Nmap Scan Report

Prepared by: Prashanth Yadav

# Objective

The purpose of this task was to perform a comprehensive network scan using Nmap to identify open ports, running services, and potential vulnerabilities on the target machine (Metasploitable2). The scan helps understand the network exposure and assists in identifying possible attack surfaces.

# Nmap Commands Used

|  |  |
| --- | --- |
| **Basic Scan** | **nmap <target-ip>** |
| Service Version Detection | nmap -sV 192.168.0.199 |
| Operating System Detection | nmap -O 192.168.0.199 |
| Aggressive Scan | nmap -A 192.168.0.199 |
| Vulnerability Script Scan | nmap --script vuln 192.168.0.199 |

# Sample Scan Results

Target IP: 192.168.0.199 Host Status: Up (0.0020s latency) Open Ports and Services: -

21/tcp — FTP — vsftpd 2.3.4 - 22/tcp — SSH — OpenSSH 4.7p1 Debian 8ubuntu1 23/tcp — Telnet — Linux telnetd - 25/tcp — SMTP — Postfix smtpd - 80/tcp — HTTP — Apache httpd 2.2.8 - 139/tcp — NetBIOS — Samba smbd 3.x - 445/tcp — SMB — Samba smbd 3.x - 3306/tcp — MySQL — MySQL 5.0.51a - 5432/tcp — PostgreSQL — PostgreSQL 8.3.0 - 5900/tcp — VNC — VNC protocol 3.3 - 6667/tcp — IRC —

UnrealIRCd Detected Operating System: Linux 2.6.8 – 2.6.32 (likely Metasploitable2)

# Vulnerability Insights

Nmap scripting engine (NSE) identified multiple medium and high severity vulnerabilities: FTP service running vsftpd 2.3.4 contains a known backdoor vulnerability. - OpenSSH and

Telnet services allow brute-force authentication attempts. - Apache web server version 2.2.8 is outdated and prone to multiple CVEs (CVE-2007-6750, CVE-2008-0455). - SMB service allows null sessions, leading to information disclosure.

# Analysis and Recommendations

The scan reveals that the target system (Metasploitable2) is intentionally vulnerable and hosts multiple insecure services. To secure a real-world system, the following measures are recommended: 1. Disable or restrict FTP, Telnet, and SMB services. 2. Use SSH with strong key-based authentication. 3. Keep software and OS up-to-date with security patches. 4. Implement firewall rules to block unused ports. 5. Regularly conduct vulnerability scans to identify and fix exposures early.

# Conclusion

Nmap successfully identified multiple open ports and outdated services on the target system. This task demonstrates how vulnerability scanning and service fingerprinting can reveal attack surfaces in a controlled environment. These findings can be used to strengthen security configurations in production networks.