

Module 05: Network Penetration Testing Methodology-External Objective

The objective of this lab is to help students in conducting network scanning, network vulnerability analysis, and network security maintenance.

You need to perform network scans to:

- Check live systems and open ports
- Perform banner grabbing and OS fingerprinting
- Identify network vulnerabilities
- Draw network diagrams of vulnerable hosts
- Pентest vulnerabilities to gain unauthorized access

Scenario

External Penetration Testing determines the possibility of network security attacks from outside of the network perimeter. It evaluates the organization's systems and network for vulnerabilities such as missing patches, unnecessary services, weak authentication, and weak encryption.

An attacker uses vulnerabilities to disrupt the confidentiality, availability or integrity of the network, thereby allowing the organization to address each weakness. Vulnerability scanning is a critical component of any penetration testing assignment. As an expert Penetration Tester or a Security Administrator, you need to conduct penetration testing and list the threats and vulnerabilities found in an organization's network, perform port scanning, network scanning, and vulnerability scanning to identify IP/hostname, live hosts, and vulnerabilities. Then, you need to take specific preventive countermeasures to overcome them.

Exercise 1: Exploring and Auditing a Machine Using Nmap

Scenario

Network scan plays a crucial role in identifying the hosts that are up and running in a network. Additionally, it helps a pentester in pulling out additional information associated with a machine such as the services running on the machine, the ports used by the service and the operating system details.

As a penetration tester, you need to have extensive knowledge of network mapping tools, top ports running different services, etc.

Lab Duration: 30 Minutes

1. By default, **CPENT-M5 Windows Server 2019** is selected. Click Ctrl+Alt+Del.





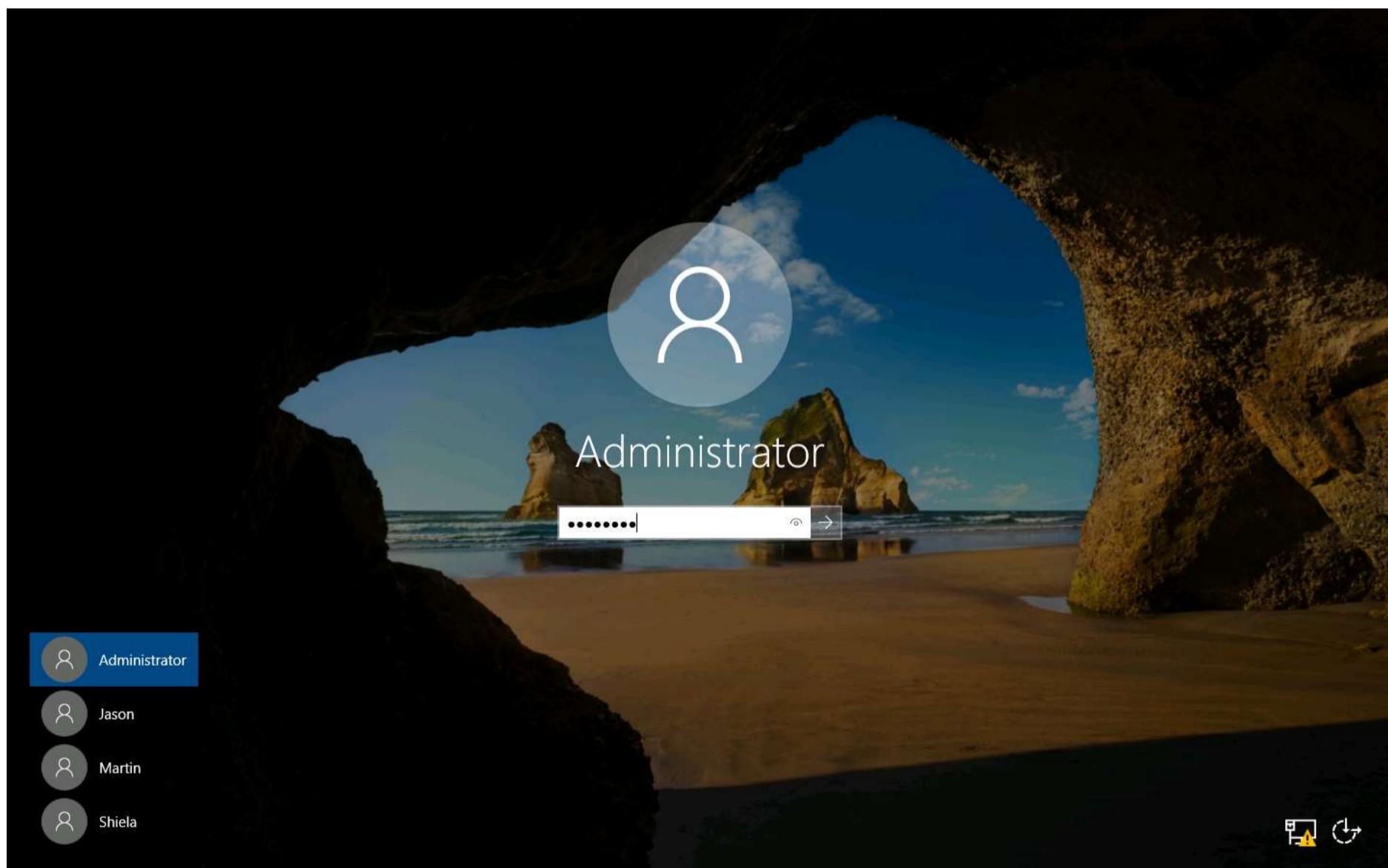
Press Ctrl+Alt+Delete to unlock.

9:23

Wednesday, August 12

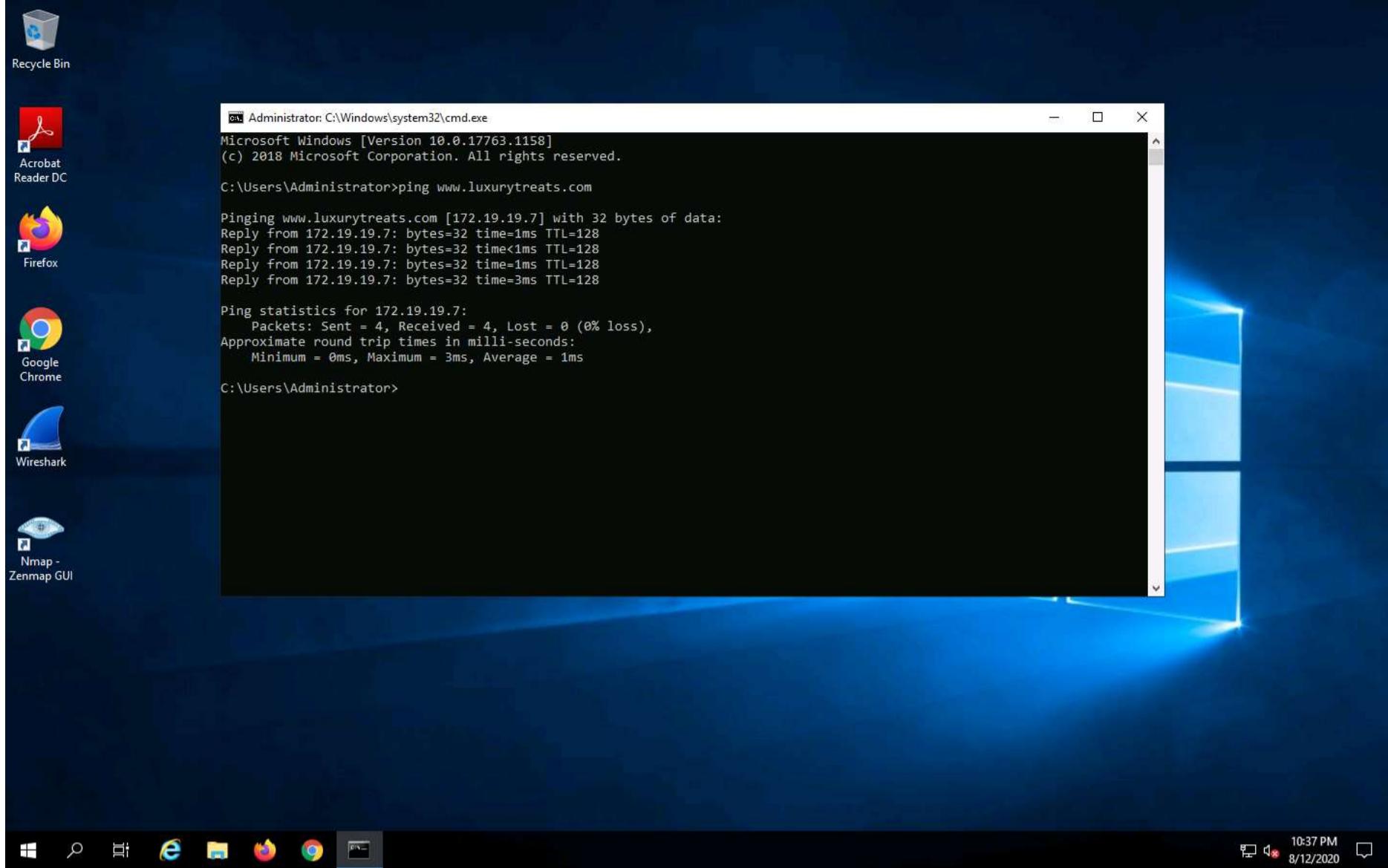


2. In the password field type **Pa\$\$w0rd** and press **Enter**

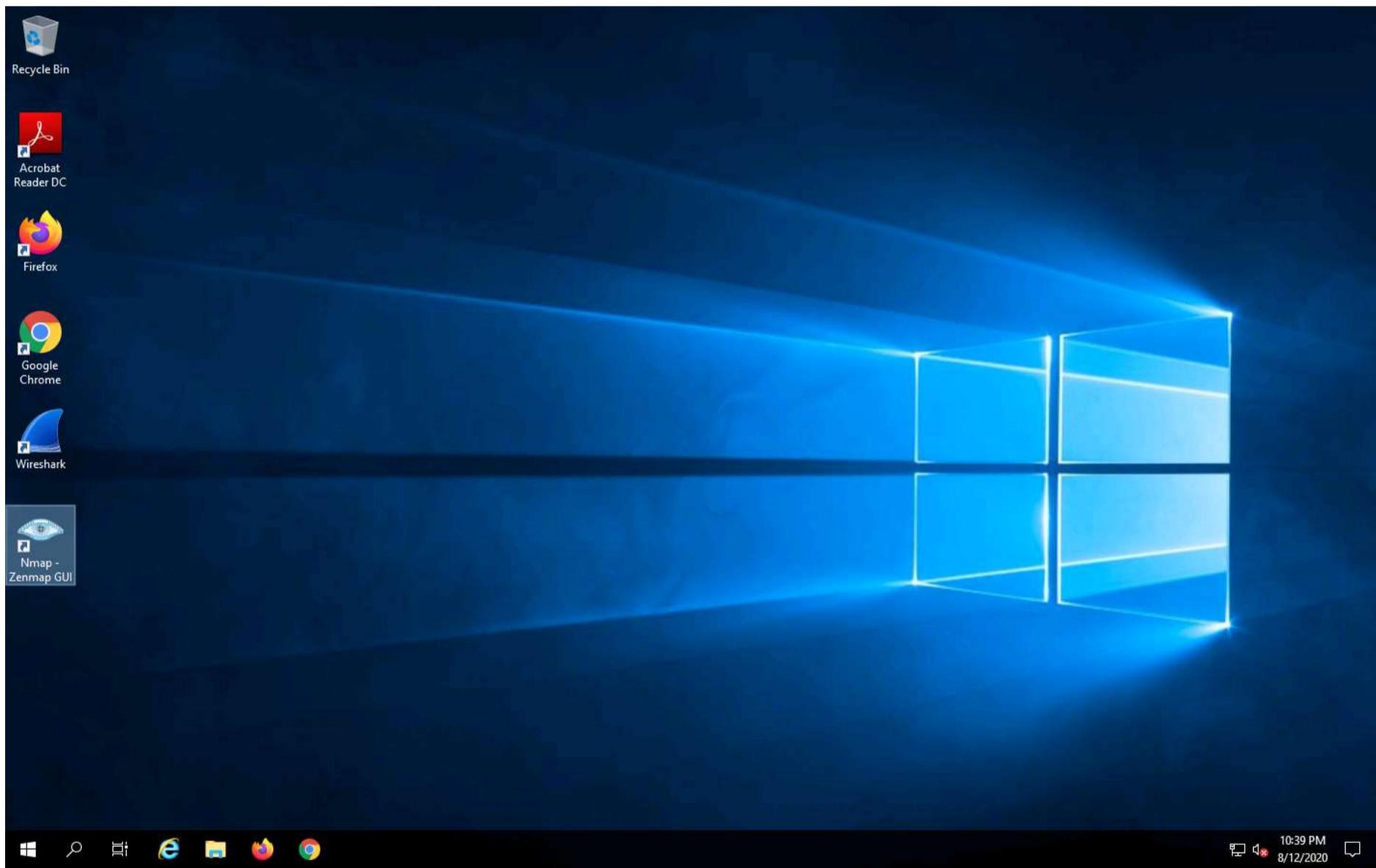


3. In this lab, you are given the assignment to audit the server hosting the website <http://www.luxurytreats.com>. So, before beginning this lab, we shall identify the IP Address of the website using the **ping** utility. Launch a command prompt, type **ping www.luxurytreats.com** and press **Enter**. This returns the IP Address of the server as **172.19.19.7** in the response. We will be scanning this IP address using Nmap in the forthcoming tasks.



