# Module 14: Hacking Web Applications

# Lab 1: Footprint the Web Infrastructure

---

**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

**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

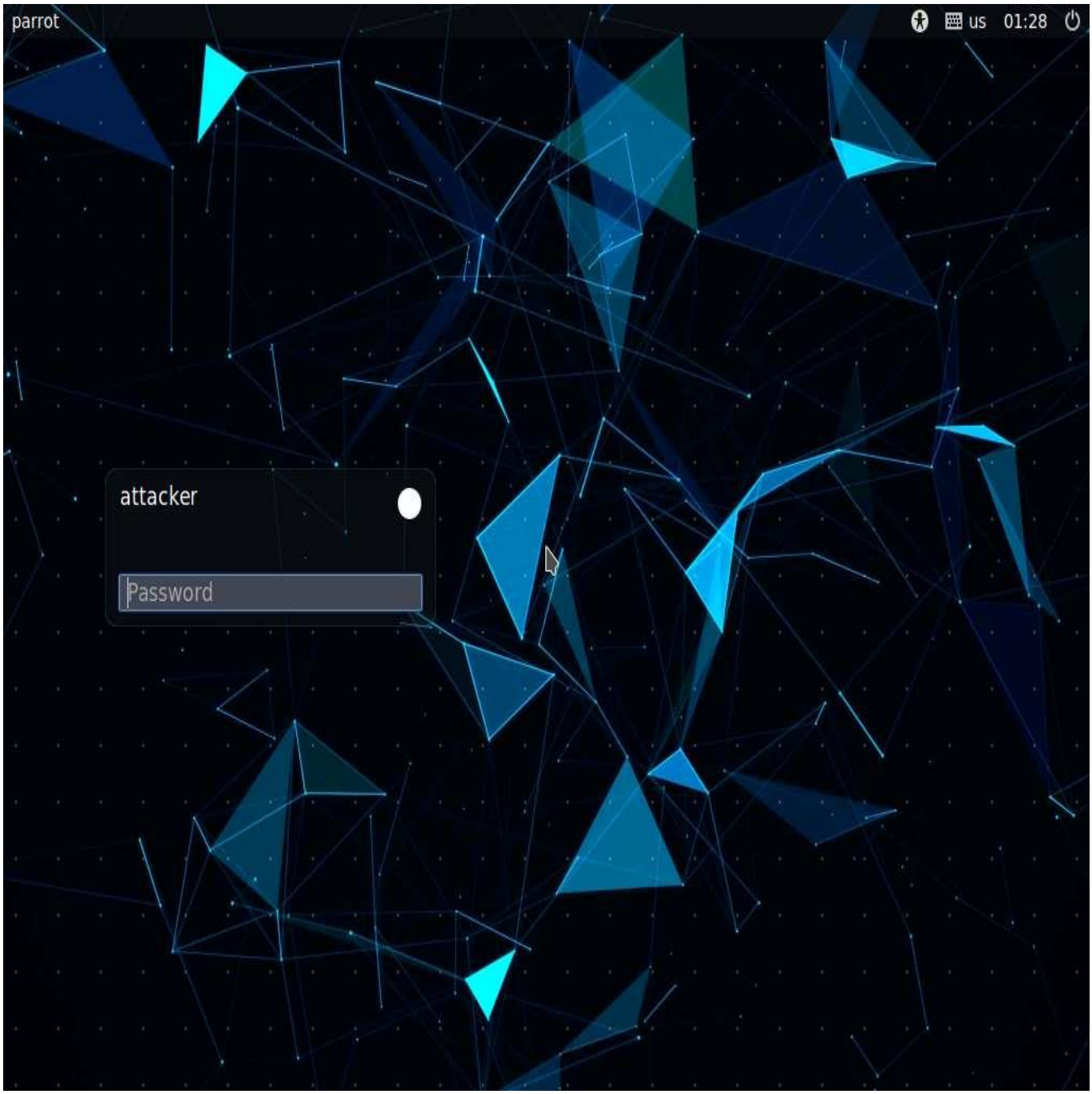
## Task 1: Perform Web Application Reconnaissance using Nmap and Telnet

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.

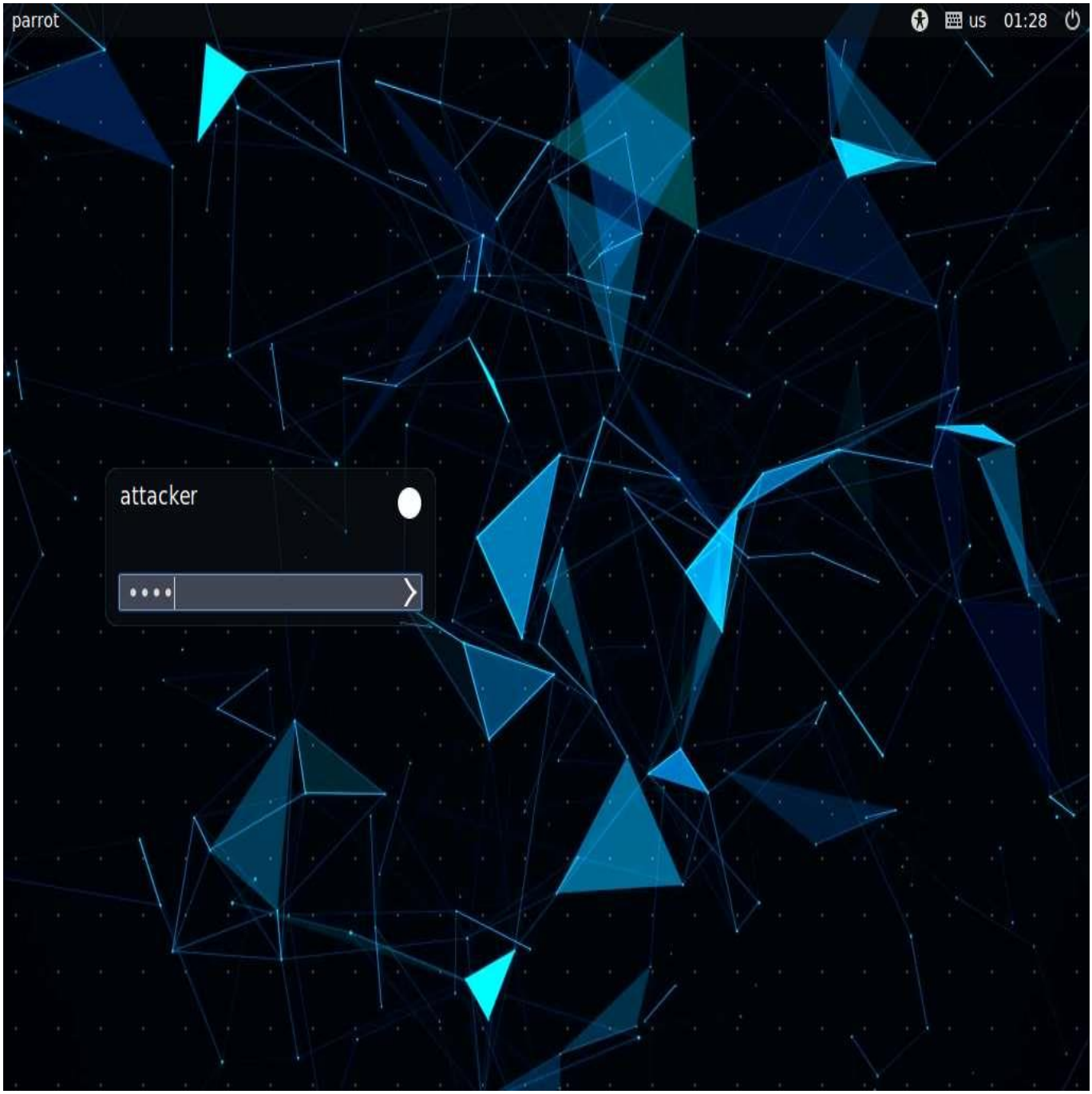
In this task, we will perform web application reconnaissance to gather information about server IP address, DNS names, location and type of server, open ports and services, make, model, version of the web server software, and server-side technology.

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.

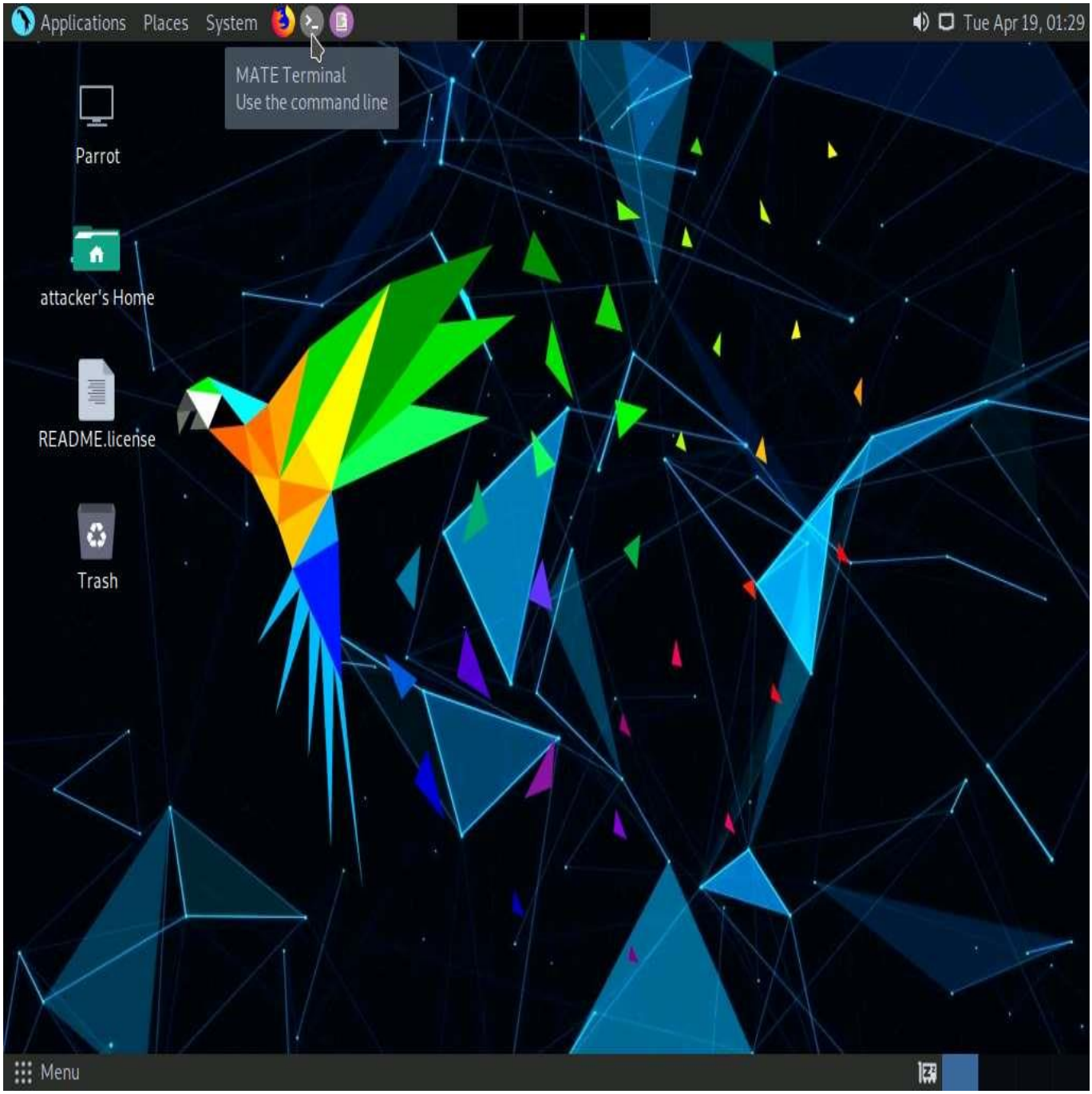
1. Click Parrot Security to switch to the **Parrot Security** machine.




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. ☐ 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.



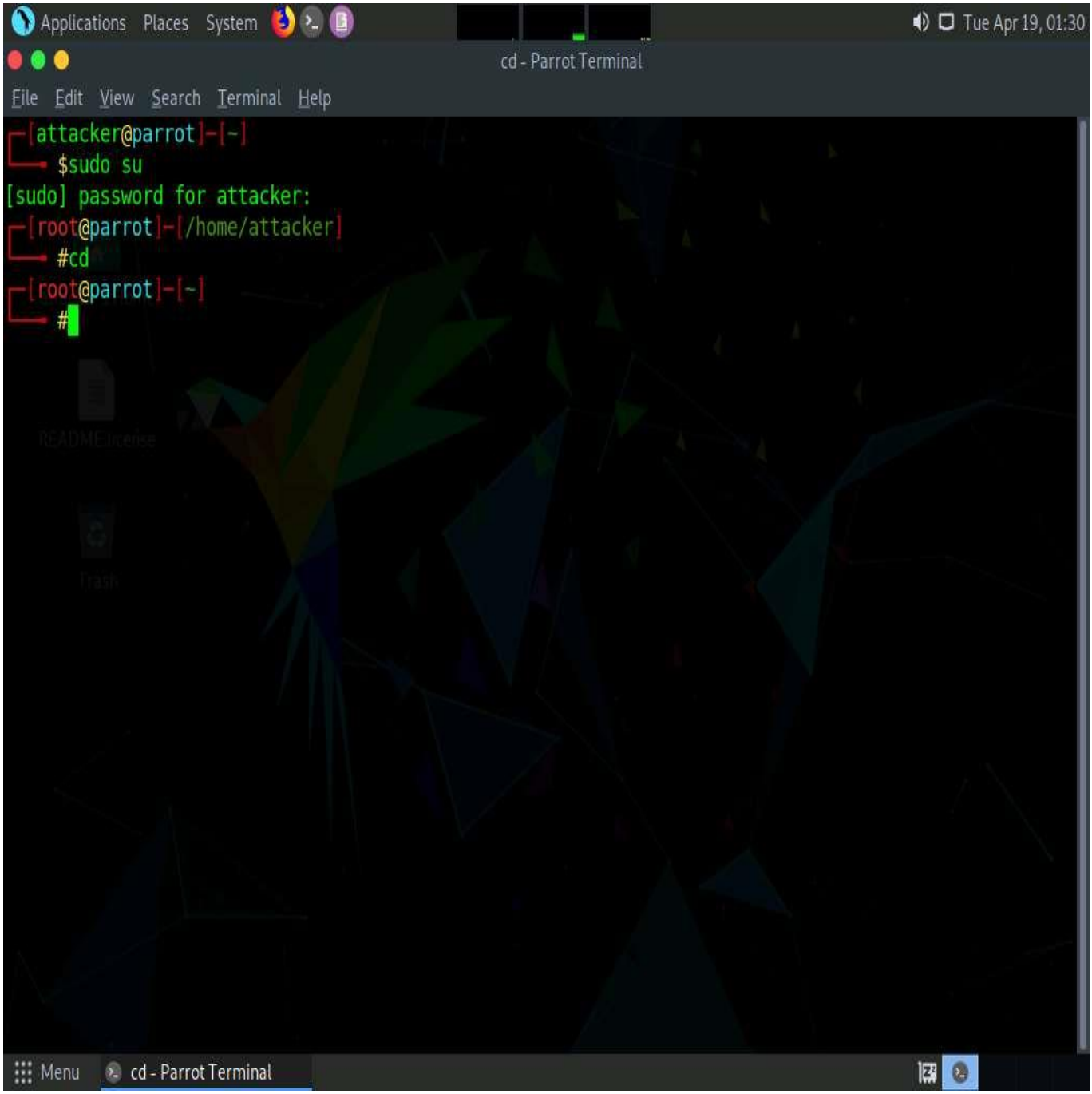

9. ☐ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.

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**.

The password that you type will not be visible.

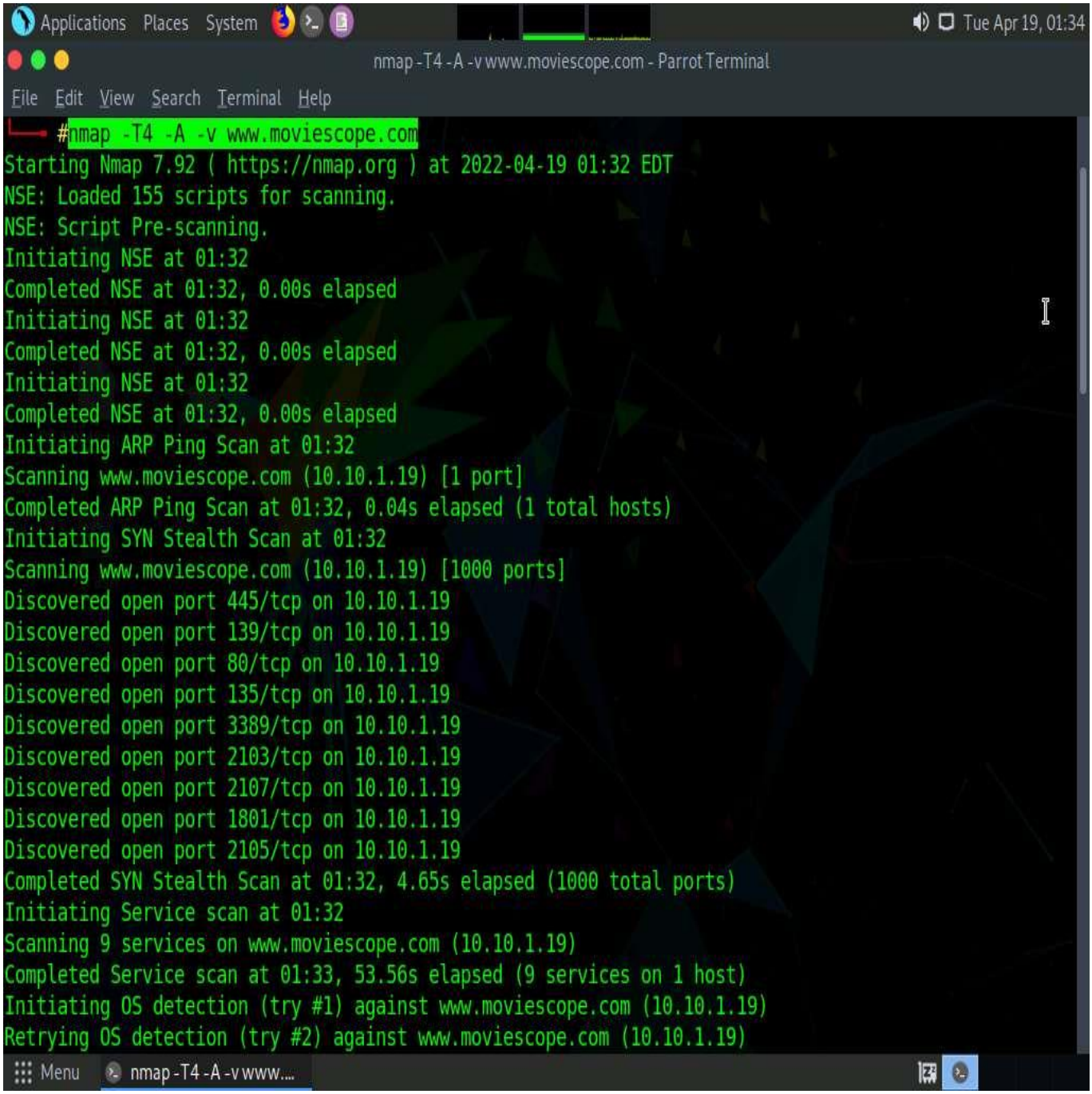
11. ☐ Now, type **cd** and press **Enter** to jump to the root directory.

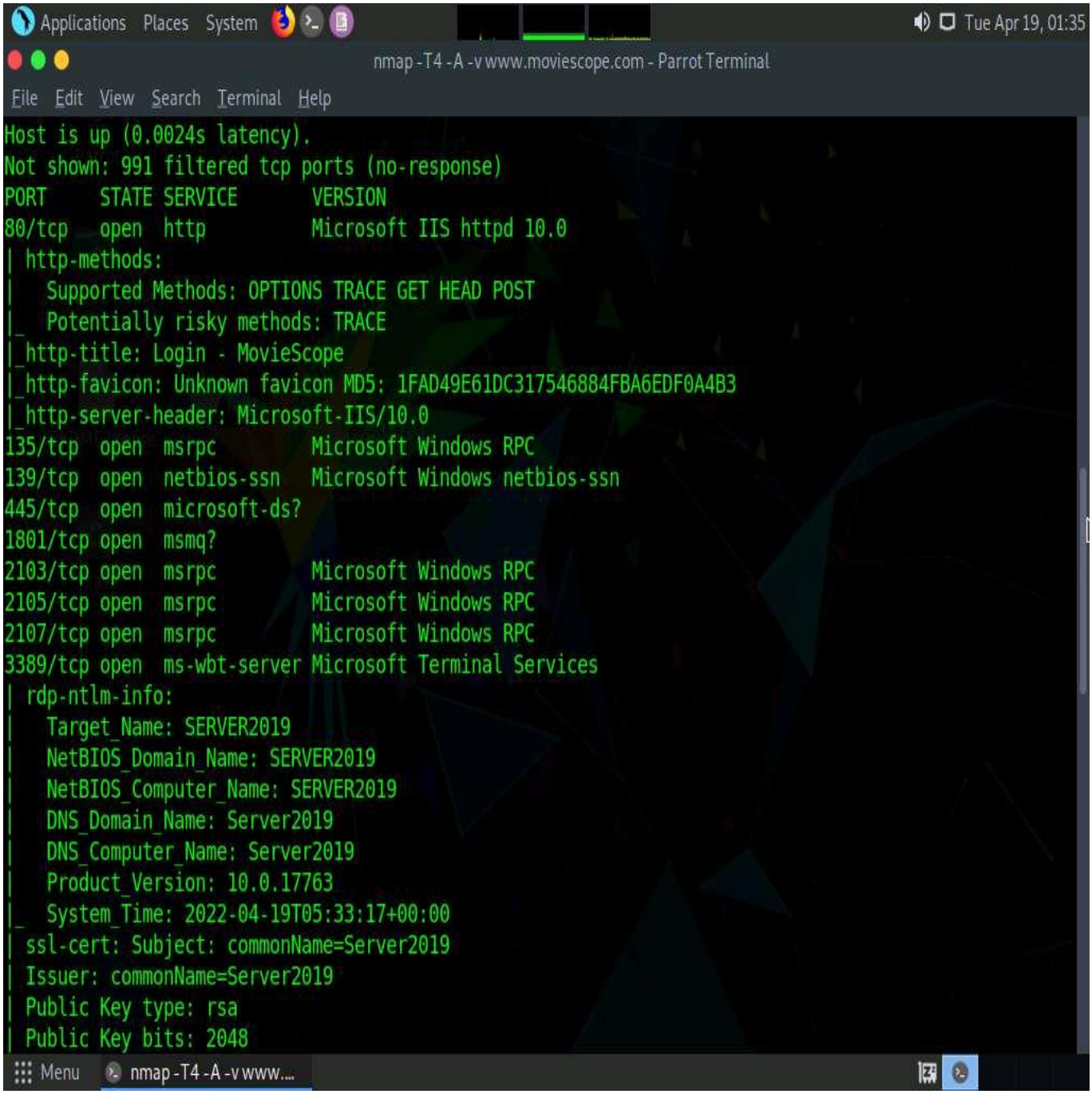



12. In the **Parrot Terminal** window, type **nmap -T4 -A -v [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform a port and service discovery scan.

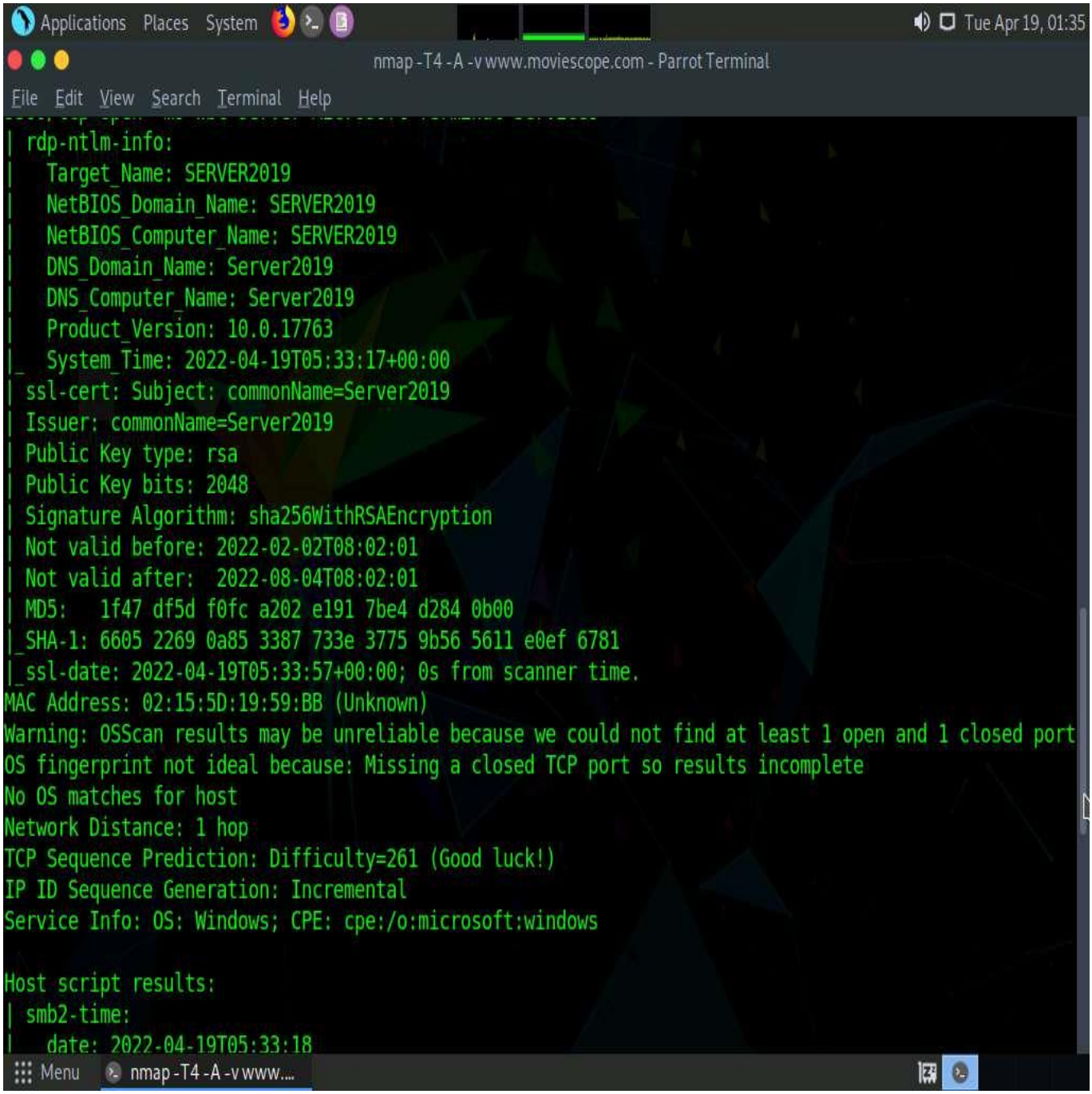
In this command, **-T4**: specifies setting time template (0-5), **-A**: specifies aggressive scan, and **-v**: enables the verbose output (include all hosts and ports in the output).

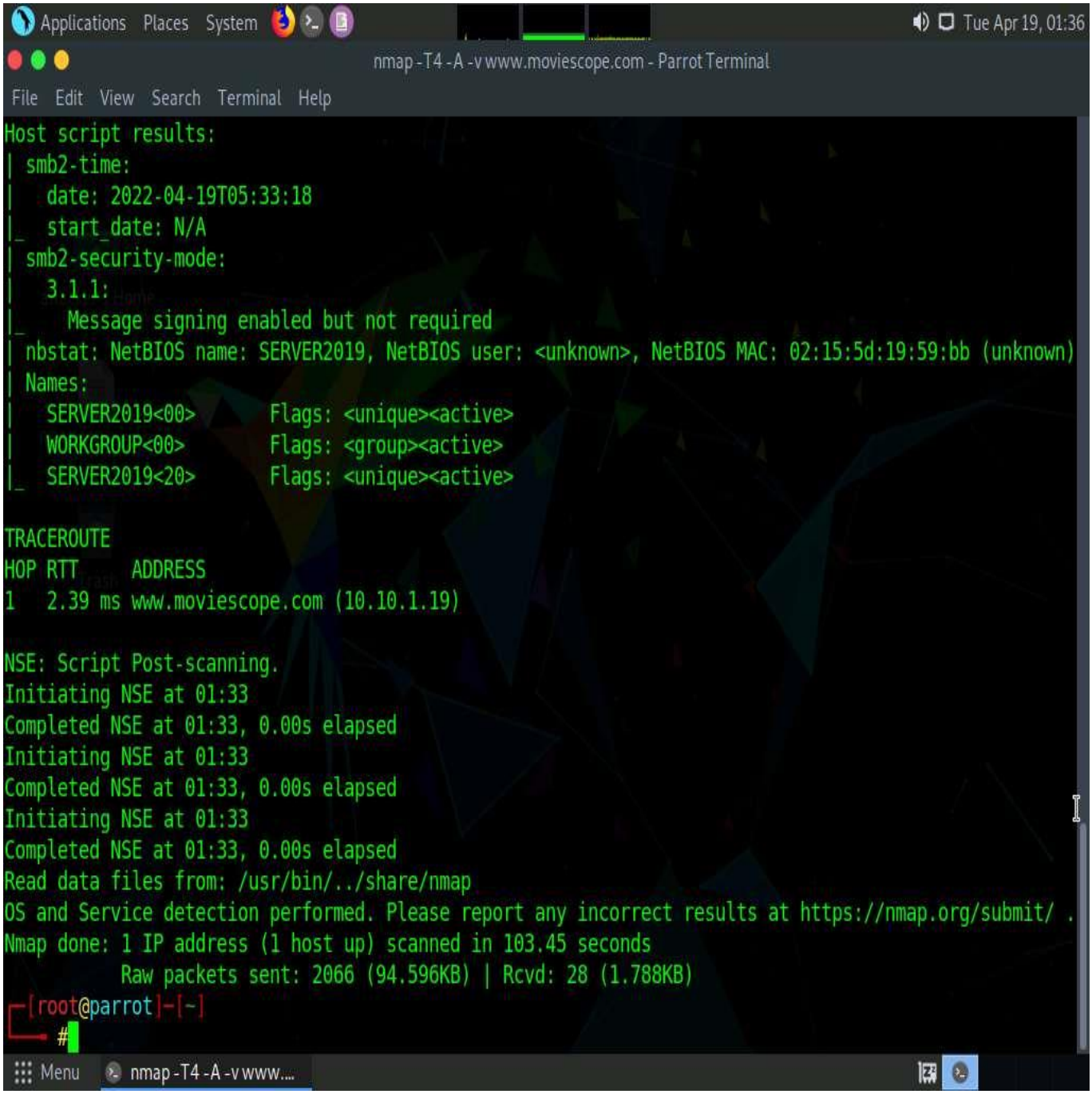
13. The result appears, displaying the open ports and services running on the machine hosting the target website.


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....




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.

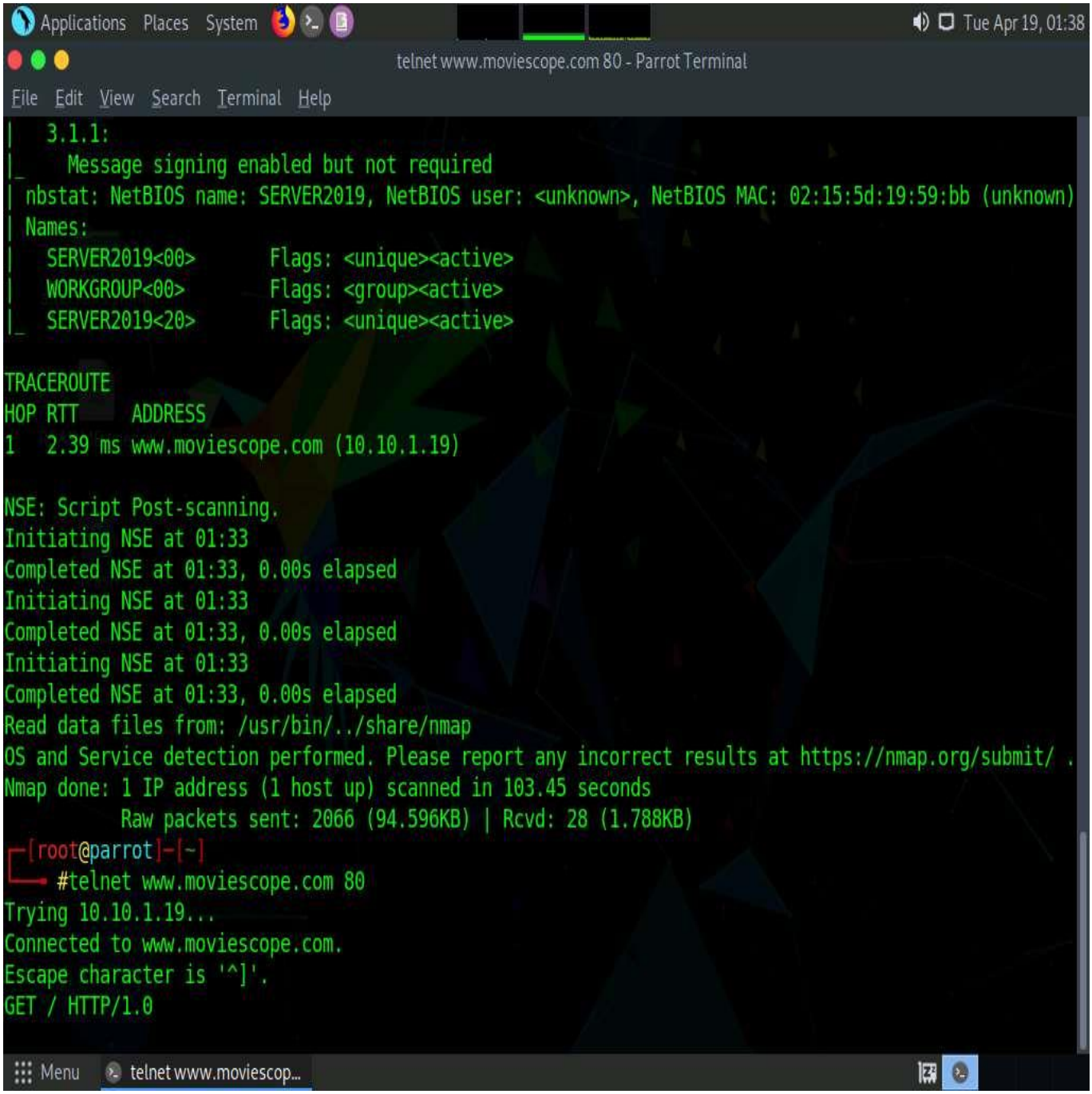

Applications Places System
Tue Apr 19, 01:35
nmap -T4 -A -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
| rdp-ntlm-info:
| Target_Name: SERVER2019
| NetBIOS_Domain_Name: SERVER2019
| NetBIOS_Computer_Name: SERVER2019
| DNS_Domain_Name: Server2019
| DNS_Computer_Name: Server2019
| 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
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-02-02T08:02:01
| Not valid after: 2022-08-04T08:02:01
| MD5: 1f47 df5d f0fc a202 e191 7be4 d284 0b00
|_SHA-1: 6605 2269 0a85 3387 733e 3775 9b56 5611 e0ef 6781
|_ssl-date: 2022-04-19T05:33:57+00:00; 0s from scanner time.
MAC Address: 02:15:5D:19:59:BB (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
| date: 2022-04-19T05:33:18
Menu
nmap -T4 -A -v www....




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.

