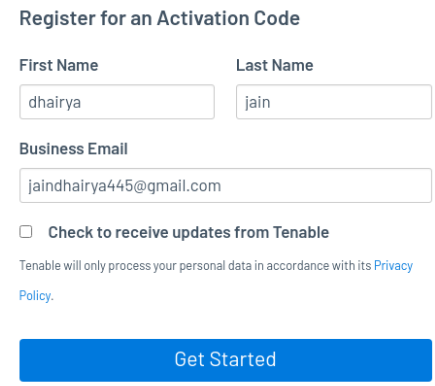

# PRATICAL FILE

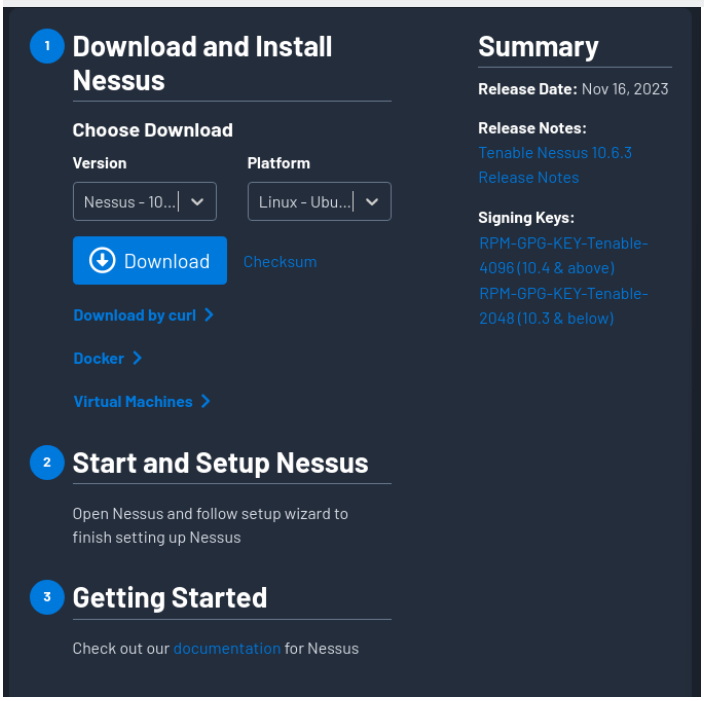
Dr. Gopal Singh Rawat
Course- Physical IT & Sec

