Date: 21/12/2024

Lab Practical #02:

Perform NMAP tool for scanning system vulnerability

Practical Assignment #02:

1. Nmap -p <Port> <IP>:

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 23 192.168.137.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 06:01 EST
Nmap scan report for 192.168.137.178
Host is up (0.0013s latency).

PORT   STATE    SERVICE
23/tcp filtered telnet

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

2. Nmap -pU:100,T:23-25 <IP> :- UDP,TCP Port Scanning

```
┌──(kali㉿kali)-[~]
└─$ nmap -pU:100,T:23-25,443 192.168.137.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 06:06 EST
WARNING: Your ports include "U:" but you haven't specified UDP scan with -sU.
Nmap scan report for 192.168.137.178
Host is up (0.0015s latency).

PORT    STATE    SERVICE
23/tcp  filtered telnet
24/tcp  filtered priv-mail
25/tcp  filtered smtp
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 1.35 seconds
```

3. Nmap -p ftp <IP>:- Port Scanning using Name

```
┌──(kali㉿kali)-[~]
└─$ nmap -p ftp 192.168.137.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 06:19 EST
Nmap scan report for 192.168.137.178
Host is up (0.019s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

4. Namp -r <IP> :- Sequential Port Scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -r 192.168.137.178
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 06:20 EST
Nmap scan report for 192.168.137.178
Host is up (0.0030s latency).
All 1000 scanned ports on 192.168.137.178 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.25 seconds
```

Date: 21/12/2024

5. **Nmap <IP> -sL : List IP without Scaning**

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.137.178-185 -sL
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-17 06:24 EST
Nmap scan report for 192.168.137.178
Nmap scan report for 192.168.137.179
Nmap scan report for 192.168.137.180
Nmap scan report for 192.168.137.181
Nmap scan report for 192.168.137.182
Nmap scan report for 192.168.137.183
Nmap scan report for 192.168.137.184
Nmap scan report for 192.168.137.185
Nmap done: 8 IP addresses (0 hosts up) scanned in 0.02 seconds
```

6. **Npam <IP> -PS22-25,80 : TCP SYN discovery on Specified port**

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.79 -PA22-25,80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:04 EST
Nmap scan report for 192.168.32.79
Host is up (0.0014s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 5.99 seconds
```

7. **Nmap <IP> -PR : ARP discovery on specified port**

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.79 -PR
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:03 EST
Nmap scan report for 192.168.32.79
Host is up (0.012s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 7.02 seconds
```

8. **Nmap <ip> -sV : try to find version of service on port**

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.79 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:11 EST
Nmap scan report for 192.168.32.79
Host is up (0.0017s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.82 seconds
```

Date: 21/12/2024

9. Nmap <IP> -sV --version-all : set intensity level

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.79 -sV --version-all
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:12 EST
Nmap scan report for 192.168.32.79
Host is up (0.0014s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3306/tcp open  mysql         MySQL (unauthorized)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.96 seconds
```

10. Nmap <IP> -O : Remote OS detection

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.79 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:16 EST
Nmap scan report for 192.168.32.79
Host is up (0.0030s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (94%), QEMU (89%), Bay Networks embedded (85%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (94%), QEMU user mode network gateway (89%), Bay Networks BayStack 450 swi
tch (software version 3.1.0.22) (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.30 seconds
```

11. Nmap -T5 <IP> : very aggressive scan

```
└─$ nmap -T5 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:31 EST
Nmap scan report for 192.168.32.79
Host is up (0.0015s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 3.60 seconds
```

12. Nmap -T4 <IP>: aggressive scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:35 EST
Nmap scan report for 192.168.32.79
Host is up (0.0012s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 5.99 seconds
```

Date: 21/12/2024

13. Nmap -T3 <IP>: Default scan timer

```
┌──(kali㉿kali)-[~]
└─$ nmap -T3 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:35 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.80% done
Nmap scan report for 192.168.32.79
Host is up (0.0045s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 6.20 seconds
```

14. Nmap <IP> -sS

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.79 -sS
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:38 EST
Nmap scan report for 192.168.32.79
Host is up (0.0027s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 5.93 seconds
```

15. Namp <IP> -sU: UDP port scane

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.32.79 -sU
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 09:43 EST
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 78.17% done; ETC: 09:47 (0:00:51 remaining)
Stats: 0:03:03 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 78.27% done; ETC: 09:47 (0:00:51 remaining)
Stats: 0:04:04 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 80.35% done; ETC: 09:48 (0:01:00 remaining)
Stats: 0:08:10 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 09:51 (0:00:00 remaining)
Stats: 0:09:39 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 09:52 (0:00:00 remaining)
Stats: 0:12:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 09:55 (0:00:00 remaining)
Nmap scan report for 192.168.32.79
Host is up (0.0018s latency).
All 1000 scanned ports on 192.168.32.79 are in ignored states.
Not shown: 974 filtered udp ports (port-unreach), 26 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 766.77 seconds
```

16. Nmap -SX <IP>: XMAS scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -sX 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:00 EST
Nmap scan report for 192.168.32.79
Host is up (0.00045s latency).
All 1000 scanned ports on 192.168.32.79 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

Date: 21/12/2024

17. Nmap -Sp <IP>: Ping Scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:01 EST
Nmap scan report for 192.168.32.79
Host is up (0.0018s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

18. Nmap -oN scan.txt <IP>: normal output

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -oN scan.txt 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:12 EST
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 48.85% done; ETC: 10:13 (0:00:03 remaining)
Nmap scan report for 192.168.32.79
Host is up (0.0019s latency).
All 1000 scanned ports on 192.168.32.79 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 19.16 seconds
```

19. Nmap -oX scan.xml <IP>: Xml format

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -oX scan.xml 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:14 EST
Nmap scan report for 192.168.32.79
Host is up (0.0023s latency).
All 1000 scanned ports on 192.168.32.79 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 19.60 seconds
```

20. Nmap -open <IP>: show open ports only

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -open 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:16 EST
Nmap done: 1 IP address (1 host up) scanned in 18.60 seconds
```

21. Nmap <IP Range>: scan range of IPs

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap 192.168.32.79-81
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:23 EST
Nmap scan report for 192.168.32.79
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.32.79 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.32.80
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.32.80 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap scan report for 192.168.32.81
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.32.81 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 3 IP addresses (3 hosts up) scanned in 43.01 seconds
```

Date: 21/12/2024

22. Nmap -sP <IP>: Ping Scan only

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sP 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:24 EST
Nmap scan report for 192.168.32.79
Host is up (0.0020s latency).
Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds
```

23. Nmap -traceroute <IP>: Tracerouter

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -traceroute 192.168.32.79
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:29 EST
Nmap scan report for 192.168.32.79
Host is up (0.0034s latency).
All 1000 scanned ports on 192.168.32.79 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   3.00 ms 10.0.2.2
2   4.13 ms 192.168.32.79

Nmap done: 1 IP address (1 host up) scanned in 31.64 seconds
```

24. Nmap <Domain name>: scan Domain

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-21 10:34 EST
Failed to resolve "scanme.nmap.org".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.06 seconds
```