

# PROJECT REPORT TASK 3

## PERFORM A BASIC VULNERABILITY SCAN ON YOUR PC

### Objective:

To identify potential vulnerabilities on a personal computer using a free vulnerability scanning tool, analyze the scan results, and document the most critical security issues along with appropriate mitigation strategies to enhance overall system security.

### Step 1: Install Nessus Essentials

1. Go to <https://www.tenable.com/products/nessus/nessus-essentials>
2. Click “**Get Started**” and register with your email.
3. You’ll receive an **activation code** via email.
4. Download the correct installer for your OS (Windows/Linux/macOS).
5. Run the installer and complete the installation process.

### Step 2: Launch Nessus & Set It Up

1. Open a browser and go to <https://localhost:8834>.
2. Choose “**Nessus Essentials**”.
3. Enter the **activation code** received in email.
4. Create a **user account (username & password)** for Nessus.
5. Let it **download and install plugins** (can take 15–30 mins).

### Step 3: Set Up a Scan for Your PC

1. Log in to the Nessus web interface.
2. Click “**New Scan**” → choose “**Advanced Scan**”.
3. Enter a **name** for the scan (e.g., *Local Vulnerability Scan*).
4. In **Target**, enter 123.123.123.123 (sample IP address) or your **local IP address** (e.g., 192.168.56.1).
  - To find your local IP on Windows, use ipconfig in CMD.

### Step 4: Launch the Scan

1. Click “**Save**”, then open your scan from the list.
2. Click “**Launch**”.
3. The scan may take **30–60 minutes** depending on system size.

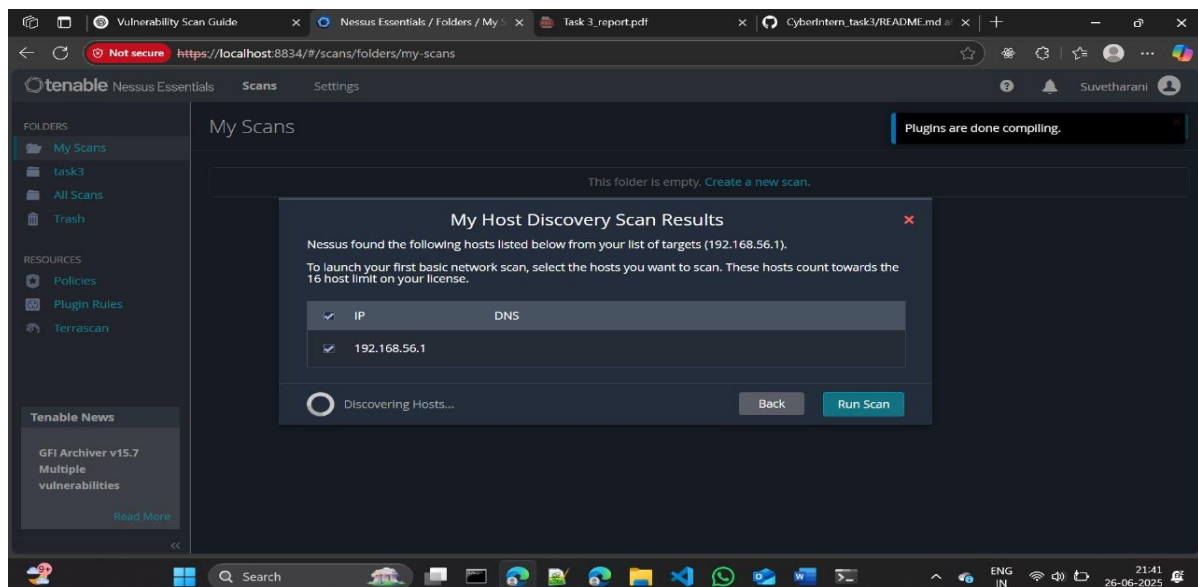
## Step 5: Review the Scan Report

1. After the scan completes, click on the scan name.
2. Review results sorted by **Critical, High, Medium, Low** vulnerabilities.
3. Click each vulnerability for:
  - **Description**
  - **Affected software**
  - **Solution or mitigation suggestions**

## Step 6: Document Key Findings

1. Note **Critical or High vulnerabilities** with:
  - Vulnerability Name
  - Severity
  - CVE Number (if present)
  - Recommended fix
2. Optionally search CVE on <https://cve.mitre.org> for more info.

## Screenshots



tenable Nessus Essentials Scans Settings

My Basic Network Scan  
[Back to My Scans](#) [Configure](#)

Hosts 1 Vulnerabilities 21 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities	%
192.168.56.1	2	68 99%

**Scan Details**

Policy: Basic Network Scan  
 Status: Running  
 Severity Base: CVSS v3.0  
 Scanner: Local Scanner  
 Start: Today at 9:41 PM

**Vulnerabilities**

Critical  
High  
Medium  
Low  
Info

Tenable News  
 How Exposure Management Helps Communicate Cyber Ri...  
[Read More](#)

21:53 26-06-2025

tenable Nessus Essentials Scans Settings

My Basic Network Scan  
[Back to My Scans](#) [Configure](#)

Hosts 1 Vulnerabilities 21 History 1

Filter Search Vulnerabilities 21 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SM...	Misc.	1
MIXED	...	...	...	S...	General	4
INFO	...	...	...	HTTP (Multiple Issues)	DWS	6
INFO	...	...	...	H...	Web Servers	4
INFO	...	...	...	M...	Windows	2
INFO	...	...	...	T...	Service detection	2
INFO	...	...	...	Net...	Port scanners	27
INFO	...	...	...	DCE...	Windows	8

