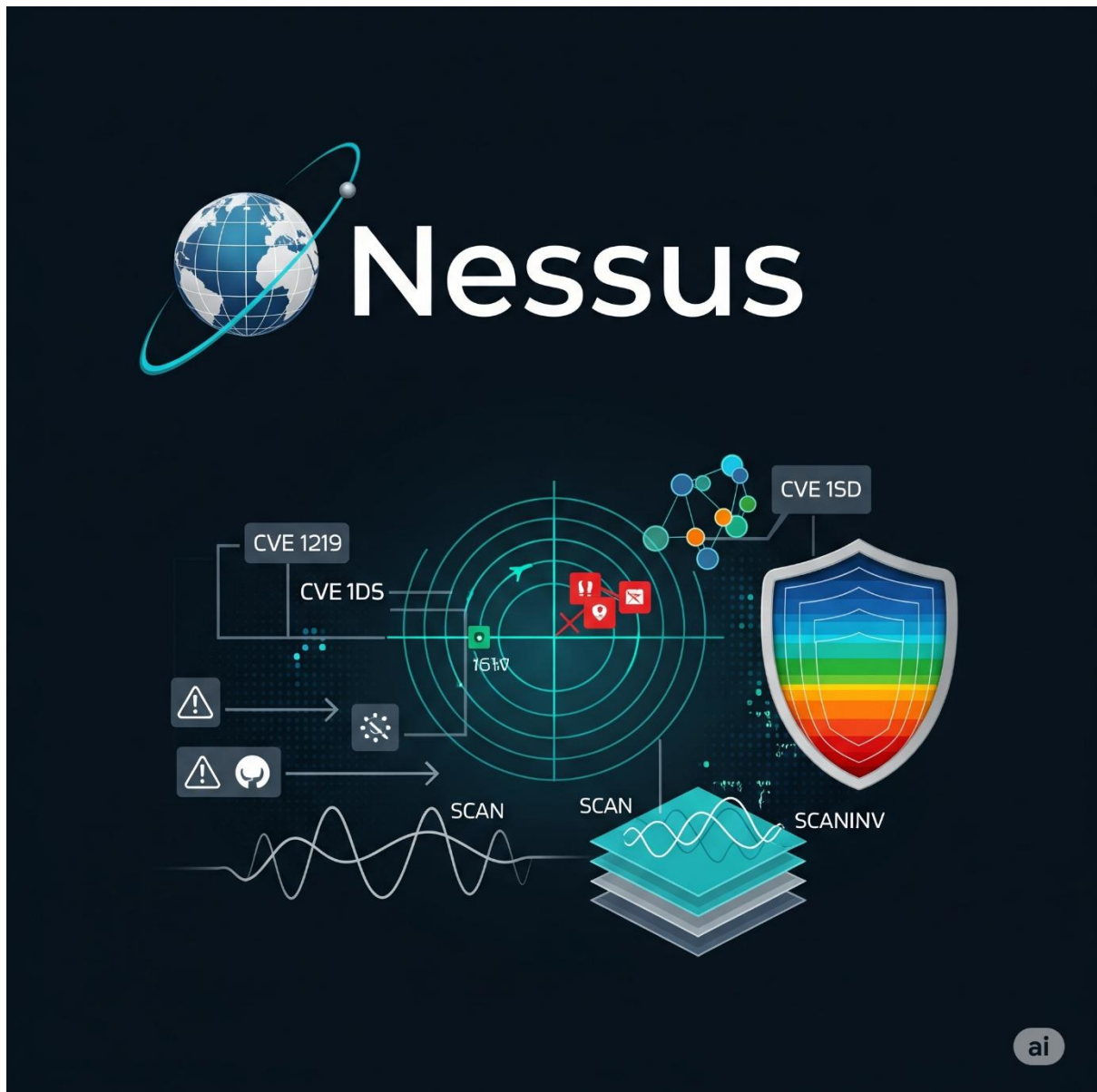


Day 10 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: Nessus



Contact Me: ayeshanm8@gmail.com

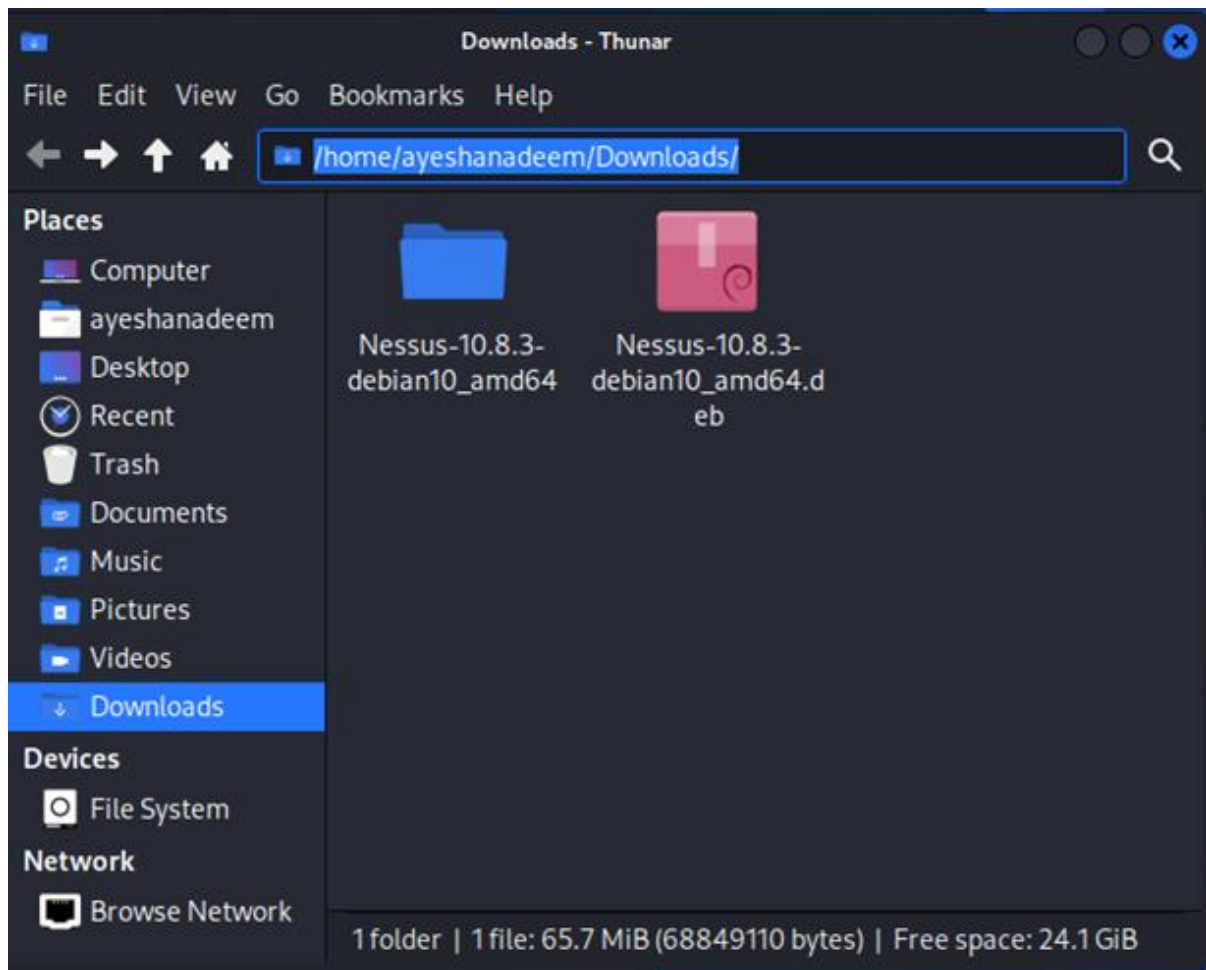
Date: 10th July, 2025

Nessus: Vulnerability Assessment Engine

Task 1: Install and Download Nessus

- Download Nessus
- Install Nessus.
- Setup scanners and verify their installation.

Nessus download:



Nessus Installation:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ cd /home/ayeshanadeem/Downloads/

(ayeshanadeem@ayeshanadeem)-[~/Downloads]
$ sudo dpkg -i Nessus-10.8.3-debian10_amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 448409 files and directories currently installed.)
Preparing to unpack Nessus-10.8.3-debian10_amd64.deb ...
Unpacking nessus (10.8.3) ...
Setting up nessus (10.8.3) ...
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://ayeshanadeem:8834/ to configure your scanner

