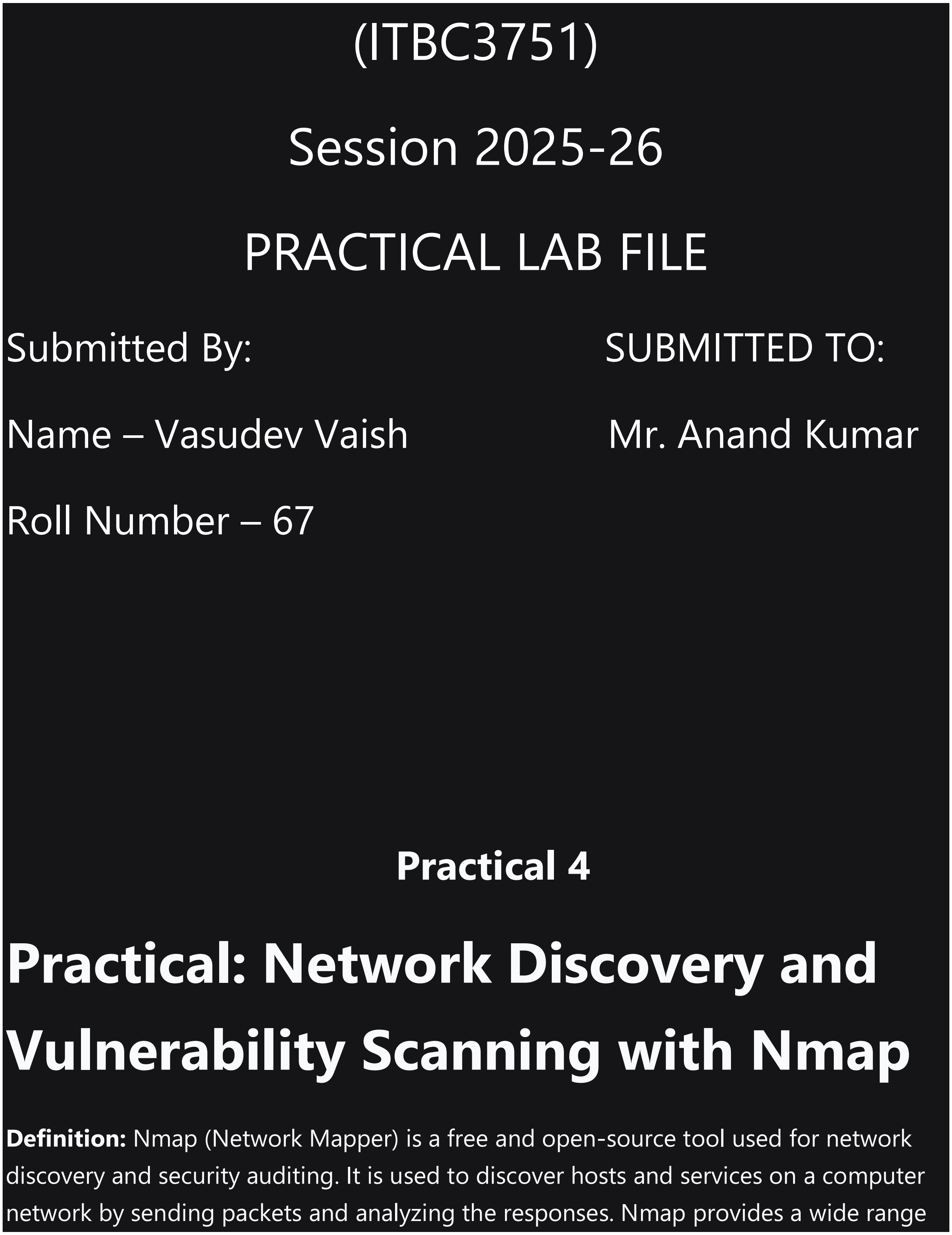
# BABU BANARASI DAS UNIVERSITY

## SCHOOL OF ENGINEERING

### Department of Computer Science & Engineering



(ITBC3751)

Session 2025-26

PRACTICAL LAB FILE

Submitted By: SUBMITTED TO:

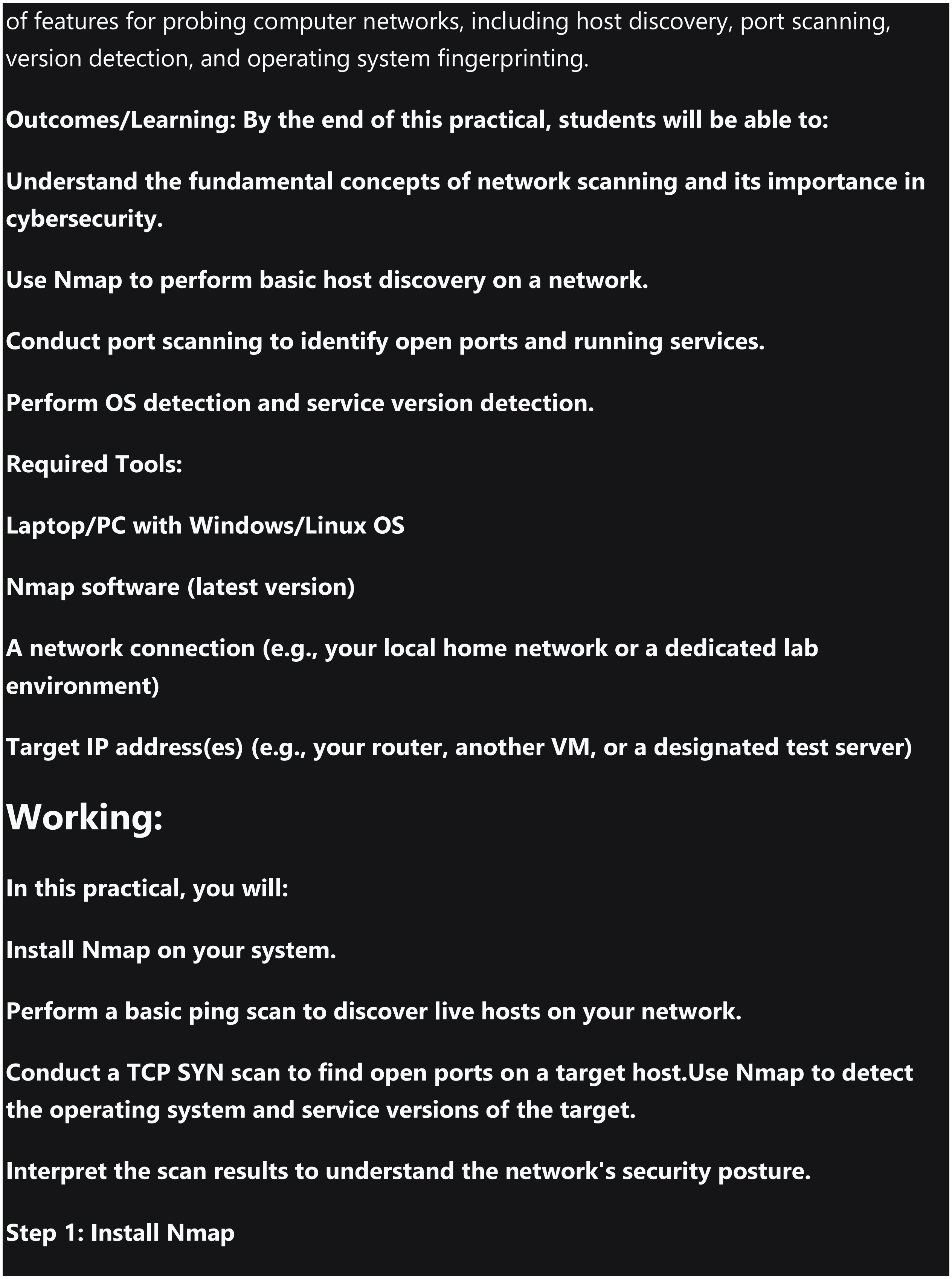
Name – Vasudev Vaish Mr. Anand Kumar

Roll Number – 67

**Practical 4**

# Practical: Network Discovery and Vulnerability Scanning with Nmap

**Definition:** Nmap (Network Mapper) is a free and open-source tool used for network discovery and security auditing. It is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap provides a wide range



of features for probing computer networks, including host discovery, port scanning, version detection, and operating system fingerprinting.

