Module 13: Hacking Web Servers

Lab 1: Footprint the Web Server

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

Overview of Web Server Footprinting

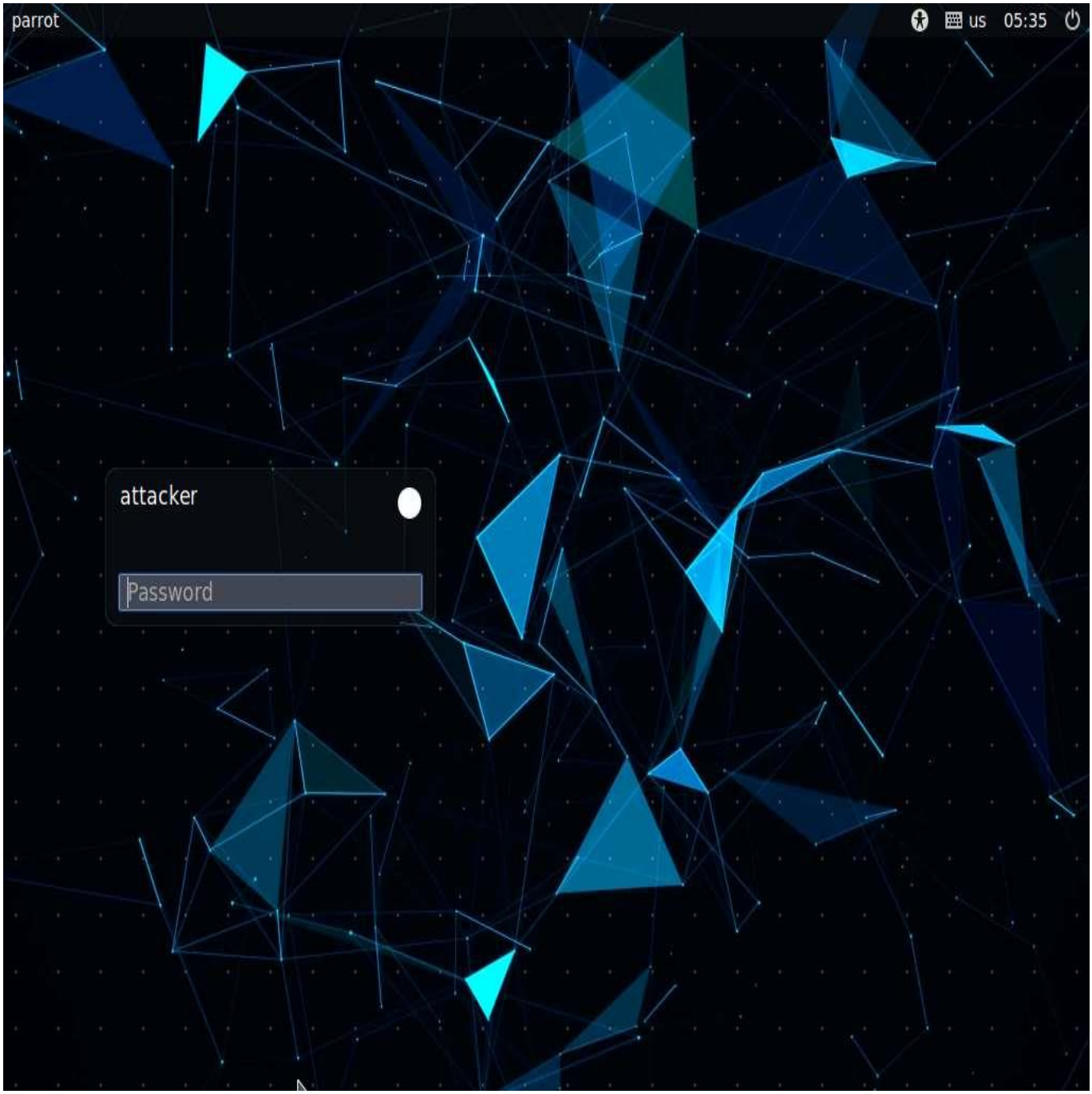
By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications 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.

Task 1: Information Gathering using Ghost Eye

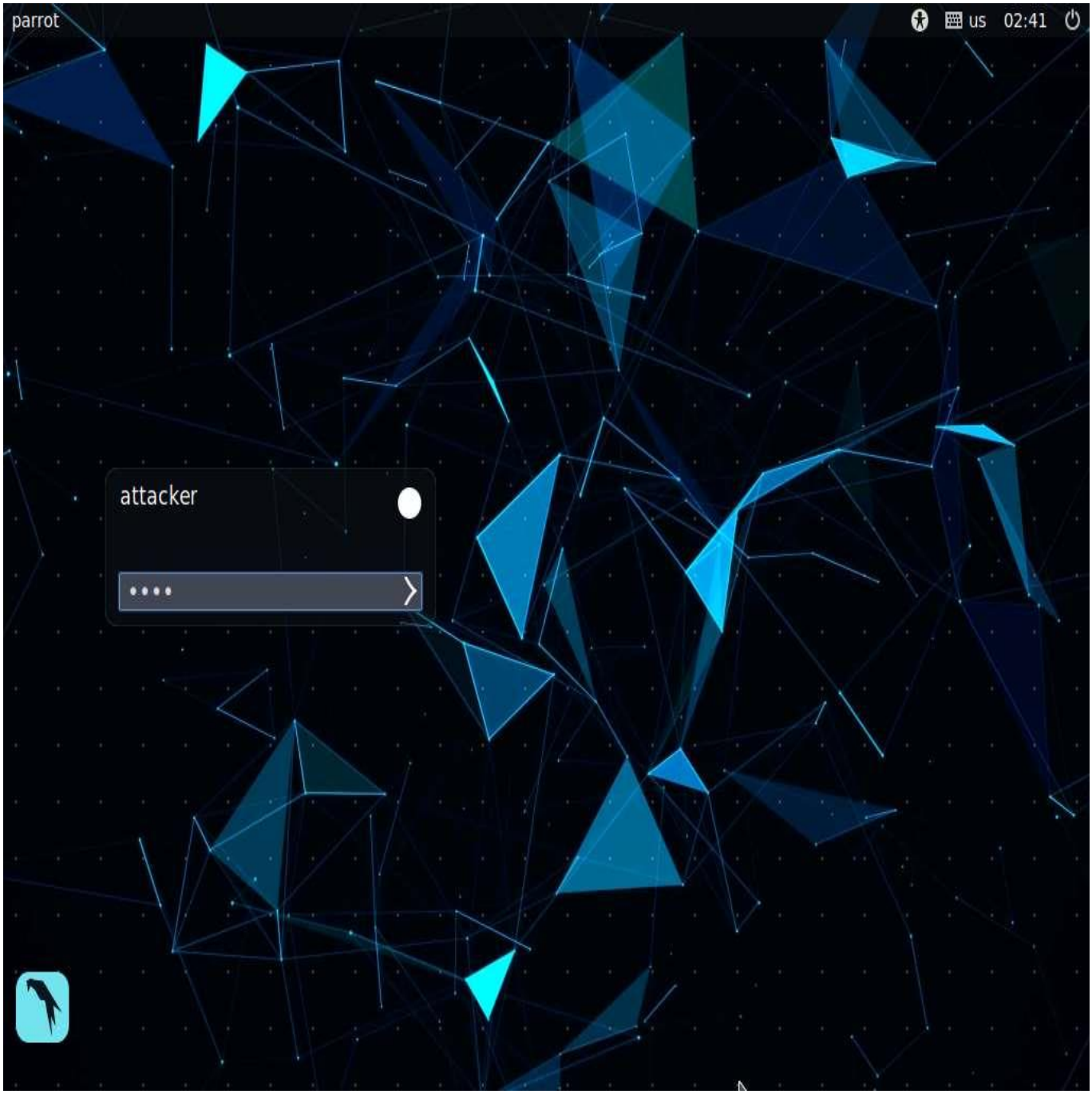
Ghost Eye is an information-gathering tool written in Python 3. To run, Ghost Eye only needs a domain or IP. Ghost Eye can work with any Linux distros if they support Python 3.

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. Click Parrot Security to switch to the **Parrot Security** 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.



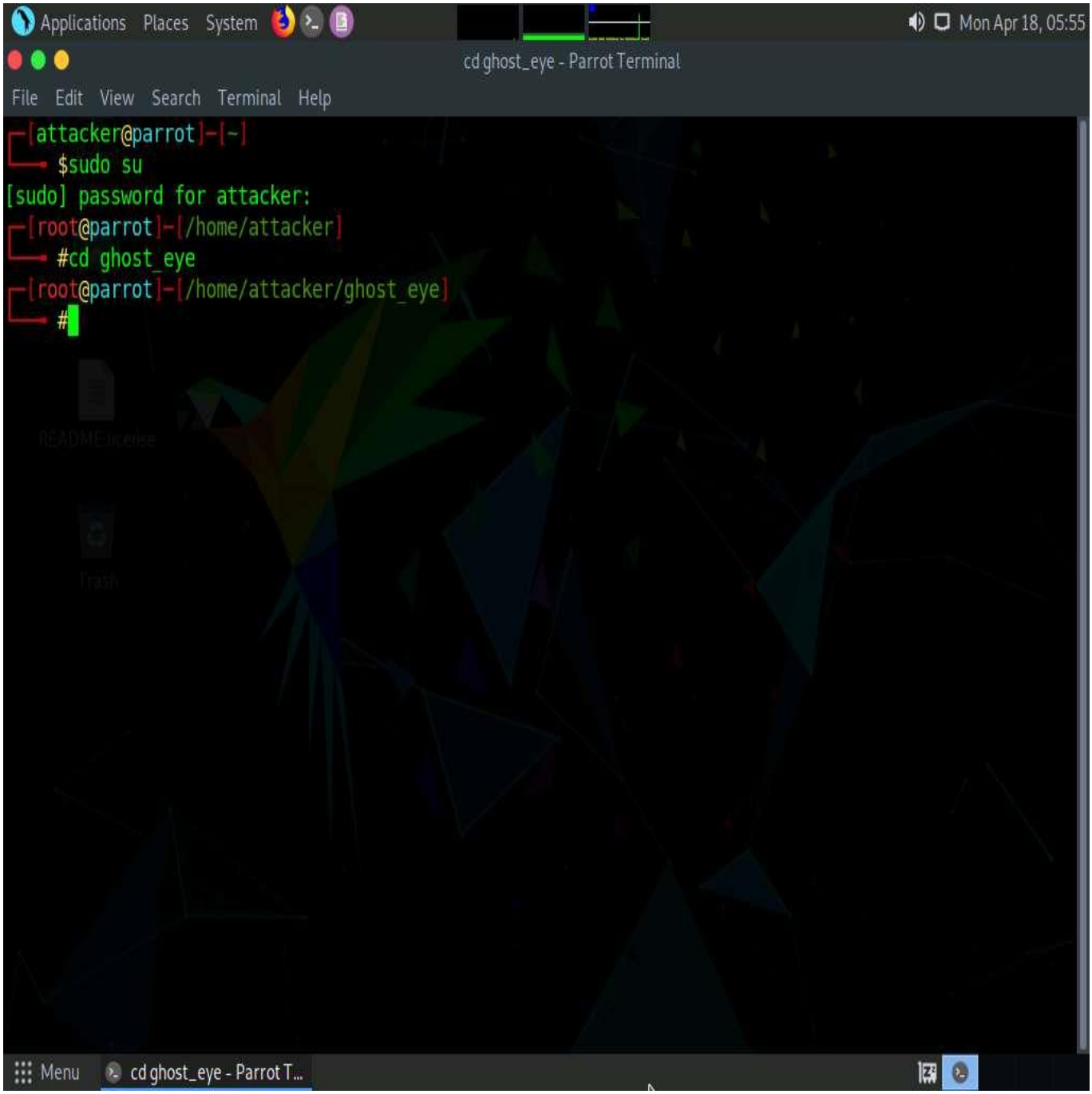
3. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

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

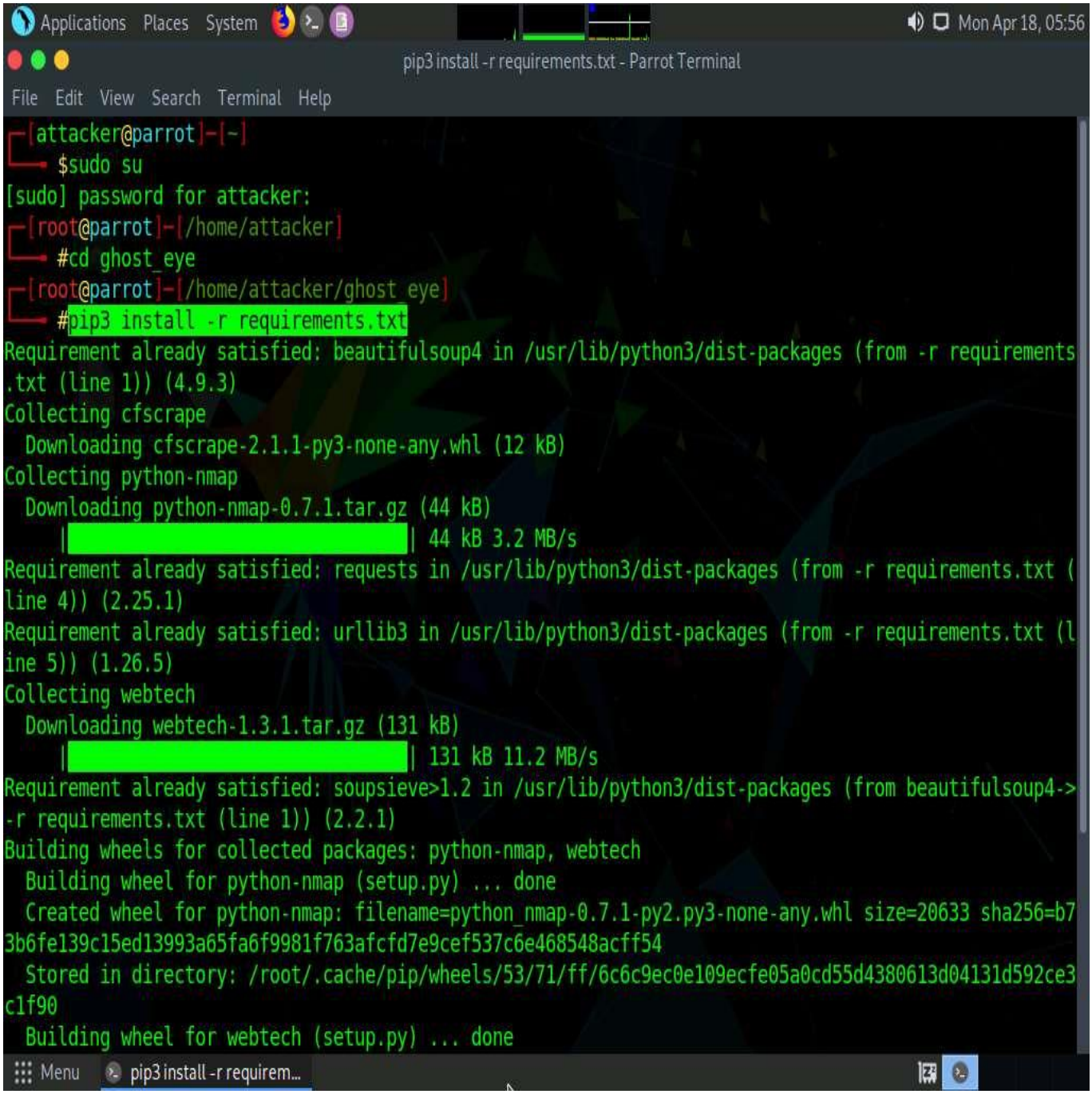
4. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
5. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

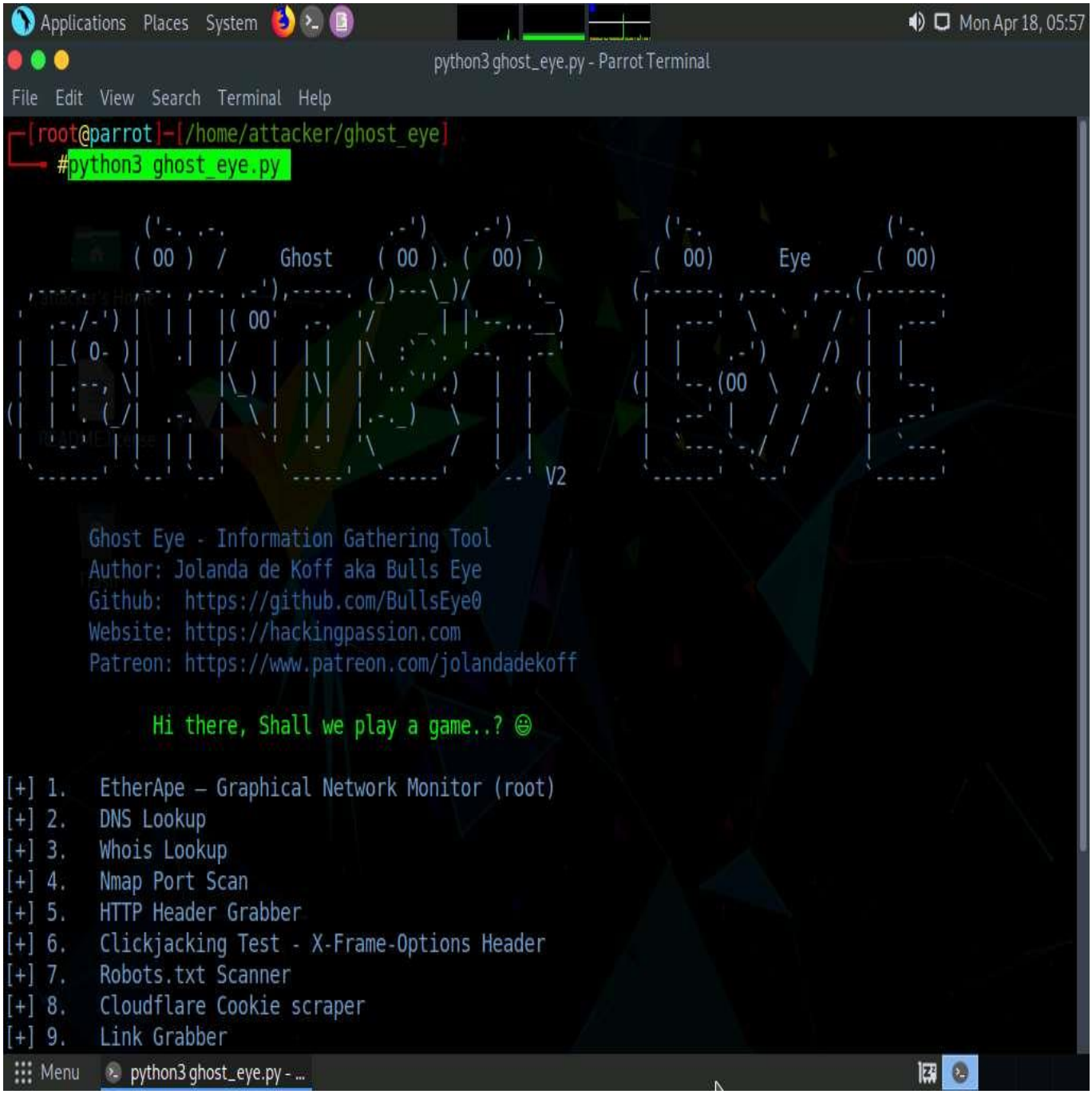
6. Now, navigate to the Ghost Eye directory. Type **cd ghost_eye** and press **Enter**.



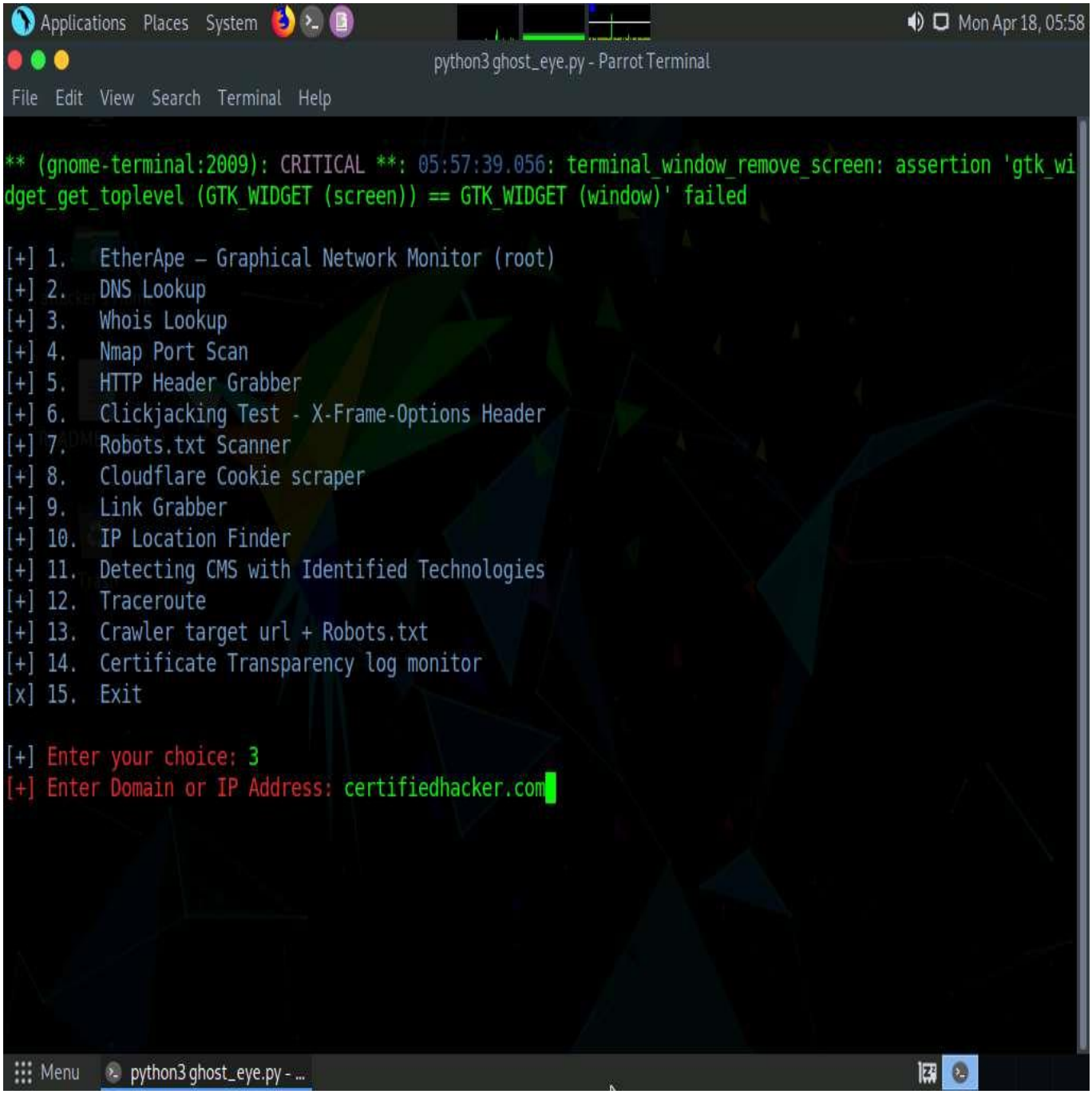
7. ☐ In the terminal window, type **pip3 install -r requirements.txt** and press **Enter**.



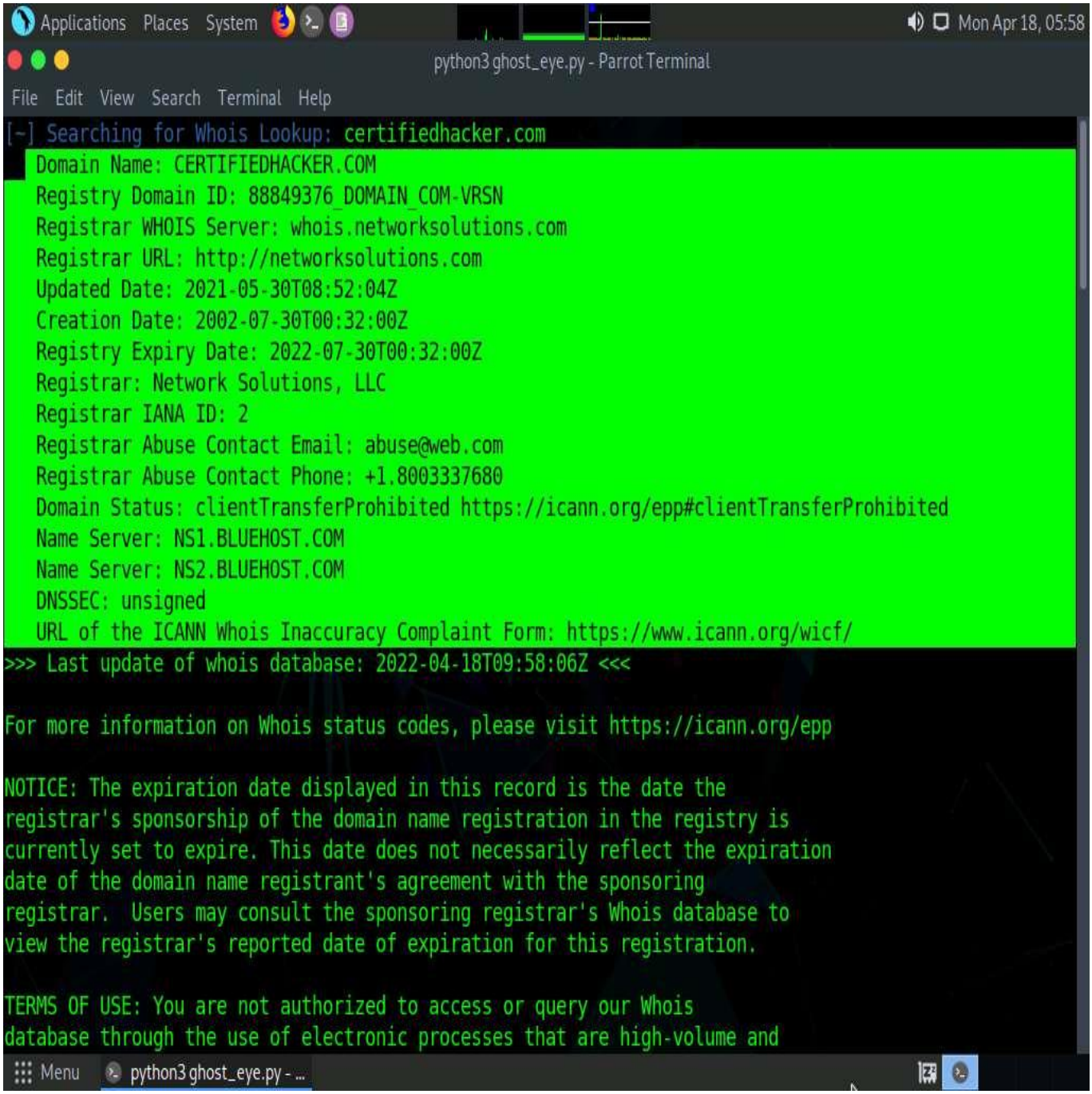
8. To launch Ghost Eye, type **python3 ghost_eye.py** and press **Enter**.



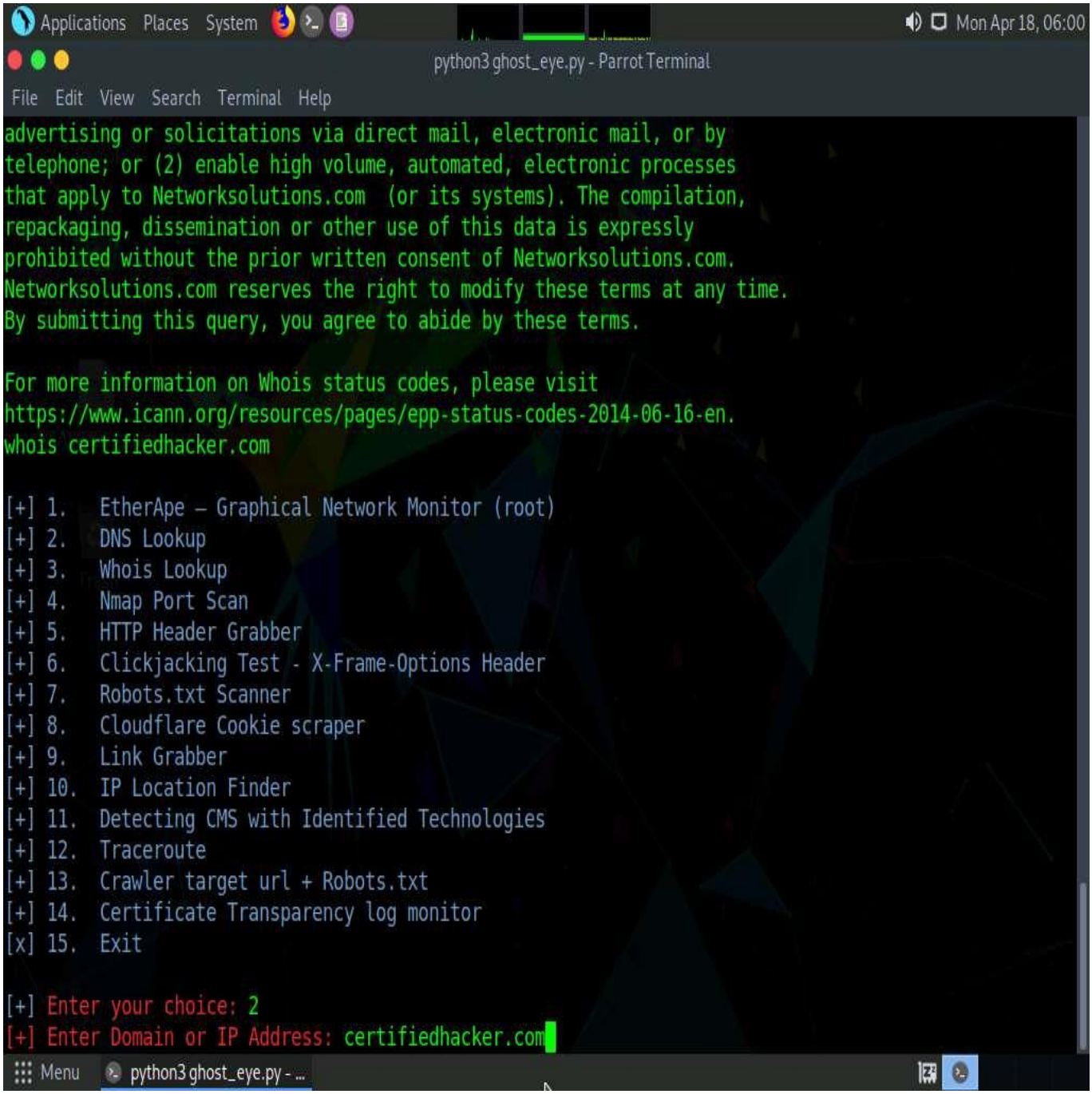
9. ☐ The Ghost Eye - Information Gathering Tool options appear, as shown in the screenshot.
10. ☐ Let us perform a Whois Lookup. Type **3** for the **Enter your choice**: option and press **Enter**.
11. ☐ Type **certifiedhacker.com** in the **Enter Domain or IP Address**: field and press **Enter**



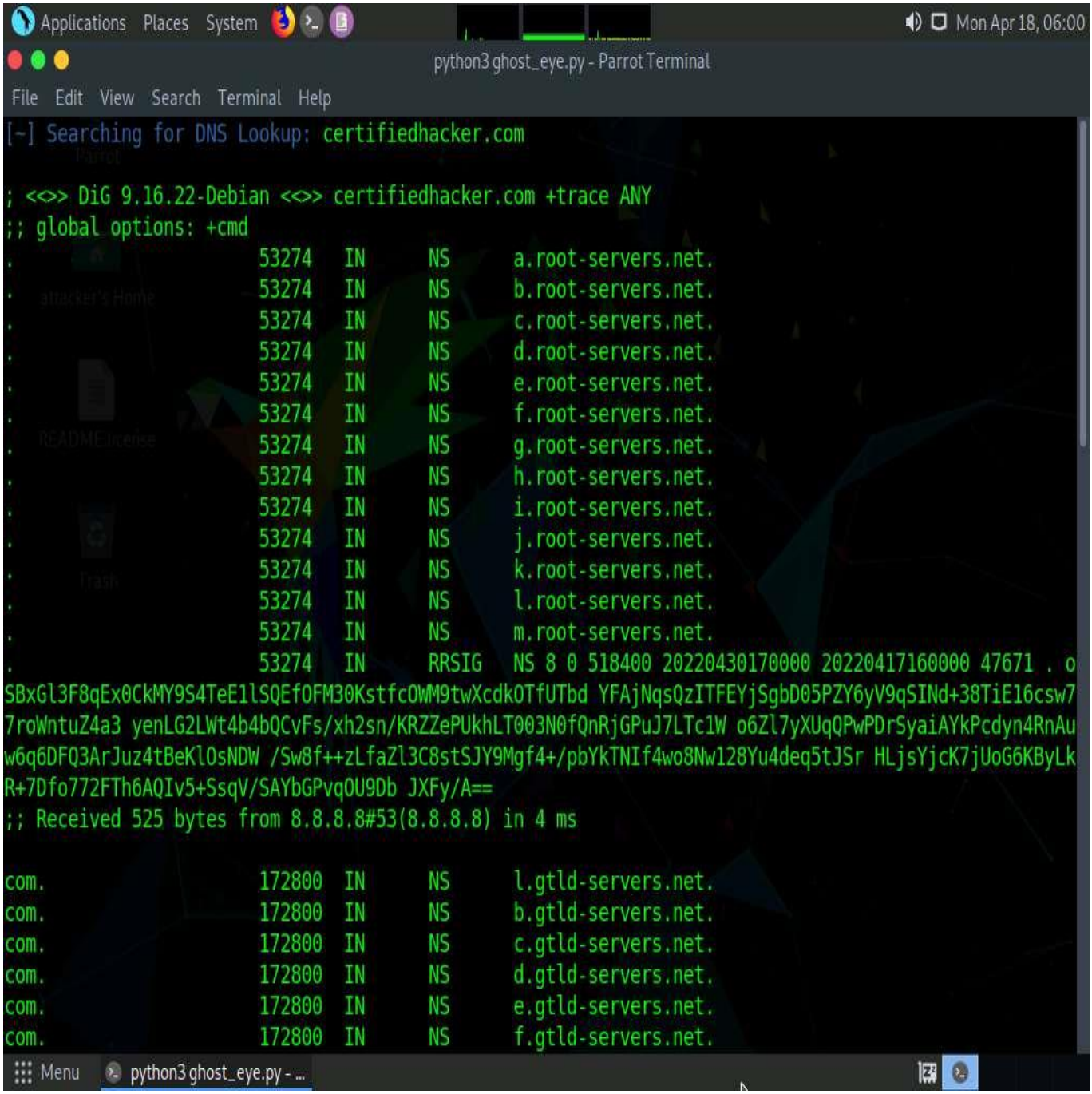
12. Scroll up to see the certifiedhacker.com result. In the result, observe the complete information of the certifiedhacker.com domain such as Domain Name, Registry Domain ID, Registrar WHOIS Server, Registrar URL, and Updated Date.



