

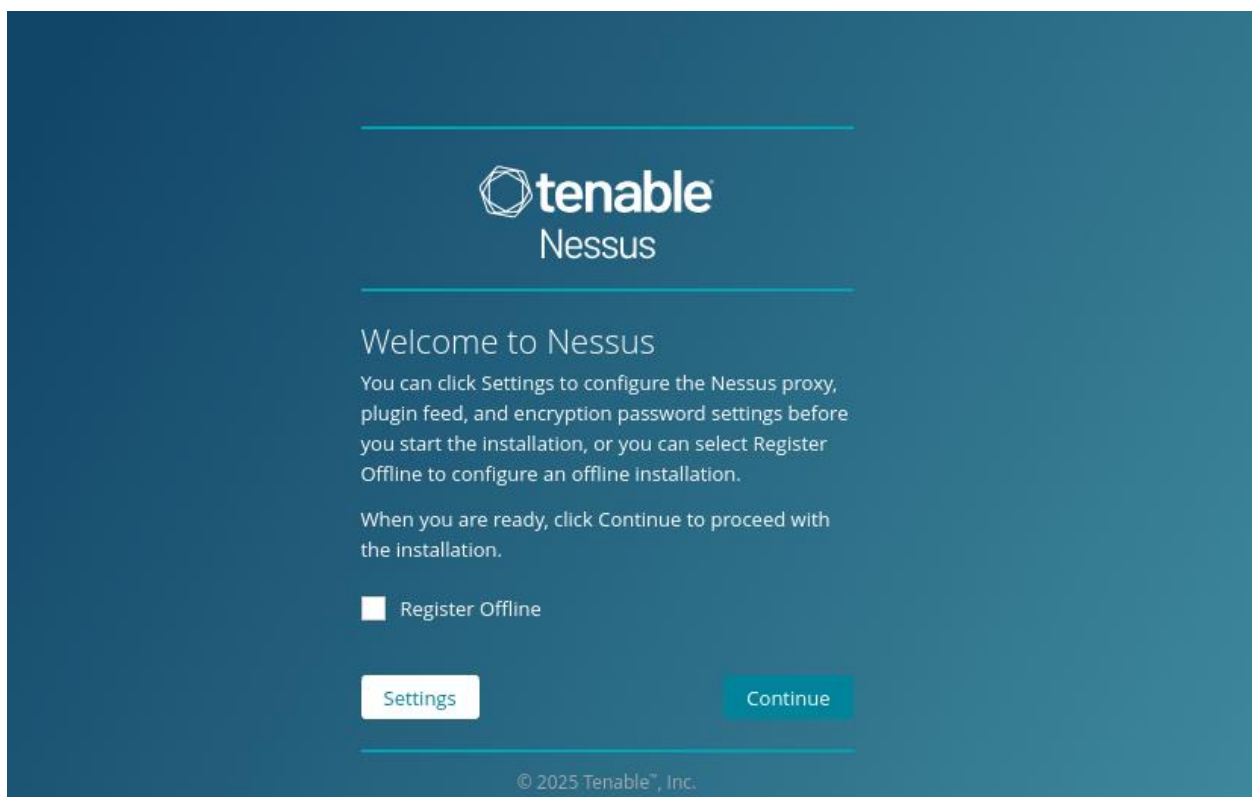
Nessus Installation on Kali Linux:

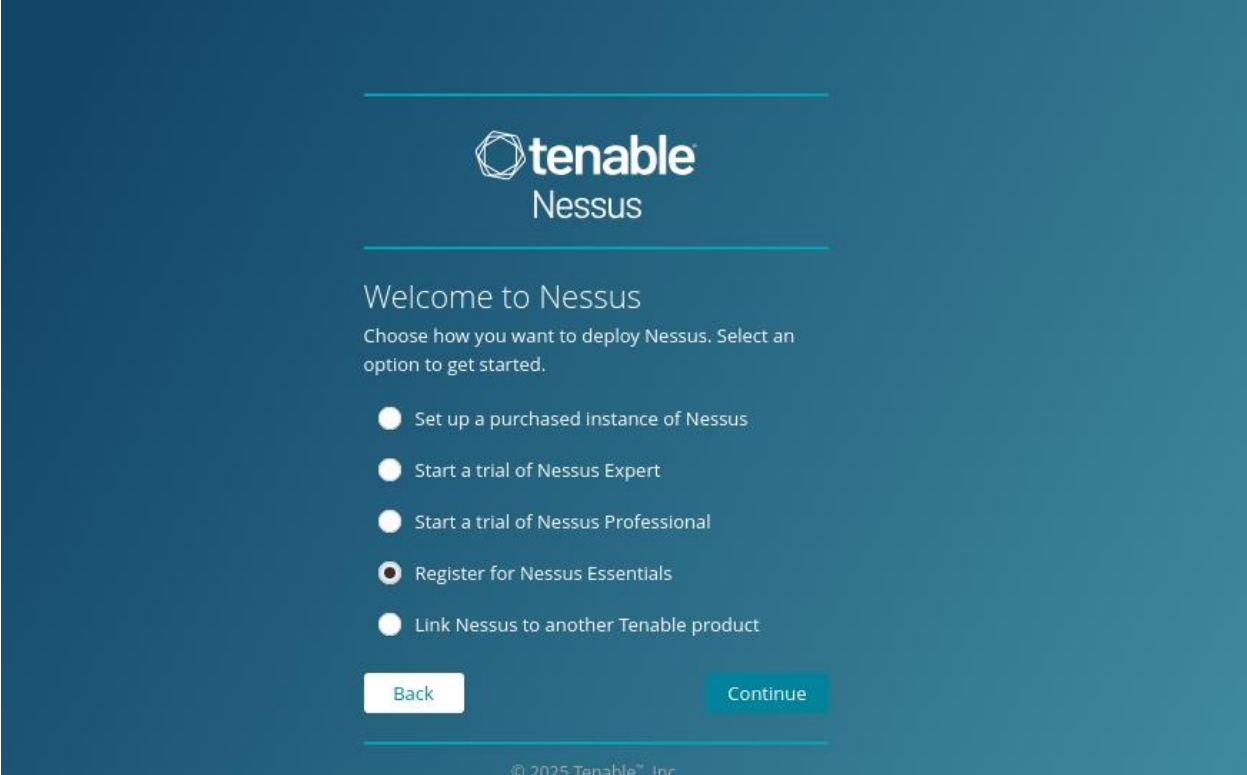
Once you downloaded the file you will need to navigate to the directory where it was saved. Use `dpkg` to install Nessus. `Dpkg` is a medium-level command line tool to install, build, remove, and manage Debian packages. Running `dpkg` with the `-i` flag will install the specified package-file. This command needs to be run with `sudo` privileges. The format for this would be:
`sudo dpkg -i <name of Nessus package you downloaded>`

After Nessus is unpacked it should provide you instructions for starting up the service and where to navigate in the browser in order to configure the scanner. The command given to me to start up the service is `/bin/systemctl start nessusd.service`. Also, start the services on boot using the command: `sudo systemctl enable nessusd`. The address for the browser should be <https://localhost:8834/>

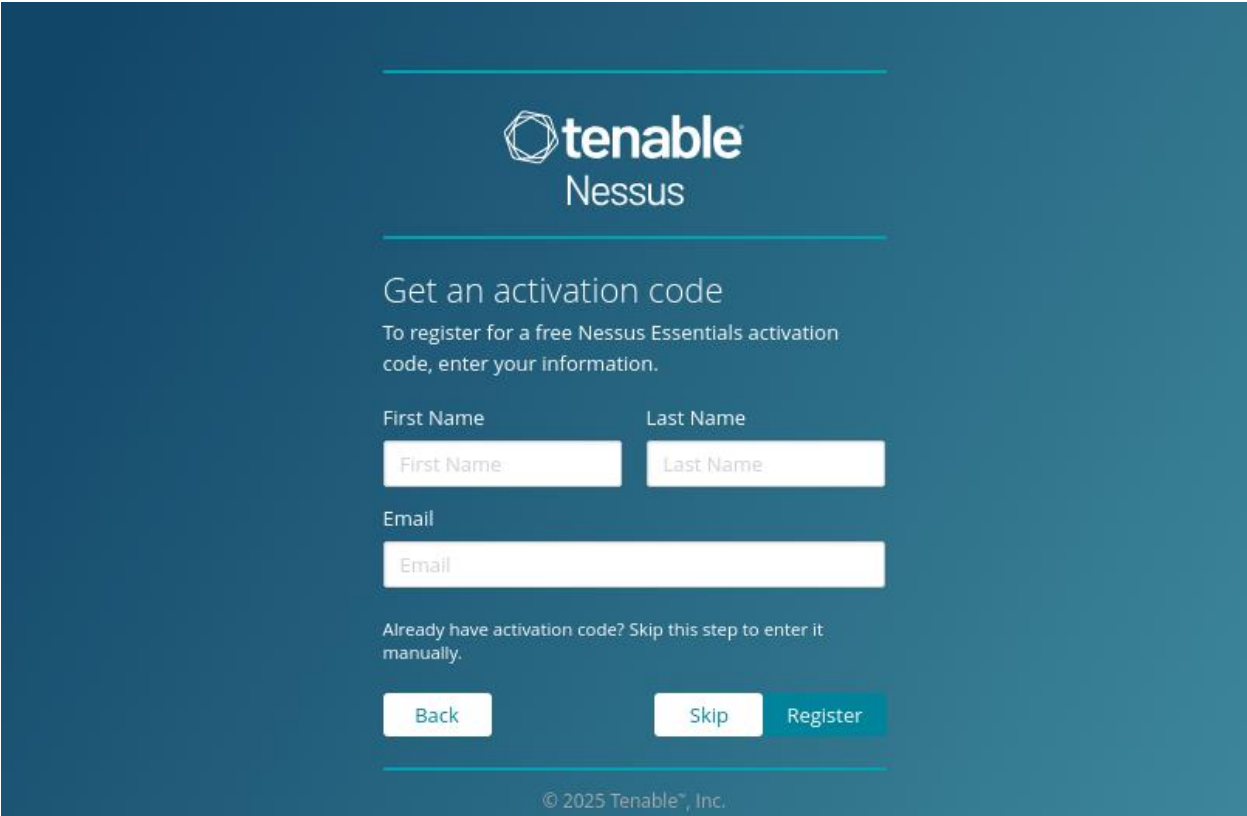
Starting Nessus:

When navigating to the site you may get a warning about the SSL certificate. You can ignore this by clicking Advanced and then Accept the Risk and Continue. On the next screen select Nessus Essentials and then `continue`.



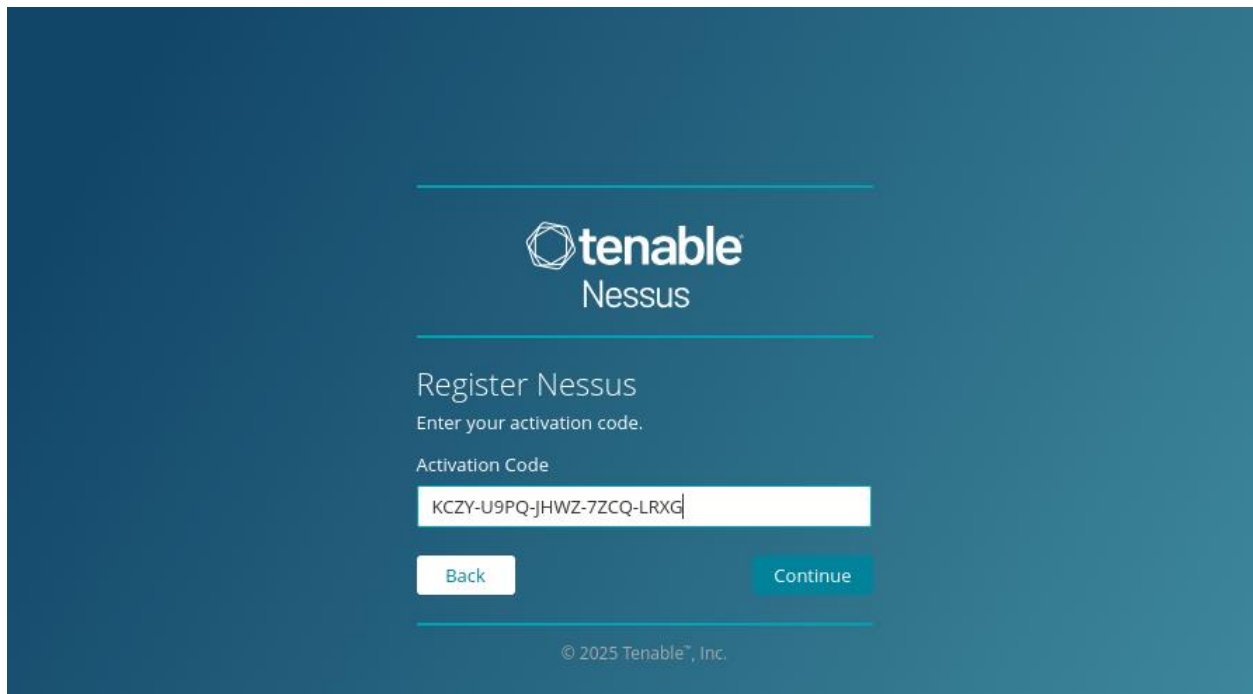


If you have already registered and requested an activation code, you can click **Skip**. However, if you haven't you can request an activation code here.

