



Performing Reconnaissance from the WAN

ETHICAL HACKING & LAB # 1

Student Info

Name : SRIJA PABBA

Student ID: 00866719

Email:

spabb6@unh.newhaven.edu

Table of Contents

I.	Executive Summary	2
	Highlights	
	Objectives	
II.	Lab Description Details	2
	Include Steps Taken, Notes, & Screen Shots demonstrating completion of lab objectives	
III.	Supporting Evidence.....	12
IV.	Conclusion & Wrap-Up	13
	Summary with observations, Success & Failures, Challenges	

Executive Summary

Highlights

In this lab, I will engage in external reconnaissance by scanning a network protected by a pfSense firewall. Using a Kali 2 Attack Machine, I will conduct port scanning and banner grabbing to identify open ports and discover the operating systems and applications running on machines behind the firewall. The lab will conclude with me obtaining administrator credentials and using Remote Desktop Protocol (RDP) to access a Windows Server.

Objectives

The objective of this lab is for me to practice network reconnaissance techniques by identifying exposed services and vulnerabilities through the pfSense firewall. I will use tools such as nmap to scan ports, perform OS and service identification, retrieve hashed passwords from the `/etc/shadow` file, and ultimately gain access to a Windows Server using the discovered credentials.

Lab Description Details

Nmap scan on www.campus.edu

The screenshot displays a web browser window with the URL `lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL`. The page is titled "Ethical Hacking and Systems Defense" and "Performing Reconnaissance from the WAN". It contains a "SAMPLE CHALLENGE" button and a terminal window showing the execution of an Nmap scan on `www.campus.edu`.

Step 6: Notice the flag of 999818. Click on the Challenge icon and type the flag number into the answer box. This is just to show you how to capture Challenge Flags you will see throughout this lab.

Step 7: Type the following Linux command and press Enter, to clear all output from the terminal.

```
root@kali2:~# clear
```

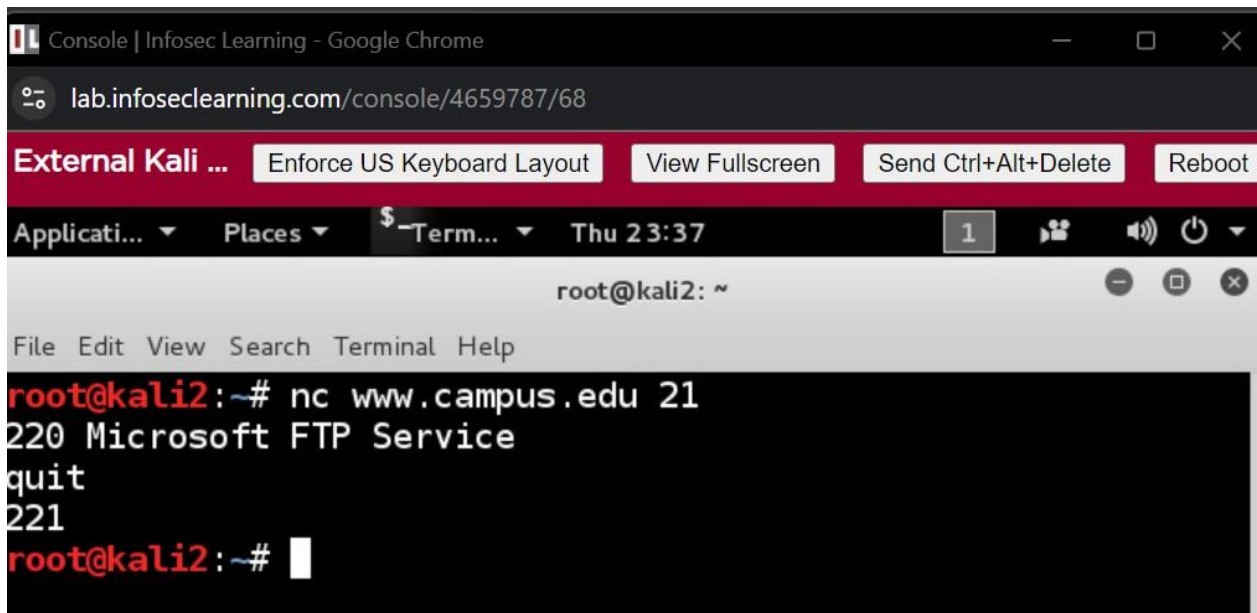
Step 8: Both netcat (nc) and TELNET can be used to perform a banner grab. Type the

