**Task 3: Perform a Basic Vulnerability Scan on Your PC.**

**Objective:** Use free tools to identify common vulnerabilities on your computer.

**Tools:** OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.

**Deliverables:** Vulnerability scan report with identified issues.

1. **Install Nessus Essentials.**

For Windows:

* Go to: [https://www.tenable.com/products/nessus/nessus-essentials](https://www.tenable.com/products/nessus/nessus-essentials?utm_source=chatgpt.com)
* Once we register with our mail, we will get an activation code.
* Installed it normally.
* After installation, Nessus runs as a web service.  
  Opened a browser and visited: https://localhost:8834/
* The activation code was entered to activate Nessus Essentials.
* It took some time to configure the plugins (around 15 minutes).

**2. Set up scan target as your local machine IP or localhost.**

A screenshot of a computer

AI-generated content may be incorrect.



**3. Start a full vulnerability scan. A screenshot of a computer

AI-generated content may be incorrect.**

**4. Wait for scan to complete (may take 30-60 mins). A screenshot of a computer

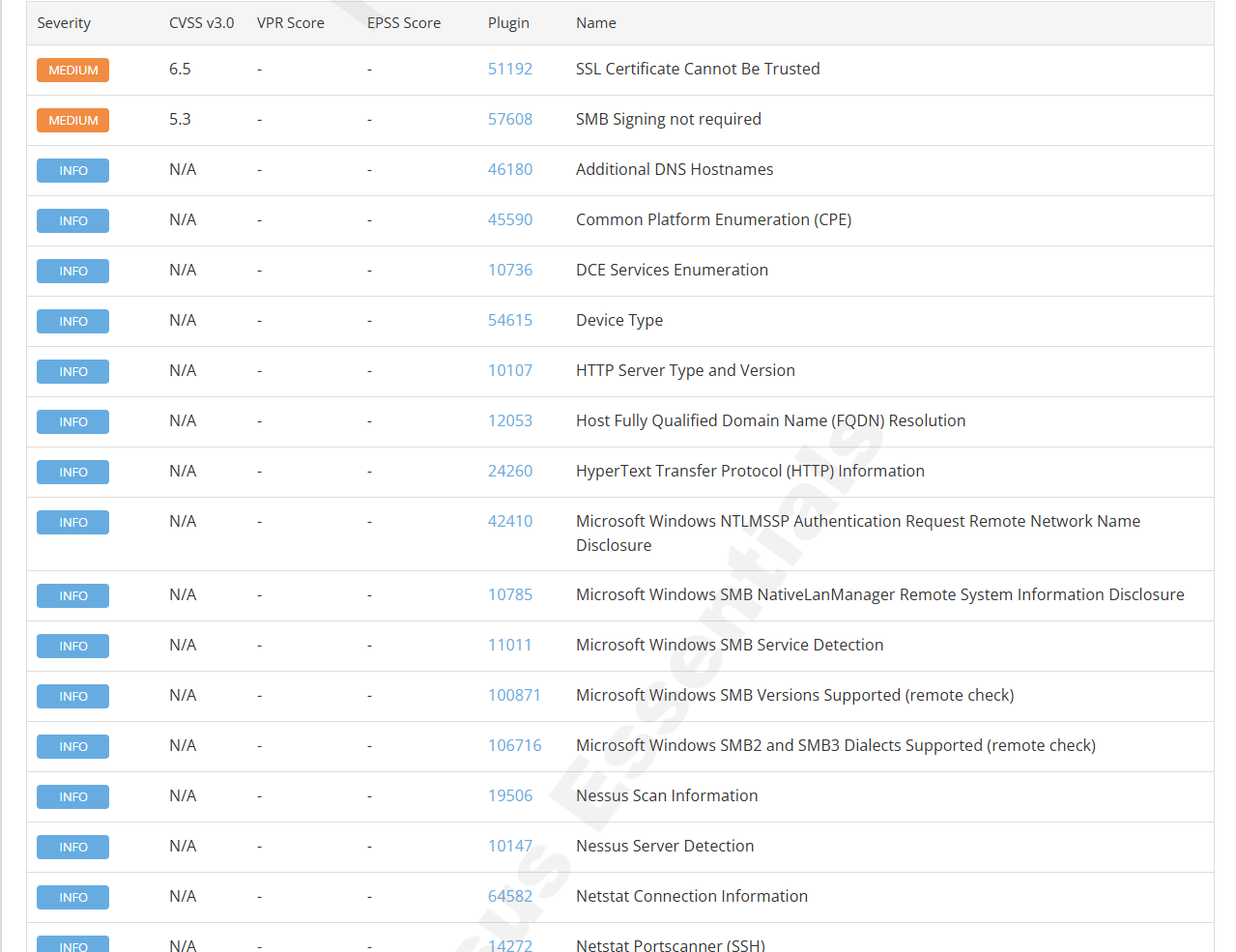
AI-generated content may be incorrect.**



**5. Review the report for vulnerabilities and severity.**

****



****

**A screenshot of a computer

AI-generated content may be incorrect.**

**6. Research simple fixes or mitigations for found vulnerabilities.**

Some severe vulnerabilities with its description:

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity** | **Vulnerability** | **Plugin ID** | **Description** |
| **Medium** | **SSL Certificate Cannot Be Trusted** | [**51192**](https://www.tenable.com/plugins/nessus/51192) | **The SSL certificate presented by the service cannot be trusted (e.g., self-signed or expired).** |
| **Medium** | **SMB Signing Not Required** | [**57608**](https://www.tenable.com/plugins/nessus/57608) | **SMB signing is not enforced, which may allow man-in-the-middle (MITM) attacks.** |
| **Info** | **Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure** | [**42410**](https://www.tenable.com/plugins/nessus/42410) | **The system discloses its network name via NTLM authentication requests.** |
| **Info** | **Microsoft Windows SMB NativeLanManager Remote System Information Disclosure** | [**10785**](https://www.tenable.com/plugins/nessus/10785) | **SMB responses include information about the OS and system, which could help attackers profile the machine.** |
| **Info** | **Additional DNS Hostnames** | [**46180**](https://www.tenable.com/plugins/nessus/46180) | **The host is reachable via multiple DNS hostnames, which may assist in mapping your network.** |

**Fixes & Mitigations**

Medium severity:

1. **SSL Certificate Cannot Be Trusted**

**Issue:**The SSL/TLS certificate is either self-signed, expired, or issued by an untrusted CA.

**Fix / Mitigation:**

Replace the certificate with one issued by a trusted Certificate Authority (CA).

**Preventive measure:**

Always use valid, up-to-date SSL certificates and enforce HTTPS where possible.

**For Windows IIS:**

Open IIS Manager → Server Certificates → Create Domain Certificate.

1. **SMB Signing Not Required**

**Issue:**  
SMB (Server Message Block) protocol allows communication without signing, making it vulnerable to **MITM** or **relay attacks**.

**Fix / Mitigation (Windows):**

* Open Local Group Policy Editor → gpedit.msc
* Navigate to:

Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

* Set the following:

Microsoft network client: Digitally sign communications (always) → Enabled

Microsoft network server: Digitally sign communications (always) → Enabled

* Reboot the system.

**Command line (PowerShell alternative):**

Set-SmbServerConfiguration -RequireSecuritySignature $true

Set-SmbClientConfiguration -RequireSecuritySignature $true

**Preventive measure:**

Enforce SMB signing on all systems and disable SMBv1 entirely if still active.

1. **NTLMSSP Authentication Request Remote Network Name Disclosure**

**Issue:**During NTLM authentication, Windows may expose its machine name to remote systems.

**Fix / Mitigation:**

* + Disable NTLM authentication if not needed:
    - Local Security Policy → Local Policies → Security Options
    - Set Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers → *Deny all*.
  + Prefer Kerberos or NTLMv2 for stronger authentication.
  + Keep systems off untrusted networks to minimize exposure.

1. **SMB NativeLanManager Information Disclosure**

**Issue:**  
SMB (Server Message Block) protocol allows communication without signing, making it vulnerable to **MITM** or **relay attacks**.

**Fix / Mitigation (Windows):**

* Open Local Group Policy Editor → gpedit.msc
* Navigate to:

Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

* Set the following:

Microsoft network client: Digitally sign communications (always) → Enabled

Microsoft network server: Digitally sign communications (always) → Enabled

* Reboot the system.

**Command line (PowerShell alternative):**

Set-SmbServerConfiguration -RequireSecuritySignature $true

Set-SmbClientConfiguration -RequireSecuritySignature $true

**Preventive measure:**

Enforce SMB signing on all systems and disable SMBv1 entirely if still active.

1. **Additional DNS Hostnames**

**Issue:**  
Multiple DNS entries point to the same IP, allowing attackers to map your internal structure.

**Fix / Mitigation:**

* Review and remove unnecessary DNS aliases (CNAMEs) that expose internal naming conventions.
* Ensure DNS records are updated and consistent.
* Implement split-horizon DNS for internal vs external name resolution.