



Lab3: Network Penetration Testing Methodology

INFO40587: ETHICAL HACKING

Kevin Harianto | 991602128 | June2, 2024

Contents

Contents

Contents	1
Executive Summary.....	2
Exercise 1: Exploring and Auditing a Machine Using Nmap	3
Exercise 2: Accessing Misconfigured FTP Connection on a Remote Machine.....	8
Exercise 3: Enumerate a Wordpress Site (APT).....	11
Exercise 4: Perform Web Application Scanning with WMAP (APT).....	12
Conclusion.....	17

Executive Summary

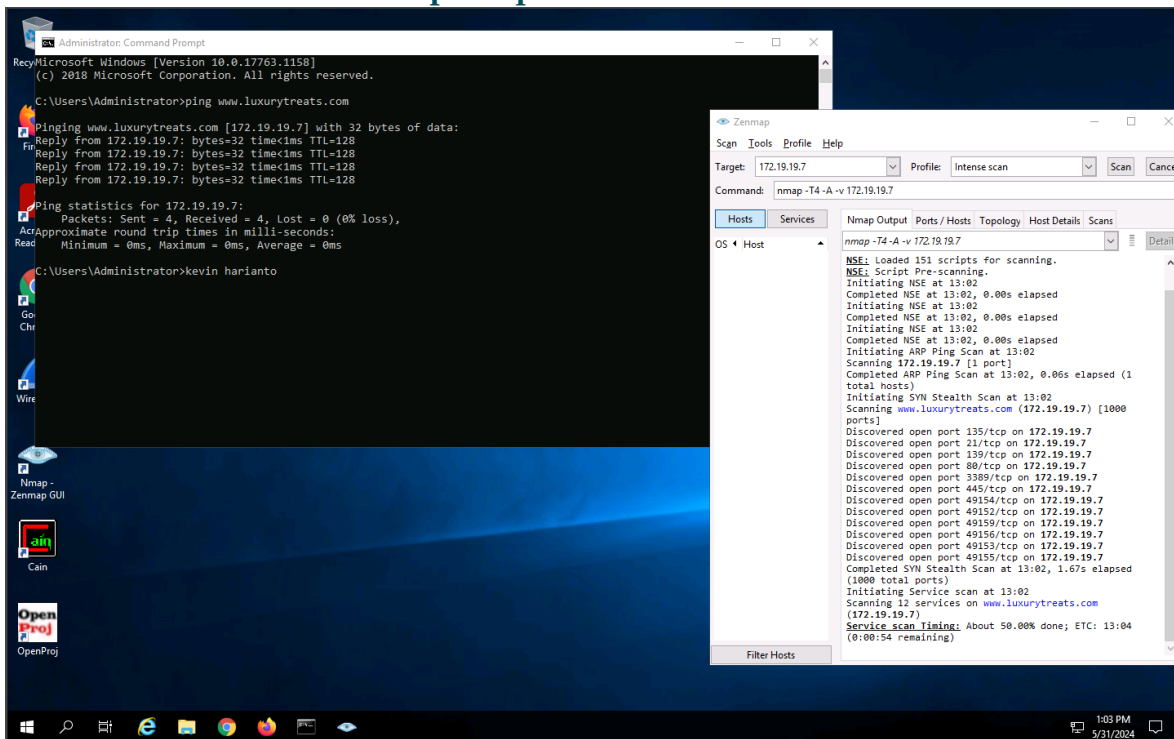
{state the objectives, approaches, methods/tools used, learning outcome, comments/overall observations}.

The objective of this lab is to help students in conducting network scanning, network vulnerability analysis, and network security maintenance. I have leveraged Nmap, ftp, wmap and Metasploit to execute reconnaissance on webpages, learning how to look for relevant information such as misconfigured websites as well as information on the background behind those applications to begin searching for vulnerabilities of those applications. This has allowed me to observe the importance that these tools have in terms of a penetration testers arsenal and how they can be leveraged to make gaining information on the web application easier and less manual.

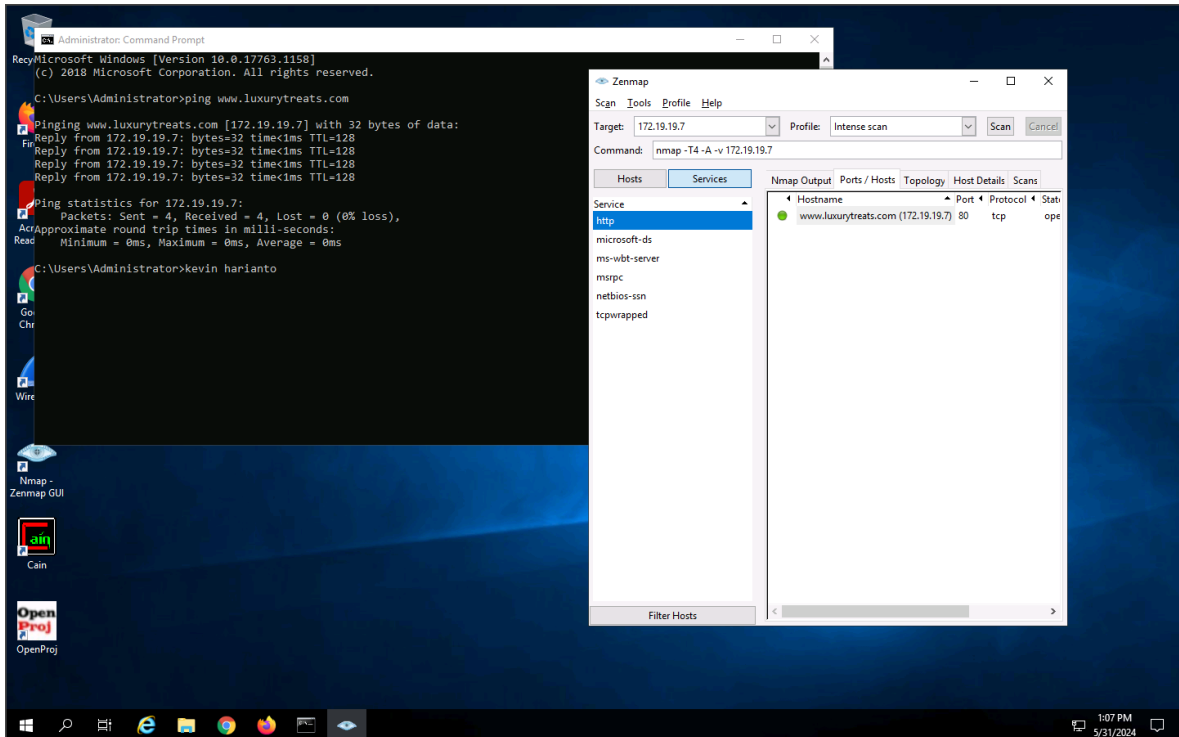
Exercise 1: Exploring and Auditing a Machine Using Nmap

