

Lab 5: 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. Open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).

The password that you type will not be visible.

2. Execute command **msfconsole** to launch Metasploit.

```
[attacker@parrot]~  
$sudo su  
[sudo] password for attacker:  
[root@parrot]~/home/attacker  
#msfconsole  
This copy of metasploit-framework is more than two weeks old.  
Consider running 'msfupdate' to update to the latest version.  
Metasploit tip: View advanced module options with advanced  
README/license  
-----  
3Kom SuperHack II Logon  
-----  
User Name: [ security ]  
Password: [ ]  
[ OK ]  
-----
```

3. An msf command line appears. Type **nmap -Pn -sS -A -oX Test 10.10.1.0/24** and press **Enter** to scan the subnet, as shown in the screenshot.

Here, we are scanning the whole subnet 10.10.1.0/24 for active hosts.

4. Nmap begins scanning the subnet and displays the results. It takes approximately 5 minutes for the scan to complete.
5. After the scan completes, Nmap displays the host information in the target network along with open ports, service and OS enumeration.

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
+ -- ==[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/

[msf](Jobs:0 Agents:0) >> nmap -Pn -sS -A -oX Test 10.10.1.0/24
[*] exec: nmap -Pn -sS -A -oX Test 10.10.1.0/24

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 03:40 EDT
Nmap scan report for 10.10.1.2
Host is up (0.00047s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain Unbound
88/tcp    open  http  nginx
|_http-title: pfSense - Login
MAC Address: 02:15:5D:43:08:58 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (91%)
OS CPE: cpe:/o:freebsd:freebsd:11.2
Aggressive OS guesses: FreeBSD 11.2-RELEASE (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

CEHv13 Module 14
Web
TRACEROUTE
HOP RTT ADDRESS
```

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help

Nmap scan report for 10.10.1.9
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3b:23:12:8c:e2:d5:91:d3:e5:5a:93:82:11:b9:fb:f6 (ECDSA)
|_  256 ae:80:12:14:aa:cb:96:ea:ec:cb:5a:e1:3a:33:76:f4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
MAC Address: 02:15:5D:43:08:5C (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.34 ms 10.10.1.9

Nmap scan report for 10.10.1.11
Host is up (0.00034s latency).
```

