

Nessus Installation and Vulnerability Scanning Guide



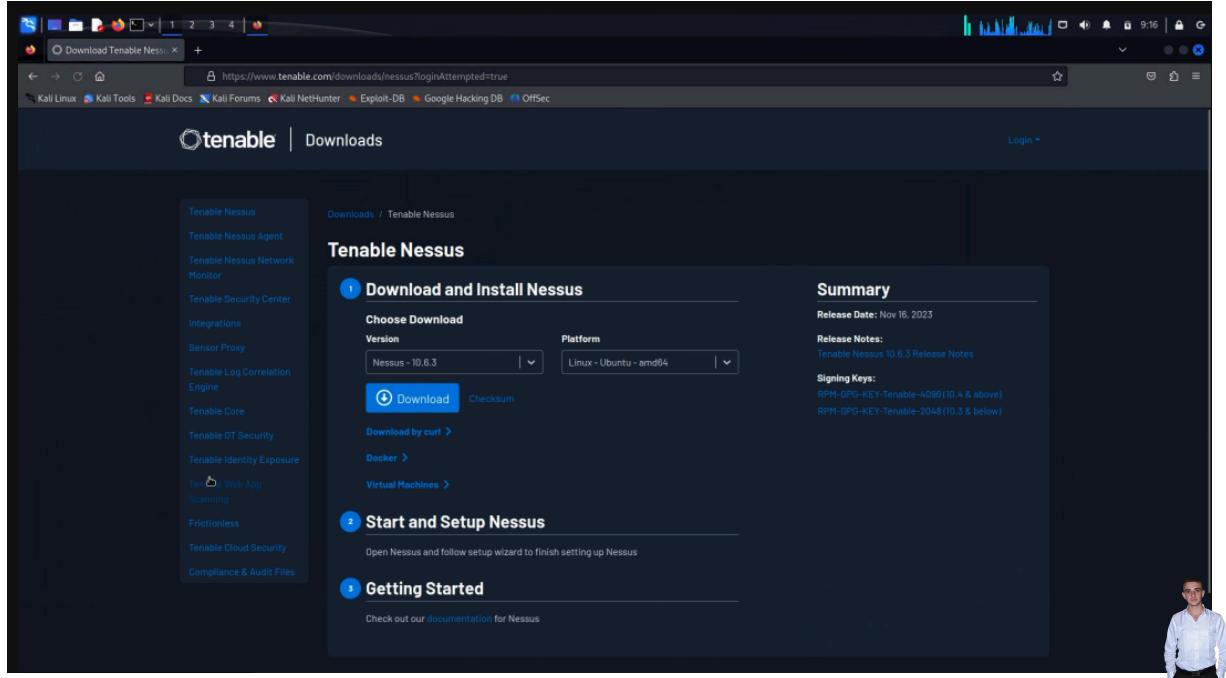
Author:



Ziad Ben Saada

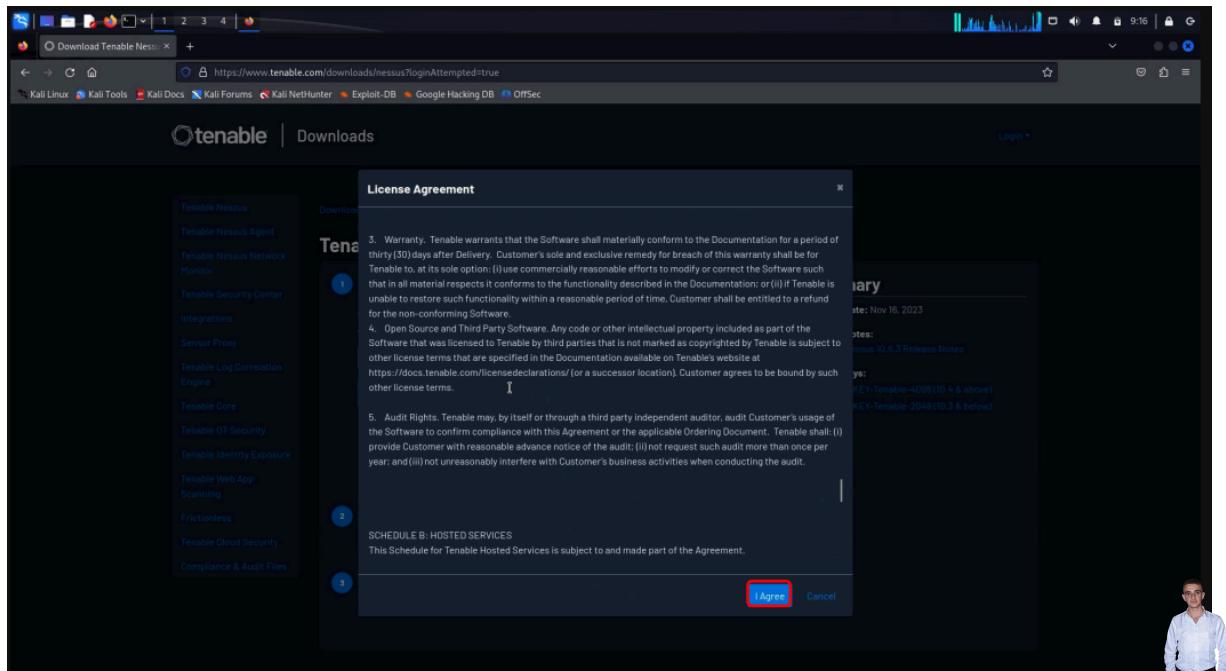
Go to website:

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

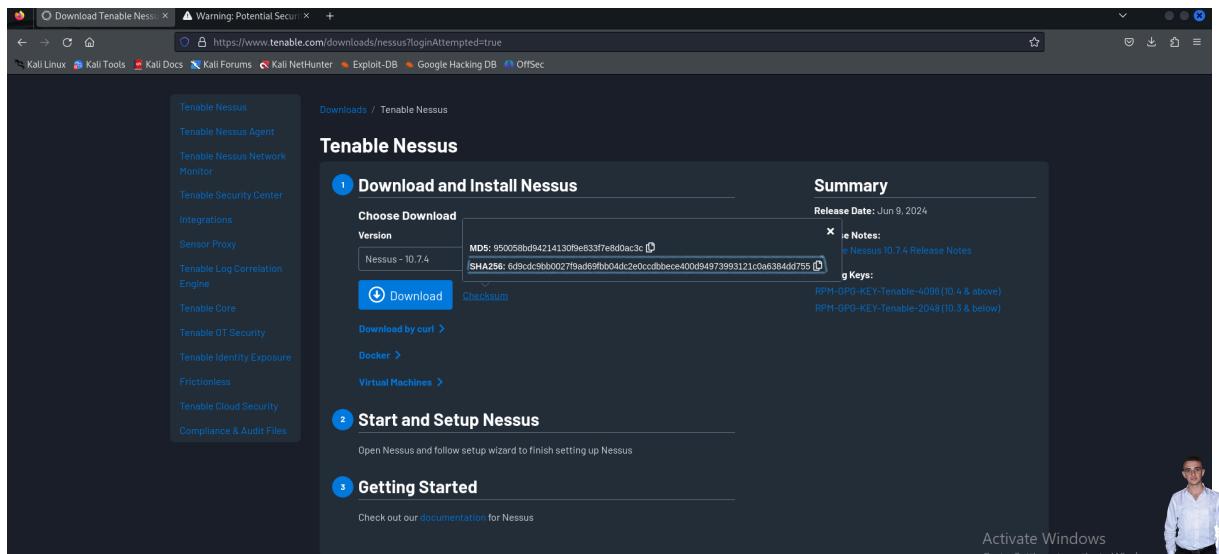


From Platform search for Linux - Debian – amd64 and download the file.

