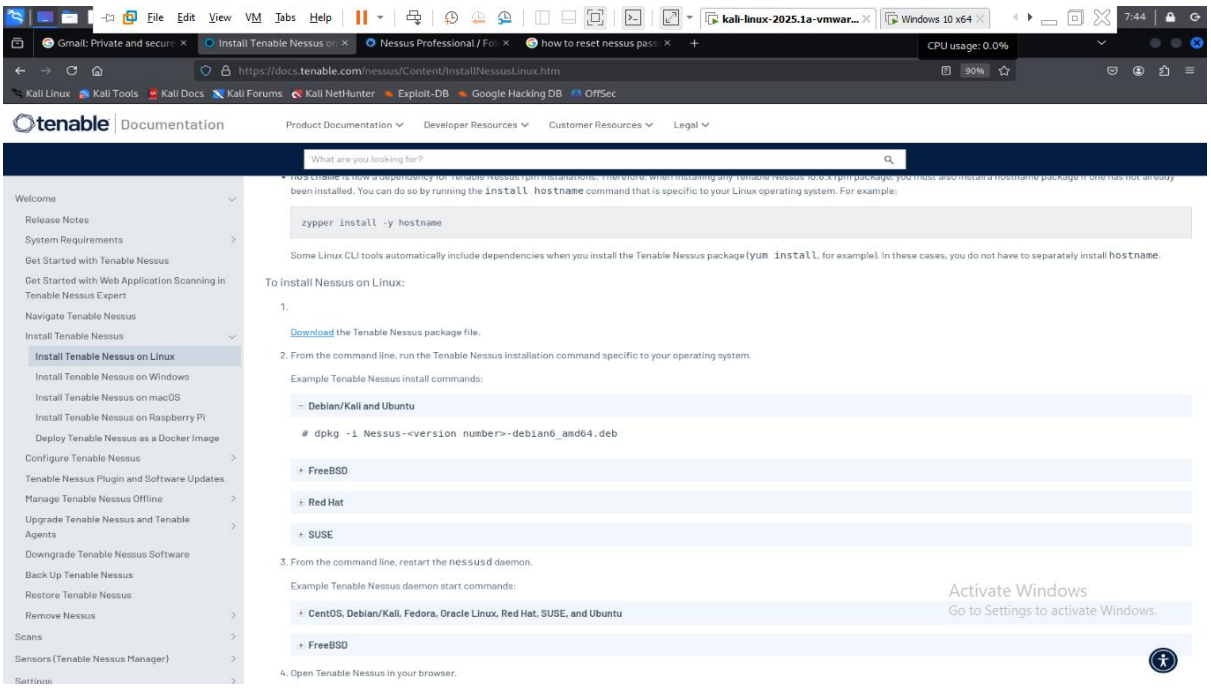
In this demonstration, we'll be observing the process of Vulnerability Scanning , Results and process of obtaining the results of scan

1. Installing Nessus

1.1 Downloading Nessus




Select the platform i.e. Operating system and download  Nessus from the link https://www.tenable.com/downloads/nessus?loginAttempted=true

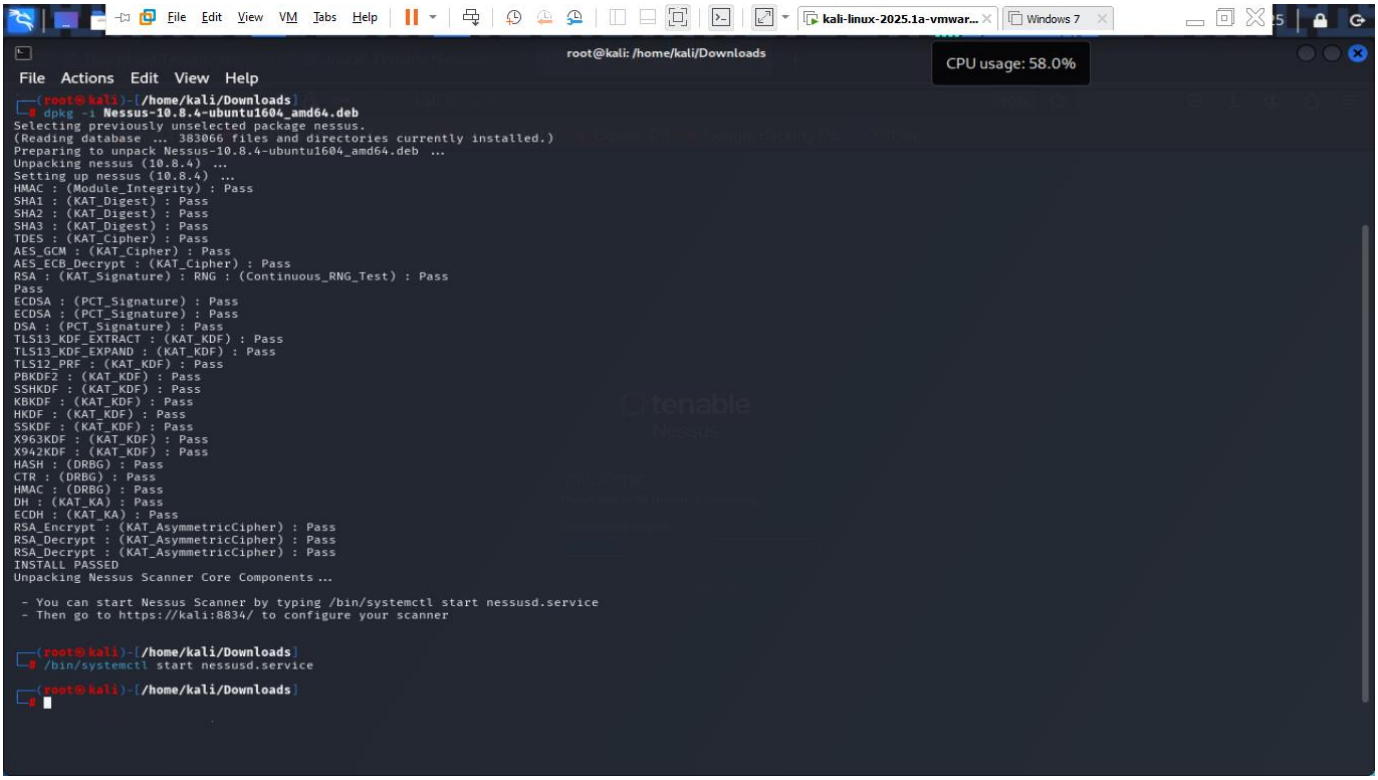
In this case, Nessus is being downloaded for Kali Linux and version 10.8.4 is selected.

