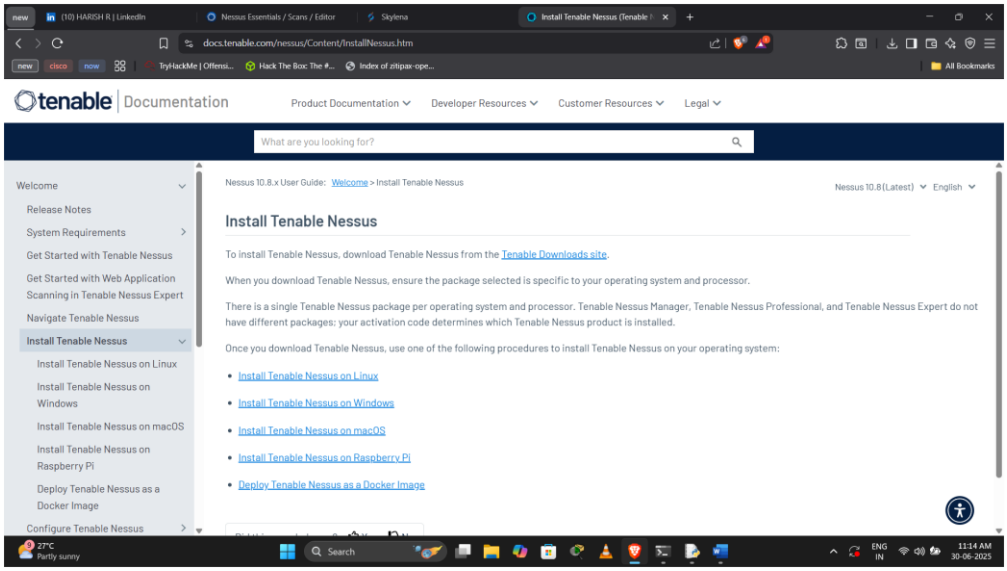
NESSUS

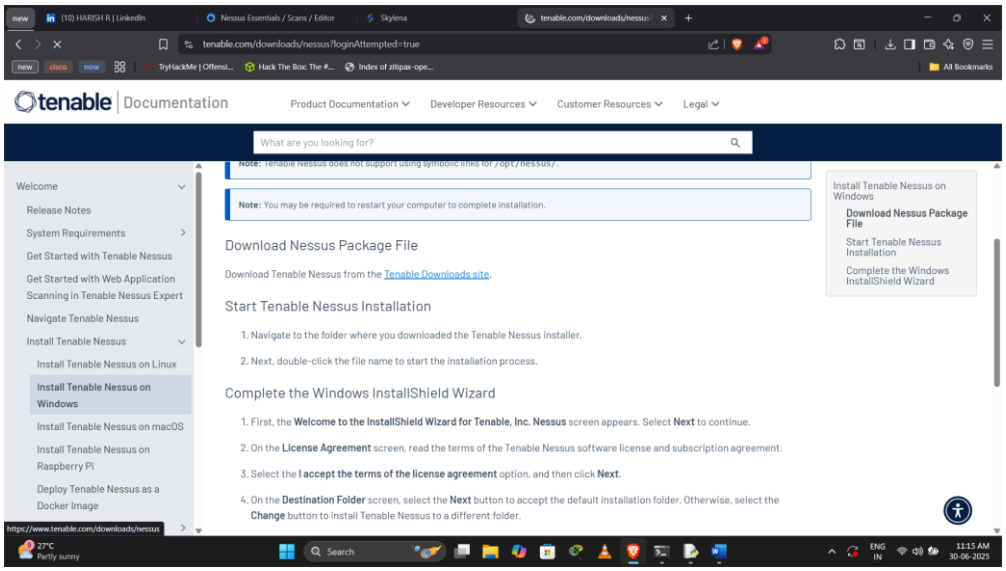
A VULNERABILITY SCANNER

Installation :

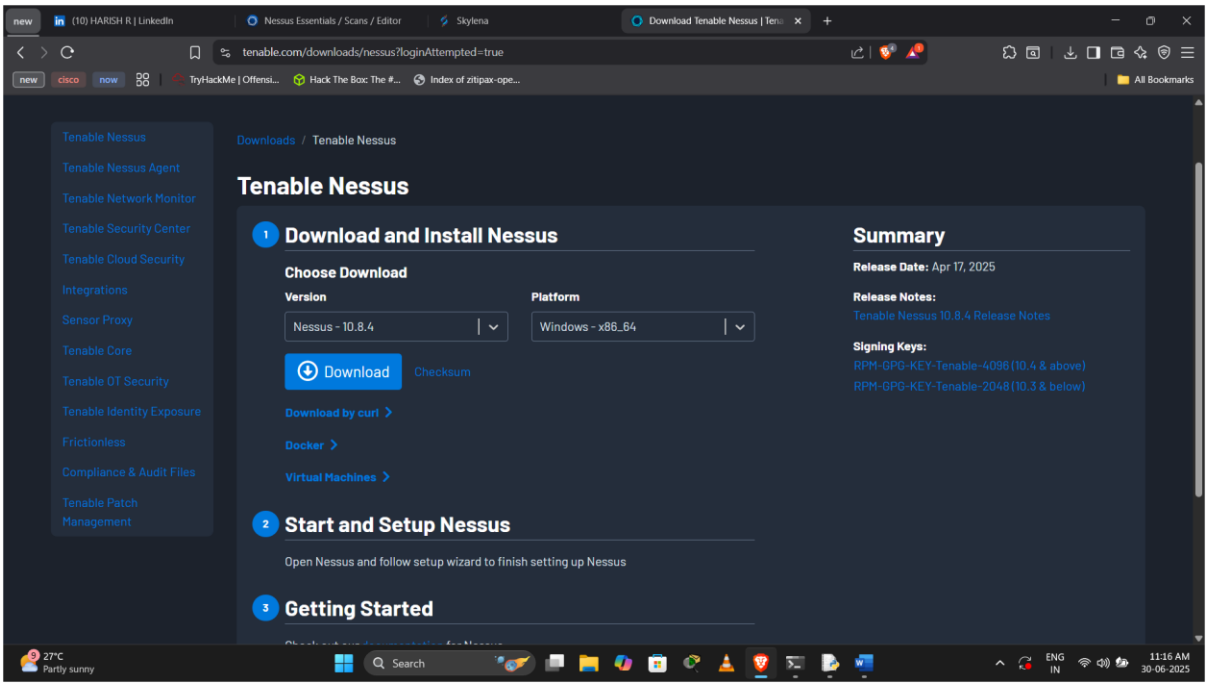
Download Nessus :

- ❖ Go to https://www.tenable.com/products/nessus.
- ❖ Click on “Download” and choose:
  - Nessus Essentials (Free for students/personal use).
  - Select the appropriate OS (e.g., Windows, Linux, macOS).

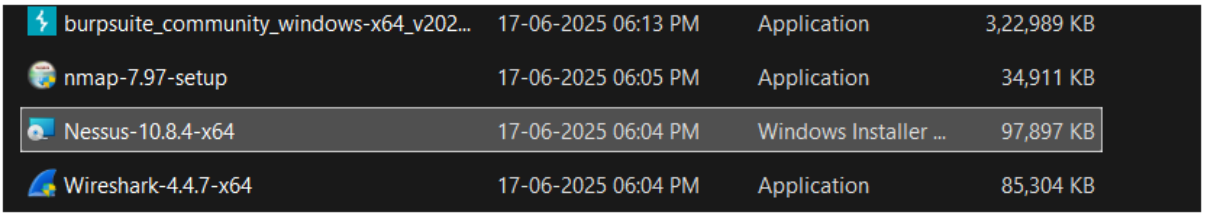




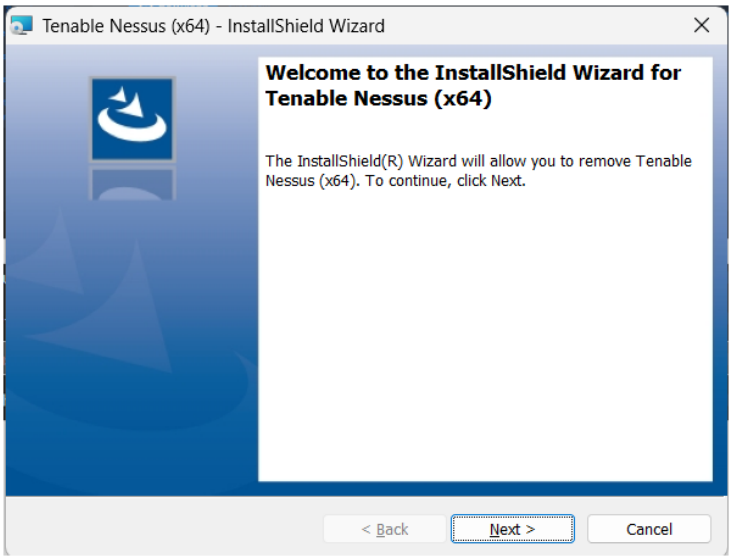
Download the NESSUS based on the version needed :

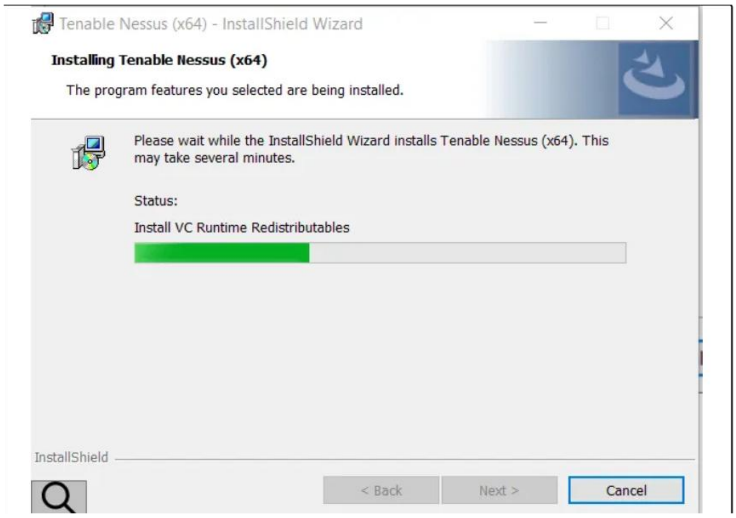


Save the downloaded file and Run the setup file for :

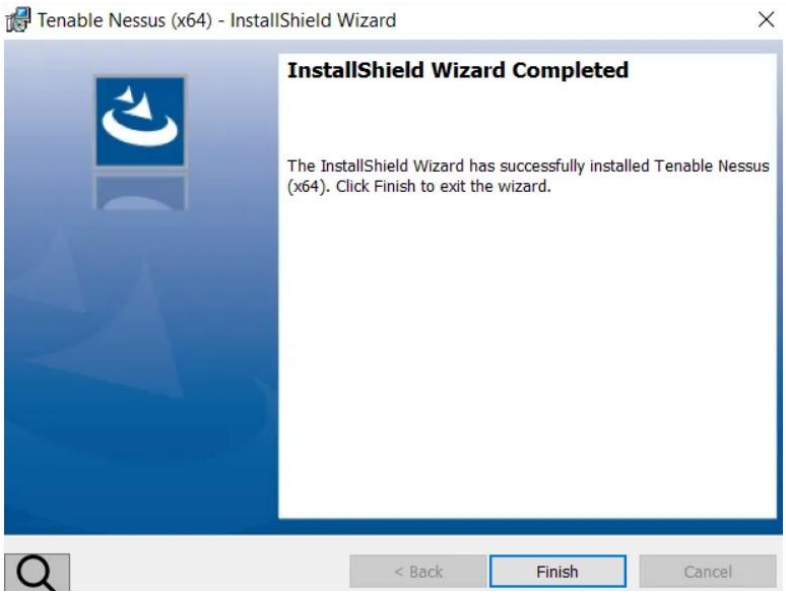


Proceed with **installation process :**





Finish the Setup file installation process :

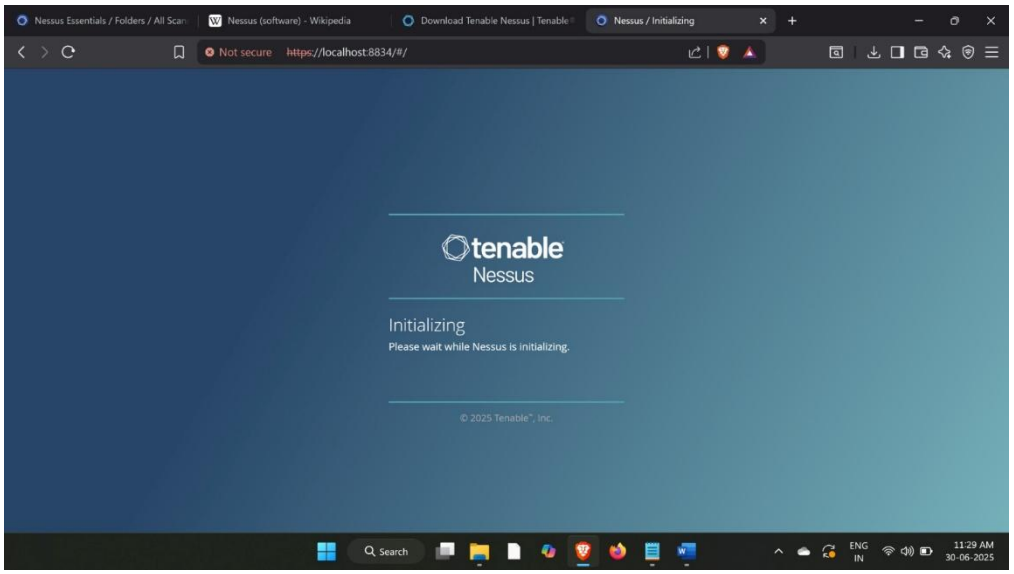


Installation Completed …!