Agree to the License Agreement



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

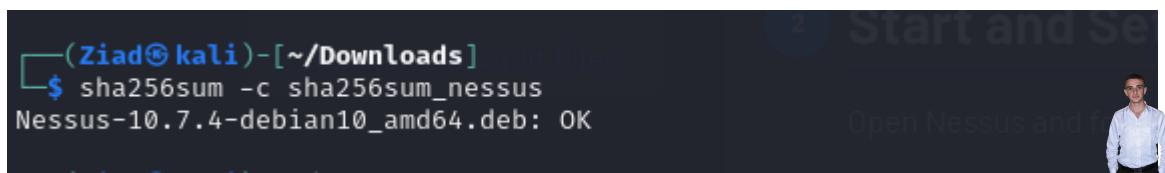


Open the ~/Downloads directory in the terminal and enter the following command (change the checksum and the Nessus version to the correct values):

```
echo "9b916de54b886e2a67a60ad32b5becccd7f334ab585f9ffe940a100efe3ca8c6  
Nessus-10.6.3- debian10_amd64.deb" > sha256sum_nessus
```

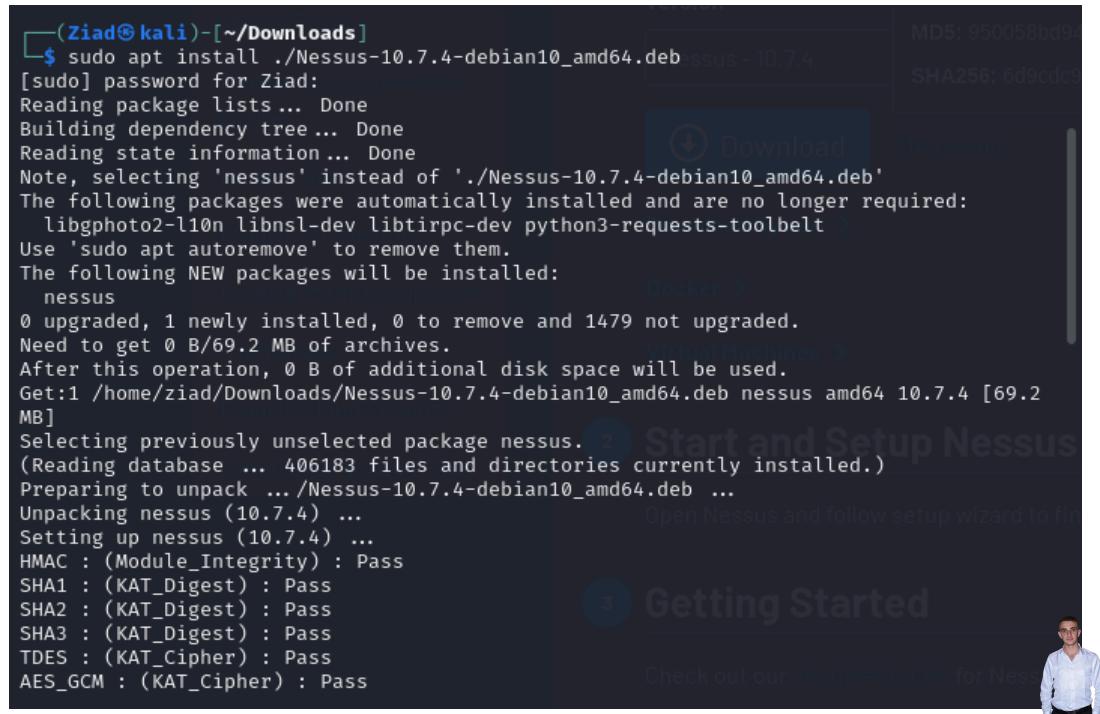


Run the command `sha256sum -c sha256sum_nessus`



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.

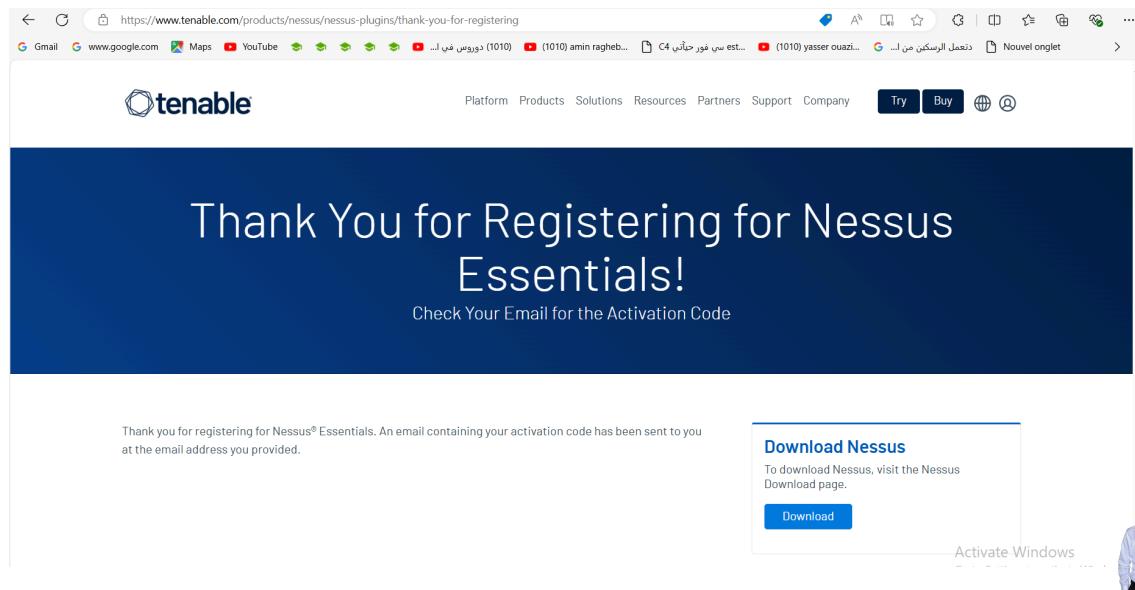


```
(Ziad@kali)-[~/Downloads]
$ sudo apt install ./Nessus-10.7.4-debian10_amd64.deb
[sudo] password for Ziad:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'nessus' instead of './Nessus-10.7.4-debian10_amd64.deb'
The following packages were automatically installed and are no longer required:
  libgphoto2-l10n libnsl-dev libtirpc-dev python3-requests-toolbelt
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  nessus
0 upgraded, 1 newly installed, 0 to remove and 1479 not upgraded.
Need to get 0 B/69.2 MB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 /home/ziad/Downloads/Nessus-10.7.4-debian10_amd64.deb nessus amd64 10.7.4 [69.2
MB]
Selecting previously unselected package nessus.
(Reading database ... 406183 files and directories currently installed.)
Preparing to unpack .../Nessus-10.7.4-debian10_amd64.deb ...
Unpacking nessus (10.7.4) ...
Setting up nessus (10.7.4) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
```

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.



Thank You for Registering for Nessus Essentials!

Check Your Email for the Activation Code

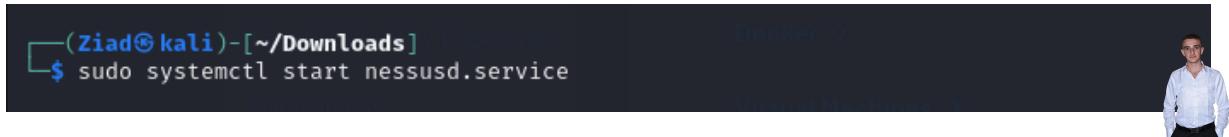
Download Nessus

To download Nessus, visit the Nessus Download page.

