PRACTICAL: 4

AIM:

Port scanning is a method for determining open ports and services available on a network or a host. It involves connecting with TCP and UDP ports on the system once you find the IP addresses of a target network or host using the Footprinting technique. You have to map the network of this targeted organization. Nmap (Network Mapper) is a powerful, flexible, open- source, easy-to-use port scanning tool available for both Linux and Windows-based operating systems. Study practical approaches to implementing scanning and enumeration techniques using Nmap.

THEORY:

Nmap ("Network Mapper") is a free and open-source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

Nmap is ...

Flexible: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many port scanning mechanisms (both TCP & UDP), OS detection, version detection, ping sweeps, and more. See the documentation page.

Powerful: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.

Portable: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.

Easy: While Nmap offers a rich set of advanced features for power users, we can start out as simply as "nmap -v -A targethost". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.

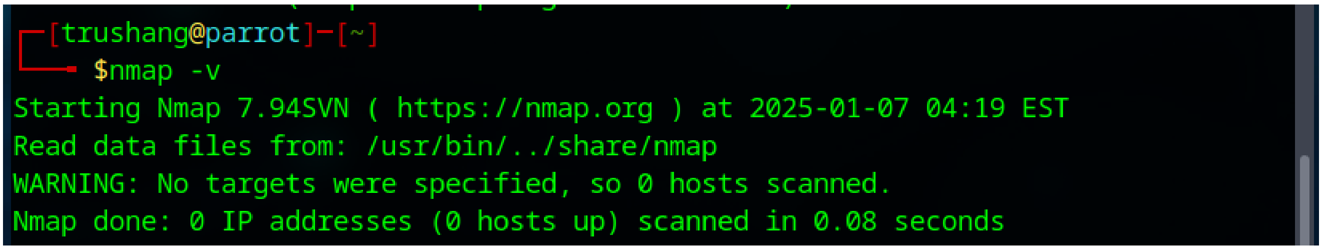
Free: The primary goals of the Nmap Project are to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for free download, and also comes with full source code that you may modify and redistribute under the terms of the license.

Well Documented: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages here.

CODE:

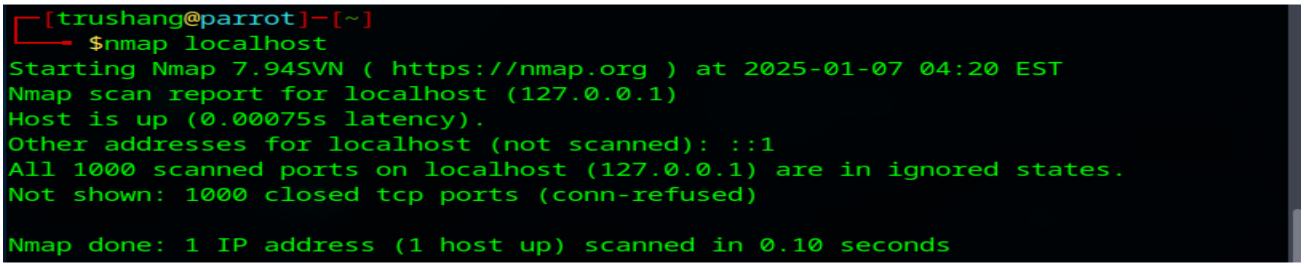
- nmap -v
- nmap localhost
- nmap 172.16.3.129 --disable-arp-ping
- nmap -v 172.16.3.129 --disable-arp-ping
- nmap -sA 172.16.3.129
- nmap -Pn 172.16.3.129
- nmap -F 172.16.3.129
- nmap –iflist
- nmap -o 172.16.3.129
- nmap -A 172.16.3.129
- nmap 172.16.3.1-255
- nmap charusat.edu.in
- nmap -sS 172.16.3.129
- nmap 172.16.3.129/24 --disable-arp-ping

OUTPUT:



