

Name: Cristian Barreno

## EXERCISE 2 – Vulnerability Scanning and Management

### Task 1

The screenshot shows the Tenable Nessus download page. On the left, there's a sidebar with links to various Tenable products. The main area is titled "Tenable Nessus" and contains a section for "Download and Install Nessus". It has fields for "Version" (set to "Nessus - 10.7.1") and "Platform" (set to "Windows - x86\_64"). Below these are "Download" and "Checksum" buttons. To the right, there's a "Summary" box with release details: "Release Date: Feb 26, 2024", "Release Notes: Tenable Nessus 10.7.1 Release Notes", and "Signing Keys: RPM-GPG-KEY-Tenable-4096 (10.4 & above), RPM-GPG-KEY-Tenable-2048 (10.3 & below)".

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.

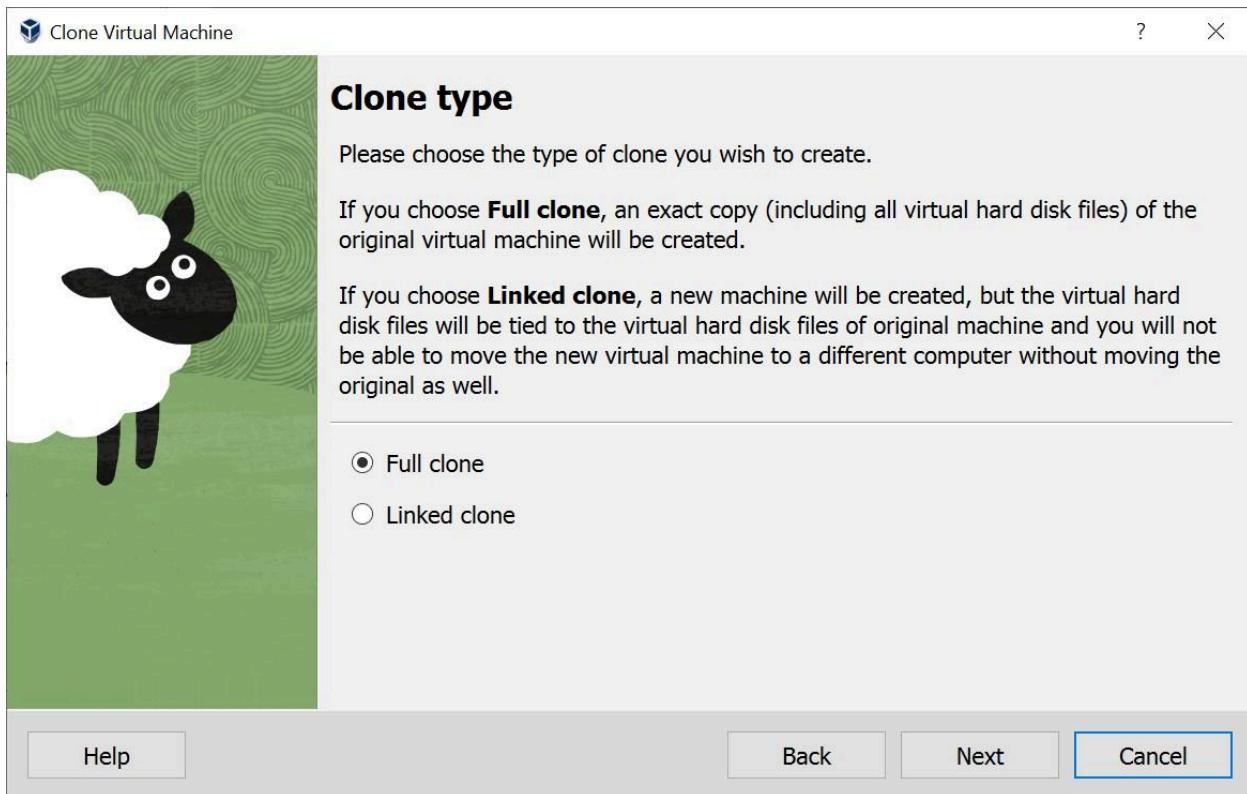
### Task 2

#### Clone your Ubuntu server VM.

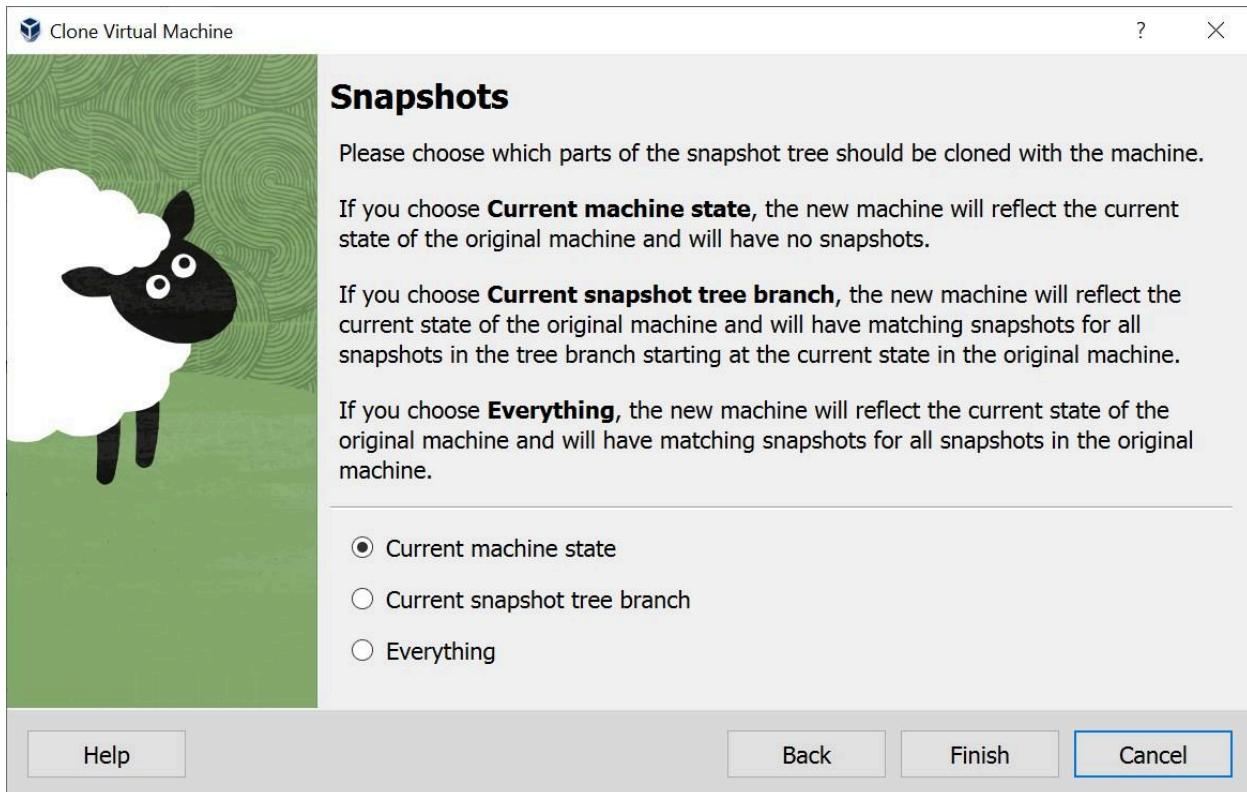
Cloning is really easy, first I selected the linux server I want to clone, next I click clone. On the next window change the name to Ubuntu Vulnerability scanner, and click next.

