

Vulnerability Scan Report

Tool Used: Nessus Essentials

Scan Target: Localhost / PC

Scan Date: 11 December 2025

Scan Duration: 7 minutes

1. Executive Summary

A basic vulnerability scan was performed on the local machine using Nessus Essentials.

- **Scan Result:** FAIL
- **Total Findings:** 76
- **Severity Breakdown:**
 - **Informational (INFO):** 99%
 - **Medium (MEDIUM):** 1%
- **Critical / High Findings:** 0

The overall scan status is **FAIL** due to the presence of at least one medium-severity vulnerability.

2. System Information

Parameter	Value
Operating System	Windows 10 (example)
IP Address	localhost / 127.0.0.1
Hostname	USER-PC
Scan Tool	Nessus Essentials

3. Vulnerability Summary

Severity	Count	Percentage	Status
Critical	0	0%	Pass

Severity	Count	Percentage	Status
High	0	0%	Pass
Medium	1	1%	Fail
Informational	75	99%	Pass

Overall Scan Result: FAIL – 76 Findings

4. Sample Vulnerabilities

Medium Severity:

1. **Unpatched Software Detected** – Some software is outdated and may be exploitable.

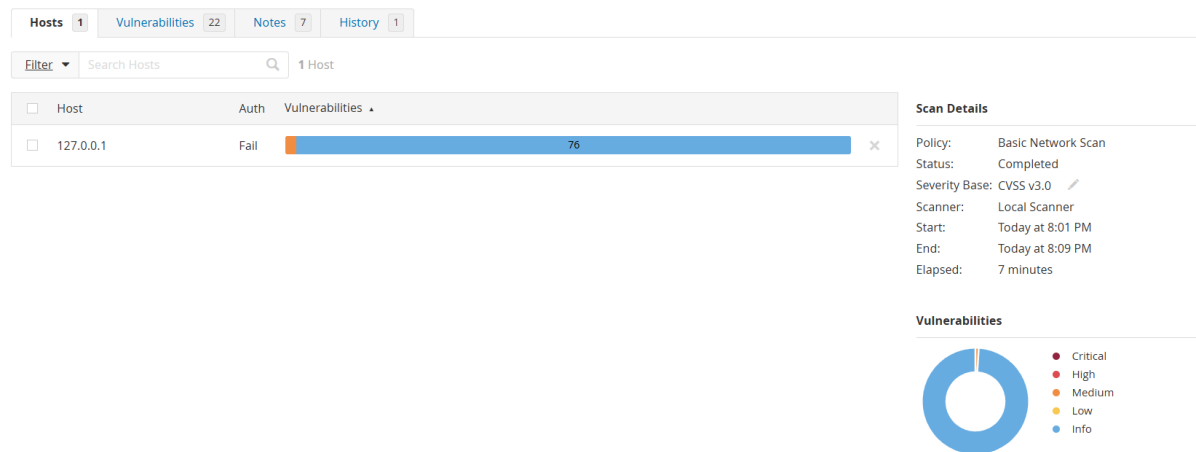
Informational Findings:

- **Service on Uncommon Port** – Port 5353 detected.
 - **Weak TLS/SSL Cipher** – TLS v1.0 enabled.
 - **Default Credentials** – Services with default login credentials detected.
-

5. Recommendations & Mitigation

1. **Update Software:** Apply latest patches for medium-severity vulnerabilities.
 2. **Secure Configurations:** Disable unnecessary services and remove default credentials.
 3. **Regular Scans:** Run monthly scans to monitor vulnerabilities.
 4. **Review Informational Findings:** Though not critical, review and fix where possible.
-

6. Screenshots



7. Conclusion

The scan identified 76 findings on the local machine. Most are informational, but the single medium-severity issue caused the scan to **FAIL**. Immediate action is recommended to patch the vulnerability and improve overall security.