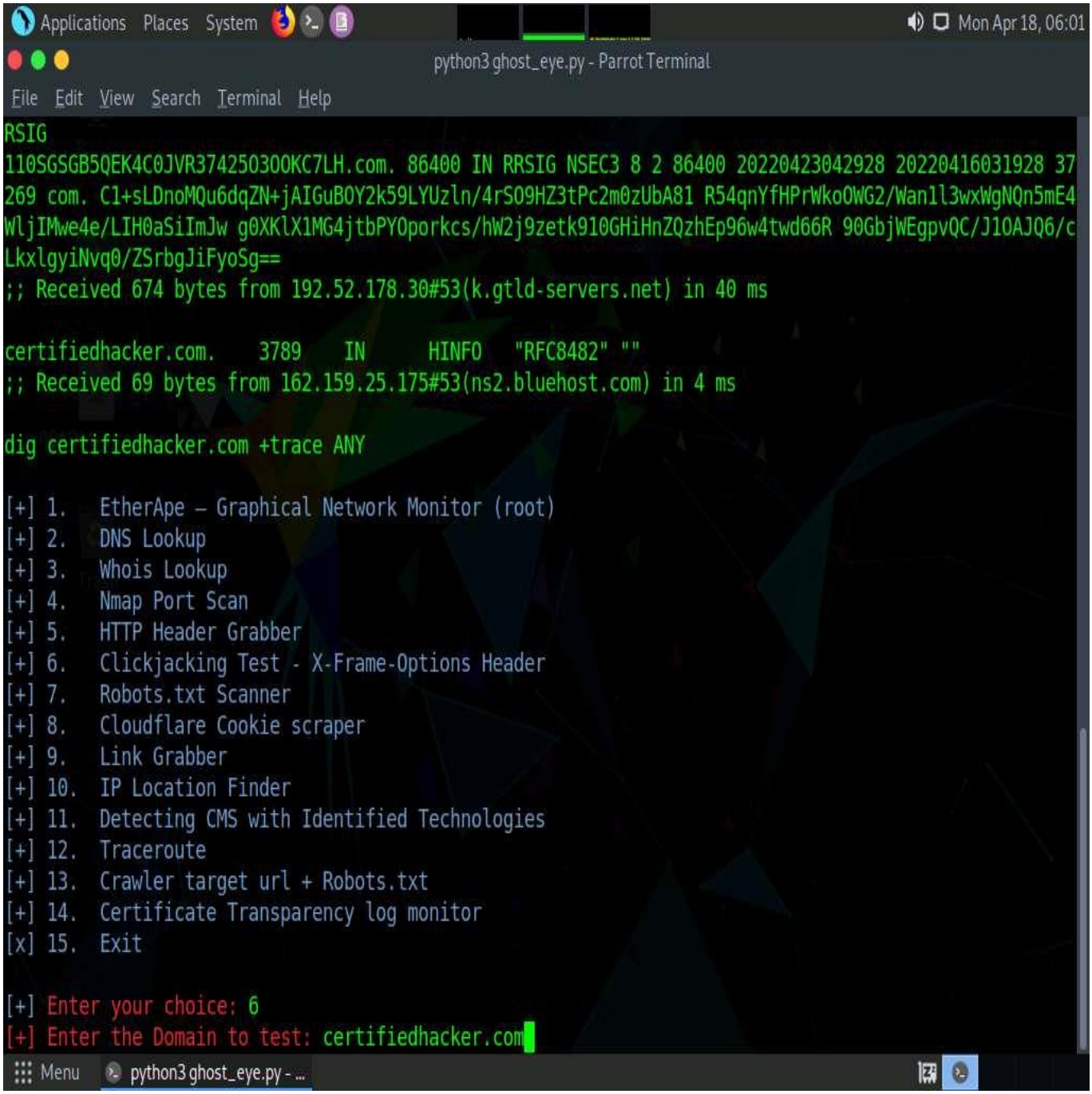
13. Let us perform a **DNS Lookup** on certifiedhacker.com. In the **Enter your choice field**, type **2** and press **Enter** to perform DNS Lookup.
14. The **Enter Domain or IP Address** field appears; type **certifiedhacker.com**, and press **Enter**.



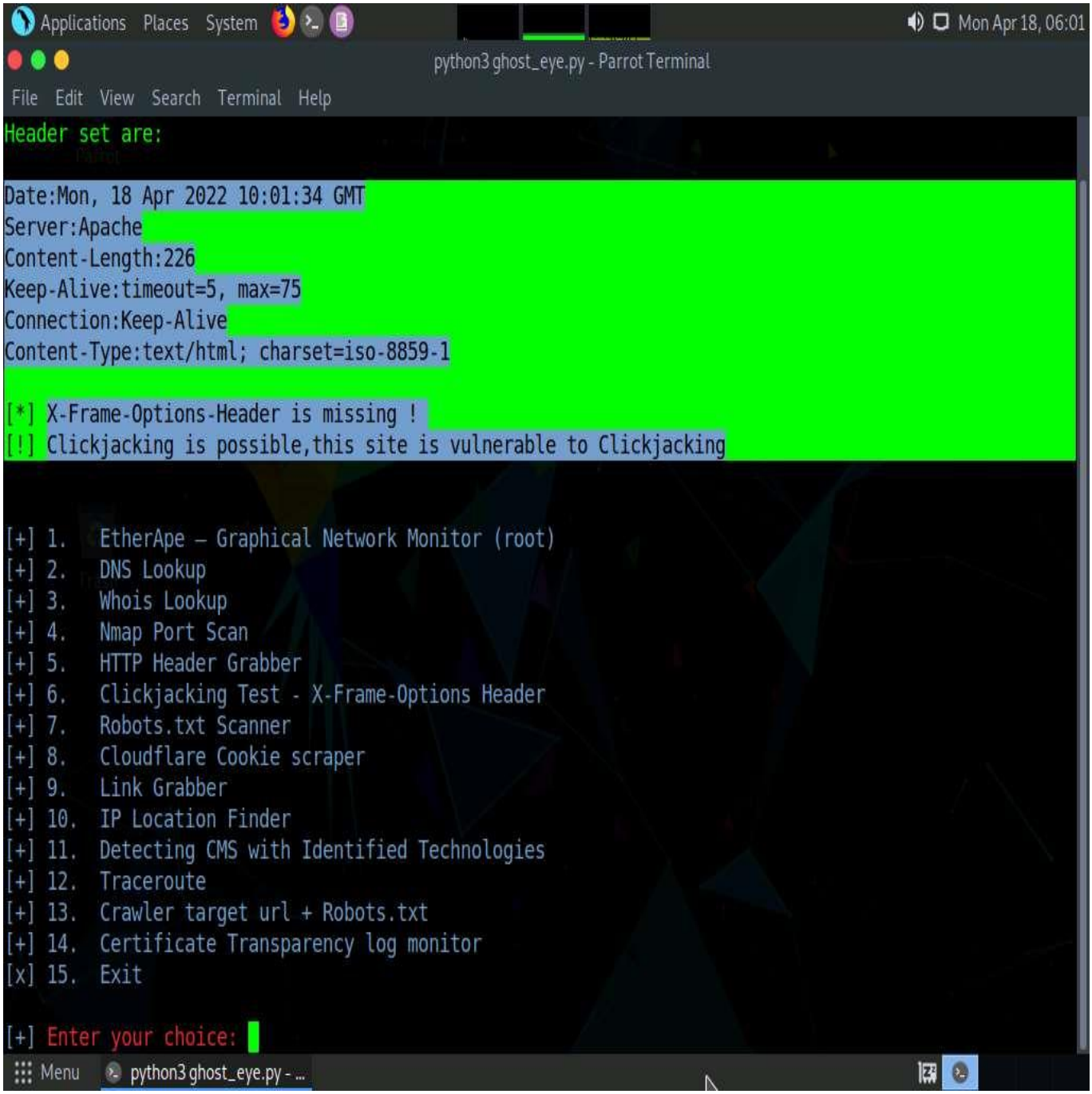
15. ☐ As soon as you hit **Enter**, Ghost Eye starts performing a DNS Lookup on the targeted domain (here, **certifiedhacker.com**).
16. ☐ Scroll up to view the DNS Lookup result.



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.

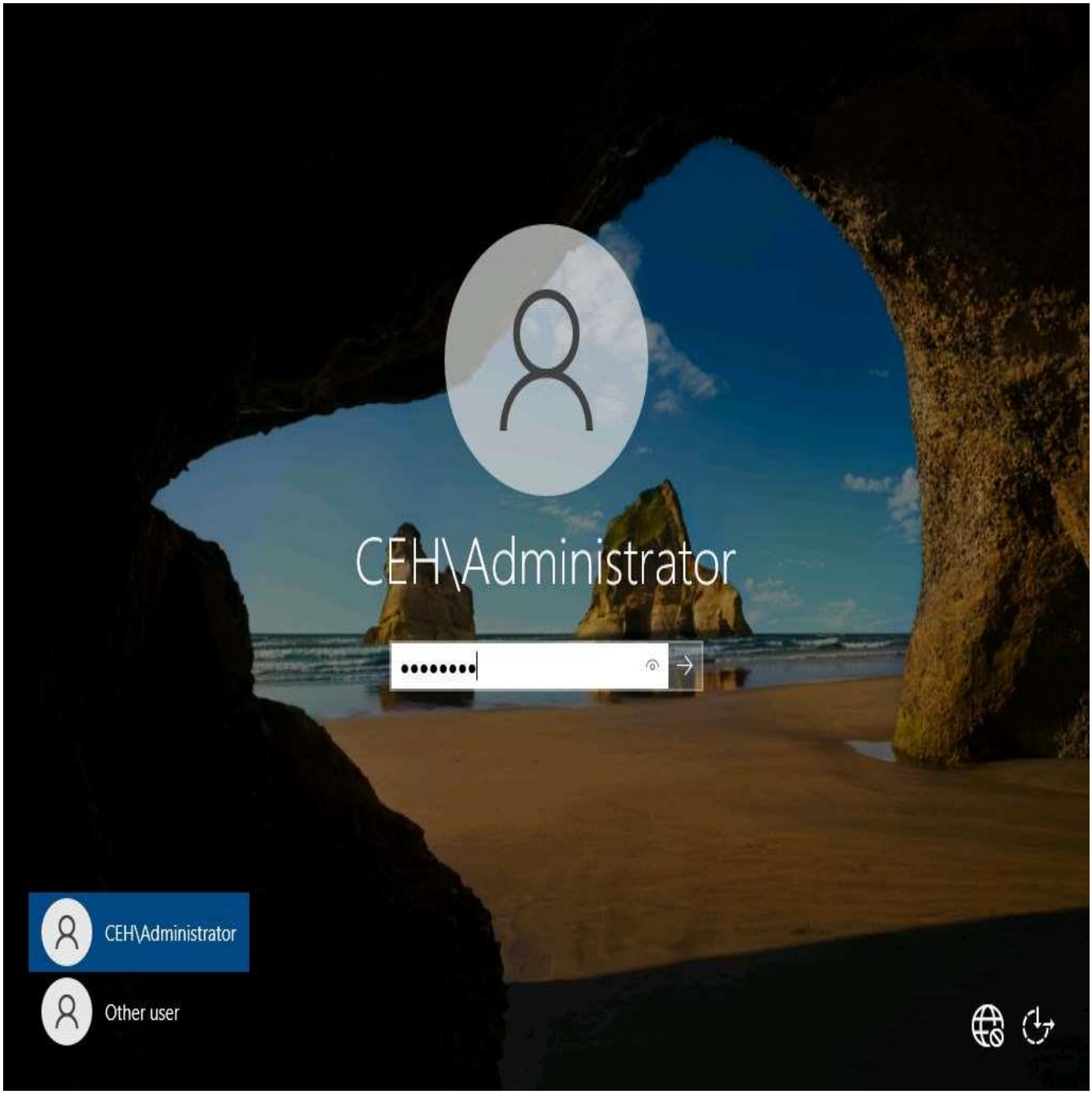
Task 2: Perform Web Server Reconnaissance using Skipfish

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.

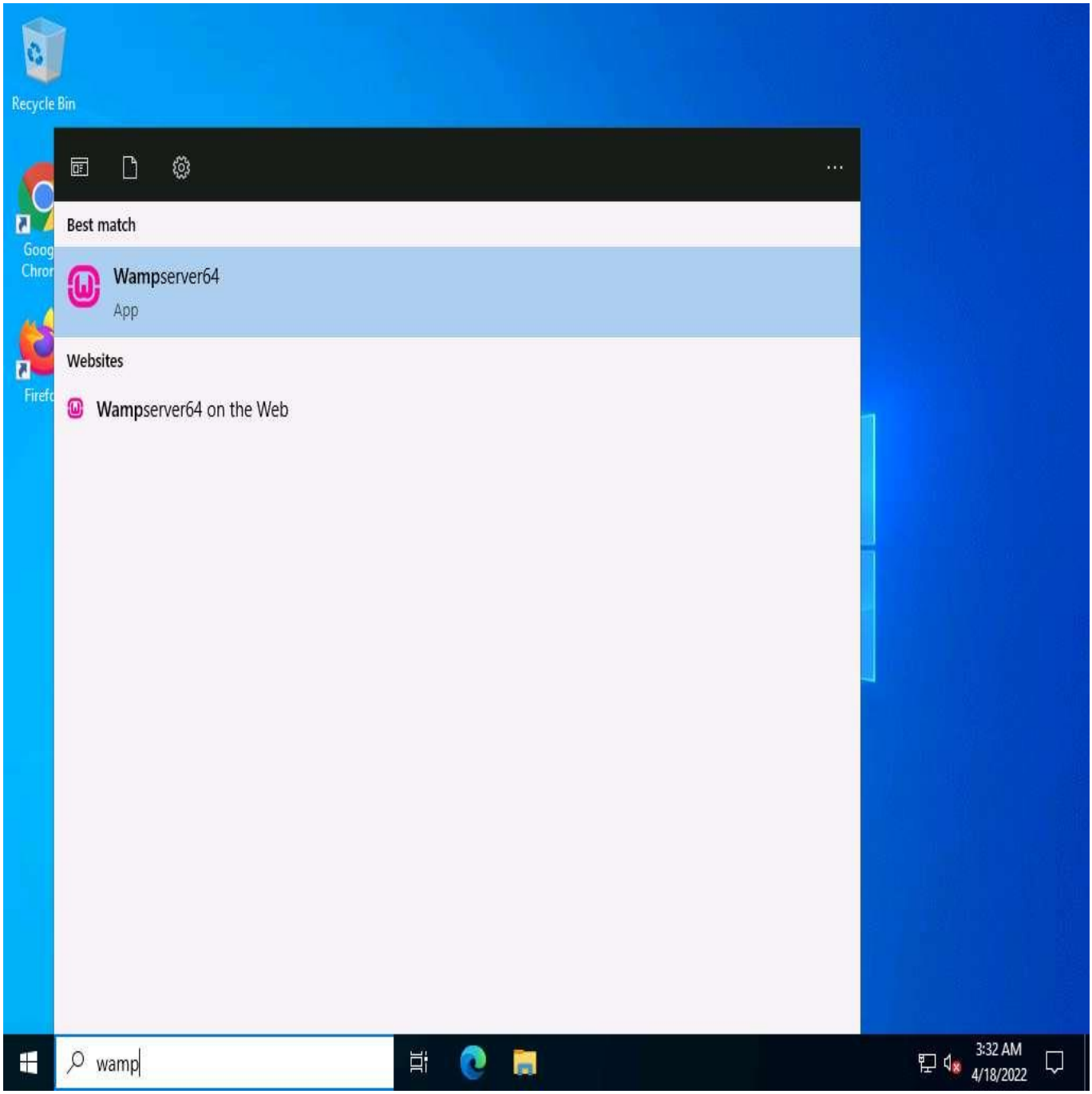
1. Click Windows Server 2022 to switch to the **Windows Server 2022** machine.

2. Click Ctrl+Alt+Delete to activate the machine. By default, **CEH\Administrator** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

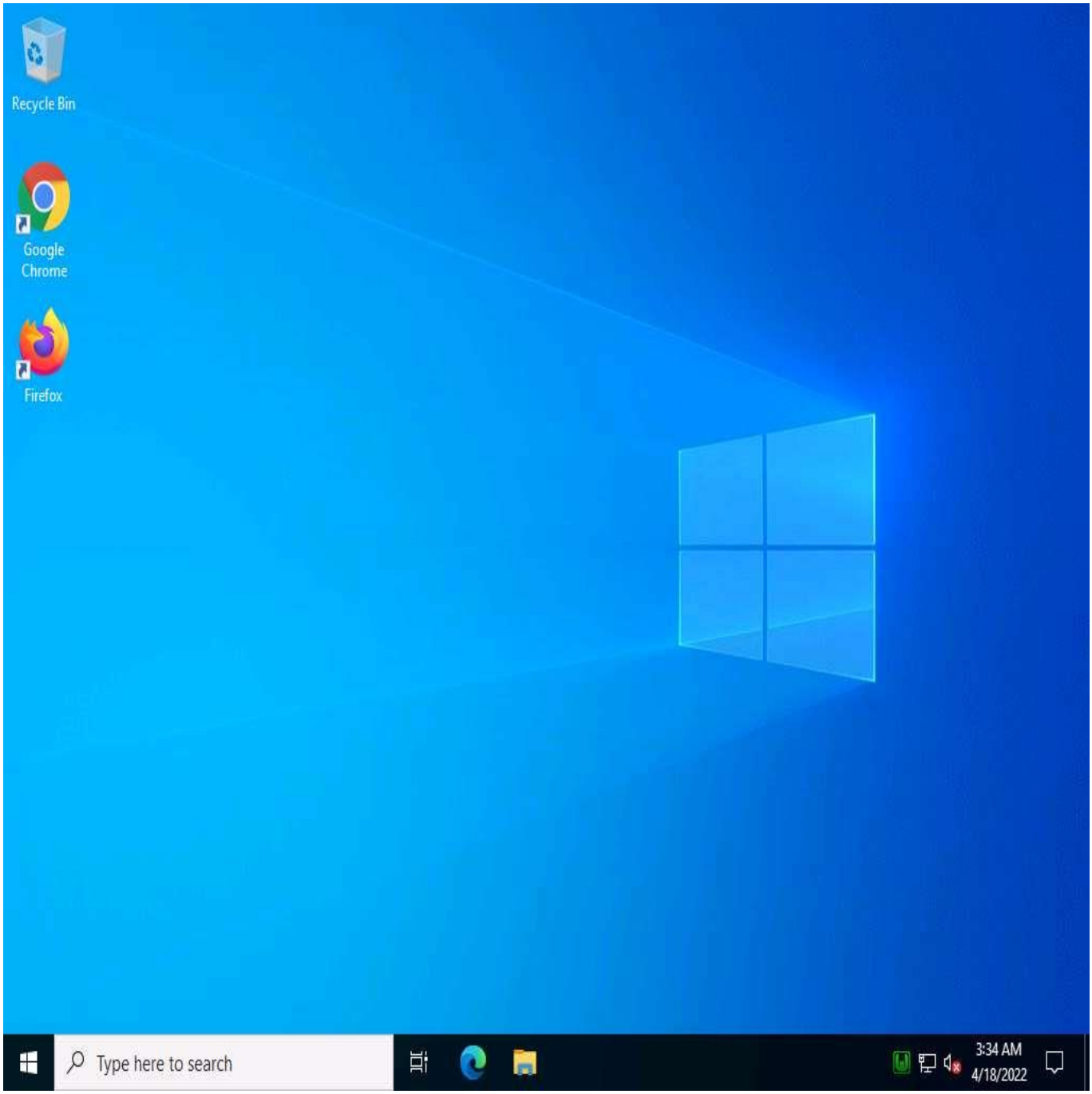
Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2022** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.



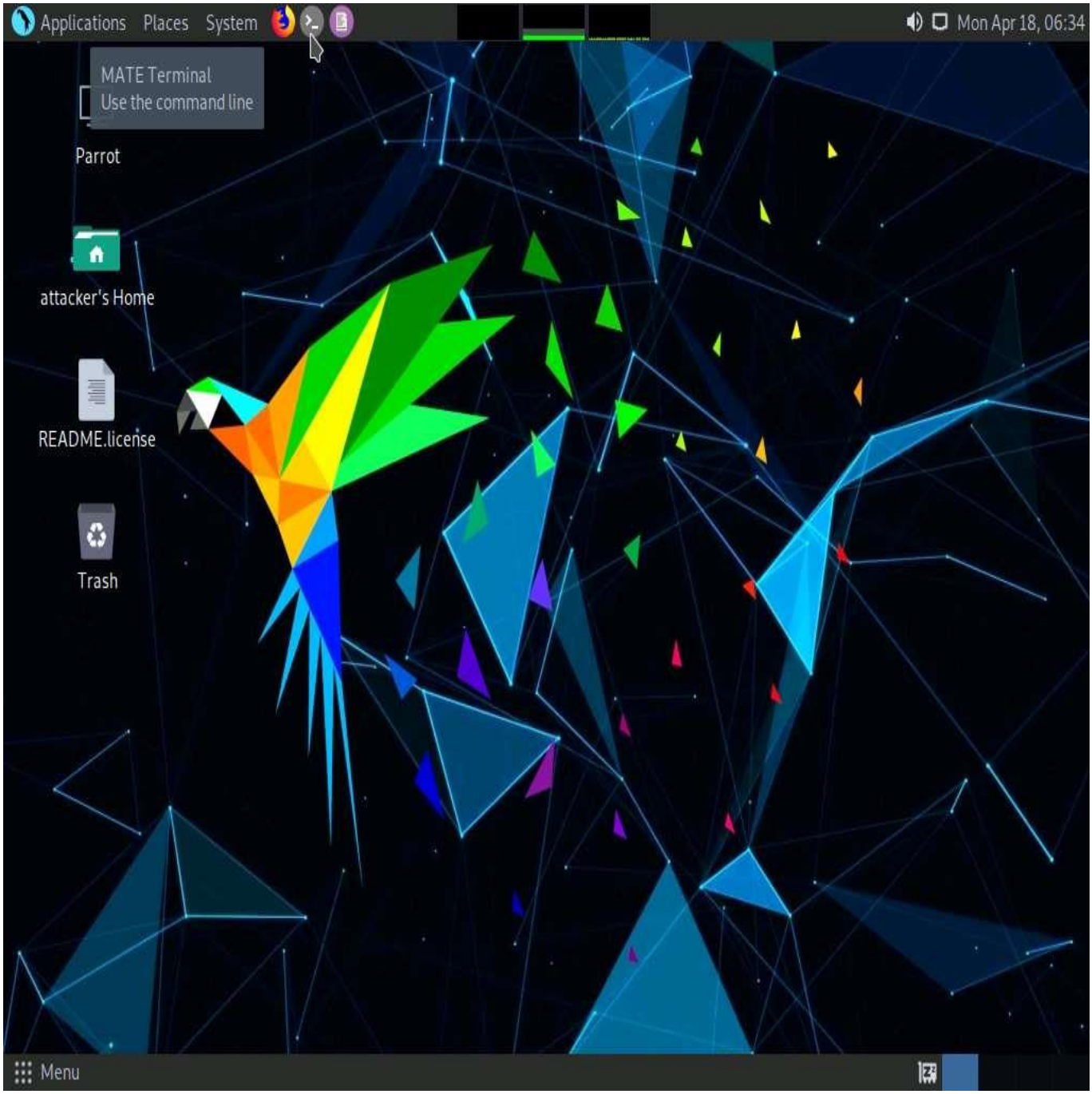
3. Click **Type here to search** field and type **wamp**. **Wamperserver64** appears in the result, press **Enter** to launch it.



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

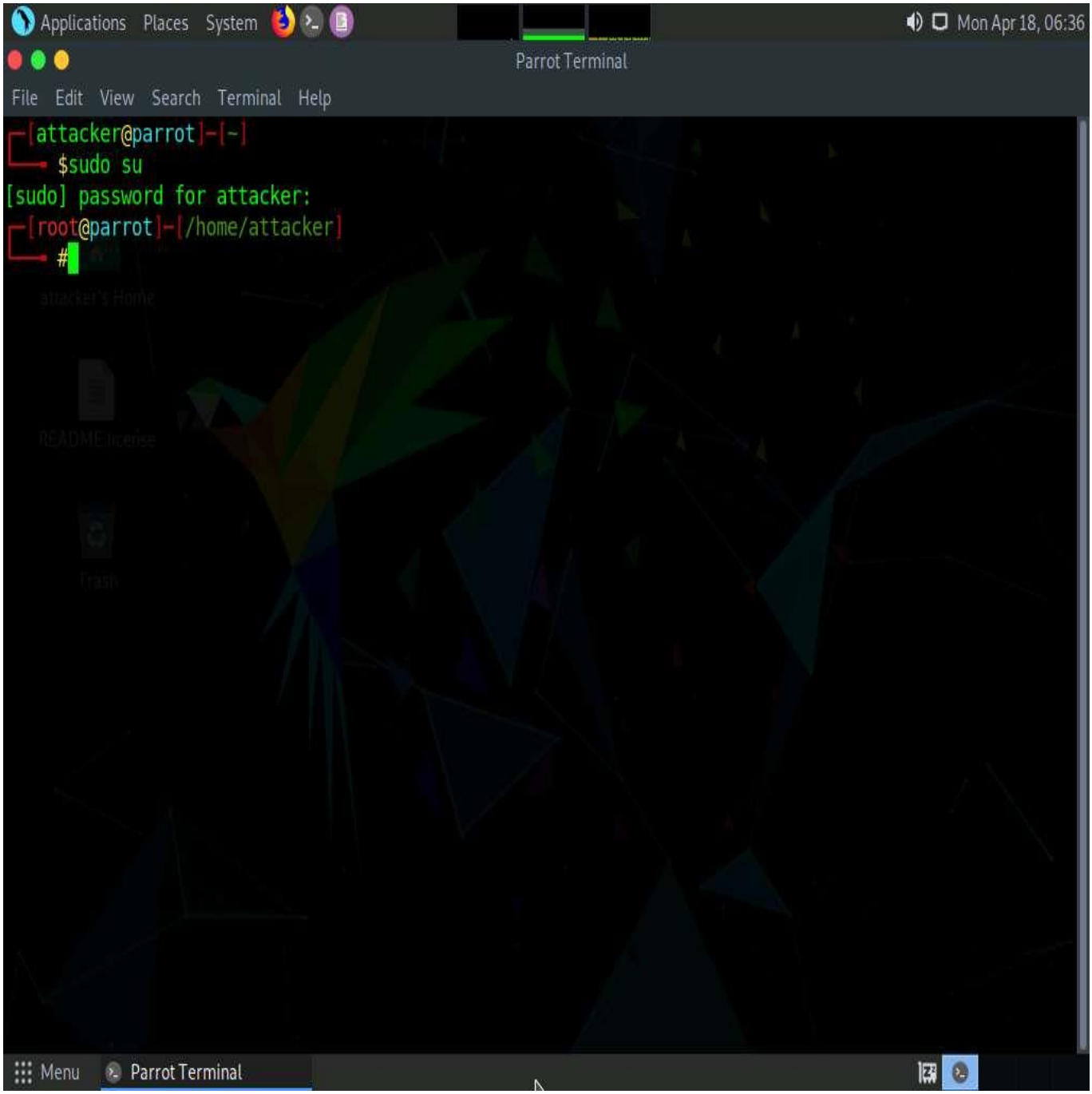


5. ☐ Click Parrot Security to switch to the **Parrot Security** machine.
6. ☐ Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

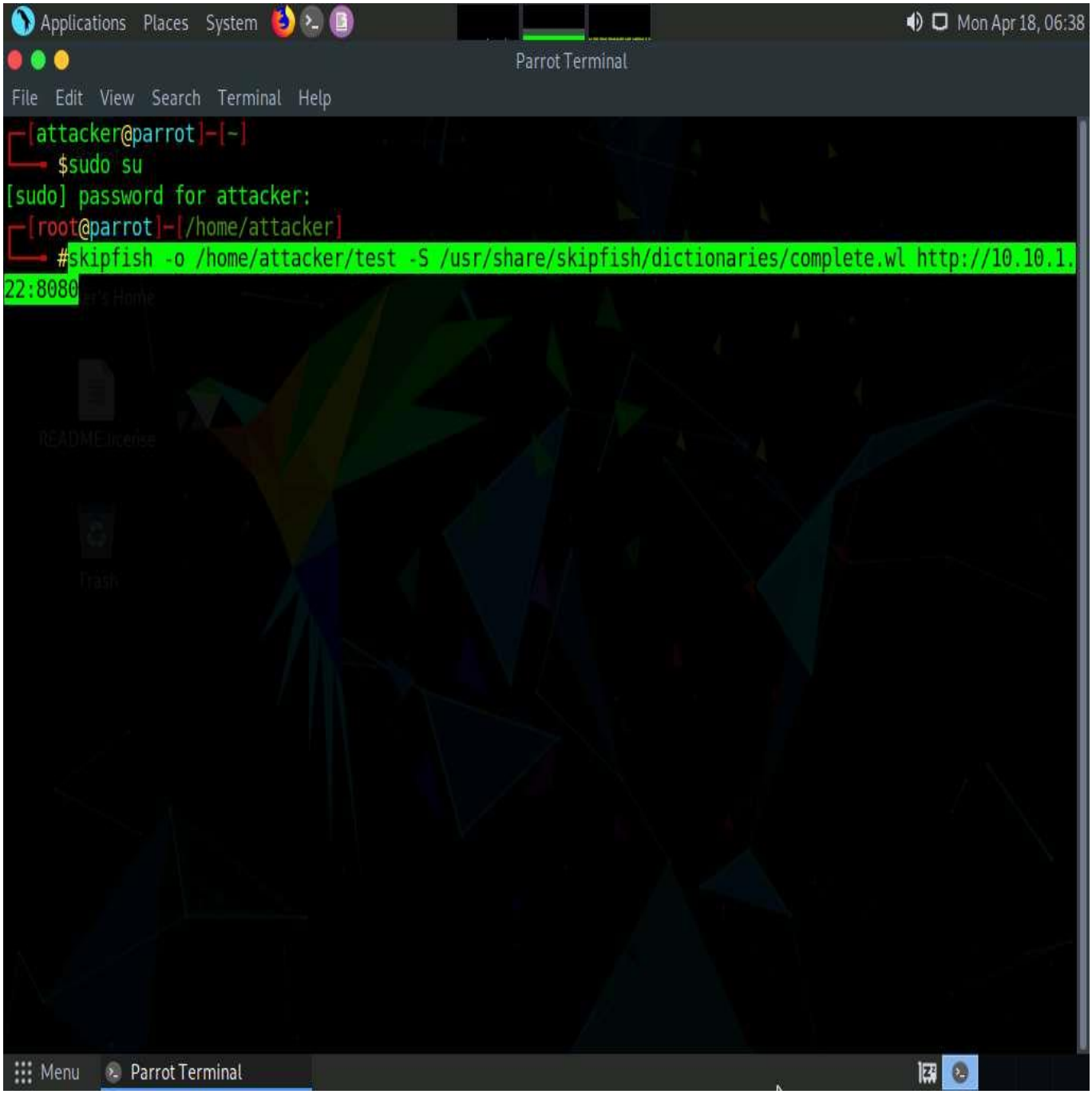


7. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
8. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

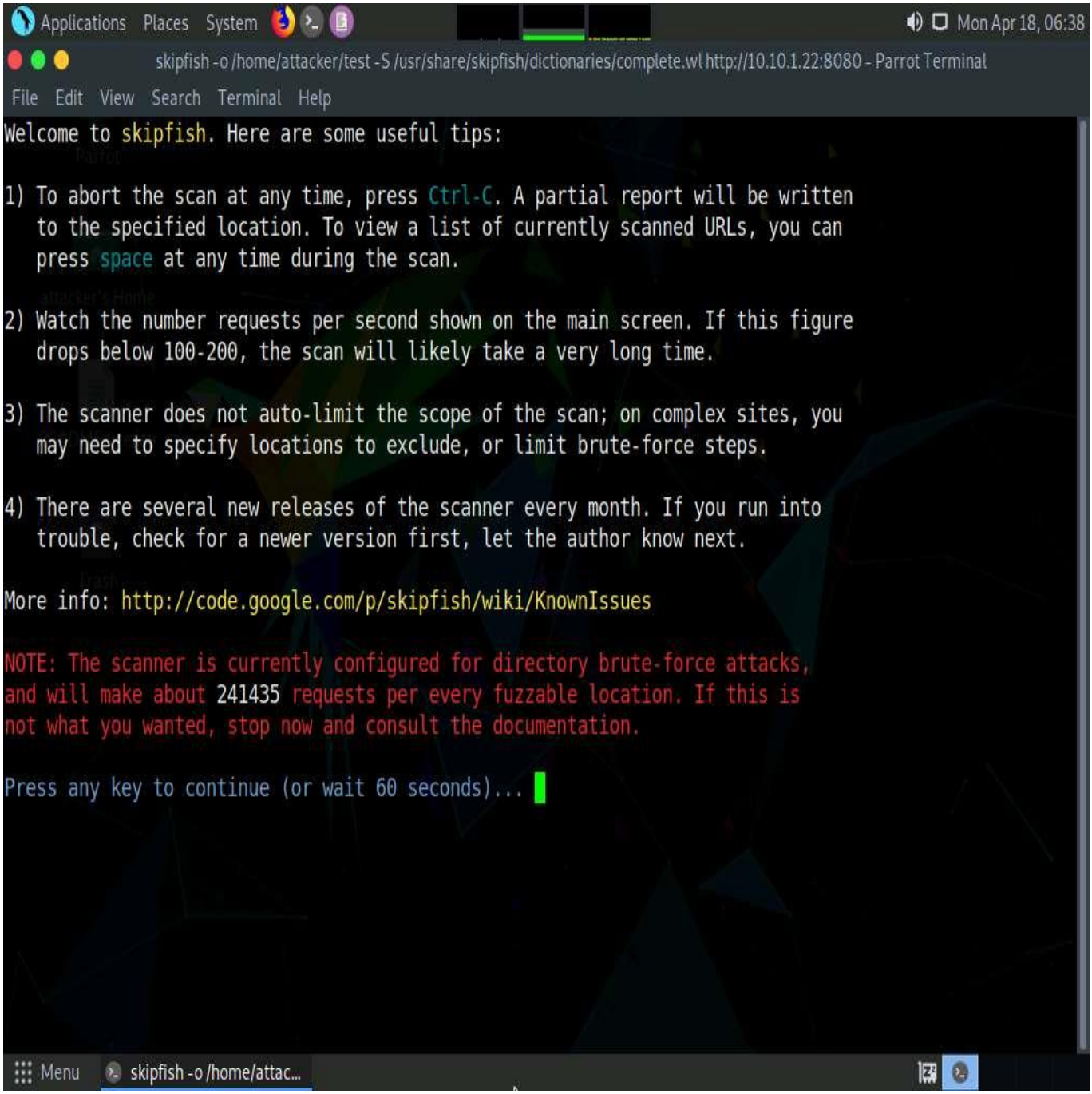
The password that you type will not be visible.