**Outcomes/Learning: By the end of this practical, students will be able to:**

**Understand the fundamental concepts of network scanning and its importance in cybersecurity.**

**Use Nmap to perform basic host discovery on a network.**

**Conduct port scanning to identify open ports and running services.**

**Perform OS detection and service version detection.**

**Required Tools:**

**Laptop/PC with Windows/Linux OS**

**Nmap software (latest version)**

**A network connection (e.g., your local home network or a dedicated lab environment)**

**Target IP address(es) (e.g., your router, another VM, or a designated test server)**

## Working:

**In this practical, you will:**

**Install Nmap on your system.**

**Perform a basic ping scan to discover live hosts on your network.**

**Conduct a TCP SYN scan to find open ports on a target host.Use Nmap to detect the operating system and service versions of the target.**

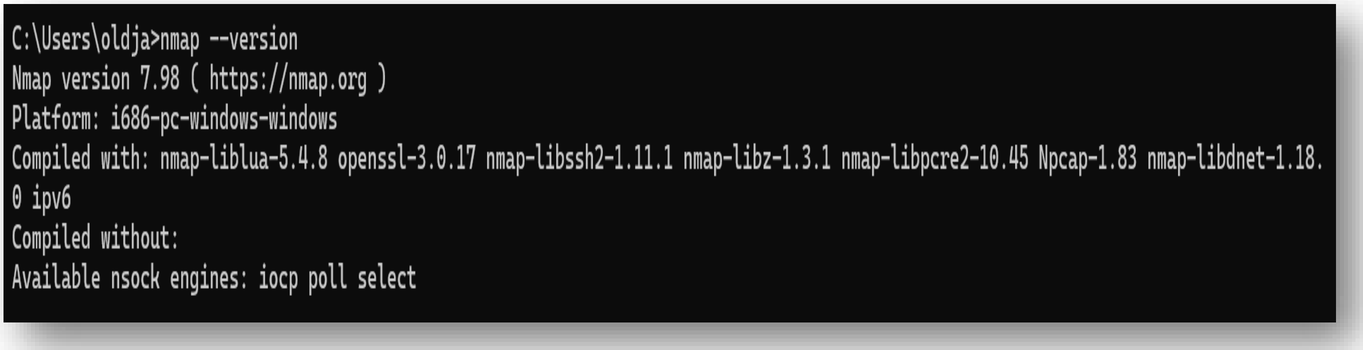
**Interpret the scan results to understand the network's security posture.**

**Step 1: Install Nmap**

Visit the official Nmap website (https://nmap.org/download.html) and download the installer for your operating system.

Run the installer and follow the setup instructions.

Alternatively, on Linux, you can often install it via the terminal using your package manager (e.g., `sudo apt-get install nmap`).



```
C:\Users\oldja>nmap --version
Nmap version 7.98 ( https://nmap.org )
Platform: i686-pc-windows-windows
Compiled with: nmap-liblua-5.4.8 openssl-3.0.17 nmap-libssh2-1.11.1 nmap-libz-1.3.1 nmap-libpcre2-10.45 Npcap-1.83 nmap-libdnet-1.18.
0 ipv6
Compiled without:
Available nsock engines: iocp poll select
```

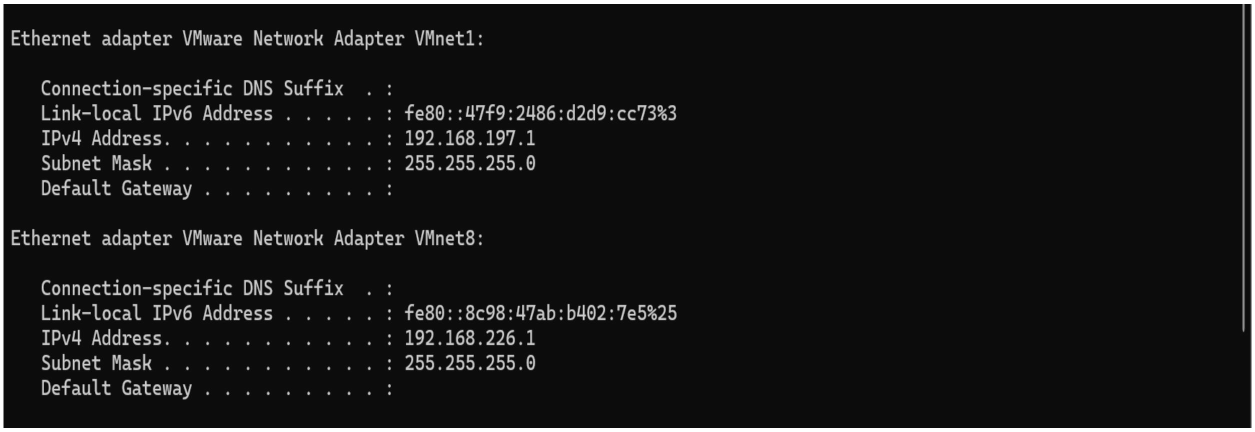
## Step 2: Identify an IP Range / Target

Determine your machine’s IP address and subnet.