Dhairya Jain
500105432 | R2142220251
B.Tech_CSE_CSF_B-1_Sem-III

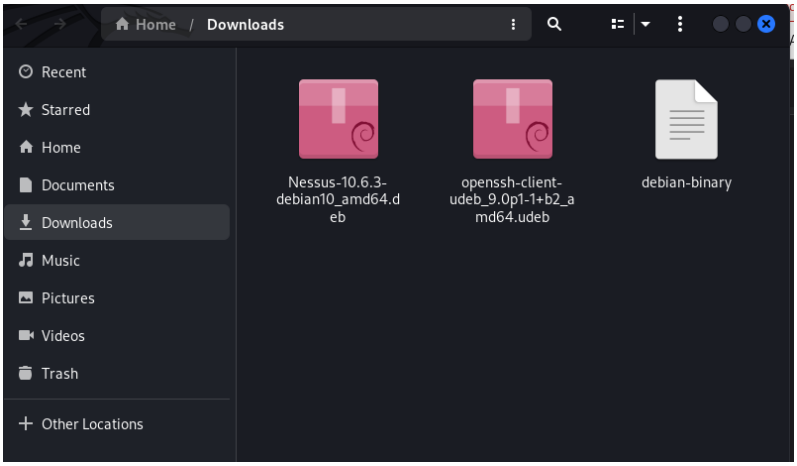
**Aim-** Nessus

- Download Nessus : https://www.tenable.com/downloads/nessus



- Install Nessus via terminal or Package Installer




- depackaging nessus using terminal

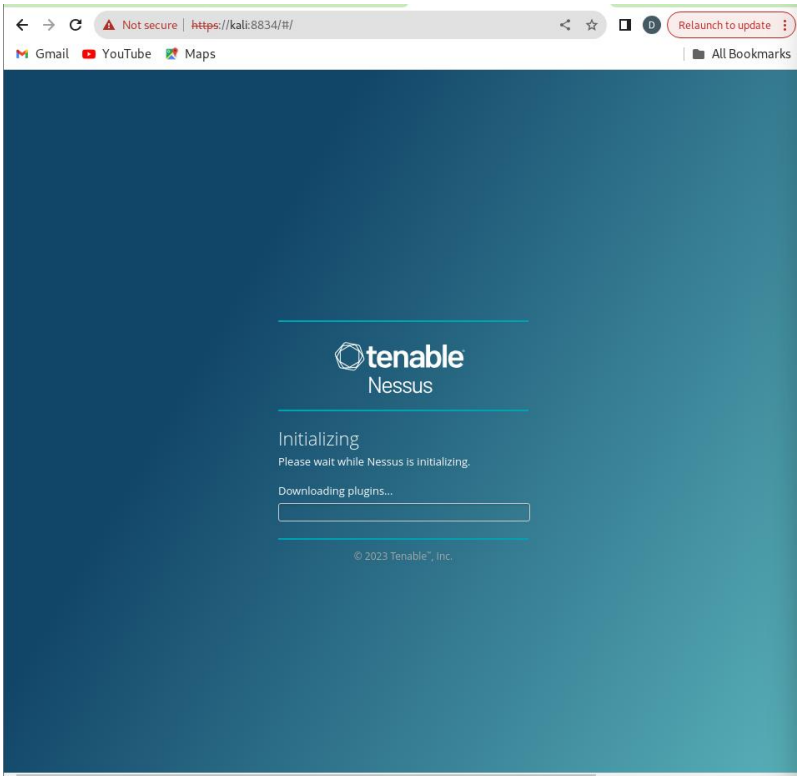
```
┌──(root㉿kali)-[/home/dhairya/Downloads]
└─# dpkg -i "Nessus-10.6.3-debian10_amd64.deb"
Selecting previously unselected package nessus.
(Reading database ... 395159 files and directories currently installed.)
Preparing to unpack Nessus-10.6.3-debian10_amd64.deb ...
Unpacking nessus (10.6.3) ...
Setting up nessus (10.6.3) ...
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.service
 - Then go to https://kali:8834/ to configure your scanner
```

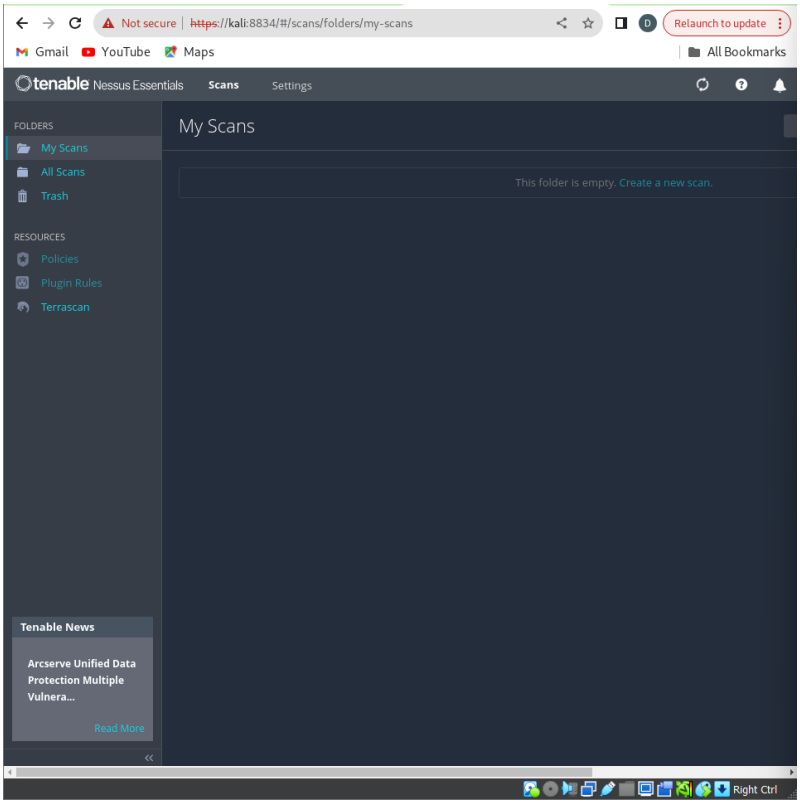
- service nessusd start

```
┌──(root㉿kali)-[/home/dhairya/Downloads]
└─# service nessusd start
```