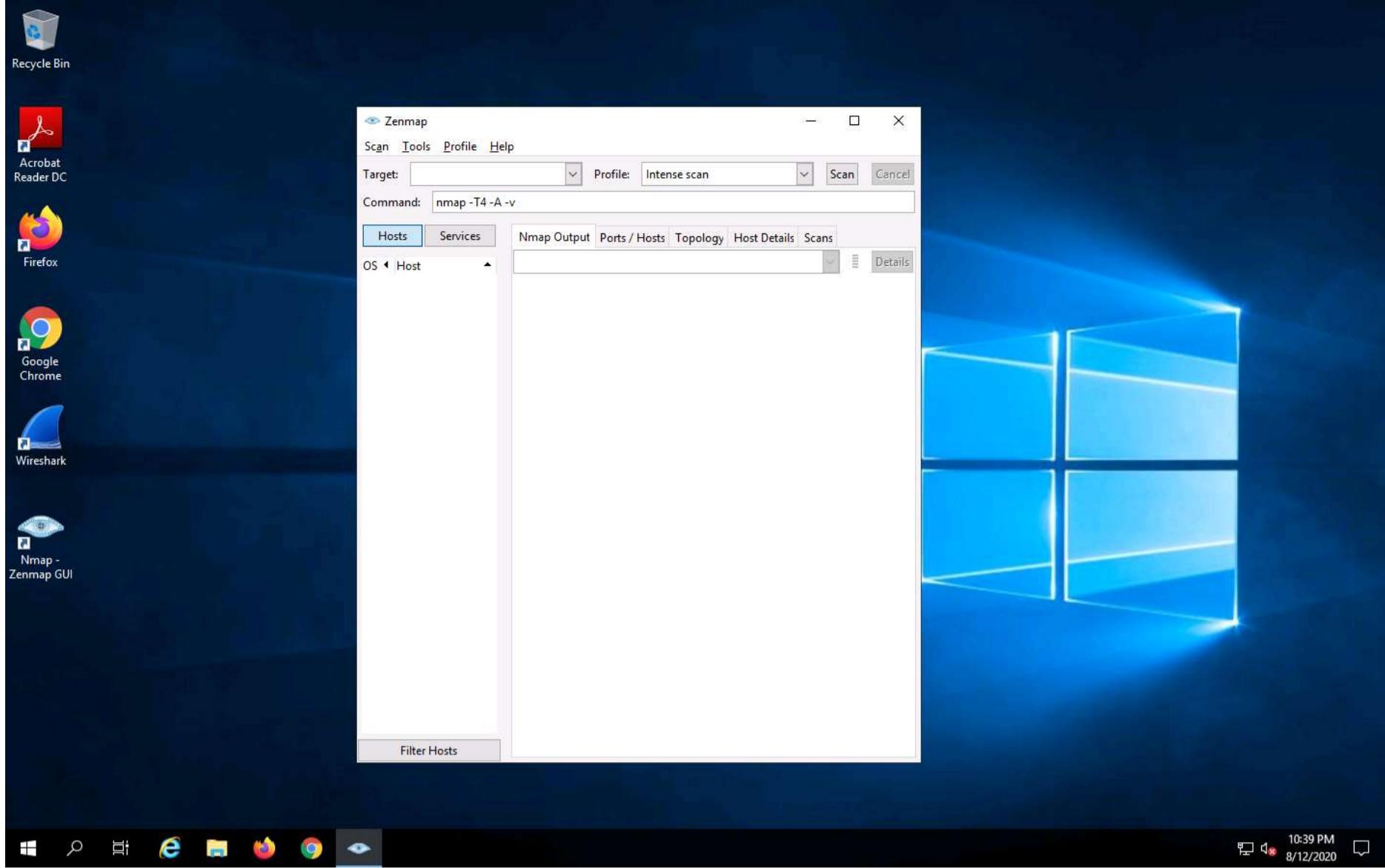


4. To launch **Nmap**, double-click **Nmap - Zenmap GUI** icon on the desktop.



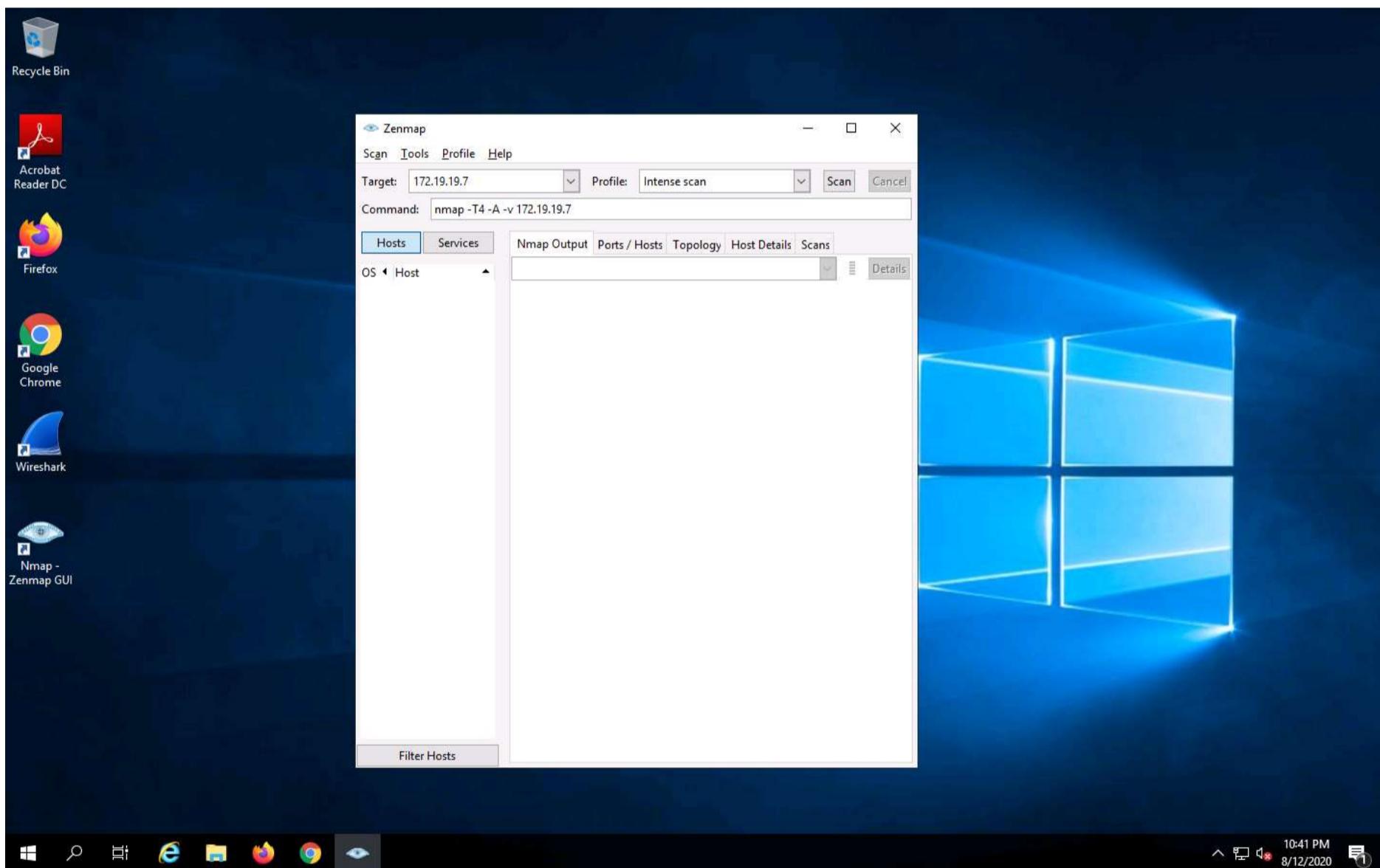
5. **Zenmap (Nmap)** main window appears as shown in the screenshot.





6. To perform **Intense Scan**, enter IP address in the **Target** field and choose **Intense Scan** from **Profile** drop-down list and click **Scan**. In this lab, we are performing Intense Scan on **Target_CPENT Web Server** machine (which is hosting www.luxurytreats.com) whose IP address, **172.19.19.7** was identified in the earlier steps.

Note: The scan will take a few minutes to complete.



7. Nmap scans the provided IP address with Intense scan and scan results are shown in the **Nmap Output** tab.

Note: Scan results might vary when you perform this task.



Zenmap

Scan Tools Profile Help

Target: 172.19.19.7

Command: nmap -T4 -A -v 172.19.19.7

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans

OS Host www.luxurytreats.c

```
nmap -T4 -A -v 172.19.19.7
Starting NSE at 22:42
Completed NSE at 22:42, 0.00s elapsed
Nmap scan report for www.luxurytreats.com (172.19.19.7)
Host is up (0.00s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  tcpwrapped
80/tcp    open  http        Microsoft IIS httpd 7.5
| http-methods:
|_ Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: ECCVApp
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds
3389/tcp  open  tcpwrapped
| rdp-ntlm-info:
| Target_Name: WIN-AG46I02QBKJ
| NetBIOS_Domain_Name: WIN-AG46I02QBKJ
| NetBIOS_Computer_Name: WIN-AG46I02QBKJ
| DNS_Domain_Name: WIN-AG46I02QBKJ
| DNS_Computer_Name: WIN-AG46I02QBKJ
| Product_Version: 6.1.7601
|_ System_Time: 2020-08-13T05:42:23+00:00
|_ssl-cert: Subject: commonName=WIN-AG46I02QBKJ
|Issuer: commonName=WIN-AG46I02QBKJ
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2020-08-09T05:24:03
| Not valid after: 2021-02-08T05:24:03
|MD5: 2842 4278 917a 444f 8a03 09ee 25c2 8cb2
|_SHA-1: d000 a1d2 4628 37cd 72c6 e248 9b40 16c7 7045 bf93
|_ssl-date: 2020-08-13T05:42:58+00:00; 0s from scanner time.
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49156/tcp open  msrpc       Microsoft Windows RPC
49157/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 00:15:D0:21:3B:85 (Microsoft)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Uptime guess: 0.007 days (since Wed Aug 12 22:32:44 2020)
Network Distance: 1 hop
```

Filter Hosts

10:44 PM 8/12/2020

8. Click the **Ports/Hosts** tab to check the Port, Protocol, State, Service, and Version of services discovered during the scan.

Note: The list of open ports might vary when you perform this task.

Zenmap

Scan Tools Profile Help

Target: 172.19.19.7

Command: nmap -T4 -A -v 172.19.19.7

Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans

OS Host www.luxurytreats.c

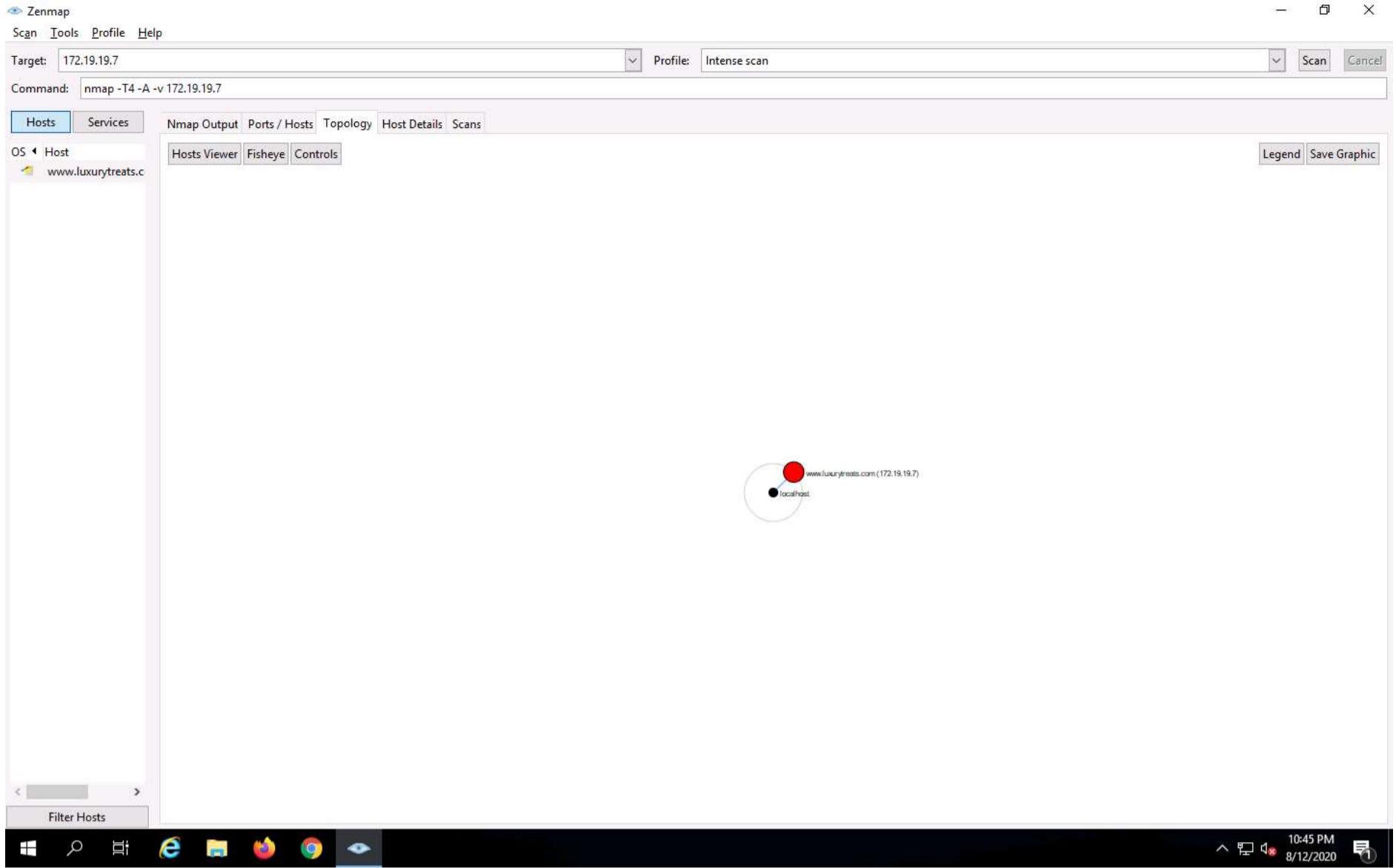
Port	Protocol	State	Service	Version
21	tcp	open	tcpwrapped	
80	tcp	open	http	Microsoft IIS httpd 7.5
135	tcp	open	msrpc	Microsoft Windows RPC
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	Windows Server 2008 R2 Enterprise 7601 Service Pack 1 microsoft-ds
3389	tcp	open	tcpwrapped	
49152	tcp	open	msrpc	Microsoft Windows RPC
49153	tcp	open	msrpc	Microsoft Windows RPC
49154	tcp	open	msrpc	Microsoft Windows RPC
49155	tcp	open	msrpc	Microsoft Windows RPC
49156	tcp	open	msrpc	Microsoft Windows RPC
49157	tcp	open	msrpc	Microsoft Windows RPC

