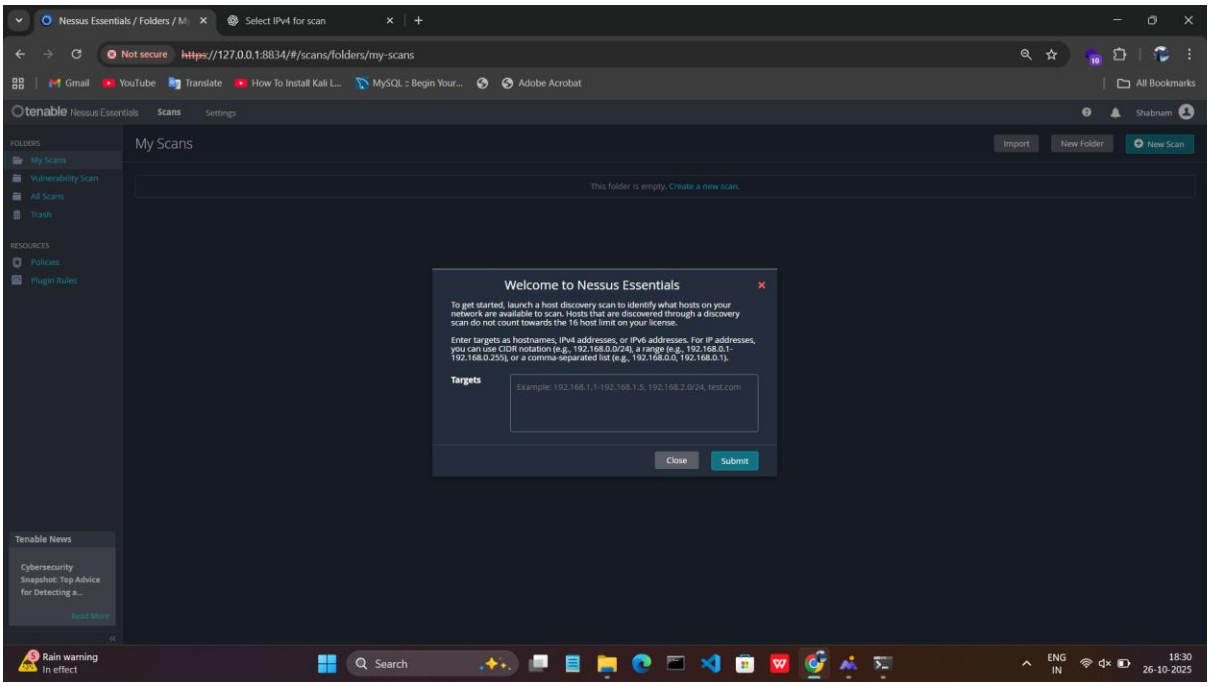
Vulnerability Assessment Report – Nessus Scan
Target System: Localhost (127.0.0.1)
Tool Used: Nessus Essentials – Basic Network Scan
Scan Duration: 8 minutes
Scan Status: Completed
Authentication: Failed (no system credentials were provided)

1. Introduction

During this internship task, a vulnerability assessment was conducted on the local system using **Nessus Essentials**. The purpose of this scan was to identify potential security weaknesses, understand their impact, and suggest appropriate remediation steps. This helps in maintaining a secure computing environment and mitigating the risks posed by cyber threats.



