acking Web Servers

Module 13

Hacking Web Servers

A webserver, which can be referred to as the hardware, the computer, or the software, is the computer application that delivers content that can be accessed through the Internet.

Lab Scenario

Most of the 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 at server side. Hackers attack web servers to steal credentials, passwords, and business information. They do this using DoS (DDoS) attacks, SYN flood, ping flood, port scan, sniffing attacks, and social engineering attacks. 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. We present 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, and IT security professionals need to be aware of common attacks on web server applications. Attackers use sniffers or protocol analyzers to capture and analyze packets. If data is sent across a network in clear text, an attacker can capture the data packets and use a sniffer to read the data. In other words, a sniffer can eavesdrop on electronic conversations. A popular sniffer is Wireshark. It's also used by administrators for legitimate purposes. One of the challenges for an attacker is to gain access to the network to capture data. If attackers have physical access to a router or switch, they can connect the sniffer and capture all traffic going through the system. Strong physical security measures help mitigate this risk.

As a penetration (pen) tester or ethical hacker for an organization, you must provide security to the company's web server. You must perform 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 help students learn to detect unpatched security flaws, verbose error messages, and much more.

The objective of this lab is to:

- Perform Web Server Security Reconnaissance
- Detect unpatched security flaws like Shellshock bug
- Crack remote passwords

Lab Environment

To carry out this, you need:

- Windows Server 2016 and Windows Server 2012 machines
- A web browser with Internet access
- Administrative privileges to run tools

Lab Duration

Time: 50 Minutes

Overview of Web Server

Most people think a web server is just the hardware, but a web server is also the software application. A web server delivers web pages on request to clients using the Hypertext Transfer Protocol (HTTP). This means delivery of HTML documents and any additional content that may be included, such as video, images, style sheets, and scripts. Many generic web servers also support server-side scripting using Active Server Pages (ASP), PHP, or other scripting languages. This means that the behavior of the web server can be scripted in separate files, while the actual server software remains unchanged. Web servers are not always used for serving the Web. They can also be found embedded in devices such as printers, routers, and webcams, and serving only a local network. The web server may then be used as a part of a system for monitoring and/or administering the device in question. This usually means that no additional software has to be installed on the client computer, since only a browser is required.

Lab Tasks

Recommended labs to demonstrate webserver hacking:

- Performing Web Server Reconnaissance using **Skipfish**
- Footprinting a Web Server using the **httprecon** Tool
- Footprinting a Web Server using **ID Serve**
- **Uniscan** Web Server Fingerprinting in Kali Linux
- Cracking **FTP Credentials** using **Dictionary Attack**

Lab Analysis

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

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

Lab

1

Performing Web Server Reconnaissance using Skipfish

Skipfish is a web application (deployed on a webserver) security reconnaissance tool that performs recursive crawl and dictionary-based probes on applications.

Lab Scenario

Every attacker tries to collect as much information as possible about the target web server. The attacker gathers the information and then analyzes the information in order to find lapses in the current security mechanism of the web server.

Lab Objectives

The objective of this lab is to help the students learn how to:

a. Perform web server reconnaissance using Skipfish

Lab Environment

To perform the lab, you need:

- Windows Server 2016 machine
- Windows Server 2012 virtual machine
- Kali Linux virtual machine

Lab Duration

Time: 15 Minutes

Overview of the Lab

This lab demonstrates how to perform security reconnaissance on a webserver and examine the findings.

Lab Tasks

1. Click **Start**, click the **downwards arrow** and then click **Wampserver64** to launch the WampServer application.

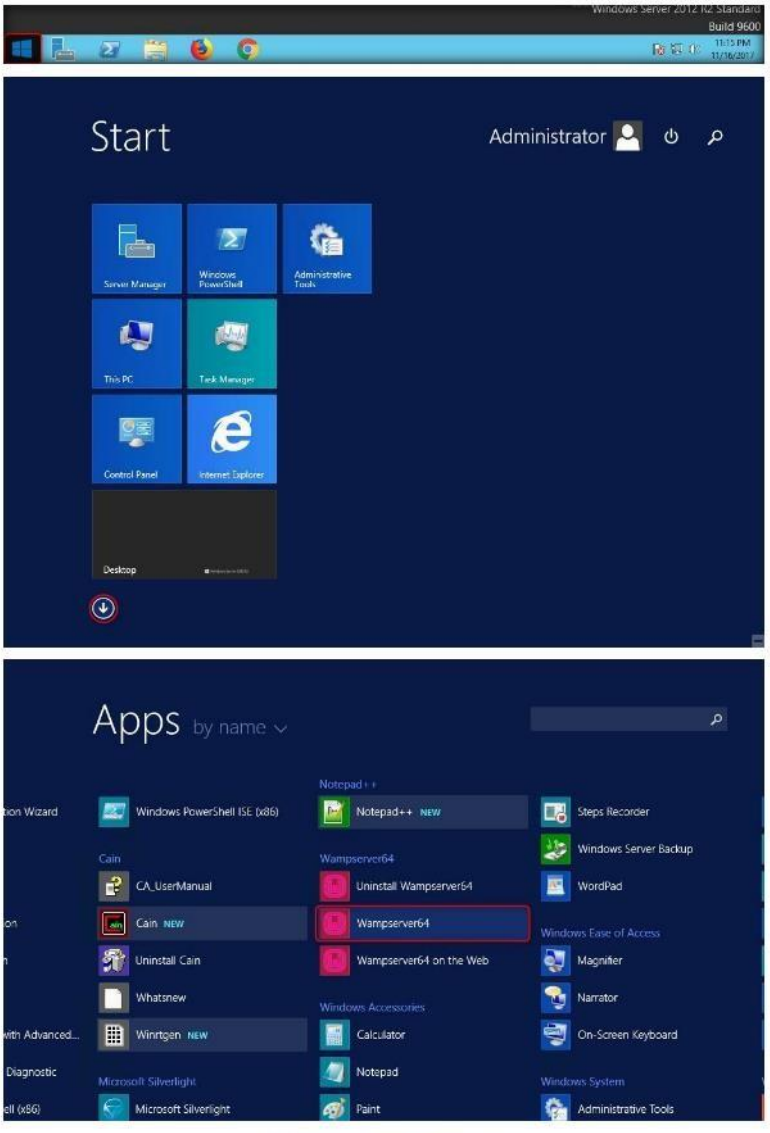

FIGURE 1.1: Starting WampServer

2. Log in to the **Kali Linux** virtual machine and launch a command line **terminal**.

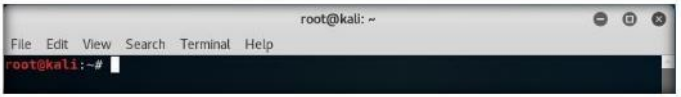

FIGURE 1.2: Launching a Command Line Terminal

3. Perform security reconnaissance on a web server using Skipfish. The target is the wordpress website **http://[IP Address of Windows Server 2012]** .

4. Specify the output directory and load a dictionary file based on the web server requirement. In this lab we are naming output directory as **test**.

5. Type **skipfish -o /root/test -S /usr/share/skipfish/dictionaries/complete.wl http://[IP Address of Windows Server 2012]:8080** and press **Enter**.

   Note: IP address may vary in your lab environment.

FIGURE 1.3: Initiating the Scan

6. Upon receiving this command, Skipfish performs a heavy **brute-force attack** on the web server by using **complete.wl** dictionary file, creates a directory named **test** in the **root** location, and stores the result in index.html inside this location.