1.1 OUTPUT SCREENSHOTS

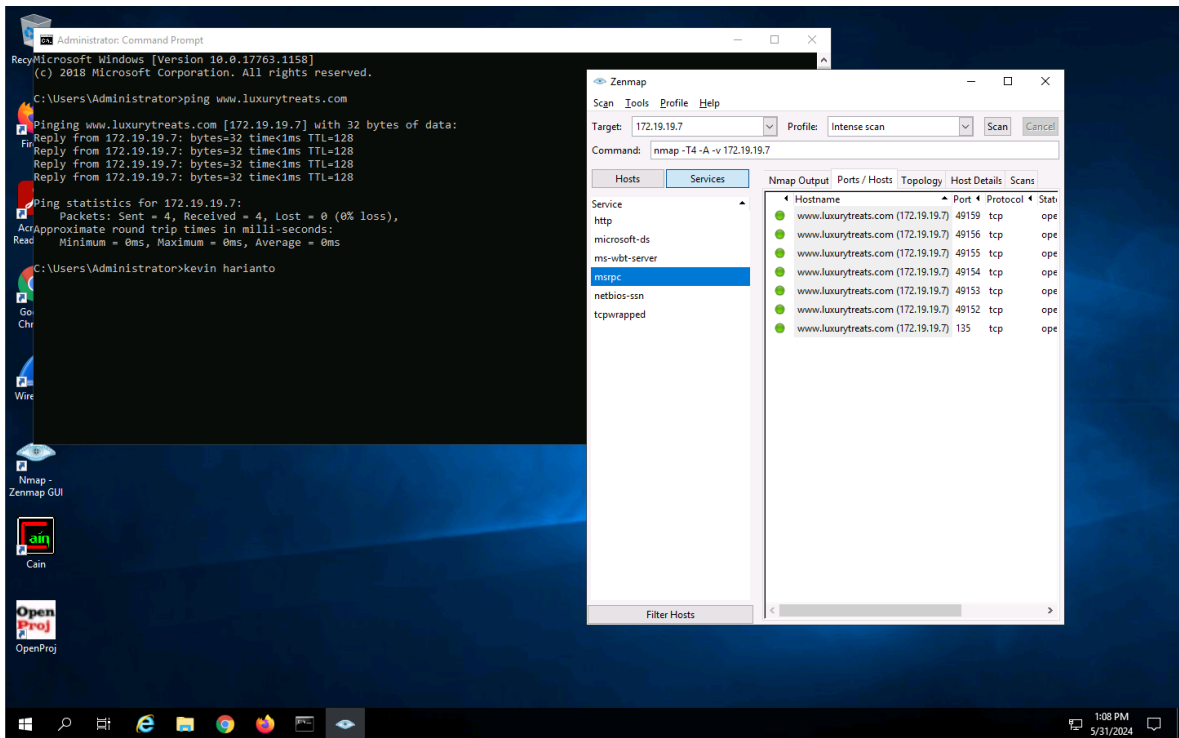
Exercise 1, Step 7: Nmap scans the provided IP address with Intense scan and scan results are shown in the **Nmap Output** tab.



Exercise 1, Step 8: Click the Ports/Hosts tab to check the Port, Protocol, State, Service, and Version of services discovered during the scan



Exercise 1, Step 13: Now, click msrpc service under Services section to view the ports on which the services are running. This way, you can access information about each service



Exercise 1, Step 17: Now, you can view the Intense Scan report in the browser as shown in the screenshot

Nmap Scan Report - Scanned at Fri May 31 13:02:46 2024

Scan Summary | www.luxurytreats.com (172.19.19.7)

Scan Summary

Nmap 7.80 was initiated at Fri May 31 13:02:46 2024 with these arguments:
`nmap -T4 -A -v 172.19.19.7`
Verbosity: 1; Debug level 0

172.19.19.7 / www.luxurytreats.com

Address

- 172.19.19.7 - (ipv4)
- 02:15:50:41:BC:9F - (mac)

Hostnames

- www.luxurytreats.com (PTR)

Ports

The 988 ports scanned but not shown below are in state: **closed**

Port	State (toggle closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp open	tcpwrapped	syn-ack			
80	tcp open	http	syn-ack	Microsoft IIS httpd	7.5	
135	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp open	microsoft-ds	syn-ack	Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds		
3389	tcp open	ms-wbt-server	syn-ack			
49152	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49153	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49154	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49156	tcp open	msrpc	syn-ack	Microsoft Windows RPC		
49159	tcp open	msrpc	syn-ack	Microsoft Windows RPC		

Remote Operating System Detection

- Used port: 80/tcp (open)
- Used port: 1/tcp (closed)
- Used port: 40219/udp (closed)
- OS match: **Microsoft Windows**

The 'Java(tm) Plug-in SSV Helper' add-on from 'Oracle America, Inc.' is ready for use. [Enable] [Don't enable] x

Go to top
Toggle Closed Ports
Toggle Filtered Ports

1:11 PM
5/31/2024

1.2 Questions

Administration: Command Prompt

Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping www.luxurytreats.com

Pinging www.luxurytreats.com [172.19.19.7] with 32 bytes of data:
Reply from 172.19.19.7: bytes=32 time=1ms TTL=128
Reply from 172.19.19.7: bytes=32 time=1ms TTL=128
Reply from 172.19.19.7: bytes=32 time=1ms TTL=128
Reply from 172.19.19.7: bytes=32 time=1ms TTL=128

Ping statistics for 172.19.19.7:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Administrator>kevin harianto

172.19.19.7

7.5

Port	State	Service	Version	OS	Extra info
80	open	http	syn-ack	Microsoft IIS httpd	
135	open	msrpc	syn-ack	Microsoft Windows RPC	
139	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn	
445	open	microsoft-ds	syn-ack	Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds	
1359	open	ms-rpc-ssr	syn-ack	Microsoft Windows RPC	
49152	open	msrpc	syn-ack	Microsoft Windows RPC	
49153	open	msrpc	syn-ack	Microsoft Windows RPC	
49154	open	msrpc	syn-ack	Microsoft Windows RPC	
49155	open	msrpc	syn-ack	Microsoft Windows RPC	
49156	open	msrpc	syn-ack	Microsoft Windows RPC	
49159	open	msrpc	syn-ack	Microsoft Windows RPC	

Remote Operating System Detection
• Used port: 80/tcp (open)
• Used port: 135/tcp (closed)
• Used port: 40219/udp
• OS match: Microsoft Windows
The 'Java(TM) Plug-in SSV Helper' add-on from 'Oracle America, Inc.' is ready for use.
Enable Don't enable

Instructions Resources

19. After analyzing the results in the report, close all the windows and the Nmap GUI.

In this lab you have analyzed all the IP addresses, open and closed ports, services, and protocols you discovered during the scan.

Question 5.11

In the Windows Server 2019 machine, use the ping utility to identify the IP address of the website on which the target domain, luxurytreats.com, is hosted. Enter the IP address.

