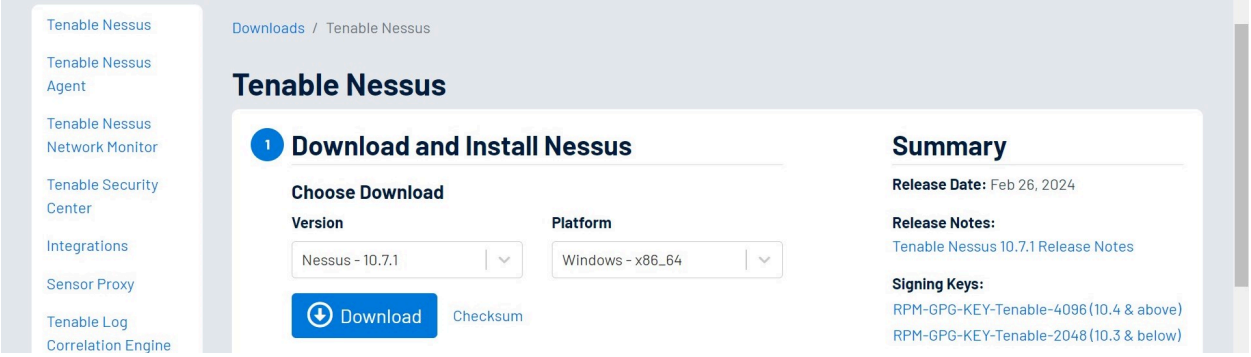
Name: Cristian Barreno

EXERCISE 2 – Vulnerability Scanning and Management

Task 1

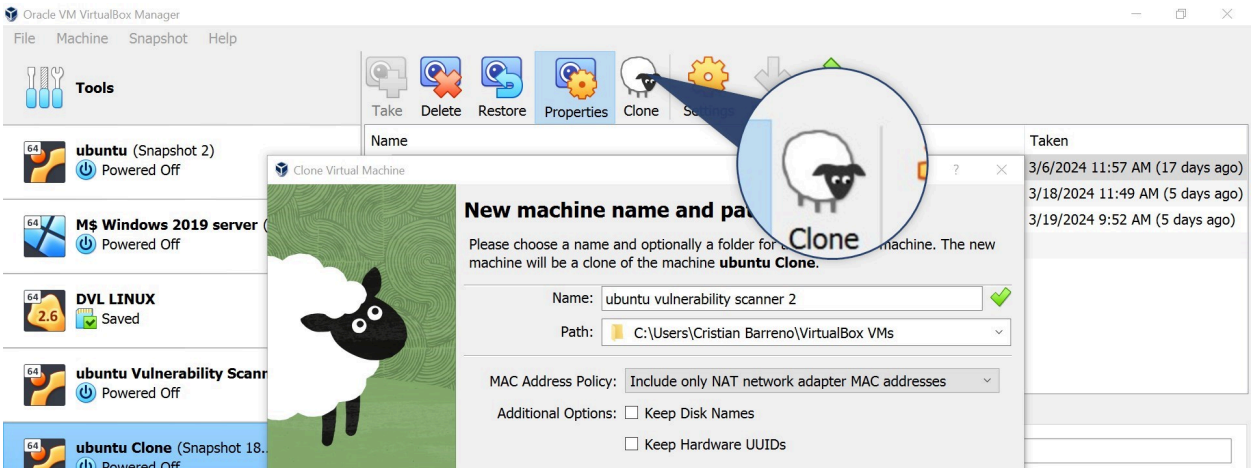


I downloaded Nessus 10.7.0 on the Linux – Ubuntu – amd64 Platform on my host operating system. The file is my download folder.

