Nessus Essentials - Sample Vulnerability Scan Report

Scan Summary

Target: 127.0.0.1 (localhost)

Scan Type: Basic Network Scan

Scanner: Nessus Essentials (Tenable)

Date: Sample Report (June 2025)

Vulnerabilities Detected

OpenSSH User Enumeration (High)

CVE: CVE-2023-38408

Description: OpenSSH allows remote attackers to determine valid usernames.

Git Configuration Vulnerability (Medium)

CVE: CVE-2022-24765

Description: Git may unintentionally execute code in user directories.

Apache Path Traversal (High)

CVE: CVE-2021-41773

Description: Exploitable in misconfigured Apache setups; allows file disclosure.

ICMP Vulnerability (FAD) (Medium)

CVE: CVE-2020-25705

Description: Improper handling of ICMP packets in some Linux kernels.

SMBv1 Remote Code Execution (EternalBlue) (Critical)

CVE: CVE-2017-0143

Description: Outdated Windows shares allow remote code execution (if present).

SSL/TLS Certificate Expiry (Info)

CVE: -

Description: Certificate is self-signed or expired.

Severity Summary

Critical: 1

High: 2

Medium: 2

Info: 1

Suggested Remediation

- Update OpenSSH to the latest secure version.

- Disable SMBv1 on legacy Windows systems.

- Apply Apache security patches.

- Audit and renew SSL/TLS certificates as needed.