172.19.19.7

Score

Correct

Question 5.12

In the Windows Server 2019 machine, perform an intense scan using Nmap on 172.19.19.7. Identify the service running on port 135.

msrpc

Score

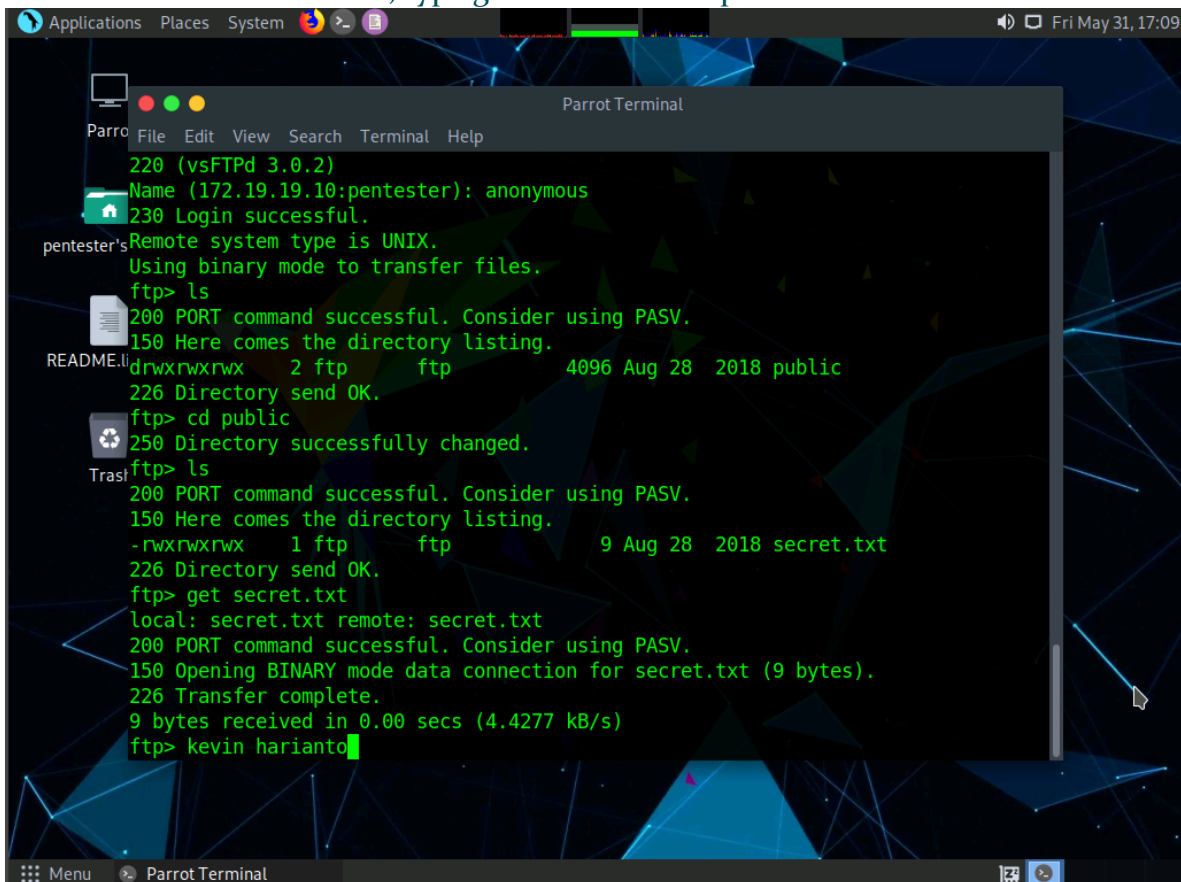
Correct

Previous Next

Exercise 2: Accessing Misconfigured FTP Connection on a Remote Machine

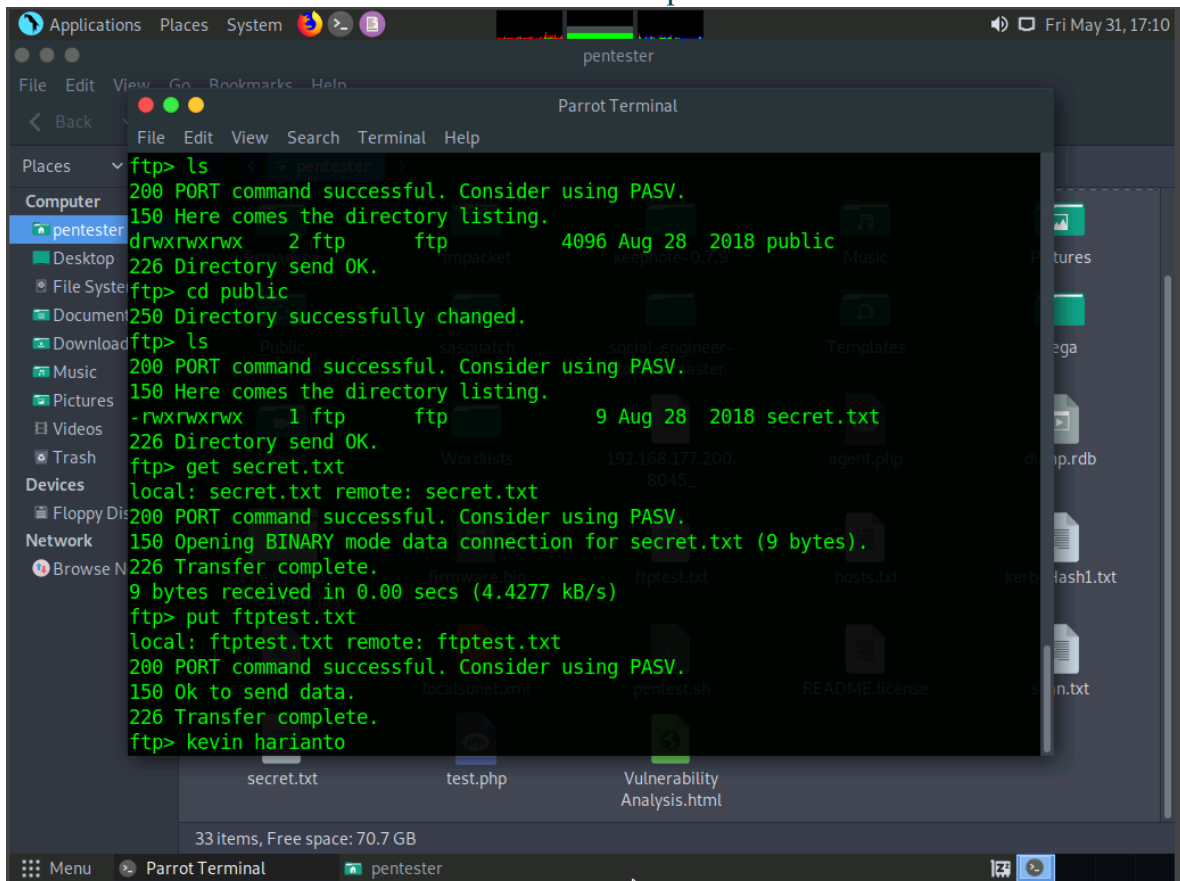
2.1 OUTPUT SCREENSHOTS

Exercise 2, Step 12: Now, we shall see if we can download the files from the server. To download secret.txt file, type get secret.txt and press Enter