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

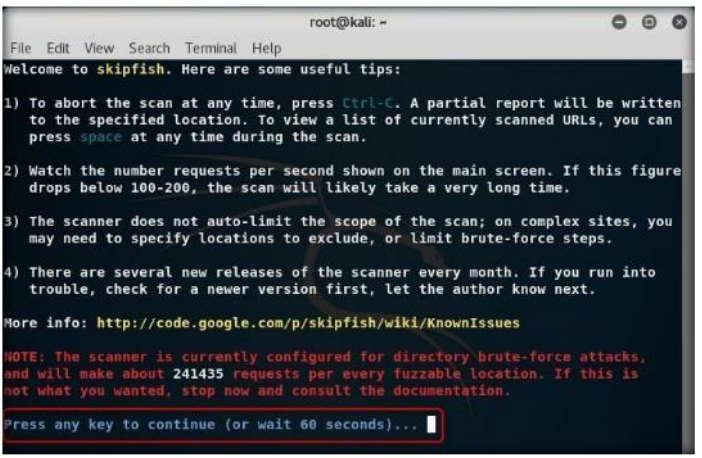

FIGURE 1.4: Initiating the Scan

8. Skipfish scans the web server as shown in the following screenshot:

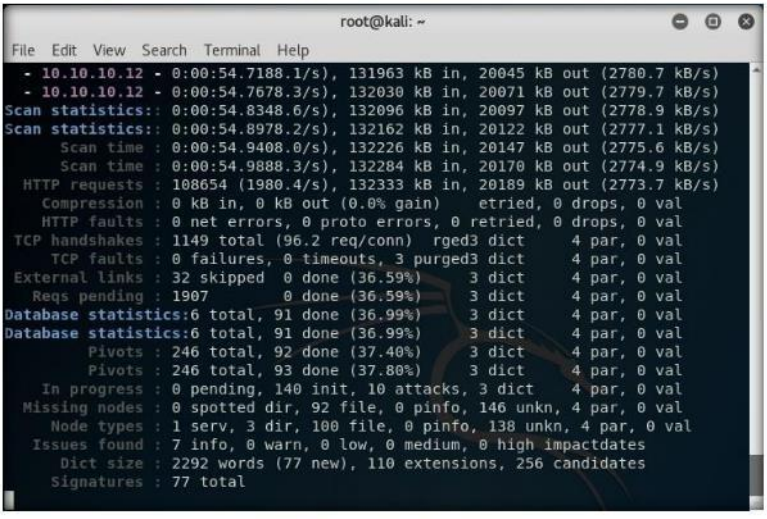

FIGURE 1.5: Skipfish Scanning the Web Server

9. Note that Skipfish takes some time (approximately 20 minutes) to complete the scan.

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

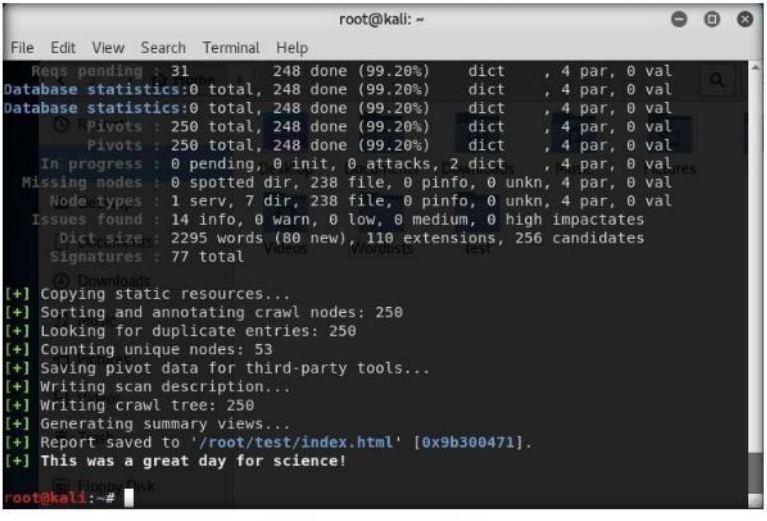

FIGURE 1.6: Completion of the Scan

10. On completion of the scan, Skipfish generates a report and stores it in the **test** directory (in **root** location). Navigate to **Home** → **test** and double-click **index.html** to view the scan result.

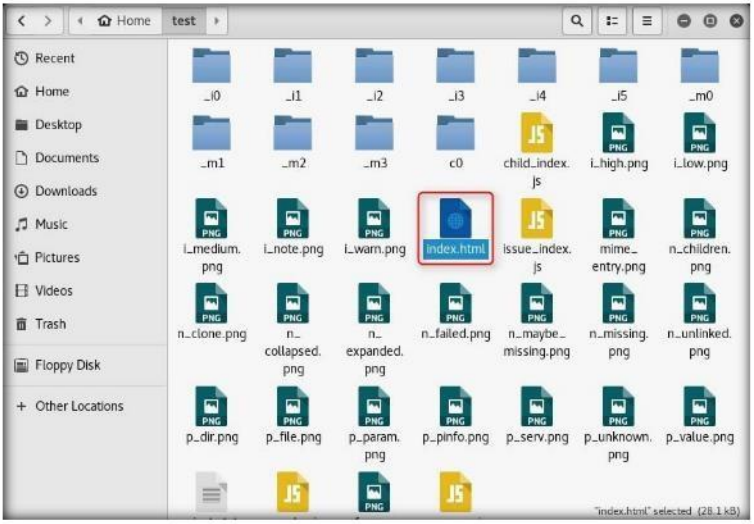

FIGURE 1.7: Viewing the Scan Result

11. The Skipfish crawl result appears in the web browser, displaying the summary overviews of document types and issue types found, as shown in the following screenshot:

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

FIGURE 1.8: Examining the Scan Result

12. Expand each node to view detailed information regarding the result.
13. Analyze an issue found in the web server. Click a node under the **Issue type overview** section to expand it.
14. Analyze the **Incorrect or missing charset** issue.