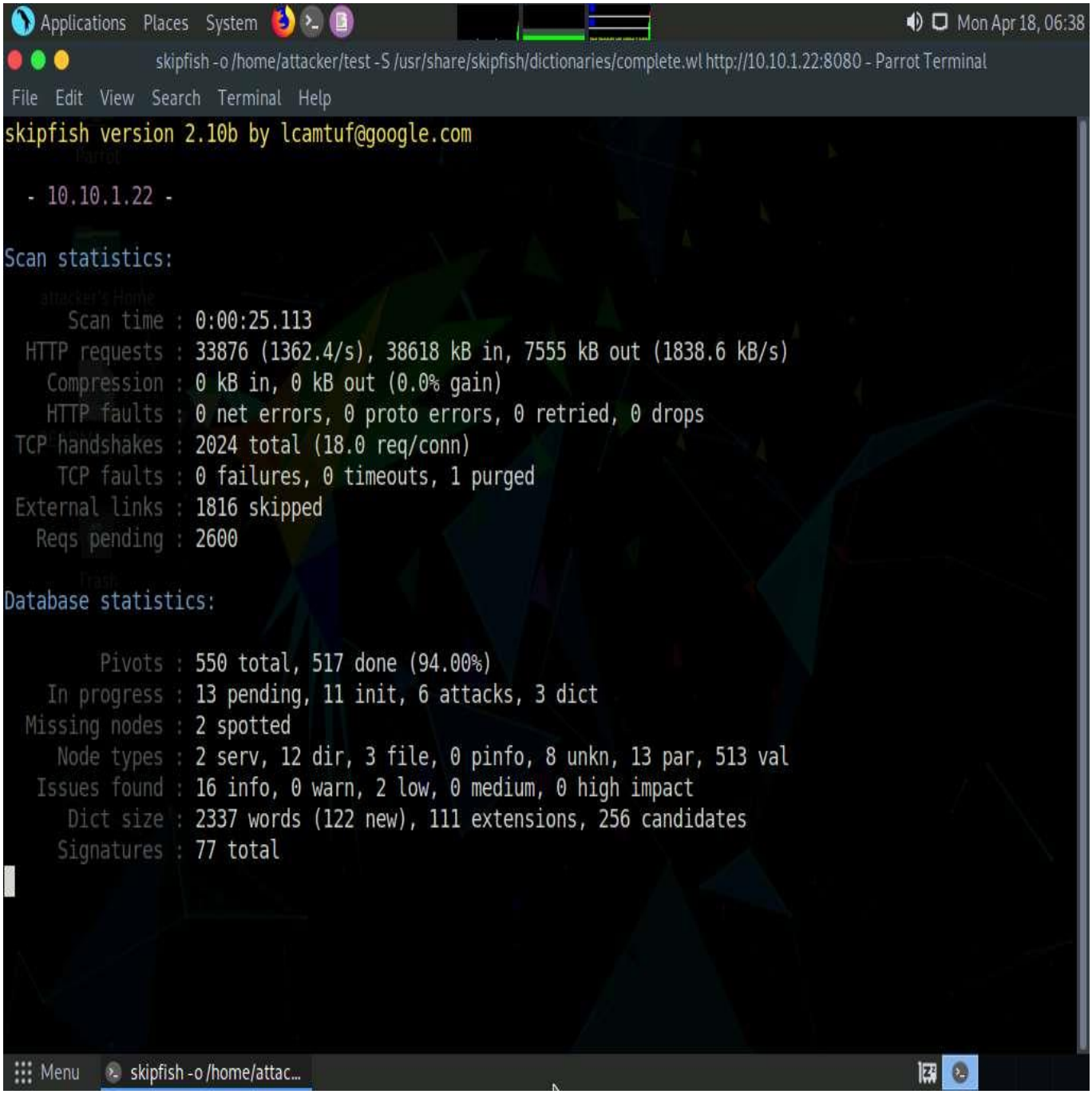
9. ☐ Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http://[IP Address of Windows Server 2022]**.
10. ☐ Specify the output directory and load a dictionary file based on the web server's requirement. In this lab, we are naming the output directory **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**.



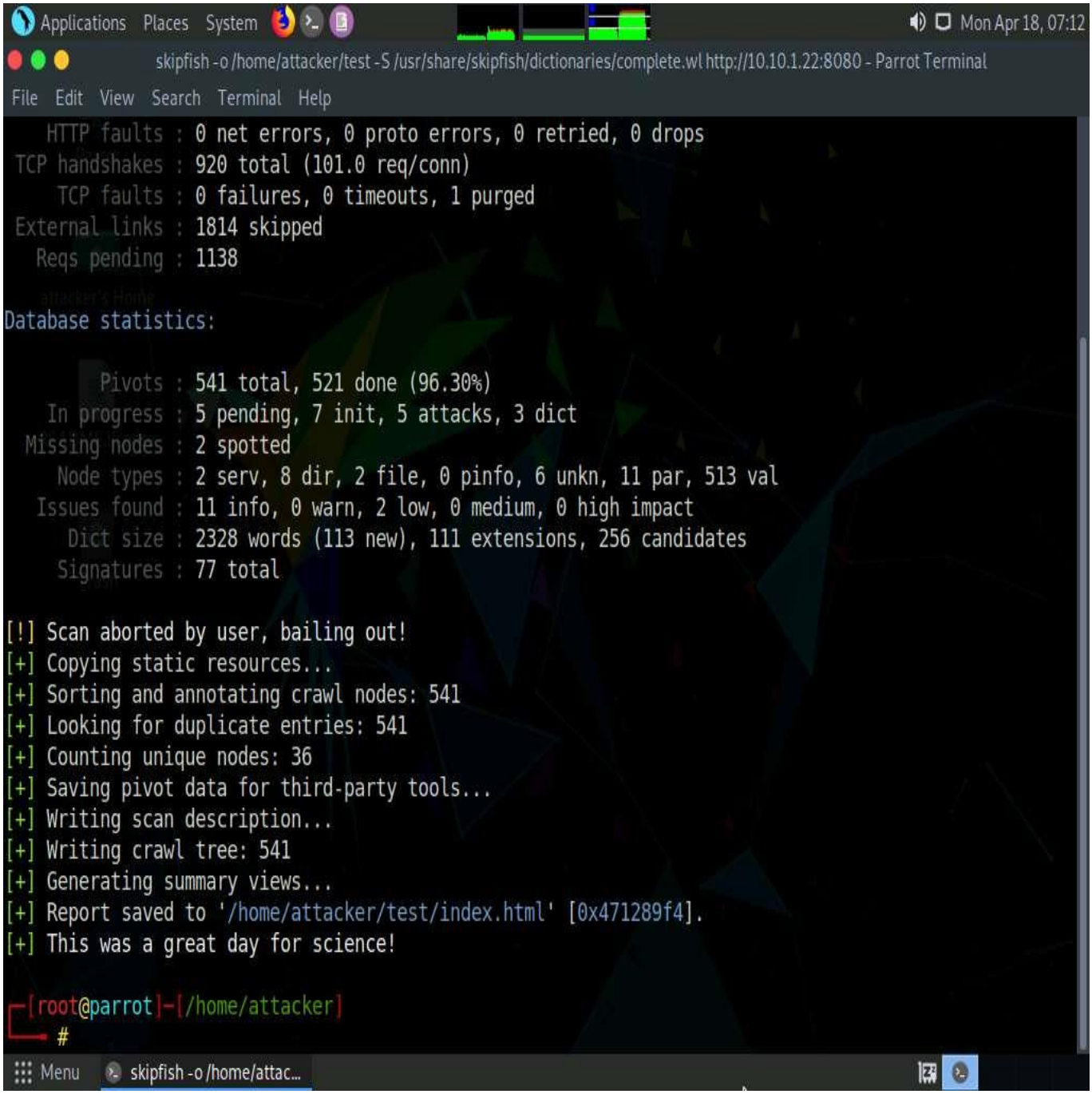
12. ☐ On receiving this command, Skipfish performs a heavy **brute-force attack** on the web server by using the **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in **index.html** inside this location.
13. ☐ Before beginning a scan, Skipfish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



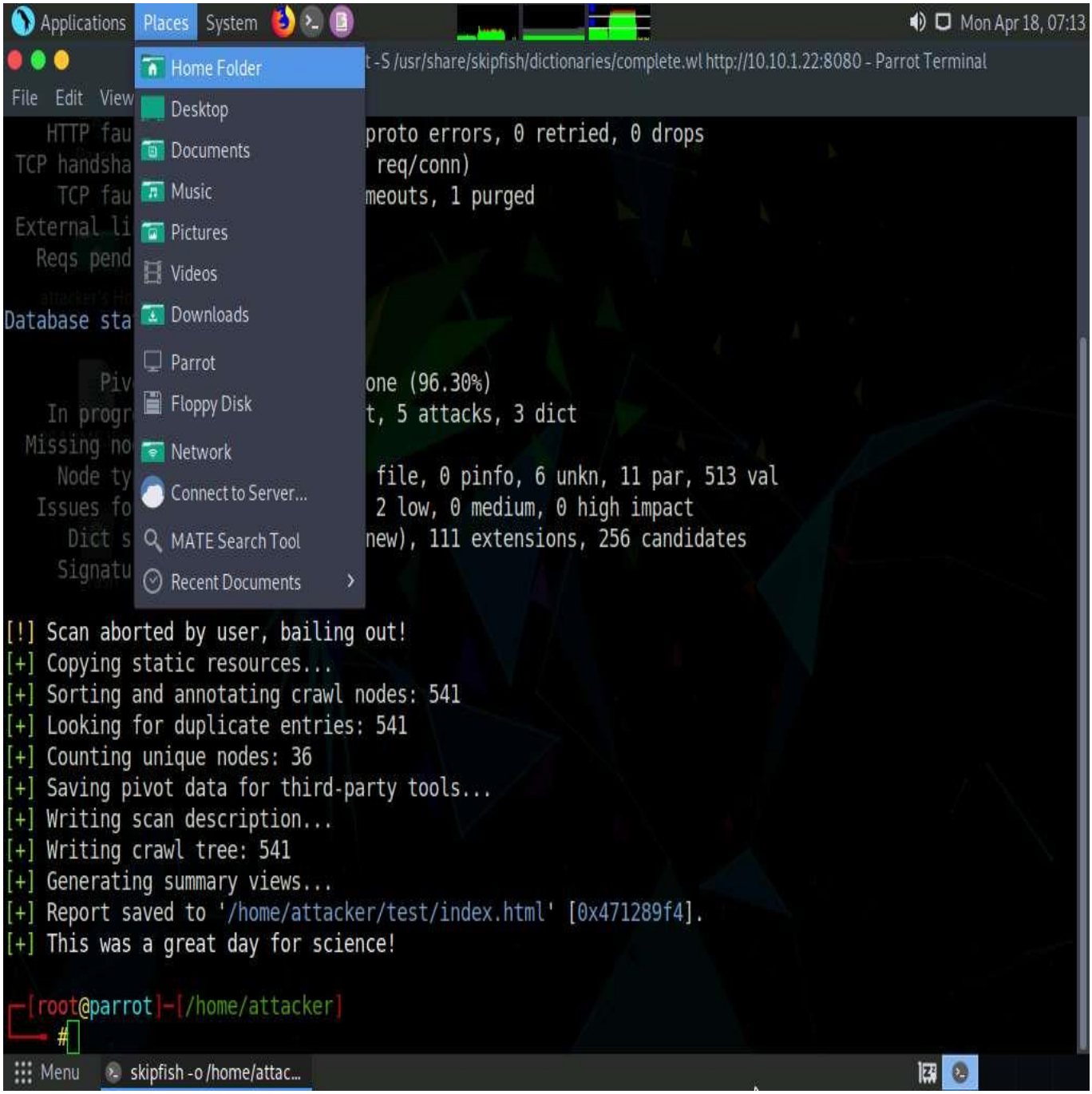
14. ☐ Skipfish scans the web server, as shown in the screenshot.



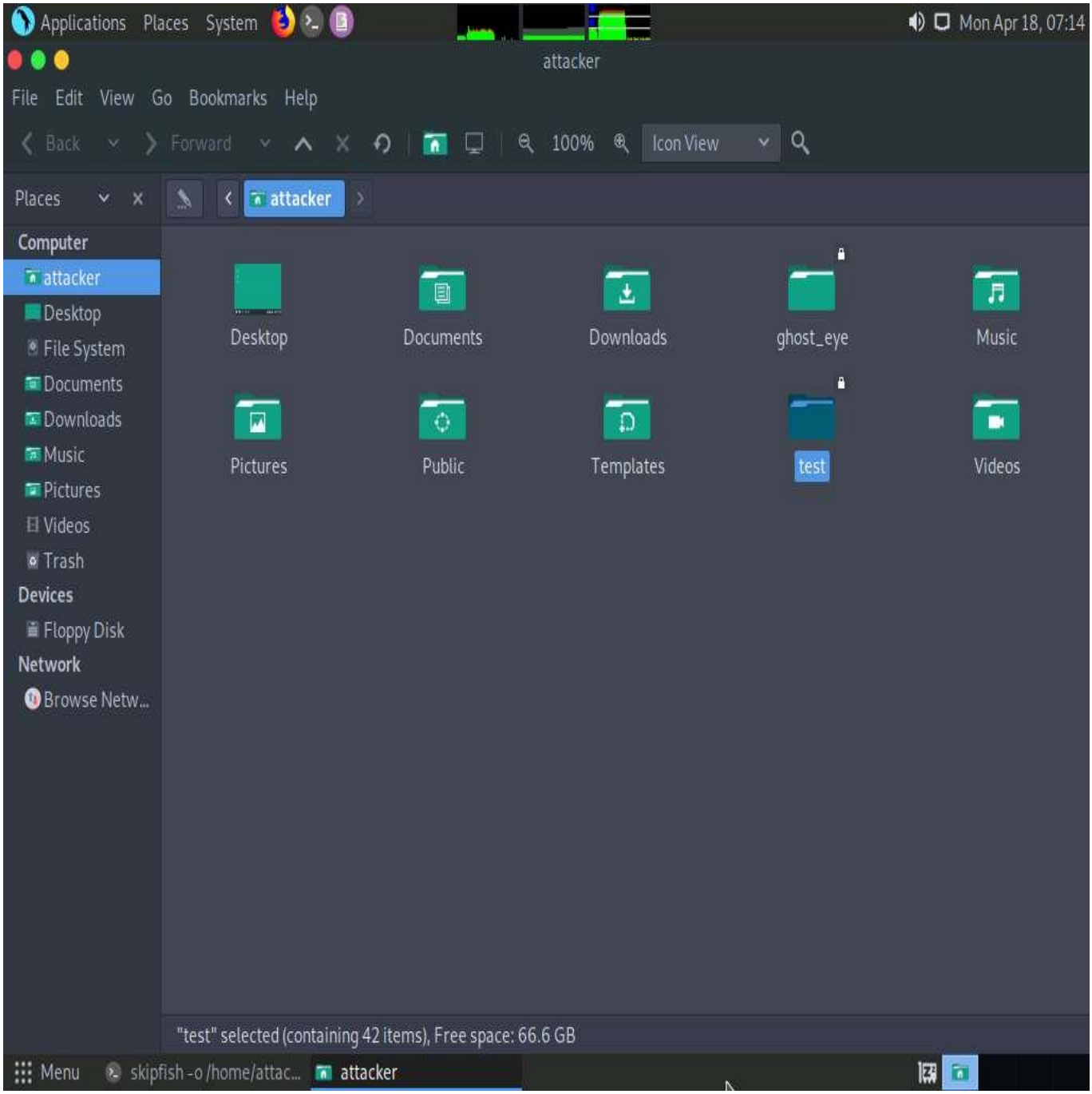
15. ☐ Let the Skipfish run the scan for 5 minutes and after that press **Ctrl+C** to terminate the scan.



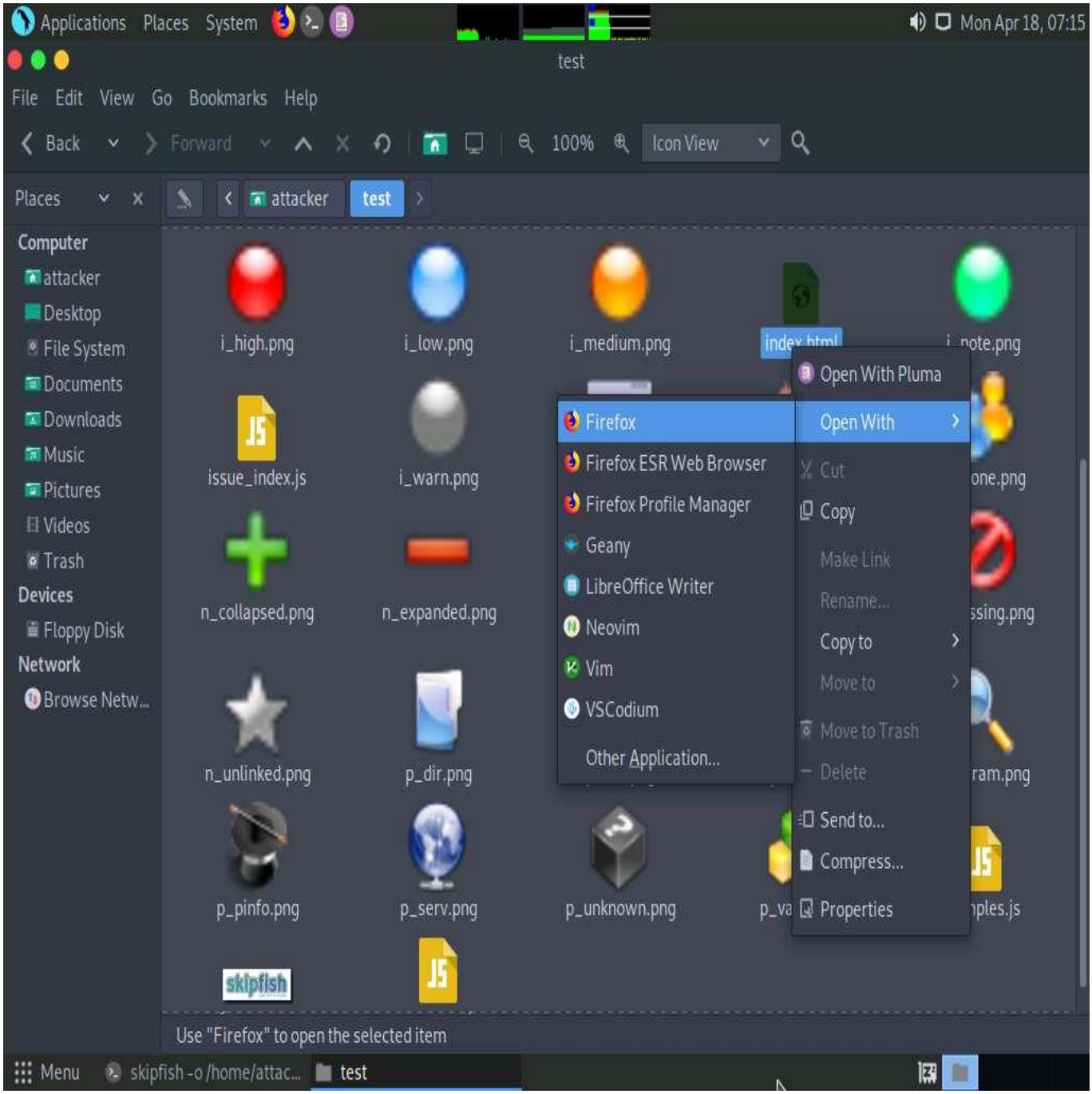
16. ☐ On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **/home/attacker/** location). Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



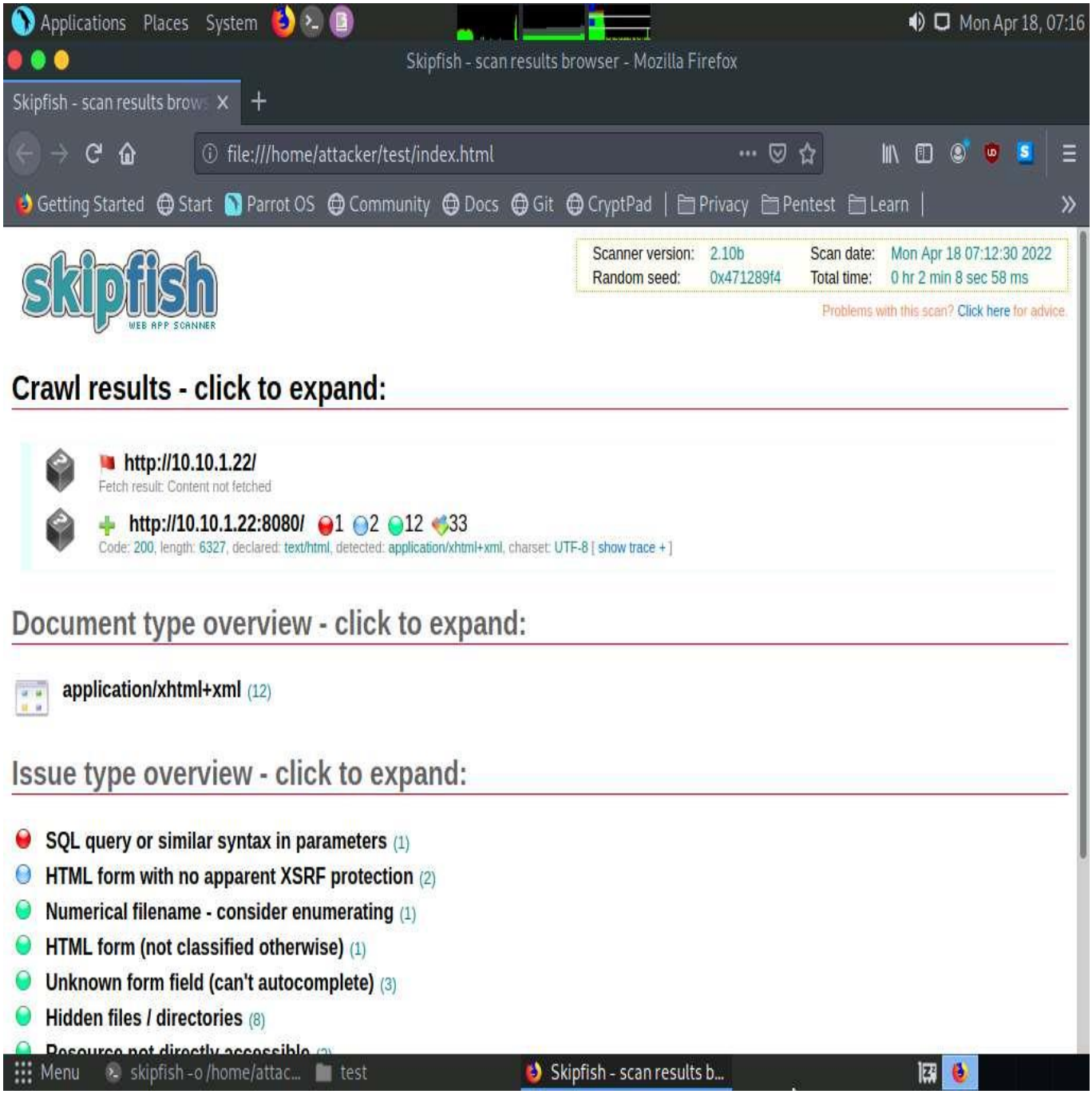
17. ☐ The **attacker** window appears, double-click **test** folder.



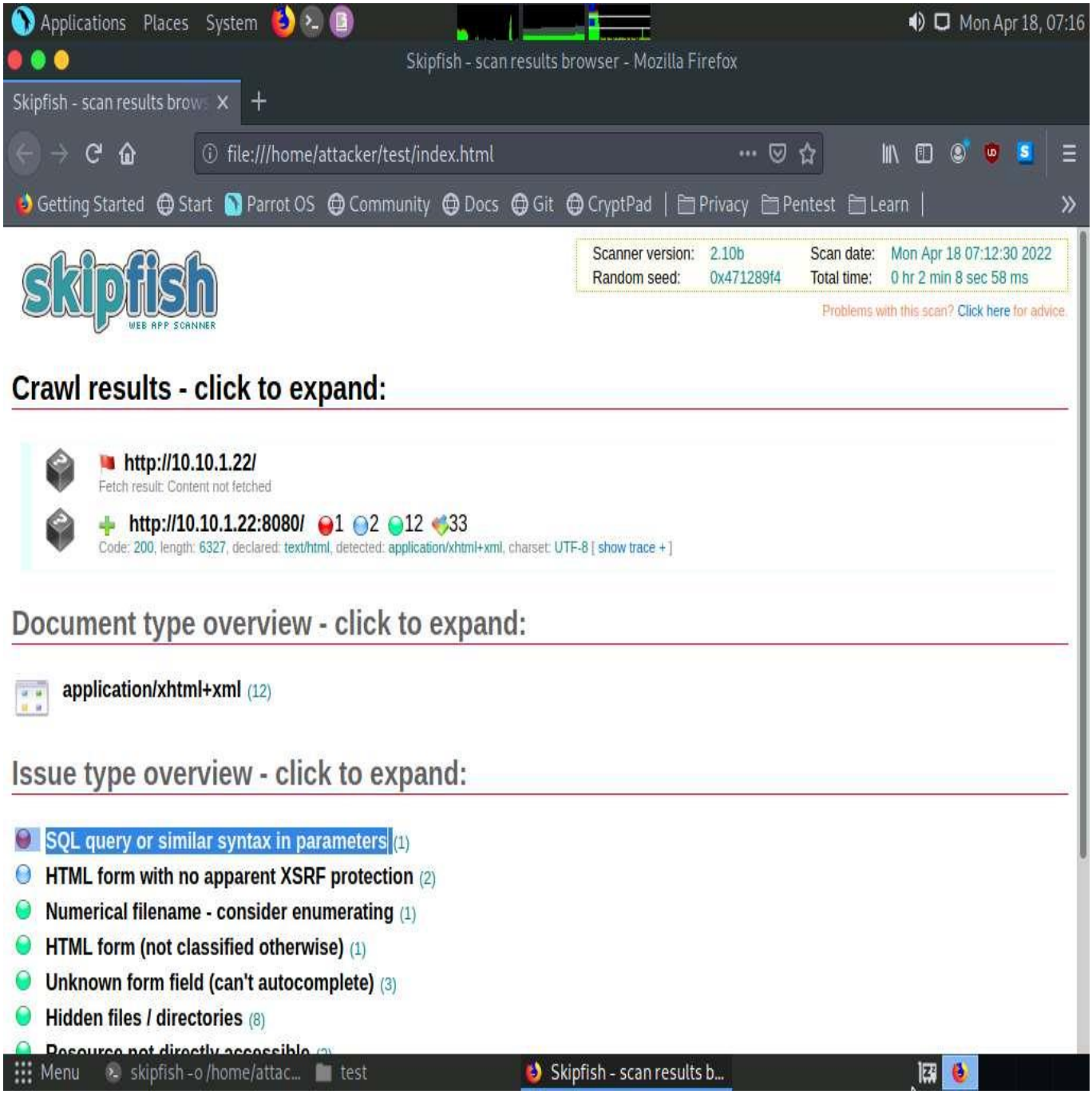
18. ☐ Right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.



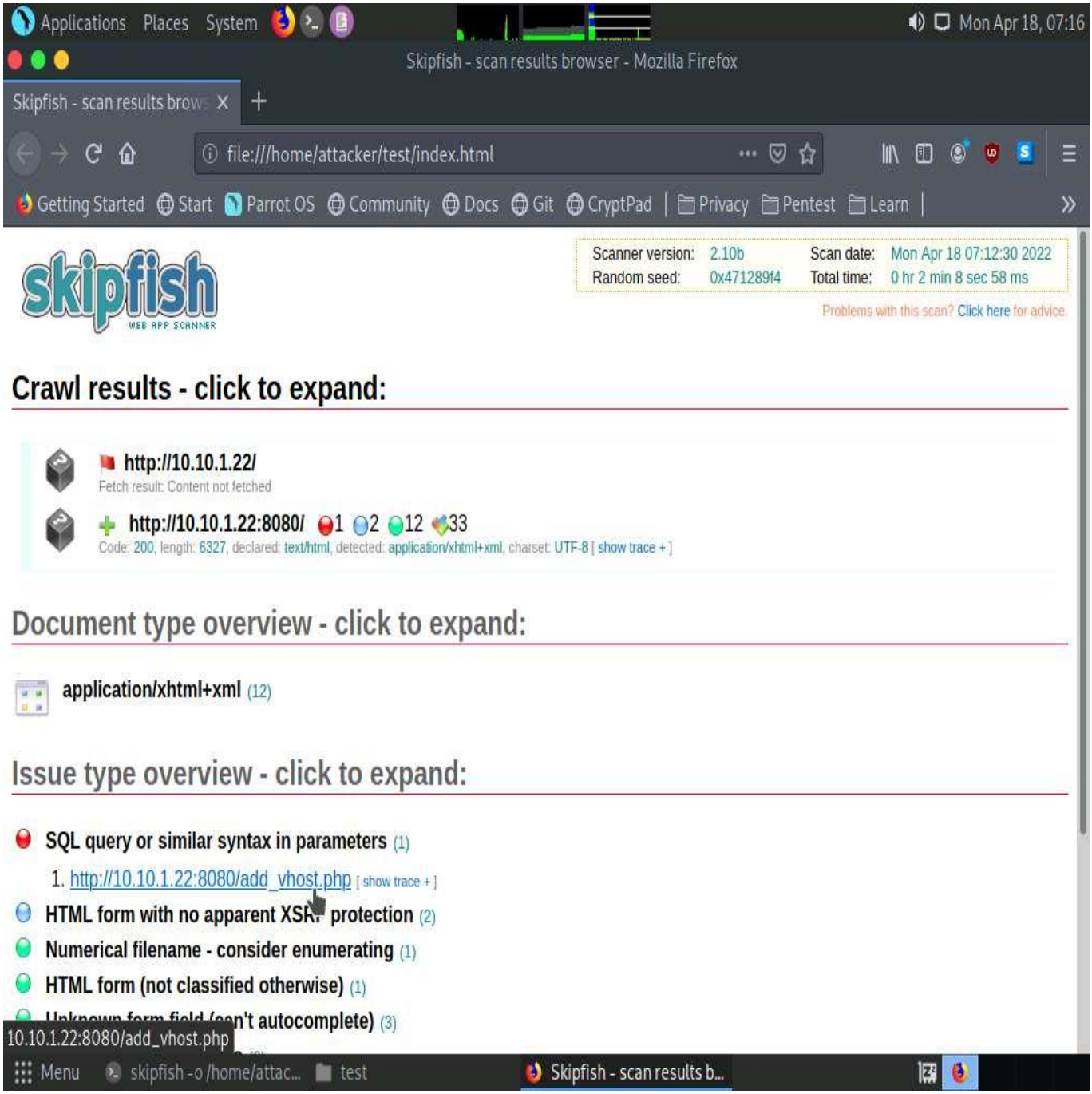
19. ☐ The Skipfish crawl result appears in the web browser, displaying a summary overview of document and issue types found, as shown in the screenshot.



