Student Name:

Lab 3: Nessus Lab

This lab uses the **Kali 2021** virtual machine (VM) as OVA file **KALI-20.ova** on Canvas. The credentials are as follows:

Username: osboxes

Password: osboxes.org

INSTALLING, CONFIGURING AND USING NESSUS

In this recipe, we install, configure, and start Nessus. Nessus depends on vulnerability checks in the form of feeds to locate vulnerabilities on our chosen target. Nessus comes into two flavors of feeds: Home and Professional.

- **Home Feed:** The Home Feed is for noncommercial/personal usage. Using Nessus in a professional environment for any reason requires the use of the Professional Feed.
- **Professional Feed:** The Professional Feed is for commercial usage. It includes support and additional features such as unlimited concurrent connections and so on. If you are a consultant and are performing tests for a client, the Professional Feed is the one for you.

For our recipe, we will assume you are utilizing the Home Feed.

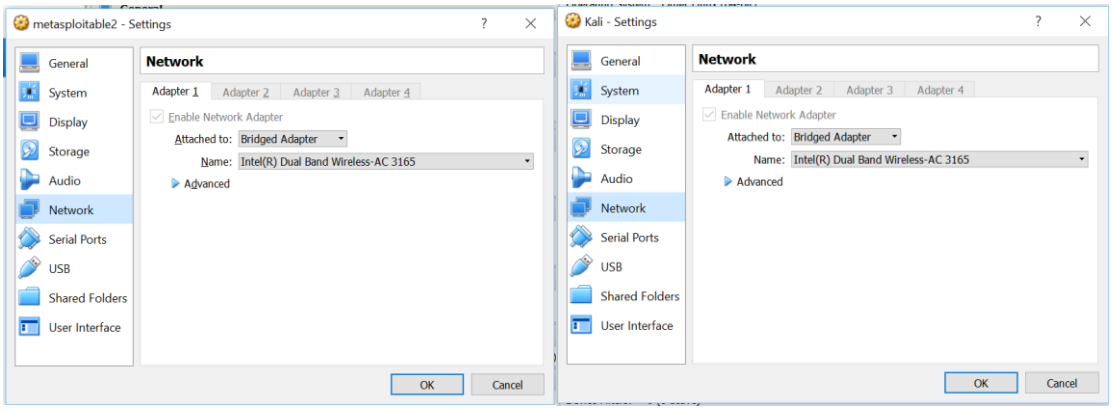
Notes:

1. **Do this Lab in Kali-20.ova VM (username : osboxes ; password : osboxes.org) and metasploitable 2 (username : msfadmin ; password : msfadmin). Download Metasploitable using Microsoft edge or Firefox for download from "https://information.rapid7.com/download-metasploitable-2017.html"**
   Note: You can follow the instructions in https://www.youtube.com/watch?v=qSPT-YlIZAc

2. **The network settings of Kali VM should be Attached to: Bridge Adapter. Example is shown in below screen shot. And change metasploitable2 and ubuntu-desktop network setting to Bridge Adapter.**

3. **Compiling plugins during initialization phase of Nessus might take lot of time depending on the size of RAM.**

4. **Allocate 8GB to Kali-20 if you have enough RAM space available.**

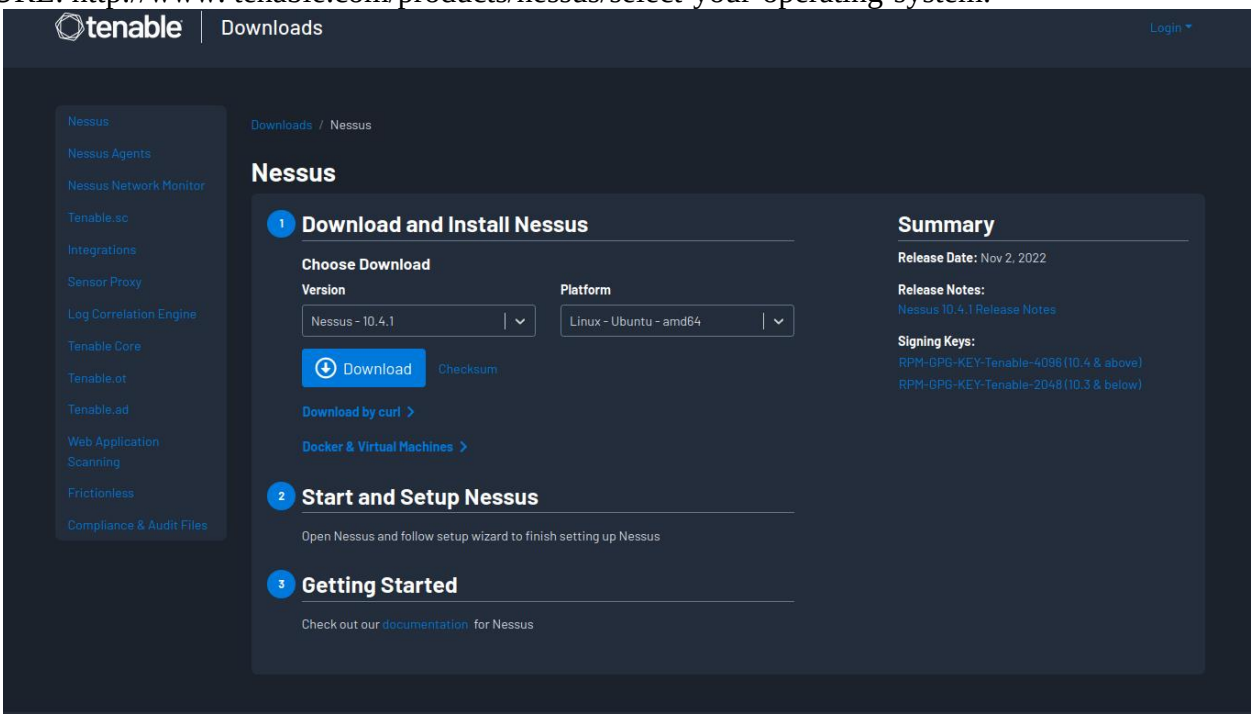


Let's begin the installation, configuring, and starting of Nessus by opening a terminal window:

Note: If you are unable to download the Nessus please change Network settings to "NAT" and after installing all turn it Back to "Bridger Adapter" to perform the lab.

1. Open the firefox esr web browser and navigate to the following

URL: http://www. tenable.com/products/nessus/select-your-operating-system.