**Scan Details**

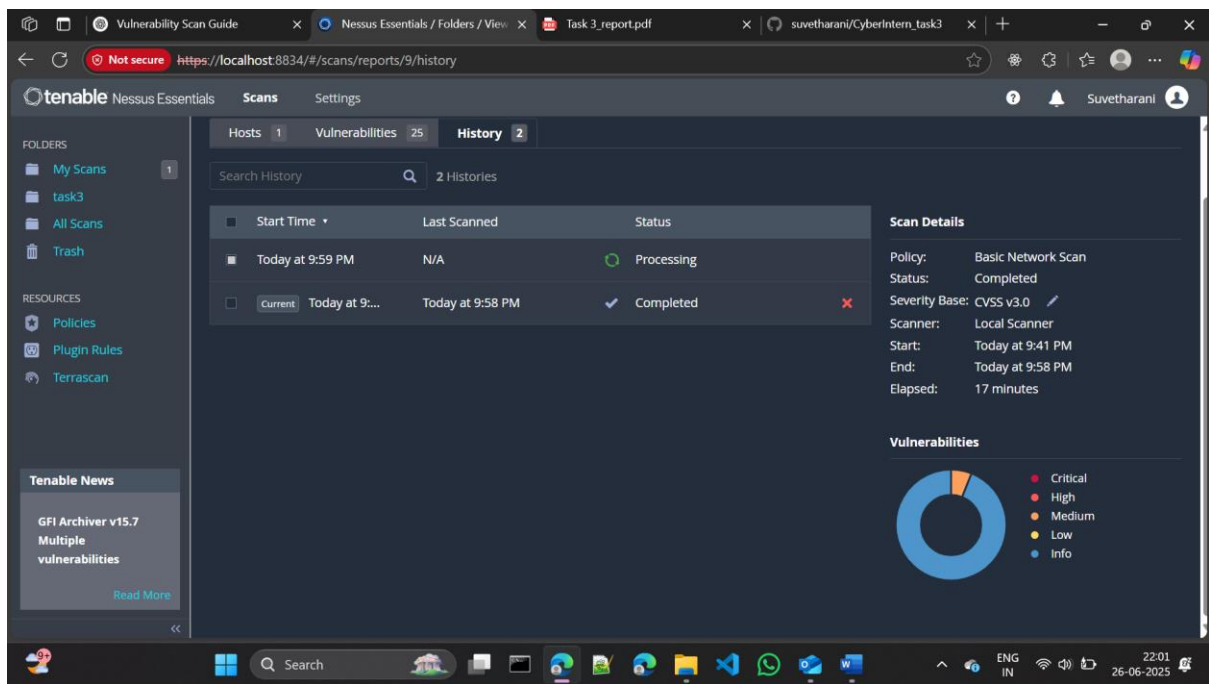
Policy: Basic Network Scan  
 Status: Running  
 Severity Base: CVSS v3.0  
 Scanner: Local Scanner  
 Start: Today at 9:41 PM

**Vulnerabilities**

Critical  
High  
Medium  
Low  
Info

Tenable News  
 The Toxic Cloud Trilogy: Why Your Workloads Are a ...  
[Read More](#)

21:46 26-06-2025



AutoSave: Off | My Basic Network Scan\_ap6... | Saved to this PC | Search

File Home Insert Draw Page Layout Formulas Data Review View Help

Paste | Clipboard | Font | Alignment | Number | Conditional Formatting | Styles | Cell Styles | Insert | Delete | Format | Cells | Editing | Add-ins

POSSIBLE DATA LOSS: Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format. Don't show again | Save As...

Plugin ID	CVE	CVSS v2.0 Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output
10107		None	192.168.5.1tcp		8080	HTTP Serv A web ser	This	n/a			The
10107		None	192.168.5.1tcp		8834	HTTP Serv A web ser	This	n/a			The
10147		None	192.168.5.1tcp		8834	Nessus Se A Nessus	(A Nessus Ensure thi	https://w			
10150		None	192.168.5.1tcp		445	Windows	It was pos	The	n/a		The
10302		None	192.168.5.1tcp		8080	Web Servi	The remot	The	Review	http://ww	Contents
10736		None	192.168.5.1tcp		135	DCE Serv	A DCE/RP	By	n/a		
10736		None	192.168.5.1tcp		445	DCE Serv	A DCE/RP	By	n/a		
10736		None	192.168.5.1tcp		49664	DCE Serv	A DCE/RP	By	n/a		
10736		None	192.168.5.1tcp		49665	DCE Serv	A DCE/RP	By	n/a		
10736		None	192.168.5.1tcp		49668	DCE Serv	A DCE/RP	By	n/a		
10736		None	192.168.5.1tcp		49669	DCE Serv	A DCE/RP	By	n/a		
10736		None	192.168.5.1tcp		49672	DCE Serv	A DCE/RP	By	n/a		
10736		None	192.168.5.1tcp		49676	DCE Serv	A DCE/RP	By	n/a		
10785		None	192.168.5.1tcp		445	Microsoft	It was	Nessus	n/a		Nessus
10863		None	192.168.5.1tcp		8834	SSL Certifi	This plugi	This	n/a		Subject
11011		None	192.168.5.1tcp		139	Microsoft	A file / pri	The	n/a		
11011		None	192.168.5.1tcp		445	Microsoft	A file / pri	The	n/a		

My Basic Network Scan\_ap6cm3

Ready | Accessibility: Unavailable | Search | ENG IN | 22:02 26-06-2025

## Conclusion:

The vulnerability scan successfully identified several potential security issues on my computer. To gain a deeper understanding of these vulnerabilities, I also tested a different target host. The findings revealed how such issues could be exploited by attackers to gain unauthorized access or cause harm to the system. This exercise highlighted the importance of performing regular vulnerability scans and keeping software up to date to maintain a secure computing environment.