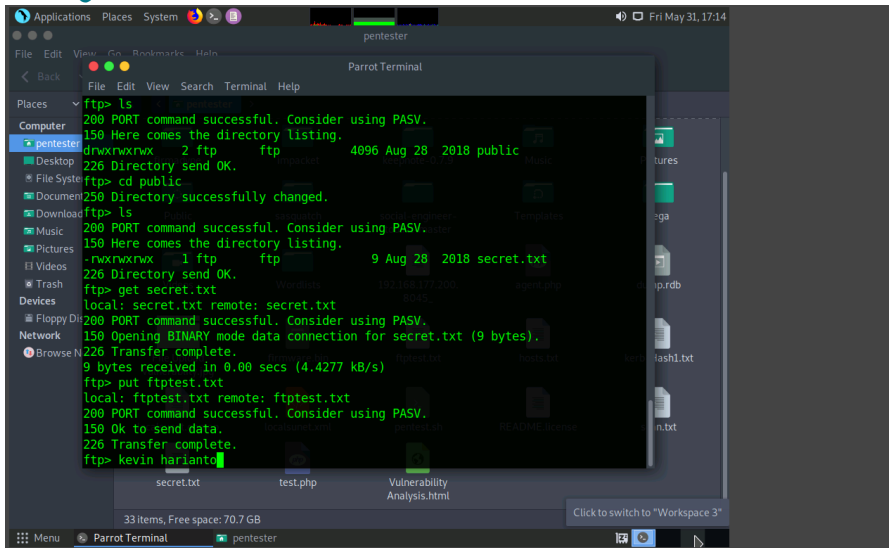
```
220 (vsFTPD 3.0.2)
Name (172.19.19.10:pentester): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx  2 ftp      ftp      4096 Aug 28  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx  1 ftp      ftp      9 Aug 28  2018 secret.txt
226 Directory send OK.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for secret.txt (9 bytes).
226 Transfer complete.
9 bytes received in 0.00 secs (4.4277 kB/s)
ftp> kevin hariato
```

Exercise 2, Step 15: The file was successfully uploaded to the server as shown in the screenshot below. This means that file upload access has been enabled on the Ubuntu Server which can allow an attacker to upload malicious files to it.



```
Applications Places System
pentester
File Edit View Go Bookmarks Help
Back
Places
Computer
pentester
Desktop
File System
Documents
Download
Music
Pictures
Videos
Trash
Devices
Floppy Dis
Network
Browse N
Parrot Terminal
File Edit View Search Terminal Help
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx  2 ftp  ftp  4096 Aug 28  2018 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx  1 ftp  ftp  9 Aug 28  2018 secret.txt
226 Directory send OK.
ftp> get secret.txt
local: secret.txt remote: secret.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for secret.txt (9 bytes).
226 Transfer complete.
9 bytes received in 0.00 secs (4.4277 kB/s)
ftp> put ftptest.txt
local: ftptest.txt remote: ftptest.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp> kevin hariato
secret.txt test.php Vulnerability Analysis.html
33 items, Free space: 70.7 GB
Menu Parrot Terminal pentester
```

2.2 QUESTIONS



The screenshot shows a Parrot OS desktop environment. A terminal window titled "Parrot Terminal" is open, displaying the output of an FTP session. The user has logged in as "ftp" and is in the "public" directory. They have listed files, changed directories, and transferred files. A file manager window is also open, showing the contents of the "public" directory, including files like "secret.txt", "test.php", and "Vulnerability Analysis.html".

