Terna Engineering College

Computer Engineering Department

Class: TE **Sem.: VI**

Course: System Security Lab

PART A

(PART A : TO BE REFFERED BY STUDENTS)

Experiment No.7

A.1 Aim: Download and install nmap. Use it with different options to scan open ports, perform OSfingerprinting, do a ping scan, tcp port scan, udp port scan, xmas scan etc.

A.2 Prerequisite:

1. Basic Knowledge of Ports, TCP, UDP, Ping

A.3 Outcome:

After successful completion of this experiment students will be able to

Install and use nmap and use it for gathering detailed network and remote host information.

A.4 Theory:

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) 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 simple 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 isalso relatively unobtrusive and stealthy since it never completes TCP connections.

A5.Procedure:

Installation of Nmap:

$ sudo apt-get install nmap

Commands:

- **nmap -sP<10.0.0.0/24>**

  Ping scans the network, listing machines that respond to ping.

- **FIN scan (-sF)**

  Sets just the TCP FIN bit.

- **-sV (Version detection) .**

  Enables version detection, as discussed above. Alternatively, can use -A, which enables version detection among other things.

- **-sO (IP protocol scan) .**

IP protocol scan allows you to determine which IP protocols (TCP, ICMP, IGMP, etc.) are

supported by target machines. This isn´t technically a port scan, since it cycles through IP protocol numbers rather than TCP or UDP port numbers.

- **-O (Enable OS detection) .**

  Enables OS detection, as discussed above. Alternatively, you can use -A to enable OS detection along with other things.

- **-p port ranges (Only scan specified ports) .**

  This option specifies which ports you want to scan and overrides the default. Individual port numbers are OK, as are ranges separated by a hyphen (e.g. 1-1023). The beginning and/or end values of a range may be omitted, causing Nmap to use 1 and 65535, respectively.

- --top-ports <integer of 1 or greater>

  Scans the N highest-ratio ports found in nmap-services file.

- nmap –iflist

host interface and route information with nmap by using ―–iflist‖ option.

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

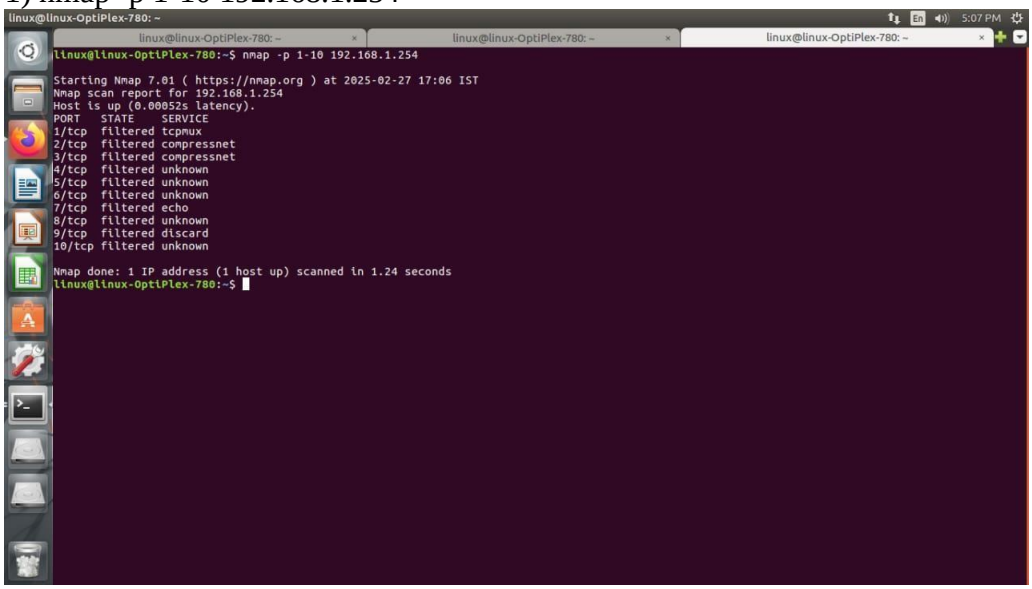
(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Blackboard or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no Black board access available)

Roll No. 30	**Name: Bhatt Pranjal Deepak**
Class : TE-B	**Batch : B2**
Date of Experiment:	**Date of Submission**
Grade :	