**On Windows,** use the `ipconfig` command.

**On Linux/macOS,** use the `ip addr` or `ifconfig` command.

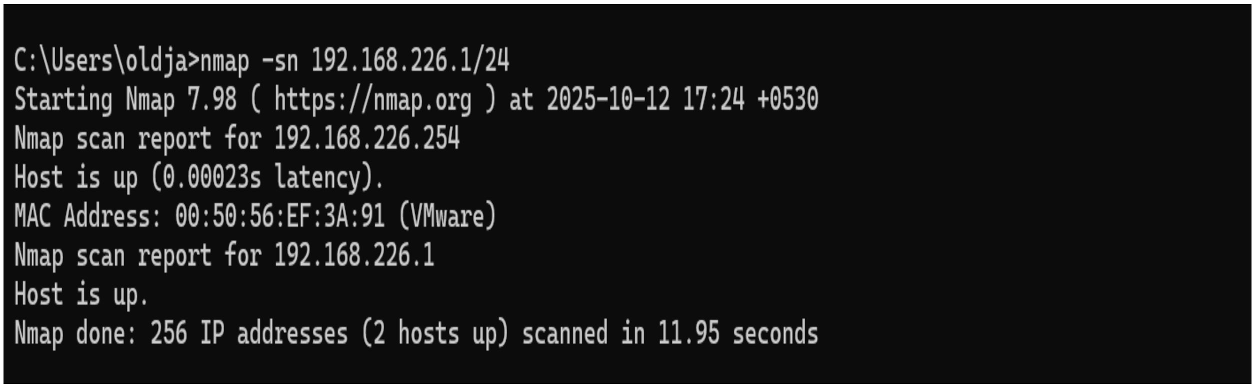
Note your IP address and subnet mask.



```
Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::47f9:2486:d2d9:cc73%3
   IPv4 Address. . . . . . . . . . . : 192.168.197.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8c98:47ab:b402:7e5%25
   IPv4 Address. . . . . . . . . . . : 192.168.226.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

## Step 3: Host Discovery (Find Live Hosts)

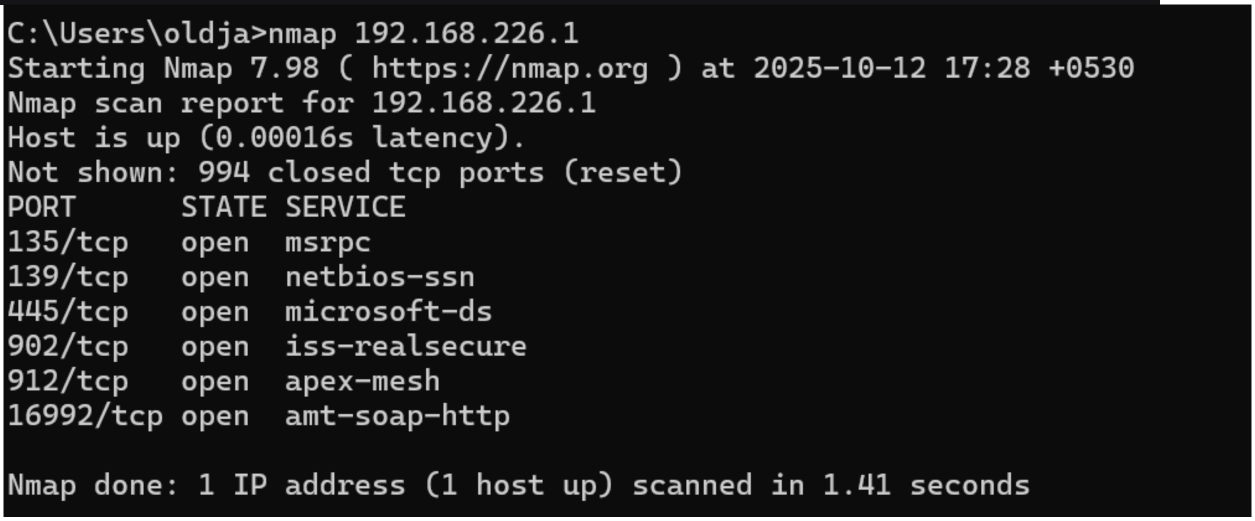
1. Perform a ping scan for fast host discovery