2. Select **Nessus-10.4.1-ubuntu1404_amd64.deb** or Latest Version of it.
3. Download the file to your local root directory.
4. Open a terminal window.
5. Execute the following command to install Nessus:

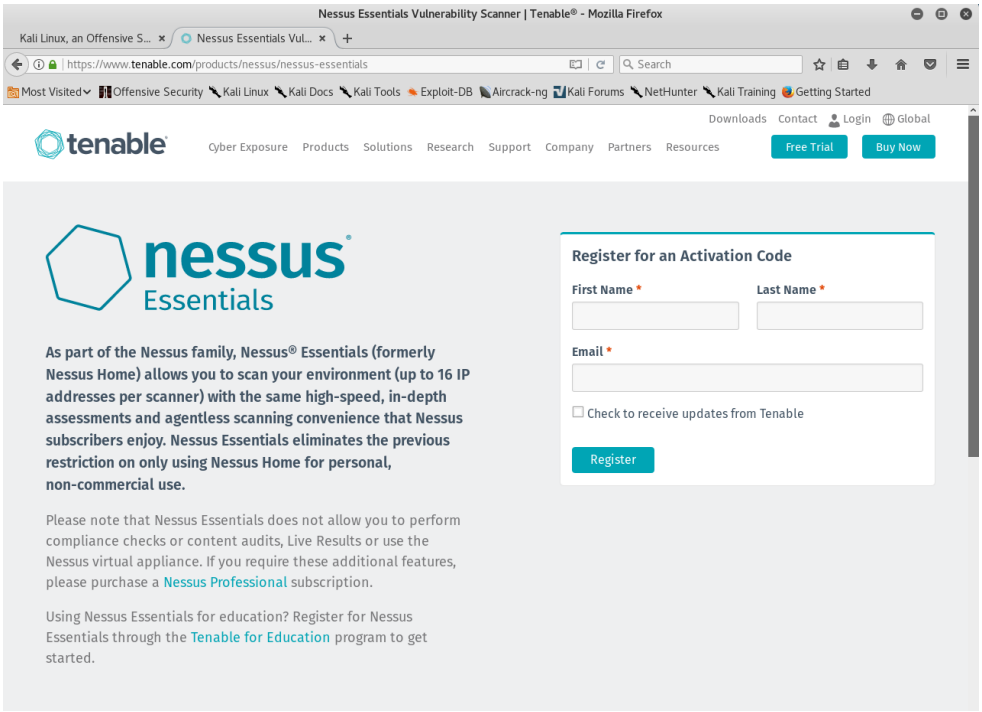
   //Type the below command
   sudo dpkg -i "Nessus-10.4.1-ubuntu1404_amd64.deb" //Nessus will be installed under the /opt/nessus directory

```
┌──(osboxes㉿osboxes)-[~]
└─$ cd Downloads

┌──(osboxes㉿osboxes)-[~/Downloads]
└─$ sudo dpkg -i "Nessus-10.4.1-ubuntu1404_amd64.deb"
Selecting previously unselected package nessus.
(Reading database ... 310184 files and directories currently installed.)
Preparing to unpack Nessus-10.4.1-ubuntu1404_amd64.deb ...
Unpacking nessus (10.4.1) ...
Setting up nessus (10.4.1) ...
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
PBKDF2 : (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 ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.serv
ice
 - Then go to https://osboxes:8834/ to configure your scanner
```

6. Once the installation completes, you can run Nessus by typing the following command: **sudo /bin/systemctl start nessusd.service** //this starts the Nessus and runs in the background

```
┌──(osboxes㉿osboxes)-[~/Downloads]
└─$ sudo /bin/systemctl start nessusd.service
```

NOTE: To register your copy of Nessus, you must have a valid license (product key), which can be obtained from http://www.tenable.com/products/nessus/nessus-essentials. After you register the activation key will be sent to your mail address specified.



7. Enable your Nessus install by executing the following command. You need to register and obtain activation Code prior to this instruction. Registration details are in above instructions.

   sudo /opt/nessus/sbin/nessuscli fetch --register XXXX-XXXX-XXXX-XXXX- XXXX

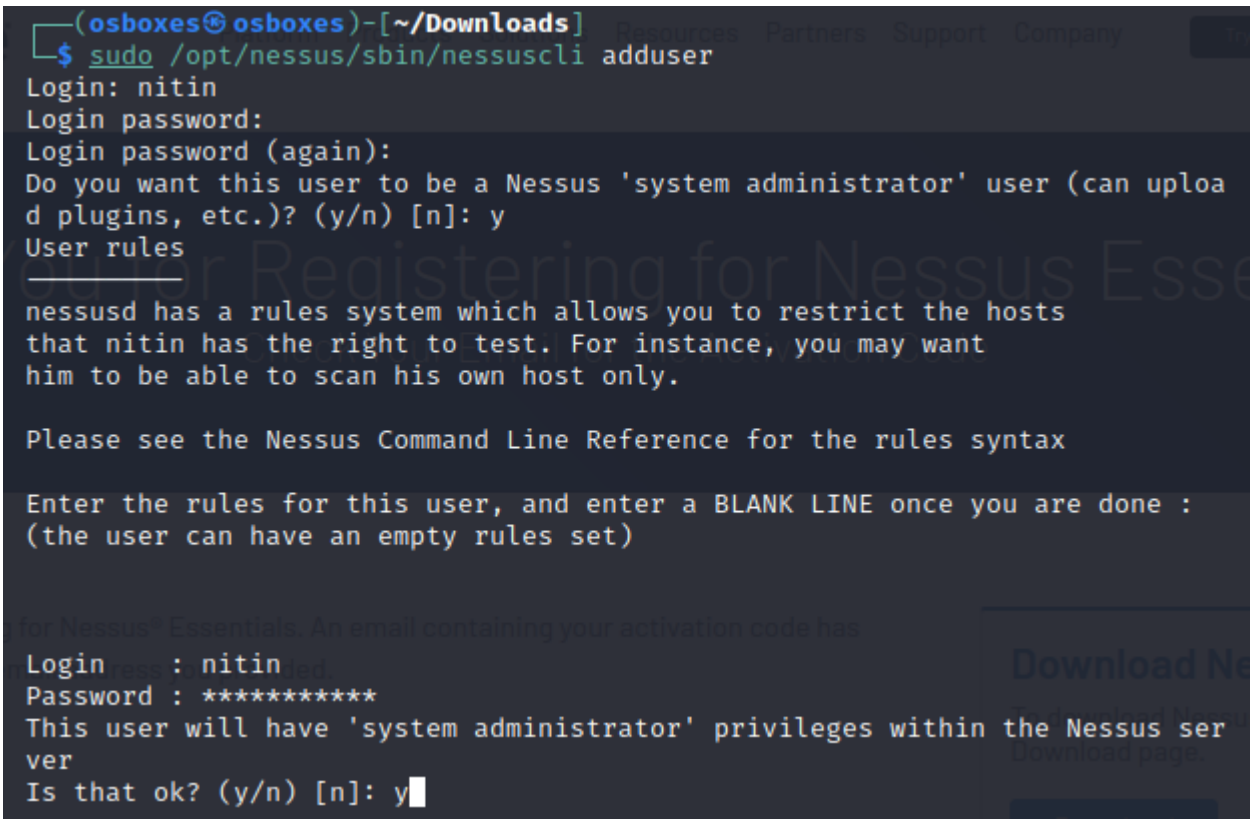
In this step, we will also grab the latest plugins from http://plugins.nessus.org.

```
┌──(osboxes㉿osboxes)-[~/Downloads]
└─$ sudo /opt/nessus/sbin/nessuscli fetch --register 26MM-AJTF-P6PZ-VD8Y-7Z
GB
Your Activation Code has been registered properly - thank you.
Refreshing Nessus license information ... complete; continuing with updates.


——— Fetching the newest updates from nessus.org ———

Nessus Plugins: Downloading (1%)
Nessus Plugins: Downloading (43%)
Nessus Plugins: Downloading (77%)
Nessus Plugins: Unpacking (0%)
Nessus Plugins: Unpacking (7%)
Nessus Plugins: Unpacking (60%)
[info] Copying templates version 202210311525 to /opt/nessus/var/nessus/tem
plates/tmp
[info] Finished copying templates.
[info] Moved new templates with version 202210311525 from plugins dir.
Nessus Plugins: Complete


Nessus Core Components: Complete


 * Nessus Plugins are now up-to-date and the changes will be automatically
processed by Nessus.
 * Nessus Core Components are now up-to-date and the changes will be automa
tically processed by Nessus.

┌──(osboxes㉿osboxes)-[~/Downloads]
```