The installation process is started by locating into the directory where Nessus is downloaded and then using the command

- dpkg -i Nessus-<version number>-debian6_amd64.deb

here, the command would be customized to

- dpkg -i Nessus-10.8.4-debian6_amd64.deb

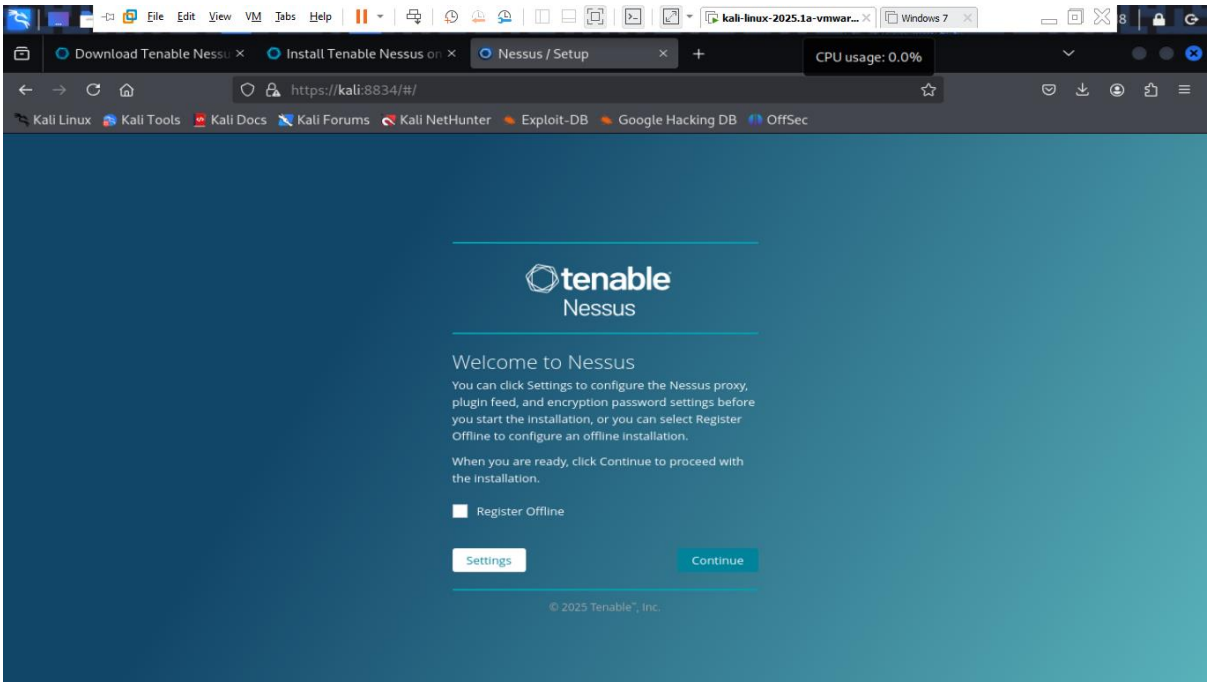



