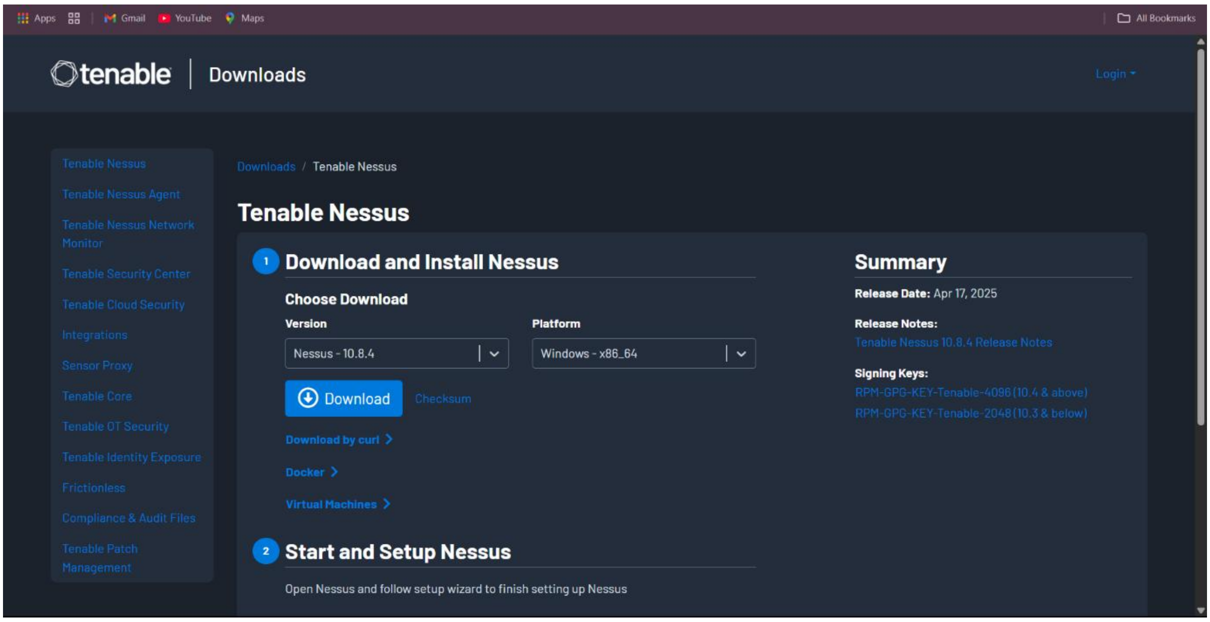
Task 3: Perform a Basic Vulnerability Scan on Your PC

- Tools Used: Nessus Essential
- Scan Type: Advanced Scan
- Target: Localhost (IP of Our PC)

To Start with the Scan, We Can Download Nessus Essential from its official website.
Register with your official mail id to generate an Activation Code which will be used at the time of installation.



Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.8.4

Platform: Windows - x86_64

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

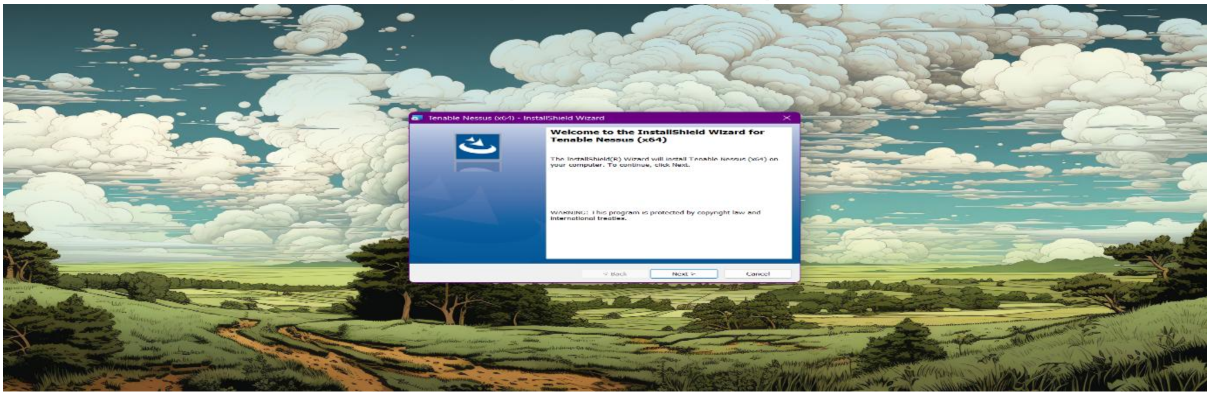
Summary

Release Date: Apr 17, 2025

Release Notes: Tenable Nessus 10.8.4 Release Notes

Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above) RPM-GPG-KEY-Tenable-2048 (10.3 & below)

Download Nessus and complete the Setup.

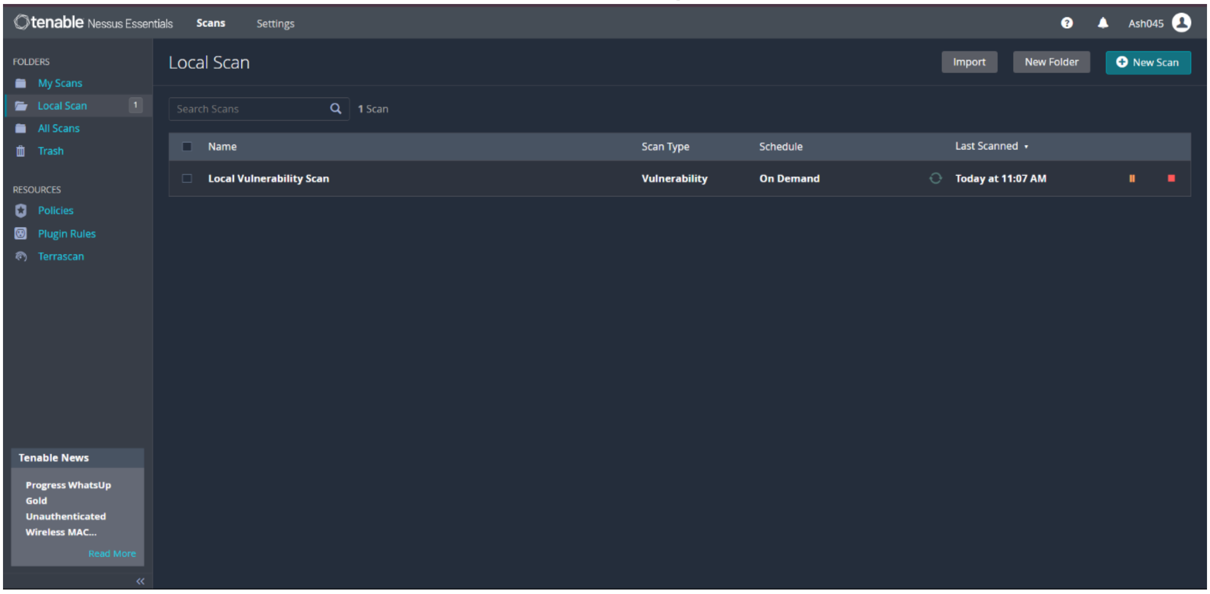


Welcome to the InstallShield Wizard for Tenable Nessus (x64)

The InstallShield(R) Wizard will install Tenable Nessus (x64) on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Now Start a New Scan with Our Local IP
We Can Check Local IP with “ipconfig” command in Windows.

