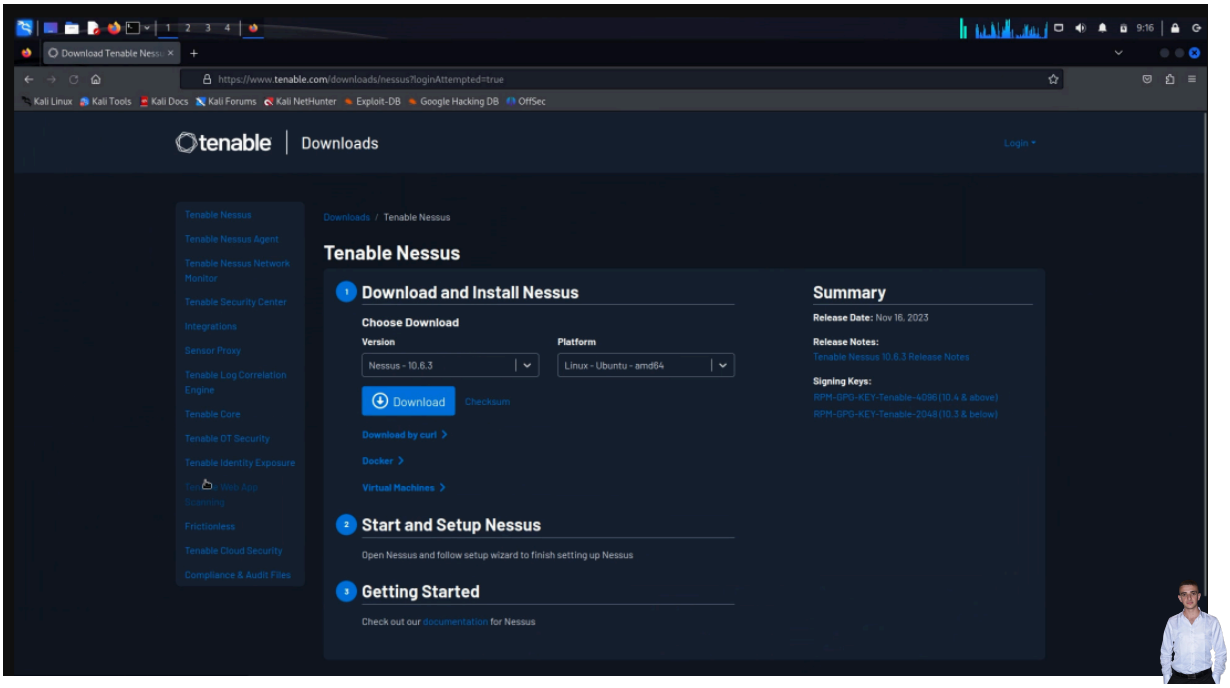
Nessus Installation and Vulnerability Scanning Guide

Author:

Ziad Ben Saada

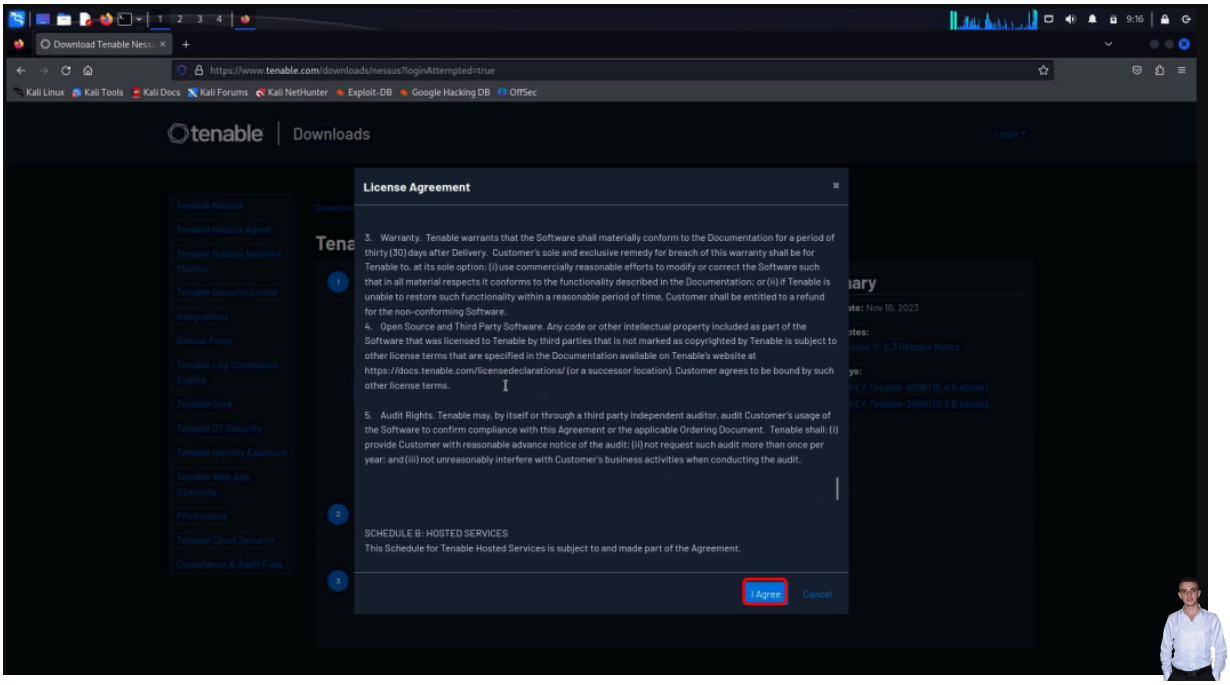
Go to website:

https://www.tenable.com/downloads/nessus?loginAttempted=true

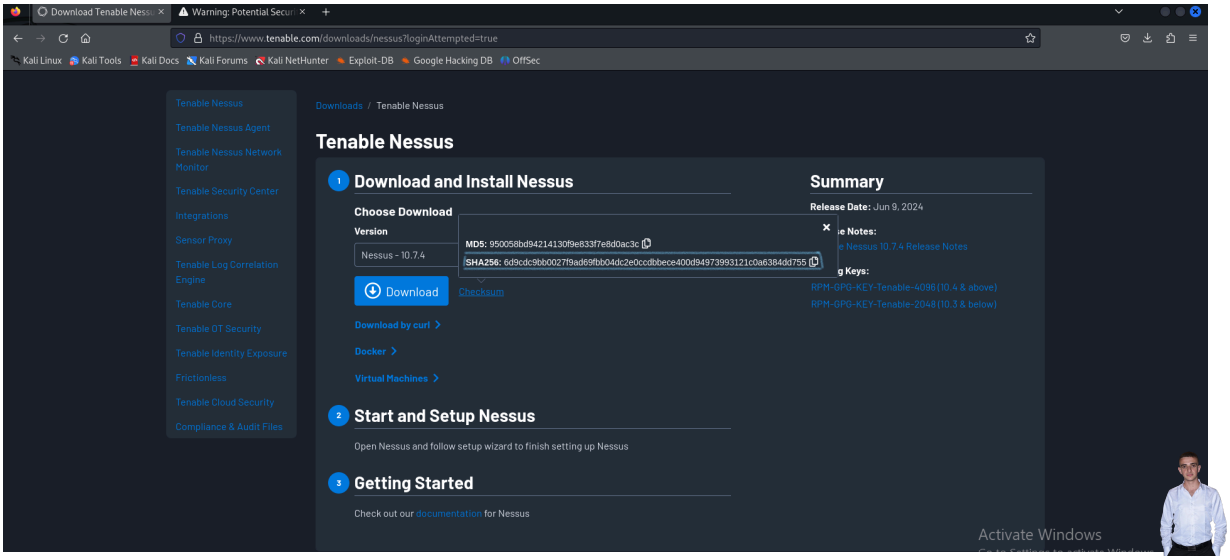


From Platform search for Linux - Debian – amd64 and download the file.

Agree to the License Agreement

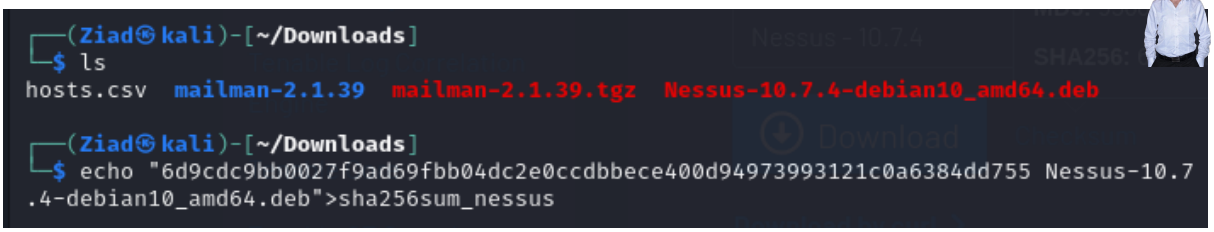


Click on Checksum right next to the download button and copy the SHA256 checksum

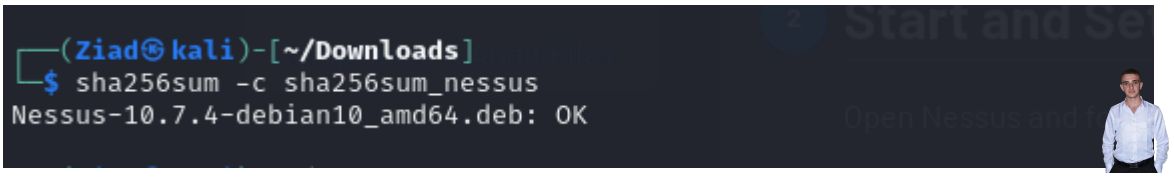


Open the ~/Downloads directory in the terminal and enter the following command (change the checksum and the Nessus version to the correct values):

echo "9b916de54b886e2a67a60ad32b5beccd7f334ab585f9fffe940a100efe3ca8c6 Nessus-10.6.3- debian10_amd64.deb" > sha256sum_nessus

