

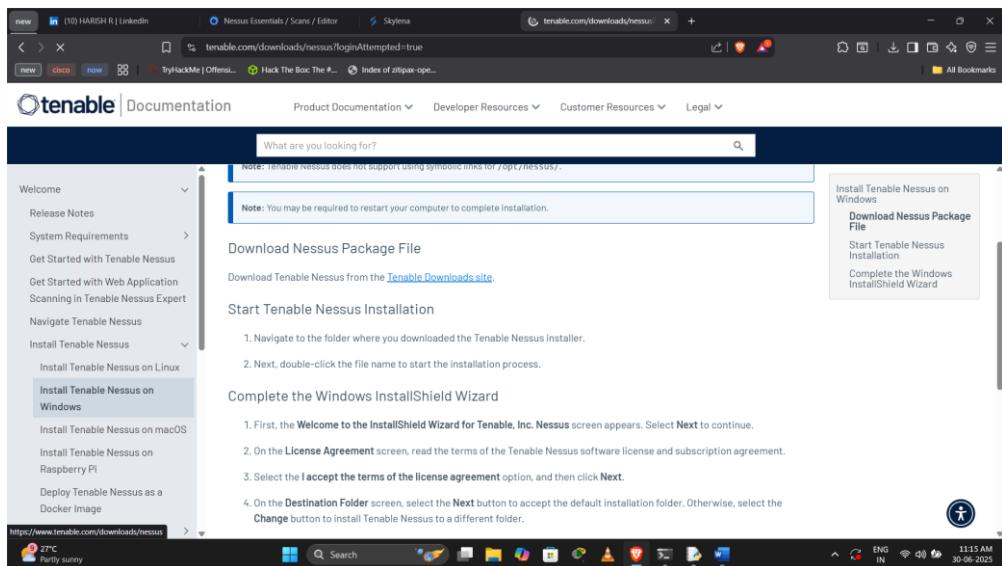
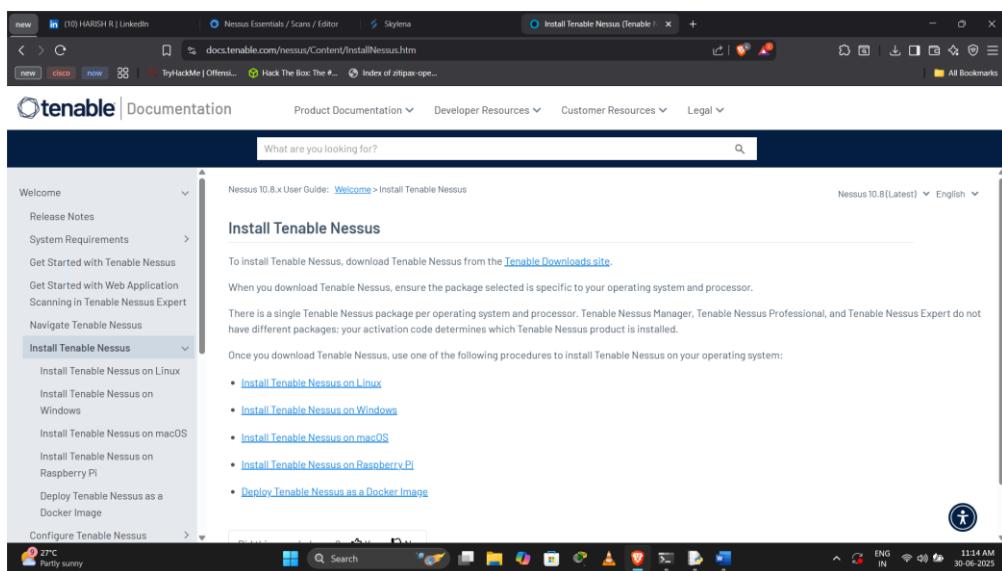
NESSUS

A VULNERABILITY SCANNER

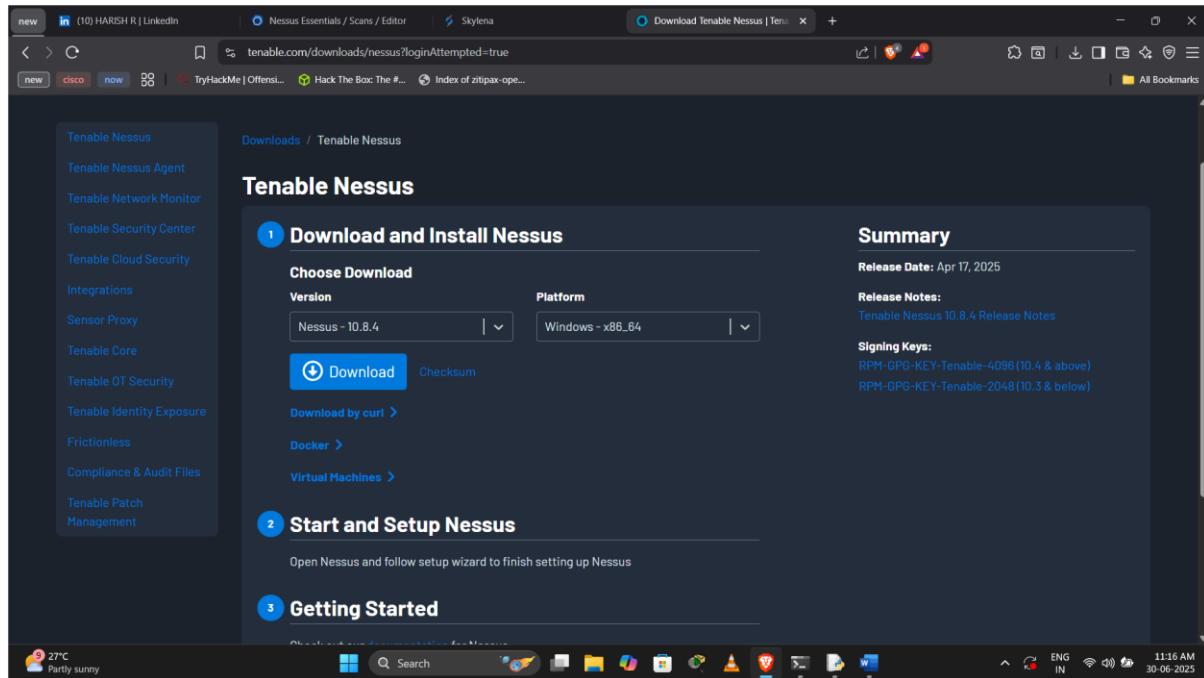
Installation :

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 :

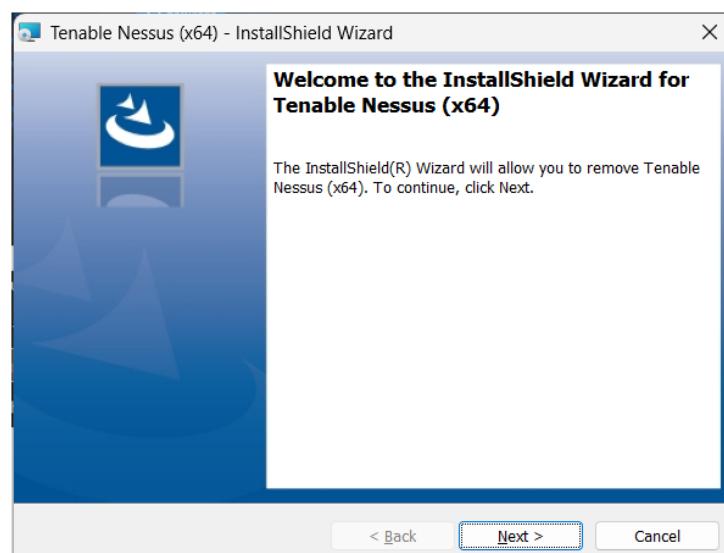


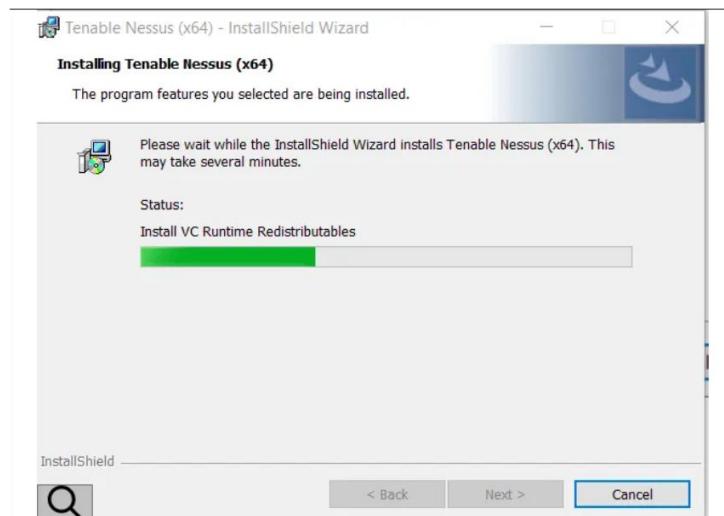
The screenshot shows a web browser window with the URL [tenable.com/downloads/nessus?loginAttempted=true](https://www.tenable.com/downloads/nessus?loginAttempted=true). The main content is the 'Tenable Nessus' download page. It features three main sections: '1 Download and Install Nessus', '2 Start and Setup Nessus', and '3 Getting Started'. In the 'Download and Install Nessus' section, there are dropdown menus for 'Version' (set to 'Nessus - 10.8.4') and 'Platform' (set to 'Windows - x86_64'). A large blue 'Download' button is prominently displayed. To the right, the 'Summary' section provides details about the release date (Apr 17, 2025) and release notes. The left sidebar contains a navigation menu with links to various Tenable products. At the bottom, a Windows taskbar is visible with icons for File Explorer, Task View, Start, Search, and other system tools.