Download

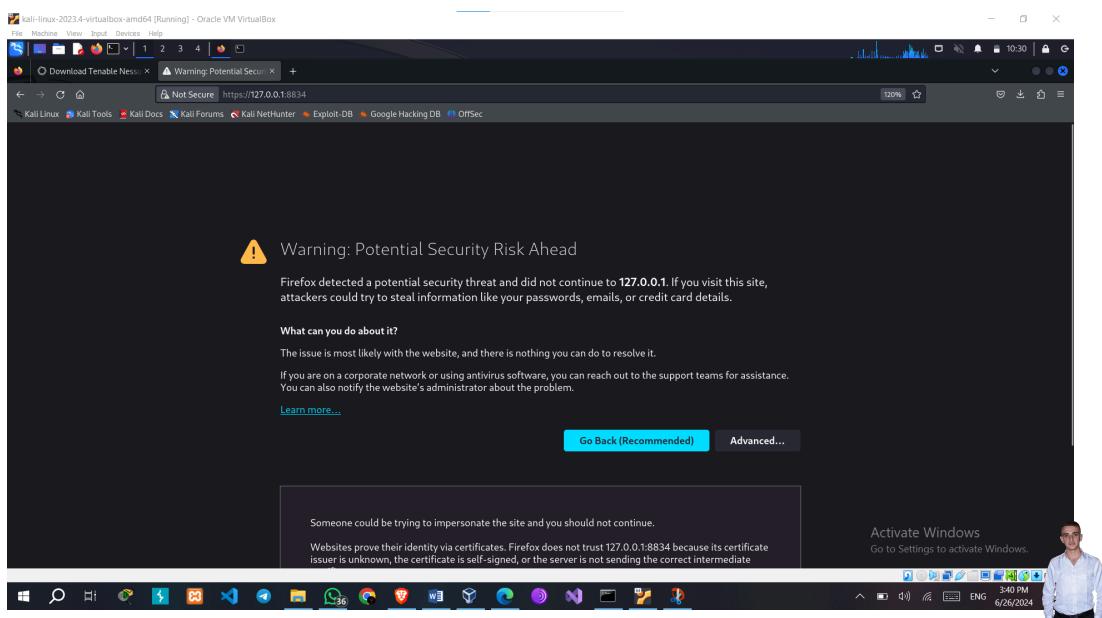
Activate Windows

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

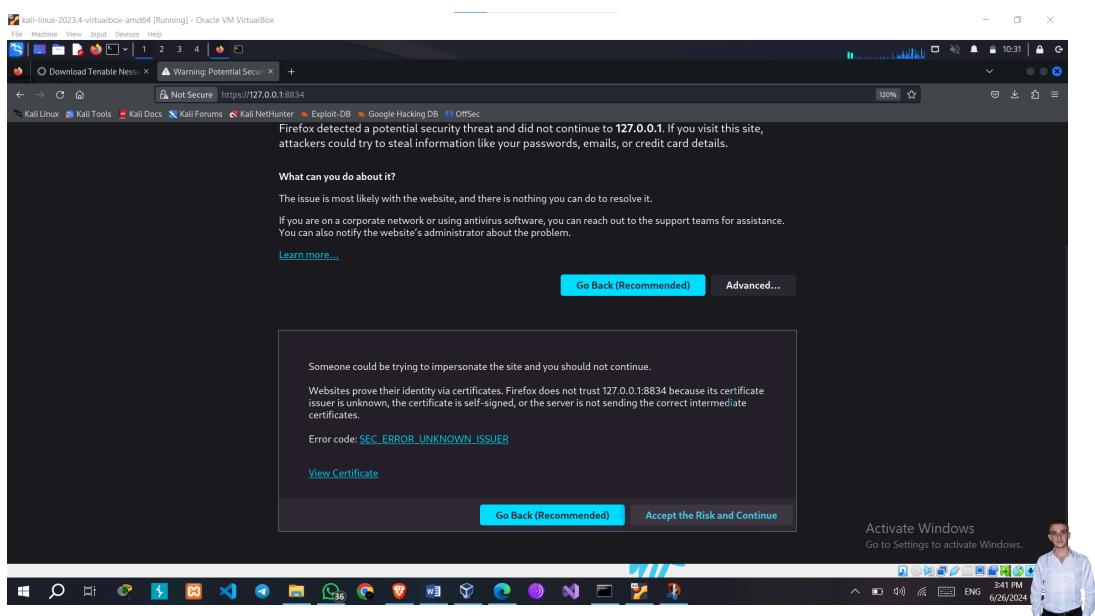


```
(Ziad@kali)-[~/Downloads] ~$ sudo systemctl start nessusd.service
```

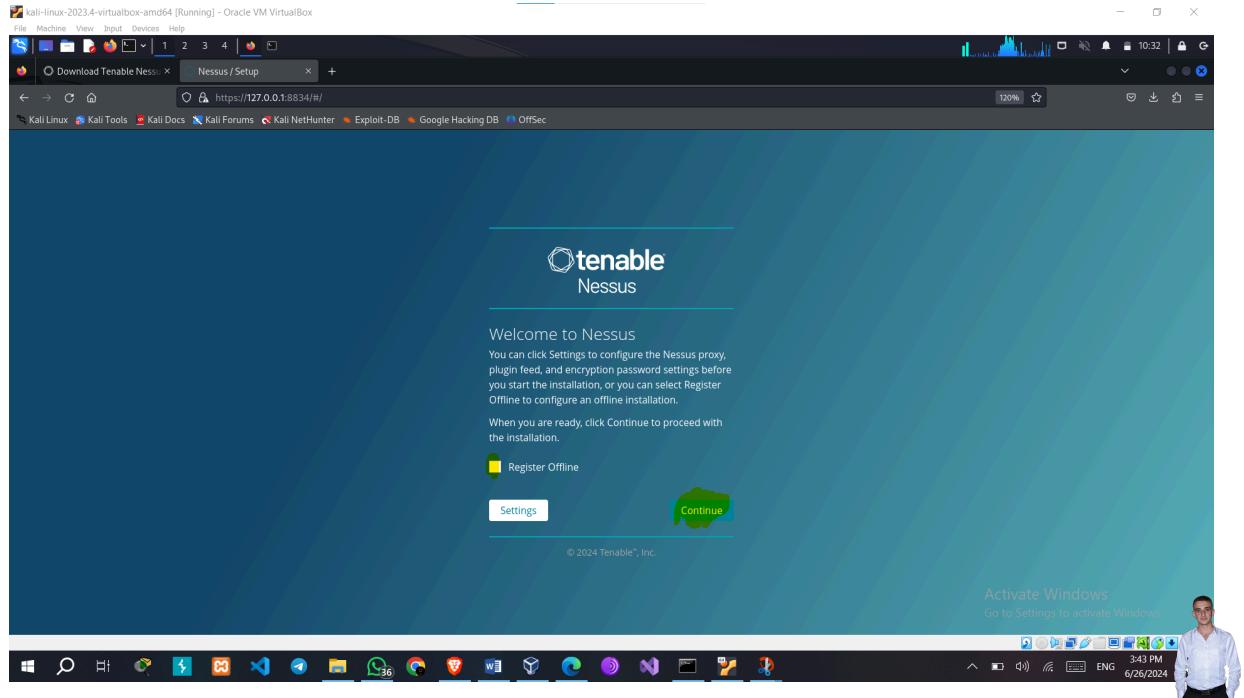
Enter the address <https://127.0.0.1:8834> in your browser.



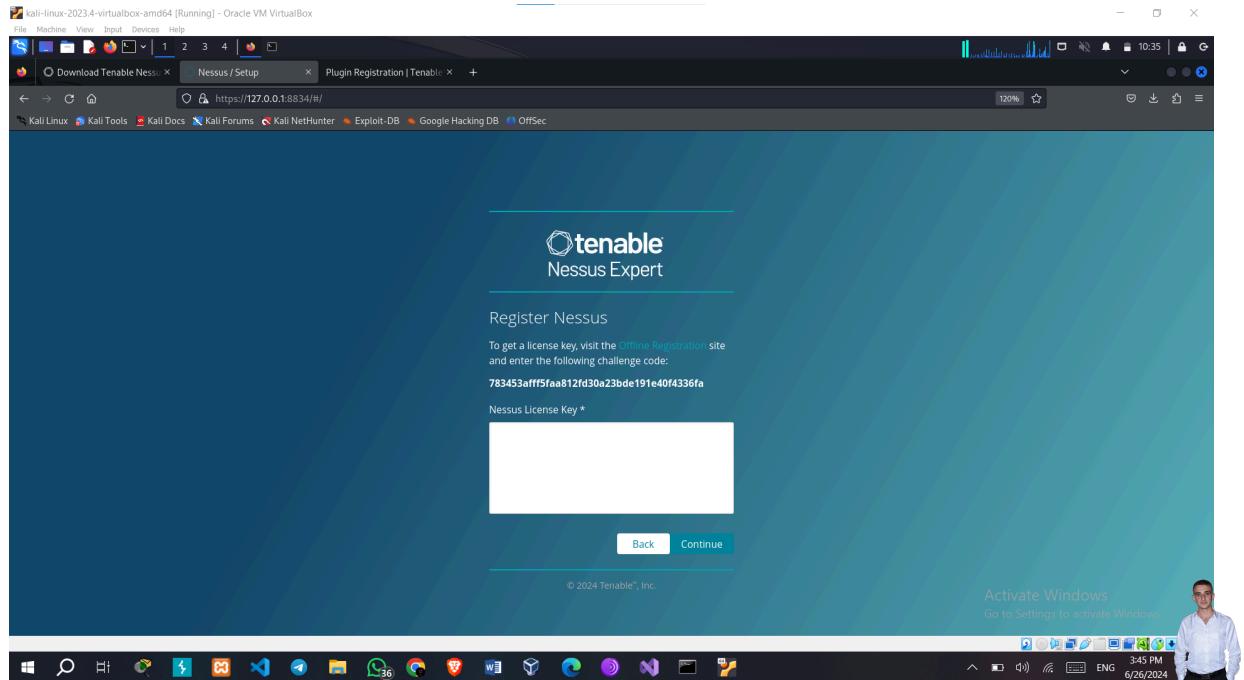
Click on Advanced. Click on Accept Risk and Continue.



