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.

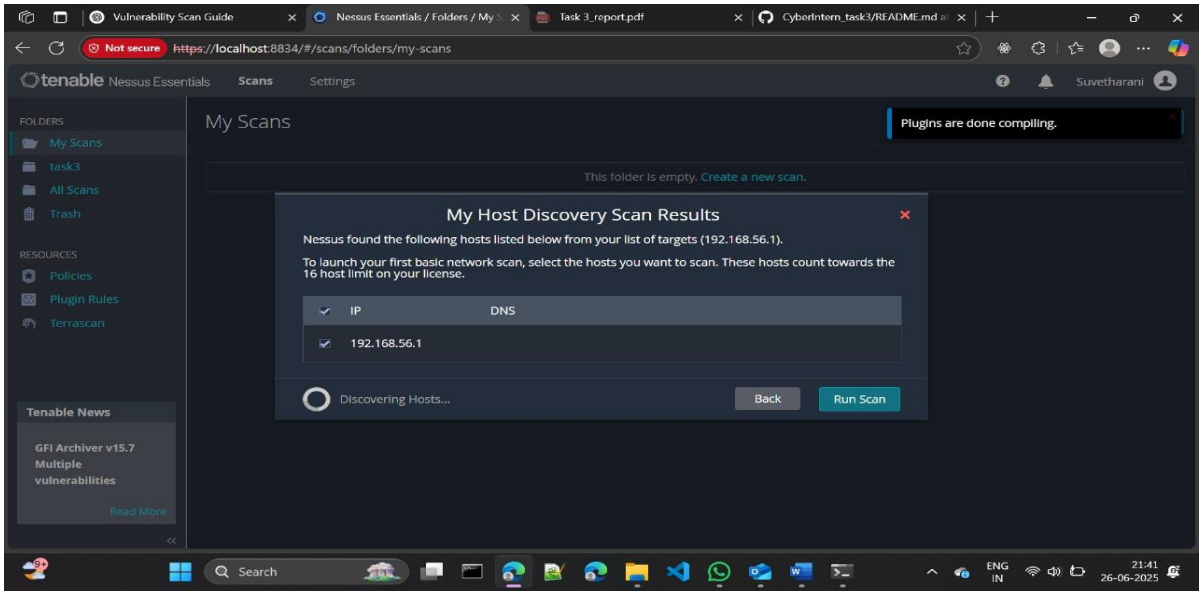
Step 5: Review the Scan Report

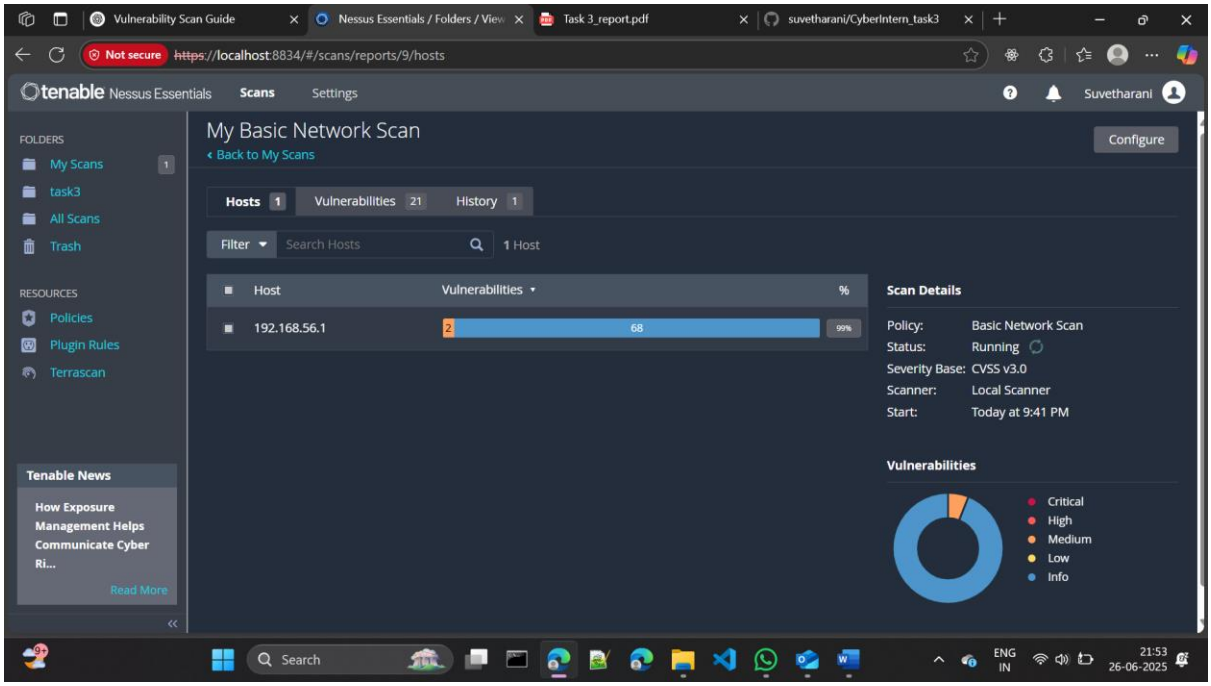
1. After the scan completes, click on the scan name.
2. Review results sorted by **Critical**, **High**, **Medium**, **Low** vulnerabilities.
3. Click each vulnerability for:
    - **Description**
    - **Affected software**
    - **Solution or mitigation suggestions**