Access the Nessus Web Interface :

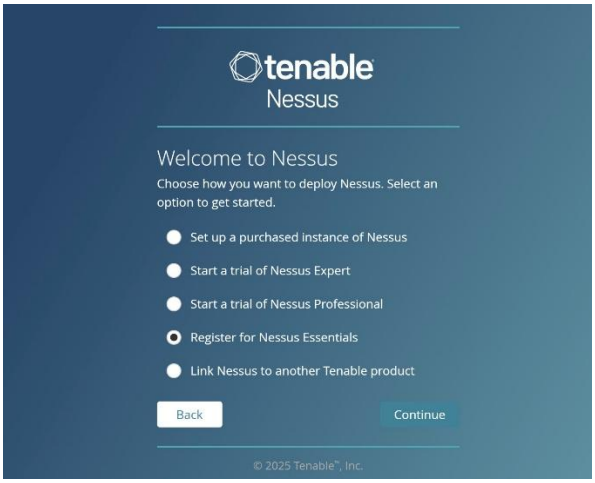
Open the nessus in the Local browser for Configuring the software

Using : https://localhost:8834/

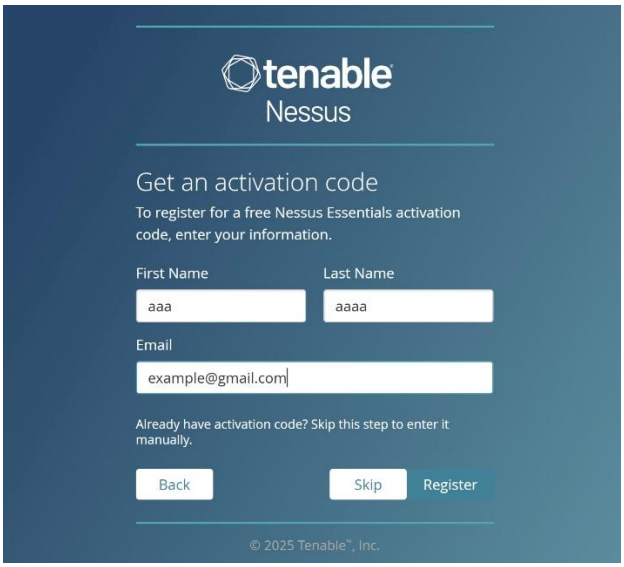


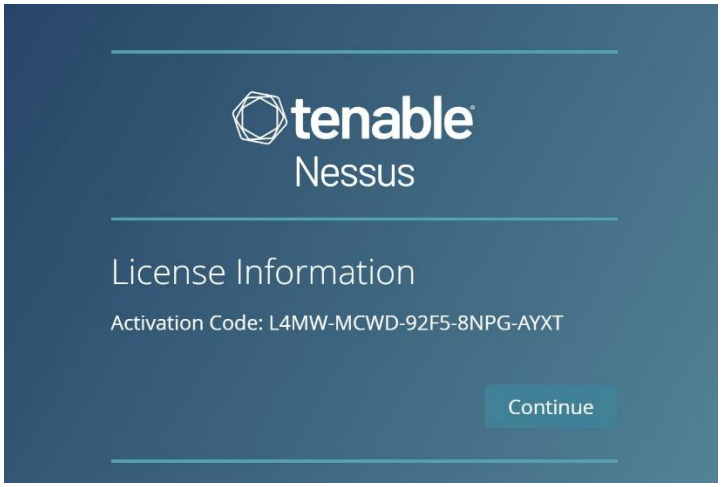
Installs necessary plugins and dependencies needed and loaded to configurations phase :

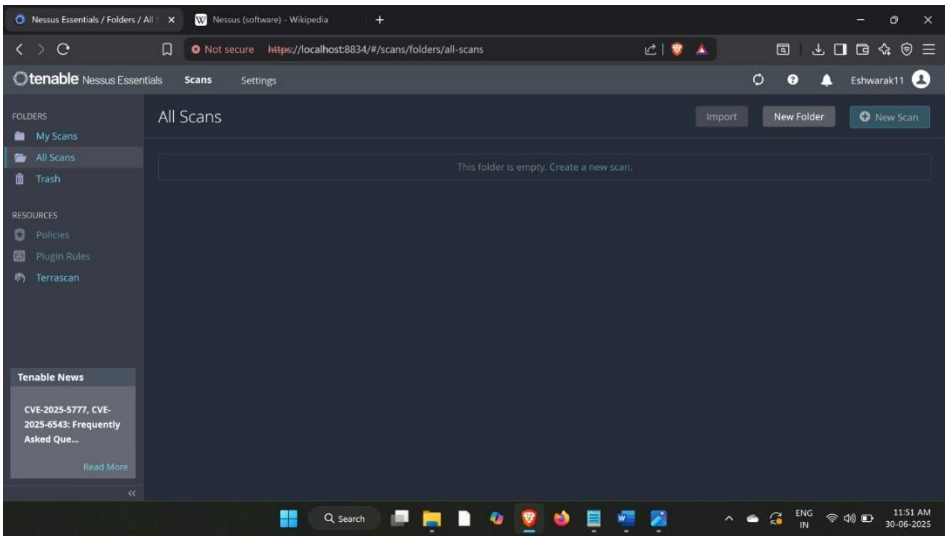
Select and register for Nessus essentials :



Register for activation code and access the interface for scanning :

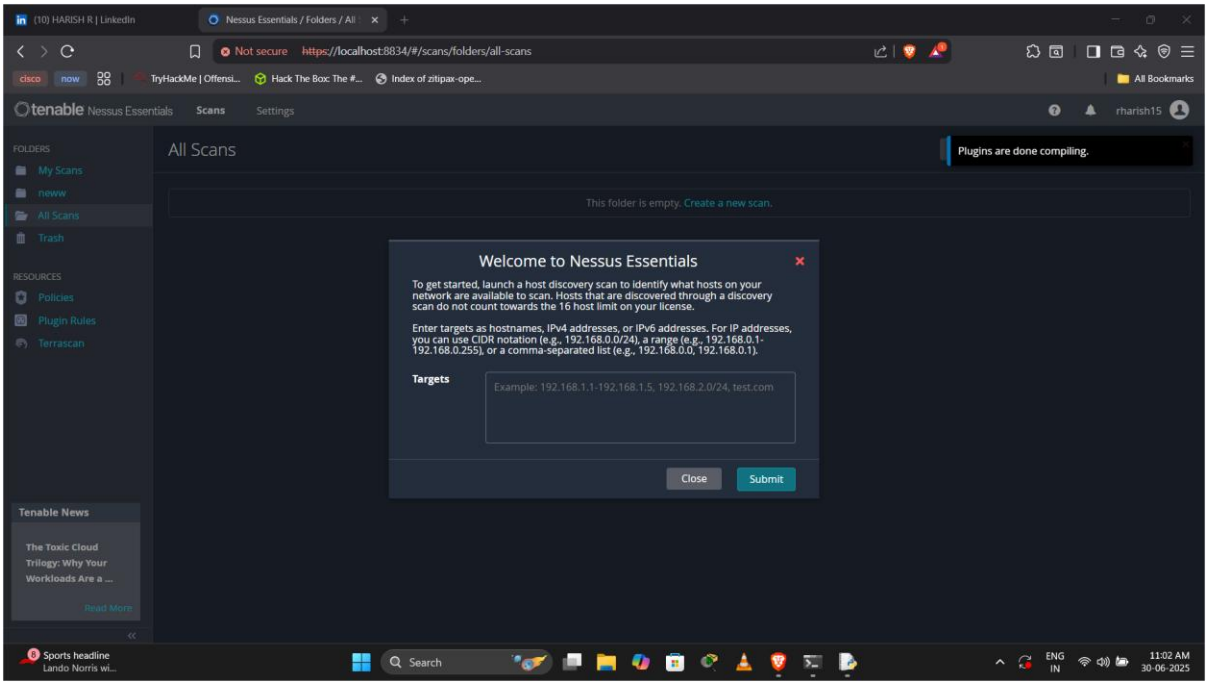






Configurations completed …!

IMPLEMENTATION :



NESSUS SCANNER consists of three Scan templates :

- ❖ Discovery
- ❖ Vulnerabilities
- ❖ Compliance

1. Discovery Scan Template :

Used to **identify active hosts and services** in a target network.

Purpose:

- To **map the network** and find **live systems**.
- Identify **open ports, services, and OS types**.
- Useful for **pre-engagement** or **asset inventory**.

Features:

- Performs **ping sweeps** and **port scanning**.
- Does **not** test for vulnerabilities.
- Can help detect **rogue devices** or unknown systems.

Use Case:

- Before vulnerability scanning.
- For network administrators to **maintain inventory**.
- In early phases of **penetration testing** or **reconnaissance**.

2. Vulnerability Scan Template

Used to **identify known security issues** in systems and applications.

Purpose:

- To **scan for CVEs**, misconfigurations, weak credentials, etc.
- Categorize risks (Critical, High, Medium, Low).
- Helps prioritize **patch management**.

Features:

- Leverages Nessus plugin database (regularly updated).
- Tests against **OWASP Top 10**, **common misconfigurations**, **missing patches**, etc.
- Includes unauthenticated and authenticated scanning.

Use Case:

- Routine **security assessments**.
- For **compliance** (PCI-DSS, ISO) and **risk management**.
- To generate **vulnerability reports** for remediation.

3. Compliance Scan Template

Used to **audit systems against regulatory or internal policies**.

Purpose:

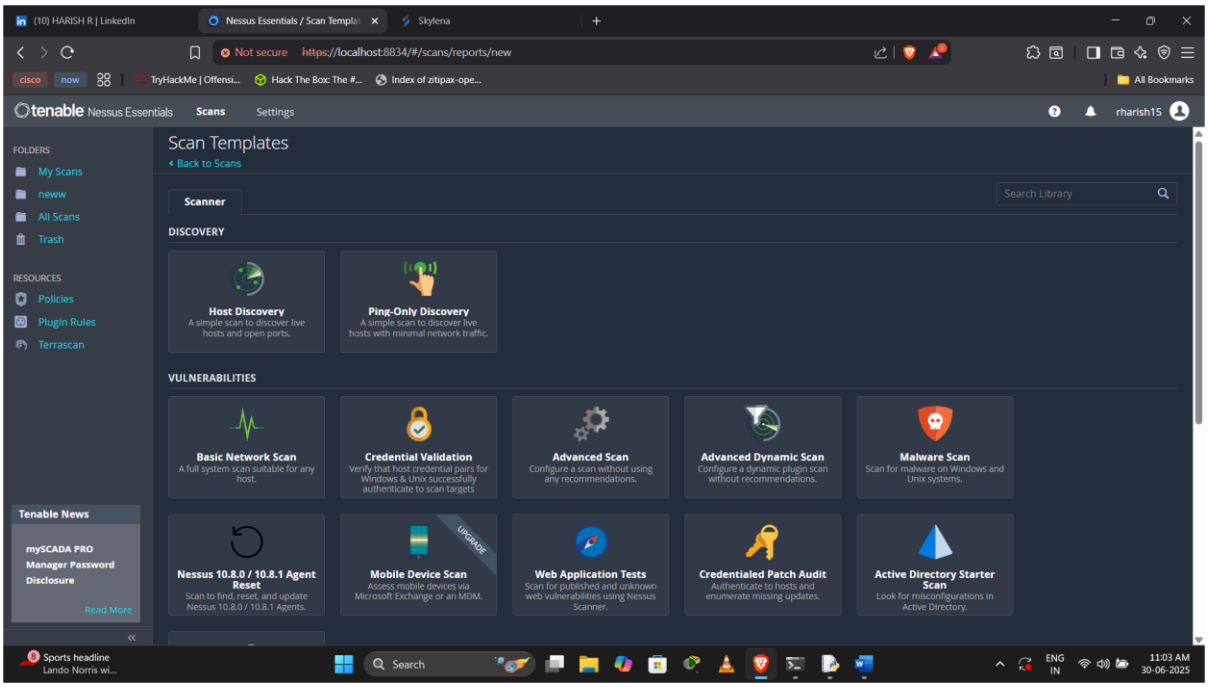
- Verify that systems are configured to **meet specific security standards**.
- Check for compliance with **CIS benchmarks, DISA STIGs, PCI-DSS**, etc.

Features:

- Requires **credentialed access** (username/password or keys).
- Compares system settings (registry, services, configs) to policy.
- Generates **pass/fail compliance reports**.

Use Case:

- For **audits** and regulatory requirements.
- To enforce **corporate security policies**.
- In organizations seeking **certification or audit readiness**.



Prerequisitics :

Find the target IP address to perform scanning :

```
PS C:\Users\rhari> nslookup skylenainfotech.in
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
Name:    skylenainfotech.in
Address:  35.154.70.151

PS C:\Users\rhari>
```

USAGE AND CONTEXT :

DISCOVERY :

- **Host Discovery**
  A simple scan to discover live hosts and open ports.
- **Ping-Only Discovery**
  A simple scan to discover live hosts with minimal network traffic.

VULNERABILITIES :

- **Basic Network Scan**
  A full system scan suitable for any host.
- **Credential Validation**
  Verify that host credential pairs for Windows & Unix successfully authenticate to scan targets.
- **Advanced Scan**
  Configure a scan without using any recommendations.
- **Advanced Dynamic Scan**
  Configure a dynamic plugin scan without recommendations.
- **Malware Scan**
  Scan for malware on Windows and Unix systems.
- **Nessus 10.8.0 / 10.8.1 Agent Reset**
  Scan to find, reset, and update Nessus 10.8.0 / 10.8.1 Agents.
- **Mobile Device Scan** *(UPGRADE)*
  Assess mobile devices via Microsoft Exchange or an MDM.
- **Web Application Tests**
  Scan for published and unknown web vulnerabilities using Nessus Scanner.
- **Credentialed Patch Audit**
  Authenticate to hosts and enumerate missing updates.
- **Active Directory Starter Scan**
  Look for misconfigurations in Active Directory.

COMPLIANCE :

Audit Cloud Infrastructure

Audit the configuration of third-party cloud services.

Internal PCI Network Scan

Perform an internal PCI DSS (11.2.1) vulnerability scan.

MDM Config Audit

Audit the configuration of mobile device managers.