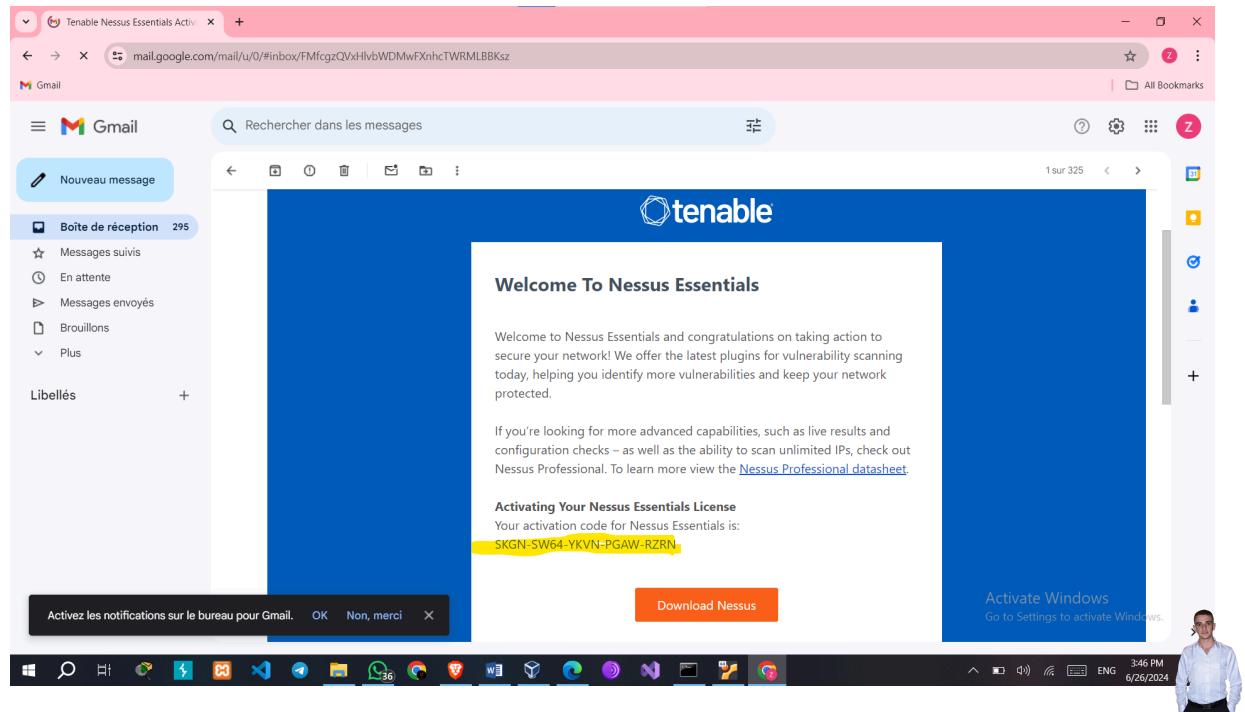
Select Register Offline and click Continue.



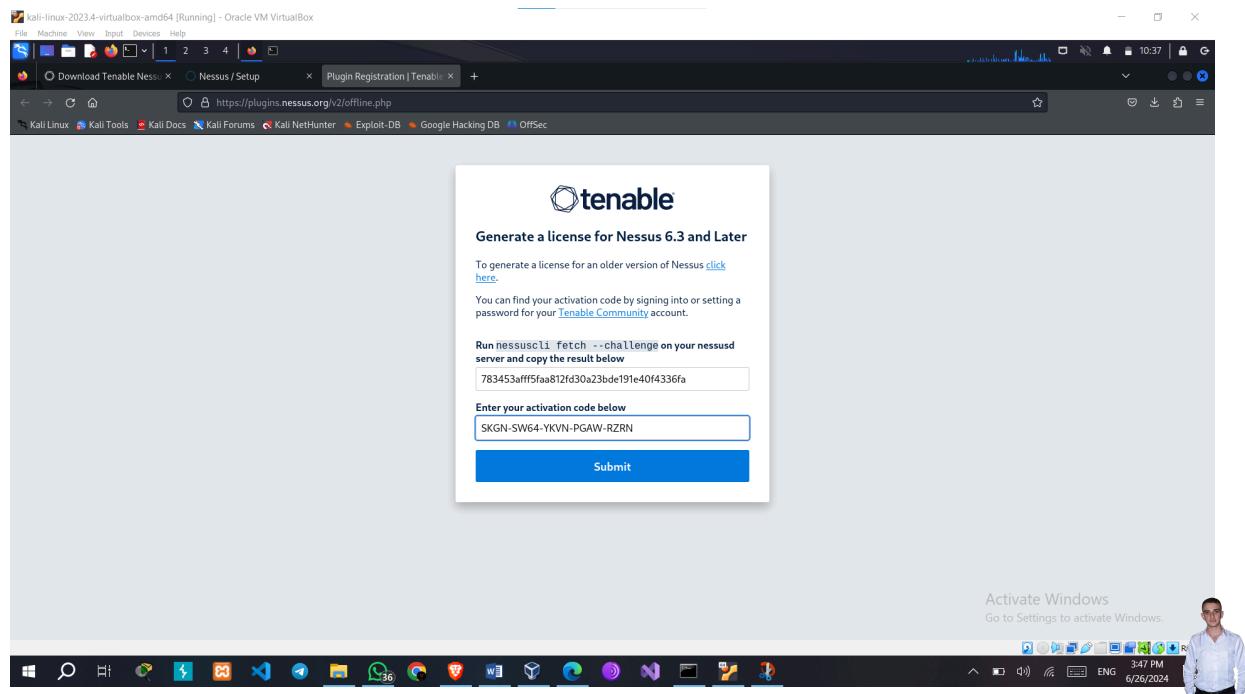
Copy the challenge code and select Offline Registration



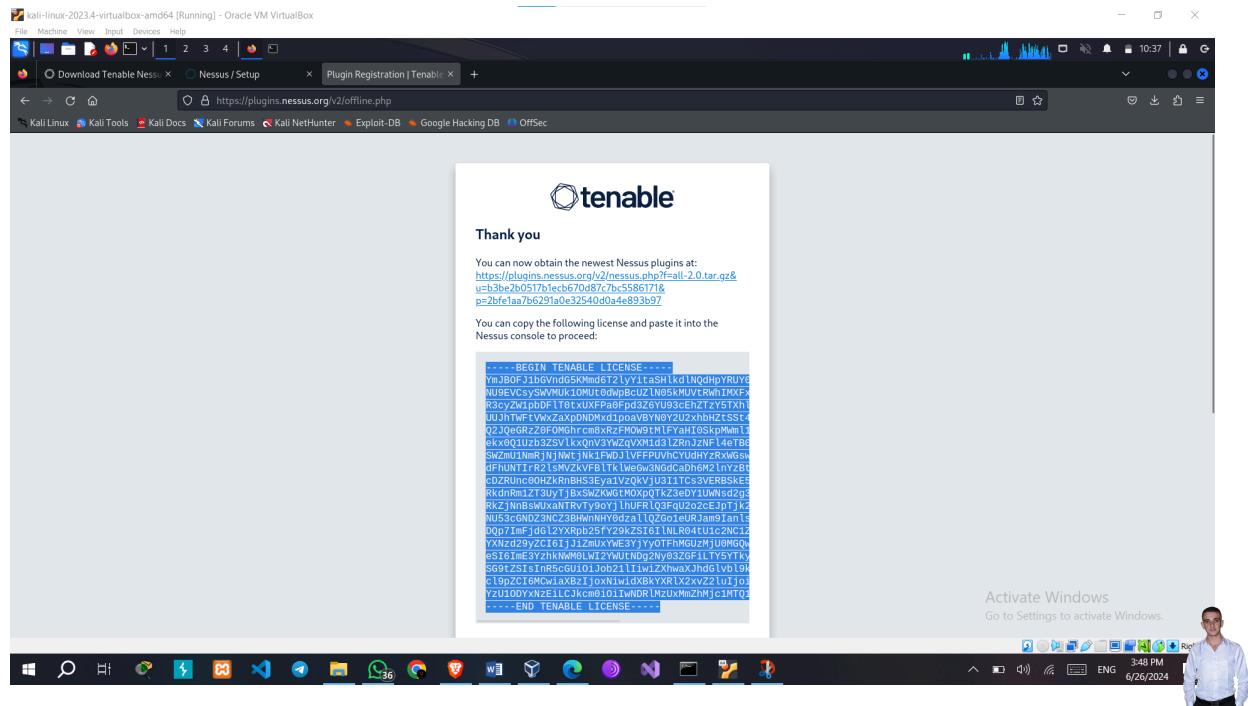
Copy your code to Activate Your Nessus Essentials License



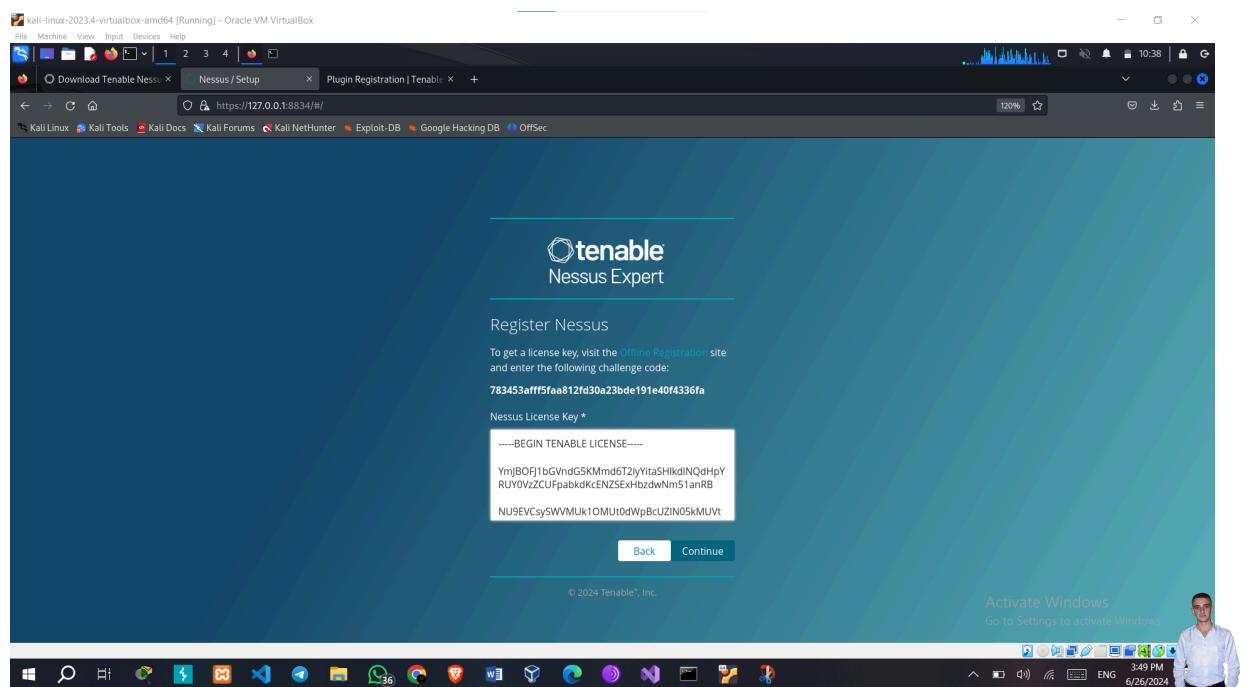
Copy your codes in the correct boxes and submit.