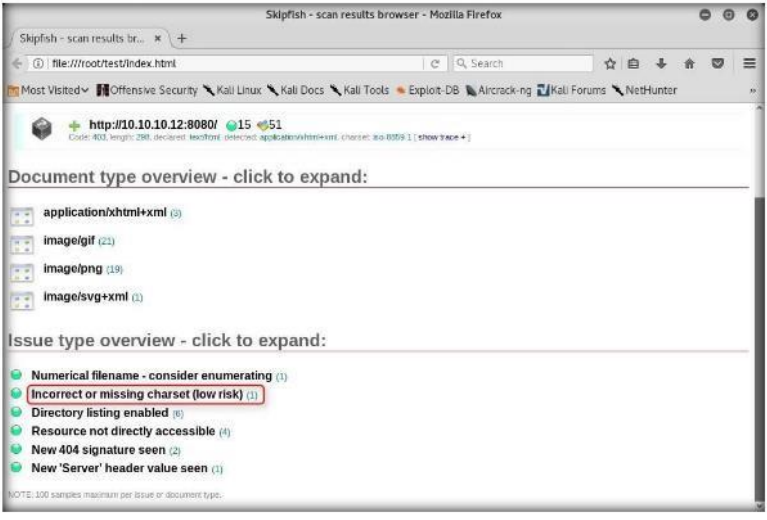

FIGURE 1.9: Examining the Scan Result

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

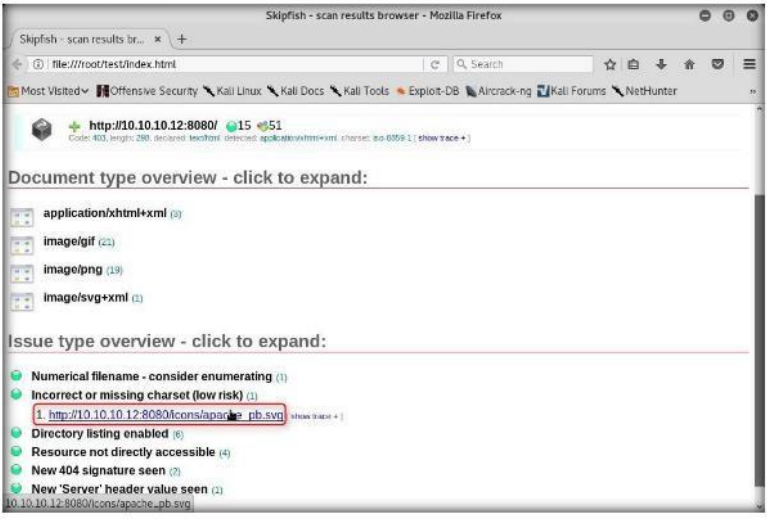

FIGURE 1.10: Examining the Scan Result

16. The webpage appears as shown in the following screenshot:

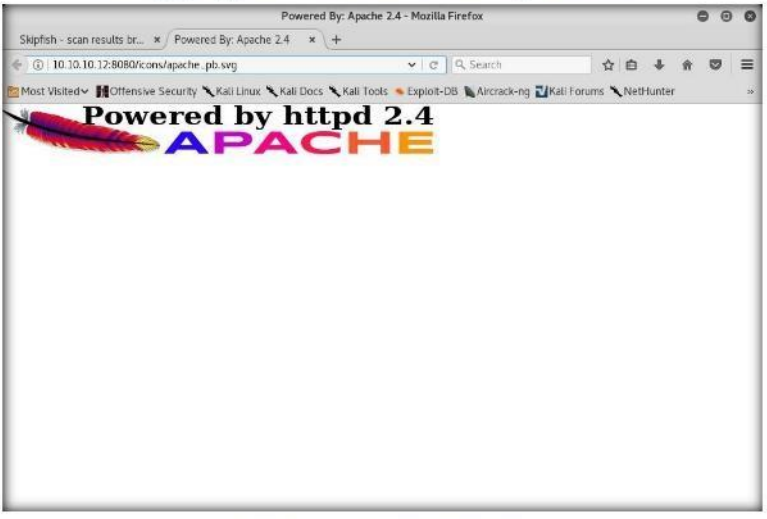

FIGURE 1.11: Examining the Scan Result

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

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

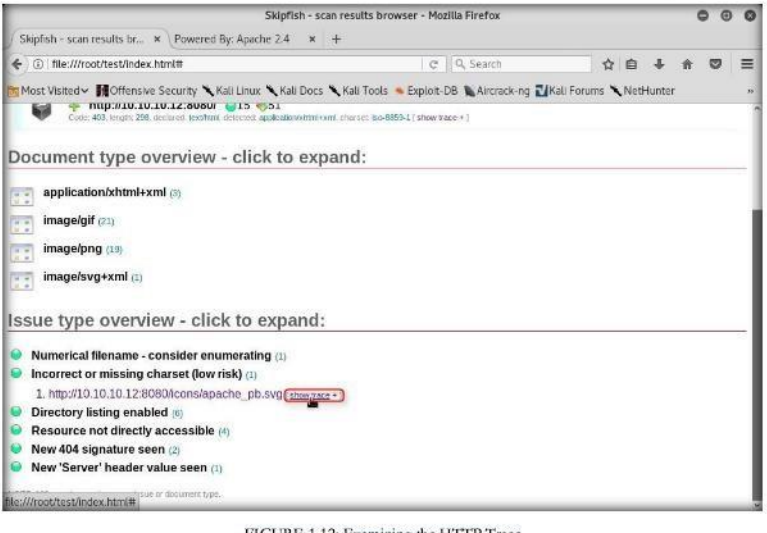

FIGURE 1.12: Examining the HTTP Trace

19. A HTTP trace window appears on the webpage, displaying the complete **HTML session**, as shown in the following screenshot:

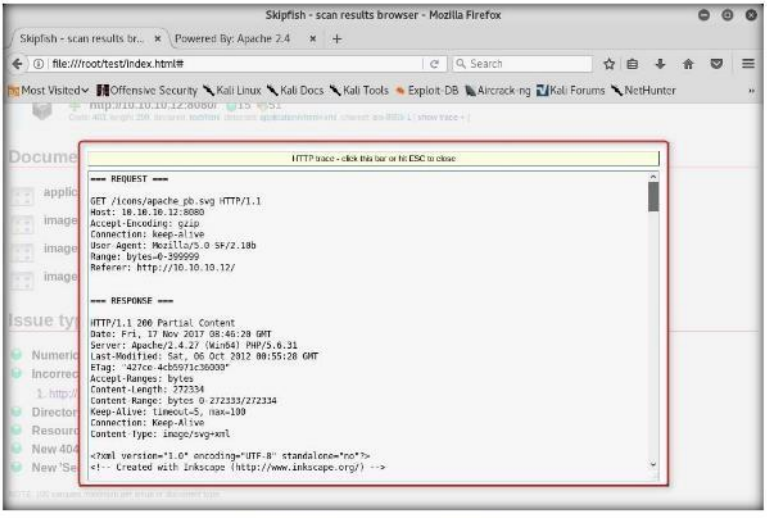

FIGURE 1.13: Examining the HTTP Trace

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

20. Examine other vulnerabilities, and patch them in the process of securing the web server.

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

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

Lab

2

Footprinting a Web Server using the httprecon Tool

The httprecon project undertakes research in the field of web server fingerprinting, also known as http fingerprinting.

Lab Scenario

Web applications can publish information, interact with Internet users, and establish an e-commerce/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 (e.g., fraud, theft, vandalism, and terrorism), they are far more dangerous. Organizations can face monetary losses, damage to reputation, or legal action if an intruder successfully violates the confidentiality of their data. DoS attacks are easy for attackers to attempt because of the number of possible attack vectors, the variety of automated tools available, and the low skill level needed to use the tools. DoS attacks, as well as threats of initiating DoS attacks, are also increasingly being used to blackmail organizations. To be an expert ethical hacker and pen tester, you must understand how to perform footprinting on webservers.

Lab Objectives

The objective of this lab is to help students learn to footprint web servers. It will teach you how to:

- Use the httprecon tool
- Get webserver footprint

Lab Environment

To carry out the lab, you need:

- The **Httprecon** tool, available at **Z:\CEH-Tools\CEHv10 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon**. You can download the latest version of **httprecon** from the link

http://www.computec.ch/projekte/httprecon. If you decide to download the **latest version**, then screenshots shown in the lab might differ.

- Windows Server 2016
- A web browser with Internet access
- Administrator privileges

Lab Duration

Time: 5 Minutes

Overview of httprecon

Httprecon is a tool for advanced **web server** fingerprinting, similar to **httprint**. The goal is highly **accurate** identification of **httpd** implementations.

