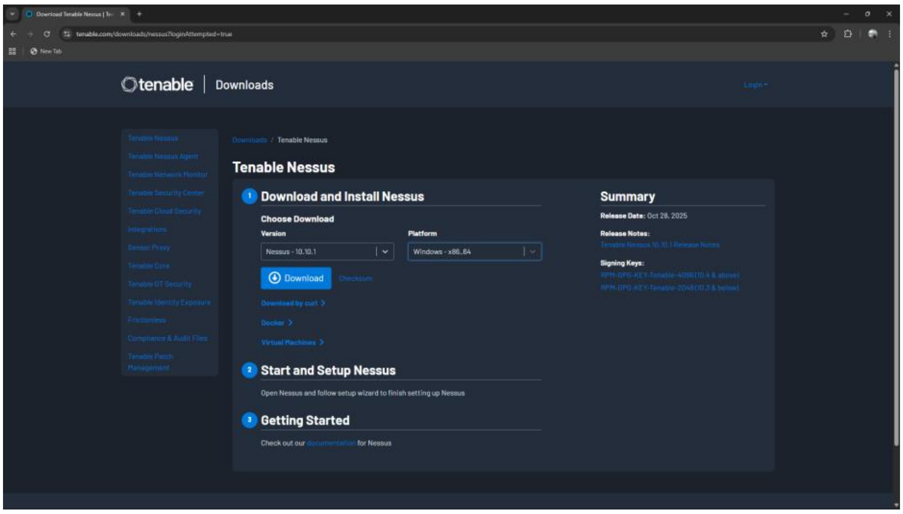
Task 3: Perform a Basic Vulnerability Scan on Your PC.

1.Install OpenVAS or Nessus Essentials.

1. Download Nessus Essentials from: https://www.tenable.com/products/nessus/nessus-essentials



tenable.com/downloads/nessus?loginAttempted=true

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.10.1

Platform: Windows - x86_64

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

3 Getting Started

Check out our documentation for Nessus

Summary

Release Date: Oct 28, 2025

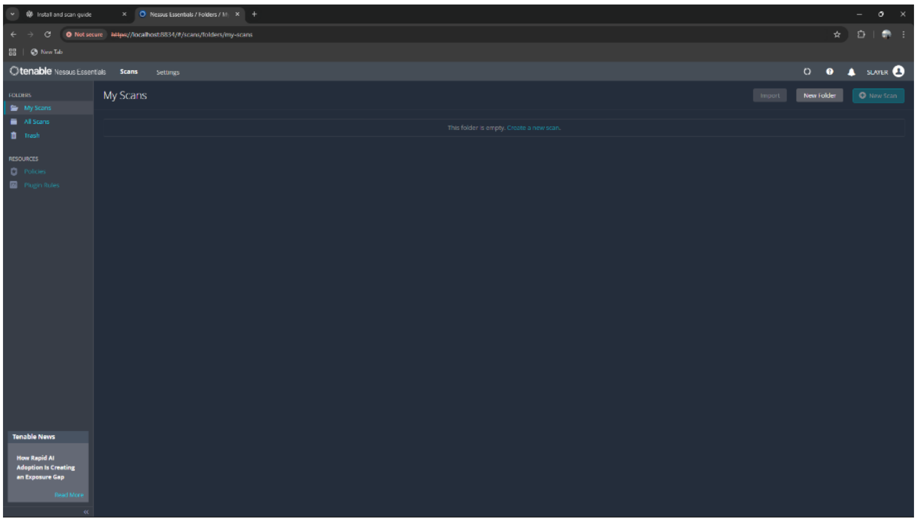
Release Notes: Tenable Nessus 10.10.1 Release Notes

Signing Keys:

RPM-GPG-KEY-Tenable-4096 (10.4 & above)

RPM-GPG-KEY-Tenable-2048 (10.3 & below)

2. Select **Windows (x64)** version and install it.
3. After installation, your browser opens automatically at: https://localhost:8834/
4. Create an admin account.
5. Enter the **Essentials Activation Code** received on email.
6. Wait 5–10 minutes while Nessus **downloads and compiles plugins**.
7. Once complete, you will reach the dashboard.



Not secure ~~https~~://localhost:8834/#/scans/folders/my-scans

My Scans

This folder is empty. Create a new scan.