Terminal Output:

```
root@kali2:~# nmap www.campus.edu
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-19 13:00 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00051s latency).
Not shown: 989 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
443/tcp   open  https
1099/tcp  open  rmiregistry
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
5432/tcp  open  postgresql
8180/tcp  open  sampleflag:999818

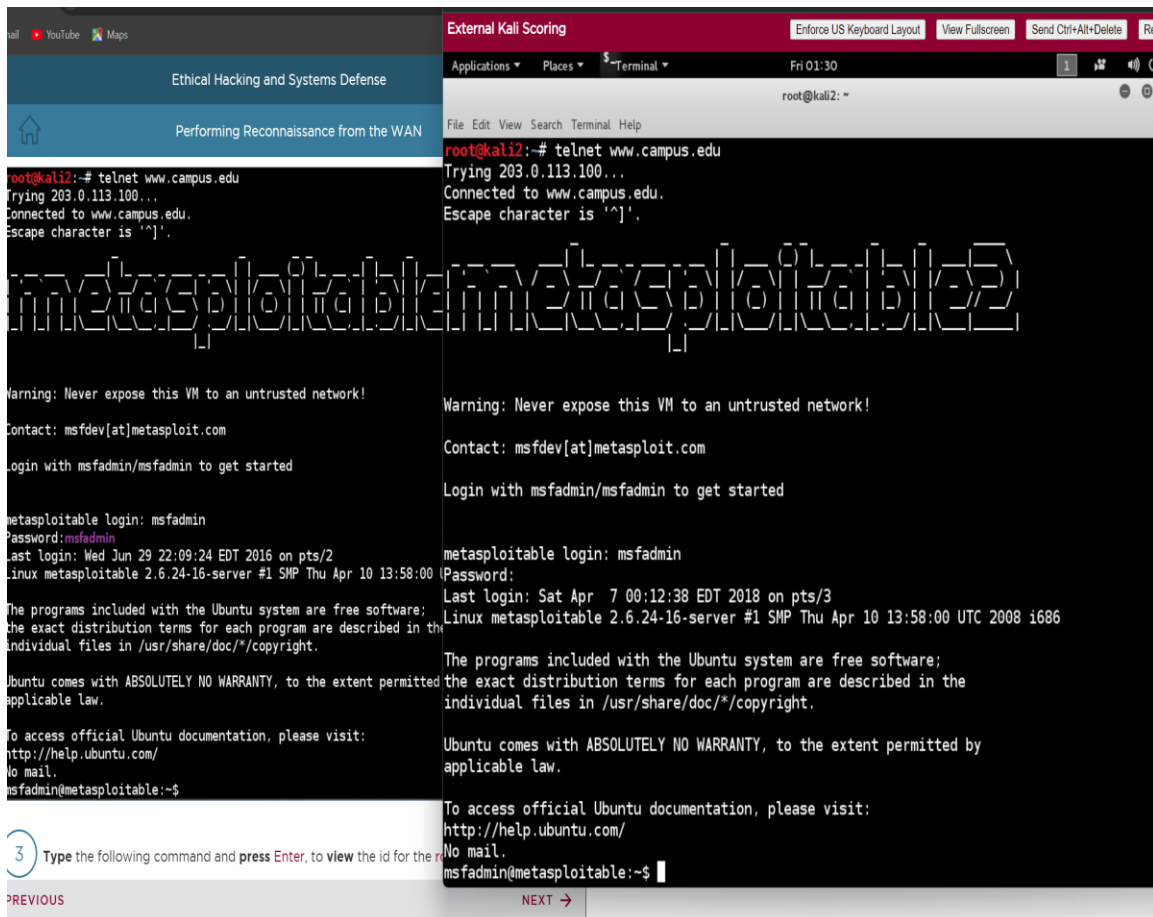
Nmap done: 1 IP address (1 host up) scanned in 20.17 seconds
root@kali2:~#
```