Lab Tasks

1. In Windows Server 2016 machine, navigate to **Z:\CEH-Tools\CEHv10 Module 13 Hacking Web Servers\Web Server Footprinting Tools\httprecon** and double-click **httprecon.exe** to launch the application.
2. If an **Open File - Security Warning** pop-up appears, click **Run**.
3. The main window of **httprecon** appears, as shown in the following screenshot:

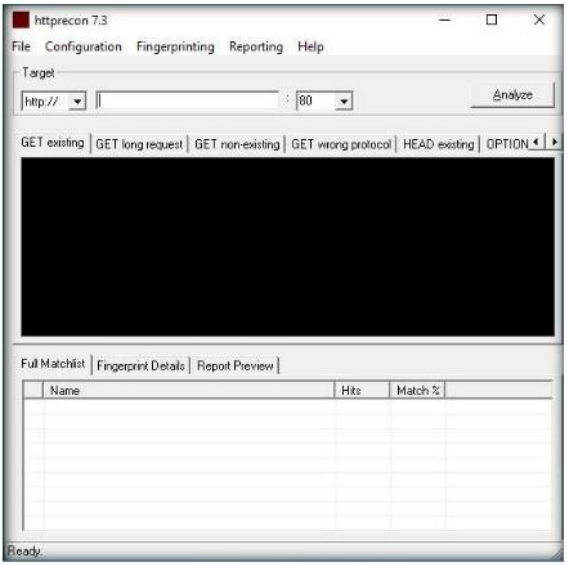

FIGURE 2.1: httprecon main window

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

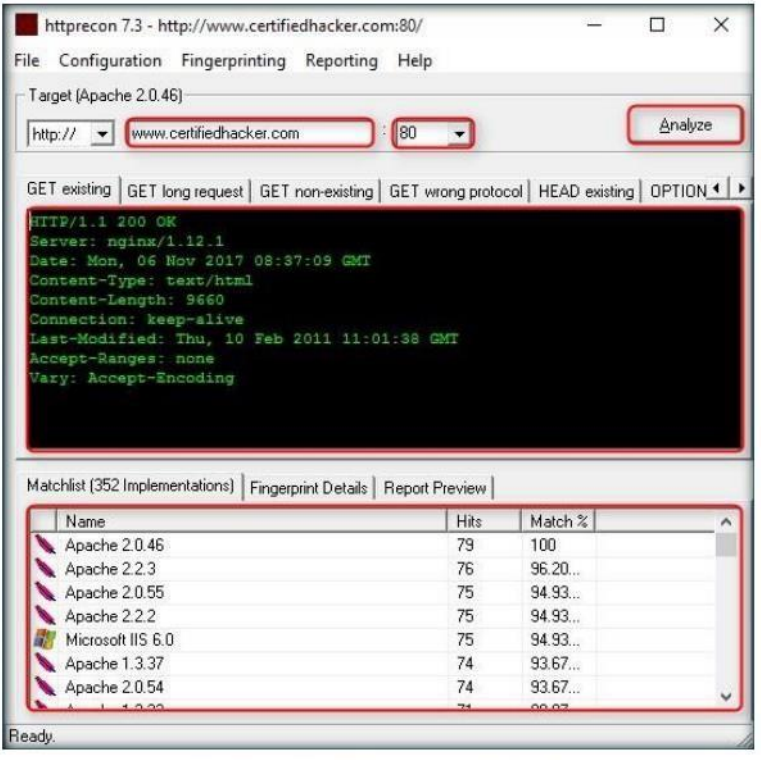

FIGURE 2.2: The footprint result of the entered website

7. Scroll down the **Get existing** tab, and observe the server used (**Microsoft IIS**), its version (**6.0**), and the server-side application used to develop the webpages (**ASP.NET**).
8. When attackers obtain this information, they research the vulnerabilities present in **ASP.NET** and **IIS version 6.0** 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 the GET requests. Then click the **Fingerprint Details** tab.

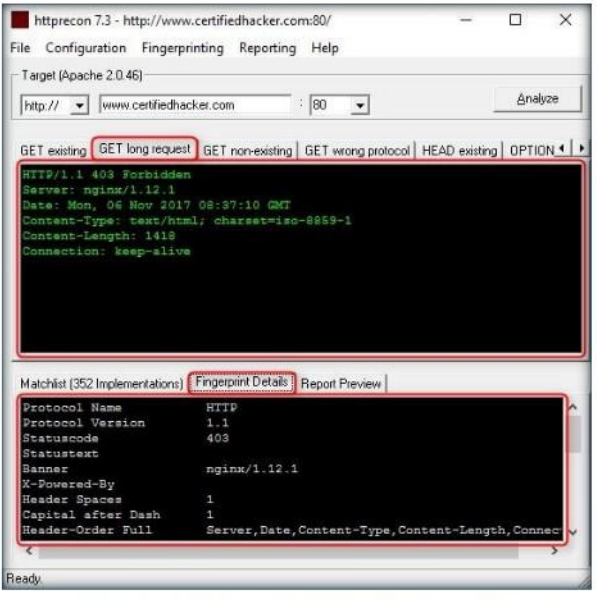

FIGURE 2.3: The fingerprint and GET long request result of the entered website

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 the vulnerabilities in HTTP to perform malicious activities such as sniffing over the HTTP channel, which might result in revealing sensitive data such as user credentials.

Lab Analysis

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

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

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

Lab

3

Footprinting a Web Server using ID Serve

ID Serve is a simple, free, small (26 Kbytes), and fast general-purpose Internet server identification utility.

Lab Scenario

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. In this lab you will learn the banner grabbing technique to determine a remote target system using ID Serve. In order to be an expert ethical hacker and pen tester, its important to understand how to footprint a webserver.

Lab Objectives

This lab shows how to footprint webservers and how to use ID Serve. It teaches how to:

- Use the ID Serve tool
- Get a webserver footprint

Lab Environment

To carry out the lab, you need:

- ID Serve located at **Z:\CEH-Tools\CEHv10 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve**. You can also download the latest version of **ID Serve** from the link **http://www.grc.com/id/idserve.htm**. If you decide to download the latest version, then screenshots shown in the lab might differ
- Windows Server 2016
- A Web browser with Internet access
- Administrator privileges to run tools

Lab Duration

Time: 5 Minutes

Overview of ID Serve

ID Serve determines the domain name associated with an IP address. This process is known as a reverse DNS lookup and is useful when checking firewall logs or receiving an IP address. Not all IP addresses that have a forward direction lookup (Domain-to-IP) have a reverse (IP-to-Domain) lookup, but many do.

Lab Tasks

1. In Windows Server 2016 machine, navigate to **Z:\CEH-Tools\CEHv10 Module 13 Hacking Web Servers\Web Server Footprinting Tools\ID Serve** and double-click **idserve.exe**.
2. If an **Open File - Security Warning** pop-up appears, click **Run**.
3. The main window of ID Server appears. Click the **Server Query** tab.

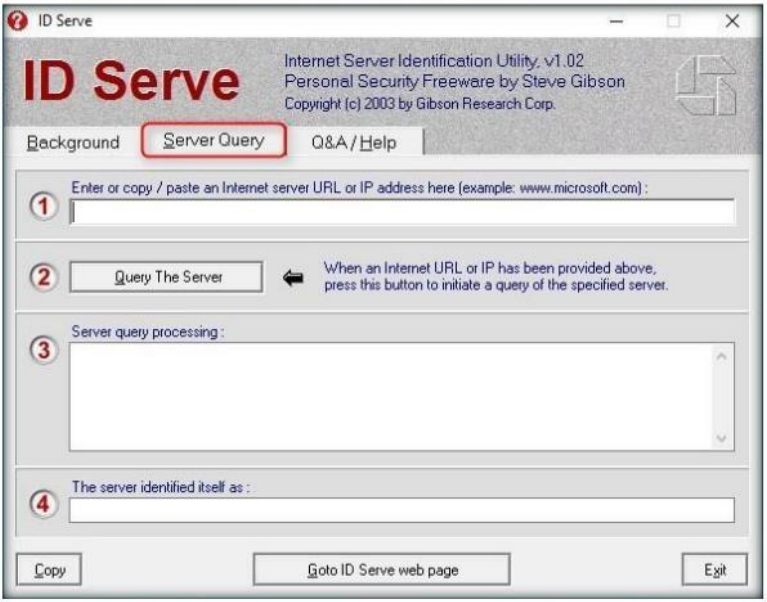

FIGURE 3.1: Welcome screen of ID Serve

4. In option **1**, enter the URL (**http://www.certifiedhacker.com**) you want to **footprint** in the **Enter or copy/paste an Internet server URL or IP address** section.
5. Click **Query the Server** to start querying the website.

