Hacking Web Servers

Module 13

Hacking Web Servers

A web server is a computer system that stores, processes, and delivers web pages to global clients via HTTP protocol. A web server attack typically involves preplanned activities, called an attack methodology, which the attacker implements to reach their goal of breaching the target web server's security.

Lab Scenario

ICON KEY

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

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

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

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

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

Lab Objectives

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

- Footprint a web server using various information-gathering tools and inbuilt commands

- Enumerate web server information
- Crack remote passwords

Lab Environment

To carry out this lab, you need:

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

Lab Duration

Time: 75 Minutes

Overview of Web Server

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

Lab Tasks

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

Lab No.	Lab Exercise Name	Core*	Self-study**	iLabs ***
1	Footprint the Web Server	√	√	√
	1.1 Information Gathering using Ghost Eye	√		√
	1.2 Perform Web Server Reconnaissance using Skipfish		√	√
	1.3 Footprint a Web Server using the httprecon Tool		√	√
	1.4 Footprint a Web Server using ID Serve		√	√

	1.5 Footprint a Web Server using Netcat and Telnet	√		√
	1.6 Enumerate Web Server Information using Nmap Scripting Engine (NSE)	√		√
	1.7 Uniscan Web Server Fingerprinting in Parrot Security		√	√
2	Perform a Web Server Attack	√		√
	2.1 Crack FTP Credentials using a Dictionary Attack	√		√

Remark

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

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

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

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

Lab Analysis

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

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

Lab 1

Footprint the Web Server

Footprinting the web server refers to the process of gathering as much information as possible about the target web server by using various tools and techniques.

ICON KEY

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

Lab Scenario

The first step of hacking web servers for a professional ethical hacker or pen tester is to collect as much information as possible about the target web server and analyze the collected information in order to find lapses in its current security mechanisms. The main purpose is to learn about the web server's remote access capabilities, its ports and services, and other aspects of its security.

The information obtained in this step helps in assessing the security posture of the web server. Footprinting may involve searching the Internet, newsgroups, bulletin boards, etc. for gathering information about the target organization's web server. There are also tools such as Whois.net and Whois Lookup that extract information such as the target's domain name, IP address, and autonomous system number.

Web server fingerprinting is an essential task for any penetration tester. Before proceeding to hack or exploit a webserver, the penetration tester must know the type and version of the webserver as most of the attacks and exploits are specific to the type and version of the server being used by the target. These methods help any penetration tester to gain information and analyze their target so that they can perform a thorough test and can deploy appropriate methods to mitigate such attacks on the server.

An ethical hacker or penetration tester must perform footprinting to detect the loopholes in the web server of the target organization. This will help in predicting the effectiveness of additional security measures for strengthening and protecting the web server of the target organization.

The labs in this exercise demonstrate how to footprint a web server using various footprinting tools and techniques.

Lab Objectives

- Information gathering using Ghost Eye
- Perform web server reconnaissance using Skipfish
- Footprint a web server using the httprecon Tool
- Footprint a web server using ID Serve
- Footprint a web server using Netcat and Telnet
- Enumerate web server information using Nmap Scripting Engine (NSE)
- Uniscan web server fingerprinting in Parrot Security

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Windows Server 2016 virtual machine
- Windows Server 2019 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection
- Administrator privileges to run the tools
- httprecon located to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**
- ID Serve located to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve**
- You can also download the latest version of the above-mentioned tools from their official websites. If you decide to download the latest version, the screenshots shown in this lab manual might differ from the image that you see on your screen.

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

Lab Duration

Time: 65 Minutes

Overview of Web Server Footprinting

By performing web server footprinting, it is possible to gather valuable system-level data such as account details, OS, software versions, server names, and database schema details. Use Telnet utility to footprint a web server and gather information such as server name, server type, OSes, and applications running. Use footprinting tools such as Netcraft, ID Serve, and httprecon to perform web server footprinting. Web server footprinting tools such as Netcraft, ID Serve, and httprecon can extract information from the target server. Let us look at the features and the types of information these tools can collect from the target server.

Lab Tasks

TASK 1 — Information Gathering using Ghost Eye

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

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

Figure 1.1.1: Parrot Security Login

Note:

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

3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

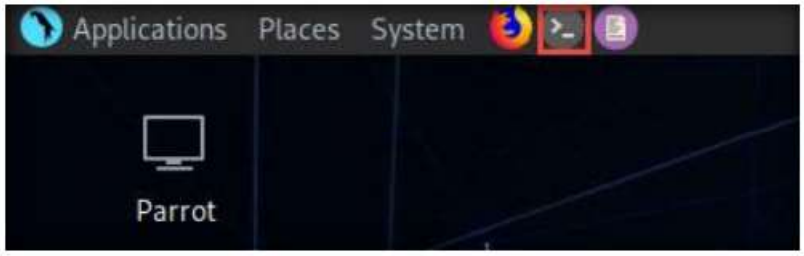


Figure 1.1.2: Launching the MATE Terminal

Ghost Eye gathers information such as Whois lookup, DNS lookup, EtherApe, Nmap port scan, HTTP header grabber, Clickjacking test, Robots.txt scanner, Link grabber, IP location finder, and traceroute.

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

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

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

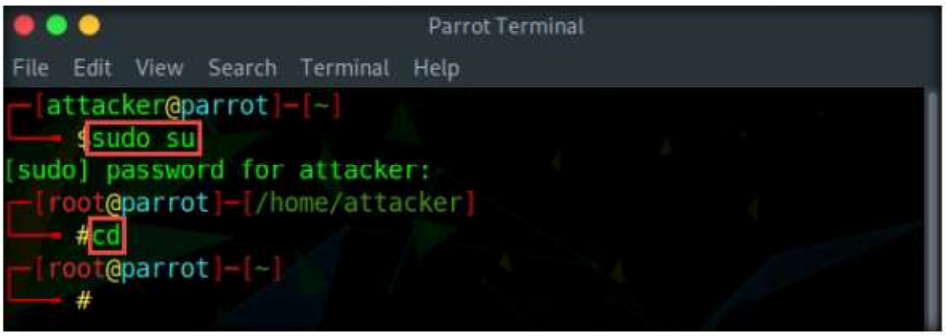


Figure 1.1.3: Running the programs as a root user

TASK 1.1

Install Ghost Eye

7. Now, install Ghost Eye. To do this, in the terminal window, type **git clone https://github.com/BullsEye0/ghost_eye.git** and press **Enter**.
8. This will install Ghost Eye in your virtual machine, as shown in the screenshot.

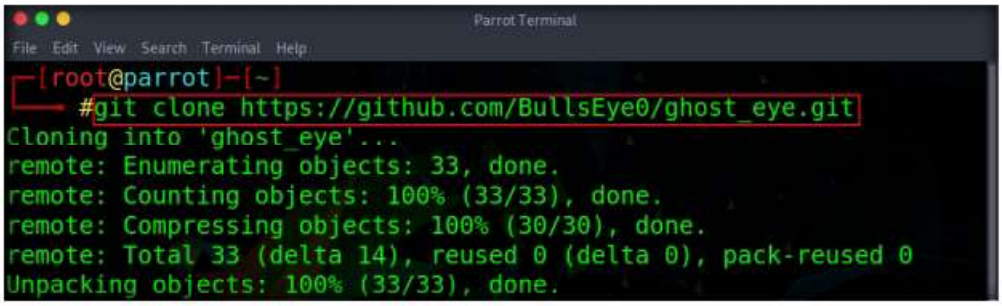


Figure 1.1.4: Cloning Ghost Eye

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

- Open a windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
- The security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
- The **Windows shares on 10.10.10.10** window appears; navigate to the location **CEH-Tools/CEHv11 Module 13 Hacking Web Servers/GitHub Tools/** and copy the **ghost_eye** folder.
- Paste the copied **ghost_eye** folder on the location **/home/attacker/**.
- In the terminal window, type **mv /home/attacker/ghost_eye /root/**.

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

Figure 1.1.5: Ghost Eye Directory

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

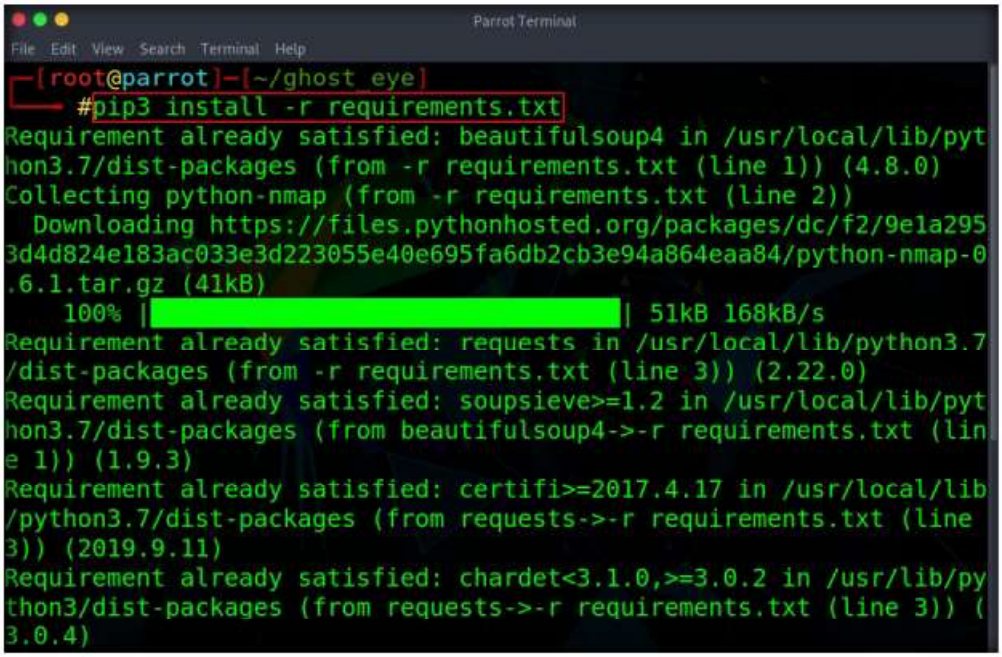


Figure 1.1.6: Installing Ghost Eye requirements

TASK 1.2

Launch Ghost Eye

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

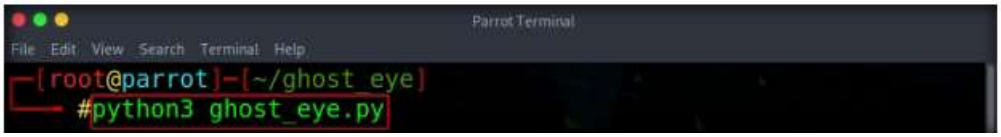


Figure 1.1.7: Launching Ghost Eye

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

TASK 1.3

Perform Whois Lookup

13. Let us perform a Whois Lookup. Type **1** for the **Enter your choice**: option and press **Enter**.

14. Type **certifiedhacker.com** in the **Enter Domain or IP Address**: field and press **Enter**.

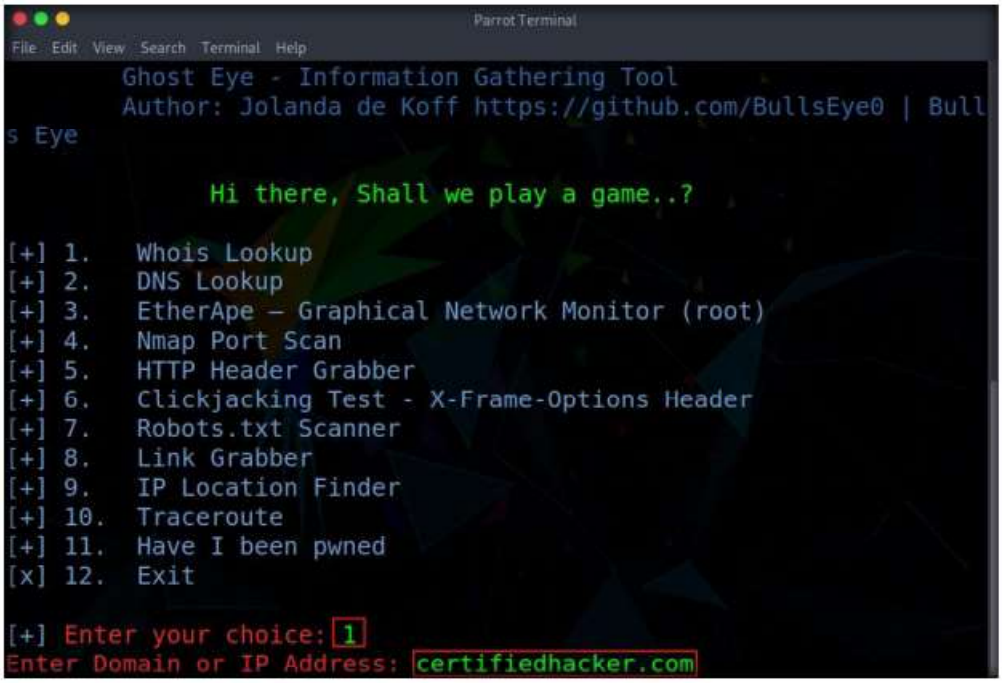


Figure 1.1.8: Performing Whois Lookup

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

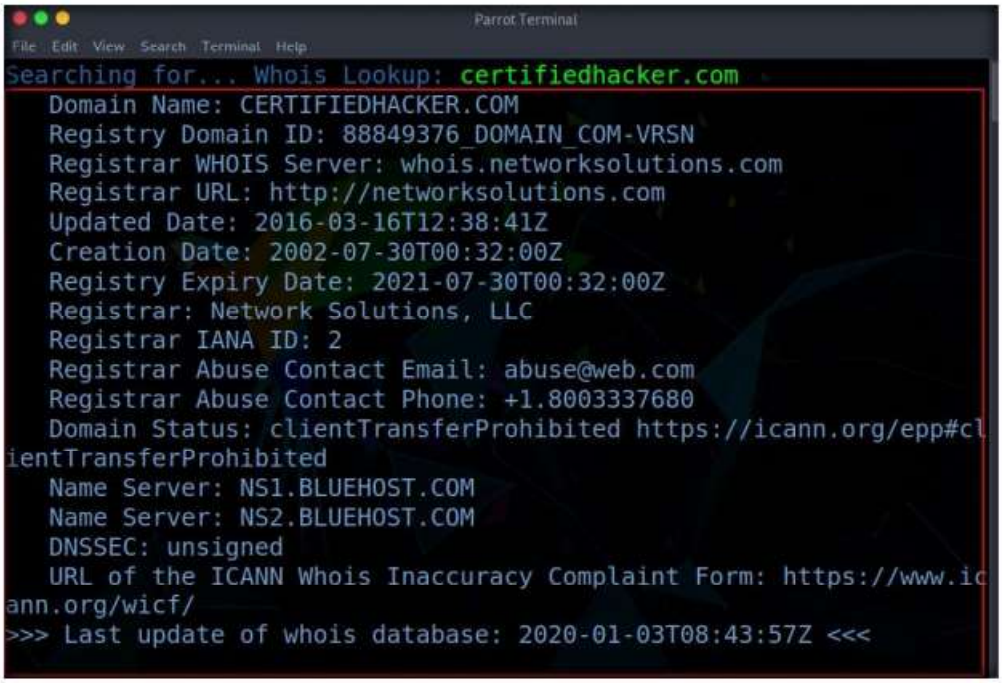


Figure 1.1.9: Whois Lookup information

TASK 1.4

Perform DNS Lookup

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

Note: The results might differ in your lab environment.