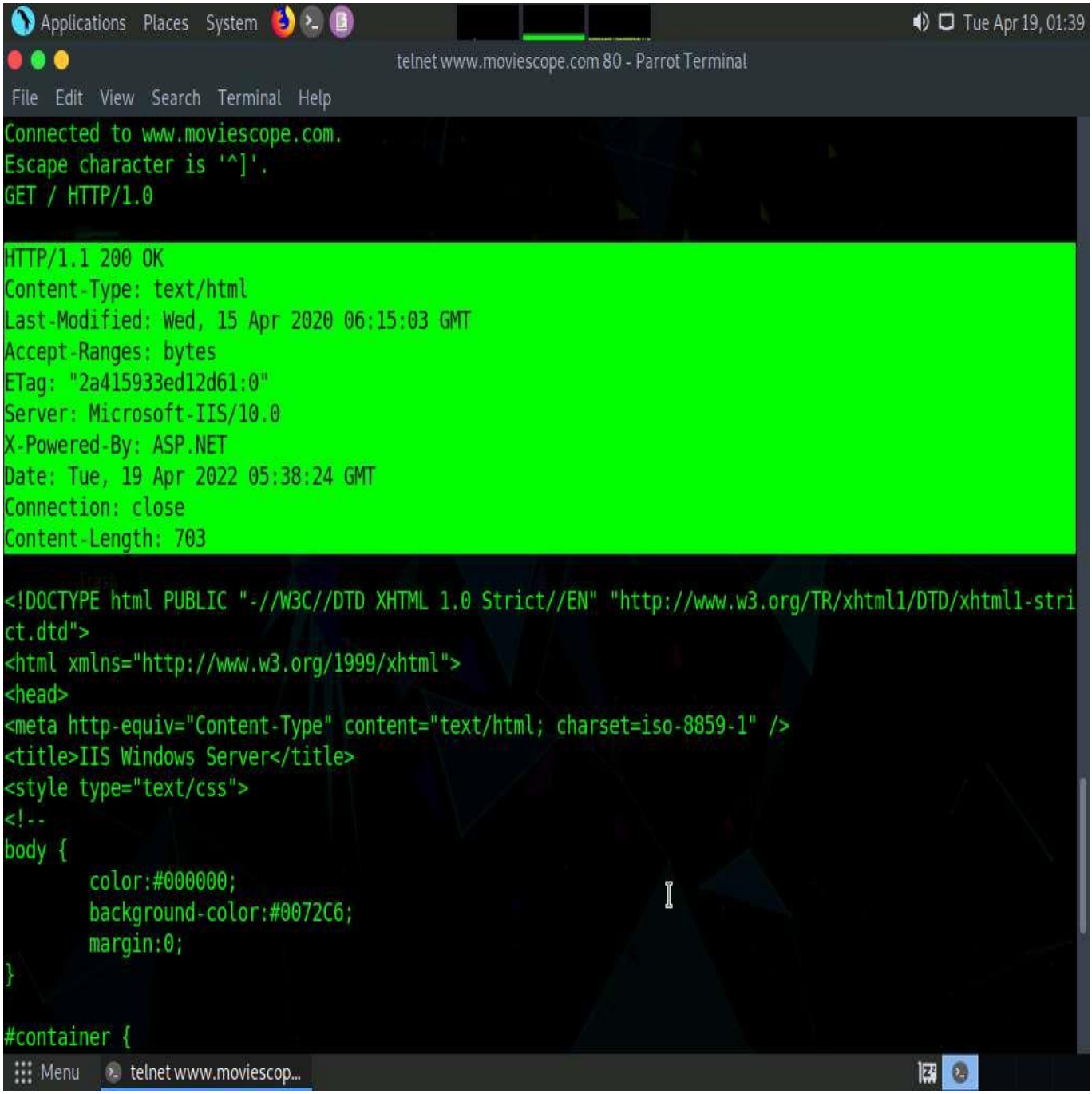
Port 80 is the port number assigned to the commonly used Internet communication protocol, Hypertext Transfer Protocol (HTTP).

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**.

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. more...




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.

---

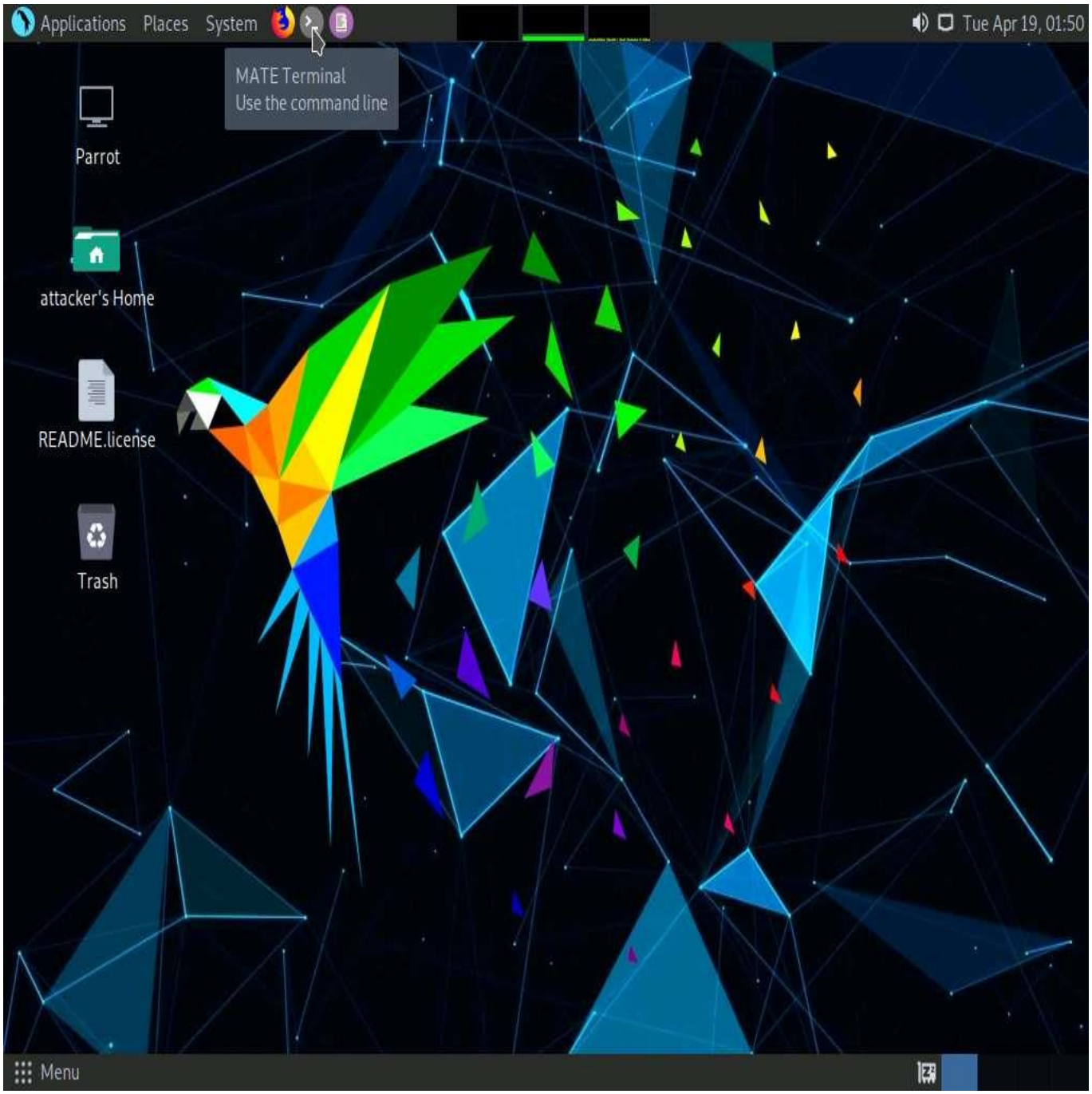
## Task 2: Perform Web Application Reconnaissance using WhatWeb

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.

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.

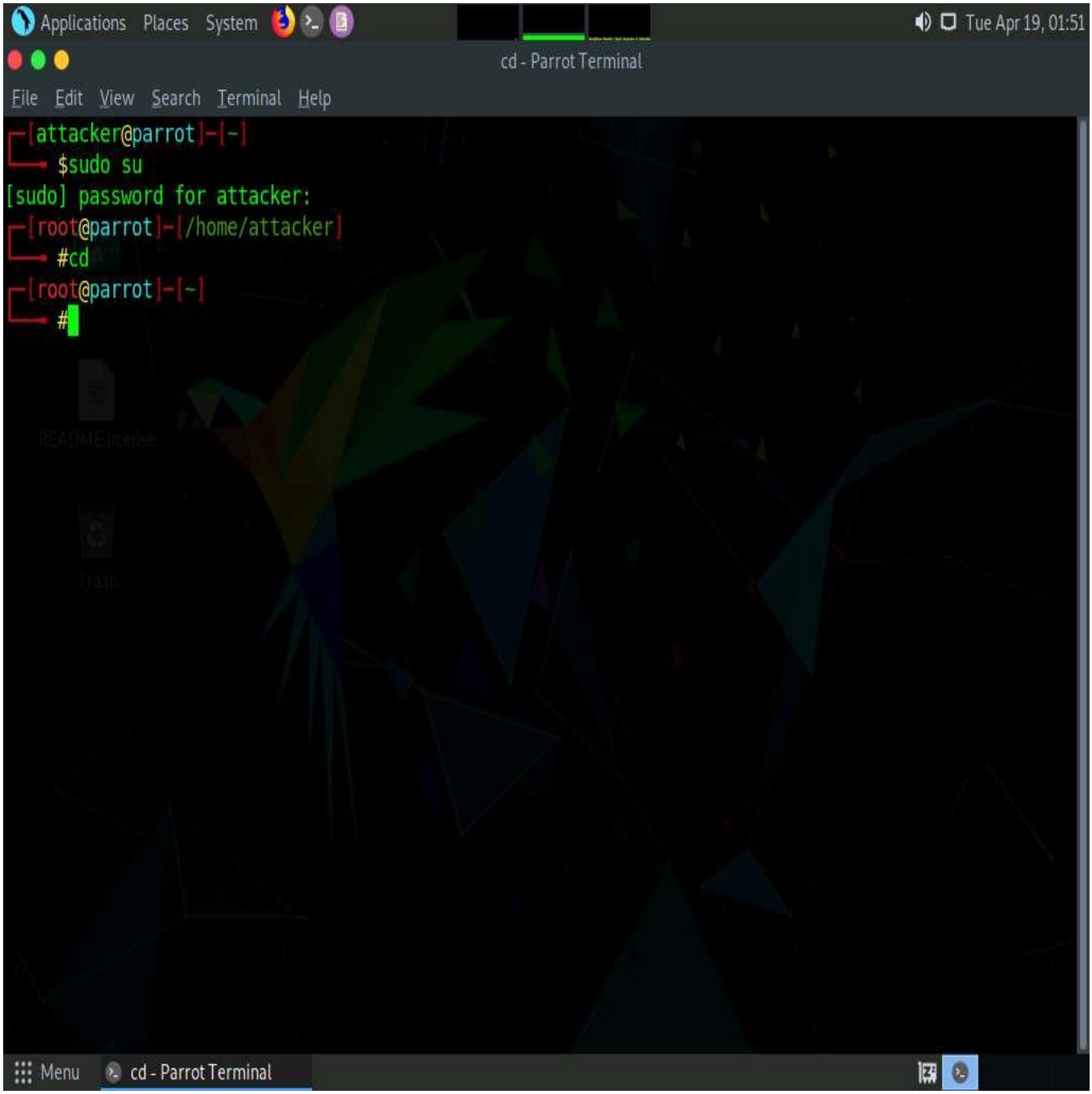
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



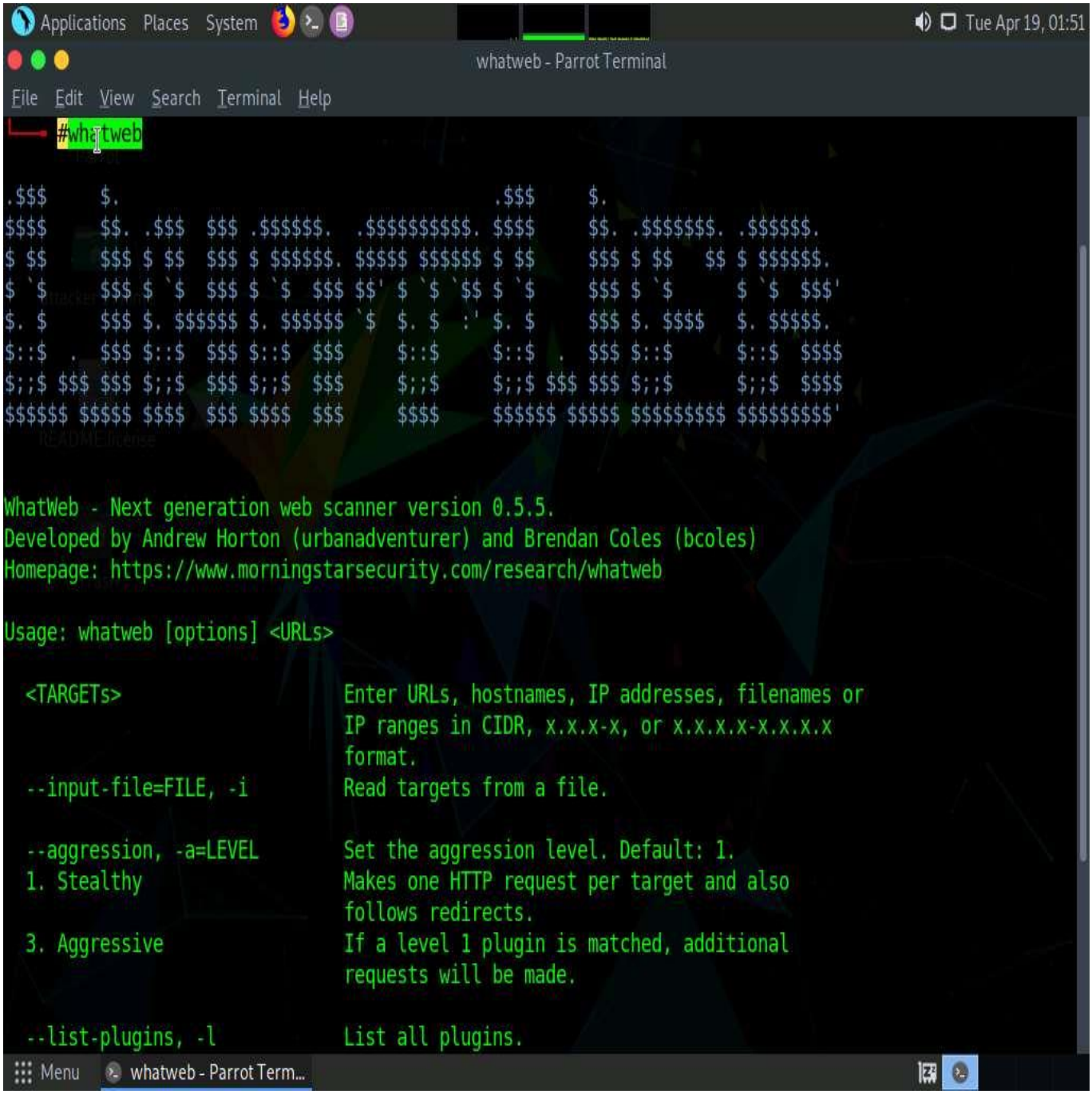

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

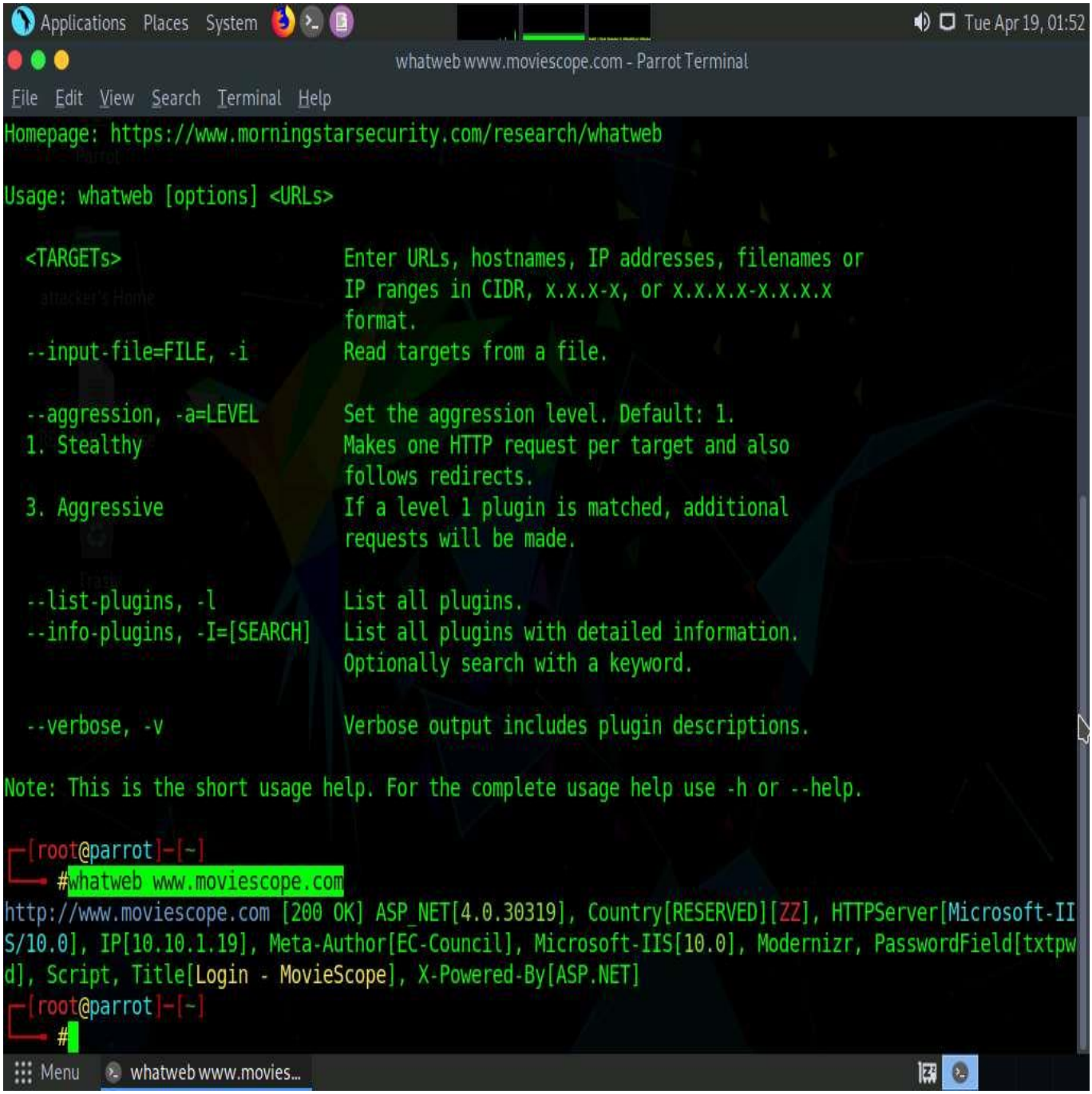
4. Now, type **cd** and press **Enter** to jump to the root directory.



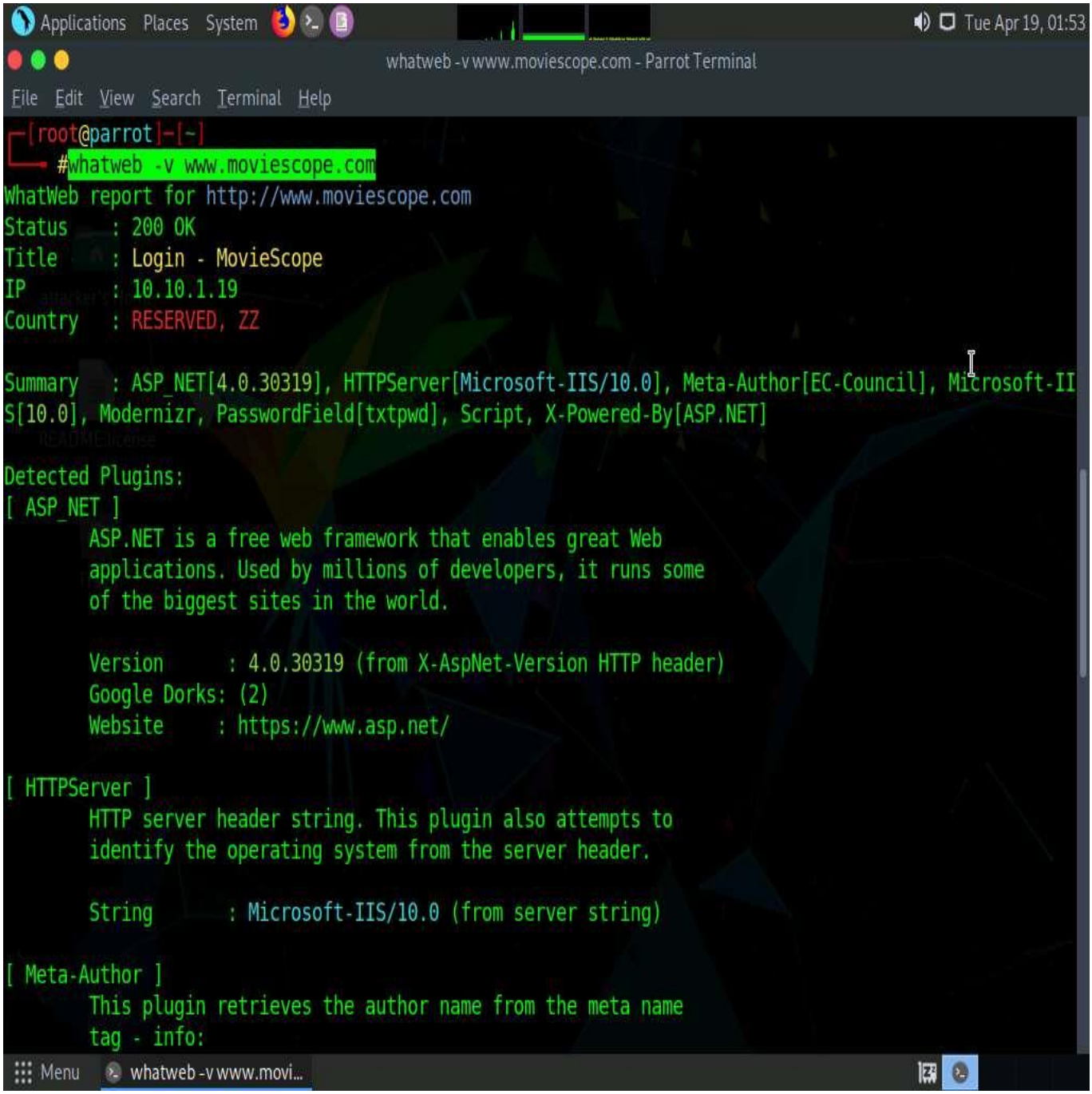

5. In the **Terminal** window, type **whatweb** and press **Enter**. It displays a list of the commands available with WhatWeb.

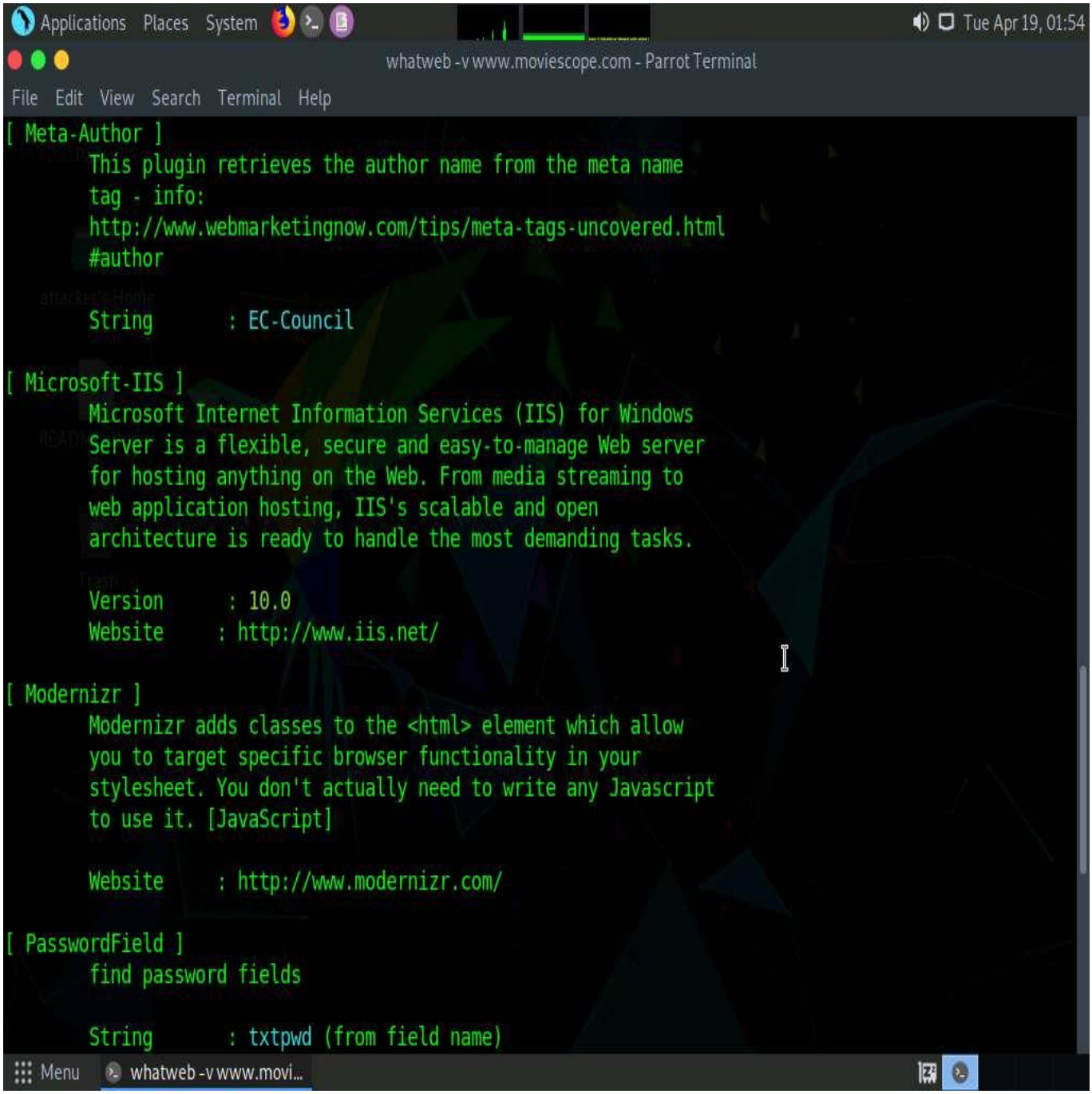


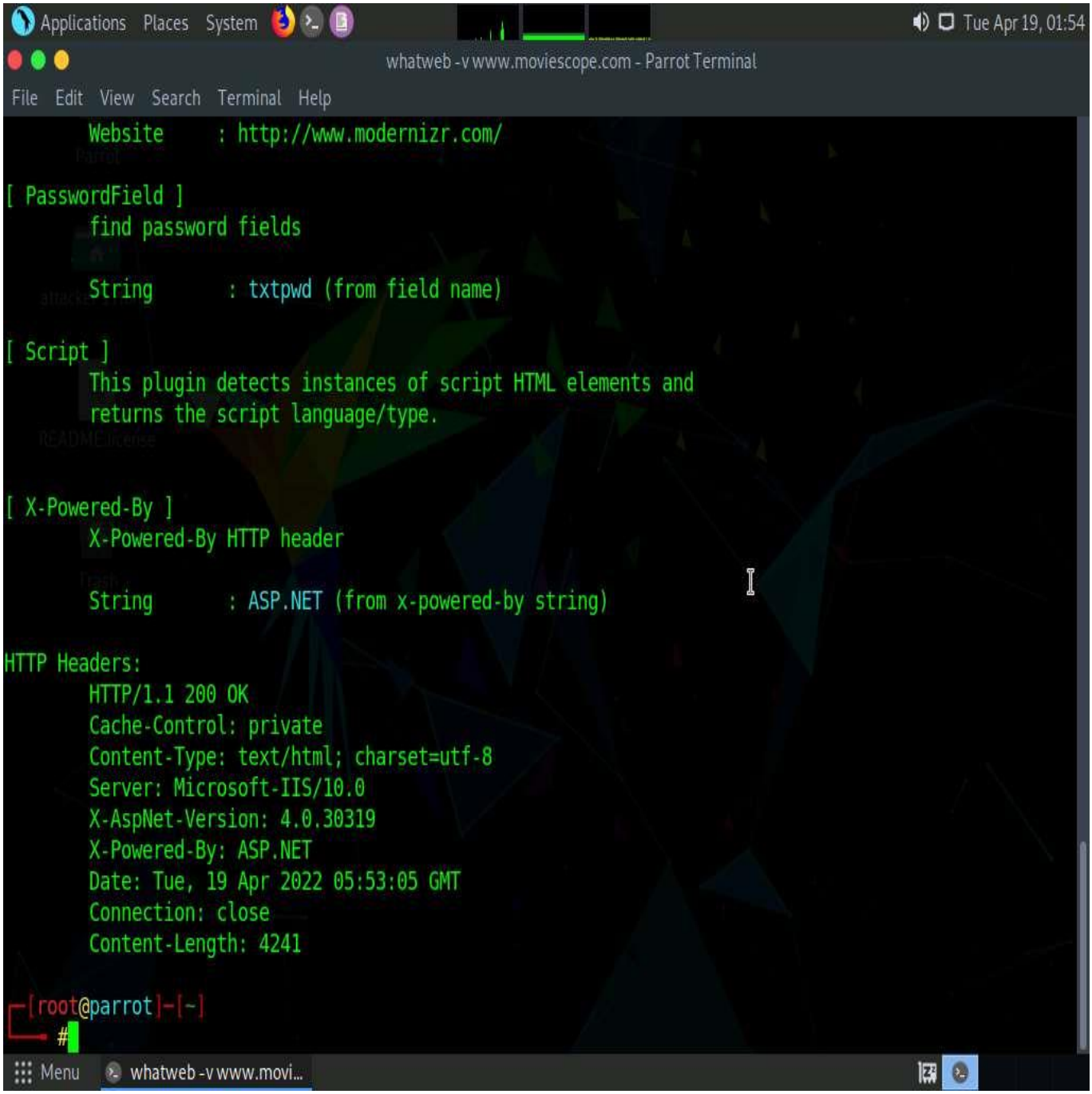

6. Now, type **whatweb [Target Web Application]** (here, the target web application is **www.moviescope.com**) and press **Enter** to perform website footprinting on the target website.
7. The result appears, displaying the **MovieScope** website infrastructure, as shown in the screenshot.




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.

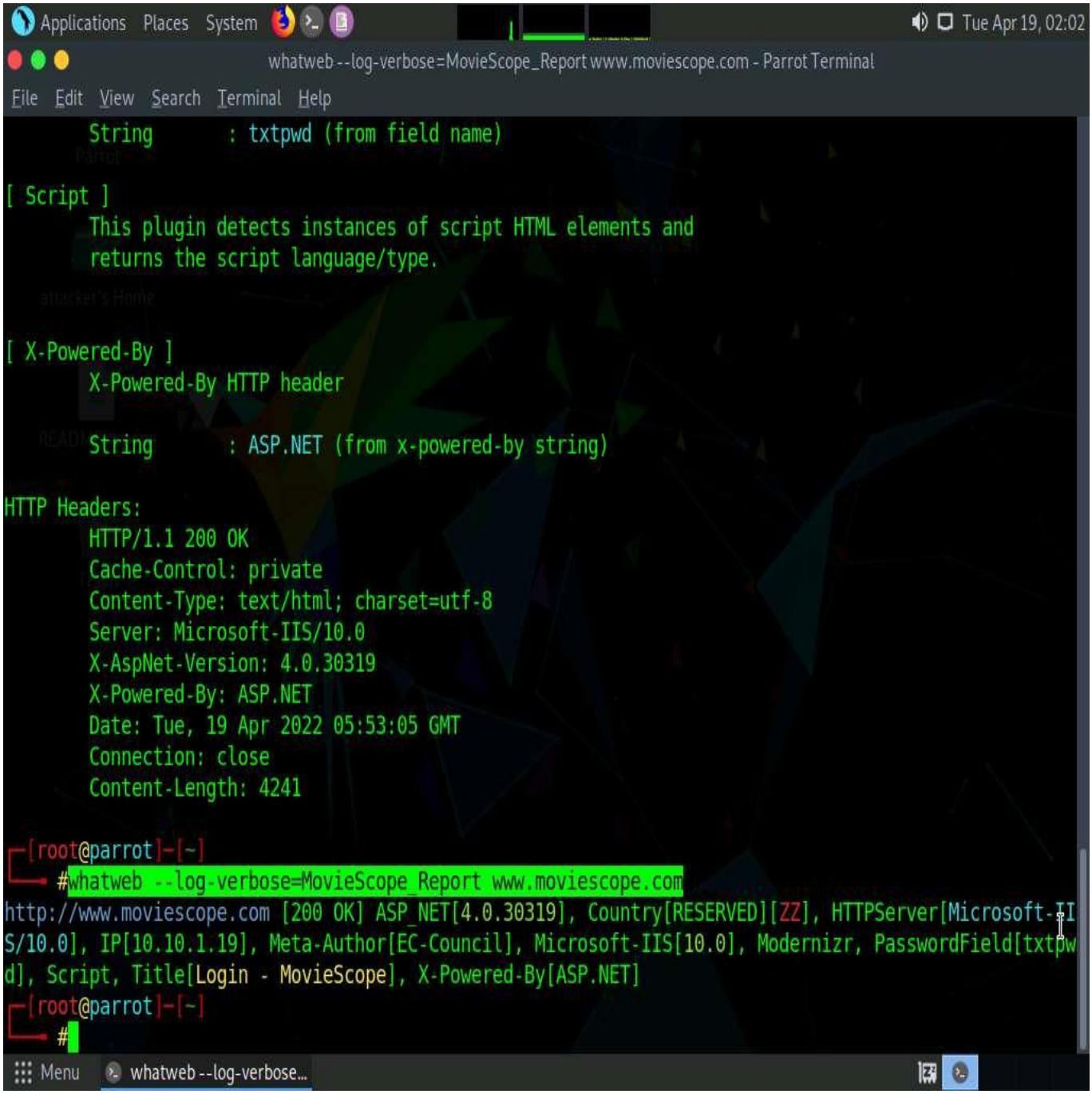

Applications Places System
Tue Apr 19, 01:53
whatweb -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[~]
#whatweb -v www.moviescope.com
WhatWeb report for http://www.moviescope.com
Status : 200 OK
Title : Login - MovieScope
IP : 10.10.1.19
Country : RESERVED, ZZ
Summary : ASP_NET[4.0.30319], HTTPServer[Microsoft-IIS/10.0], Meta-Author[EC-Council], Microsoft-IIS[10.0], Modernizr, PasswordField[txtpwd], Script, X-Powered-By[ASP.NET]
Detected Plugins:
[ ASP_NET ]
ASP.NET is a free web framework that enables great Web applications. Used by millions of developers, it runs some of the biggest sites in the world.
Version : 4.0.30319 (from X-AspNet-Version HTTP header)
Google Dorks: (2)
Website : https://www.asp.net/
[ HTTPServer ]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.
String : Microsoft-IIS/10.0 (from server string)
[ Meta-Author ]
This plugin retrieves the author name from the meta name tag - info:
Menu
whatweb -v www.movi...


Applications Places System
Tue Apr 19, 01:54
whatweb -v www.moviescope.com - Parrot Terminal
File Edit View Search Terminal Help
[ Meta-Author ]
This plugin retrieves the author name from the meta name
tag - info:
http://www.webmarketingnow.com/tips/meta-tags-uncovered.html
#author
String : EC-Council
[ Microsoft-IIS ]
Microsoft Internet Information Services (IIS) for Windows
Server is a flexible, secure and easy-to-manage Web server
for hosting anything on the Web. From media streaming to
web application hosting, IIS's scalable and open
architecture is ready to handle the most demanding tasks.
Version : 10.0
Website : http://www.iis.net/
[ Modernizr ]
Modernizr adds classes to the <html> element which allow
you to target specific browser functionality in your
stylesheet. You don't actually need to write any Javascript
to use it. [JavaScript]
Website : http://www.modernizr.com/
[ PasswordField ]
find password fields
String : txtpwd (from field name)
Menu
whatweb -v www.movi...

