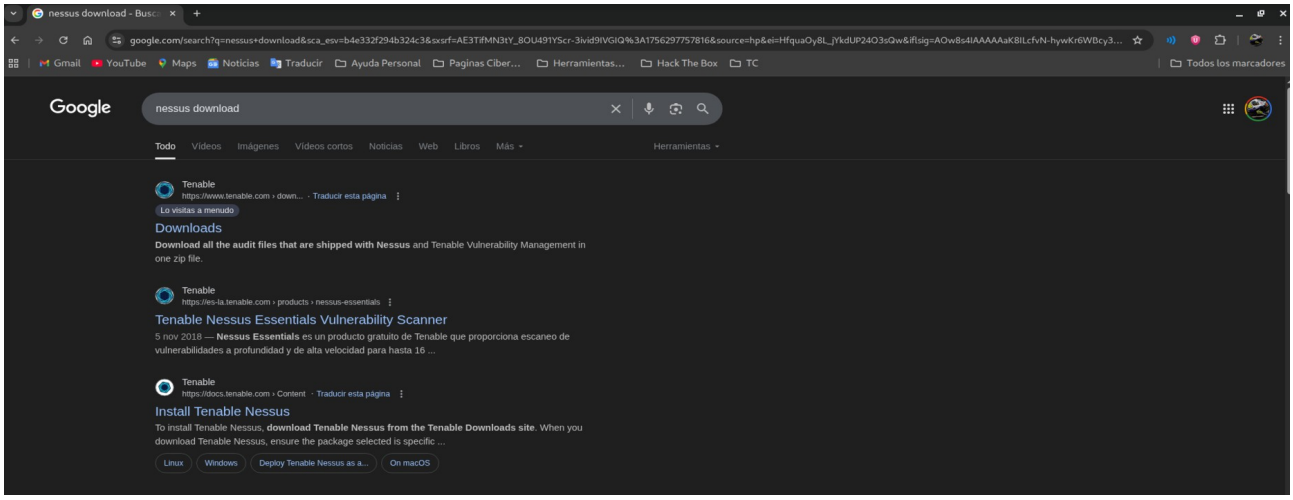
Martin Dalla Pozza

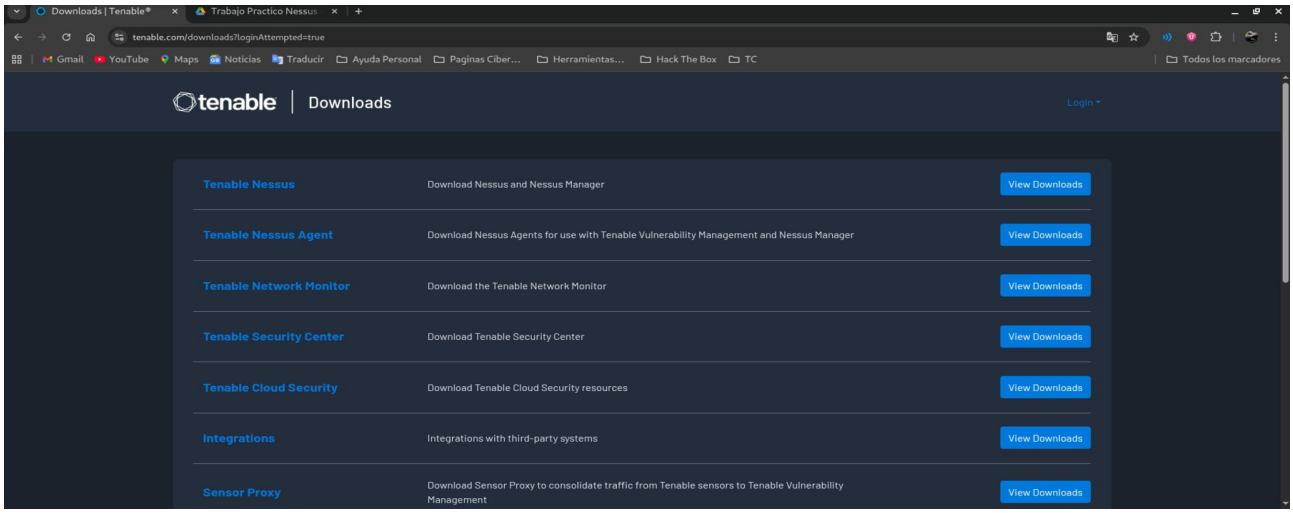
Trabajo practico Nessus

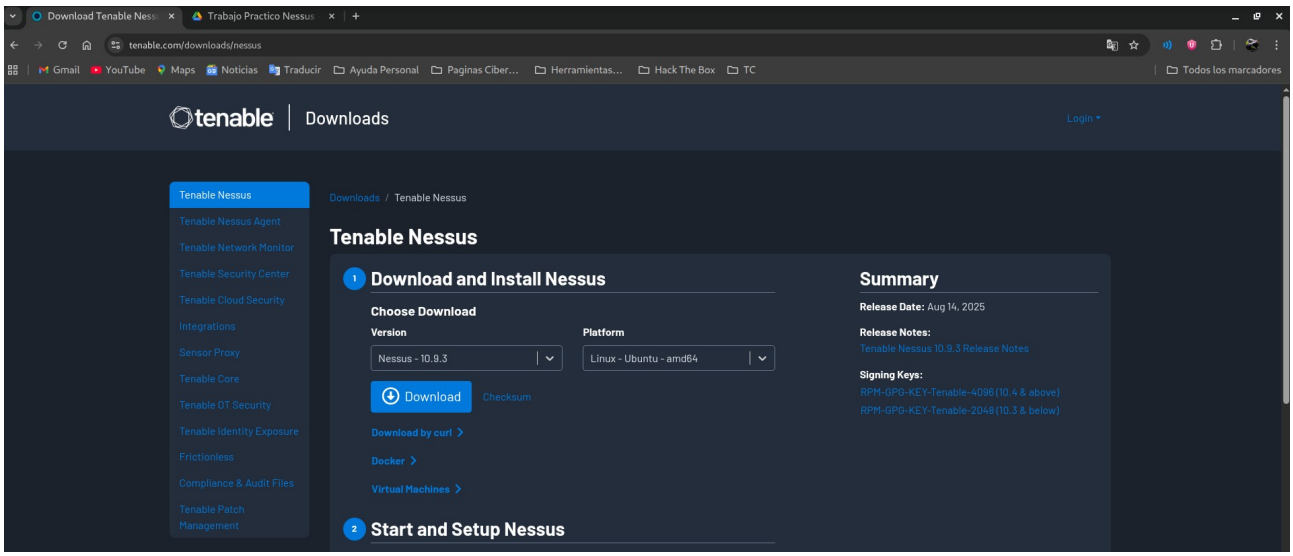
1…..Instalacion de Nessus