After executing the command, to start the service another command is executed

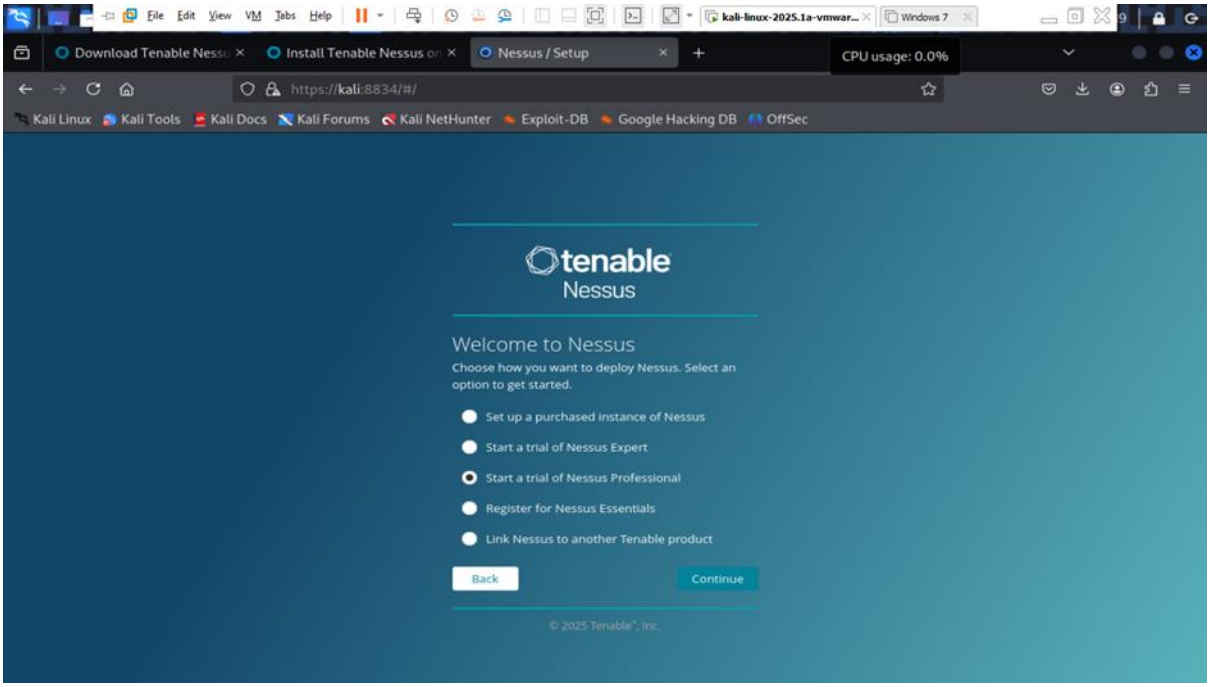
- /bin/systemctl start nessusd.service

After this starts the registration process of which screenshots are attached below

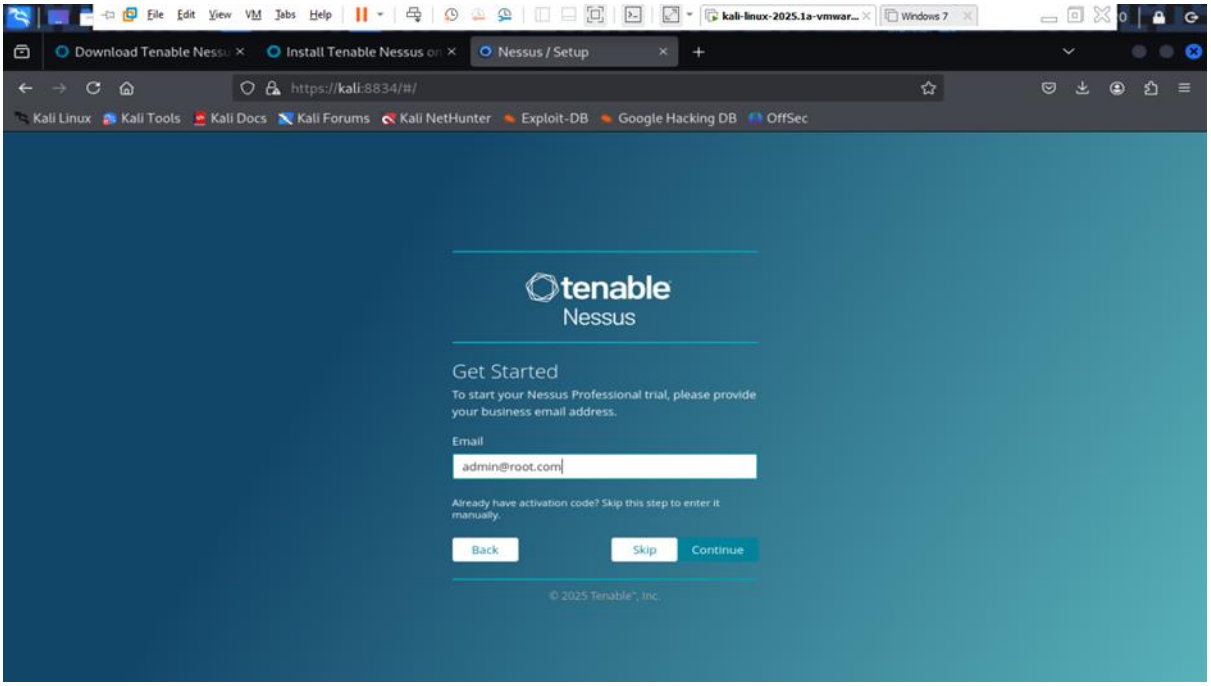
- The process starts by registering offline



