Vulnerability Assessment Report – Task 3

1. Executive Summary

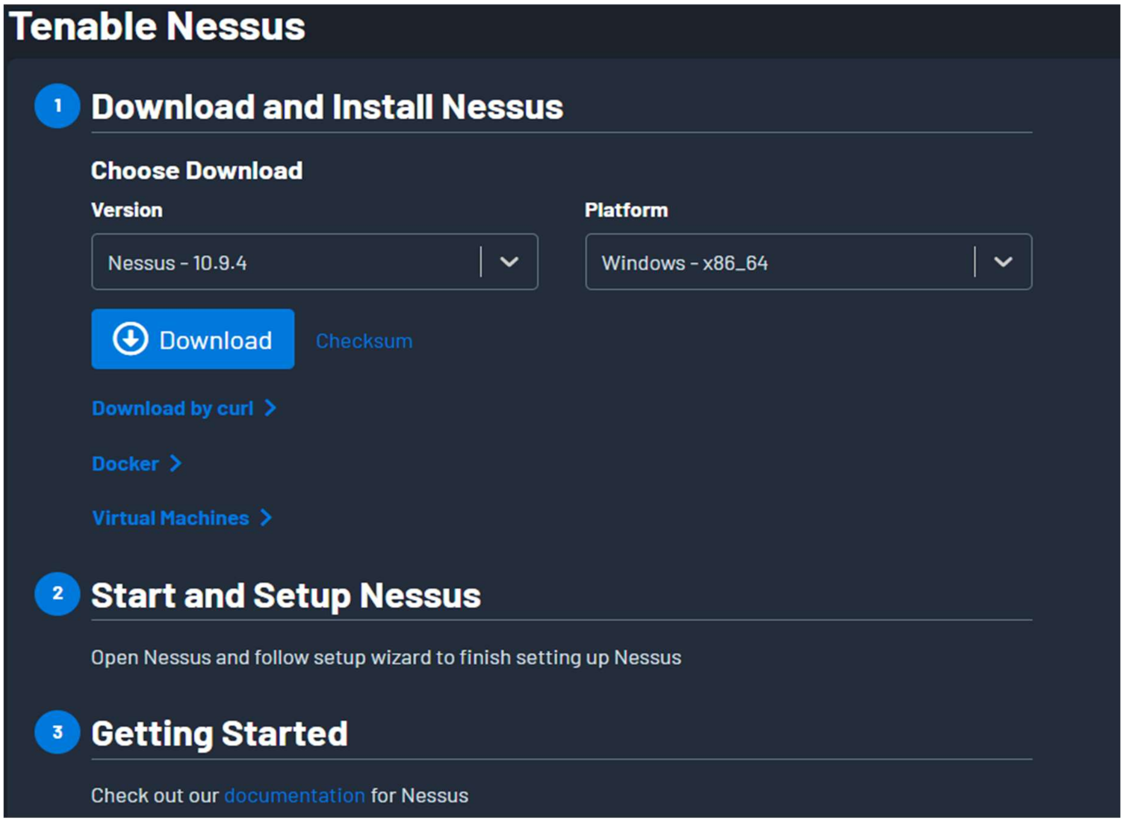
A basic vulnerability scan was performed on the local machine using Nessus Essentials. The scan identified **X vulnerabilities** (Critical: Y, High: Z, Medium: W, Low: V). The report summarizes the issues, their potential impact, and recommended remediation steps.

2. Scope of Work

- **Target:** Machine IP
- **Tool Used:** Nessus Essentials
- **Scan Type:** Full System Vulnerability Scan
- **Scan Date:** [25/09/2025]

