

Lab 6: Perform Network Scanning using Various Scanning Tools

Lab Scenario

The information obtained in the previous steps might be insufficient to reveal potential vulnerabilities in the target network: there may be more information available that could help in finding loopholes in the target network. As an ethical hacker and pen tester, you should look for as much information as possible about systems in the target network using various network scanning tools when needed. This lab will demonstrate other techniques/commands/methods that can assist you in extracting information about the systems in the target network using various scanning tools.

Lab Objectives

- Scan a target network using Metasploit

Overview of Network Scanning Tools

Scanning tools are used to scan and identify live hosts, open ports, running services on a target network, location-info, NetBIOS info, and information about all TCP/IP and UDP open ports. Information obtained from these tools will assist an ethical hacker in creating the profile of the target organization and to scan the network for open ports of the devices connected.

Task 1: Scan a Target Network using Metasploit

Metasploit Framework is a tool that provides information about security vulnerabilities in the target organization's system, and aids in penetration testing and IDS signature development. It facilitates the tasks of attackers, exploit writers, and payload writers. A major advantage of the framework is the modular approach, that is, allowing the combination of any exploit with any payload.

Here, we will use Metasploit to discover active hosts, open ports, services running, and OS details of systems present in the target network.

1. ☐ Click [Parrot Security](#) to switch to the **Parrot Security** machine.
2. ☐ Click the **MATE Terminal** icon in the top of the **Desktop** window to open a **Terminal** window.



Parrot



CEHv11 Module 16
Hacking Wireless
Networks



attacker's Home



Security_Script.-
html



README.license



Trash



CEHv11 Module 13
Hacking Web
Servers



CEHv11 Module 14
Hacking Web
Applications



3. ☐ A **Parrot Terminal** window appears. In the terminal window, type **sudo su** and press **Enter** to run the programs as a root user.
4. ☐ In the **[sudo] password for attacker** field, type **toor** as a password and press **Enter**.

The password that you type will not be visible.

5. ☐ Now, type **cd** and press **Enter** to jump to the root directory.

File Edit View Search Terminal Help

```
[attacker@parrot]-[~] Module 16  
$sudo su  
[sudo] password for attacker:  
[root@parrot]-[/home/attacker]  
#cd  
[root@parrot]-[~]  
#
```

README_license

Trash

CEHv11 Module 13
Hacking Web
ServersCEHv11 Module 14
Hacking Web
Applications

6. ☐ In the **Parrot Terminal** window, type **service postgresql start** and hit **Enter**.

File Edit View Search Terminal Help

```
[attacker@parrot]-[~] Module 16  
$sudo su Hacking Wireless  
[sudo] password for attacker:  
[root@parrot]-[/home/attacker]  
#cd  
[root@parrot]-[~]  
#service postgresql start  
[root@parrot]-[~]  
#
```

README_license

Trash

CEHv11 Module 13
Hacking Web
ServersCEHv11 Module 14
Hacking Web
Applications

7. ☐ Now, type **msfconsole** and hit **Enter** to launch Metasploit.

File Edit View Search Terminal Help

```
[root@parrot]~# msfconsole
```

```
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
```

```
Trace program: running
```

```
wake up, Neo...
```

```
the matrix has you
```

```
follow the white rabbit.
```

```
knock, knock, Neo.
```

```
https://metasploit.com
```


8. ☐ An msf command line appears. Type **db_status** and hit **Enter** to check if Metasploit has connected to the database successfully. If you receive the message "**postgresql selected, no connection,**" then the database did not connect to msf.

File Edit View Search Terminal Help

knock, knock, Neo.

<https://metasploit.com>

```
CEHV11 Module 13
Her=[ metasploit v6.0.0-dev ]
+ -- --=[ 2052 exploits - 1108 auxiliary - 345 post ]
+ -- --=[ 566 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]
```

Metasploit tip: When in a module, use back to go back to the top level prompt

```
CEHV11 Module 14
msf6 > db status
[*] postgresql selected, no connection
msf6 >
```

9. ☐ Exit the Metasploit framework by typing **exit** and press **Enter**. Then, to initiate the database, type **msfdb init**, and press **Enter**.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:17
File Edit View Search Terminal Help

msf6 > db_status
[*] postgresql selected, no connection
msf6 > exit
[root@parrot]-[~]
#msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema
rake aborted!
TypeError: superclass mismatch for class Command
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/thor-1.0.1/lib/thor/command.rb:2:in `<class:Thor>'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/thor-1.0.1/lib/thor/command.rb:1:in `<top (required)>'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/thor-1.0.1/lib/thor/base.rb:1:in `require_relative'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/thor-1.0.1/lib/thor/base.rb:1:in `<top (required)>'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/thor-1.0.1/lib/thor/group.rb:1:in `require_relative'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/thor-1.0.1/lib/thor/group.rb:1:in `<top (required)>'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/railties-5.2.4.3/lib/rails/generators.rb:6:in `require'
/usr/share/metasploit-framework/vendor/bundle/ruby/2.7.0/gems/railties-5.2.4.3/lib/rails/generators.rb:6:in `<top (required)>'

Menu Parrot Terminal
```

10. ☐ To restart the postgresql service, type **service postgresql restart** and press **Enter**. Now, start the Metasploit Framework again by typing **msfconsole** and pressing **Enter**.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:20
File Edit View Search Terminal Help
(See full trace by running task with --trace)
[*]-[root@parrot]-[~] Wireless
#service postgresql restart
[root@parrot]-[~]
#msfconsole

attacker's Home
Security_Script
html 'cdk000ko:.'
.:ok000kdc'
.x0000000000000000c c000000000000000x.
:0000000000000000k, ,k0000000000000000:
'000000000k000000: :000000000000000000'
o00000000. ,o0000o0000l. ,00000000o
d00000000. ,c00000c. ,00000000x
l00000000. ;d; ,00000000l
.00000000. .; ; ,00000000.
c0000000. .00c. 'o00. ,0000000c
o000000. .0000. :0000. ,000000o
l00000. .0000. :0000. ,00000l
;0000' .0000. :0000. ;0000;
CEHv11,d00oe13 .0000o000x0000. x00d.
Hacking ,k0l .00000000000000. .d0k,
Servers :kk; .00000000000000. c0k:
;k0000000000000000k:
,x00000000000000x,
.l00000000l.
,d0d,
CEHv11Module14
Hacking Web
App=[ metasploit v6.0.0-dev ]
+ -- --=[ 2052 exploits - 1108 auxiliary - 345 post ]
```

