Title: Network Reconnaissance & Mapping — Assessment Report
Author: Salmata Lamin
Date: *2025-11-04*
Environment: Kali Linux (VM), target network 10.10.10.0/24

Objective

The purpose of this assessment was to identify active hosts, open ports, and running services within the controlled enterprise subnet 10.10.10.0/24. The goal was to produce an initial asset inventory and identify obvious exposure points for follow-up enumeration and vulnerability scanning.

Tools & Environment

- OS: Kali Linux (VM)
- Tools: netdiscover, nmap (versions supporting -sS -sV -O -A), Zenmap (for visualization)
- Target network: 10.10.10.0/24 (virtual lab)

Host discovery — A subnet sweep was performed to detect live hosts using netdiscover:

```
sudo netdiscover -r 10.10.10.0/24
```

Port & service discovery — A comprehensive Nmap scan was executed to enumerate ports, services, and attempt OS fingerprinting:

```
sudo nmap -sS -sV -O -A 10.10.10.0/24 -oN Nmap_Results.txt
```

Output was saved to Results/Nmap_Results.txt. Zenmap was used for an optional graphical topology view.

Verification — Scan results were correlated with ARP tables and VM inventory to reduce false positives.

Findings (summary)

- Active hosts detected: 8

- Common open services: HTTP (80/tcp) on 3 hosts; SMB (445/tcp) on 2 hosts; SSH (22/tcp) on 2 hosts.

- Notable service/version findings:

Host 10.10.10.20 — Apache httpd 2.2.31 (end-of-life; may be vulnerable)

Host 10.10.10.12 — Microsoft Windows Server (SMBv1 enabled)

- OS fingerprinting: Mixture of Linux and Windows servers detected.

- Potential risks: Legacy webserver versions and SMBv1 exposure that could be exploited or used for lateral movement

Recommendations

1. **Patch web servers** — Upgrade Apache on affected hosts to a supported version and apply security patches.
2. **Harden SMB** — Disable SMBv1 where possible and enforce SMB signing and NTLMv2.
3. **Network segmentation** — Limit unnecessary cross-subnet access to services like SMB and management ports.
4. **Follow-up** — Perform targeted service enumeration and authenticated vulnerability scans (Nessus/OpenVAS) on identified critical hosts.

Appendix

- Command used for capture: sudo nmap -sS -sV -O -A 10.10.10.0/24 -oN Nmap_Results.txt
- Evidence files: Results/Nmap_Results.txt, Screenshots/Scan_Proof.png
- Report prepared by: Salmata Lamin