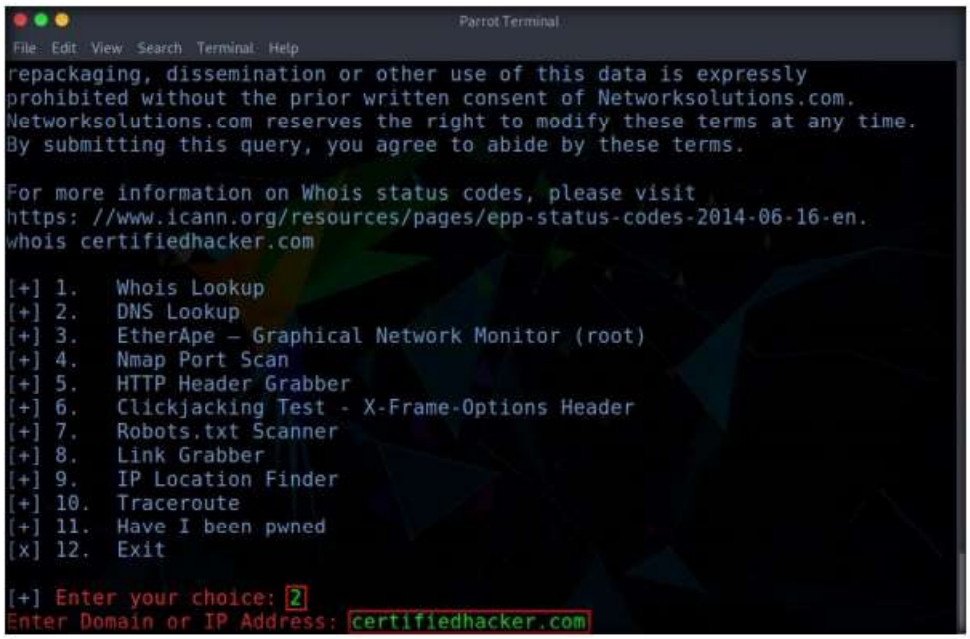


Figure 1.1.10: Performing DNS Lookup

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

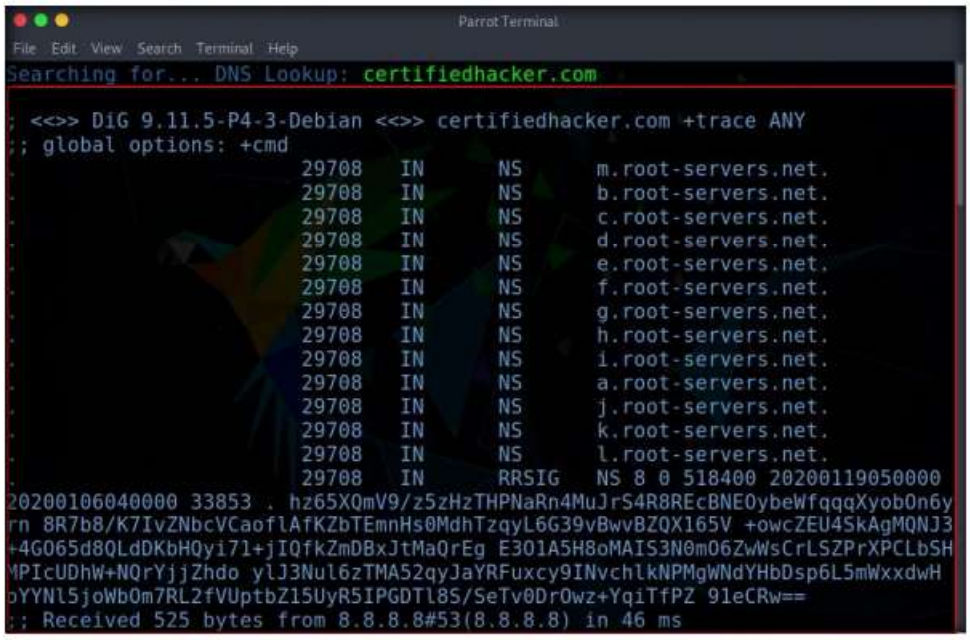


Figure 1.1.11: DNS Lookup information

TASK 1.5

Perform Clickjacking Test

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

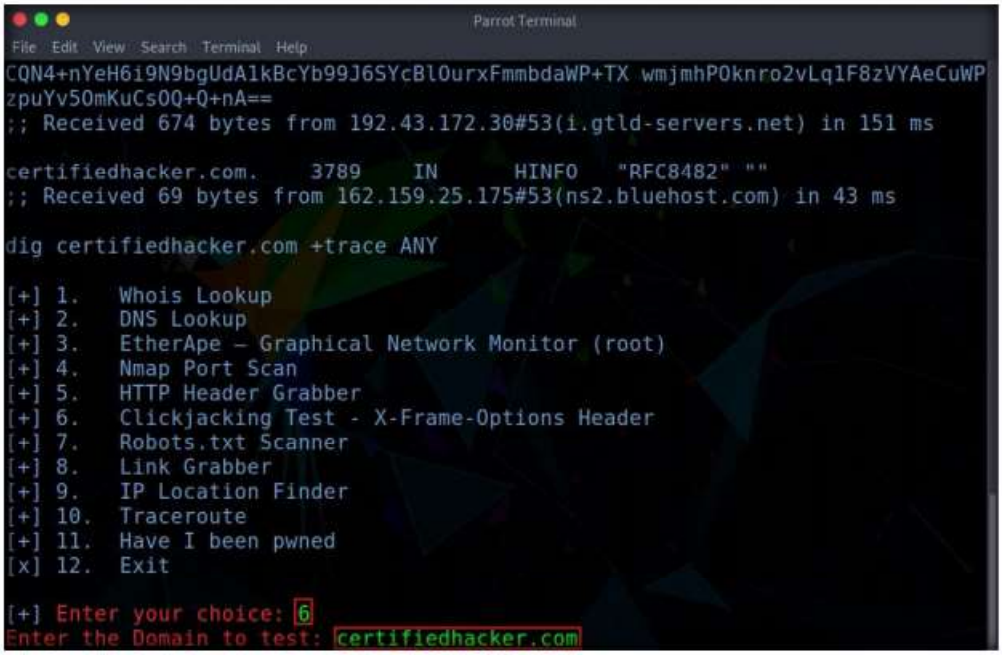


Figure 1.1.12: Performing Clickjacking test

22. By performing this test, Ghost Eye will provide the complete architecture of the web server, and also reveal whether the domain is vulnerable to Clickjacking attacks or not.

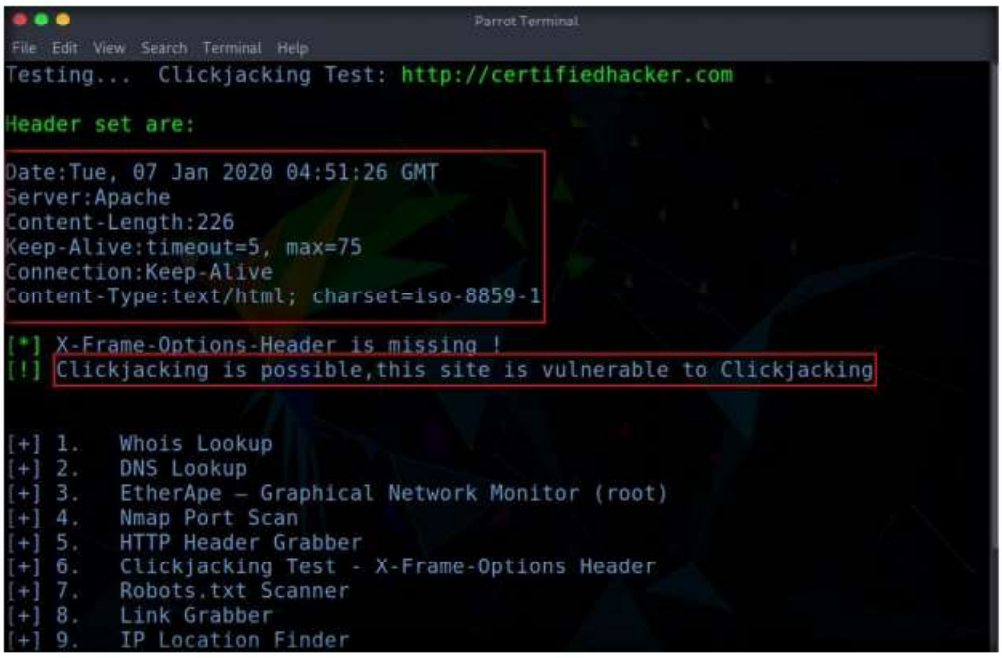


Figure 1.1.13: Clickjacking test information

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

TASK 2 Perform Web Server Reconnaissance using Skipfish

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

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **Pa$$w0rd**.

TASK 2.1

Start WampServer in Windows Server 2016

2. Double-click the **WAMP Server** shortcut icon from **Desktop** to start WAMP Server services. Alternatively, you can also launch the WAMP Server services from the **Start** menu apps

Figure 1.2.1: Starting WampServer

Skipfish is an active web application (deployed on a webserver) security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes. The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

3. Wait until the WAMP Server icon turns **Green** in the **Notification** area. Leave the **Windows Server 2016** virtual machine running.

Figure 1.2.2: WampServer icon

4. Switch to the **Parrot Security** virtual machine and launch **MATE Terminal** from the menu bar.
5. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
6. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

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

TASK 2.2

Scan the Web Server

8. Now, perform security reconnaissance on a web server using Skipfish. The target is the WordPress website **http://[IP Address of Windows Server 2016]**.
9. Specify the output directory and load a dictionary file based on the web server's requirement. In this lab, we are naming the output directory **test**.
10. In the terminal window, type **skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2016]:8080** and press **Enter**.

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

Figure 1.2.3: Initiating the scan

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

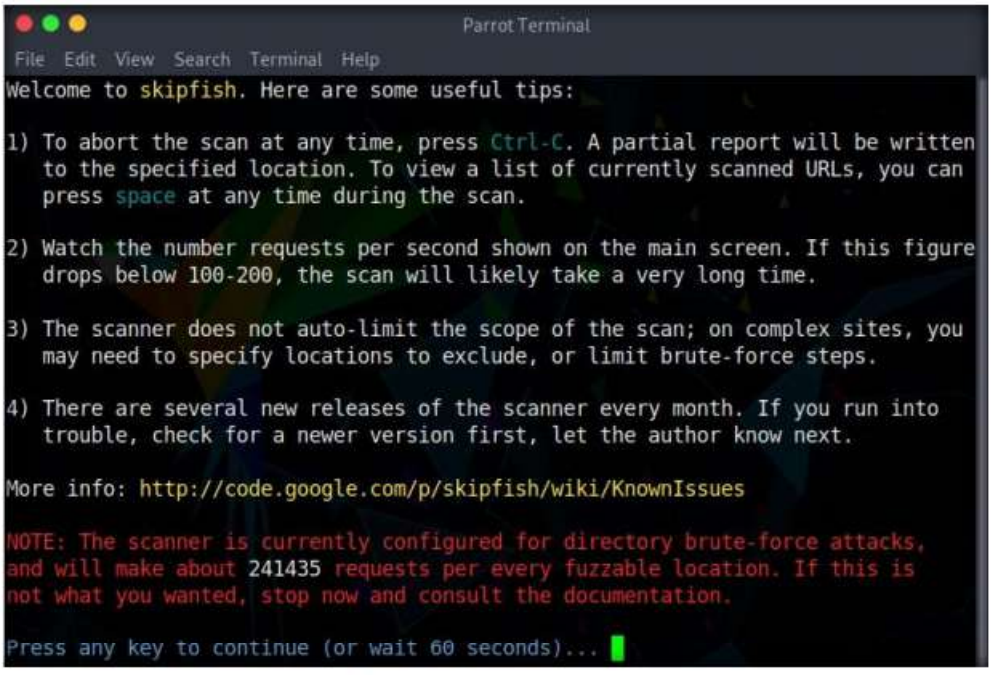


Figure 1.2.4: Initiating the scan

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

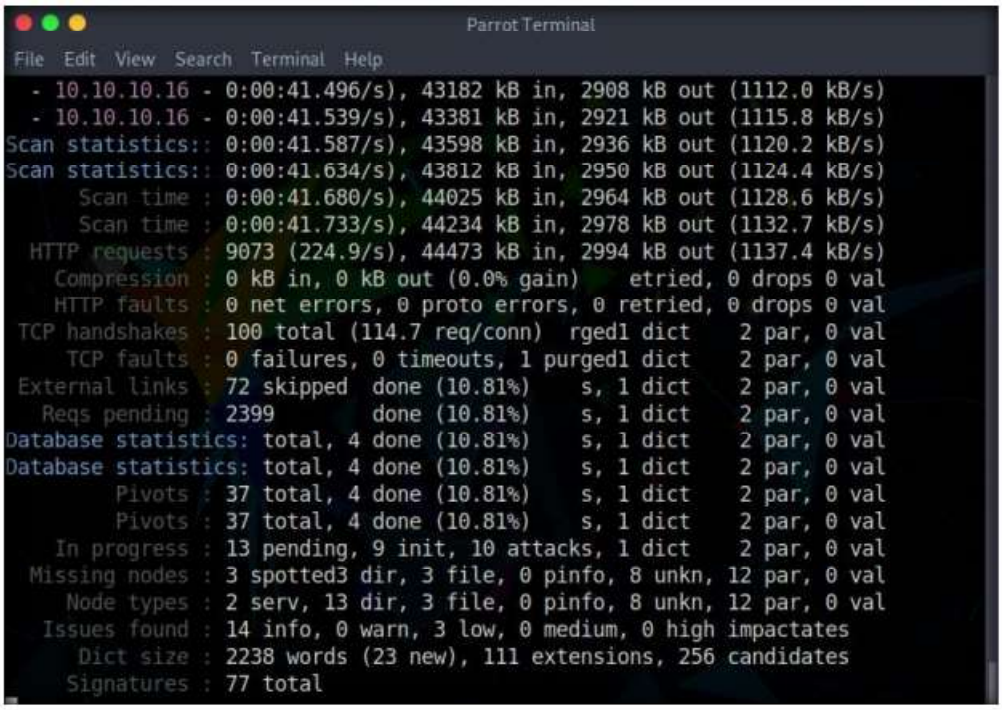


Figure 1.2.5: Skipfish scanning the web server

14. Note that Skipfish takes some time (approximately 20 minutes) to complete its scan.

Note: You can press **Ctrl+C** to terminate the scan if it is taking longer.

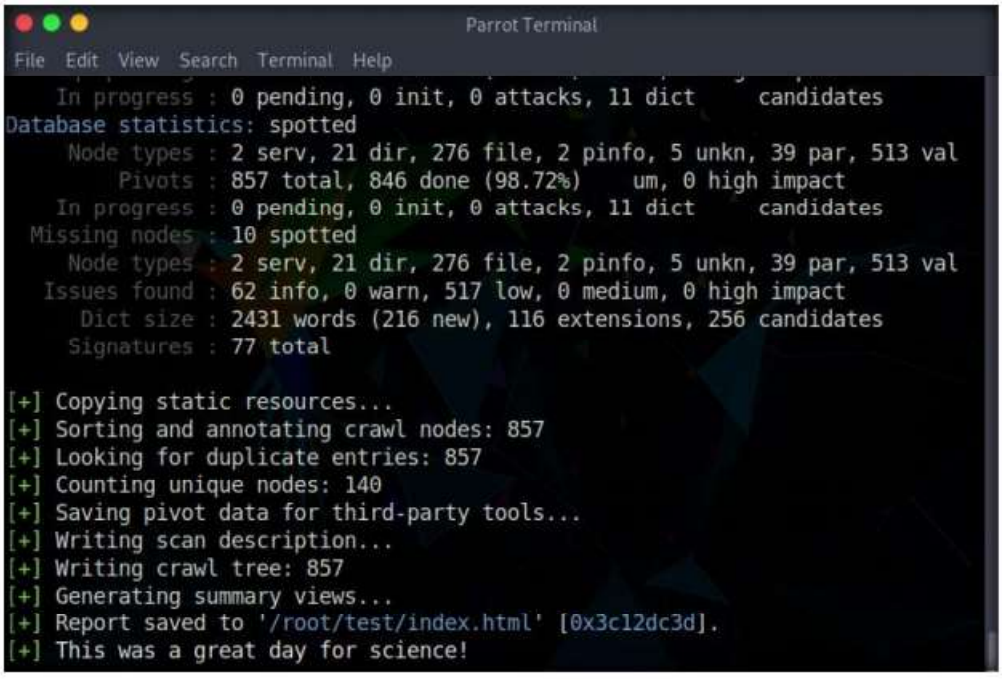


Figure 1.2.6: Completion of the scan

TASK 2.3

Examine the Scan Result

15. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in the **root** location). Navigate to **location**, right-click **index.html**, hover your mouse cursor on **Open With**, and click **Firefox** to view the scan result.

