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:

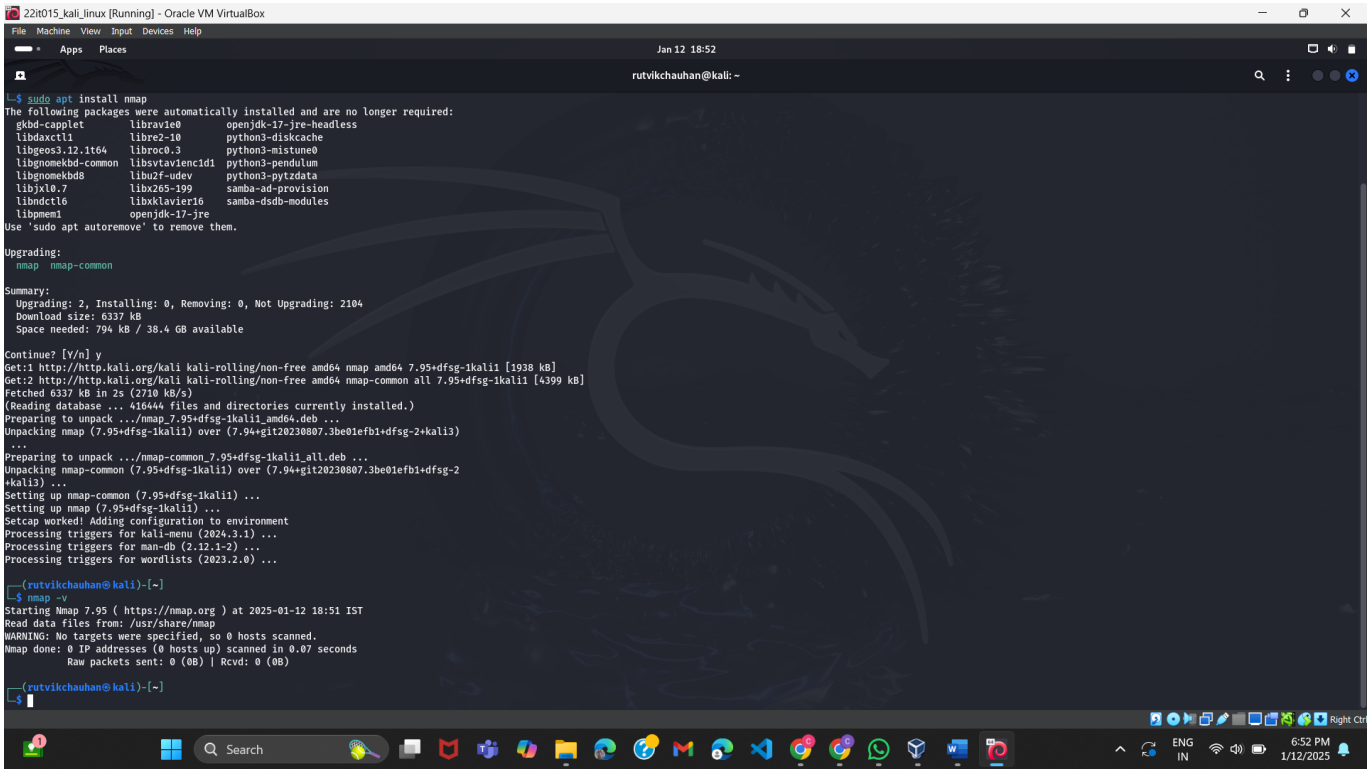

Figure 1:Check the version of Nmap and scanning

```
┌──(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

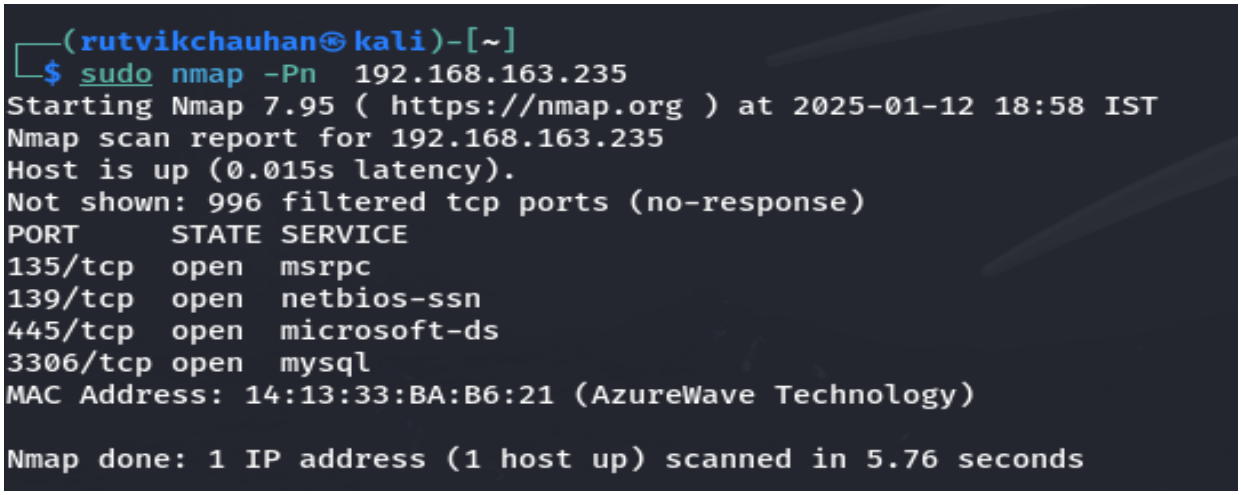

