

# **Martin**

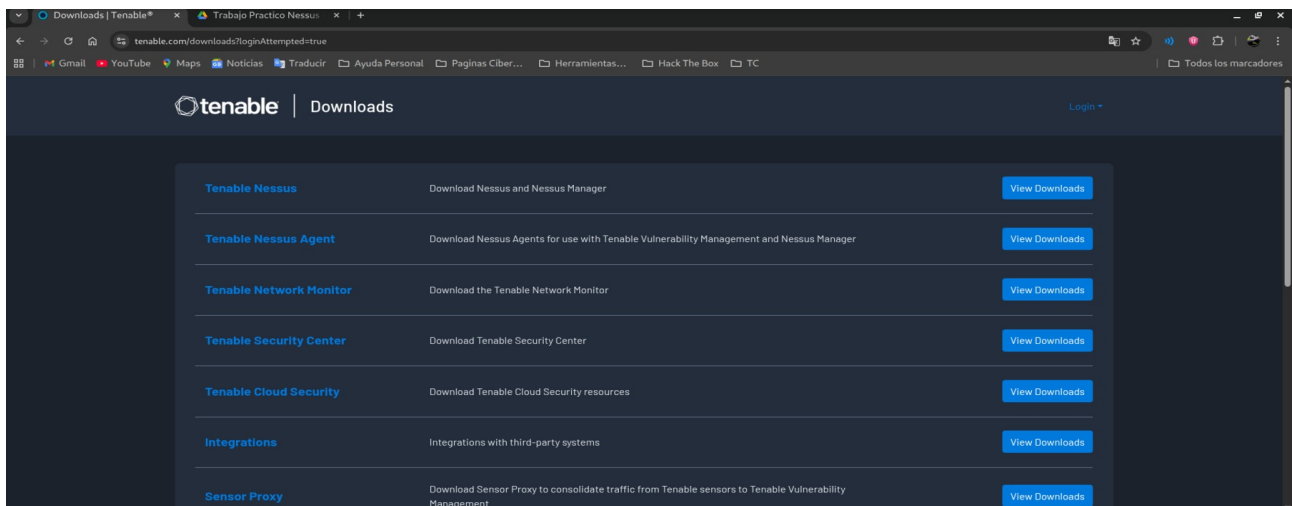
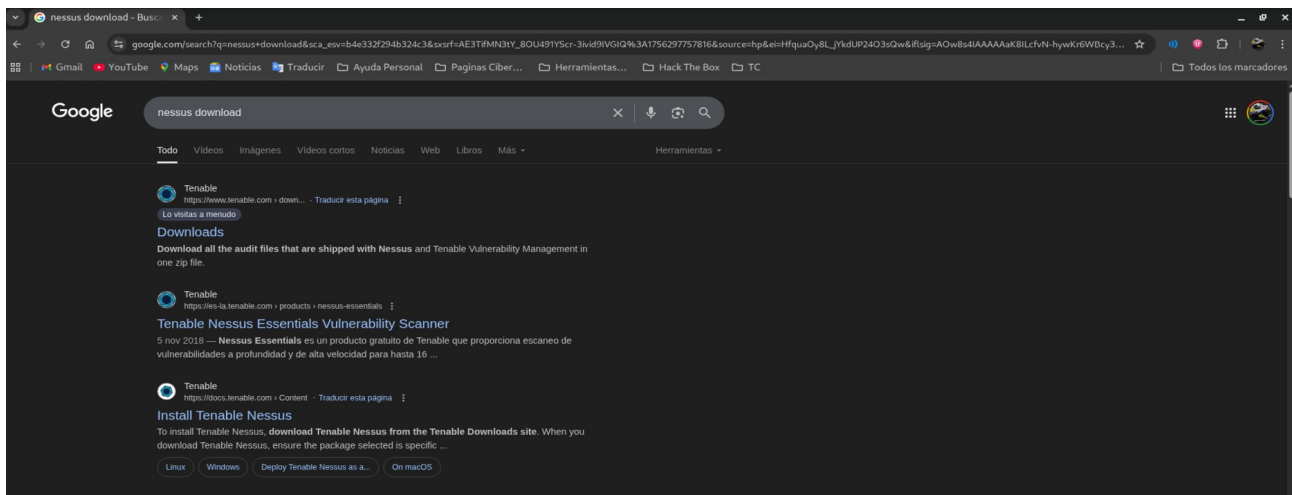
# **Dalla Pozza**

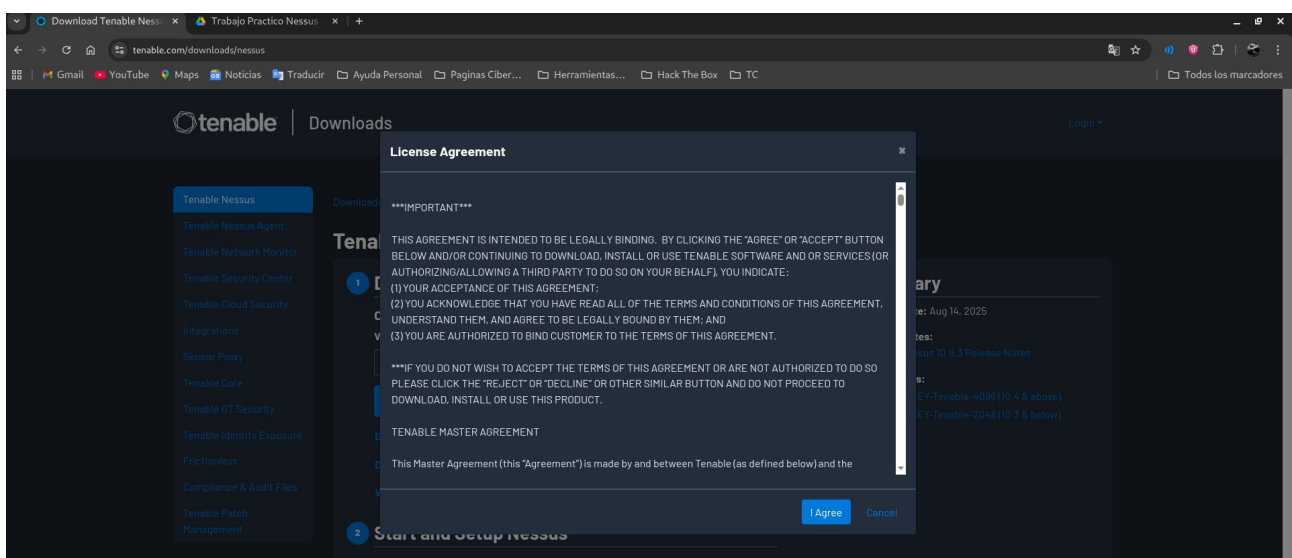
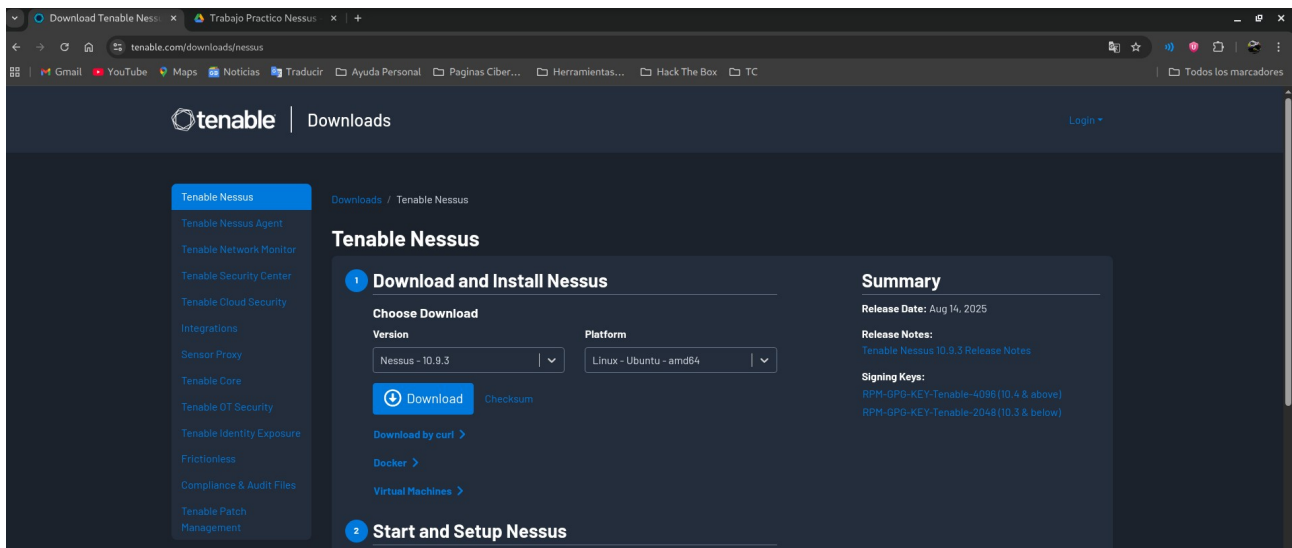
## **Trabajo practico Nessus**

- 1.....Instalacion de Nessus**
- 2.....Ejecucion de analisis de vulnerabilidades**
- 3.....Vulnerabilidades encontradas**
- 4.....Explicacion del alumno**

# 1.....Instalacion

En estas primeras capturas, es el 1er procedimiento de instalacion. Se pone en el buscador: **Nessus Download** y pinchamos en download. Paso siguiente, nos metemos **Tenable Nessus**. Y nos dirige a **Download and Install Nessus**. Nos detecta el sistema operativo y procedemos a bajarlo. Y en el apartado de Licencia pulsamos en **I Agree**.