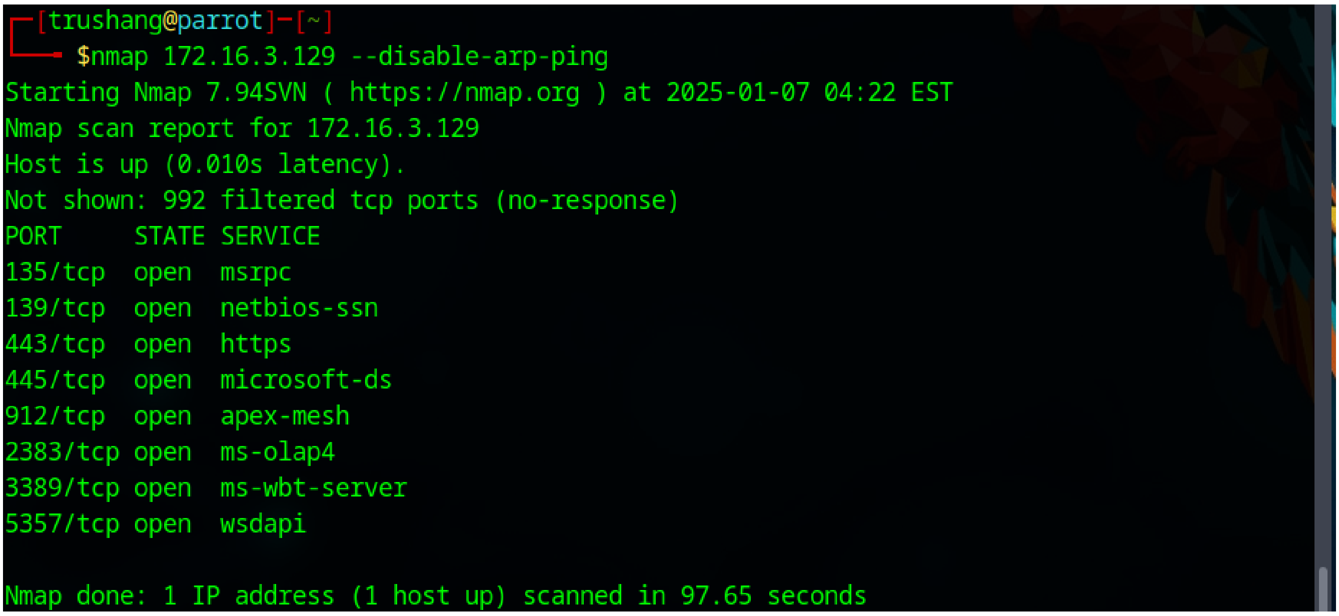
```
┌─[trushang@parrot]─[~]
└──╼ $nmap -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:19 EST
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.08 seconds
```

