Network Vulnerability Scanning Report

Using Nmap

1. Introduction

Network security is a critical aspect of modern computing systems as most devices today are connected to networks. Network Vulnerability Scanning is the process of identifying weaknesses in a network that could be exploited by attackers. These vulnerabilities may exist in the form of open ports, outdated services, misconfigurations, or insecure protocols.

This report focuses on performing a network vulnerability scan using **Nmap (Network Mapper)**, a widely used open-source security tool. Nmap helps in discovering hosts on a network, identifying open ports, detecting running services, and analyzing potential security risks. The purpose of this scan is to understand the security posture of a local network and highlight possible vulnerabilities.

---

2. Objectives

The main objectives of this network scanning activity are:

- To scan the local network and identify active hosts
- To detect open ports on target systems
- To identify running services and their versions
- To detect the operating system of devices
- To analyze potential vulnerabilities
- To document findings and assess security risks

---

3. Tool Used

Nmap (Network Mapper)
Nmap is a powerful network scanning and security auditing tool used by cybersecurity professionals. It supports various scanning techniques such as port scanning, service detection, OS fingerprinting, and vulnerability detection using scripts.

---

4. System and Network Environment

- **Operating System:** Windows / Linux
- **Network Type:** Local Area Network (LAN)
- **Scanning Tool:** Nmap
- **Target:** Devices within the local network
- **Scan Type:** TCP Scan, Service Detection, OS Detection, Vulnerability Scan

---

5. Methodology

5.1 Network Discovery

The first step was to scan the local network to identify all active devices connected to it. This helps in understanding the number of hosts and detecting any unknown devices.

5.2 Port Scanning

After identifying active hosts, port scanning was performed to find open ports. Open ports indicate services that are accessible and may become entry points for attackers if not properly secured.

5.3 Service and Version Detection

Service detection was used to identify the applications running on open ports along with their versions. This step is important to detect outdated or vulnerable services.

5.4 Operating System Detection

Nmap’s OS detection feature was used to identify the operating system of target machines. Knowing the OS helps in understanding possible OS-specific vulnerabilities.

5.5 Vulnerability Analysis

Using Nmap scripting engine (NSE), vulnerability scripts were executed to detect common security issues such as weak configurations or known service vulnerabilities.

5.6 Saving Scan Results

The scan results were saved in text and XML formats for documentation and further analysis.

---

6. Commands Used

Some of the commonly used Nmap commands during the scan include:

```
nmap -sn 192.168.1.0/24
nmap -sS 192.168.1.1
nmap -sV 192.168.1.1
nmap -O 192.168.1.1
nmap --script vuln 192.168.1.1
```

---

7. Results and Observations

The scan successfully identified multiple active devices within the local network. Several open ports were detected on the target system, along with the services running on them. Some services were found to be using older versions, which may contain known vulnerabilities.

Example observations:

- Port 22 (SSH) was open and accessible
- Port 80 (HTTP) was running a web service
- Operating system detection indicated a Linux-based system

These findings indicate that the system could be vulnerable if proper security measures are not implemented.

---

8. Risk Analysis

- **Open ports** increase the attack surface
- **Outdated services** may be exploited using known vulnerabilities
- **Unnecessary running services** can be misused by attackers

If these issues are not addressed, attackers could gain unauthorized access, perform data theft, or disrupt network services.

---

9. Recommendations

To improve network security, the following measures are recommended:

- Close unused or unnecessary ports
- Regularly update and patch services
- Use firewalls to restrict access
- Implement strong authentication methods
- Perform regular vulnerability scans

10. Conclusion

This project demonstrated the effective use of Nmap for network vulnerability scanning. By scanning the local network, identifying open ports, detecting services, and analyzing potential risks, valuable insights into the network’s security posture were obtained. Network vulnerability scanning is an essential security practice that helps organizations detect weaknesses early and take preventive actions. Regular scanning and proper security controls are necessary to maintain a secure network environment.