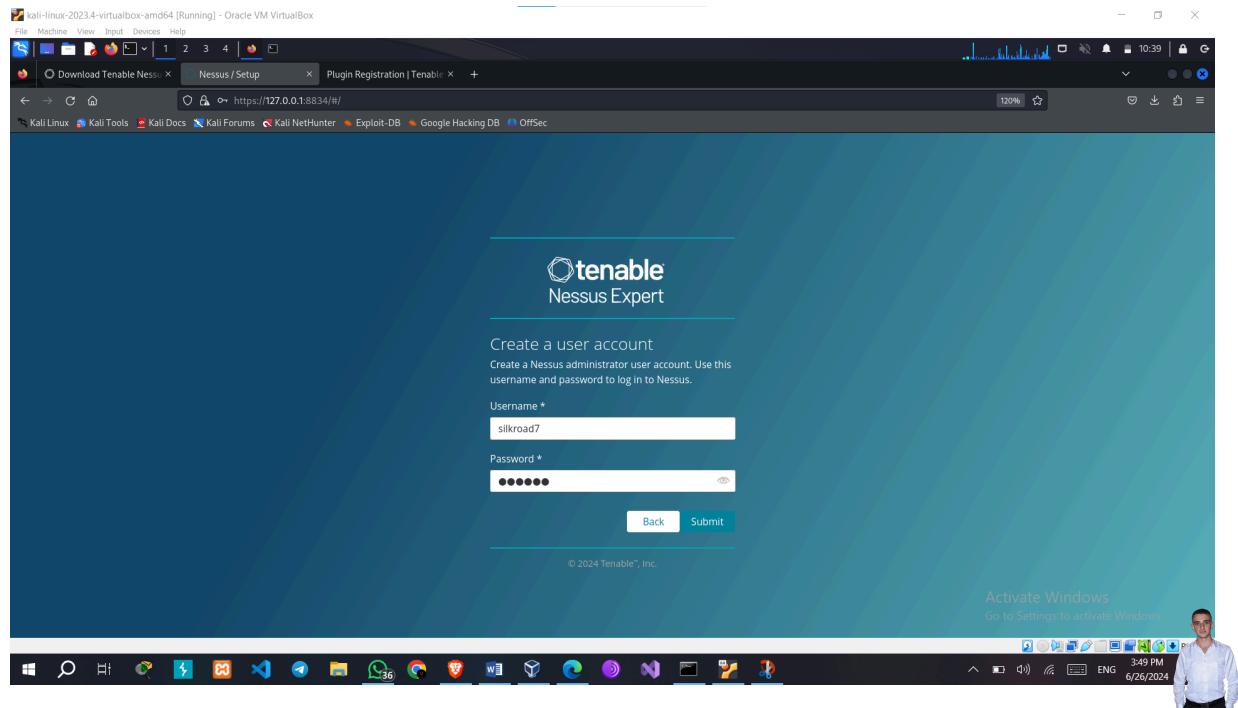
Copy the license code.



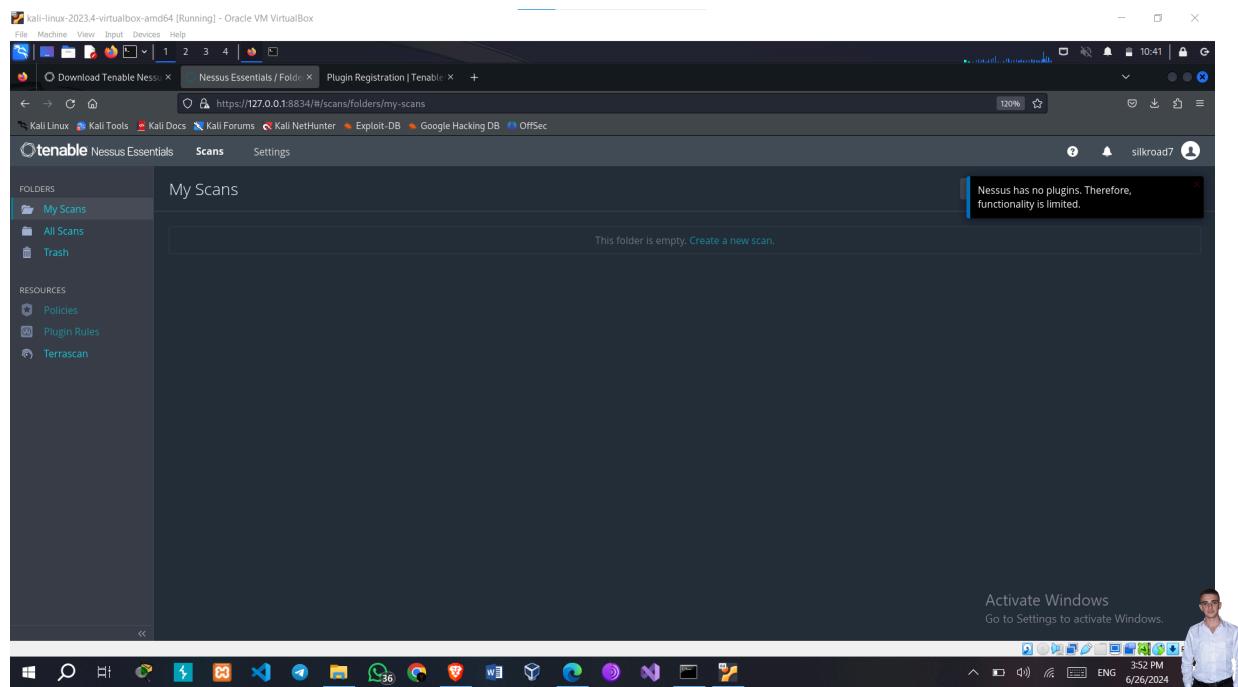
Paste it under Nessus License Key, and click continue



