

Name: Ritesh Lakhani


Enrollment No: 22010101099

Nessus Tool :

Task 1:

Introduction about nessus

Task 1 Introduction



Nessus vulnerability scanner is exactly what you think is its! A vulnerability scanner!
It uses techniques similar to Nmap to find and report vulnerabilities, which are then, presented in a nice GUI for us to look at.
Nessus is different from other scanners as it doesn't make assumptions when scanning,
like assuming the web application is running on port 80 for instance.

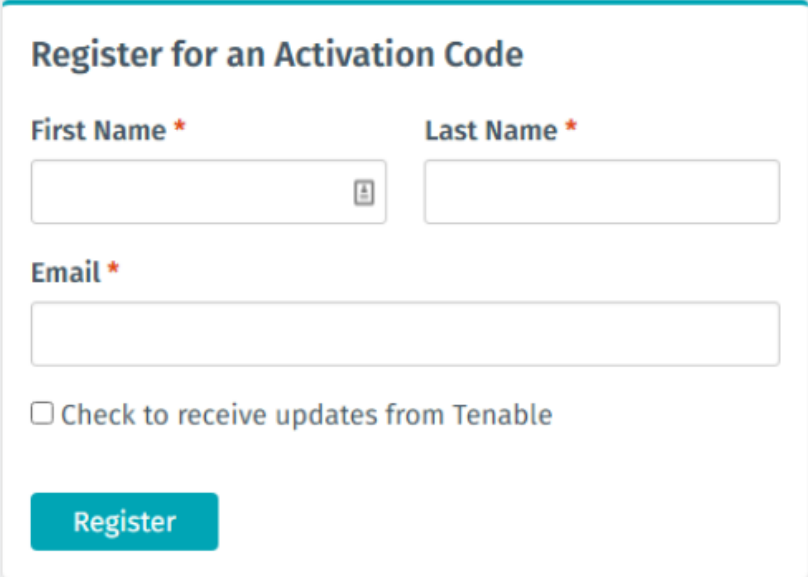
Nessus offers a free and paid service, in which some features are left out from the free to make you more inclined to buy the paid service.
Their pricing is similar to Burp Suite, so unless you got some spare change, we will be just be using their free version.

You can check out their pricing options here: <https://www.tenable.com/products/nessus>

Task 2:

Installation step :

Step #1



The image shows a registration form titled "Register for an Activation Code". It contains three input fields: "First Name" with a red asterisk, "Last Name" with a red asterisk, and "Email" with a red asterisk. The "First Name" field has a small icon of a person. Below the email field is a checkbox labeled "Check to receive updates from Tenable". At the bottom is a teal button labeled "Register".

Register for an Activation Code

First Name * Last Name *

Email *

☐ Check to receive updates from Tenable

Register

Goto <https://www.tenable.com/products/nessus/nessus-essentials> and register an account.

Click on url and register your self then it shows download button click on it and download the Nessus.

Step #2

 [Nessus-8.12.1-debian6_amd64.deb](#)

Debian 6, 7, 8, 9 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64

42.9 MB

Oct 29, 2020

[Checksum](#)

We will then download the Nessus-8.12.1-debian6_amd64.deb file

Save it to your **/Downloads/** folder

No answer needed

✓ Correct Answer

Step #3

In the terminal we will navigate to that folder and run the following command:

`sudo dpkg -i package_file.deb`

Remember to replace **package_file.deb** with the file name you downloaded.

```
A root ~/Downloads
$ sudo dpkg -i Nessus-8.12.1-debian6_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 366461 files and directories currently installed.)
Preparing to unpack Nessus-8.12.1-debian6_amd64.deb ...
Unpacking nessus (8.12.1) ...
Setting up nessus (8.12.1) ...
Unpacking Nessus Scanner Core Components...

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

No answer needed

✓ Correct Answer

After downloading perform given command and install Nessus

Step #4

We will now start the Nessus Service with the command:

`sudo /bin/systemctl start nessusd.service`