https://127.0.0.1:8834/#/scans/folders/my-scans

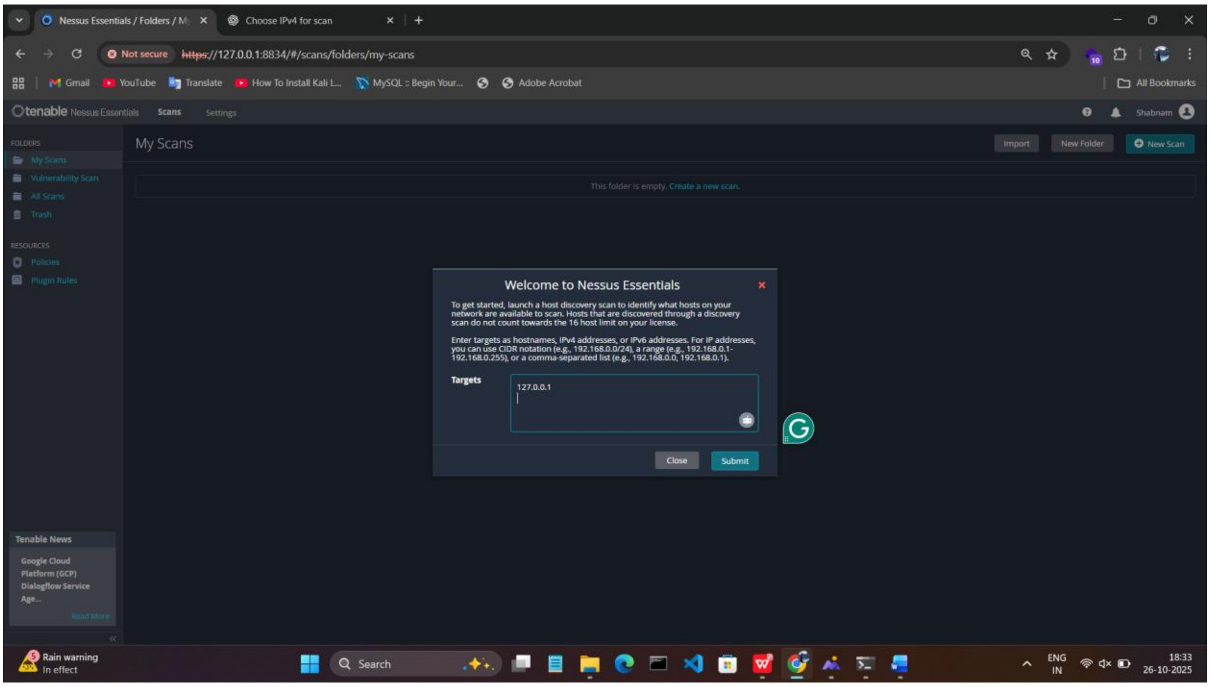
This folder is empty. Create a new scan.

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



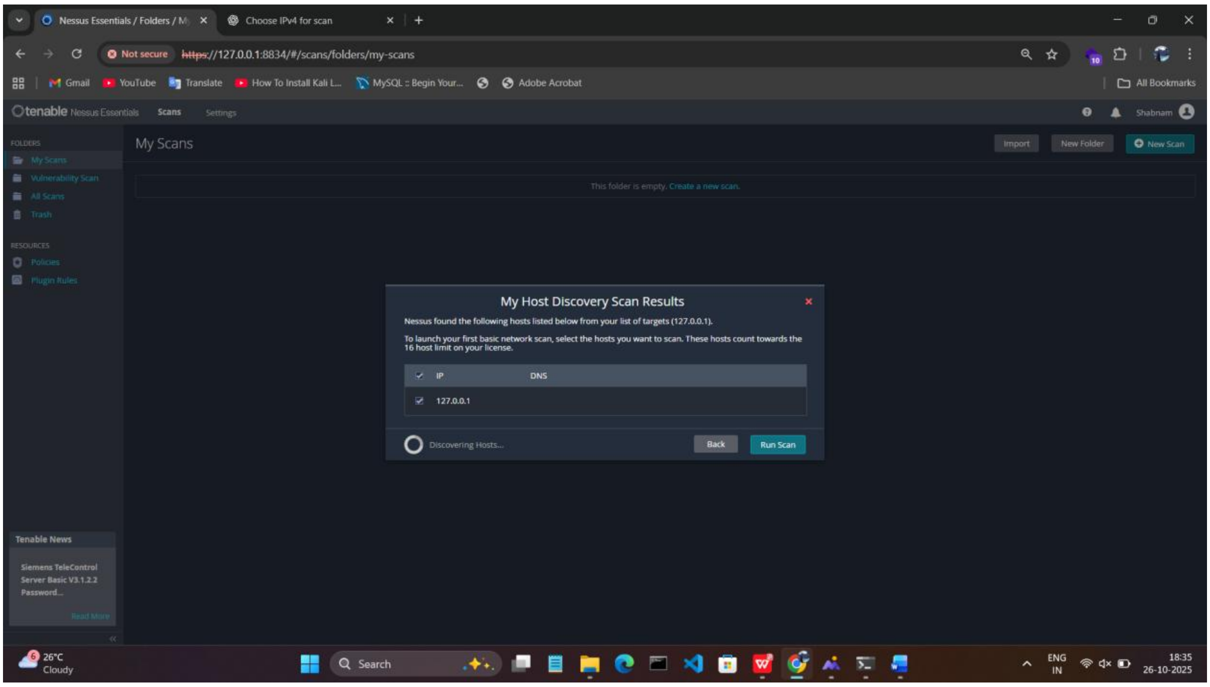
This folder is empty. Create a new scan.

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: 127.0.0.1



This folder is empty. Create a new scan.

My Host Discovery Scan Results

Nessus found the following hosts listed below from your list of targets (127.0.0.1).