Offline Config Audit

Audit the configuration of network devices.

PCI Quarterly External Scan

Approved for quarterly external scanning as required by PCI.

Policy Compliance Auditing

Audit system configurations against a known baseline.

SCAP and OVAL Auditing

Audit systems using SCAP and OVAL definitions.

Tabular Representation :

Discovery Scans – *Used to find live hosts and open ports*

Scan Template	**Purpose**	**Traffic Level**	**Use Case**
Host Discovery	Scans for live hosts + open ports	Moderate	Initial asset inventory
Ping-Only Discovery	Only checks for host availability via ICMP	Very Low	Minimal scan to check if hosts are alive

Vulnerability Scans – *Check for security issues*

Scan Template	Purpose	Dynamic Plugins	Credentialed?	Use Case
Basic Network Scan	Full system scan, suitable for most environments	No	Optional	General-purpose vulnerability scan
Advanced Scan	Full manual control, no preset recommendations	No	Optional	Custom scan setup, plugin and target control
Advanced Dynamic Scan	Dynamic plugin scan based on live discovery	Yes	Optional	Adaptive scan with conditional logic for plugins
Malware Scan	Malware detection on Windows & Unix systems	Limited to malware checks	Credentialed preferred	Malware-focused scanning only
Web Application Tests	Web vulnerability scan including published and unknown issues	Yes (Web focused)	Not required	Targeted for web applications (XSS, SQLi, etc.)
Credentialed Patch Audit	Authenticated scan for missing OS/software patches	Yes	Required	Used for patch verification using system-level access

Credential & Identity-Related Scans

Scan Template	Purpose	Credential Requirement	Use Case
Credential Validation	Verifies if Windows/Unix credentials work for scan targets	Yes	Check if auth is successful before full scans

Scan Template	Purpose	Credential Requirement	Use Case
Active Directory Starter Scan	Checks AD for misconfigurations	Recommended	Internal AD misconfiguration detection

Specialized Scans

Scan Template	Purpose	Upgrade Needed	Use Case
Mobile Device Scan	Assesses mobile security via Exchange or MDM	Yes	MDM-integrated environments
Nessus Agent Reset (10.8.0/10.8.1)	Resets outdated Nessus agents	No	Fix stale agents for proper functioning

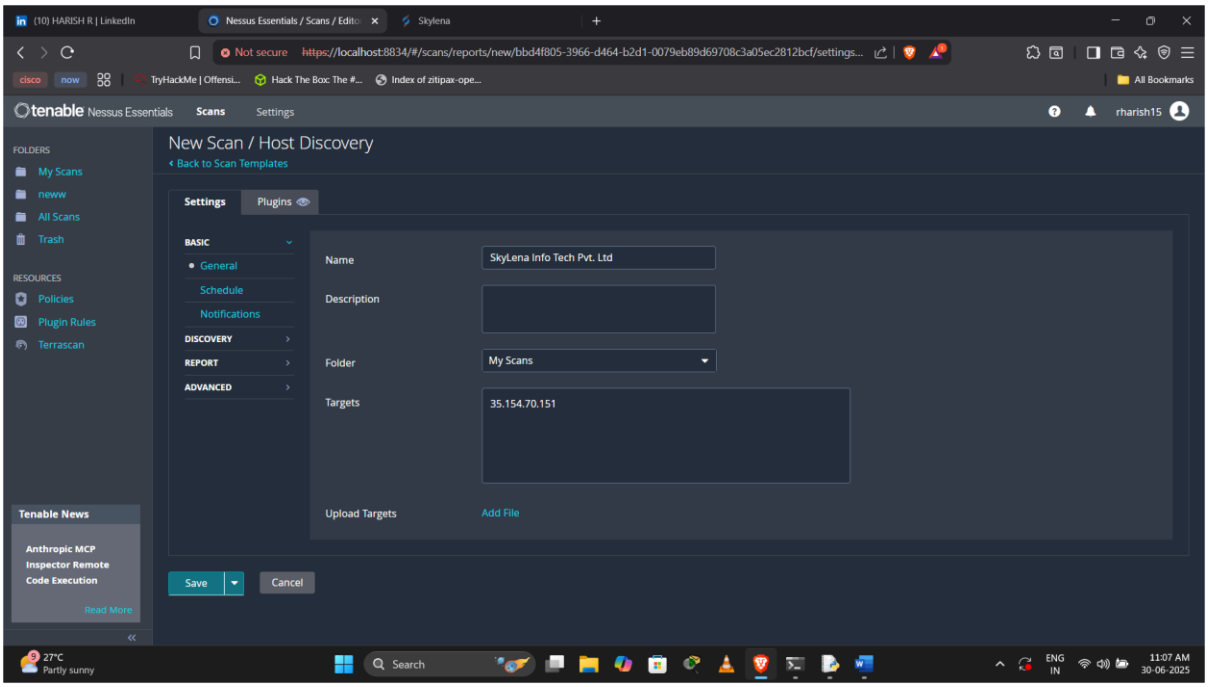
COMPLIANCE Scans

Scan Template	Description
Audit Cloud Infrastructure	Audit the configuration of third-party cloud services.
Internal PCI Network Scan	Perform an internal PCI DSS (11.2.1) vulnerability scan.
MDM Config Audit	Audit the configuration of mobile device managers.
Offline Config Audit	Audit the configuration of network devices.
PCI Quarterly External Scan	Approved for quarterly external scanning as required by PCI.
Policy Compliance Auditing	Audit system configurations against a known baseline.
SCAP and OVAL Auditing	Audit systems using SCAP and OVAL definitions.

Host Discovery :

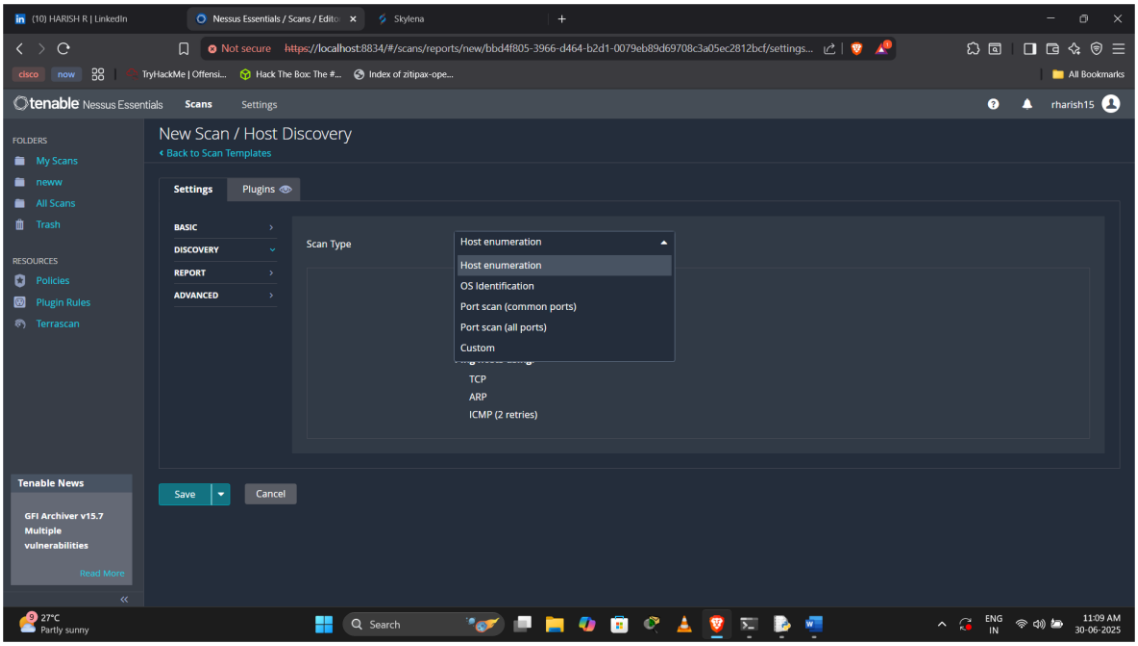
Configure the Scan

- ❖ Set:
  - **Name** of the scan.
  - **Targets** (IP address or domain).
  - **Schedule** (optional).



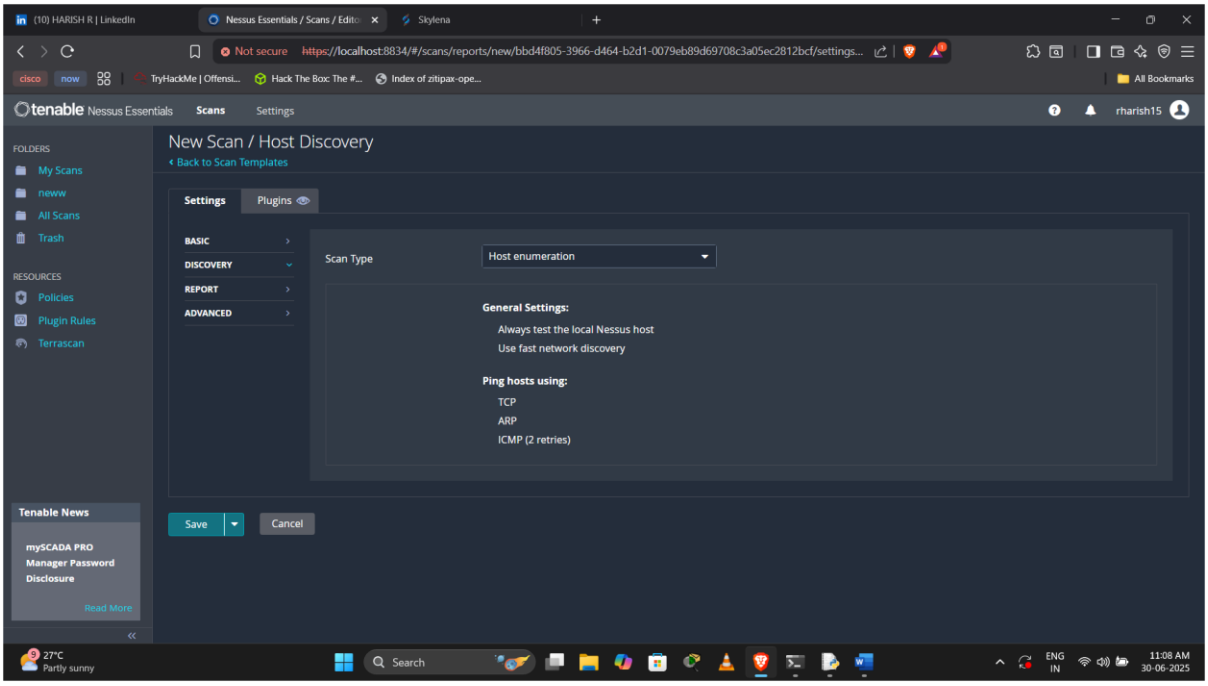
Provide the scan type :

