Project Report: Network Scanning and Vulnerability Analysis

Author: Ladan Abdi | Cybersecurity Analyst in Training

Date: November 2025

Methodology: CEH v13 Framework

1. Executive Summary

In this project I performed a structured network assessment on a controlled laboratory subnet. The goal was to identify active hosts, open ports and exposed services that could be abused by an attacker. Using industry standard reconnaissance tools I mapped the network, discovered running services and highlighted areas of potential risk. This report explains the approach and provides recommendations for improving security.

Objective: Determine the security posture of the target network by identifying reachable hosts and vulnerable or misconfigured services.

2. Lab Environment and Tools

Environment:

- Attacker machine: Kali Linux in a virtual machine

- Target network: 192.168.1.0/24 isolated lab subnet

- Target machine: Metasploitable 2 intentionally vulnerable Linux host

Tools used:

- Nmap for network discovery, port scanning and service version detection

- Wireshark to observe and validate scanning traffic

- Netdiscover for layer 2 host discovery using ARP

3. Methodology and Execution

Phase 1: Host discovery

I began by identifying which IP addresses were active on the subnet. I used Netdiscover for ARP based discovery and then confirmed the results with an Nmap ping sweep on the full range 192.168.1.0 to 192.168.1.255.

Example command:

nmap -sn 192.168.1.0/24

The sn switch tells Nmap to perform host discovery only. This reduces noise and focuses on identifying live hosts without performing a full port scan.

Phase 2: Service enumeration

After identifying the target host at 192.168.1.10 I performed a full TCP scan to identify open ports and the software versions running on those ports.

Example command:

nmap -sV -p- 192.168.1.10

Key options:

- sV probes open ports to determine service and version information

- p- instructs Nmap to scan all 65,535 TCP ports

The scan showed several important services listening on the target including FTP on port 21, SSH on port 22, HTTP on port 80 and SMB on port 445. Versions of these services are known to contain security weaknesses in default installations of Metasploitable 2.

Phase 3: Vulnerability identification

To identify specific weaknesses I used the Nmap Scripting Engine. The vulnerability category scripts run a set of checks for known issues that match the detected services and versions.

Example command:

nmap --script vuln 192.168.1.10

The results confirmed that the FTP service allowed anonymous login and that the SMB service version had known remote code execution issues. These findings represent meaningful risk if similar configurations exist in a production environment.

4. Security Recommendations

Based on the scan results and service enumeration the following actions are recommended to harden the system and reduce exposure:

1. Disable unnecessary services and close any ports that are not required.

2. Apply patches and updates to FTP, web and file sharing services to remove known vulnerabilities.

3. Restrict access to remote administration services such as SSH and SMB to trusted management networks only.

4. Disable anonymous FTP access and enforce strong authentication and logging for all remote connections.

5. Ethical Considerations

This assessment was performed in an isolated laboratory environment using systems that I own and control. No external or production networks were scanned. All work followed the principles of responsible disclosure and the EC Council Code of Ethics. Skills used in this lab are applied only in authorized contexts to improve security.

Conclusion

Network scanning and service enumeration are essential steps in understanding the security posture of any environment. When performed ethically and with proper authorization these activities help defenders identify weaknesses before attackers do. This project strengthened my practical skills in reconnaissance and vulnerability analysis and reinforced the importance of combining technical ability with strong ethical standards.