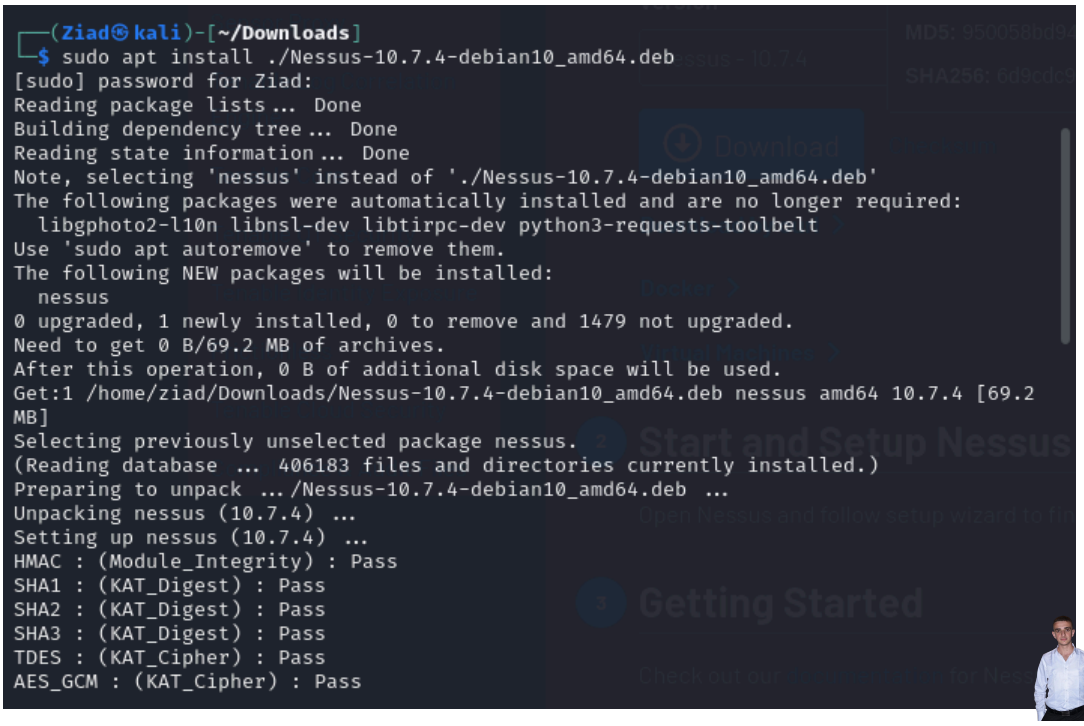


Run the command sha256sum –c sha256sum_nessus



Install Nessus by running the command: (change the Nessus version to the correct value):

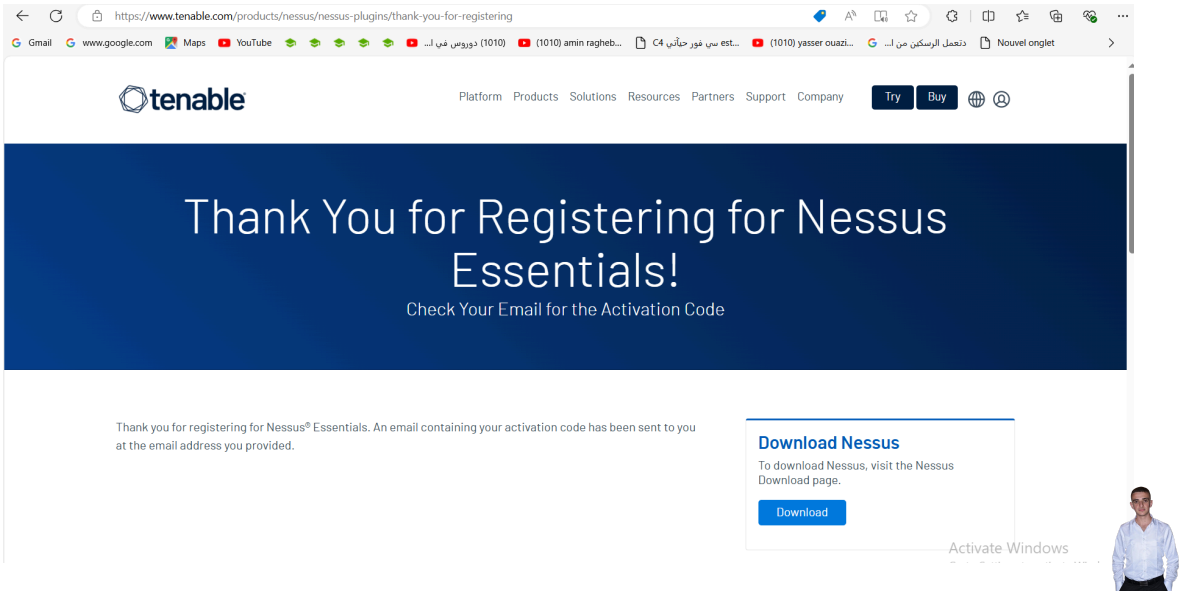
sudo apt install ./ Nessus-10.6.3-debian10_amd64.deb This will install Nessus.



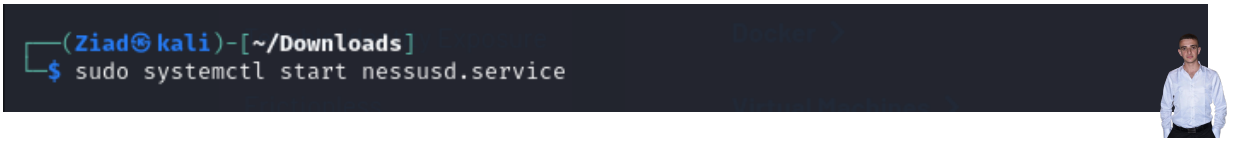
You will now need to go to the following website:

https://www.tenable.com/tenable-for-education/nessus-essentials

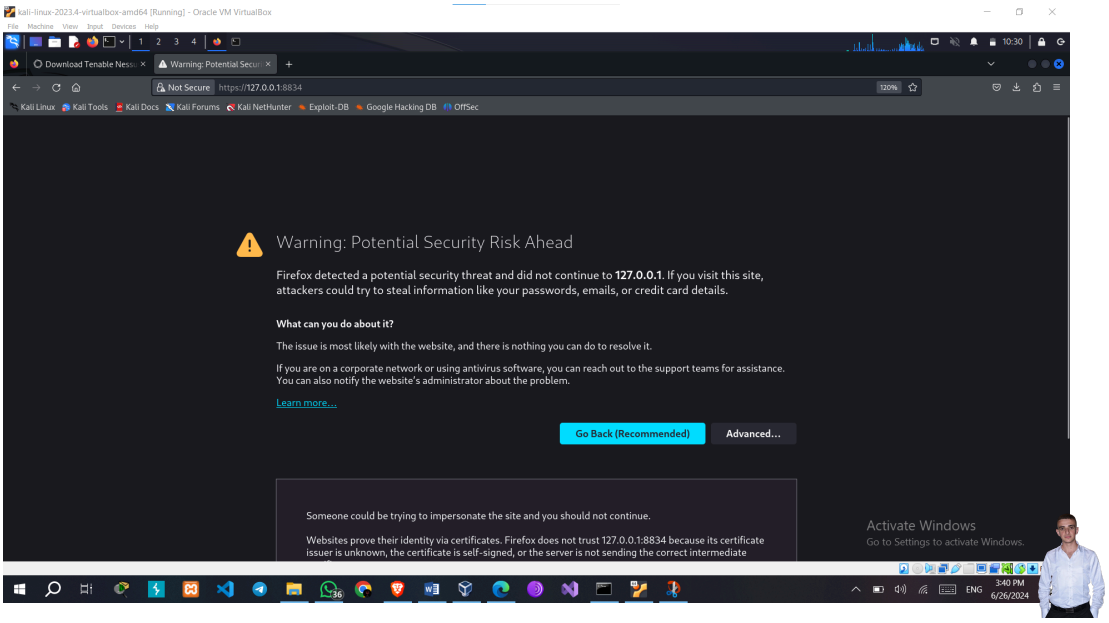
fill in your details and click Get Started.



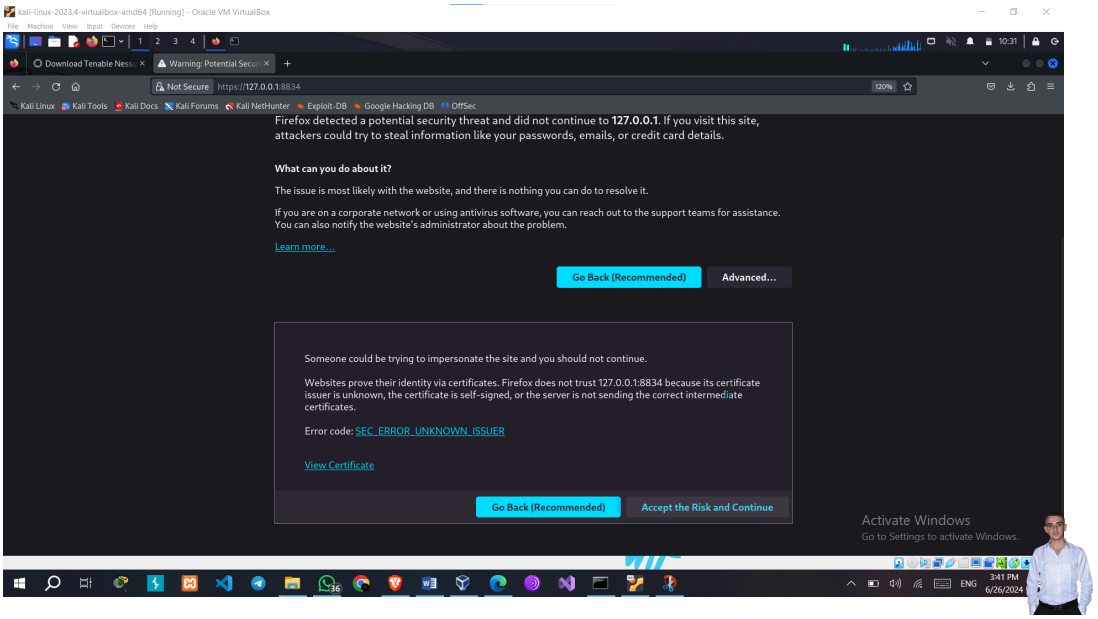
Open the terminal and run the command sudo systemctl start nessusd.service