NC www.campus.edu on port 21



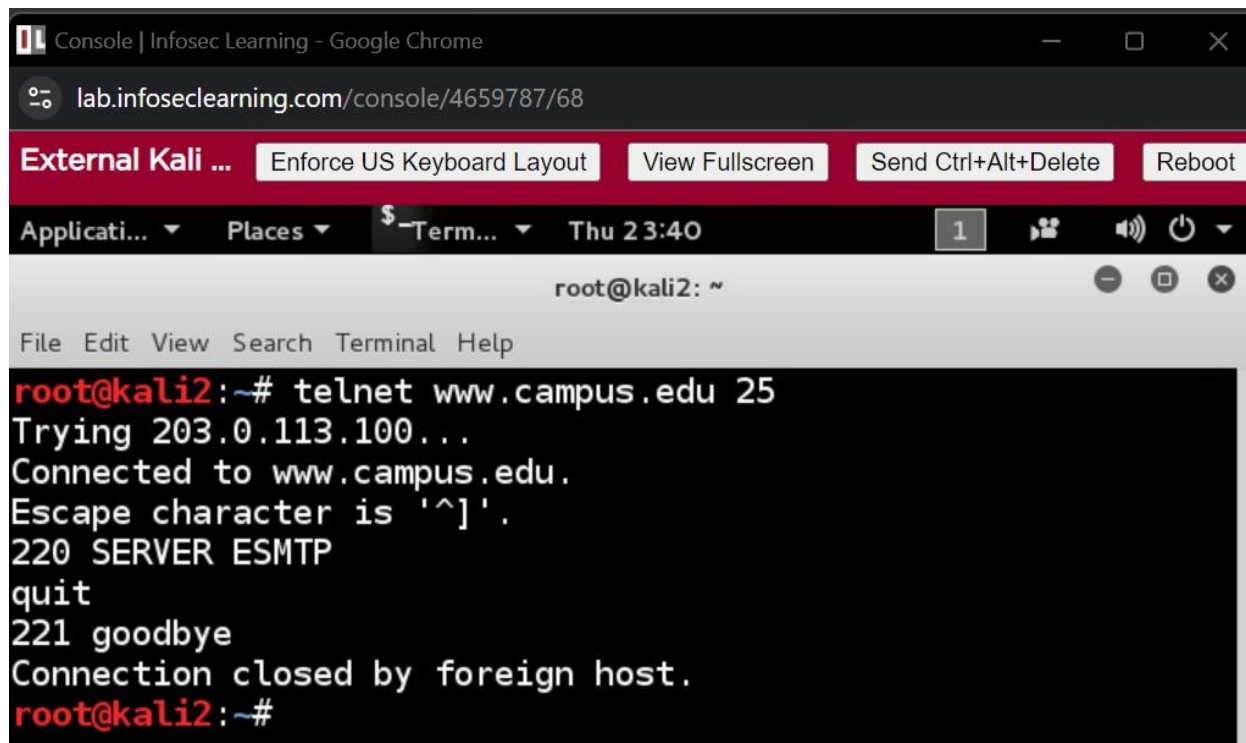
The screenshot shows a web browser window with the address bar at `lab.infoseclearning.com/console/4659787/68`. Below the address bar is a red navigation bar with buttons: "External Kali ...", "Enforce US Keyboard Layout", "View Fullscreen", "Send Ctrl+Alt+Delete", and "Reboot". Below this is a terminal window titled "root@kali2: ~". The terminal shows the command `nc www.campus.edu 21` being executed. The output is: `220 Microsoft FTP Service`, `quit`, `221`, and then the prompt `root@kali2:~#` with a cursor.

Teleport on port 23



The screenshot shows a Metasploit terminal session. The top bar is red with buttons: "External Kali Scoring", "Enforce US Keyboard Layout", "View Fullscreen", "Send Ctrl+Alt+Delete", and "Ret". Below this is a terminal window titled "root@kali2: ~". The terminal shows the command `telnet www.campus.edu` being executed. The output is: `Trying 203.0.113.100...`, `Connected to www.campus.edu.`, `Escape character is '^['.`, and then the Metasploit logo. Below the logo is a warning: "Warning: Never expose this VM to an untrusted network!". Then, the contact information: `Contact: msfdev[at]metasploit.com`. Then, the login instructions: `Login with msfadmin/msfadmin to get started`. Then, the login prompt: `metasploitable login: msfadmin`. Then, the password prompt: `Password:`. Then, the last login information: `Last login: Sat Apr 7 00:12:38 EDT 2018 on pts/3`. Then, the Linux version information: `Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686`. Then, the Ubuntu disclaimer: `The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.` Then, the Ubuntu disclaimer: `Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.` Then, the Ubuntu documentation link: `To access official Ubuntu documentation, please visit: http://help.ubuntu.com/`. Then, the Ubuntu disclaimer: `No mail.` Then, the prompt: `msfadmin@metasploitable:~$`.

