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 or your **local IP address** (e.g., 192.168.1.x).
   - 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.

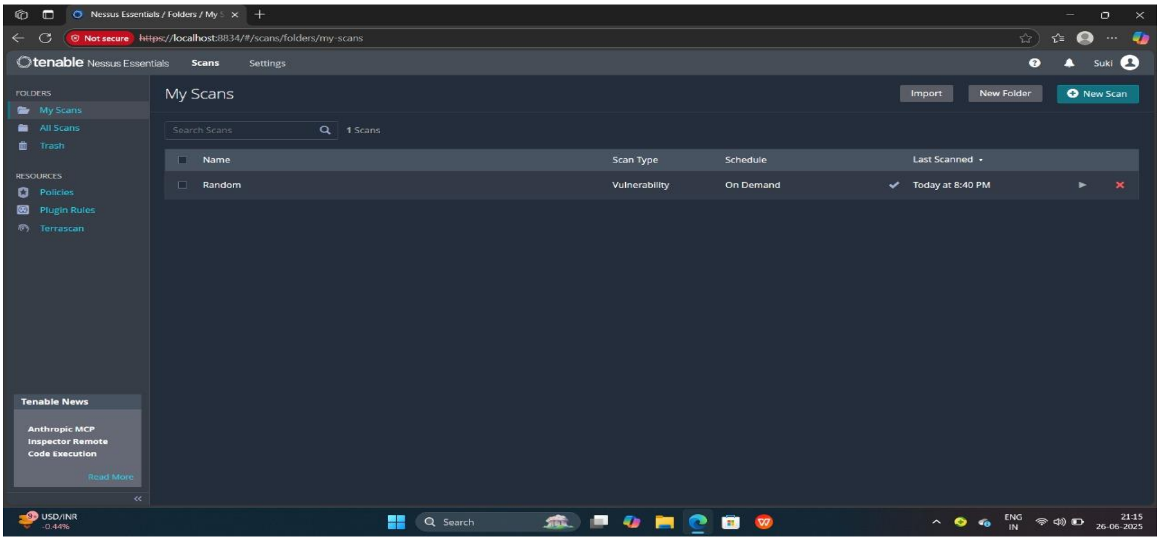
Step 5: Review the Scan Report

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.

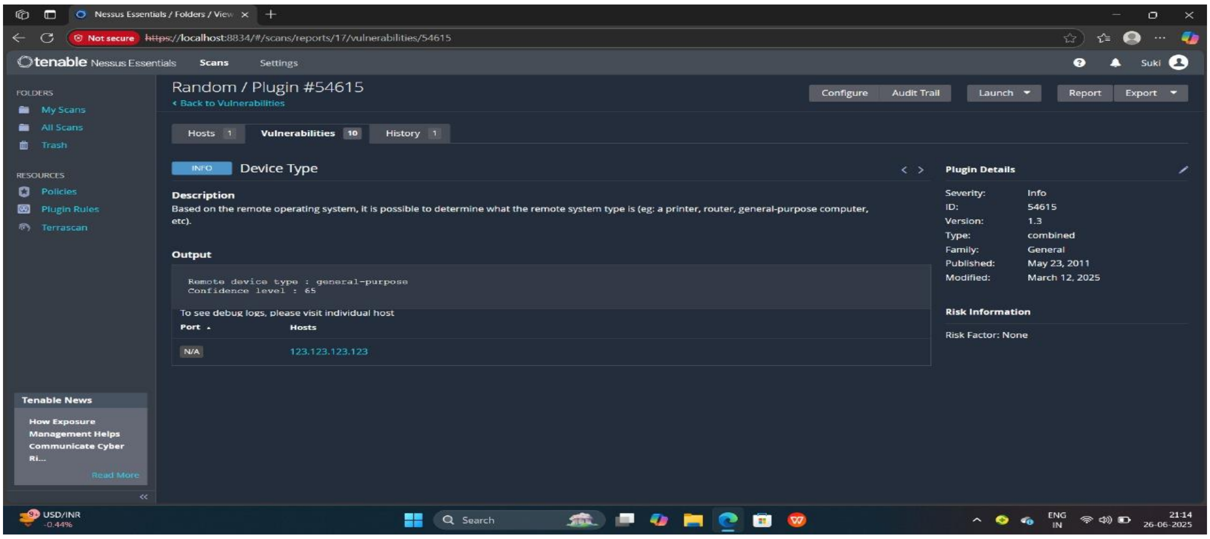
Screenshots



My Scans

1 Scans

Name	Scan Type	Schedule	Last Scanned
Random	Vulnerability	On Demand	✓ Today at 8:40 PM