Seguimos.....

Vamos a descargar y con **ls** localizamos el archivo para instalar.

Ponemos **sudo dpkg -i** y al lado ponemos el archivos de Nessus.

Se pone **N** y con el tabulador aparace todo el archivo completo. Le damos a enter y se procede a la instalacion. En una de las capturas se ve en blanco lo siguiente: **sudo systemctl start nessusd** y y para comprobar que este activo se pone **sudo systemctl status nessusd**.

```
kali@kali: ~/Descargas
Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ cd Descargas
(kali@kali)-[~/Descargas]
$ ls
Nessus-10.9.3-ubuntu1604_amd64.deb
(kali@kali)-[~/Descargas]
$
```

```
kali@kali: ~/Descargas
Archivo Acciones Editar Vista Ayuda
(kali@kali)-[~]
$ cd Descargas
(kali@kali)-[~/Descargas]
$ ls
Nessus-10.9.3-ubuntu1604_amd64.deb
(kali@kali)-[~/Descargas]
$ sudo dpkg -i Nessus-10.9.3-ubuntu1604_amd64.deb
```

```
kali@kali: ~/Descargas
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://NESSUS_HOSTNAME_OR_IP:8834/ to configure your scanner
```

```
Archivo Acciones Editar Vista Ayuda
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://NESSUS_HOSTNAME_OR_IP:8834/ to configure your scanner

(kali㉿kali)-[~/Descargas]
$

(kali㉿kali)-[~/Descargas]
$ /bin/systemctl start nessusd.service

(kali㉿kali)-[~/Descargas]
$ sudo systemctl status nessusd
```

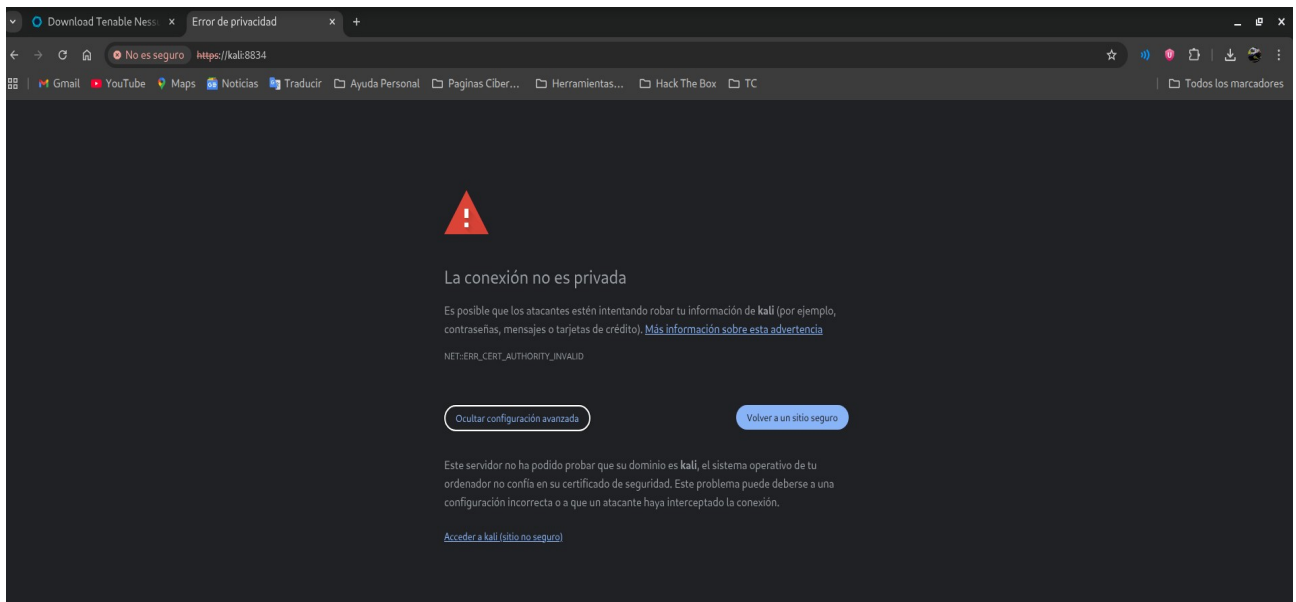
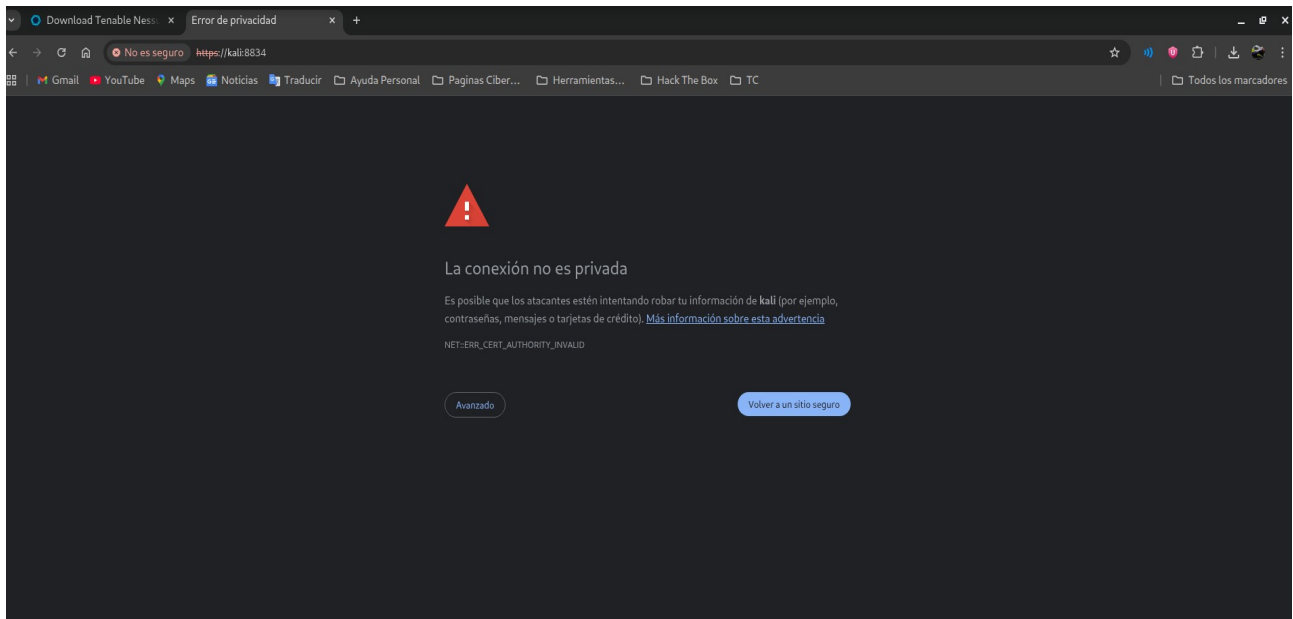
```
Archivo Acciones Editar Vista Ayuda
(kali㉿kali)-[~/Descargas]
$ /bin/systemctl start nessusd.service

(kali㉿kali)-[~/Descargas]
$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Wed 2025-08-27 15:58:08 CEST; 1min 6s ago
 Invocation: b7e8e9c7d4904761bda6088403ed87c0
    Main PID: 48572 (nessus-service)
      Tasks: 16 (limit: 9377)
     Memory: 168.1M (peak: 171.7M)
        CPU: 1min 695ms
    CGroup: /system.slice/nessusd.service
            └─48572 /opt/nessus/sbin/nessus-service -q
               └─48574 nessusd -q

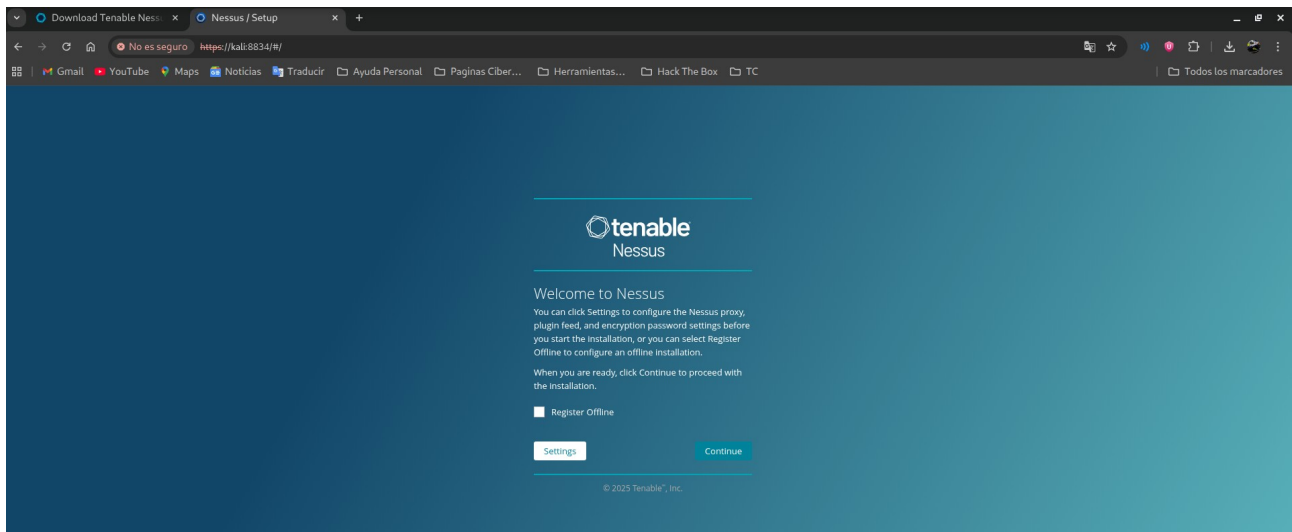
ago 27 15:58:08 kali systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner.
ago 27 15:58:08 kali nessus-service[48572]: nessus-service [48572][INFO] : Nessus 19.13.3 [build 20023] Started
```

