Module 13: Hacking Web Servers

Scenario

Most organizations consider their web presence to be an extension of themselves. Organizations create their web presence on the World Wide Web using websites associated with their business. Most online services are implemented as web applications. Online banking, search engines, email applications, and social networks are just a few examples of such web services. Web content is generated in real-time by a software application running on the server-side. Web servers are a critical component of web infrastructure. A single vulnerability in a web server’s configuration may lead to a security breach on websites. This makes web server security critical to the normal functioning of an organization.

Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS, DDoS, DNS server hijacking, DNS amplification, directory traversal, Man-in-the-Middle (MITM), sniffing, phishing, website defacement, web server misconfiguration, HTTP response splitting, web cache poisoning, SSH brute force, web server password cracking, and other methods. Attackers can exploit a poorly configured web server with known vulnerabilities to compromise the security of the web application. A leaky server can harm an organization.

In the area of web security, despite strong encryption on the browser-server channel, web users still have no assurance about what happens at the other end. This module presents a security application that augments web servers with trusted co-servers composed of high-assurance secure co-processors, conﬁgured with a publicly known guardian program. Web users can then establish their authenticated, encrypted channels with a trusted co-server, which can act as a trusted third party in the browser-server interaction. Systems are constantly being attacked, so IT security professionals need to be aware of the common attacks on web server applications.

A penetration (pen) tester or ethical hacker for an organization must provide security to the company’s web server. This includes performing checks on the web server for vulnerabilities, misconfigurations, unpatched security flaws, and improper authentication with external systems.

Objective

The objective of this lab is to perform web server hacking and other tasks that include, but are not limited to:

* Footprint a web server using various information-gathering tools and inbuilt commands
* Enumerate web server information
* Crack remote passwords

Overview of Web Server

Most people think a web server is just hardware, but a web server also includes software applications. In general, a client initiates the communication process through HTTP requests. When a client wants to access any resource such as web pages, photos, or videos, then the client’s browser generates an HTTP request to the web server. Depending on the request, the web server collects the requested information or content from data storage or the application servers and responds to the client’s request with an appropriate HTTP response. If a web server cannot find the requested information, then it generates an error message.

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack a target web server. Recommended labs that will assist you in learning various web server hacking techniques include:

1. Footprint the web server
   * Information gathering using Ghost Eye
   * Perform web server reconnaissance using Skipfish
   * Footprint a web server using the httprecon Tool
   * Footprint a web server using Netcat and Telnet
   * Enumerate web server information using Nmap Scripting Engine (NSE)
   * Uniscan web server fingerprinting in Parrot Security
2. Perform a web server attack
   * Crack FTP credentials using a Dictionary Attack

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 Netcat and Telnet
* Enumerate web server information using Nmap Scripting Engine (NSE)
* Uniscan web server fingerprinting in Parrot Security

**Overview of Web Server Footprinting**

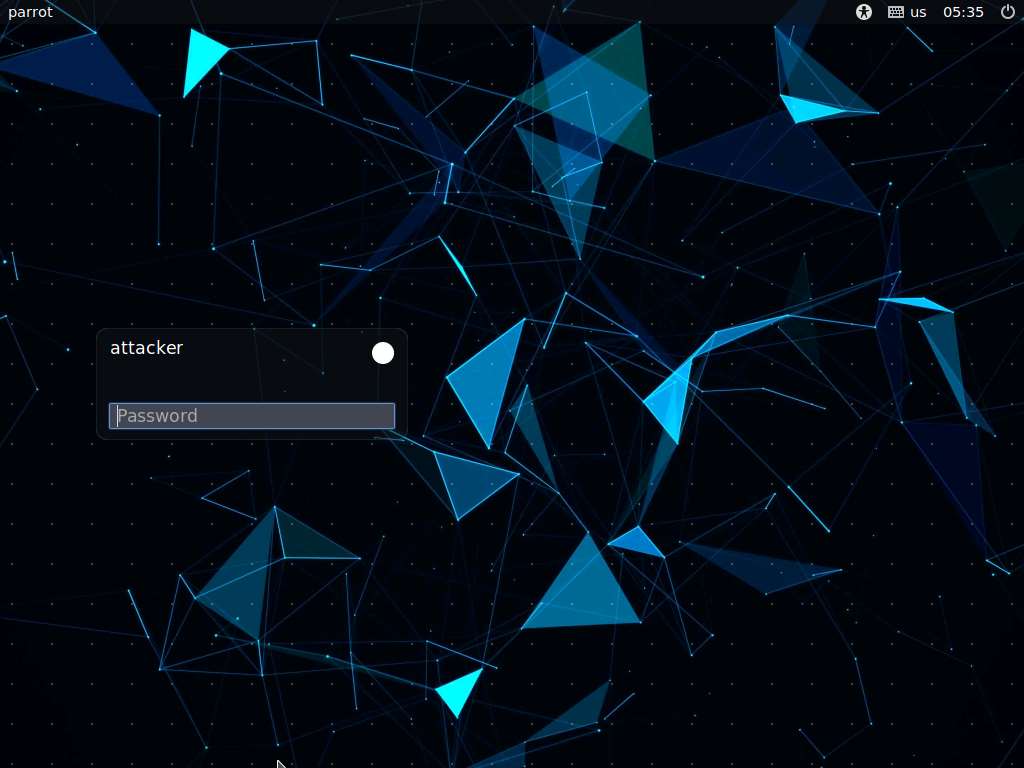
By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications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

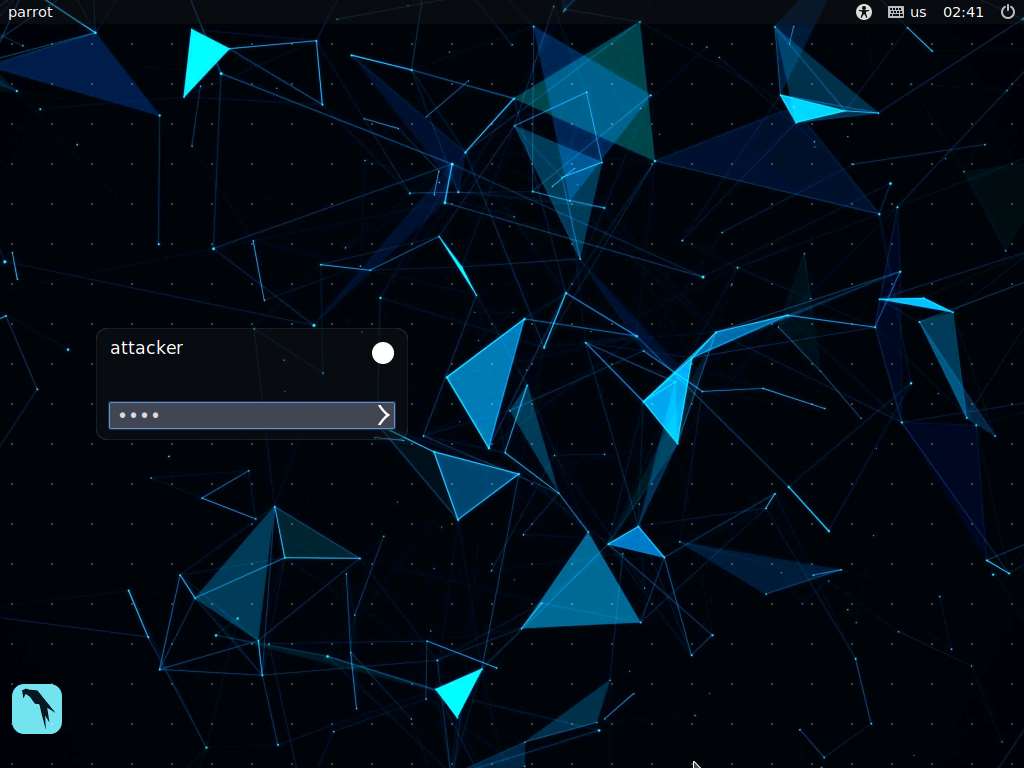
Ghost Eye is an information-gathering tool written in Python 3. To run, Ghost Eye only needs a domain or IP. Ghost Eye can work with any Linux distros if they support Python 3.

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. By default, the **Parrot Security** machine is selected.



1. 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.



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

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

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

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

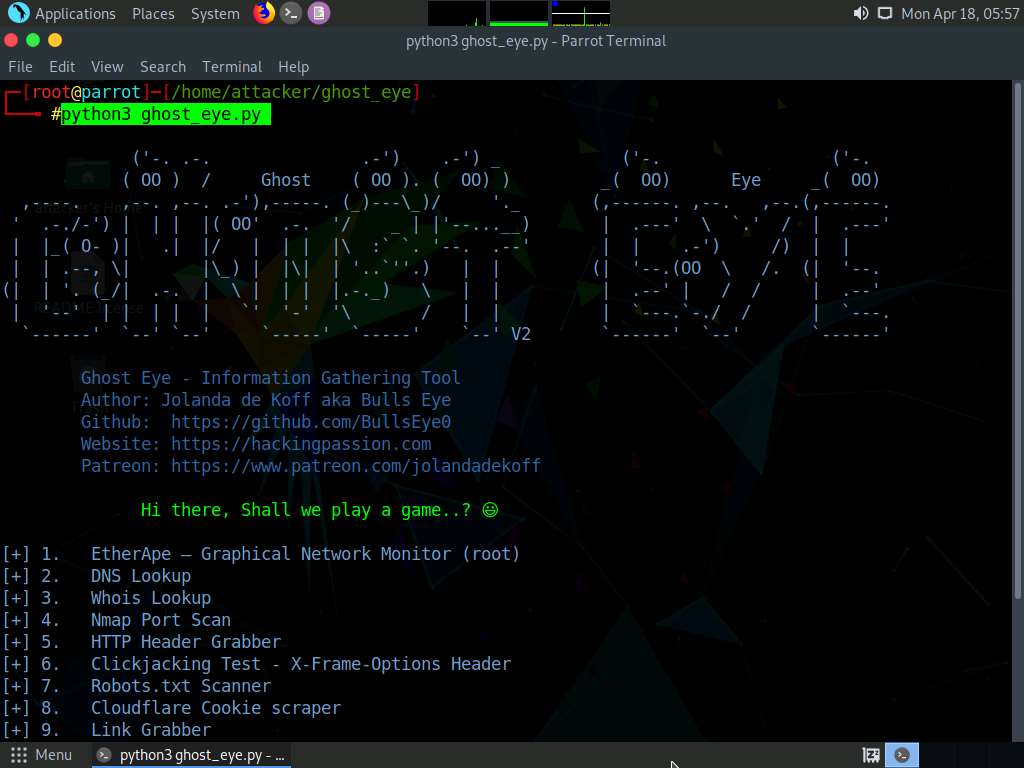
1. Now, navigate to the Ghost Eye directory. Type **cd ghost\_eye** and press **Enter**.



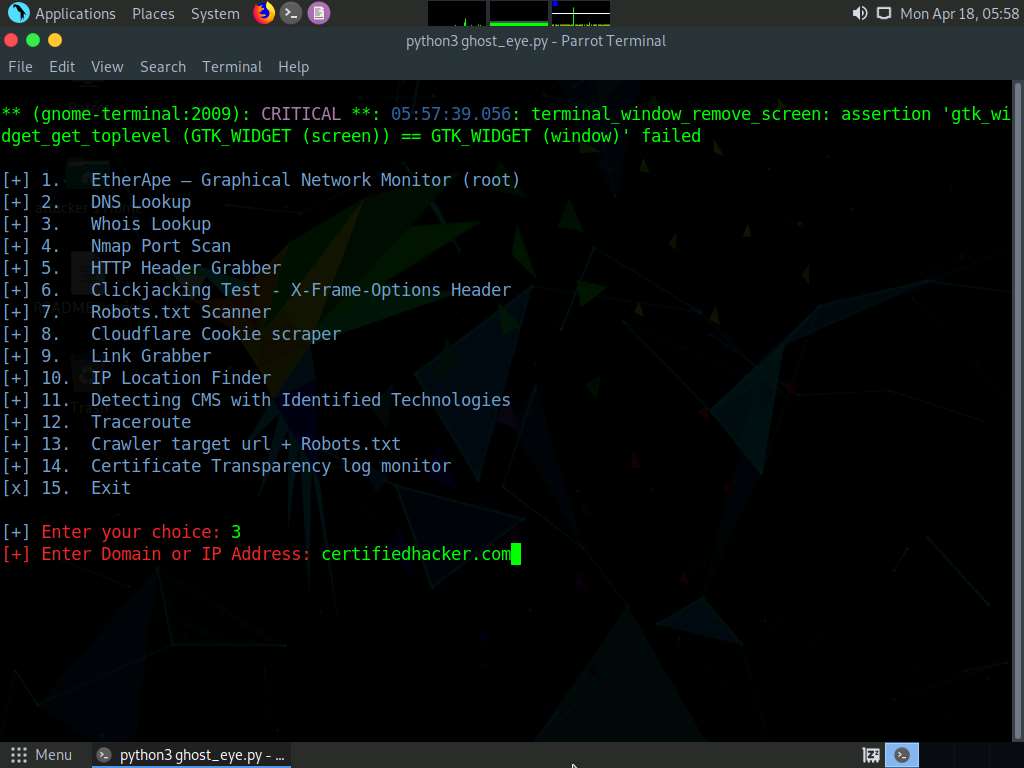
1. In the terminal window, type **pip3 install -r requirements.txt** and press **Enter**.



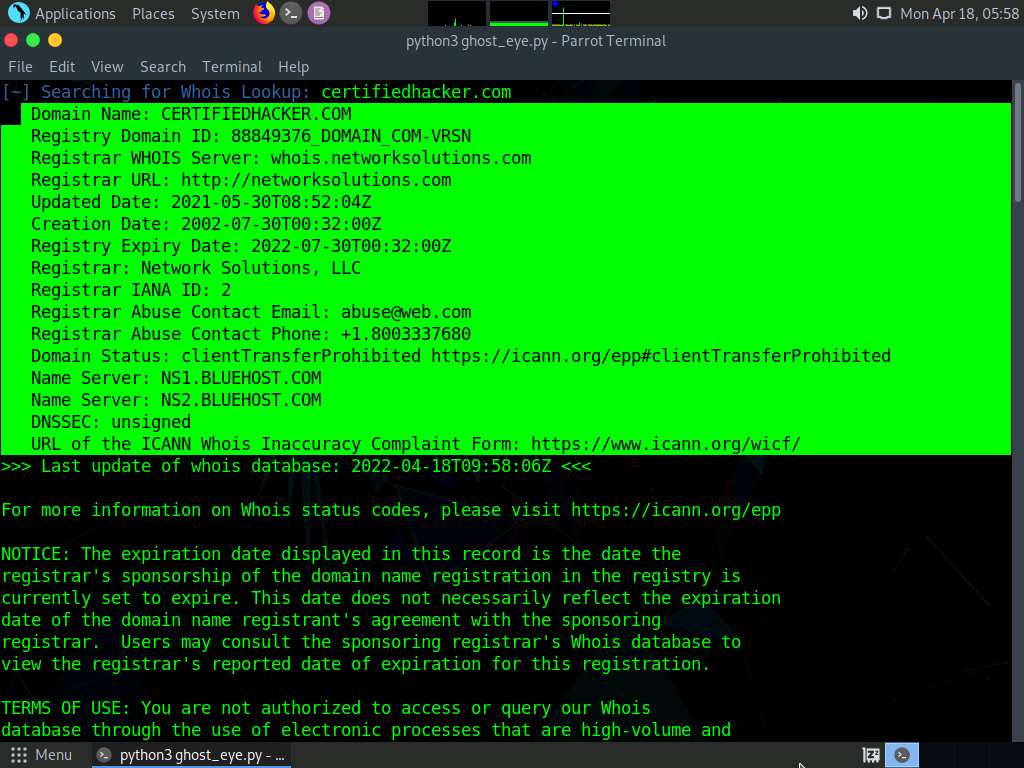
1. To launch Ghost Eye, type **python3 ghost\_eye.py** and press **Enter**.



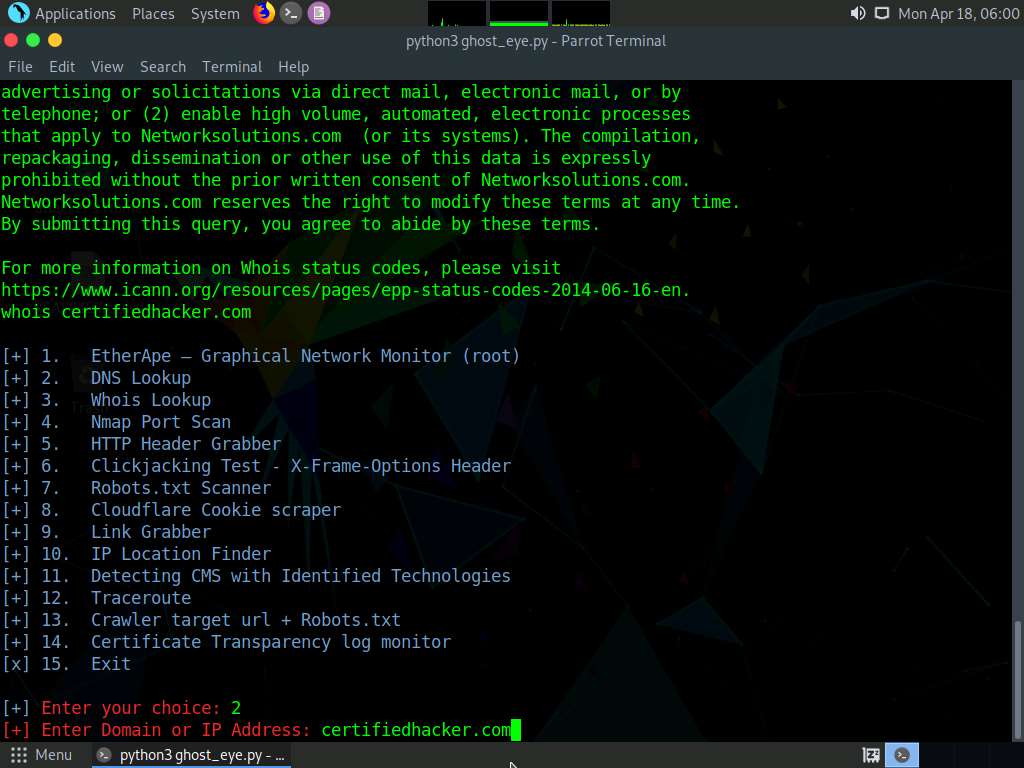
1. The Ghost Eye - Information Gathering Tool options appear, as shown in the screenshot.
2. Let us perform a Whois Lookup. Type **3** for the **Enter your choice**: option and press **Enter**.
3. Type **certifiedhacker.com** in the **Enter Domain or IP Address**: field and press **Enter**



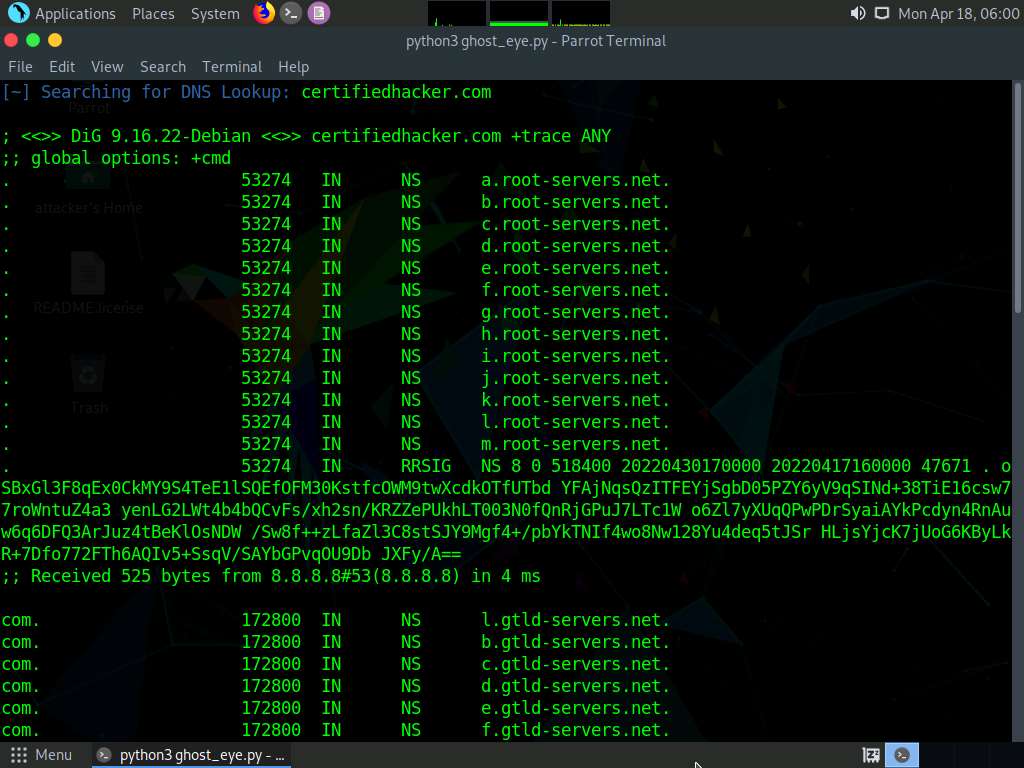
1. Scroll up to see the certifiedhacker.com result. In the result, observe the complete information of the certifiedhacker.com domain such as Domain Name, Registry Domain ID, Registrar WHOIS Server, Registrar URL, and Updated Date.



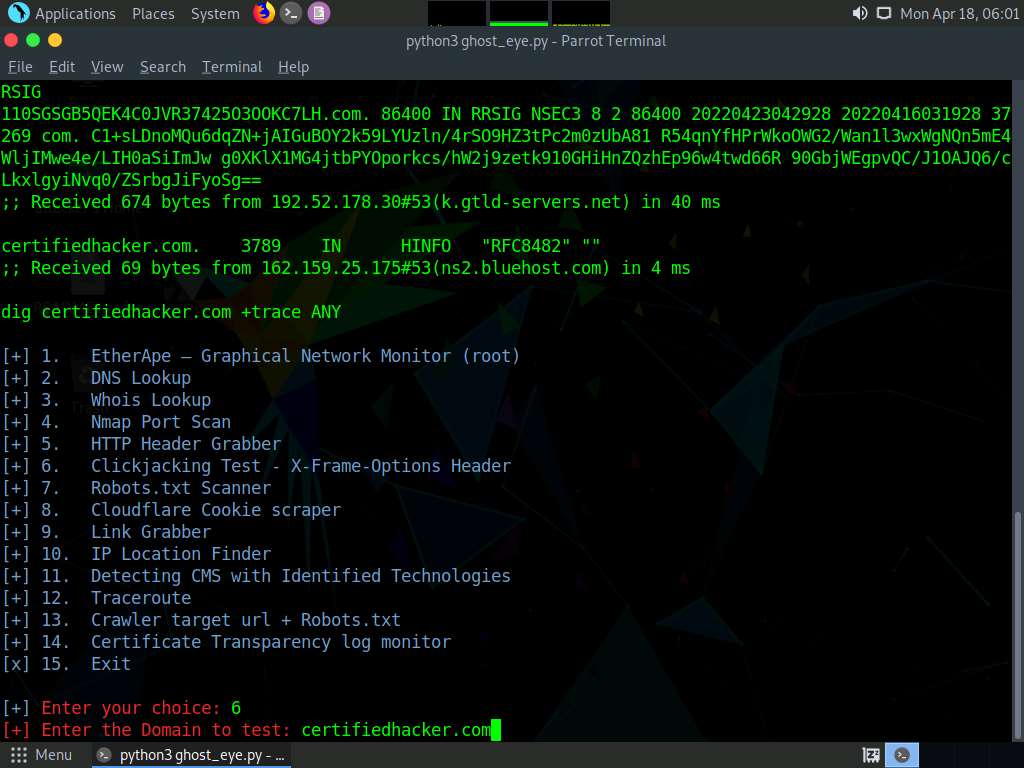
1. Let us perform a **DNS Lookup** on certifiedhacker.com. In the **Enter your choice field**, type **2** and press **Enter** to perform DNS Lookup.
2. The **Enter Domain or IP Address** field appears; type **certifiedhacker.com**, and press **Enter**.



