Sample Reports

Below are two sample report formats for documenting the vulnerability assessment: a **detailed report** and a **summary report** . a scan of a local machine (127.0.0.1) using OpenVAS.

1. Detailed Vulnerability Assessment Report

Title: Vulnerability Assessment Report for Local Machine

Date: May 29, 2025

Tool Used: OpenVAS (Greenbone Vulnerability Management)

Target: 127.0.0.1 (Local Machine, Ubuntu 22.04)

1. Executive Summary

A full vulnerability scan was conducted on the local machine (127.0.0.1) on May 29, 2025, using OpenVAS. The scan identified 12 vulnerabilities: 3 high-severity, 5 medium-severity, and 4 low-severity. Critical issues include an outdated Log4j library (CVE-2021-44228), an unpatched OpenSSL version (CVE-2020-1971), and an exposed SMB service on port 445. Immediate remediation is recommended for high-severity issues to prevent potential remote code execution and denial-of-service attacks.

2. Scan Details

- **Scan Date/Time**: May 29, 2025, 17:00–18:15 IST

- **Scan Configuration**: Full and Fast (all TCP/UDP ports, comprehensive NVTs)

- **Target System**: Ubuntu 22.04, hosting Apache (port 8080), OpenSSL (port 443), SMB (port 445)

- **Scan Duration**: minutes

3. Findings

Vulnerability	**CVE ID**	**Severity**	**Affected Service/Port**	**Description**	**Impact**	**Mitigation**
Log4j RCE	CVE-2021-44228	High (CVSS 10.0)	Apache (port 8080)	Remote code execution via JNDI lookups in Log4j 2.14.0	Complete system compromise	Update to Log4j 2.17.0; set `log4j2.formatMsgNoLookups=true`
OpenSSL Buffer Overflow	CVE-2020-1971	Medium (CVSS 5.9)	HTTPS (port 443)	Buffer overflow in OpenSSL 1.1.0, exploitable for DoS	Service disruption	Update to OpenSSL 1.1.1; disable TLS 1.0/1.1
SMBv1 Enabled	N/A	Medium	SMB (port 445)	Outdated SMBv1 protocol vulnerable to exploits (e.g., EternalBlue)	Data theft, ransomware	Disable SMBv1; restrict port 445 via firewall
Open SSH Port	N/A	Low	SSH (port 22)	Open port with strong configuration, but unnecessary exposure	Potential brute-force attacks	Restrict SSH to specific IPs; use key-based authentication

4. Recommendations

- **Immediate Actions**:
  - Patch Log4j to version 2.17.0 or later (source: Apache Log4j security advisory).
  - Update OpenSSL to the latest version (`sudo apt install openssl`).
  - Disable SMBv1 (`sudo systemctl disable smb`) and block port 445 (`ufw deny 445`).
- **Long-Term Actions**:
  - Implement regular patch management using tools like `apt` or WSUS.
  - Configure a host-based firewall (e.g., `ufw`) to limit open ports.
  - Monitor system logs for suspicious activity using tools like `fail2ban`.

5. Conclusion

The scan revealed critical vulnerabilities that could allow attackers to compromise the system. Prompt remediation, especially for high-severity issues, is essential. A follow-up scan is recommended after applying fixes to verify resolution.

2. Summary Vulnerability Report

Vulnerability Scan Summary

Date: May 29, 2025

Target: Local Machine (127.0.0.1)

Tool: OpenVAS

Key Findings:

- **Total Vulnerabilities**: 12 (3 High, 5 Medium, 4 Low)
- **Critical Issues**:
  1. **Log4j RCE (CVE-2021-44228)**: High risk, update to Log4j 2.17.0.
  2. **OpenSSL Vulnerability (CVE-2020-1971)**: Medium risk, update OpenSSL.
  3. **SMBv1 Enabled (Port 445)**: Medium risk, disable SMBv1.

Additional Research on Common Vulnerabilities

To provide deeper insight, I’ve researched the vulnerabilities listed in the sample reports using authoritative sources (NIST NVD, MITRE CVE, and cybersecurity blogs). Below is detailed information on each, including mitigations and their relevance to a local machine.

1. Log4j Remote Code Execution (CVE-2021-44228)

- **Source**: NIST NVD (https://nvd.nist.gov/vuln/detail/CVE-2021-44228), Apache Log4j Security Advisory

- **Details**:

  - Affects Apache Log4j versions 2.0 to 2.14.1.

  - Allows remote code execution via malicious JNDI lookups, often exploited through user inputs in web applications (e.g., Apache Solr, Tomcat).