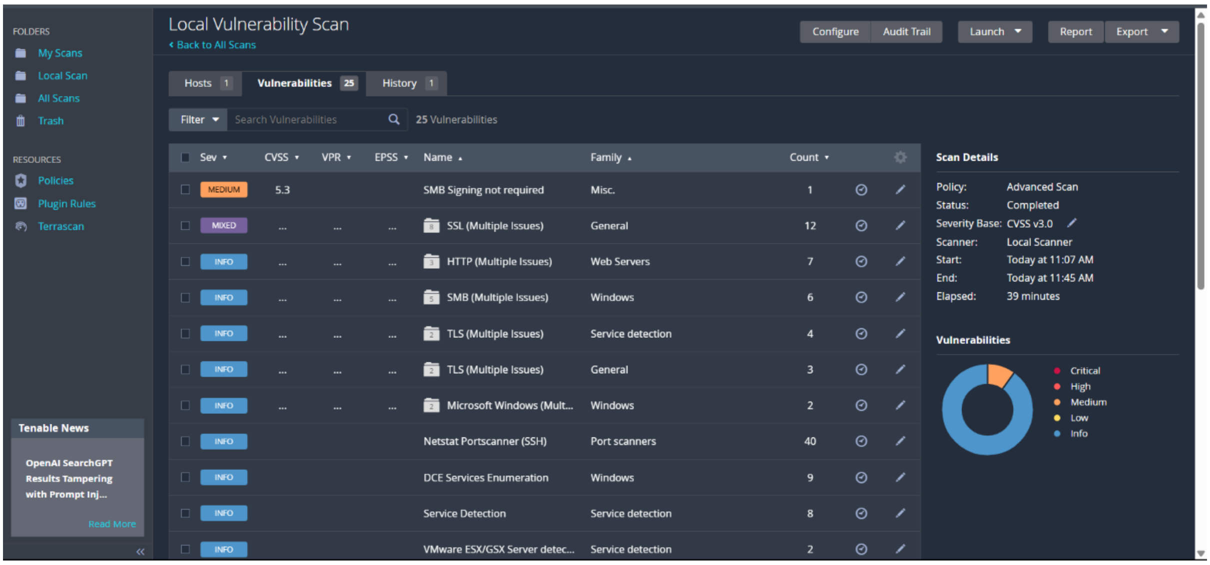


Local Scan

1 Scan

Name	Scan Type	Schedule	Last Scanned
Local Vulnerability Scan	Vulnerability	On Demand	Today at 11:07 AM

Let’s Start the Scan and wait for the Results.



Local Vulnerability Scan
‹ Back to All Scans

25 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED	...	...	...	SSL (Multiple Issues)	General	12
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	7
INFO	...	...	...	SMB (Multiple Issues)	Windows	6
INFO	...	...	...	TLS (Multiple Issues)	Service detection	4
INFO	...	...	...	TLS (Multiple Issues)	General	3
INFO	...	...	...	Microsoft Windows (Mult...	Windows	2
INFO				Netstat Portscanner (SSH)	Port scanners	40
INFO				DCE Services Enumeration	Windows	9
INFO				Service Detection	Service detection	8
INFO				VMware ESX/GSX Server detec...	Service detection	2

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:07 AM
End:	Today at 11:45 AM
Elapsed:	39 minutes

Vulnerabilities

Let’s Export the Result and make a Report

Summary of Vulnerability Findings

- **Total Vulnerabilities:** 25

- **Severity Breakdown:**
    - **Critical:** 0
    - **High:** 0
    - **Medium:** 1
    - **Low:** 0
    - **Info:** 24

Key Identified Vulnerability

1. SMB Signing not required

- **Severity:** Medium
- **CVSS:** 5.3
- **Plugin Family:** Misc.
- **Count:** 1
- **Description:** SMB signing ensures message integrity and prevents man-in-the-middle (MITM) attacks. If not required, attackers can intercept or alter SMB traffic.
- **Mitigation:** Configure Group Policy or registry to require SMB signing:
    - **Windows Path:** Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options
    - **Policy:** *Microsoft network client: Digitally sign communications (always)* – **Enable**
    - **Policy:** *Microsoft network server: Digitally sign communications (always)* – **Enable**