Figure 1:Check the version of Nmap



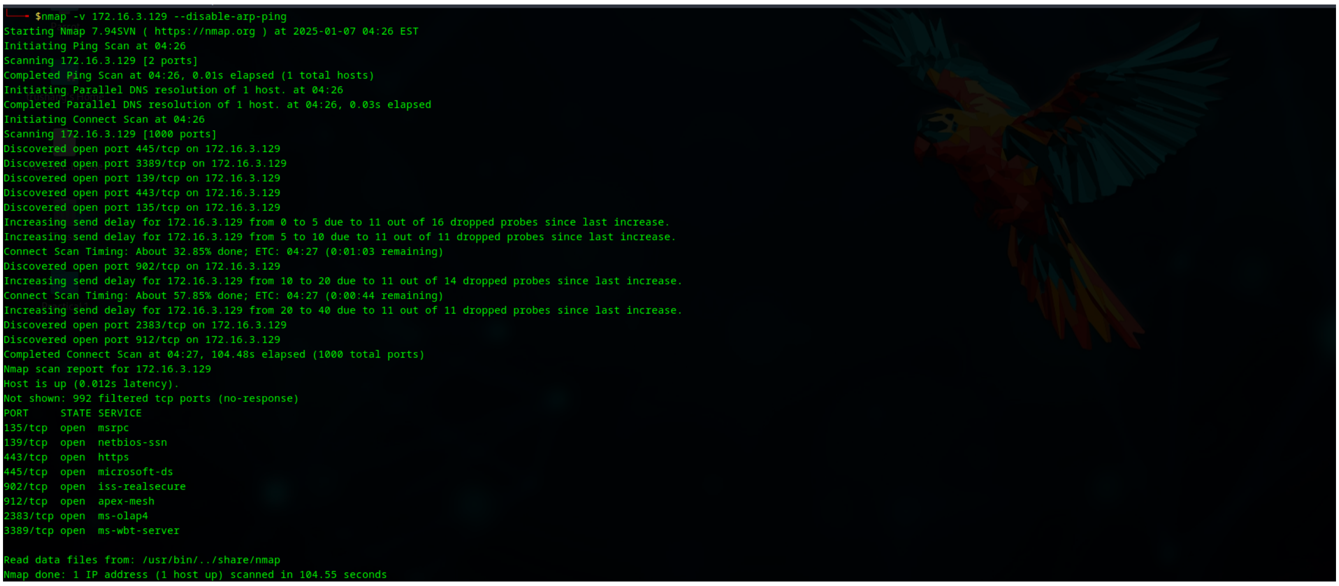
```
┌─[trushang@parrot]─[~]
└──╼ $nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:20 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00075s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Figure 2:Scan using Nmap



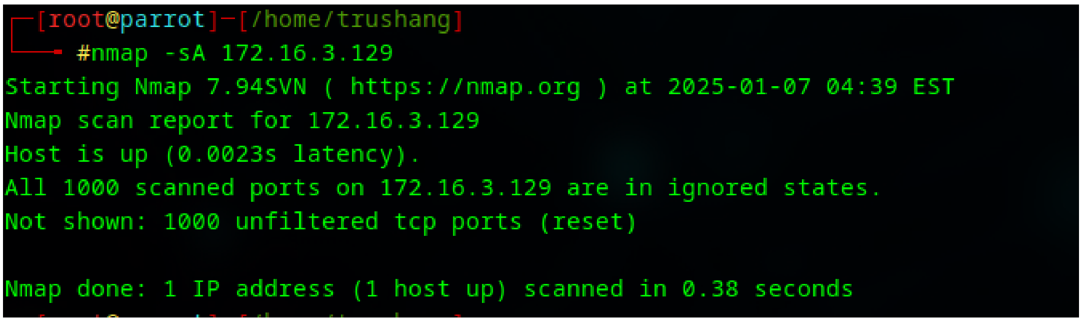
```
┌─[trushang@parrot]─[~]
└──╼ $nmap 172.16.3.129 --disable-arp-ping
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:22 EST
Nmap scan report for 172.16.3.129
Host is up (0.010s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
912/tcp  open  apex-mesh
2383/tcp open  ms-olap4
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 97.65 seconds
```

Figure 3:Scan using ip address



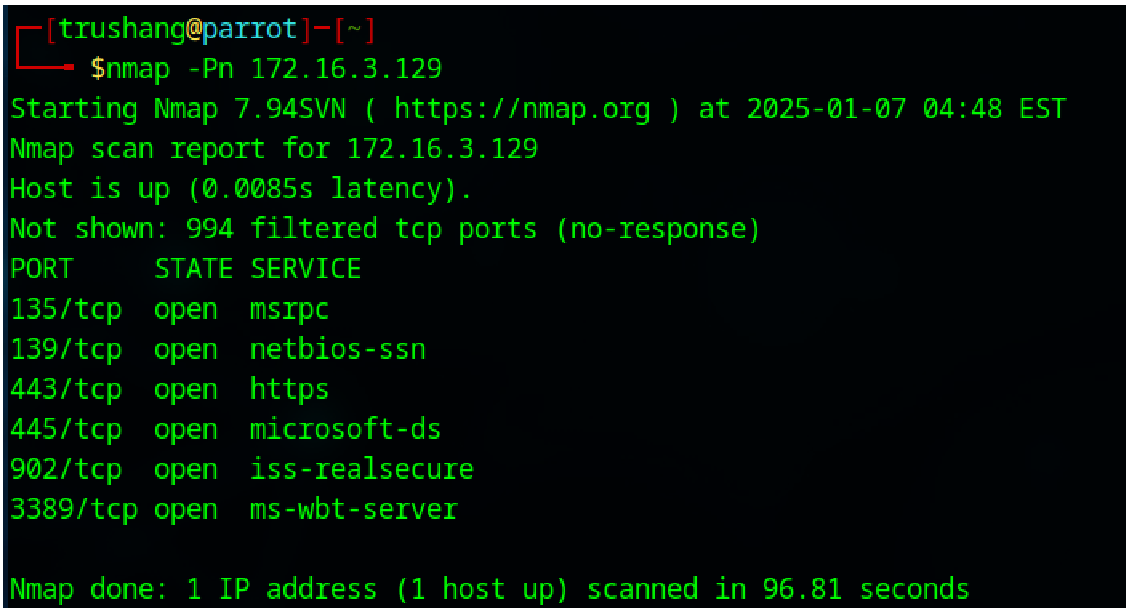
```
└──╼ $nmap -v 172.16.3.129 --disable-arp-ping
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:26 EST
Initiating Ping Scan at 04:26
Scanning 172.16.3.129 [2 ports]
Completed Ping Scan at 04:26, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:26
Completed Parallel DNS resolution of 1 host. at 04:26, 0.03s elapsed
Initiating Connect Scan at 04:26
Scanning 172.16.3.129 [1000 ports]
Discovered open port 445/tcp on 172.16.3.129
Discovered open port 3389/tcp on 172.16.3.129
Discovered open port 139/tcp on 172.16.3.129
Discovered open port 443/tcp on 172.16.3.129
Discovered open port 135/tcp on 172.16.3.129
Increasing send delay for 172.16.3.129 from 0 to 5 due to 11 out of 16 dropped probes since last increase.
Increasing send delay for 172.16.3.129 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Connect Scan Timing: About 32.85% done; ETC: 04:27 (0:01:03 remaining)
Discovered open port 902/tcp on 172.16.3.129
Increasing send delay for 172.16.3.129 from 10 to 20 due to 11 out of 14 dropped probes since last increase.
Connect Scan Timing: About 57.85% done; ETC: 04:27 (0:00:44 remaining)
Increasing send delay for 172.16.3.129 from 20 to 40 due to 11 out of 11 dropped probes since last increase.
Discovered open port 2383/tcp on 172.16.3.129
Discovered open port 912/tcp on 172.16.3.129
Completed Connect Scan at 04:27, 104.48s elapsed (1000 total ports)
Nmap scan report for 172.16.3.129
Host is up (0.012s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
2383/tcp open  ms-olap4
3389/tcp open  ms-wbt-server