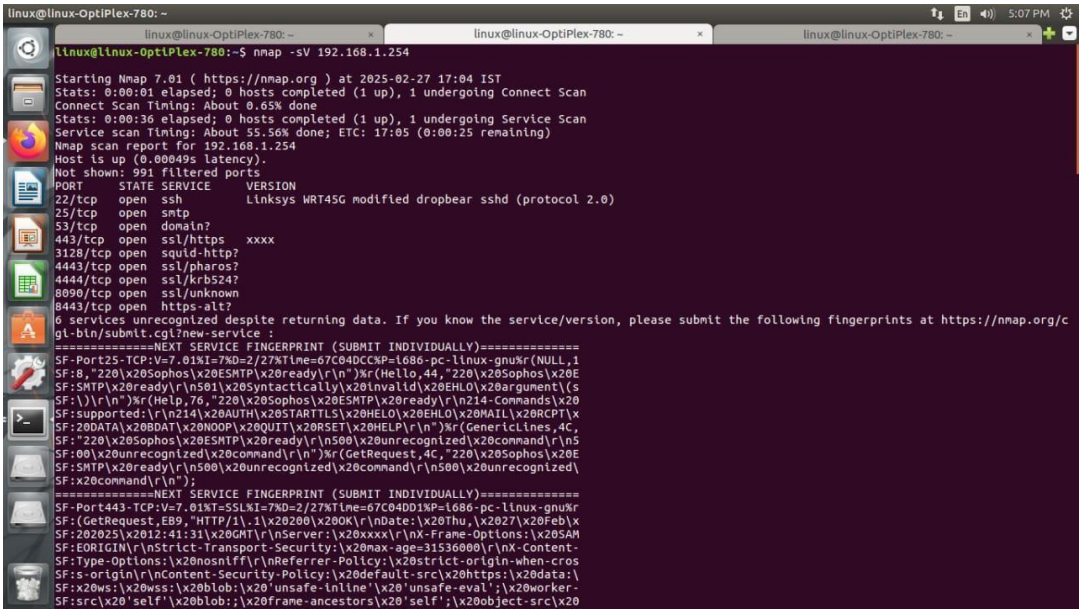
B.1 Output

(add snapshot of output)