The screenshot shows the Oracle VM VirtualBox Manager interface. On the left, a list of existing VMs includes "ubuntu (Snapshot 2)", "MS Windows 2019 server", "DVL LINUX 2.6", "ubuntu Vulnerability Scanner", and "ubuntu Clone (Snapshot 18...)". In the center, a "Clone Virtual Machine" dialog box is open. It features a cartoon sheep icon and a message: "Please choose a name and optionally a folder for the new machine. The new machine will be a clone of the machine **ubuntu Clone**". The "Name" field is set to "ubuntu vulnerability scanner 2" and the "Path" is set to "C:\Users\Cristian Barreno\VirtualBox VMs". At the bottom, there are options for "MAC Address Policy" (set to "Include only NAT network adapter MAC addresses"), "Additional Options" (with checkboxes for "Keep Disk Names" and "Keep Hardware UUIDs"), and a "Clone" button. A blue callout points to the "Clone" button.

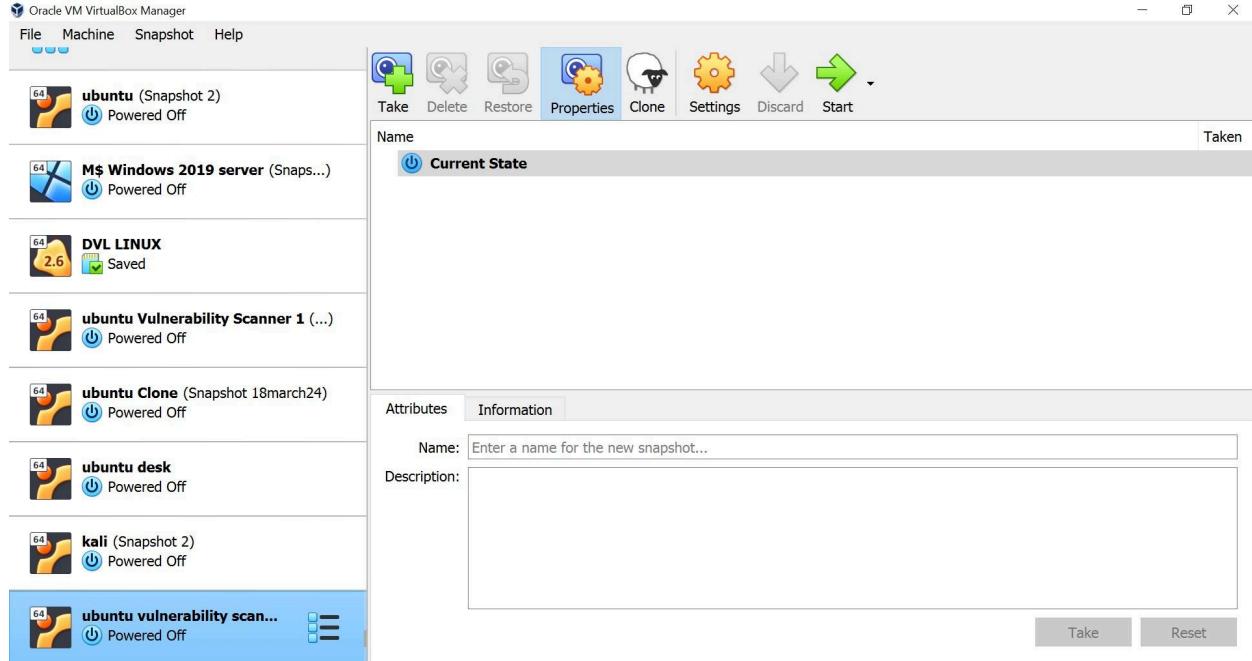
Next i selected Full clone



And lastly, "current machine state".