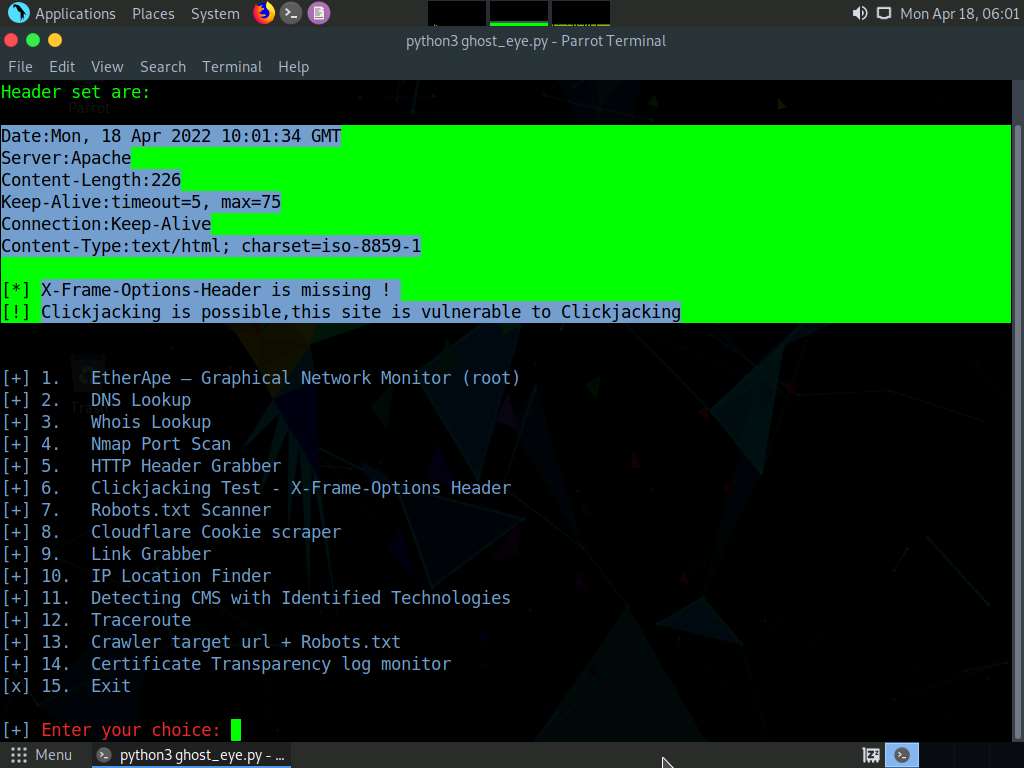
1. As soon as you hit **Enter**, Ghost Eye starts performing a DNS Lookup on the targeted domain (here, **certifiedhacker.com**).
2. Scroll up to view the DNS Lookup result.



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



1. 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.



1. 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.
2. This concludes the demonstration of how to gather information about a target web server using Ghost Eye.
3. Close all open windows on the **Parrot Security** machine.

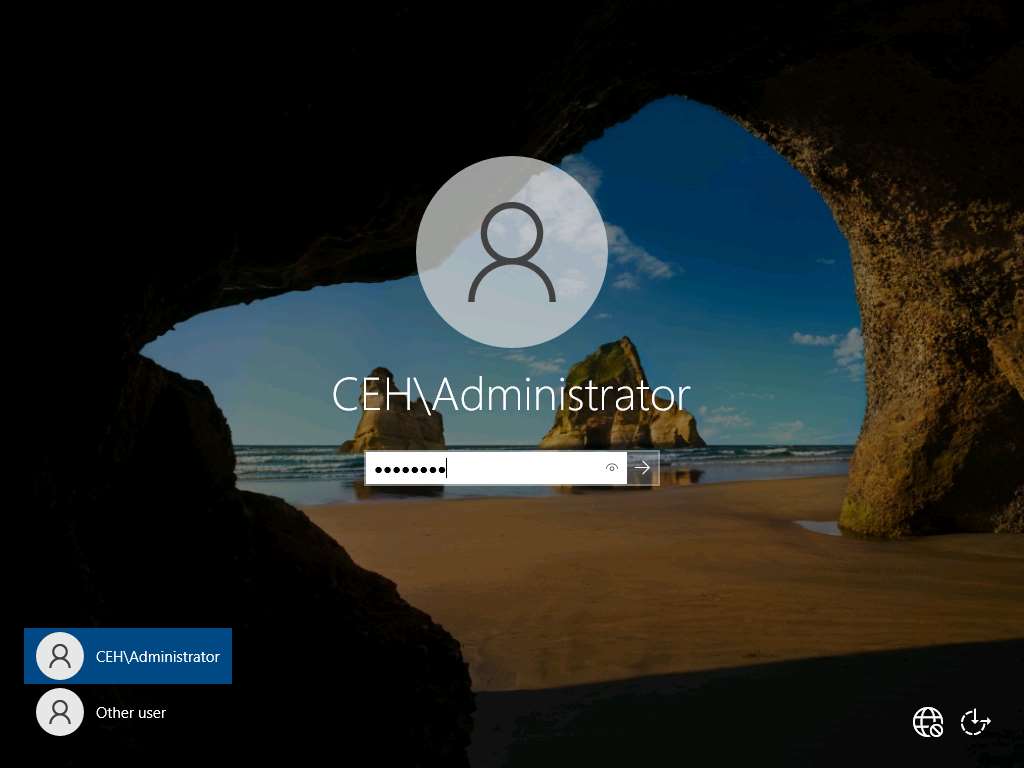
Task 2: Perform Web Server Reconnaissance using Skipfish

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.

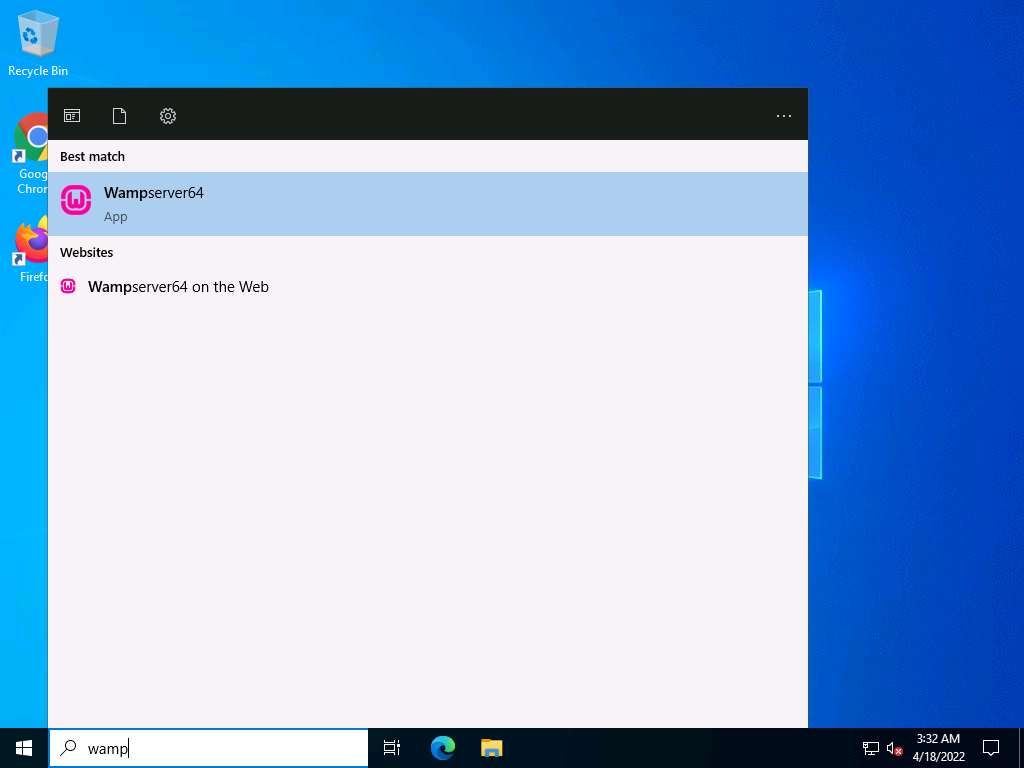
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine.



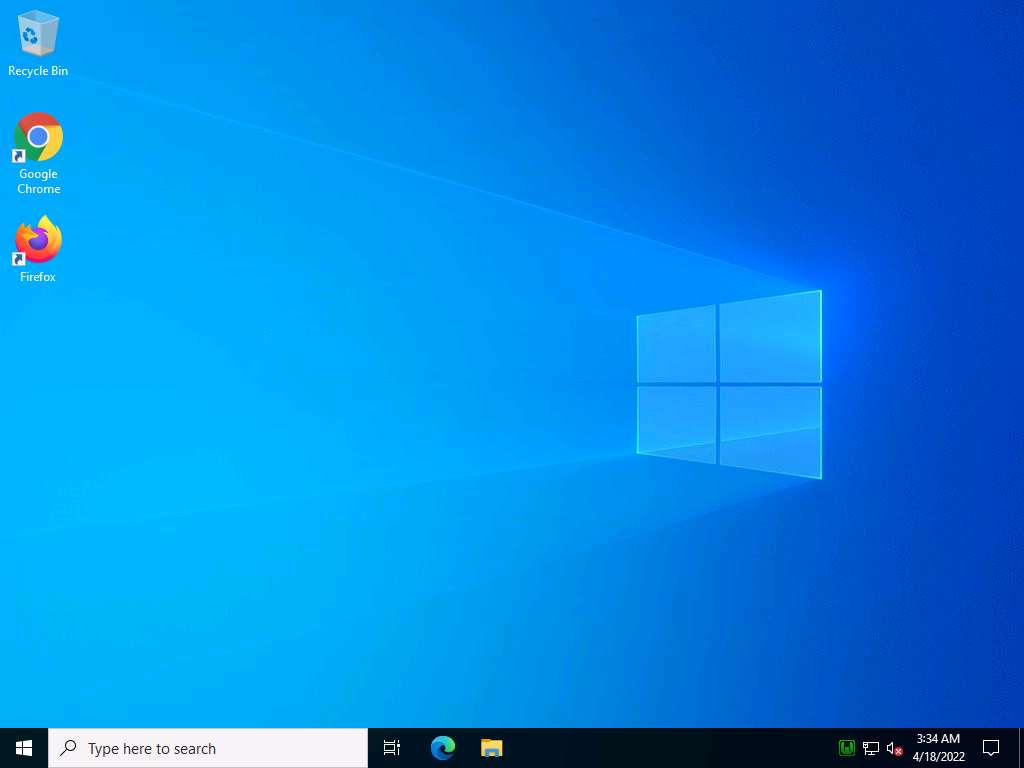
1. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



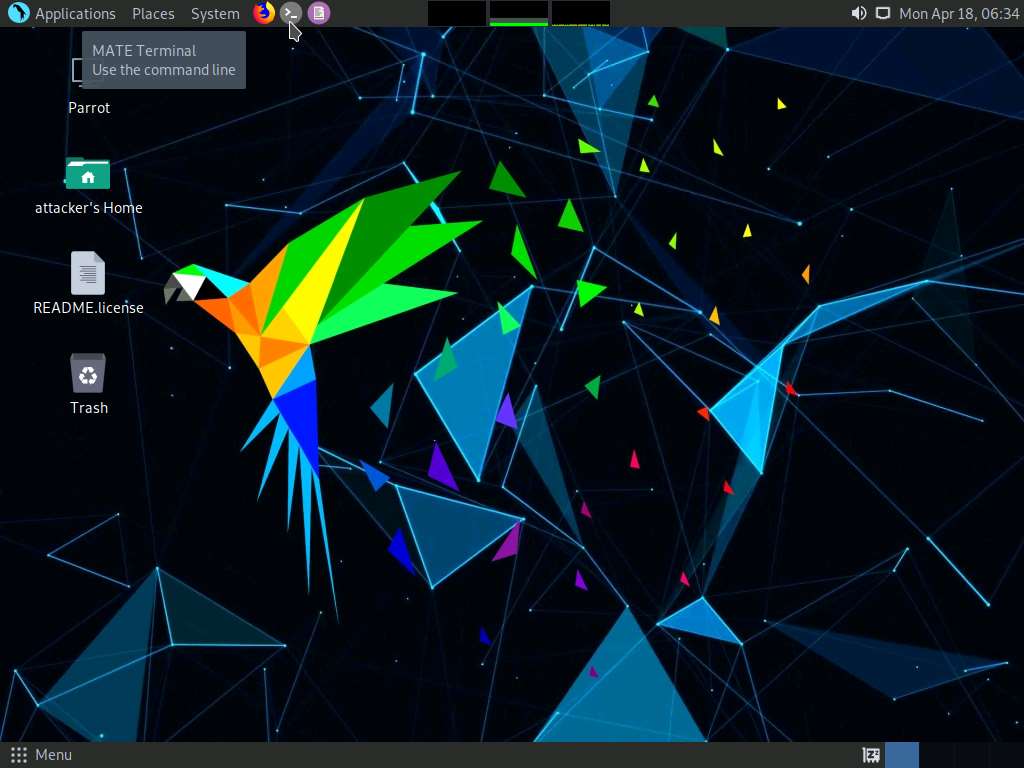
1. Click **Type here to search** field and type **wamp**. **Wamperserver64** appears in the result, press **Enter** to launch it.



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

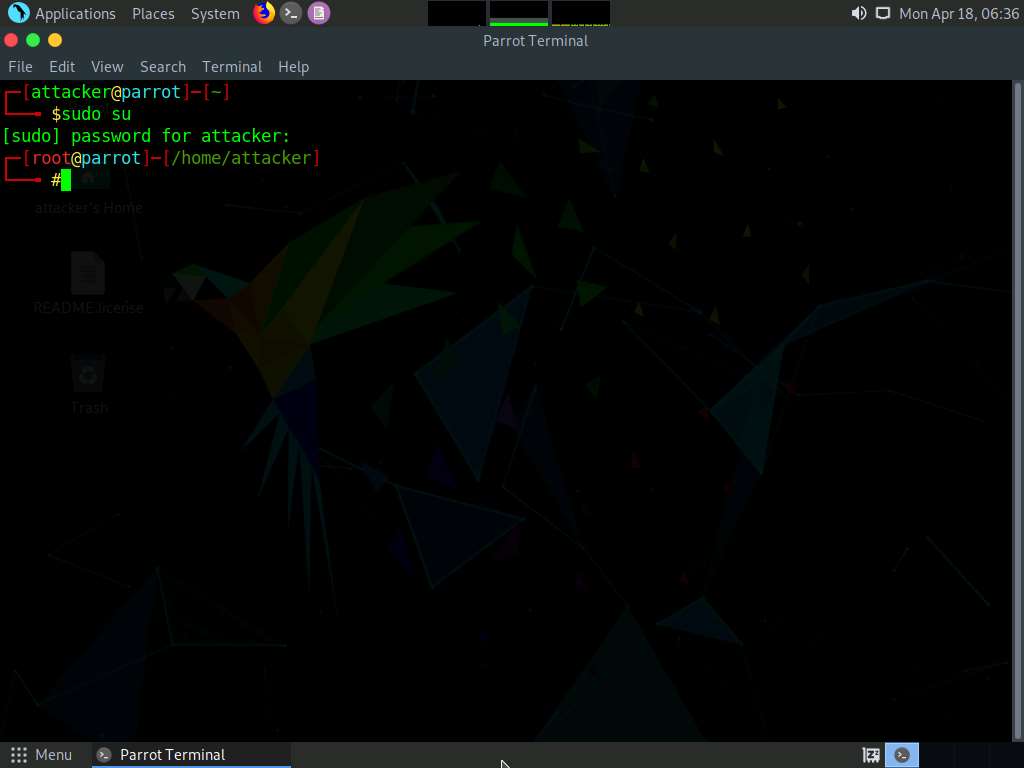


1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window.

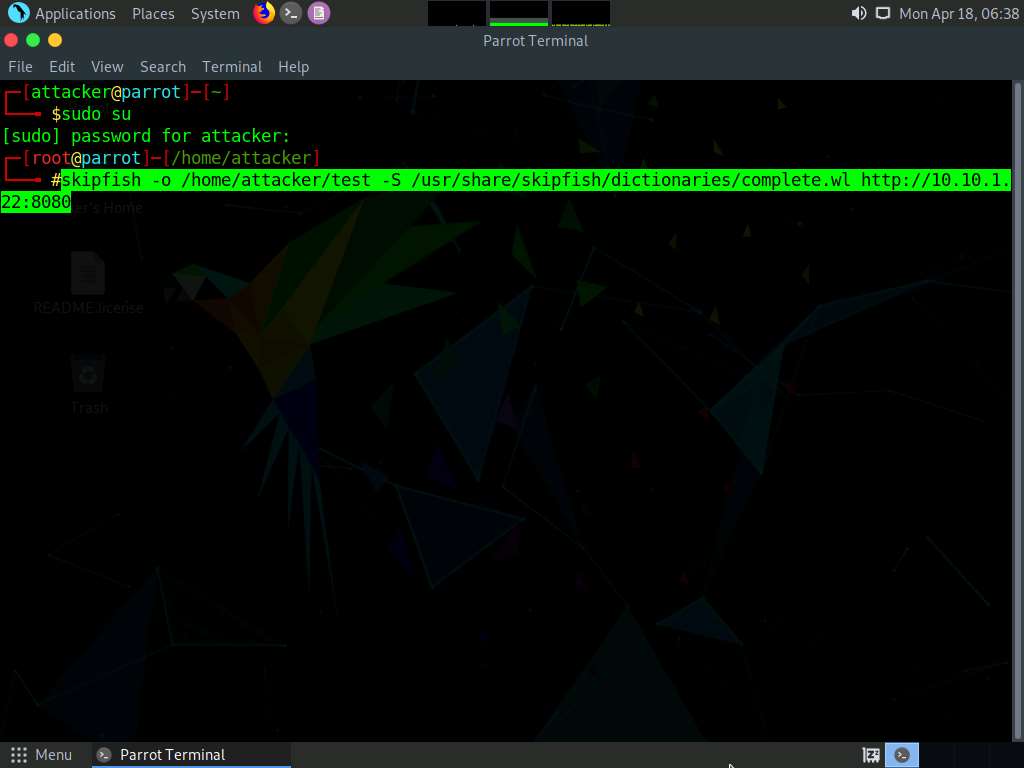


1. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
2. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

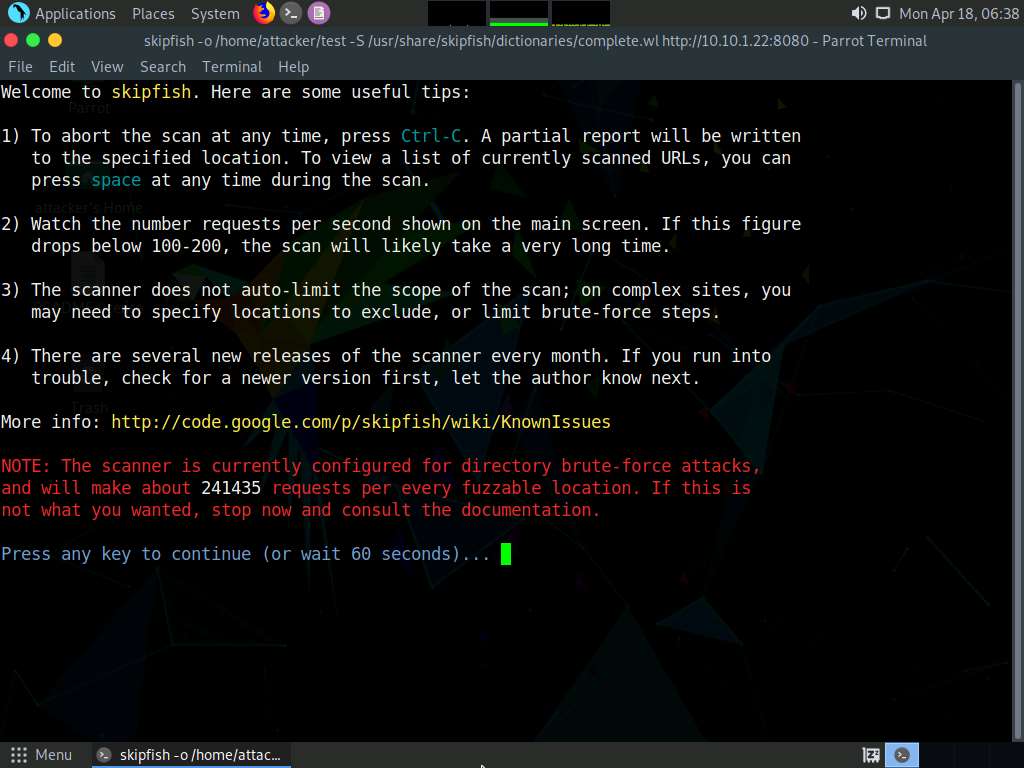
Note: The password that you type will not be visible.



1. Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http://[IP Address of Windows Server 2022]**.
2. 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**.
3. 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**.



1. 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.
2. Before beginning a scan, Skipfish displays some tips. Press **Enter** to start the security reconnaissance.



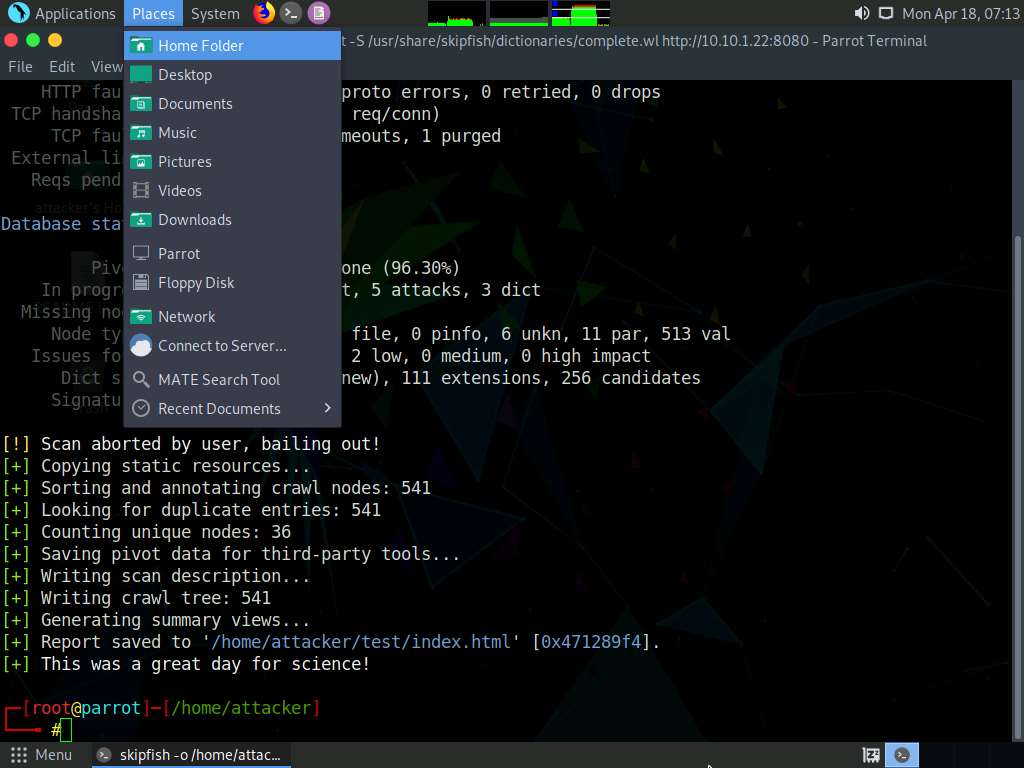
1. Skipfish scans the web server, as shown in the screenshot.