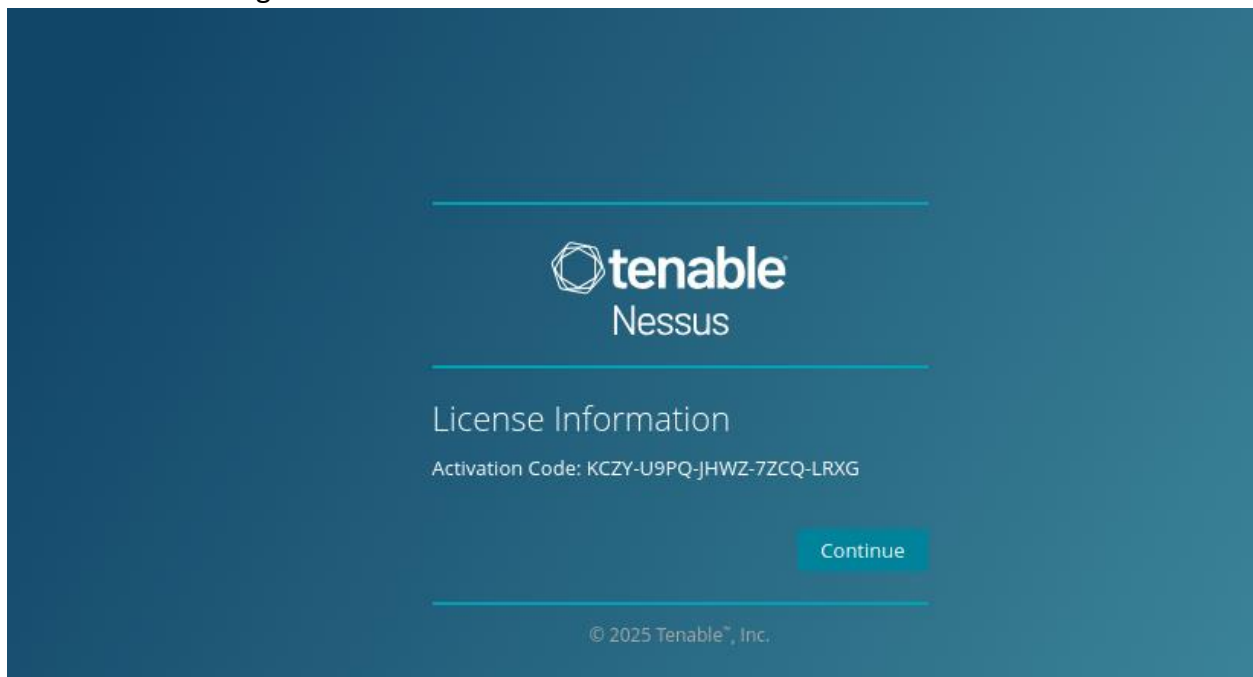


Enter the activation code you received and click **Continue**.

Your activation code for Nessus Essentials is: YHH2-N5LN-E35D-JK4U-VSDG



Click on **Continue** again

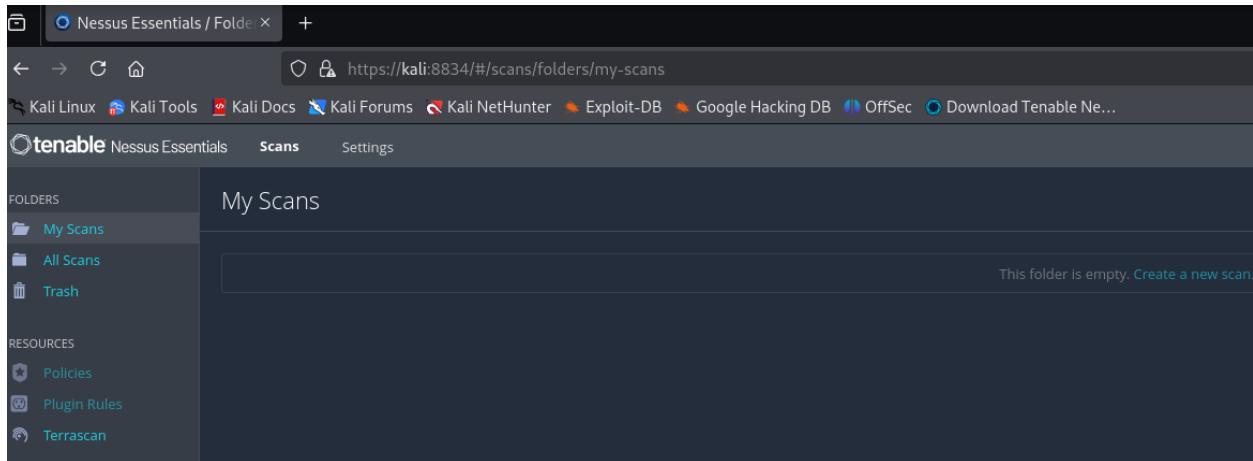


Create your Username and Password and click **Submit**. [Admin/Admin@12345](#)

Next, you will be greeted by Nessus compiling plugins that will be used for scanning. This may take a while depending on various factors.

Main Screen:

When you load in for the first time it will ask you if you want to do a host discovery and what IPv4 CIDR ranges you want to scan.



Scan Templates

[Back to Scans](#)

Scanner

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.
- Find AI**
AI, LLM, ML related detections and vulnerabilities.