6. After the completion of the **query**, ID Serve displays the results of the entered website, as shown in the following screenshot:

FIGURE 3.2: ID Serve detecting the footprint

Note: The result might vary in your lab environment.

7. By obtaining this information, attackers may perform vulnerability analysis on of that particular version of webserver and implement various techniques to perform exploitation.

Lab Analysis

Document all the server information.

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

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

Lab

4

Uniscan Web Server Fingerprinting in Kali Linux

Uniscan is a simple Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.

Lab Scenario

Webserver fingerprinting is an essential task for any penetration tester. Before proceeding to hacking/exploiting a webserver, it is critical for the penetration tester to know the type and version of the webserver as most of the attacks/exploits are specific to the type and version of 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 for mitigation of such attacks on the server.

Lab Objectives

The objective of this lab is to help the students learn how to perform fingerprinting of a webserver

Lab Environment

To perform the lab, you need:

- A computer running Windows Server 2012
- Kali Linux running as a virtual machine

Lab Duration

Time: 15 Minutes

Overview of Uniscan

Uniscan is an open source project and is preinstalled in kali linux distribution. It is a versatile server fingerprinting tools which not only performs the simple commands like ping, traceroute, nslookup, etc. but can also do static, dynamic and stress checks

on a web server. Apart from scanning websites, uniscan also has the feature of performing automated bing and google searches on provided IPs. Uniscan takes all this and combines them in a comprehensive report file for the user.

Lab Tasks

1. Click **Start** and then click **Wampserver64** to launch the WampServer application. Wait till all the services are running and the wamp icon in the taskbar turns green.

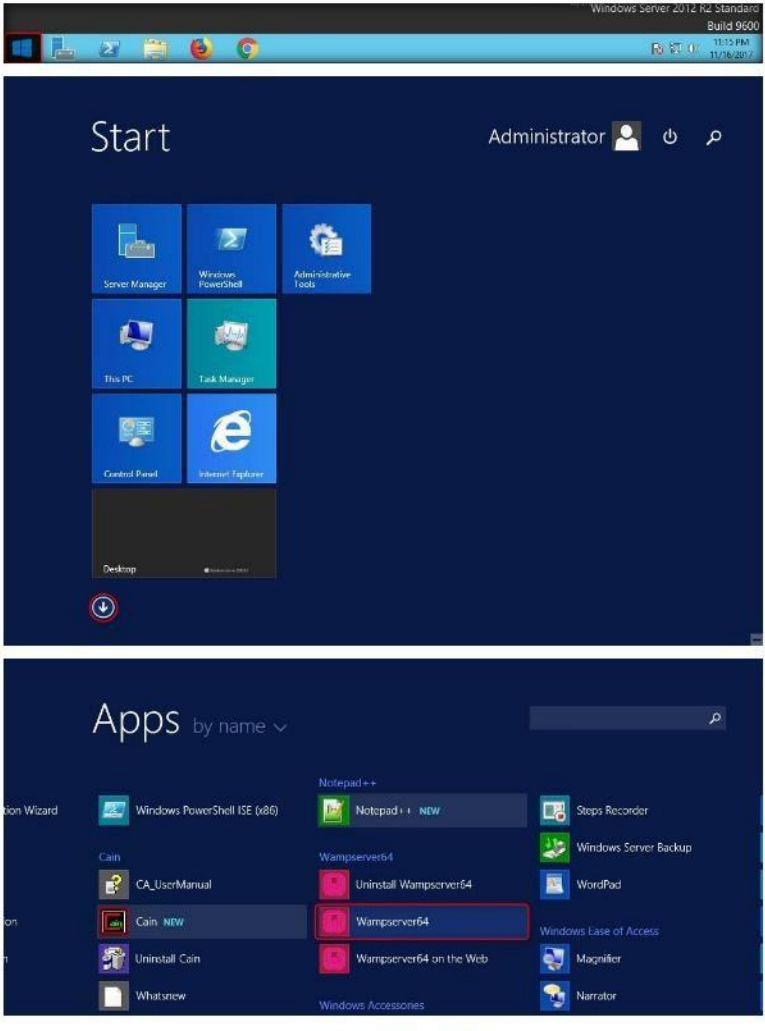

FIGURE 4.1: Starting WampServer

2. Log in to the **Kali Linux** virtual machine and launch a command line **terminal**.

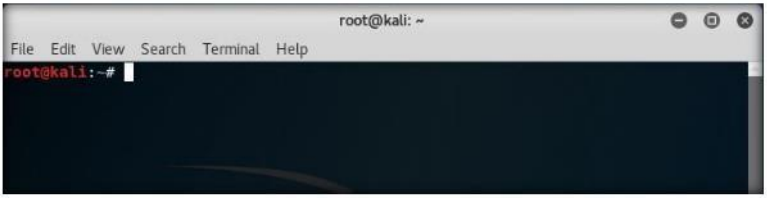

FIGURE 4.2: Launching a Command Line Terminal

3. In the terminal window, type **uniscan -h** and hit **Enter** to display the help options of uniscan.

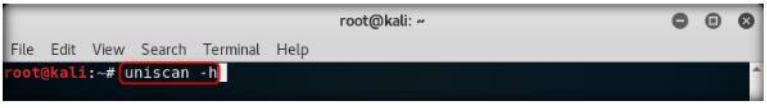

FIGURE 4.3: Uniscan help command

4. The help menu appears as shown in the screenshot. First use the **-q** command to search for the directories of the web server.

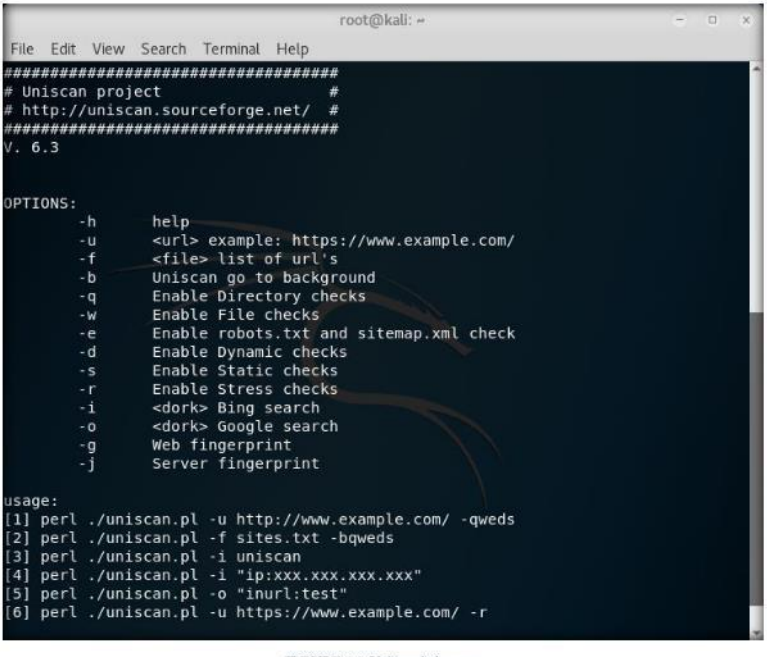

FIGURE 4.4: Uniscan help menu

5. In the terminal window type **uniscan -u http://10.10.10.12:8080/CEH -q** and hit **Enter** to start the scan for directories.

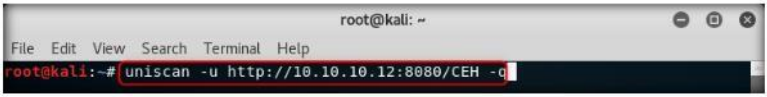

FIGURE 4.5: Run uniscan with -q command

6. Uniscan starts performing different tests on the webserver and finds out **web directories** as shown in the screenshot.