Filter Hosts

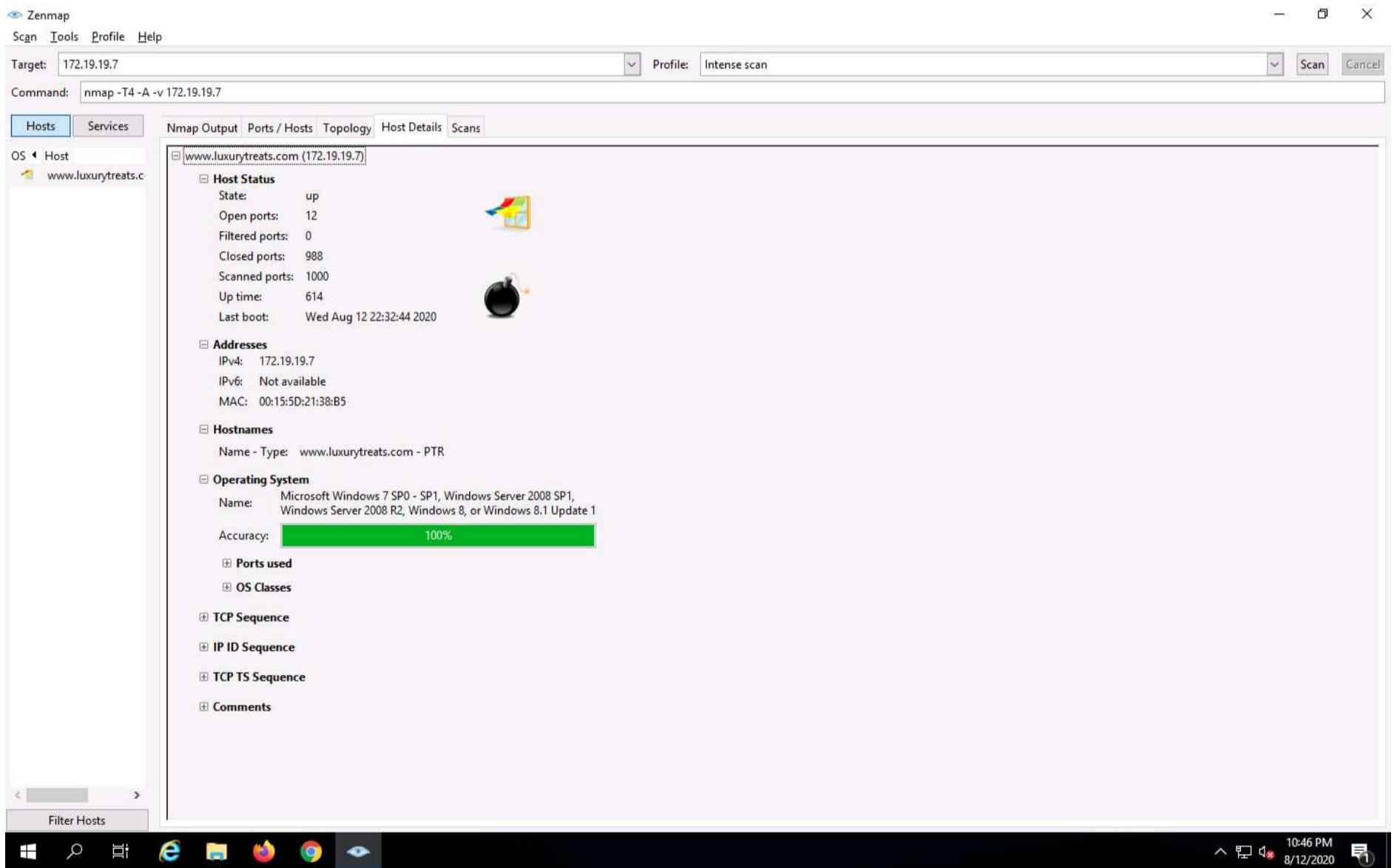
10:45 PM 8/12/2020

9. Click the **Topology** tab to view network topology of the target system.

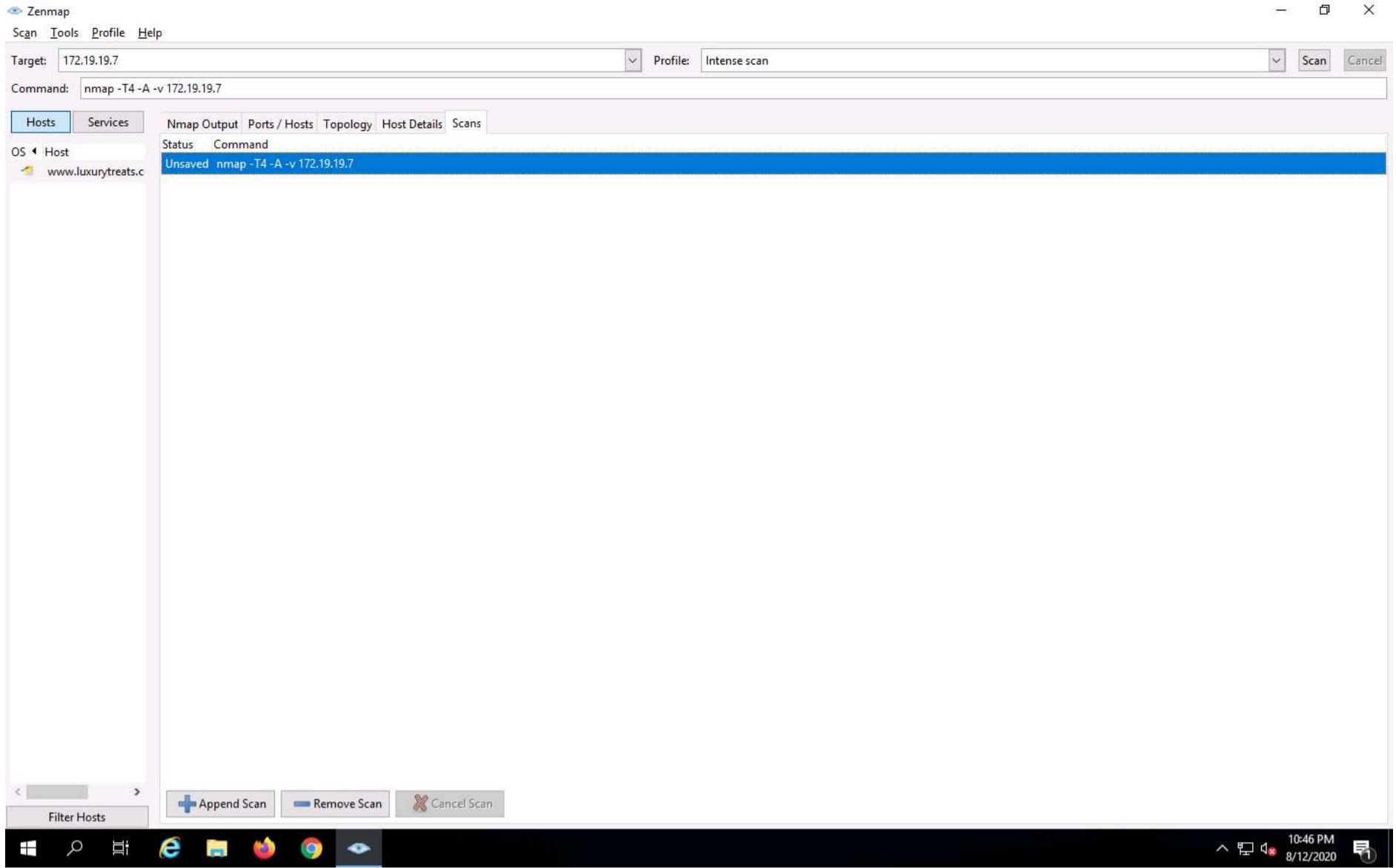




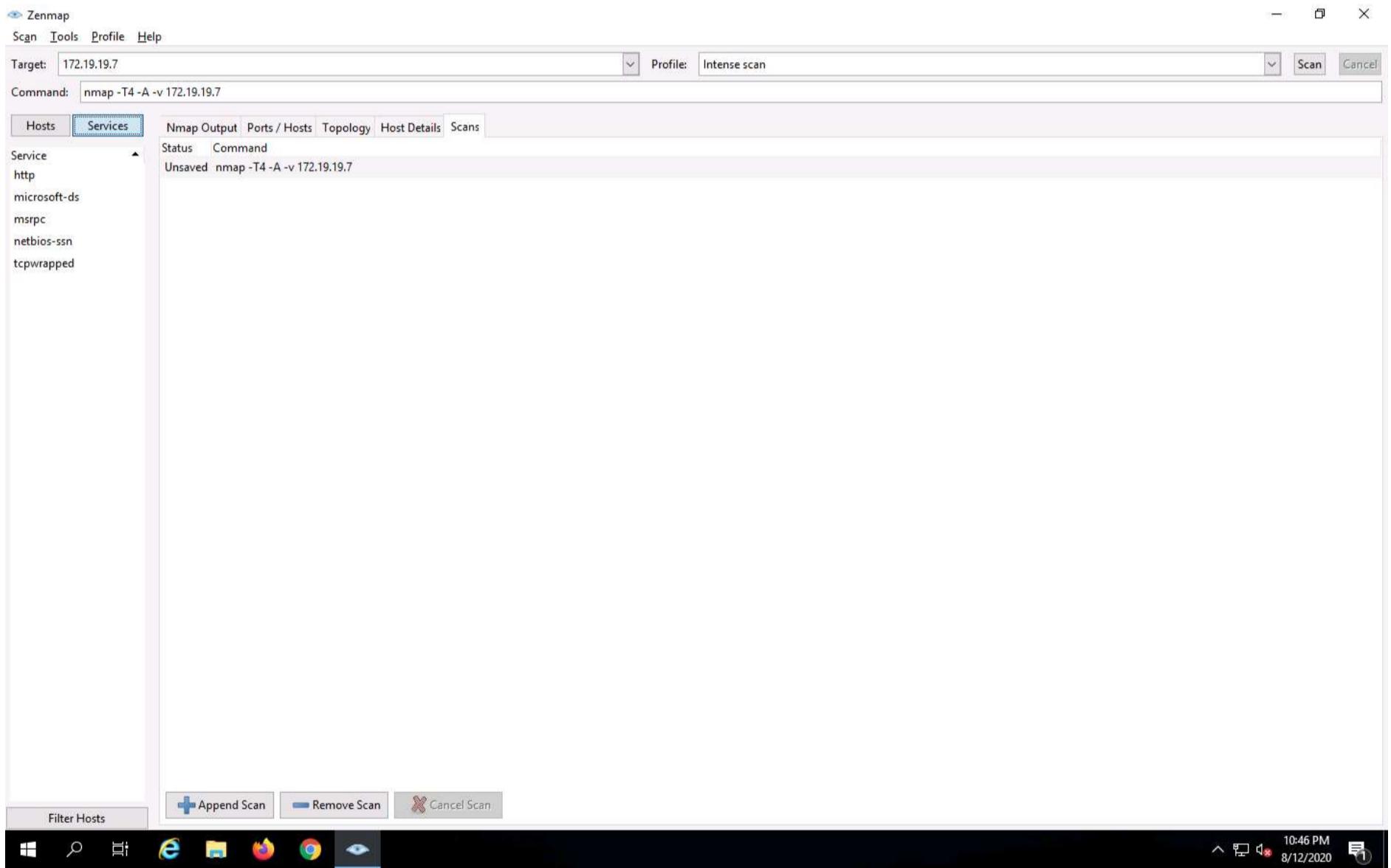
10. Click the **Host Details** tab to see the details of the hosts discovered during the intense scan.



11. Click the **Scans** tab to view the status of the scan, and command used.



12. Now, click the **Services** tab in the left pane. This tab displays the list of services running on the machine.



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.



The screenshot shows the Zenmap interface after a scan. The 'Services' tab is active, displaying a table of open ports:

Hostname	Port	Protocol	State	Version
www.luxurytreats.com (172.19.19.7)	49157	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49156	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49155	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49154	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49153	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49152	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	135	tcp	open	Microsoft Windows RPC

14. To save the scanned result, navigate to **Scan** and click **Save Scan** from the menu bar.

The screenshot shows the Zenmap interface with the 'Scan' menu open. The 'Save Scan' option is selected. The Services tab is active, displaying the same port list as before:

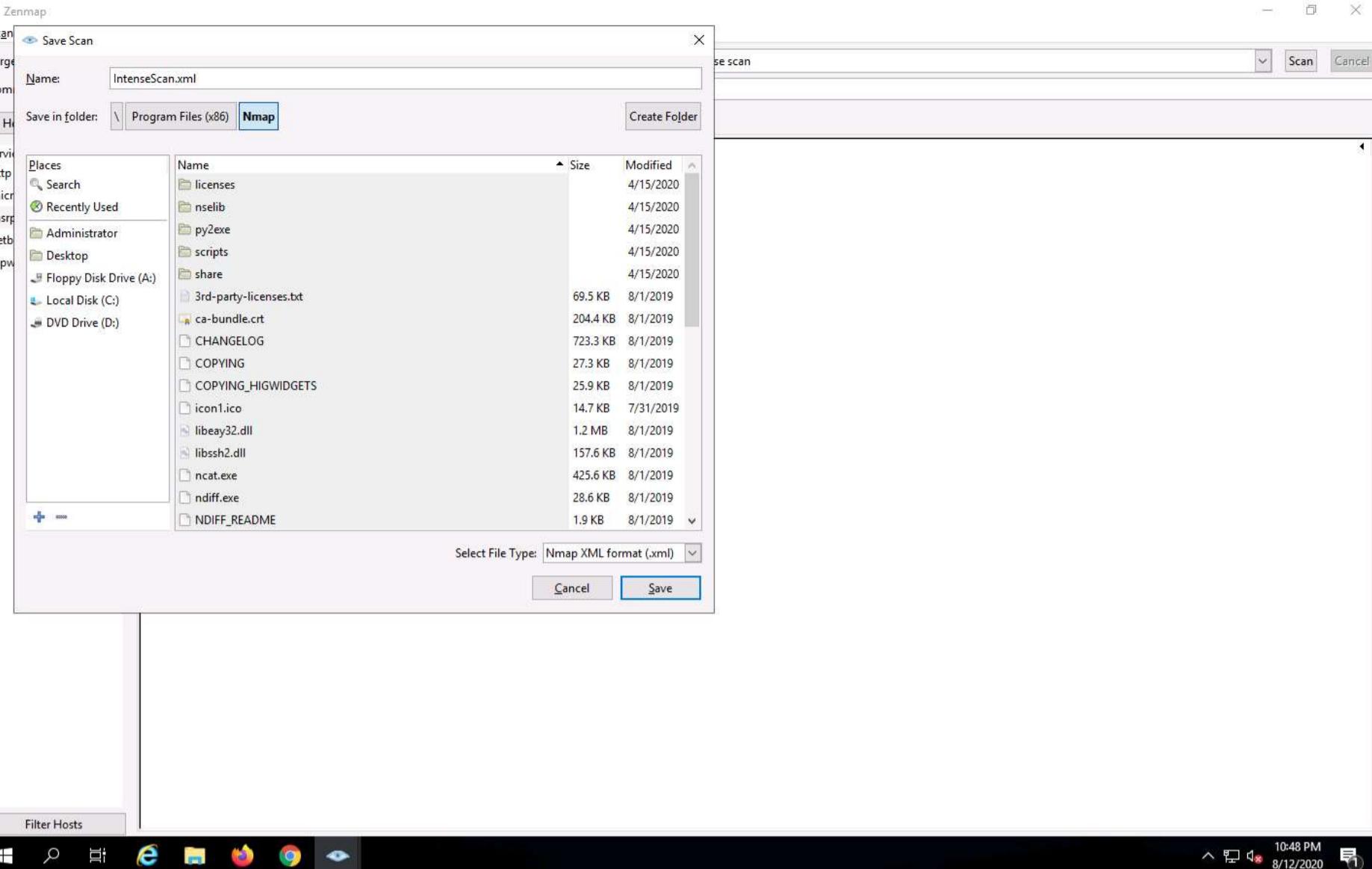
Hostname	Port	Protocol	State	Version
www.luxurytreats.com (172.19.19.7)	49157	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49156	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49155	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49154	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49153	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	49152	tcp	open	Microsoft Windows RPC
www.luxurytreats.com (172.19.19.7)	135	tcp	open	Microsoft Windows RPC

15. **Save Scan** window appears, specify the scan name in the **Name:** text field as **Intense Scan.xml**, specify the destination location in **Save in folder:** field, file type in **Select File Type:** field and click **Save**.

Note: In this lab, the default file location and default file type have been chosen.

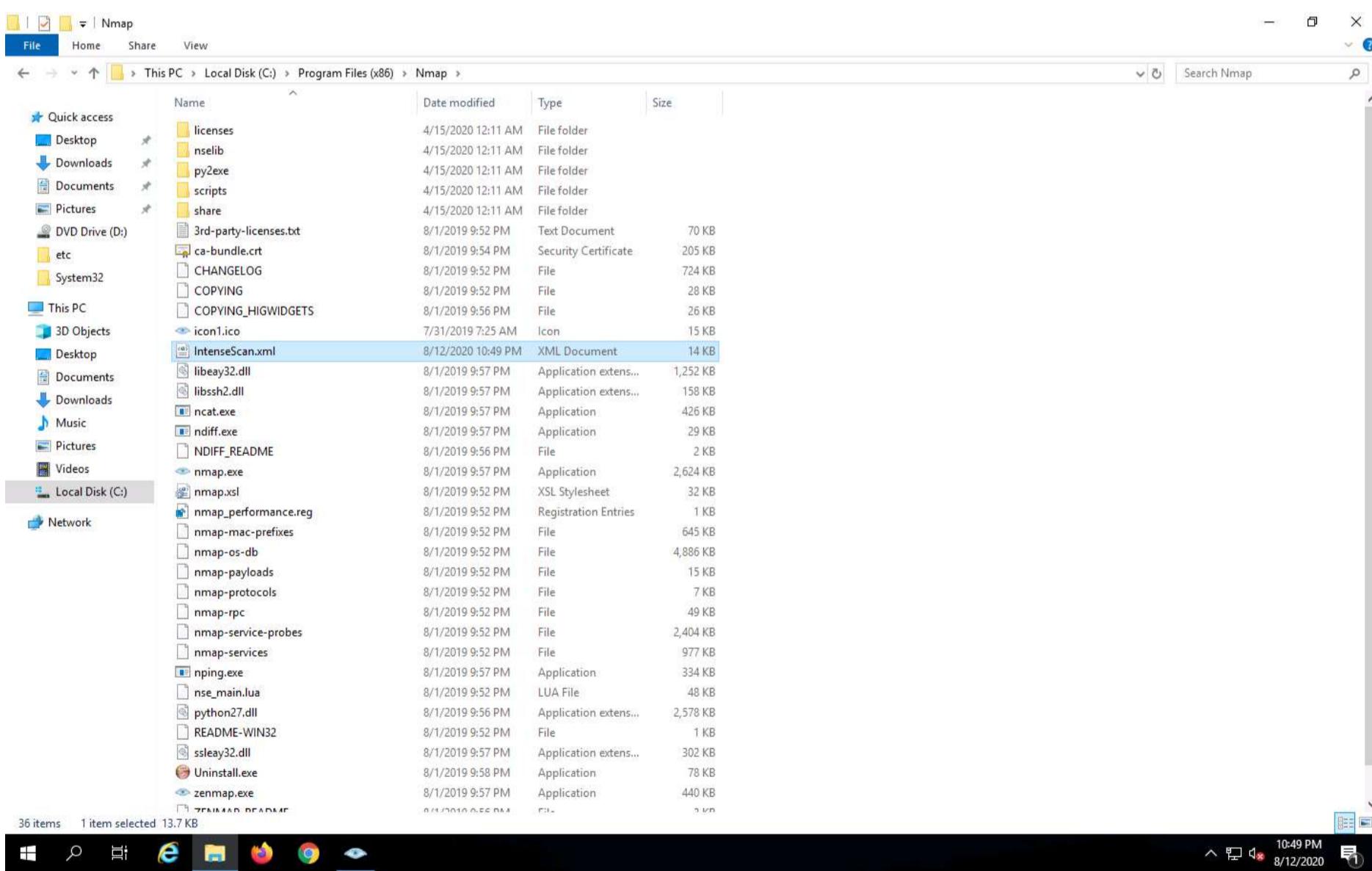
Note: You can even choose your desired location to save the result.





16. To view the result, navigate to **C:\Program Files (x86)\Nmap** and double-click **Intense Scan.xml**.

Note: Here, the saved file location is **C:\Program Files (x86)\Nmap**.



17. Now, you can view the **Intense Scan** report in the browser as shown in the screenshot.

Nmap Scan Report - Scanned at Wed Aug 12 22:41:19 2020

Scan Summary | [www.luxurytreats.com \(172.19.19.7\)](#)

Scan Summary

Nmap 7.80 was initiated at Wed Aug 12 22:41:19 2020 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)
- 00:15:5D:21:38:B5 - Microsoft (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	tcpwrapped	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		
49157	tcp open	msrpc	syn-ack	Microsoft Windows RPC		

Remote Operating System Detection

- Used port: 80/tcp (open)
- Used port: 1/tcp (closed)
- Used port: 40563/udp (closed)
- OS match: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (100%)

Go to top
Toggle Closed Ports
Toggle Filtered Ports

18. Now, close all the windows.

Note: If **Errors Occurred** pop-up appears, click **OK**.

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.

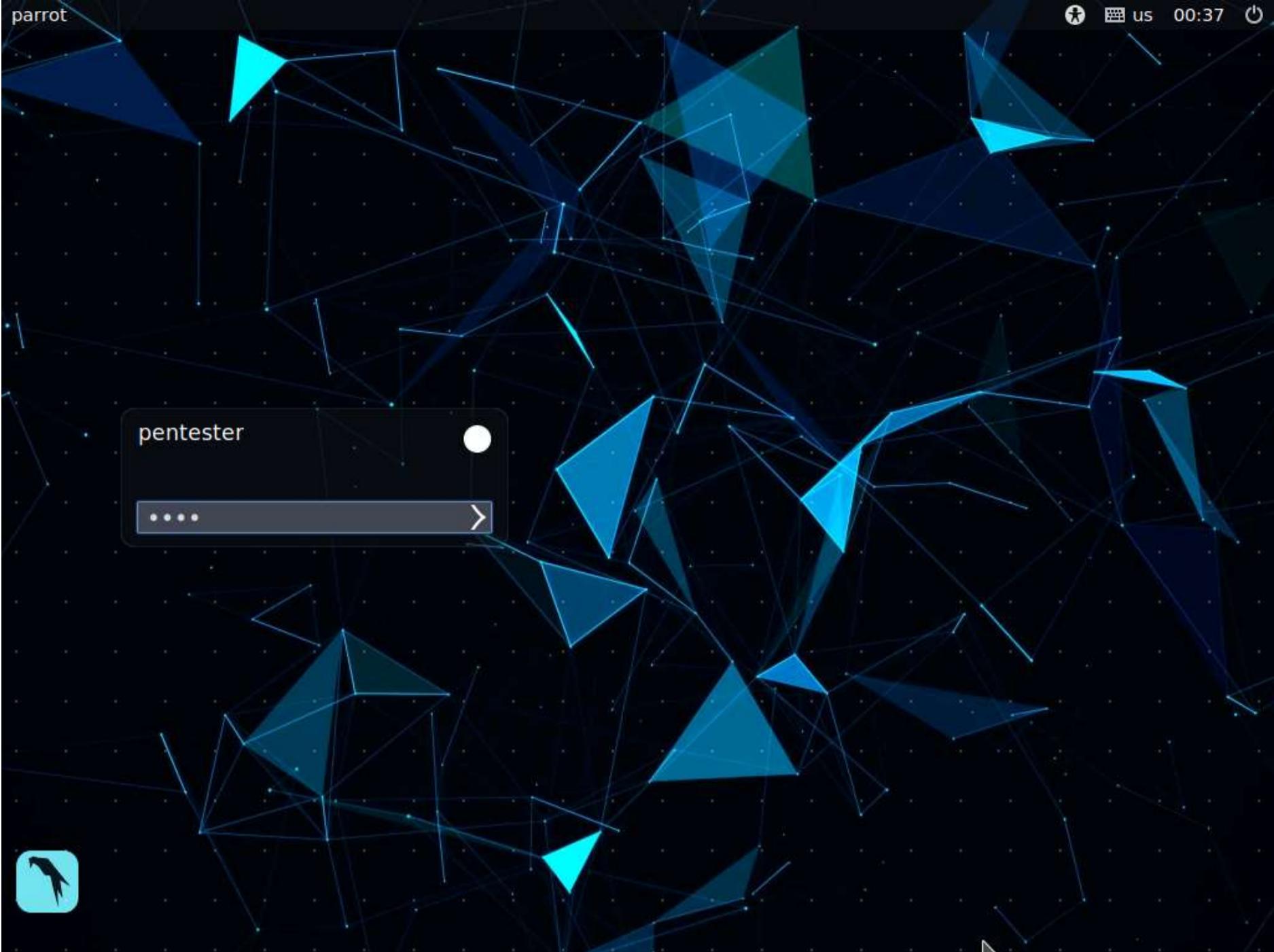
Exercise 2: Accessing Misconfigured FTP Connection on a Remote Machine Scenario

File transfer protocol allows authenticated users to upload/access and download files and folders between a client and a server. When anonymous access is enabled on the server, it allows everyone access files on it, leaving the security of sensitive information at risk.

