Aim: Simulate port scanning attack using Nmap

Theory:

Nmap (Network Mapper) is a security scanner which is used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simples port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap 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

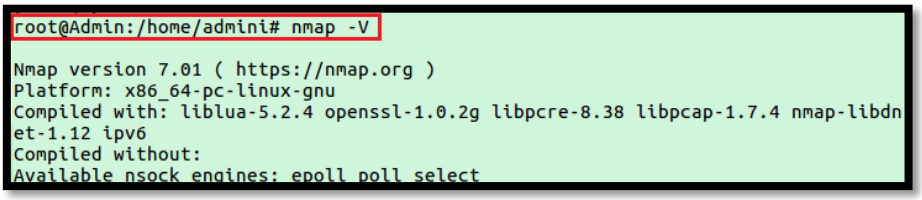
Steps: -

1. Get root access: $ sudo su 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.

```
root@Admin:/home/admini# nmap 192.168.0.107

Starting Nmap 7.01 ( https://nmap.org ) at 2020-02-27 13:14 IST
Nmap scan report for 192.168.0.107
Host is up (0.000011s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
1521/tcp open  oracle

Nmap done: 1 IP address (1 host up) scanned in 1.64 seconds
root@Admin:/home/admini#
```

3. #nmap –v 192.168.23.20

   It gives the detailed information about remote host.

```
root@Admin:/home/admini# nmap -v 192.168.0.133

Starting Nmap 7.01 ( https://nmap.org ) at 2020-02-27 13:18 IST
Initiating ARP Ping Scan at 13:18
Scanning 192.168.0.133 [1 port]
Completed ARP Ping Scan at 13:18, 0.24s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:18
Completed Parallel DNS resolution of 1 host. at 13:18, 0.00s elapsed
Initiating SYN Stealth Scan at 13:18
Scanning 192.168.0.133 [1000 ports]
Discovered open port 139/tcp on 192.168.0.133
Discovered open port 21/tcp on 192.168.0.133
Discovered open port 445/tcp on 192.168.0.133
Discovered open port 80/tcp on 192.168.0.133
Discovered open port 1521/tcp on 192.168.0.133
Discovered open port 902/tcp on 192.168.0.133
Completed SYN Stealth Scan at 13:18, 1.26s elapsed (1000 total ports)
Nmap scan report for 192.168.0.133
Host is up (0.00030s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
1521/tcp open  oracle
MAC Address: E4:54:E8:C6:8E:C1 (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
           Raw packets sent: 1002 (44.072KB) | Rcvd: 1002 (40.092KB)
root@Admin:/home/admini#
```

4. #nmap –O 192.168.23.20

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

5. # nmap –sP 192.168.23.0/24

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

```
root@Admin:/home/admini# nmap -sP 192.168.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2020-02-27 13:22 IST
Nmap scan report for 192.168.0.1
Host is up (0.00017s latency).
MAC Address: 14:CC:20:F5:71:26 (Tp-link Technologies)
Nmap scan report for 192.168.0.100
Host is up (0.00025s latency).
MAC Address: D4:BE:D9:C7:69:28 (Dell)
Nmap scan report for 192.168.0.102
Host is up (0.00038s latency).
MAC Address: E4:54:E8:C6:38:A1 (Unknown)
Nmap scan report for 192.168.0.104
Host is up (-0.10s latency).
MAC Address: 44:87:FC:E0:E4:F0 (Elitegroup Computer System)
Nmap scan report for 192.168.0.105
Host is up (-0.10s latency).
MAC Address: E4:54:E8:C6:38:2A (Unknown)
Nmap scan report for 192.168.0.106
Host is up (-0.10s latency).
MAC Address: E4:54:E8:C6:38:6D (Unknown)
Nmap scan report for 192.168.0.110
Host is up (0.00065s latency).
MAC Address: E4:54:E8:C6:36:85 (Unknown)
Nmap scan report for 192.168.0.111
Host is up (0.00020s latency).
MAC Address: D4:BE:D9:C7:89:45 (Dell)
Nmap scan report for 192.168.0.112
Host is up (0.00015s latency).
MAC Address: E4:54:E8:C6:37:78 (Unknown)
Nmap scan report for 192.168.0.115
```