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

Verify Nessus is in running condition:

```
(ayeshanadeem@ayeshanadeem) [~/Downloads]
$ sudo systemctl status nessusd
[sudo] password for ayeshanadeem:
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Thu 2025-03-20 10:53:50 EDT; 1h 47min ago
 Invocation: 933f02c2cd7b41e2a3c1e7437cb9f339
   Main PID: 5710 (nessus-service)
      Tasks: 20 (limit: 2210)
  Memory: 338.5M (peak: 1.2G, swap: 36M, swap peak: 63.1M)
     CPU: 4min 16.744s
    CGroup: /system.slice/nessusd.service
            └─5710 /opt/nessus/sbin/nessus-service -q
              └─5712 nessusd -q

Mar 20 10:53:50 ayeshanadeem systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
Mar 20 10:54:25 ayeshanadeem nessus-service[5712]: Cached 306 plugin libs in 102msec
Mar 20 10:54:25 ayeshanadeem nessus-service[5712]: Cached 306 plugin libs in 276msec

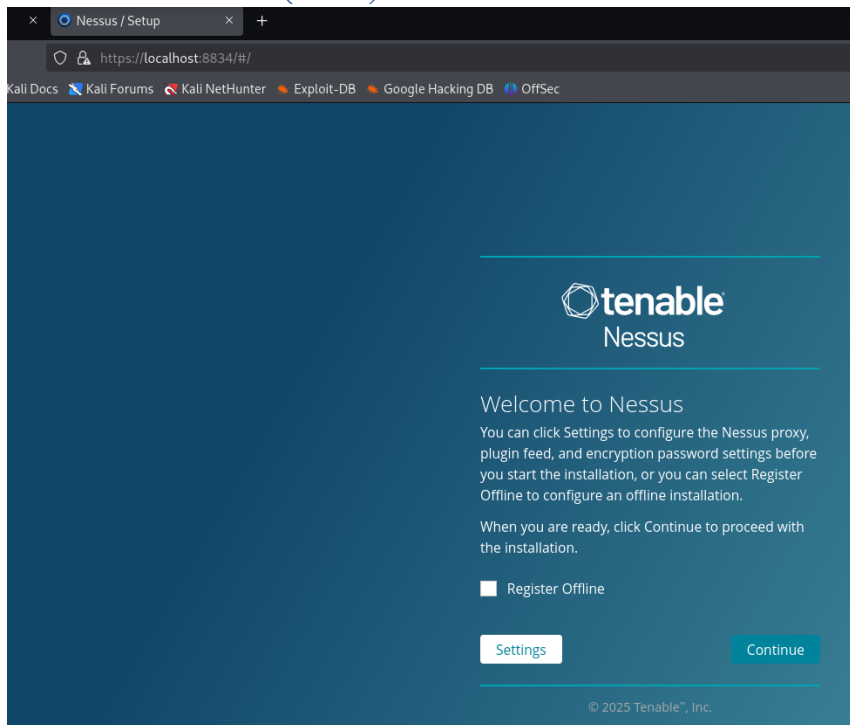
(ayeshanadeem@ayeshanadeem) [~/Downloads]
```