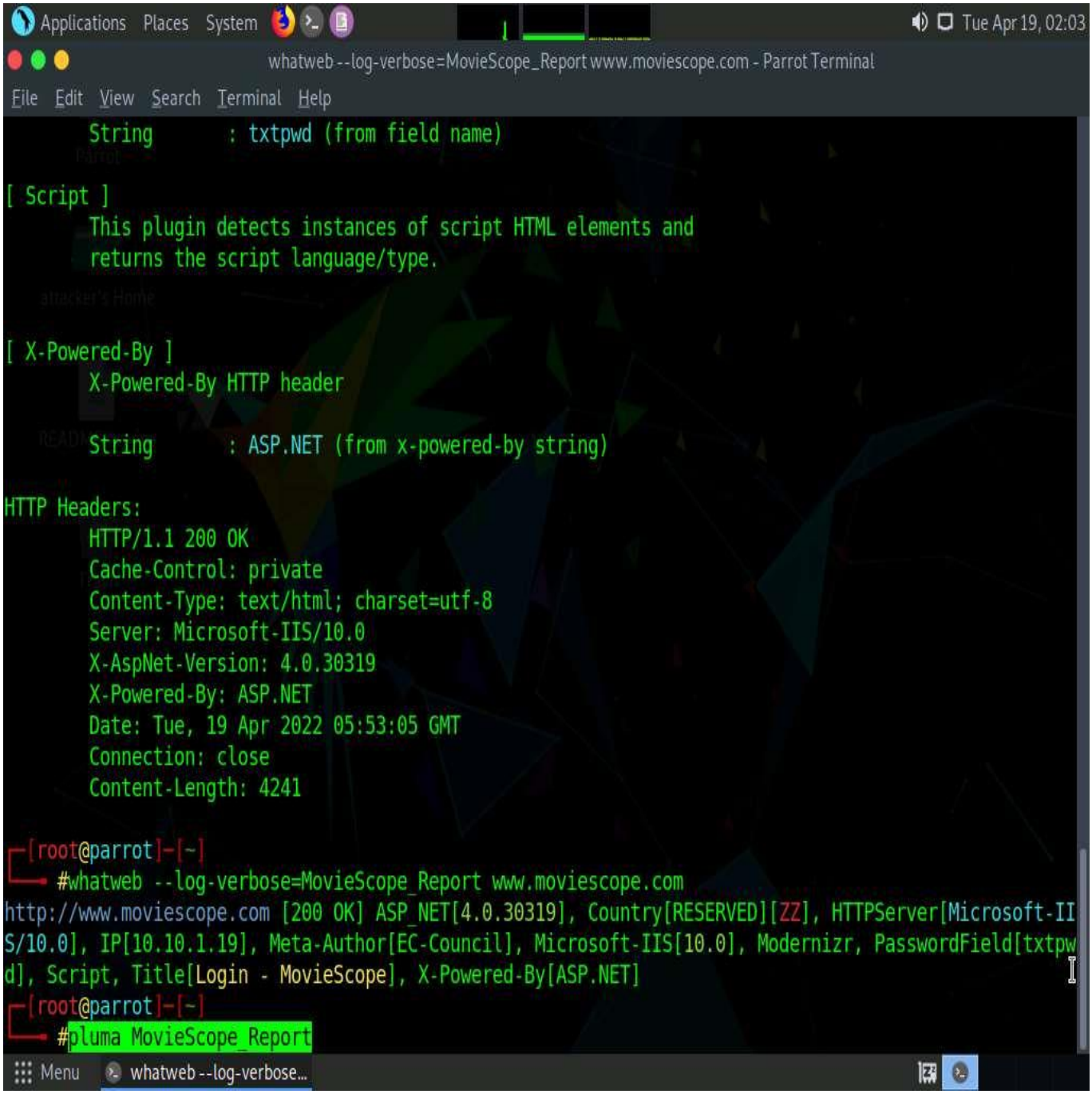



10. Now, type **whatweb --log-verbose=MovieScope_Report www.moviescope.com** and press **Enter** to export the results returned by WhatWeb as a text file.

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

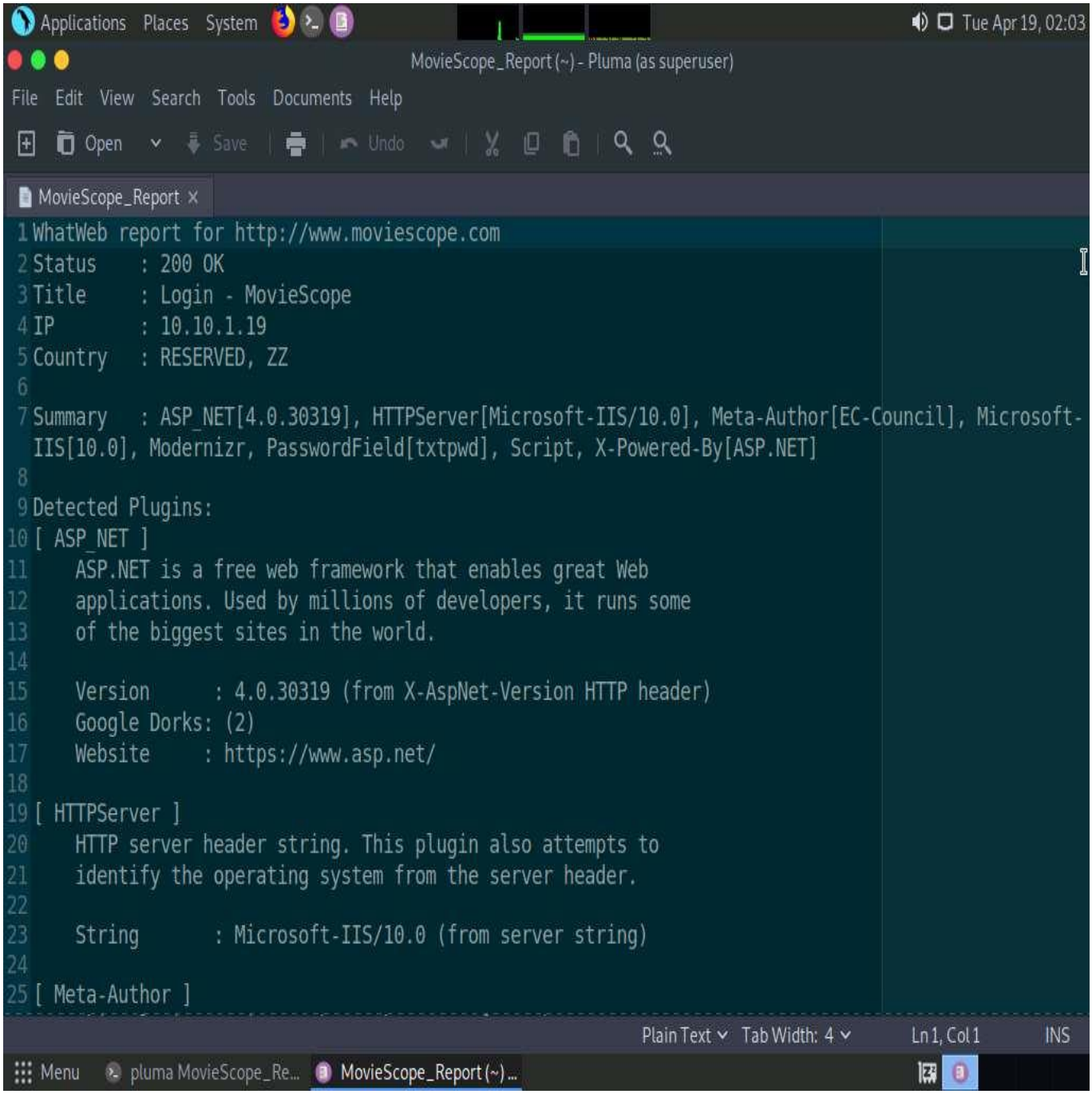



11. Type, **pluma MovieScope_Report** and press **Enter** to open the file.




12. The **MovieScope_Report** text file appears, as shown in the screenshot.

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.

---

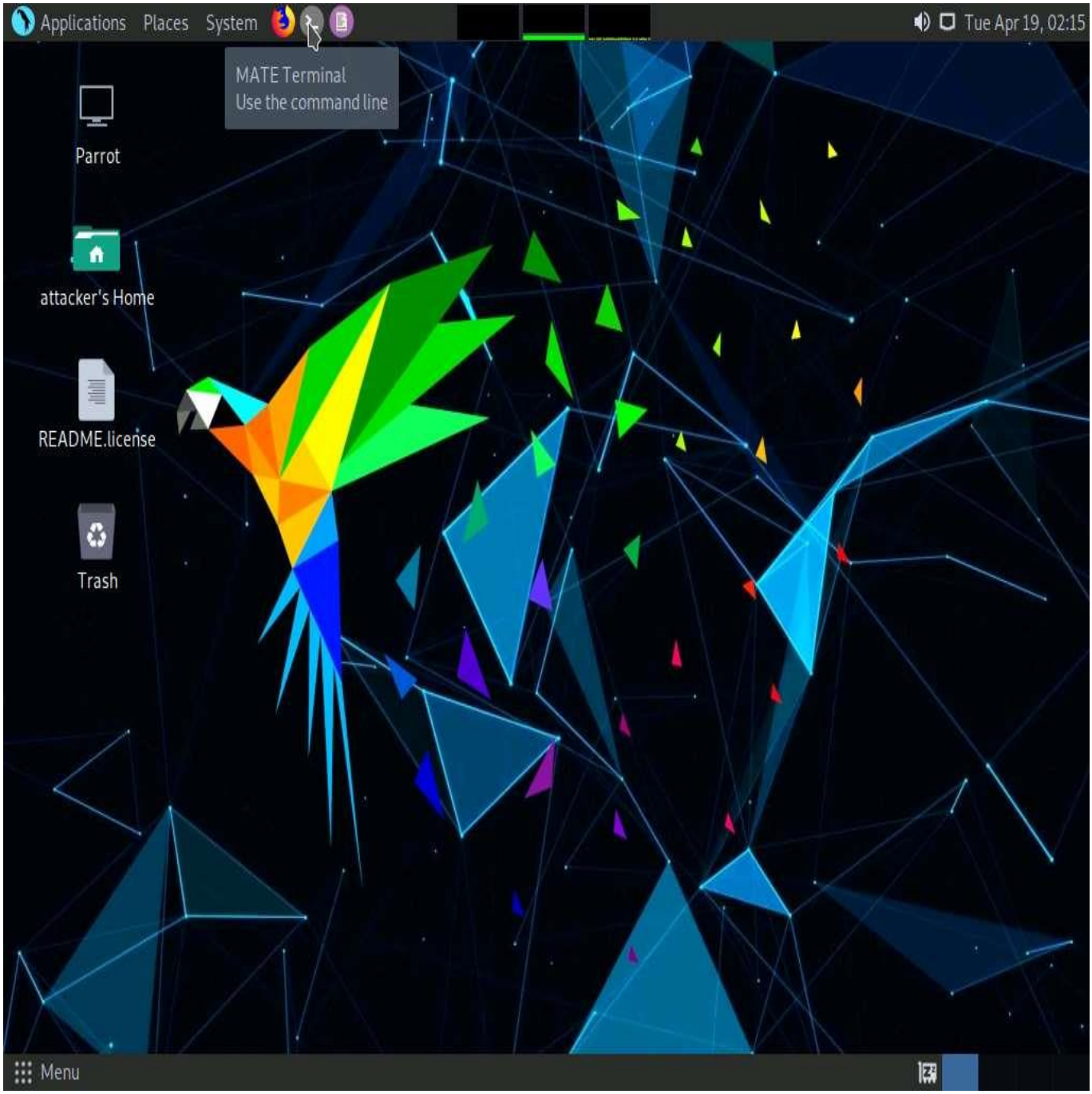
## Task 3: Perform Web Spidering using OWASP ZAP

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.

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.

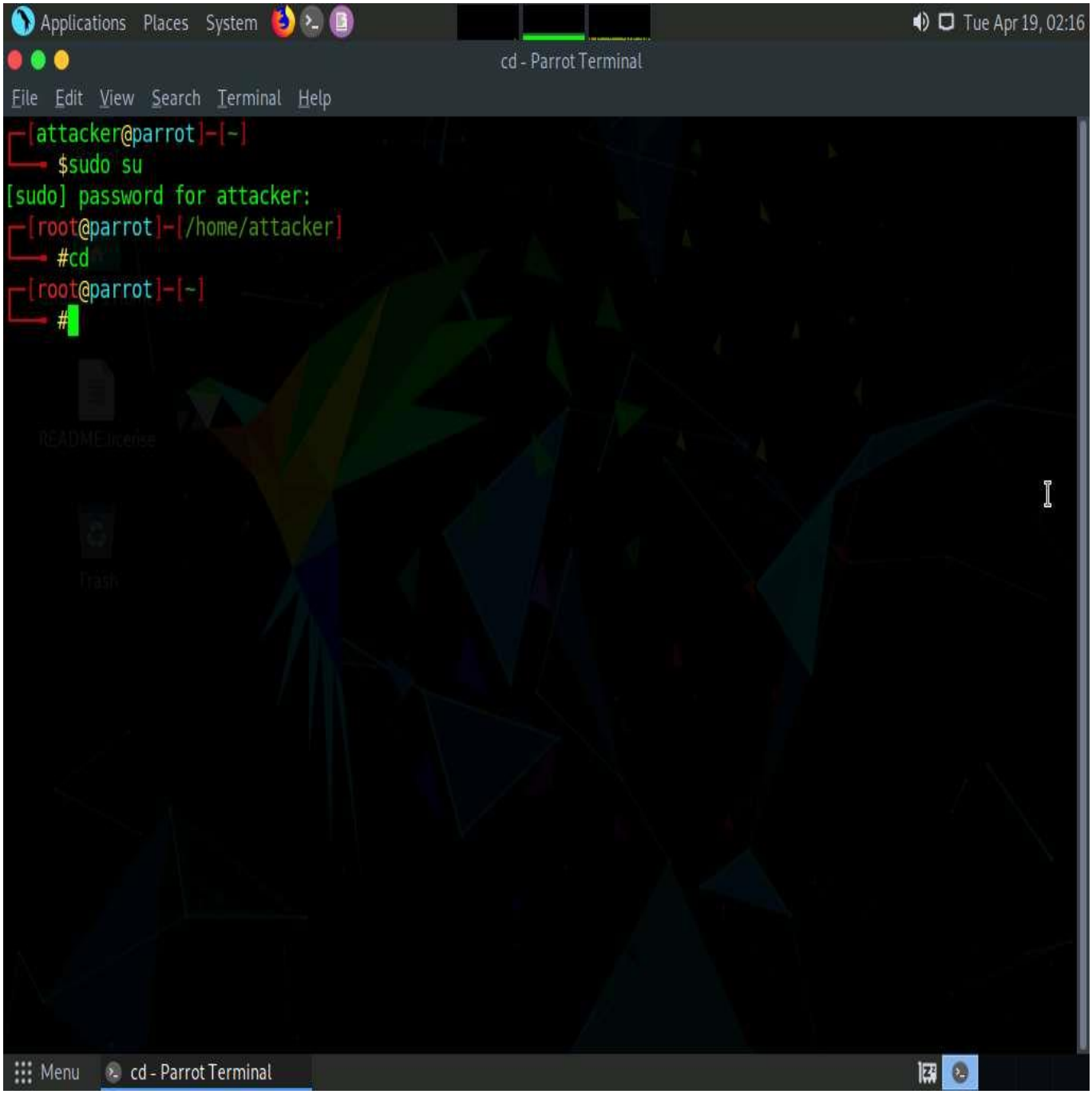
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



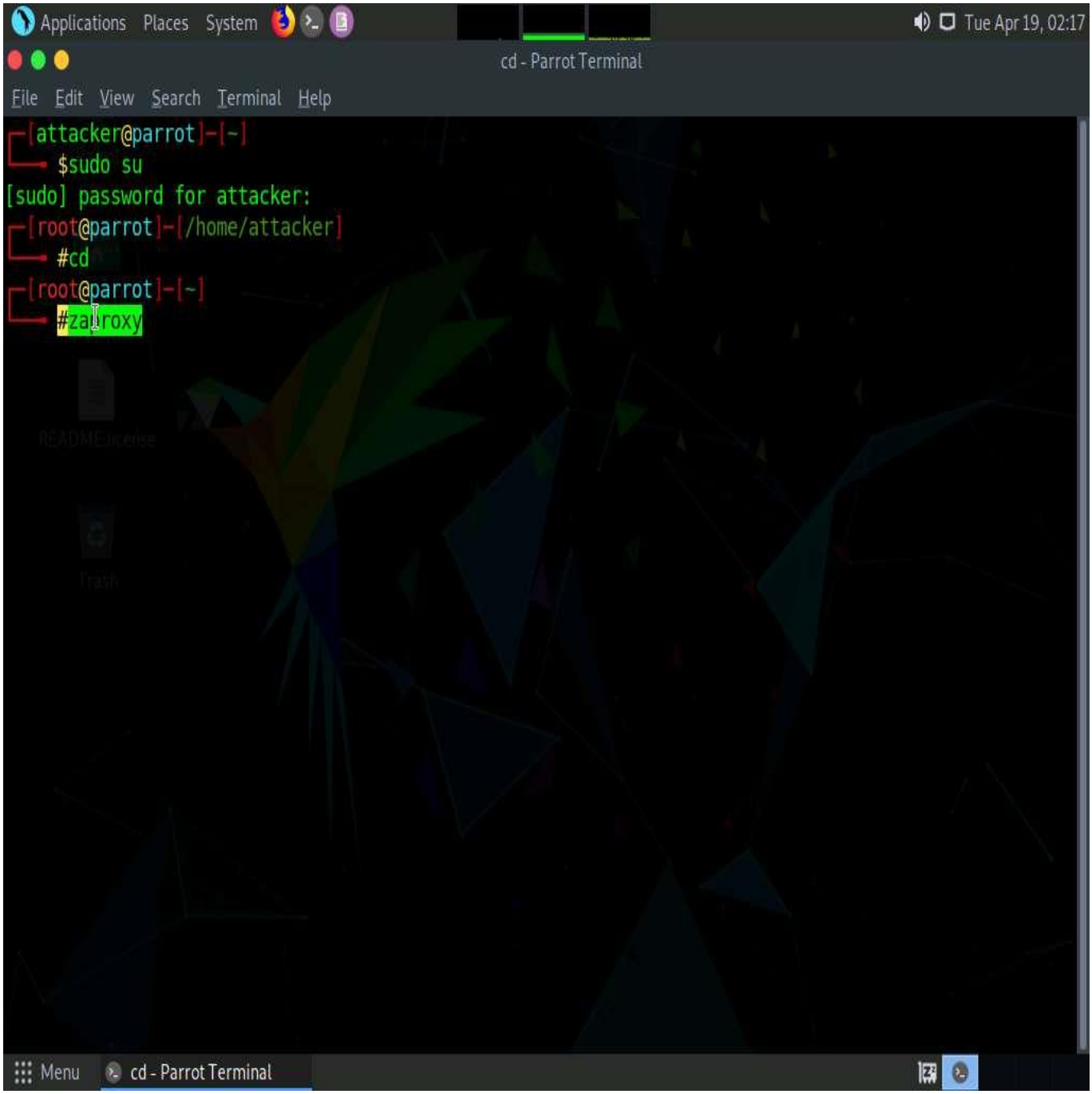

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

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

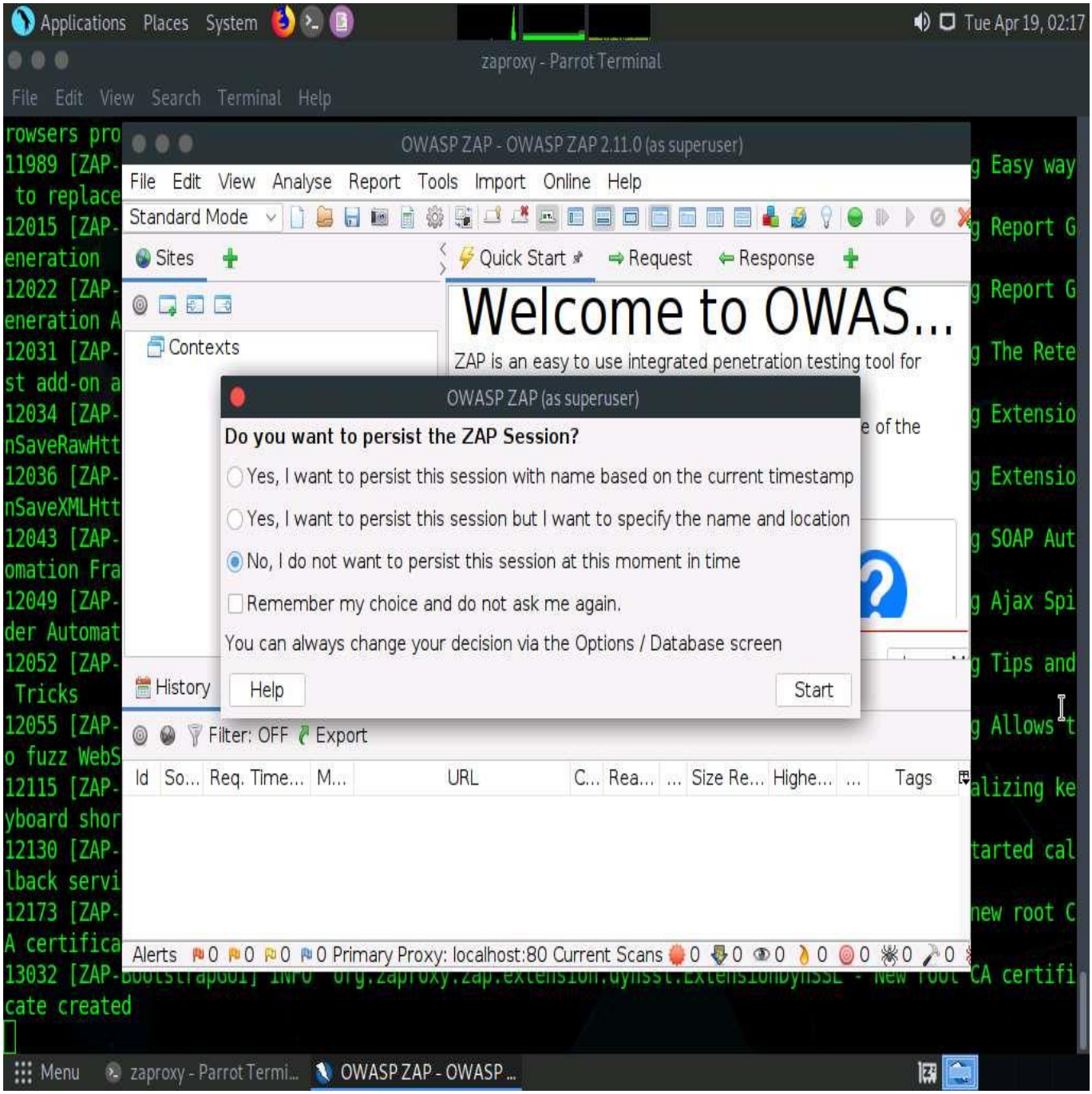



5. In the **Terminal** window, type **zaproxy** and press **Enter** to launch OWASP ZAP.

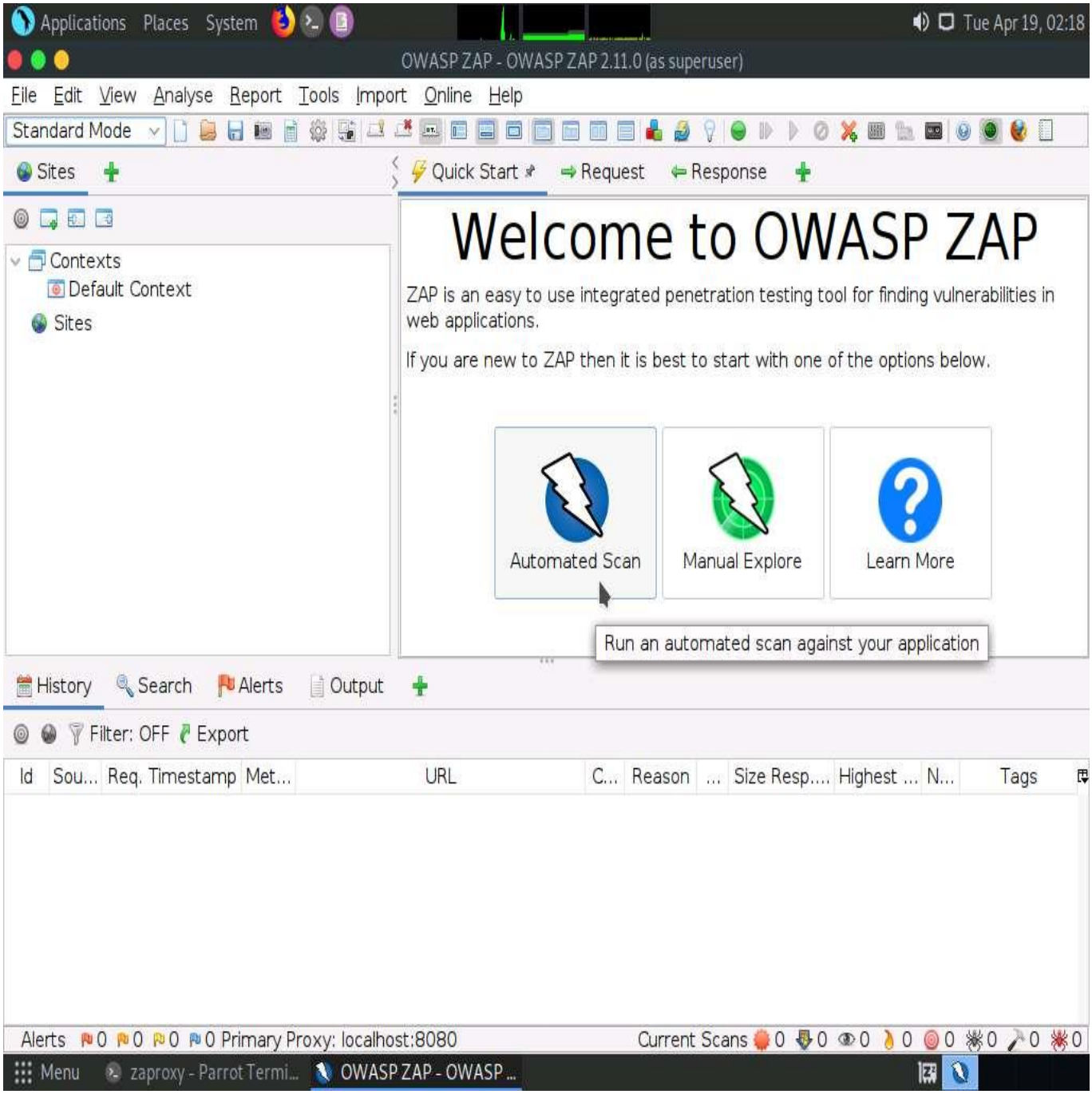



6. ☐ The **OWASP ZAP** initializing window appears; wait for it to complete.
7. ☐ After completing initialization, a prompt that reads **Do you want to persist the ZAP Session?** appears; select the **No, I do not want to persist this session at this moment in time** radio button and click **Start**.

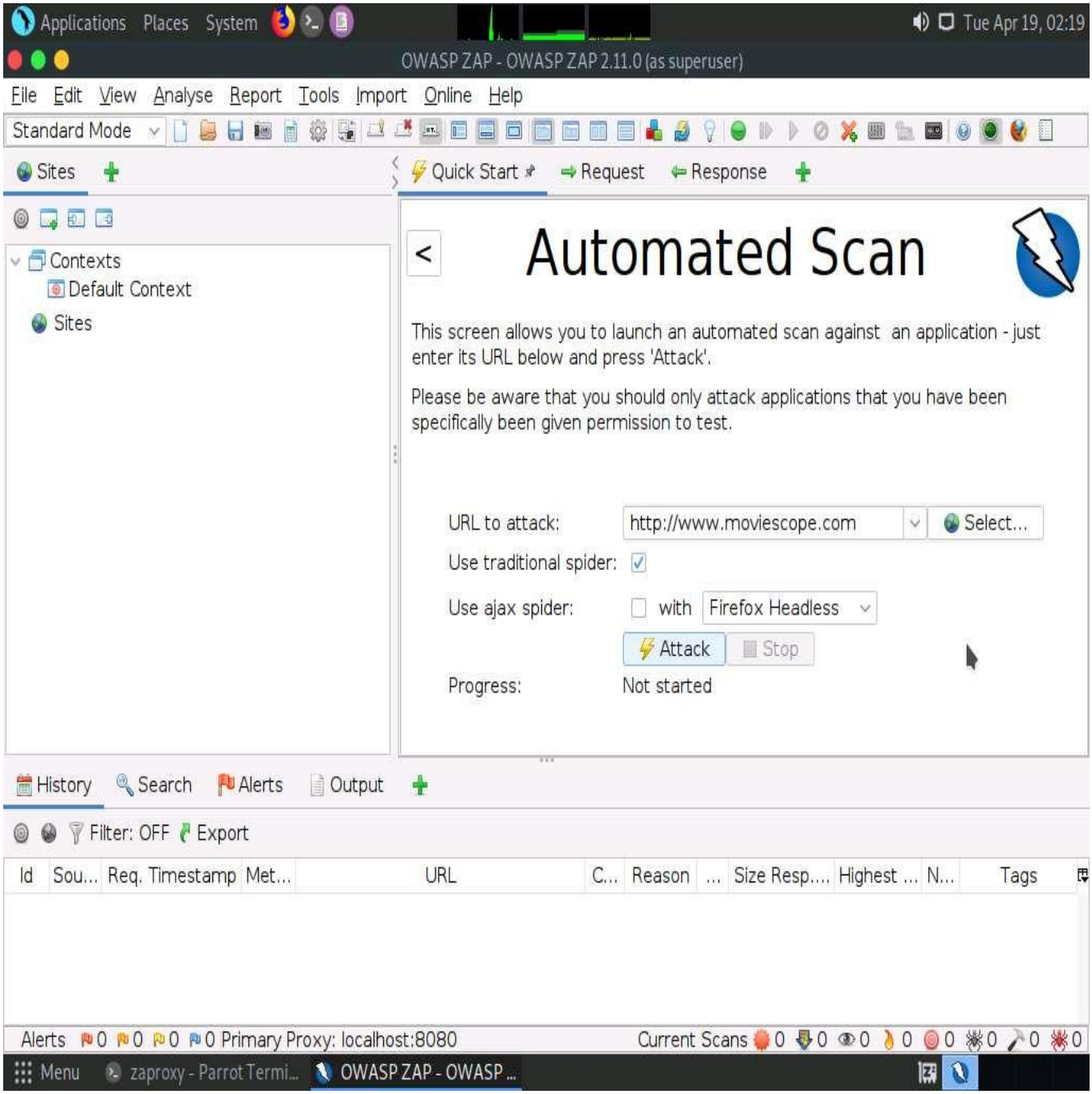
If a **Manage Add-ons** window appears, click the **Close** button.



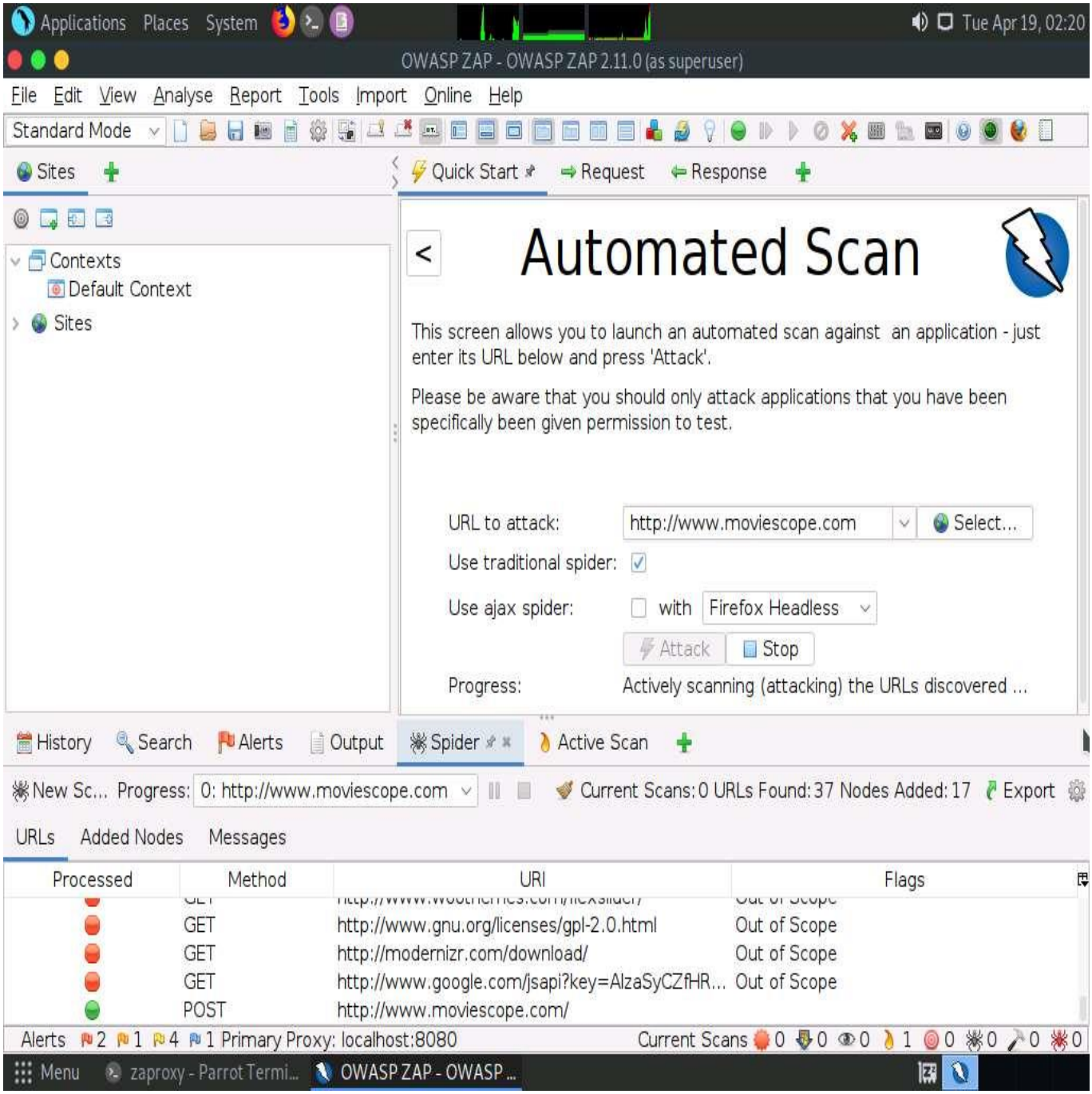

8. The **OWASP ZAP** main window appears. Under the **Quick Start** tab, click the **Automated Scan** option under **Welcome to OWASP ZAP**.



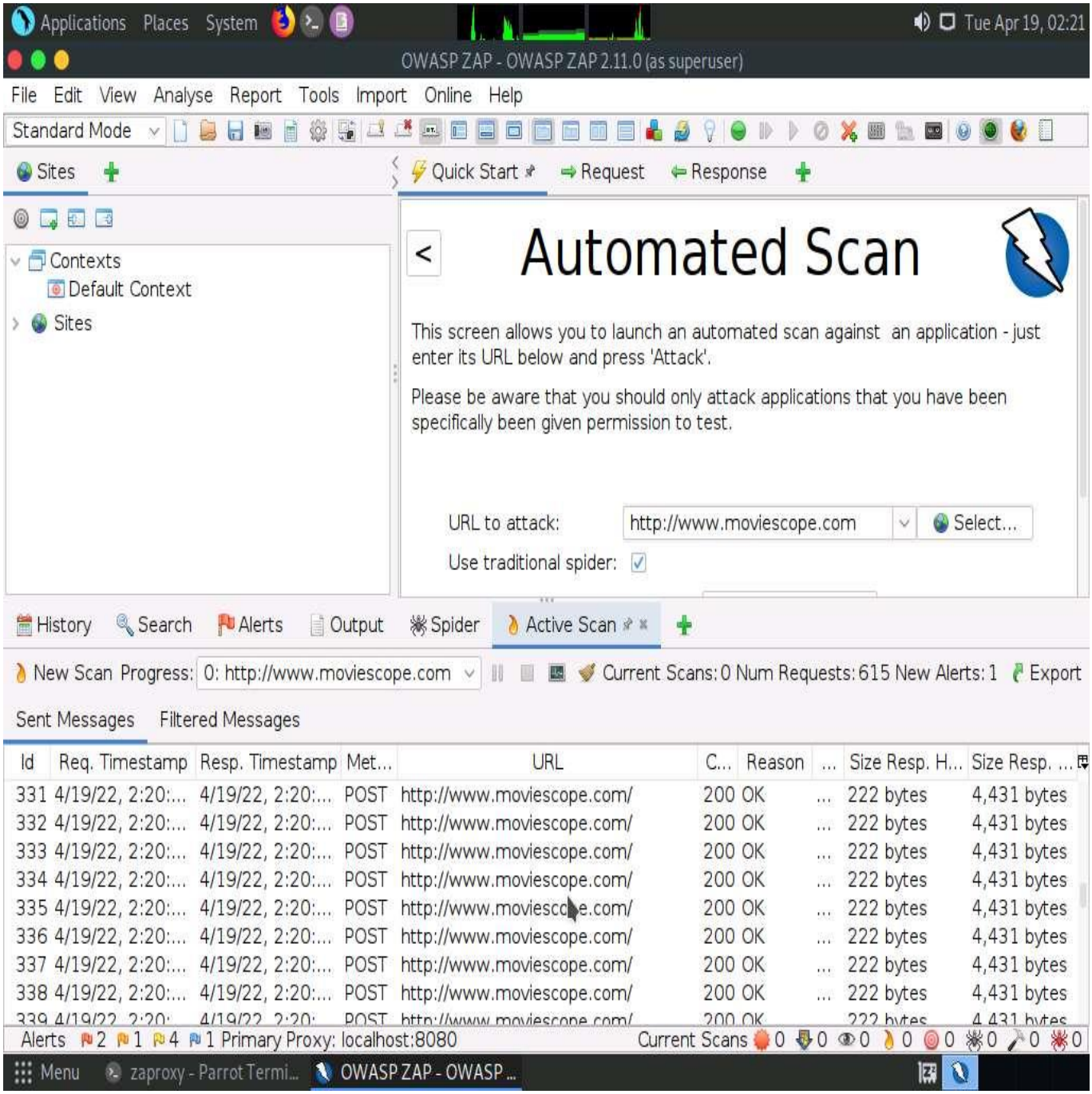

9. ☐ The **Automated Scan** wizard appears; enter the target website under the **URL to attack** field (here, **www.moviescope.com**). Leave the other settings to default and click the **Attack** button.