To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

☑	IP	DNS
☑	127.0.0.1	

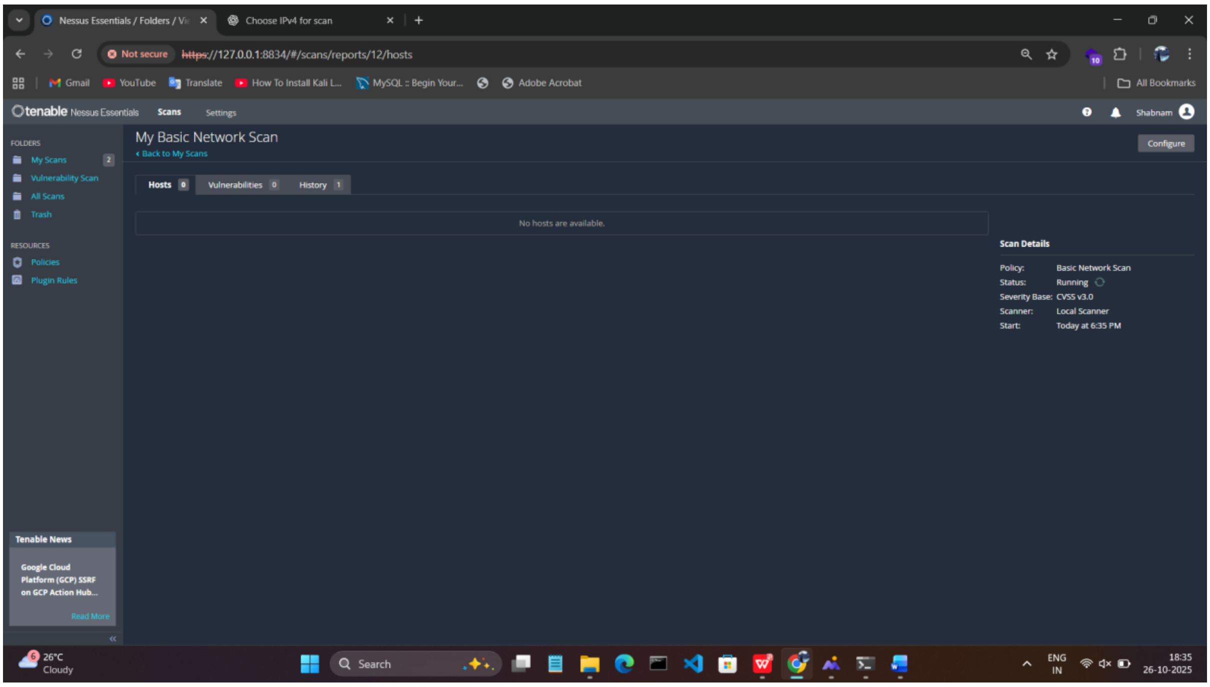
Discovering Hosts...

2. Scan Overview

The scan evaluated the system for known vulnerabilities and misconfigurations. The results were categorized based on severity:

Severity	Count
Critical	0
High	0
Medium	2
Low	0
Info	88

Key Observation: While there were no critical or high vulnerabilities, two medium-level vulnerabilities were identified. These issues, if left unaddressed, could allow attackers to exploit the system for man-in-the-middle attacks or compromise the trust of secure communications.



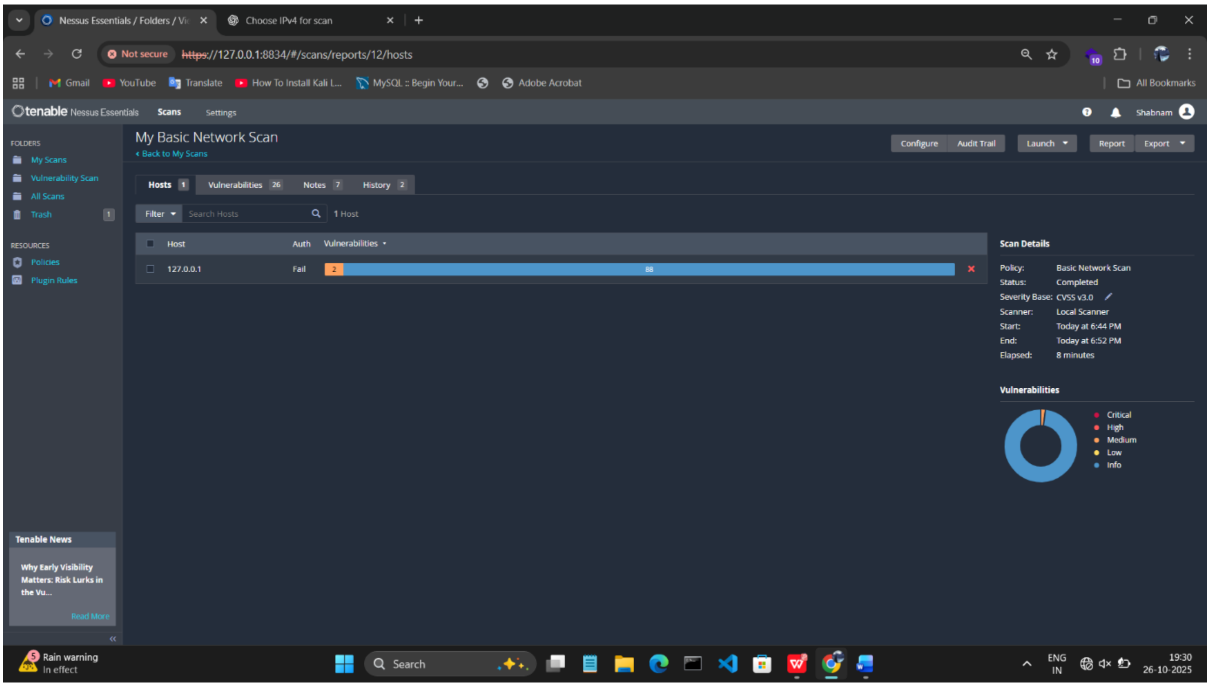
https://127.0.0.1:8834/#/scans/reports/12/hosts

My Basic Network Scan

No hosts are available.

Scan Details

Policy: Basic Network Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:35 PM



My Basic Network Scan

‹ Back to My Scans

1 Host

Host	Auth	Vulnerabilities
127.0.0.1	Fail	2 88

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:44 PM
End: Today at 6:52 PM
Elapsed: 8 minutes

Vulnerabilities

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Info

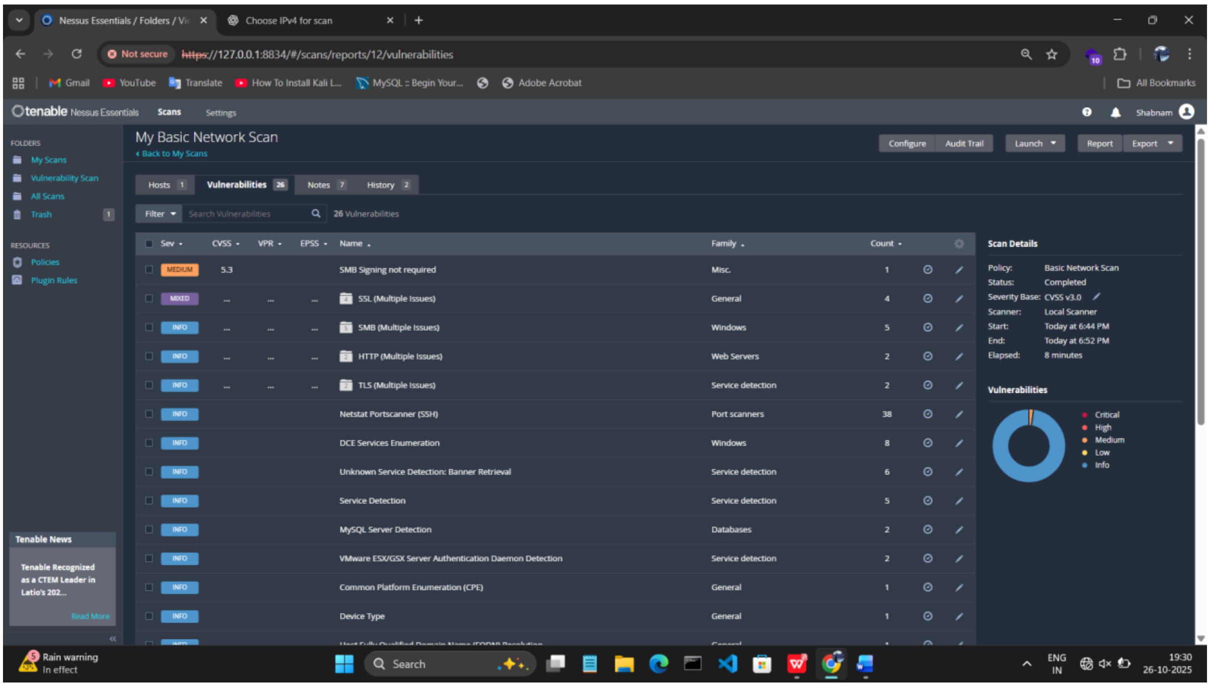
3. Identified Vulnerabilities and Analysis

