#TASK 3

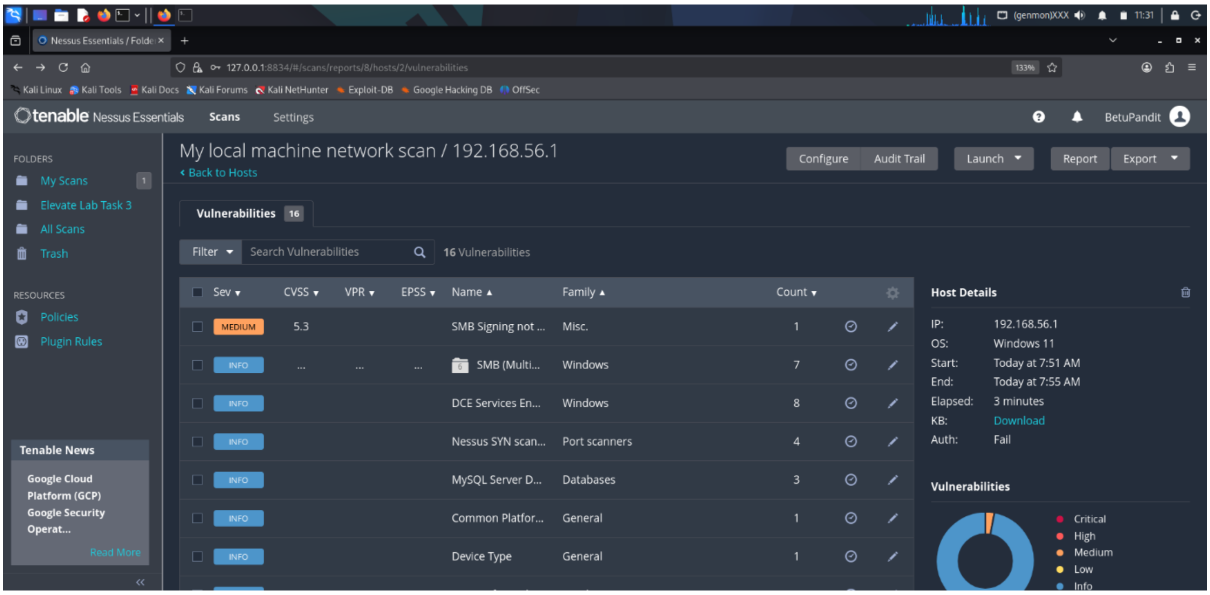
VULNERABILITY REPORT

Name: SMB Signing Not Required

Plugin ID: 57608

Severity: Medium

Affected Host: Windows Local Machine



My local machine network scan / 192.168.56.1

‹ Back to Hosts

Vulnerabilities 16

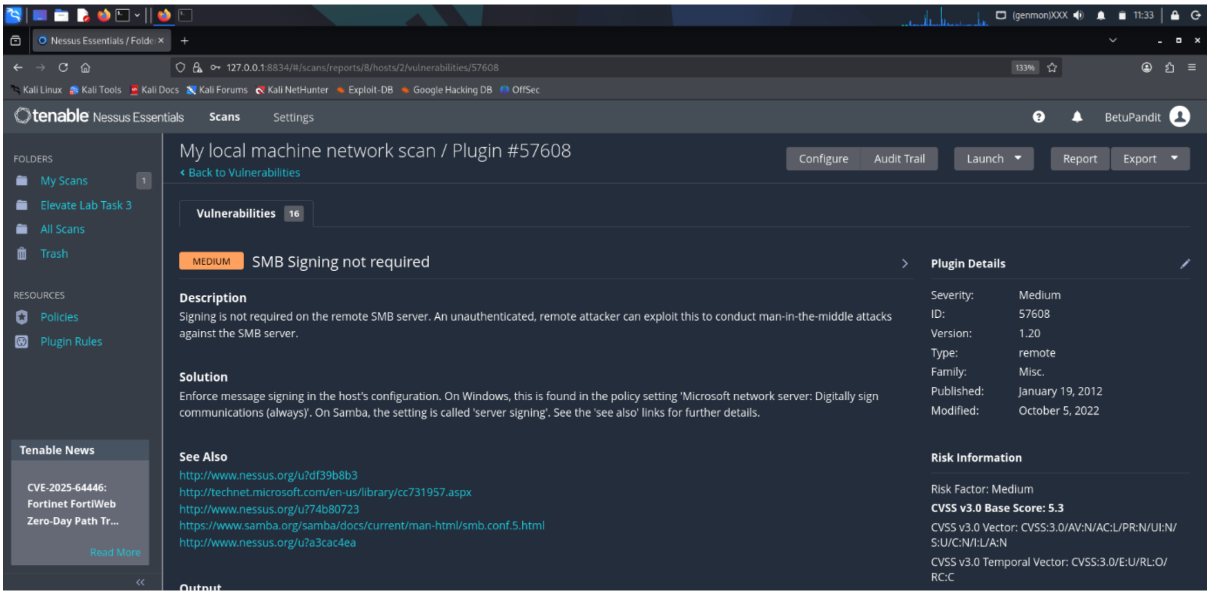
16 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not ...	Misc.	1
INFO	...	...	...	6 SMB (Multi...	Windows	7
INFO				DCE Services En...	Windows	8
INFO				Nessus SYN scan...	Port scanners	4
INFO				MySQL Server D...	Databases	3
INFO				Common Platfor...	General	1
INFO				Device Type	General	1

Host Details

IP:	192.168.56.1
OS:	Windows 11
Start:	Today at 7:51 AM
End:	Today at 7:55 AM
Elapsed:	3 minutes
KB:	Download
Auth:	Fail