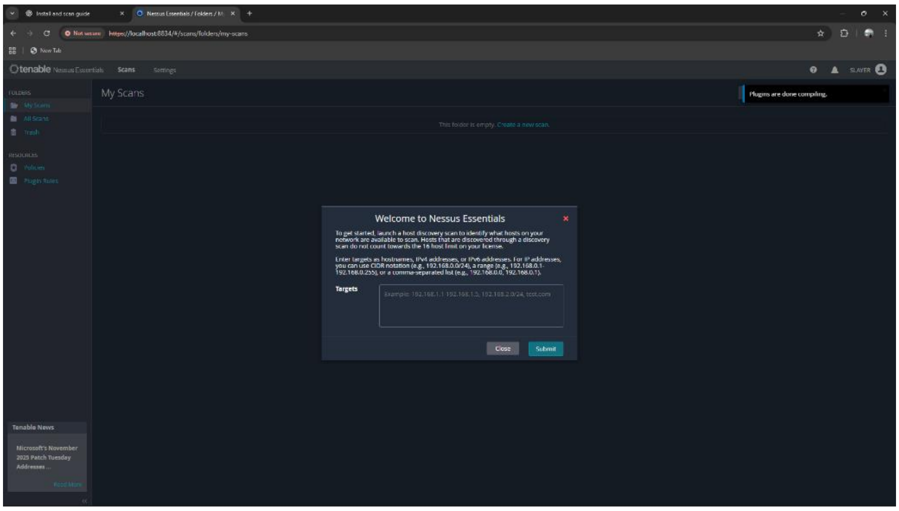
Tenable News

How Rapid AI Adoption Is Creating an Exposure Gap

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

Basic Network Scan Setup

1. Go to: https://localhost:8834/
2. Left sidebar → **Scans**
3. Click **New Scan**
4. Select **Basic Network Scan**
5. Fill fields:
   - **Name:** Localhost Full Scan
   - **Targets:** 127.0.0.1
     (or your IP: 192.168.x.x)
6. Click **Save**.



https://localhost:8834/#/scans/folders/my-scans

My Scans

Plugins are done compiling.

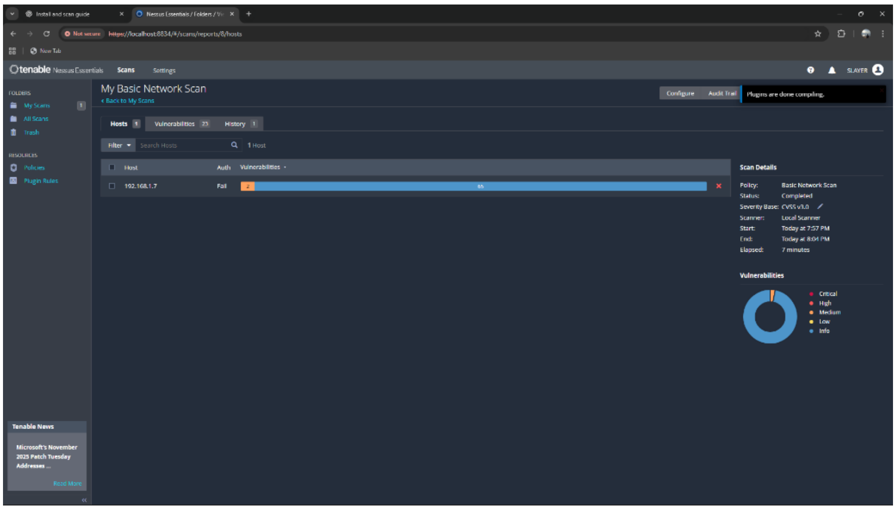
This folder is empty. Create a new scan.

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: Example: 192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com



https://localhost:8834/#/scans/reports/8/hosts

My Basic Network Scan

Plugins are done compiling.

