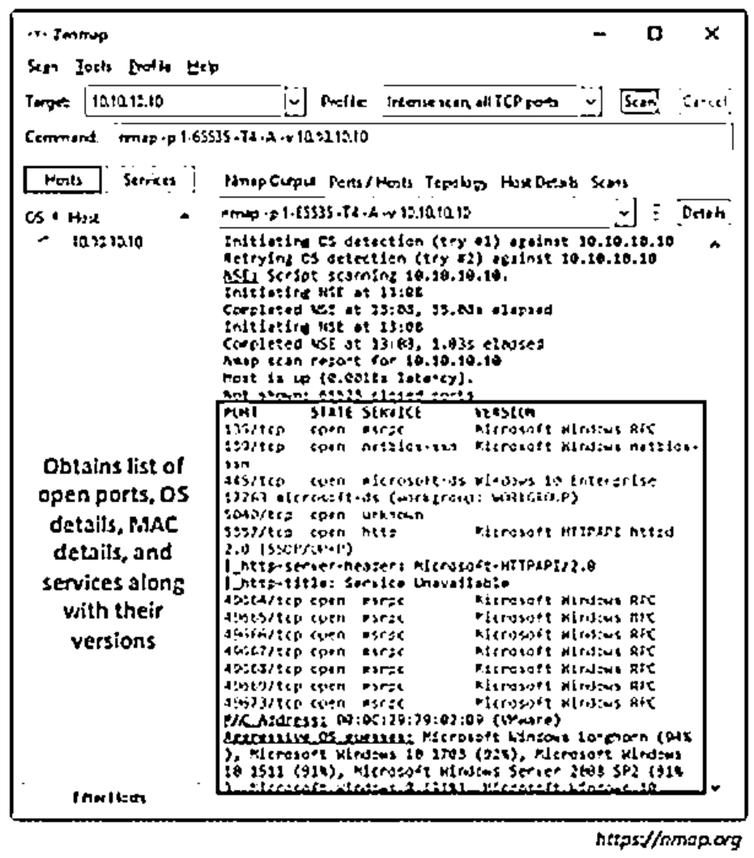
Module Flow

1. Network Scanning Concepts
2. Scanning Tools
3. Host Discovery
4. Port and Service Discovery
5. OS Discovery (Banner Grabbing/ OS Fingerprinting)
6. Scanning Beyond IDS and Firewall
7. Draw Network Diagrams

Scanning Tools: Nmap

- Network administrators can use Nmap for inventorying a network, managing service upgrade schedules, and monitoring host or service uptime
- Attackers use Nmap to extract information such as live hosts on the network, open ports, services (application name and version), types of packet filters/ firewalls, as well as operating systems and versions used





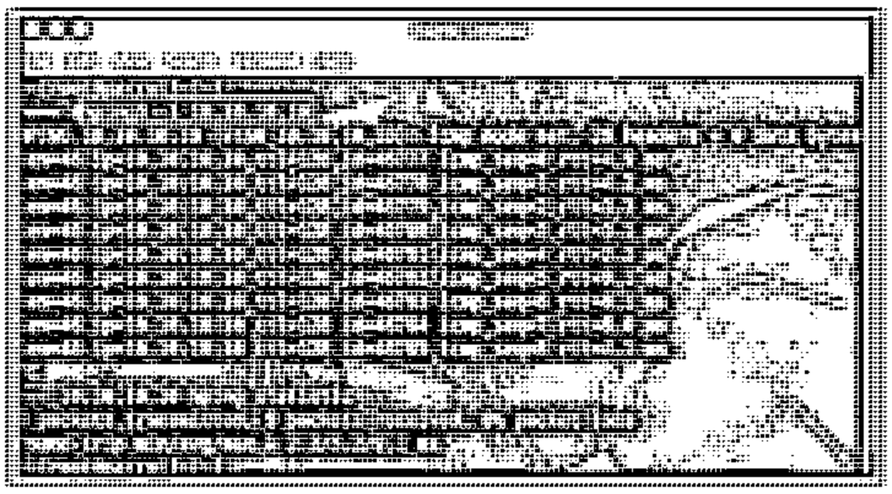
Obtains list of open ports, OS details, MAC details, and services along with their versions

https://nmap.org

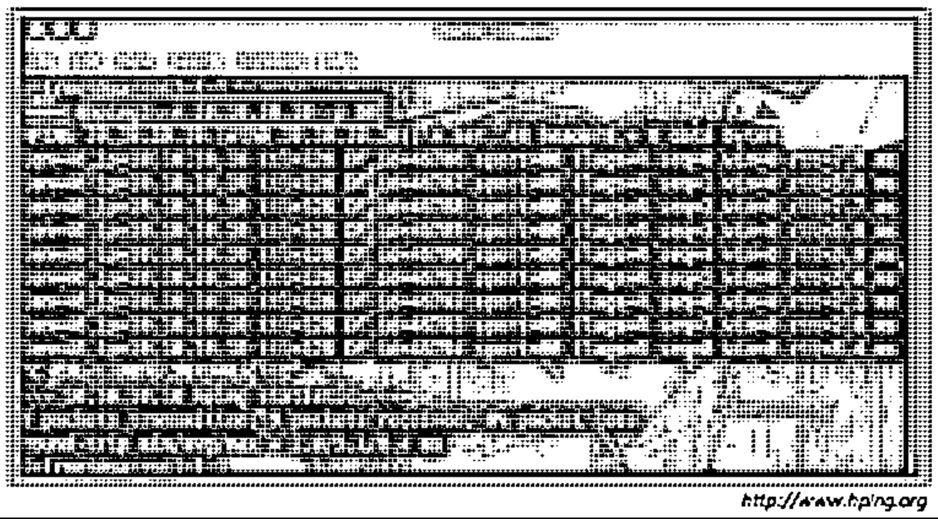
Scanning Tools: Hping2/Hping3

1. Command line network scanning and packet crafting tool for the TCP/IP protocol
2. It can be used for network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, etc.

ICMP Scanning



ACK Scanning on port 80



http://www.hping.org

Hping Commands

ICMP Ping

```
hping3 -1 10.0.0.25
```

ACK scan on port 80

```
hping3 -A 10.0.0.25 -p 80
```

UDP scan on port 80

```
hping3 -2 10.0.0.25 -p 80
```

Collecting Initial Sequence Number

```
hping3 192.168.1.103 -Q -p 139 -s
```

Firewalls and Timestamps

```
hping3 -S 72.14.207.99 -p 80 --tcp-timestamp
```

SYN scan on port 50-60

```
hping3 -8 50-60 -S 10.0.0.25 -V
```

FIN, PUSH and URG scan on port 80

```
hping3 -F -P -U 10.0.0.25 -p 80
```

Scan entire subnet for live host

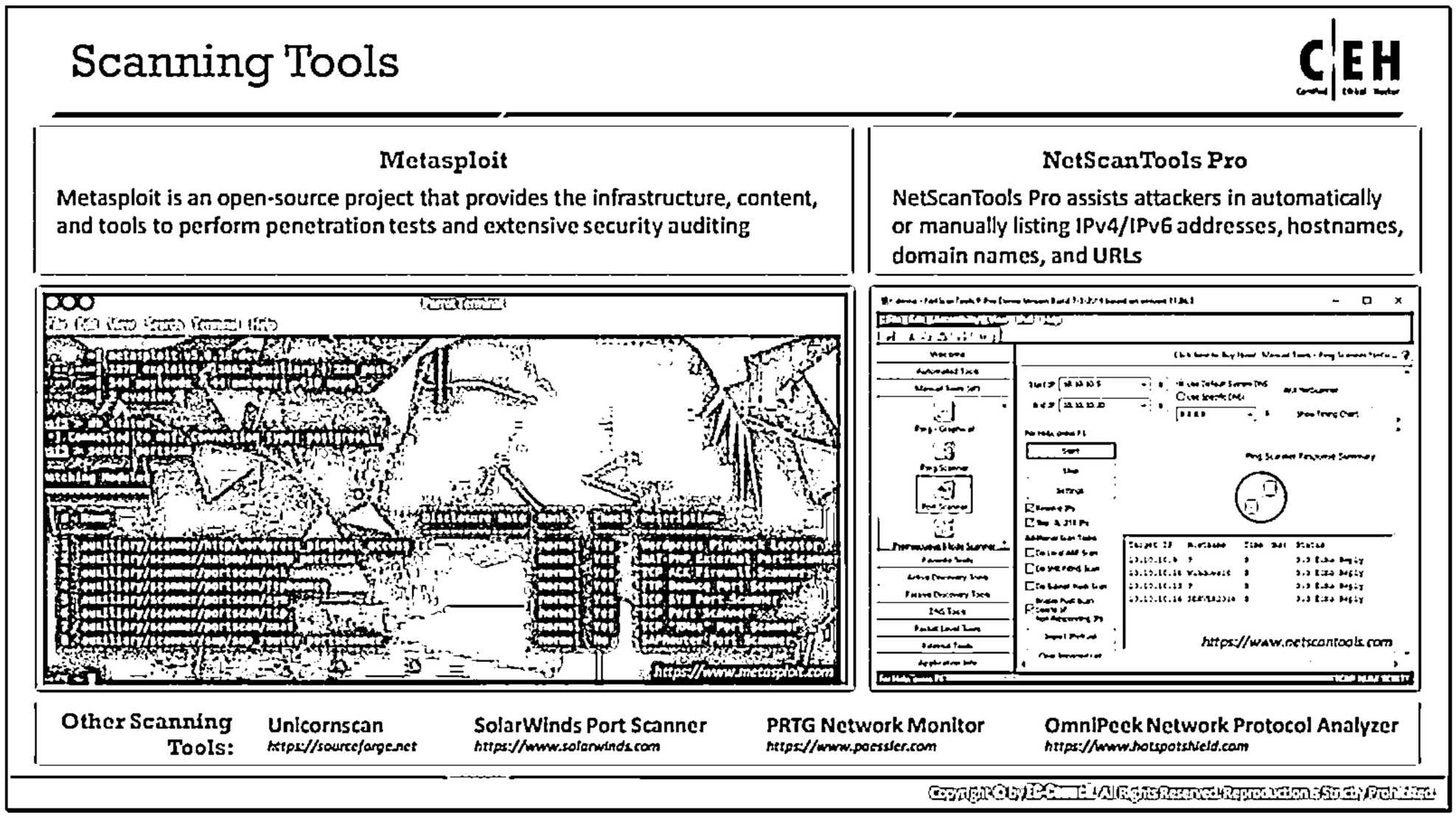
```
hping3 -1 10.0.1.x --rand-dest -I eth0
```

Intercept all traffic containing HTTP signature

```
hping3 -9 HTTP -I eth0
```

SYN flooding a victim

```
hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood
```



Scanning Tools

Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location info, NetBIOS info, and information about all TCP/IP and UDP open ports. The information obtained from these tools will help an ethical hacker in creating the profile of the target organization and scanning the network for open ports of the devices connected.

- **Nmap**

  Source: *https://nmap.org*

  Nmap ("Network Mapper") is a security scanner for network exploration and hacking. It allows you to discover hosts, ports, and services on a computer network, thus creating a "map" of the network. It sends specially crafted packets to the target host and then analyzes the responses to accomplish its goal. It scans vast networks of literally hundreds of thousands of machines. Nmap includes many mechanisms for port scanning (TCP and UDP), OS detection, version detection, ping sweeps, and so on.

  Either a network administrator or an attacker can use this tool for their specific needs. Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime. Attackers use Nmap to extract information such as live hosts on the network, open ports, services (application name and version), type of packet filters/firewalls, MAC details, and OSs along with their versions.

  Syntax: `# nmap <options> <Target IP address>`

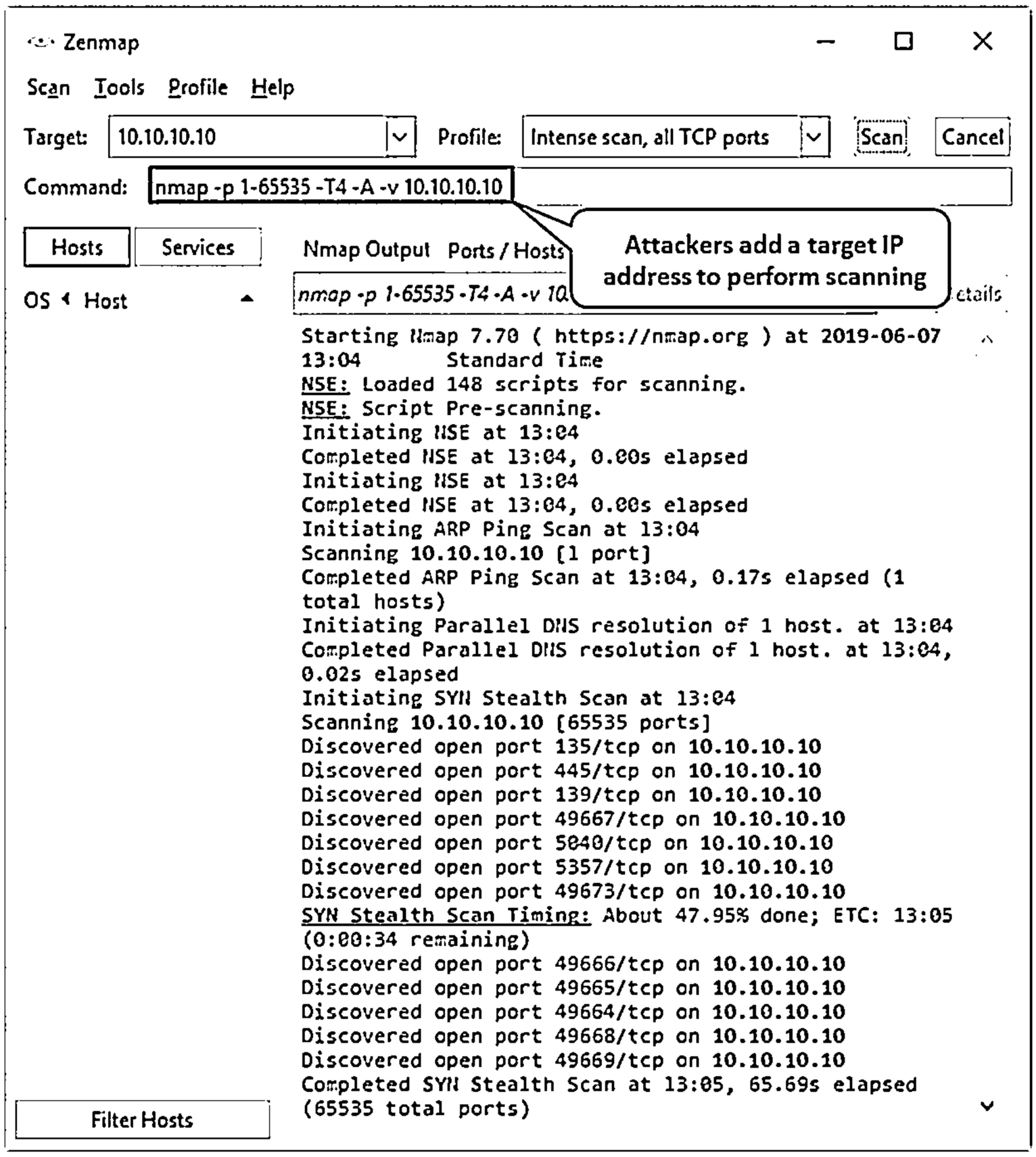


Figure 3.6: Screenshot displaying Nmap scan

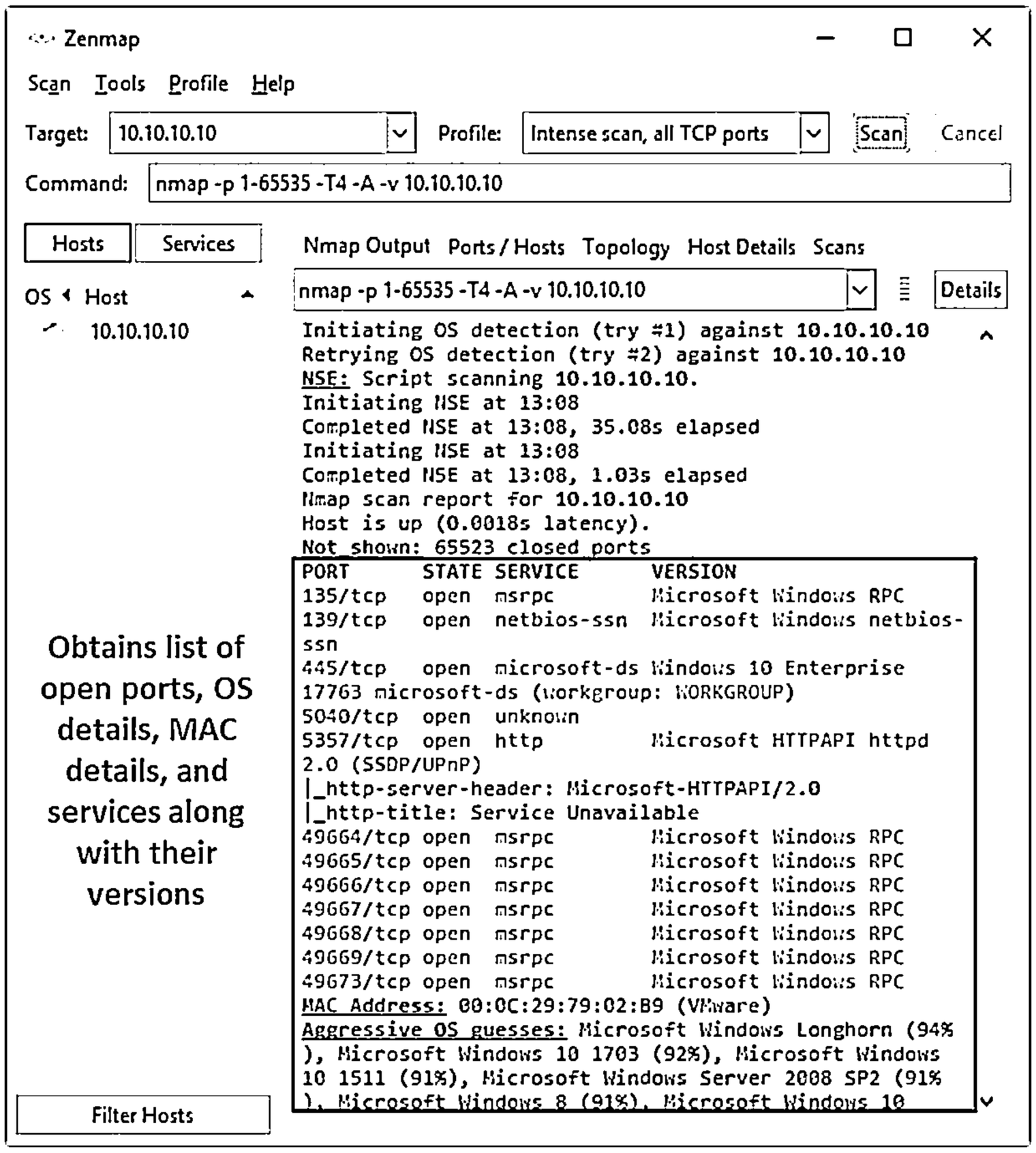


Figure 3.7: Screenshot displaying Nmap scan result

- **Hping2/Hping3**

  Source: *http://www.hping.org*

  Hping2/Hping3 is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, and other functions. It can send custom TCP/IP packets and display target replies similarly to a ping program with ICMP replies. It handles fragmentation as well as arbitrary packet body and size, and it can be used to transfer encapsulated files under the supported protocols. It also supports idle host scanning. IP spoofing and network/host scanning can be used to perform an anonymous probe for services. Hping2/Hping3 also has a Traceroute mode, which enables attackers to send files between covert channels. It also determines whether the host is up even when the host

blocks ICMP packets. Its firewalk-like usage allows the discovery of open ports behind firewalls. It performs manual path MTU discovery and enables attackers to perform remote OS fingerprinting.

Using Hping, an attacker can study the behavior of an idle host and gain information about the target, such as the services that the host offers, the ports supporting the services, and the OS of the target. This type of scan is a predecessor to either heavier probing or outright attacks.

Syntax: `# hping <options> <Target IP address>`

ICMP Scanning

A ping sweep or Internet Control Message Protocol (ICMP) scanning is a process of sending an ICMP request or ping to all the hosts on the network to determine the ones that are up.

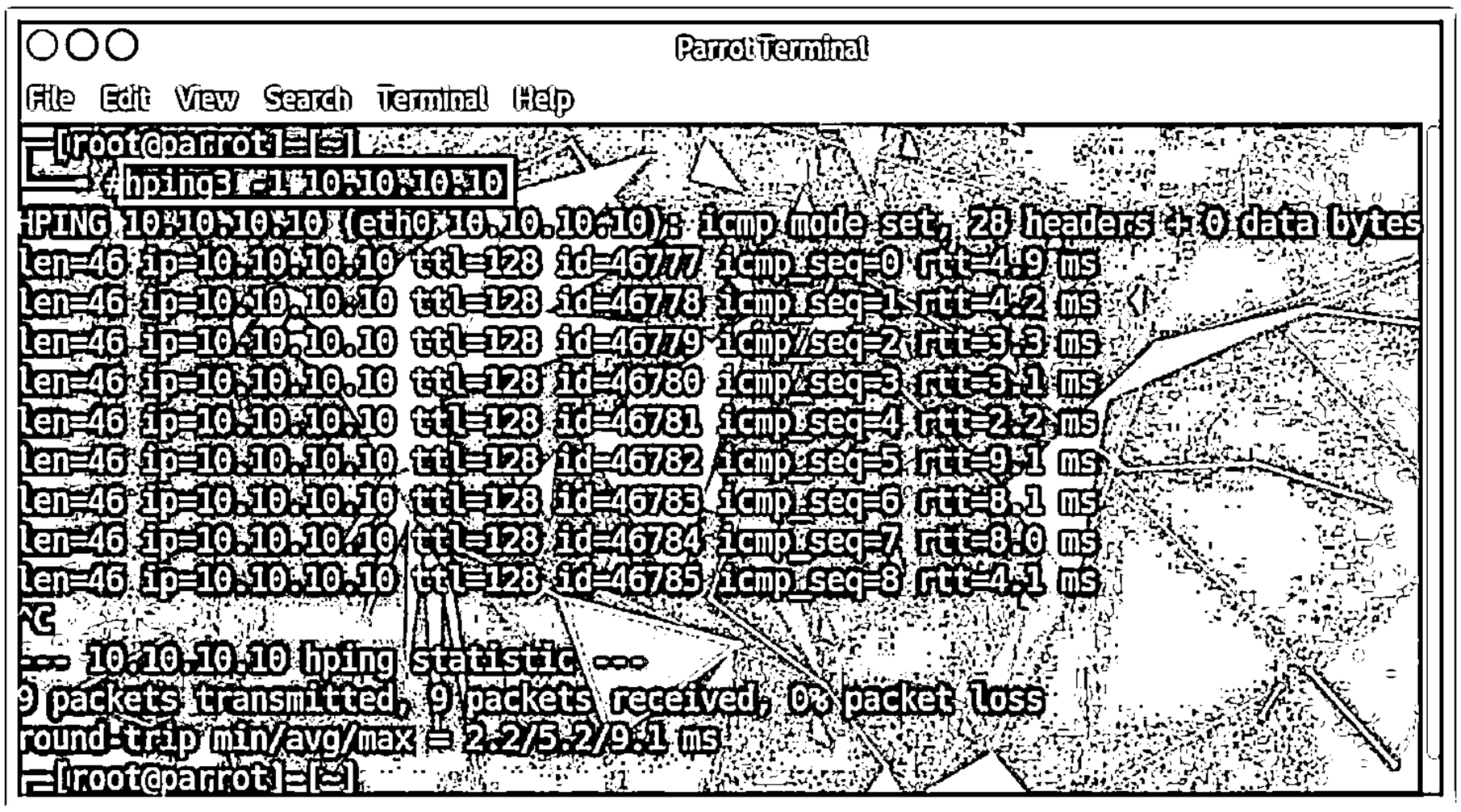


Figure 3.8: ICMP scanning

The OS, router, switch, and IP-based devices use this protocol via the ping command for echo request and echo response as a connectivity tester between different hosts.

ACK Scanning on Port 80

This scanning technique can be used to probe the existence of a firewall and its rule sets. Simple packet filtering allows the establishment of a connection (packets with the ACKbitset), whereas a sophisticated stateful firewall does not allow the establishment of a connection.

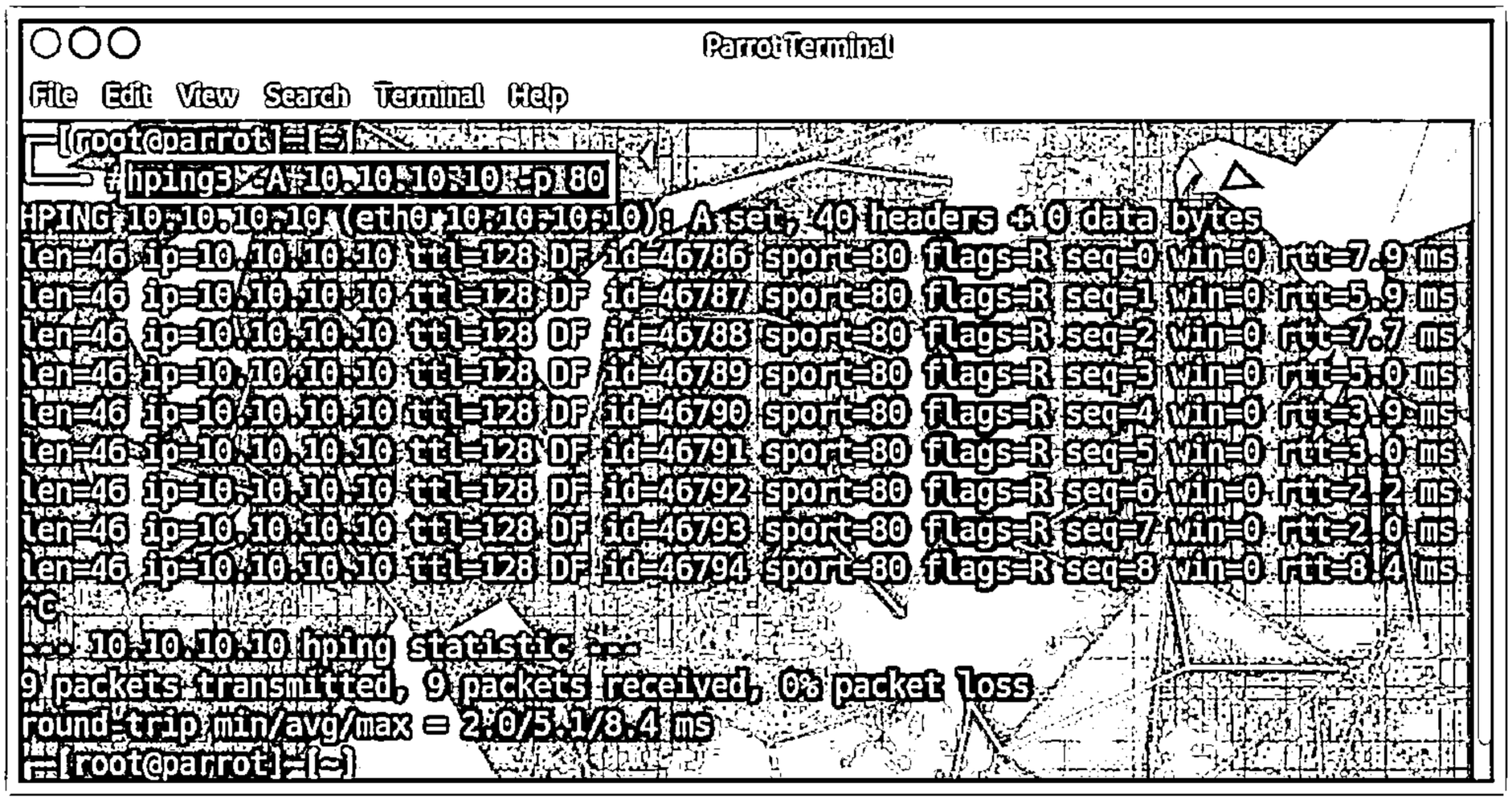


Figure 3.9: ACK scanning on port 80

Hping Commands

The various Hping commands are as follows:

- **ICMP ping**

  Ex. `hping3 -1 10.0.0.25`

  Hping performs an ICMP ping scan by specifying the argument -1 in the command line. You may use --ICMP or -1 as the argument in the command line. By issuing the above command, hping sends an ICMP echo request to 10.0.0.25 and receives an ICMP reply similarly to a ping utility.

- **ACK scan on port 80**

  Ex. `hping3 –A 10.0.0.25 –p 80`

  Hping can be configured to perform an ACK scan by specifying the argument -A in the command line. Here, you set the ACK flag in the probe packets and perform the scan. You perform this scan when a host does not respond to a ping request. By issuing this command, Hping checks if a host is alive on a network. If it finds a live host and an open port, it returns an RST response.

- **UDP scan on port 80**

  Ex. `hping3 –2 10.0.0.25 –p 80`

  Hping uses TCP as its default protocol. Using the argument -2 in the command line specifies that Hping operates in the UDP mode. You may use either --udp or -2 as the argument in the command line.

By issuing the above command, Hping sends UDP packets to port 80 on the host (10.0.0.25). It returns an ICMP port unreachable message if it finds the port closed and does not return a message if the port is open.

- **Collecting Initial Sequence Number**

  Ex. `hping3 192.168.1.103 -Q -p 139 -s`

  Using the argument -Q in the command line, Hping collects all the TCP sequence numbers generated by the target host (192.168.1.103).

- **Firewalls and Timestamps**

  Ex. `hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`

  Many firewalls drop those TCP packets that do not have the TCP Timestamp option set. By adding the --tcp-timestamp argument in the command line, you can enable the TCP timestamp option in Hping and try to guess the timestamp update frequency and uptime of the target host (72.14.207.99).

- **SYN scan on port 50-60**

  Ex. `hping3 -8 50-60 -S 10.0.0.25 -V`

  Using the argument -8 or --scan in the command line, you are operating Hping in the scan mode to scan a range of ports on the target host. Adding the argument -S allows you to perform a SYN scan.

  Therefore, the above command performs a SYN scan on ports 50–60 on the target host.

- **FIN, PUSH and URG scan on port 80**

  Ex. `hping3 –F –P –U 10.0.0.25 –p 80`

  By adding the arguments –F, –P, and –U in the command line, you are setting FIN, PUSH, and URG packets in the probe packets. By issuing this command, you are performing FIN, PUSH, and URG scans on port 80 on the target host (10.0.0.25). If port 80 is open, you will not receive a response. If the port is closed, Hping will return an RST response.

- **Scan entire subnet for live host**

  Ex. `hping3 -1 10.0.1.x --rand-dest –I eth0`

  By issuing this command, Hping performs an ICMP ping scan on the entire subnet 10.0.1.x; in other words, it sends an ICMP echo request randomly (--rand-dest) to all the hosts from 10.0.1.0 to 10.0.1.255 that are connected to the interface eth0. The hosts whose ports are open will respond with an ICMP reply. In this case, you have not set a port; hence, Hping sends packets to port 0 on all IP addresses by default.

- **Intercept all traffic containing HTTP signature**

  Ex. `hping3 -9 HTTP -I eth0`

  The argument -9 will set the Hping to the listen mode. Hence, by issuing the command -9 HTTP, Hping starts listening on port 0 (of all the devices connected in the network to interface eth0), intercepts all the packets containing the HTTP signature, and dumps from the signature end to the packet's end.

  For example, on issuing the command `hping2 -9 HTTP`, if Hping reads a packet that contains data `234-09sdflkjs45-HTTPhello_world`, it will display the result as `hello_world`.

- **SYN flooding a victim**

  Ex. `hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

  The attacker employs TCP SYN flooding techniques using spoofed IP addresses to perform a DoS attack.

The following table lists the various scanning methods and their respective Hping commands:

Scan	Commands
ICMP ping	`hping3 -1 10.0.0.25`
ACK scan on port 80	`hping3 -A 10.0.0.25 -p 80`
UDP scan on port 80	`hping3 -2 10.0.0.25 -p 80`
Collecting initial sequence number	`hping3 192.168.1.103 -Q -p 139 -s`
Firewalls and timestamps	`hping3 -S 72.14.207.99 -p 80 --tcp-timestamp`
SYN scan on port 50-60	`hping3 -8 50-56 -S 10.0.0.25 -V`
FIN, PUSH, and URG scan on port 80	`hping3 -F -P -U 10.0.0.25 -p 80`
Scan entire subnet for live host	`hping3 -1 10.0.1.x --rand-dest -I eth0`
Intercept all traffic containing HTTP signature	`hping3 -9 HTTP -I eth0`
SYN flooding a victim	`hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood`

Table 3.1: Hping command and its respective function

- **Metasploit**

  Source: *https://www.metasploit.com*

  Metasploit is an open-source project that provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing. It provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploits writers, and payload writers. A major advantage of the framework is the modular approach, i.e., allowing the combination of any exploit with any payload.

  It enables you to automate the process of discovery and exploitation and provides you with the necessary tools to perform the manual testing phase of a penetration test. You can use Metasploit Pro to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results.

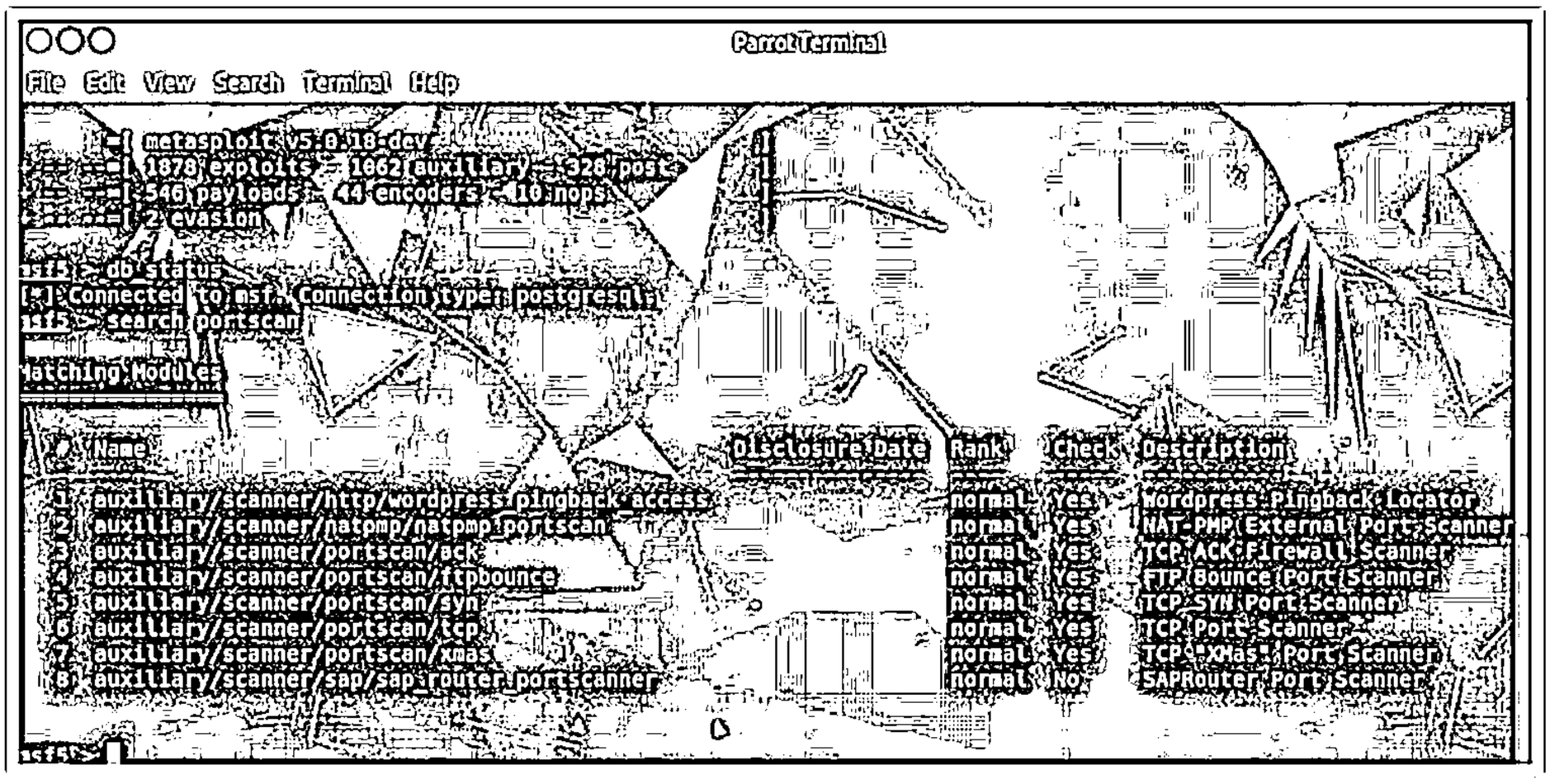


Figure 3.10: Screenshot displaying various Metasploit port scan modules

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro is an investigation tool that allows you to troubleshoot, monitor, discover, and detect devices on your network. Using this tool, you can easily gather information about the local LAN as well as Internet users, IP addresses, ports, and so on. Attackers can find vulnerabilities and exposed ports in the target system. It helps the attackers to list IPv4/IPv6 addresses, hostnames, domain names, email addresses, and URLs automatically or manually (using manual tools). NetScanTools Pro combines many network tools and utilities categorized by their functions, such as active, passive, DNS, and local computer.

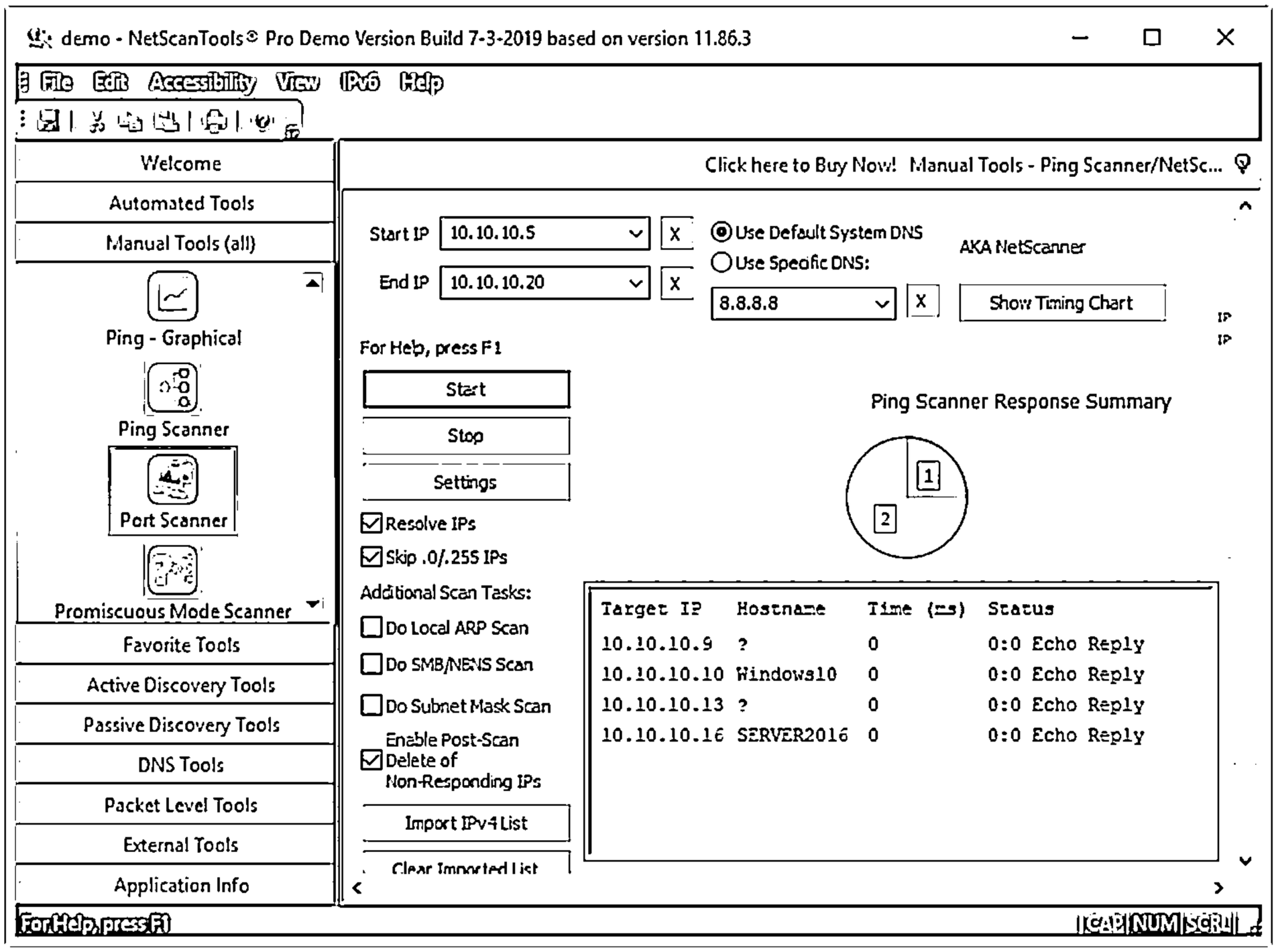
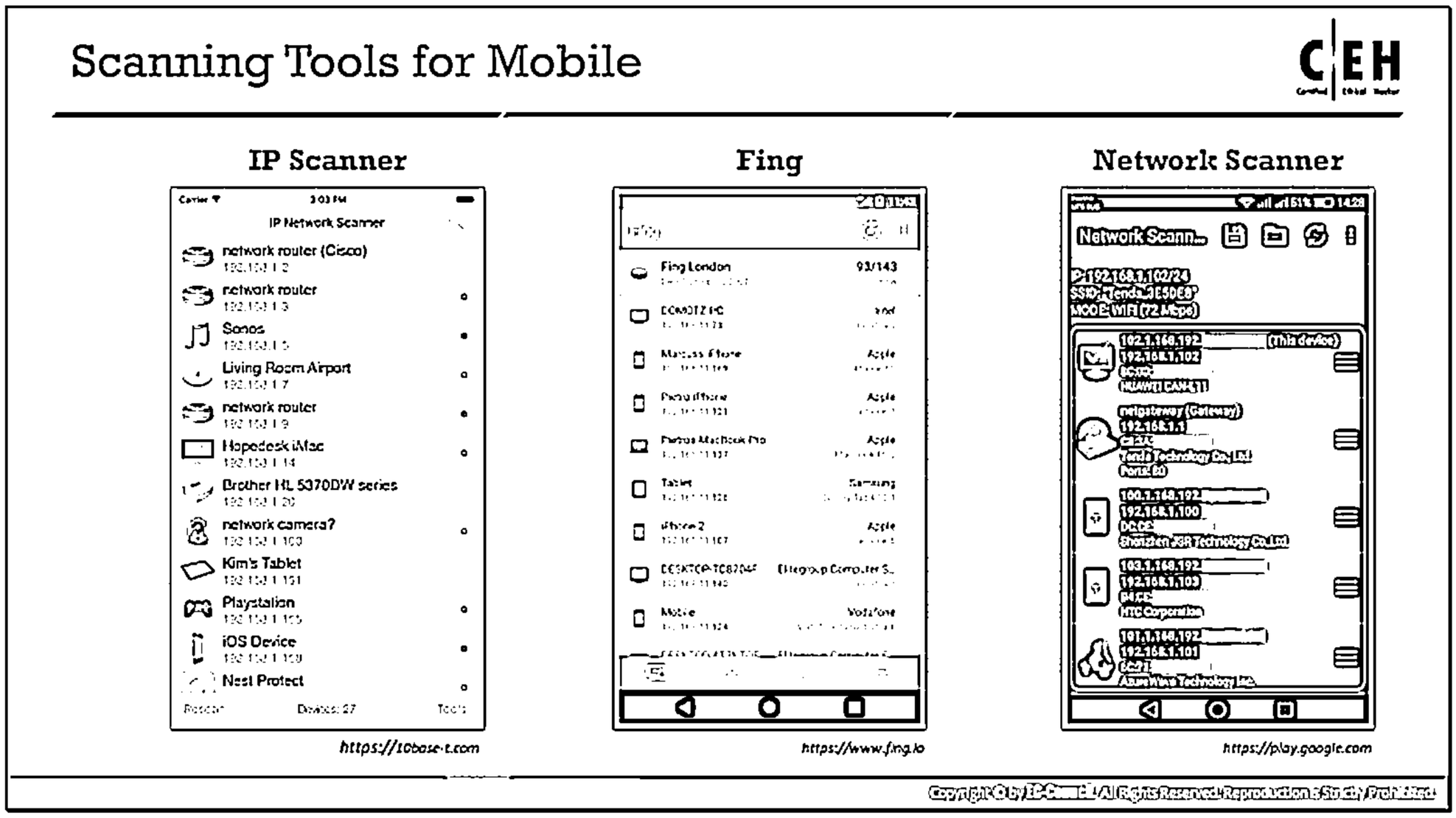


Figure 3.11: Screenshot of NetScanTools Pro

Some additional scanning tools are listed below:

- Unicornscan (*https://sourceforge.net*)
- SolarWinds Port Scanner (*https://www.solarwinds.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- OmniPeek Network Protocol Analyzer (*https://www.savvius.com*)



Scanning Tools for Mobile

- **IP Scanner**

  Source: *https://10base-t.com*

  IP Scanner for iOS scans your local area network to determine the identity of all its active machines and Internet devices. It allows attackers to perform network scanning activities along with ping and port scans.

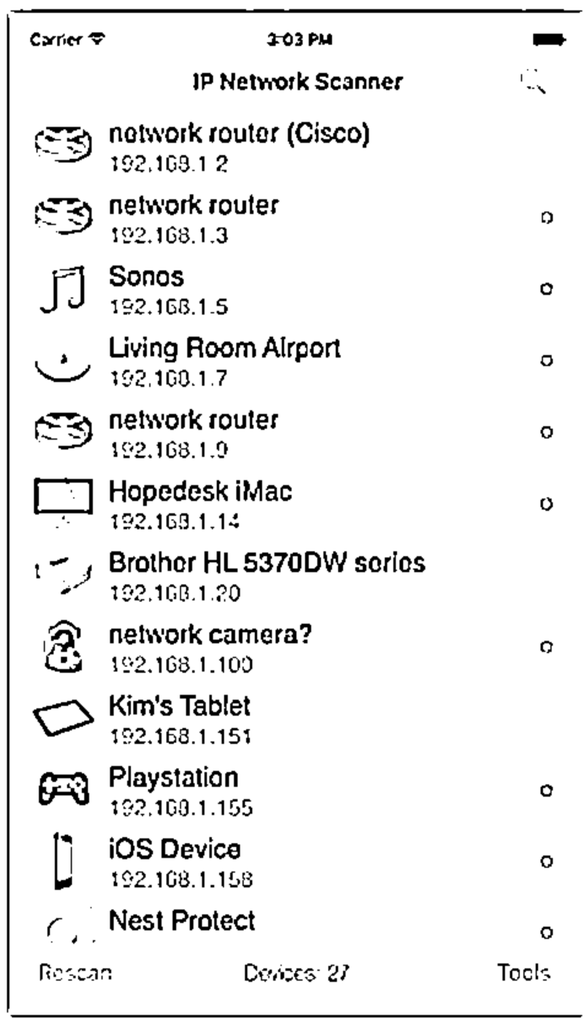


Figure 3.12: Screenshot of IP Scanner

- **Fing**

  Source: *https://www.fing.io*

  Fing is a mobile app for Android and iOS that scans and provides complete network information, such as IP address, MAC address, device vendor, and ISP location. It allows attackers to discover all devices connected to a Wi-Fi network along with their IP and MAC address as well as the name of the vendor/device manufacturer. It also allows attackers to perform network pinging and traceroute activities through specific ports such as SSH, FTP, NetBIOS, etc.

Figure 3.13: Screenshot of Fing

- **Network Scanner**

  Source: *https://play.google.com*

  Network Scanner is an Android mobile application that allows attackers to identify the active host in the range of possible addresses in a network. It also displays IP addresses, MAC addresses, host names, and vendor details of all the available devices in the network. This tool also allows attackers to port scan targets with specific port numbers.

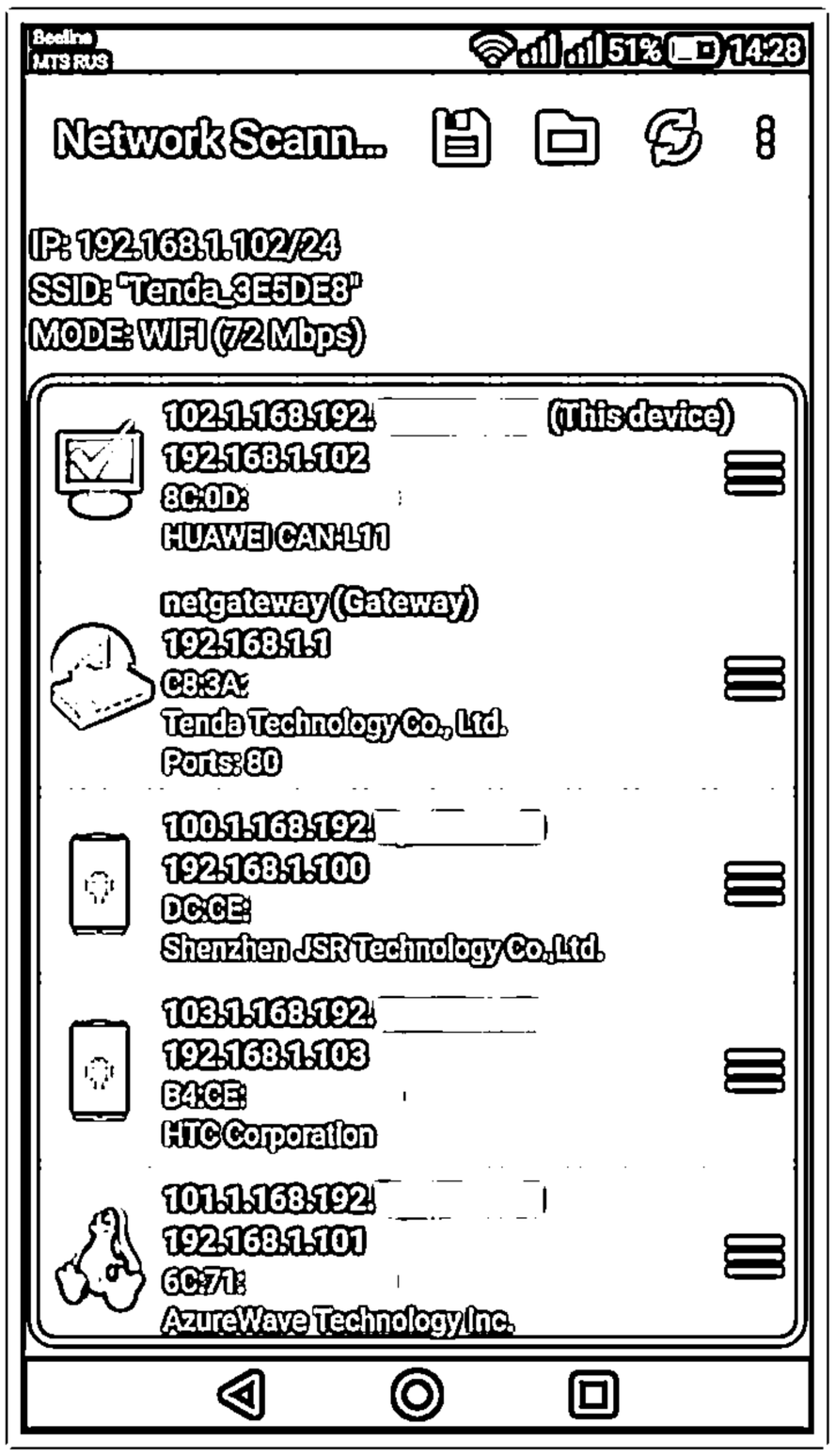
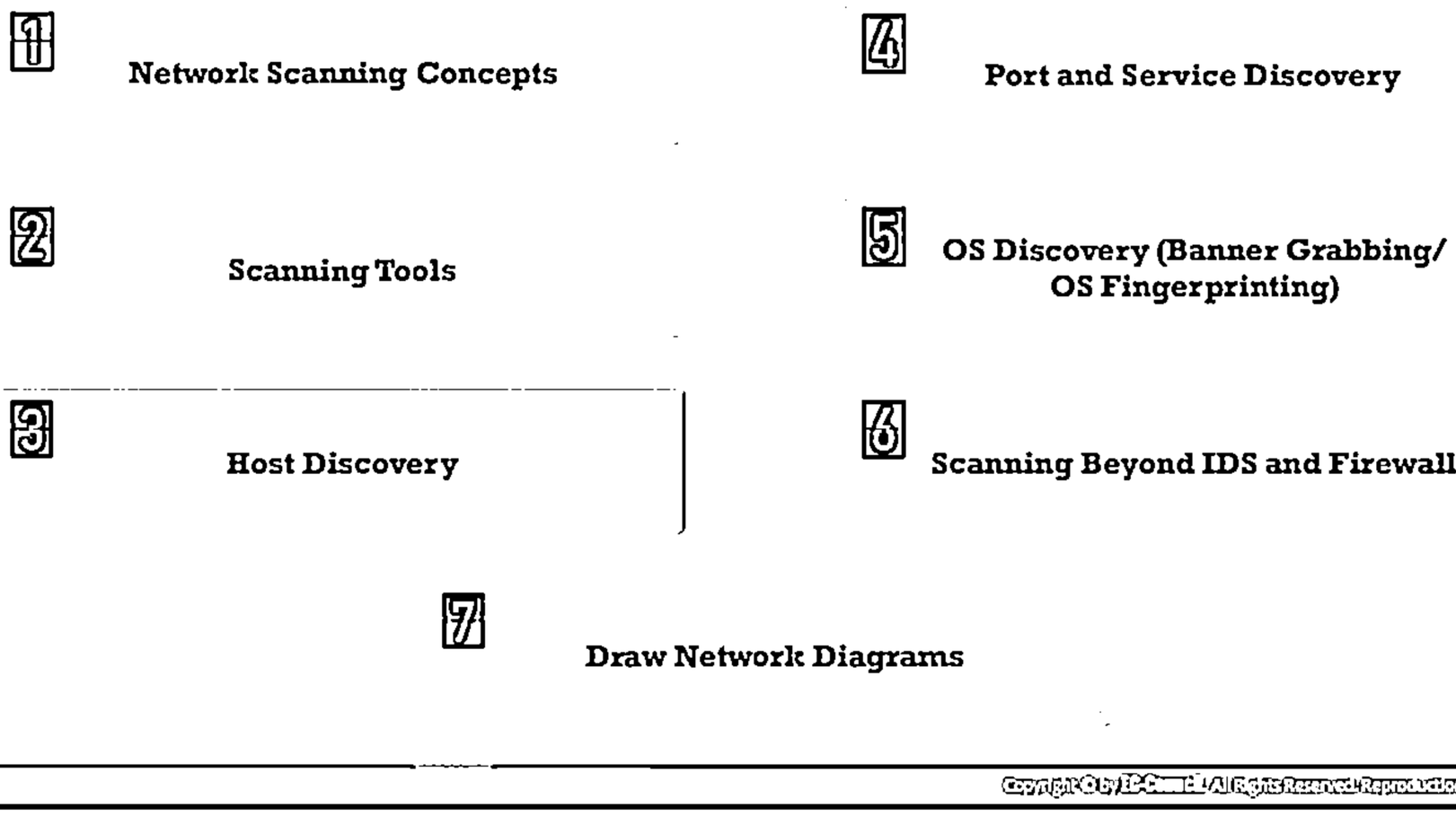


Figure 3.14: Screenshot of Network Scanner

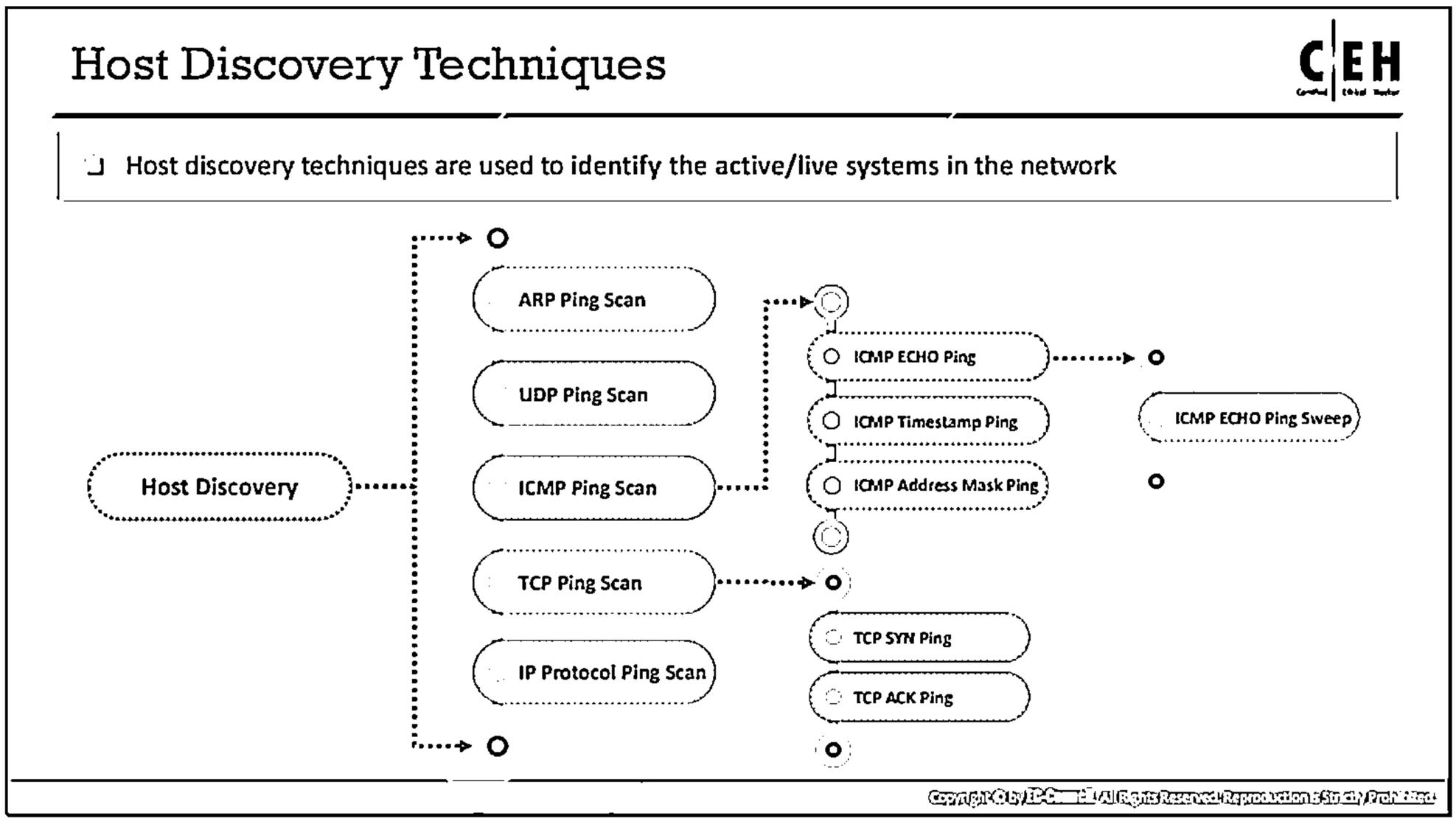
Module Flow



Host Discovery

Scanning is the process of gathering information about systems that are "alive" and responding on the network. Host discovery is considered as the primary task in the network scanning process. To perform a complete scan and identify open ports and services, it is necessary to check for live systems. Host discovery provides an accurate status of the systems in the network, which enables an attacker to avoid scanning every port on every system in a sea of IP addresses to identify whether the target host is up.

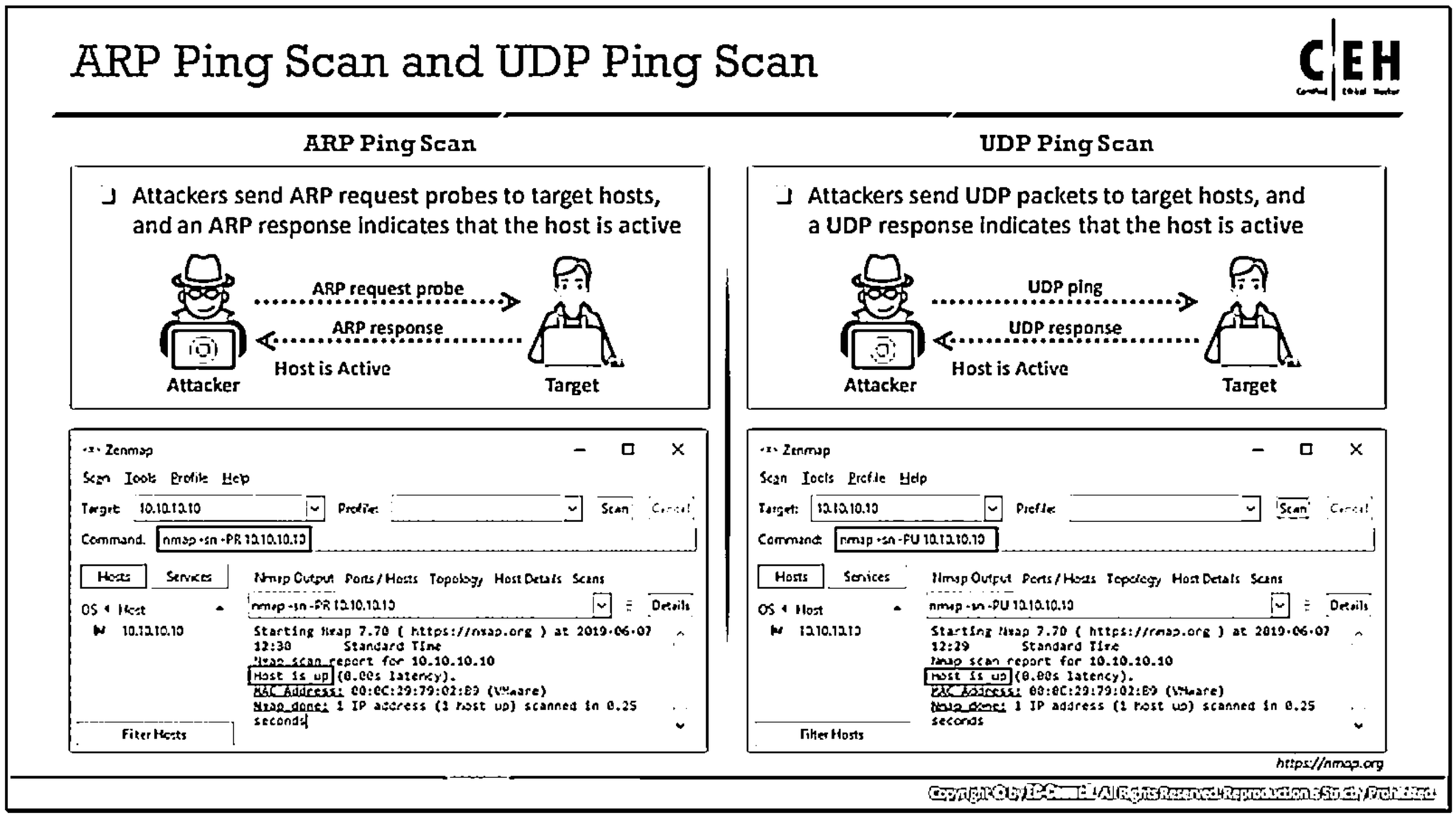
Host discovery is the first step in network scanning. This section highlights how to check for live systems in a network using various ping scan techniques. It also discusses how to ping sweep a network to detect live hosts/systems along with various ping sweep tools.



Host Discovery Techniques

Host discovery techniques can be adopted to discover the active/live hosts in the network. As an ethical hacker, you must be aware of the various types of host discovery techniques. Some host discovery techniques are listed below:

- ARP Ping Scan
- UDP Ping Scan
- ICMP Ping Scan
  - ICMP ECHO Ping
    - ICMP ECHO Ping Sweep
  - ICMP Timestamp Ping
  - ICMP Address Mask Ping
- TCP Ping Scan
  - TCP SYN Ping
  - TCP ACK Ping
- IP Protocol Scan



ARP Ping Scan and UDP Ping Scan

ARP Ping Scan

In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls. In most networks, many IP addresses are unused at any given time, specifically in the private address ranges of the LAN. Hence, when the attackers try to send IP packets such as ICMP echo request to the target host, the OS must determine the hardware destination address (ARP) corresponding to the target IP for addressing the ethernet frame correctly. For this purpose, a series of ARP requests are issued. ARP scan is used to show the MAC address of the network interface on the device, and it can also show the MAC addresses of all devices sharing the same IPv4 address on the LAN. If the host IP with the respective hardware destination address is active, then the ARP response will be generated by the host; otherwise, after a certain number of ping attempts, the original OS gives up on the host. In other words, when attackers send ARP request probes to the target host, if they receive any ARP response, then the host is active. In case the destination host is found to be unresponsive, the source host adds an incomplete entry to the destination IP in its kernel ARP table.

Attackers use the Nmap tool to perform ARP ping scan for discovering live hosts in the network. In Zenmap, the `-PR` option is used to perform ARP ping scan.

Note: `-sn` is the Nmap command to disable the port scan. Since Nmap uses ARP ping scan as the default ping scan, to disable it and perform other desired ping scans, you can use `--disable-arp-ping`.

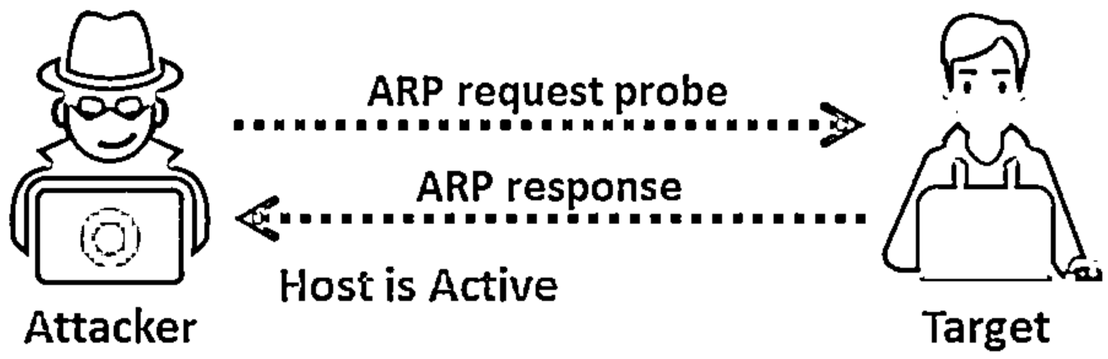


Figure 3.15: ARP ping scan

Advantages:

- ARP ping scan is considered to be more efficient and accurate than other host discovery techniques
- ARP ping scan automatically handles ARP requests, retransmission, and timeout at its own discretion
- ARP ping scan is useful for system discovery, where you may need to scan large address spaces
- ARP ping scan can display the response time or latency of a device to an ARP packet

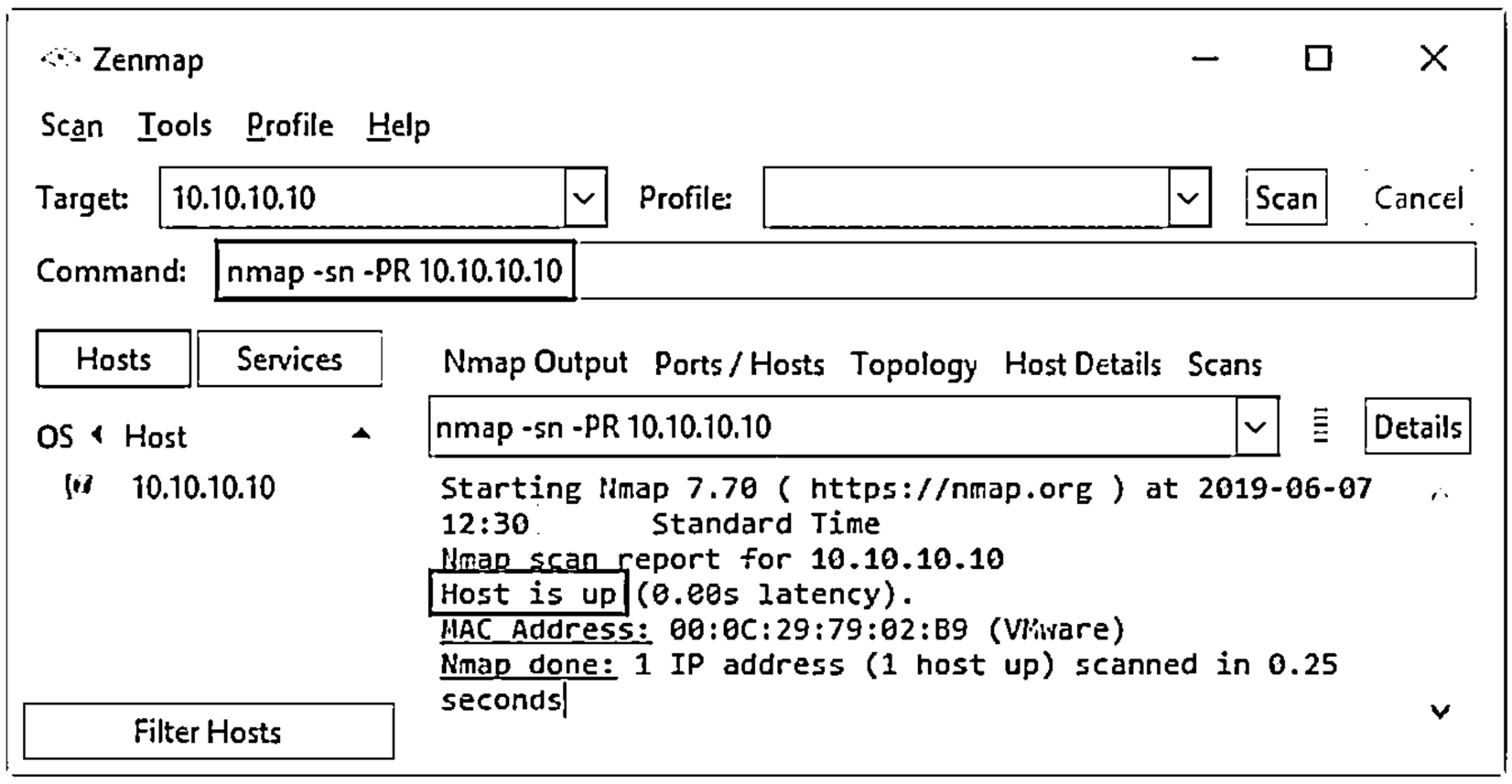


Figure 3.16: ARP scan in Zenmap

UDP Ping scan

UDP ping scan is similar to TCP ping scan; however, in the UDP ping scan, Nmap sends UDP packets to the target host. The default port number used by Nmap for the UDP ping scan is 40,125. This highly uncommon port is used as the default for sending UDP packets to the target. This default port number can be configured using `DEFAULT_UDP_PROBE_PORT_SPEC` during compile time in Nmap.

Attackers send UDP packets to the target host, and a UDP response means that the target host is active. If the target host is offline or unreachable, various error messages such as host/network unreachable or TTL exceeded could be returned. In Zenmap, the **-PU** option is used to perform the UDP ping scan.

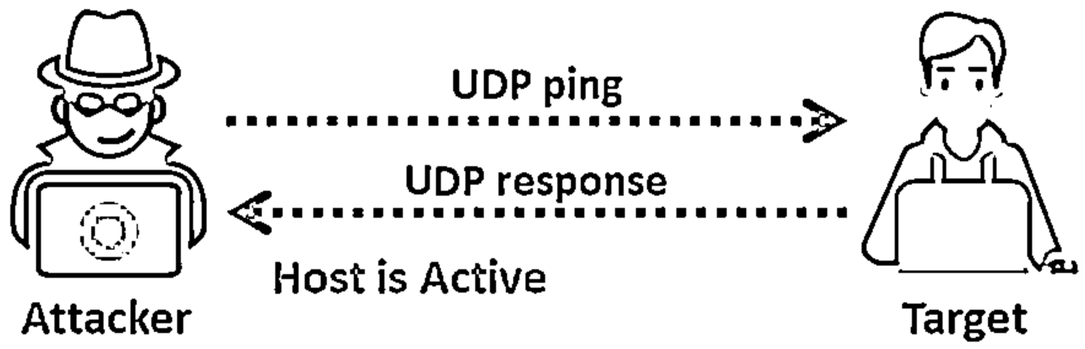


Figure 3.17: UDP ping scan to determine if the host is active

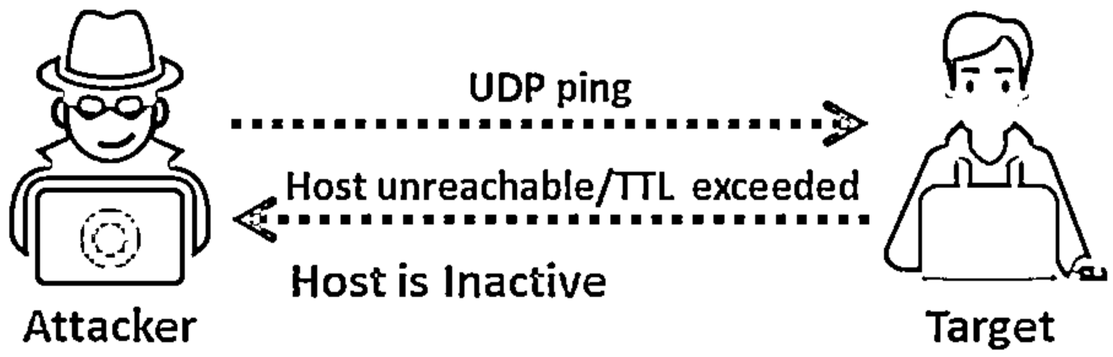


Figure 3.18: UDP ping scan to determine if the host is offline

Advantages:

- UDP ping scans have the advantage of detecting systems behind firewalls with strict TCP filtering, leaving the UDP traffic forgotten.

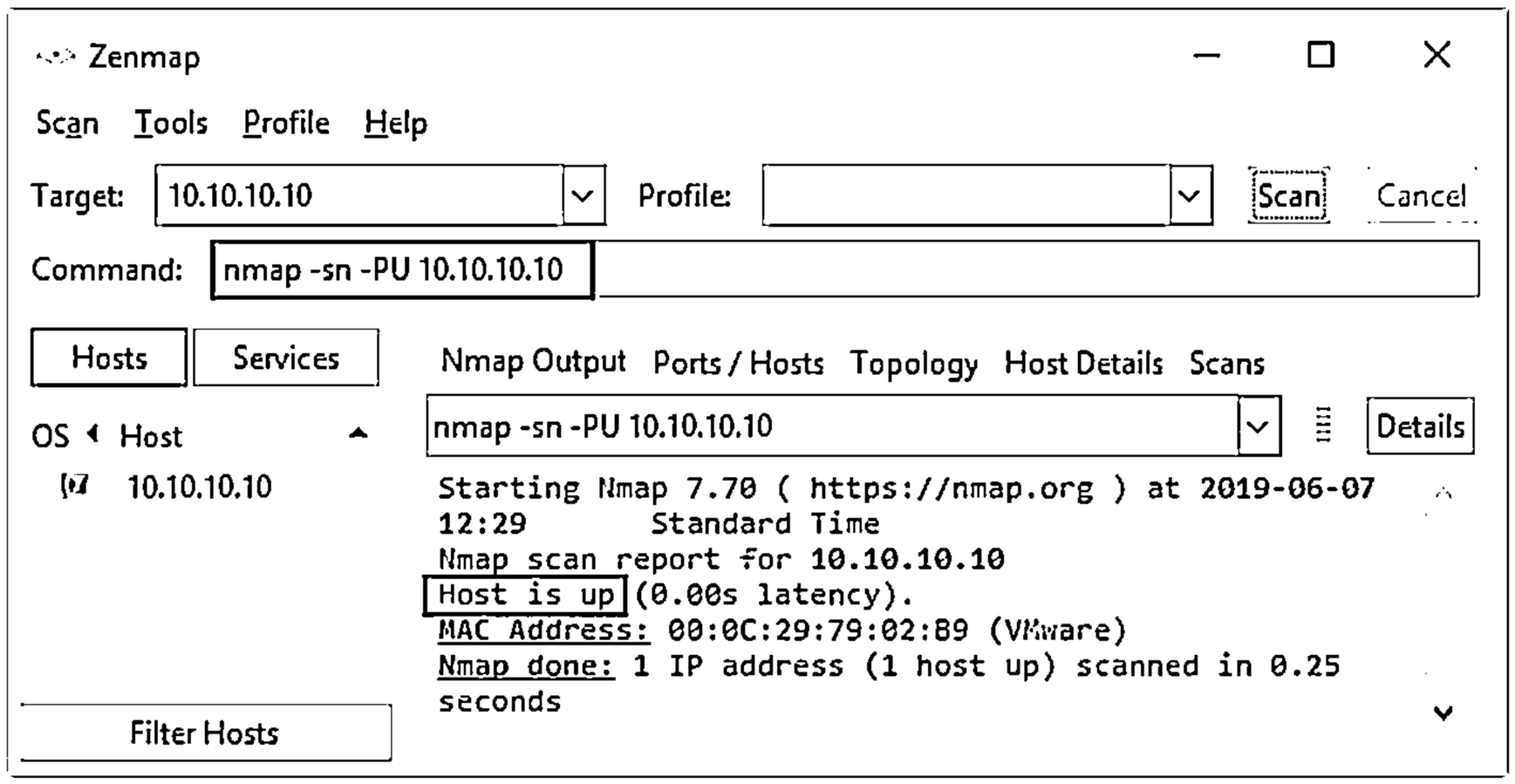
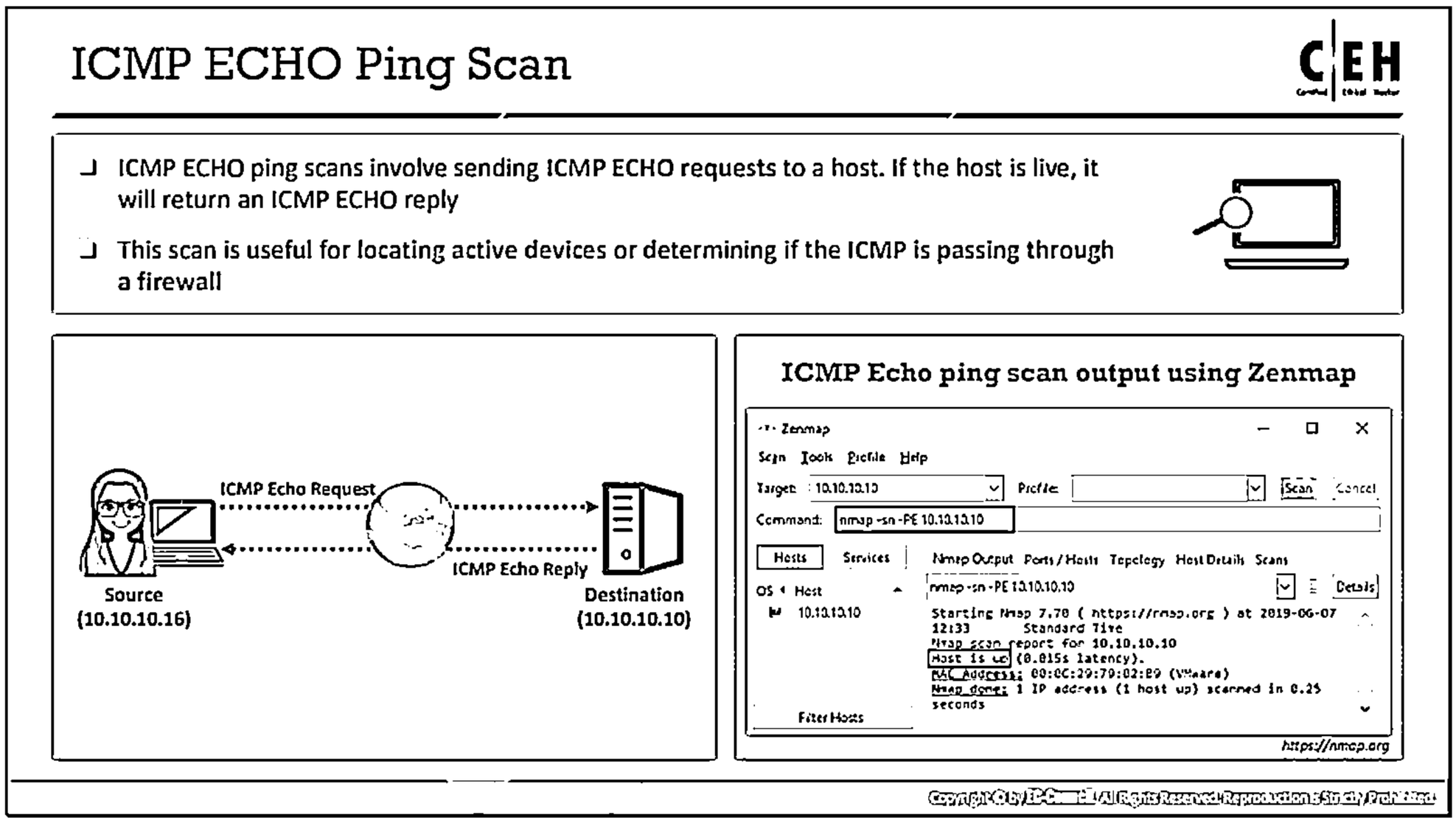


Figure 3.19: UDP ping scan in Zenmap



ICMP ECHO Ping Scan

Attackers use the ICMP ping scan to send ICMP packets to the destination system to gather all necessary information about it. This is because ICMP does not include port abstraction, and it is different from port scanning. However, it is useful to determine what hosts in a network are running by pinging them all.

ICMP ECHO ping scan involves sending ICMP ECHO requests to a host. If the host is alive, it will return an ICMP ECHO reply. This scan is useful for locating active devices or determining if ICMP is passing through a firewall.

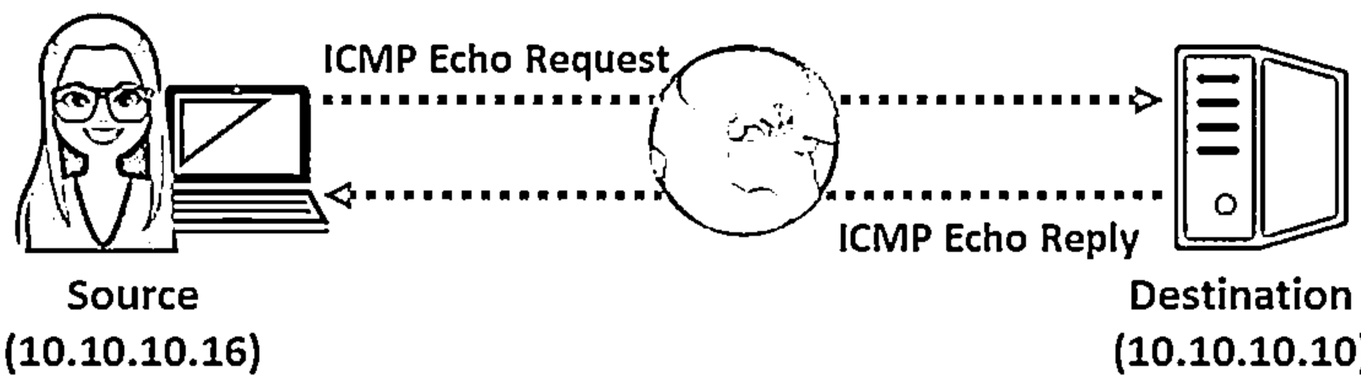


Figure 3.20: ICMP echo request and reply

UNIX/Linux and BSD-based machines use ICMP echo scanning; the TCP/IP stack implementations in these OSs respond to the ICMP echo requests to the broadcast addresses. This technique does not work on Windows-based networks, as their TCP/IP stack implementation does not reply to ICMP probes directed at the broadcast address.

Nmap uses the `-P` option to ICMP scan the target. The user can also increase the number of pings in parallel using the `-L` option. It may also be useful to tweak the ping timeout value using the `-T` option.

In Zenmap, the **-PE** option is used to perform the ICMP ECHO ping scan. Active hosts are displayed as "**Host is up,**" as shown in the screenshot.

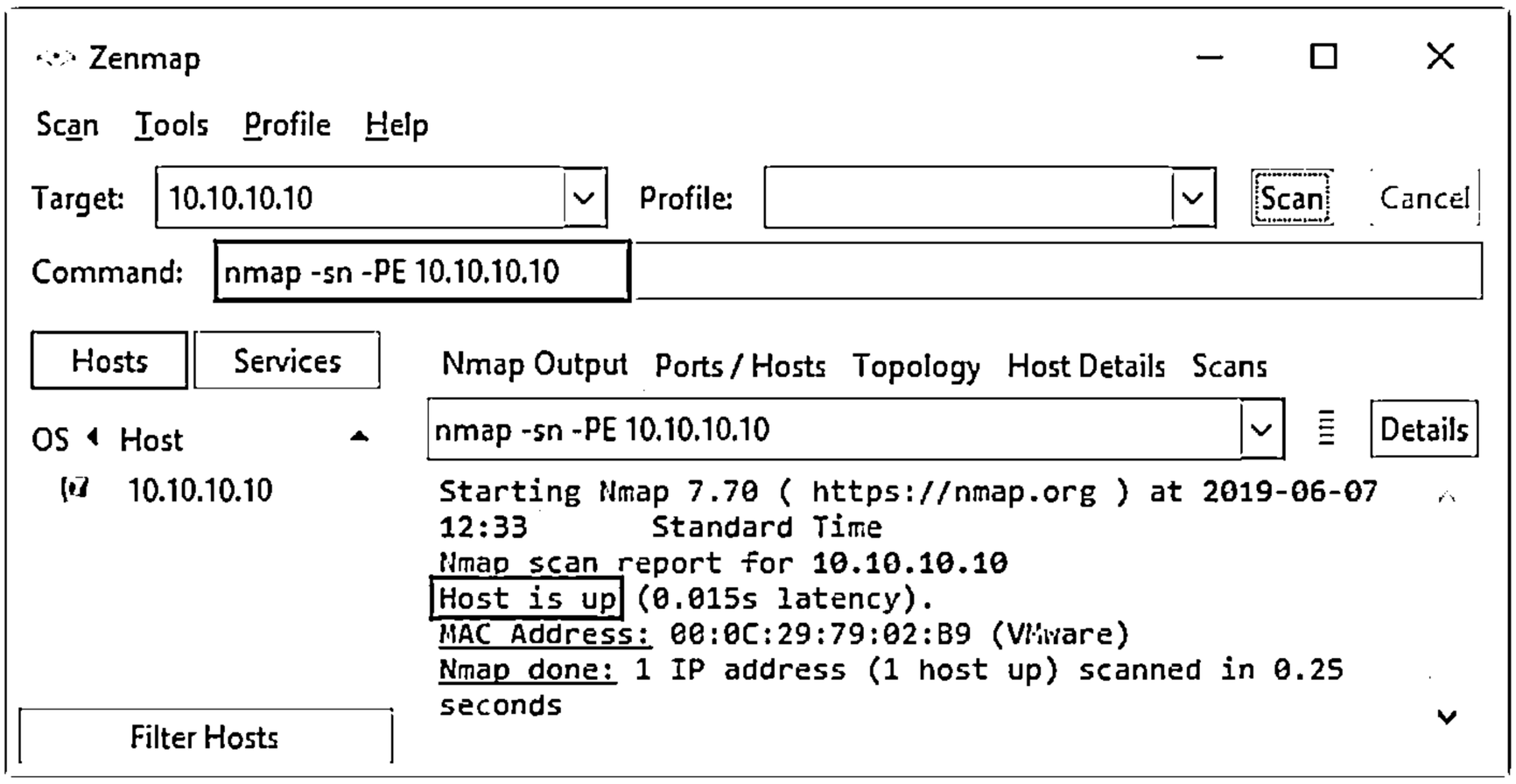
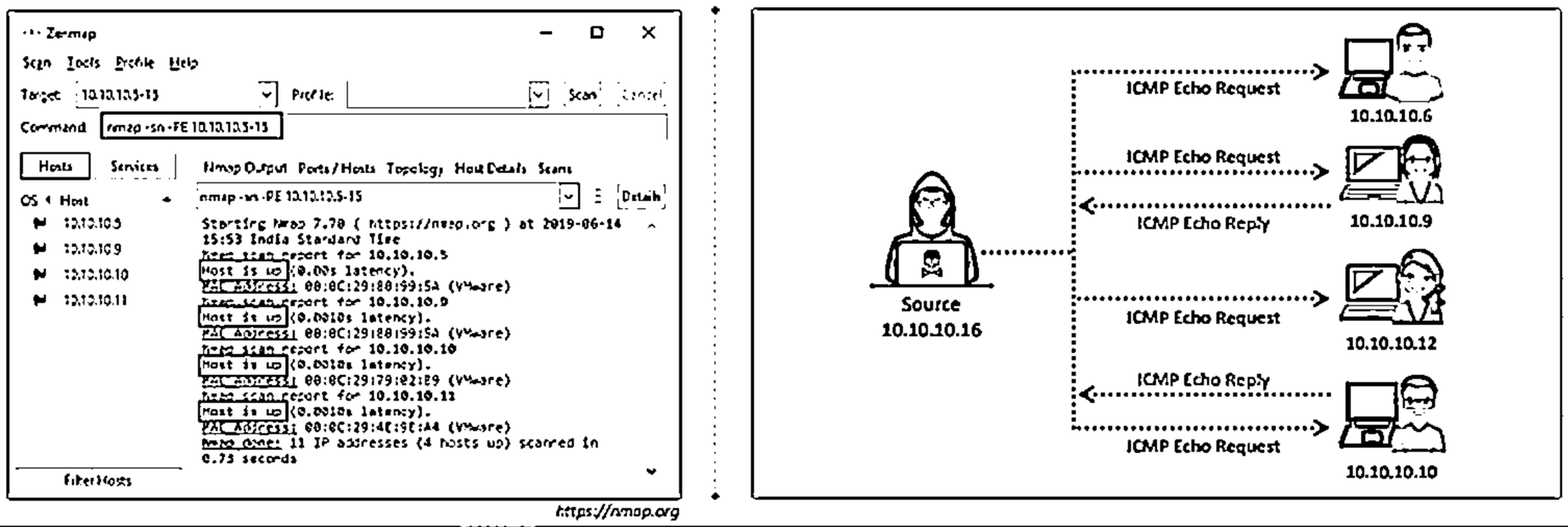


Figure 3.21: ICMP Echo ping scan output using Zenmap

ICMP ECHO Ping Sweep

- Ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is alive, it will return an ICMP ECHO reply
- Attackers calculate subnet masks by using a Subnet Mask Calculator to identify the number of hosts that are present in the subnet
- Attackers subsequently use a ping sweep to create an inventory of live systems in the subnet



ICMP ECHO Ping Sweep

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique that is adopted to determine the range of IP addresses that map to live hosts (computers). Although a single ping will tell the user whether a specified host computer exists on the network, a ping sweep consists of ICMP ECHO requests sent to multiple hosts. If a specified host is active, it will return an ICMP ECHO reply.

Ping sweeps are among the oldest and slowest methods used to scan a network. This utility is distributed across nearly all platforms, and it acts as a roll call for systems; a system that is active on the network answers the ping query that another system sends out.

ICMP echo scanning pings all the machines in the target network to discover live machines. Attackers send ICMP probes to the broadcast or network address, which relays to all the host addresses in the subnet. The live systems will send the ICMP echo reply message to the source of the ICMP echo probe.

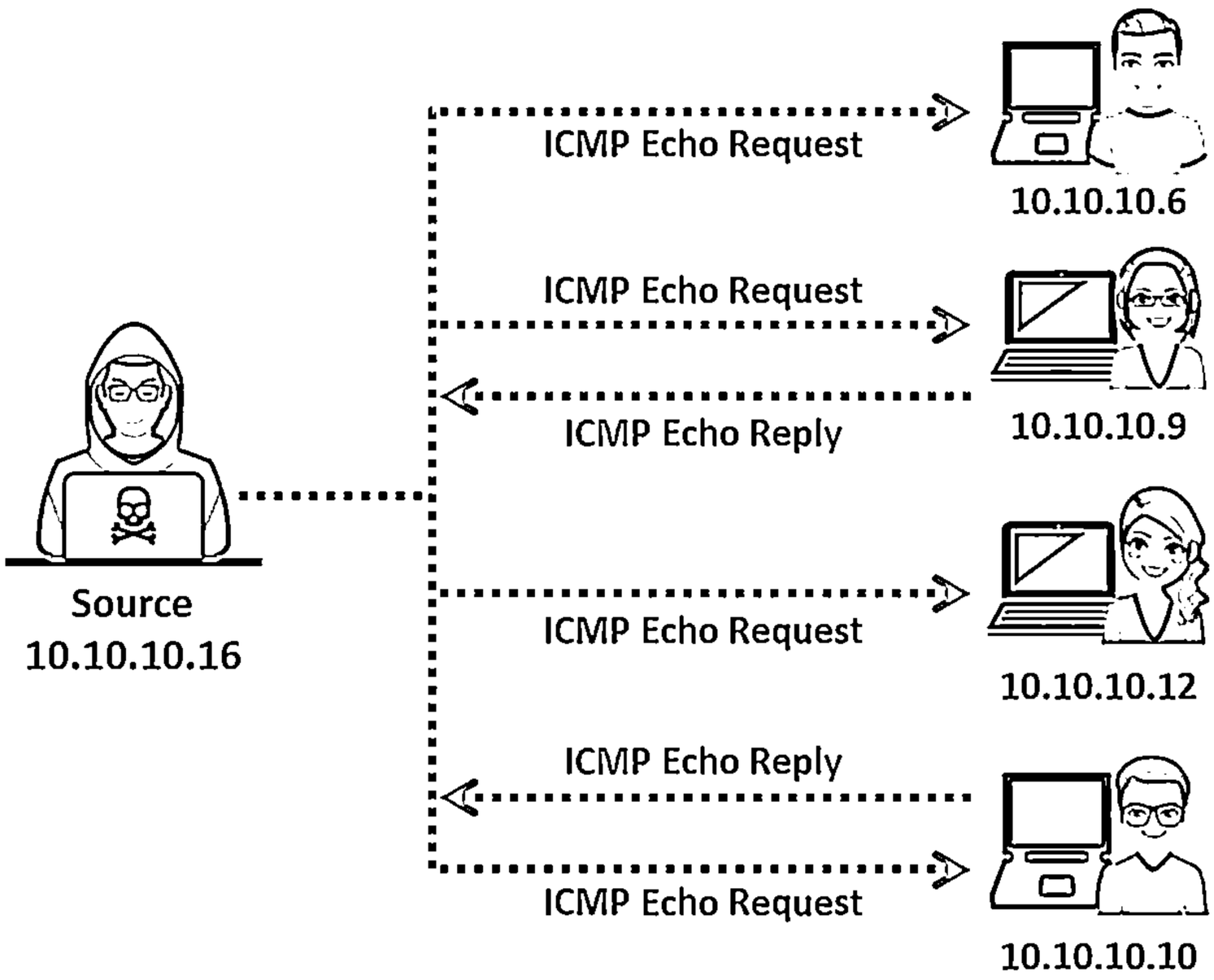


Figure 3.22: ICMP ECHO Ping Sweep

To understand pings better, one should be able to understand the TCP/IP packet. When a system pings, it sends a single packet across the network to a specific IP address. This packet contains 64 bytes (56 data bytes and 8 bytes of protocol header information). The sender then waits or listens for a return packet from the target system. If the connections are good and the target computer is "alive," a good return packet is expected. However, this will not be the case if there is a disruption in communication. Pings also detail the time taken for a packet to make a complete trip, called the "round-trip time." They also help in resolving hostnames. In this case, if the packet bounces back when sent to the IP address, but not when sent to the name, then the system is unable to reconcile the name with the specific IP address.

Attackers calculate subnet masks using subnet mask calculators to identify the number of hosts that are present in the subnet. They subsequently use ping sweep to create an inventory of live systems in the subnet.

ICMP ECHO Ping Sweep Using Nmap

Source: *https://nmap.org*

Nmap helps an attacker to perform a ping sweep that determines live hosts from a range of IP addresses. In Zenmap, the `-PE` option with a list of IP addresses is used to perform ICMP ECHO ping sweep.

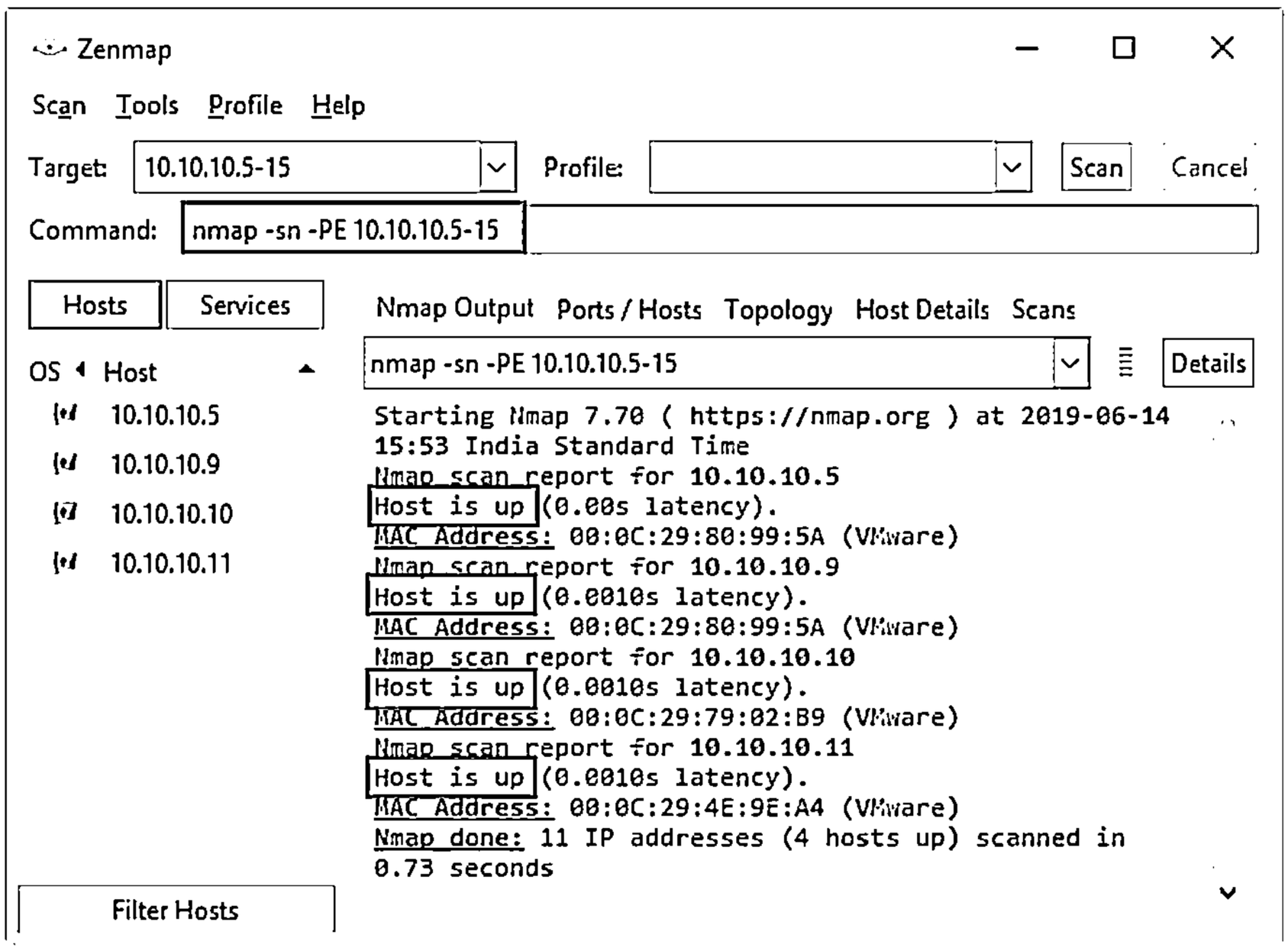
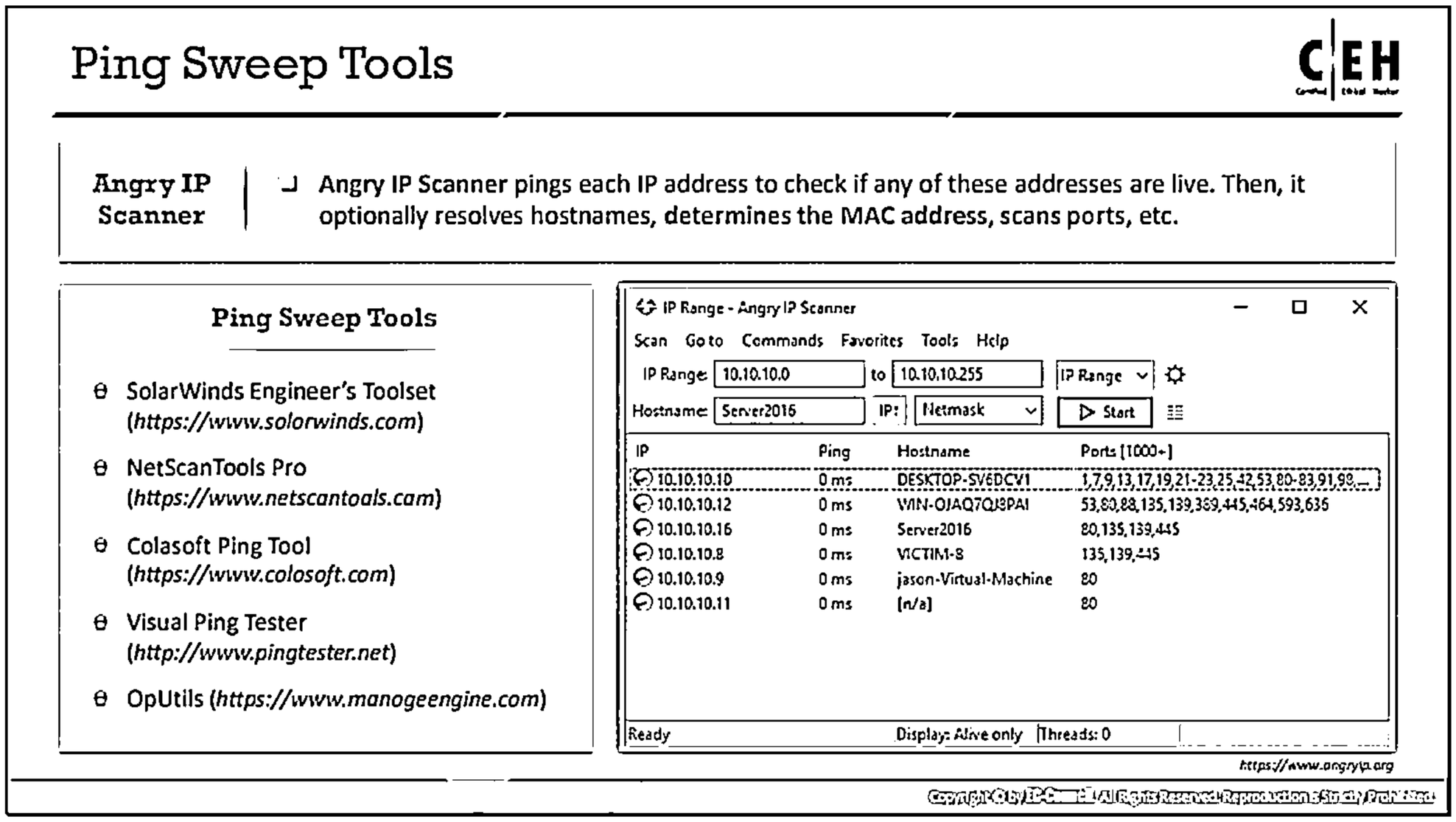


Figure 3.23: Ping Sweep output using Zenmap



Ping Sweep Tools

Ping sweep tools ping an entire range of network IP addresses to identify the live systems. The following are ping sweep tools that enable one to determine live hosts on the target network by sending multiple ICMP ECHO requests to various hosts on the network at a time.

- **Angry IP Scanner**

  Source: https://www.angryip.org

  Angry IP scanner is an IP address and port scanner. It can scan IP addresses in any range as well as any of their ports. It pings each IP address to check if it is alive; then, it optionally resolves its hostname, determines the MAC address, scans ports, and so on. The amount of data gathered about each host increases with plugins. Angry IP scanner has additional features, such as NetBIOS information (computer name, workgroup name, and currently logged in Windows user), favorite IP address ranges, web server detection, and customizable openers. The tool allows the user to save the scanning results to CSV, TXT, XML, or IP-Port list files. To increase the scanning speed, it uses a multithreaded approach: a separate scanning thread is created for each scanned IP address.

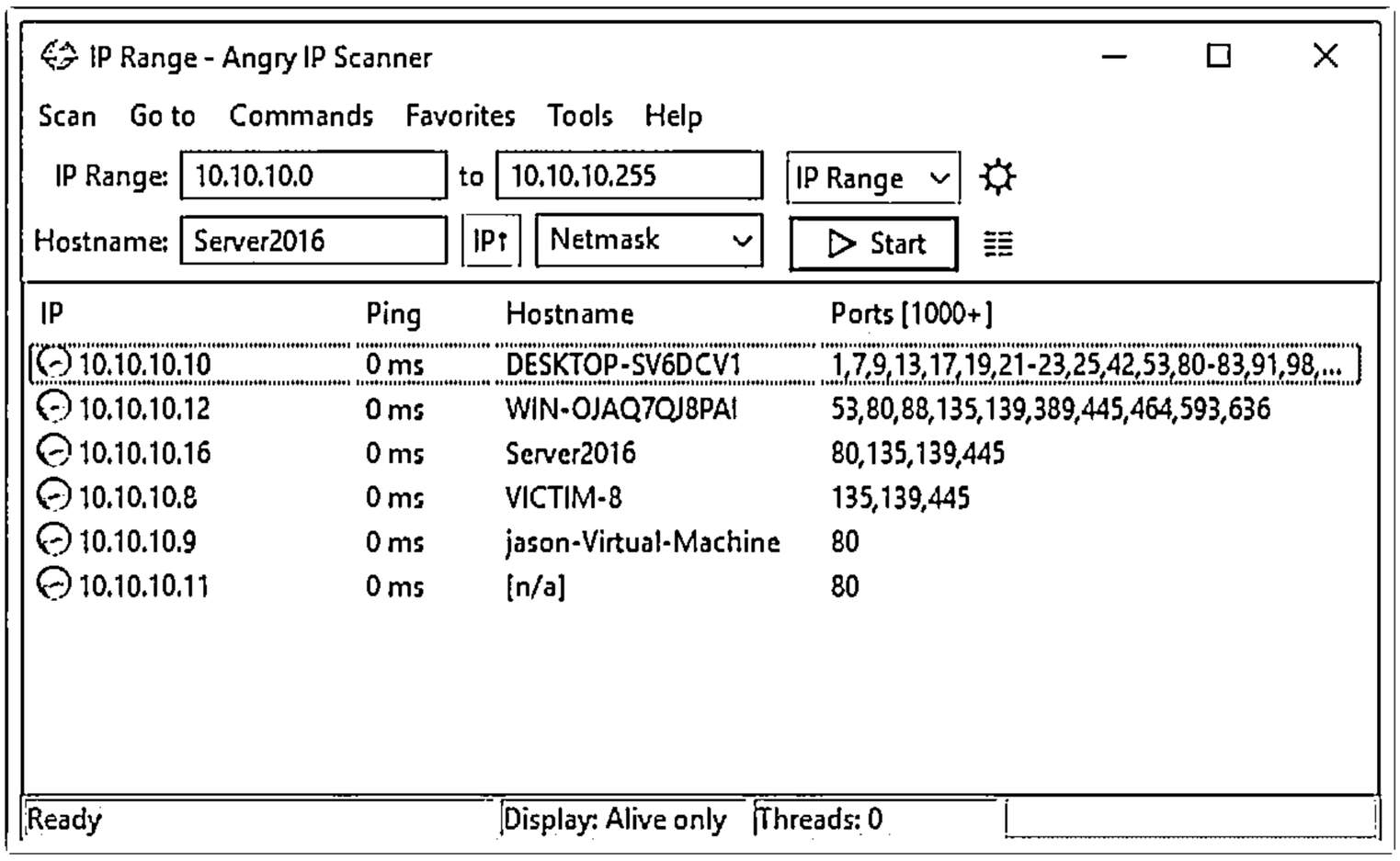


Figure 3.24: Screenshot of Angry IP Scanner showing live hosts

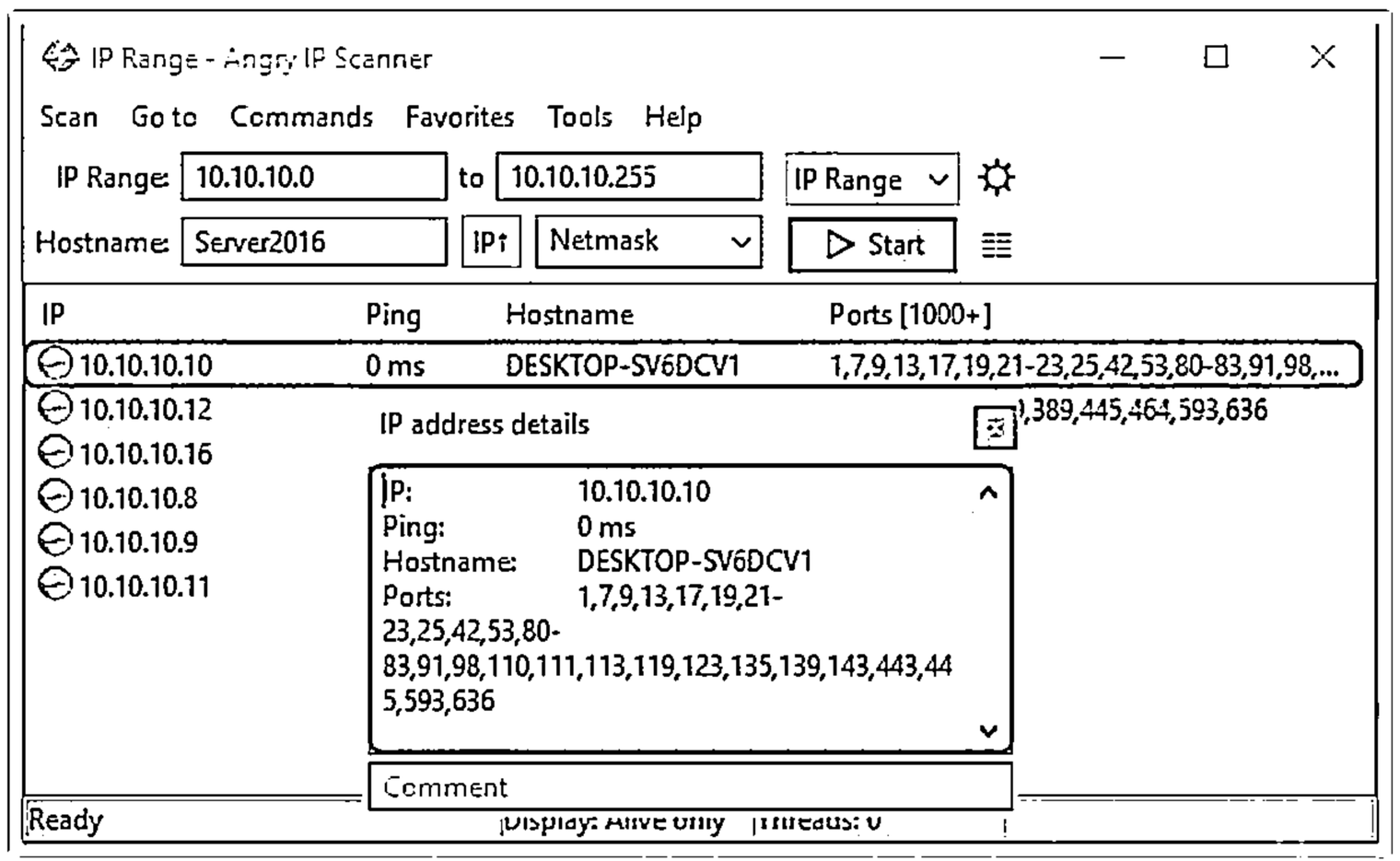
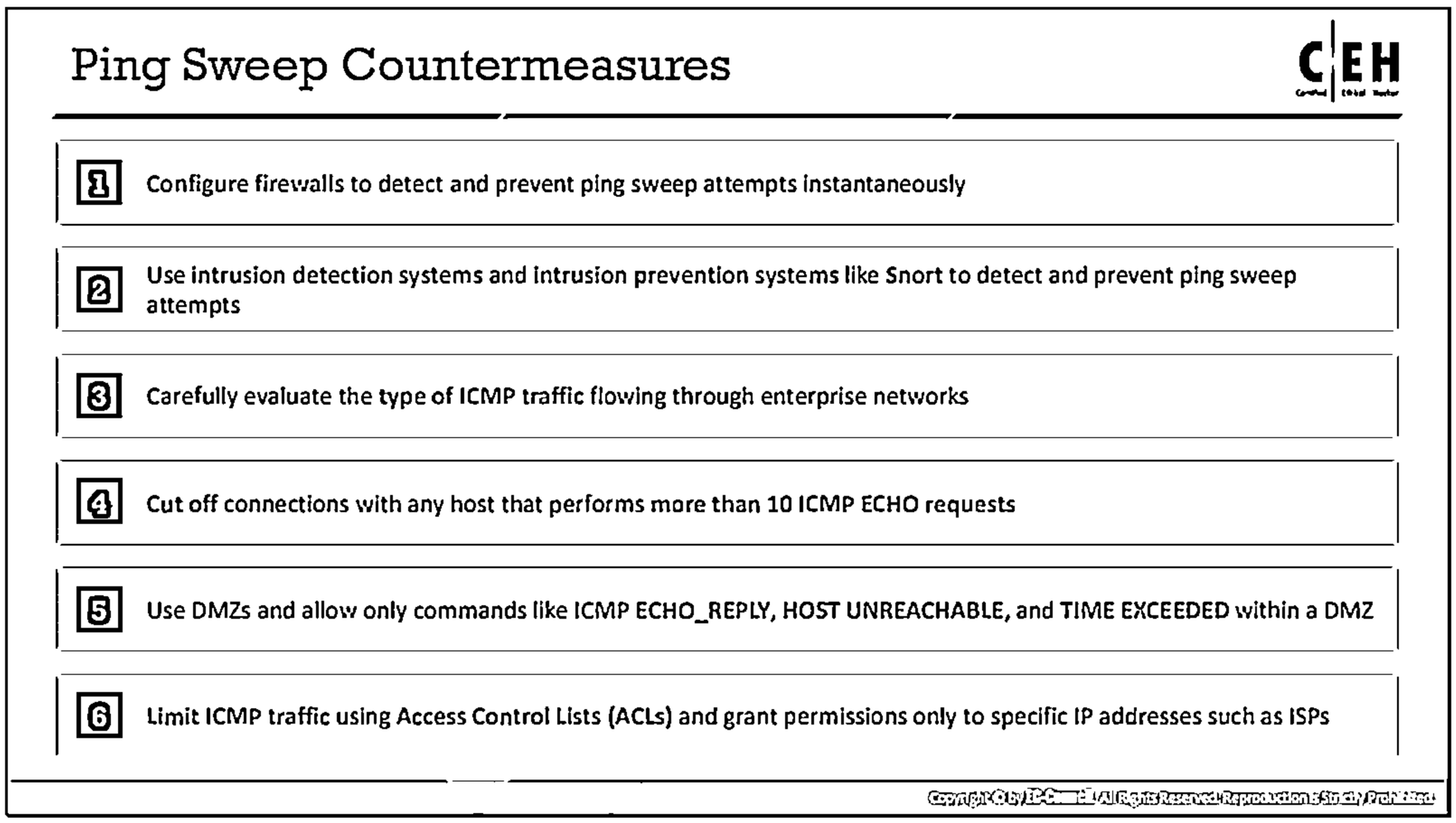


Figure 3.25: Screenshot of Angry IP Scanner showing complete details of live hosts

Some additional ping sweep tools that an attacker uses to determine live hosts on the target network are listed below:

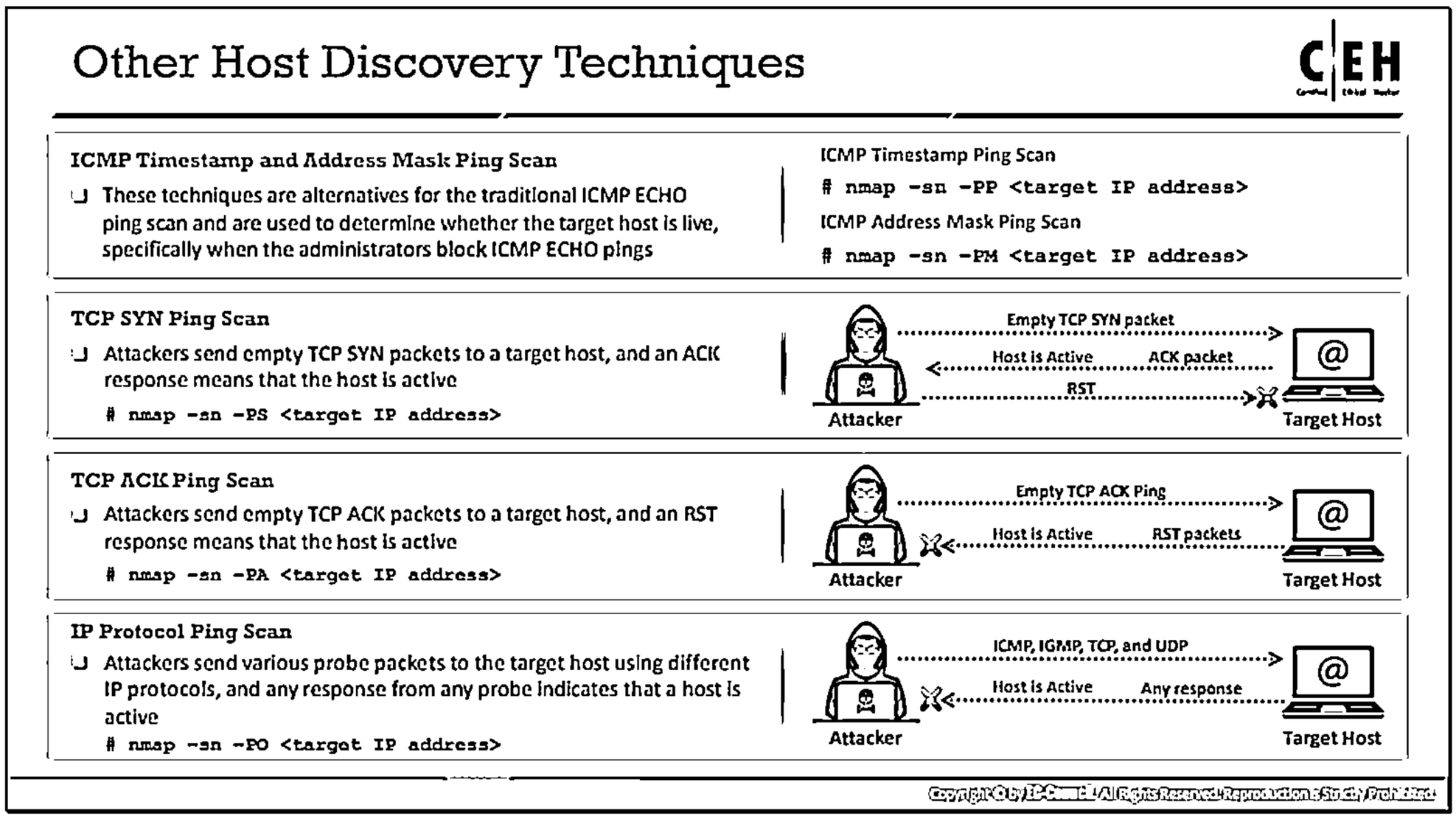
- SolarWinds Engineer's Toolset (*https://www.solarwinds.com*)
- NetScanTools Pro (*https://www.netscantools.com*)
- Colasoft Ping Tool (*https://www.colasoft.com*)
- Visual Ping Tester (*http://www.pingtester.net*)
- OpUtils (*https://www.manageengine.com*)



Ping Sweep Countermeasures

Some countermeasures for avoiding ping sweep are as follows:

- Configure the firewall to detect and prevent ping sweep attempts instantaneously
- Use intrusion detection systems and intrusion prevention systems such as Snort (*https://www.snort.org*) to detect and prevent ping sweep attempts
- Carefully evaluate the type of ICMP traffic flowing through the enterprise networks
- Terminate the connection with any host that is performing more than 10 ICMP ECHO requests
- Use DMZ and allow only commands such as `ICMP ECHO_REPLY`, `HOST UNREACHABLE`, and `TIME EXCEEDED` in DMZ Zone
- Limit the ICMP traffic with Access Control Lists (ACLs) to your ISP's specific IP addresses



Other Host Discovery Techniques

ICMP Timestamp Ping Scan

Besides the traditional ICMP ECHO ping, there are some other types of ICMP pinging techniques such as ICMP timestamp ping scan and ICMP address mask ping scan, which an attacker can adopt in specific conditions.

