

Perform a Basic Vulnerability Scan on Your PC (Tenable Nessus Essentials)

1. Install Nessus Essentials

Download Nessus Essentials from Tenable

- Register With Email ID for Trial (Activation Code)

Kali CLI — install & start Nessus

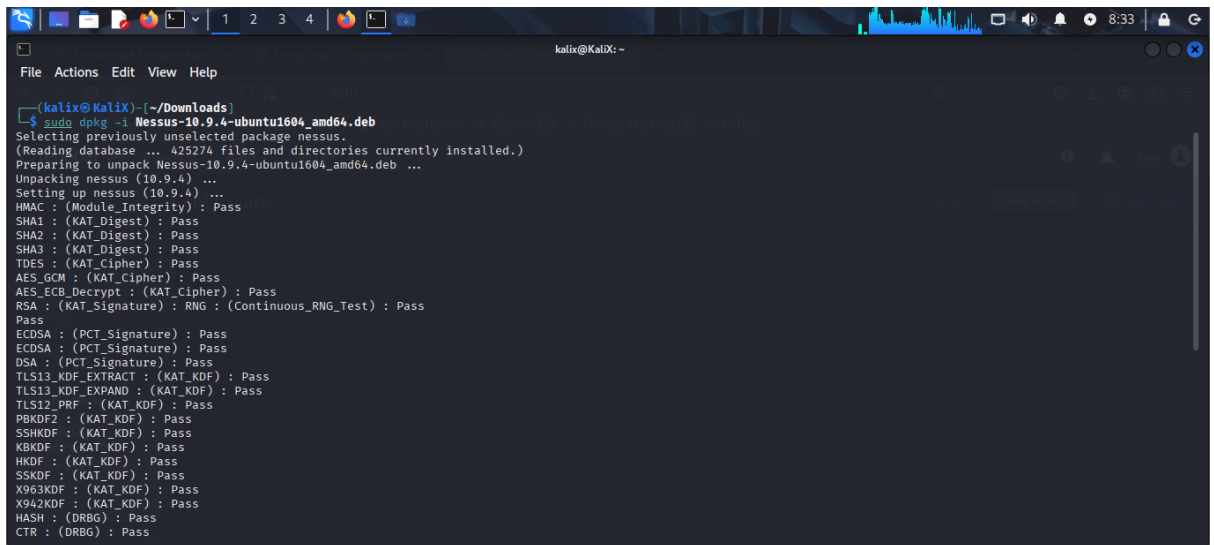
- **Install** the Nessus DEB package

```
$sudo dpkg -i Nessus-10.9.3-ubuntu1604_amd64.deb
```

- **Start** and enable the Nessus

```
$ sudo systemctl start nessusd.service
```

```
#sudo systemctl enable nessusd.service
```



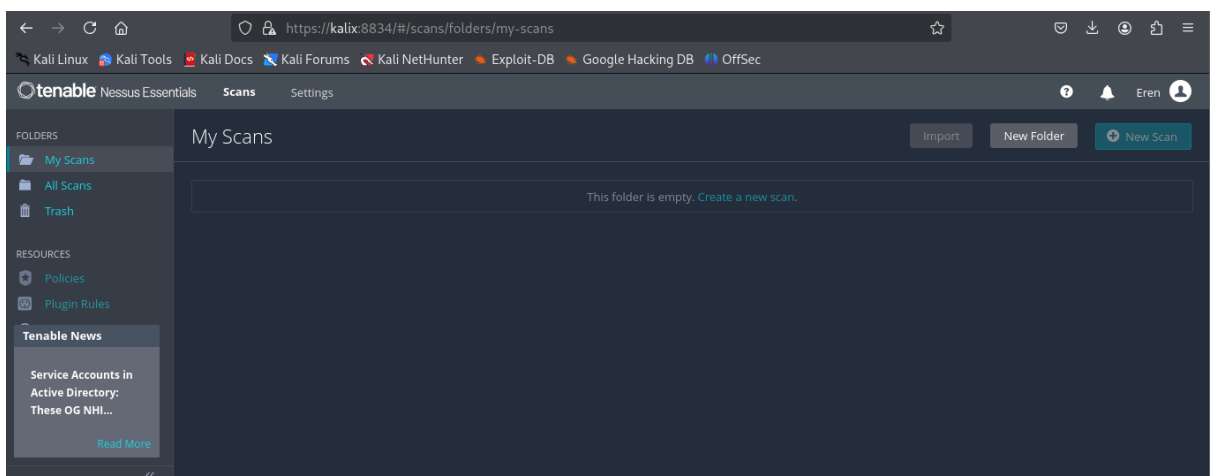
```
(kalix@KaliX)-[~/Downloads]
$ sudo dpkg -i Nessus-10.9.4-ubuntu1604_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 425274 files and directories currently installed.)
Preparing to unpack Nessus-10.9.4-ubuntu1604_amd64.deb ...
Unpacking nessus (10.9.4) ...
Setting up nessus (10.9.4) ...
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
HKDF : (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
```