Task 4: Configure and Start Nessus

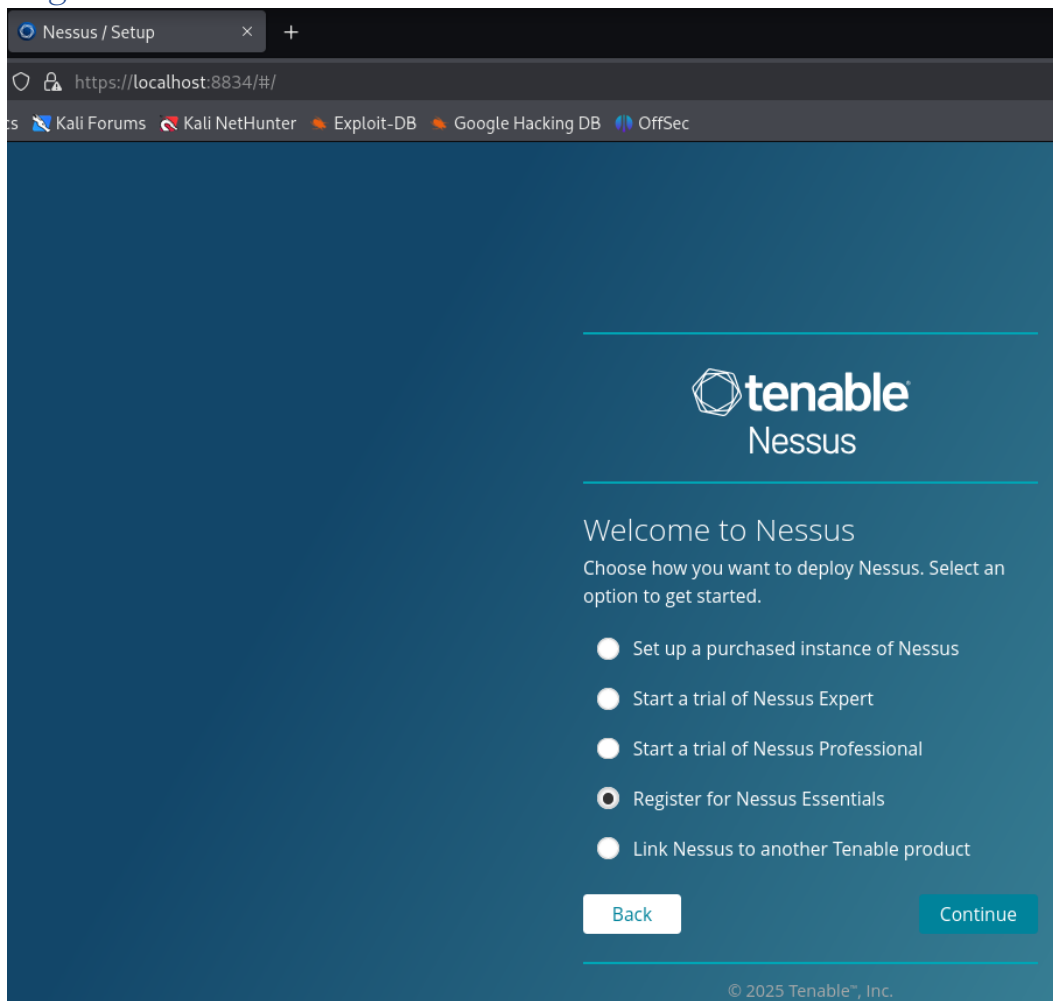
- Start the Nessus service.
- Register and activate Nessus Essentials.
- Login and explore the Nessus interface.

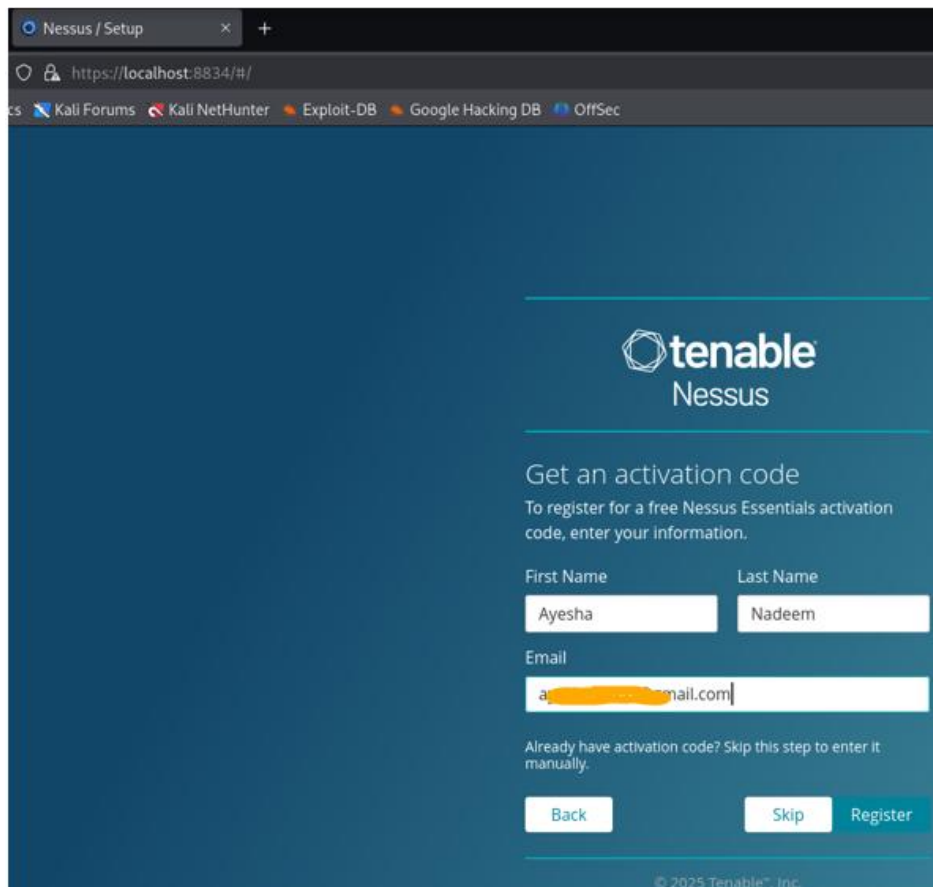
Type <https://localhost:8834> on firefox browser