Save the downloaded file and Run the setup file for :

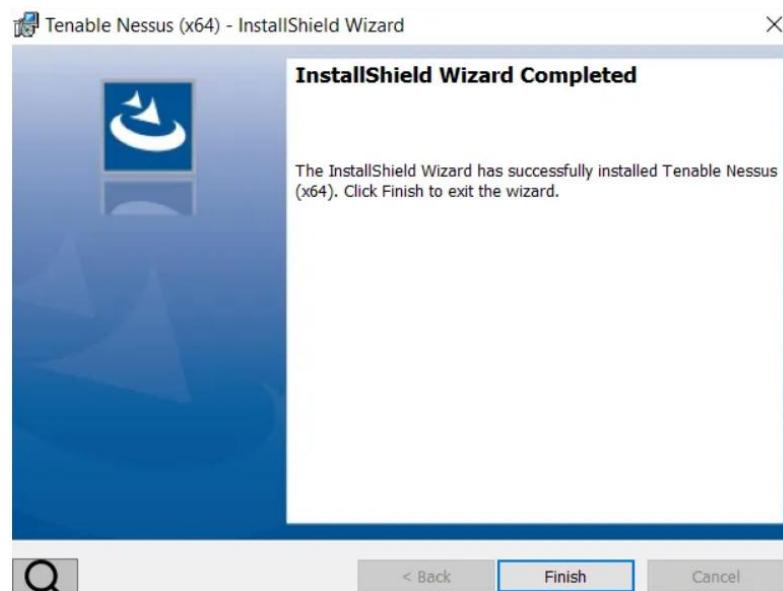
 burpsuite_community_windows-x64_v202...	17-06-2025 06:13 PM	Application	3,22,989 KB
 nmap-7.97-setup	17-06-2025 06:05 PM	Application	34,911 KB
 Nessus-10.8.4-x64	17-06-2025 06:04 PM	Windows Installer ...	97,897 KB
 Wireshark-4.4.7-x64	17-06-2025 06:04 PM	Application	85,304 KB

Proceed with **installation process** :





Finish the Setup file installation process :

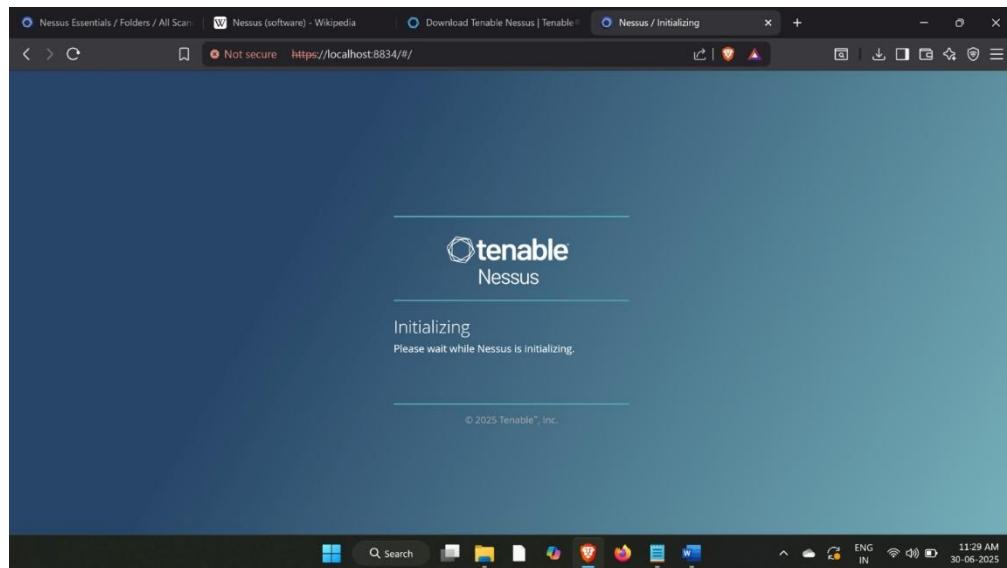


Installation Completed ...!

Access the Nessus Web Interface :

Open the nessus in the Local browser for Configuring the software

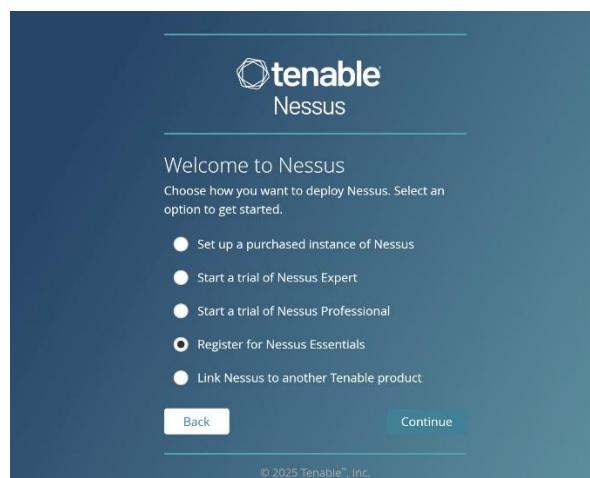
Using : <https://localhost:8834/>



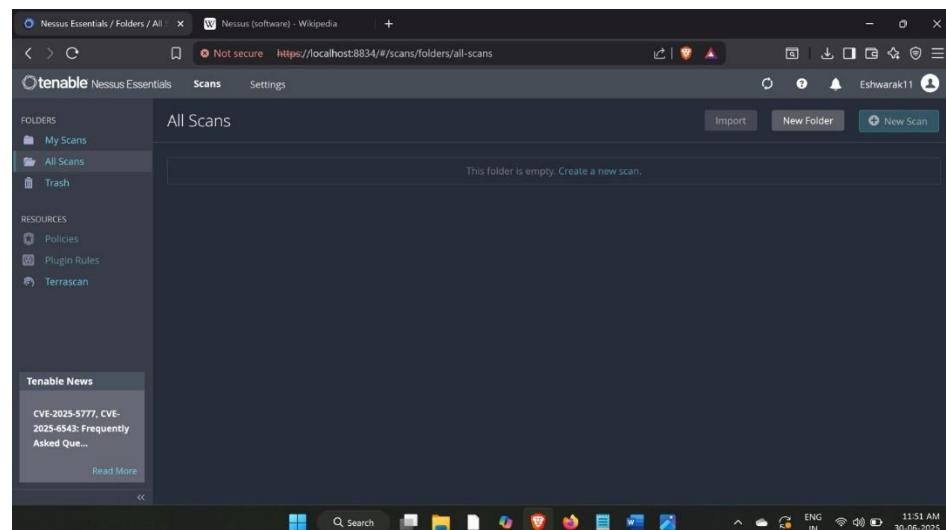
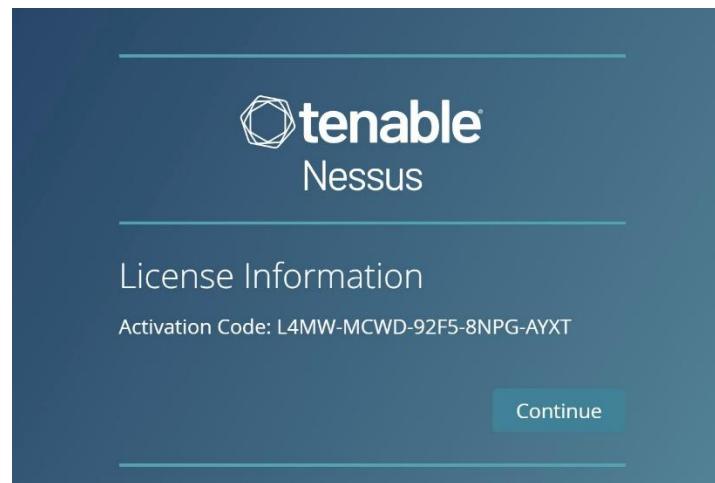
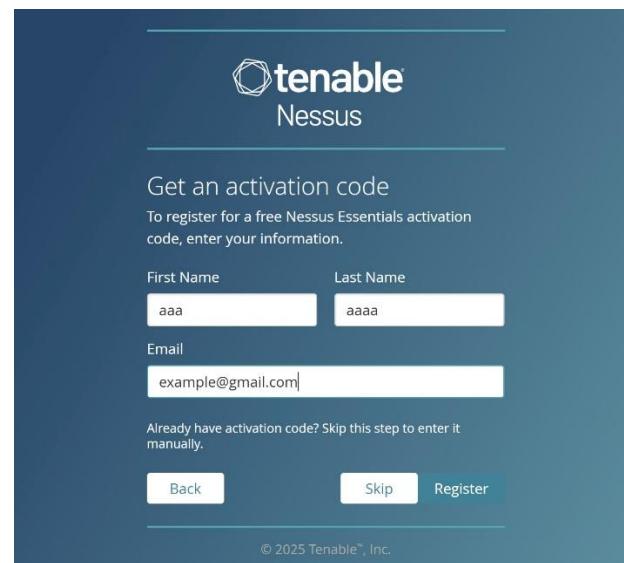
Installs necessary plugins and dependencies needed and loaded to configurations phase :



Select and register for Nessus essentials :