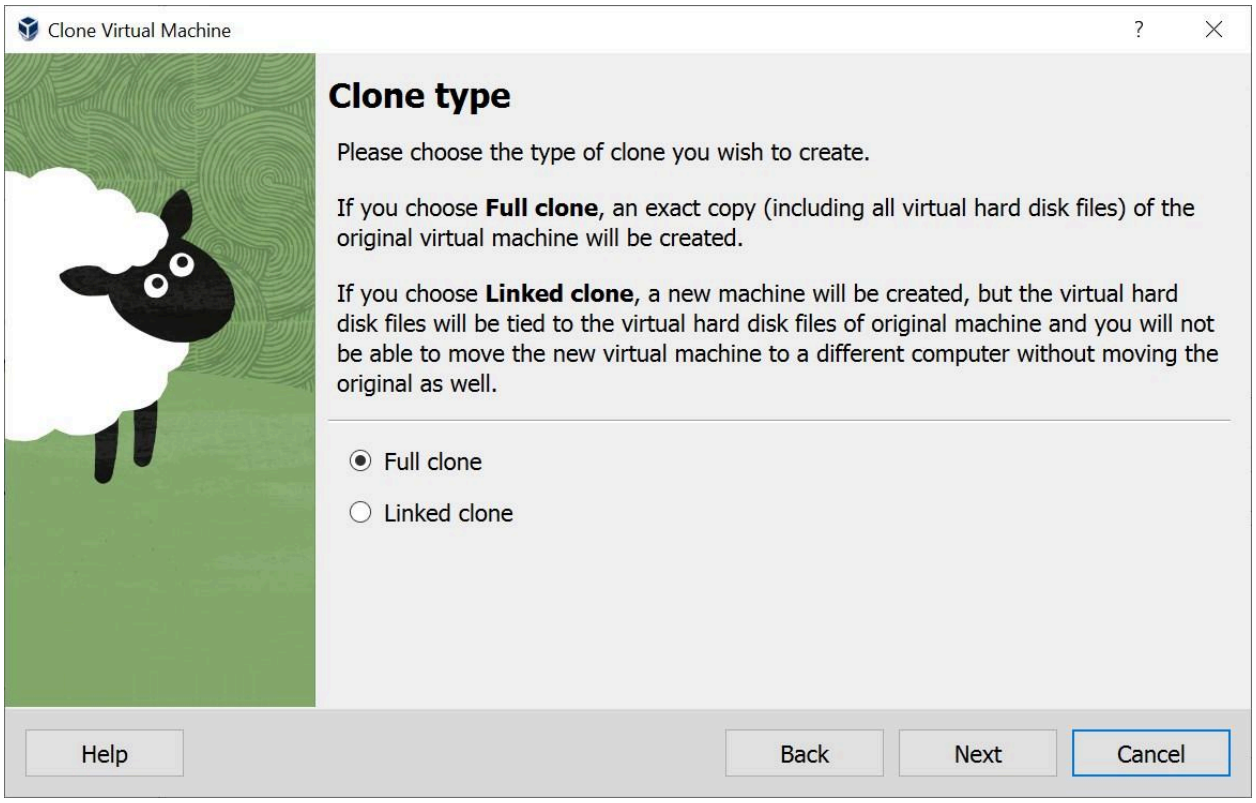
Next I SCP (Secure copy) the file to my Linux guest VM.

Task 2
Clone your Ubuntu server VM.

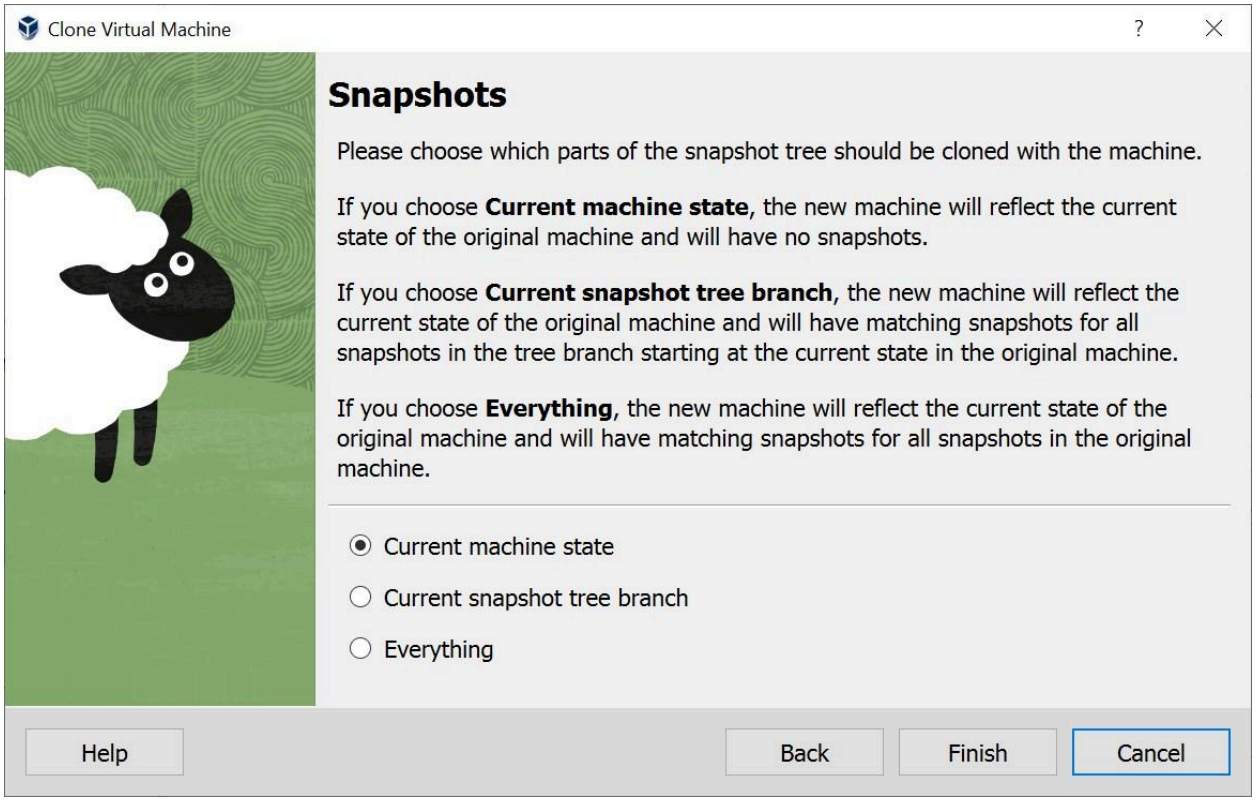
Cloning is really easy, first I selected the linux server I want to clone, next I click clone. On the next window change the name to Ubuntu Vulnerability scanner, and click next.