```
A root ~/Downloads
$ sudo /bin/systemctl start nessusd.service
```

No answer needed

✓ Correct Answer

Now for starting run above code

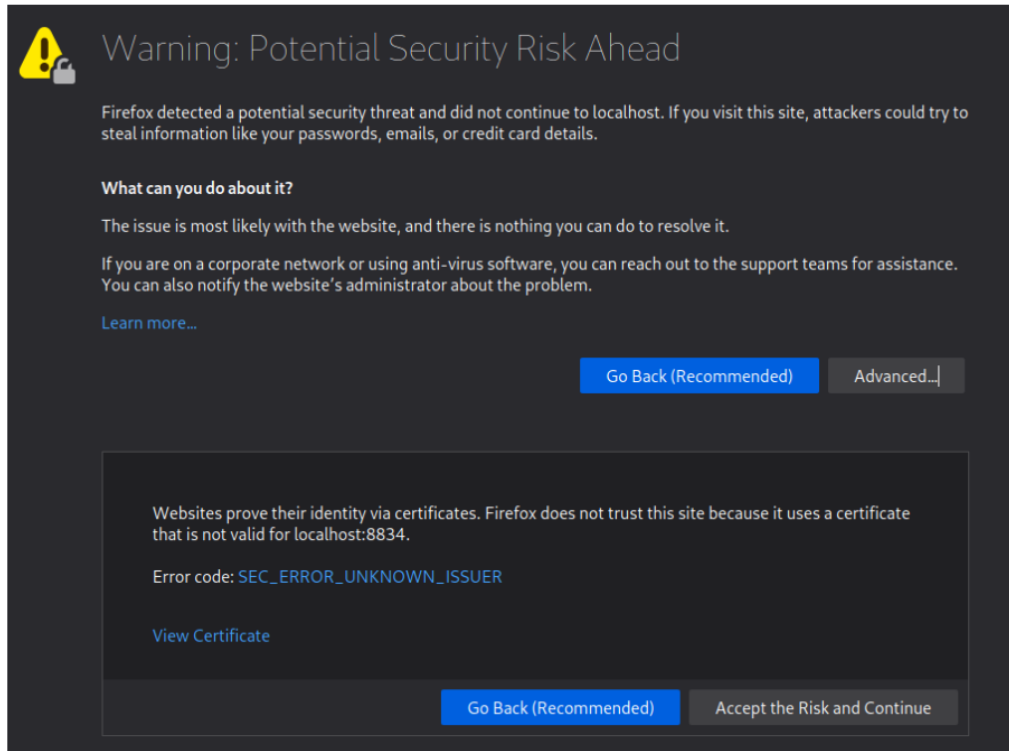
Step #5

Open up Firefox and goto the following URL:

<https://localhost:8834/>

You may be prompted with a security risk alert.

Click **Advanced...** -> **Accept the Risk and Continue**



Now go to that url and start the Nessus

Then follow steps accordingly

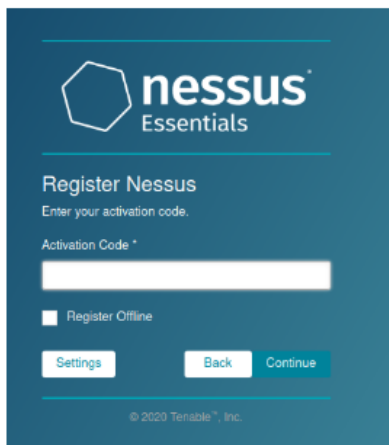
Step #6

Next, we will set up the scanner.

Select the option **Nessus Essentials**



Clicking the **Skip** button will bring us to a page, which we will input that code we got in the email from Nessus.



No answer needed

✓ Correct Answer

Step #7

Fill out the **Username** and **Password** fields. Make sure to use a strong password!

No answer needed

✓ Correct Answer

Step #8

Nessus will now install the **plugins** required for it to function.

This will take some time, which will depend on your internet connection and the hardware attached to your VM.

If the progress bar appears to be **not moving**, it means you do not have **enough space** on the VM to install.

No answer needed

✓ Correct Answer

Step #9

Log in with the account credentials you made earlier.

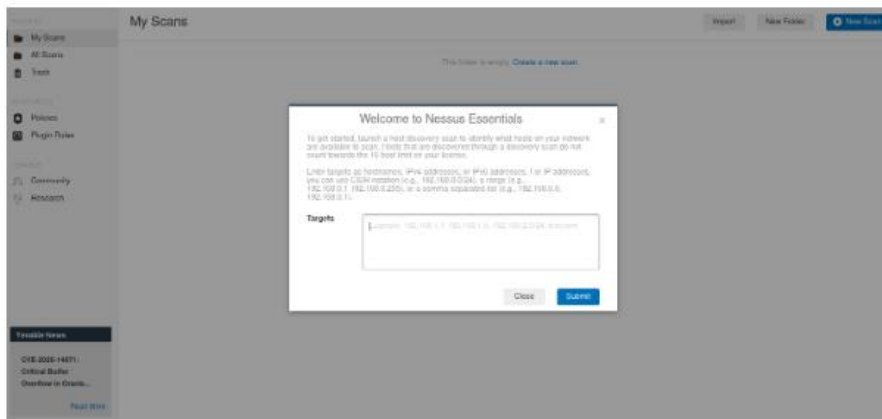


No answer needed

✓ Correct Answer

Step #10

You have now successfully installed Nessus!



No answer needed


✓ Correct Answer

After this you can see a interface like this

Task 3:


Navigations and Scans

DISCOVERY




Host Discovery
A simple scan to discover live hosts and open ports.


VULNERABILITIES




Basic Network Scan
A full system scan suitable for any host.




Advanced Scan
Configure a scan without using any recommendations.




Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.




Malware Scan
Scan for malware on Windows and Unix systems.




Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.




Web Application Tests
Scan for published and unknown web vulnerabilities.




Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.




Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.




Bash Shellshock Detection
Remote and local checks for CVE-2014-4271 and CVE-2014-7169.




DHROWN Detection
Remote checks for CVE-2016-0803.




Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.




Shadow Brokers Scan
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.




Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.



WannaCry Ransomware
Remote and local checks for MS17-010.



Hippie20 Remote Scan
A remote scan to fingerprint hosts potentially running the Tweek stack in the network.