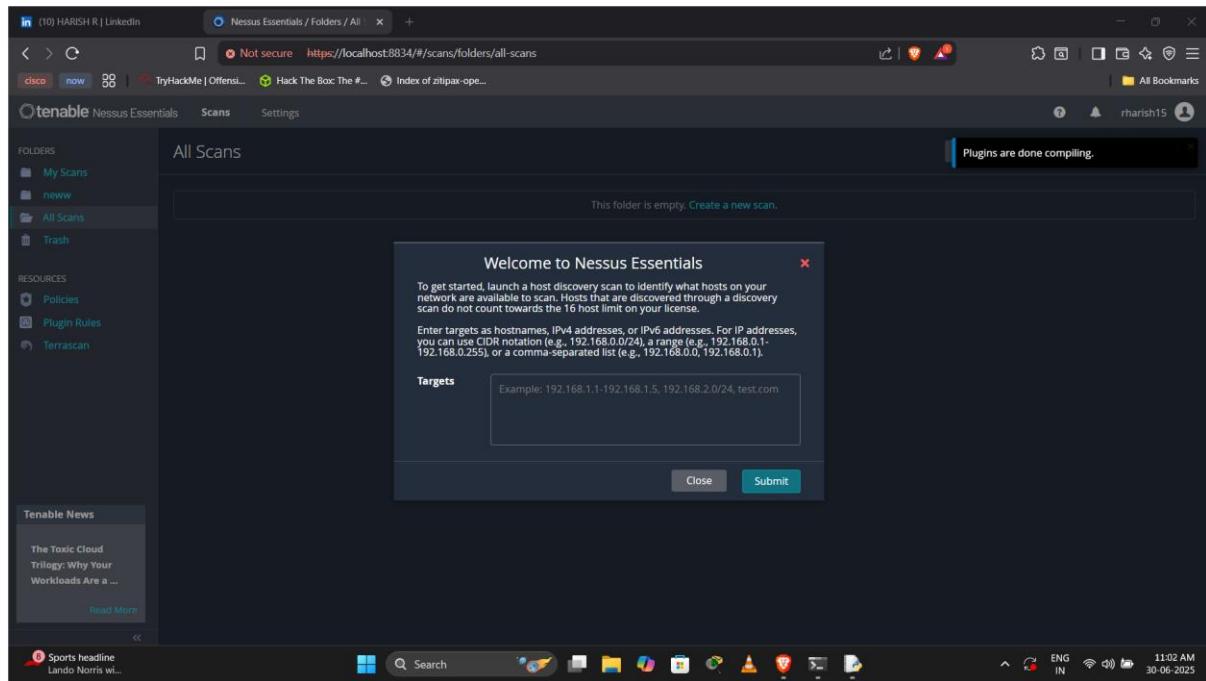


Register for activation code and access the interface for scanning :



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:

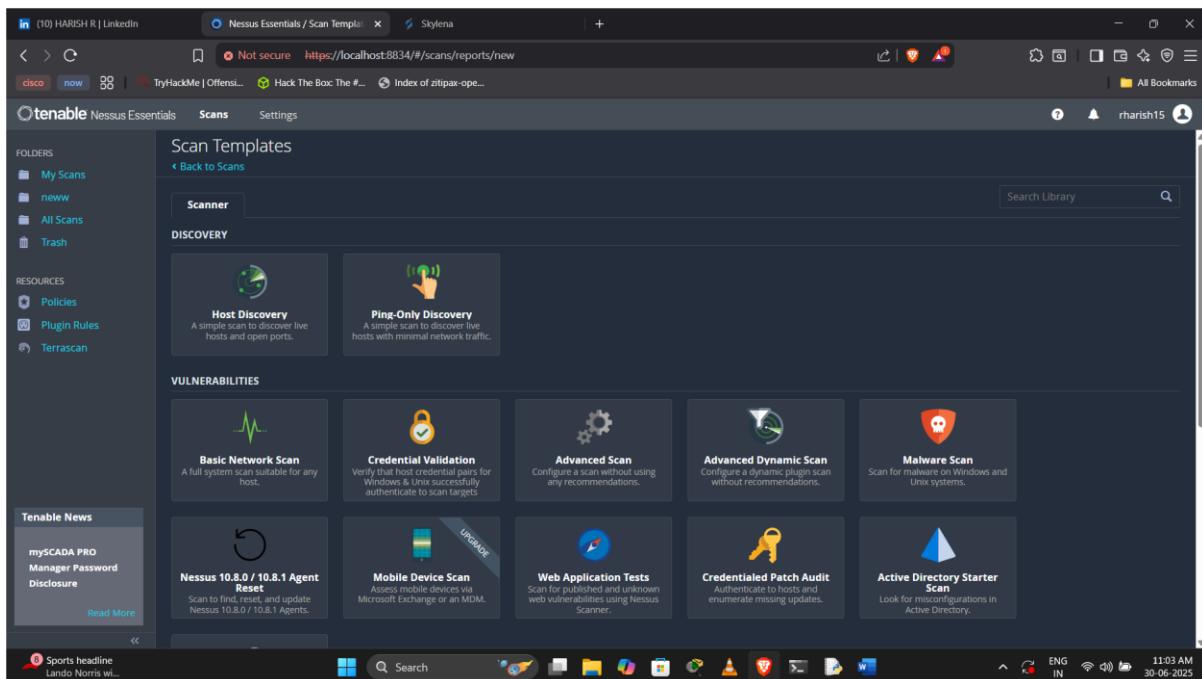
- Verify that systems are configured to **meet specific security standards**.
- Check for compliance with **CIS benchmarks, DISA STIGs, PCI-DSS**, etc.

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**.



Prerequisites :

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

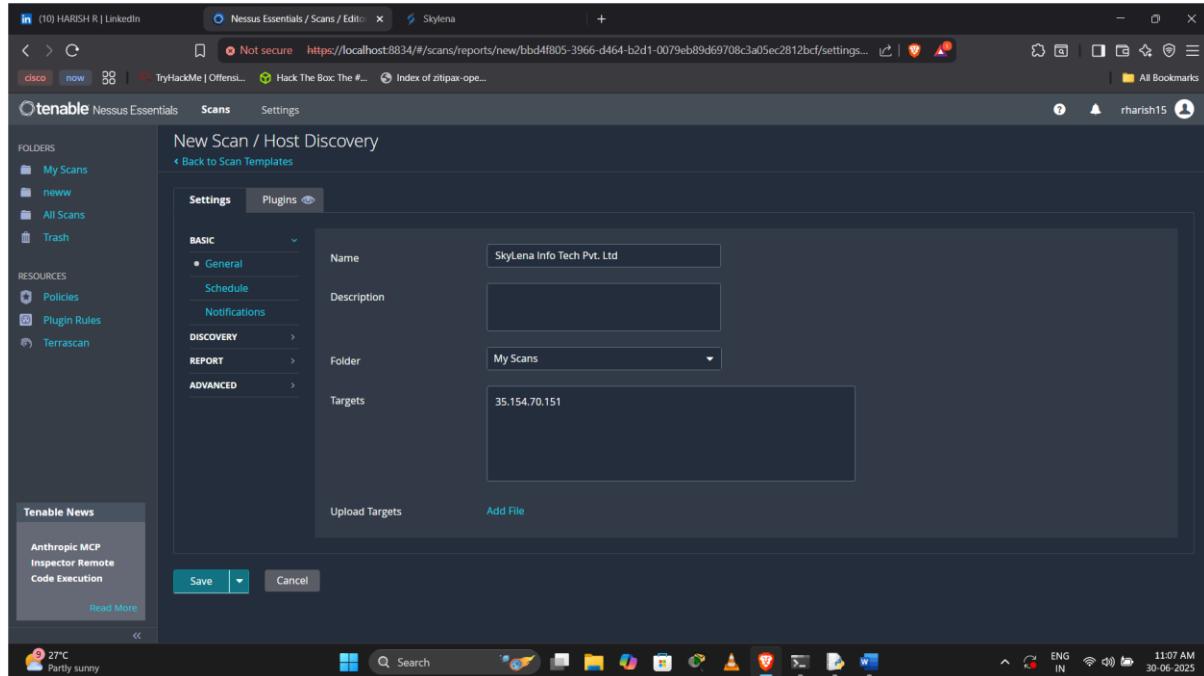
Scan Template	Description
Audit Cloud Infrastructure	Audit the configuration of third-party cloud services.
Internal PCI Network Scan	Perform an internal PCI DSS (11.2.1) vulnerability scan.
MDM Config Audit	Audit the configuration of mobile device managers.
Offline Config Audit	Audit the configuration 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

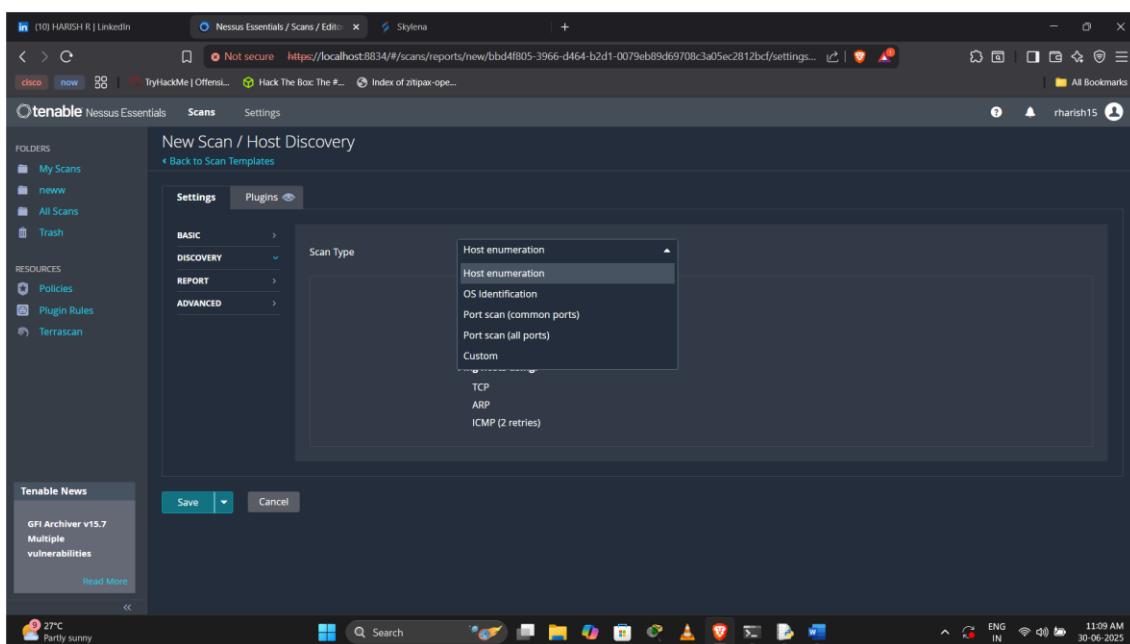
❖ Set:

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



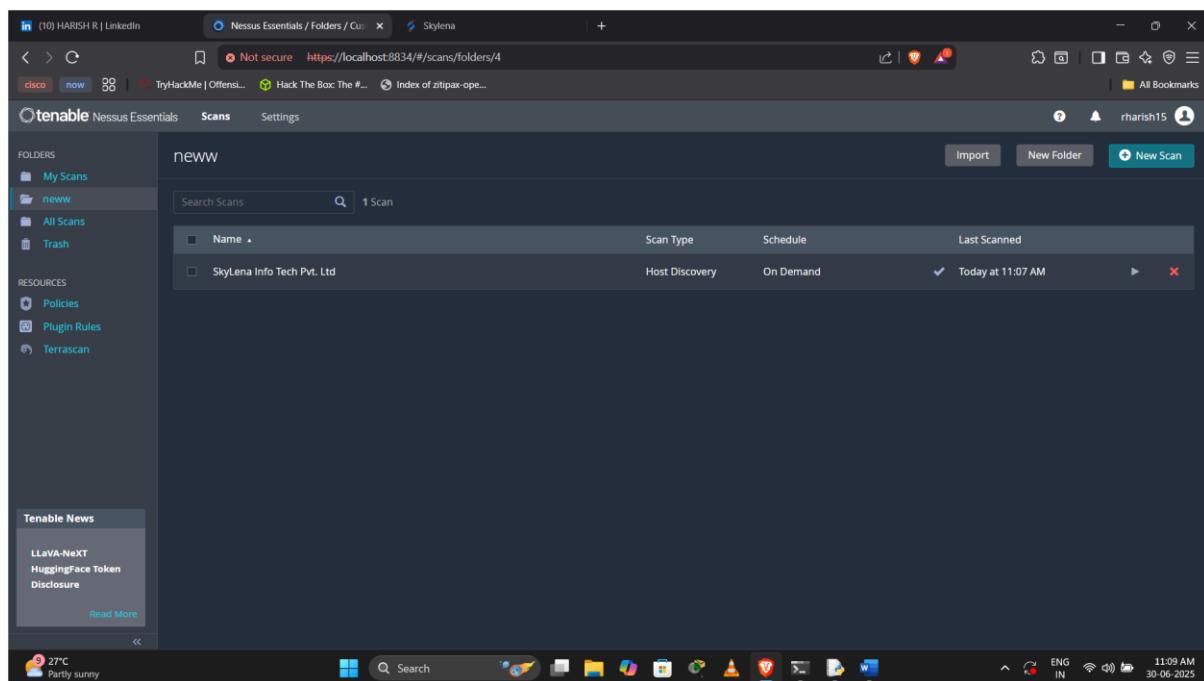
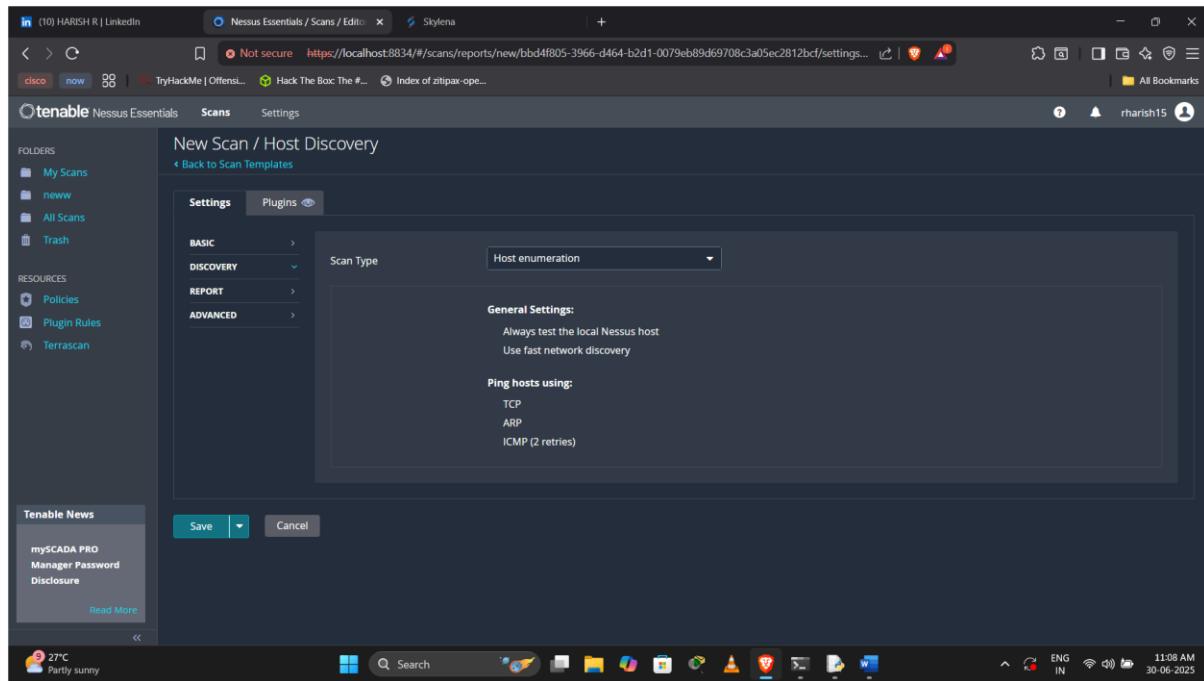
Provide the scan type :

- 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 :

The screenshot shows the Nessus Essentials web interface. On the left, there's a sidebar with 'Folders' (My Scans, new, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (with items like CVE-2025-5777, CVE-2025-6543). The main area displays 'Scan Details' for a completed 'Host Discovery' scan. It shows the 'Severity Base' as CVSS v3.0, 'Scanner' as Local Scanner, and the 'Start' and 'End' times as Today at 11:05 AM and Today at 11:07 AM, with an 'Elapsed' time of 2 minutes. Below this is a 'Vulnerabilities' section with a donut chart showing the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

OS identification :

Configure the Scan

❖ Set:

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

❖ Provide the scan type :

The screenshot shows the 'New Scan / Host Discovery' configuration page. The 'Settings' tab is selected. Under 'Scan Type', 'OS Identification' is chosen. In the 'General Settings' section, it says 'Always test the local Nessus host' and 'Use fast network discovery'. Under 'Ping hosts using:', options for TCP, ARP, and ICMP are listed. At the bottom, there are 'Save' and 'Cancel' buttons.

❖ Launch the Scan

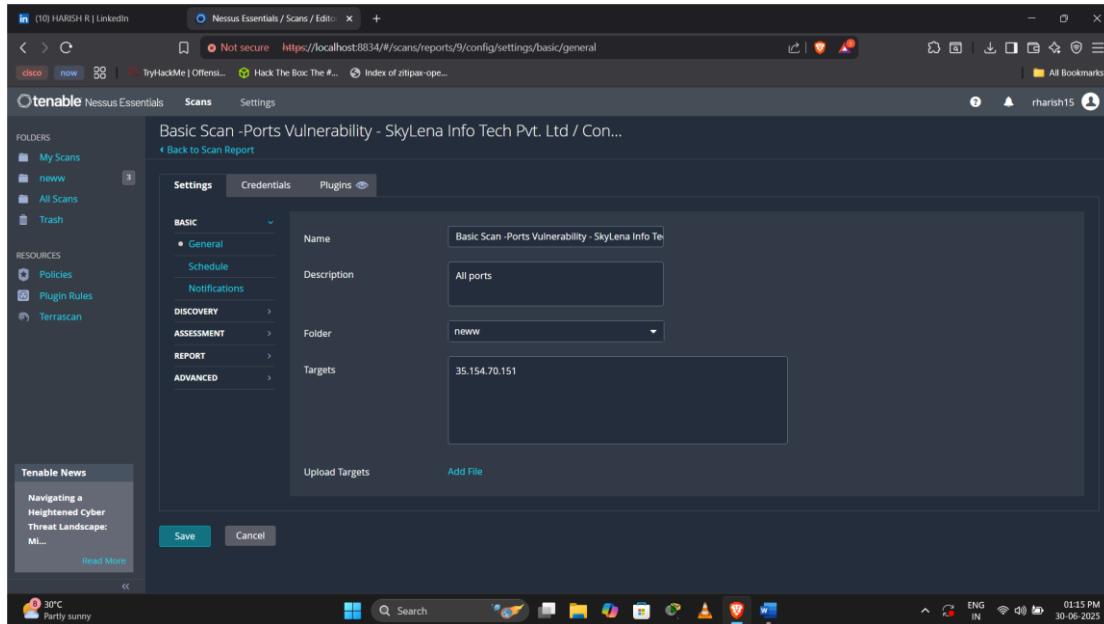
- Click “Save” and then “Launch”.