Create Username & Password for Nessus



Nessus has started



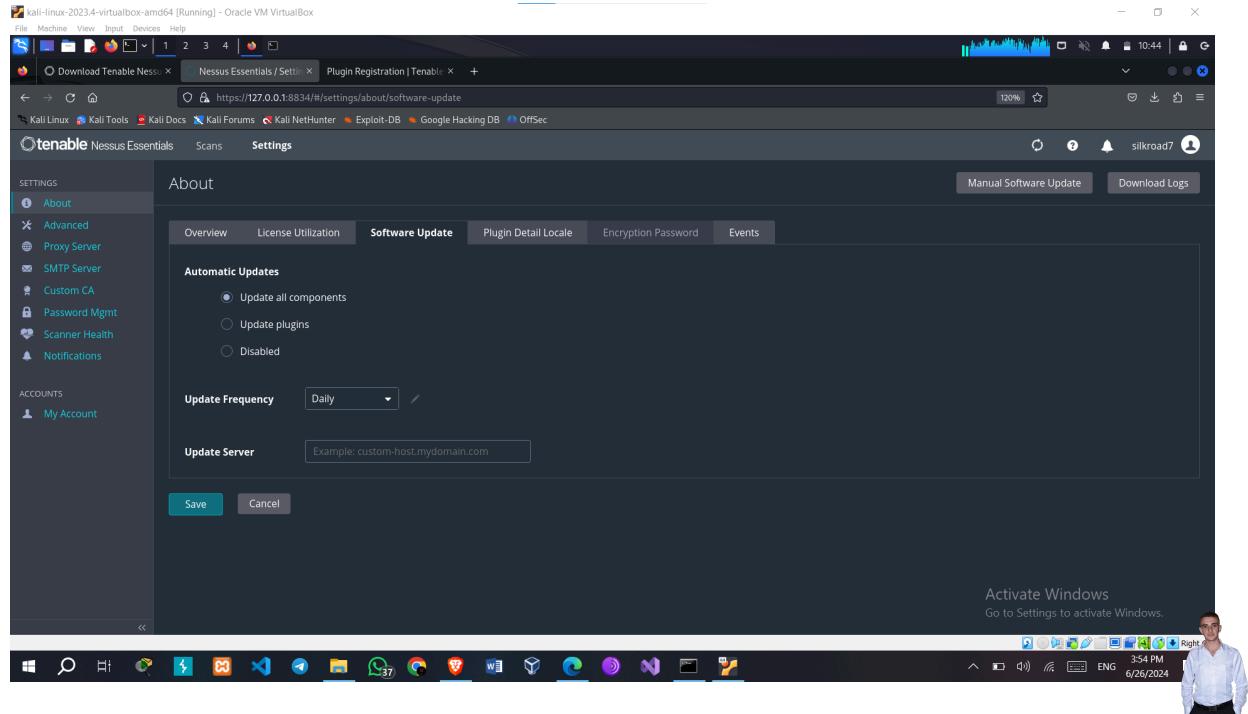
Go to settings

The screenshot shows a web browser window titled "kali-linux-2023.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The URL is <https://127.0.0.1:8834/#/settings/about>. The page is titled "About" and has tabs for Overview, License Utilization, Software Update, Plugin Detail Locale, Encryption Password, and Events. The "Overview" tab is selected. It displays information about Nessus Essentials, including Version 10.7.4 (#55) LINUX, Licensed Hosts 0 of 16 used, and various plugin details like Last Updated N/A, License Expiration June 25, 2029, and Activation Code SKGN-SW64-YKVN-PGAW-RZRN. A message on the right states: "Nessus has no plugins. Therefore, functionality is limited." The left sidebar shows sections for SETTINGS (About, Advanced, Proxy Server, SMTP Server, Custom CA, Password Mgmt, Scanner Health, Notifications), ACCOUNTS (My Account), and a navigation bar with links like Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

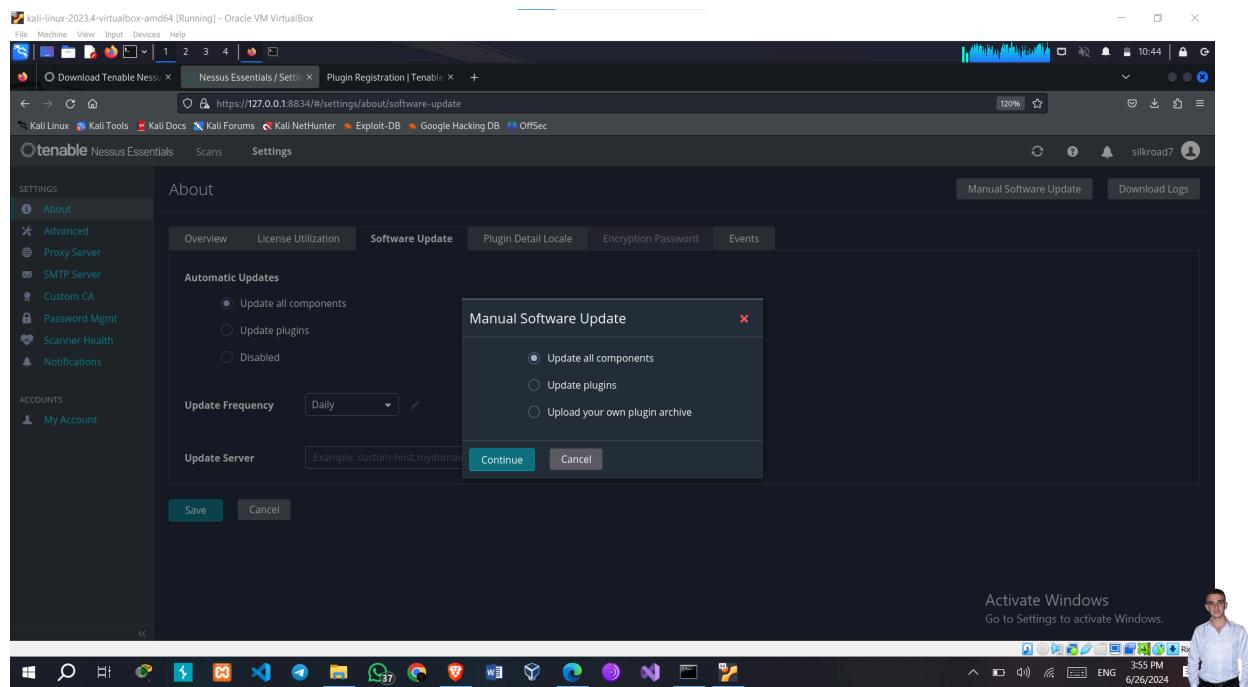
Select Software Update

The screenshot shows the same web browser window from the previous screenshot, but the "Software Update" tab is now selected. The page title is "About" and the tabs include Overview, License Utilization, Software Update, Plugin Detail Locale, Encryption Password, and Events. The "Software Update" tab is selected. It shows options for "Automatic Updates" with three radio buttons: "Update all components" (unchecked), "Update plugins" (unchecked), and "Disabled" (checked). Below this is a "Update Server" input field with the placeholder "Example: custom-host.mydomain.com". At the bottom are "Save" and "Cancel" buttons. The right side of the page still displays the message: "Nessus has no plugins. Therefore, functionality is limited." The left sidebar and navigation bar remain the same as in the first screenshot.