Para abrir e inicia Nessus se pone en el buscador **https://kali8834**

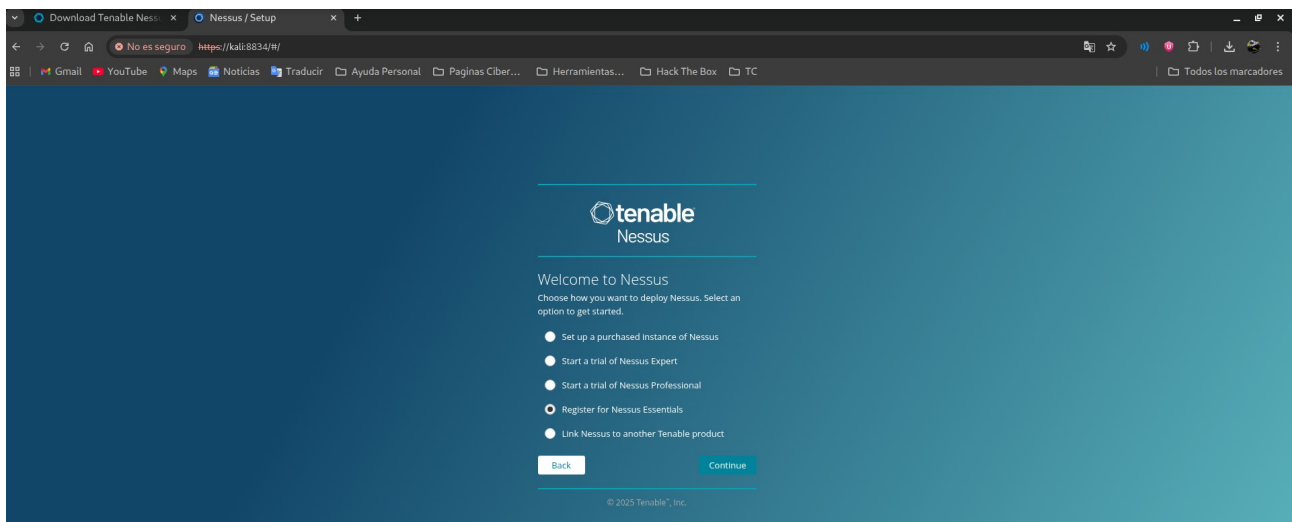
Nos pondra una advertencia, pero avanzamos y entramos en la pagina.



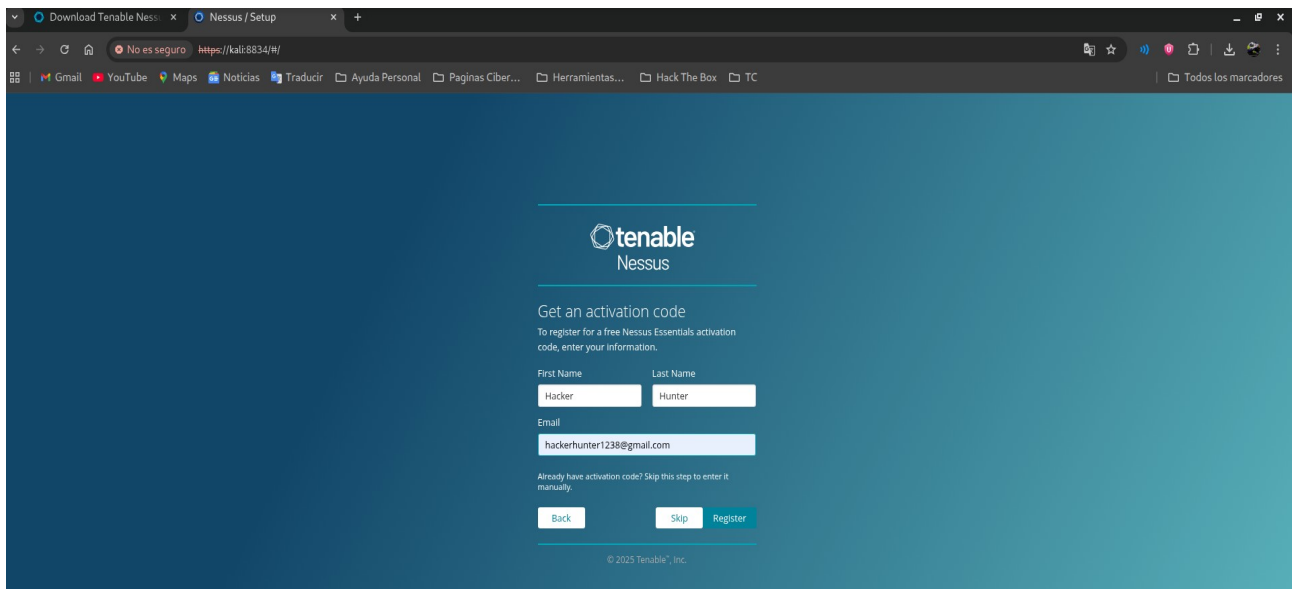
Pulsamos en continuar.....



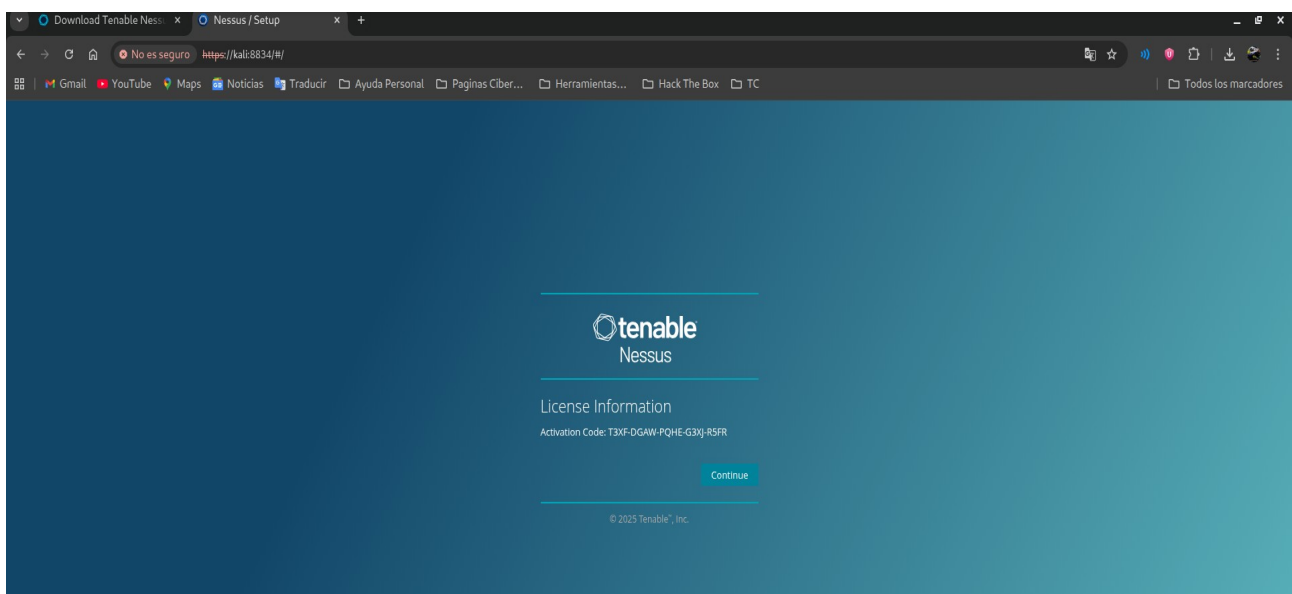
Marcamos la opcion **Register Nessus Essentials**.



Llenamos los casilleros con Nombre y Apellido (puede ser cualquiera) y ponemos un correo electronico.