As a pentester, you should be able to find the FTP servers inside a network which have anonymous access enabled. In this lab, you will be learning how to identify the FTP servers which have anonymous access enabled.

Lab Duration: 20 Minutes

1. Click **CPENT-M5 Parrot Security**. Parrot logon screen appears, type **toor** in the Password field and press **Enter**.



2. In this lab, we will be performing penetration testing on a machine to find any loopholes and gain access to its resources. For this, we are going to scan **CPENT-M5 Ubuntu Server** for open ports and services running on the machine. To scan, launch a command line terminal, type **nmap 172.19.19.10** and press **Enter**. This performs a Nmap regular scan on the machine and displays the results as shown in the screenshot.

Note: In this lab, we are scanning IP address of the target machine located in the external network, whereas, in real-time, you will be scanning domains for eg. **ftp.[targetwebsite].com**.



Applications Places System Parrot Terminal

File Edit View Search Terminal Help

```
[pentester@parrot] ~
└─ $ nmap 172.19.19.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-01 03:16 EDT
Nmap scan report for 172.19.19.10
Host is up (0.00051s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
READMELICENSE
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
[pentester@parrot] ~
└─ $
```

3. In the previous task, it was observed that ports **21, 22, 80** are open. Let us begin with port **21**. We shall first check if we can access FTP on the machine anonymously. For that, we will run Nmap scan with the **ftp-anon** script to find out whether anonymous login is enabled on the machine. Type **nmap -p 21 --script ftp-anon 172.19.19.10** and press **Enter** to begin the Nmap scan.

4. It is observed that Anonymous FTP Login is enabled on the FTP Server.

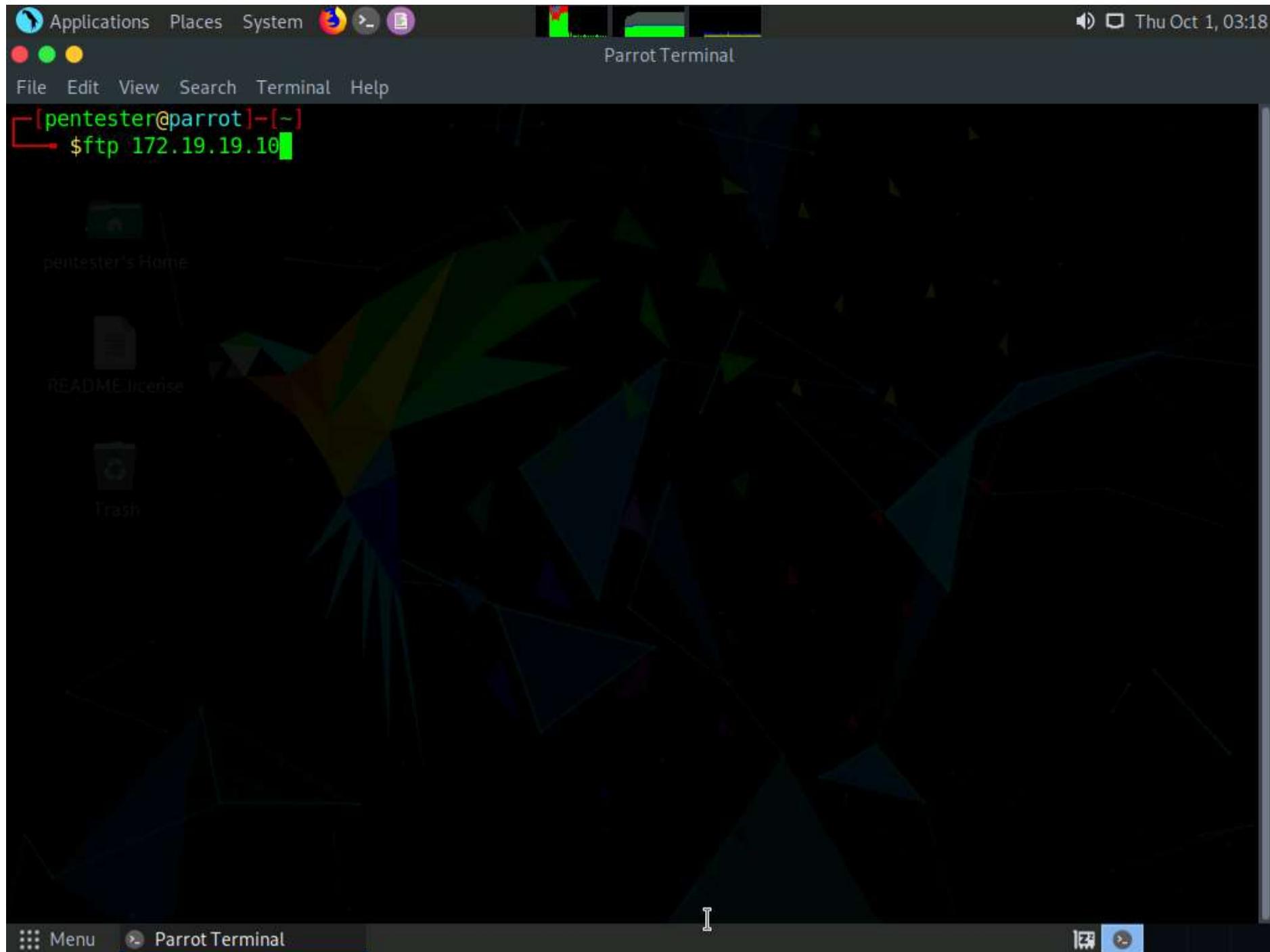
Applications Places System Parrot Terminal

File Edit View Search Terminal Help

```
[pentester@parrot] ~
└─ $ nmap -p 21 --script ftp-anon 172.19.19.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-01 03:18 EDT
Nmap scan report for 172.19.19.10
Host is up (0.00056s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxrwxrwx  2 ftp      ftp          4096 Aug 28  2018 public [NSE: writeable]
READMELICENSE
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
[pentester@parrot] ~
└─ $
```

5. Now, we shall log in to the FTP server and access contents in the FTP directory. Type **ftp 172.19.19.10** and press **Enter**.



6. You will be asked to enter a login name. Type **anonymous** and press **Enter**.

Note: If a **Password** field appears, leave it empty and press **Enter** to proceed.

7. Upon entering the login name, an ftp shell appears, stating that the FTP login has been successful. This shows we have successfully logged in to the remote machine using FTP.



```
[pentester@parrot] ~
└─ $ ftp 172.19.19.10
Connected to 172.19.19.10.
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>
```

8. Now, we shall view the files and directories inside the FTP root directory. To view them, type **ls** and press **Enter**. This displays all the directories and files in the FTP root directory, along with their file/directory permissions as shown in the screenshot below. It is observed that the directory permissions for "public" folder have read-write-execute access enabled to all the user groups. We shall attempt to upload a file to this directory in the forthcoming tasks.

```
[pentester@parrot] ~
└─ $ ftp 172.19.19.10
Connected to 172.19.19.10.
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> [REDACTED]
```

9. Now, we shall navigate to the **public** folder to view its contents. To navigate, type **cd public** and press **Enter**.



File Edit View Search Terminal Help

```
[pentester@parrot]~$ ftp 172.19.19.10
Connected to 172.19.19.10.
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>
```

10. Type **ls** and press Enter to view the files and folders inside the "public" folder.

File Edit View Search Terminal Help

```
[pentester@parrot]~$ ftp 172.19.19.10
Connected to 172.19.19.10.
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>
```

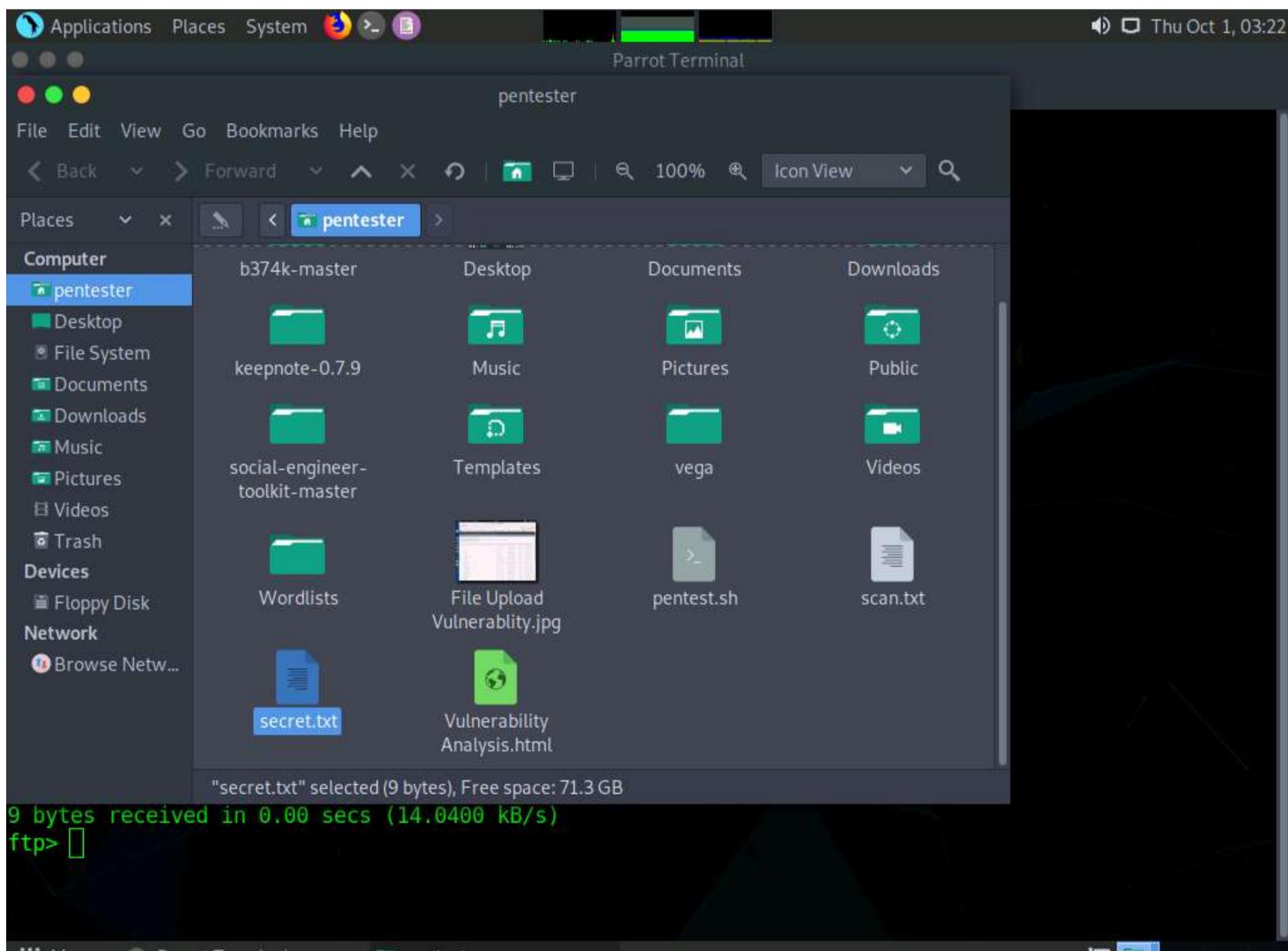
11. You will observe the file named **secret.txt** in the folder.

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**.



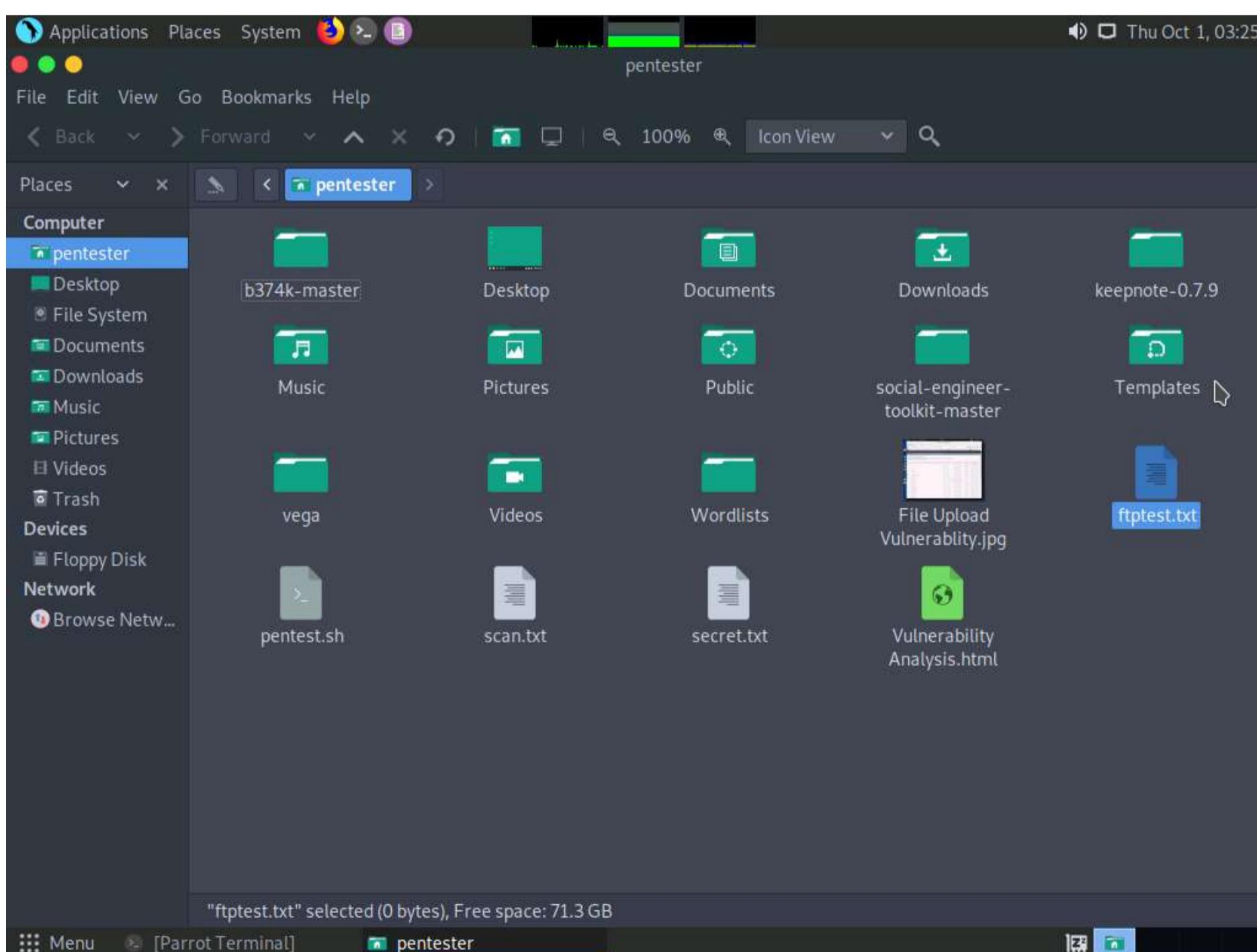
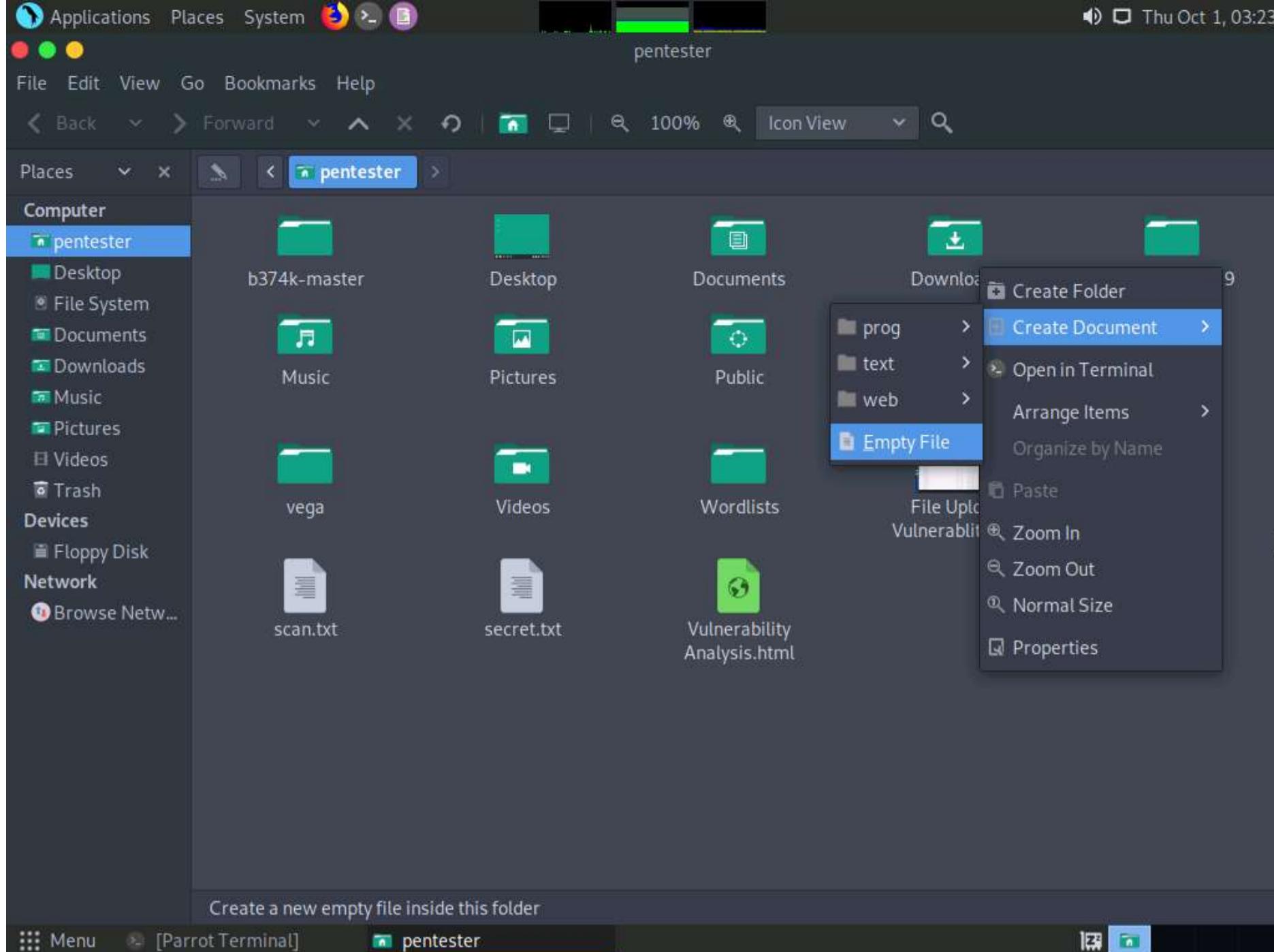
```
[pentester@parrot] ~
$ ftp 172.19.19.10
Connected to 172.19.19.10.
220 (vsFTPd 3.0.2)
Name (172.19.19.10:pentester): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory 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 (14.0400 kB/s)
ftp> 
```