ICMP timestamp ping is an optional and additional type of ICMP ping whereby the attackers query a timestamp message to acquire the information related to the current time from the target host machine. The target machine responds with a timestamp reply to each timestamp query that is received. However, the response from the destination host is conditional, and it may or may not respond with the time value depending on its configuration by the administrator at the target's end. This ICMP timestamp pinging is generally used for time synchronization. Such a ping method is effective in identifying whether the destination host machine is active, specifically in the condition where the administrator blocks the traditional ICMP ECHO ping requests. In Zenmap, the `-PP` option is used to perform an ICMP timestamp ping scan.

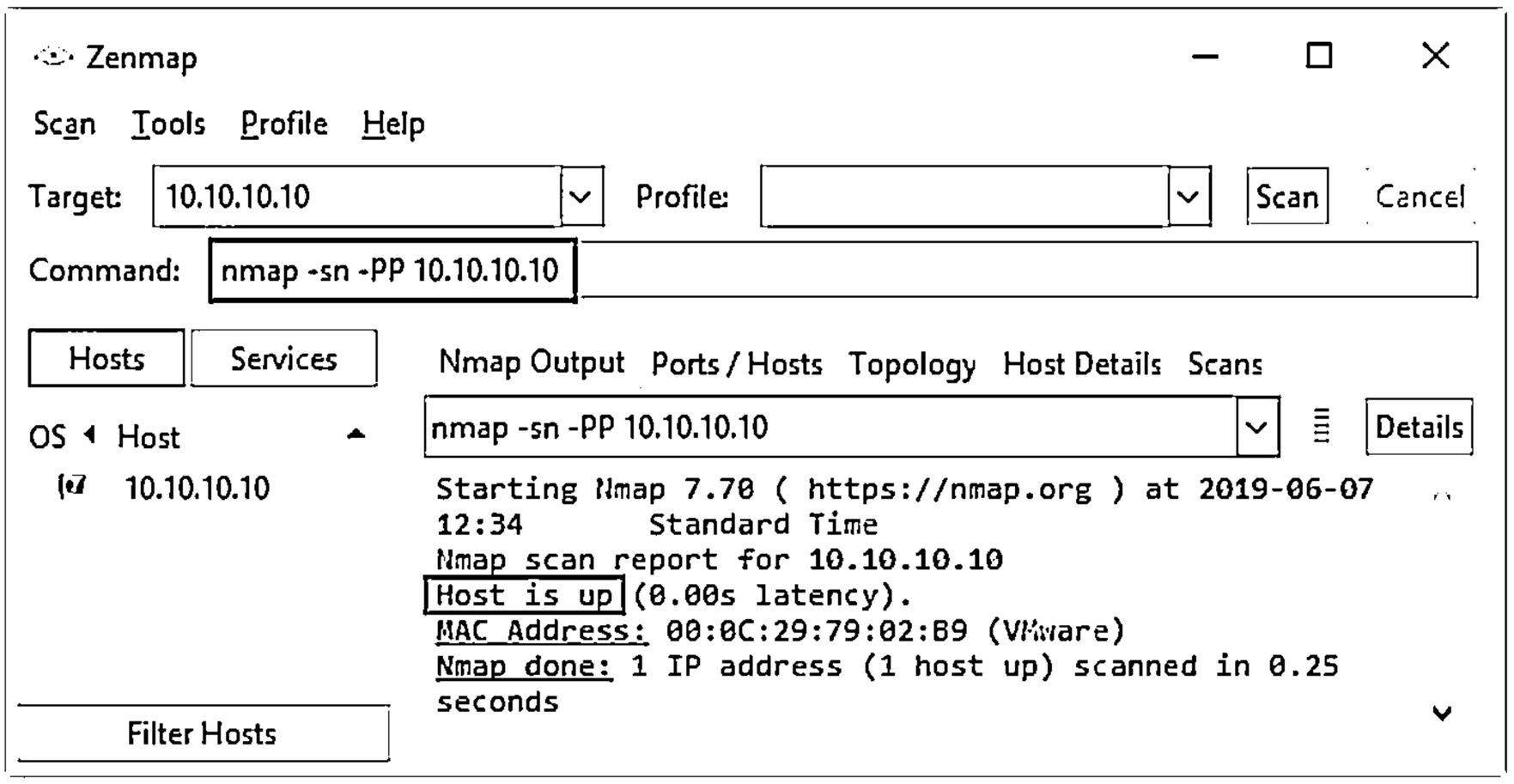


Figure 3.26: ICMP timestamp ping in Zenmap

ICMP Address Mask Ping Scan

ICMP address mask ping is another alternative to the traditional ICMP ECHO ping, where the attackers send an ICMP address mask query to the target host to acquire information related to the subnet mask. However, the address mask response from the destination host is conditional, and it may or may not respond with the appropriate subnet value depending on its configuration by the administrator at the target's end. This type of ping method is also effective in identifying the active hosts similarly to the ICMP timestamp ping, specifically when the administrator blocks the traditional ICMP Echo ping. In Zenmap, the `-PM` option is used to perform an ICMP address mask ping scan.

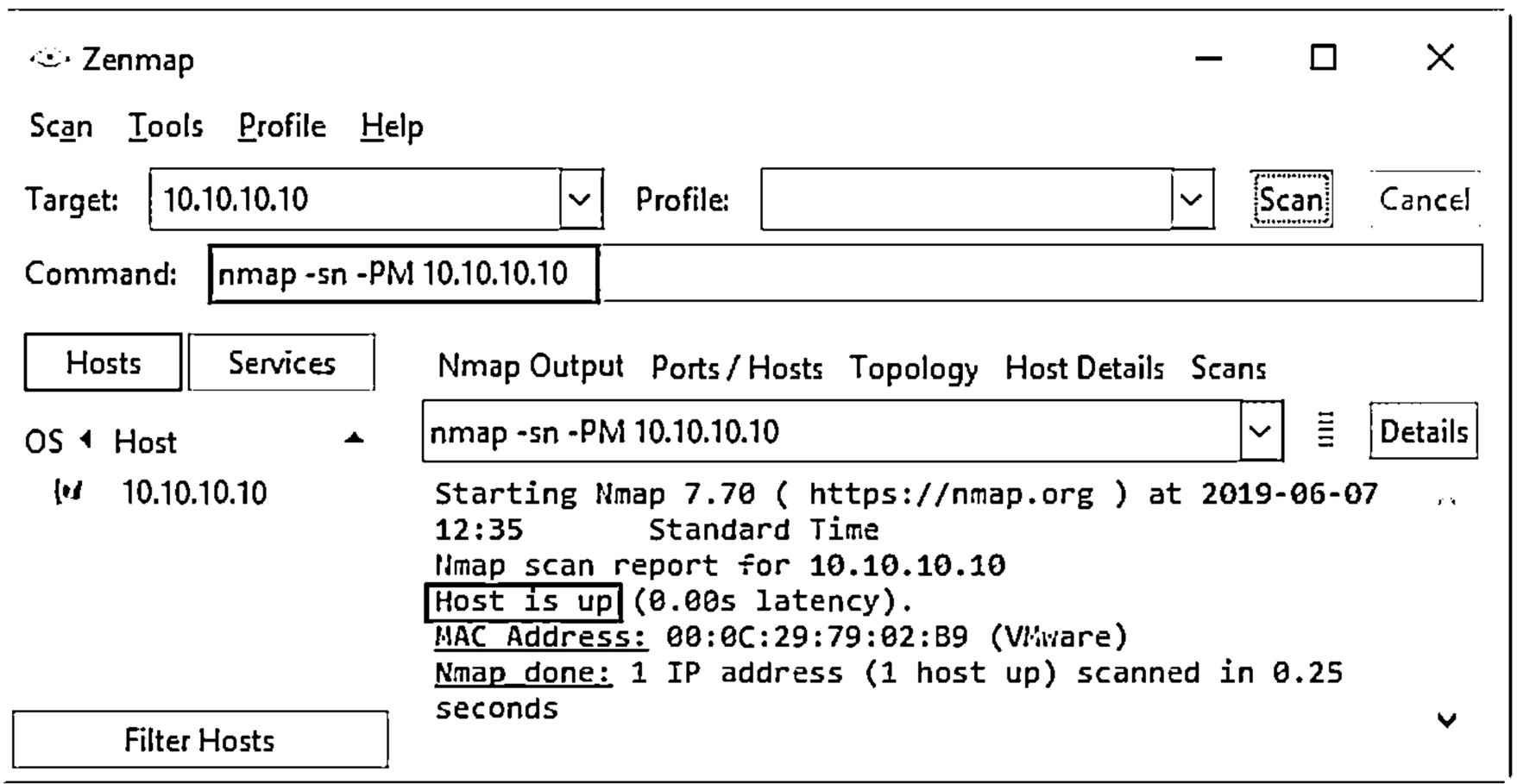


Figure 3.27: ICMP address mask ping in Zenmap

TCP SYN Ping Scan

TCP SYN ping is a host discovery technique for probing different ports to determine if the port is online and to check if it encounters any firewall rule sets. In this type of host discovery technique, an attacker uses the Nmap tool to initiate the three-way handshake by sending the empty TCP SYN flag to the target host. After receiving SYN, the target host acknowledges the receipt with an ACK flag. After reception of the ACK flag, the attacker confirms that the target host is active and terminates the connection by sending an RST flag to the target host machine (since his/her objective of host discovery is accomplished). Port 80 is used as the default destination port. A range of ports can also be specified in this type of pinging format without inserting a space between -PS and the port number (e.g., **PS22-25,80,113,1050,35000**), where the probe will be performed against each port parallelly. In Zenmap, the **-PS** option is used to perform a TCP SYN ping scan.

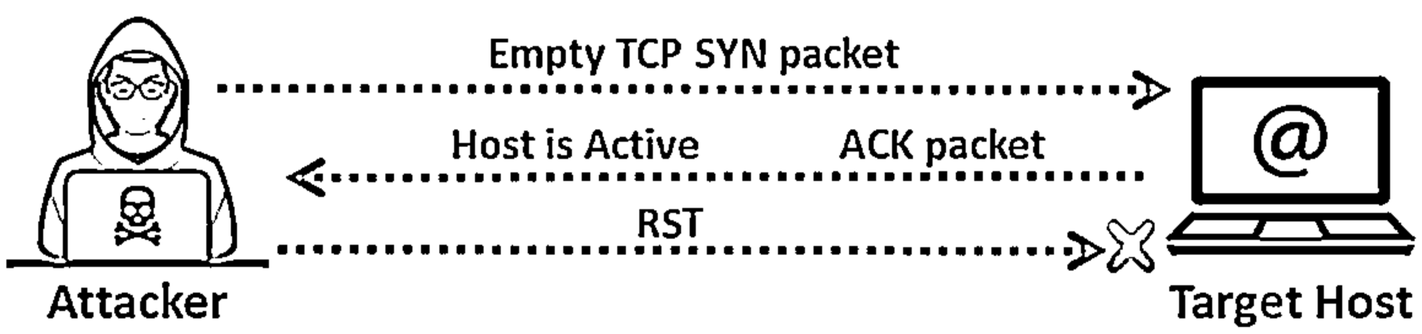


Figure 3.28: TCP SYN ping scan for host discovery

Advantages:

- As the machines can be scanned parallelly, the scan never gets the time-out error while waiting for the response.
- TCP SYN ping can be used to determine if the host is active without creating any connection. Hence, the logs are not recorded at the system or network level, enabling the attacker to leave no traces for detection.

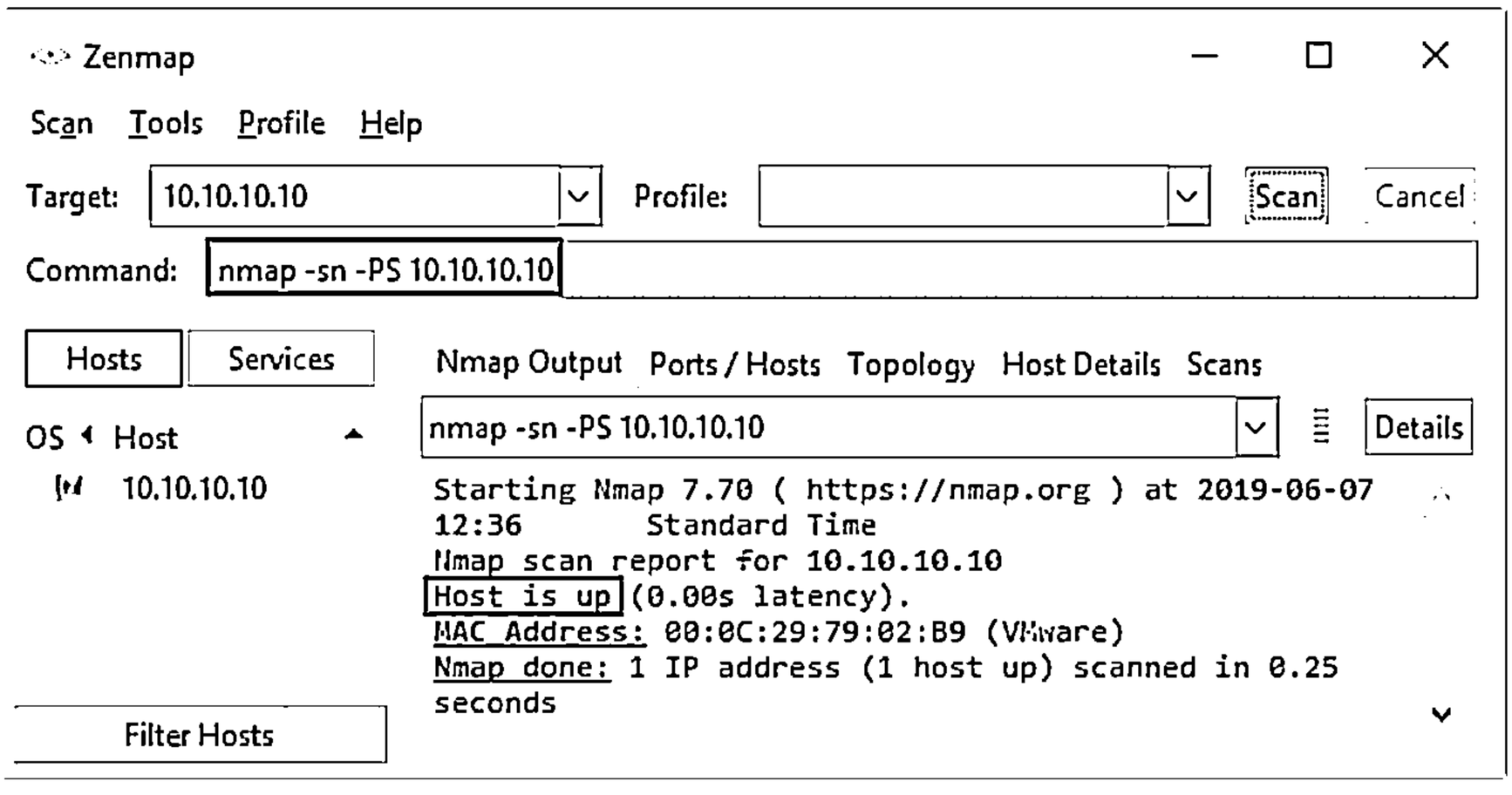


Figure 3.29: TCP SYN ping scan in Zenmap

TCP ACK Ping Scan

TCP ACK ping is similar to TCP SYN ping, albeit with minor variations. TCP ACK ping also uses the default port 80. In the TCP ACK ping technique, the attackers send an empty TCP ACK packet to the target host directly. Since there is no prior connection between the attacker and the target host, after receiving the ACK packet, the target host responds with an RST flag to terminate the request. The reception of this RST packet at the attacker's end indicates that the host inactive. In Zenmap, the `-PA` option is used to perform a TCP ACK ping scan.

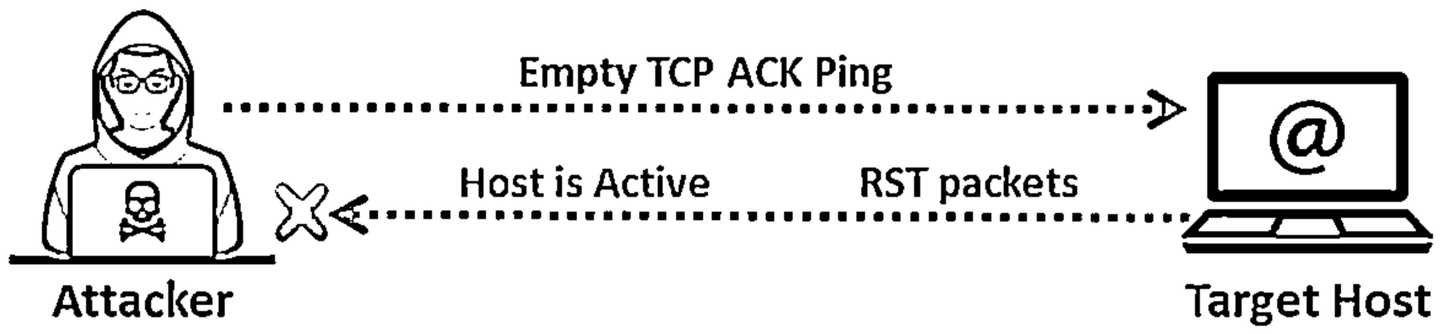


Figure 3.30: TCP ACK ping scan for host discovery

Advantages:

- Both the SYN and the ACK packet can be used to maximize the chances of bypassing the firewall. However, firewalls are mostly configured to block the SYN ping packets, as they are the most common pinging technique. In such cases, the ACK probe can be effectively used to bypass these firewall rule sets easily.

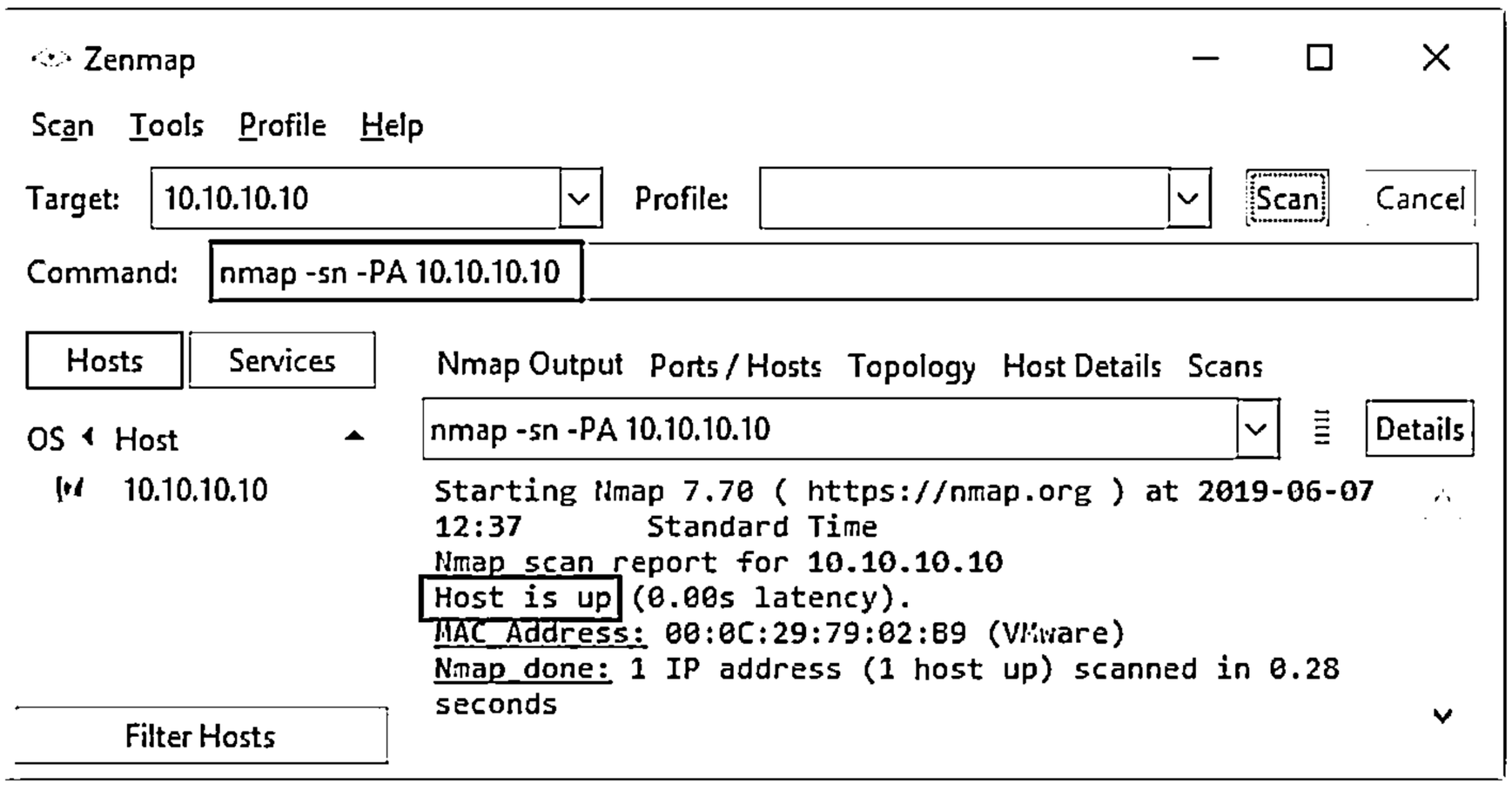


Figure 3.31: TCP ACK ping scan in Zenmap

IP Protocol Ping Scan

IP protocol ping is the latest host discovery option that sends IP ping packets with the IP header of any specified protocol number. It has the same format as the TCP and UDP ping. This technique tries to send different packets using different IP protocols, hoping to get a response indicating that a host is online.

Multiple IP packets for ICMP (protocol 1), IGMP (protocol 2), and IP-in-IP (protocol 4) are sent by default when no protocols are specified. For configuring the default protocols, change `DEFAULT_PROTO_PROBE_PORT_SPEC` in `nmap.h` during compile time. For specific protocols such as ICMP, IGMP, TCP (protocol 6), and UDP (protocol 17), the packets are to be sent with proper protocol headers, and for the remaining protocols, only the IP header data is to be sent with the packets.

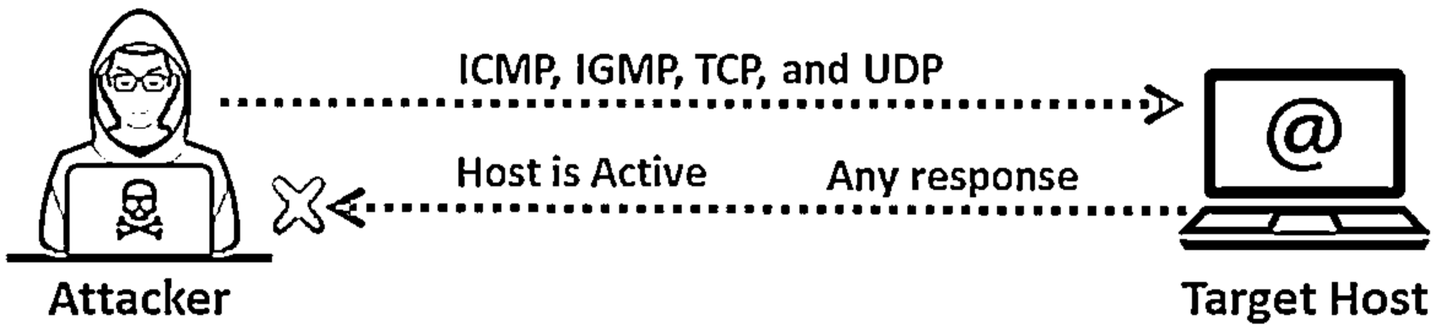


Figure 3.32: IP protocol ping scan for host discovery

In a nutshell, attackers send different probe packets of different IP protocols to the target host; any response from any probe indicates that a host is online. In Zenmap, the `-PO` option is used to perform an IP protocol ping scan.

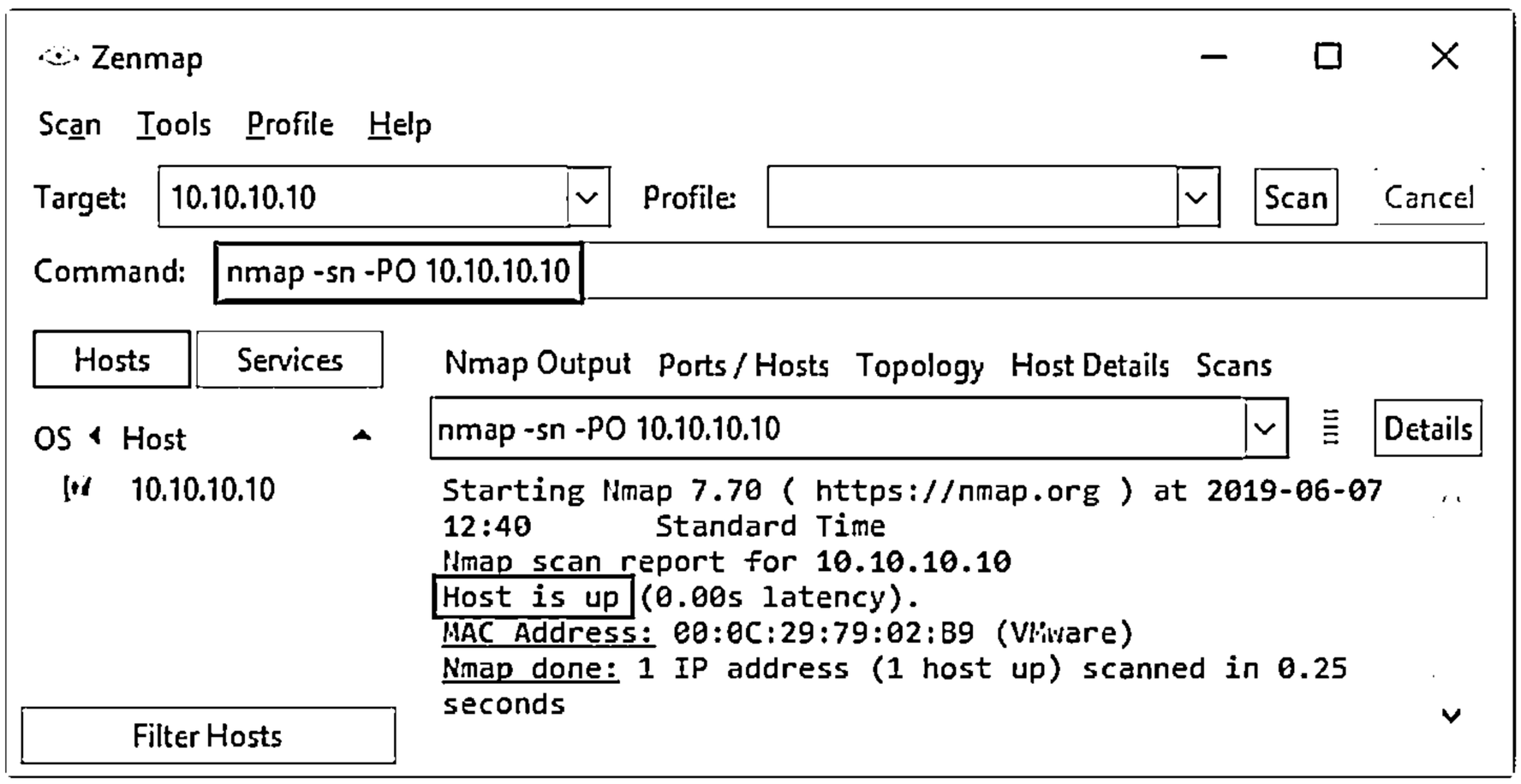
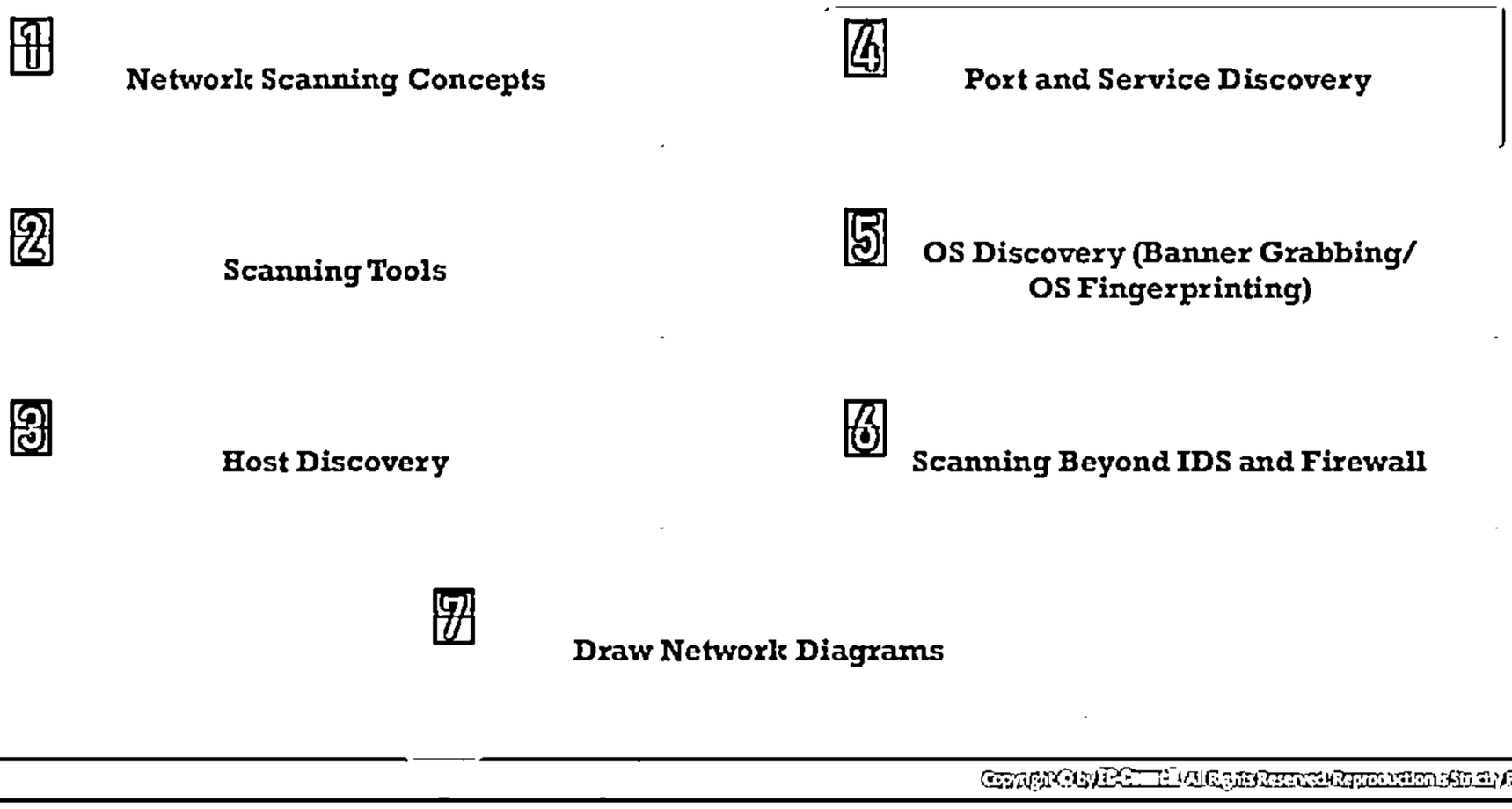


Figure 3.33: IP protocol ping scan in Zenmap

Module Flow



Port and Service Discovery

The next step in the network scanning process involves checking the open ports and services in live systems. After performing a ping scan, once attackers detect the live systems in the target network, they try to find open ports and services in the discovered live systems. This discovery of open ports and services can be performed via various port scanning techniques. Administrators often use port scanning techniques to verify the security policies of their networks, whereas attackers use them to identify open ports and running services on a host with the intent of compromising the network. Moreover, sometimes, users unknowingly keep unnecessary open ports on their systems. An attacker takes advantage of such open ports to launch attacks.

This section describes the common ports and corresponding services along with various port scanning techniques and tools used by the attacker to perform port scanning.

List of Common Ports and Services

The important reserved ports are listed below:

Name	Port/Protocol	Service Description
echo	7/tcp	
echo	7/udp	
discard	9/tcp	sink null
discard	9/udp	sink null
systat	11/tcp	Users
daytime	13/tcp	

daytime	13/udp	
netstat	15/tcp	
qotd	17/tcp	Quote
chargen	19/tcp	ttytst source
chargen	19/udp	ttytst source
ftp-data	20/tcp	ftp data transfer
ftp	21/tcp	ftp command
ssh	22/tcp	Secure Shell
telnet	23/tcp	
SMTP	25/tcp	Mail
time	37/tcp	Timeserver
time	37/udp	Timeserver
rlp	39/udp	resource location
nickname	43/tcp	who is
domain	53/tcp	domain name server
domain	53/udp	domain name server
sql*net	66/tcp	Oracle SQL*net
sql*net	66/udp	Oracle SQL*net
bootps	67/tcp	bootp server
bootps	67/udp	bootp server
bootpc	68/tcp	bootp client
bootpc	68/udp	bootp client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	gopher server
finger	79/tcp	Finger
www-http	80/tcp	WWW
www-http	80/udp	WWW
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
pop2	109/tcp	PostOffice V.2
Pop3	110/tcp	PostOffice V.3
sunrpc	111/tcp	RPC 4.0 portmapper
sunrpc	111/udp	RPC 4.0 portmapper
auth/ident	113/tcp	Authentication Service
auth	113/udp	Authentication Service

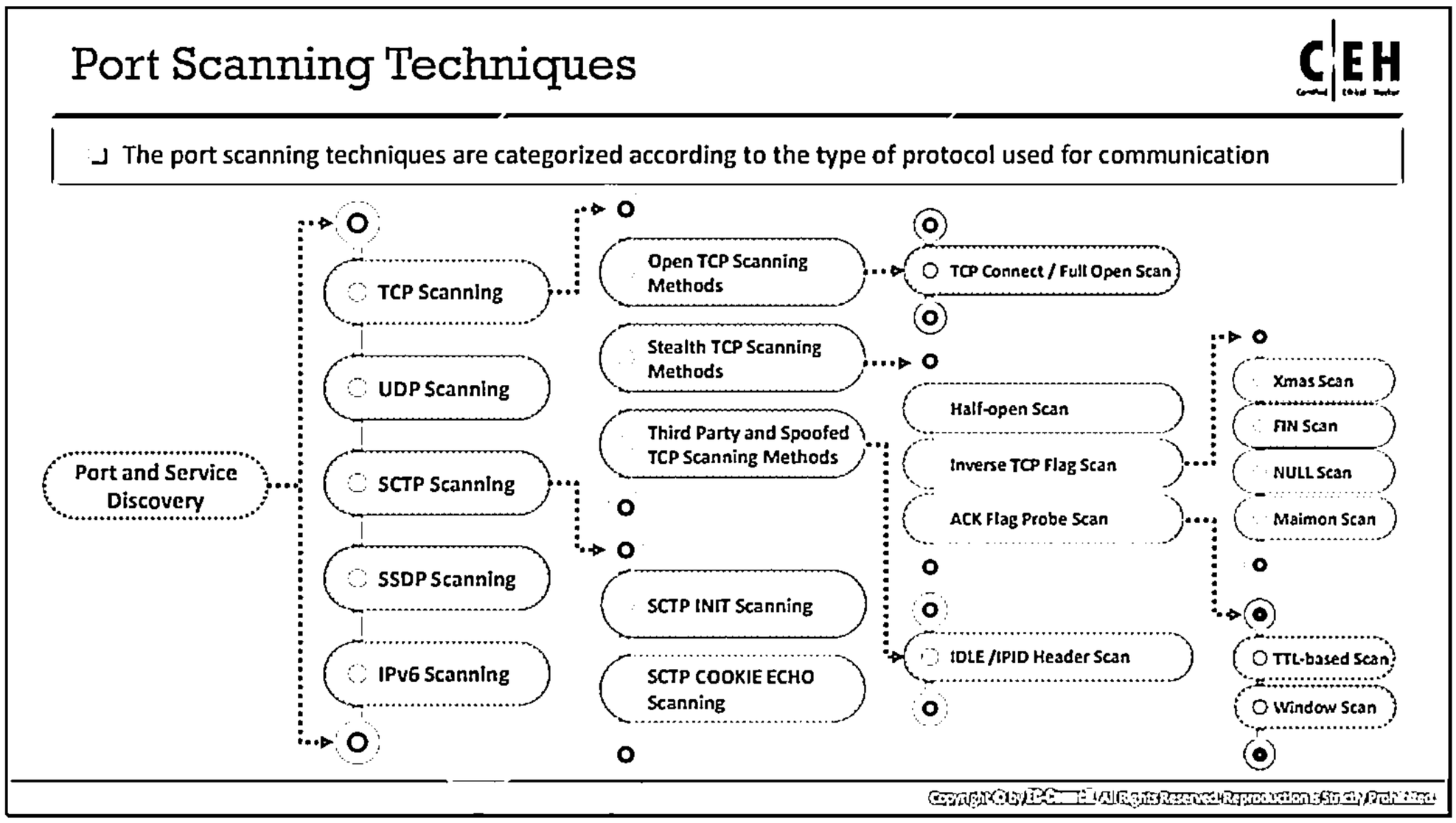
audionews	114/tcp	Audio News Multicast
audionews	114/udp	Audio News Multicast
nntp	119/tcp	Usenet Network News Transfer
nntp	119/udp	Usenet Network News Transfer
ntp	123/tcp	Network Time Protocol
Name	Port/Protocol	Description
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
imap	143/tcp	Internet Message Access Protocol
imap	143/udp	Internet Message Access Protocol
sql-net	150/tcp	SQL-NET
sql-net	150/udp	SQL-NET
sqlsrv	156/tcp	SQL Service
sqlsrv	156/udp	SQL Service
snmp	161/tcp	
snmp	161/udp	
snmp-trap	162/tcp	
snmp-trap	162/udp	
cmip-man	163/tcp	CMIP/TCP Manager
cmip-man	163/udp	CMIP
cmip-agent	164/tcp	CMIP/TCP Agent
cmip-agent	164/udp	CMIP
irc	194/tcp	Internet Relay Chat
irc	194/udp	Internet Relay Chat
at-rtmp	201/tcp	AppleTalk Routing Maintenance
at-rtmp	201/udp	AppleTalk Routing Maintenance
at-nbp	202/tcp	AppleTalk Name Binding
at-nbp	202/udp	AppleTalk Name Binding
at-3	203/tcp	AppleTalk
at-3	203/udp	AppleTalk
at-echo	204/tcp	AppleTalk Echo

at-echo	204/udp	AppleTalk Echo
at-5	205/tcp	AppleTalk
at-5	205/udp	AppleTalk
at-zis	206/tcp	AppleTalk Zone Information
at-zis	206/udp	AppleTalk Zone Information
at-7	207/tcp	AppleTalk
at-7	207/udp	AppleTalk
at-8	208/tcp	AppleTalk
at-8	208/udp	AppleTalk
ipx	213/tcp	Novel
ipx	213/udp	Novel
imap3	220/tcp	Interactive Mail Access Protocol v3
imap3	220/udp	Interactive Mail Access Protocol v3
aurp	387/tcp	AppleTalk Update-Based Routing
aurp	387/udp	AppleTalk Update-Based Routing
netware-ip	396/tcp	Novell Netware over IP
netware-ip	396/udp	Novell Netware over IP
Name	Port/Protocol	Description
rmt	411/tcp	Remote mt
rmt	411/udp	Remote mt
kerberos-ds	445/tcp	Microsoft DS
kerberos-ds	445/udp	Microsoft DS
isakmp	500/udp	ISAKMP/IKE
fcp	510/tcp	First Class Server
exec	512/tcp	BSD rexecd(8)
comsat/biff	512/udp	used by mail system to notify users
login	513/tcp	BSD rlogind(8)
who	513/udp	whod BSD rwhod(8)
shell	514/tcp	cmd BSD rshd(8)
syslog	514/udp	BSD syslogd(8)
printer	515/tcp	spooler BSD lpd(8)
printer	515/udp	Printer Spooler
talk	517/tcp	BSD talkd(8)
talk	517/udp	Talk
ntalk	518/udp	New Talk (ntalk)
ntalk	518/udp	SunOS talkd(8)

netnews	532/tcp	Readnews
uucp	540/tcp	uucpd BSD uucpd(8)
uucp	540/udp	uucpd BSD uucpd(8)
klogin	543/tcp	Kerberos Login
klogin	543/udp	Kerberos Login
kshell	544/tcp	Kerberos Shell
kshell	544/udp	Kerberos Shell
ekshell	545/tcp	krcmd Kerberos encrypted remote shell –kfall
pcserver	600/tcp	ECD Integrated PC board srvr
mount	635/udp	NFS Mount Service
pcnfs	640/udp	PC-NFS DOS Authentication
bwnfs	650/udp	BW-NFS DOS Authentication
flexlm	744/tcp	Flexible License Manager
flexlm	744/udp	Flexible License Manager
kerberos-adm	749/tcp	Kerberos Administration
kerberos-adm	749/udp	Kerberos Administration
kerberos	750/tcp	kdc Kerberos authentication—tcp
kerberos	750/udp	Kerberos
kerberos_master	751/udp	Kerberos authentication
kerberos_master	751/tcp	Kerberos authentication
krb_prop	754/tcp	Kerberos slave propagation
	999/udp	Applixware
socks	1080/tcp	
socks	1080/udp	
kpop	1109/tcp	Pop with Kerberos
ms-sql-s	1433/tcp	Microsoft SQL Server
ms-sql-s	1433/udp	Microsoft SQL Server
ms-sql-m	1434/tcp	Microsoft SQL Monitor
ms-sql-m	1434/udp	Microsoft SQL Monitor
pptp	1723/tcp	Pptp
pptp	1723/udp	Pptp
nfs	2049/tcp	Network File System
nfs	2049/udp	Network File System
eklogin	2105/tcp	Kerberos encrypted rlogin

rkinit	2108/tcp	Kerberos remote kinit
kx	2111/tcp	X over Kerberos
kauth	2120/tcp	Remote kauth
lyskom	4894/tcp	LysKOM (conference system)
sip	5060/tcp	Session Initiation Protocol
sip	5060/udp	Session Initiation Protocol
x11	6000-6063/tcp	X Window System
x11	6000-6063/udp	X Window System
irc	6667/tcp	Internet Relay Chat
afs	7000-7009/udp	Andrew File System
afs	7000-7009/udp	Andrew File System

Table 3.2: Reserved ports table



Port Scanning Techniques

Port scanning techniques are further categorized as described below. This categorization is based on the type of protocol used for communication in the network.

TCP Scanning:

- Open TCP Scanning Methods
  - TCP Connect/Full Open Scan
- Stealth TCP Scanning Methods
  - Half-open Scan
  - Inverse TCP Flag Scan
    - Xmas Scan
    - FIN Scan
    - NULL Scan
    - Maimon Scan
  - ACK Flag Probe Scan
    - TTL-Based Scan
    - Window Scan
- Third Party and Spoofed TCP Scanning Methods
  - IDLE/IP ID Header Scan

UDP Scanning:

- UDP Scanning

SCTP Scanning:

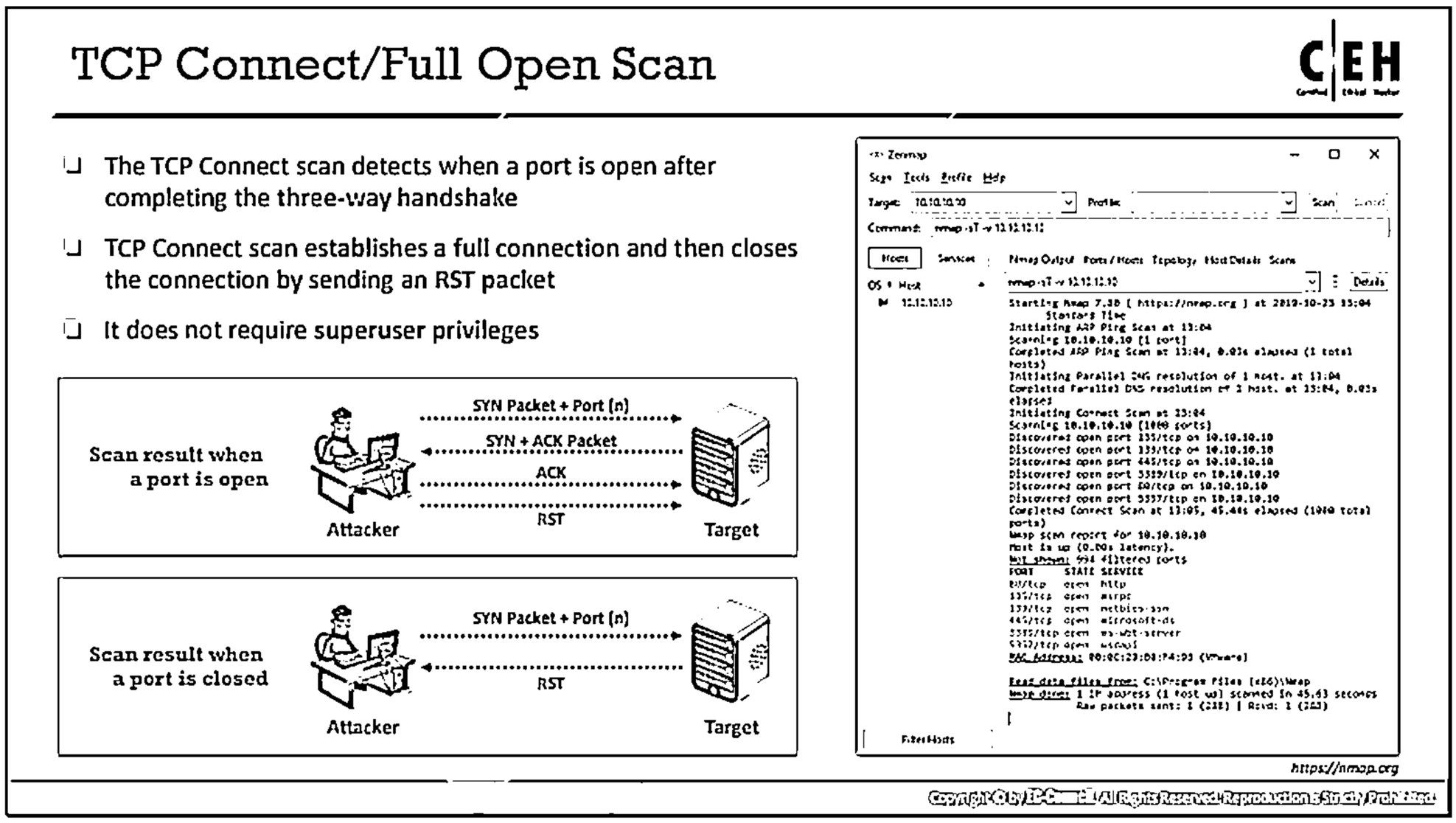
- SCTP INIT Scanning
- SCTP COOKIE/ECHO Scanning

SSDP Scanning:

- SSDP and List Scanning

IPv6 Scanning:

- IPv6 Scanning



TCP Connect/Full Open Scan

Source: *http://insecure.org*

TCP Connect/Full Open Scan is one of the most reliable forms of TCP scanning. In TCP Connect scanning, the OS's TCP `connect()` system call tries to open a connection to every port of interest on the target machine. If the port is listening, the `connect()` call will result in a successful connection with the host on that particular port; otherwise, it will return an error message stating that the port is not reachable.

TCP Connect scan completes a three-way handshake with the target machine. In the TCP three-way handshake, the client sends a SYN packet, which the recipient acknowledges with a SYN+ACK packet. Then, the client acknowledges the SYN+ACK packet with an ACK packet to complete the connection. Once the handshake is completed, the scanner sends an RST packet to end the connection.

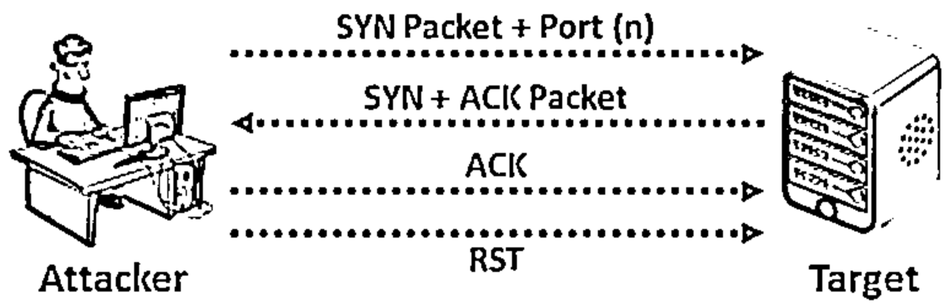


Figure 3.34: Scan result when a port is open

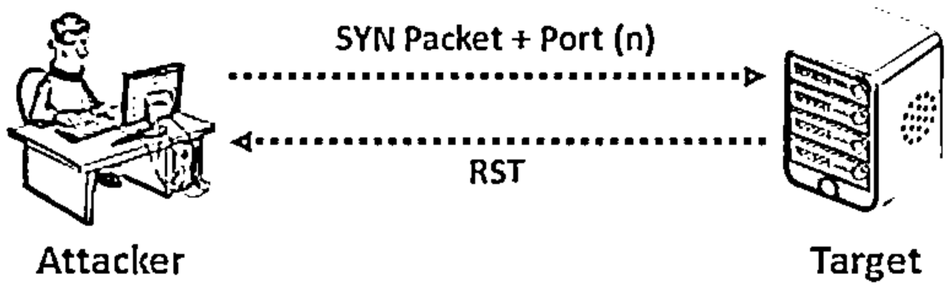


Figure 3.35: Scan result when a port is closed

Making a separate `connect()` call for every targeted port in a linear manner would take a long time over a slow connection. The attacker can accelerate the scan using many sockets in parallel. Using non-blocking, I/O allows the attacker to set a short time-out period and watch all the sockets simultaneously. In Zenmap, the `-sT` option is used to perform TCP Connect/full open scan.

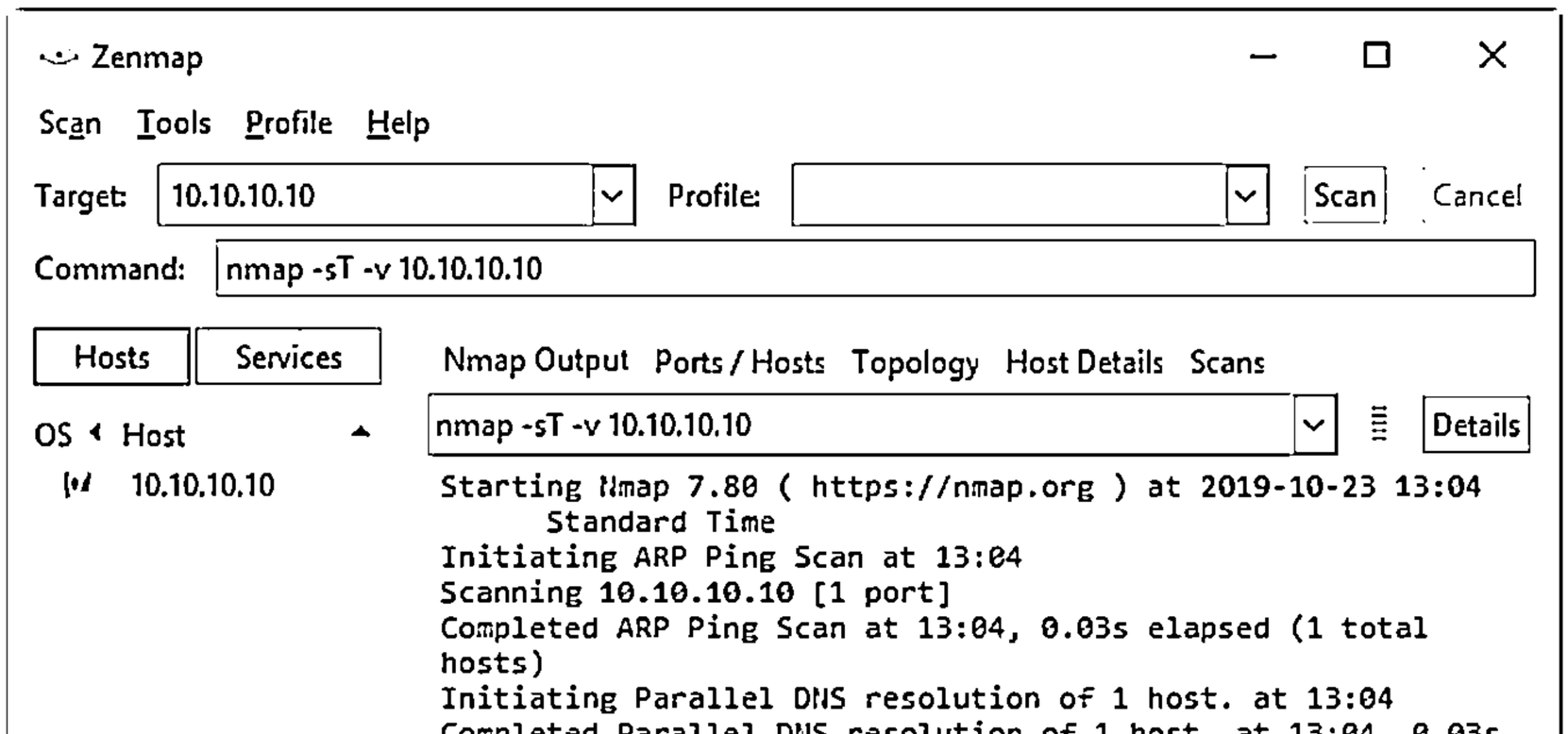
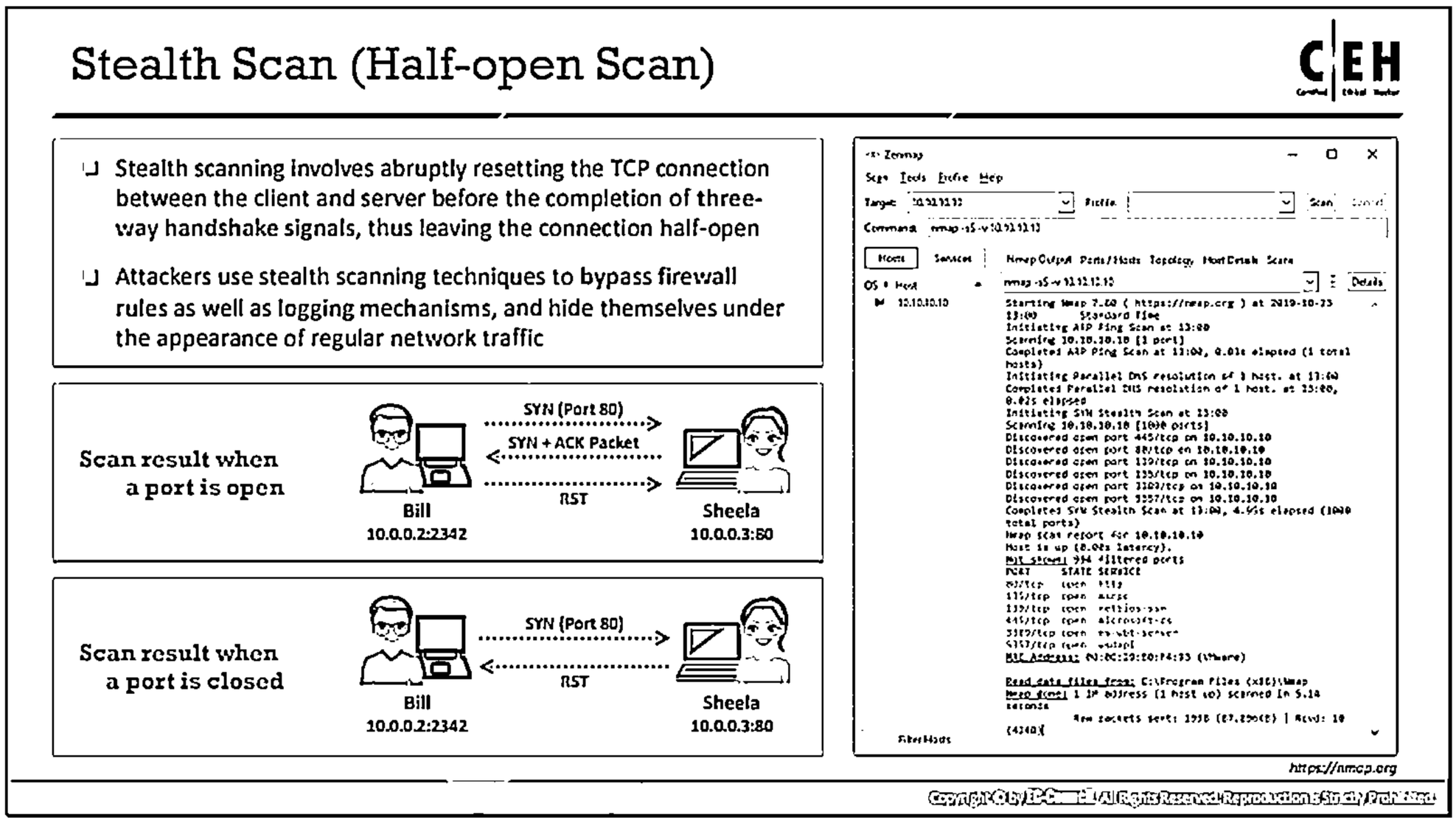


Figure 3.36: TCP Connect/Full Open scan using Zenmap

The drawback of this type of scan is that it is easily detectable and filterable. The logs in the target system will disclose the connection. Such scanning does not require superuser privileges.



Stealth Scan (Half-open Scan)

The stealth scan involves resetting the TCP connection between the client and the server abruptly before completion of the three-way handshake signals, hence making the connection half-open. A stealth scan sends a single frame to a TCP port without any TCP handshaking or additional packet transfers. This type of scan sends a single frame with the expectation of a single response. The half-open scan partially opens a connection but stops halfway through. The stealth scan is also called a "SYN scan," because it only sends the SYN packet. This prevents the service from notifying the incoming connection. TCP SYN or half-open scanning is a stealth method of port scanning.

The stealth scan also implements the three-way handshake methodology. In the last stage, it examines the packets entering the interface and terminates the connection before triggering a new initialization to identify remote ports. The stealth scan process is described below.

- The client sends a single SYN packet to the server on the appropriate port.
- If the port is open, the server subsequently responds with a SYN/ACK packet.
- If the server responds with an RST packet, then the remote port is in the "closed" state.
- The client sends the RST packet to close the initiation before a connection can be established.

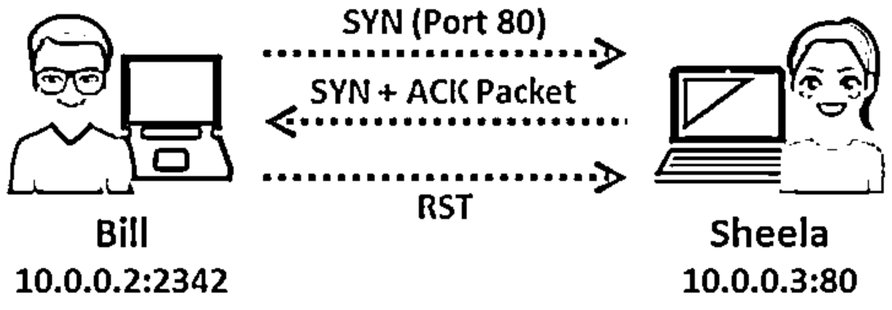


Figure 3.37: Port is open

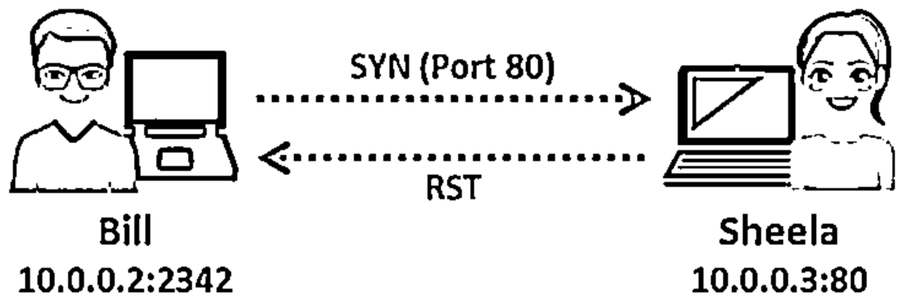


Figure 3.38: Port is closed

Attackers use stealth scanning techniques to bypass firewall rules and logging mechanisms, and they hide themselves as usual under network traffic. In Zenmap, the `-sS` option is used to perform a stealth scan/TCP half-open scan.

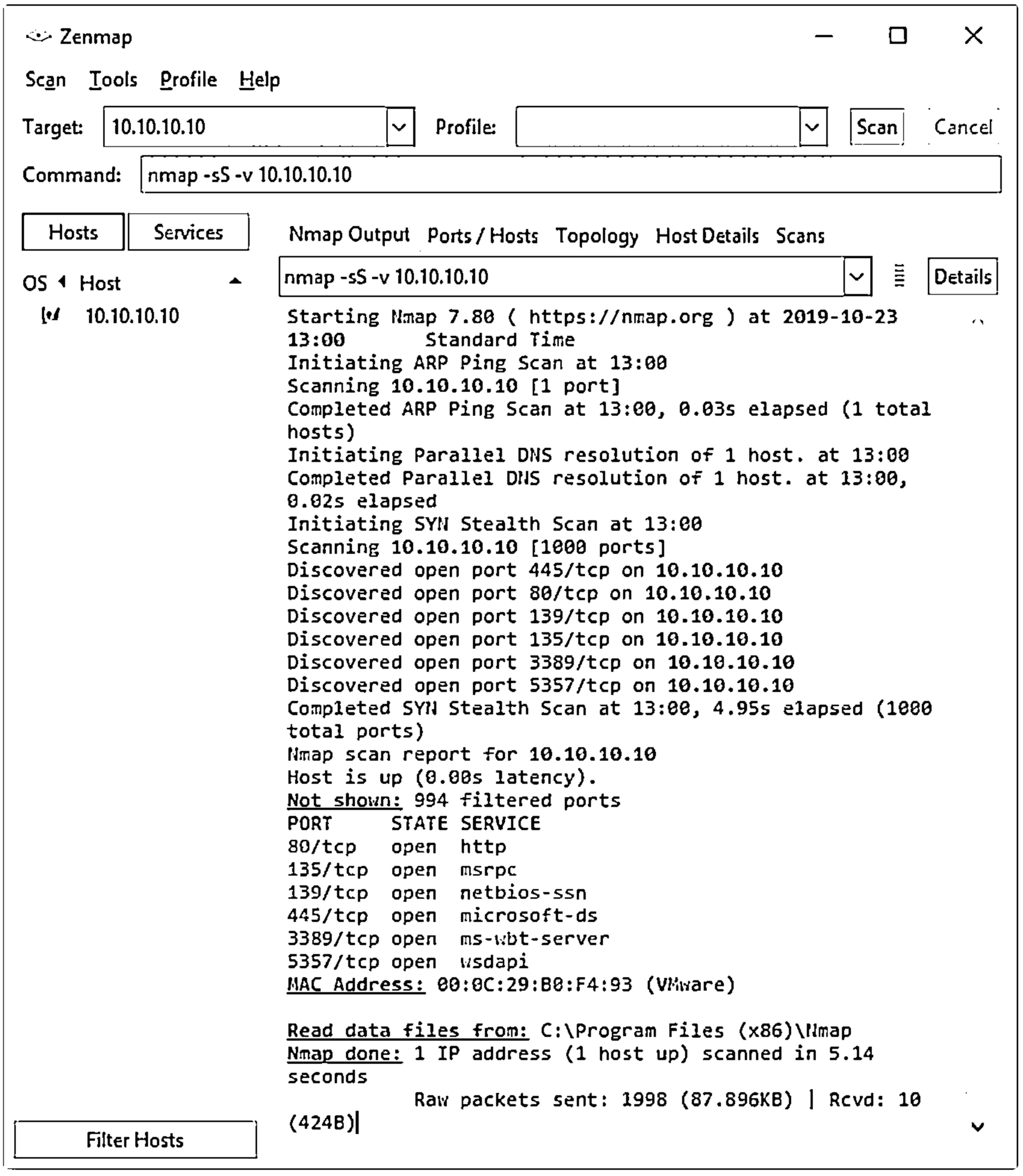
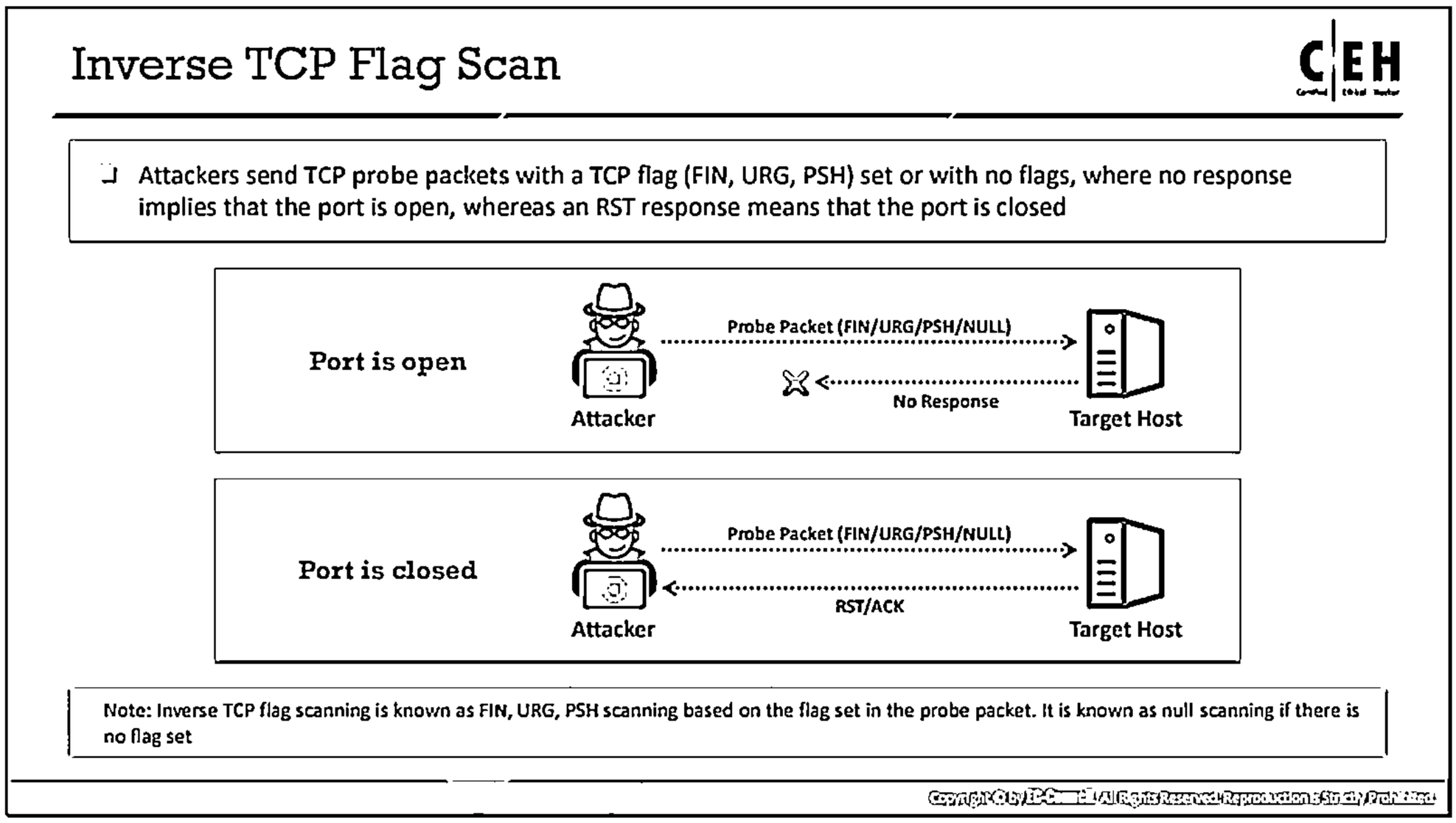


Figure 3.39: TCP Stealth/Half Open scan using Zenmap



Inverse TCP Flag Scan

Attackers send TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags. When the port is open, the attacker does not get any response from the host, whereas when the port is closed, he or she receives the RST from the target host.

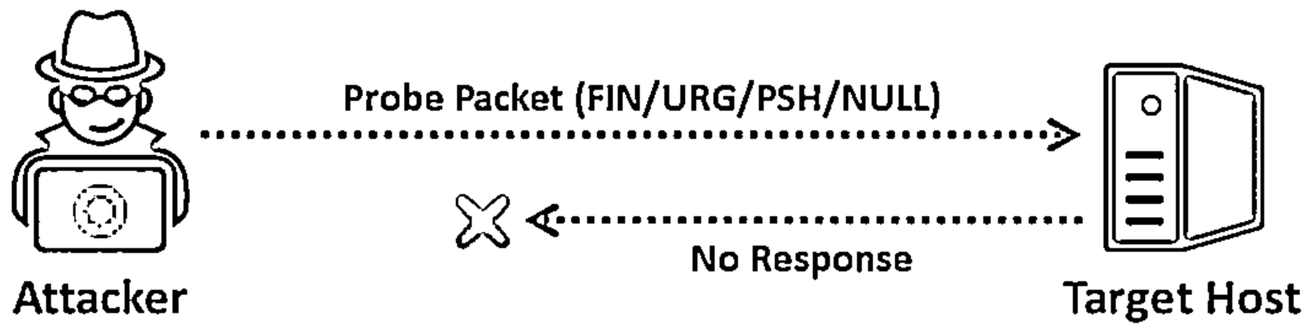


Figure 3.40: Inverse TCP flag scan when port is open

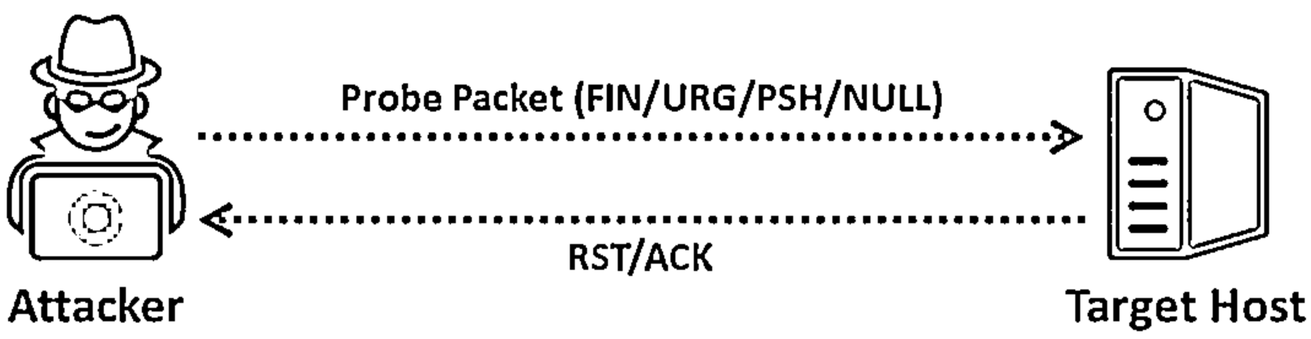


Figure 3.41: Inverse TCP flag scan when port is closed

Security mechanisms such as firewalls and IDS detect the SYN packets sent to the sensitive ports of the targeted hosts. Programs such as Synlogger and Courtney are available to log half-open SYN flag scan attempts. At times, the probe packets enabled with TCP flags can pass through filters undetected, depending on the security mechanisms installed.

An inverted technique involves probing a target using a half-open SYN flag because the closed ports can only send the response back. According to RFC 793, an RST/ACK packet is sent for

connection reset when the host closes a port. Attackers take advantage of this feature to send TCP probe packets to each port of the target host with various TCP flags set.

Common flag configurations used for a probe packet include:

- A FIN probe with the FIN TCP flag set
- An Xmas probe with the FIN, URG, and PUSH TCP flags set
- A NULL probe with no TCP flags set
- A SYN/ACK probe

All closed ports on the targeted host will send an RST/ACK response. Since OSs such as Windows completely ignore the RFC 793 standard, you cannot see the RST/ACK response when connected to a closed port on the target host. However, this technique is effective when used with UNIX-based OSs.

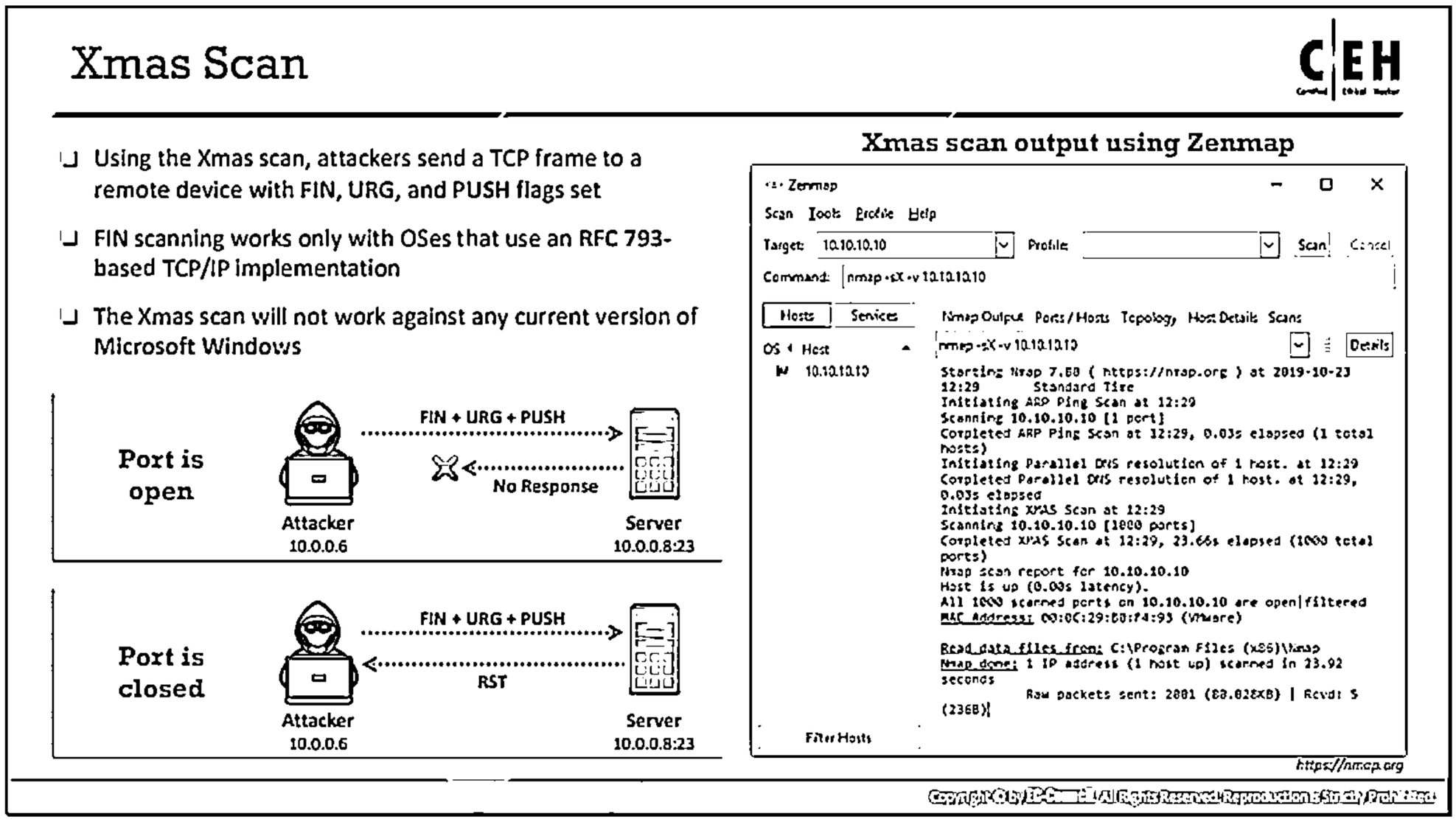
Advantages

- Avoids many IDS and logging systems; highly stealthy

Disadvantages

- Needs raw access to network sockets, thus requiring super-user privileges
- Mostly effective against hosts using a BSD-derived TCP/IP stack (not effective against Microsoft Windows hosts, in particular).

Note: Inverse TCP flag scanning is known as FIN, URG, and PSH scanning based on the flag set in the probe packet. If there is no flag set, it is known as NULL scanning. If only the FIN flag is set, it is known as FIN scanning, and if all of FIN, URG, and PSH are set, it is known as Xmas scanning.



Xmas Scan

Xmas scan is a type of inverse TCP scanning technique with the FIN, URG, and PUSH flags set to send a TCP frame to a remote device. If the target has opened the port, then you will receive no response from the remote system. If the target has closed the port, then you will receive a remote system reply with an RST. You can use this port scanning technique to scan large networks and find which host is up and what services it is offering. This technique describes all TCP flag sets. When all flags are set, some systems hang; hence, the flags are often set in the nonsense pattern URG-PSH-FIN. Attackers use the TCP Xmas scan to determine if ports are closed on the target machine via the RST packet. This scan only works when systems are compliant with RFC 793-based TCP/IP implementation. It will not work against any current version of Microsoft Windows.

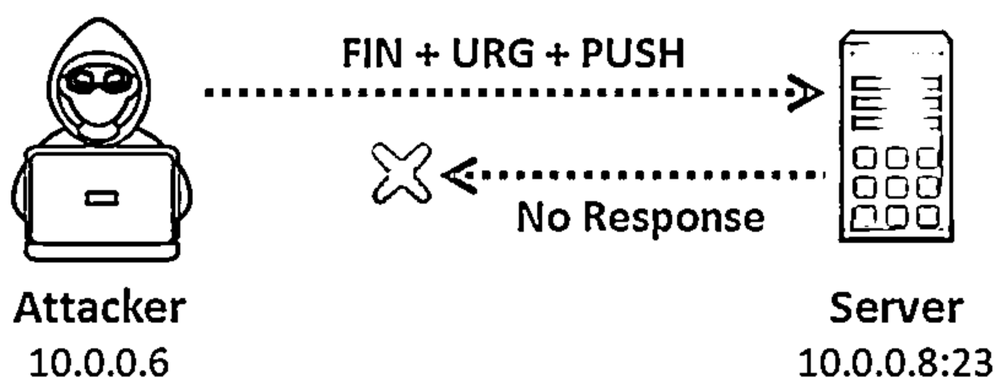


Figure 3.42: Xmas scan when the port is open

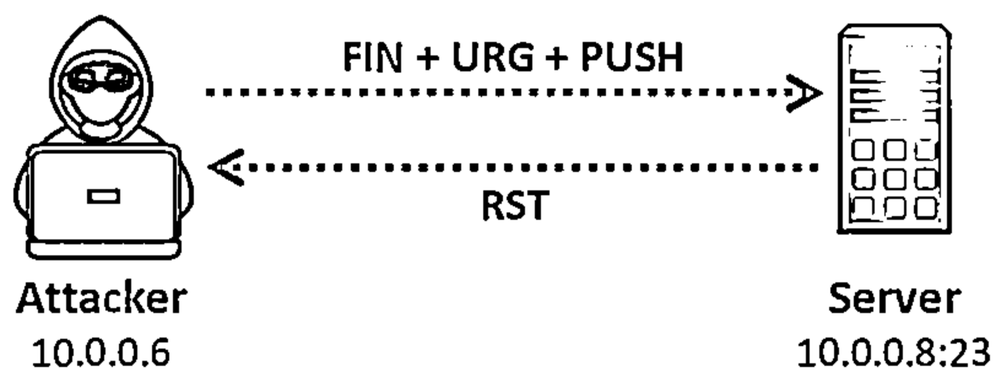


Figure 3.43: Xmas scan when the port is closed

BSD Networking Code

This method relies on the BSD networking code. Thus, you can use this only for UNIX hosts; it does not support Windows NT. If the user scans any Microsoft system, it will show that all the ports on the host are open.

Transmitting Packets

You can initialize all the flags when transmitting the packet to a remote host. If the target system accepts the packet and does not send any response, it means that the port is open. If the target system sends an RST flag, then it implies that the port is closed.

Advantages

- It avoids IDS and TCP three-way handshake.

Disadvantages

- It works on the UNIX platform only.

In Zenmap, the **-sX** option is used to perform Xmas scan whereas the **-sF** and **-sN** options are used to perform FIN scan and NULL scan, respectively.

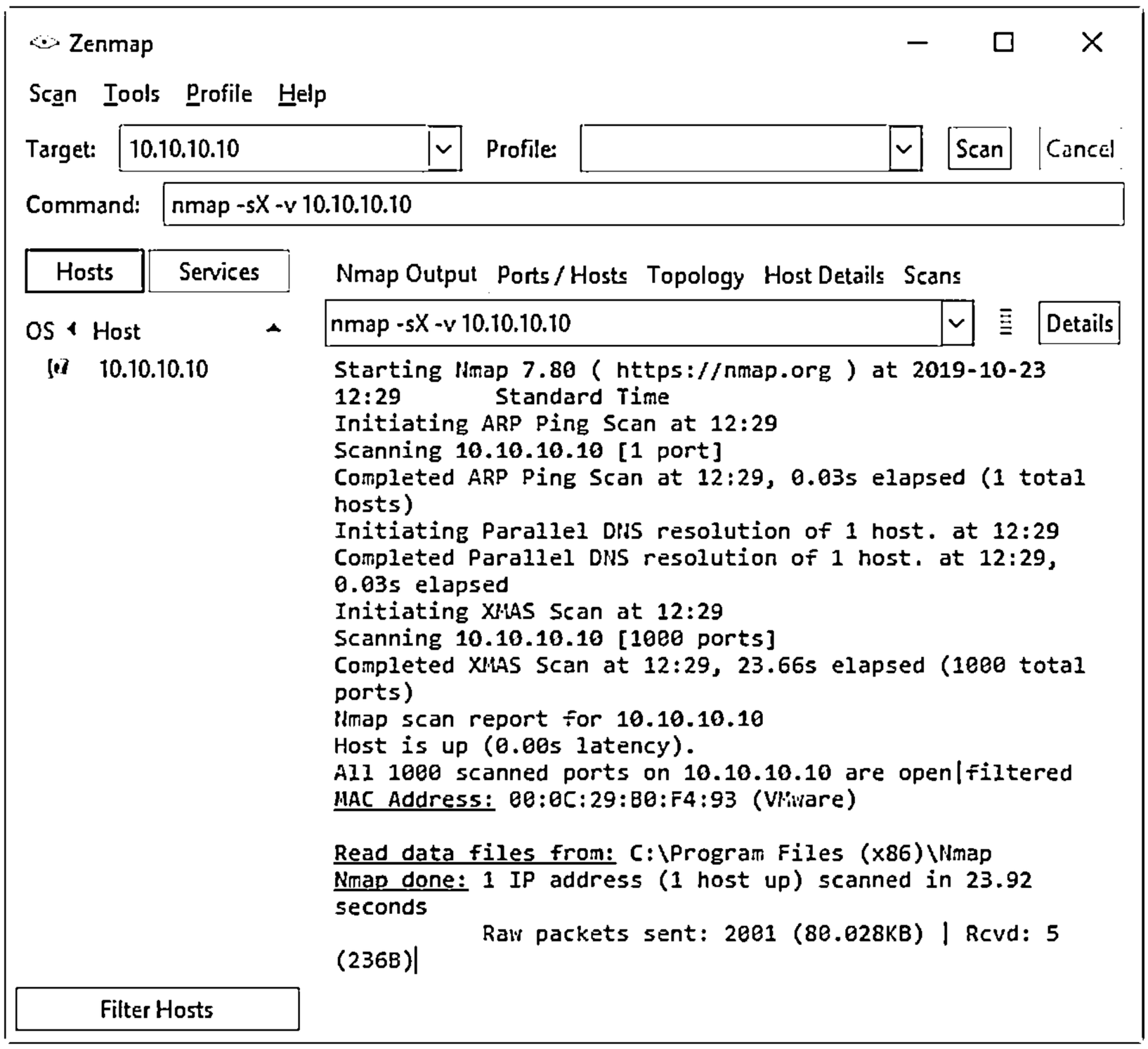
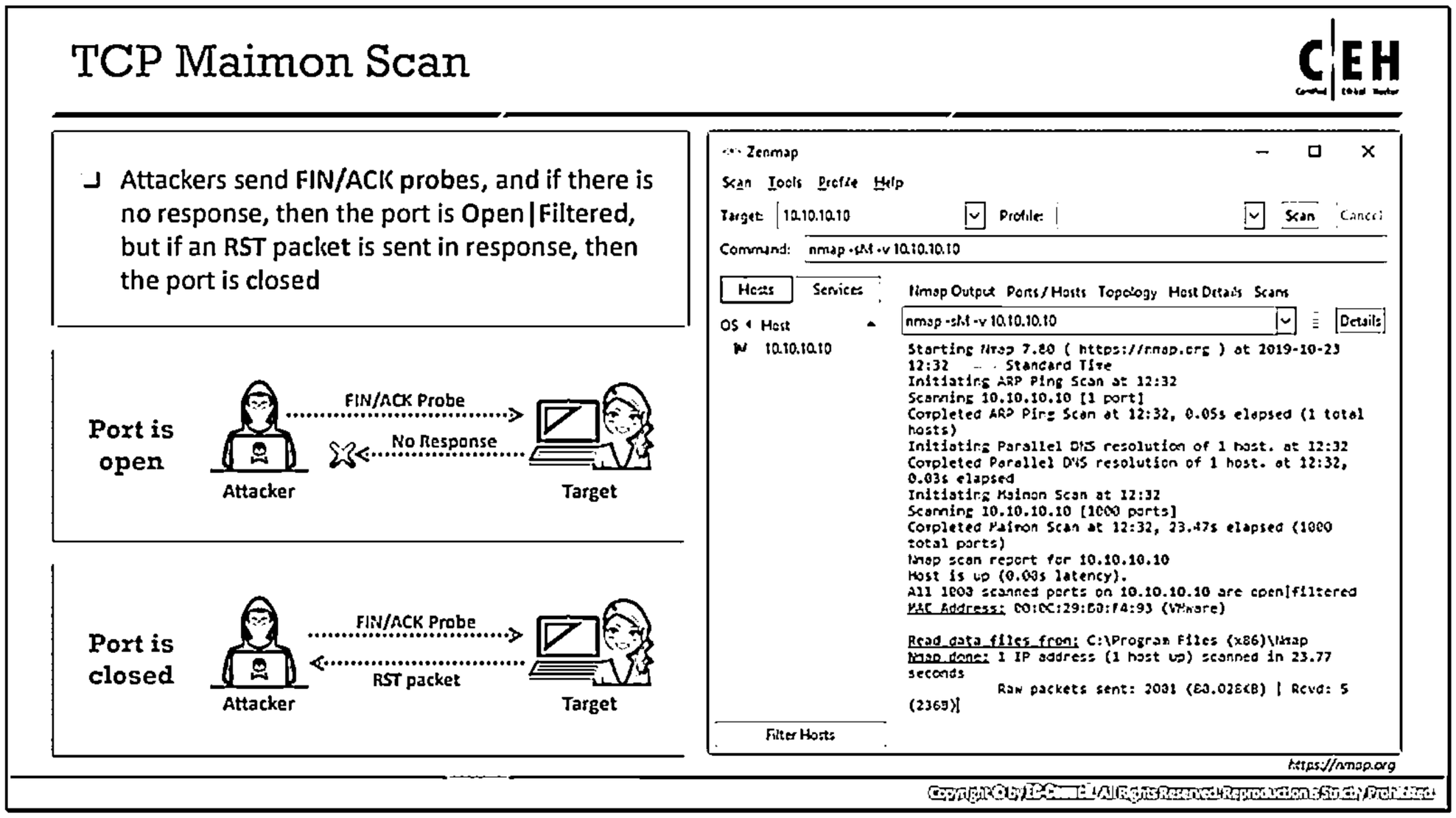


Figure 3.44: Xmas scan output using Zenmap



TCP Maimon scan

This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe.

Nmap interprets a port as open|filtered when there is no response from the Maimon scan probe even after many retransmissions. The port is closed if the probe gets a response as an RST packet. The port is filtered when the ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) is returned from the target host. In Zenmap, the `-sM` option is used to perform the TCP Maimon scan.

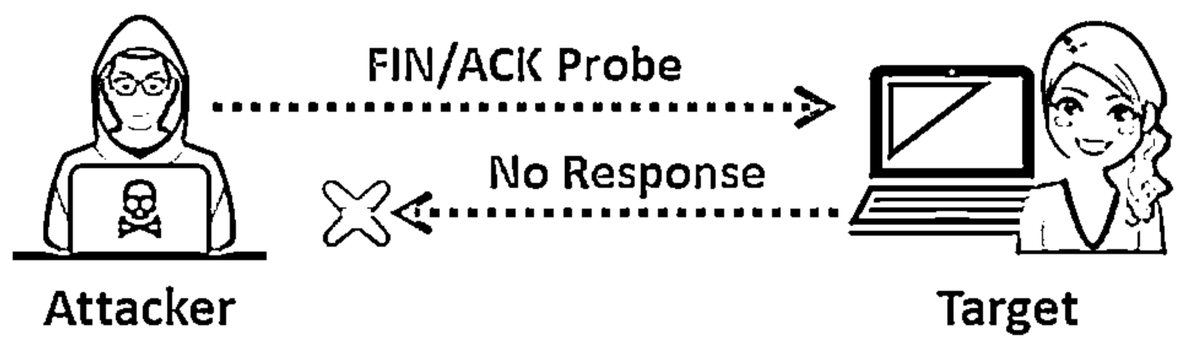


Figure 3.45: TCP Maimon scan result of open port

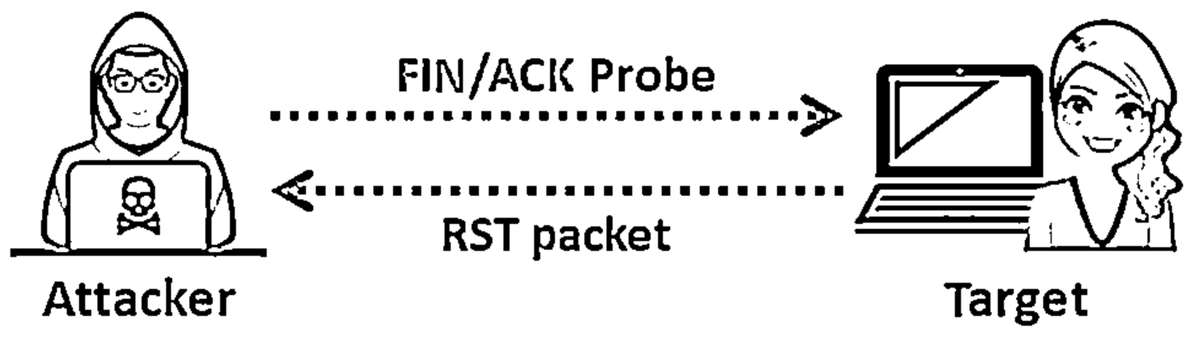


Figure 3.46: TCP Maimon scan result of closed port

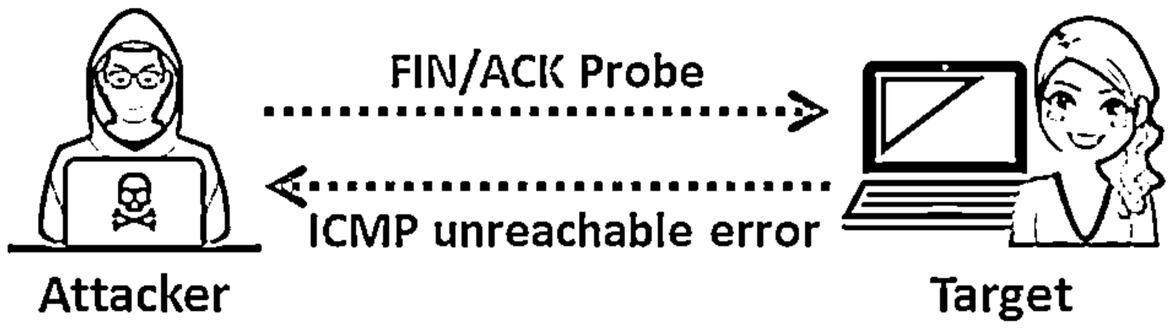


Figure 3.47: TCP Maimon scan result of filtered port

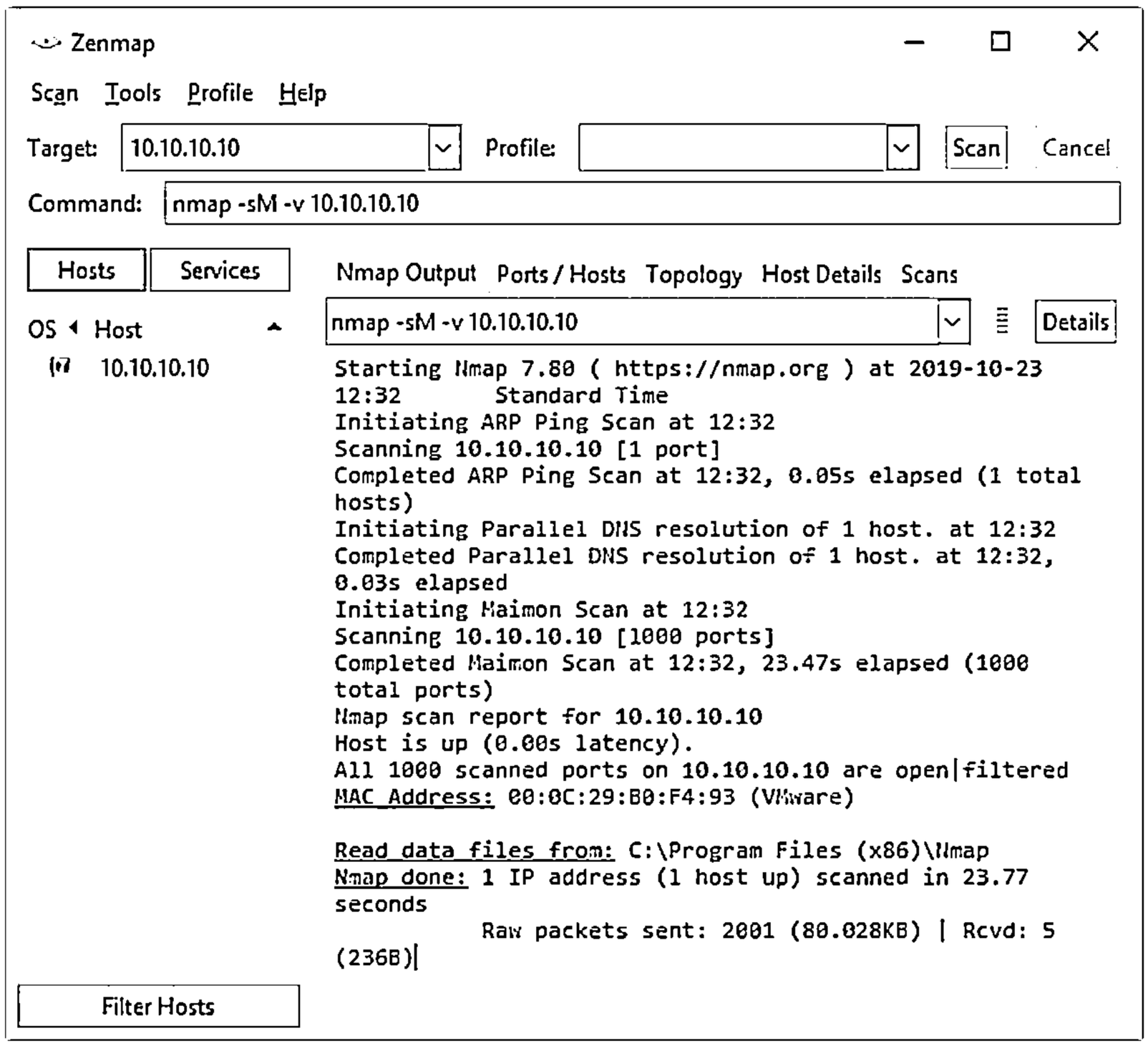
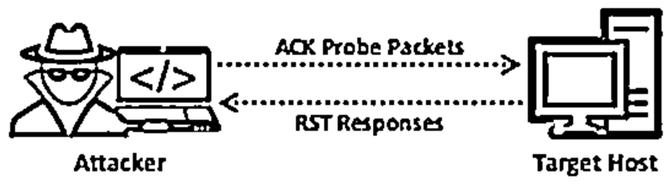


Figure 3.48: TCP Maimon scan displaying port state in Zenmap

ACK Flag Probe Scan

- Attackers send TCP probe packets set with an ACK flag to a remote device, and then analyze the header information (TTL and WINDOW field) of received RST packets to determine if the port is open or closed

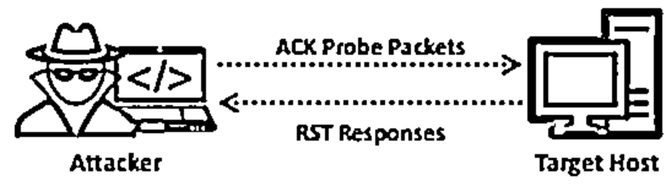
TTL-based ACK Flag Probe scanning




```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

If the TTL value of the RST packet on a particular port is less than the boundary value of 64, then that port is open

Window-based ACK Flag Probe scanning



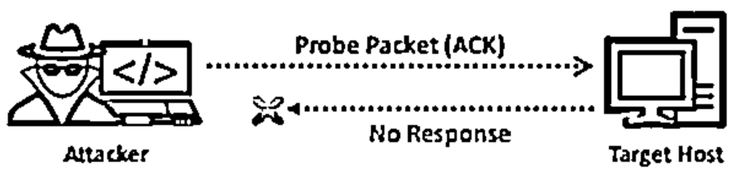

```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

If the window value of the RST packet on a particular port has a non-zero value, then that port is open

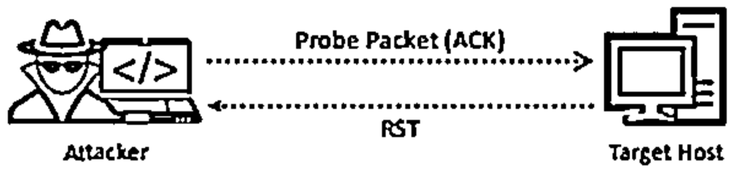
ACK Flag Probe Scan (Cont'd)

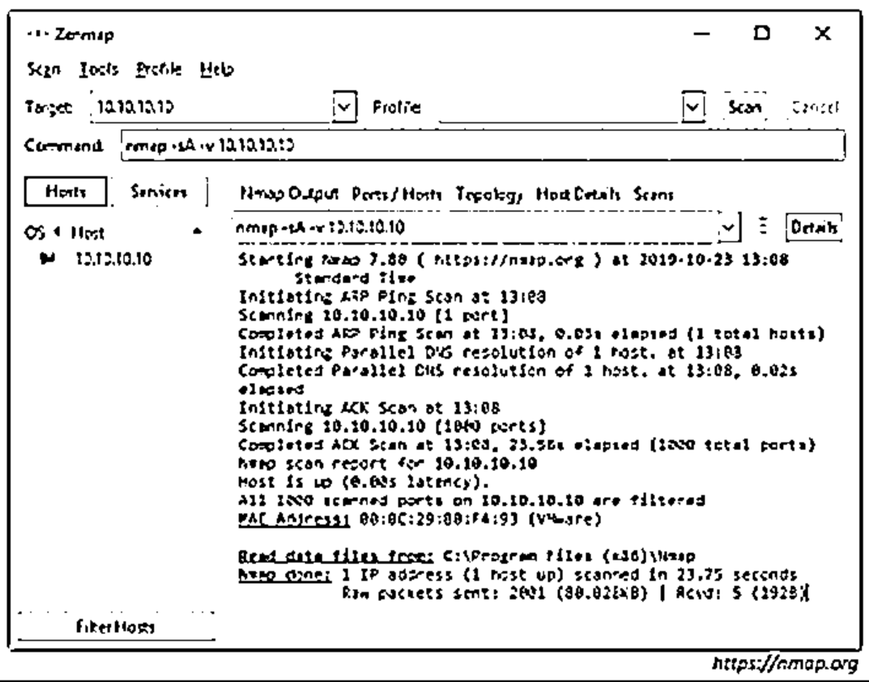
- ACK flag probe scanning can also be used to check the filtering system of a target
- Attackers send an ACK probe packet with a random sequence number, and no response implies that the port is filtered (stateful firewall is present), whereas an RST response means that the port is not filtered

Stateful Firewall is Present



No Firewall





ACK Flag Probe Scan

Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of the received RST packets to find out if the port is open or closed. The ACK flag probe scan exploits the vulnerabilities within the BSD-derived TCP/IP stack. Thus, such scanning is effective only on those OSs and platforms on which the BSD derives TCP/IP stacks.

Categories of ACK flag probe scanning include:

- **TTL-based ACK Flag Probe scanning**

  In this scanning technique, you will first need to send ACK probe packets (several thousands) to different TCP ports and then analyze the TTL field value of the RST packets received. In Zenmap, the syntax `nmap –ttl [time] [target]` is used to perform TTL-based scan.

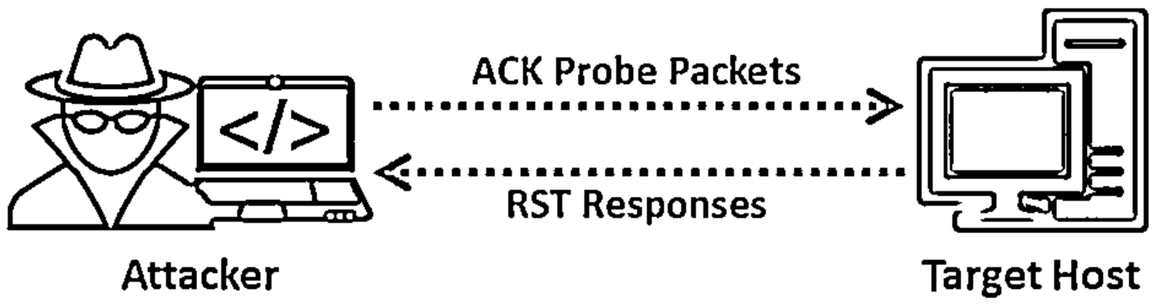


Figure 3.49: TTL-based ACK flag probe scanning

If the TTL value of the RST packet on a particular port is less than the boundary value of 64, then that port is open. An example showing a log of the first four RST packets received is presented below:

```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

Figure 3.50: Screenshot showing the open port based on the TTL value of the RST packet

In this example, port 22 returned a TTL value of 50, which is less than 64; all other ports returned a TTL value of 80, which is greater than 64. Therefore, port 22 is open.

- **Window-based ACK Flag Probe scanning**

  In this scanning technique, you will first need to send ACK probe packets (several thousands) to different TCP ports and then analyze the window field value of the received RST packets. The user can use this scanning technique when all the ports return the same TTL value. In Zenmap, the `-sW` option is used to perform a window scan.

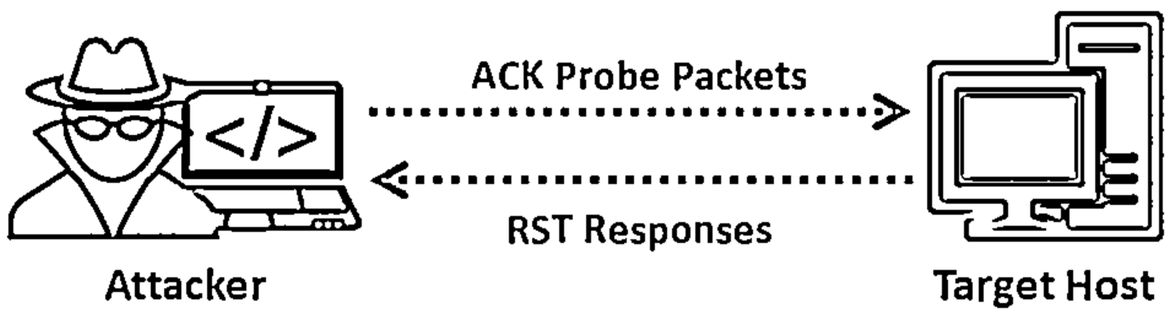


Figure 3.51: Window-based ACK flag probe scanning

If the window value of the RST packet on a particular port is non-zero, then that port is open. An example showing a log of the first four RST packets received is presented below:

```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

Figure 3.52: Screenshot showing the open port based on the window value of the RST packet

The above figure shows that the TTL value returned for each packet is the same; hence, you cannot perform TTL-based ACK flag probe scanning to find the open ports. Therefore, when you observe the window value, the third packet has a non-zero window value, which means that the port is open. When the returned RST value is zero, then the port is closed. If there is no response even after many retransmissions and an ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) is returned, then the port is inferred to be a filtered port.

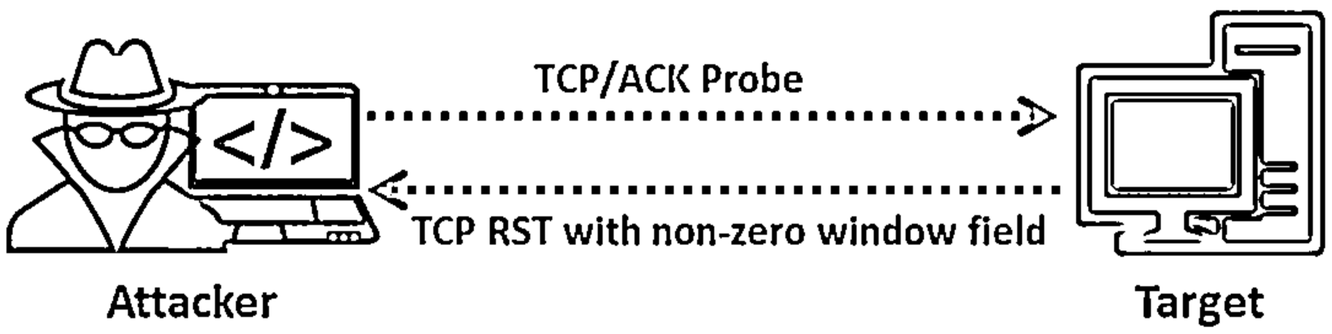


Figure 3.53: TCP Window scan result of an open port

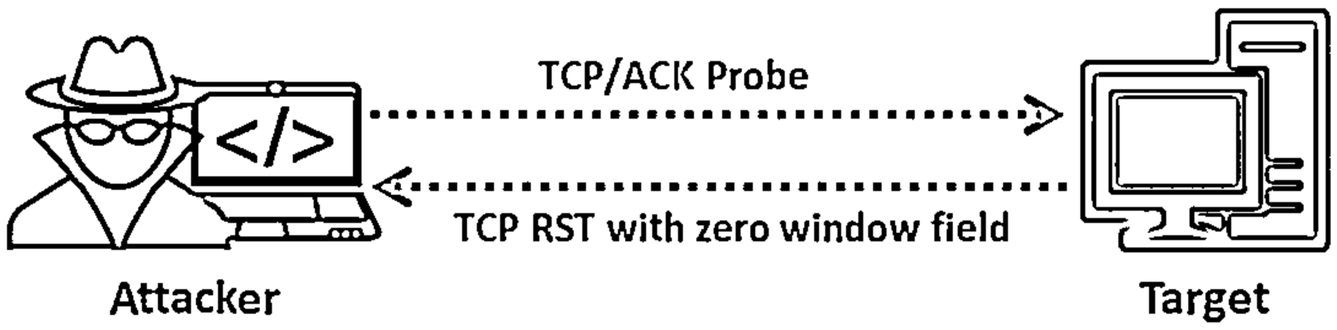


Figure 3.54: TCP Window scan result of a closed port

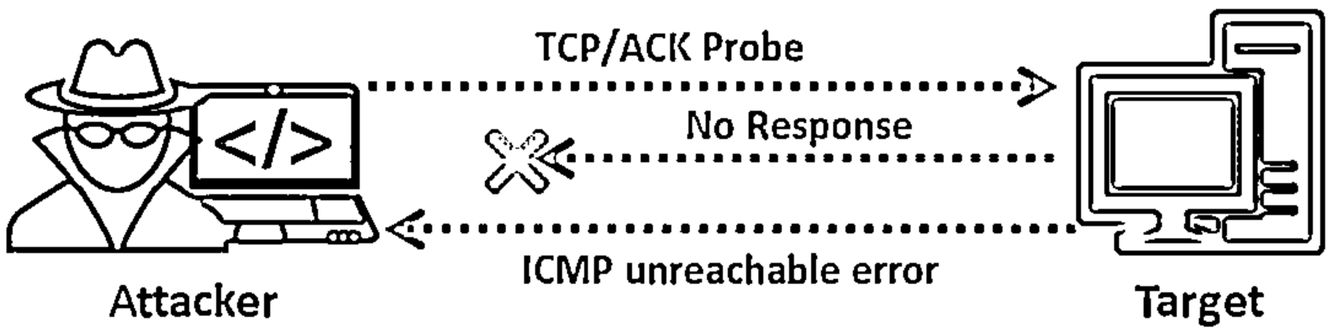


Figure 3.55: TCP Window scan result of a filtered port

Advantages:

- This type of scan can evade IDS in most cases.

Disadvantages:

- It is extremely slow and can exploit only older OSs with vulnerable BSD-derived TCP/IP stacks.

Checking the Filtering Systems of Target Networks

The ACK flag probe scanning technique also helps in checking the filtering systems of target networks. The attacker sends an ACK probe packet to check the filtering mechanism (firewalls) of packets employed by the target network.

Sending an ACK probe packet with a random sequence number and getting no response from the target means that the port is filtered (stateful firewall is present); an RST response from the target means that the port is not filtered (no firewall is present).

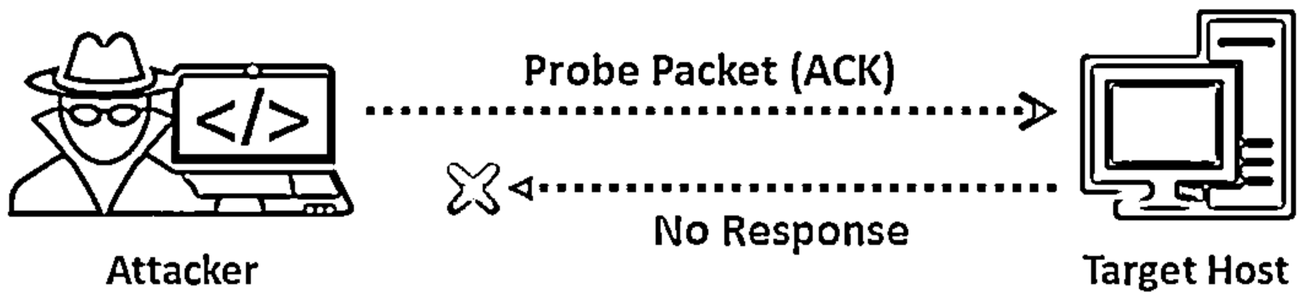


Figure 3.56: Stateful Firewall is present

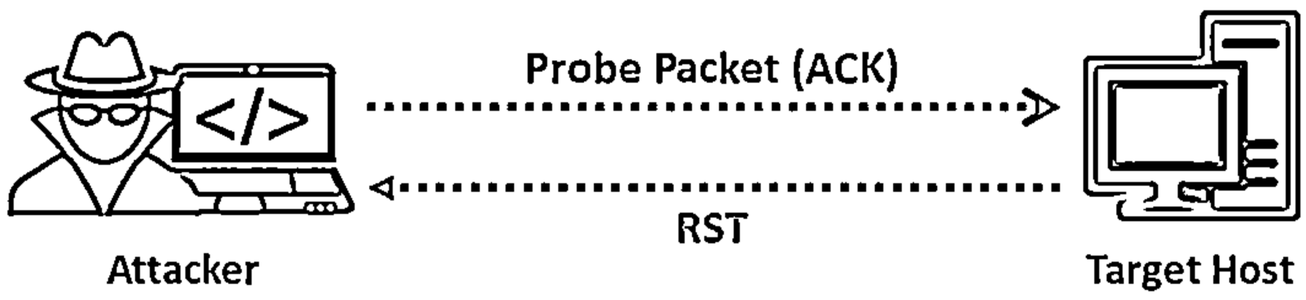


Figure 3.57: No Firewall

ACK Flag Probe Scanning using Nmap

In Zenmap, the **-sA** option is used to perform an ACK flag probe scan.

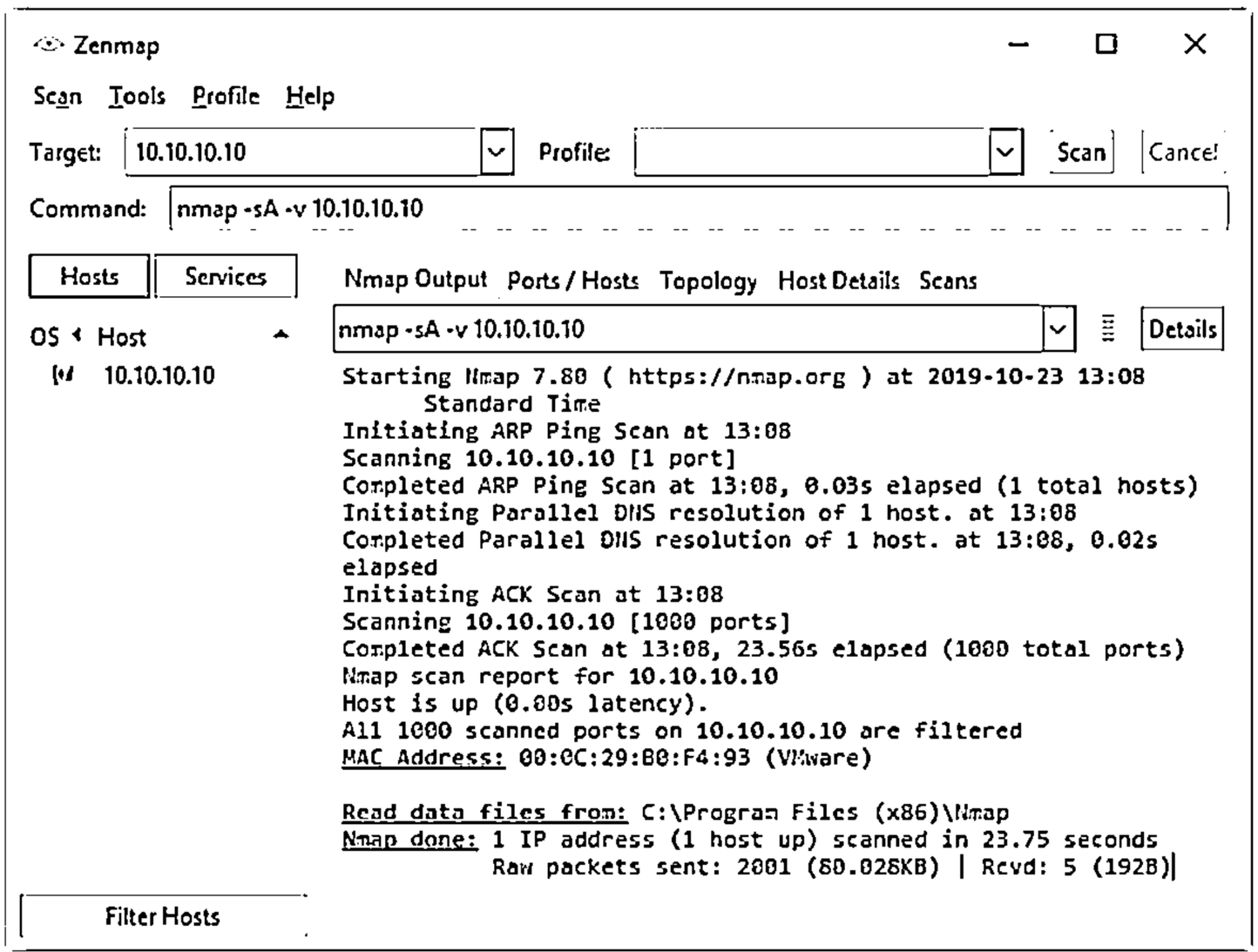
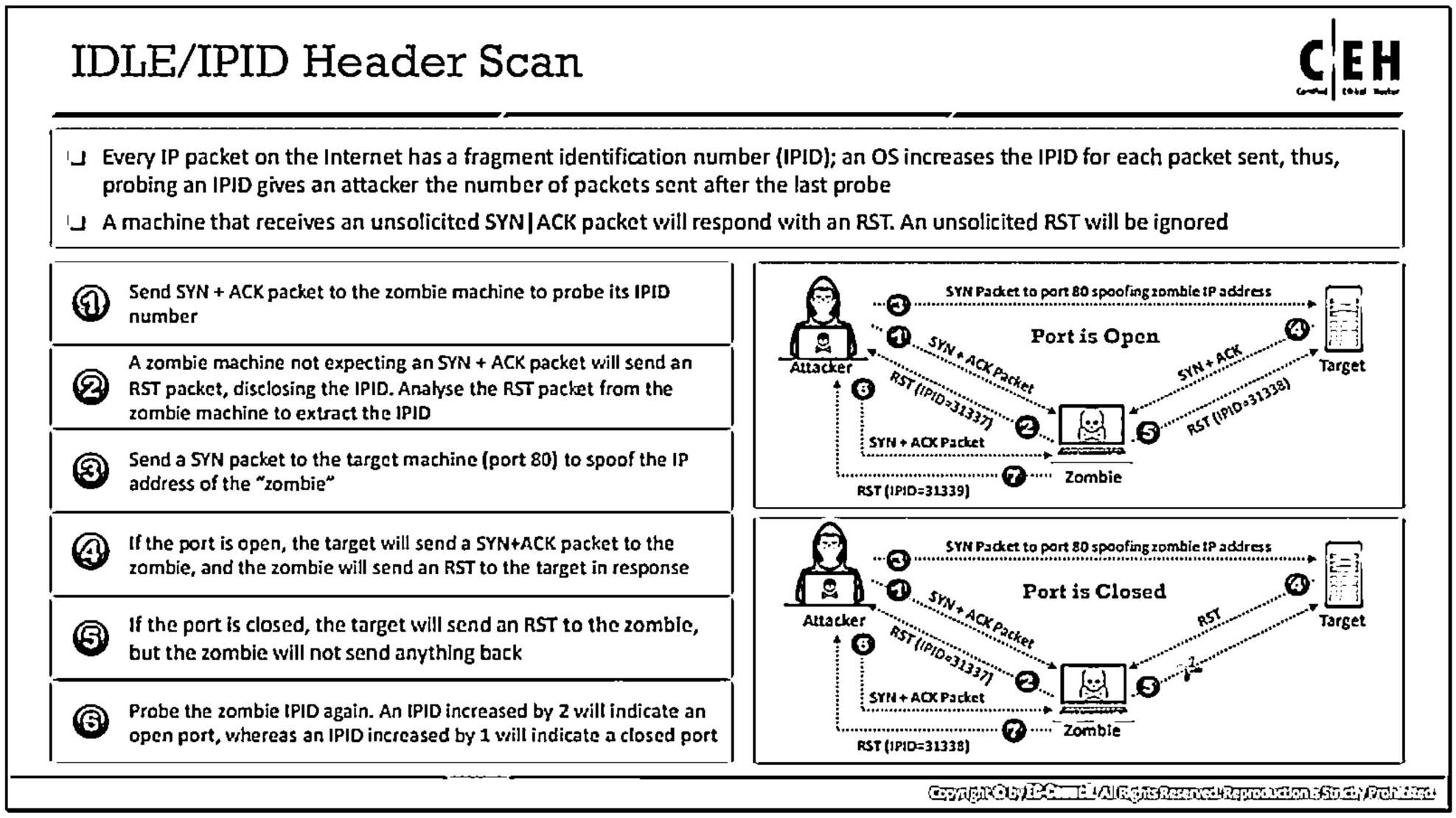


Figure 3.58: ACK Flag Probe scanning using Zenmap



IDLE/IPID Header Scan

The IDLE/IPID Header scan is a TCP port scan method that you can use to send a spoofed source address to a computer to find out what services are available. It offers complete blind scanning of a remote host. Most network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25. A port is considered "open" if an application is listening on the port. One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port. The target machine will send back a "SYN|ACK" (session request acknowledgement) packet if the port is open or an "RST" (Reset) packet if the port is closed. A machine that receives an unsolicited SYN|ACK packet will respond with an RST. An unsolicited RST will be ignored. Every IP packet on the Internet has a "fragment identification" number (IPID). The OS increases the IPID for each packet sent; thus, probing an IPID gives an attacker the number of packets sent since the last probe. In Zenmap, the `-sI` option is used to perform the IDLE scan.