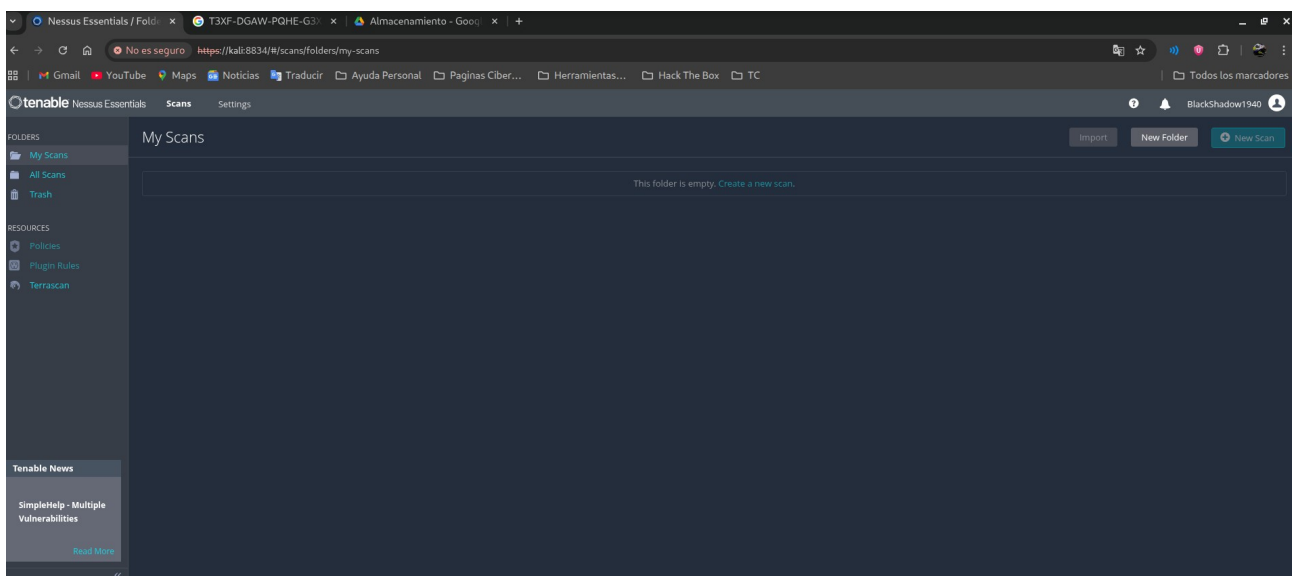
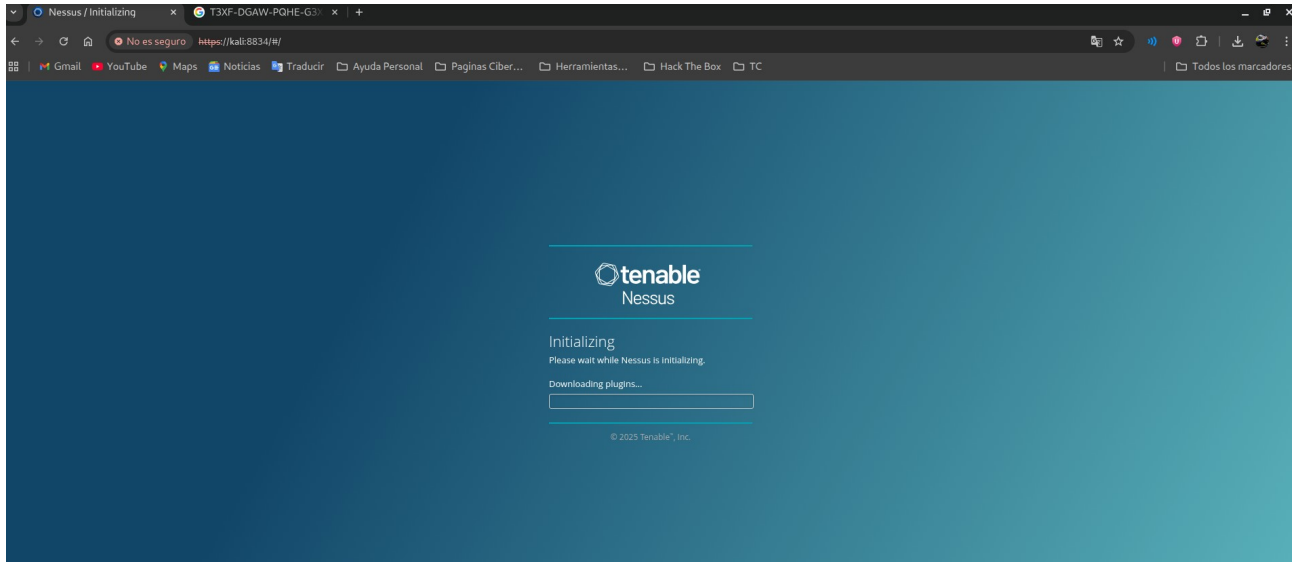


Aca veremos la informacion de licencia y el numero.

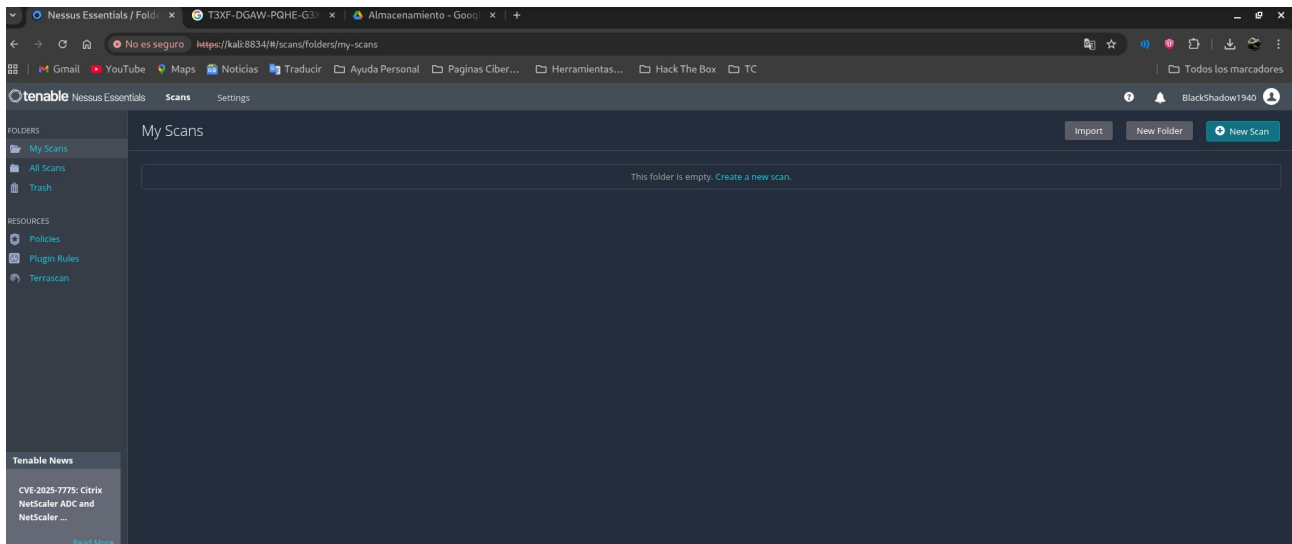




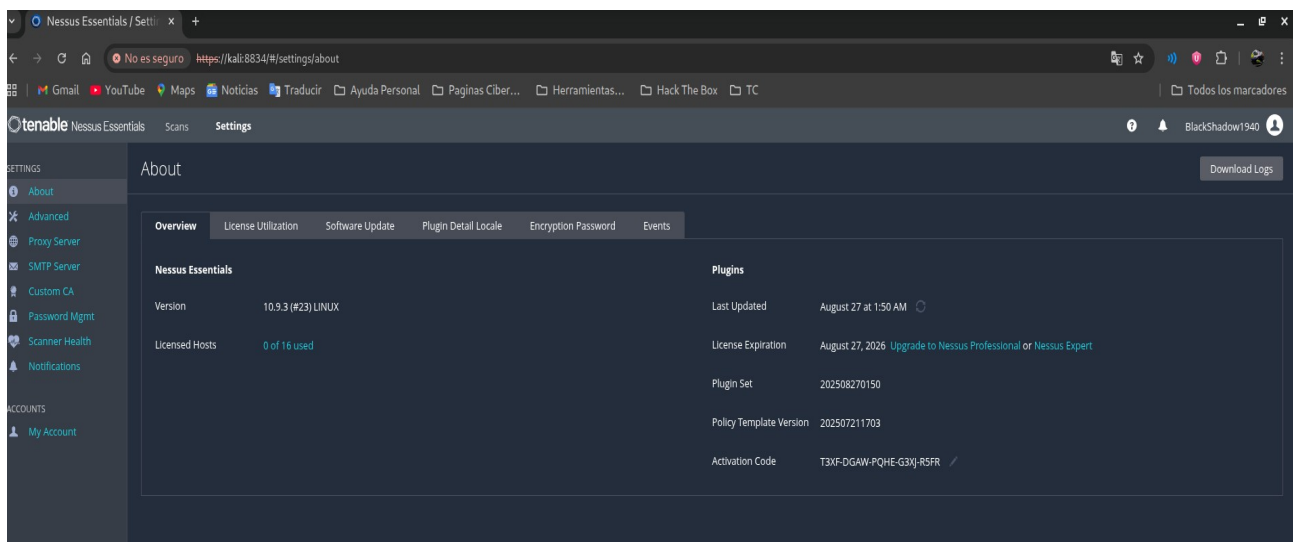
Se empiezan a cargar los plugins.



Al terminar aparecera en el tablero en activo la opcion **New Scan** y **Create New Scan**.



En el panel podemos ver.....  
Informacion del sistema.....  
Actualizacion.....  
Cambiar la clave.....  
Licencia del producto.....