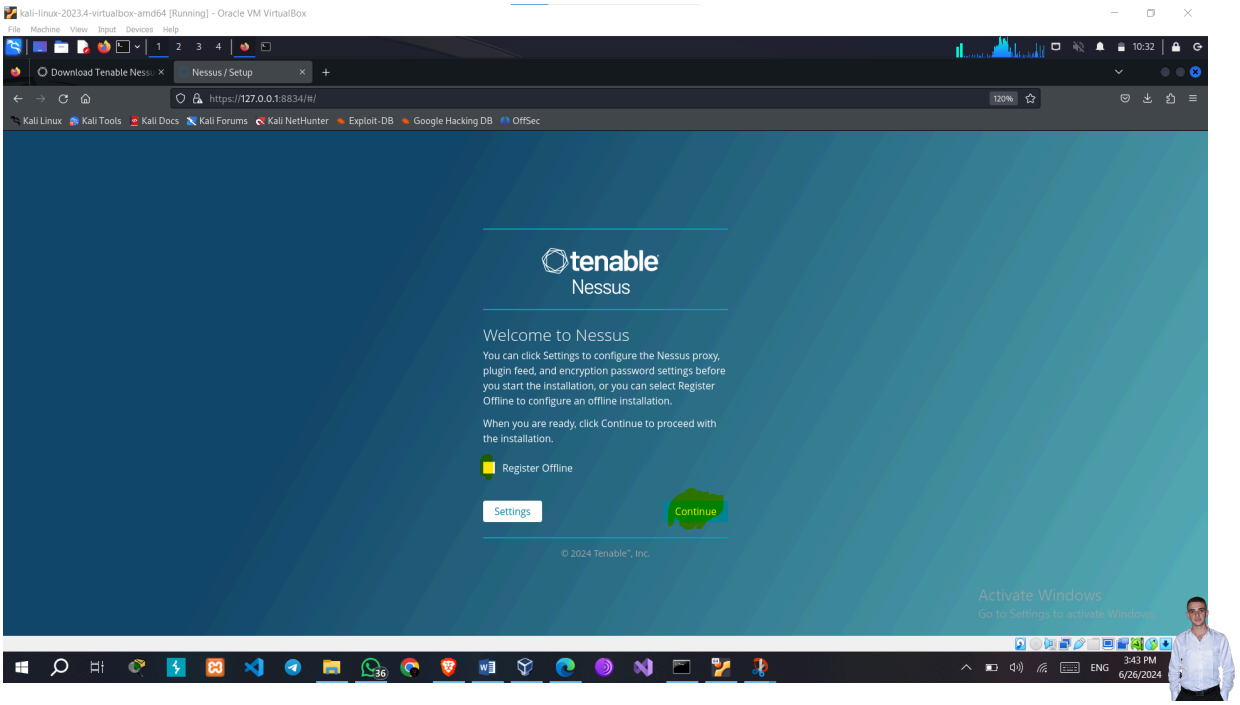
Enter the address https://127.0.0.1:8834 in your browser.



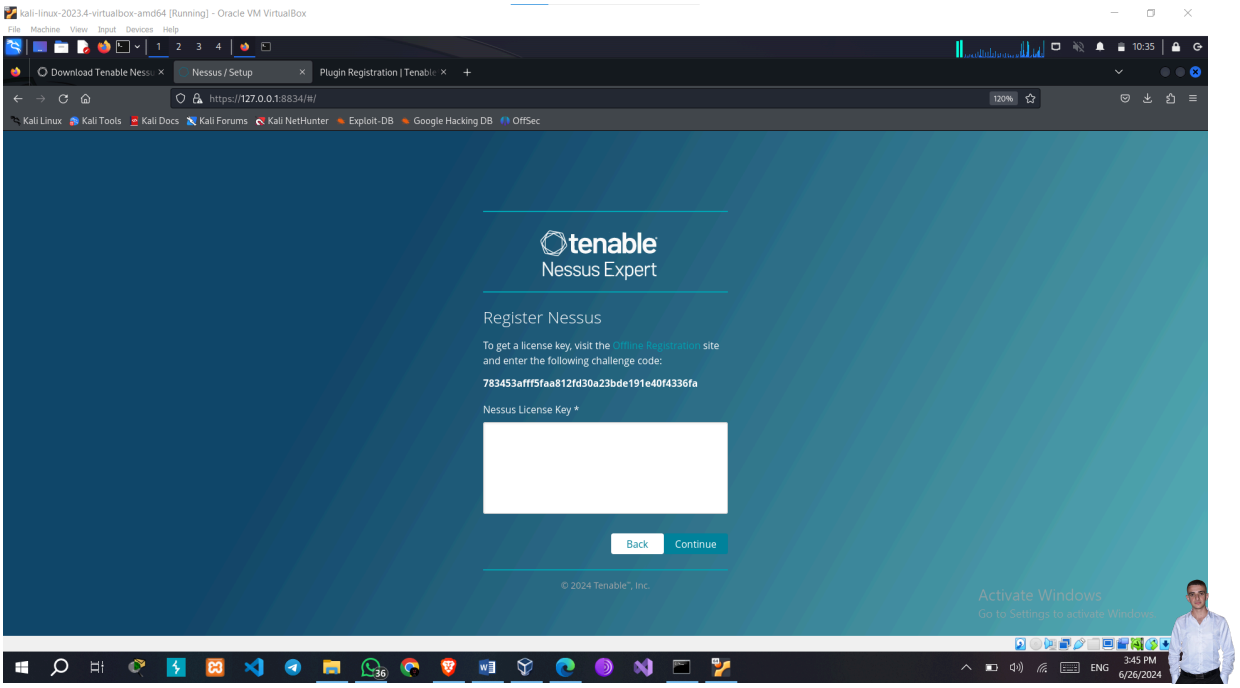
Click on Advanced. Click on Accept Risk and Continue.



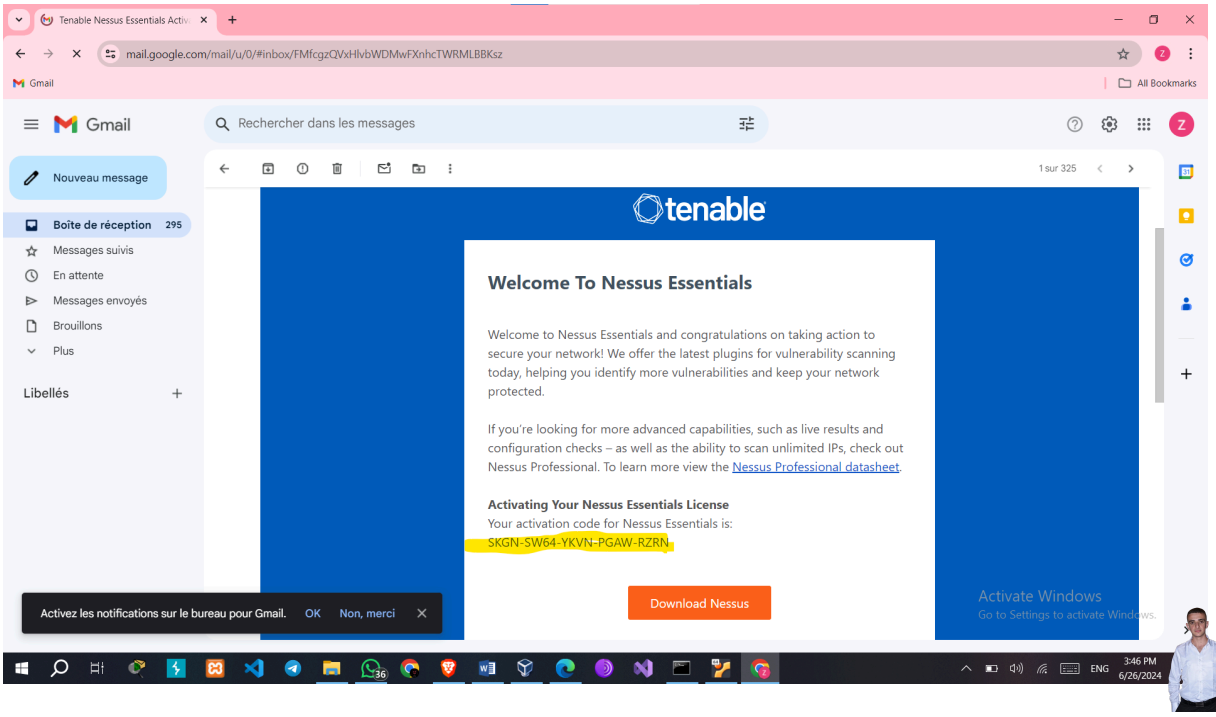
Select Register Offline and click Continue.