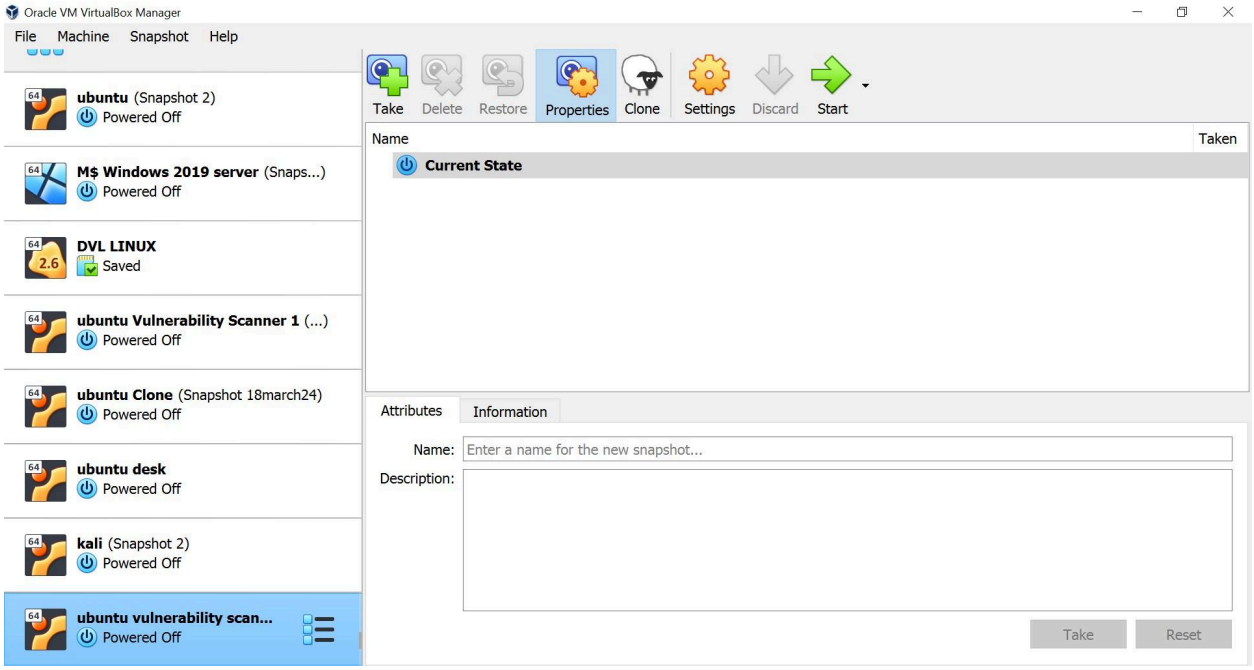
Next i selected Full clone



And lastly, “current machine state”.



