

Task 1:

Objective: Learn to discover open ports on devices in your local network to understand network exposure.

Tools: Nmap

Scanning IP:

Nmap result:

```
(kali㉿kali)-[~]
└─$ sudo nmap -sS [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 20:02 IST
Nmap scan report for [redacted]
Host is up (0.0014s 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
3306/tcp   open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for [redacted]
Host is up (0.00021s latency).
All 1000 scanned ports on [redacted] are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EA:53:EC (VMware)

Nmap scan report for [redacted]
Host is up (0.0000040s latency).
All 1000 scanned ports on [redacted] are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 32.32 seconds
```

```
Home X kali-linux-2025-W25-vmwar... X
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help
L-$ sudo nmap -sS -sV -O --script=default [redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 20:04 IST
Nmap scan report for [redacted]
Host is up (0.0024s 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)
3306/tcp   open  mysql            MySQL (unauthorized)
MAC Address: 00:50:56:C0:00:08 (VMware)
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=7.95E=4%D=10/20%OT=135%CT=1%CU=41773%PV=Y%DS=1%DC=D%G=Y%M=005056
OS:%TM=68F648BE%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=107%TI=I%CI=I%II
OS:=I%SS=S%TS=A)SEQ(SP=102%GCD=1%ISR=102%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=10
OS:3%GCD=1%ISR=100%TI=I%CI=I%II=I%SS=S%TS=A)SEQ(SP=104%GCD=1%ISR=10A%TI=I%CI
OS:=I%II=I%SS=S%TS=A)SEQ(SP=108%GCD=1%ISR=109%TI=I%CI=I%II=I%SS=S%TS=A)OPS
OS:(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8ST11%O5=M5B4NW8
OS:ST11%O6=M5B4ST11)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN
OS:(R=Y%DF=Y%T=80%W=FFFF%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=80%S=0%A=S+F=A
OS:S%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=80%
OS:W=0%S=Z%A=0%F=AR%O=RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=A%O=0%F=AR%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%A
OS:=0%F=AR%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%D
OS:F=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=8
OS:0%CD=Z)
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-time:
|_  date: 2025-10-20T14:35:36
|_  start_date: N/A
|_  smb2-security-mode:
|_    3:1:1:
|_      Message signing enabled but not required
|_ nbstat: NetBIOS name: LAPTOP-B19RJD7C, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:c0:00:08 (VMware)
Nmap scan report for [redacted]
Host is up (0.00036s latency).
All 1000 scanned ports on [redacted] in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:EA:53:EC (VMware)
Too many fingerprints match this host to give specific OS details
```

Open ports:-

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
- 3306/tcp open mysql

Potential security risks from open ports:-

135/tcp (msrpc)

Exposes Windows RPC endpoint used for service discovery—can be leveraged for enumeration and to pivot using RPC-based exploits.

If unpatched or reachable from untrusted networks, attackers may enumerate services and use RPC to launch further attacks or remote code execution.

139/tcp (netbios-ssn)

Allows NetBIOS name resolution and SMB-over-NetBIOS share enumeration; it can reveal share names, users, and machine info.

If exposed, it enables information disclosure, null-session abuse, and easier lateral movement or credential attacks.

445/tcp (microsoft-ds / SMB)

SMB exposure is a high-value target for ransomware, worms, and remote code exploits—vulnerable/old SMB implementations are actively exploited.

Open SMB can permit file/share abuse, credential theft or relay attacks, and full network compromise if not patched or properly restricted.

902/tcp (VMware management)

Often used by VMware management/console services—if reachable, it can leak VM/host management interfaces and metadata.

Misconfiguration or vulnerable VMware versions can allow remote management abuse or information disclosure about VMs and hypervisor.

912/tcp (apex-mesh / vendor service)

Uncommon/vendor-specific service — unknown daemons increase risk due to lack of visibility and potentially weak/default configs.

If unnecessary or unpatched, it may contain exploitable bugs or allow unauthorized control/information leakage.

3306/tcp (MySQL)

Publicly reachable database port risks data exfiltration, brute-force access, and exploitation of database-specific vulnerabilities.

If bound to 0.0.0.0 or using weak credentials, attackers can access or dump sensitive data and pivot into internal systems.

Saved scan results in text:-

```
(kali@kali)-[~]
ls
yfile.txt  ciscat-test  Downloads  ignite.crt  list.txt  namoo.txt
lkactf     Desktop     EfmqxTGS.jpeg  ignite.key  lst.txt  nmap_output
rt.pem     dik.txt     'ftp anumeration.pcapng'  ignite.pem  Music  passwd.txt
pher.txt   Documents  iEWWDJPN.jpeg  ILzVpdbT.jpeg  mywork.txt  payl.exe
```