1) nmap -p 1-10 192.168.1.254

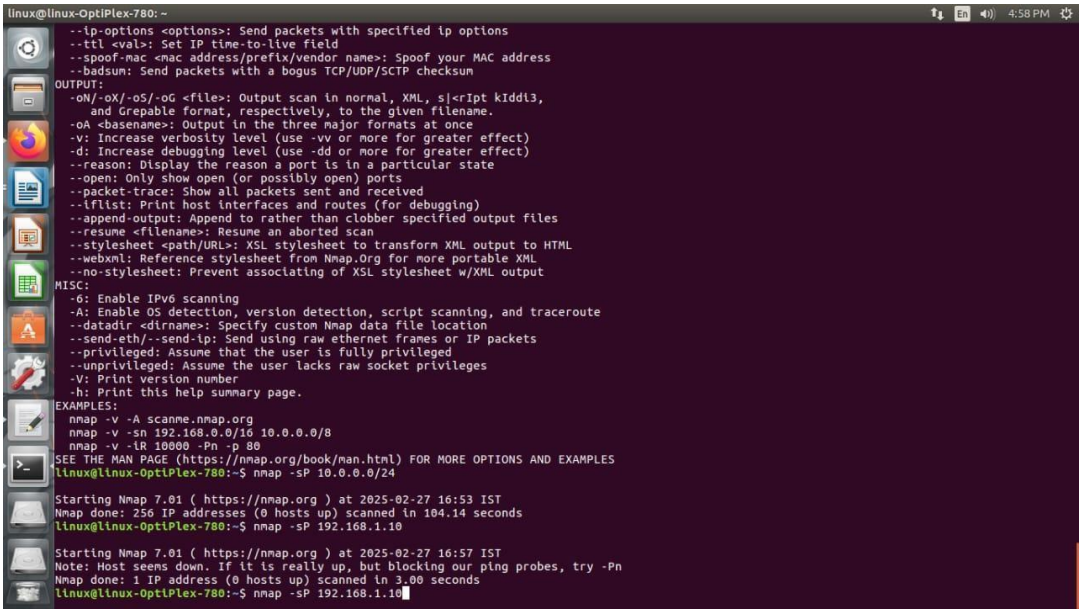


2) nmap -sV 192.168.1.254



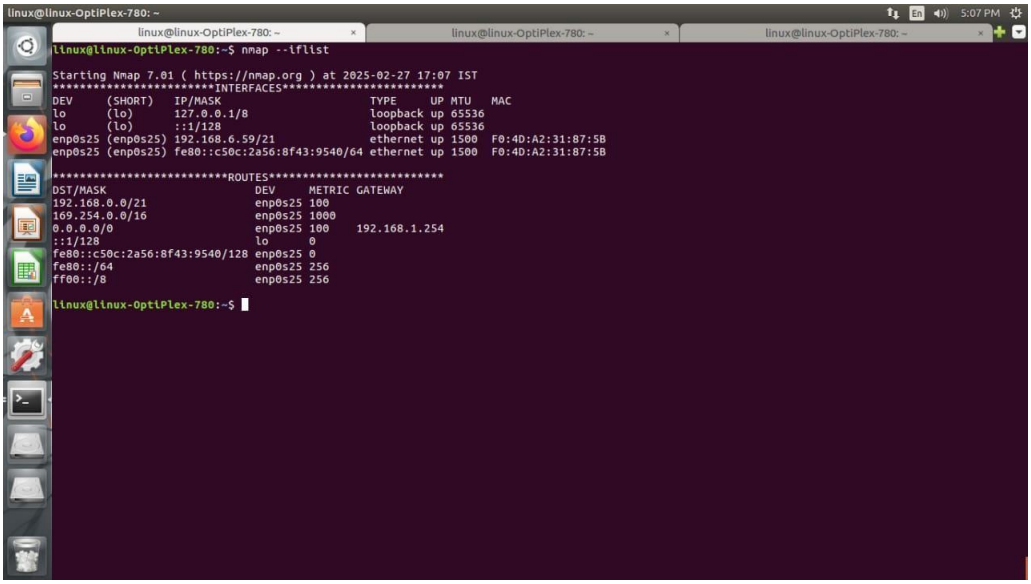
```
linux@linux-OptiPlex-780: ~
linux@linux-OptiPlex-780:~$ nmap -sV 192.168.1.254

Starting Nmap 7.01 ( https://nmap.org ) at 2025-02-27 17:04 IST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.65% done
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 55.56% done; ETC: 17:05 (0:00:25 remaining)
Nmap scan report for 192.168.1.254
Host is up (0.00049s latency).
Not shown: 991 filtered ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         Linksys WRT45G modified dropbear sshd (protocol 2.0)
25/tcp   open  smtp
53/tcp   open  domain?
443/tcp  open  ssl/https   xxxx
3128/tcp open  squid-http?
4443/tcp open  ssl/pharos?
4444/tcp open  ssl/krb524?
8090/tcp open  ssl/unknown
8443/tcp open  https-alt?
6 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/c
gi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.01%I=7%D=2/27%Time=67C04DCC%P=i686-pc-linux-gnu%r(NULL,1
SF:8,"220\x20Sophos\x20ESMTP\x20ready\r\n")%r(Hello,44,"220\x20Sophos\x20E
SF:SMTP\x20ready\r\n501\x20Syntactically\x20invalid\x20EHLO\x20argument\(s
SF:\)\r\n")%r(Help,76,"220\x20Sophos\x20ESMTP\x20ready\r\n214-Commands\x20
SF:supported:\r\n214\x20AUTH\x20STARTTLS\x20HELO\x20EHLO\x20MAIL\x20RCPT\x
SF:20DATA\x20BDAT\x20NOOP\x20QUIT\x20RSET\x20HELP\r\n")%r(GenericLines,4C,
SF:"220\x20Sophos\x20ESMTP\x20ready\r\n500\x20unrecognized\x20command\r\n5
SF:00\x20unrecognized\x20command\r\n")%r(GetRequest,4C,"220\x20Sophos\x20E
SF:SMTP\x20ready\r\n500\x20unrecognized\x20command\r\n500\x20unrecognized\
SF:x20command\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.01%T=SSL%I=7%D=2/27%Time=67C04DD1%P=i686-pc-linux-gnu%r
SF:(GetRequest,EB9,"HTTP/1\.1\x20200\x20OK\r\nDate:\x20Thu,\x2027\x20Feb\x
SF:202025\x2012:41:31\x20GMT\r\nServer:\x20xxxx\r\nX-Frame-Options:\x20SAM
SF:EORIGIN\r\nStrict-Transport-Security:\x20max-age=31536000\r\nX-Content-
SF:Type-Options:\x20nosniff\r\nReferrer-Policy:\x20strict-origin-when-cros
SF:s-origin\r\nContent-Security-Policy:\x20default-src\x20https:\x20data:\
SF:x20ws:\x20wss:\x20blob:\x20'unsafe-inline'\x20'unsafe-eval';\x20worker-
SF:src\x20'self'\x20blob:;\x20frame-ancestors\x20'self';\x20object-src\x20
```

3) nmap -sP 10.0.0.0/8

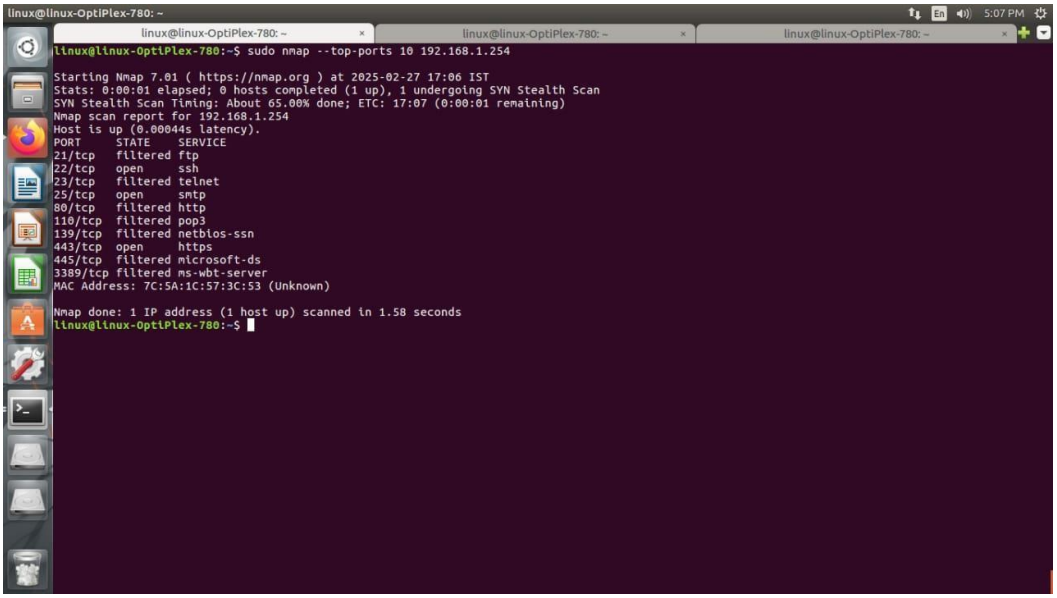


```
linux@linux-OptiPlex-780: ~
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
linux@linux-OptiPlex-780:~$ nmap -sP 10.0.0.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-02-27 16:53 IST
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.14 seconds
linux@linux-OptiPlex-780:~$ nmap -sP 192.168.1.10

Starting Nmap 7.01 ( https://nmap.org ) at 2025-02-27 16:57 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 3.00 seconds
linux@linux-OptiPlex-780:~$ nmap -sP 192.168.1.10
```