Figure 5: Scan a host to detect firewall

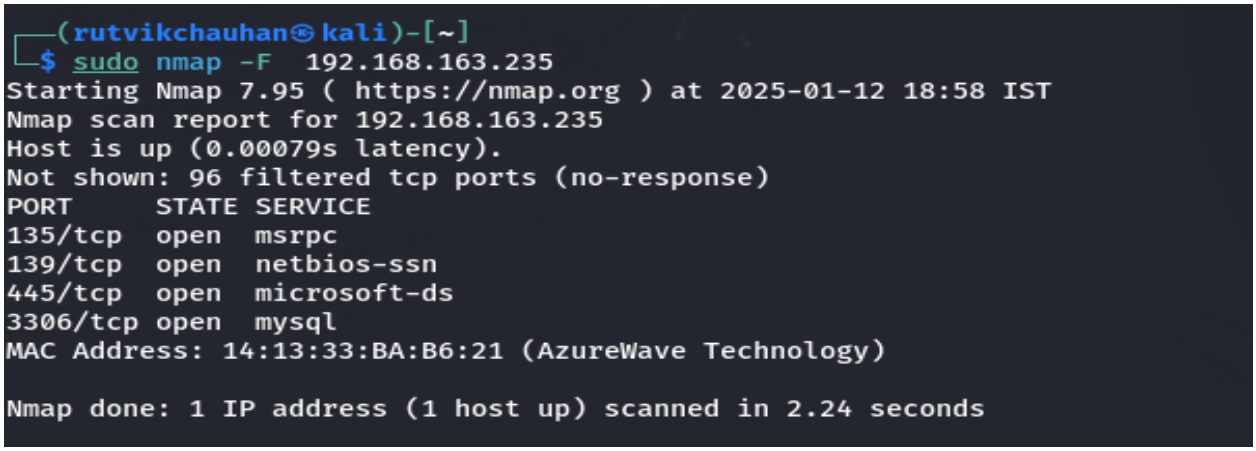

Figure 6:perform fast scan

Figure 7: Scanning OS for target IP address

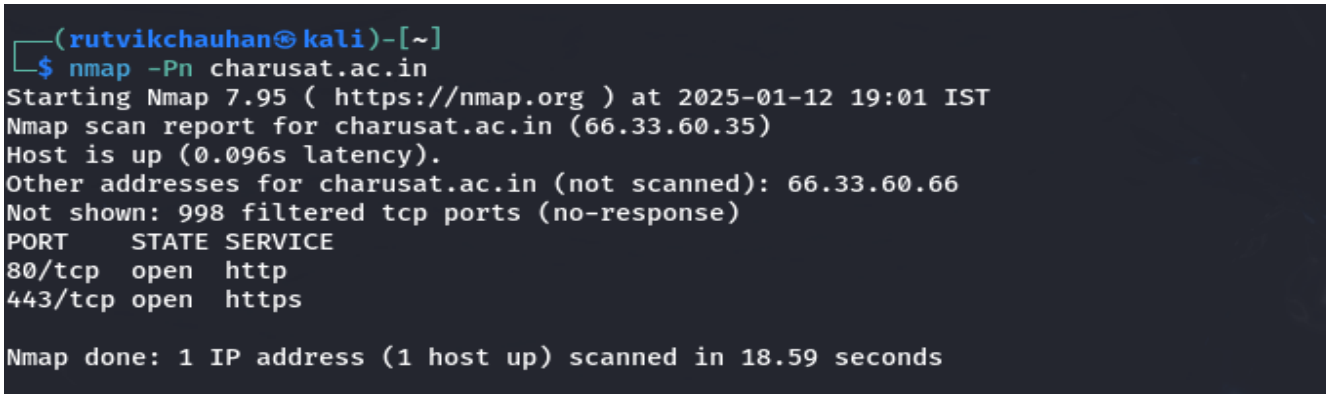

Figure 8: Scan a domain

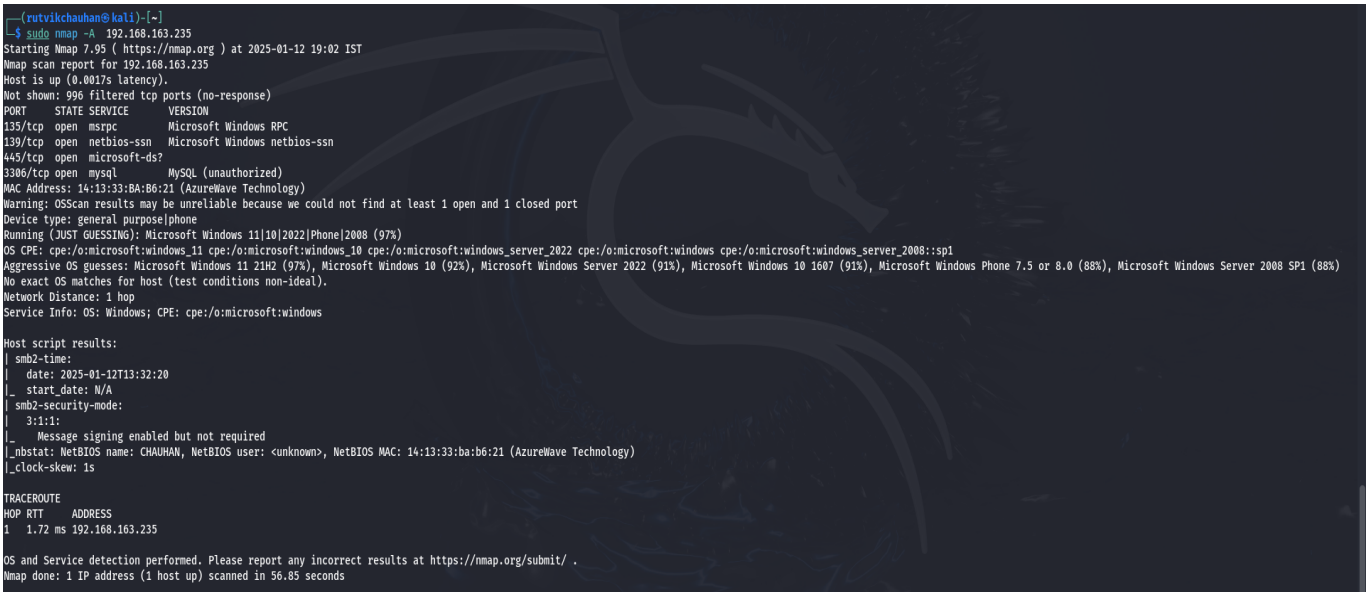