Basic Network Scan :

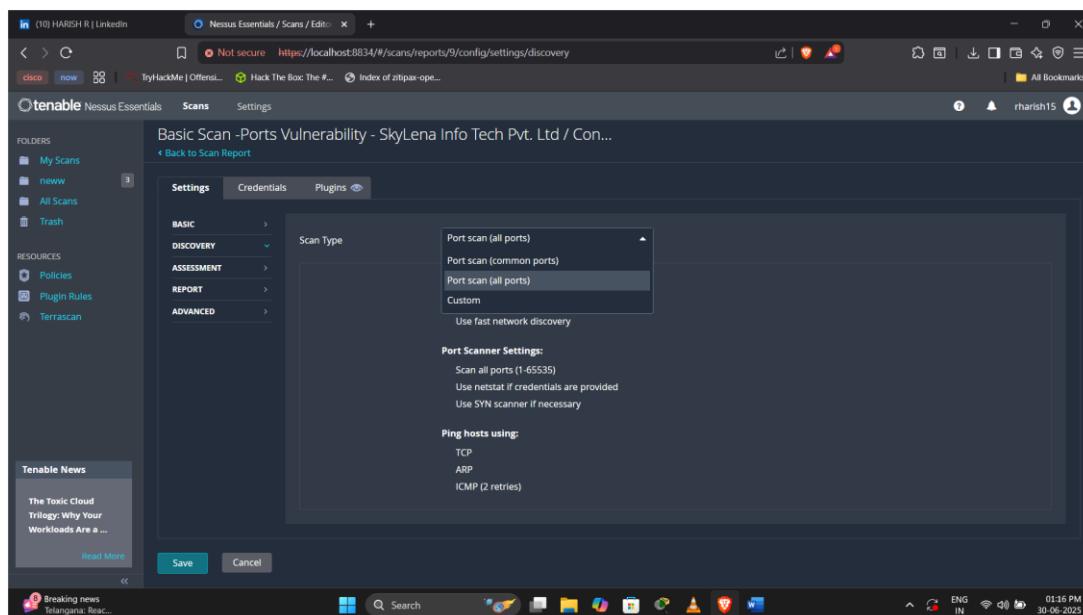
Configure the Scan

❖ 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:

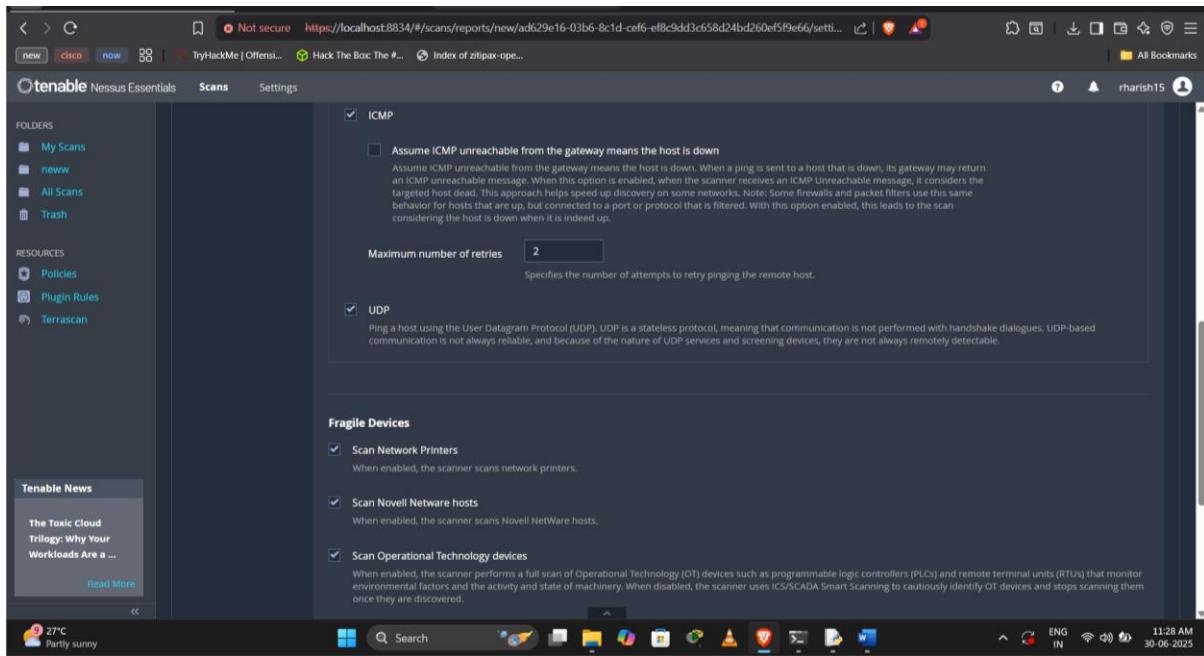
- **Name** of the scan.
- **Targets** (IP address or domain).
- **Schedule** (optional).

The screenshot shows the 'New Scan / Advanced Scan' configuration page. The 'Settings' tab is active. In the 'BASIC' section, the 'Name' field is populated with 'SkyLena Info Tech Pvt. Ltd'. The 'Targets' field contains the IP address '35.154.70.151'. The 'Folder' dropdown is set to 'neww'. The 'Description' field is empty. At the bottom, there are 'Save' and 'Cancel' buttons.

Provide the scan Configurations :

- ❖ General Settings
- ❖ Ping methods
- ❖ Fragile Devices

The screenshot shows the 'Remote Host Ping' configuration page under the 'Discovery' tab. The 'Ping the remote host' toggle is turned on. The 'General Settings' section has 'Test the local Nessus host' checked and 'Use fast network discovery' unchecked. The 'Ping Methods' section has 'ARP' and 'TCP' checked, with 'Destination ports' set to 'built-in'. A note at the bottom states: 'Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are'.



❖ Launch the Scan

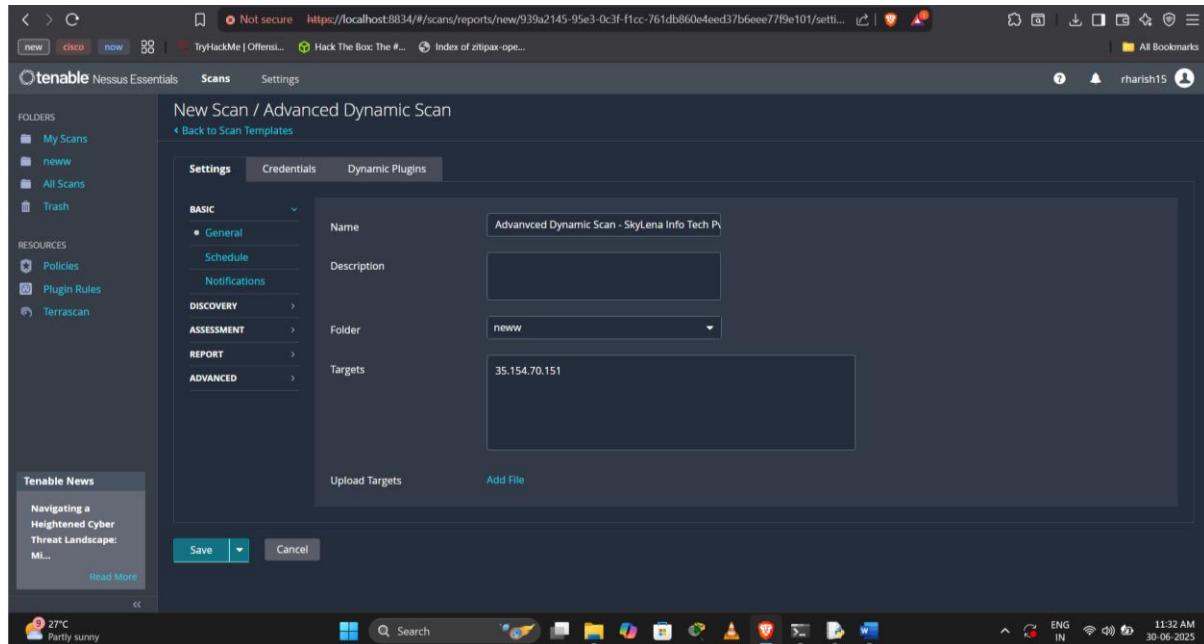
- Click “Save” and then “Launch”.

Advanced Dynamic Scan :

Configure the Scan

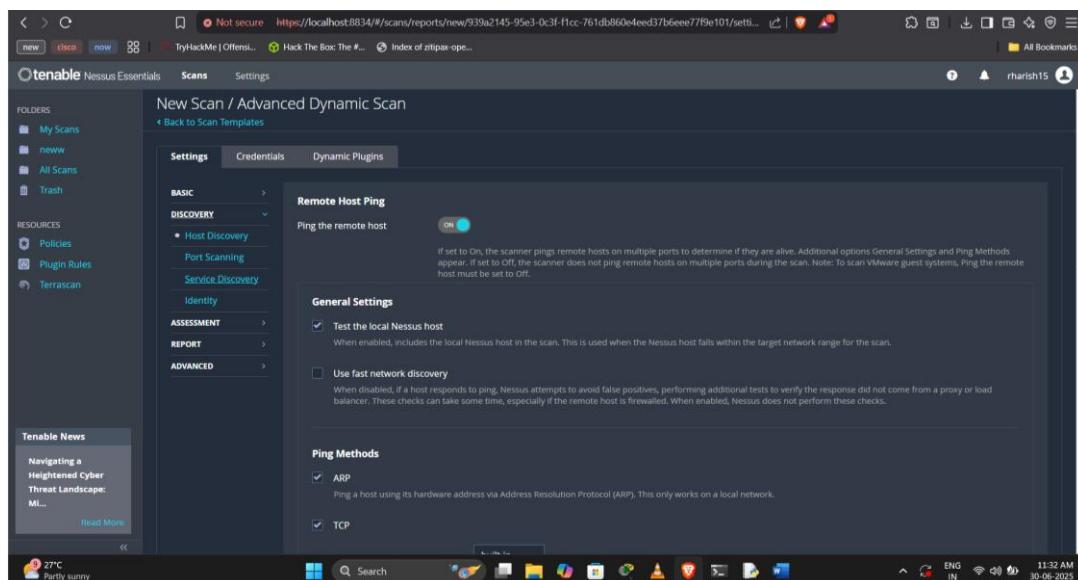
❖ Set:

- **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 :

The screenshots illustrate the configuration of dynamic plugins in Nessus. The first two panels show general plugin types: CVE, CPE, Exploit Database ID, ExploitHub, Exploitability Ease, Exploited By Malware, Exploited By Nessus, Hostname, and IAVA ID. The third panel shows specific exploit-related details: Malware, Metasploit Exploit Framework, Metasploit Name, Microsoft Bulletin, Microsoft KB, OSVDB ID, and Patch Publication Date. The fourth panel shows detailed vulnerability information: See Also, Solution, Synopsis, Target Hostname, Unsupported By Vendor, VPR Score, and Vulnerability Publication Date.