Tenable Interface (Start) :



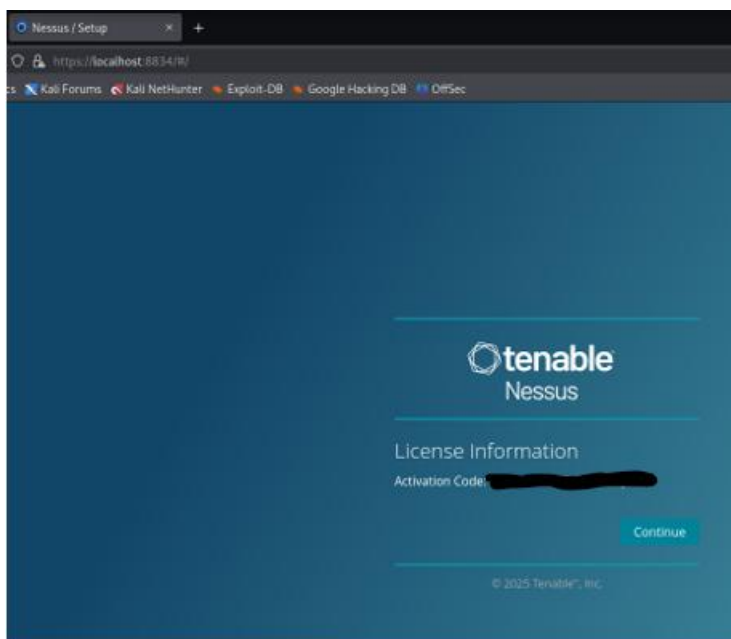
Register and Activated Nessus Essential:





The screenshot shows a web browser window with the title "Nessus / Setup". The address bar displays "https://localhost:8834/#/". The browser's tab bar includes links to "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area features the Tenable Nessus logo and the heading "Get an activation code". Below this, a subheading reads "To register for a free Nessus Essentials activation code, enter your information." The registration form consists of three input fields: "First Name" (containing "Ayesha"), "Last Name" (containing "Nadeem"), and "Email" (containing "a. [redacted]@gmail.com"). A link "Already have activation code? Skip this step to enter it manually." is positioned below the email field. At the bottom of the form are three buttons: "Back", "Skip", and "Register". The footer of the page displays "© 2025 Tenable®, Inc."

→ Clicked Register:



The screenshot shows the "License Information" screen after clicking "Register". The Tenable Nessus logo is at the top. Below it, the heading "License Information" is displayed. Under this heading, the text "Activation Code:" is followed by a blacked-out activation code. A "Continue" button is located at the bottom right of the form. The footer of the page displays "© 2025 Tenable®, Inc."

Nessus / Setup

https://localhost:8834/#/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable
Nessus

Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

Back Submit

© 2025 Tenable™, Inc.