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 104.55 seconds
```

Figure 4:Get a more detailed output of the scan, such as status updates on scanning the host and ports



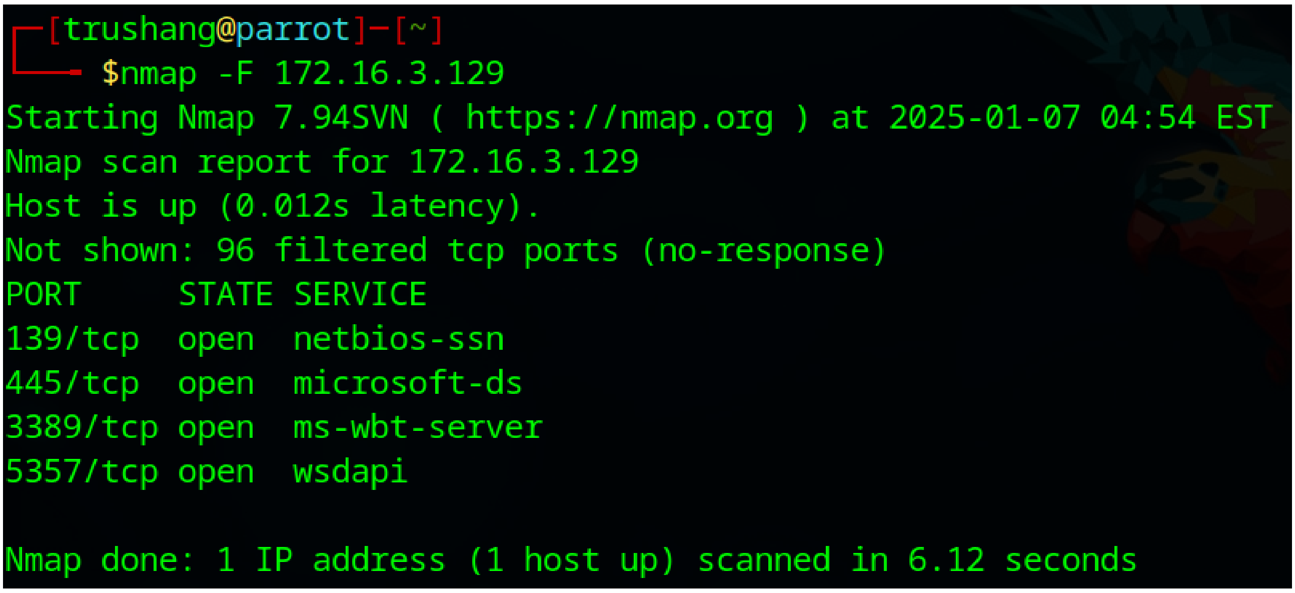
```
┌─[root@parrot]─[/home/trushang]
└──╼ #nmap -sA 172.16.3.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:39 EST
Nmap scan report for 172.16.3.129
Host is up (0.0023s latency).
All 1000 scanned ports on 172.16.3.129 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Figure 5:TCP ACK port scan



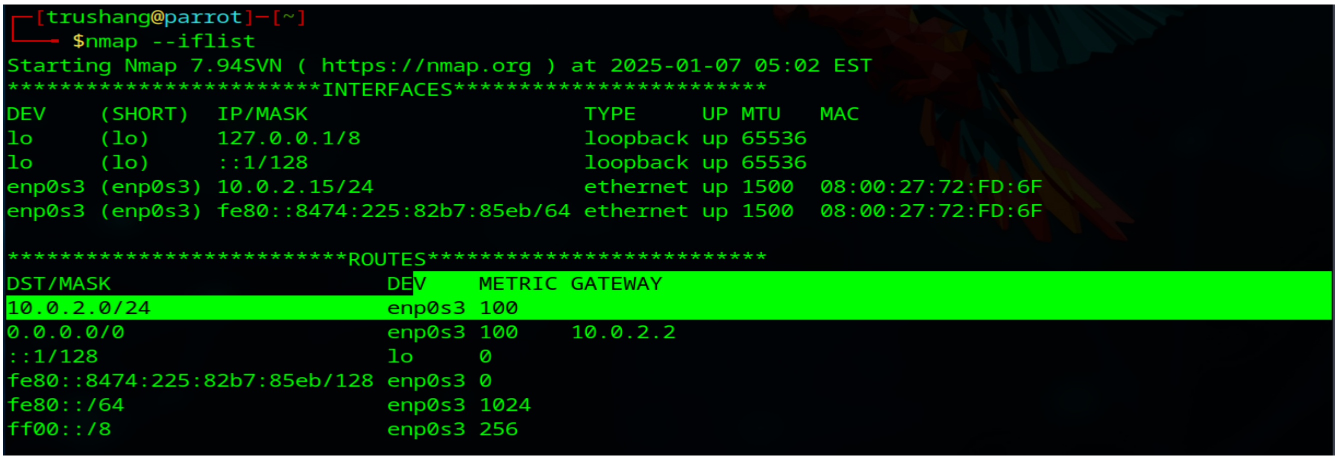
```
┌─[trushang@parrot]─[~]
└──╼ $nmap -Pn 172.16.3.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:48 EST
Nmap scan report for 172.16.3.129
Host is up (0.0085s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
902/tcp  open  iss-realsecure
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 96.81 seconds
```