2…..Ejecucion de analisis de vulnerabilidades
3…..Vulnerabilidades encontradas
4…..Explicacion del alumno

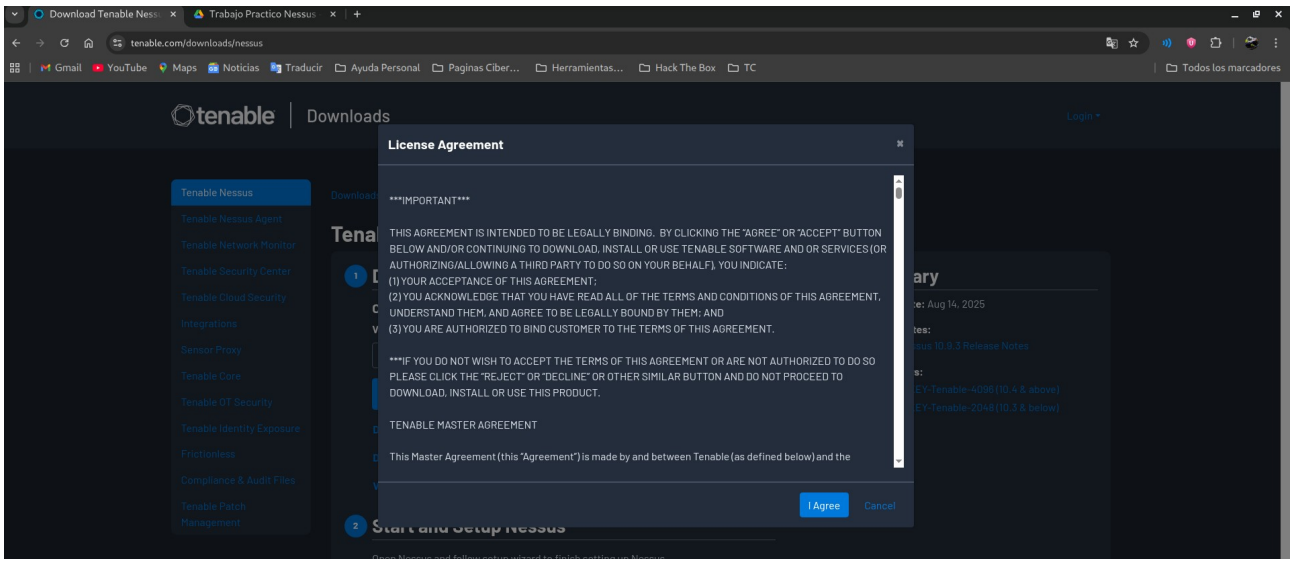
1…..Instalacion

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**.