8. Now enter the following command in the terminal

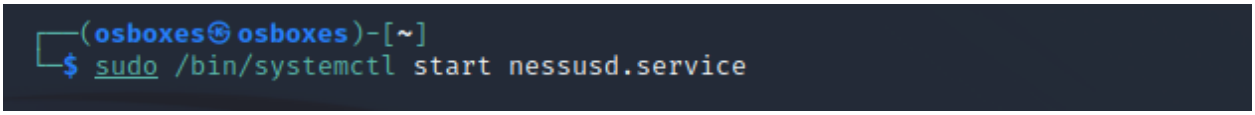
   sudo /opt/nessus/sbin/nessuscli adduser //adds the user to access nessus

9. At the login prompt, enter the login name of the user.
10. Enter the password of your choice twice.
11. Answer as Y (Yes) to make this user an administrator.

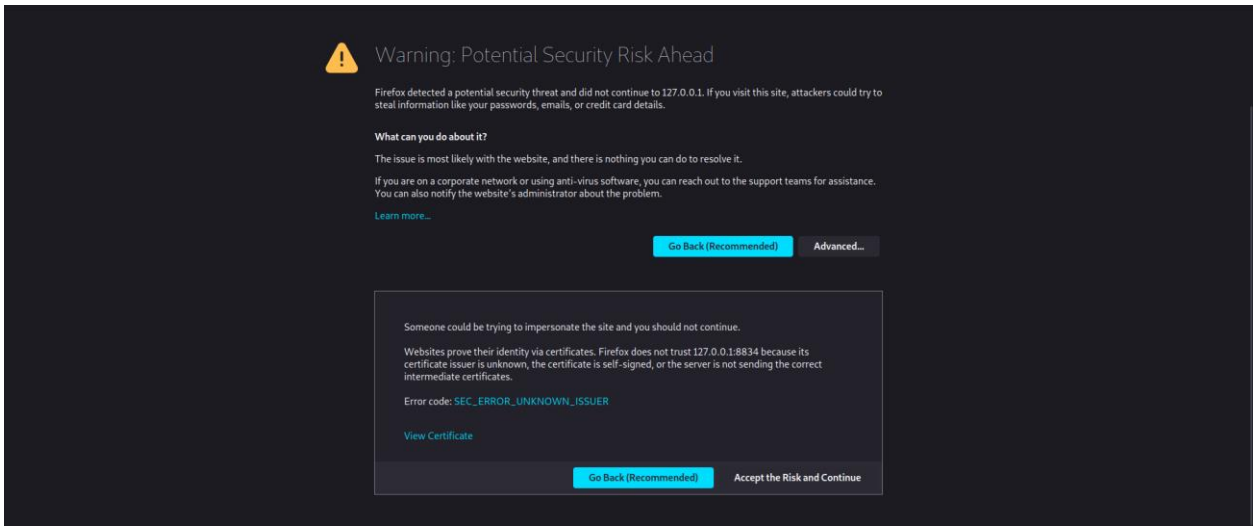


12. Once complete, you can run Nessus by typing the following command (it won't work without a user account)

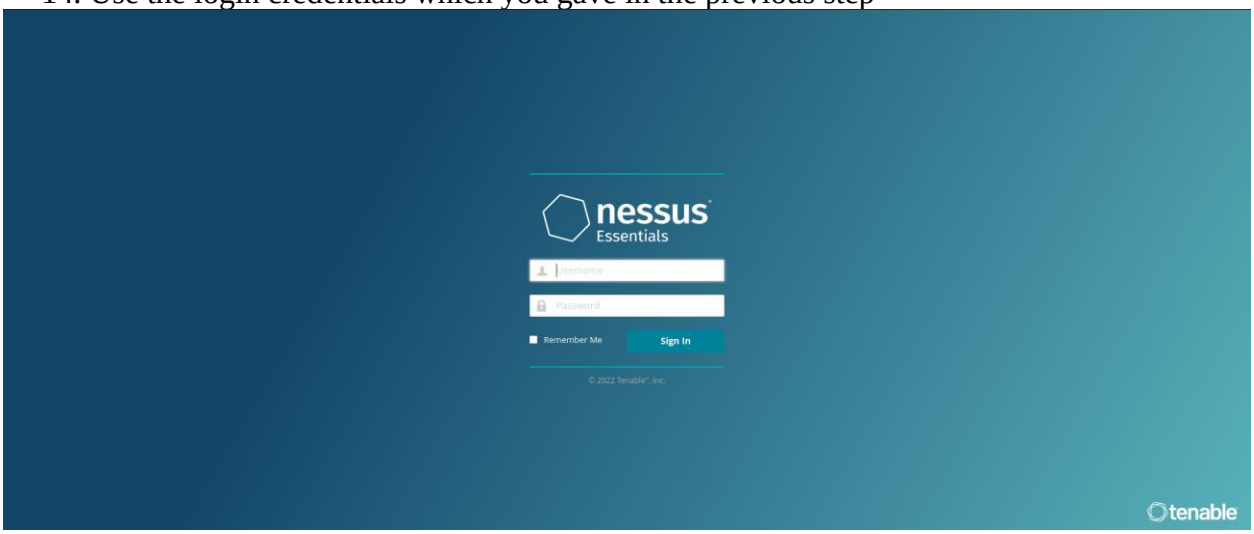
    sudo /bin/systemctl start nessusd.service



13. Now got to URL “https://127.0.0.1:8834/html5.html#/” which will bring you to below page. Add Exception and confirm the security Exception.