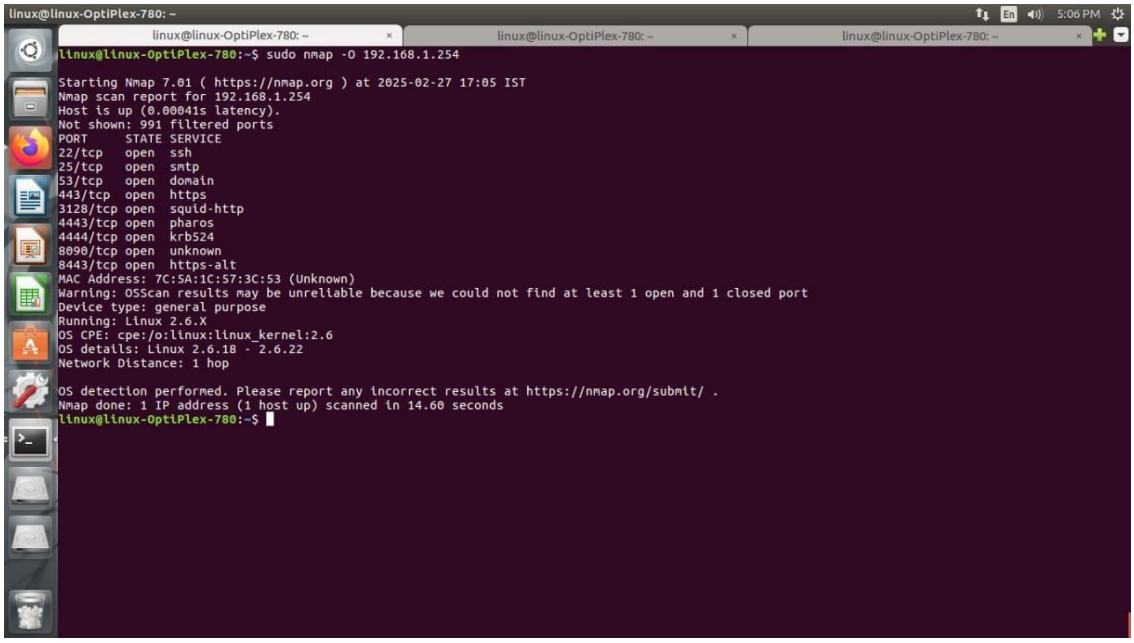
4) nmap --iflist



5) sudo nmap –top-ports 10 192.168.1.254

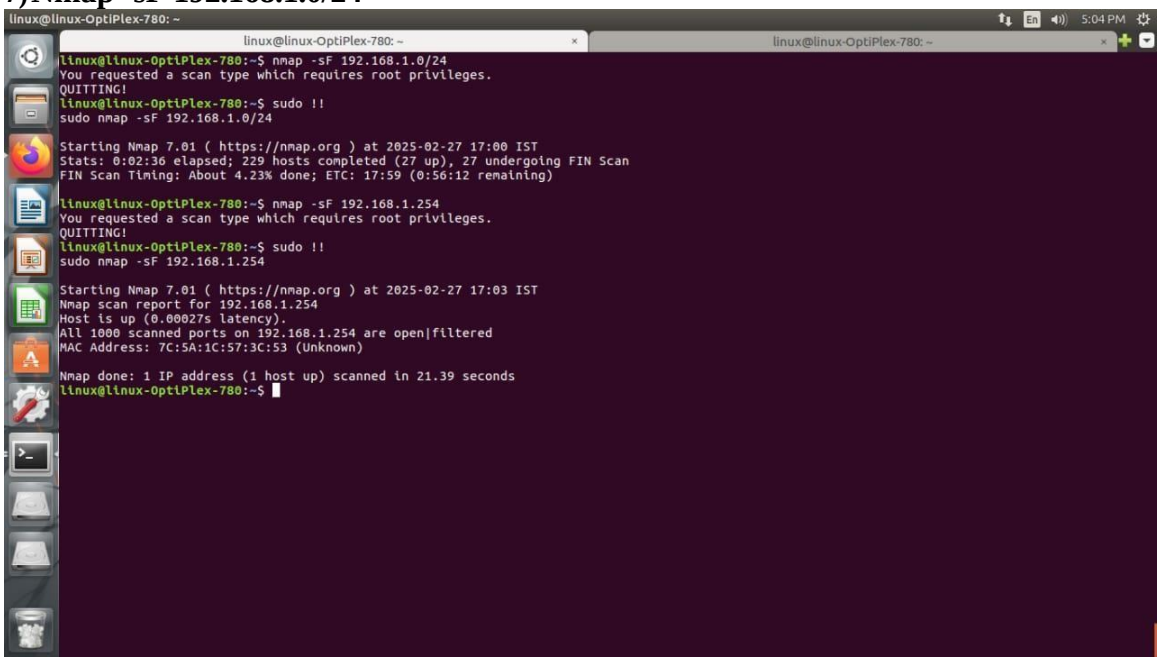


6) sudo nmap -o 192.168.1.254



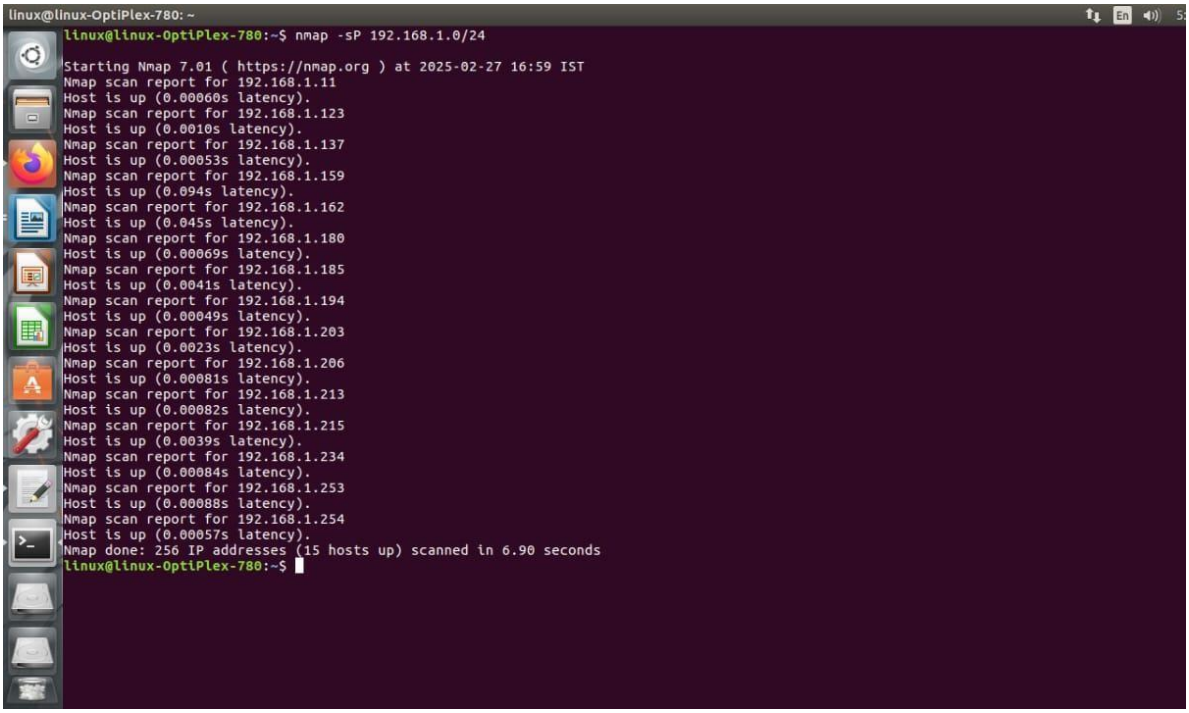
```
linux@linux-OptiPlex-780: ~
linux@linux-OptiPlex-780:~$ sudo nmap -O 192.168.1.254

Starting Nmap 7.01 ( https://nmap.org ) at 2025-02-27 17:05 IST
Nmap scan report for 192.168.1.254
Host is up (0.00041s latency).
Not shown: 991 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
53/tcp   open  domain
443/tcp  open  https
3128/tcp open  squid-http
4443/tcp open  pharos
4444/tcp open  krb524
8090/tcp open  unknown
8443/tcp open  https-alt
MAC Address: 7C:5A:1C:57:3C:53 (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: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.22
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.60 seconds
linux@linux-OptiPlex-780:~$
```