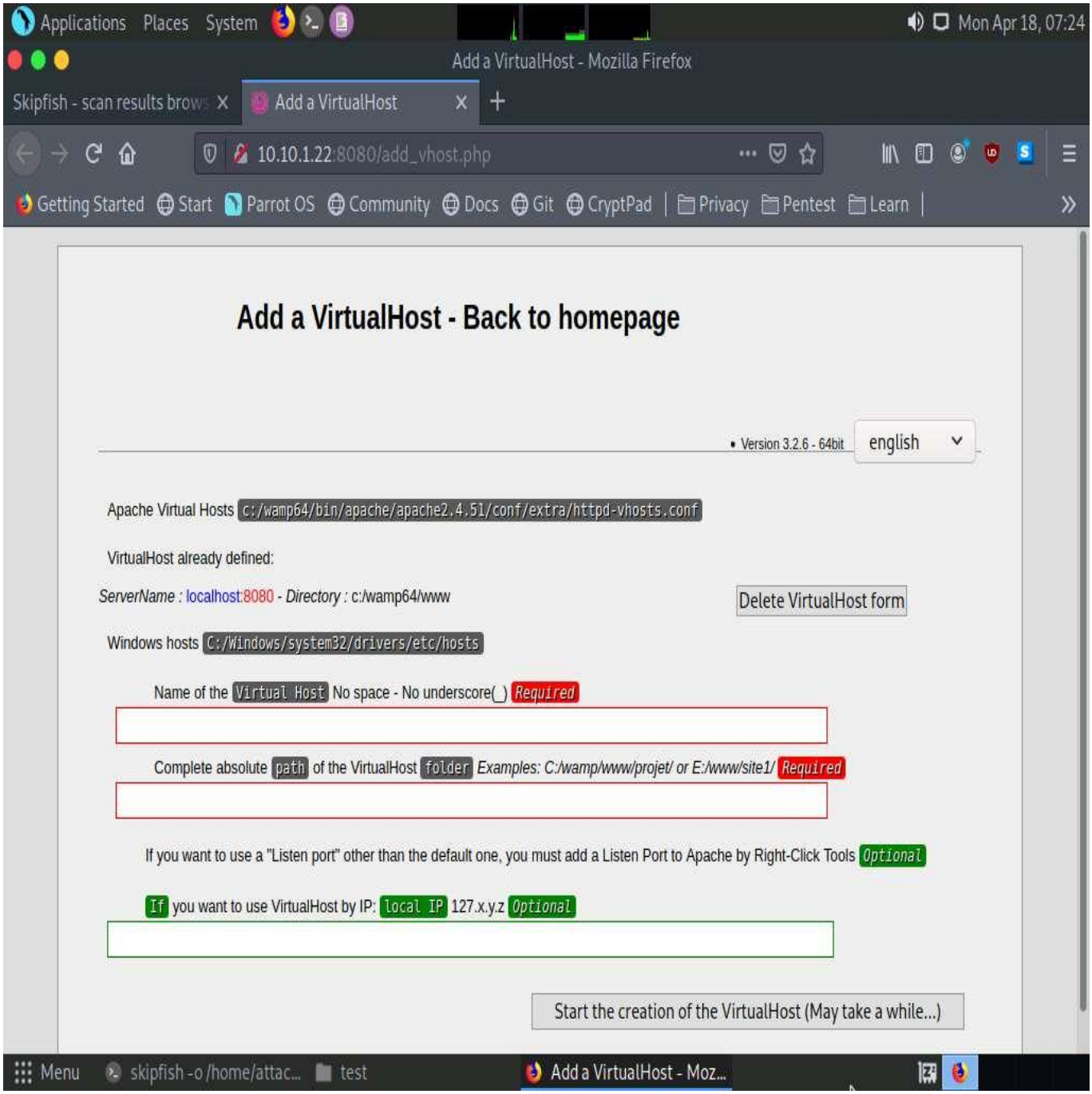
20. ☐ Expand each node to view detailed information regarding the result.
21. ☐ Analyze an issue found in the web server. To do this, click a node under the **Issue type overview** section to expand it.
22. ☐ Analyze the **SQL query or similar syntax in parameters** issue.



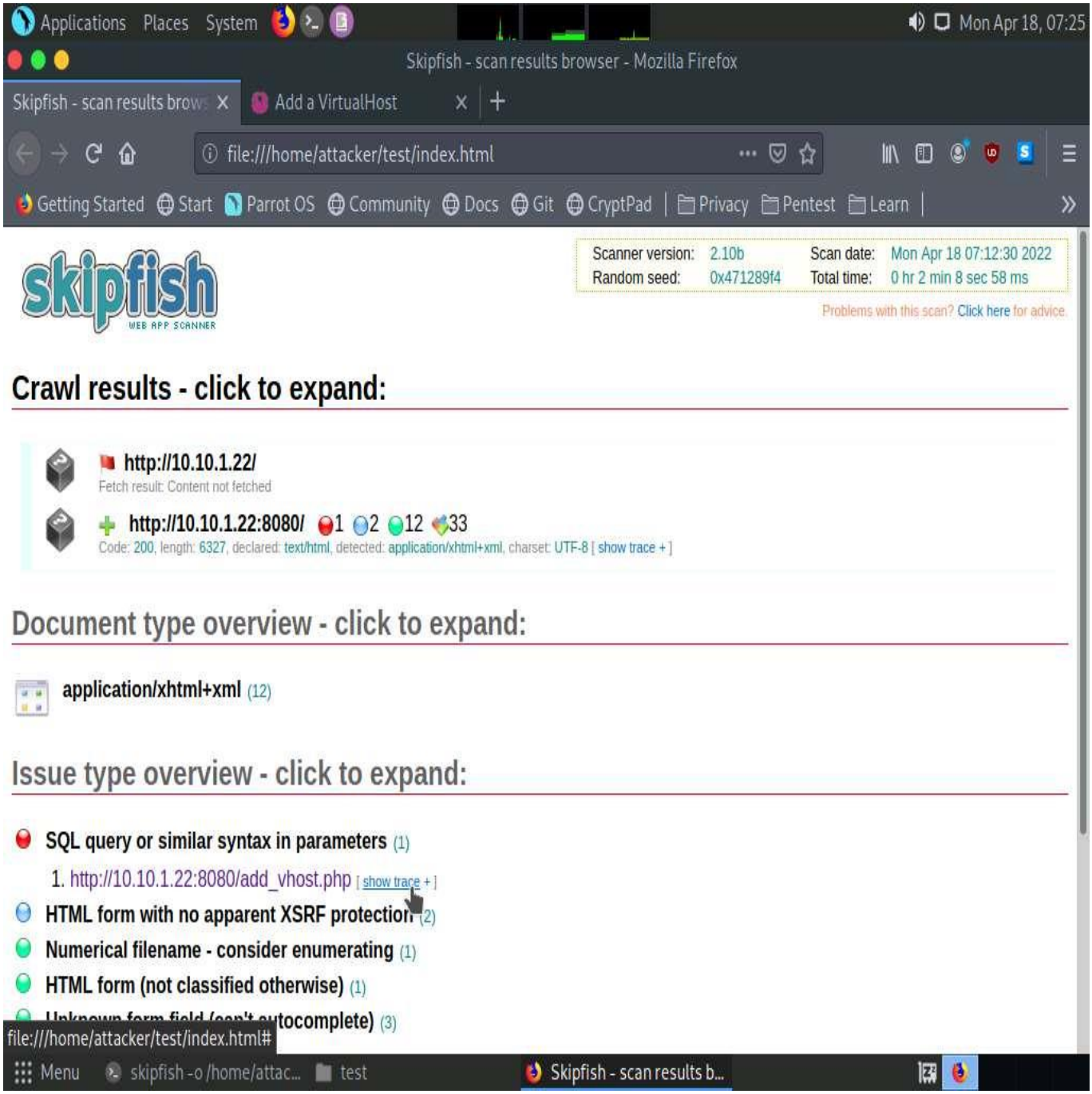
23. ☐ Observe the **URL** of the webpage associated with the vulnerability. Click the URL.



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

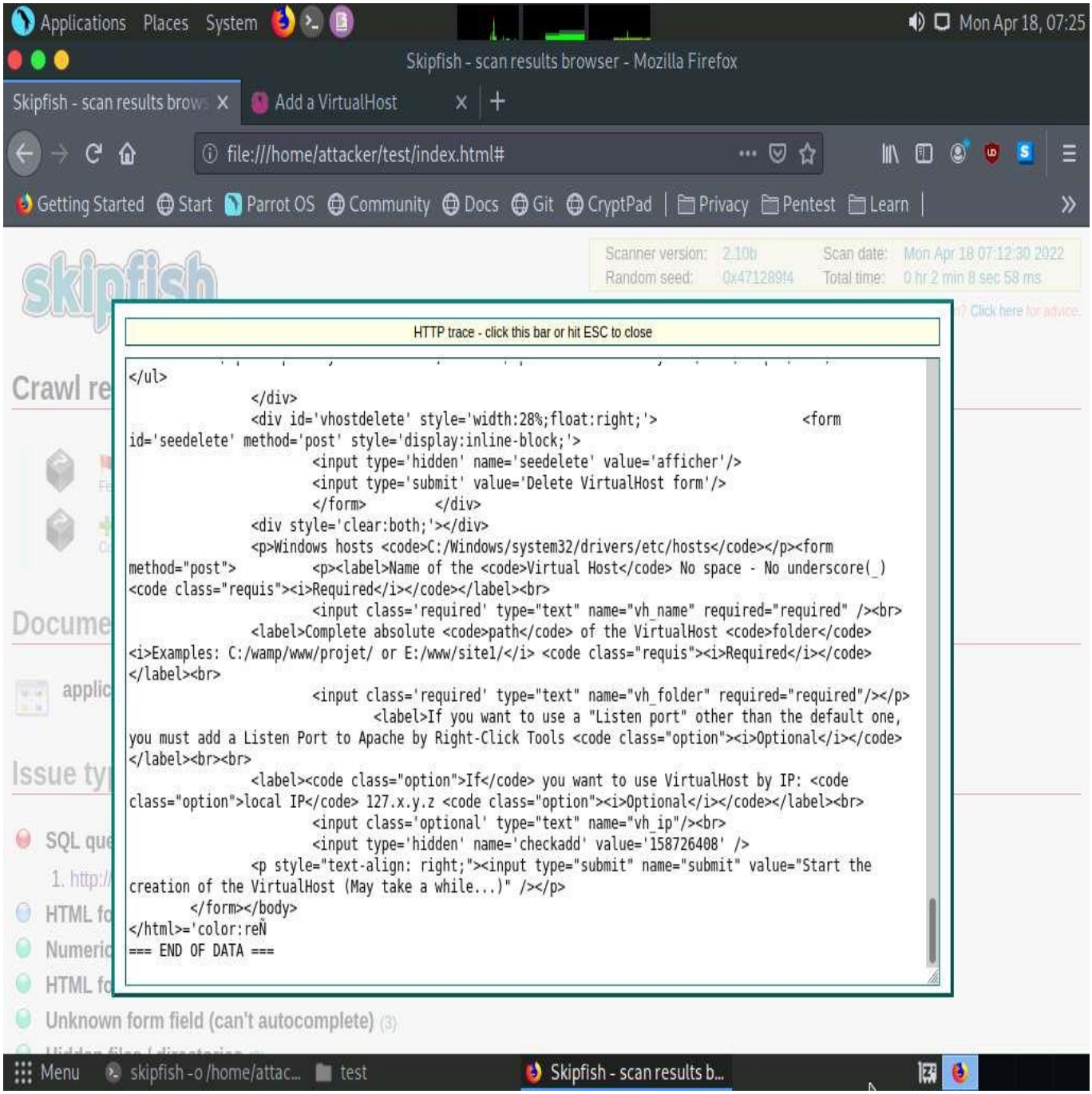


25. ☐ The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.
26. ☐ Switch back to the first tab and click **show trace** next to the URL to examine the vulnerability in detail.



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

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.

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.

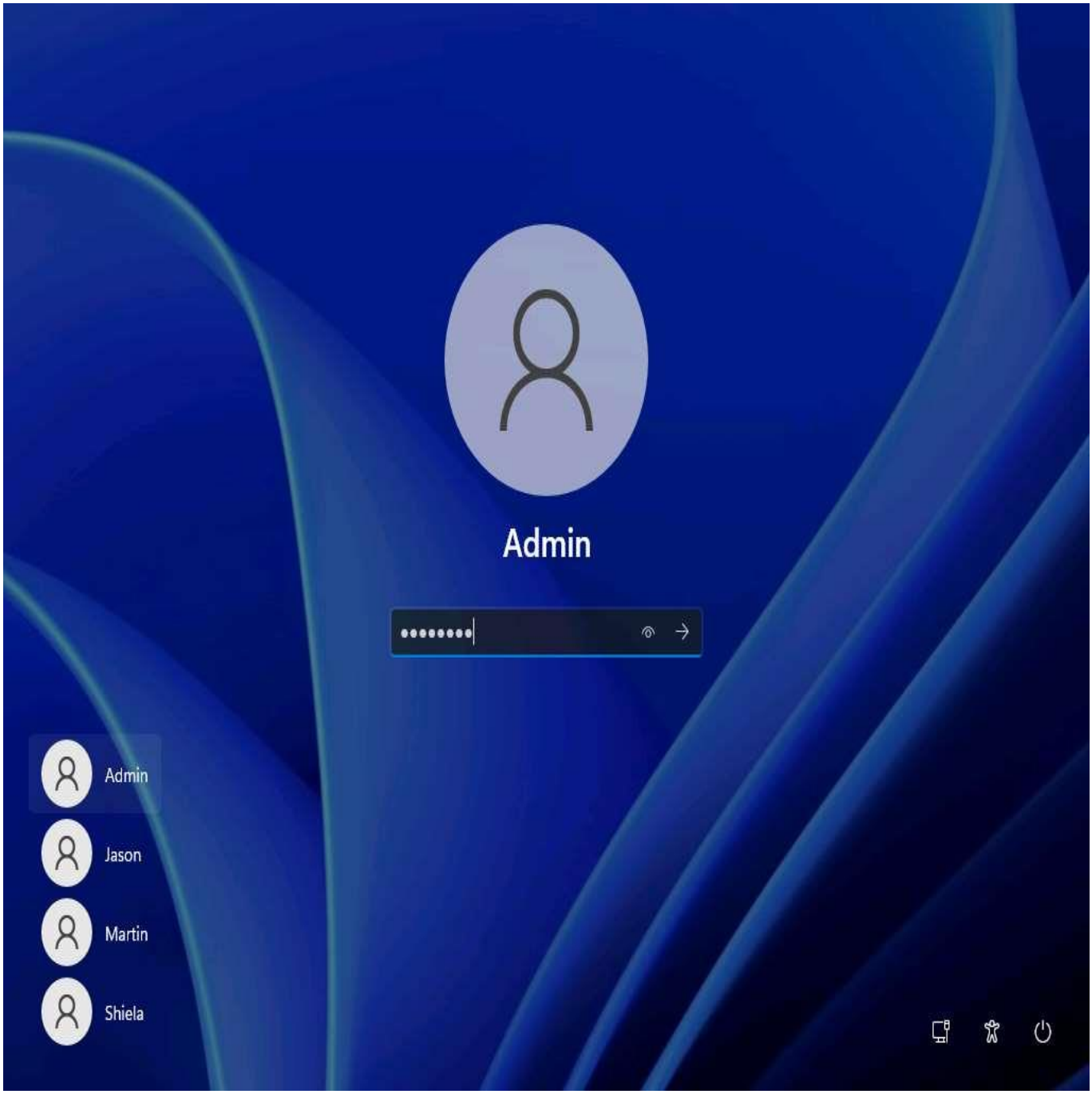
Here, we will use the httprecon tool to gather information about a target web server.

1. Click Windows 11 to switch to the **Windows 11**, click Ctrl+Alt+Delete.

   Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

2. By default, **Admin** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

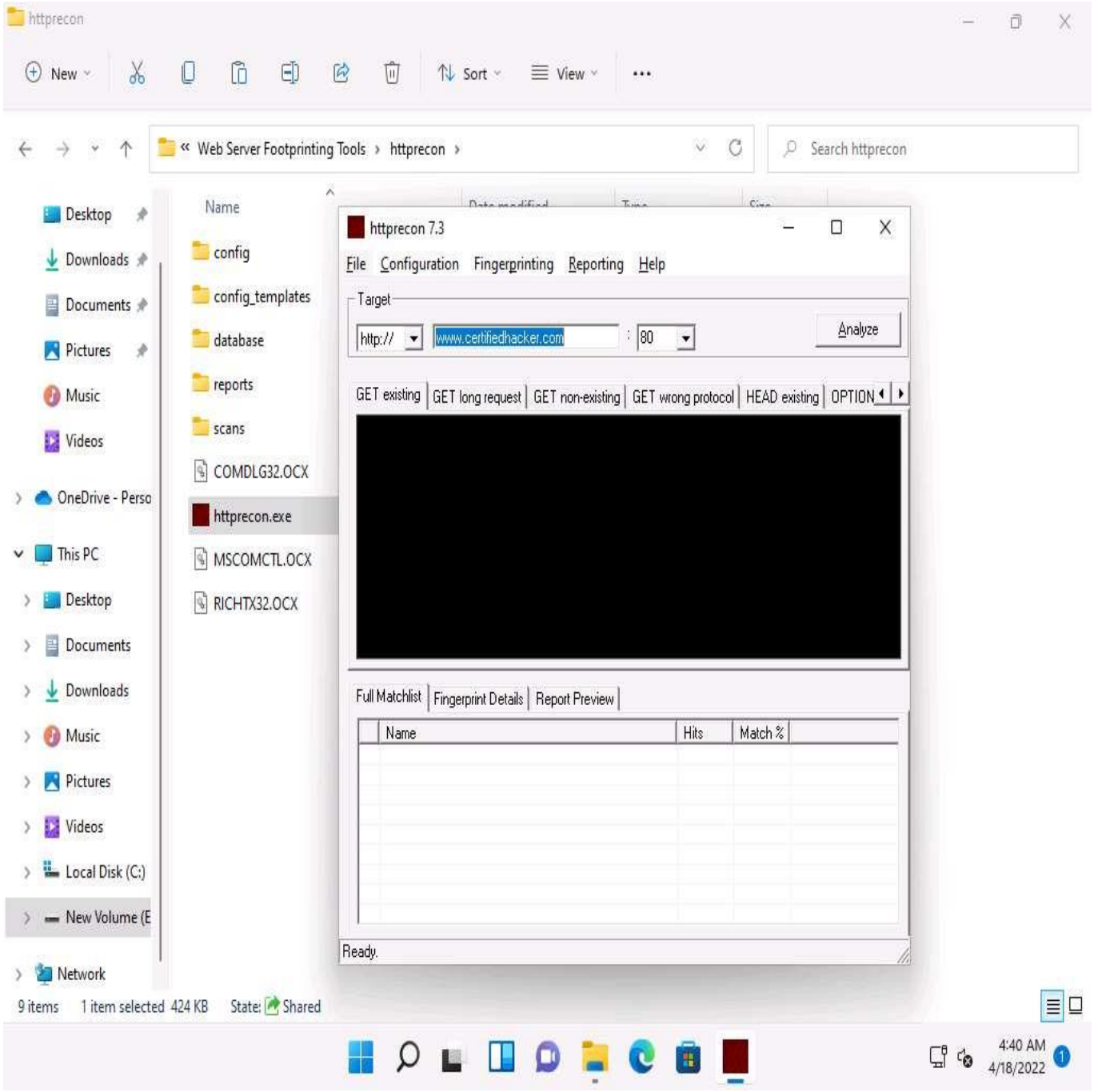
   Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.
   Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



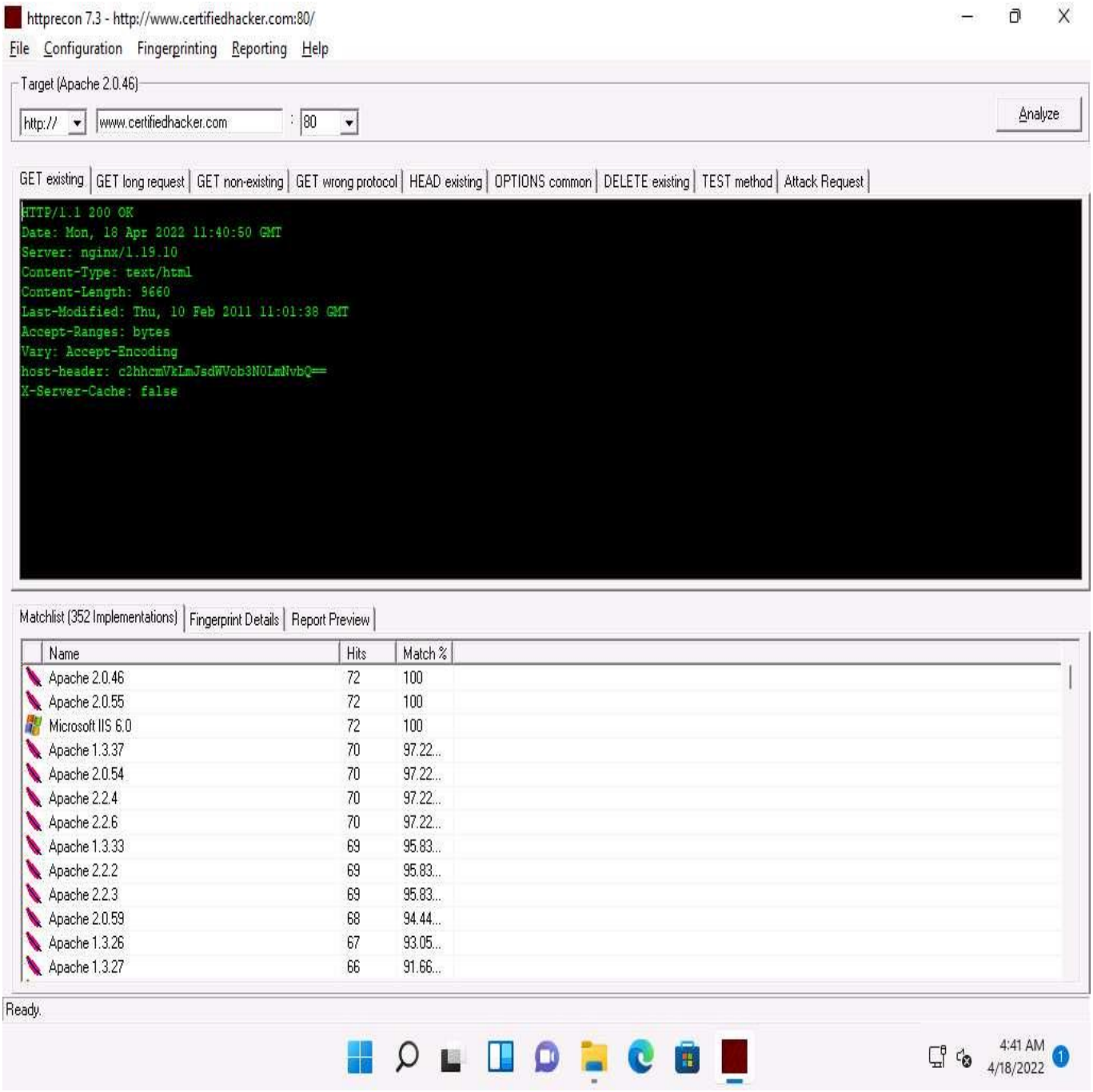
3. Navigate to **E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**, right-click **httprecon.exe**, and, from the context menu, click **Run as administrator** double-click to launch the application.

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

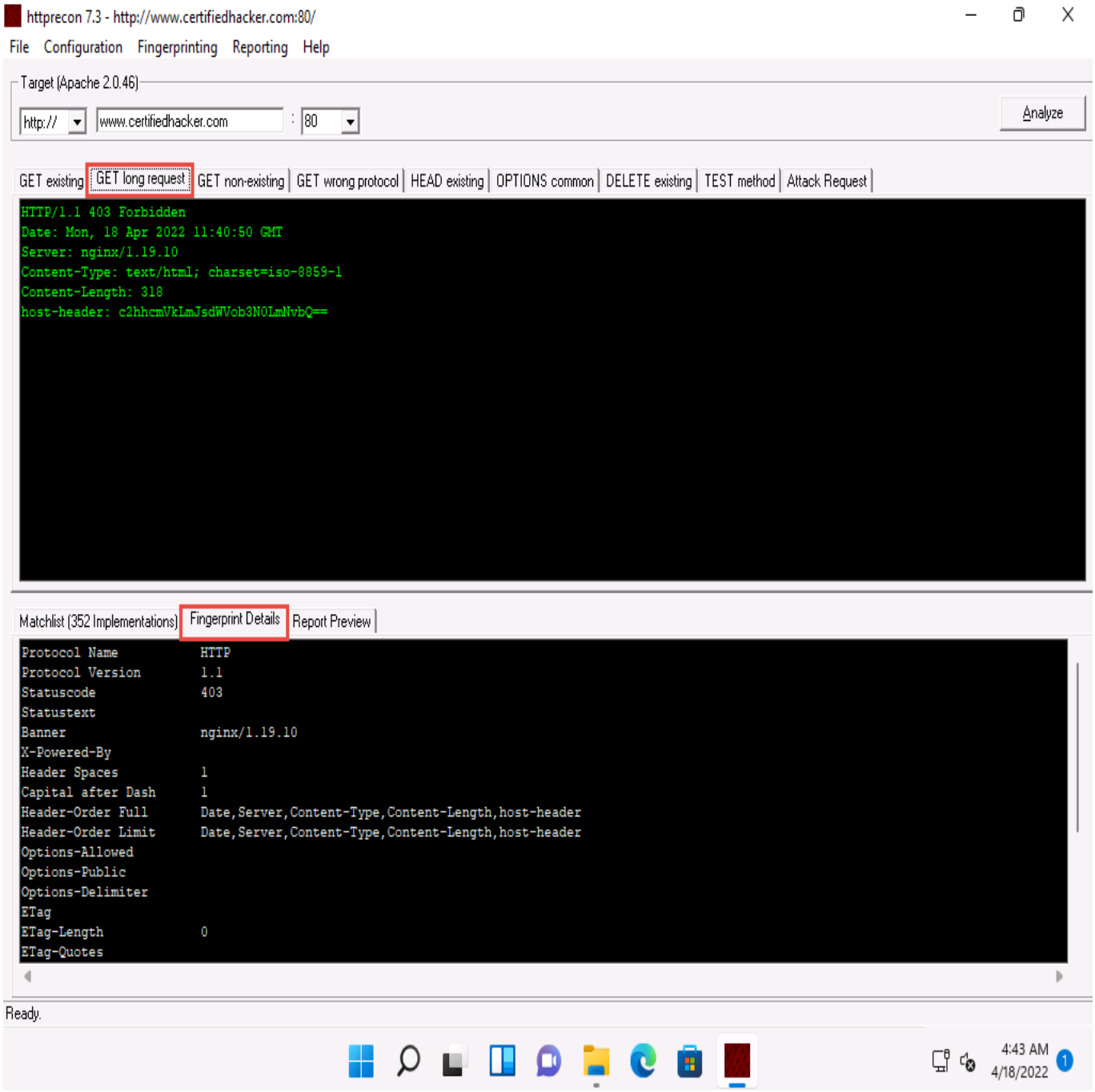
4. Main window of **httprecon** appears, enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number (80)** in the **Target** section.



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

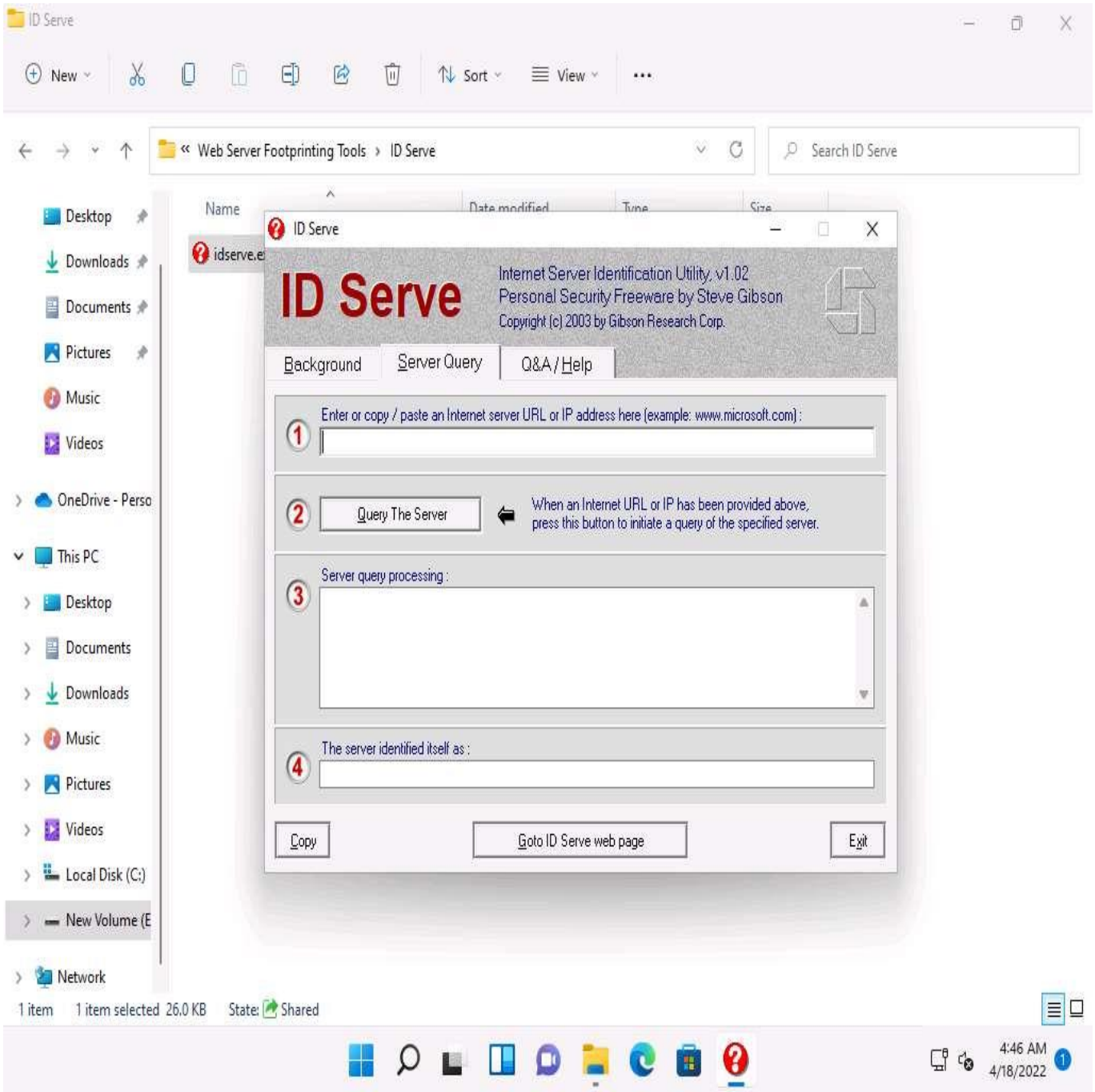
Pen testers must be familiar with banner grabbing techniques to monitor servers and ensure compliance and appropriate security updates. This technique also helps in locating rogue servers or determining the role of

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:

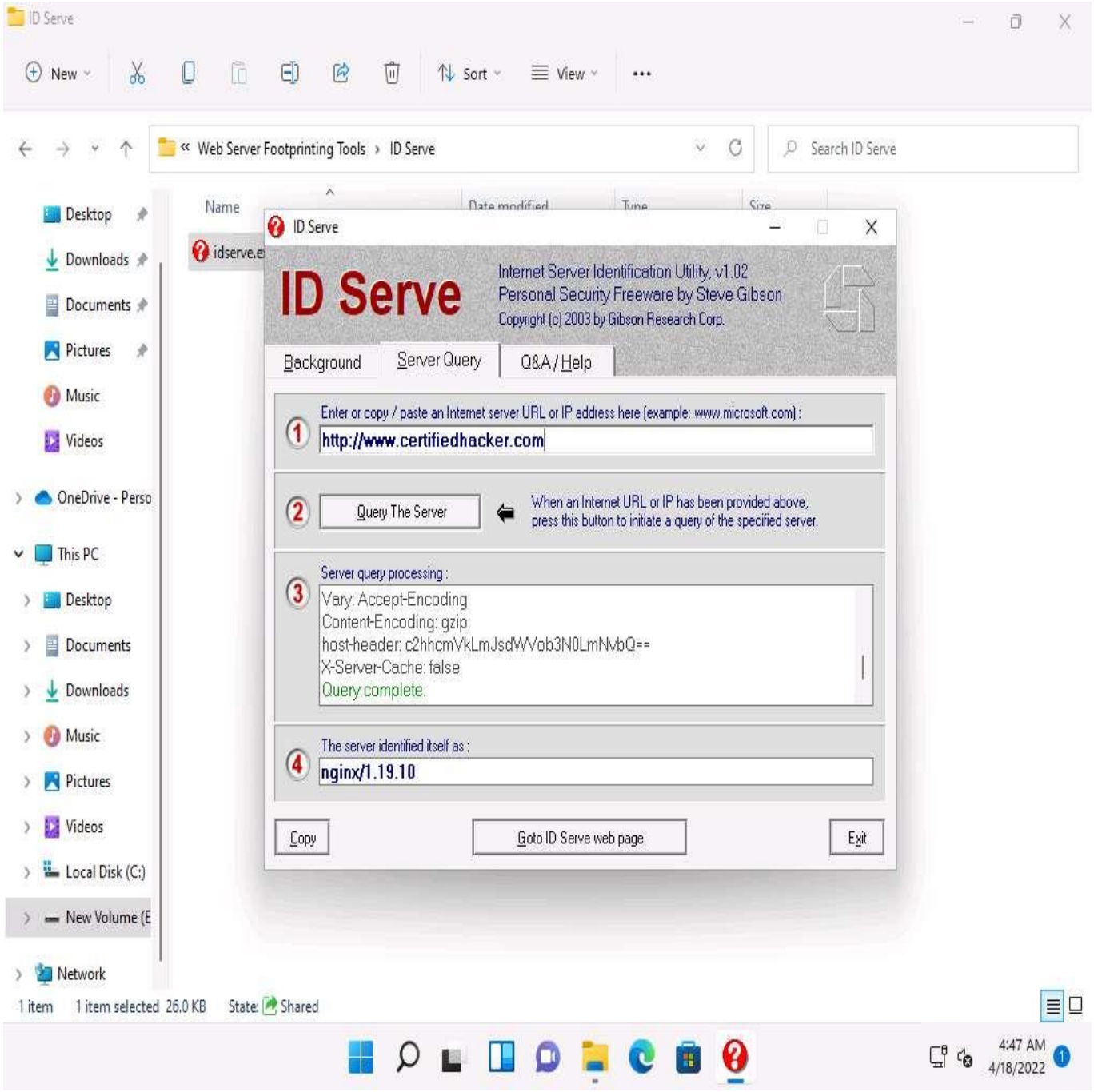
- HTTP server identification
- Non-HTTP server identification
- Reverse DNS lookup

1. Click Windows 11 to switch to the **Windows 11** 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.

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.