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

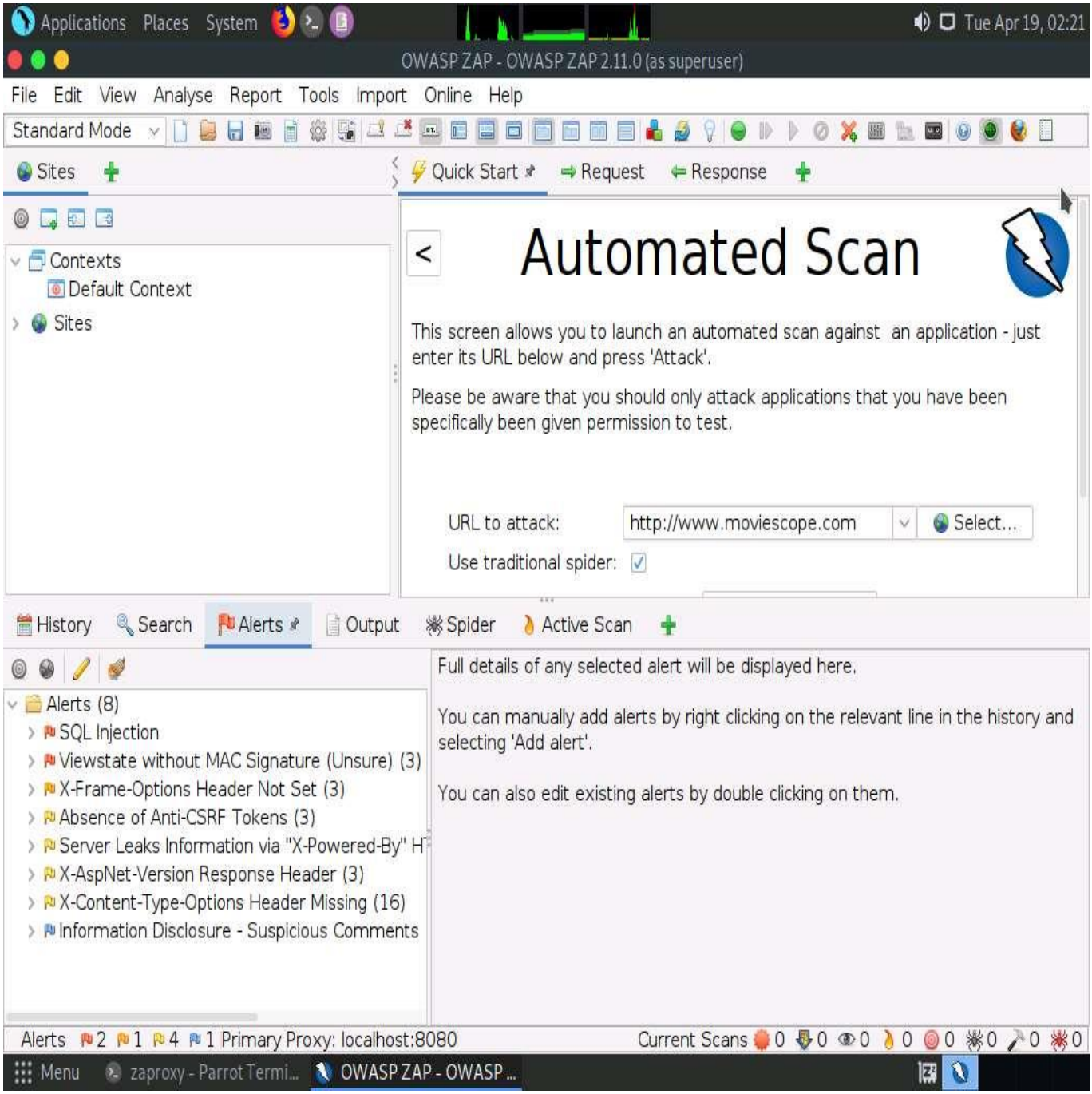



11. ☐ After performing web spidering, **OWASP ZAP** performs active scanning. Navigate to the **Active Scan** tab to observe the various scanned links.

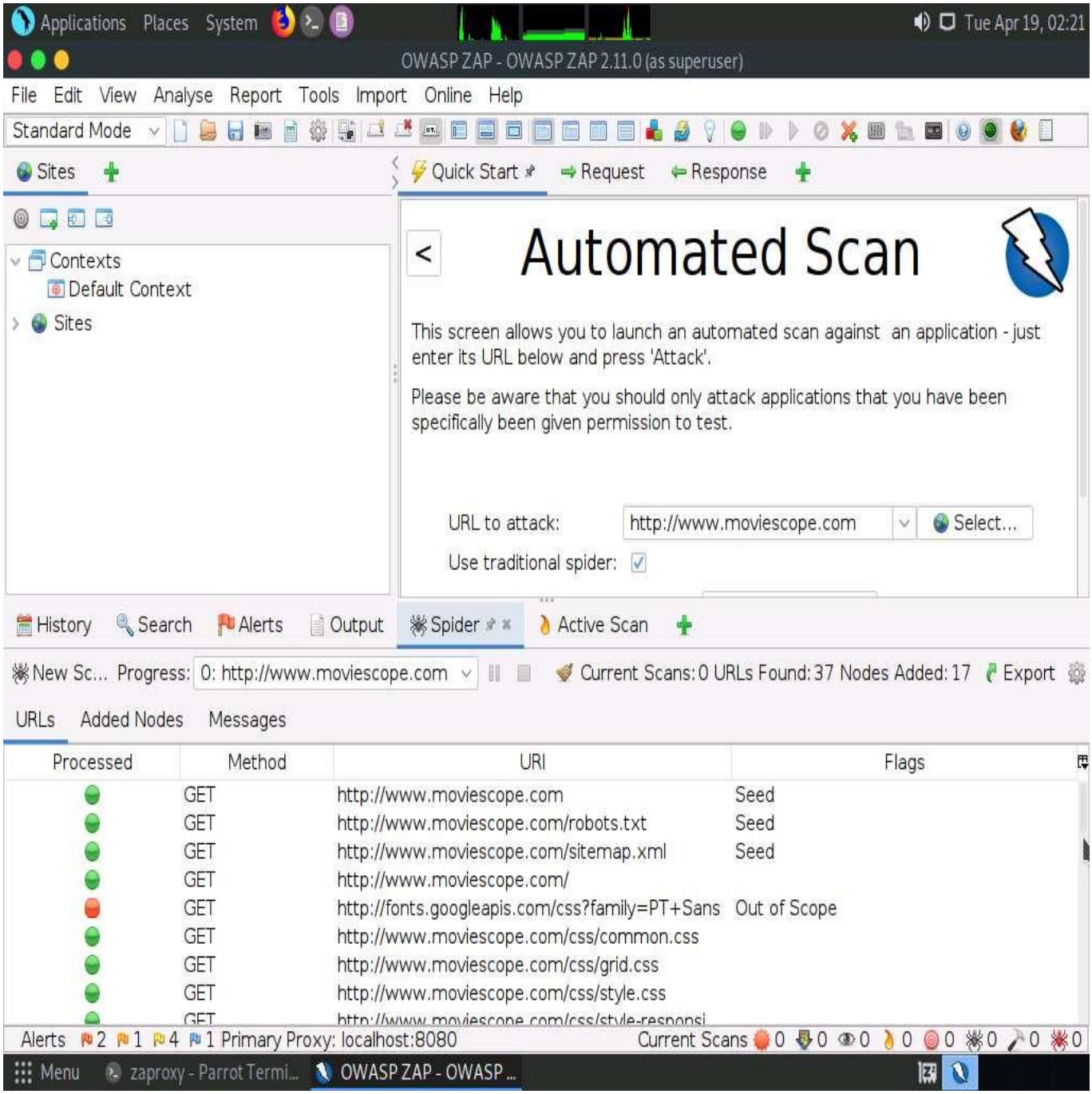



12. ☐ After completing the active scan, the results appear under the **Alerts** tab, displaying the various vulnerabilities and issues associated with the target website, as shown in the screenshot.

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

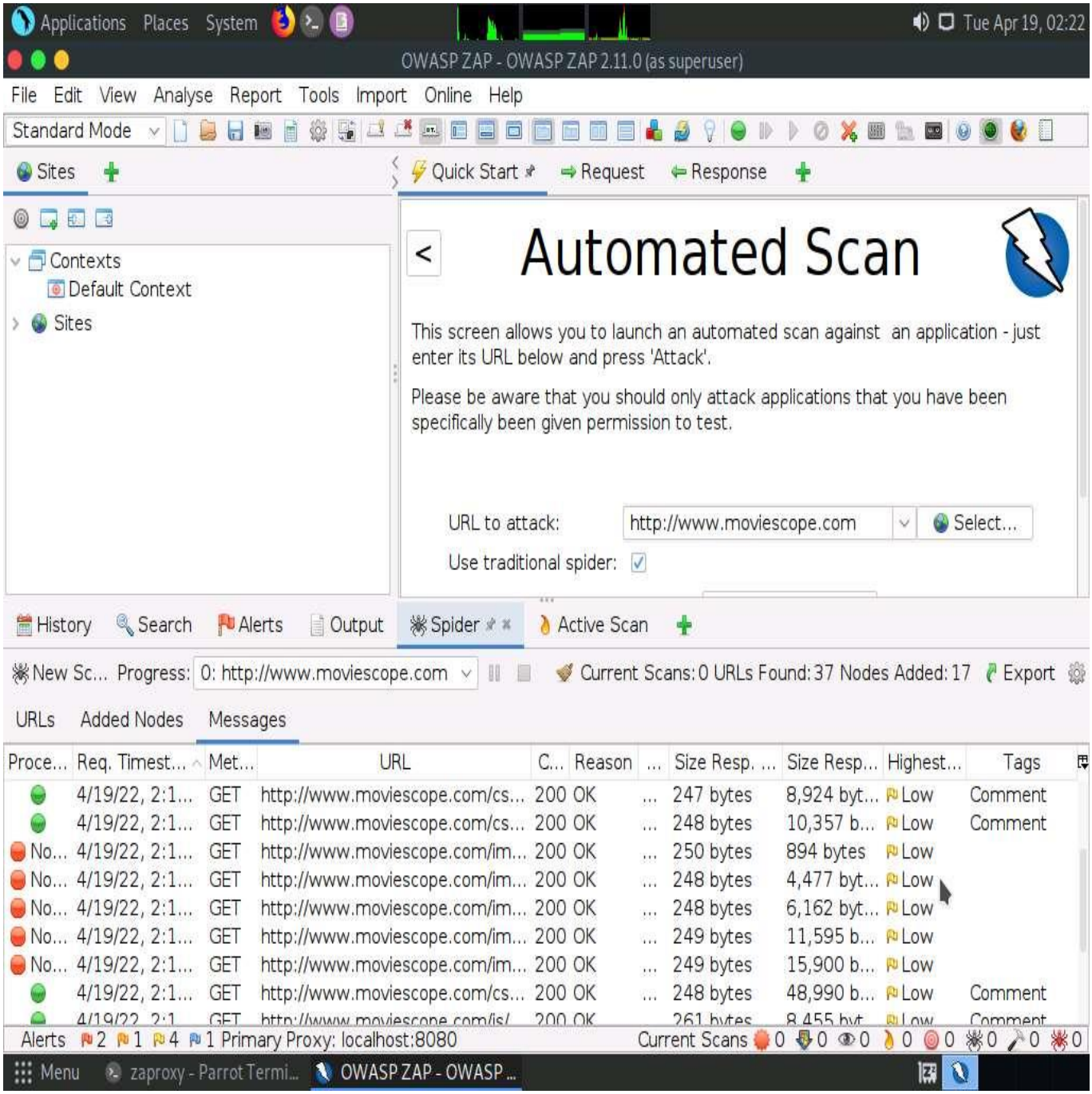



13. ☐ Now, click on the **Spider** tab from the lower section of the window to view the web spidering information. By default, the **URLs** tab appears under the **Spider** tab.
14. ☐ The **URLs** tab contains various links for hidden content and functionality associated with the target website (**www.moviescope.com**).




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.

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.
more...




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.

---

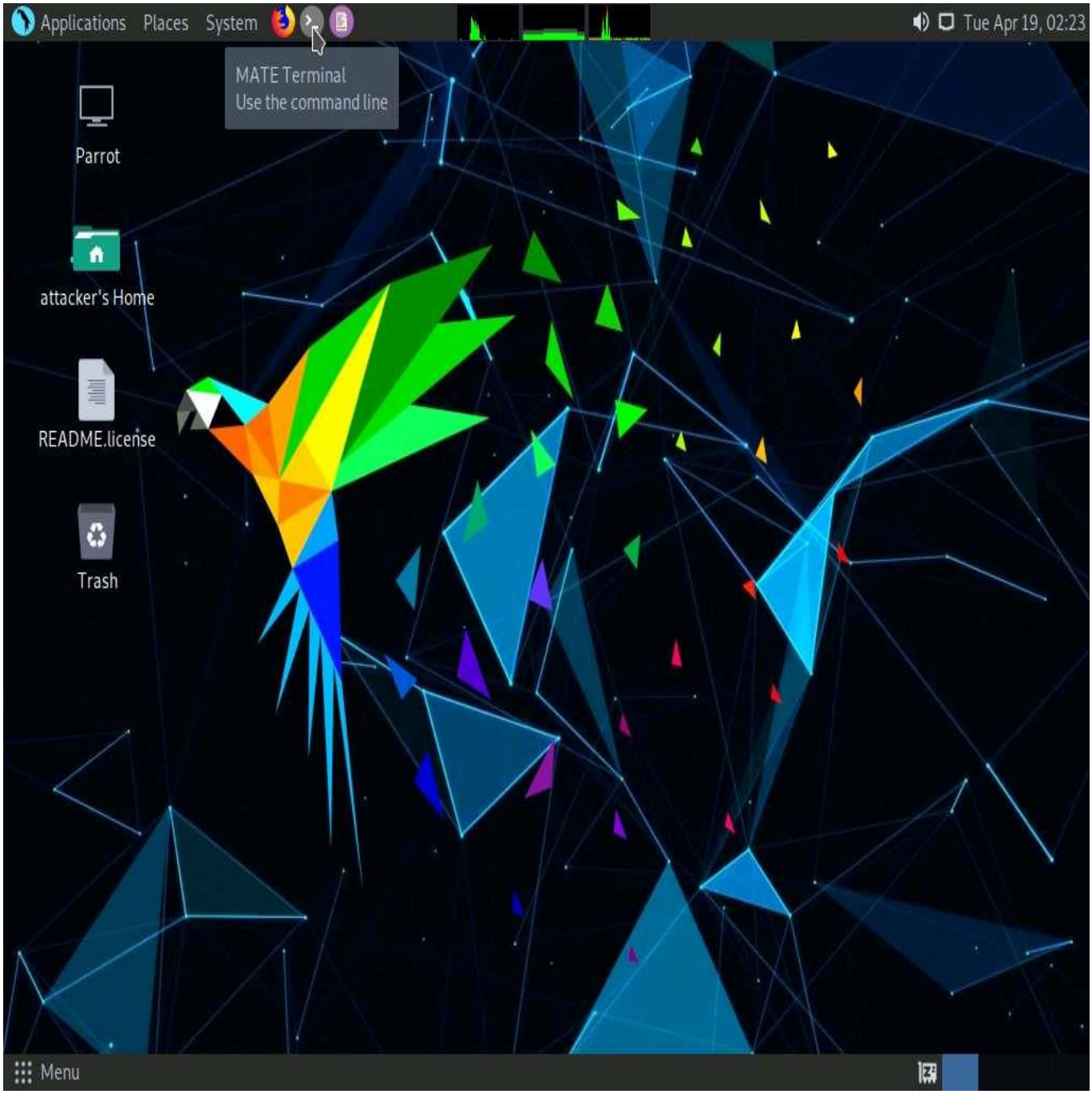
## Task 4: Detect Load Balancers using Various Tools

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.

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.

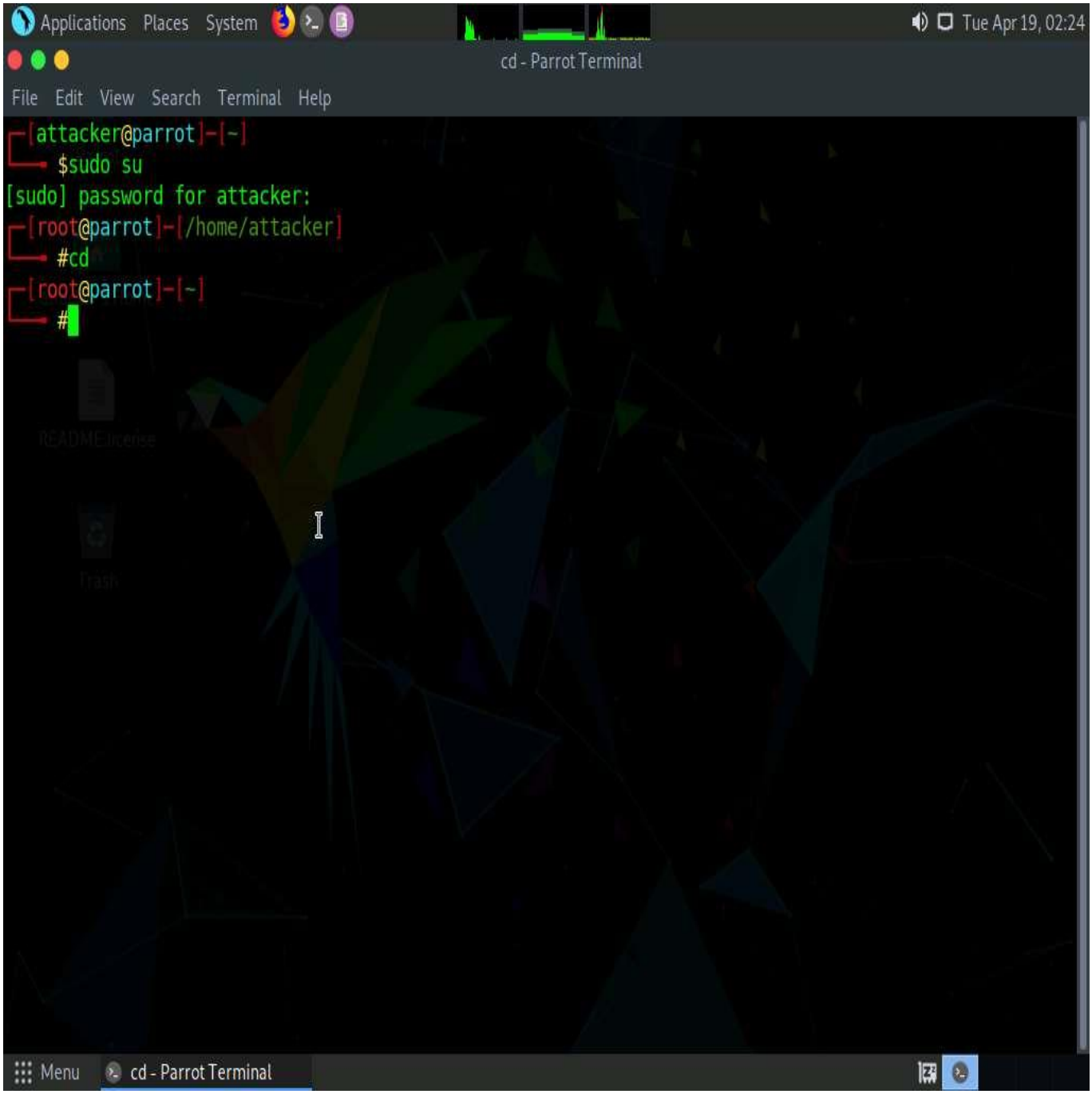
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.



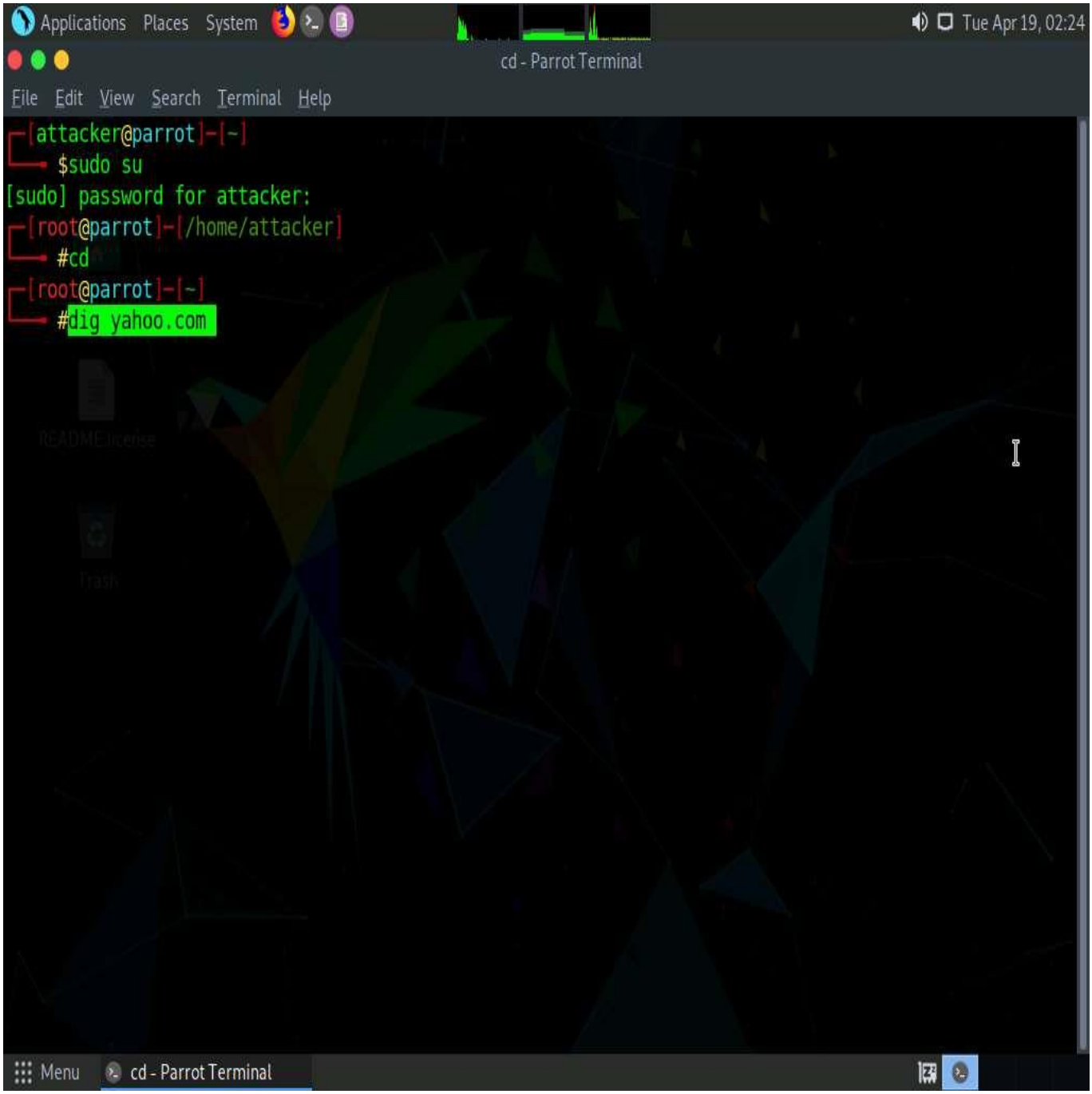

2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

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

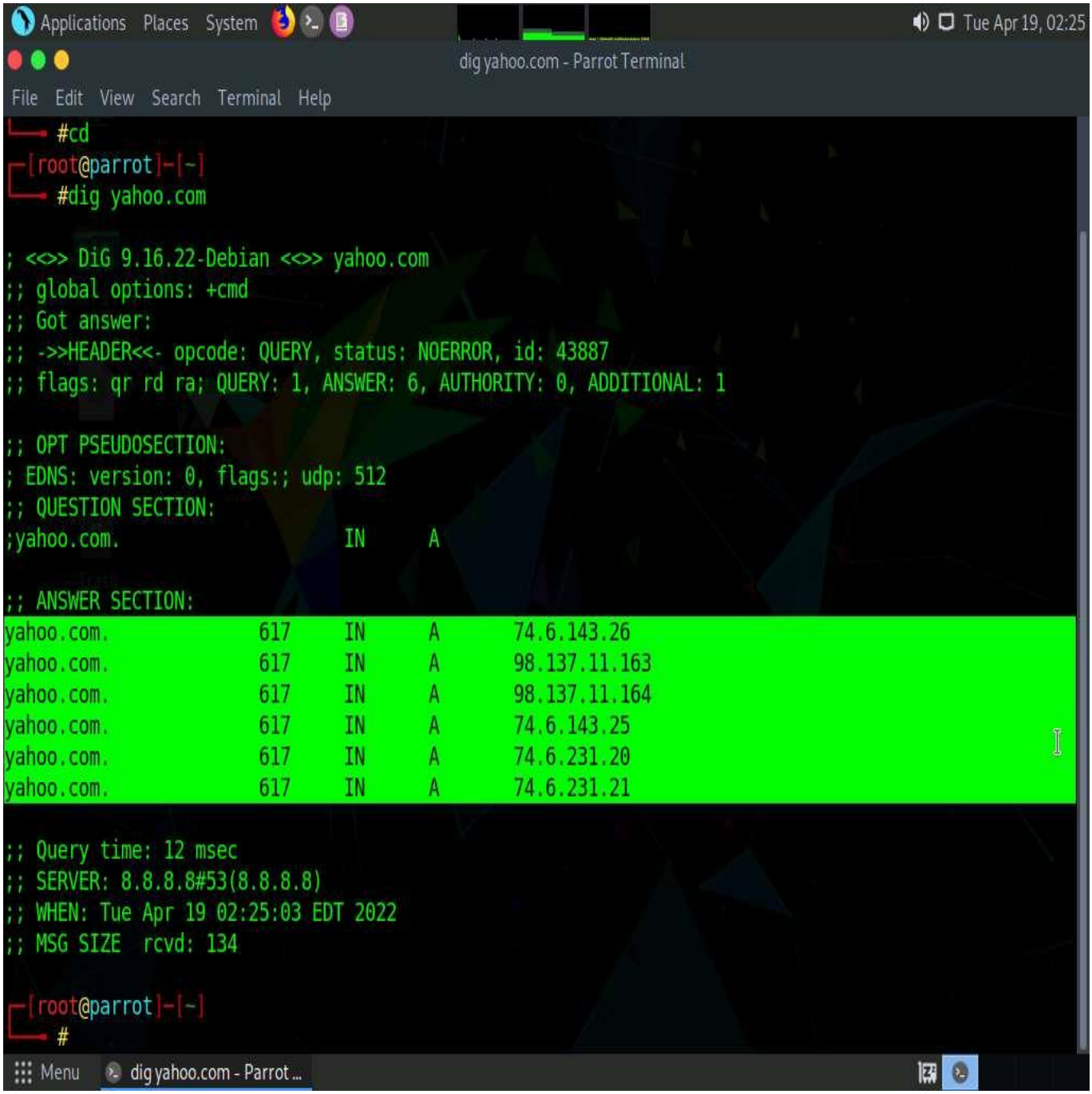



5. A **Parrot Terminal** window appears; type **dig yahoo.com** and press **Enter**.



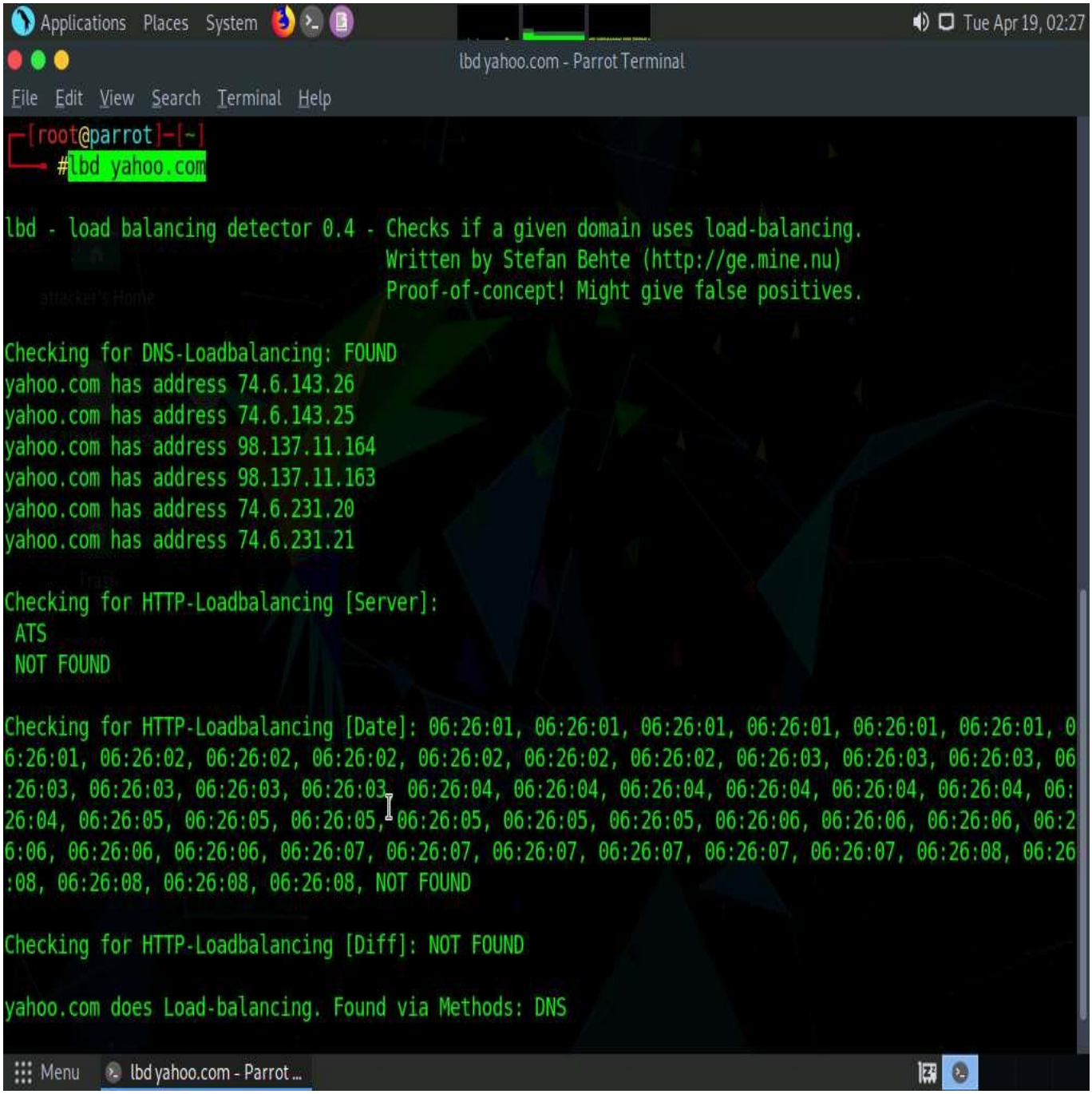

6. ☐ The result appears, displaying the available load balancers of the target website, as the screenshot demonstrates. Here, a single host resolves to multiple IP addresses, which possibly indicates that the host is using a load balancer.

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.

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.

---

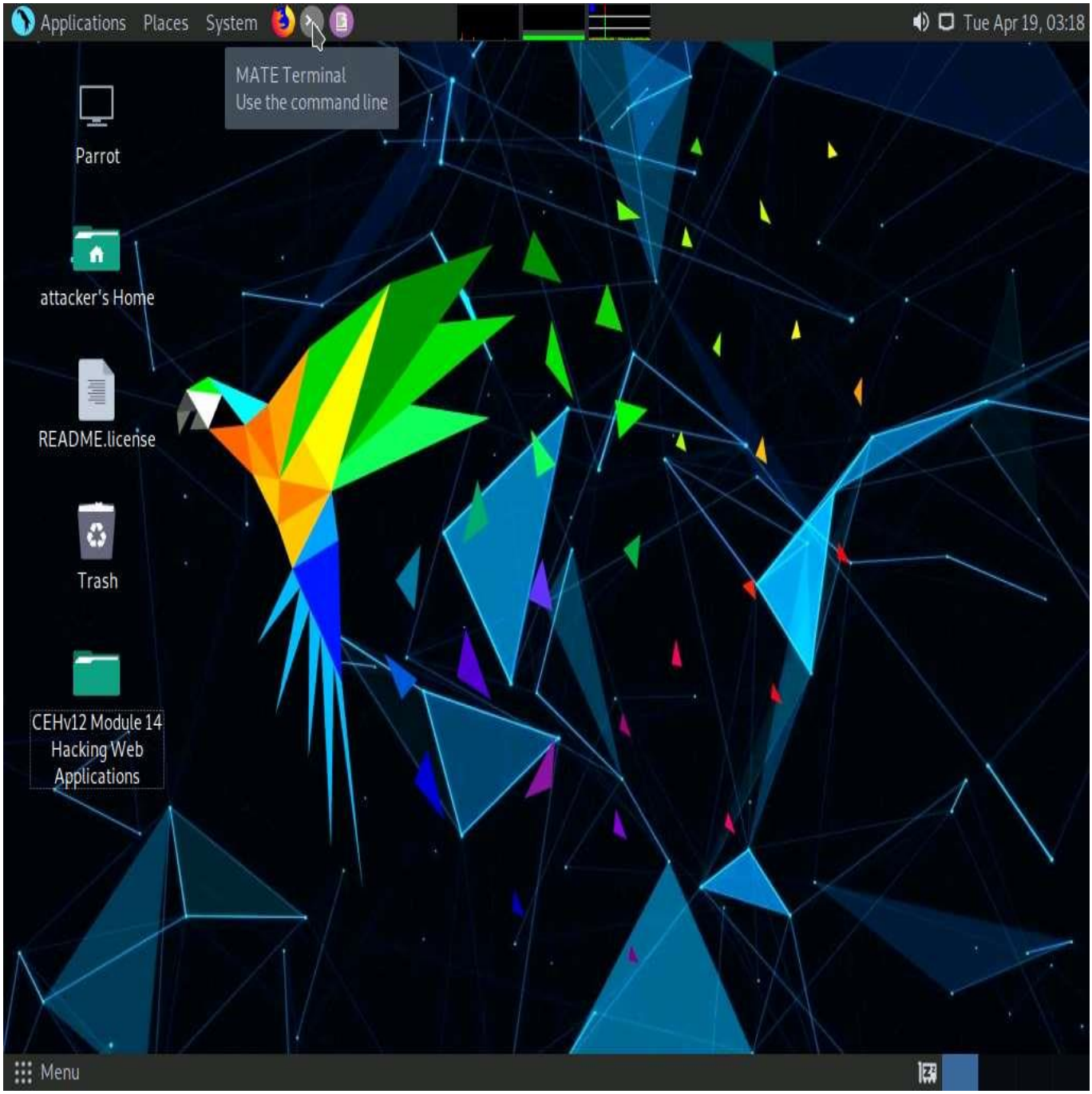
## Task 5: Identify Web Server Directories using Various Tools

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.

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.