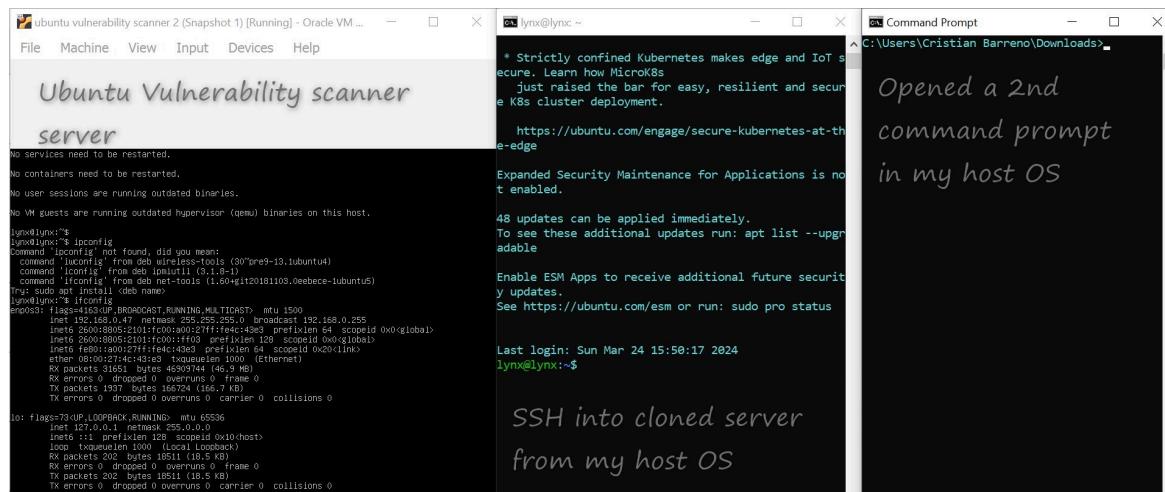
Cloning didn't take a lot of time. It was much faster than installing a server from zero. The next thing i did was double check the processor, RAM, and networking configurations



## 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.



```
C:\ Command Prompt
C:\Users\Cristian Barreno\Downloads>dir *.deb
Volume in drive C is Windows
Volume Serial Number is 5EB7-BA34

Directory of C:\Users\Cristian Barreno\Downloads

02/27/2024  12:28 PM           68,540,738 Nessus-10.7.0-ubuntu1404_amd64.deb
   1 File(s)      68,540,738 bytes
   0 Dir(s)  777,431,719,936 bytes free

C:\Users\Cristian Barreno\Downloads>scp Nessus-10.7.0-ubuntu1404_amd64.deb lynx@192.168.0.47:
Password:
Verification code:
Nessus-10.7.0-ubuntu1404_amd64.deb                                         100%   65MB 104.3MB/s   00:00

C:\Users\Cristian Barreno\Downloads>
```

## Task 4

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



```
lynx@lynx: ~$ ls -l
total 66936
-rw-rw-r-- 1 lynx lynx 68540738 Mar 24 16:17 Nessus-10.7.0-ubuntu1404_amd64.deb
lynx@lynx: ~$ chmod +x Nessus-10.7.0-ubuntu1404_amd64.deb
lynx@lynx: ~$ ls -l
total 66936
-rwxrwxr-x 1 lynx lynx 68540738 Mar 24 16:17 Nessus-10.7.0-ubuntu1404_amd64.deb
lynx@lynx: ~$
```

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)



```
lynx@lynx: ~$ ls -l
total 66936
-rw-rw-r-- 1 lynx lynx 68540738 Mar 24 16:17 Nessus-10.7.0-ubuntu1404_amd64.deb
lynx@lynx: ~$ chmod +x Nessus-10.7.0-ubuntu1404_amd64.deb
lynx@lynx: ~$ ls -l
total 66936
-rwxrwxr-x 1 lynx lynx 68540738 Mar 24 16:17 Nessus-10.7.0-ubuntu1404_amd64.deb
lynx@lynx: ~$
```

## Installing Nessus via dpkg

The screenshot shows a navigation sidebar on the left with links like Welcome, Release Notes, System Requirements, Get Started with Tenable Nessus, Get Started with Web Application Scanning in Tenable Nessus Expert, Navigate Tenable Nessus, Install Tenable Nessus (selected), Install Tenable Nessus on Linux (selected), and Install Tenable Nessus on [other]. At the top, there's a search bar and links for Product Documentation, Developer Resources, Customer Resources, and Legal. The main content area is titled "To Install Nessus on Linux." It lists steps: 1. Download the Tenable Nessus package file, 2. From the command line, run the Tenable Nessus installation command specific to your operating system. Below this, it says "Example Tenable Nessus install commands:" and shows a list of operating systems: Debian/Kali and Ubuntu (selected), FreeBSD, Red Hat, and SUSE. A red box highlights the command for Debian/Kali and Ubuntu: "# dpkg -i Nessus-<version number>-debian6\_amd64.deb".