13. The downloaded file is saved to the **Home** folder as shown in the screenshot below.



14. Now, we shall see if we can upload a file to the FTP server. Create a file **ftptest.txt** (as an example) in the **Home** folder of Parrot machine to send it to the FTP Server. Open your **Home** Folder and **Right Click** and navigate to **Create Document** and click **Empty File** and name the file as **ftptest.txt**. Go back to **Terminal**, to upload type **put ftptest.txt** and press **Enter**.





```
[pentester@parrot]~$ ftp 172.19.19.10
Connected to 172.19.19.10.
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 (14.0400 kB/s)
ftp> put ftptest.txt
```

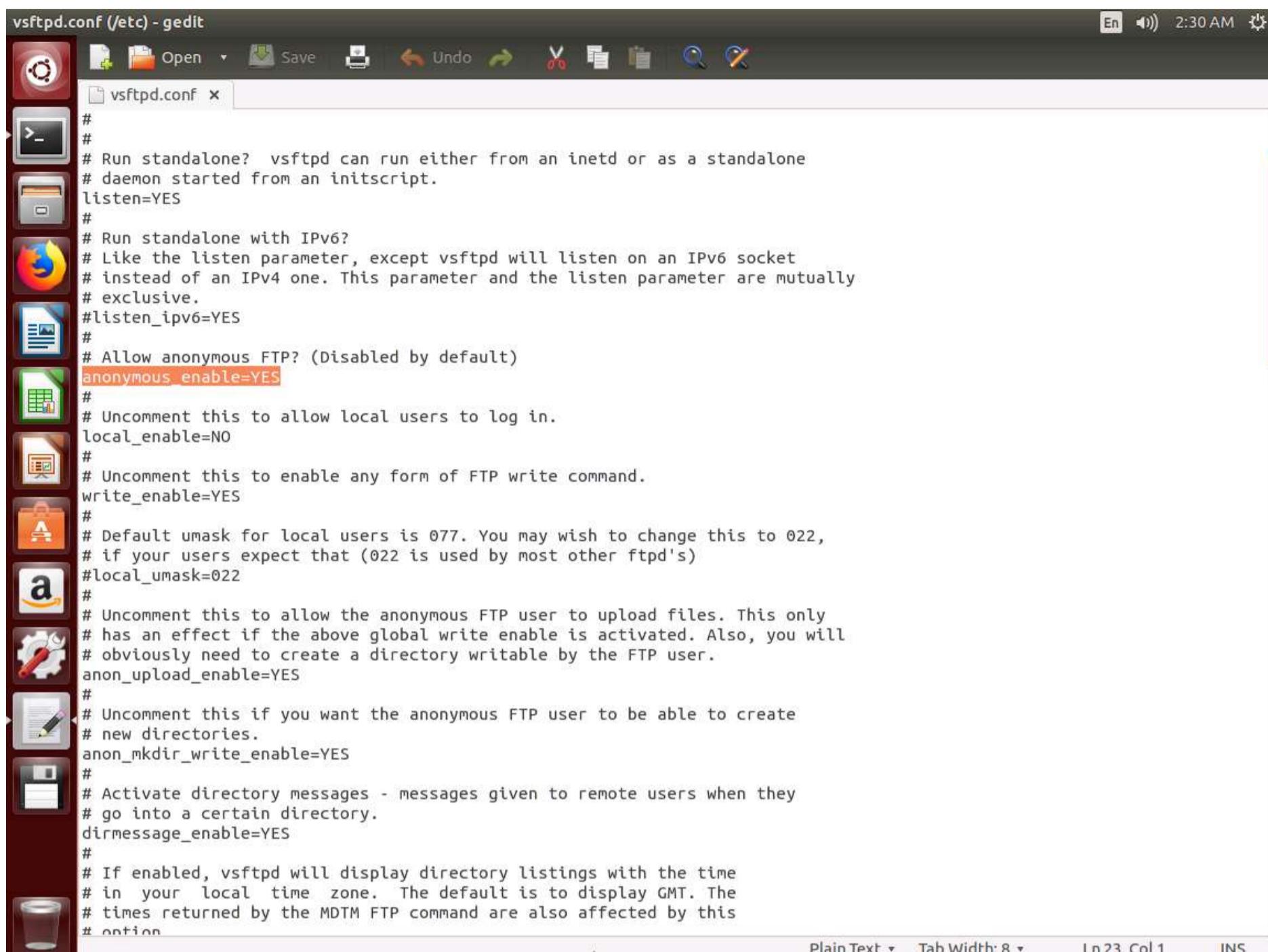
15. The file was successfully uploaded to the server as shown in the screenshot below. This means that file upload access has been enabled on the Ubuntu Server which can allow an attacker to upload malicious files to it.

```
[pentester@parrot]~$ ftp 172.19.19.10
Connected to 172.19.19.10.
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 (14.0400 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>
```

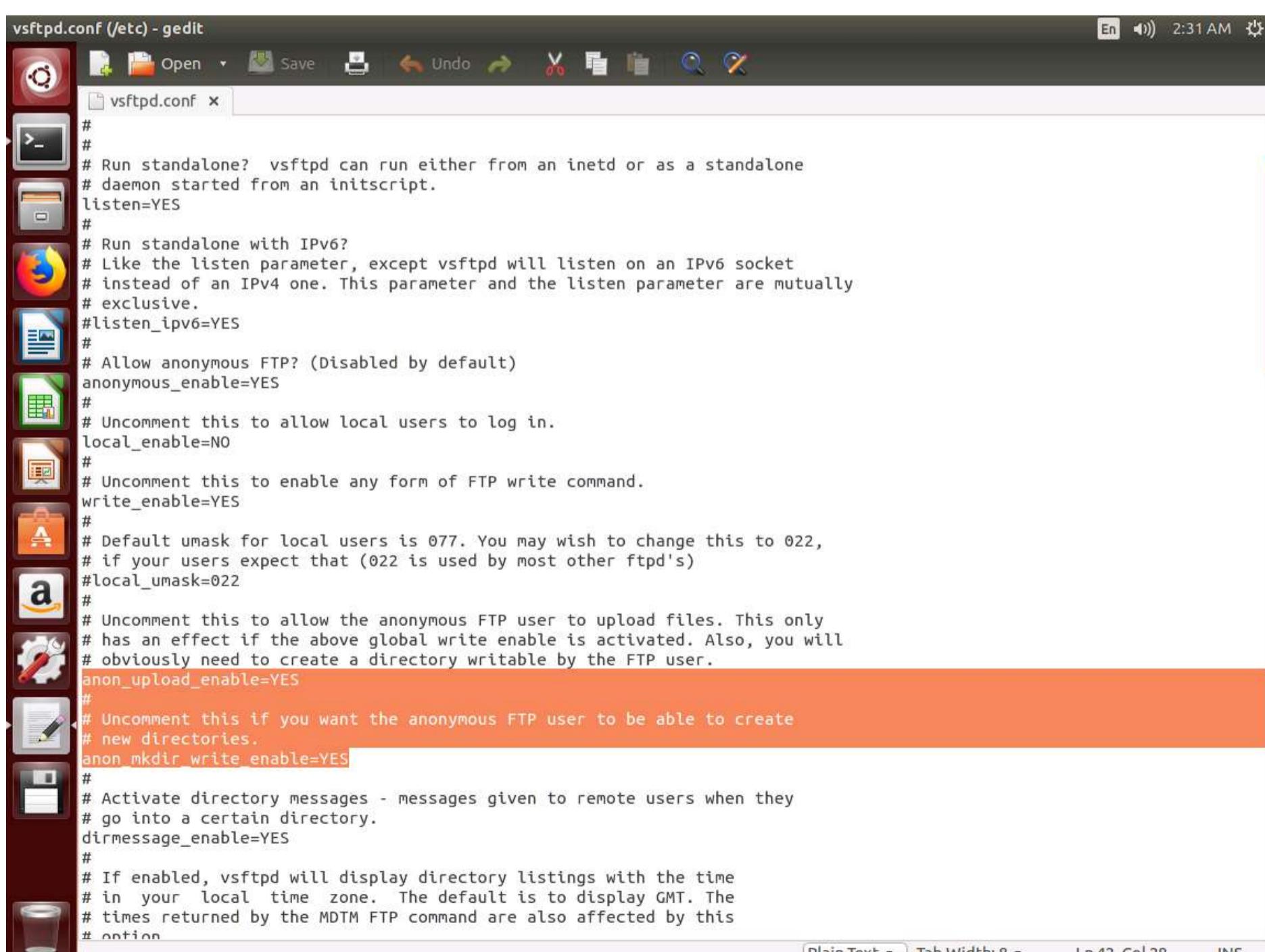
16. Now, we will switch to **CPENT-M5 Ubuntu Server** machine (credentials: **Student/password**) and check the vsftpd.conf file.

Note: To access vsftpd.conf file, open **Files** and navigate to **Other Locations --> Computer --> etc**. In the **/etc** folder, scroll-down to the end of the page and double-click **vsftpd.conf** file.

17. As highlighted in the screenshot, the options **anonymous_enable**, **anon_upload_enable** and **anon_mkdir_write_enable** have been enabled which allowed us to login to FTP server anonymously and upload files to it.



```
vsftpd.conf (/etc) - gedit
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# Run standalone with IPv6?
# Like the listen parameter, except vsftpd will listen on an IPv6 socket
# instead of an IPv4 one. This parameter and the listen parameter are mutually
# exclusive.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default)
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=NO
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option
```



```
vsftpd.conf (/etc) - gedit
# Run standalone? vsftpd can run either from an inetd or as a standalone
# daemon started from an initscript.
listen=YES
#
# Run standalone with IPv6?
# Like the listen parameter, except vsftpd will listen on an IPv6 socket
# instead of an IPv4 one. This parameter and the listen parameter are mutually
# exclusive.
#listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default)
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=NO
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
#local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
# in your local time zone. The default is to display GMT. The
# times returned by the MDTM FTP command are also affected by this
# option
```

Exercise 3: Enumerate a Wordpress Site

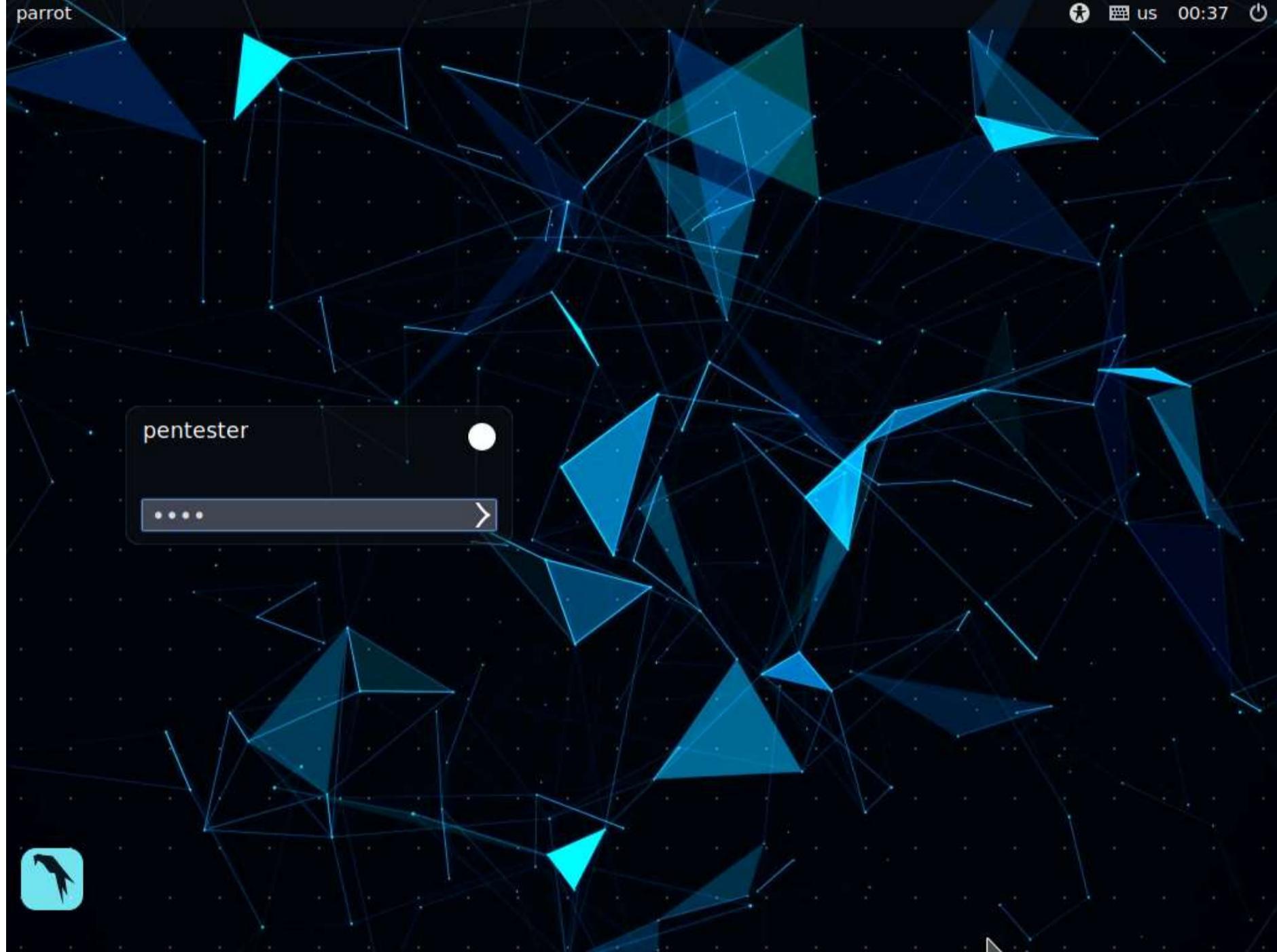
Scenario

In this lab, you will:

- Use the wpscan tool
- Enumerate a Wordpress site

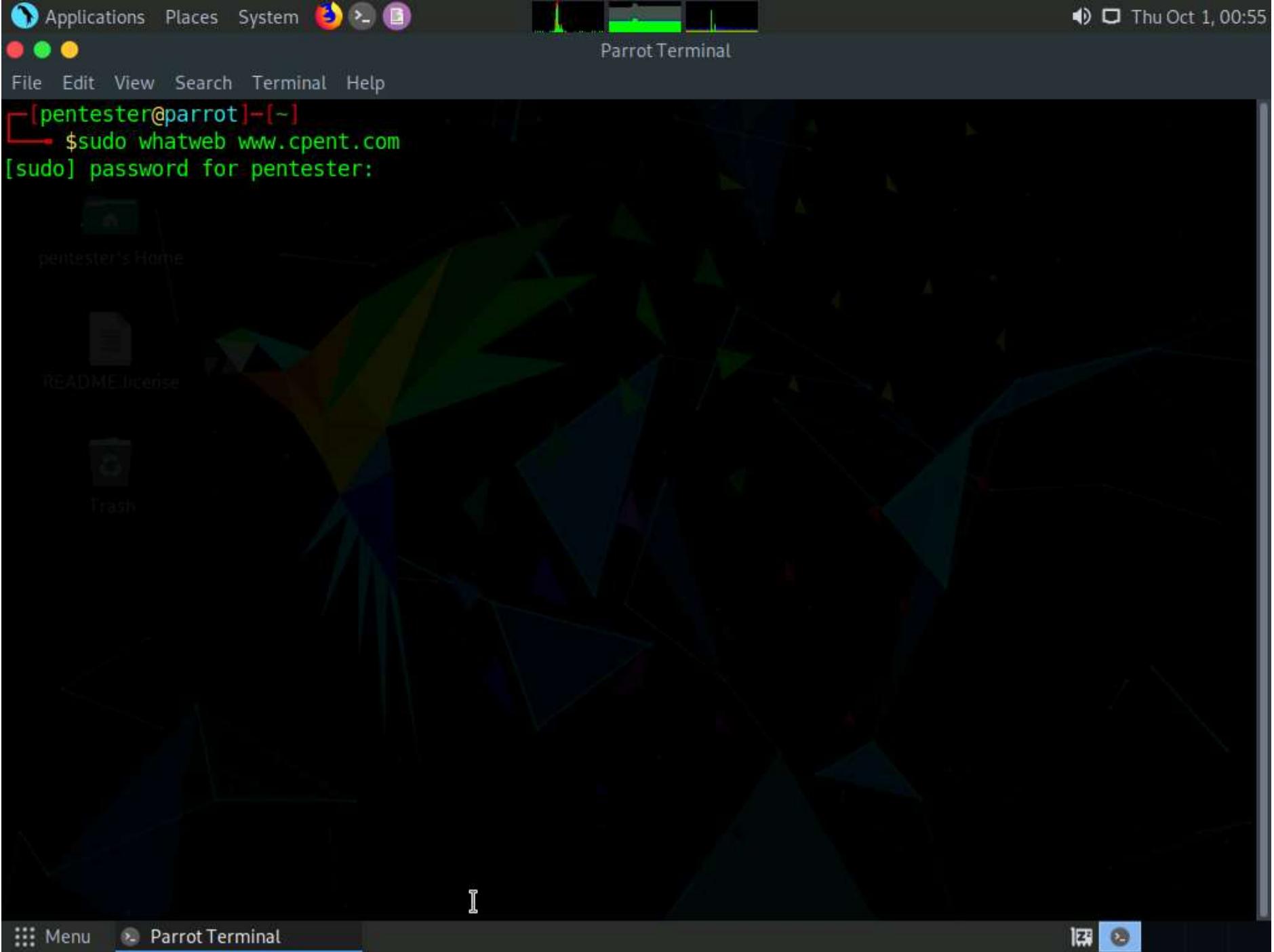
Lab Duration: 25 Minutes

1. Click **CPENT-M5 Parrot Security**. Parrot logon screen appears, type **toor** in the Password field and press **Enter**.