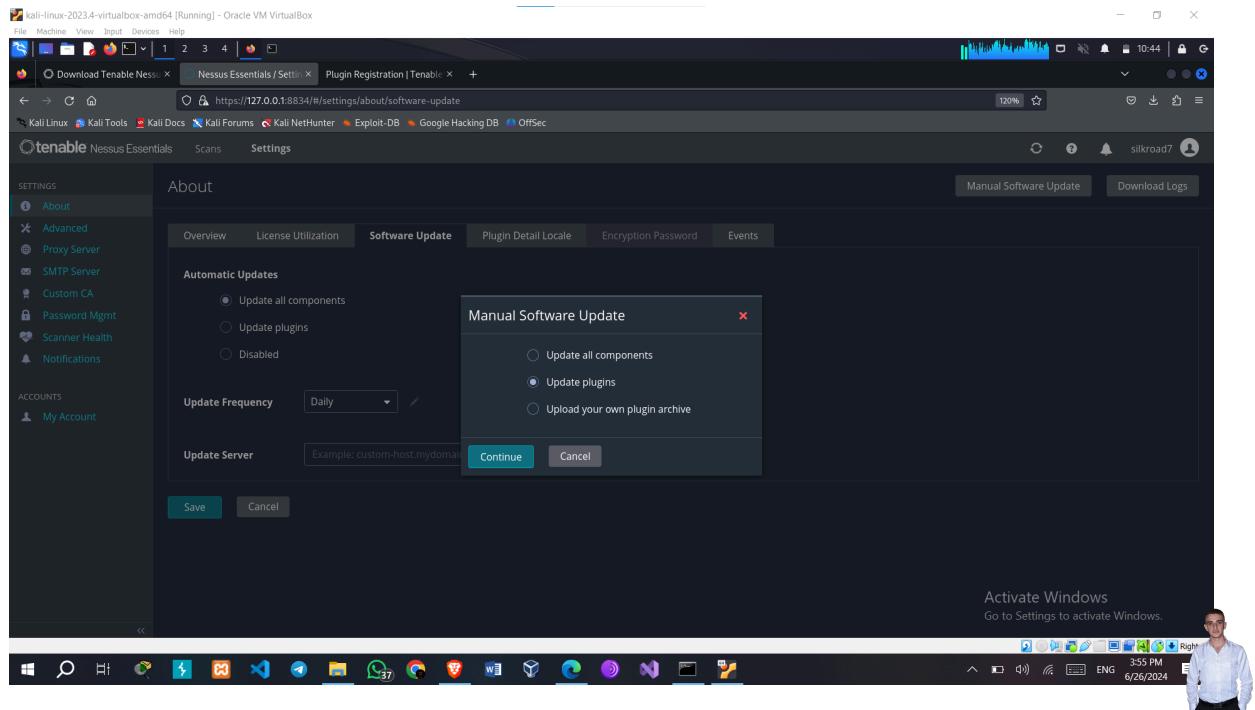
Select Update all components



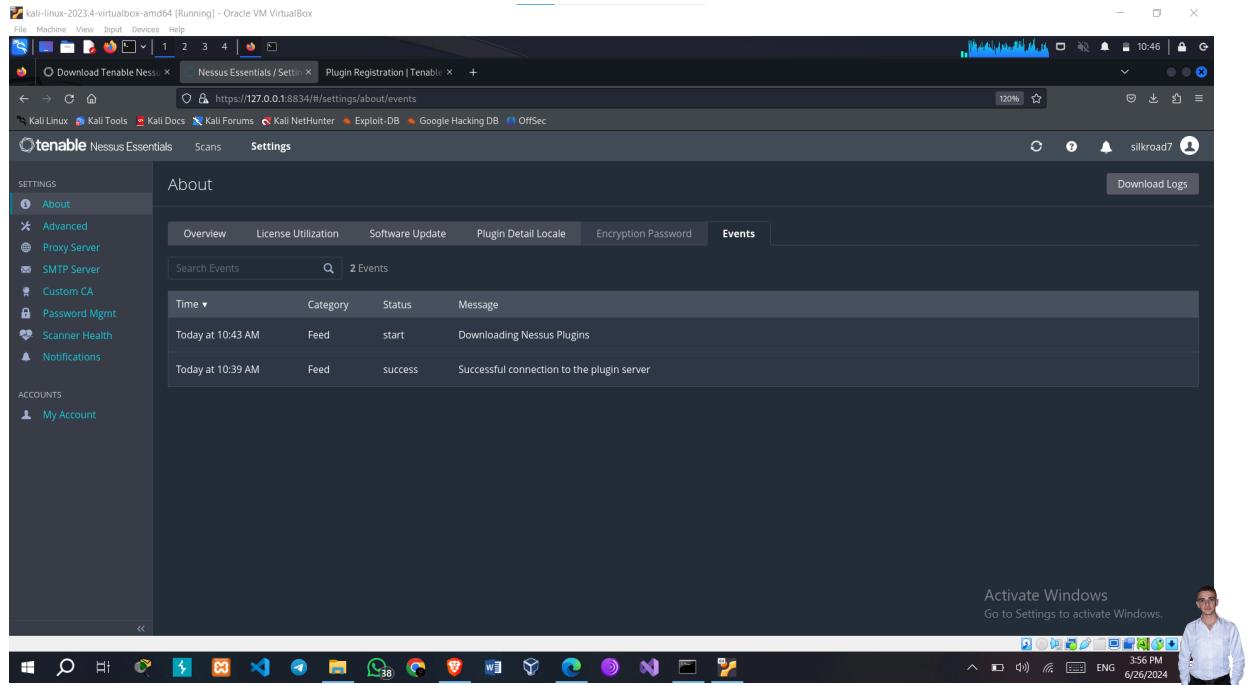
Go to Manual Software Update Right in the top



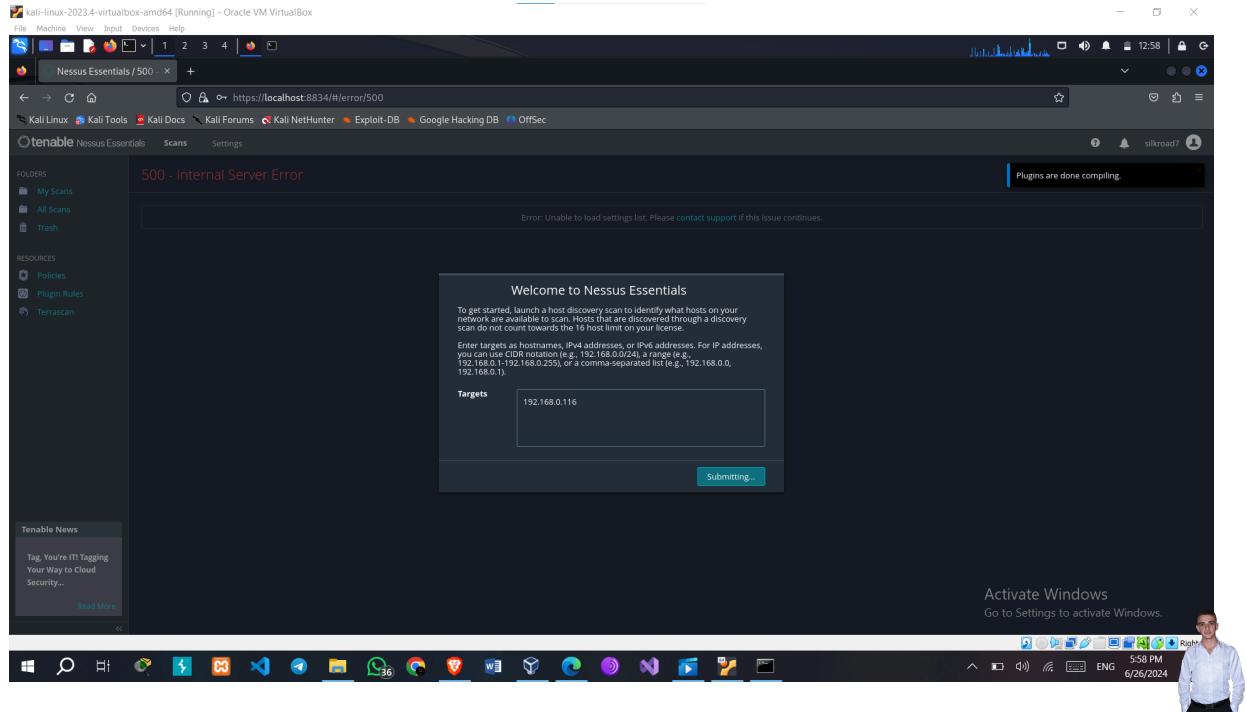
Update plugins



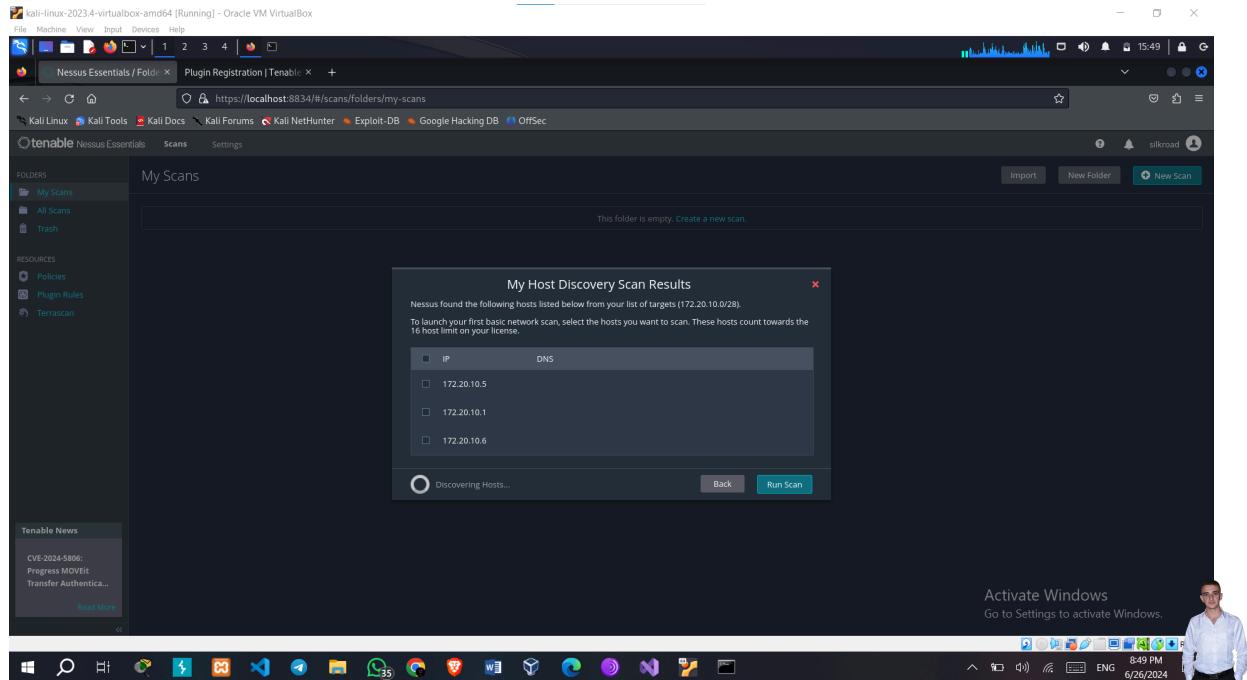
Wait Until the Update is finished



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 screenshot shows the Tenable Nessus Essentials interface. On the left, there's a sidebar with 'FOLDERS' (My Scans, All Scans, Trash), 'RESOURCES' (Policies, Plugin Rules, Terrascan), and 'Tenable News'. The main area displays 'My Basic Network Scan' results. Under 'Vulnerabilities', there are two entries:

Severity	CVSS	VPR	Name	Family	Count
INFO			DCE Services Enumeration	Windows	8
INFO			Nessus SYN scanner	Port scanners	1

On the right, 'Scan Details' show the policy as 'Basic Network Scan', status as 'Running', severity baseline as 'CVSS v3.0', scanner as 'Local Scanner', and start time as 'Today at 3:49 PM'. A pie chart indicates the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (light gray).