	Host	Auth	Vulnerabilities
□	192.168.1.7	Fail	2 65

1 Host

Scan Details

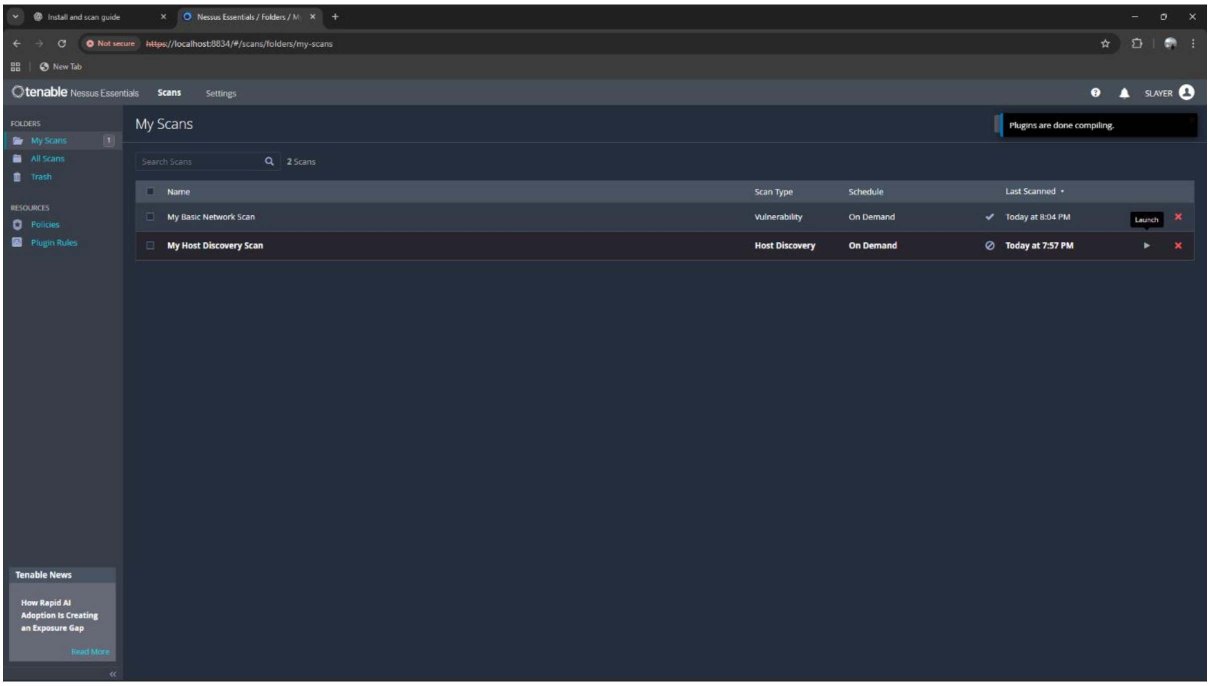
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 7:57 PM
End: Today at 8:04 PM
Elapsed: 7 minutes

Vulnerabilities

3.Start a full vulnerability scan.

1. Open **Scans → My Scans**
2. Hover over your scan → click **Launch**
3. Nessus begins scanning:
    - ports
    - services
    - SSL
    - SMB
    - Windows settings
    - outdated software
    - misconfigurations

Scan takes **10–25 minutes**.



My Scans

Plugins are done compiling.

2 Scans

Name	Scan Type	Schedule	Last Scanned
My Basic Network Scan	Vulnerability	On Demand	✓ Today at 8:04 PM
My Host Discovery Scan	Host Discovery	On Demand	⊘ Today at 7:57 PM