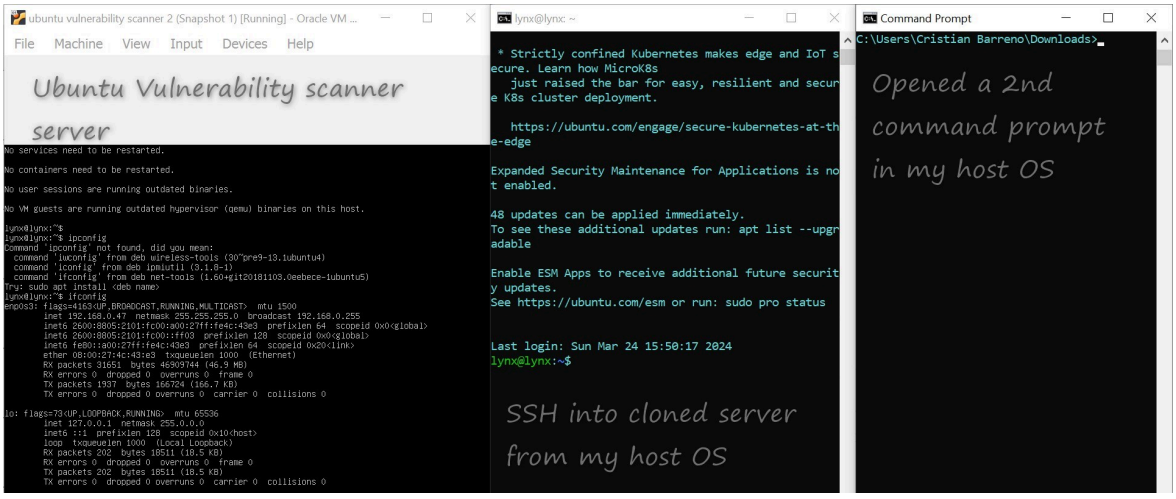
Cloning didn't take a lot of time. It was much faster than installing a server from zero. The next thing i did was double check the processor, RAM, and networking configurations



Task 3

Prerequisites

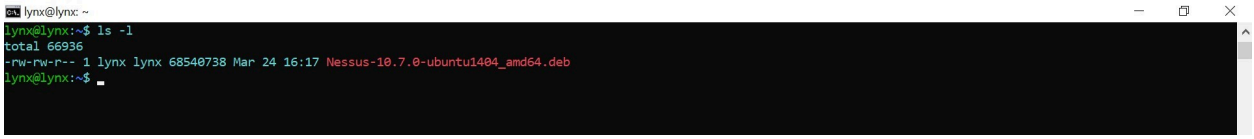
- Ubuntu Server 22.04 Installed, Updated, Upgraded and running in Virtual Box
- Ubuntu Guest VM Networking settings is set to Bridged Mode in Virtual Box
- The Ubuntu Guest VM is running
- Have an open CLI in your HOST OS, and test that you can SSH into the Guest VM



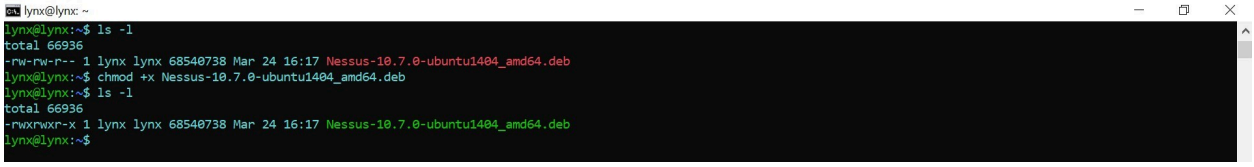
In the second command prompt i navigated to my downloads folder, and then i used dir *.deb to find Nessus 10.7.0 on the Linux – Ubuntu – amd64.deb.
Next I used the secure copy protocol to copy the file into my linux server.