  - CVSS Score: 10.0 (Critical).

  - Impact: Full system compromise, including data theft, ransomware, or persistence.

- **Mitigations**:

  - **Immediate**: Update to Log4j 2.17.0 or later (`mvn dependency:tree` to check dependencies).

  - **Temporary**: Set `log4j2.formatMsgNoLookups=true` or remove JNDI classes (`zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class`).

  - **Network**: Block outbound LDAP/RMI traffic (ports 389, 1099) using a firewall.

- **Research Notes**:

  - Posts on X (searched May 29, 2025) highlight ongoing exploitation attempts, even in 2025, due to unpatched systems.

  - BleepingComputer (2021–2022 archives) reported widespread attacks, emphasizing patch urgency.

  - Common on local machines running Java-based services (e.g., development environments).

2. OpenSSL Buffer Overflow (CVE-2020-1971)

- **Source**: NIST NVD (https://nvd.nist.gov/vuln/detail/CVE-2020-1971), OpenSSL Security Advisory

- **Details**:

  - Affects OpenSSL versions 1.0.2–1.1.0.

  - Buffer overflow in X.509 certificate parsing, potentially leading to denial-of-service (DoS) attacks.

  - CVSS Score: 5.9 (Medium).

  - Impact: Service crashes, potential for limited code execution in specific configurations.

- **Mitigations**:

  - **Immediate**: Update to OpenSSL 1.1.1 or 3.0 (`sudo apt install openssl` or compile from source).

  - **Temporary**: Disable affected protocols (TLS 1.0/1.1) in `/etc/ssl/openssl.cnf`: `MinProtocol = TLSv1.2`.

  - **Monitoring**: Use tools like `nmap` to verify exposed SSL/TLS services.

- **Research Notes**:

  - OpenSSL vulnerabilities are common in local setups with outdated web servers (e.g., Apache, Nginx).

  - Cybersecurity blogs (e.g., The Hacker News) stress regular updates, as OpenSSL is critical for HTTPS services.

  - Check for affected versions using `openssl version` on the local machine.

3. SMBv1 Enabled (Port 445)

- **Source**: Microsoft Security Guidance, CISA Alerts

- **Details**:

  - SMBv1 is an outdated protocol vulnerable to exploits like EternalBlue (used in WannaCry ransomware).

  - Often enabled by default on older Windows systems or misconfigured Linux Samba servers.

  - Severity: Medium (no CVE, but high risk if exploited).

  - Impact: Remote code execution, data theft, or lateral movement in networks.

- **Mitigations**:

  - **Immediate**: Disable SMBv1:

    - Linux: Edit `/etc/samba/smb.conf` to include `server min protocol = SMB2`; restart Samba (`sudo systemctl restart smbd`).

    - Windows: Run `Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol`.

  - **Network**: Block port 445 (`ufw deny 445` or Windows Firewall rule).

  - **Monitoring**: Use `nmap 127.0.0.1 -p 445` to confirm the port is closed.

- **Research Notes**:

  - CISA (https://www.cisa.gov) recommends disabling SMBv1 due to its obsolescence and exploitability.

  - X posts from 2023–2025 show persistent SMB-based attacks targeting misconfigured servers.

  - Common on local machines running file-sharing services for development or testing.

4. Open SSH Port (Port 22)

- **Source**: OpenSSH Documentation, OWASP Guidelines

- **Details**:

  - Open SSH ports are low risk if configured securely (e.g., key-based authentication, strong passwords).

  - Unnecessary exposure increases the risk of brute-force attacks.

  - Severity: Low.

  - Impact: Unauthorized access if weak credentials are used.

- **Mitigations**:

  - Restrict SSH access: Edit `/etc/ssh/sshd_config` to set `PermitRootLogin no` and `AllowUsers <username>`.

  - Use key-based authentication: Generate keys (`ssh-keygen`) and disable password logins (`PasswordAuthentication no`).

  - Firewall: Allow SSH only from trusted IPs (`ufw allow from <trusted_ip> to any port 22`).

- **Research Notes**:

  - OWASP (https://owasp.org) emphasizes SSH hardening for servers exposed to the internet.

  - Tools like `fail2ban` can mitigate brute-force attempts by banning malicious IPs.
  - Common on local machines used for development or remote access testing.

Additional Research Notes

- **Sources Used**:
  - **NIST NVD**: Primary source for CVE details, CVSS scores, and affected versions.
  - **MITRE CVE**: Provides exploit references and attack vectors.