Analyzing Common Vulnerabilities

June 26, 2025

1 Summary

Conducted various types of scanning on a Windows 11 system and found several security vulnerabilities. Nessus for vulnerability assessment and manual verification for confirmation. The Scope of the assessment - Windows 11 system.

2 Findings

No:	Severity	Finding Name	Description
1	Medium	SMB Signing	Signing is not required on remote SMB Server. An unauthenticated, remote attacker can exploit this to conduct MITM attacks against SMB Server.
2	Medium	SSL Certificates cannot be trusted	Server's X.509 certificate cannot be trusted. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity. Leads to MITM attacks.
3	Info	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	The remote host listens on TCP port 445 and replies to SMB requests.
4	Info	WMI Not Available	Windows Management Instrumentation is not available on the remote host over DCOM. WMI queries are used to gather information and remote host data, such as network interface configuration.
5	Info	DCE Services Enumeration	By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE), it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.
6	Info	TLS Version 1.2 and 1.3 Protocol Detection	The remote service accepts connections encrypted using TLS 1.2 and 1.3.

3 Detailed Walkthrough

Test done using tool named Nessus Essentials. Done an advance scan on the Host 127.0.0.1 windows 11 system. Found vulnerabilities like SMB signing not required, open ports etc.

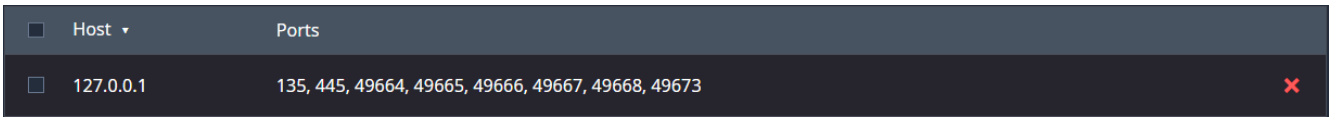

Figure 1: Open-Ports

Figure 2: Vulnerabity

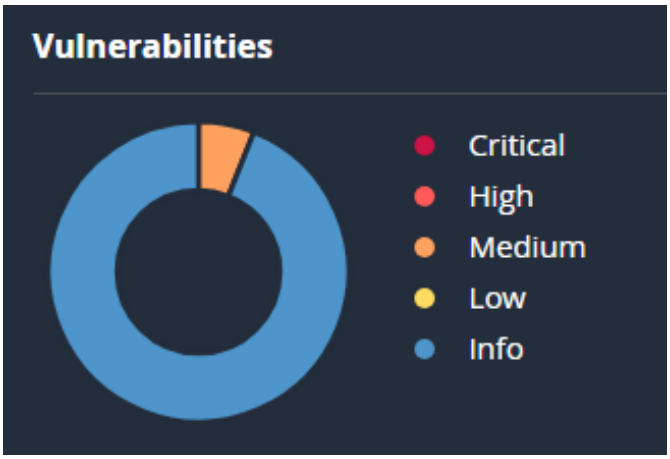

Figure 3: Rating-Level

4 Impact

4.1 SMB Signing Not Required

Without SMB signing, an attacker on the same network can intercept and modify SMB traffic (Man-in-the-Middle attack), potentially gaining unauthorized access or injecting malicious data

4.2 SSL Certificates Cannot Be Trusted

Users may be unable to verify the authenticity of the host. Attackers could impersonate the server in a phishing or MITM attack, compromising data confidentiality and integrity.

4.3 NTLMSSP Network Name Disclosure

Leaks information about the system through SMB that can be used for OS fingerprinting or further enumeration. While not directly exploitable, it aids in planning targeted attacks.

4.4 WMI Not Available

Limits administrative tools and automated management over the network. While not a direct security risk, attackers using WMI for remote reconnaissance will be blocked.

4.5 DCE Services Enumeration

Reveals RPC services and their bindings. Attackers can use this to identify potential weak services and exploit known vulnerabilities tied to those services.

4.6 TLS 1.2 and 1.3 Protocol Detection

Indicates the server supports modern encryption (which is good). However, publicly revealing supported protocols allows attackers to target known weaknesses or fingerprint services.

5 Remediation Advice

5.1 SMB Signing Not Required

Enforce SMB signing via Group Policy for both client and server. Mitigation steps:

1. **Open Group Policy Editor:** Win + R → Type gpedit.msc → Enter
2. **Navigate to:** Win + R → Type gpedit.msc → Enter
3. **Find and enable:** Microsoft network client → Digitally sign communications and Microsoft network server → Digitally sign communications.
4. Apply changes and restart the system or run gpupdate /force in CMD.

5.2 SSL Certificates Cannot Be Trusted

Replace with CA-signed certificates and ensure full certificate chain is valid. Mitigation steps:

1. **Use certificates signed by a trusted Certificate Authority (CA):** Obtain a certificate from a public CA (e.g., Let's Encrypt, DigiCert).

   Or use an internal enterprise CA and distribute the root cert to clients.
2. **Ensure proper certificate chain:** Install intermediate certificates on the host server.

   Use tools like SSL Labs or openssl to verify the chain.
3. Update expired or weak certs regularly.