PARSHVANATH CHARITABLE TRUST'S

# A. P. SHAH INSTITUTE OF TECHNOLOGY

Department of Information Technology

(NBA Accredited)

## Department of Information Technology

**Academic Year: 2025-26**
**Semester: V**
**Class / Branch: TEIT/Div C**
**Subject: Security Lab**
**Name of Instructor: Prof. Vishal Badgujar**

**Name of Student: Suyash Y Mane**
**Student ID: 24204008**
**Date of Performance: 07/07/2025**
**Date of Submission: 07/07/2025**

---

## Experiment No. 5

## Aim: To use nmap for network discovery and security auditing.

## Output Screenshots:

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sudo apt-get install nmap
[sudo] password for apsit:
Reading package lists... Done
Building dependency tree
Reading state information... Done
nmap is already the newest version (7.60-1ubuntu5).
The following packages were automatically installed and are no longer required:
  g++-7 libstdc++-7-dev
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1362 not upgraded.
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ nmap -sP 192.168.91.49

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 10:38 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 3.03 seconds
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ nmap -sP 192.168.91.49/24

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 10:40 IST
Nmap scan report for 192.168.91.1
Host is up (0.00061s latency).
Nmap scan report for 192.168.91.2
Host is up (0.00045s latency).
Nmap scan report for 192.168.91.3
Host is up (0.00056s latency).
Nmap scan report for 192.168.91.7
Host is up (0.00081s latency).
Nmap scan report for apsit-HP-ProDesk-600-G4-PCI-MT (192.168.91.8)
Host is up (0.000083s latency).
Nmap scan report for 192.168.91.9
Host is up (0.00056s latency).
Nmap scan report for 192.168.91.10
Host is up (0.00055s latency).
Nmap scan report for 192.168.91.11
Host is up (0.00099s latency).
Nmap scan report for 192.168.91.15
Host is up (0.00088s latency).
Nmap scan report for 192.168.91.17
Host is up (0.0013s latency).
Nmap scan report for 192.168.91.19
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ nmap -sP 192.168.91.1 192.168.91.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 10:42 IST
Nmap scan report for 192.168.91.1
Host is up (0.00047s latency).
Nmap scan report for 192.168.91.2
Host is up (0.00050s latency).
Nmap done: 2 IP addresses (2 hosts up) scanned in 3.01 seconds
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ nmap -sP 192.168.91.49/24 -exclude 192.1
68.91.1

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 10:47 IST
Nmap scan report for 192.168.91.2
Host is up (0.00049s latency).
Nmap scan report for 192.168.91.3
Host is up (0.00038s latency).
Nmap scan report for 192.168.91.7
Host is up (0.00022s latency).
Nmap scan report for apsit-HP-ProDesk-600-G4-PCI-MT (192.168.91.8)
Host is up (0.00011s latency).
Nmap scan report for 192.168.91.9
Host is up (0.00046s latency).
Nmap scan report for 192.168.91.10
Host is up (0.00034s latency).
Nmap scan report for 192.168.91.11
Host is up (0.00044s latency).
Nmap scan report for 192.168.91.15
Host is up (0.00032s latency).
Nmap scan report for 192.168.91.17
Host is up (0.00042s latency).
Nmap scan report for 192.168.91.19
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ nmap -p 80,21,23 192.168.91.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 10:55 IST
Nmap scan report for 192.168.91.2
Host is up (0.00050s latency).

PORT   STATE  SERVICE
21/tcp closed ftp
23/tcp closed telnet
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 3.03 seconds
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ nmap --top-ports 5 192.168.91.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 10:53 IST
Nmap scan report for 192.168.91.2
Host is up (0.00059s latency).

PORT    STATE  SERVICE
21/tcp  closed ftp
22/tcp  closed ssh
23/tcp  closed telnet
80/tcp  closed http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 3.05 seconds
```

## Nmap Scanning Techniques

**Table 1: Scanning Techniques**

| Scanning Technique | Syntax | Use |
|---|---|---|
| TCP SYN | -sS | Stealth scan |
| TCP connect() | -sT | Scan without root privileges |
| FIN | -sF | Stealth scan |
| Xmas | -sX | Stealth scan |
| Null | -sN | Stealth scan |
| Ping | -sP | Identify live hosts |
| Version Detection | -sV | Identify services |
| UDP | -sU | Find UDP services |
| IP Protocol | -sO | Discover supported protocols |
| ACK | -sA | Identify firewalls |
| Window | -sW | Advanced ACK scan |
| RPC | -sR | Information on RPC services |
| List | -sL | Dummy for test purposes |
| Idle | -sI | Scan via third party |
| FTP Bounce | -b | Historic |

| Scan Type | Syntax | Example |
|---|---|---|
| TCP SYN Scan | -sS | nmap -sS 10.20.3.100 |
| TCP Connect Scan | -sT | nmap -sT 10.20.3.100 |
| Fin Scan | -sF | nmap -sF 10.20.3.100 |
| XMAS Scan | -sX | nmap -sX 10.20.3.100 |
| Null Scan | -sN | nmap -sN 10.20.3.100 |
| Ping Scan | -sP | nmap -sP 10.20.3.100 |
| Version Detection | -sV | nmap -sV 10.20.3.100 |
| UDP Scan | -sU | nmap -sU 10.20.3.100 |
| IP Protocol Scan | -sO | nmap -sO 10.20.3.100 |
| ACK Scan | -sA | nmap -sA 10.20.3.100 |
| Windows Scan | -sW | nmap -sW 10.20.3.100 |
| List Scan | -sL | nmap -sL 10.20.3.100 |

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sudo nmap -sS 192.168.91.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 10:59 IST
Nmap scan report for 192.168.91.2
Host is up (0.00036s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
902/tcp open  iss-realsecure
MAC Address: C8:D9:D2:29:AF:FC (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sudo nmap -sT 192.168.91.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 11:02 IST
Nmap scan report for 192.168.91.2
Host is up (0.00023s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
902/tcp open  iss-realsecure
MAC Address: C8:D9:D2:29:AF:FC (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.33 seconds
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sudo nmap -sF 192.168.91.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 11:05 IST
Nmap scan report for 192.168.91.2
Host is up (0.00017s latency).
Not shown: 999 closed ports
PORT    STATE         SERVICE
902/tcp open|filtered iss-realsecure
MAC Address: C8:D9:D2:29:AF:FC (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.37 seconds
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sudo nmap -sV 192.168.91.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 11:07 IST
Nmap scan report for 192.168.91.2
Host is up (0.00055s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE         VERSION
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
MAC Address: C8:D9:D2:29:AF:FC (Unknown)
```

```
apsit@apsit-HP-ProDesk-600-G4-PCI-MT:~$ sudo nmap -O 192.168.91.2

Starting Nmap 7.60 ( https://nmap.org ) at 2025-08-07 11:13 IST
Nmap scan report for 192.168.91.2
Host is up (0.00040s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
902/tcp open  iss-realsecure
MAC Address: C8:D9:D2:29:AF:FC (Unknown)
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=7.60%E=4%D=8/7%OT=902%CT=1%CU=32615%PV=Y%DS=1%DC=D%G=Y%M=C8D9D2%T
OS:M=68943D30%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%CI=Z%TS=A
OS:)SEQ(SP=104%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4
OS:ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1
OS:=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O
OS:=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N
OS:)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=
OS:S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF
OS:=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

**Conclusion:**

In this experiment, we learnt and understood how to use nmap for network discovery and security auditing more clearly.