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

ℹ️ 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.

ℹ️ 3. SMB (Multiple Issues) – Info

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

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

ℹ️ 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).

ℹ️ 5. TLS (Multiple Issues) – Info

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

ℹ️ 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.

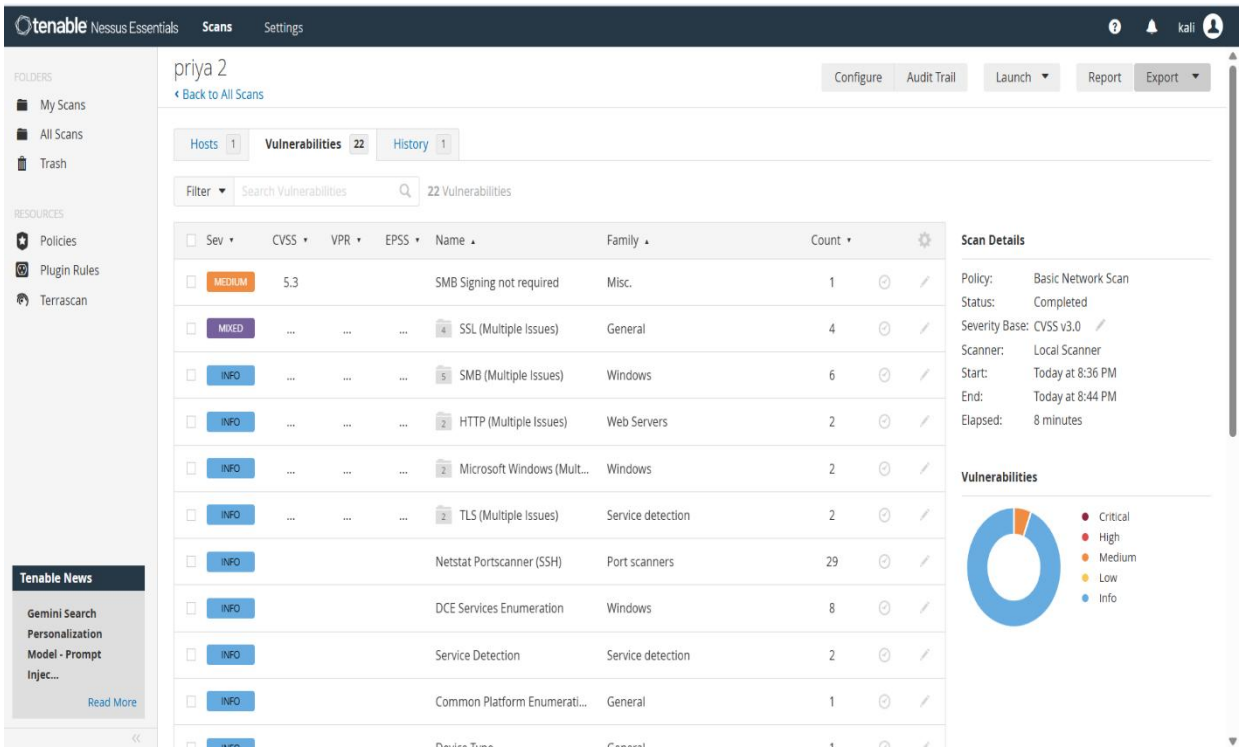
ℹ️ 7. DCE Services Enumeration – Info

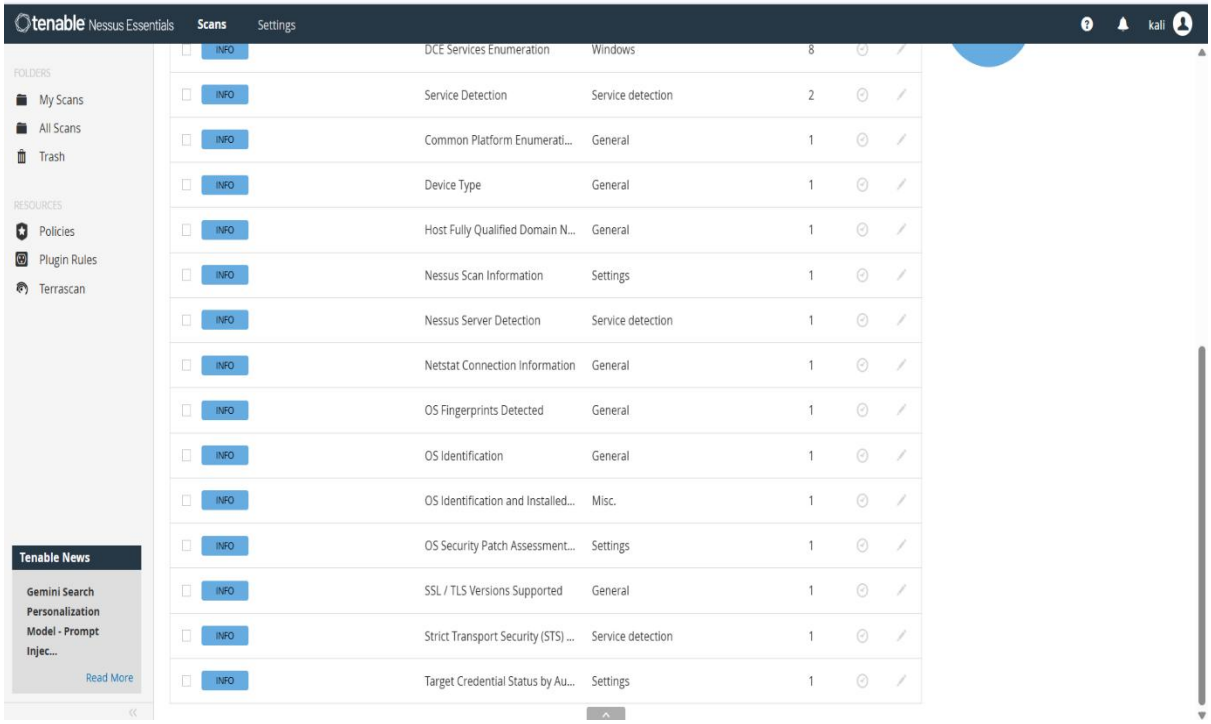
- **Fix**: DCE (Distributed Computing Environment) services should be disabled if not used.
  - Use Windows Features or services.msc to stop them.

ℹ️ 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.





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.