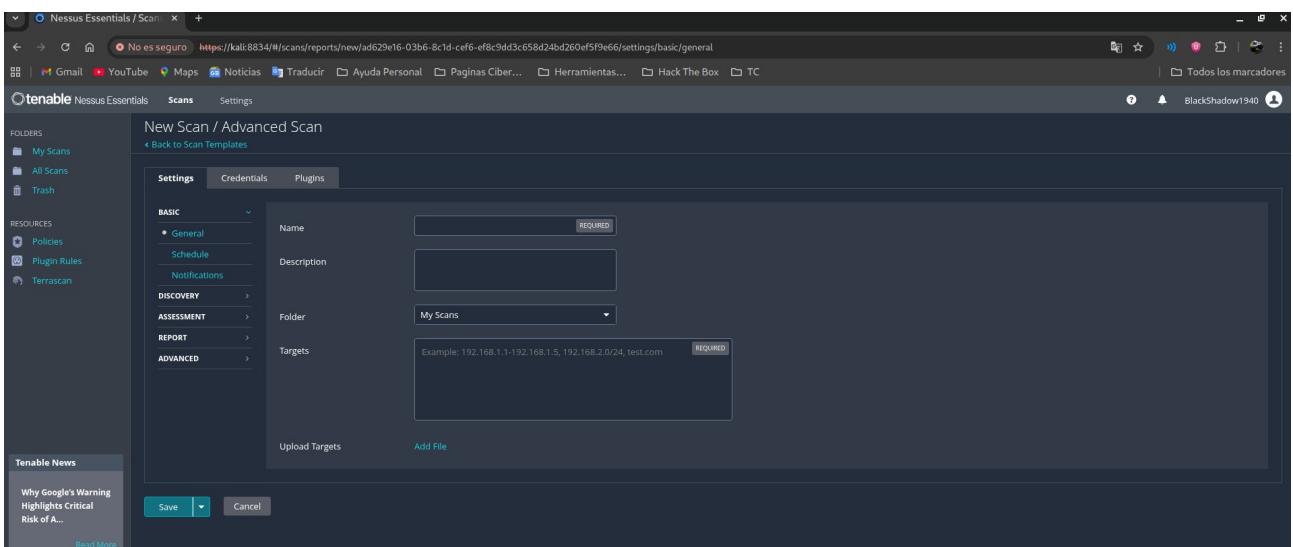
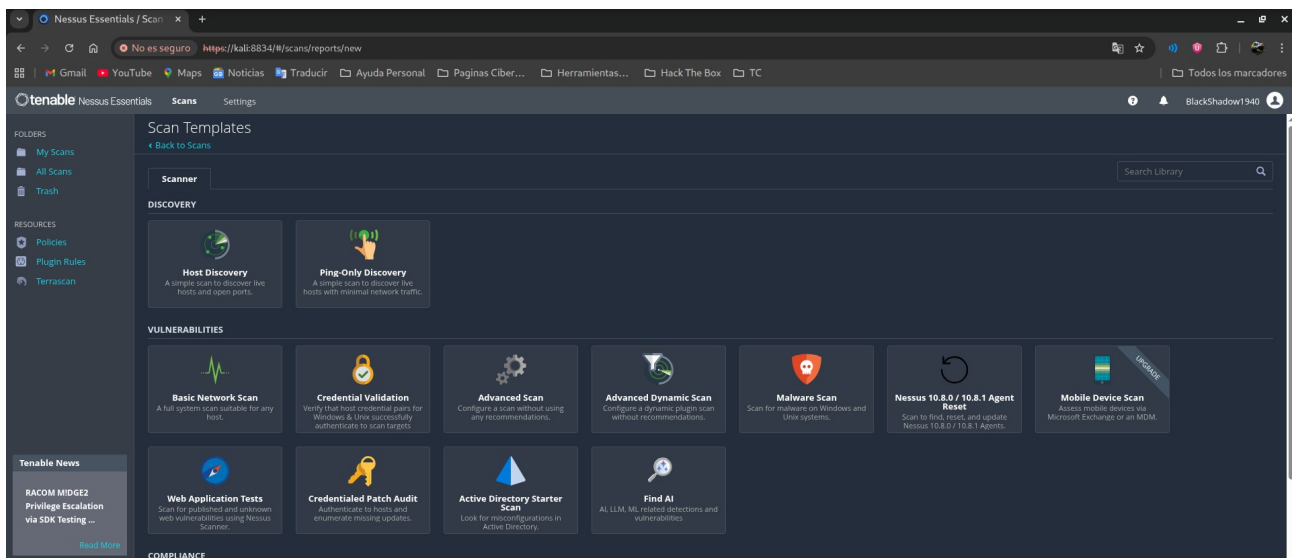
## 2.....Ejecucion de analisis de vulnerabilidades

Hay que pulsar la opcion **Create New Scan**.

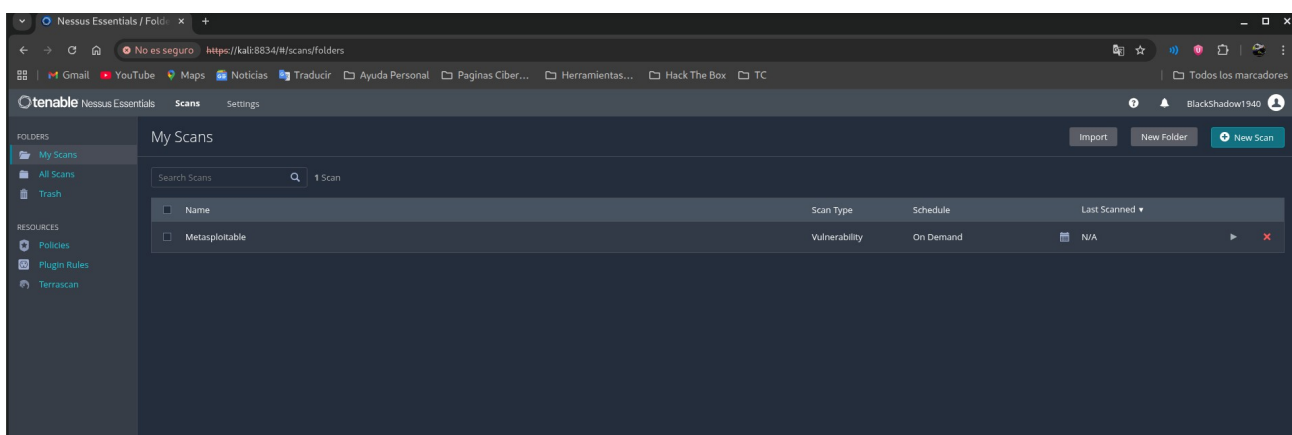
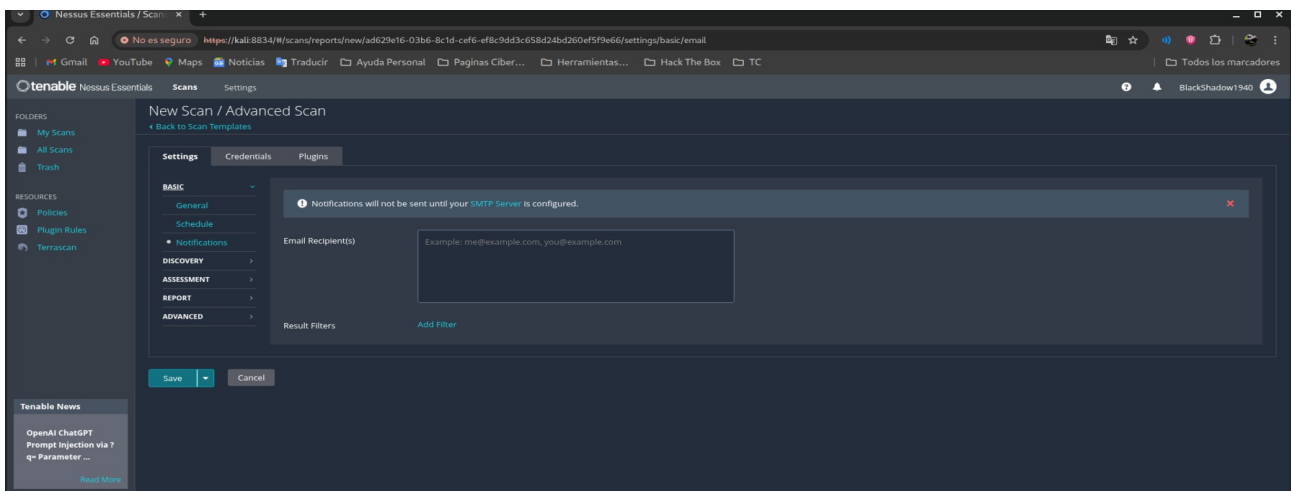
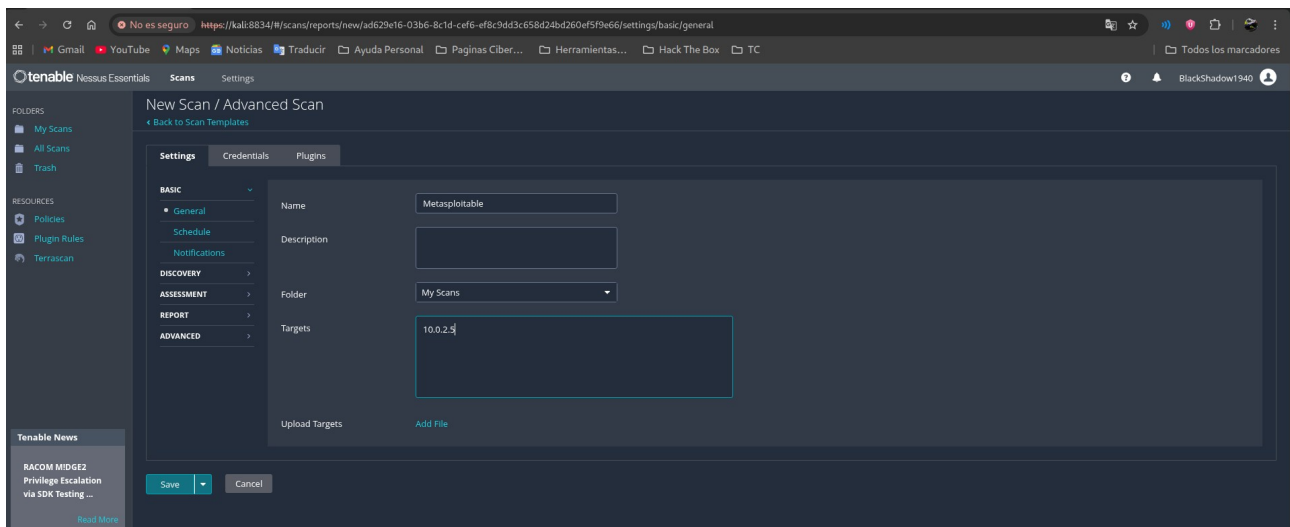
En Settings, pulsamos en **Advanced Scan**.