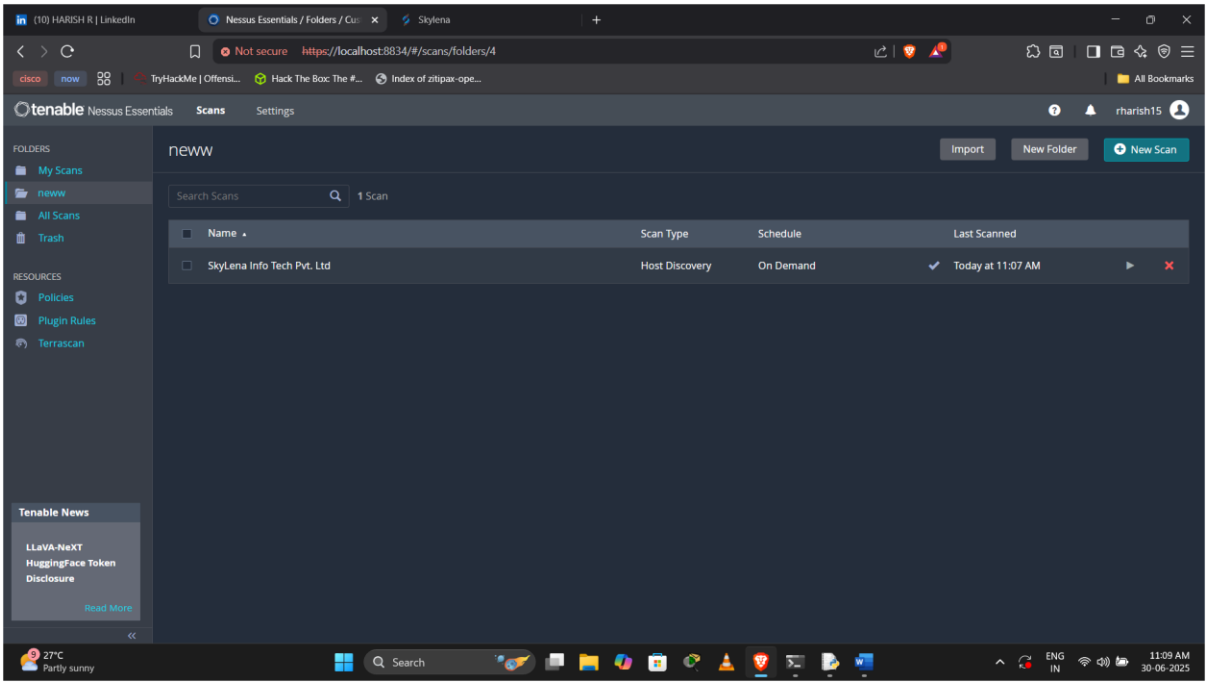
- Host Enumeration
- OS enumeration



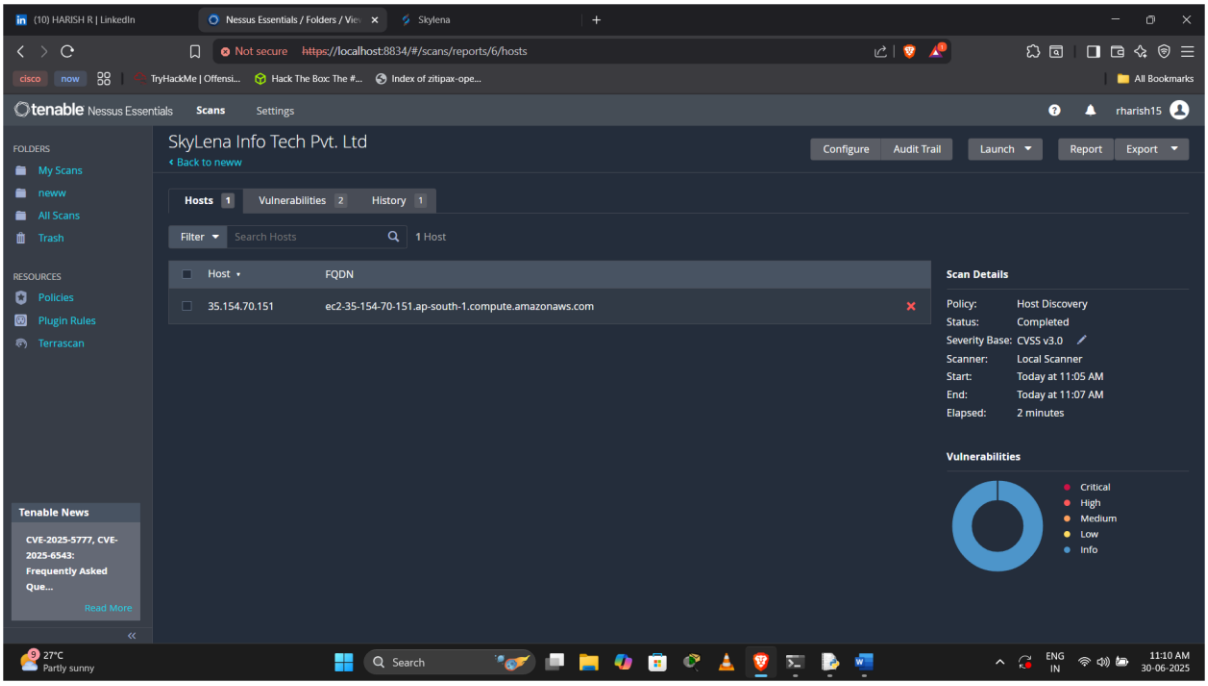
❖ Launch the Scan

- Click **“Save”** and then **“Launch”**.





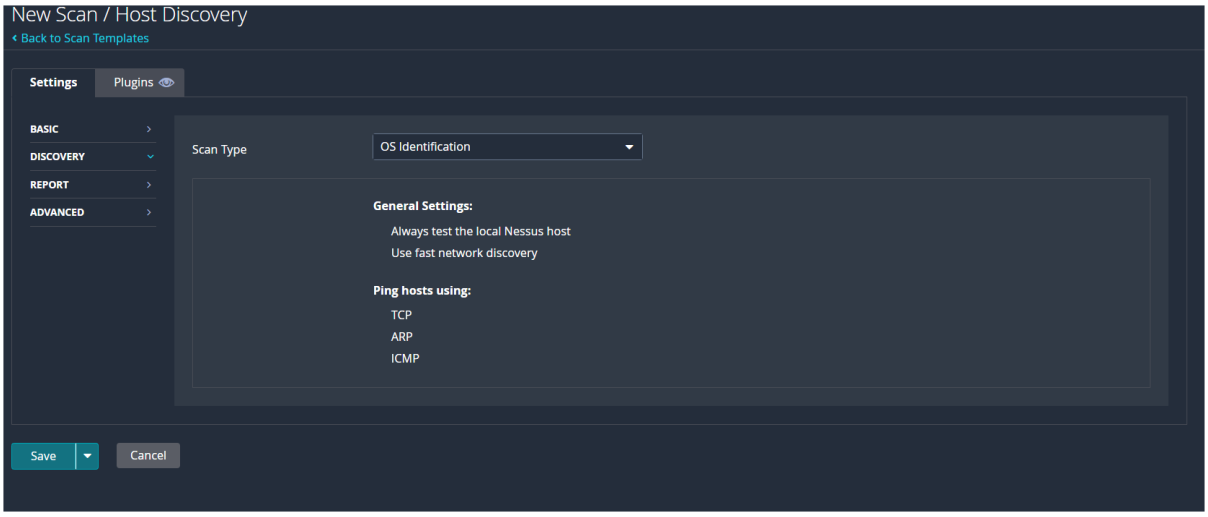
After completion of the scan the results can be seen and exported as various file formats :



OS identification :

Configure the Scan

- Set:
  - **Name** of the scan.
  - **Targets** (IP address or domain).
  - **Schedule** (optional).
- Provide the scan type :

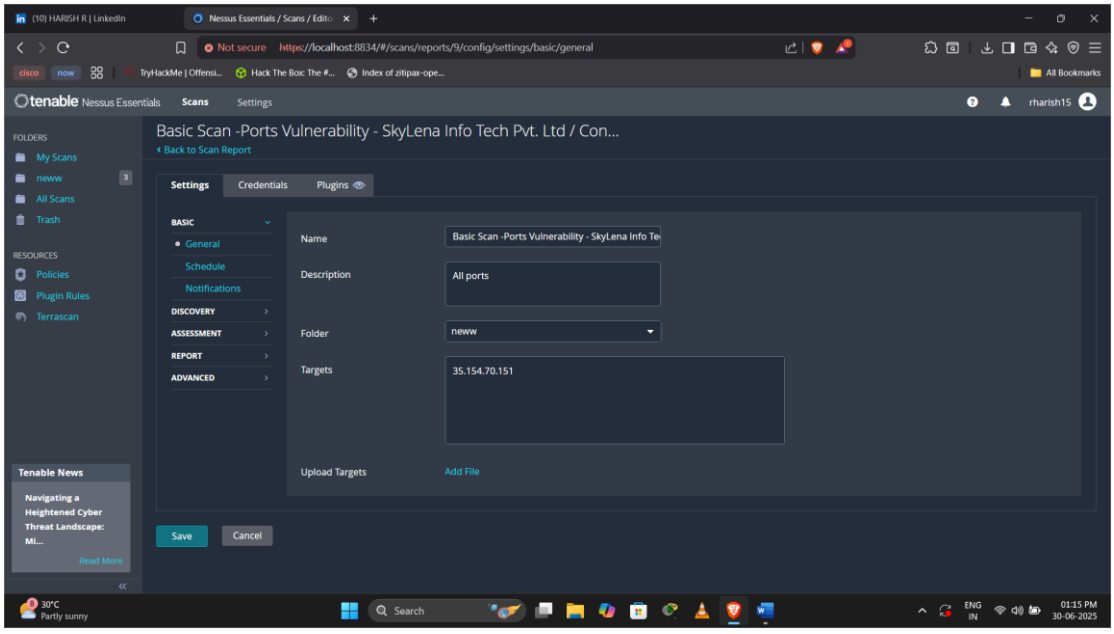


- **Launch the Scan**
  - Click **"Save"** and then **"Launch"**.

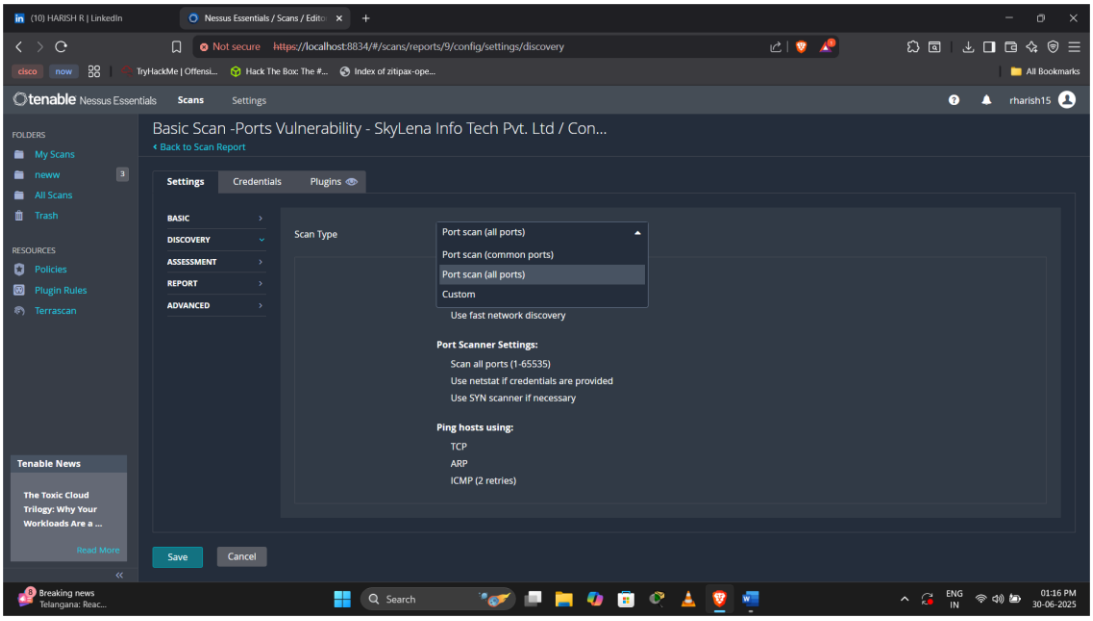
Basic Network Scan :

Configure the Scan

- Set:
  - **Name** of the scan.
  - **Targets** (IP address or domain).
  - **Schedule** (optional).



- Provide the scan type :

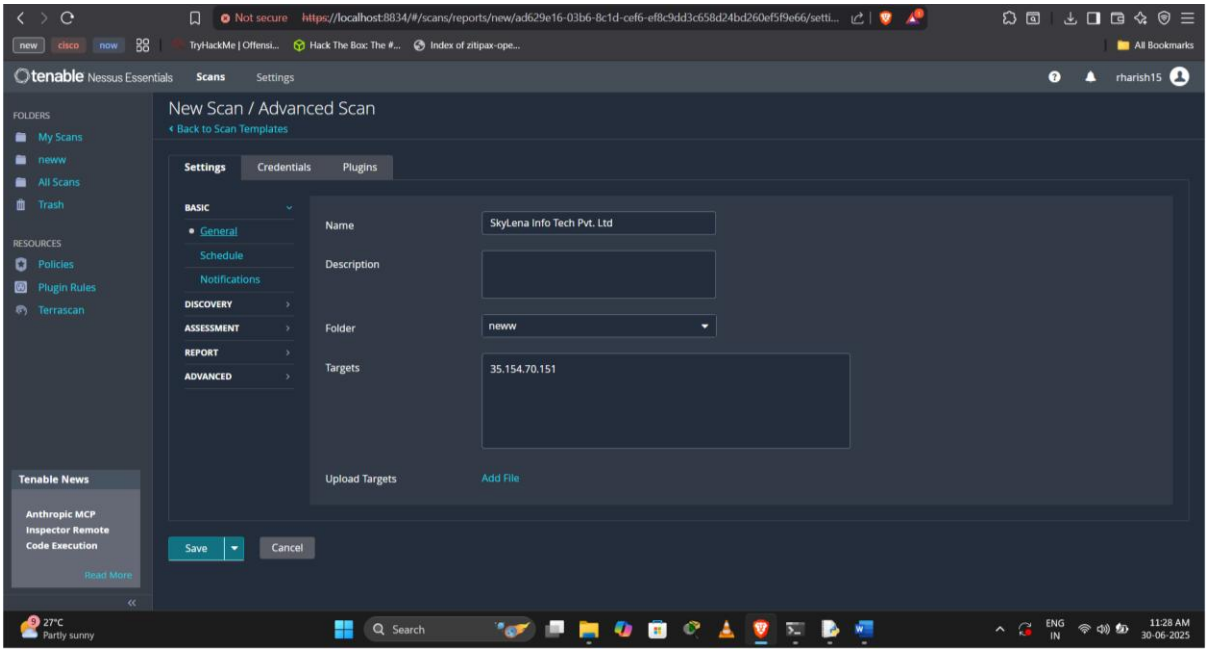


- **Launch the Scan**
  - Click **“Save”** and then **“Launch”**.