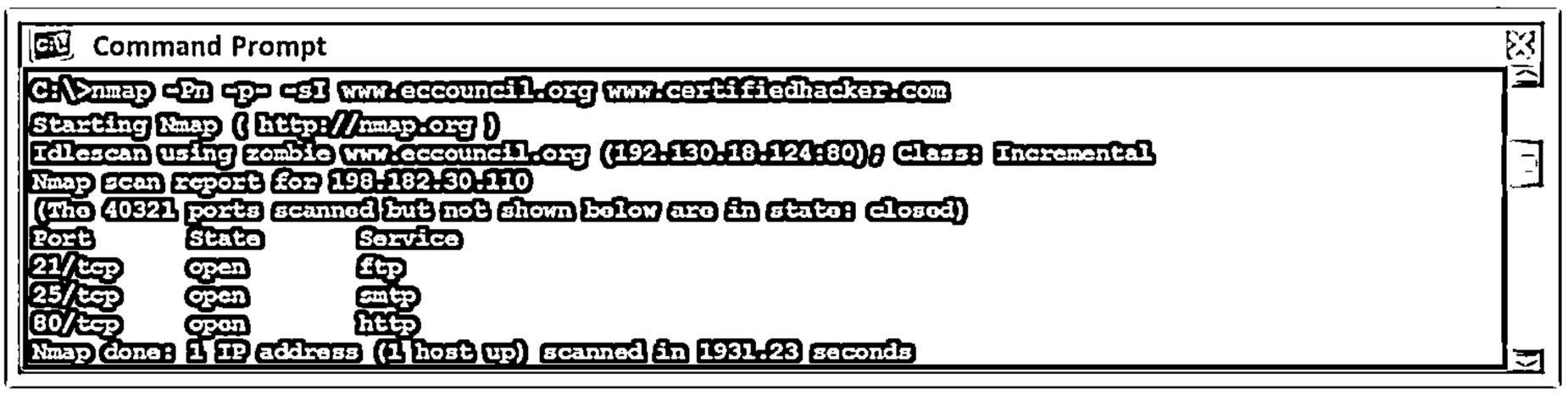


Figure 3.59: IDLE/IPID Header scan using Zenmap

The attacker performs this scan by impersonating another computer via spoofing. The attacker does not send a packet from her/his IP address; instead, he/she uses another host, often called a "zombie," to scan the remote host and identify any open ports. In this attack, the attacker

expects the sequence numbers of the zombie host, and if the remote host checks the IP of the scanning party, the IP of the zombie machine will be displayed.

IDLE Scan

Every IP packet on the Internet has a fragment Internet protocol identification (IPID) number that uniquely identifies fragments of an original IP datagram. As many OSs simply increase this number for each packet that they send, probing the IPID can tell an attacker how many packets the user sent since the last probe.

- **Step 1**

  The first step in performing an idle scan is to find an appropriate zombie. A zombie that assigns IPID packets incrementally on a global basis is an appropriate or idle zombie for performing the idle scan. The shorter the time interval for request/response between the attacker-zombie and the zombie-target, the faster is the scan.

  Choose a "Zombie" and Probe its Current IP Identification (IPID) Number

  In the first step, you will send the SYN+ACK packet to the zombie machine to probe its IPID number. Here, the SYN+ACK packet is sent to probe the IPID number but not establish a TCP connection (three-way handshake).

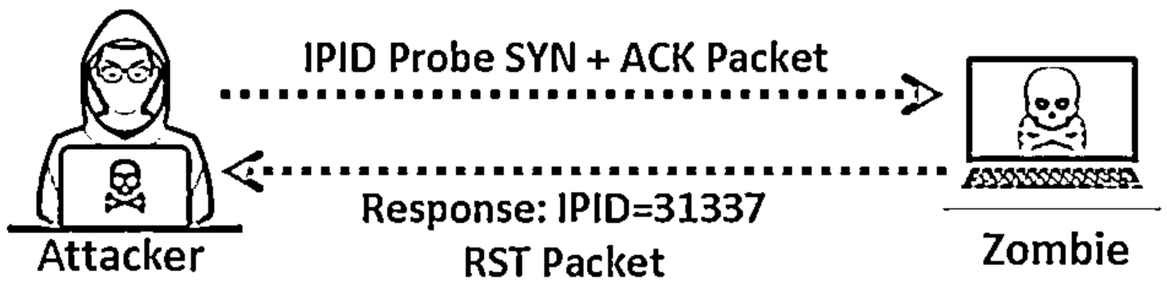


Figure 3.60: IDLE scan: Step 1

  As the zombie does not expect a SYN+ACK packet, it will deny the connection by sending back an RST packet. Analyze the RST packet sent by the zombie machine to extract the IPID. In the diagram shown in the slide above, assume that the zombie responds with `IPID=31337`. Furthermore, assume that this IPID is X.

- **Step 2**

  The attacker sends a SYN packet to the target machine on port 80, spoofing the IP address of the zombie.

  Idle Scan: Step 2.1 (Open Port)

  If the port is open, the target will send the SYN+ACK packet to the zombie (as the IP address was spoofed) to proceed with the three-way handshake. Since the zombie did not expect a SYN+ACK packet from the target machine, it will respond with an RST packet.

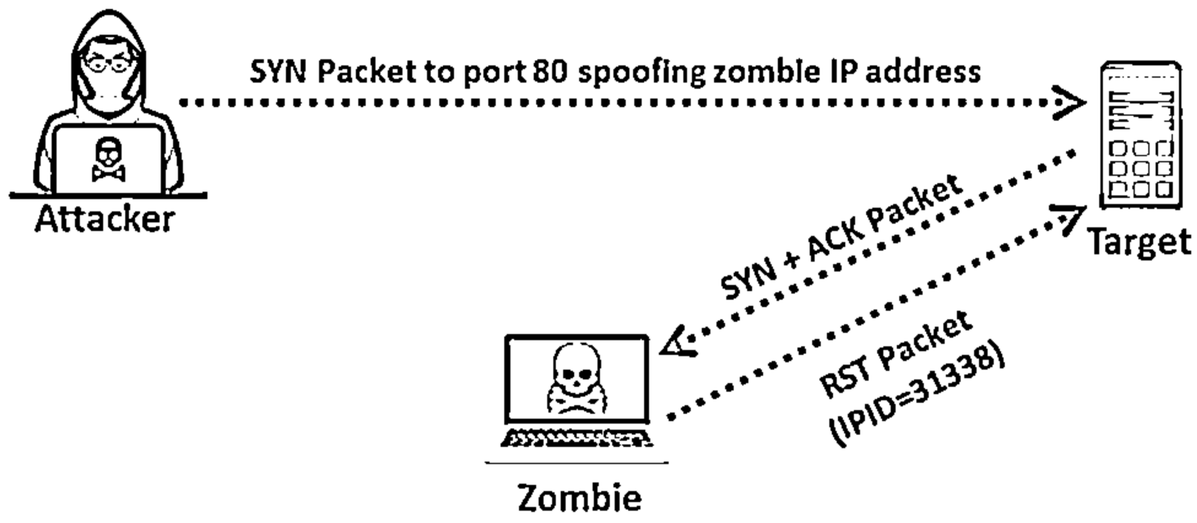


Figure 3.61: Port is open

Since every IP packet has a "fragment identification" number, which increases by one for every packet transmission, the zombie will now use its next available IPID, i.e., 31338 (X + 1).

Idle Scan: Step 2.2 (Closed Port)

Assume that the port on the target is closed. Subsequently, on receiving the SYN packet from the attacker (you), the target will respond with an RST, and the zombie will remain idle without taking any further action.

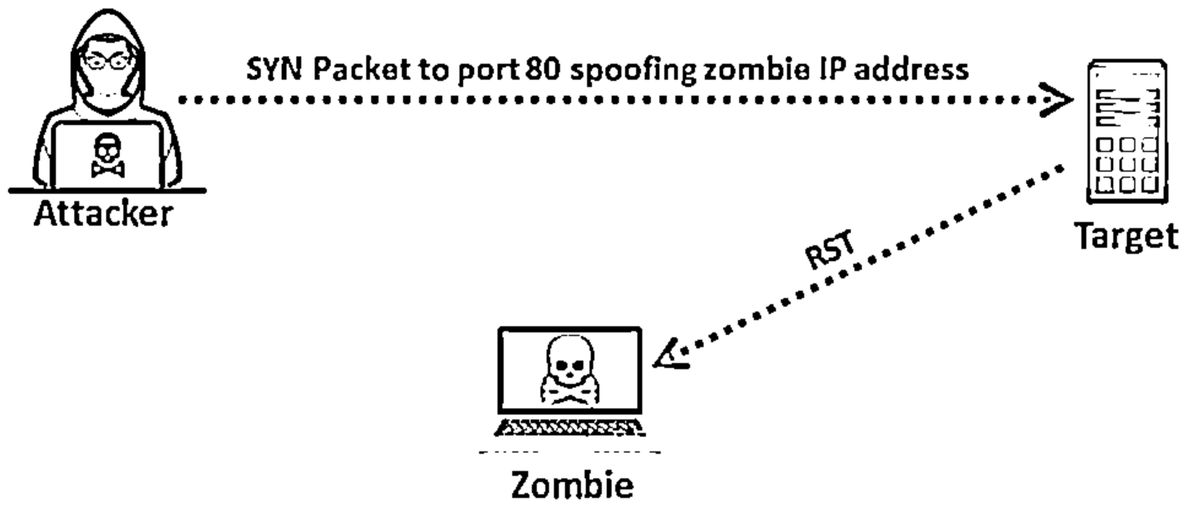


Figure 3.62: Port is closed

- **Step 3**

Now, follow step 1 again to probe the IPID number.

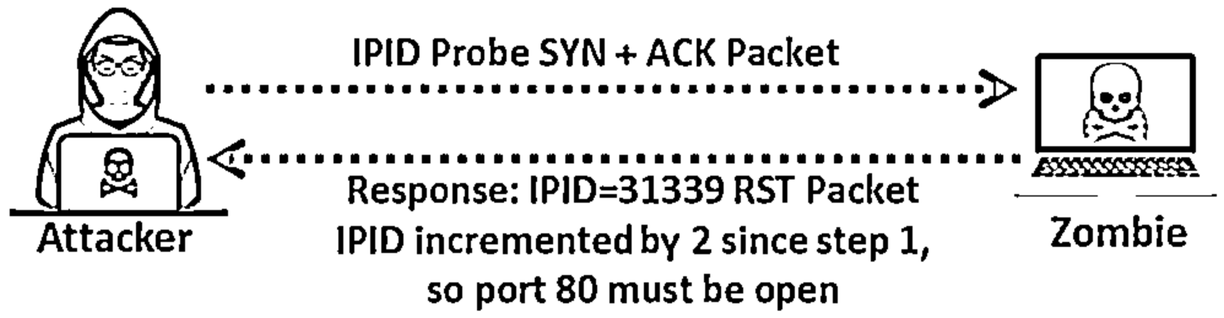
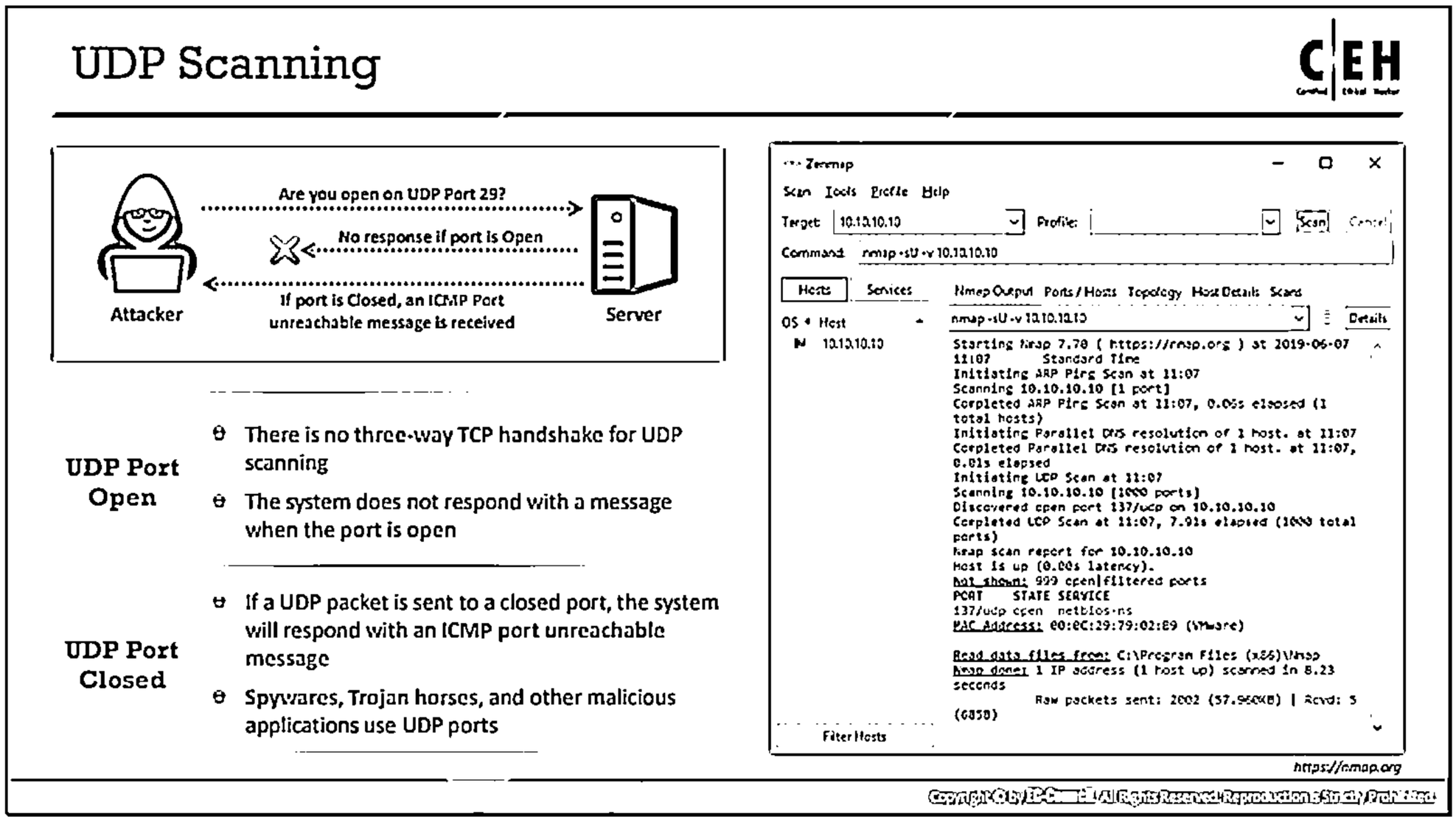


Figure 3.63: Idle scan: Step 3

Send a SYN+ACK packet to the zombie, and it will respond with an RST packet containing the IPID. Assume that the port on the target was open and that the zombie has already sent an RST packet to the target; then, the IPID number is increased by 1. Now, the zombie responds with an RST packet to the attacker using its next IPID, i.e., 31339 (X + 2). Consequently, the IPID is increased by 2, which implies that the port on the target machine was open. Thus, using an idle scan, an attacker can find out the open ports and services on the target machine by spoofing his/her IP address with a zombie's IP address.



UDP Scanning

UDP Raw ICMP Port Unreachable Scanning

UDP port scanners use the UDP protocol instead of TCP. There is no three-way handshake for the UDP scan. The UDP protocol can be more challenging to use than TCP scanning because you can send a packet but you cannot determine whether the host is alive, dead, or filtered. However, you can use one ICMP that checks for open or closed ports. If you send a UDP packet to a port without an application bound to it, the IP stack will return an ICMP port unreachable packet. If any port returns an ICMP error, it will be closed, leaving the ports that did not answer if they are open or filtered through the firewall.

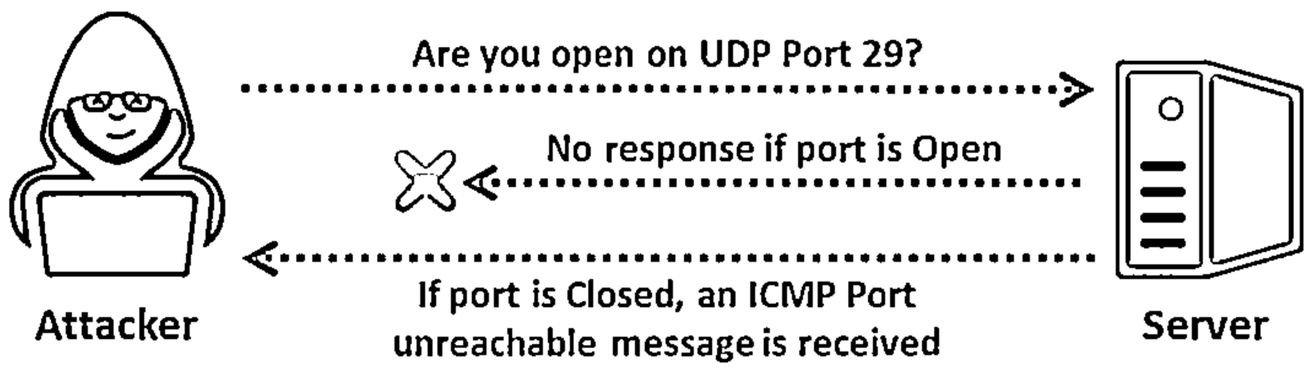


Figure 3.64: UDP scanning

This happens because open ports do not have to send an acknowledgement in response to a probe, and closed ports are not even required to send an error packet.

UDP Packets

Source: *https://nmap.org*

When you send a packet to a closed UDP port, most of the hosts send an `ICMP_PORT_UNREACH` error. Thus, you can determine whether a port is not open if UDP packets or ICMP errors are not guaranteed to arrive. Thus, UDP scanners of this type must implement retransmission of packets

that appear lost. UDP scanners interpret lost traffic as open ports. In Zenmap, the **-sU** option is used to perform a UDP scan.

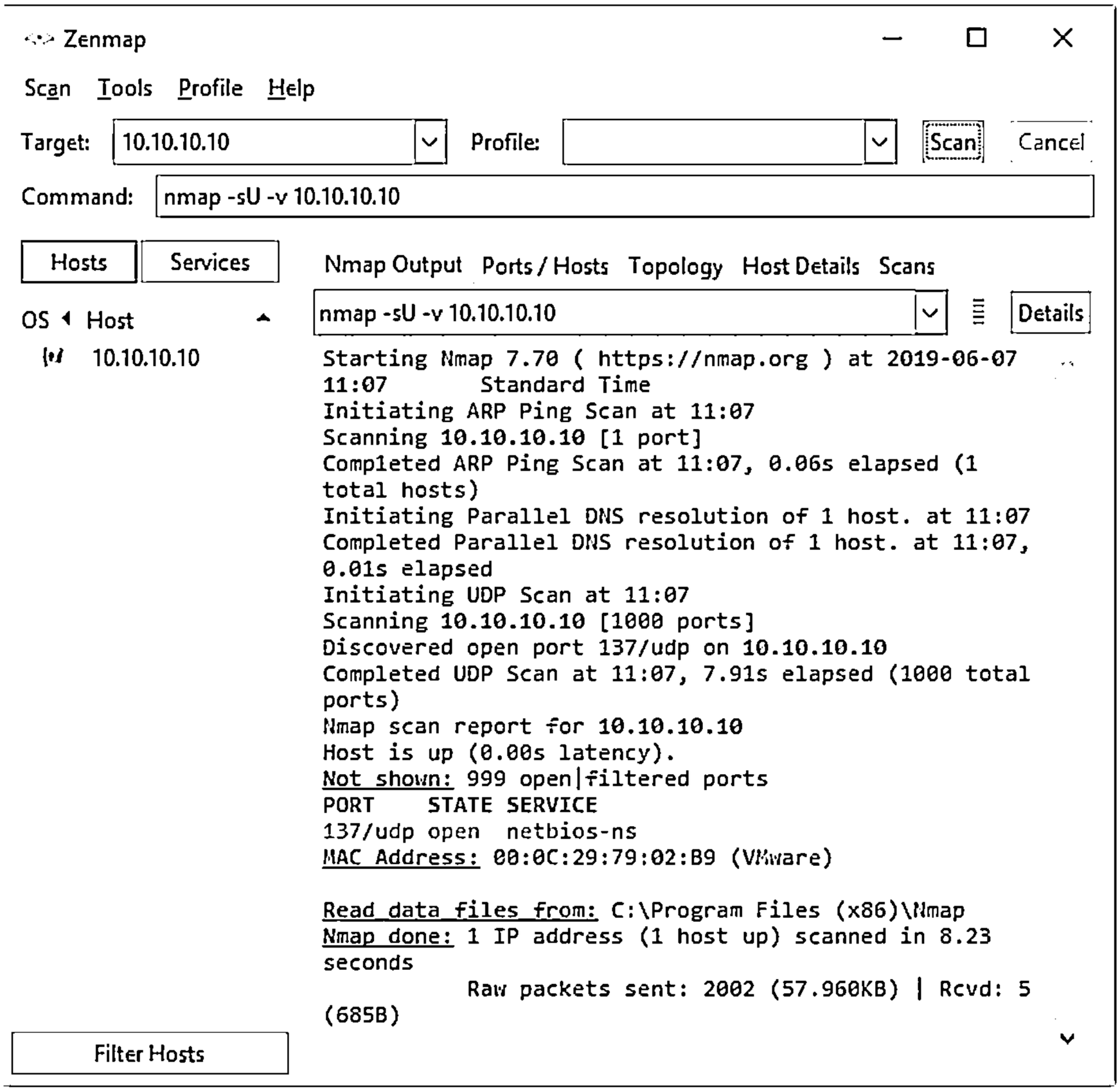


Figure 3.6S: UDP scanning using Zenmap

In addition, this scanning technique is slow because it limits the ICMP error message rate as a form of compensation to machines that apply RFC 1812 section 4.3.2.8. A remote host will require access to the raw ICMP socket to distinguish closed ports from unreachable ports.

UDP RECVFROM () and WRITE () Scanning

Although non-root users cannot read unreachable port errors directly, Linux informs you indirectly when it receives messages.

- **Example:**

  For example, a second `write ()` call to a closed port will usually fail. Various scanners, such as Netcat and Pluvial `pscan.c`, perform `recvfrom ()` on non-blocking UDP sockets, and they usually return `EAGAIN` (`"Try Again,"` `errno 13`) if the ICMP error has

not been received or `ECONNREFUSED` ("`Connection refused`," `errno 111`) otherwise. This technique is used for determining open ports when non-root users use `-u` (UDP). Root users can also use the `-l` (lamer UDP scan) option to force this process.

Advantage:

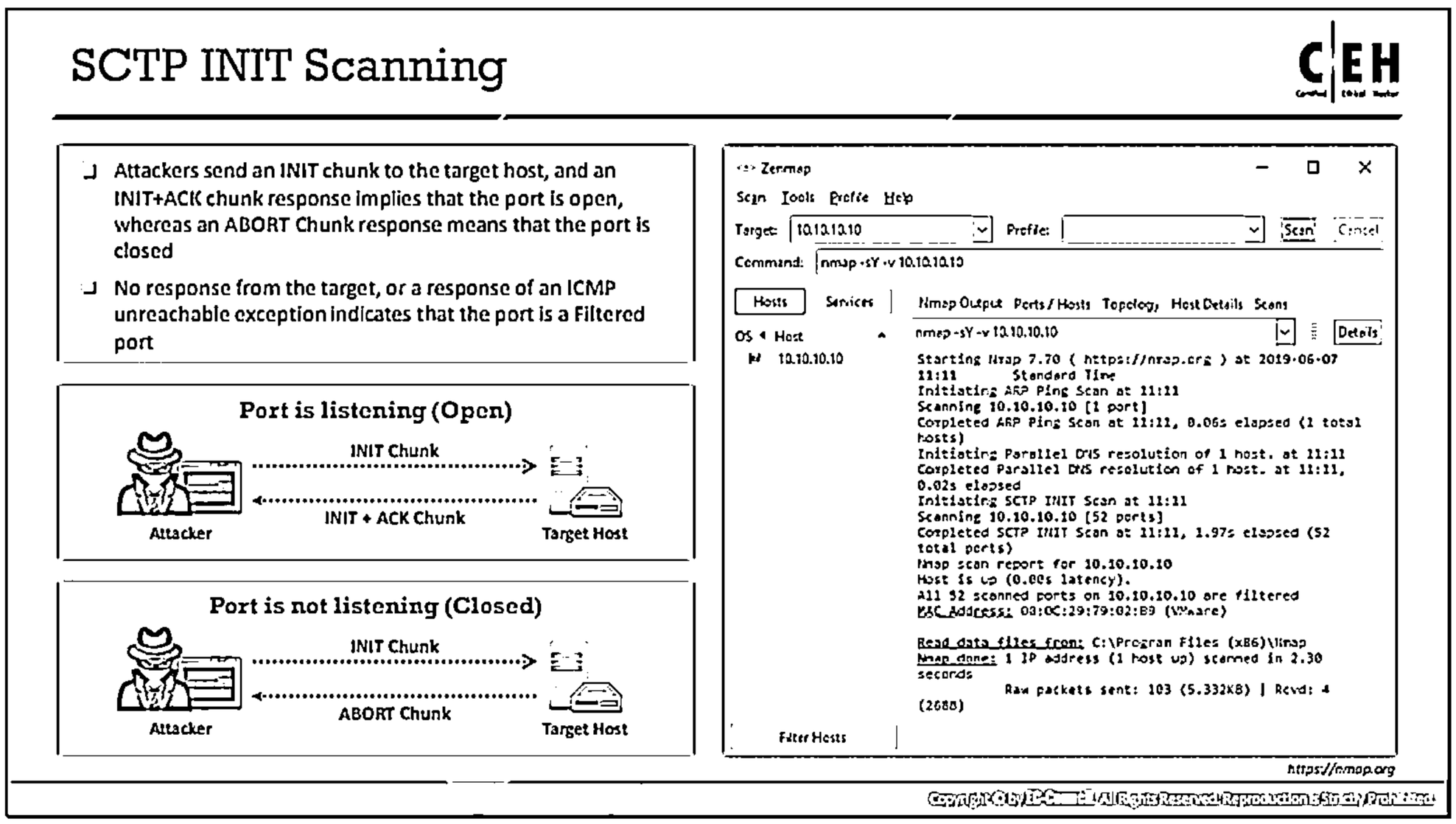
The UDP scan is less informal with regard to an open port because there is no overhead of a TCP handshake. However, if ICMP is responding to each unavailable port, the total number of frames can exceed that from a TCP scan. Microsoft-based OSs do not usually implement any ICMP rate limiting; hence, this scan operates very efficiently on Windows-based devices.

Disadvantage:

The UDP scan provides port information only. If additional information of the version is needed, the scan must be supplemented with a version detection scan (`-sV`) or the OS fingerprinting option (-o).

The UDP scan requires privileged access; hence, this scan option is only available on systems with the appropriate user permissions.

Most networks have massive amounts of TCP traffic; as a result, the efficiency of the UDP scan is low. The UDP scan will locate open ports and provide the security manager with valuable information for identifying successful attacker invasions on open UDP ports owing to spyware applications, Trojan horses, and other malicious software.



SCTP INIT Scanning

Stream Control Transport Protocol (SCTP) is a reliable message-oriented transport layer protocol. It is used as an alternative to the TCP and UDP protocols, as its characteristics are similar to those of TCP and UDP. SCTP is specifically used to perform multi-homing and multi-streaming activities. Some SCTP applications include discovering VoIP, IP telephony, and Signaling System 7/SIGnaling TRANsport (SS7/SIGTRAN)-related services. SCTP association comprises a four-way handshake method, as shown in the screenshot below.

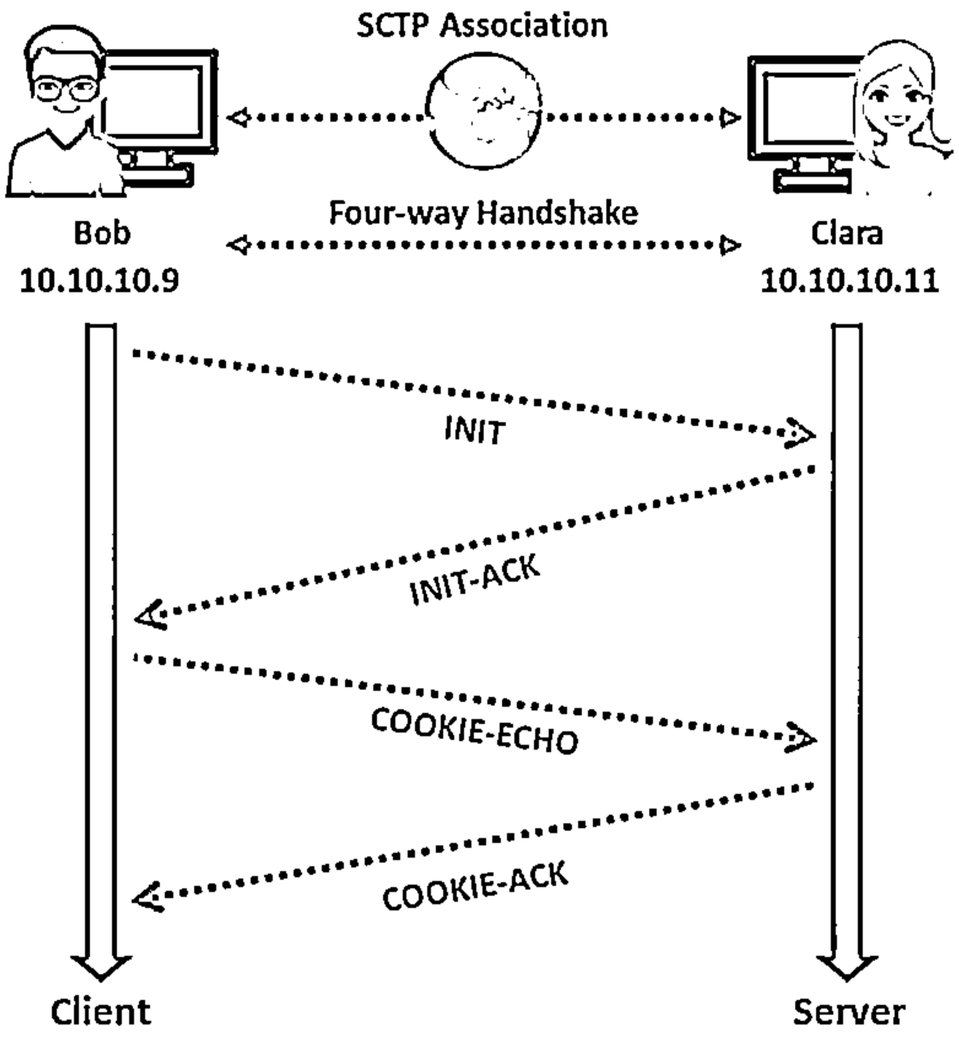


Figure 3.66: SCTP Association four-way handshake

In SCTP, the INIT scan is performed quickly by scanning thousands of ports per second on a fast network not obstructed by a firewall offering a stronger sense of security. The SCTP INIT scan is very similar to the TCP SYN scan; comparatively, it is also stealthy and unobtrusive, as it cannot complete SCTP associations, hence making the connection half-open.

Attackers send INIT chunk to the target host. If the port is listening or open, it sends an acknowledgement as an INIT+ACK chunk.

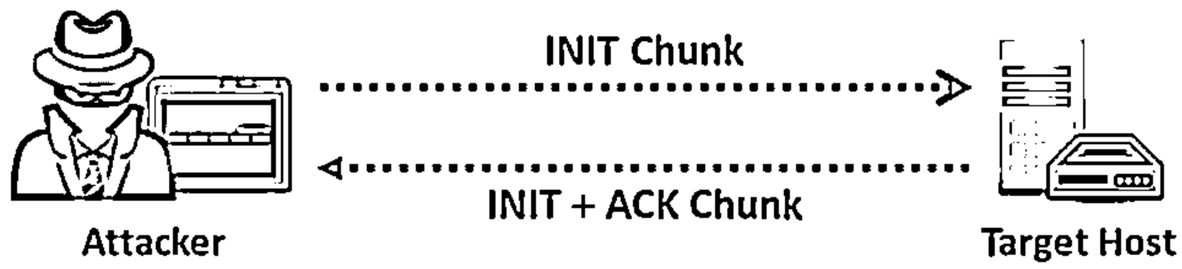


Figure 3.67: SCTP INIT scan result when a port is listening (Open)

If the target is inactive and it is not listening, then it sends an acknowledgement as an ABORT chunk.

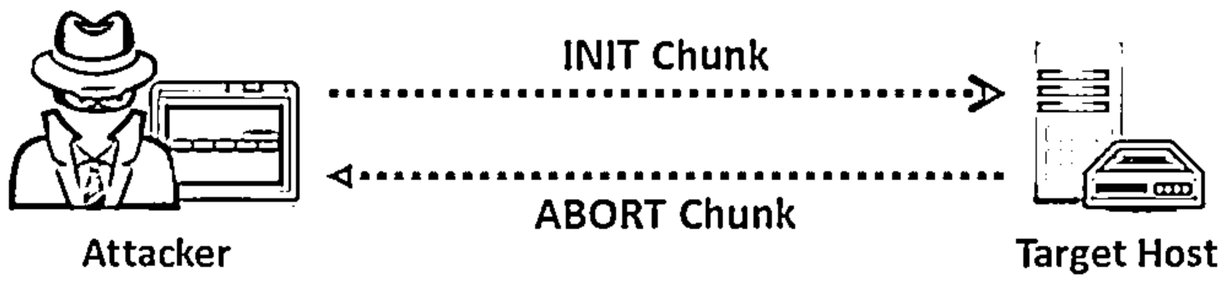


Figure 3.68: SCTP INIT scan result when a port is not listening (Closed)

After several retransmissions, if there is no response, then the port is indicated as a filtered port. The port is also indicated as a filtered port if the target server responds with an ICMP unreachable exception (type 3, code 0, 1, 2, 3, 9, 10, or 13). In Zenmap, the `-sY` option is used to perform the SCTP INIT scan.

Advantages:

- INIT scan can clearly differentiate between various ports such as open, closed, and filtered states

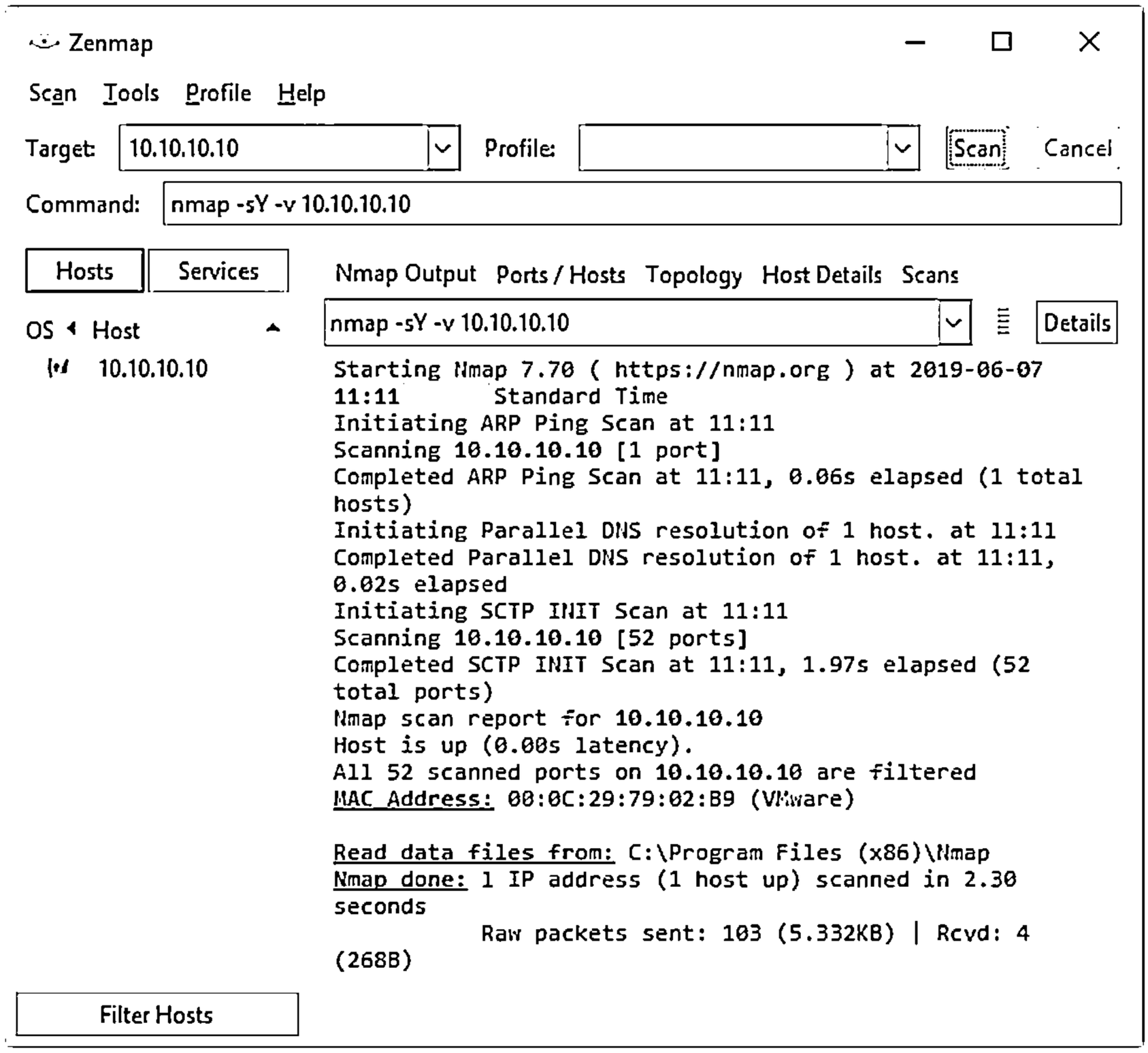
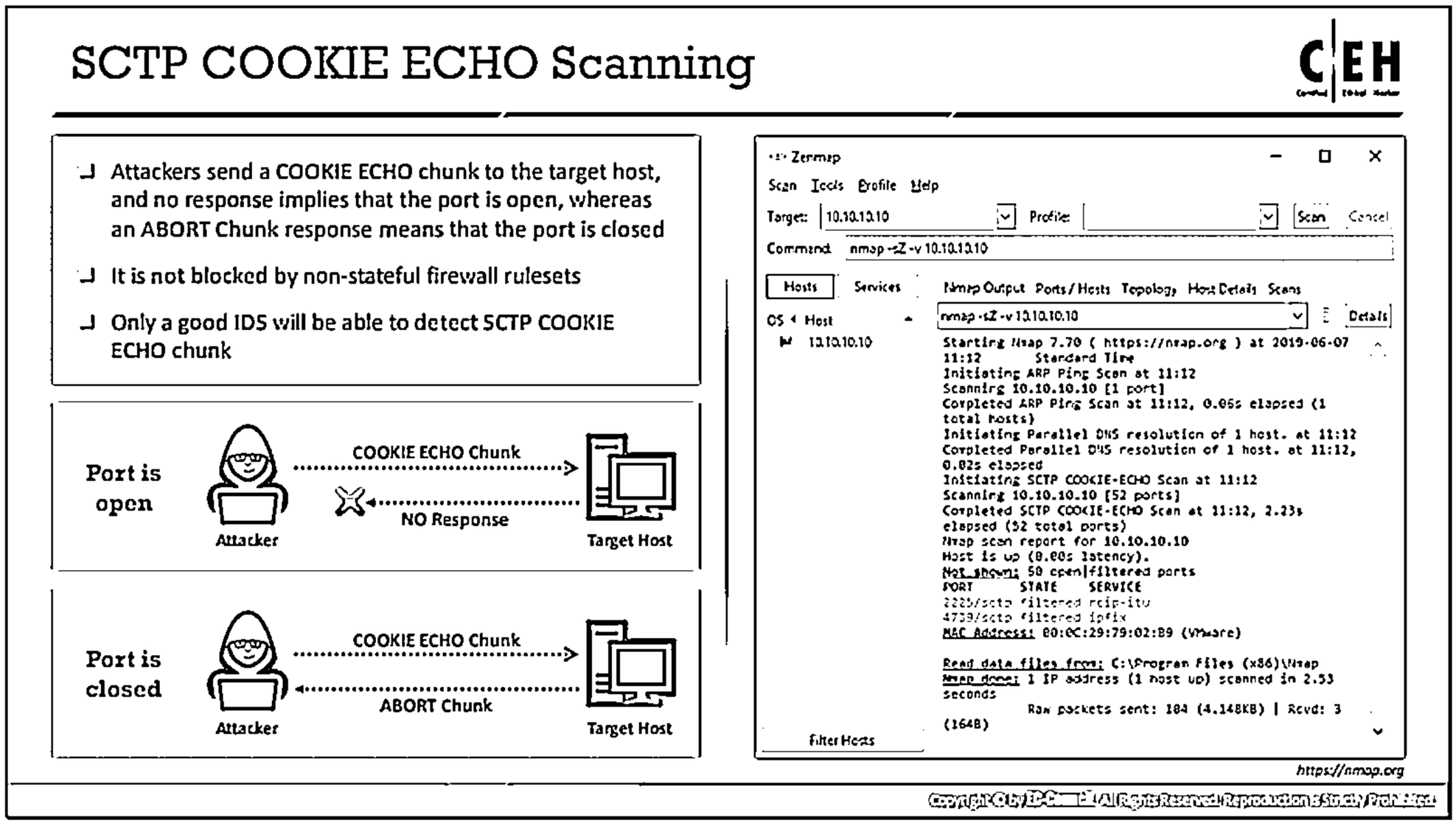


Figure 3.69: SCTP INIT scan in Zenmap



SCTP COOKIE ECHO Scanning

SCTP COOKIE ECHO scan is a more advanced type of scan. In this type of scan, attackers send the COOKIE ECHO chunk to the target, and if the target port is open, it will silently drop the packets onto the port and you will not receive any response from the target. If the target sends back the ABORT chunk response, then the port is considered as a closed port. The COOKIE ECHO chunk is not blocked by non-stateful firewall rule sets as in the INIT scan. Only an advanced IDS can detect the SCTP COOKIE ECHO scan. In Zenmap, the `-sZ` option is used to perform the SCTP COOKIE ECHO scan.

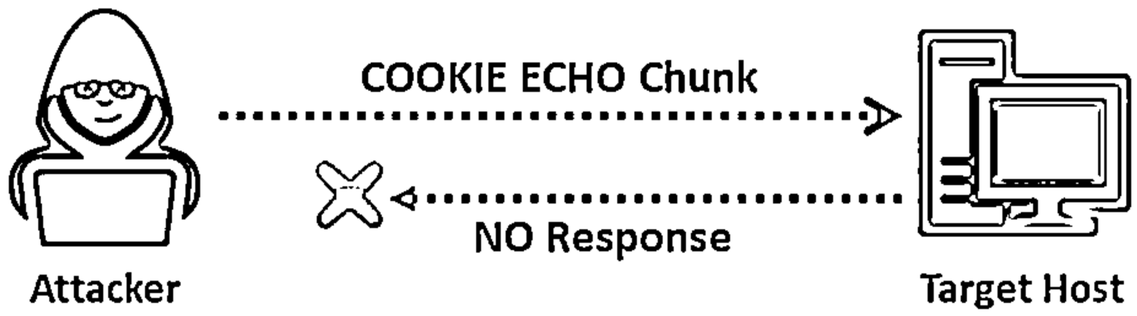


Figure 3.70: SCTP COOKIE ECHO scan result when port is open

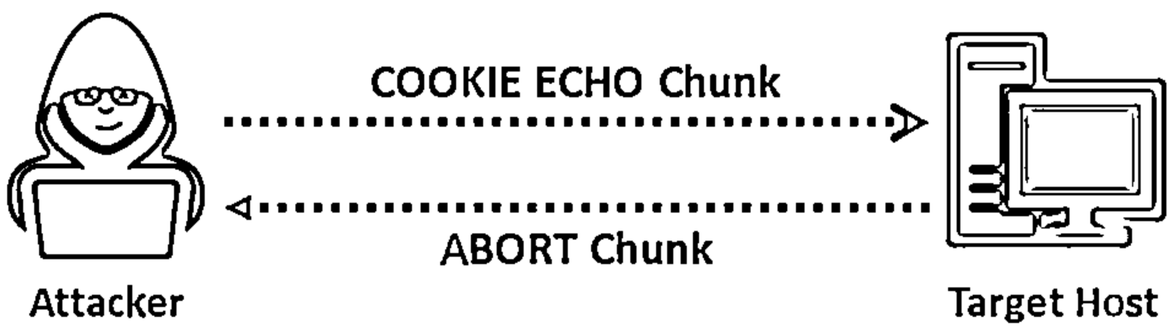


Figure 3.71: SCTP COOKIE ECHO scan result when port is closed

Advantages:

- The port scan is not as conspicuous as the INIT scan.

Disadvantages:

- SCTP COOKIE ECHO scan cannot differentiate clearly between open and filtered ports, and it shows the output as open|filtered in both cases.

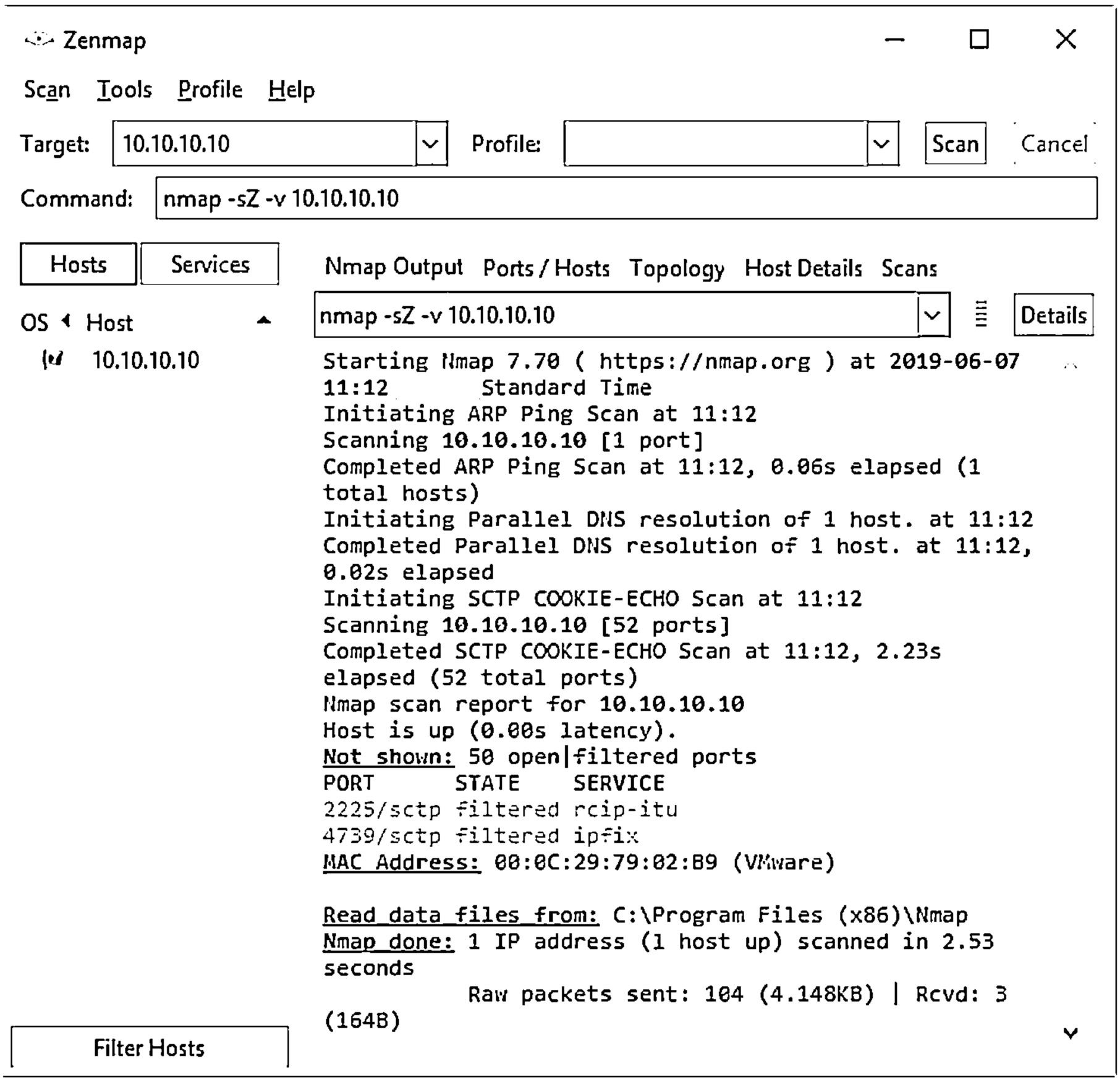


Figure 3.72: SCTP COOKIE-ECHO scan in Zenmap

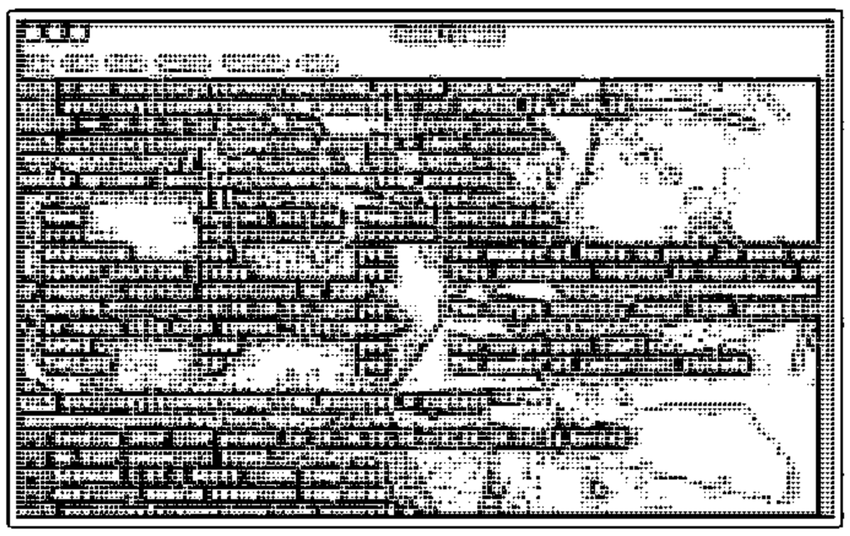
SSDP and List Scanning

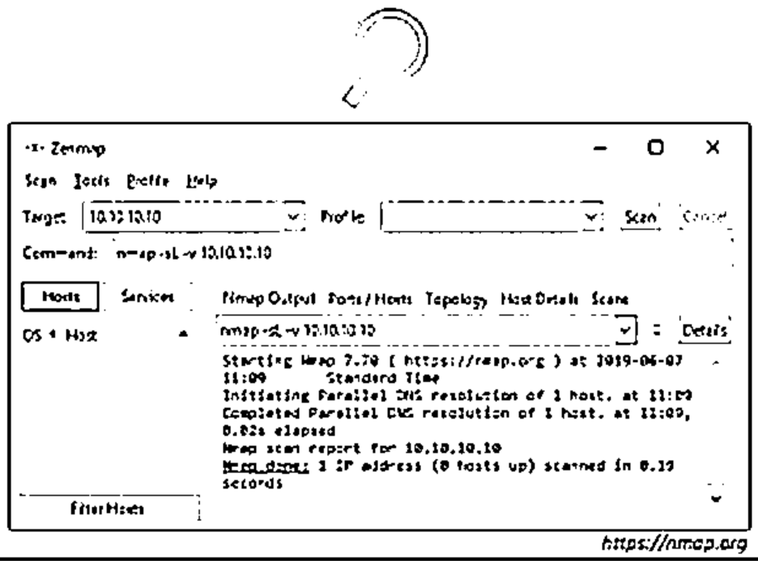
SSDP Scanning

- The Simple Service Discovery Protocol (SSDP) is a network protocol that works in conjunction with the UPnP to detect plug and play devices
- Vulnerabilities in UPnP may allow attackers to launch Buffer overflow or DoS attacks
- Attacker may use the UPnP SSDP M-SEARCH information discovery tool to check if the machine is vulnerable to UPnP exploits or not

List Scanning

- This type of scan simply generates and prints a list of IPs/Names without actually pinging them
- A reverse DNS resolution is performed to identify the host names





https://nmap.org

SSDP and List Scanning

SSDP Scanning

Simple Service Discovery Protocol (SSDP) is a network protocol that generally communicates with machines when querying them with routable IPv4 or IPv6 multicast addresses. The SSDP service controls communication for the Universal Plug and Play (UPnP) feature. It generally works when the machine is not firewalled; however, it can sometimes work through a firewall. The SSDP service will respond to a query sent over IPv4 or IPv6 broadcast addresses. This response includes information about the UPnP feature associated with it. The attacker uses SSDP scanning to detect UPnP vulnerabilities that may allow him/her to launch buffer overflow or DoS attacks.

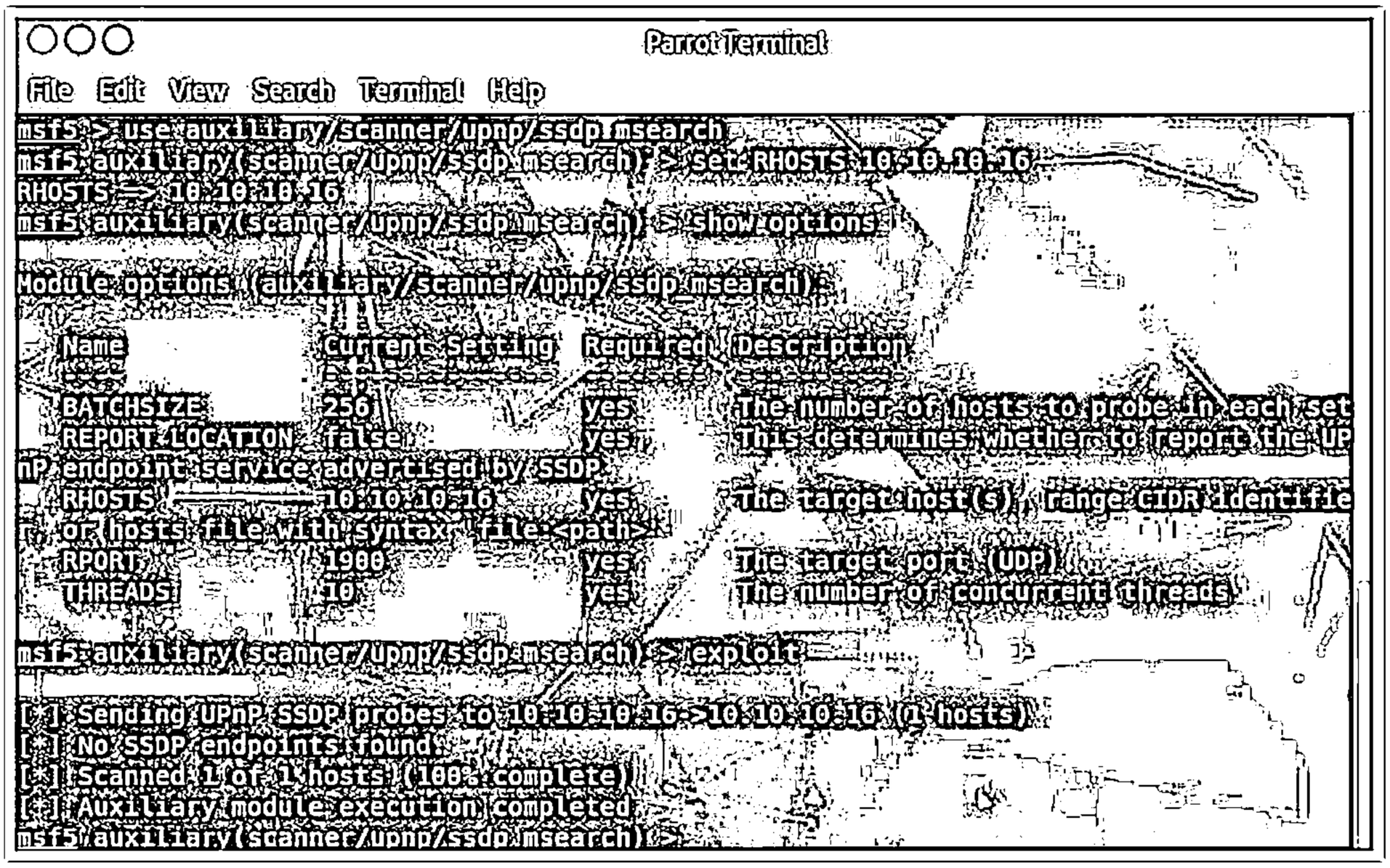


Figure 3.73: UPnP SSDP M-SEARCH in Parrot Security

The attacker may use the UPnP SSDP M-SEARCH information discovery tool to check whether the machine is vulnerable to UPnP exploits. The UPnP SSDP M-SEARCH information discovery tool gleans information from UPnP-enabled systems, as shown in the figure.

List Scanning

In a list scan, the discovery of the active network host is indirect. A list scan simply generates and prints a list of IPs/Names without actually pinging or scanning the hosts. As a result, the list scan shows all IP addresses as "not scanned" (0 hosts up). By default, a reverse DNS resolution is still carried out on each host by Nmap to learn their names. In Zenmap, the `-sL` option is used to perform a list scan.

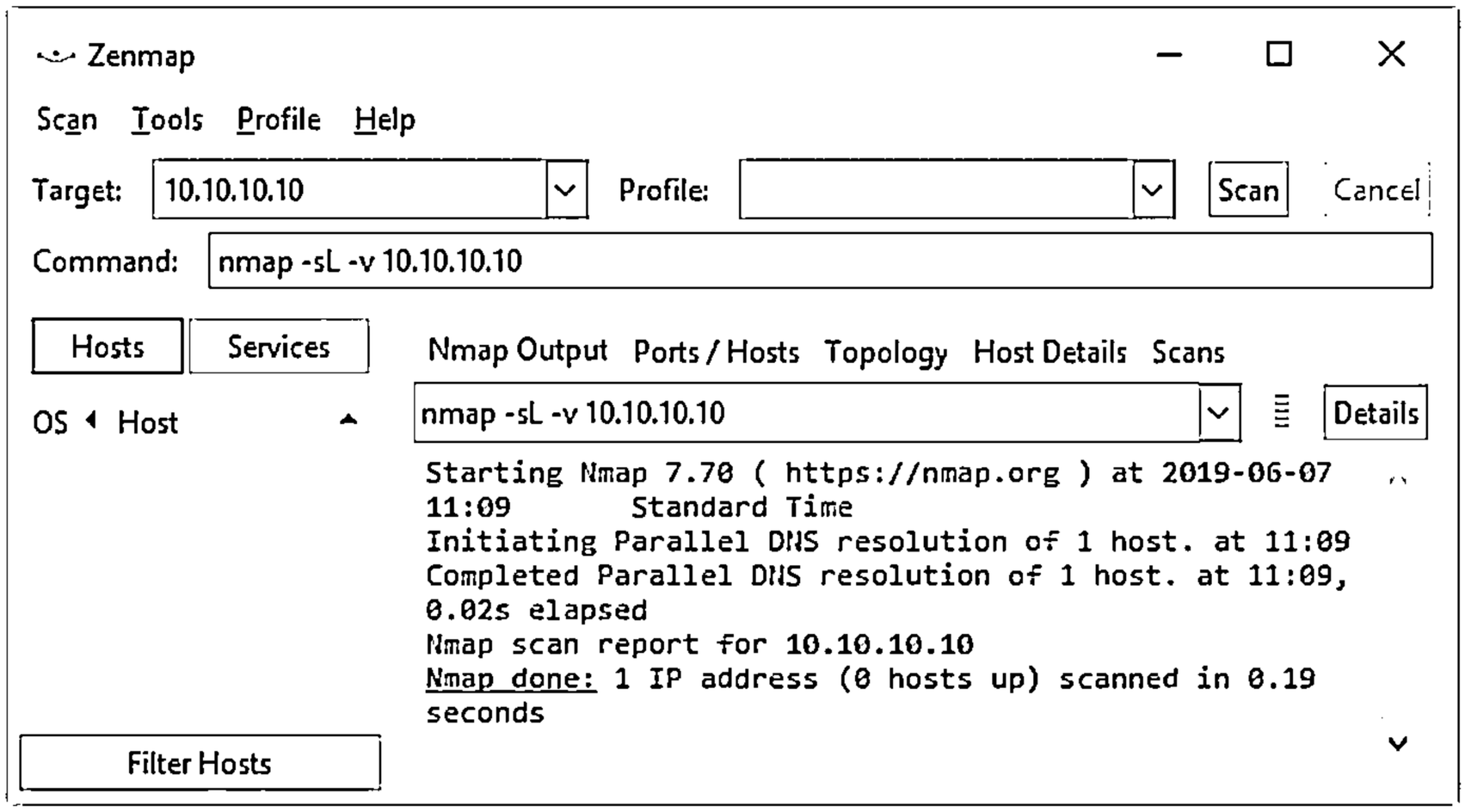


Figure 3.74: List scan using Zenmap

Advantages:

- A list scan can perform a good sanity check.
- The list scan detects incorrectly defined IP addresses in the command line or in an option file. It primarily repairs the detected errors to run any "active" scan.

IPv6 Scanning

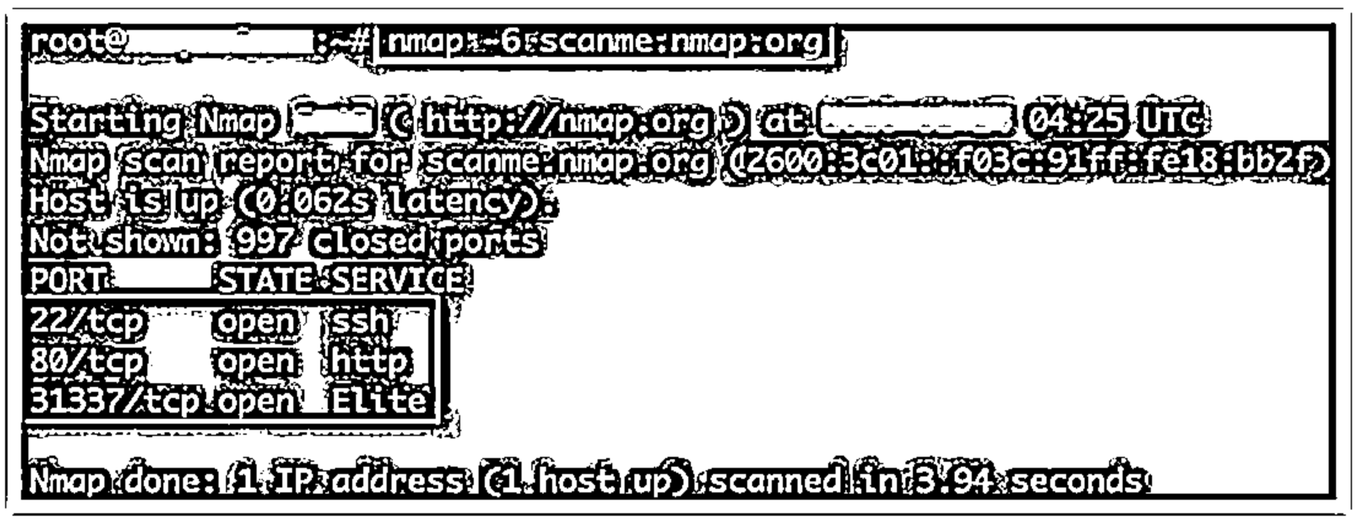
- IPv6 increases the IP address size from 32 bits to 128 bits to support more levels of address hierarchy
- Attackers need to harvest IPv6 addresses from network traffic, recorded logs, or Received from: header lines in archived emails
- Attackers can use the -6 option in Zenmap to perform IPv6 scanning

```
root@          :~# nmap -6 scanme.nmap.org

Starting Nmap      ( http://nmap.org ) at          04:25 UTC
Nmap scan report for scanme.nmap.org (2600:3c01::f03c:91ff:fe18:bb2f)
Host is up (0.062s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 3.94 seconds
```

https://nmap.org

IPv6 Scanning

IPv6 increases the size of the IP address space from 32 bits to 128 bits to support higher levels of the addressing hierarchy. Traditional network scanning techniques are computationally less feasible because of the larger search space (64 bits of host address space, or 2^{64} addresses) provided by IPv6 in a subnet. Scanning the IPv6 network is more difficult and complex compared to IPv4. Additionally, a number of scanning tools do not support ping sweeps on IPv6 networks. Attackers need to harvest IPv6 addresses from network traffic, recorded logs, or "Received from" and other header lines in archived email or Usenet news messages to identify IPv6 addresses for subsequent port scanning. However, scanning an IPv6 network provides a large number of hosts in a subnet; if an attacker can compromise one subnet host, he/she can probe the "all hosts" link local multicast address if the hosts numbers are sequential or use any regular scheme. An attacker needs to analyze 2^{64} addresses to verify if a particular open service is running on a host in that subnet. At a conservative rate of one probe per second, such a scan would take about 5 billion years to complete. Attackers can use Nmap to perform IPv6 scanning. In Zenmap, the -6 option is used to perform the IPv6 scan.

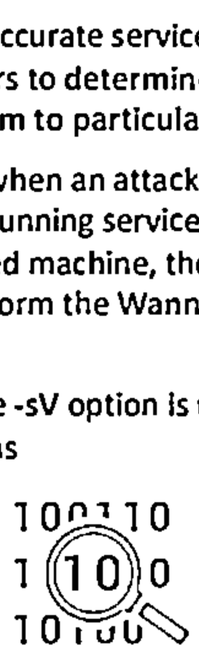


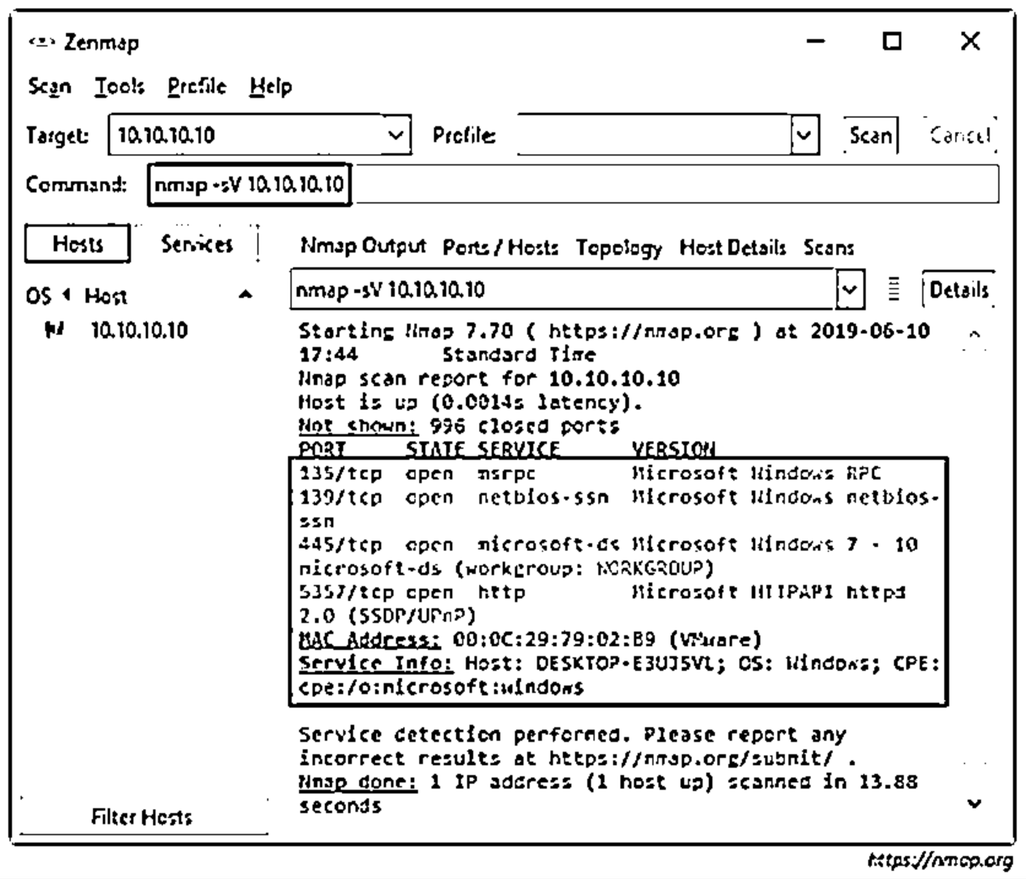
```
root@          :~# nmap -6 scanme.nmap.org

Starting Nmap      ( http://nmap.org ) at          04:25 UTC
Nmap scan report for scanme.nmap.org (2600:3c01::f03c:91ff:fe18:bb2f)
Host is up (0.062s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 3.94 seconds
```

Figure 3.75: IPv6 Scan in Zenmap

Service Version Discovery

- Service version detection helps attackers to obtain information about running services and their versions on a target system
- Obtaining an accurate service version number allows attackers to determine the vulnerability of target system to particular exploits
- For example, when an attacker detects SMBv1 protocol as a running service on a target Windows-based machine, then the attacker can easily perform the WannaCry ransomware attack
- In Zenmap, the -sV option is used to detect service versions





Service Version Discovery

Every port is assigned a specific service, and every service has its own version. Some versions of the protocols are insecure, and they can allow attackers to compromise the machine by exploiting this vulnerability. Service version detection helps attackers to obtain information about the running services and their versions on a target system. By obtaining accurate service version numbers, an attacker can determine which exploits the target system is vulnerable to. For example, when the attacker detects the SMBv1 protocol as a running service on the target Windows machine, then he/she can easily perform a WannaCry ransomware attack with the help of the eternalblue and doublepulsar backdoor combination in Metasploit.

The version detection technique is nothing but examination of the TCP and UDP ports. The probes from the Nmap `service-probes` database are used for querying various services and matching expressions for recognizing and parsing responses. In Zenmap, the `-sV` option is used to detect service versions.

Zenmap

Scan Tools Profile Help

Target: 10.10.10.10 Profile: Scan Cancel

Command: nmap -sV 10.10.10.10

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

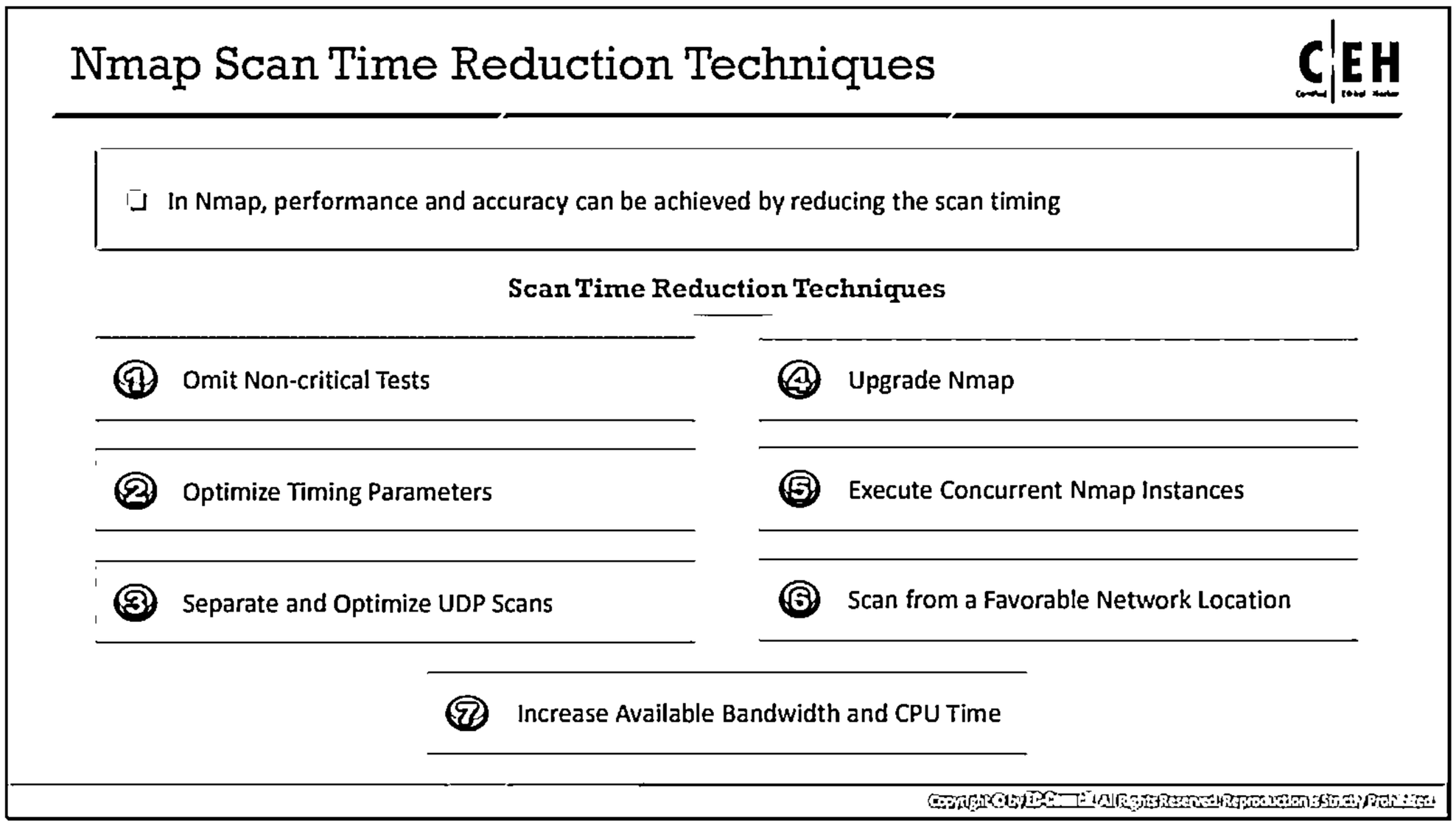
10.10.10.10

nmap -sV 10.10.10.10 Details

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-10
17:44        Standard Time
Nmap scan report for 10.10.10.10
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-
ssn
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10
microsoft-ds (workgroup: WORKGROUP)
5357/tcp open  http         Microsoft HTTPAPI httpd
2.0 (SSDP/UPnP)
MAC Address: 00:0C:29:79:02:B9 (VMware)
Service Info: Host: DESKTOP-E3UJ5VL; OS: Windows; CPE:
cpe:/o:microsoft:windows

Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.88
seconds
```

Filter Hosts

Figure 3.76: Service version discovery in Zenmap



Nmap Scan Time Reduction Techniques

In Nmap, performance and accuracy take high priority, and this only be achieved only by reducing the long scan time. The important techniques for reducing the scan time are as follows:

- **Omit Non-critical Tests**

  While performing the Nmap scan, the time complexity can be reduced by the following methods:

  - Avoiding an intense scan if only a minimal amount of information is required.
  - The number of ports scanned can be limited using specific commands.
  - The port scan (`-sn`) can be skipped if and only if one has to check whether the hosts are online or not.
  - Advanced scan types (`-sC`, `-sV`, `-O`, `--traceroute`, and `-A`) can be avoided.
  - The DNS resolution should be turned on only when it is necessary.

- **Optimize Timing Parameters**

  To control the scan activity, Nmap provides the `-T` option for scanning ranging from high-level to low-level timing aggressiveness. This can be extremely useful for scanning highly filtered networks.

- **Separate and Optimize UDP Scans**

  As many vulnerable services use the UDP protocol, scanning the UDP protocol is vital, and it should be scanned separately, as TCP scans have different performance requirements and timing characteristics. Moreover, the UDP scan is more affected by the ICMP error rate-limiting compared to the TCP scan.

- **Upgrade Nmap**

  It is always advisable to use the upgraded version of Nmap as it contains many bug fixes, important algorithmic enhancements, and high-performance features such as local network ARP scanning.

- **Execute Concurrent Nmap Instances**

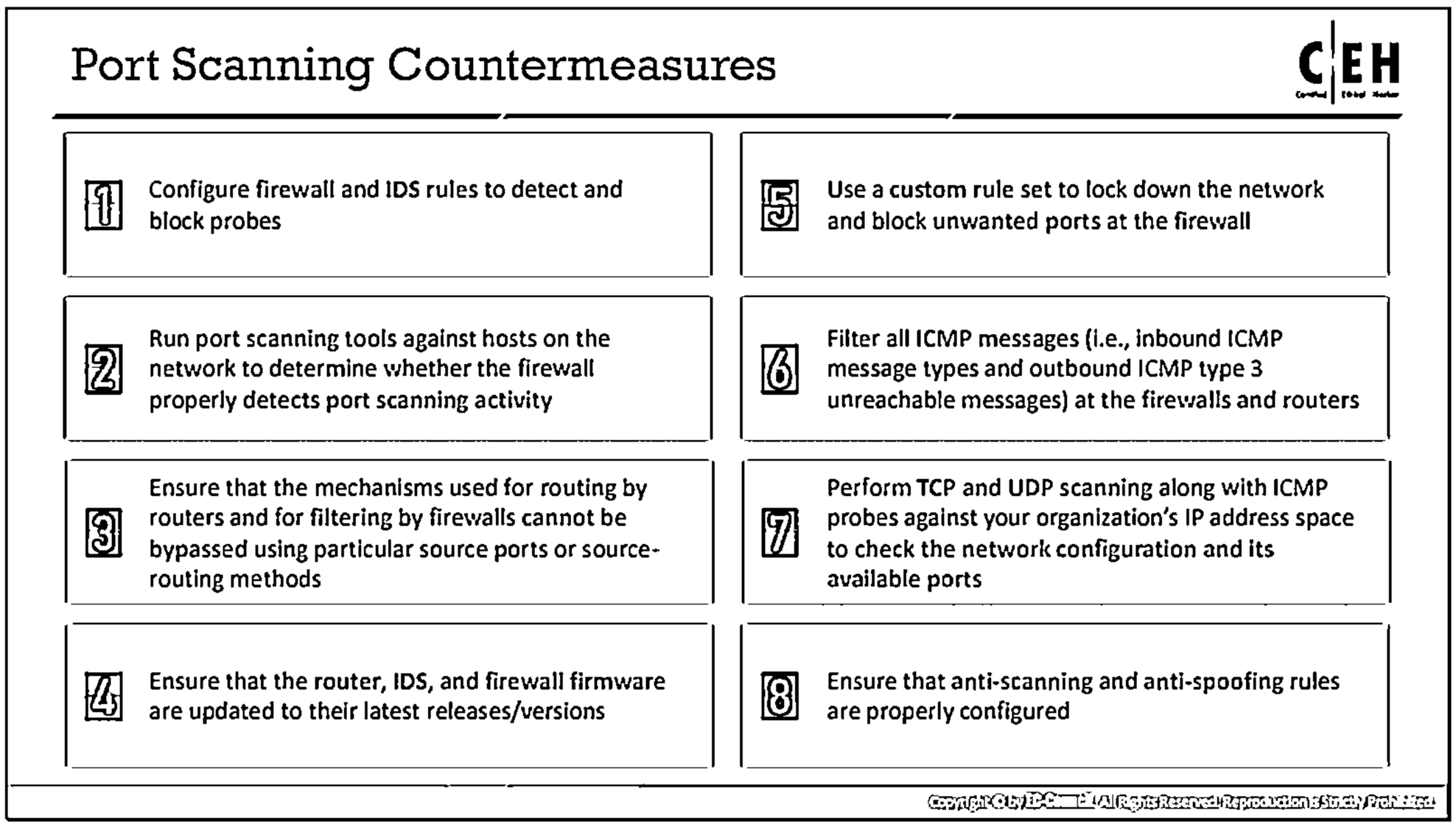
  Running Nmap against the whole network usually makes the system slower and less efficient. Nmap supports parallelization and it can also be customized according to specific needs. It becomes very efficient by getting an idea of the network reliability while scanning a larger group. The overall speed of the scan can be improved by dividing it into many groups and running them simultaneously.

- **Scan from a Favorable Network Location**

  It is always advisable to run Nmap from the host's local network to the target while in the internal network, as it offers defense-in-depth security. External scanning is obligatory when performing firewall testing or when the network should be monitored from the external attacker's viewpoint.

- **Increase Available Bandwidth and CPU Time**

  By increasing the available bandwidth or CPU power, the Nmap scan time can be reduced. This can be done by installing a new data line or stopping any running applications. Nmap is controlled by its own congestion control algorithms, so that network flooding can be prevented. This improves its accuracy. The Nmap bandwidth usage can be tested by running it in the verbose mode `-v`.



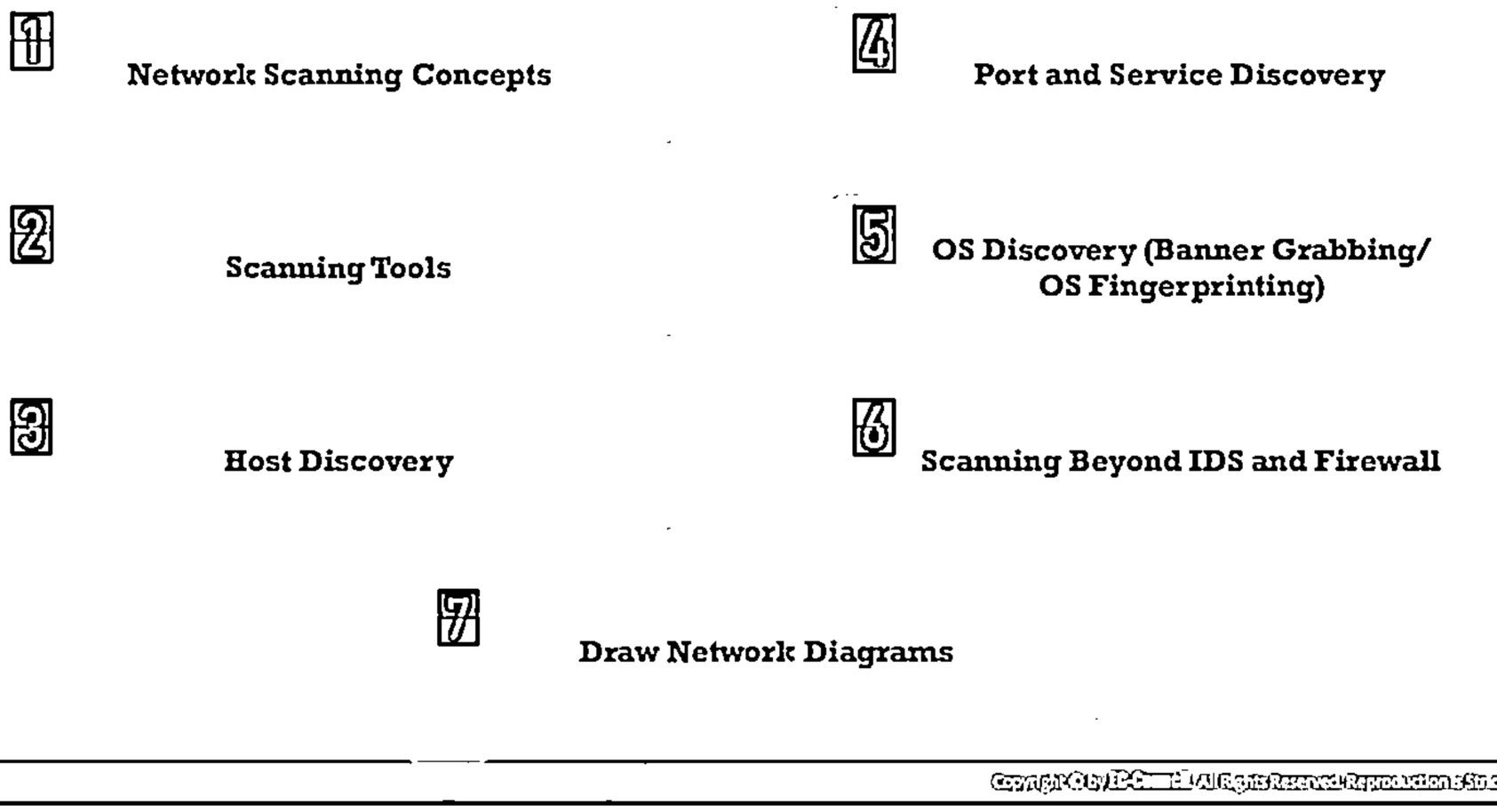
Port Scanning Countermeasures

As discussed previously, port scanning provides a large amount of useful information to the attacker, such as IP addresses, host names, open ports, and services running on ports. Open ports specifically offer an easy means for the attacker to break into the network. However, there is no cause for concern, provided that you secure your system or network against port scanning by adopting the following countermeasures:

- Configure firewall and IDS rules to detect and block probes.
- The firewall should be capable of detecting probes sent by the attackers using port scanning tools. It should not allow traffic to pass through it after simply inspecting the TCP header. The firewall should be able to examine the data contained in each packet before allowing the traffic to pass through it.
- Run the port scanning tools against hosts on the network to determine whether the firewall accurately detects the port scanning activity.
- Some firewalls do a better job than others in terms of detecting stealth scans. For example, many firewalls have specific options to detect SYN scans, while others completely ignore FIN scans.
- Ensure that the router, IDS, and firewall firmware are updated with their latest releases/versions.
- Configure commercial firewalls to protect your network against fast port scans and SYN floods. You can run tools such as port entry to detect and stop port scan attempts on Linux/UNIX systems.

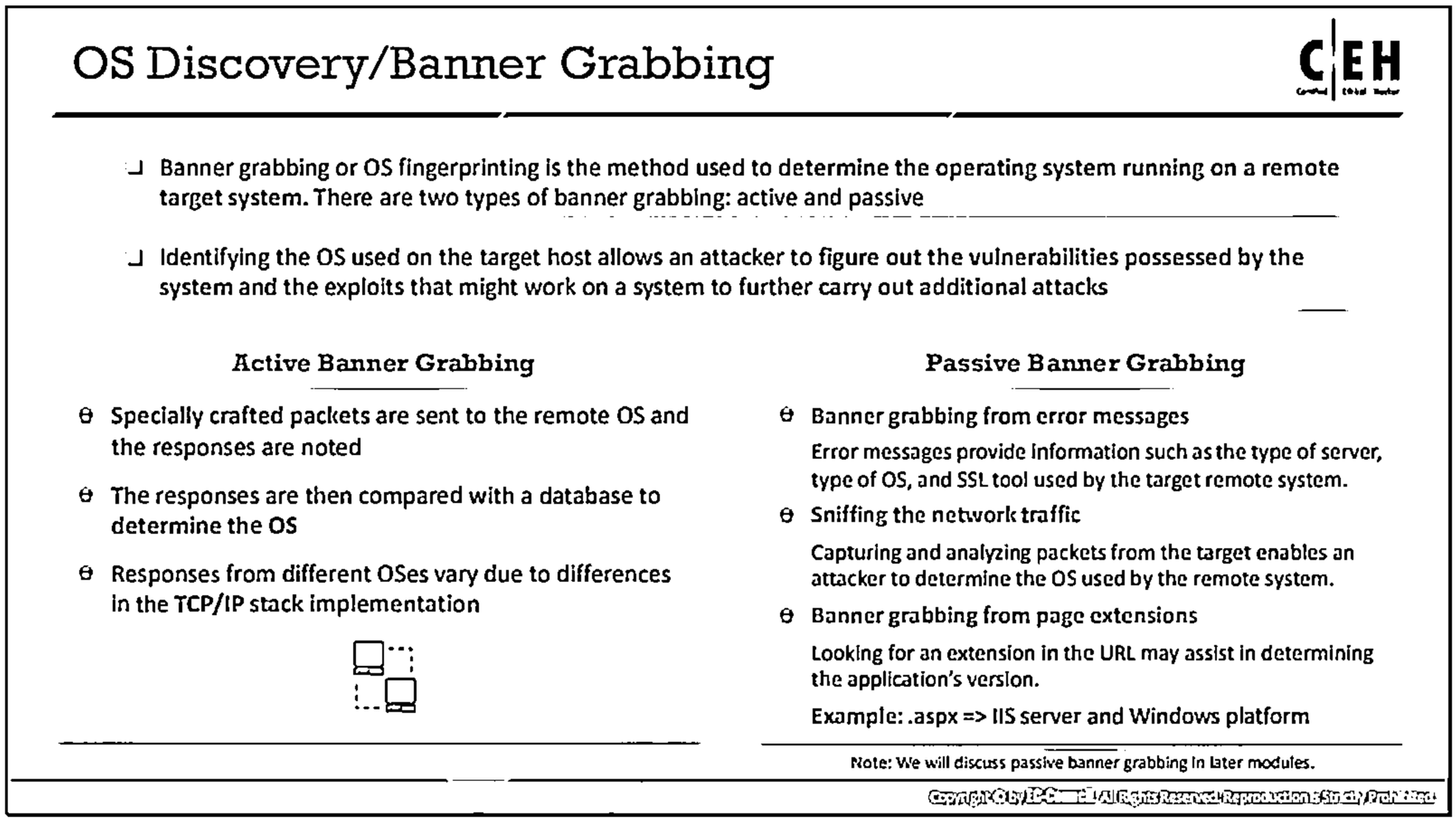
- Hackers use tools such as Nmap and perform OS detection to sniff the details of a remote OS. Thus, it is important to employ intrusion detection systems in such cases. Snort (*https://www.snort.org*) is an intrusion detection and prevention technology that is very useful, mainly because signatures are frequently available from the public authors.
- Keep as few ports open as possible and filter the rest, as the intruder will try to enter through any open port. Use a custom rule set to lock down the network, block unwanted ports at the firewall, and filter the following ports: 135–159, 256–258, 389, 445, 1080, 1745, and 3268.
- Block unwanted services running on the ports and update the service versions.
- Ensure that the versions of services running on the ports are non-vulnerable.
- Block inbound ICMP message types and all outbound ICMP type-3 unreachable messages at border routers arranged in front of a company's main firewall.
- Attackers try to perform source routing and send packets to the targets (which may not be reachable via the Internet) using an intermediate host that can interact with the target. Hence, it is necessary to ensure that your firewall and router can block such source-routing techniques.
- Ensure that the mechanism used for routing and filtering at the routers and firewalls, respectively, cannot be bypassed using a particular source port or source-routing methods.
- Test your IP address space using TCP and UDP port scans as well as ICMP probes to determine the network configuration and accessible ports.
- Ensure that the anti-scanning and anti-spoofing rules are configured.
- If a commercial firewall is in use, then ensure that:
  - It is patched with the latest updates
  - It has correctly defined antispoofing rules
  - Its fastmode services are unusable in Check Point Firewall-1 environments

Module Flow



OS Discovery (Banner Grabbing/OS Fingerprinting)

An attacker uses OS discovery or banner grabbing techniques to identify network hosts running application and OS versions with known exploits. This section introduces you to banner grabbing, its types, and its tools, as well as useful countermeasures that you can adopt against it.



OS Discovery/Banner Grabbing

Banner grabbing, or "OS fingerprinting," is a method used to determine the OS that is running on a remote target system. It is an important scanning method, as the attacker will have a higher probability of success if the OS of the target system is known (many vulnerabilities are OS-specific). The attacker can then formulate an attack strategy based on the OS of the target system.

There are two methods for banner grabbing: spotting the banner while trying to connect to a service, such as an FTP site, and downloading the binary file/bin/ls to check the system architecture.

A more advanced fingerprinting technique depends on stack querying, which transfers the packets to the network host and evaluates them by the reply. The first stack-querying method designed with regard to the TCP mode of communication evaluates the response to connection requests.

The next method, known as initial sequence number (ISN) analysis, identifies the differences in random number generators found in the TCP stack.

ICMP response analysis is another method used to fingerprint an OS. It consists of sending ICMP messages to a remote host and evaluating the reply.

Two types of banner grabbing techniques are described below:

- **Active Banner Grabbing**

  Active banner grabbing applies the principle that an OS's IP stack has a unique way of responding to specially crafted TCP packets. This happens because of different interpretations that vendors apply while implementing the TCP/IP stack on a particular

OS. In active banner grabbing, the attacker sends a variety of malformed packets to the remote host, and the responses are compared with a database. Responses from different OS vary because of differences in TCP/IP stack implementation.

For instance, the scanning utility Nmap uses a series of nine tests to determine an OS fingerprint or banner grabbing. The tests listed below provide some insights into an active banner grabbing attack, as described at *www.packetwatch.net*:

- **Test 1:** A TCP packet with the SYN and ECN-Echo flags enabled is sent to an open TCP port.
- **Test 2:** A TCP packet with no flags enabled is sent to an open TCP port. This type of packet is a NULL packet.
- **Test 3:** A TCP packet with the URG, PSH, SYN, and FIN flags enabled is sent to an open TCP port.
- **Test 4:** A TCP packet with the ACK flag enabled is sent to an open TCP port.
- **Test 5:** A TCP packet with the SYN flag enabled is sent to a closed TCP port.
- **Test 6:** A TCP packet with the ACK flag enabled is sent to a closed TCP port.
- **Test 7:** A TCP packet with the URG, PSH, and FIN flags enabled is sent to a closed TCP port.
- **Test 8 PU (Port Unreachable):** A UDP packet is sent to a closed UDP port. The objective is to extract an "ICMP port unreachable" message from the target machine.
- **Test 9 TSeq (TCP Sequence ability test):** This test tries to determine the sequence generation patterns of the TCP initial sequence numbers (also known as TCP ISN sampling), the IP identification numbers (also known as IPID sampling), and the TCP timestamp numbers. It sends six TCP packets with the SYN flag enabled to an open TCP port.

The objective of these tests is to find patterns in the initial sequence of numbers that the TCP implementations chose while responding to a connection request. They can be categorized into groups, such as traditional 64K (many old UNIX boxes), random increments (newer versions of Solaris, IRIX, FreeBSD, Digital UNIX, Cray, and many others), or true random (Linux 2.0.*, OpenVMS, newer AIX, etc.). Windows boxes use a "time-dependent" model in which the ISN is incremented by a fixed amount for each occurrence.

- **Passive Banner Grabbing**

  Source: *https://www.symantec.com*

  Like active banner grabbing, passive banner grabbing also depends on the differential implementation of the stack and the various ways in which an OS responds to packets. However, instead of relying on scanning the target host, passive fingerprinting captures packets from the target host via sniffing to study telltale signs that can reveal an OS.

Passive banner grabbing includes:

- **Banner grabbing from error messages**: Error messages provide information, such as type of server, type of OS, and SSL tools used by the target remote system.
- **Sniffing the network traffic**: Capturing and analyzing packets from the target enables an attacker to determine the OS used by the remote system.
- **Banner grabbing from page extensions**: Looking for an extension in the URL may help in determining the application version. For example, .aspx => IIS server and Windows platform.

The four areas that typically determine the OS are given below:

- TTL (time to live) of the packets: What does the OS sets as the Time To Live on the outbound packet?
- Window Size: What is the Window size set by the OS?
- Whether the DF (Don't Fragment) bit is set: Does the OS set the DF bit?
- TOS (Type of Service): Does the OS set the TOS, and if so, what setting is it?

Passive fingerprinting is neither fully accurate nor limited to these four signatures. However, one can improve its accuracy by looking at several signatures and combining the information. The following is an analysis of a sniffed packet described by Lance Spitzner in his paper on passive fingerprinting (*https://www.symantec.com/connect/articles/passive-fingerprinting*):