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.11
Host is up (0.00034s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http           Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_ http-title: IIS Windows
|_ http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Windows 10 Enterprise 22000 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server?
|_ ssl-date: 2024-05-28T07:42:06+00:00; 0s from scanner time.
| rdp-ntlm-info:
| Target_Name: WINDOWS11
| NetBIOS_Domain_Name: WINDOWS11
| NetBIOS_Computer_Name: WINDOWS11
| DNS_Domain_Name: Windows11
| DNS_Computer_Name: Windows11
| Product_Version: 10.0.22000
|_ System_Time: 2024-05-28T07:41:57+00:00
| ssl-cert: Subject: commonName=Windows11
Menu msfconsole - Parrot T...
```



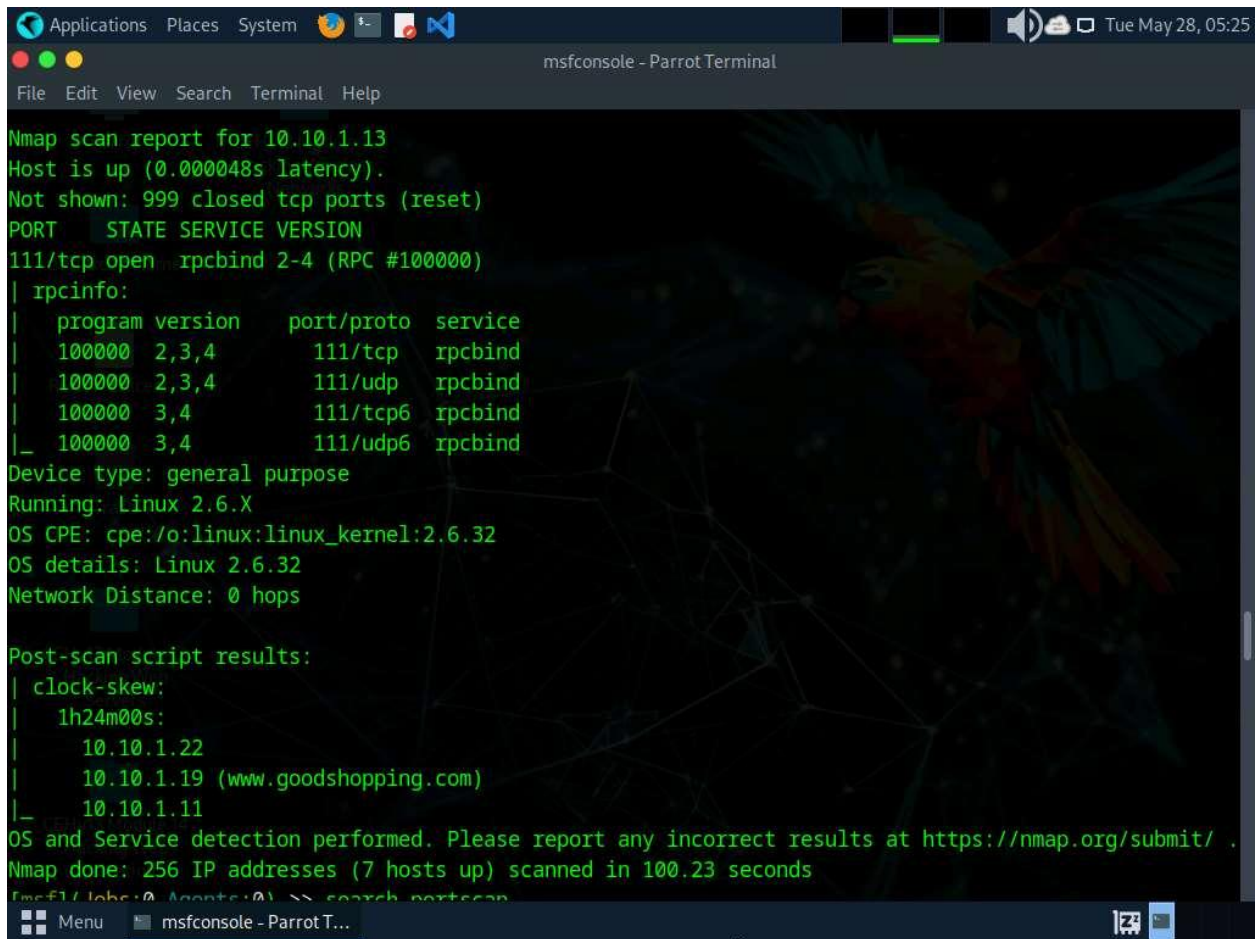
```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.14
Host is up (0.00039s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
5555/tcp  open  adb      Android Debug Bridge device (name: android_x86_64; model: Virtual Machine; device: x86_64; features: cmd,stat_v2,shell_v2)
MAC Address: 02:15:5D:43:08:5D (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Android; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.39 ms  10.10.1.14

Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00038s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      Microsoft ESMTTP 10.0.17763.1
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
```

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00038s latency).
Not shown: 989 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp         Microsoft ESMT
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
TURN ETRN BDAT VRFY
80/tcp    open  http         Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_http-title: GoodShopping
|_http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2022 16.00.1000.00; RC0+
|_ssl-date: 2024-05-28T07:42:06+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-05-28T07:38:18
|_Not valid after: 2054-05-28T07:38:18
| ms-sql-info:
| 10.10.1.19\SQLEXPRESS:
| Instance name: SQLEXPRESS
| Version:
```

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap scan report for 10.10.1.22
Host is up (0.00045s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
|_http-methods:
|_ Potentially risky methods: TRACE
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2024-05-28 07:40:52Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Windows Server 2022 Standard 20348 microsoft-ds (workgroup: CEH)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1801/tcp  open  msmq?
2103/tcp  open  msrpc        Microsoft Windows RPC
2105/tcp  open  msrpc        Microsoft Windows RPC
2107/tcp  open  msrpc        Microsoft Windows RPC
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
Menu msfconsole - Parrot T...
```