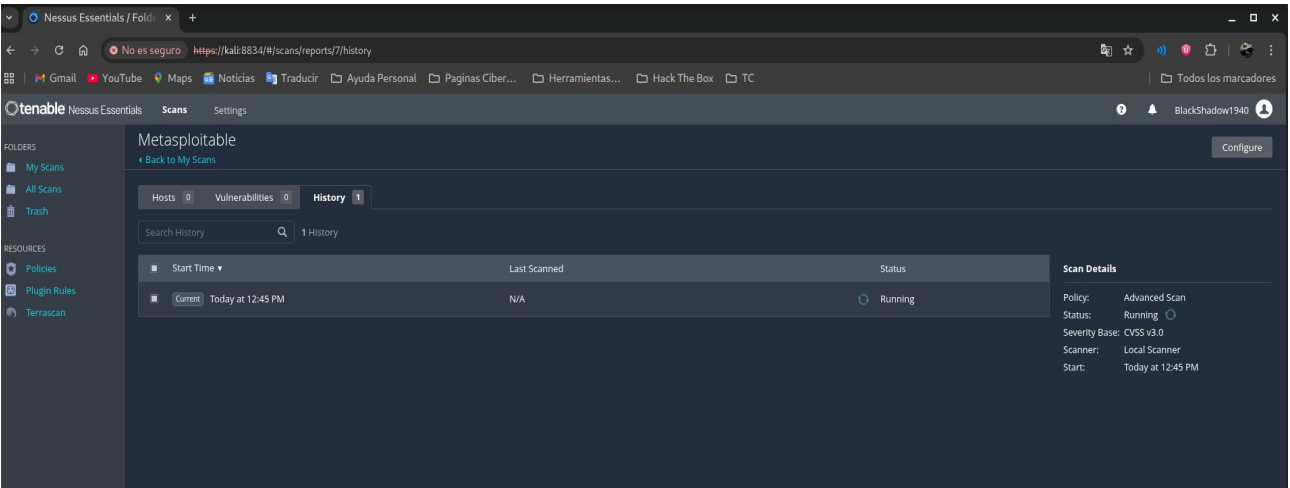
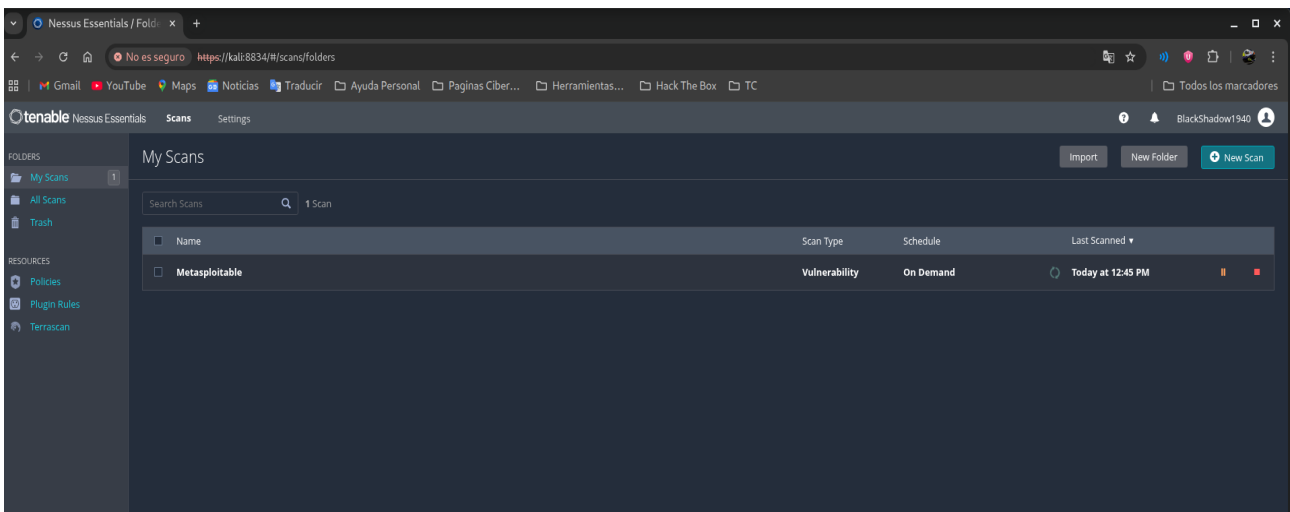
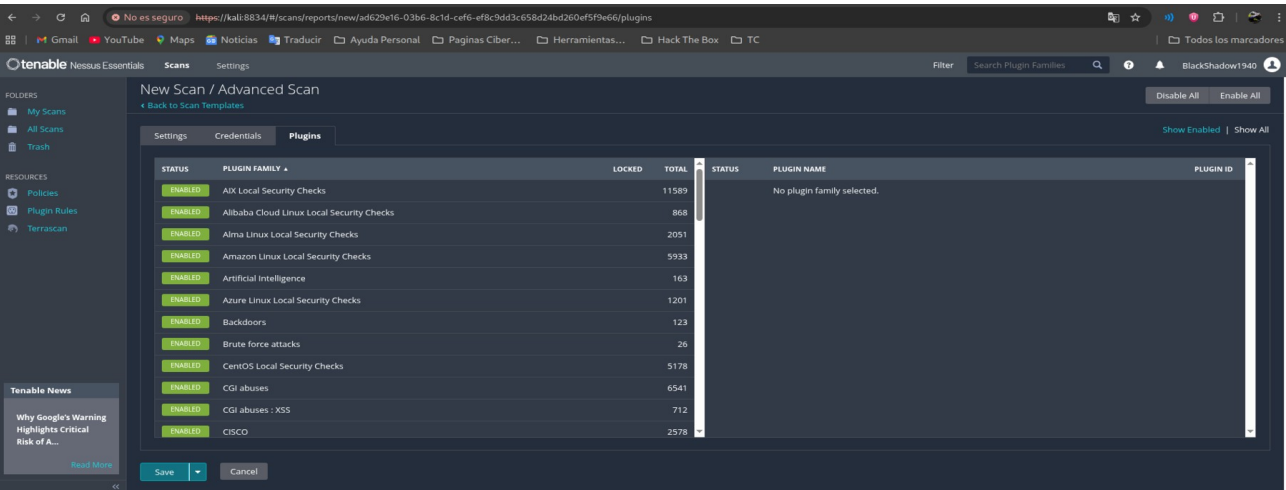
Ponemos el nombre del proyecto y la direccion IP que queremos hacer el analisis.

En capturas posteriores, se puede apreciar, que en el panel, hay opciones, poner dia y hora que queremos programar un analisis. Los Plugins. Y muchas otras cosas que vienen por defecto. Que al principio para conocer la herramienta, conviene no tocar.



Pulsamos salvar y luego arriba a la izquierda pulsamos **launch** para iniciar el analisis.





Nessus Essentials / Folders | Almacenamiento - Google | +

No es seguro https://kali:8834/#/scans/reports/7/history

Gmail YouTube Maps Noticias Traducir Ayuda Personal Paginas Ciber... Herramientas... Hack The Box TC Todos los marcadores

tenable Nessus Essentials Scans Settings

BlackShadow1940

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

How Exposure Management Has Helped Tenable Reduce ...

Read More

### Metasploitable

Back to My Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 4 History 1

Search History 1 History

Start Time	Last Scanned	Status
Current	Today at 12:45 PM	Today at 12:57 PM
Completed		

#### Scan Details

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 12:45 PM  
End: Today at 12:56 PM  
Elapsed: 12 minutes

#### Vulnerabilities

Critical  
High  
Medium  
Low  
Info

Nessus Essentials / Folders | Almacenamiento - Google | +

No es seguro https://kali:8834/#/scans/reports/7/hosts

Gmail YouTube Maps Noticias Traducir Ayuda Personal Paginas Ciber... Herramientas... Hack The Box TC Todos los marcadores

tenable Nessus Essentials Scans Settings

BlackShadow1940

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

SimpleHelp - Multiple Vulnerabilities

Read More

### Metasploitable

Back to My Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 4 History 1

Filter Search Hosts 1 Host

Host	Auth	Vulnerabilities
10.0.2.5	Fail	4

#### Scan Details

Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 12:45 PM  
End: Today at 12:56 PM  
Elapsed: 12 minutes

#### Vulnerabilities

Critical  
High  
Medium  
Low  
Info

Nessus Essentials / Folders | Almacenamiento - Google | +

No es seguro https://kali:8834/#/scans/reports/7/vulnerabilities

Gmail YouTube Maps Noticias Traducir Ayuda Personal Paginas Ciber... Herramientas... Hack The Box TC Todos los marcadores

tenable Nessus Essentials Scans Settings

BlackShadow1940

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules
- Terrascan

Tenable News

Gemini Search Personalization Model - Prompt Injec...