```
04/20-21:41:48.129662 129.142.224.3:659 -> 172.16.1.107:604
TCP TTL:45 TOS:0x0 ID:56257
***F**A* Seq: 0x9DD90553
Ack: 0xE3C65D7 Win: 0x7D78
```

According to the four criteria, the following are identified:

- TTL: 45
- Window Size: 0x7D78 (or 32120 in decimal)
- DF: The DF bit is set
- TOS: 0x0

Compare this information with a database of signatures.

TTL: The TLL from the analysis is 45. The original packet went through 19 hops to get to the target, so it sets the original TTL to 64. Based on this TTL, it appears that the user sent the packet from a Linux or FreeBSD box (however, more system signatures need to be added to the database). This TTL confirms it by implementing a traceroute to the remote host. If the trace needs to be performed stealthily, the traceroute TTL (default 30 hops) can be set to one or two hops fewer than the remote host (-m option). Setting the

traceroute in this manner reveals the path information (including the upstream provider) without actually contacting the remote host.

Window Size: In this step, the window sizes are compared. The window size is another effective tool for determining precisely what window size is used and how often it is changed. In the previous signature, the window size is set at 0x7D78, which is the default window size used by Linux. In addition, FreeBSD and Solaris tend to maintain the same window size throughout a session. However, Cisco routers and Microsoft Windows NT window sizes constantly change. The window size is more accurate when measured after the initial three-way handshake (due to TCP slow start).

DF bit: Most systems use the DF bit set; hence, this is of limited value. However, this makes it easier to identify a few systems that do not use the DF flag (such as SCO or OpenBSD).

TOS: TOS is also of limited value, as it seems to be more session-based than OS-based. In other words, it is not so much the OS as the protocol used that determines the TOS to a large extent.

Using the information obtained from the packet, specifically the TTL and the window size, one can compare the results with the database of signatures and determine the OS with some degree of confidence (in this case, Linux kernel 2.2.x).

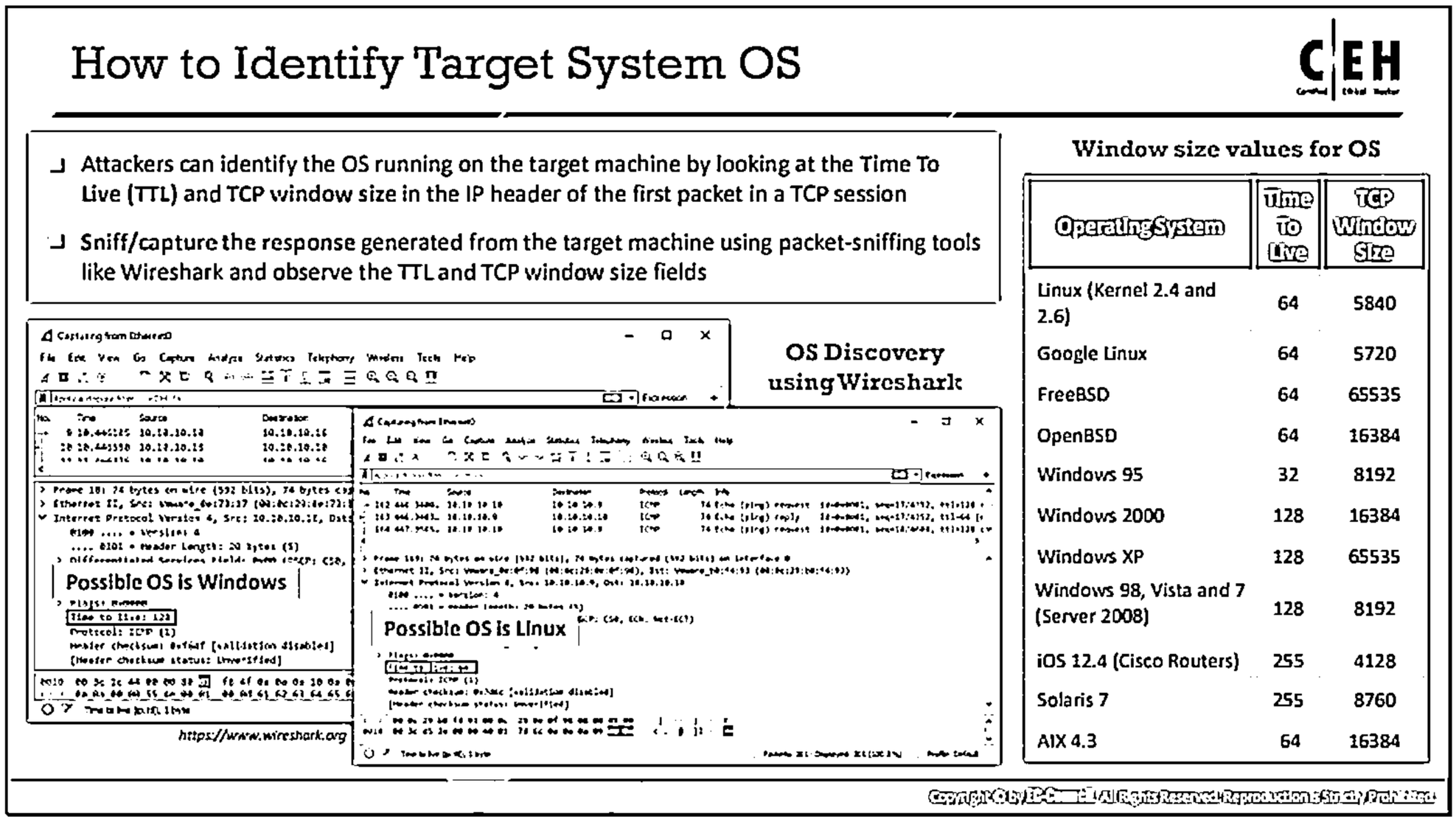
Passive fingerprinting, like active fingerprinting, has some limitations. First, applications that build their own packets (e.g., Nmap, Hunt, Nemesis, etc.) will not use the same signatures as the OS. Second, it is relatively simple for a remote host to adjust the TTL, window size, DF, or TOS setting on the packets.

Passive fingerprinting has several other uses. For example, attackers can use stealthy fingerprinting to determine the OS of a potential target such as a web server. A user only needs to request a web page from the server and then analyze the sniffer traces. This bypasses the need for using an active tool that various IDS systems can detect. Passive fingerprinting also helps in identifying remote proxy firewalls. It may be possible to ID proxy firewalls from the signatures as discussed above, simply because proxy firewalls rebuild connections for clients. Similarly, passive fingerprinting can be used to identify rogue systems.

Note: We will discuss passive banner grabbing in later modules.

Why Banner Grabbing?

An attacker uses banner grabbing to identify the OS used on the target host and thus determine the system vulnerabilities and exploits that might work on that system to carry out further attacks.



How to Identify Target System OS

Identifying the target OS is one of the important tasks for an attacker to compromise the target network/machine. In a network, various standards are implemented to allow different OSs to communicate with each other. These standards govern the functioning of various protocols such as IP, TCP, UDP, etc. By analyzing certain parameters/fields in these protocols, one can reveal the details of the OS. Parameters such as Time to Live (TTL) and TCP window size in the IP header of the first packet in a TCP session help identify the OS running on the target machine. The TTL field determines the maximum time that a packet can remain in a network, and the TCP window size determines the length of the packet reported. These values vary among OSs, as described in the following table:

Operating System	Time To Live	TCP Window Size
Linux (Kernel 2.4 and 2.6)	64	5840
Google Linux	64	5720
FreeBSD	64	65535
OpenBSD	64	16384
Windows 95	32	8192
Windows 2000	128	16384
Windows XP	128	65535
Windows 98, Vista, and 7 (Server 2008)	128	8192
iOS 12.4 (Cisco Routers)	255	4128

Solaris 7	255	8760
AIX 4.3	64	16384

Table 3.3: TTL and TCP Window size values for OS

Attackers can use various tools to perform OS discovery on the target machine, including Wireshark, Nmap, Unicornscan, and Nmap Script Engine. Attackers can also adopt the IPv6 fingerprinting method to grab the target OS details.

OS Discovery using Wireshark

Source: *https://www.wireshark.org*

To identify the target OS, sniff/capture the response generated from the target machine to the request-originated machine using packet-sniffing tools such as Wireshark, etc., and observe the TTL and TCP window size fields in the first captured TCP packet. By comparing these values with those in the above table, you can determine the target OS that has generated the response.

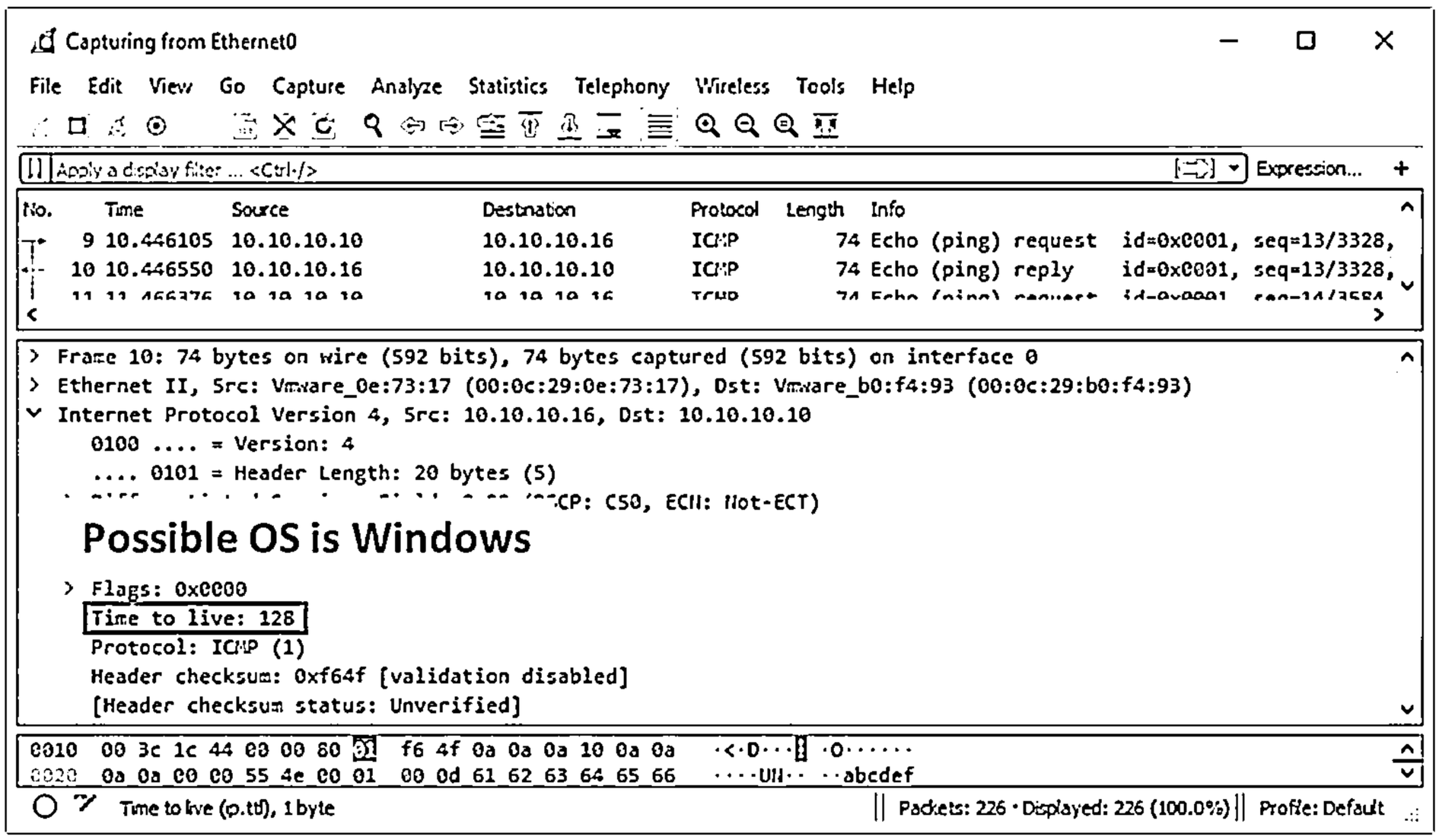


Figure 3.77: Wireshark screenshot showing TTL value (Possible OS is Windows)

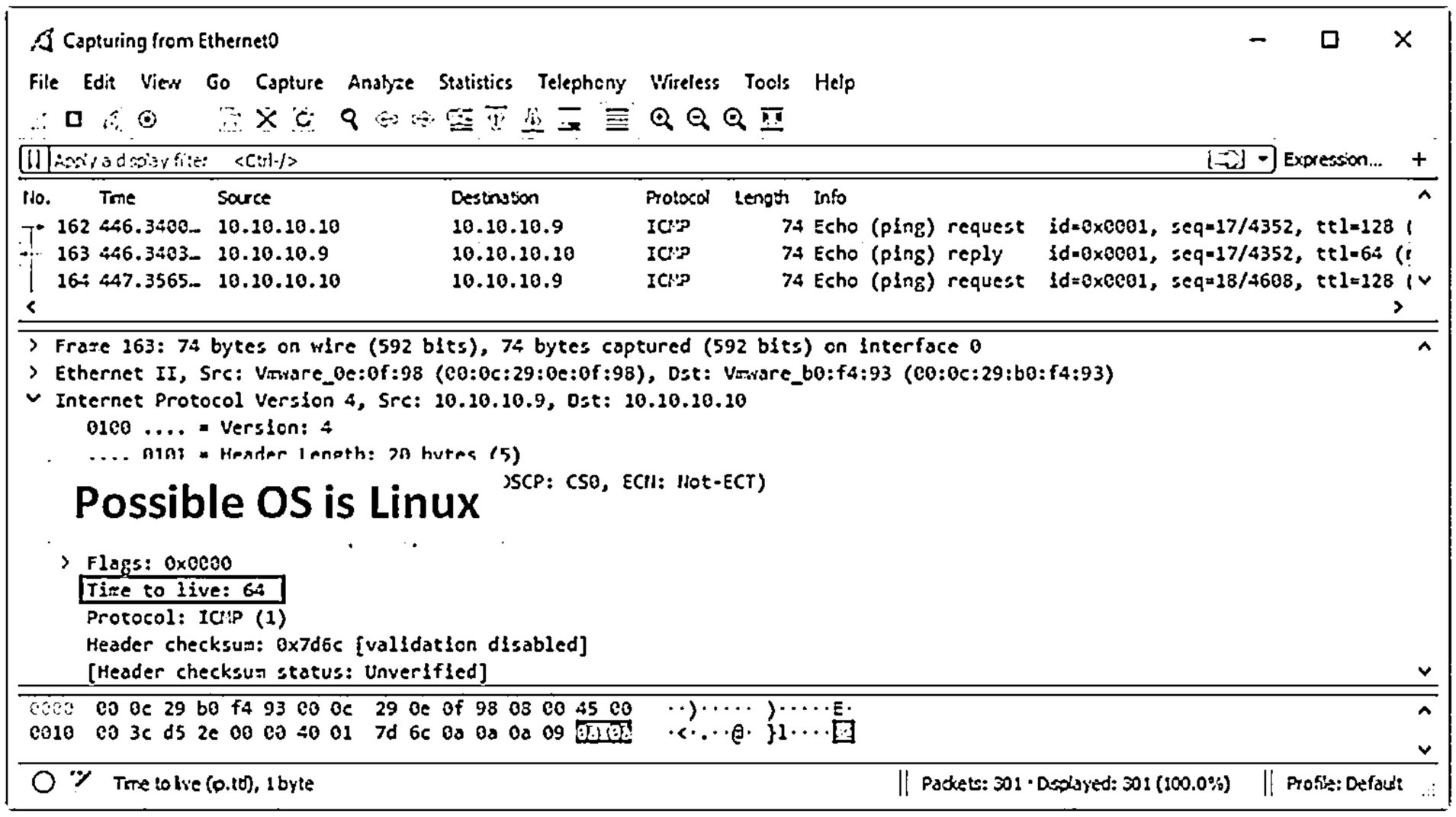
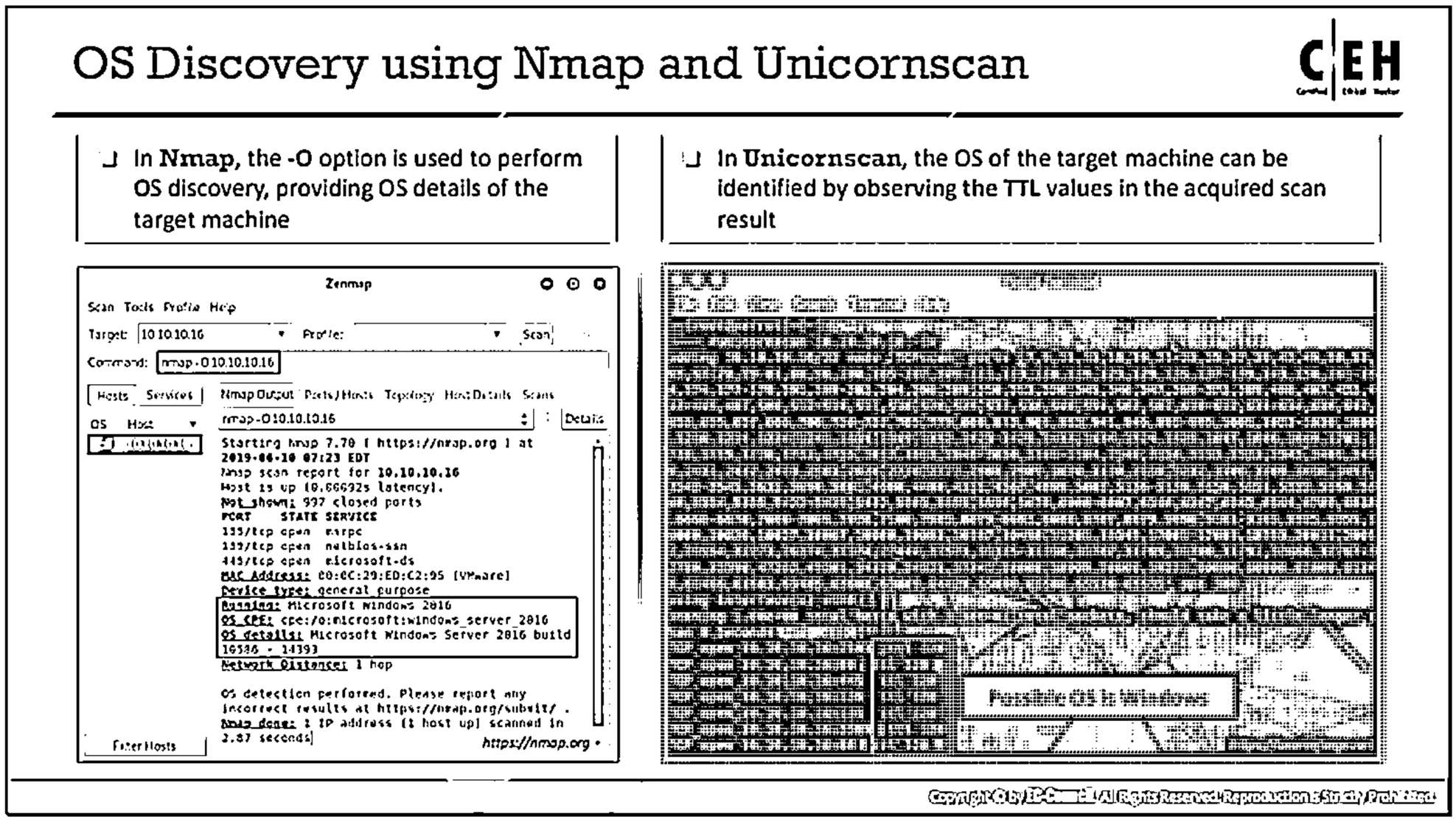


Figure 3.78: Wireshark screenshot showing TTL value (Possible OS is Linux)



OS Discovery using Nmap and Unicornscan

OS Discovery using Nmap

Source: *https://nmap.org*

To exploit the target, it is highly essential to identify the OS running on the target machine. Attackers can employ various tools to acquire the OS details of the target. Nmap is one of the effective tools for performing OS discovery activities. In Zenmap, the –o option is used to perform OS discovery, which displays the OS details of the target machine.

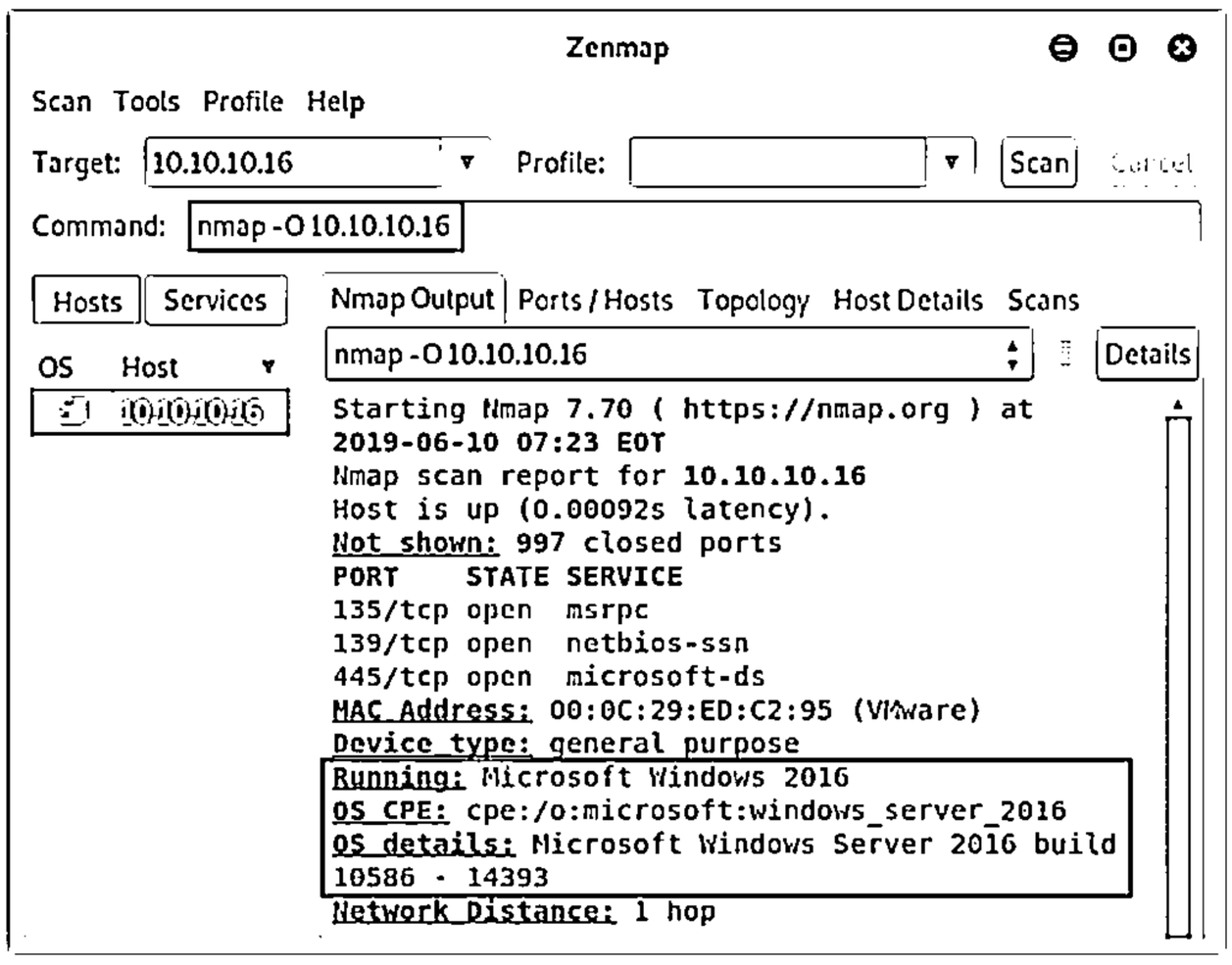


Figure 3.79: OS Discovery using Zenmap

OS Discovery using Unicornscan

Source: *https://sourceforge.net*

In Unicornscan, the OS of the target machine can be identified by observing the TTL values in the acquired scan result. To perform Unicornscan, the syntax `#unicornscan <target IP address>` is used. As shown in the screenshot, the `ttl` value acquired after the scan is `128`; hence, the OS is possibly Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16).

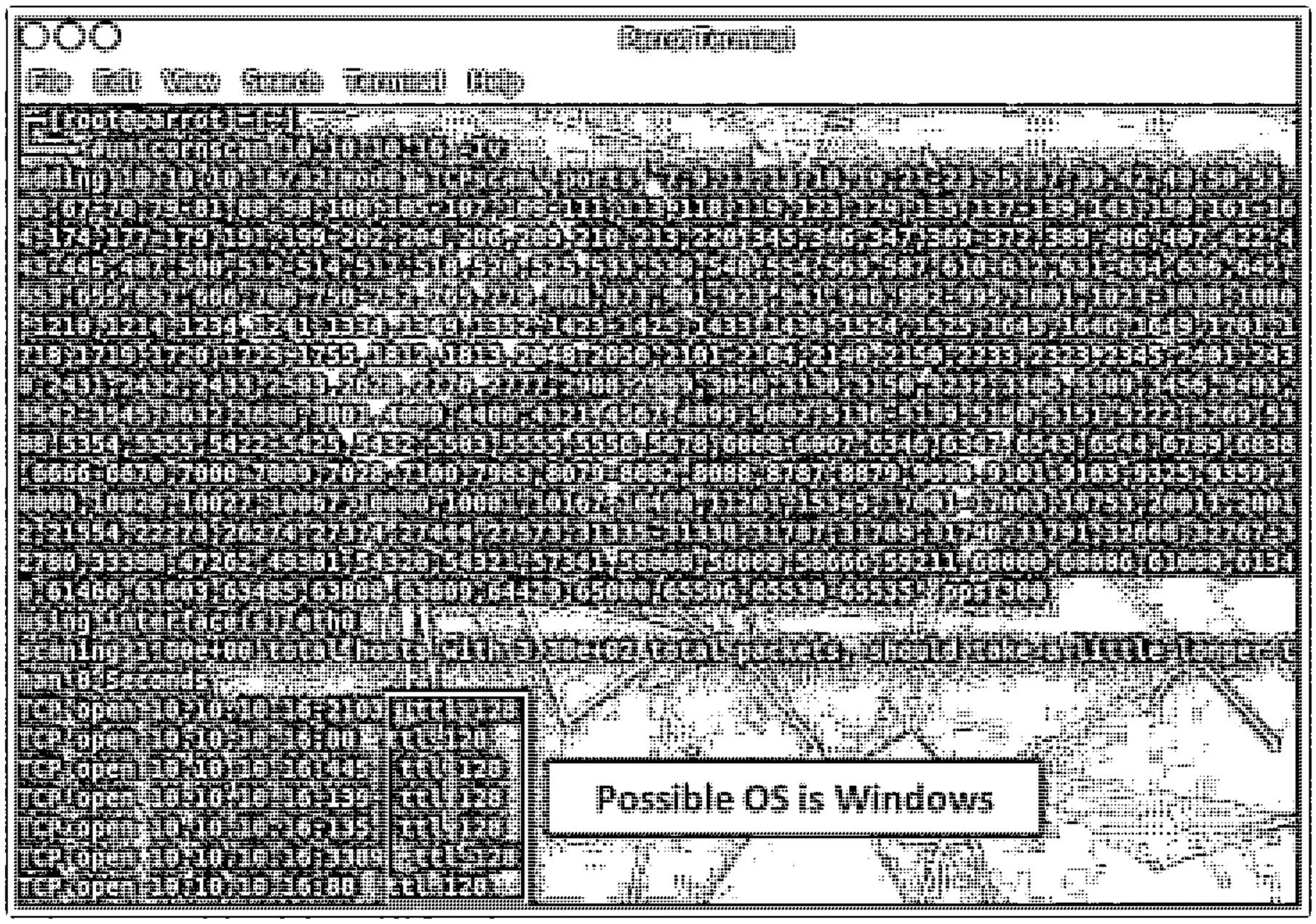
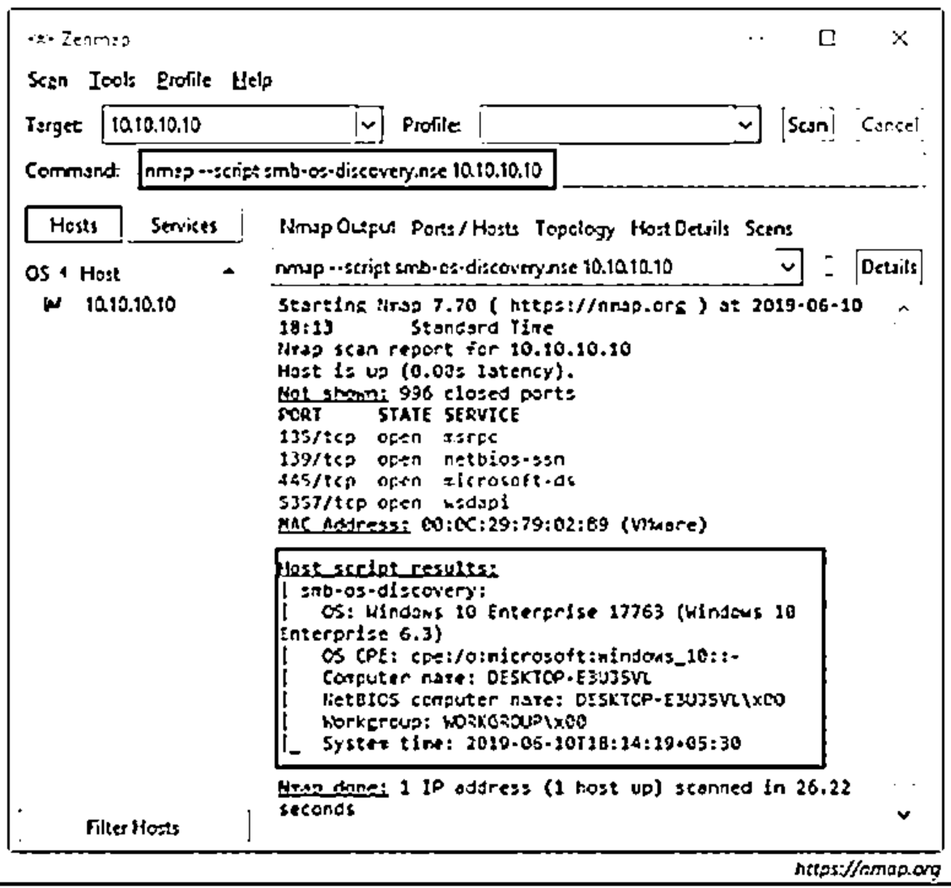


Figure 3.80: OS Discovery using Unicornscan

OS Discovery using Nmap Script Engine

- Nmap script engine (NSE) can be used to automate a wide variety of networking tasks by allowing the users to write and share scripts
- Attackers use various scripts in the Nmap Script Engine to perform OS discovery on the target machine
- For example, in Nmap, smb-os-discovery is an inbuilt script that can be used for collecting OS information on the target machine through the SMB protocol
- In Zenmap, the -sC option or –script option is used to activate the NSE scripts



OS Discovery using Nmap Script Engine

Source: *https://nmap.org*

Nmap Scripting Engine (NSE) in Nmap can be used to automate a wide variety of networking tasks by allowing users to write and share scripts. These scripts can be executed parallelly with the same efficiency and speed as Nmap. Attackers can also use various scripts in the Nmap Script Engine for performing OS discovery on the target machine. For example, in Nmap, `smb-os-discovery` is an inbuilt script used for collecting OS information on the target machine through the SMB protocol.

In Zenmap, NSE can be generally activated using the `-sC` option. If the custom scripts are to be specified, then attackers can use the `--script` option. The NSE results will be displayed with both the Nmap normal and XML outputs.

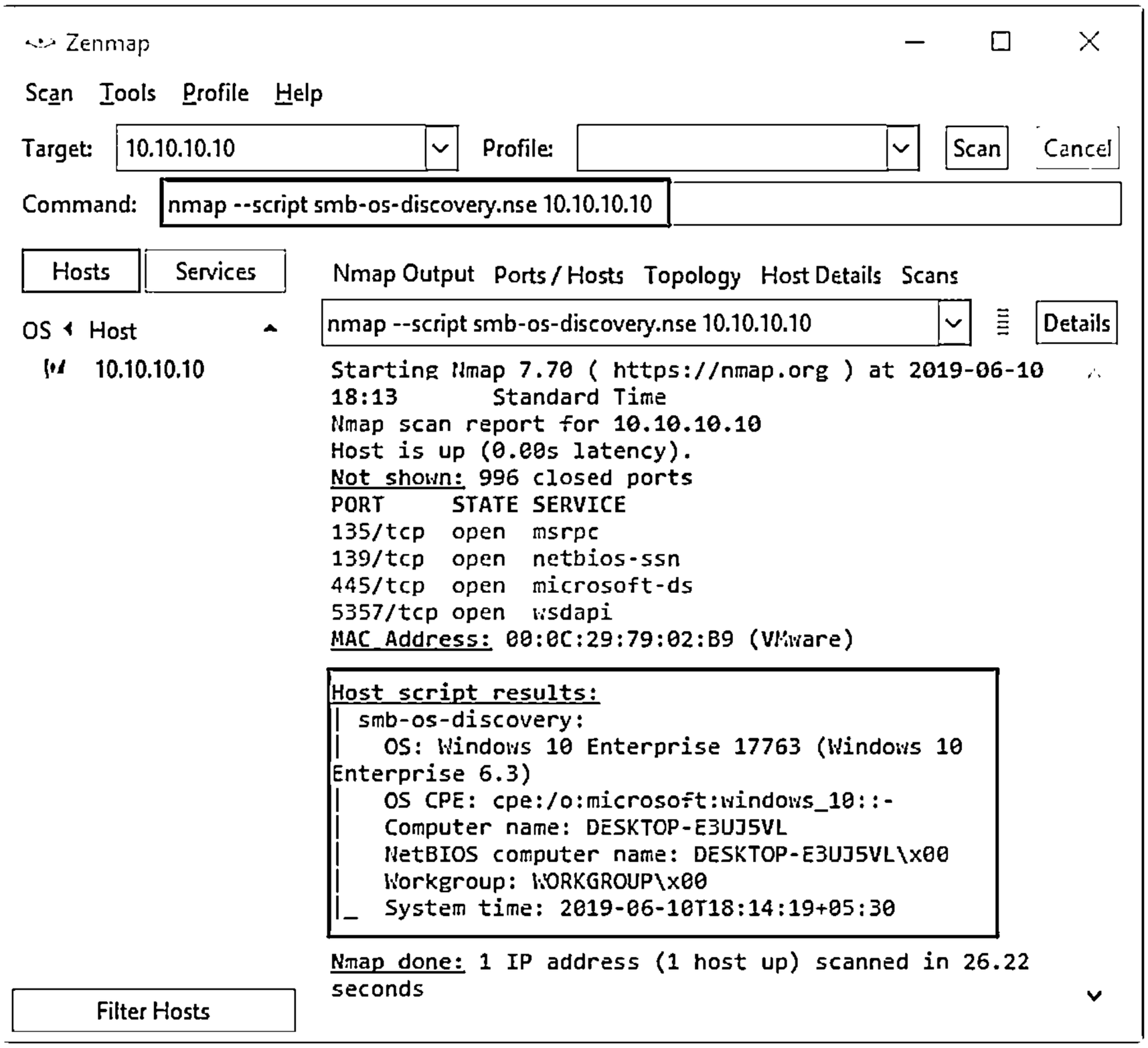
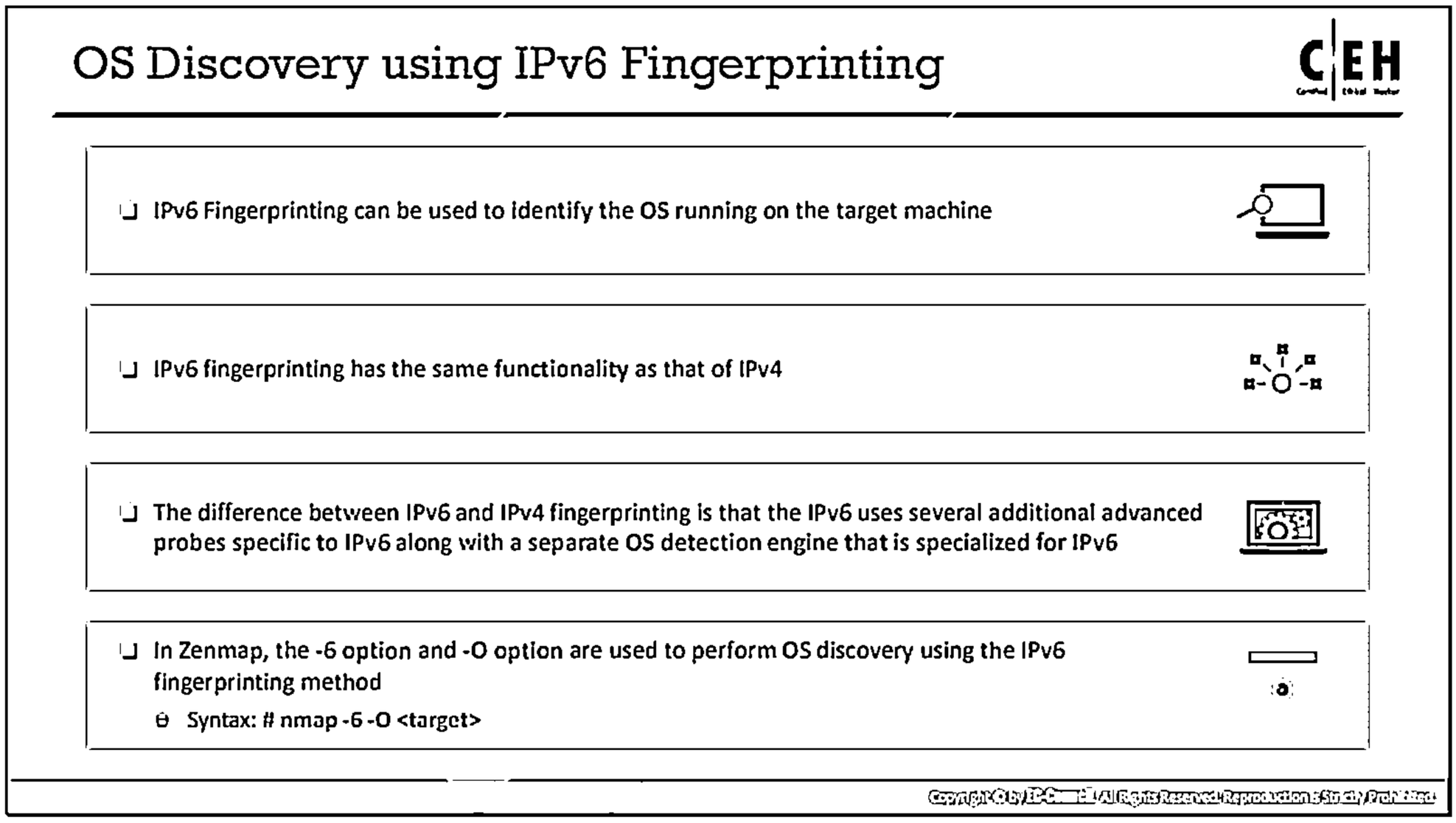


Figure 3.81: OS Discovery using Nmap Script Engine



OS Discovery using IPv6 Fingerprinting

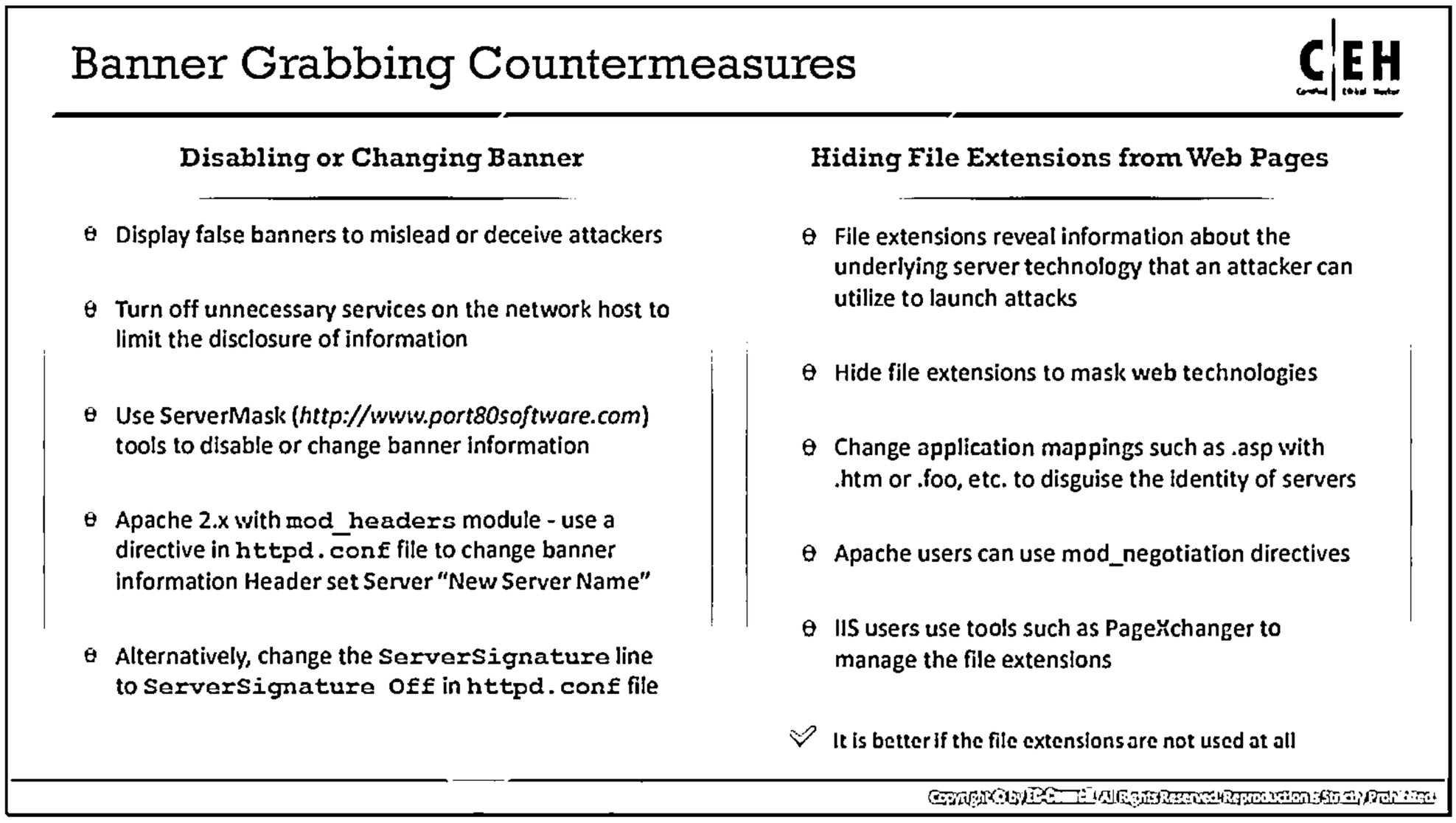
Source: *https://nmap.org*

IPv6 Fingerprinting is another technique used to identify the OS running on the target machine. It has the same functionality as IPv4, such as sending probes, waiting and collecting the responses, and matching them with the database of fingerprints. The difference between IPv6 and IPv4 fingerprinting is that IPv6 uses several additional advanced IPv6-specific probes along with a separate IPv6-specifc OS detection engine. Nmap sends nearly 18 probes in the following order to identify the target OS using the IPv6 fingerprinting method.

- Sequence generation (S1–S6)
- ICMPv6 echo (IE1)
- ICMPv6 echo (IE2)
- Node Information Query (NI)
- Neighbor Solicitation (NS)
- UDP (U1)
- TCP explicit congestion notification (TECN)
- TCP (T2–T7)

In Zenmap, the `-6` option along with `-O` option is used to perform OS discovery using the IPv6 fingerprinting method.

Syntax: `# nmap -6 -O <target>`



Banner Grabbing Countermeasures

- **Disabling or Changing Banner**

  Whenever a port is open, it implies that a service/banner is running on it. When attackers connect to the open port using banner grabbing techniques, the system presents a banner containing sensitive information such as OS, server type, and version. Using the information gathered, the attacker identifies specific vulnerabilities to exploit and then launches attacks. The countermeasures against banner grabbing attacks are as follows:

  - Display false banners to mislead or deceive attackers.
  - Turn off unnecessary services on the network host to limit information disclosure.
  - Use ServerMask (*https://www.port80software.com*) tools to disable or change banner information.
  - ServerMask removes unnecessary HTTP header and response data and camouflages the server by providing false signatures. It also provides you with the option of eliminating file extensions such as `.asp` or `.aspx`, and it clearly indicates that a site is running on a Microsoft server.
  - Apache 2.x with `mod_headers` module: use a directive in the `httpd.conf` file to change the banner information header and set the server as "`New Server Name`".
  - Alternatively, change the `ServerSignature` line to `ServerSignatureOff` in the `httpd.conf` file.
  - The details of the vendor and version in the banners should be disabled.

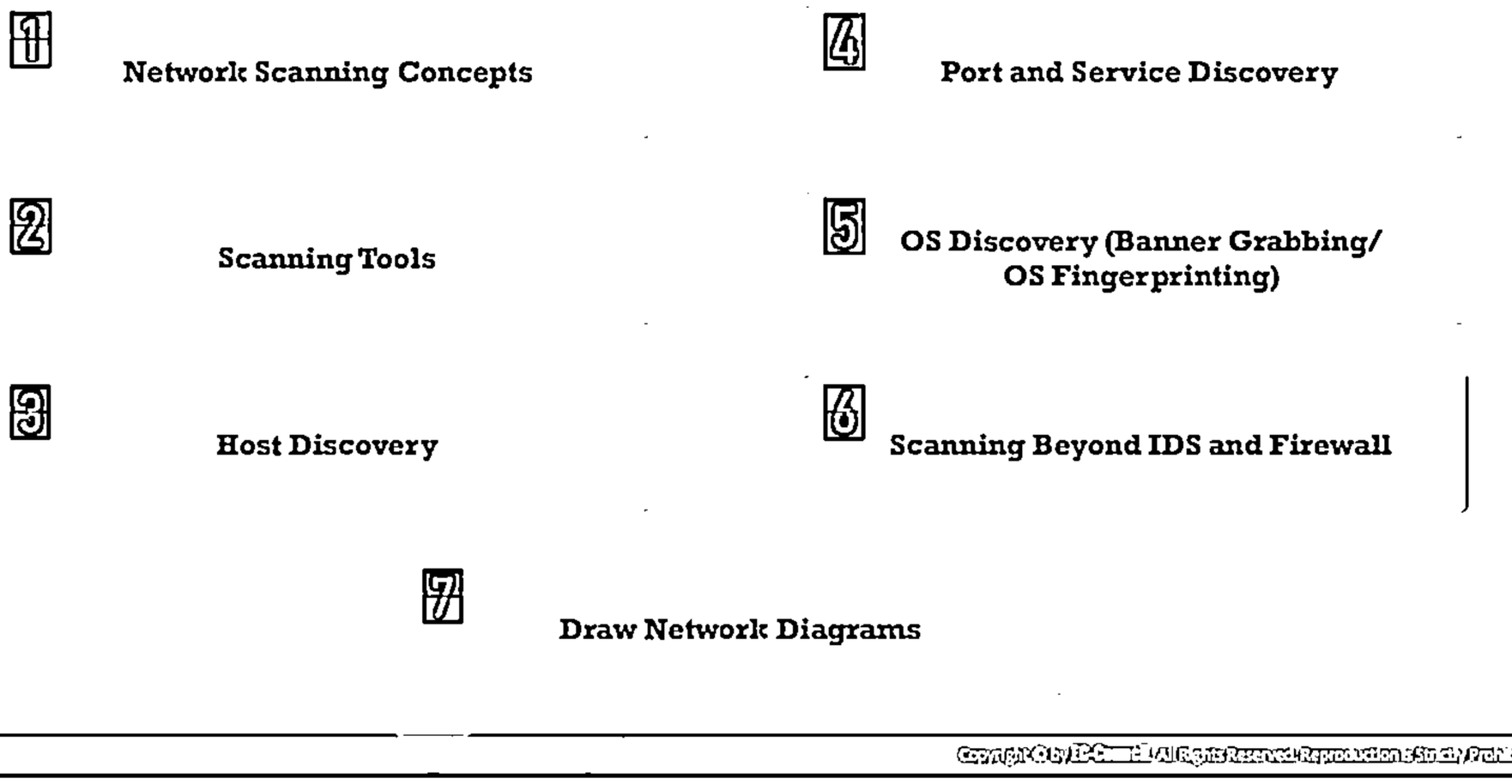
- **Hiding File Extensions from Web Pages**

  File extensions reveal information about the underlying server technology that an attacker can use to launch attacks. The countermeasures against such banner grabbing attacks are as follows:

  - Hide file extensions to mask the web technology.
  - Replace application mappings such as .asp with .htm or .foo, etc., to disguise the identity of the servers.
  - Apache users can use `mod_negotiation` directives.
  - IIS users can use tools such as PageXchanger to manage the file extensions.

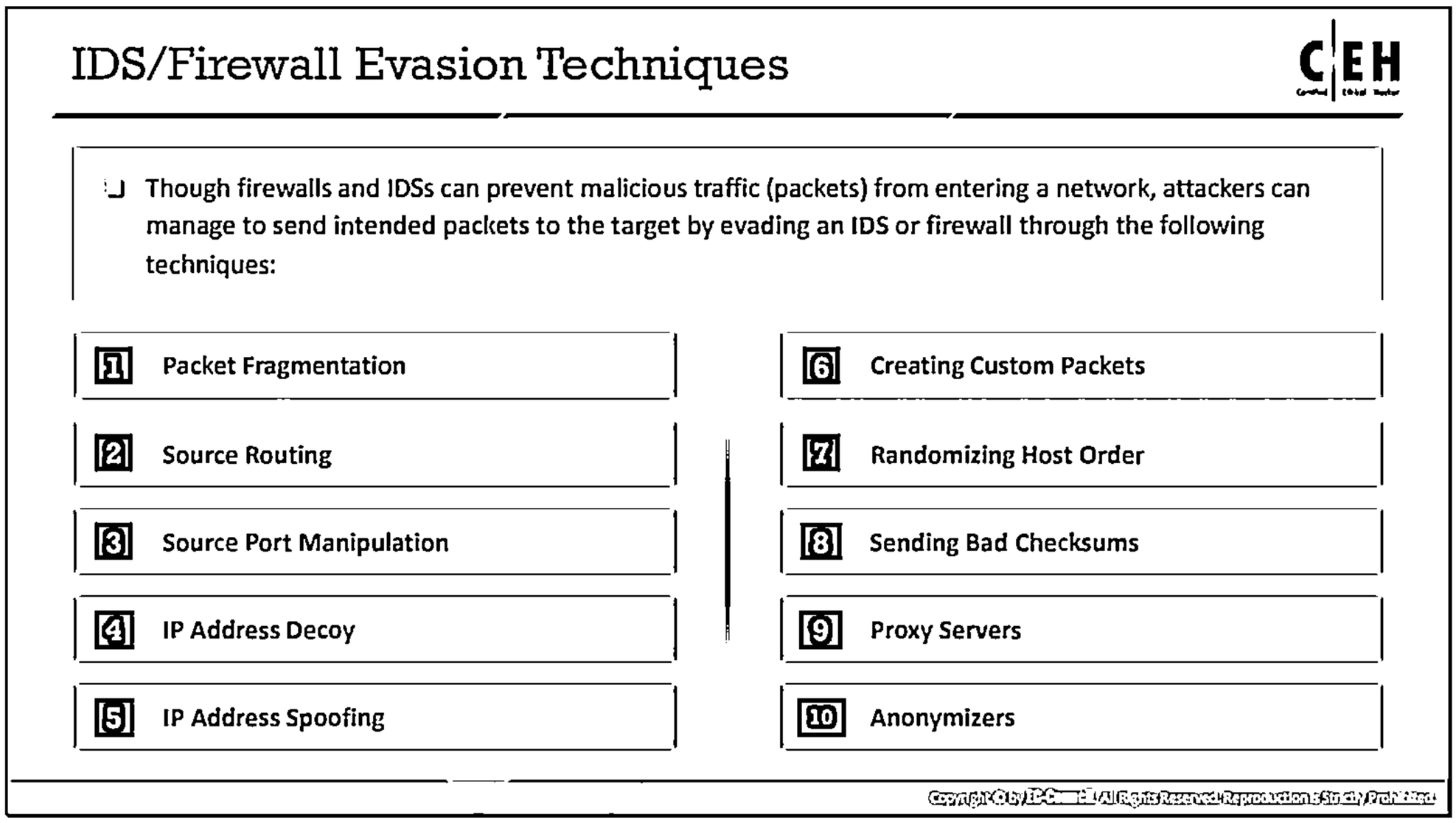
Note: It would be better if the file extensions are not used at all.

Module Flow



Scanning Beyond IDS and Firewall

Intrusion detection systems (IDS) and firewalls are security mechanisms intended to prevent an attacker from accessing a network. However, even IDS and firewalls have some security limitations. Attackers try to launch attacks to exploit these limitations. This section highlights various IDS/firewall evasion techniques such as packet fragmentation, source routing, IP address spoofing, etc.

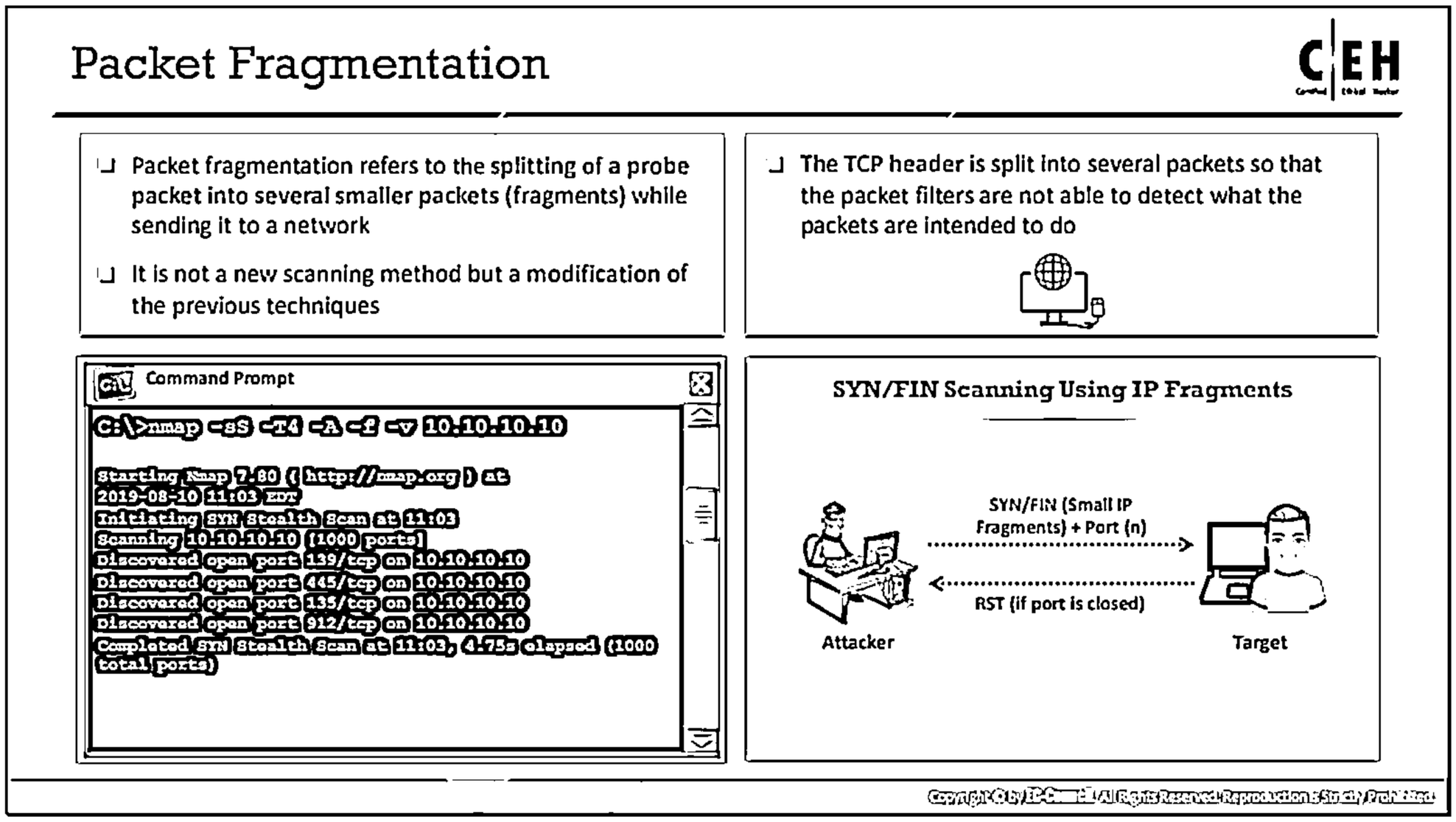


IDS/Firewall Evasion Techniques

Although firewalls and IDS can prevent malicious traffic (packets) from entering a network, attackers can send intended packets to the target that evade the IDS/firewall by implementing the following techniques:

- **Packet Fragmentation**: The attacker sends fragmented probe packets to the intended target, which reassembles the fragments after receiving all of them.
- **Source Routing**: The attacker specifies the routing path for the malformed packet to reach the intended target.
- **Source Port Manipulation**: The attacker manipulates the actual source port with the common source port to evade the IDS/firewall.
- **IP Address Decoy**: The attacker generates or manually specifies IP addresses of decoys so that the IDS/firewall cannot determine the actual IP address.
- **IP Address Spoofing**: The attacker changes the source IP addresses so that the attack appears to be coming from someone else.
- **Creating Custom Packets**: The attacker sends custom packets to scan the intended target beyond the firewalls.
- **Randomizing Host Order**: The attacker scans the number of hosts in the target network in a random order to scan the intended target that lies beyond the firewall.
- **Sending Bad Checksums**: The attacker sends packets with bad or bogus TCP/UPD checksums to the intended target.

- **Proxy Servers:** The attacker uses a chain of proxy servers to hide the actual source of a scan and evade certain IDS/firewall restrictions.
- **Anonymizers:** The attacker uses anonymizers, which allows them to bypass Internet censors and evade certain IDS and firewall rules.



Packet Fragmentation

Packet fragmentation refers to the splitting of a probe packet into several smaller packets (fragments) while sending it to a network. When these packets reach a host, the IDS and firewalls behind the host generally queue all of them and process them one by one. However, since this method of processing involves greater CPU and network resource consumption, the configuration of most IDS cause them to skip fragmented packets during port scans.

Therefore, attackers use packet fragmentation tools such as Nmap and fragroute to split the probe packet into smaller packets that circumvent the port-scanning techniques employed by IDS. Once these fragments reach the destined host, they are reassembled to form a single packet.

SYN/FIN Scanning Using IP Fragments

SYN/FIN scanning using IP fragments is not a new scanning method but a modification of previous techniques. This process of scanning was developed to avoid false positives generated by other scans because of a packet filtering device on the target system. The TCP header splits into several packets to evade the packet filter. For any transmission, every TCP header must have the source and destination port for the initial packet (8-octet, 64-bit). The initialized flags in the next packet allow the remote host to reassemble the packets upon receipt via an Internet protocol module that detects the fragmented data packets using field-equivalent values of the source, destination, protocol, and identification.

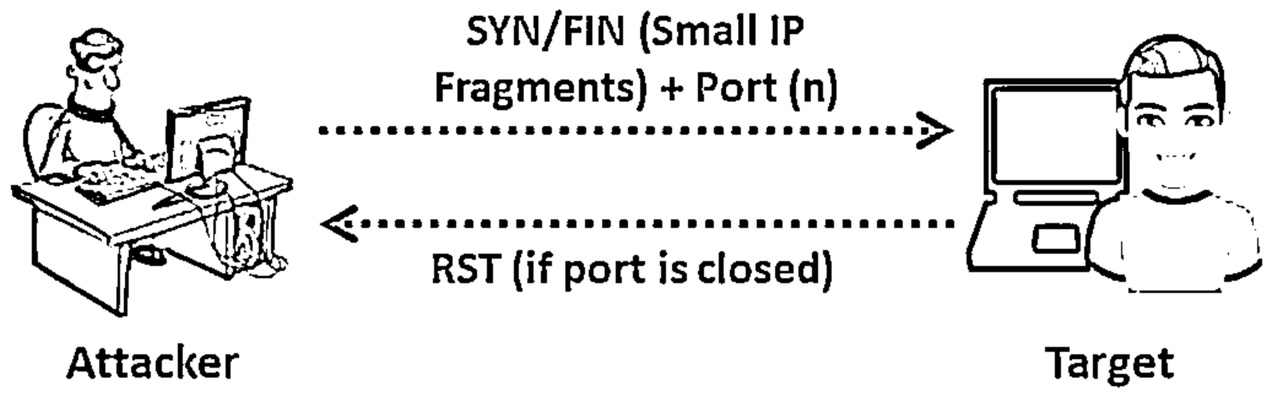


Figure 3.82: SYN/FIN scanning

In this scan, the system splits the TCP header into several fragments and transmits them over the network. However, IP reassembly on the server side may result in unpredictable and abnormal results, such as fragmentation of the IP header data. Some hosts may fail to parse and reassemble the fragmented packets, which may lead to crashes, reboots, or even network device monitoring dumps.

Some firewalls might have rule sets that block IP fragmentation queues in the kernel (e.g., CONFIG_IP_ALWAYS_DEFRAG option in the Linux kernel), although this is not widely implemented because of its adverse effects on performance. Since many IDS use signature-based methods to indicate scanning attempts on IP and/or TCP headers, the use of fragmentation will often evade this type of packet filtering and detection, resulting in a high probability of causing problems on the target network. Attackers use the SYN/FIN scanning method with IP fragmentation to evade this type of filtering and detection.

The screenshot below shows the SYN/FIN scan using the Nmap tool.

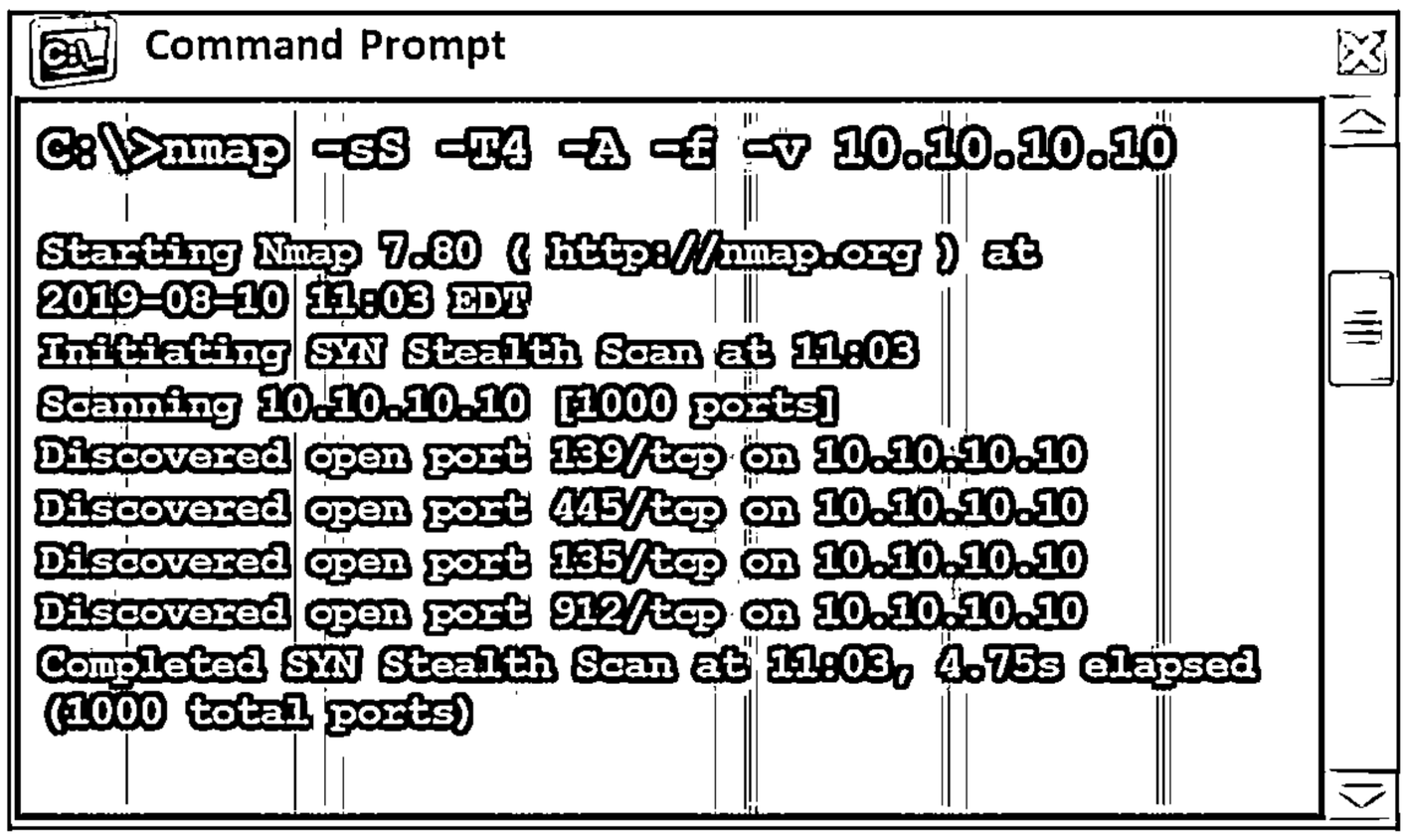
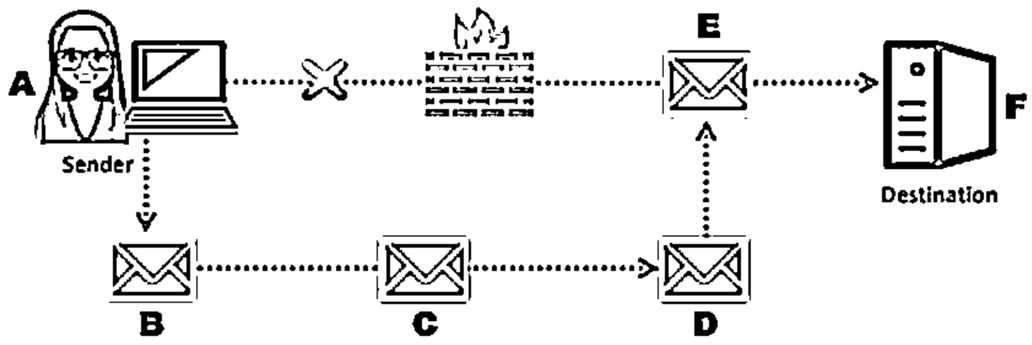


Figure 3.83: SYN/FIN scan using Nmap

Source Routing

- As the packet travels through the nodes in the network, each router examines the destination IP address and chooses the next hop to direct the packet to the destination
- Source routing refers to sending a packet to the intended destination with a partially or completely specified route (without firewall-/IDS-configured routers) in order to evade an IDS or firewall
- In source routing, the attacker makes some or all of these decisions on the router

This figure shows source routing, where the originator dictates the eventual route of the traffic



Source Routing

An IP datagram contains various fields, including the IP options field, which stores source routing information and includes a list of IP addresses through which the packet travels to its destination. As the packet travels through the nodes in the network, each router examines the destination IP address and chooses the next hop to direct the packet to the destination.

When attackers send malformed packets to a target, these packets hop through various routers and gateways to reach the destination. In some cases, the routers in the path might include configured firewalls and IDS that block such packets. To avoid them, attackers enforce a loose or strict source routing mechanism, in which they manipulate the IP address path in the IP options field so that the packet takes the attacker-defined path (without firewall-/IDS-configured routers) to reach the destination, thereby evading firewalls and IDS.

The figure below shows source routing, where the originator dictates the eventual route of the traffic.

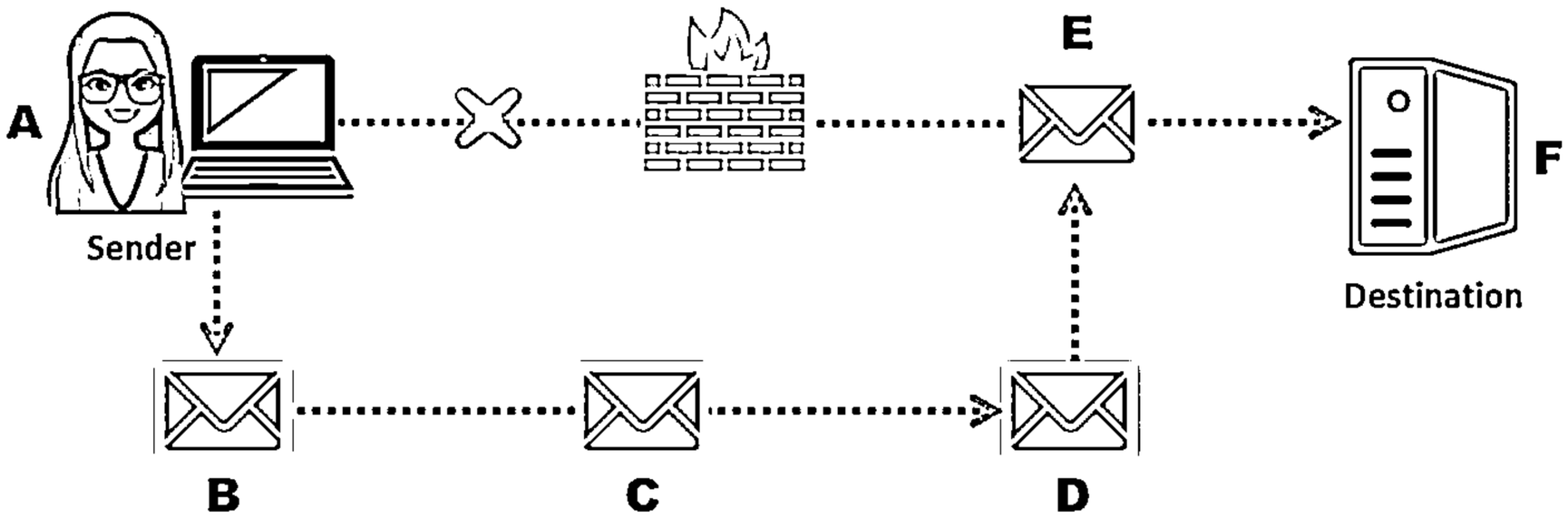
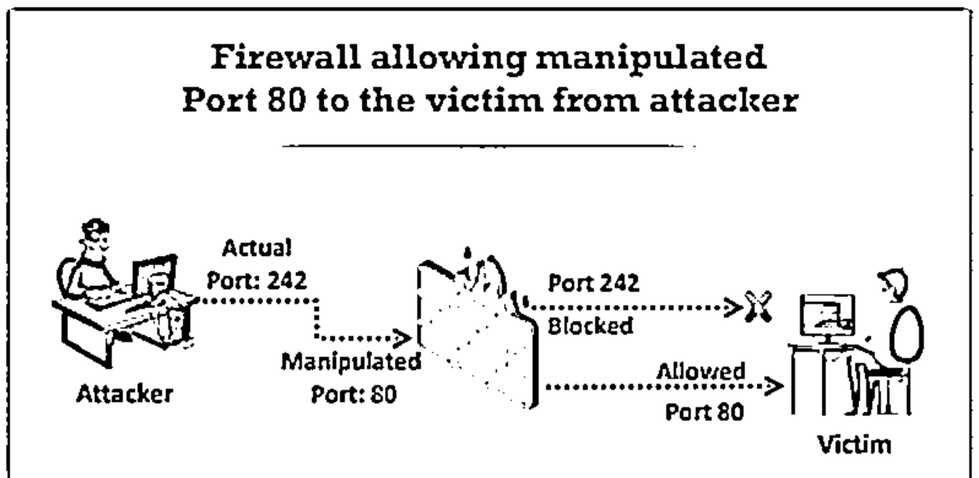
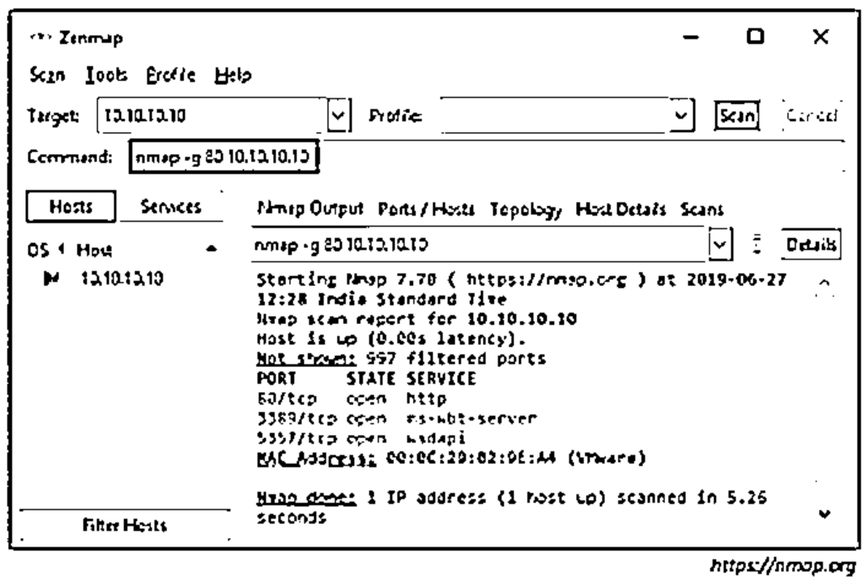


Figure 3.84: Source Routing

Source Port Manipulation

- Source port manipulation refers to manipulating actual port numbers with common port numbers in order to evade an IDS or firewall
- It occurs when a firewall is configured to allow packets from well-known ports like HTTP, DNS, FTP, etc.
- Nmap uses the -g or --source-port options to perform source port manipulation





Source Port Manipulation

Source port manipulation is a technique used for bypassing the IDS/firewall, where the actual port numbers are manipulated with common port numbers for evading certain IDS and firewall rules. The main security misconfigurations occur because of blindly trusting the source port number. The administrator mostly configures the firewall by allowing the incoming traffic from well-known ports such as HTTP, DNS, FTP, etc. The firewall can simply allow the incoming traffic from the packets sent by the attackers using such common ports.

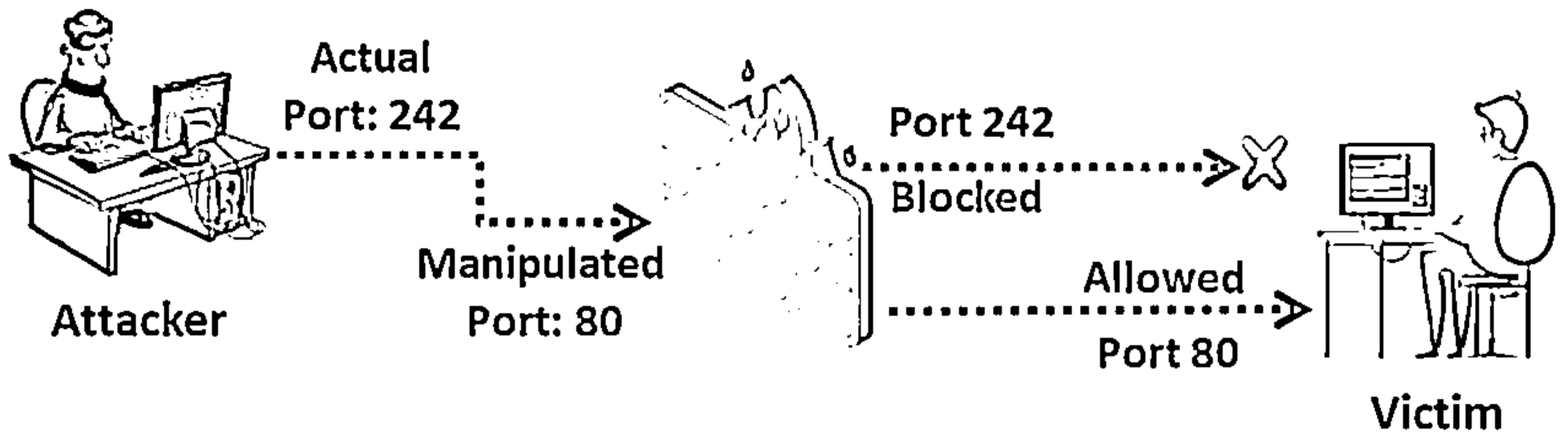


Figure 3.85: Firewall allowing manipulated port 80 to the victim from attacker

Although the firewalls can be made secure using application-level proxies or protocol-parsing firewall elements, this technique helps the attacker to bypass the firewall rules easily. The attacker tries to manipulate the original port number with the common port numbers, which can easily bypass the IDS/firewall. In Zenmap, the `-g` or `--source-port` option is used to perform source port manipulation.

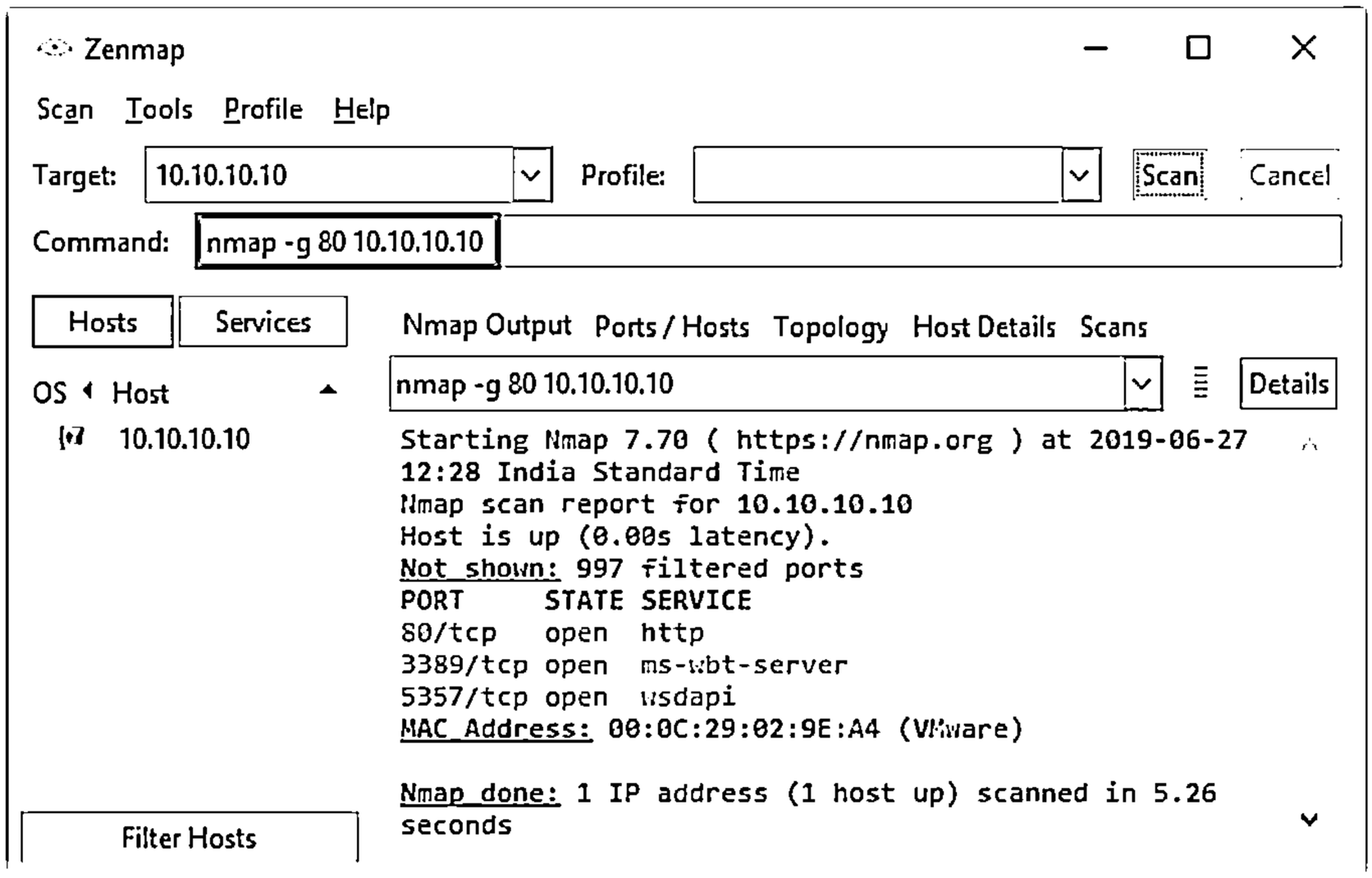


Figure 3.86: Scanning over Firewall using Nmap

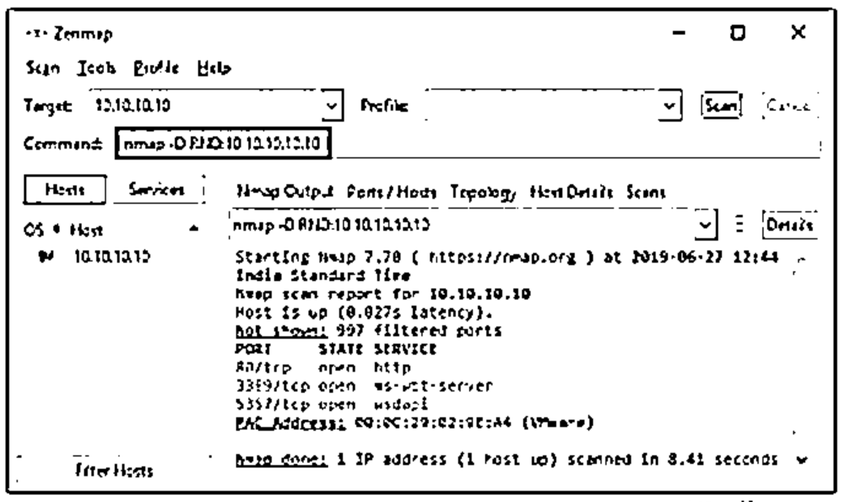
IP Address Decoy

- IP address decoy technique refers to generating or manually specifying the IP addresses of decoys in order to evade an IDS or firewall
- It appears to the target that the decoys as well as the host(s) are scanning the network
- This technique makes it difficult for the IDS or firewall to determine which IP address was actually scanning the network and which IP addresses were decoys

Decoy Scanning using Nmap

Nmap has two options for decoy scanning:

- `nmap -D RND:10 [target]`
  (Generates a random number of decoys)
- `nmap -D decoy1,decoy2,decoy3,.. etc.`
  (Manually specify the IP addresses of the decoys)



IP Address Decoy

The IP address decoy technique refers to generating or manually specifying IP addresses of the decoys to evade IDS/firewalls. It appears to the target that the decoys as well as the host(s) are scanning the network. This technique makes it difficult for the IDS/firewall to determine which IP address is actually scanning the network and which IP addresses are decoys.

The Nmap scanning tool comes with a built-in scan function called a decoy scan, which cloaks a scan with decoys. This technique generates multiple IP addresses to perform a scan, thus making it difficult for the target security mechanisms such as IDS, firewalls, etc., to identify the original source from the registered logs. The target IDS might report scanning from 5– 0 IP addresses; however, it cannot differentiate between the actual scanning IP address and the innocuous decoy IPs.

You can perform two types of decoy scans using Nmap:

- **nmap -D RND:10 [target]**

  Using this command, Nmap automatically generates a random number of decoys for the scan and randomly positions the real IP address between the decoy IPs.

  Ex. Assume that 10.10.10.10 is the target IP address to be scanned. Thus, the Nmap decoy scan command will be:

  ```
  # nmap -D RND:10 10.10.10.10
  ```

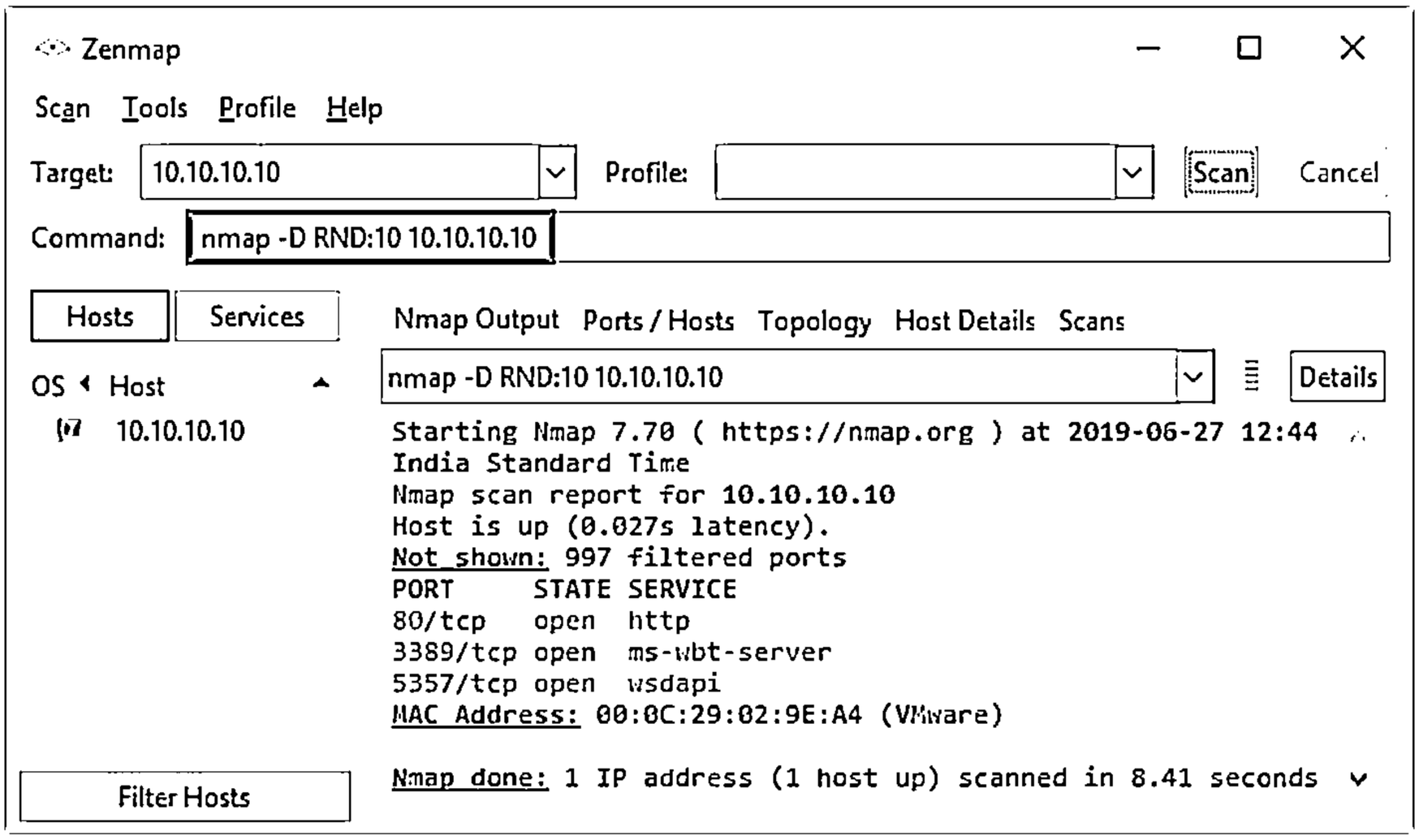


Figure 3.87: Decoy using Nmap RND option

- **nmap -D decoy1,decoy2,decoy3,...,ME,... [target]**

  Using this command, you can manually specify the IP addresses of the decoys to scan the victim's network. Here, you have to separate each decoy IP with a comma (,) and you can optionally use the ME command to position your real IP in the decoy list. If you place ME in the 4th position of the command, your real IP will be positioned at the 4th position accordingly. This is an optional command, and if you do not mention ME in your scan command, then Nmap will automatically place your real IP in any random position.

  For example, assume that 10.10.10.16 is the real source IP and 10.10.10.10 is the target IP address to be scanned. Then, the Nmap decoy command will be:

  Syntax:

```
# nmap -D 192.168.0.1,172.120.2.8,192.168.2.8,10.10.10.16,10.10.10.5
10.10.10.10
```

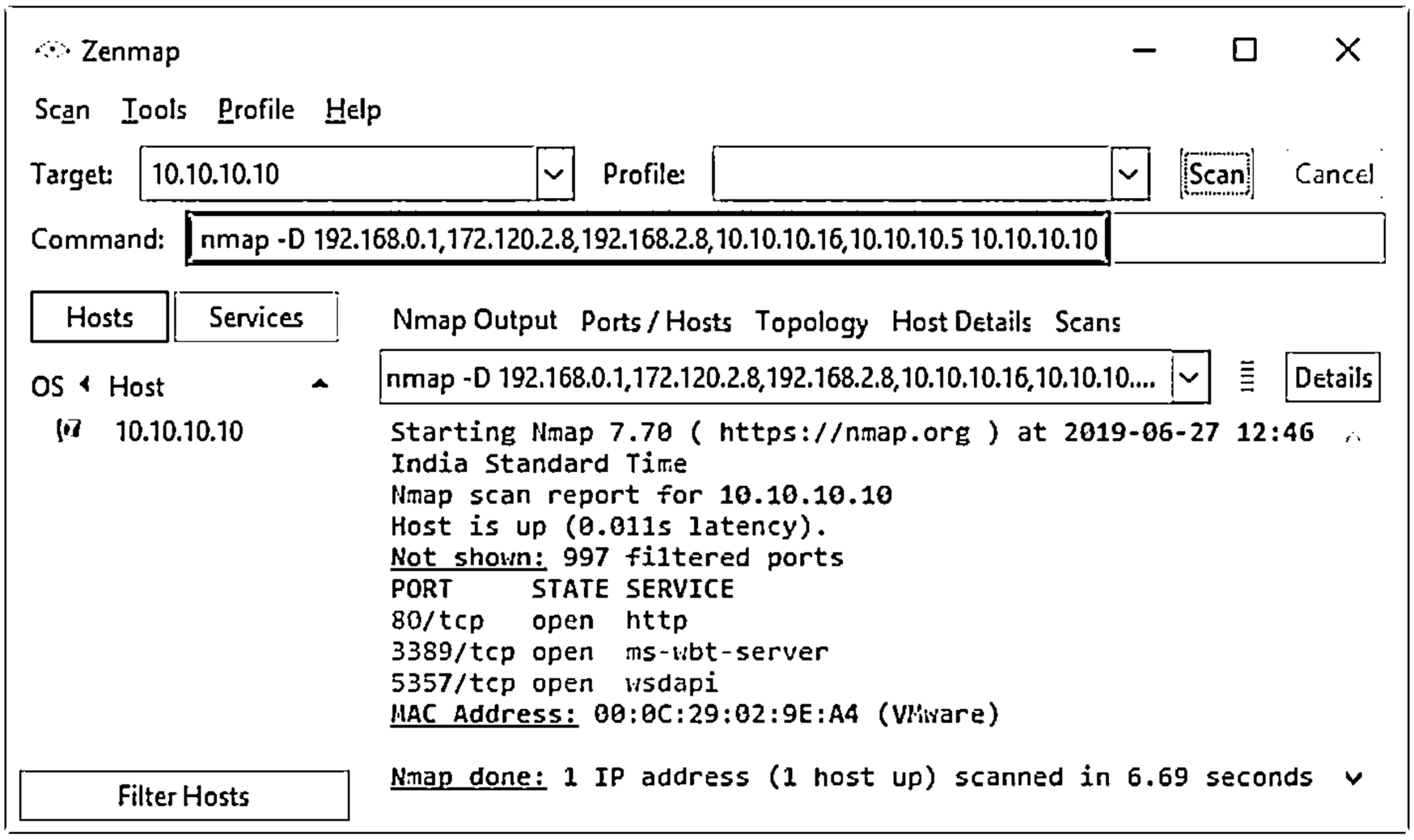
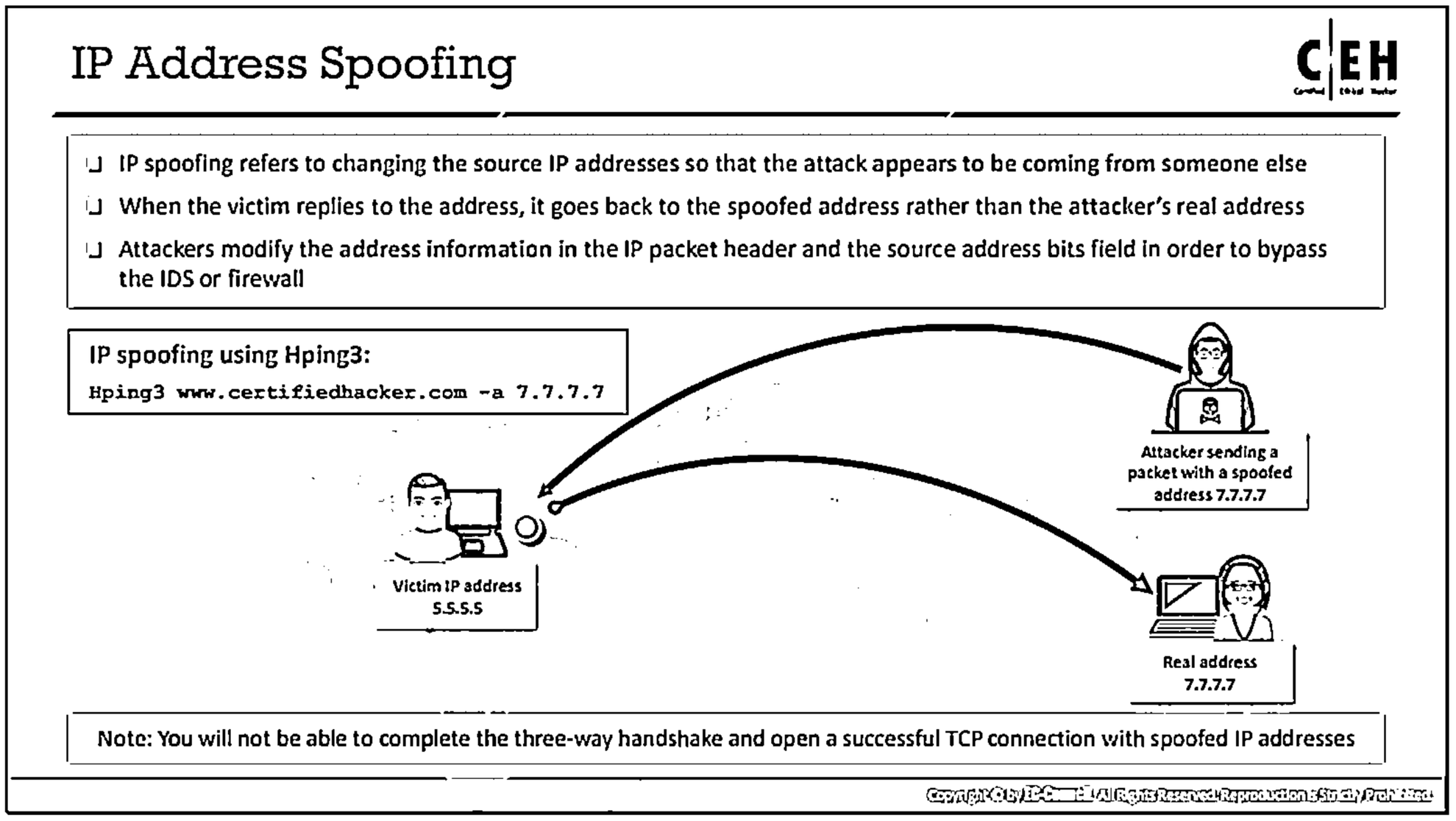


Figure 3.88: Decoy using Nmap with manual decoy list

These decoys can be generated in both initial ping scans such as ICMP, SYN, ACK, etc., and during the actual port scanning phase.

IP address decoy is a useful technique for hiding your IP address. However, it will not be successful if the target employs active mechanisms such as router path tracing, response dropping, etc. Moreover, using many decoys can slow down the scanning process and affect the accuracy of the scan.



IP Address Spoofing

Most firewalls filter packets based on the source IP address. These firewalls examine the source IP address and determine whether the packet is coming from a legitimate source or an illegitimate source. The IDS filters packets from illegitimate sources. Attackers use IP spoofing technique to bypass such IDS/firewalls.

IP address spoofing is a hijacking technique in which an attacker obtains a computer's IP address, alters the packet headers, and sends request packets to a target machine, pretending to be a legitimate host. The packets appear to be sent from a legitimate machine but are actually sent from the attacker's machine, while his/her machine's IP address is concealed. When the victim replies to the address, it goes back to the spoofed address and not to the attacker's real address. Attackers mostly use IP address spoofing to perform DoS attacks.

When the attacker sends a connection request to the target host, the target host replies to the spoofed IP address. When spoofing a nonexistent address, the target replies to a nonexistent system and then hangs until the session times out, thus consuming a significant amount of its own resources.

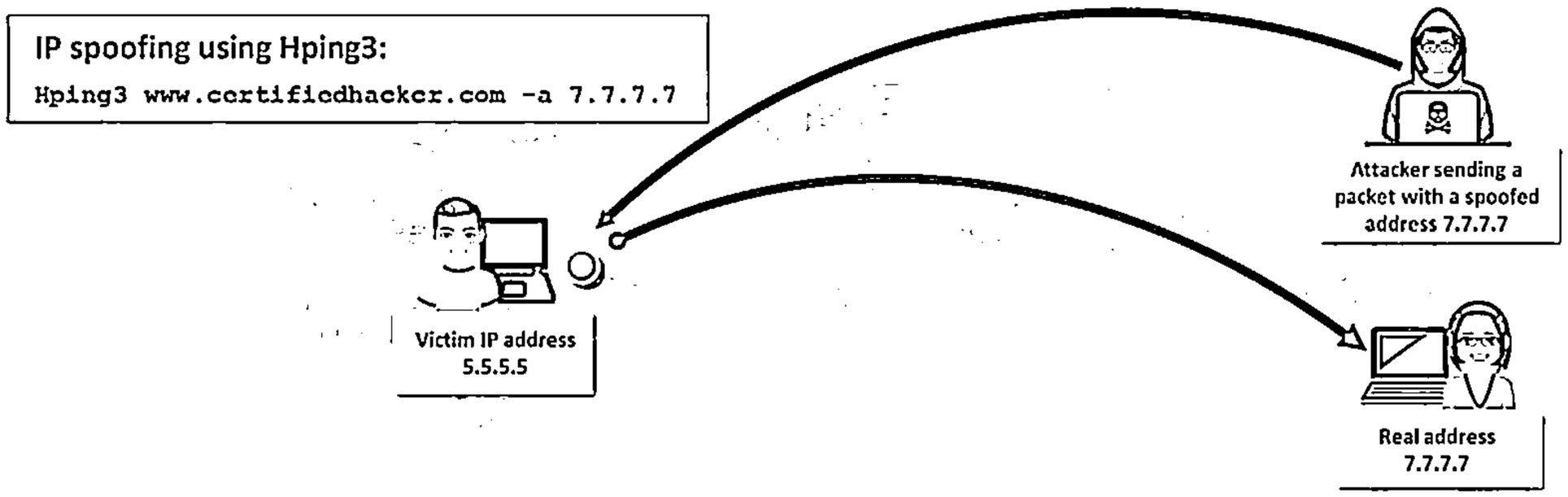


Figure 3.89: IP Spoofing using Hping3

IP spoofing using Hping3:

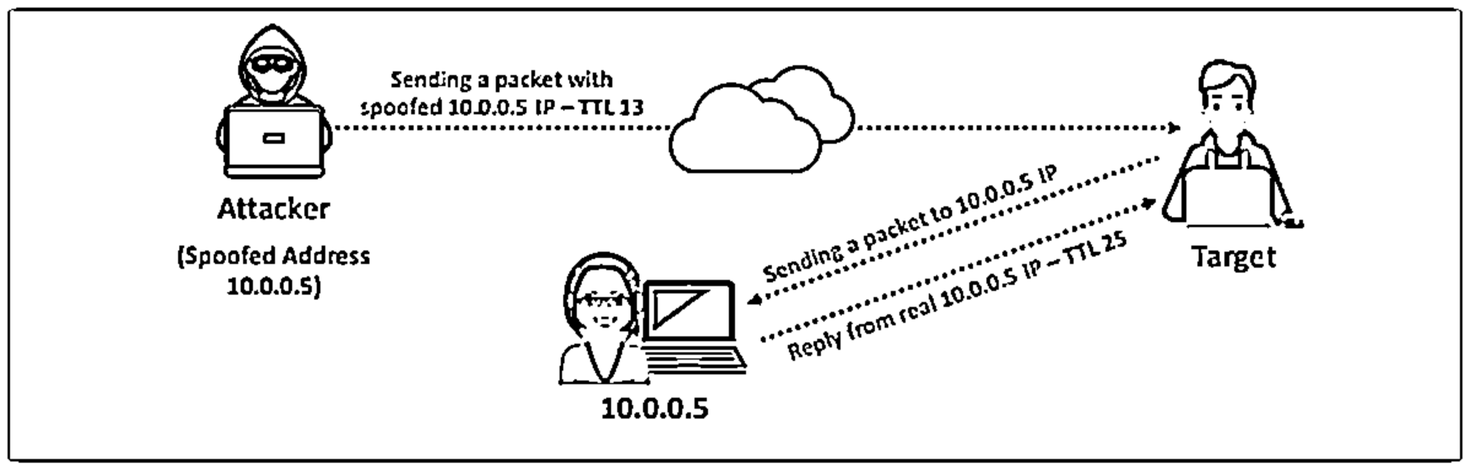
```
Hping3 www.certifiedhacker.com -a 7.7.7.7
```

You can use Hping3 to perform IP spoofing. The above command helps you to send arbitrary TCP/IP packets to network hosts.

Note: You will not be able to complete the three-way handshake and open a successful TCP connection with spoofed IP addresses.

IP Spoofing Detection Techniques: Direct TTL Probes

1. Send a packet to the host of a suspected spoofed packet that triggers a reply and compare the TTL with that of the suspected packet; if the TTL in the reply is not the same as the packet being checked, this implies that it is a spoofed packet
2. This technique is successful when the attacker is in a different subnet from that of the victim



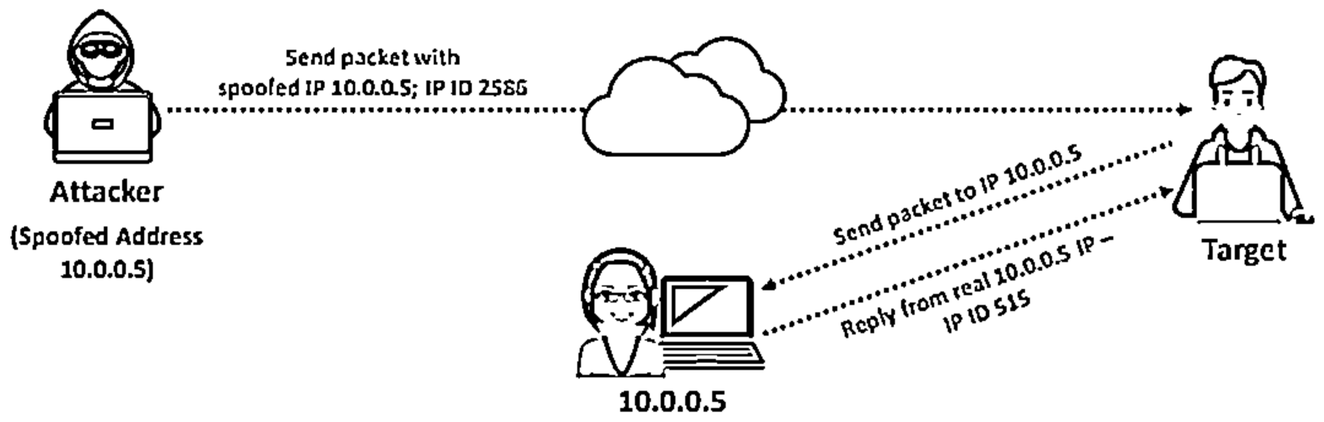
Note: Normal traffic from one host can contrast TTLs depending on traffic patterns

IP Spoofing Detection Techniques: IP Identification Number

01 Send a probe to the host of a suspected spoofed traffic that triggers a reply and compare the IPID with the suspected traffic

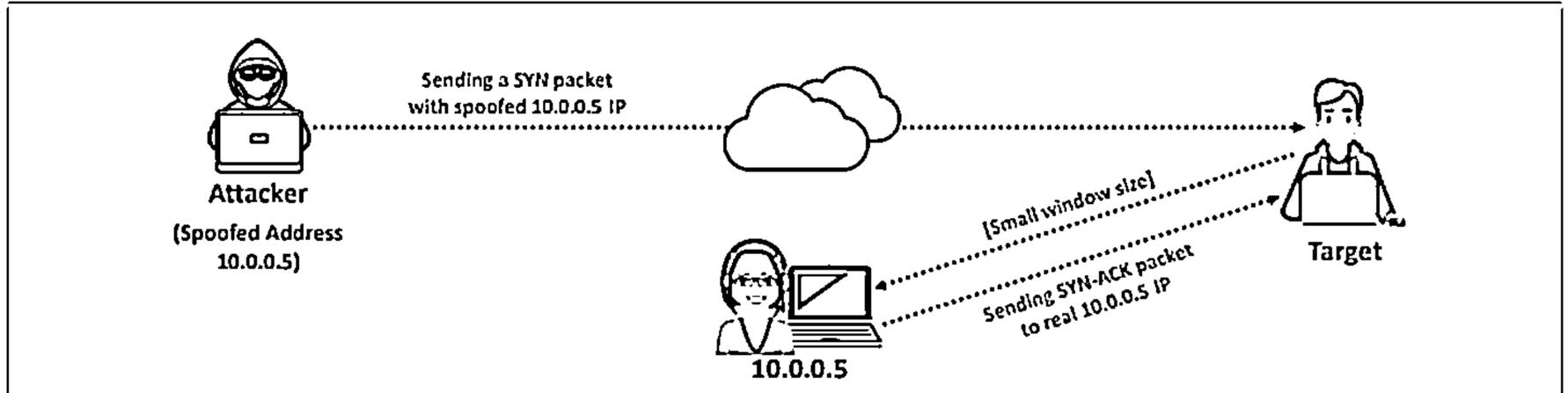
02 If the IPIDs are not close in value to the packet being checked, then the suspected traffic is spoofed

03 This technique is considered reliable even if the attacker is in the same subnet



IP Spoofing Detection Techniques: TCP Flow Control Method

- Attackers sending spoofed TCP packets will not receive the target's SYN-ACK packets
- Therefore, attackers cannot respond to a change in the congestion window size
- When received traffic continues after a window size is exhausted, the packets are most likely spoofed



IP Spoofing Detection Techniques

- **Direct TTL Probes**

  In this technique, you initially send a packet (ping request) to the legitimate host and wait for a reply. Check whether the TTL value in the reply matches with that of the packet you are checking. Both will have the same TTL if they are using the same protocol. Although the initial TTL values vary according to the protocol used, a few initial TTL values are commonly used. For TCP/UDP, the values are 64 and 128; for ICMP, they are 128 and 255.

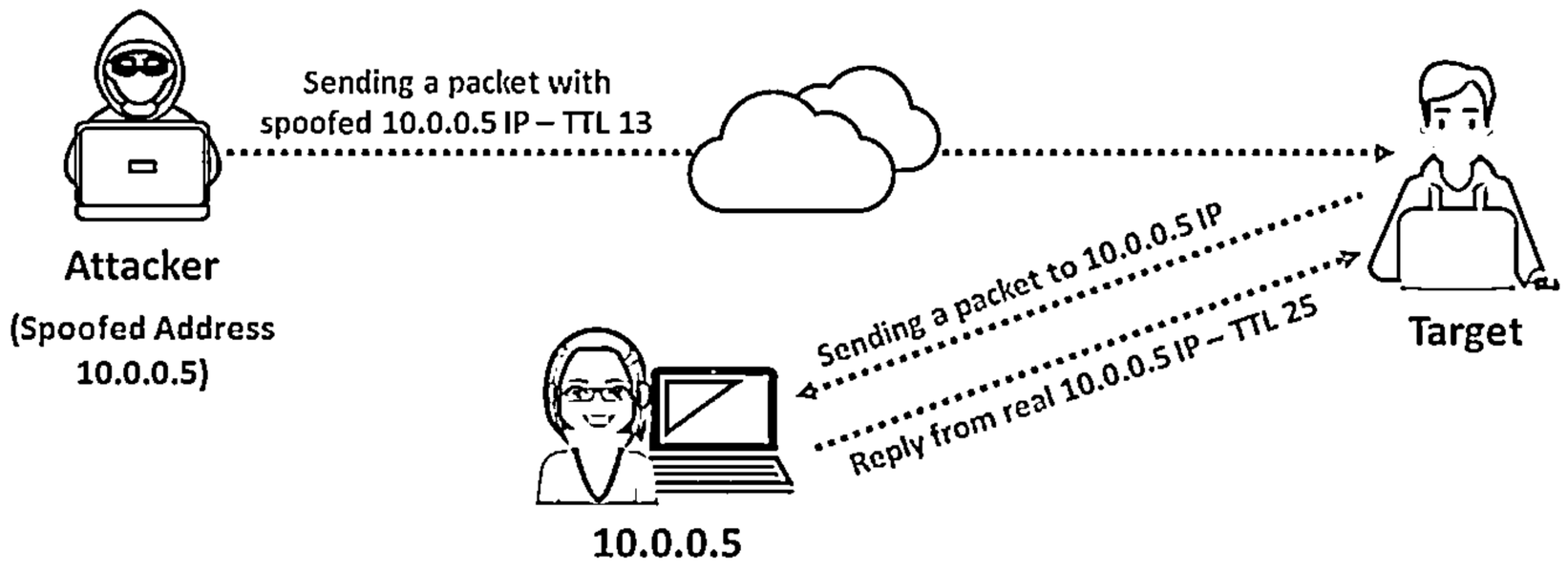


Figure 3.90: IP Spoofing detection technique: Direct TTL Probes

If the reply is from a different protocol, then you should check the actual hop count to detect the spoofed packets. Deduct the TTL value in the reply from the initial TTL value to determine the hop count. The packet is a spoofed packet if the reply TTL does not match the TTL of the packet. It will be very easy to launch an attack if the attacker knows the hop count between the source and the host. In this case, the test result is a false negative.

This technique is successful when the attacker is in a different subnet from that of the victim.

Note: Normal traffic from one host can contrast TTLs depending on traffic patterns.

- **IP Identification Number**

  Users can identify spoofed packets by monitoring the IP identification (IPID) number in the IP packet headers. The IPID increases incrementally each time a system sends a packet. Every IP packet on the network has a "fragment identification" number, which is increased by one for every packet transmission. To identify whether a packet is spoofed, send a probe packet to the source IP address of the packet and observe the IPID number in the reply. The IPID value in the response packet must be close to but slightly greater than the IPID value of the probe packet. The source address of the IP packet is spoofed if the IPID of the response packet is not close to that of the probe packet.

  This method is effective even when both the attacker and the target are on the same subnet.

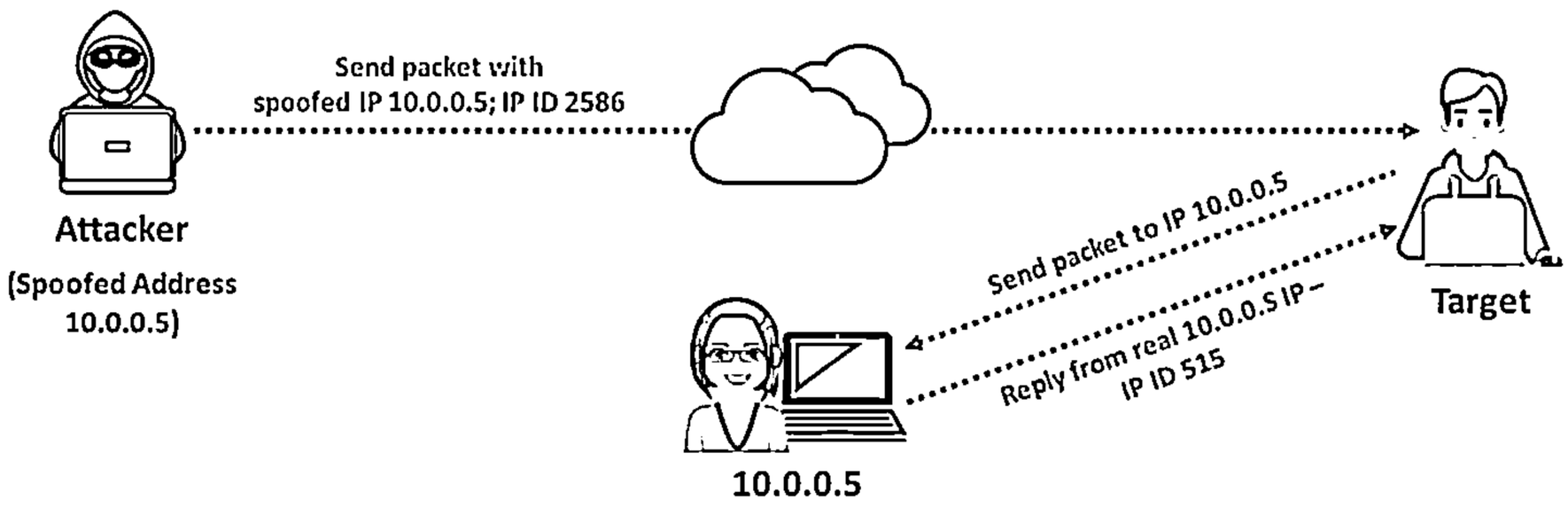


Figure 3.91: IP Spoofing detection technique: IP Identification Number

- **TCP Flow Control Method**

  The TCP can optimize the flow control on both the sender's and the receiver's end with its algorithm. The algorithm accomplishes flow control using the sliding window principle. The user can control the flow of IP packets by the window size field in the TCP header. This field represents the maximum amount of data that the recipient can receive and the maximum amount of data that the sender can transmit without acknowledgement. Thus, this field helps to control data flow. The sender should stop sending data whenever the window size is set to zero.

  In general flow control, the sender should stop sending data once the initial window size is exhausted. The attacker, who is unaware of the ACK packet containing window size information, might continue to send data to the victim. If the victim receives data packets beyond the window size, they are spoofed packets. For effective flow control and early detection of spoofing, the initial window size must be very small.

  Most spoofing attacks occur during the handshake, as it is challenging to build multiple spoofing replies with the correct sequence number. Therefore, apply the flow control spoofed packet detection method to the handshake. In a TCP handshake, the host sending

the initial SYN packet waits for SYN-ACK before sending the ACK packet. To check whether you are getting the SYN request from a genuine client or a spoofed one, set SYN-ACK to zero. If the sender sends an ACK with any data, it means that the sender is a spoofed one. This is because when SYN-ACK is set to zero, the sender must respond to it only with the ACK packet, without additional data.

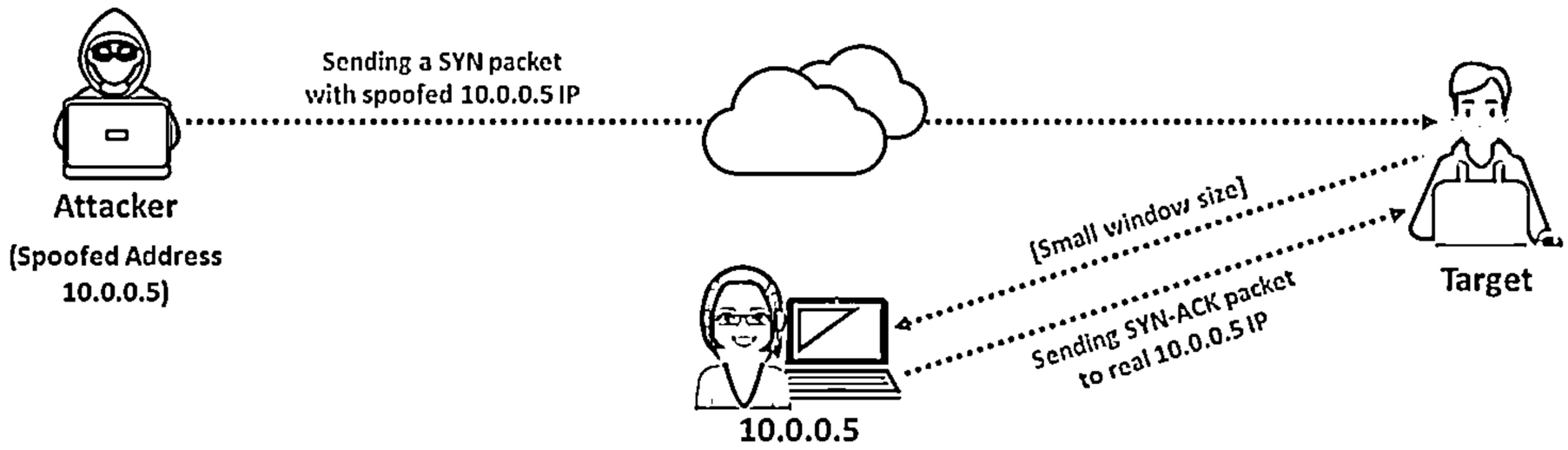
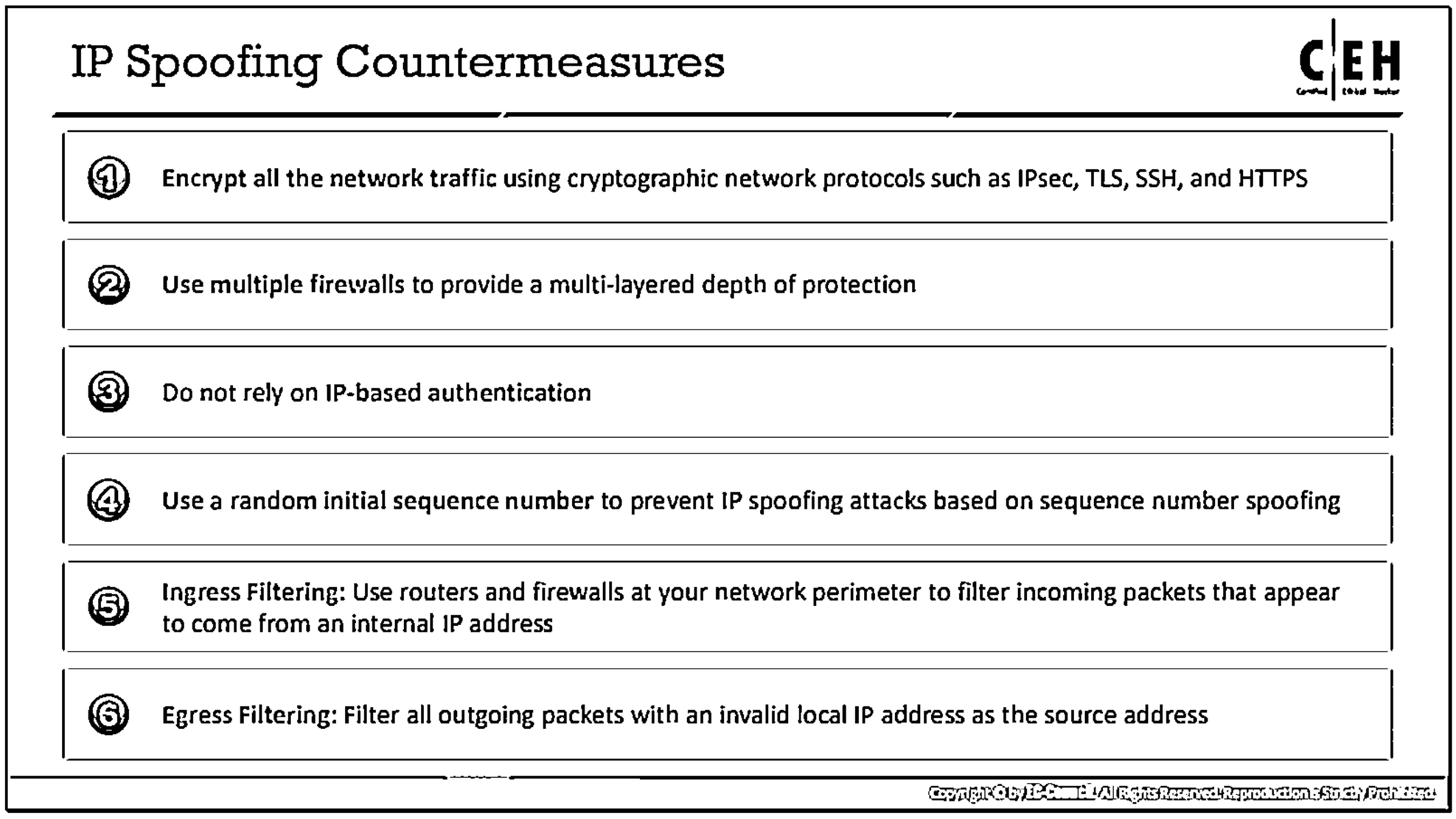


Figure 3.92: IP Spoofing detection technique: TCP Flow Control Method

Attackers sending spoofed TCP packets will not receive the target's SYN-ACK packets. Attackers cannot respond to changes in the congestion window size. When the received traffic continues after a window size is exhausted, the packets are most likely spoofed.



IP Spoofing Countermeasures

In ethical hacking, the ethical hacker, also known as the "pen tester," has to perform an additional task that a normal hacker does not follow (i.e., adopting countermeasures against the respective vulnerabilities determined through hacking). This is essential because knowing security loopholes in your network is worthless unless you adopt measures to protect them against real hackers. As mentioned previously, IP spoofing is one of the techniques that a hacker adopts to break into the target network. Therefore, to protect your network from external hackers, you should apply IP spoofing countermeasures to your network security settings. Some IP spoofing countermeasures that you can apply are as follows:

- **Avoid trust relationships**

  Do not rely on IP-based authentication. Attackers may spoof themselves as trusted hosts and send malicious packets to you. If you accept these packets under the assumption that they are "clean" because they are from your trusted host, the malicious code will infect your system. Therefore, it is advisable to test all packets, even when they come from one of your trusted hosts. You can avoid this problem by implementing password authentication along with trust-relationship-based authentication.

- **Use firewalls and filtering mechanisms**

  As stated above, you should filter all the incoming and outgoing packets to avoid attacks and sensitive information loss. A firewall can restrict malicious packets from entering your private network and prevent severe data loss. You can use access control lists (ACLs) to block unauthorized access. At the same time, there is a possibility of an insider attack. Inside attackers can send sensitive information about your business to your competitors, which could lead to monetary loss and other issues. Another risk of outgoing packets is that an attacker will succeed in installing a malicious sniffing program running in a hidden

mode on your network. These programs gather and send all your network information to the attacker without any notification after filtering the outgoing packets. Therefore, you should assign the same importance to the scanning of outgoing packets as you would to that of incoming packets.

- **Use random initial sequence numbers**

  Most devices choose their ISN based on timed counters. This makes the ISNs predictable, as it is easy for an attacker to determine the concept of generating the ISN. The attacker can determine the ISN of the next TCP connection by analyzing the ISN of the current session or connection. If the attacker can predict the ISN, then he/she can establish a malicious connection to the server and sniff out your network traffic. To avoid this risk, use random initial sequence numbers.

- **Ingress filtering**

  Ingress filtering prevents spoofed traffic from entering the Internet. It is applied to routers because it enhances the functionality of the routers and blocks spoofed traffic. Configuring and using ACLs that drop packets with the source address outside the defined range is one method of implementing ingress filtering.

- **Egress filtering**

  Egress filtering refers to a practice that aims to prevent IP spoofing by blocking outgoing packets with a source address that is not inside.

- **Use encryption**

  If you want to attain maximum network security, then use strong encryption for all the traffic placed onto the transmission media without considering its type and location. This is the best way to prevent IP spoofing attacks. IPsec can be used to reduce the IP spoofing risk drastically, as it provides data authentication, integrity, and confidentiality. Furthermore, ACLs can be used for blocking private IP addresses at the downstream interfaces. Encryption sessions should be enabled on the router so that trusted hosts can communicate securely with local hosts. Attackers tend to focus on easy-to-compromise targets. If an attacker wants to break into the encrypted network, he or she has to decrypt a whole slew of encrypted packets, which is a difficult task. Therefore, the attacker is likely to move on and try to find another target that is easy to compromise or simply abort the attempt. Moreover, use the latest encryption algorithms that provide strong security.

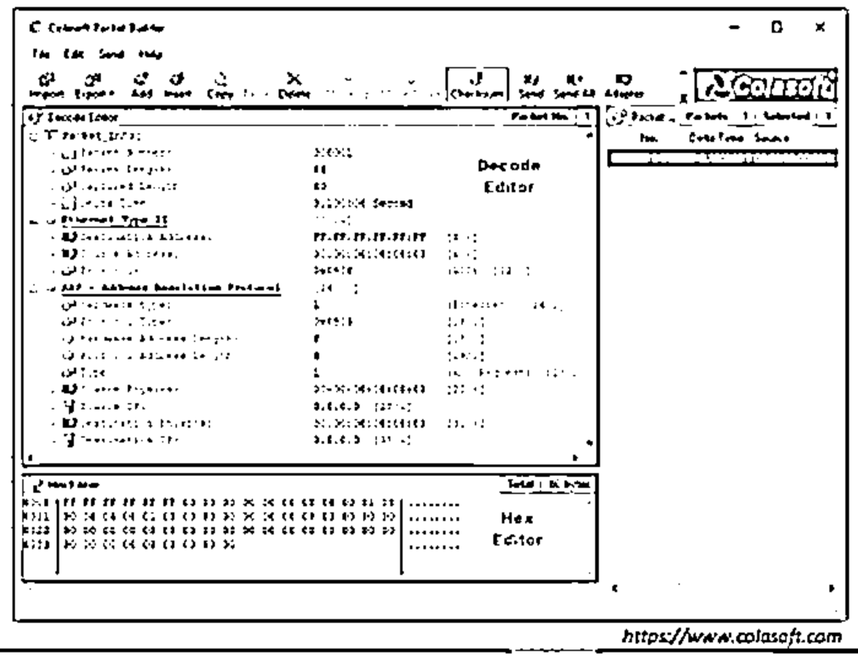
- **SYN flooding countermeasures**

  Countermeasures against SYN flooding attacks can also help you to avoid IP spoofing attacks.

Creating Custom Packets

Creating Custom Packets by using Packet Crafting Tools

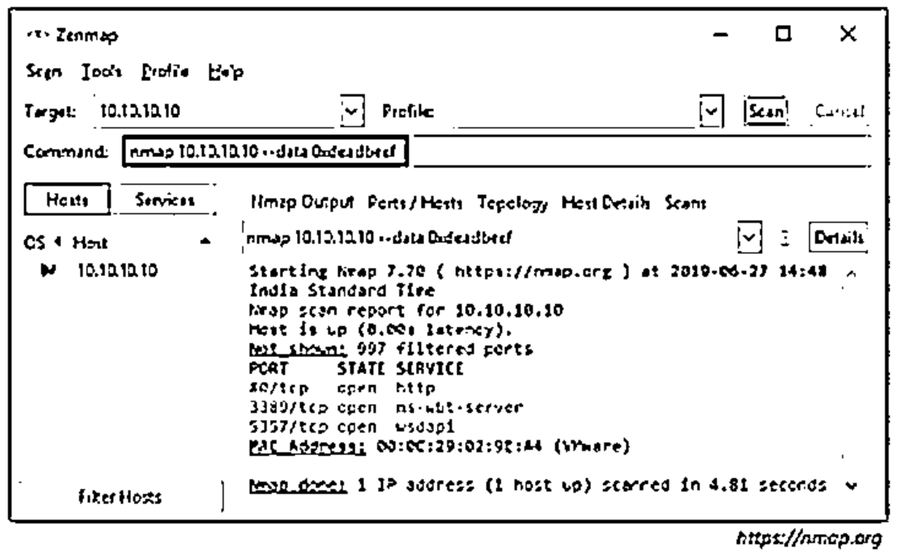
- Attackers create custom TCP packets using various packet crafting tools like Colasoft Packet Builder, NetScanTools Pro, etc. to scan a target beyond a firewall



https://www.colasoft.com

Creating Custom Packets by Appending Custom Binary Data

- Attackers send binary data (0's and 1's) as payloads in transmitted packets to scan beyond firewalls
- Example: --data 0xdeadbeef

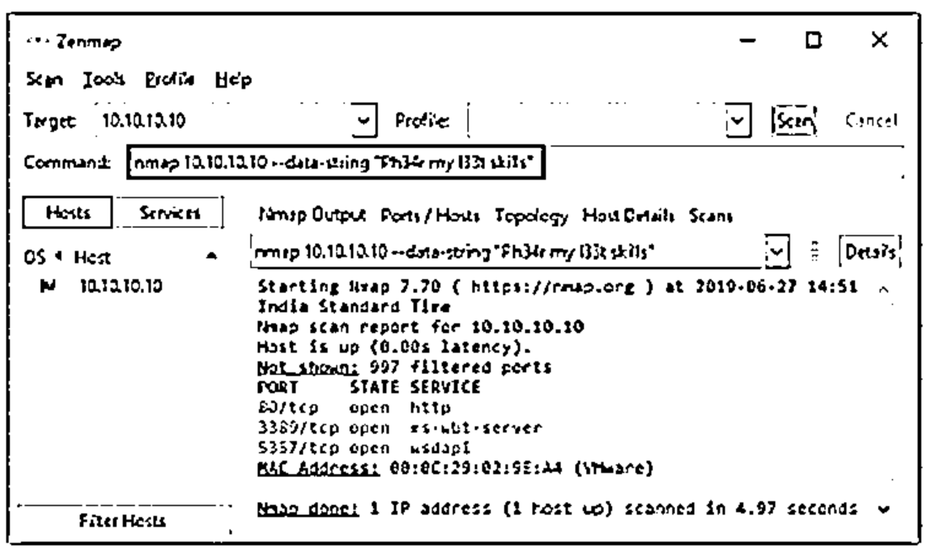


https://nmap.org

Creating Custom Packets (Cont'd)

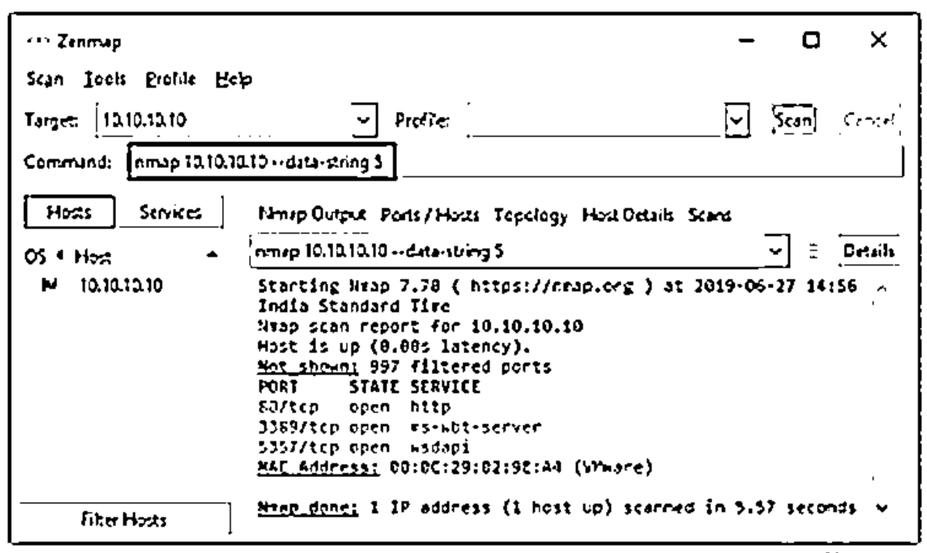
Creating Custom Packets by Appending Custom String

- Attackers send a regular string as payloads in the packets sent to the target machine for scanning beyond the firewall
- Example: --data-string "Ph34r my l33t skills"



Creating Custom Packets by Appending Random Data

- Attackers append a number of random data bytes to most of the packets sent without any protocol-specific payloads
- Example: --data-string 5



https://nmap.org

Creating Custom Packets

The attacker creates and sends custom packets to scan the intended target beyond the IDS/firewalls. Various techniques are used to create custom packets. Some of them are mentioned below:

- **Creating Custom Packets by using Packet Crafting Tools**

Attackers create custom TCP packets to scan the target by bypassing the firewalls. Attackers use various packet crafting tools such as Colasoft packet builder (*https://www.colasoft.com*), NetScanTools Pro (*https://www.netscantools.com*), etc., to scan the target that is beyond the firewall. Packet crafting tools craft and send packet streams (custom packets) using different protocols at different transfer rates.

- **Colasoft Packet Builder**

  Source: *https://www.colasoft.com*

  Colasoft Packet Builder is a tool that allows an attacker to create custom network packets and helps security professionals assess the network. The attacker can select a TCP packet from the provided templates and change the parameters in the decoder, hexadecimal, or ASCII editor to create a packet. In addition to building packets, Colasoft Packet Builder supports saving packets to packet files and sending packets to the network.

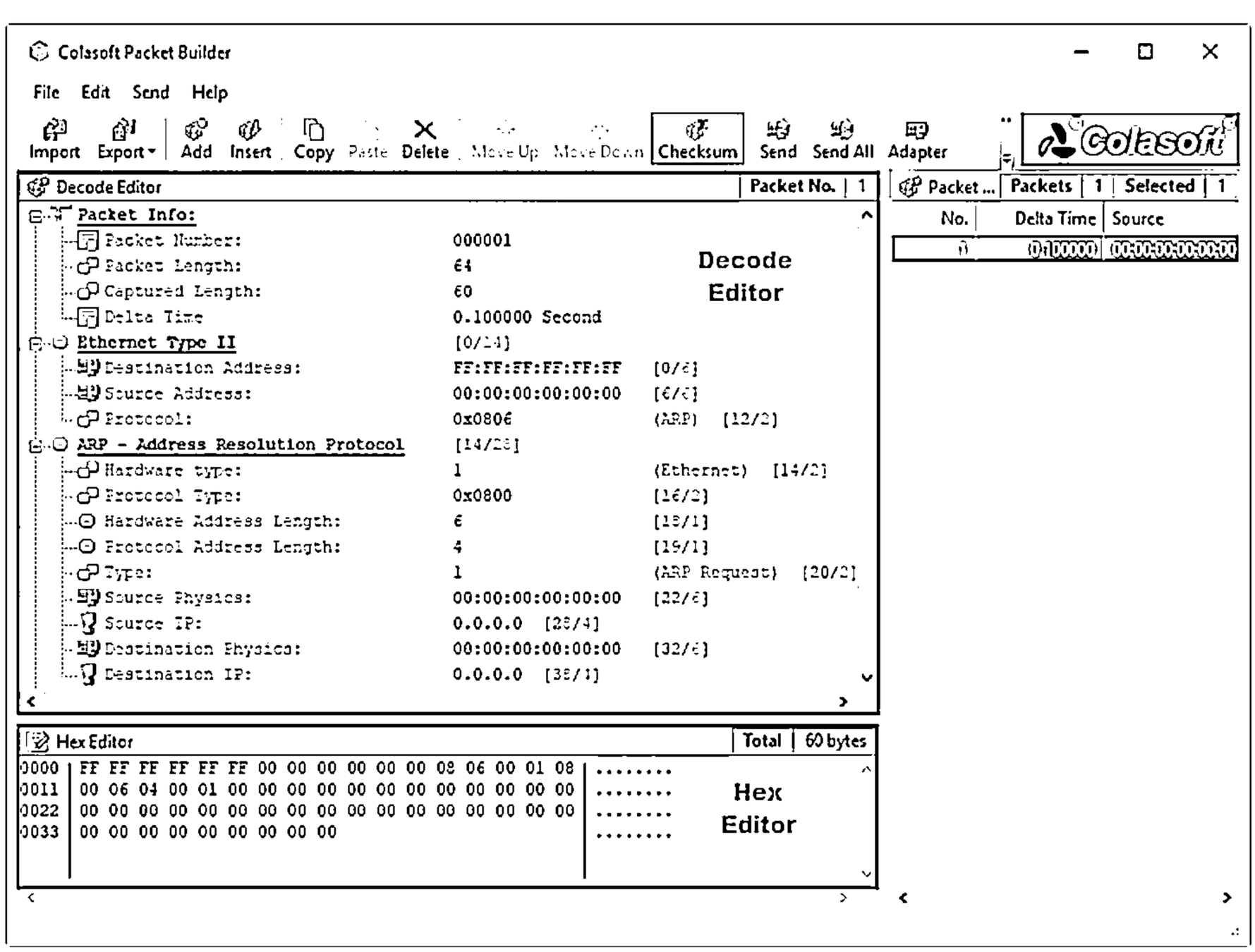


Figure 3.93: Screenshot of Colasoft Packet Builder

There are three views in the Packet Builder: Packet List, Decode Editor, and Hex Editor.

- Packet List displays all the constructed packets. When you select one or more packets in Packet List, the first highlighted packet is displayed in both Decode Editor and Hex Editor for editing.

- In Hex Editor, the data of the packet are represented as hexadecimal values and ASCII characters; nonprintable characters are represented by a dot (".") in the ASCII section. You can edit either the hexadecimal values or the ASCII characters.
- Decode Editor allows the attacker to edit packets without remembering the value length, byte order, and offsets. You can select a field and change the value in the edit box.

For creating a packet, you can use the add or insert packet command in the Edit menu or the Toolbar to create a new packet.

The attacker can send a constructed packet to wire directly and control how Colasoft Packet Builder sends the packets, specifying, for example, the interval between packets, loop times, and delay between loops.

This packet builder audits networks and checks the network protection against attacks and intruders. Attackers may use this packet builder to create fragmented packets to bypass network firewalls and IDS systems. They can also create packets and flood the victim with a very large number of packets, which could result in DoS attacks.

- **Creating Custom Packets by Appending Custom Binary Data**

  Attackers send binary data (0's and 1's) as payloads in the packets sent to the target machine present behind the firewall. The option used by Nmap for appending custom binary data to the sent packets is `--data <hex string>`. Any `<hex string>` is specified in the formats `0xAABBCCDDEEFF<...>`, `AABBCCDDEEFF<...>`, or `\xAA\xBB\xCC\xDD\xEE\xFF<...>`. To perform a byte-order conversion, the specified information should be based on the receiver's expectations. Attackers can use this technique to scan the target by manipulating the firewalls by appending custom binary or hex data to the sent packets.

  Example: `--data 0xdeadbeef` (or) `--data \xCA\xFE\x09`

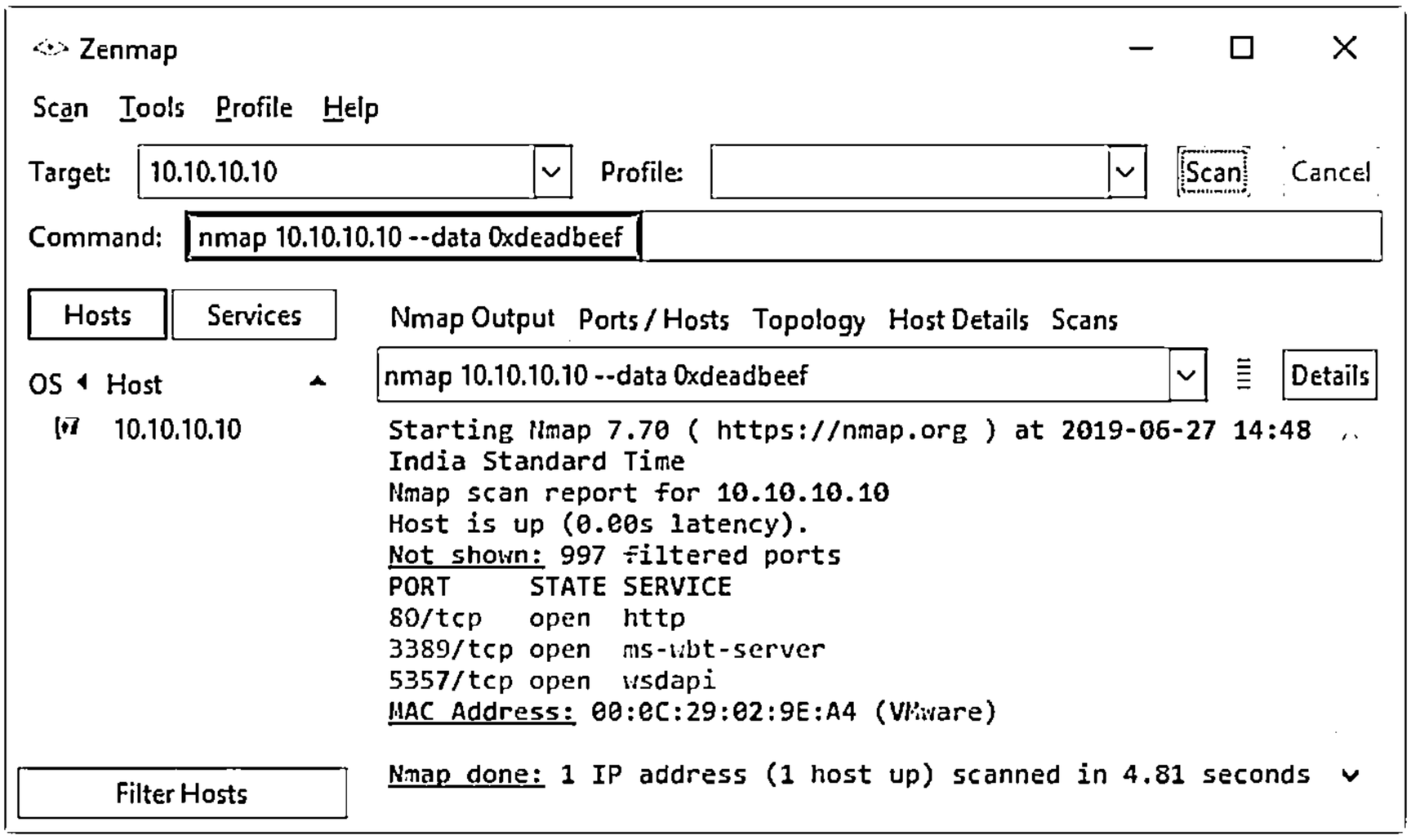


Figure 3.94: Screenshot of appending binary string in Zenmap

- **Creating Custom Packets by Appending Custom String**

  Attackers send regular strings as payloads in the packets sent to the target machine for scanning beyond the firewall. The option used by Nmap for appending a custom string to the sent packets is `--data-string <string>`. The `<string>` can contain any string and a few characters depend on the system's location; however, it is not guaranteed whether the same information is retrieved. The string is enclosed with double quotes (" ") and special characters from the shell are not used. Attackers can use this technique to scan the target by manipulating the firewalls by appending custom string data to the sent packets.

  Example: `--data-string "Scan conducted by Security Ops, extension 7192"` (or) `--data-string "Ph34r my l33t skills"`.

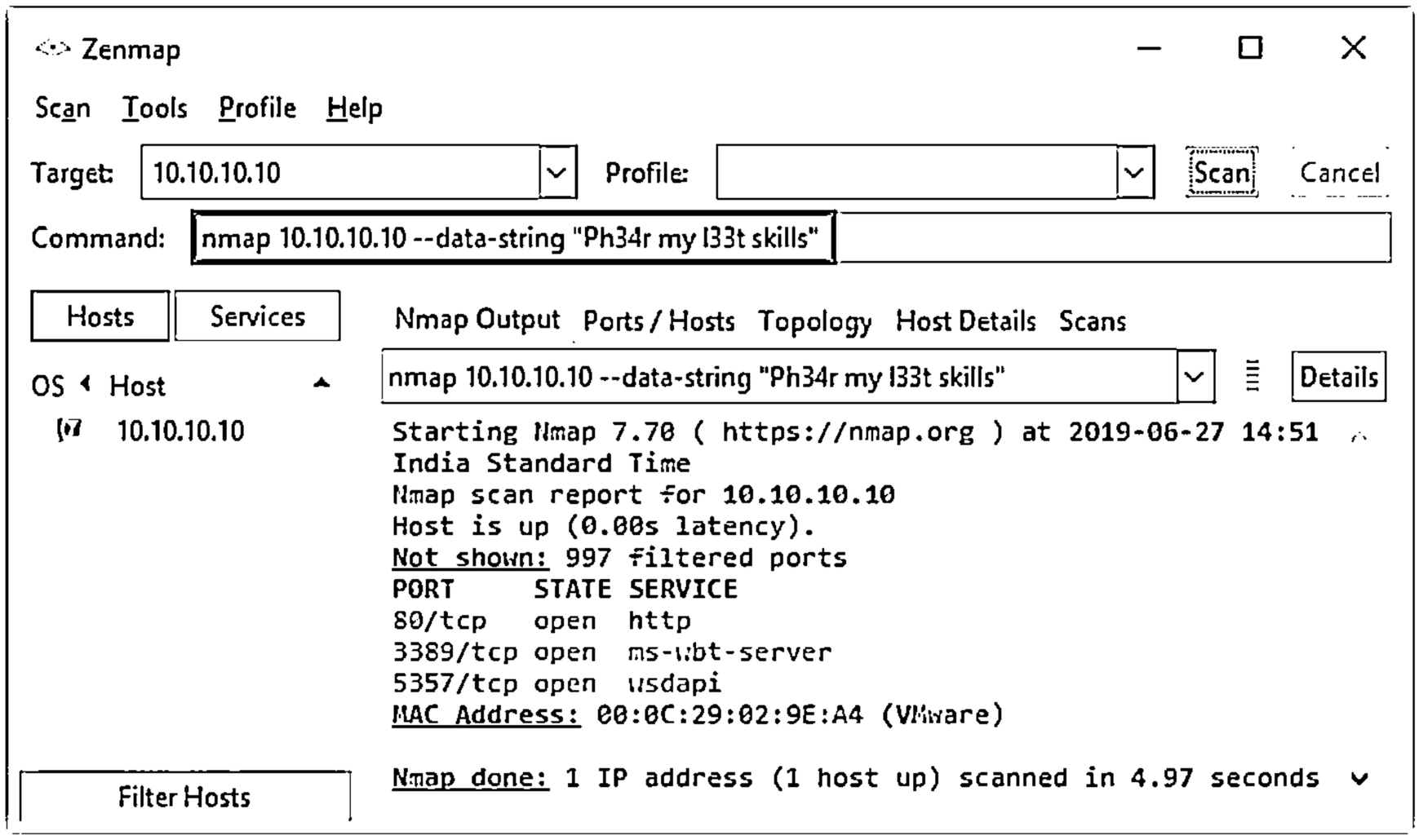


Figure 3.95: Screenshot of appending custom string in Zenmap

- **Creating Custom Packets by Appending Random Data**

  Attackers append a number of random data bytes to most packets sent without using any protocol-specific payloads. The option used by Nmap for appending random data to the sent packets is `--data-length <number>`. For protocol-specific and no random payloads, `--data-length 0` is used. The (-O) OS detection packets are not usually affected, as probe consistency is needed for it to be accurate. By default, a few UDP ports and IP protocols get a custom payload. Attackers can use this technique to scan the target by manipulating the firewalls by appending random data or numbers to the sent packets.

  Example: `--data-string 1` (or) `--data-string 5`

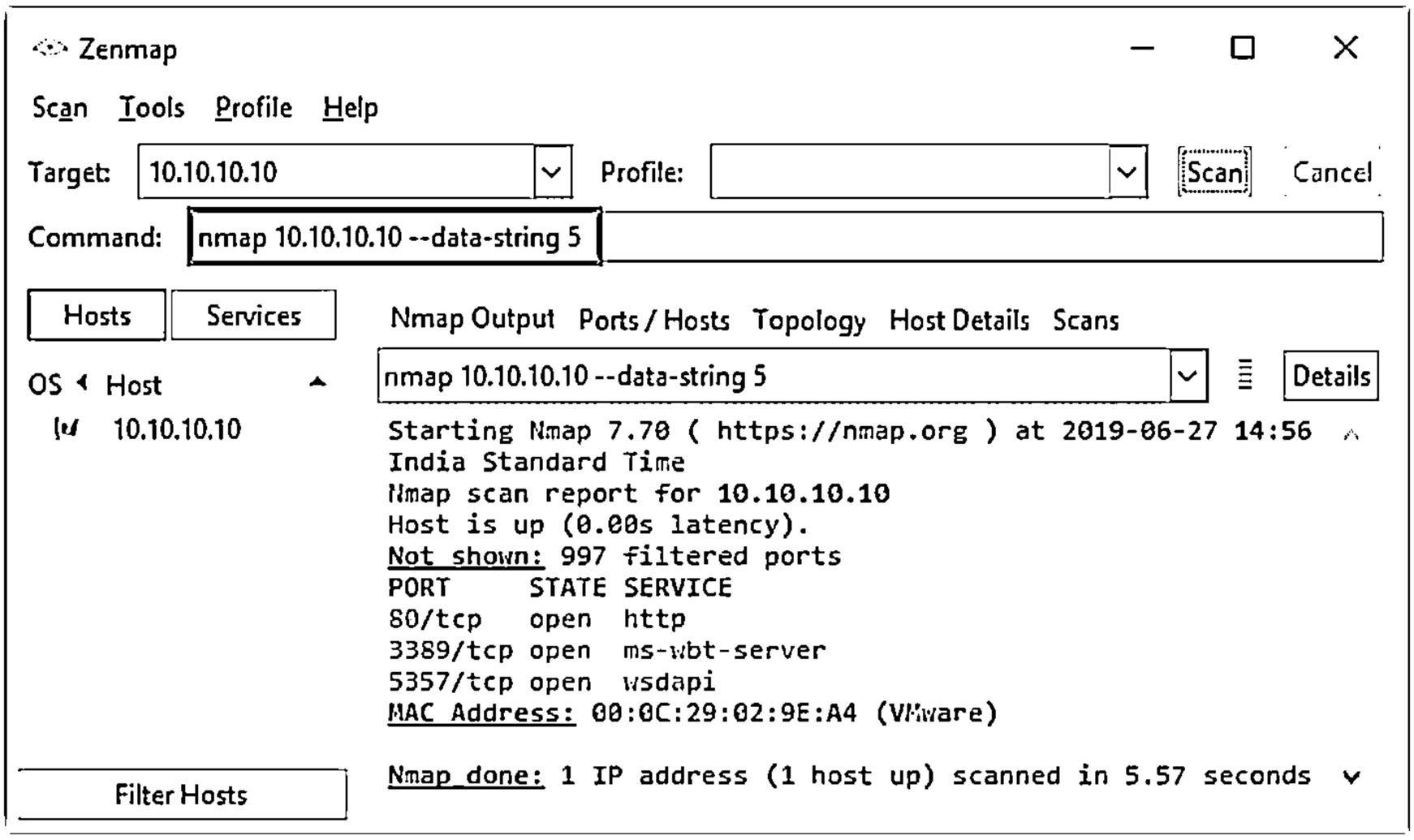
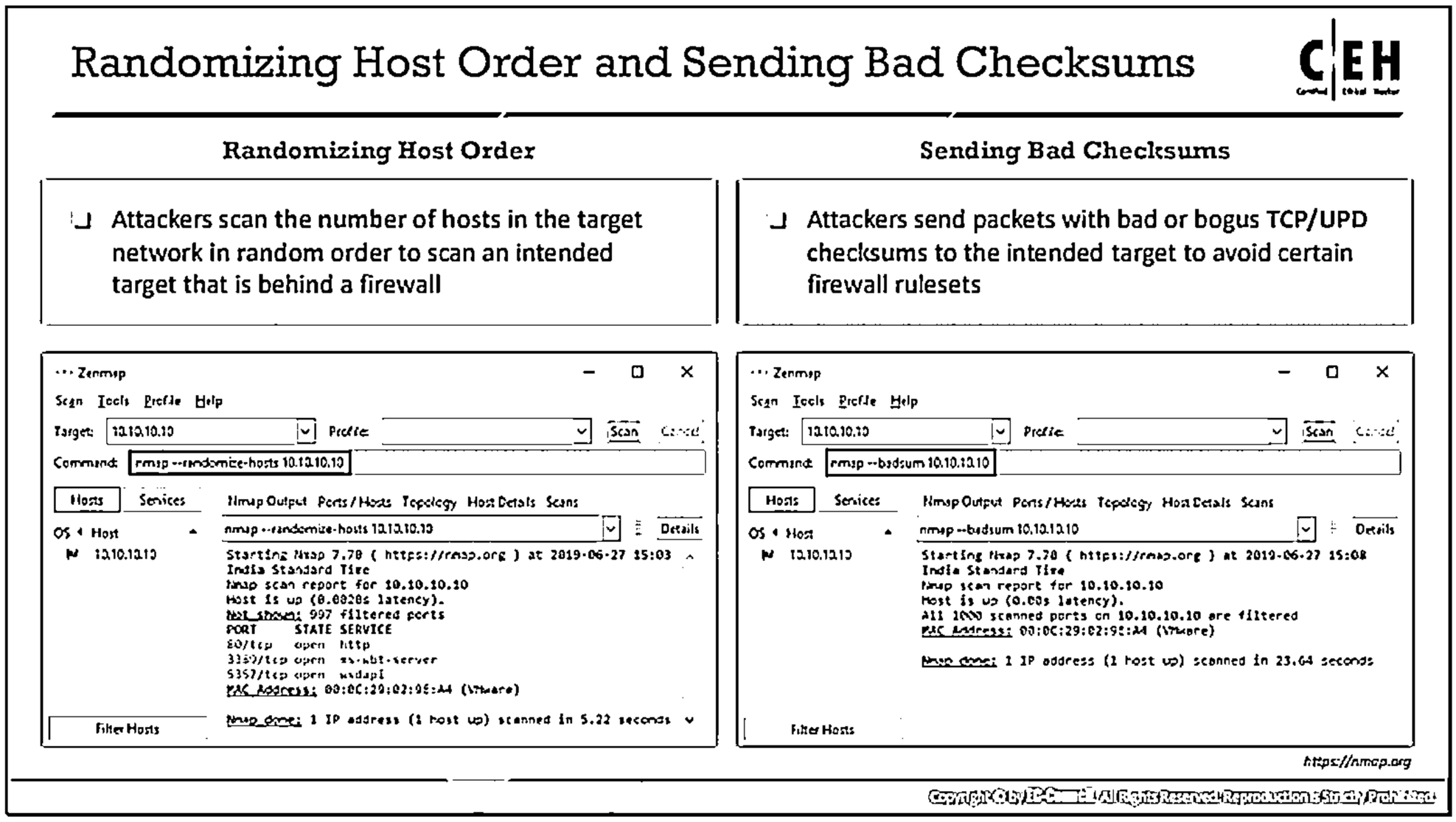


Figure 3.96: Screenshot of appending random string in Zenmap



Randomizing Host Order and Sending Bad Checksums

Randomizing Host Order

The attacker scans the number of hosts in the target network in a random order to scan the intended target that is lying beyond the firewall. The option used by Nmap to scan with a random host order is **`--randomize-hosts`**.

This technique instructs Nmap to shuffle each group of 16384 hosts before scanning with slow timing options, thus making the scan less notable to network monitoring systems and firewalls. If larger group sizes are randomized, the **`PING_GROUP_SZ`** should be increased in **`nmap.h`** and it should be compiled again. Another method can be followed by generating the target IP list with the list scan command **`-sL -n -oN <filename>`** and then randomizing it with a Perl script and providing the whole list to Nmap using the **`-iL`** command.

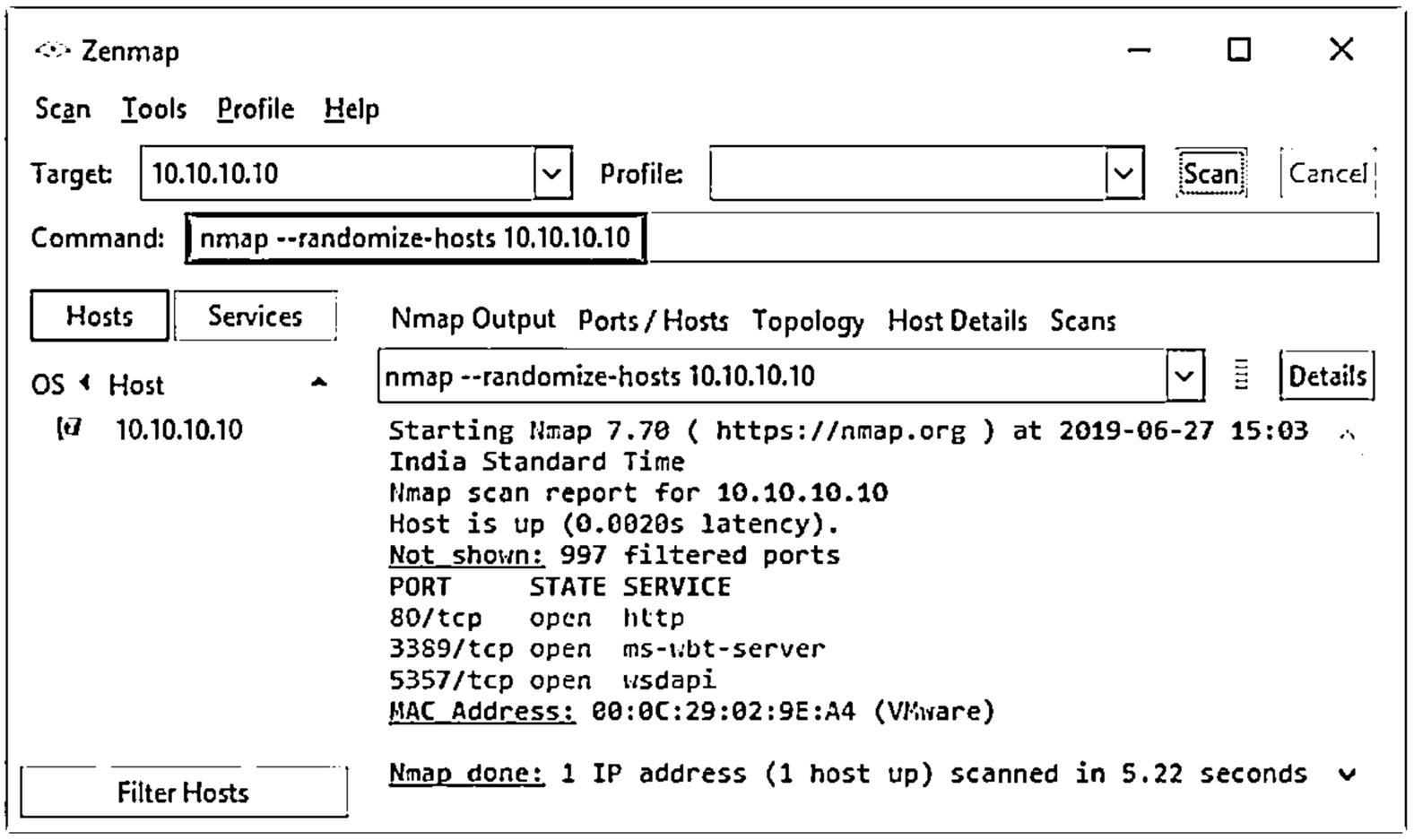


Figure 3.97: Screenshot of randomizing hosts in Zenmap

Sending Bad Checksums

The attacker sends packets with bad or bogus TCP/UPD checksums to the intended target to avoid certain firewall rule sets. TCP/UPD checksums are used to ensure data integrity. Sending packets with incorrect checksums can help attackers to acquire information from improperly configured systems by checking for any response. If there is a response, then it is from the IDS or firewall, which did not verify the obtained checksum. If there is no response or the packets are dropped, then it can be inferred that the system is configured. This technique instructs Nmap to send packets with invalid TCP, UDP, or SCTP checksums to the target host. The option used by Nmap is **`--badsum`**.

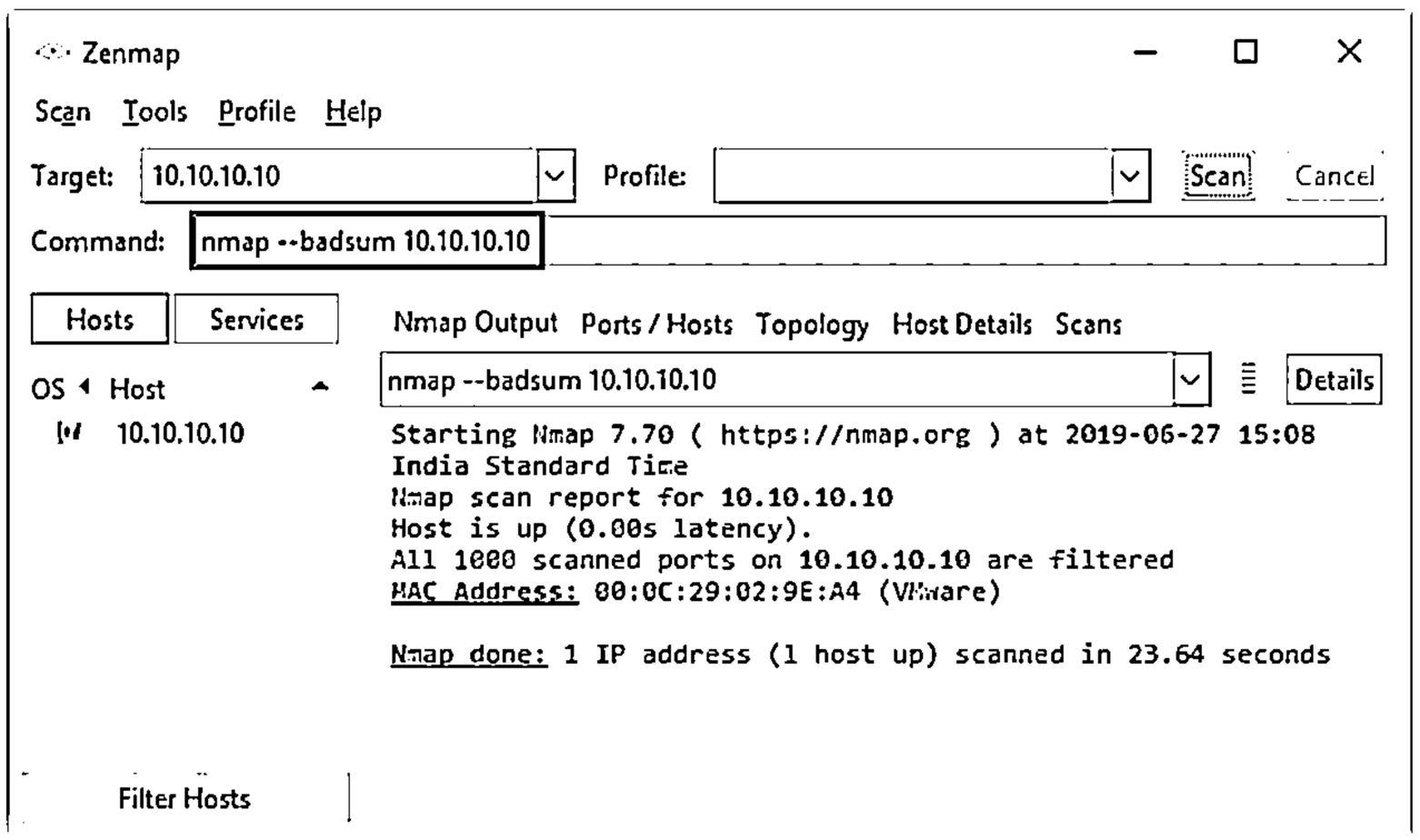
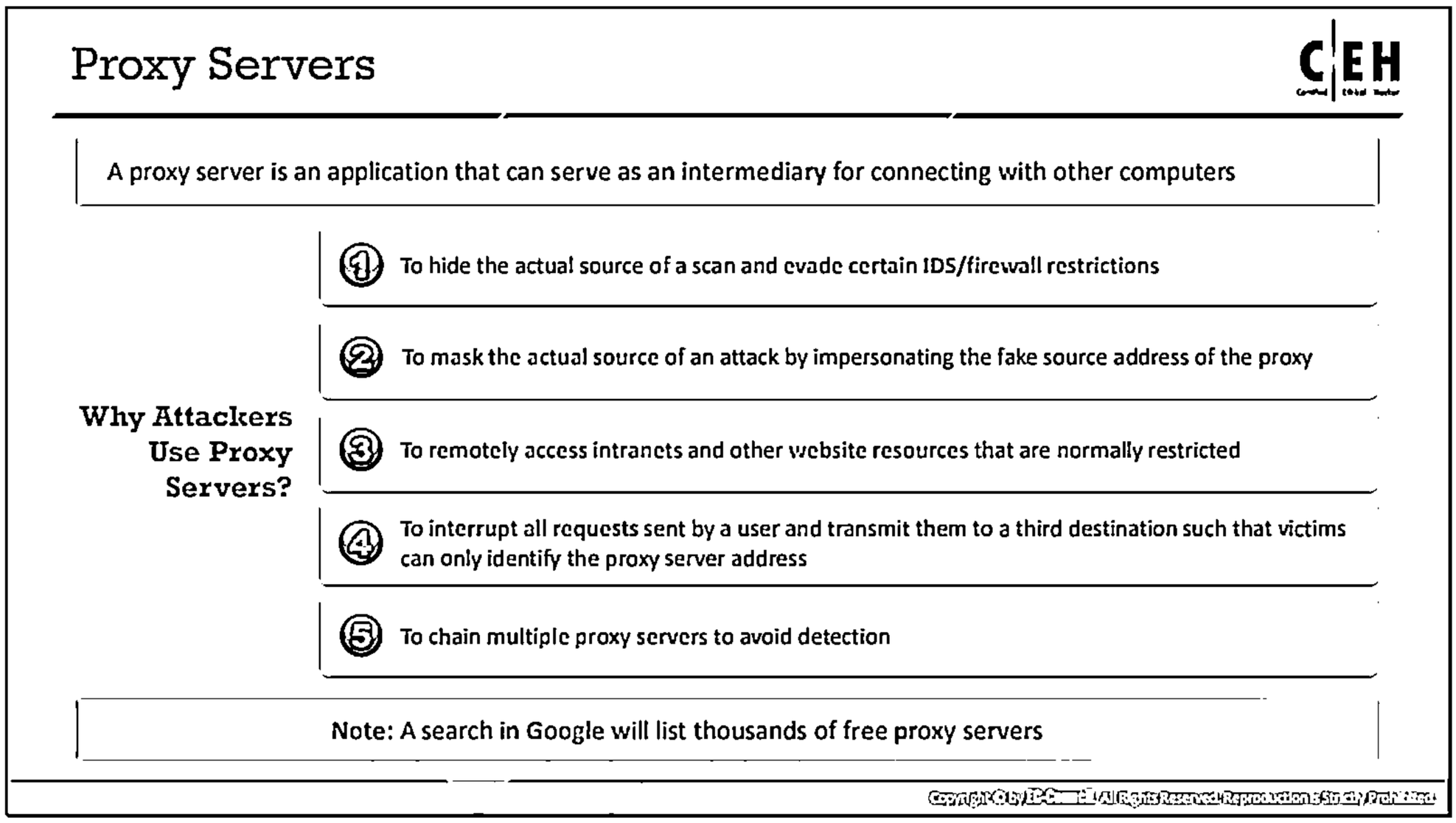


Figure 3.98: Screenshot of scanning by sending bad checksums in Zenmap



Proxy Servers

A proxy server is an application that can serve as an intermediary for connecting with other computers.

A proxy server is used:

- As a firewall and to protect the local network from external attacks.
- As an IP address multiplexer that allows several computers to connect to the Internet when you have only one IP address (NAT/PAT).
- To anonymize web surfing (to some extent).
- To extract unwanted content, such as ads or "unsuitable" material (using specialized proxy servers).
- To provide some protection against hacking attacks.
- To save bandwidth.

How does a proxy server work?

Initially, when you use a proxy to request a particular web page on an actual server, the proxy server receives it. The proxy server then sends your request to the actual server on your behalf. It mediates between you and the actual server to transmit and respond to the request, as shown in the figure below.

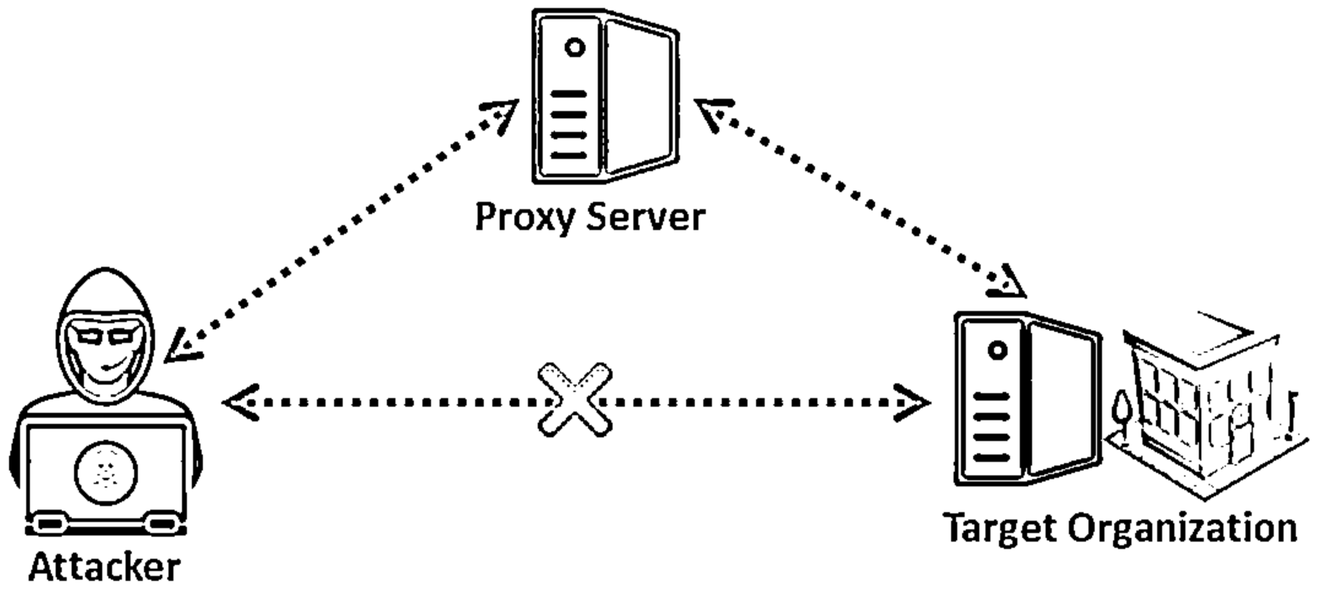


Figure 3.99: Attacker using a proxy server for connecting to the target

In this process, the proxy receives the communication between the client and the destination application. To take advantage of a proxy server, an attacker must configure client programs so that they can send their requests to the proxy server instead of the final destination.

Why Attackers Use Proxy Servers?

It is easier for an attacker to attack or hack a particular system than to conceal the attack source. Therefore, the primary challenge for an attacker is to hide his/her identity so that he/she cannot be traced. Thus, the attacker uses a proxy server to avoid attack detection by masking his/her IP address. When the attacker uses a proxy to connect to the target system, the server logs will record the proxy's source address rather than the attacker's source address.

Proxy sites help the attacker to browse the Internet anonymously and access blocked sites (i.e., evade firewall restrictions). Thus, the attacker can surf restricted sites anonymously without using the source IP address.

Attackers use proxy servers:

- To hide the actual source of a scan and evade certain IDS/firewall restrictions.
- To hide the source IP address so that they can hack without any legal corollary.
- To mask the actual source of the attack by employing a fake source address of the proxy.
- To remotely access intranets and other website resources that are normally off limits.
- To interrupt all the requests sent by a user and transmit them to a third destination; hence, victims will only be able to identify the proxy server address.
- To chain multiple proxy servers to avoid detection.

Free Proxy Servers

Some free proxy servers available on the Internet, which can help you to access restricted sites without revealing your IP address. In the **Google** search engine, type "**Free Proxy Servers**" to see a list of such servers. Select one from this list and download and install it to browse anonymously without revealing your legitimate IP address.

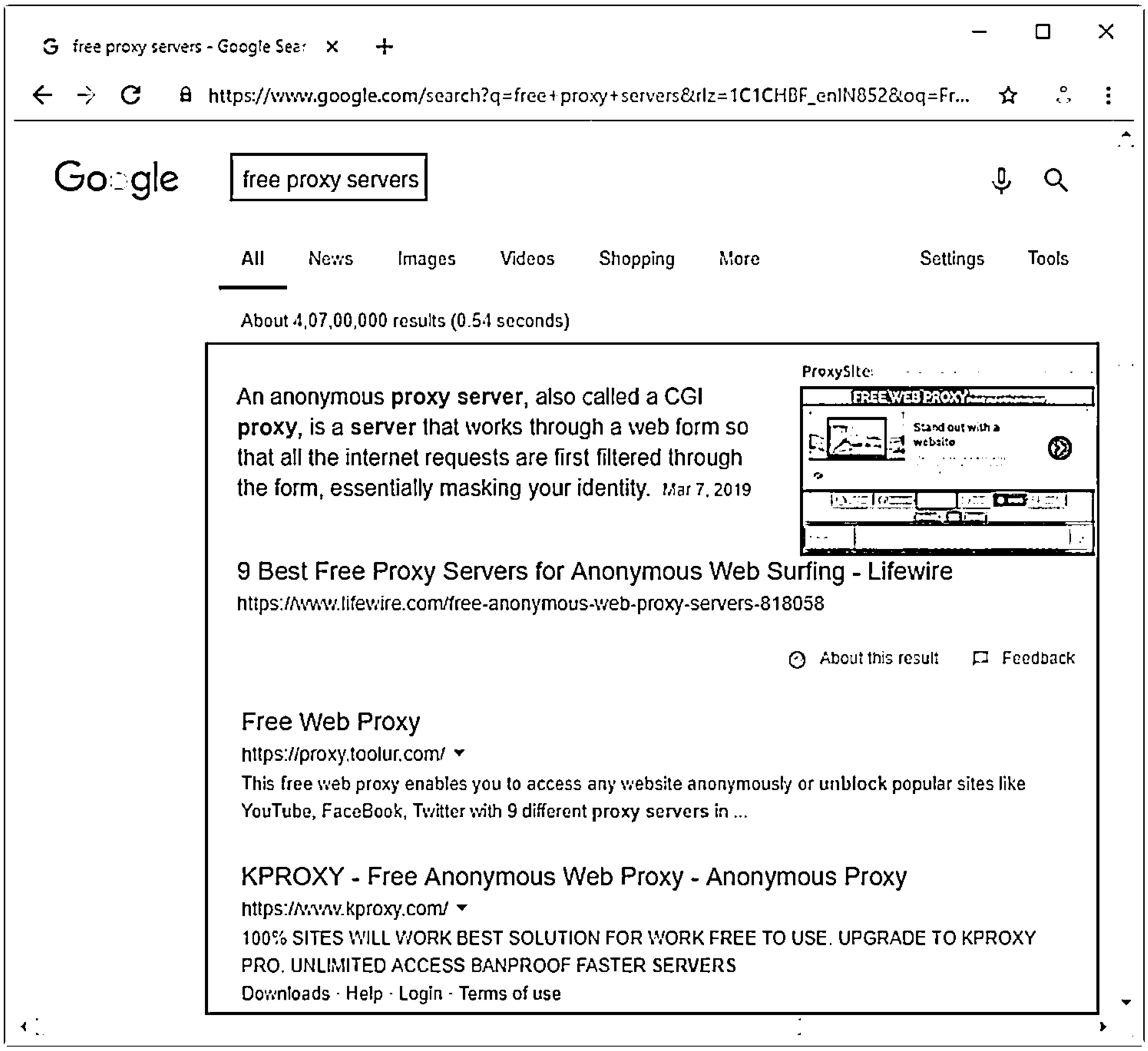
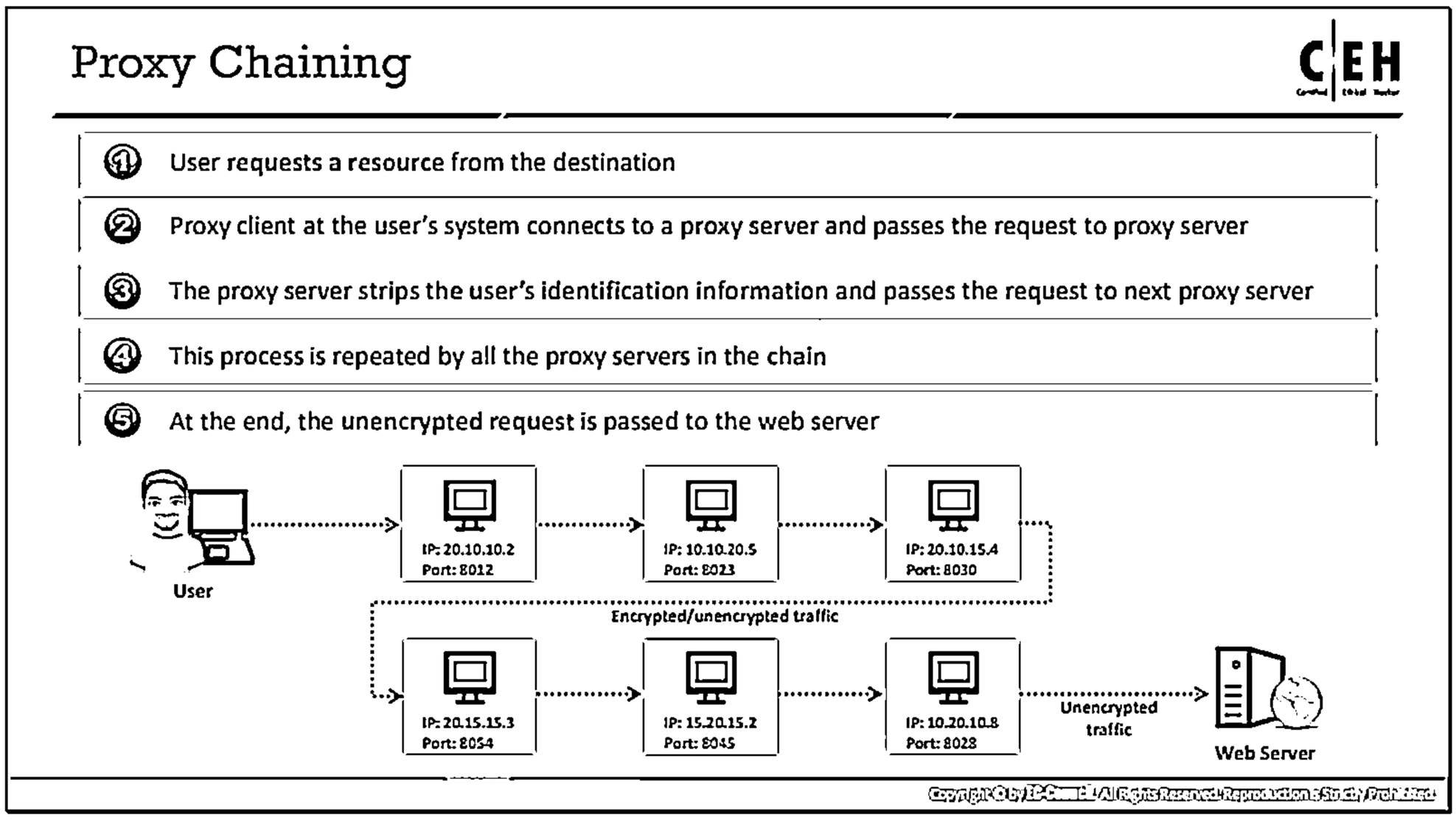


Figure 3.100: Free Proxy Servers



Proxy Chaining

Proxy chaining helps an attacker to increase his/her Internet anonymity. Internet anonymity depends on the number of proxies used for fetching the target application; the larger the number of proxy servers used, the greater is the attacker's anonymity.

The proxy chaining process is described below:

- The user requests a resource from the destination.
- A proxy client in the user's system connects to a proxy server and passes the request to the proxy server.
- The proxy server strips the user's identification information and passes the request to the next proxy server.
- This process is repeated by all the proxy servers in the chain.
- Finally, the unencrypted request is passed to the web server.

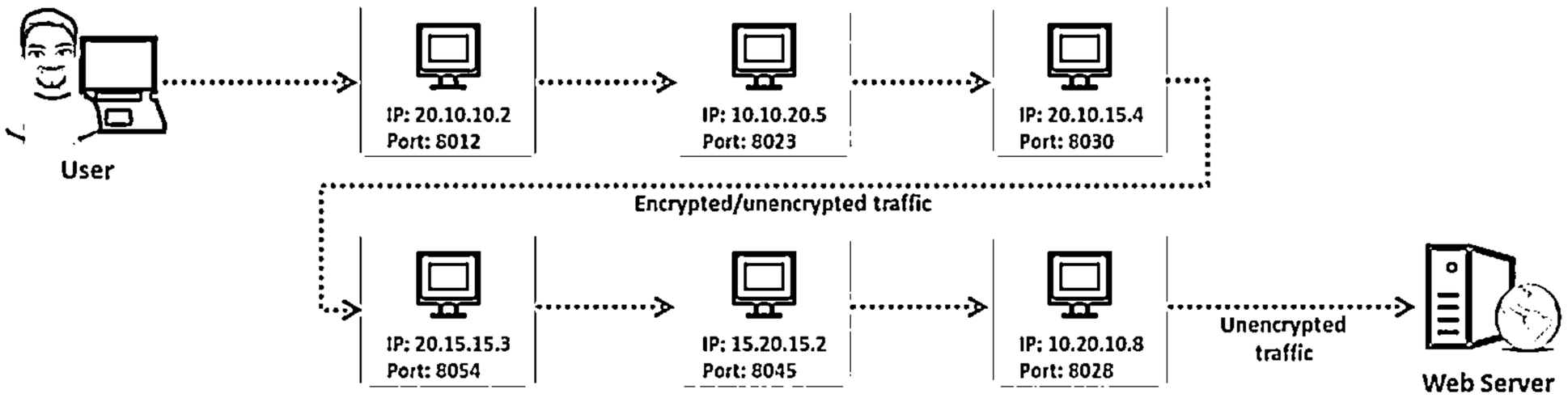
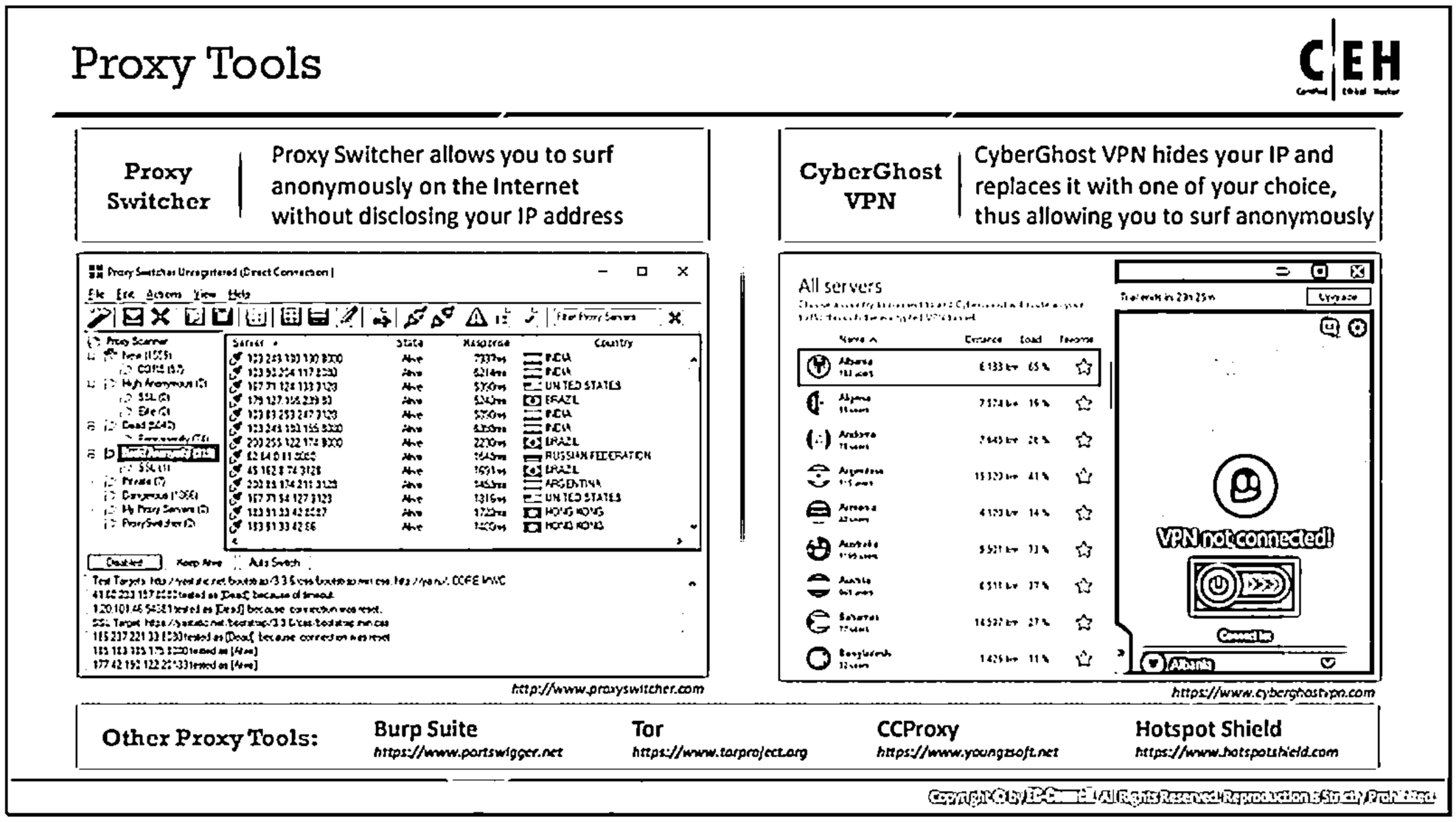


Figure 3.101: Proxy Chaining



Proxy Tools

Proxy tools are intended to allow users to surf the Internet anonymously by keeping their IP hidden through a chain of SOCKS or HTTP proxies. These tools can also act as HTTP, mail, FTP, SOCKS, news, telnet, and HTTPS proxy servers.

- **Proxy Switcher**

  Source: *http://www.proxyswitcher.com*

  Proxy Switcher allows attackers to surf the Internet anonymously without disclosing their IP address. It also helps attackers to access various blocked sites in the organization. In addition, it avoids all sorts of limitations imposed by target sites.

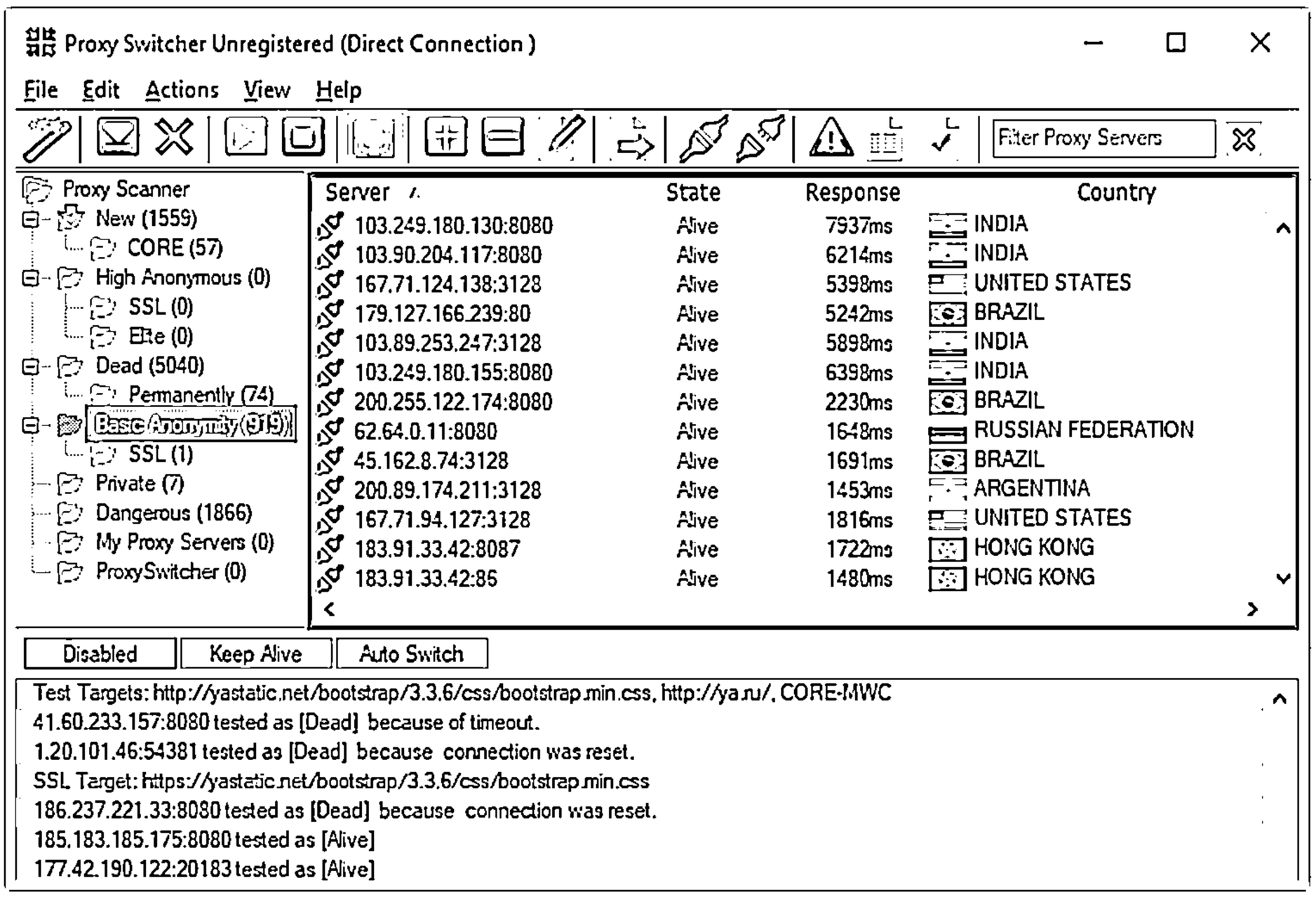


Figure 3.102: Screenshot of Proxy Switcher

- **CyberGhost VPN**

  Source: *https://www.cyberghostvpn.com*

  CyberGhost VPN hides the attacker's IP and replaces it with a selected IP, allowing him or her to surf anonymously and access blocked or censored content. It encrypts the connection and does not keep logs, thus securing data.

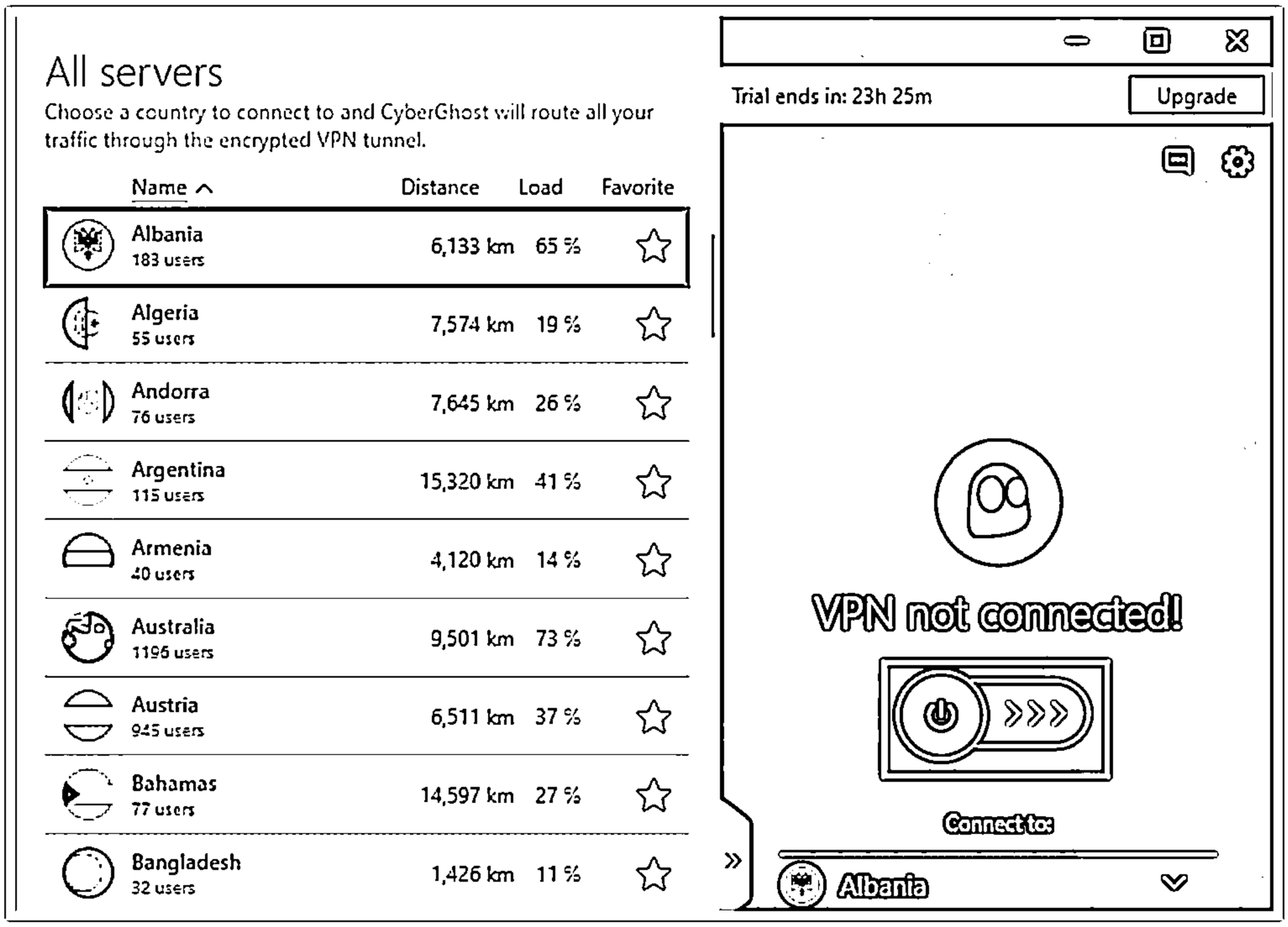
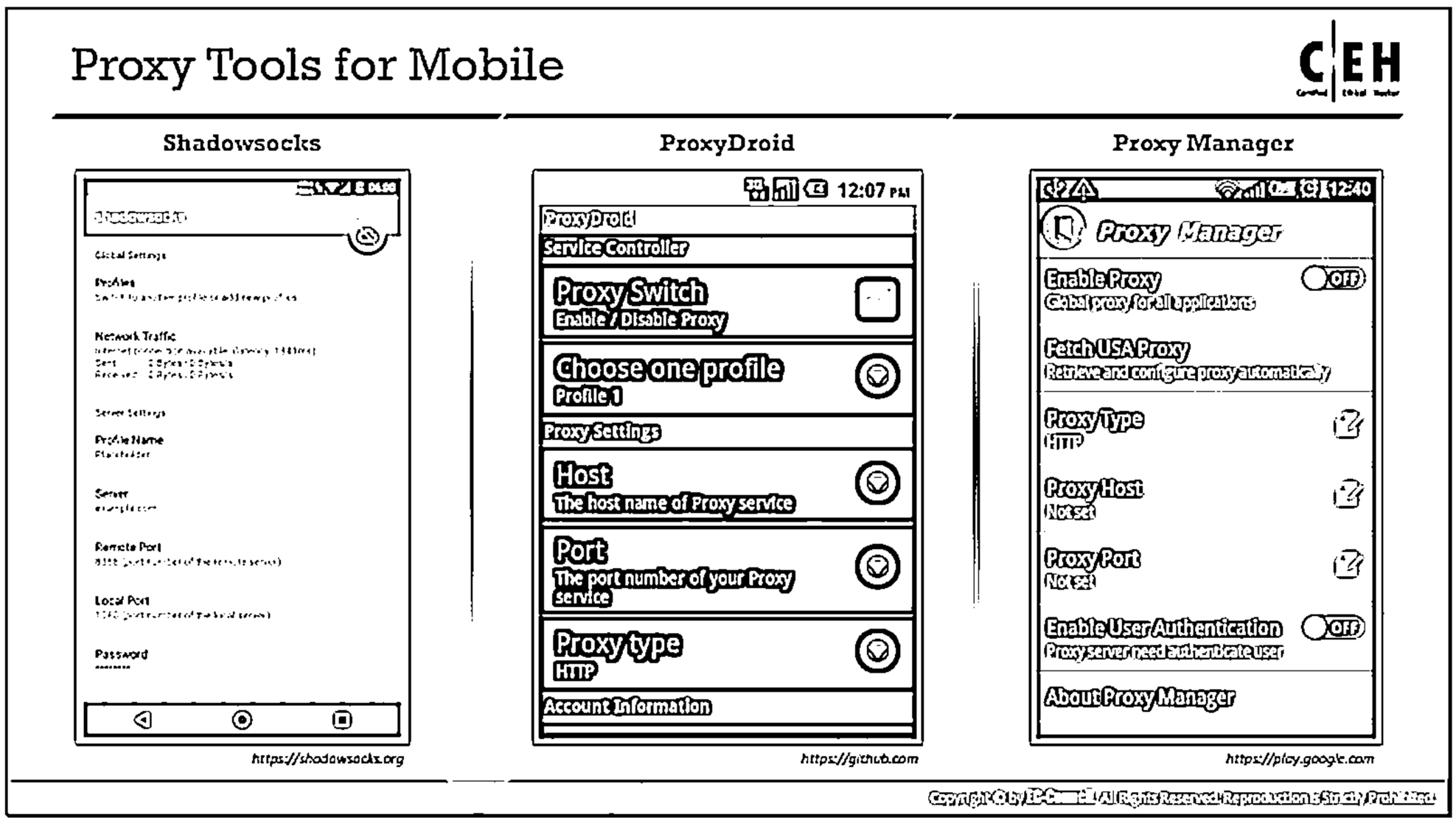


Figure 3.103: Screenshot of CyberGhost

In addition to the proxy tools mentioned above, there are many other proxy tools intended to allow users to surf the Internet anonymously. Some additional proxy tools are listed below:

- Burp Suite (*https://www.portswigger.net*)
- Tor (*https://www.torproject.org*)
- CCProxy (*https://www.youngzsoft.net*)
- Hotspot Shield (*https://www.hotspotshield.com*)



Proxy Tools for Mobile

- **Shadowsocks**

  Source: *https://shadowsocks.org*

  Shadowsocks is a high-performance, cross-platform secured socks5 proxy. It adopts bleeding-edge techniques with asynchronous I/O and event-driven programming. This tool is available on multiple platforms, including PC, MAC, mobile devices (Android and iOS), and routers (OpenWRT). It is a low-resource-consumption tool that is suitable for low-end boxes and embedded devices. It supports open-source implementations in python, node.js, golang, C#, and pure C.

  Shadowsocks help attackers to surf the Internet privately and securely.

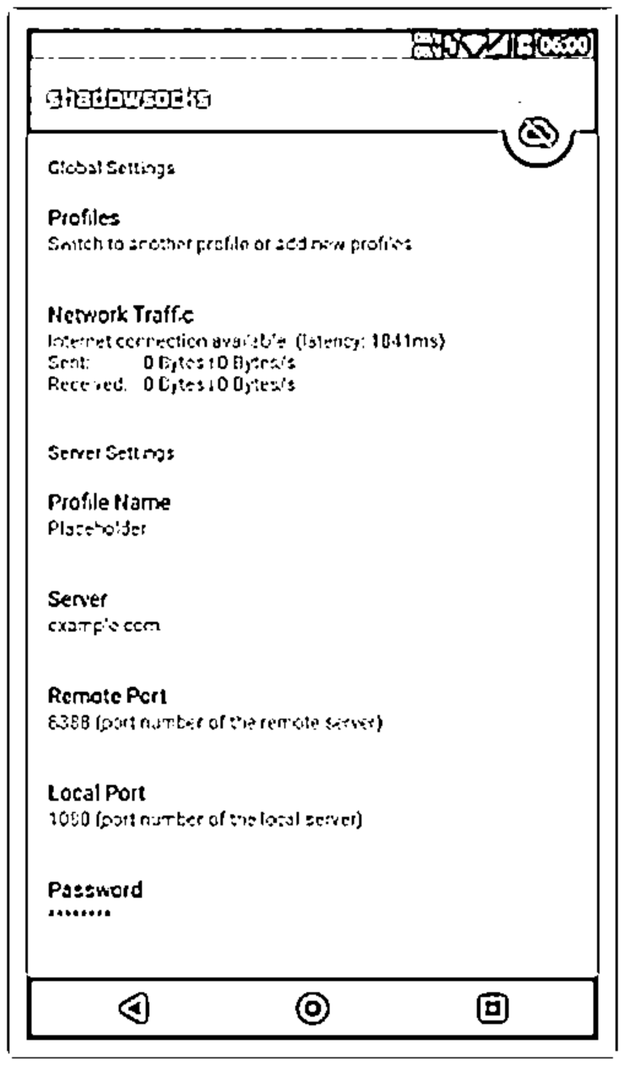


Figure 3.104: Screenshot of Shadowsocks

- **ProxyDroid**

  Source: *https://github.com*

  ProxyDroid is an app that can help you to set the proxy (http/socks4/socks5) on your Android devices. It supports HTTP/HTTPS/SOCKS4/SOCKS5 proxy and also supports basic/NTLM/NTLMv2 authentication methods. Attackers can use this tool as a DNS proxy to access IP addresses that are beyond the firewalls.

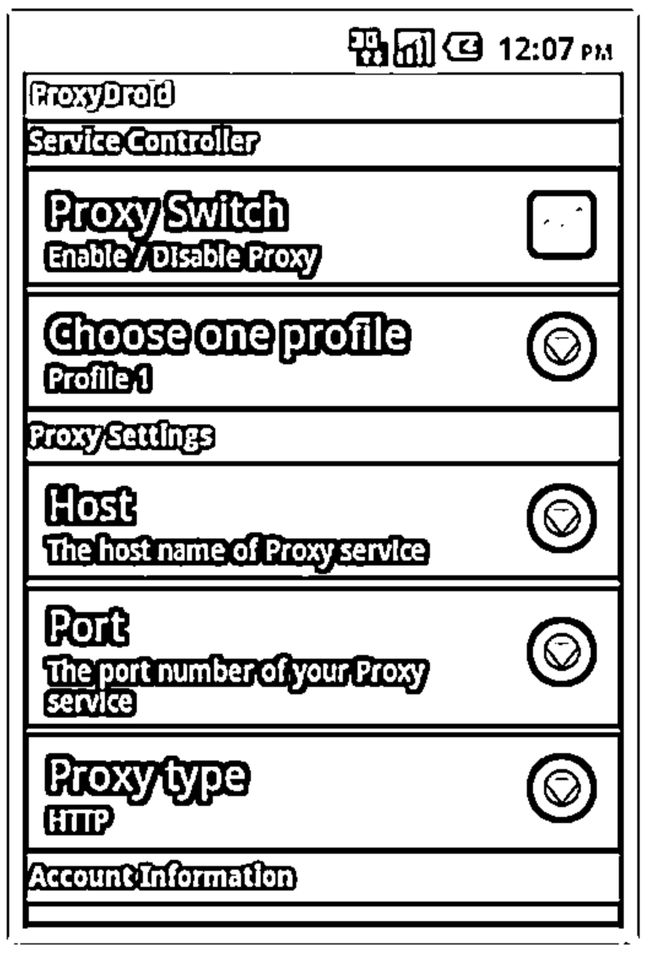


Figure 3.105: Screenshot of ProxyDroid

- **Proxy Manager**

  Source: *https://play.google.com*

  Proxy Manager is another Android-based proxy tool that supports HTTP/SOCKS4/SOCKS5 proxy and user authentication. It enables attackers to surf the Internet anonymously.

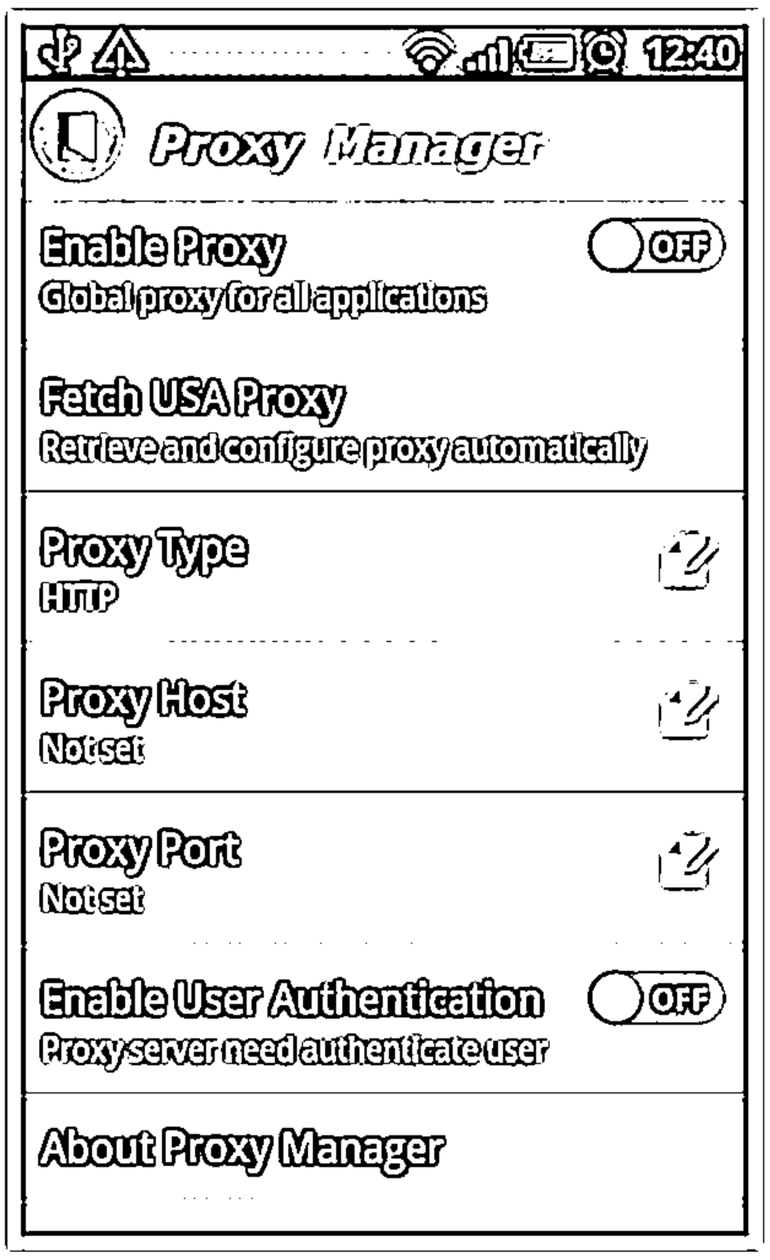
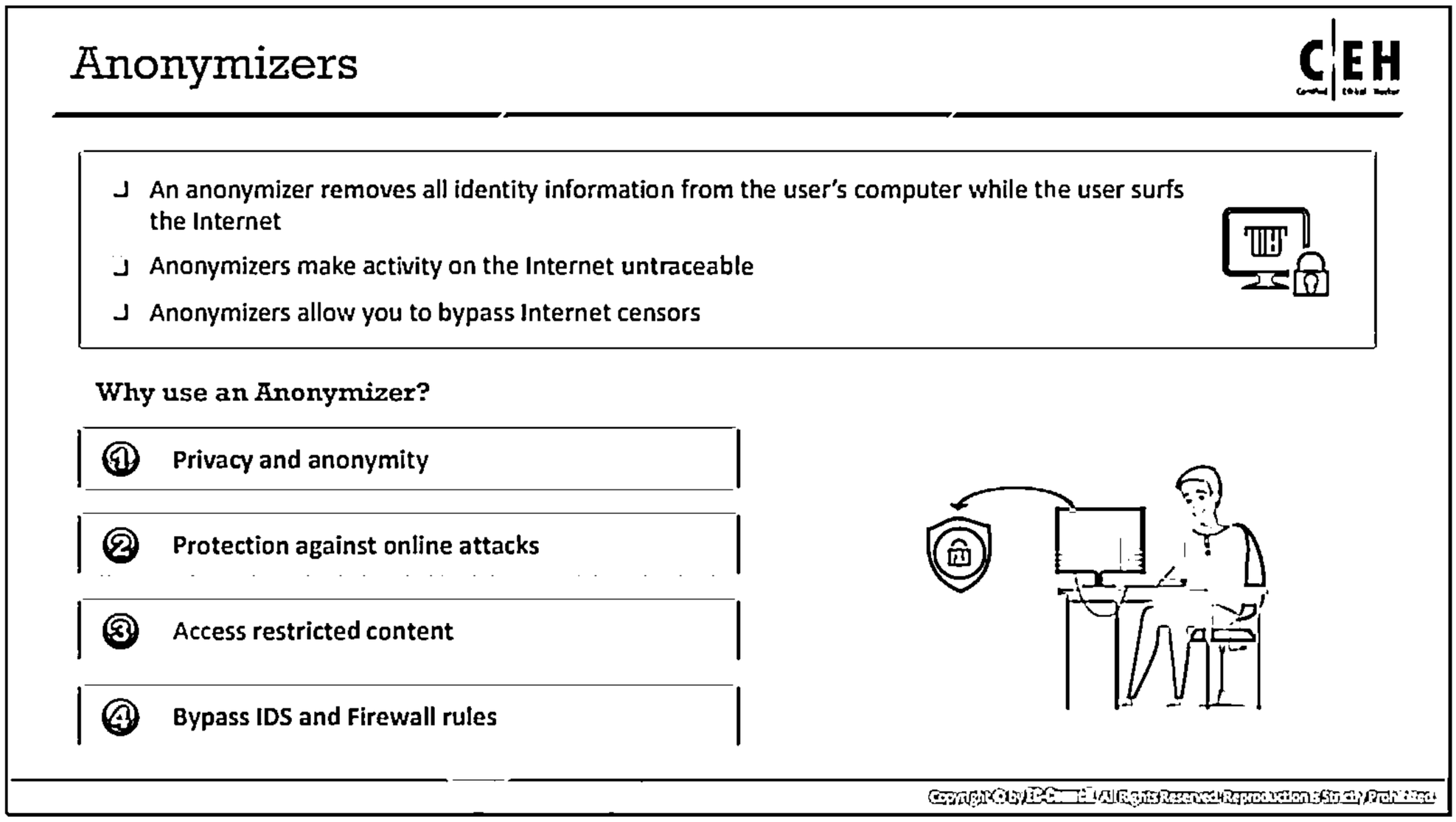


Figure 3.106: Screenshot of Proxy Manager



Anonymizers

An anonymizer is an intermediate server placed between you as the end user and the website to access the website on your behalf and make your web surfing activities untraceable. Anonymizers allows you to bypass Internet censors. An anonymizer eliminates all the identifying information (IP address) from your system while you are surfing the Internet, thereby ensuring privacy. Most anonymizers can anonymize the web (HTTP:), file transfer protocol (FTP:), and gopher (gopher:) Internet services.

To visit a page anonymously, you can visit your preferred anonymizer site and enter the name of the target website in the anonymization field. Alternatively, you can set your browser home page to point to an anonymizer to anonymize subsequent web access. In addition, you can choose to anonymously provide passwords and other information to sites without revealing any additional information, such as your IP address. Attackers may configure an anonymizer as a permanent proxy server by making the site name the setting for the HTTP, FTP, Gopher, and other proxy options in their application configuration menu, thereby cloaking their malicious activities.

Why Use an Anonymizer?

The reasons for using anonymizers include:

- **Ensuring privacy**: Protect your identity by making your web navigation activities untraceable. Your privacy is maintained until and unless you disclose your personal information on the web, for example, by filling out forms.
- **Accessing government-restricted content**: Most governments prevent their citizens from accessing certain websites or content deemed inappropriate or sensitive. However, these sites can still be accessed using an anonymizer located outside the target country.

- **Protection against online attacks**: An anonymizer can protect you from all instances of online pharming attacks by routing all customer Internet traffic via its protected DNS server.
- **Bypassing IDS and firewall rules**: Firewalls are typically bypassed by employees or students accessing websites that they are not supposed to access. An anonymizer service gets around your organization's firewall by setting up a connection between your computer and the anonymizer service. Thus, firewalls see only the connection from your computer to the anonymizer's web address. The anonymizer will subsequently connect to any website (e.g., Twitter) with the help of an Internet connection and then direct the content back to you. To your organization, your system appears to be simply connected to the anonymizer's web address but not to the actual site that you are browsing.

In addition to protecting users' identities, anonymizers can also be used to attack a website without being traced.

Types of Anonymizers

An anonymizer is a service through which one can hide one's identity when using certain Internet services. It encrypts the data from your computer to the Internet service provider. Anonymizers are of two basic types: networked anonymizers and single-point anonymizers.

- **Networked Anonymizers**

  A networked anonymizer first transfers your information through a network of Internet-connected computers before passing it on to the website. Because the information passes through several Internet computers, it becomes cumbersome for anyone trying to track your information to establish the connection between you and the anonymizer.

  Example: If you want to visit any web page, you have to make a request. The request will first pass through A, B, and C Internet computers before going to the website.

  Advantage: Complication of the communications makes traffic analysis complex.

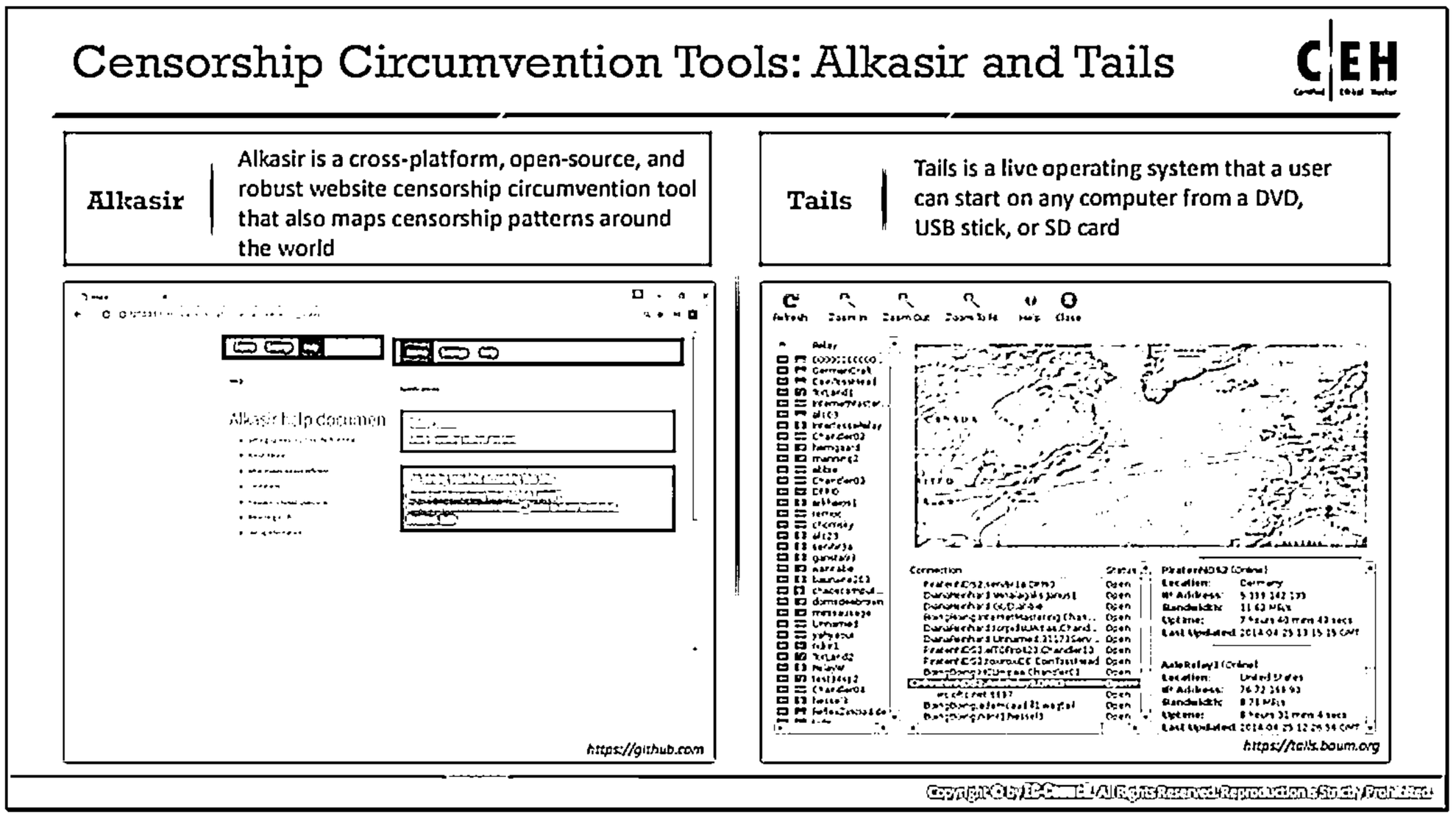
  Disadvantage: Any multi-node network communication incurs some degree of risk of compromising confidentiality at each node.

- **Single-Point Anonymizers**

  Single-point anonymizers first transfer your information through a website before sending it to the target website and then pass back the information gathered from the target website to you via the website to protect your identity.

  Advantage: Arms-length communication hides the IP address and related identifying information.

  Disadvantage: It offers less resistance to sophisticated traffic analysis.



Censorship Circumvention Tools

- Alkasir

  Source: *https://github.com*

  Alkasir is a cross-platform, open-source, and robust website censorship circumvention tool that also maps censorship patterns around the world. Alkasir enables attackers to identify censored links. It keeps them informed about links that are still blocked and links that are not blocked.

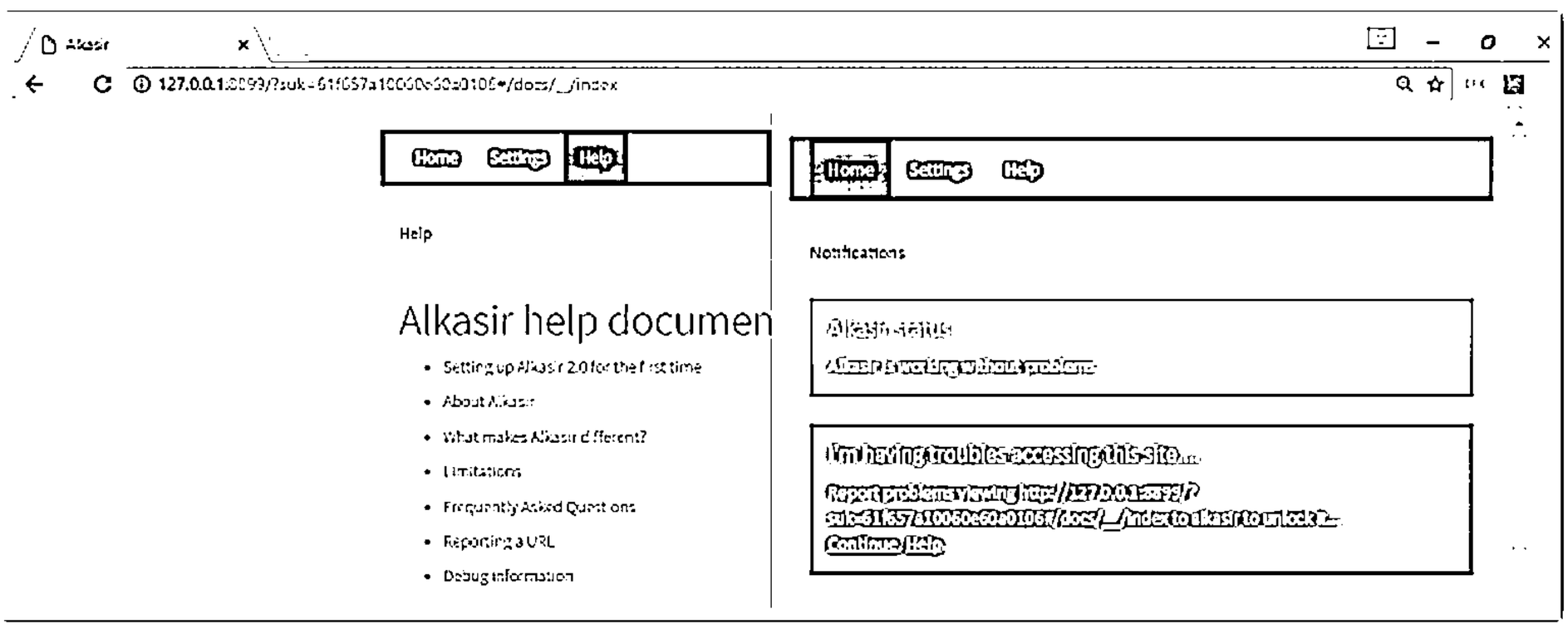


Figure 3.107: Screenshot of Alkasir

- **Tails**

  Source: *https://tails.boum.org*

  Tails is a live OS that users can run on any computer from a DVD drive, USB stick, or SD card. It uses state-of-the-art cryptographic tools to encrypt files, emails, and instant messaging. It allows attackers to use the Internet anonymously and circumvent censorship. It leaves no trace on the computer.

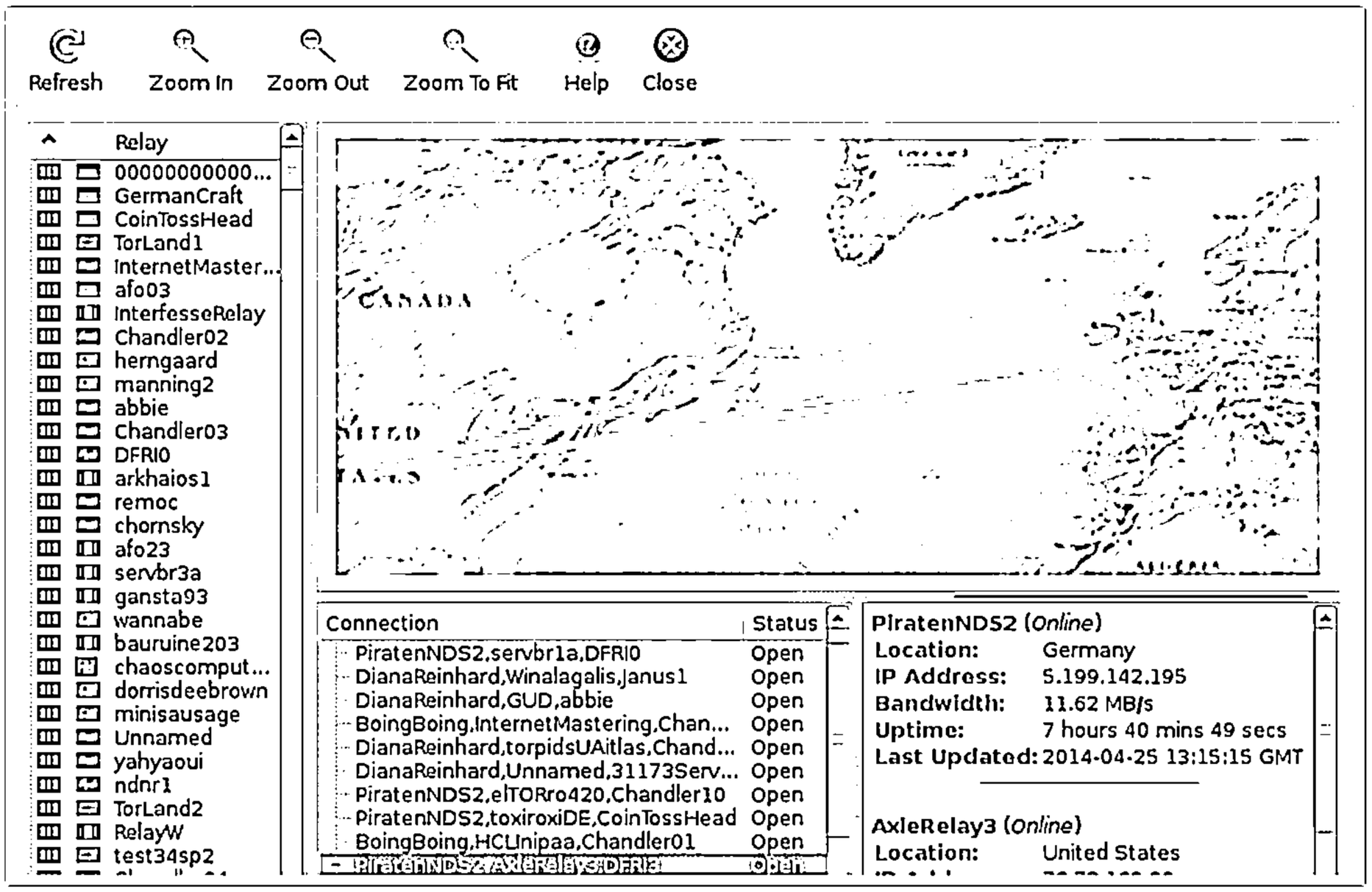
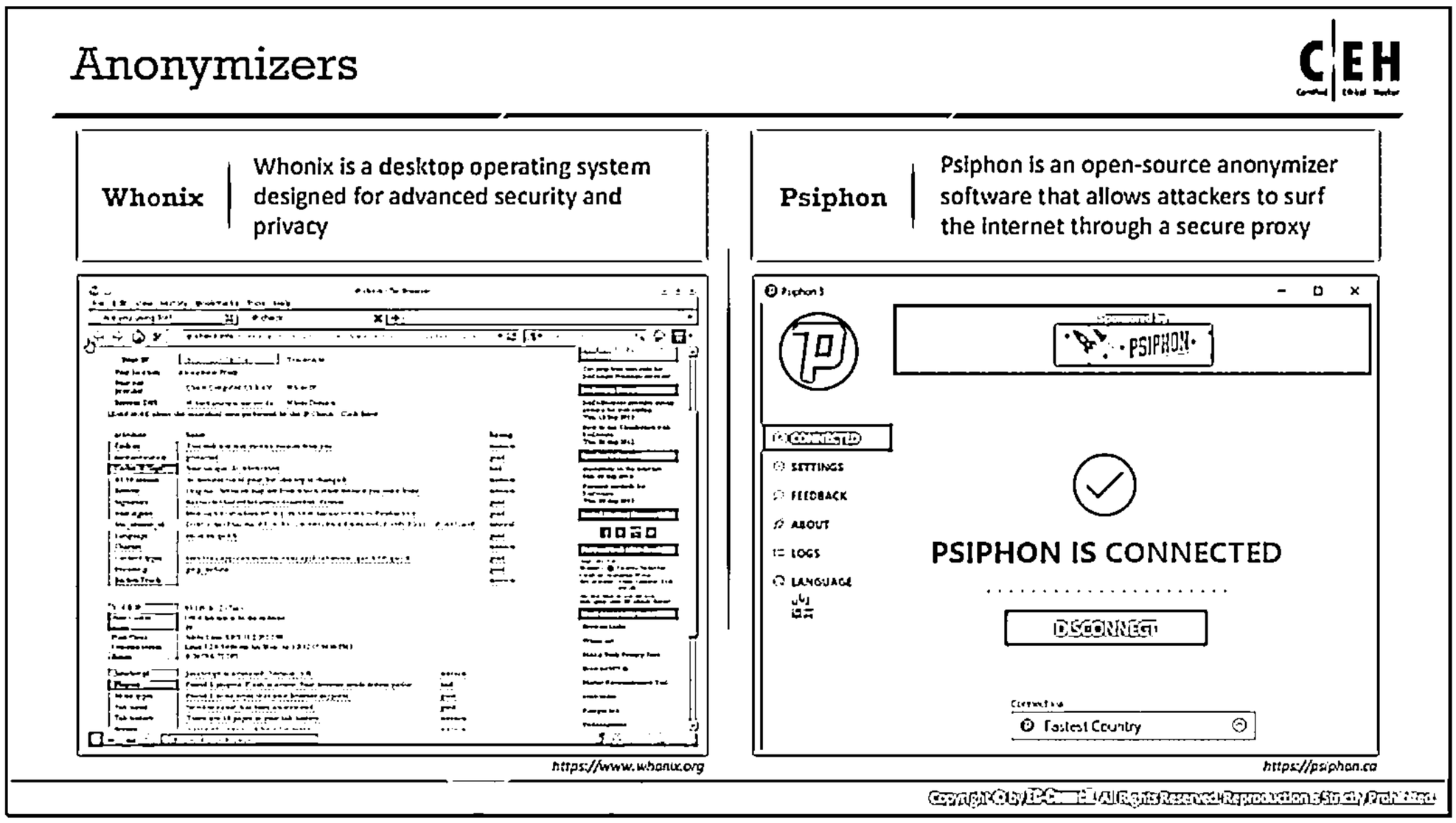


Figure 3.108: Screenshot of Tails



Anonymizers

An anonymizer helps you to mask your IP address so that you can visit websites without being tracked or identified while keeping your activity and identity protected. It uses various techniques such as SSH, VPN, and HTTP proxies, which allow you to access blocked or censored content on the Internet with omitted advertisements.

- **Whonix**

  Source: *https://www.whonix.org*

  Whonix is a desktop OS designed for advanced security and privacy. It mitigates the threat of common attack vectors while maintaining usability. Online anonymity is realized via fail-safe, automatic, and desktop-wide use of the Tor network. It consists of a heavily reconfigured Debian base that is run inside multiple virtual machines, providing a substantial layer of protection from malware and IP address leaks.

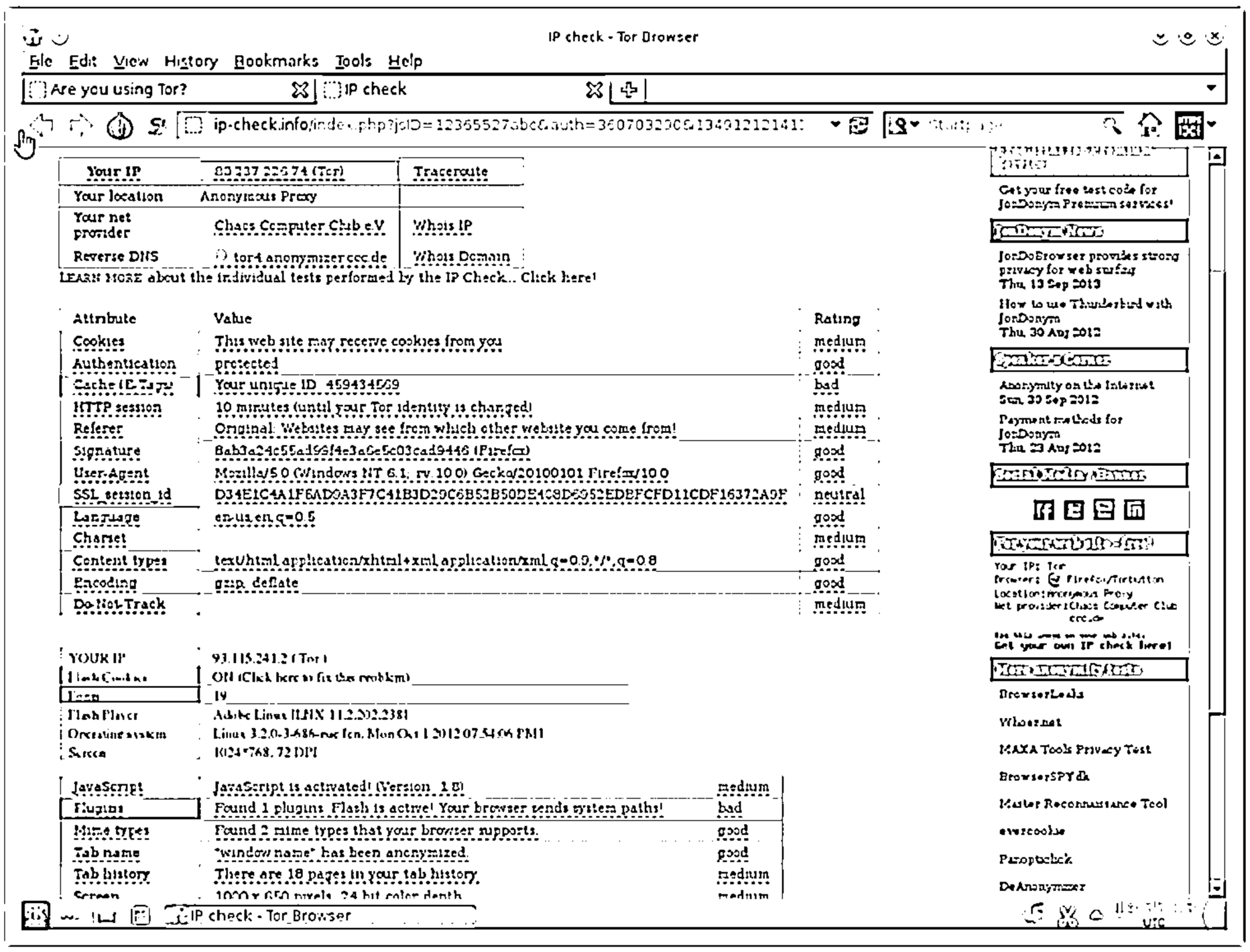


Figure 3.109: Screenshot of Whonix

- **Psiphon**

  Source: *https://psiphon.ca*

  Psiphon is an open-source anonymizer software that allows attackers to surf the Internet through a secure proxy. After installation, it will automatically configure the Windows machine's proxy configurations in such a way that the network traffic for the web applications and browsers that operate through these configurations will be tunneled through Psiphon.

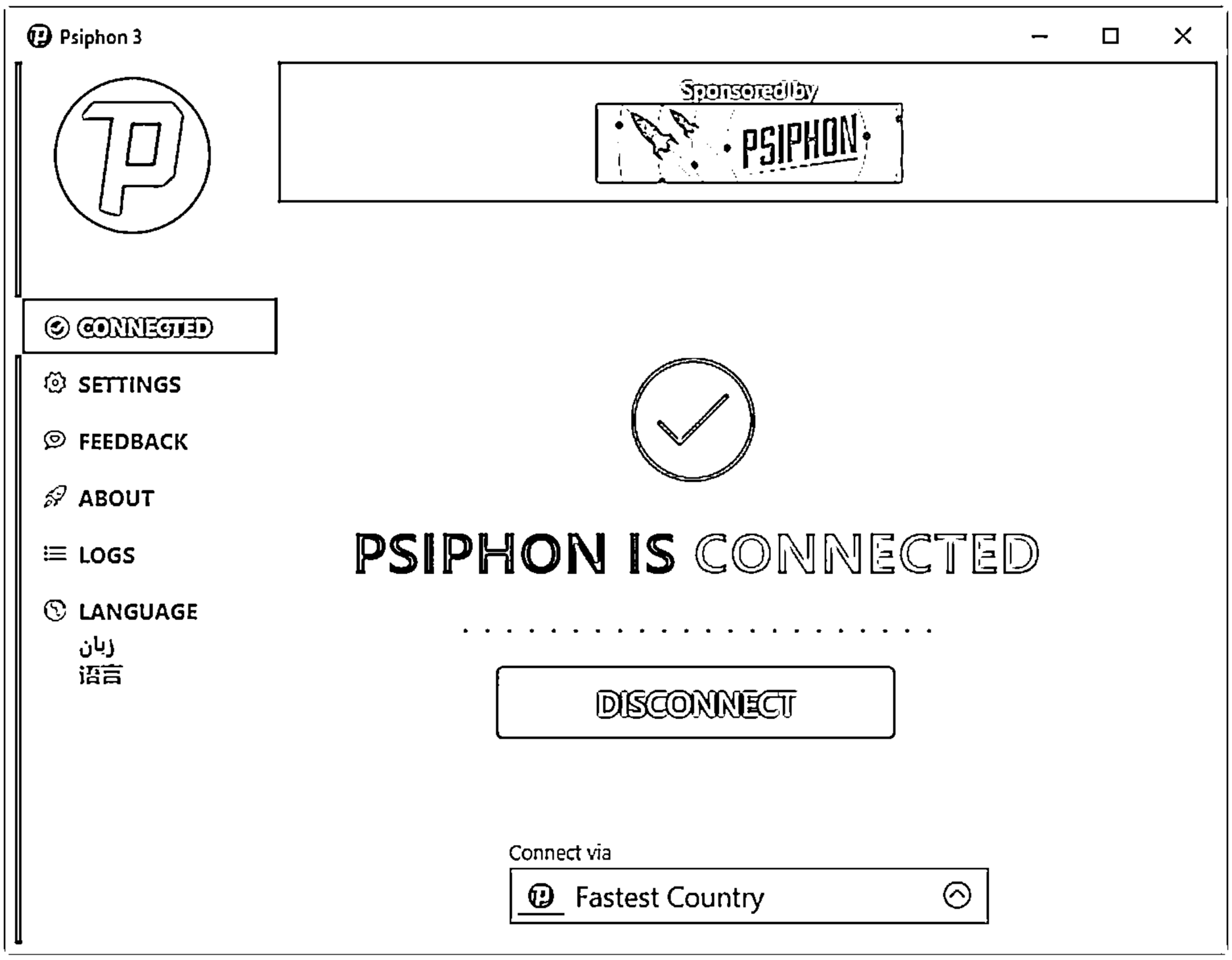
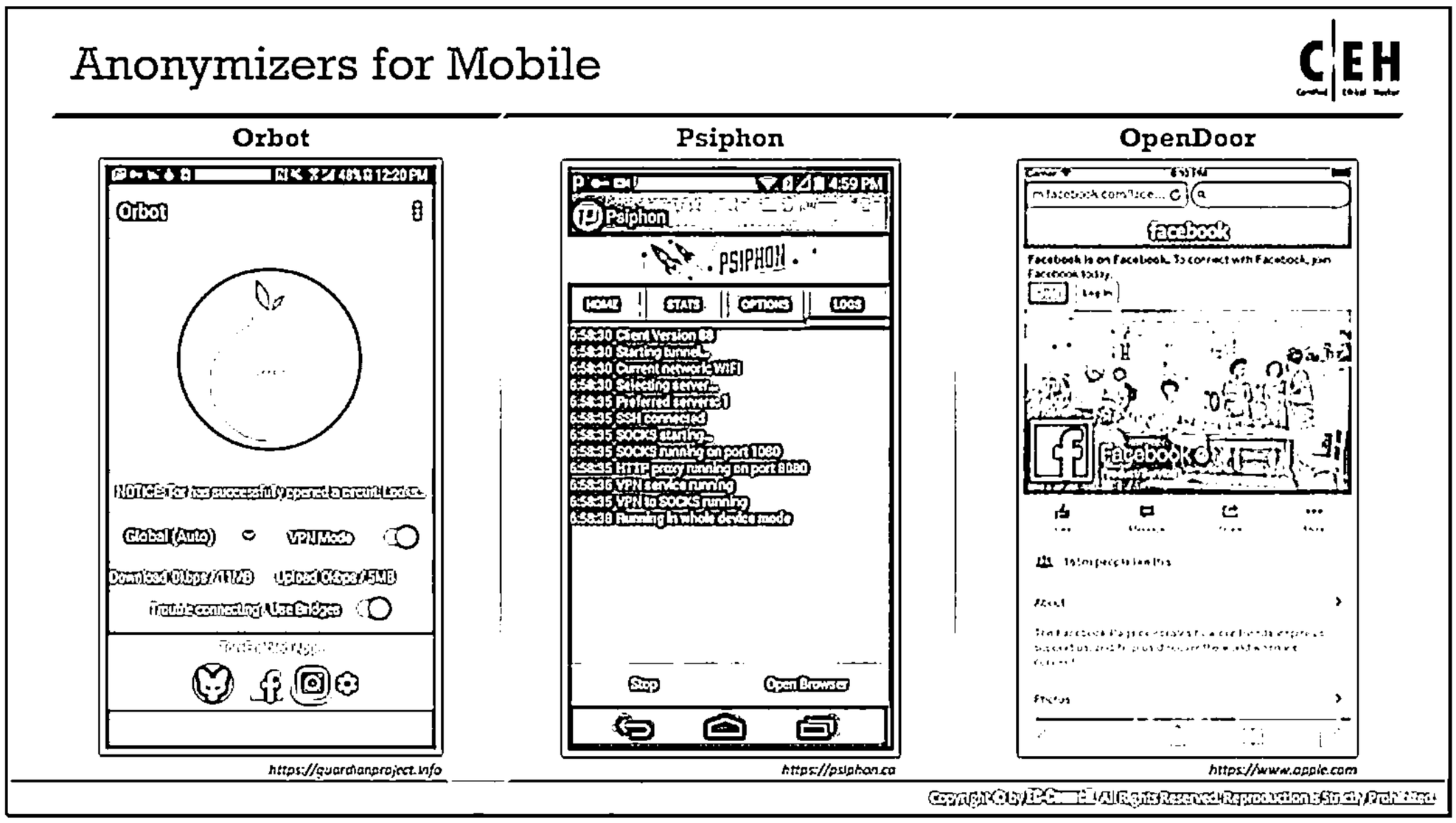


Figure 3.110: Screenshot of Psiphon



Anonymizers for Mobile

- **Orbot**

  Source: *https://guardianproject.info*

  Orbot is a proxy app that allows other apps to use the Internet more securely. It uses Tor to encrypt Internet traffic and then hides it by bouncing through a series of computers around the world. Tor is a free software that provides an open network to help defend your system against any form of network surveillance that may compromise personal freedom and privacy as well as confidential business activities and relationships through a type of state security monitoring known as "traffic analysis." Orbot creates a truly private Internet connection.

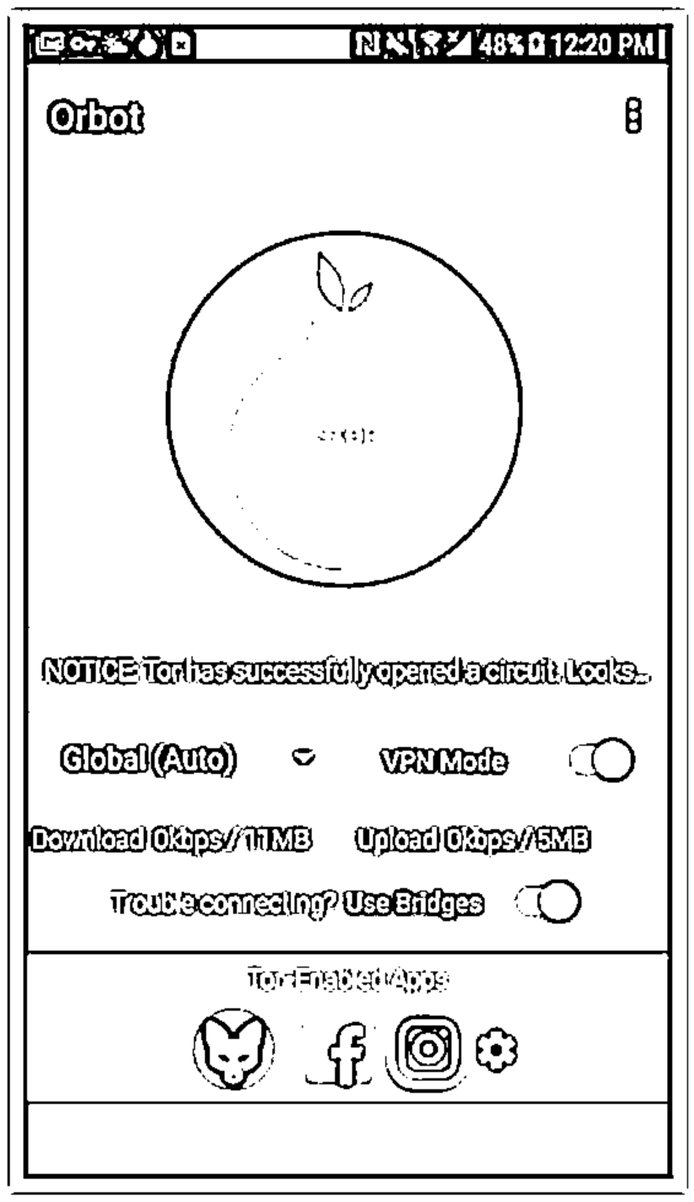


Figure 3.111: Screenshot of Orbot

- **Psiphon**

  Source: *https://psiphon.ca*

  Psiphon is a circumvention tool developed by Psiphon, Inc., which uses VPN, SSH, and HTTP proxy technology to provide you with open and uncensored access to Internet content. However, Psiphon does not increase online privacy and is not an online security tool.

  Features:

  - **Browser** or **VPN** (whole-device) **mode:** one can choose whether to tunnel everything or just the web browser.
  - **In-app stats**: This lets you know how much traffic you have been using.

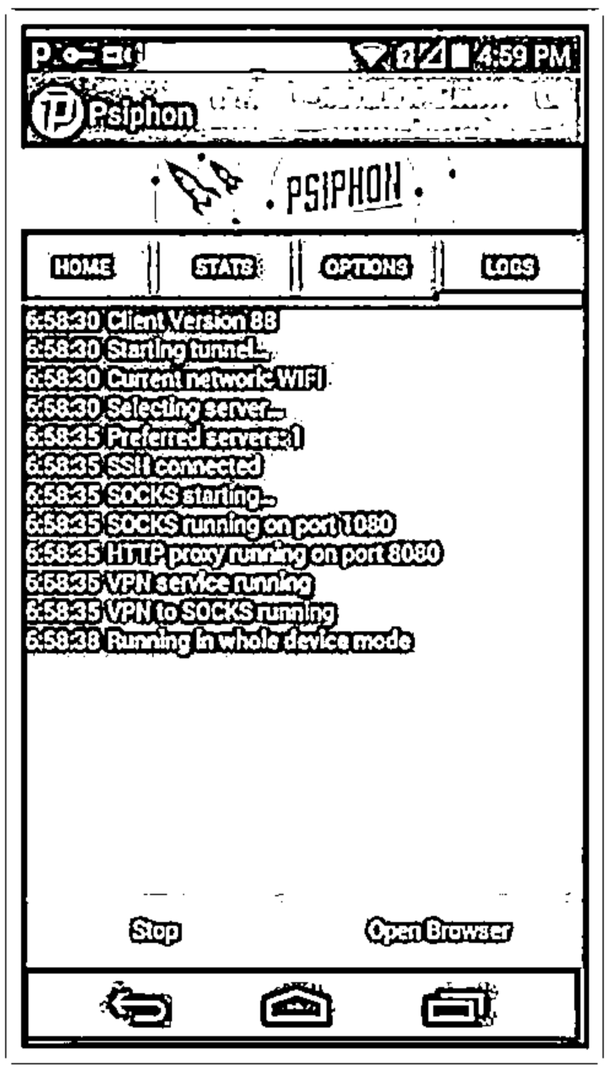


Figure 3.112: Screenshot of Psiphon

- **OpenDoor**

  Source: *https://www.apple.com*

  OpenDoor is an app designed for both iPhone and iPad; it allows attackers to browse websites smoothly and anonymously.

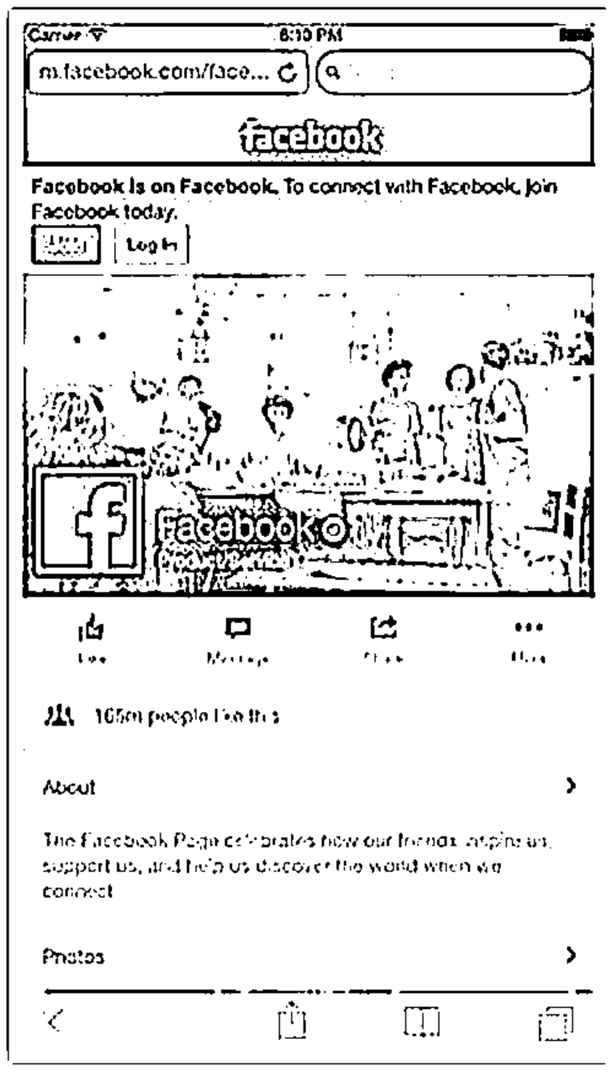


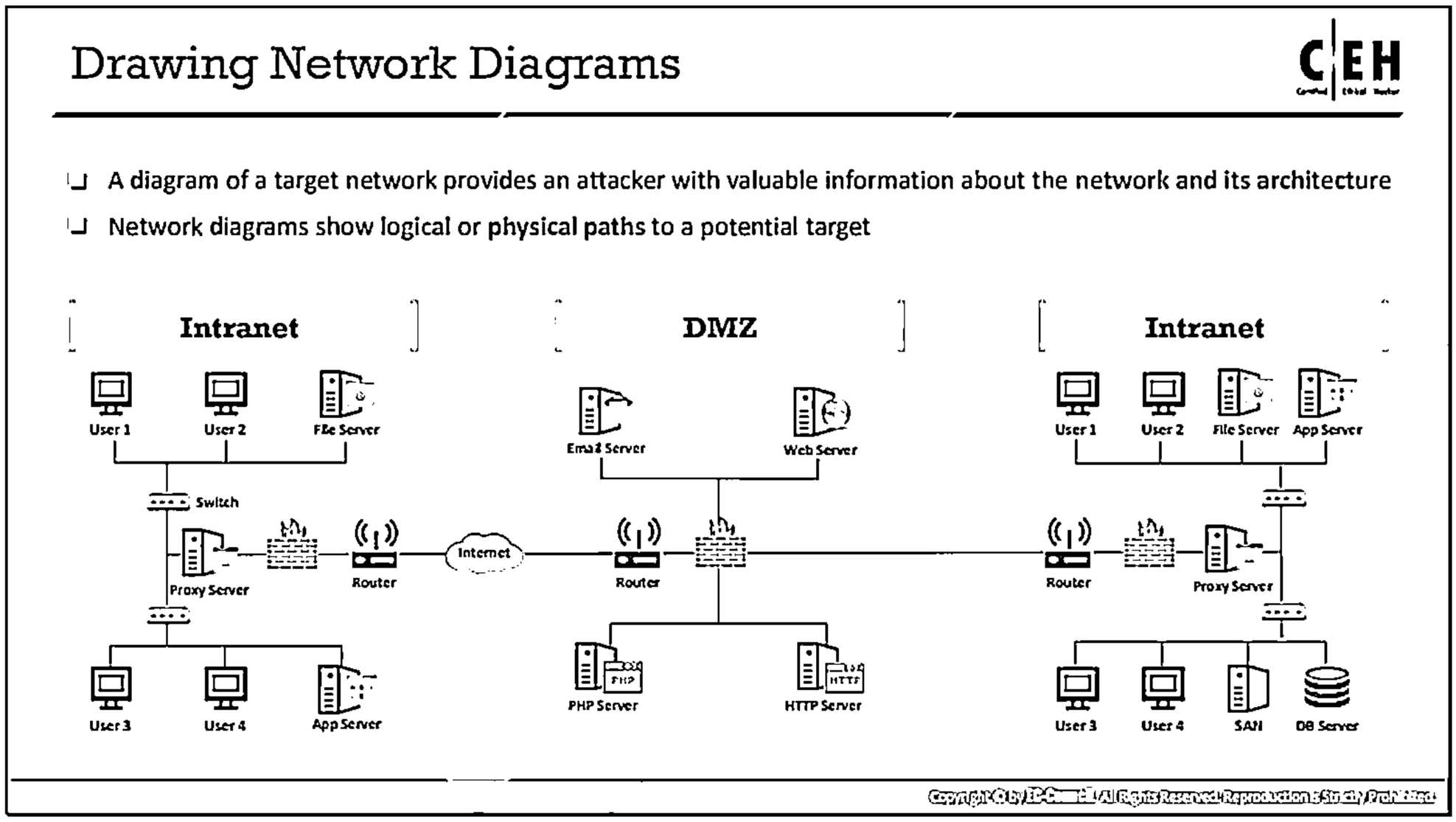
Figure 3.113: Screenshot of OpenDoor

Module Flow

1. Network Scanning Concepts
2. Scanning Tools
3. Host Discovery
4. Port and Service Discovery
5. OS Discovery (Banner Grabbing/ OS Fingerprinting)
6. Scanning Beyond IDS and Firewall
7. Draw Network Diagrams

Draw Network Diagrams

A network diagram helps in analyzing the complete network topology. This section highlights the importance of network diagrams, how to draw them, how an attacker uses them to launch an attack, and the tools used for drawing them.



Drawing Network Diagrams

Drawing a network diagram helps an attacker to identify the topology or architecture of a target network. The network diagram also helps to trace the path to the target host in the network and enables the attacker to understand the positions of firewalls, IDS, routers, and other access control devices. Once the attacker has this information, he/she can try to find the vulnerabilities or weak points in these security mechanisms. Then, the attacker can exploit these weaknesses to find his/her way into the victim's network.

The network diagram also helps network administrators to manage their networks. Attackers use network discovery or mapping tools to draw network diagrams of target networks. An example of a network diagram is shown below.

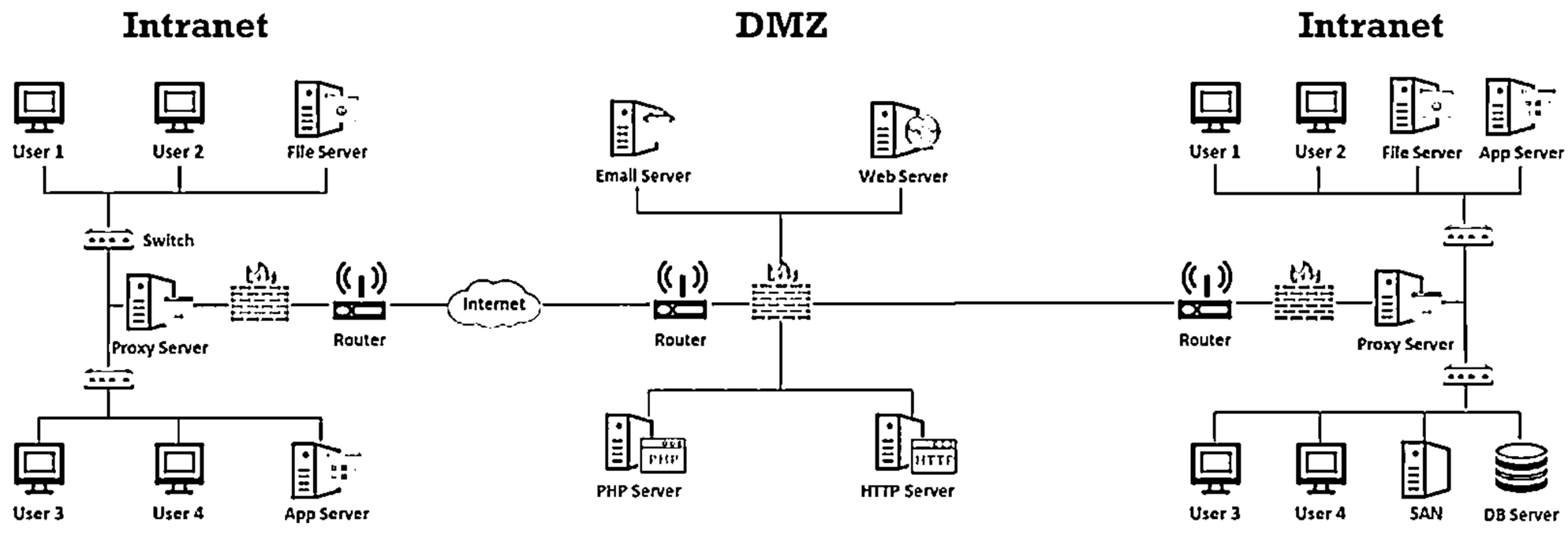
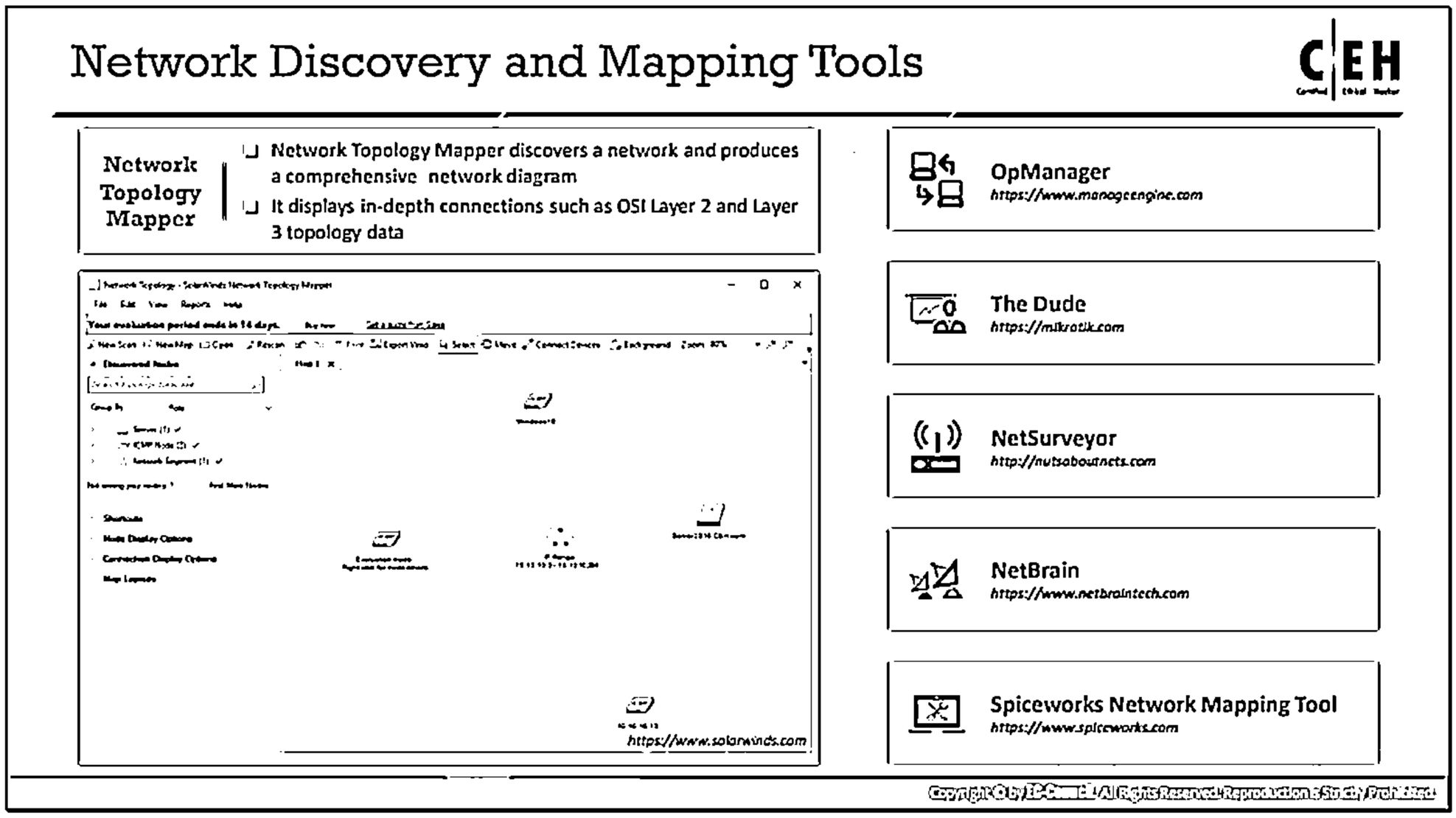


Figure 3.114: Example of Network Diagram



Network Discovery and Mapping Tools

Network discovery and mapping tools allow you to view the map of your network. They help you to detect rogue hardware and software violations and notify you whenever a particular host becomes active or goes down. Thus, you can also determine server outages or problems related to performance. An attacker can use the same tools to draw a diagram of the target network, analyze the topology, find the vulnerabilities or weak points, and launch an attack by exploiting these weak points.

- **Network Topology Mapper**

  Source: *https://www.solarwinds.com*

  The Network Topology Mapper tool allows one to automatically discover and create a network map of the target network. It can also display in-depth connections such as OSI Layer 2 and Layer 3 topology data (e.g., switch-to-switch, switch-to-node, and switch-to-router connections). It can keep track of network changes and allow the user to perform inventory management of hardware and software assets.

  Features:

  - **Network topology discovery and mapping**

    Automatically discovers the entire network and creates comprehensive and detailed network maps

  - **Export network diagrams to Visio**

    Exports network diagrams to Microsoft Office® Visio®, Orion Network Atlas, PDF, and PNG formats

- **Network mapping for regulatory compliance**

  Allows one to directly address PCI compliance and other regulations that require maintenance of an up-to-date network diagram

- **Multi-level network discovery**

  Performs multi-level network discovery to produce an integrated OSI Layer 2 and Layer 3 network map that includes detailed device information

- **Auto-detection of changes to network topology**

  Automatically detects new devices and changes to a network topology with scheduled network scanning

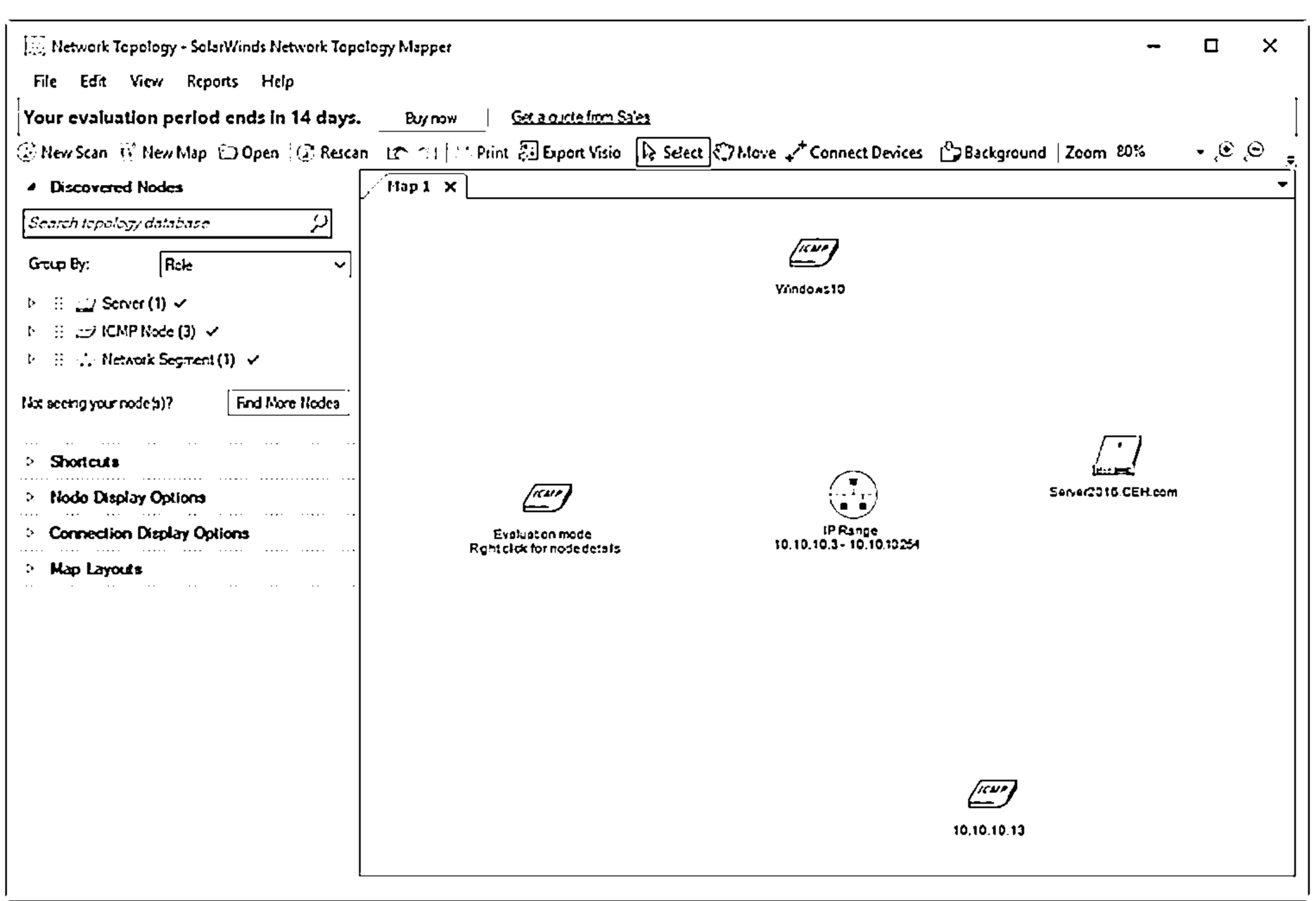
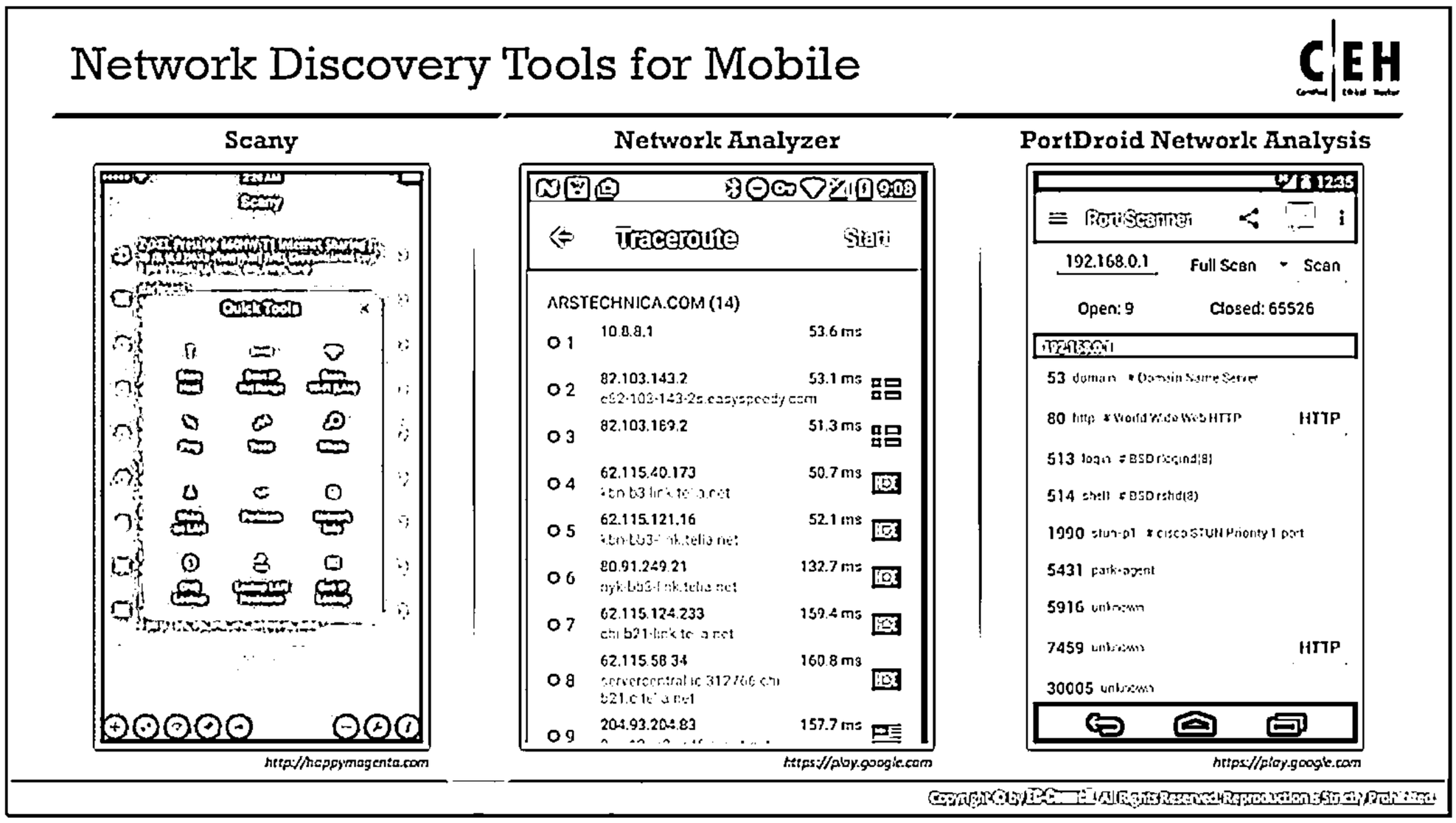


Figure 3.115: Screenshot of SolarWinds Network Topology Mapper

Some network discovery and mapping tools that an attacker can use to create a network map are listed below:

- OpManager (*https://www.manageengine.com*)
- The Dude (*https://www.mikrotik.com*)
- NetSurveyor (*http://nutsaboutnets.com*)
- NetBrain (*https://www.netbraintech.com*)
- Spiceworks Network Mapping Tool (*https://www.spiceworks.com*)



Network Discovery Tools for Mobile

Some network discovery tools for mobile devices are as follows:

- **Scany**

  Source: *http://happymagenta.com*

  Scany, a network scanner app for iPhone and iPad, scans LAN, Wi-Fi networks, websites, and open ports, discovers network devices, and digs network info. It supports several networking protocols and anti-stealth technologies. It is a multifunctional networking instrument for finding connected devices, looking up detailed device information, network troubleshooting, scanning ports, and testing network security and firewalls.

  Attackers use this tool to scan both the LAN and the Internet, scan any IP address or network range, perform hostname, device name, MAC address, and hardware vendor lookups, ping/trace hosts with integrated tools and WHOIS hostnames, IP addresses, ASNs, etc.

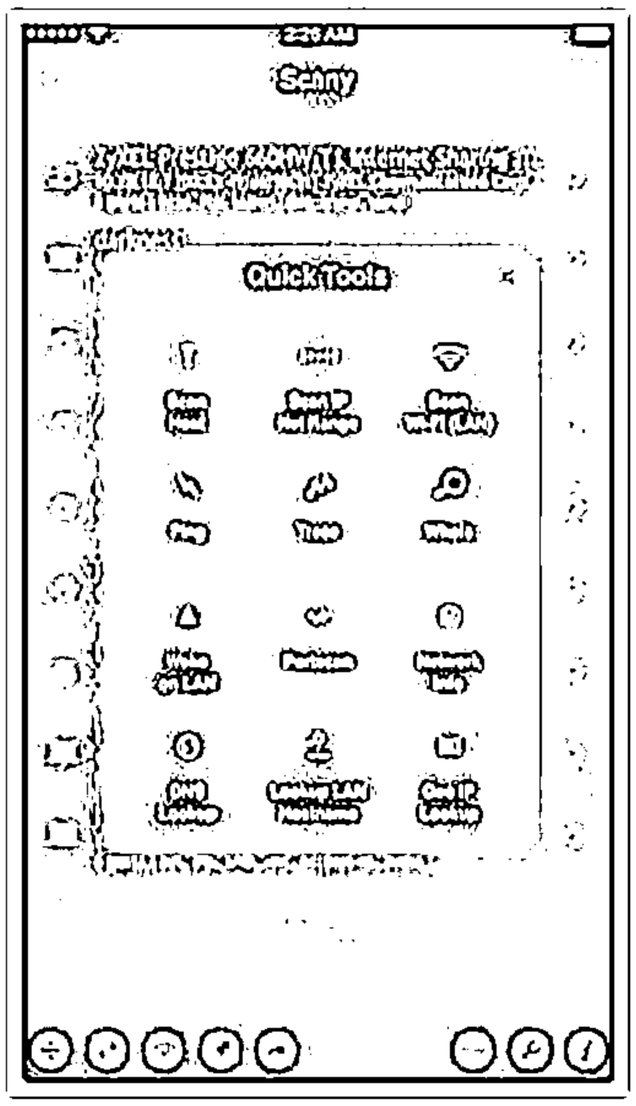


Figure 3.116: Screenshot of Scany

- **Network Analyzer**

  Source: *https://play.google.com*

  Network Analyzer can diagnose various problems in the Wi-Fi network setup or Internet connectivity, and it can also detect various issues in remote servers based on its wide range of in-built tools. Attackers can use it to perform ping, traceroute, port scanning, Whois, and DNS lookup activities.

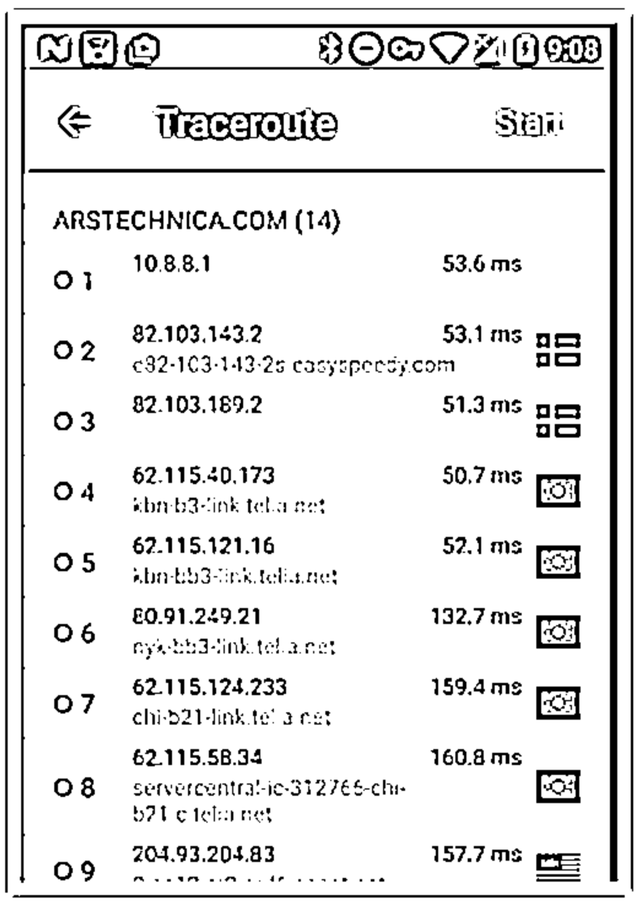


Figure 3.117: Screenshot of Network Analyzer

- **PortDroid Network Analysis**

  Source: *https://play.google.com*

  Attackers can use PortDroid Network Analysis to perform local network discovery. It is also effective in analyzing the network and performing port scanning as well as banner grabbing using certain protocols, including ssh, telnet, http, https, ftp, smb, etc.

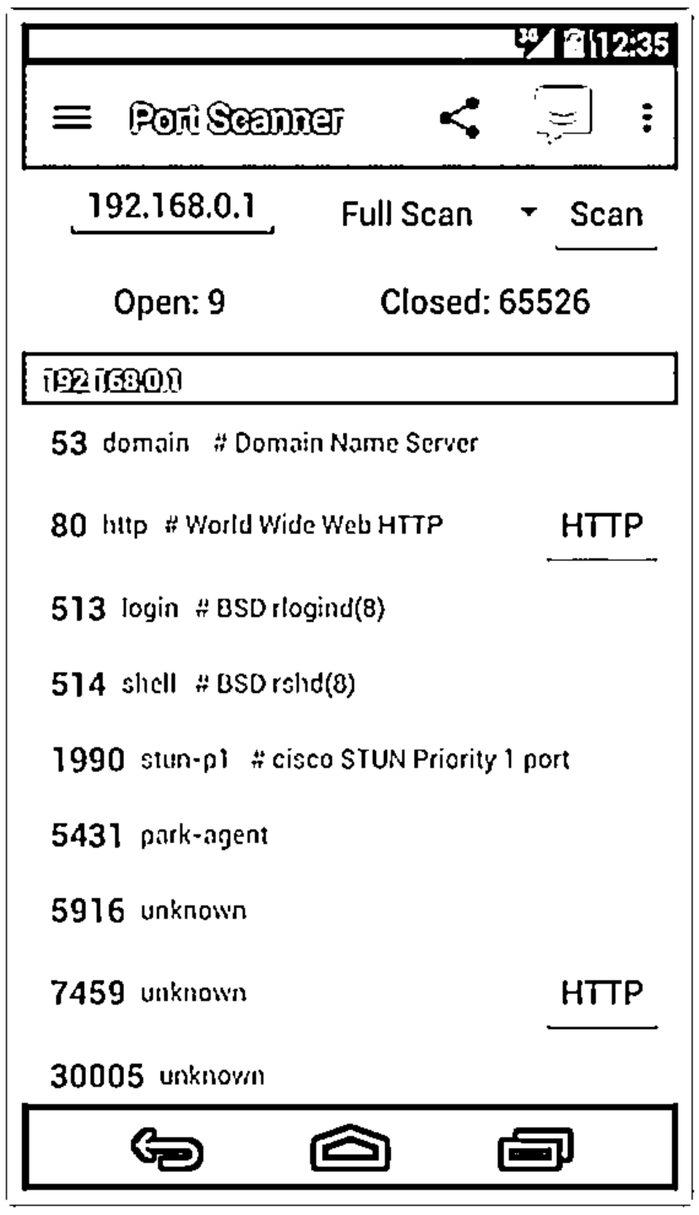


Figure 3.118: Screenshot of Network Analyzer

Module Summary

- In this module, we have discussed the following:
  - How attackers discover live hosts from a range of IP addresses by sending various ping scan requests to multiple hosts
  - How attackers perform different scanning techniques to determine open ports, services, service versions, etc. on the target system
  - How attackers perform banner grabbing or OS fingerprinting to determine the operating system running on a remote target system
  - Various scanning techniques that attackers can employ to bypass IDS/firewall rules and logging mechanisms, and disguise themselves as regular network traffic
  - Drawing diagrams of target networks and their significance in providing valuable information about a network and its architecture to an attacker
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform enumeration to collect information about a target before an attack or audit

Module Summary

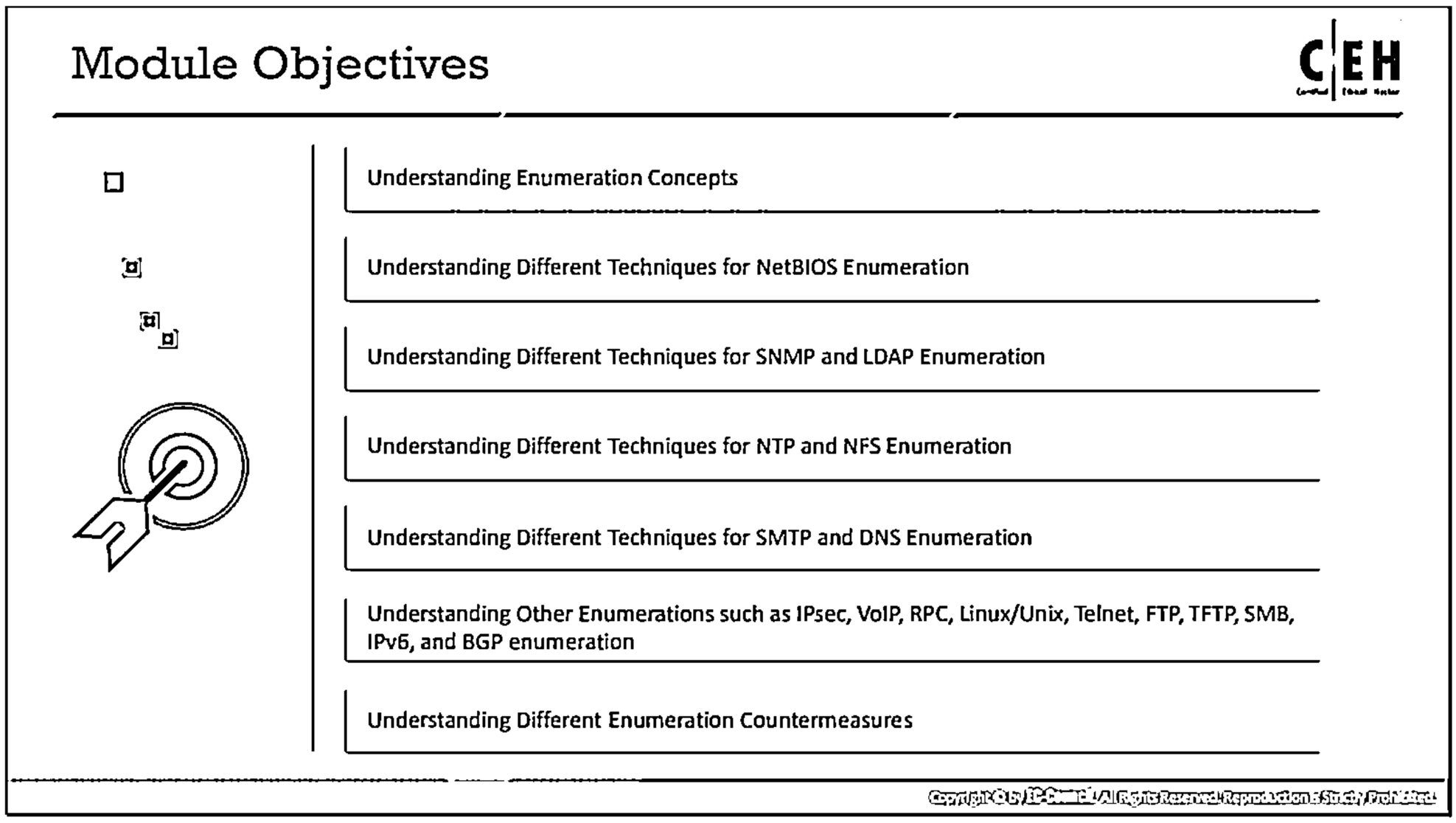
This module discussed how attackers determine live hosts from a range of IP addresses by sending various ping scan requests to multiple hosts. It also described how attackers perform different scanning techniques to determine open ports, services, service versions, etc., on the target system. Furthermore, it explained how attackers perform banner grabbing or OS fingerprinting to determine the OS running on a remote target system. It also illustrated various scanning techniques that attackers can adopt to bypass IDS/firewall rules and logging mechanisms and hide themselves as usual under network traffic. Finally, it ended with a detailed discussion on drawing the target's network diagram and its significance in providing valuable information about the network and its architecture to an attacker.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers perform enumeration to collect information about a target before an attack or audit.

C|EH™

Certified Ethical Hacker

Module 04: Enumeration



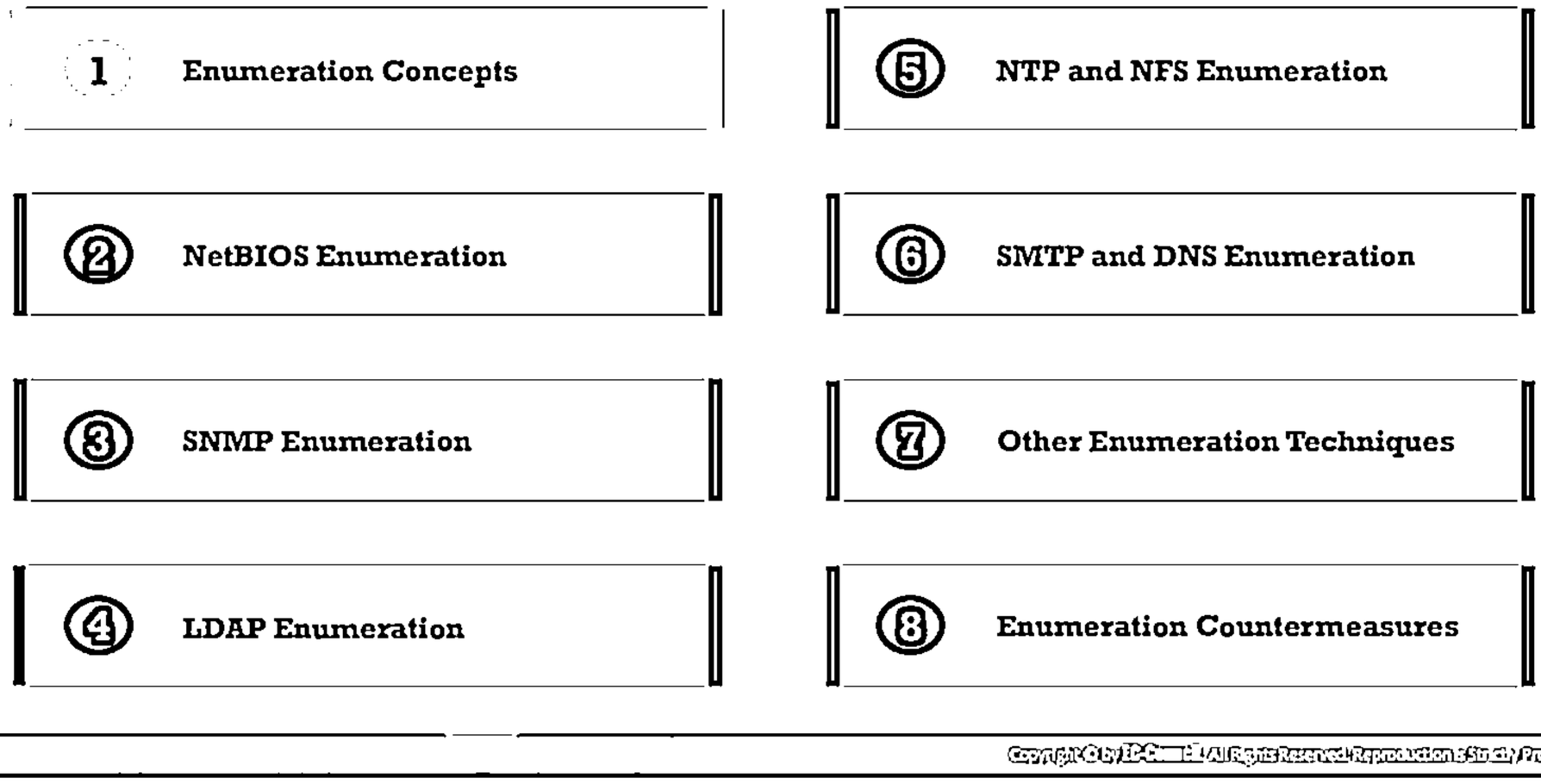
Module Objectives

In the previous modules, you learned about footprinting and network scanning. This module covers the next phase, enumeration. We start with an introduction to enumeration concepts. Subsequently, the module provides insight into different techniques for Network Basic Input/Output System (NetBIOS), Simple Network Management Protocol (SNMP), Lightweight Directory Access Protocol (LDAP), Network Time Protocol (NTP), Network File System (NFS), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Internet Protocol Security (IPsec), Voice over Internet Protocol (VoIP), remote procedure call (RPC), Linux/Unix, Telnet, File Transfer Protocol (FTP), Trivial FTP (TFTP), Server Message Block (SMB), Internet Protocol version 6 (IPv6), and Border Gateway Protocol (BGP) enumeration. The module ends with an overview of enumeration countermeasures.

At the end of this module, you will be able to:

- Describe enumeration concepts
- Explain different techniques for NetBIOS enumeration
- Explain different techniques for SNMP enumeration
- Explain different techniques for LDAP enumeration
- Explain different techniques for NTP enumeration
- Explain different techniques for NFS enumeration
- Explain different techniques for SMTP and DNS enumeration
- Explain other enumeration techniques such as IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration
- Apply enumeration countermeasures

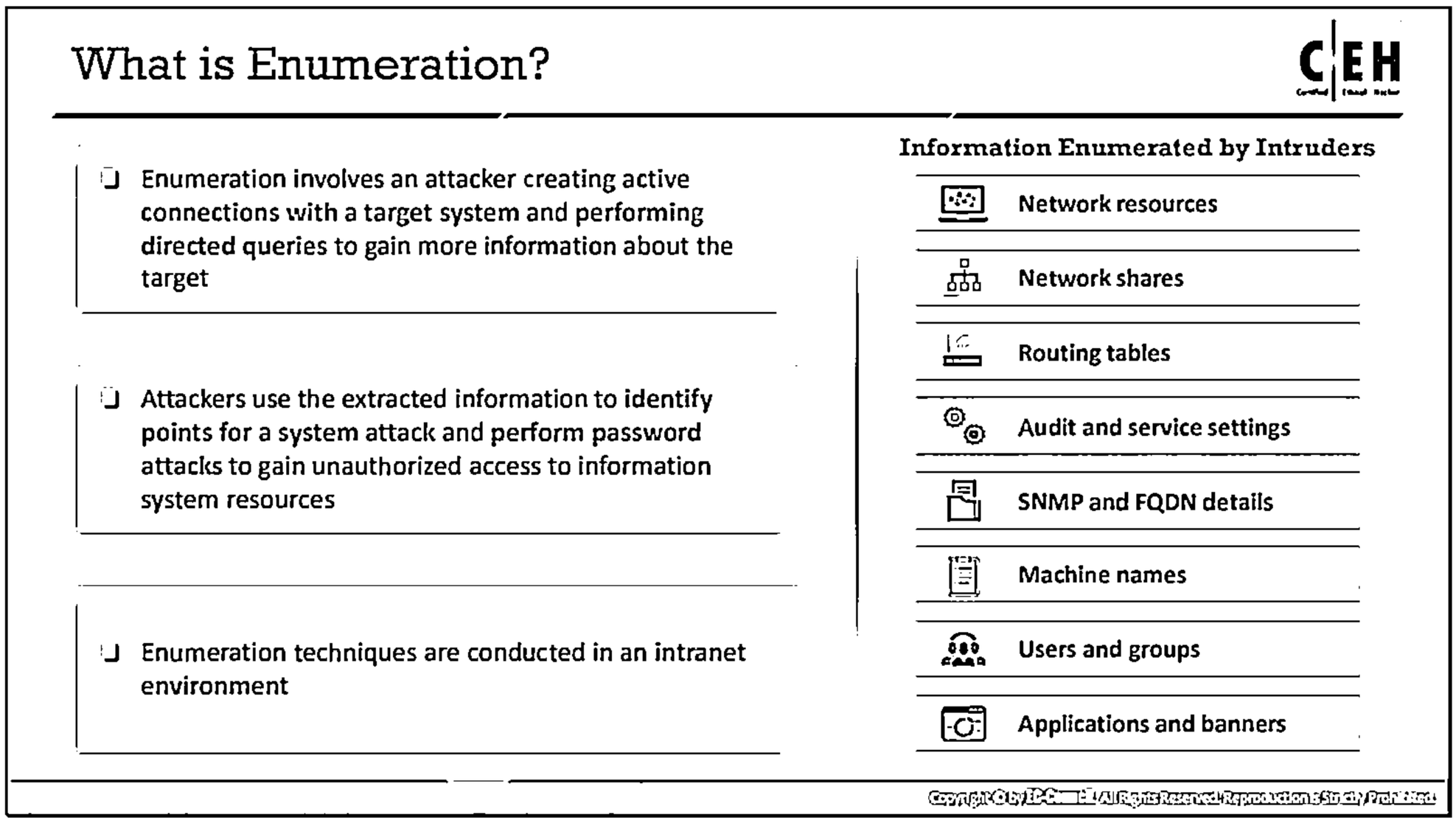
Module Flow



Enumeration Concepts

In the enumeration phase, attackers enumerate usernames and other information on the groups, network shares, and services of networked computers. This information helps attackers identify vulnerabilities in the target network and exploit them to hack the system.

Different sections of this module deal with the enumeration of different services and ports. Before discussing the actual enumeration process, we introduce concepts related to enumeration.



What is Enumeration?

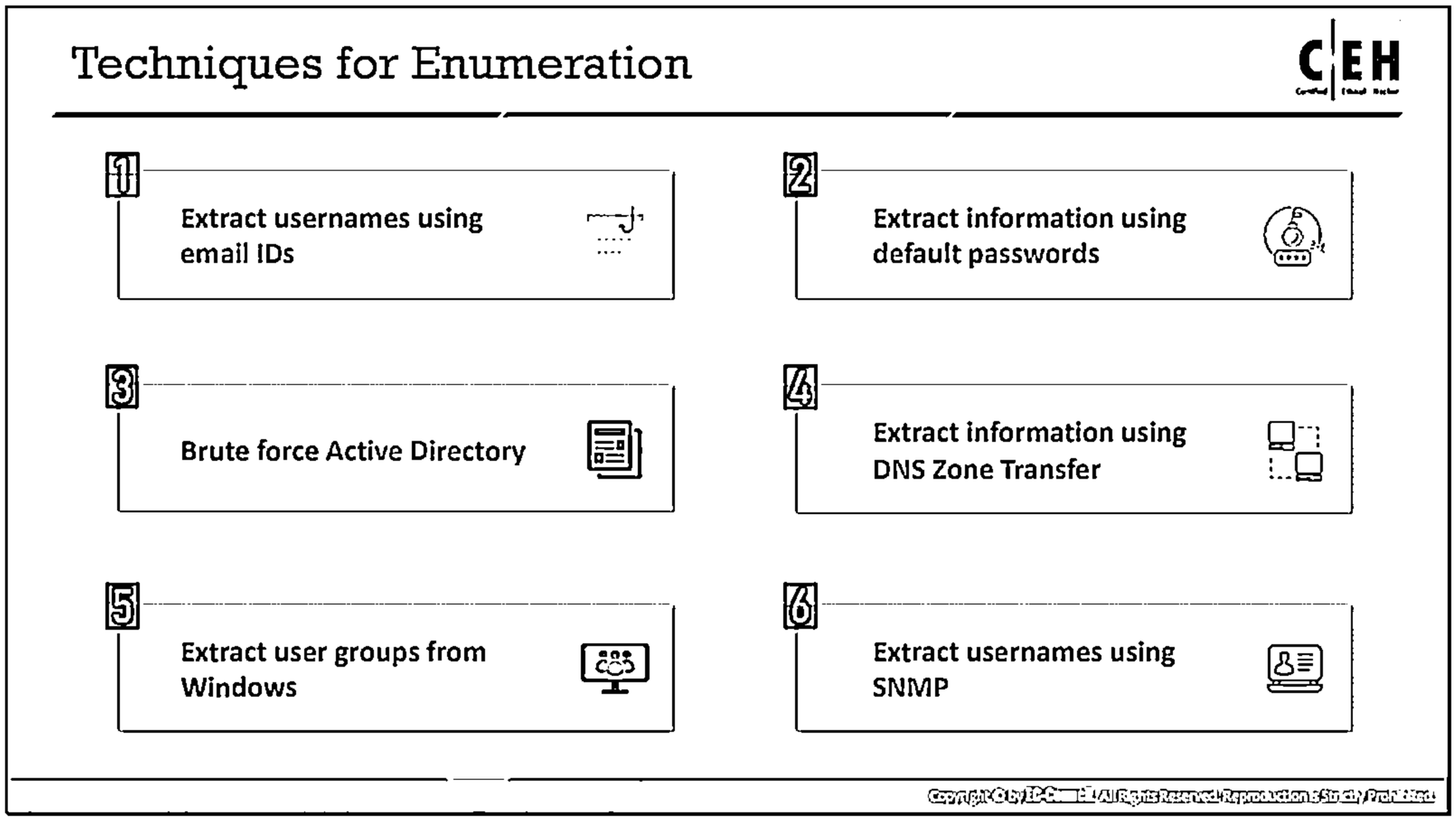
Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network. In the enumeration phase, an attacker creates active connections with the system and sends directed queries to gain more information about the target. The attacker uses the information collected using enumeration to identify vulnerabilities in the system security, which help them exploit the target system. In turn, enumeration allows the attacker to perform password attacks to gain unauthorized access to information system resources. Enumeration techniques work in an intranet environment.

In particular, enumeration allows the attacker to collect the following information:

- Network resources
- Network shares
- Routing tables
- Audit and service settings
- SNMP and fully qualified domain name (FQDN) details
- Machine names
- Users and groups
- Applications and banners

During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents.

The previous modules highlighted how attackers gather necessary information about a target without any illegal activity. However, enumeration activities may be illegal depending on the organization's policies and the laws that are in effect. An ethical hacker or pen tester should always acquire proper authorization before performing enumeration.



Techniques for Enumeration

The following techniques are used to extract information about a target.

- **Extract usernames using email IDs**

  Every email address contains two parts, a username and a domain name, in the format "username@domainname."

- **Extract information using default passwords**

  Many online resources provide a list of default passwords assigned by manufacturers to their products. Users often ignore recommendations to change the default usernames and passwords provided by the manufacturer or developer of a product. This eases an attacker's task of enumerating and exploiting the target system.

- **Brute force Active Directory**

  Microsoft Active Directory is susceptible to username enumeration at the time of user-supplied input verification. This is a design error in the Microsoft Active Directory implementation. If a user enables the "logon hours" feature, then all the attempts at service authentication result in different error messages. Attackers take advantage of this to enumerate valid usernames. An attacker who succeeds in extracting valid usernames can conduct a brute-force attack to crack the respective passwords.

- **Extract information using DNS Zone Transfer**

  A network administrator can use DNS zone transfer to replicate DNS data across several DNS servers or back up DNS files. For this purpose, the administrator needs to execute a specific zone-transfer request to the name server. If the name server permits zone

transfer, it will convert all the DNS names and IP addresses hosted by that server to ASCII text.

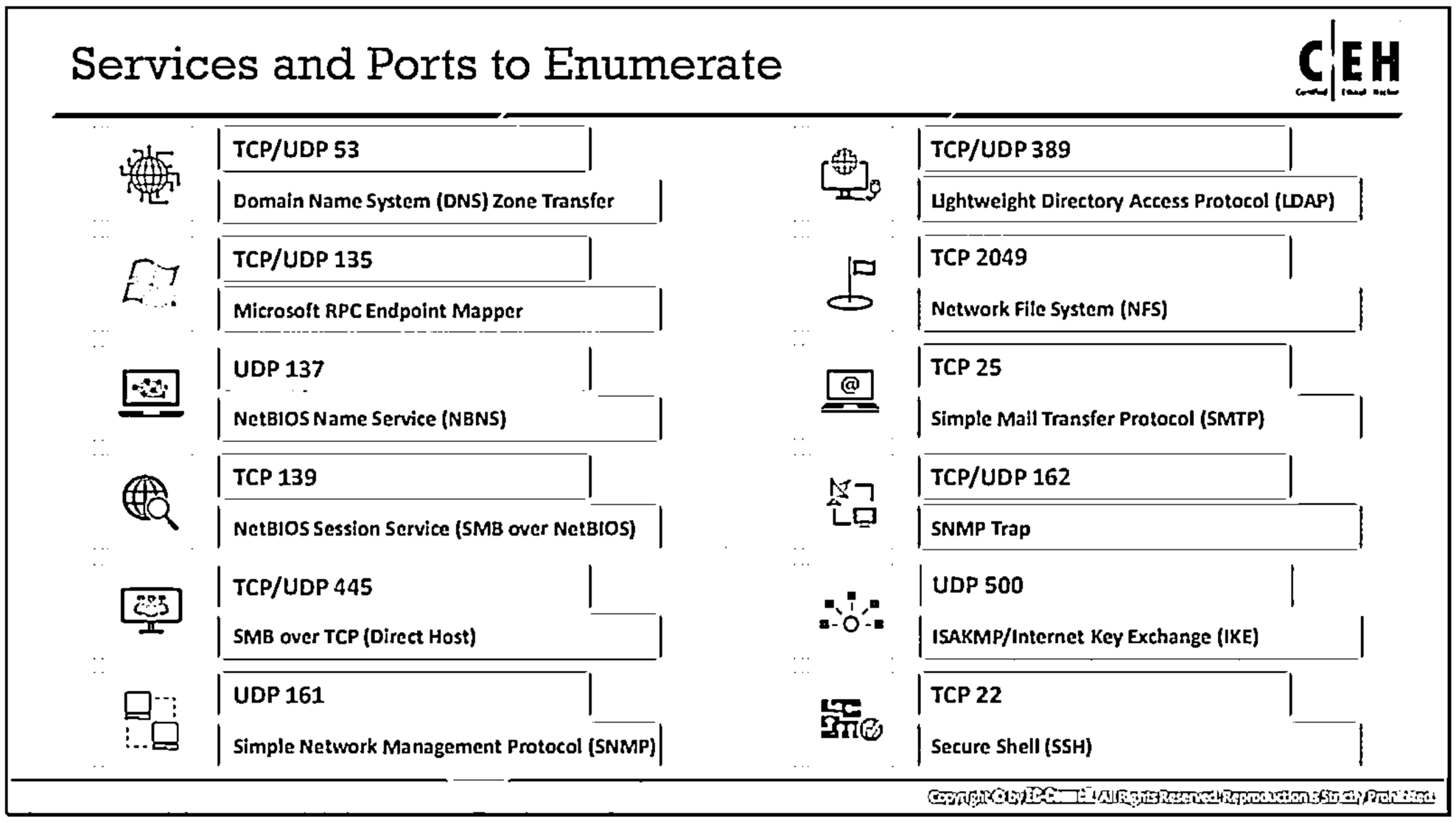
If the network administrators did not configure the DNS server properly, the DNS zone transfer can be an effective method to obtain information about the organization's network. This information may include lists of all named hosts, sub-zones, and related IP addresses. A user can perform DNS zone transfer using nslookup and dig commands.

- **Extract user groups from Windows**

  To extract user groups from Windows, the attacker should have a registered ID as a user in the Active Directory. The attacker can then extract information from groups in which the user is a member by using the Windows interface or command-line method.

- **Extract usernames using SNMP**

  Attackers can easily guess read-only or read-write community strings by using the SNMP application programming interface (API) to extract usernames.



Services and Ports to Enumerate

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) manage data communications between terminals in a network.

TCP is a connection-oriented protocol capable of carrying messages or emails over the Internet. It provides a reliable multi-process communication service in a multi-network environment. The features and functions of TCP include the following:

- Supports acknowledgement for receiving data through a sliding window acknowledgement system
- Offers automatic retransmission of lost or acknowledged data
- Allows addressing and multiplexing of data
- A connection can be established, managed, or terminated
- Offers quality-of-service transmission
- Offers congestion management and flow control

UDP is a connectionless protocol that carries short messages over a computer network. It provides unreliable service. The applications of UDP include the following:

- Audio streaming
- Videoconferencing and teleconferencing

Services and TCP/UDP ports that can be enumerated include the following.

- **TCP/UDP 53: DNS Zone Transfer**

  The DNS resolution process establishes communication between DNS clients and DNS servers. DNS clients send DNS messages to DNS servers listening on UDP port 53. If the DNS message size exceeds the default size of UDP (512 octets), the response contains only the data that UDP can accommodate, and the DNS server sets a flag to indicate the truncated response. The DNS client can now resend the request via TCP over port 53 to the DNS server. In this approach, the DNS server uses UDP as a default protocol. In the case of lengthy queries for which UDP fails, TCP is used as a failover solution. Malware such as ADM worm and Bonk Trojan uses port 53 to exploit vulnerabilities within DNS servers, helping intruders launch attacks.

- **TCP/UDP 135: Microsoft RPC Endpoint Mapper**

  Source: *https://technet.microsoft.com*

  RPC is a protocol used by a client system to request a service from a server. An endpoint is the protocol port on which the server listens for the client's RPCs. The RPC Endpoint Mapper enables RPC clients to determine the port number currently assigned to a specific RPC service. There is a flaw in the part of RPC that exchanges messages over TCP/IP. The incorrect handling of malformed messages causes failure. This affects the RPC Endpoint Mapper, which listens on TCP/IP port 135. This vulnerability could allow an attacker to send RPC messages to the RPC Endpoint Mapper process on a server to launch a denial-of-service (DoS) attack.

- **UDP 137: NetBIOS Name Service (NBNS)**

  NBNS, also known as the Windows Internet Name Service (WINS), provides a name-resolution service for computers running NetBIOS. NetBIOS name servers maintain a database of the NetBIOS names for hosts and the corresponding IP address the host is using. NBNS aims to match IP addresses with NetBIOS names and queries. Attackers usually attack the name service first. Typically, NBNS uses UDP 137 as its transport protocol. It can also use TCP 137 as its transport protocol for a few operations, though this might never occur in practice.

- **TCP 139: NetBIOS Session Service (SMB over NetBIOS)**

  TCP 139 is perhaps the most well-known Windows port. It is used to transfer files over a network. Systems use this port for both null-session establishment as well as file and printer sharing. A system administrator considering the restriction of access to ports on a Windows system should make the restriction of TCP 139 a top priority. An improperly configured TCP 139 port can allow an intruder to gain unauthorized access to critical system files or the complete file system, resulting in data theft or other malicious activities.

- **TCP/UDP 445: SMB over TCP (Direct Host)**

  Windows supports file- and printer-sharing traffic using the SMB protocol directly hosted on TCP. In earlier OSs, SMB traffic required the NetBIOS over TCP (NBT) protocol to work

on TCP/IP transport. Directly hosted SMB traffic uses port 445 (TCP and UDP) instead of NetBIOS.

- **UDP 161: Simple Network Management Protocol (SNMP)**

  SNMP is widely used in network management systems to monitor network-attached devices such as routers, switches, firewalls, printers, and servers. It consists of a manager and agents. The agent receives requests on port 161 from the managers and responds to the managers on port 162.

- **TCP/UDP 389: Lightweight Directory Access Protocol (LDAP)**

  LDAP is a protocol for accessing and maintaining distributed directory information services over an IP network. By default, LDAP uses TCP or UDP as its transport protocol over port 389.

- **TCP 2049: Network File System (NFS)**

  NFS protocol is used to mount file systems on a remote host over a network, and users can interact with the file systems as if they are mounted locally. NFS servers listen to its client systems on TCP port 2049. If NFS services are not properly configured, then attackers may exploit the NFS protocol to gain control over a remote system, perform privilege escalation, inject backdoors or malware on a remote host, etc.

- **TCP 25: Simple Mail Transfer Protocol (SMTP)**

  SMTP is a TCP/IP mail delivery protocol. It transfers email across the Internet and across local networks. It runs on the connection-oriented service provided by TCP and uses the well-known port number 25. Below table lists some commands used by SMTP and their respective syntaxes.

Hello	HELO <sending-host>
From	MAIL FROM:<from-address>
Recipient	RCPT TO:<to-address>
Data	DATA
Reset	RESET
Verify	VRFY<string>
Expand	EXPN<string>
Help	HELP[string]
Quit	QUIT

Table 4.1: SMTP commands and their respective syntaxes

- **TCP/UDP 162: SNMP Trap**

  An SNMP trap uses TCP/UDP port 162 to send notifications such as optional variable bindings and the sysUpTime value from an agent to a manager.

- **UDP 500: Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE)**

  Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE) is a protocol used to set up a security association (SA) in the IPsec protocol suite. It uses UDP port 500 to establish, negotiate, modify, and delete SAs and cryptographic keys in a virtual private network (VPN) environment.

- **TCP 22: Secure Shell (SSH)**

  Secure Shell (SSH) is a command-level protocol mainly used for managing various networked devices securely. It is generally used as an alternative protocol to the unsecure Telnet protocol. SSH uses the client/server communication model, and the SSH server, by default, listens to its client on TCP port 22. Attackers may exploit the SSH protocol by brute-forcing SSH login credentials.

- **TCP/UDP 3268: Global Catalog Service**

  Microsoft's Global Catalog server, a domain controller that stores extra information, uses port 3268. Its database contains rows for every object in the entire organization, instead of rows for only the objects in one domain. Global Catalog allows one to locate objects from any domain without having to know the domain name. LDAP in the Global Catalog server uses port 3268. This service listens to port 3268 through a TCP connection. Administrators use port 3268 for troubleshooting issues in the Global Catalog by connecting to it using LDP.

- **TCP/UDP 5060, 5061: Session Initiation Protocol (SIP)**

  The Session Initiation Protocol (SIP) is a protocol used in Internet telephony for voice and video calls. It typically uses TCP/UDP port 5060 (non-encrypted signaling traffic) or 5061 (encrypted traffic with TLS) for SIP to servers and other endpoints.

- **TCP 20/21: File Transfer Protocol**

  FTP is a connection-oriented protocol used for transferring files over the Internet and private networks. FTP is controlled on TCP port 21, and for data transmission, FTP uses TCP port 20 or some dynamic port numbers depending on the server configuration. If attackers identify that FTP server ports are open, then they perform enumeration on FTP to find information such as the software version and state of existing vulnerabilities to perform further exploitations such as the sniffing of FTP traffic and FTP brute-force attacks.

- **TCP 23: Telnet**

  The Telnet protocol is used for managing various networked devices remotely. It is an unsecure protocol because it transmits login credentials in the cleartext format. Therefore, it is mostly used in private networks. The Telnet server listens to its clients on port 23. Attackers can take advantage of the Telnet protocol to perform banner grabbing on other protocols such as SSH and SMTP, brute-forcing attacks on login credentials, port-forwarding attacks, etc.

- **UDP 69: Trivial File Transfer Protocol (TFTP)**

  TFTP is a connectionless protocol used for transferring files over the Internet. TFTP depends on connectionless UDP; therefore, it does not guarantee the proper transmission of the file to the destination. TFTP is mainly used to update or upgrade software and firmware on remote networked devices. It uses UDP port 69 for transferring files to a remote host. Attackers may exploit TFTP to install malicious software or firmware on remote devices.

- **TCP 179: Border Gateway Protocol (BGP)**

  BGP is widely used by Internet service providers (ISPs) to maintain huge routing tables and for efficiently processing Internet traffic. BGP routers establish sessions on TCP port 179. The misconfiguration of BGP may lead to various attacks such as dictionary attacks, resource-exhaustion attacks, flooding attacks, and hijacking attacks.

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

NetBIOS Enumeration

- A NetBIOS name is a unique 16 ASCII character string used to identify the network devices over TCP/IP; fifteen characters are used for the device name, and the sixteenth character is reserved for the service or name record type

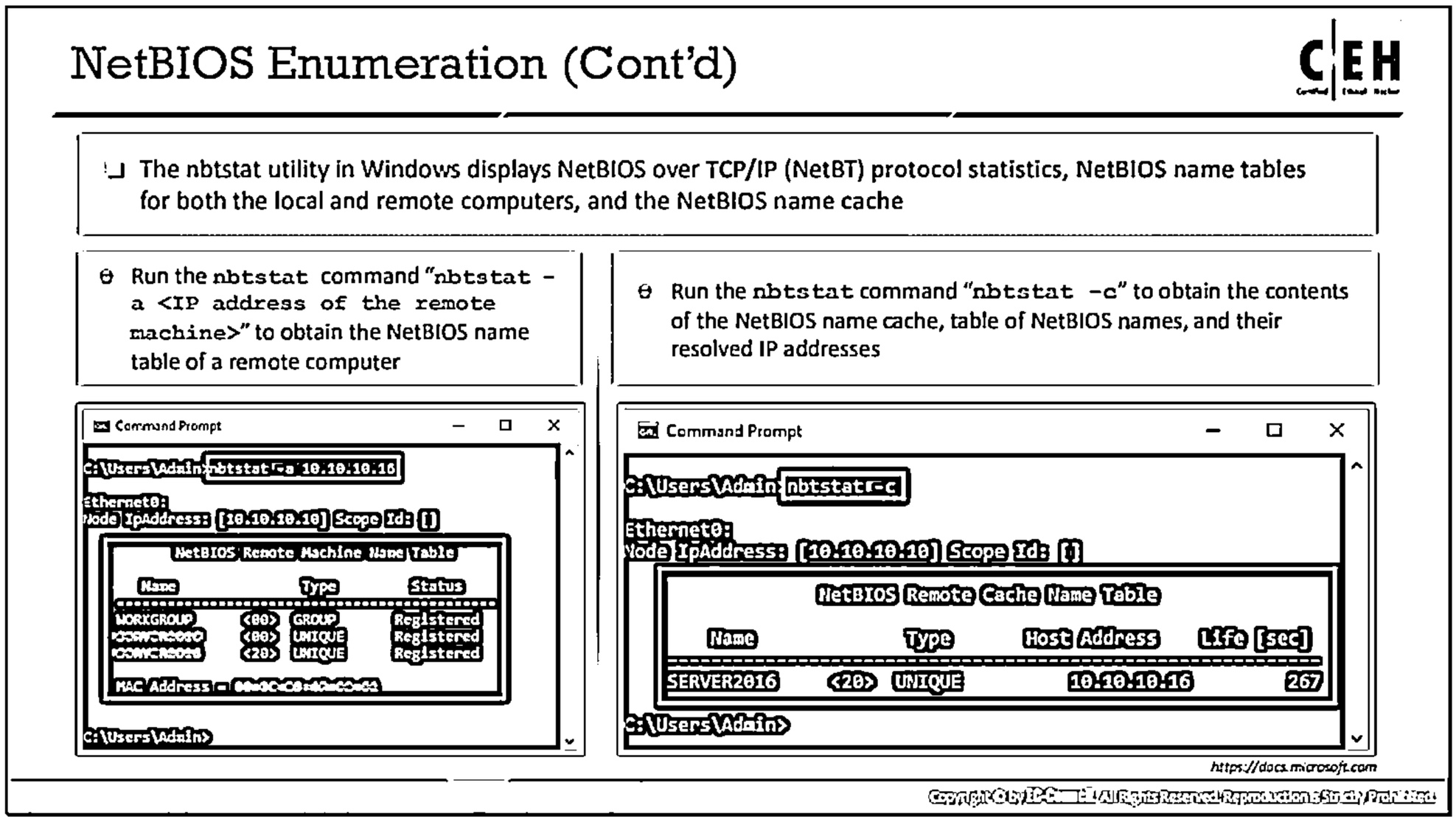
Attackers use the NetBIOS enumeration to obtain

- The list of computers that belong to a domain
- The list of shares on the individual hosts in the network
- Policies and passwords

NetBIOS name list

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, identifies the primary domain controller (PDC) for the domain

Note: NetBIOS name resolution is not supported by Microsoft for Internet Protocol Version 6 (IPv6)



NetBIOS Enumeration

Thus far, we discussed enumeration concepts and resources that provide valuable information. This section describes NetBIOS enumeration, the information obtained, and various NetBIOS enumeration tools. NetBIOS is considered first for enumeration because it extracts a large amount of sensitive information about the target network, such as users and network shares.

The first step in enumerating a Windows system is to take advantage of the NetBIOS API. NetBIOS was originally developed as an API for client software to access local area network (LAN) resources. Windows uses NetBIOS for file and printer sharing. The NetBIOS name is a unique 16-character ASCII string assigned to Windows systems to identify network devices over TCP/IP; 15 characters are used for the device name, and the 16th is reserved for the service or record type. NetBIOS uses UDP port 137 (name services), UDP port 138 (datagram services), and TCP port 139 (session services). Attackers usually target the NetBIOS service because it is easy to exploit and run on Windows systems even when not in use.

Attackers use NetBIOS enumeration to obtain the following:

- The list of computers that belong to a domain
- The list of shares on the individual hosts in a network
- Policies and passwords

An attacker who finds a Windows system with port 139 open can check to see which resources can be accessed or viewed on a remote system. However, to enumerate the NetBIOS names, the remote system must have enabled file and printer sharing. NetBIOS enumeration may enable an attacker to read or write to a remote computer system, depending on the availability of shares, or launch a DoS attack.

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, which identifies the primary domain controller (PDC) for the domain
<domain>	<1E>	GROUP	Browser service elections

Table 4.2: NetBIOS name list

Note that Microsoft does not support NetBIOS name resolution for IPv6.

Nbtstat Utility

Source: *https://docs.microsoft.com*

Nbtstat is a Windows utility that helps in troubleshooting NETBIOS name resolution problems. The `nbtstat` command removes and corrects preloaded entries using several case-sensitive switches. Attackers use Nbtstat to enumerate information such as NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both local and remote computers, and the NetBIOS name cache.

The syntax of the nbtstat command is as follows:

```
nbtstat [-a RemoteName] [-A IP Address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]
```

The table shown below lists various Nbtstat parameters and their respective functions.

Nbtstat Parameter	Function
`-a RemoteName`	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer
`-A IP Address`	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer
`-c`	Lists the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses
`-n`	Displays the names registered locally by NetBIOS applications such as the server and redirector
`-r`	Displays a count of all names resolved by a broadcast or WINS server

`-R`	Purges the name cache and reloads all #PRE-tagged entries from the Lmhosts file
`-RR`	Releases and re-registers all names with the name server
`-s`	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names
`-S`	Lists the current NetBIOS sessions and their status with the IP addresses
`Interval`	Re-displays selected statistics, pausing at each display for the number of seconds specified in Interval

Table 4.3: Nbtstat parameters and their respective functions

The following are some examples for nbtstat commands.

- The nbtstat command "`nbtstat -a <IP address of the remote machine>`" can be executed to obtain the NetBIOS name table of a remote computer.

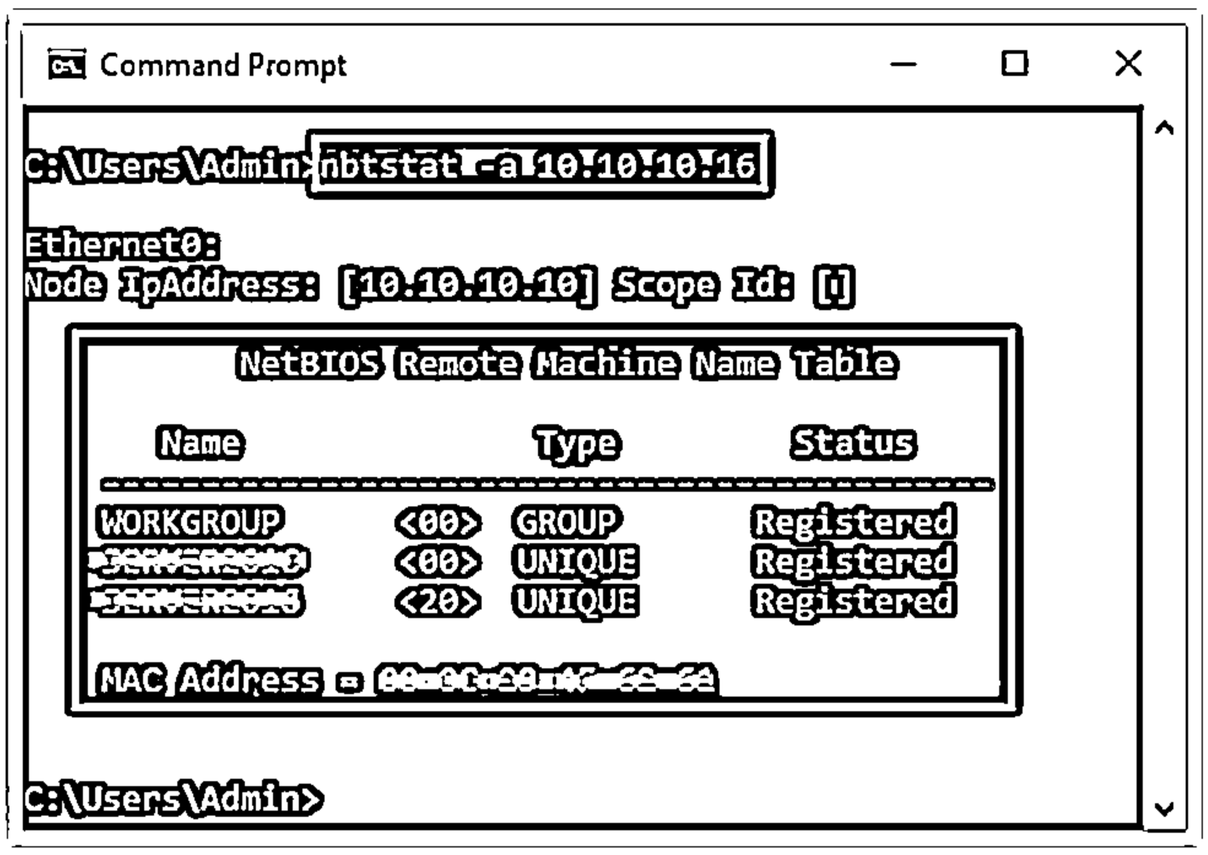


Figure 4.1: Nbtstat command to obtain the name table of a remote system

- The nbtstat command "`nbtstat -c`" can be executed to obtain the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses.

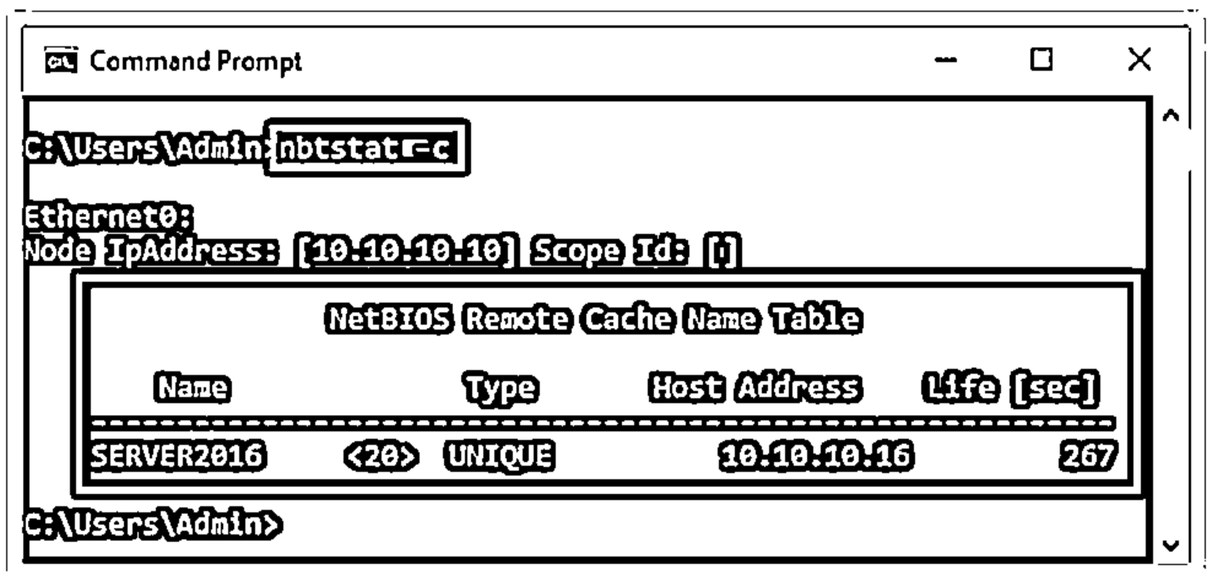
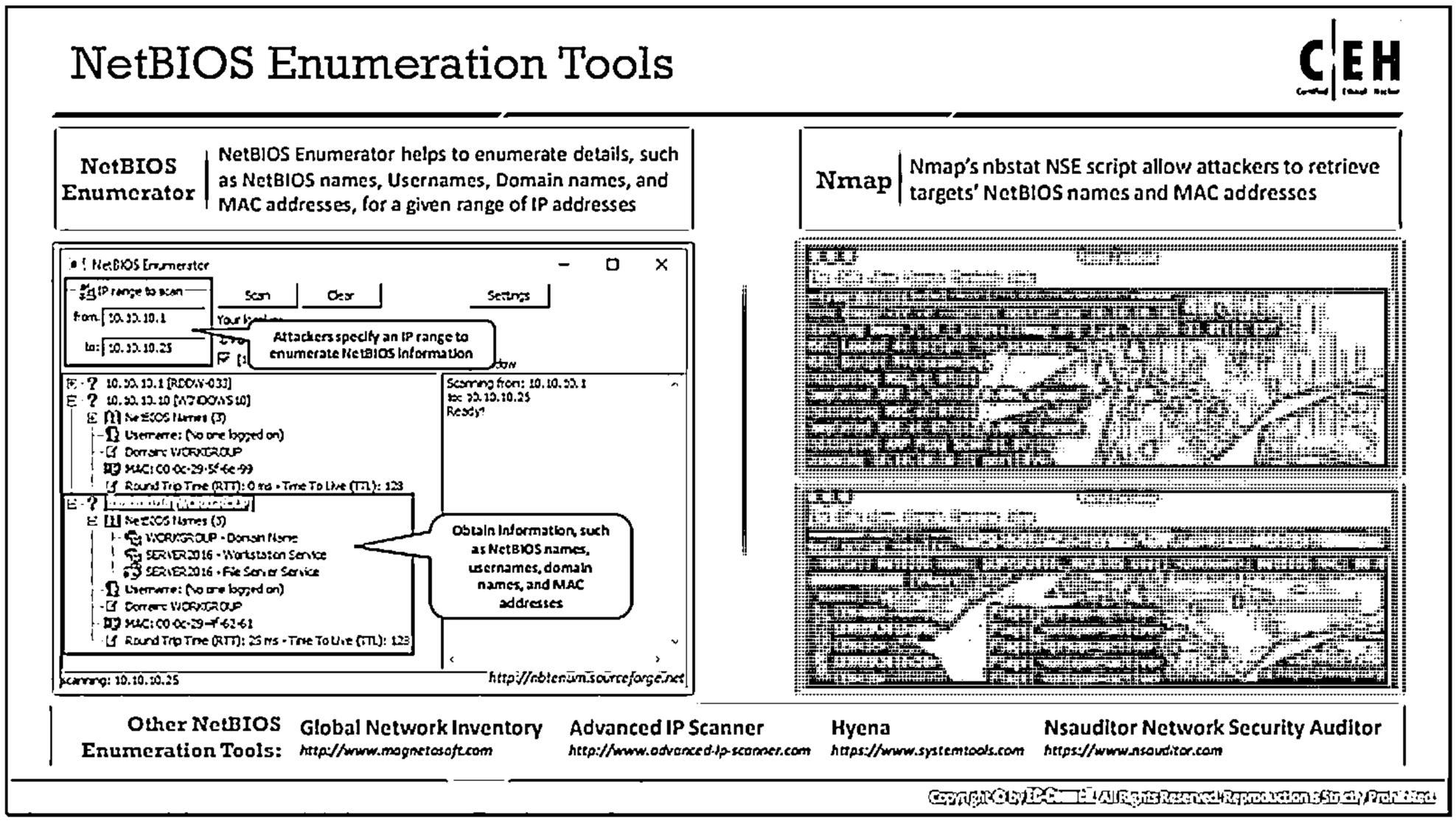


Figure 4.2: Nbtstat command to obtain the contents of the NetBIOS name table



NetBIOS Enumeration Tools

NetBIOS enumeration tools explore and scan a network within a given range of IP addresses and lists of computers to identify security loopholes or flaws in networked systems. These tools also enumerate operating systems (OSs), users, groups, Security Identifiers (SIDs), password policies, services, service packs and hotfixes, NetBIOS shares, transports, sessions, disks and security event logs, etc.

- **NetBIOS Enumerator**

  Source: *http://nbtenum.sourceforge.net*

  NetBIOS Enumerator is an enumeration tool that shows how to use remote network support and to deal with some other web protocols, such as SMB. As shown in the screenshot, attackers use NetBIOS Enumerator to enumerate details such as NetBIOS names, usernames, domain names, and media access control (MAC) addresses for a given range of IP addresses.

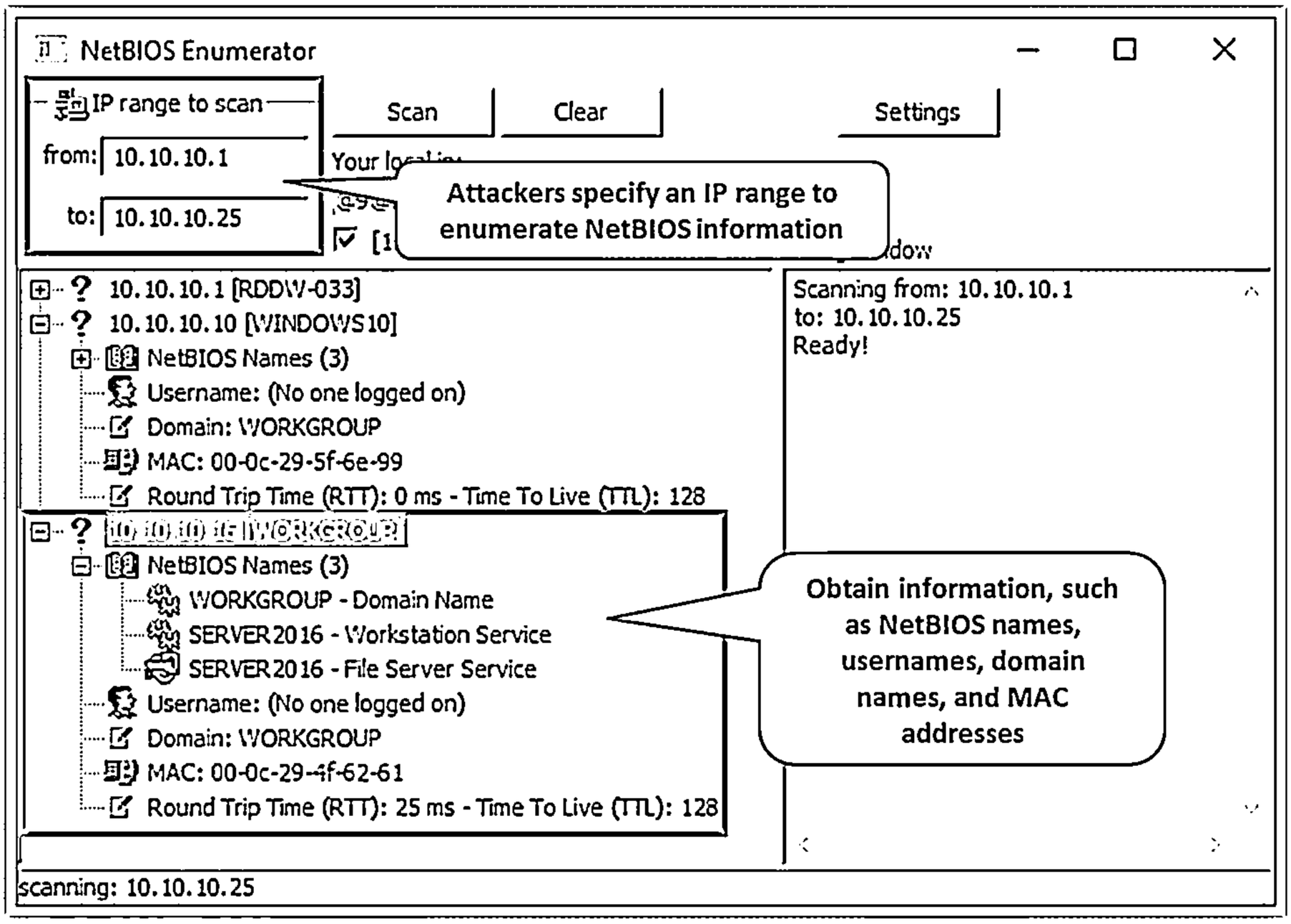


Figure 4.3: Screenshot of NetBIOS Enumerator

- **Nmap**

  Source: *https://nmap.org*

  Attackers use the Nmap Scripting Engine (NSE) for discovering NetBIOS shares on a network. The nbstat script of NSE allows attackers to retrieve the target's NetBIOS names and MAC addresses. By default, the script displays the name of the computer and the logged-in user. However, if the verbosity is turned up, it displays all names related to that system.

  As shown in the screenshot, an attacker uses the following Nmap command to perform NetBIOS enumeration on a target host:

```
nmap -sV -v --script nbstat.nse <target IP address>
```

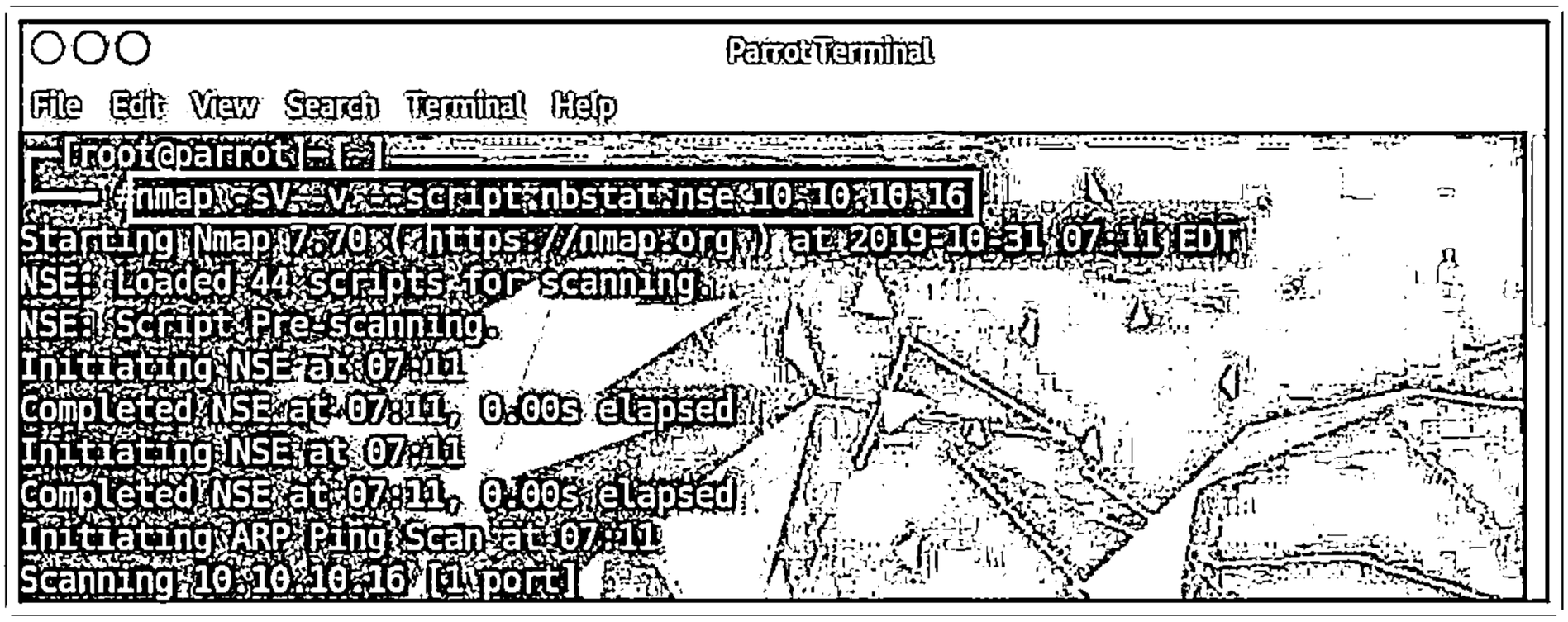


Figure 4.4: Screenshot of Nmap command for NetBIOS enumeration

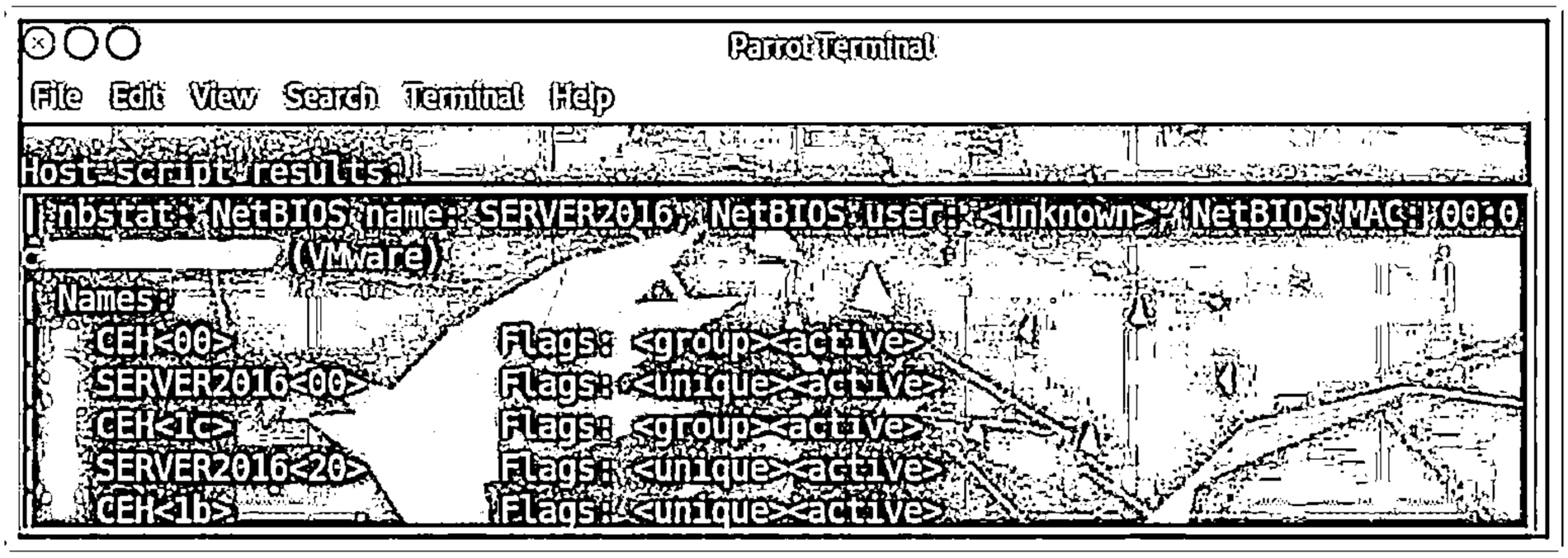
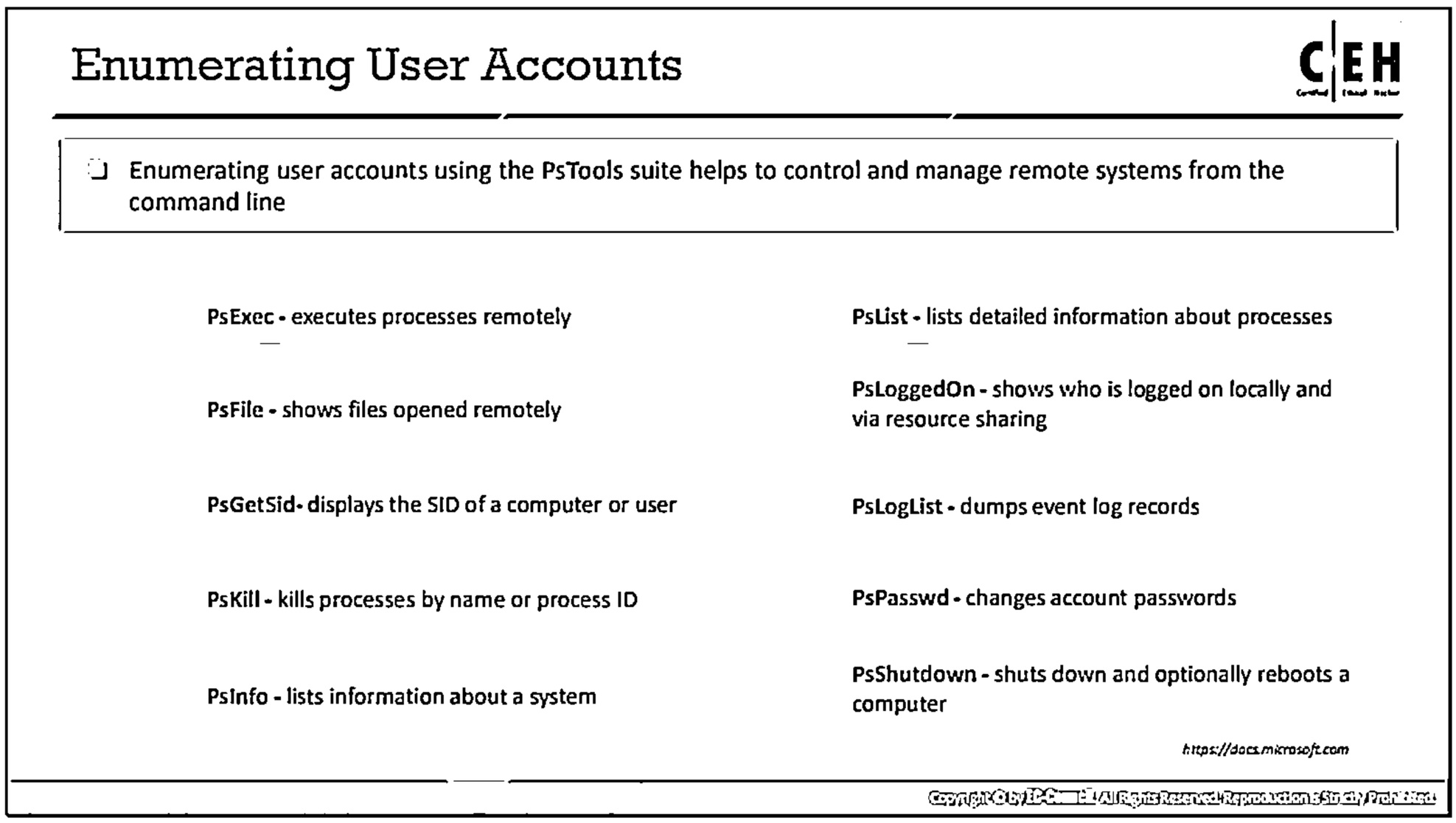


Figure 4.5: Screenshot of Nmap NetBIOS enumeration output

The following are some additional NetBIOS enumeration tools:

- Global Network Inventory (*http://www.magnetosoft.com*)
- Advanced IP Scanner (*http://www.advanced-ip-scanner.com*)
- Hyena (*https://www.systemtools.com*)
- Nsauditor Network Security Auditor (*https://www.nsauditor.com*)



Enumerating User Accounts

Source: *https://docs.microsoft.com*

Enumerating user accounts using the PsTools suite helps in controlling and managing remote systems from the command line. The following are some commands for enumerating user accounts.

- **PsExec**

  PsExec is a lightweight Telnet replacement that can execute processes on other systems, complete with full interactivity for console applications, without having to install client software manually. PsExec's most powerful use case is the launch of interactive command prompts on remote systems and remote-enabling tools such as Ipconfig that otherwise cannot show information about remote systems. The syntax of the PsExec command is as follows:

  ```
  psexec [\\computer[,computer2[,...] | @file]][-u user [-p psswd][-n s][-r servicename][-h][-l][-s|-e][-x][-I [session]][-c [-f|-v]][-w directory][-d][-<priority>][-a n,n,...] cmd [arguments]
  ```

- **PsFile**

  PsFile is a command-line utility that shows a list of files on a system that opened remotely, and it can close opened files either by name or by a file identifier. The default behavior of PsFile is to list the files on the local system opened by remote systems. Typing a command followed by "- " displays information on the syntax for that command. The syntax of the PsFile command is as follows:

  ```
  psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id | path] [-c]]
  ```

- **PsGetSid**

  PsGetSid translates SIDs to their display name and vice versa. It works on built-in accounts, domain accounts, and local accounts. It also displays the SIDs of user accounts and translates an SID into the name that represents it. It works across the network to query SIDs remotely. The syntax of the PsGetSid command is as follows:

  ```
  psgetsid [\\computer[,computer[,...] | @file] [-u username [-p password]]] [account|SID]
  ```

- **PsKill**

  PsKill is a kill utility that can kill processes on remote systems and terminate processes on the local computer. Running PsKill with a process ID directs it to kill the process of that ID on the local computer. If a process name is specified, PsKill will kill all processes that have that name. One need not install a client on the target computer to use PsKill to terminate a remote process. The syntax of the PsKill command is as follows:

  ```
  pskill [- ] [-t] [\\computer [-u username] [-p password]] <process name | process id>
  ```

- **PsInfo**

  PsInfo is a command-line tool that gathers key information about local or remote legacy Windows NT/2000 systems, including the type of installation, kernel build, registered organization and owner, number of processors and their type, amount of physical memory, installation date of the system, and expiration date in the case of a trial version. By default, PsInfo shows information for the local system. A remote computer name can be specified to obtain information for a remote system. The syntax of the PsInfo command is as follows:

  ```
  psinfo [[\\computer[,computer[,..] | @file [-u user [-p psswd]]] [-h] [-s] [-d] [-c [-t delimiter]] [filter]
  ```

- **PsList**

  PsList is a command-line tool that displays central processing unit (CPU) and memory information or thread statistics. Tools in the Resource Kits, pstat and pmon, show different types of data only for the processes on the system on which the tools are run.

- **PsLoggedOn**

  PsLoggedOn is an applet that displays both the locally logged-in users and users logged in via resources for either the local computer or a remote one. If a username is specified instead of a computer, PsLoggedOn searches the computers in the network neighborhood and reveals if the user currently logged in. PsLoggedOn defines a locally logged-in user is one that has a profile loaded into the registry. Therefore, PsLoggedOn determines who is logged in by scanning the keys under the HKEY_USERS key. For each key that has a name or user SID, PsLoggedOn looks up the corresponding username and displays it. To determine who logged into a computer via resource shares, PsLoggedOn uses the NetSessionEnum API. The syntax of the PsLoggedOn command is as follows:

  ```
  psloggedon [- ] [-l] [-x] [\\computername | username]
  ```

- **PsLogList**

  The elogdump utility dumps the contents of an Event Log on a local or remote computer. PsLogList is a clone of elogdump except that PsLogList can log in to remote systems in situations where the user's security credentials would not permit access to the Event Log, and PsLogList retrieves message strings from the computer on which the event log is stored. The default function of PsLogList is to display the contents of the System Event Log on the local computer with visually friendly formatting. The syntax of the PsLogList command is as follows:

  ```
  psloglist [- ] [\\computer[,computer[,...] | @file [-u username [-
  p password]]] [-s [-t delimiter]] [-m #|-n #|-h #|-d #|-w][-c][-
  x][-r][-a mm/dd/yy][-b mm/dd/yy][-f filter] [-i ID[,ID[,...] | -e
  ID[,ID[,...]]] [-o event source[,event source][,..]]] [-q event
  source[,event source][,..]]] [-l event log file] <eventlog>
  ```

- **PsPasswd**

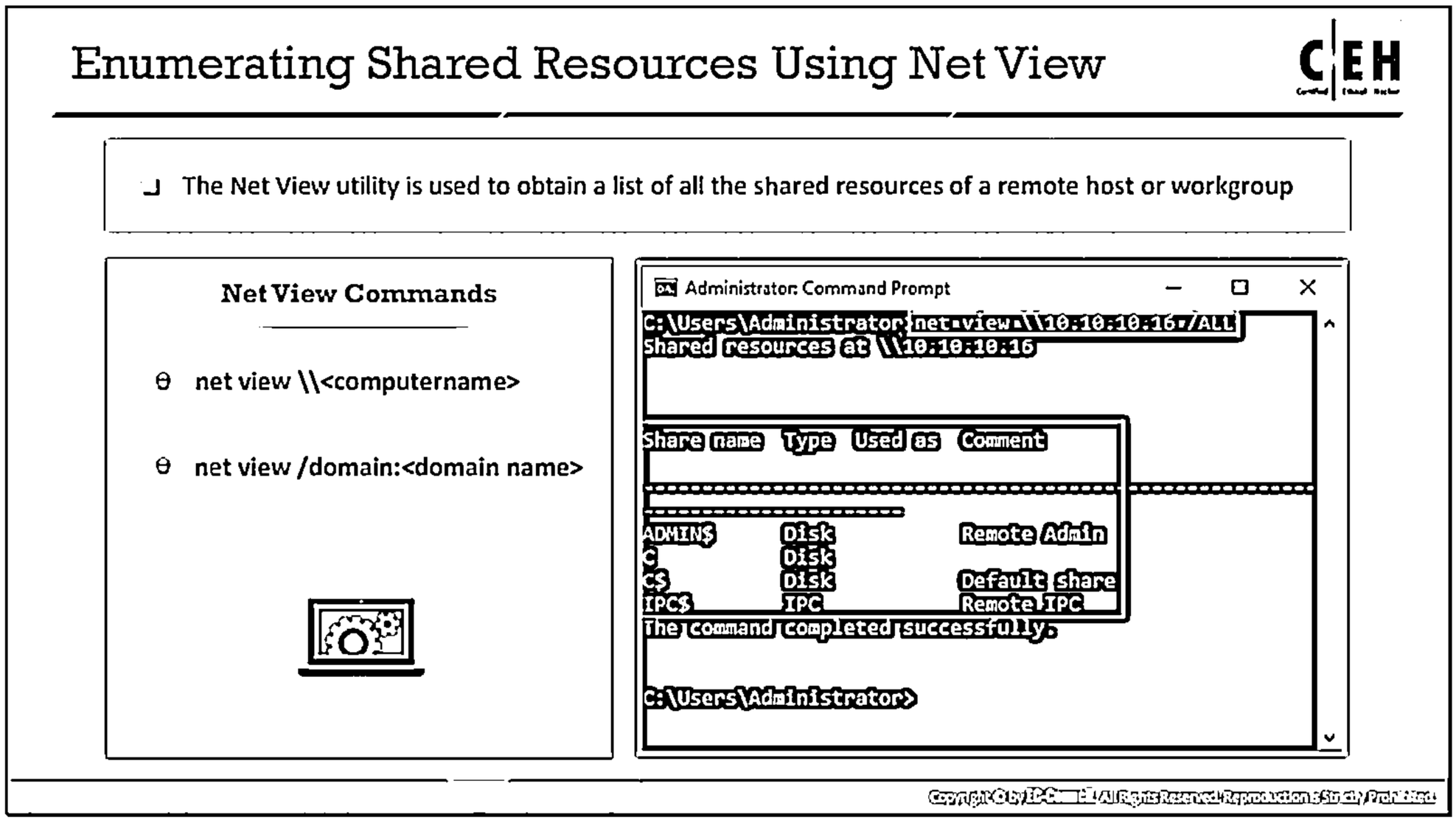
  PsPasswd can change an account password on local or remote systems, and administrators can create batch files that run PsPasswd on the computers they manage to perform a mass change of the administrator password. PsPasswd uses Windows password reset APIs; therefore, it does not send passwords over the network in the cleartext. The syntax of the PsPasswd command is as follows:

  ```
  pspasswd [[\\computer[,computer[,..] | @file [-u user [-p psswd]]]
  Username [NewPassword]
  ```

- **PsShutdown**

  PsShutdown can shut down or reboot a local or remote computer. It requires no manual installation of client software. The syntax of the PsShutdown command is as follows:

  ```
  psshutdown [[\\computer[,computer[,..] | @file [-u user [-p
  psswd]]] -s|-r|-h|-d|-k|-a|-l|-o [-f] [-c] [-t nn|h:m] [-n s] [-v
  nn] [-e [u|p]:xx:yy] [-m "message"]
  ```



Enumerating Shared Resources Using Net View

Net View is a command-line utility that displays a list of computers in a specified workgroup or shared resources available on a specified computer. It can be used in the following ways.

```
net view \\<computername>
```

In the above command, `<computername>` is the name or IP address of a specific computer, the resources of which are to be displayed.

```
net view \\<computername> /ALL
```

The above command displays all the shares on the specified remote computer, along with hidden shares.

```
net view /domain
```

The above command displays all the shares in the domain.

```
net view /domain:<domain name>
```

The above command displays all the shares on the specified domain.

The screenshot shows the shared resources available on the specified computer.

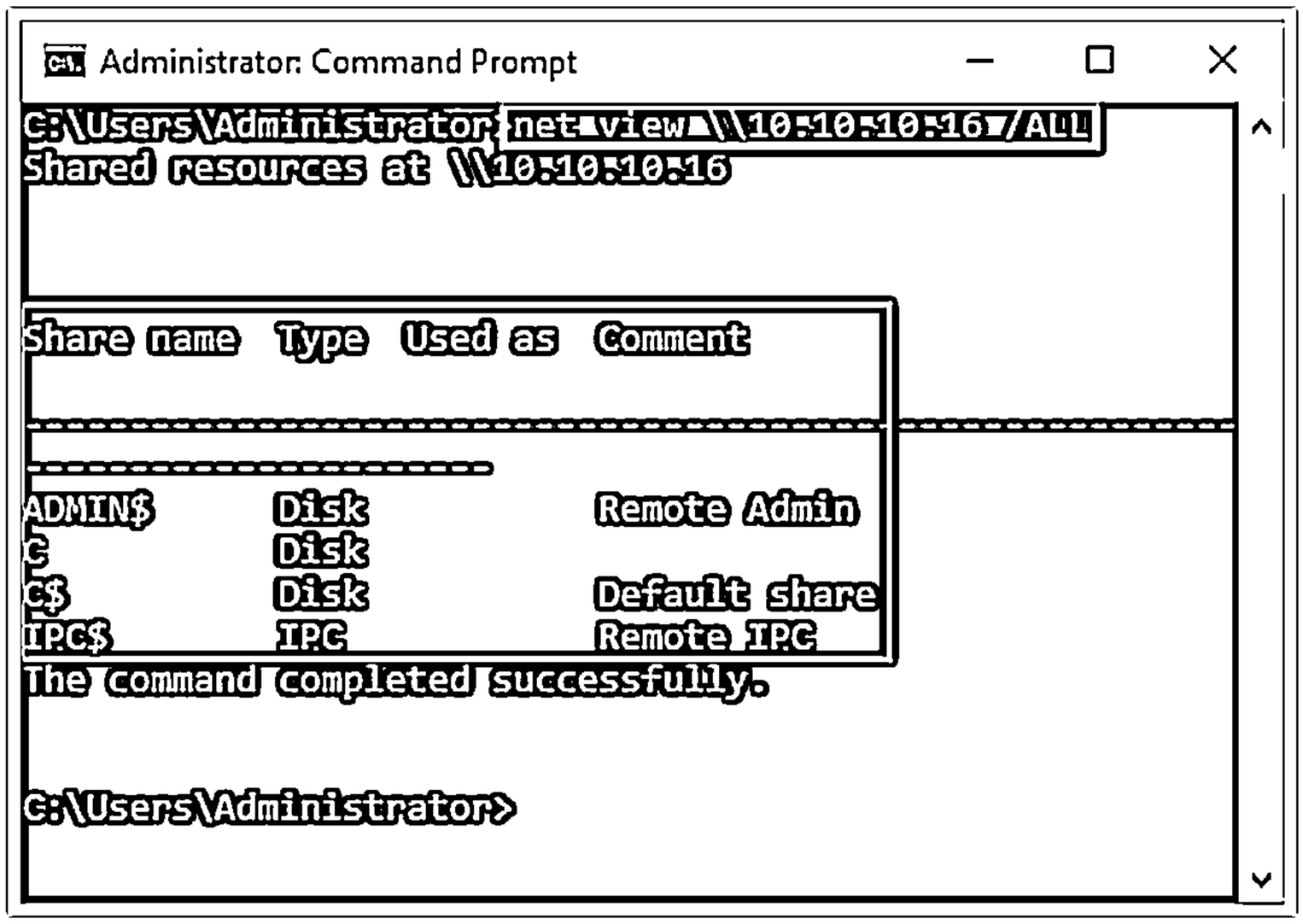


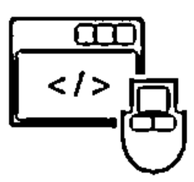
Figure 4.6: Output of Net View command

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

SNMP (Simple Network Management Protocol) Enumeration

- SNMP enumeration is the process of enumerating user accounts and devices on a target system using SNMP
- SNMP consists of a manager and an agent; agents are embedded on every network device, and the manager is installed on a separate computer
- SNMP holds two passwords to access and configure the SNMP agent from the management station
  - Read community string: It is public by default; it allows for the viewing of the device/system configuration
  - Read/write community string: It is private by default; it allows remote editing of configuration
- Attackers use these default community strings to extract information about a device
- Attackers enumerate SNMP to extract information about network resources, such as hosts, routers, devices, and shares, and network information, such as ARP tables, routing tables, and traffic



SNMP Enumeration

SNMP allows network administrators to manage network devices from a remote location. However, SNMP has many security vulnerabilities, such as a lack of auditing. Attackers may take advantage of these vulnerabilities to perform account and device enumeration. This section describes SNMP enumeration, the information extracted via SNMP enumeration, and various SNMP enumeration tools used to enumerate user accounts and devices on a target system.

SNMP is an application-layer protocol that runs on UDP and maintains and manages routers, hubs, and switches on an IP network. SNMP agents run on Windows and Unix networks on networking devices.

SNMP enumeration is the process of creating a list of the user's accounts and devices on a target computer using SNMP. SNMP employs two types of software components for communication: the SNMP agent and SNMP management station. The SNMP agent is located on the networking device, and the SNMP management station communicates with the agent.

Almost all the network infrastructure devices such as routers and switches contain an SNMP agent for managing the system or devices. The SNMP management station sends requests to the agent; after receiving the request, the agent replies. Both requests and replies are configuration variables accessible by the agent software. SNMP management stations send requests to set values to some variables. Traps let the management station know if an abnormal event such as a reboot or an interface failure has occurred at the agent's side.

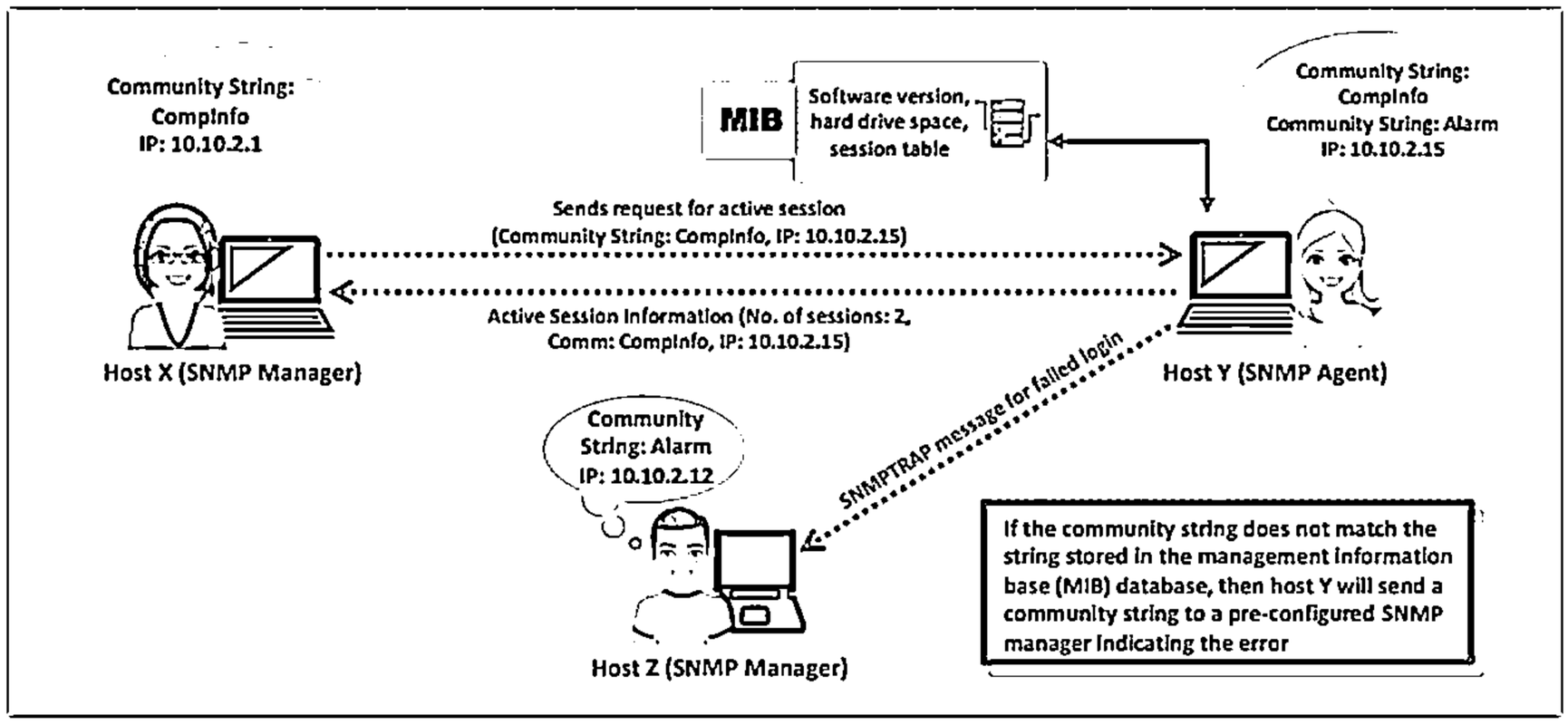
SNMP contains the following two passwords for configuring and accessing the SNMP agent from the management station.

- **Read Community String**
  - The configuration of the device or system can be viewed with the help of this password.
  - These strings are public.
- **Read/Write Community String**
  - The device configuration can be changed or edited using this password.
  - These strings are private.

When administrators leave the community strings at the default setting, attackers can use these default community strings (passwords) for changing or viewing the configuration of the device or system. Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, and shares as well as network information such as ARP tables, routing tables, device-specific information, and traffic statistics.

Commonly used SNMP enumeration tools include OpUtils (*https://www.manageengine.com*) and Network Performance Monitor (*https://www.solarwinds.com*).

Working of SNMP



Working of SNMP

SNMP uses a disturbed architecture comprising SNMP managers, SNMP agents, and several related components. The following are some commands associated with SNMP.

- **GetRequest**: Used by the SNMP manager to request information from an SNMP agent
- **GetNextRequest**: Used by the SNMP manager continuously to retrieve all the data stored in an array or table
- **GetResponse**: Used by an SNMP agent to satisfy a request made by the SNMP manager
- **SetRequest**: Used by the SNMP manager to modify the value of a parameter within an SNMP agent's management information base (MIB)
- **Trap**: Used by an SNMP agent to inform the pre-configured SNMP manager of a certain event

The communication process between an SNMP manager and SNMP agent is as follows.

- The SNMP manager (Host X, 10.10.2.1) uses the GetRequest command to send a request for the number of active sessions to the SNMP agent (Host Y, 10.10.2.15). To perform this step, the SNMP manager uses an SNMP service library such as the Microsoft SNMP Management API library (Mgmtapi.dll) or Microsoft WinSNMP API library (Wsnmp32.dll).
- The SNMP agent (Host Y) receives the message and verifies if the community string (Compinfo) is present on its MIB, checks the request against its list of access permissions for that community, and verifies the source IP address.

- If the SNMP agent does not find the community string or access permission in Host Y's MIB database and the SNMP service is set to send an authentication trap, it sends an authentication failure trap to the specified trap destination, Host Z.
- The master agent component of the SNMP agent calls the appropriate extension agent to retrieve the requested session information from the MIB.
- Using the session information retrieved from the extension agent, the SNMP service forms a return SNMP message that contains the number of active sessions and the destination IP address (10.10.2.1) of the SNMP manager, Host X.
- Host Y sends the response to Host X.

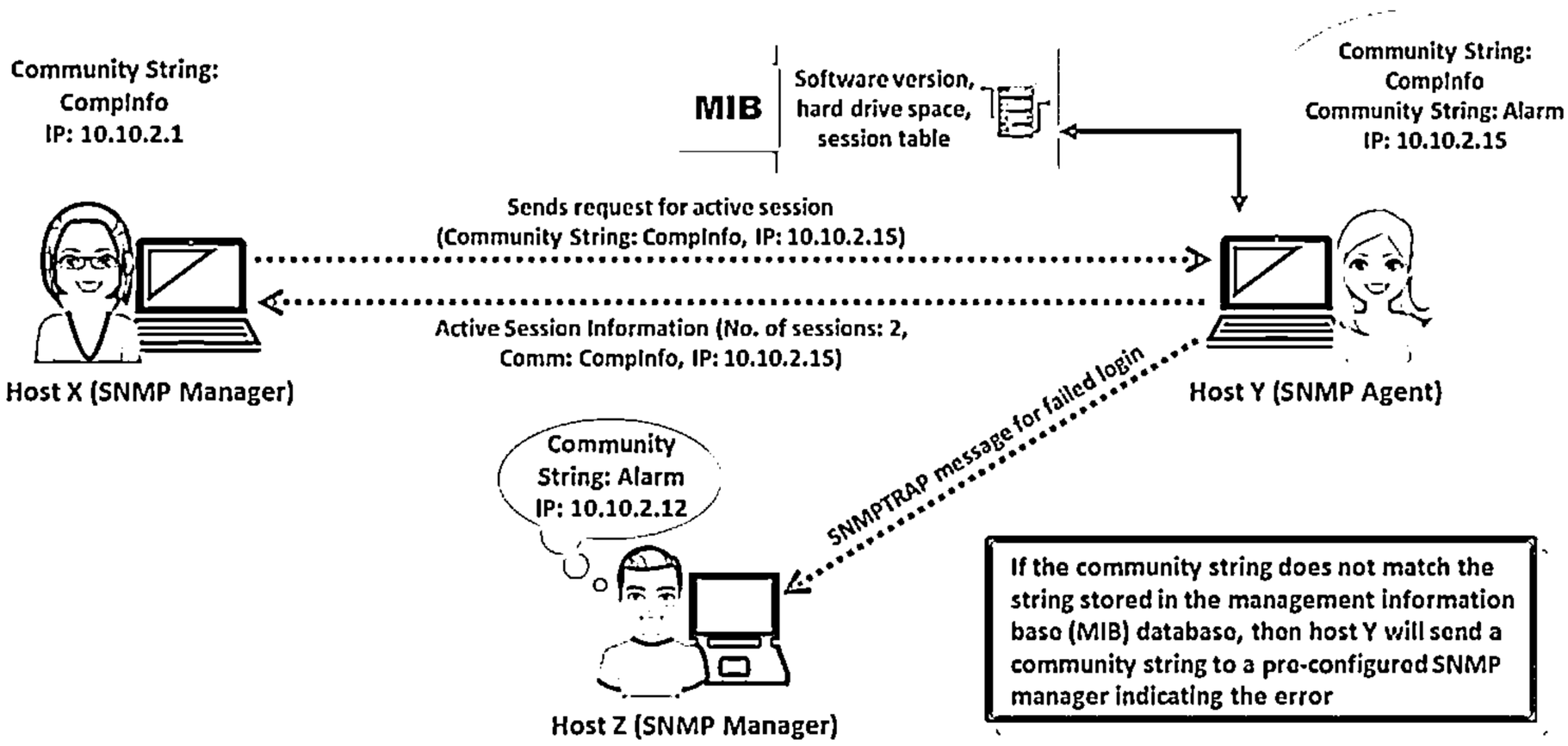
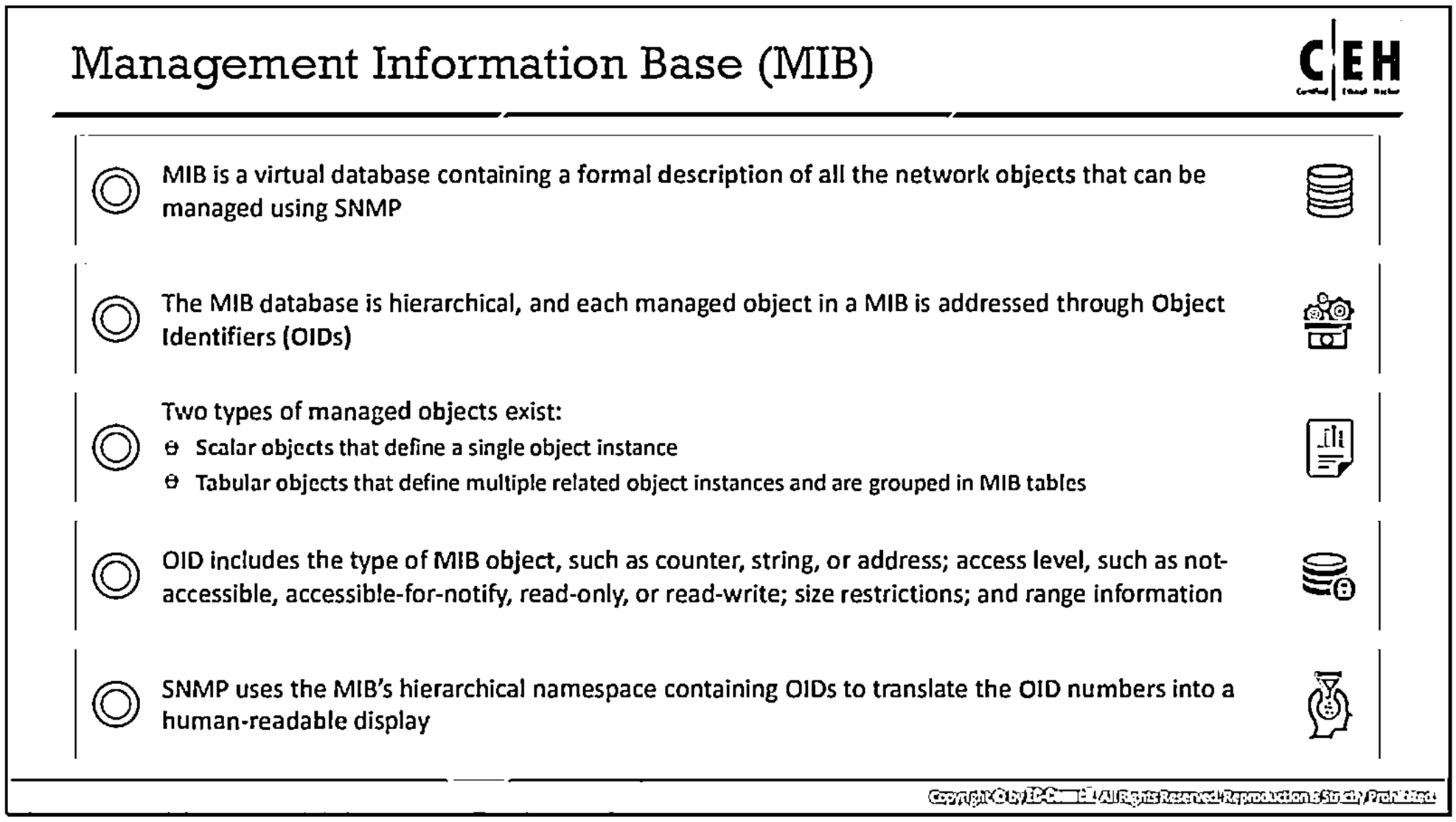


Figure 4.7: Illustration of the working of SNMP



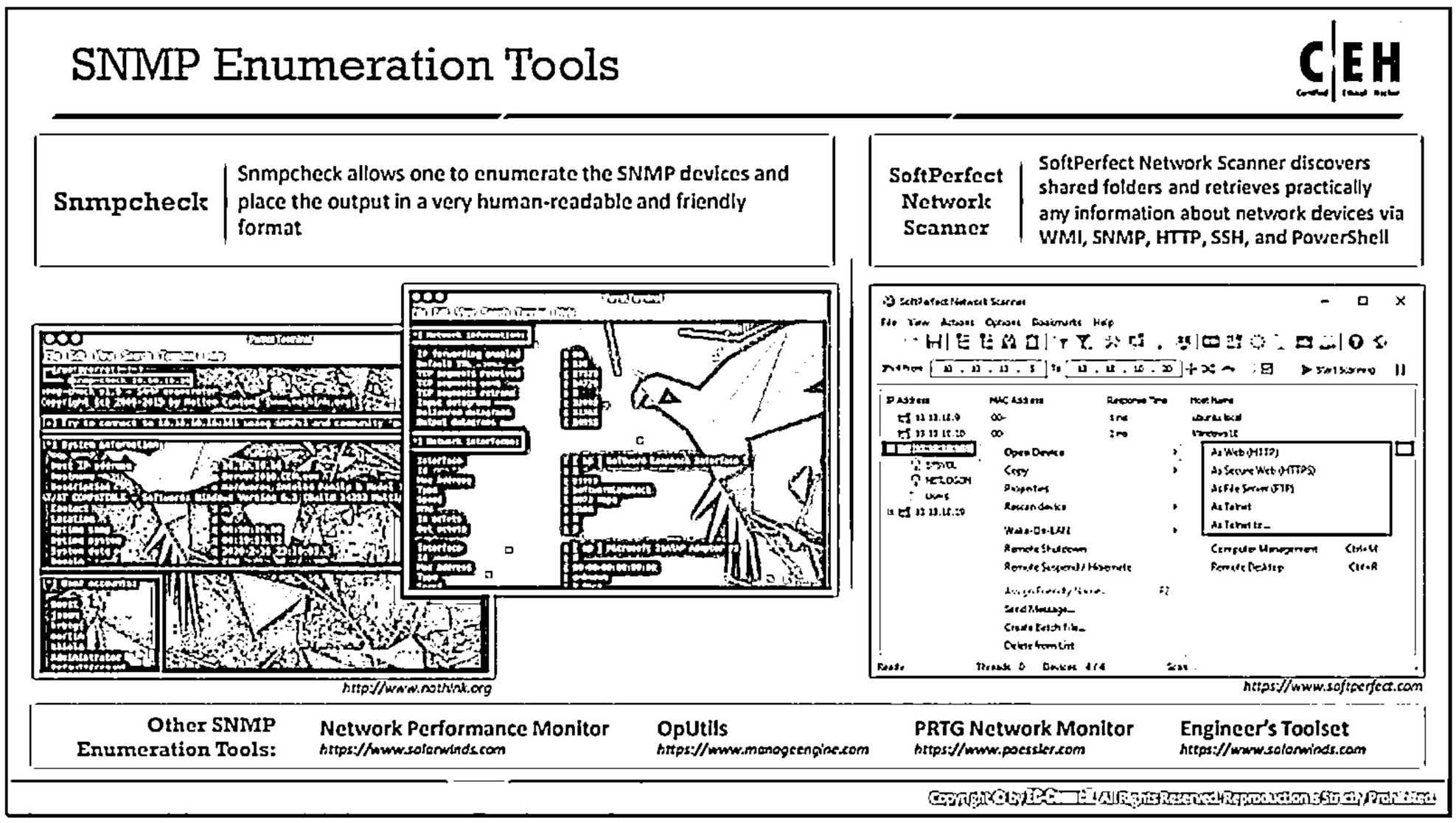
Management Information Base (MIB)

MIB is a virtual database containing a formal description of all the network objects that SNMP manages. It is a collection of hierarchically organized information. It provides a standard representation of the SNMP agent's information and storage. MIB elements are recognized using object identifiers (OIDs). An OID is the numeric name given to an object and begins with the root of the MIB tree. The OID can uniquely identify the object in the MIB hierarchy.

MIB-managed objects include scalar objects, which define a single object instance, and tabular objects, which define a group of related object instances. OIDs include the object's type (such as counter, string, or address), access level (such as read or read/write), size restrictions, and range information. The SNMP manager converts the OIDs into a human-readable display using the MIB as a codebook.

A user can access the contents of the MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. For example, http://IP.Address/Lseries.mib or http://library_name/Lseries.mib.Microsoft provides the list of MIBs that are installed with the SNMP service in the Windows resource kit. The major MIBs are .as follows:

- **DHCP.MIB**: Monitors network traffic between DHCP servers and remote hosts
- **HOSTMIB.MIB**: Monitors and manages host resources
- **LNMIB2.MIB**: Contains object types for workstation and server services
- **MIB_II.MIB:** Manages TCP/IP-based Internet using a simple architecture and system
- **WINS.MIB**: For the Windows Internet Name Service (WINS)



SNMP Enumeration Tools

SNMP enumeration tools are used to scan a single IP address or a range of IP addresses of SNMP-enabled network devices to monitor, diagnose, and troubleshoot security threats.

- **Snmpcheck (snmp_enum Module)**

  Source: *http://www.nothink.org*

  Snmpcheck is an open-source tool distributed under the GNU General Public License (GPL). Its goal is to automate the process of gathering information on any device with SNMP support (Windows, Unix-like, network appliances, printers, etc.). Snmpcheck allows the enumeration of SNMP devices and places the output in a human-readable and user-friendly format. It could be useful for penetration testing or systems monitoring.

  Attackers use this tool to gather information about the target, such as contact, description, write access, devices, domain, hardware and storage information, hostname, Internet Information Services (IIS) statistics, IP forwarding, listening UDP ports, location, mountpoints, network interfaces, network services, routing information, software components, system uptime, TCP connections, total memory, uptime, and user accounts.

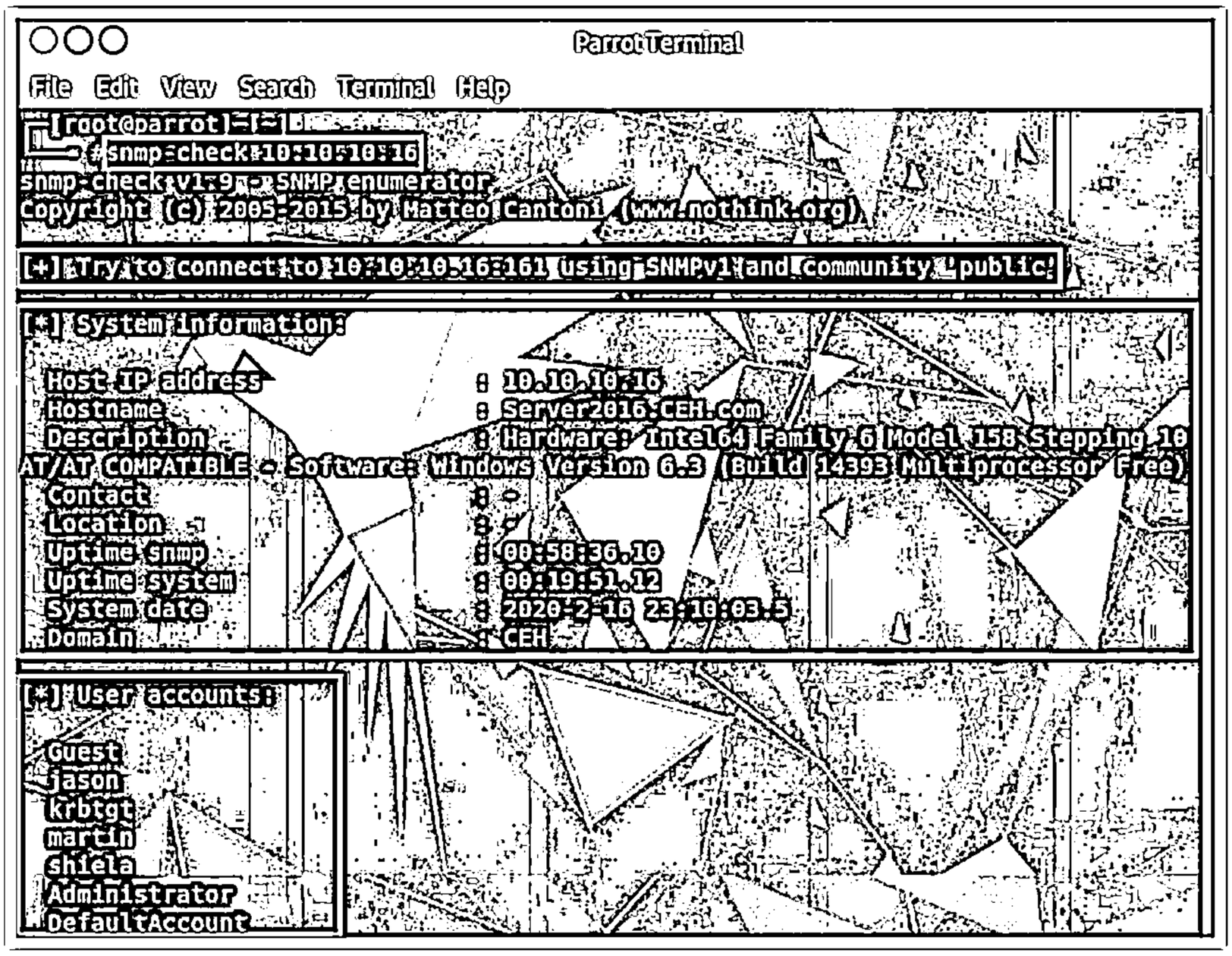


Figure 4.8: Screenshot of snmpcheck showing system information and user accounts

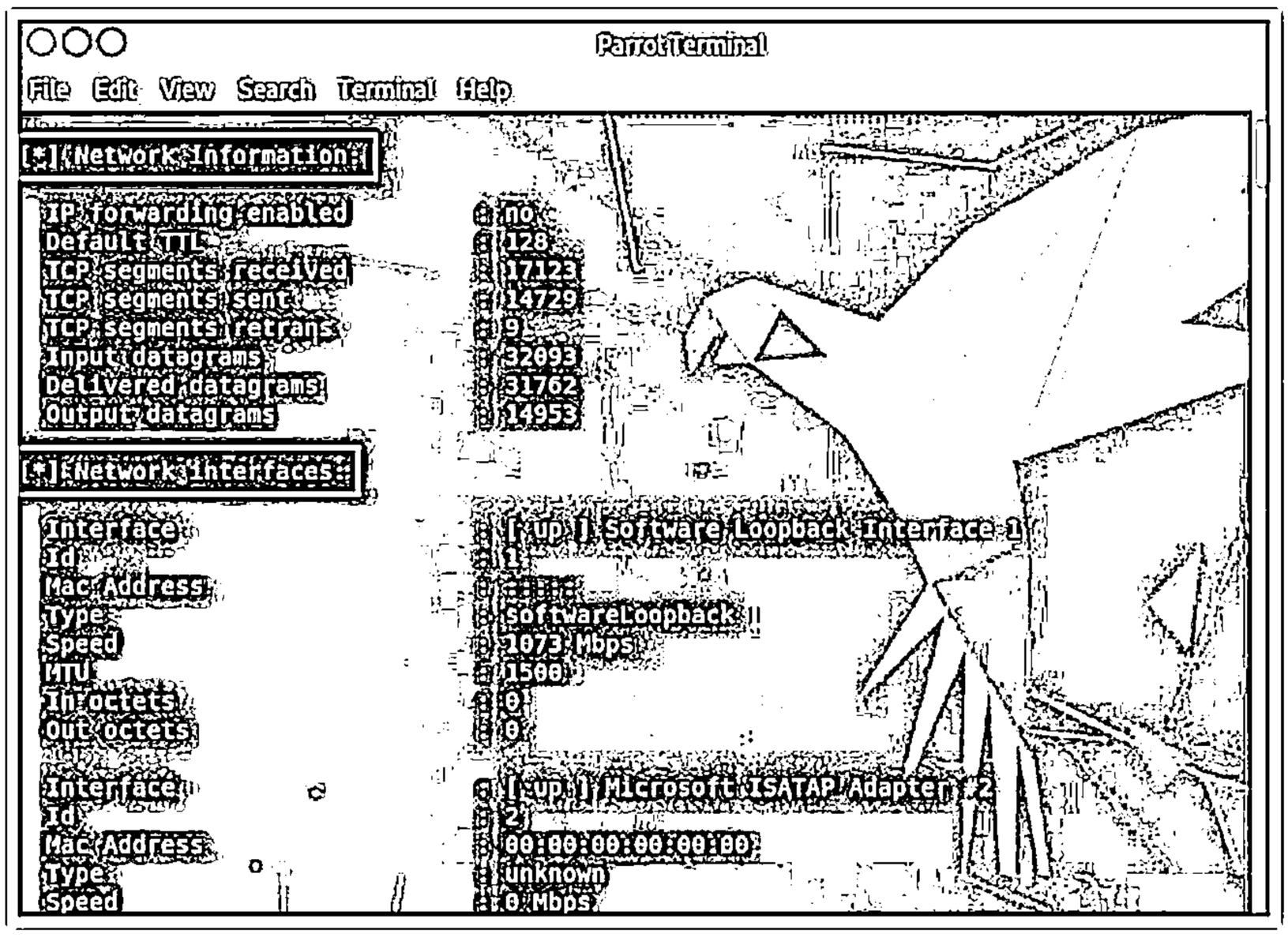


Figure 4.9: Screenshot of snmpcheck showing network information and interfaces

- **SoftPerfect Network Scanner**

  Source: *https://www.softperfect.com*

  SoftPerfect Network Scanner can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via Windows Management Instrumentation (WMI), SNMP, Hypertext Transfer Protocol (HTTP), SSH, and PowerShell. It also scans for remote services, registry, files, and performance counters; offers flexible filtering and display options; and exports NetScan results to a variety of formats ranging from Extensible Markup Language (XML) to JavaScript Object Notation (JSON).

  Moreover, SoftPerfect Network Scanner can check for a user-defined port and report if one is open. In addition, it can resolve host names and auto-detect the local and external IP range. It supports remote shutdown and Wake-on-LAN.

  Attackers uses this tool to gather information about a shared folder and network devices.

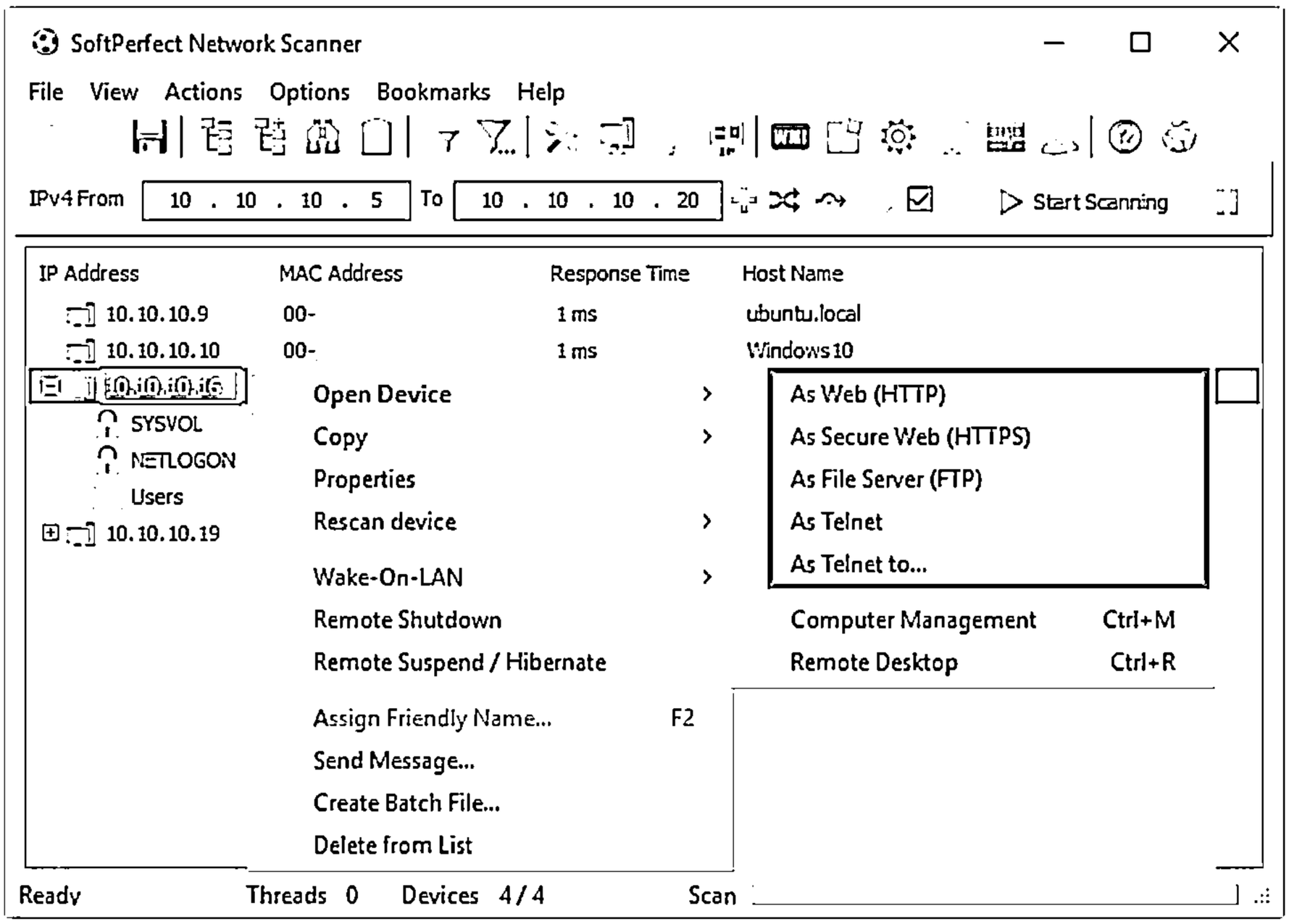


Figure 4.10: Screenshot of SoftPerfect Network Scanner

The following are some additional SNMP enumeration tools:

- Network Performance Monitor (*https://www.solarwinds.com*)
- OpUtils (*https://www.manageengine.com*)
- PRTG Network Monitor (*https://www.paessler.com*)
- Engineer's Toolset (*https://www.solarwinds.com*)

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

LDAP Enumeration

1. Lightweight directory access protocol (LDAP) is an Internet protocol for accessing distributed directory services
2. Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory
3. A client starts a LDAP session by connecting to a directory system agent (DSA) on TCP port 389 and then sends an operation request to the DSA
4. Information is transmitted between the client and server using basic encoding rules (BER)
5. Attackers query the LDAP service to gather information, such as valid usernames, addresses, and departmental details, which can be further used to perform attacks

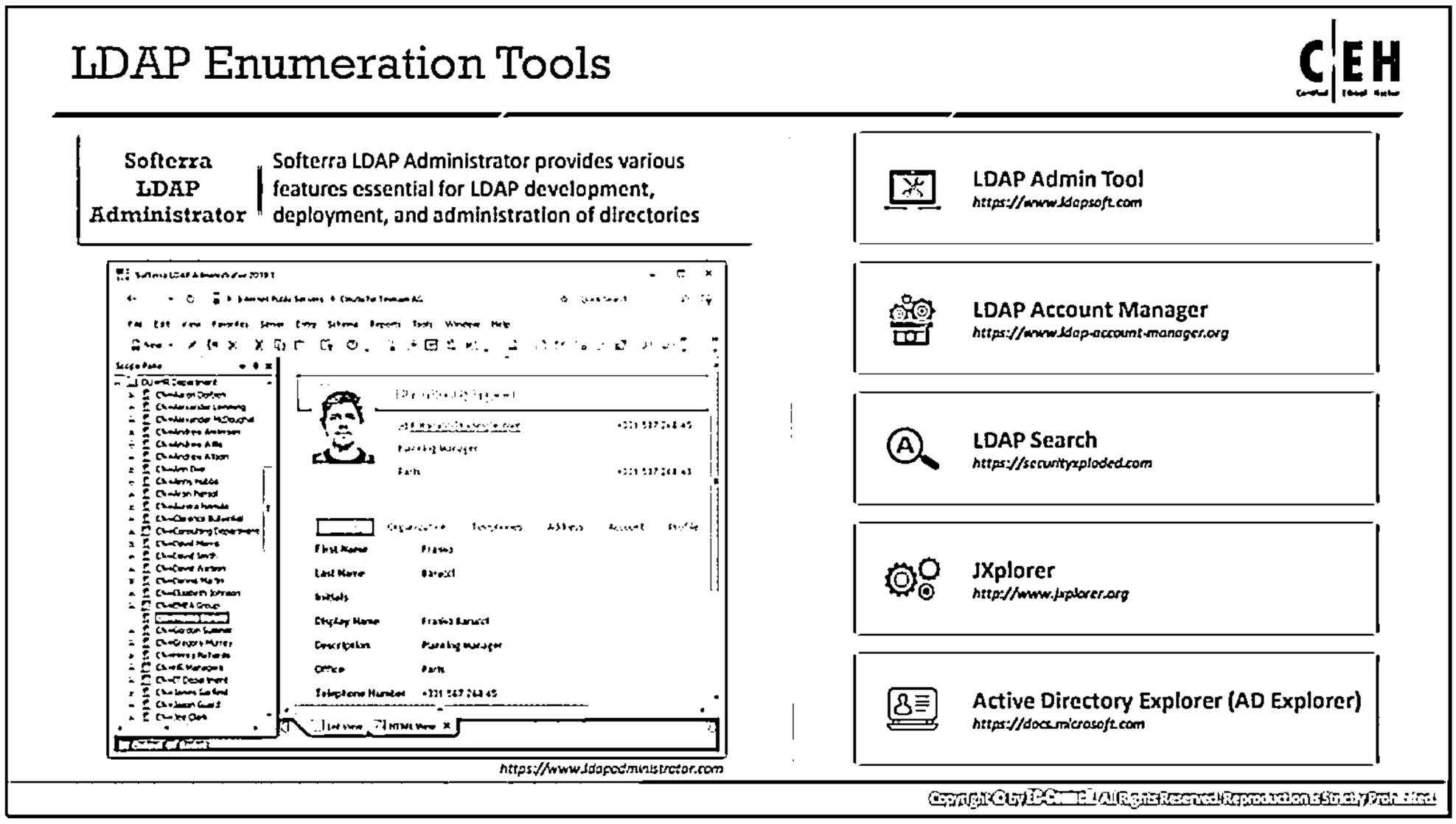
LDAP Enumeration

Various protocols enable communication and manage data transfer between network resources. All these protocols carry valuable information about network resources along with the data. An external user who successfully enumerates that information by manipulating the protocols can break into the network and may misuse the network resources. The Lightweight Directory Access Protocol (LDAP) is one such protocol that accesses the directory listings. This section focuses on

LDAP enumeration, the information extracted via LDAP enumeration, and LDAP enumeration tools.

LDAP is an Internet protocol for accessing distributed directory services. LDAP accesses directory listings within Active Directory or from other directory services. LDAP is a hierarchical or logical form of a directory, similar to a company's organizational chart. Directory services may provide any organized set of records, often in a hierarchical and logical structure, such as a corporate email directory. It uses DNS for quick lookups and the fast resolution of queries. A client starts an LDAP session by connecting to a Directory System Agent (DSA), typically on TCP port 389, and sends an operation request to the DSA. The Basic Encoding Rules (BER) format is used to transmit information between the client and server.

An attacker can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names, which an attacker can use to launch attacks.



LDAP Enumeration Tools

There are many LDAP enumeration tools that access the directory listings within Active Directory or other directory services. By using these tools, attackers can enumerate information such as valid usernames, addresses, and departmental details from different LDAP servers.

- **Softerra LDAP Administrator**

  Source: *https://www.ldapadministrator.com*

  Softerra LDAP Administrator is an LDAP administration tool that works with LDAP servers such as Active Directory, Novell Directory Services, and Netscape/iPlanet. It browses and manages LDAP directories. As shown in the screenshot, attackers use Softerra LDAP Administrator to enumerate user details such as first name, last name, email address, designation, office location, and telephone number.

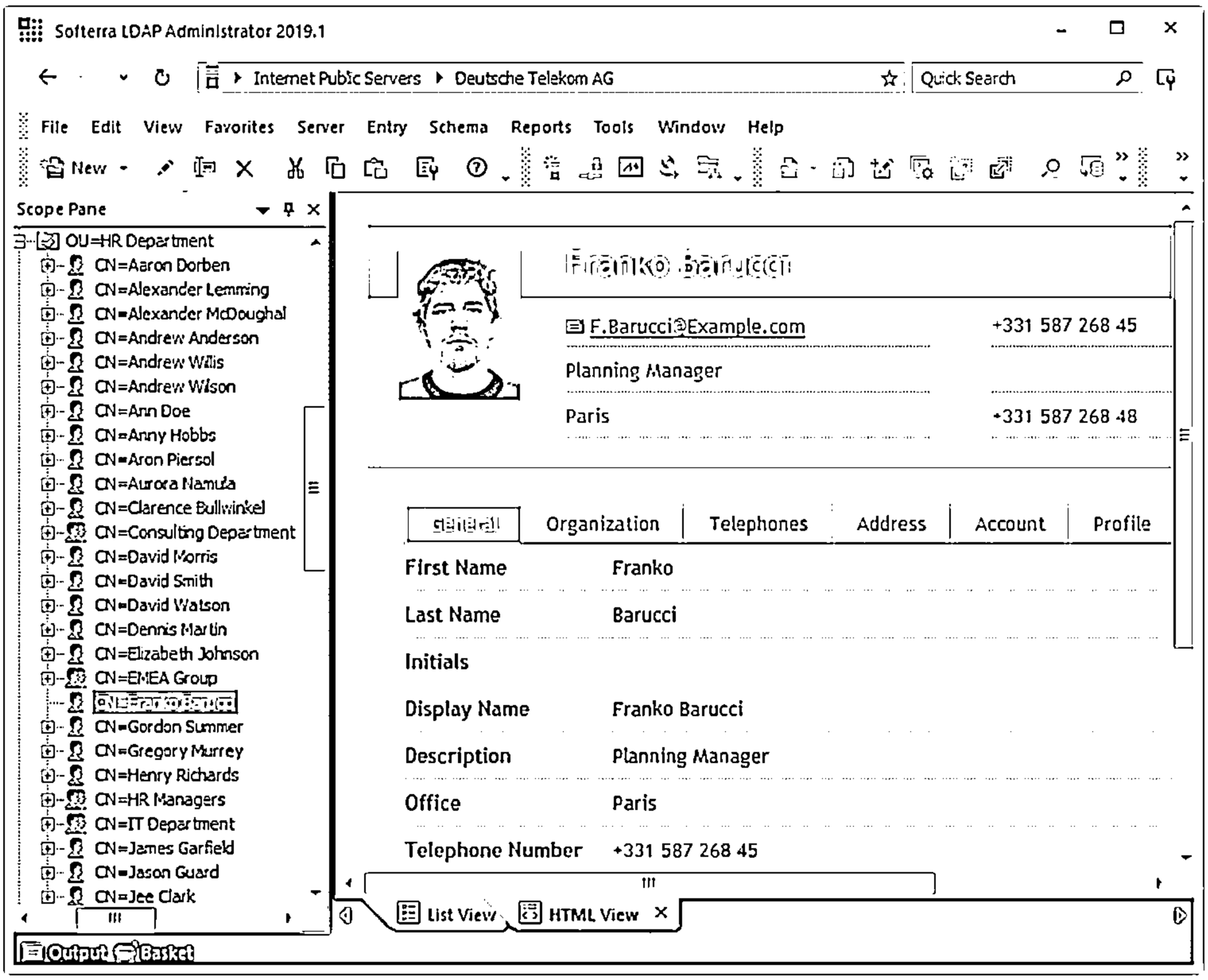
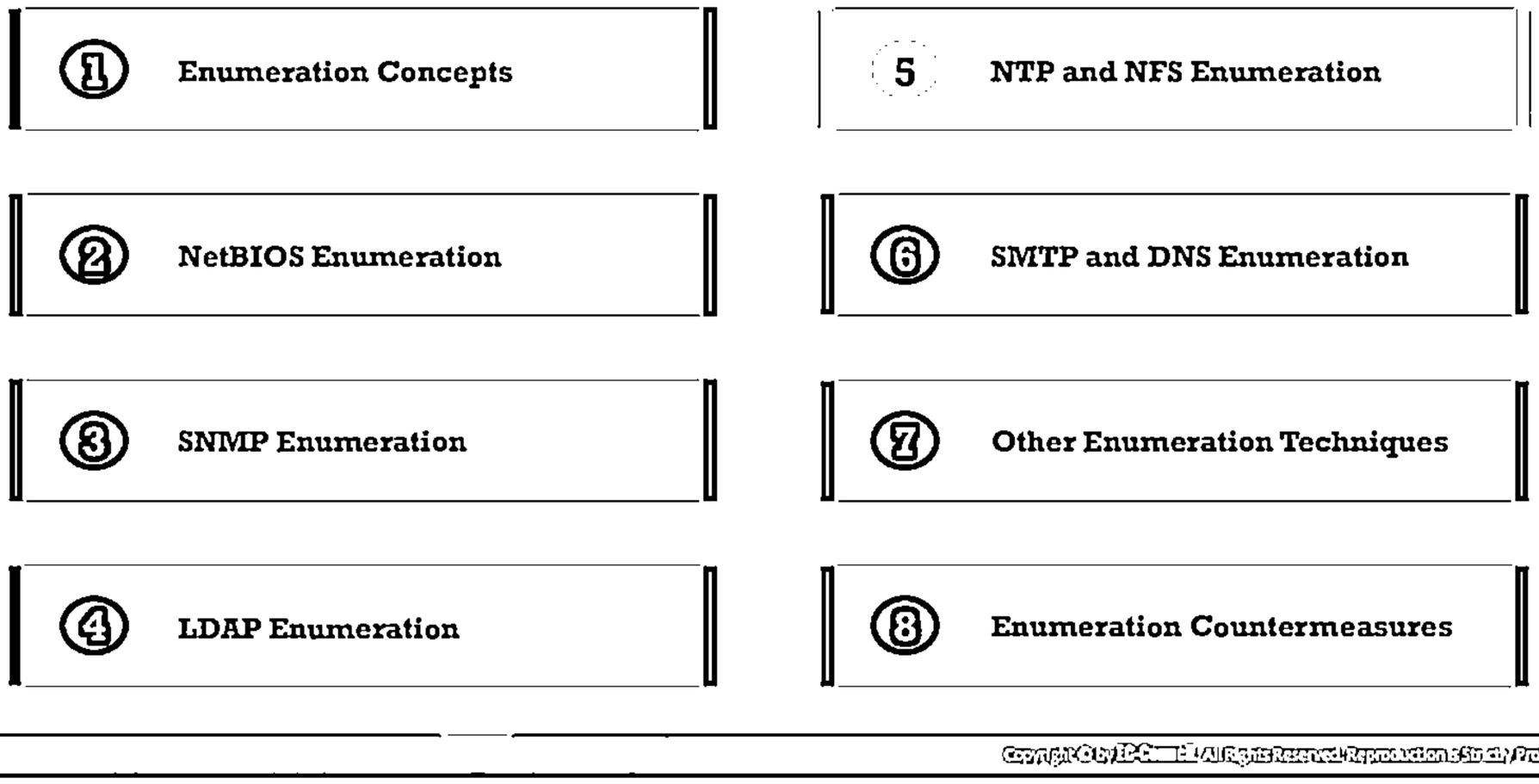


Figure 4.11: Screenshot of Softerra LDAP Administrator

The following are some additional LDAP enumeration tools:

- LDAP Admin Tool (*https://www.ldapsoft.com*)
- LDAP Account Manager (*https://www.ldap-account-manager.org*)
- LDAP Search (*https://securityxploded.com*)
- JXplorer (*http://www.jxplorer.org*)
- Active Directory Explorer (AD Explorer) (*https://docs.microsoft.com*)

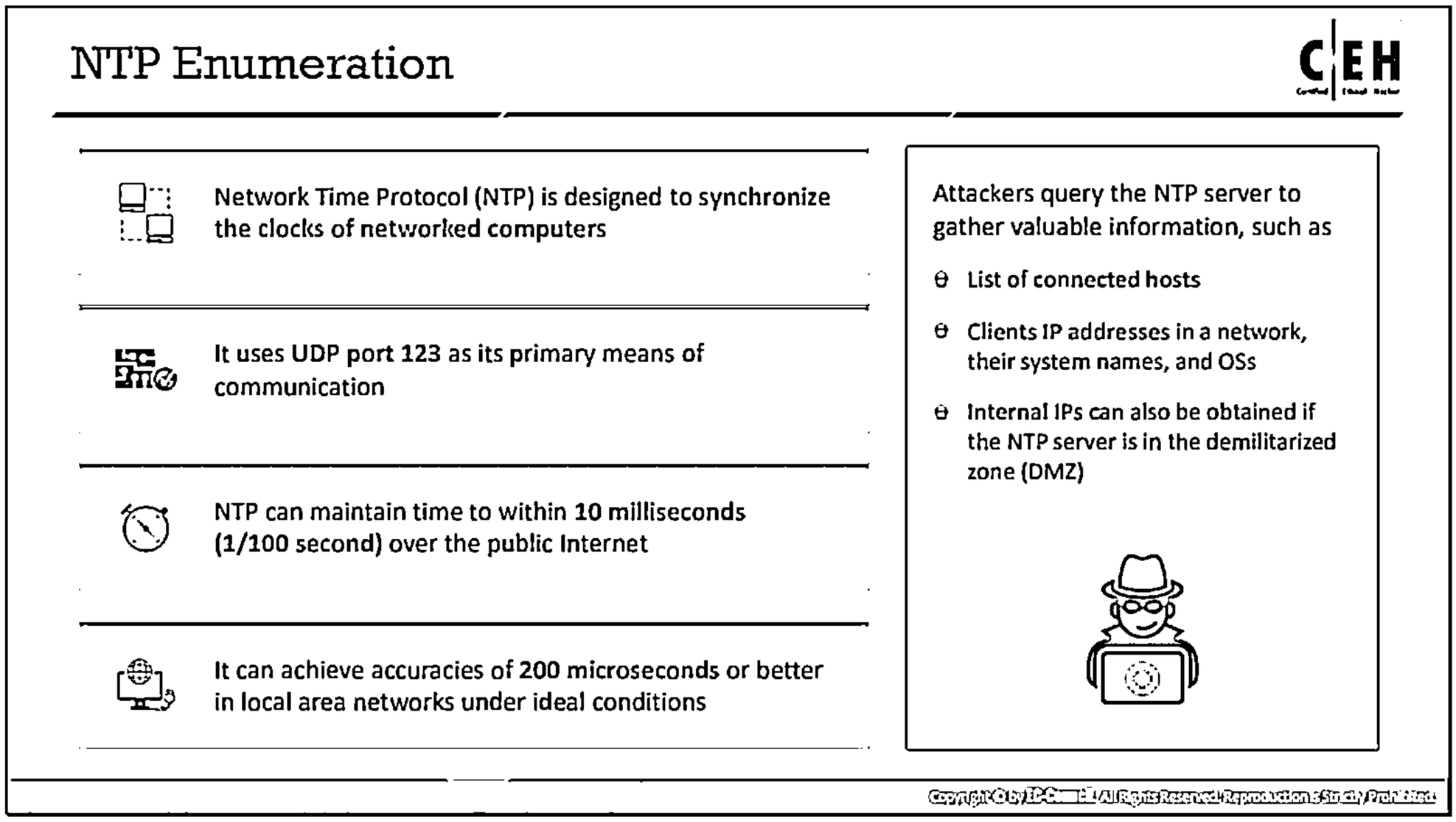
Module Flow



NTP and NFS Enumeration

Administrators often overlook the Network Time Protocol (NTP) server when considering security. However, if queried properly, it can provide valuable network information to an attacker. Therefore, it is necessary to know what information an attacker can obtain about a network through NTP enumeration. The Network File System (NFS) is used for the management of remote file access. NFS enumeration helps attackers to gather information such as a list of clients connected to the NFS server, along with their IP addresses, and exported directories.

This section describes NTP enumeration, the information extracted via NTP enumeration, various NTP enumeration commands, NTP enumeration tools, and NFS enumeration techniques and tools.

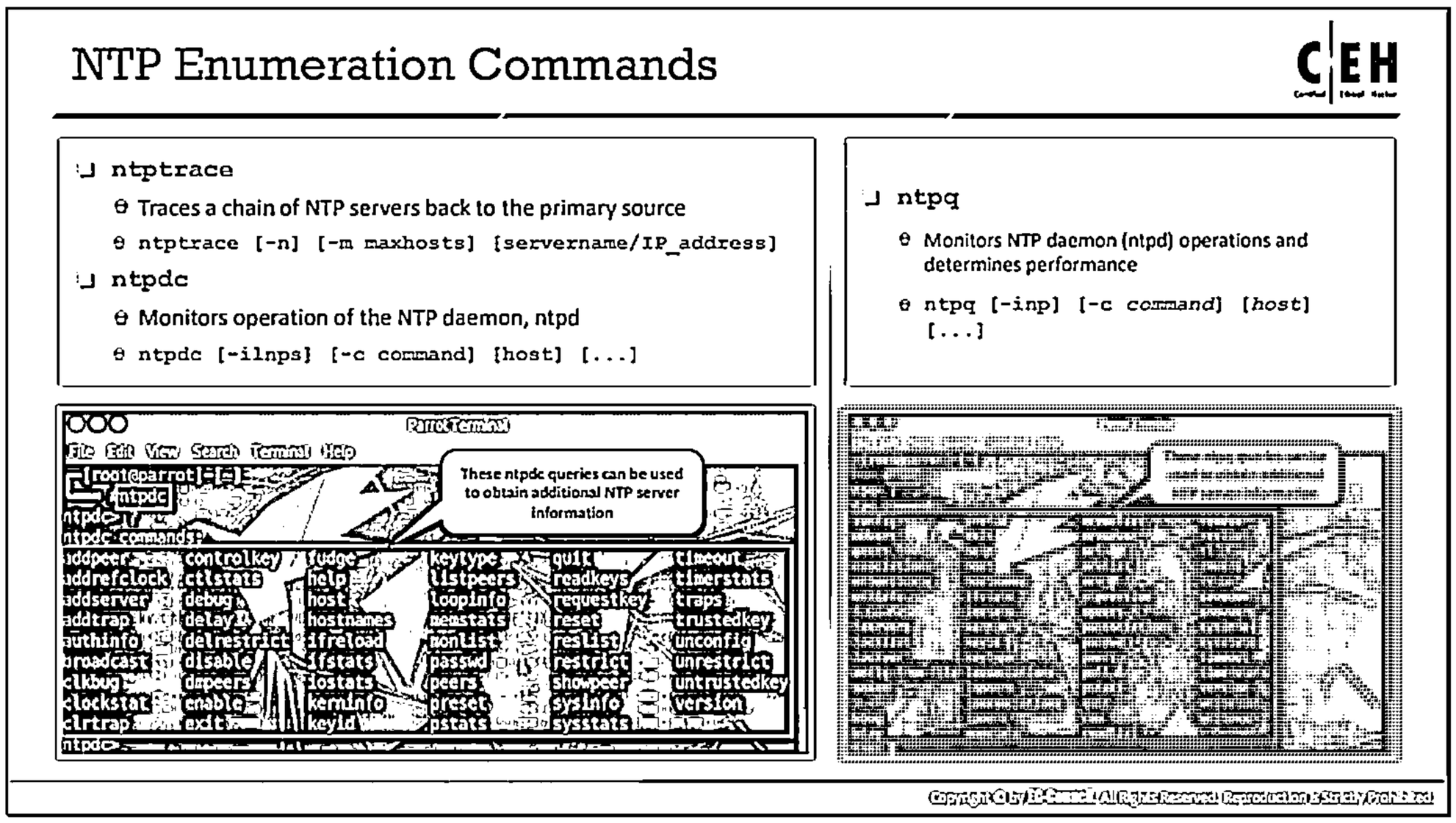


NTP Enumeration

NTP is designed to synchronize clocks of networked computers. It uses UDP port 123 as its primary means of communication. NTP can maintain time within an error of 10 ms over the public Internet. Furthermore, it can achieve an accuracy of 200 µs or better in LANs under ideal conditions.

The following are some pieces of information an attacker can obtain by querying an NTP server:

- List of hosts connected to the NTP server
- Clients IP addresses in the network, their system names, and OSs
- Internal IPs, if the NTP server is in the demilitarized zone (DMZ)



NTP Enumeration Commands

NTP enumeration commands such as `ntpdate`, `ntptrace`, `ntpdc`, and `ntpq` are used to query an NTP server for valuable information.

- **ntpdate**

  This command collects the number of time samples from several time sources. Its syntax is as follows:

  ```
  ntpdate [-46bBdqsuv] [-a key] [-e authdelay] [-k keyfile] [-o version] [-p samples] [-t timeout] [ -U user_name] server [...]
  ```

`-4`	Force DNS resolution of given host names to the IPv4 namespace
`-6`	Force DNS resolution of given host names to the IPv6 namespace
`-a key`	Enable the authentication function/specify the key identifier to be used for authentication
`-B`	Force the time to always be slewed
`-b`	Force the time to be stepped
`-d`	Enable debugging mode
`-e authdelay`	Specify the processing delay to perform an authentication function
`-k keyfile`	Specify the path for the authentication key file as the string “keyfile”; the default is /etc/ntp/keys
`-o version`	Specify the NTP version for outgoing packets as an integer version, which can be 1 or 2; the default is 4

`-p samples`	Specify the number of samples to be acquired from each server, with values ranging from 1–8; the default is 4
`-q`	Query only; do not set the clock
`-s`	Divert logging output from the standard output (default) to the system syslog facility
`-t timeout`	Specify the maximum wait time for a server response; the default is 1 s
`-u`	Use an unprivileged port for outgoing packets
`-v`	Be verbose; logs ntpdate's version identification string

Table 4.4: ntpdate parameters and their respective functions

Figure 4.12: Screenshot of the ntpdate command, showing debugging information for a given IP

- **ntptrace**

  This command determines where the NTP server obtains the time from and follows the chain of NTP servers back to its primary time source. Attackers use this command to trace the list of NTP servers connected to the network. Its syntax is as follows:

  `ntptrace [-n] [-m maxhosts] [servername/IP_address]`

`-n`	Do not print host names and show only IP addresses; may be useful if a name server is down
`-m maxhosts`	Set the maximum number of levels up the chain to be followed

Table 4.5: ntptrace parameters and their respective functions

Example:

```
# ntptrace
localhost: stratum 4, offset 0.0019529, synch distance 0.143235
10.10.0.1: stratum 2, offset 0.01142
73, synch distance 0.115554
10.10.1.1: stratum 1, offset 0.0017698, synch distance 0.011193
```

- **ntpdc**

  This command queries the ntpd daemon about its current state and requests changes in that state. Attackers use this command to retrieve the state and statistics of each NTP server connected to the target network. Its syntax is as follows:

  ```
  ntpdc [-ilnps] [-c command] [hostname/IP_address]
  ```

`-c`	Following argument interpreted as an interactive format command; multiple -c options may be given
`-i`	Force ntpdc to operate in the interactive mode
`-l`	Obtain a list of peers known to the server(s); this switch is equivalent to -c listpeers
`-n`	Output all host addresses in the dotted-quad numeric format, rather than host names
`-p`	Print a list of the peers as well as a summary of their states; this is equivalent to -c peers
`-s`	Print a list of the peers as well as a summary of their states, but in a slightly different format than the -p switch; this is equivalent to -c dmpeers.

Table 4.6: ntpdc parameters and their respective functions

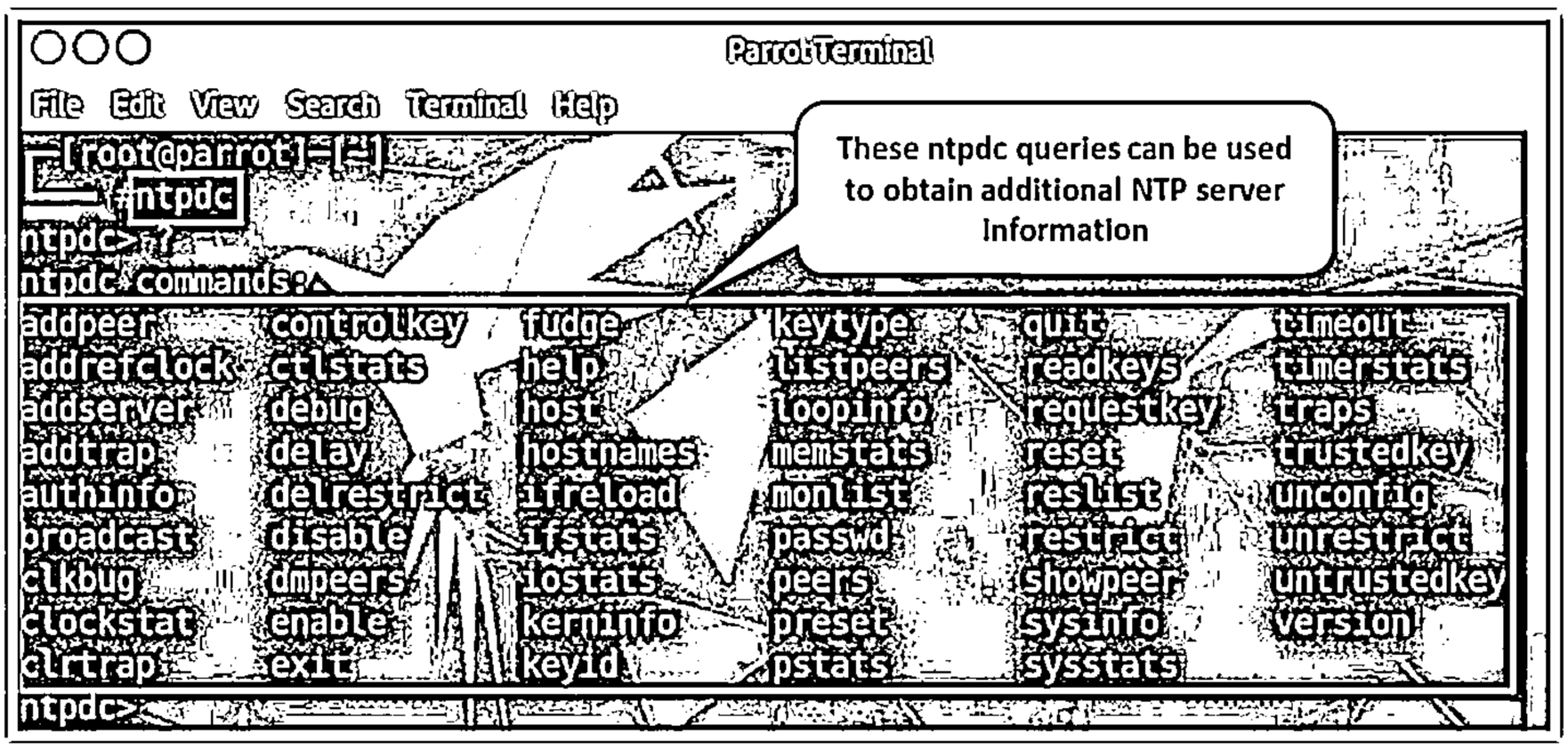


Figure 4.13: Screenshot of the ntpdc command

- **ntpq**

  This command monitors the operations of the NTP daemon `ntpd` and determines performance. Its syntax is as follows:

  ```
  ntpq [-inp] [-c command] [host/IP_address]
  ```

`-c`	Following argument is an interactive format command; multiple -c options may be given
`-d`	Debugging mode
`-i`	Force ntpq to operate in the interactive mode
`-n`	Output all host addresses in the dotted-quad numeric format, rather than host names
`-p`	Print a list of the peers as well as a summary of their states

Table 4.7: ntpq parameters and their respective functions

Example:

```
ntpq> version
ntpq 4.2.8p10@1.3728-o
ntpq> host
current host is localhost
```

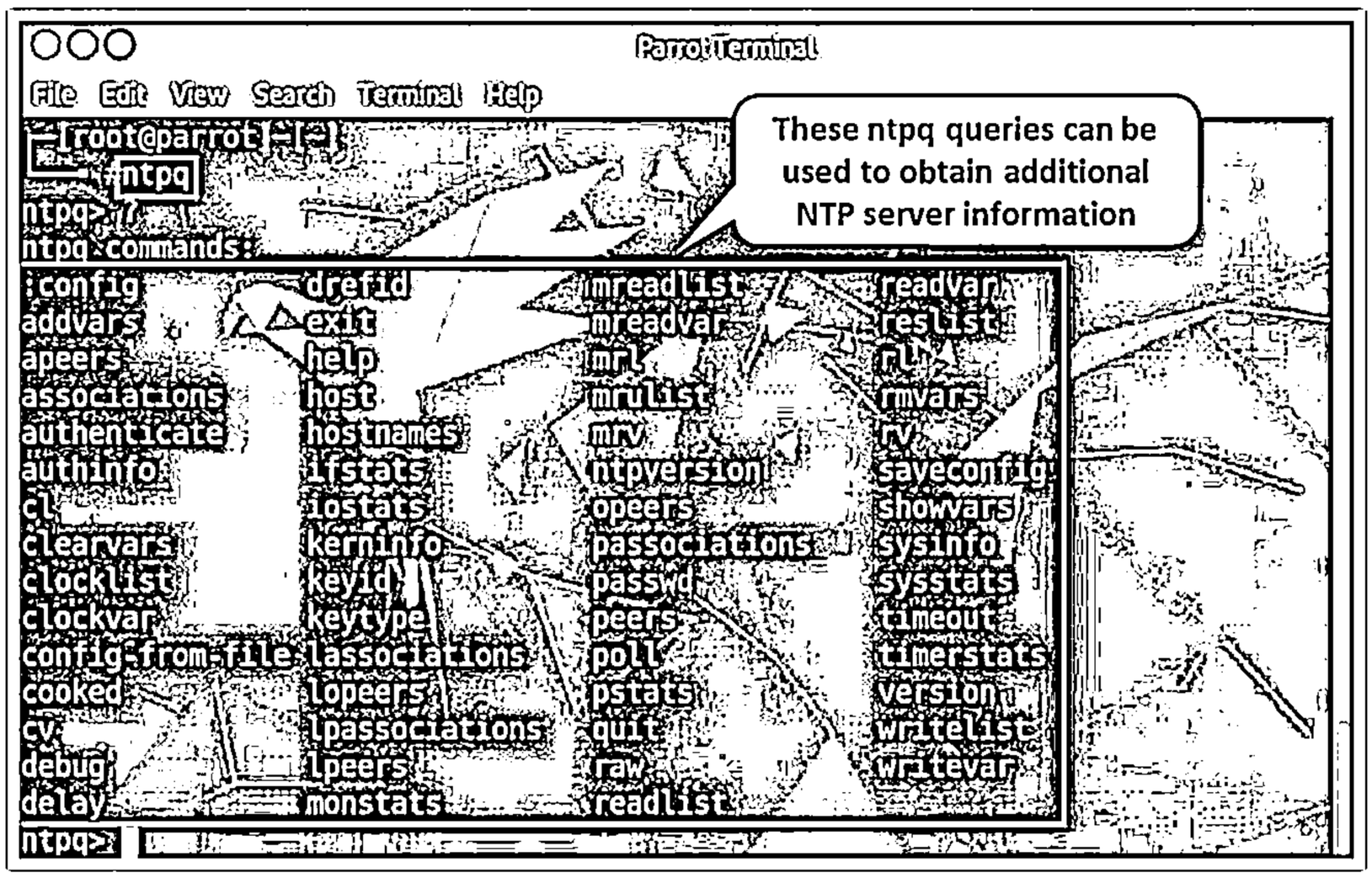
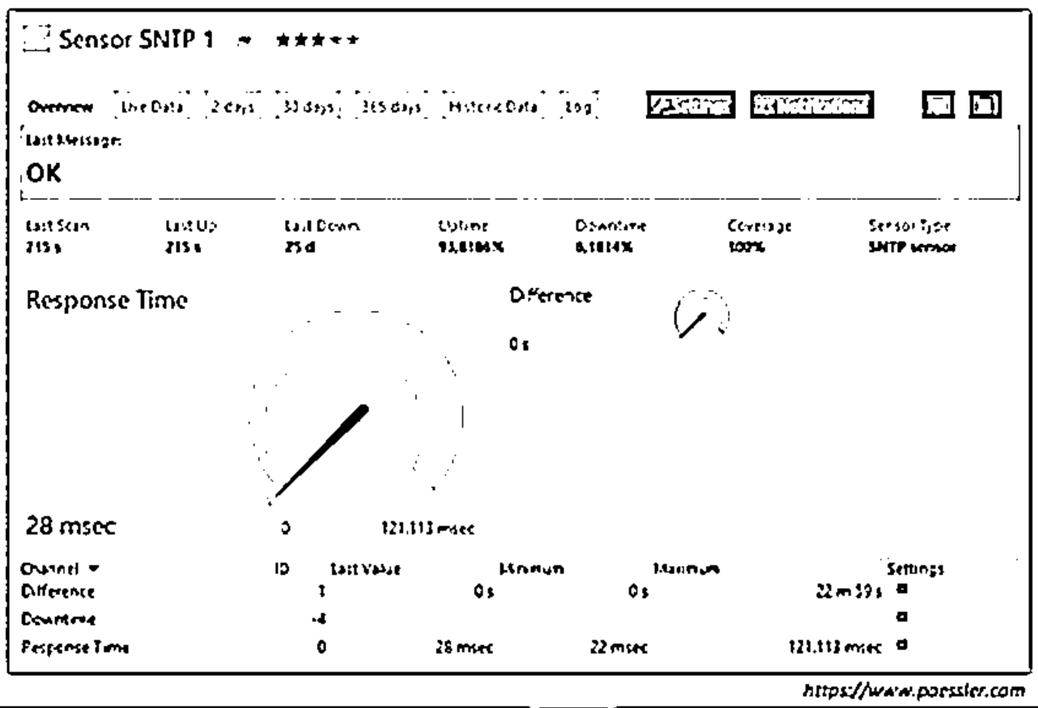


Figure 4.14: Screenshot of ntpq command

NTP Enumeration Tools

- PRTG Network Monitor includes SNTP Sensor monitor, a simple network time protocol (SNTP) server that shows the response time of the server and time difference in comparison to the local system time



NTP Enumeration Tools

- Nmap (*https://nmap.org*)
- Wireshark (*https://www.wireshark.org*)
- udp-proto-scanner (*https://labs.portcullis.co.uk*)
- NTP Server Scanner (*http://www.bytefusion.com*)

NTP Enumeration Tools

NTP enumeration tools are used to monitor the working of NTP and SNTP servers in the network and help in the configuration and verification of connectivity from the time client to the NTP servers.

- **PRTG Network Monitor**

  Source: *https://www.paessler.com*

  PRTG monitors all systems, devices, traffic, and applications of IT infrastructure by using various technologies such as SNMP, WMI, and SSH.

  As shown in the screenshot, attackers use PRTG Network Monitor to retrieve SNTP server details such as the response time from the server, active sensors with the server, and synchronization time.

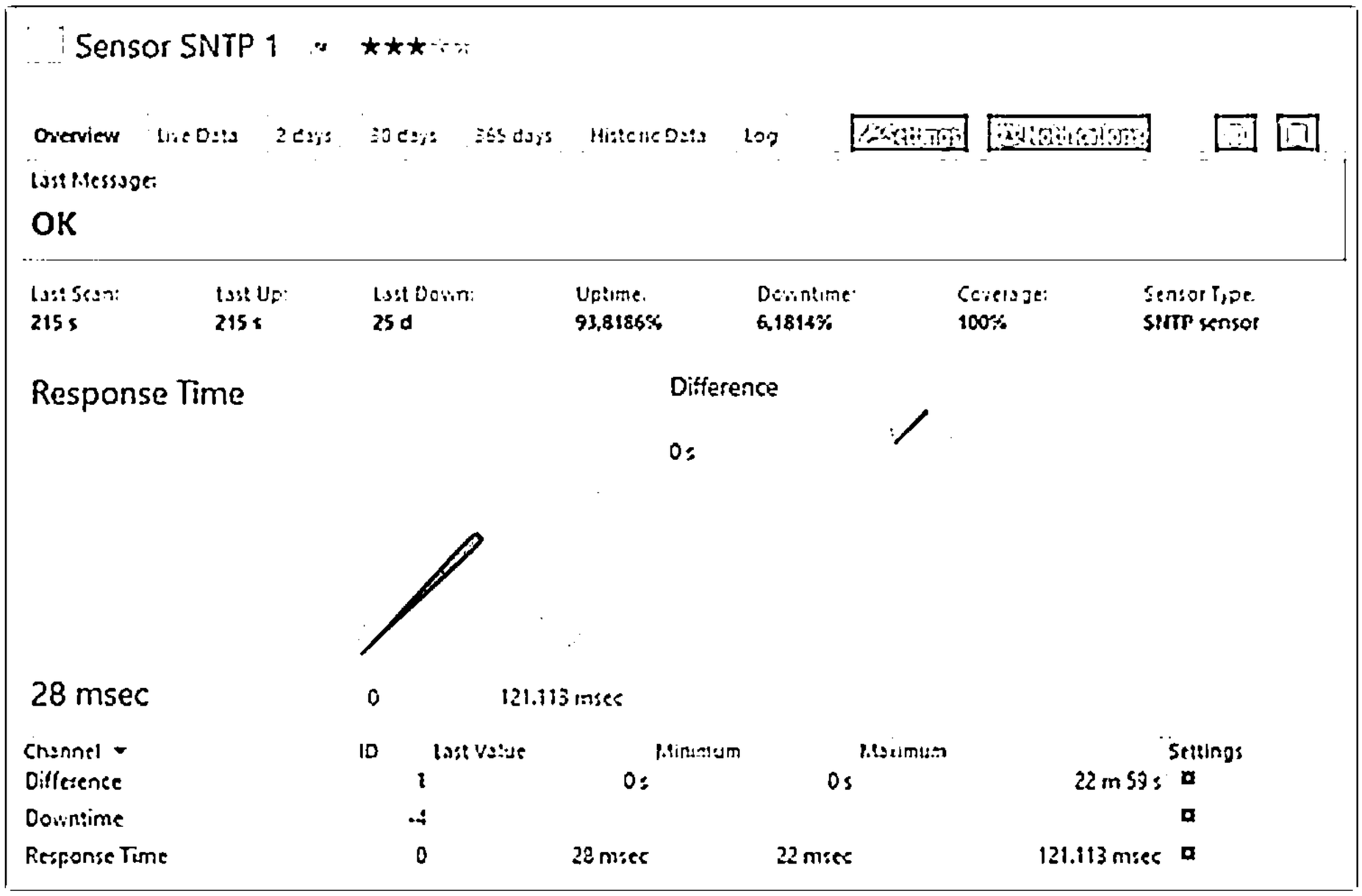
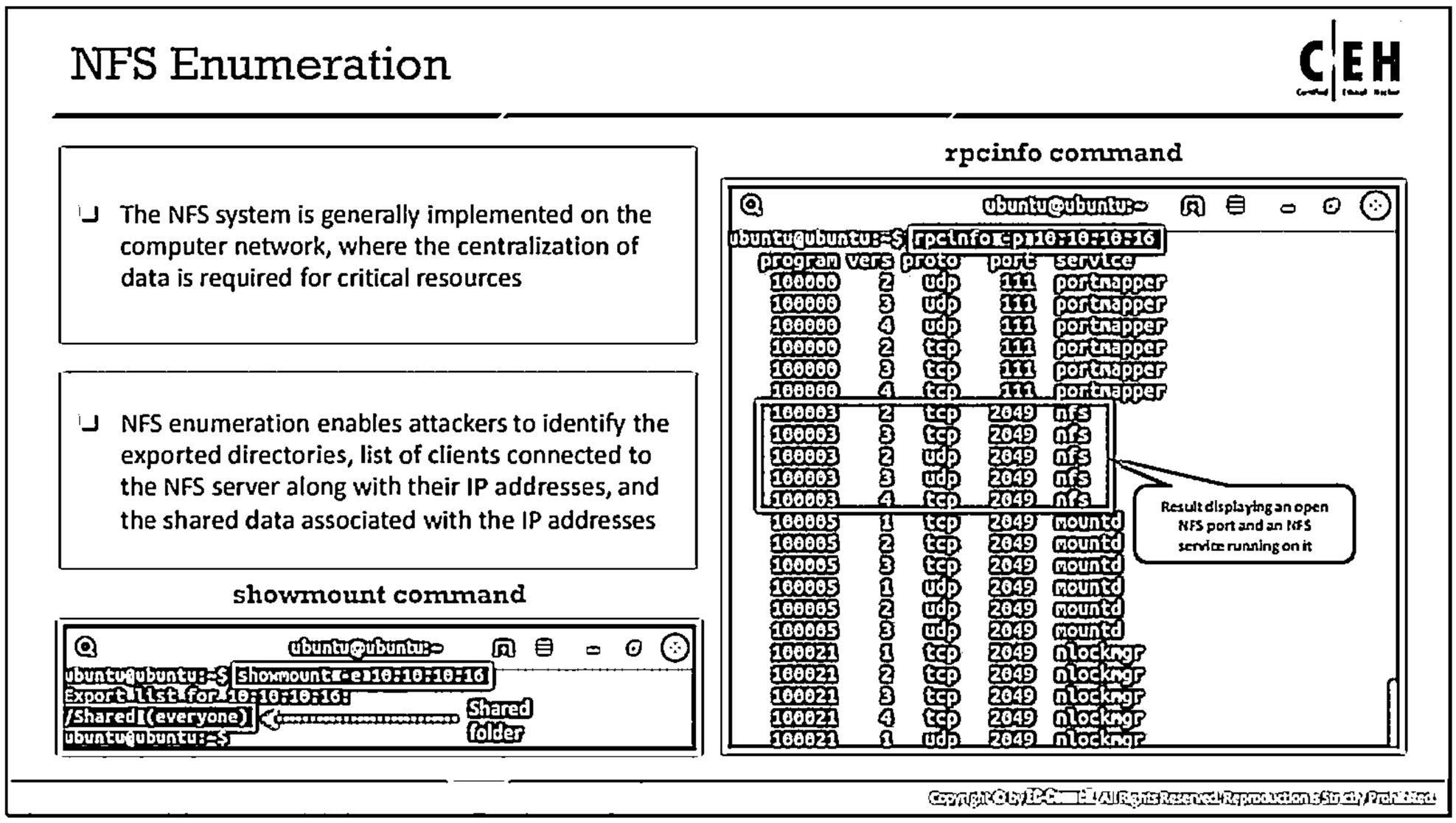


Figure 4.15: Screenshot of PRTG Network Monitor

The following are some NTP enumeration tools:

- Nmap (*https://nmap.org*)
- Wireshark (*https://www.wireshark.org*)
- udp-proto-scanner (*https://labs.portcullis.co.uk*)
- NTP Server Scanner (*http://www.bytefusion.com*)



NFS Enumeration

NFS is a type of file system that enables users to access, view, store, and update files over a remote server. These remote data can be accessed by the client in the same way it is accessed on the local system. Depending on the privileges assigned to the clients, they can either only read or both read and write the data.

An NFS system is generally implemented on a computer network in which the centralization of data is required for critical resources. The remote procedure call (RPC) is used to route and process the request between clients and servers.

To accomplish the task of sharing files and directories over the network, the "exporting" process is used. However, the client first attempts to make the file available for sharing by using the "mounting" process. The `/etc/exports` location on the NFS server contains a list of clients allowed to share files on the server. In this approach, to access the server, the only credential used is the client's IP address. NFS versions before version 4 run on the same security specification.

Enumerating NFS services enables attackers to identify the exported directories, list of clients connected to the NFS server along with their IP addresses, and the shared data associated with the IP addresses. After gathering this information, the attackers can spoof their IP addresses to gain full access to the shared files on the server.

As shown in the screenshot, an attacker runs the following `rpcinfo` command to scan the target IP address for an open NFS port (port 2049) and the NFS services running on it:

```
rpcinfo -p 10.10.10.16
```

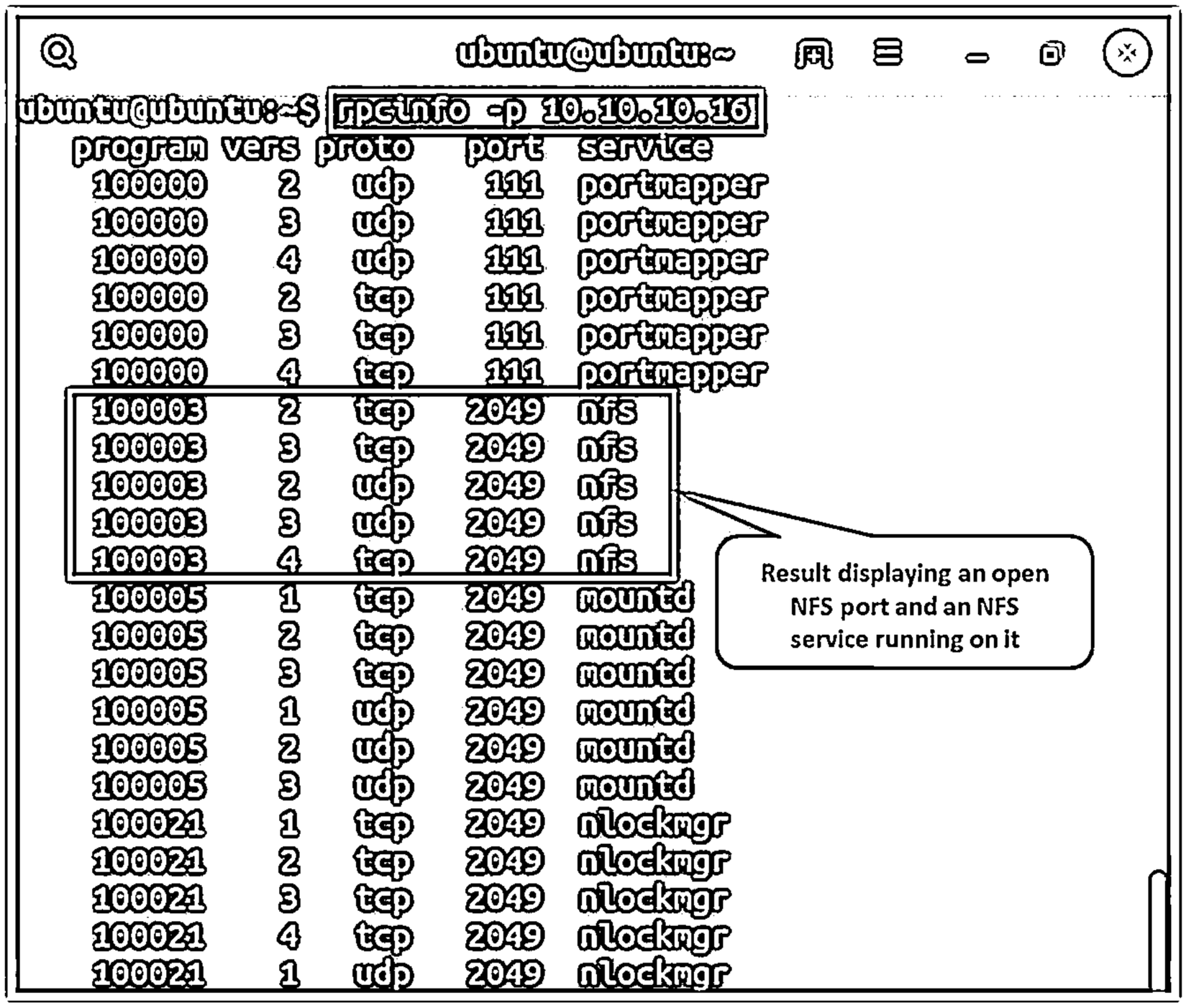


Figure 4.16: Screenshot of rpcinfo command displaying open NFS port and services

As shown in the screenshot, an attacker runs the following command to view the list of shared files and directories:

```
showmount -e 10.10.10.16
```

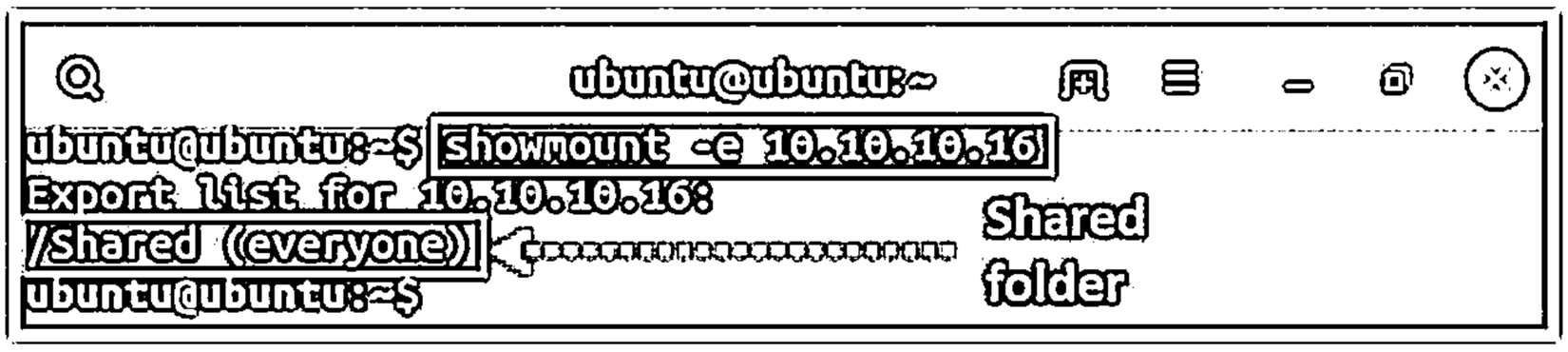
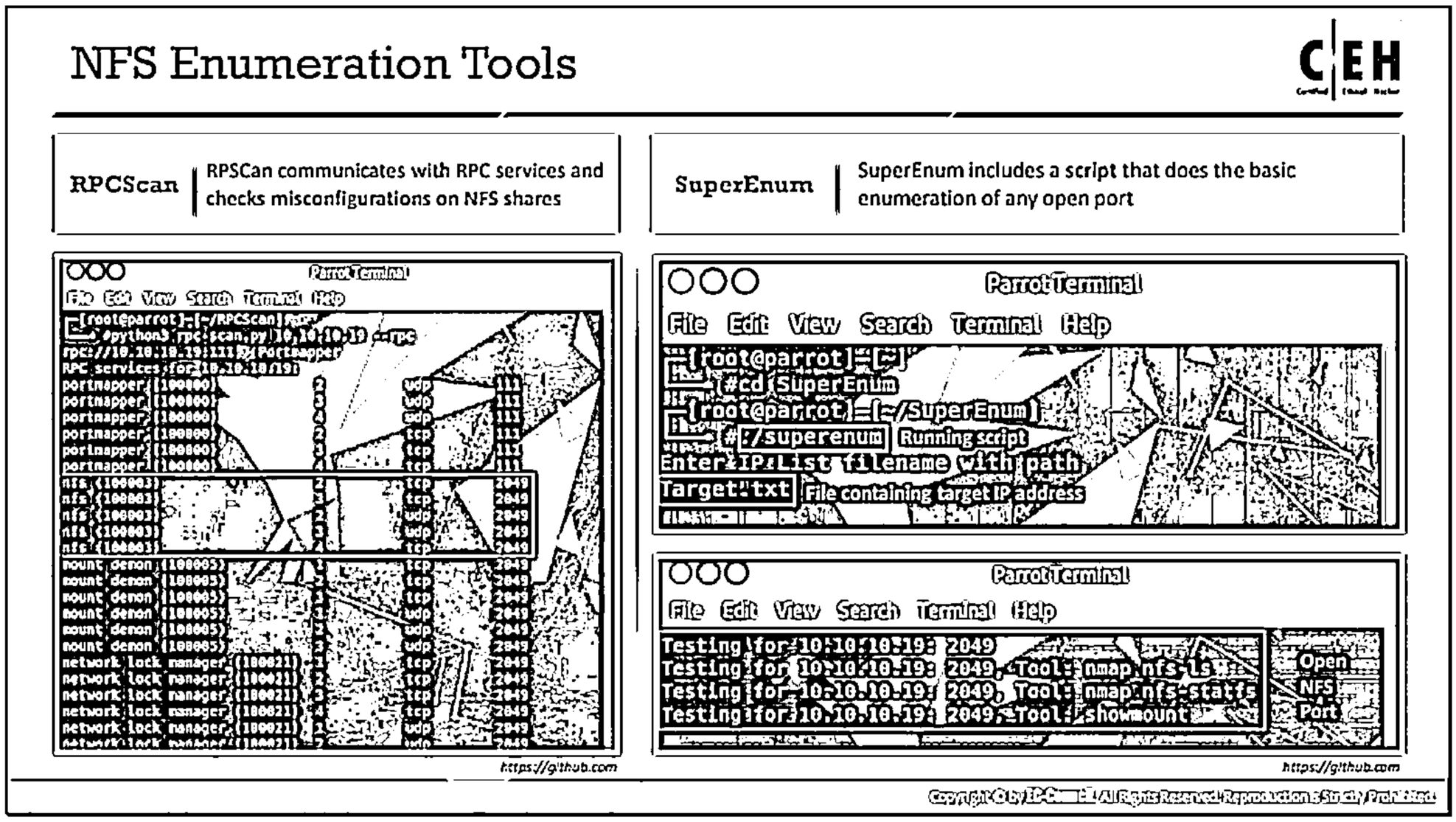


Figure 4.17: Screenshot of the showmount command displaying a shared directory

Further, an attacker can use various other commands and tools to gain access to the NFS server and upload malicious files on the server to launch further attacks.



NFS Enumeration Tools

NFS enumeration tools scan a network within a given range of IP addresses or a single IP address to identify the NFS services running on it. These tools also assist in obtaining a list of RPC services using portmap, a list of NFS shares, and a list of directories accessible through NFS; further, they allow downloading a file shared through the NFS server. Attackers use tools such as RPCScan and SuperEnum to perform NFS enumeration.

- **RPCScan**

  Source: *https://github.com*

  RPCScan communicates with RPC services and checks misconfigurations on NFS shares. As shown in the screenshot, an attacker runs the following command to enumerate a target IP address for active NFS services:

```
Python3 rpc-scan.py 10.10.10.19 --rpc
```

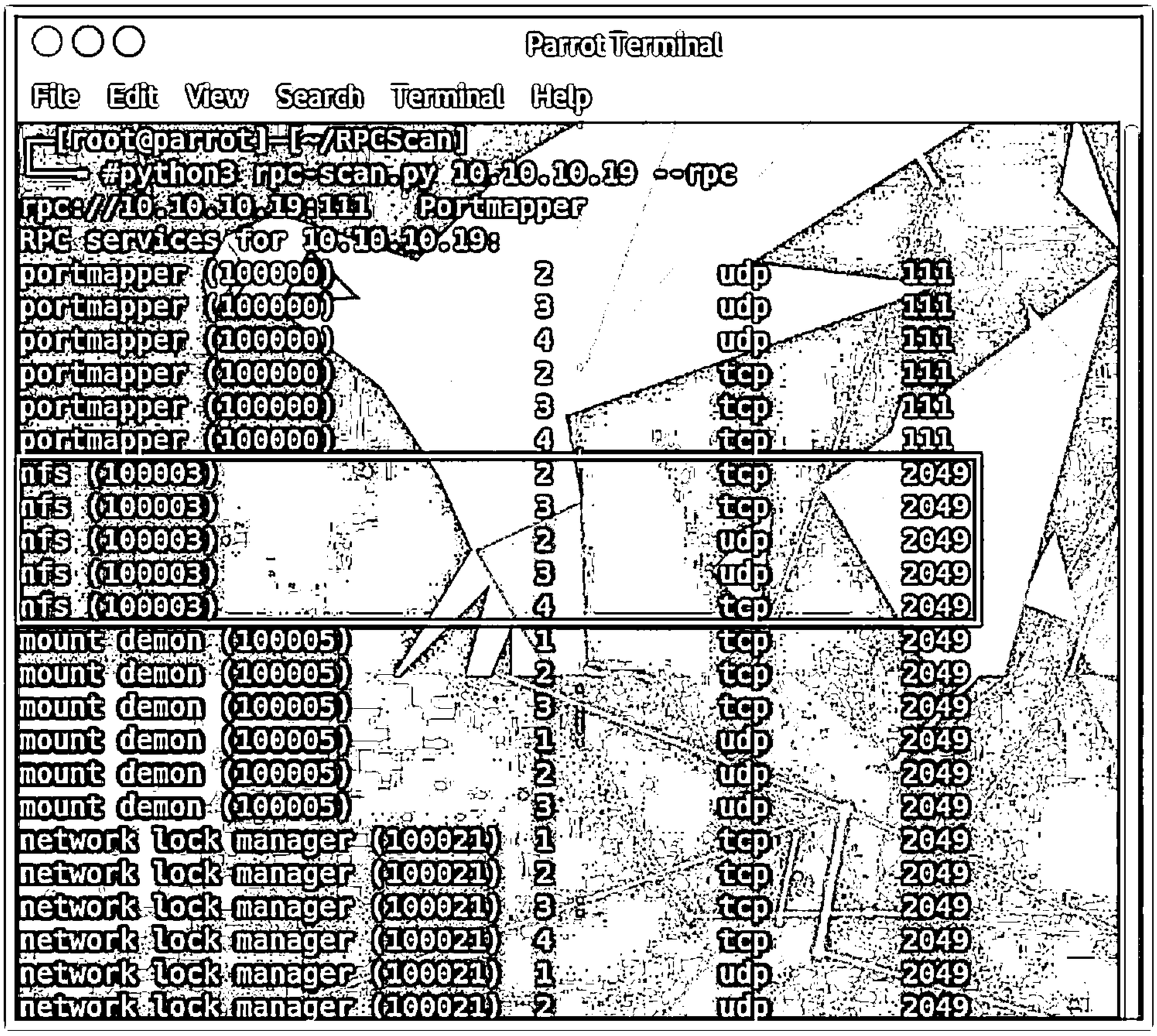


Figure 4.18: Screenshot of RPCScan displaying open NFS ports and services

- **SuperEnum**

  Source: *https://github.com*

  SuperEnum includes a script that performs the basic enumeration of any open port. As shown in the screenshot, an attacker uses the `./superenum` script and then enters a text file name "`Target.txt`" having a target IP address or a list of IP addresses for enumeration.

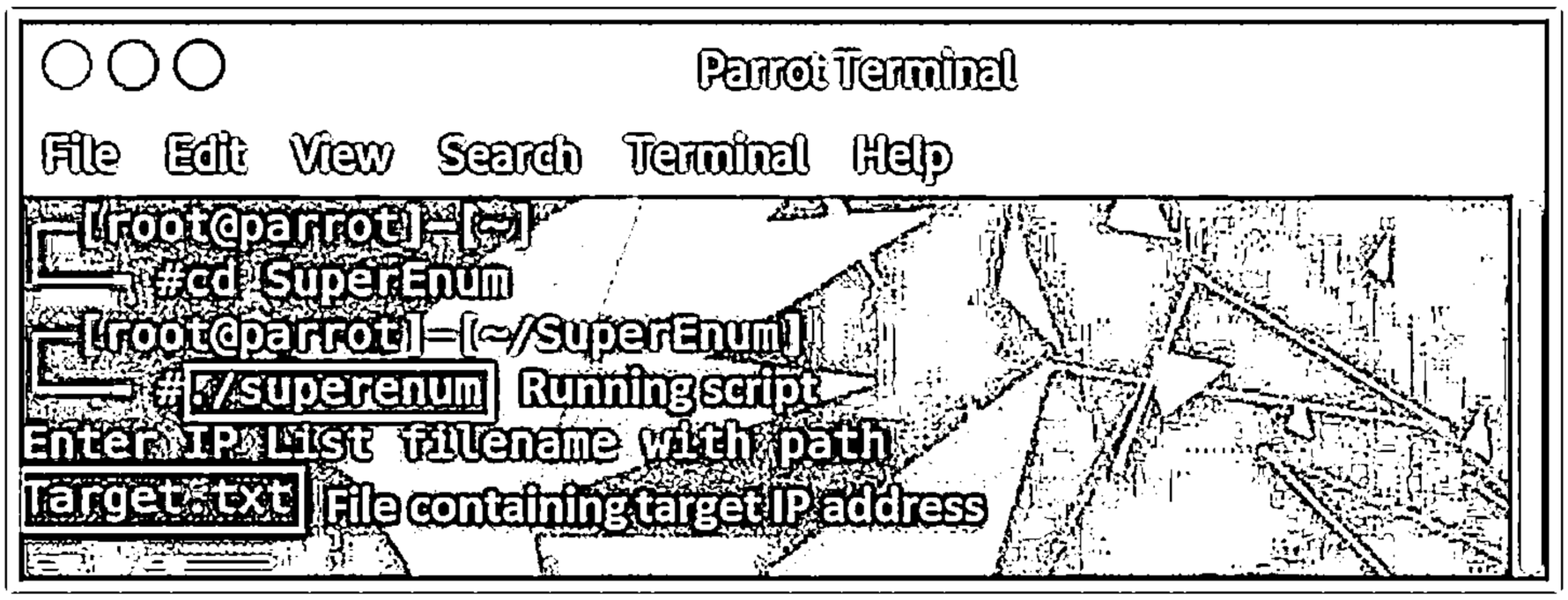


Figure 4.19: Screenshot of SuperEnum running a script

After scanning a target IP address, the script displays all the open ports, as shown in the below screenshot. Port 2049 has an NFS service running.

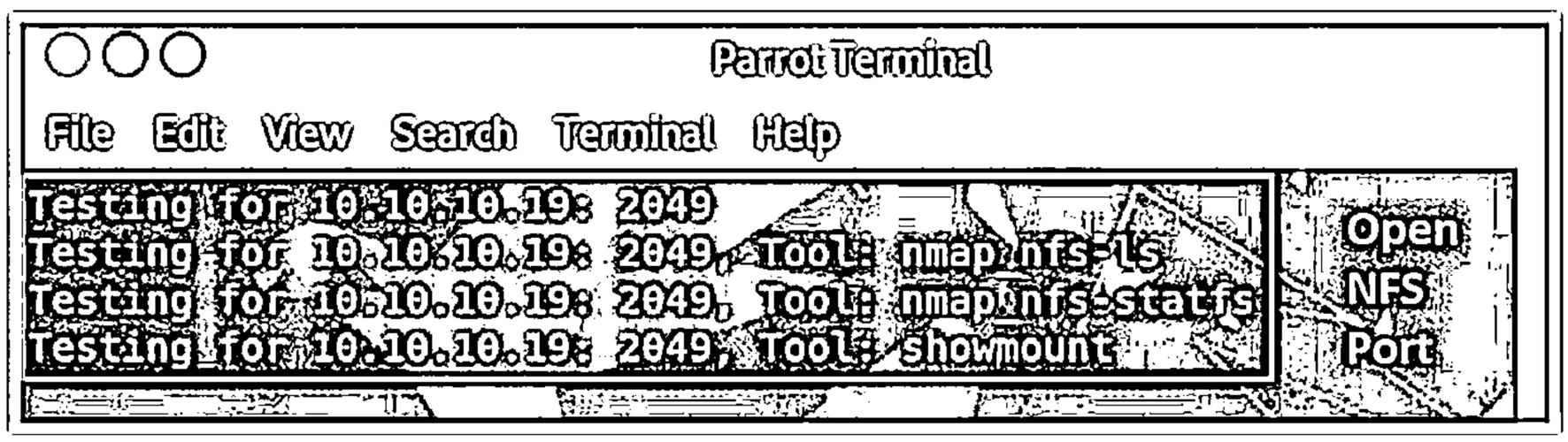
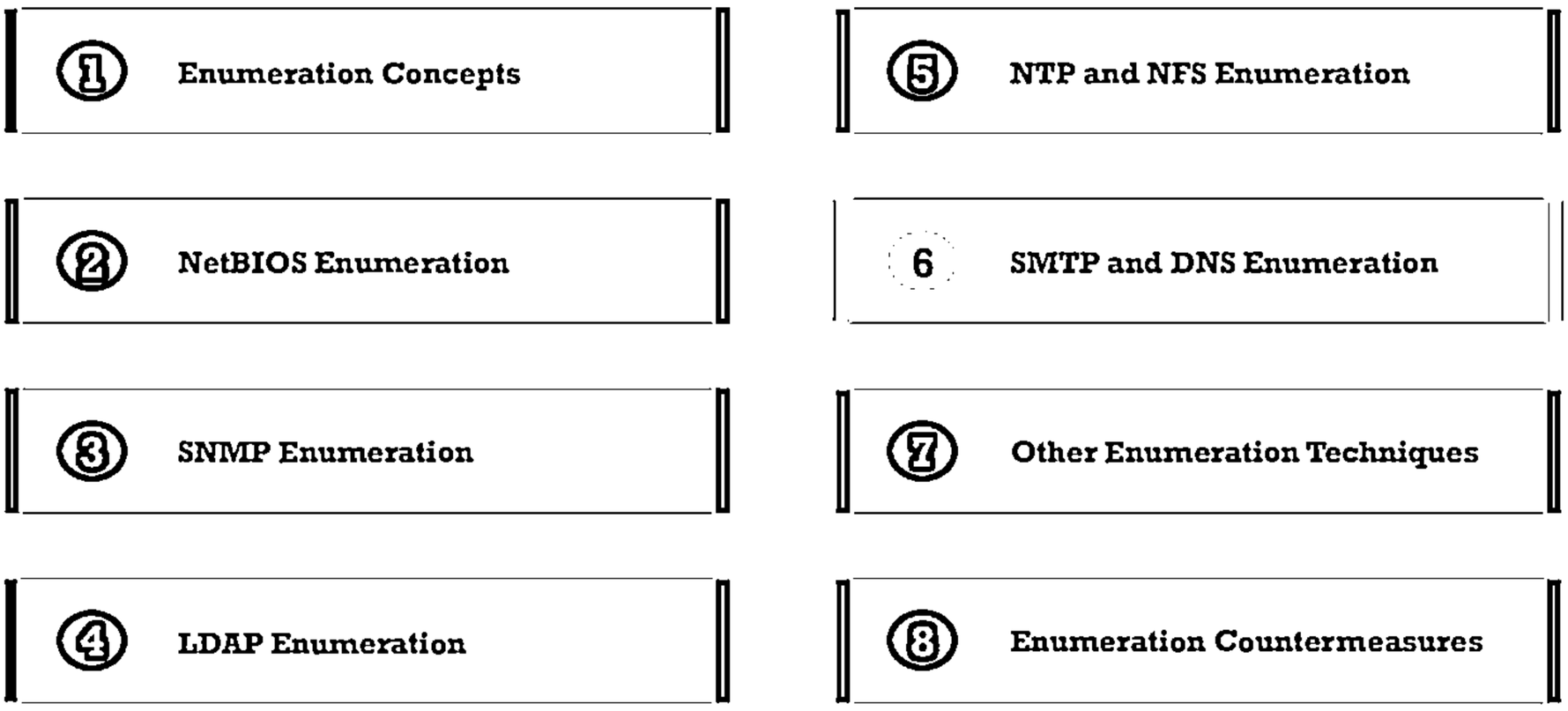


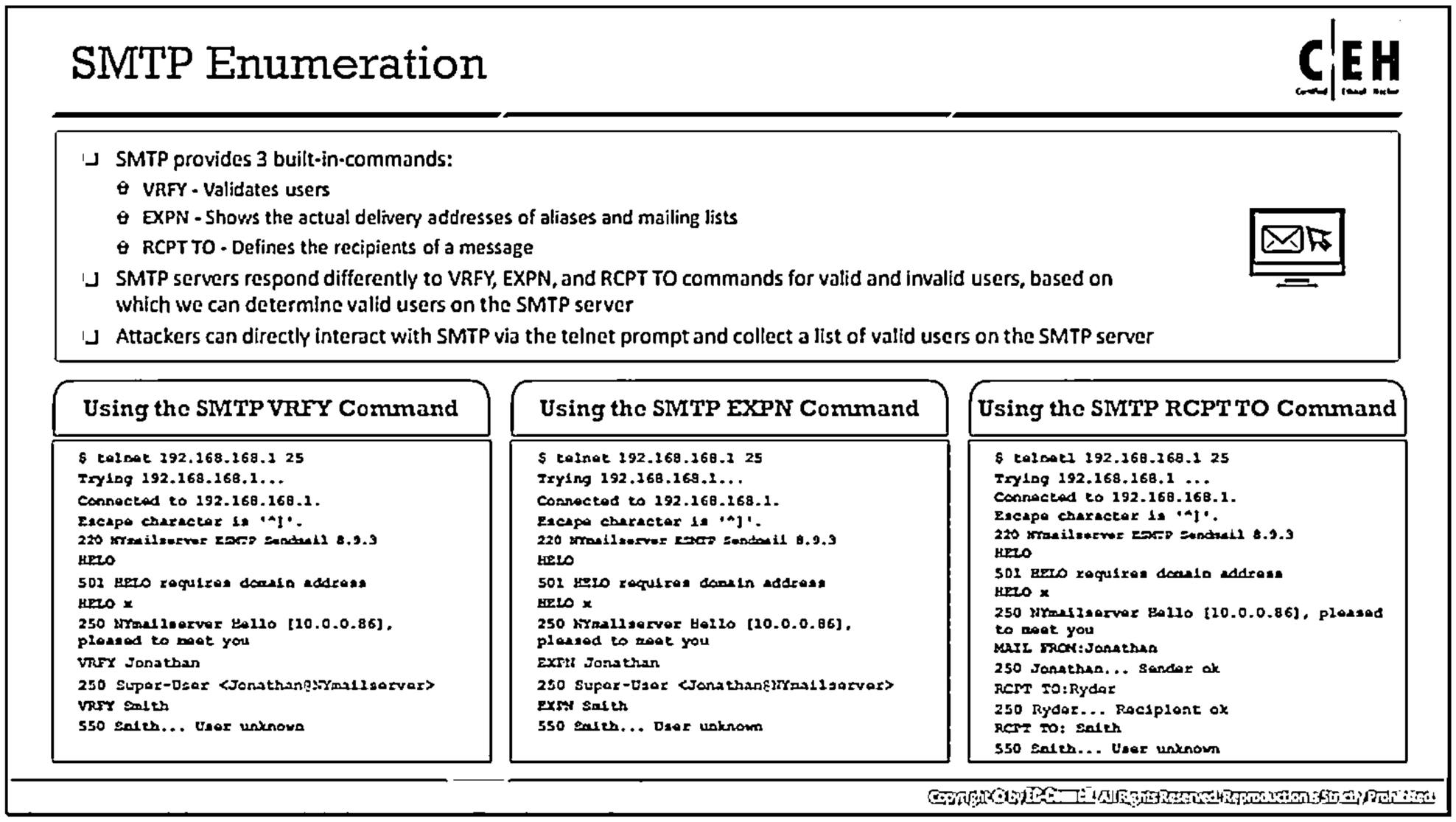
Figure 4.20: Screenshot of SuperEnum displaying open NFS ports

Module Flow



SMTP and DNS Enumeration

This section describes enumeration techniques to extract information related to network resources. It also covers DNS enumeration techniques that yield information about the DNS servers and network infrastructure of the target organization. The section discusses both SMTP and DNS enumeration techniques, covering SMTP enumeration, the process of obtaining a list of valid users on an SMTP server, SMTP enumeration tools, DNS zone transfer enumeration, DNS cache snooping, and DNS zone walking.



SMTP Enumeration

Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

SMTP provides the following three built-in commands.

- **VRFY:** Validates users

```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
VRFY Jonathan
250 Super-User <Jonathan@NYmailserver>
VRFY Smith
550 Smith... User unknown
```

- **EXPN:** Displays the actual delivery addresses of aliases and mailing lists

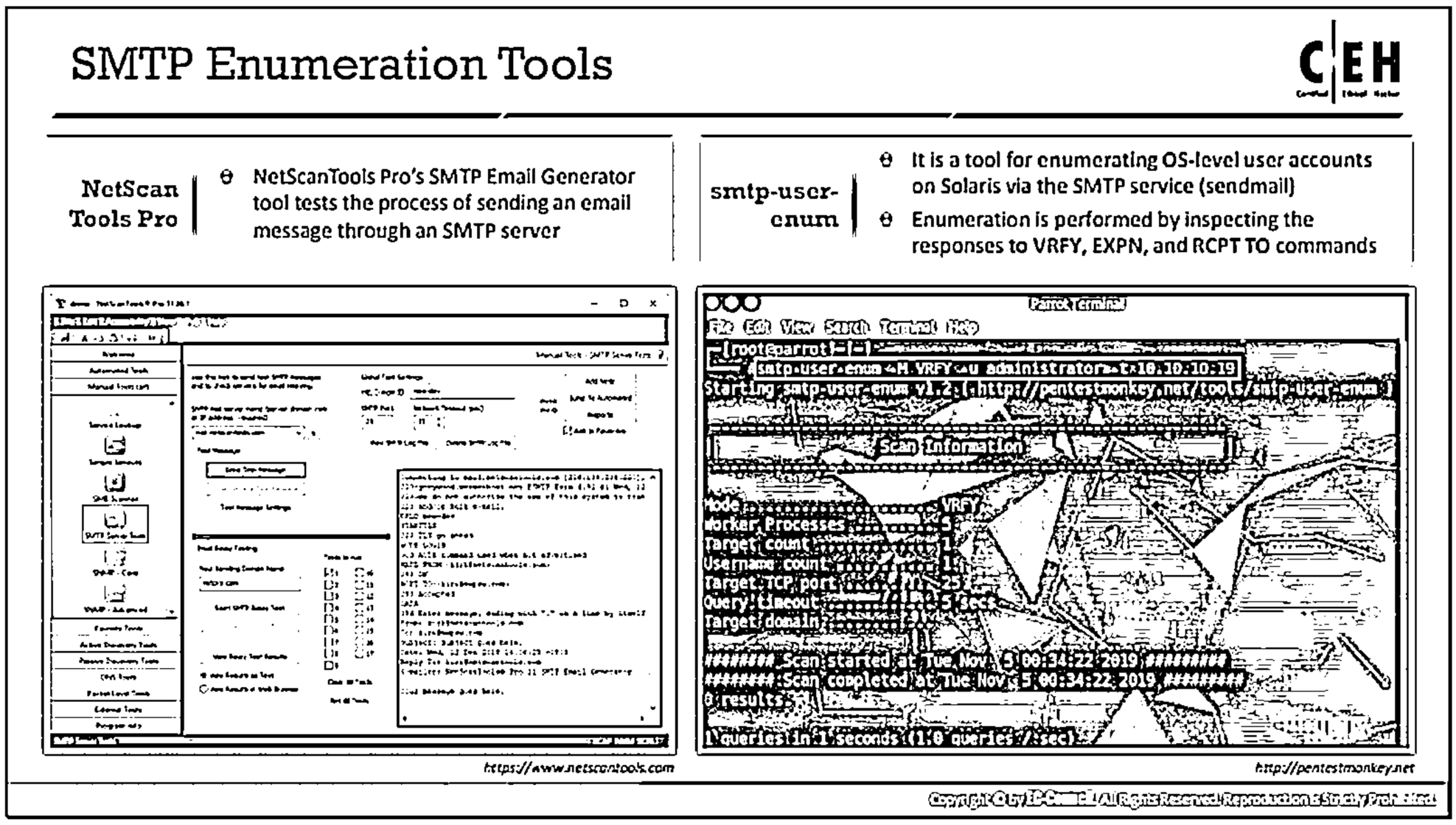
```
$ telnet 192.168.168.1 25
Trying 192.168.168.1...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
EXPN Jonathan
250 Super-User <Jonathan@NYmailserver>
EXPN Smith
550 Smith... User unknown
```

- **RCPT TO:** Defines the recipients of the message

```
$ telnetl 192.168.168.1 25
Trying 192.168.168.1 ...
Connected to 192.168.168.1.
Escape character is '^]'.
220 NYmailserver ESMTP Sendmail 8.9.3
HELO
501 HELO requires domain address
HELO x
250 NYmailserver Hello [10.0.0.86], pleased to meet you
MAIL FROM:Jonathan
250 Jonathan... Sender ok
RCPT TO:Ryder
250 Ryder... Recipient ok
RCPT TO: Smith
550 Smith... User unknown
```

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users; therefore, valid users on the SMTP server can be determined. Attackers can directly interact with SMTP via the Telnet prompt and collect a list of valid users on the SMTP server.

Administrators and pen testers can perform SMTP enumeration using command-line utilities such as Telnet and netcat or by using tools such as Metasploit, Nmap, NetScanTools Pro, and smtp-user-enum to collect a list of valid users, delivery addresses, message recipients, etc.



SMTP Enumeration Tools

SMTP enumeration tools are used to perform username enumeration. Attackers can use the usernames obtained from this enumeration to launch further attacks on other systems in the network.

- **NetScanTools Pro**

  Source: *https://www.netscantools.com*

  NetScanTools Pro's SMTP Email Generator tool tests the process of sending an email message through an SMTP server. Attackers use NetScanTools Pro for SMTP enumeration and extract all the email header parameters, including confirm/urgent flags. Attackers can also record the email session in a log file and then view the communications between NetScanTools Pro and the SMTP server in the log file.

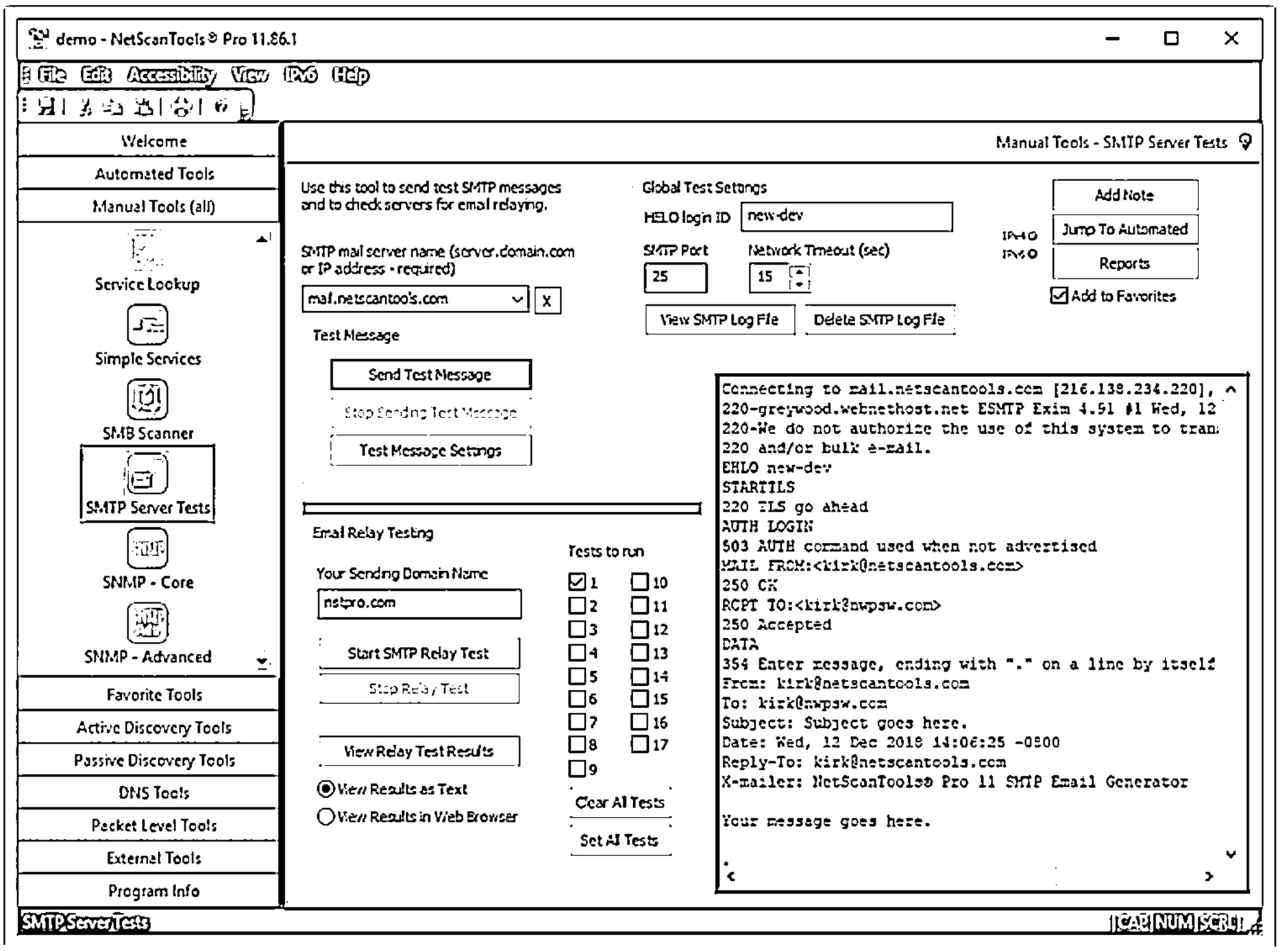


Figure 4.21: Screenshot of NetScanTools Pro

- **smtp-user-enum**

  Source: *http://pentestmonkey.net*

  smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN, and RCPT TO commands. As shown in the screenshot, smtp-user-enum needs to be passed on to a list of users and at least one target running an SMTP service. The syntax for using smtp-user-enum is as follows:

  ```
  smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-t host|-T file-of-targets)
  ```

  smtp-user-enum has the following options:

  - **-m n**: Maximum number of processes (default: 5)
  - **-M mode**: Specify the SMTP command to use for username guessing from among EXPN, VRFY, and RCPT TO (default: VRFY)
  - **-u user**: Check if a user exists on the remote system
  - **-f addr**: Specify the from email address to use for "RCPT TO" guessing (default: user@example.com)

- **-D dom**: Specify the domain to append to the supplied user list to create email addresses (default: none)
- **-U file**: Select the file containing usernames to check via the SMTP service
- **-t host**: Specify the server host running the SMTP service
- **-T file**: Select the file containing hostnames running the SMTP service
- **-p port**: Specify the TCP port on which the SMTP service runs (default: 25)
- **-d**: Debugging output
- **-t n**: Wait for a maximum of n seconds for the reply (default: 5)
- **-v**: Verbose
- **-h**: Help message

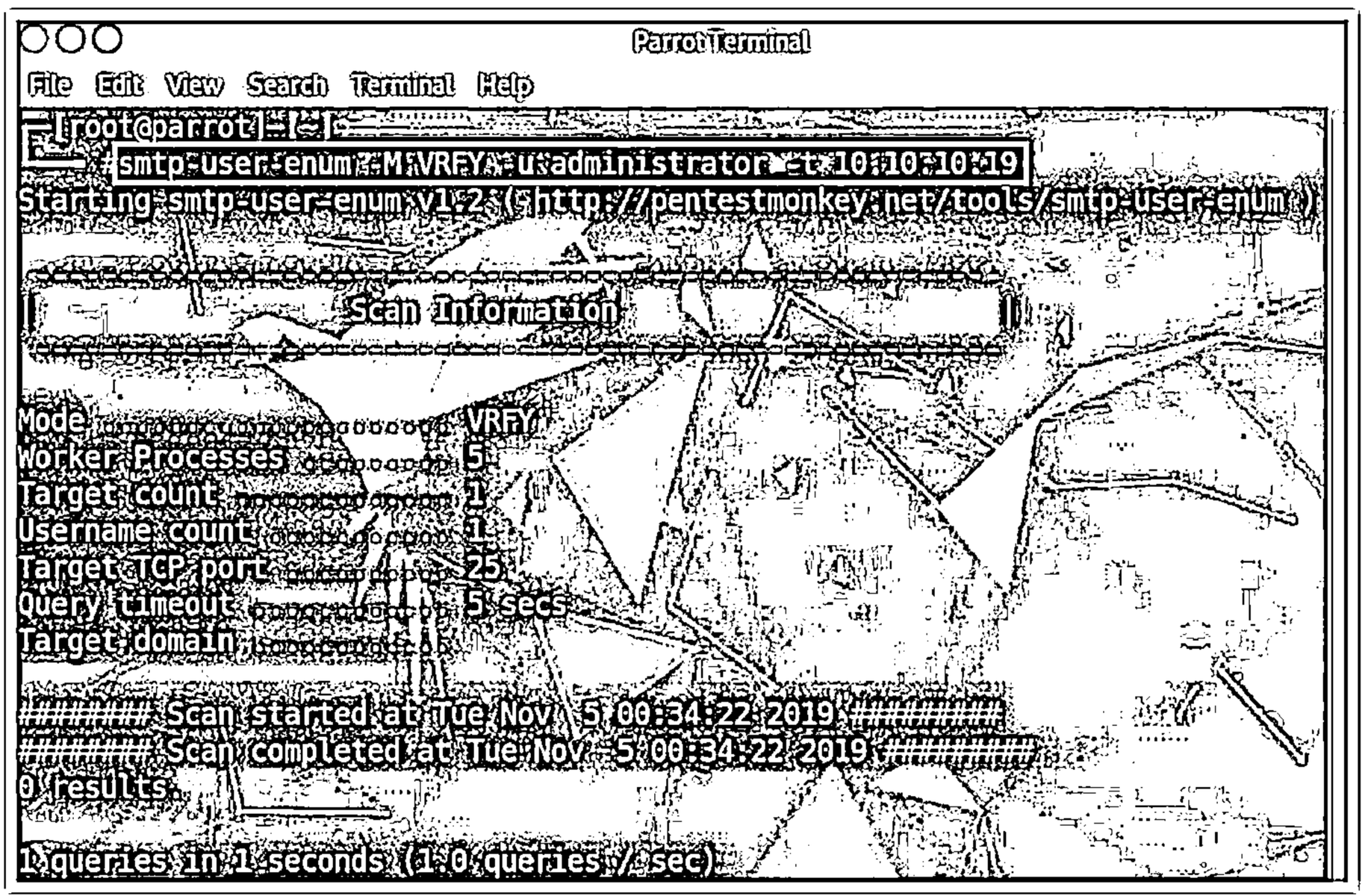
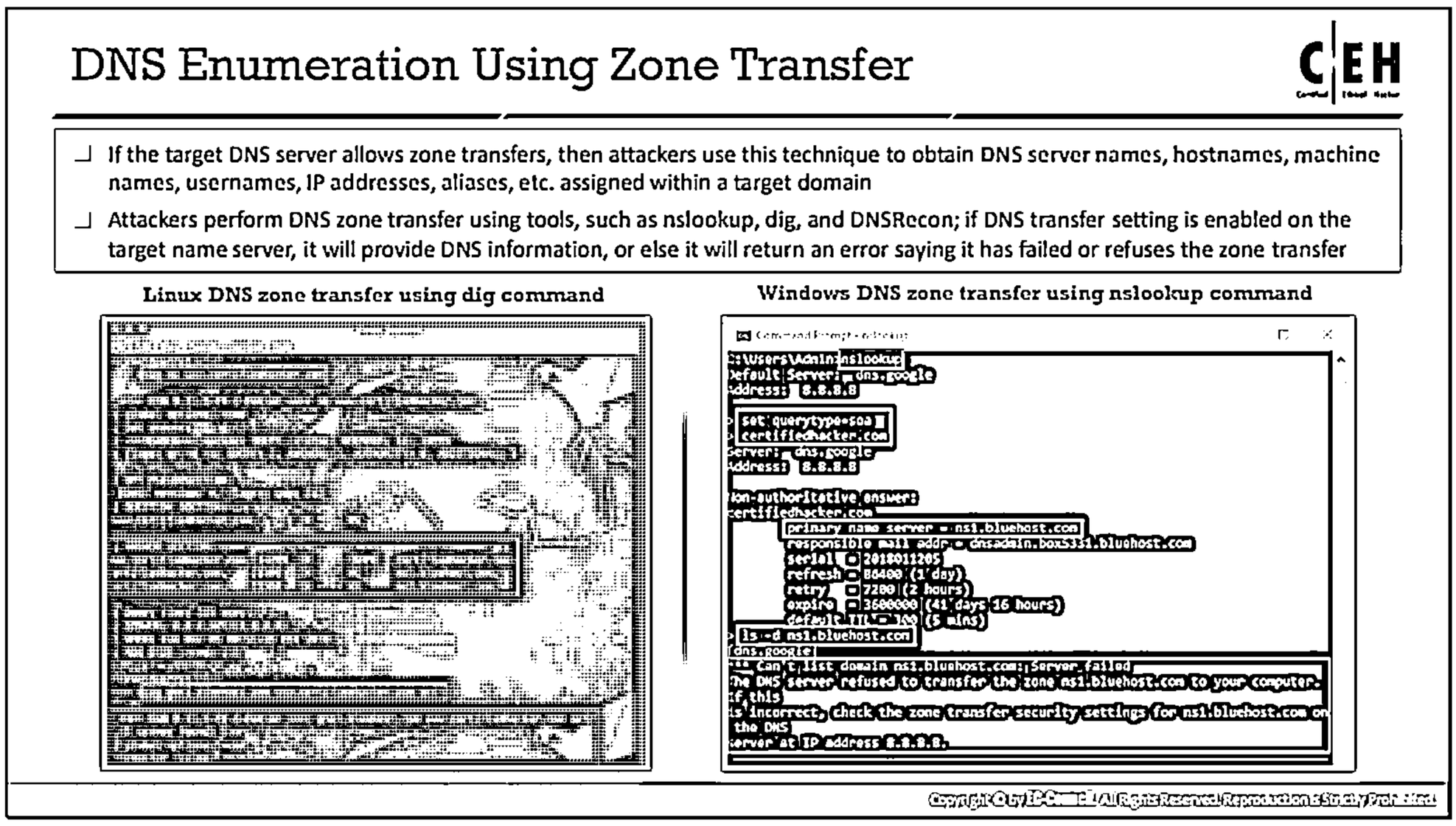


Figure 4.22: Screenshot of smtp-user-enum



DNS Enumeration Using Zone Transfer

DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. In most cases, the primary DNS server maintains a backup or secondary server for redundancy, which holds all the information stored in the primary server. The DNS server uses zone transfer to distribute changes made to the main server to the secondary server(s). An attacker performs DNS zone transfer enumeration to locate the DNS server and access records of the target organization. If the DNS server of the target organization allows zone transfers, then attackers can perform DNS zone transfer to obtain DNS server names, hostnames, machine names, usernames, IP addresses, aliases, etc. assigned within a target domain.

In DNS enumeration using zone transfer, an attacker attempts to retrieve a copy of the entire zone file for a domain from the DNS server. Attackers can perform DNS zone transfer using tools such as nslookup, dig command, and DNSRecon. If the DNS transfer setting is enabled on the target name server, it will provide the DNS information; else, it will return an error stating it has failed or refused the zone transfer.

To perform a DNS zone transfer, the attacker sends a zone-transfer request to the DNS server pretending to be a client; the DNS server then sends a portion of its database as a zone to the attacker. This zone may contain a large amount of information about the DNS zone network.

- **dig Command**

  Attackers use the `dig` command on Linux-based systems to query the DNS name servers and retrieve information about the target host addresses, name servers, mail exchanges, etc. As shown in the screenshot, attackers use the following command to perform DNS zone transfer:

  ```
  dig ns <target domain>
  ```

  The above command retrieves all the DNS name servers of the target domain. Next, attackers use one of the name servers from the output of the above command to test whether the target DNS allows zone transfers. They use the following command for this purpose:

  ```
  dig @<domain of name server> <target domain> axfr
  ```

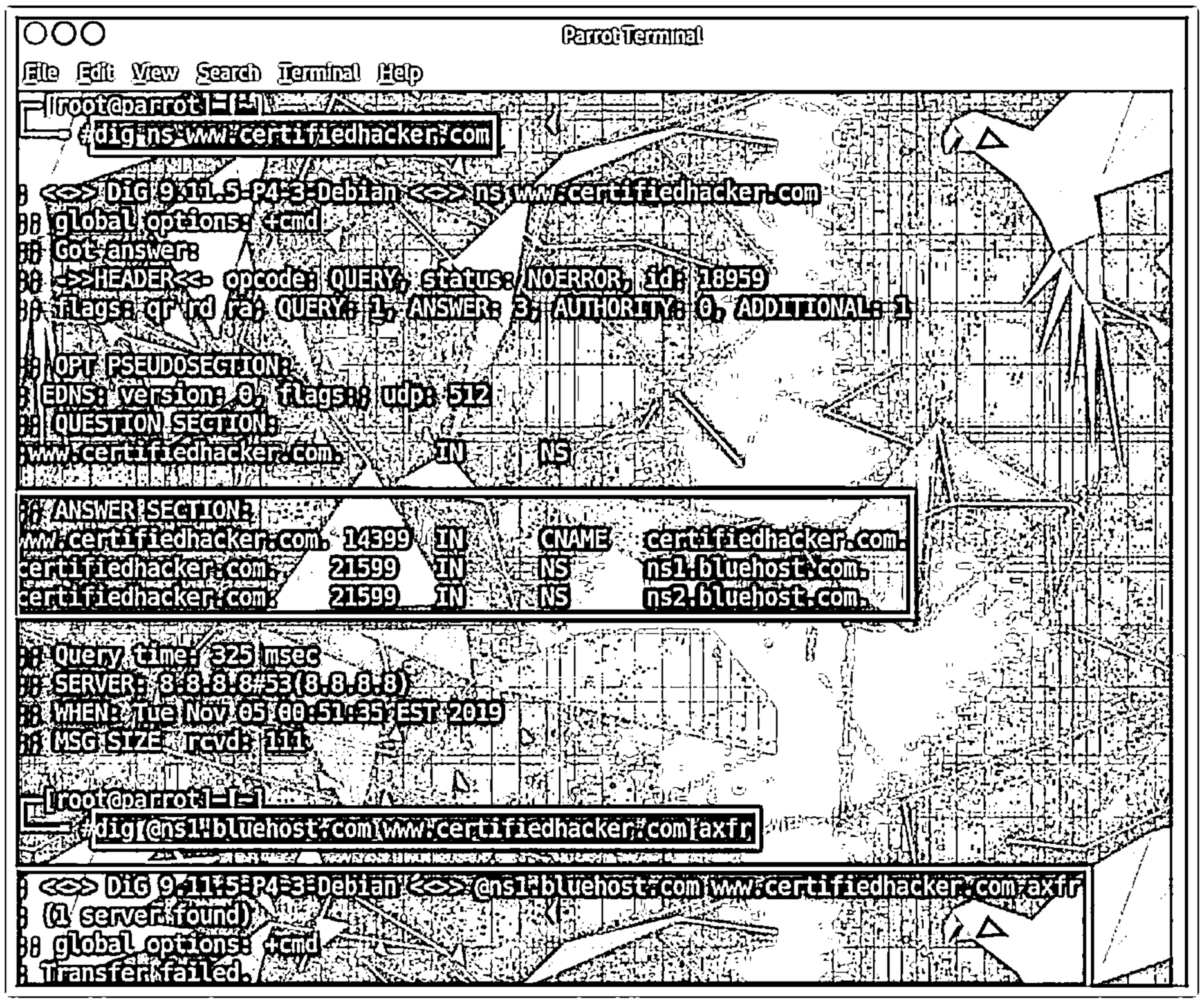


Figure 4.23: Screenshot of Linux DNS zone transfer using dig command

- **nslookup Command**

  Source: *https://docs.microsoft.com*

  Attackers use the nslookup command on Windows-based systems to query the DNS name servers and retrieve information about the target host addresses, name servers, mail exchanges, etc. As shown in the screenshot, attackers use the following command to perform DNS zone transfer:

  ```
  nslookup
  set querytype=soa
  <target domain>
  ```

  The above command sets the query type to the Start of Authority (SOA) record to retrieve administrative information about the DNS zone of the target domain `certifiedhacker.com`. The following command is used to attempt to transfer the zone of the specified name server:

  ```
  /ls -d <domain of name server>
  ```

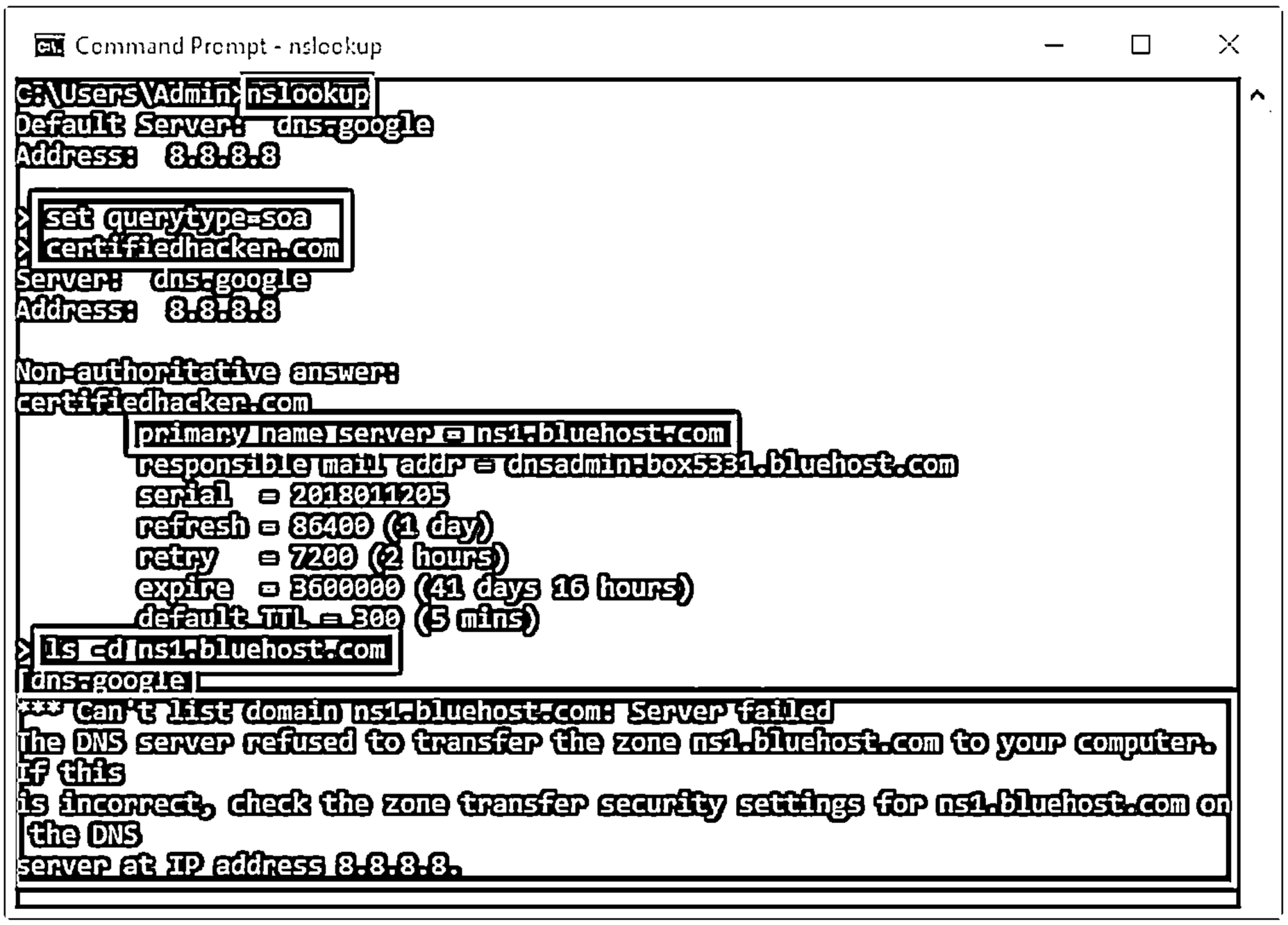


Figure 4.24: Screenshot of Windows DNS zone transfer using the nslookup command

- **DNSRecon**

  Source: *https://github.com*

  Attackers use DNSRecon to check all NS records of the target domain for zone transfers. As shown in the screenshot, attackers use the following command for DNS zone transfer:

  `dnsrecon -t axfr -d <target domain>`

  In the above command, the -t option specifies the type of enumeration to be performed, axfr is the type of enumeration in which all NS servers are tested for a zone transfer, and the -d option specifies the target domain.

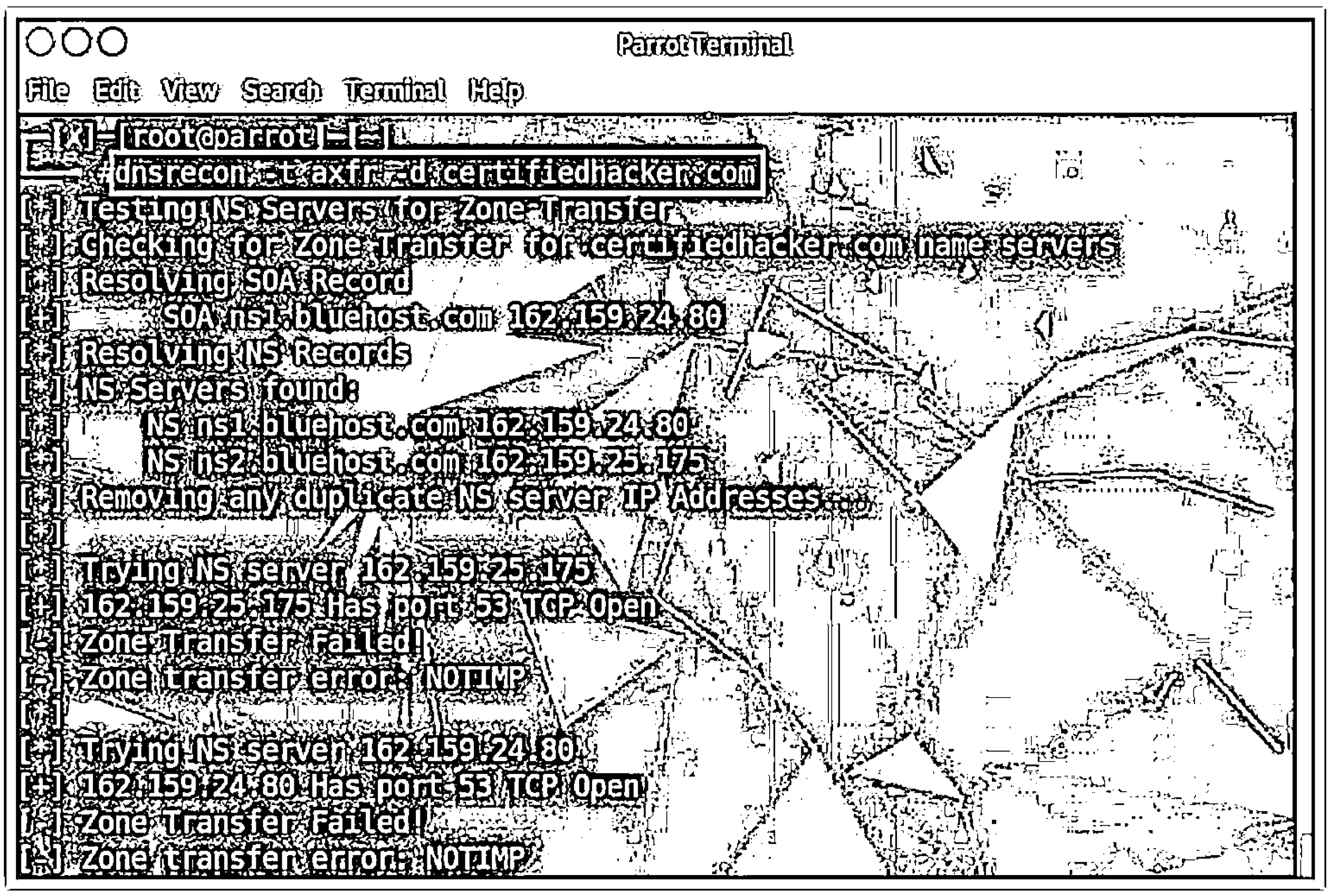
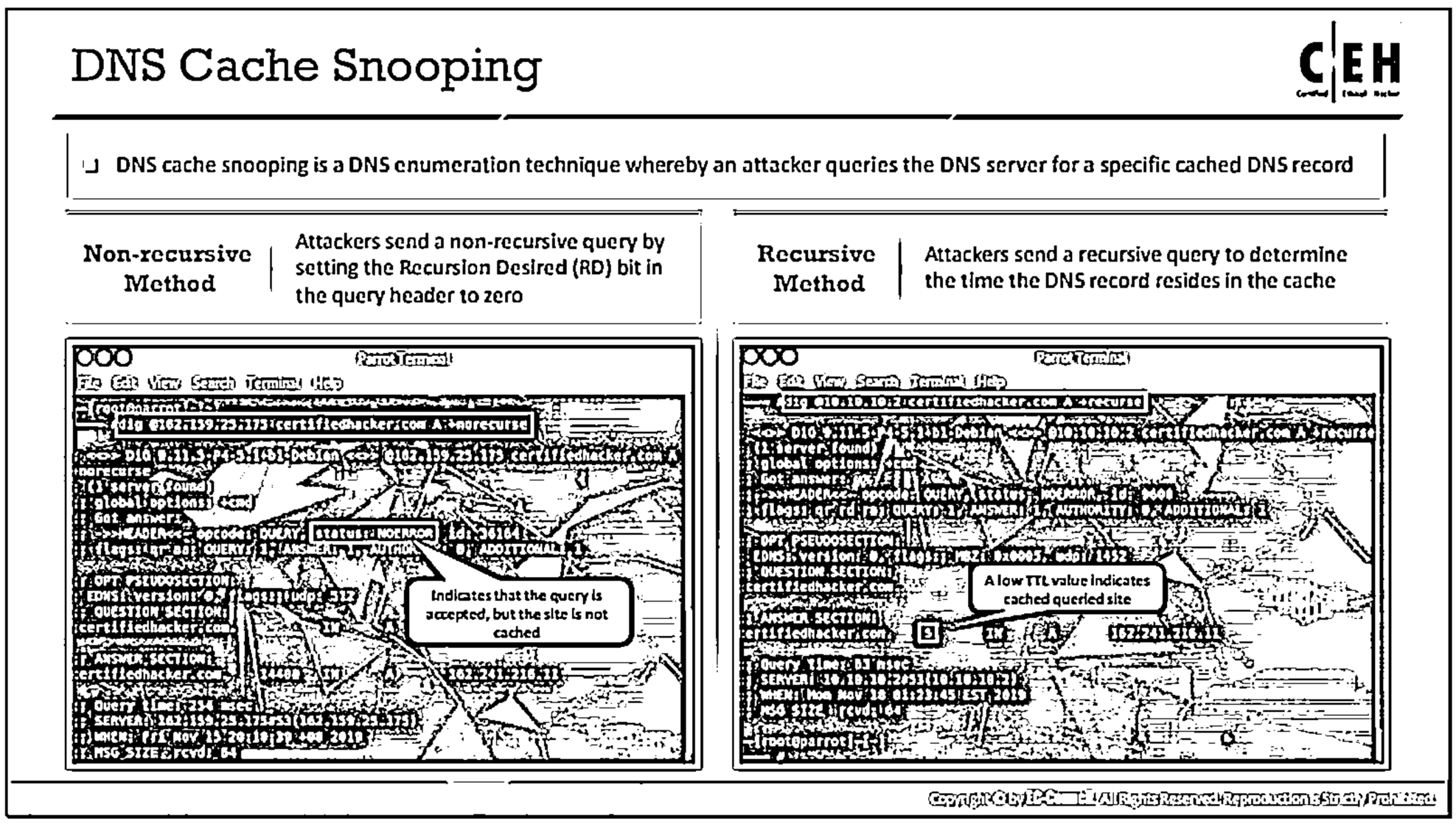


Figure 4.25: Screenshot of DNS zone transfer using DNSRecon



DNS Cache Snooping

DNS cache snooping is a type of DNS enumeration technique in which an attacker queries the DNS server for a specific cached DNS record. By using this cached record, the attacker can determine the sites recently visited by the user. This information can further reveal important information such as the name of the owner of the DNS server, its service provider, the name of its vendor, and bank details. By using this information, the attacker can perform a social engineering attack on the target user. Attackers perform DNS cache snooping using various tools such as the dig command, DNS Snoop Dogg, and DNSRecon.

Attackers use the following two DNS cache snooping methods to snoop on a target domain.

- **Non-recursive Method**

  In this method, to snoop on a DNS server, attackers send a non-recursive query by setting the Recursion Desired (RD) bit in the query header to zero. Attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX. If the queried record is present in the DNS cache, the DNS server responds with the information indicating that some user on the system has visited a specific domain. Otherwise, the DNS server responds with the information about another DNS server that can return an answer to the query, or it replies with the `root.hints` file containing information about all root DNS servers.

  Attackers use the `dig` command followed by the name/IP address of the DNS server, domain name, and type of DNS record file. The `+norecurse` option is used to set the query to non-recursive.