```
Nmap scan report for 10.10.1.13
Host is up (0.000048s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
111/tcp    open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp     rpcbind
|   100000  2,3,4      111/udp     rpcbind
|   100000  3,4        111/tcp6    rpcbind
|_  100000  3,4        111/udp6    rpcbind
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

Post-scan script results:
| clock-skew:
|   1h24m00s:
|     10.10.1.22
|     10.10.1.19 (www.goodshopping.com)
|_    10.10.1.11
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 100.23 seconds
[msf1/lobr:0 (Agents:0)] >> search portscan
```

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

```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
Nmap done: 256 IP addresses (7 hosts up) scanned in 100.23 seconds
[msf] (Jobs:0 Agents:0) >> search portscan

Matching Modules
=====

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/portscan/ftpbounce . normal No FTP Bounce Po
rt Scanner
1 auxiliary/scanner/natpmp/natpmp_portscan . normal No NAT-PMP Exter
nal Port Scanner
2 auxiliary/scanner/sap/sap_router_portscanner . normal No SAPRouter Por
t Scanner
3 auxiliary/scanner/portscan/xmas . normal No TCP "XMas" Po
rt Scanner
4 auxiliary/scanner/portscan/ack . normal No TCP ACK Firew
all Scanner
5 auxiliary/scanner/portscan/tcp . normal No TCP Port Scan
ner
6 auxiliary/scanner/portscan/syn . normal No TCP SYN Port
Scanner
7 auxiliary/scanner/http/wordpress_pingback_access . normal No Wordpress Pin
gback Locator
```

7. 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 hit **Enter**.
8. We will use this module to perform an SYN scan against the target IP address range (**10.10.1.5-23**) to look for open port 80 through the eth0 interface.

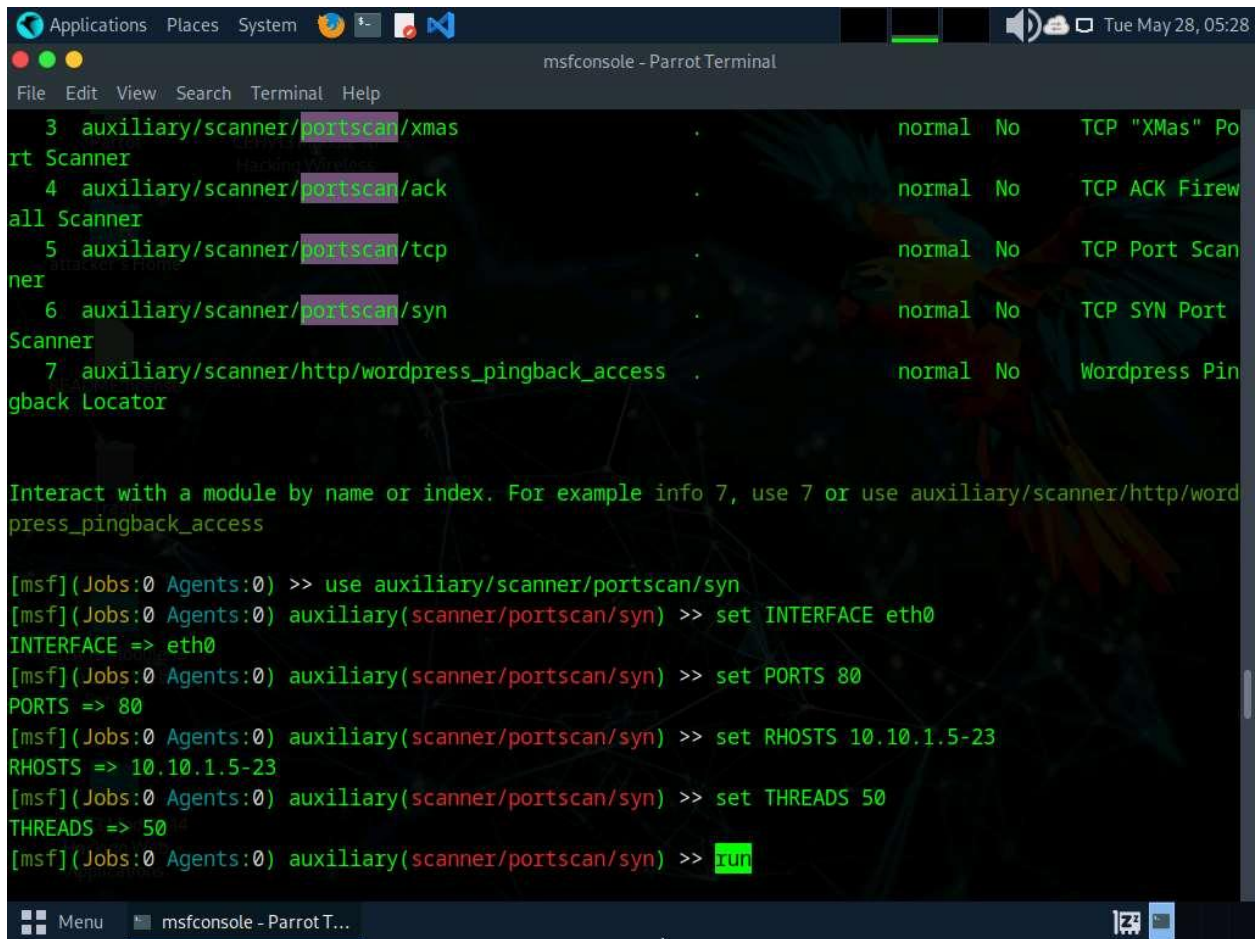
To do so, issue the below commands:

- **set INTERFACE eth0**
- **set PORTS 80**
- **set RHOSTS 10.10.1.5-23**
- **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).

9. 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.



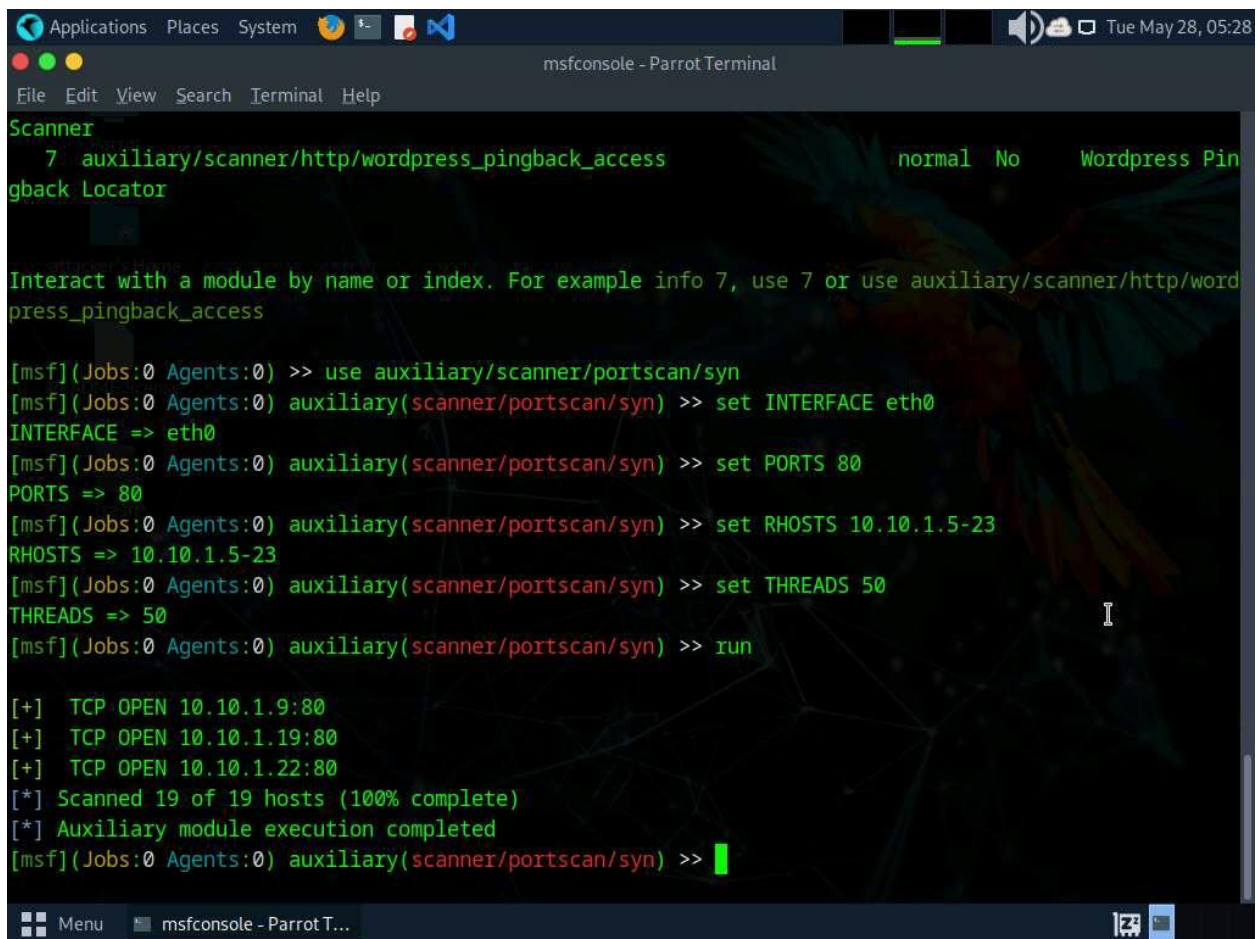
```
Applications  Places  System  msfconsole - Parrot Terminal
File Edit View Search Terminal Help

