Cyber Security Internship Report

Cyber Security Internship – Task 9

Network Vulnerability Scanning – Experiment Report

Submitted by: Hetal Antala

Date : 30 / 01 / 2026

1. Introduction

Computer networks are the backbone of modern communication systems, connecting multiple devices and enabling data exchange. However, insecure network configurations and exposed services can become entry points for attackers. Network vulnerability scanning helps identify these weaknesses before they are exploited.

This task focuses on performing network reconnaissance and vulnerability assessment using industry-standard tools to detect open ports, running services, and potential risks within a local network.

---

2. What is Network Vulnerability Scanning?

Network vulnerability scanning is the process of examining network devices to discover open ports, active services, and security weaknesses that may be exploited by attackers.

It helps organizations:

- Identify exposed services
- Detect misconfigurations
- Reduce attack surface
- Strengthen overall security posture

---

3. Key Concepts

The following concepts are important in network scanning:

- Port Scanning – Identifying open communication ports
- Service Enumeration – Detecting running services and versions
- OS Detection – Identifying the operating system
- Vulnerability Detection – Finding known security weaknesses
- Risk Assessment – Evaluating the severity of threats

---

4. Tools Used

- **Nmap** – Network scanning and service detection
- **Nmap NSE Scripts** – Vulnerability analysis
- **Terminal / Command Prompt** – Command execution
- **Local Network Environment** – Testing platform

---

5. Environment Setup

The scanning environment consisted of a local private network. The system was connected to the same network as the target devices. Nmap was installed and configured to perform host discovery, port scanning, service enumeration, and vulnerability analysis.

Network Range: 192.168.56.0/24
Target Host: 192.168.56.102 (example)

---

6. Host Discovery

Host discovery was performed to identify active devices connected to the network.

Steps Performed

- Executed ping scan using Nmap
- Identified live hosts

Command Used

nmap -sn 192.168.56.0/24

Observation

Multiple active devices were detected on the network, confirming connectivity and available targets for scanning.

7. Port Scanning and Service Enumeration

Port scanning was conducted to detect open ports and running services on the target machine.

Steps Performed

- Scanned target IP for open ports
- Enumerated services and versions

Commands Used

nmap -sV 192.168.56.102

Observation

The scan revealed several open ports such as SSH and HTTP, indicating that remote access and web services were running on the system.

8. OS Detection

Operating system detection helps identify the type of system running on the target host.

Steps Performed

- Performed OS fingerprinting

Command Used

sudo nmap -O 192.168.1.5

Observation

The target machine was identified as a Linux-based operating system.

---

9. Vulnerability Analysis

Nmap vulnerability scripts were used to detect known security issues.

Steps Performed

- Executed vulnerability scan using NSE scripts
- Checked for outdated services and weak configurations

Command Used

sudo nmap --script vuln 192.168.56.102

Observation

Some services showed potential risks such as exposed SSH access and service version disclosure, which may be exploited by attackers.

---

10. Scan Results Summary

Port	State	Service	Risk Level
21	Open	FTP	Medium
22	Open	SSH	Medium
53	Open	Domain	Medium

---

11. Mitigation Techniques

To improve network security, the following measures are recommended:

- Close unused ports using firewall rules
- Update services to latest versions
- Use strong authentication for SSH
- Disable unnecessary services
- Perform regular vulnerability scans
- Monitor logs for suspicious activities

---

12. Importance of Network Scanning

- Detects vulnerabilities early
- Prevents unauthorized access
- Reduces attack surface
- Improves system security
- Helps maintain secure network infrastructure

---

13. Conclusion

This task provided practical exposure to network vulnerability scanning using Nmap. Host discovery, port scanning, service enumeration, OS detection, and vulnerability analysis were successfully performed. The experiment improved understanding of real-world reconnaissance techniques and strengthened hands-on cybersecurity skills required for roles such as SOC Analyst and Penetration Tester.

---

14. Appendix (Commands Used)

```
nmap -sn 192.168.56.0/24
nmap -sV 192.168.56.102
sudo nmap -O 192.168.56.102
sudo nmap -A 192.168.56.102
sudo nmap --script vuln 192.168.56.102
```