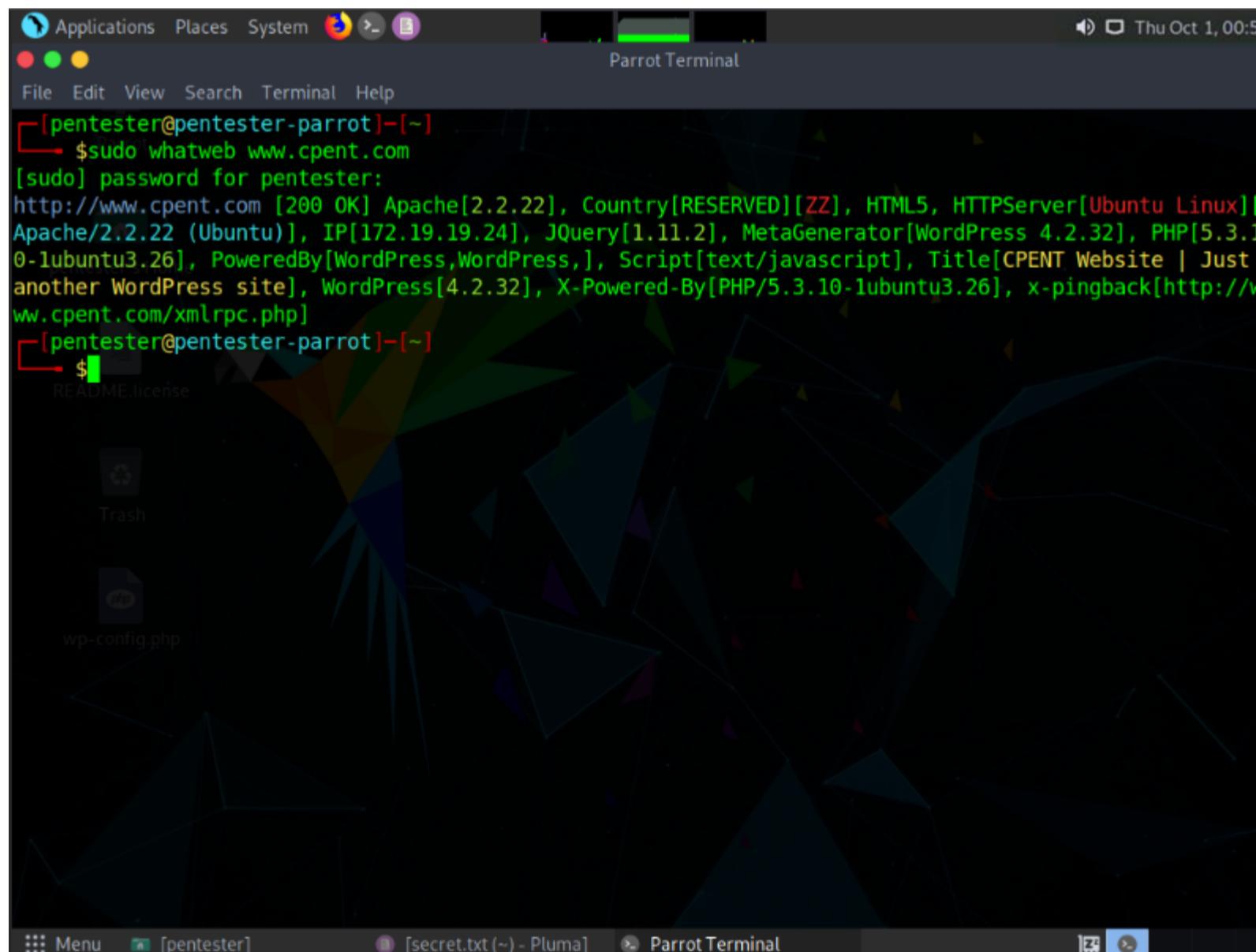


2. Use the **wpscan** tool to scan a website that is running **Wordpress**. First, scan the site to check what installed software and version number come up.
3. Launch a Terminal, and type **sudo whatweb www.cpent.com** and press **Enter**. Type **toor** when prompted for Password and press **Enter**.





4. Record the information as required onto your target database. Once you are successful, search for vulnerabilities using the version of **Wordpress** available, which is **4.2.32**.



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.

[pentester@parrot] ~]\$ sudo wpscan --url http://www.cpent.com --enumerate u

Wordpress Security Scanner by the WPScan Team
Version 3.8.6

@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://www.cpent.com/ [172.19.19.24]
[+] Started: Thu Oct 1 00:59:29 2020

Interesting Finding(s):

[+] Headers
| Interesting Entries:
| - Server: Apache/2.2.22 (Ubuntu)
| - X-Powered-By: PHP/5.3.10-1ubuntu3.26
| Found By: Headers (Passive Detection)
| Confidence: 100%

Menu Parrot Terminal

File Edit View Search Terminal Help

Found By: Css Style In Homepage (Passive Detection)

Version: 1.6 (80% confidence)
Found By: Style (Passive Detection)
- http://www.cpent.com/wp-content/themes/twentyfifteen/style.css?ver=4.6.10, Match: Version: 1.6

[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:01 <===== (10 / 10) 100.00% Time: 00:00:01

READMEDisclaimer

[i] User(s) Identified:

[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

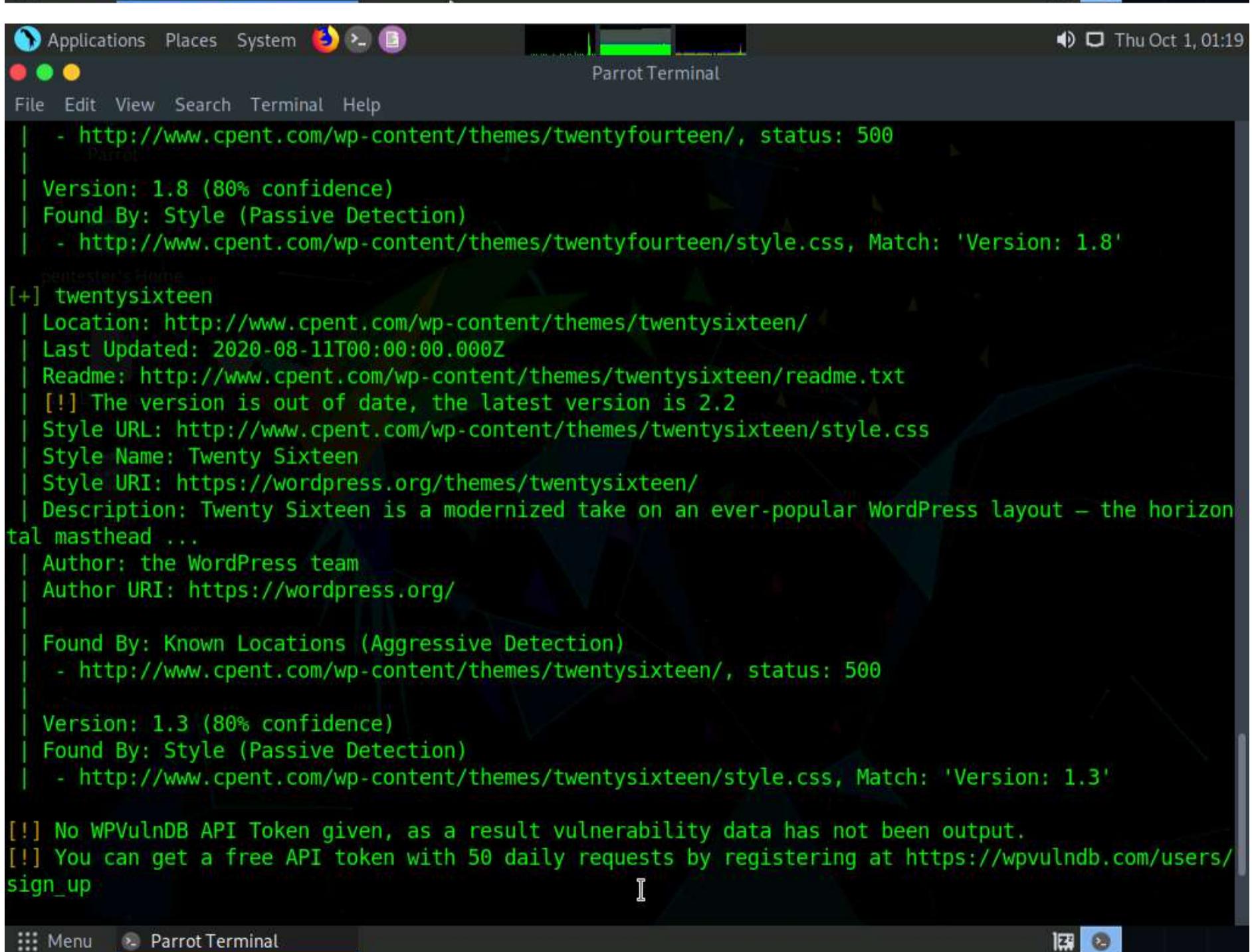
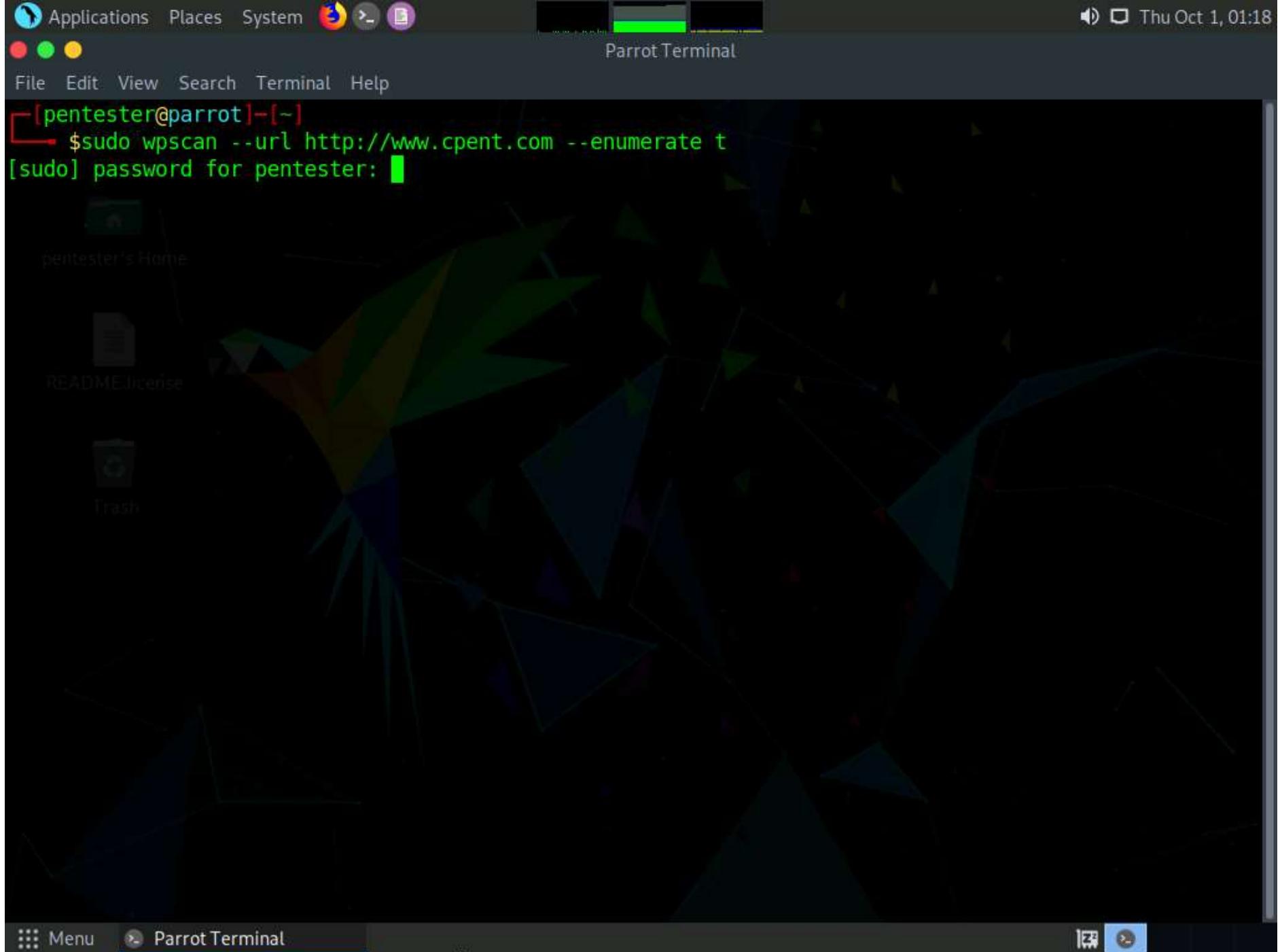
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[+] Finished: Thu Oct 1 00:59:34 2020
[+] Requests Done: 66
[+] Cached Requests: 5
[+] Data Sent: 13.041 KB
[+] Data Received: 15.559 MB
[+] Memory used: 162.164 MB
[+] Elapsed time: 00:00:04

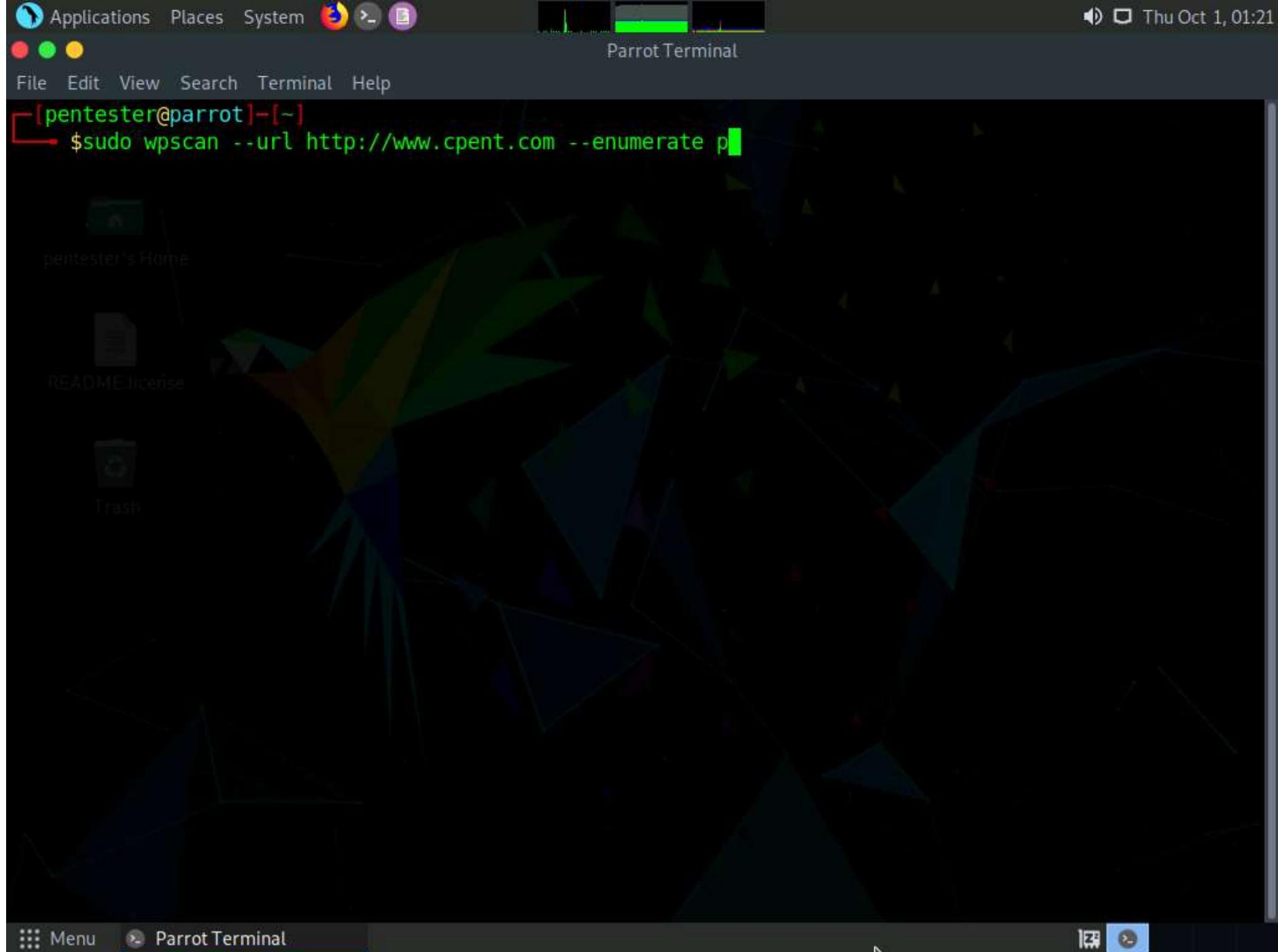
[pentester@parrot] ~]\$

Menu Parrot Terminal

6. Type **sudo wpscan --url http://www.cpent.com --enumerate t** and press **Enter**. Type **toor** if prompted for Password and press **Enter**. This will enumerate the installed themes, if there exists any. Explore all themes that appear.