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx  2 ftp      ftp      4096 Aug 28  2018 public
ftp> cd public
226 Directory send OK.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxrwx  1 ftp      ftp      9 Aug 28  2018 secret.txt
ftp> get secret.txt
226 Directory send OK.
local: secret.txt remote: secret.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for secret.txt (9 bytes).
226 Transfer complete.
9 bytes received in 0.00 secs (4.4277 kB/s)
ftp> put ftptest.txt
local: ftptest.txt remote: ftptest.txt
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
ftp> kevin hariato
```

In this lab, you have learned how to identify and connect to FTP servers that have anonymous access enabled.

Question 5.2.1

In the Parrot machine, use the Nmap tool to identify the FTP servers with anonymous access enabled. Enter the script used to determine whether anonymous login is enabled on the machine hosting the IP 172.19.19.10.

Score

✓ Correct

Question 5.2.2

In the Parrot machine, use the Nmap tool to identify the FTP servers with anonymous access enabled. Enter the remote system type identified after logging in to the remote machine 172.19.19.10 using FTP (the answer must be in ALL CAPS).

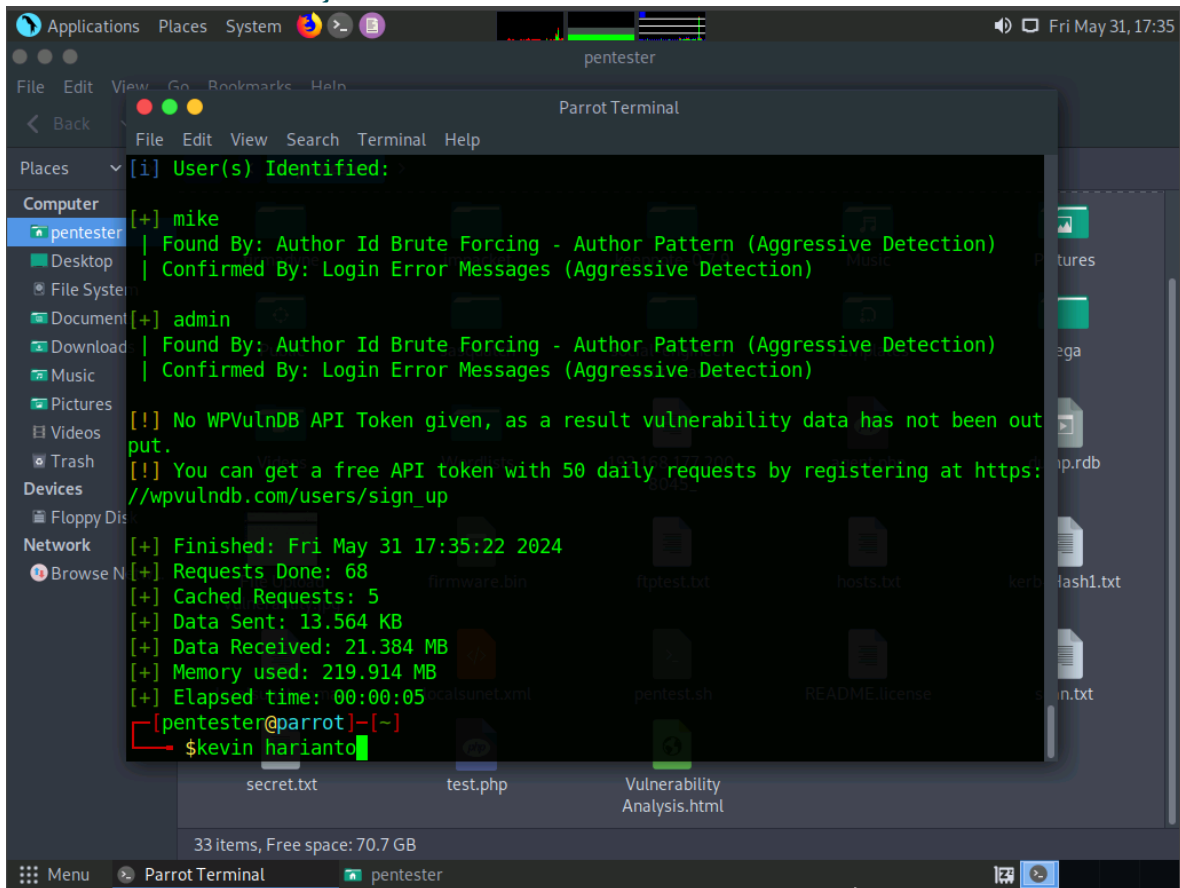
Score

✓ Correct

Exercise 3: Enumerate a Wordpress Site (APT)

3.1 OUTPUT SCREENSHOTS

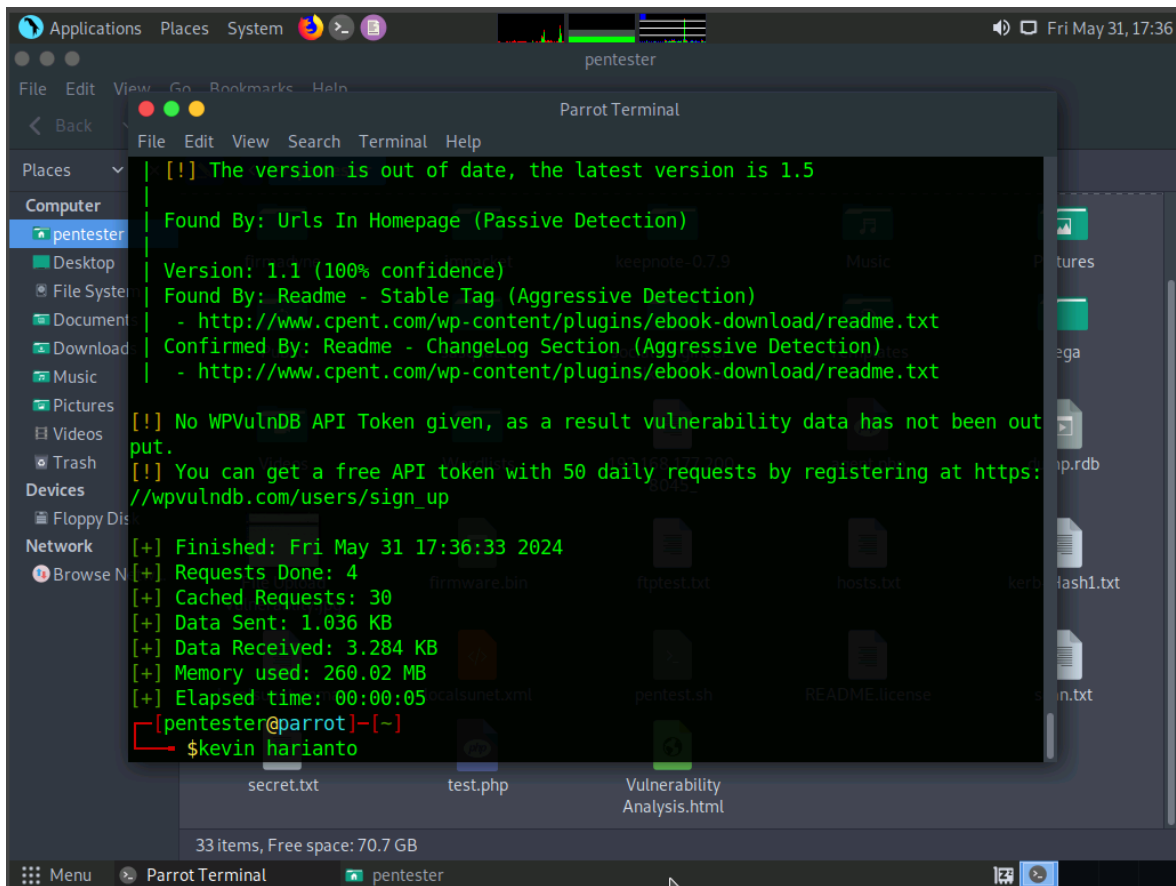
Exercise 3, Step 5: Next, scan the Wordpress website with whatweb tool. In the terminal type `sudo wpscan --url http://www.cpent.com --enumerate u` and press Enter. Type `toor` if prompted for Password and press Enter. This will enumerate the users, if there exists any.



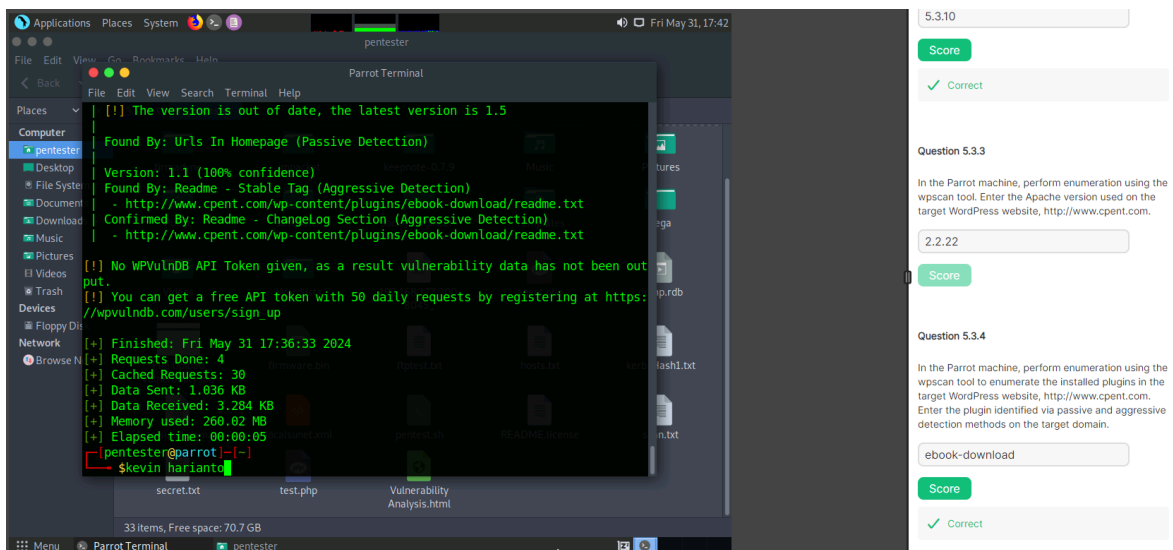
```
Applications Places System pentester
File Edit View Go Bookmarks Help
Parrot Terminal
Back File Edit View Search Terminal Help
Places Computer
pentester
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Dis
Network
Browse N
secret.txt test.php Vulnerability Analysis.html
33 items, Free space: 70.7 GB
Menu Parrot Terminal pentester