3. Methodology

1. Installed and configured the vulnerability scanner.



Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.9.4

Platform: Windows - x86_64

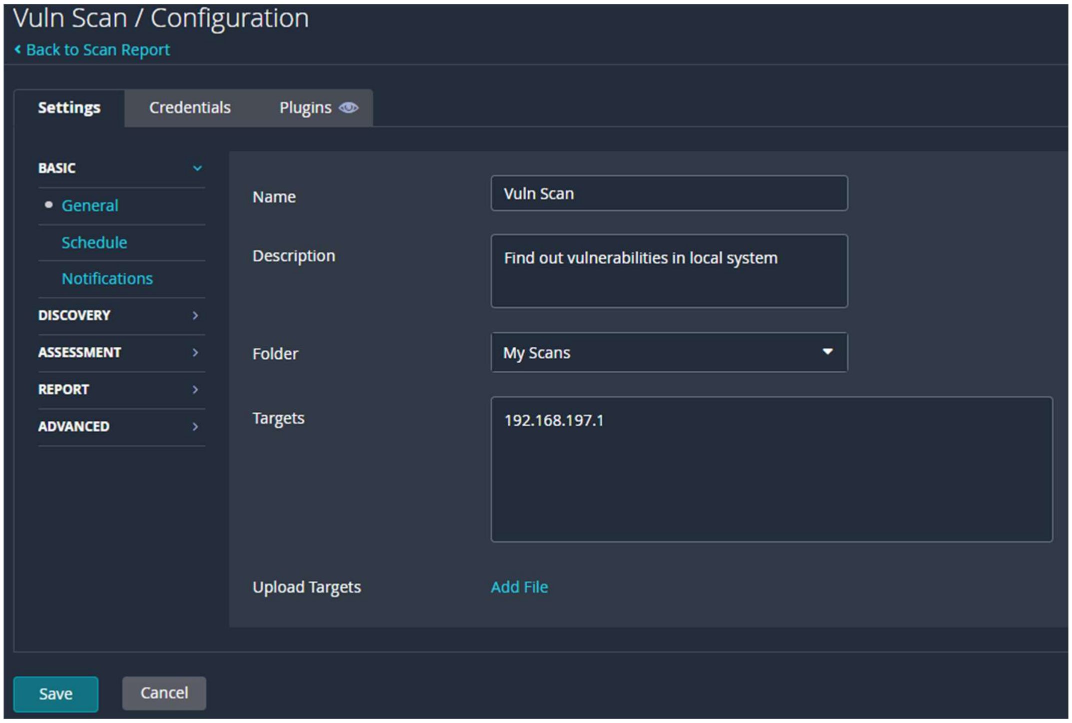
2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

3 Getting Started

Check out our documentation for Nessus

2. Defined the target as the local machine IP.



Vuln Scan / Configuration

‹ Back to Scan Report

Name: Vuln Scan

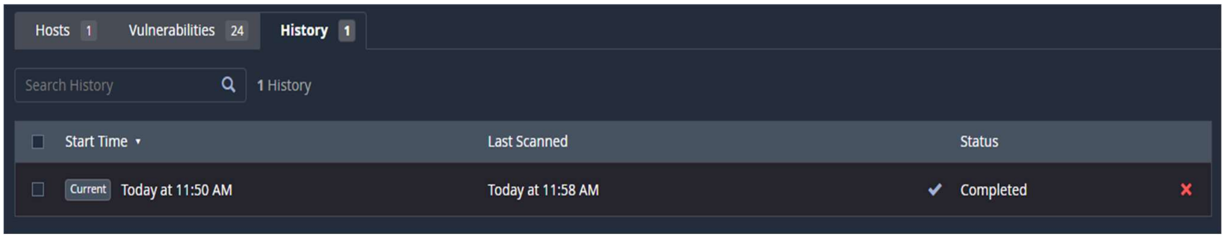
Description: Find out vulnerabilities in local system

Folder: My Scans

Targets: 192.168.197.1

Upload Targets: Add File

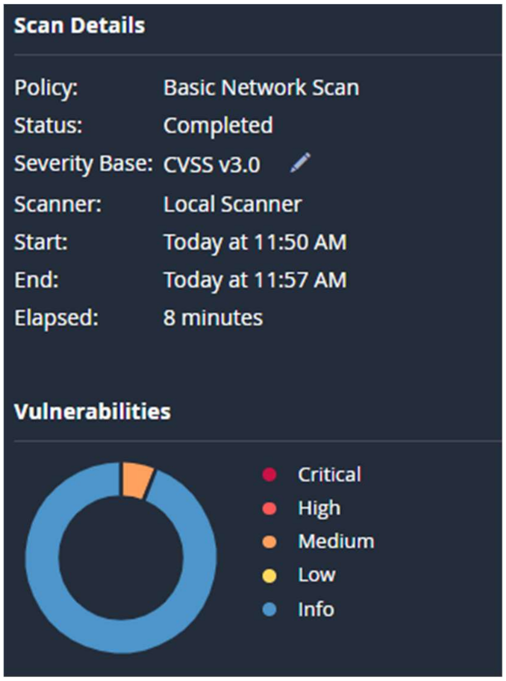
3. Performed a **full scan** to identify vulnerabilities.



1 History

☐	Start Time ▾	Last Scanned	Status	
☐	Current Today at 11:50 AM	Today at 11:58 AM	✓ Completed	✕

4. Collected scan results and categorized vulnerabilities.



Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

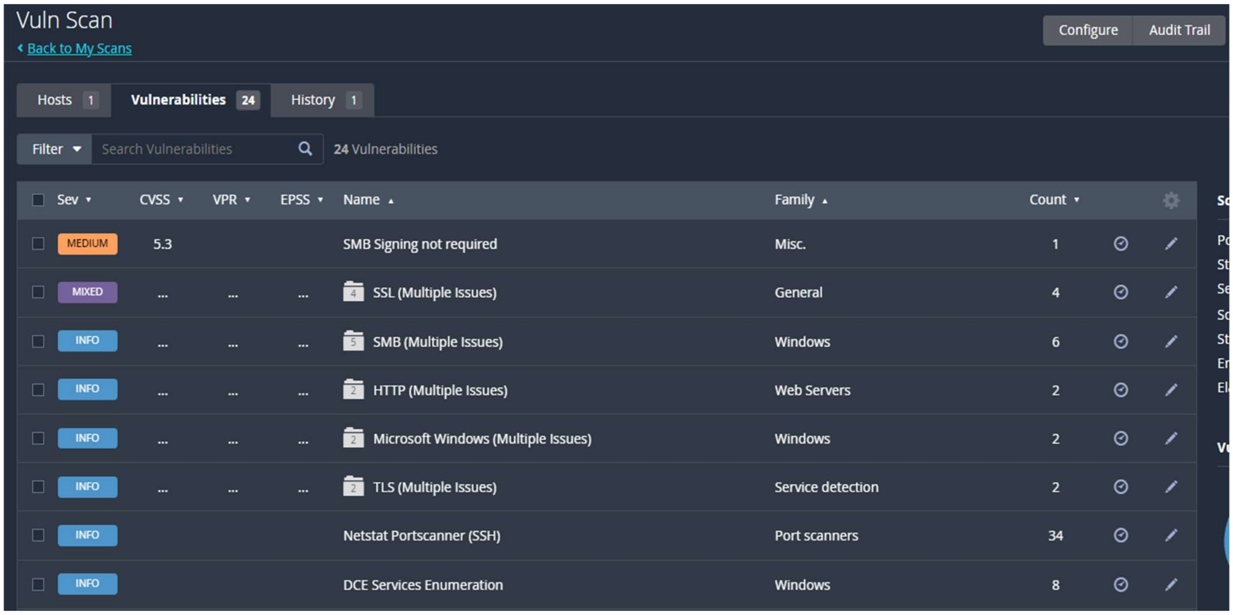
Start: Today at 11:50 AM

End: Today at 11:57 AM

Elapsed: 8 minutes

Vulnerabilities

5. Documented the most critical vulnerabilities. (include in findings)



24 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 Microsoft Windows (Multiple Issues)	Windows	2	⊘	✎
□	INFO	...	...	...	2 TLS (Multiple Issues)	Service detection	2	⊘	✎
□	INFO				Netstat Portscanner (SSH)	Port scanners	34	⊘	✎
□	INFO				DCE Services Enumeration	Windows	8	⊘	✎

4. Findings

Vuln-Id: 001
Vuln-Name: SMB signing not required
Severity: Medium
CVSS: 5.3

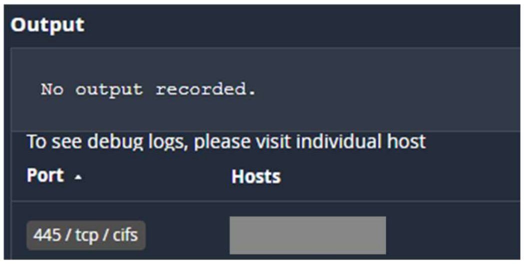
Description

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.

Remediation

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 ‘references' links for further details.

Output



Output

```
No output recorded.
```

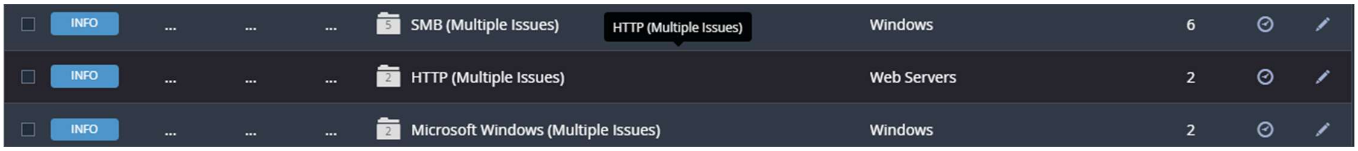
To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	[redacted]

References

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

Other Vulns Severity Level (Info)



HTTP (Multiple Issues)

□	INFO	...	...	...	5 SMB (Multiple Issues)	Windows	6	⊘	✎
□	INFO	...	...	...	2 HTTP (Multiple Issues)	Web Servers	2	⊘	✎
□	INFO	...	...	...	2 Microsoft Windows (Multiple Issues)	Windows	2	⊘	✎

7. Remediation Plan for Endpoint Security

1) Apply security patches for outdated software.
2) Disable legacy services (like SMBv1, weak ciphers).
3) Regularly update OS and applications.
4) Schedule monthly vulnerability scans.

8. Conclusion

The scan revealed multiple vulnerabilities ranging from low to critical severity. Addressing these issues will significantly improve the security posture of the system. Regular vulnerability scans, combined with timely patching, are recommended.