Note: To navigate to the **root** directory, click **Places** from the top-section of the **Desktop** and click **Home Folder** from the drop-down options. In the **attacker** window, click **File System** from the left-pane and navigate to the location **root**.

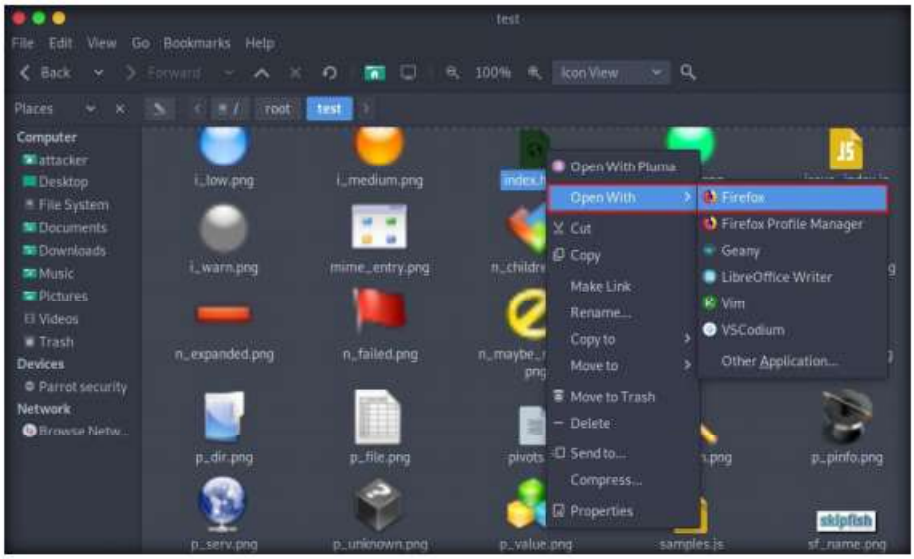


Figure 1.2.7: Viewing the scan result

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

Note: The scan result might vary in your lab environment.

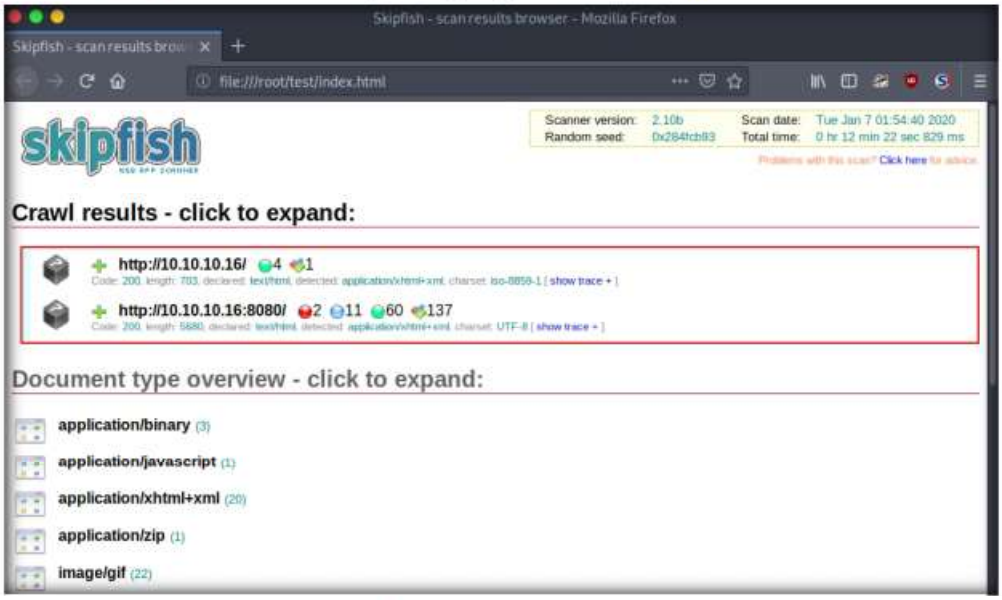


Figure 1.2.8: Examining the scan result

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

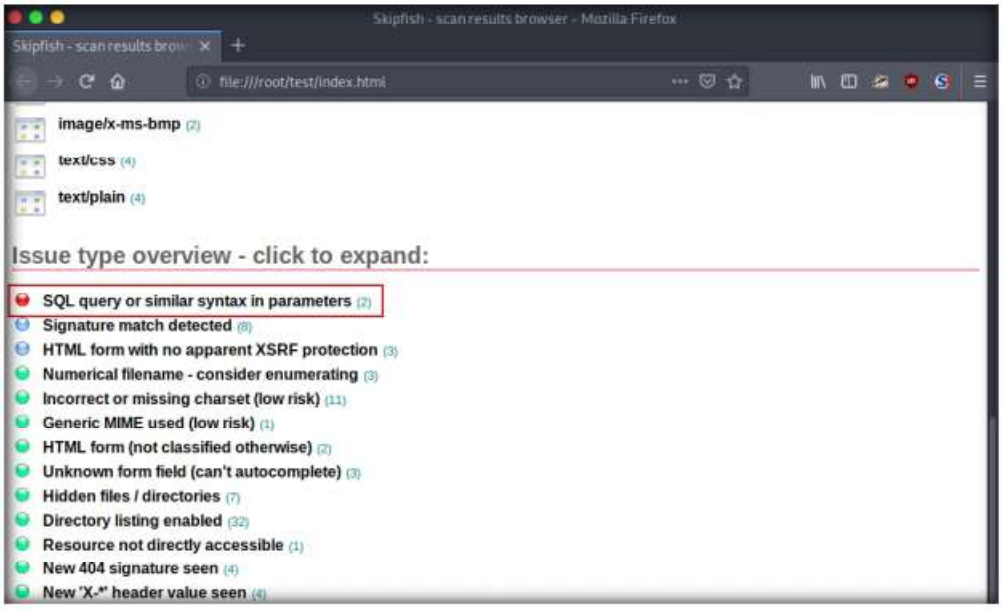


Figure 1.2.9: Examining the scan result

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

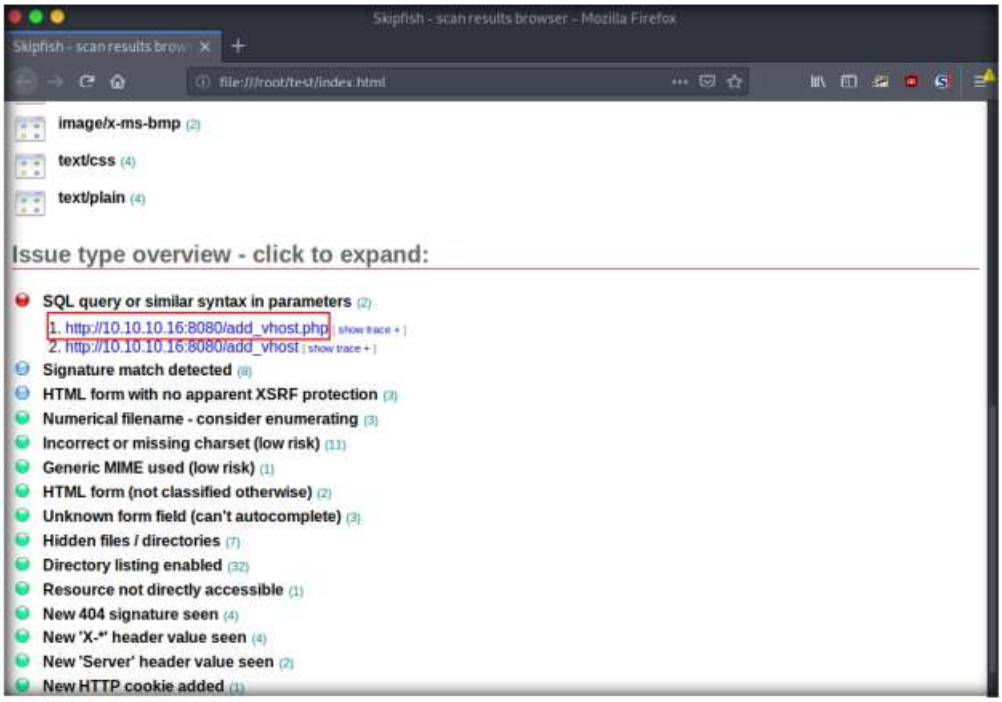


Figure 1.2.10: Examining the scan result

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

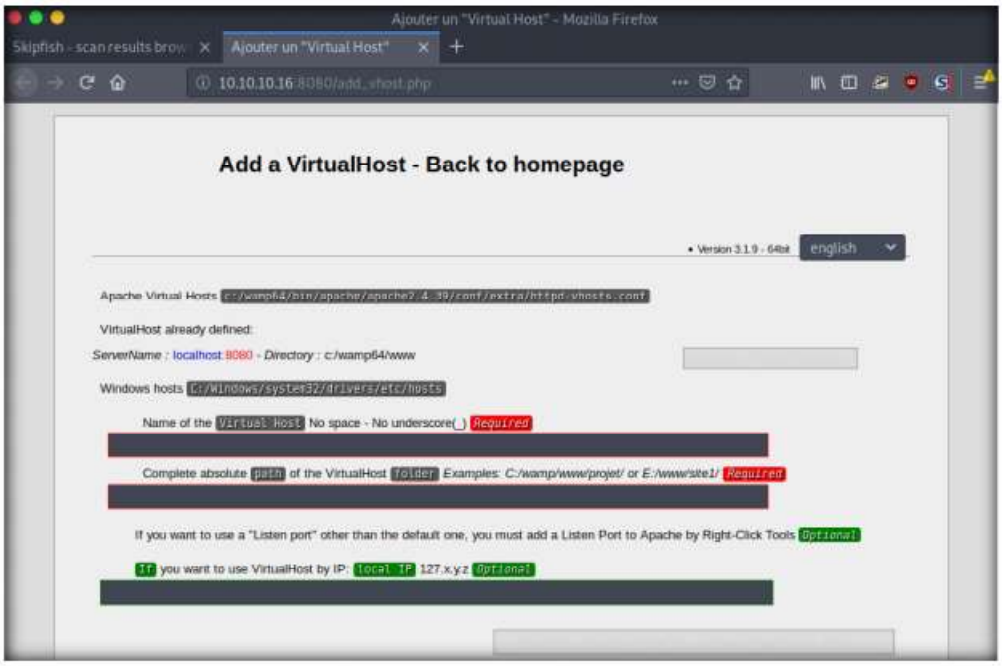


Figure 1.2.11: Examining the scan result

22. The PHP version webpage appears, displaying details related to the machine, as well as the other resources associated with the web server infrastructure and PHP configuration.

23. Click **show trace** next to the URL to examine the vulnerability in detail.

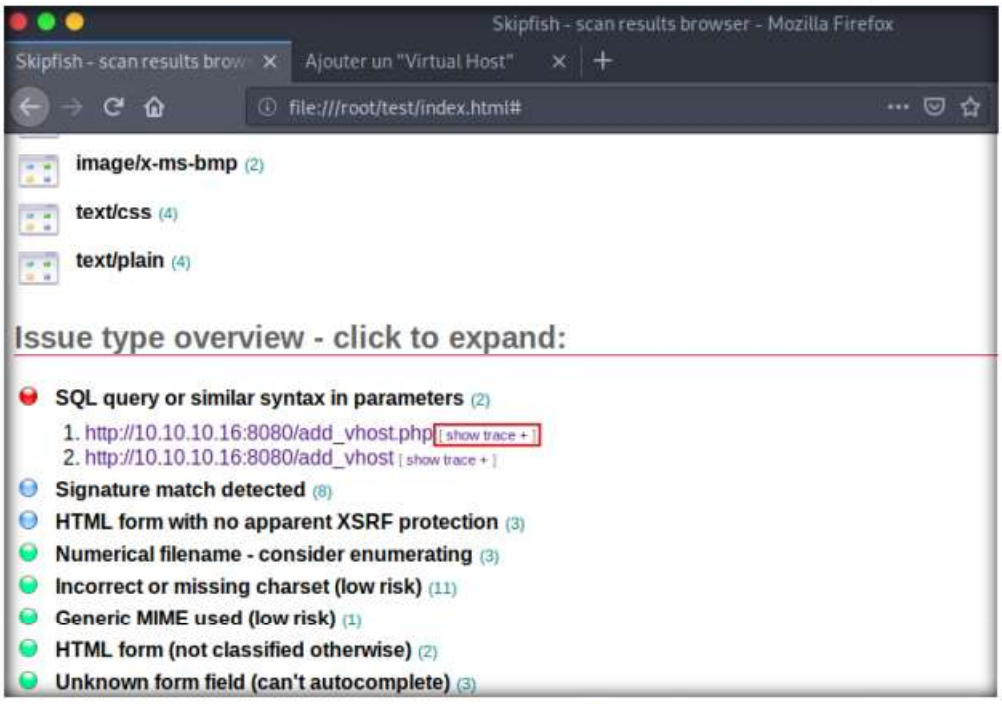


Figure 1.2.12: Examining the HTTP trace

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

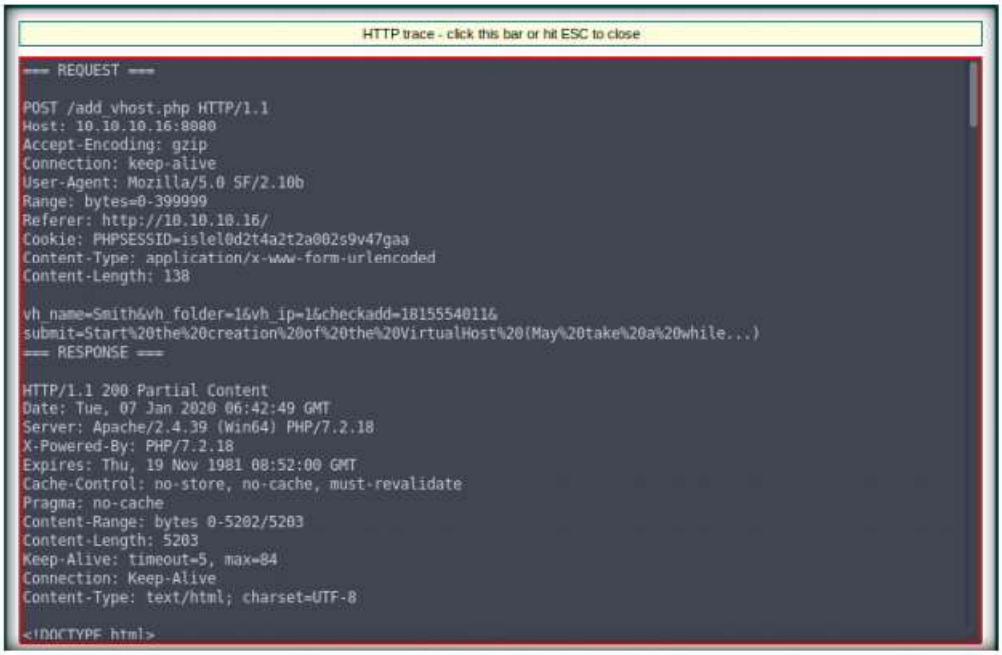


Figure 1.2.13: Examining the HTTP trace

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

25. Examine other vulnerabilities and patch them to secure the web server.
26. This concludes the demonstration of how to gather information about a target web server using Skipfish.
27. Close all open windows on both the **Parrot Security** and **Windows Server 2016** virtual machines and turn off the machines.

Footprint a Web Server using the httprecon Tool

TASK 3

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

TASK 3.1

Launch the httprecon Application

1. Turn on the **Windows 10** and log in with the credentials **Admin** and **Pa$$w0rd**.
2. Navigate to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**, right-click **httprecon.exe**, and, from the context menu, click **Run as administrator** double-click to launch the application.

