Nmap Vulnerability Scanning Project Report

Project Objective

To demonstrate the use of Nmap as a vulnerability scanning tool against a local host (192.168.29.99). The project identifies open ports, services, and potential vulnerabilities using Nmap scripts.

Target Information

Target IP: 192.168.29.99

Assumption: The target is a machine in a private lab environment with known vulnerable services for testing purposes.

Tools Used

Operating System: Kali Linux

Tool: Nmap

Nmap Version: 7.94 (or latest available)

Optional GUI: Zenmap (for visualization)

Step-by-Step Process

- Ping Scan - Check Host Availability

Command: nmap -sn 192.168.29.99

- Port Scanning - Identify Open Ports

Command: nmap -sS -p- 192.168.29.99

Nmap Vulnerability Scanning Project Report

- Service and Version Detection

Command: nmap -sV 192.168.29.99

- Operating System Detection

Command: nmap -O 192.168.29.99

- Aggressive Scan (All-in-One)

Command: nmap -A 192.168.29.99

- Vulnerability Scan Using NSE Scripts

Command: nmap --script vuln 192.168.29.99

Sample Scan Output Summary (Fictional Example)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 7.2p2

80/tcp open http Apache httpd 2.4.18

139/tcp open netbios-ssn Samba smbd 3.X - 4.X

Host script results:

| ftp-vsftpd-backdoor: Vulnerable version detected!

| http-dombased-xss: Potential DOM-based XSS vulnerability found.

Nmap Vulnerability Scanning Project Report

| smb-vuln-ms17-010: VULNERABLE: EternalBlue

Result Analysis

- FTP service running vulnerable version of vsftpd 2.3.4 (backdoor exploit known).
- HTTP service might be prone to DOM-based XSS.
- Samba is vulnerable to MS17-010 (EternalBlue) - critical.

Recommendations

- Upgrade vulnerable services (e.g., vsftpd, Apache, Samba).
- Apply system and security patches.
- Restrict access to sensitive ports via firewall rules.
- Implement vulnerability management and periodic scans.

Conclusion

Nmap, though primarily a port scanner, can be used effectively as a basic vulnerability scanner when combined with NSE scripts. It provides a lightweight and fast way to identify common misconfigurations and outdated services.