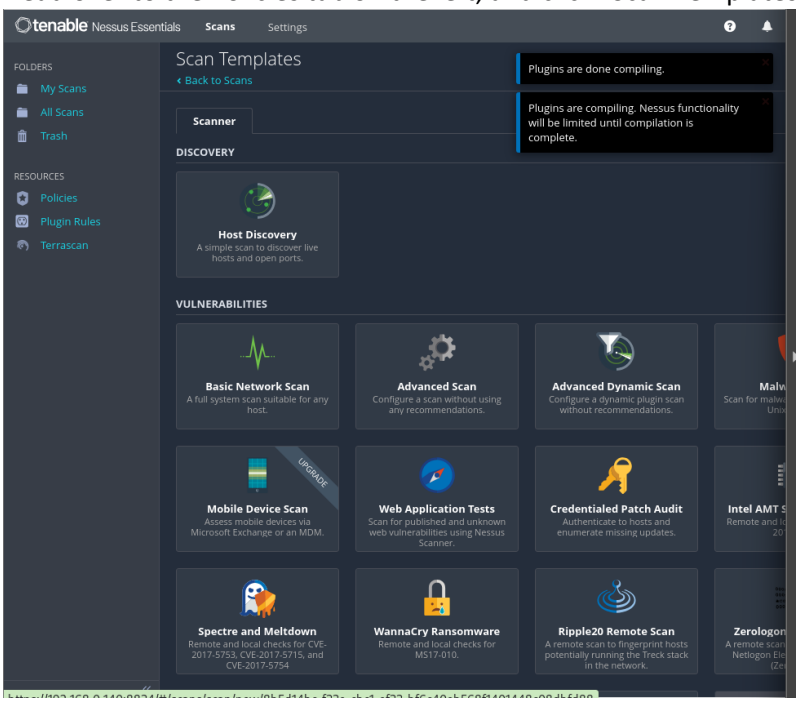
- go to : https://kali:8834/

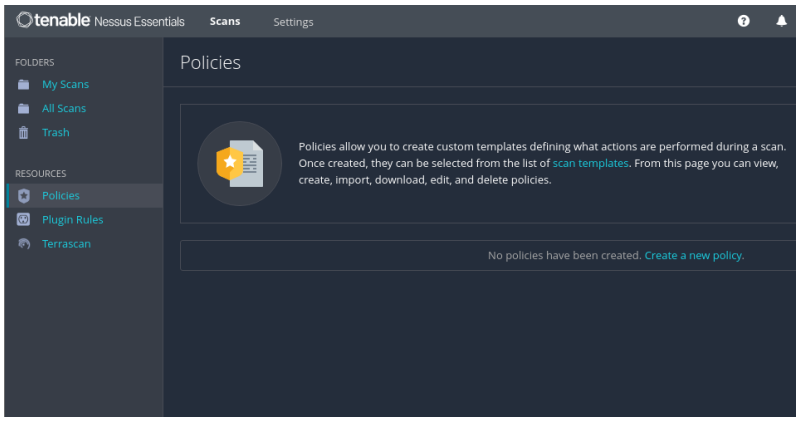



- Nessus interface



- Next we're going to perform a simple scan of our own machine to demonstrate how scans work, and what the results look like.
- Head over to the Policies tab on the left, and click "Scan Templates" in the description text.