6. # nmap -sA 192.168.23.20

   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.

```
root@Admin:/home/admini# nmap -sA 192.168.0.133

Starting Nmap 7.01 ( https://nmap.org ) at 2020-02-27 13:39 IST
Nmap scan report for 192.168.0.133
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.0.133 are unfiltered
MAC Address: E4:54:E8:C6:8E:C1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
root@Admin:/home/admini#
```

7. # nmap -p T:23 192.168.23.20
   It scans TCP port 23

```
root@Admin:/home/admini# nmap -p T:23 192.168.0.133

Starting Nmap 7.01 ( https://nmap.org ) at 2020-02-27 13:43 IST
Nmap scan report for 192.168.0.133
Host is up (0.00047s latency).
PORT   STATE  SERVICE
23/tcp closed telnet
MAC Address: E4:54:E8:C6:8E:C1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

8. # nmap -p 80,443 192.168.23.20
   It scans multiple ports at one time

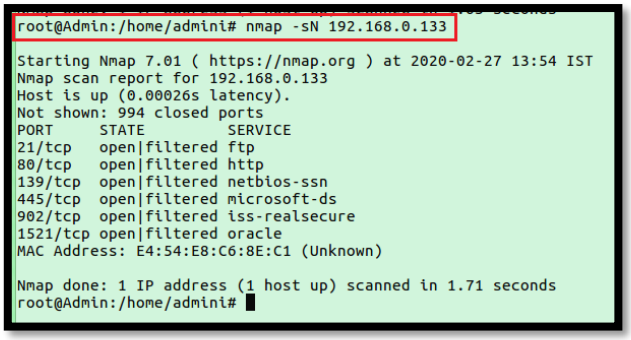
```
root@Admin:/home/admini# nmap -p 80,21,4000,8000,5000 192.168.0.133

Starting Nmap 7.01 ( https://nmap.org ) at 2020-02-27 13:45 IST
Nmap scan report for 192.168.0.133
Host is up (0.00047s latency).
PORT     STATE  SERVICE
21/tcp   open   ftp
80/tcp   open   http
4000/tcp closed remoteanything
5000/tcp closed upnp
8000/tcp closed http-alt
MAC Address: E4:54:E8:C6:8E:C1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
root@Admin:/home/admini#
```

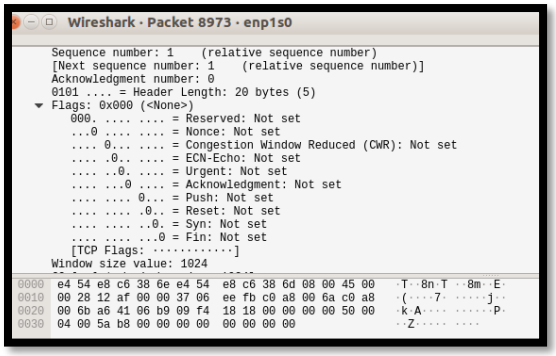
9. # nmap -sV 192.168.23.20
   It detect remote services (server / daemon) version numbers. Version numbers are displayed only if the Port is open
10. nmap -sS 192.168.23.20
    It performs SYN scan or Stealth scan.
    Open wireshark.
    Set the Filter to TCP.
    See the grey and red color packets
    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