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

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.

3. The main window of **httprecon** appears, as shown in the screenshot.

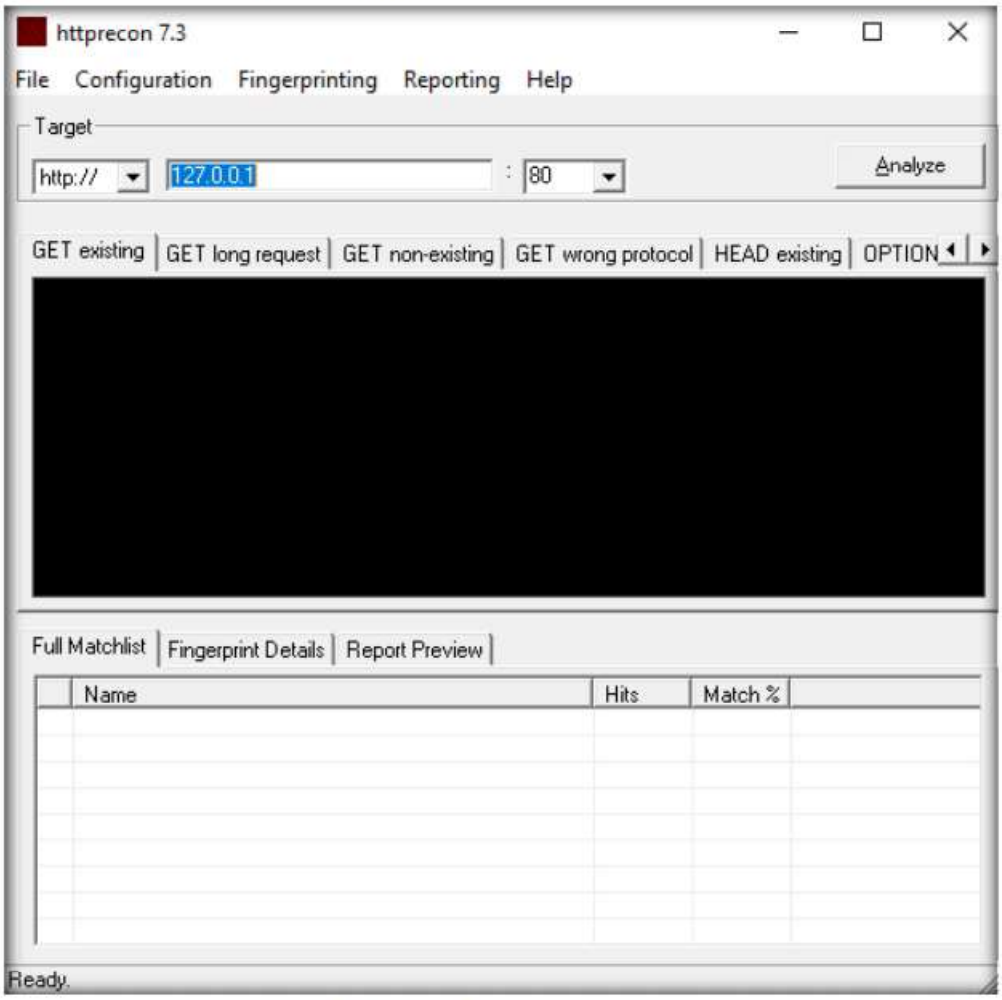


Figure 1.3.1: httprecon main window

TASK 3.2

Provide the Target URL and Analyze the Results

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

4. Enter the website URL (here, **www.certifiedhacker.com**) that you want to footprint and select **port number** (**80**) in the **Target** section.
5. Click **Analyze** to start analyzing the designated website.
6. A **footprint** of the website appears, as shown in the screenshot.

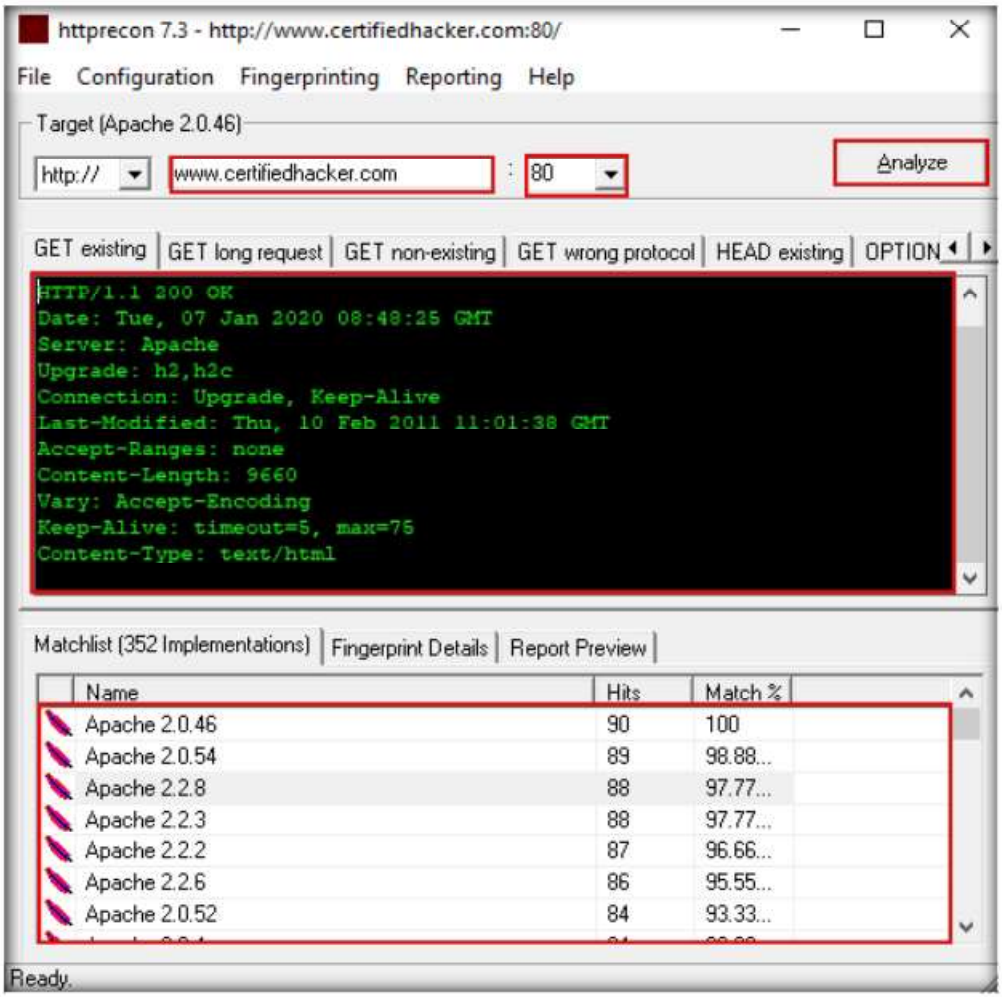


Figure 1.3.2: The footprint results of the entered website

7. Look at the **Get existing** tab, and observe the server (**Apache**) and the server-side application (**ASP.NET**) used to develop the webpages.
8. When attackers obtain this information, they research the vulnerabilities present in **ASP.NET** and **Apache** and try to exploit them, which results in either full or partial control over the web application.
9. Click the **GET long request** tab, which lists all GET requests. Next, click the **Fingerprint Details** tab.

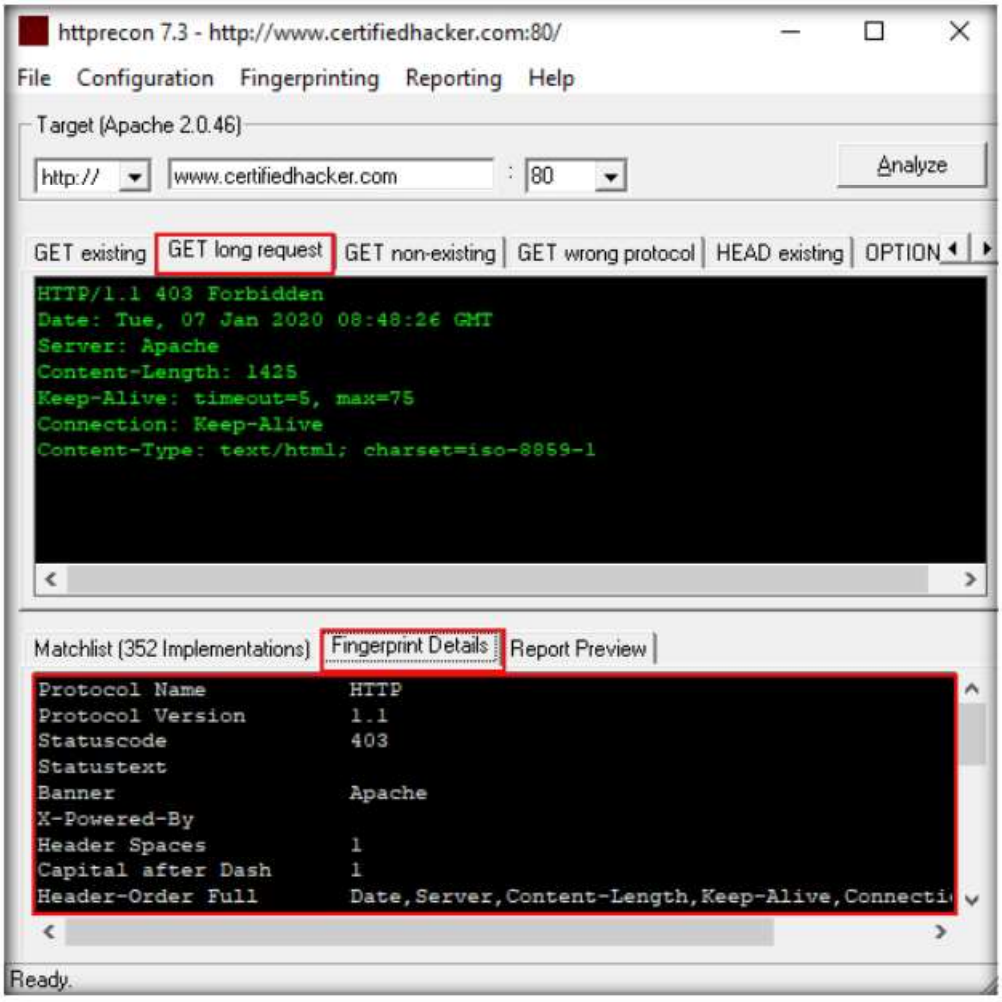


Figure 1.3.3: The fingerprint and GET long request result of the entered website

10. The details displayed in the screenshot above include the name of the protocol the website is using and its version.
11. By obtaining this information, attackers can manipulate HTTP vulnerabilities in order to perform malicious activities such as sniffing over the HTTP channel, which might result in revealing sensitive data such as user credentials.
12. This concludes the demonstration of how to gather information about the target web server using httprecon.
13. Close all open windows on the **Windows 10** virtual machine.

TASK 4

Footprint a Web Server using ID Serve

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

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

TASK 4.1

Launch ID Server

1. On the **Windows 10** virtual machine, navigate to **E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve** and double-click **idserve.exe**.
2. The main window of **ID Serve** appears. Click the **Server Query** tab.

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

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

Figure 1.4.1: Welcome screen of ID Serve

TASK 4.2

Provide the Target URL and Examine the Result

3. For option **1**, in the **Enter or copy/paste an Internet server URL or IP address** section, enter the URL (**http://www.certifiedhacker.com**) you want to footprint.
4. Click **Query the Server** to start querying the website.
5. After the completion of the query, ID Serve displays the results of the entered website, as shown in the screenshot.

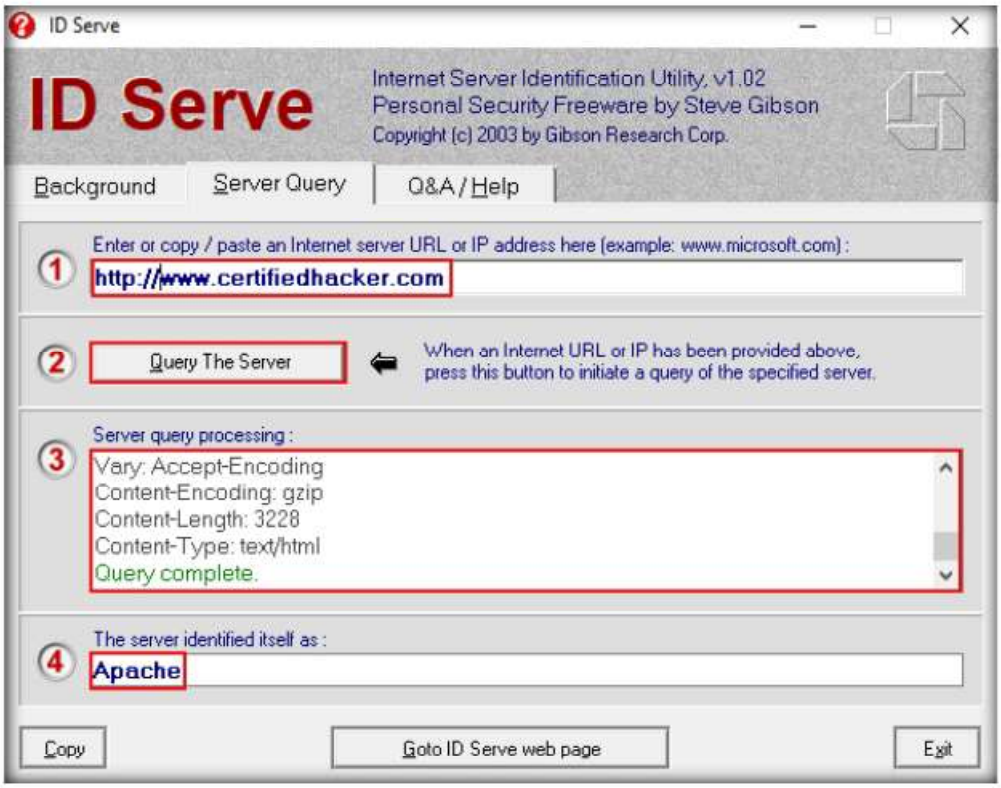


Figure 1.4.2: ID Serve detecting the footprint

Note: The result might vary in your lab environment.

6. After obtaining this information, the attacker may perform a vulnerability analysis on that particular version of the web server and implement various techniques to perform exploitation.
7. Click **Exit** to close the application. Close all open windows and turn off the **Windows 10** virtual machine.

TASK 5 Footprint a Web Server using Netcat and Telnet

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.