3.1 SMB Signing Not Required (Medium)

- **Description:** The scan revealed that the **Server Message Block (SMB) protocol** on the system does not enforce message signing. This means an unauthenticated attacker could potentially intercept and modify SMB traffic between the server and clients.
- **Impact:** Without SMB signing, sensitive information transmitted over the network could be compromised, allowing attackers to manipulate or capture data. This is a serious concern in environments where file sharing is frequent.
- **Recommended Mitigation:** Enable SMB message signing. On Windows systems, this can be configured via the policy setting: *“Microsoft network server: Digitally sign communications (always)”*. For Samba servers, the corresponding configuration is server signing = mandatory. Implementing this step ensures data integrity and reduces the risk of man-in-the-middle attacks.

3.2 SSL Certificate Cannot Be Trusted (Medium)

- **Description:** The server uses an X.509 certificate that is either self-signed, expired, or part of an incomplete certificate chain. This breaks the chain of trust, meaning users or applications cannot fully verify the authenticity of the server.
- **Impact:** When a certificate cannot be trusted, it opens the door for attackers to perform man-in-the-middle attacks. Users may also see security warnings, which can reduce confidence in the system’s reliability.
- **Recommended Mitigation:** Obtain and install a **trusted SSL certificate** from a recognized Certificate Authority (CA). Ensure the certificate chain is complete and valid. This step will restore trust, enable secure communication, and prevent potential interception by attackers.



Nessus Essentials / Folders / Vi… | Choose IPv4 for scan

Not secure ~~https~~://127.0.0.1:8834/#/scans/reports/12/vulnerabilities

Gmail | YouTube | Translate | How To Install Kali L... | MySQL :: Begin Your... | Adobe Acrobat | All Bookmarks

tenable Nessus Essentials | Scans | Settings | Shabnam

FOLDERS
- My Scans
- Vulnerability Scan
- All Scans
- Trash 1

RESOURCES
- Policies
- Plugin Rules

Tenable News

Tenable Recognized as a CTEM Leader in Latio's 202...

Read More

My Basic Network Scan

‹ Back to My Scans

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | Vulnerabilities 26 | Notes 7 | History 2

Filter | Search Vulnerabilities | 26 Vulnerabilities

Scan Details

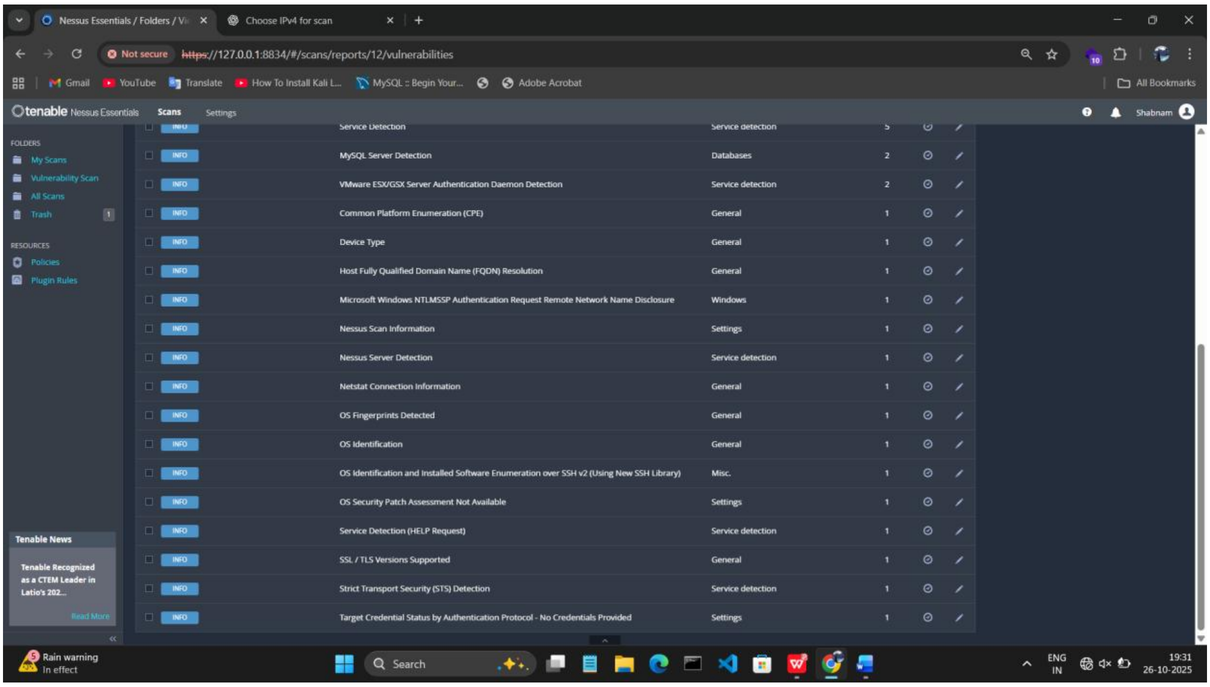
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:44 PM
End:	Today at 6:52 PM
Elapsed:	8 minutes

Vulnerabilities

Rain warning
In effect

Search

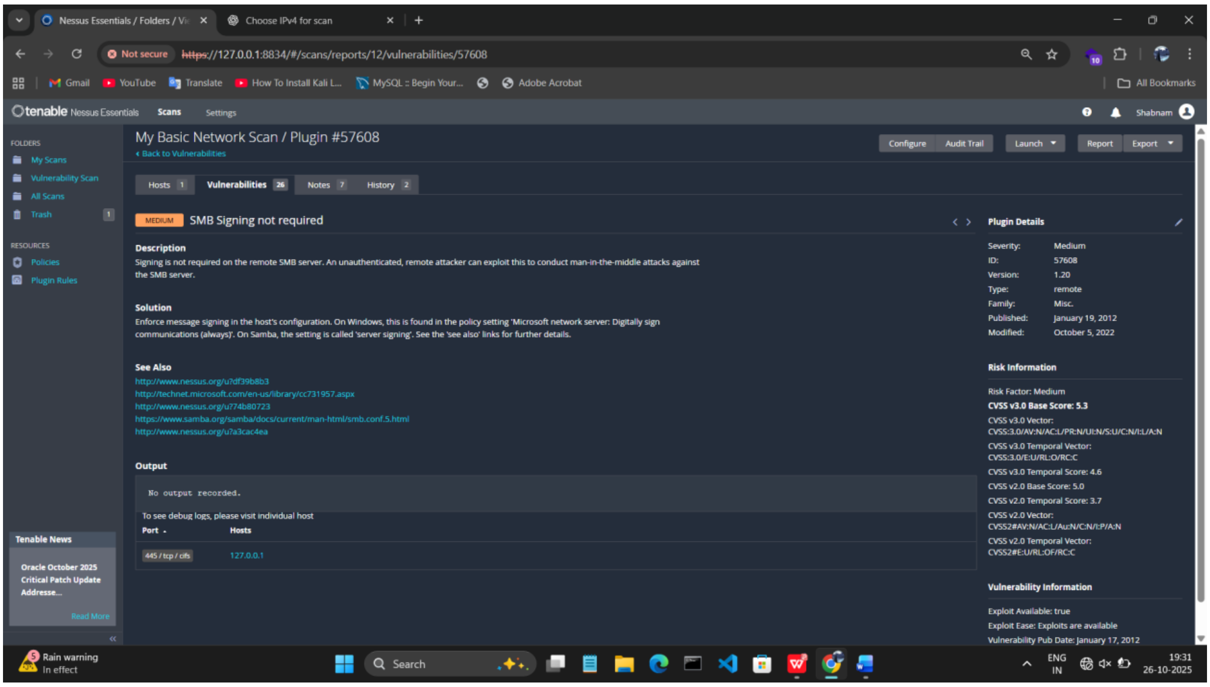
ENG IN 19:30 26-10-2025



Rain warning
In effect

ENG IN 19:31 26-10-2025

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED	...	...	...	SSL (Multiple Issues)	General	4
INFO	...	...	...	SMB (Multiple Issues)	Windows	5
INFO	...	...	...	HTTP (Multiple Issues)	Web Servers	2
INFO	...	...	...	TLS (Multiple Issues)	Service detection	2
INFO				Netstat Portscanner (SSH)	Port scanners	38
INFO				DCE Services Enumeration	Windows	8
INFO				Unknown Service Detection: Banner Retrieval	Service detection	6
INFO				Service Detection	Service detection	5
INFO				MySQL Server Detection	Databases	2
INFO				VMware ESX/GSX Server Authentication Daemon Detection	Service detection	2
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
INFO				Netstat Connection Information	General	1
INFO				OS Fingerprints Detected	General	1
INFO				OS Identification	General	1
INFO				OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)	Misc.	1
INFO				OS Security Patch Assessment Not Available	Settings	1
INFO				Service Detection (HELP Request)	Service detection	1
INFO				SSL / TLS Versions Supported	General	1
INFO				Strict Transport Security (STS) Detection	Service detection	1
INFO				Target Credential Status by Authentication Protocol - No Credentials Provided	Settings	1



