

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:

Port Scanning:

- Port scanning involves systematically sending requests to a target system's network ports to:
 - **Identify Open Ports:** Ports that accept incoming connections and are actively running services.
 - **Determine Closed Ports:** Ports that are not actively listening for connections.
 - **Detect Filtered Ports:** Ports that are blocked or protected by a firewall.
 - Ports are entry points for network communication and are classified as:
- **Well-Known Ports (0-1023):** Commonly used by standard services like HTTP (port 80) and FTP (port 21).
 - **Registered Ports (1024-49151):** Used by less common applications.
 - **Dynamic/Private Ports (49152-65535):** Temporarily assigned for client-side connections.
- Nmap is a powerful and flexible tool that supports a variety of scanning techniques. It is used by network administrators and security professionals for tasks like:
 - Host discovery
 - Port and service scanning
 - OS detection
 - Network inventory creation
 - Vulnerability assessment

CODE:

- `nmap -v`
 - `nmap localhost`
 - `nmap -v 172.16.3.84 --disable-arp-ping`
 - `nmap -sA 172.16.3.84`

- nmap -Pn 172.16.3.84
- nmap -F 172.16.3.84
- nmap -O 172.16.3.84
- nmap -A 172.16.3.84
- nmap chikhli.abschool.in
- nmap 172.16.3.84-sL
- nmap -sW 172.16.3.48

OUTPUT:

```

22IT015_kali_linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Jan 12 18:52
rutvikchauhan@kali: ~
$ sudo apt install nmap
The following packages were automatically installed and are no longer required:
gkdb-capplet libavie0 openjdk-17-jre-headless
libdaxctl1 libre2-10 python3-diskcache
libgeos3.12.1t64 libioct.3 python3-mistune0
libgnomekbd-common libgtk4-1 python3-pendulum
libgnomekbd8 libu2f-udev python3-pytdata
libjxl0.7 libx265-199 samba-ad-provision
libndctl6 libxklavier16 samba-dsdb-modules
libpnm1 openjdk-17-jre
Use 'sudo apt autoremove' to remove them.

Upgrading:
nmap nmap-common

Summary:
Upgrading: 2, Installing: 0, Removing: 0, Not Upgrading: 2104
Download size: 6337 kB
Space needed: 794 kB / 38.4 GB available

Continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/non-free amd64 nmap amd64 7.95+dfsg-1kali1 [1938 kB]
Get:2 http://http.kali.org/kali kali-rolling/non-free amd64 nmap-common all 7.95+dfsg-1kali1 [4399 kB]
Fetched 6337 kB in 2s (2710 kB/s)
(Reading database ... 416444 files and directories currently installed.)
Preparing to unpack .../nmap_7.95+dfsg-1kali1_amd64.deb ...
Unpacking nmap (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-2+kali3) ...
Preparing to unpack .../nmap-common_7.95+dfsg-1kali1_all.deb ...
Unpacking nmap-common (7.95+dfsg-1kali1) over (7.94+git20230807.3be01efb1+dfsg-2+kali3) ...
Setting up nmap-common (7.95+dfsg-1kali1) ...
Setting up nmap (7.95+dfsg-1kali1) ...
Setcap worked! Adding configuration to environment
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for wordlists (2023.2.0) ...

(rutvikchauhan@kali)~$ nmap -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 18:51 IST
Read data files from: /usr/share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.07 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)

(rutvikchauhan@kali)~$

```

Figure 1: Check the version of Nmap and scanning

```

(rutvikchauhan@kali)~$ sudo nmap 192.168.163.235
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 18:55 IST
Nmap scan report for 192.168.163.235
Host is up (0.0024s latency).
Not shown: 995 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
6646/tcp  open  unknown
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 6.21 seconds

```

Figure 2: Scanning IP address

```
(rutvikchauhan@kali)-[~]
$ sudo nmap -v 192.168.163.235 --disable-arp-ping
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 18:56 IST
Initiating Ping Scan at 18:56
Scanning 192.168.163.235 [4 ports]
Completed Ping Scan at 18:56, 0.26s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:56
Completed Parallel DNS resolution of 1 host. at 18:56, 0.03s elapsed
Initiating SYN Stealth Scan at 18:56
Scanning 192.168.163.235 [1000 ports]
Discovered open port 445/tcp on 192.168.163.235
Discovered open port 3306/tcp on 192.168.163.235
Discovered open port 135/tcp on 192.168.163.235
Discovered open port 139/tcp on 192.168.163.235
Completed SYN Stealth Scan at 18:56, 5.09s elapsed (1000 total ports)
Nmap scan report for 192.168.163.235
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
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.58 seconds
Raw packets sent: 2003 (88.108KB) | Rcvd: 8 (336B)
```