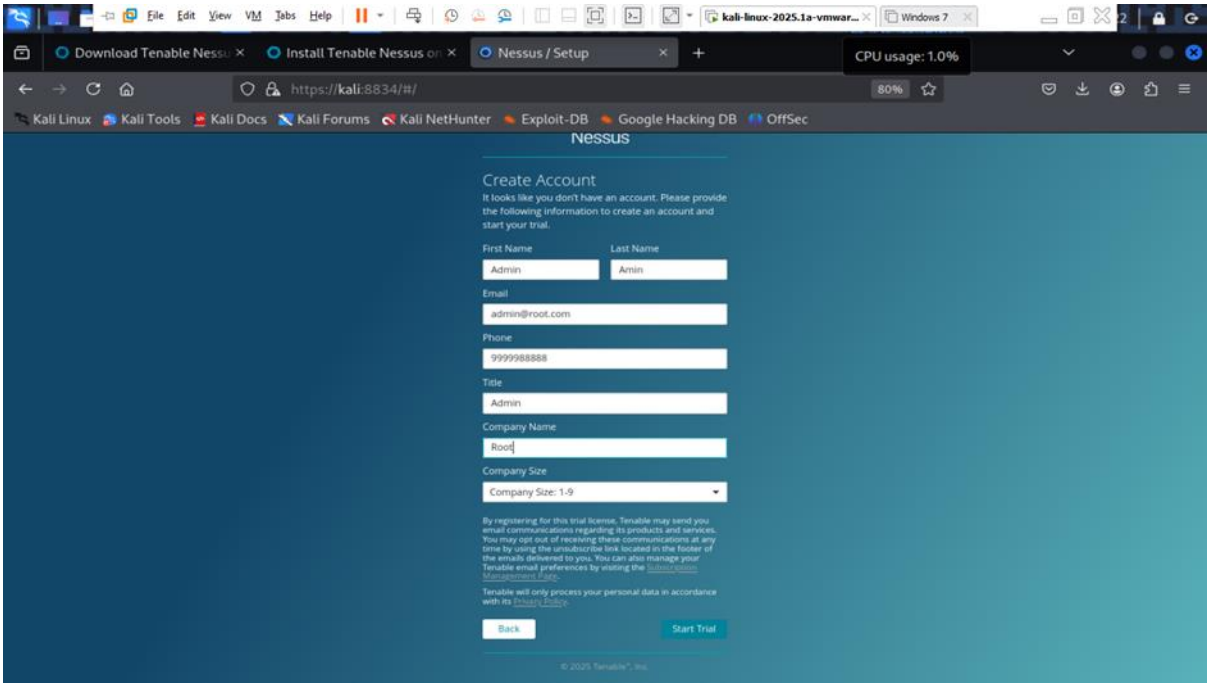
- Now, the option of " start a trial of Nessus Professional"



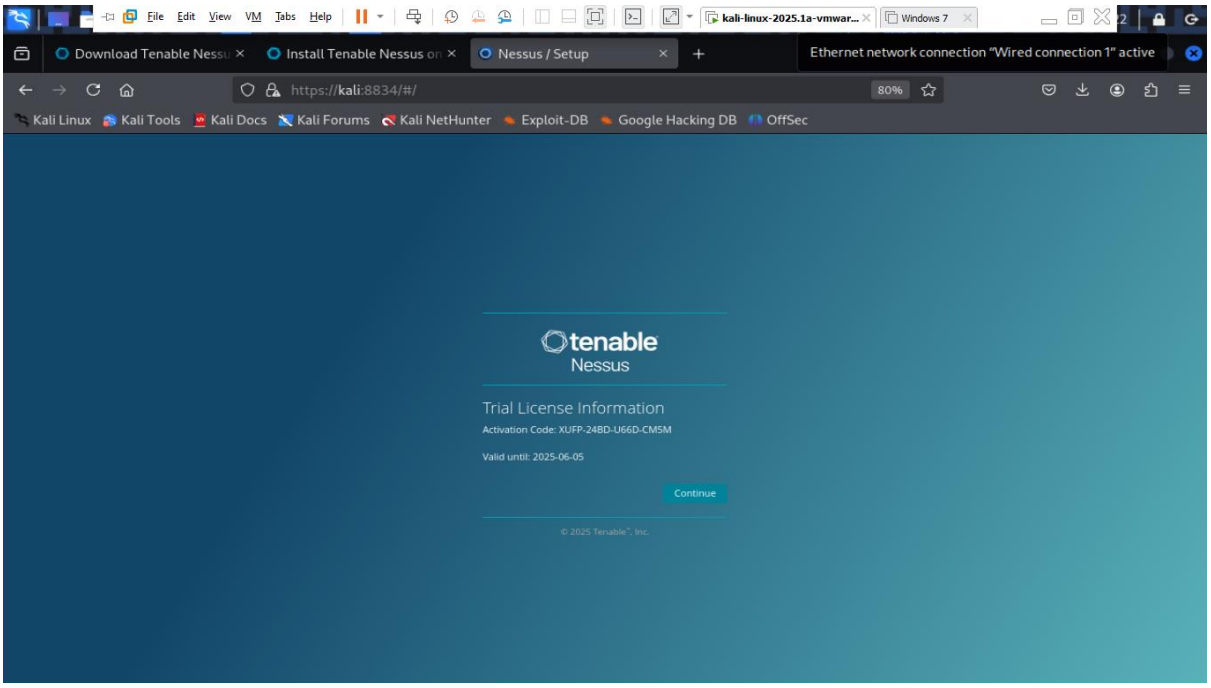

- To get started, a professional email ID is required, for which we use admin@root.com



