Task 1 — Local Network Open Ports Scan — Detailed Report

Date: 2025-10-20
Network scanned: 192.168.1.0/24

Table of contents

1. Executive summary
2. Scope & rules of engagement
3. Methodology & tools
4. Findings (detailed)
    - Per-host observations
    - Evidence/artefacts
5. Risk assessment
6. Remediation & hardening (step-by-step)
7. Next steps & recommendations
8. Artifacts & appendix

---

1. Executive summary

This report documents a host-discovery reconnaissance run of the local network `192.168.1.0/24` conducted on **2025-10-20**. The scan used `nmap -sn` (ICMP/ARP host discovery) to determine which IPs are alive. The scan observed **4 live hosts** (192.168.1.1, 192.168.1.3, 192.168.1.4, 192.168.1.5) out of 256 addresses. No port or service enumeration was performed during this run; therefore, there are no confirmed open services or vulnerabilities discovered yet. The goal of this engagement was to enumerate live hosts so a follow-up service scan (`-sS -sV`) can be run safely and efficiently on confirmed targets.

---

2. Scope & rules of engagement

- **Target network:** 192.168.1.0/24
- **Allowed activities:** passive and active host discovery (nmap -sn), targeted TCP/UDP scanning only after explicit authorization.
- **Out of scope:** intrusive exploitation, privilege escalation, DoS testing, or any action affecting production services.
- **Assumptions:** scanning was performed from an internal system with permission to scan the subnet. Ensure you have written permission before proceeding with further scans.

---

3. Methodology & tools

Tools used:

- `nmap` — for host discovery and later service enumeration.
- (Optional) `arp-scan`, `netdiscover` — useful if ARP discovery is preferred.

Commands executed (this session):

nmap -sn 192.168.1.0/24 -oN port_scan.txt

Notes: This command performs host discovery using ICMP/ARP and reports hosts that respond as "up". Output was saved to `port_scan.txt`.

Planned follow-up commands (after authorization):

sudo nmap -sS -T4 --open 192.168.1.0/24 -oA ElevateLabsWork/Task1-Port-Scan/scans/network_scan
sudo nmap -sS -sV -p- -oN ElevateLabsWork/Task1-Port-Scan/scans/host-192.168.1.4-sv.txt 192.168.1.4
sudo nmap -sU -p 53,161 192.168.1.4 -oN ElevateLabsWork/Task1-Port-Scan/scans/udp-192.168.1.4.txt

---

4. Findings (detailed)

> **Note:** This section reflects the host discovery (`-sn`) results. No ports or services were enumerated in this scan. For each host, we provide observed metadata, a preliminary device classification, recommended immediate checks, and placeholders for images/screenshots where you can paste evidence (e.g., `nmap` output screenshots, router web GUI screenshots, Wireshark captures).

Summary table — Host discovery results

IP	MAC	Vendor	Observed status	Preliminary device type
192.168.1.1	F4:F6:47:71:03:E0	ZTE	up	Router / ISP gateway
192.168.1.5	52:04:2C:68:80:C1	Unknown	up	Unknown (possibly IoT)
192.168.1.4	2C:7B:A0:8D:E6:63	Intel Corporate	up	Laptop / Desktop
192.168.1.3	—	—	up	Unknown (no MAC shown in output)

192.168.1.1 — vendor: ZTE (MAC: F4:F6:47:71:03:E0)

Observed: Host responded to discovery probes and appears to be an ISP-supplied ZTE router or gateway.

Why it matters: Routers/gateways provide network services (DHCP, NAT) and host administrative interfaces (HTTP/HTTPS, telnet/ssh). Misconfigured or outdated routers can expose admin interfaces or run vulnerable firmware.

Immediate next steps (commands):

sudo nmap -sS -sV -p- -oN ElevateLabsWork/Task1-Port-Scan/scans/host-192.168.1.1-sv.txt 192.168.1.1

Recommended checks:

- Are HTTP/HTTPS admin pages exposed? If yes, ensure HTTPS-only and strong credentials.
- Is remote management (WAN) enabled? Disable or restrict to trusted IPs.
- Is SSH/telnet present? Disable telnet; prefer SSH with key-based auth.
- Check firmware version against vendor advisories and update if needed.

192.168.1.5 — vendor: Unknown (MAC: 52:04:2C:68:80:C1)

Observed: Host is up; vendor lookup returned Unknown.

Why it matters: Unknown vendor devices often include IoT devices that have default credentials or unpatched stacks.

Immediate next steps (commands):

sudo nmap -sS -sV -p- -oN ElevateLabsWork/Task1-Port-Scan/scans/host-192.168.1.5-sv.txt 192.168.1.5
sudo nmap -sU -p 53,161 192.168.1.5 -oN ElevateLabsWork/Task1-Port-Scan/scans/host-192.168.1.3-udp.txt

Recommended checks once the service scan completes:

- Identify open ports and services; map those services to common IoT device management ports.
- If Telnet/HTTP with default creds is found: replace with secure alternatives or isolate device to guest VLAN.
- If SNMP is present: check community strings and switch to SNMPv3 if required.