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

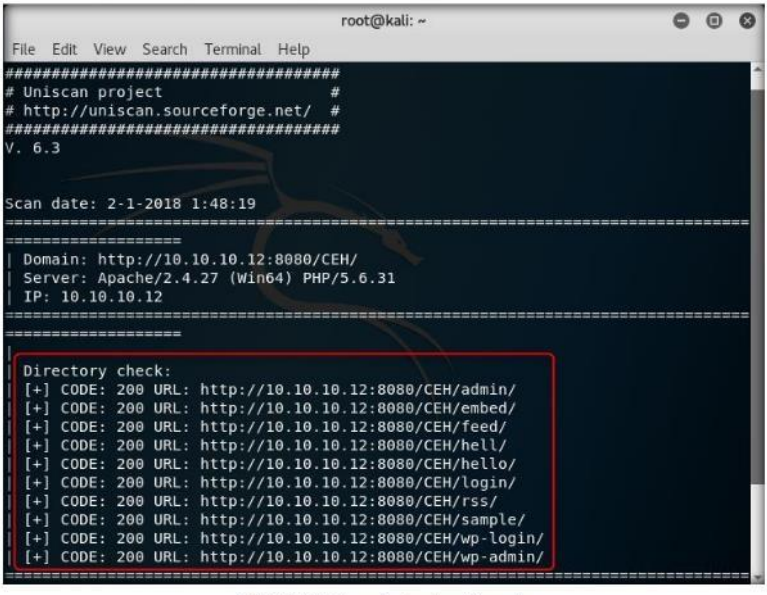

FIGURE 4.6: Uniscan showing found directories

7. Now we will run uniscan using two options together. Here **-w** and **-e** are used together to enable file check, robots.txt and sitemap.xml check. In the terminal window type **uniscan -u http://10.10.10.12:8080/CEH -we** and hit **Enter** to start the scan.

FIGURE 4.7: Uniscan command with -we option

8. Uniscan starts file check and shown output as shown in the screenshot.

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

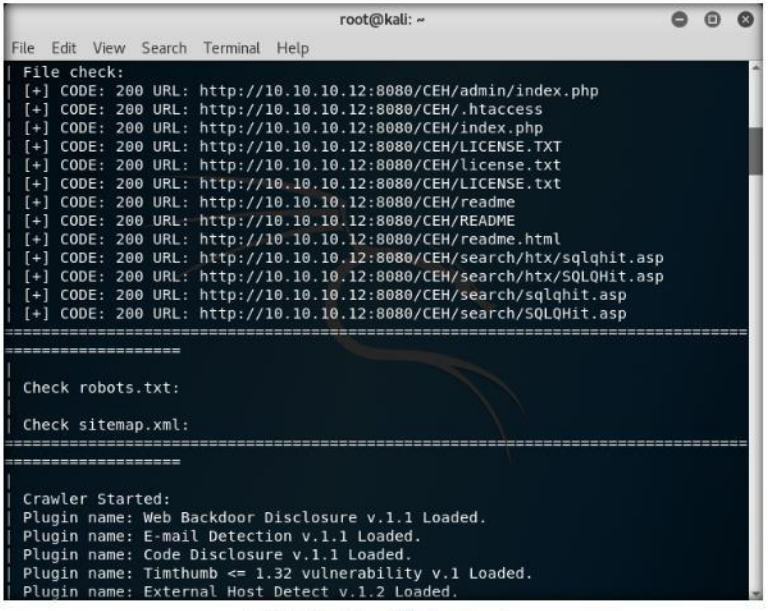

FIGURE 4.8: Uniscan displaying scan results

9. Now, we shall use the dynamic testing option by giving the command **-d**. Type **uniscan -u http://10.10.10.12:8080/CEH -d** and hit Enter to start dynamic scan on the webserver.

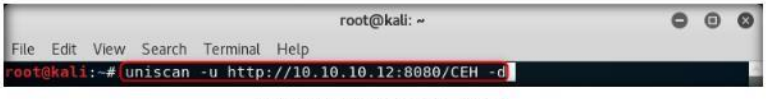

FIGURE 4.9: Run uniscan with -d option

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

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

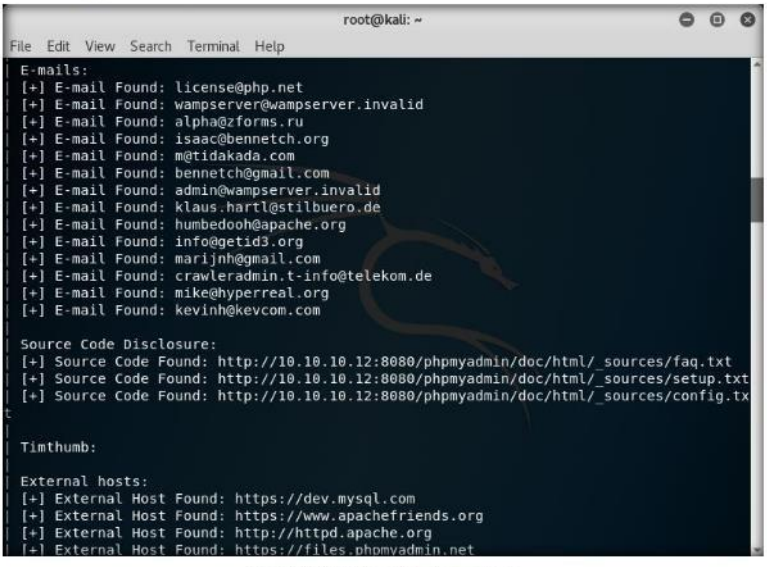

FIGURE 4.10: Uniscan displaying scan results

11. Then uniscan displays the **PHP info** as given in the screenshot below.

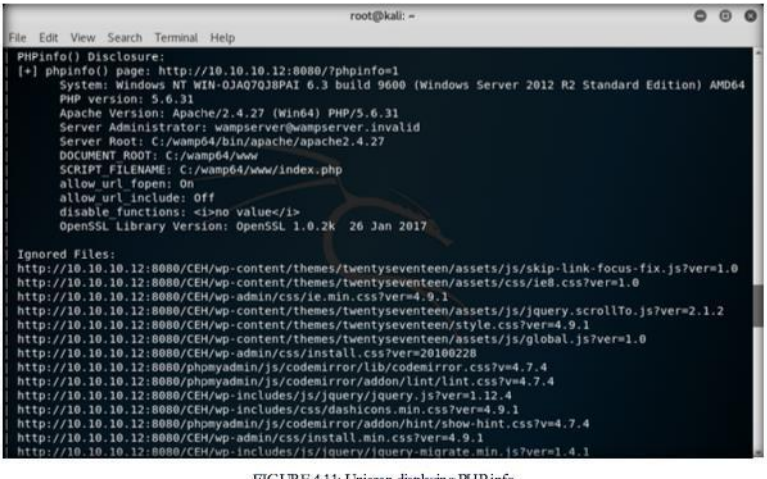

FIGURE 4.11: Uniscan displaying PHP info

12. After the scanning, navigate to **/usr/share/uniscan/report** and double-click **10.10.10.12.html** to view the scan report.