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.

```
lynx@lynx:~  
lynx@lynx:~$ sudo dpkg -i Nessus-10.7.0-ubuntu1404_amd64.deb  
[sudo] password for lynx:  
Selecting previously unselected package nessus.  
(Reading database ... 74478 files and directories currently installed.)  
Preparing to unpack Nessus-10.7.0-ubuntu1404_amd64.deb ...  
Unpacking nessus (10.7.0) ...  
Setting up nessus (10.7.0) ...  
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  
AES_ECB_Decrypt : (KAT_Cipher) : Pass  
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass  
Pass  
ECDSA : (PCT_Signature) : Pass  
ECDSA : (PCT_Signature) : Pass  
DSA : (PCT_Signature) : Pass  
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass  
TLS13_KDF_EXPAND : (KAT_KDF) : Pass  
TLS12_PRF : (KAT_KDF) : Pass  
TLSKDF2 : (KAT_KDF) : Pass  
SSHKDF : (KAT_KDF) : Pass  
KBKDF : (KAT_KDF) : Pass  
HKDF : (KAT_KDF) : Pass  
SSKDF : (KAT_KDF) : Pass  
X963KDF : (KAT_KDF) : Pass  
X942KDF : (KAT_KDF) : Pass  
HASH : (DRBG) : Pass  
CTR : (DRBG) : Pass  
HMAC : (DRBG) : Pass  
DH : (KAT_KA) : Pass  
ECDH : (KAT_KA) : Pass  
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass  
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass  
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass  
INSTALL PASSED  
Unpacking Nessus Scanner Core Components...  
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.  
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.
```

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

The screenshot shows a navigation sidebar on the left with links like Welcome, Release Notes, System Requirements, Get Started with Tenable Nessus, Get Started with Web Application Scanning in Tenable Nessus Expert, Navigate Tenable Nessus, Install Tenable Nessus (selected), Install Tenable Nessus on Linux (selected), and Install Tenable Nessus on ...

The main content area has a search bar at the top. A section titled "3. From the command line, restart the nessusd daemon." contains the text "Example Tenable Nessus daemon start commands:" followed by a list under "CentOS, Debian/Kali, Fedora, Oracle Linux, Red Hat, SUSE, and Ubuntu": "# systemctl start nessusd". This line is highlighted with a red box.

Below this, there's a section for "FreeBSD" and a numbered step "4. Open Tenable Nessus in your browser." with two bullet points: "To access a remotely installed Tenable Nessus instance, go to https://<remote IP address>:8834 (for example, https://111.49.7.180:8834)." and "To access a locally installed Tenable Nessus instance, go to https://localhost:8834."