11. ☐ Check the database status by typing **db_status** and press **Enter**. This time, the database should successfully connect to msf, as shown in the screenshot.


```
Applications Places System Parrot Terminal Thu Aug 20, 03:20
File Edit View Search Terminal Help

..x000000000000cEHv11 Module 13c000000000000x.
:0000000000000000k,kong,k0000000000000000:
'000000000k000000:le:00000000000000000000'
o00000000. .o0000o0000l. ,000000000o
d00000000. .c000000c. ,000000000x
l00000000. ;d; ,000000000l
.00000000. .; Security_Scri; ,00000000.
c0000000. .00c. .htm'o00. ,00000000c
o0000000. .0000. :0000. ,0000000o
l00000. .0000. :0000. ,00000l
;0000rise .0000. :0000. ;0000;
.d00o .0000occcx0000. x00d,
,k0l .00000000000000. .d0k,
:kk;.00000000000000.c0k:
;k0000000000000000k:
,x000000000000x,
,l00000000l.
,d0d,

CEHv11 Module 13
Her=[ metasploit v6.0.0-dev ]
+ -- --=[ 2052 exploits - 1108 auxiliary - 345 post ]
+ -- --=[ 566 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: Adapter names can be used for IP params set LHOST eth0

CEHv11 Module 14
msf6 > db status
[*] Connected to msf. Connection type: postgresql.
msf6 >
```

12. ☐ Type **nmap -Pn -sS -A -oX Test 10.10.10.0/24** and hit **Enter** to scan the subnet, as shown in the screenshot.

Here, we are scanning the whole subnet 10.10.10.0/24 for active hosts.

13. ☐ Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:27
File Edit View Search Terminal Help
msf6 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > nmap -Pn -sS -A -oX Test 10.10.10.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.10.10.0/24

Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-20 03:21 EDT
Nmap scan report for 10.10.10.1
Host is up (0.00077s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.5 (protocol 2.0)
| ssh-hostkey:
|_ 4096 d9:85:76:71:65:6a:89:8d:ea:cc:86:f8:5e:f0:92:8b (RSA)
53/tcp    open  domain   (generic dns response: NOTIMP)
| fingerprint-strings:
|_ DNSVersionBindReqTCP:
|   version
|   bind
88/tcp    open  http     nginx
|_ http-title: pfSense - Login
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=8/20%Time=5F3E249B%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x85\0\x01\0\0\0\0\0\0\0\0\0\07version\
SF:x04bind\0\0\x10\0\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\0\x90\x04\0\0
SF:\0\0\0\0\0\0");
MAC Address: 00:15:5D:27:08:B0 (Microsoft)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
```

14. ☐ After the scan completes, Nmap displays the number of active hosts in the target network (here, **7**).
15. ☐ Now, type **db_import Test** and hit **Enter** to import the Nmap results from the database.

TRACEROUTE

HOP	RTT	ADDRESS
1	0.74 ms	www.goodshopping.com (10.10.10.19)

Nmap scan report for 10.10.10.13

Host is up (0.000037s latency).

All 1000 scanned ports on 10.10.10.13 are closed

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

Post-scan script results:

| clock-skew:

| 48m00s:

| 10.10.10.10

| 10.10.10.19 (www.goodshopping.com)

| 10.10.10.16

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 256 IP addresses (7 hosts up) scanned in 267.93 seconds

msf6 > db import Test

[*] Importing 'Nmap XML' data

[*] Import: Parsing with 'Nokogiri v1.10.10'

[*] Importing host 10.10.10.1

[*] Importing host 10.10.10.9

[*] Importing host 10.10.10.10

[*] Importing host 10.10.10.14

[*] Importing host 10.10.10.16

[*] Importing host 10.10.10.19

[*] Importing host 10.10.10.13

[*] Successfully imported /root/Test

msf6 >

16. ☐ Type **hosts** and hit **Enter** to view the list of active hosts along with their MAC addresses, OS names, etc. as shown in the screenshot.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:29
File Edit View Search Terminal Help
| clock-skew:
| 48m00s:
| 10.10.10.10
| 10.10.10.19 (www.goodshopping.com)
| 10.10.10.16
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 267.93 seconds
msf6 > db import Test
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.10.10'
[*] Importing host 10.10.10.1
[*] Importing host 10.10.10.9
[*] Importing host 10.10.10.10
[*] Importing host 10.10.10.14
[*] Importing host 10.10.10.16
[*] Importing host 10.10.10.19
[*] Importing host 10.10.10.13
[*] Successfully imported /root/Test
msf6 > hosts

Hosts
=====

address mac name os_name os_flavor os_sp purpose info comment
-----
10.10.10.1 00:15:5d:27:08:b0 Unknown
10.10.10.9 00:15:5d:27:08:b6 Linux 2.6.X server
10.10.10.10 00:15:5d:27:08:b2 Windows Longhorn device
10.10.10.13 Unknown device
10.10.10.14 00:15:5d:27:08:b7 Linux 3.X server
10.10.10.16 00:15:5d:27:08:b4 Windows 2016 server
10.10.10.19 00:15:5d:27:08:b3 www.goodshopping.com Windows Longhorn device

msf6 >
```


17. ☐ Type **services** or **db_services** and hit **Enter** to receive a list of the services running on the active hosts, as shown in the screenshot.

In addition to running Nmap, there are a variety of other port scanners that are available within the Metasploit framework to scan the target systems.