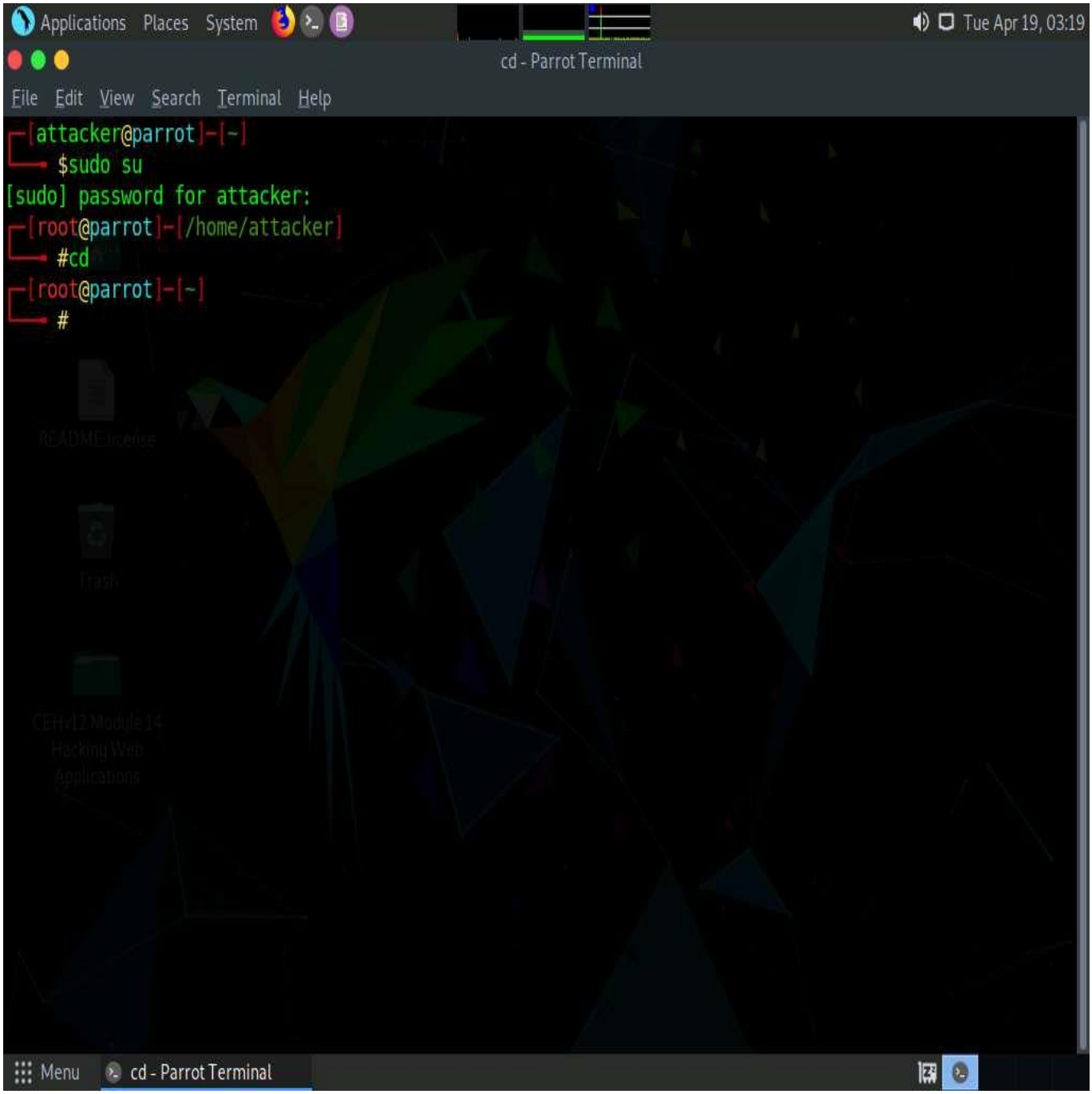
1. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.




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**.

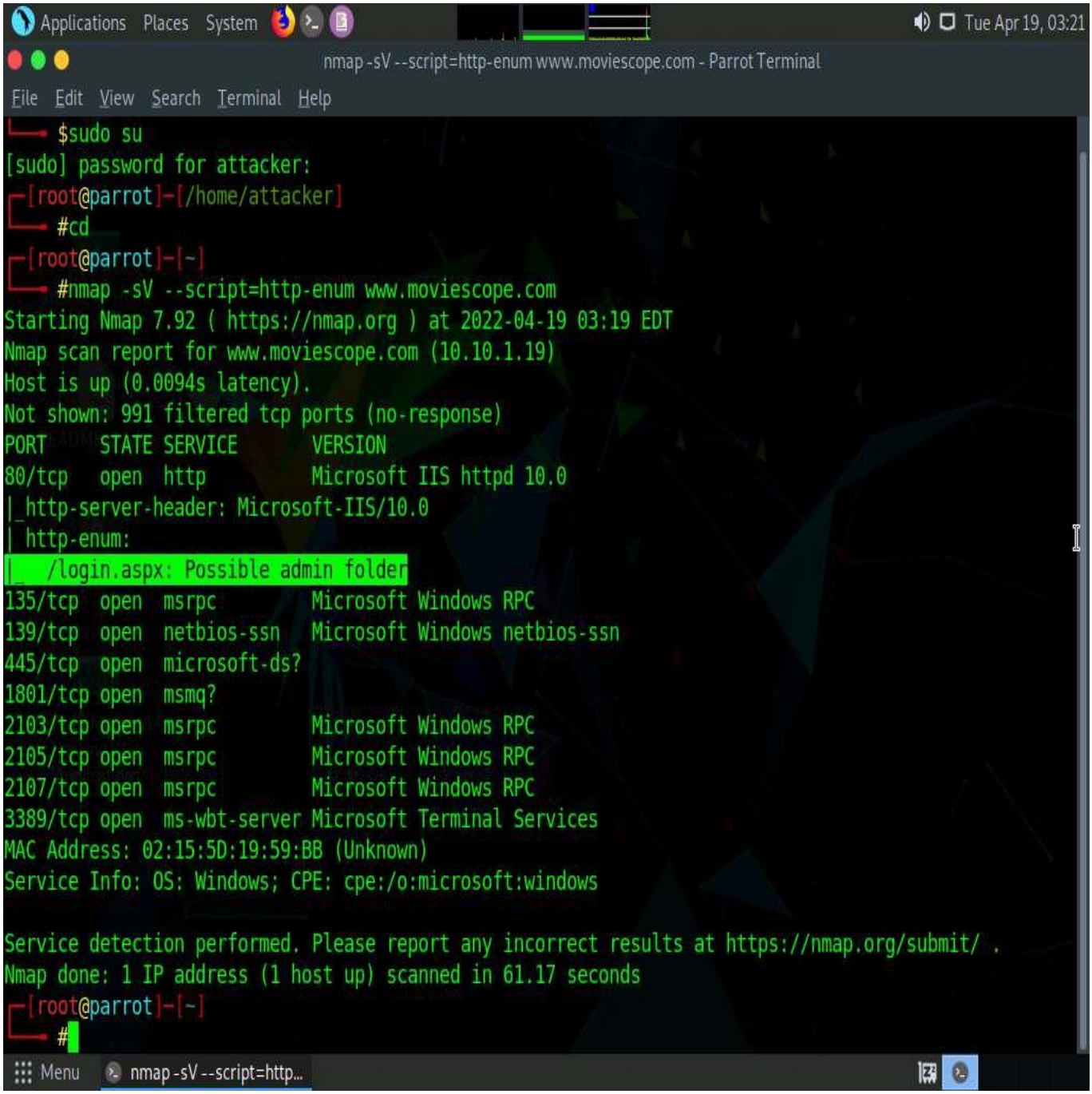
The password that you type will not be visible.

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

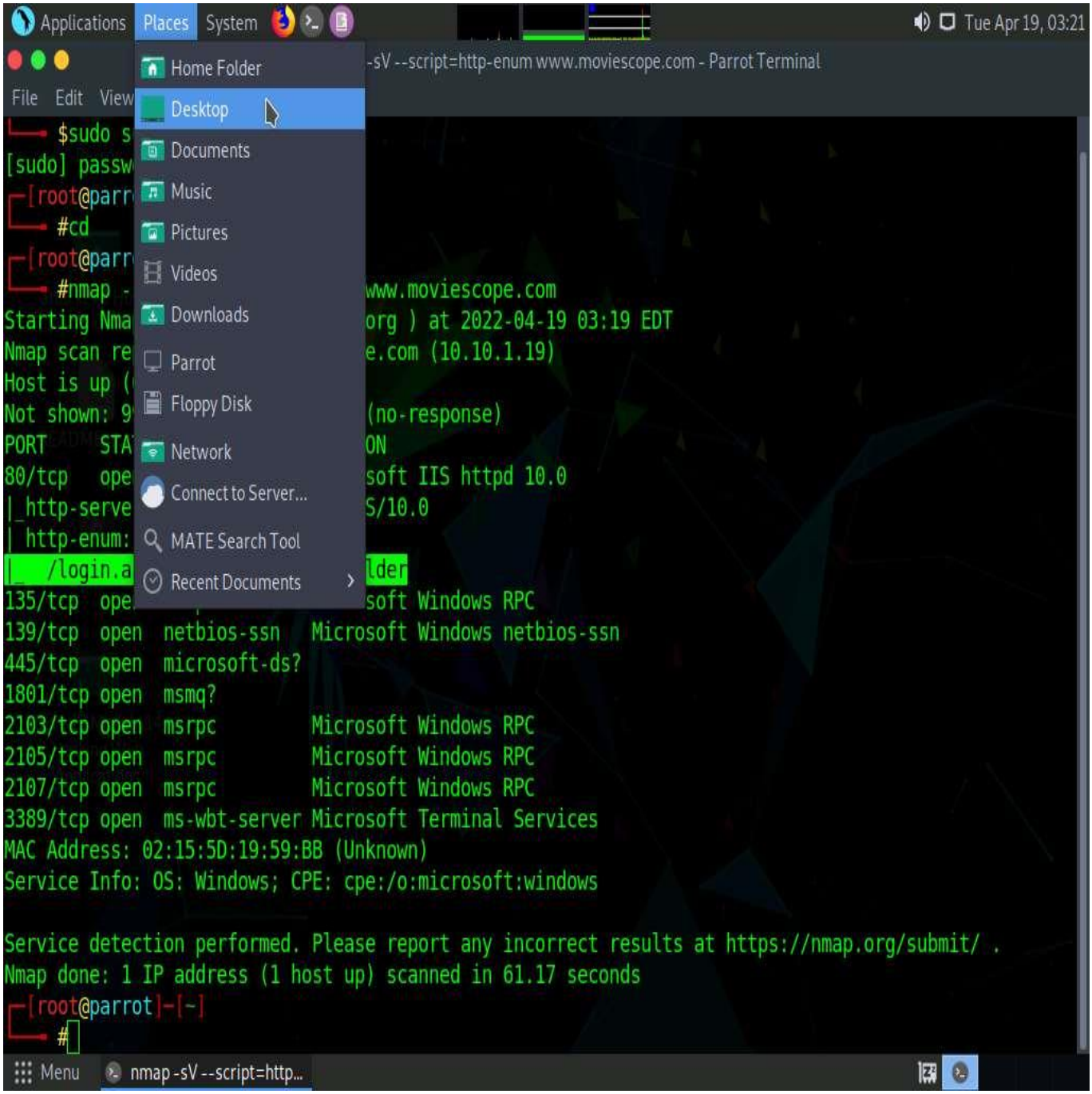



5. ☐ A **Parrot Terminal** window appears; type **nmap -sV --script=http-enum [target domain or IP address]** (here, the target website is **www.moviescope.com**) and press **Enter**.
6. ☐ The result appears, displaying open ports and services, along with their version.
7. ☐ Scroll-down in the result and observe the identified web server directories under the **http-enum** section, as shown in the screenshot.

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.
more...

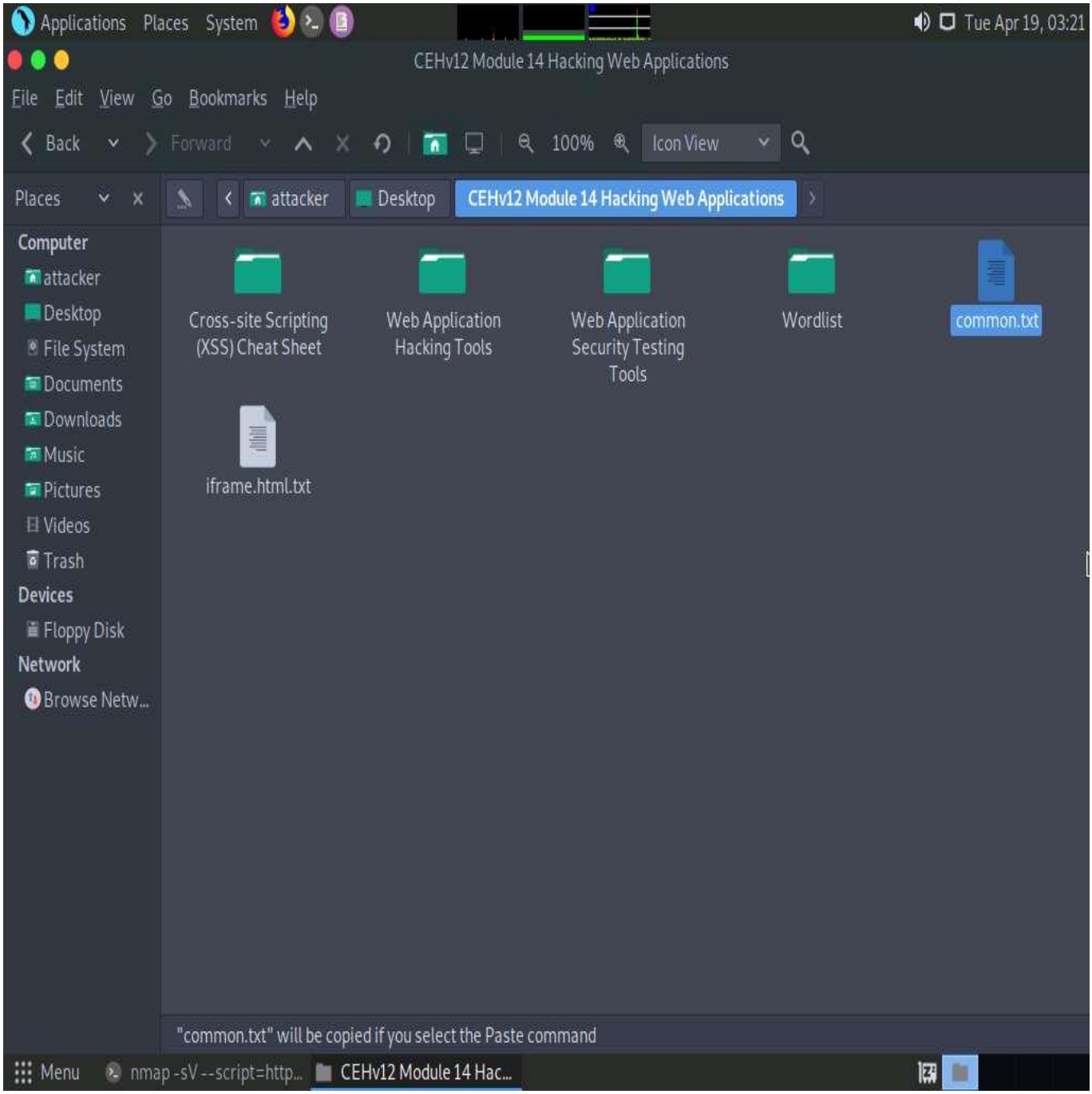



8. ☐ Now, we shall copy the wordlist file (**common.txt**) from a shared network drive. We will use this file in the Gobuster tool.
9. ☐ Minimize the **Terminal** window.
10. ☐ Click **Places** from the top-section of the **Desktop** and click **Desktop** from the drop-down options.



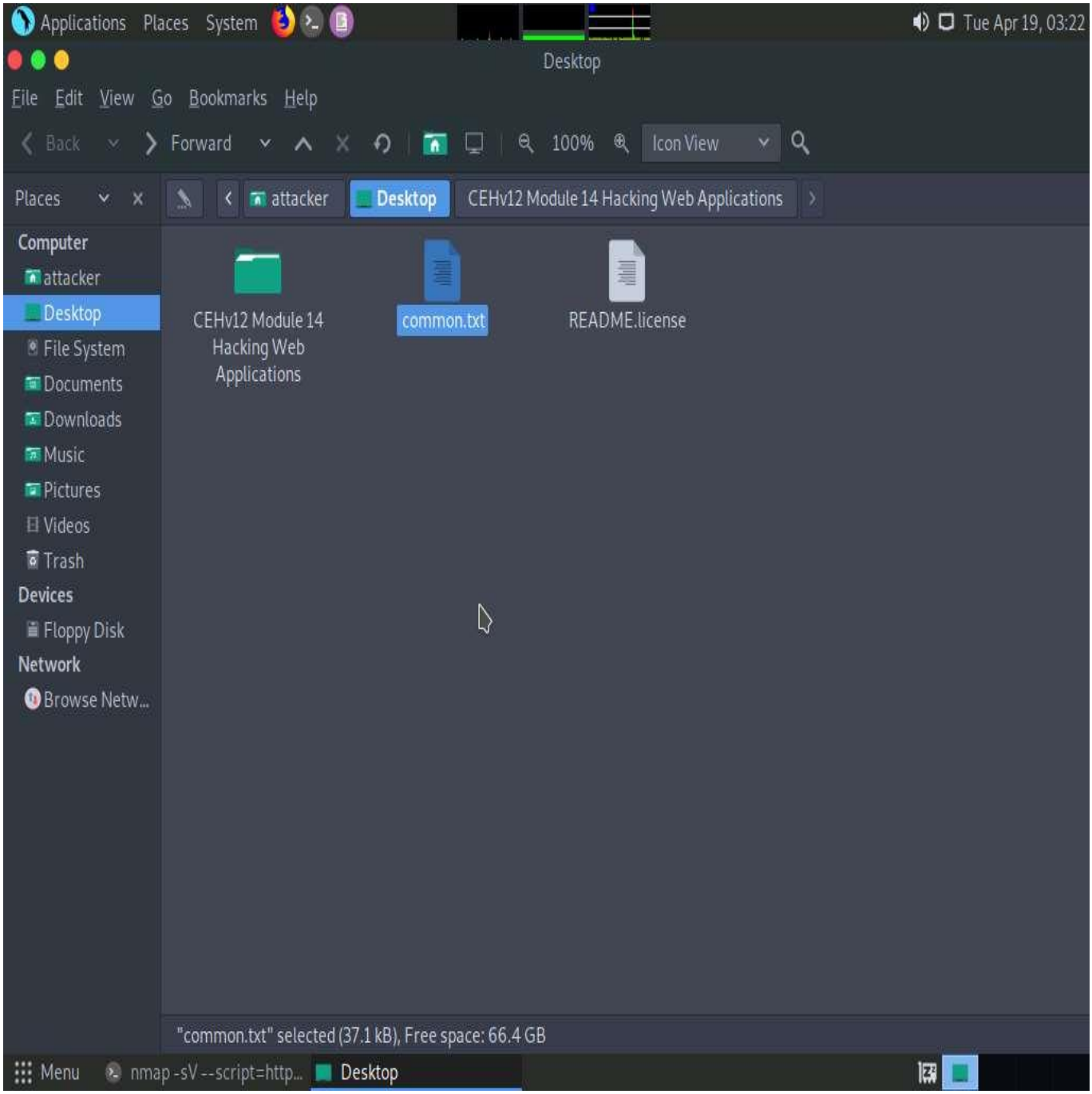

11. ☐ Navigate to **CEHv12 Module 14 Hacking Web Applications** folder and copy **common.txt** file.

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



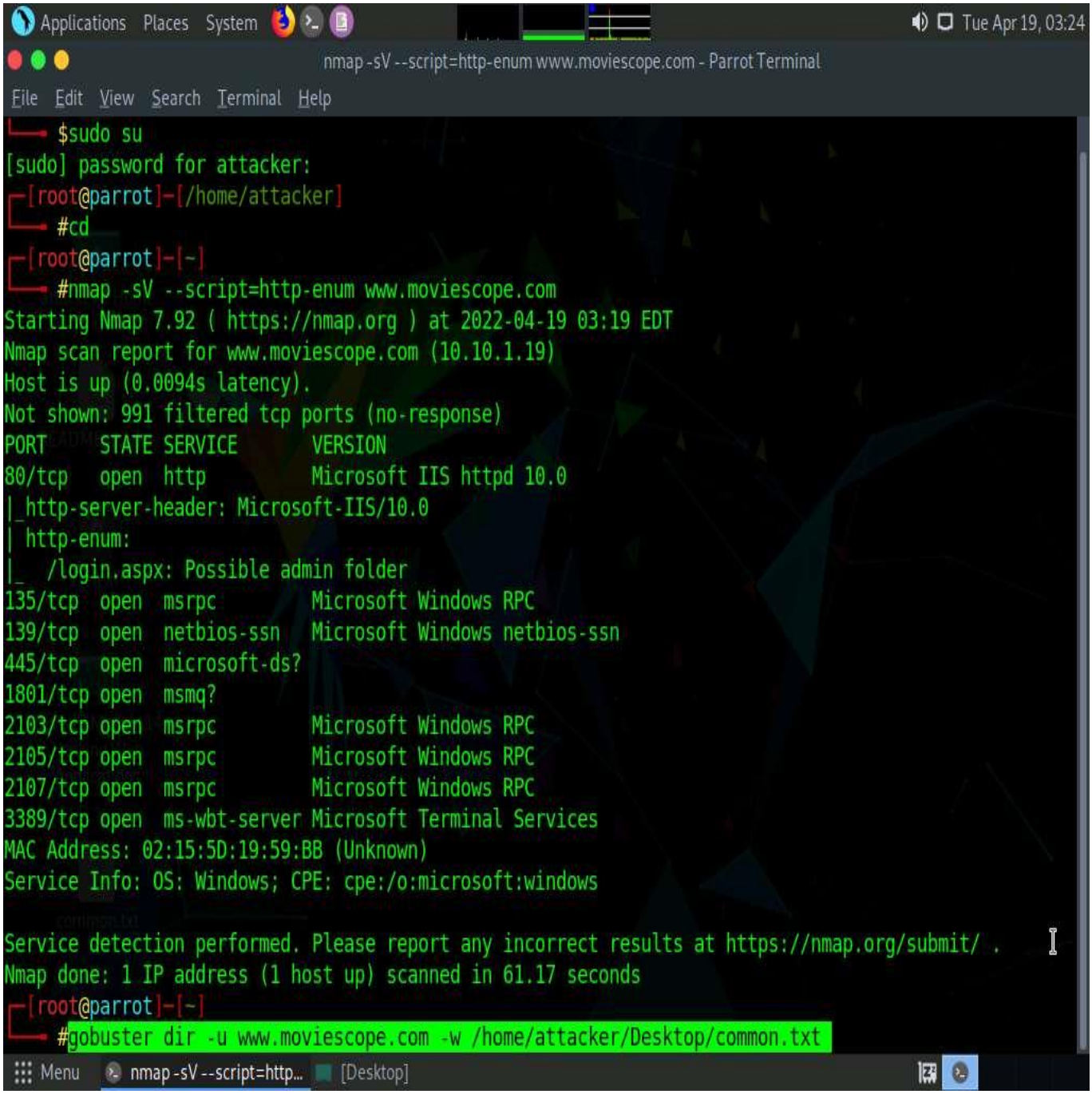

12. ☐ Paste the copied file (**common.txt**) on the **Desktop**. Close the window.

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



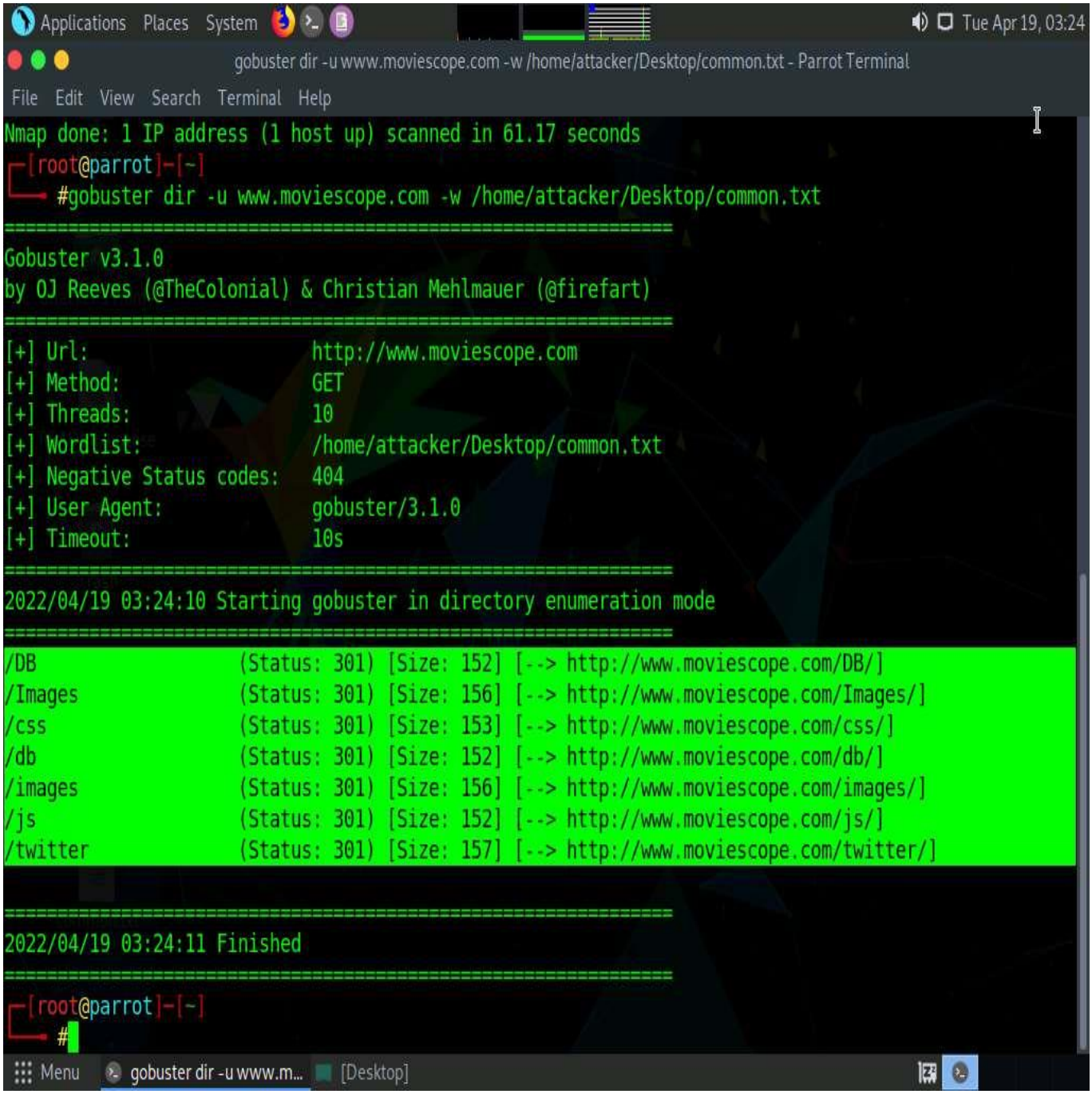

13. Now, switch back to the **Terminal** window, type **gobuster dir -u [Target Website] -w /home/attacker/Desktop/common.txt**, and press **Enter**.

**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**).



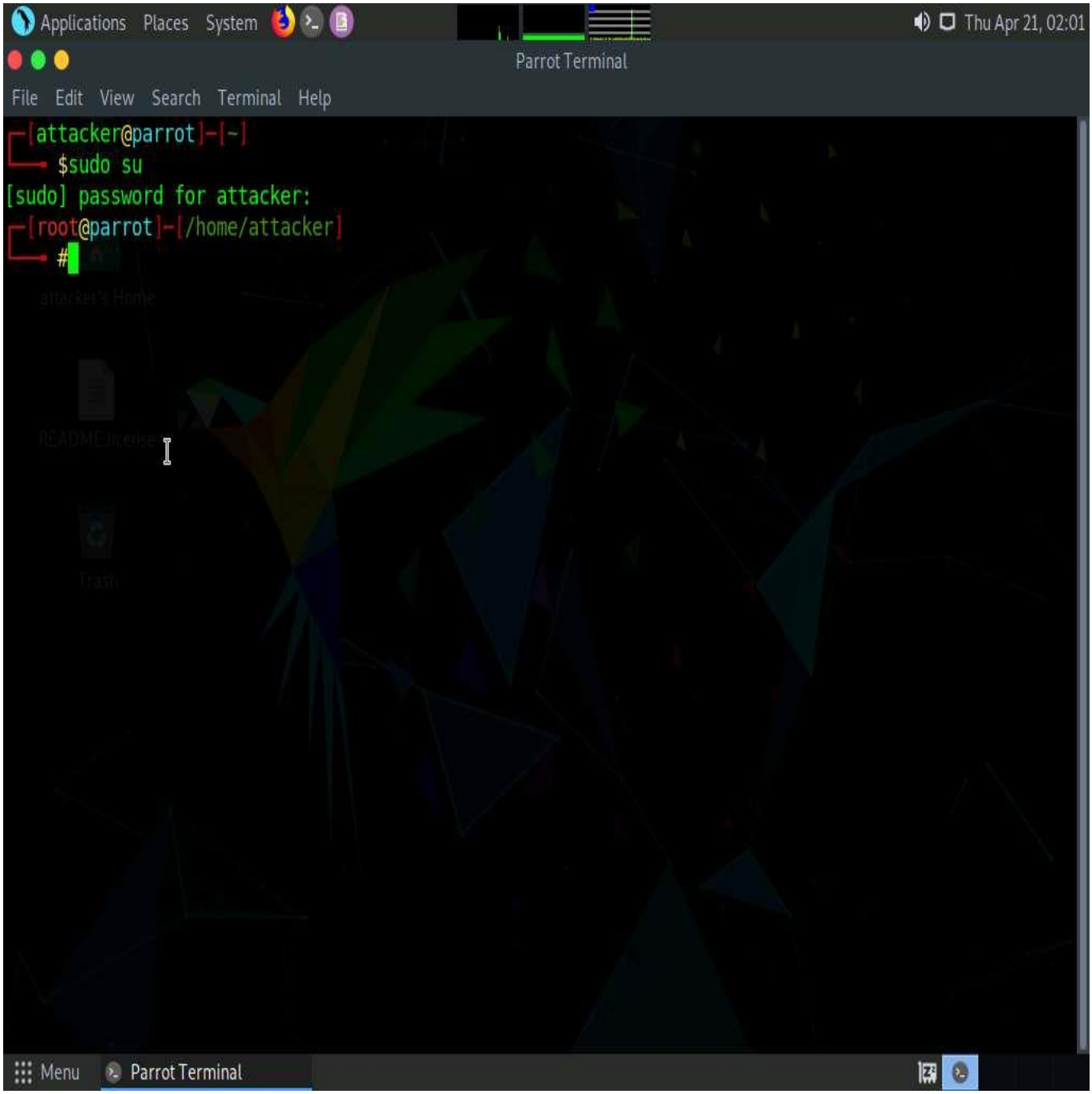

14. ☐ The result appears, displaying the identified web server directories, as shown in the screenshot.

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.

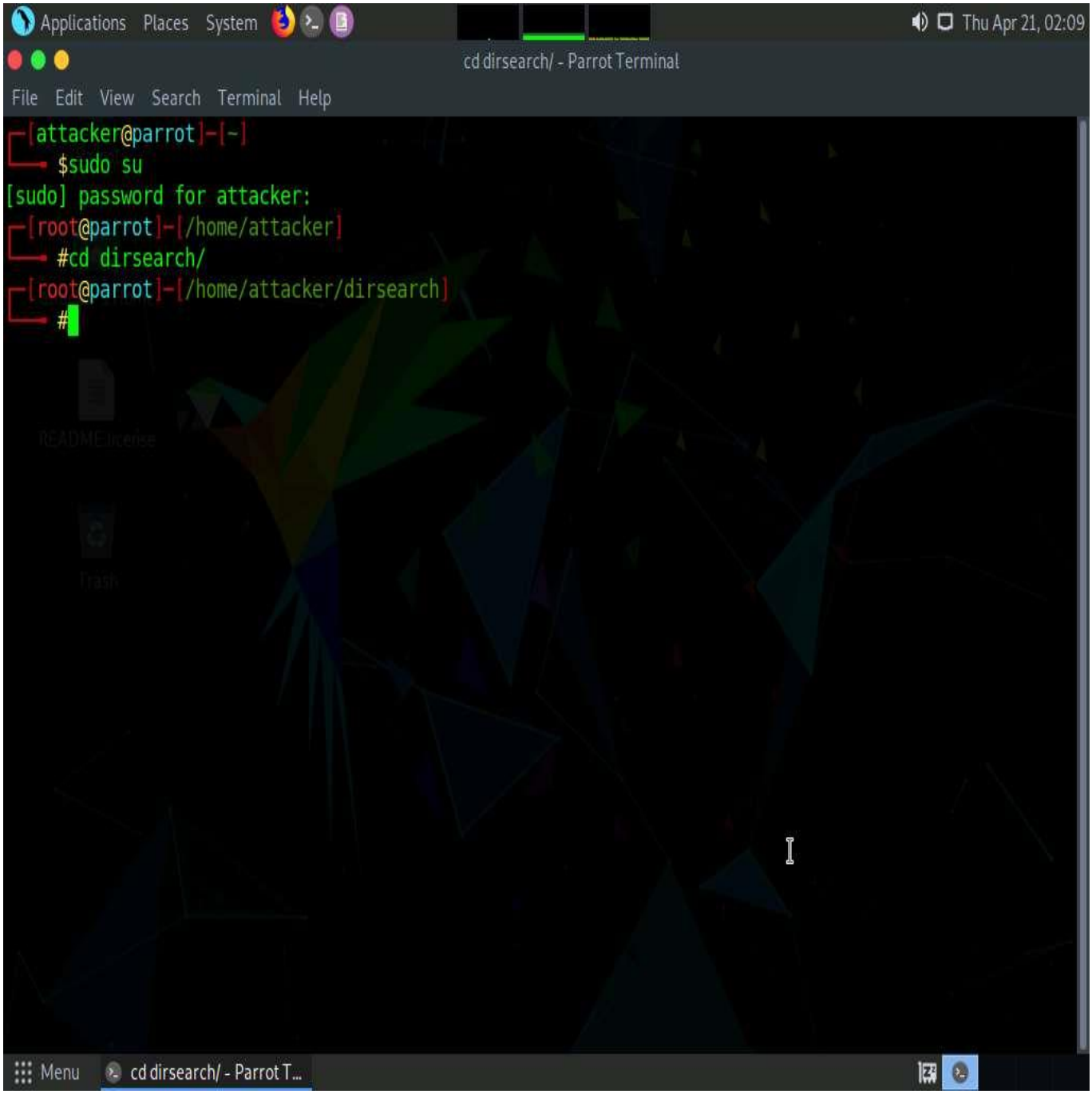



15. ☐ Now, click the **MATE Terminal** icon at the top of the **Desktop** window to open a **Terminal** window.
16. ☐ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
17. ☐ In the **[sudo] password for attacker** field,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

The password that you type will not be visible.