Advanced Scan :

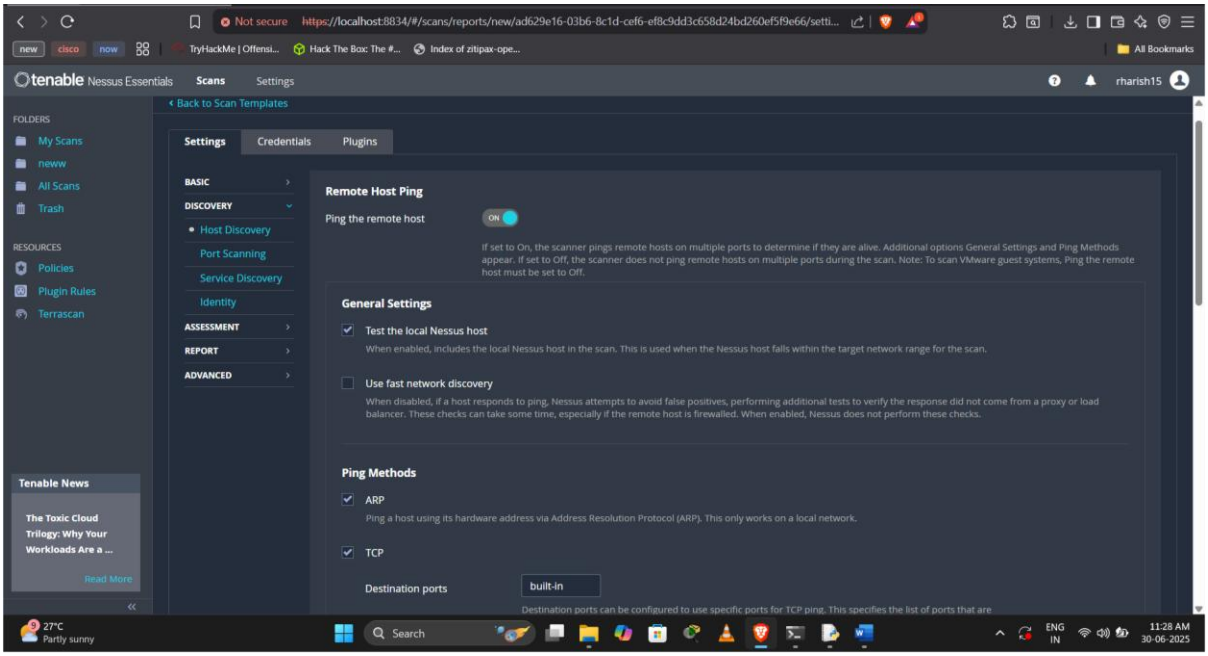
Configure the Scan

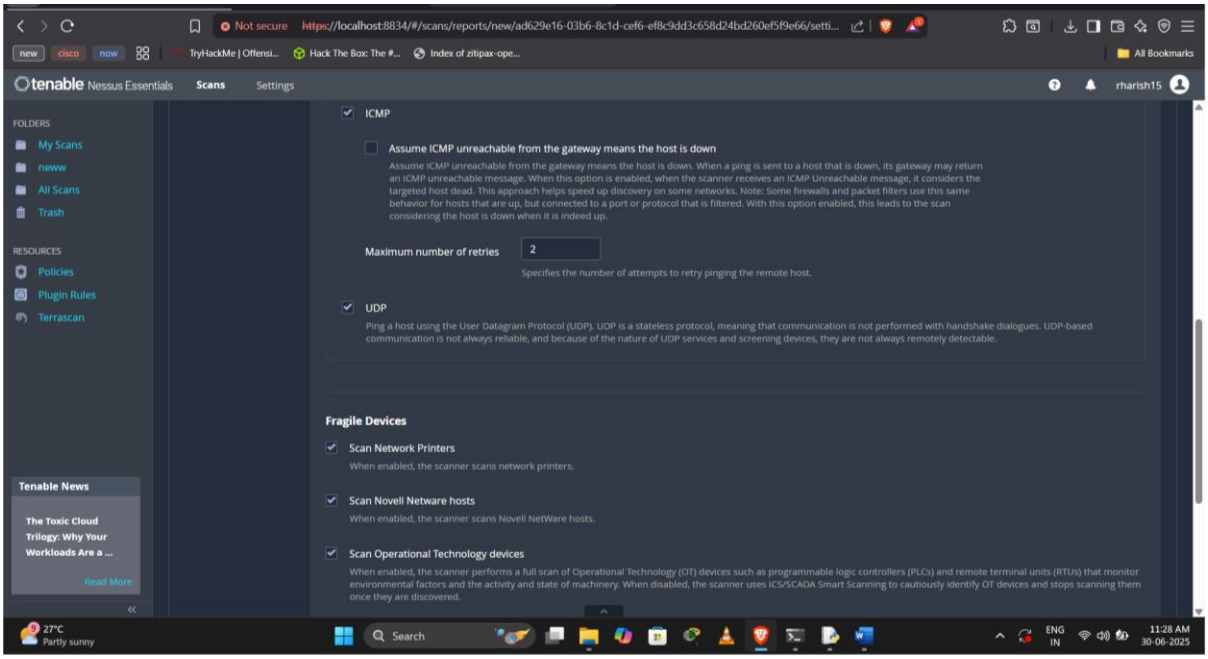
- Set:
  - **Name** of the scan.
  - **Targets** (IP address or domain).
  - **Schedule** (optional).



Provide the scan Configurations :

- General Settings
- Ping methods
- Fragile Devices





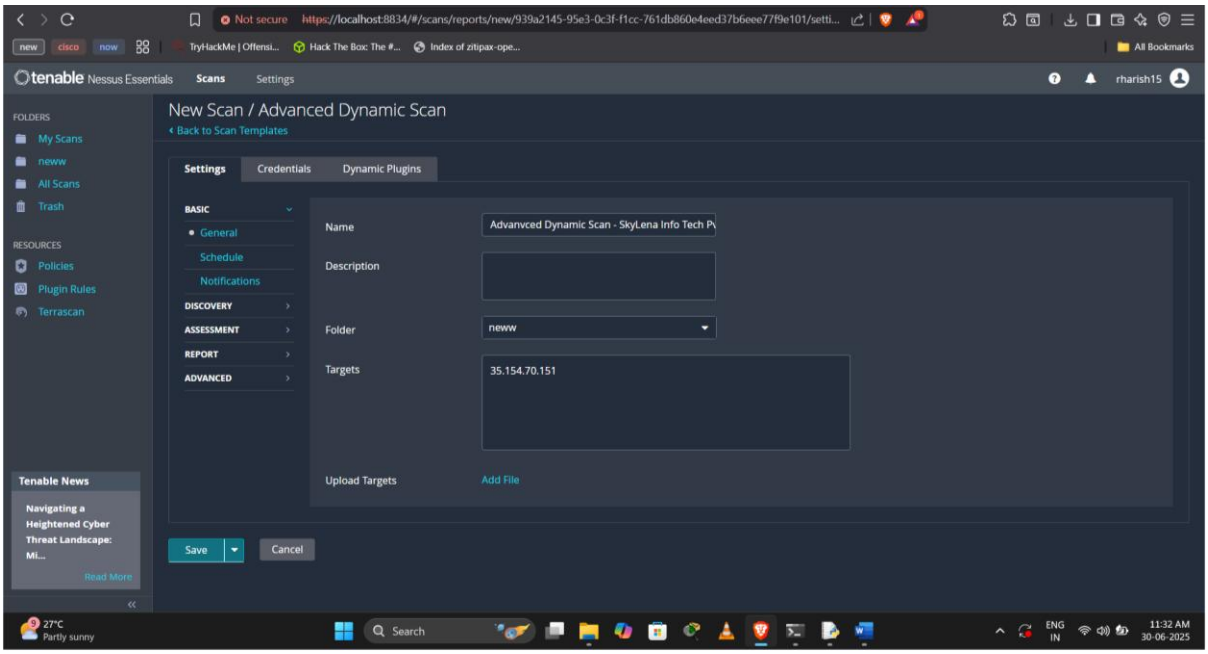
❖ Launch the Scan

- Click **“Save”** and then **“Launch”**.

Advanced Dynamic Scan :

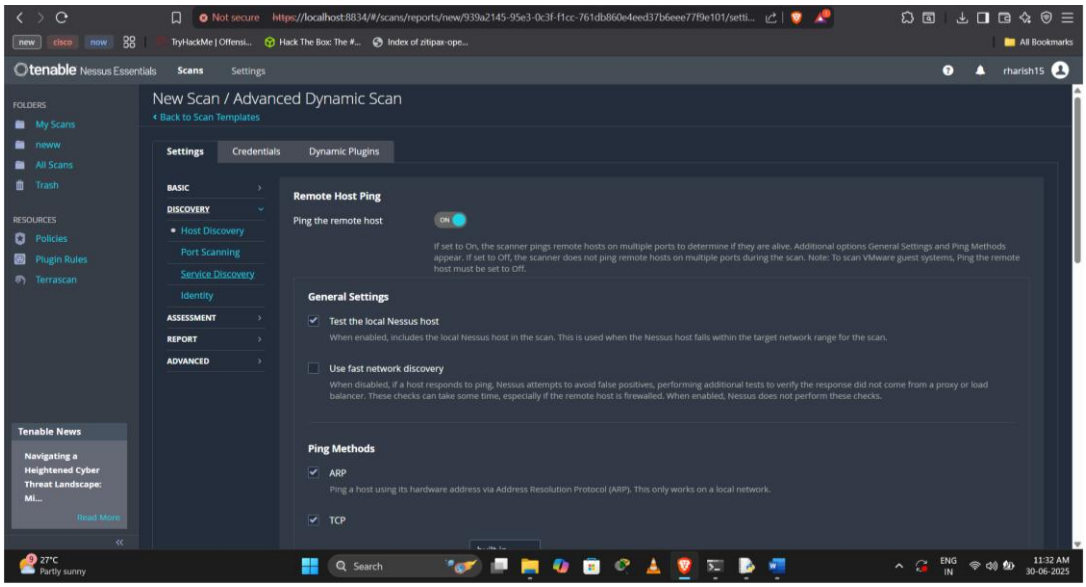
Configure the Scan

- Set:
    - **Name** of the scan.
    - **Targets** (IP address or domain).
    - **Schedule** (optional).



Provide the scan Configurations :

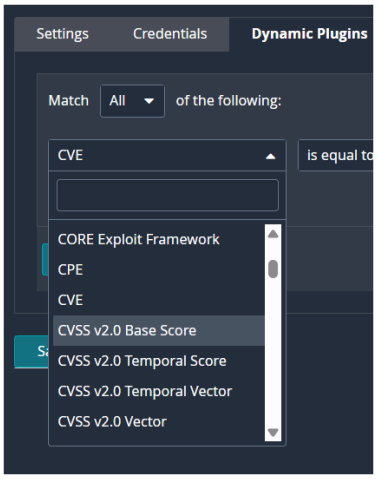
- General Settings
- Ping methods
- Fragile Devices

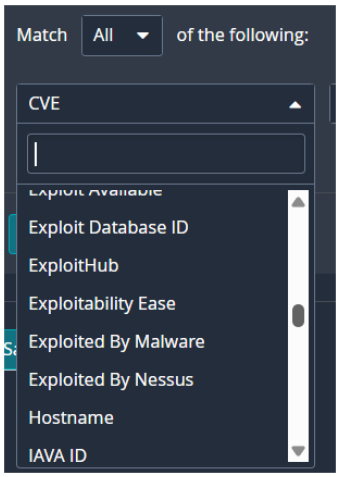


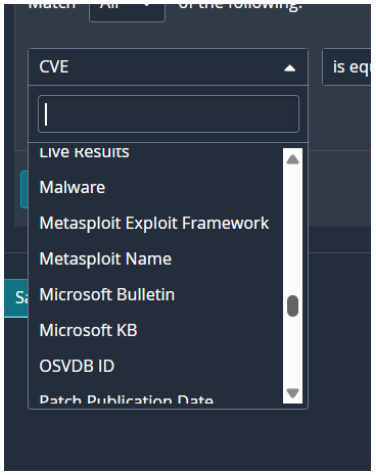
Provide the Dynamic Plugins :

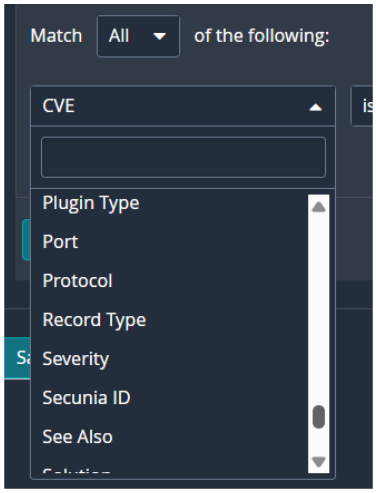
Manually provide the plugins needed :

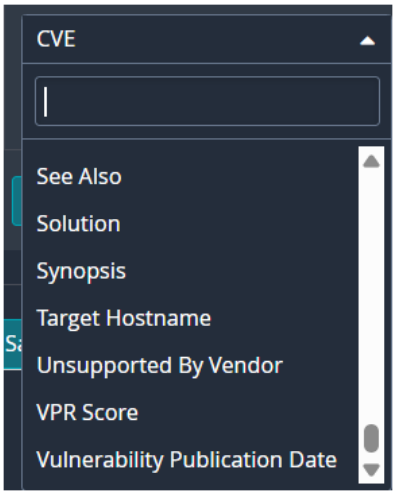
Plugins :

