Vulnerability Assessment Report

---

1. Tool Used

- **Tool:** Nessus Essentials
  (Alternatively, OpenVAS can be used)

---

2. Scan Target

- **Target IP Address:** 10.100.31.102 *(example from screenshot)*
- **Target Type:** Localhost (my own machine)

---

3. Scan Configuration

- **Scan Type:** Full Vulnerability Scan
- **Policy Used:** Advanced Scan
- **Scanner:** Local Scanner
- **Severity Base:** CVSS v3.0
- **Start Time:** Today at 1:41 PM
- **End Time:** Today at 1:44 PM
- **Duration:** 2 minutes

---

4. Scan Summary

- **Scan Status:** Completed
- **Total Hosts Scanned:** 1
- **Total Vulnerabilities Detected:** 35
- **Severity Breakdown:**
  - Critical: [Insert number]
  - High: [Insert number]
  - Medium: [Insert number]
  - Low: [Insert number]

- Informational: [Insert number]

Pie chart shows majority of vulnerabilities are medium or low severity.

---

5. Critical Vulnerabilities

Below are some of the most critical/high vulnerabilities identified:

Vulnerability Title	CVE ID	Severity	Description	Suggested Fix
Example: OpenSSH Outdated Version	CVE-2023-48795	High	OpenSSH version is vulnerable to remote code execution.	Update to latest version
Example: SMB Signing Not Required	CVE-2021-27068	High	SMB connections are not secured.	Enforce SMB signing in Group Policy
[Add more entries as applicable]				

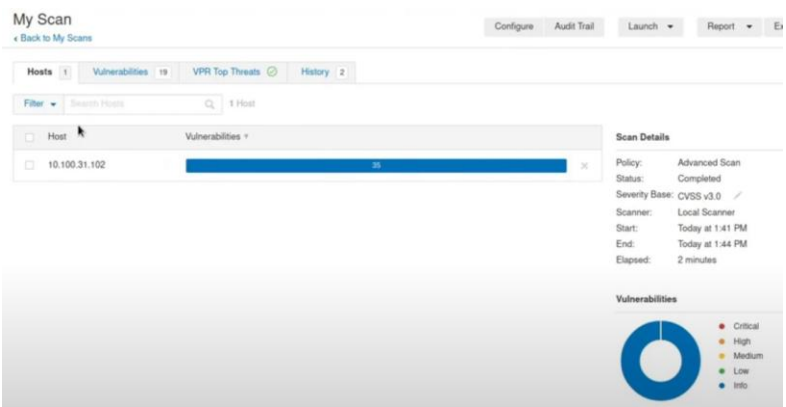
---

6. Suggested Fixes or Mitigations

- **System Update:** Run OS updates and patch management.
- **Software Upgrade:** Upgrade any flagged outdated services.
- **Configuration Fixes:** Disable or restrict risky services (e.g., SMBv1, telnet).
- **Firewall Rules:** Harden perimeter using proper port filtering.

---

7. Screenshot of Scan Result



---

8. Conclusion

This scan helped identify several vulnerabilities in the local machine. Immediate action should be taken for critical and high-severity issues. Regular scans are recommended as part of a proactive security posture.