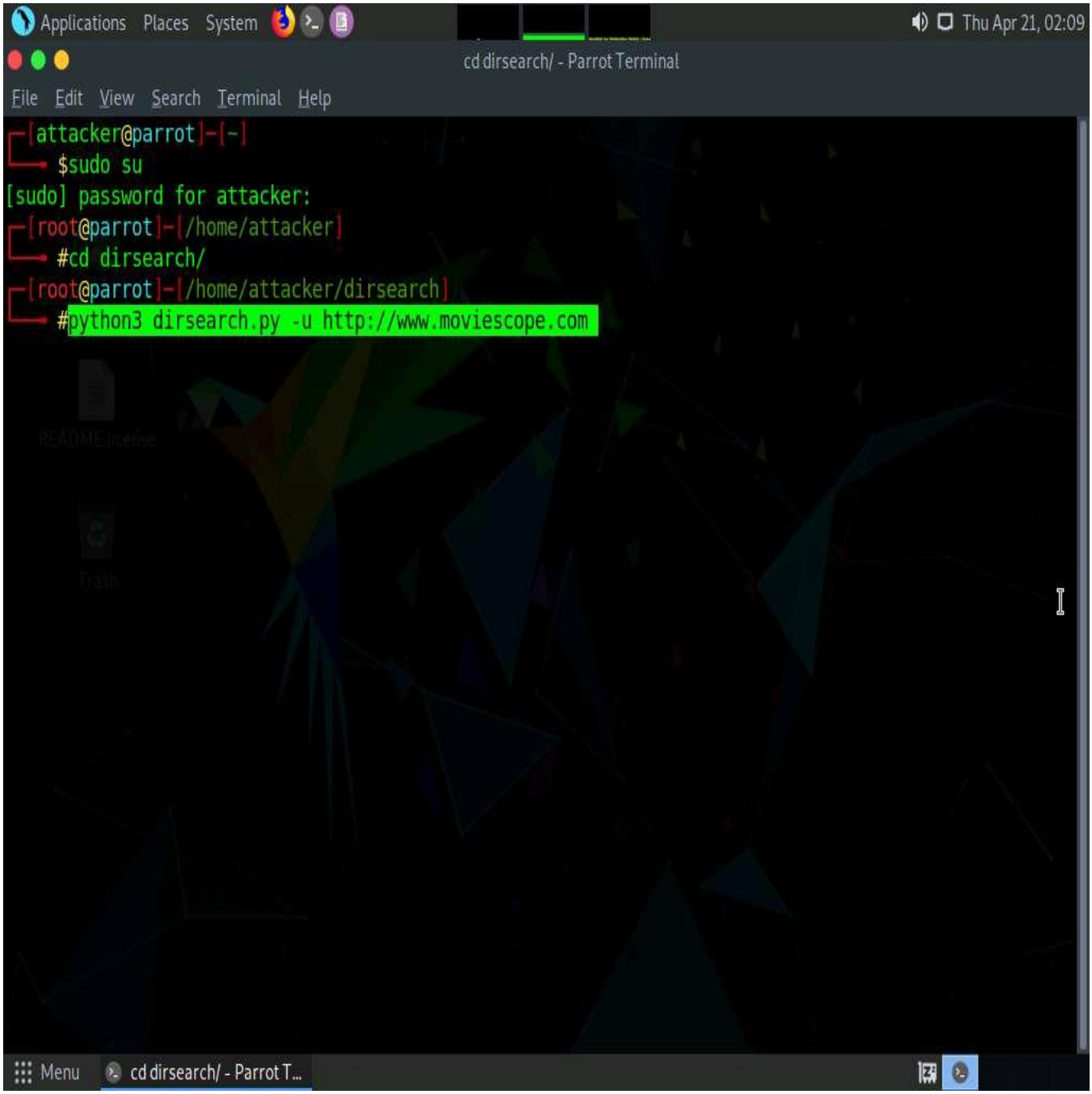



18. Navigate to the dirsearch directory to do that, type **cd dirsearch/** and press **Enter**.

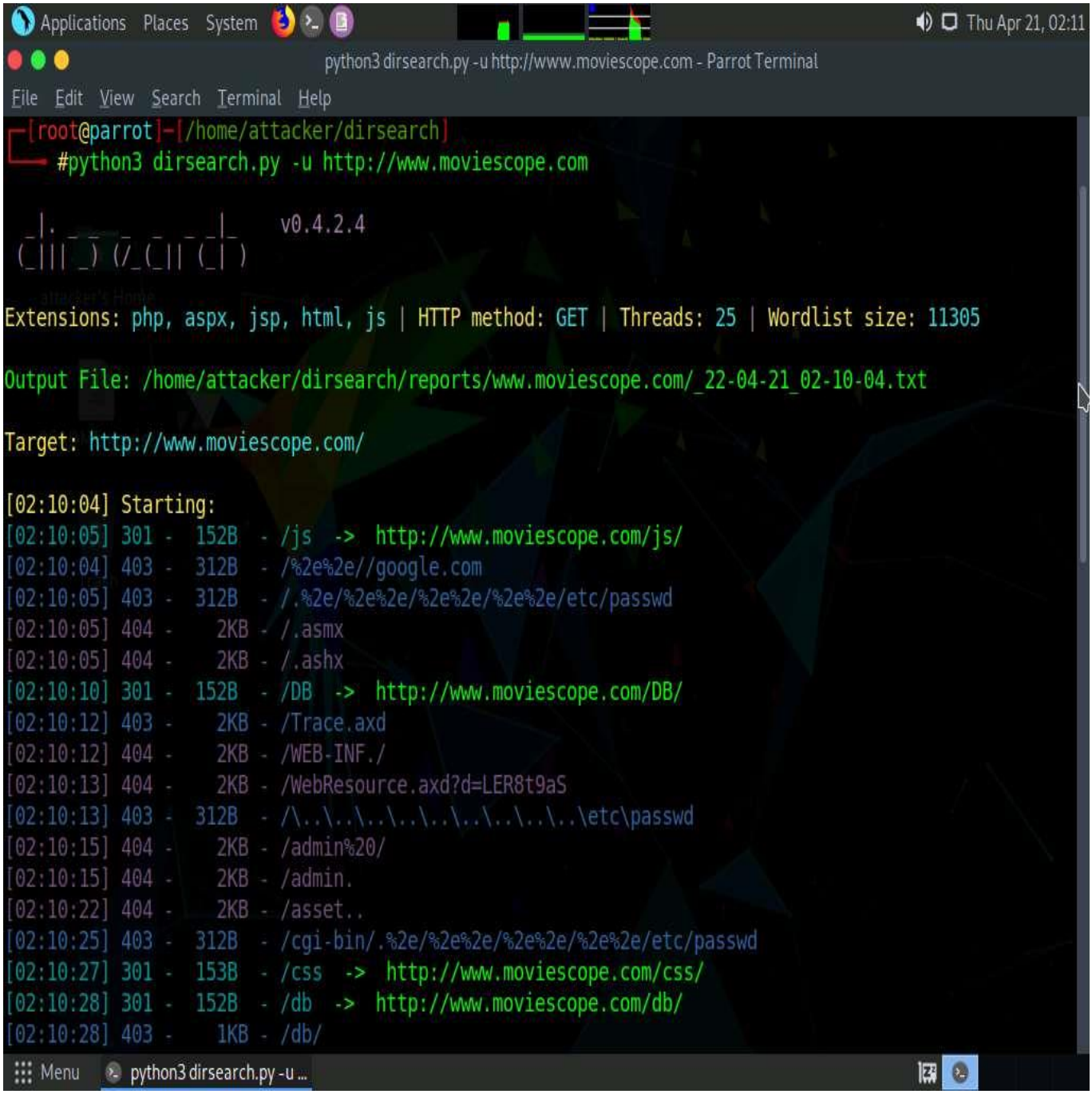



19. ☐ Type **python3 dirsearch.py -u http://www.moviescope.com** and press **Enter**, to start directory brute forcing.

**-u**: specifies target URL.

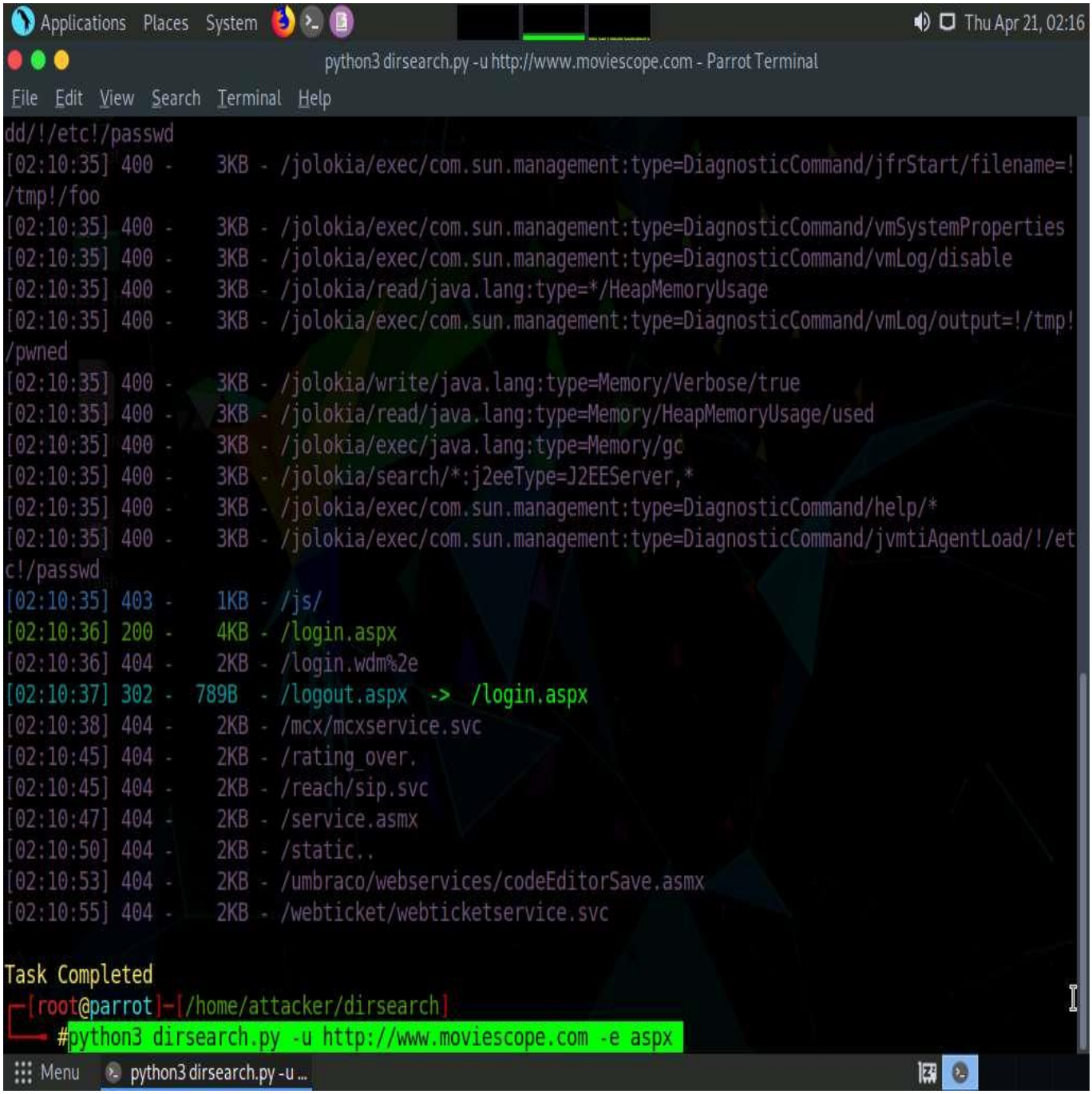



20. **dirsearch** starts listing all the directories of the target website.

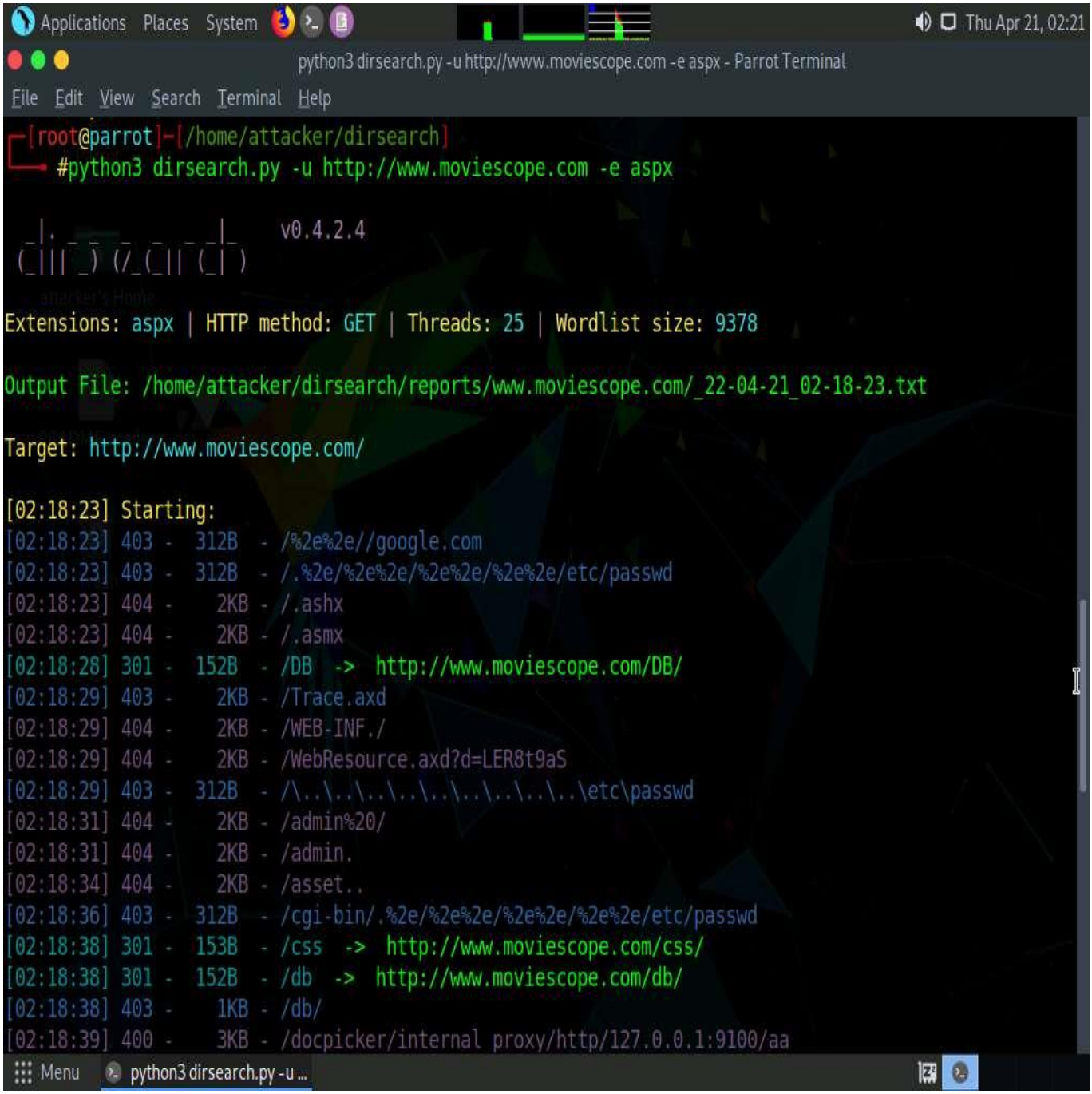



21. ☐ Now, we will perform directory bruteforcing on a specific file extension.
22. ☐ Type **python3 dirsearch.py -u http://www.moviescope.com -e aspx** and press **Enter**.

**-u**: specifies URL and **–e**: specifies extension of the file.

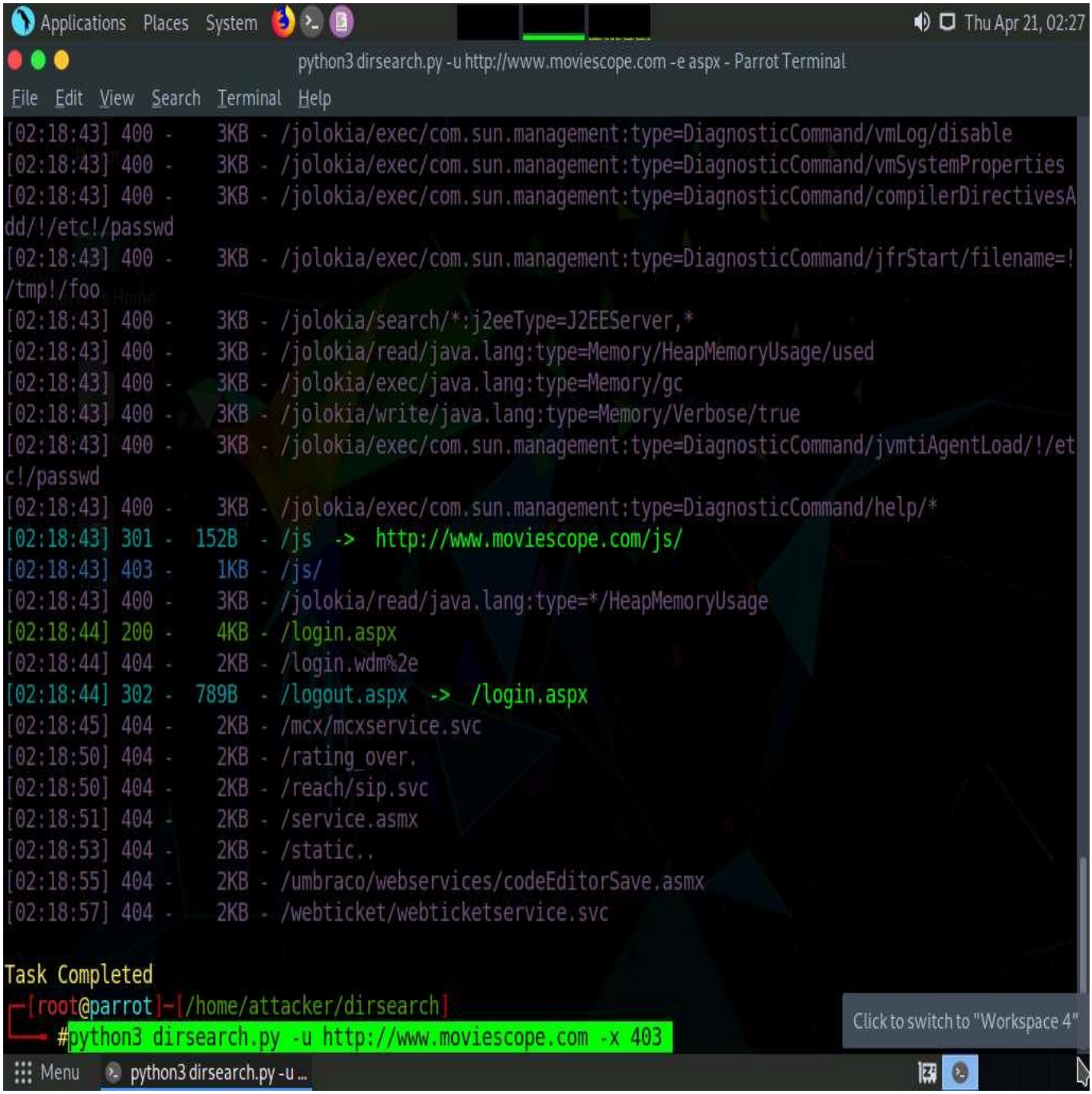



23. **dirsearch** lists all the files containing **aspx** extension, as shown in the screenshot.

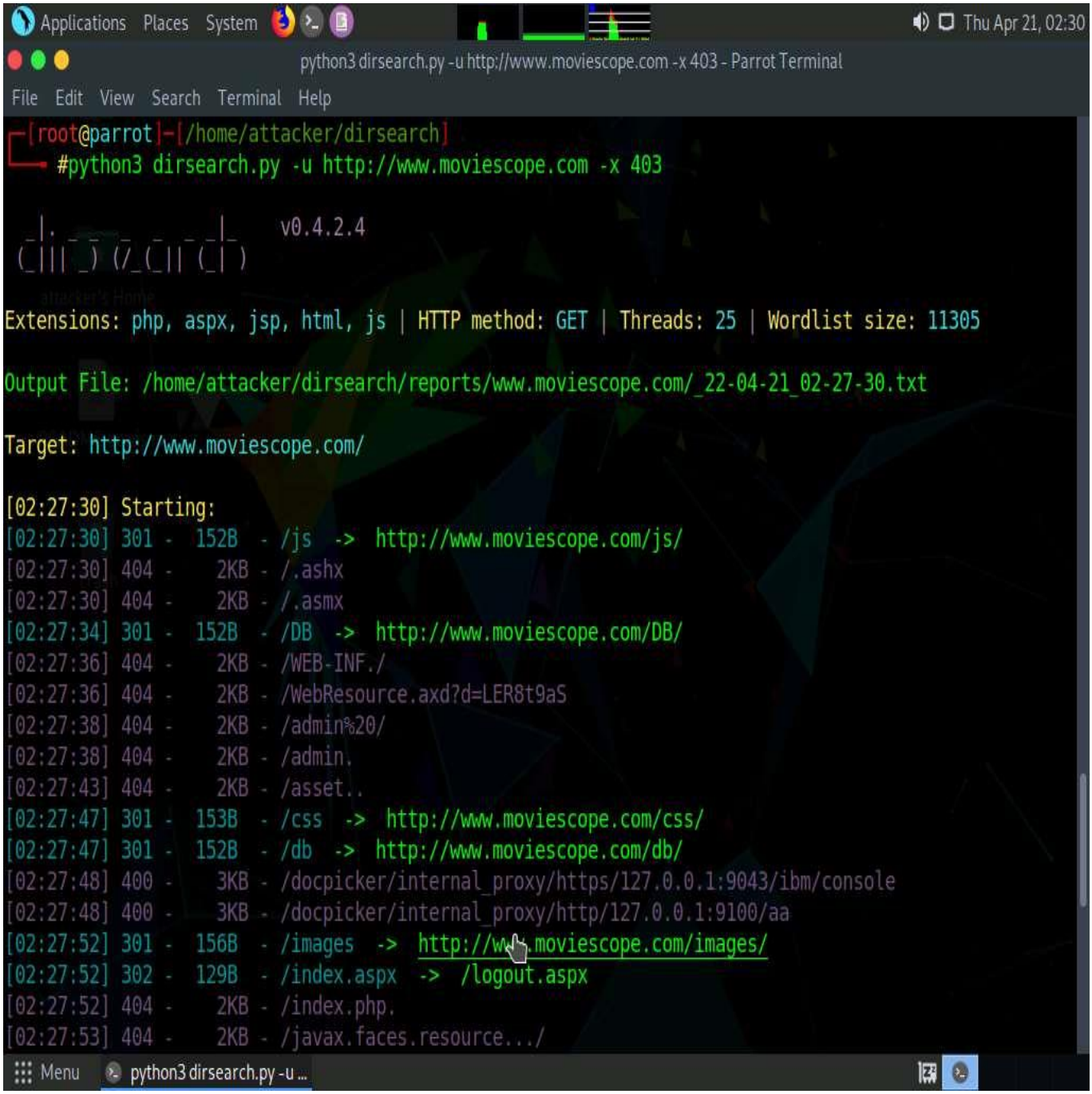



24. Now, we will perform directory bruteforcing by excluding the status code **403**.
25. In the terminal, type **python3 dirsearch.py -u http://www.moviescope.com -x 403** and press **Enter**.

**-x**: specifies exclude status code.




26. **dirsearch** lists the directories from the target website excluding **403** status code.




27. ☐ This concludes the demonstration of identifying web server directories using Nmap and Gobuster.
28. ☐ Close all open windows and document all acquired information.

---

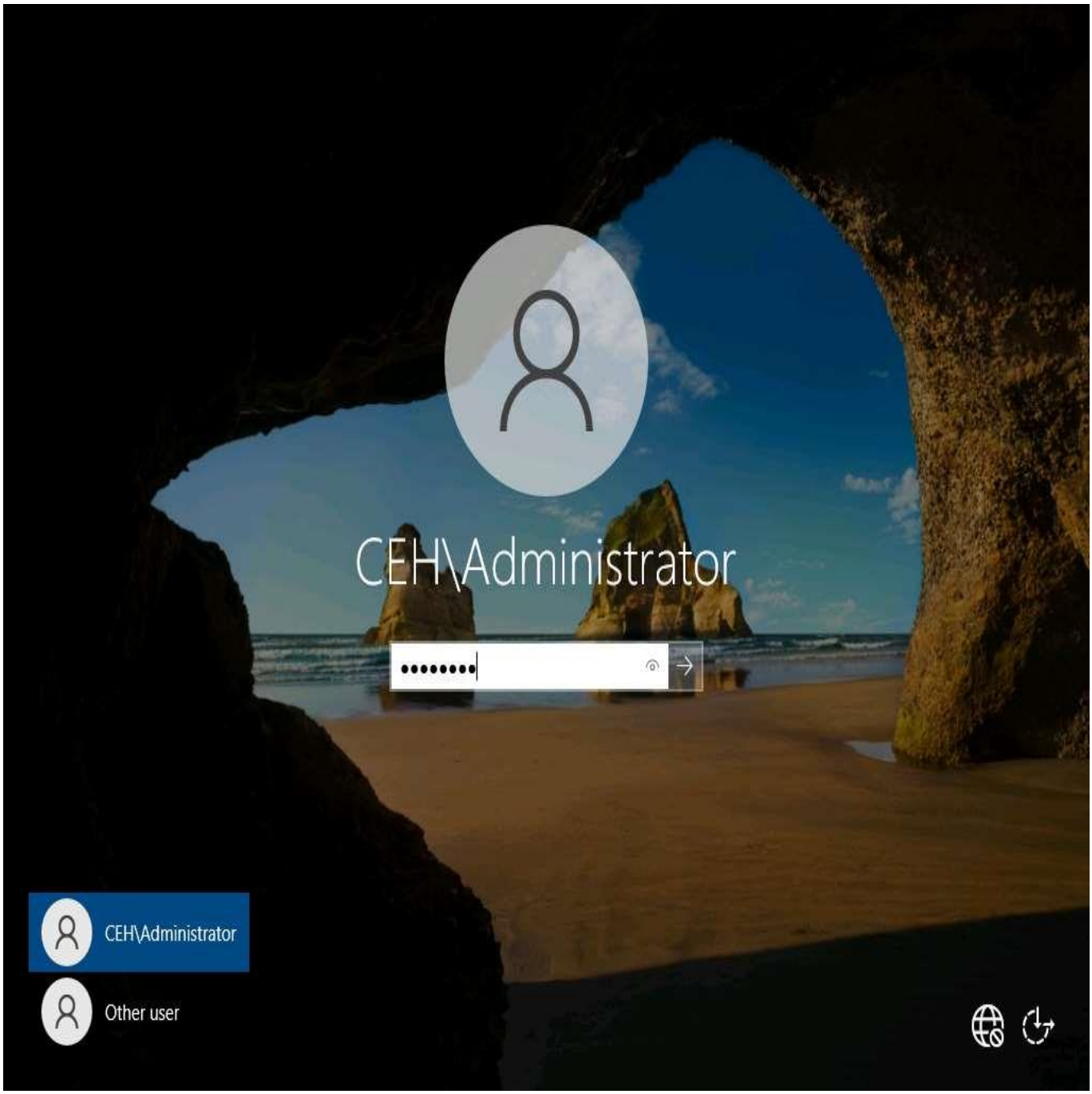
## Task 6: Perform Web Application Vulnerability Scanning using Vega

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.

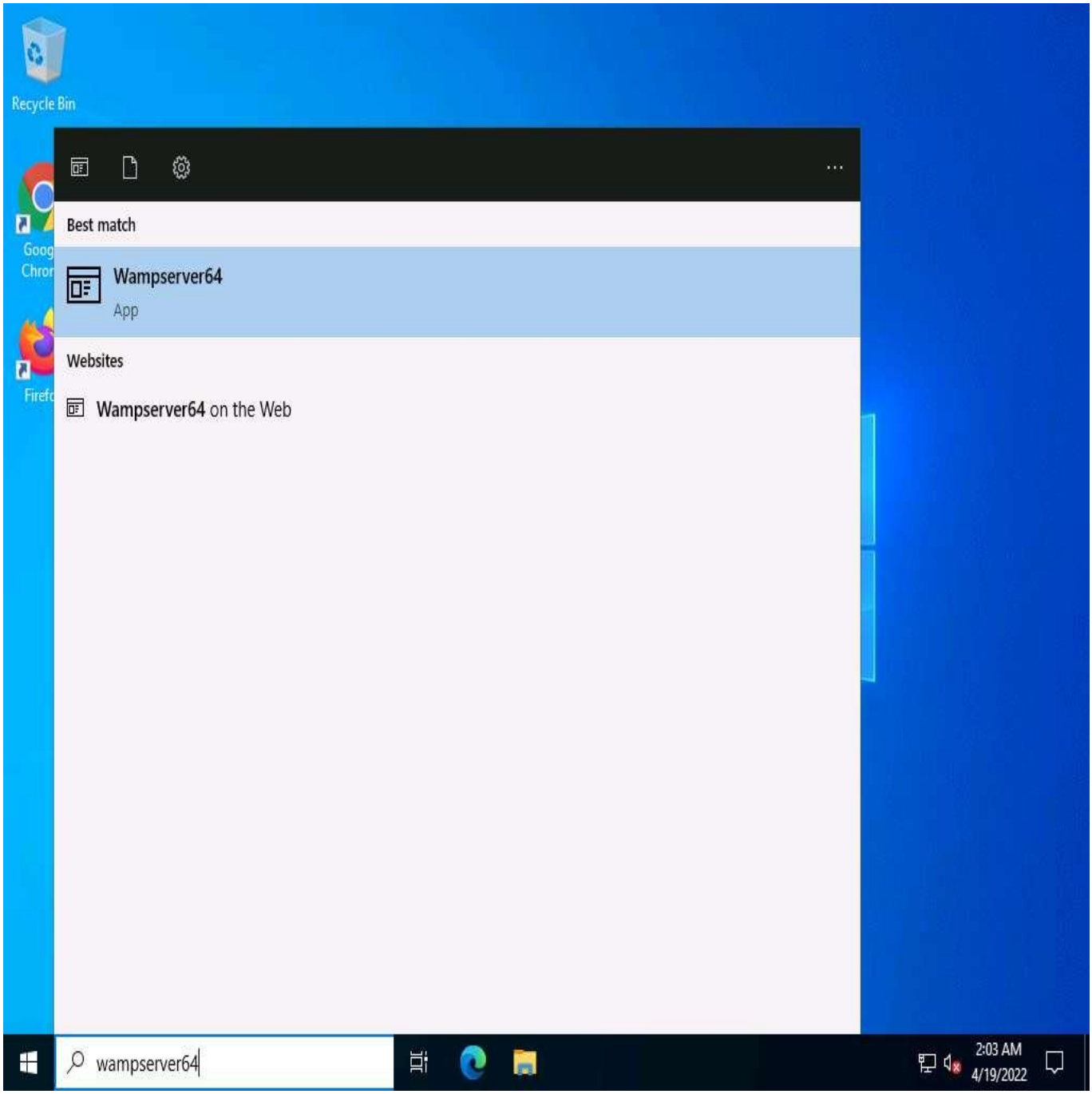
Here, we will discover vulnerabilities in the target web application using Vega.

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.

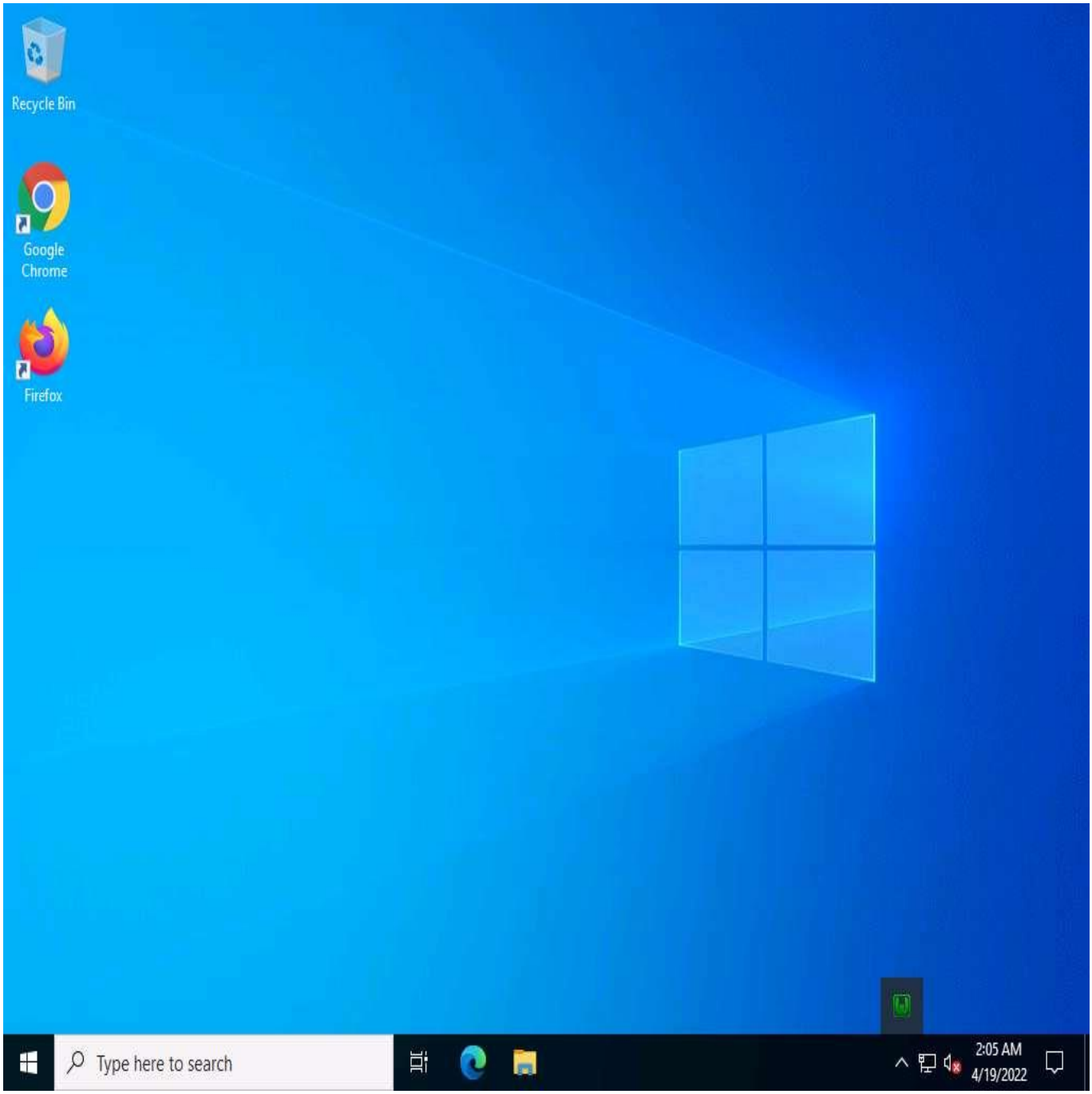
1. Click Windows Server 2022 to switch to the **Windows Server 2022** machine Click Ctrl+Alt+Delete to activate the machine, by default, **CEH\Administrator** account is selected, type **Pa$$w0rd** in the Password field and press **Enter**.




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.

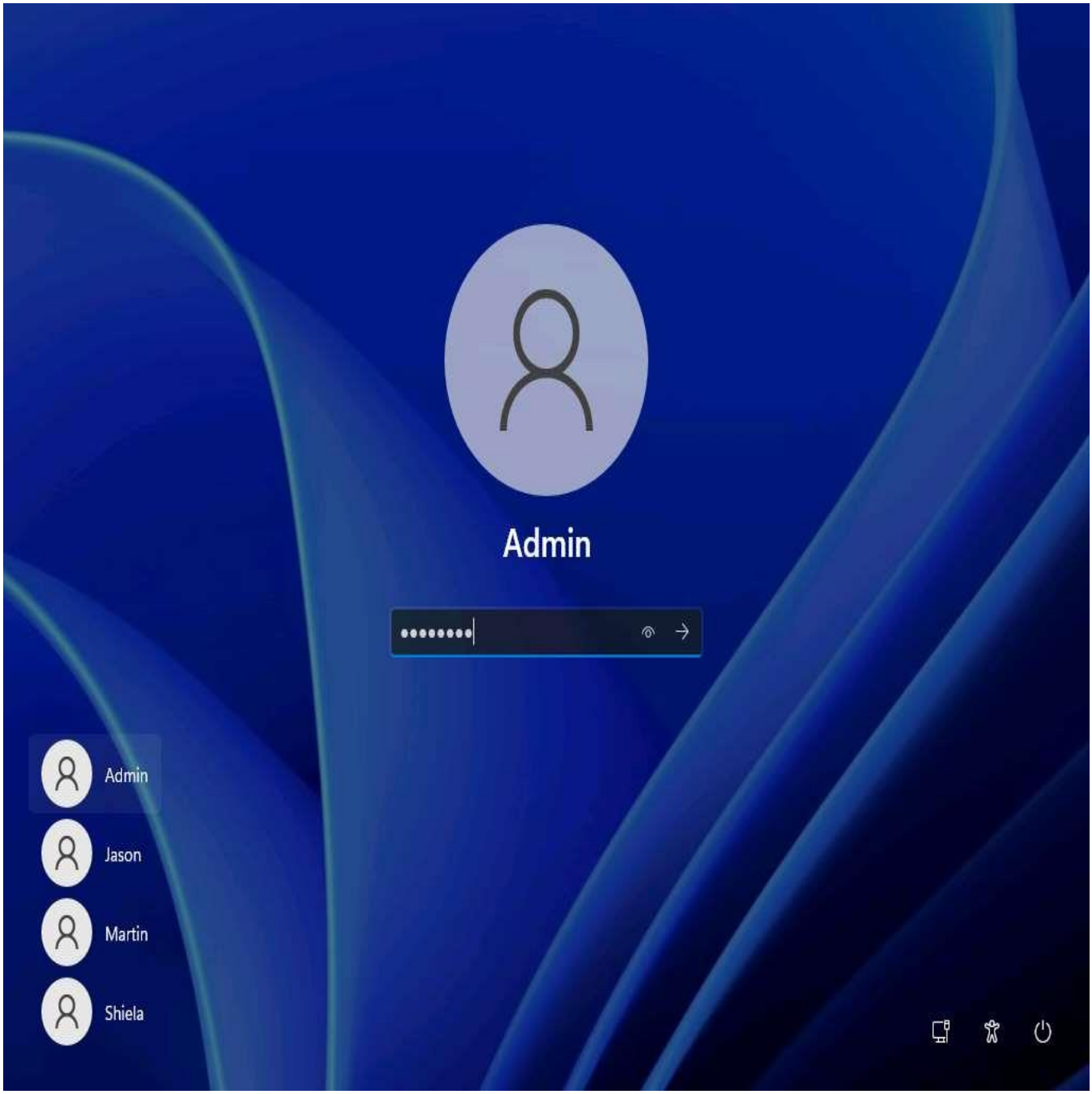



5. Click Windows 11 to switch to the **Windows 11** machine, click Ctrl+Alt+Delete to activate the machine.

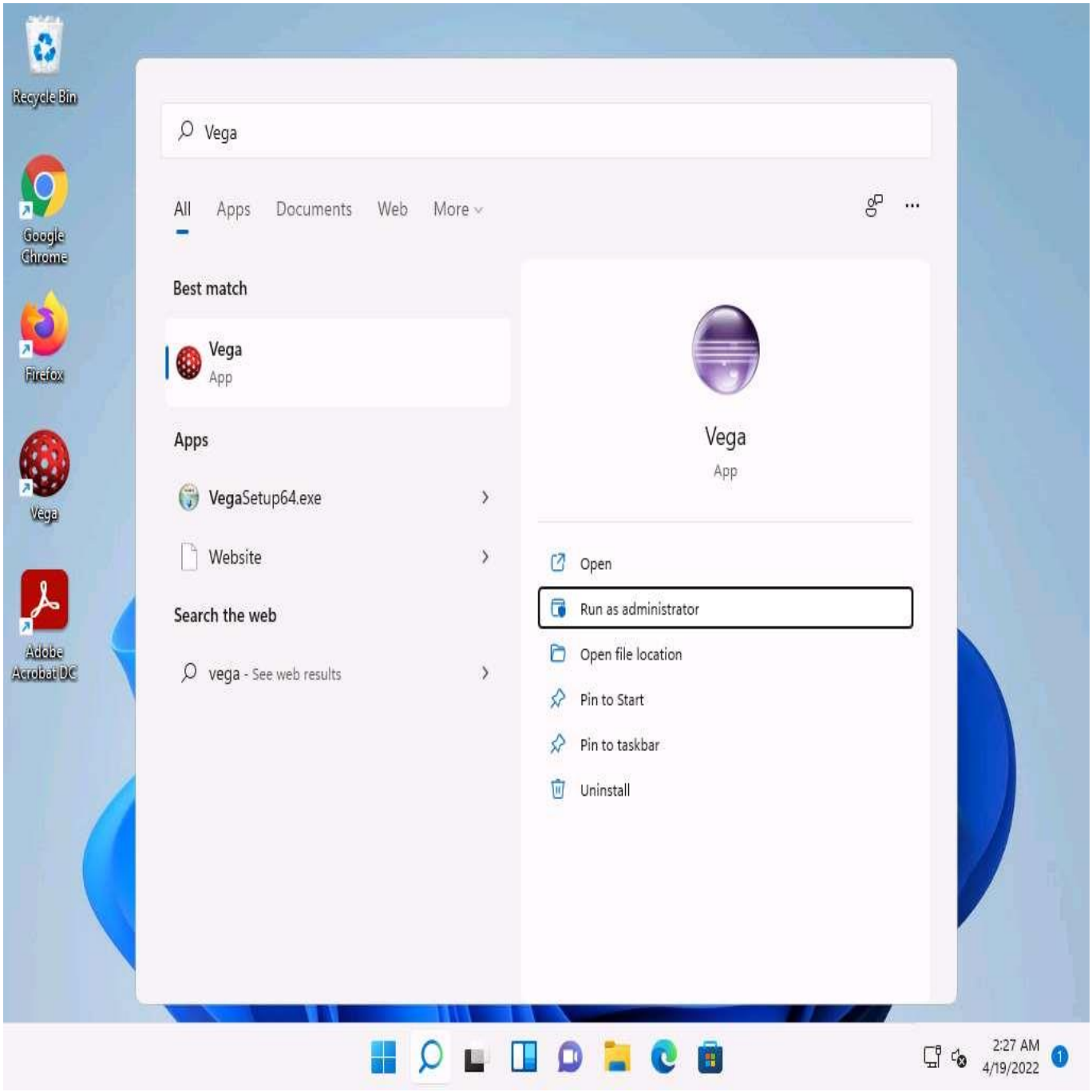
Alternatively, you can also click **Ctrl+Alt+Delete** button under **Windows 11** machine thumbnail in the **Resources** pane or Click **Ctrl+Alt+Delete** button under Commands (**thunder** icon) menu.