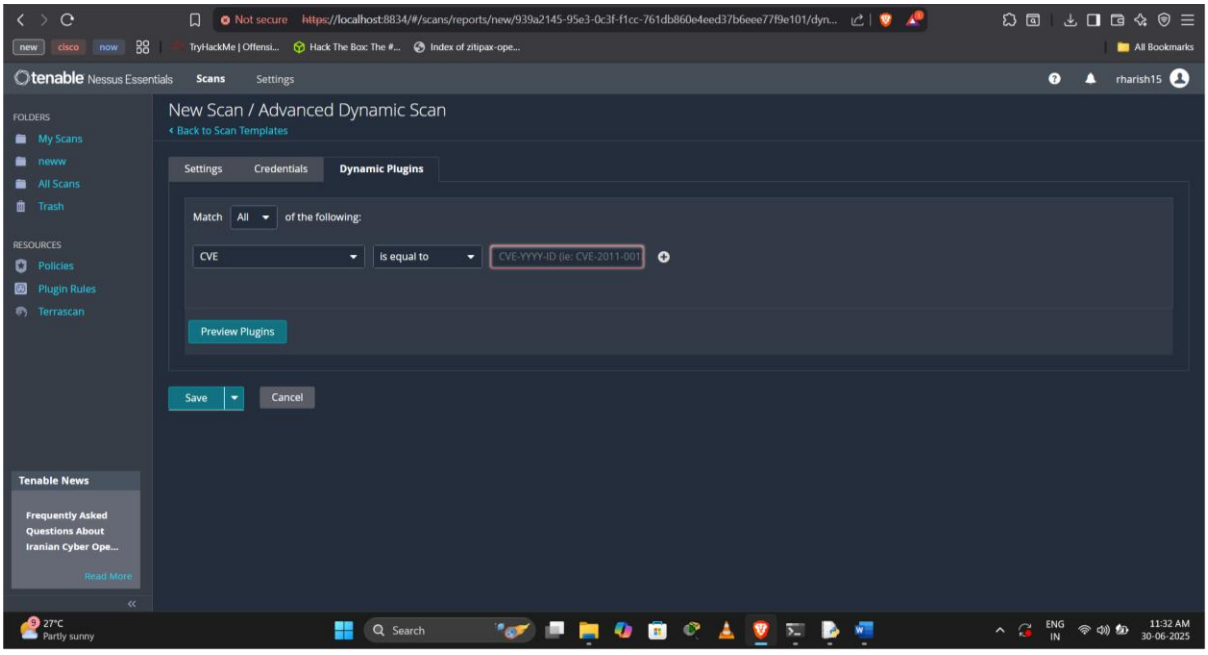










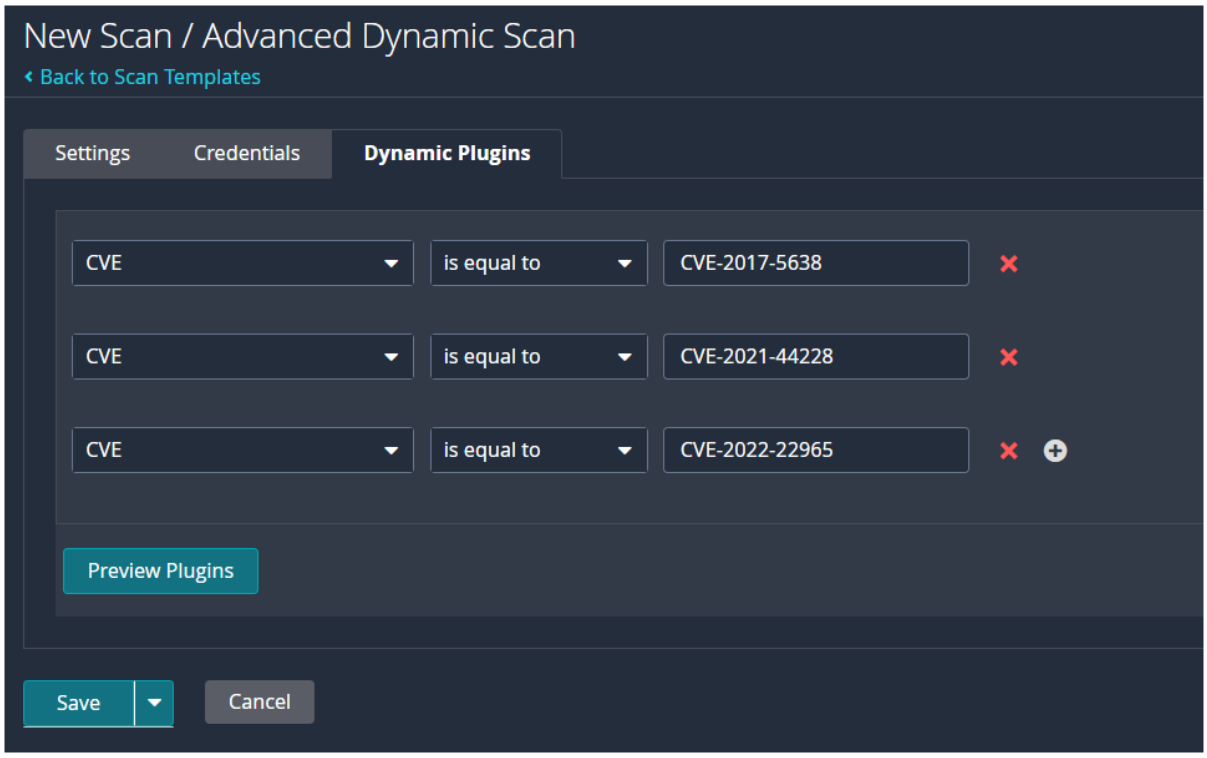


EXAMPLE :

CVE-2017-5638 – Apache Struts RCE

CVE-2021-44228 – Log4Shell in Log4j

CVE-2022-22965 – Spring4Shell in Spring Core

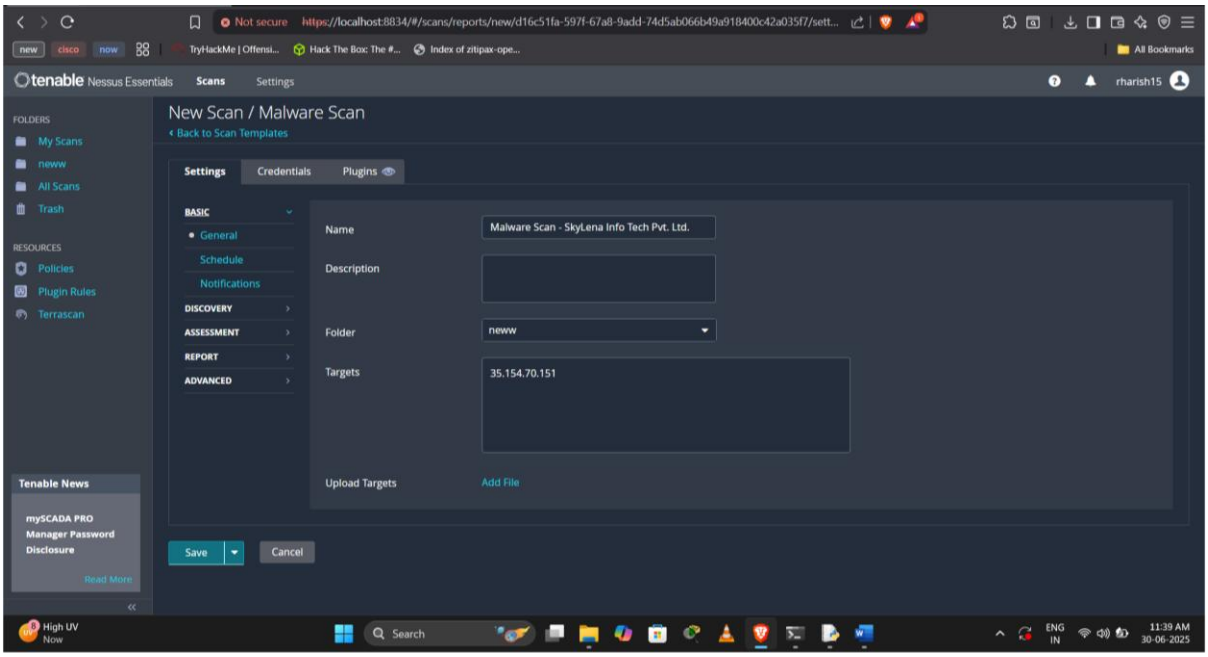


- ❖ **Launch the Scan**
  - Click **"Save"** and then **"Launch"**.

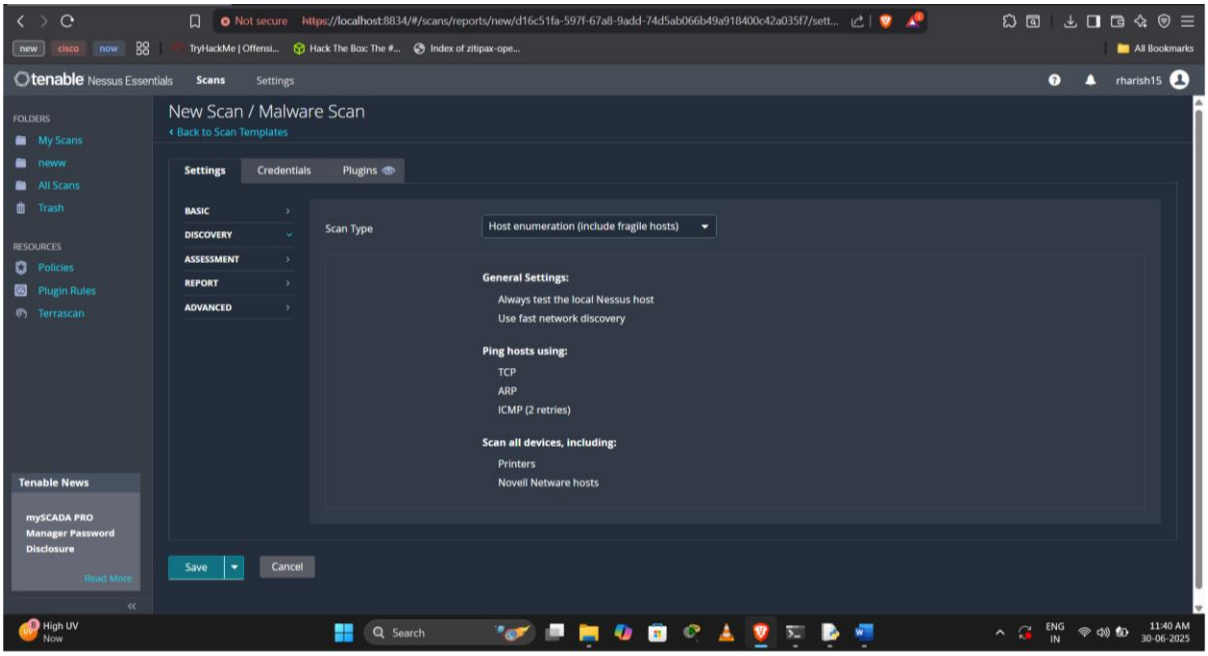
Malware Scan :

Configure the Scan

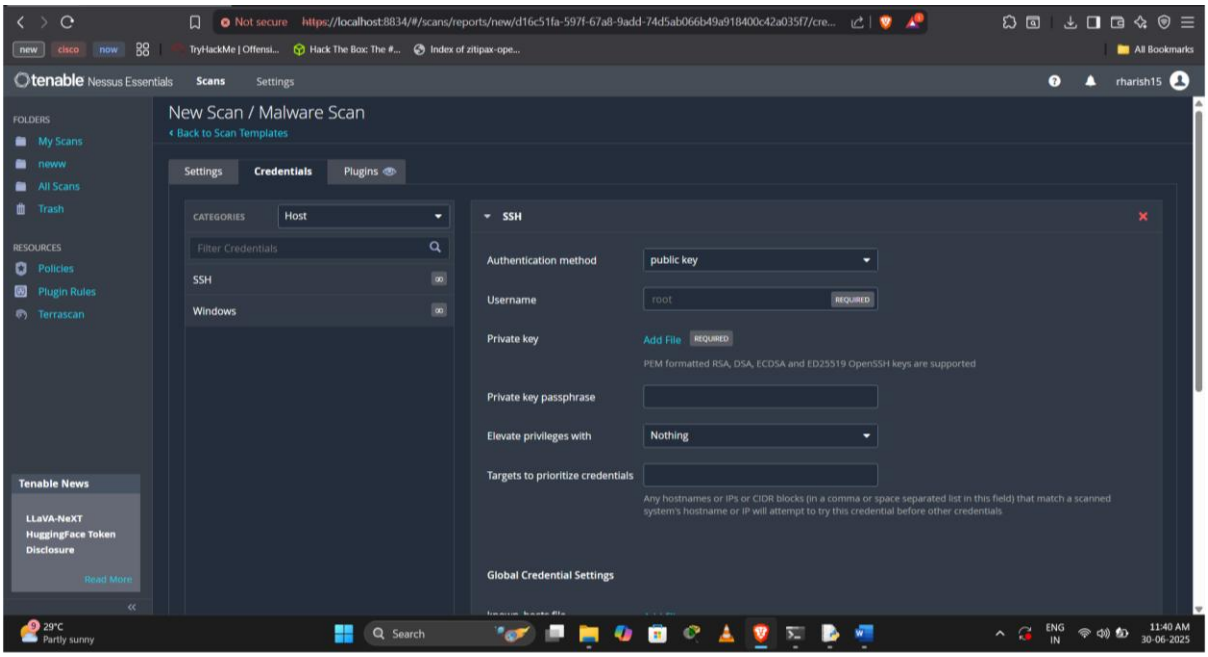
- Set:
    - **Name** of the scan.
    - **Targets** (IP address or domain).
    - **Schedule** (optional).

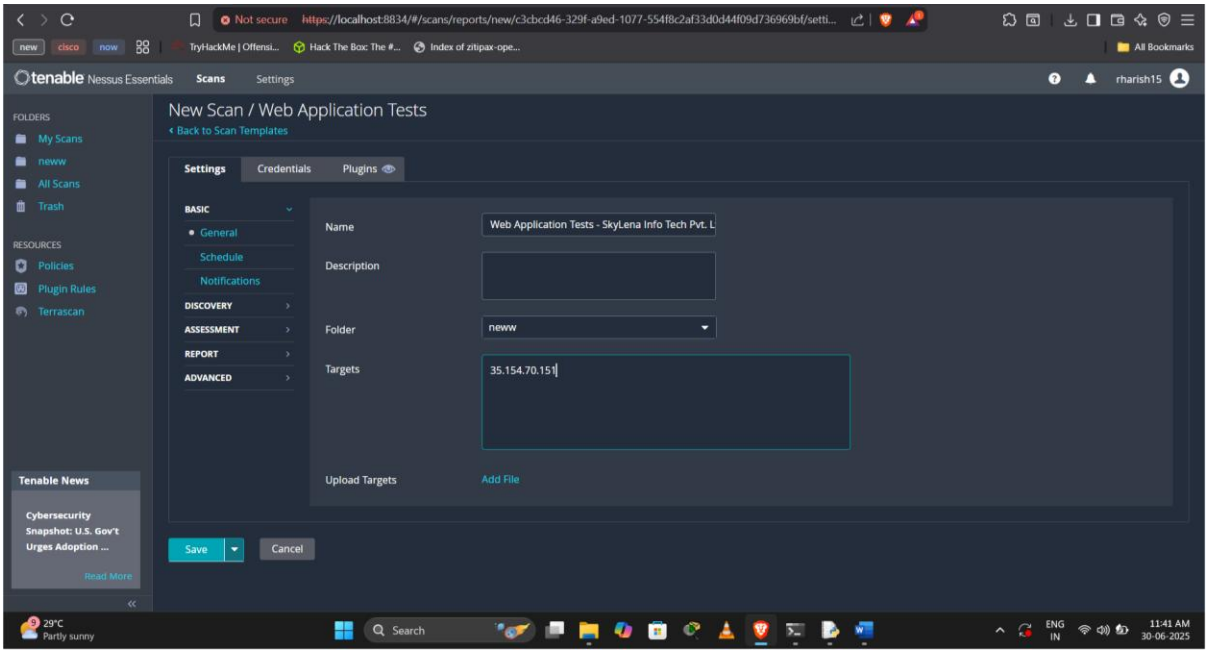


Provide the scan type :



Provide the Plugins Credentials for SSH and Windows (if Needed) :