Figure 6:Scan a host to detect firewall



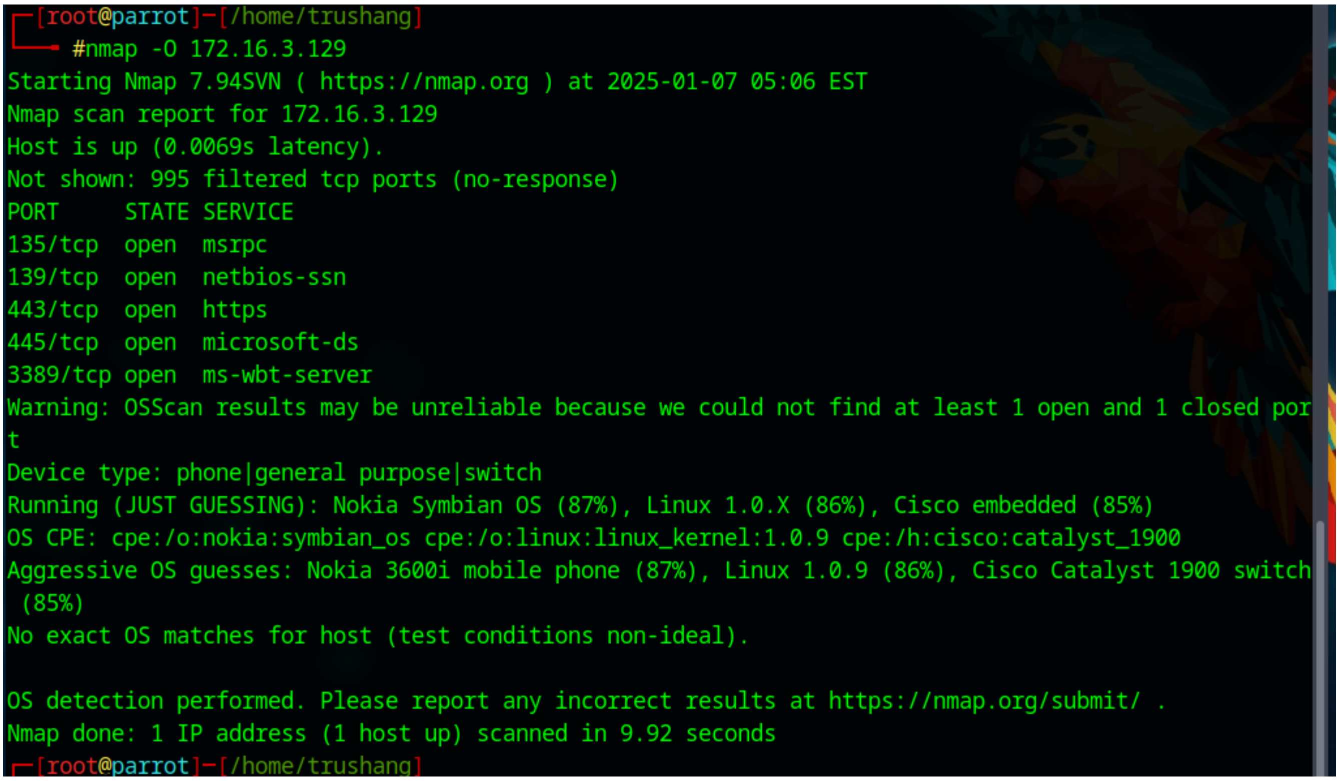
```
┌─[trushang@parrot]─[~]
└──╼ $nmap -F 172.16.3.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 04:54 EST
Nmap scan report for 172.16.3.129
Host is up (0.012s latency).
Not shown: 96 filtered tcp ports (no-response)
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 6.12 seconds
```