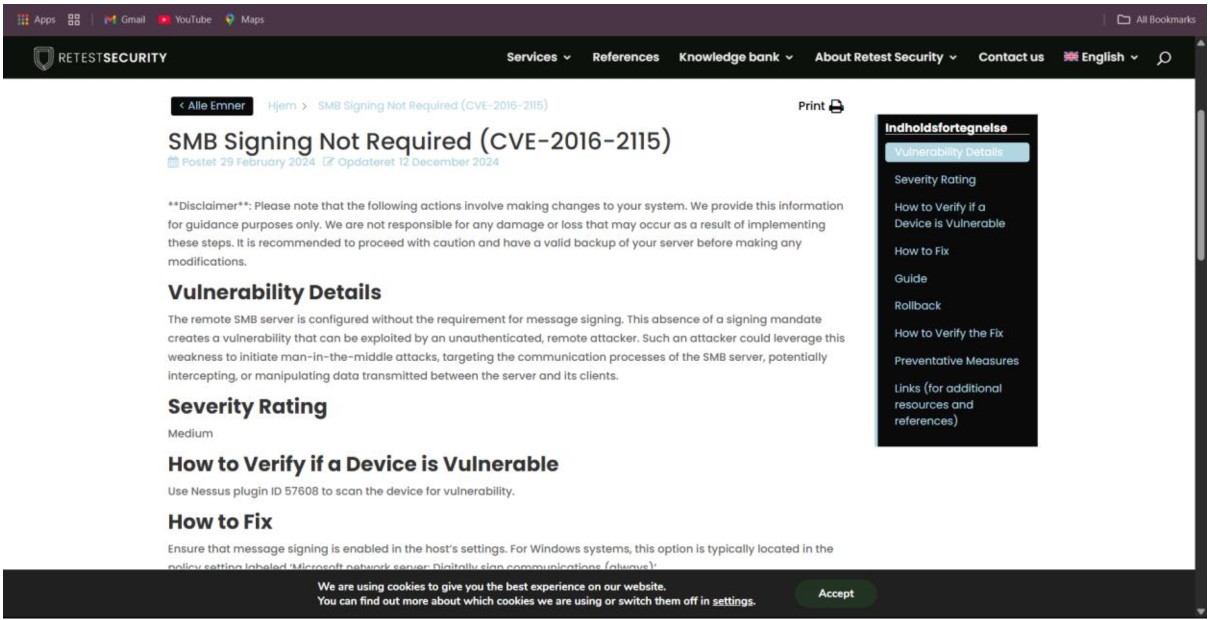
Informational Findings (Safe but Useful)

These are mostly for network profiling and hardening awareness:

- **SSL/HTTP/SMB/TLS – Multiple Issues**
- **Netstat Ports Scanner**
- **OS Fingerprinting / Identification**
- **DCE/RPC Services Detected**
- **Service Detection**
- **Device Type**
- **SSH Key/No Credential Warning**

- **Web Server 404 Error Code Check**
- **SSL Certificate CA Info**
- **Nessus Scan Info**

Now Let's try to fix the Vulnerability found in the scan, search on web with the plugin Id and try to fix it.



SMB Signing Not Required (CVE-2016-2115)

Postet 29 February 2024 Opdateret 12 December 2024

Disclaimer: Please note that the following actions involve making changes to your system. We provide this information for guidance purposes only. We are not responsible for any damage or loss that may occur as a result of implementing these steps. It is recommended to proceed with caution and have a valid backup of your server before making any modifications.

Vulnerability Details

The remote SMB server is configured without the requirement for message signing. This absence of a signing mandate creates a vulnerability that can be exploited by an unauthenticated, remote attacker. Such an attacker could leverage this weakness to initiate man-in-the-middle attacks, targeting the communication processes of the SMB server, potentially intercepting, or manipulating data transmitted between the server and its clients.