Task 4

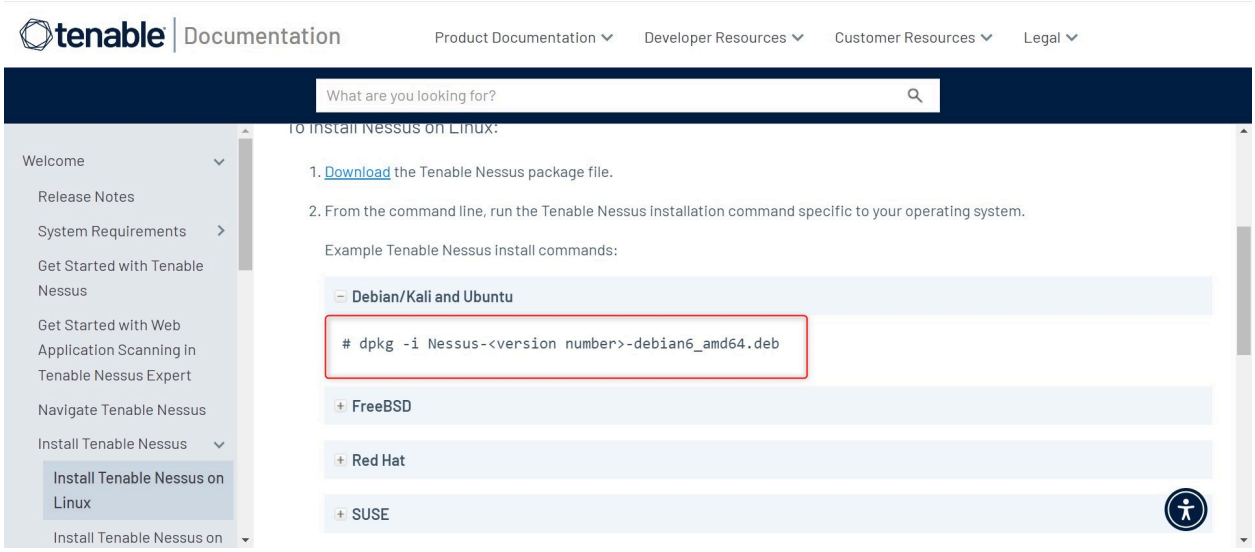
In the screenshot below i verified that the file is in my home folder



Below I changed the permissions for the file so it can be executed. The three sets of permissions characters are r (read), w (write), and x (execute) corresponding to the three types of users : owner, group, and others.
I used the symbolic method below. This method uses three different symbols: + (adds the specified permission), - (removes the specified permission), and = (Sets the specified permission explicitly, removing any others)