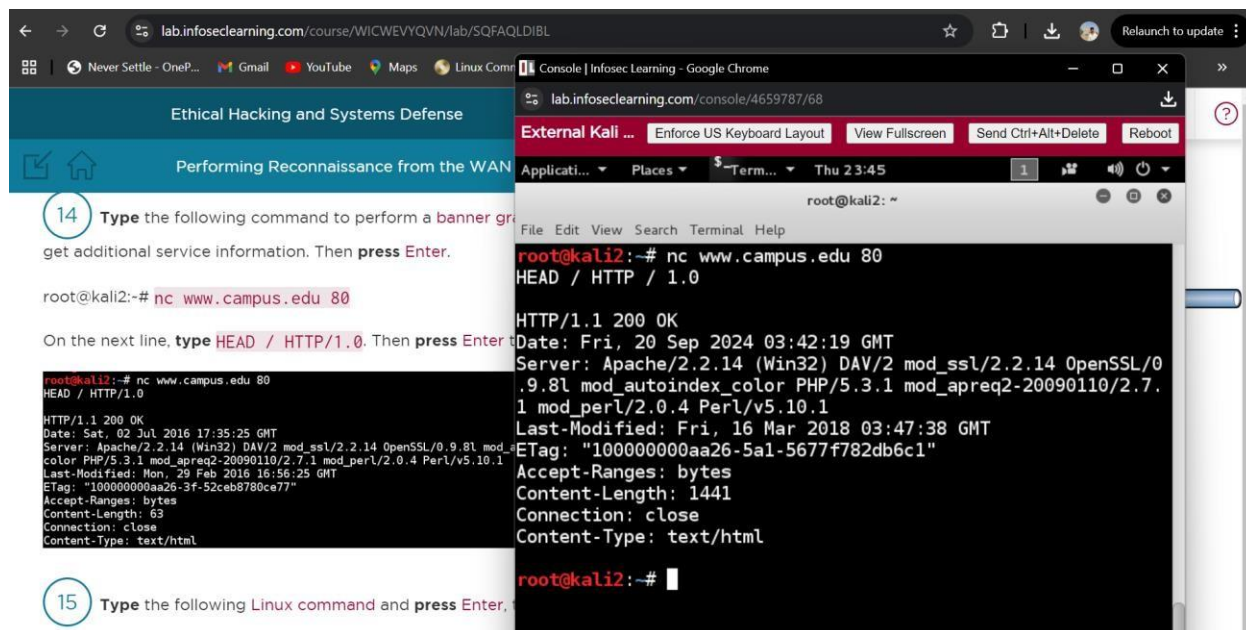
telnet scan on www.campus.edu 25



The screenshot shows a terminal window titled "Console | Infosec Learning - Google Chrome". The address bar displays "lab.infoseclearning.com/console/4659787/68". Below the address bar, there are buttons for "External Kali ...", "Enforce US Keyboard Layout", "View Fullscreen", "Send Ctrl+Alt+Delete", and "Reboot". The terminal prompt is "root@kali2: ~". The user enters the command "telnet www.campus.edu 25". The output shows the connection attempt to 203.0.113.100, successful connection to www.campus.edu, and the escape character is '^]'. The server responds with "220 SERVER ESMTTP". The user enters "quit", and the server responds with "221 goodbye". The connection is closed by the foreign host.

```
root@kali2:~# telnet www.campus.edu 25
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.
220 SERVER ESMTTP
quit
221 goodbye
Connection closed by foreign host.
root@kali2:~#
```

NC on www.campus.edu over port 80



The screenshot shows a terminal window titled "Console | Infosec Learning - Google Chrome". The address bar displays "lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL". Below the address bar, there are buttons for "External Kali ...", "Enforce US Keyboard Layout", "View Fullscreen", "Send Ctrl+Alt+Delete", and "Reboot". The terminal prompt is "root@kali2: ~". The user enters the command "nc www.campus.edu 80". The output shows the connection attempt to www.campus.edu port 80, successful connection, and the HTTP response from the server. The response includes the status "HTTP/1.1 200 OK", the date "Fri, 20 Sep 2024 03:42:19 GMT", the server "Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1", the last modified date "Fri, 16 Mar 2018 03:47:38 GMT", the ETag "10000000aa26-5a1-5677f782db6c1", the accept ranges "bytes", the content length "1441", and the content type "text/html".

```
root@kali2:~# nc www.campus.edu 80
HEAD / HTTP / 1.0

HTTP/1.1 200 OK
Date: Fri, 20 Sep 2024 03:42:19 GMT
Server: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
Last-Modified: Fri, 16 Mar 2018 03:47:38 GMT
ETag: "10000000aa26-5a1-5677f782db6c1"
Accept-Ranges: bytes
Content-Length: 1441
Connection: close
Content-Type: text/html

root@kali2:~#
```

telnet on www.campus.edu on port 110

The screenshot shows a web browser window with the URL `lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL`. The page title is "Ethical Hacking and Systems Defense" and the sub-header is "Performing Reconnaissance from the WAN". A terminal window is open, showing the following commands and output:

```
root@kali2:~# telnet www.campus.edu 110
Trying 203.0.113.100...
Connected to www.campus.edu.
Escape character is '^]'.
+OK POP3
quit
+OK POP3 server saying goodbye...
Connection closed by foreign host.
```

Below the terminal output, there are two numbered instructions:

- 16 Type the following command and **press Enter**, to perform a **banner grab** and get additional service information.
- 17 Type the following Linux command and **press Enter**, to view all output from the terminal.