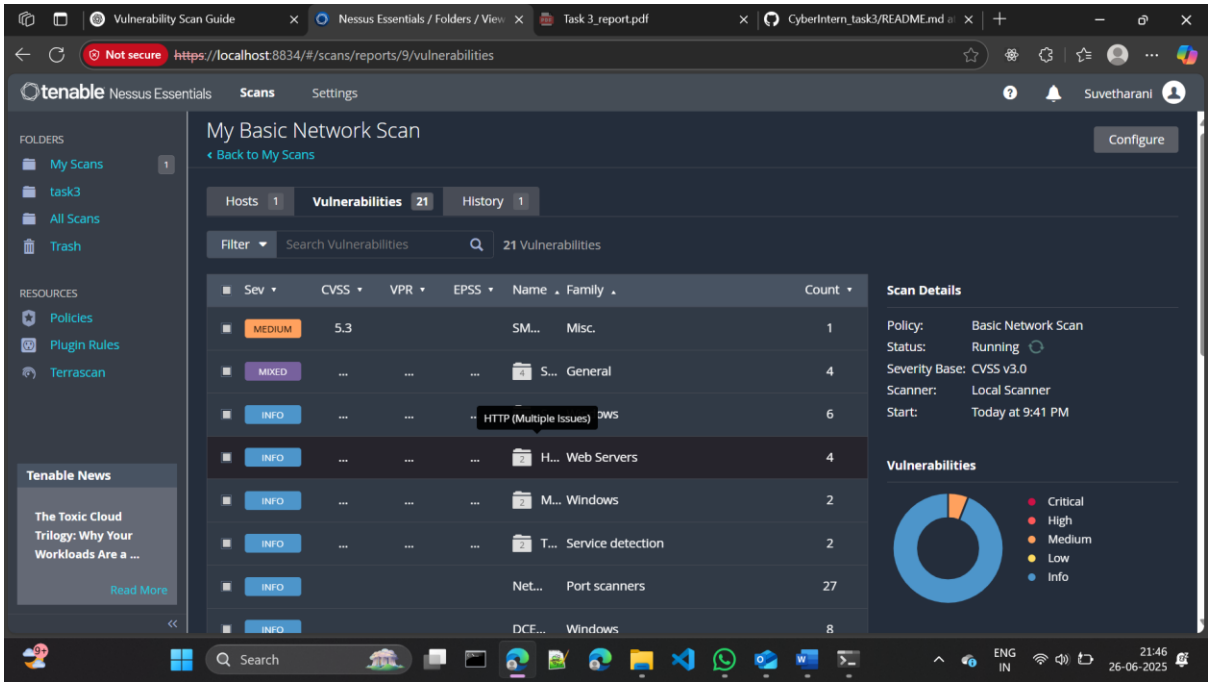
Step 6: Document Key Findings

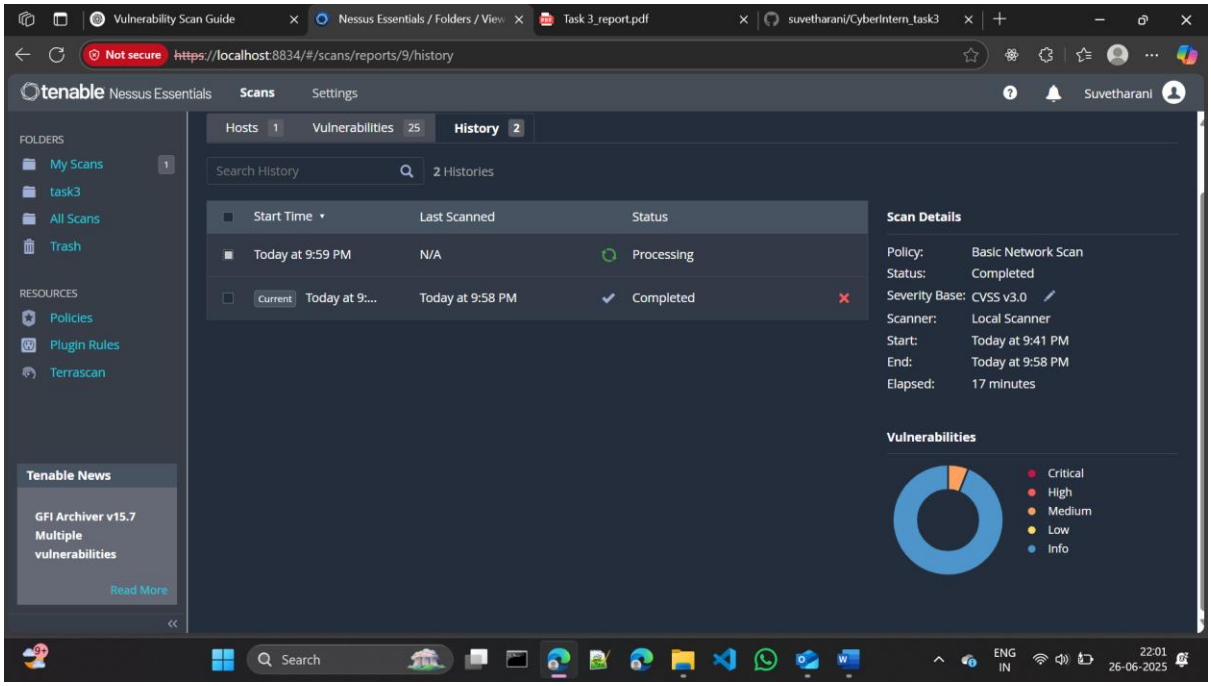
1. Note **Critical or High vulnerabilities** with:
    - Vulnerability Name
    - Severity
    - CVE Number (if present)
    - Recommended fix
2. Optionally search CVE on https://cve.mitre.org for more info.