Figure 7:Perform fast scan



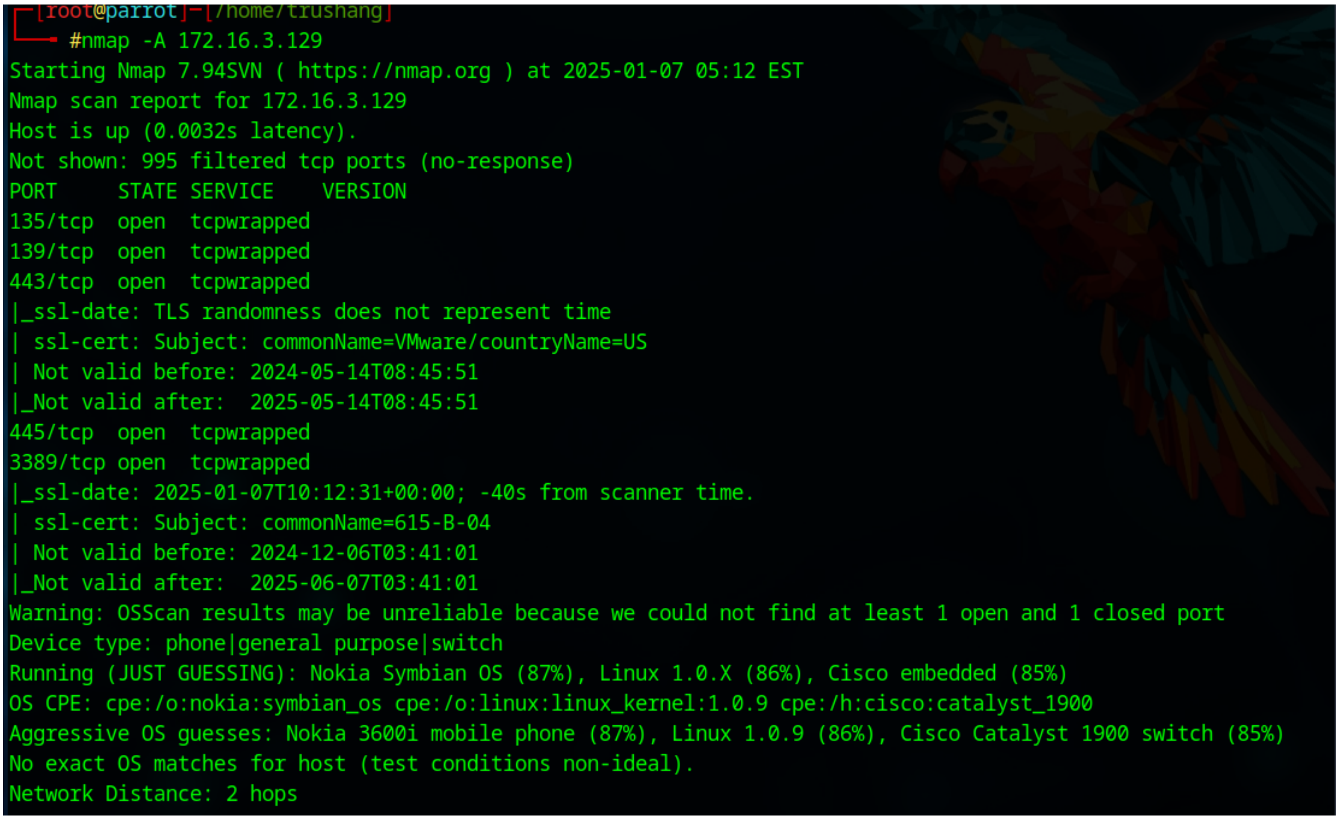
```
┌─[trushang@parrot]─[~]
└──╼ $nmap --iflist
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 05:02 EST
************************INTERFACES************************
DEV     (SHORT)   IP/MASK                        TYPE     UP MTU   MAC
lo      (lo)      127.0.0.1/8                    loopback up 65536
lo      (lo)      ::1/128                        loopback up 65536
enp0s3 (enp0s3) 10.0.2.15/24                   ethernet up 1500  08:00:27:72:FD:6F
enp0s3 (enp0s3) fe80::8474:225:82b7:85eb/64 ethernet up 1500  08:00:27:72:FD:6F

**************************ROUTES**************************
DST/MASK                      DEV    METRIC GATEWAY
10.0.2.0/24                   enp0s3 100
0.0.0.0/0                     enp0s3 100    10.0.2.2
::1/128                       lo     0
fe80::8474:225:82b7:85eb/128 enp0s3 0
fe80::/64                     enp0s3 1024
ff00::/8                      enp0s3 256
```

Figure 8:Print Host interface and route



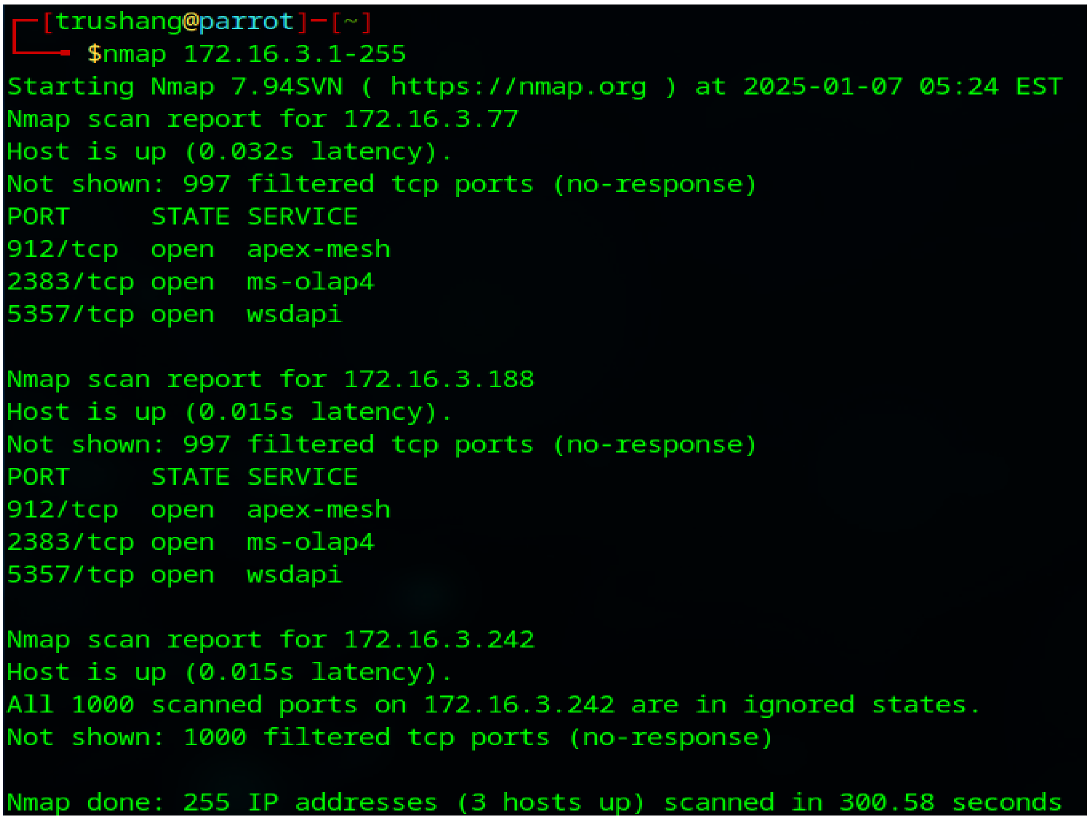
```
┌─[root@parrot]─[/home/trushang]
└──╼ #nmap -O 172.16.3.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 05:06 EST
Nmap scan report for 172.16.3.129
Host is up (0.0069s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed por
t
Device type: phone|general purpose|switch
Running (JUST GUESSING): Nokia Symbian OS (87%), Linux 1.0.X (86%), Cisco embedded (85%)
OS CPE: cpe:/o:nokia:symbian_os cpe:/o:linux:linux_kernel:1.0.9 cpe:/h:cisco:catalyst_1900
Aggressive OS guesses: Nokia 3600i mobile phone (87%), Linux 1.0.9 (86%), Cisco Catalyst 1900 switch
 (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 9.92 seconds
┌─[root@parrot]─[/home/trushang]
```