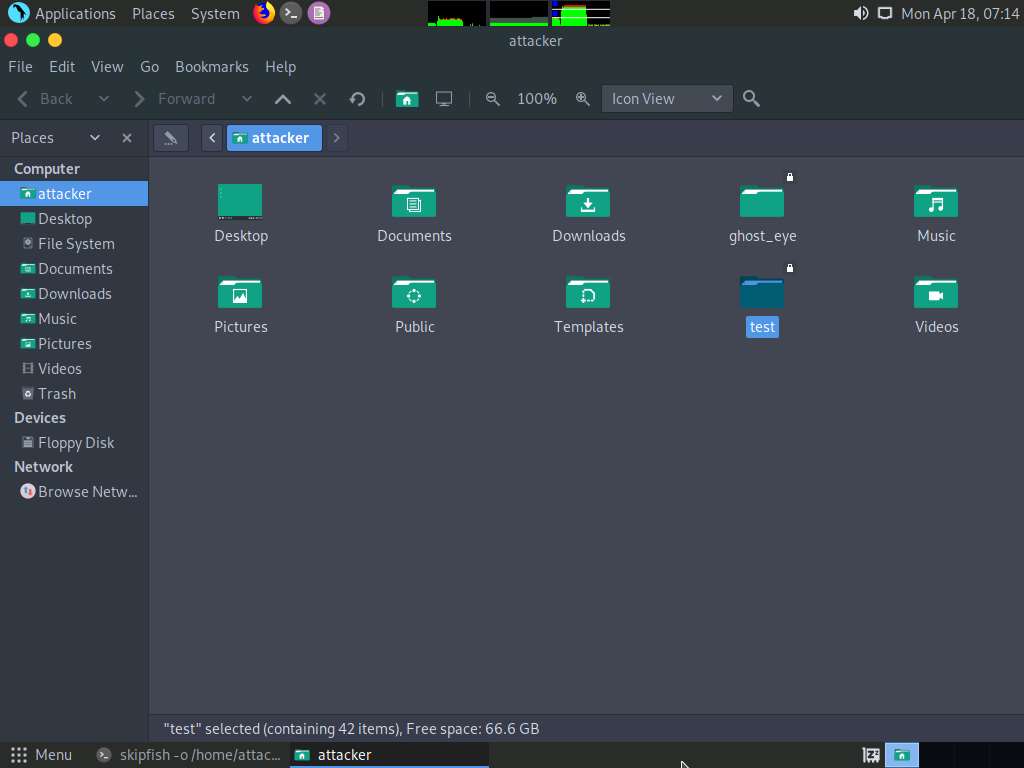
1. Let the Skipfish run the scan for 5 minutes and after that press **Ctrl+C** to terminate the scan.



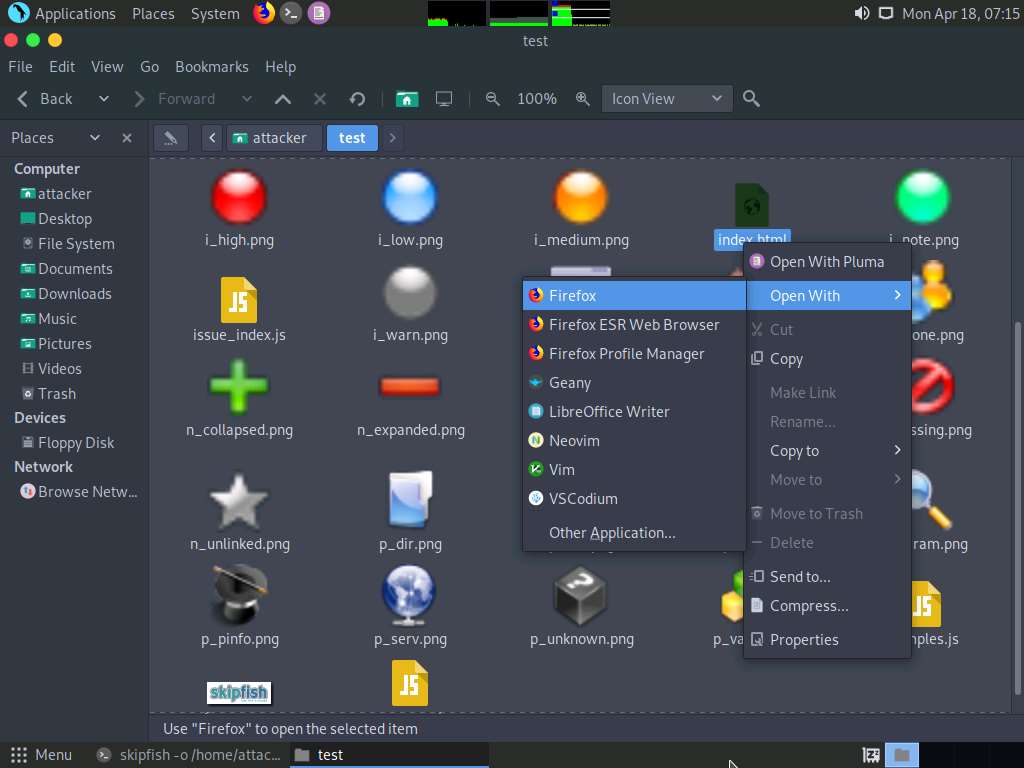
1. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **/home/attacker/** location). Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



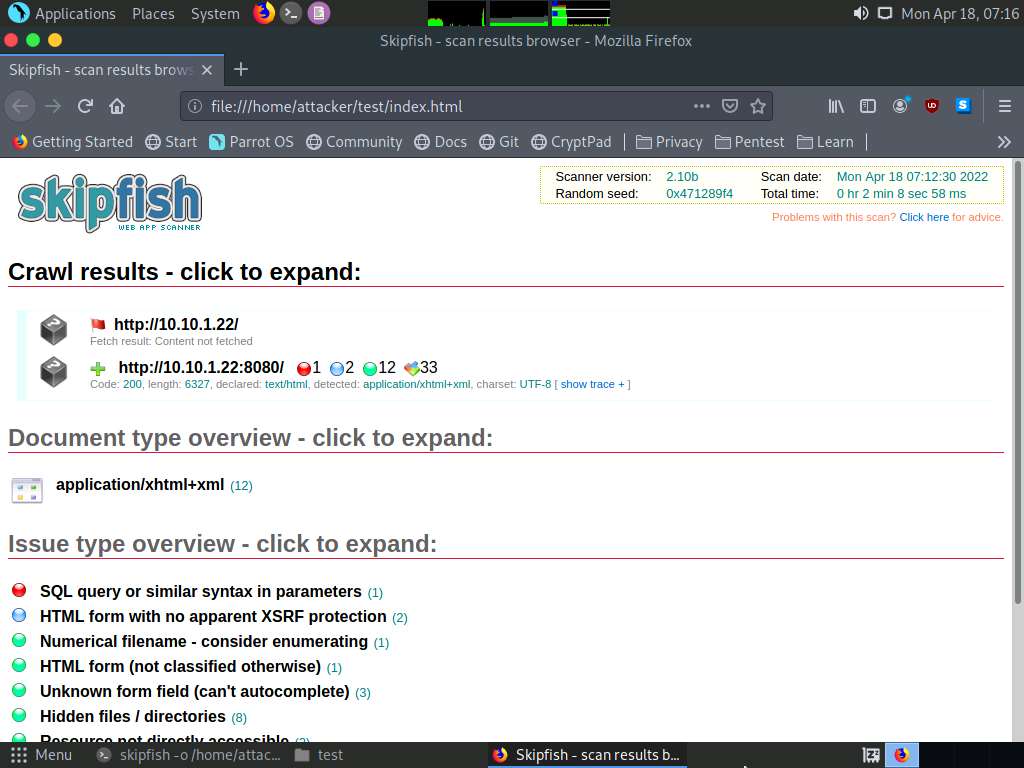
1. The **attacker** window appears, double-click **test** folder.



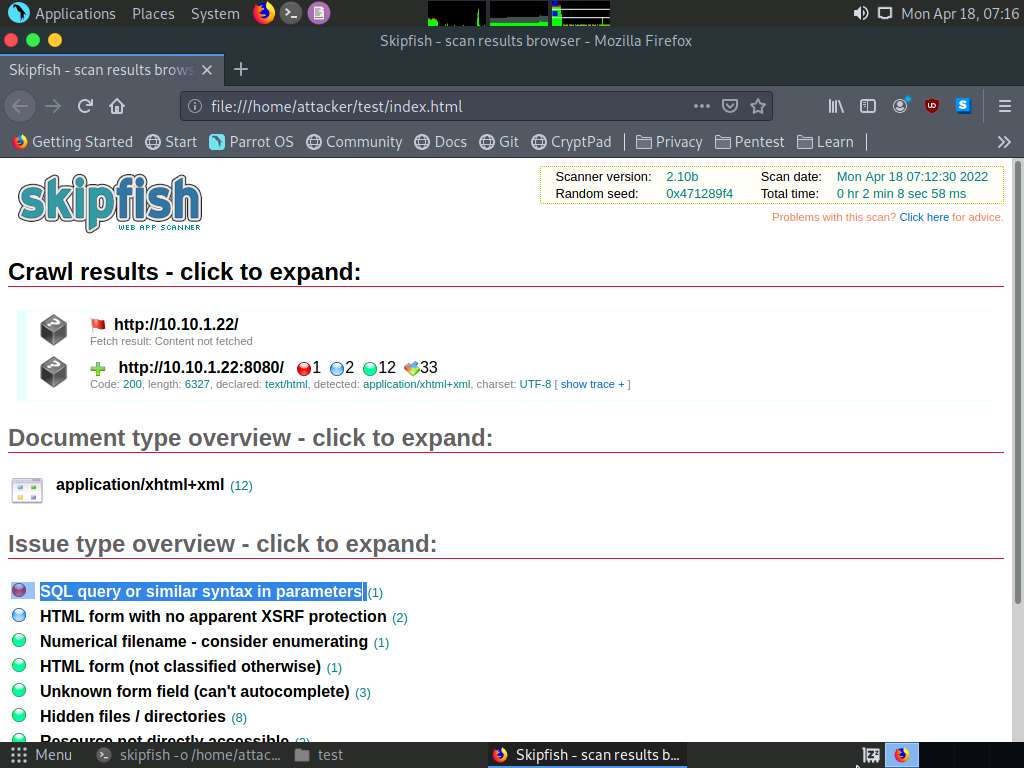
1. Right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.



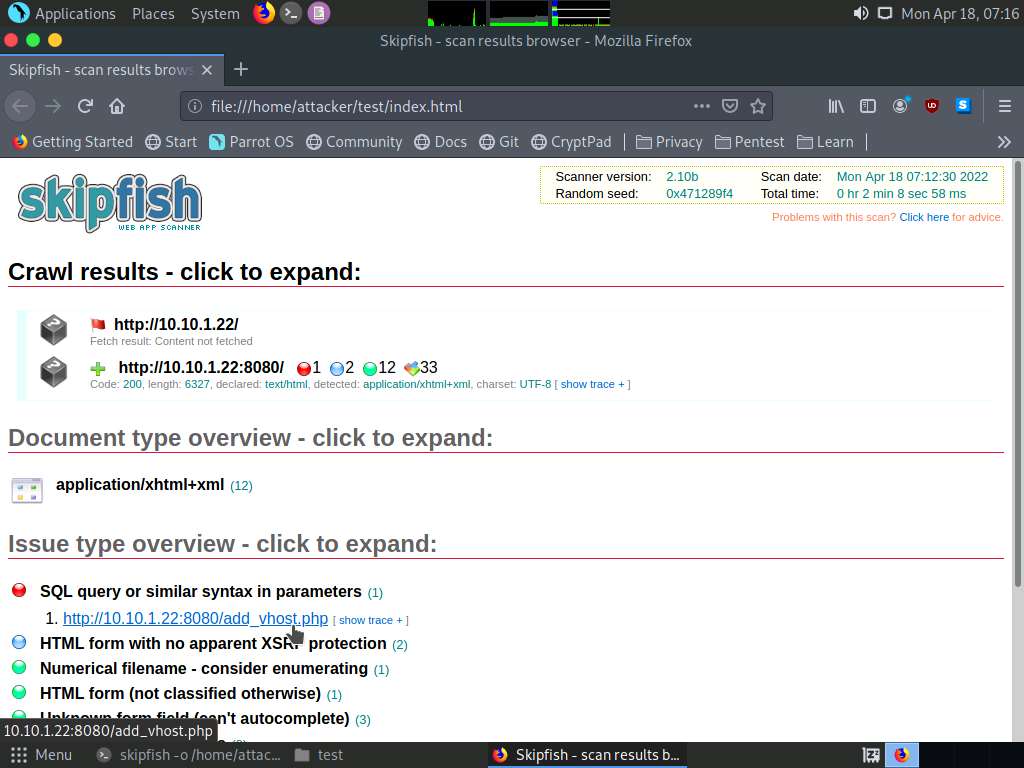
1. The Skipfish crawl result appears in the web browser, displaying a summary overview of document and issue types found, as shown in the screenshot.



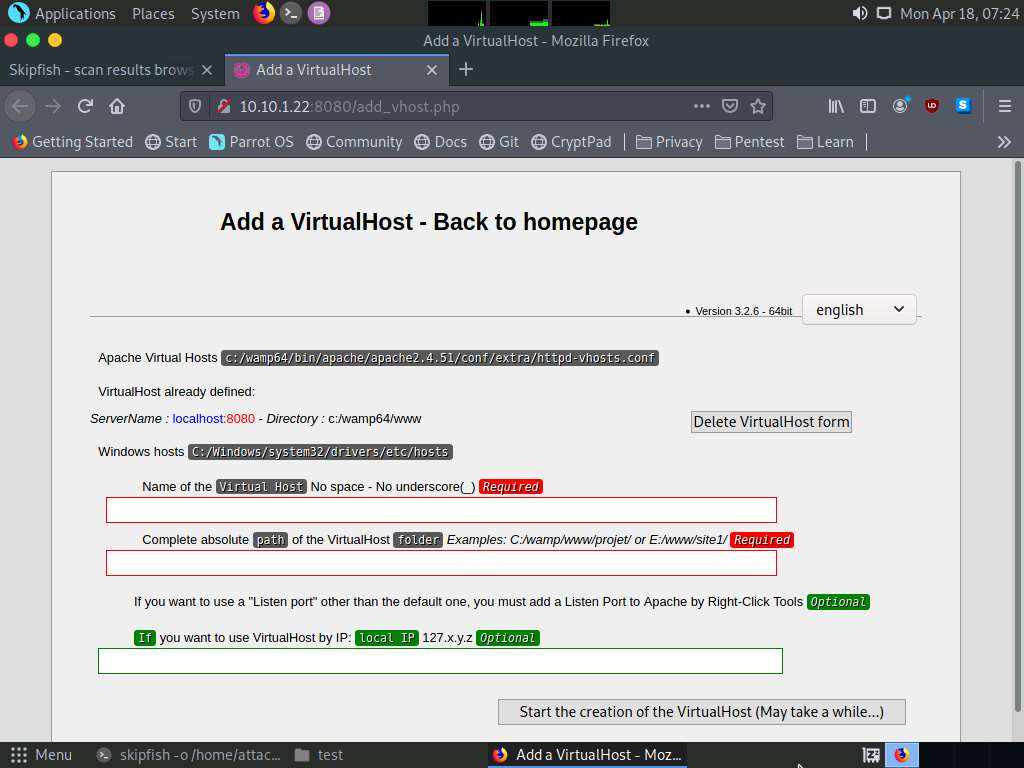
1. Expand each node to view detailed information regarding the result.
2. Analyze an issue found in the web server. To do this, click a node under the **Issue type overview** section to expand it.
3. Analyze the **SQL query or similar syntax in parameters** issue.



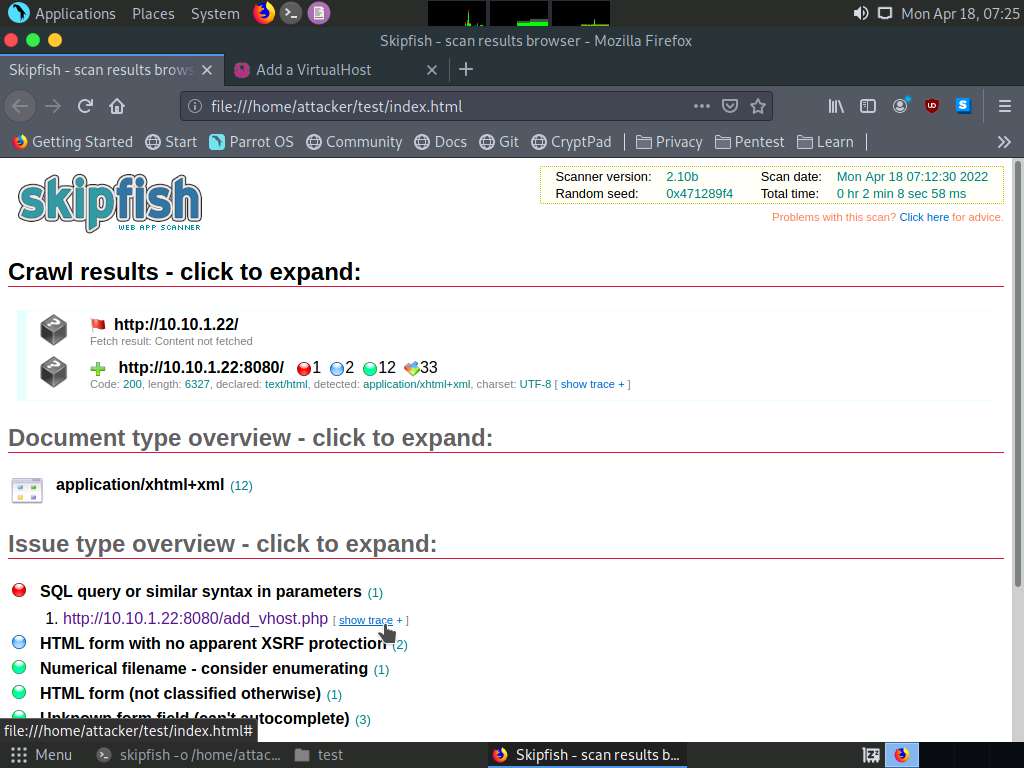
1. Observe the **URL** of the webpage associated with the vulnerability. Click the URL.



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

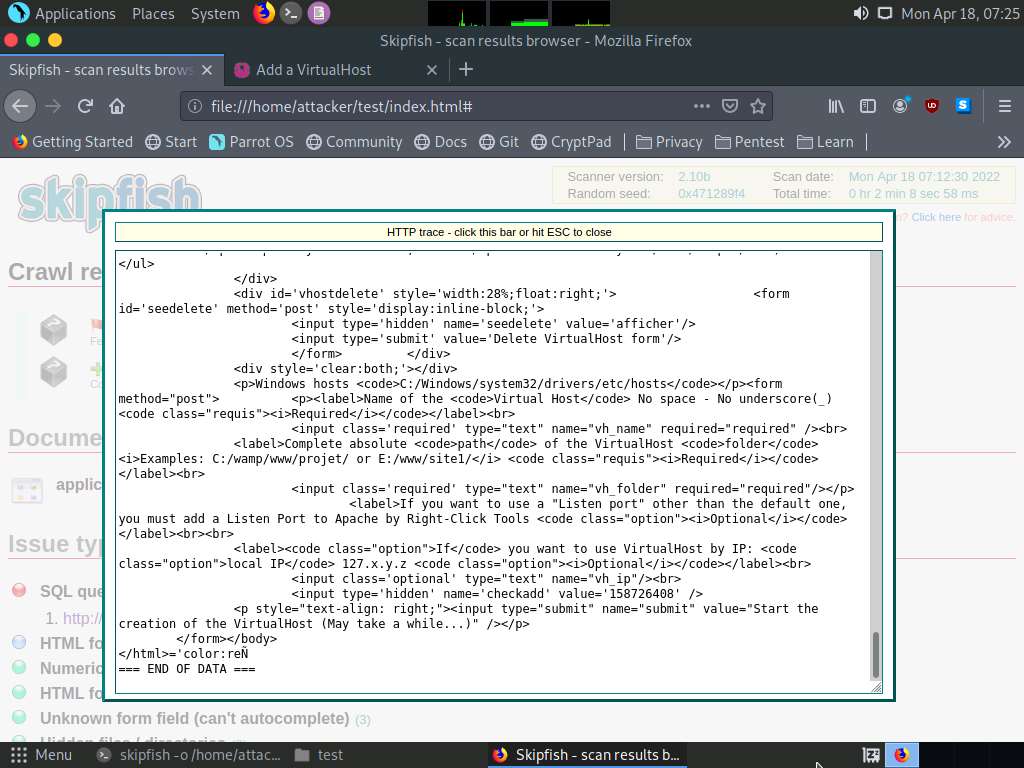


1. The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.
2. Switch back to the first tab and click **show trace** next to the URL to examine the vulnerability in detail.



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

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



1. Examine other vulnerabilities and patch them to secure the web server.
2. This concludes the demonstration of how to gather information about a target web server using Skipfish.
3. Close all open windows on both the **Parrot Security** and **Windows Server 2022** machines.

Task 3: Footprint a Web Server using the httprecon Tool

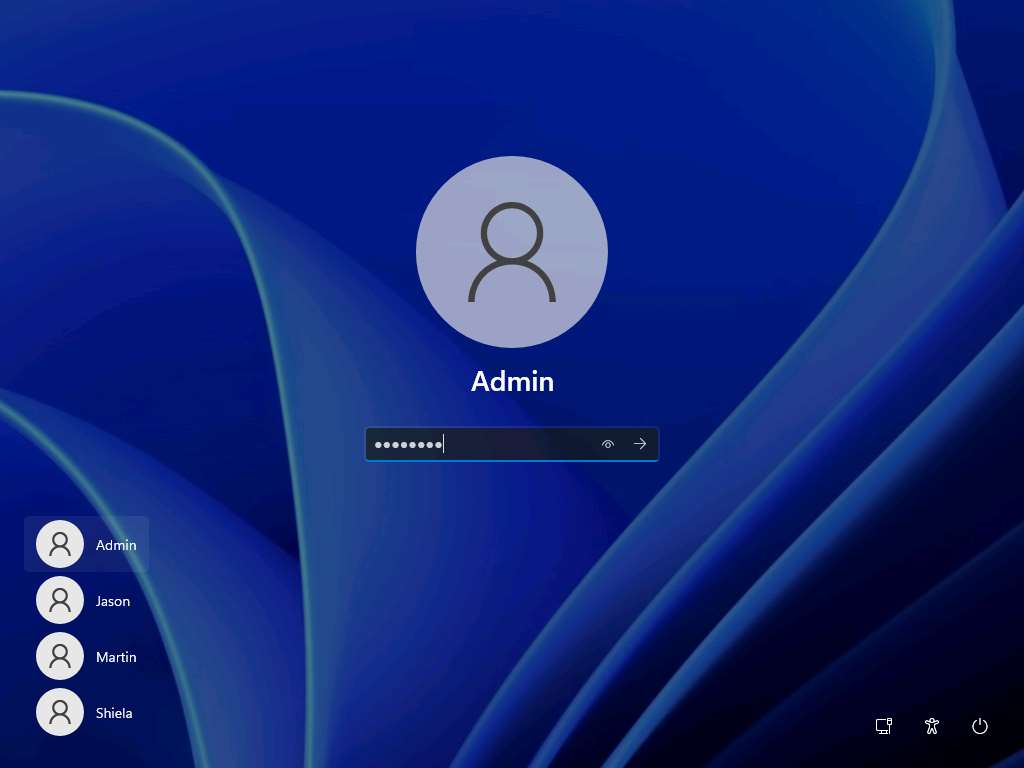
Web applications can publish information, interact with Internet users, and establish an e-commerce or e-government presence. However, if an organization is not rigorous in configuring and operating its public website, it may be vulnerable to a variety of security threats. Although the threats in cyberspace 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 **CEHv12 Windows 11** to switch to the **Windows 11**, click **Ctrl+Alt+Del**.
2. By default, **Admin** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.

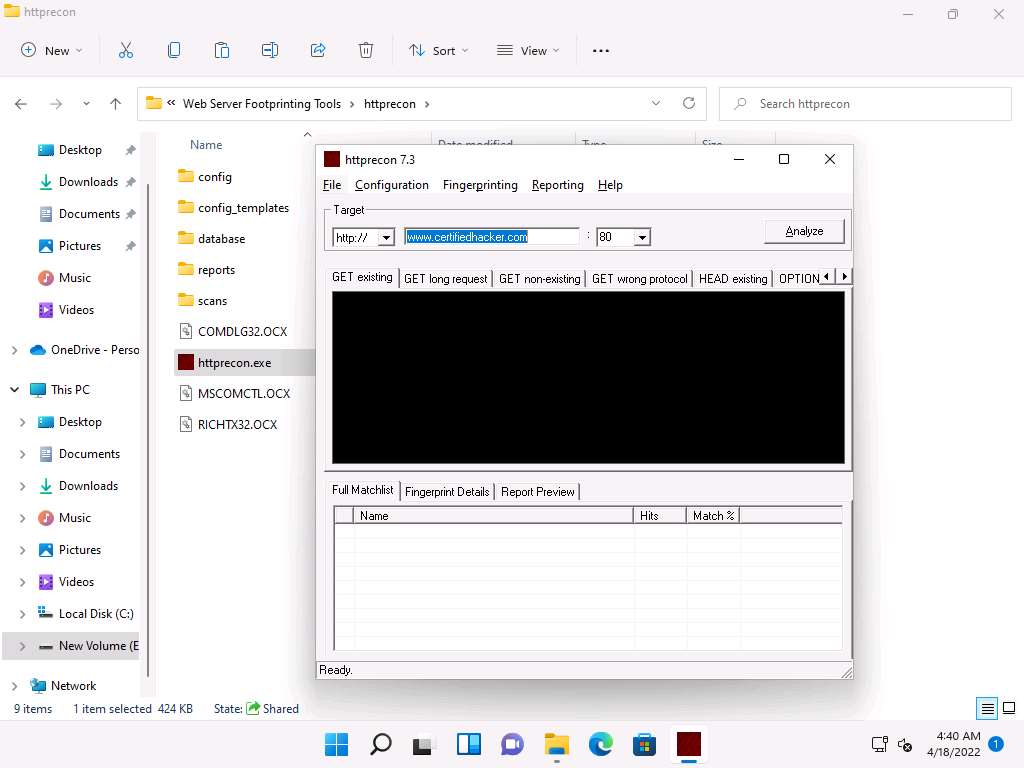
Note: Networks screen appears, click **Yes** to allow your PC to be discoverable by other PCs and devices on the network.