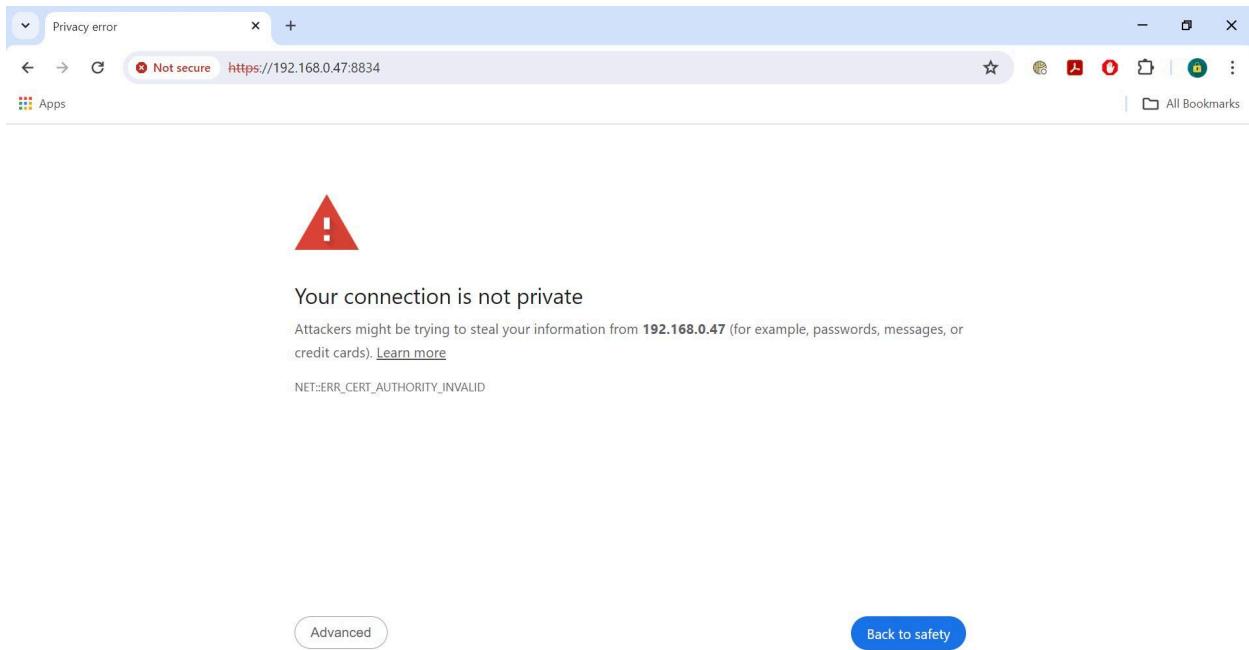
I ran the command **sudo systemctl start nessusd**, and after I entered my password, I didn't get any feedback. I entered **systemctl status nessusd** to ensure that it's running.

```
lynx@lynx:~$ systemctl start nessusd
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ===
Authentication is required to start 'nessusd.service'.
Authenticating as: cristian (lynx)
Password:
==== AUTHENTICATION COMPLETE ===
lynx@lynx:~$ systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
    Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor preset: enabled)
    Active: active (running) since Sun 2024-03-24 17:41:45 UTC; 1min 29s ago
      Main PID: 2967 (nessus-service)
        Tasks: 16 (limit: 9389)
       Memory: 64.2M
          CPU: 50.42ms
         CGroup: /system.slice/nessusd.service
                 └─2967 /opt/nessus/sbin/nessus-service -q
                  ├─2968 nessusd -q

Mar 24 17:41:45 lynx systemd[1]: Started The Nessus Vulnerability Scanner.
Mar 24 17:41:47 lynx nessus-service[2968]: Cached 0 plugin libs in 0ms
Mar 24 17:41:47 lynx nessus-service[2968]: Cached 0 plugin libs in 0ms
lynx@lynx:~$
```