Nessus / Initializing

https://localhost:8834/#/

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

tenable
Nessus

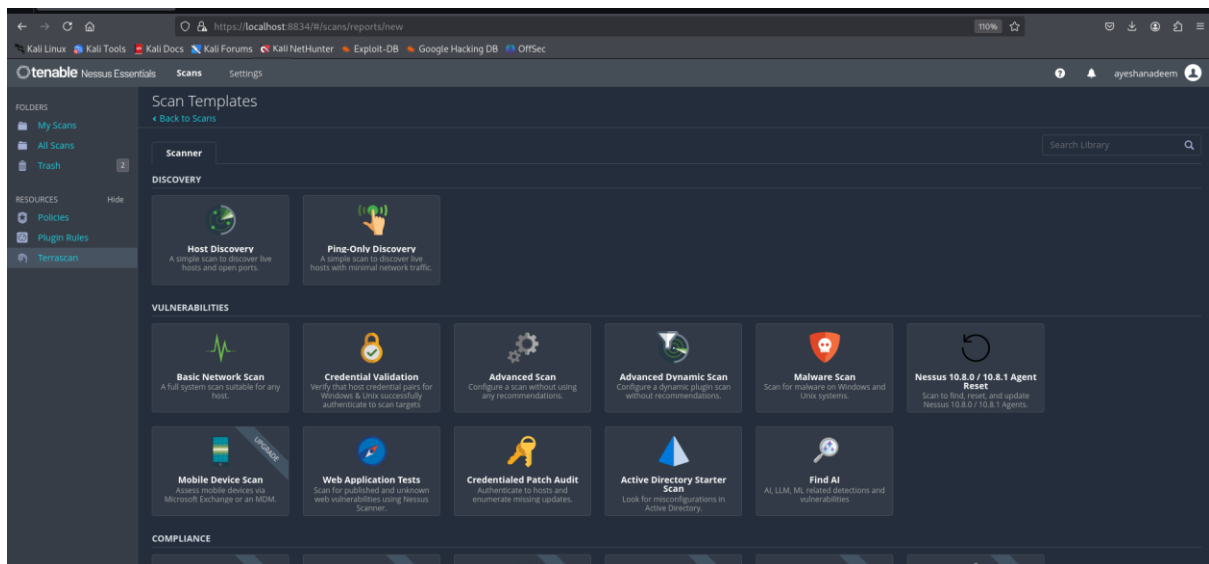
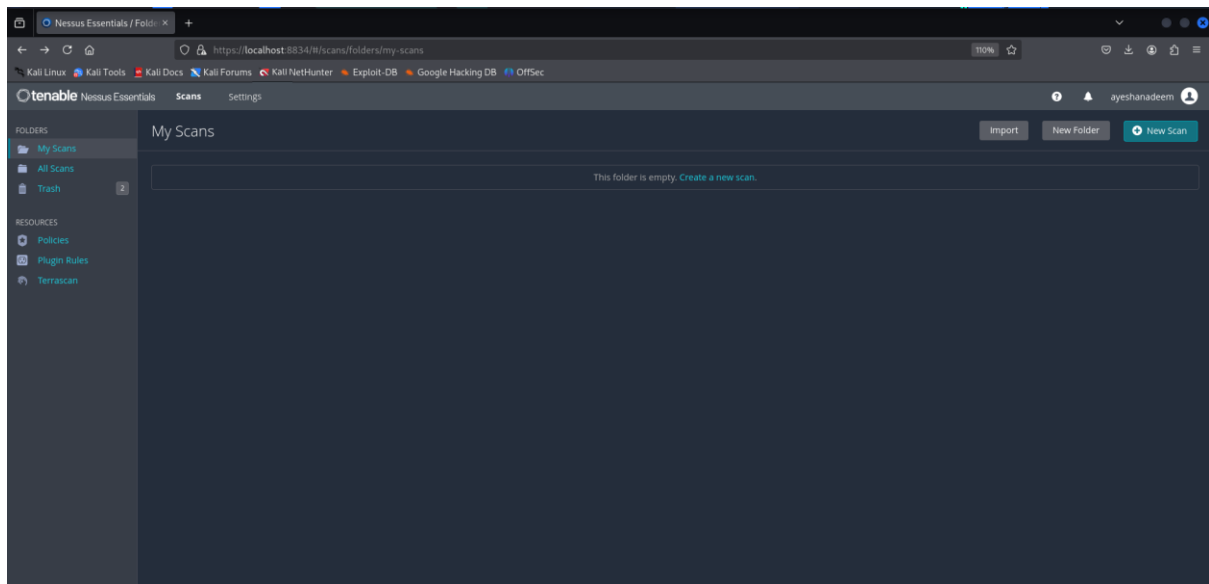
Initializing

Please wait while Nessus is initializing.

Downloading plugins...

© 2025 Tenable™, Inc.

My dashboard:



Task 5: Perform a Basic Vulnerability Scan Using Nessus

- Create a new scan task.
- Configure scan settings and targets.
- Run and analyze scan results.