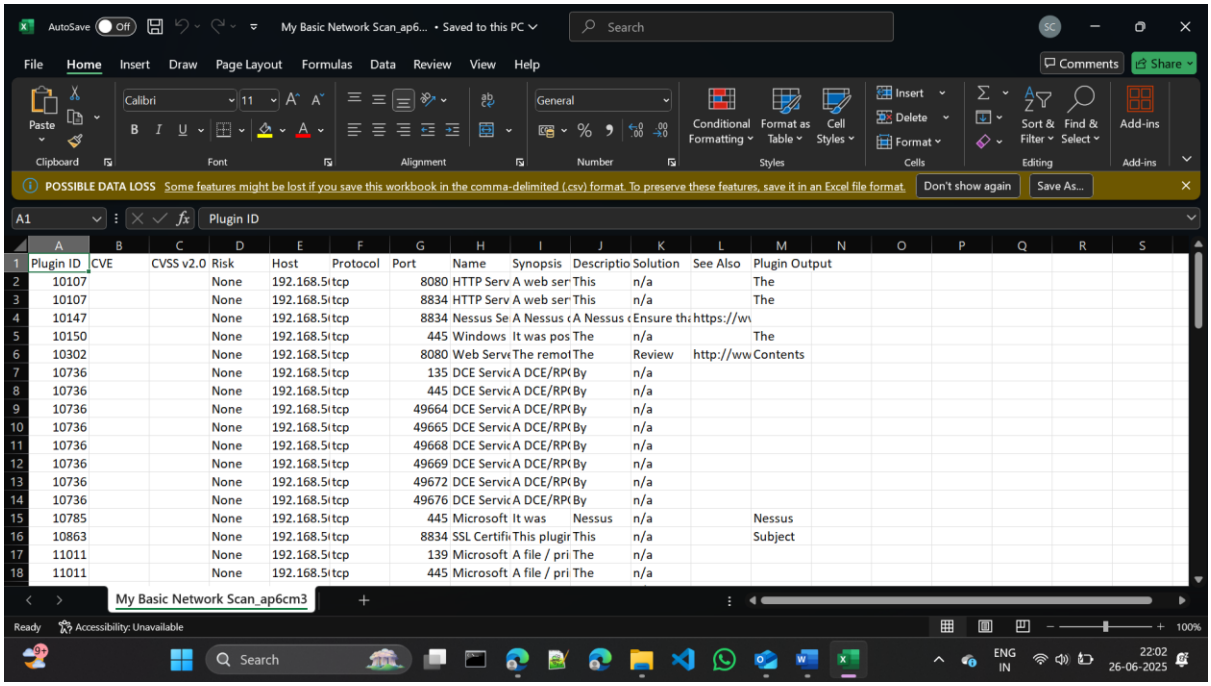
Screenshots




Vulnerability Scan Guide
Nessus Essentials / Folders / View
Task 3_report.pdf
suvetharani/CyberIntern_task3
Not secure
https://localhost:8834/#/scans/reports/9/hosts
tenable Nessus Essentials
Scans
Settings
Suvetharani
FOLDERS
My Scans
task3
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
How Exposure Management Helps Communicate Cyber Ri...
Read More
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
Search
ENG
IN
21:53
26-06-2025


Vulnerability Scan Guide
Nessus Essentials / Folders / View
Task 3_report.pdf
CyberIntern_task3/README.md
Not secure
https://localhost:8834/#/scans/reports/9/vulnerabilities
tenable Nessus Essentials
Scans
Settings
Suvetharani
FOLDERS
My Scans
task3
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
The Toxic Cloud Trilogy: Why Your Workloads Are a ...
Read More
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
6
HTTP (Multiple Issues)
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
Search
ENG
IN
21:46
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.