 # Task 01 — Scan Local Network for Open Ports

Objective

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

Tools

Nmap (required)
tcpdump (optional, for packet capture)
Wireshark (optional, for packet analysis)

Quick setup / install

`bash
sudo apt update
sudo apt install -y nmap tcpdump wireshark xsltproc
```

# Steps (copy-paste commands)

1. Find your subnet

`bash
ip -4 addr show

2. Discover live hosts (fast ARP/ping scan)

`bash
sudo nmap -sn 192.168.1.0/24 -oN nmap_hosts_up.txt

3. Scan common ports (top 1000)

`bash
sudo nmap -sS --top-ports 1000 -T4 192.168.1.0/24

4. Full TCP port scan for a specific host

`bash
sudo nmap -sS -p- -T4 -v 192.168.1.50 -oA 192.168.1.50_full

5. Service/version & OS detection (deeper)

`bash
sudo nmap -sS -sV -O -p 22,80,443 192.168.1.50 -oN nmap_service_192.168.1.50.txt

6. UDP scan (optional)
```

`bash
sudo nmap -sU --top-ports 200 -T3 192.168.1.0/24 -oN nmap_udp.txt

7. Skip discovery if pings are blocked

`bash
sudo nmap -Pn -sS --top-ports 1000 192.168.1.50 -oN scan_no_ping.txt

Packet capture with tcpdump (optional)

1. Identify interface:

`bash
ip -o -4 route show to default | awk '{print $5}'

2. Start capture:

`bash
sudo tcpdump -i <iface> -w ~/pcap/scan_capture.pcap
```

3. Run your Nmap scan in another terminal, then stop tcpdump
4. Open capture in Wireshark:

`bash
wireshark ~/pcap/scan_capture.pcap

#Analyze in Wireshark — useful display filters

- Show traffic to/from a host: `ip.addr == 192.168.1.50`
- Show only TCP: `tcp`
- SYN packets (scan attempts): `tcp.flags.syn == 1 && tcp.flags.ack == 0`
- SYN/ACK (open port replies): `tcp.flags.syn == 1 && tcp.flags.ack == 1`

# Research services & map ports → services

Common ports to check (examples):

- `22` — SSH
- `21` — FTP
- `23` — Telnet
- `80` / `443` — HTTP / HTTPS
- `139`, `445` — SMB
- `3306` — MySQL
- `3389` — RDP
- `5900` — VNC
```

Use `-sV` output to look up exact versions and search for CVEs: e.g. `OpenSSH 7.2p2 CVE`.

Identify potential security risks (what to document)

For each open port / service include:

- IP address
- Open ports
- Service name & version (from `-sV`)
- Is the service expected/required? (Yes / No)
- Risk rating: Critical / High / Medium / Low (brief justification)
- Recommended remediation (close, patch, firewall rule, change creds, segmentation)

Example entry:

- 192.168.1.50
  - ports: 22/tcp (OpenSSH 7.2p2)
  - expected: Yes (admin server)
  - risk: Medium — check for weak passwords; ensure key-based auth
  - remediation: disable password auth, enforce keys and 2FA, restrict IPs

Notes & Ethics
- Only scan networks you own or have explicit permission to test. Scanning without permission can be illegal and disruptive.
- Remove or redact any sensitive information (passwords, private keys, personal data) before publishing.