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

Note:

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

3. Click the **MATE Terminal** icon from the menu bar to launch the terminal.

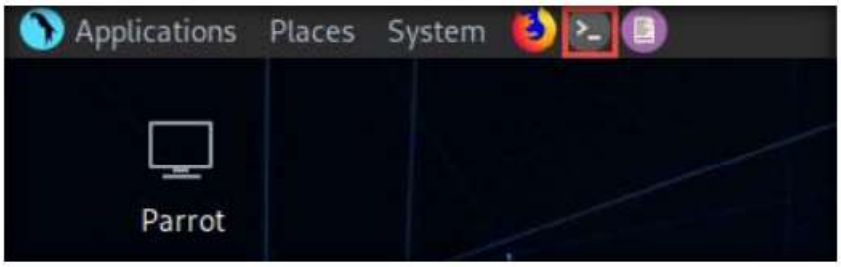


Figure 1.5.1: Launching MATE terminal

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

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

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

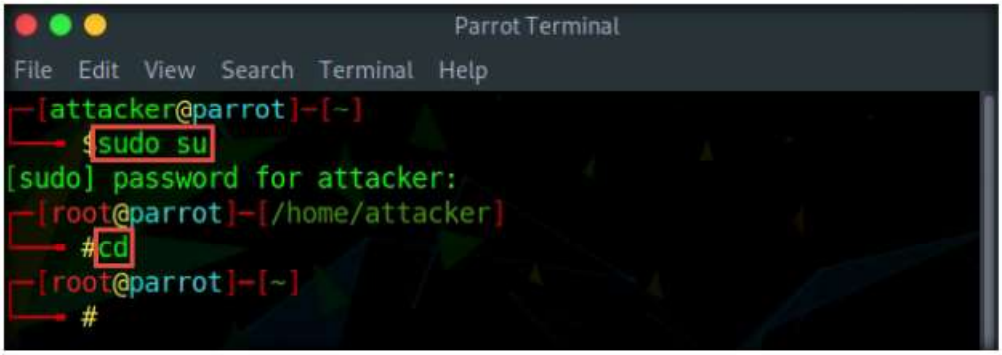


Figure 1.5.2: Running the programs as a root user

TASK 5.1

Footprint using Netcat

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

Figure 1.5.3: Perform Banner Grabbing using Netcat

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

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

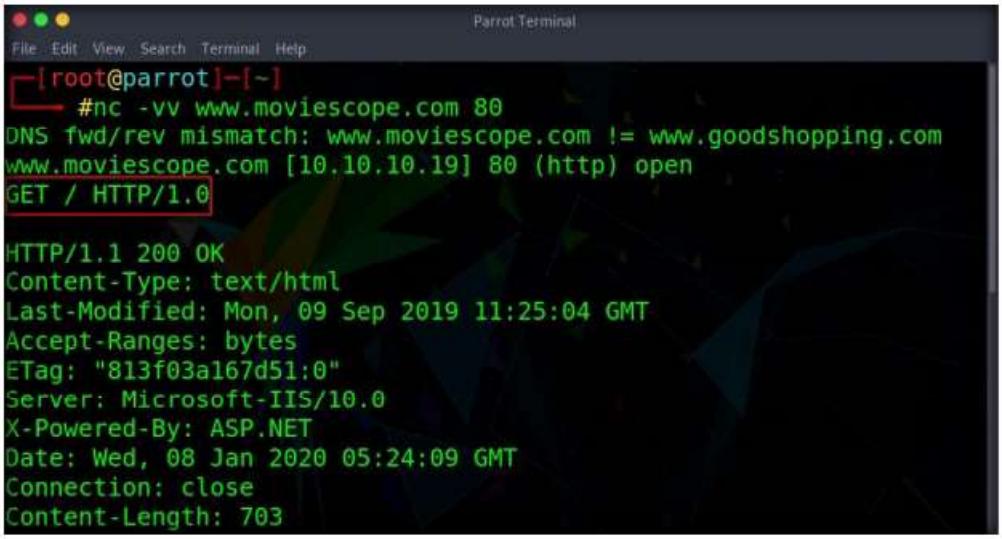


Figure 1.5.4: Netcat Banner Grabbing result

TASK 5.2

Footprint using Telnet

Telnet- Telnet is a client-server network protocol. It is widely used on the Internet or LANs. It provides the login session for a user on the Internet. The single terminal attached to another computer emulates with Telnet.

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.

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

Figure 1.5.5: Perform Banner Grabbing using Telnet

13. Telnet will connect to the domain, as shown in the screenshot.
14. Now, type **GET / HTTP/1.0** and press **Enter** twice. Telnet will perform the banner grabbing and gather information such as content type, last modified date, accept ranges, ETag, and server information.

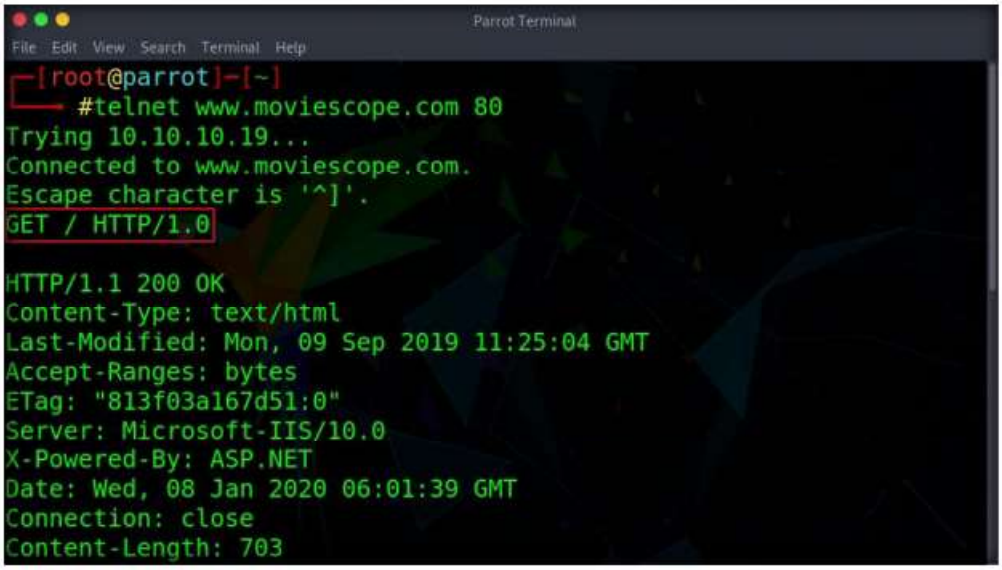


Figure 1.5.6: Telnet Banner Grabbing result

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

TASK 6

Enumerate Web Server Information using Nmap Scripting Engine (NSE)

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

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

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

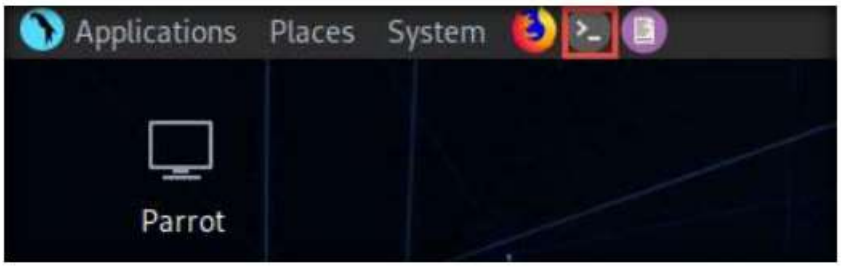


Figure 1.6.1: Launch MATE terminal

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

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

4. Now, type **cd** and press **Enter** to jump to the root directory
5. Enumerate the directories used by web servers and web applications, in the terminal window. Type **nmap -sV --script=http-enum <target website>** and press **Enter**.
6. In this scan, we are enumerating the **www.goodshopping.com** website.

TASK 6.1

Enumerate Web Server using Nmap

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

Figure 1.6.2: HTTP-Enum on target host

Through this technique, it is possible to discover genuine (and extremely dumb) security imperfections on a site such as some sites (like WordPress and PrestaShop) that maintain accessibility to envelopes that ought to be erased once the task has been settled. Once you have identified a vulnerability, you can discover a fix for it.

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

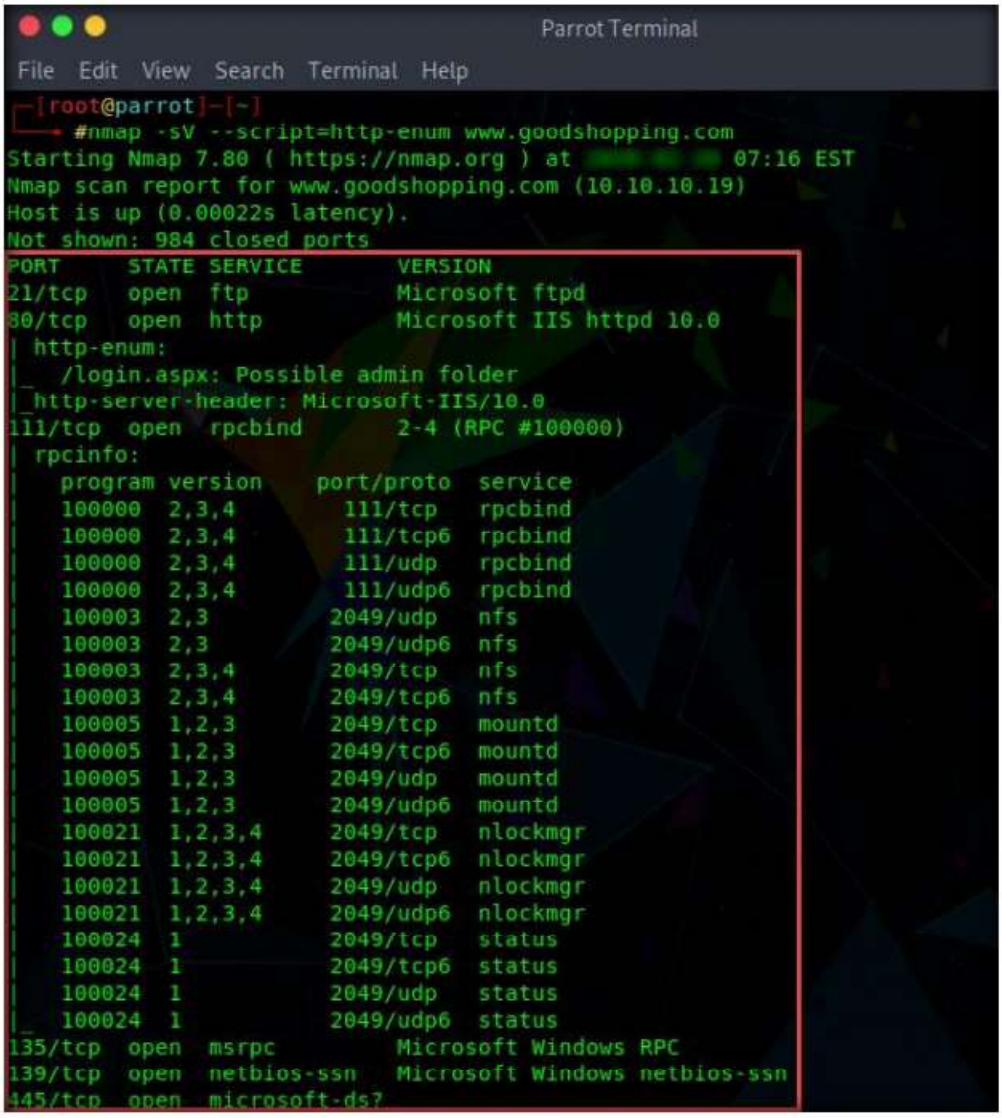


Figure 1.6.3: HTTP-Enum on target host result

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

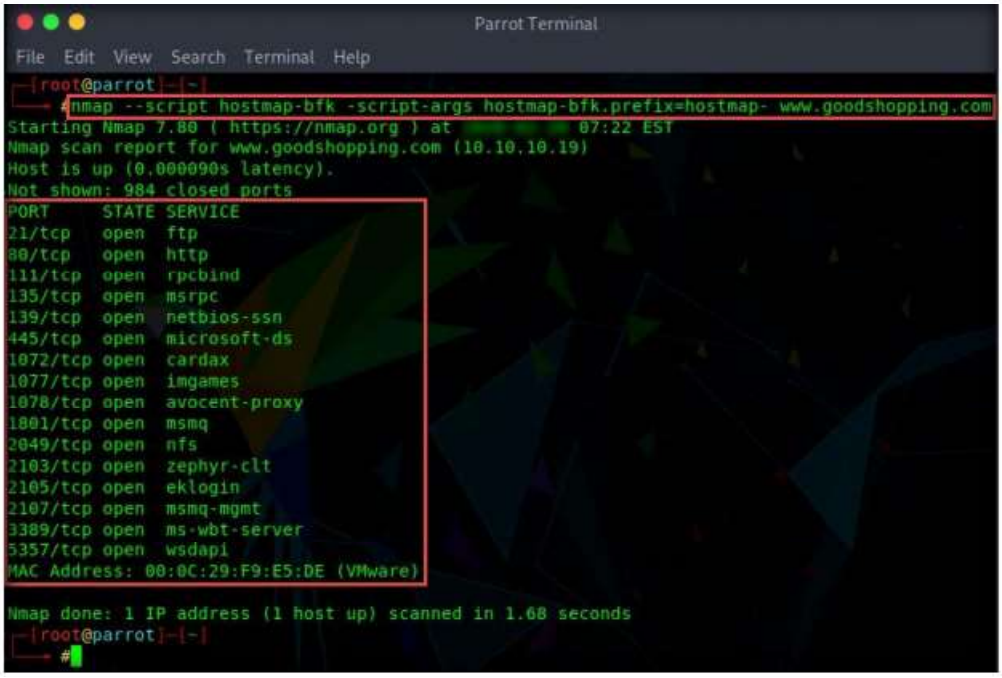
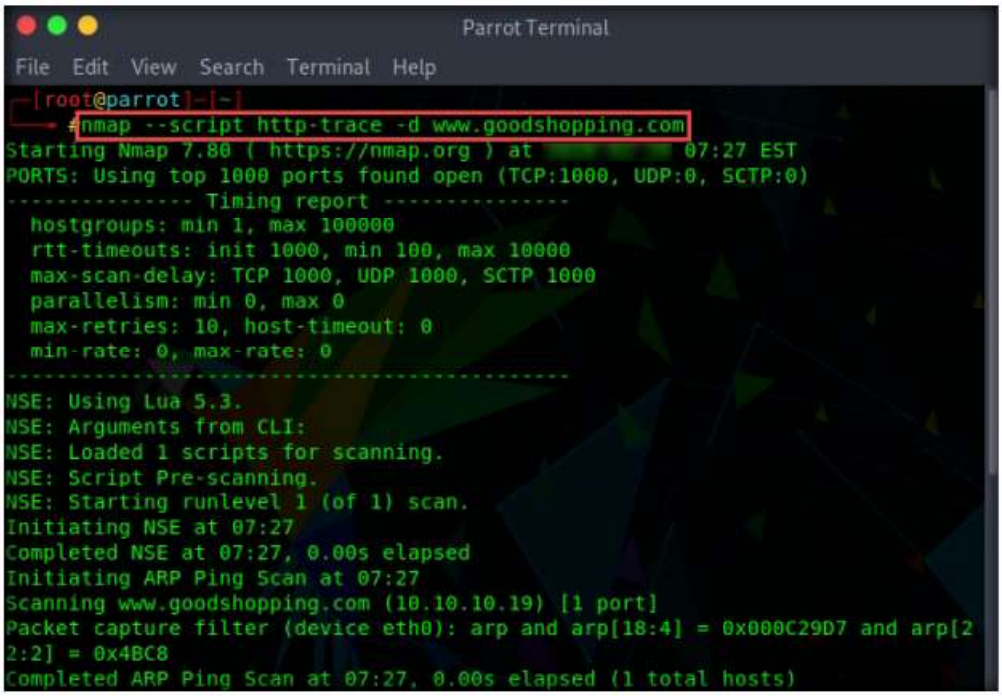
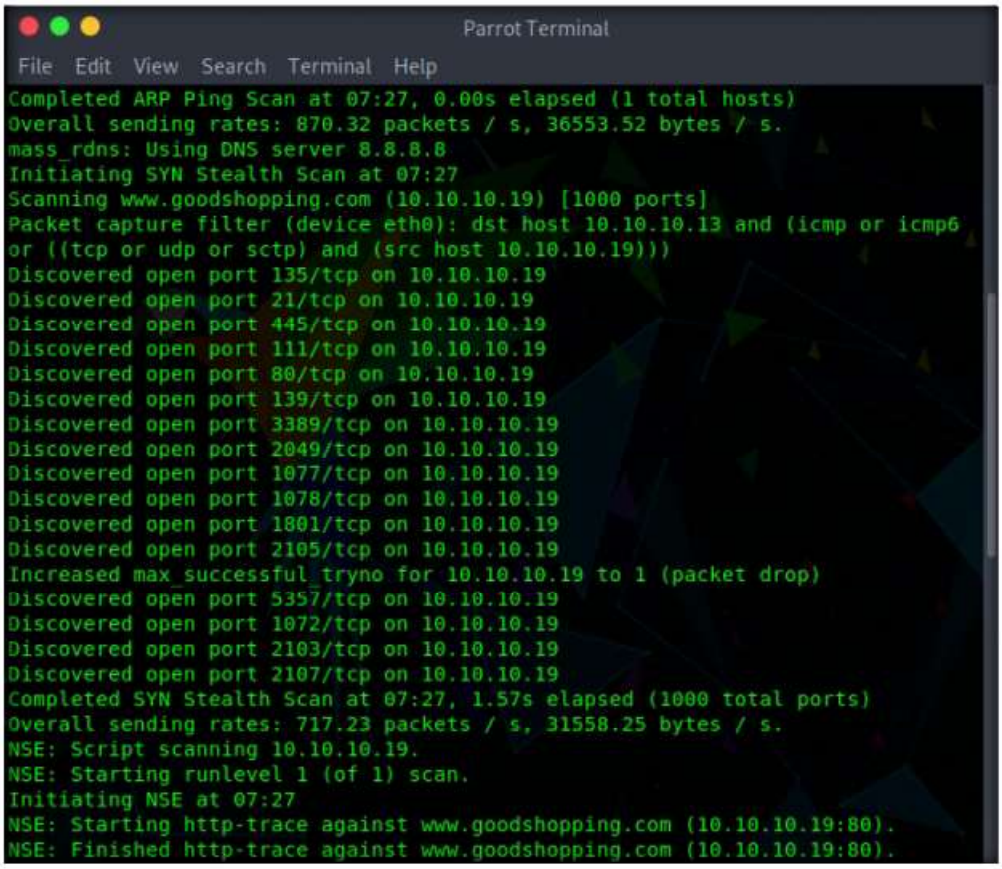


