

PRACTICAL-2

AIM:

Perform a Vulnerability Scan on a system within the Local Area Network and Submit the report

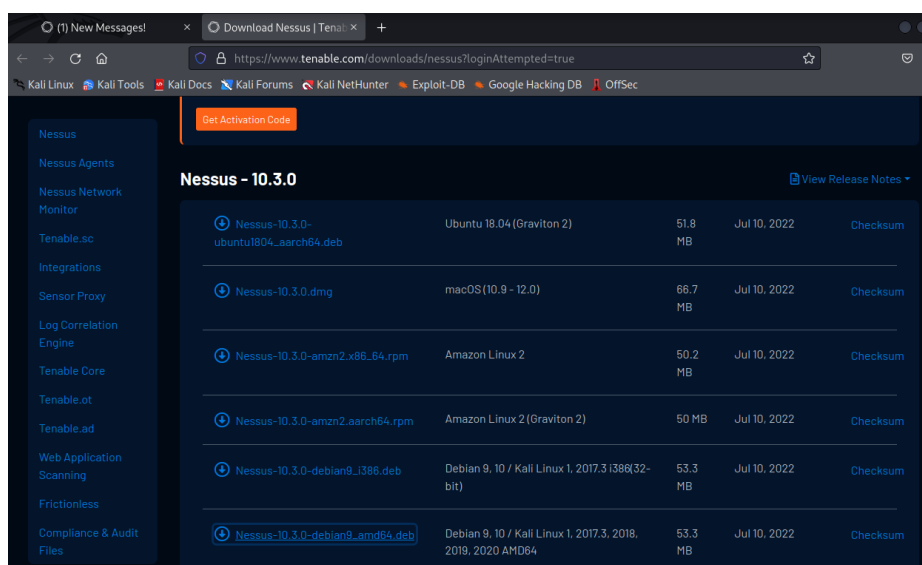
THEORY:

NESSUS ESSENTIALS:

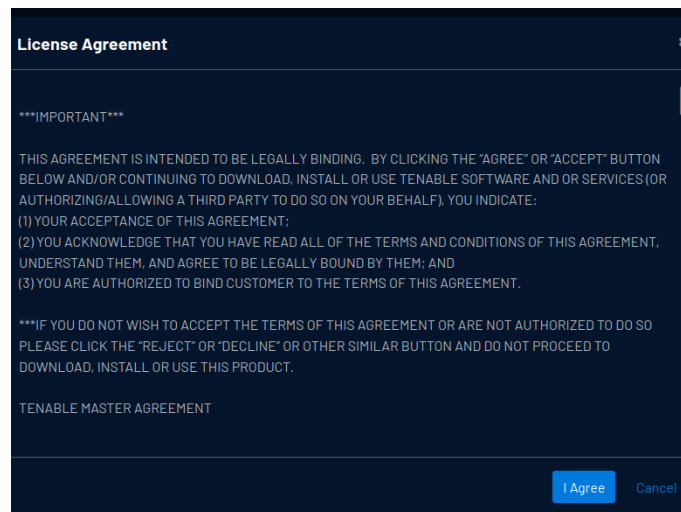
- Nessus Essentials is a free vulnerability assessment solution for up to 16 IPs that provides an entry point into the Tenable ecosystem.
- Backed by market leading functionality from Nessus Professional, Nessus Essentials gives you the accuracy and speed you need to discover, prioritize and remediate vulnerabilities.

IMPLEMENTATION:

- Firstly, Nessus Essential is not pre-installed. Hence, we need to download it.



- Accept the Agreement.