7. Now, 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.



```
File Edit View Search Terminal Help
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[i] Plugin(s) Identified:
[+] ebook-download
| Location: http://www.cpent.com/wp-content/plugins/ebook-download/
| Last Updated: 2020-03-12T12:52:00.000Z
| [!] The version is out of date, the latest version is 1.5
| Found By: Urls In Homepage (Passive Detection)
| Version: 1.1 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://www.cpent.com/wp-content/plugins/ebook-download/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://www.cpent.com/wp-content/plugins/ebook-download/readme.txt
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
[+] Finished: Thu Oct 1 01:22:06 2020
[+] Requests Done: 4
[+] Cached Requests: 30
[+] Data Sent: 1.036 KB
[+] Data Received: 3.284 KB
[+] Memory used: 199.266 MB
[+] Elapsed time: 00:00:03
[pentester@parrot]~
```

8. As noted earlier, the process itself is key; once you follow the steps, the data can be enumerated irrespective of the target version.

Exercise 4: Perform Web Application Scanning with WMAP

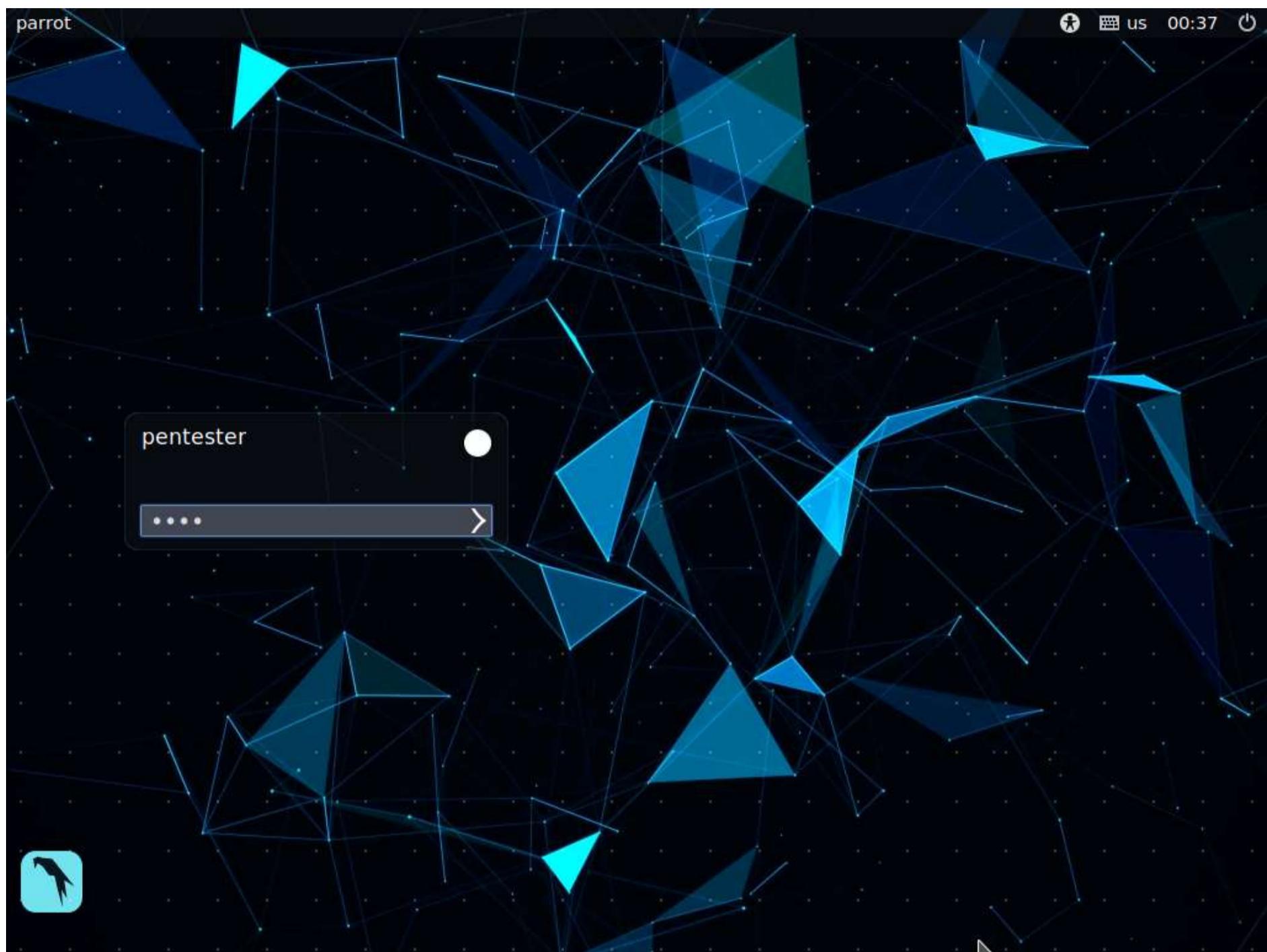


Scenario

The WMAP tool is used for web application scanning from within the Metasploit console. In this lab you will

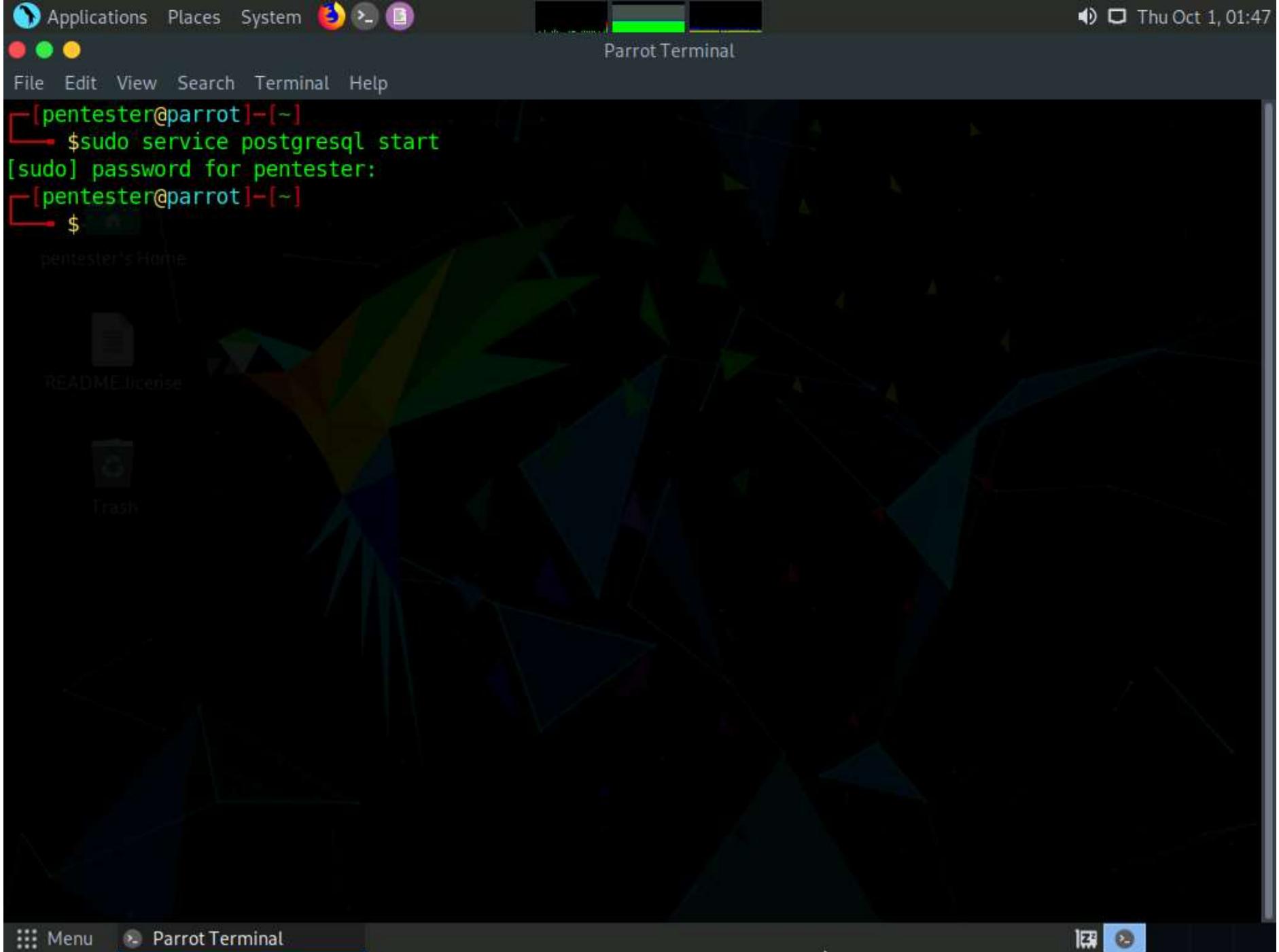
- Use the tool WMAP that is part of the Metasploit tools
- Scan a web servers with WMAP

1. Click **CPENT-M5 Parrot Security**. Parrot logon screen appears, type **toor** in the Password field and press **Enter**.

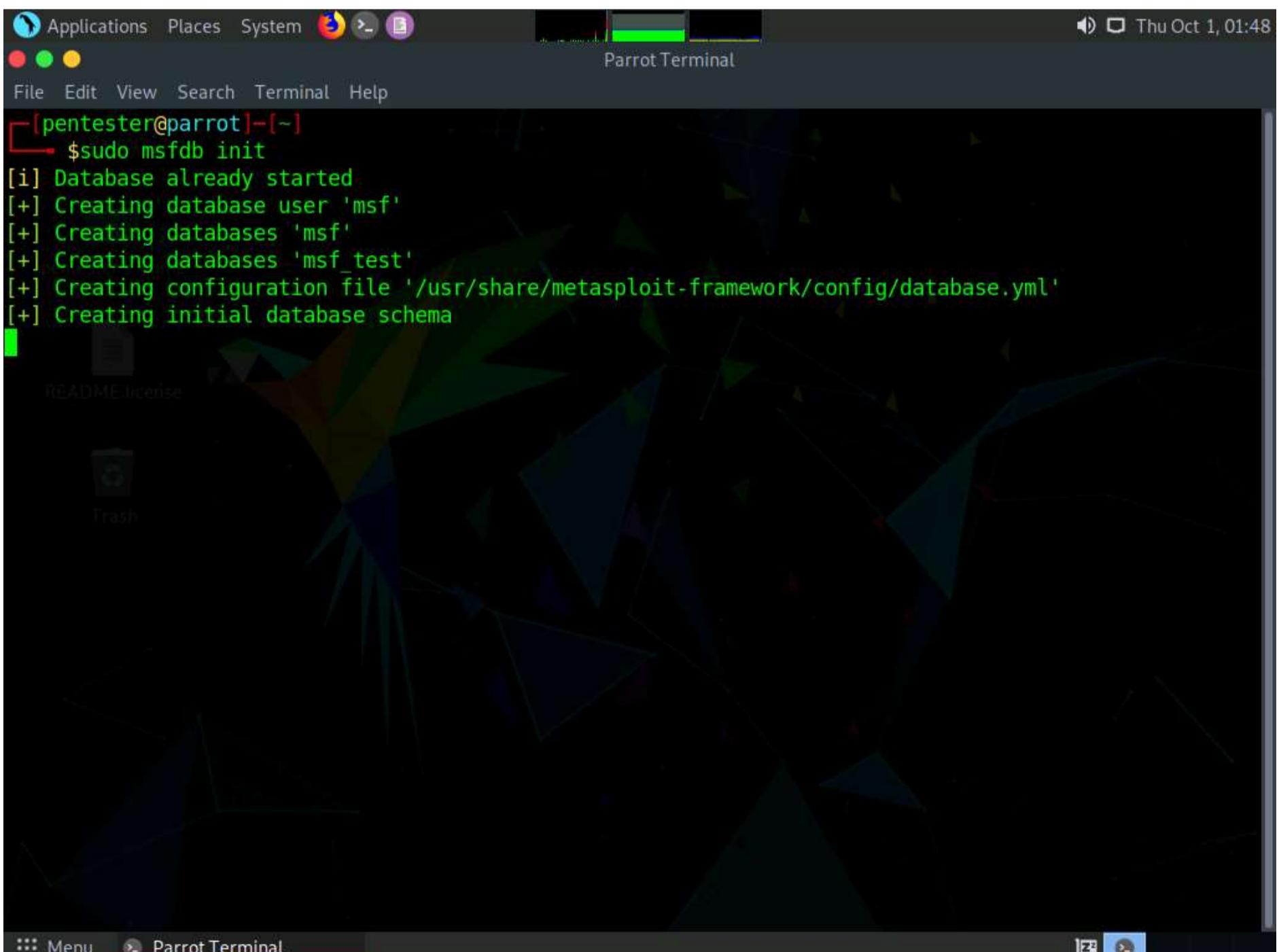


2. The WMAP tool is used for web application scanning from within the Metasploit console, as we did before, we have to setup the database before launching the console, so let us do that now. Open a terminal window and type **sudo service postgresql start** and press **Enter**. Type **toor** when prompted for Password and press **Enter**.





3. If this is the first time running Metasploit, then we need to run **msfdb init** but if it is not the first time, then we can launch the console. Type **sudo msfdb init** and press **Enter**.



4. Type **sudo msfconsole** and press **Enter** to launch the metasploit framework.



```
[pentester@parrot] ~
$ sudo msfconsole

[metasploit v6.0.0-dev]
+ [ 2052 exploits - 1108 auxiliary - 345 post ]
+ [ 566 payloads - 45 encoders - 10 nops ]
+ [ 7 evasion ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf6 >
```

5. Once msfconsole opens we now have to load the wmap tool, type **load wmap** and press **Enter**. This will load the tool, once the tool is loaded we can now setup the scans with it.

```
[pentester@parrot] ~
$ sudo msfconsole

[metasploit v6.0.0-dev]
+ [ 2052 exploits - 1108 auxiliary - 345 post ]
+ [ 566 payloads - 45 encoders - 10 nops ]
+ [ 7 evasion ]

Metasploit tip: Search can apply complex filters such as search cve:2009 type:exploit, see all the filters with help search

msf6 > load wmap

[*] WMAP 1.5.1 loaded
[*] Successfully loaded plugin: wmap
msf6 >
```

6. The next thing we have to do is add the sites, type **wmap_sites -a http://www.goodshopping.com** and press **Enter** to add the first site. Once the one site is added, add another site, type **wmap_sites -a http://www.luxurytreats.com** and press **Enter** to add the second site.



```
File Edit View Search Terminal Help
msf6 > wmap_sites -a http://www.goodshopping.com
[*] Site created.
msf6 > wmap_sites -a http://www.luxurytreats.com
[*] Site created.
msf6 >
```

7. Now we want to add our two targets, type **wmap_targets -t http://172.19.19.22** and press **Enter**. Enter the 2nd target, type **wmap_targets -t http://172.19.19.7** and press **Enter**.

Note: **172.19.19.22** is the IP address of the machine where **www.goodshopping.com** is hosted and **172.19.19.7** is the IP address of the machine where **www.luxurytreats.com** is hosted.

```
File Edit View Search Terminal Help
msf6 > wmap_targets -t http://172.19.19.22
msf6 > wmap_targets -t http://172.19.19.7
msf6 >
```