Figure 3: getting detailed out of scan IP address

```
(rutvikchauhan@kali)-[~]
$ sudo nmap -sA 192.168.163.235
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 18:57 IST
Nmap scan report for 192.168.163.235
Host is up (0.00055s latency).
All 1000 scanned ports on 192.168.163.235 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 22.26 seconds
```

Figure 4: TCP ACK port scan

```
(rutvikchauhan@kali)-[~]  
$ sudo nmap -Pn 192.168.163.235  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 18:58 IST  
Nmap scan report for 192.168.163.235  
Host is up (0.015s 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  
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)  
  
Nmap done: 1 IP address (1 host up) scanned in 5.76 seconds
```

Figure 5: Scan a host to detect firewall

```
(rutvikchauhan@kali)-[~]  
$ sudo nmap -F 192.168.163.235  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 18:58 IST  
Nmap scan report for 192.168.163.235  
Host is up (0.00079s latency).  
Not shown: 96 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  
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.24 seconds
```

Figure 6:perform fast scan

```
(rutvikchauhan@kali)-[~]
└─$ sudo nmap -O 192.168.163.235
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 18:59 IST
Nmap scan report for 192.168.163.235
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
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose/phone
Running (JUST GUESSING): Microsoft Windows 11|10|2022|Phone|2008 (97%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:sp1
Aggressive OS guesses: Microsoft Windows 11 21H2 (97%), Microsoft Windows 10 (92%), Microsoft Windows Server 2022 (91%), Microsoft Windows 10 1607 (91%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows Server 2008 SP1 (88%)
No exact OS matches for host (test conditions non-ideal).
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 10.00 seconds
```

Figure 7: Scanning OS for target IP address

```
(rutvikchauhan@kali)-[~]
└─$ nmap -Pn charusat.ac.in
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 19:01 IST
Nmap scan report for charusat.ac.in (66.33.60.35)
Host is up (0.096s latency).
Other addresses for charusat.ac.in (not scanned): 66.33.60.66
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 18.59 seconds
```

Figure 8: Scan a domain

```

(rutvikchauhan@kali)-[~]
└─$ sudo nmap -A 192.168.163.235
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 19:02 IST
Nmap scan report for 192.168.163.235
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)
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone
Running (JUST GUESSING): Microsoft Windows 11|10|2022|Phone|2008 (97%)
OS CPE: cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008::sp1
Aggressive OS guesses: Microsoft Windows 11 21H2 (97%), Microsoft Windows 10 (92%), Microsoft Windows Server 2022 (91%), Microsoft Windows 10 1607 (91%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows Server 2008 SP1 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ smb2-time:
|   date: 2025-01-12T13:32:20
|   start_date: N/A
|_ smb2-security-mode:
|   3:1!
|     Message signing enabled but not required
|_ nbstat: NetBIOS name: CHAUHAN, NetBIOS user: <unknown>, NetBIOS MAC: 14:13:33:ba:b6:21 (AzureWave Technology)
|_ clock-skew: 1s

TRACEROUTE
HOP RTT ADDRESS
1 1.72 ms 192.168.163.235

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 56.85 seconds

```

Figure 9 : performs an **aggressive scan** on the target IP

```

(rutvikchauhan@kali)-[~]
└─$ nmap -sW 192.168.163.235
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 19:05 IST
Nmap scan report for 192.168.163.235
Host is up (0.0011s latency).
All 1000 scanned ports on 192.168.163.235 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 22.05 seconds

```

Figure 10: Windows scan to determine if the target IP is running a Windows-based operating system.

```
(rutvikchauhan@kali)-[~]
$ nmap 192.168.163.235 -sL
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 19:06 IST
Nmap scan report for 192.168.163.235
Nmap done: 1 IP address (0 hosts up) scanned in 0.12 seconds

(rutvikchauhan@kali)-[~]
$ nmap 192.168.163.235 -sn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-12 19:06 IST
Nmap scan report for 192.168.163.235
Host is up (0.00053s latency).
MAC Address: 14:13:33:BA:B6:21 (AzureWave Technology)
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

Figure 11: lists the hostnames and IP addresses in the given range

LATEST APPLICATIONS:

- Penetration Testing: Used by ethical hackers to identify vulnerabilities in a network.
- Network Security Assessments: Helps in evaluating a network's security by identifying exposed services or open ports.
- Vulnerability Scanning: Scans systems for outdated software or vulnerable services that could be exploited.
- Network Configuration Management: Administrators use Nmap to ensure unauthorized ports or services aren't running.

LEARNING OUTCOME:

Learning port scanning and enumeration with Nmap helps individuals identify open ports, running services, and operating systems on target systems. They gain hands-on experience with various scanning techniques to assess security, uncover vulnerabilities, and apply Nmap in real-world cybersecurity scenarios for both defensive and offensive tasks.

REFERENCES:

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