- Now, unpack the package

```
(kali@kali)~[/Downloads]
$ ls
Nessus-10.3.0-debian9_amd64.deb

(kali@kali)~[/Downloads]
$ sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb

Selecting previously unselected package nessus.
(Reading database ... 298561 files and directories currently installed.)
Preparing to unpack Nessus-10.3.0-debian9_amd64.deb ...
Unpacking nessus (10.3.0) ...
Setting up nessus (10.3.0) ...
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
```

- Now, enter the following commands.

```
(kali@kali)~[/Downloads]
$ ls
Nessus-10.3.0-debian9_amd64.deb

(kali@kali)~[/Downloads]
$ sudo dpkg -i Nessus-10.3.0-debian9_amd64.deb
[sudo] password for kali:
(Reading database ... 298810 files and directories currently installed.)
Preparing to unpack Nessus-10.3.0-debian9_amd64.deb ...
Unpacking nessus (10.3.0) over (10.3.0) ...
Setting up nessus (10.3.0) ...
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

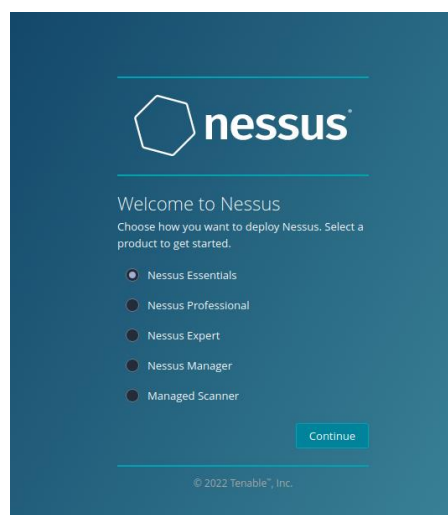
(kali@kali)~[/Downloads]
$ sudo systemctl start nessusd.service
```

- Check the status.

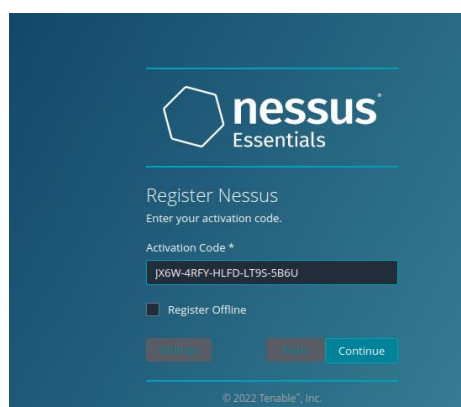
```
(kali@kali)-[~/Downloads]
$ sudo systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; vendor preset: disabled)
   Active: active (running) since Wed 2022-07-27 13:51:48 EDT; 12s ago
     Main PID: 22007 (nessus-service)
        Tasks: 13 (limit: 2264)
      Memory: 127.7M
         CPU: 10.874s
    CGroup: /system.slice/nessusd.service
            └─22007 /opt/nessus/sbin/nessus-service -q
              └─22009 nessusd -q

Jul 27 13:51:48 kali systemd[1]: Started The Nessus Vulnerability Scanner.
Jul 27 13:51:49 kali nessus-service[22009]: Cached 0 plugin libs in 0msec
Jul 27 13:51:49 kali nessus-service[22009]: Cached 0 plugin libs in 0msec
```

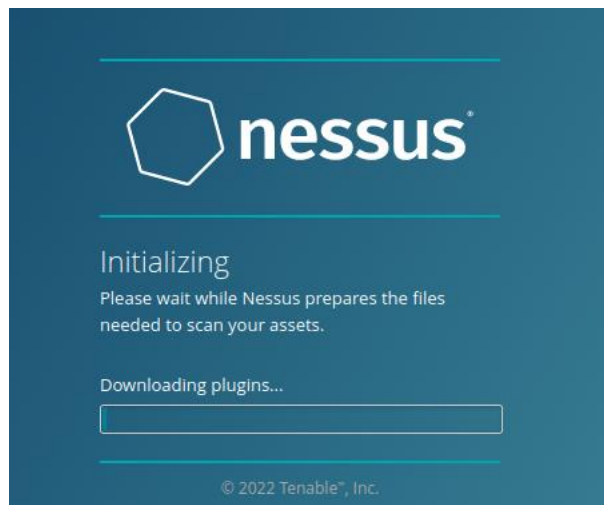
- Go to the link provided and proceed further. (<https://kali:8834>)
- The installation page will arrive



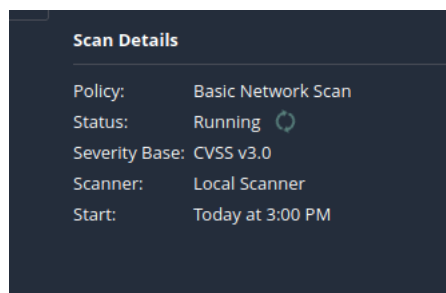
- Apply the activation code.