Figure 1.6.4: Host Map on target host

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





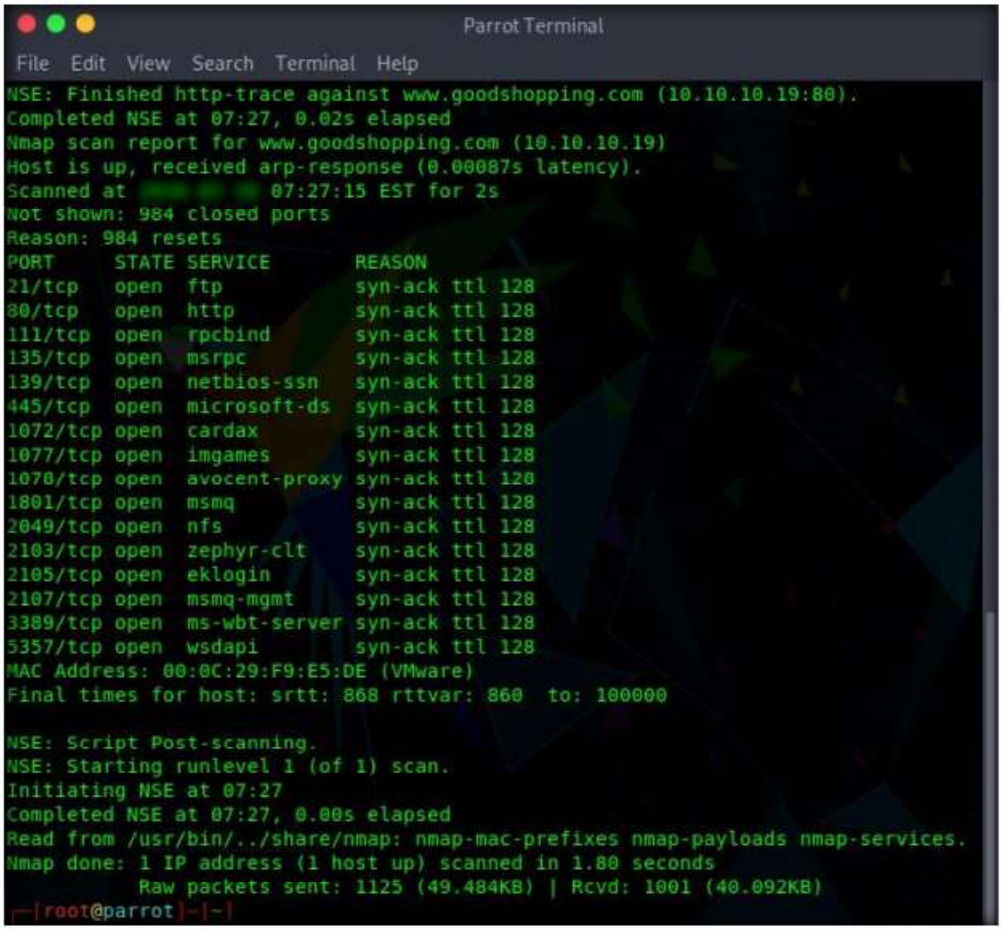


Figure 1.6.5: Host Map on target host result

12. Now, check whether Web Application Firewall is configured on the target host or domain. In the terminal window, type **nmap -p80 --script http-waf-detect www.goodshopping.com** and press **Enter**.
13. This command will scan the host and attempt to determine whether a web server is being monitored by an IPS, IDS, or WAF.
14. This command will probe the target host with malicious payloads and detect the changes in the response code.

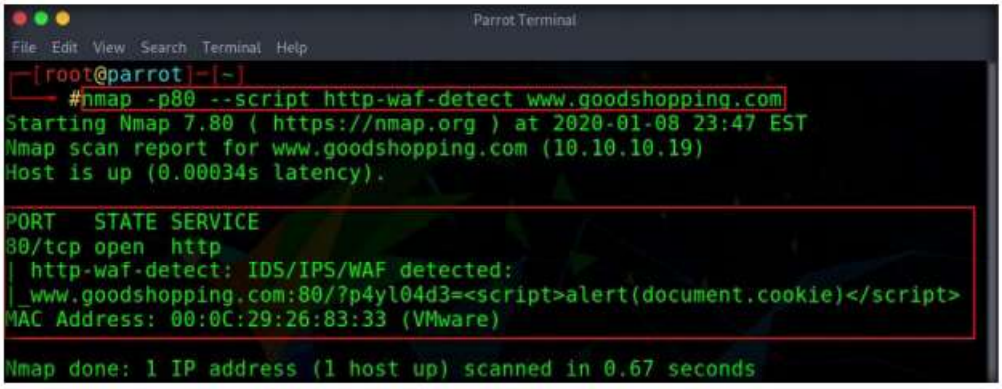


Figure 1.6.6: WAF Detection on target host result

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

TASK 7 Uniscan Web Server Fingerprinting in Parrot Security

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

TASK 7.1

Start WampServer in Windows Server 2016

1. Turn on the **Windows Server 2016** virtual machine and log in with the credentials **Administrator** and **pa$$word**.
2. Start WAMPServer on the **Windows Server 2016** virtual machine. Double-click the **WAMPServer** shortcut icon on **Desktop** to start the service.
3. Wait until the WAMPServer icon turns **green** in the notification area, as shown in the screenshot.
4. Leave the **Windows Server 2016** virtual machine running and switch to the **Parrot Security** virtual machine.

Figure 1.7.1: Windows Server 2016 WAMP Server

5. Now, on the **Parrot Security** virtual machine, click the **MATE Terminal** icon from the menu bar to launch the terminal.
6. A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
7. In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

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

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

TASK 7.2

View Uniscan Help Options

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

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

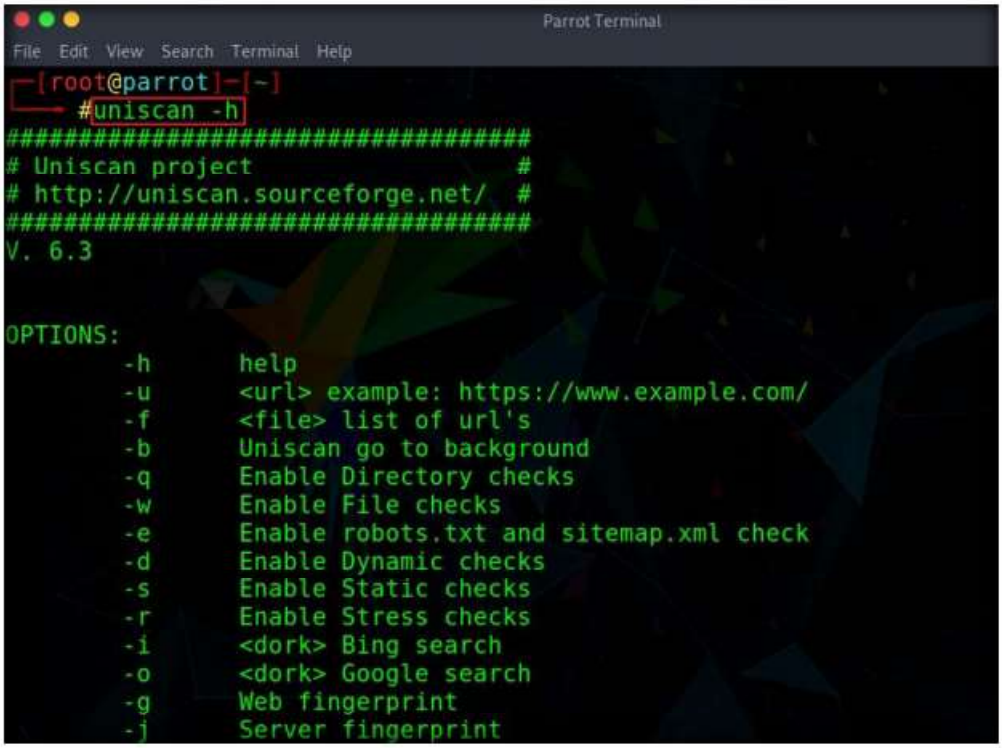


Figure 1.7.2: Uniscan help command

TASK 7.3

Perform Directory Scan

11. In the terminal window, type **uniscan -u http://10.10.10.16:8080/CEH -q** and hit **Enter** to start scanning for directories.
12. Here, 10.10.10.16 is the IP address of the **Windows Server 2016** virtual machine. This may vary in your lab environment.
13. In the above command, the -u switch is used to provide the target URL, and the -q switch is used to scan the directories in the web server.

Figure 1.7.3: Run uniscan with -q command

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

Note: Scroll to analyze the complete output of the scan. It should take approximately 10 minutes for the scan to finish.

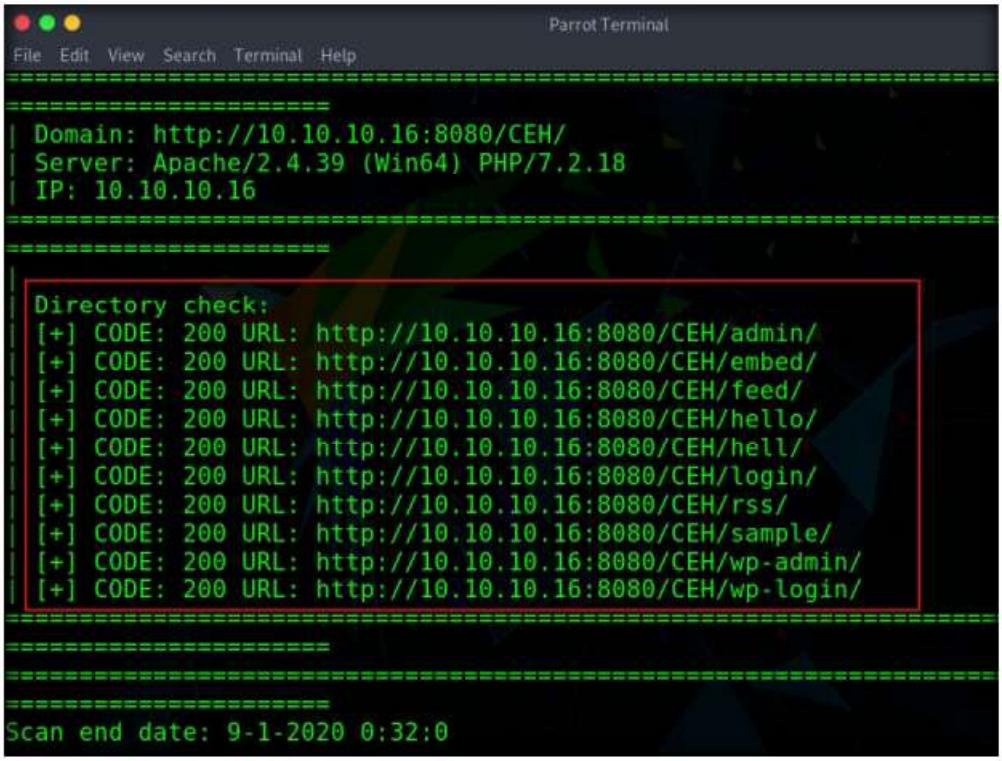


Figure 1.7.4: Uniscan showing found directories

TASK 7.4

Perform File Check

15. Now, run uniscan using two options together. Here **-w** and **-e** are used together to enable the file check (robots.txt and sitemap.xml file). In the terminal window, type **uniscan -u http://10.10.10.16:8080/CEH -we** and hit **Enter** to start the scan.

Figure 1.7.5: Uniscan command with -we option

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

Note: Scroll to analyze the complete scan result. It should take approximately 10 minutes for the scan to finish.

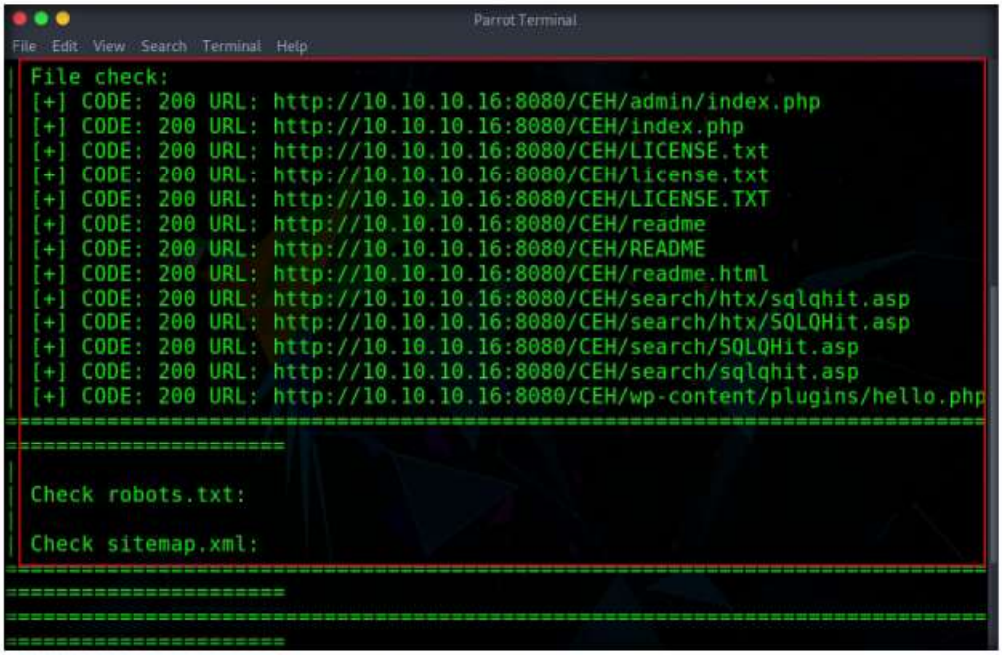


Figure 1.7.6: Uniscan displaying scan results

TASK 7.5

Perform Dynamic Tests

17. Now, use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.10.16:8080/CEH -d** and hit Enter to start a dynamic scan on the web server.

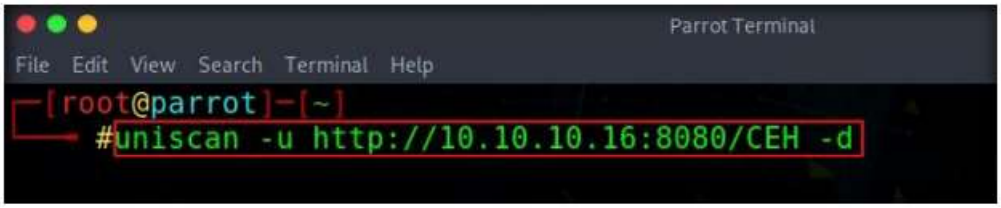


Figure 1.7.7: Run uniscan with -d option

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

Note: Scroll to analyze the complete output of the scan. It should take approximately 10 minutes for the scan to finish.