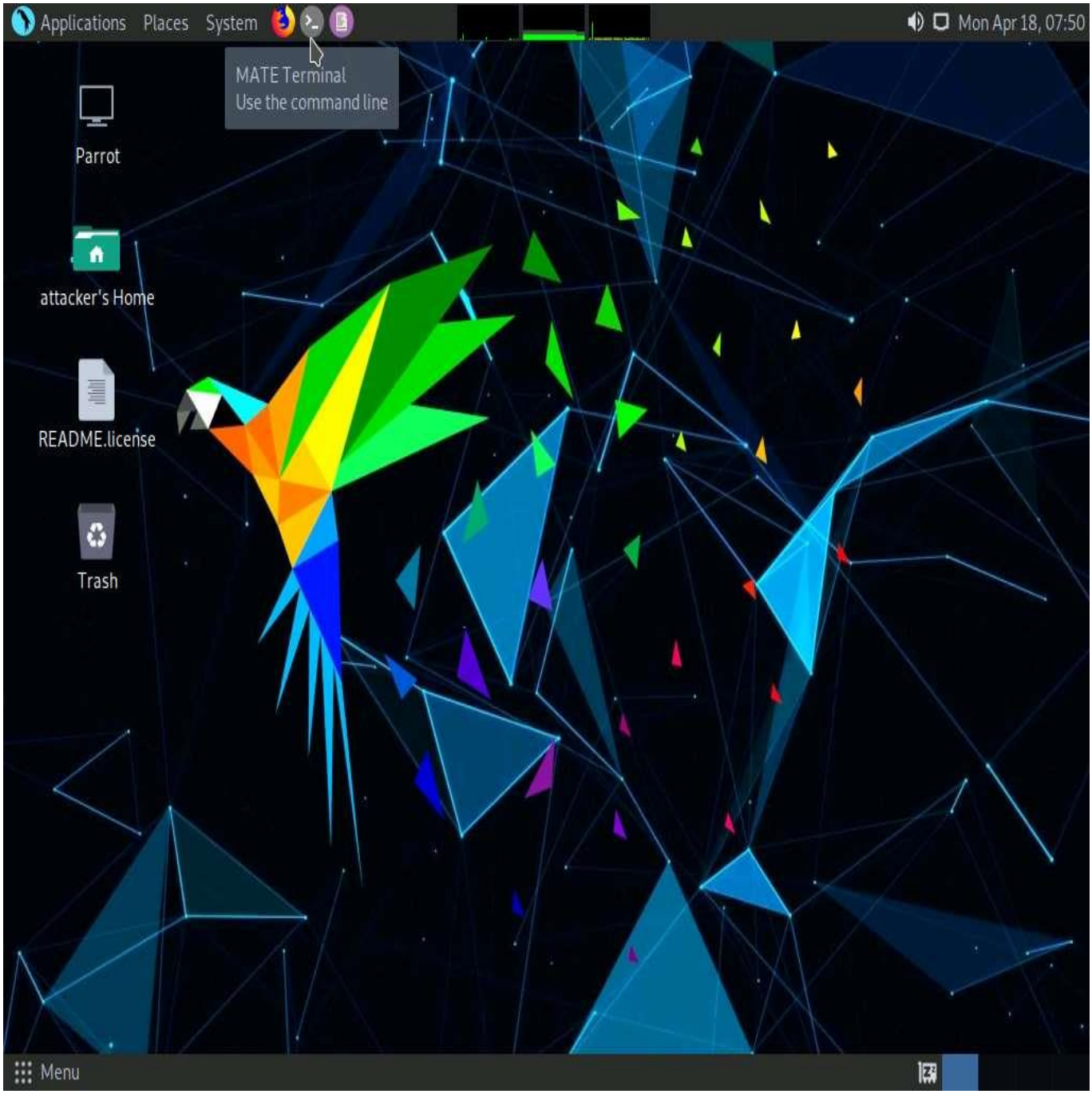
Telnet

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.

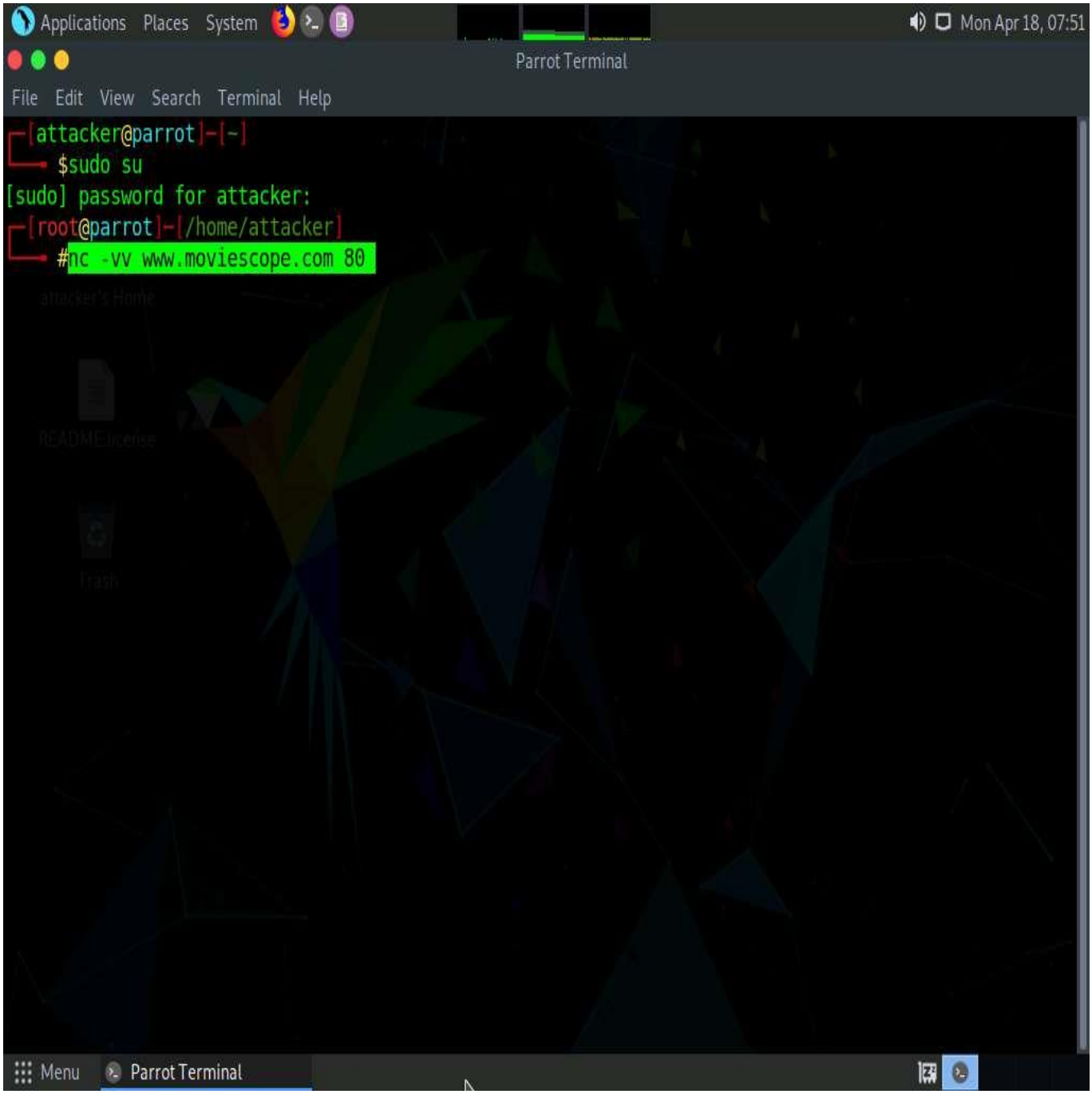
1. Click Parrot Security to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon from the menu bar to launch the terminal.



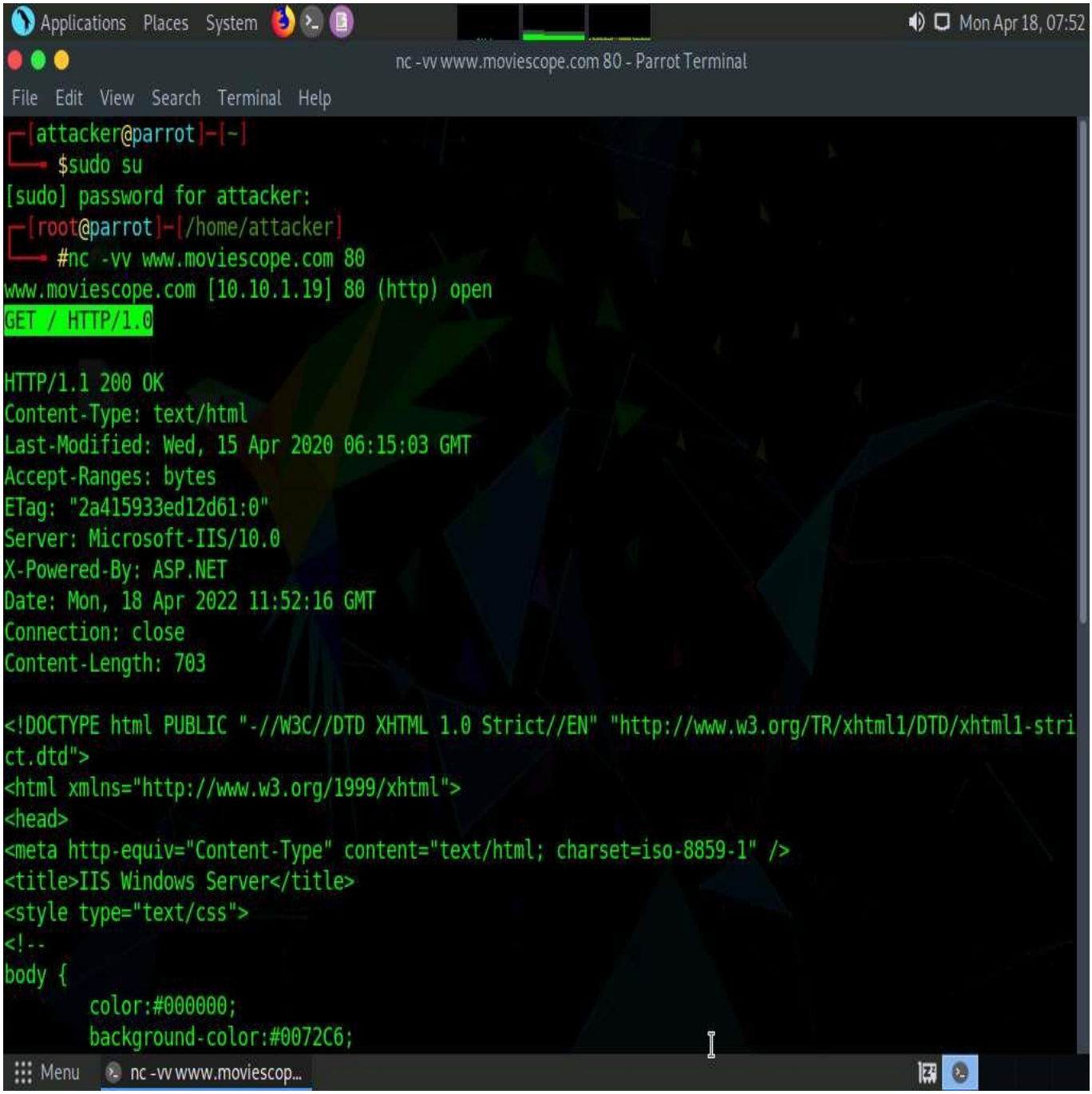
3. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

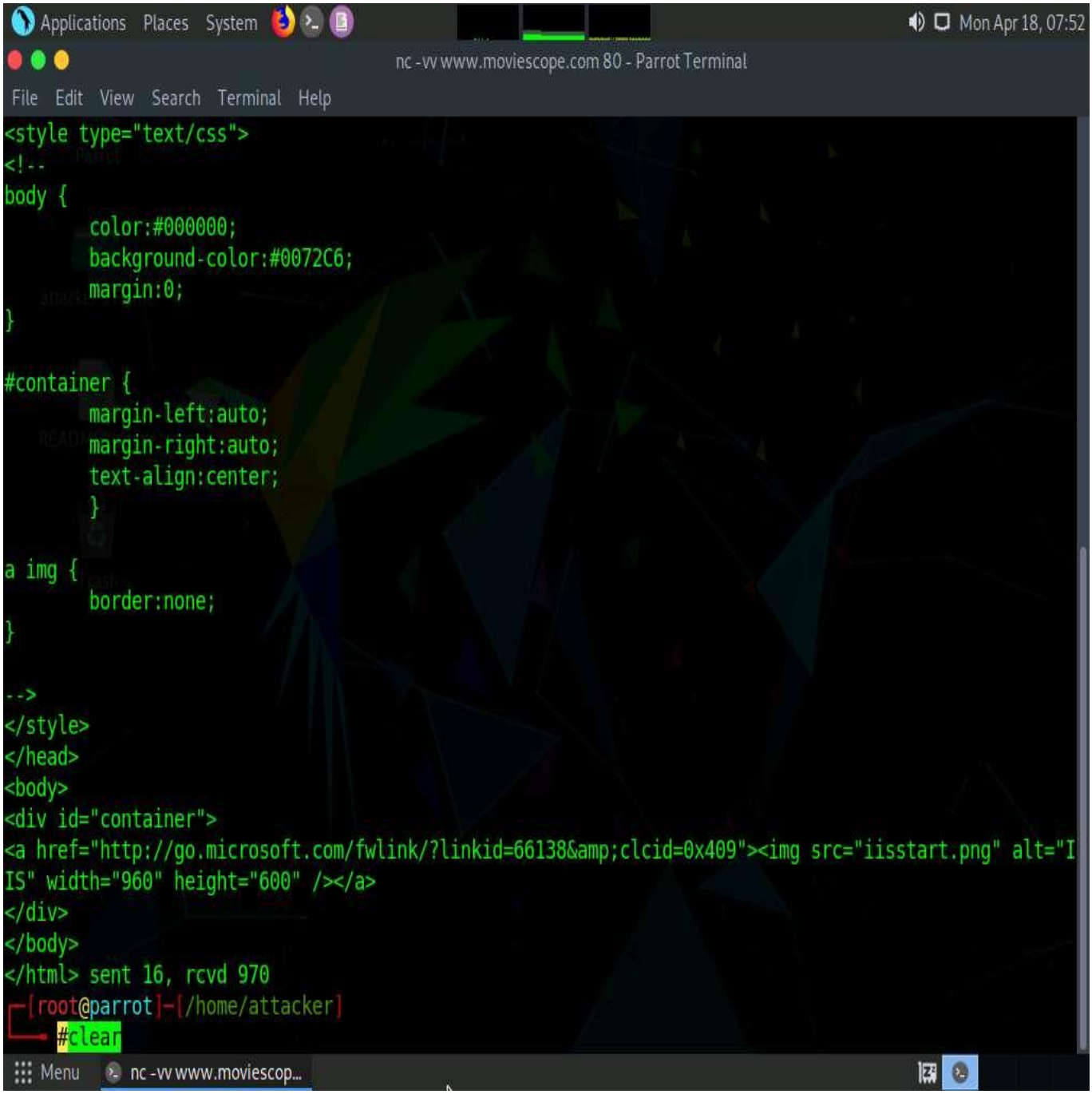
5. In the terminal window, type **nc -vv www.moviescope.com 80** and press **Enter**.



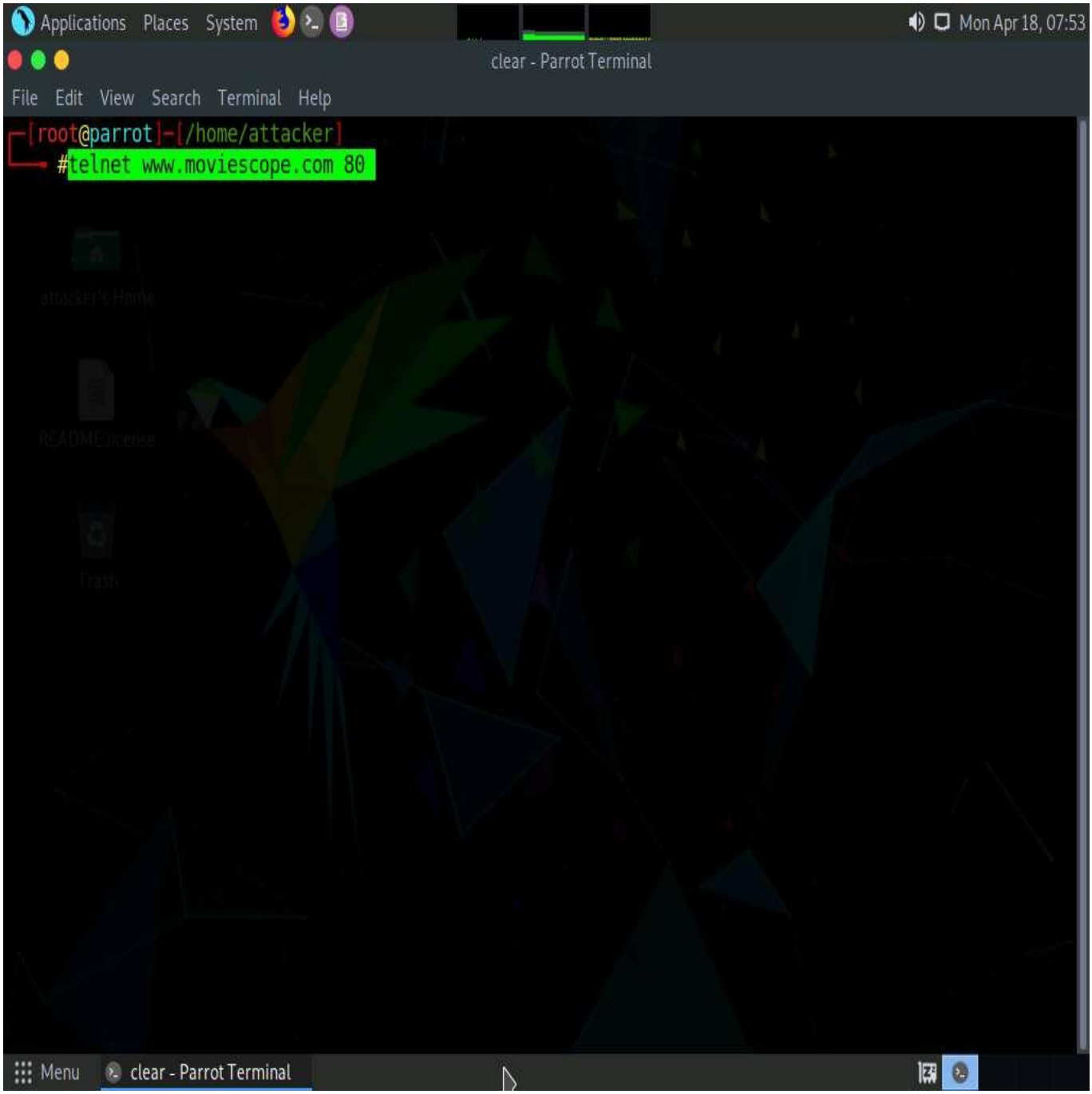
6. ☐ Once you hit **Enter**, the netcat will display the hosting information of the provided domain, as shown in the screenshot.
7. ☐ Now, type **GET / HTTP/1.0** and press **Enter** twice.
8. ☐ Netcat will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.



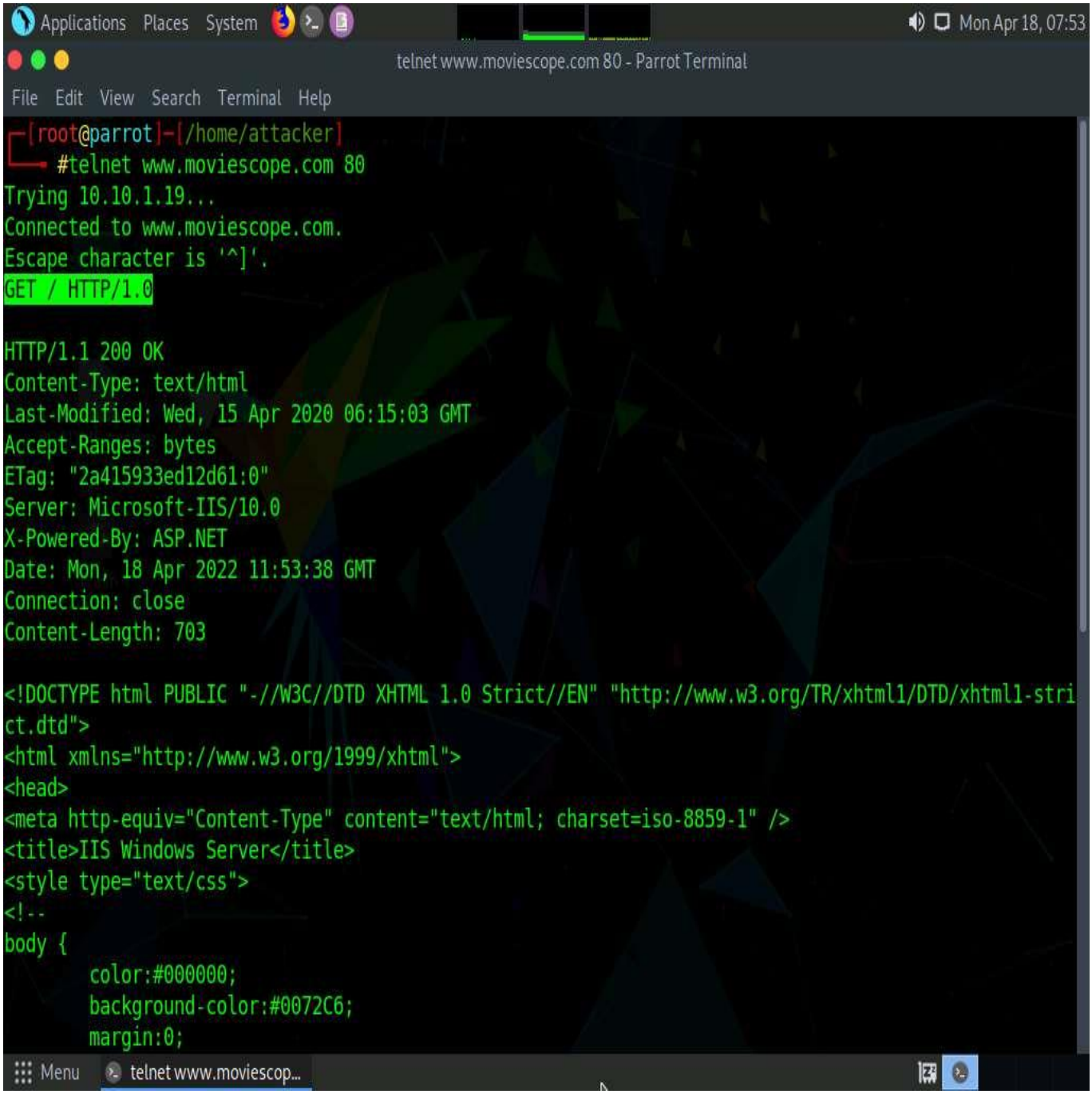
9. ☐ In the terminal windows, type **clear** and press **Enter** to clear the netcat result in the terminal window.



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



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



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

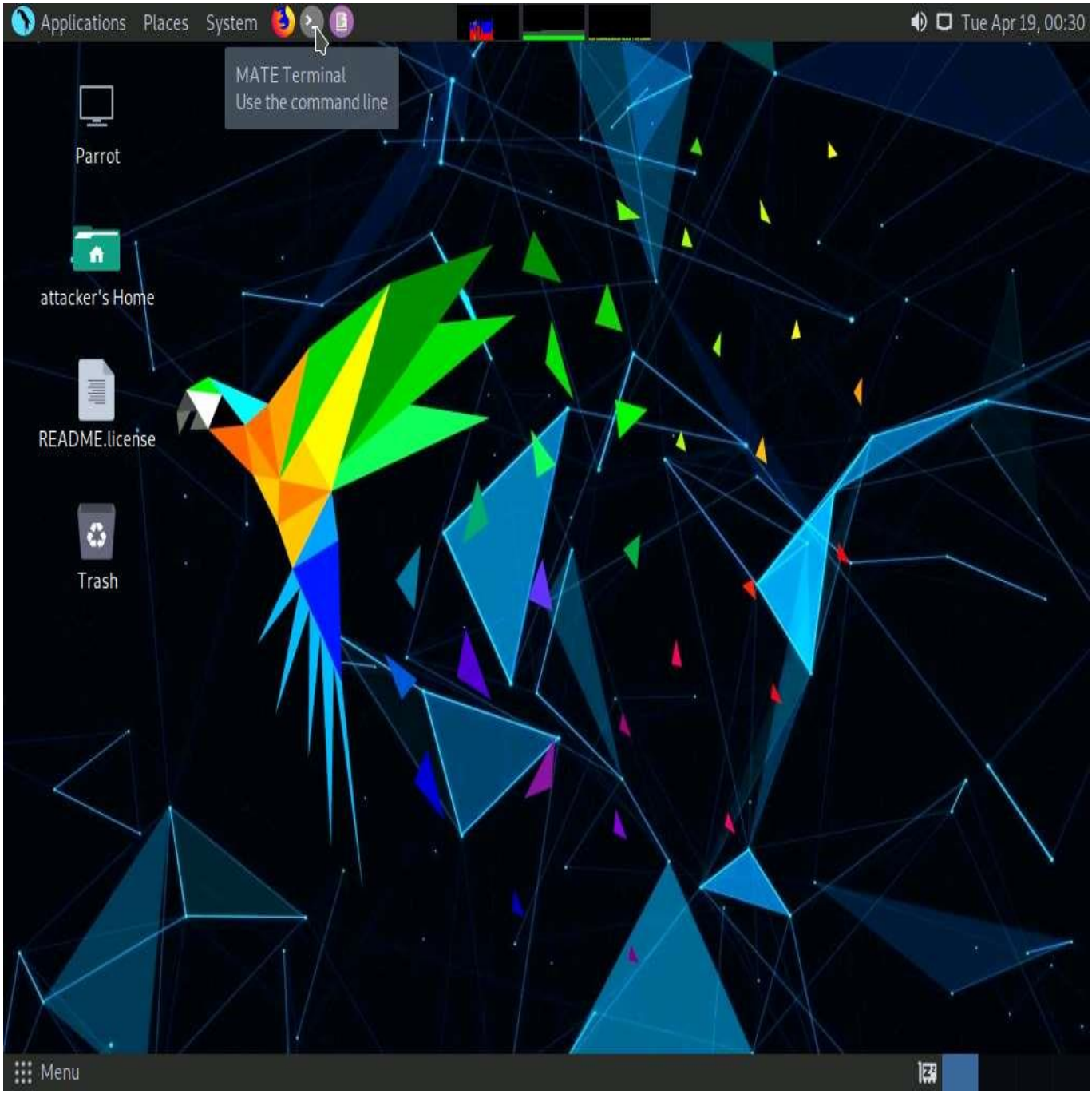
Task 6: Enumerate Web Server Information using Nmap Scripting Engine (NSE)

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.

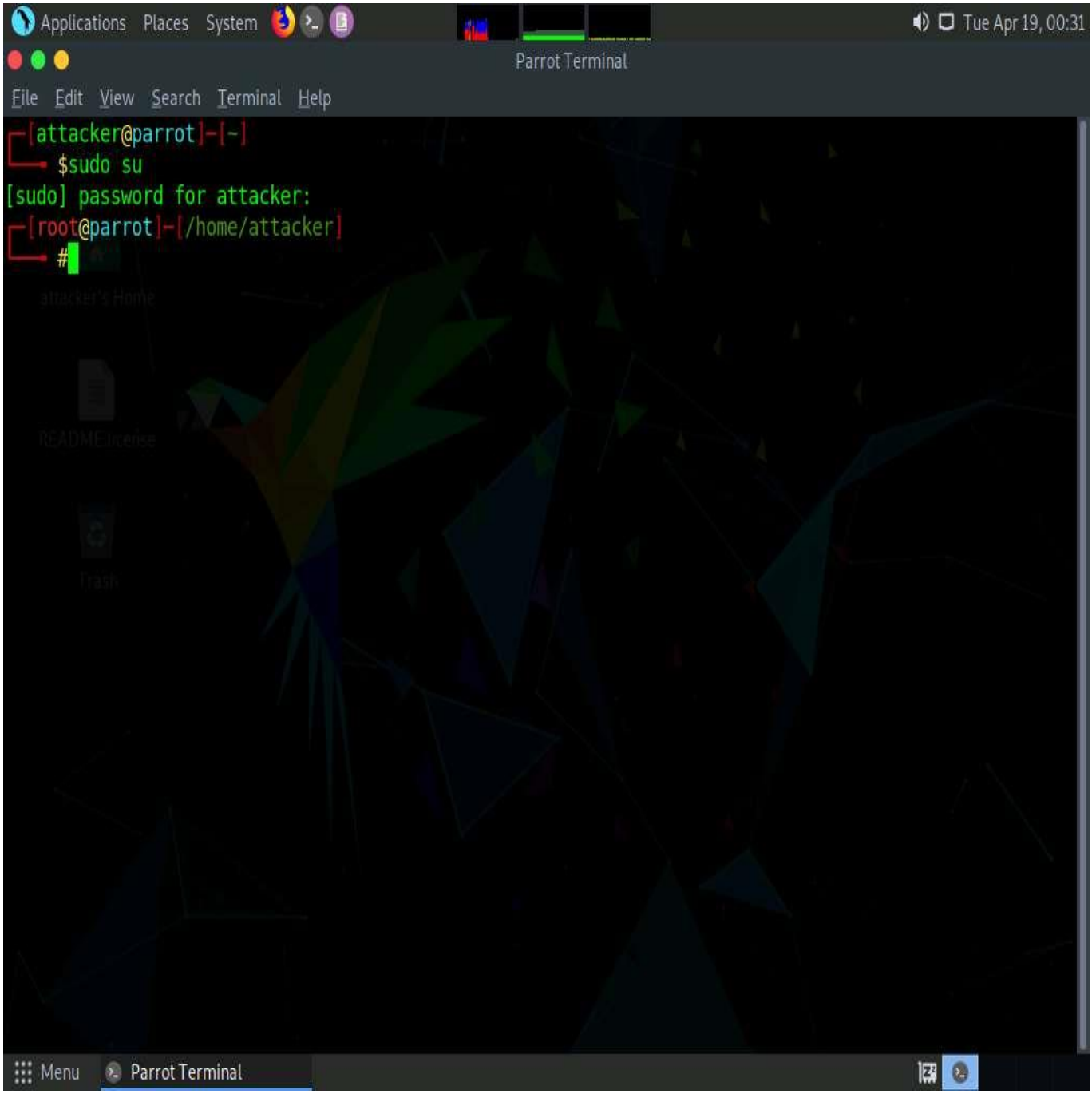
Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE)provides scripts that reveal various useful information about the target web server to an attacker.