Applications Places System Thu Aug 20, 03:30

Parrot Terminal

File Edit View Search Terminal Help

10.10.10.19 00:15:5d:27:08:b3 www.goodshopping.com Windows Longhorn device


msf6 > services

Services

=====

host	port	proto	name	state	info
10.10.10.1	22	tcp	ssh	open	OpenSSH 7.5 protocol 2.0
10.10.10.1	53	tcp	domain	open	generic dns response: NOTIMP
10.10.10.1	88	tcp	http	open	nginx
10.10.10.9	80	tcp	http	open	Apache httpd 2.4.38 (Ubuntu)
10.10.10.10	21	tcp	ftp	open	Microsoft ftpd
10.10.10.10	80	tcp	http	open	Microsoft IIS httpd 10.0
10.10.10.10	135	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.10	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
10.10.10.10	445	tcp	microsoft-ds	open	Windows 10 Enterprise 18362 microsoft-ds workgroup: WORKGROUP
10.10.10.10	1042	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.10	3389	tcp	ms-wbt-server	open	Microsoft Terminal Services
10.10.10.14	5555	tcp	freeciv	open	
10.10.10.16	53	tcp	domain	open	
10.10.10.16	80	tcp	http	open	Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
10.10.10.16	88	tcp	kerberos-sec	open	Microsoft Windows Kerberos server time: 2020-08-20 07:21:58Z
10.10.10.16	135	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.16	139	tcp	netbios-ssn	open	Microsoft Windows netbios-ssn
10.10.10.16	389	tcp	ldap	open	Microsoft Windows Active Directory LDAP Domain: CEH.com, Site: D
10.10.10.16	445	tcp	microsoft-ds	open	Windows Server 2016 Standard 14393 microsoft-ds workgroup: CEH
10.10.10.16	464	tcp	kpasswd5	open	
10.10.10.16	593	tcp	ncacn_http	open	Microsoft Windows RPC over HTTP 1.0
10.10.10.16	636	tcp	tcpwrapped	open	
10.10.10.16	1060	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.16	1801	tcp	msmq	open	
10.10.10.16	2103	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.16	2105	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.16	2107	tcp	msrpc	open	Microsoft Windows RPC
10.10.10.16	3268	tcp	ldap	open	Microsoft Windows Active Directory LDAP Domain: CEH.com, Site: D

Menu Parrot Terminal

18.  Type **search portscan** and hit **Enter**. The Metasploit port scanning modules appear, as shown in the screenshot.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:30
File Edit View Search Terminal Help
default-First-Site-Name
10.10.10.16 3269 tcp tcpwrapped open
10.10.10.16 3389 tcp ms-wbt-server open Microsoft Terminal Services
10.10.10.16 8080 tcp http open Apache httpd 2.4.39 (Win64) PHP/7.2.18
10.10.10.19 80 tcp http open Microsoft IIS httpd 10.0
10.10.10.19 135 tcp msrpc open Microsoft Windows RPC
10.10.10.19 139 tcp netbios-ssn open Microsoft Windows netbios-ssn
10.10.10.19 445 tcp microsoft-ds open
10.10.10.19 1801 tcp msmq open
10.10.10.19 2103 tcp msrpc open Microsoft Windows RPC
10.10.10.19 2105 tcp msrpc open Microsoft Windows RPC
10.10.10.19 2107 tcp msrpc open Microsoft Windows RPC
10.10.10.19 3389 tcp ms-wbt-server open Microsoft Terminal Services

msf6 > search portscan

Matching Modules
=====
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pingback Locat
or
1 auxiliary/scanner/natpmp/natpmp_portscan normal No NAT-PMP External Port Sc
anner
2 auxiliary/scanner/portscan/ack normal No TCP ACK Firewall Scanner
3 auxiliary/scanner/portscan/ftpbounce normal No FTP Bounce Port Scanner
4 auxiliary/scanner/portscan/syn normal No TCP SYN Port Scanner
5 auxiliary/scanner/portscan/tcp normal No TCP Port Scanner
6 auxiliary/scanner/portscan/xmas normal No TCP "XMas" Port Scanner
7 auxiliary/scanner/sap/sap_router_portscanner normal No SAPRouter Port Scanner

Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner
msf6 > 
```

19. ☐ Here, we will use the **auxiliary/scanner/portscan/syn** module to perform an SYN scan on the target systems. To do so, type **use auxiliary/scanner/portscan/syn** and press **Enter**.
20. ☐ We will use this module to perform an SYN scan against the target IP address range (**10.10.10.5-20**) to look for open port 80 through the eth0 interface.

To do so, issue the below commands:

- **set INTERFACE eth0**
- **set PORTS 80**
- **set RHOSTS 10.10.10.5-20**
- **set THREADS 50**

PORTS: specifies the ports to scan (e.g., 22-25, 80, 110-900), **RHOSTS:** specifies the target address range or CIDR identifier, and **THREADS:** specifies the number of concurrent threads (default 1).


```
Applications Places System Parrot Terminal Thu Aug 20, 03:32
File Edit View Search Terminal Help
10.10.10.19 2103 tcp msrpc open Microsoft Windows RPC
10.10.10.19 2105 tcp msrpc open Microsoft Windows RPC
10.10.10.19 2107 tcp msrpc open Microsoft Windows RPC
10.10.10.19 3389 tcp ms-wbt-server open Microsoft Terminal Services

msf6 > search portscan

Matching Modules
=====

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pingback Locat
or
1 auxiliary/scanner/natpmp/natpmp_portscan normal No NAT-PMP External Port Sc
anner
2 auxiliary/scanner/portscan/ack normal No TCP ACK Firewall Scanner
3 auxiliary/scanner/portscan/ftpbounce normal No FTP Bounce Port Scanner
4 auxiliary/scanner/portscan/syn normal No TCP SYN Port Scanner
5 auxiliary/scanner/portscan/tcp normal No TCP Port Scanner
6 auxiliary/scanner/portscan/xmas normal No TCP "XMas" Port Scanner
7 auxiliary/scanner/sap/sap_router_portscanner normal No SAPRouter Port Scanner

Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner

msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(scanner/portscan/syn) > set PORTS 80
PORTS => 80
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf6 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/portscan/syn) >
```

21. ☐ After specifying the above values, type **run**, and press **Enter** to initiate the scan against the target IP address range.

Similarly, you can also specify a range of ports to be scanned against the target IP address range.

22. ☐ The result appears, displaying open port 80 in active hosts, as shown in the screenshot.

File Edit View Search Terminal Help

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/http/wordpress_pingback_access		normal	No	Wordpress Pingback Locat
1	auxiliary/scanner/natpmp/natpmp_portscan		normal	No	NAT-PMP External Port Sc
2	auxiliary/scanner/portscan/ack		normal	No	TCP ACK Firewall Scanner
3	auxiliary/scanner/portscan/ftpbounce		normal	No	FTP Bounce Port Scanner
4	auxiliary/scanner/portscan/syn		normal	No	TCP SYN Port Scanner
5	auxiliary/scanner/portscan/tcp		normal	No	TCP Port Scanner
6	auxiliary/scanner/portscan/xmas		normal	No	TCP "XMas" Port Scanner
7	auxiliary/scanner/sap/sap_router_portscanner		normal	No	SAPRouter Port Scanner

Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner

```
msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(scanner/portscan/syn) > set PORTS 80
PORTS => 80
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf6 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/portscan/syn) > run
```

```
[+] TCP OPEN 10.10.10.9:80
[+] TCP OPEN 10.10.10.10:80
[+] TCP OPEN 10.10.10.19:80
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) >
```

- 23. ☐ Now, we will perform a TCP scan for open ports on the target systems.
- 24. ☐ To load the **auxiliary/scanner/portscan/tcp** module, type **use auxiliary/scanner/portscan/tcp** and press **Enter**.
- 25. ☐ Type **hosts -R** and press **Enter** to automatically set this option with the discovered hosts present in our database.

OR

Type **set RHOSTS [Target IP Address]** and press **Enter**.

Here, we will perform a TCP scan for open ports on a single IP address (**10.10.10.16**), as scanning multiple IP addresses consumes much time.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:38
File Edit View Search Terminal Help

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pingback Locat
or
1 auxiliary/scanner/natpmp/natpmp_portscanner normal No NAT-PMP External Port Sc
anner
2 auxiliary/scanner/portscan/ack normal No TCP ACK Firewall Scanner
3 auxiliary/scanner/portscan/ftpbounce normal No FTP Bounce Port Scanner
4 auxiliary/scanner/portscan/syn normal No TCP SYN Port Scanner
5 auxiliary/scanner/portscan/tcp normal No TCP Port Scanner
6 auxiliary/scanner/portscan/xmas normal No TCP "XMas" Port Scanner
7 auxiliary/scanner/sap/sap_router_portscanner normal No SAPRouter Port Scanner

Interact with a module by name or index, for example use 7 or use auxiliary/scanner/sap/sap_router_portscanner

msf6 > use auxiliary/scanner/portscan/syn
msf6 auxiliary(scanner/portscan/syn) > set INTERFACE eth0
INTERFACE => eth0
msf6 auxiliary(scanner/portscan/syn) > set PORTS 80
PORTS => 80
msf6 auxiliary(scanner/portscan/syn) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf6 auxiliary(scanner/portscan/syn) > set THREADS 50
THREADS => 50
msf6 auxiliary(scanner/portscan/syn) > run

[+] TCP OPEN 10.10.10.9:80
[+] TCP OPEN 10.10.10.10:80
[+] TCP OPEN 10.10.10.19:80
[*] Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/syn) > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 10.10.10.16
RHOSTS => 10.10.10.16
msf6 auxiliary(scanner/portscan/tcp) >
```

26. ☐ Type **run** and press **Enter** to discover open TCP ports in the target system.
27. ☐ The results appear, displaying all open TCP ports in the target IP address (10.10.10.16).


```
Applications Places System Parrot Terminal Thu Aug 20, 03:39
File Edit View Search Terminal Help
msf6 auxiliary(scanner/portscan/tcp) > run

[+] 10.10.10.16: - 10.10.10.16:53 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:80 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:88 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:139 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:135 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:389 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:445 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:464 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:593 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:636 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1060 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1537 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1538 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1539 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1536 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1549 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1546 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1547 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1545 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1552 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1559 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1574 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1801 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:2103 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:2105 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:2107 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:3269 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:3268 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:3389 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:5985 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:8080 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:9389 - TCP OPEN
[*] 10.10.10.16: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

28. ☐ Now that we have determined the active hosts on the target network, we can further attempt to determine the OSes running on the target systems. As there are systems in our scan that have port 445 open, we will use the module `scanner/smb/version` to determine which version of Windows is running on a target and which Samba version is on a Linux host.
29. ☐ To do so, first type **back**, and then press **Enter** to revert to the msf command line. Then, type **use auxiliary/scanner/smb/smb_version** and press **Enter**.
30. ☐ We will use this module to run a SMB version scan against the target IP address range (**10.10.10.5-20**). To do so, issue the below commands:
- **set RHOSTS 10.10.10.5-20**
 - **set THREADS 11**

Applications Places System Parrot Terminal Thu Aug 20, 03:41

File Edit View Search Terminal Help