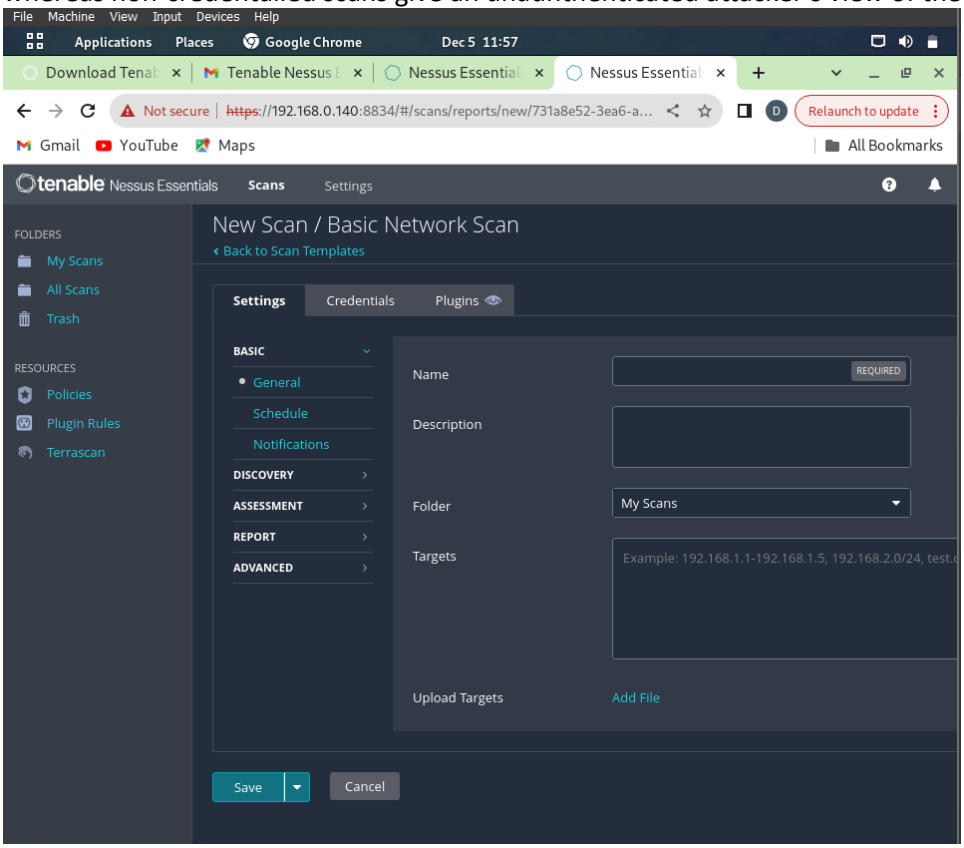



Follow the below steps

- After clicking on our scan template, we'll be able to customize the settings for this specific scan.
- Take a look at all of the settings you can change, as well as the Credentials tab, and Plugins tab.
- They allow the scanner to log into the system, and collect much more valuable information, as
- opposed to being locked out and only being able to collect surface information.
  Companies will usually run credentialed scans internally to get the most valuable information,

whereas non-credentailed scans give an unaunthenticated attacker's view of the network.



