Simulated OpenVAS Vulnerability Scan Report

Scan Target: 127.0.0.1

Scan Date: May 29, 2025

Scan Duration: 47 minutes

Summary of Vulnerabilities

- Critical: 2
- High: 3
- Medium: 4
- Low: 6
- Info: 10

Top Critical Vulnerabilities

1. CVE-2023-27350 - PaperCut NG Remote Code Execution
   - Severity: Critical
   - Affected Service: PaperCut Server (port 9191)
   - Fix: Update to PaperCut NG 22.1.3 or later

2. CVE-2021-44228 - Apache Log4j2 RCE ("Log4Shell")
   - Severity: Critical
   - Affected Service: Java-based Web Server
   - Fix: Upgrade Log4j to version 2.17.1+

3. CVE-2022-1388 - F5 BIG-IP iControl REST Auth Bypass
   - Severity: High
   - Fix: Upgrade BIG-IP firmware

Simulated OpenVAS Vulnerability Scan Report

4. Open SSH Port Detected (Port 22)

- Severity: High
- Risk: Brute force login attempts possible
- Fix: Restrict SSH to internal IPs or use keys

5. SMBv1 Enabled

- Severity: High
- Risk: Vulnerable to EternalBlue (used in WannaCry)
- Fix: Disable SMBv1 protocol