Nc on www.campus.edu over 443

The screenshot shows a web browser window with the URL `lab.infoseclearning.com/console/4659787/68`. The page title is "Ethical Hacking and Systems Defense" and the sub-header is "Performing Reconnaissance from the WAN". A terminal window is open, showing the following commands and output:

```
root@kali2:~# nc www.campus.edu 443
HEAD / HTTP/1.0
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="en" xml:lang="en">
<head>
<title>Bad request!</title>
<link rev="made" href="mailto:webmaster@localhost" />
<style type="text/css"><!--/*--><![CDATA[/*><!--*/
body { color: #000000; background-color: #FFFFFF; }
a:link { color: #0000CC; }
p, address {margin-left: 3em;}
span {font-size: smaller;}
/*]]>!--></style>
</head>
```


Nmap scan on www.campus.edu over port 21

The screenshot shows a web application titled "Ethical Hacking and Systems Defense" with a sub-header "Performing Reconnaissance from the WAN". It contains two numbered instructions:

- 3 Type the following command and press Enter, to perform service and script scan of the target on port 21.
`root@kali2:~# nmap -sV -sC www.campus.edu -p 21`
- 4 Type the following Linux command and press Enter, to clear all output from the terminal.
`root@kali2:~# clear`

Below the instructions is a terminal window showing the output of the Nmap scan:

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:14 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00056s latency).
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: TIMEOUT
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 31.16 seconds
```

Nmap scan on www.campus.edu over port 23

The screenshot shows the same web application as above, but with a different instruction:

- 5 Type the following command and press Enter, to perform service and script scan of the target on port 23.
`root@kali2:~# nmap -sV -sC www.campus.edu -p 23`

Below the instruction is a terminal window showing the output of the Nmap scan:

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:17 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00055s latency).
PORT      STATE SERVICE VERSION
23/tcp    open  telnet?

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 138.31 seconds
```

Nmap scan on www.campus.edu over port 25

Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

7

Type the following command and press Enter, to perform a service and script scan of the target on port 25.

```
root@kali2:~# clear
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 25
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 25
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:18 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00053s latency).
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      hMailServer smtpd
|_ smtp-commands: SERVER, SIZE 20480000, AUTH LOGIN,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.64 seconds
```

8

Type the following Linux command and press Enter,

lab.infoseclearning.com/console/4659787/68

External Kali Scoring

Enforce US Keyboard Layout

View Fullscreen

Send Ctrl+Alt+Delete

Reboot

Applications

Places

Terminal

Fri 00:06

1

root@kali2: ~

File Edit View Search Terminal Help

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 25
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:05 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00040s latency).
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      hMailServer smtpd
|_ smtp-commands: SERVER, SIZE 20480000, AUTH LOGIN,
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
Service Info: Host: SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.61 seconds
```

Nmap scan on www.campus.edu over port 80

Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

9

Type the following command and press Enter, to perform a service and script scan of the target on port 80.

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 80
```

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 80
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:29 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00068s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
|_ http-methods: Potentially risky methods: TRACE
|_ http-robots.txt: 1 disallowed entry
|_ /webdav/
|_ http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_ http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.25 seconds
```

10

Type the following Linux command and press Enter,

lab.infoseclearning.com/console/4659787/68

External Kali Scoring

Enforce US Keyboard Layout

View Fullscreen

Send Ctrl+Alt+Delete

Reboot

Applications

Places

Terminal

Fri 00:08

1

root@kali2: ~

File Edit View Search Terminal Help

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 80
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:07 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00039s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.14 ((Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
|_ http-methods: Potentially risky methods: TRACE
|_ http-robots.txt: 1 disallowed entry
|_ /webdav/
|_ http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_ http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

← PREVIOUS

Nmap scan on www.campus.edu over port 110

lab.infoseclearning.com/course/WICWEVYQVN/lab/SQAQLDIBL

Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

11 Type the following command and press Enter, to perform a service and script scan of the target on port 110.

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 110
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:09 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00000s latency).
PORT      STATE SERVICE
110/tcp    open  pop3
hMailServer pop3d
|_pop3-capabilities: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 7.16 seconds
```