ZeroLogon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (ZeroLogon).

Answer the questions below

What is the name of the **button** which is used to launch a scan?

New Scan

✓ Correct Answer

🔍 Hint

What side menu option allows us to create **custom templates**?

Policies

✓ Correct Answer

🔍 Hint

What menu allows us to change **plugin** properties such as hiding them or changing their severity?

Plugin Rules

✓ Correct Answer

🔍 Hint

In the '**Scan Templates**' section after clicking on '**New Scan**', what scan allows us to see simply what hosts are alive?

Host Discovery

✓ Correct Answer

One of the most useful scan types, which is considered to be '**suitable for any host**'?

Basic Network Scan

✓ Correct Answer

What scan allows you to '**Authenticate to hosts and enumerate missing updates**'?

Credentialed Patch Audit

✓ Correct Answer

What scan is specifically used for scanning **Web Applications**?

Web Application Tests

✓ Correct Answer

Task 4: Scanning

Create a new '**Basic Network Scan**' targeting the deployed VM. What option can we set under '**BASIC**' (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue.

Schedule

✓ Correct Answer

Under '**DISCOVERY**' (on the left) set the '**Scan Type**' to cover ports 1-65535. What is this type called?

Port scan (all ports)

✓ Correct Answer

What '**Scan Type**' can we change to under '**ADVANCED**' for lower bandwidth connection?

Scan low bandwidth links

✓ Correct Answer



With these options set, launch the scan.

No answer needed

✓ Correct Answer

After the scan completes, which '**Vulnerability**' in the '**Port scanners**' family can we view the details of to see the open ports on this host?

Nessus SYN scanner

✓ Correct Answer

What **Apache HTTP Server Version** is reported by Nessus?

2.4.99

✓ Correct Answer

🔍 Hint

Task 5 : Scanning A WebApp

(Running this Scan will take some time to complete, please be patient)

Answer the questions below

What is the plugin id of the plugin that determines the HTTP server type and version?

10107

✓ Correct Answer

🔍 Hint

What authentication page is discovered by the scanner that transmits credentials in cleartext?

login.php

✓ Correct Answer

🔍 Hint

What is the file extension of the config backup?

.bak

✓ Correct Answer

🔍 Hint

Which directory contains example documents? (This will be in a php directory)

/external/phpids/0.6/docs/examples/

✓ Correct Answer

🔍 Hint

What vulnerability is this application susceptible to that is associated with X-Frame-Options?

Clickjacking

✓ Correct Answer

🔍 Hint