Sample Vulnerability Scan Report

Tool Used: Tenable Nessus Essentials
Scan Date: 08 August 2025
Scan Target: 127.0.0.1 (Localhost)
Scan Profile: Advanced Scan – Full System
Scanner Version: Nessus Essentials v10.7.2

1. Scan Summary

Field	Value
Scan Name	Localhost Nessus Vulnerability Scan
Target IP	127.0.0.1
Total Vulnerabilities	22
Critical	3
High	4
Medium	7
Low	5
Info	3
Duration	14 mins 18 sec

2. Top Vulnerabilities (Summary)

Severity	CVE ID	Vulnerability Name	Affected Component	Risk
Critical	CVE-2017-0144	Microsoft SMBv1 RCE (EternalBlue)	SMB Service (Port 445)	RCE
Critical	CVE-2021-3156	Sudo Buffer Overflow (Baron Samedit)	Sudo binary	Priv. Esc.
Critical	CVE-2022-22965	Spring Framework RCE (Spring4Shell)	Apache Tomcat App	RCE
High	CVE-2020-1472	Zerologon Netlogon Privilege Escalation	Windows RPC	Priv. Esc.
High	CVE-2019-0708	Remote Desktop Services RCE (BlueKeep)	RDP Service (Port 3389)	RCE
Medium	-	Outdated OpenSSH version	OpenSSH 7.2	Info Leak
Medium	CVE-2021-3449	OpenSSL Denial of Service Vulnerability	OpenSSL 1.1.1	DoS

3. Detailed Vulnerability Example

Vulnerability: Microsoft SMBv1 Remote Code Execution (EternalBlue)
Severity: Critical
CVE ID: CVE-2017-0144
Port: 445/tcp
Description: A remote code execution vulnerability exists in SMBv1, enabling unauthenticated attackers to execute arbitrary code via crafted packets.
Impact: Full system compromise
Affected Component: smbd (Server Message Block Daemon)
Exploit Available: Yes (used in WannaCry attack)
Solution: Disable SMBv1 and apply Microsoft patch KB4012598.

4. Recommendations

• Patch all critical vulnerabilities immediately.
• Update outdated software packages (OpenSSH, OpenSSL, Apache).
• Restrict access to sensitive ports (RDP 3389, SMB 445) via firewall.
• Disable unused services like Telnet, FTP, and SMBv1.
• Schedule regular Nessus scans every month.