Read More

### Metasploitable

Back to My Scans

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 4 History 1

Filter Search Vulnerabilities 4 Vulnerabilities

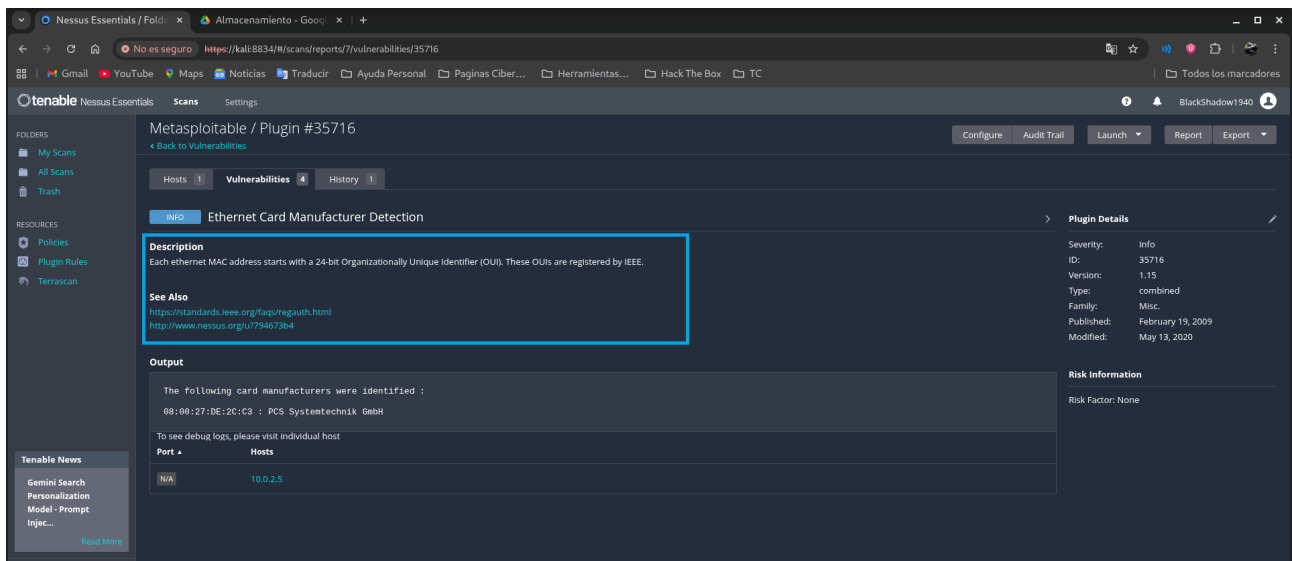
Ser	CVSS	WPR	EPSS	Name	Family	Count
INFO				Ethernet Card Manufacturer Detection	Misc.	1
INFO				Ethernet MAC Addresses	General	1
INFO				Nessus Scan Information	Settings	1
INFO				Traceroute Information	General	1

#### Scan Details

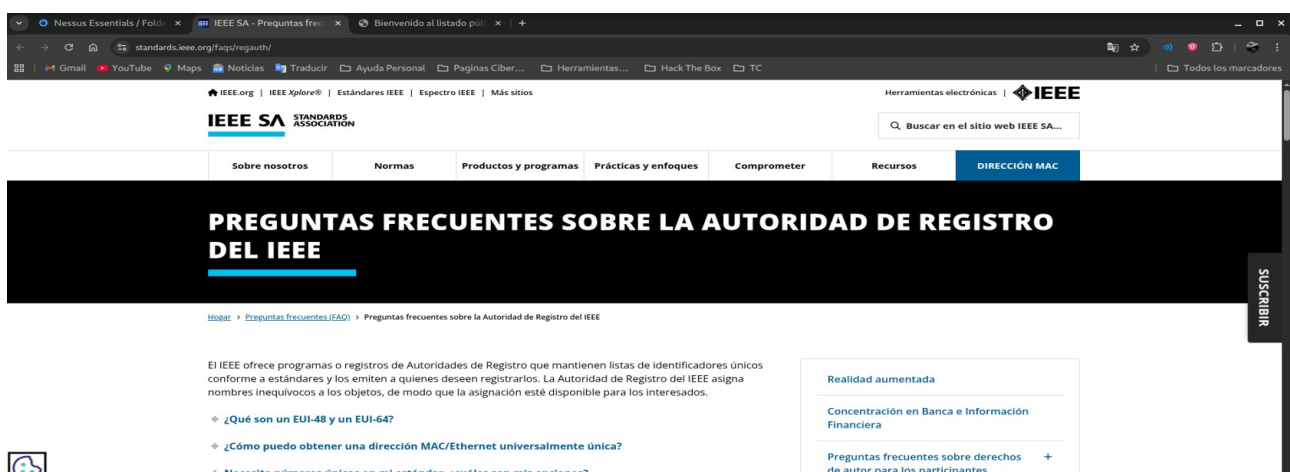
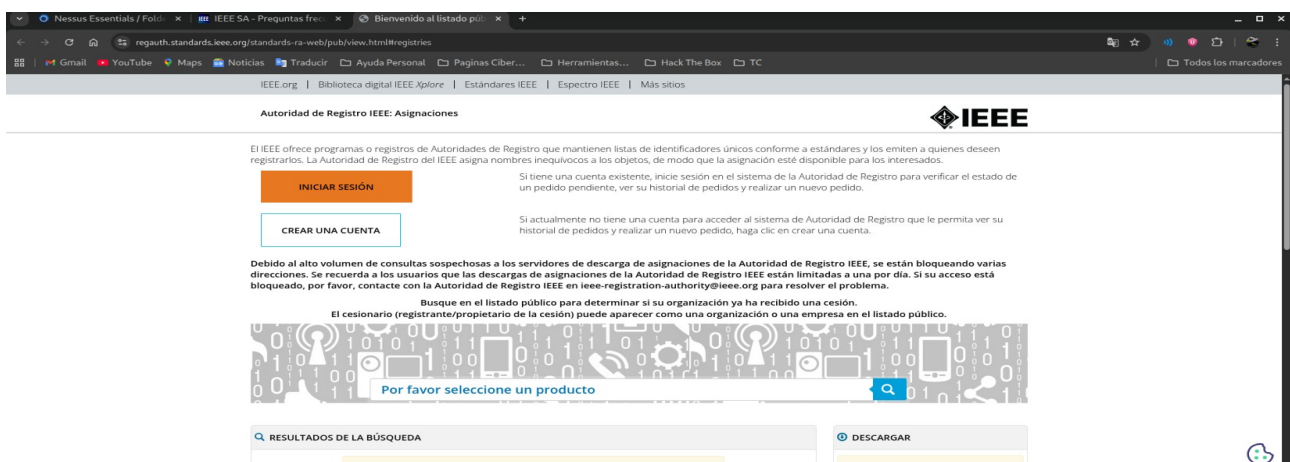
Policy: Advanced Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 12:45 PM  
End: Today at 12:56 PM  
Elapsed: 12 minutes

#### Vulnerabilities

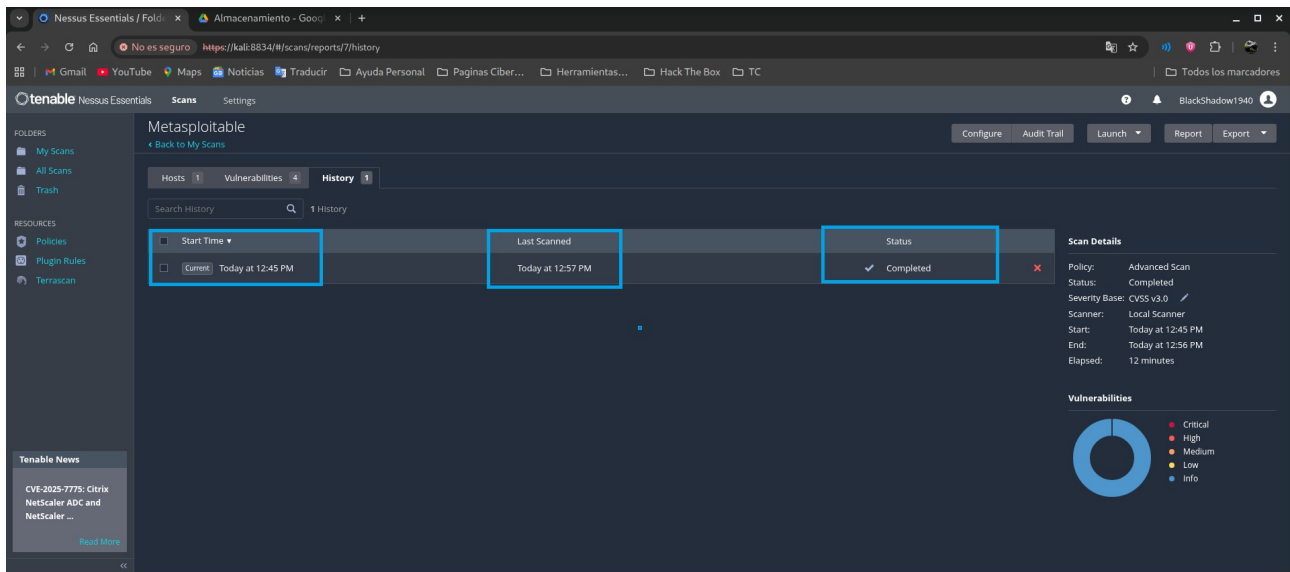
Critical  
High  
Medium  
Low  
Info



Aca esta finalizado el analisis. Se encontraron 4 vulnerabilidades. En la captura que tiene marcado un recuadro, nos informa la descripcion y abajo dos enlaces relaciones a post con informacion de la vulnerabilidad.



Aca estan los dos enlaces, ahi podremos encontrar informacion mas amplia, como comente antes.



Esta ultima captura nos muestra la hora del inicio y la finalizacion del analisis. Y el ultimo recuadro, que esta completa.