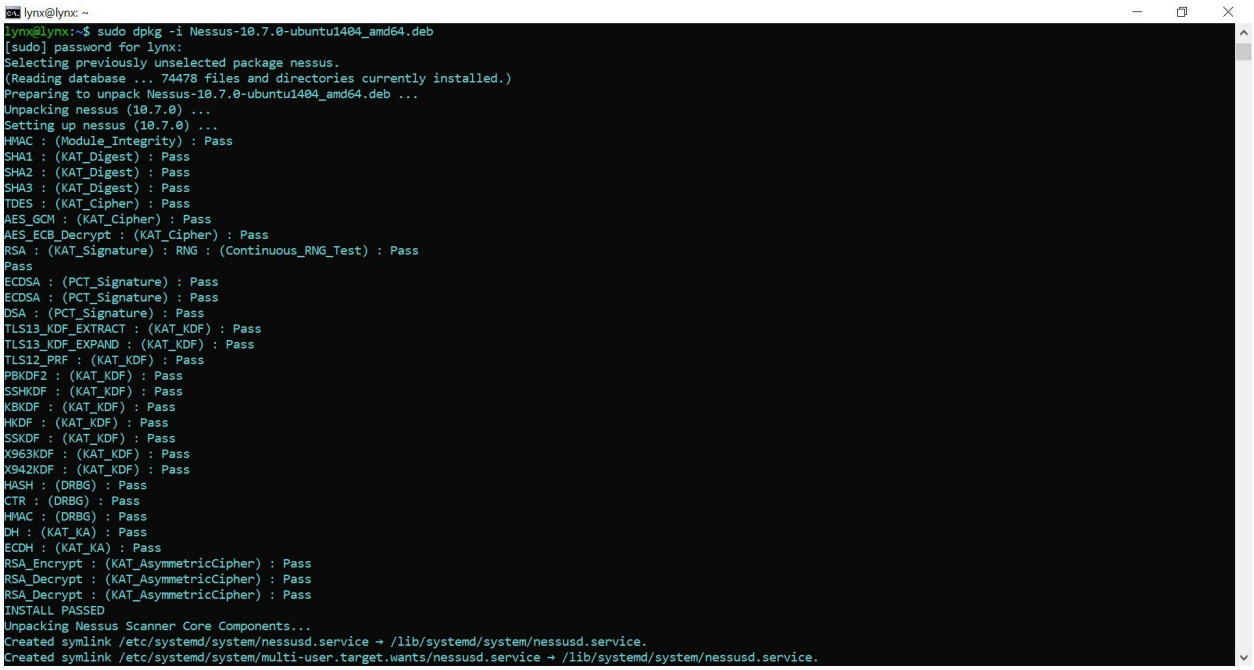


Installing Nessus via dpkg

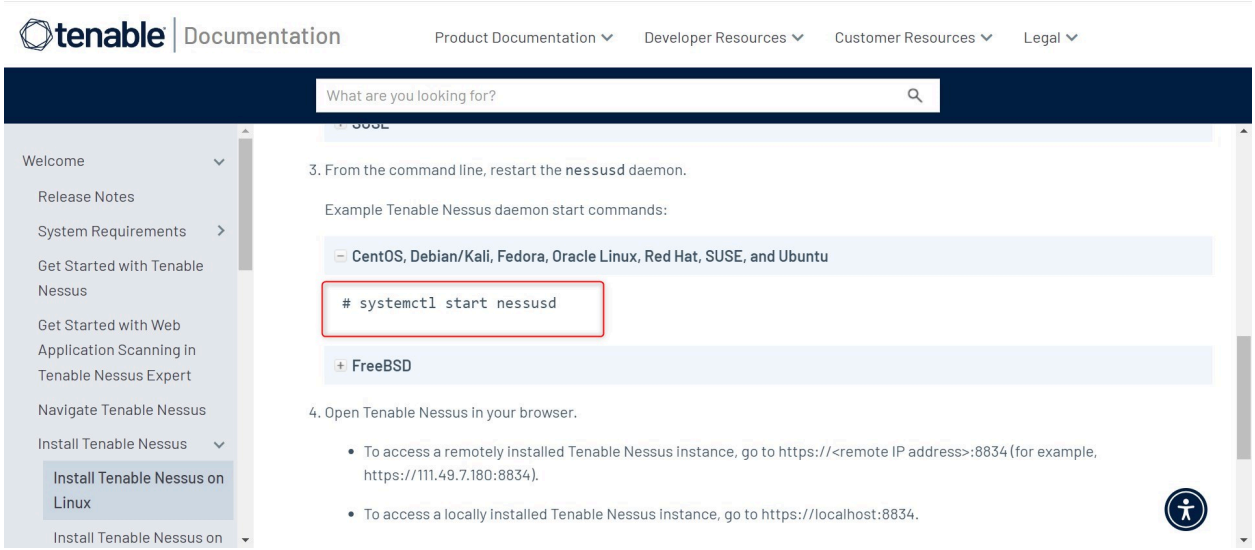


The guide from the Nessus website is telling us to install the Nessus Debian package.

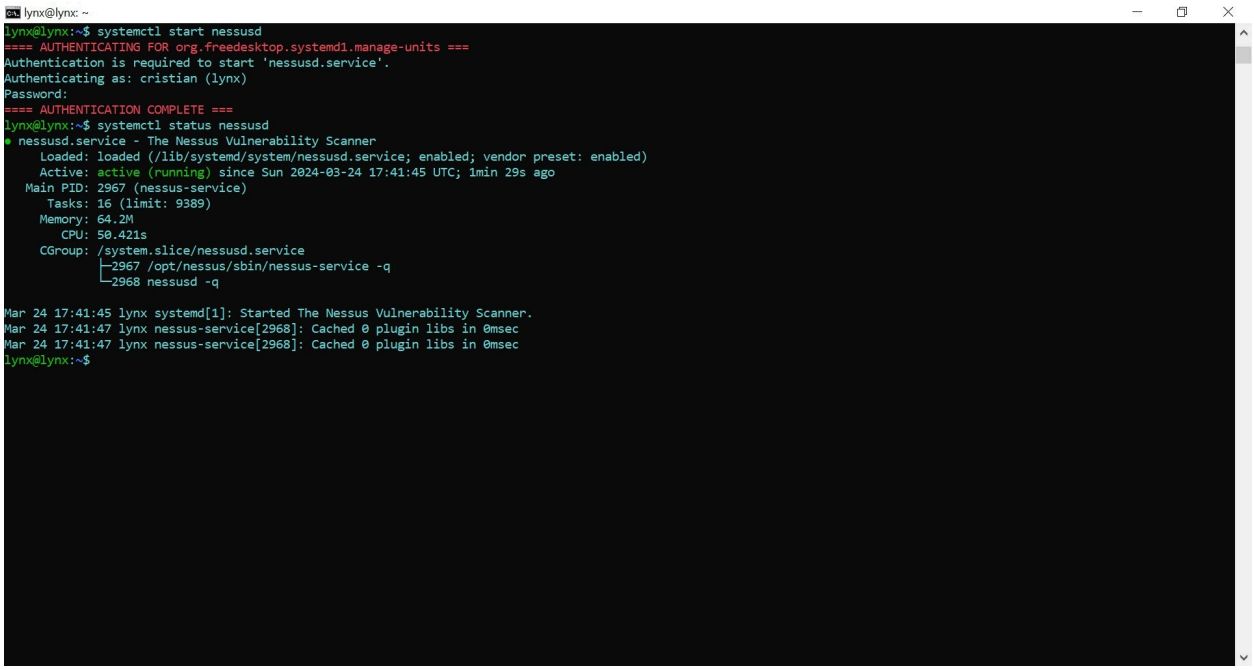
I used super user do (sudo), then the package management system used by debian based linux distributions (dpkg), then -i for install, followed by the file. Towards the bottom of the screen I can see that the installation was successful.