Random / Plugin #54615

‹ Back to Vulnerabilities

INFO Device Type

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Output

```
Remote device type : general-purpose
Confidence level : 65
```

To see debug logs, please visit individual host

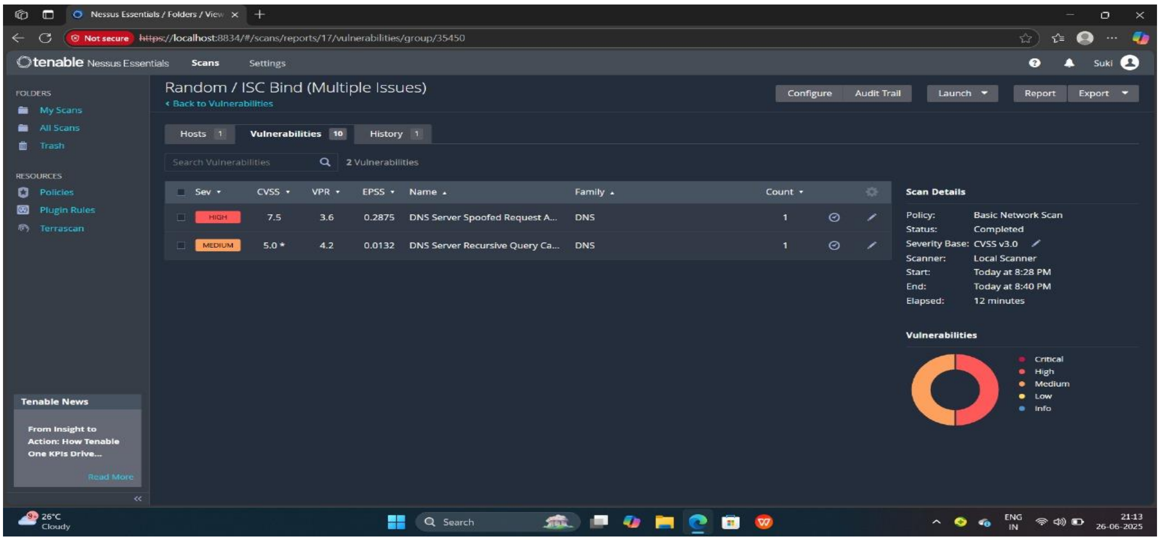
Port ▴	Hosts
N/A	123.123.123.123

Plugin Details

Severity:	Info
ID:	54615
Version:	1.3
Type:	combined
Family:	General
Published:	May 23, 2011
Modified:	March 12, 2025

Risk Information

Risk Factor: None



Random / ISC Bind (Multiple Issues)

‹ Back to Vulnerabilities

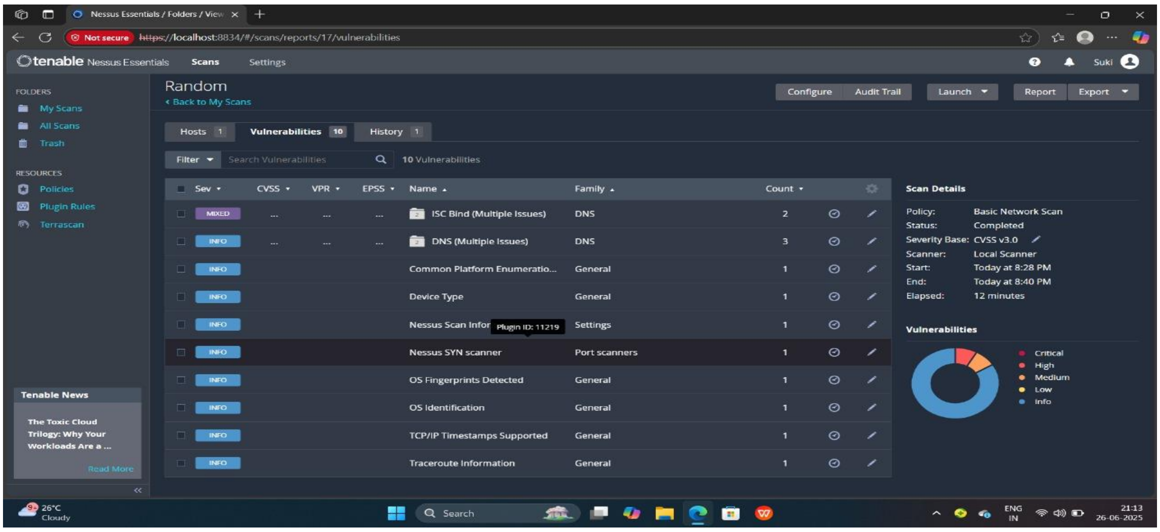
2 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
HIGH	7.5	3.6	0.2875	DNS Server Spoofed Request A...	DNS	1
MEDIUM	5.0 *	4.2	0.0132	DNS Server Recursive Query Ca...	DNS	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:28 PM
End:	Today at 8:40 PM
Elapsed:	12 minutes