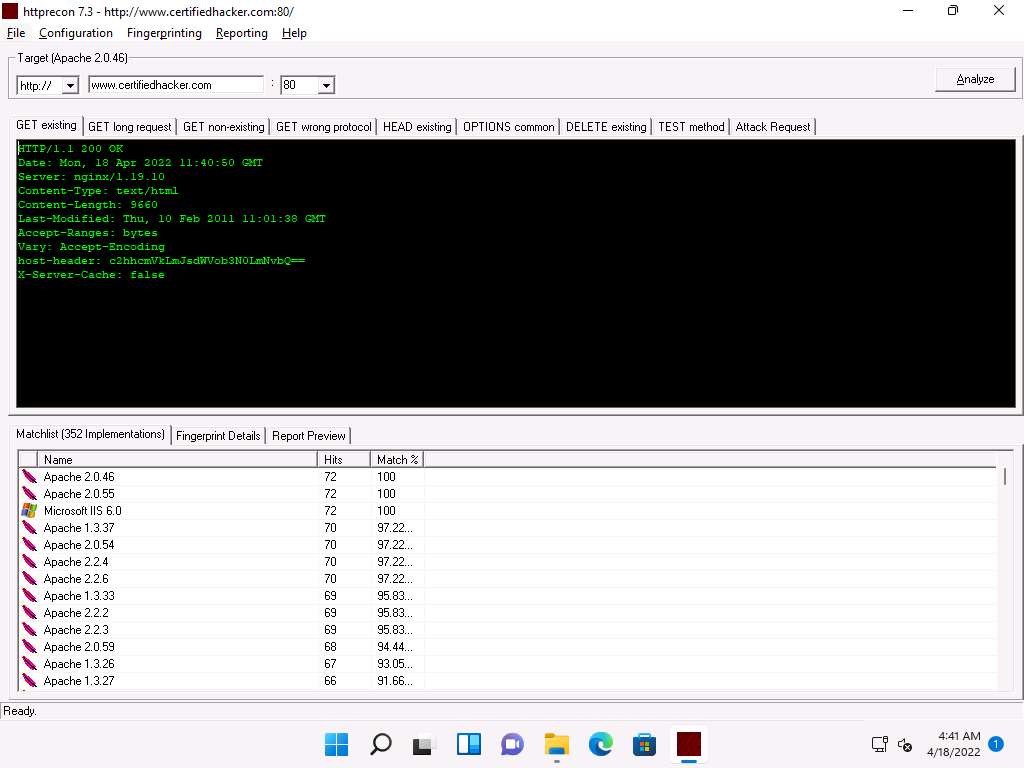
1. Navigate to **E:\CEH-Tools\CEHv12 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**, right-click **httprecon.exe**, and, from the context menu, click **Run as administrator** double-click to launch the application.

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

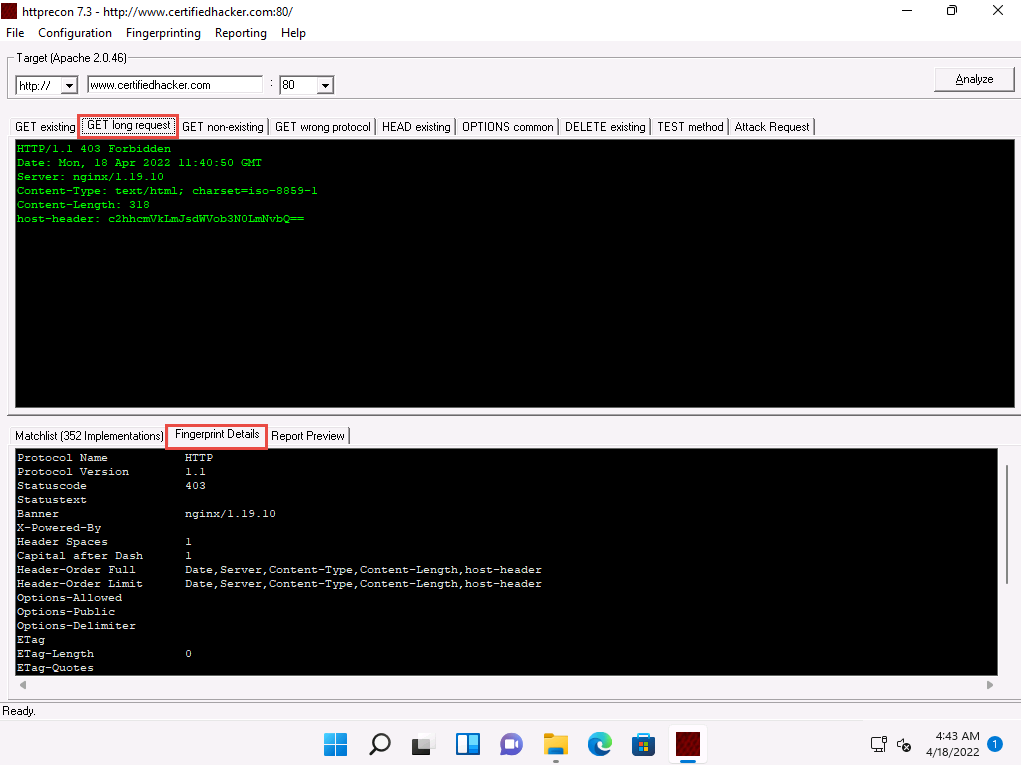
1. Main window of **httprecon** appears, enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number (80)** in the **Target** section.



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



1. Look at the **Get existing** tab, and observe the server (**nginx**) used to develop the webpages.
2. 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.
3. Click the **GET long request** tab, which lists all GET requests. Next, click the **Fingerprint Details** tab.



1. The details displayed in the screenshot above include the name of the protocol the website is using and its version.
2. 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.
3. This concludes the demonstration of how to gather information about the target web server using httprecon.
4. Close all open windows on the **Windows 11** machine.

Task 4: 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.

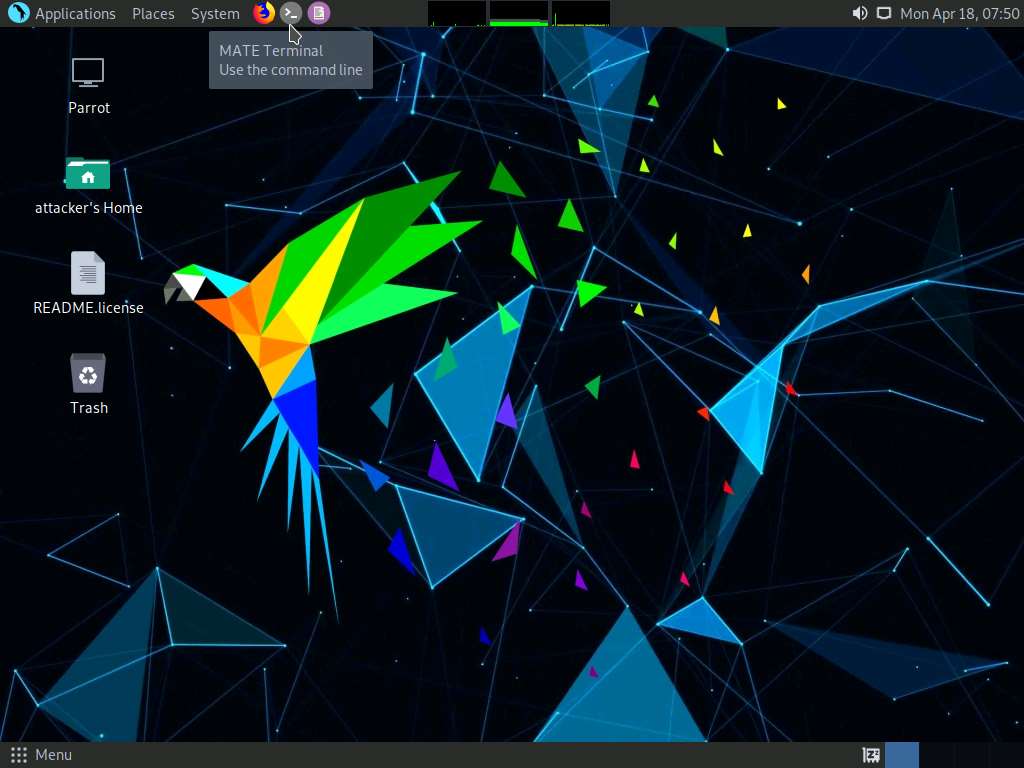
**Telnet**

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.

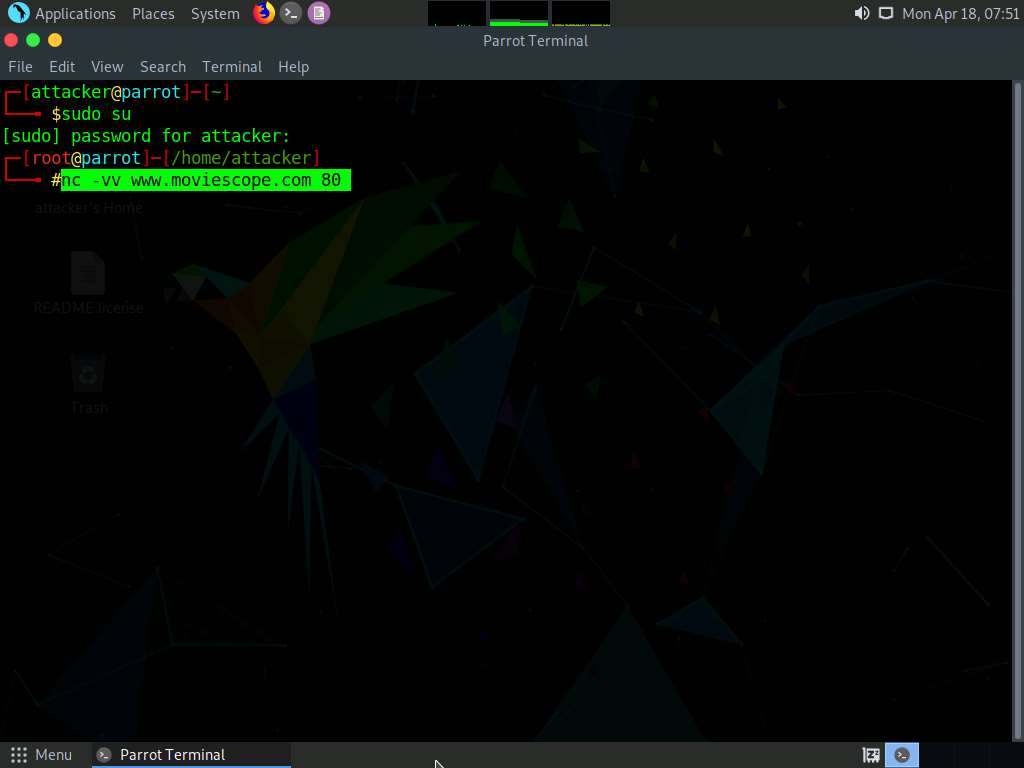
1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.
2. Click the **MATE Terminal** icon from the menu bar to launch the terminal.



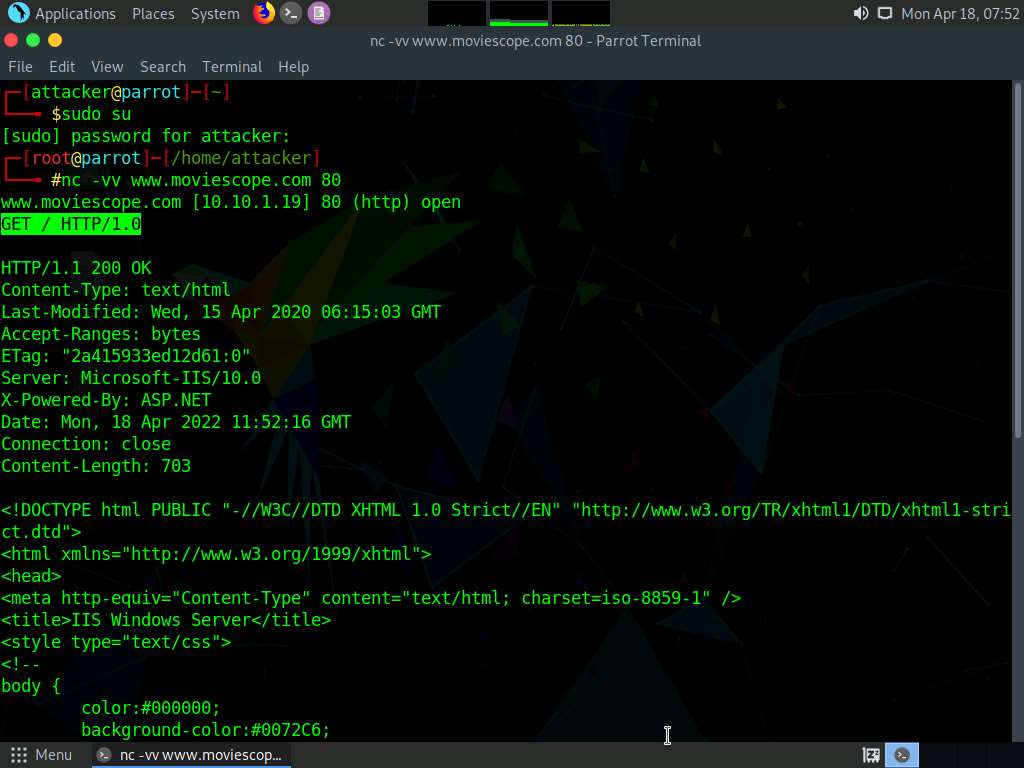
1. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
2. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

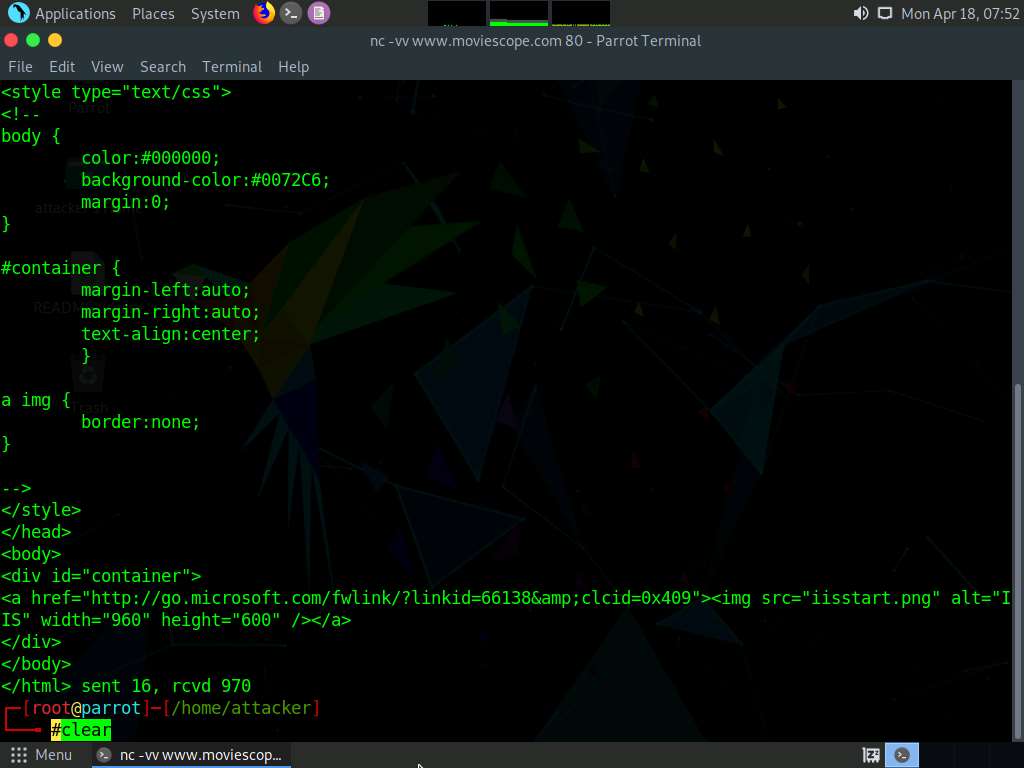
1. In the terminal window, type **nc -vv www.moviescope.com 80** and press **Enter**.



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



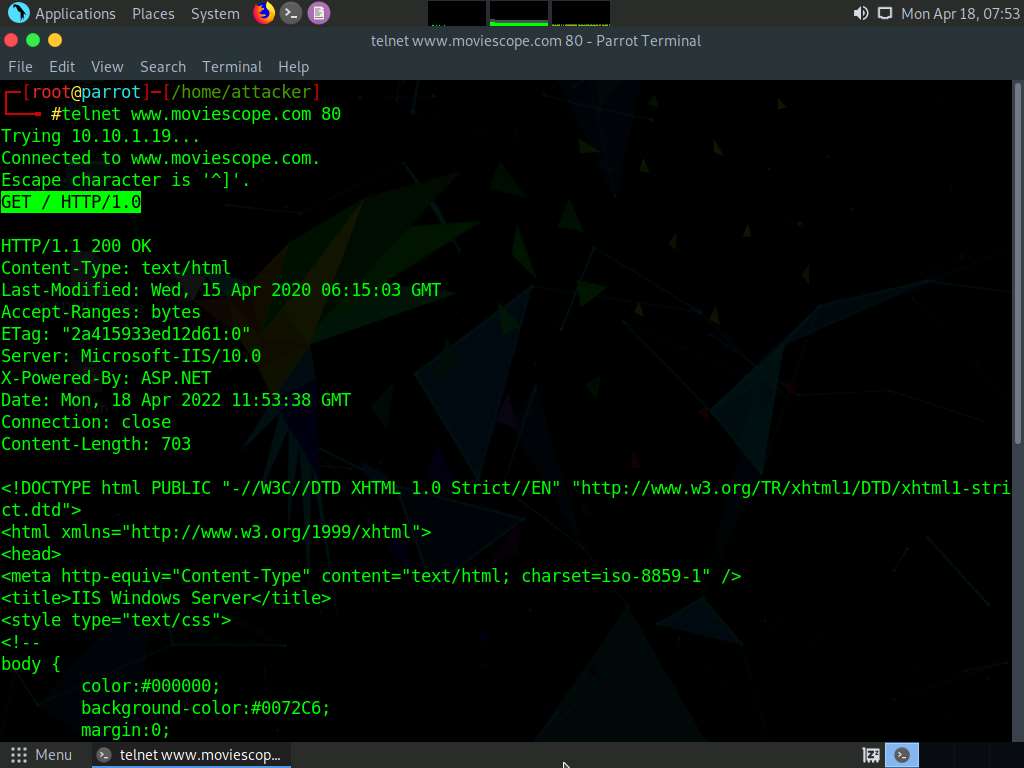
1. In the terminal windows, type **clear** and press **Enter** to clear the netcat result in the terminal window.



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



1. Telnet will connect to the domain, as shown in the screenshot.
2. 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.



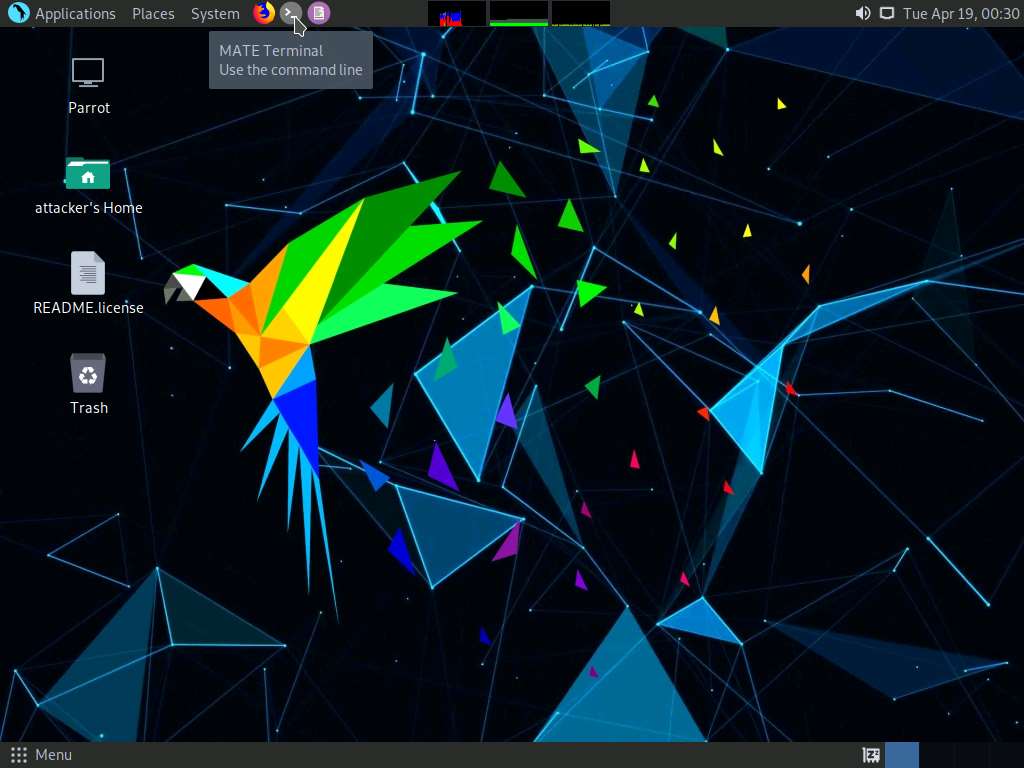
1. This concludes the demonstration of how to gather information about the target web server using the Netcat and Telnet utilities.
2. Close the terminal window on the **Parrot Security** machine.

Task 5: 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.

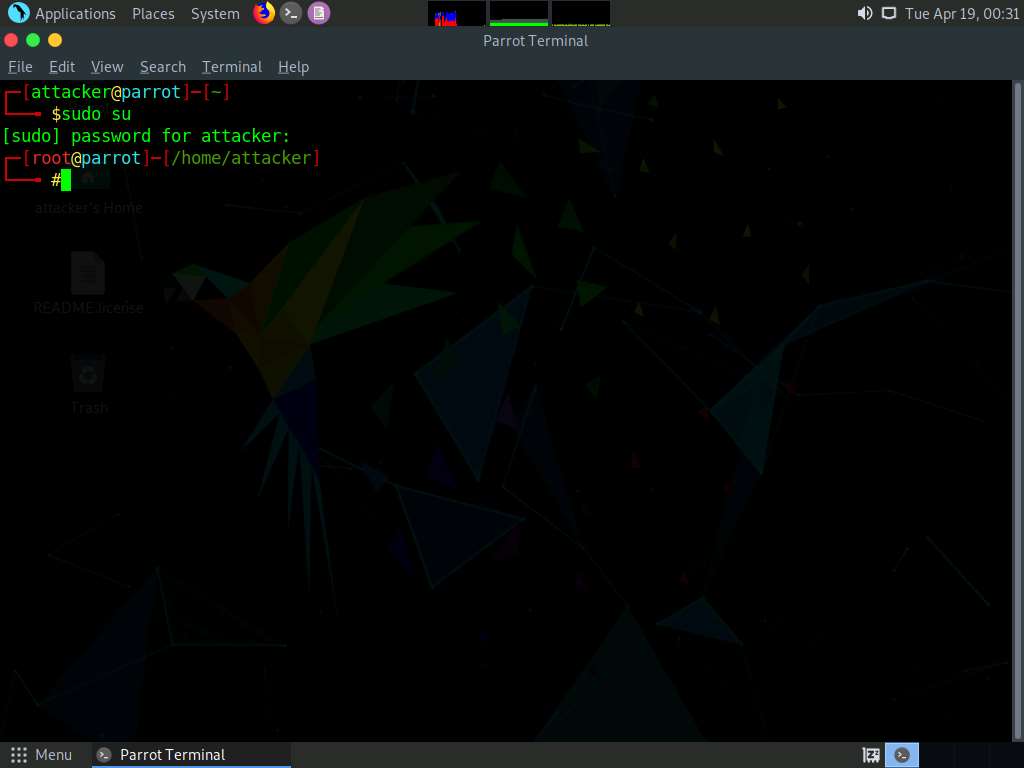
Nmap, along with Nmap Scripting Engine, can extract a lot of valuable information from the target web server. In addition to Nmap commands, Nmap Scripting Engine (NSE)provides scripts that reveal various useful information about the target web server to an attacker.