The screenshot shows the Nessus interface for creating a new scan. The 'Dynamic Plugins' tab is active, displaying a configuration for a plugin of type 'CVE' set to 'is equal to' 'CVE-YYYY-ID'. The 'Preview Plugins' button is visible below the configuration fields. The interface includes a sidebar with 'Folders' (My Scans, neww, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The bottom of the screen shows a Windows taskbar with various icons and system status.

EXAMPLE :

CVE-2017-5638 – Apache Struts RCE

CVE-2021-44228 – Log4Shell in Log4j

CVE-2022-22965 – Spring4Shell in Spring Core

New Scan / Advanced Dynamic Scan

[Back to Scan Templates](#)

Settings Credentials **Dynamic Plugins**

CVE	is equal to	CVE-2017-5638	X
CVE	is equal to	CVE-2021-44228	X
CVE	is equal to	CVE-2022-22965	X +

[Preview Plugins](#)

Save | Cancel

The screenshot shows a web-based interface for creating a new scan. At the top, it says 'New Scan / Advanced Dynamic Scan' and has a link to 'Back to Scan Templates'. Below that is a navigation bar with tabs: 'Settings', 'Credentials', and 'Dynamic Plugins', where 'Dynamic Plugins' is currently selected. Under the 'Dynamic Plugins' tab, there are three rows of configuration fields. Each row consists of a dropdown menu set to 'CVE', an operator dropdown set to 'is equal to', and an input field containing a specific CVE ID. To the right of each input field is a red 'X' icon. The first two rows have standard 'X' icons, while the third row has a red 'X' followed by a small '+' sign. At the bottom of the interface are two buttons: a teal 'Save' button and a grey 'Cancel' button.

❖ 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).

New Scan / Malware Scan

Settings Credentials Plugins

BASIC

- General
- Schedule
- Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name: Malware Scan - SkyLena Info Tech Pvt. Ltd.

Description:

Folder: neww

Targets: 35.154.70.151

Upload Targets Add File

Save Cancel

Provide the scan type :

New Scan / Malware Scan

Settings Credentials Plugins

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Scan Type: Host enumeration (include fragile hosts)

General Settings:

Always test the local Nessus host
Use fast network discovery

Ping hosts using:

TCP
ARP
ICMP (2 retries)

Scan all devices, including:

Printers
Novell Netware hosts

Save Cancel

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

New Scan / Malware Scan

Credentials

SSH

Authentication method: public key

Username: root

Private key: Add File

Private key passphrase:

Elevate privileges with: Nothing

Targets to prioritize credentials:

Global Credential Settings

New Scan / Web Application Tests

BASIC

Name: Web Application Tests - SkyLena Info Tech Pvt. Ltd.

Description:

Folder: neww

Targets: 35.154.70.15

Upload Targets Add File

Save Cancel

❖ Launch the Scan

- Click “Save” and then “Launch”.

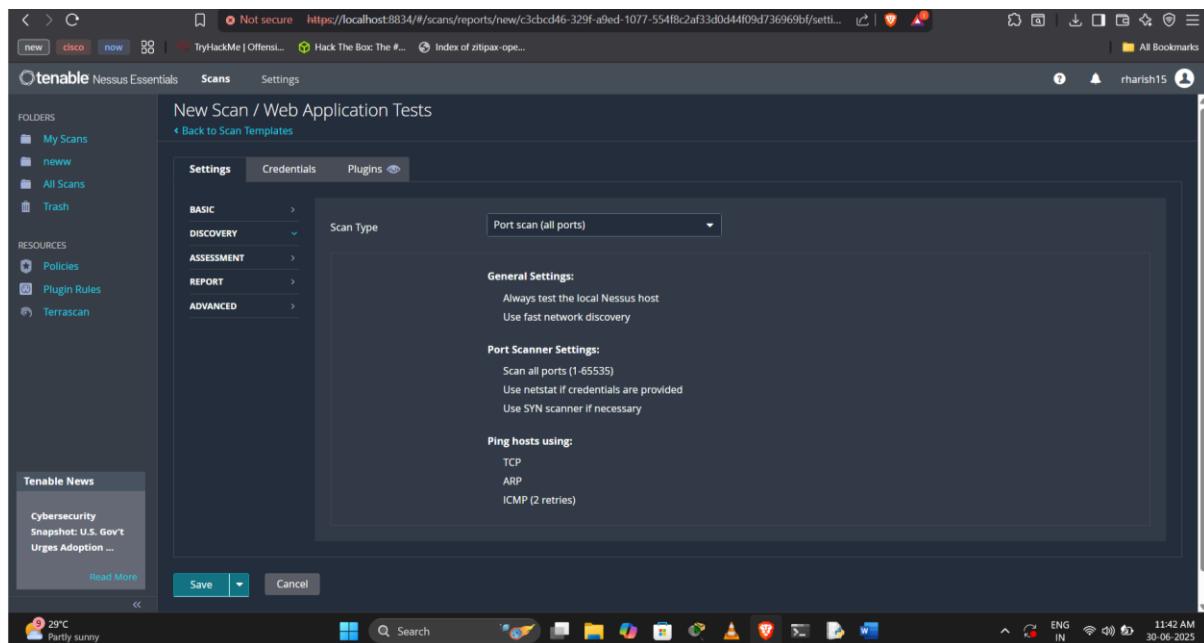
Web Application Tests Scan :

Configure the Scan

❖ Set:

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

❖ Provide the scan type :



❖ Launch the Scan

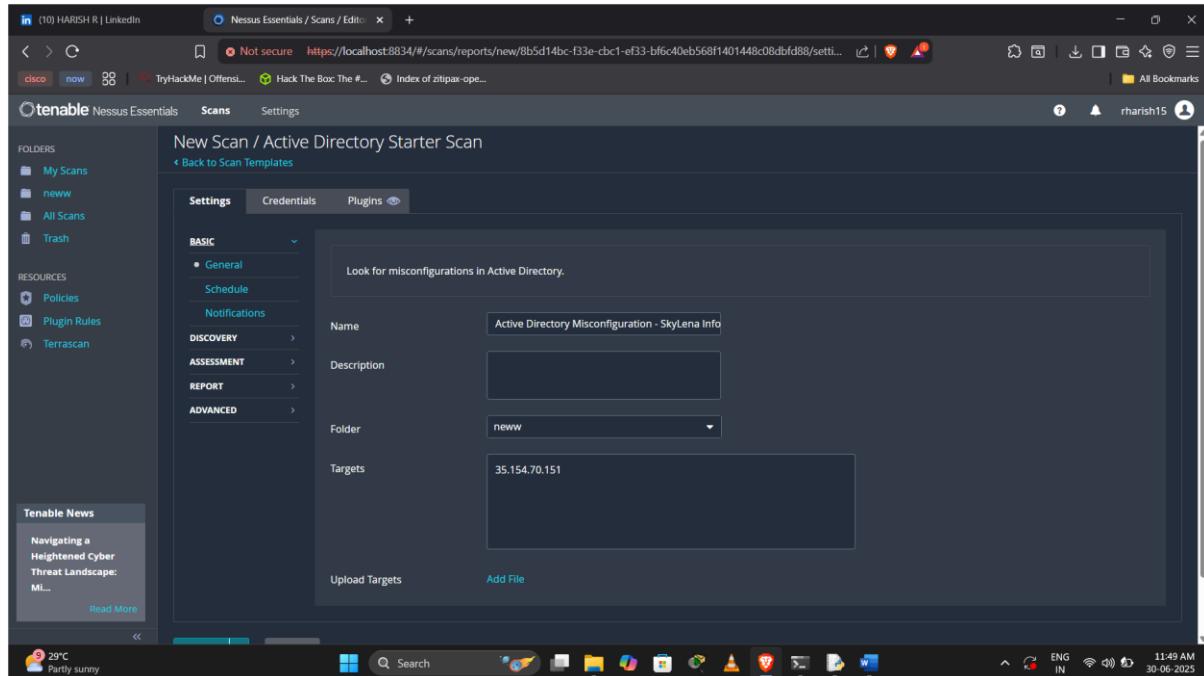
- Click “Save” and then “Launch”.