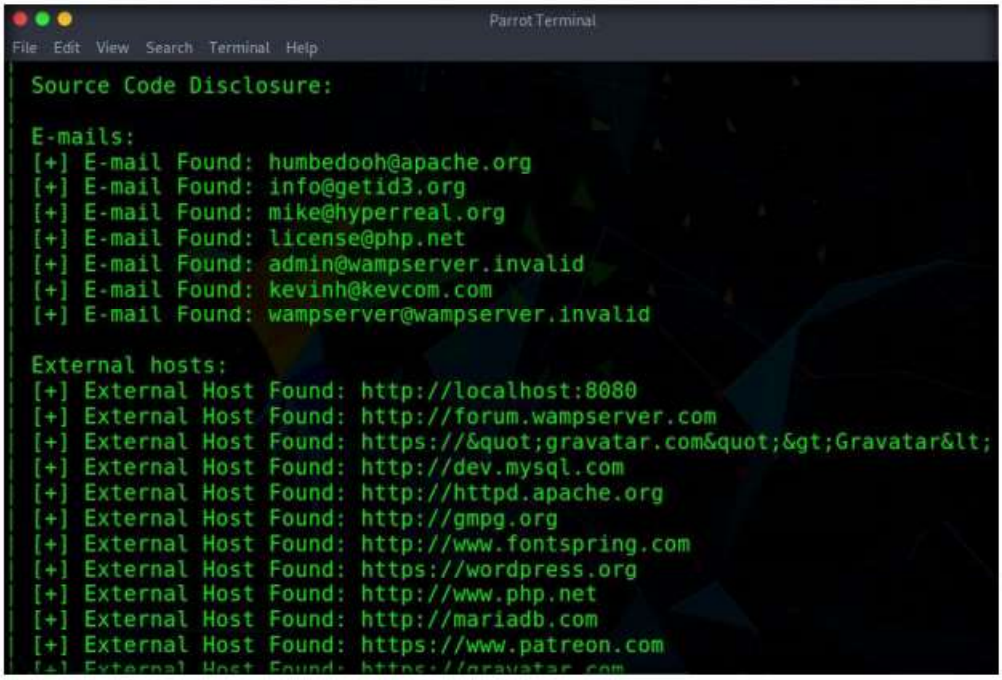


Figure 1.7.8: Uniscan displaying scan results

19. Uniscan displays the **PHP info**, as shown in the screenshot below. Close the terminal window.

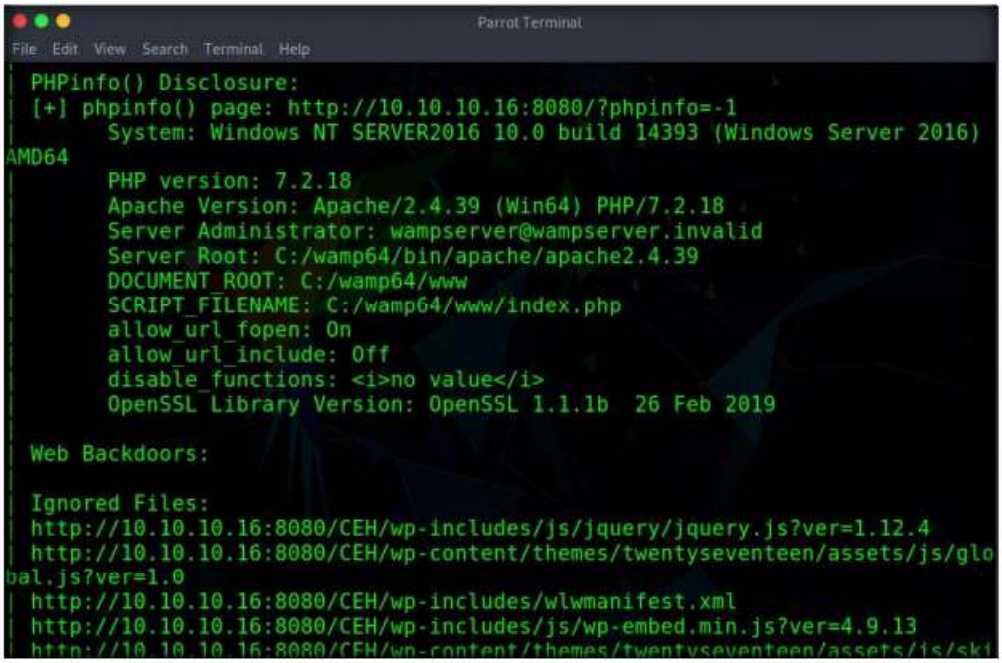


Figure 1.7.9: Uniscan displaying PHP info

TASK 7.6

View Report

20. After scanning, navigate to **/usr/share/uniscan/report** and right-click on **10.10.10.16.html**. Hover your mouse cursor on **Open With** and click **Firefox** from the menu to view the scan report.

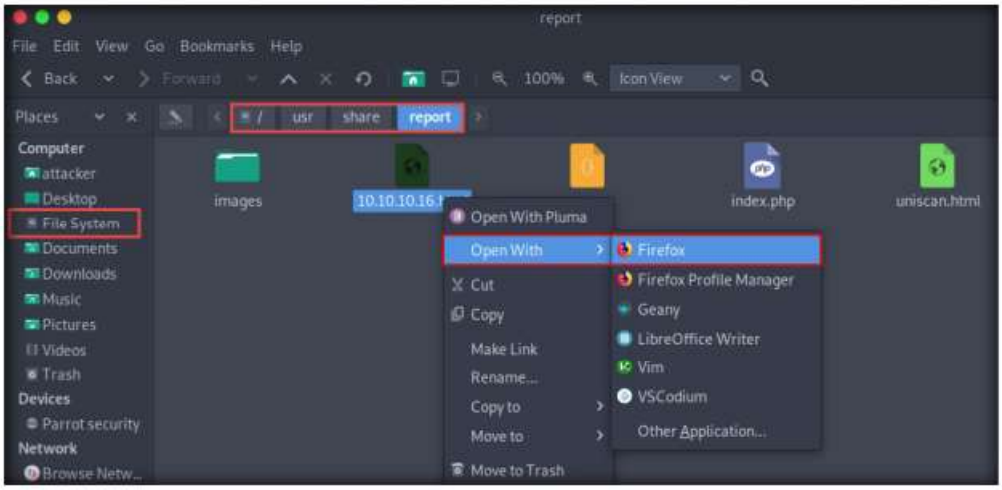


Figure 1.7.10: Scan report generated

You can also use other web server footprinting tools such as **SpiderFoot** (https://www.spiderfoot.net), **httprint** (https://www.net-square.com), **Winfingerprint** (https://qpdownload.com), and **NetworkMiner** (https://www.netresec.com) to gather information about the target web server.

21. The report opens in the browser, giving you all **scan details** in a more comprehensive manner.

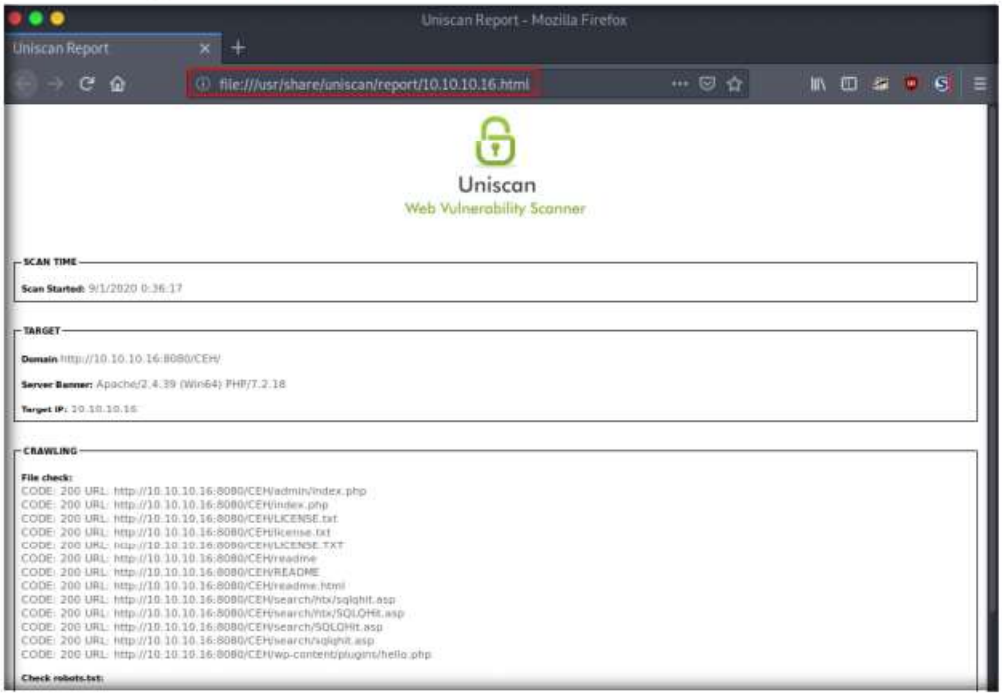


Figure 1.7.11: View the scan report

22. This concludes the demonstration of how to gather information about the target web server using Uniscan.
23. Close all terminal windows on the **Parrot Security** virtual machine.
24. Turn off the **Parrot Security** and **Windows Server 2016** virtual machines.

Lab Analysis

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

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

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

Lab 2

Perform a Web Server Attack

An expert hacker and pen tester must implement various techniques to launch web server attacks on the target web server.

ICON KEY

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

Lab Scenario

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

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

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

Tools demonstrated in this lab are available in E:\CEH-Tools\CEHv11 Module 13 Hacking Web Servers

Lab Objectives

- Crack FTP credentials using a Dictionary Attack

Lab Environment

To carry out this lab, you need:

- Windows 10 virtual machine
- Parrot Security virtual machine
- Web browsers with an Internet connection

- Administrator privileges to run the tools

Lab Duration

Time: 10 Minutes

Overview of Web Server Attack

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

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

Lab Tasks

TASK 1

Crack FTP Credentials using a Dictionary Attack

Here, we will firstly find the open FTP port using Nmap, and then perform a dictionary attack using the THC Hydra tool.

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

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

TASK 1.1

Copy and Paste Wordlists Folder

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

3. First, we will copy the **Wordlists** folder containing the sample username and password files (named **Passwords.txt** and **Usernames.txt**) from the shared network drive to the **root/Home** directory of the **Parrot Security** virtual machine.
4. To do so, open any windows explorer and press **Ctrl+L**. The **Location** field appears; type **smb://10.10.10.10** and press **Enter** to access **Windows 10** shared folders.
5. A security pop-up appears; enter the **Windows 10** virtual machine credentials (**Username**: **Admin** and **Password**: **Pa$$w0rd**) and click **Connect**.
6. The **Windows shares on 10.10.10.10** window appears. Double-click the **CEH-Tools** folder.

7. Navigate to **CEHv11 Module 13 Hacking Web Servers** and copy the **Wordlists** folder.

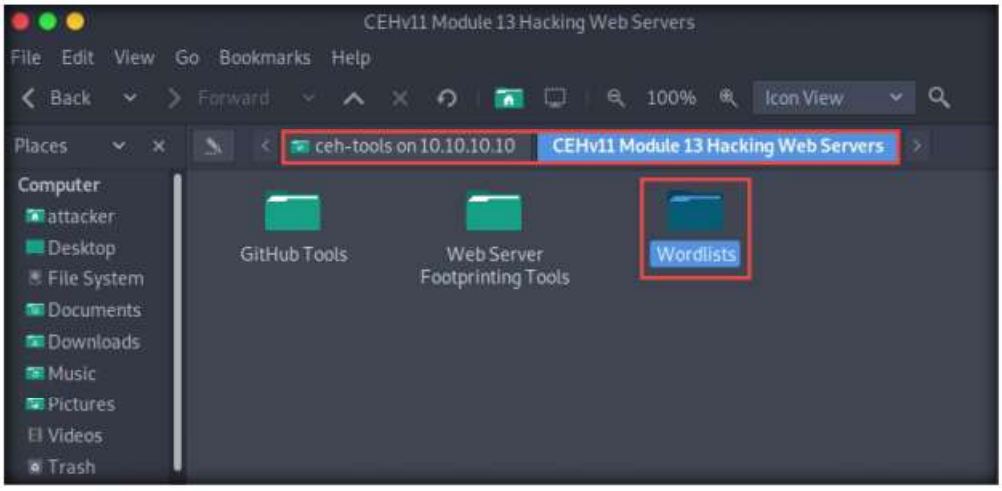


Figure 2.1.1: Copy the Wordlists file

8. Paste the **Wordlists** folder into the **/home/attacker** directory, as shown in the screenshot.

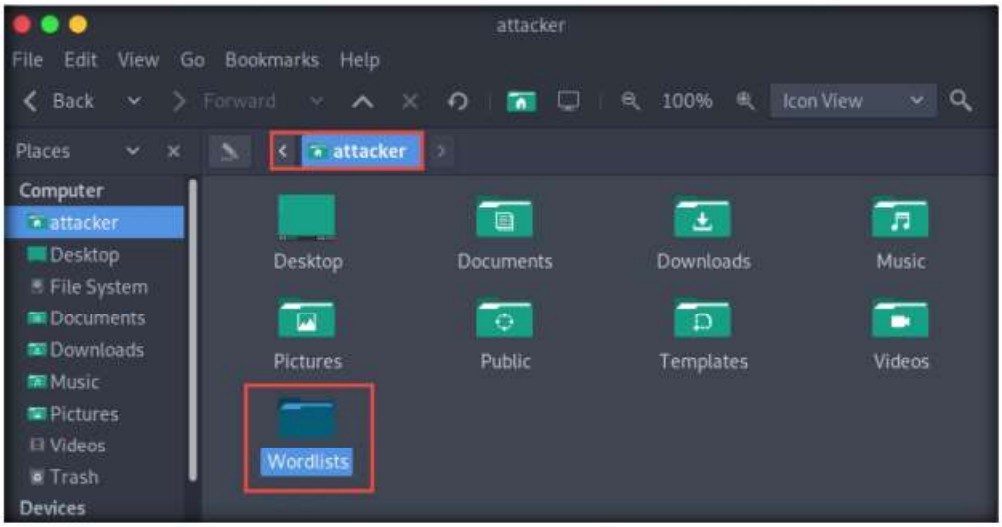


Figure 2.1.2: Paste the Wordlists directory

TASK 1.2

Perform Nmap Scan

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

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

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

13. Type **mv /home/attacker/Wordlists /root/** and press **Enter** to move the Wordlists folder to the root directory.

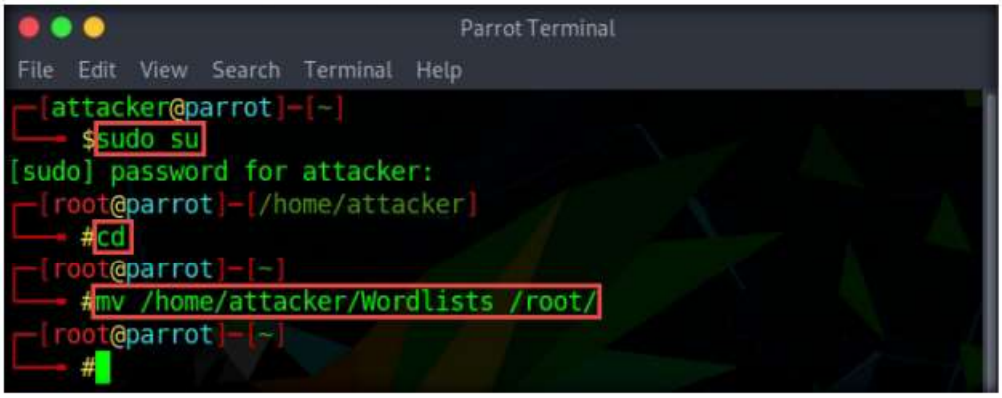


Figure 2.1.3: Move Wordlists folder to the root directory

14. Assume that you are an attacker, and you have observed that the FTP service is running on the **Windows 10** virtual machine.
15. Perform an **Nmap scan** on the target machine (**Windows 10**) to check if the FTP port is open.
16. In the parrot terminal window, type **nmap -p21 [IP Address of Windows 10]**, and press **Enter**.