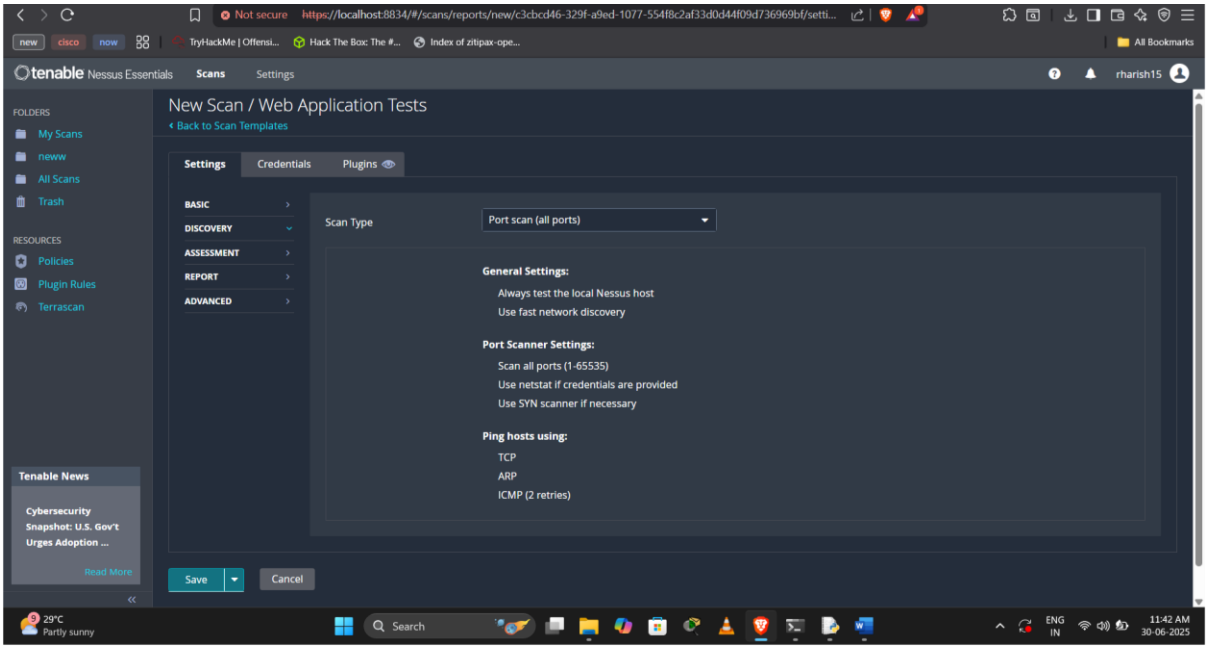
❖ Launch the Scan

- Click **"Save"** and then **"Launch"**.

Web Application Tests Scan :

Configure the Scan

- Set:
    - **Name** of the scan.
    - **Targets** (IP address or domain).
    - **Schedule** (optional).
- Provide the scan type :

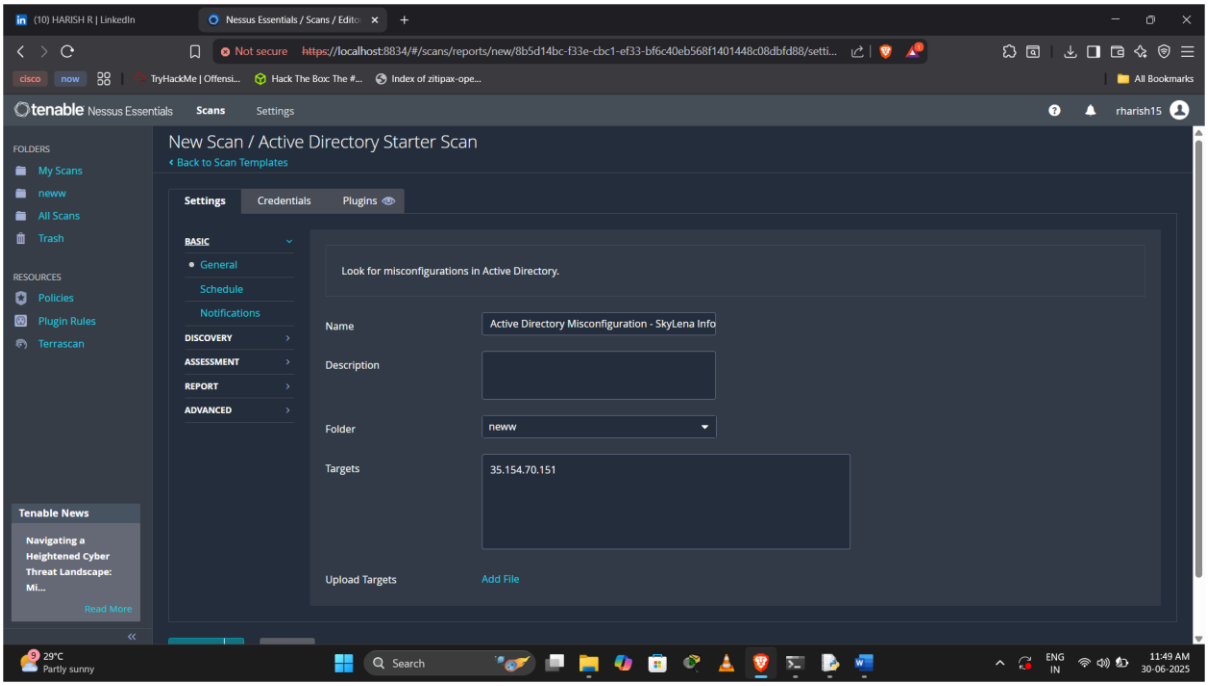


- **Launch the Scan**
    - Click **“Save”** and then **“Launch”**.

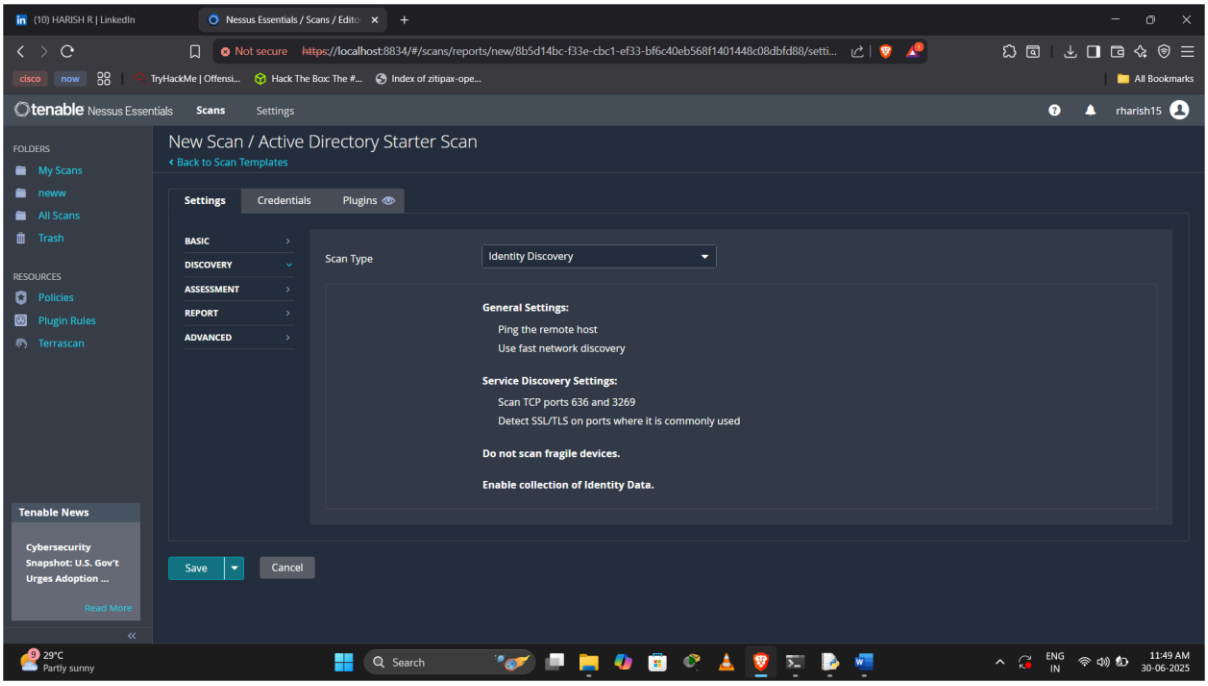
Active Directory starter Scan :

Configure the Scan

- Set:
  - **Name** of the scan.
  - **Targets** (IP address or domain).
  - **Schedule** (optional).



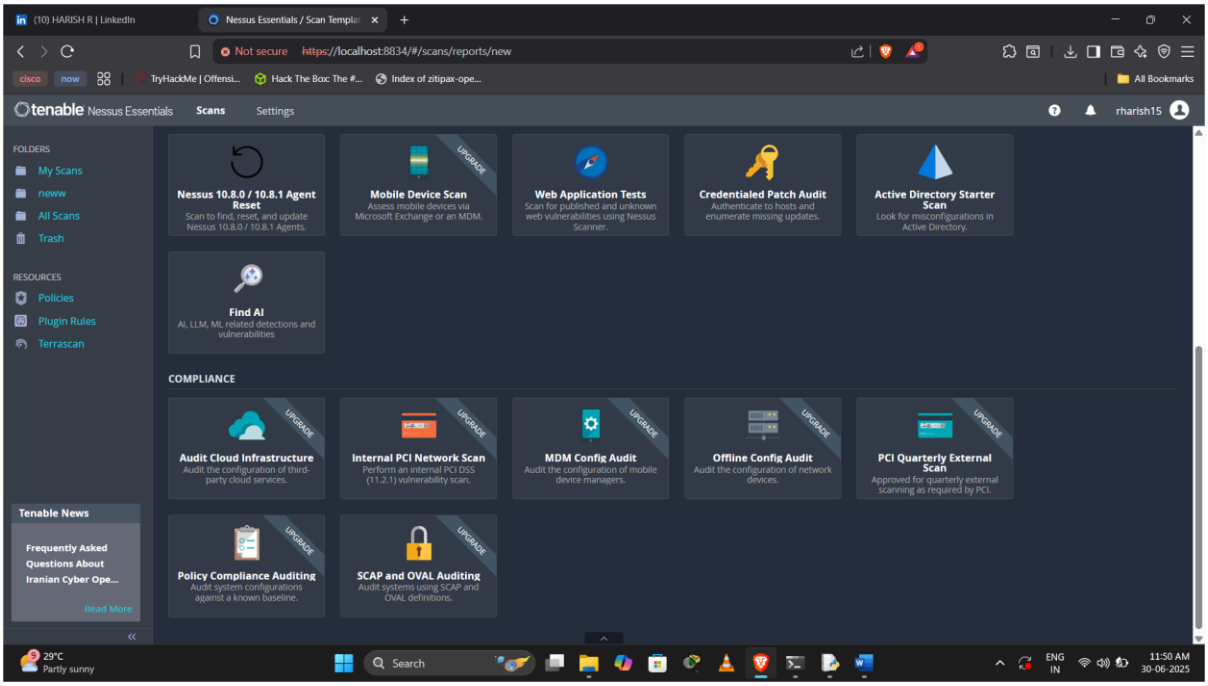
- Provide the scan type :



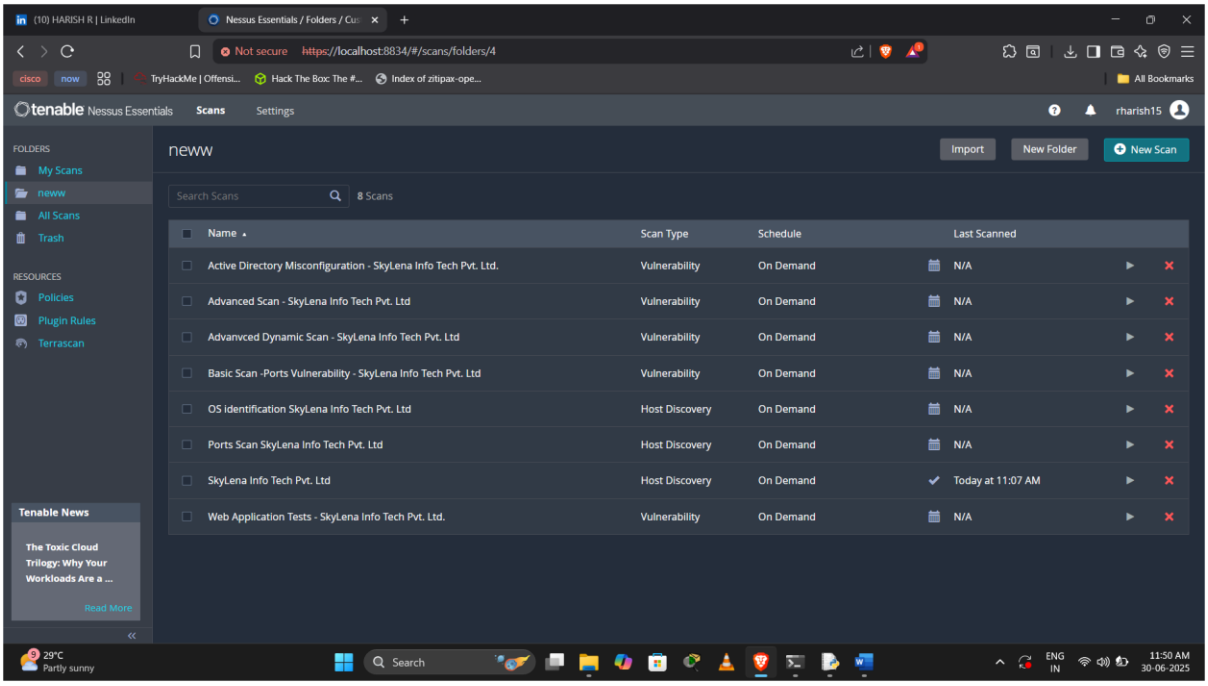
❖ Launch the Scan

- Click **“Save”** and then **“Launch”**.