12 Type the following Linux command and press Enter, to clear all output from the terminal.

```
root@kali2:~# clear
```

← PREVIOUS

Nmap scan on www.campus.edu over port 443

lab.infoseclearning.com/course/WICWEVYQVN/lab/SQAQLDIBL

Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

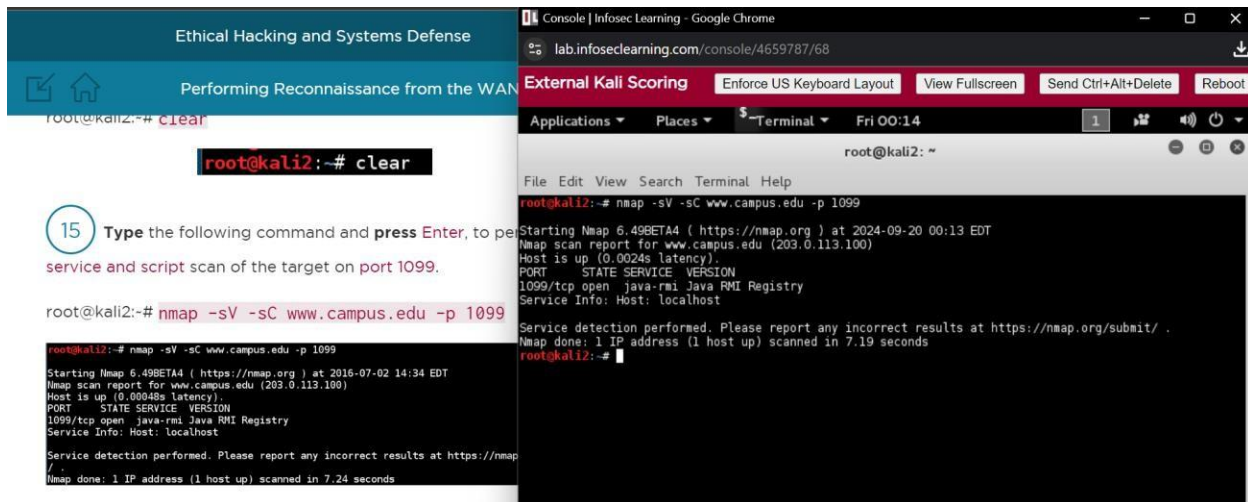
13 Type the following command and press Enter, to perform a service and script scan of the target on port 443.

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 443
```

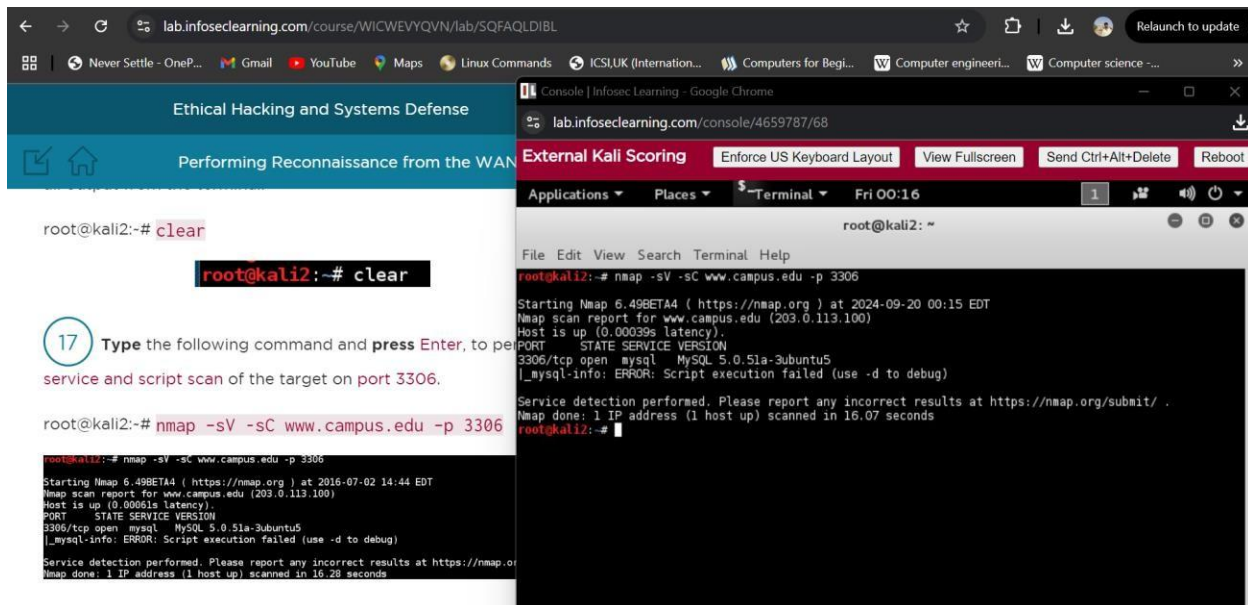
```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:10 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00042s latency).
PORT      STATE SERVICE
443/tcp    open  ssl/http
Apache httpd 2.2.14 (DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1)
|_http-cisco-anyconnect:
|_ ERROR: Not a Cisco ASA or unsupported version
|_ http-methods: Potentially risky methods: TRACE
|_ See http://nmap.org/nmapdoc/scripts/http-methods.html
|_ http-robots.txt: 1 disallowed entry
|_ /webdav/
|_ http-server-header: Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
|_ http-title: Site doesn't have a title (text/html).
|_ ssl-cert: Subject: commonName=localhost
|_ Not valid before: 2009-11-10T23:48:47
|_ Not valid after: 2019-11-08T23:48:47
|_ ssl-date: 2016-07-02T18:32:39+00:00: 0s from scanner time.
|_ sslv2:
|_ SSLv2 supported
|_ ciphers:
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_IDEA_128_CBC_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC2_CBC_128_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
```

← PREVIOUS

Nmap scan on www.campus.edu over port 1099



Nmap scan on www.campus.edu over port 3306



Nmap scan on www.campus.edu over port 3389

The screenshot shows a web browser window with the URL `lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL`. The page title is "Ethical Hacking and Systems Defense" and the sub-header is "Performing Reconnaissance from the WAN". The main content area shows a terminal window with the command `root@kali2:~# clear` and the output of an Nmap scan on `www.campus.edu` over port 3389. The scan results show that the host is up and the service is `ssl/ms-wbt-server?`. The terminal output is as follows:

```
root@kali2:~# clear

root@kali2:~# clear

19 Type the following command and press Enter, to perform a service and script scan of the target on port 3389.

root@kali2:~# nmap -sV -sC www.campus.edu -p 3389

root@kali2:~# nmap -sV -sC www.campus.edu -p 3389

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:49 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00058s latency).
PORT      STATE SERVICE      VERSION
3389/tcp  open  ssl/ms-wbt-server?
|_ ssl-cert: Subject: commonName=SERVER.campus.edu
|_ Not valid before: 2016-02-02T04:17:03
|_ Not valid after: 2016-08-04T04:17:03
|_ ssl-date: 2016-07-02T18:49:52+00:00; 0s from scanner time.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
```

Nmap scan on www.campus.edu over port 5432

The screenshot shows a web browser window with the URL `lab.infoseclearning.com/console/4659787/68`. The page title is "Ethical Hacking and Systems Defense" and the sub-header is "Performing Reconnaissance from the WAN". The main content area shows a terminal window with the command `root@kali2:~# clear` and the output of an Nmap scan on `www.campus.edu` over port 5432. The scan results show that the host is up and the service is `postgresql PostgreSQL DB 8.3.0 - 8.3.7`. The terminal output is as follows:

```
root@kali2:~# clear

root@kali2:~# clear

21 Type the following command and press Enter, to perform a service and script scan of the target on port 5432.

root@kali2:~# nmap -sV -sC www.campus.edu -p 5432

root@kali2:~# nmap -sV -sC www.campus.edu -p 5432

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2016-07-02 14:50 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00044s latency).
PORT      STATE SERVICE      VERSION
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.13 seconds
```


Nmap scan on www.campus.edu over port 8180

The screenshot shows a web browser window with the URL `lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL`. The page title is "Ethical Hacking and Systems Defense" and the sub-header is "Performing Reconnaissance from the WAN". A terminal window is open in the foreground, showing the command `root@kali2:~# clear` and the Nmap scan command `root@kali2:~# nmap -sV -sC www.campus.edu -p 8180`. The scan results show that the host is up and the service is Apache Tomcat/5.5 on port 8180.

23 Type the following command and press Enter, to perform a service and script scan of the target on port 8180.

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 8180
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 00:20 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00043s latency).
PORT      STATE SERVICE VERSION
8180/tcp   open  http      Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.17 seconds
root@kali2:~#
```

The screenshot shows a web browser window with the URL `lab.infoseclearning.com/course/WICWEVYQVN/lab/SQFAQLDIBL`. The page title is "Ethical Hacking and Systems Defense" and the sub-header is "Performing Reconnaissance from the WAN". A terminal window is open in the foreground, showing the command `root@kali2:~# clear` and the Nmap scan command `root@kali2:~# nmap -sV -sC www.campus.edu -p 3389`. The scan results show that the host is up and the service is Apache Tomcat/5.5 on port 3389.