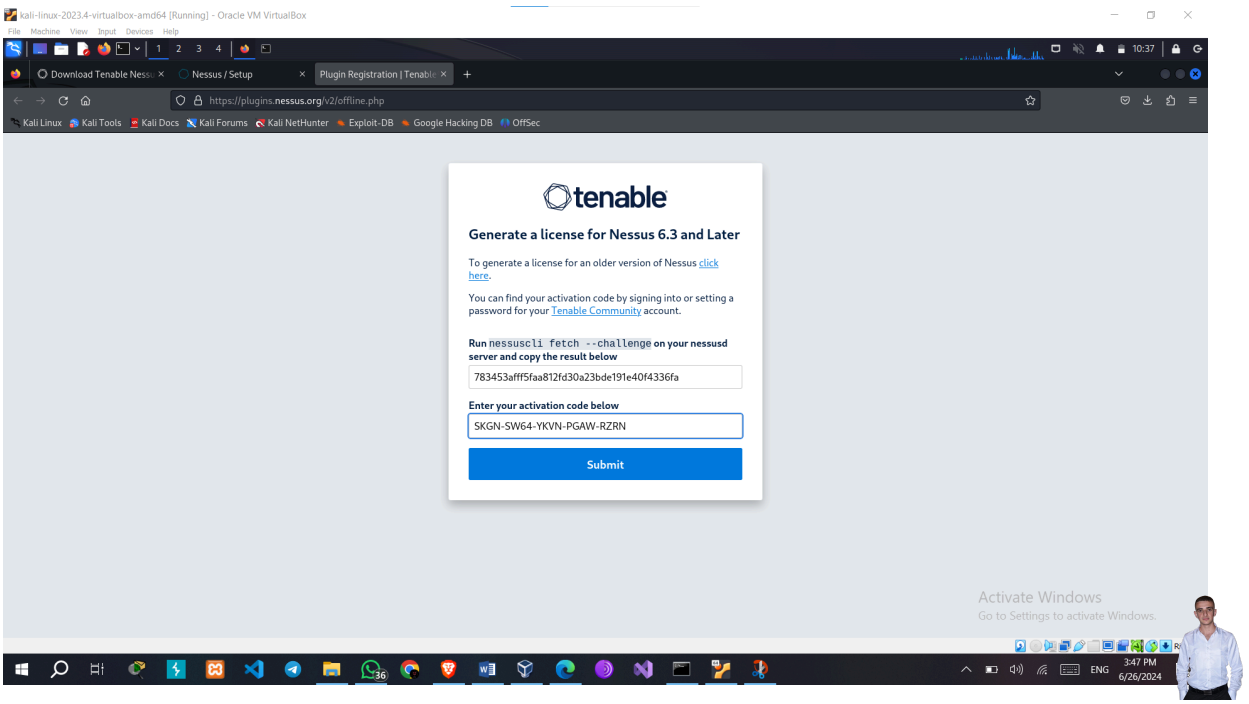
Copy the challenge code and select Offline Registration



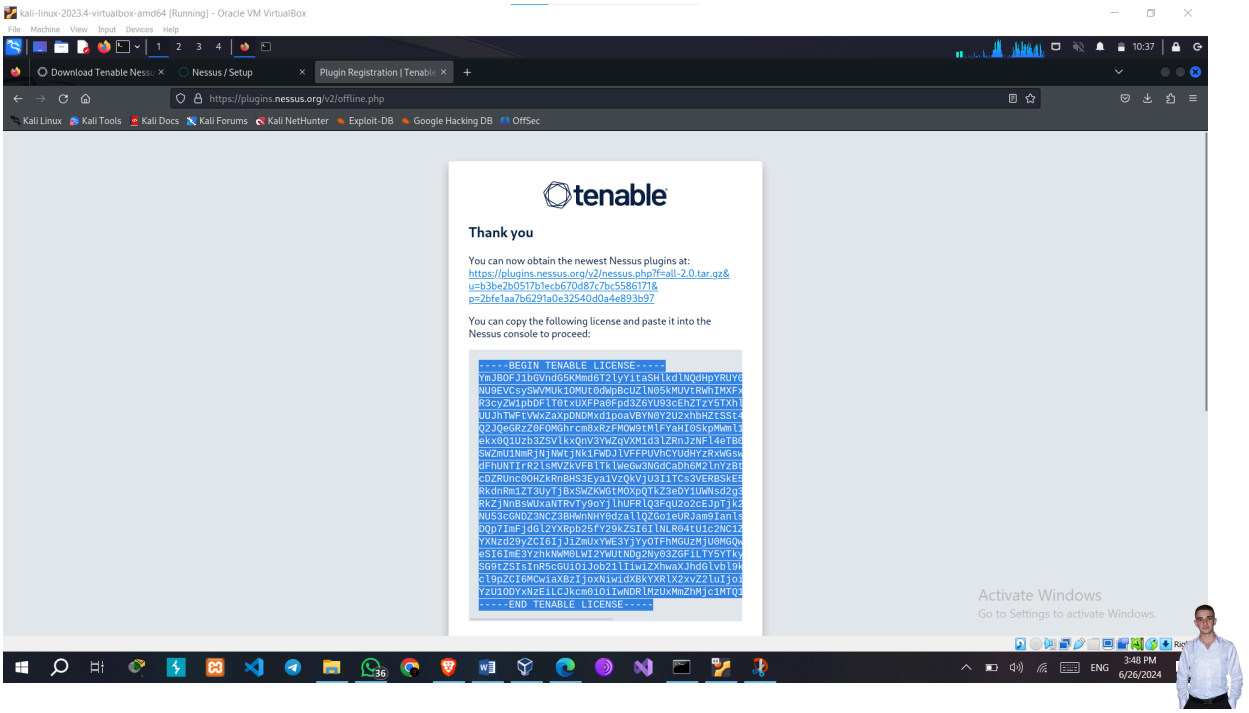
Copy your code to Activate Your Nessus Essentials License



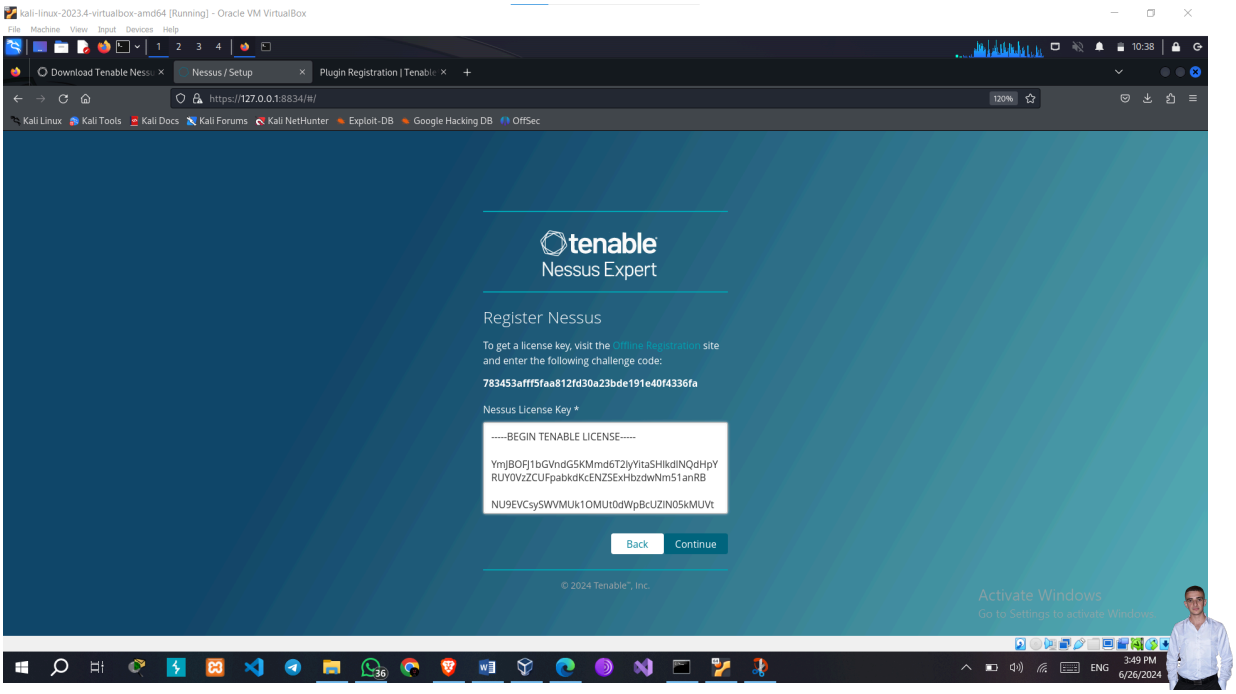
Copy your codes in the correct boxes and submit.



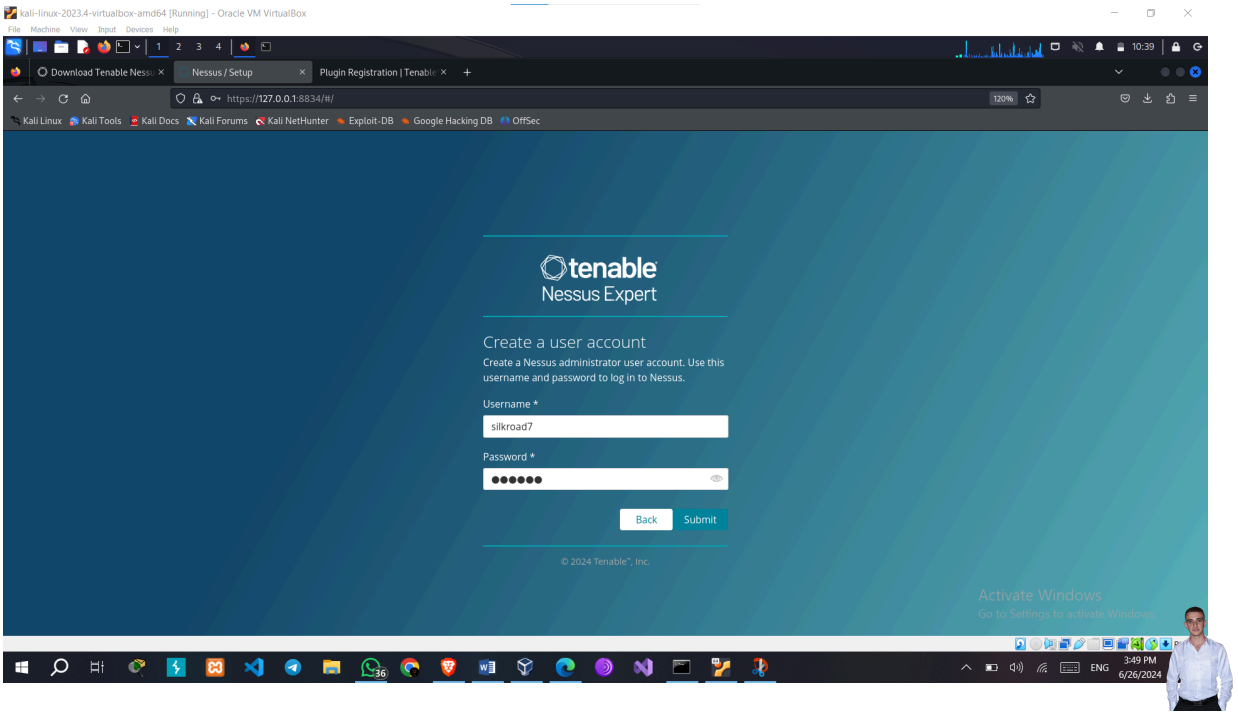
Copy the license code.