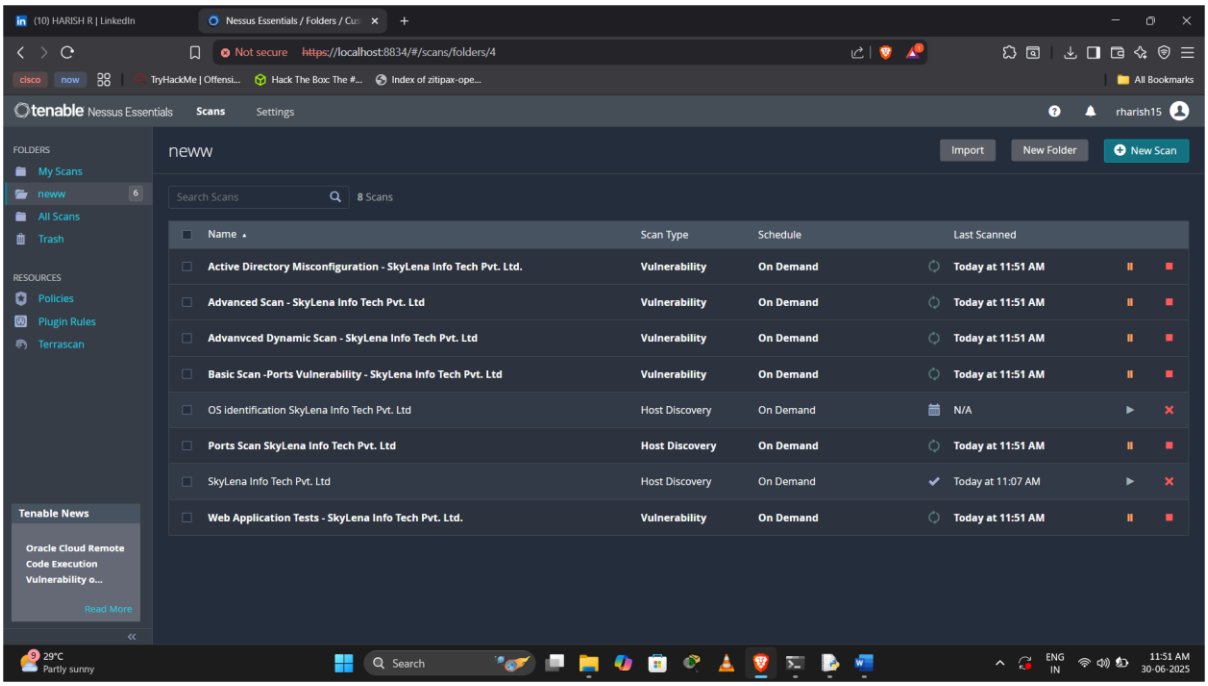
Perform variety of the scans needed :



Wait for the launched scans to be completed :

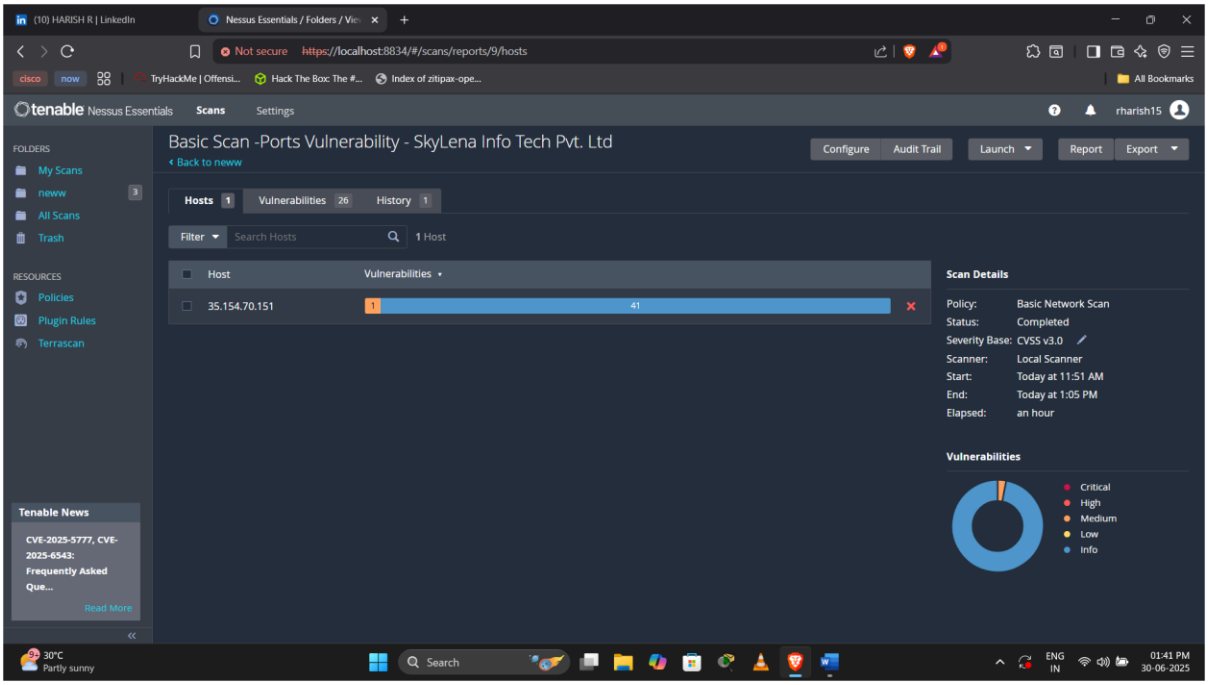


If any unlanched scan found lauch the scan in the specified folder and even can pause, resume and stop the scans if needed :

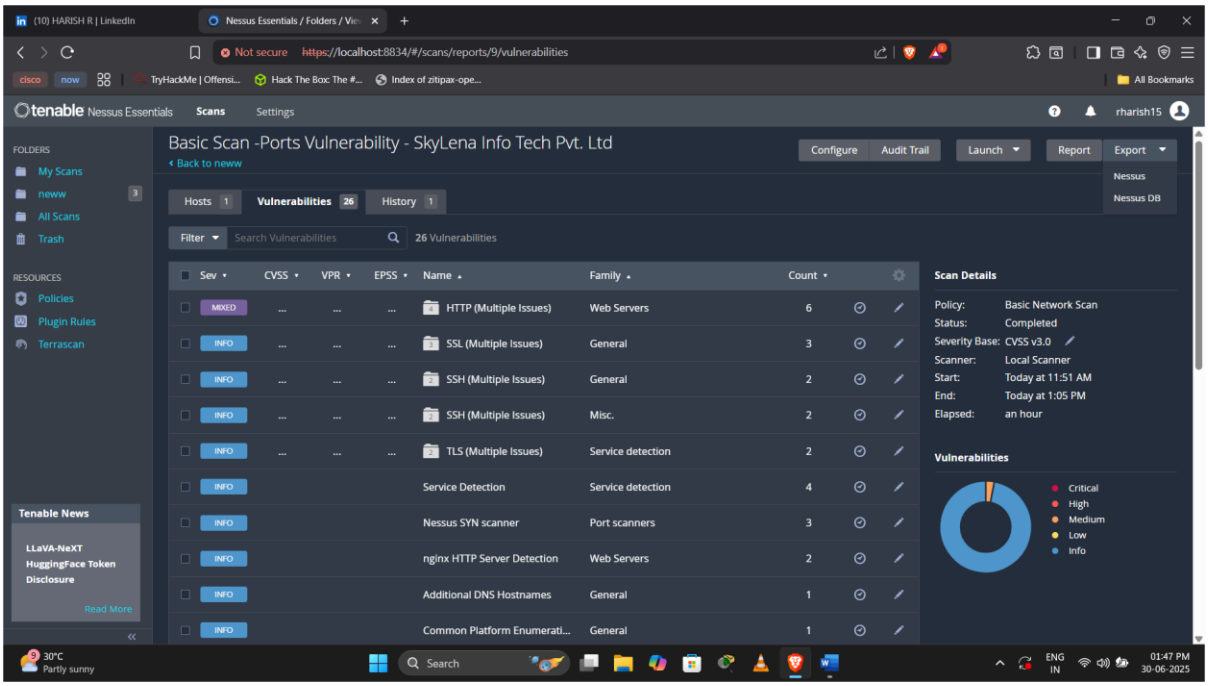


DOCUMENTATION :

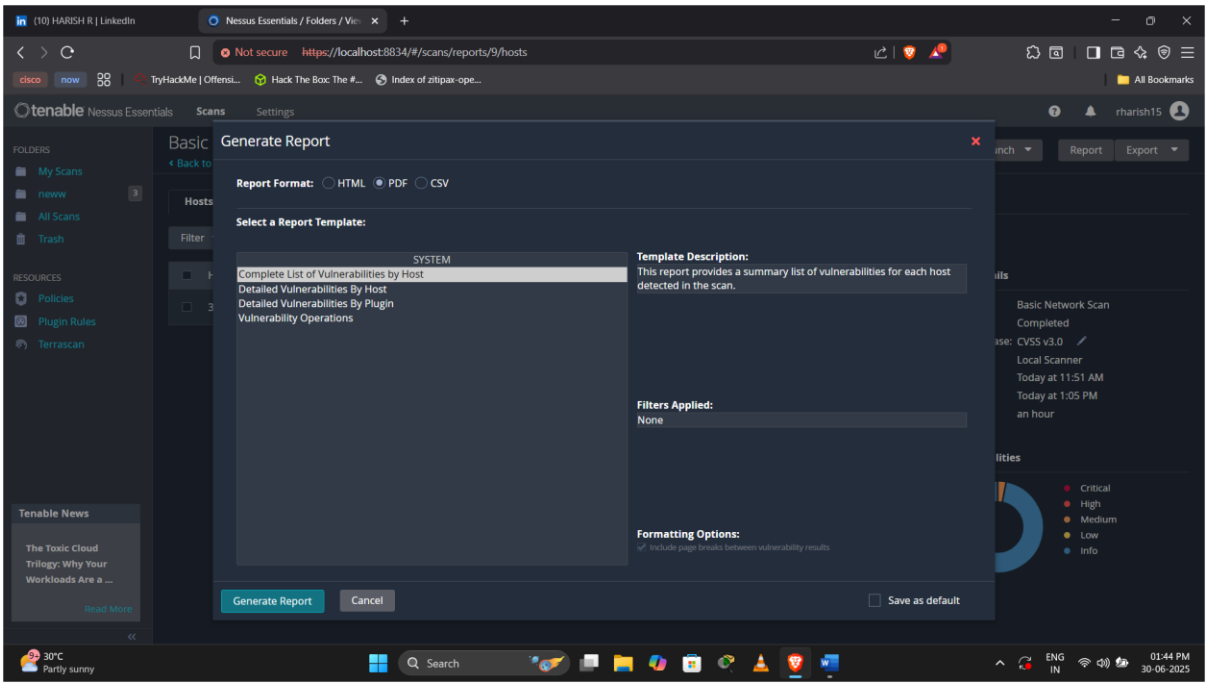
Result :



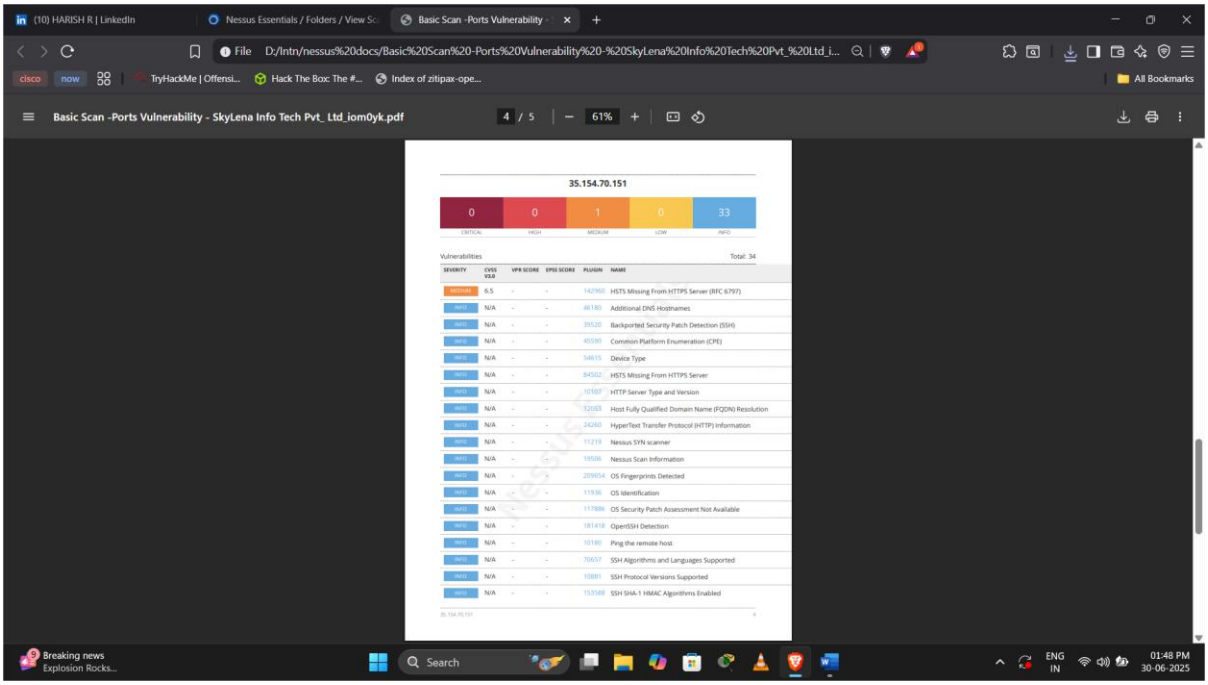
- Select the export option to export the file as “.nessus” and “.db” formats for further analysis by others.



- Select report to provide report in as “pdf ”, ”HTML” , “CSV” formats.



Sample Report from **Basic network scan :**



Reports :

https://drive.google.com/drive/u/5/folders/1vSRSNlFFbH0_mag3Xi0XWaDy558fQLlD