## Step 4

### Open Tenable Nessus in your browser



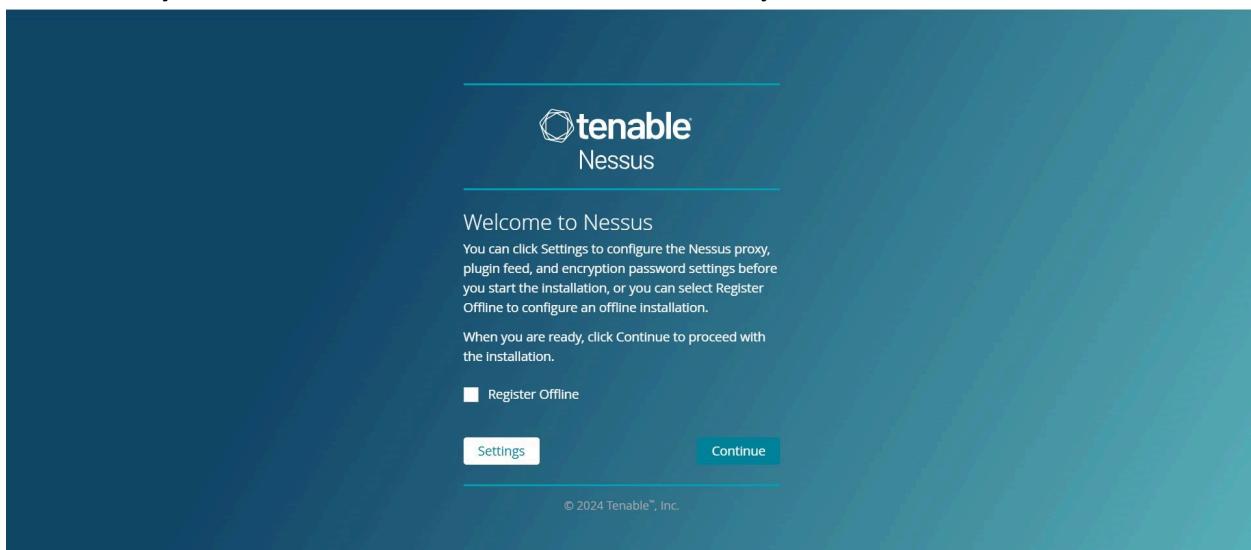
In the screenshot above i entered **https//** followed by the local ip of the web interface for the Nessus Server, followed by : (colon), and the port **8834**. I got a “Your connection is not private” window”.

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

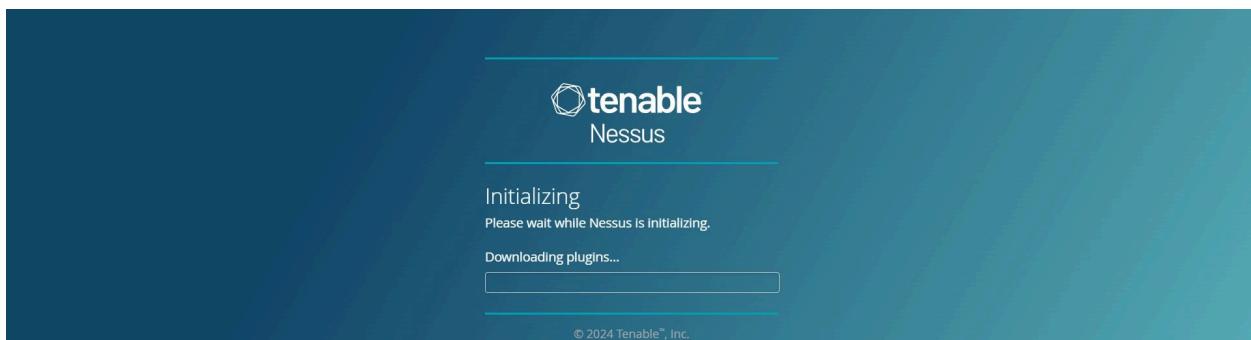
This server could not prove that it is **192.168.0.47**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 192.168.0.47 \(unsafe\)](#)

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.

A screenshot of the Tenable Nessus homepage. The navigation bar includes "Nessus Essentials", "Scans", and "Settings". On the left sidebar, there are sections for "FOLDERS" (My Scans, All Scans, Trash), "RESOURCES" (Policies, Plugin Rules, Terrascan), and "Tenable News" (Cybersecurity, Snapshot: NSA Picks, Top Cloud Securi...). The main content area is titled "My Scans" and shows a message: "This folder is empty. Create a new scan." A black callout box in the upper right corner states: "Plugins are compiling. Nessus functionality will be limited until compilation is complete." The bottom right corner shows a user profile for "barreno".