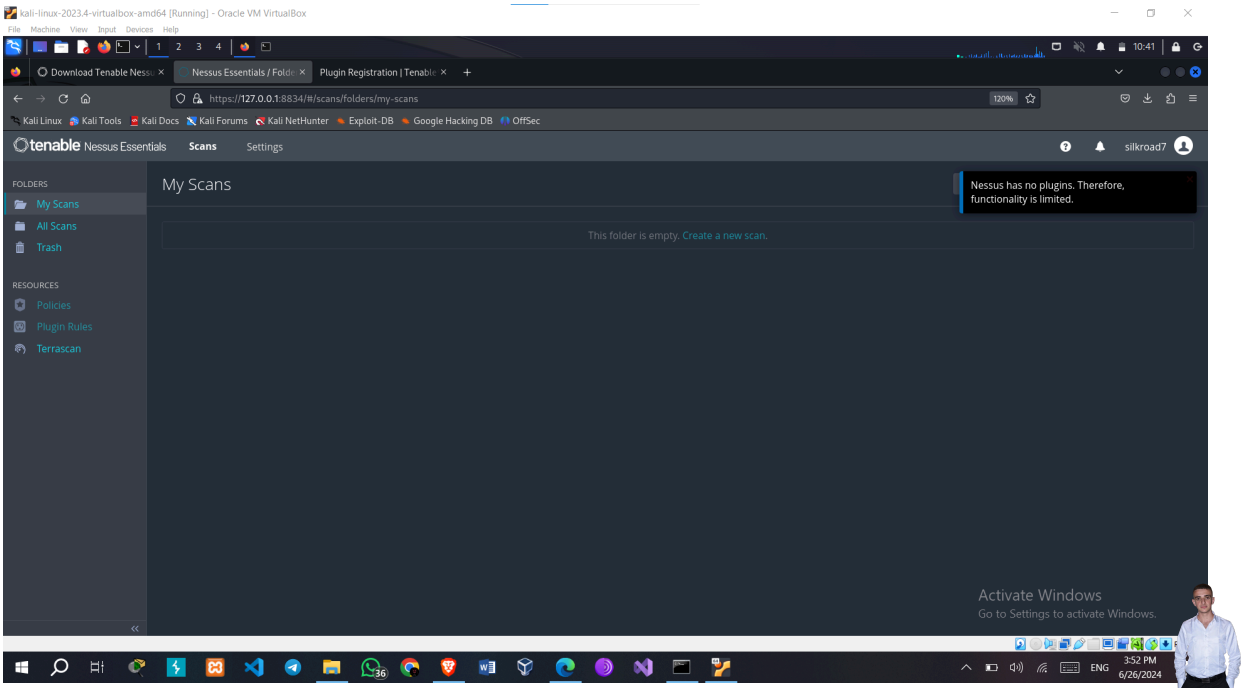
Paste it under Nessus License Key, and click continue