3 auxiliary/scanner/portscan/xmas . normal No TCP "XMas" Po
rt Scanner
4 auxiliary/scanner/portscan/ack . normal No TCP ACK Firew
all Scanner
5 auxiliary/scanner/portscan/tcp . normal No TCP Port Scan
ner
6 auxiliary/scanner/portscan/syn . normal No TCP SYN Port
Scanner
7 auxiliary/scanner/http/wordpress_pingback_access . normal No Wordpress Pin
gback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/word
press_pingback_access

[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/portscan/syn
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set INTERFACE eth0
INTERFACE => eth0
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set PORTS 80
PORTS => 80
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set THREADS 50
THREADS => 50
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> run
```

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



The screenshot shows a terminal window titled "msfconsole - Parrot Terminal". The background has a dark theme with a parrot illustration. The terminal displays the following text:

```
Scanner
  7 auxiliary/scanner/http/wordpress_pingback_access normal No Wordpress Pin
gback Locator

Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/word
press_pingback_access

[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/portscan/syn
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set INTERFACE eth0
INTERFACE => eth0
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set PORTS 80
PORTS => 80
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> set THREADS 50
THREADS => 50
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> run

[+] TCP OPEN 10.10.1.9:80
[+] TCP OPEN 10.10.1.19:80
[+] TCP OPEN 10.10.1.22:80
[*] Scanned 19 of 19 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >>
```

11. Now, we will perform a TCP scan for open ports on the target systems.
12. To load the **auxiliary/scanner/portscan/tcp** module, type **use auxiliary/scanner/portscan/tcp** and press **Enter**. Run **show options** command to view module options.