```
C:\Users\oldja>nmap -sn 192.168.226.1/24
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-12 17:24 +0530
Nmap scan report for 192.168.226.254
Host is up (0.00023s latency).
MAC Address: 00:50:56:EF:3A:91 (VMware)
Nmap scan report for 192.168.226.1
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 11.95 seconds
```

## Step 4: Basic TCP Port Scan

1. Choose a target IP address from the list found in Step 3 (e.g., `192.168.1.1`).
2. Perform a scan of the top 1000 TCP ports on that target:



```
C:\Users\oldja>nmap 192.168.226.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-12 17:28 +0530
Nmap scan report for 192.168.226.1
Host is up (0.00016s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
16992/tcp open  amt-soap-http

Nmap done: 1 IP address (1 host up) scanned in 1.41 seconds
```

1. **Results:** The scan revealed 6 open ports:

`135/tcp` - msrpc (Microsoft RPC)

`139/tcp` - netbios-ssn (NetBIOS Session Service)

`445/tcp` - microsoft-ds (Microsoft Directory Services)

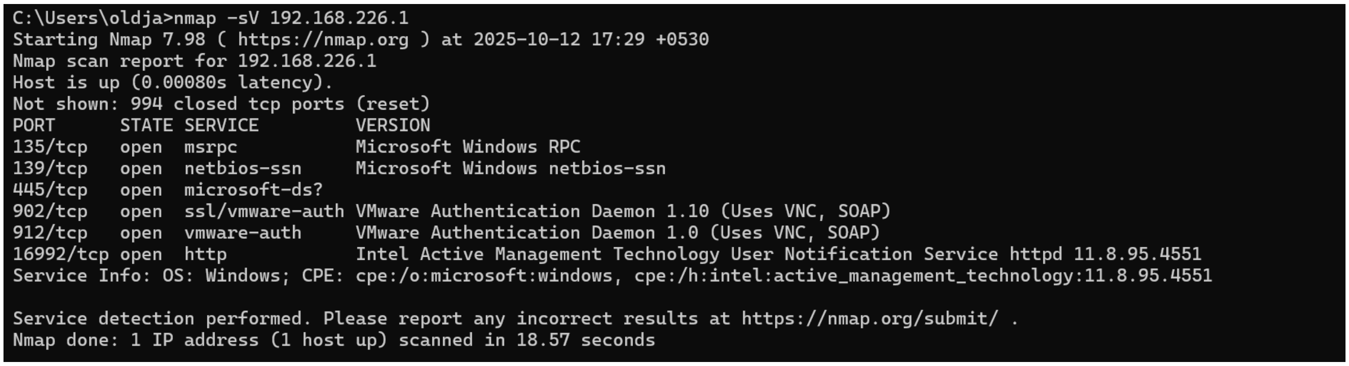
`902/tcp` - iss-realsecure

`912/tcp` - apex-mesh

`16992/tcp` - amt-soap-http (Intel AMT)

## Step 5: Service/Version Detection

1. To get detailed information about the services, run: nmap -sV 192.168.226.1



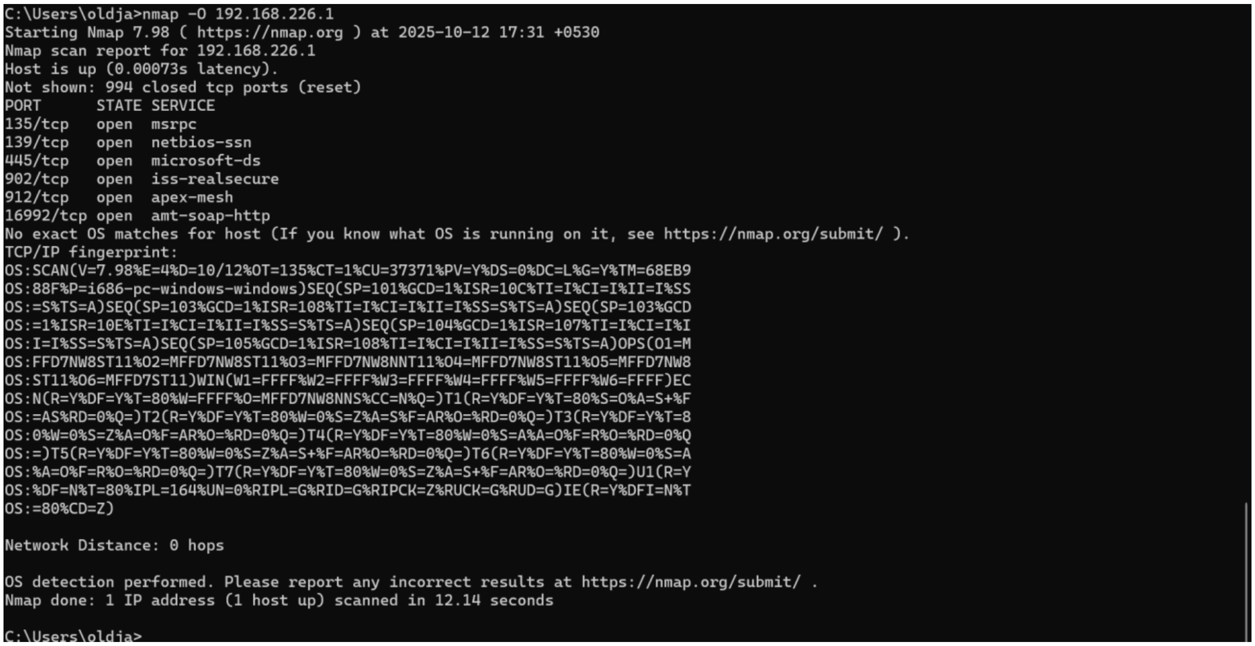
```
C:\Users\oldja>nmap -sV 192.168.226.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-12 17:29 +0530
Nmap scan report for 192.168.226.1
Host is up (0.00080s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE         VERSION
135/tcp   open  msrpc           Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
16992/tcp open  http            Intel Active Management Technology User Notification Service httpd 11.8.95.4551
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/h:intel:active_management_technology:11.8.95.4551