Figure 9:Remote OS detection using TCP/IP stack fingerprinting



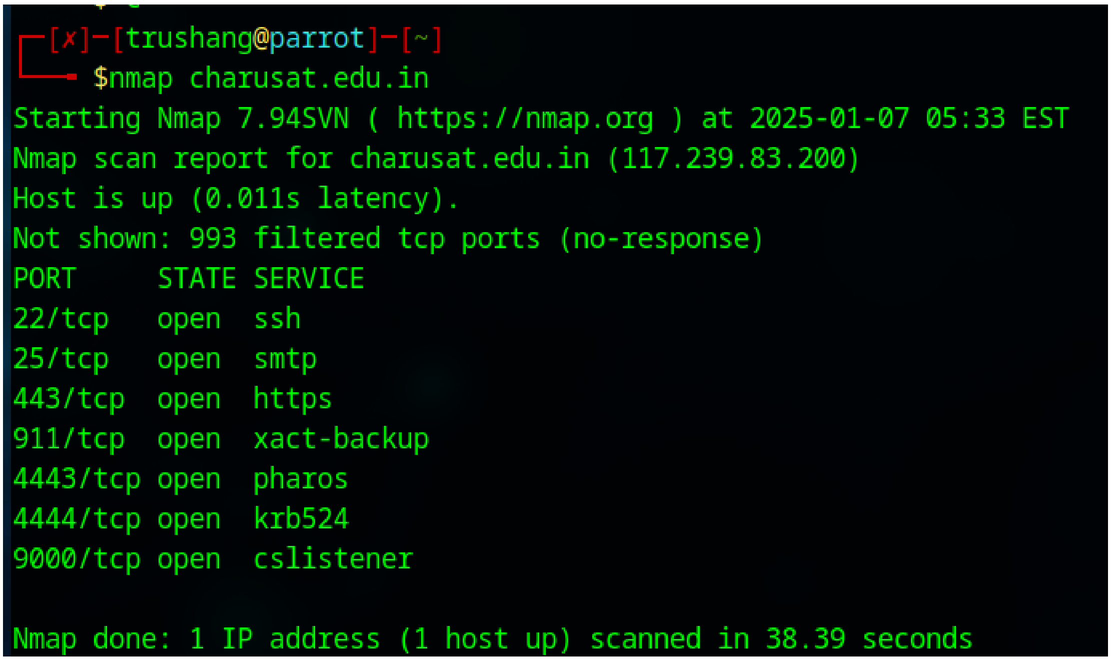
```
┌─[root@parrot]─[/home/trushang]
└──╼ #nmap -A 172.16.3.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 05:12 EST
Nmap scan report for 172.16.3.129
Host is up (0.0032s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
135/tcp  open  tcpwrapped
139/tcp  open  tcpwrapped
443/tcp  open  tcpwrapped
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=VMware/countryName=US
| Not valid before: 2024-05-14T08:45:51
|_Not valid after:  2025-05-14T08:45:51
445/tcp  open  tcpwrapped
3389/tcp open  tcpwrapped
|_ssl-date: 2025-01-07T10:12:31+00:00; -40s from scanner time.
| ssl-cert: Subject: commonName=615-B-04
| Not valid before: 2024-12-06T03:41:01
|_Not valid after:  2025-06-07T03:41:01
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose|switch
Running (JUST GUESSING): Nokia Symbian OS (87%), Linux 1.0.X (86%), Cisco embedded (85%)
OS CPE: cpe:/o:nokia:symbian_os cpe:/o:linux:linux_kernel:1.0.9 cpe:/h:cisco:catalyst_1900
Aggressive OS guesses: Nokia 3600i mobile phone (87%), Linux 1.0.9 (86%), Cisco Catalyst 1900 switch (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

Figure 10: Enables OS detection, version detection, script scanning, and traceroute



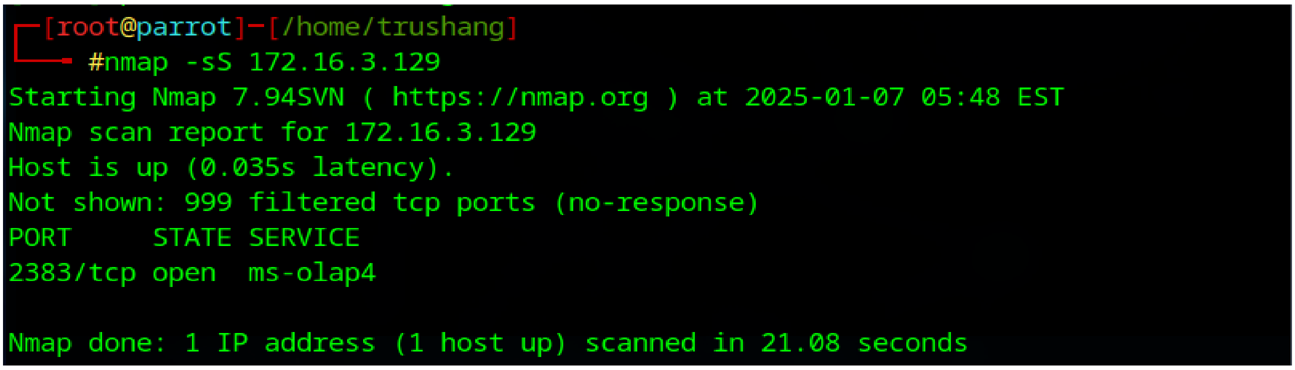
```
┌─[trushang@parrot]─[~]
└──╼ $nmap 172.16.3.1-255
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 05:24 EST
Nmap scan report for 172.16.3.77
Host is up (0.032s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
912/tcp  open  apex-mesh
2383/tcp open  ms-olap4
5357/tcp open  wsdapi