```
Applications Places System msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/syn) >> use auxiliary/scanner/portscan/tcp
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/tcp) >> show options

Module options (auxiliary/scanner/portscan/tcp):

  Name      Current Setting  Required  Description
  ----      -
  CONCURRENCY 10              yes       The number of concurrent ports to c
             check per host
  DELAY       0               yes       The delay between connections, per
             thread, in milliseconds
  JITTER      0               yes       The delay jitter factor (maximum va
             lue by which to +/- DELAY) in milli
             seconds.
  PORTS       1-10000         yes       Ports to scan (e.g. 22-25,80,110-90
             0)
  RHOSTS      Module ID: 0    yes       The target host(s), see https://doc
             s.metasploit.com/docs/using-metasplo
             it/basics/using-metasploit.html
  THREADS     1               yes       The number of concurrent threads (m
             ax one per host)
  TIMEOUT     1000            yes       The socket connect timeout in milli
             seconds
```

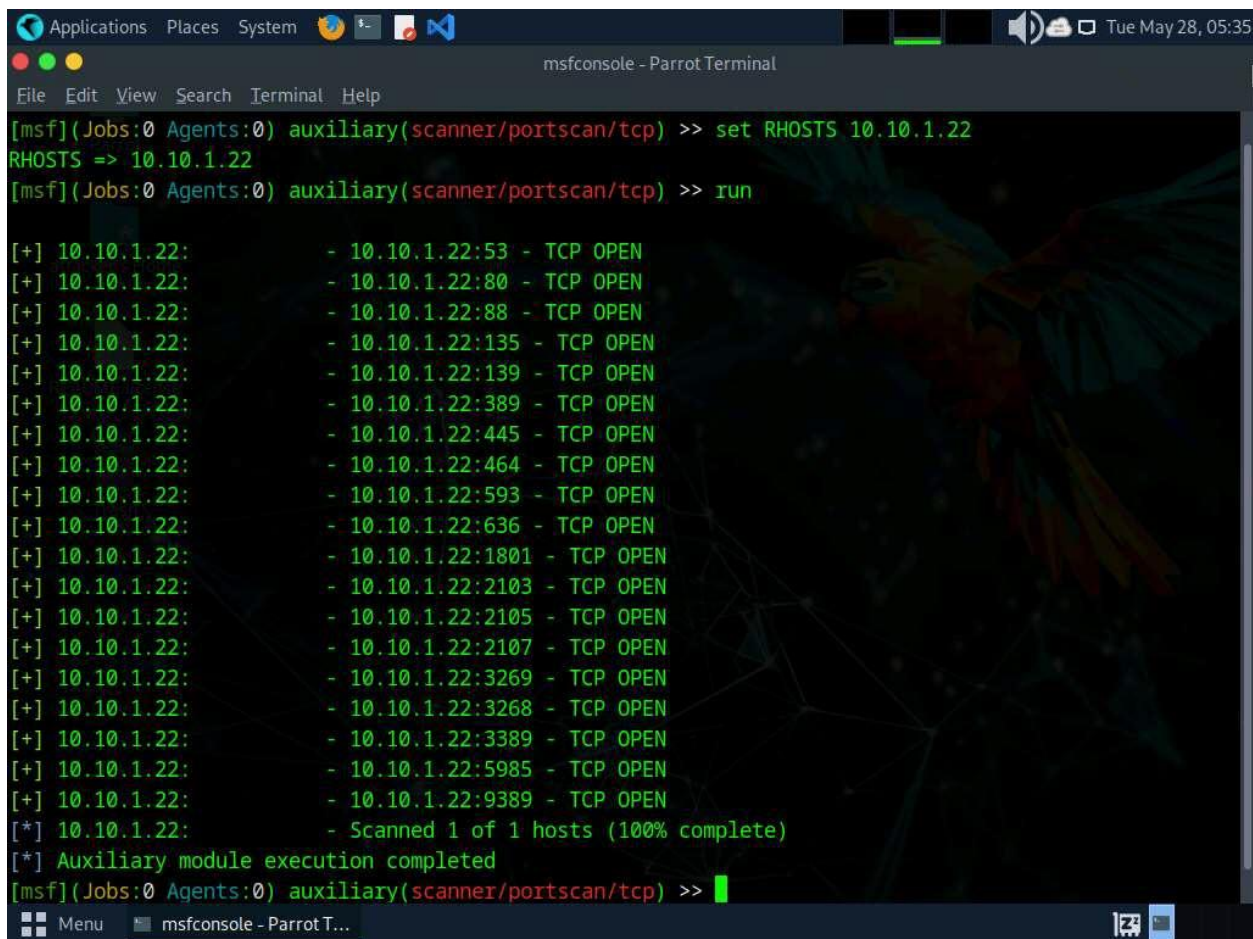
13. Type **set RHOSTS [Target IP Address]** and press **Enter**.

Here, we will perform a TCP scan for open ports on a single IP address (**10.10.1.22**), as scanning multiple IP addresses consumes much time.

14. Type **run** and press **Enter** to discover open TCP ports in the target system.

It will take approximately 20 minutes for the scan to complete.

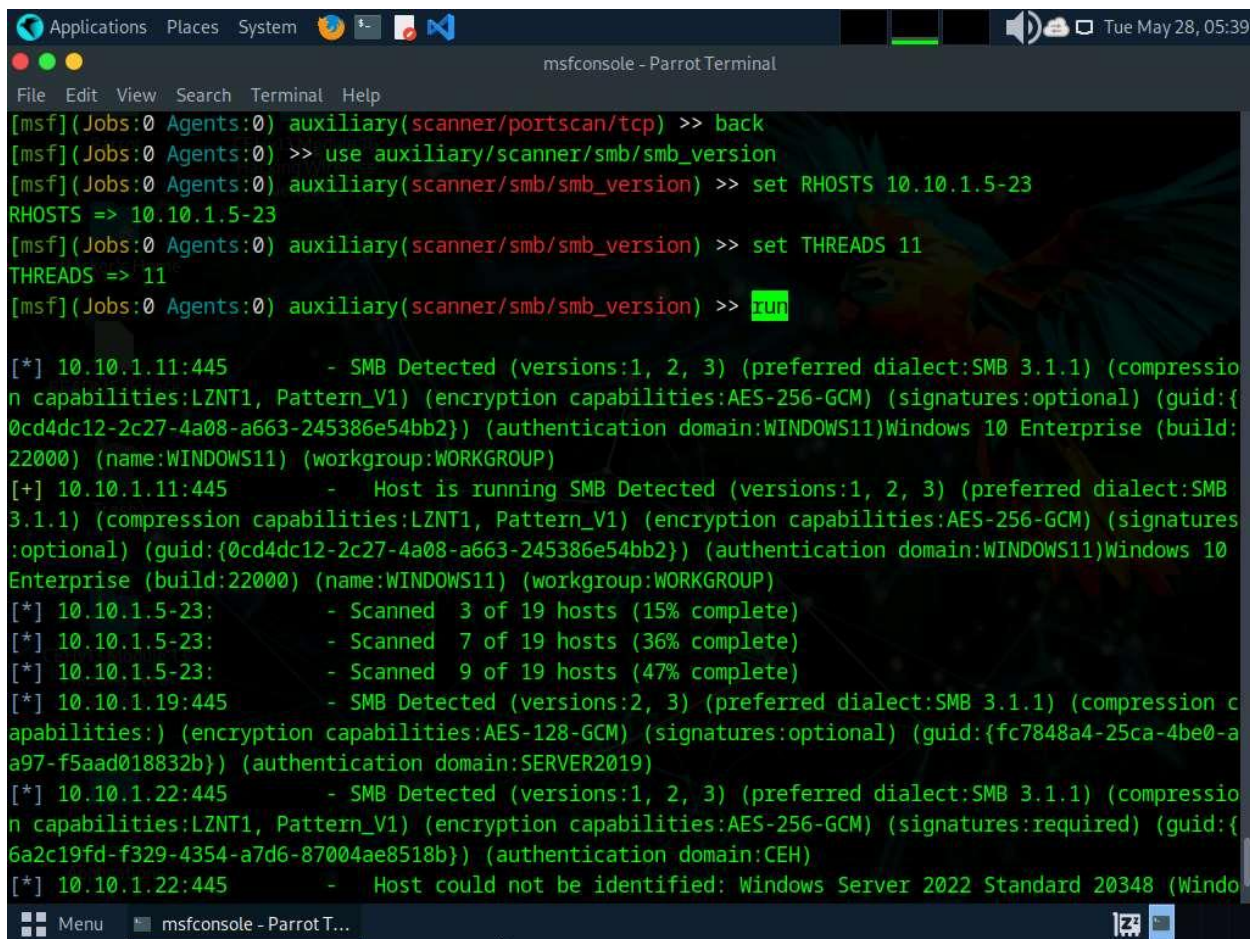
15. The results appear, displaying all open TCP ports in the target IP address (**10.10.1.22**).