```
[+] 10.10.10.16: - 10.10.10.16:389 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:445 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:464 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:593 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:636 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1060 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1537 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1538 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1539 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1536 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1549 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1546 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1547 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1545 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1552 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1559 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1574 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:1801 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:2103 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:2105 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:2107 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:3269 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:3268 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:3389 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:5985 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:8080 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:9389 - TCP OPEN
[*] 10.10.10.16: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > back
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf6 auxiliary(scanner/smb/smb_version) >
```

Menu Parrot Terminal

31. ☐ Type **run** and press **Enter** to discover SMB version in the target systems.
32. ☐ The result appears, displaying the OS details of the target hosts.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:41
File Edit View Search Terminal Help
[+] 10.10.10.16: - 10.10.10.16:3268 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:3389 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:5985 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:8080 - TCP OPEN
[+] 10.10.10.16: - 10.10.10.16:9389 - TCP OPEN
[*] 10.10.10.16: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > back
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.10.10.10:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{a81bec98-5621-4809-8cea-481c7337c67e}) (authentication domain:WINDOWS10)
[+] 10.10.10.10:445 - Host is running Windows 10 Enterprise (build:18362) (name:WINDOWS10) (workgroup:WORKGROUP)
[*] 10.10.10.5-20: - Scanned 5 of 16 hosts (31% complete)
[*] 10.10.10.5-20: - Scanned 10 of 16 hosts (62% complete)
[*] 10.10.10.5-20: - Scanned 11 of 16 hosts (68% complete)
[*] 10.10.10.19:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{df489eac-cf3b-43f0-b4f9-83191f18ca4d}) (authentication domain:SERVER2019)
[*] 10.10.10.16:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:required) (uptime:2h 40m 56s) (guid:{07cfc4d4-f7b3-4ef3-a600-2bfdd850cc93}) (authentication domain:CEH)
[+] 10.10.10.16:445 - Host is running Windows 2016 Standard (build:14393) (name:SERVER2016) (domain:CEH)
[*] 10.10.10.5-20: - Scanned 13 of 16 hosts (81% complete)
[*] 10.10.10.5-20: - Scanned 14 of 16 hosts (87% complete)
[*] 10.10.10.5-20: - Scanned 15 of 16 hosts (93% complete)
[*] 10.10.10.5-20: - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

33. ☐ While performing a scan using Nmap, we discovered that the FTP port 21 is open on the host 10.10.10.10 in the target network. Now, we will scan the target host to identify the FTP version.
34. ☐ Type **back** and press **Enter**. To load an FTP module, type **use auxiliary/scanner/ftp/ftp_version** and press **Enter**.
35. ☐ Type **set RHOSTS 10.10.10.10** and press **Enter** to specify the target host.


```
Applications Places System Parrot Terminal Thu Aug 20, 03:42
File Edit View Search Terminal Help
[+] 10.10.10.16: - 10.10.10.16:9389 - TCP OPEN
[*] 10.10.10.16: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) > back
msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf6 auxiliary(scanner/smb/smb_version) > run


[*] 10.10.10.10:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{a81bec98-5621-4809-8cea-481c7337c67e}) (authentication domain:WINDOWS10)
[+] 10.10.10.10:445 - Host is running Windows 10 Enterprise (build:18362) (name:WINDOWS10) (workgroup:WORKGROUP)
[*] 10.10.10.5-20: - Scanned 5 of 16 hosts (31% complete)
[*] 10.10.10.5-20: - Scanned 10 of 16 hosts (62% complete)
[*] 10.10.10.5-20: - Scanned 11 of 16 hosts (68% complete)
[*] 10.10.10.19:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{df489eac-cf3b-43f0-b4f9-83191f18ca4d}) (authentication domain:SERVER2019)
[*] 10.10.10.16:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:required) (uptime:2h 40m 56s) (guid:{07cfc4d4-f7b3-4ef3-a600-2bfdd850cc93}) (authentication domain:CEH)
[+] 10.10.10.16:445 - Host is running Windows 2016 Standard (build:14393) (name:SERVER2016) (domain:CEH)
[*] 10.10.10.5-20: - Scanned 13 of 16 hosts (81% complete)
[*] 10.10.10.5-20: - Scanned 14 of 16 hosts (87% complete)
[*] 10.10.10.5-20: - Scanned 15 of 16 hosts (93% complete)
[*] 10.10.10.5-20: - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > use auxiliary/scanner/ftp/ftp_version
msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.10.10.10
RHOSTS => 10.10.10.10
msf6 auxiliary(scanner/ftp/ftp_version) >
```

36. ☐ Type **run** and press **Enter** to initiate the FTP version identification scan.
37. ☐ The result appears, displaying the FTP version details of the target host, as shown in the screenshot.


```
Applications Places System Parrot Terminal Thu Aug 20, 03:42
File Edit View Search Terminal Help
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.10.10.5-20
RHOSTS => 10.10.10.5-20
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 11
THREADS => 11
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 10.10.10.10:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{a81bec98-5621-4809-8cea-481c7337c67e}) (authentication domain:WINDOWS10)
[+] 10.10.10.10:445 - Host is running Windows 10 Enterprise (build:18362) (name:WINDOWS10) (workgroup:WORKGROUP)
[*] 10.10.10.5-20: - Scanned 5 of 16 hosts (31% complete)
[*] 10.10.10.5-20: - Scanned 10 of 16 hosts (62% complete)
[*] 10.10.10.5-20: - Scanned 11 of 16 hosts (68% complete)
[*] 10.10.10.19:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:optional) (guid:{df489eac-cf3b-43f0-b4f9-83191f18ca4d}) (authentication domain:SERVER2019)
[*] 10.10.10.16:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:required) (uptime:2h 40m 56s) (guid:{07cfc4d4-f7b3-4ef3-a600-2bfdd850cc93}) (authentication domain:CEH)
[+] 10.10.10.16:445 - Host is running Windows 2016 Standard (build:14393) (name:SERVER2016) (domain:CEH)
[*] 10.10.10.5-20: - Scanned 13 of 16 hosts (81% complete)
[*] 10.10.10.5-20: - Scanned 14 of 16 hosts (87% complete)
[*] 10.10.10.5-20: - Scanned 15 of 16 hosts (93% complete)
[*] 10.10.10.5-20: - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > use auxiliary/scanner/ftp/ftp_version
msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.10.10.10
RHOSTS => 10.10.10.10
msf6 auxiliary(scanner/ftp/ftp_version) > run