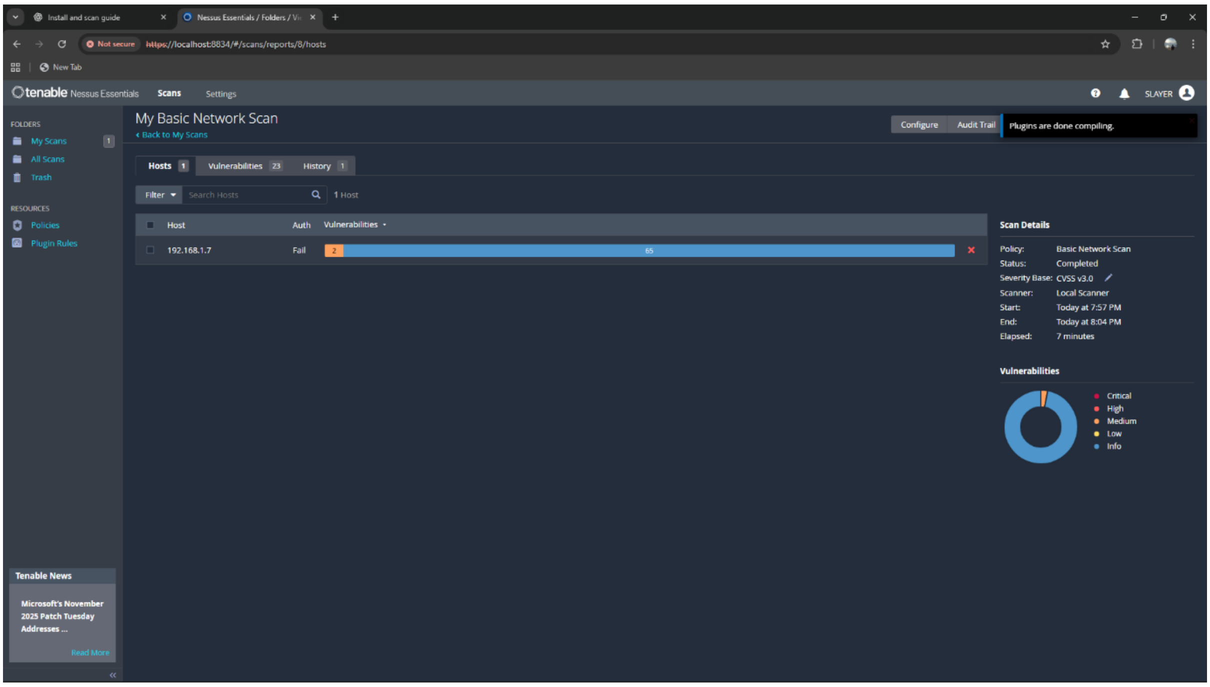
How Rapid AI Adoption Is Creating an Exposure Gap

4.Wait for scan to complete (may take 30-60 mins).

While the scan runs, Nessus shows:

- Count of vulnerabilities
- Breakdown by severity
- Progress percentage
- Hosts discovered

You can leave it running.
Once done, the scan status changes to **Completed**.



My Basic Network Scan

‹ Back to My Scans

Plugins are done compiling.

Host	Auth	Vulnerabilities
192.168.1.7	Fail	2 65

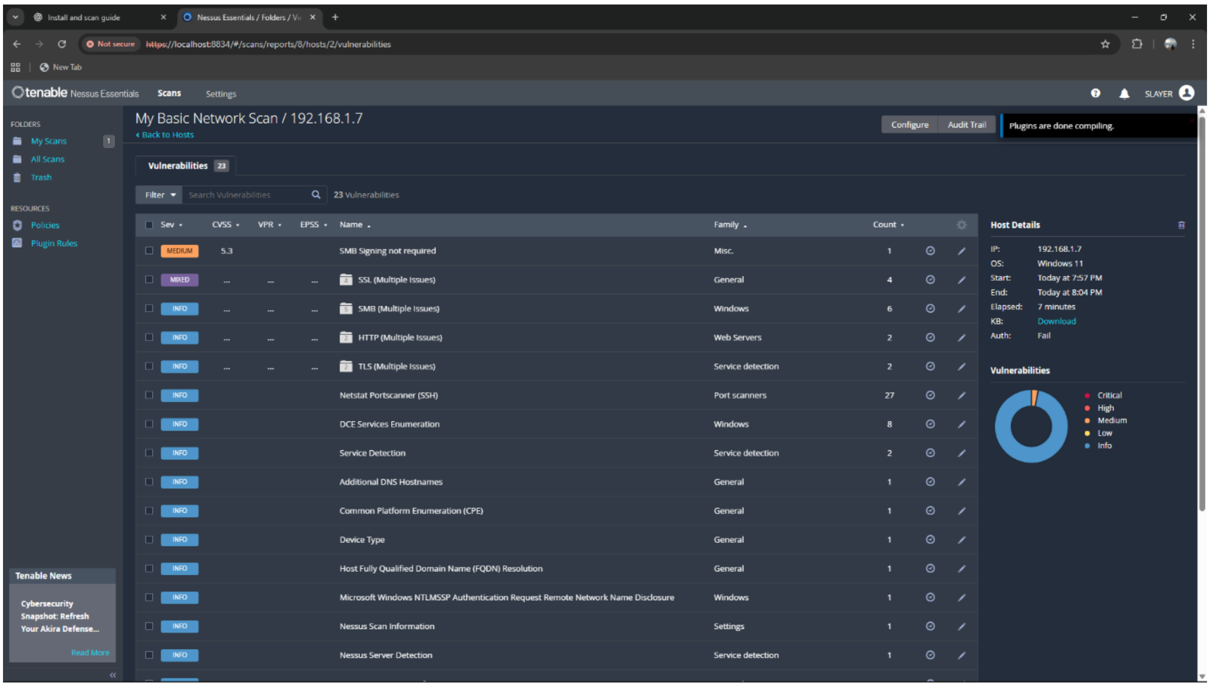
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 7:57 PM
End:	Today at 8:04 PM
Elapsed:	7 minutes

