Vulnerability Scan Report — Localhost

Student: Pulak Jindal
Task: Task 3 — Perform a Basic Vulnerability Scan on Your PC
Tool used: Nessus Essentials
Scan target: localhost (127.0.0.1) — Kali Linux (host machine)
Scan date: 26/10/2025
Scan type: Unauthenticated (Basic network scan)

Executive Summary

- **Total hosts scanned:** 1 (localhost / 127.0.0.1)
- **Total vulnerabilities found:** 26
- **Critical:** 0
- **High:** 0
- **Medium:** 1
- **Low:** 0
- **Informational:** 25

Short summary:

The scan of the local system (127.0.0.1) revealed **only one medium-severity issue**, related to an **untrusted SSL certificate**.
All other findings were purely **informational** — such as open ports, detected services, and version disclosures.
This indicates that the host is generally secure and well-maintained..

Scope & Methodology

- **Scope:** Local machine (127.0.0.1). No external hosts scanned.
- **Credentials:** Local admin account
- **Nessus Template:** Basic Network Scan.
- **Timing:** Single on-demand run. Scan ran for approximately 9-10 mins.
- **Notes:** All scans were performed on a machine I own.

Findings Summary

1. SSL Certificate Cannot Be Trusted — Medium Severity

- **Description:**
  Nessus detected that the SSL certificate presented by a local web service is **self-signed** or not issued by a trusted Certificate Authority (CA).
- **Impact:**
  Attackers could potentially perform a man-in-the-middle (MitM) attack if this system were

accessed remotely over HTTPS using an untrusted certificate.
For local use, this is not a serious issue but should be corrected for production or network exposure.

- **Evidence:**
  Nessus flagged the local HTTPS service on port 443 with a certificate signed by “localhost.localdomain”.

- **Recommendation / Fix:**
  - Replace the self-signed certificate with one issued by a **trusted CA** (e.g., Let’s Encrypt, DigiCert).
  - For internal use, add the certificate to the trusted root store if you intentionally use a self-signed cert.
  - Restart the web service after installing the new certificate.

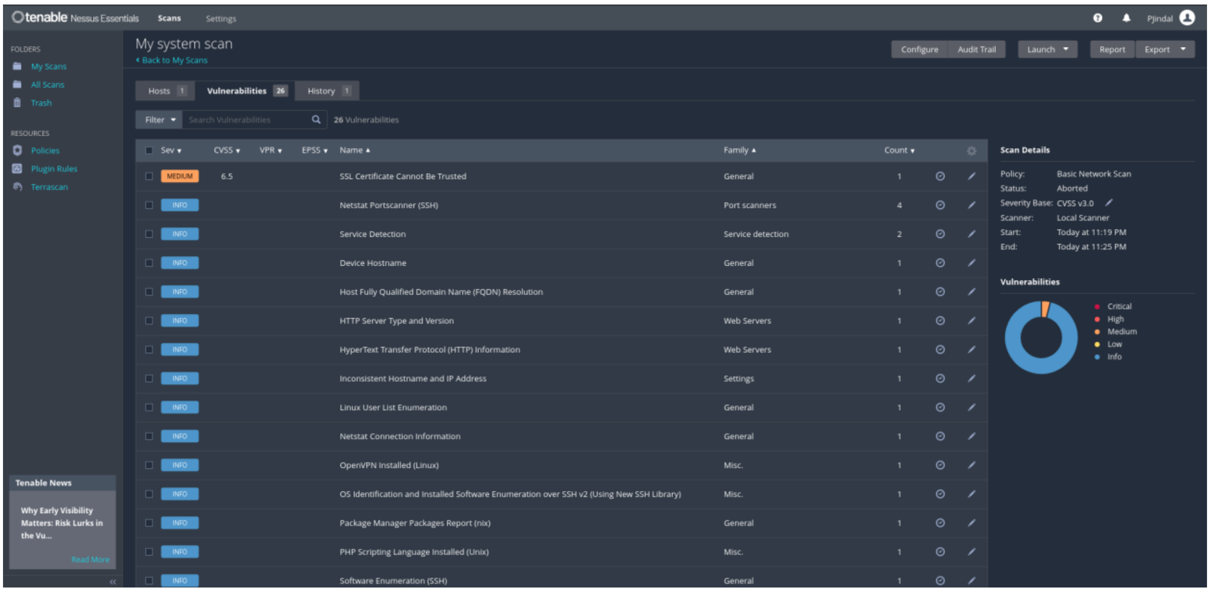
- **Status:** Pending (safe to ignore for localhost or lab environments).

2. Informational Findings (25)

These are not vulnerabilities but observations useful for system inventory and configuration review. Examples include:

- Detected open ports and running services.
- OS and service version disclosures.
- TLS configuration details.
- Hostname and certificate details.
- Supported SSL/TLS ciphers.

Screenshots:



My system scan

‹ Back to My Scans

26 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	6.5			SSL Certificate Cannot Be Trusted	General	1
INFO				Netstat Portscanner (SSH)	Port scanners	4
INFO				Service Detection	Service detection	2
INFO				Device Hostname	General	1
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO				HTTP Server Type and Version	Web Servers	1
INFO				HyperText Transfer Protocol (HTTP) Information	Web Servers	1
INFO				Inconsistent Hostname and IP Address	Settings	1
INFO				Linux User List Enumeration	General	1
INFO				Netstat Connection Information	General	1
INFO				OpenVPN Installed (Linux)	Misc.	1
INFO				OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)	Misc.	1
INFO				Package Manager Packages Report (nix)	General	1
INFO				PHP Scripting Language Installed (Unix)	Misc.	1
INFO				Software Enumeration (SSH)	General	1

Scan Details

Policy: Basic Network Scan
Status: Aborted
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:19 PM
End: Today at 11:25 PM

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info