The next step from the Nessus installation guide is to start the service.

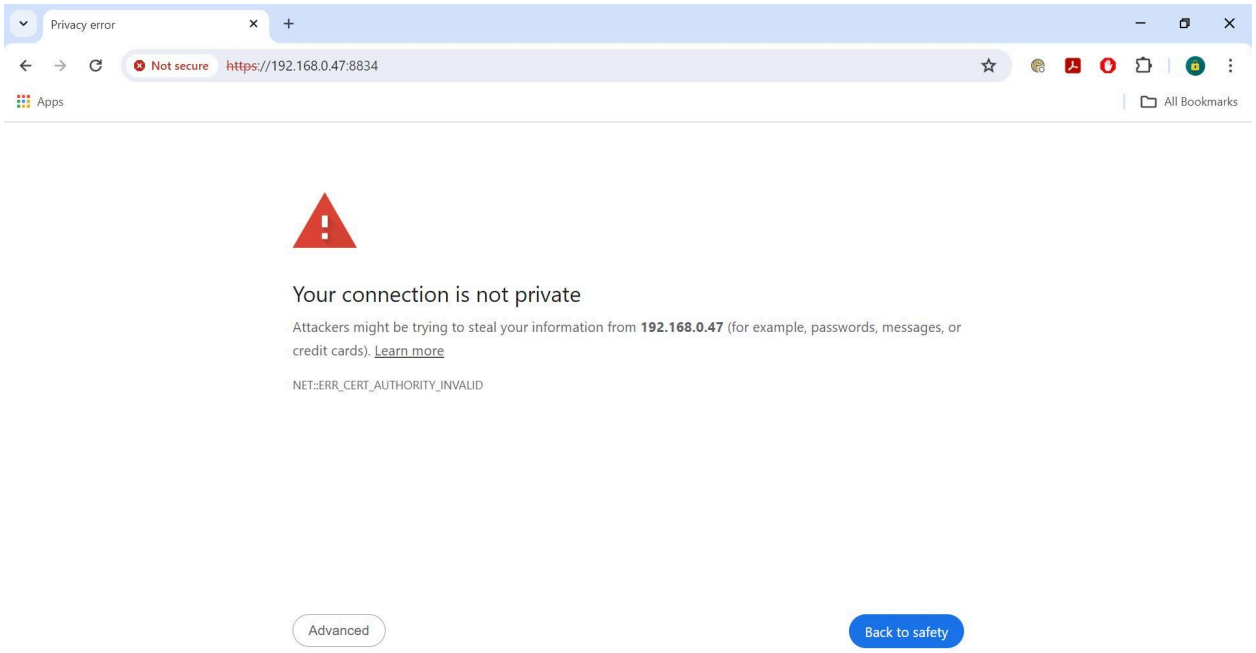


I ran the command sudo systemctl start nessusd, and after I entered my password, I didn't get any feedback. I entered systemctl status nessusd to ensure that it's running.