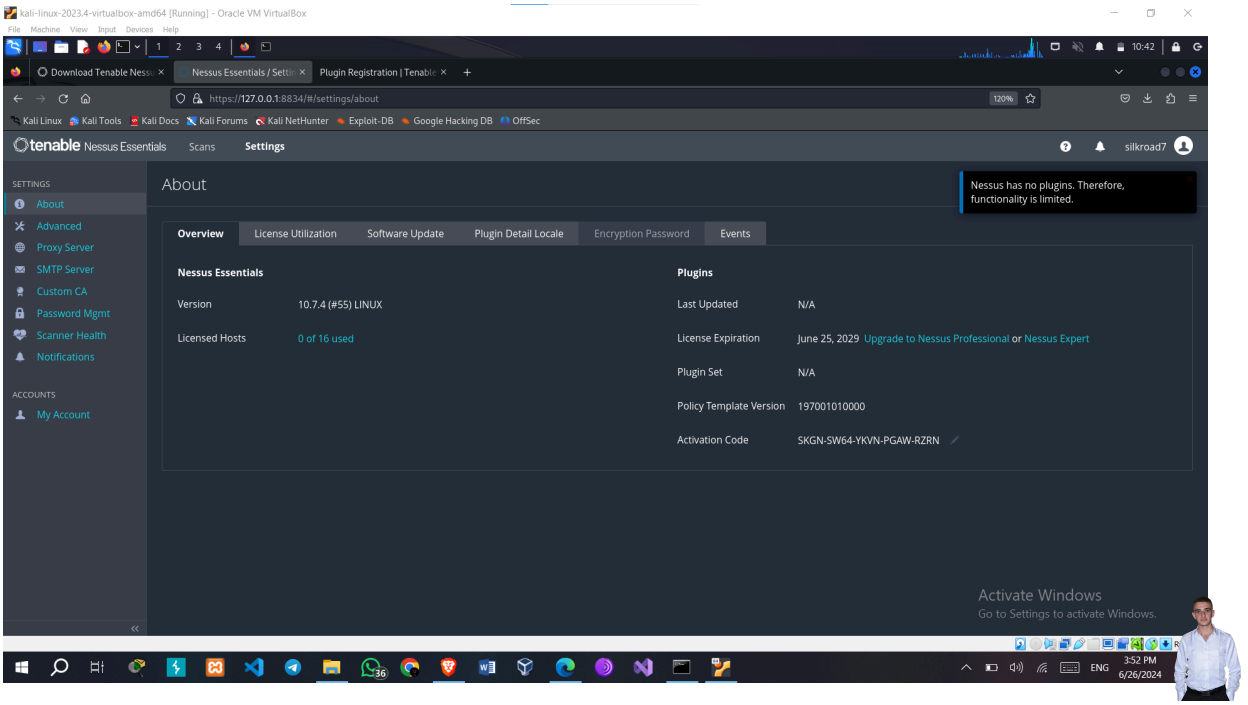
Create Username & Password for Nessus



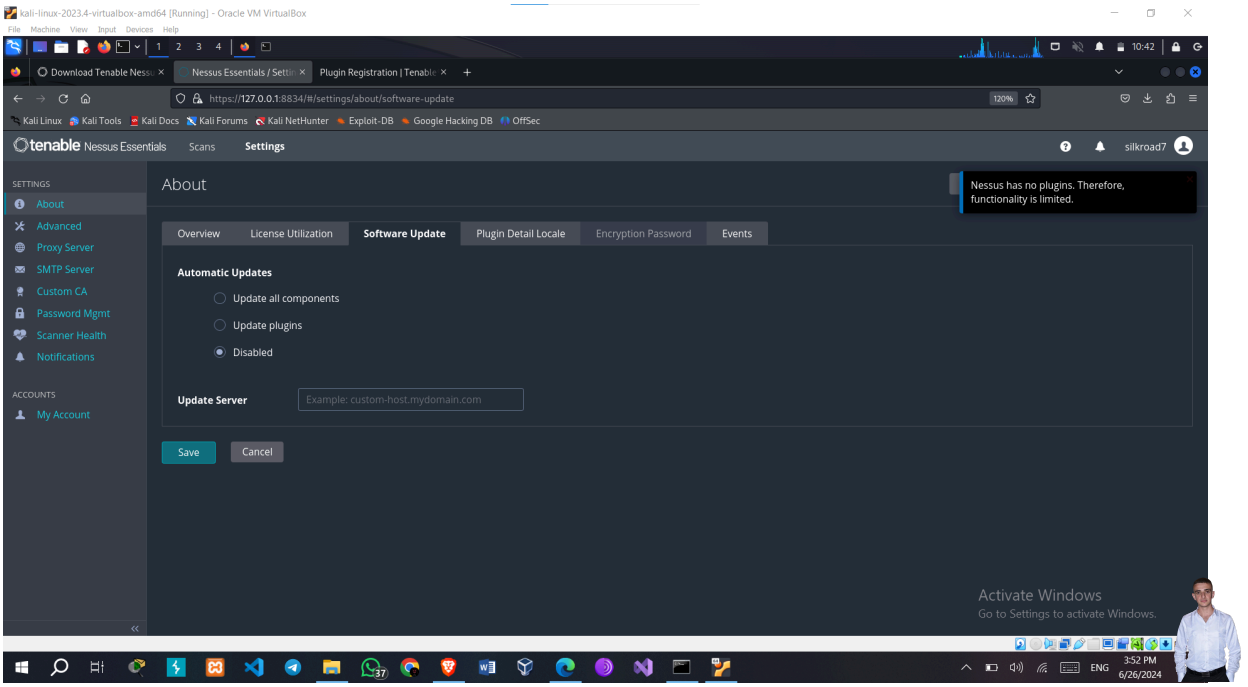
Nessus has started



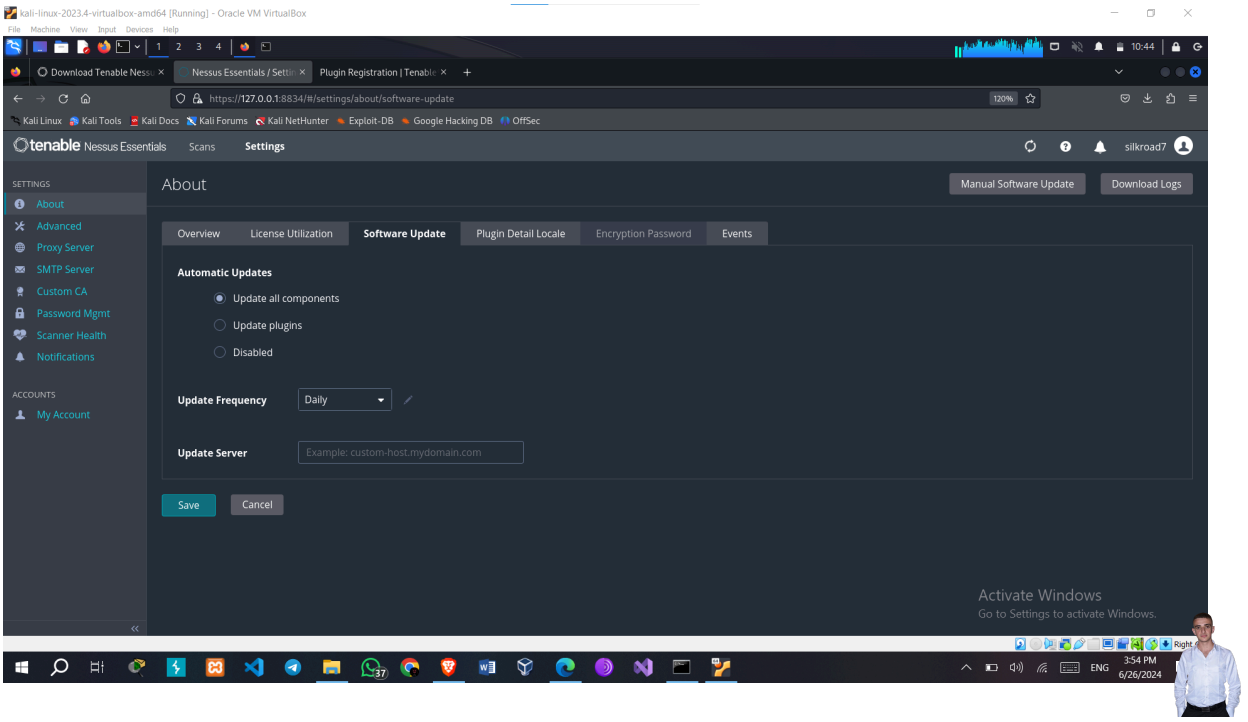
Go to settings



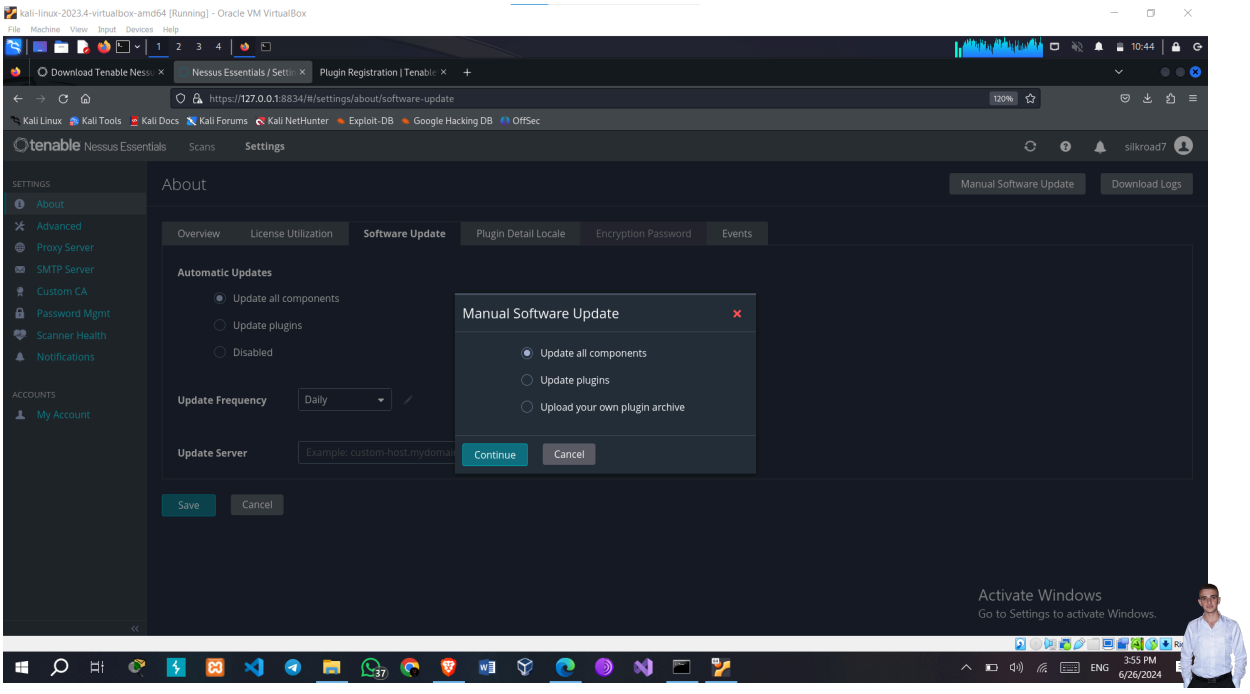
Select Software Update



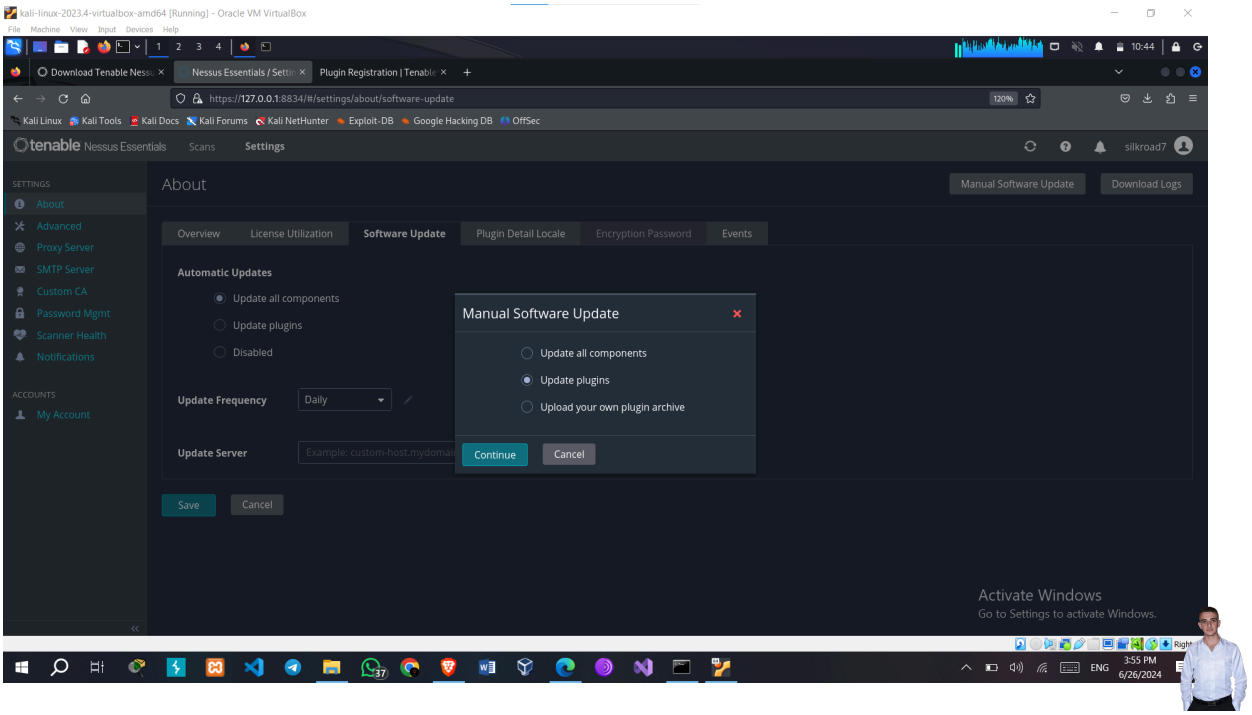
Select Update all componenets



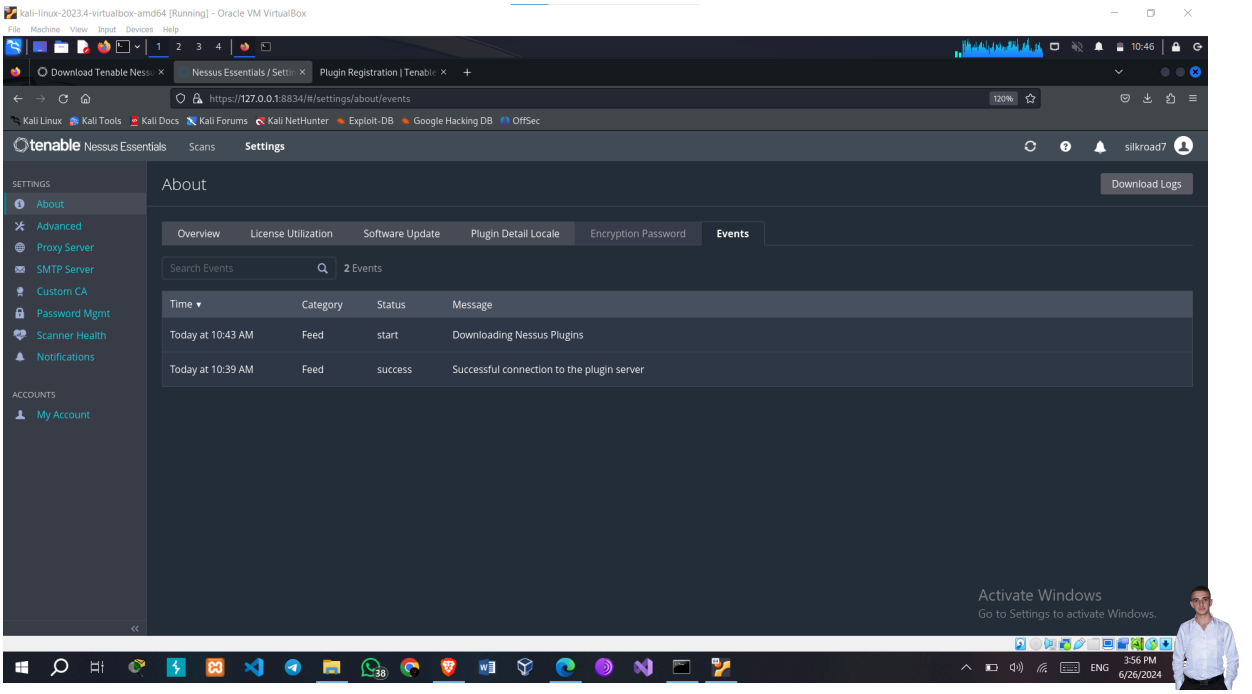
Go to Manual Software Update Right in the top