  ```
  dig @<IP of DNS server> <Target domain> A +norecurse
  ```

As shown in the screenshot, the status `NOERROR` implies that the query was accepted but no answer was returned, thereby indicating that no user from the system had visited the queried site.

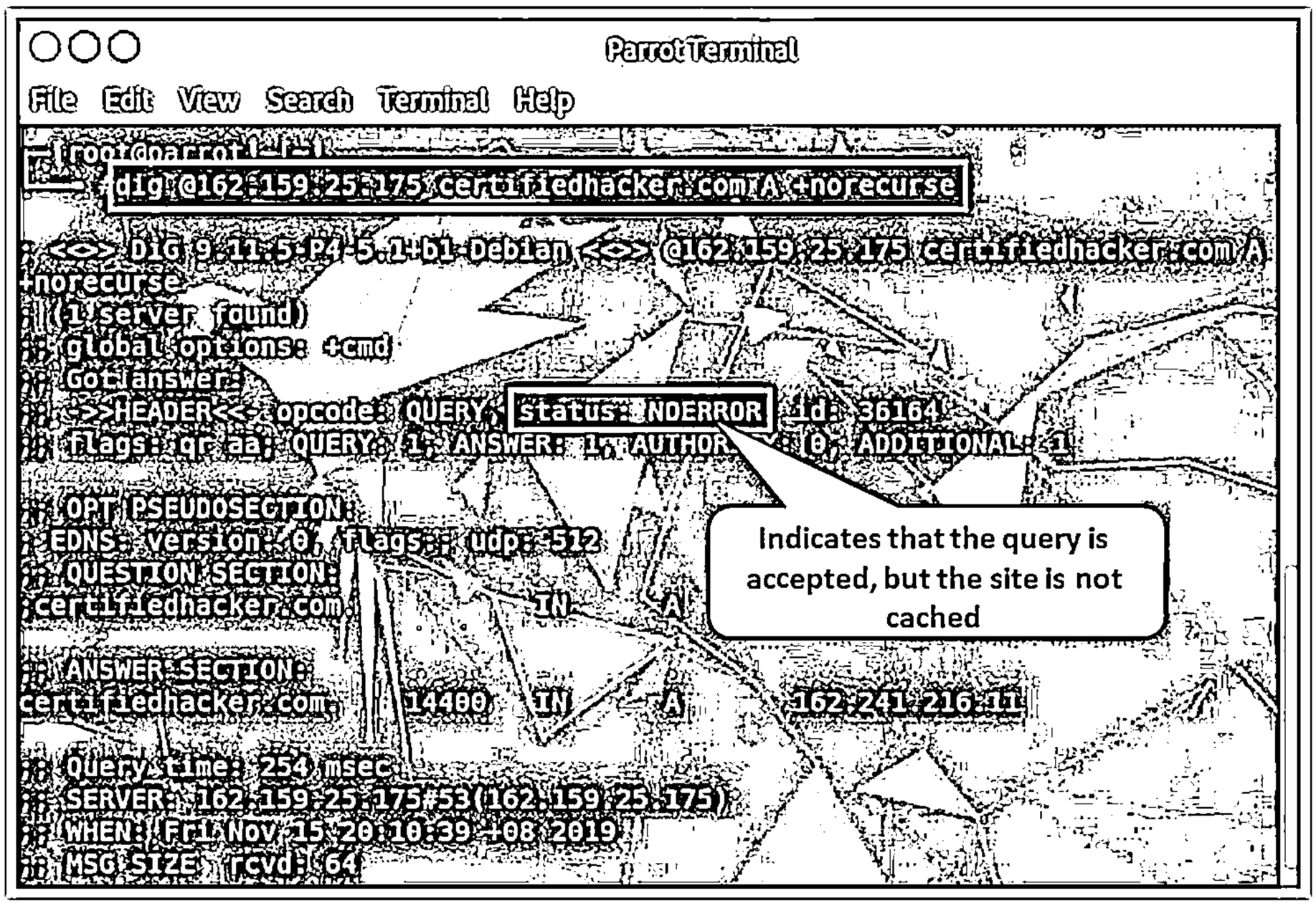


Figure 4.26: Screenshot of a dig query for a site that is not cached

- **Recursive Method**

  In this method, to snoop on the DNS server, attackers send a recursive query by setting the `+recurse` option instead of the `+norecurse` option. Similar to the non-recursive method, the attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX.

  In this method, the time-to-live (TTL) field is examined to determine the duration for which the DNS record remains in the cache. Here, the TTL value obtained from the result is compared with the TTL that was initially set in the TTL field. If the TTL value in the result is less than the initial TTL value, the record is cached, indicating that someone on the system has visited that site. However, if the queried record were not present in the cache, it will be added to the cache after the first query is sent.

  Attackers use the same `dig` command as in the non-recursive method but with the `+recurse` option instead of the `+norecurse` option:

  ```
  dig @<IP of DNS server> <Target domain> A +recurse
  ```

As shown in the screenshot, the TTL value for the domain `certifiedhacker.com` is considerably low, which strongly suggests that the domain was already in the cache when the query was issued.

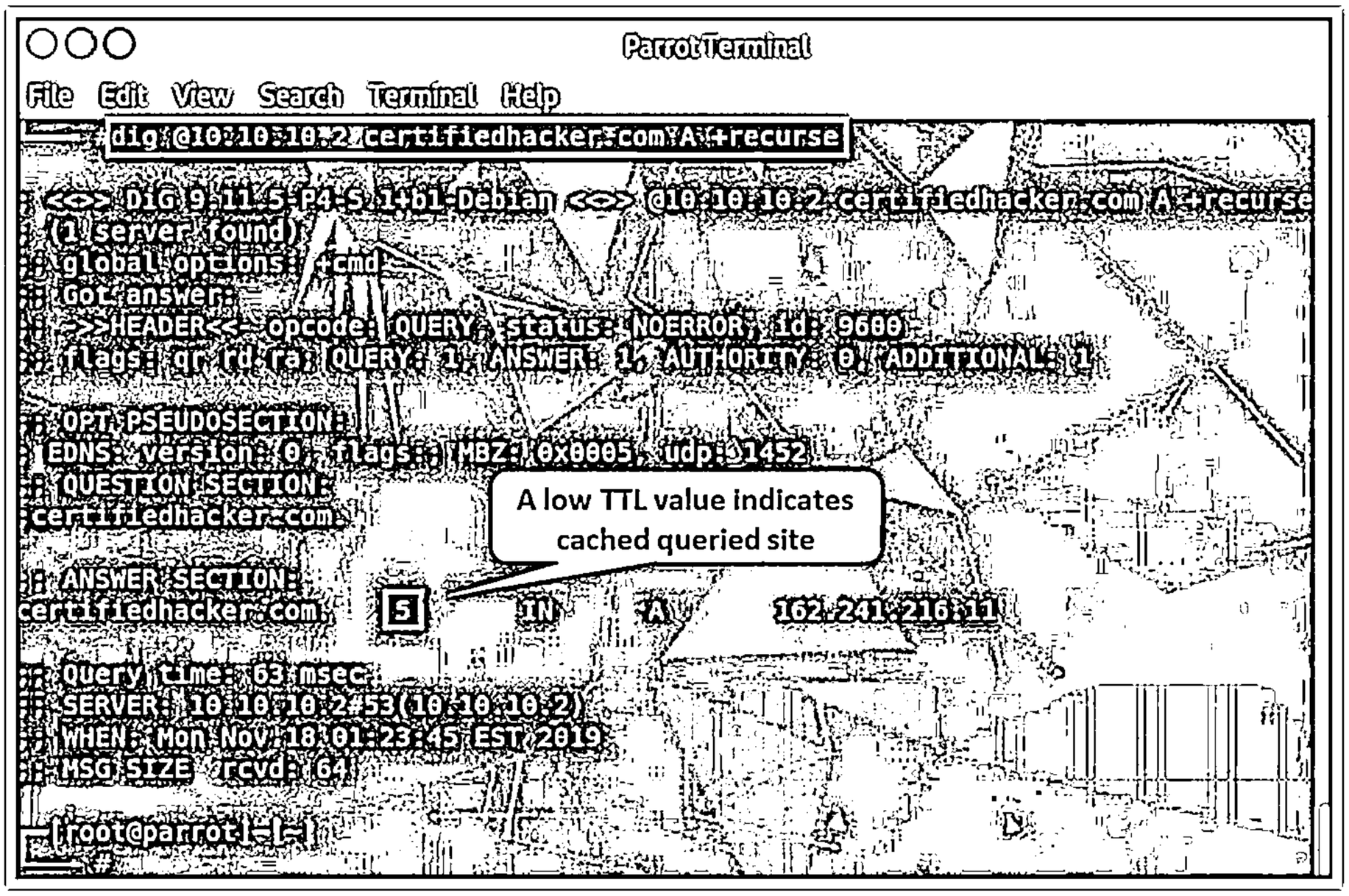
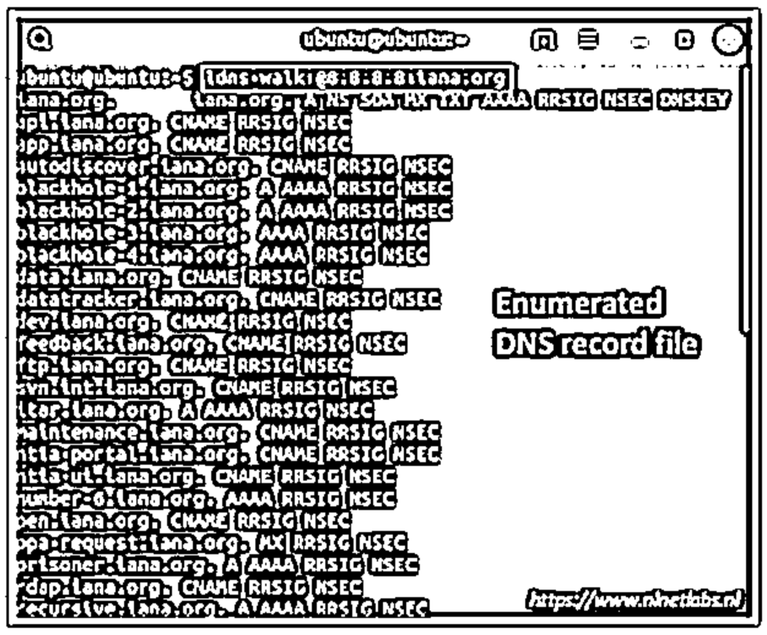


Figure 4.27: Screenshot of a dig query for a cached site

DNSSEC Zone Walking

- DNSSEC zone walking is a DNS enumeration technique where an attacker attempts to obtain internal records of the DNS server if the DNS zone is not properly configured
- Attackers use tools, such as LDNS and DNSRecon, to exploit this vulnerability and obtain the network information of a target domain and further launch Internet-based attacks

LDNS



DNSRecon

DNSSEC Zone Walking

Domain Name System Security Extensions (DNSSEC) zone walking is a type of DNS enumeration technique in which an attacker attempts to obtain internal records if the DNS zone is not properly configured. The enumerated zone information can assist the attacker in building a host network map.

Organizations use DNSSEC to add security features to the DNS data and provide protection against known threats to the DNS. This security feature uses digital signatures based on public-key cryptography to strengthen authentication in DNS. These digital signatures are stored in the DNS name servers along with common records such as MX, A, AAAA, and CNAME.

While DNSSEC provides Internet security, it is also susceptible to a vulnerability called zone enumeration or zone walking. By exploiting this vulnerability, attackers can obtain network information of a target domain, based on which they may launch Internet-based attacks.

To overcome the zone enumeration vulnerability, a new version of DNSSEC that uses Next Secure version 3 (NSEC3) is used. The NSEC3 record provides the same functionality as NSEC records, except that it provides cryptographically hashed record names that are designed to prevent the enumeration of record names present in the zone.

To perform zone enumeration, attackers can use various DNSSEC zone enumerators such as LDNS, DNSRecon, nsec3map, nsec3walker, and DNSwalk.

DNSSEC Zone Walking Tools

DNSSEC zone walking tools are used to enumerate the target domain's DNS record files. These tools can also perform zone enumeration on NSEC and NSEC3 record files and further use the gathered information to launch attacks such as denial-of-service (DoS) attacks and phishing attacks.

- **LDNS**

  Source: *https://www.nlnetlabs.nl*

  LDNS-walk enumerates the DNSSEC zone and obtains results on the DNS record files.

  As shown in the screenshot, attackers use the following query to enumerate a target domain `iana.org` using the DNS server `8.8.8.8` to obtain DNS record files:

  ```
  ldns-walk @<IP of DNS Server> <Target domain>
  ```

Figure 4.28: Screenshot of LDNS displaying results on the target domain

- **DNSRecon**

  Source: *https://www.github.com*

  DNSRecon is a zone enumeration tool that assists users in enumerating DNS records such as A, AAAA, and CNAME. It also performs NSEC zone enumeration to obtain DNS record files of a target domain.

  As shown in the screenshot, attackers use the following query to perform zone enumeration against a target domain `certifiedhacker.com`:

  ```
  dnsrecon -d <target domain> -z
  ```

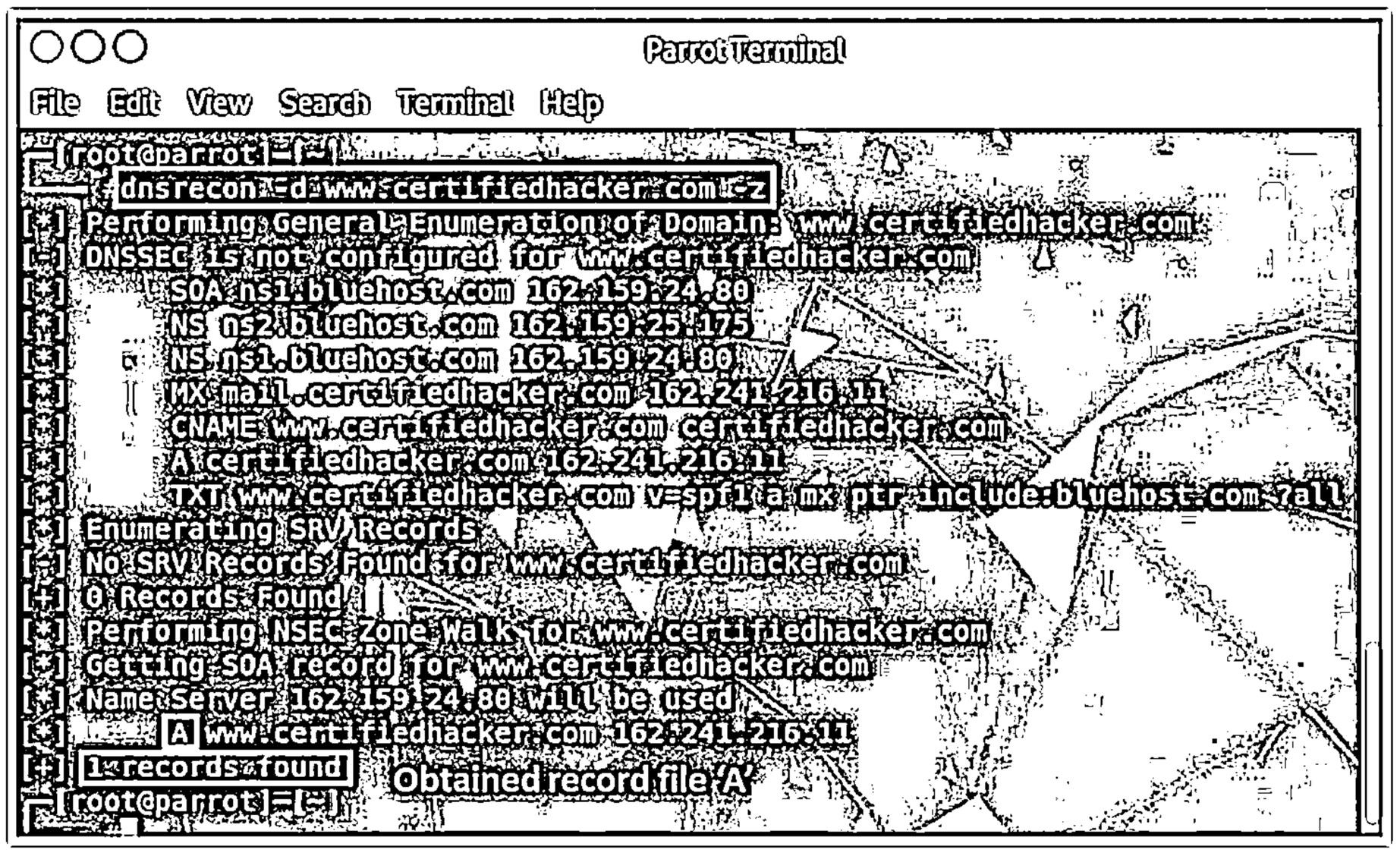
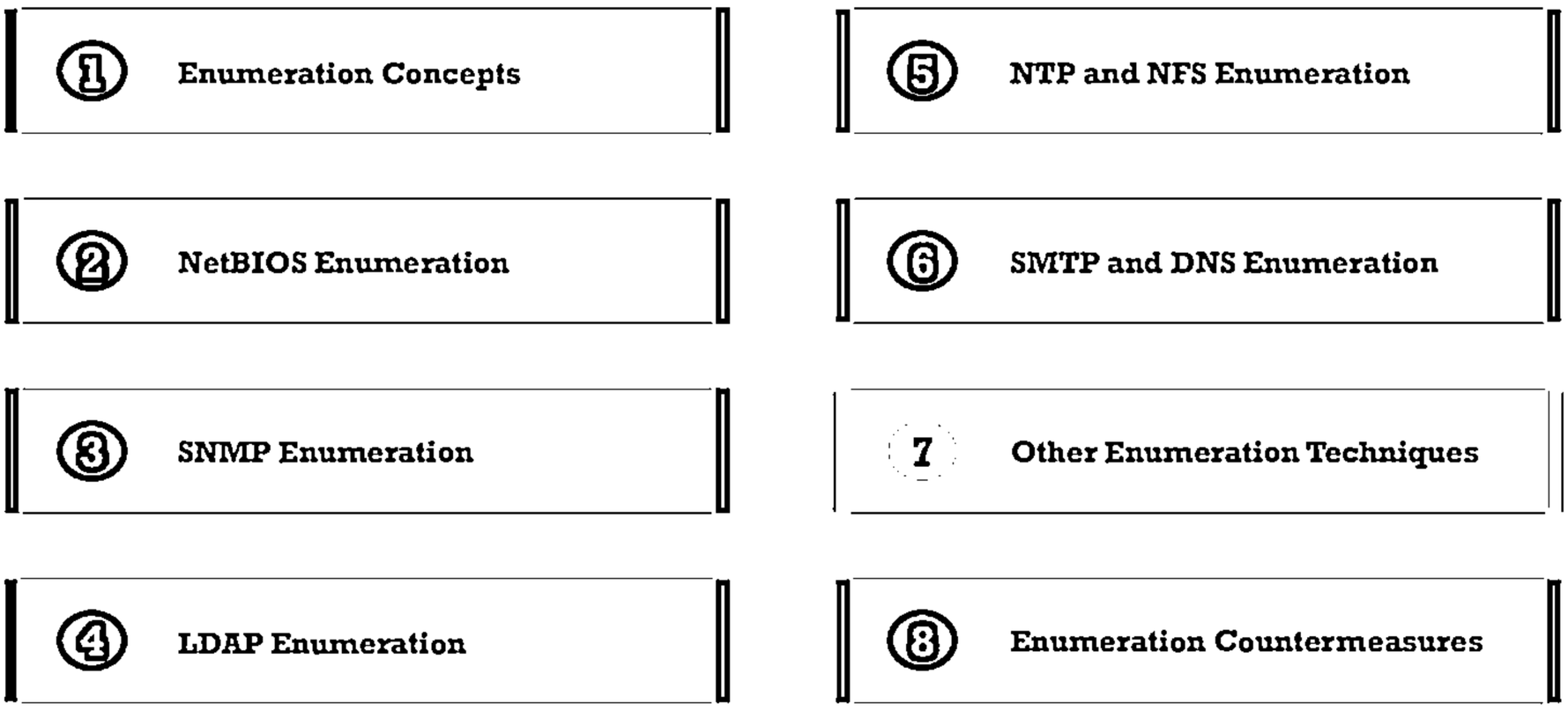


Figure 4.29: Screenshot of DNSRecon displaying results on the target domain

Module Flow

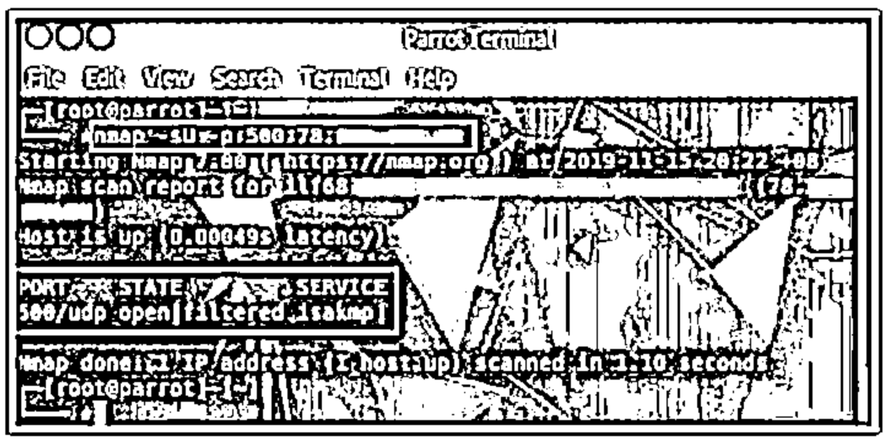


Other Enumeration Techniques

This section discusses IPsec, VoIP, RPC, Unix/Linux user, Telnet, SSH user, FTP, TFTP, SMB, IPv6, and BGP enumeration.

IPsec Enumeration

- IPsec uses Encapsulation Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) to secure communication between virtual private network (VPN) end points
- Most IPsec based VPNs use Internet Security Association and Key Management Protocol (ISAKMP), a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment
- A simple scanning for ISAKMP at UDP port 500 can indicate the presence of a VPN gateway
- Attackers can probe further using a tool, such as ike-scan, to enumerate sensitive information, including encryption and hashing algorithm, authentication type, key distribution algorithm, and SA LifeDuration



IPsec Enumeration

IPsec is the most commonly implemented technology for both gateway-to-gateway (LAN-to-LAN) and host-to-gateway (remote access) enterprise VPN solutions. IPsec provides data security by employing various components such as Encapsulating Security Payload (ESP), Authentication Header (AH), and Internet Key Exchange (IKE) to secure communication between VPN endpoints.

Most IPsec-based VPNs use the Internet Security Association Key Management Protocol (ISAKMP), a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment.

Attackers can perform simple direct scanning for ISAKMP at UDP port 500 with tools such as Nmap to acquire information related to the presence of a VPN gateway.

The following command can be used to perform an Nmap scan for checking the status of ISAKMP over port 500:

```
# nmap -sU -p 500 <target IP address>
```

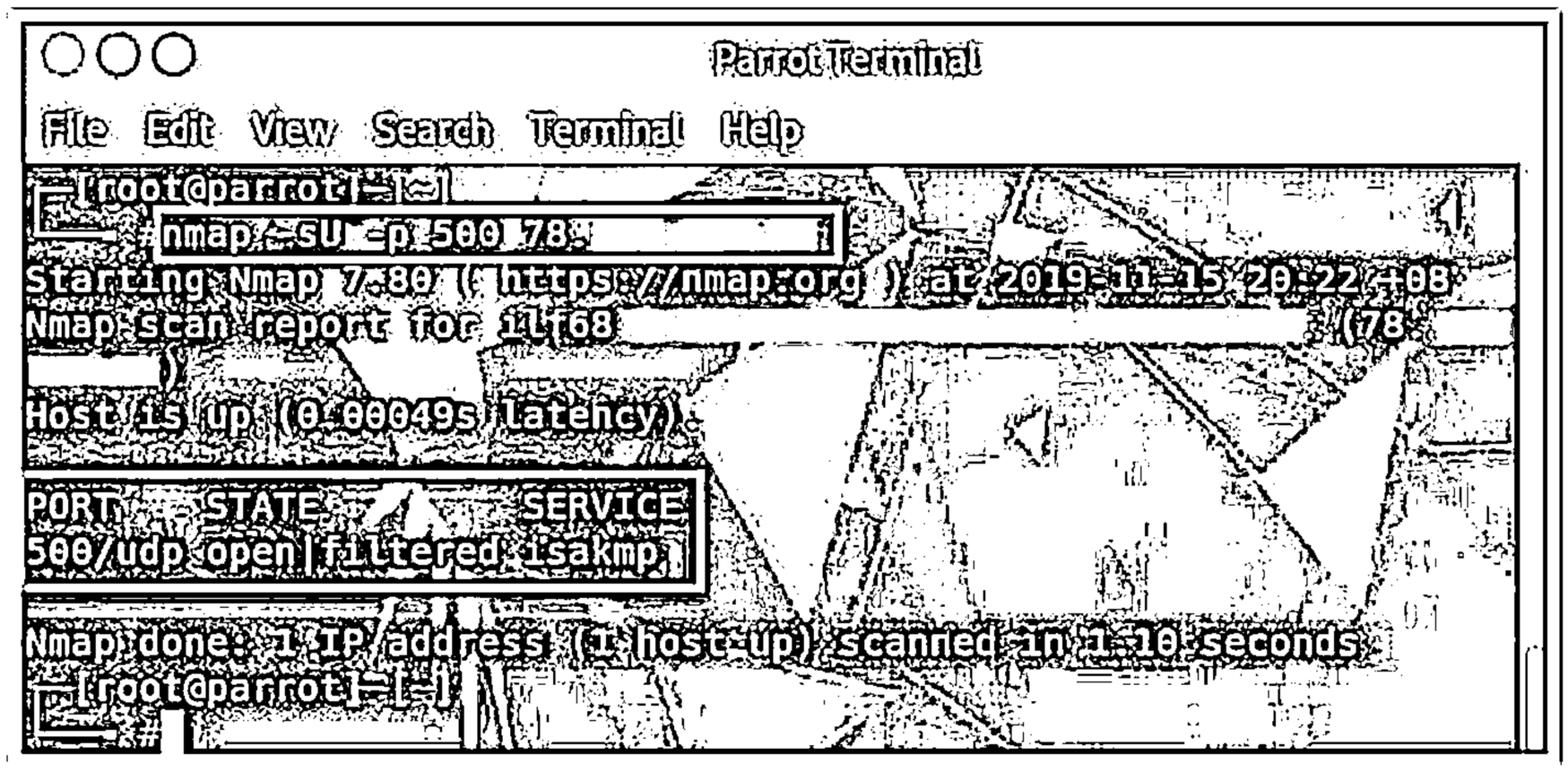


Figure 4.30: Screenshot displaying an Nmap scan over port 500 for ISAKMP

Attackers can probe further using fingerprinting tools such as ike-scan to enumerate sensitive information, including the encryption and hashing algorithm, authentication type, key distribution algorithm, and SA LifeDuration. In this type of scan, specially crafted IKE packets with an ISAKMP header are sent to the target gateway, and the responses are recorded.

The following command is used for initial IPsec VPN discovery with ike-scan tool:

```
# ike-scan -M <target gateway IP address>
```

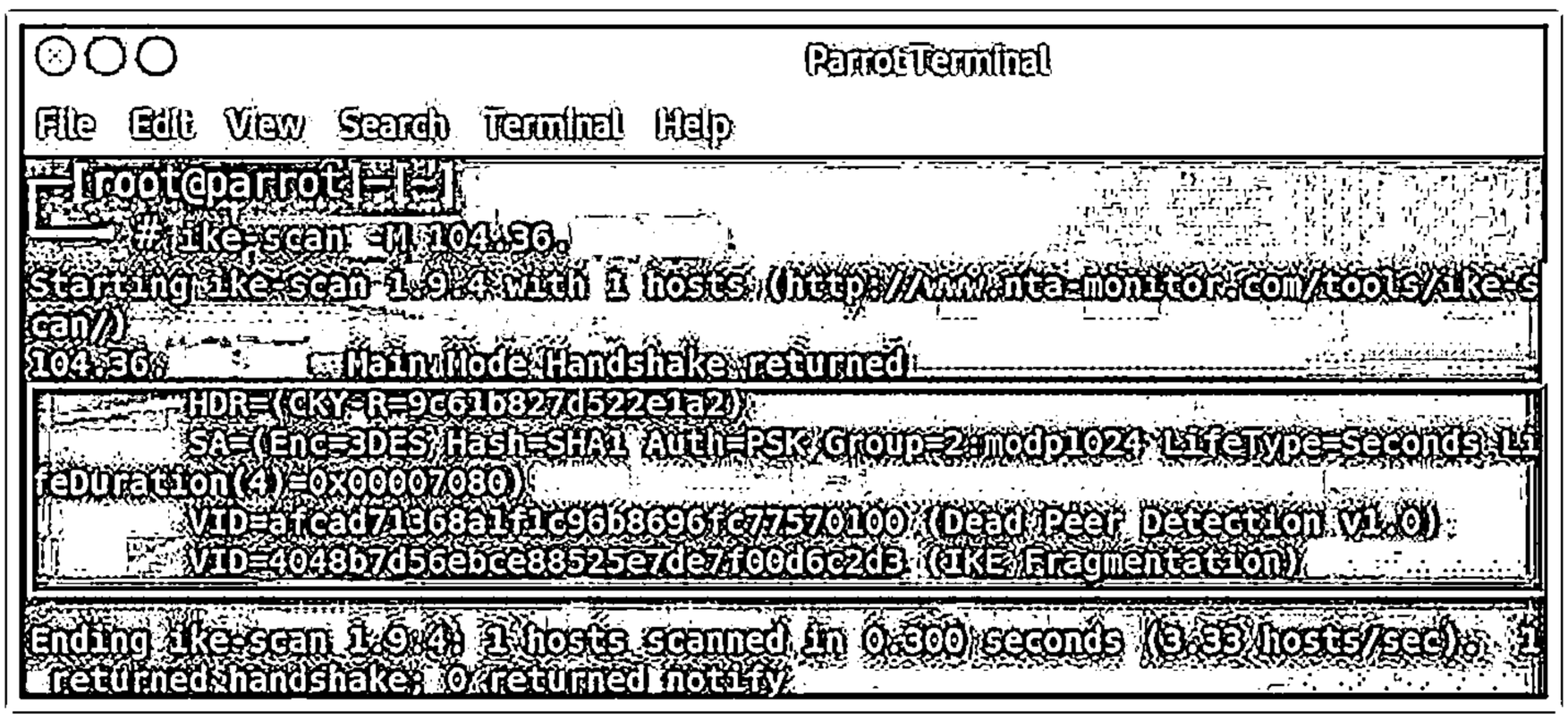


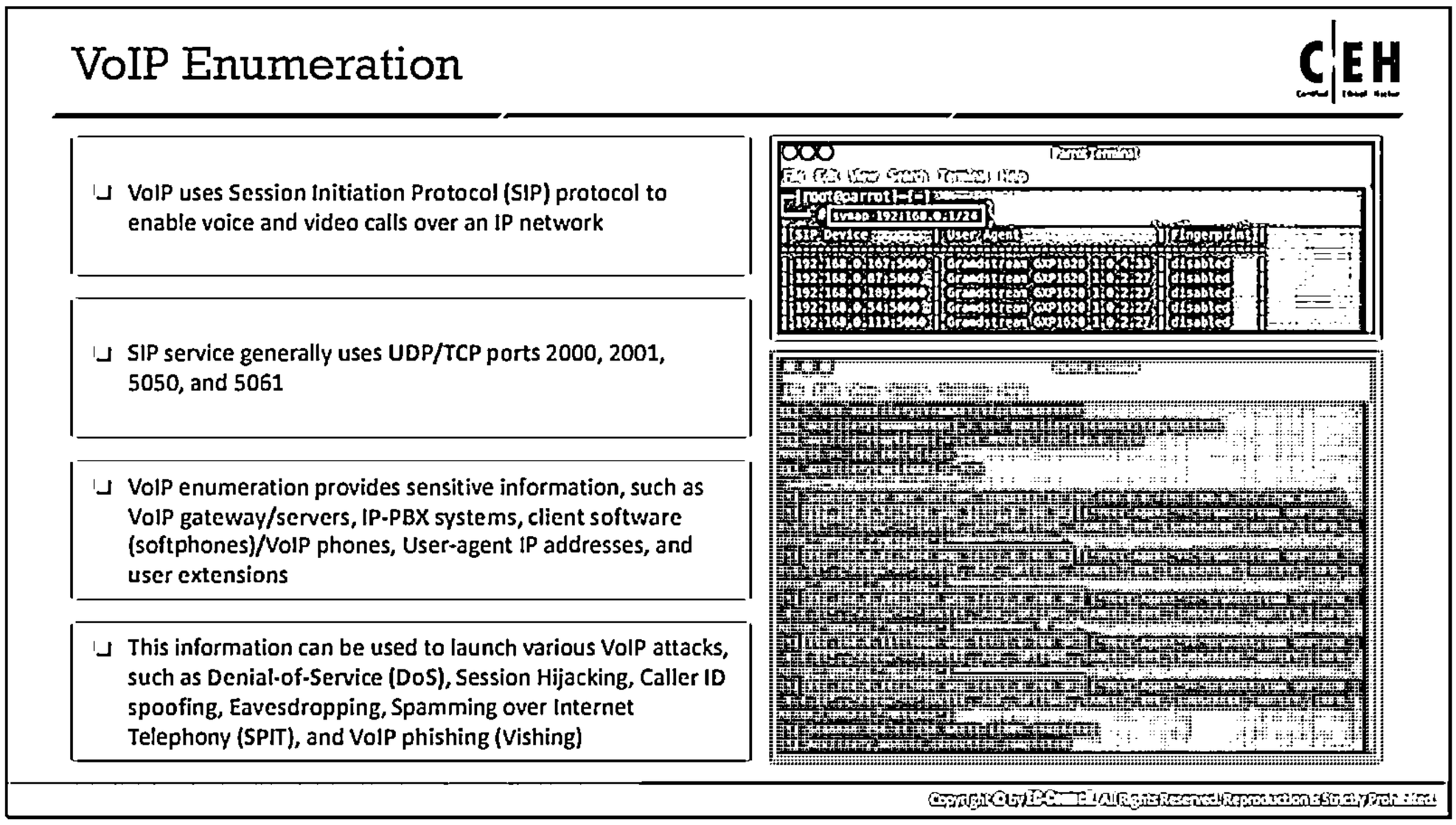
Figure 4.31: Screenshot displaying ike-scan enumeration

ike-scan

Source: *https://github.com*

ike-scan discovers IKE hosts and can fingerprint them using the retransmission backoff pattern. ike-scan can perform the following functions.

- **Discovery**: The hosts running IKE in a given IP range can be determined by displaying the hosts that respond to the IKE requests sent by ike-scan.
- **Fingerprinting**: The IKE implementation used by the hosts can be determined, and in some cases, the version of the software they are running can be determined. This is done in two ways: UDP backoff fingerprinting, which involves recording the times of arrival of the IKE response packets from the target hosts and comparing the observed retransmission backoff pattern against known patterns, and Vendor ID fingerprinting, which compares Vendor ID payloads from the VPN servers against known Vendor ID patterns.
- **Transform enumeration**: The transform attributes supported by the VPN server for IKE phase 1 (e.g., encryption algorithm and hash algorithm) can be determined.
- **User enumeration**: For some VPN systems, valid VPN usernames can be discovered.
- **Pre-shared key cracking**: Offline dictionary or brute-force password cracking can be performed for IKE Aggressive Mode with pre-shared key authentication. This uses ike-scan to obtain the hash and other parameters as well as psk-crack, which is a part of the ike-scan package, to perform the cracking.



VoIP Enumeration

VoIP is an advanced technology that has replaced the conventional public switched telephone network (PSTN) in both corporate and home environments. VoIP uses internet infrastructure to establish connections for voice calls; data are also transmitted on the same network. However, VoIP is vulnerable to TCP/IP attack vectors. Session Initiation Protocol (SIP) is one of the protocols used by VoIP for performing voice calls, video calls, etc. over an IP network. This SIP service generally uses UDP/TCP ports 2000, 2001, 5050, and 5061.

Attackers use Svmap and Metasploit tools to perform VoIP enumeration. Through VoIP enumeration, attackers can gather sensitive information such as VoIP gateway/servers, IP-private branch exchange (PBX) systems, and User-Agent IP addresses and user extensions of client software (softphones) or VoIP phones. This information can be used to launch various VoIP attacks such as DoS attacks, session hijacking, caller ID spoofing, eavesdropping, spam over Internet telephony (SPIT), and VoIP phishing (Vishing).

- **Svmap**

  Source: *https://github.com*

  Svmap is an open-source scanner that identifies SIP devices and PBX servers on a target network. It can be helpful for system administrators when used as a network inventory tool.

  Attackers use Svmap to perform the following:

  - Identify SIP devices and PBX servers on default and non-default ports
  - Scan large ranges of networks

- Scan one host on different ports for an SIP service on that host or multiple hosts on multiple ports
- Ring all the phones on a network simultaneously using the INVITE method

Below screenshot shows an example for the enumeration of SIP device details using the Svmap tool through the following command:

```
# svmap <target network range>
```

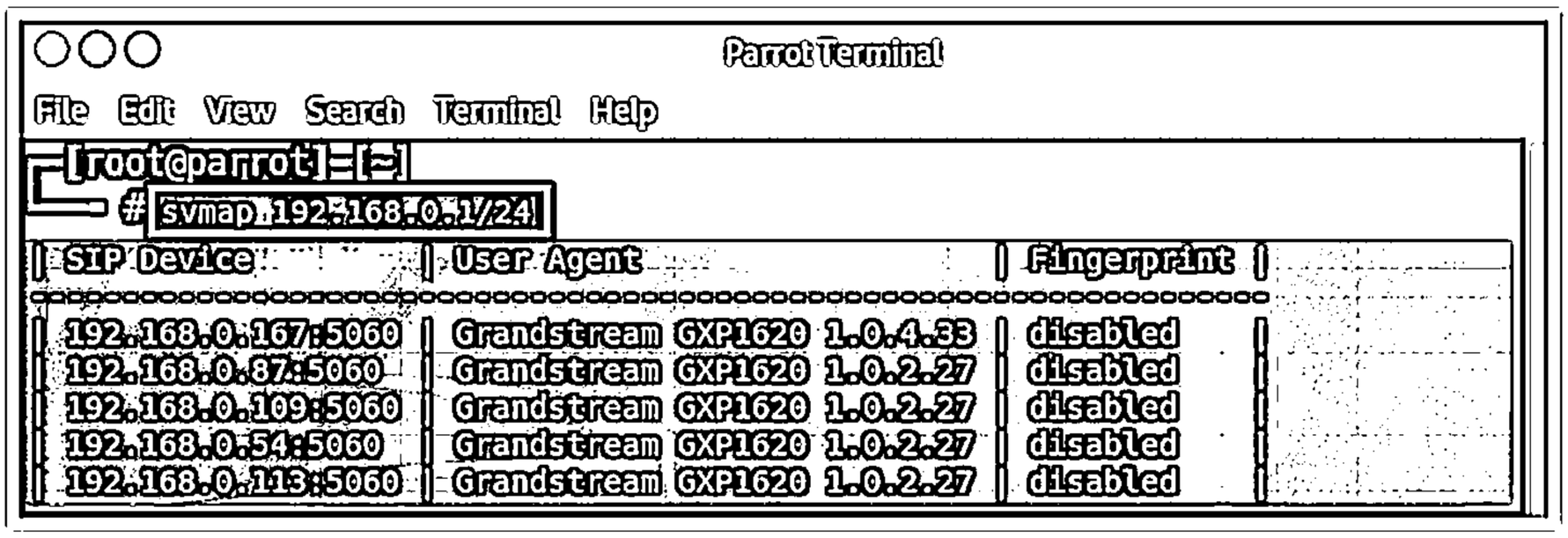


Figure 4.32: Screenshot displaying Svmap scan for enumerating SIP details

Attackers use Metasploit's SIP Username Enumerator to scan numeric usernames/extensions of VoIP phones. Below screenshot shows an example for enumerating SIP using Metasploit.

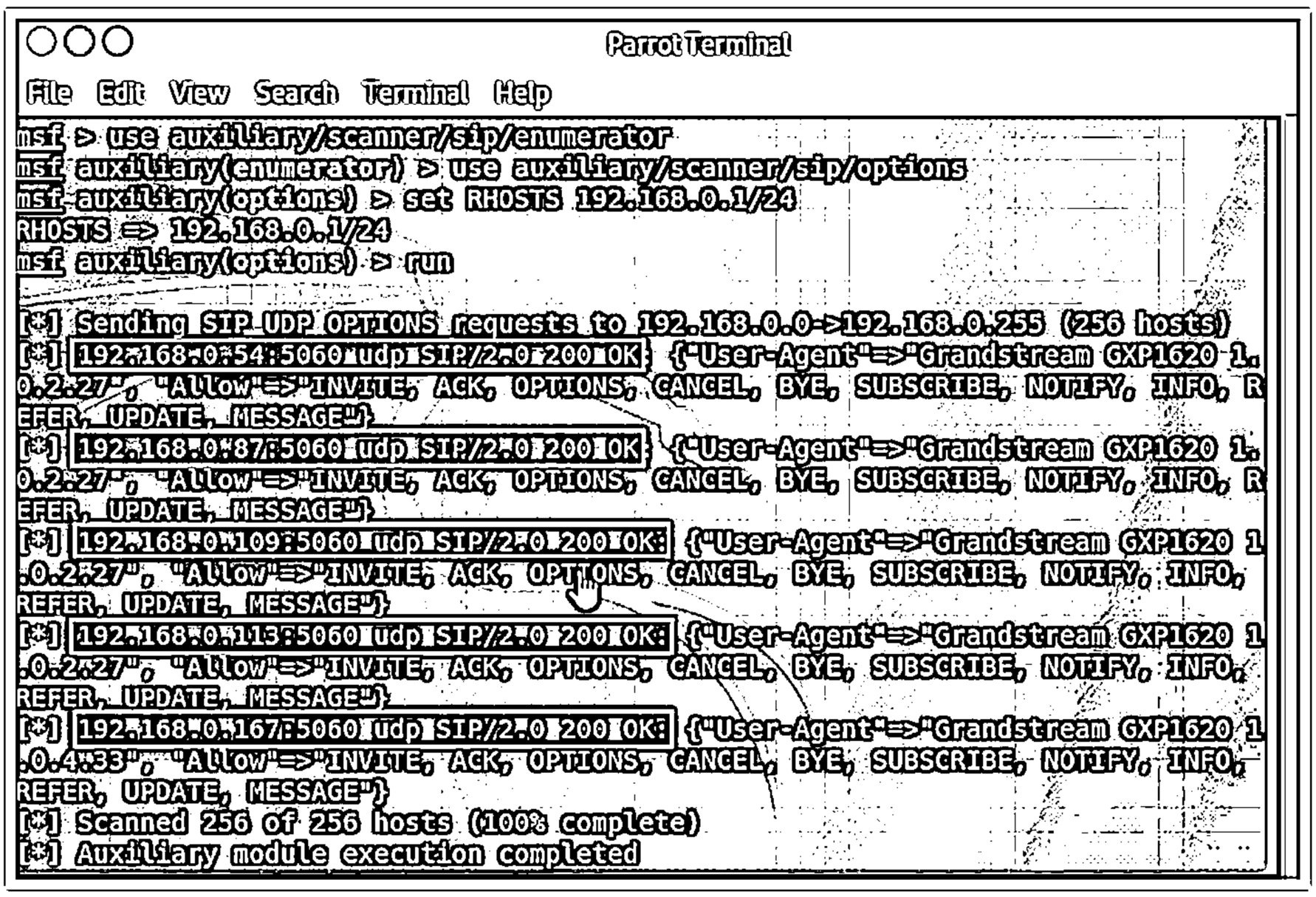
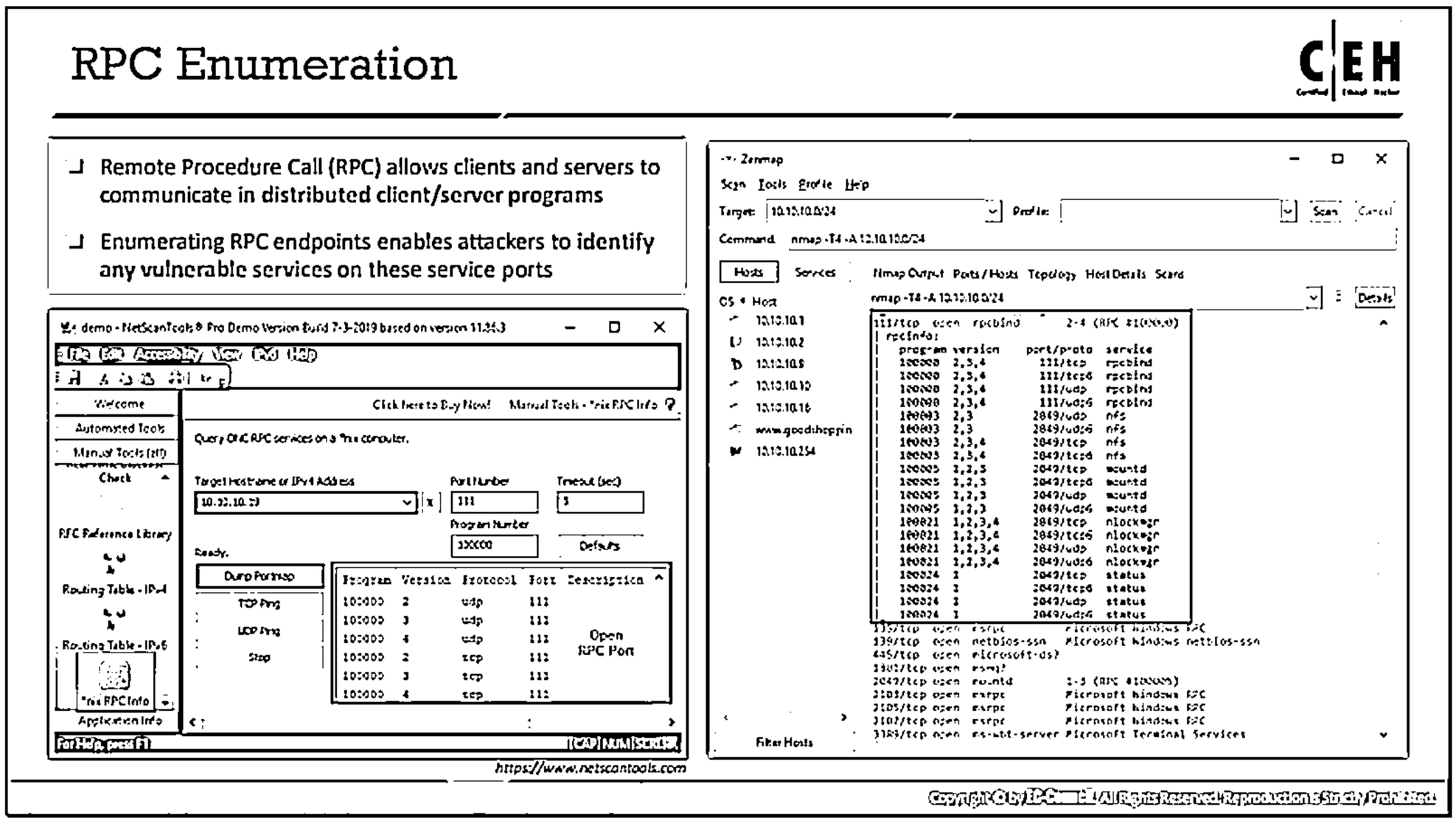


Figure 4.33: Screenshot displaying Metasploit exploit for SIP enumeration



RPC Enumeration

The remote procedure call (RPC) is a technology used for creating distributed client/server programs. RPC allows clients and servers to communicate in distributed client/server programs. It is an inter-process communication mechanism, which enables data exchange between different processes. In general, RPC consists of components such as a client, a server, an endpoint, an endpoint mapper, a client stub, and a server stub, along with various dependencies.

The portmapper service listens on TCP and UDP port 111 to detect the endpoints and present clients, along with details of listening RPC services. Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan wide port ranges to identify RPC services that are open to direct attack.

Attackers use the following Nmap scan commands to identify the RPC service running on the network:

```
# nmap -sR <target IP/network>
# nmap -T4 -A <target IP/network>
```

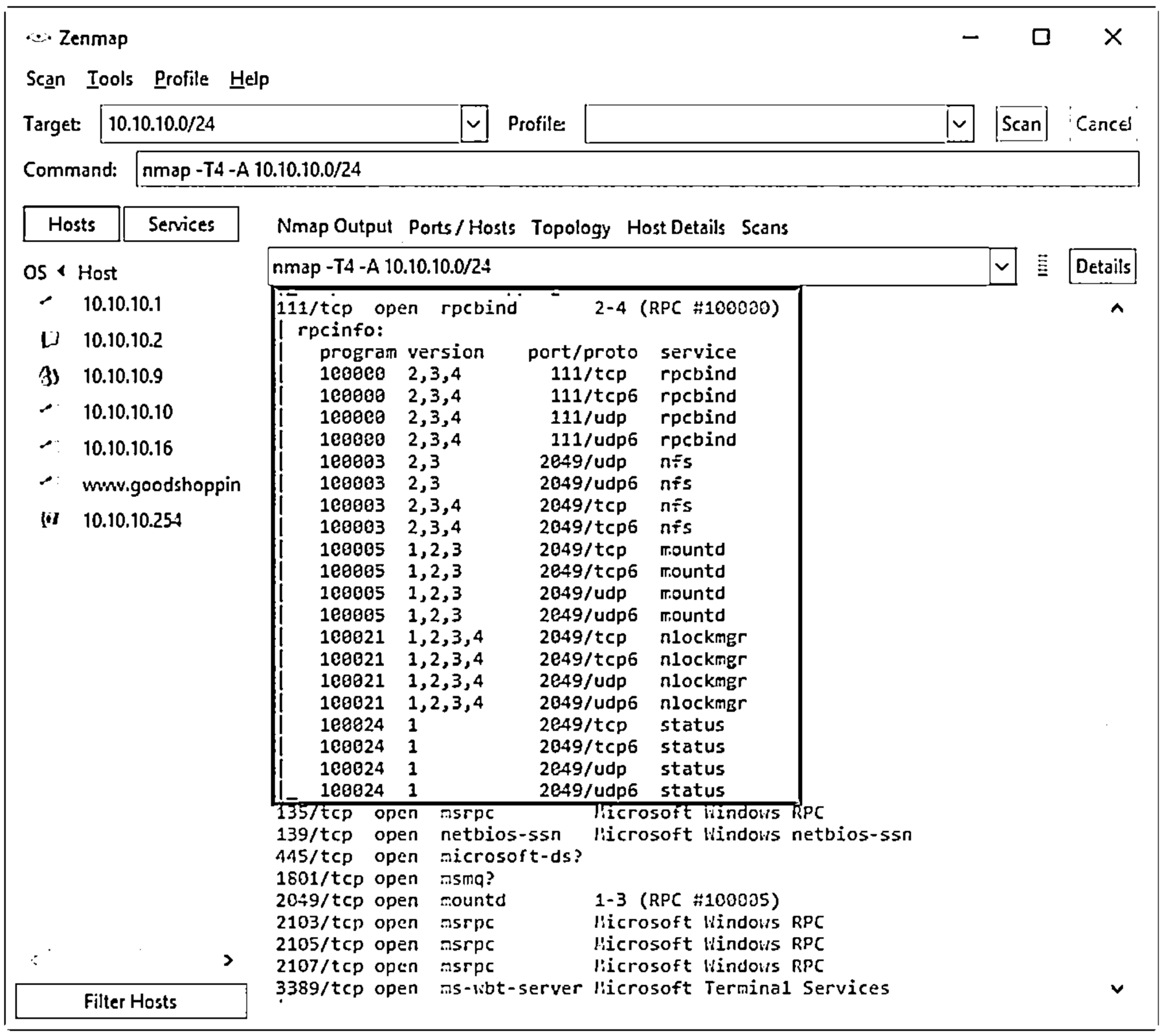


Figure 4.34: Screenshot displaying an Nmap scan result for RPC enumeration

Additionally, attackers use tools such as NetScanTools Pro to capture the RPC information of the target network. The NetScanTools Pro RPC Info tool helps attackers detect and access the portmapper daemon/service that typically runs on port 111 of Unix or Linux machines.

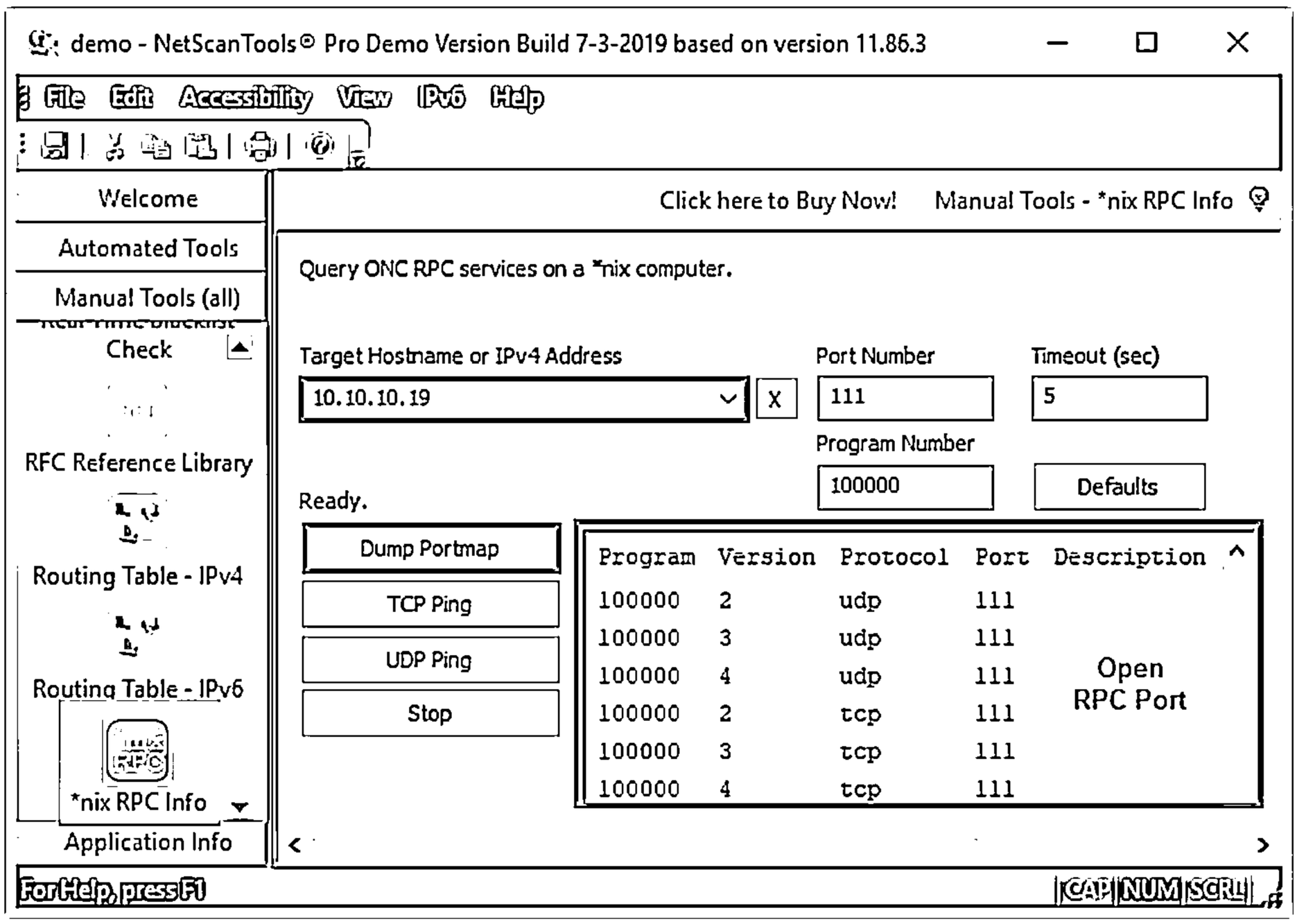
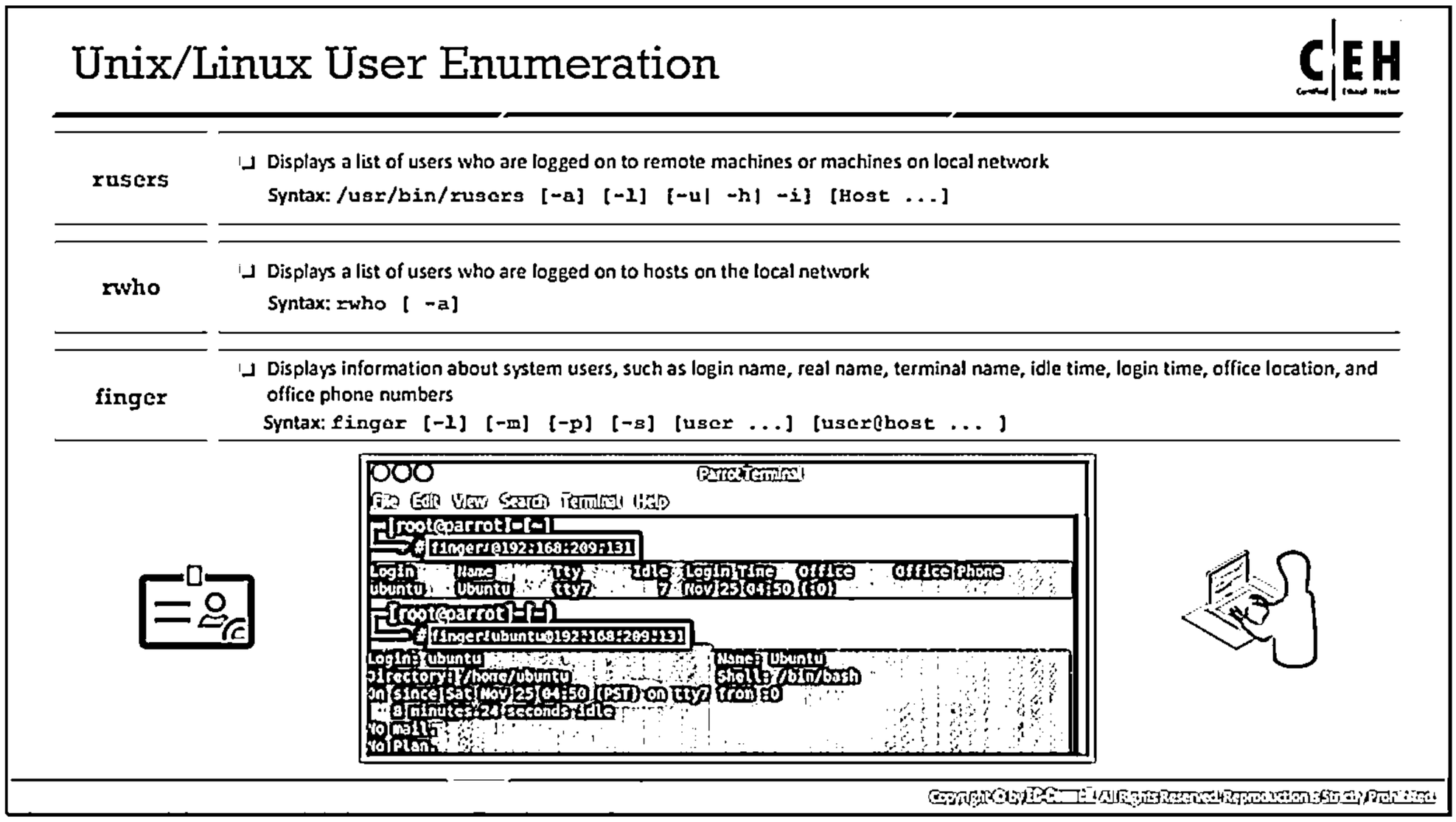


Figure 4.35: Screenshot displaying NetScanTools Pro tool for RPC enumeration



Unix/Linux User Enumeration

One of the important steps for enumeration is to perform Unix/Linux user enumeration. Unix/Linux user enumeration provides a list of users along with details such as the username, host name, and start date and time of each session.

The following command-line utilities can be used to perform Unix/Linux user enumeration.

- **rusers**

  rusers displays a list of users who are logged in to remote machines or machines on the local network. It displays an output similar to the who command, but for the hosts/systems on the local network. Its syntax is as follows:

  ```
  /usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]
  ```

  The options are as follows.

  - **-a**: Gives a report for a machine even if no users are logged in
  - **-h**: Sorts alphabetically by host name
  - **-l**: Gives a longer listing similar to the who command
  - **-u**: Sorts by the number of users
  - **-i**: Sorts by idle time

- **rwho**

  rwho displays a list of users who are logged in to hosts on the local network. Its output is similar to that of the who command and contains information about the username, host name, and start date and time of each session for all machines on the local network running the rwho daemon. Its syntax is as follows:

```
rwho [ -a]
```

It has the following option.

- **-a**: Includes all users; without this flag, users whose sessions are idle for an hour or more are not included in the report

- **finger**

  finger displays information about system users such as the user's login name, real name, terminal name, idle time, login time, office location, and office phone numbers. Its syntax is as follows:

  ```
  finger [-l] [-m] [-p] [-s] [user ...] [user@host ...]
  ```

  The options are as follows.

  - **-s**: Displays the user's login name, real name, terminal name, idle time, login time, office location, and office phone number
  - **-l**: Produces a multi-line format displaying all of the information described for the -s option as well as the user's home directory, home phone number, login shell, mail status, and the contents of the files ".plan," ".project," ".pgpkey," and ".forward" from the user's home directory
  - **-p**: Prevents the -l option of finger from displaying the contents of the ".plan," ".project," and ".pgpkey" files.
  - **-m**: Prevents the matching of usernames.

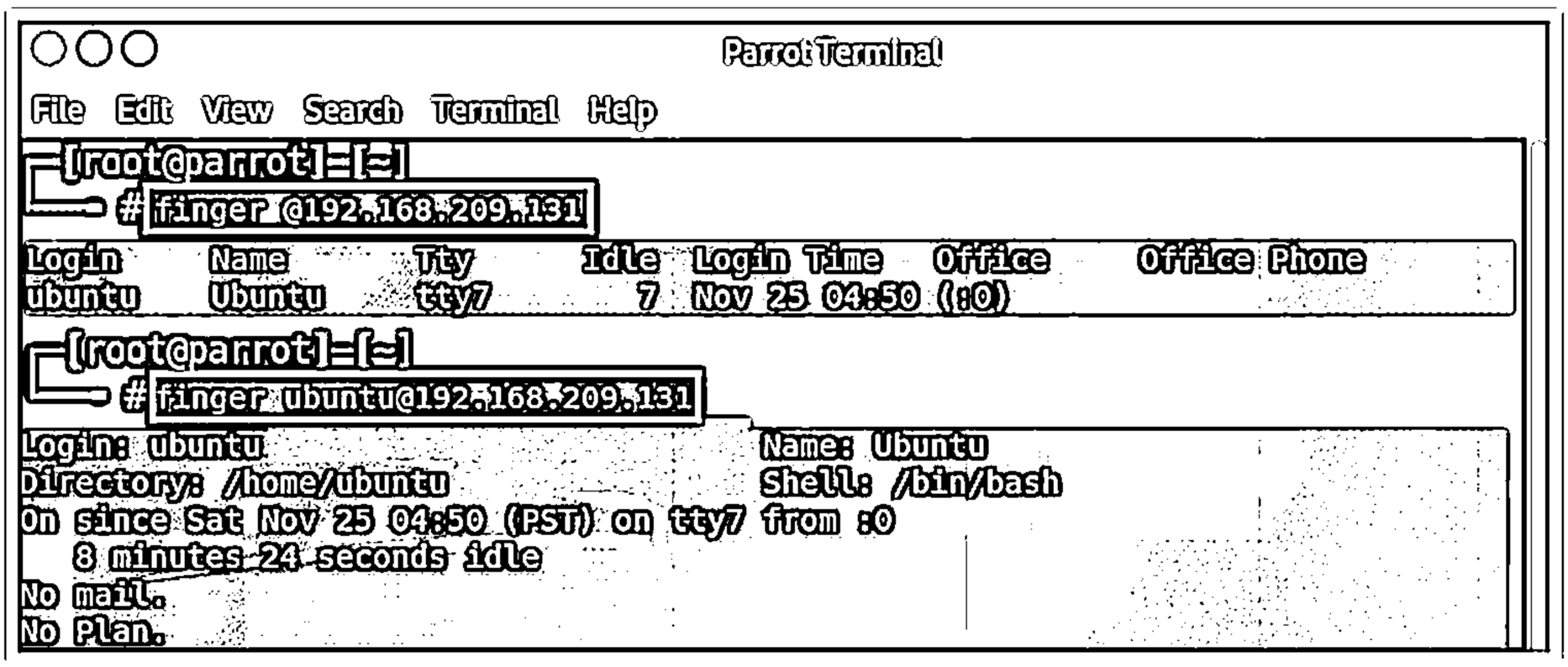
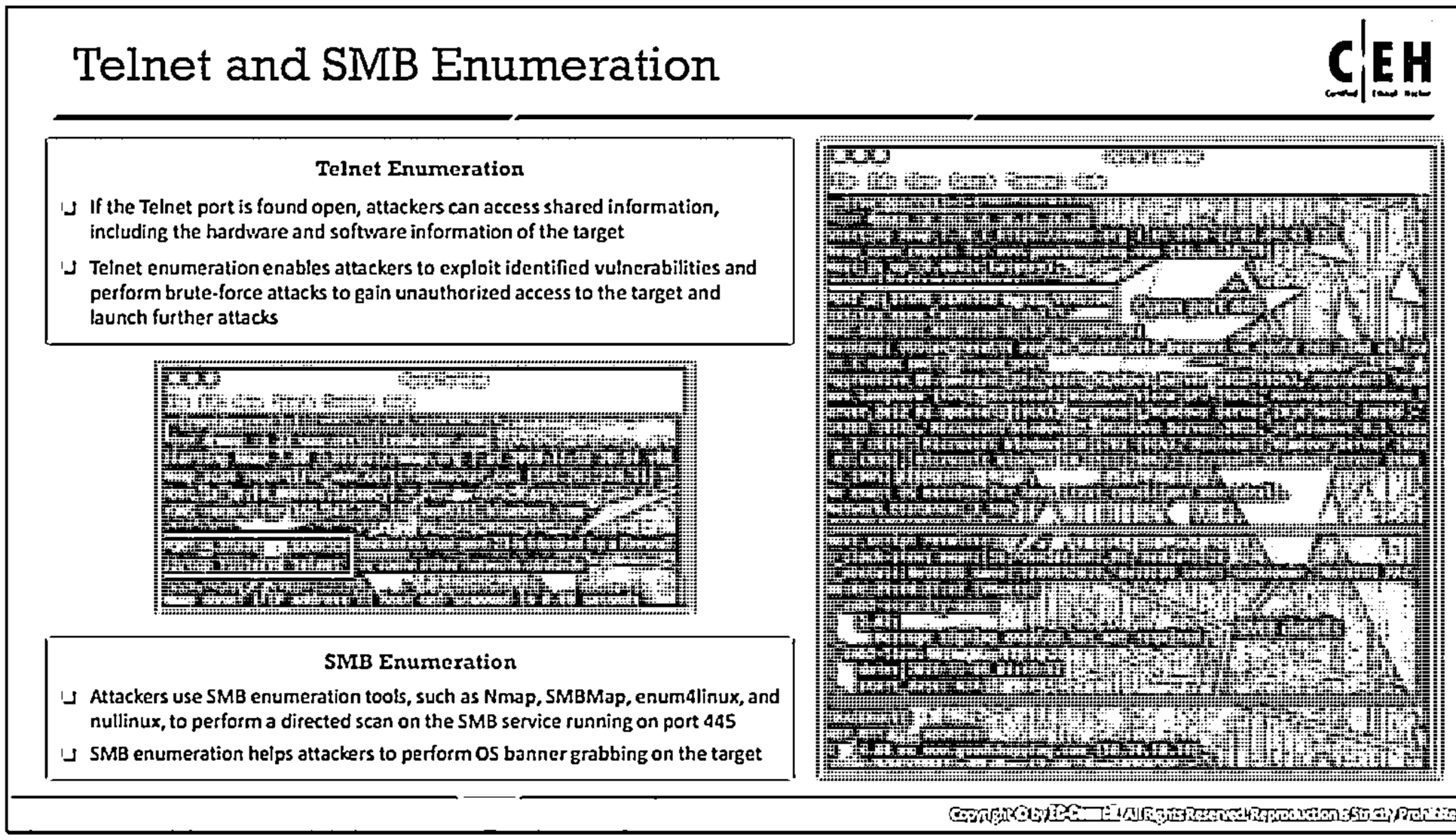


Figure 4.36: Screenshot displaying the execution of the finger command for user enumeration



Telnet Enumeration

Telnet is a network terminal protocol that allows users to access remote computers or servers over the Internet. This protocol provides two-way interactive communication for computers on LANs and the Internet. Depending on the privileges assigned to the users, they can use Telnet to log in to the remote system to access specific files, services, data, etc.

Attackers perform port scanning to gather information regarding open ports and services on the target server. If the Telnet port is found to be open, attackers can learn about the information being shared, including hardware and software information of the target. By using this information, attackers can exploit their specific vulnerabilities and perform a brute-force attack to gain unauthorized access to the target system. Attackers can use the Nmap tool to perform simple direct scanning for Telnet port 23.

As shown in the screenshot, the following Nmap command is used by attackers to enumerate the Telnet service running on the target system:

```
# nmap -p 23 <target domain>
```

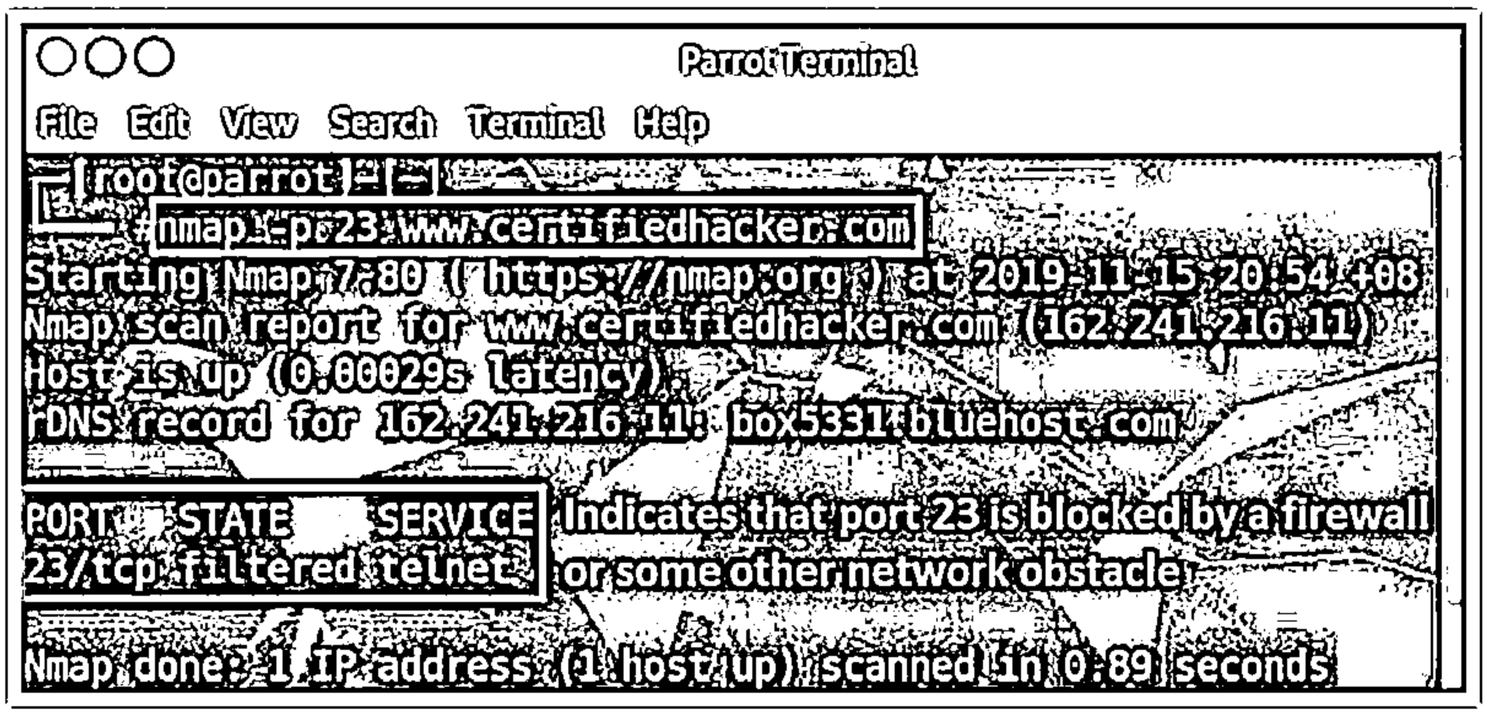


Figure 4.37: Screenshot of Nmap displaying a Telnet enumeration result

Attackers can further use the following script to enumerate information from remote Microsoft Telnet services with New Technology LAN Manager (NTLM) authentication enabled:

```
# nmap -p 23 --script telnet-ntlm-info <target IP>
```

Once the information about the target server is obtained, the attackers can use the following script to perform a brute-force attack against the Telnet server:

```
# nmap -p 23 –script telnet-brute.nse –script-args
userdb=/root/Desktop/user.txt,passdb=/root/Desktop/pass.txt <target
IP>
```

SMB Enumeration

Server Message Block (SMB) is a transport protocol that is generally used by Windows systems for providing shared access to files, printers, and serial ports as well as remote access to Windows services. By default, SMB runs directly on TCP port 445 or via the NetBIOS API on UDP ports 137 and 138 and TCP ports 137 and 139. By using the SMB service, users can access files and other data stored at a remote server. The SMB service also allows application users to read, write, and modify the files on the remote server. A network running this service is highly vulnerable to SMB enumeration, which provides a good amount of information about the target.

In SMB enumeration, attackers generally perform banner grabbing to obtain information such as OS details and versions of services running. By using this information, attackers can perform various attacks such as SMB relay attacks and brute-force attacks. Attackers can also use SMB enumeration tools such as Nmap, SMBMap, enum4linux, nullinux, and NetScanTool Pro to perform a directed scan on the SMB service running on port 445.

As shown in the screenshot, attackers use the following Nmap command to enumerate the SMB service running on the target IP address:

```
# nmap -p 445 -A <target IP>
```

In the above command, the option `-p` specifies a port to scan (`445` in this case), and option `-A` is used for OS detection, version detection, script scanning, and traceroute information.

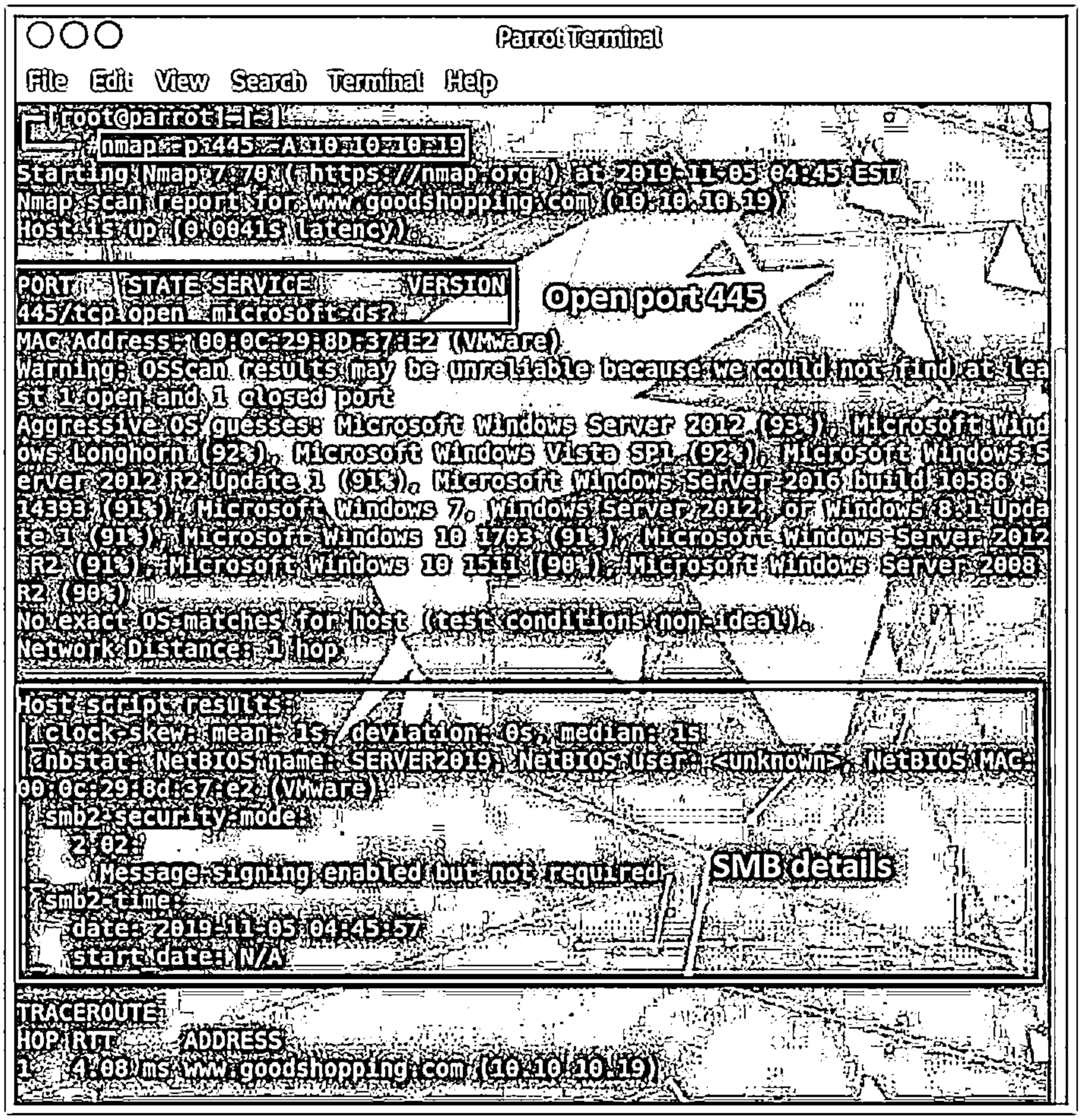
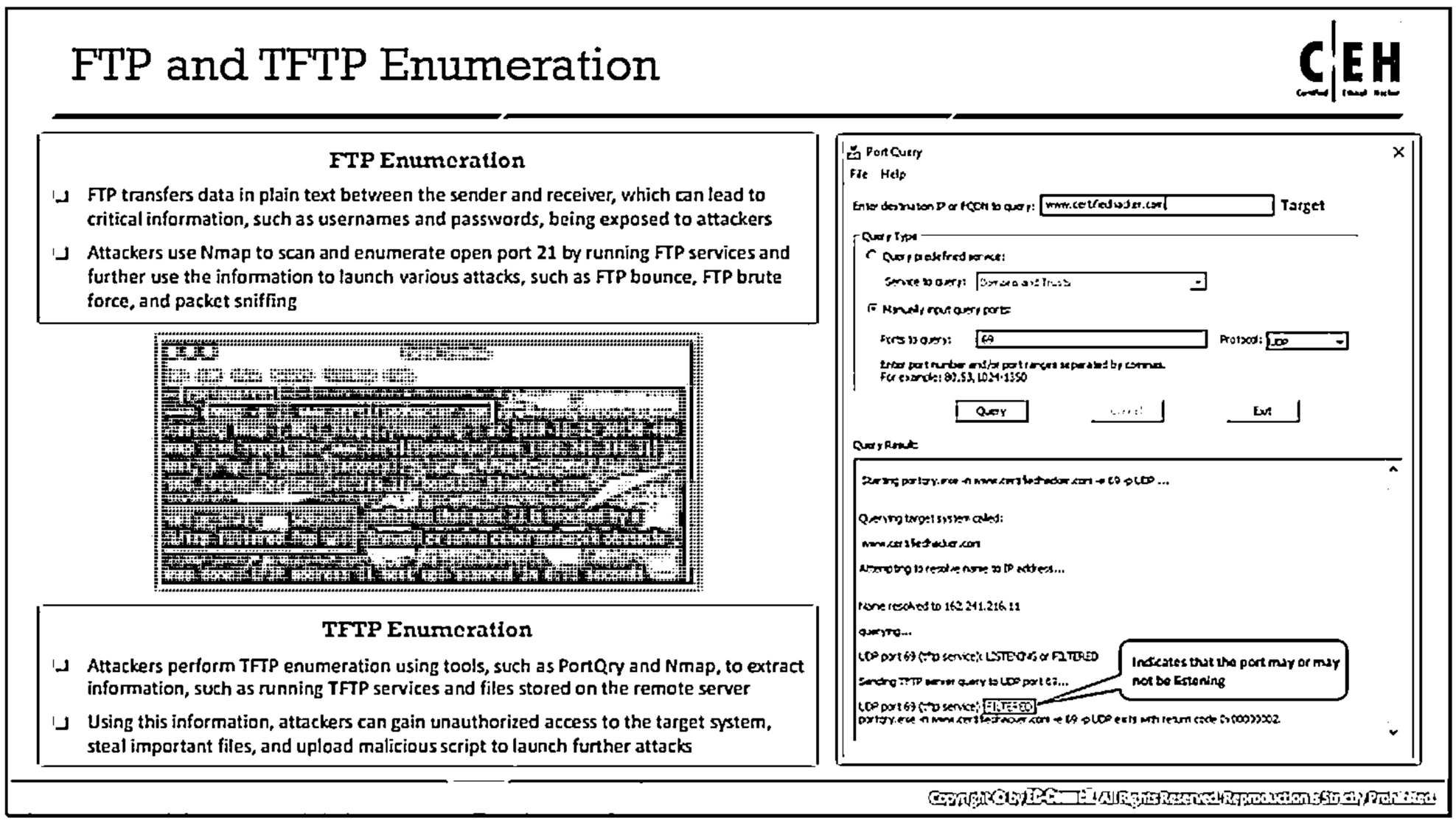


Figure 4.38: Screenshot of Nmap performing SMB enumeration

The `STATE` of `PORT 445/tcp` is `OPEN`, which indicates that port 445 is open and that the SMB service is running. By using this command, attackers can also obtain details on the OS and traceroute of the specified target.



FTP Enumeration

The File Transfer Protocol (FTP) is used to transfer files over TCP, and its default port is 21. In FTP, data are transferred between a sender and receiver in plaintext, exposing critical information such as usernames and passwords to attackers. FTP offers neither a secure network environment nor secure user authentication. Individuals do not need authentication to access an FTP server in a network. This provides an easy method for attackers to access network resources.

The implementation of FTP in an organization's network makes the data accessible to external sources. Attackers can scan and enumerate open port 21 running FTP services and further use this information to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing.

As shown in the screenshot, the following Nmap command is used by the attackers to enumerate the FTP service running on the target domain:

```
# nmap -p 21 <target domain>
```

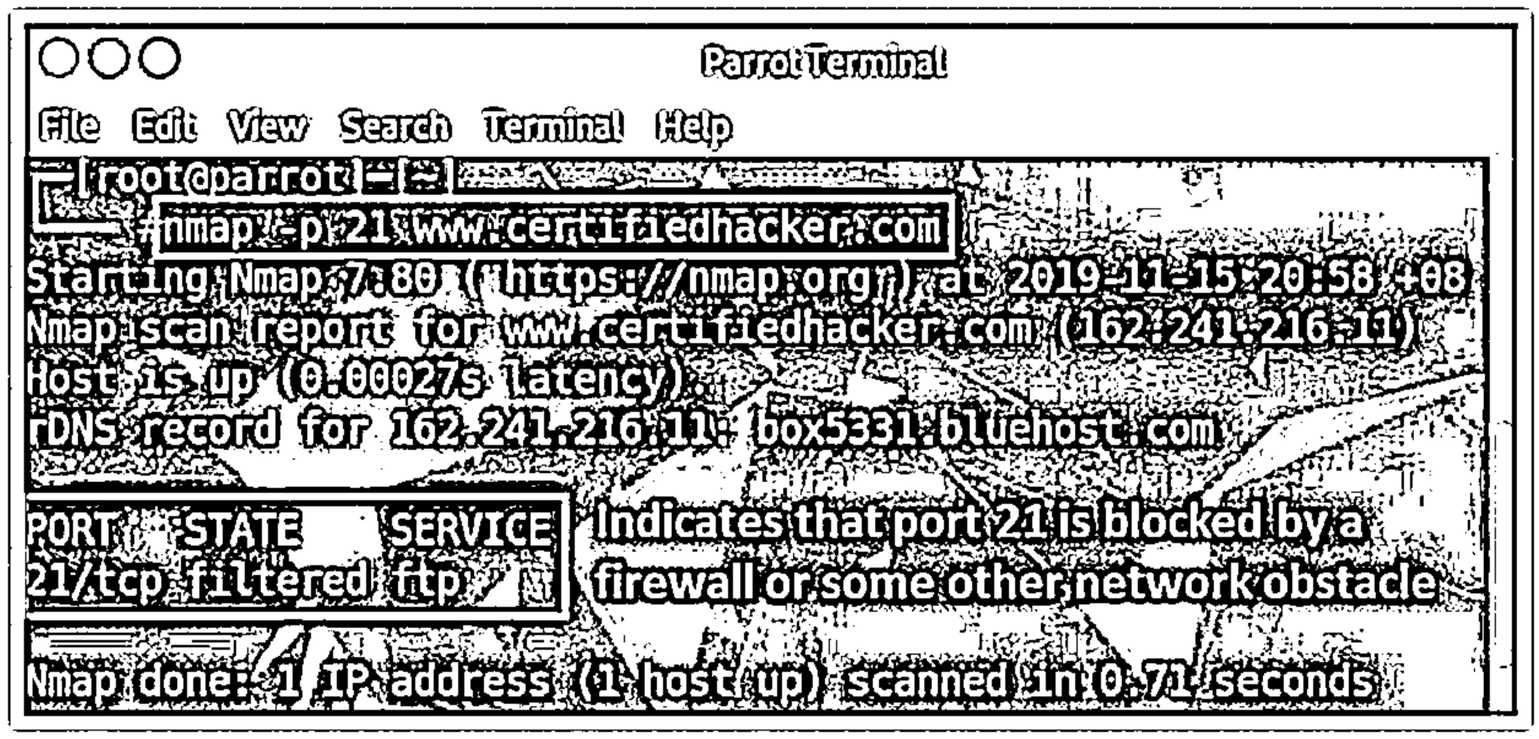


Figure 4.39: Screenshot of Nmap displaying a FTP enumeration result

Attackers also use Metasploit to enumerate FTP services running on remote hosts. The following commands can be used to detect the FTP version of the target server:

```
use auxiliary/scanner/ftp/ftp_version
msf auxiliary(scanner/ftp/ftp_version) > set RHOSTS <target IP>
msf auxiliary(scanner/ftp/ftp_version) > exploit
```

TFTP Enumeration

The Trivial File Transfer Protocol (TFTP) is a simplified version of FTP and is used for transferring files between network devices. By default, TFTP servers listen on UDP port 69. This protocol is used when directory visibility and user authentication are not required; therefore, it provides no security features.

To perform TFTP enumeration, attackers can use tools such as PortQry and Nmap to extract information such as running TFTP services and files stored on a remote server. By using the enumerated information, attackers can further gain unauthorized access to the target system, steal important files, and upload malicious scripts to launch further attacks. Furthermore, this information enables attackers to perform various attacks such as DNS amplification attacks, TFTP reflection attacks, and DDoS attacks.

- **PortQry**

  Source: *https://www.microsoft.com*

  The PortQry utility reports the port status of TCP and UDP ports on a selected target. Attackers can use the PortQry tool to perform TFTP enumeration. This utility reports the port status of target TCP and UDP ports on a local or remote computer.

  In the PortQry tool, the attackers can specify the target to scan for a running TFTP service on open port 69. As shown in the screenshot, attackers perform TFTP enumeration on the target domain by setting the `Ports to query:` value to 69 and `Protocol` to UDP.

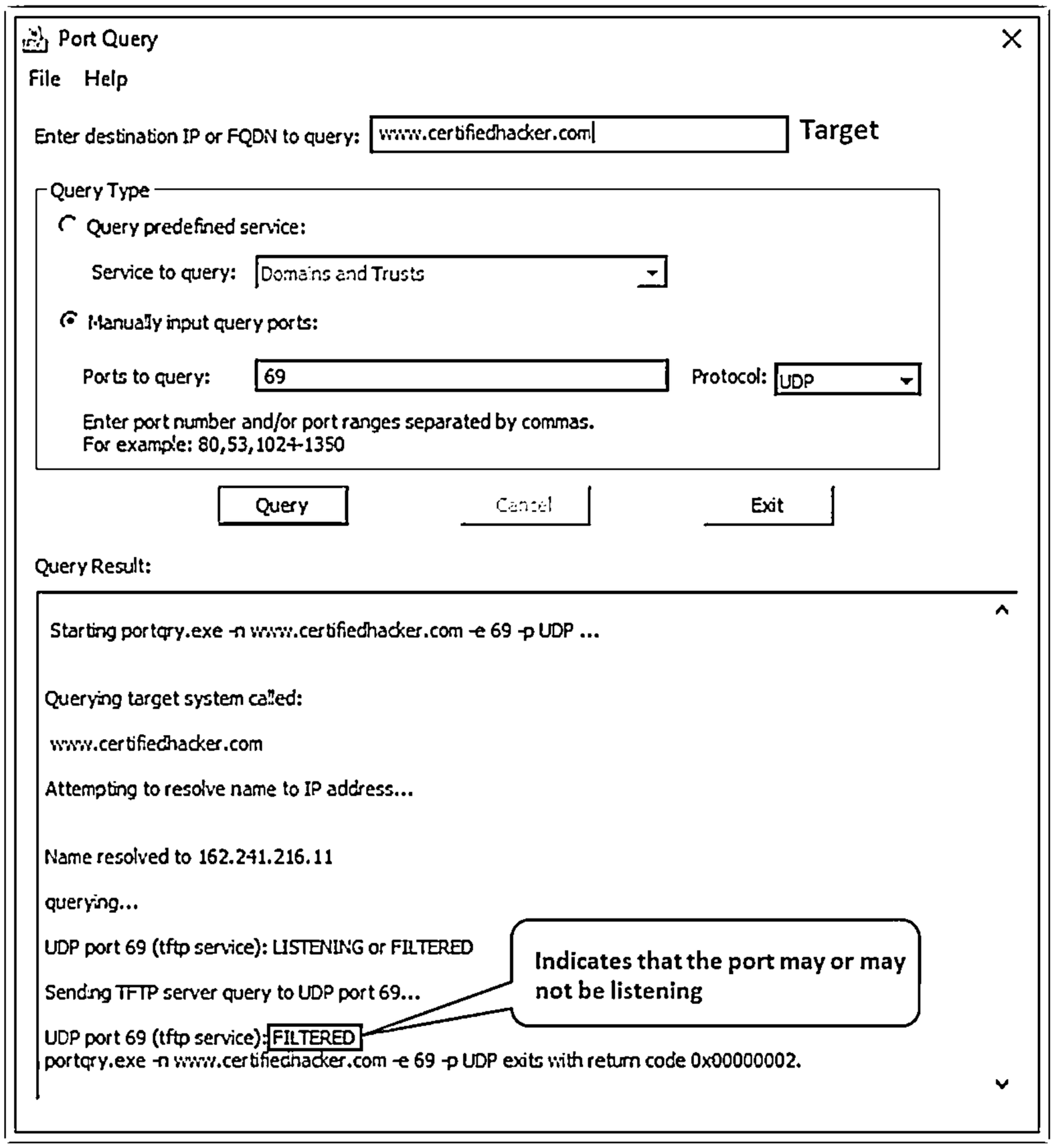


Figure 4.40: Screenshot of the PortQry tool displaying a TFTP scan result

Attackers can also use the PortQry command-line utility to perform TFTP enumeration using the following command:

```
portqry -n <target domain> -e 69 -p udp
```

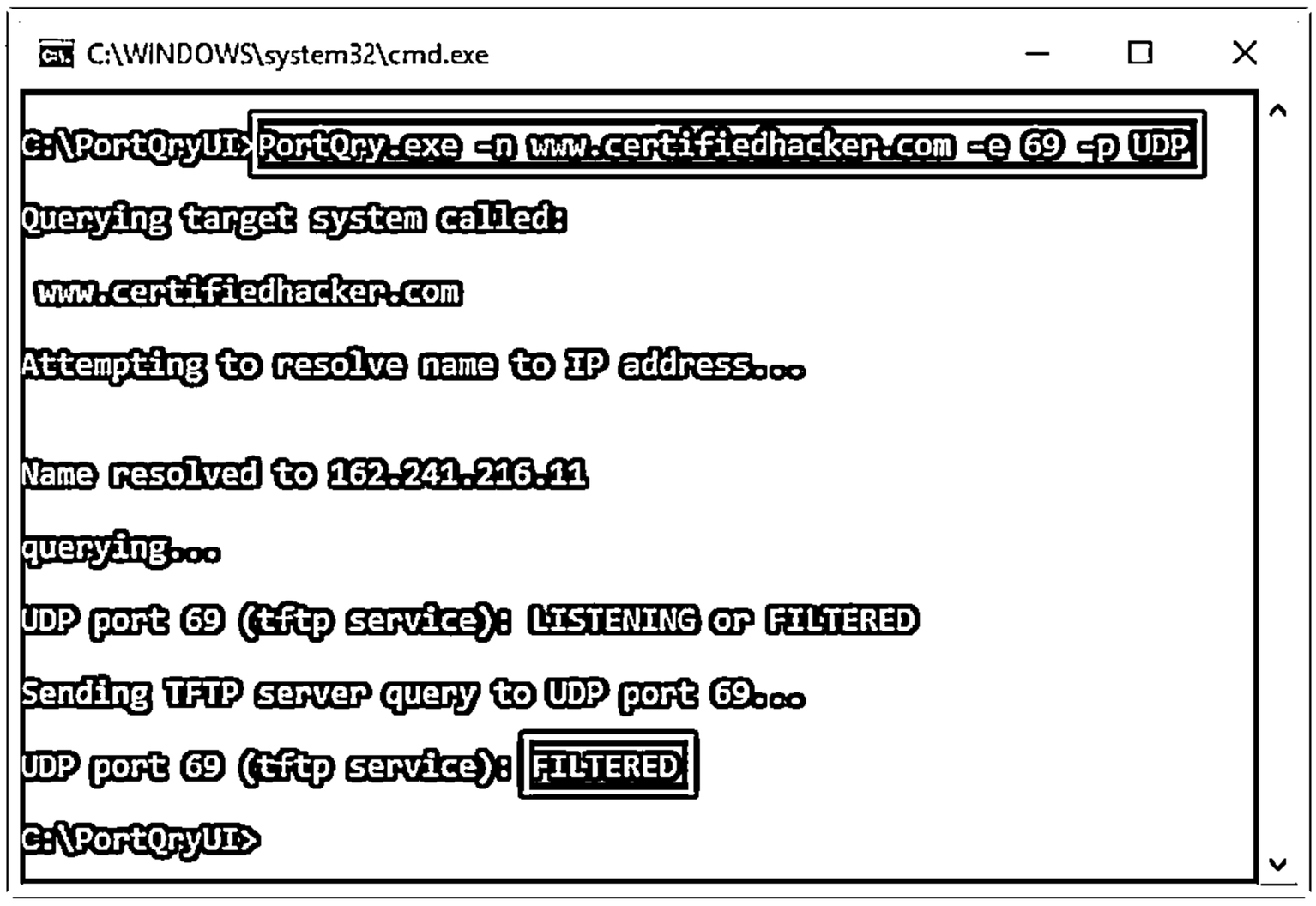


Figure 4.41: Screenshot of the PortQry command-line utility showing a TFTP scan result

- **Nmap**

  Source: *https://nmap.org*

  Attackers can use the Nmap tool to perform simple direct scanning for TFTP port 69. As shown in the screenshot, the following Nmap command is used by attackers to enumerate the TFTP service running on the target domain:

  ```
  # nmap -p 69 <target domain>
  ```

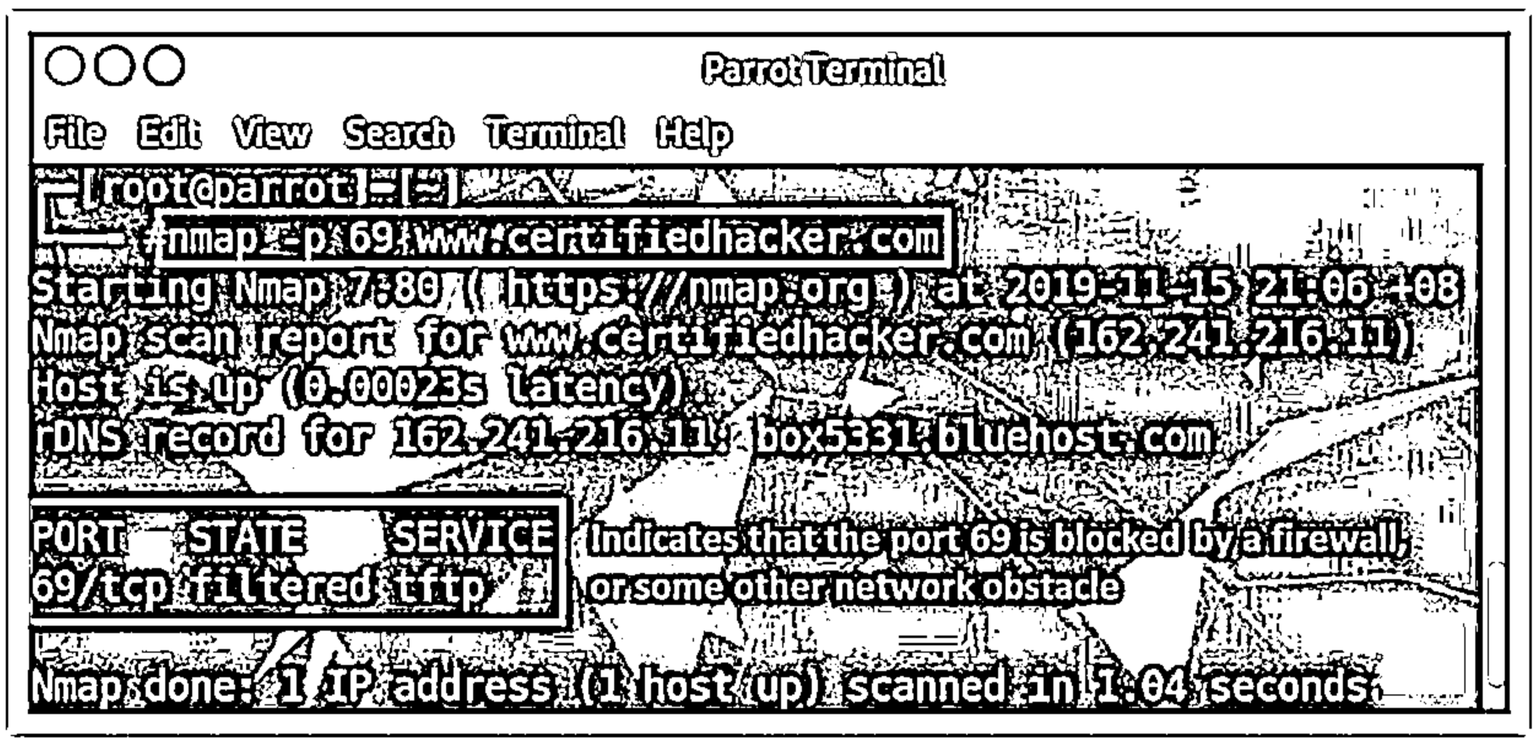
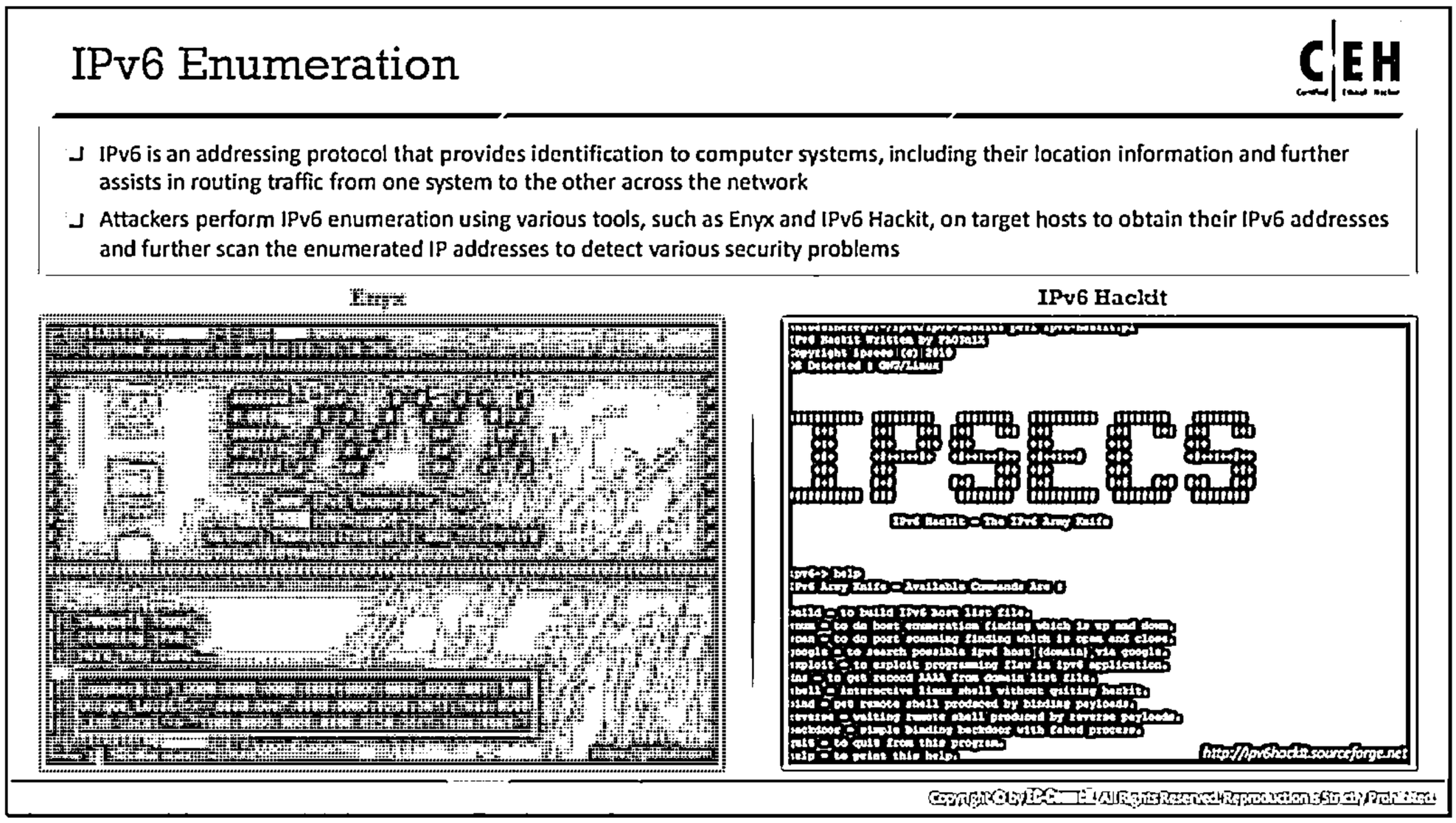


Figure 4.42: Screenshot of Nmap command displaying a TFTP scan result



IPv6 Enumeration

Internet Protocol version 6 (IPv6) is an addressing protocol that identifies computer systems, including location information, and assists in routing traffic from one system to another system across a network. It is an advanced version of IPv4 and, therefore, supports a greater number of hosts as compared to IPv4. It was designed to overcome the problem of IPv4 address exhaustion.

Attackers perform IPv6 enumeration on target hosts to obtain their IPv6 addresses and further scan the enumerated IP addresses to detect various security problems such as access to routing structure, exposure of sensitive content, and users' access control lists. By using this information, attackers can launch various attacks such as SYN flood attacks, DNS amplification attacks, and DDoS attacks. Attackers can scan and enumerate the IPv6 address of a target machine in the network by using various tools such as Enyx and IPv6 Hackit.

- **Enyx**

  Source: *https://github.com*

  Enyx is an enumeration tool that fetches the IPv6 address of a machine through SNMP.

  As shown in the screenshot, attackers use the following command to enumerate the IPv6 address of a target machine (`10.10.10.20`) by setting the SNMP version to `2c` and community string to `public`:

  ```
  Python enyx.py 2c public <target IP>
  ```

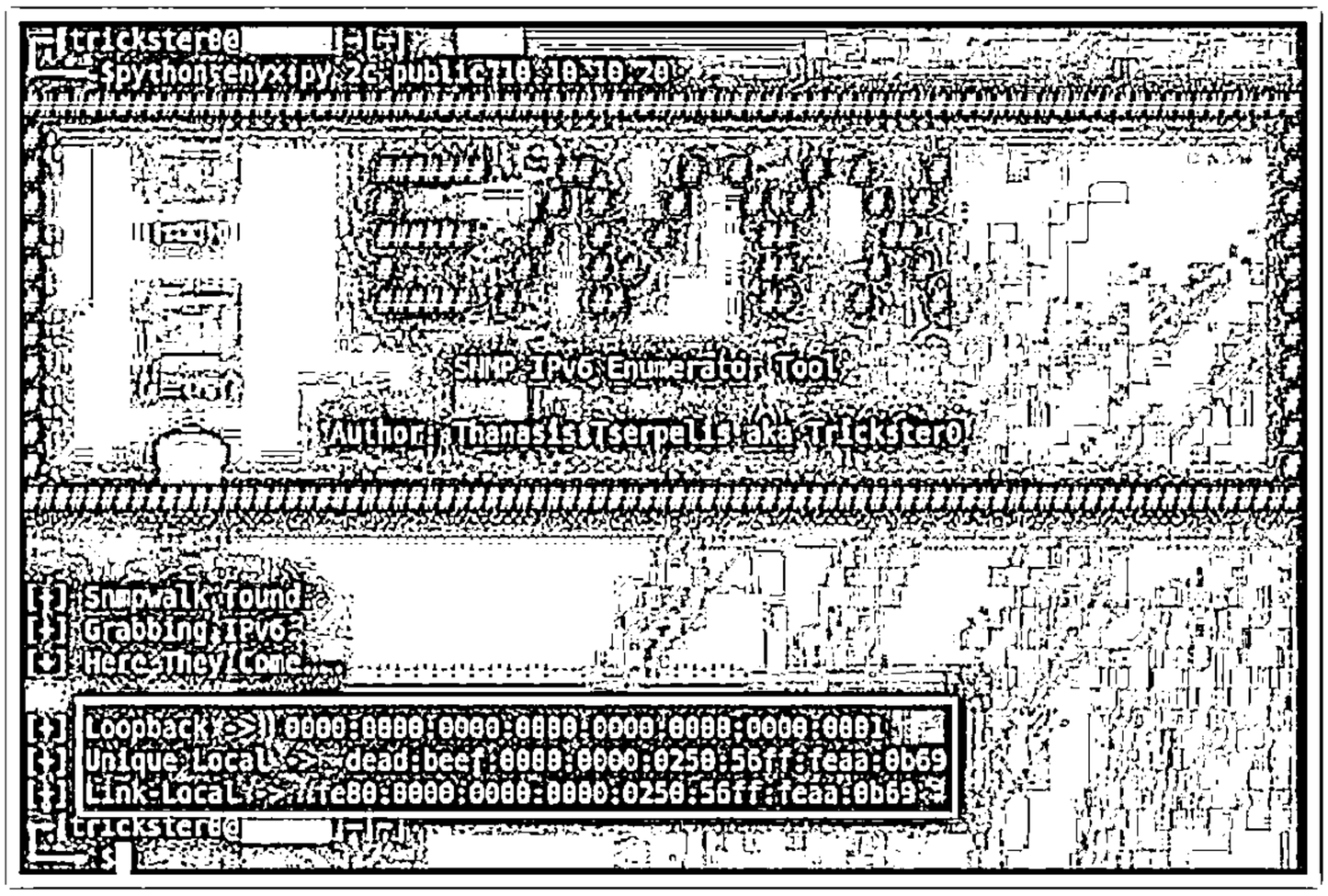


Figure 4.43: Screenshot of Enyx tool displaying enumerated results

- **IPv6 Hackit**

  Source: *http://ipv6hackit.sourceforge.net*

  Hackit is a scanning tool that provides a list of active IPv6 hosts. It can perform TCP port scanning and identify AAAA IPv6 host records.

  As shown in the screenshot, attackers can specify the target machine and run a scan to enumerate the IPv6 information.

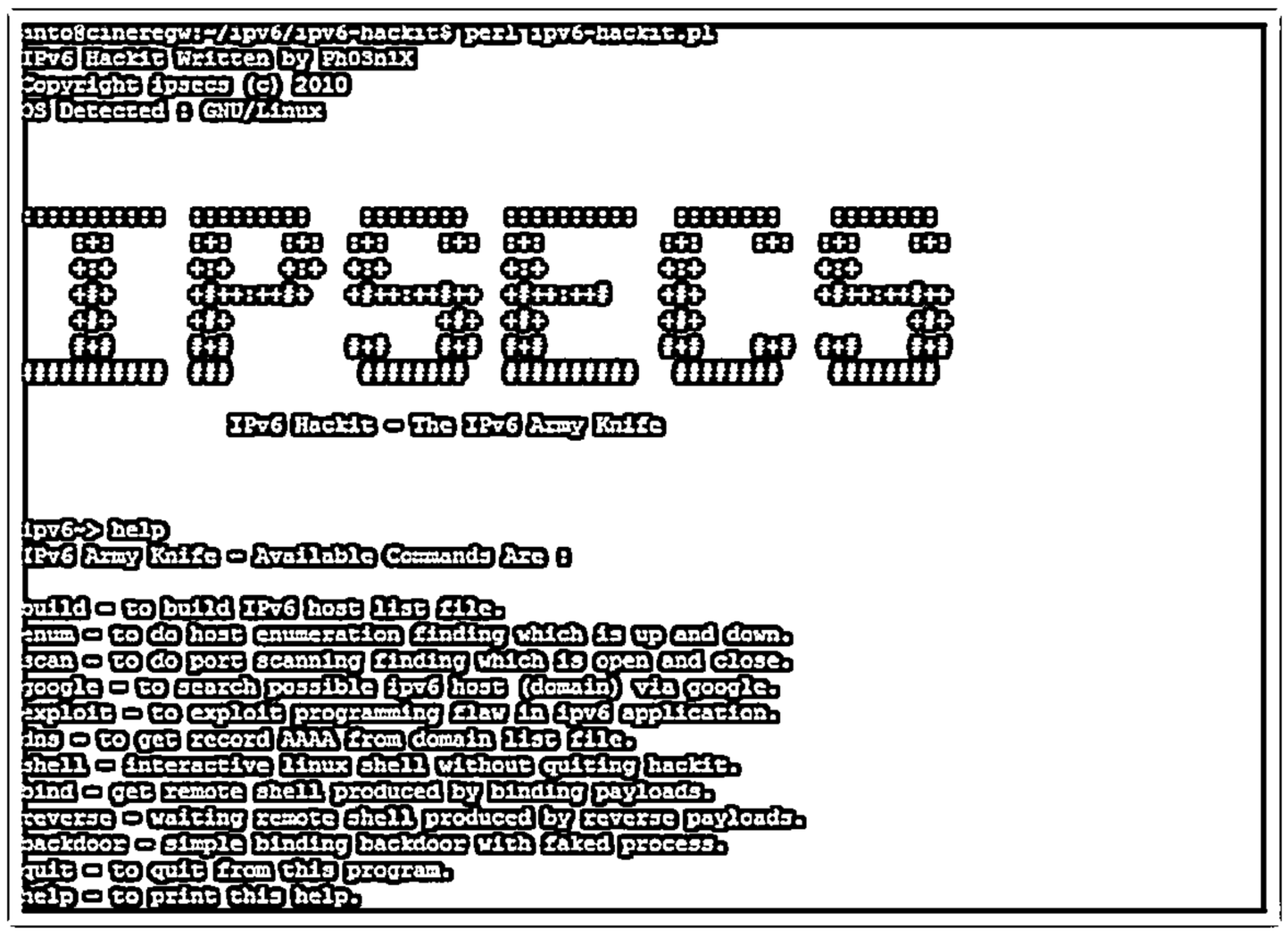
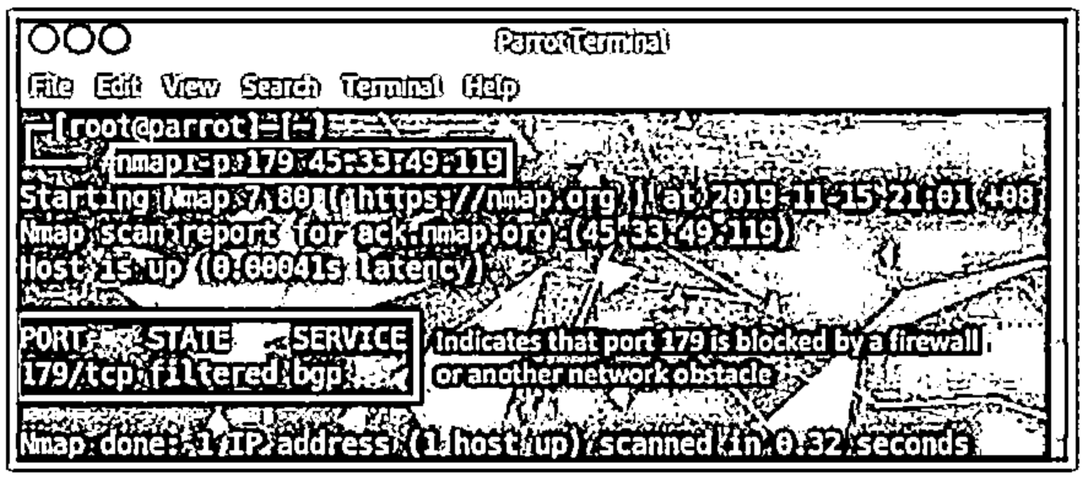
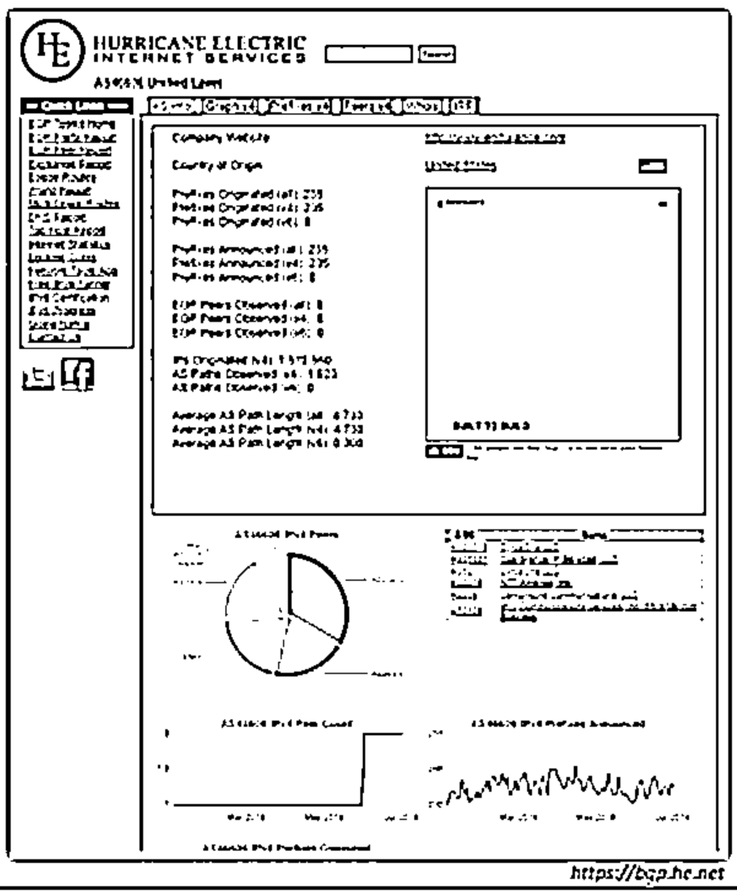


Figure 4.44: Screenshot displaying the IPv6 Hackit tool

BGP Enumeration

- Border Gateway Protocol (BGP) is a routing protocol used to exchange routing and reachability information between different autonomous systems (AS) present on the Internet
- Attackers perform BGP enumeration using tools, such as Nmap and BGP Toolkit, to discover the IPv4 prefixes announced by the AS number and routing path followed by the target
- Attackers use this information to launch various attacks, such as man-in-the-middle attack, BGP hijacking attack, and DoS attack against the target





BGP Enumeration

The Border Gateway Protocol (BGP) is a routing protocol used to exchange routing and reachability information between different autonomous systems (AS) on the Internet. Because this protocol is used to connect one AS to other ASs, it is also called external BGP (eBGP). BGP finds the shortest path to route traffic from one IP address to another efficiently. BGP creates its TCP session on port 179.

Attackers perform BGP enumeration on the target using tools such as Nmap and BGP Toolkit to discover the IPv4 prefixes indicated by the AS number and the routing path followed by the target. Attackers use this information to launch various attacks against the target, such as man-in-the-middle attacks, BGP hijacking attacks, and DoS attacks.

As shown in the screenshot, attackers use the following Nmap command to enumerate BGP running on the target system:

```
# nmap -p 179 <target IP>
```

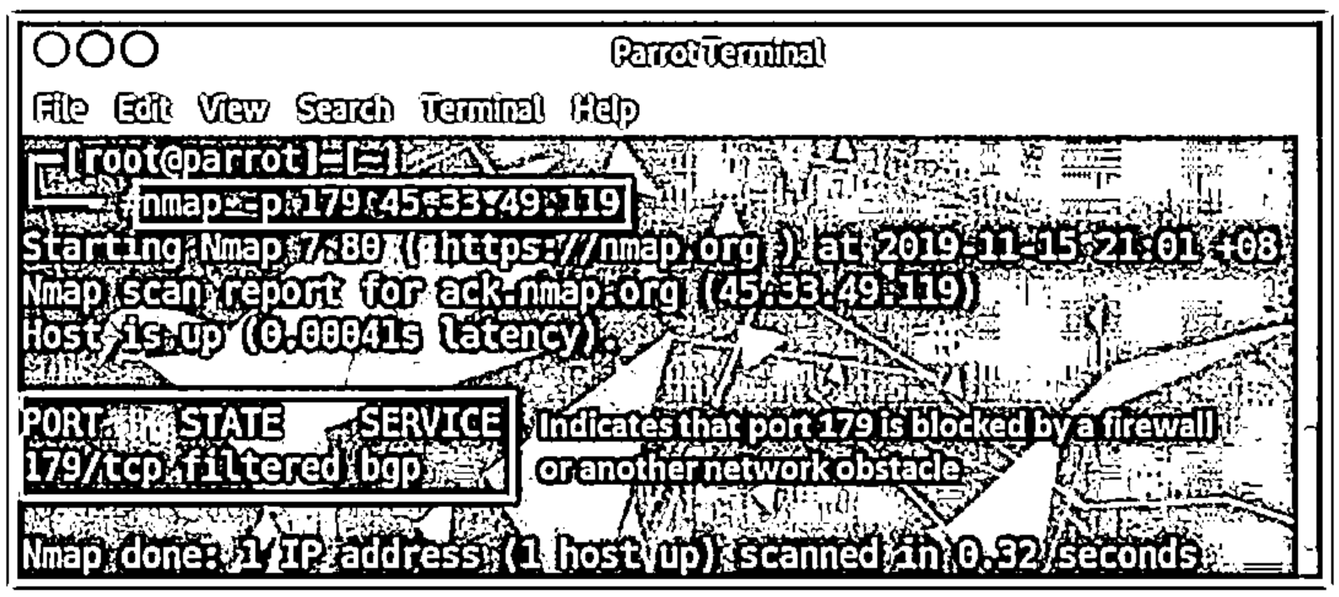


Figure 4.45: Screenshot of Nmap displaying a BGP enumeration result

As shown in the screenshot, attackers use BGP Toolkit to perform BGP enumeration on the target domain. This online tool can be used to search for the target domain and obtain details such as DNS information, website information, IP information, AS information, and whois information. Based on the identified ASs, attackers can further enumerate details such as IPv4 prefixes, BGP routing graphs, and IPv4 peers.

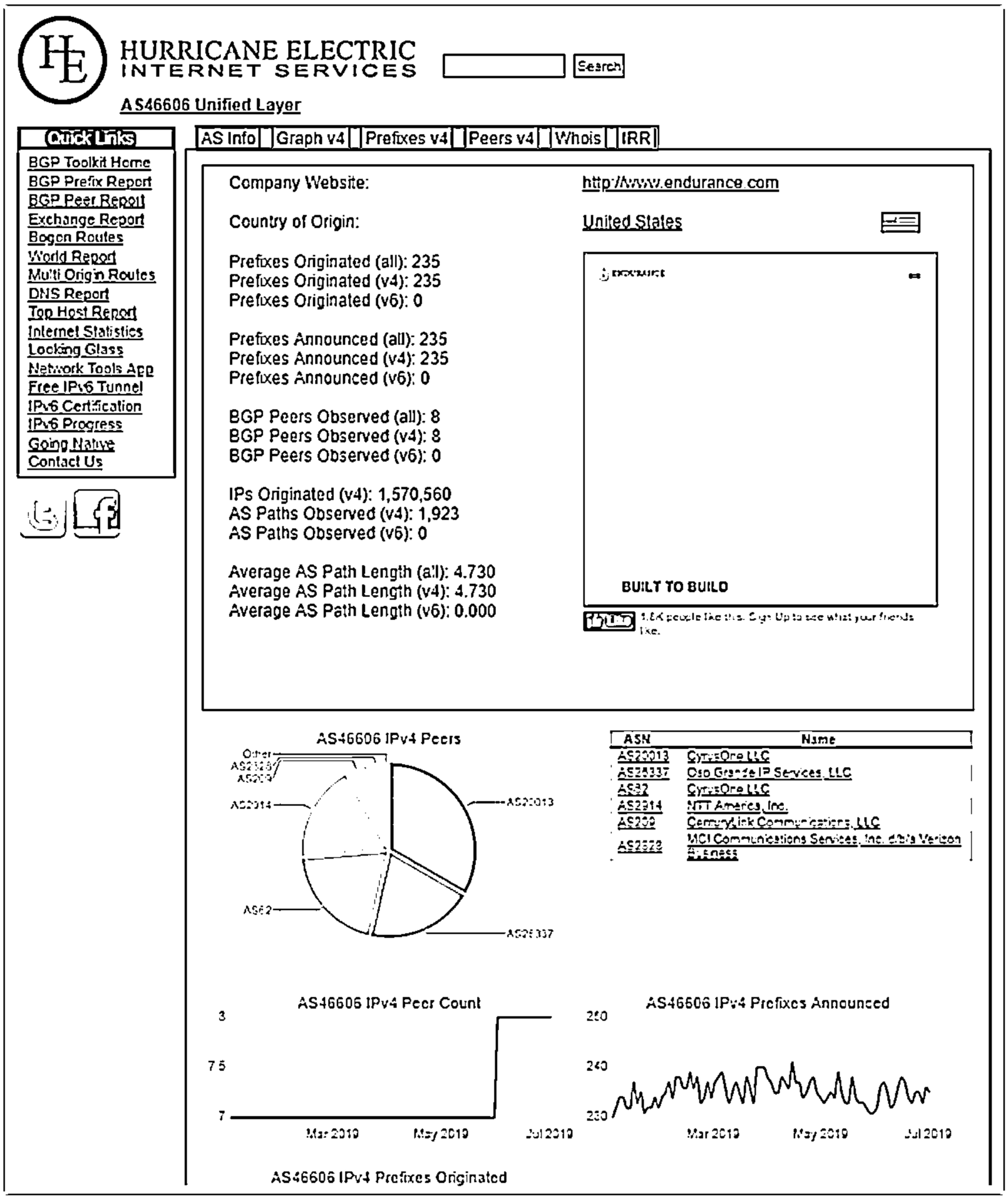


Figure 4.46: Screenshot of BGP Toolkit

Module Flow

1. Enumeration Concepts
2. NetBIOS Enumeration
3. SNMP Enumeration
4. LDAP Enumeration
5. NTP and NFS Enumeration
6. SMTP and DNS Enumeration
7. Other Enumeration Techniques
8. Enumeration Countermeasures

Enumeration Countermeasures

SNMP

- Remove the SNMP agent or turn off the SNMP service
- If shutting off SNMP is not an option, then change the default community string names
- Upgrade to SNMP3, which encrypts passwords and messages
- Implement the Group Policy security option called "Additional restrictions for anonymous connections"
- Ensure that the access to null session pipes, null session shares, and IPSec filtering is restricted
- Do not misconfigure SNMP service with read-write authorization

DNS

- Disable the DNS zone transfers to the untrusted hosts
- Ensure that the private hosts and their IP addresses are not published in DNS zone files of public DNS servers
- Use premium DNS registration services that hide sensitive information, such as host information (HINFO) from the public
- Use standard network admin contacts for DNS registrations to avoid social engineering attacks

Enumeration Countermeasures (Cont'd)

SMTP

Configure SMTP servers to

- Ignore email messages to unknown recipients
- Exclude sensitive mail server and local host information in mail responses
- Disable open relay feature
- Limit the number of accepted connections from a source to prevent brute-force attacks

LDAP

- By default, LDAP traffic is transmitted unsecured; use SSL or STARTTLS technology to encrypt the traffic
- Select a username different from your email address and enable account lockout
- Use NTLM or any basic authentication mechanism to limit access to legitimate users only

SMB

- Disable SMB protocol on Web and DNS Servers
- Disable SMB protocol on Internet facing servers
- Disable ports TCP 139 and TCP 445 used by the SMB protocol
- Restrict anonymous access through RestrictNullSessAccess parameter from the Windows Registry

Enumeration Countermeasures (Cont'd)

NFS

- Implement proper permissions (read/write must be restricted to specific users) on exported file systems
- Implement firewall rules to block NFS port 2049
- Ensure proper configuration of files, such as `/etc/smb.conf`, `/etc/exports` and `etc/hosts.allow`, to protect the data stored in servers
- Log requests to access system files on the NFS server
- Keep the `root_squash` option in `/etc/exports` file turned ON, so that no requests made as root on the client are trusted

FTP

- Implement secure FTP (SFTP, which uses SSH) or FTP secure (FTPS, which uses SSL) to encrypt the FTP traffic over the network
- Implement strong passwords or a certification-based authentication policy
- Ensure that unrestricted uploading of files on the FTP server is not allowed
- Disable anonymous FTP accounts; if not feasible, regularly monitor anonymous FTP accounts
- Restrict access by IP or domain name to the FTP server

Enumeration Countermeasures

Thus far, we have described enumeration techniques and tools used to extract valuable information from targets. Next, we discuss countermeasures that can prevent attackers from enumerating sensitive information from a network or host. This section focuses on methods to avoid information leakage through SNMP, DNS, SMTP, LDAP, SMB, NFS, and FTP enumeration.

SNMP Enumeration Countermeasures

- Remove the SNMP agent or turn off the SNMP service.
- If turning off SNMP is not an option, then change the default community string names.
- Upgrade to SNMP3, which encrypts passwords and messages.
- Implement the Group Policy security option called "Additional restrictions for anonymous connections."
- Ensure that the access to null session pipes, null session shares, and IPsec filtering is restricted.
- Block access to TCP/UDP port 161.
- Do not install the management and monitoring Windows component unless required.
- Encrypt or authenticate using IPsec.
- Do not misconfigure the SNMP service with read-write authorization.

DNS Enumeration Countermeasures

- Disable DNS zone transfers to untrusted hosts.
- Ensure that the private hosts and their IP addresses are not published in the DNS zone files of the public DNS server.
- Use premium DNS registration services that hide sensitive information such as host information (HINFO) from the public.
- Use standard network admin contacts for DNS registrations to avoid social engineering attacks.
- Prune DNS zone files to prevent revealing unnecessary information.

SMTP Enumeration Countermeasures

SMTP servers should be configured in the following manner.

- Ignore email messages to unknown recipients.
- Exclude sensitive information on mail servers and local hosts in mail responses.
- Disable the open relay feature.
- Limit the number of accepted connections from a source to prevent brute-force attacks.
- Disable EXPN, VRFY, and RCPT TO commands or restrict them to authentic users.
- Ignore emails to unknown recipients by configuring SMTP servers.

LDAP Enumeration Countermeasures

- By default, LDAP traffic is transmitted unsecured; therefore, use Secure Sockets Layer (SSL) or STARTTLS technology to encrypt the traffic.
- Select a username different from the email address and enable account lockout.

- Restrict access to Active Directory by using software such as Citrix.
- Use NTLM or any basic authentication mechanism to limit access to legitimate users.

SMB Enumeration Countermeasures

Common sharing services or other unused services may provide doorways for attackers to break into a network's security. A network running SMB is at a high risk of enumeration. Since web and DNS servers do not require this protocol, it is advisable to disable it on them. The SMB protocol can be disabled by disabling the properties **Client for Microsoft Networks** and **File and Printer Sharing for Microsoft Networks** in **Network and Dial-up Connections**. On servers that are accessible from the Internet, also known as bastion hosts, SMB can be disabled by disabling the same two properties of the **TCP/IP properties** dialog box. Another method of disabling the SMB protocol on bastion hosts, without explicitly disabling it, is by blocking the ports used by the SMB service. These are TCP ports 139 and 445.

Because disabling SMB services is not always a feasible option, other countermeasures against SMB enumeration may be required. Windows Registry can be configured to limit anonymous access from the Internet to a specified set of files. These files and folders are specified in the settings **Network access: Named pipes that can be accessed anonymously** and **Network access: Shares that can be accessed anonymously**. This configuration involves adding the RestrictNullSessAccess parameter to the registry key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

The RestrictNullSessAccess parameter takes binary values, with 1 denoting enabled and 0 denoting disabled. Setting this parameter to 1 or enabled restricts the access of anonymous users to the files specified in the **Network access** settings.

The following are additional countermeasures for defending against SMB enumeration.

- Ensure that Windows Firewall or similar endpoint protection systems are enabled on the system.
- Install the latest security patches for Windows and third-party software.
- Implement a proper authentication mechanism with a strong password policy.
- Implement strong permissions to keep the stored information safe.
- Perform a regular audit of system logs.
- Perform active system monitoring to monitor the systems for any malicious incident.

NFS Enumeration Countermeasures

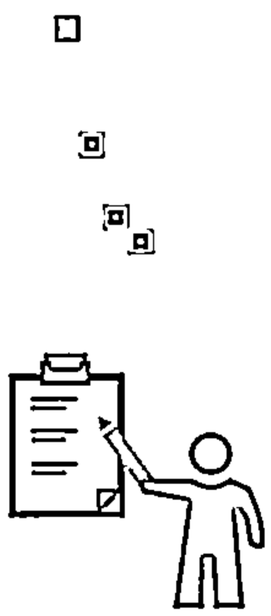
- Implement proper permissions (read/write must be restricted to specific users) in exported file systems.
- Implement firewall rules to block NFS port 2049.
- Ensure the proper configuration of files such as `/etc/smb.conf`, `/etc/exports`, and `etc/hosts.allow` to protect the data stored in the server.

- Log the requests to access the system files on the NFS server.
- Keep the `root_squash` option in `/etc/exports` file turned **ON** so that no requests made as root on the client are trusted.
- Implement NFS tunneling through SSH to encrypt the NFS traffic over the network.

FTP Enumeration Countermeasures

- Implement secure FTP (SFTP, which uses SSH) or FTP secure (FTPS, which uses SSL) to encrypt the FTP traffic over the network.
- Implement strong passwords or a certification-based authentication policy.
- Ensure that the unrestricted uploading of files on the FTP server is not allowed.
- Disable anonymous FTP accounts. If this is not possible, monitor anonymous FTP accounts regularly.
- Restrict access by IP or domain name to the FTP server.
- Configure access controls on authenticated FTP accounts with the help of access control lists (ACLs).
- Restrict login attempts and time.
- Configure filtering rules for the FTP services.
- Use SSL/FTPS for authenticated FTP accounts.

Module Summary



- In this module, we have discussed the following:
  - Enumeration concepts along with techniques, services, and ports used for enumeration
  - How attackers perform enumeration using different techniques (NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration) to gather more information about a target
  - How organizations can defend against enumeration activities
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen testers, perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems

Module Summary

In this module, we discussed the enumeration concepts along with the techniques, services, and ports used for enumeration. We have also discussed how attackers perform different enumeration techniques (NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6, and BGP enumeration) to gather information about the target. This module ended with a detailed discussion on the countermeasures that organizations can adopt to defend against enumeration activities.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen testers, perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems.