

TASK-3

1. Review of Vulnerabilities and Severity

The Nessus scan conducted on host 127.0.0.1 identified a total of 33 vulnerabilities. These vulnerabilities are categorized by severity as follows:

- CRITICAL: 0
- HIGH: 0
- MEDIUM: 2
- LOW: 0
- INFO: 31

While there are no critical or high severity findings, the presence of medium and numerous informational findings still poses risks, particularly if they are leveraged together.

2. Fixes or Mitigations

Below are suggested remediations for some of the identified vulnerabilities:

- SSL Certificate Cannot Be Trusted (Plugin ID 51192):
Use a certificate from a trusted certificate authority (CA).
- SMB Signing Not Required (Plugin ID 57608):
Enable SMB signing in group policies to prevent man-in-the-middle attacks.

For informational findings, it is recommended to review exposure and disable unnecessary services.

3. Most Critical Vulnerabilities

The following medium severity vulnerabilities require attention:

1. SSL Certificate Cannot Be Trusted

- CVSS: 6.5
- Remediation: Replace with a certificate signed by a trusted authority.

2. SMB Signing Not Required

- CVSS: 5.3
- Remediation: Configure SMB to require signing for added security.

4. Screenshot of Scan Results

tenable

Nessus Essentials

Scans

Settings

maxranjan

FOLDERS

Hide

My Scans

All Scans

Trash

RESOURCES

Policies

Plugin Rules

Terrascan

Tenable News

Where Capability Meets Opportunity: Introducing th...

Read More

mine

Back to My Scans

Configure

Audit Trail

Launch

Report

Export

Hosts

Vulnerabilities

Notes

History

Filter

Search Hosts

1 Host

Host

Vulnerabilities

127.0.0.1

2

77

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 8:15 PM

End: Today at 8:23 PM

Elapsed: 8 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

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

21:52