Vivekanand Education Society's Institute of Technology

Department of AI & DS Engineering

Subject: Cryptography and System Security

Class: D11AD

Roll No: 46	**Name: Ashish Patil**
Practical No:8	**Title: Port Scanning using NMAP**
DOP:	**DOS:**
Grades:	**LOs Mapped:**
Signature:	

Title: Port Scanning using NMAP
DOP: /3/24
DOS: /3/24

(Attach output screenshots)

Aim: To download and use nmap to simulate port scanning

Theory:

features include:

- **Host Discovery** – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
- **Port Scanning** – Enumerating the open ports on one or more target hosts.
- **Version Detection** – Interrogating listening network services listening on remote devices to determine the application name and version number.
- **OS Detection** – Remotely determining the operating system and some hardware characteristics of network devices.

Basic commands working in Nmap:

•For target specifications: nmap<target‘s URL or IP with spaces between them>

•For OS detection: nmap -O <target-host's URL or IP>

•For version detection: nmap -sV<target-host's URL or IP>

SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections

Steps:-

1.Get root access: $ sudosu root

2.#ifconfig

3.# apt-get install nmap

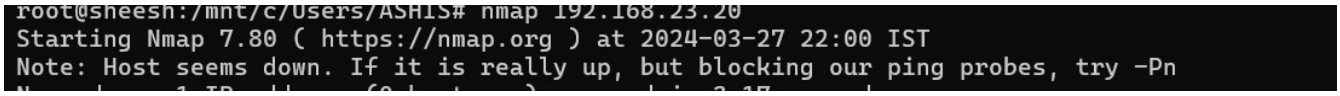
Commands:-

1. # nmap -

V

It gives the version of Nmap

2. # nmap 192.168.23.20



It gives information about a single host. It gives the output in column form where first column is the PORT, second column is the STATE and third column is the SERVICE

3. #nmap –v 192.168.23.20

```
root@sheesh:/mnt/c/Users/ASHIS# nmap -v 192.168.23.20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:00 IST
Failed to resolve "-v".
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.18 seconds
root@sheesh:/mnt/c/Users/ASHIS# nmap --v 192.168.23.20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:00 IST
Failed to resolve "--v".

root@sheesh:/mnt/c/Users/ASHIS# nmap 192.168.23.20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:01 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds
root@sheesh:/mnt/c/Users/ASHIS# nmap -v 192.168.23.20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:02 IST
Initiating Ping Scan at 22:02
Scanning 192.168.23.20 [4 ports]
Completed Ping Scan at 22:02, 3.04s elapsed (1 total hosts)
Nmap scan report for 192.168.23.20 [host down]
```

It gives the detailed information about remote host.

4. #nmap –O 192.168.23.20

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:0
WARNING: No targets were specified, so 0 hosts scanned.
```

It finds the remote host operating system and version (OS detection)

5. # nmap –sP 192.168.23.0/24

```
root@sheesh:/mnt/c/Users/ASHIS# nmap -o 192.168.23.20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:03 IST
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds
root@sheesh:/mnt/c/Users/ASHIS# nmap -sP 192.168.23.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:03 IST
Failed to resolve "-sP".

root@sheesh:/mnt/c/Users/ASHIS# nmap -sP 192.168.23.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:03 IST
```

It scans a network and discover which servers and devices are up and running(ping scan)

6. # nmap -sA 192.168.23.20

```
root@sheesh:/mnt/c/Users/ASHIS# nmap -sA 192.168.23.20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:05 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
```

To discover if a host/network is protected by a firewall. The output has the word **FILTERED**which shows presence of firewall. **UNFILTERED**means no firewall**.**

7. # nmap -p T:23 192.168.23.20

```
root@sheesh:/mnt/c/Users/ASHIS# nmap -p T:23 192.168.23.20
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:06 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -
```

It scans TCP port 23

8. #nmap -p 80,443 192.168.23.20

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:06 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
```