Severity Rating

Medium

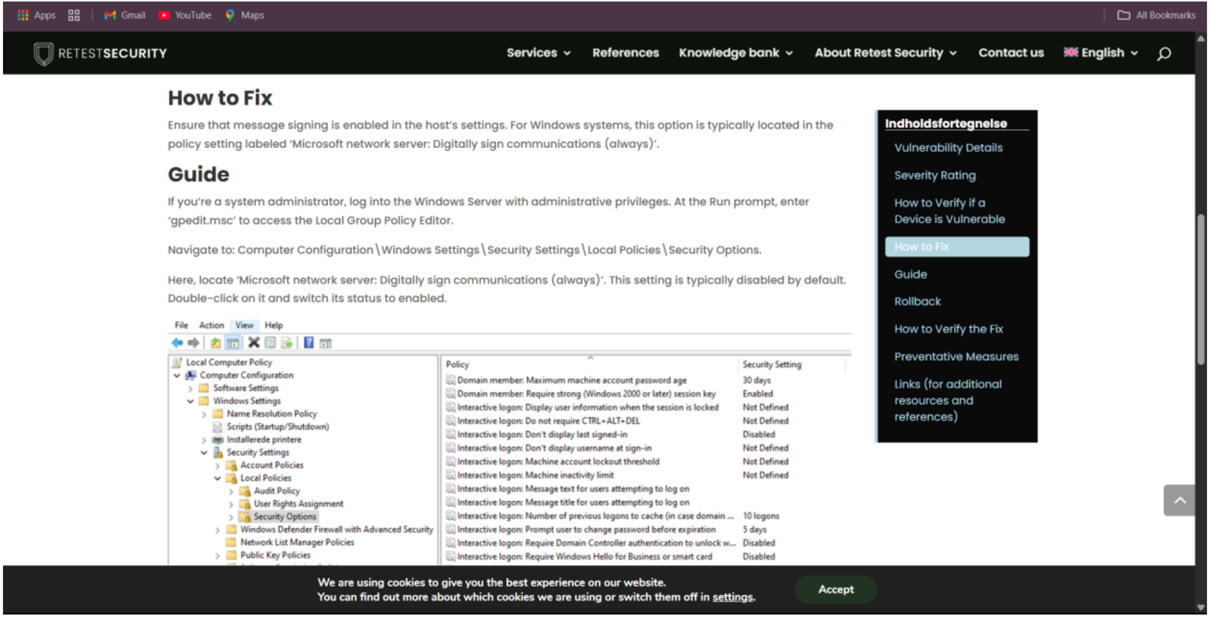
How to Verify if a Device is Vulnerable

Use Nessus plugin ID 57608 to scan the device for vulnerability.

How to Fix

Ensure that message signing is enabled in the host's settings. For Windows systems, this option is typically located in the policy setting labeled 'Microsoft network server: Digitally sign communications (always)'.

We are using cookies to give you the best experience on our website.
You can find out more about which cookies we are using or switch them off in settings.



How to Fix

Ensure that message signing is enabled in the host's settings. For Windows systems, this option is typically located in the policy setting labeled 'Microsoft network server: Digitally sign communications (always)'.

Guide

If you're a system administrator, log into the Windows Server with administrative privileges. At the Run prompt, enter 'gpedit.msc' to access the Local Group Policy Editor.

Navigate to: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.

Here, locate 'Microsoft network server: Digitally sign communications (always)'. This setting is typically disabled by default. Double-click on it and switch its status to enabled.

Policy	Security Setting
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Disabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	
Interactive logon: Message title for users attempting to log on	
Interactive logon: Number of previous logons to cache (in case domain ...	10 logons
Interactive logon: Prompt user to change password before expiration	5 days
Interactive logon: Require Domain Controller authentication to unlock w...	Disabled
Interactive logon: Require Windows Hello for Business or smart card	Disabled

We are using cookies to give you the best experience on our website.
You can find out more about which cookies we are using or switch them off in settings.

Conclusion: The vulnerability scan conducted using **Nessus Essentials** on the local machine revealed a total of **25 findings**, including **1 Medium severity vulnerability** and **24 informational notices**. The most critical issue identified was **"SMB Signing Not**

Required", which can potentially allow **man-in-the-middle (MITM) attacks** if not mitigated.

While no high or critical vulnerabilities were found, the scan highlighted several areas of improvement, such as outdated or weak configurations in SMB, TLS, and HTTP services. These configurations could expose system information to attackers during enumeration phases of an attack.

Implementing recommended mitigations, such as **enforcing SMB signing**, **disabling unused services**, and **tightening SSL/TLS configurations**, will significantly improve the system's security posture. Additionally, supplying administrative credentials in future scans can uncover deeper vulnerabilities related to OS misconfigurations or missing patches.

This initial scan provides a strong baseline for assessing local system security and demonstrates the importance of continuous monitoring and hardening practices to defend against evolving threats.