Network Port Scanning & Security Analysis Report

1. Introduction

Network scanning is a fundamental cybersecurity practice used to identify open ports, running services, and potential vulnerabilities on a system. By simulating the actions of an attacker, security analysts can proactively detect weaknesses before they are exploited. This project demonstrates how to use Nmap to scan a vulnerable machine (Metasploitable2) and analyze the risks associated with exposed services.

2. Methodology

Tools Used:

- Kali Linux (attacker machine)
- Nmap (network scanning tool)
- VirtualBox (virtualization environment)
- Metasploitable2 (target VM)

Scan Types:

- Basic Scan: Identify open ports.
- Service Detection Scan (-sV): Detect service versions.
- Vulnerability Scripts (--script vuln): Identify known weaknesses.

Environment Setup:

- Both VMs configured with Host-Only Adapter networking.
- Target IP identified using ifconfig.

3. Findings

The Nmap scans revealed several open ports and services on the target system:

Port	Service	Risk
21	FTP	Anonymous login enabled; cleartext credentials vulnerable to sniffing.
22	SSH	Susceptible to brute force attacks if weak passwords are used.
23	Telnet	Cleartext authentication; highly insecure and deprecated.
25	SMTP	Possible open relay; risk of email spoofing.

80	HTTP	Web attack surface (SQL injection, XSS, directory listing).
3306	MySQL	Default credentials may allow unauthorized database access.
445	SMB	File sharing service vulnerable to remote code execution in outdated versions.

Key Observations:

- Multiple services are outdated and expose known vulnerabilities (e.g., vsFTPd backdoor, Apache misconfigurations).

- Cleartext protocols (FTP, Telnet) significantly increase risk of credential theft.

- Web server (HTTP) provides a large attack surface for common web exploits.

4. Recommendations

- Disable unused ports/services: Shut down Telnet, anonymous FTP, and unnecessary services.

- Use firewalls: Restrict access to critical services (SSH, MySQL) to trusted IPs only.

- Patch and update services: Apply latest security updates to FTP, SSH, Apache, MySQL, and SMB.

- Enforce strong authentication: Use SSH keys instead of passwords; disable root login.

- Encrypt communications: Replace FTP/Telnet with secure alternatives (SFTP, SSH).

- Web hardening: Disable directory listing, hide server banners, and implement security headers.

- Continuous monitoring: Regular vulnerability scans and log analysis to detect anomalies.

5. Conclusion

This project demonstrates how Nmap can be used to identify open ports and services on a vulnerable system. The findings highlight the importance of proactive security measures, as exposed services and outdated configurations pose significant risks. By disabling unnecessary services, applying patches, and enforcing strong security controls, organizations can reduce their attack surface and strengthen overall network resilience.