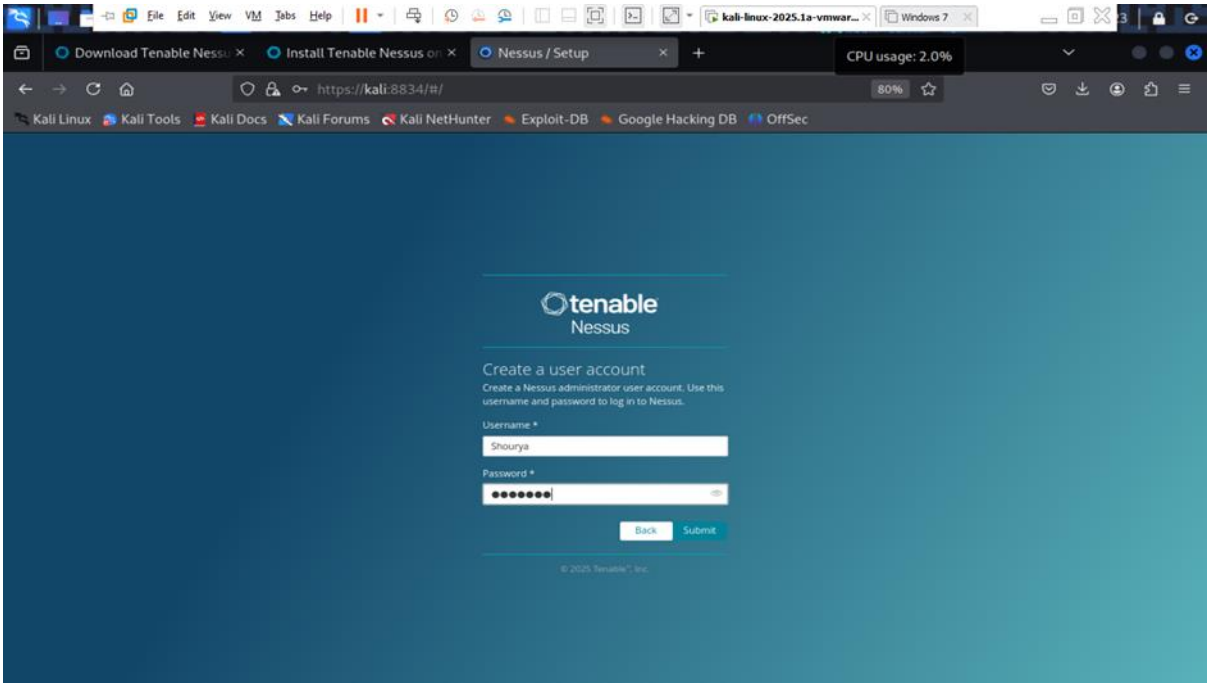
- In this section basic details are filled up and proceeded further