14. Use the login credentials which you gave in the previous step



Q1. Provide Screen Shot of your above Logged in Nessus Page.

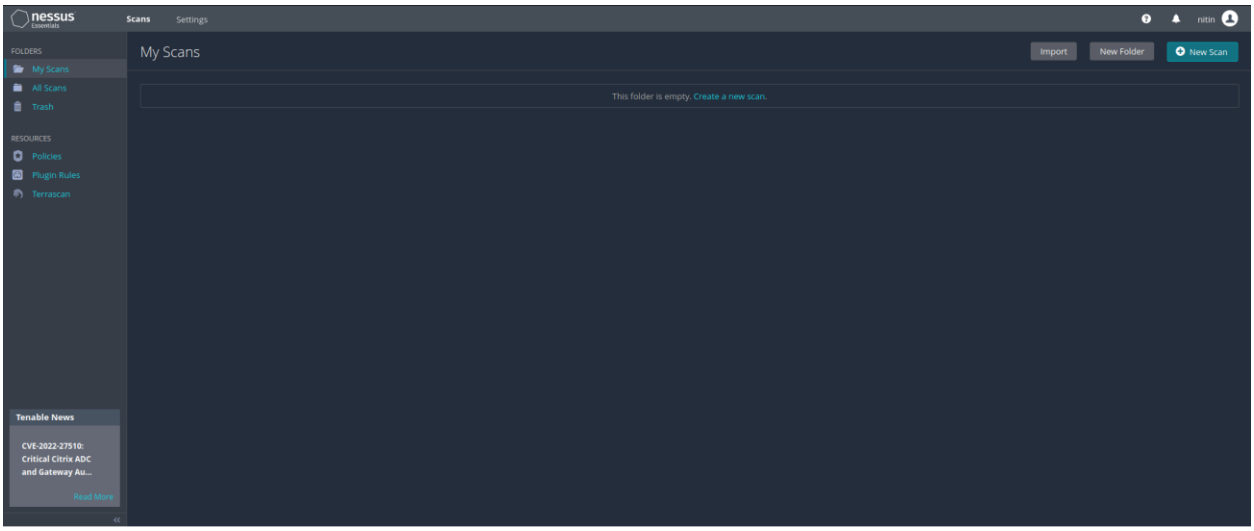
Nessus – finding Local Vulnerabilities:

Now that we have Nessus installed and configured, we will be able to begin testing of our first set of vulnerabilities. Nessus allows us to attack a wide range of vulnerabilities depending on our feed, and we will confine our list of assessing the vulnerabilities of our target to those specific to the type of information we seek to gain from the assessment. In this recipe, we will begin by finding local vulnerabilities. These are vulnerabilities specific to the operating system we are using.

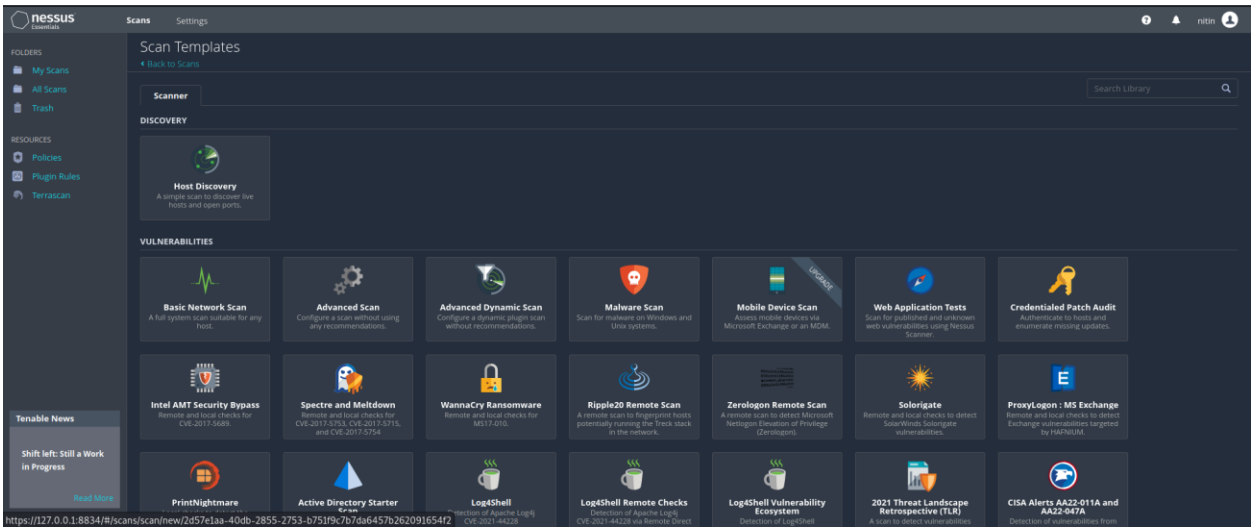
Disable Firewalls if you get empty reports after the scan.

Let's begin the process of finding vulnerabilities with Nessus by opening the web browser:

1. Log in to Nessus at https://127.0.0.1:8834.
2. Click on “New Scans” on the Top Right corner**.**

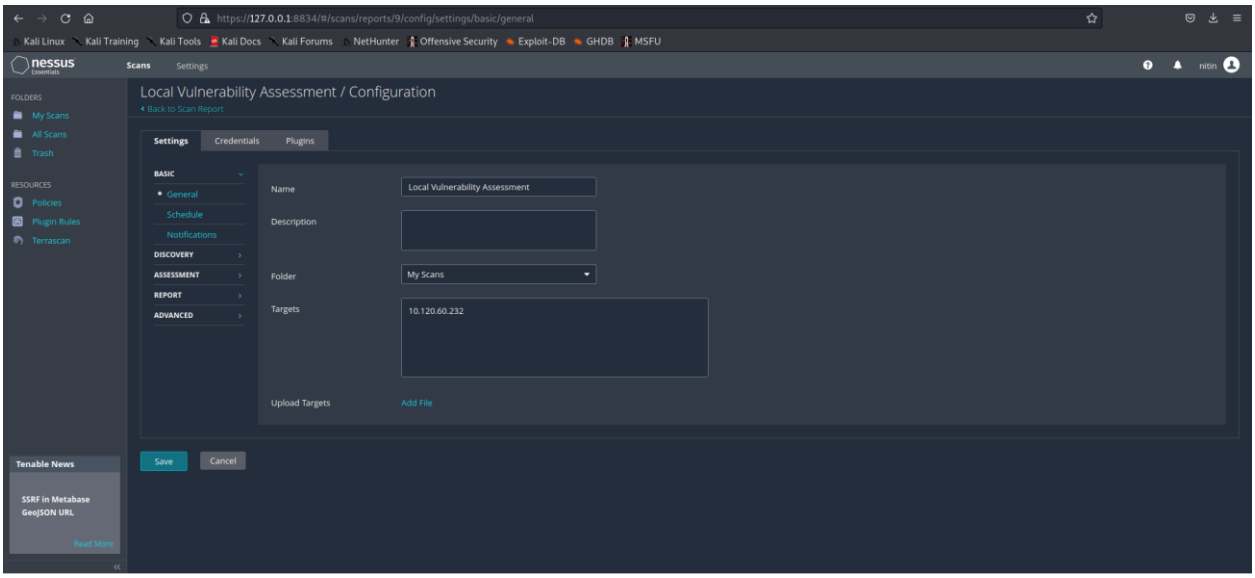


3. Click on **New Scan**. You Will see the below window, select Advanced Scan.



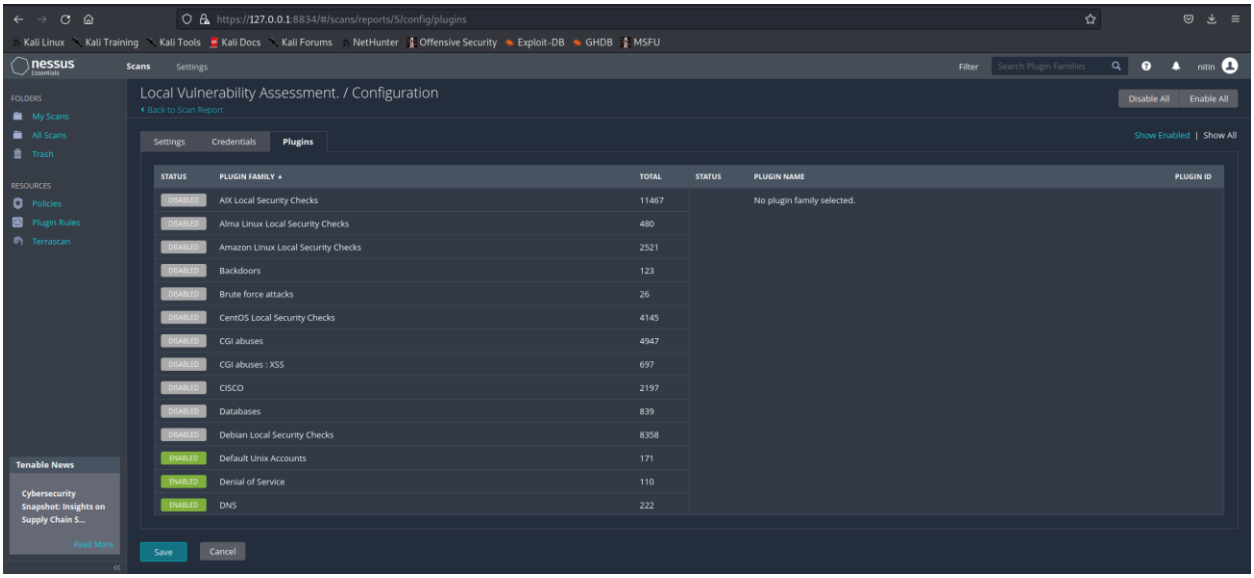
4. Click on **Advanced Scan**, perform the following tasks:
    1. Under **General Type,**
    2. Enter a name for your scan. We chose Local Vulnerability Assessment.
    3. Let the Folder field be My Scans.
    4. Choose your targets considering the following points:
        - Targets must be entered one per line.
        - You can also enter ranges of targets on each line.
    5. You may also upload a target's file (if you have one) or select Add Target IP Address.
    6. To enter the host IP address, go to virtual box and start metasploitable 2 (network settings as bridged adapter)giving username and password as **msfadmin.**
    7. Then type **ifconfig** to obtain the ipaddress

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:52:ae:28
          inet addr:10.120.60.232  Bcast:10.120.61.255  Mask:255.255.25
          inet6 addr: fe80::a00:27ff:fe52:ae28/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1575222 (1.5 MB)  TX bytes:7188 (7.0 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```



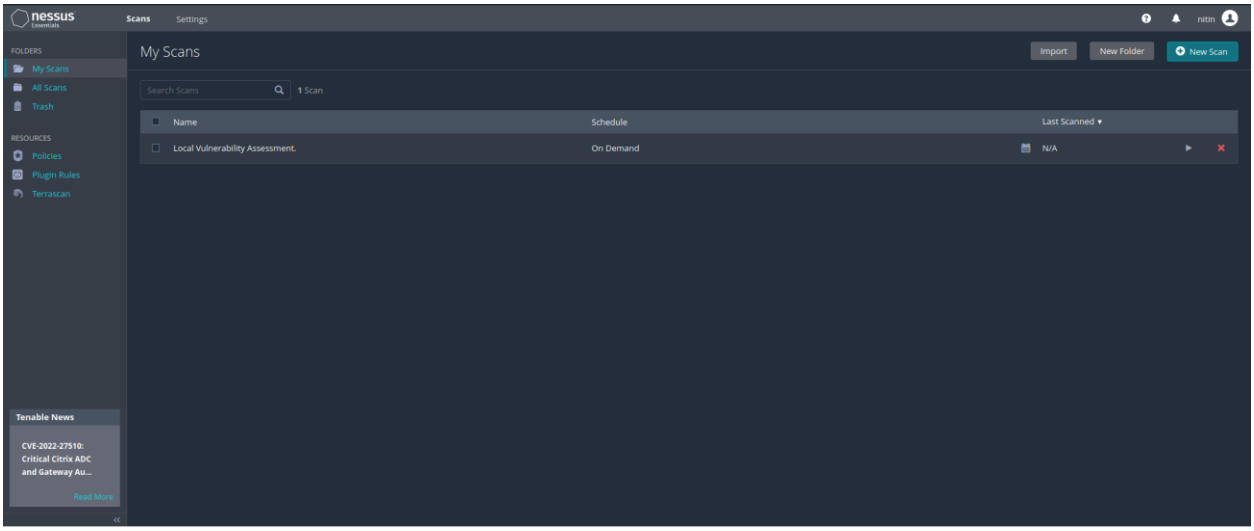
5. On the **Plugins** tab, select **Disable All** and **Enable** the following specific vulnerabilities:
   - Ubuntu Local Security Checks
   - Default Unix Accounts
   - DNS
   - FTP
   - SMTP Problems
   - SNMP
   - Settings
   - Web Servers