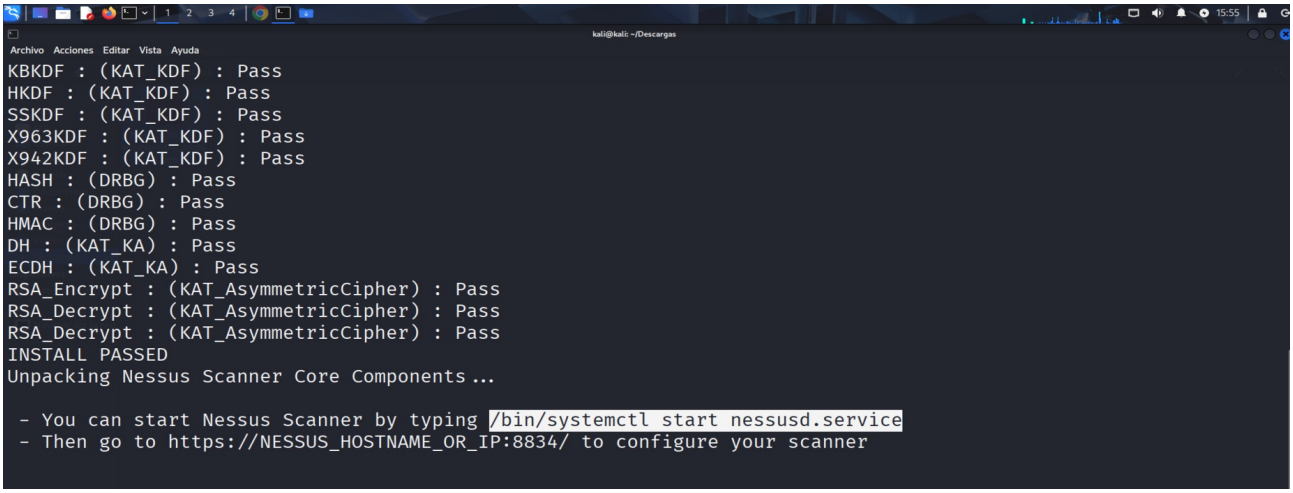


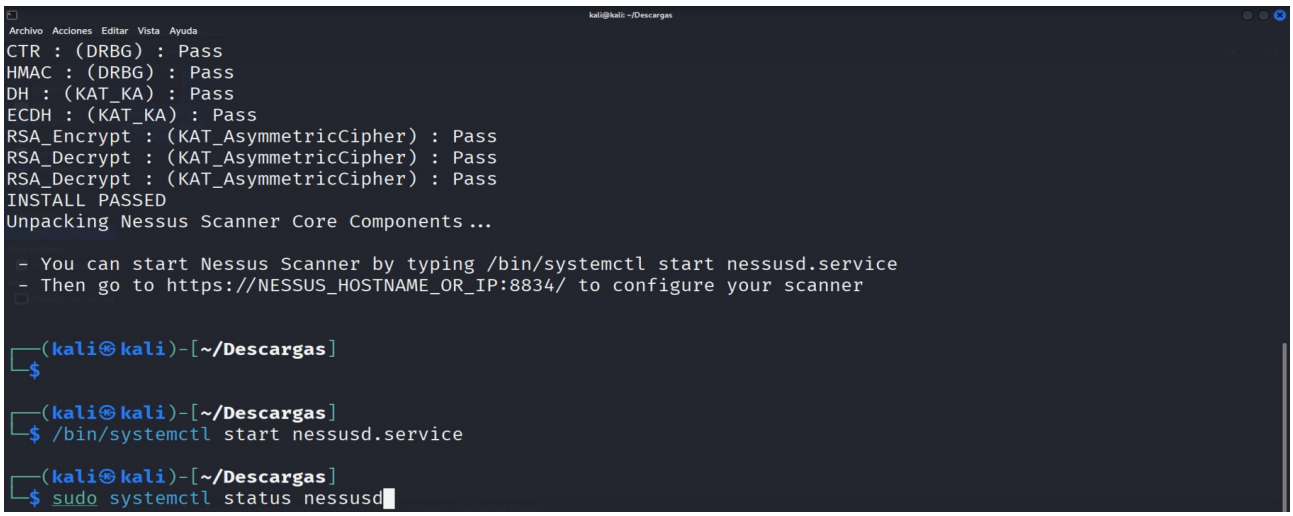


Seguimos……
Vamos a descargas y con **ls** localizamos el archivo para instalar.
Ponemos **sudo dpkg -i** y al lado ponemos el archivos de Nessus.
Se pone N y con el tabulador aparace todo el archivo completo. Le damos a enter y se procede a la instalacion. En una de las capturas se ve en blanco lo siguiente: **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]
$