8. To view the targets type **wmap_targets -l** and press **Enter**.

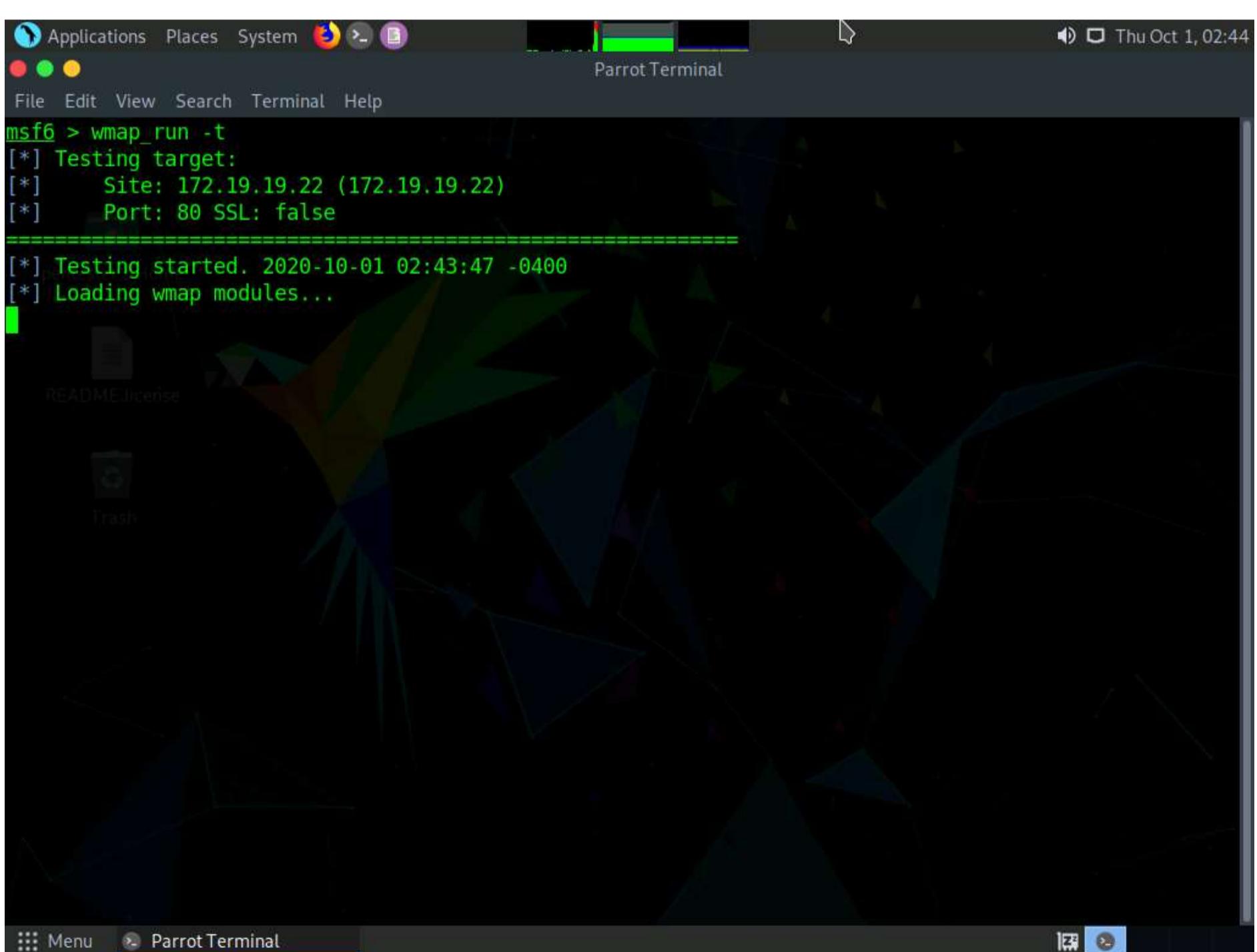
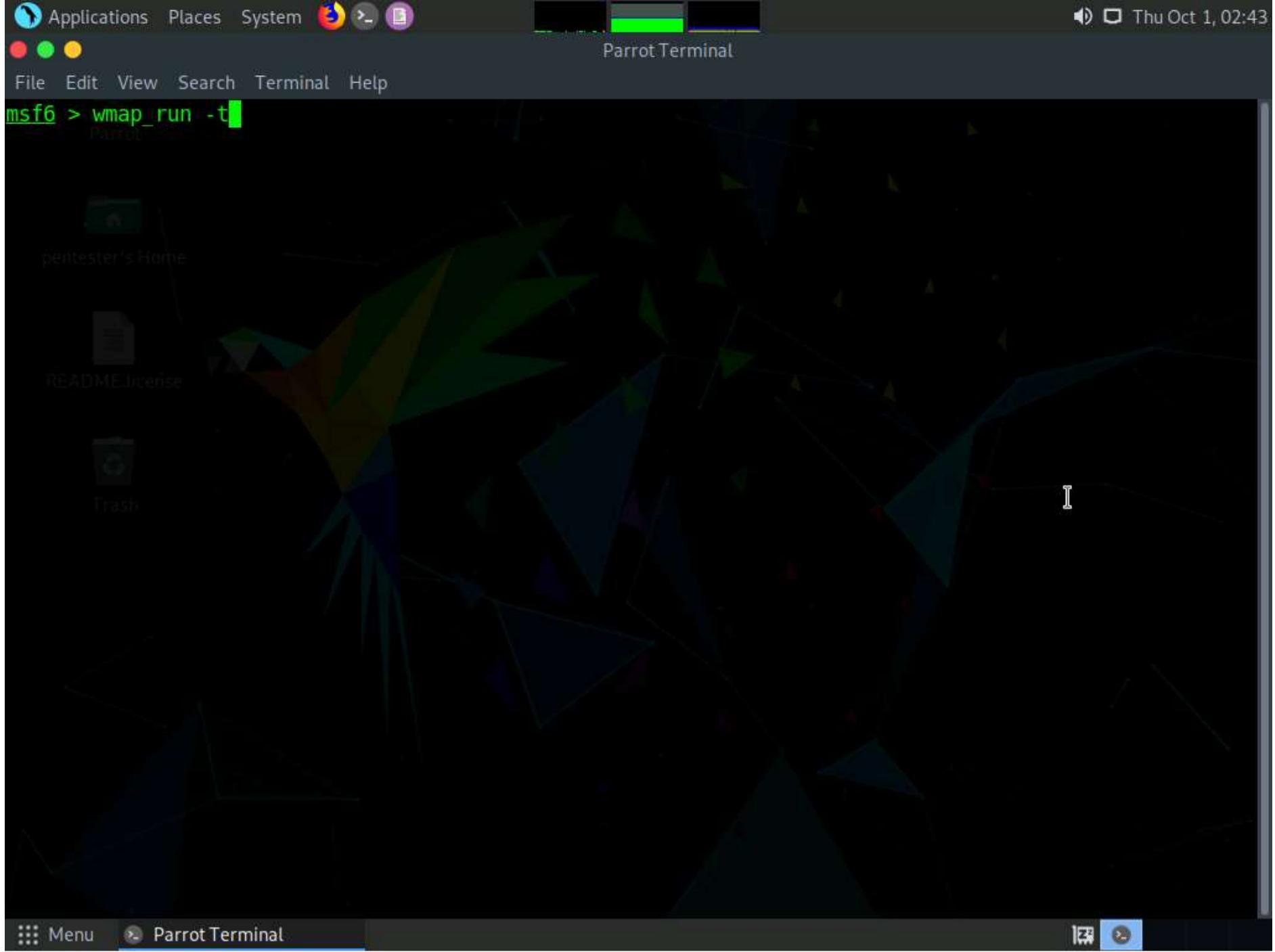
```
msf6 > wmap_targets -l
[*] Defined targets
=====
  Id  Vhost        Host        Port  SSL  Path
  0  172.19.19.22 172.19.19.22  80   false  /
  1  172.19.19.7  172.19.19.7   80   false  /
```

9. The next thing to do, is look at the options for the **wmap_run** command, type **wmap_run -h** and press **Enter**.

```
msf6 > wmap_run -h
[*] Usage: wmap_run [options]
      -h          Display this help text
      -t          Show all enabled modules
      -m [regex]   Launch only modules that name match provided regex.
      -p [regex]   Only test path defined by regex.
      -e [/path/to/profile] Launch profile modules against all matched targets.
                           (No profile file runs all enabled modules.)
```

10. We now need to run the modules that we are going to use to test the target, type **wmap_run -t** and press **Enter**. Once the command has completed, take a few minutes and review the information from the lab, as you can see there are many modules that have been loaded based on the site.





File Edit View Search Terminal Help

```
msf6 > wmap_run -t
[*] Testing target:
[*]   Site: 172.19.19.22 (172.19.19.22)
[*]   Port: 80 SSL: false
=====
[*] Testing started. 2020-10-01 02:43:47 -0400
[*] Loading wmap modules...
[*] 39 wmap enabled modules loaded.
[*]
=[ SSL testing ]=
=====
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
=====
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/trace
[*] Module auxiliary/scanner/http/vhost_scanner
[*] Module auxiliary/scanner/http/webdav_internal_ip
[*] Module auxiliary/scanner/http/webdav_scanner
```

Menu Parrot Terminal

File Edit View Search Terminal Help

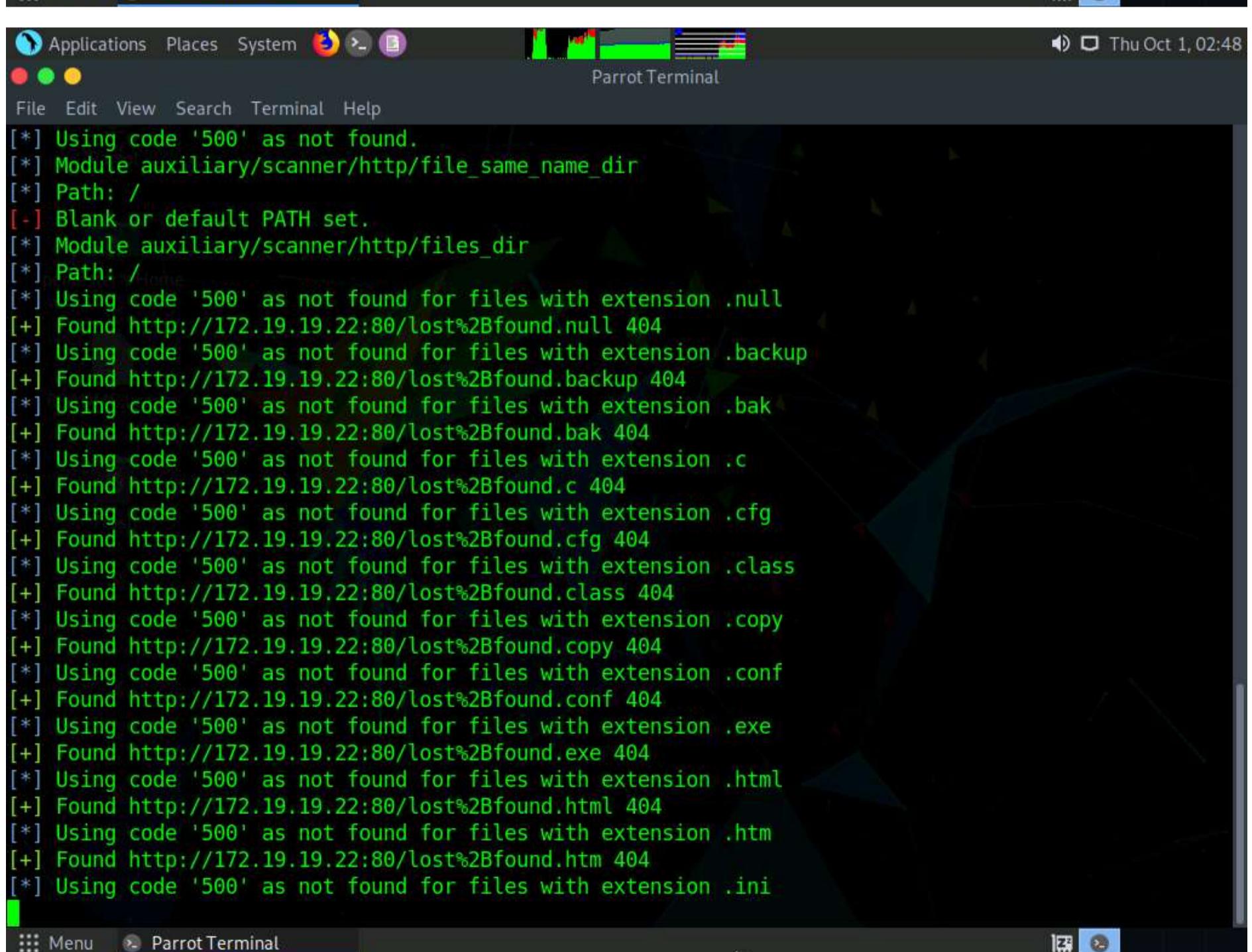
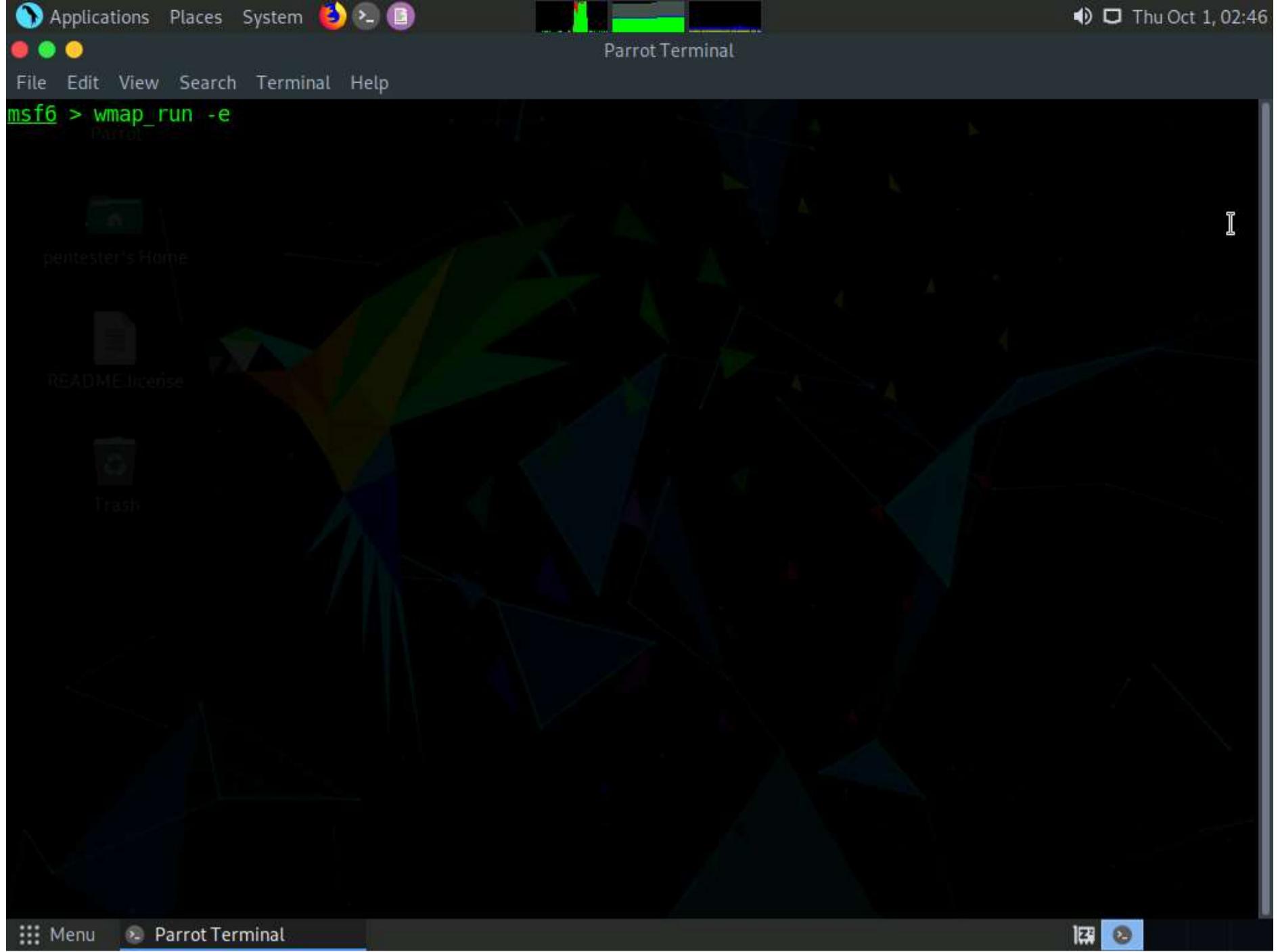
```
[*]
=[ General testing ]=
=====
[*] Done.
[*] Testing target:
[*]   Site: 172.19.19.7 (172.19.19.7)
[*]   Port: 80 SSL: false
=====
[*] Testing started. 2020-10-01 02:44:40 -0400
[*]
=[ SSL testing ]=
=====
[*] Target is not SSL. SSL modules disabled.
[*]
=[ Web Server testing ]=
=====
[*] Module auxiliary/scanner/http/http_version
[*] Module auxiliary/scanner/http/open_proxy
[*] Module auxiliary/admin/http/tomcat_administration
[*] Module auxiliary/admin/http/tomcat_utf8_traversal
[*] Module auxiliary/scanner/http/drupal_views_user_enum
[*] Module auxiliary/scanner/http/frontpage_login
[*] Module auxiliary/scanner/http/host_header_injection
[*] Module auxiliary/scanner/http/options
[*] Module auxiliary/scanner/http/robots_txt
[*] Module auxiliary/scanner/http/scraper
[*] Module auxiliary/scanner/http/svn_scanner
[*] Module auxiliary/scanner/http/trace
[*] Module auxiliary/scanner/http/vhost_scanner
[*] Module auxiliary/scanner/http/webdav_internal_ip
```

Menu Parrot Terminal

11. Once you have finished reading about the modules, it is now time to run the assessment, type **wmap_run -e** and press **Enter**. Once the scan has completed, you can review the results of the scan and take a few minutes to look for where the attack surface of the target is, and the vector you think you can use to attack these targets. You can press **Ctrl+C** to terminate the scan, as it will take lot off time to complete since there are a lot of modules.

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**.





The screenshot shows a Parrot OS desktop environment. A terminal window titled "Parrot Terminal" is open, displaying the output of a Metasploit scan. The terminal window has a dark background with green text. The terminal title bar includes the application menu, system status icons, and the date/time. The terminal window itself has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main area of the terminal shows the following Metasploit scan results:

```
[*] Module auxiliary/scanner/http/prev_dir_same_name_file
[*] Path: /
[-] Blank or default PATH set.
[*] Module auxiliary/scanner/http/replace_ext
[*] Module auxiliary/scanner/http/soap_xml
[*] Path: /
[*] Starting scan with 0ms delay between requests
[*] Server 172.19.19.7:80 returned HTTP 404 for /. Use a different one.
[*] Module auxiliary/scanner/http/trace_axd
[*] Path: /
[*] Module auxiliary/scanner/http/verb_auth_bypass
[*]
=[ Unique Query testing ]=
=====
[*] Module auxiliary/scanner/http/blind_sql_query
[*] Module auxiliary/scanner/http/error_sql_injection
[*] Module auxiliary/scanner/http/http_traversal
[*] Module auxiliary/scanner/http/rails_mass_assignment
[*] Module exploit/multi/http/lcms_php_exec
[*]
=[ Query testing ]=
=====
[*]
=[ General testing ]=
=====
+++++
Launch completed in 541.5694150924683 seconds.
+++++
[*] Done.
msf6 >
```

13. To look at the vulnerabilities that have been written to the database, type **wmap_vulns -l** and press **Enter**.

The screenshot shows a Parrot OS desktop environment. A terminal window titled "Parrot Terminal" is open, displaying the output of the command **wmap_vulns -l**. The terminal window has a dark background with green text. The terminal title bar includes the application menu, system status icons, and the date/time. The terminal window itself has a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". The main area of the terminal shows the following list of vulnerabilities:

```
msf6 > wmap_vulns -l
[*] + [172.19.19.7] (172.19.19.7): scraper /
    scraper Scraper
[*]     GET IIS7
[*] + [172.19.19.7] (172.19.19.7): directory /aspnet_client/
    directory Directory found.
[*]     GET Res code: 403
[*] + [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
[*] + [172.19.19.22] (172.19.19.22): directory /...
    directory Directory found.
[*]     GET Res code: 404
[*] + [172.19.19.22] (172.19.19.22): directory /WEB-INF./
    directory Directory found.
```

14. You can also display the vulnerabilities by typing **vulns** and press **Enter**.

File Edit View Search Terminal Help

msf6 > vulns

Parrot

Vulnerabilities

Timestamp	Host	Name	References
2020-10-01 06:52:46 UTC	172.19.19.7	HTTP Trace Method Allowed	CVE-2005-3398,CVE-2005-3498,OSVDB-877,BID-11604,BID-9506,BID-9561

msf6 >



Trash

Menu Parrot Terminal

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