Nmap scan report for 172.16.3.188
Host is up (0.015s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
912/tcp  open  apex-mesh
2383/tcp open  ms-olap4
5357/tcp open  wsdapi

Nmap scan report for 172.16.3.242
Host is up (0.015s latency).
All 1000 scanned ports on 172.16.3.242 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 255 IP addresses (3 hosts up) scanned in 300.58 seconds
```

Figure 11:Scan a range of Ip range



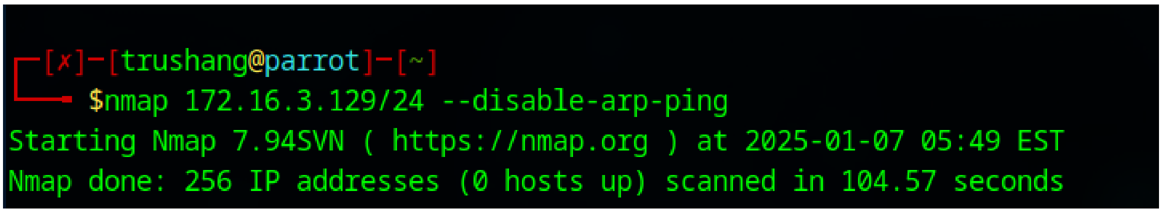
```
┌─[✗]─[trushang@parrot]─[~]
└──╼ $nmap charusat.edu.in
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 05:33 EST
Nmap scan report for charusat.edu.in (117.239.83.200)
Host is up (0.011s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
443/tcp  open  https
911/tcp  open  xact-backup
4443/tcp open  pharos
4444/tcp open  krb524
9000/tcp open  cslistener

Nmap done: 1 IP address (1 host up) scanned in 38.39 seconds
```

Figure 12:Scan a domain



```
┌─[root@parrot]─[/home/trushang]
└──╼ #nmap -sS 172.16.3.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 05:48 EST
Nmap scan report for 172.16.3.129
Host is up (0.035s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
2383/tcp open  ms-olap4

Nmap done: 1 IP address (1 host up) scanned in 21.08 seconds
```

Figure 13:TCP SYN port scan (Default)



```
┌─[✗]─[trushang@parrot]─[~]
└──╼ $nmap 172.16.3.129/24 --disable-arp-ping
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-07 05:49 EST
Nmap done: 256 IP addresses (0 hosts up) scanned in 104.57 seconds
```

Figure 14:Scan using CIDR notation

LATEST APPLICATIONS:

- Vulnerability Scanning & Exploitation
- Cloud Security
- IoT Device Discovery and Security
- Automated Network Discovery and Asset Management
- Remote Monitoring and Incident Response
- Automating Network Scans with APIs

LEARNING OUTCOME:

In this practical, we learn that port scanning with Nmap is used to identify open ports and services on a network. By combining foot printing and enumeration techniques, Nmap helps security professionals map networks and assess vulnerabilities.

REFERENCES:

1. YouTube: https://www.youtube.com/watch?v=fp1042XK4A8
2. Nmap: https://nmap.org/