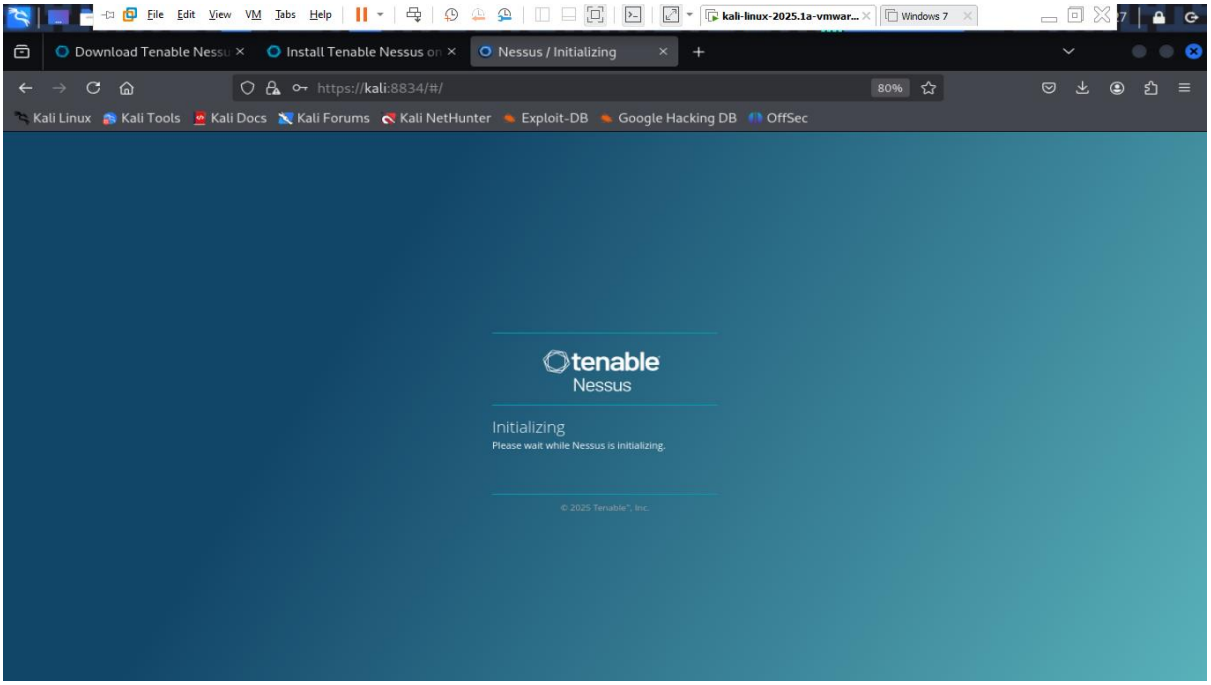

- Now the Nessus is active for use



- Now a username and password is setup to login into the account

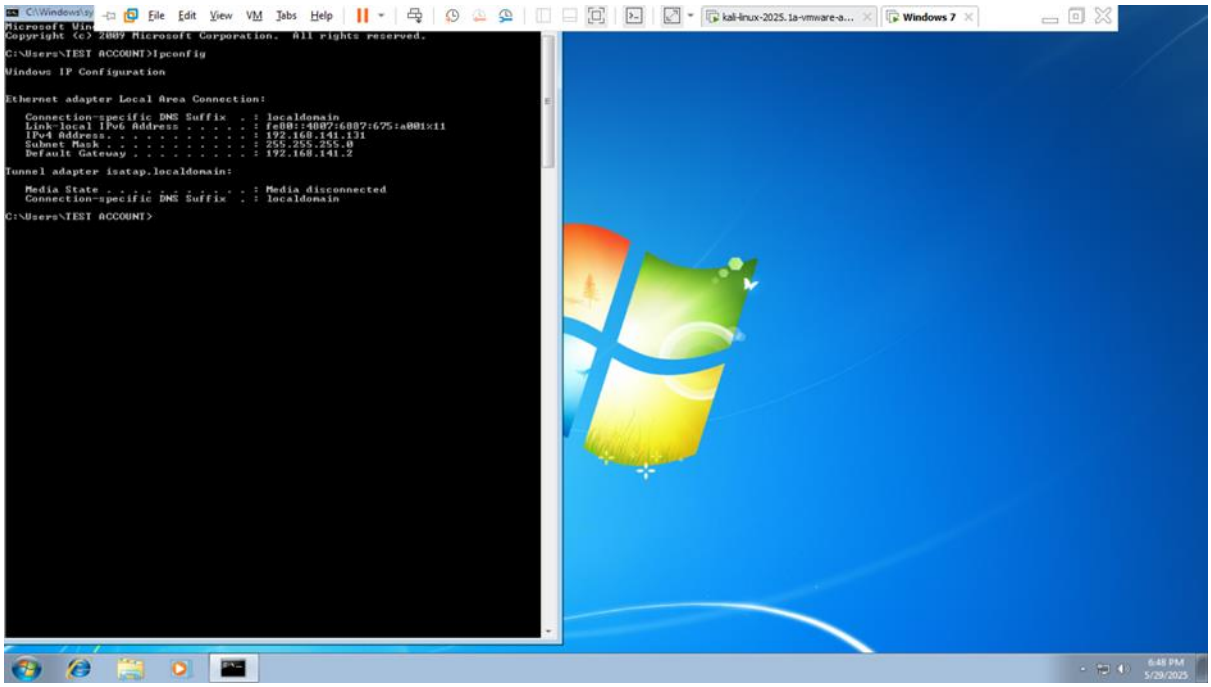



- After setup and registration, this is the initializing screen after login



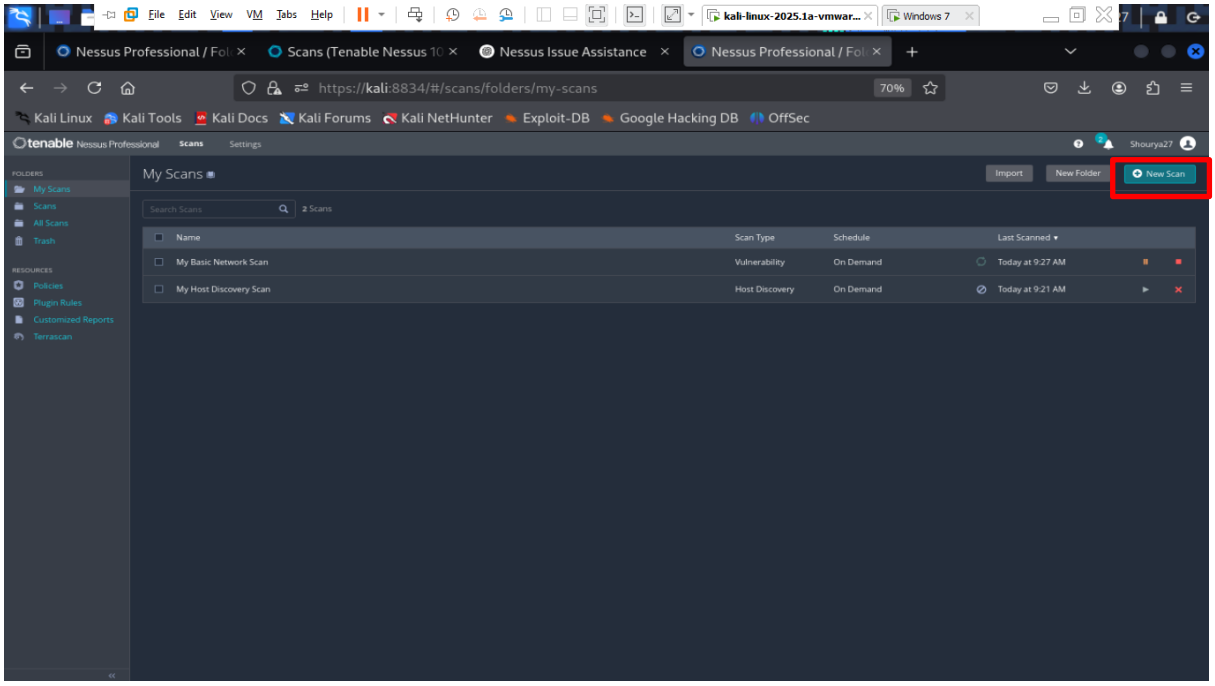
2. Targeting a localhost machine

- In this step we target a windows machine in VMware, where a freshly installed windows is used with few vulnerabilities are made up
- The IP Address of the Windows machine used is : 192.168. 141.131

