

TASK – 3 ELEVATE LABS : Perform a Basic Vulnerability Scan on Your PC.

OBJECTIVE : Use free tools to identify common vulnerabilities on your computer

NAME : PRIYA ROSE

DATE OF SUBMISSION : 07 – 08 -2025

Vulnerability Assessment Report

Scan Information

Field	Details
Tool	Tenable Nessus Essentials
Scan Name	priya 2
Scan Policy	Basic Network Scan
Scanner	Local Scanner
Scan Target	localhost (127.0.0.1)
Start Time	08:36 PM, 07-Aug-2025
End Time	08:44 PM, 07-Aug-2025
Elapsed Time	8 minutes
Severity Base	CVSS v3.0

Vulnerability Summary

Severity Level Count

Critical	0
High	0
Medium	1
Low	0
Info	20

Critical or Noteworthy Vulnerabilities and Fixes

i 1. SMB Signing Not Required (Severity: Medium, CVSS 5.3)

- **Risk:** Allows man-in-the-middle (MITM) attacks on SMB traffic.
- **Fix/Mitigation:**
 - **Windows:** Enforce SMB signing.
 - Open gpedit.msc → Local Computer Policy → Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options.
 - Enable: Microsoft network client: Digitally sign communications (always) and Microsoft network server: Digitally sign communications (always).
 - **Restart** the machine for changes to take effect.
 - **Alternative:** Block SMB ports (135–139, 445) in your firewall if not needed

■ 2. SSL (Multiple Issues) – Mixed Severity

- **Risk:** May include use of weak SSL versions (e.g., SSLv2/3), weak ciphers, or missing secure settings.
- **Fix/Mitigation:**
 - Disable old SSL versions (SSLv2, SSLv3) and **prefer TLS 1.2 or 1.3**.
 - Reconfigure the affected service (Apache, Nginx, etc.) to:

```
apache
```

```
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite HIGH:!aNULL:!MD5
```

-
- Use tools like SSL Labs Test to verify changes.

i 3. SMB (Multiple Issues) – Info

- **Fix:** Review for:
 - SMB version (use SMBv3 if possible).
 - Disable SMBv1 using:

```
powershell
```

```
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
```

i 4. HTTP (Multiple Issues) – Info

- **Fix:**
 - Use HTTPS only.
 - Set HTTP headers like X-Frame-Options, X-Content-Type-Options, and Content-Security-Policy.
 - Use secure cookie flags (HttpOnly, Secure).

i 5. TLS (Multiple Issues) – Info

- **Fix:**
 - Only allow **TLS 1.2 and 1.3**.
 - Disable weak ciphers.
 - Use updated libraries (e.g., OpenSSL)

i 6. Netstat Portscanner (SSH) – Info

- **Note:** This isn't a vulnerability. It just shows which ports are open.
- **Fix:**
 - Close unused ports using firewall rules.
 - For SSH: Use key-based authentication, change default port if needed.

i 7. DCE Services Enumeration – Info

- **Fix:** DCE (Distributed Computing Environment) services should be disabled if not used.
 - Use Windows Features or services.msc to stop them.

i 8. Service Detection – Info

- **Note:** This is just part of the scanning process.

- **Fix:** No action needed unless you want to harden the system to avoid service fingerprinting.

Otenable Nessus Essentials Scans Settings

priya 2 [Back to All Scans](#)

Hosts 1 Vulnerabilities 22 History 1

Filter Search Vulnerabilities 22 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Actions
MEDIUM	5.3	SMB Signing not required	Misc.	1	🔗
MIXED	SSL (Multiple Issues)	General	4	🔗
INFO	SMB (Multiple Issues)	Windows	6	🔗
INFO	HTTP (Multiple Issues)	Web Servers	2	🔗
INFO	Microsoft Windows (Multi...	Windows	2	🔗
INFO	TLS (Multiple Issues)	Service detection	2	🔗
INFO	Netstat Portscanner (SSH)	Port scanners	29	🔗
INFO	DCE Services Enumeration	Windows	8	🔗
INFO	Service Detection	Service detection	2	🔗
INFO	Common Platform Enumerati...	General	1	🔗

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:36 PM
End: Today at 8:44 PM
Elapsed: 8 minutes

Vulnerabilities

Critical: 0%, High: 0%, Medium: 0%, Low: 0%, Info: 100%

Otenable Nessus Essentials Scans Settings

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terrascan

Tenable News Gemini Search Personalization Model - Prompt Injec... Read More

INFO	DCE Services Enumeration	Windows	8	🔗
INFO	Service Detection	Service detection	2	🔗
INFO	Common Platform Enumerati...	General	1	🔗
INFO	Device Type	General	1	🔗
INFO	Host Fully Qualified Domain N...	General	1	🔗
INFO	Nessus Scan Information	Settings	1	🔗
INFO	Nessus Server Detection	Service detection	1	🔗
INFO	Netstat Connection Information	General	1	🔗
INFO	OS Fingerprints Detected	General	1	🔗
INFO	OS Identification	General	1	🔗
INFO	OS Identification and Installed...	Misc.	1	🔗
INFO	OS Security Patch Assessment...	Settings	1	🔗
INFO	SSL / TLS Versions Supported	General	1	🔗
INFO	Strict Transport Security (STS) ...	Service detection	1	🔗
INFO	Target Credential Status by Au...	Settings	1	🔗

Analysis & Recommendations

- Although no critical or high vulnerabilities were found, **medium-level SMB misconfiguration** and multiple **SSL/TLS/HTTP issues** indicate potential security weaknesses.
- Addressing these ensures better protection against MITM attacks and data leakage.
- All services should be reviewed for necessity; close ports and disable legacy services (like SMBv1 or DCE) to reduce the attack surface.



Conclusion

The local system is **not critically vulnerable**, but shows signs of **misconfigurations and outdated protocol support**. Prompt hardening (disabling old protocols, enabling encryption, service reduction) will greatly improve the system's security posture.

