Nessus Vulnerability Scan Report (Simulated)

Target IP: 192.168.50.1

Scan Date: 26-06-2025 15:37:34

Scan Tool: Simulated Nessus (For Internship Report)

Detected Open Ports and Services:

[Medium] Port 22/tcp - OpenSSH 7.9

- Vulnerability: Weak SSH Algorithms Supported
- CVE: CVE-2018-15473

[High] Port 80/tcp - Apache HTTPD 2.4.29

- Vulnerability: Directory Traversal Vulnerability
- CVE: CVE-2021-41773

[Critical] Port 139/tcp - Samba smbd 3.6.25

- Vulnerability: Remote Code Execution Vulnerability
- CVE: CVE-2017-7494

[Medium] Port 443/tcp - OpenSSL 1.1.1

- Vulnerability: TLS 1.0 Protocol Detection
- CVE: CVE-2009-3555

[High] Port 3306/tcp - MySQL 5.7.29

- Vulnerability: Authentication Bypass
- CVE: CVE-2016-6662

Recommendations:

- Update all vulnerable services to the latest stable versions.
- Disable weak encryption protocols (e.g., TLS 1.0).
- Use strong SSH configurations and limit access by IP.

- Apply OS and software patches regularly.

- Use a firewall to restrict unnecessary open ports.