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.57 seconds
```

**Results:** The service version detection revealed:

- `135/tcp` - Microsoft Windows RPC
- `139/tcp` - Microsoft Windows netbios-ssn
- `445/tcp` - Microsoft Directory Services (specific version undetermined)
- `902/tcp` - VMware Authentication Daemon 1.10 (Uses VNC, SOAP) with SSL
- `912/tcp` - VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
- `16992/tcp` - Intel Active Management Technology User Notification Service httpd 11.8.95.455

## Step 6: OS Detection

Attempt to identify the target host's operating system



```
C:\Users\oldja>nmap -O 192.168.226.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-10-12 17:31 +0530
Nmap scan report for 192.168.226.1
Host is up (0.00073s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
16992/tcp open  amt-soap-http
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.98%E=4%D=10/12%OT=135%CT=1%CU=37371%PV=Y%DS=0%DC=L%G=Y%TM=68EB9
OS:88F%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS
OS:=S%TS=A)SEQ(SP=103%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=103%GCD
OS:=1%ISR=10E%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=1%ISR=107%TI=I%CI=I%I
OS:I=I%SS=S%TS=A)SEQ(SP=105%GCD=1%ISR=108%TI=I%CI=I%II=I%SS=S%TS=A)OPS(O1=M
OS:FFD7NW8ST11%O2=MFFD7NW8ST11%O3=MFFD7NW8NNT11%O4=MFFD7NW8ST11%O5=MFFD7NW8
OS:ST11%O6=MFFD7ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)EC
OS:N(R=Y%DF=Y%T=80%W=FFFF%O=MFFD7NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S%F=AR%O=%RD=0%Q=)T3(R=Y%DF=Y%T=8
OS:0%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q
OS:=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A
OS:%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y
OS:%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=Z%RUCK=G%RUD=G)IE(R=Y%DFI=N%T
OS:=80%CD=Z)

Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.14 seconds

C:\Users\oldja>
```

**Result:** No exact OS matches for host

**Observation:** TCP/IP fingerprint suggests Windows-based system but cannot determine exact version