[+] 10.10.10.10:21 - FTP Banner: '220 Microsoft FTP Service\x0d\x0a'
[*] 10.10.10.10:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_version) >
```


38.  Type **hosts** and press **Enter** to view detailed information on active hosts in the target network.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:42
File Edit View Search Terminal Help
[*] 10.10.10.16:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:required) (uptime:2h 40m 56s) (guid:{07cfc4d4-f7b3-4ef3-a600-2bfdd850cc93}) (authentication domain:CEH)
[+] 10.10.10.16:445 - Host is running Windows 2016 Standard (build:14393) (name:SERVER2016) (domain:CEH)
[*] 10.10.10.5-20: - Scanned 13 of 16 hosts (81% complete)
[*] 10.10.10.5-20: - Scanned 14 of 16 hosts (87% complete)
[*] 10.10.10.5-20: - Scanned 15 of 16 hosts (93% complete)
[*] 10.10.10.5-20: - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > use auxiliary/scanner/ftp/ftp_version
msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.10.10.10
RHOSTS => 10.10.10.10
msf6 auxiliary(scanner/ftp/ftp_version) > run

[+] 10.10.10.10:21 - FTP Banner: '220 Microsoft FTP Service\x0d\x0a'
[*] 10.10.10.10:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_version) > hosts

Hosts
=====
address  name  os_name  os_flavor  os_sp  purpose  info  comment
-----
10.10.10.1  00:15:5d:27:08:b0  Unknown
10.10.10.9  00:15:5d:27:08:b6  Linux
10.10.10.10  00:15:5d:27:08:b2  WINDOWS10  Windows 10  Enterprise  client
10.10.10.13  00:15:5d:27:08:b7  Unknown
10.10.10.14  00:15:5d:27:08:b7  Linux
10.10.10.16  00:15:5d:27:08:b4  SERVER2016  Windows 2016  Standard  server
10.10.10.19  00:15:5d:27:08:b3  www.goodshopping.com  Windows Longhorn  device

msf6 auxiliary(scanner/ftp/ftp_version) >
```

39. ☐ You can further export this information to a CSV file. To do so, first type **back**, and then press **Enter**. Now, type **hosts -o /root/Desktop/Metasploit_Scan_Results.csv** and press **Enter**.

```
Applications Places System Parrot Terminal Thu Aug 20, 03:52
File Edit View Search Terminal Help
ies:LZNT1) (encryption capabilities:AES-128-CCM) (signatures:required) (uptime:2h 50m 13s) (guid:{07cfc4d4-f7b3-4ef3-a600-2bfdd850cc93}) (authentication domain:CEH)
[+] 10.10.10.16:445 - Host is running Windows 2016 Standard (build:14393) (name:SERVER2016) (domain:CEH)
[*] 10.10.10.5-20: - Scanned 13 of 16 hosts (81% complete)
[*] 10.10.10.5-20: - Scanned 16 of 16 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > back
msf6 > use auxiliary/scanner/ftp/ftp_version
msf6 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.10.10.10
RHOSTS => 10.10.10.10
msf6 auxiliary(scanner/ftp/ftp_version) > run

[+] 10.10.10.10:21 - FTP Banner: '220 Microsoft FTP Service\x0d\x0a'
[*] 10.10.10.10:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/ftp_version) > hosts

Hosts
=====
address mac name os_name os_flavor os_sp purpose info comment
-----
10.10.10.1 00:15:5d:27:08:b0 Unknown
10.10.10.9 00:15:5d:27:08:b6 Linux 2.6.X server
10.10.10.10 00:15:5d:27:08:b2 WINDOWS10 Windows 10 Enterprise client
10.10.10.13 Unknown device
10.10.10.14 00:15:5d:27:08:b7 Linux 3.X server
10.10.10.16 00:15:5d:27:08:b4 SERVER2016 Windows 2016 Standard server
10.10.10.19 00:15:5d:27:08:b3 www.goodshopping.com Windows Longhorn device

msf6 auxiliary(scanner/ftp/ftp_version) > back
msf6 > hosts -o /root/Desktop/Metasploit Scan Results.csv
[*] Wrote hosts to /root/Desktop/Metasploit_Scan_Results.csv
msf6 >
```

40. ☐ Click **Places** from the top-section of **Desktop** and click **Home Folder** from the drop-down options.

Applications Places System Thu Aug 20, 03:54

File Edit View

Home Folder Desktop Documents Music Pictures Videos Downloads Parrot Floppy Disk Network Connect to Server... MATE Search Tool Recent Documents