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	127.0.0.1

Plugin Details

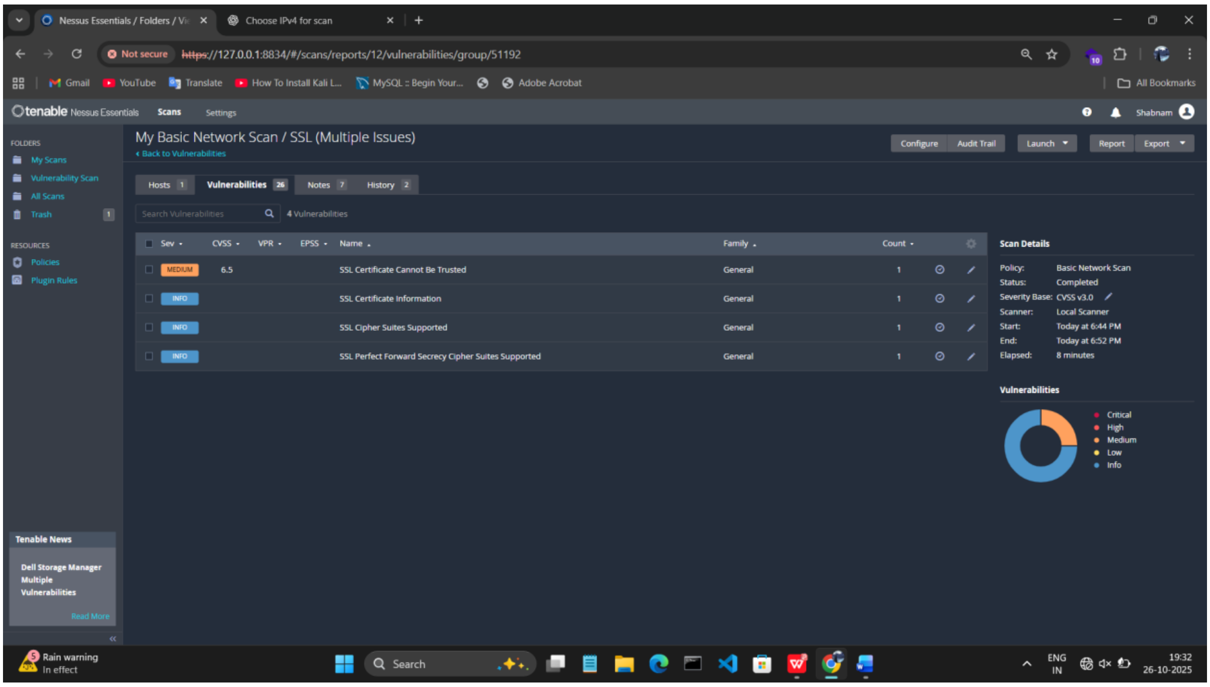
Severity:	Medium
ID:	57608
Version:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