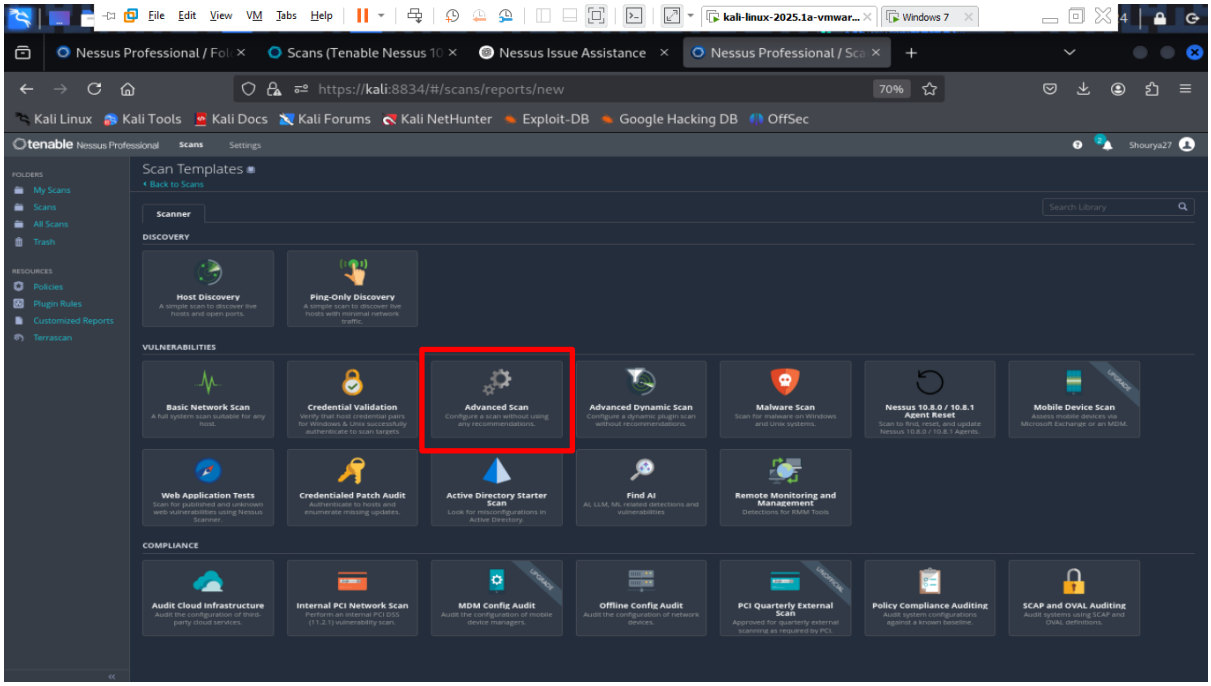



3. Starting a full Vulnerability Scan

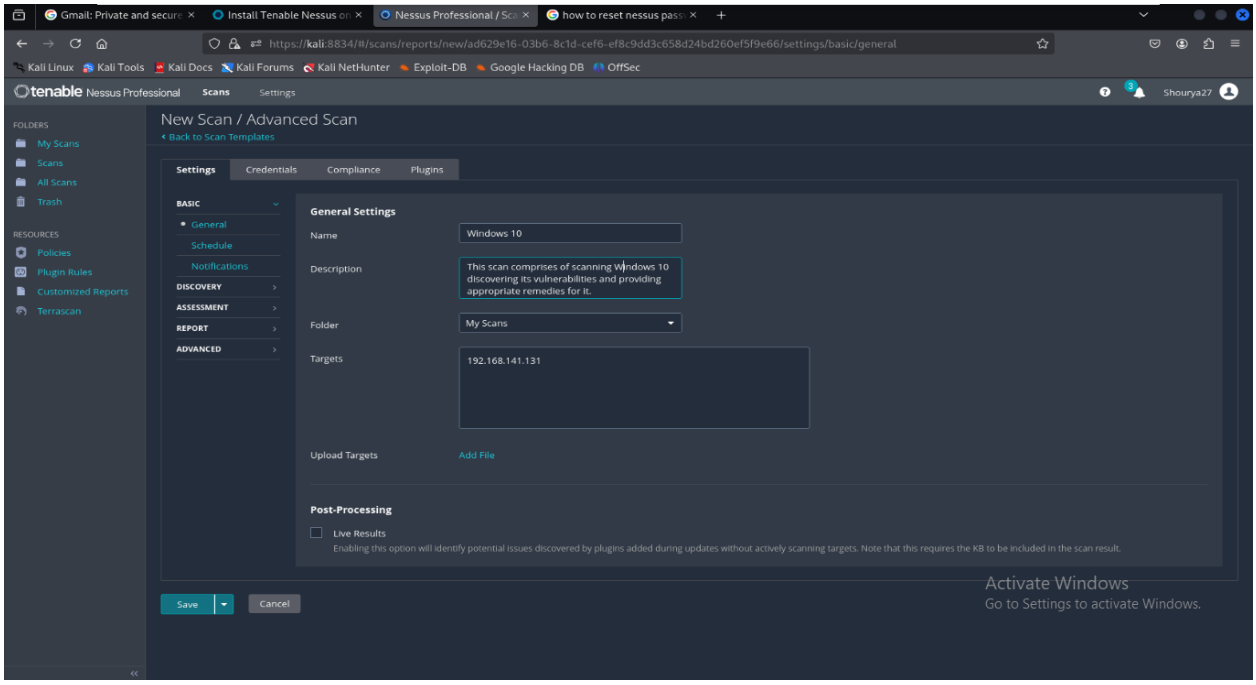
- To start a full vulnerability scan, we navigate to Nessus scan page and select New scan



- A new page opens up selecting the type of scan to be performed, where we select Advanced Scan




- After which details about the target host is entered and name of the scan is entered




5. Reviewing the Report for vulnerabilities and severity
   - The scan report for target 192.168.141.131 reports  311 vulnerabilities
   - In this report, the vulnerabilities is classified into :-

   - **Critical**: 37
   - **High**: 73
   - **Medium**: 27
   - **Low**: 1
   - **Info**: 173

6. Documenting the most critical vulnerabilities

- In this step, the most critical vulnerabilities are studied

These pose the highest risk and should be prioritized at the earliest.

- Outdated Windows Security Updates
  Multiple critical patches are missing from as early as 2020 to mid-2024, such as:
  - KB4551853, KB5003171, KB5004244, KB5005030 (2020–2021)
  - KB5039217 (June 2024)
- Apache Log4j vulnerabilities:
  - CVE-2021-4104: Remote Code Execution (RCE)
  - Apache Log4j SEoL (<= 1.x) – End-of-life components still present
- Adobe Flash Player (<= 32.0.0.371) – High CVSS 9.8
- Microsoft Message Queuing (QueueJumper): CVE-2023-21554 – RCE
- Mozilla Firefox < 128.0 – Known exploitable versions
- Oracle Java (April 2024 CPU) – Includes unpatched RCE issues

7. Providing appropriate remedy to critical vulnerabilities

7.1. Missing Windows Security Updates (Multiple KBs)