[+] User(s) Identified:
[+] mike
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPVulnDB API Token given, as a result vulnerability data has not been out
put.
[!] You can get a free API token with 50 daily requests by registering at https:
//wpvuln.db.com/users/sign_up
[+] Finished: Fri May 31 17:35:22 2024
[+] Requests Done: 68
[+] Cached Requests: 5
[+] Data Sent: 13.564 KB
[+] Data Received: 21.384 MB
[+] Memory used: 219.914 MB
[+] Elapsed time: 00:00:05
[+] pentester@parrot]-[~]
$kevin hariato
```

Exercise 3, Step 7: enumerate the plugins. Type `sudo wpscan --url http://www.cpent.com --enumerate p` and press Enter. Type `toor` if prompted for Password and press Enter. This will enumerate the installed plugins in the wordpress site, if there exists any.



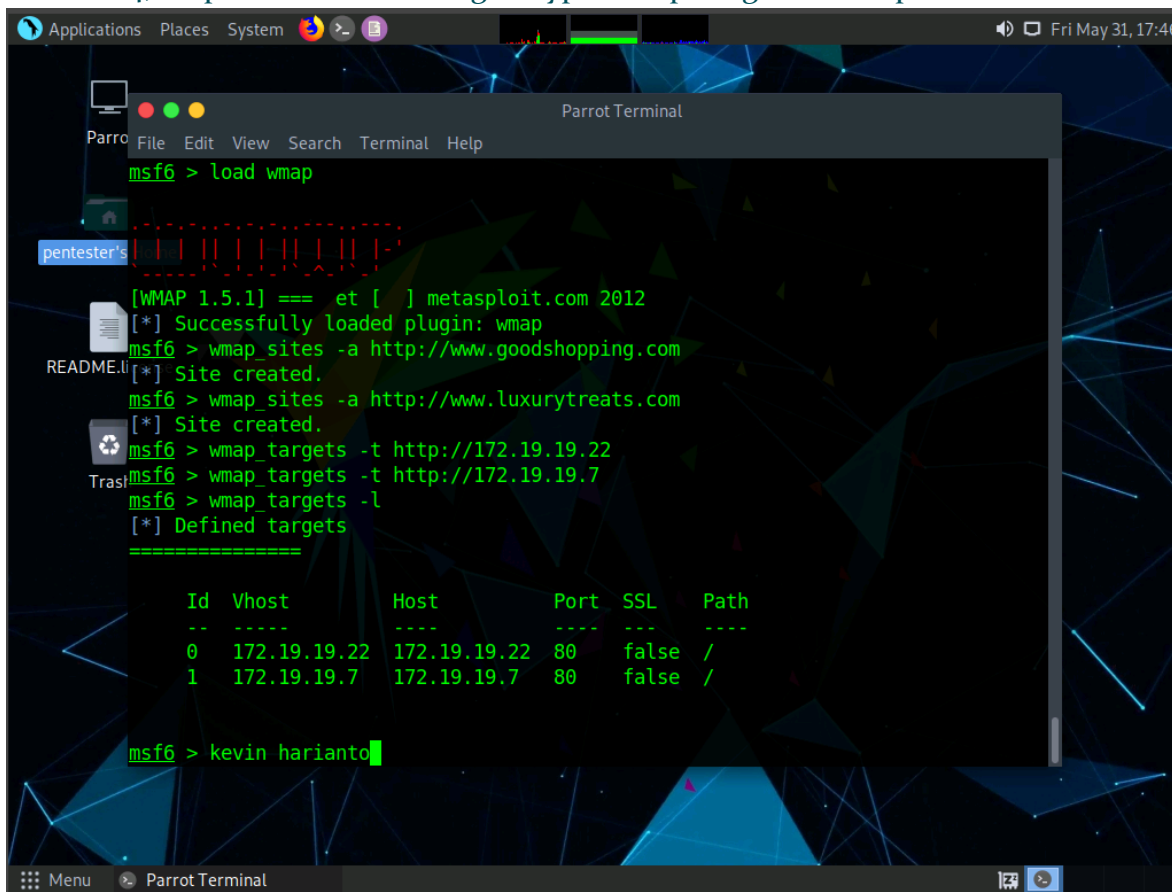
3.2 QUESTIONS



Exercise 4: Perform Web Application Scanning with WMAP (APT)

4.1 OUTPUT SCREENSHOTS

Exercise 4, Step 8: To view the targets type `wmap_targets -l` and press Enter.



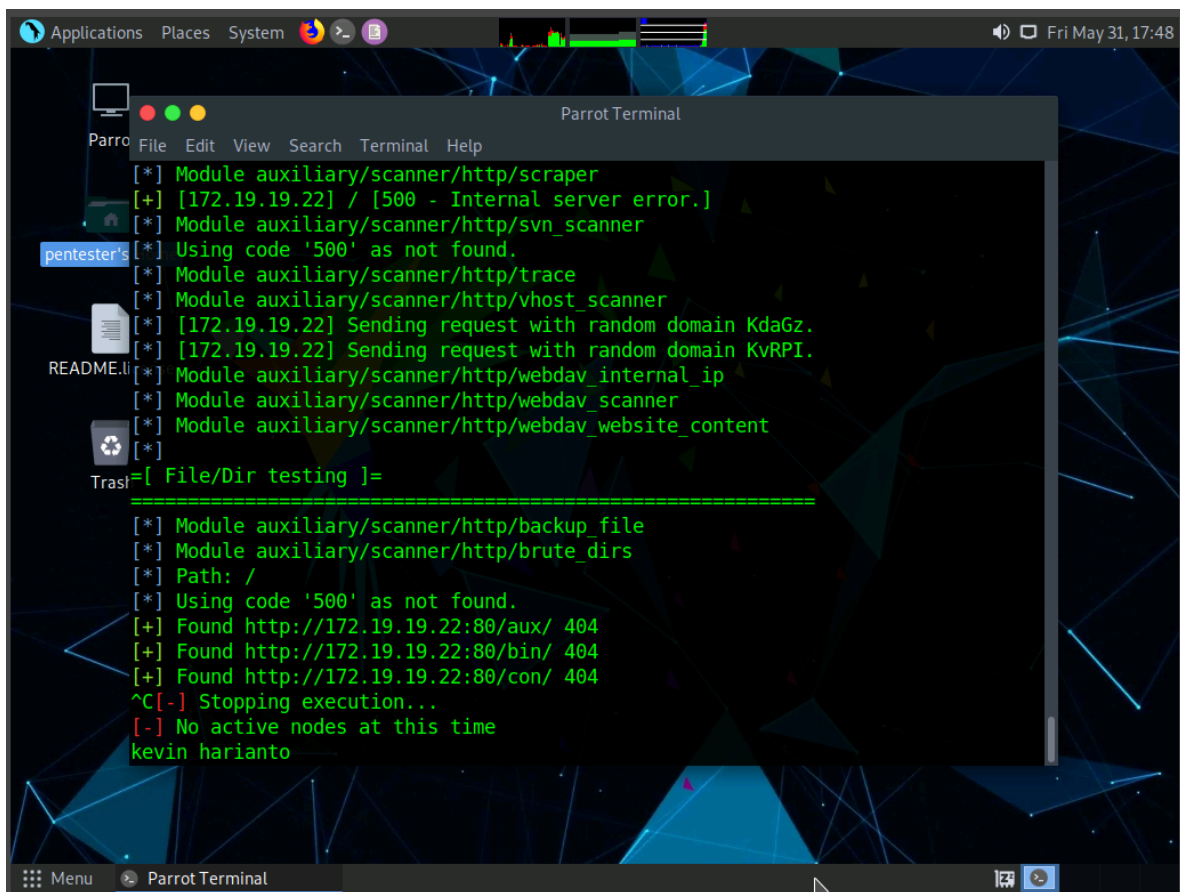
```
msf6 > load wmap