7) Nmap -sF 192.168.1.0/24



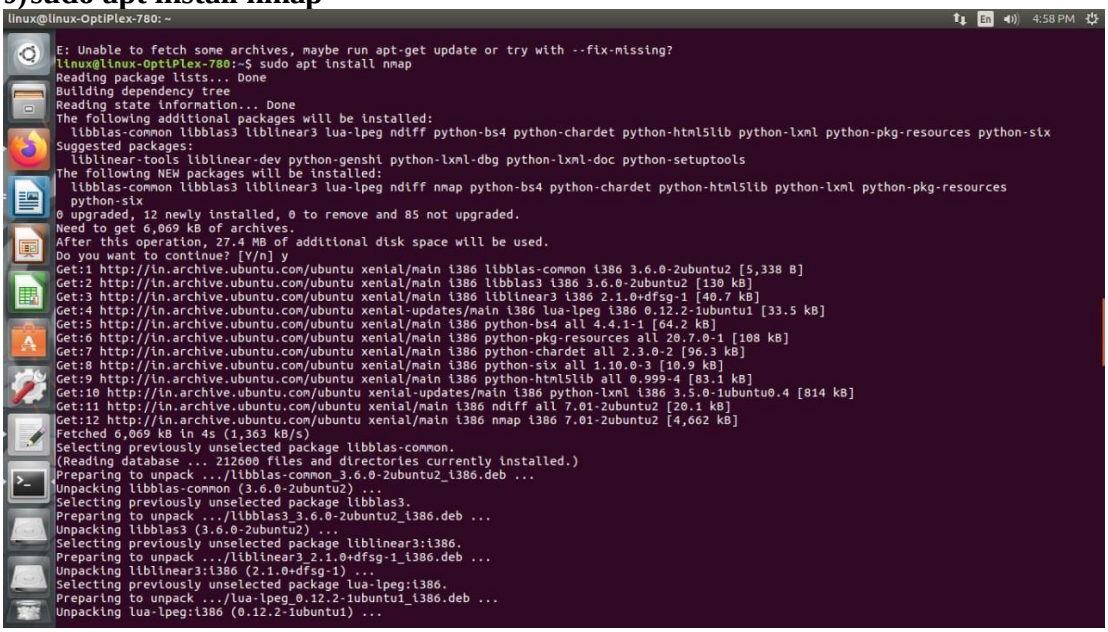
```
linux@linux-OptiPlex-780: ~
linux@linux-OptiPlex-780:~$ nmap -sF 192.168.1.0/24
You requested a scan type which requires root privileges.
QUITTING!
linux@linux-OptiPlex-780:~$ sudo !!
sudo nmap -sF 192.168.1.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-02-27 17:00 IST
Stats: 0:02:36 elapsed; 229 hosts completed (27 up), 27 undergoing FIN Scan
FIN Scan Timing: About 4.23% done; ETC: 17:59 (0:56:12 remaining)

linux@linux-OptiPlex-780:~$ nmap -sF 192.168.1.254
You requested a scan type which requires root privileges.
QUITTING!
linux@linux-OptiPlex-780:~$ sudo !!
sudo nmap -sF 192.168.1.254

Starting Nmap 7.01 ( https://nmap.org ) at 2025-02-27 17:03 IST
Nmap scan report for 192.168.1.254
Host is up (0.00027s latency).
All 1000 scanned ports on 192.168.1.254 are open|filtered
MAC Address: 7C:5A:1C:57:3C:53 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds
linux@linux-OptiPlex-780:~$
```