Vulnerabilities

5.Review the report for vulnerabilities and severity.

1. Open the completed scan result.
2. Go to **Vulnerabilities** tab.
3. Nessus groups issues by severity:
   - **Critical** (red)
   - **High** (orange)
   - **Medium** (yellow)
   - **Low** (blue)
   - **Info** (grey)
4. Click each vulnerability to see:
   - Description
   - Risk
   - CVEs
   - Affected ports/services
   - Output from scan
   - Solution steps



My Basic Network Scan / 192.168.1.7

‹ Back to Hosts

Plugins are done compiling.

23 Vulnerabilities

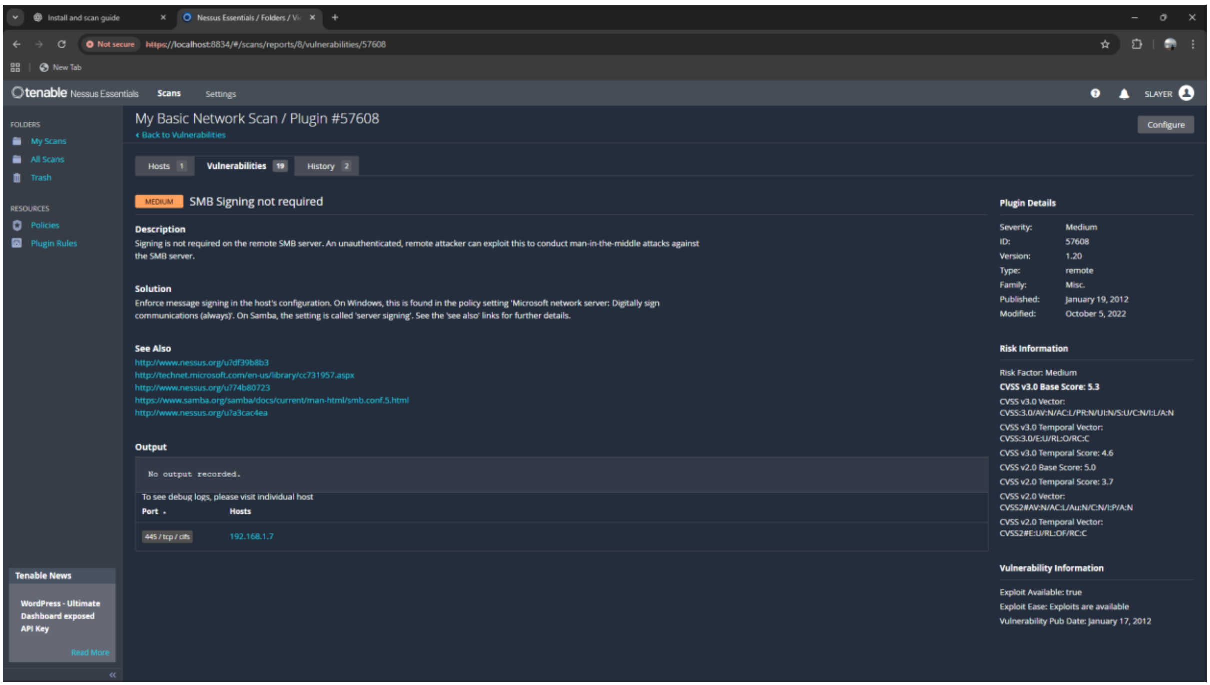
Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED	...	...	...	4 SSL (Multiple Issues)	General	4
INFO	...	...	...	5 SMB (Multiple Issues)	Windows	6
INFO	...	...	...	2 HTTP (Multiple Issues)	Web Servers	2
INFO	...	...	...	2 TLS (Multiple Issues)	Service detection	2
INFO				Netstat Portscanner (SSH)	Port scanners	27
INFO				DCE Services Enumeration	Windows	8
INFO				Service Detection	Service detection	2
INFO				Additional DNS Hostnames	General	1
INFO				Common Platform Enumeration (CPE)	General	1
INFO				Device Type	General	1
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	1
INFO				Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	Windows	1
INFO				Nessus Scan Information	Settings	1
INFO				Nessus Server Detection	Service detection	1