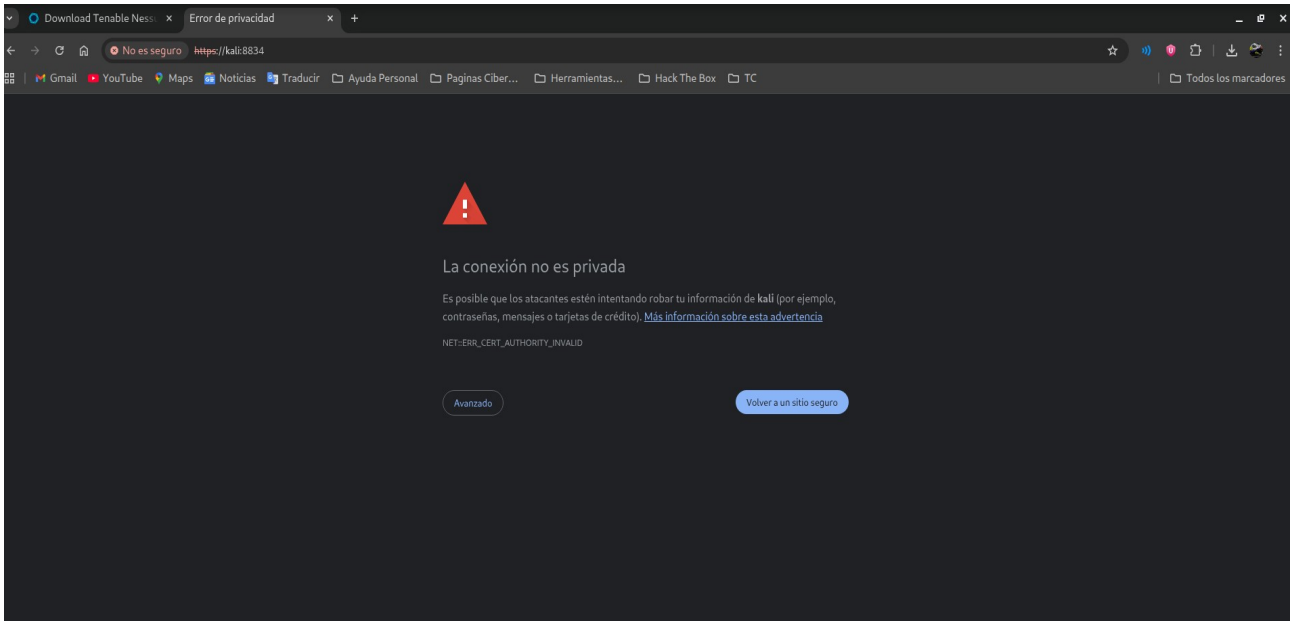

kali@kali: ~/Descargas
Archivo Acciones Editar Vista Ayuda
(kali㉿kali)-[~]
$ cd Descargas
(kali㉿kali)-[~/Descargas]
$ ls
Nessus-10.9.3-ubuntu1604_amd64.deb
(kali㉿kali)-[~/Descargas]
$ sudo dpkg -i Nessus-10.9.3-ubuntu1604_amd64.deb

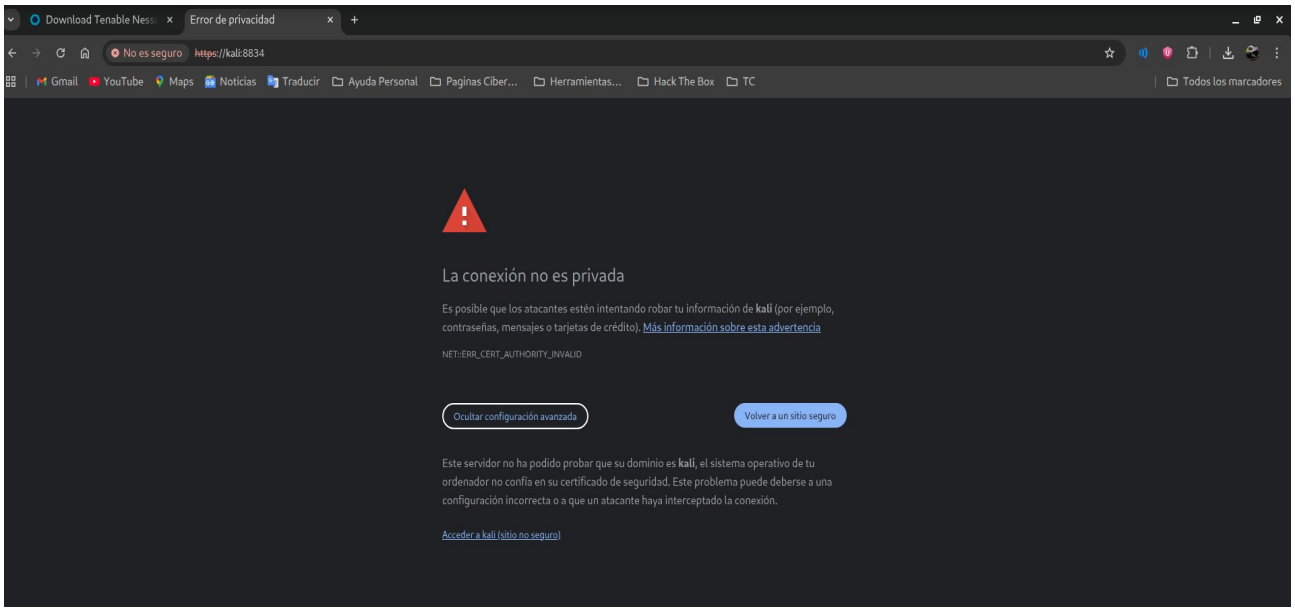

kali@kali: ~/Descargas
Archivo Acciones Editar Vista Ayuda
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (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