- Denial of Service

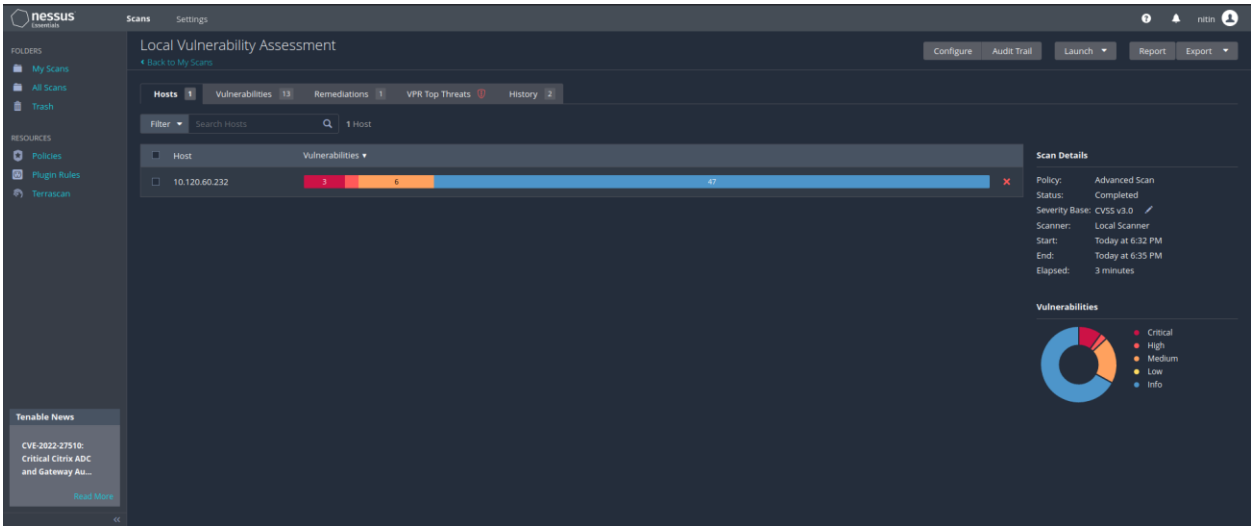


6. Click on **save** to save your new scan.

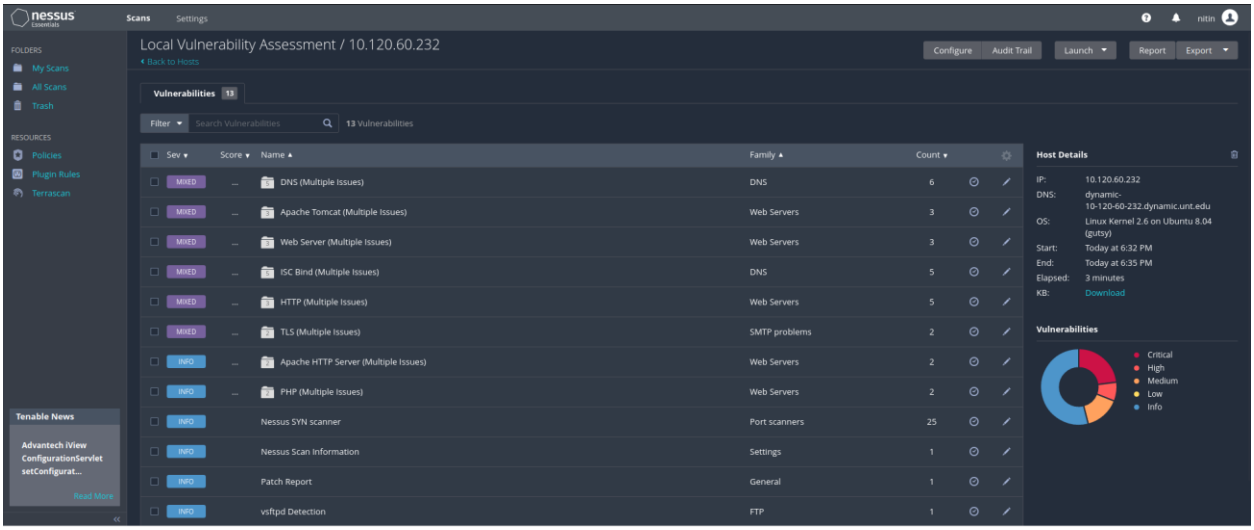
7. Click on **Launch**.



10. You will get a confirmation and your test will complete (depending on how many targets are selected and the number of tests performed).
11. Once completed, you can export a report.



12. Double-click on the report to analyze the following points (on the **Results** tab):
    - Each target in which vulnerability is found will be listed
    - Double-click on the IP address to see the ports and issues on each port
    - Click on the number under the column to get the list of specific issues/vulnerabilities found
    - The vulnerabilities will be listed in detail



13. Click on **export Report -** Complete List of Vulnerabilities by host.

Q2. Attach the Downloaded report while submitting and write down summary of scanned analysis in brief.

Nessus – Finding network vulnerabilities:

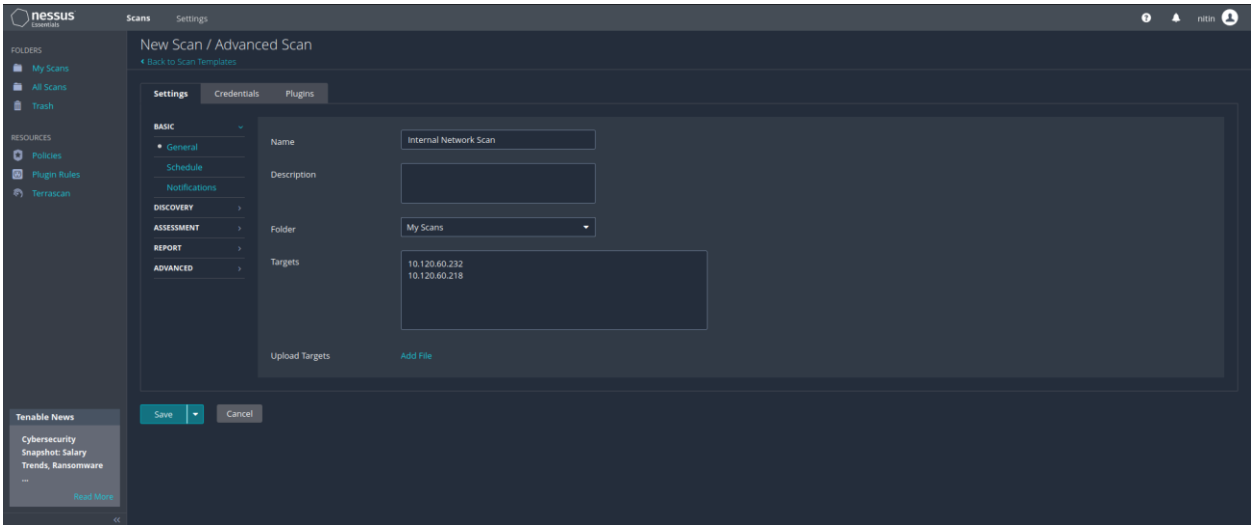
Nessus allows us to attack a wide range of vulnerabilities depending on our feed, and we will confine our list of assessing the vulnerabilities of our target to those specific to the type of information we seek to gain from the assessment. In this recipe, we will configure Nessus to find network vulnerabilities on our targets. These are vulnerabilities specific to the machines or protocols on our network.

To complete this recipe, you will need a virtual machine(s) to test against: Start all VM's with network settings as bridged adapter.

- Metasploitable 2.0 (VM creds: msfadmin/msfadmin)
- UbuntuDesktop VM (VM creds: sec-lab/untccdc) → Use the cscelab.ova file.

1. Log in to Nessus at https://127.0.0.1:8834.
2. Go to Scans.
3. Click on "New Scan" then Select "Advanced Scan".
2. Under **General Type,**
3. Enter a name for your scan. We chose, Internal Network Scan.
4. Let the Folder field be My Scans.
5. Choose your targets considering the following points:
    - Targets must be entered one per line
    - You can also enter ranges of targets on each line
6. You may also upload a target's file (if you have one) or select Add Target IP Address.
7. To enter the host ip address go to virtual box and start metasploitable 2 giving username and password as **msfadmin and** Start Ubuntu desktop VM with user id as **sec-lab** and password as **untccdc.** You can use your own windows IP address for use.
8. Then type **ifconfig** to obtain the ipaddress in Ubuntu and metasploitable.

```
sec-lab@unt-sec:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.120.60.218  netmask 255.255.254.0  broadcast 10.120.61.255
        inet6 fe80::c3c4:4431:2e3e:e3f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b8:60:9d  txqueuelen 1000  (Ethernet)
        RX packets 13201  bytes 9162776 (9.1 MB)
        RX errors 0  dropped 347  overruns 0  frame 0
        TX packets 1025  bytes 171641 (171.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 567  bytes 55706 (55.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 567  bytes 55706 (55.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec-lab@unt-sec:~$
```

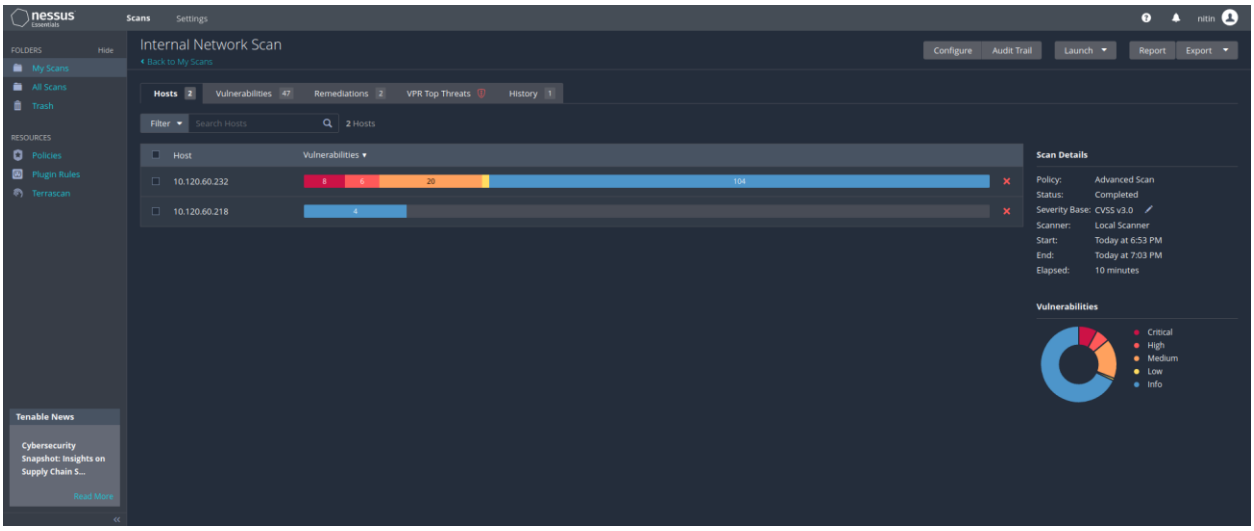


9. On the Plugins tab, click on Disable All and select the following specific vulnerabilities:
    - CISCO
    - DNS
    - Default Unix Accounts
    - FTP
    - Firewalls
    - Gain a shell remotely
    - General
    - Netware
    - Peer-To-Peer File Sharing
    - Policy Compliance
    - SCADA
    - SMTP Problems
    - SNMP
    - Service Detection
    - Settings

10. Click on **save** to save your new scan

11. On the main menu, click on the Scan. Then Click on Launch button to start scanning.

12. Once completed, you will receive a report inside of the Results tab.
13. Double-click on the report to analyze the following points:
    - Each target in which a vulnerability is found will be listed
    - Double-click on the IP address to see the ports and issues on each port
    - Click on the number under the column to get the list of specific issues vulnerabilities found
    - The vulnerabilities will be listed in detail



14. Click on export Report – Complete List of Vulnerabilities by host

Q3. Attach the Downloaded report while submitting and write down summary of scanned analysis in brief.