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

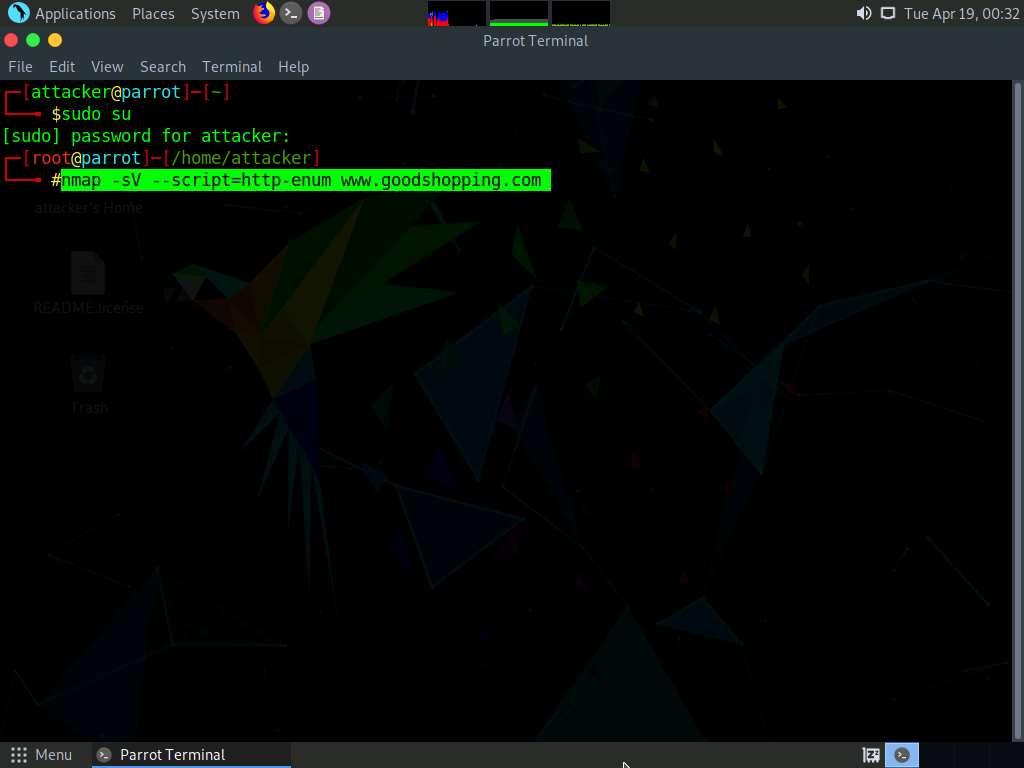


1. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
2. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

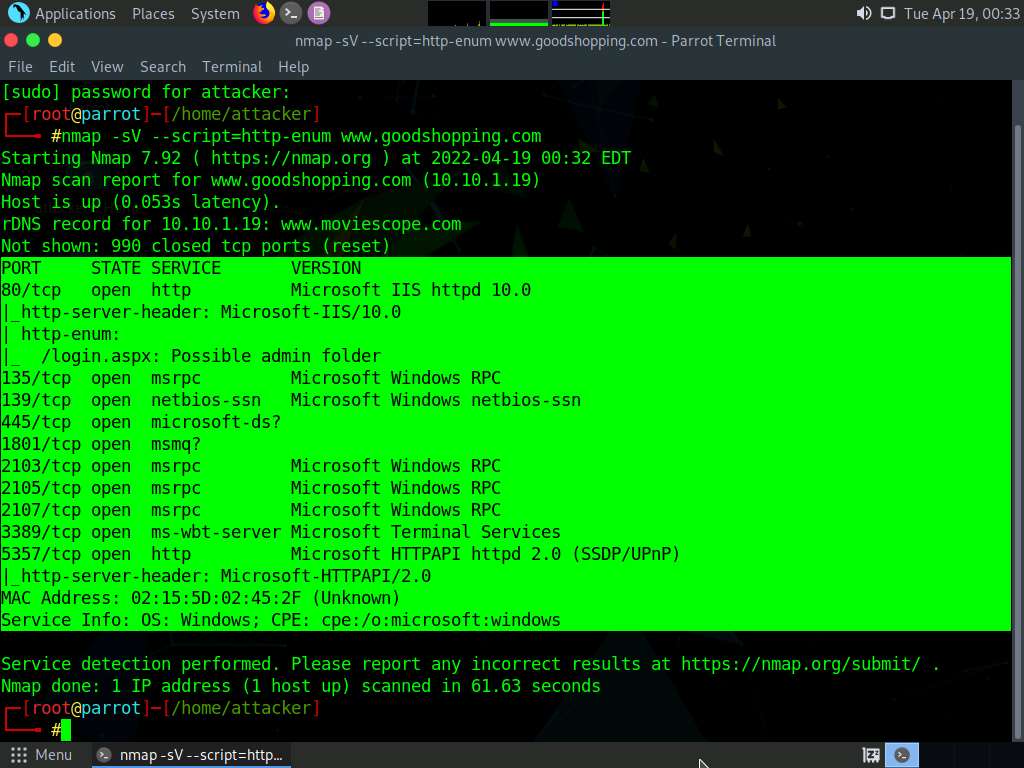
Note: The password that you type will not be visible.



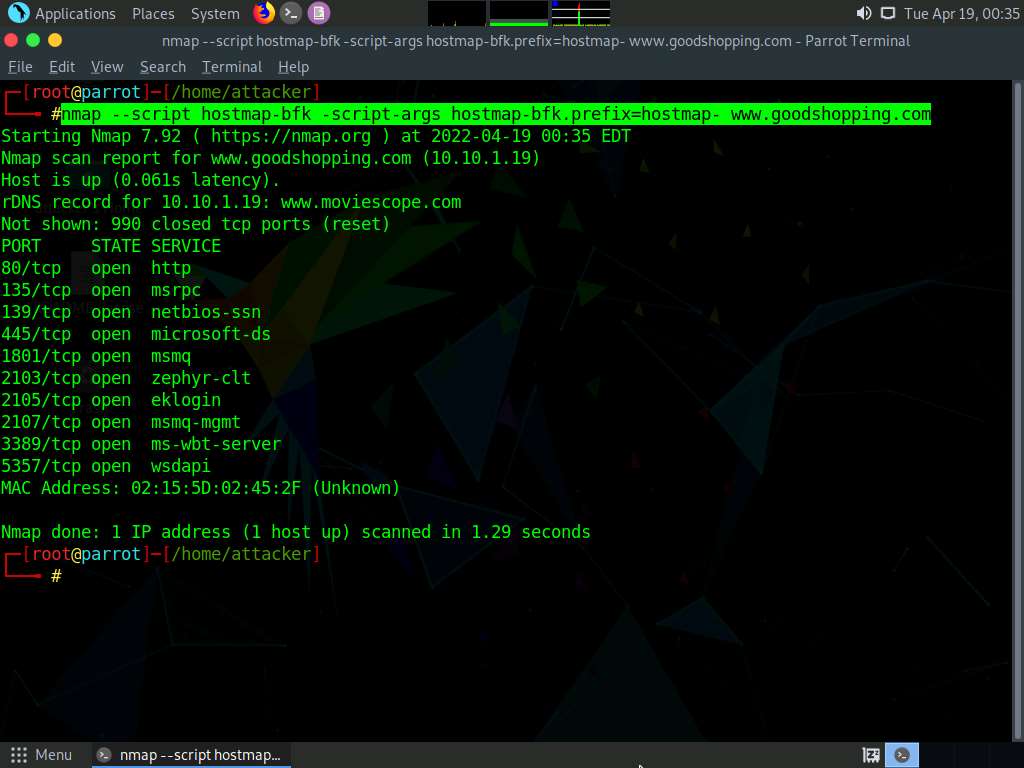
1. Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum [target website]** and press **Enter**.
2. In this scan, we are enumerating the **www.goodshopping.com** website.



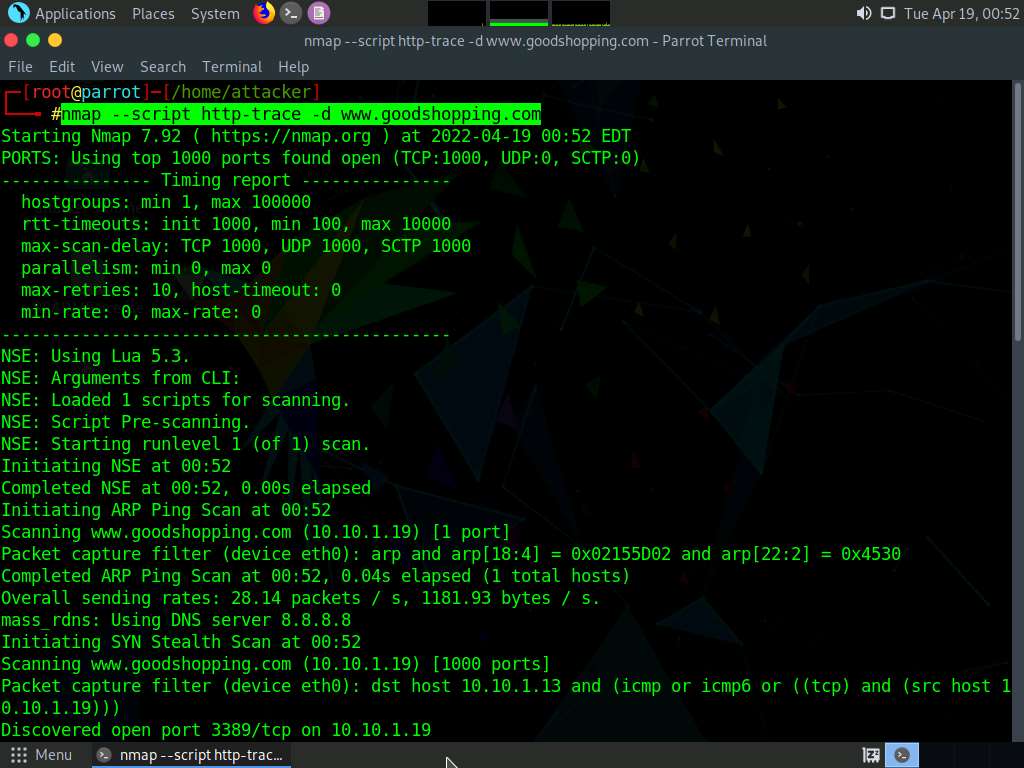
1. This script enumerates and provides you with the output details, as shown in the screenshot.

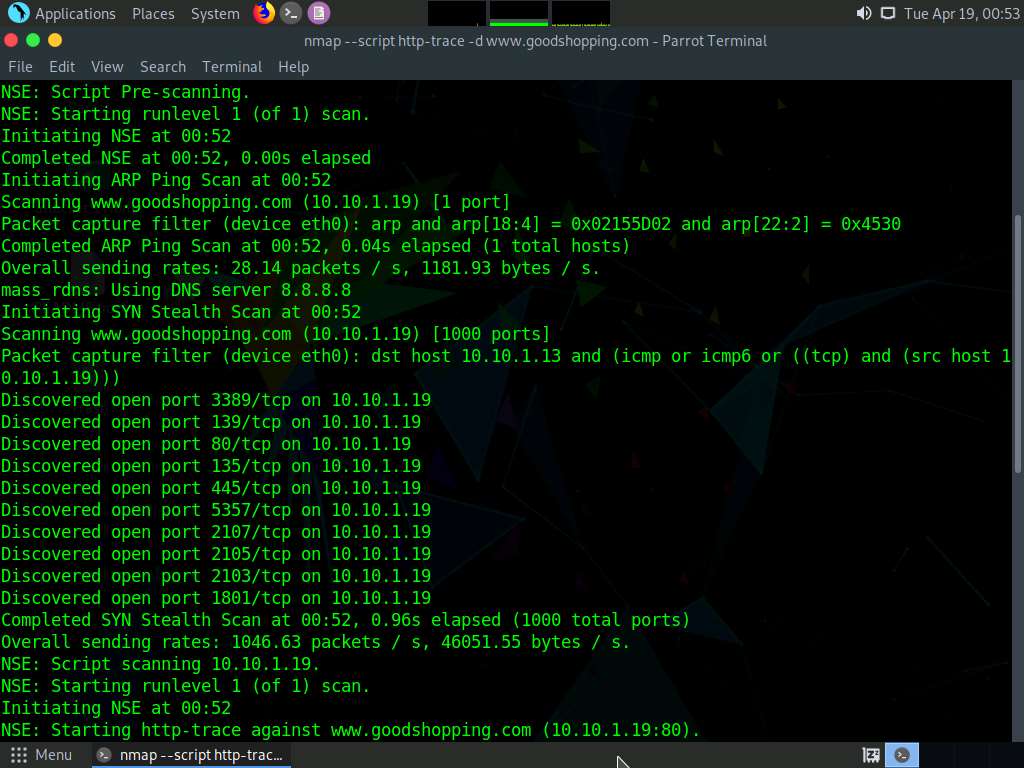


1. The next step is to discover the hostnames that resolve the targeted domain.
2. In the terminal window, type **nmap --script hostmap-bfk -script-args hostmap-bfk.prefix=hostmap- www.goodshopping.com** and press **Enter**.



1. Perform an HTTP trace on the targeted domain. In the terminal window, type **nmap --script http-trace -d www.goodshopping.com** and press **Enter**.
2. 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.







1. 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**.
2. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.
3. This command will probe the target host with malicious payloads and detect the changes in the response code.



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

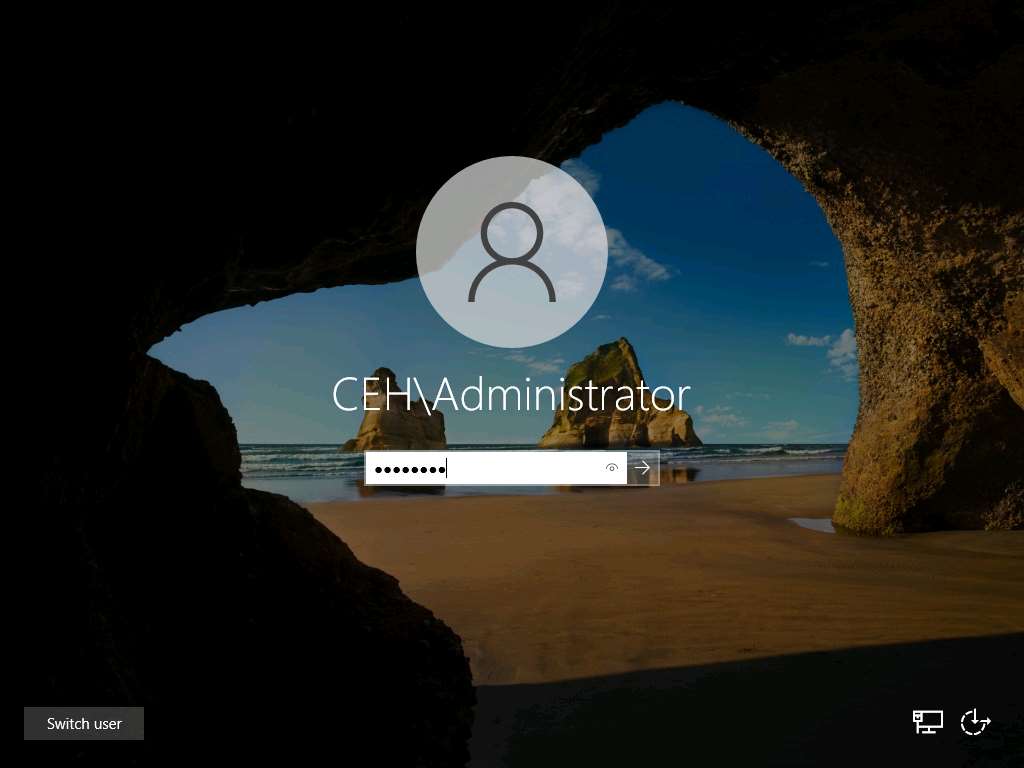
Task 6: Uniscan Web Server Fingerprinting in Parrot Security

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.

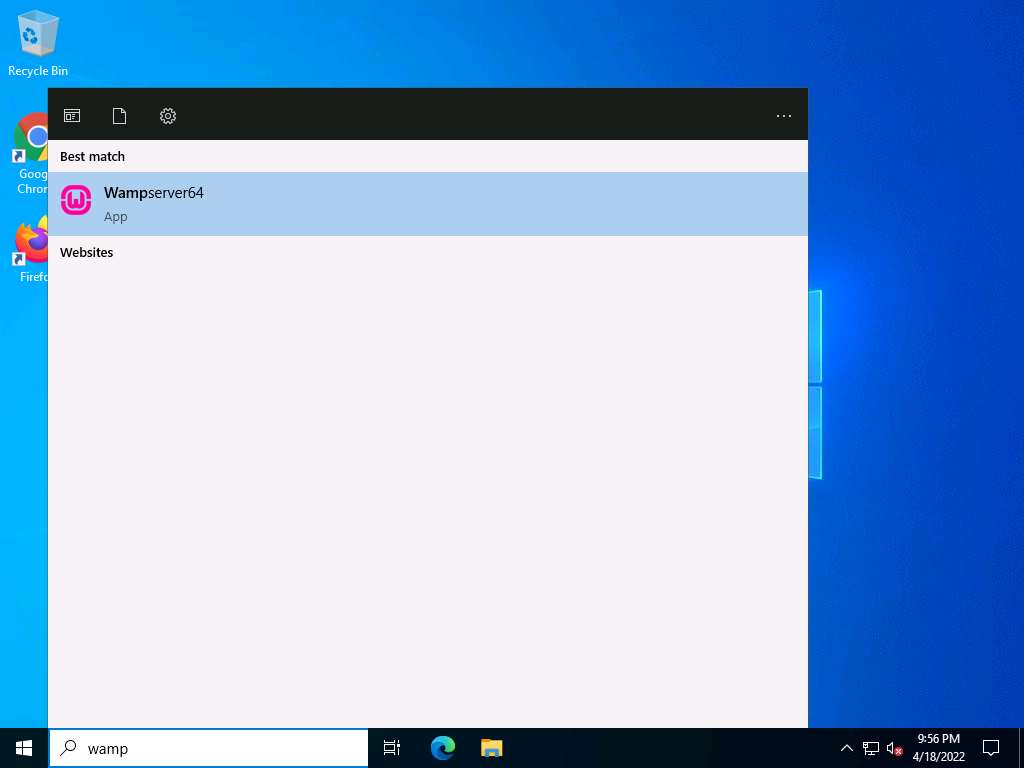
1. Click **CEHv12 Windows Server 2022** to switch to the **Windows Server 2022** machine.



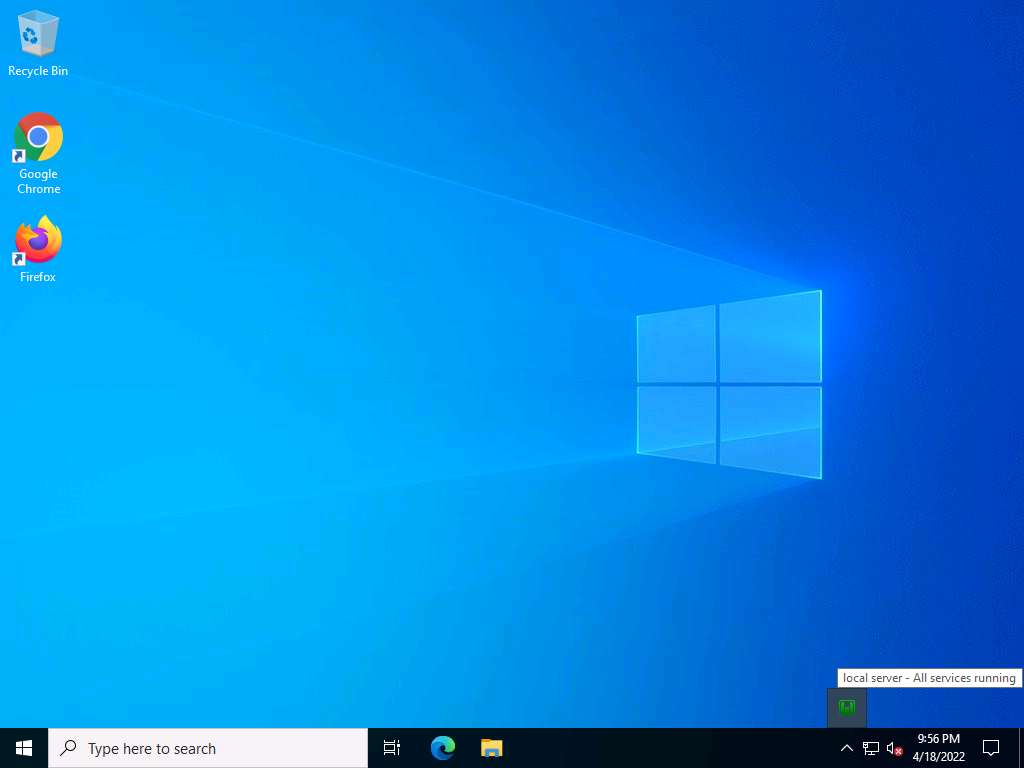
1. Click **Ctrl+Alt+Del** to activate the machine. By default, **CEH\Administrator** user profile is selected, type **Pa$$w0rd** in the Password field and press **Enter** to login.



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

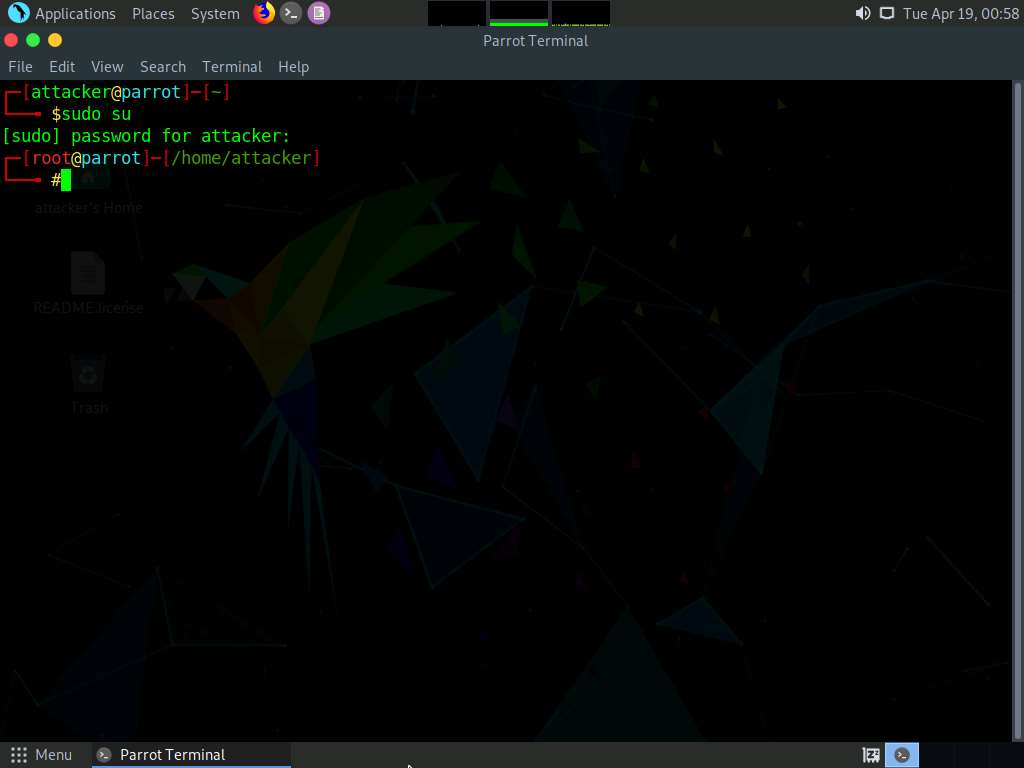


1. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2022** machine running.