Host Details

IP:	192.168.1.7
OS:	Windows 11
Start:	Today at 7:57 PM
End:	Today at 8:04 PM
Elapsed:	7 minutes
KB:	Download
Auth:	Fail

Vulnerabilities

Cybersecurity Snapshot: Refresh Your Akira Defense...



My Basic Network Scan / Plugin #57608

‹ Back to Vulnerabilities

MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▴	Hosts
445 / tcp / cifs	192.168.1.7

Plugin Details

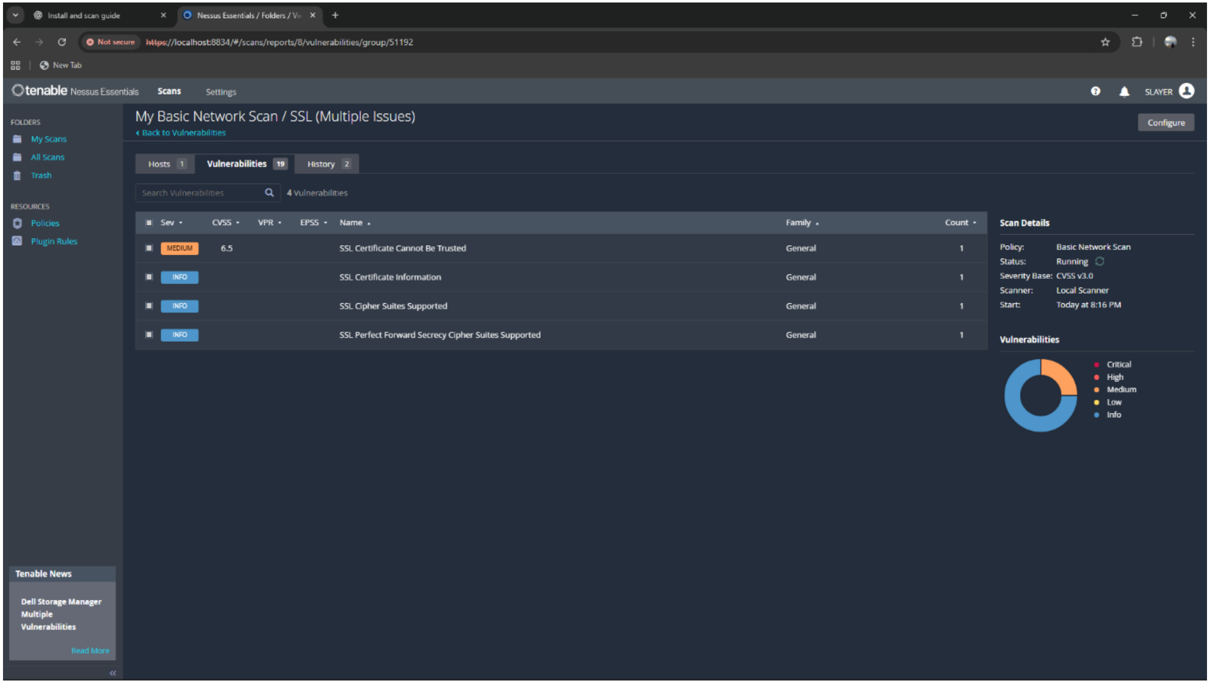
Severity:	Medium
ID:	57608
Version:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 5.3
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector:
CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 4.6
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Temporal Score: 3.7
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N
CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:OF/RC:C

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Vulnerability Pub Date: January 17, 2012



My Basic Network Scan / SSL (Multiple Issues)