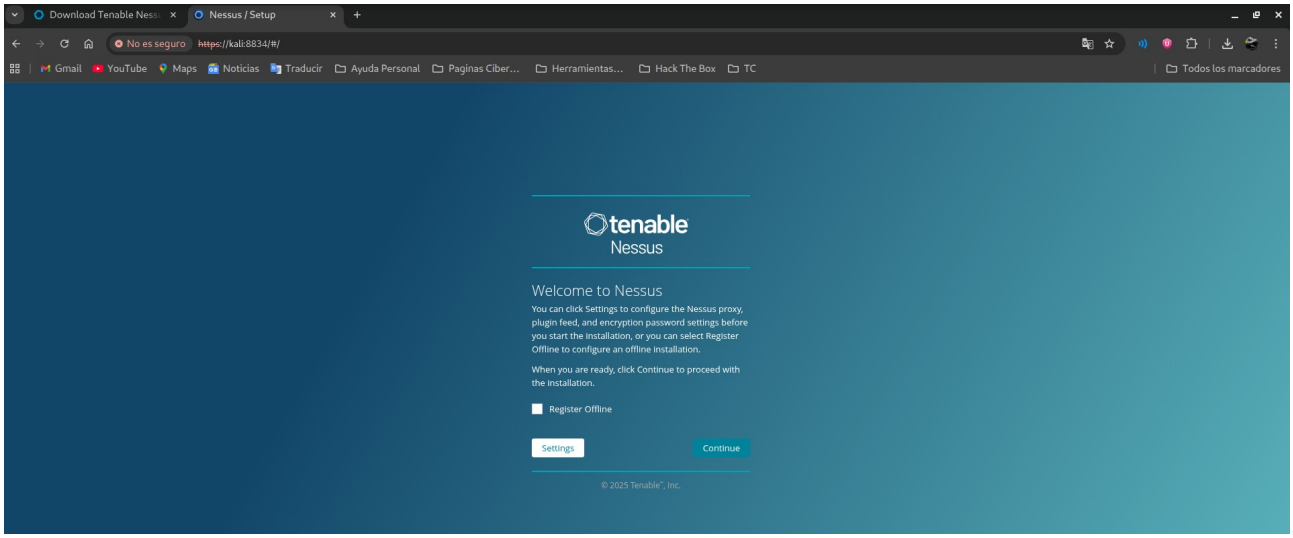
Para abrir e inicua Nessus se pone en el buscador **https//:kali8834**

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

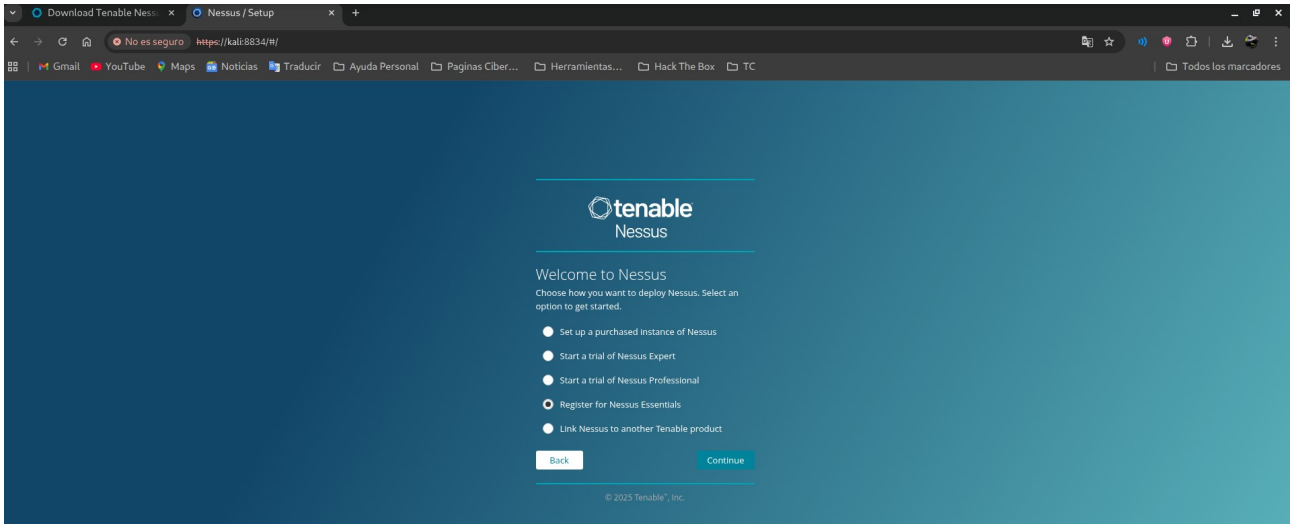




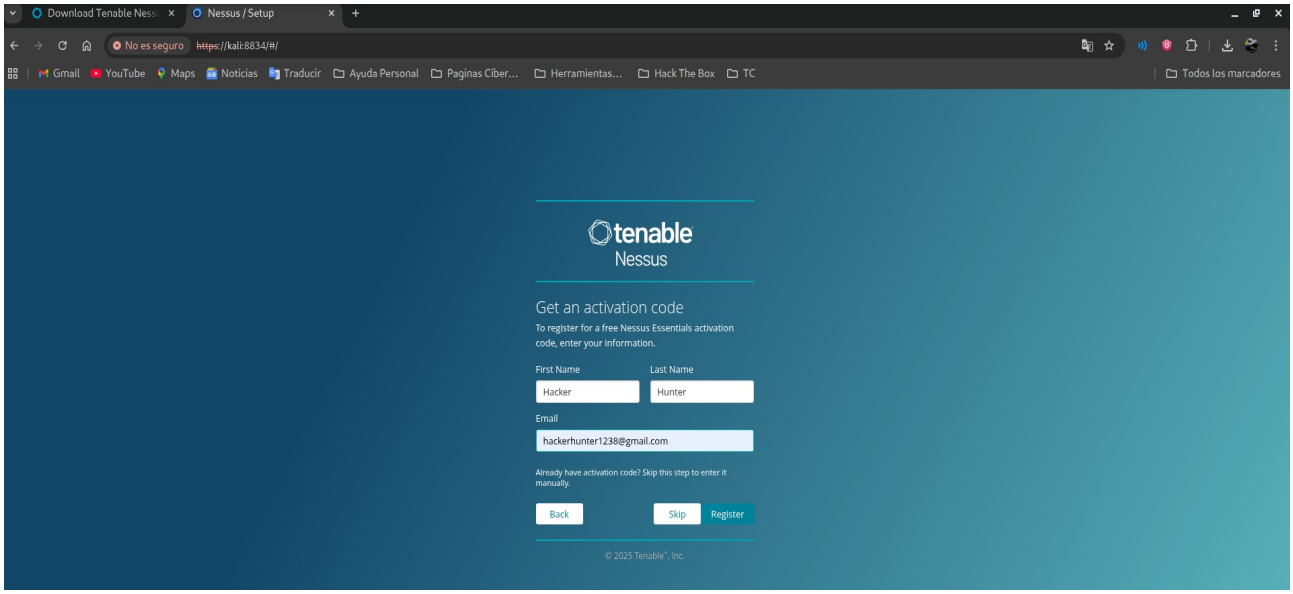
Pulsamos en continuar…..