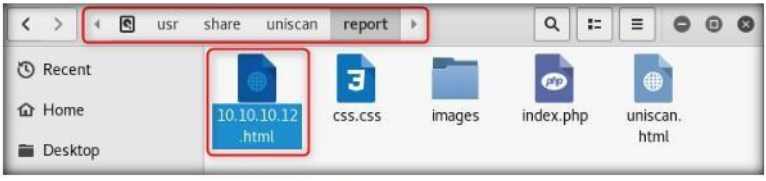

FIGURE 4.12: Scan report generated

13. The report opens in a browser giving you all the **scan details** in a more comprehensive way.

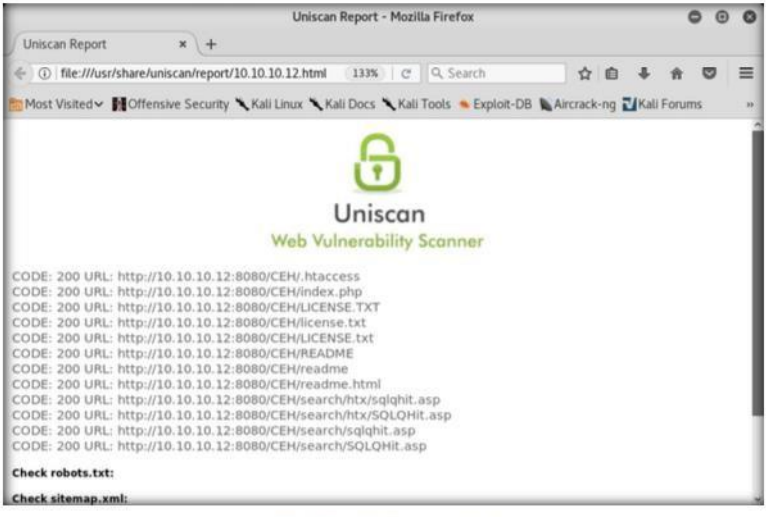

FIGURE 4.13: View the scan report

Lab Analysis

Document the output and give your views about the security posture of the server.

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

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

Lab

5

Cracking FTP Credentials using Dictionary Attack

A dictionary attack bypasses the authentication mechanism employed in a password-protected machine by trying numerous combinations of keywords present in a dictionary file.

Lab Scenario

In this phase of web server hacking, an attacker tries to crack web server passwords. The attacker tries all possible techniques to extract passwords, including password guessing, dictionary attacks, brute force attacks, hybrid attacks, pre-computed hashes, rule-based attacks, distributed network attacks, rainbow attacks, etc. The attacker needs patience, as some of these techniques are tedious and time-consuming. The attacker can also use automated tools such as Brutus, THC-Hydra, etc. to crack web passwords.

Lab Objectives

The objective of this lab is to help the students how to:

a. Perform Nmap scan to find whether an ftp port is open

b. Perform a dictionary attack using hydra

Lab Environment

To perform the lab, you need:

- Windows Server 2016 virtual machine
- Windows 10 virtual machine
- Kali Linux virtual machine

Lab Duration

Time: 10 Minutes

Overview of Dictionary Attacks

A Dictionary/wordlist contains thousands of words that are used by password cracking tools to break into a password-protected system. Dictionary attacks are often successful because many users insist on using ordinary words as passwords.

Lab Tasks

1. Before beginning this lab, launch the **Windows 10** virtual machine from **VMware Workstation** and log in.
2. Launch the **Kali Linux** virtual machine from **VMware Workstation** and log in.
3. Double-click **CEH-Tools** shared folder on Desktop and navigate to **CEHv10 Module 13 Hacking Web Servers**, and copy the **Wordlists** folder and paste it in the Home directory as shown in the screenshot:

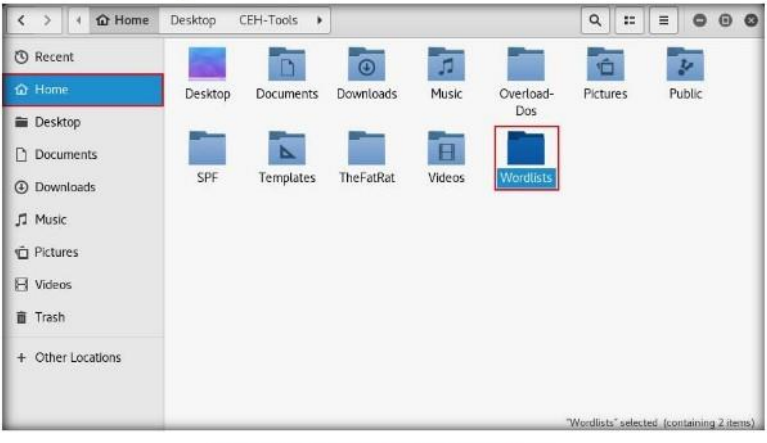

FIGURE 5.1: Wordlists folder in the Home directory

4. Perform an **Nmap scan** on the target machine (**Windows 10**) to check if the FTP port is open.

5. Launch a command line terminal in the **Kali Linux** machine and enter **nmap -p 21 [IP Address of Windows 10]**.

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

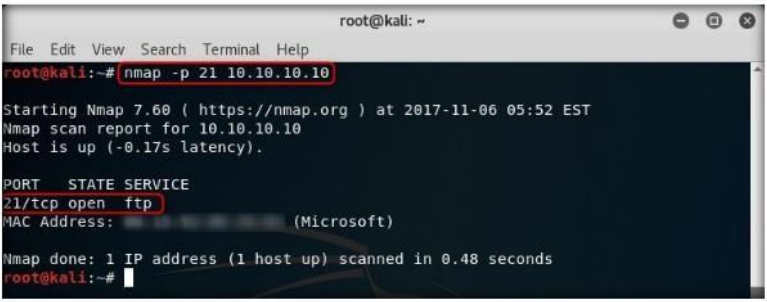

FIGURE 5.2: Performing Nmap Port Scan

6. Observe that **port 21** is open in **Windows 10**.
7. Check if an FTP server is hosted on the Windows 10 machine.
8. Enter **ftp [IP Address of Windows 10]**. You will be prompted to enter user credentials, which implies that an FTP server is hosted on the machine and requires credentials.

Note: The IP Address of **Windows 10** in this lab is **10.10.10.10**.

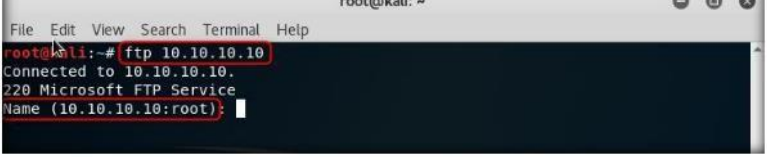

FIGURE 5.3: Test for FTP Server

9. Try to enter random usernames and passwords in an attempt to gain ftp access.

Note: The password you enter will not be visible.

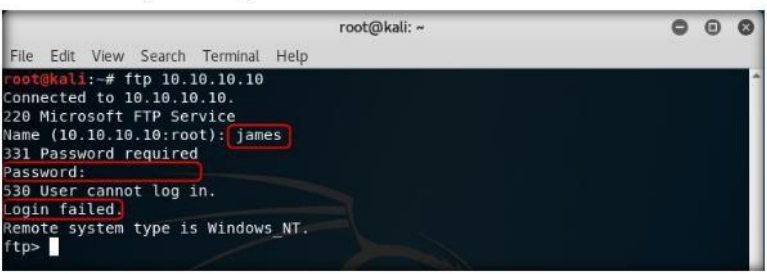

FIGURE 5.4: Test Log In

10. Perform an attack on the FTP server in an attempt to gain access to it.
11. This lab uses hydra.
12. Open a new command line terminal.
13. Type **hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://[IP Address of Windows 10]**.