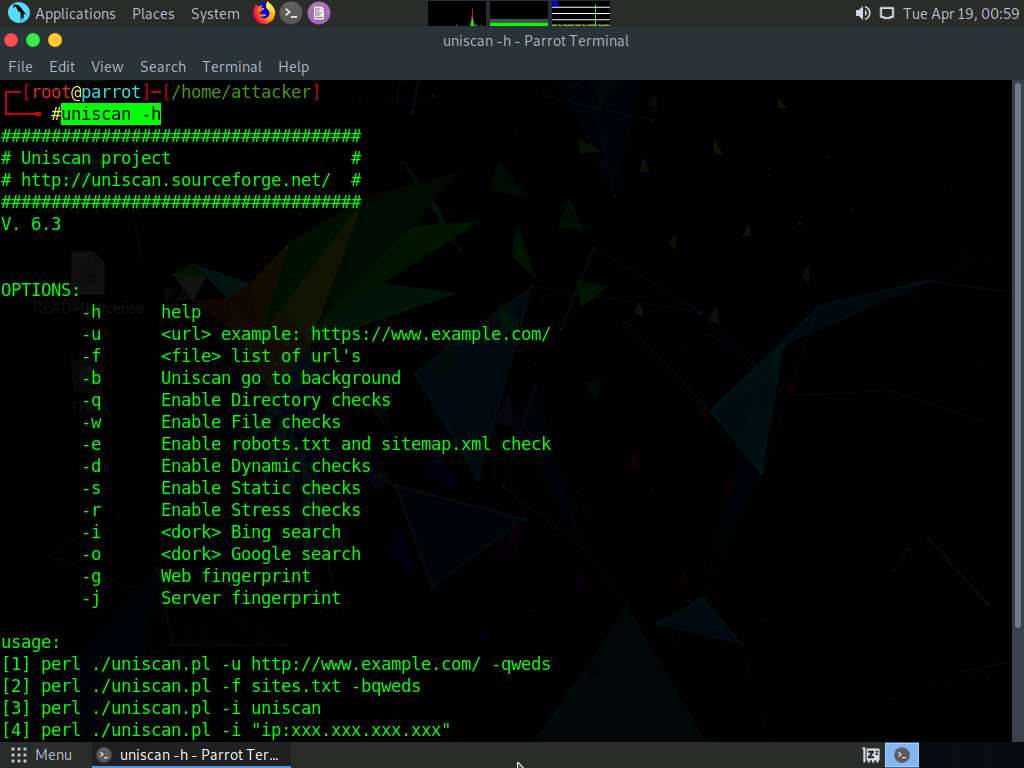


1. Leave the **Windows Server 2022** machine running and switch to the **Parrot Security** machine.
2. Now, click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
3. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

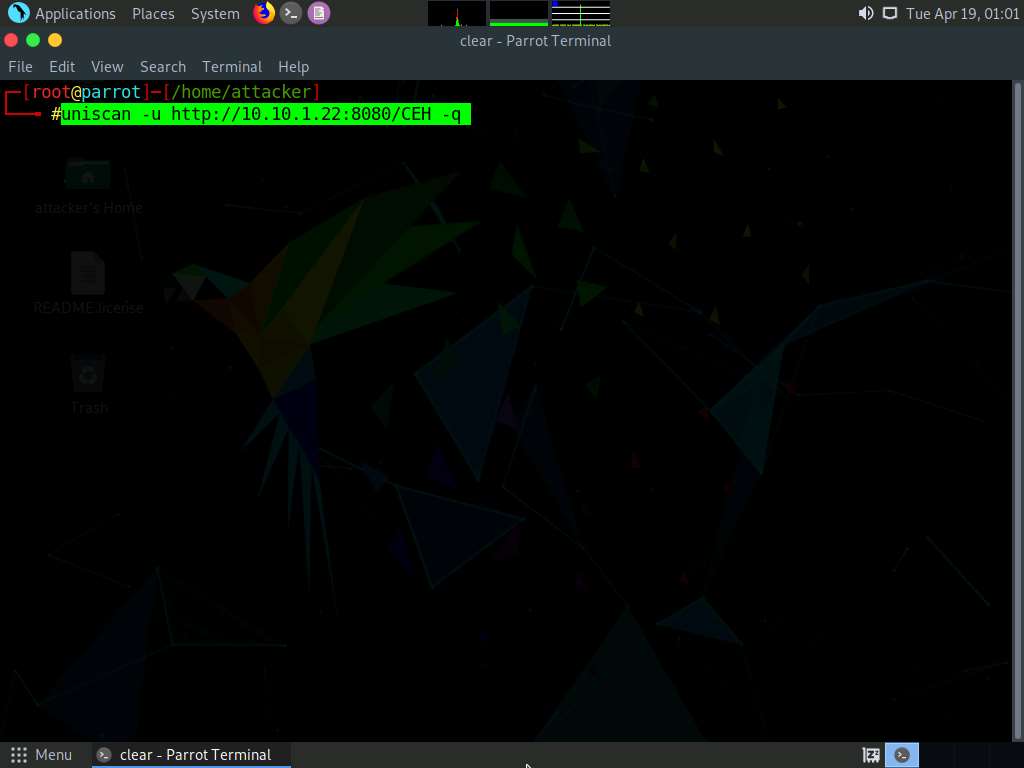
Note: The password that you type will not be visible.



1. In the terminal window, type **uniscan -h** and hit **Enter** to display the uniscan help options.
2. The help menu appears, as shown in the screenshot. First, use the **-q** command to search for the directories of the web server.

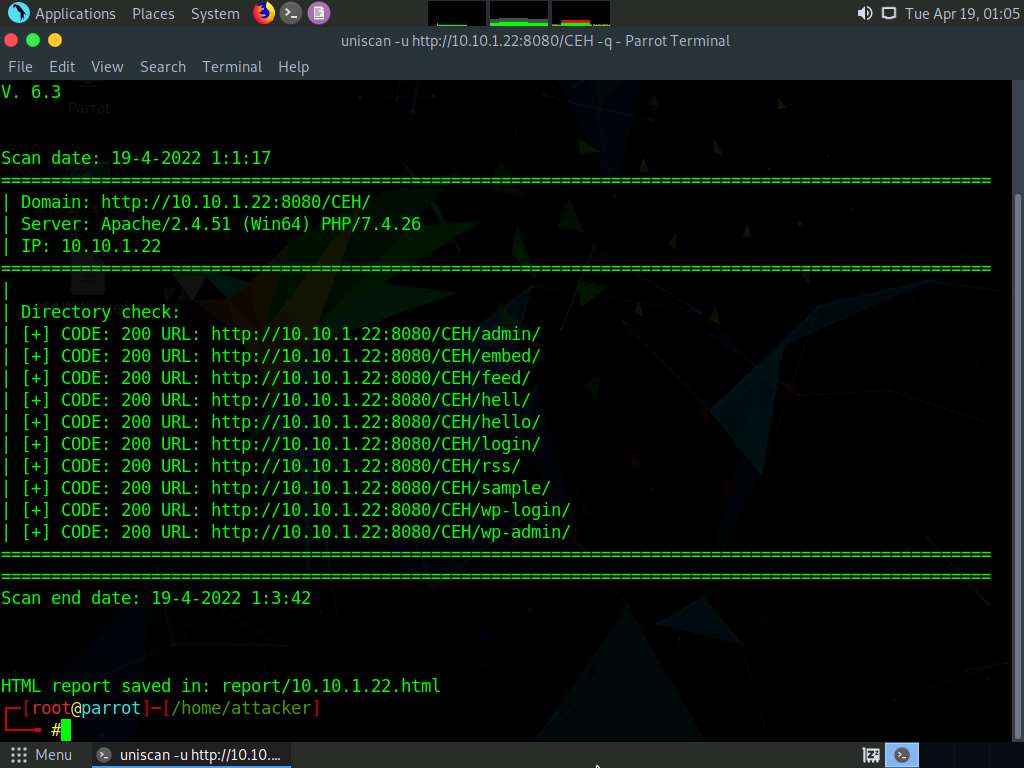


1. In the terminal window, type **uniscan -u http://10.10.1.22:8080/CEH -q** and hit **Enter** to start scanning for directories.
2. Here, **10.10.1.22** is the IP address of the **Windows Server 2022** machine. This may vary in your lab environment.
3. In the above command, the **-u** switch is used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

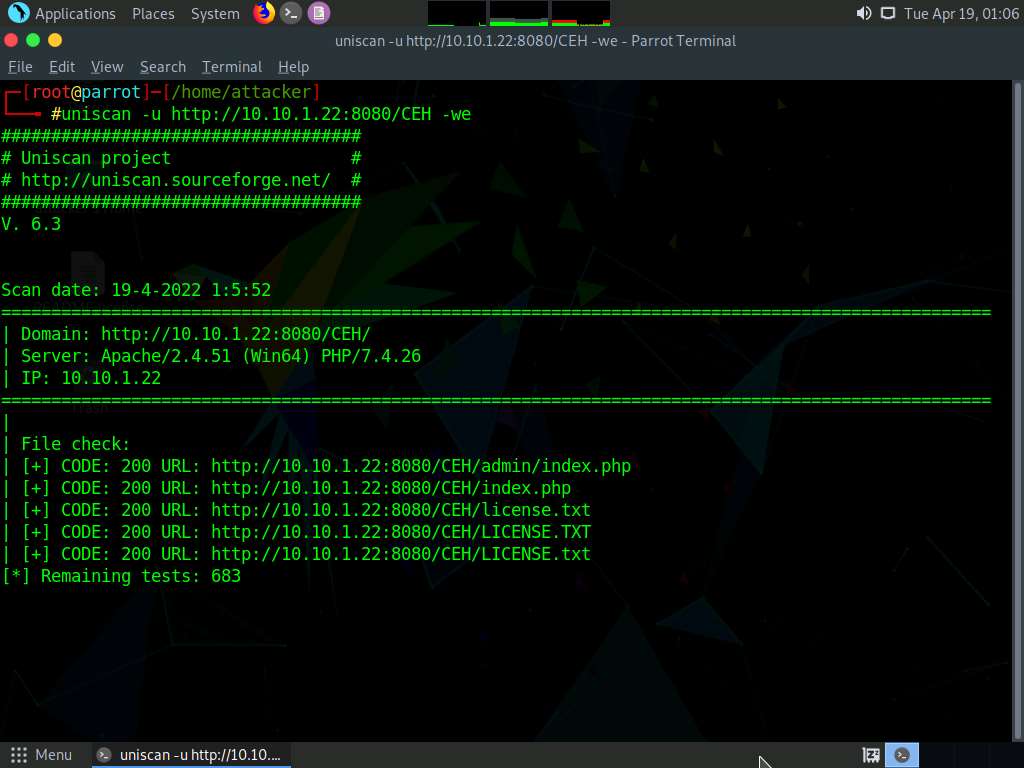


1. Uniscan starts performing different tests on the webserver and discovering **web directories**, as shown in the screenshot.

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

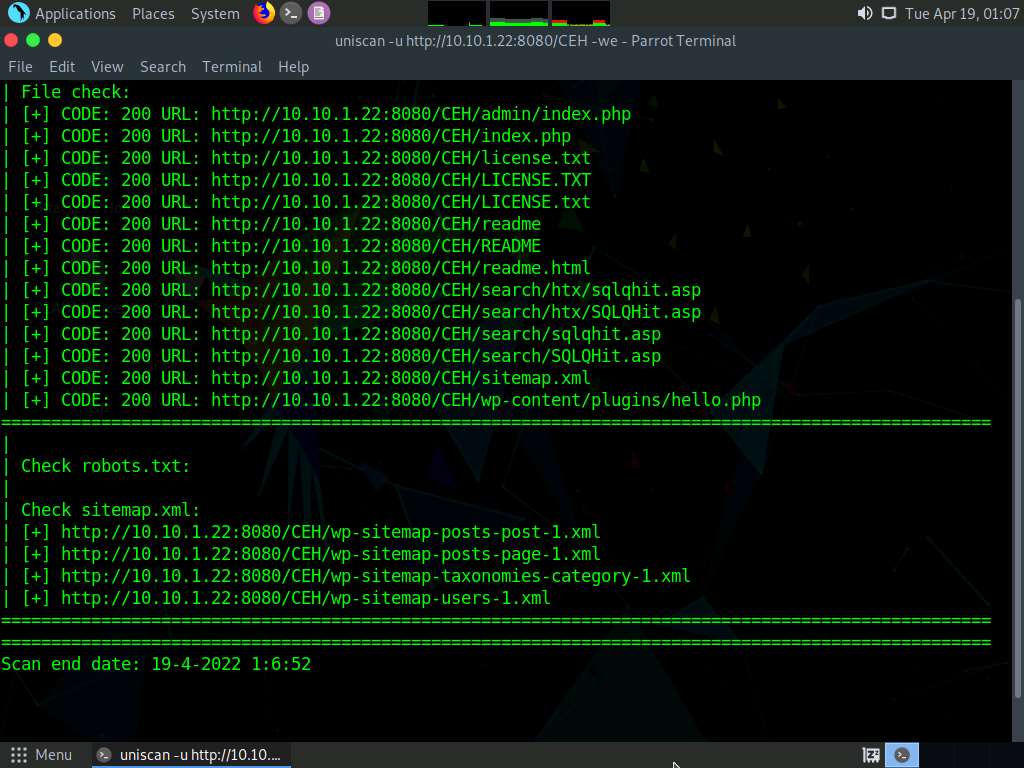


1. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (**robots.txt** and **sitemap.xml** file). In the **terminal** window, type **uniscan -u http://10.10.1.22:8080/CEH -we** and hit **Enter** to start the scan.

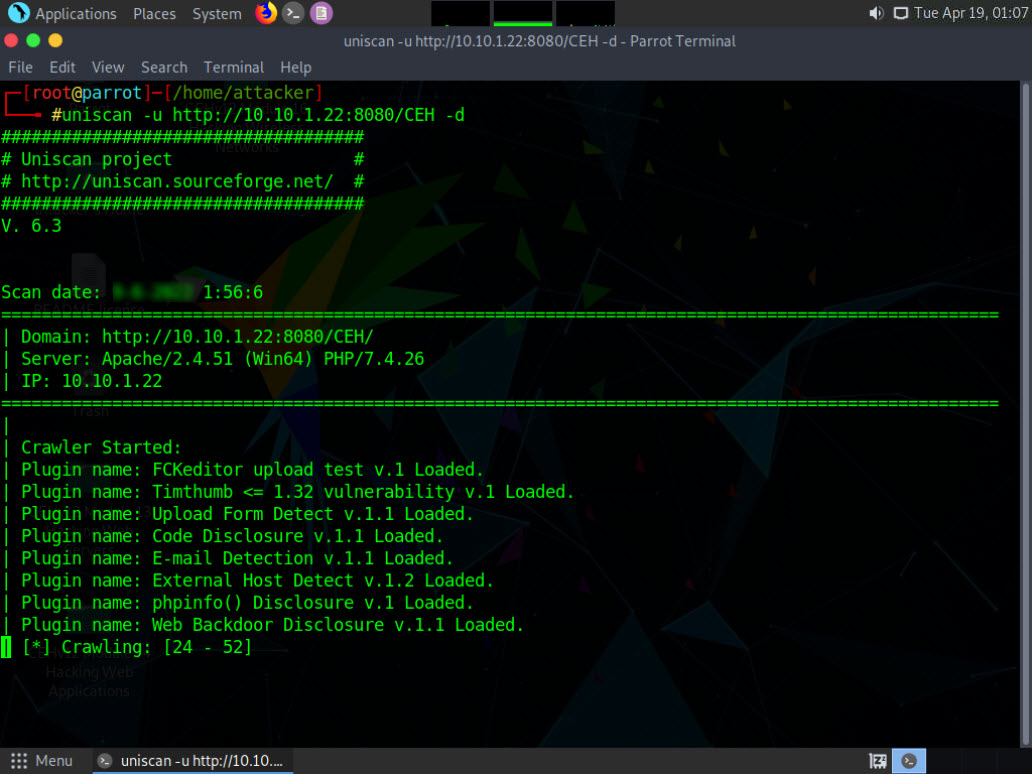


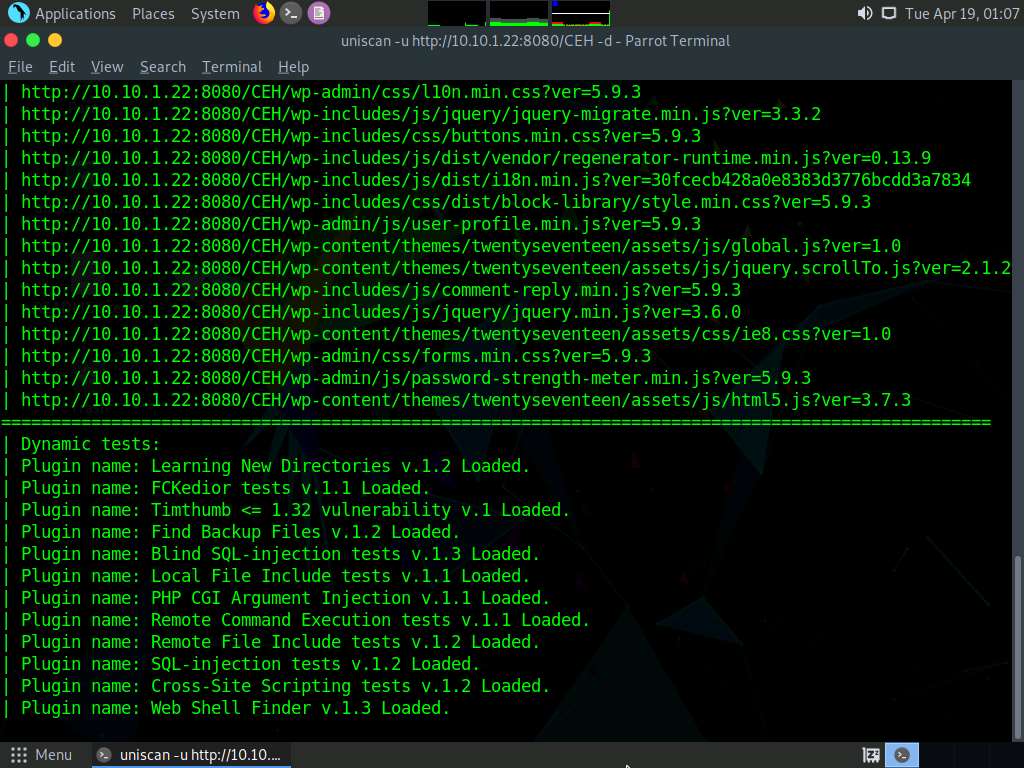
1. Uniscan starts the file check and displays the results, as shown in the screenshot.

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



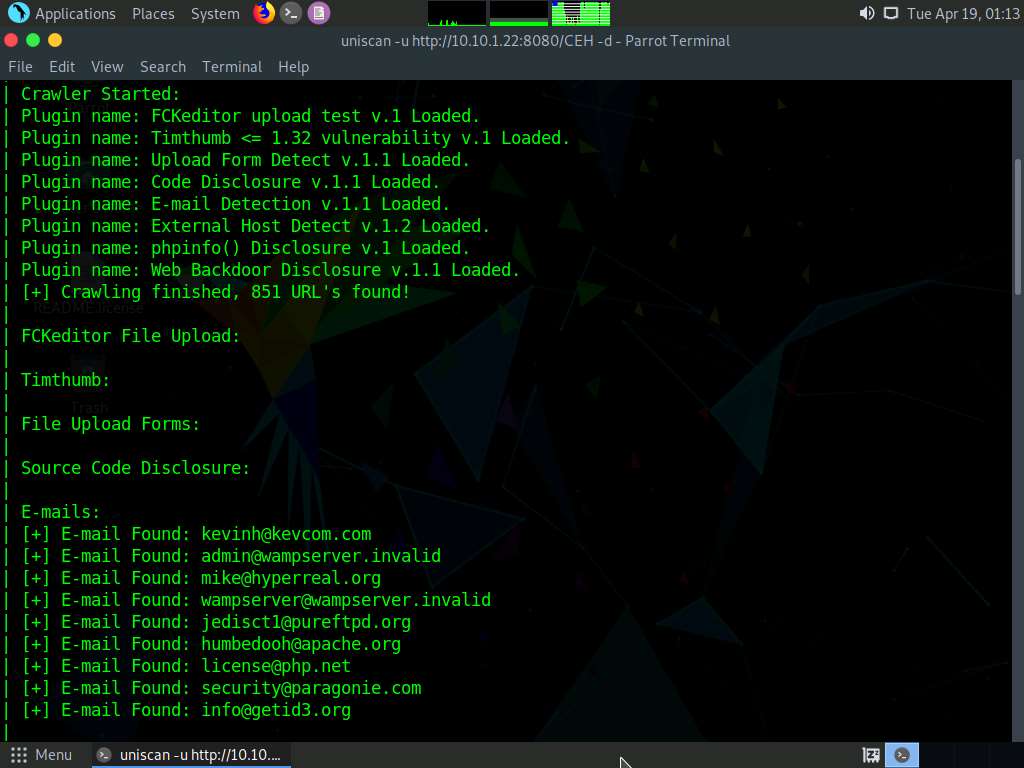
1. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.1.22:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

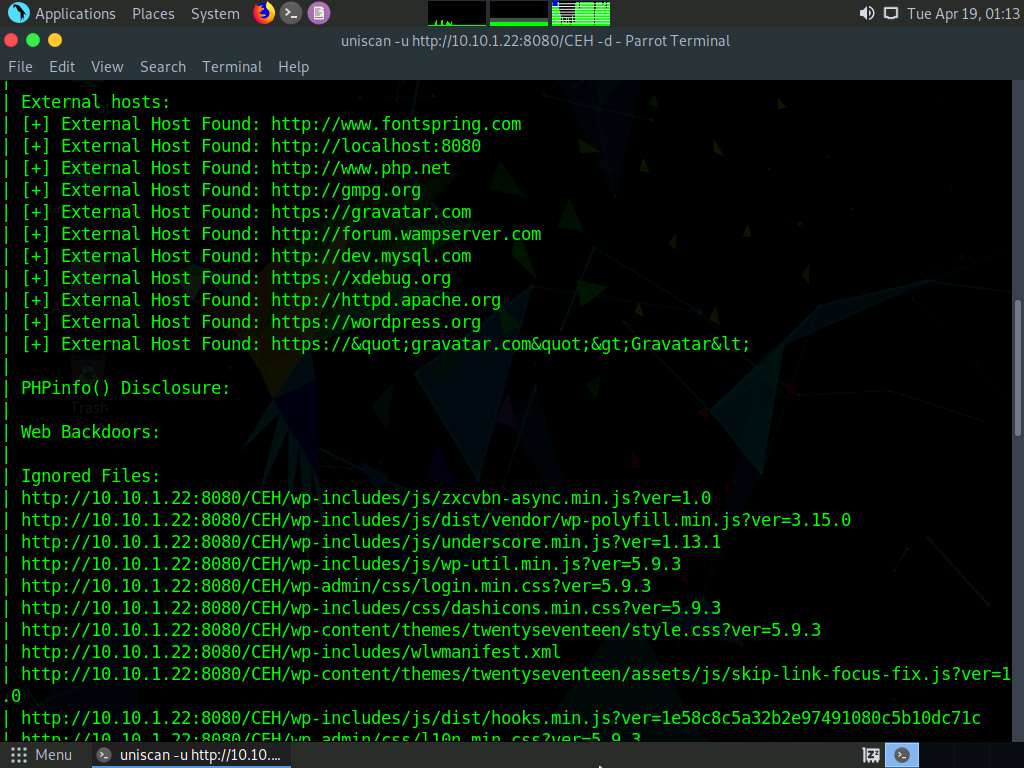


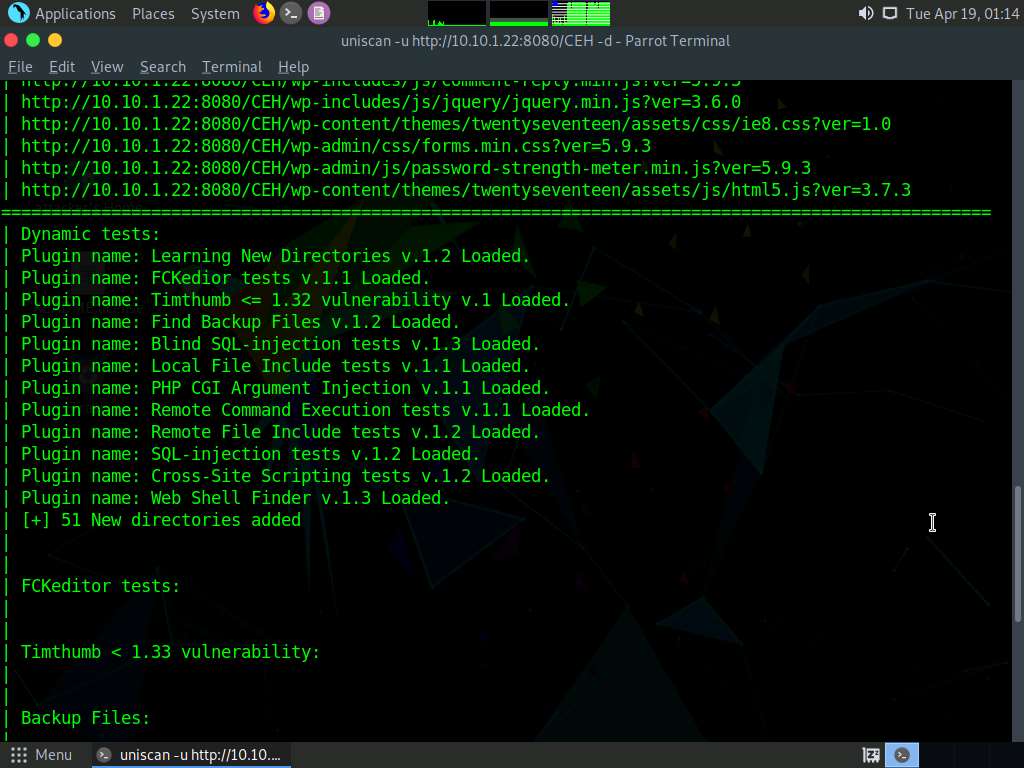


1. Uniscan starts performing dynamic tests, obtaining more information about email-IDs, Source code disclosures, and external hosts, web backdoors, dynamic tests.