192.168.1.4 — vendor: Intel Corporate (MAC: 2C:7B:A0:8D:E6:63)

Observed: Host is up; vendor suggests a laptop/desktop NIC.

Why it matters: End-user machines often run services (SSH, file sharing, remote desktop) that can be attack vectors if misconfigured.

Immediate next steps (commands):

sudo nmap -sS -sV -p 22,80,139,445,3389 -oN ElevateLabsWork/Task1-Port-Scan/scans/host-192.168.1.4-commonports.txt 192.168.1.4
# or a full port scan
sudo nmap -sS -sV -p- -oN ElevateLabsWork/Task1-Port-Scan/scans/host-192.168.1.4-sv.txt 192.168.1.4

Recommended checks once the service scan completes:

- If SMB (445/139) is open: ensure file sharing is restricted and up-to-date (disable SMBv1).
- If RDP (3389) is open: restrict to trusted IPs, enable Network Level Authentication.

- If SSH (22) is open: enforce key-based authentication and disable password auth.

Evidence/image placeholder:

192.168.1.3 — vendor: (not shown)

Observed: Host is up; no MAC vendor printed in discovery output.

Why it matters: Devices not showing MAC in the output may be using MAC randomization (mobile devices) or the scanner failed to capture ARP/MAC.

Immediate next steps (commands):

sudo nmap -sS -sV -p- -oN ElevateLabsWork/Task1-Port-Scan/scans/host-192.168.1.3-sv.txt 192.168.1.3

Recommended checks once the service scan completes:

- Identify services and correlate with known device presence (mobile, printer, etc.).
- If the device is unmanaged or unknown, consider isolating it to the guest VLAN until inventoried.

---

5. Risk assessment

Current risk level: Low (scan only confirmed host presence; no services enumerated yet). However, risk cannot be fully assessed without service/version enumeration.

Potential high-impact findings to watch for in follow-up scans:

- Exposed management interfaces (HTTP/HTTPS) on routers and IoT devices with default credentials or outdated firmware.
- Unrestricted RDP/SMB exposure on endpoints.
- Clear-text services (Telnet, FTP) running on devices.
- UDP services (SNMP, DNS) with weak settings or open community strings.

---

6. Remediation & hardening (step-by-step)

Below are recommended remediation steps mapped to common findings. Execute these after you confirm a given service is present.

Router/gateway (likely 192.168.1.1)

1. **Disable remote management:** Disable WAN-side admin access. If remote management is required, restrict to specific source IPs and use VPN.
2. **Use HTTPS and strong admin creds:** Ensure the admin console uses HTTPS and set a strong, unique password. Change the default username.
3. **Update firmware:** Check vendor advisory and update firmware to the latest stable release.
4. **Disable unused services:** Disable telnet, UPnP, and WPS if not needed.
5. **Backup config and document:** Keep a secure copy of the router configuration after hardening.

Commands/checks:

- Check open management ports:

```
sudo nmap -p 80,443,22,23,8080 192.168.1.1
```

IoT / unknown device (e.g., 192.168.1.3)

1. Identify the device and owner.
2. If the device uses default creds, change them or isolate the device on a separate VLAN.
3. Limit network access via firewall policies (only allow necessary ports/IPs).
4. Update firmware where applicable.

End-user machines (e.g., 192.168.1.4)

1. Disable unnecessary network file-sharing protocols.
2. Ensure OS and applications are patched.
3. Use a host-based firewall to restrict inbound management ports to trusted networks.
4. Enforce MFA for remote access where possible.

General network controls

- **Network segmentation:** Place IoT/guest devices on separate VLANs with limited access to critical resources.
- **Inventory & monitoring:** Maintain an asset inventory and enable network monitoring/alerting for unusual port scans or new devices.
- **Access control lists (ACLs):** Restrict access to management ports to admin subnets.

---

7. Next steps & recommendations

1. **Obtain authorization** to run TCP SYN (`-sS`) and service/version (`-sV`) scans against discovered hosts.
2. Run the follow-up scans (copy-paste commands in Section 3 or Section 6) and attach the outputs to this repo: `ElevateLabsWork/Task1-Port-Scan/scans/*`.
3. For any high-risk service discovered, create a per-host remediation ticket with screenshots and exact commands to fix the issue.
4. Consider running an authenticated vulnerability scan or using tools like `OpenVAS`/`nikto` where appropriate and authorized.

---

8. Artifacts & appendix

Files produced / to produce:

- `port_scan.txt` — host discovery output (this session).
- `ElevateLabsWork/Task1-Port-Scan/scans/network_scan.nmap`, `.xml`, `.gnmap` — after running `-sS` on subnet.
- `ElevateLabsWork/Task1-Port-Scan/scans/host-<IP>-sv.txt` — per-host service/version outputs.
- `ElevateLabsWork/Task1-Port-Scan/scans/udp-<IP>.txt` — optional UDP checks where appropriate.
- `captures/scan.pcapng` — optional packet capture if you collect traffic using Wireshark/tcpdump.

End of report

Prepared by: Pratyush Raj — Task 1: Local Network Open Ports Scan