8) Nmap - -sP 192.168.1.0/24



```
linux@linux-OptiPlex-780: ~
linux@linux-OptiPlex-780:~$ nmap -sP 192.168.1.0/24

Starting Nmap 7.01 ( https://nmap.org ) at 2025-02-27 16:59 IST
Nmap scan report for 192.168.1.11
Host is up (0.00060s latency).
Nmap scan report for 192.168.1.123
Host is up (0.0010s latency).
Nmap scan report for 192.168.1.137
Host is up (0.00053s latency).
Nmap scan report for 192.168.1.159
Host is up (0.094s latency).
Nmap scan report for 192.168.1.162
Host is up (0.045s latency).
Nmap scan report for 192.168.1.180
Host is up (0.00069s latency).
Nmap scan report for 192.168.1.185
Host is up (0.0041s latency).
Nmap scan report for 192.168.1.194
Host is up (0.00049s latency).
Nmap scan report for 192.168.1.203
Host is up (0.0023s latency).
Nmap scan report for 192.168.1.206
Host is up (0.00081s latency).
Nmap scan report for 192.168.1.213
Host is up (0.00082s latency).
Nmap scan report for 192.168.1.215
Host is up (0.0039s latency).
Nmap scan report for 192.168.1.234
Host is up (0.00084s latency).
Nmap scan report for 192.168.1.253
Host is up (0.00088s latency).
Nmap scan report for 192.168.1.254
Host is up (0.00057s latency).
Nmap done: 256 IP addresses (15 hosts up) scanned in 6.90 seconds
linux@linux-OptiPlex-780:~$
```

9) sudo apt install nmap



```
linux@linux-OptiPlex-780: ~
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
linux@linux-OptiPlex-780:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libblas-common libblas3 liblinear3 lua-lpeg ndiff python-bs4 python-chardet python-html5lib python-lxml python-pkg-resources python-six
Suggested packages:
  liblinear-tools liblinear-dev python-genshi python-lxml-dbg python-lxml-doc python-setuptools
The following NEW packages will be installed:
  libblas-common libblas3 liblinear3 lua-lpeg ndiff nmap python-bs4 python-chardet python-html5lib python-lxml python-pkg-resources
  python-six
0 upgraded, 12 newly installed, 0 to remove and 85 not upgraded.
Need to get 6,069 kB of archives.
After this operation, 27.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu xenial/main i386 libblas-common i386 3.6.0-2ubuntu2 [5,338 B]
Get:2 http://in.archive.ubuntu.com/ubuntu xenial/main i386 libblas3 i386 3.6.0-2ubuntu2 [130 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu xenial/main i386 liblinear3 i386 2.1.0+dfsg-1 [40.7 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu xenial-updates/main i386 lua-lpeg i386 0.12.2-1ubuntu1 [33.5 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu xenial/main i386 python-bs4 all 4.4.1-1 [64.2 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu xenial/main i386 python-pkg-resources all 20.7.0-1 [108 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu xenial/main i386 python-chardet all 2.3.0-2 [96.3 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu xenial/main i386 python-six all 1.10.0-3 [10.9 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu xenial/main i386 python-html5lib all 0.999-4 [83.1 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu xenial-updates/main i386 python-lxml i386 3.5.0-1ubuntu0.4 [814 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu xenial/main i386 ndiff all 7.01-2ubuntu2 [20.1 kB]
Get:12 http://in.archive.ubuntu.com/ubuntu xenial/main i386 nmap i386 7.01-2ubuntu2 [4,662 kB]
Fetched 6,069 kB in 4s (1,363 kB/s)
Selecting previously unselected package libblas-common.
(Reading database ... 212600 files and directories currently installed.)
Preparing to unpack .../libblas-common_3.6.0-2ubuntu2_i386.deb ...
Unpacking libblas-common (3.6.0-2ubuntu2) ...
Selecting previously unselected package libblas3.
Preparing to unpack .../libblas3_3.6.0-2ubuntu2_i386.deb ...
Unpacking libblas3 (3.6.0-2ubuntu2) ...
Selecting previously unselected package liblinear3:i386.
Preparing to unpack .../liblinear3_2.1.0+dfsg-1_i386.deb ...
Unpacking liblinear3:i386 (2.1.0+dfsg-1) ...
Selecting previously unselected package lua-lpeg:i386.
Preparing to unpack .../lua-lpeg_0.12.2-1ubuntu1_i386.deb ...
Unpacking lua-lpeg:i386 (0.12.2-1ubuntu1) ...
```

B.2 Commands / tools used with syntax:

.

1) **nmap -p 1-10 192.168.1.254**

2) **nmap -sV 192.168.1.254**

3) **nmap -sP 10.0.0.0/8**
4) **nmap –iflist**
5) **sudo nmap –top-ports 10 192.168.1.254**
6) **sudo nmap -o 192.168.1.254**
7) **Nmap -sF 192.168.1.0/24**
8) **Nmap - -sP 192.168.1.0/24**
9) **sudo apt install nmap**

B.3 Question of Curiosity:

What are the ethical considerations when using Nmap for scanning networks?

Exp 7

Date: / /
Page No.:

Q.1 What are the ethical considerations when using Nmap for scanning networks?