Esto esta hecho con la IP del Windows10 instalado en Virtual Box.

El siguiente va a ser con la IP de Windows11 en mi PC personal.

Vamos a explicar el circulo con colores ubicado abajo a la derecha.

Las azules aunque parescan de modo informativo. Hay mucho casos, que te indican cosas, que a simple vista no te das cuenta. Si profundizas cosas, podrian servir para hacer un pentesting, a traves de ese puerto.

Las rojas son criticas.

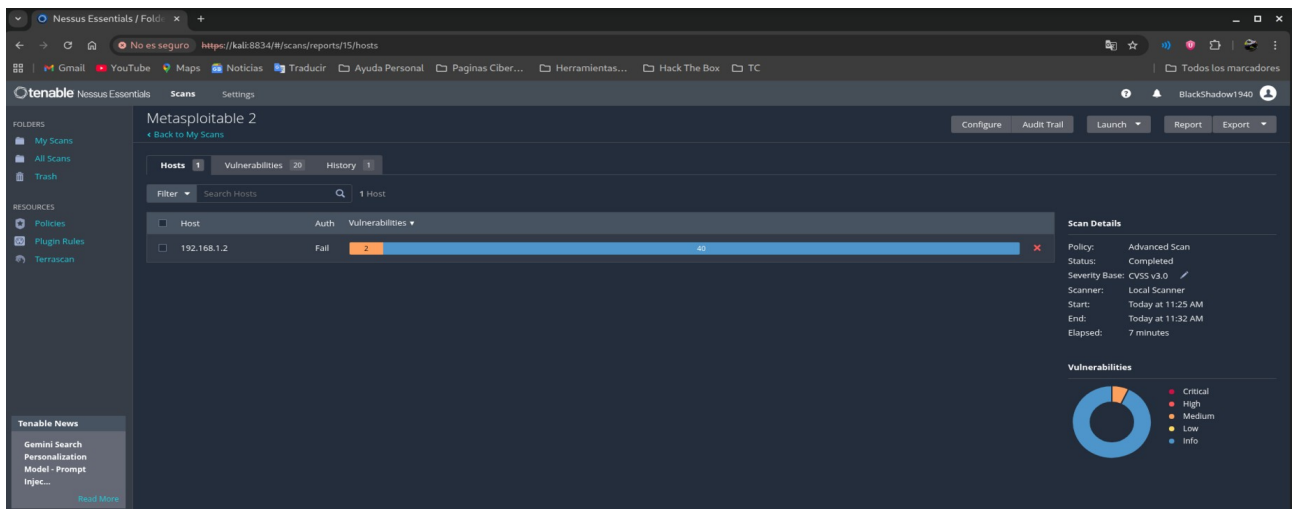
Las naranjas son altas.

Las amarillas bajas.

Entonces todas pueden ser una amenaza.



Vamos a ver los resultados de la IP de mi PC personal.



**Metasploitable 2**

Hosts: 1 | Vulnerabilities: 20 | History: 1

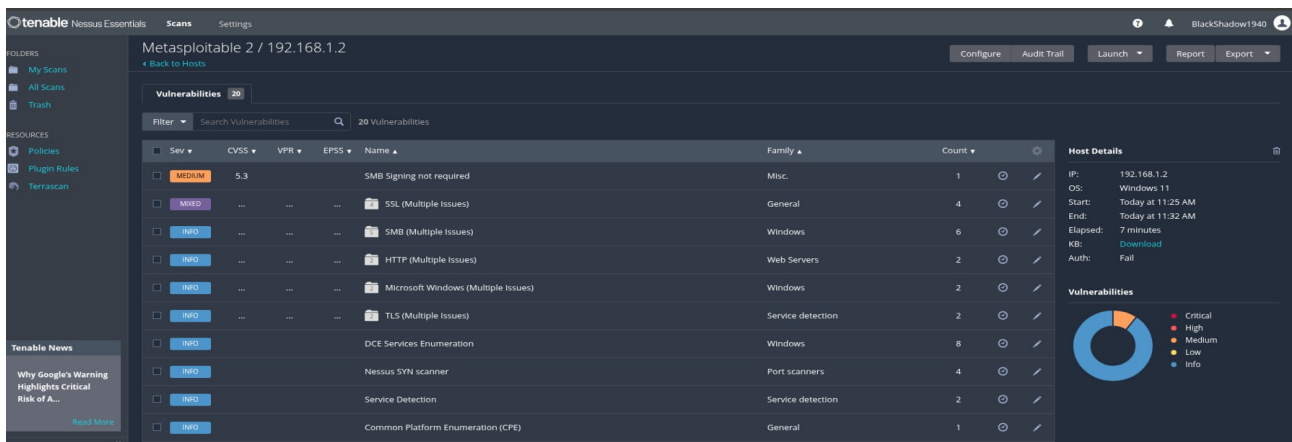
Host	Auth	Vulnerabilities
192.168.1.2	Fail	2

**Scan Details**

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 11:25 AM
- End: Today at 11:32 AM
- Elapsed: 7 minutes

**Vulnerabilities**

- 2 Critical
- 18 High
- 0 Medium
- 0 Low
- 0 Info



**Metasploitable 2 / 192.168.1.2**

Vulnerabilities: 20

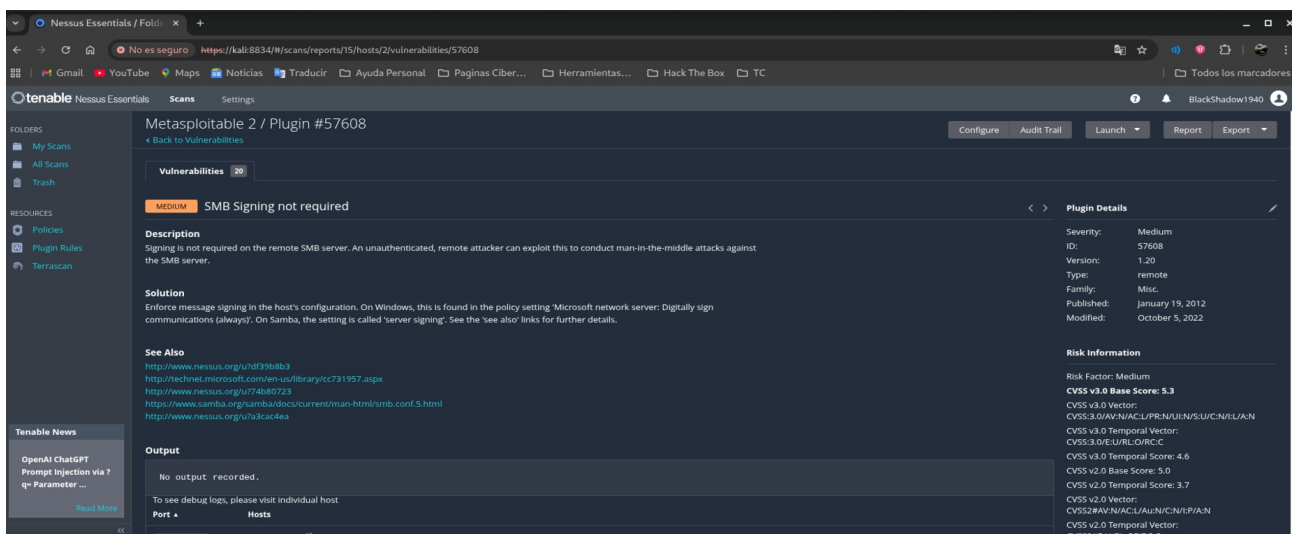
Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	1
MIXED				SSL (Multiple Issues)	General	4
INFO				SMB (Multiple Issues)	Windows	6
INFO				HTTP (Multiple Issues)	Web Servers	2
INFO				Microsoft Windows (Multiple Issues)	Windows	2
INFO				TLS (Multiple Issues)	Service detection	2
INFO				DCE Services Enumeration	Windows	8
INFO				Nessus SYN scanner	Port scanners	4
INFO				Service Detection	Service detection	2
INFO				Common Platform Enumeration (CPE)	General	1

**Host Details**

- IP: 192.168.1.2
- OS: Windows 11
- Start: Today at 11:25 AM
- End: Today at 11:32 AM
- Elapsed: 7 minutes
- KB: Download
- Auth: Fail

**Vulnerabilities**

- 2 Critical
- 18 High
- 0 Medium
- 0 Low
- 0 Info



**Metasploitable 2 / Plugin #57608**

Vulnerabilities: 20

**SMB Signing not required**

**Description**

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**

- <https://www.nessus.org/u/df39b8b3>
- <https://technet.microsoft.com/en-us/library/cc731957.aspx>
- <https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
- <https://www.nessus.org/u/a3cacdaa>

**Output**

No output recorded.

To see debug logs, please visit individual host

Port: Hosts

**Plugin Details**

- Severity: Medium
- ID: 57608
- Version: 1.20
- Type: remote
- Family: Misc
- Published: January 19, 2012
- Modified: October 5, 2022

**Risk Information**

- Risk Factor: Medium
- CVSS v3.0 Base Score: 5.3
- CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:LC/C:N/L:N/A:N
- CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
- CVSS v3.0 Temporal Score: 4.6
- CVSS v2.0 Base Score: 5.0
- CVSS v2.0 Temporal Score: 3.7
- CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/N:P/A:N
- CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:O/RC:C

Aca vemos que hay 20 vulnerabilidades. En las cuales dos son naranja. Que son tambien consideradas criticas. Las naranjas mas clara. Son de clase media.