[WMAP 1.5.1] == et [ ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf6 > wmap_sites -a http://www.goodshopping.com
[*] Site created.
msf6 > wmap_sites -a http://www.luxurytreats.com
[*] Site created.
msf6 > wmap_targets -t http://172.19.19.22
msf6 > wmap_targets -t http://172.19.19.7
msf6 > wmap_targets -l
[*] Defined targets

=====
  Id  Vhost          Host          Port  SSL  Path
  --  -
  0    172.19.19.22   172.19.19.22  80    false /
  1    172.19.19.7    172.19.19.7   80    false /

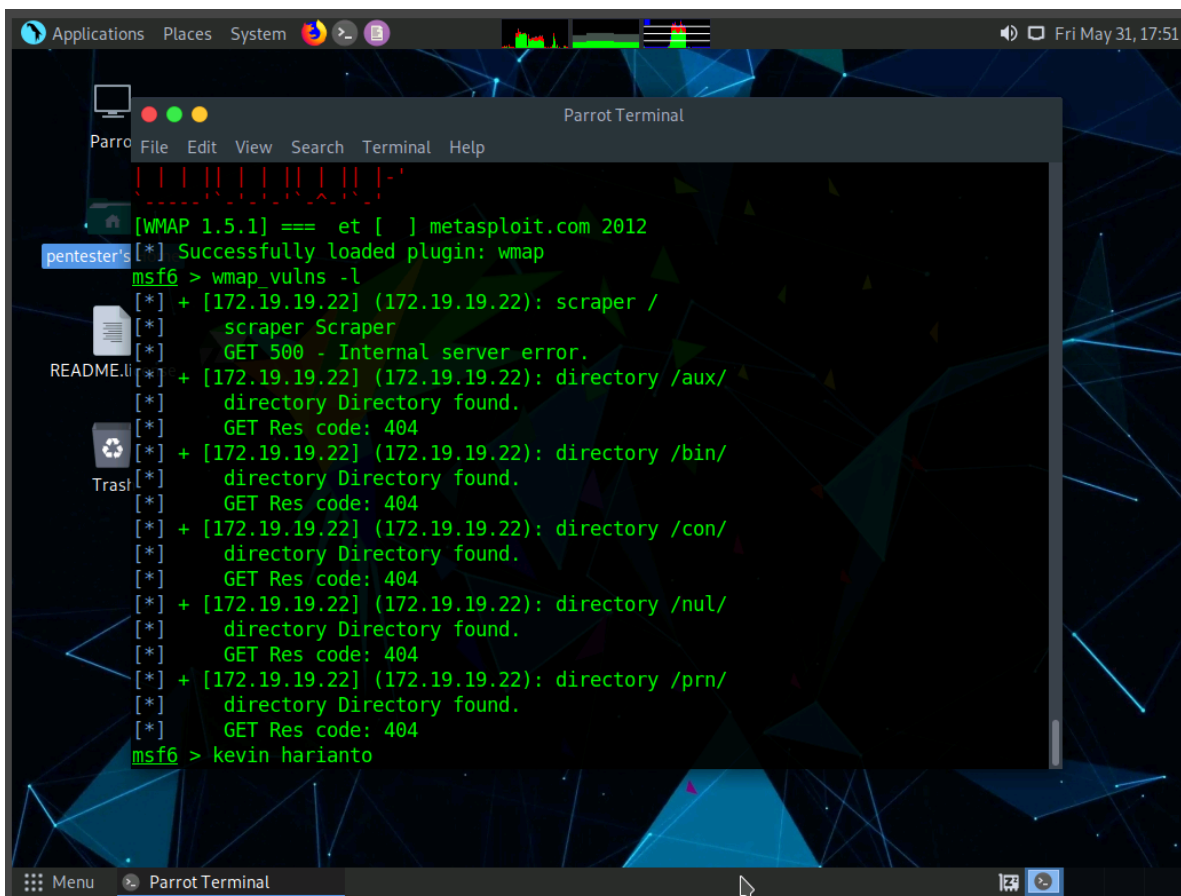
msf6 > kevin hariato
```

Exercise 4, Step 12: As the scan results show, the WMAP tool is not perfect, but it is another tool we can use to compliment our normal web scanning tools like Nikto and Vega.



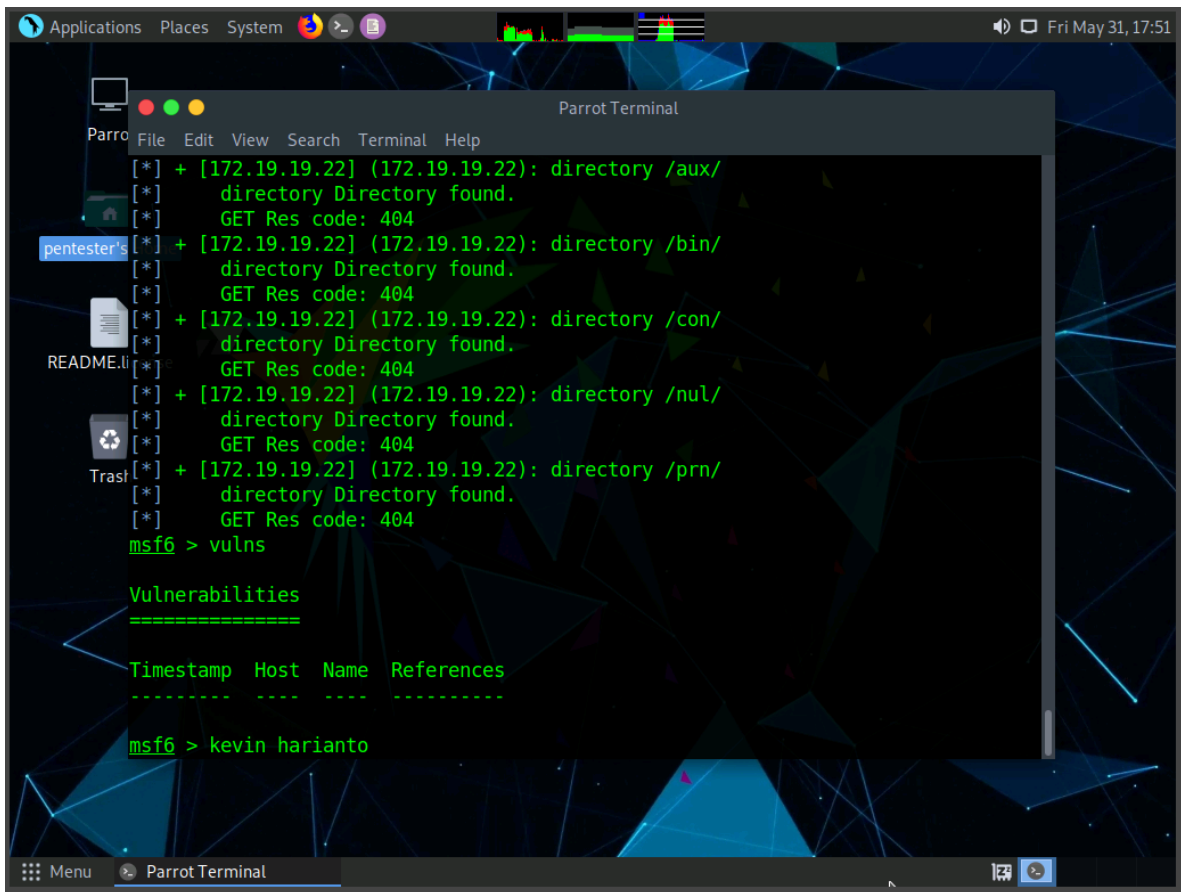
```
Parrot Terminal
File Edit View Search Terminal Help
[*] Module auxiliary/scanner/http/scraper
[+] [172.19.19.22] / [500 - Internal server error.]
[*] Module auxiliary/scanner/http/svn_scanner
[*] Using code '500' as not found.
[*] Module auxiliary/scanner/http/trace
[*] Module auxiliary/scanner/http/vhost_scanner
[*] [172.19.19.22] Sending request with random domain KdaGz.
[*] [172.19.19.22] Sending request with random domain KVRPI.
[*] Module auxiliary/scanner/http/webdav_internal_ip
[*] Module auxiliary/scanner/http/webdav_scanner
[*] Module auxiliary/scanner/http/webdav_website_content
[*]
Trasl=[ File/Dir testing ]=
=====
[*] Module auxiliary/scanner/http/backup_file
[*] Module auxiliary/scanner/http/brute_dirs
[*] Path: /
[*] Using code '500' as not found.
[+] Found http://172.19.19.22:80/aux/ 404
[+] Found http://172.19.19.22:80/bin/ 404
[+] Found http://172.19.19.22:80/con/ 404
^C[-] Stopping execution...
[-] No active nodes at this time
kevin harianto
```

Exercise 4, Step 13: To look at the vulnerabilities that have been written to the database, type `wmap_vulns -l` and press Enter