Targetting cust.edu.pk:

- Fetch ip of cust through ping
- Fetch ip of cust through nslookup

```
Pinging cust.edu.pk [162.159.135.42] with 32 bytes of data:
Reply from 162.159.135.42: bytes=32 time=241ms TTL=53
Reply from 162.159.135.42: bytes=32 time=156ms TTL=53
Reply from 162.159.135.42: bytes=32 time=172ms TTL=53
Reply from 162.159.135.42: bytes=32 time=192ms TTL=53

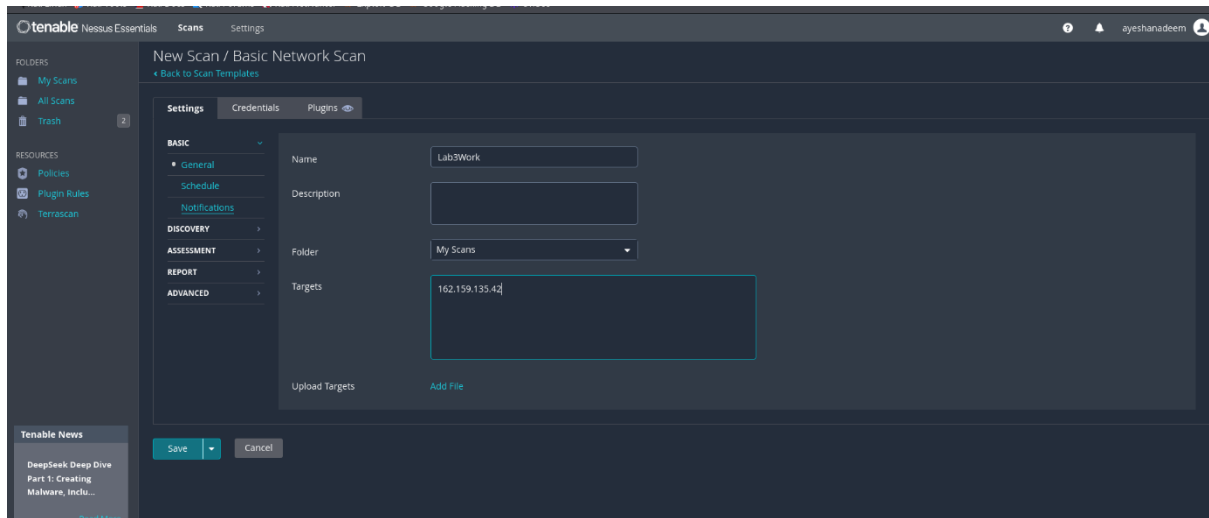
Ping statistics for 162.159.135.42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 156ms, Maximum = 241ms, Average = 190ms

C:\Users\Nadeem Arif>nslookup cust.edu.pk
Server:    UnKnown
Address:   192.168.64.37

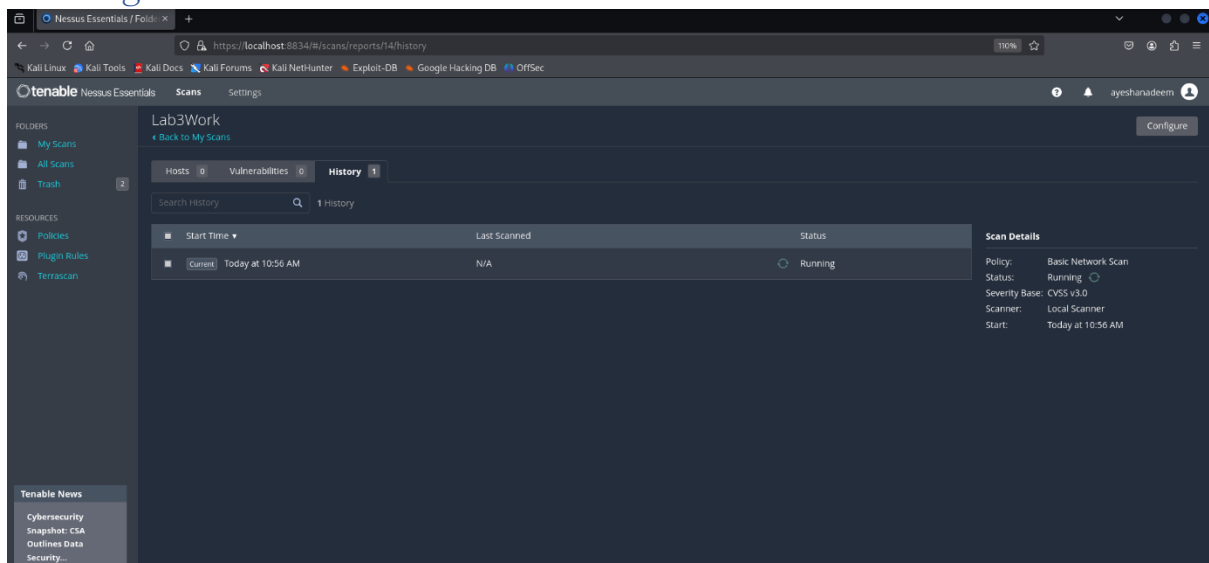
Non-authoritative answer:
Name:     cust.edu.pk
Address:  162.159.135.42
```

Setting parameters:

Just hit on scan button, you will see this interface. Here set you target and give any name to you scan.