```
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/tcp) >> set RHOSTS 10.10.1.22
RHOSTS => 10.10.1.22
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/tcp) >> run

[+] 10.10.1.22:      - 10.10.1.22:53 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:80 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:88 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:135 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:139 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:389 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:445 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:464 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:593 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:636 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:1801 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:2103 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:2105 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:2107 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:3269 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:3268 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:3389 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:5985 - TCP OPEN
[+] 10.10.1.22:      - 10.10.1.22:9389 - TCP OPEN
[*] 10.10.1.22:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/tcp) >>
```

16. 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.
17. To do so, first type **back**, to revert to the msf command line. Then, type **use auxiliary/scanner/smb/smb_version** and hit **enter**.
18. We will use this module to run a SMB version scan against the target IP address range (**10.10.1.5-23**). To do so, issue the below commands:
 - **set RHOSTS 10.10.1.5-23**
 - **set THREADS 11**
19. Type **run** to discover SMB version in the target systems.
20. The result appears, displaying the OS details of the target hosts.



```
msfconsole - Parrot Terminal
File Edit View Search Terminal Help
[msf](Jobs:0 Agents:0) auxiliary(scanner/portscan/tcp) >> back
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/smb/smb_version
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> set RHOSTS 10.10.1.5-23
RHOSTS => 10.10.1.5-23
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> set THREADS 11
THREADS => 11
[msf](Jobs:0 Agents:0) auxiliary(scanner/smb/smb_version) >> run

[*] 10.10.1.11:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:optional) (guid:{0cd4dc12-2c27-4a08-a663-245386e54bb2}) (authentication domain:WINDOWS11)Windows 10 Enterprise (build:22000) (name:WINDOWS11) (workgroup:WORKGROUP)
[+] 10.10.1.11:445 - Host is running SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:optional) (guid:{0cd4dc12-2c27-4a08-a663-245386e54bb2}) (authentication domain:WINDOWS11)Windows 10 Enterprise (build:22000) (name:WINDOWS11) (workgroup:WORKGROUP)
[*] 10.10.1.5-23: - Scanned 3 of 19 hosts (15% complete)
[*] 10.10.1.5-23: - Scanned 7 of 19 hosts (36% complete)
[*] 10.10.1.5-23: - Scanned 9 of 19 hosts (47% complete)
[*] 10.10.1.19:445 - SMB Detected (versions:2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:) (encryption capabilities:AES-128-GCM) (signatures:optional) (guid:{fc7848a4-25ca-4be0-a97-f5aad018832b}) (authentication domain:SERVER2019)
[*] 10.10.1.22:445 - SMB Detected (versions:1, 2, 3) (preferred dialect:SMB 3.1.1) (compression capabilities:LZNT1, Pattern_V1) (encryption capabilities:AES-256-GCM) (signatures:required) (guid:{6a2c19fd-f329-4354-a7d6-87004ae8518b}) (authentication domain:CEH)
[*] 10.10.1.22:445 - Host could not be identified: Windows Server 2022 Standard 20348 (Windows)
```

21. You can further explore various modules of Metasploit such as FTP module to identify the FTP version running in the target host.
22. This information can further be used to perform vulnerability analysis on the open services discovered in the target hosts.
23. 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.
24. Close all open windows and document all the acquired information.

Question 3.5.1.1

Use the Metasploit to scan the target machine. While using Metasploit auxiliary module “auxiliary/scanner/smb/smb_version”, enter the specified range of remote hosts (RHOSTS).