

TASK 3: - Basic Vulnerability Scan Report

This report documents the results of a basic vulnerability scan performed on my PC using Nessus Essentials.

SCAN SUMMARY:

Total vulnerability found	23
Critical	0
High	0
Medium	1
Low	0
Info	21
Mixed	1

Top identified vulnerabilities:

1. SMB signing not required

Vulnerability Name	SMB signing not required
Severity	Medium
Risk	May allow man-in-the-middle attacks by altering SMB traffic.
Fix	Enable SMB signing in Windows group policy.

2.SSL (Multiple issues)

Vulnerability Name	SSL (Multiple Issues)
Severity	Mixed
Risk	Outdated or Weak SSL/TLS configurations may expose encrypted data.
Fix	Disable weak ciphers and update TLS settings.

3.Service Detection /Enumeration Findings

Vulnerability Name	Service Detection/Enumeration Findings
Severity	Info
Risk	Information disclosure can aid attackers in mapping services.
Fix	Limit services exposure and disable unused services.

SCAN Evidence (Screenshots)

Below are screenshots from the Nessus Essentials vulnerability:

1: Host Scan Result

Hosts 1 **Vulnerabilities** 23 **History** 1

Filter Search Hosts 1 Host

Host	Auth	Vulnerabilities
10.98.71.3	Fail	23

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:49 PM
End: Today at 1:58 PM
Elapsed: 8 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (0), High (0), Medium (0), Low (0), Info (23).

2.Vulnerability Summary page:

Hosts 1 **Vulnerabilities** 23 **History** 1

Filter Search Vulnerabilities 23 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED				SSL (Multiple Issues)	General	4
INFO				SMB (Multiple Issues)	Windows	6
INFO				HTTP (Multiple Issues)	Web Servers	2
INFO				Microsoft Windows (Mu...	Windows	2
INFO				TLS (Multiple Issues)	Service detection	2
INFO				Netstat Portscanner (SSH)	Port scanners	25
INFO				DCE Services Enumeration	Windows	8
INFO				Service Detection	Service detection	2
INFO				Additional DNS Hostnames	General	1
INFO				Common Platform Enumerat...	General	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:49 PM
End: Today at 1:58 PM
Elapsed: 8 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical (0), High (0), Medium (0), Low (0), Info (23).

3.Scan History page

The screenshot shows the Tenable Nessus Essentials interface. The top navigation bar includes 'tenable', 'Nessus Essentials', 'Scans', and 'Settings'. On the right, there are icons for help, notifications, and a user profile. The left sidebar contains 'FOLDERS' (My Scans, vaishnavi2001@dec..., All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Terrascan). The main content area is titled 'vulnerability_scanning' and includes a '< Back to All Scans' link. Below this are tabs for 'Hosts' (1), 'Vulnerabilities' (23), and 'History' (1). A search bar labeled 'Search History' shows '1 History'. A table lists scan history with columns for checkboxes, Start Time, Last Scanned, and Status. One entry is shown: 'Current' (checkbox), 'Today at 1:49 PM' (Start Time), 'Today at 1:58 PM' (Last Scanned), and 'Completed' (Status). To the right of the table is a 'Scan Details' section with fields for Policy (Basic Network Scan), Status (Completed), Severity Base (CVSS v3.0), Scanner (Local Scanner), Start (Today at 1:49 PM), End (Today at 1:58 PM), and Elapsed (8 minutes). Below this is a 'Vulnerabilities' section with a donut chart and a legend for Critical, High, Medium, Low, and Info. The donut chart is mostly blue, indicating 'Info' level vulnerabilities. At the bottom left, there is a 'Tenable News' section with a link to 'Defusing Cloud Misconfiguration Risk: Finding and ...'.

tenable Nessus Essentials Scans Settings

vulnerability_scanning
< Back to All Scans

Configure Audit Trail Launch Report Export

FOLDERS

- My Scans
- vaishnavi2001@dec...
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Search History 1 History

<input type="checkbox"/>	Start Time	Last Scanned	Status
<input type="checkbox"/>	Current	Today at 1:49 PM	Today at 1:58 PM
<input type="checkbox"/>			Completed

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 1:49 PM
End: Today at 1:58 PM
Elapsed: 8 minutes

Vulnerabilities

Donut chart showing vulnerability distribution: Critical, High, Medium, Low, Info.

Tenable News

Defusing Cloud Misconfiguration Risk: Finding and ...
[Read More](#)

Outcome:

Through this task, I gained hands- on experience in running a vulnerability scan, analysing the results, and identifying potential risk on my PC. i also learned how to document findings and propose mitigation for issues like SMB signing misconfiguration, SSL weaknesses, and unnecessary service exposure.