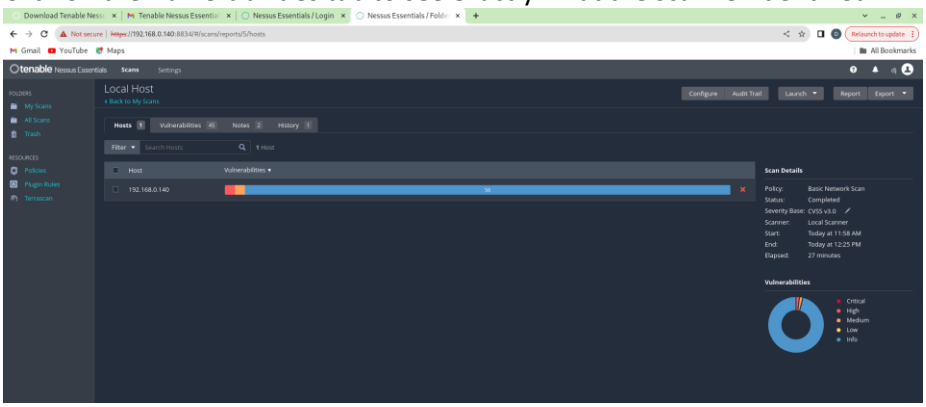

Follow the steps

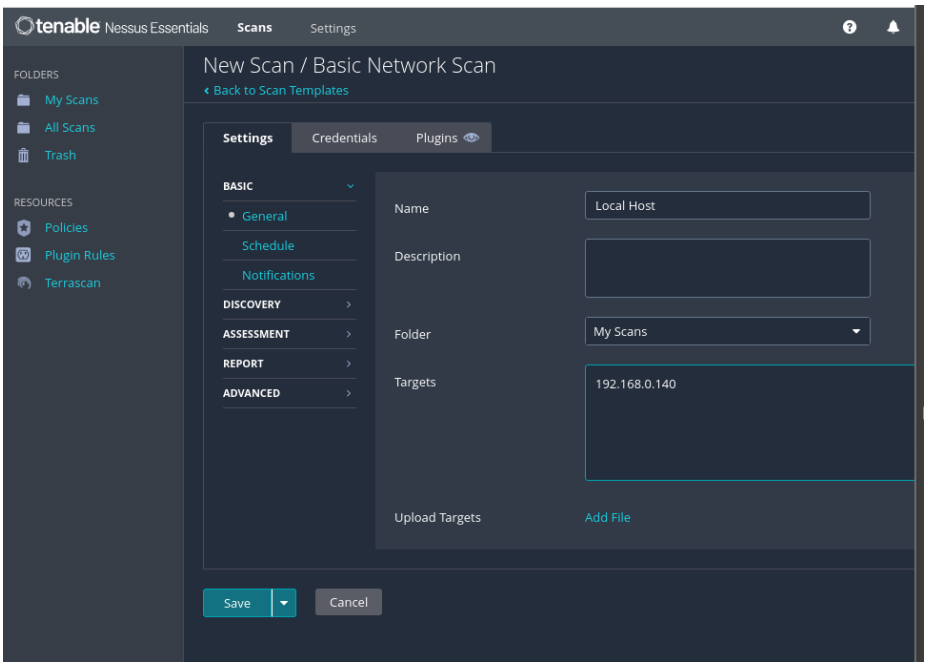
- Click Save in the bottom left-hand corner, and you'll be taken to the "My Scans" page.
- From here, we can launch our scan by pressing on the play icon to the right.