2. Access Nessus on Browser

Open a **browser on the Kali machine** and type:

- <https://localhost:8834/>

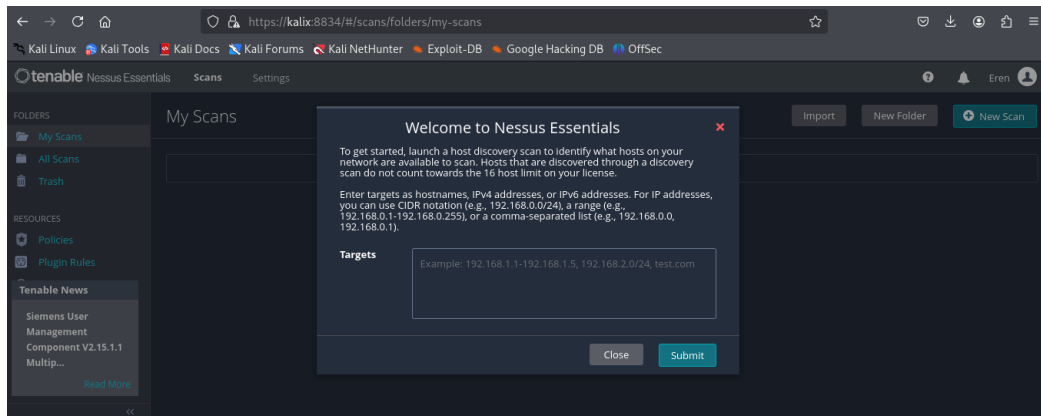
Activate and download the plugins.



3. Create a target & run a scan

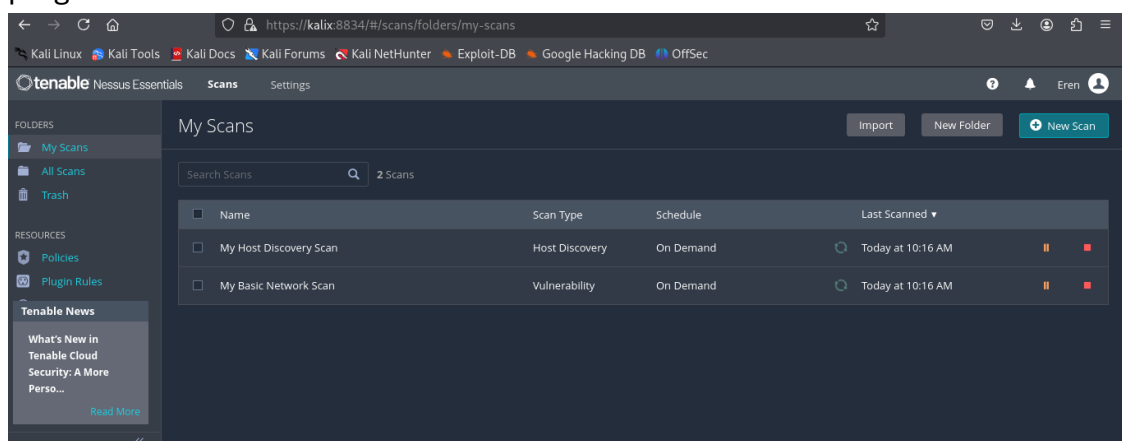
After you log in:

1. **Scans** → **New Scan** (upper-right)
2. From the **Scan Templates** page choose **Basic Network Scan** (recommended for a first, full scan).



3. Configure the new scan:

- **Name:** Localhost - Basic Scan
 - **Targets:** 127.0.0.1 to scan local machine; or your LAN IP like 192.168.1.100 if scanning from Kali to another host.
 - (Optional) **Credentials** tab: add SSH credentials for a credentialed Linux scan (this gives deeper checks). *Only add credentials you own.*
 - (Optional) **Plugins / Port Scanning / Advanced options** — accept defaults for first run.
4. **Save** then **Launch** the scan.
 5. Monitor progress on **Scans** → **My Scans**. Click the running job to view live progress and counts.