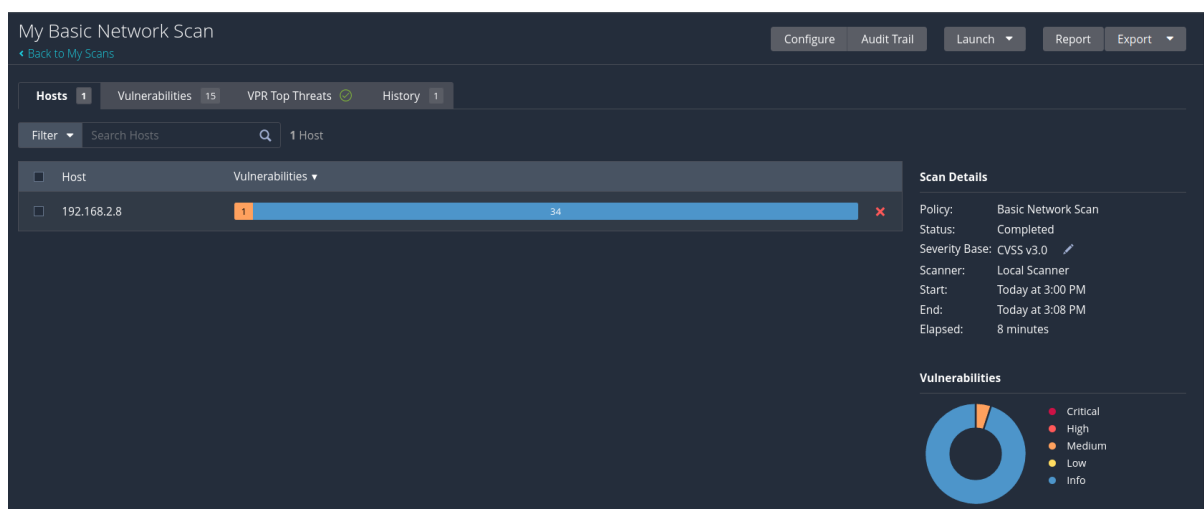
- After providing the user_name and password, download process will begin.





- Once, all plugins are installed, it will prompt you to enter the details of hosts that you want to check for.
- After that, it will start the scanning.




- Once completed, following information will be shown.



<input type="checkbox"/> Sev ▼	Score ▼	Name ▲	Family ▲	Count ▼	⚙
<input type="checkbox"/> MEDIUM	5.3	SMB Signing not required	Misc.	1	🔄 ✎
<input type="checkbox"/> INFO	...	 SMB (Multiple Issues)	Windows	6	🔄 ✎
<input type="checkbox"/> INFO	...	 Microsoft Windows (Multiple Issues)	Windows	2	🔄 ✎
<input type="checkbox"/> INFO		DCE Services Enumeration	Windows	8	🔄 ✎
<input type="checkbox"/> INFO		Nessus SYN scanner	Port scanners	6	🔄 ✎
<input type="checkbox"/> INFO		Service Detection	Service detection	2	🔄 ✎
<input type="checkbox"/> INFO		VMware ESX/GSX Server detection	Service detection	2	🔄 ✎
<input type="checkbox"/> INFO		Common Platform Enumeration (CPE)	General	1	🔄 ✎
<input type="checkbox"/> INFO		Device Type	General	1	🔄 ✎
<input type="checkbox"/> INFO		Nessus Scan Information	Settings	1	🔄 ✎
<input type="checkbox"/> INFO		OS Identification	General	1	🔄 ✎

Hosts 1
Vulnerabilities 15
VPR Top Threats 🟢
History 1



Assessed Threat Level: **None**

No vulnerabilities have been found as prioritized by Tenable's patented Vulnerability Priority Rating (VPR) system.
To learn more about Tenable's VPR scoring system, see [Predictive Prioritization](#).

No prioritized vulnerabilities found.

CONCLUSION:

- By performing the above practical, I learnt how to scan for vulnerability using Nessus essentials software.