13 Type the following command and press Enter, to perform a service and script scan of the target on port 3389.

```
root@kali2:~# nmap -sV -sC www.campus.edu -p 3389
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2024-09-20 01:37 EDT
Nmap scan report for www.campus.edu (203.0.113.100)
Host is up (0.00058s latency).
PORT      STATE SERVICE VERSION
3389/tcp   open  ssl/tls  Apache Tomcat/5.5
|_ssl-cert: Subject: commonName=SERVER.campus.edu
|_ssl-date: 2024-09-20T01:37:00Z; 0s from scanner time.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.74 seconds
root@kali2:~#
```

14 Type the following Linux command and press Enter, to clear all output from the terminal

Supporting Evidence

The screenshot provides the progress in completing challenges related to identifying the flages during the lab exercise.

Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

19

Below the sentence "Your browser (or proxy) sent a request that this server could not understand." You will find flag2. Type the flag for flag2.

CHALLENGE #1

20

Below the sentence "Your browser (or proxy) sent a request that this server could not understand." You will find flag3. Type the flag for flag3.

CHALLENGE #2

21

We will stop at port 443 and switch to a better form of service detection in the next section of the lab. Type the following command and press Enter, to clear all output from the terminal.

root@kali2:~# clear

root@kali2:~# clear

Discussion Questions

lab.infoseclearning.com/console/4656472/68

External Kali Scoring

Enforce US Keyboard Layout View Fullscreen Send

Applications Places Terminal Thu 13:25

root@kali2: ~

<p>

Your browser (or proxy) sent a request that this server could not understand.

flag2:877612

flag3:765114

</p>

<p>

If you think this is a server error, please contact the webmaster.

</p>

<h2>Error 400</h2>

<address>

localhost

9/19/2024 1:21:00 PM

Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex

PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1

</address>

</body>

Ethical Hacking and Systems Defense

Performing Reconnaissance from the WAN

msfadmin@metasploitable:~\$ id root

uid=0(root) gid=0(root) groups=0(root)

4

Get the information for below Challenge Flag by using the same techniques from the previous steps.

CHALLENGE #3

CHALLENGE #4

CHALLENGE #5

5

Type the following command and press Enter, to view the hashes in the shadow file.

msfadmin@metasploitable:~\$ sudo tail /etc/shadow

When asked for the password, type msfadmin, then press Enter.

Note: The password will not be displayed for security purposes.

PREVIOUS

NEXT

Applications Places Terminal Fri 01:34

root@kali2: ~

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin

Password:

Last login: Sat Apr 7 00:12:38 EDT 2018 on pts/3

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 6

The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

To access official Ubuntu documentation, please visit: http://help.ubuntu.com/

No mail.

msfadmin@metasploitable:~\$ id root

uid=0(root) gid=0(root) groups=0(root)

msfadmin@metasploitable:~\$ uid root

-bash: uid: command not found

msfadmin@metasploitable:~\$ id flag4

uid=444551(flag4) gid=444551(flag4) groups=444551(flag4)

msfadmin@metasploitable:~\$ id flag5

uid=444778(flag5) gid=444778(flag5) groups=444778(flag5)

msfadmin@metasploitable:~\$ id flag6

uid=616778(flag6) gid=616778(flag6) groups=616778(flag6)

msfadmin@metasploitable:~\$

Conclusion & Wrap-Up

Summary with:

Observations

The Kali 2 machine successfully identified open ports on the pfSense firewall, detected Linux and Windows systems via port forwarding, retrieved the /etc/shadow file, and logged into the Windows Server using RDP.

Identified risks

Exposing services like Telnet, retrieving password hashes from /etc/shadow, and forwarding ports to internal systems pose significant security risks, leaving the network vulnerable to exploitation.

Suggested recommendations

Disable insecure services, apply strong firewall rules, update systems regularly, and enforce multi-factor authentication with monitoring to detect unauthorized access

Your successes & failures

Successfully performed port scanning, identified operating systems, retrieved sensitive files, and accessed the Windows Server via RDP

Some tasks took longer than expected, and reliance on default tools limited the depth of scanning.

Challenges

Challenges included avoiding detection during scans, cracking complex password hashes, and ensuring stable RDP access to the Windows Server.