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

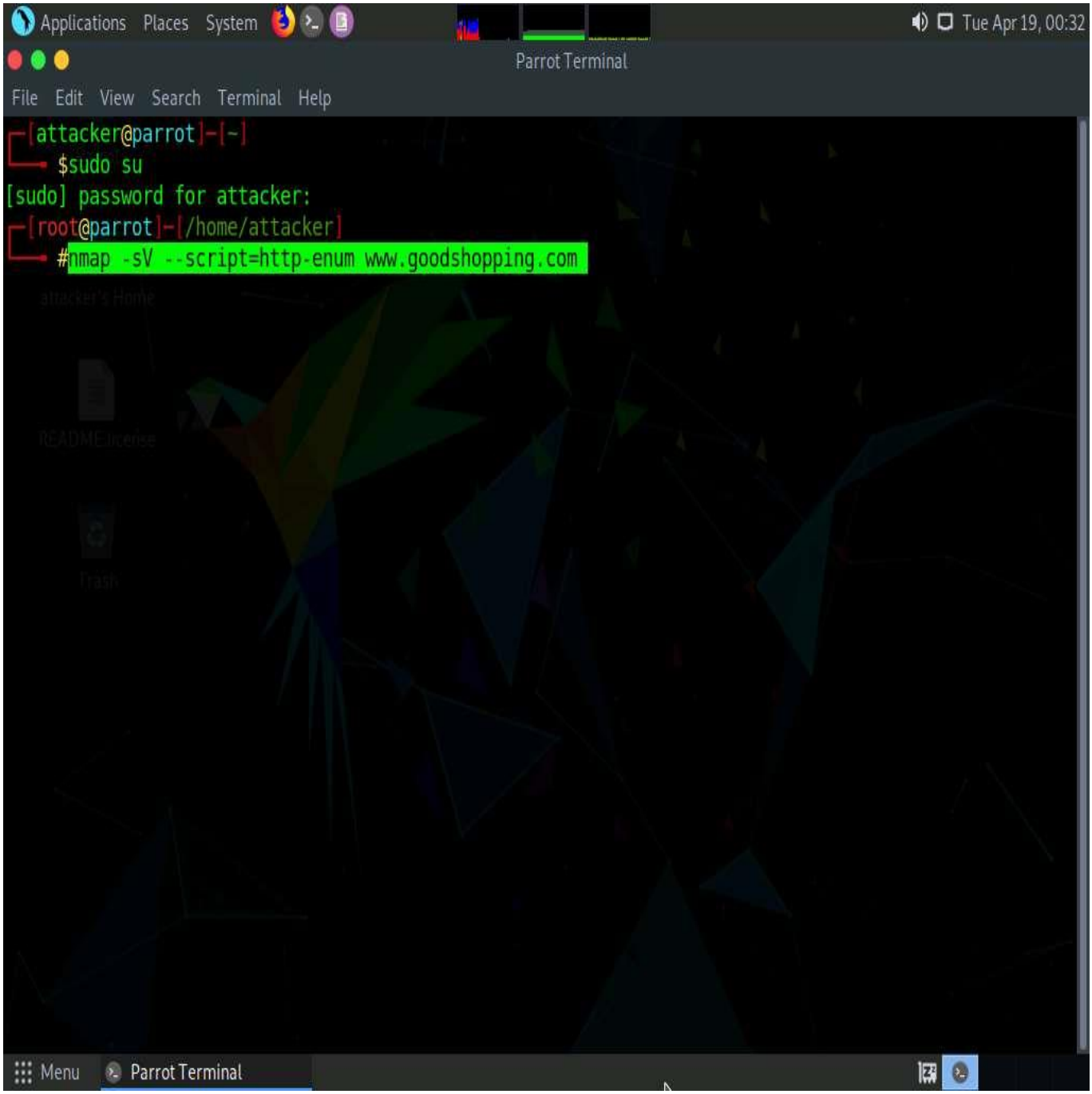


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

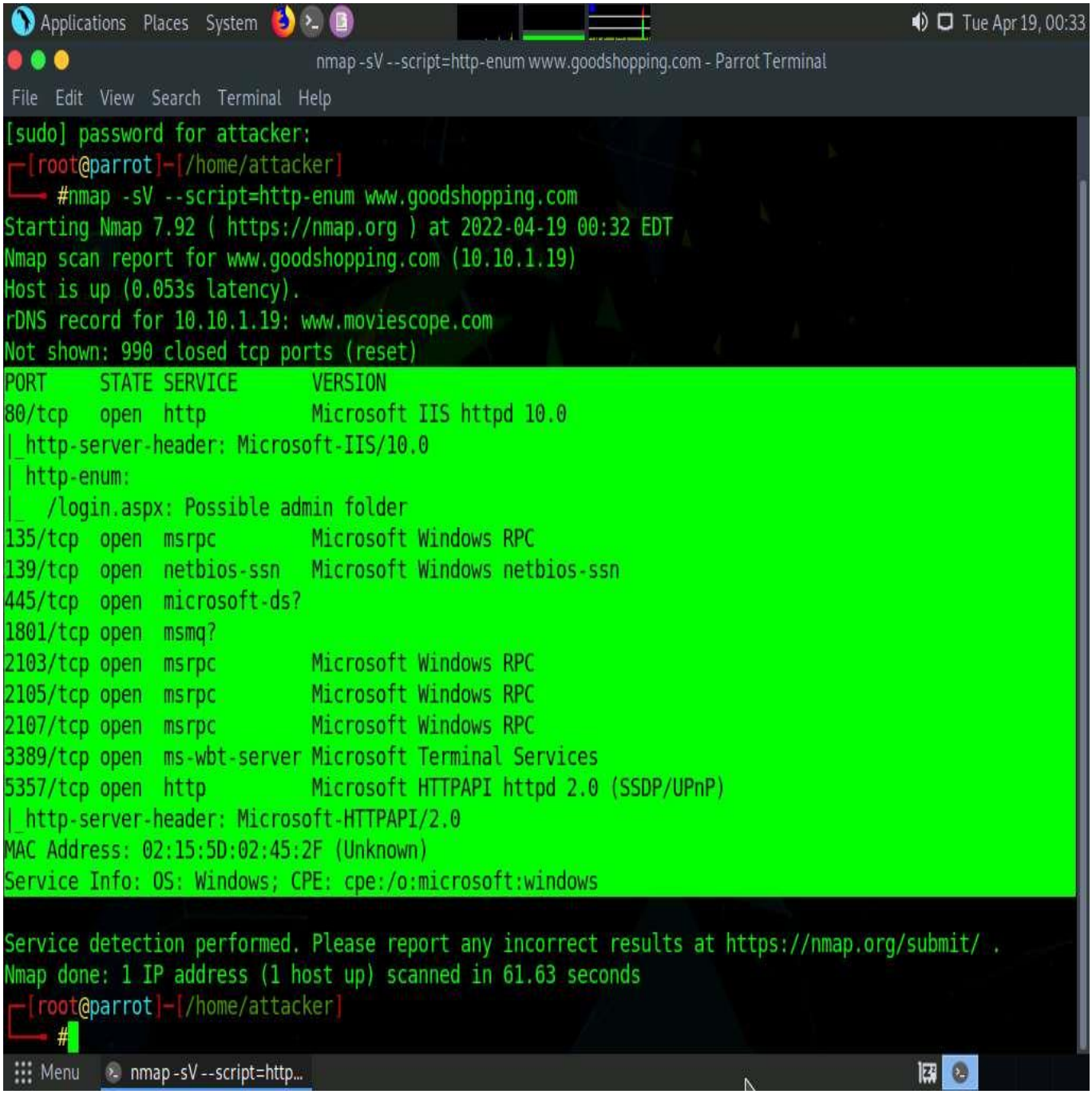
The password that you type will not be visible.



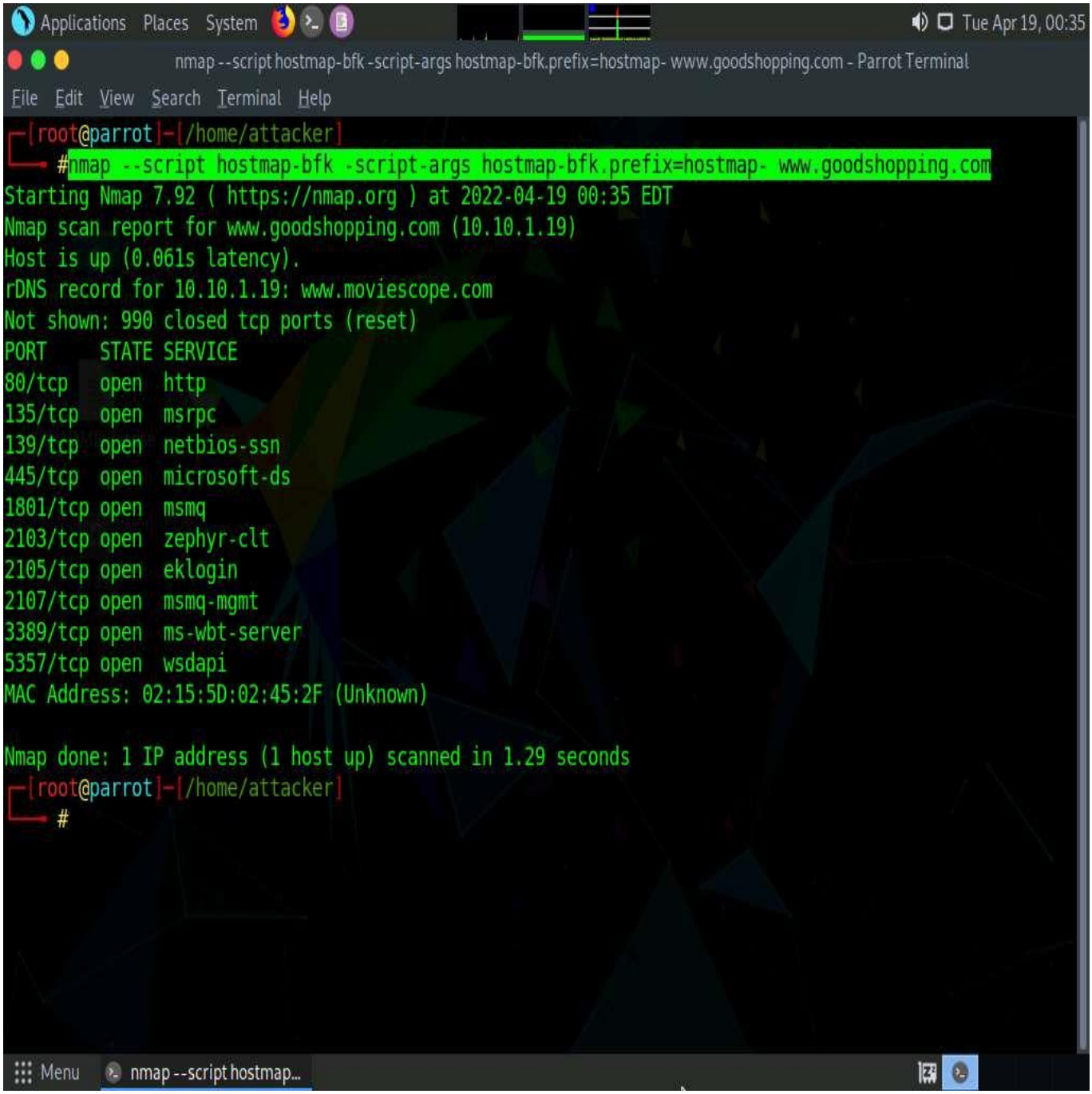
4. ☐ Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum [target website]** and press **Enter**.
5. ☐ In this scan, we are enumerating the **www.goodshopping.com** website.



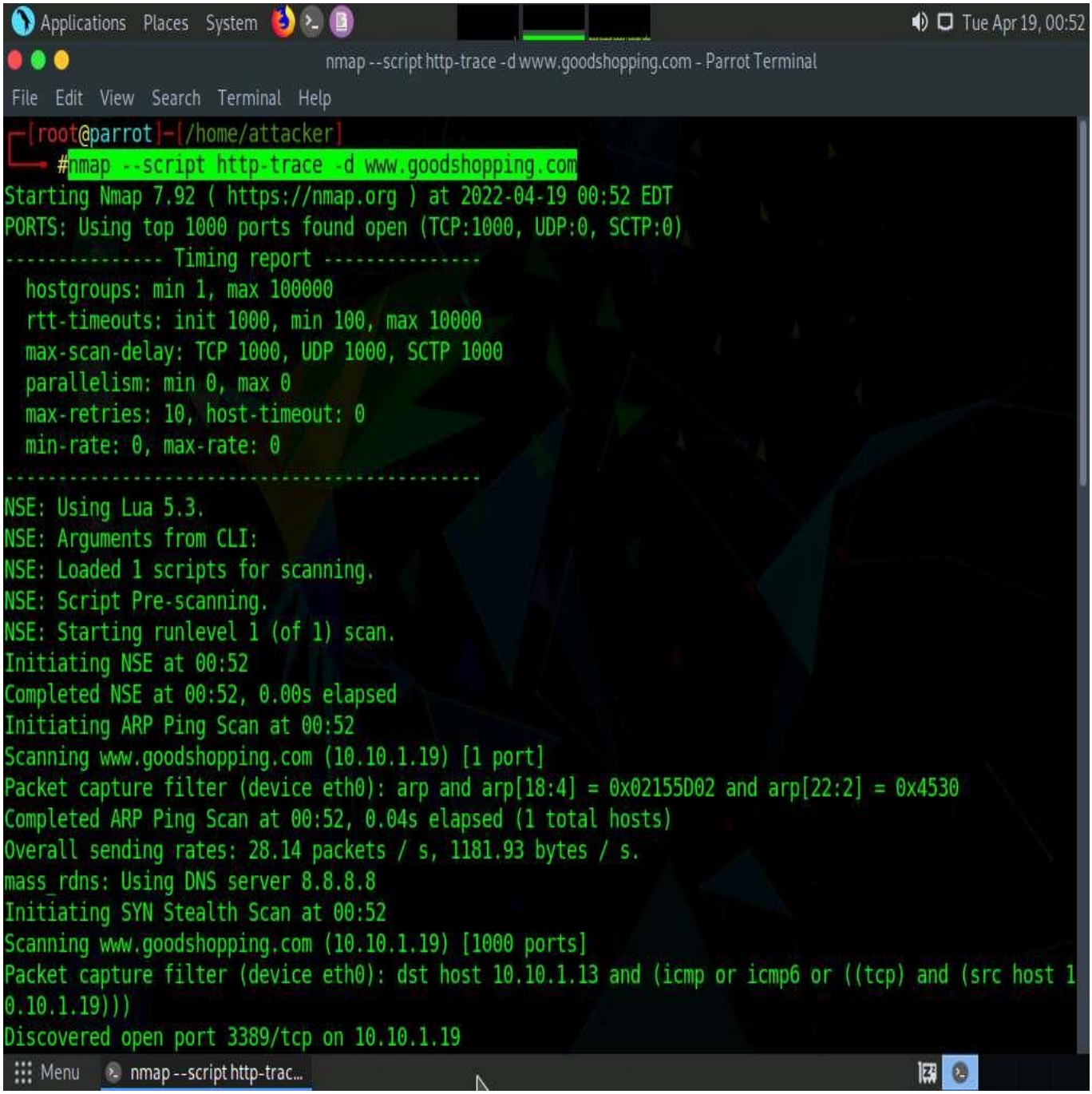
6. This script enumerates and provides you with the output details, as shown in the screenshot.

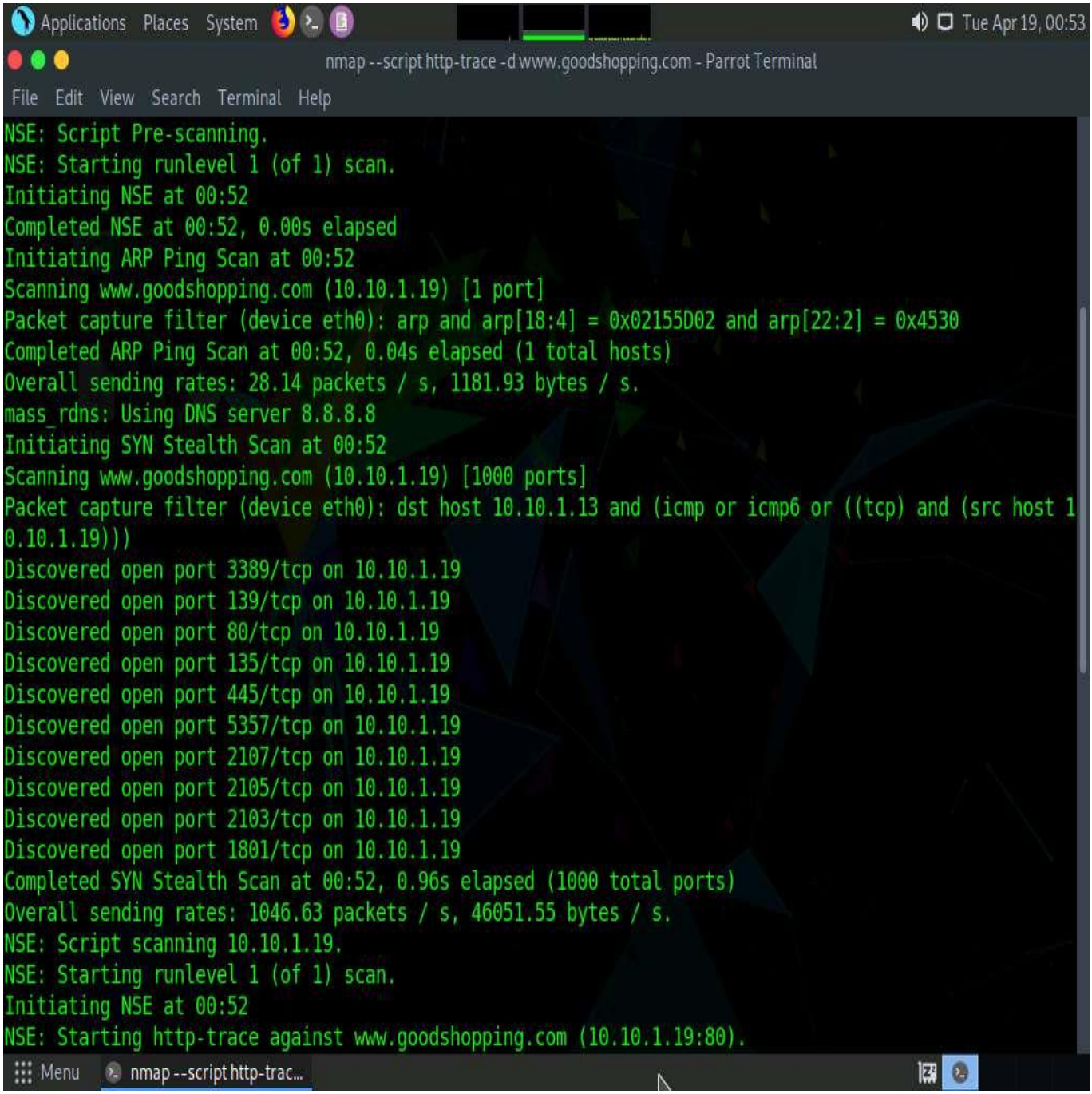


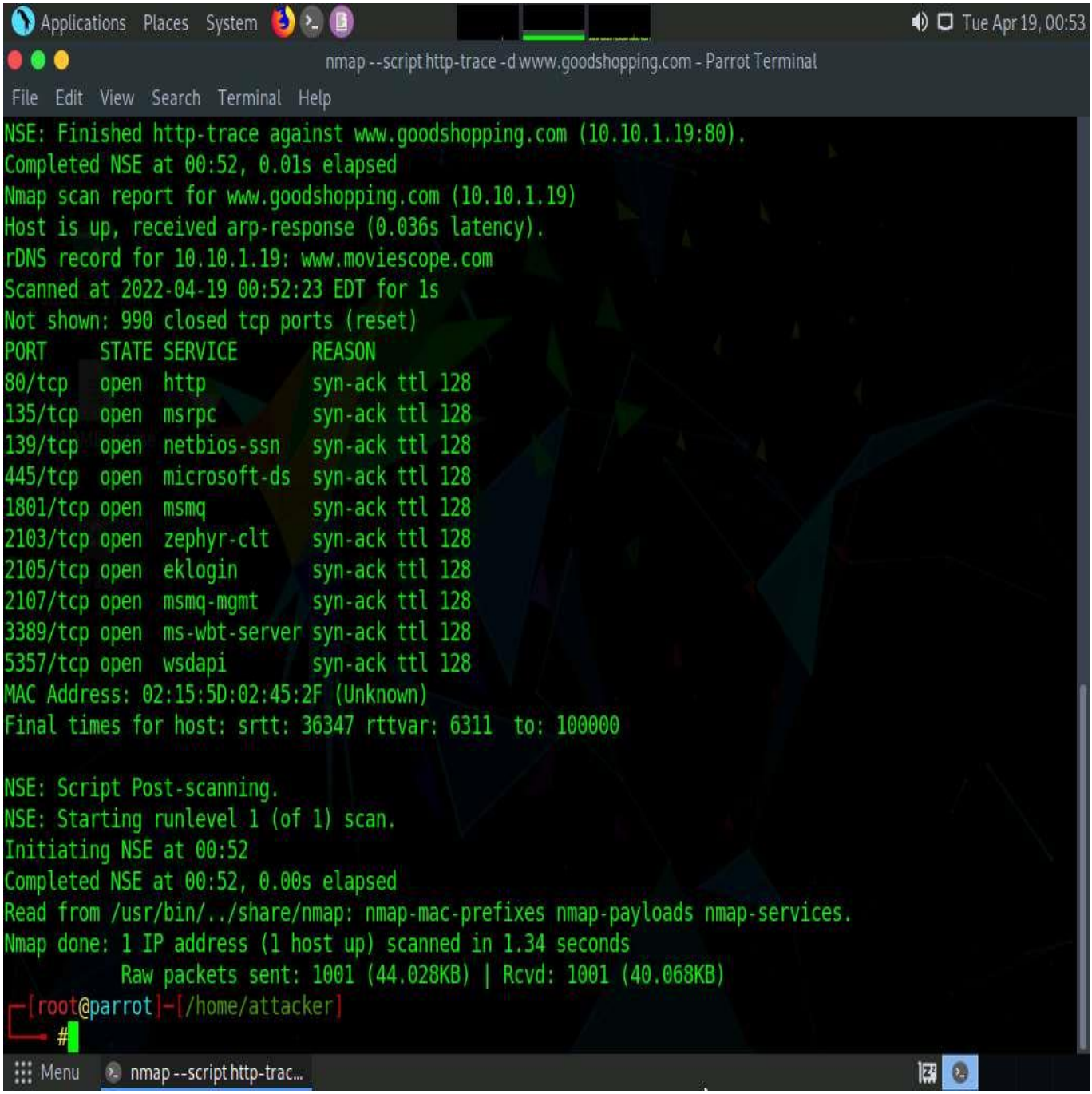
7. ☐ The next step is to discover the hostnames that resolve the targeted domain.
8. ☐ In the terminal window, type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.



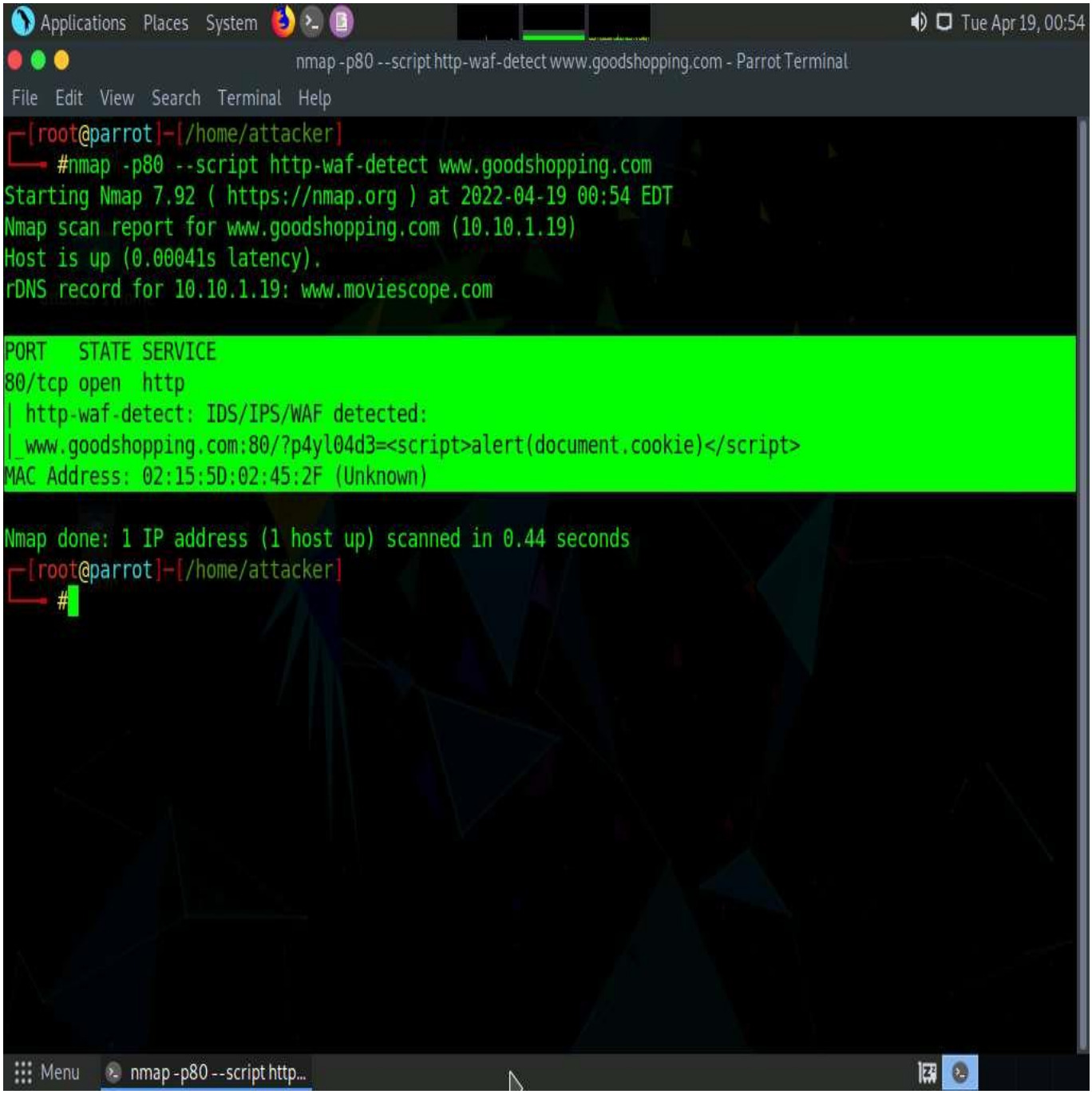
9. ☐ Perform an HTTP trace on the targeted domain. In the terminal window, type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.
10. ☐ This script will detect a vulnerable server that uses the TRACE method by sending an HTTP TRACE request that shows if the method is enabled or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


Applications Places System
Tue Apr 19, 00:52
nmap --script http-trace -d www.goodshopping.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/attacker]
#nmap --script http-trace -d www.goodshopping.com
Starting Nmap 7.92 (https://nmap.org) at 2022-04-19 00:52 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
-------------- Timing report --------------
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 1 scripts for scanning.
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
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: 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...



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.

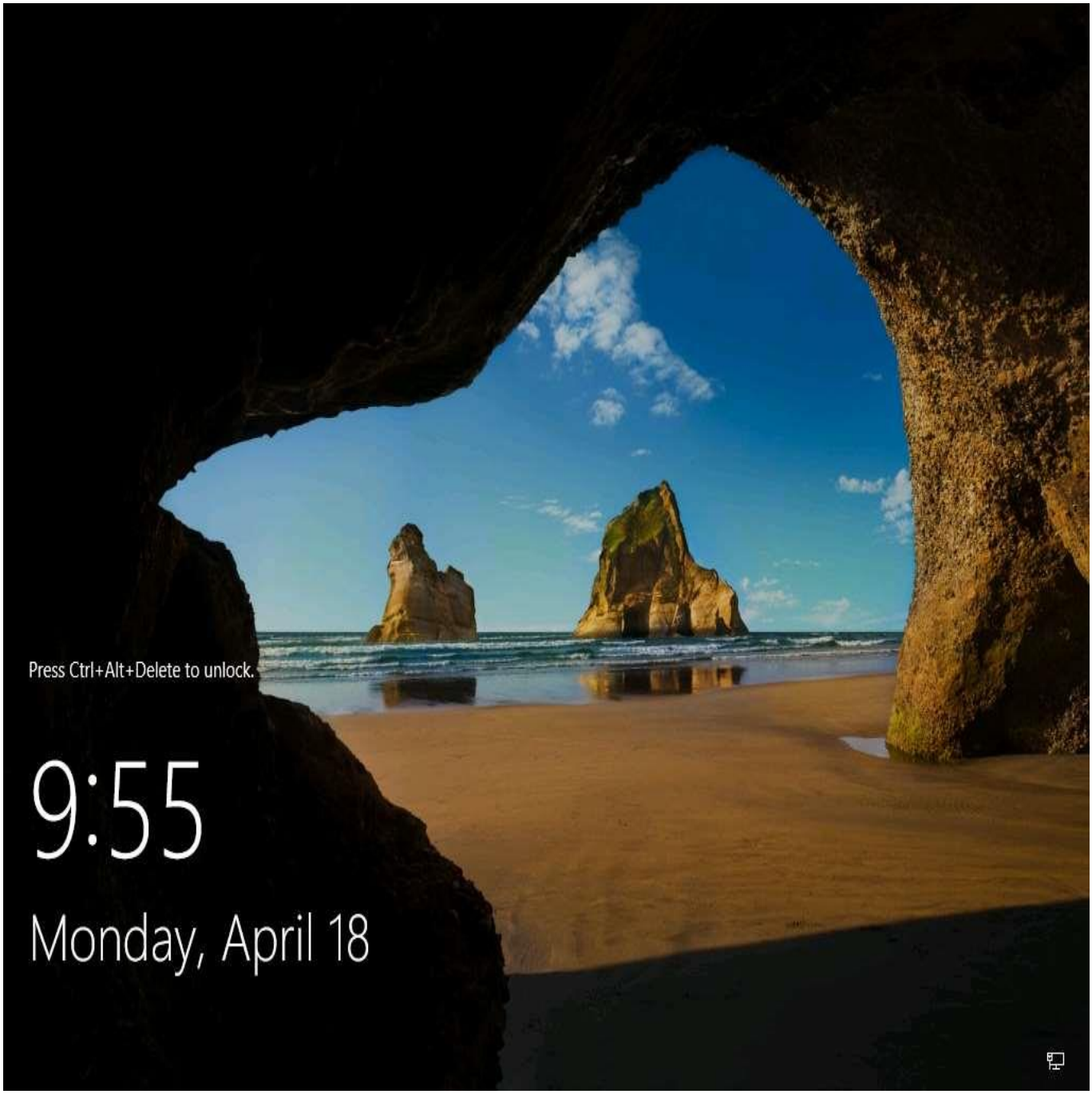


14. ☐ This concludes the demonstration of how to enumerate web server information using the Nmap Scripting Engine (NSE).
15. ☐ Close the terminal windows on the **Parrot Security** machine.