Vulnerabilities



Random

‹ Back to My Scans

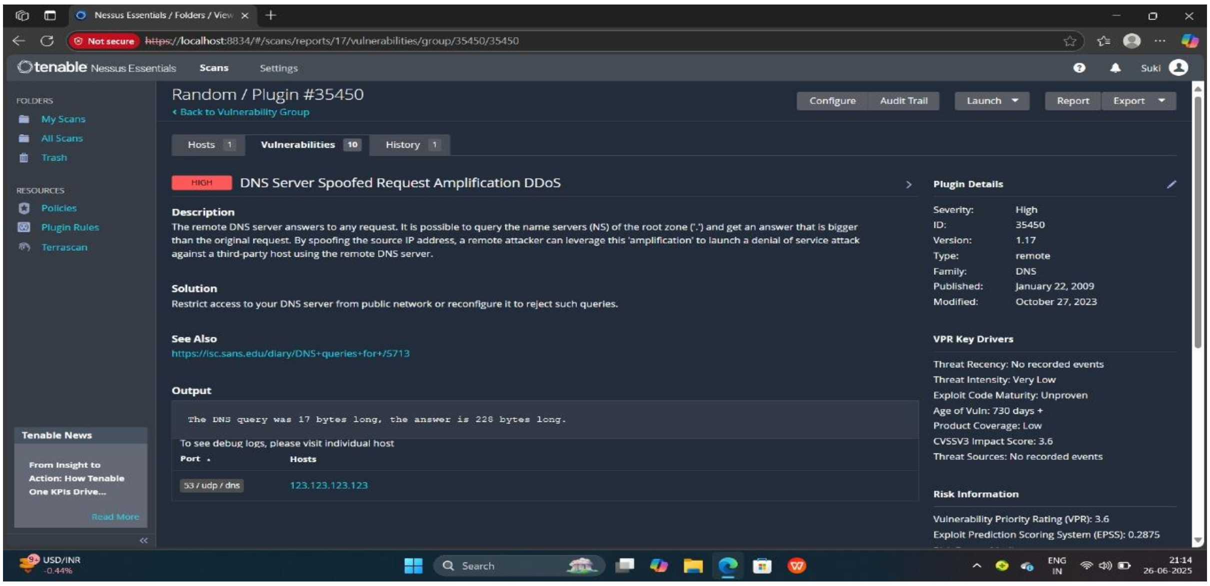
10 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
MIXED	...	...	...	2 ISC Bind (Multiple Issues)	DNS	2
INFO	...	...	...	2 DNS (Multiple Issues)	DNS	3
INFO				Common Platform Enumeratio...	General	1
INFO				Device Type	General	1
INFO				Nessus Scan Infor	Settings	1
INFO				Nessus SYN scanner	Port scanners	1
INFO				OS Fingerprints Detected	General	1
INFO				OS Identification	General	1
INFO				TCP/IP Timestamps Supported	General	1
INFO				Traceroute Information	General	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 8:28 PM
End:	Today at 8:40 PM
Elapsed:	12 minutes

Vulnerabilities



Random / Plugin #35450

‹ Back to Vulnerability Group

HIGH DNS Server Spoofed Request Amplification DDoS

Description

The remote DNS server answers to any request. It is possible to query the name servers (NS) of the root zone ('.') and get an answer that is bigger than the original request. By spoofing the source IP address, a remote attacker can leverage this 'amplification' to launch a denial of service attack against a third-party host using the remote DNS server.

Solution

Restrict access to your DNS server from public network or reconfigure it to reject such queries.

See Also

https://isc.sans.edu/diary/DNS+queries+for+/5713

Output

```
The DNS query was 17 bytes long, the answer is 228 bytes long.
```

To see debug logs, please visit individual host

Port ▴	Hosts
53 / udp / dns	123.123.123.123

Plugin Details

Severity:	High
ID:	35450
Version:	1.17
Type:	remote
Family:	DNS
Published:	January 22, 2009
Modified:	October 27, 2023

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 3.6
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 3.6
Exploit Prediction Scoring System (EPSS): 0.2875

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.