Running the scan:



17 minor Vulnerabilities Found

The screenshot shows the Nessus Essentials interface for a scan named 'Lab3Work'. The 'Vulnerabilities' tab is selected, showing a table with 1 host and 17 vulnerabilities. The scan details on the right indicate a Basic Network Scan completed at 10:36 AM.

Host	Vulnerabilities
162.159.135.42	17

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 10:36 AM
- End: Today at 12:10 PM
- Elapsed: an hour

Vulnerabilities

A donut chart shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

The screenshot shows the Nessus Essentials interface for a scan named 'Lab3Work'. The 'Vulnerabilities' tab is selected, showing a table with 17 vulnerabilities. The scan details on the right indicate a Basic Network Scan completed at 10:36 AM.

Sev	CVSS	VPR	EPSS	Name	Family	Count
Info	SSL (Multiple Issues)	General	30
Info	HTTP (Multiple Issues)	Web Servers	26
Info	TLS (Multiple Issues)	General	18
Info	IETF Mds (Multiple Issues)	General	12
Info	TLS (Multiple Issues)	Misc.	12
Info	TLS (Multiple Issues)	Service detection	12
Info	Service Detection	Service detection	16
Info	Nessus SYN scanner	Port scanners	13
Info	SSL Certificate Chain Contains Certificates Expiring Soon	Misc.	6
Info	Additional DNS Hostnames	General	1
Info	Common Platform Enumeration (CPE Plugin ID: S4615)	General	1

Scan Details

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 10:36 AM
- End: Today at 12:10 PM
- Elapsed: an hour

Vulnerabilities

A donut chart shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

My Exploration:

Tools Scans Settings

Family: Web Servers
Published: January 30, 2007
Modified: February 26, 2024

Output

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Warning :
more...

To see debug logs, please visit individual host

Port	Hosts
80/tcp/www	162.159.135.42

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
HTTP/2 TLS Support: Yes
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Warning :
more...

To see debug logs, please visit individual host

Port	Hosts
443/tcp/www	162.159.135.42

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

Tools Scans Settings

Family: Web Servers
Published: January 30, 2007
Modified: February 26, 2024

Output

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
HTTP/2 TLS Support: Yes
HTTP/2 Cleartext Support: No
SSL : yes
Keep-Alive : no
Options allowed : (Not implemented)
Warning :
more...

To see debug logs, please visit individual host

Port	Hosts
2087/tcp/www	162.159.135.42

Response Code : HTTP/1.1 403 Forbidden

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Warning :
more...

To see debug logs, please visit individual host

Port	Hosts
2093/tcp/www	162.159.135.42

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

Tools Scans Settings

OS Fingerprints Detected

Description

Using a combination of remote probes (TCP/IP, SMB, HTTP, NTP, SNMP, etc), it was possible to gather one or more fingerprints from the remote system. While the highest-confidence result was reported in plugin 11936, "OS Identification", the complete set of fingerprints detected are reported here.

Output

Following OS Fingerprints were found

Remote operating system : AIX 5.3
Confidence level : 65
Method : SInFP
Type : general-purpose
Fingerprint : SInFP:
P1: B11013:F0X12:M65535:00204ffff:M1460:
P2: B11013:F0X12:M65535:00204ffff:M1460:
P3: B00000:F0X00:M0:00:M0
P4: 191003_7_p=443K

Following fingerprints could not be used to determine OS :
HTTP: Server: cloudflare
SSLCert: I:/CN:WE11/O:Google Trust Services/CN:kinsta.cloud
c44fc103d72575064ffe01778d1ea7281b06ee5c
I:/CN:WE11/O:Google Trust Services/CN:kinsta.cloud
c44fc103d72575064ffe01778d1ea7281b06ee5c
I:/CN:WE11/O:Google Trust Services/CN:kinsta.cloud
c44fc103d72575064ffe01778d1ea7281b06ee5c

Plugin Details

Severity: Info
ID: 209654
Version: 1.3
Type: combined
Family: General
Published: February 26, 2025
Modified: March 3, 2025

Risk Information

Risk Factor: None

Vulnerability Information

Asset Inventory: True