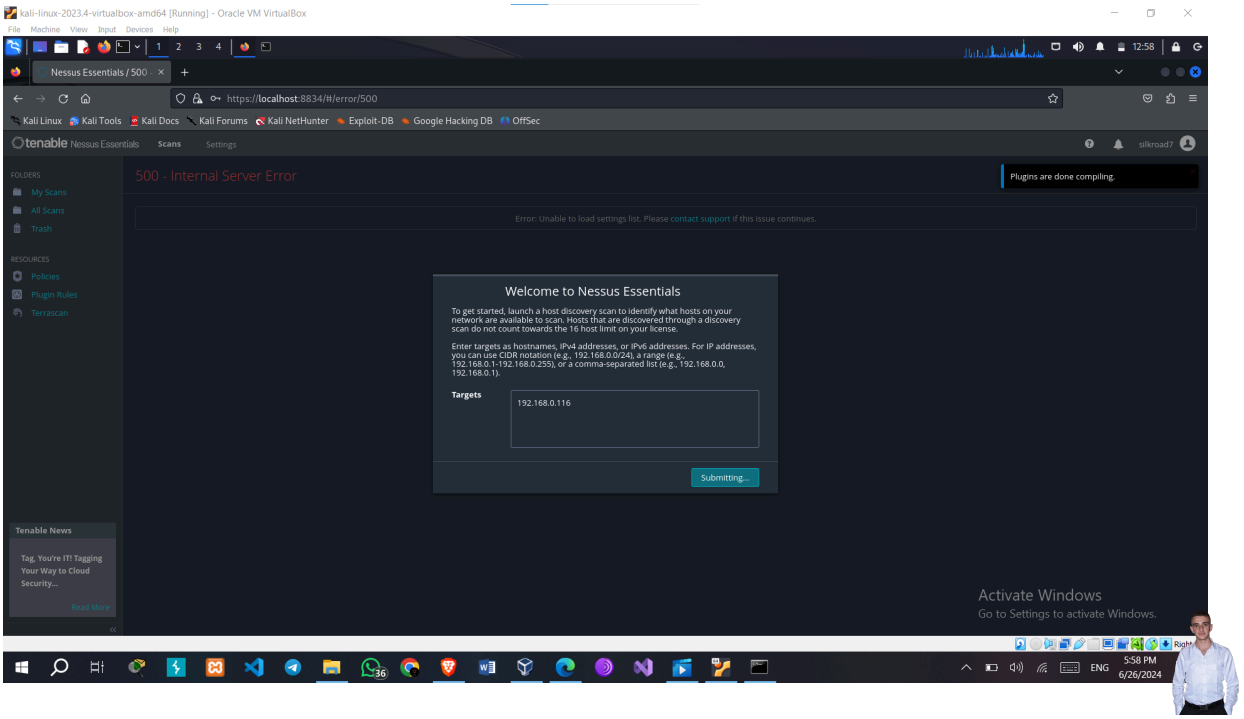
Update plugins



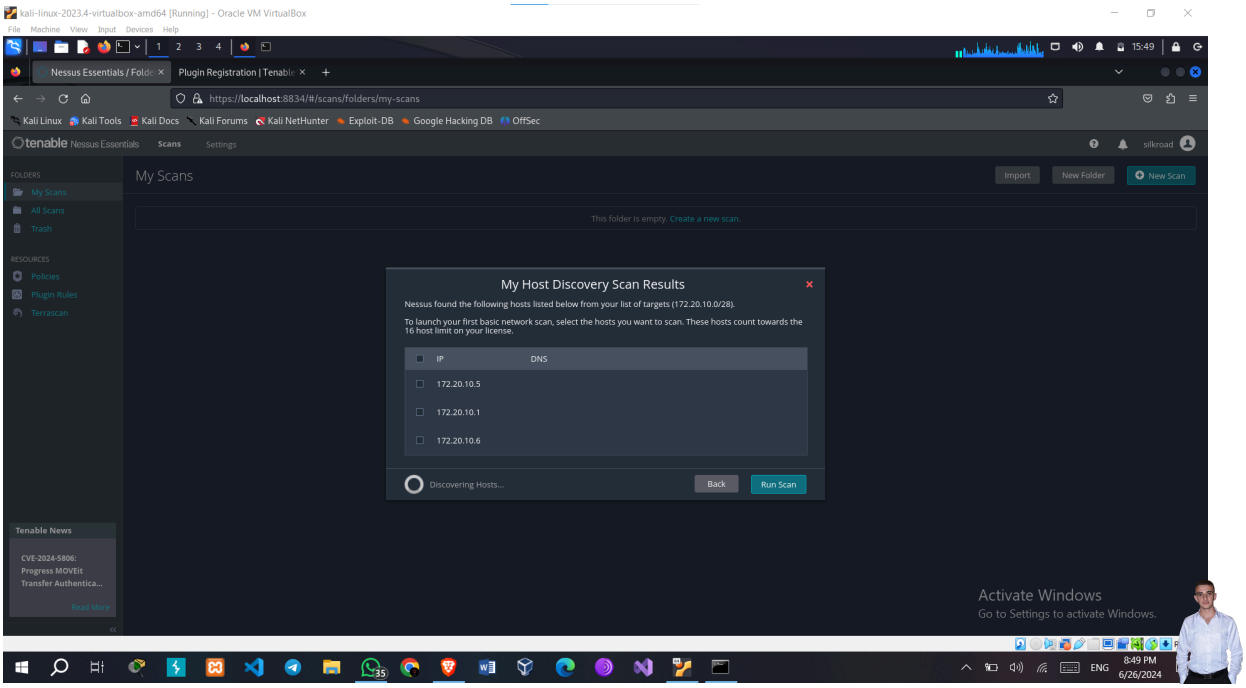
Wait Until the Update is finished



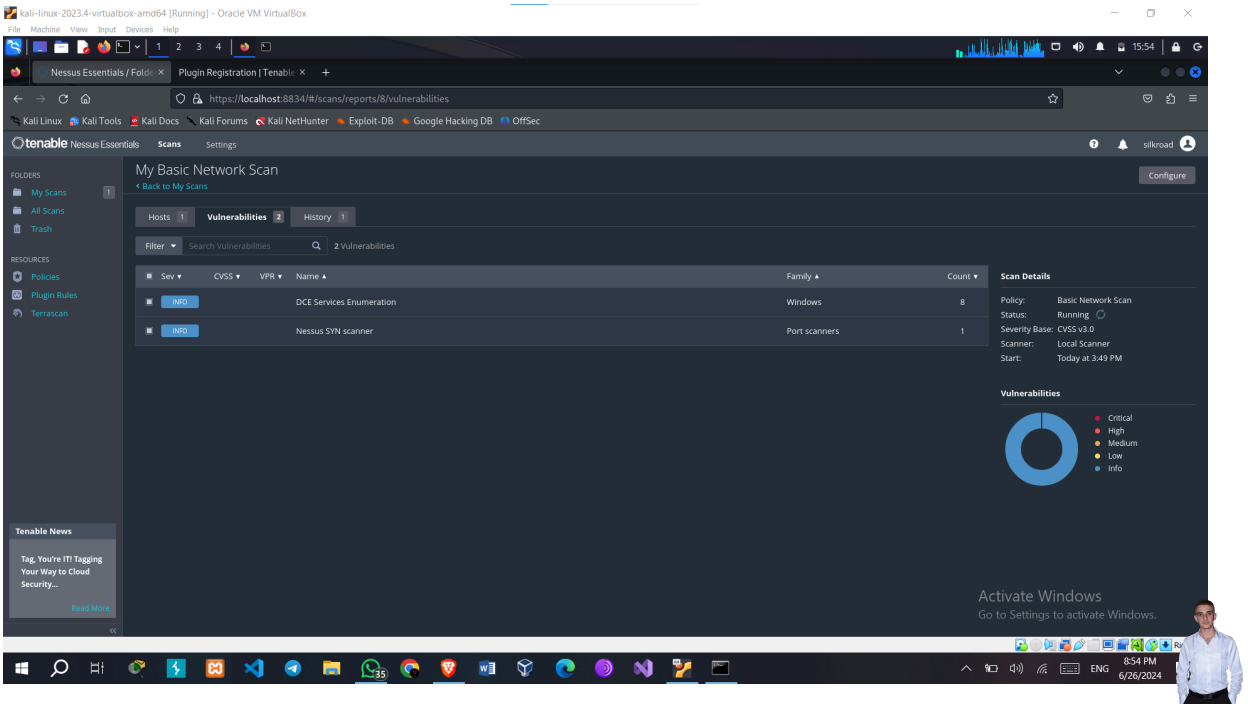
Add your targets here (Network Address)