- Remedy:
  - Use Windows Update or WSUS/SCCM to install the latest cumulative updates for:
    - Windows 10 Version 1809
    - Windows Server 2019
  - Or download and install updates manually from Microsoft Update Catalogue
- Tools: Windows Update, WSUS, SCCM

7.2. Apache Log4j 1.x / SEoL Vulnerabilities

- Remedy:
  - Identify Java applications using Log4j 1.x.
  - Replace Log4j 1.x with Log4j 2.17.1+.
  - Remove unused JAR files and restart the services.
- Tools: Dependency scanners (e.g., OWASP Dependency-Check, Syft), file search tools

7.3. Adobe Flash Player (End-of-Life)

- Fix Complexity: □ Very Easy
- Remedy:
- Uninstall Flash via:
  - Control Panel > Programs > Uninstall a Program
  - Or run official Adobe Flash uninstaller
- Tools: Flash Uninstaller, Windows Control Panel

7.4. Microsoft Message Queuing (QueueJumper RCE - CVE-2023-21554)

- Remedy:
    - If MSMQ is not required:

      Disable it via:

      ruby
    - CopyEdit
    - dism /Online /Disable-Feature /FeatureName:MSMQ-Server
- Tools: DISM, Windows Update

7.5. Mozilla Firefox < 128.0

- Remedy:
    - Download and install the latest version of Firefox from mozilla.org
    - Alternatively, update via group policy or enterprise deployment tools.
- Tools: Browser installer, software deployment tools

7.6. Oracle Java (April 2024 CPU)

- Remedy:
    - Identify Java versions in use:
    - Uninstall old versions and install latest Java LTS version (e.g., Java 17 or 21).
    - Download from Oracle JDK website or use OpenJDK.
- Tools used : Java uninstallers, scriptable installers