# Task 1 — Local Network Port Scan & Packet Capture Report

**Author:** Bhargav S
**Date:** 2025-09-22

## 1. Objective

Scan the local network to discover open ports and services, capture network packets during the scan for verification, research the common services found, identify potential security risks, and save the scan & capture results as submission-ready files.

## 2. Scope

Target: Local LAN (subnet used in this report
Devices scanned: All hosts on the local LAN that responded to the scan.
Only devices owned by or permitted to be scanned were targeted.

## 3. Tools & Environment

Tools used:
- Nmap 7.95
- tcpdump/tshark/Wireshark (if packet capture performed)

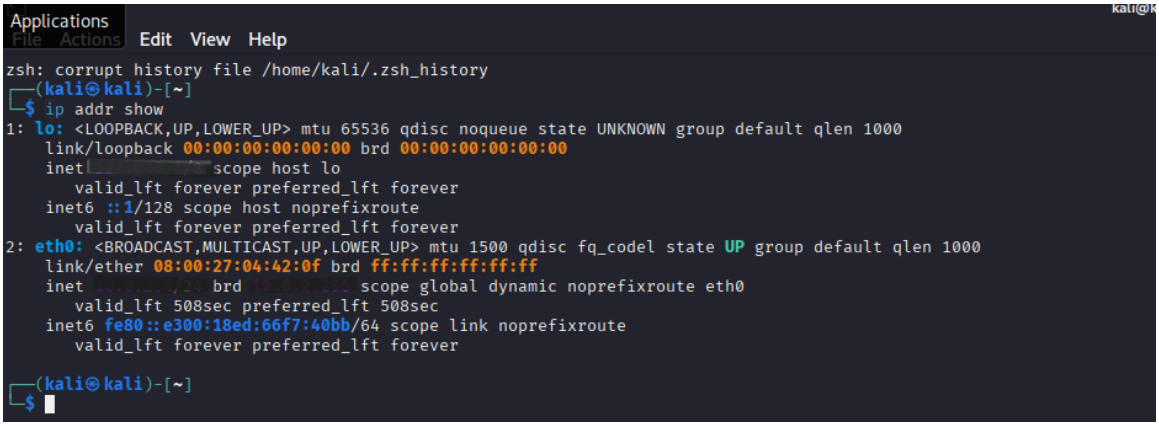
OS used to run scans: Linux .
Files produced: nmap_scan.txt , host_scan.txt

.

## 4. Methodology

Commands run (used to produce the attached nmap output):

Ip addr show
To find the ip address range

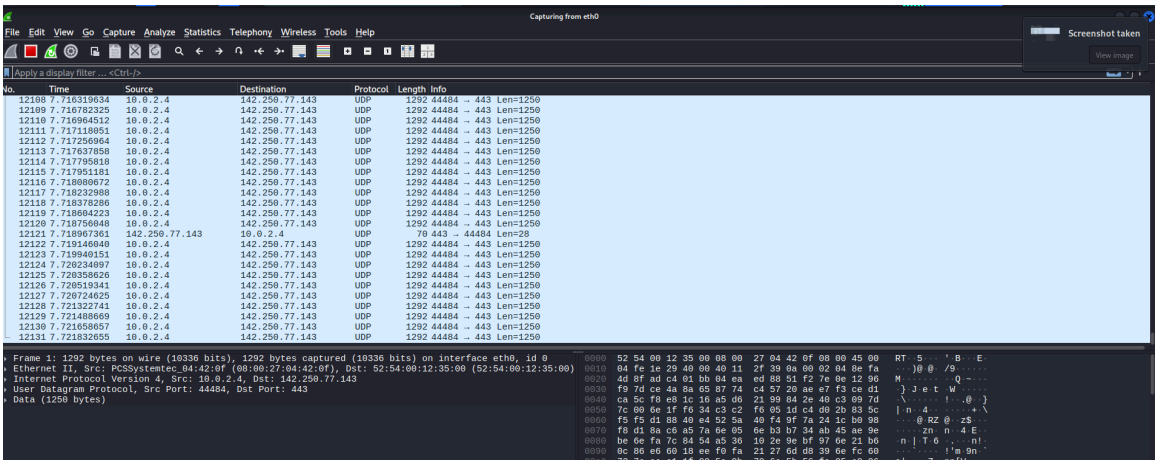



sudo nmap -sS -oN nmap_scan.txt <ip_address>

Notes: -sS performs a TCP SYN scan; -oN saves human-readable output.

```
└─$ nmap -sS 10.0.2.4/24 -oN nmap_scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-22 11:10 EDT
Nmap scan report for 10.0.2.1
Host is up (0.0014s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0026s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
2323/tcp open  3d-nfsd
7778/tcp open  interwise
8080/tcp open  http-proxy
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00054s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:DB:07:A8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
443/tcp open  https

Nmap done: 256 IP addresses (4 hosts up) scanned in 16.14 seconds
```

Sudo nmap -sS -oN host_scan.txt <ip_address>




## 5. Analysis & Findings

Summary of hosts discovered (from the nmap output):

- 10.0.2.1: port 53/tcp open (domain/DNS)
- 10.0.2.2: ports 135/tcp (msrpc), 445/tcp (microsoft-ds), 2323/tcp (3d-nfsd), 7778/tcp (interwise), 8080/tcp (http-proxy) open
- 10.0.2.3: all scanned ports filtered (no response)
- 10.0.2.4: port 443/tcp open (https)

These findings are taken directly from the uploaded scan file (nmap_scan.txt).

Interpretation & immediate observations:

1. DNS (53/tcp) on 10.0.2.1 - this host is running a DNS service or responding on the DNS port. If unnecessary, restrict or firewall.

2. 10.0.2.2 shows multiple typical Windows / network services:
  - 135 (msrpc) and 445 (SMB/microsoft-ds): commonly Windows RPC and file sharing services. These can expose file shares or remote procedure interfaces.
  - 2323 (3d-nfsd) and 7778 (interwise): less common services; may indicate custom or emulator services on virtual hosts.
  - 8080 (http-proxy): a web/proxy service — investigate the web application on that host.

3. 10.0.2.4 has HTTPS (443) open — web admin or web application likely running.

4. 10.0.2.3 did not respond to scans (filtered) - likely protected by firewall or offline.

## 7. Potential Security Risks

Based on the services found, the following risks may apply:

- Exposed SMB/RPC (10.0.2.2: 135, 445): risk of unauthorized file access and known historical vulnerabilities. Recommendation: restrict access to trusted subnets, disable SMBv1, apply patches, and require authentication.

- Open DNS (10.0.2.1:53): if configured as an open resolver it could be abused for amplification attacks. Recommendation: ensure the resolver is authoritative or restricted to internal clients.

- Web/proxy (8080) and HTTPS (443): web applications may contain vulnerabilities (XSS, SQLi, outdated components). Recommendation: run web app scanners (OWASP ZAP), ensure TLS config is secure, and patch software.

- Uncommon ports (2323, 7778): investigate service purpose and disable if unnecessary. Unknown services increase attack surface.

## 8. Recommendations (Actionable)

1. Disable or firewall unnecessary services.
2. Harden remote access: enable authentication, use strong passwords/keys, restrict by IP or VPN.
3. Patch and update services and OS images.
4. For web services: enforce HTTPS, test TLS (SSL Labs) and scan the app for vulnerabilities.
5. For DNS: ensure it is not an open resolver and rate-limit responses if needed.
6. Keep a regular scanning schedule and maintain logs of changes.

## 9. Deliverables & Attached Files

- nmap_scan.txt (raw nmap output) — included in submission
- wireshark_analysis.pcap — packet capture