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

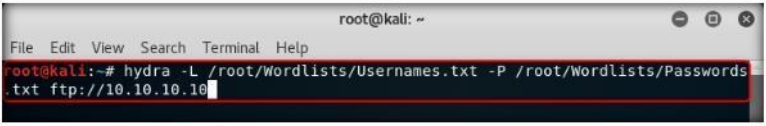

FIGURE 5.5: Attacking the FTP Server

14. Hydra tries various combinations of usernames and passwords (present in the Usernames.txt and Passwords.txt files) on the ftp server, and starts displaying the cracked usernames and passwords, as shown in the following screenshot:

FIGURE 5.6: Hydra Cracking User Credentials

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

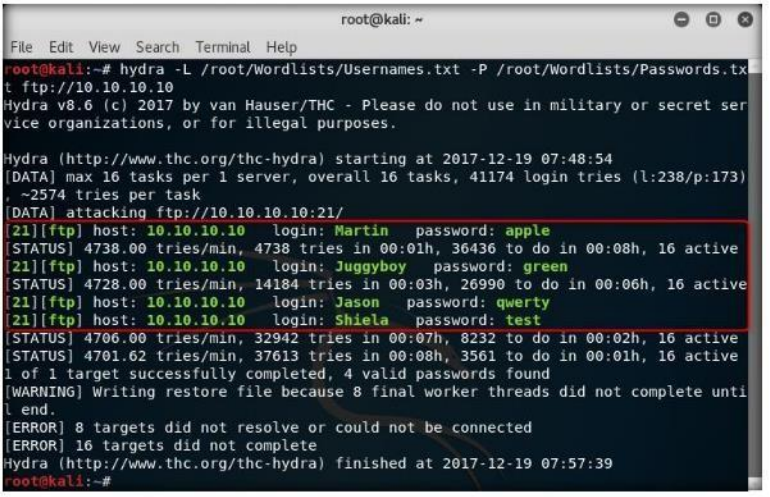

FIGURE 5.7: User Credentials Cracked Successfully

16. 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.

17. Open a command line terminal and enter **ftp [IP Address of Windows 10]**.

18. Enter Martin's user credentials (**Martin/apple**) to check whether you can successfully log in to the server.

19. On entering the credentials, you will be able to successfully log in to the server. An ftp terminal appears as shown in the following screenshot:

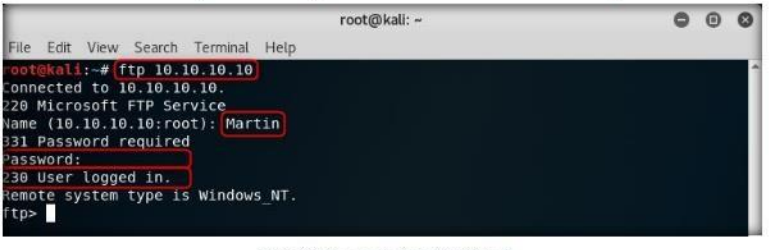

FIGURE 5.8: Logging in to FTP Server

20. Remotely access the FTP server hosted on the Windows 10 machine.

21. Enter **mkdir Hacked** to create a directory named **Hacked** through the ftp terminal.

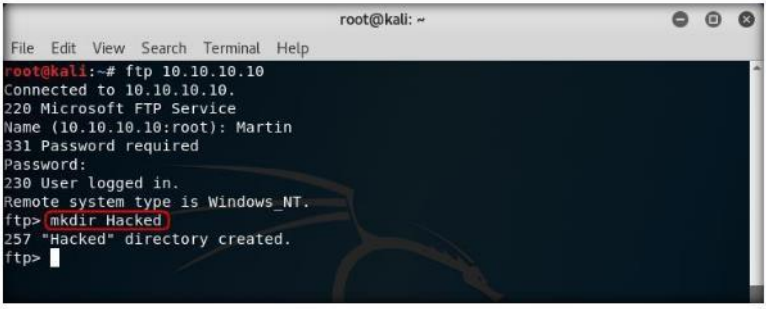

FIGURE 5.9: Creating a Directory

22. Switch to the **Windows 10** virtual machine and navigate to C:\FTP.

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

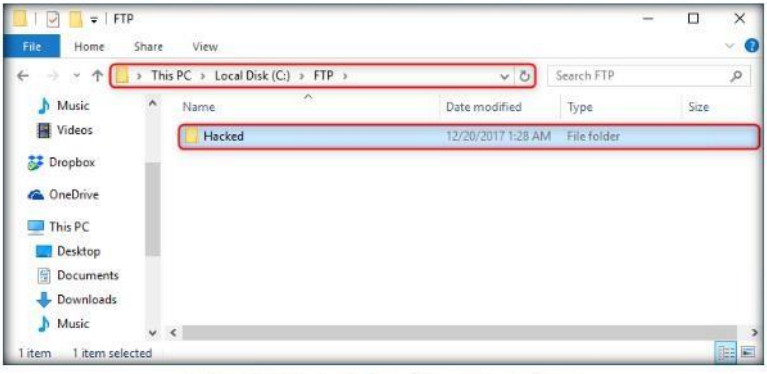

FIGURE 5.10: Viewing the Created Directory in Windows 10

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

25. Switch to the **Kali Linux** virtual machine.

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

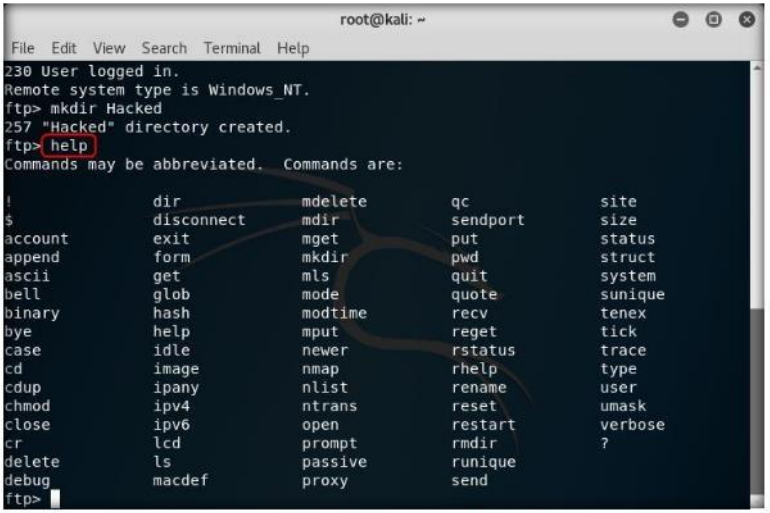

FIGURE 5.11: Viewing the Other FTP Commands

27. On completing the lab, enter **quit** to exit the FTP terminal.

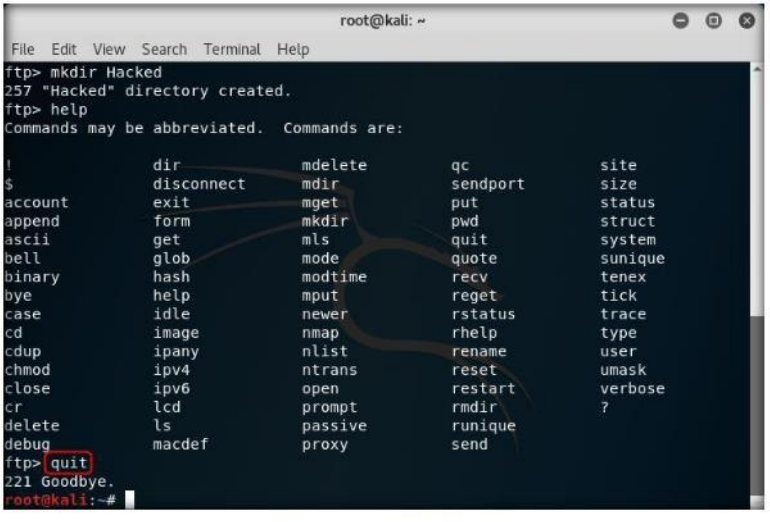

FIGURE 5.12: Exiting the FTP Shell

28. You have gained **remote access** to FTP server.

Lab Analysis

Document the output.

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

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