Parrot Terminal

```
S-128-CCM) (signatures:required) (uptime:2h 50m 13s) (guid:{07cfc4d4-f7b3-
on domain:CEH)
running Windows 2016 Standard (build:14393) (name:SERVER2016) (domain:CEH)
of 16 hosts (81% complete)
of 16 hosts (100% complete)
ed
) > back
version
) > set RHOSTS 10.10.10.10
) > run

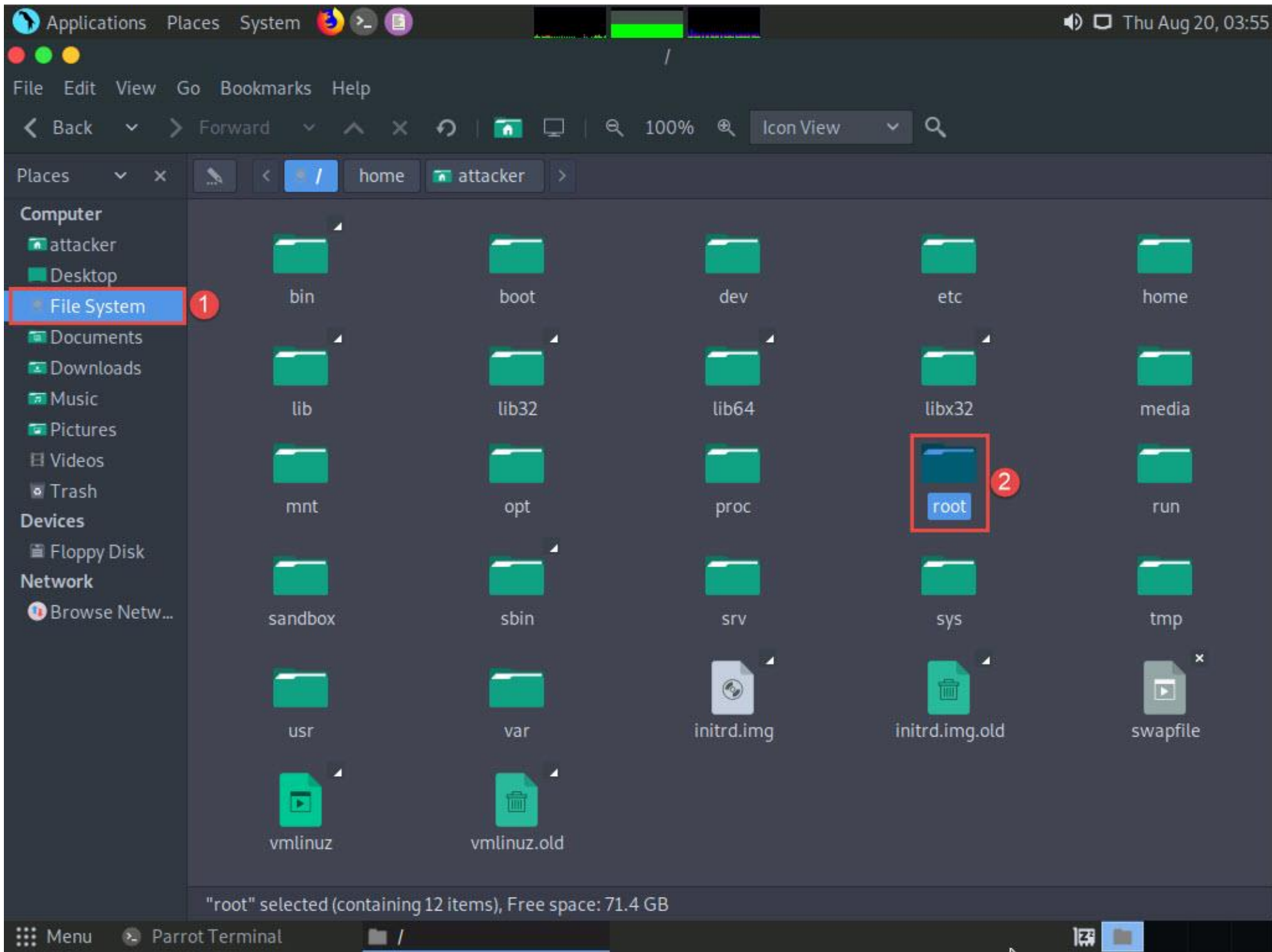
: '220 Microsoft FTP Service\x0d\x0a'
of 1 hosts (100% complete)
ed
) > hosts
```


address	mac	name	os_name	os_flavor	os_sp	purpose	info	comment
10.10.10.1	00:15:5d:27:08:b0		Unknown			device		
10.10.10.9	00:15:5d:27:08:b6		Linux		2.6.X	server		
10.10.10.10	00:15:5d:27:08:b2	WINDOWS10	Windows 10	Enterprise		client		
10.10.10.13			Unknown			device		
10.10.10.14	00:15:5d:27:08:b7		Linux		3.X	server		
10.10.10.16	00:15:5d:27:08:b4	SERVER2016	Windows 2016	Standard		server		
10.10.10.19	00:15:5d:27:08:b3	www.goodshopping.com	Windows Longhorn			device		

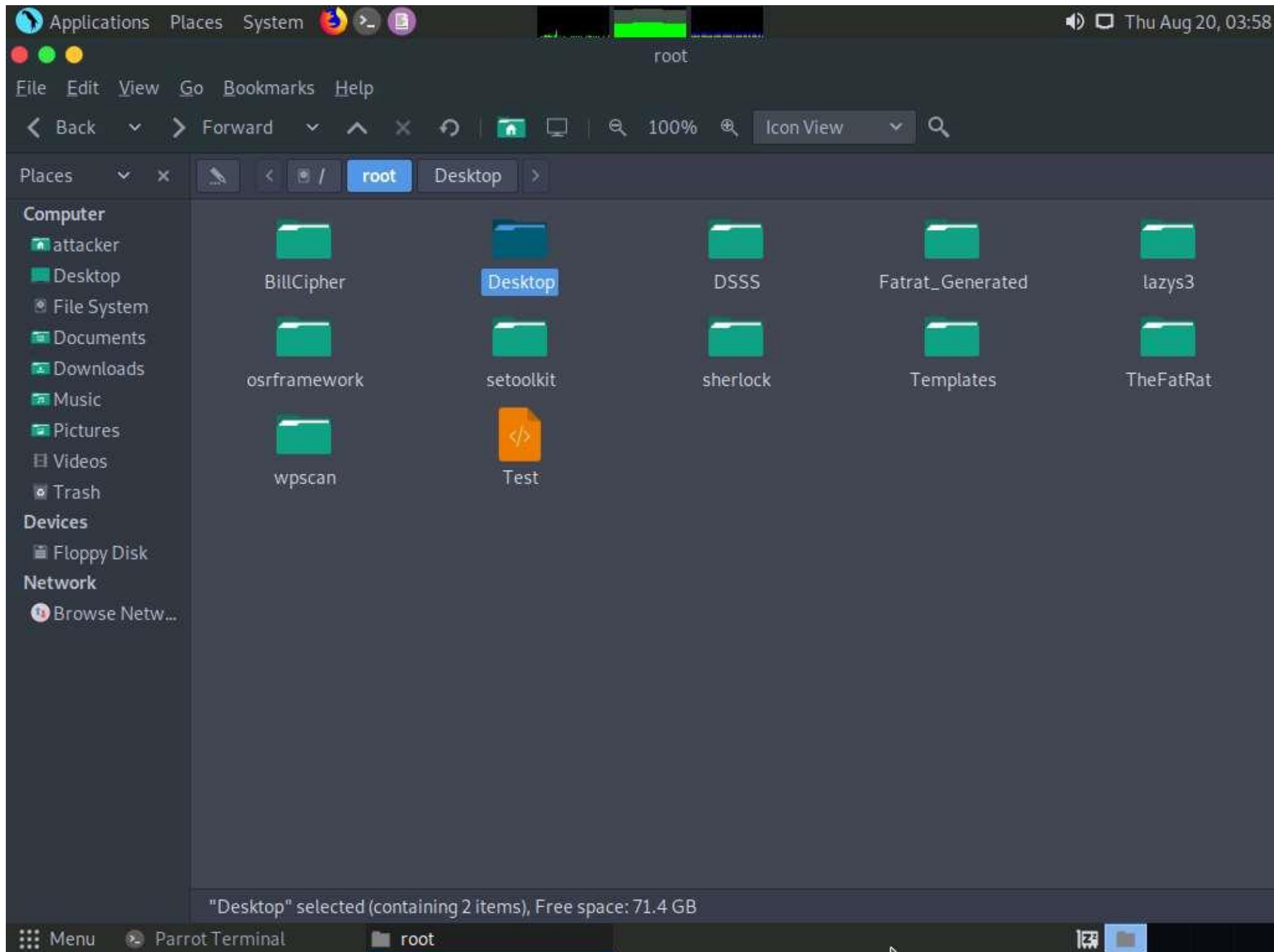
```
msf6 auxiliary(scanner/ftp/ftp version) > back
msf6 > hosts -o /root/Desktop/Metasploit Scan Results.csv
[*] Wrote hosts to /root/Desktop/Metasploit_Scan_Results.csv
msf6 >
```