Active Directory starter Scan :

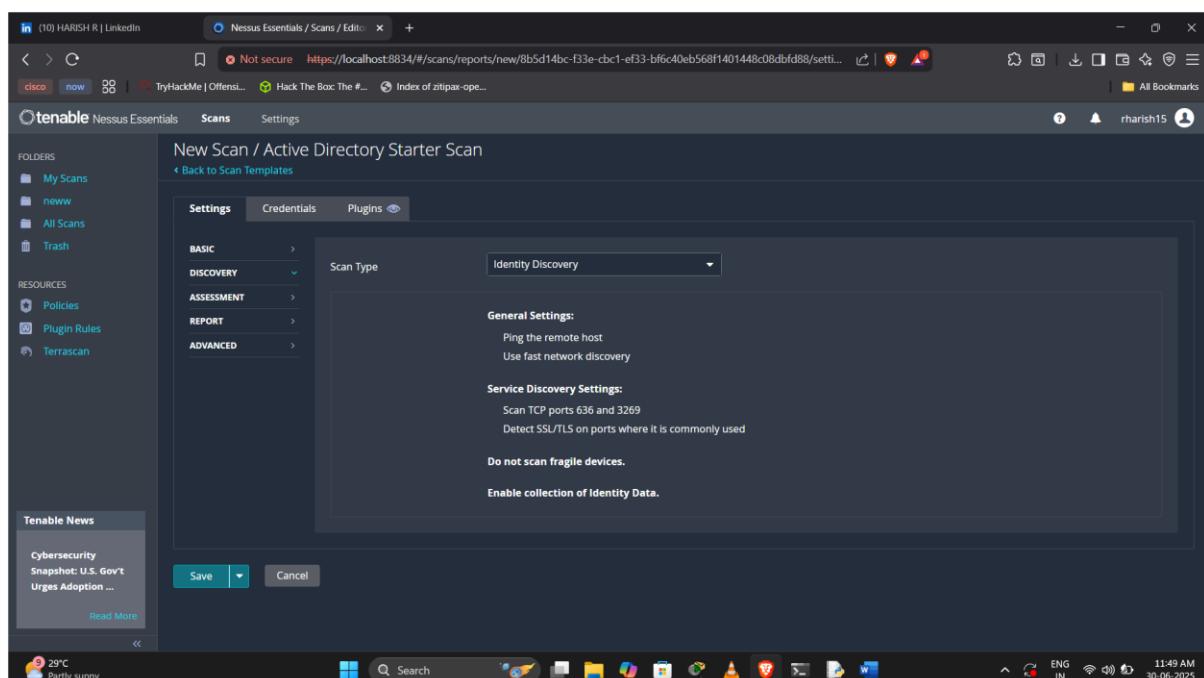
Configure the Scan

❖ Set:

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



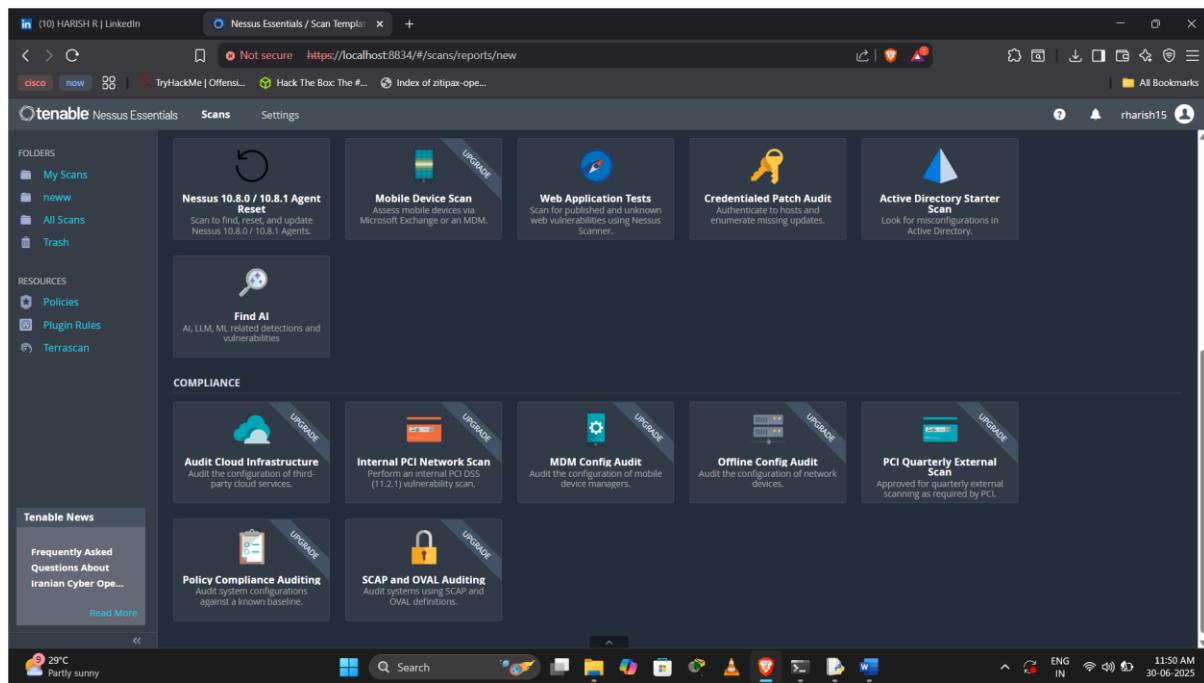
❖ Provide the scan type :



❖ Launch the Scan

- Click “Save” and then “Launch”.

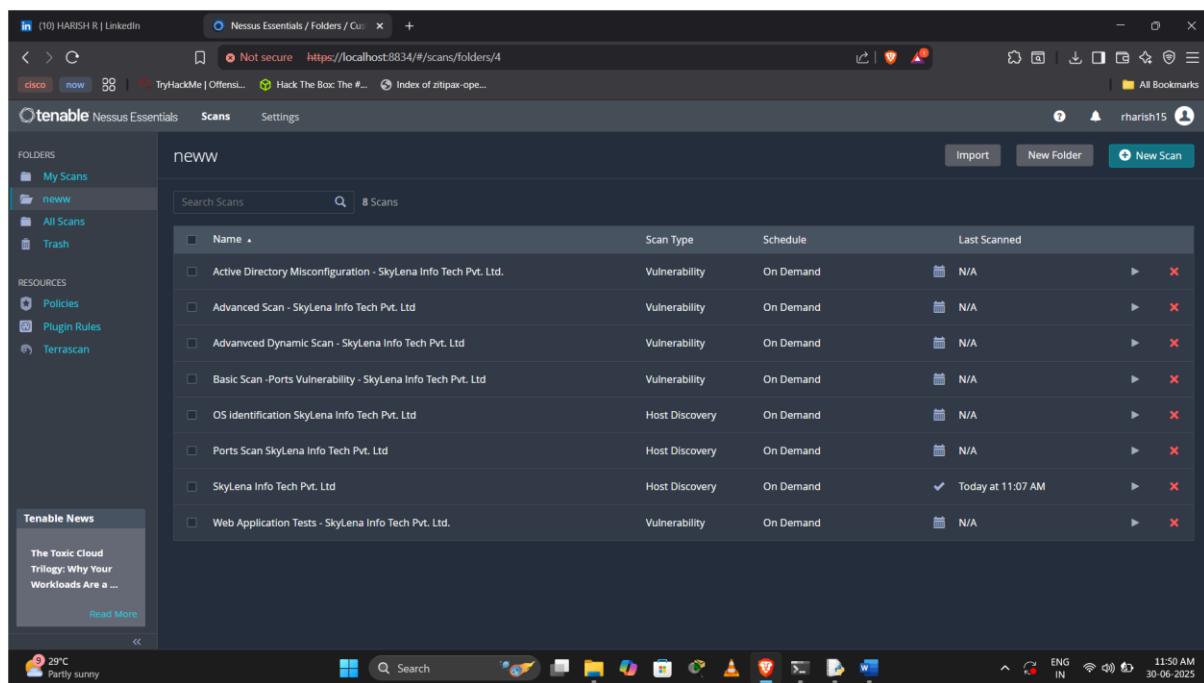
Perform variety of the scans needed :



The screenshot shows the Otenable Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, neww, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Terrascan). The main area displays several scan templates:

- Nessus 10.8.0 / 10.8.1 Agent Reset: Scan to find, detect, and update Nessus 10.8.0 / 10.8.1 Agents.
- Mobile Device Scan: 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.
- Find AI: AI, LLM, ML related detections and vulnerabilities.
- 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.
- SCAP and OVAL Auditing: Audit system configurations against a known baseline.
- Policy Compliance Auditing: Audit system configurations using SCAP and OVAL definitions.

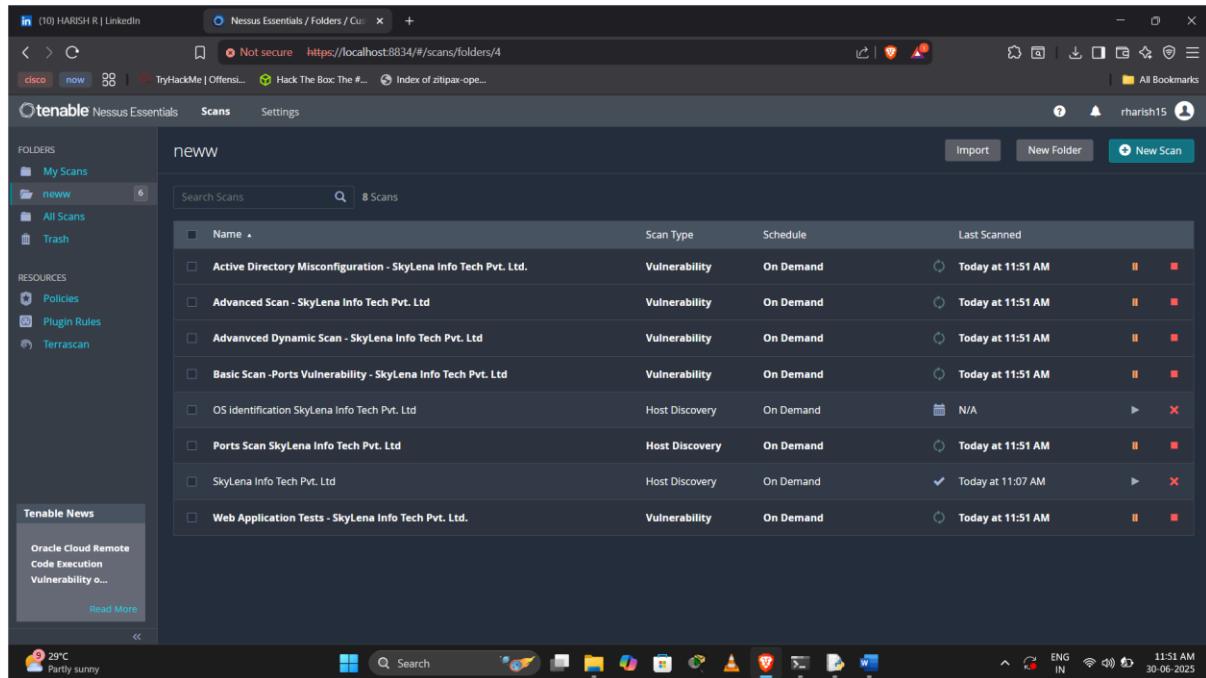
Wait for the launched scans to be completed :