→ when using Nmap, follow these ethical, Hyddie-

1) Get Permission – Always obtain authentication from the network owner before scanning

2) Privacy :- Avoid collecting or exposing sensitive user data without permission.

3) Minimize Disruption – Use non intrusive scans to prevent network slowdowns or crashes

4) Responsible use :- Do not exploit discovered vulnerabilities for malicious purpose.

5) Compliance – follow organizational policily & legal regulations like GDPR, HIPAP

6) Logging & Disclousere – Keep reload of scan & reports finding responsibly to the concerned parties

Q3 What is purpose of OS finger printing in network scanning?

→ OS finger printing in network scanning is used to identify the operating system running on a target device. Its purpose include

1) Security Assessment – Helps detect vulnerabilities specific to an OS

2) Network inventory – Identifies devices for network management & auditing.

3) Penetration Testing – Assists ethical hacker in simulating attacks based on OS-specific weakness

4) Incident respone – Helps security team analyze & respond to potential threats

Supervisor's Sign.:

2.What precautions should be taken to avoid detection when using Nmap for network scanning?

To avoid detection when using Nmap for network scanning, take these precautions:

Use Stealth Scanning – Opt for SYN scan (-sS) instead of full connect scan (-sT).

Slow Down Scans – Use --scan-delay and --max-rate to avoid triggering IDS/IPS.

Fragment Packets – Use -f to split packets and evade detection.

Use Decoys – Use -D <decoy1,decoy2> to mask your real IP.

Spoof Source IP – Use -S <spoofed IP> to disguise your real IP.

Scan Random Ports – Avoid predictable patterns with -r or --randomize-hosts.

Use Legitimate User-Agent – Modify headers in version scans (--script-args).

Encrypt Traffic – Use --data-length to obfuscate scan signatures.

Check Firewall Rules – Use -Pn to avoid being blocked by ping restrictions.

Run as Root/Admin – Some stealth features require elevated privileges.

4. ow does an Xmas scan work, and what does it detect?

An Xmas scan (-sX in Nmap) is a stealthy port scanning technique that sends TCP packets with the FIN, PSH, and URG flags set, making the packet appear "lit up" like a Christmas tree.

How It Works:

If a port is closed, the target responds with an RST (Reset) packet.

If a port is open or filtered, there is no response (as per RFC 793 behavior).

This scan works best on systems following the RFC-compliant TCP/IP stack, like older UNIX-based systems. However, Windows devices do not respond predictably to this scan, making it ineffective against them.

What It Detects:

Closed ports (which send an RST response).

Open or filtered ports (which remain silent).

Firewall rules that might block responses.

5. What is the difference between TCP and UDP port scanning?

Date : / /
Page No. :

Q.5

TCP Port Scanning	UDP Port scanning
1) Protocol use is TCP connection oriented	1) Protocol used in UDP. connection.
2) Uses 3-way handshake	2) No handshake; just sends packet
3) More reliable (ensure packet delivery)	3) less reliable (packet may be droppped)
4) Slower due to hand-shake	faster but may be affected by packet loss
5) Easier to detect	Harder to detect
6) Use for penetration sliding	Used for finding open UDP ~~services~~ services

6. How can Nmap be used to detect firewalls and filtering devices?

Nmap can detect firewalls and filtering devices using various scanning techniques and options.

Methods to Detect Firewalls and Filtering Devices:

Ping Scan (-Pn)

If a host does not respond to a ping request, it may be behind a firewall that blocks ICMP.

TCP SYN Scan (-sS)

If all ports show as filtered (no response), a firewall is likely blocking traffic.

ACK Scan (-sA)

Used to detect stateless firewalls by sending TCP ACK packets. If all ports are filtered, a firewall is blocking the packets.

Xmas Scan (-sX) and FIN Scan (-sF)

Can identify firewalls that follow RFC-compliant behavior. If there's no response, the port is open/filtered. If an RST is received, the port is closed.

Firewalk Technique

Uses TTL (Time-To-Live) values to map out firewall rules by sending packets with incremented TTL values.

Version Detection (-sV)

Helps identify firewall brands and versions based on the responses received.

Aggressive Scan (-A)

Combines OS detection, version detection, script scanning, and traceroute to find firewall devices.

B.4 Conclusion:

(Write appropriate conclusion.)

Nmap is a powerful network scanning tool used for security auditing and reconnaissance. It can identify open ports (-sS for TCP, -sU for UDP), helping detect vulnerable services. OS fingerprinting (-O) determines the target system's operating system, aiding in security assessments. Ping scans (-sn) detect live hosts without scanning ports, useful for network mapping. The Xmas scan (-sX) helps find open/filtered ports by analyzing packet responses. Firewall detection is possible using ACK scans (-sA) and analyzing response behavior. Service and version detection (-sV) helps in vulnerability assessment by identifying running services. These scans help in penetration testing, security analysis, and network troubleshooting.