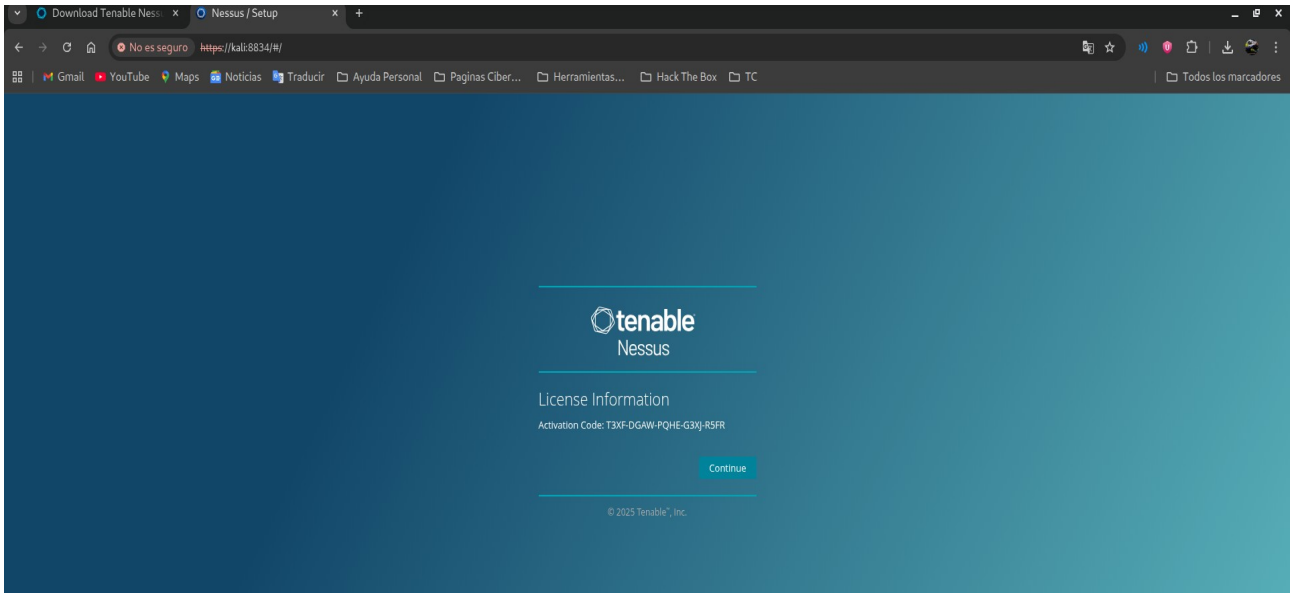
Marcamos la opcion **Register Nessus Essentials.**



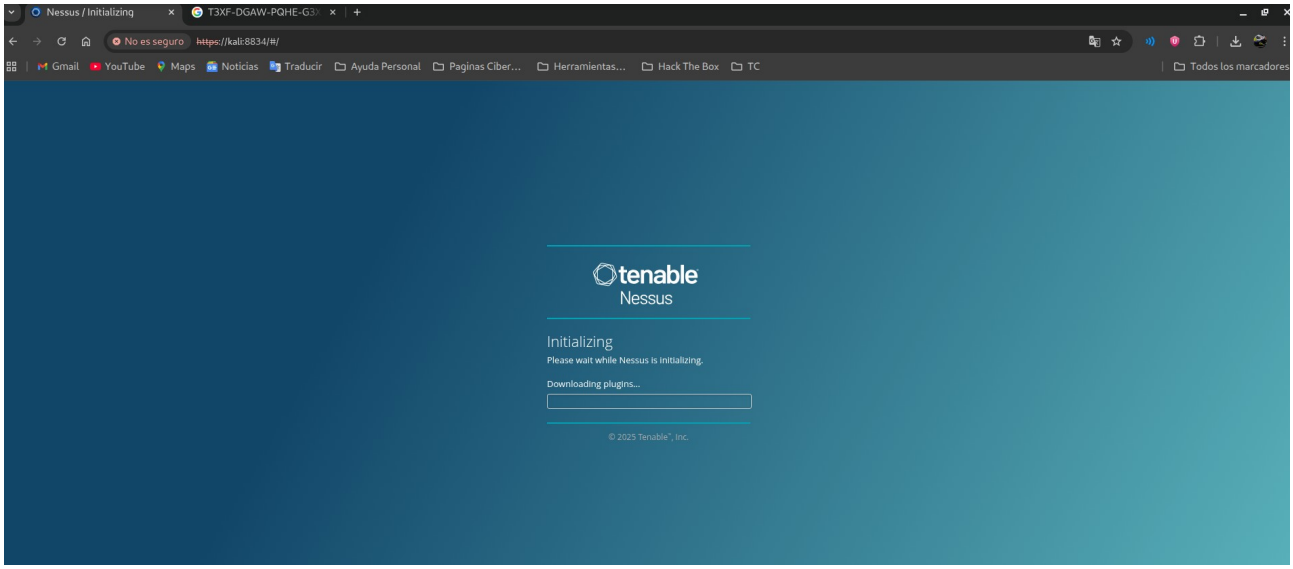
Llenamos los casilleros con Nombre y Apellido (puede ser cualquiera) y ponemos un correo electronico.