‹ Back to Vulnerabilities

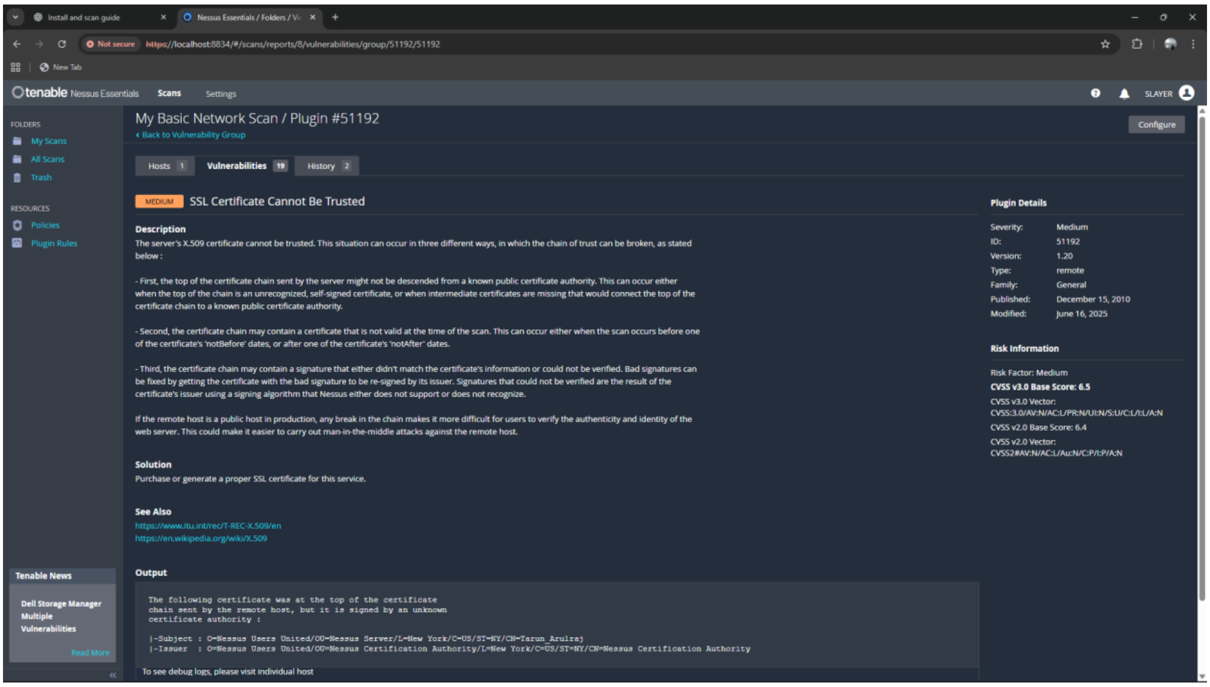
4 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
MEDIUM	6.5			SSL Certificate Cannot Be Trusted	General	1
INFO				SSL Certificate Information	General	1
INFO				SSL Cipher Suites Supported	General	1
INFO				SSL Perfect Forward Secrecy Cipher Suites Supported	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:16 PM

Vulnerabilities



My Basic Network Scan / Plugin #51192

‹ Back to Vulnerability Group

MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

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 and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=Tarun_Arulraj
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
```

To see debug logs, please visit individual host

Plugin Details

Severity:	Medium
ID:	51192
Version:	1.20
Type:	remote
Family:	General
Published:	December 15, 2010
Modified:	June 16, 2025

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS v2.0 Base Score: 6.4
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:N

6.Research simple fixes or mitigations for found vulnerabilities.

1. SMB Signing Not Required (Medium)

Cause: Windows allows SMB traffic without mandatory signing → risk of MITM.

Fix (Windows Home):

Run in **PowerShell (Admin)**:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters" -Name RequireSecuritySignature -Value 1
```

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" -Name RequireSecuritySignature -Value 1
```

2. SSL Certificate Cannot Be Trusted (Medium)

- **Cause:** Nessus UI uses a **self-signed SSL certificate**.
  Browsers don’t trust it — this is normal.
- Fix:
- Not needed for local usage.
- (Optional) Import the certificate into **Trusted Root Certificate Authorities** to suppress warnings

STEP 7 AND 8 ARE ALREADY DONE WITH ABOVE DOCUMENTATION