It scansmultiple ports at one time

9. # nmap -sV 192.168.23.20

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-03-27 22:07 IST
Note: Host seems down. If it is really up, but blocking our ping probes
Nmap done: 1 IP address (0 hosts up) scanned in 3.35 seconds
```

It detect remote services (server / daemon) version numbers. Version numbers are displayed only if the Port is open

10. nmap -sS 192.168.23.20

```
root@sheesh:/mnt/c/Users/ASHIS# nmap -sU 192.168.0.107
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 02:18 IST
Note: Host seems down. If it is really up, but blocking our ping probes, t
Nmap done: 1 IP address (0 hosts up) scanned in 3.16 seconds
root@sheesh:/mnt/c/Users/ASHIS# nmap -sU -Pn 192.168.0.107
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 02:18 IST
Nmap scan report for host.docker.internal (192.168.0.107)
Host is up (0.00033s latency).
Not shown: 991 closed ports
PORT     STATE         SERVICE
137/udp  open|filtered netbios-ns
138/udp  open|filtered netbios-dgm
500/udp  open|filtered isakmp
1900/udp open|filtered upnp
3702/udp open|filtered ws-discovery
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Nmap done: 1 IP address (1 host up) scanned in 43.37 seconds
root@sheesh:/mnt/c/Users/ASHIS# nmap -sF -Pn 192.168.0.107
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-01 02:20 IST
```

It performs SYN scan or Stealth scan.

Open wireshark.

Set the Filter to TCP.

See the grey and red color packets

Double click any grey color TCP packet where destination address is the neighbour's address

See the Flag field of TCP: SYN bit should be set to 1

11. # nmap -sN 192.168.23.20