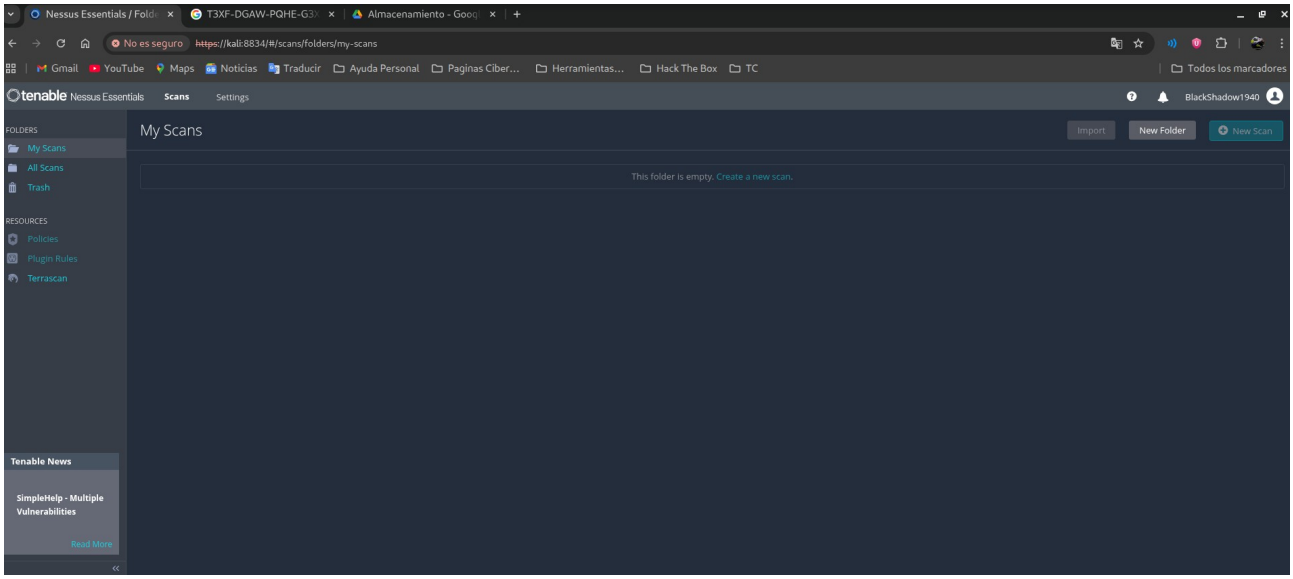


Aca veremos la informacion de licencia y el numero.

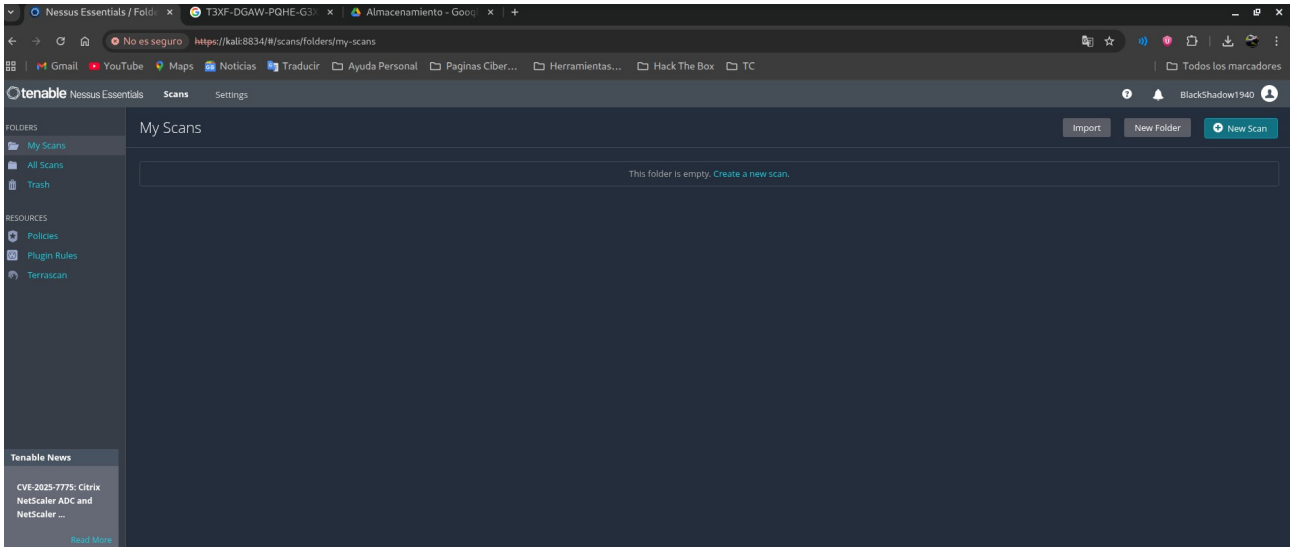


Se empiezan a cargar los plugins.