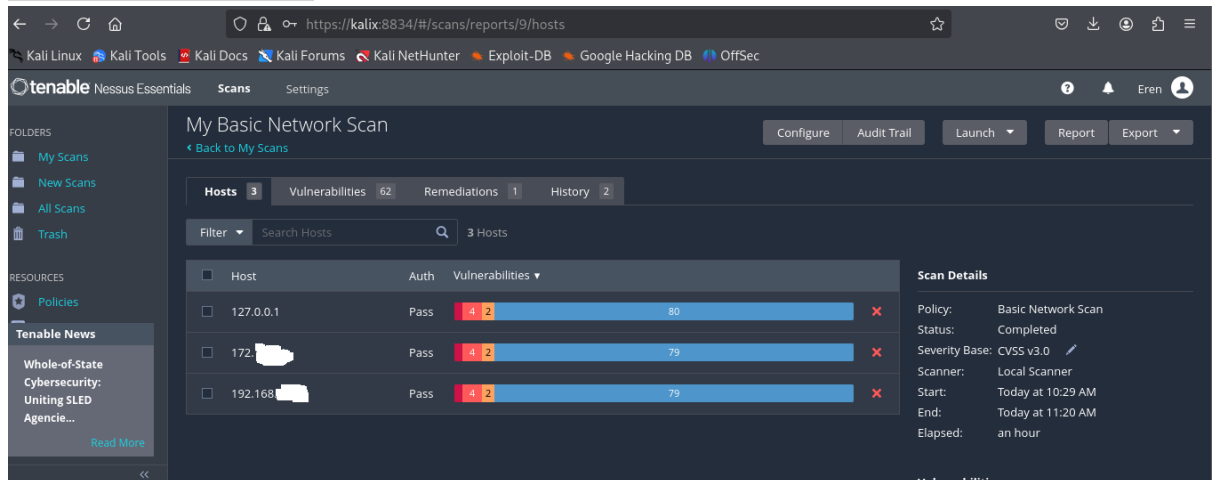


Timing: First full scan of a single host typically **~30–60 minutes**, depending on scan depth and system resources.

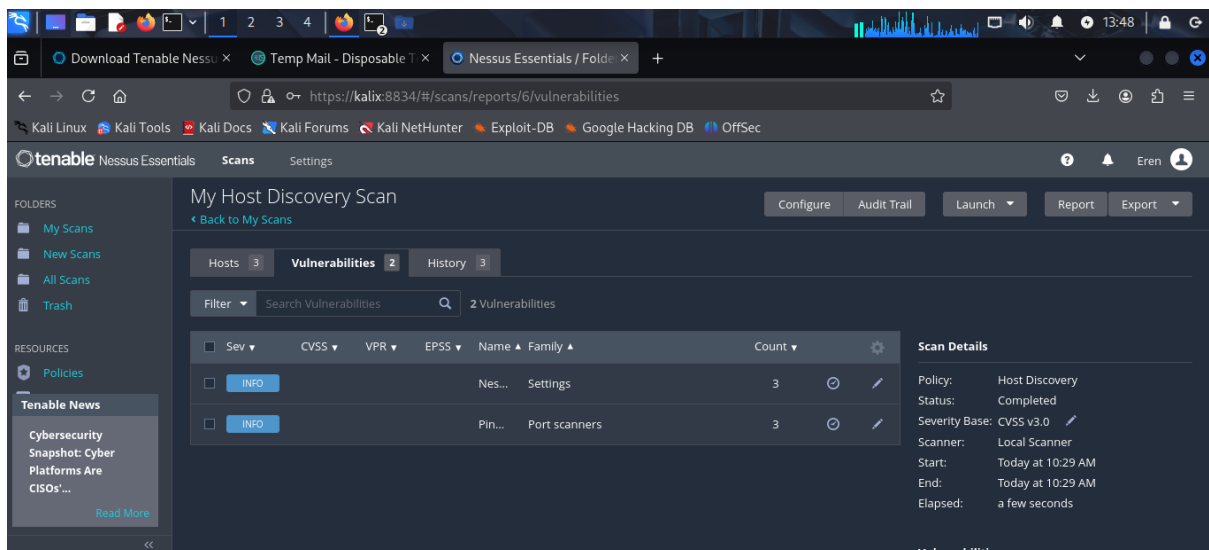
4. View results & export report

When the scan completes:

1. Open the completed scan result (Scans → click scan name).
2. Explore Vulnerabilities.



3. To export: click **Export** (upper-right of scan results) → choose **Nessus (.nessus)**. Save the file to your Kali `~/Documents` or `~/Downloads` or repo folder.



5. Interpreting results & basic remediation commands (Kali examples)

For each *Critical* / *High* item, record:

- vulnerability name, CVE(s), evidence, affected package/service, and remediation steps.

Common fixes (Commands)

1. Update all packages (fixes many outdated software issues)

`$sudo apt update && sudo apt full-upgrade -y`

2. Check open/listening ports (see what Nessus may have flagged)

```
$sudo ss -tulpen
```

3. Stop & disable unnecessary service (example: ftp)

```
$sudo systemctl stop vsftpd.service
```

```
$sudo systemctl disable vsftpd.service
```

4. Harden SSH (example: disable password auth if using keys)

```
$sudo sed -i 's/^#PasswordAuthentication yes/PasswordAuthentication no/'  
/etc/ssh/sshd_config
```

```
$sudo systemctl restart sshd
```

5. Reboot after large kernel / core updates

```
$sudo reboot
```