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

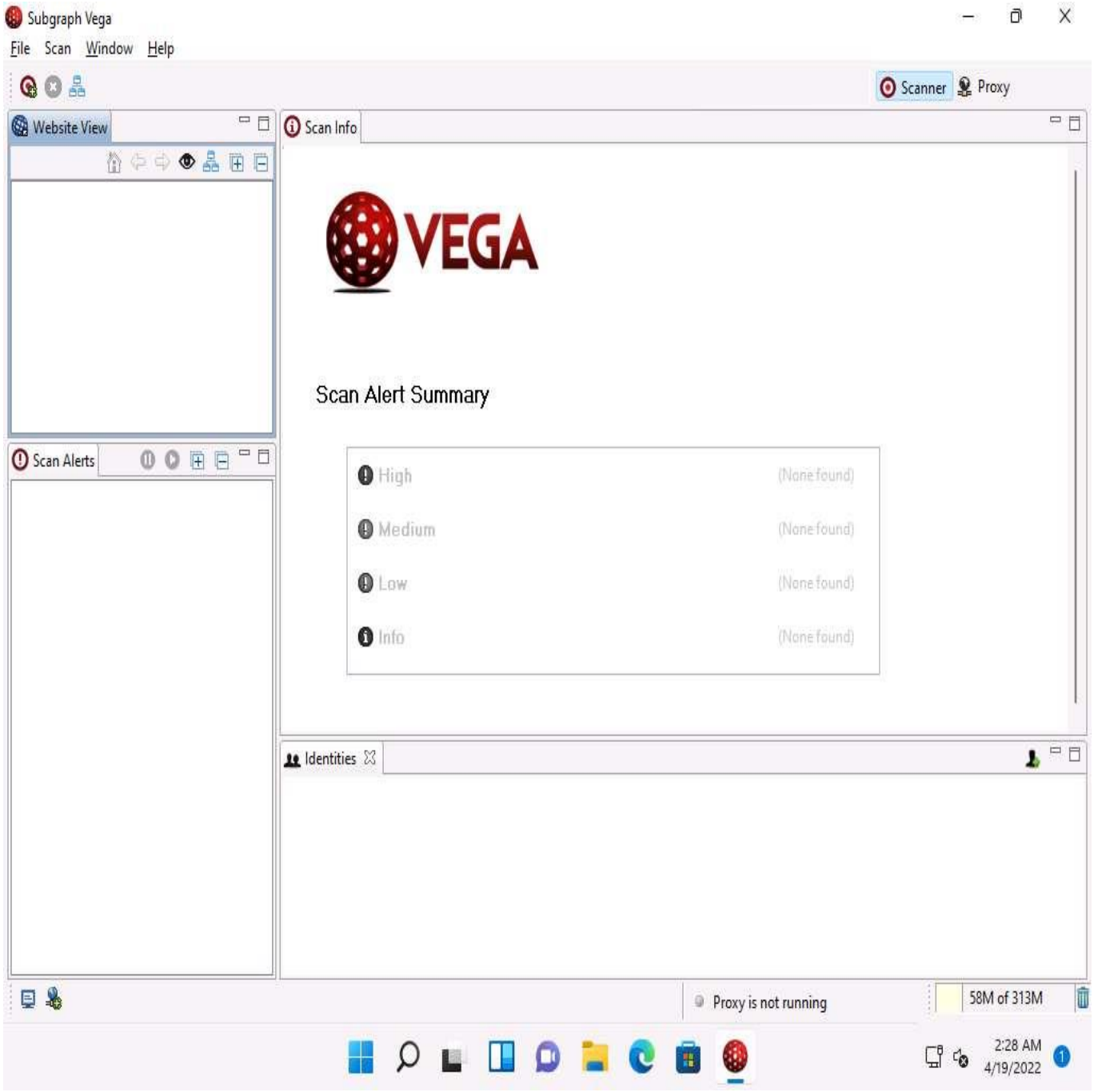
Alternatively, you can also click **Pa$$w0rd** under **Windows 11** machine thumbnail in the **Resources** pane or Click **Type Text | Type Password** button under Commands (**thunder** icon) menu.
Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on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



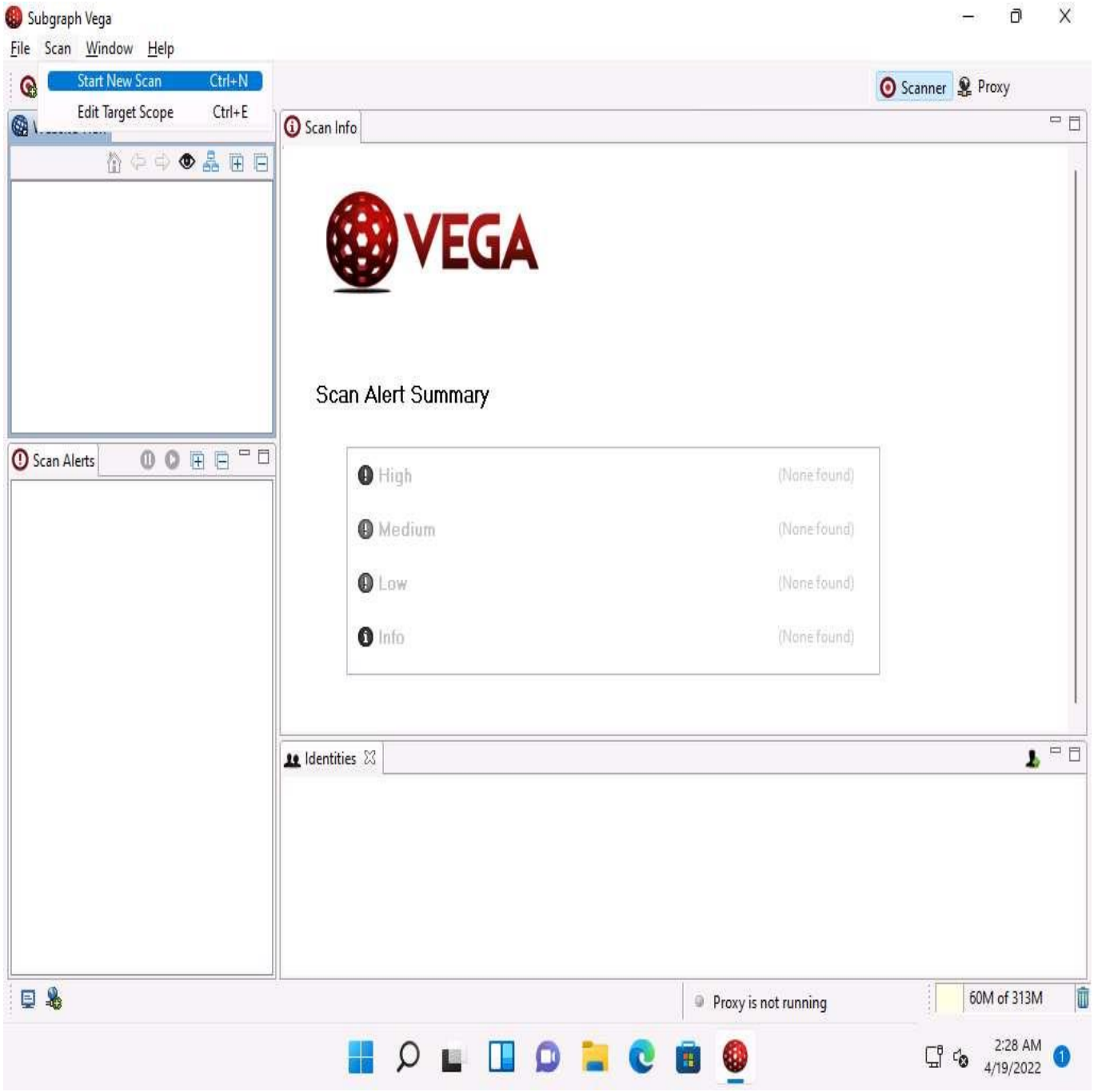

7. ☐ Click **Search** icon ( ) on the **Desktop**. Type **vega** in the search field, the **Vega** appears in the results, click **Run as administrator** to launch it.




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

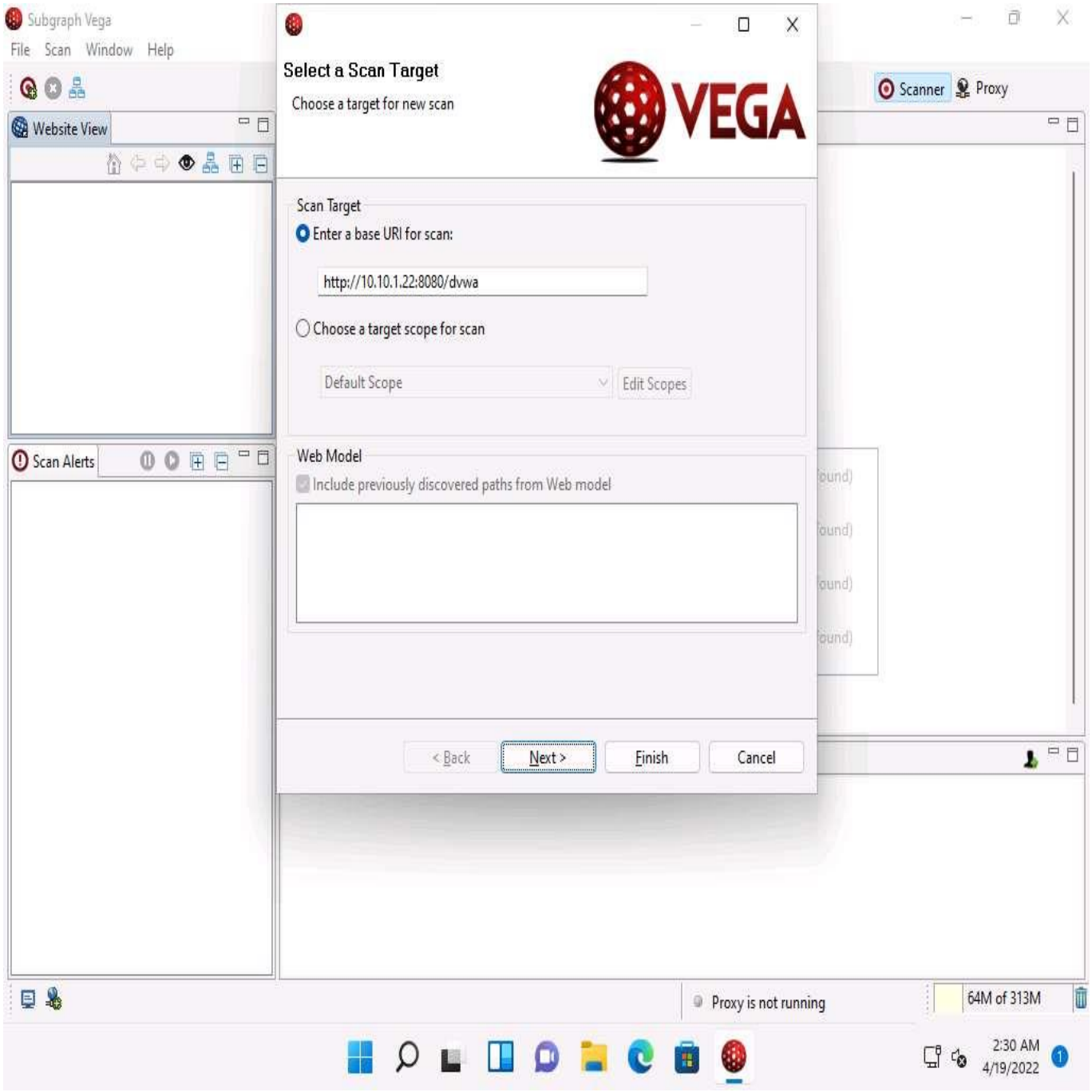



9. Click **Scan** from the menu bar and select **Start New Scan** from the available options.

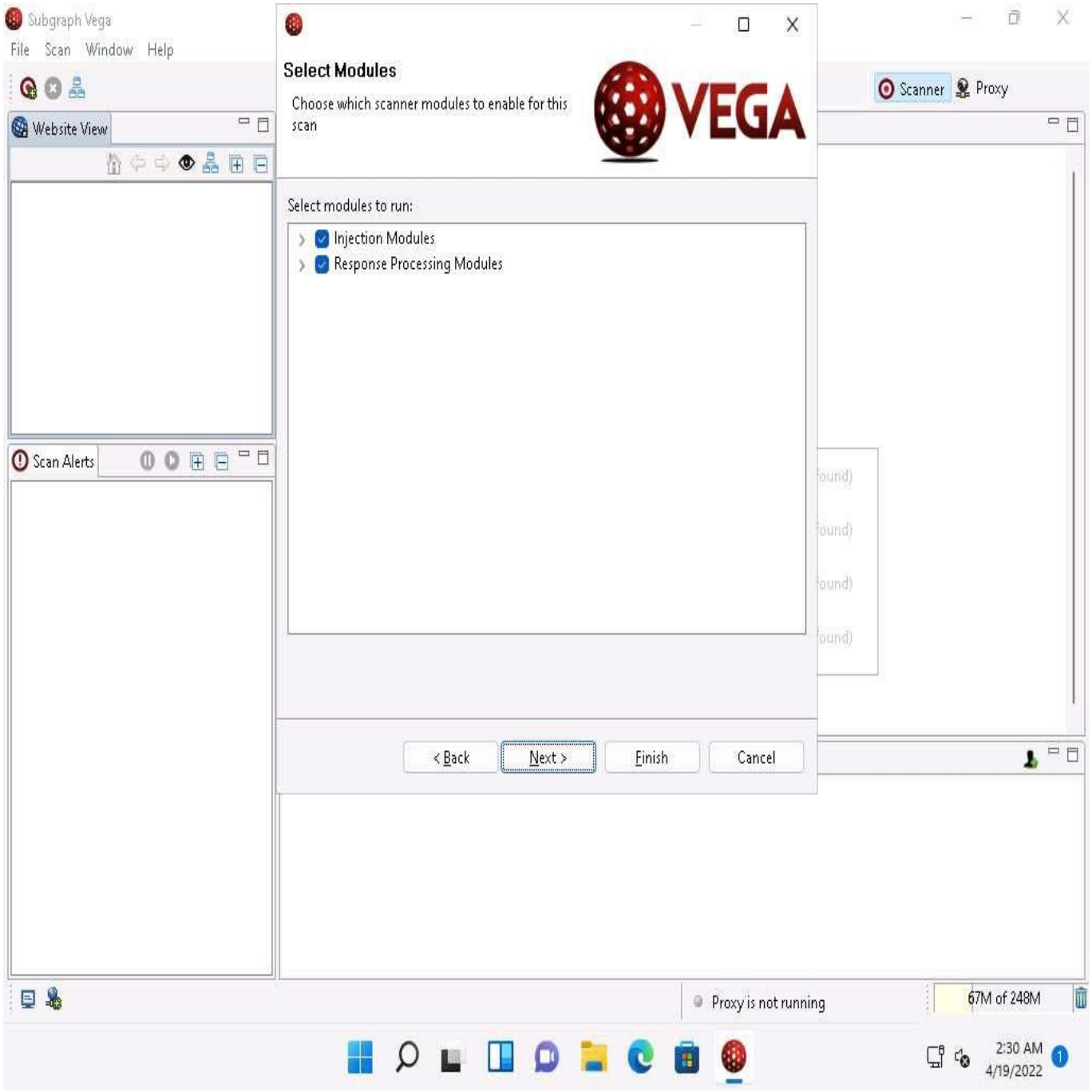



10. ☐ The **Select a Scan Target** window appears on the screen. Ensure that the **Enter a base URI for scan** radio button is selected under the **Scan Target** section.
11. ☐ In the **Enter a base URI for scan** field, enter the target URL as **http://10.10.1.22:8080/dvwa** and click **Next**.

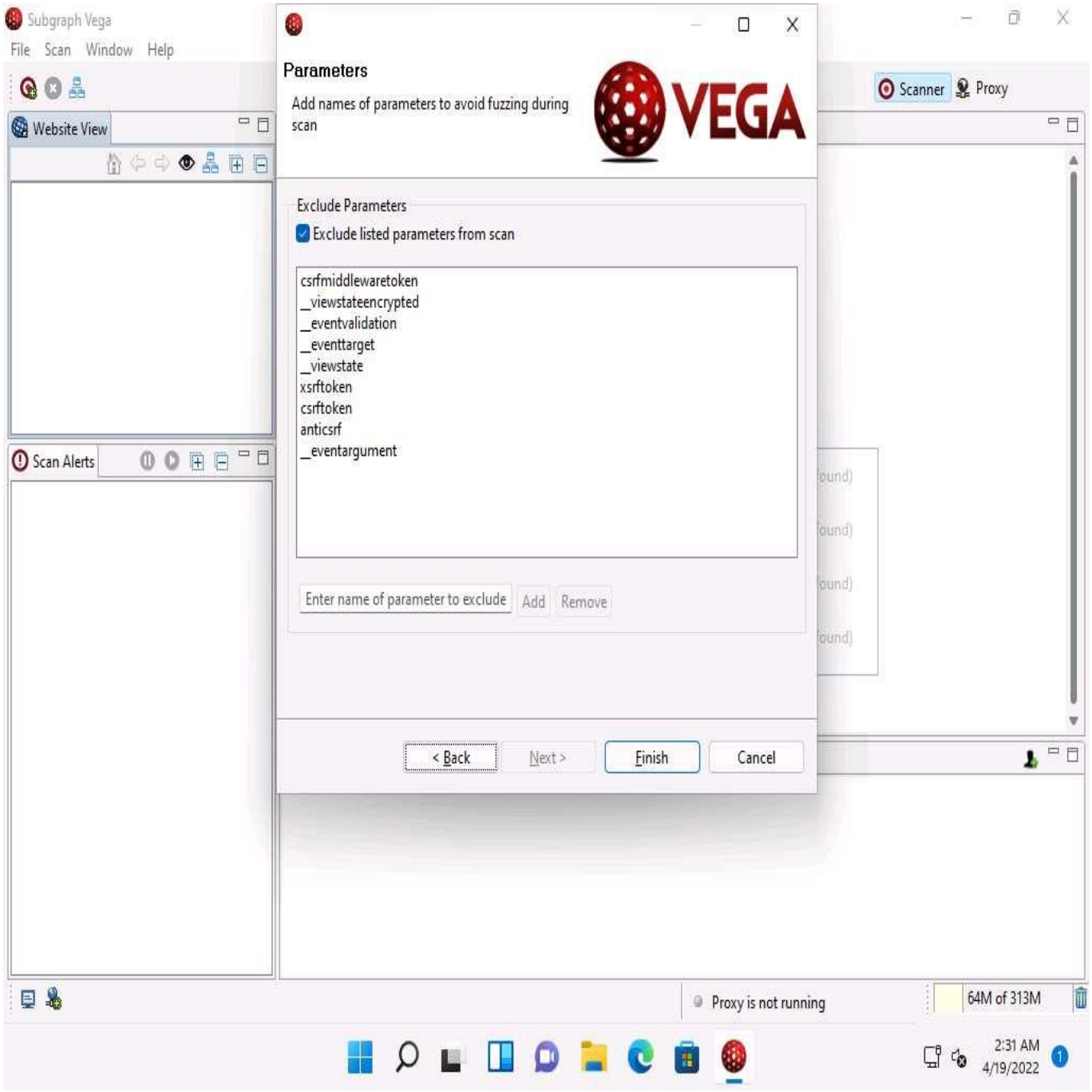
**10.10.1.22** is the IP address of **Windows Server 2022**, where the **DVWA** site is hosted on port **8080**.



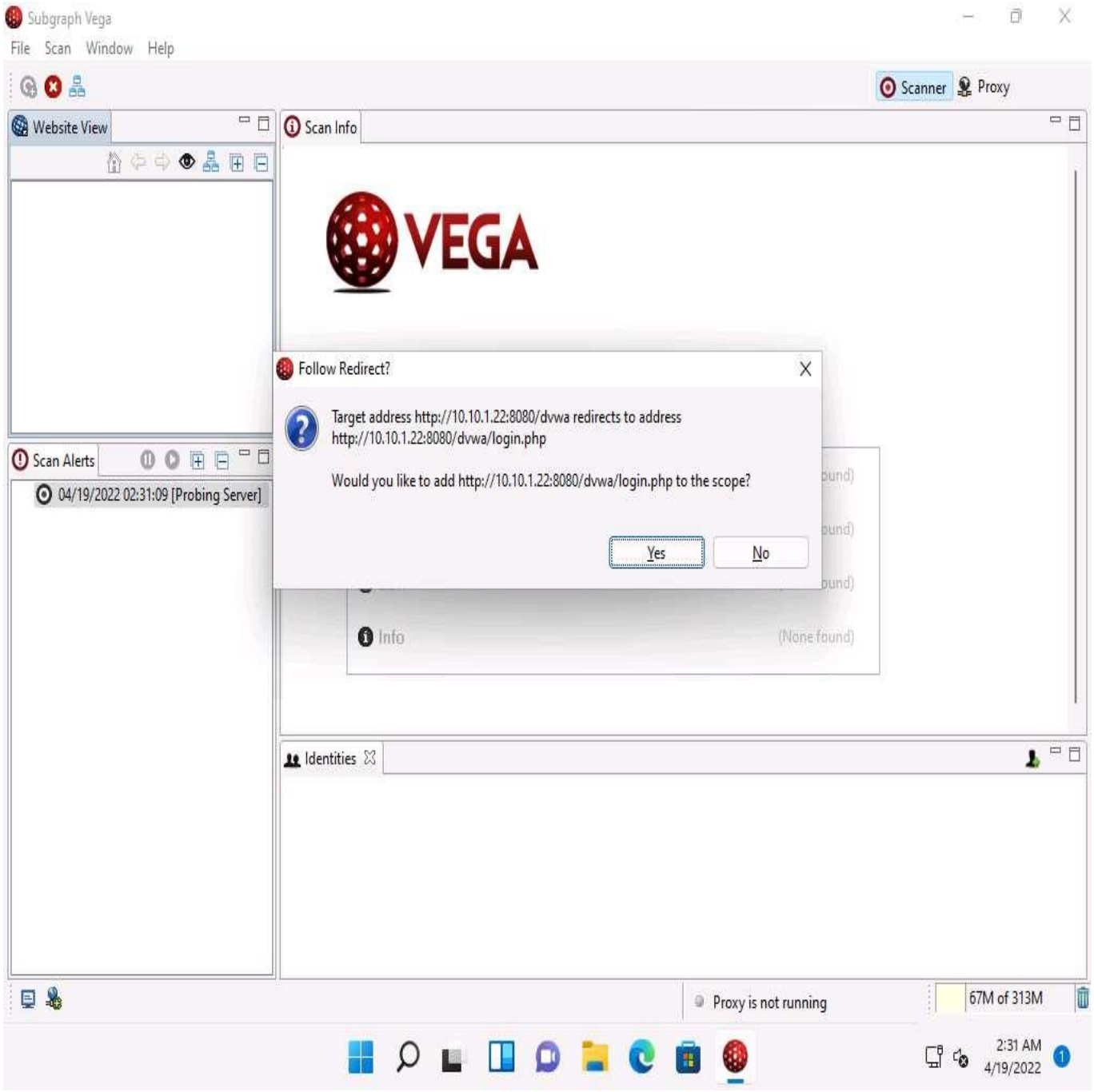

12. ☐ The **Select Modules** wizard appears; double-click on both of the checkboxes (**Injection Modules** and **Response Processing Modules**) to select all options.
13. ☐ By checking these options, all modules under these options will be selected. Click **Next**.




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.

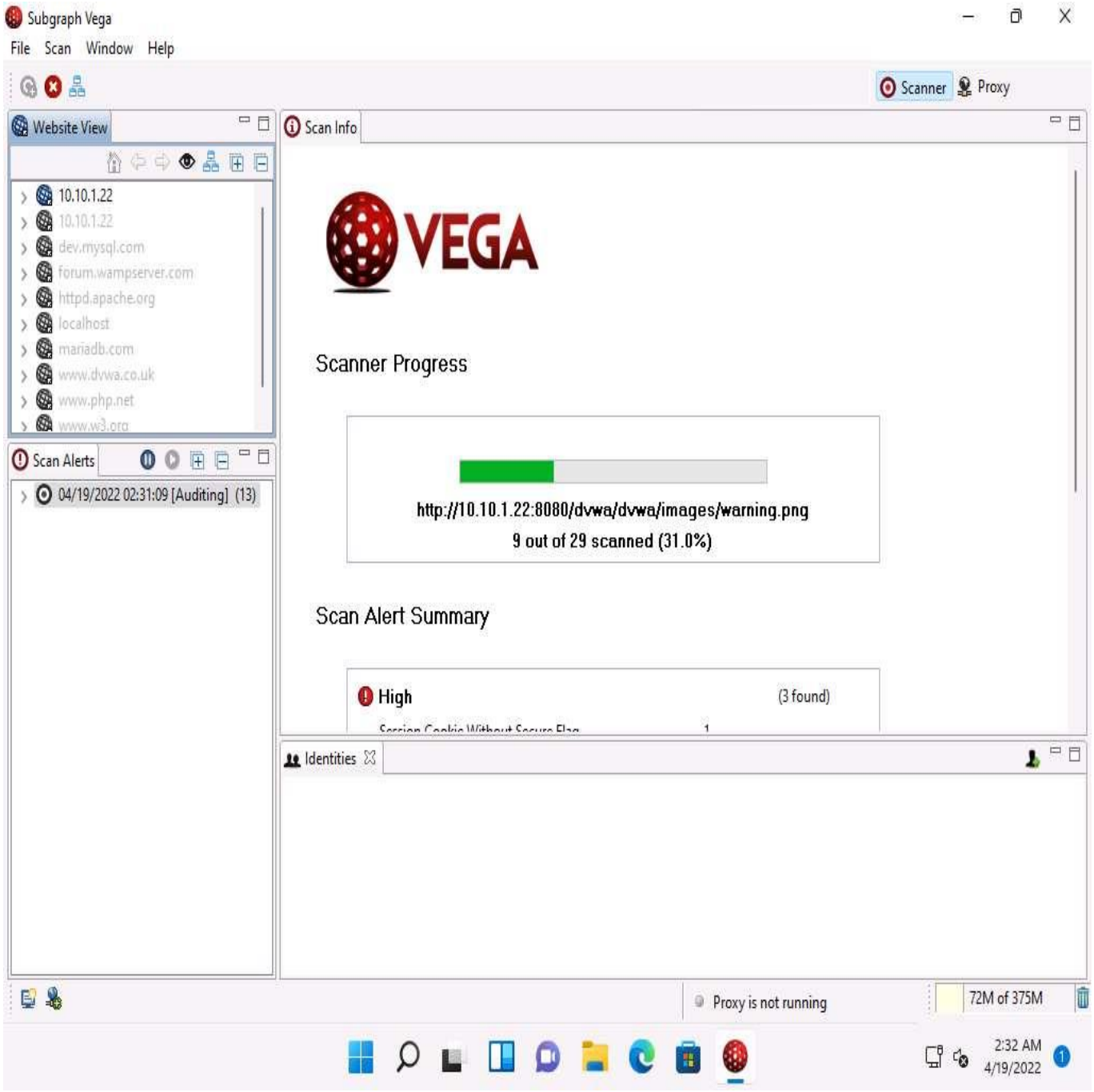



16. ☐ The **Follow Redirect?** pop-up appears; click **Yes** to continue.

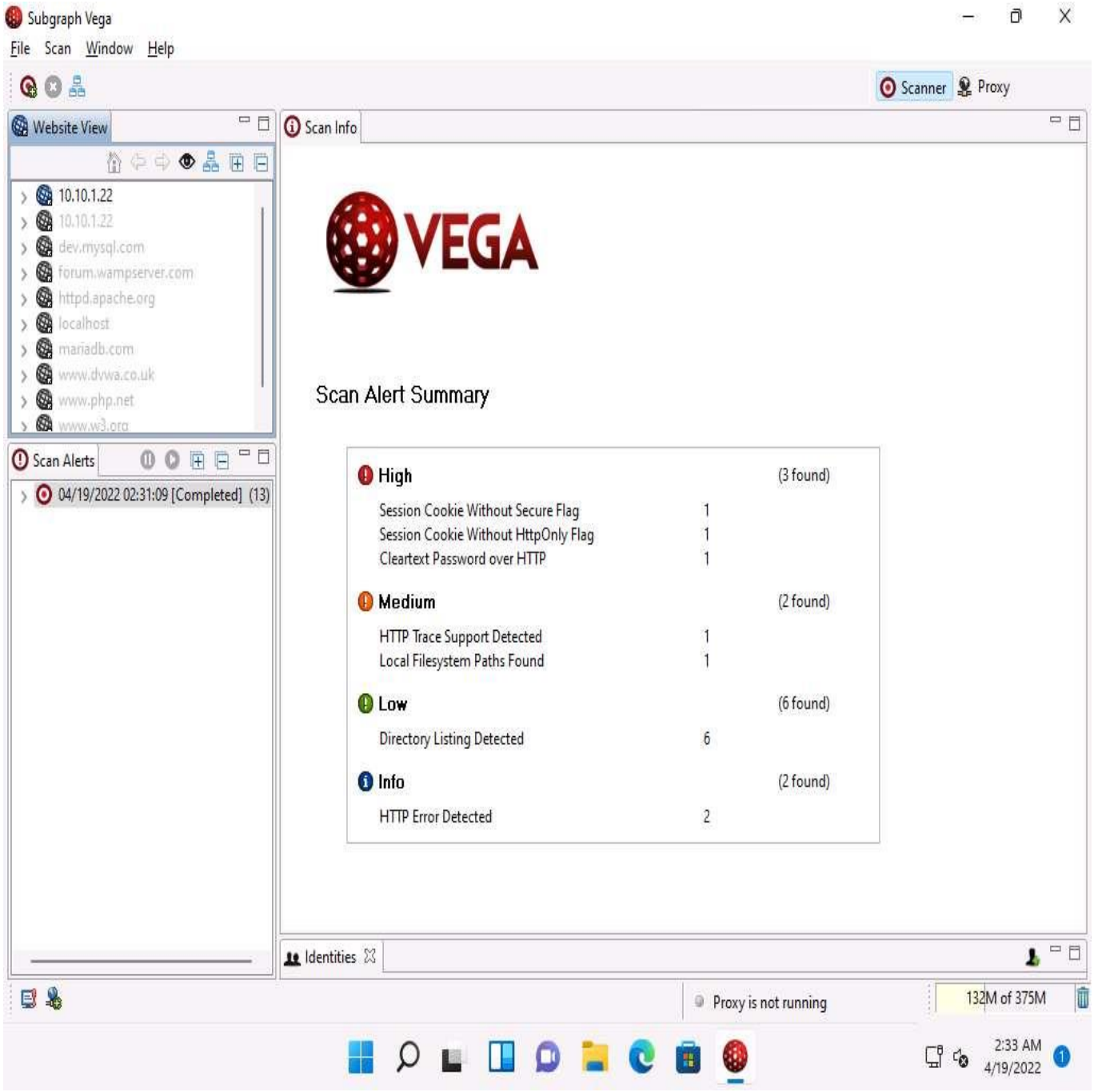



17. ☐ The Vega application starts scanning the target website for vulnerabilities. Observe the **Scanner Progress** bar and wait for it to finish.

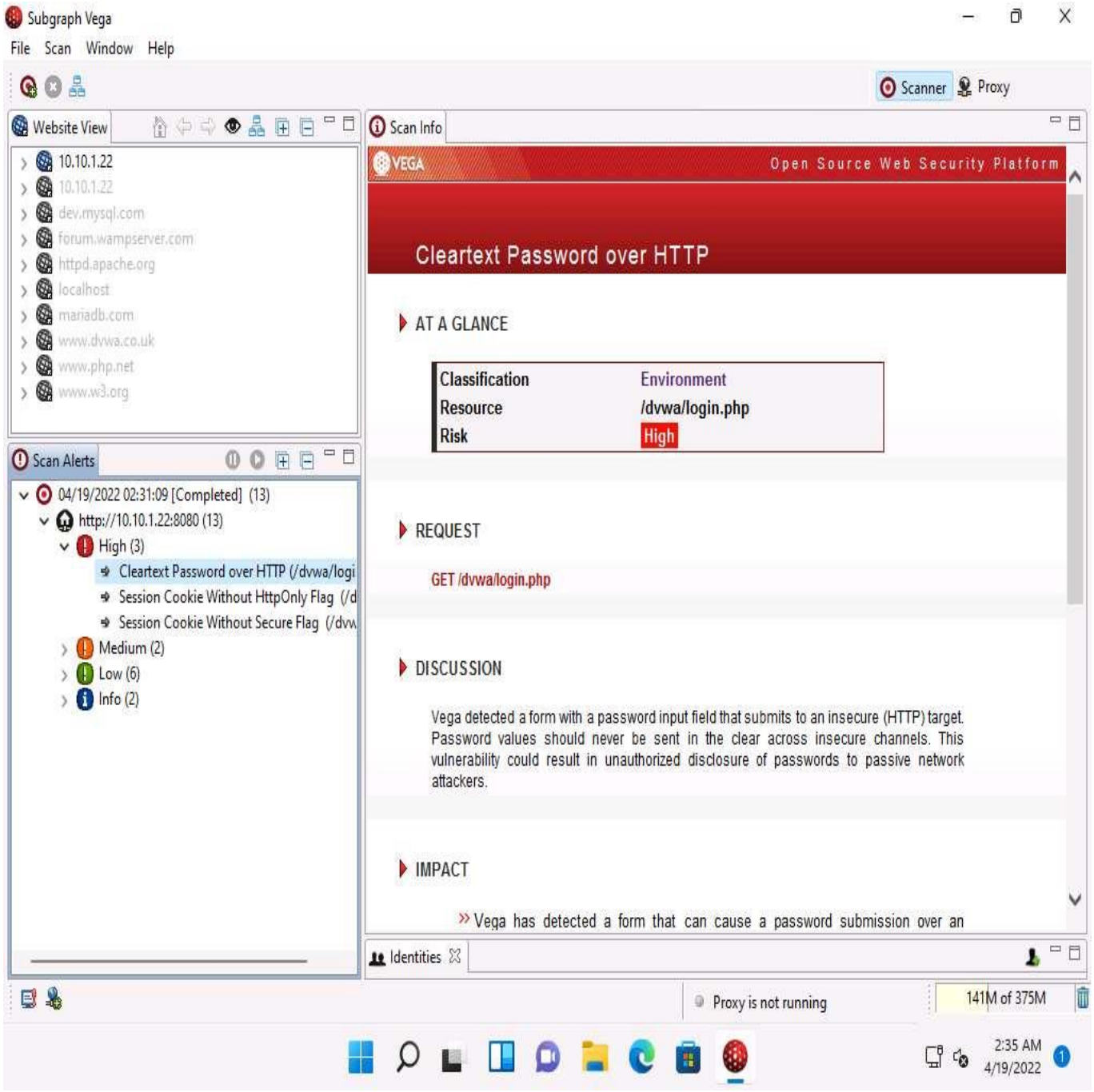
In the left-hand pane, under the **Scan Alerts** section, you can see the scan status as **Auditing**. As soon as Vega completes, the scan status changes to **Completed**.