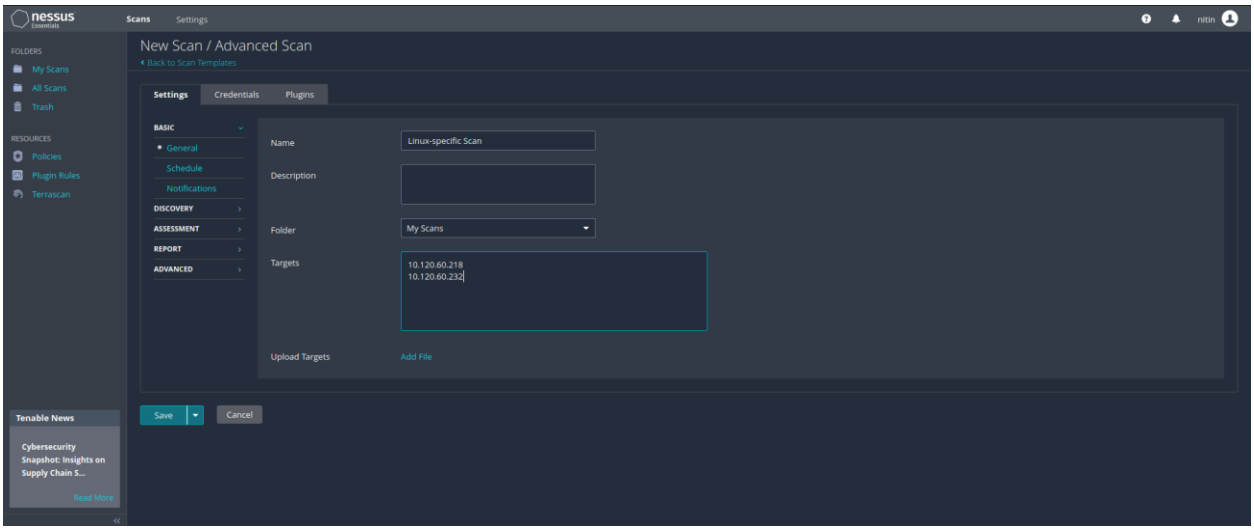
Nessus – Finding Linux-specific vulnerabilities:

To complete this recipe, you will need a virtual machine(s) to test against:

- Ubuntu Desktop
- Metasploitable

1. Log in to Nessus at https://127.0.0.1:8834.
2. Go to Scans.
3. Click on “New Scan” then Select “Advanced Scan”.
4. Under **General Type,**
5. Enter a name for your scan. We chose, Linux-specific Scan.
6. Let the Folder field be My Scans.
7. Choose your targets considering the following points:
    - Targets must be entered one per line
    - You can also enter ranges of targets on each line
8. You may also upload a target's file (if you have one) or select Add Target IP Address.
9. To enter the host ip address go to virtual box and start metasploitable 2 giving username and password as **msfadmin and** Start Ubuntu desktop VM with user id as **sec-lab** and password as **untccdc.** You can use your own windows IP address for use.
10. Then type **ifconfig** to obtain the ipaddress in Ubuntu and metasploitable.

```
sec-lab@unt-sec:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.120.60.218  netmask 255.255.254.0  broadcast 10.120.61.255
        inet6 fe80::c3c4:4431:2e3e:e3f  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b8:60:9d  txqueuelen 1000  (Ethernet)
        RX packets 13201  bytes 9162776 (9.1 MB)
        RX errors 0  dropped 347  overruns 0  frame 0
        TX packets 1025  bytes 171641 (171.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 567  bytes 55706 (55.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 567  bytes 55706 (55.7 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec-lab@unt-sec:~$
```



9. On the Plugins tab, click on Disable All and enter the following specific vulnerabilities. This list is going to be rather long as we are scanning for services that may be running on our Linux target:

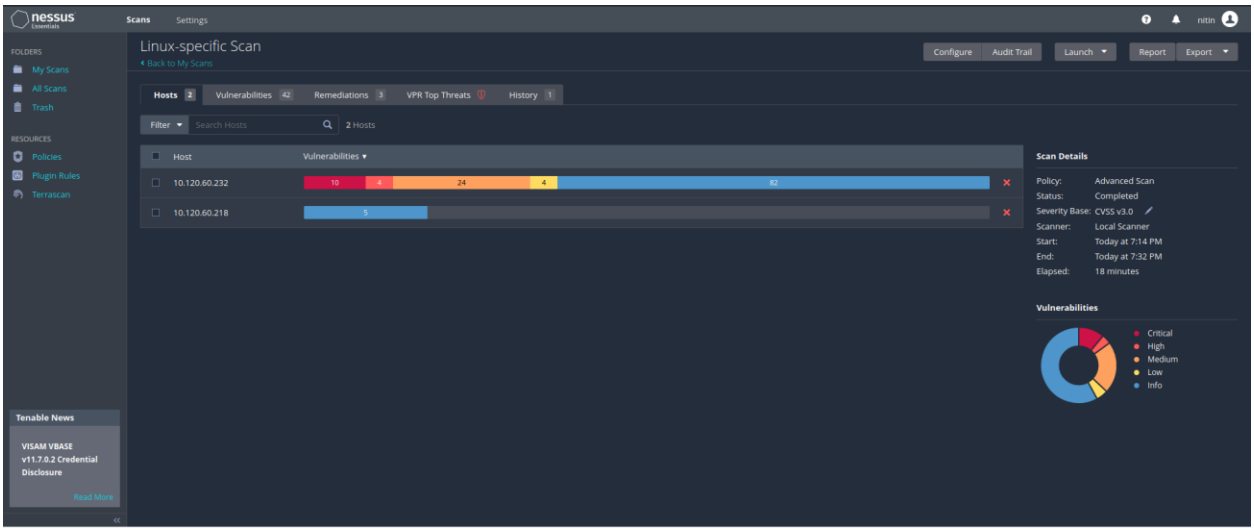
- Backdoors
- Brute Force Attacks
- CentOS Local Security Checks
- DNS
- Debian Local Security Checks
- Default Unix Accounts
- Denial of Service
- FTP
- Fedora Local Security Checks
- Firewalls
- FreeBSD Local Security Checks
- Gain a shell remotely

- General
- Gentoo Local Security Checks
- HP-UX Local Security Checks
- Mandriva Local Security Checks
- Misc
- Red Hat Local Security Checks
- SMTP Problems
- SNMP
- Scientific Linux Local Security Checks
- Slackware Local Security Checks
- Solaris Local Security Checks
- SuSE Local Security Checks
- Ubuntu Local Security Checks
- Web Servers

10. Click on **save** to save your new scan

11. On the main menu, click on the Scan. Then Click on Launch button to start scanning.

12. Once completed, you will receive a report inside of the Results tab.
13. Double-click on the report to analyze the following points:
    - Each target in which a vulnerability is found will be listed
    - Double-click on the IP address to see the ports and issues on each port
    - Click on the number under the column to get the list of specific issues vulnerabilities found
    - The vulnerabilities will be listed in detail



14. Click on export Report – Complete List of Vulnerabilities by host

Q4. Attach the Downloaded report while submitting and write down summary of scanned analysis in brief.