Task 7: Uniscan Web Server Fingerprinting in Parrot Security

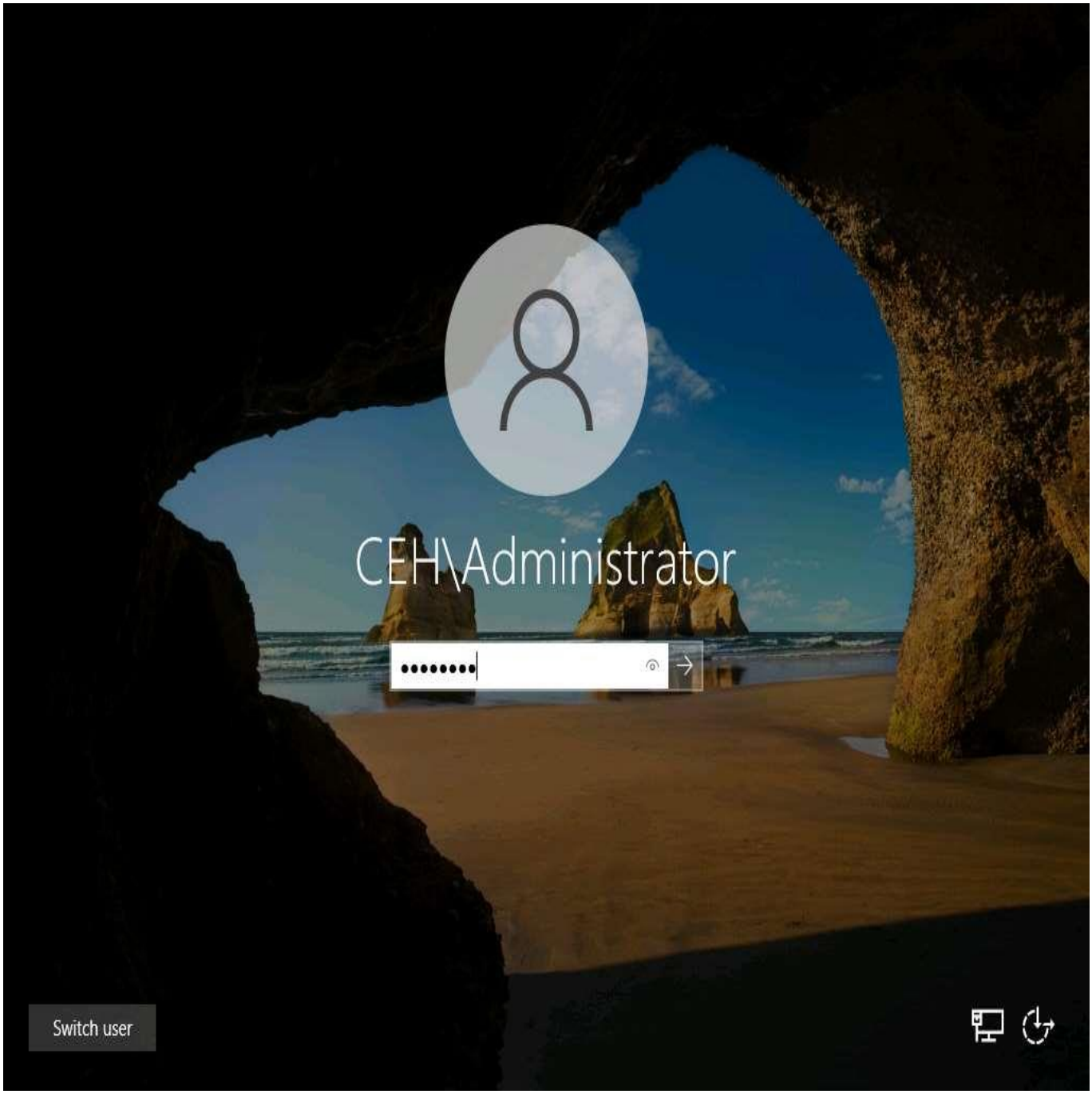
Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan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

1. ☐ Click Windows Server 2022 to switch to the **Windows Server 2022** machine.

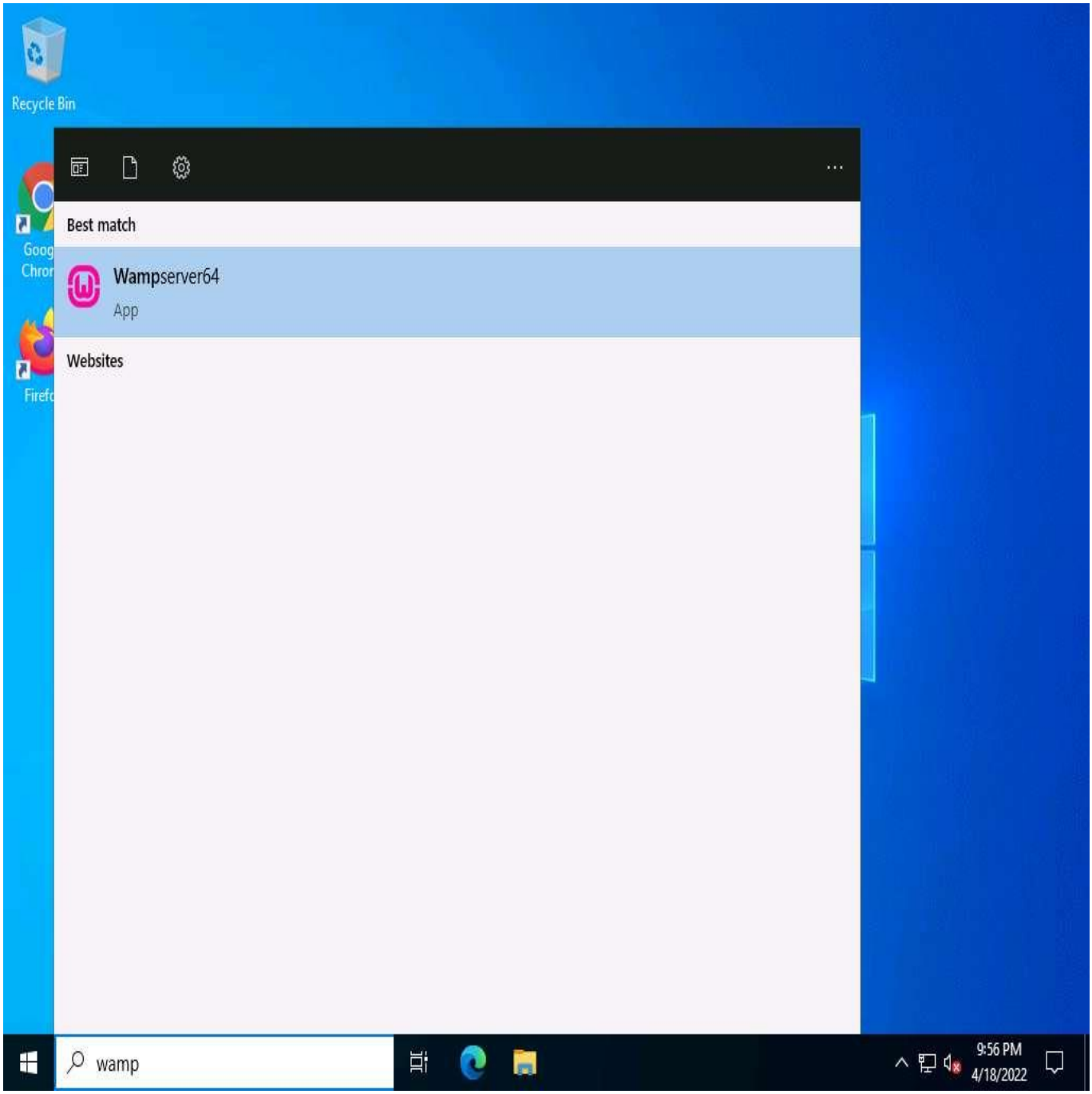


2. Click Ctrl+Alt+Delete to activate the machine. By default, **CEH\Administrator** user profile is selected, click Pa$$w0rd to paste the password in the Password field and press **Enter** to login.

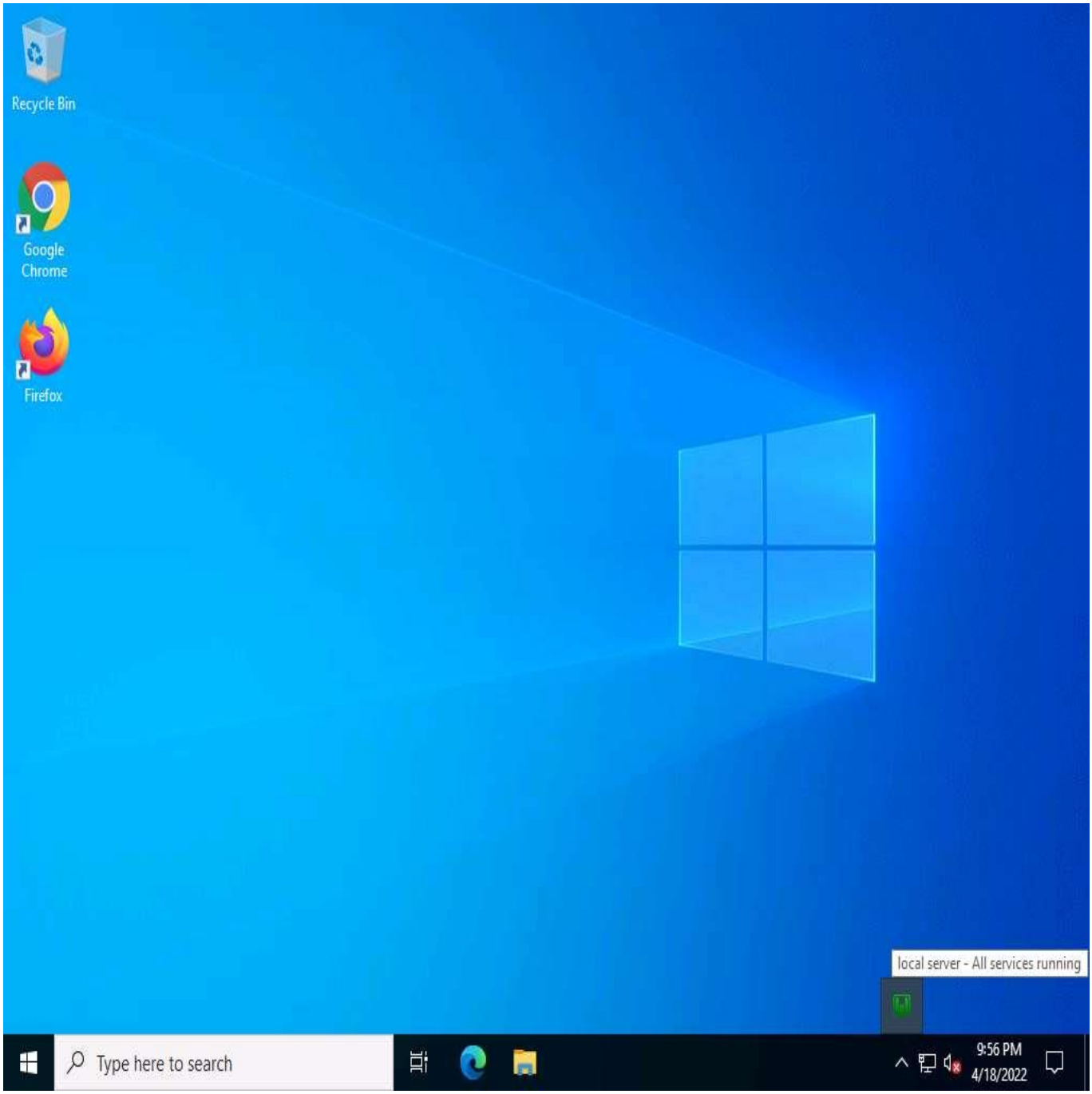
Alternatively, you can also click **Pa$$w0rd** under **Windows Server 2022** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.



3. Click **Type here to search** field and type **wamp**. **Wamperserver64** appears in the result, press **Enter** to launch it.

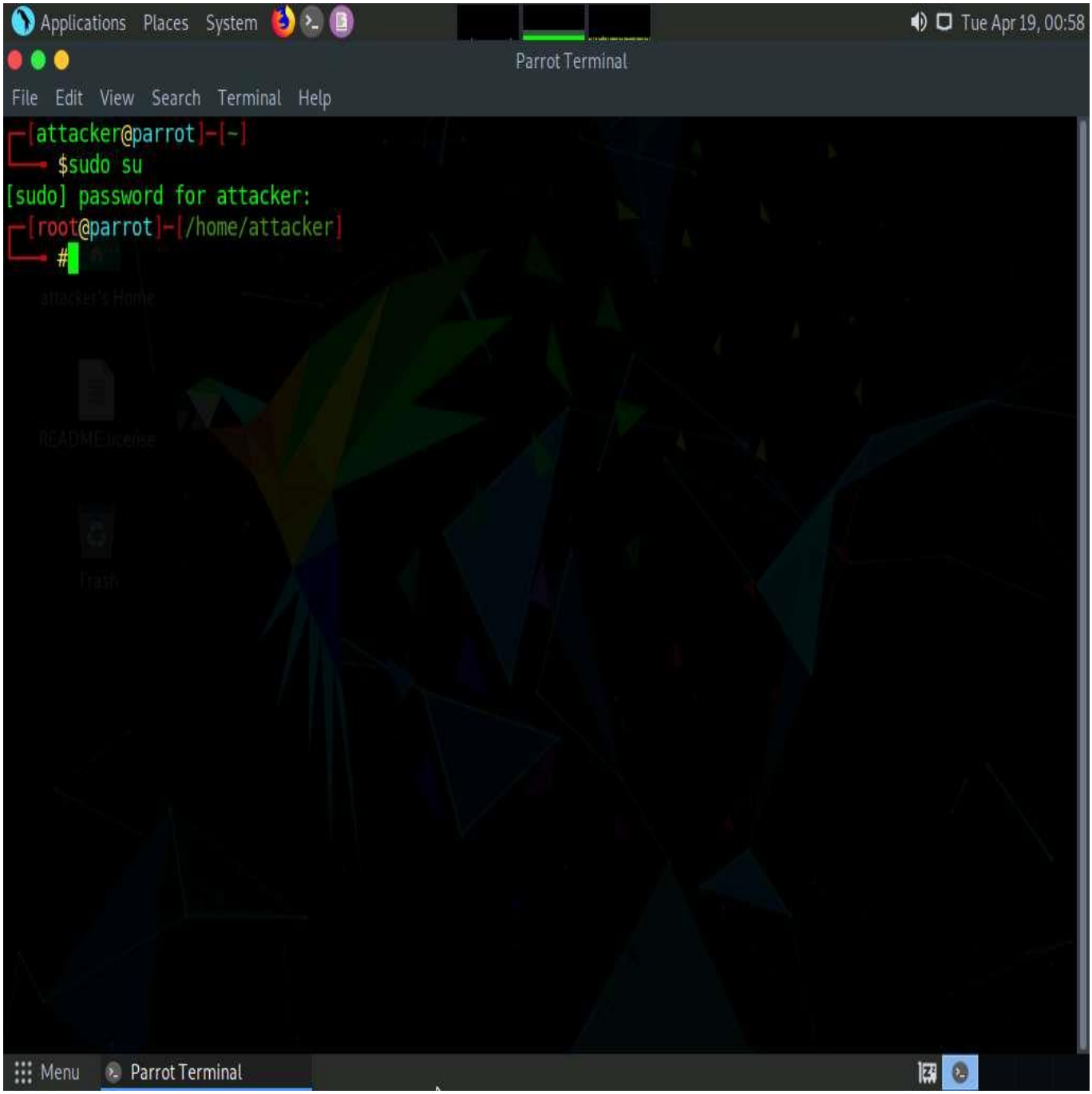


4. ☐ Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2022** machine running.

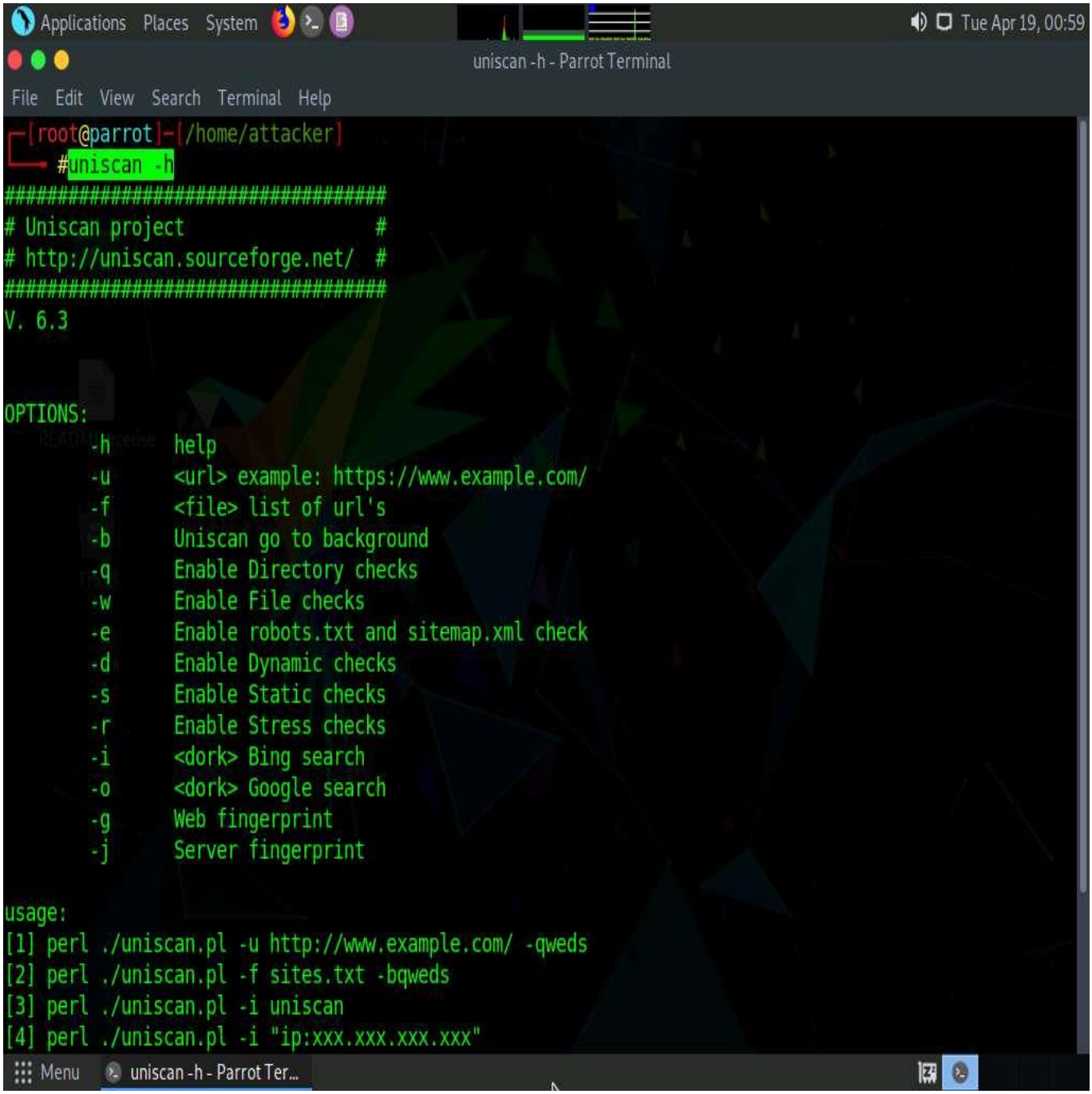


5. ☐ Leave the **Windows Server 2022** machine running and switch to the **Parrot Security** machine.
6. ☐ Now, click Parrot Security to switch to the **Parrot Security** machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
7. ☐ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

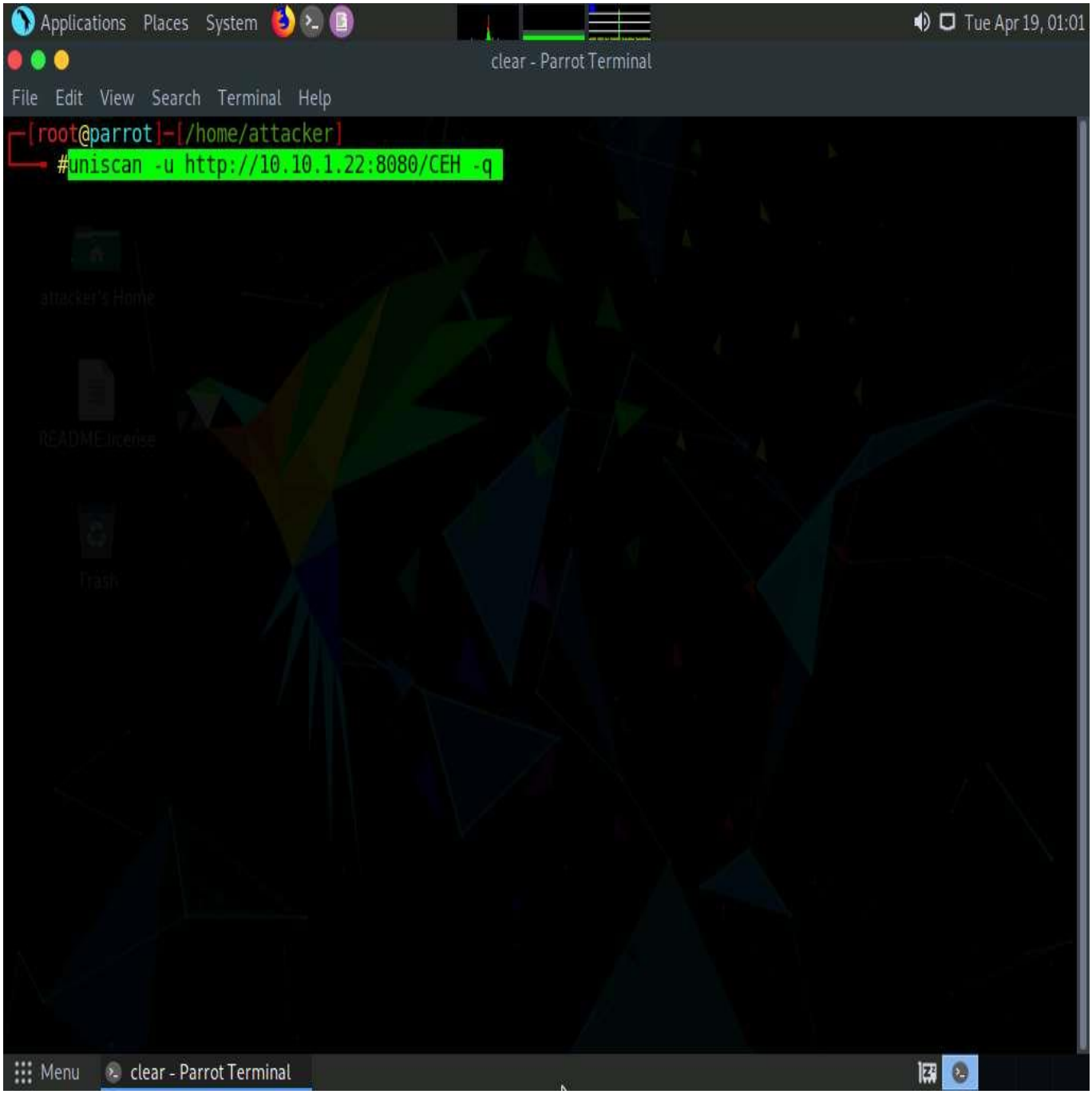
The password that you type will not be visible.



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.

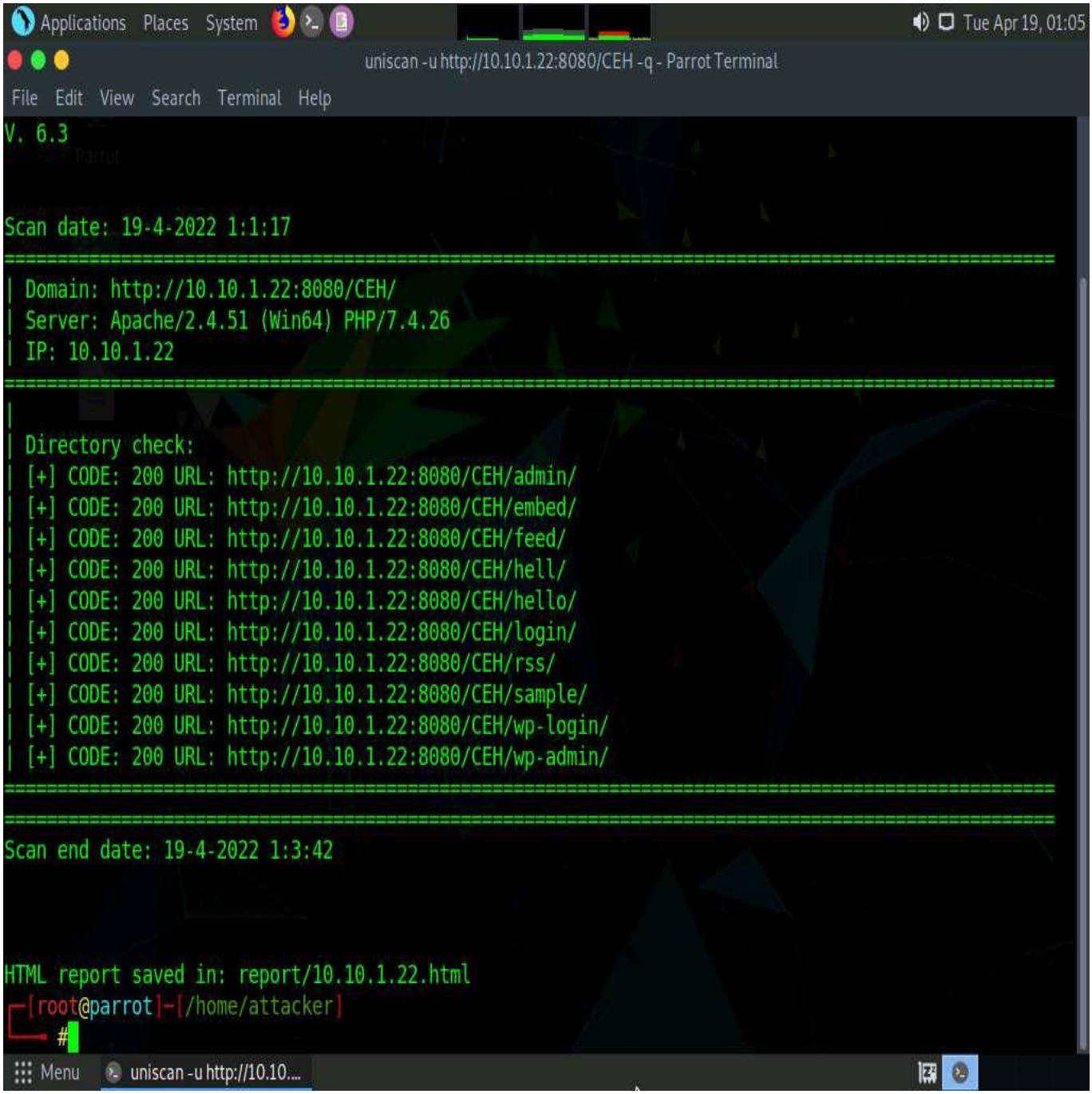


10. In the terminal window, type **uniscan -u http://10.10.1.22:8080/CEH -q** and hit **Enter** to start scanning for directories.
11. Here, **10.10.1.22** is the IP address of the **Windows Server 2022** machine. This may vary in your lab environment.
12. In the above command, the **-u** switch is used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

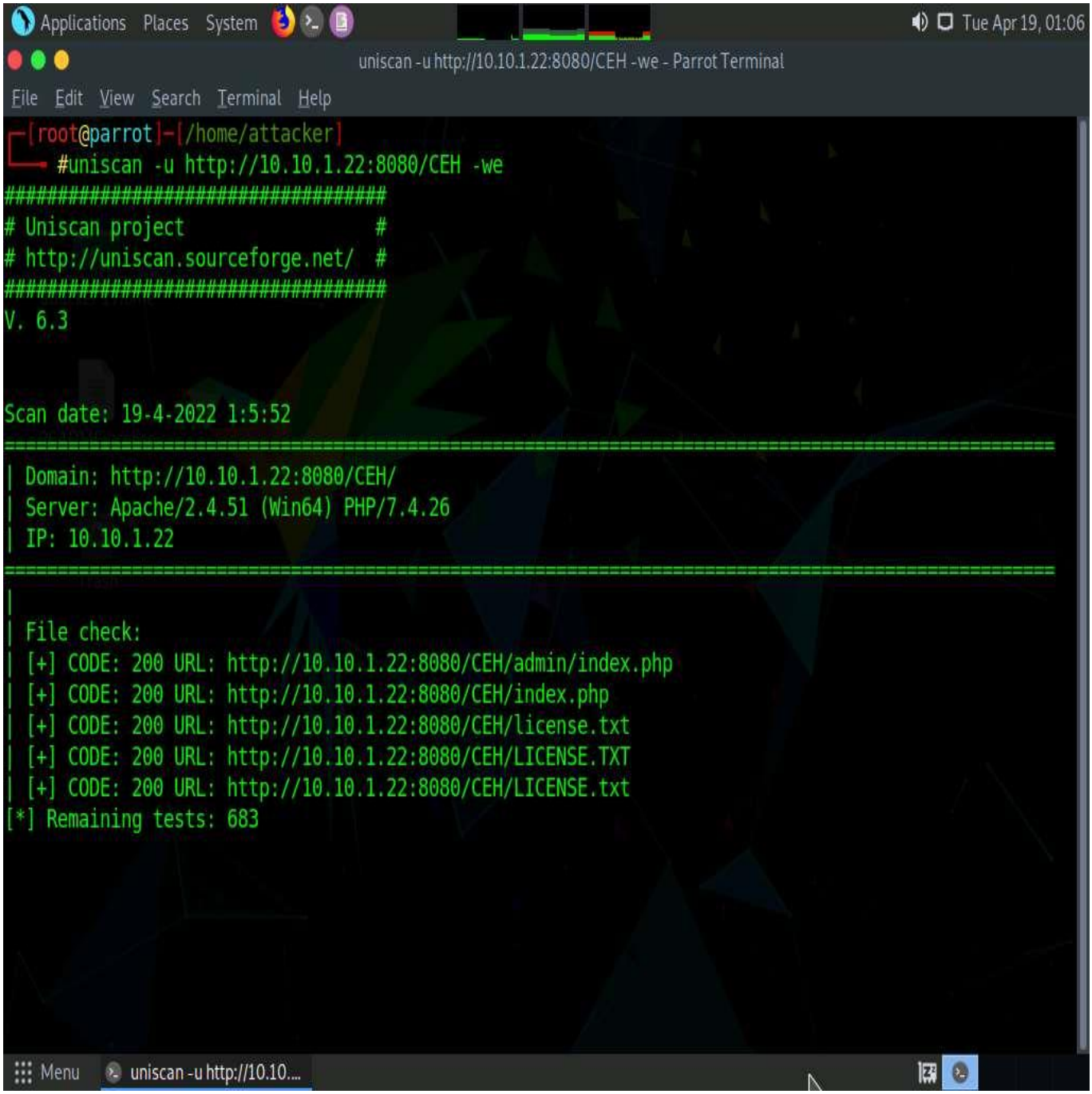


13. Uniscan starts performing different tests on the webserver and discovering **web directories**, as shown in the screenshot.

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

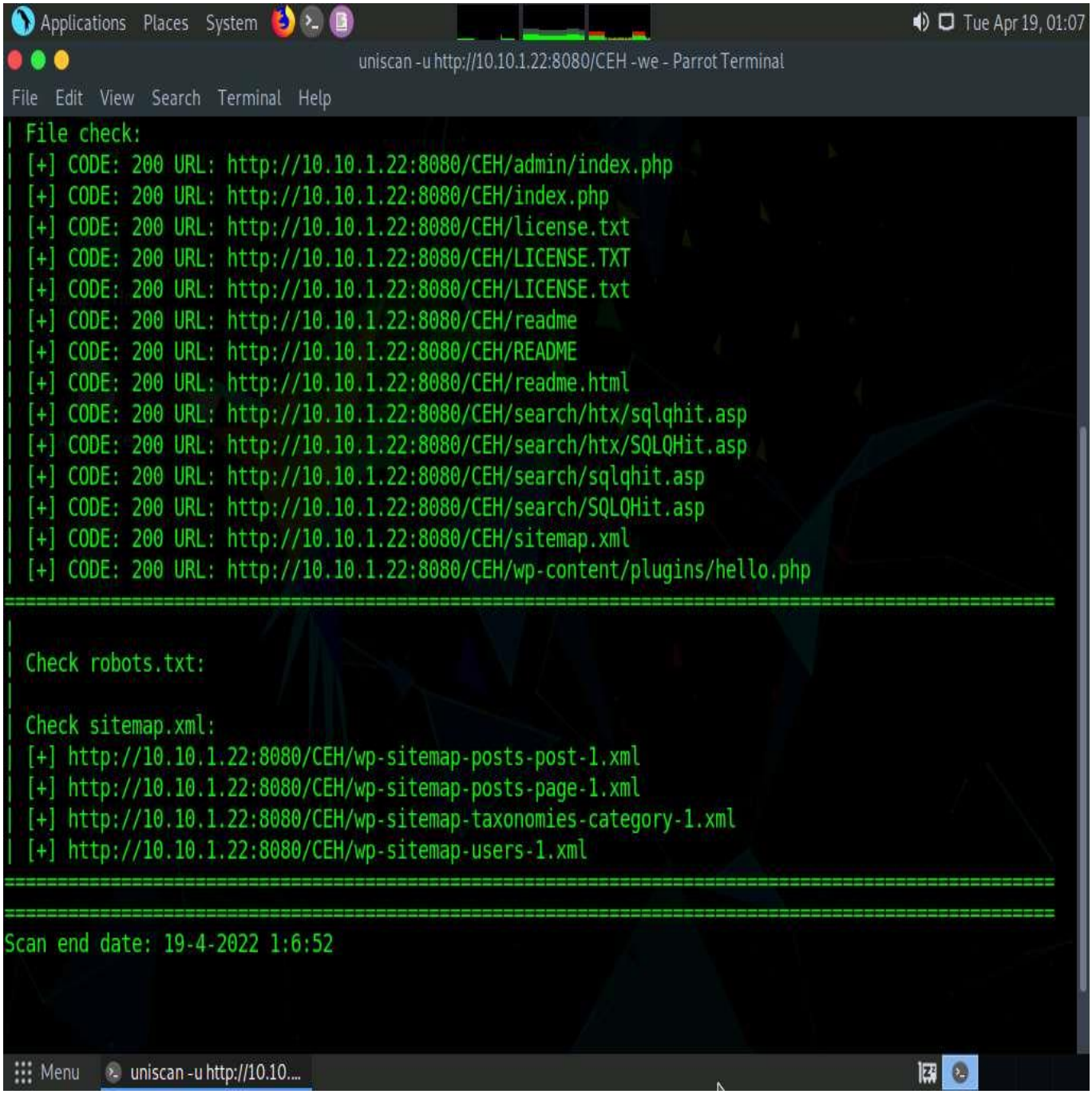


14. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (**robots.txt** and **sitemap.xml** file). In the **terminal** window, type **uniscan -u http://10.10.1.22:8080/CEH -we** and hit **Enter** to start the scan.