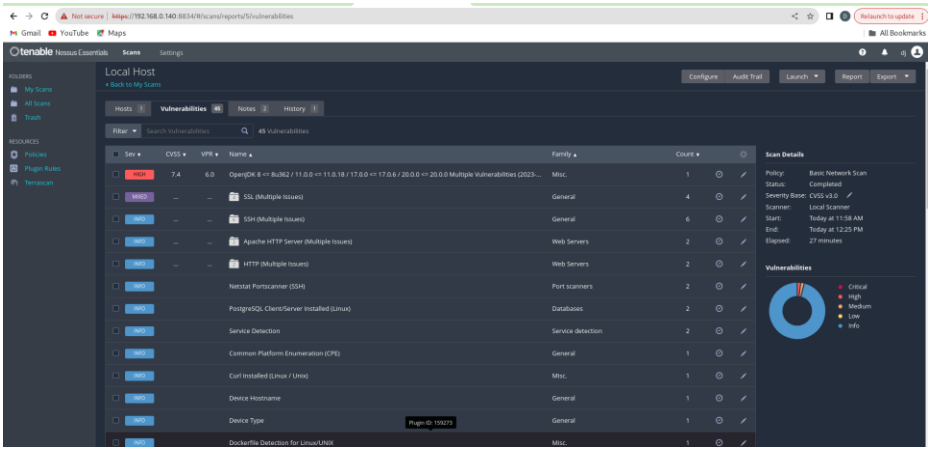

Follow the steps

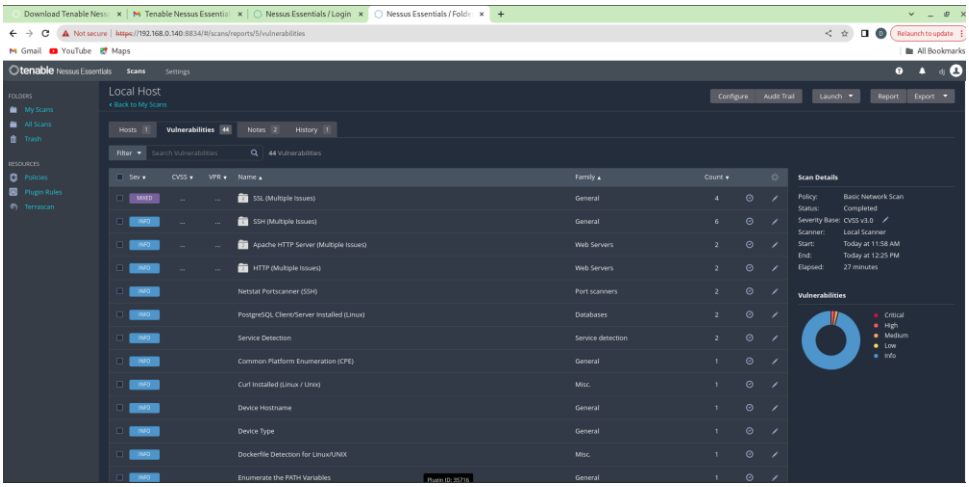
- Once clicked, the scan will get to work. Once it's finished, a tick will appear, and we'll be able to take a look at the results.
- This is the results pane and provides us with all of the information the scan collected. On the left we have a list of hosts scanned, along with a summary of any vulnerabilities discovered.
- This would be full of different hosts if we were scanning an entire network and is arranged by criticality of vulnerability by default.
- On the right we have the Scan Details, and below it we have a donut chart for the security issues identified.

- Click on the Vulnerabilities tab to see exactly what the scanner identified.






Download Tenable Ness
Tenable Nessus Essential
Nessus Essentials / Login
Nessus Essentials / Folde
Not secure
https://192.168.0.140:8834/#/scans/reports/5/vulnerabilities
Relaunch to update
Gmail
YouTube
Maps
All Bookmarks
tenable Nessus Essentials
Scans
Settings
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Local Host
« Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 44
Notes 2
History 1
Filter
Search Vulnerabilities
44 Vulnerabilities
Sev
CVSS
VPR
Name
Family
Count
MIXED
SSL (Multiple Issues)
General
4
INFO
SSH (Multiple Issues)
General
6
Apache HTTP Server (Multiple Issues)
Web Servers
2
HTTP (Multiple Issues)
Web Servers
2
Netstat Portscanner (SSH)
Port scanners
2
PostgreSQL Client/Server Installed (Linux)
Databases
2
Service Detection
Service detection
2
Common Platform Enumeration (CPE)
General
1
Curl Installed (Linux / Unix)
Misc.
1
Device Hostname
General
1
Device Type
General
1
Dockerfile Detection for Linux/UNIX
Misc.
1
Enumerate the PATH Variables
General
1
Plugin ID: 35716
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:58 AM
End: Today at 12:25 PM
Elapsed: 27 minutes
Vulnerabilities
Critical
High
Medium
Low
Info