The screenshot shows the 'neww' folder in the Nessus Essentials interface. The left sidebar shows 'My Scans' is selected. The main area displays a list of scheduled scans:

Name	Scan Type	Schedule	Last Scanned
Active Directory Misconfiguration - SkyLena Info Tech Pvt. Ltd.	Vulnerability	On Demand	N/A
Advanced Scan - SkyLena Info Tech Pvt. Ltd	Vulnerability	On Demand	N/A
Advanced Dynamic Scan - SkyLena Info Tech Pvt. Ltd	Vulnerability	On Demand	N/A
Basic Scan - Ports Vulnerability - SkyLena Info Tech Pvt. Ltd	Vulnerability	On Demand	N/A
OS Identification SkyLena Info Tech Pvt. Ltd	Host Discovery	On Demand	N/A
Ports Scan SkyLena Info Tech Pvt. Ltd	Host Discovery	On Demand	N/A
SkyLena Info Tech Pvt. Ltd	Host Discovery	On Demand	Today at 11:07 AM
Web Application Tests - SkyLena Info Tech Pvt. Ltd.	Vulnerability	On Demand	N/A

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

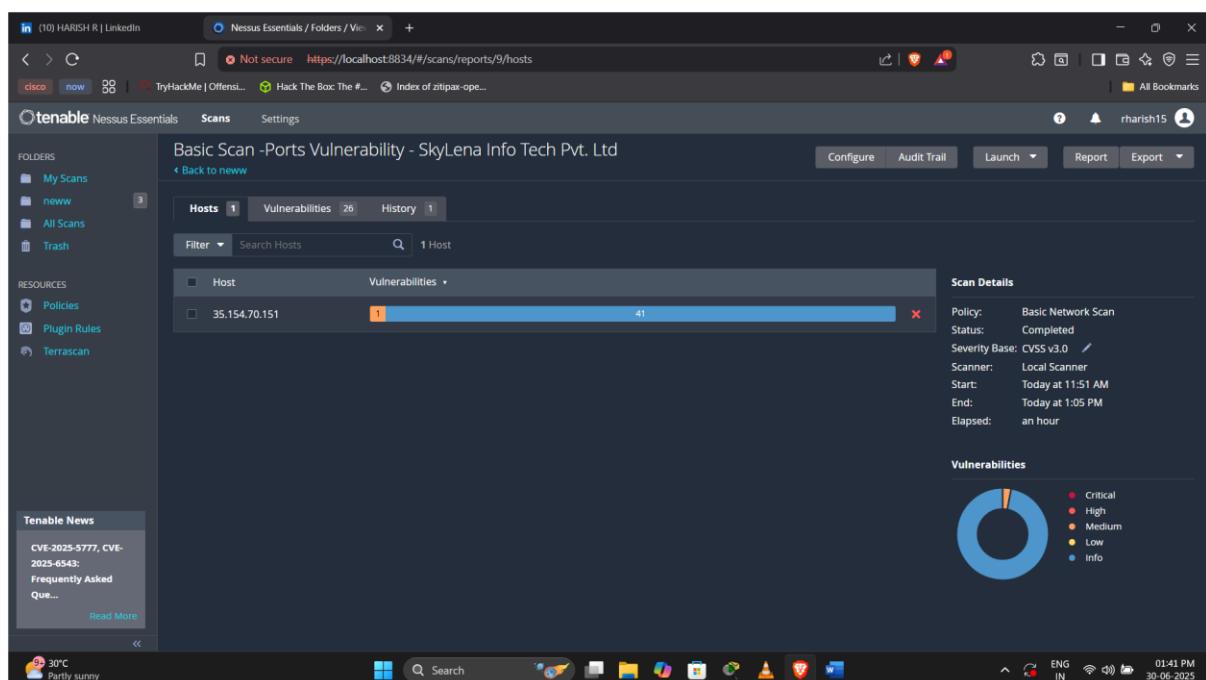


The screenshot shows the Okteto Nessus Essentials web interface. The left sidebar has sections for FOLDERS (My Scans, neww, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (Oracle Cloud Remote code Execution Vulnerability...). The main area displays a table of 8 scans under the 'neww' folder. The columns are Name, Scan Type, Schedule, and Last Scanned. The scans listed are:

Name	Scan Type	Schedule	Last Scanned
Active Directory Misconfiguration - SkyLena Info Tech Pvt. Ltd.	Vulnerability	On Demand	Today at 11:51 AM
Advanced Scan - SkyLena Info Tech Pvt. Ltd	Vulnerability	On Demand	Today at 11:51 AM
Advanvced Dynamic Scan - SkyLena Info Tech Pvt. Ltd	Vulnerability	On Demand	Today at 11:51 AM
Basic Scan -Ports Vulnerability - SkyLena Info Tech Pvt. Ltd	Vulnerability	On Demand	Today at 11:51 AM
OS Identification SkyLena Info Tech Pvt. Ltd	Host Discovery	On Demand	N/A
Ports Scan SkyLena Info Tech Pvt. Ltd	Host Discovery	On Demand	Today at 11:51 AM
SkyLena Info Tech Pvt. Ltd	Host Discovery	On Demand	Today at 11:07 AM
Web Application Tests - SkyLena Info Tech Pvt. Ltd.	Vulnerability	On Demand	Today at 11:51 AM

DOCUMENTATION :

Result :



The screenshot shows the Okteto Nessus Essentials web interface. The left sidebar has sections for FOLDERS (My Scans, neww, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and Tenable News (CVE-2025-5777, CVE-2025-6543: Frequently Asked Que...). The main area displays the results of a scan titled "Basic Scan -Ports Vulnerability - SkyLena Info Tech Pvt. Ltd". The interface includes tabs for Hosts (1), Vulnerabilities (26), and History (1). The Hosts tab shows one host, 35.154.70.151, with 41 vulnerabilities. The Vulnerabilities tab shows a pie chart of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue). The Scan Details panel on the right provides the following information:

Policy	Basic Network Scan
Status	Completed
Severity Base	CVSS v3.0
Scanner	Local Scanner
Start	Today at 11:51 AM
End	Today at 1:05 PM
Elapsed	an hour

- ❖ 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 :

The screenshot shows a web browser window displaying a Nessus scan report for IP 35.154.70.151. The report is titled "Basic Scan - Ports Vulnerability". The main content area shows a summary bar with the following counts: Critical (0), High (0), Medium (1), Low (0), and Info (33). Below this is a table of vulnerabilities:

Severity	CVSS	Nmap	VPR Score	EPPS Score	Plugin	Name
Critical	6.5	-	-	143960	HSTS Missing From HTTPS Server (RFC 6797)	
High	N/A	-	-	40180	Additional DNS Hostnames	
Medium	N/A	-	-	35030	Background Security Patch Detection (BSP)	
Low	N/A	-	-	45590	Common Platform Enumeration (CPE)	
Info	N/A	-	-	54815	Device Type	
Info	N/A	-	-	84502	HSTS Missing From HTTPS Server	
Info	N/A	-	-	10107	HTTP Server Type and Version	
Info	N/A	-	-	12003	Host Fully Qualified Domain Name (FQDN) Resolution	
Info	N/A	-	-	24200	HyperText Transfer Protocol (HTTP) Information	
Info	N/A	-	-	11219	Nessus SYN scanner	
Info	N/A	-	-	19506	Nessus Scan Information	
Info	N/A	-	-	209004	OS Fingerprints Detected	
Info	N/A	-	-	11936	OS Identification	
Info	N/A	-	-	117986	OS Security Patch Assessment Not Available	
Info	N/A	-	-	181410	OpenSSH Detection	
Info	N/A	-	-	10180	Ping the remote host	
Info	N/A	-	-	70607	SSH Algorithms and Languages Supported	
Info	N/A	-	-	10081	SSH Protocol Versions Supported	
Info	N/A	-	-	15938	SSH SHA-1 HMAC Algorithms Enabled	

Reports :

https://drive.google.com/drive/u/5/folders/1vSRSNlFFbH0_mag3Xi0XWaDy558fQLID

The screenshot shows a Windows File Explorer window with the title "scan reports". The folder contains the following files:

- Active Directory Misconfiguration - Skylena Info Tech Pvt Ltd.pdf
- Advanced Scan - Skylena Info Tech Pvt Ltd.pdf
- Advanced Dynamic Scan - Skylena Info Tech Pvt Ltd.pdf
- Basic Scan - Ports Vulnerability - Skylena Info Tech Pvt Ltd.pdf
- Host Discovery - Skylena Info Tech Pvt Ltd.pdf
- OS identification Skylena Info Tech Pvt Ltd.pdf
- Ports Scan Skylena Info Tech Pvt Ltd.pdf
- Web Application Tests - Skylena Info Tech Pvt Ltd.pdf