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

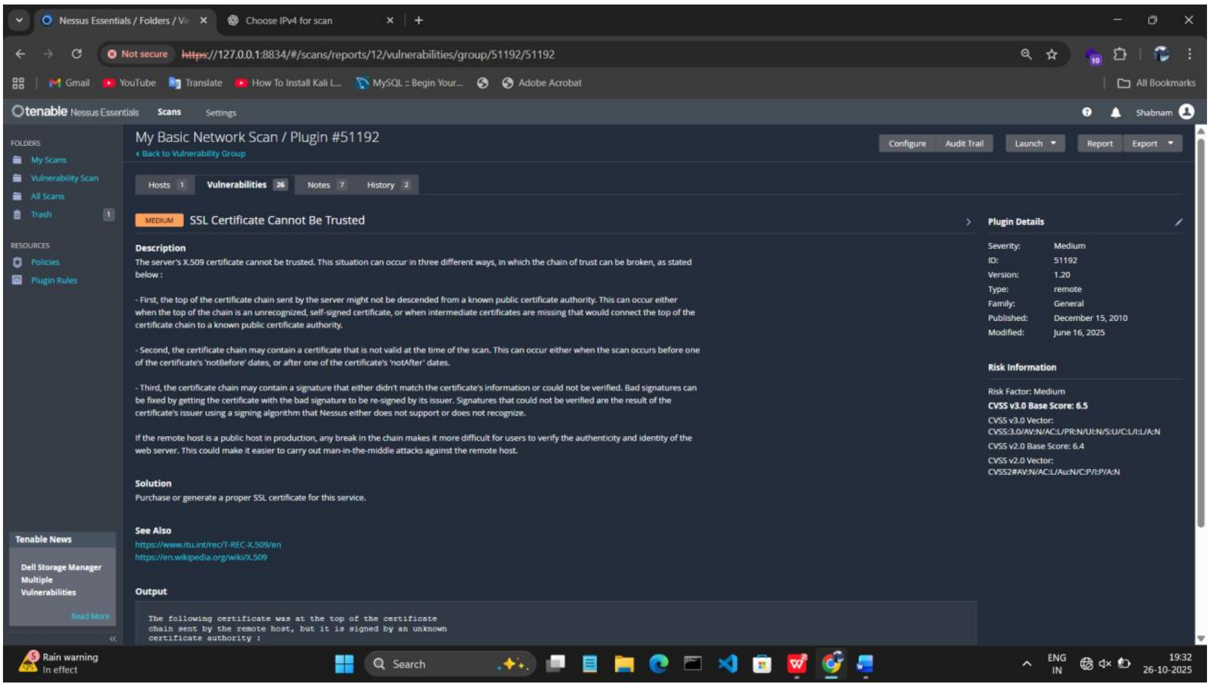
4 Vulnerabilities

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:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:44 PM
End:	Today at 6:52 PM
Elapsed:	8 minutes

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

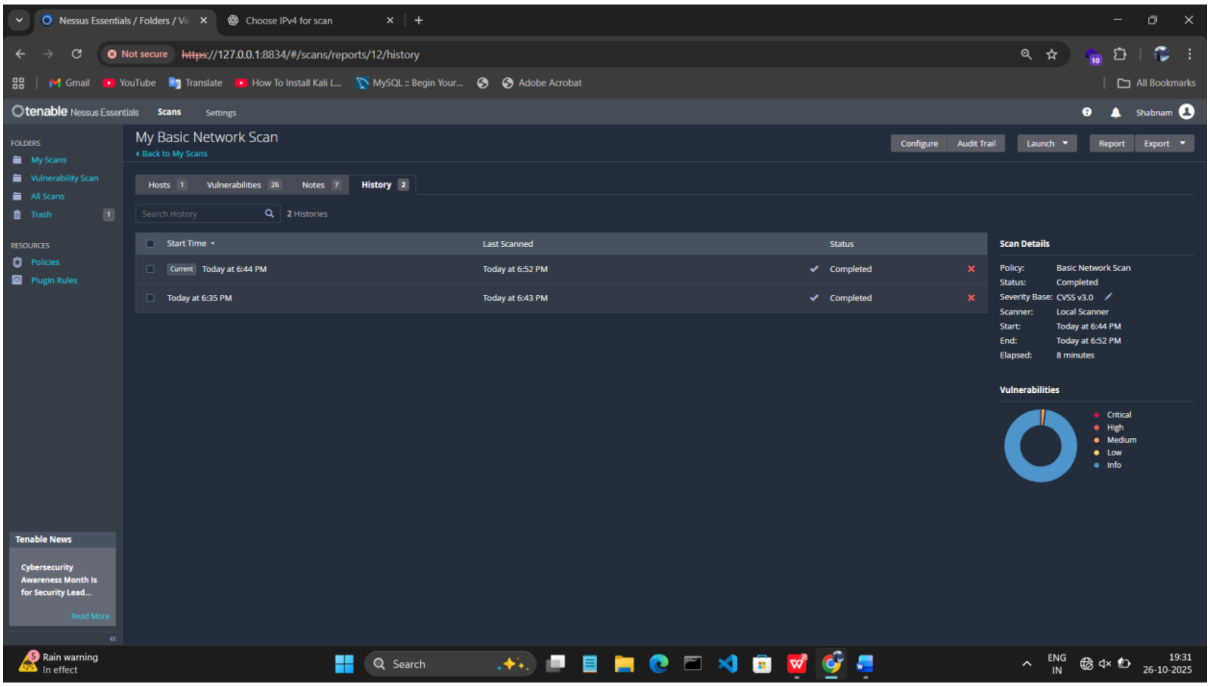
```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :
```

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



My Basic Network Scan

‹ Back to My Scans

Start Time	Last Scanned	Status
Current Today at 6:44 PM	Today at 6:52 PM	✓ Completed
Today at 6:35 PM	Today at 6:43 PM	✓ Completed

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 6:44 PM
End:	Today at 6:52 PM
Elapsed:	8 minutes

Vulnerabilities

Conclusion:

The Nessus scan identified two medium-level vulnerabilities on the localhost system. While no critical or high-risk issues were detected, addressing these medium vulnerabilities is essential for improving system security.