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



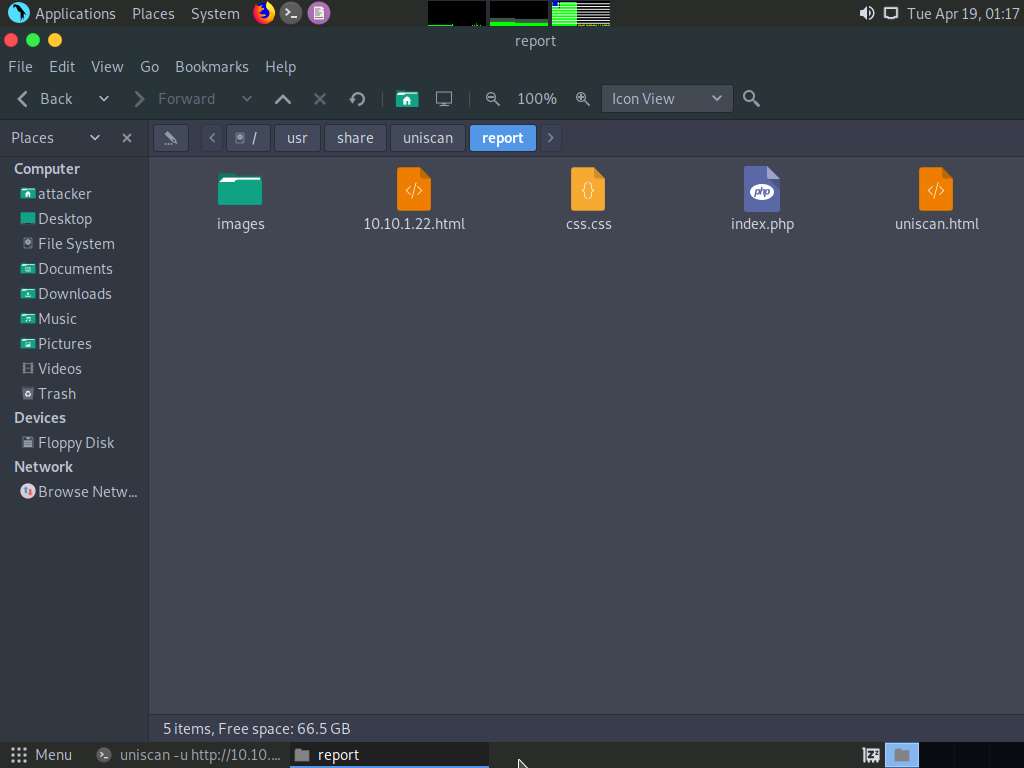




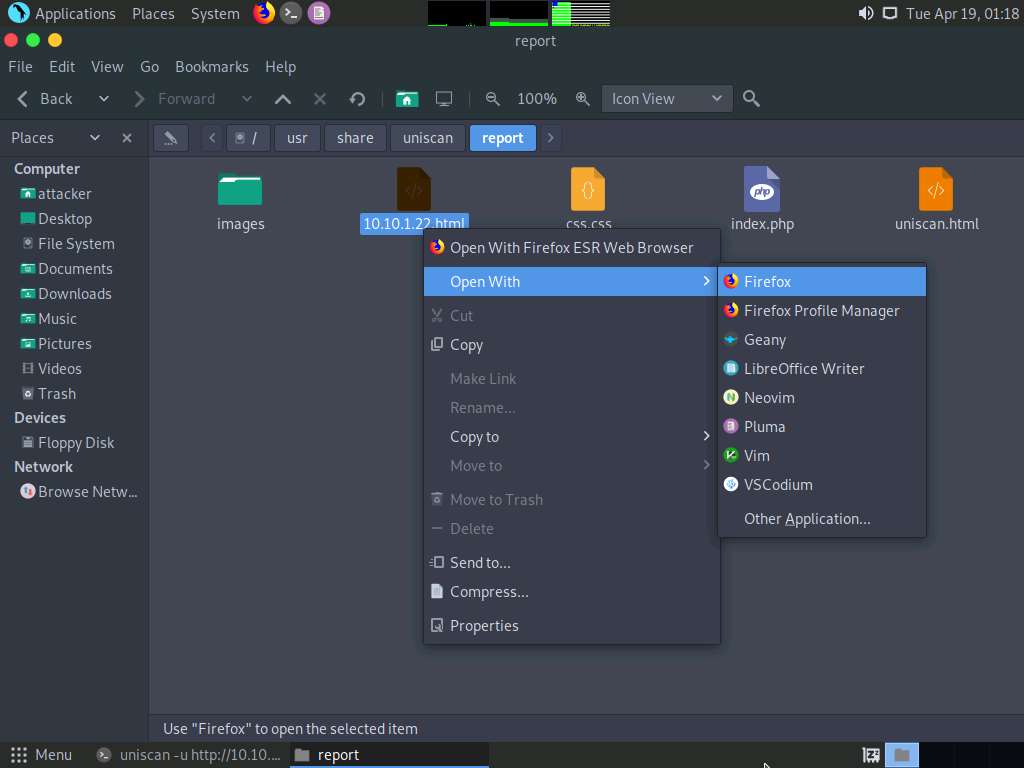
1. Click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options.



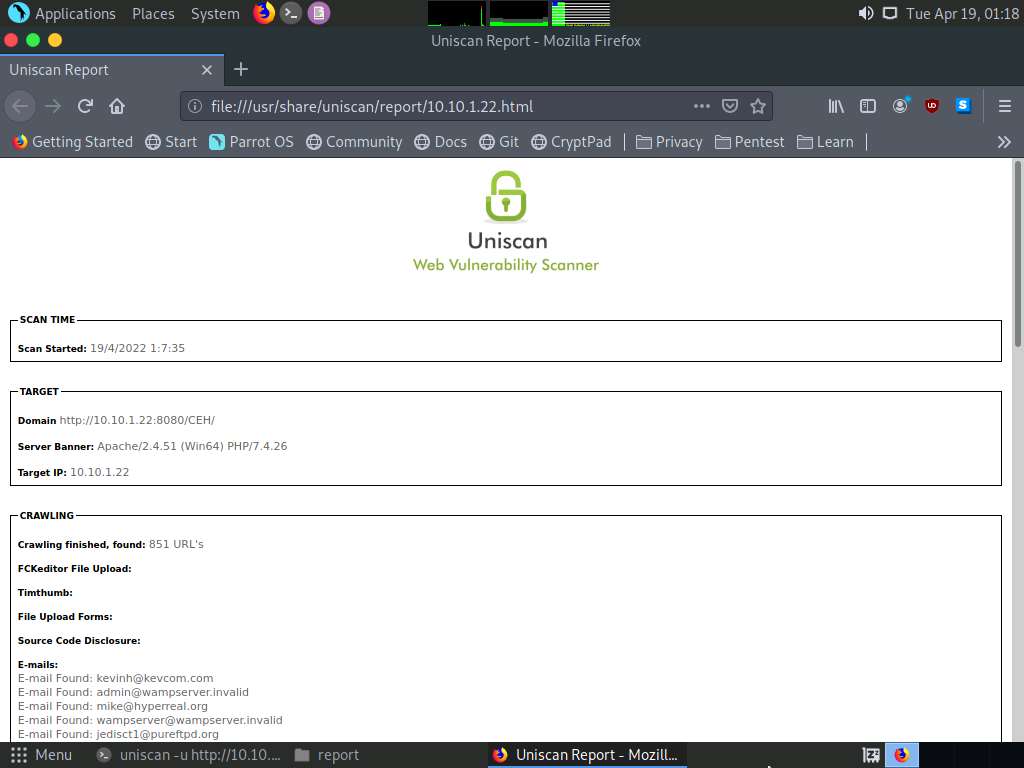
1. Click **File System** from the left-pane and click **usr** --> **share** --> **uniscan** --> **report**.



1. 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.



1. 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.



1. This concludes the demonstration of how to gather information about the target web server using Uniscan.
2. Close all terminal windows on the **Parrot Security** machine.

Lab 2: Perform a Web Server Attack

**Lab Scenario**

After gathering required information about the target web server, the next task for an ethical hacker or pen tester is to attack the web server in order to test the target network’s web server security infrastructure. This requires knowledge of how to perform web server attacks.

Attackers perform web server attacks with certain goals in mind. These goals may be technical or non-technical. For example, attackers may breach the security of the web server to steal sensitive information for financial gain, or merely for curiosity’s sake. The attacker tries all possible techniques to extract the necessary passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, and rainbow attacks. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus and THC-Hydra, to crack web passwords.

An ethical hacker or pen tester must test the company’s web server against various attacks and other vulnerabilities. It is important to find various ways to extend the security test by analyzing web servers and employing multiple testing techniques. This will help to predict the effectiveness of additional security measures for strengthening and protecting web servers of the organization.

**Lab Objectives**

* Crack FTP credentials using a Dictionary Attack

**Overview of Web Server Attack**

Attackers can cause various kinds of damage to an organization by attacking a web server, including:

* Compromise of a user account
* Secondary attacks from the website and website defacement
* Root access to other applications or servers
* Data tampering and data theft
* Damage to the company’s reputation

Task 1: Crack FTP Credentials using a Dictionary Attack

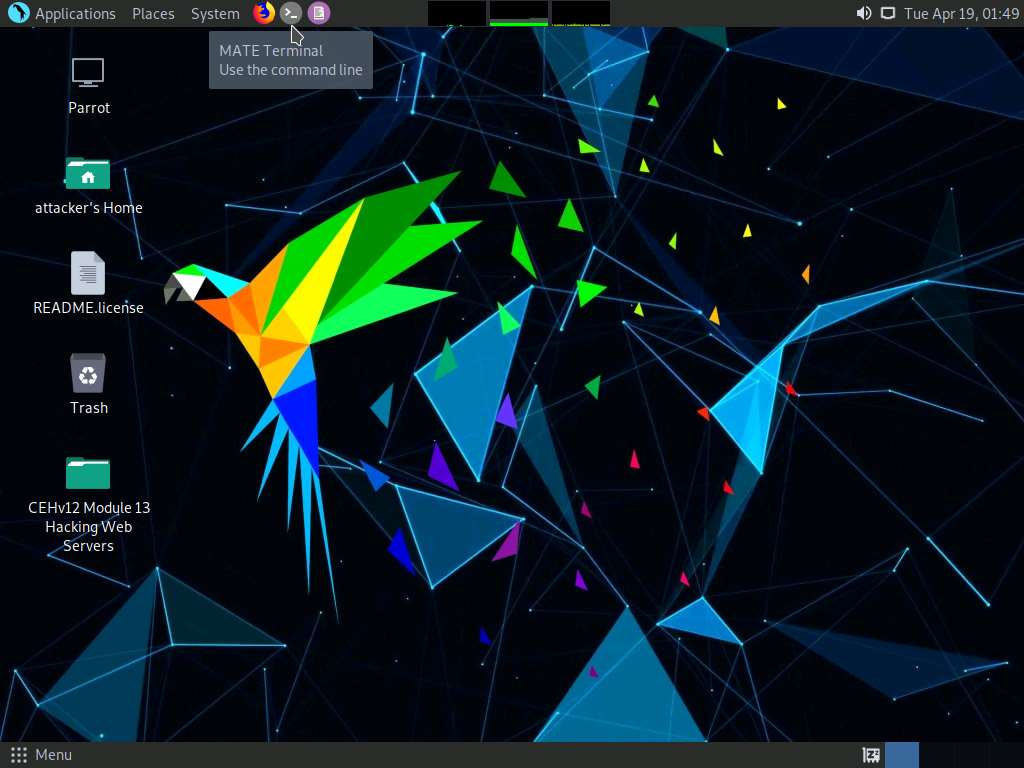
A dictionary or wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. An attacker may either manually crack a password by guessing it or use automated tools and techniques such as the dictionary method. Most password cracking techniques are successful, because of weak or easily guessable passwords.

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

1. Click **CEHv12 Parrot Security** to switch to the **Parrot Security** machine.

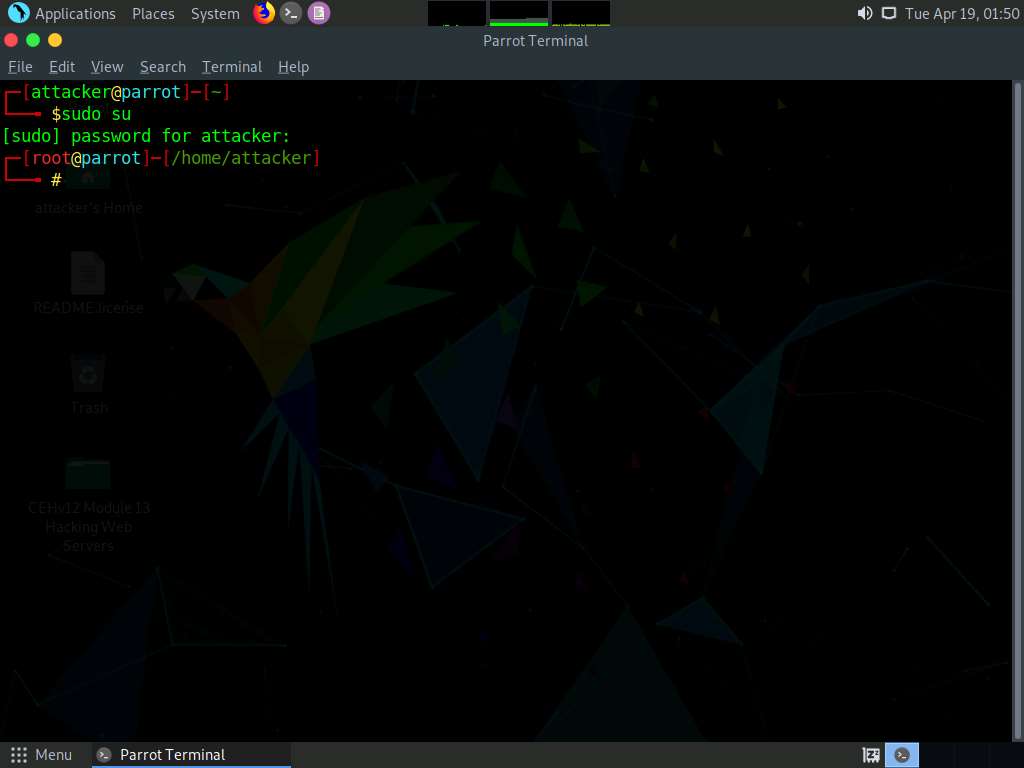
Note: Here, we will use a sample password file (**Passwords.txt**) containing a list of passwords to crack the FTP credentials on the target machine.

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



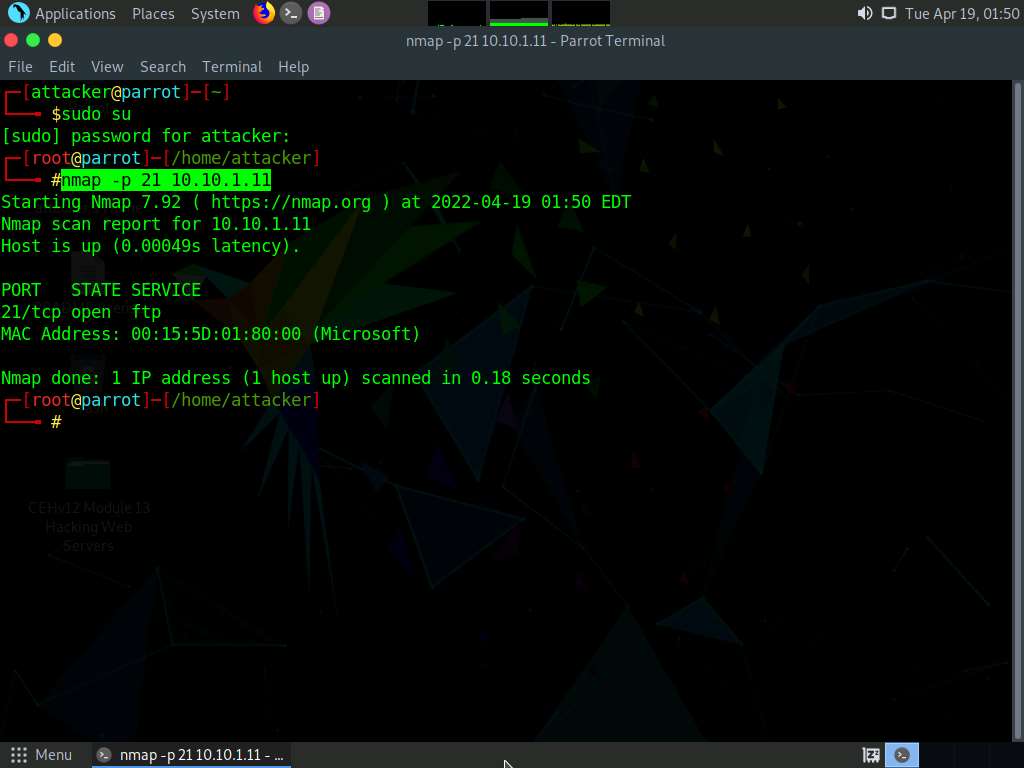
1. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
2. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

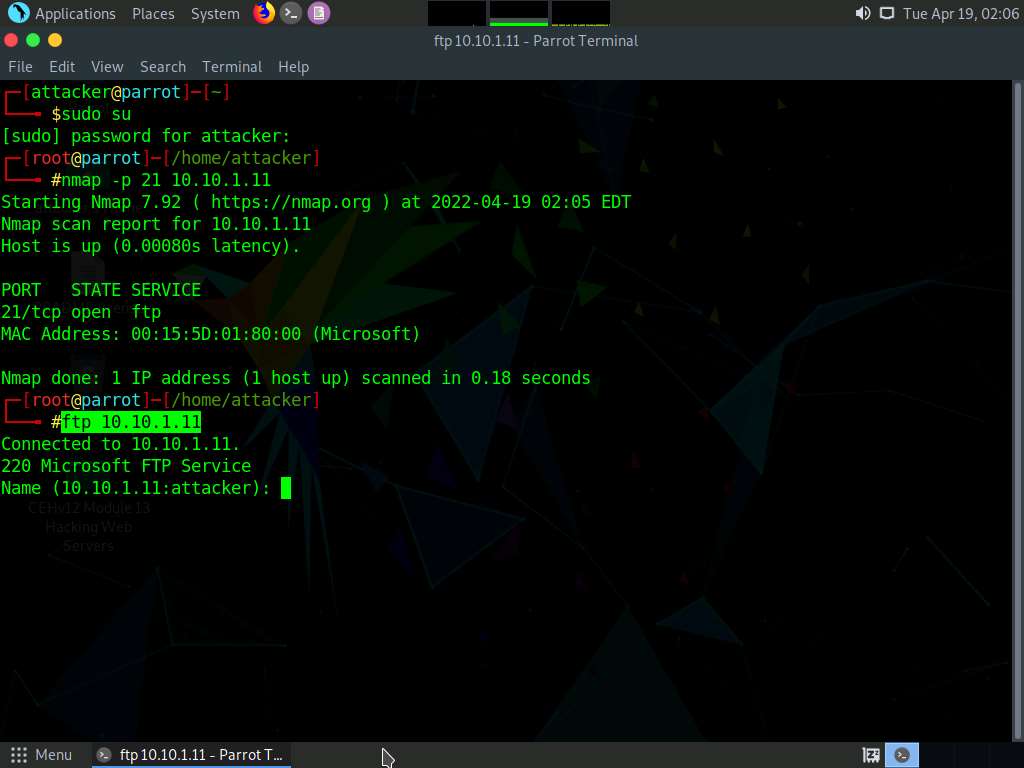


1. In the terminal window, type **nmap -p 21 [IP Address of Windows 11]**, and press **Enter**.

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



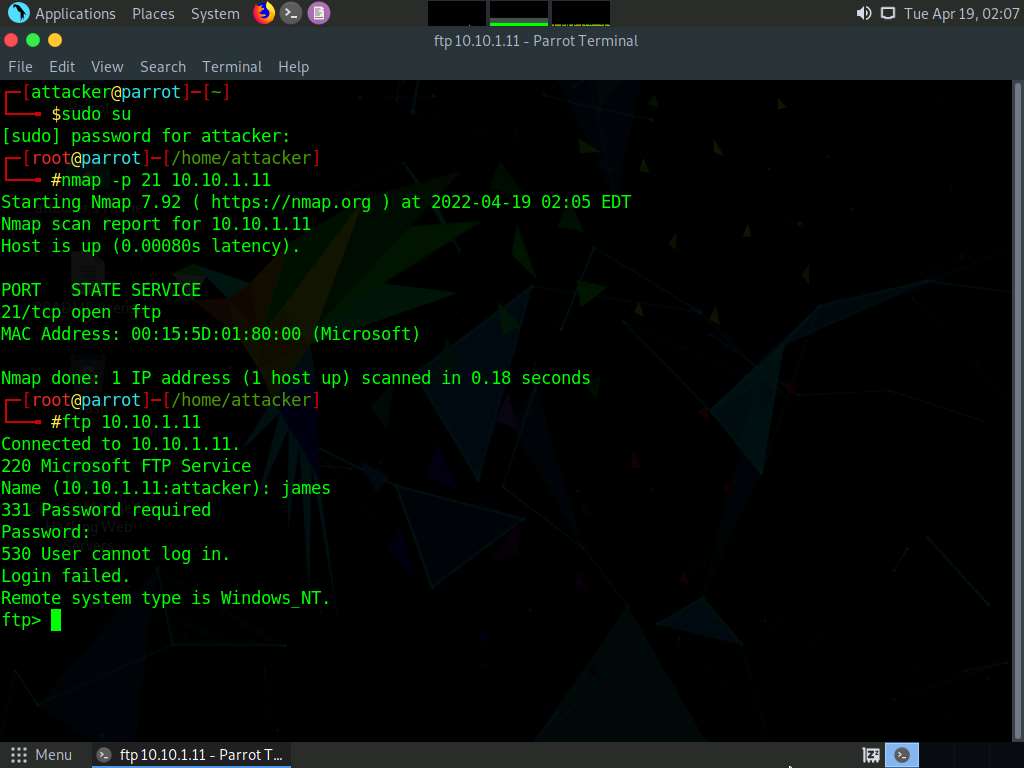
1. Observe that **port 21** is open in **Windows 11**.
2. Check if an FTP server is hosted on the **Windows 11** machine.
3. Type **ftp [IP Address of Windows 11]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the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



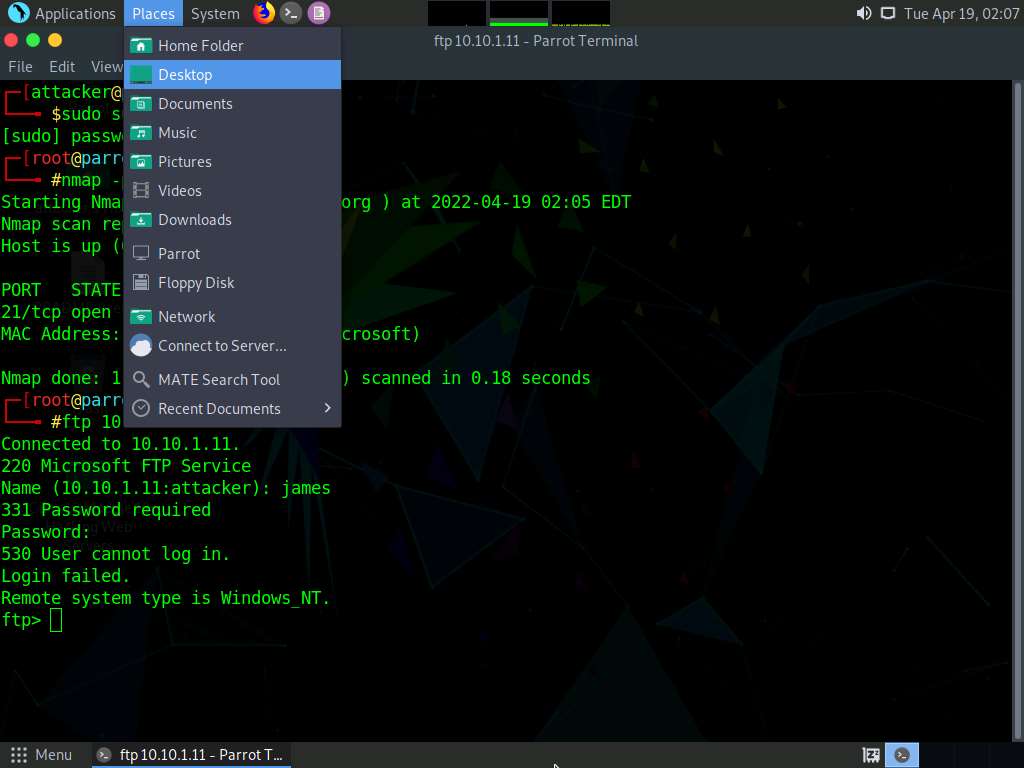
1. Try entering random usernames and passwords in an attempt to gain FTP access.