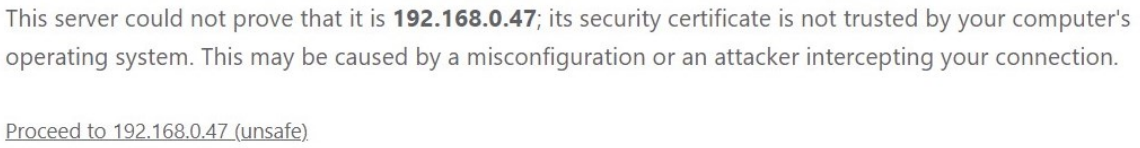
Step 4

Open Tenable Nessus in your browser

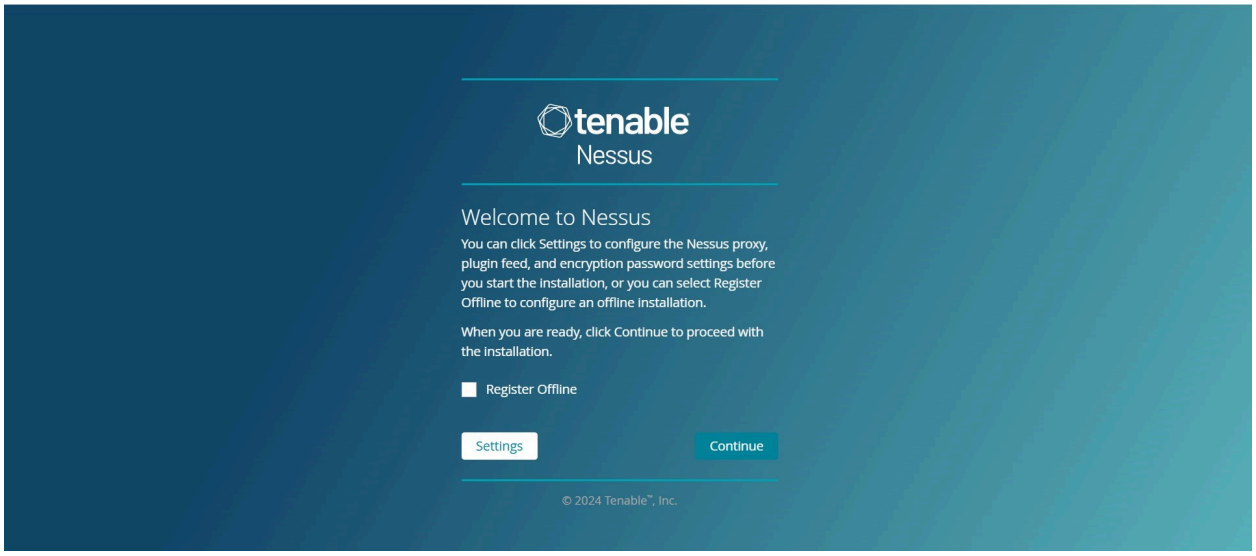


In the screenshot above i entered https// followed by the local ip of the web interface for the Nessus Server, followed by : (colon), and the port 8834.
I got a “Your connection is not private” window”.

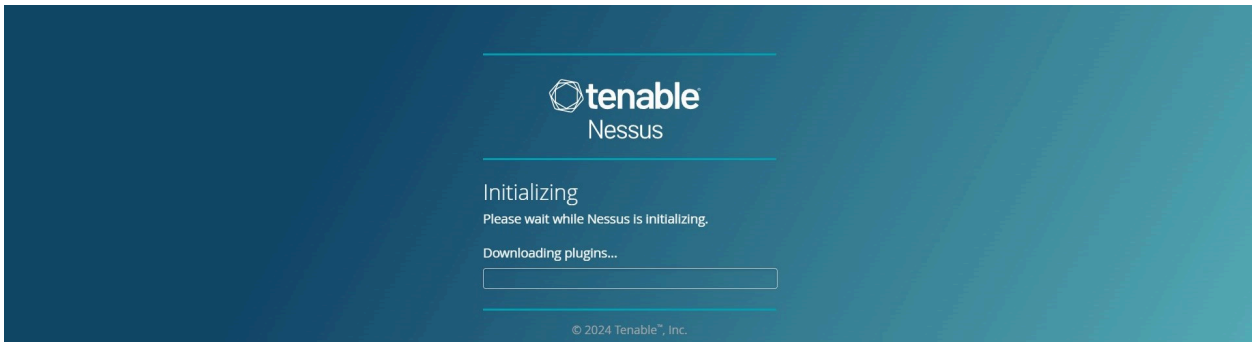
In the screenshot below i clicked on advanced, and then proceed to 192.168.0.47



I successfully made it to the website of Nessus Vulnerability scanner



I registered for an activation code, and in the following page i entered the activation code i got on my email.



Now I made it to the Nessus Vulnerability scanner homepage. I see the plugins are still compelling. Right now all the CVE (Common Vulnerabilities and Exposures) are downloading, and it might take a while.