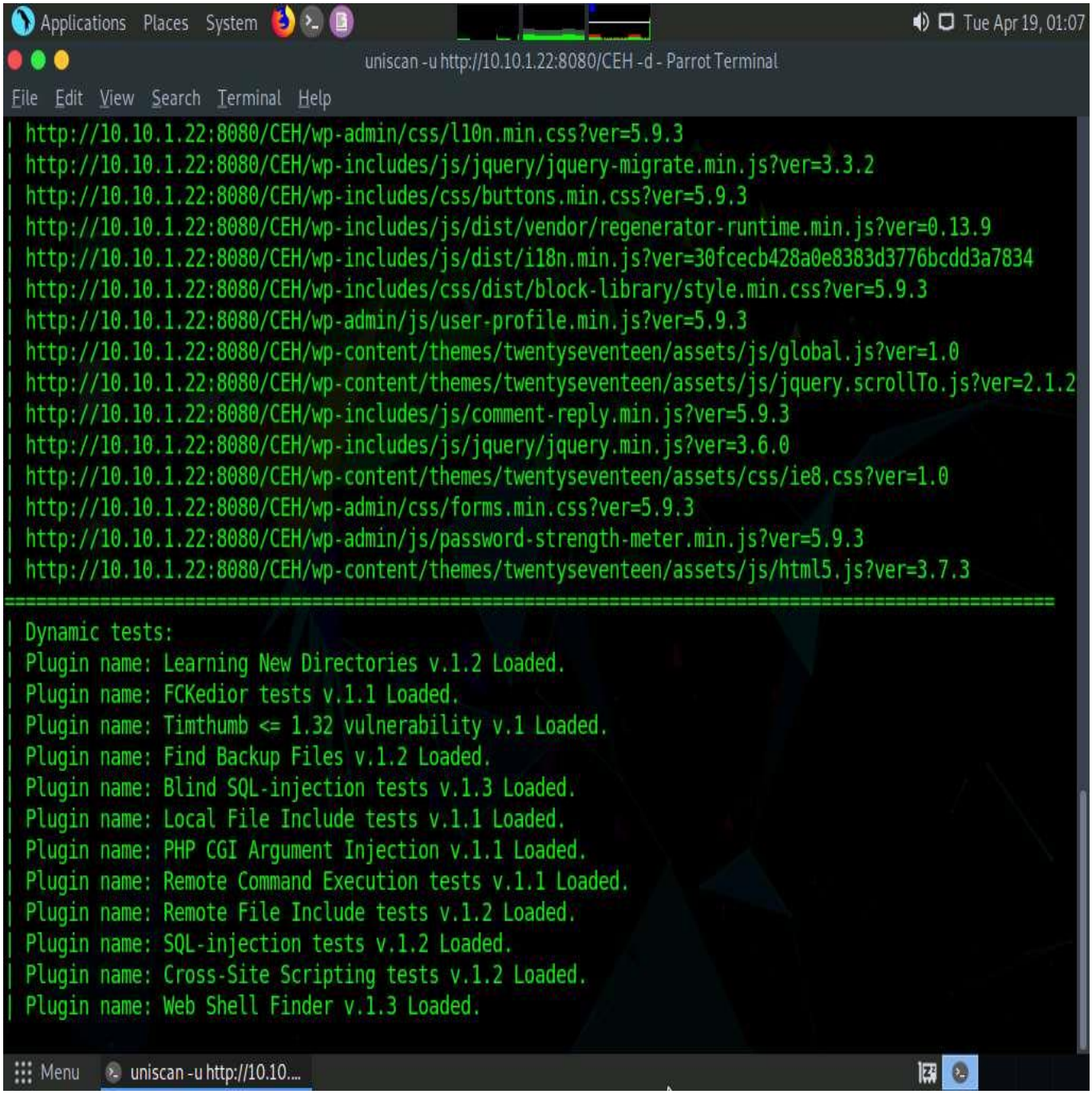


15. Uniscan starts the file check and displays the results, as shown in the screenshot.

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

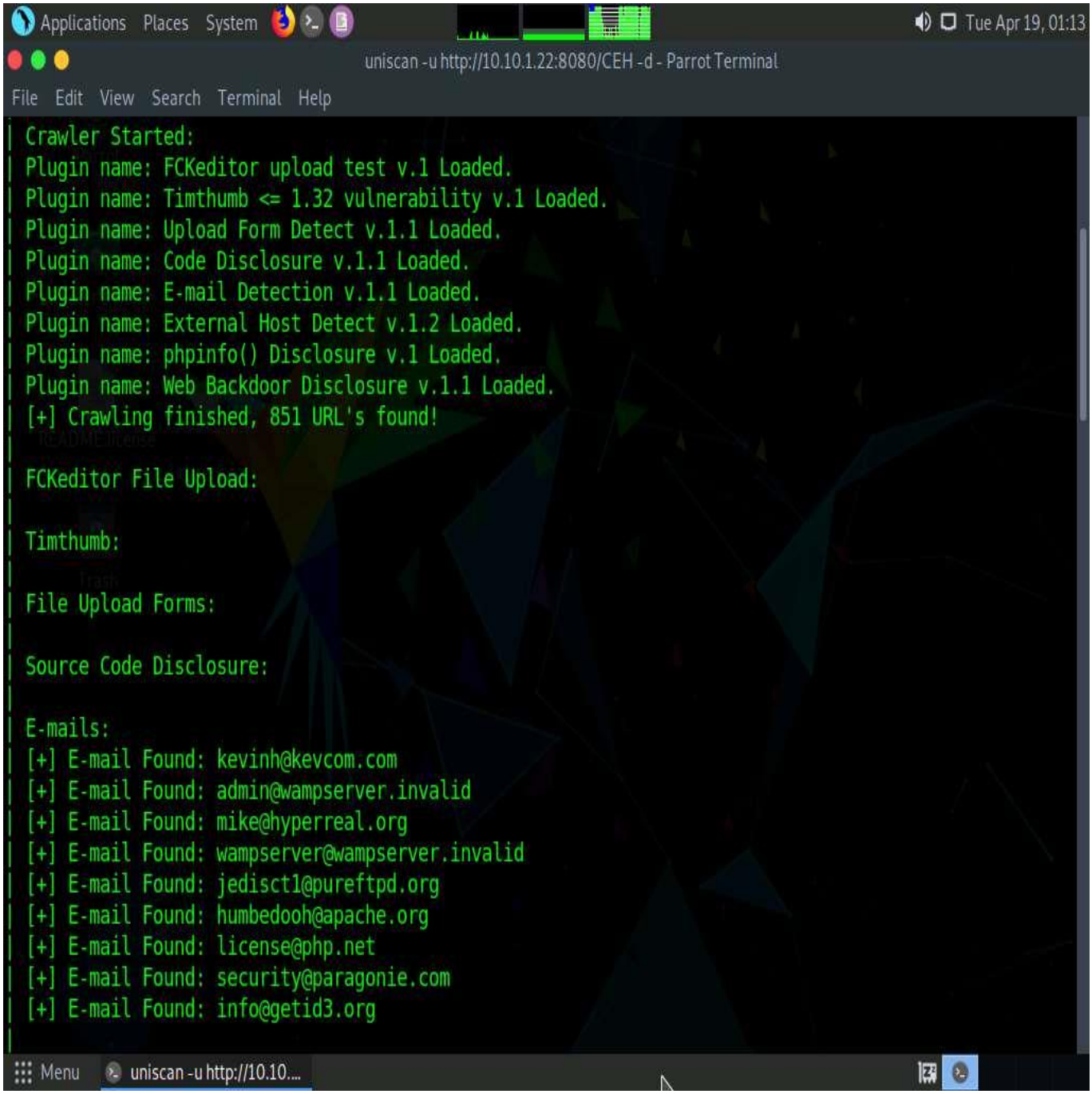


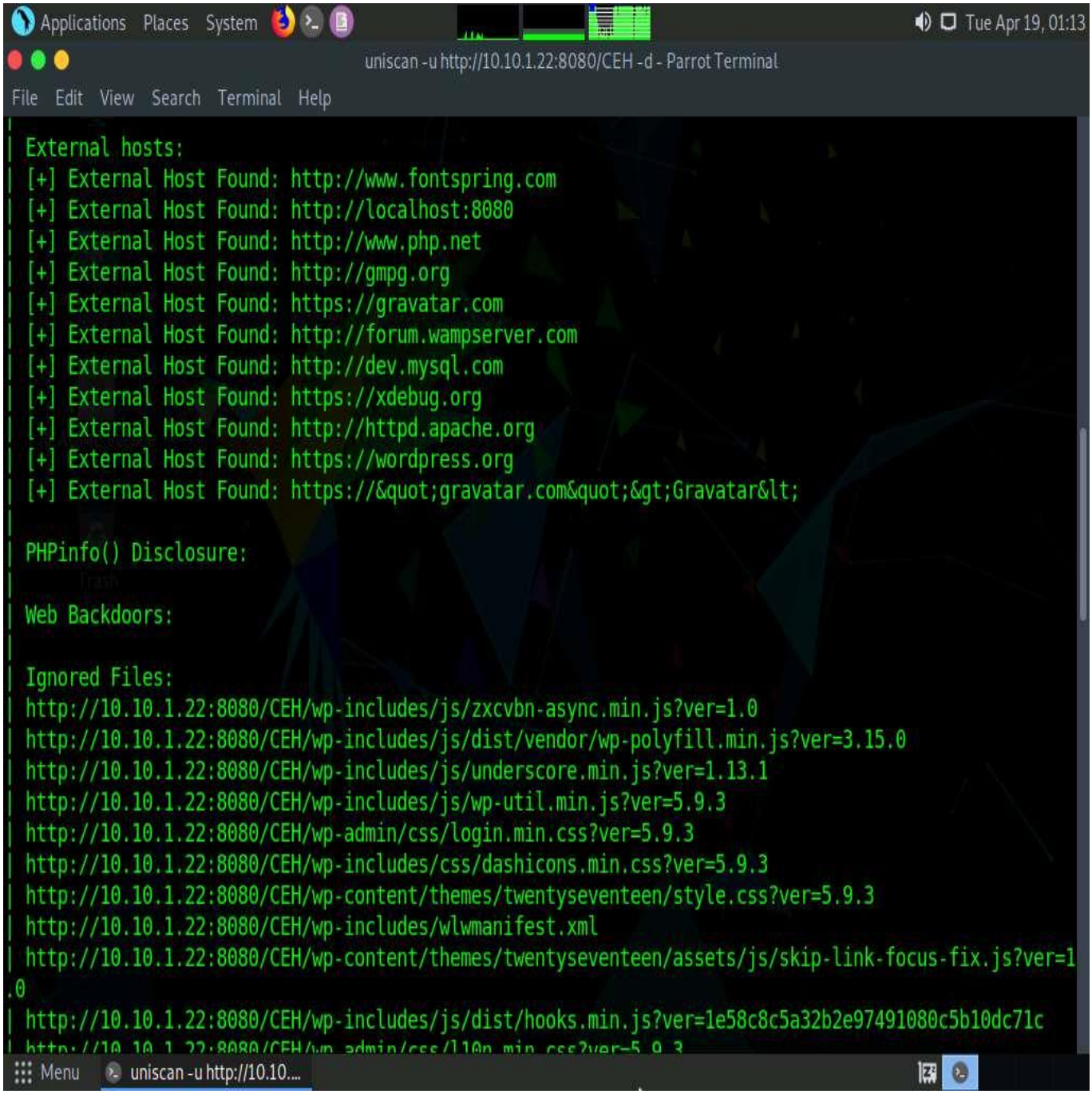
16. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.1.22:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

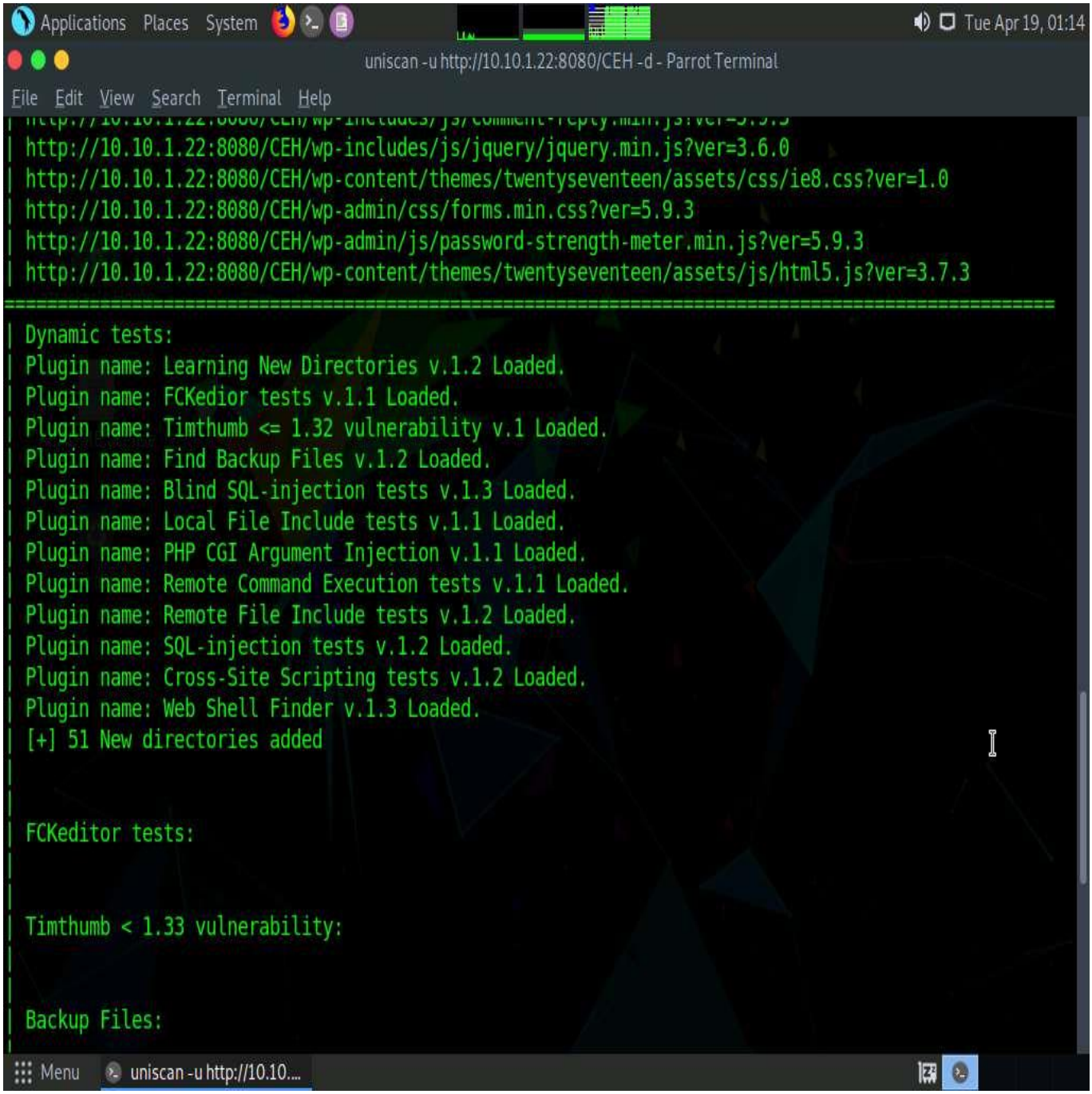


17. Uniscan starts performing dynamic tests, obtaining more information about email-IDs, Source code disclosures, and external hosts, web backdoors, dynamic tests.

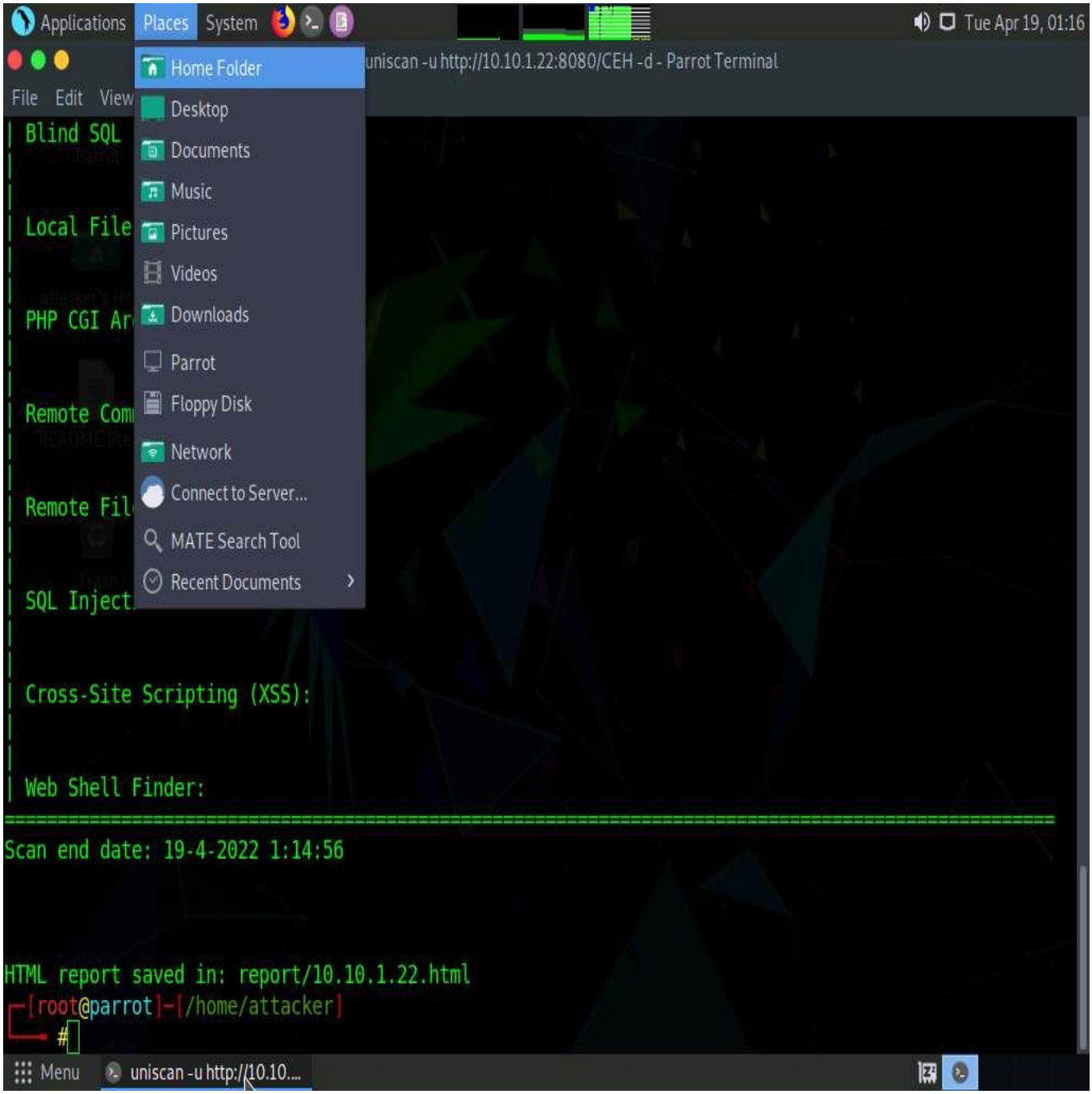
Scroll to analyze the complete output of the scan. It should take approximately 18 minutes for the scan to finish.


Applications Places System
Tue Apr 19, 01:13
uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
| Crawler Started:
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| [+] Crawling finished, 851 URL's found!
|
| FCKeditor File Upload:
|
| Timthumb:
|
| File Upload Forms:
|
| Source Code Disclosure:
|
| E-mails:
| [+] E-mail Found: kevinh@kevcom.com
| [+] E-mail Found: admin@wampserver.invalid
| [+] E-mail Found: mike@hyperreal.org
| [+] E-mail Found: wampserver@wampserver.invalid
| [+] E-mail Found: jedisct1@pureftpd.org
| [+] E-mail Found: humbedooh@apache.org
| [+] E-mail Found: license@php.net
| [+] E-mail Found: security@paragonie.com
| [+] E-mail Found: info@getid3.org
|
Menu
uniscan -u http://10.10....

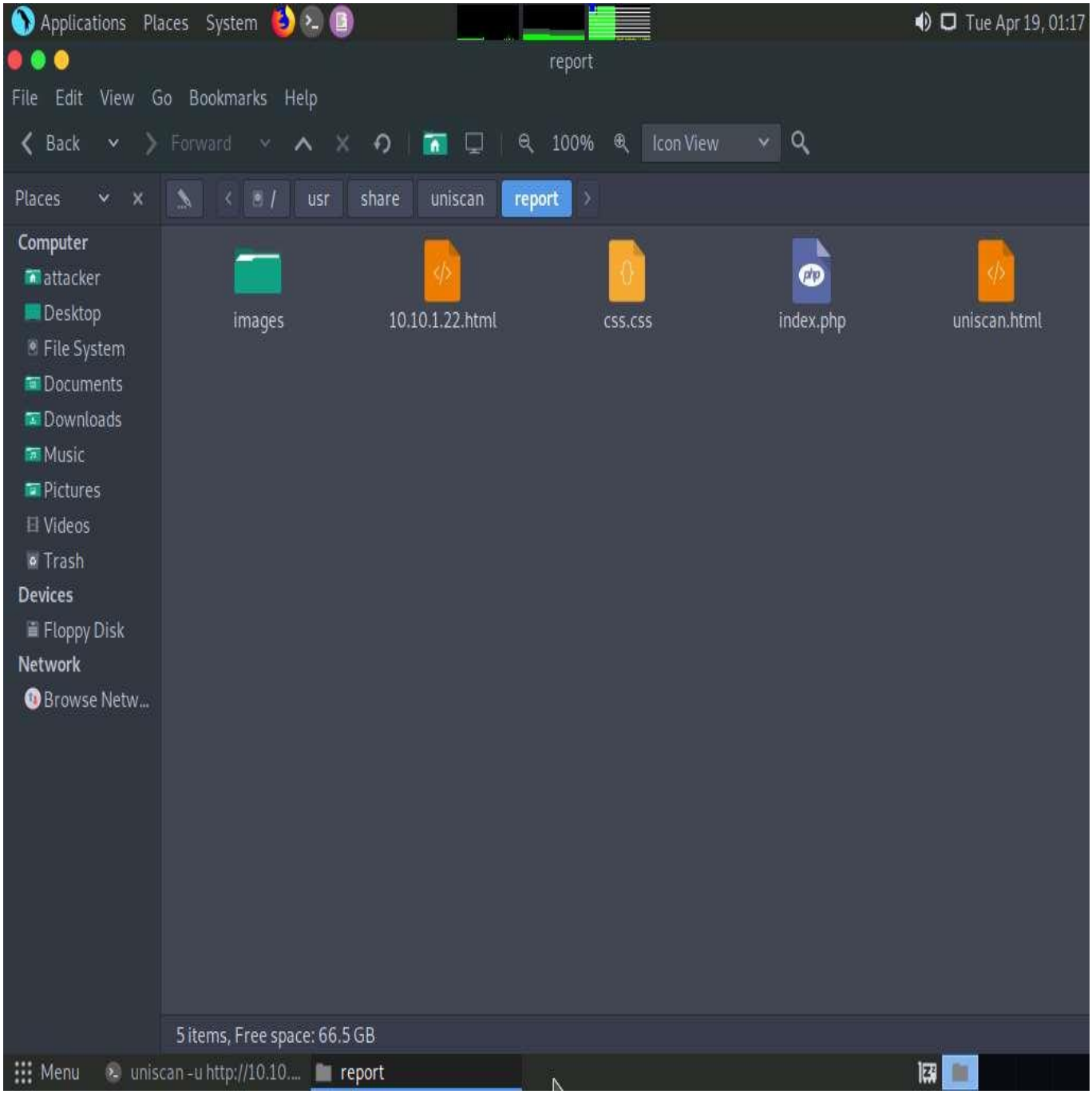

Applications Places System
Tue Apr 19, 01:13
uniscan -u http://10.10.1.22:8080/CEH -d - Parrot Terminal
File Edit View Search Terminal Help
| External hosts:
| [+] External Host Found: http://www.fontspring.com
| [+] External Host Found: http://localhost:8080
| [+] External Host Found: http://www.php.net
| [+] External Host Found: http://gmpg.org
| [+] External Host Found: https://gravatar.com
| [+] External Host Found: http://forum.wampserver.com
| [+] External Host Found: http://dev.mysql.com
| [+] External Host Found: https://xdebug.org
| [+] External Host Found: http://httpd.apache.org
| [+] External Host Found: https://wordpress.org
| [+] External Host Found: https://"gravatar.com">Gravatar<
|
| PHPinfo() Disclosure:
|
| Web Backdoors:
|
| Ignored Files:
| http://10.10.1.22:8080/CEH/wp-includes/js/zxcvbn-async.min.js?ver=1.0
| http://10.10.1.22:8080/CEH/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
| http://10.10.1.22:8080/CEH/wp-includes/js/underscore.min.js?ver=1.13.1
| http://10.10.1.22:8080/CEH/wp-includes/js/wp-util.min.js?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-admin/css/login.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-includes/css/dashicons.min.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/style.css?ver=5.9.3
| http://10.10.1.22:8080/CEH/wp-includes/wlwmanifest.xml
| http://10.10.1.22:8080/CEH/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1
.0
| http://10.10.1.22:8080/CEH/wp-includes/js/dist/hooks.min.js?ver=1e58c8c5a32b2e97491080c5b10dc71c
Menu
uniscan -u http://10.10....



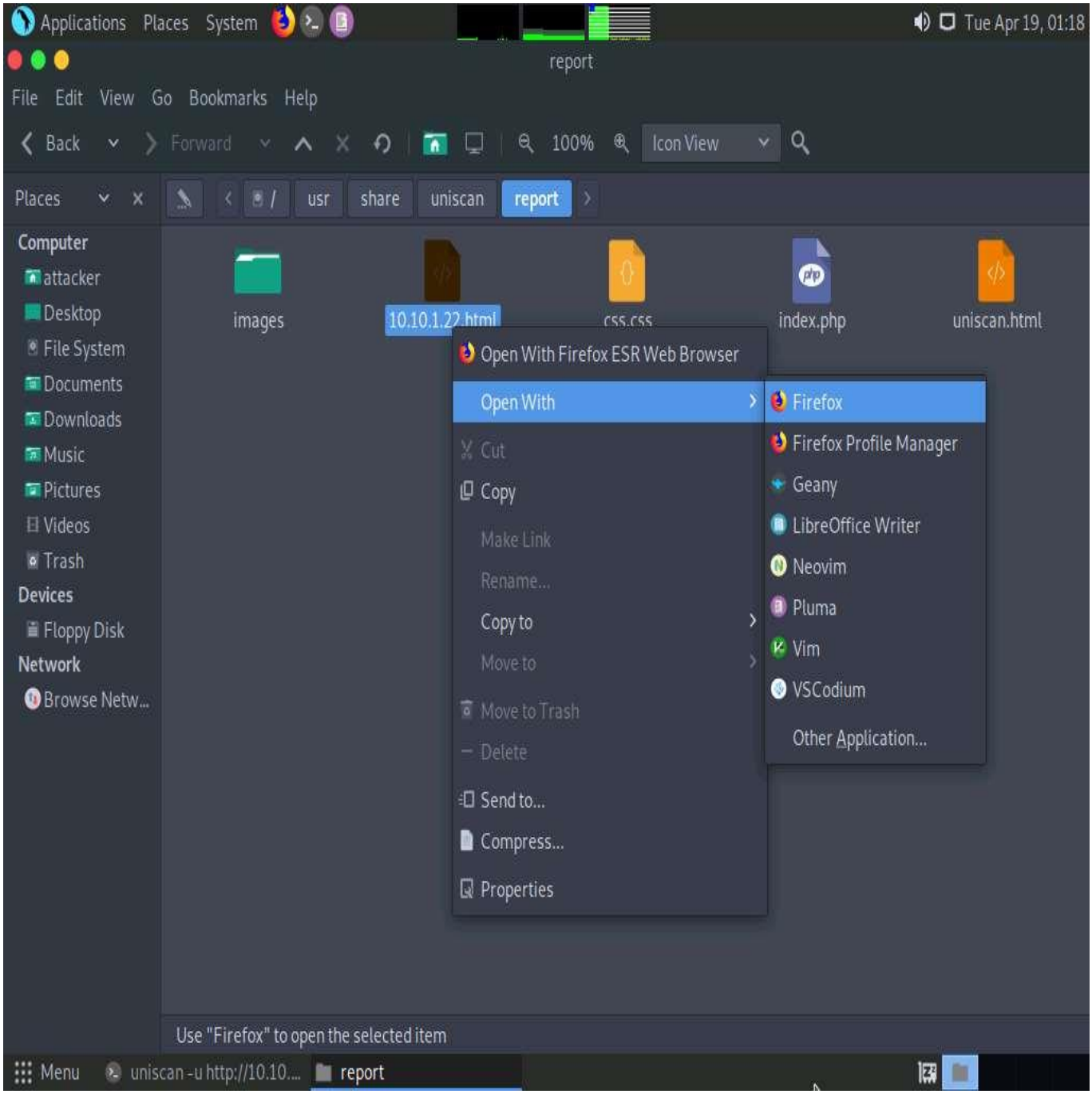
18. ☐ Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



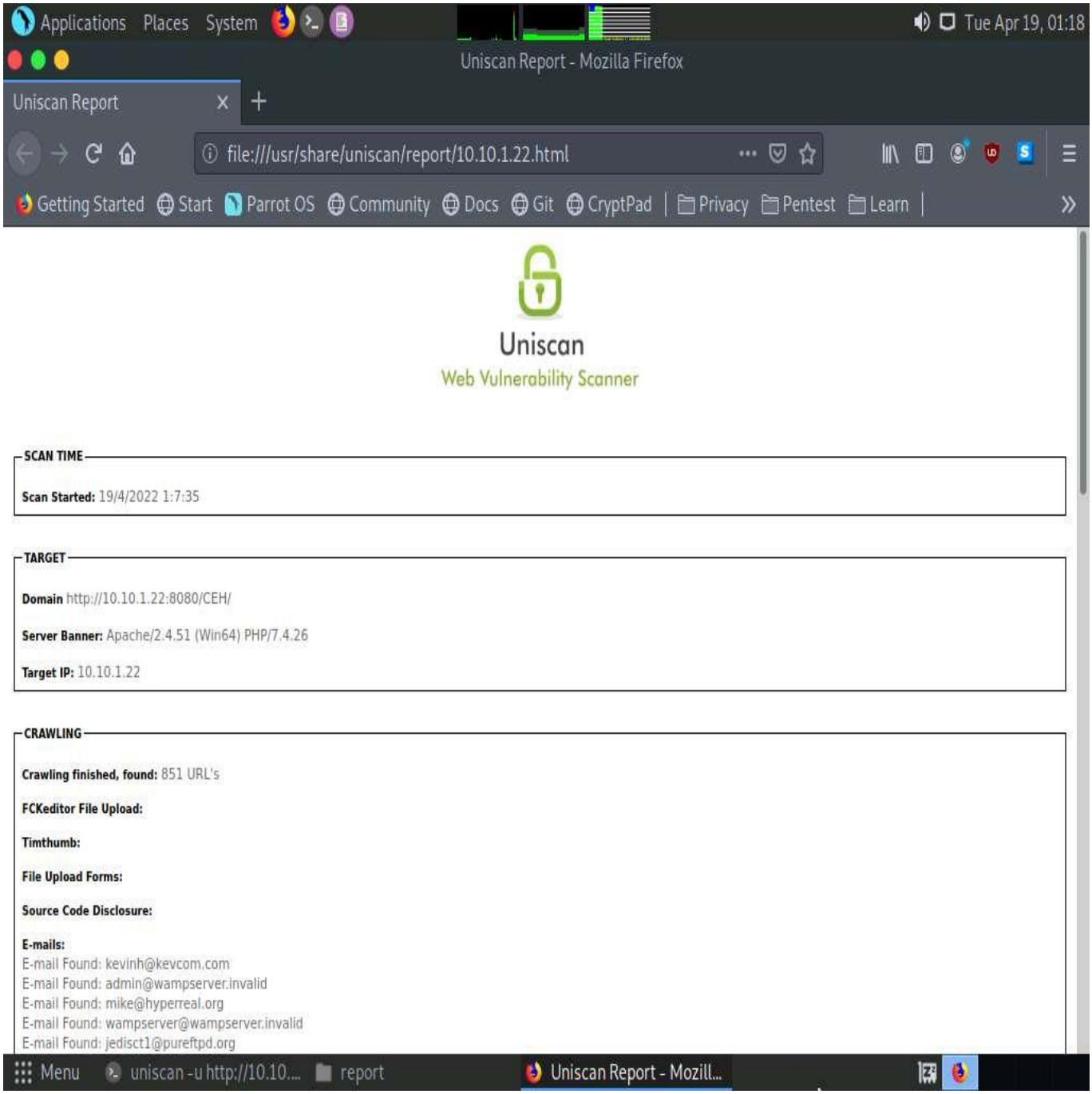
19. Click **File System** from the left-pane and click **usr** --> **share** --> **uniscan** --> **report**.



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.