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

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



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



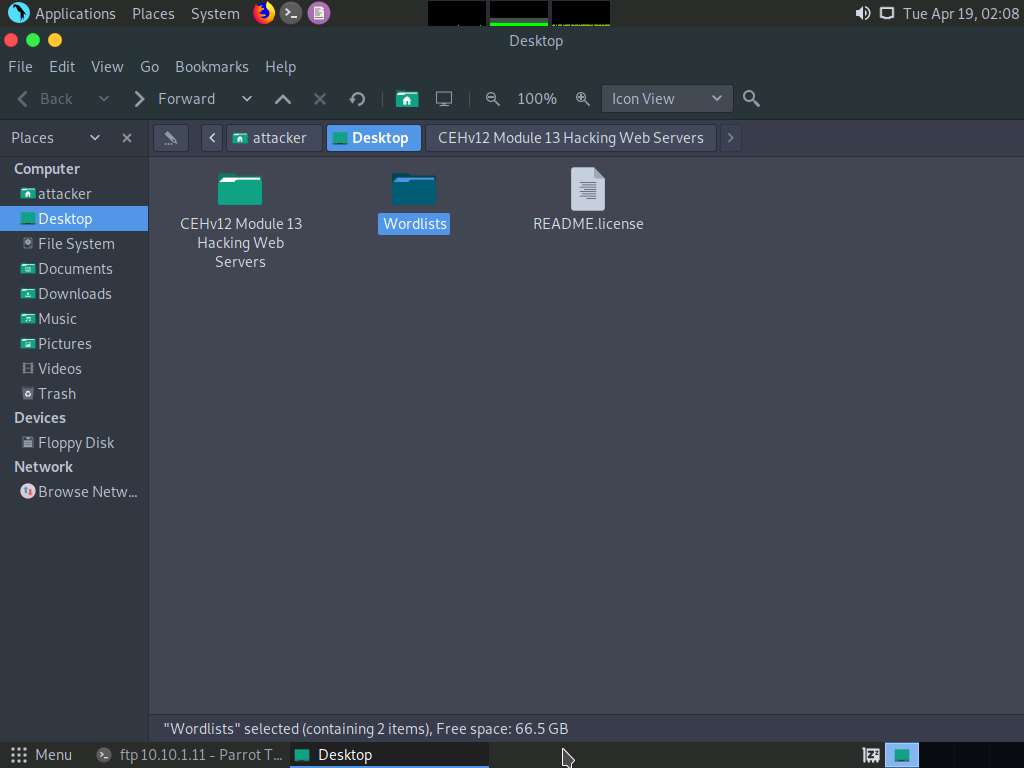
1. Navigate to **CEHv12 Module 13 Hacking Web Servers** folder and copy **Wordlists** folder.

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

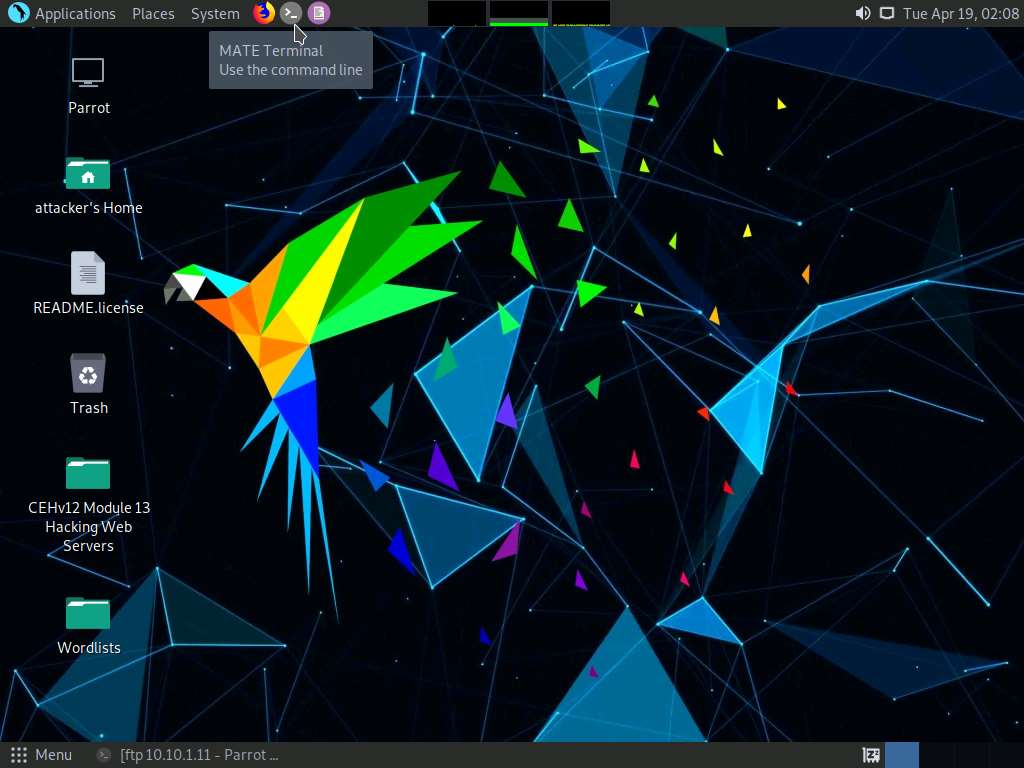


1. Paste the copied folder (**Wordlists**) on the **Desktop**. Close the window

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



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

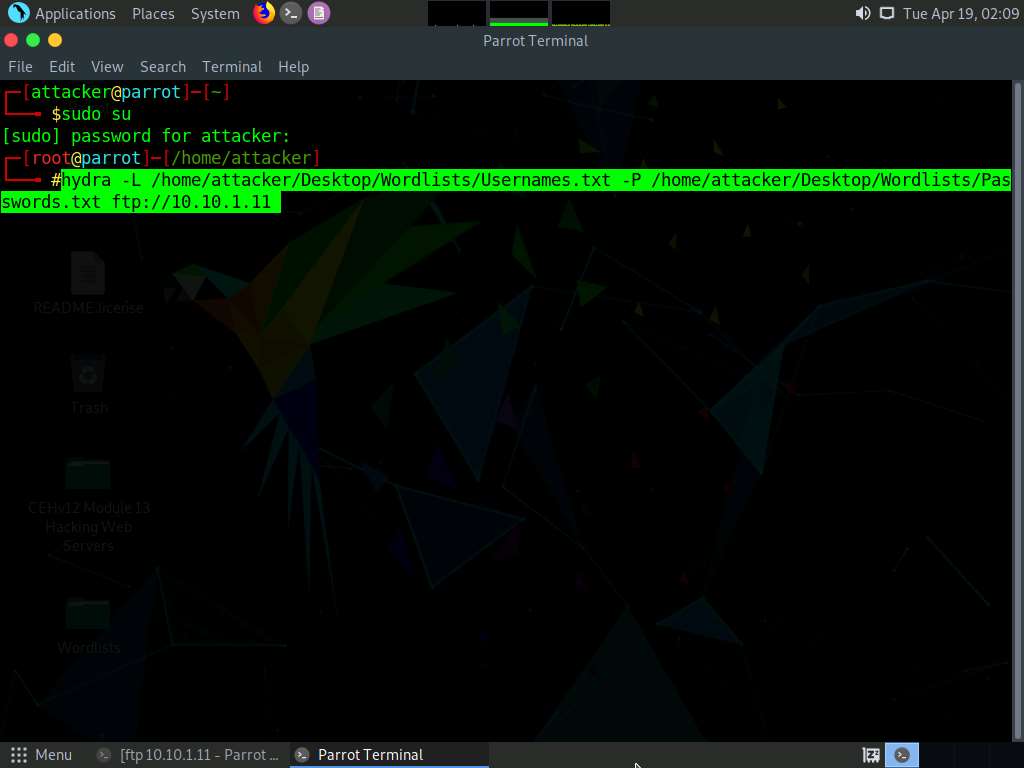


1. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
2. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

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

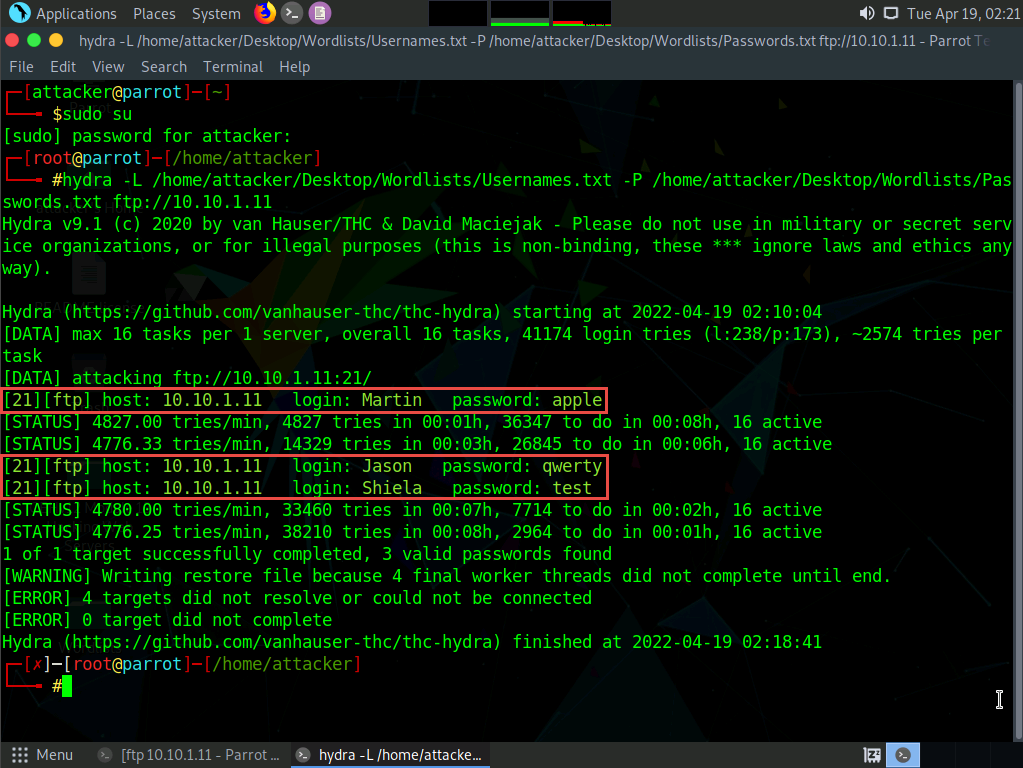
Note: The IP address of **Windows 11** in this lab exercise is **10.10.1.11**. This IP address might vary in your lab environment.



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

Note: This might take some time to complete.

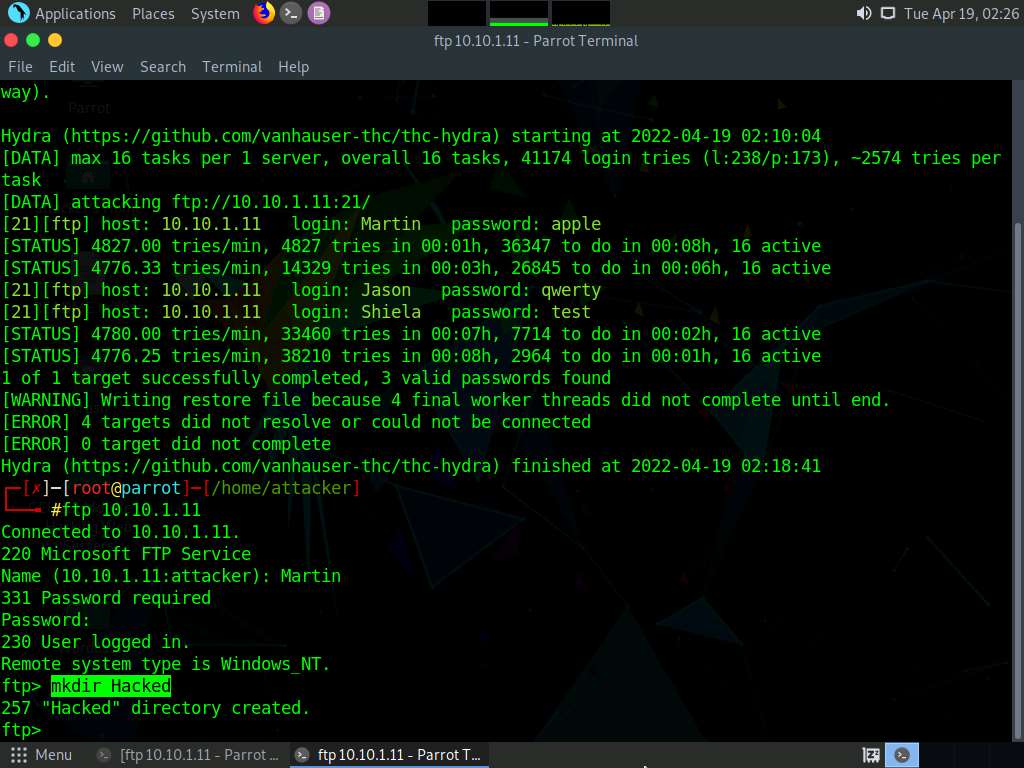
1. On completion of the password cracking, the **cracked credentials** appear, as shown in the screenshot.



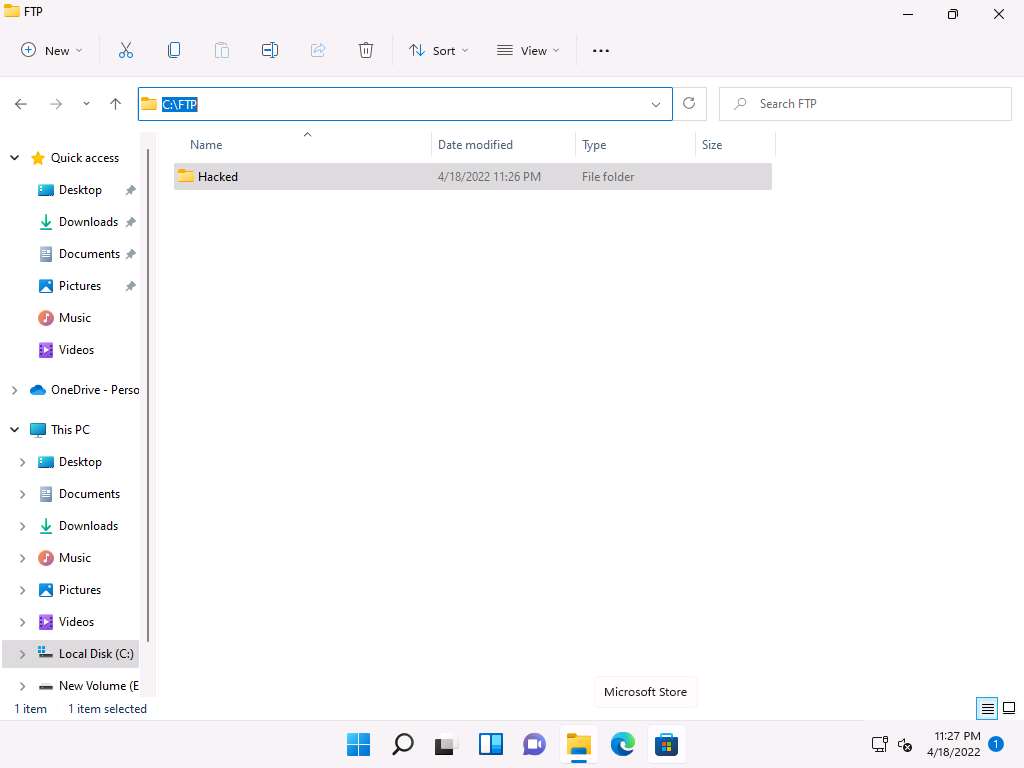
1. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin’s credentials to gain access to the server.
2. In the terminal window, type **ftp [IP Address of Windows 11]**, and press **Enter**.
3. Enter Martin’s user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.
4. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.



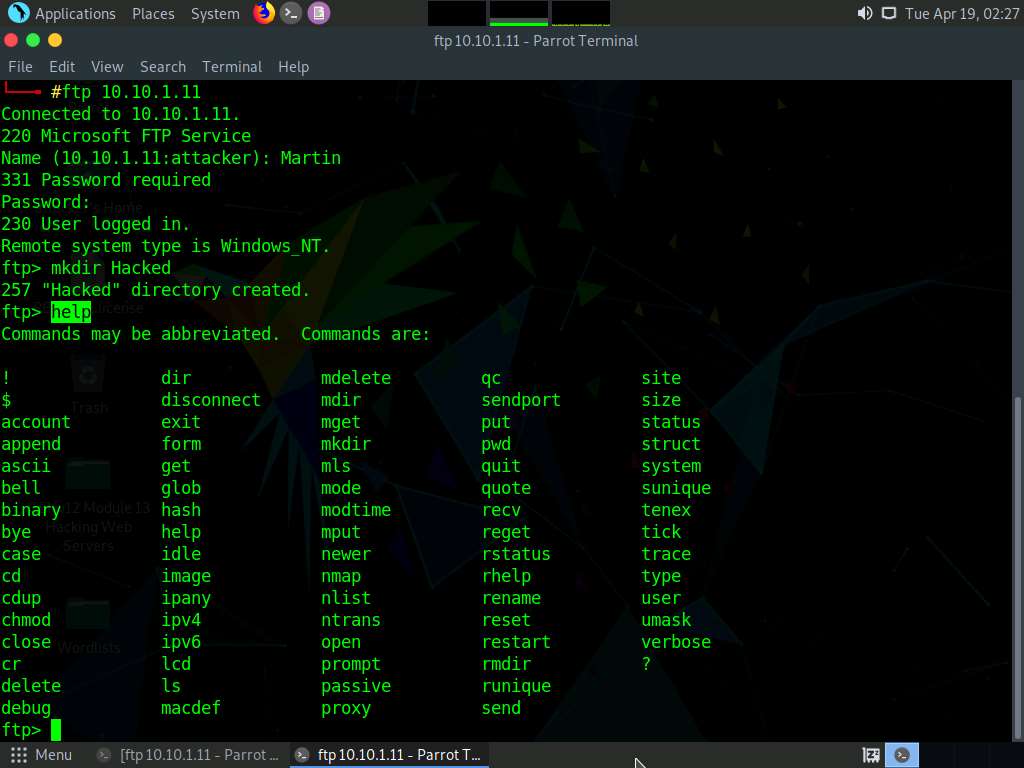
1. Now you can remotely access the FTP server hosted on the **Windows 11** machine.
2. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 11** machine through the ftp terminal.



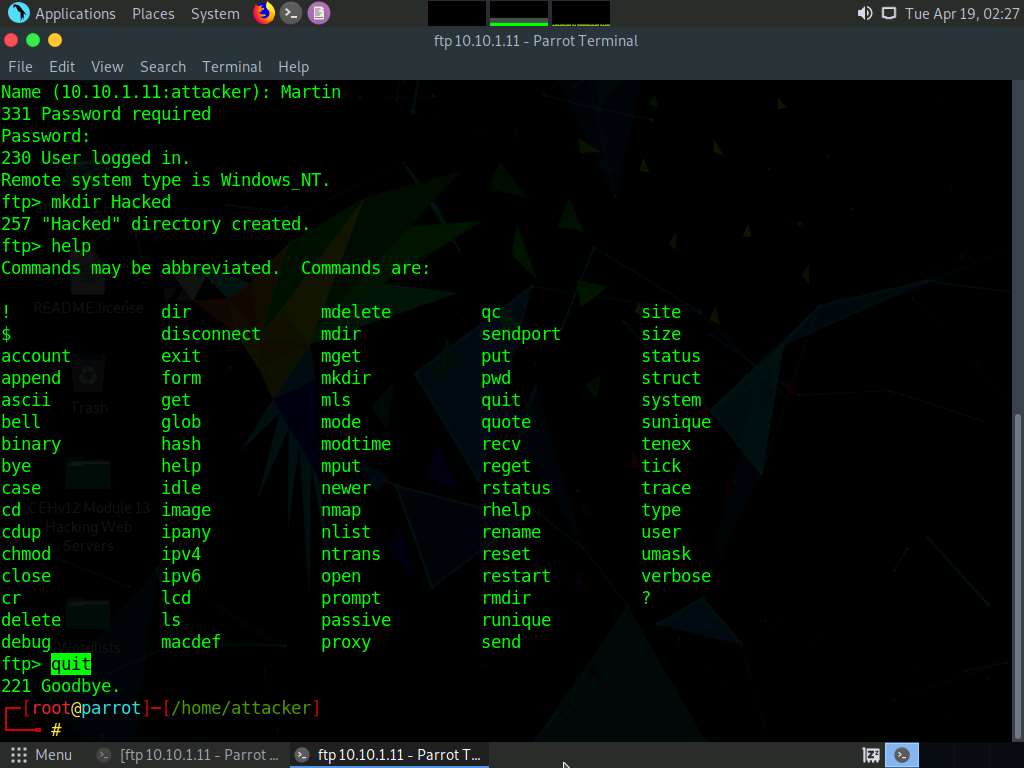
1. Click **CEHv12 Windows 11** to switch to the **Windows 11** machine and navigate to **C:\FTP**.
2. View the directory named **Hacked**, as shown in the screenshot:



1. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.
2. Click **CEHv12 Parrot Security** to switch back to the **Parrot Security** machine.
3. Enter **help** to view all other commands that you can use through the FTP terminal.



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



1. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.
2. Close all open windows on both the **Parrot Security** and **Windows 11** machines.