Vulnerability Scan Report — Task 3

Analyst: Arshiya Sulthana

Date: [25-09-25]

Tool Used: Nessus Essentials

Target: Localhost / My PC

1. Scan Setup

- Type of Scan: Basic Network Scan

- Target IP: 127.0.0.1

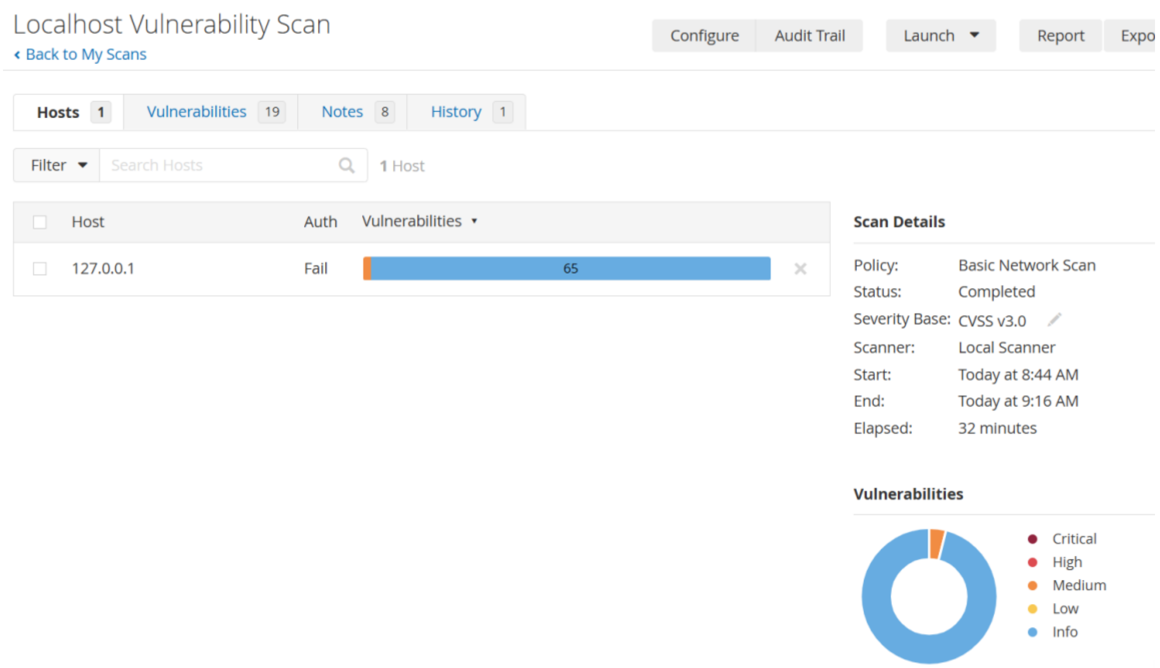
- Duration: 30 minutes

2. Scan Summary

Total Vulnerabilities Found:

- Critical: 0   - High: 0

Medium: 1   - Low: 0   - Info: 18



Localhost Vulnerability Scan

□	Host	Auth	Vulnerabilities ▾
□	127.0.0.1	Fail	65

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:44 AM
End:	Today at 9:16 AM
Elapsed:	32 minutes

Vulnerabilities

3. Key Vulnerabilities Identified

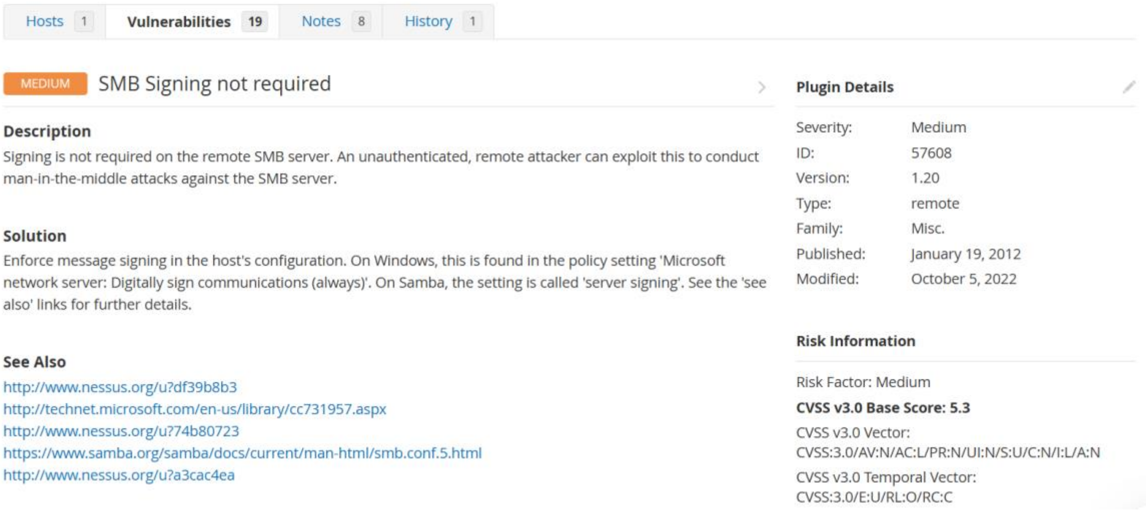
▨ Medium Vulnerability 1

Name: SMB Signing Not Required

Affected Port/Service: 445 / tcp / cifs

Risk: Allows attackers to perform man-in-the-middle attacks.

Recommendation: Enable SMB signing or apply latest Windows patches.



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

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

4. Observations and simple fixes

- **Observations**

- The Nessus scan identified **1 Medium vulnerability (SMB Signing not required)** and **18 informational findings**.
- While the informational findings do not pose direct risk, they highlight services and configurations that could be exploited if combined with other attacks.
- The most notable risk is the missing SMB signing, which can expose the system to **man-in-the-middle (MITM) attacks**.

-Simple Fixes

- Enable SMB signing in Windows security policies.
- Regularly apply Windows security updates.

- Disable unused network services (e.g., SMBv1, NetBIOS).
- Configure firewall rules to limit unnecessary network exposure.