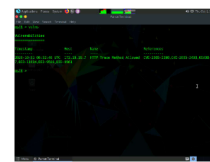
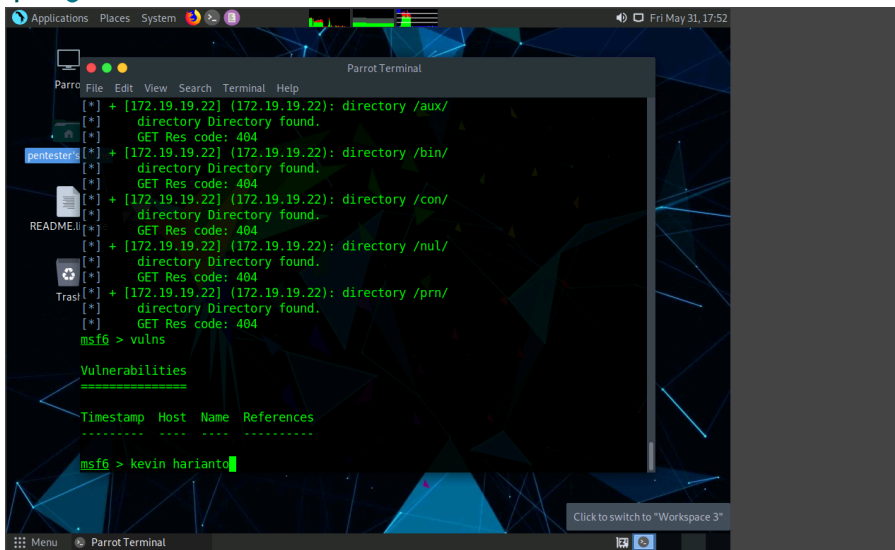


```
[WMAP 1.5.1] == et [ ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
msf6 > wmap_vulns -l
[*] + [172.19.19.22] (172.19.19.22): scraper /
[*] scraper Scraper
[*] GET 500 - Internal server error.
[*] + [172.19.19.22] (172.19.19.22): directory /aux/
[*] directory Directory found.
[*] GET Res code: 404
[*] + [172.19.19.22] (172.19.19.22): directory /bin/
[*] directory Directory found.
[*] GET Res code: 404
[*] + [172.19.19.22] (172.19.19.22): directory /con/
[*] directory Directory found.
[*] GET Res code: 404
[*] + [172.19.19.22] (172.19.19.22): directory /nul/
[*] directory Directory found.
[*] GET Res code: 404
[*] + [172.19.19.22] (172.19.19.22): directory /prn/
[*] directory Directory found.
[*] GET Res code: 404
msf6 > kevin hariato
```

Exercise 4, Step 14: You can also display the vulnerabilities by typing vulns and press Enter



4.2 QUESTIONS



15. We have accomplished what we wanted to in this lab, so we can clean up from the exercise and close all programs.

In this lab you have learnt how to:

- Use the tool WMAP that is part of the Metasploit tools
- Scan a web servers with WMAP

Question 5.4.1

Perform web application scanning from within the Metasploit console using the WMAP tool. Add the sites <http://www.goodsshopping.com> and <http://www.luxurytreats.com> to the WMAP tool. Enter the wmap_run command option that shows all enabled modules.

wmap_run -t

Score

Correct

Conclusion

In conclusion I have learned how to leverage nmap to scan websites and IP addresses to find any misconfigurations and send data across accordingly. I have also learned how to execute reconnaissance through the employment of Metasploit and Wmap for intelligence gathering as well as ftp into the misconfigured servers.