Note: In this lab, the IP address of **Windows 10** is **10.10.10.10**.

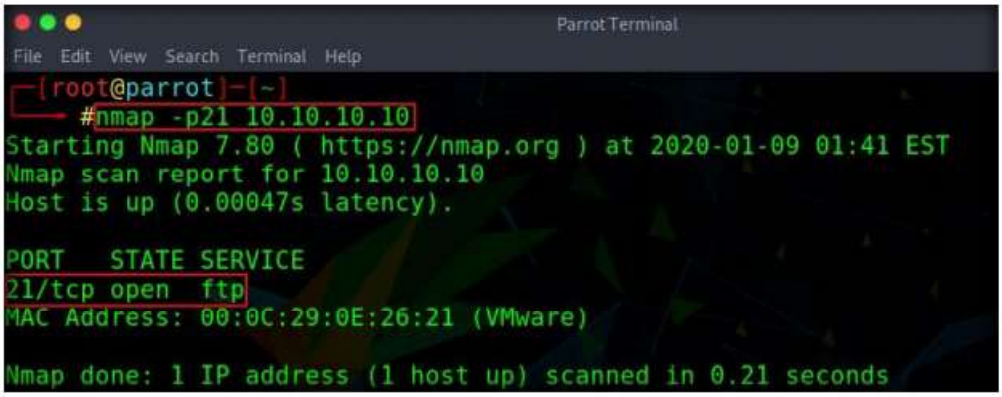


Figure 2.1.4: Performing Nmap port scan

17. Observe that **port 21** is open in **Windows 10**.
18. Check if an FTP server is hosted on the **Windows 10** machine.

19. Type **ftp [IP Address of Windows 10]** and press **Enter**. You will be prompted to enter user credentials. The need for credentials implies that an FTP server is hosted on the machine.

Figure 2.1.5: Test for FTP server

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

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

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

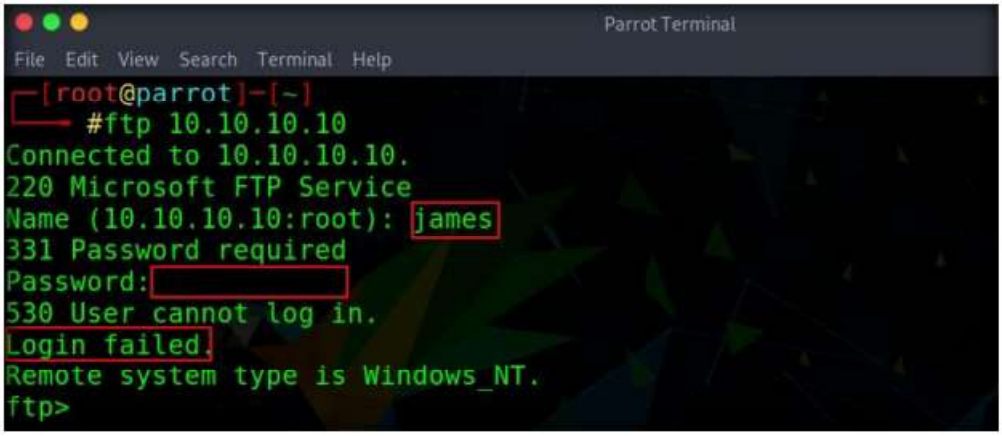


Figure 2.1.6: Test Log In

22. Now, to attempt to gain access to the FTP server, perform a dictionary attack using the THC Hydra tool.

TASK 1.3

Perform Dictionary Attack

23. Open a new terminal and jump to the root directory. Now, type **hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]** and press **Enter**.

Note: The IP address of **Windows 10** in this lab exercise is **10.10.10.10**. This IP address might vary in your lab environment.

Figure 2.1.7: Attacking the FTP server

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

Note: This might take some time to complete.

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

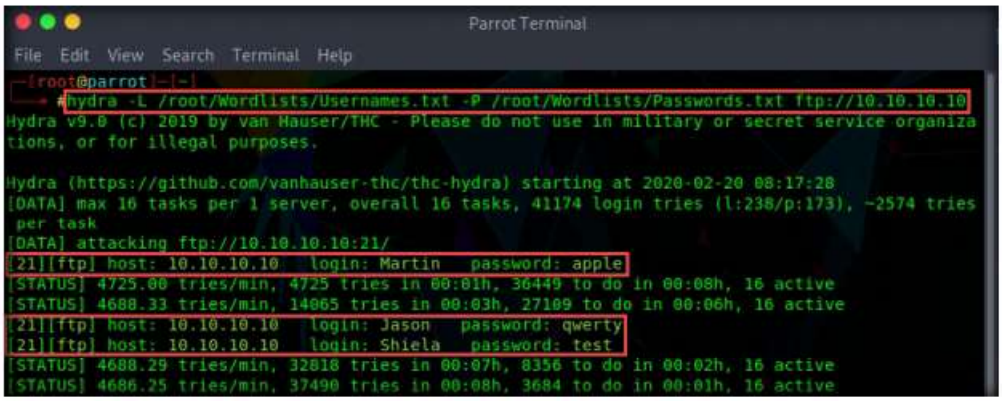


Figure 2.1.8: User credentials cracked successfully

26. Try to log in to the FTP server using one of the cracked username and password combinations. In this lab, use Martin's credentials to gain access to the server.

TASK 1.4

Access the FTP Server Remotely

27. Open a new terminal window and jump to the root directory. Now, type **ftp [IP Address of Windows 10]**, and press **Enter**.
28. Enter Martin's user credentials (**Martin** and **apple**) to check whether you can successfully log in to the server.
29. On entering the credentials, you will successfully be able to log in to the server. An ftp terminal appears, as shown in the screenshot.

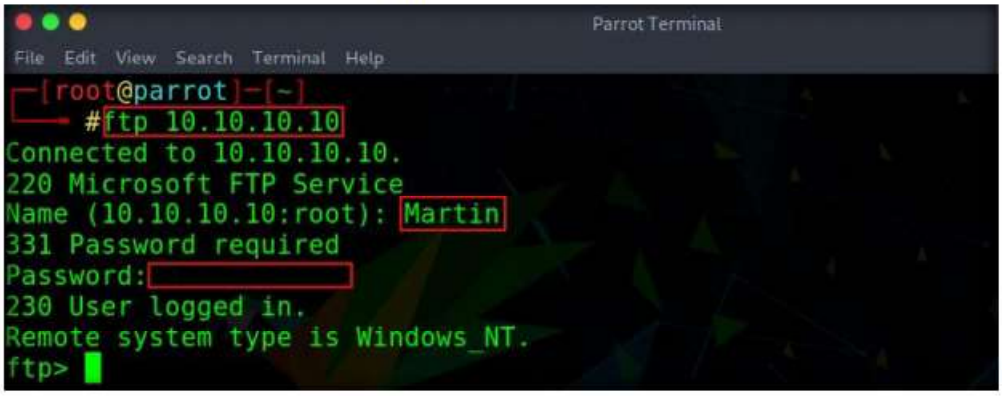


Figure 2.1.9: Logging in to FTP server

30. Now you can remotely access the FTP server hosted on the **Windows 10** machine.

31. Type **mkdir Hacked** and press **Enter** to remotely create a directory named **Hacked** on the **Windows 10** virtual machine through the ftp terminal.

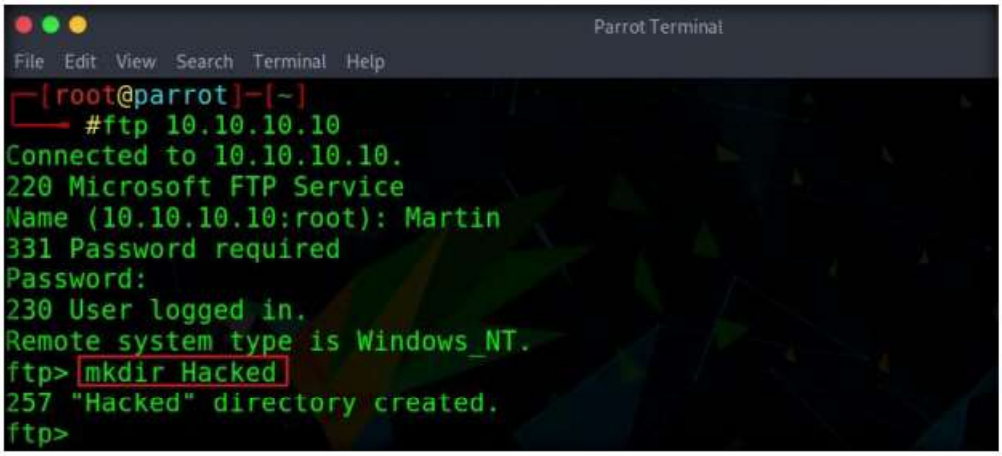


Figure 2.1.10: Creating a directory

32. Switch to the **Windows 10** virtual machine, log in with the credentials **Admin** and **Pa$$w0rd**, and navigate to **C:\FTP**.

33. View the directory named **Hacked**, as shown in the screenshot:

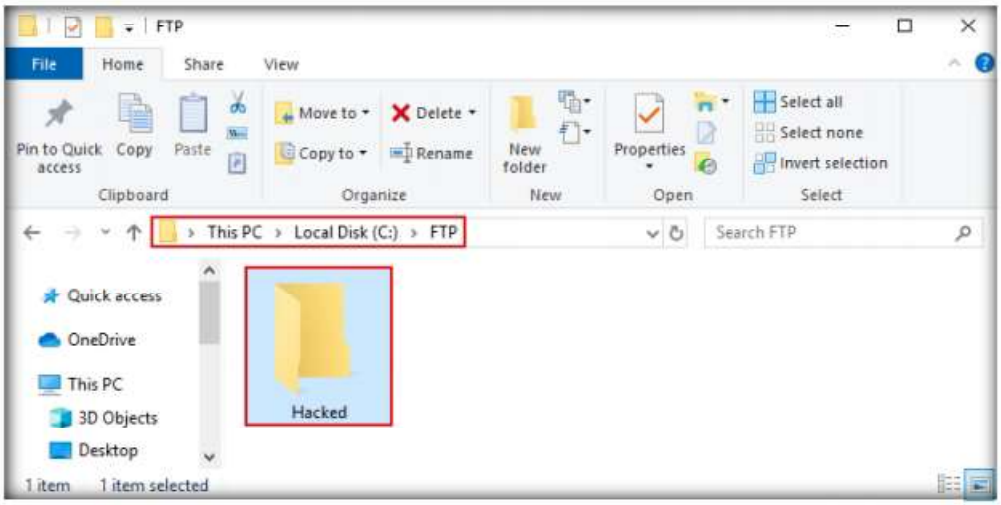


Figure 2.1.11: Viewing the created directory in Windows 10

34. You have successfully gained remote access to the **FTP server** by obtaining the appropriate credentials.

35. Switch back to the **Parrot Security** virtual machine.

36. Enter **help** to view all other commands that you can use through the FTP terminal.

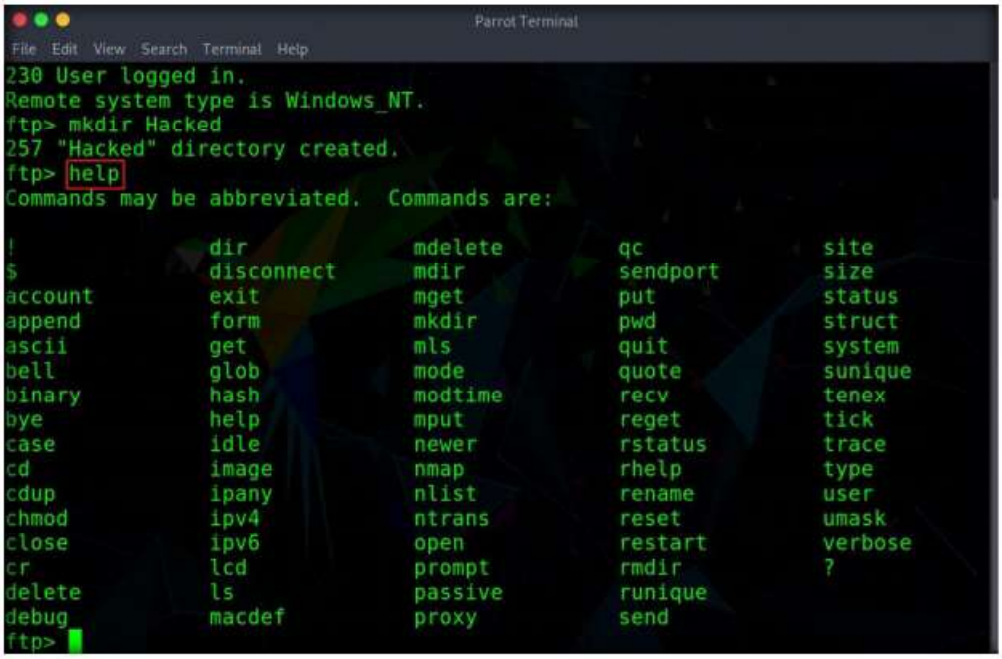


Figure 2.1.12: Viewing the other FTP commands

> You can also use other web server attack tools such as **Burp Suite** (https://portswigger.net), **JHijack** (https://sourceforge.net), **Hashcat** (https://hashcat.net), or **Metasploit** (https://www.metasploit.com) to perform various attacks on the target web server.

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

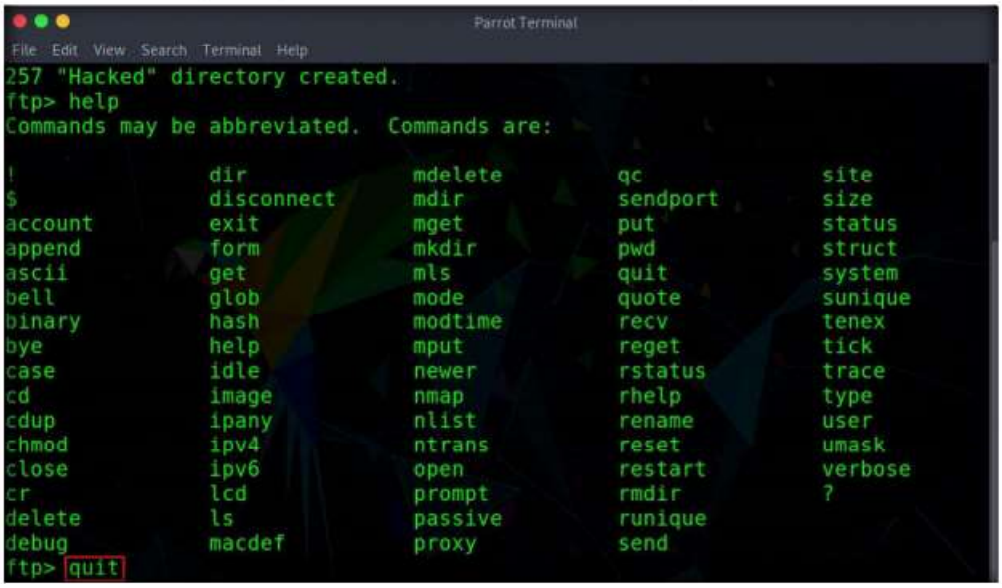


Figure 2.1.13: Exiting the FTP shell

38. This concludes the demonstration of how to crack FTP credentials using a dictionary attack and gain remote access to the FTP server.
39. Close all open windows on both the **Parrot Security** and **Windows 10** virtual machines.
40. Turn off the **Parrot Security** and **Windows 10** virtual machines.

Lab Analysis

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

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

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