```
root@Admin:/home/admini# nmap -sS 192.168.0.133

Starting Nmap 7.01 ( https://nmap.org ) at 2020-02-27 13:51 IST
Nmap scan report for 192.168.0.133
Host is up (0.00027s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
1521/tcp open  oracle
MAC Address: E4:54:E8:C6:8E:C1 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
root@Admin:/home/admini#
```

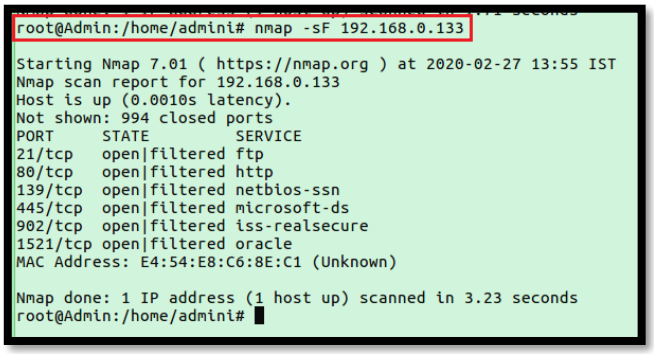
```
Wireshark · Packet 2328 · enp1s0
    [Next sequence number: 0    (relative sequence number)]
    Acknowledgment number: 0
    0110 .... = Header Length: 24 bytes (6)
  ▼ Flags: 0x002 (SYN)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...0 .... = Acknowledgment: Not set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ▼ .... .... ..1. = Syn: Set
      ▼ [Expert Info (Chat/Sequence): Connection establish request (SYN): server port 2043]
          [Connection establish request (SYN): server port 2043]
          [Severity level: Chat]
          [Group: Sequence]

0000  e4 54 e8 c6 8e c1 e4 54  e8 c6 38 6e 08 00 45 00   ·T·····T ··8n··E·
0010  00 2c 7a 0b 00 00 28 06  96 80 c0 a8 00 6b c0 a8   ·,z···(· ·····k··
0020  00 85 ef 41 07 fb 57 80  11 cc 00 00 00 00 60 02   ···A··W· ......`·
0030  04 00 b1 5c 00 00 02 04  05 b4                     ···\···· ··
```

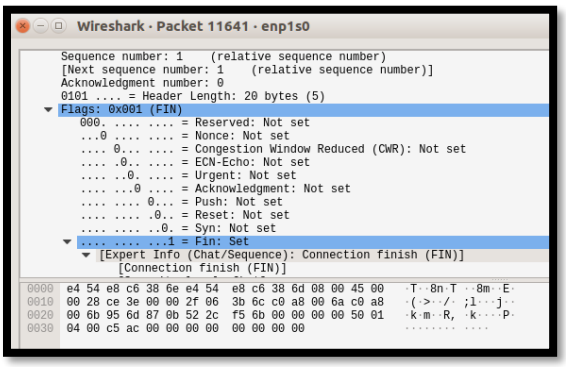
11. # nmap -sN 192.168.23.20
    It performs TCP Null Scan. It does not set any bits (TCP flag header is 0)
    Open wireshark.
    Set the Filter to TCP.
    Double click any grey color TCP packet where destination address is the neighbour's address.
    See the Flag field of TCP: No flag bits should be set.



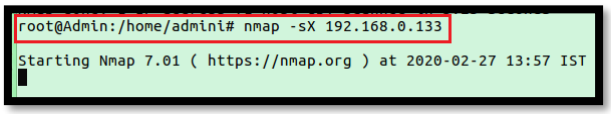


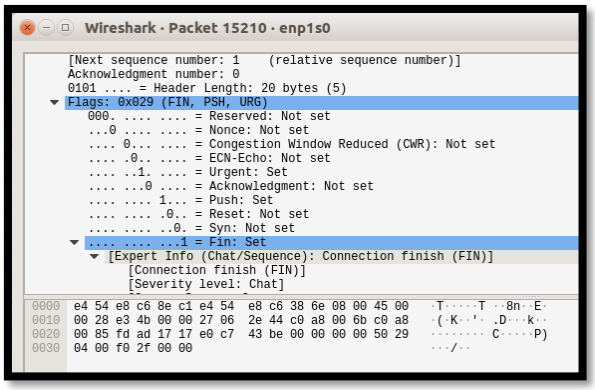
12. # nmap –sF 192.168.23.20
    It performs FIN scan. It sets just the TCP FIN bit.
    Open wireshark.
    Set the Filter to TCP.
    Double click any grey color TCP packet where destination address is the neighbour's address.
    See the Flag field of TCP: FIN flag should be set to 1.





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 flags should be set to 1.





14. # nmap –sO 192.168.23.20
    It performs IP protocol scan and allows us to determine which IP protocols) are supported by target machines.
15. #nmap –sU 192.168.23.20
    It performs UDP port scan.