It performs TCP Null Scan. It does not set any bits (TCP flag header is 0)

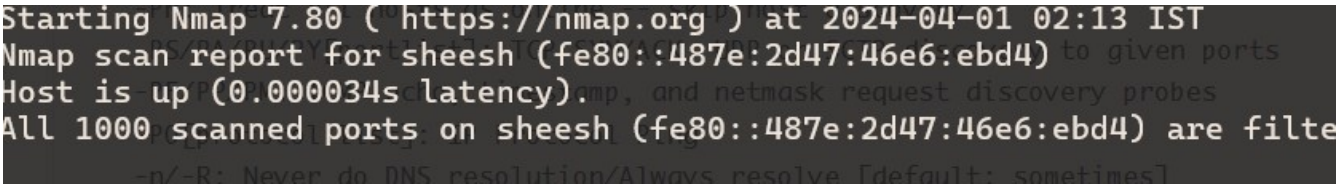
Open wireshark.

Set the Filter to TCP.

Double click any grey color TCP packet where destination address is the neighbour's address

See the Flag field of TCP: No flag bits should be set

12. # nmap –sF 192.168.23.20



It performs FIN scan. It sets just the TCP FIN bit.

Open wireshark.

Set the Filter to TCP.

Double click any grey color TCP packet where destination address is the neighbour's address

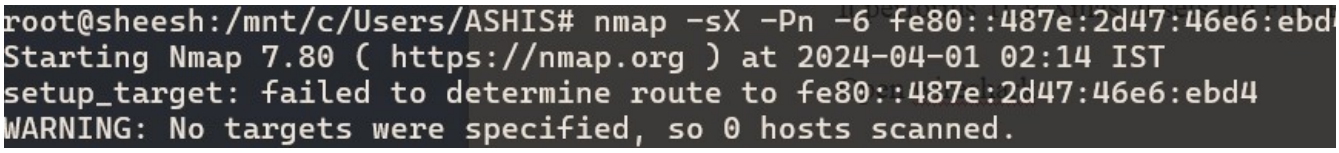
See the Flag field of TCP: FIN flag should be set to 1

13.# nmap -sX 192.168.23.20

It performs TCP Xmas. It sets the FIN, PSH, and URG flags.

Open wireshark.

Set the Filter to TCP.

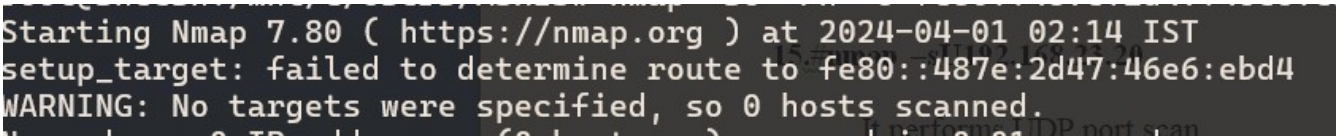


Double click any grey color TCP packet where destination address is the neighbour's address

See the Flag field of TCP: FIN, PSH, and URG flagsshould be set to 1

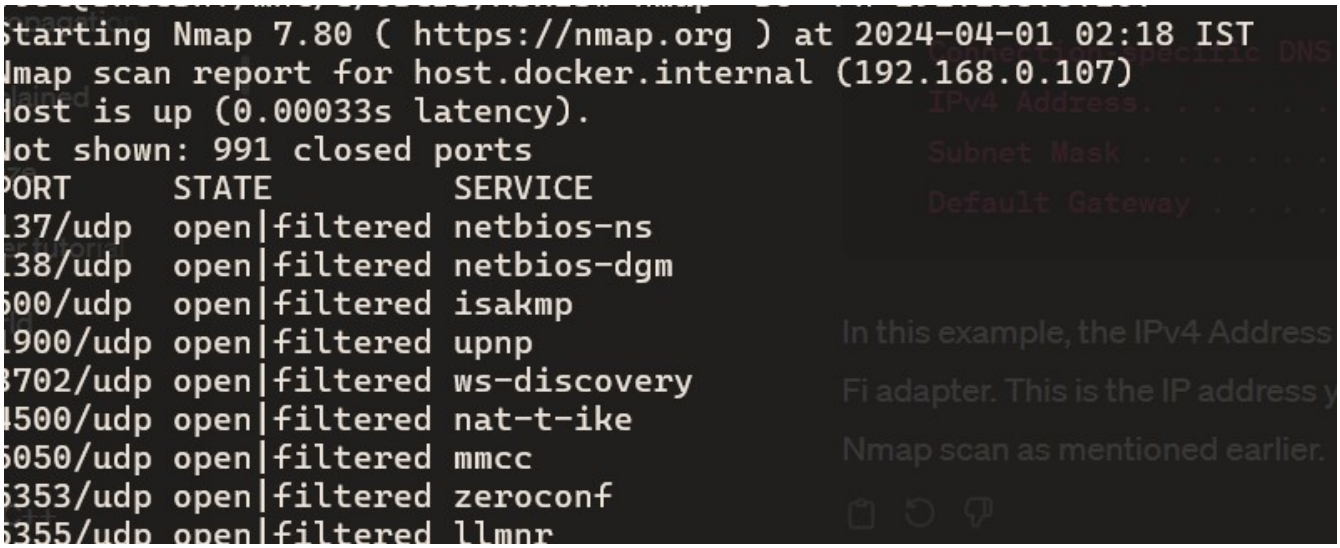
14.# nmap –sO192.168.23.20

It performs IP protocol scan and allows us to determine which IP protocols) are supported by target machines.



15.#nmap –sU192.168.23.20

It performs UDP port scan.


Starting Nmap 7.80 (https://nmap.org) at 2024-04-01 02:18 IST
Nmap scan report for host.docker.internal (192.168.0.107)
Host is up (0.00033s latency).
Not shown: 991 closed ports
PORT STATE SERVICE
137/udp open|filtered netbios-ns
138/udp open|filtered netbios-dgm
500/udp open|filtered isakmp
1900/udp open|filtered upnp
3702/udp open|filtered ws-discovery
4500/udp open|filtered nat-t-ike
5050/udp open|filtered mmcc
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr

Conclusion: