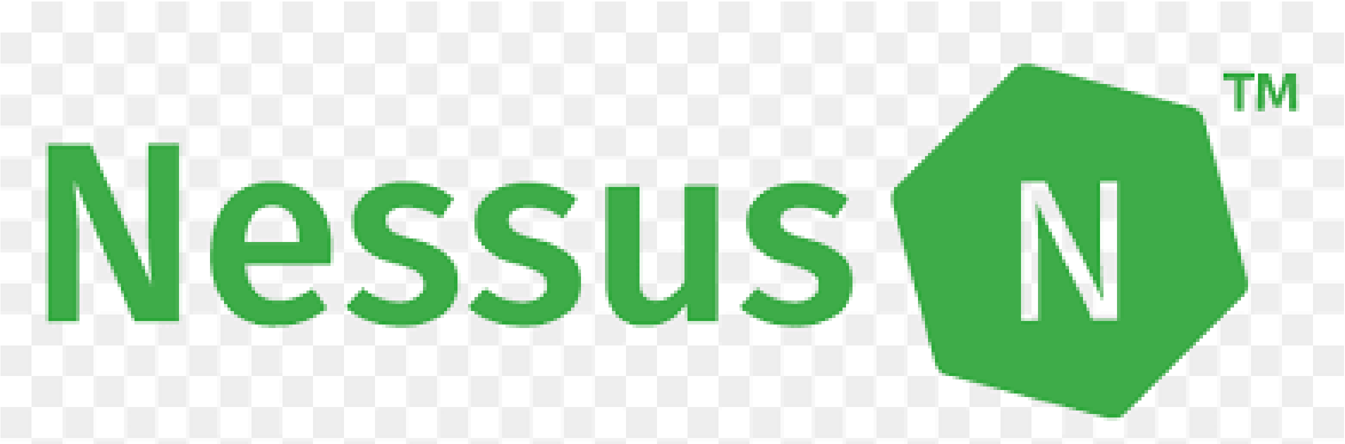
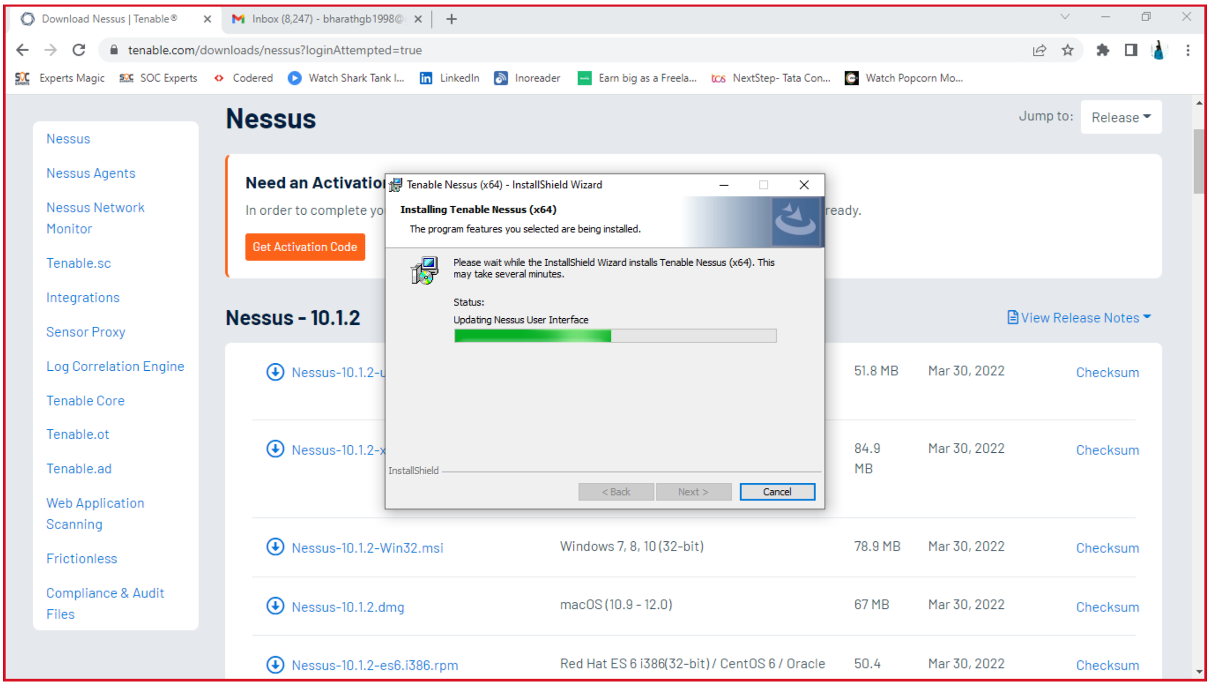
NESSUS

- Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.
- It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.
- Nessus is not a complete security solution; it is only a tool that checks your computers to find vulnerabilities that hackers COULD exploit. IT IS UP TO THE SYSTEM ADMINISTRATOR TO PATCH THESE VULNERABILITIES IN ORDER TO CREATE A SECURITY SOLUTION.
- Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.



Installation of Nessus

1. Register yourself in Nessus site(https://www.tenable.com/products/nessus/nessus-essentials) to receive activation code.
2. Download the executable file according to your system architecture(64bit/32bit).
3. Initiate installation it will take some time for installing and compiling the plugins.



Nessus

Need an Activatio

In order to complete yo ready.

Tenable Nessus (x64) - InstallShield Wizard

Installing Tenable Nessus (x64)

The program features you selected are being installed.

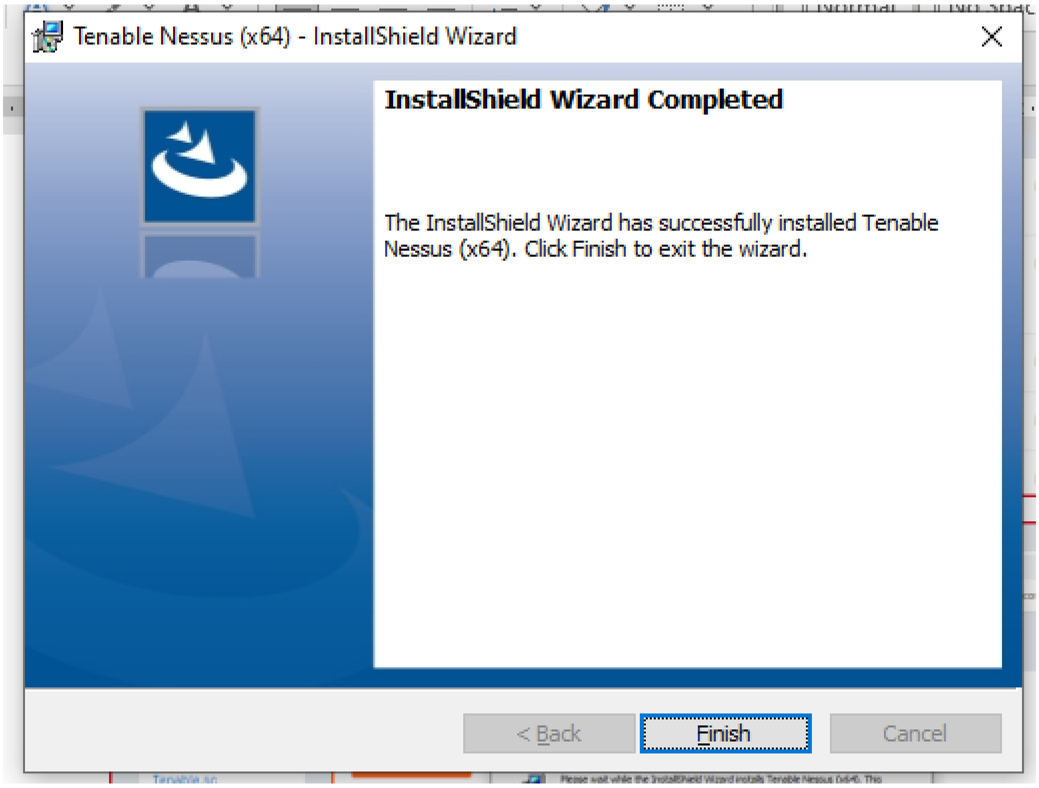
Please wait while the InstallShield Wizard installs Tenable Nessus (x64). This may take several minutes.

Status:

Updating Nessus User Interface

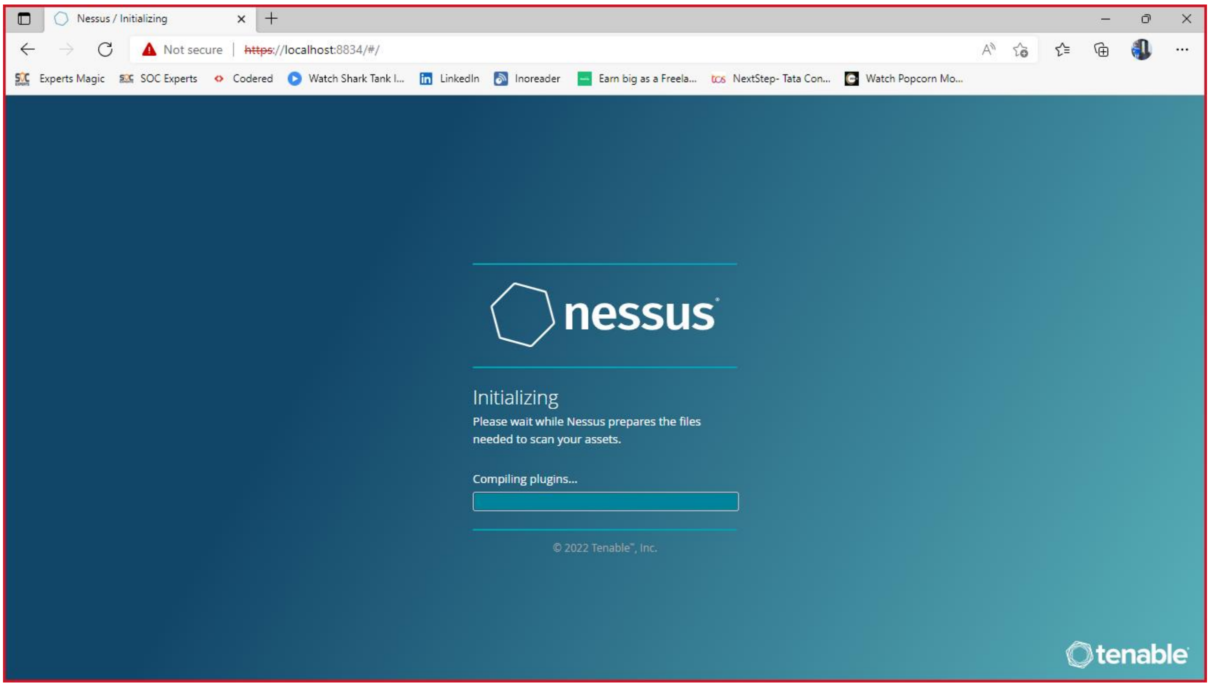
Nessus - 10.1.2

Nessus-10.1.2-u		51.8 MB	Mar 30, 2022	Checksum
Nessus-10.1.2-x		84.9 MB	Mar 30, 2022	Checksum
Nessus-10.1.2-Win32.msi	Windows 7, 8, 10 (32-bit)	78.9 MB	Mar 30, 2022	Checksum
Nessus-10.1.2.dmg	macOS (10.9 - 12.0)	67 MB	Mar 30, 2022	Checksum
Nessus-10.1.2-es6.i386.rpm	Red Hat ES 6 i386(32-bit) / CentOS 6 / Oracle	50.4	Mar 30, 2022	Checksum



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Tenable Nessus (x64). Click Finish to exit the wizard.

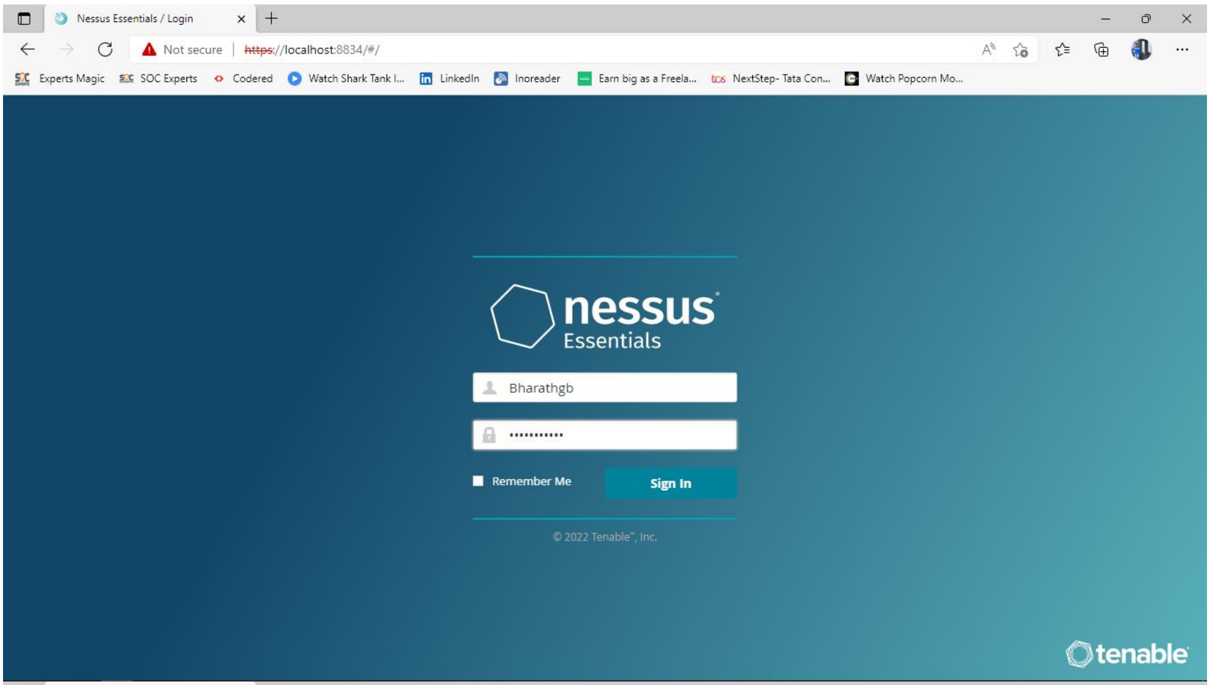


Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Compiling plugins...

© 2022 Tenable®, Inc.



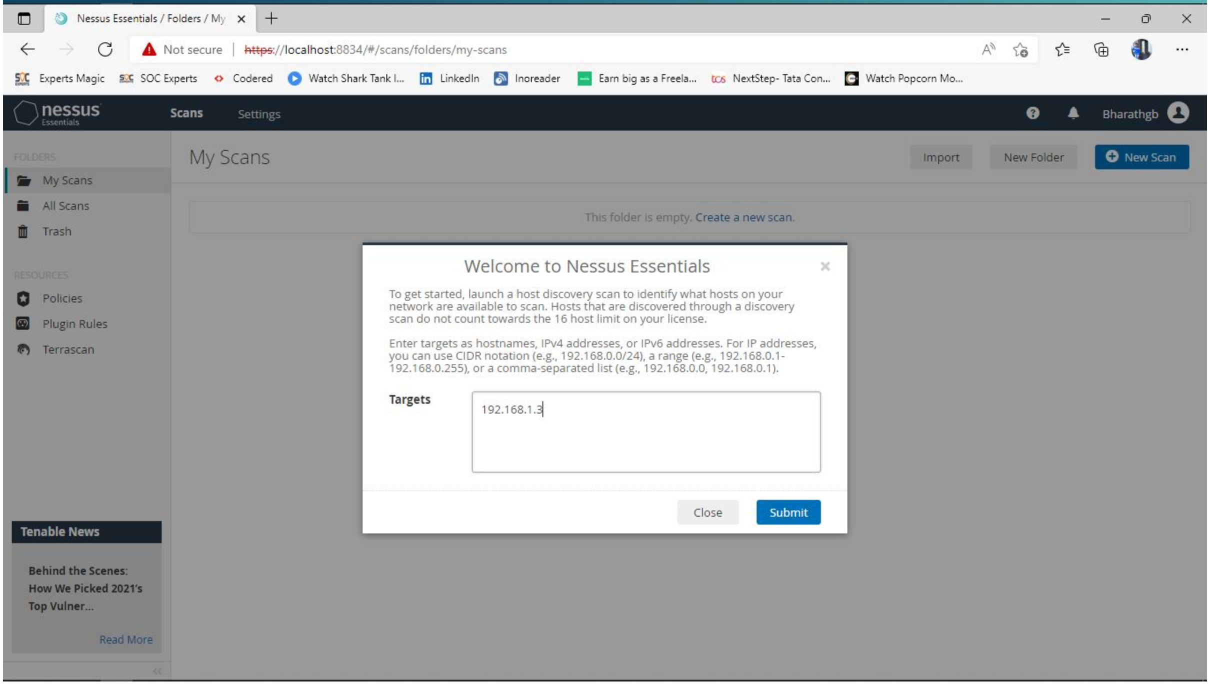
Bharathgb

••••••••••••

□ Remember Me

Sign In

© 2022 Tenable®, Inc.



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.

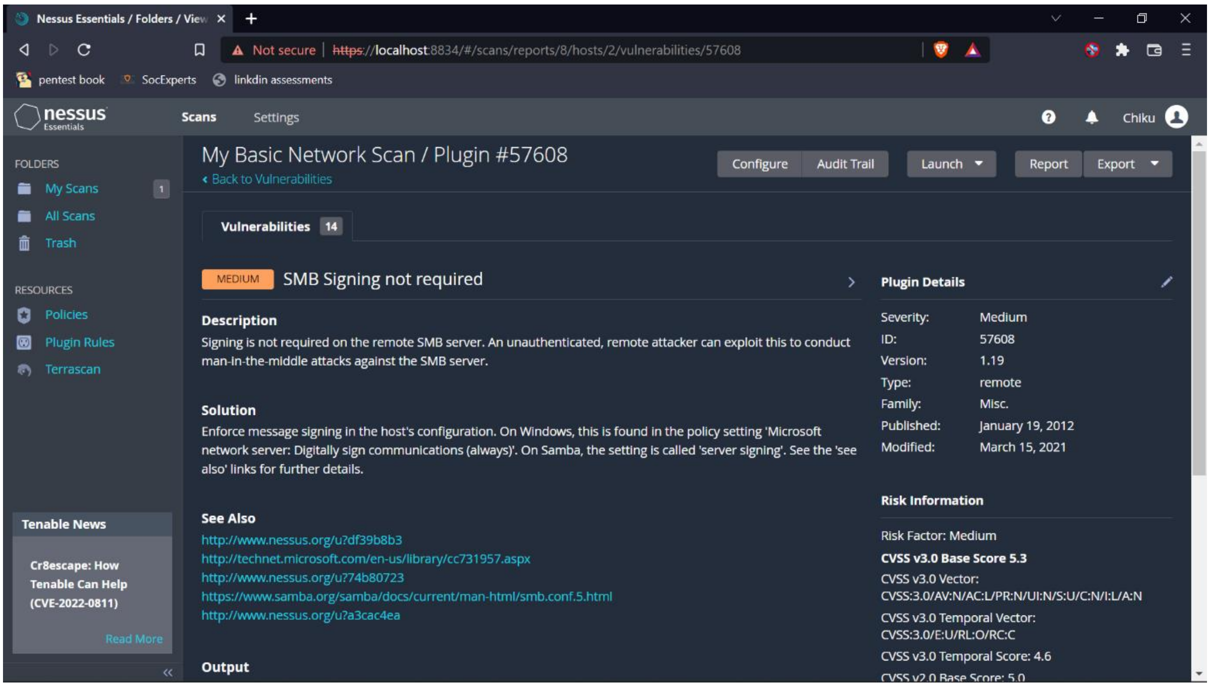
Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets 192.168.1.3

Close Submit

Basic scans using Nessus.

1. Start a scan
2. Give your system IP and start scan.



My Basic Network Scan / Plugin #57608

‹ Back to Vulnerabilities

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

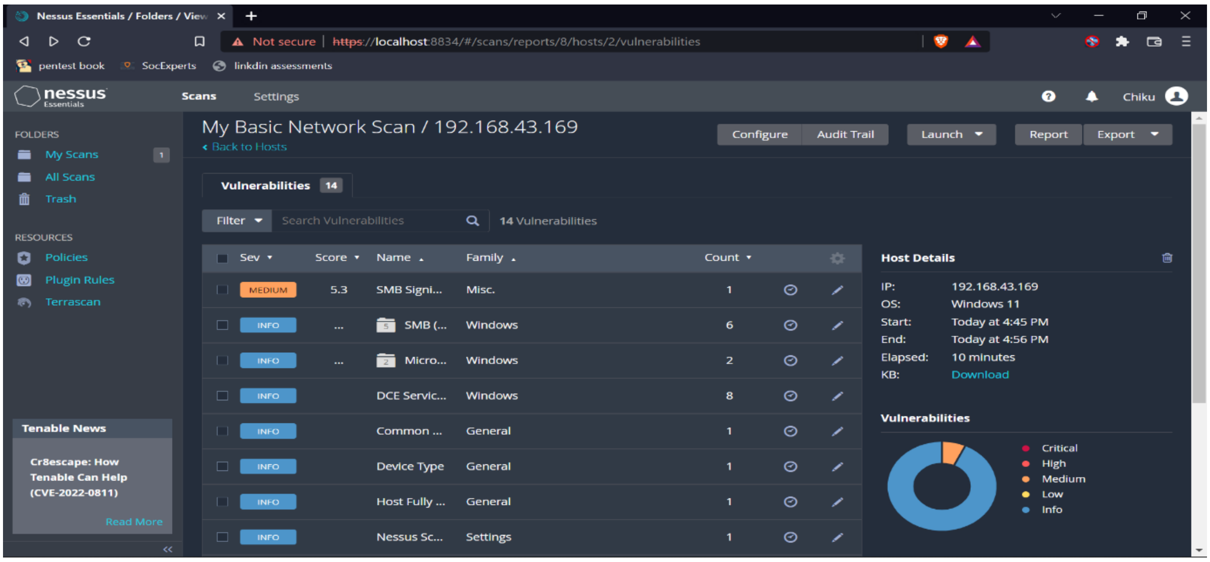
Output

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.19
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	March 15, 2021

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



My Basic Network Scan / 192.168.43.169

‹ Back to Hosts

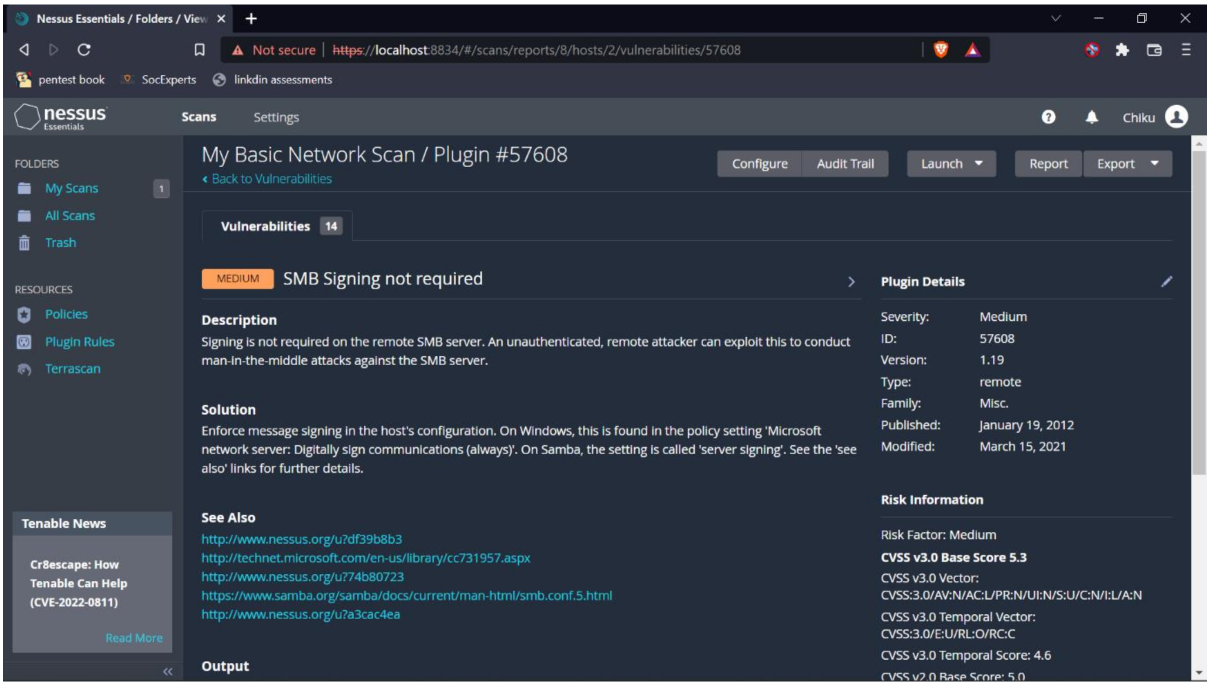
14 Vulnerabilities

Sev	Score	Name	Family	Count
MEDIUM	5.3	SMB Signi...	Misc.	1
INFO	...	5 SMB (...	Windows	6
INFO	...	2 Micro...	Windows	2
INFO		DCE Servic...	Windows	8
INFO		Common ...	General	1
INFO		Device Type	General	1
INFO		Host Fully ...	General	1
INFO		Nessus Sc...	Settings	1

Host Details

IP:	192.168.43.169
OS:	Windows 11
Start:	Today at 4:45 PM
End:	Today at 4:56 PM
Elapsed:	10 minutes
KB:	Download

Vulnerabilities



My Basic Network Scan / Plugin #57608

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

Plugin Details

Severity:	Medium
ID:	57608
Version:	1.19
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	March 15, 2021

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