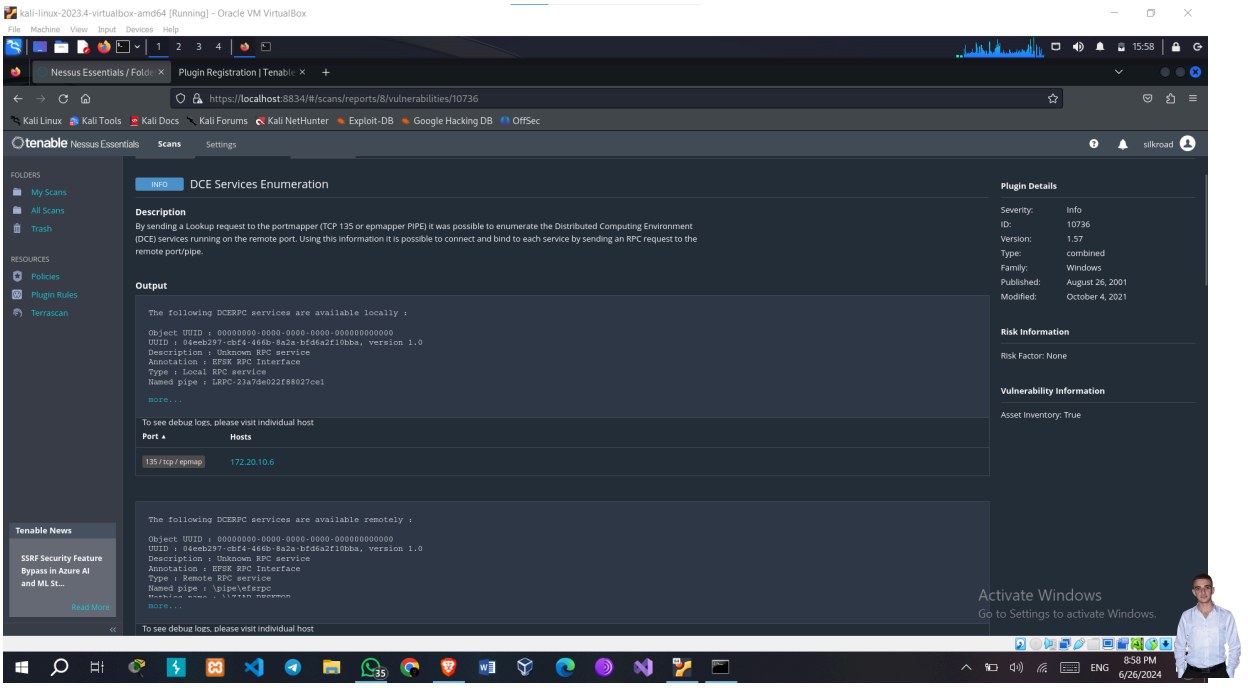
Scan Results and Get all Ips Connected



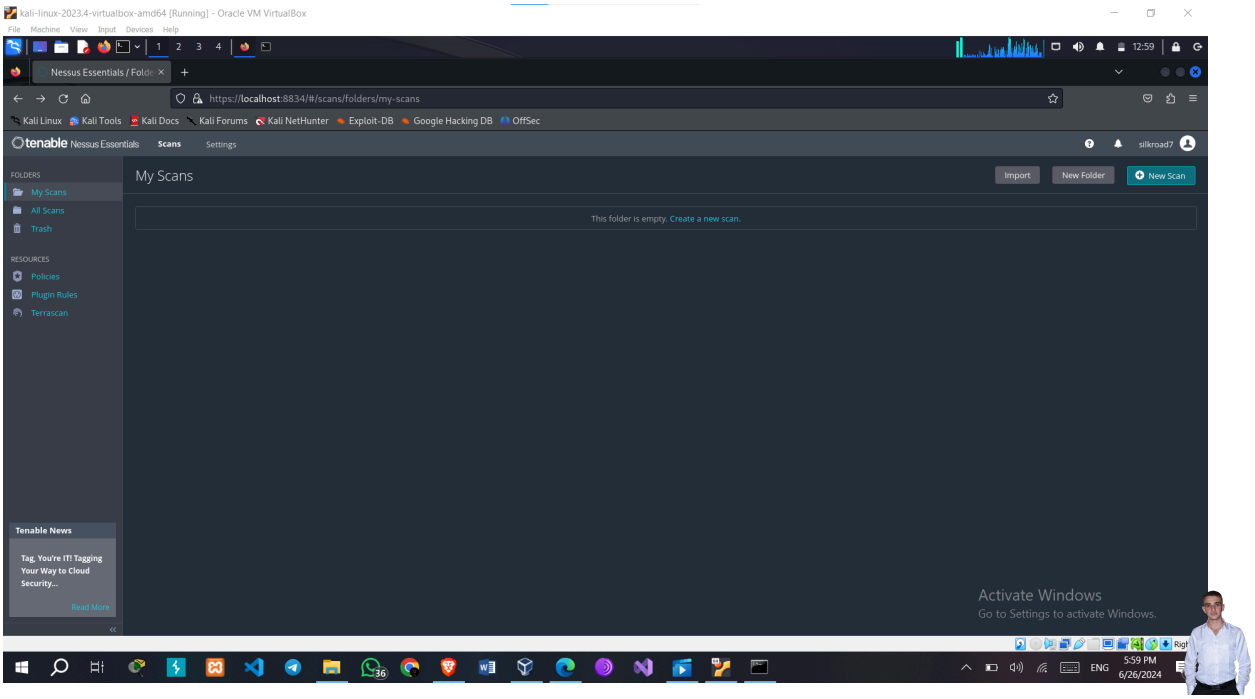
Here, we have a list of all the vulnerabilities that were found.



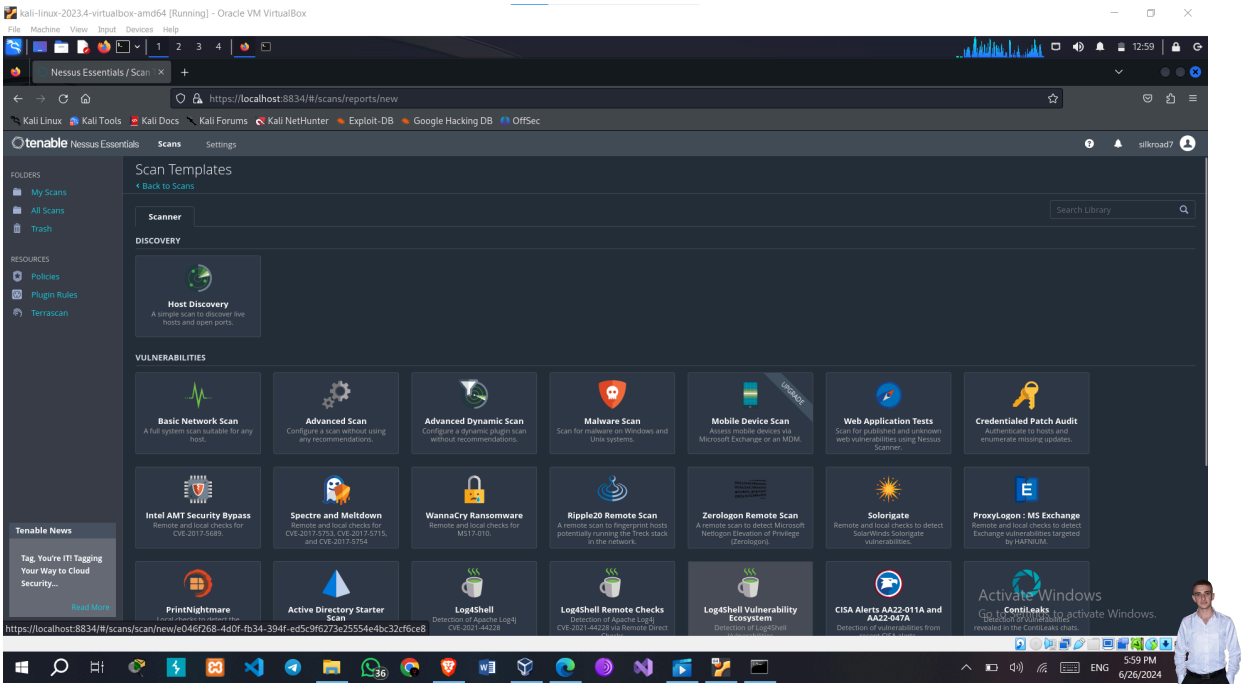
The description of the vulnerability



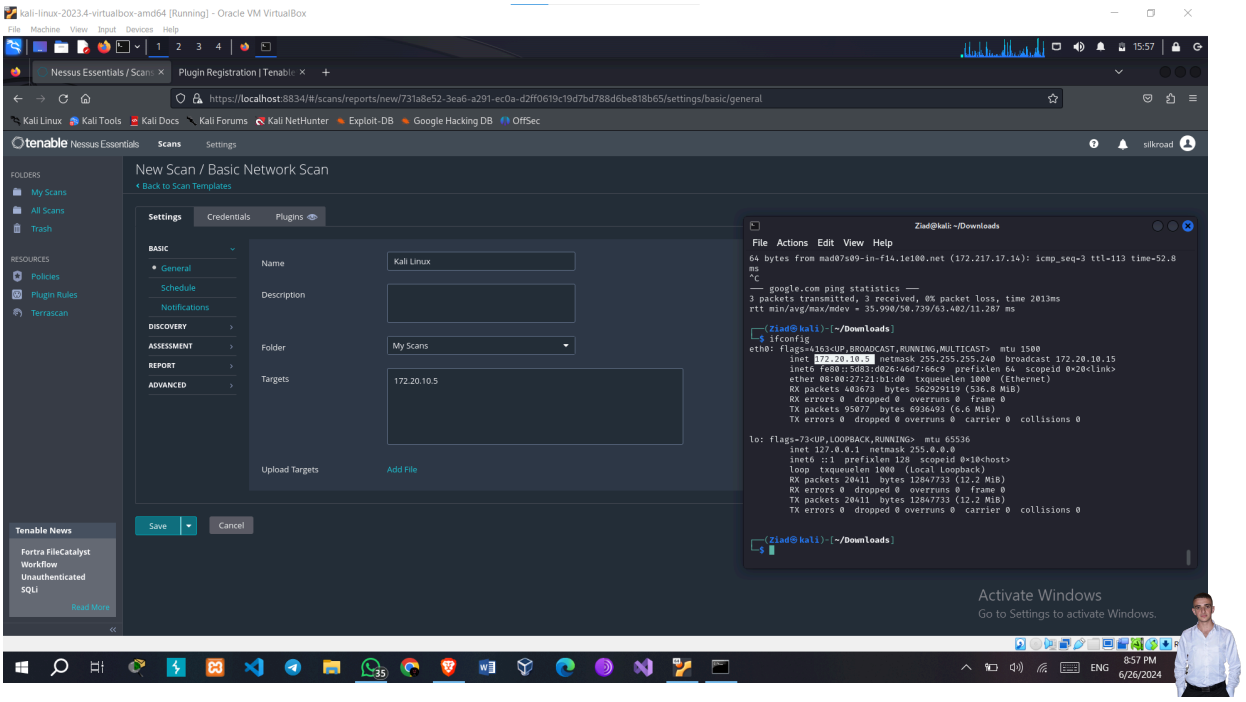
Or, go to 'Scan' at the top, and click on 'New Scan'



Choose Basic Network Scan or What you need



Add the Name & the Targets ip address



For More Info:

GitHub: https://github.com/ziadbensaada

LinkedIn: https://www.linkedin.com/in/ziad-ben-saada-850219226/