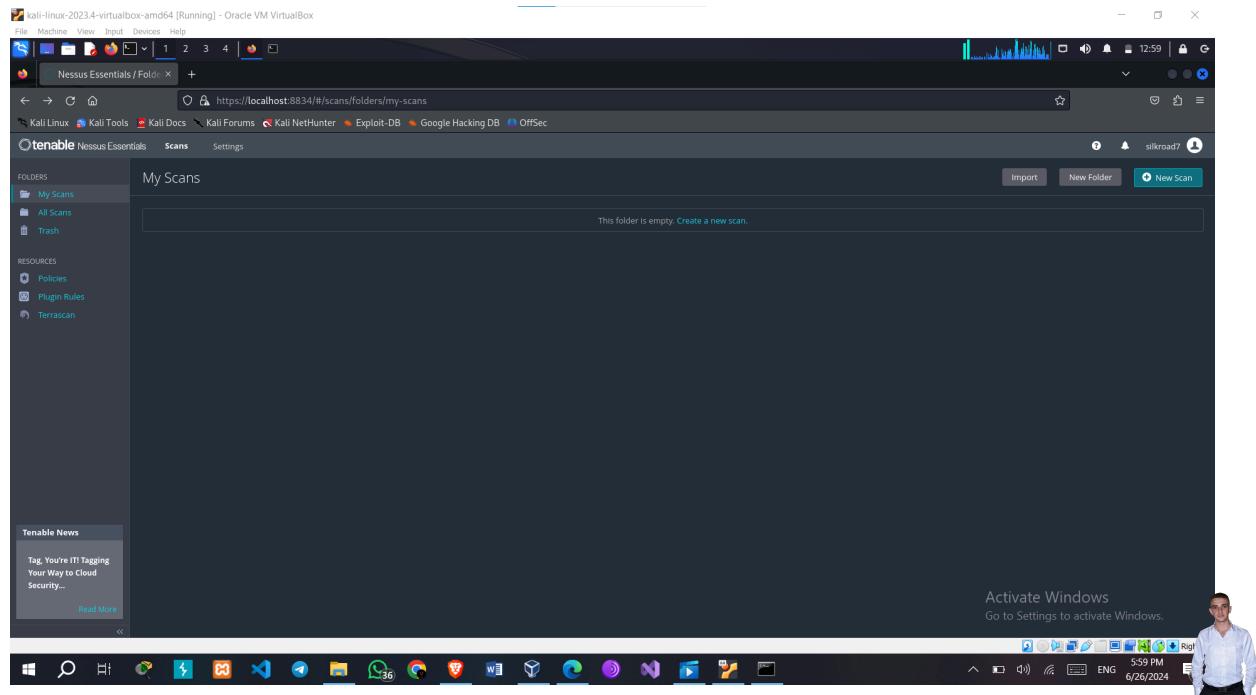
The description of the vulnerability

The screenshot shows the detailed description of the 'DCE Services Enumeration' vulnerability from the previous scan. The 'Description' section states: 'By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote portpipe.' The 'Output' section shows the command-line output of the enumeration:

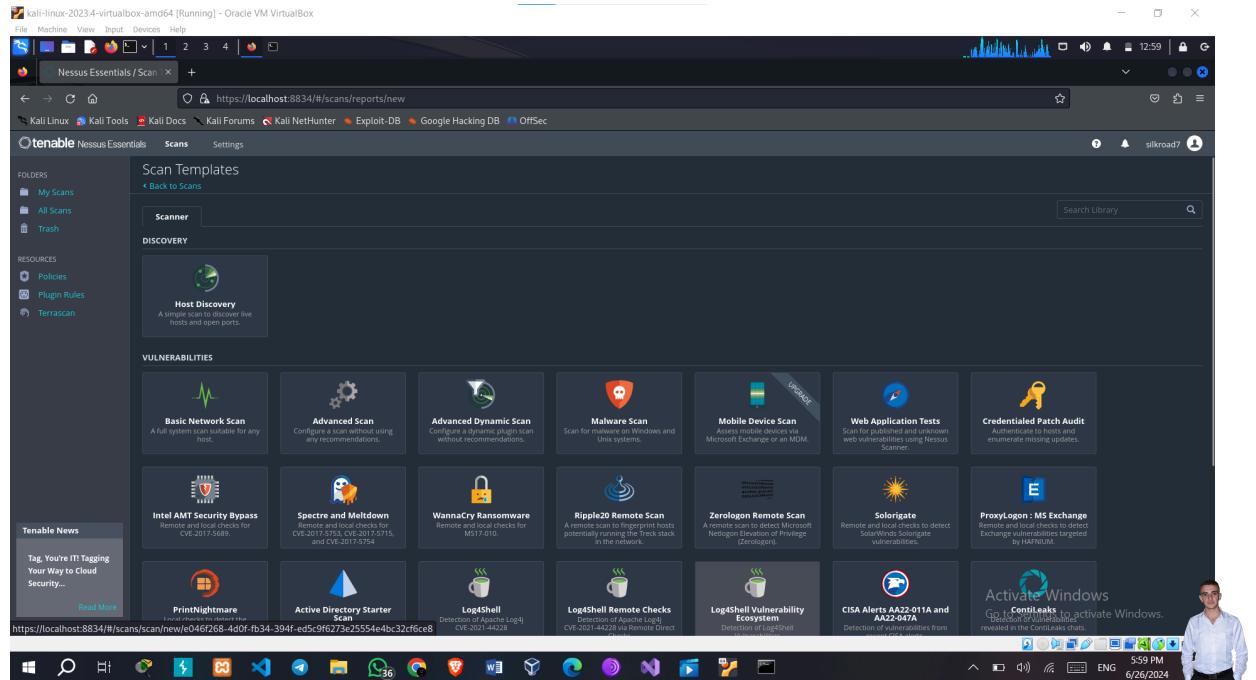
```
The following DCERPC services are available locally :  
Object UUID : 00000000-0000-0000-0000-000000000000  
UUID : 9e6cb297-cb24-4460-8a2a-bfdeaf2f10bba, version 1.0  
Description : Unknown RPC service  
Implementation : Local RPC Interface  
Type : Local RPC service  
Named pipe : LRPC-23a7de02288027ce1  
more...  
To see debug logs, please visit individual host
```

The 'Plugin Details' panel provides metadata: Severity: Info, ID: 10736, Version: 1.57, Type: combined, Family: Windows, Published: August 26, 2001, Modified: October 4, 2021. The 'Risk Information' panel notes 'Risk Factor: None'. The 'Vulnerability Information' panel includes 'Asset Inventory: True'.

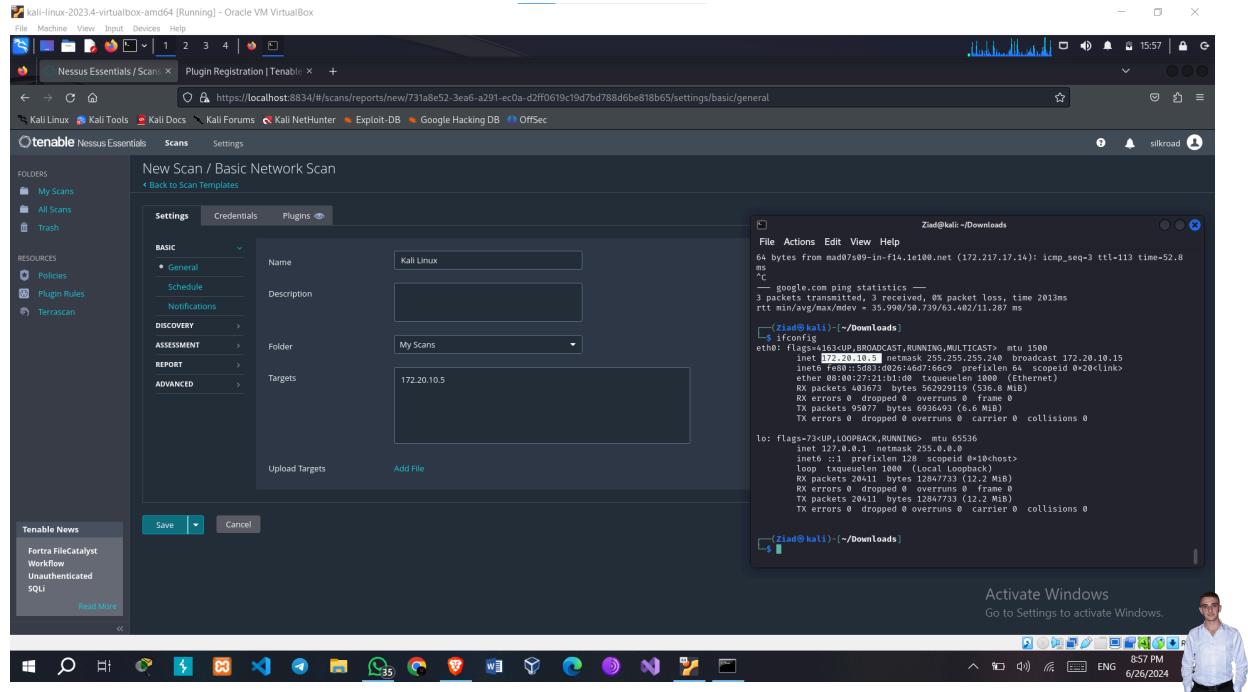
Or, go to 'Scan' at the top, and click on 'New Scan'



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/>