*Figure 9 : performs an **aggressive scan** on the target IP*

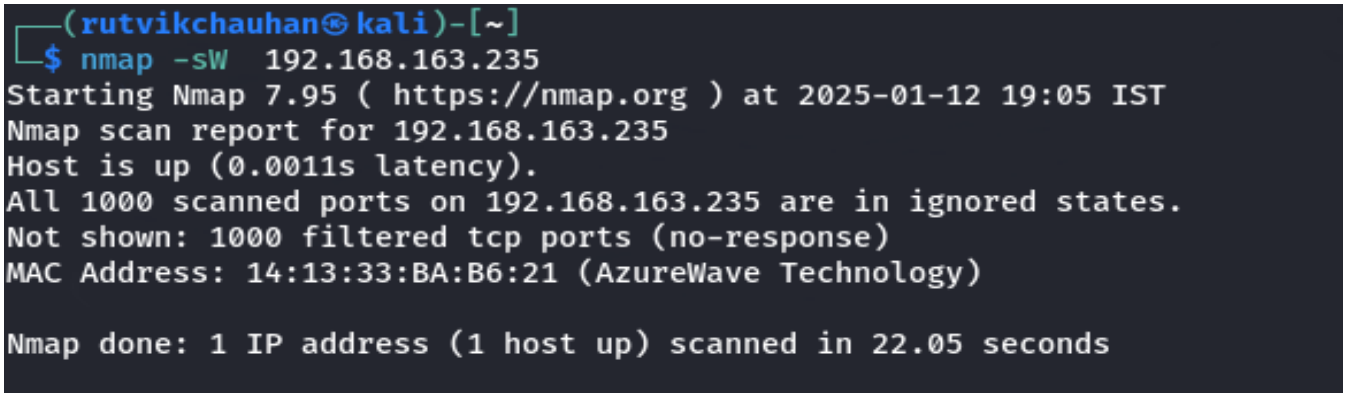

Figure 10:Windows scan to determine if the target IP is running a Windows-based operating system.

```
┌──(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/