Vulnerabilities



My local machine network scan / Plugin #57608

‹ Back to Vulnerabilities

Vulnerabilities 16

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:	1.20
Type:	remote
Family:	Misc.
Published:	January 19, 2012
Modified:	October 5, 2022

Risk Information

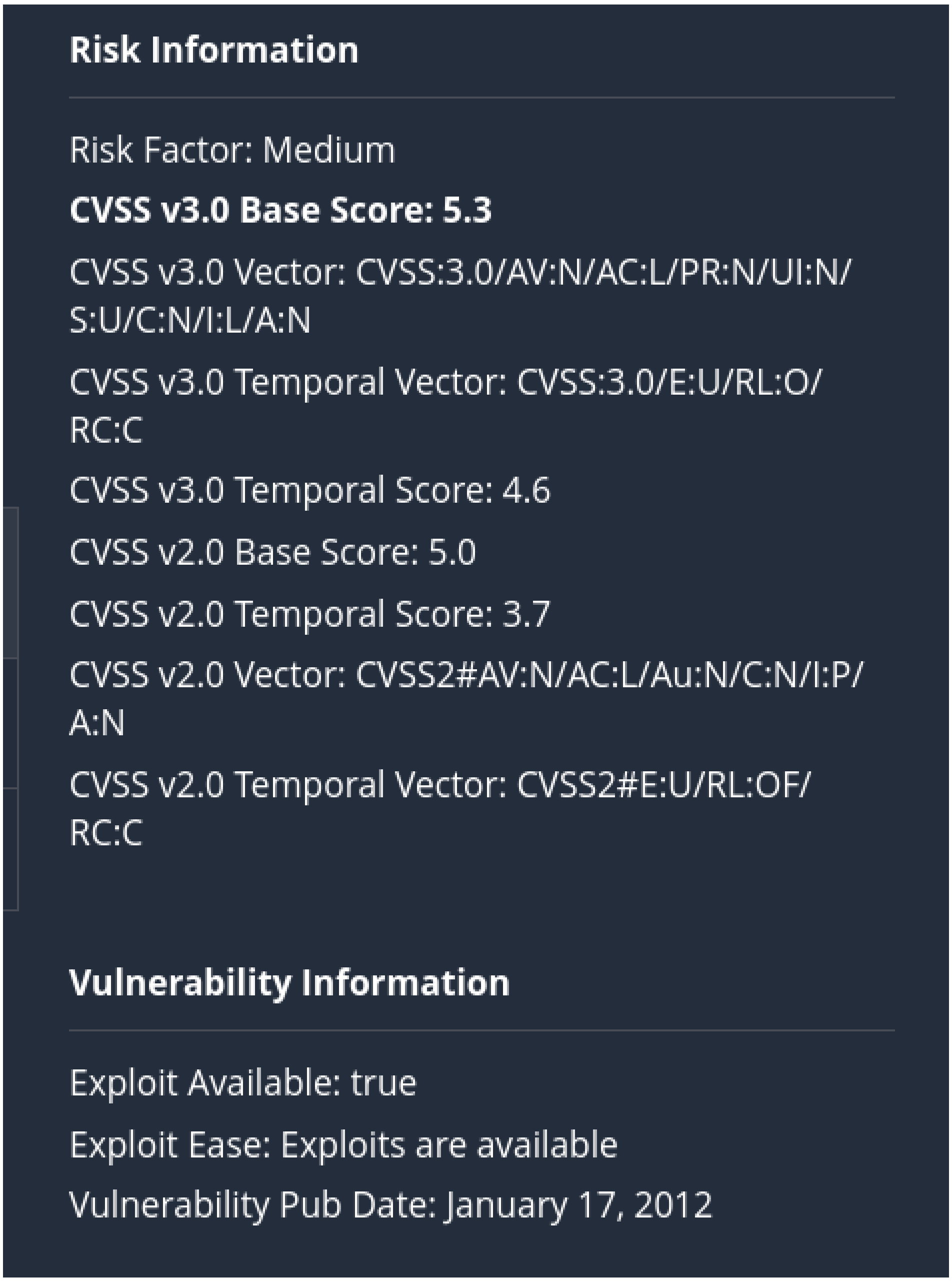
Risk Factor: Medium

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 Score and Risk Information



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

1. Description

The target system has SMB (Server Message Block) signing disabled or not required.

SMB signing ensures that all SMB packets exchanged between the client and server are digitally signed to prevent tampering.

When SMB signing is not required, an attacker on the same network can:

- Modify SMB packets (man-in-the-middle attack)
- Impersonate an SMB server
- Inject malicious responses
- Capture NTLM authentication attempts

This weakens the integrity of SMB communication.

2. Impact

Without SMB signing, the system becomes vulnerable to:

- MITM (Man-in-the-Middle) attacks
- Session hijacking
- Replay attacks
- Credential interception
- Unauthorized file access
- Attackers can modify or inject SMB traffic without detection, threatening both confidentiality and integrity.

3. Evidence (from Nessus Output)

- Nessus identified that the SMB server on this system does not enforce signing.
- This means SMB clients can communicate without validating signatures.

(You can show screenshot here)

4. Solution

Enable and enforce SMB packet signing on the host:

For Windows:

1. Open Local Group Policy Editor

gpedit.msc

2. Navigate to:

Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

3. Enable the following policies:

✓ Microsoft network client: Digitally sign communications (always)

✓ Microsoft network server: Digitally sign communications (always)

4. Restart the system for changes to apply.

5. Risk Level

Medium – Exploitation requires attacker to be on the same network, but the impact is significant if performed successfully.

6. Recommendation

It is recommended to enable SMB signing on all systems to prevent unauthorized modification of SMB traffic and to protect against network-based attacks, especially in environments where file sharing is used.