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.

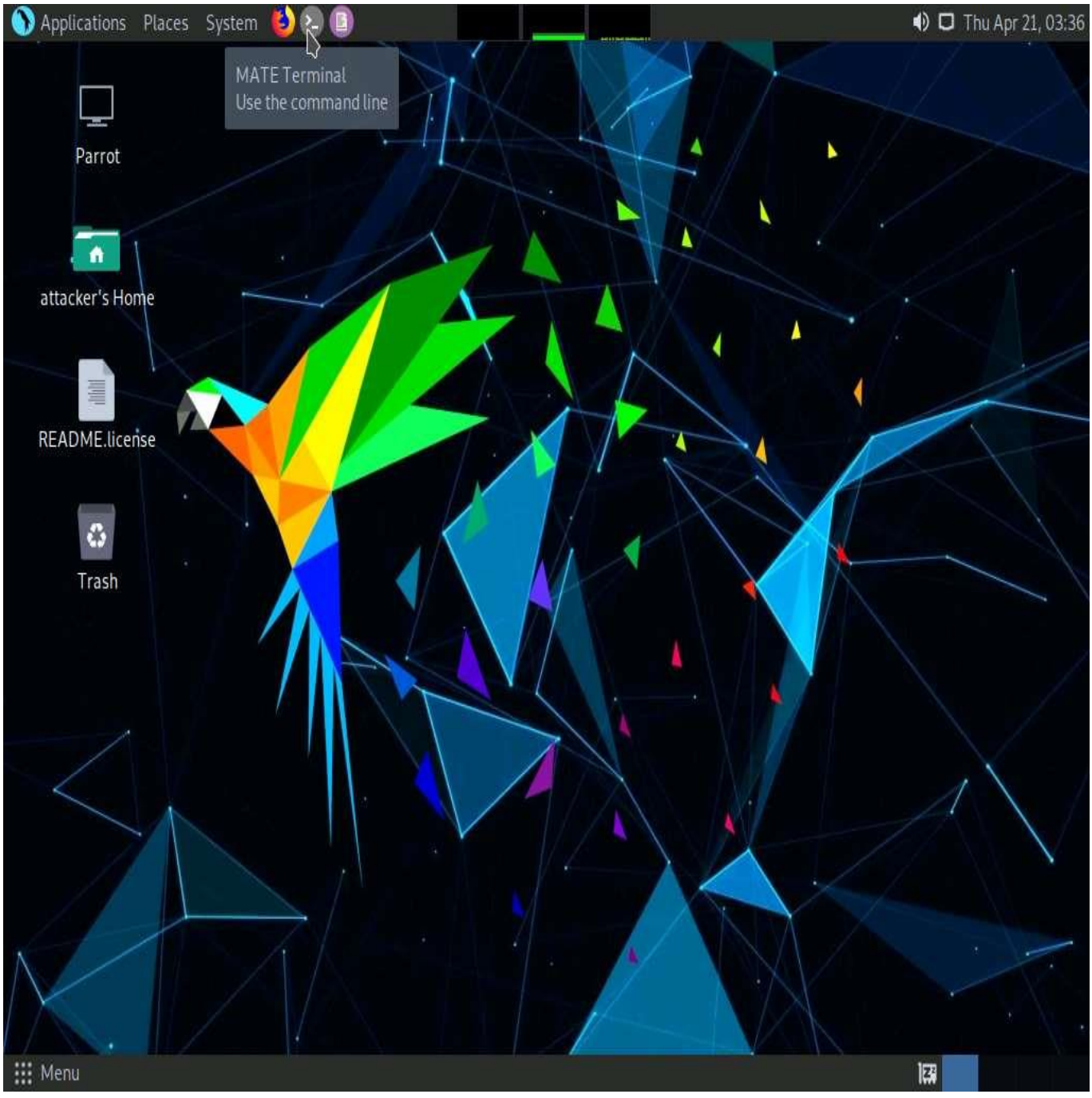
# Task 7: Identify Clickjacking Vulnerability using ClickjackPoc

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.

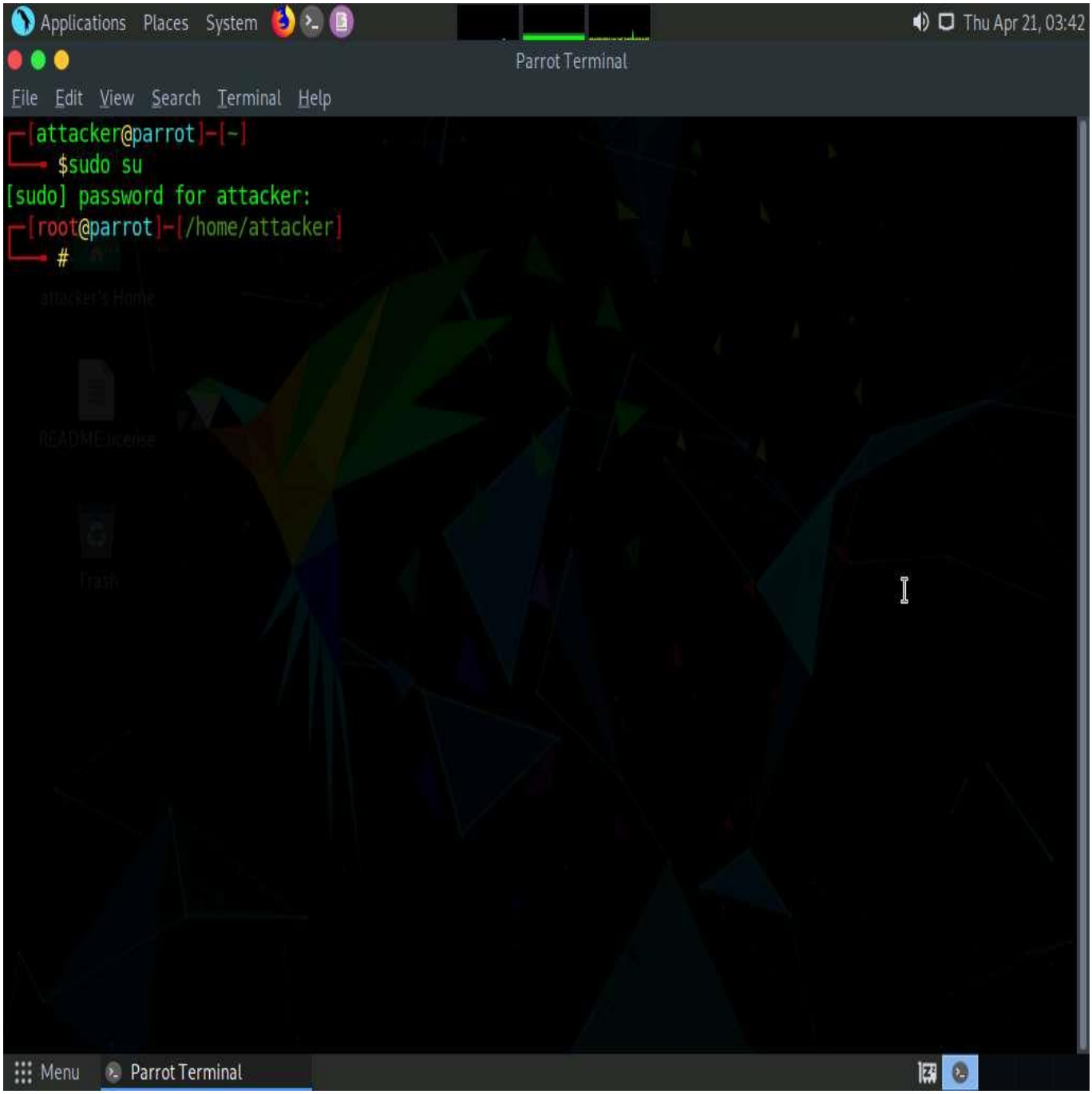
In this task, we will identify a clickjacking vulnerability in the target website (**www.moviescope.com**) hosted by the **Windows Server 2019** machine, and we will use the **Parrot Security** machine as the host machine.

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

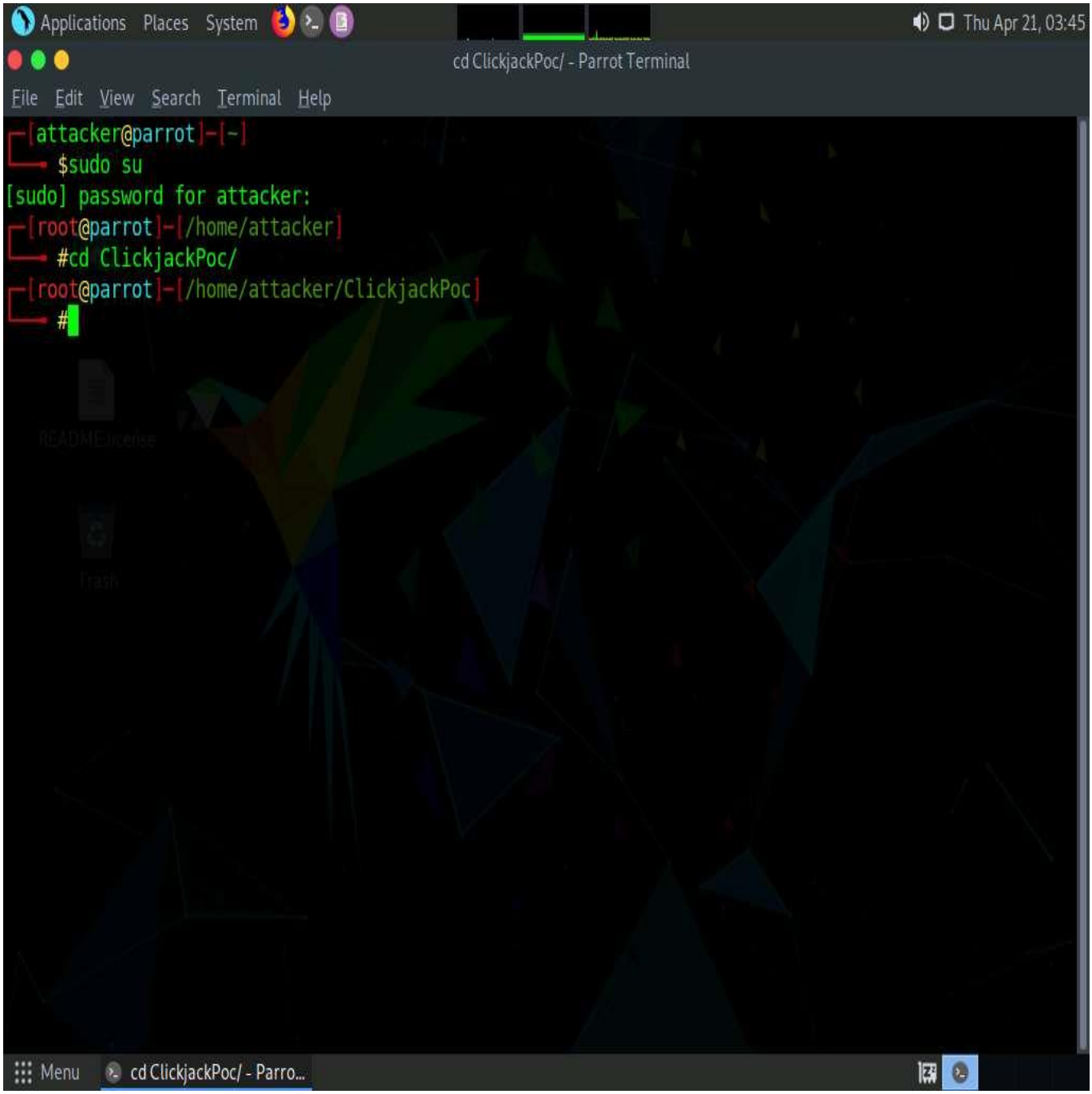


2. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

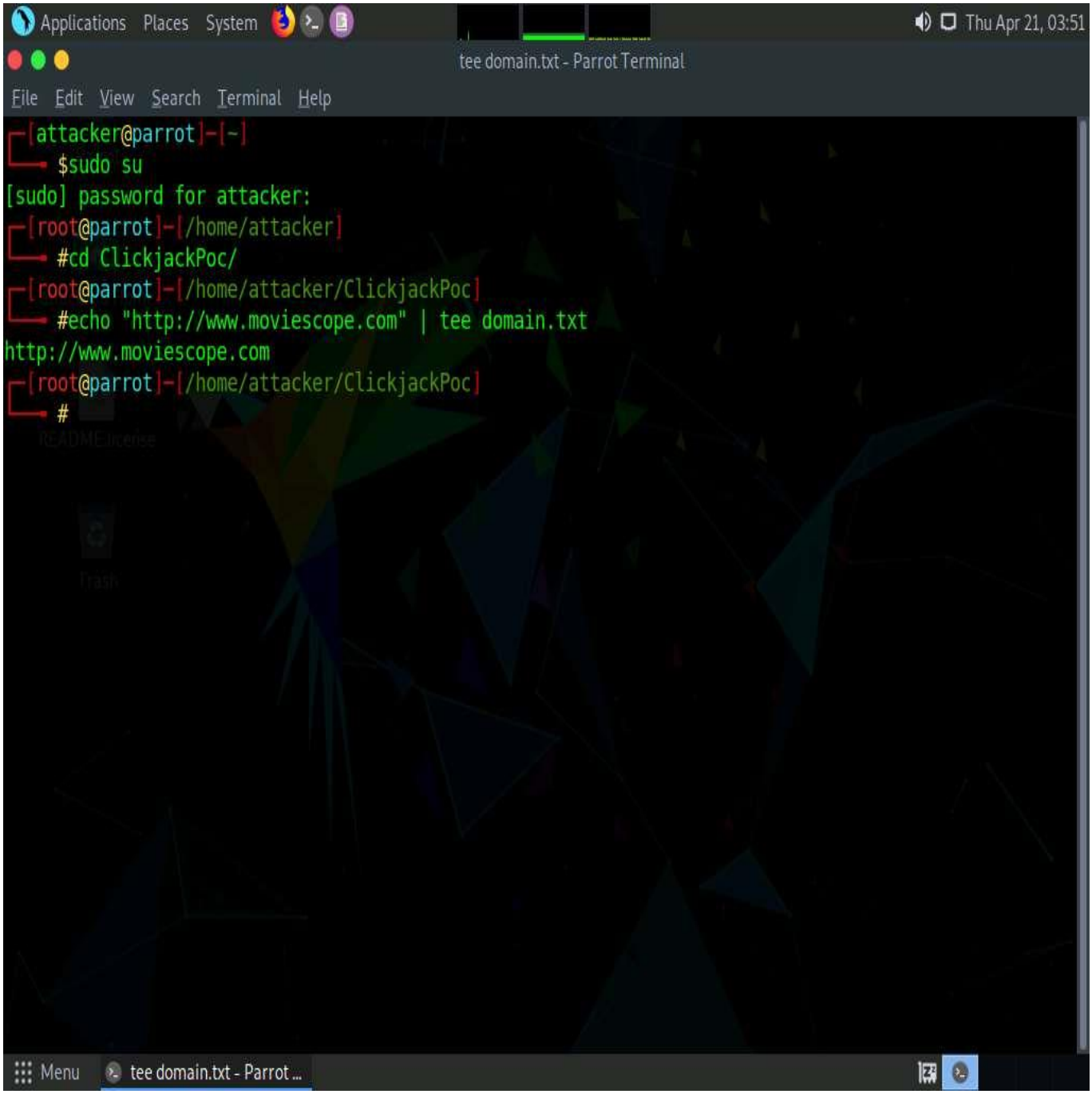
The password that you type will not be visible.




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



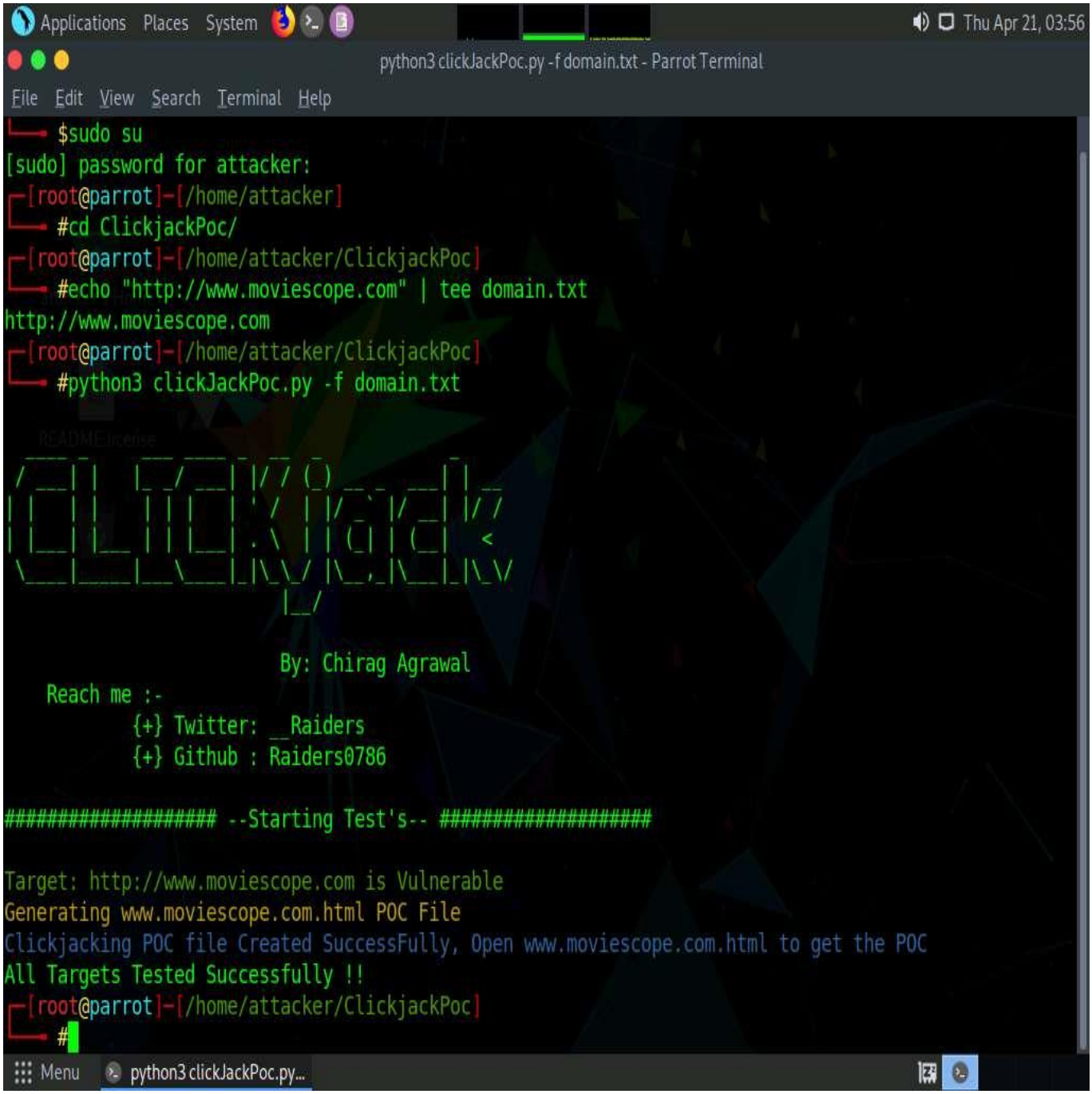

5. ☐ In the terminal window, type **echo "http://www.moviescope.com" | tee domain.txt** and press **Enter**.
6. ☐ This will create a file named **domain.txt** containing the website link.



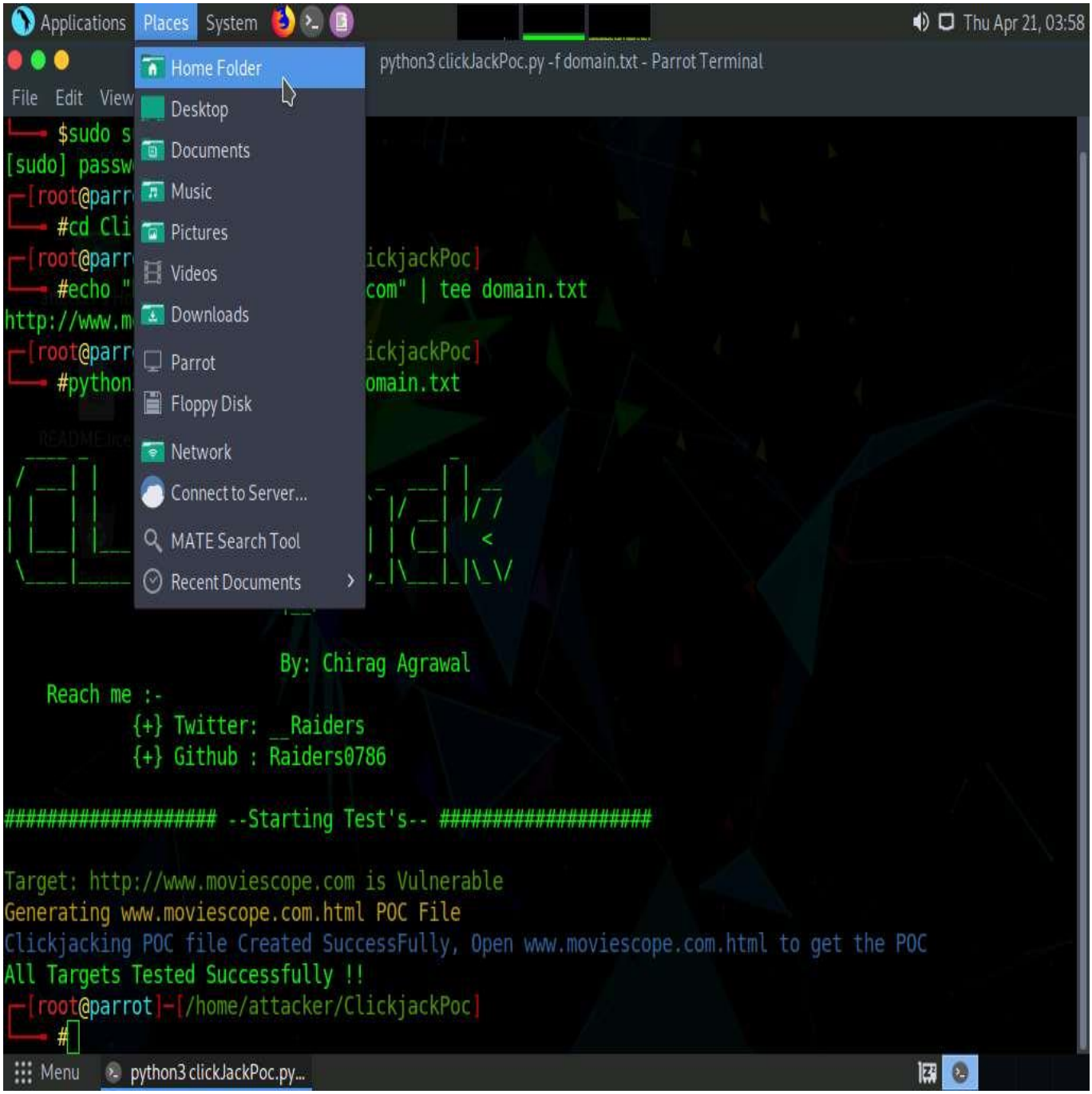

7. Type **python3 clickJackPoc.py -f domain.txt** press **Enter** to start the scan.

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

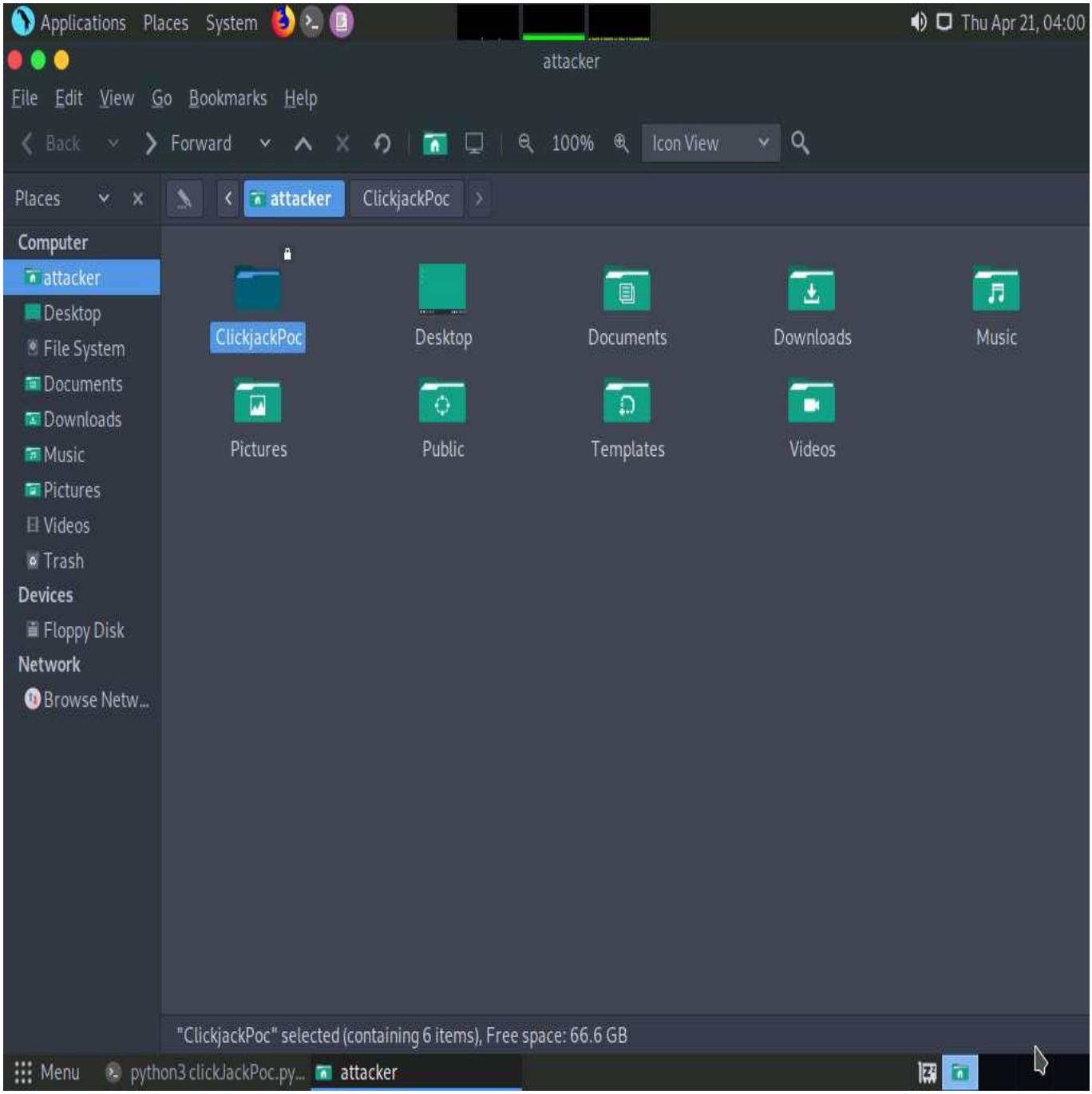
8. The result appears, displaying that the target website is vulnerable to clickjacking as shown in screenshot.



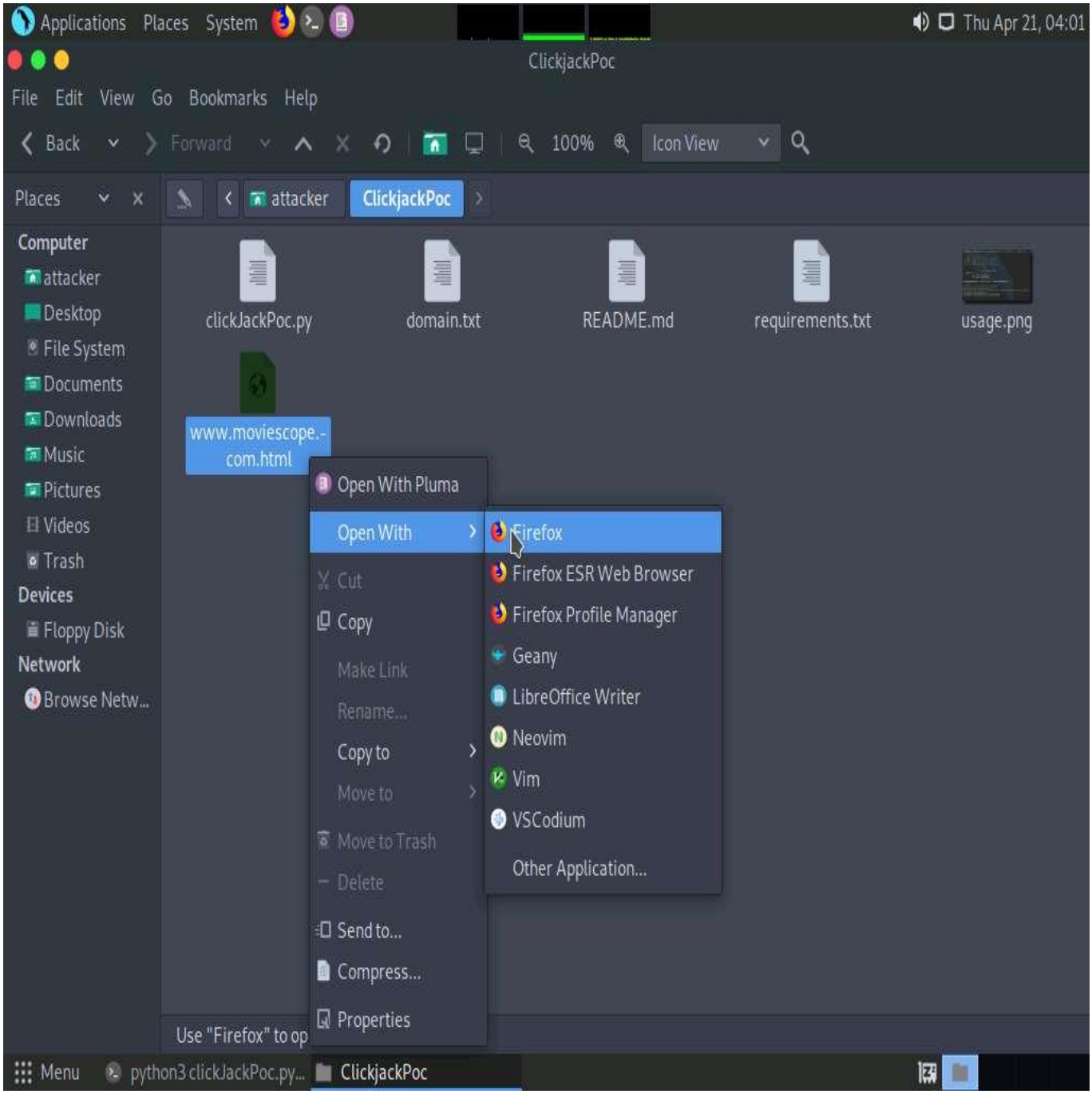

9. Now, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



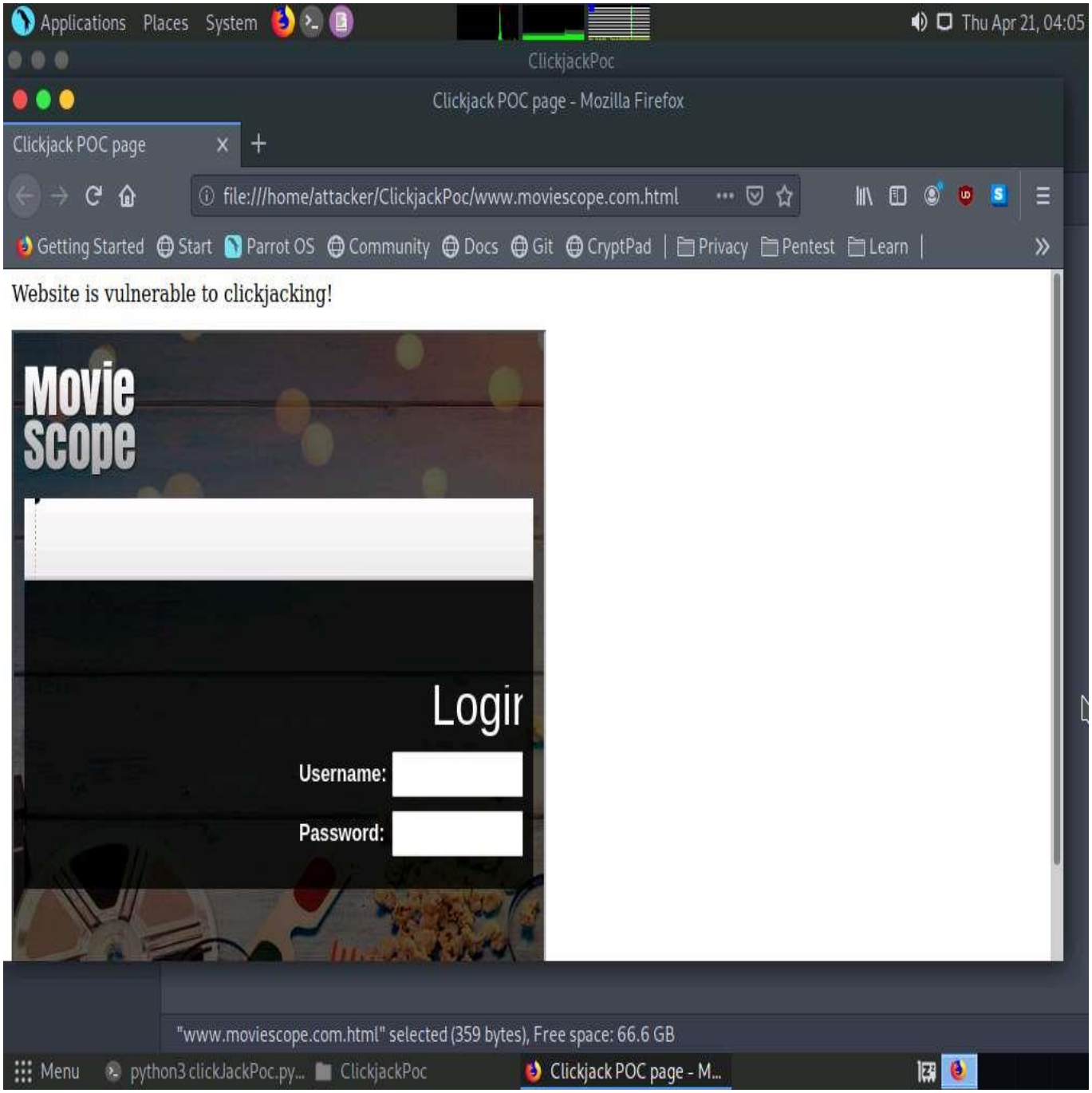

10. ☐ An **attacker** window appears, double click on **ClickjackPoc** directory.




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




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




13. ☐ This concludes the demonstration of identifying clickjacking vulnerability in the target website using ClickjackPoc.
14. ☐ Close all open windows and document all acquired information.