Menu Parrot Terminal

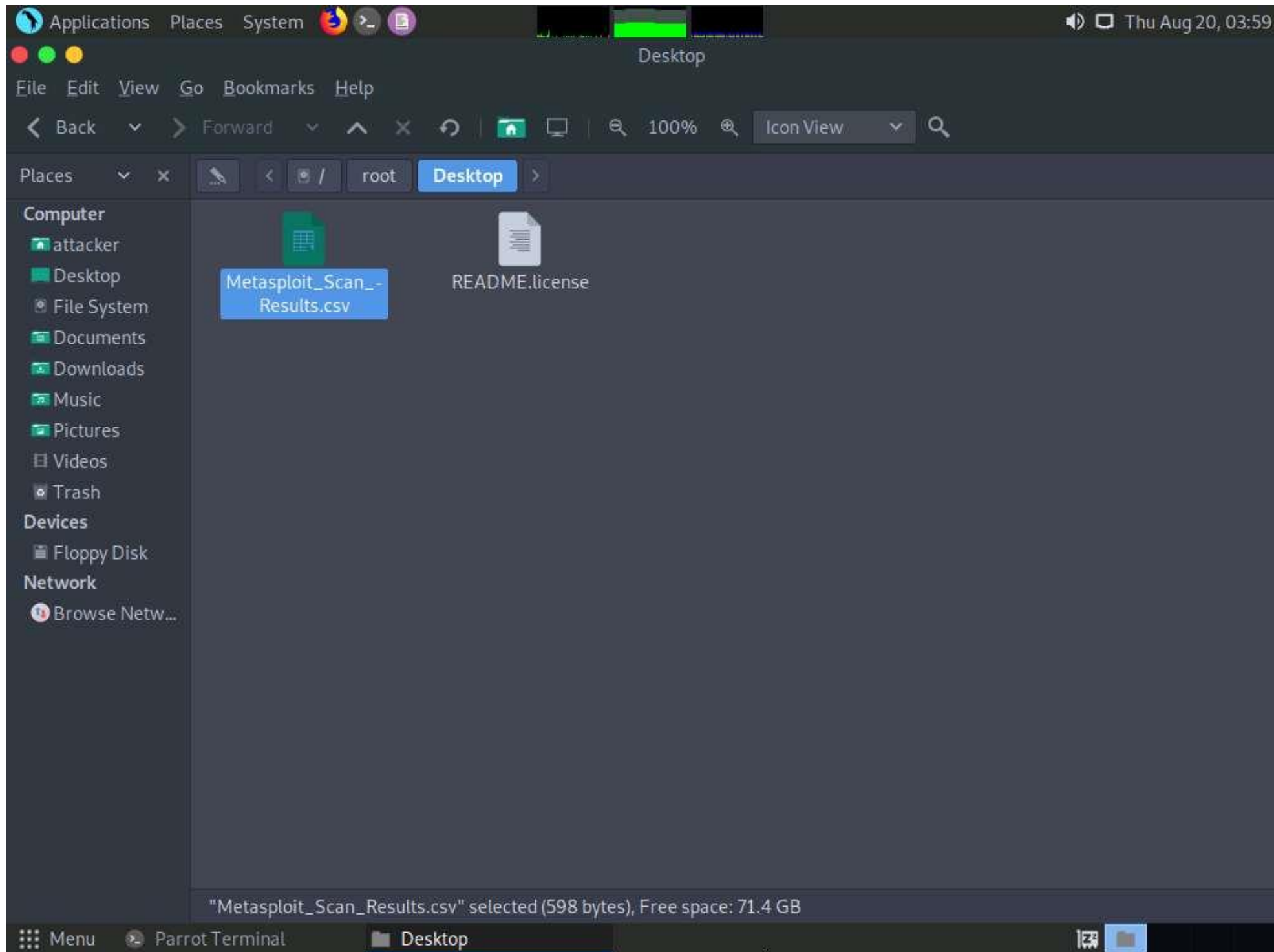
41.  The **attacker** window appears, click **File System** and double-click **root** folder.



42.  The **root** window appears, double-click **Desktop** folder.



43. ☐ You can observe **Metasploit_Scan_Results.csv** file. This CSV file, contains detailed information on the active hosts in the target IP range.ss



- 44. ☐ This information can further be used to perform vulnerability analysis on the open services discovered in the target hosts.
- 45. ☐ This concludes the demonstration of gathering information on open ports, a list of services running on active hosts, and information related to OSes, amongst others.
- 46. ☐ Close all open windows and document all the acquired information.