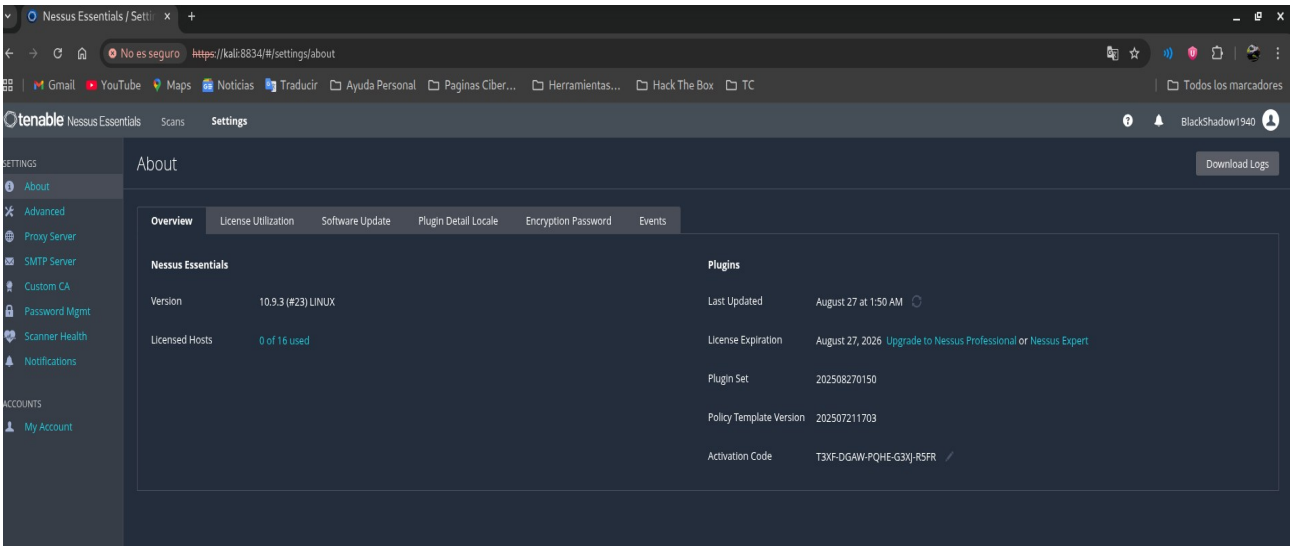




Al terminar aparecera en el tablero en activo la opcion **New Scan** y **Create New Scan**.

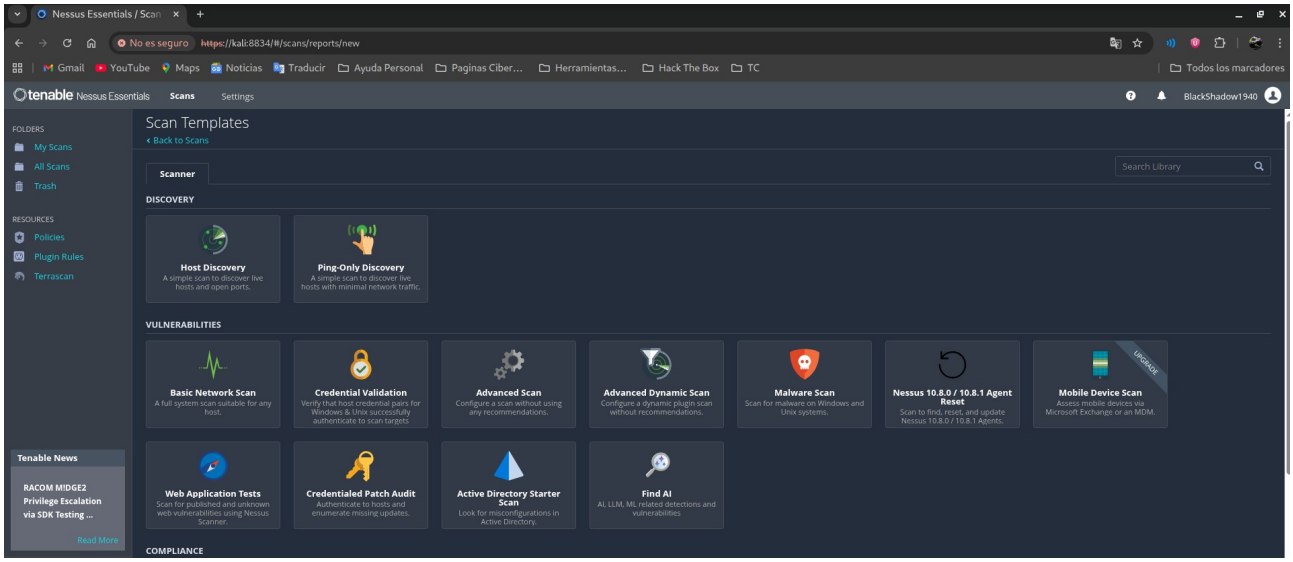


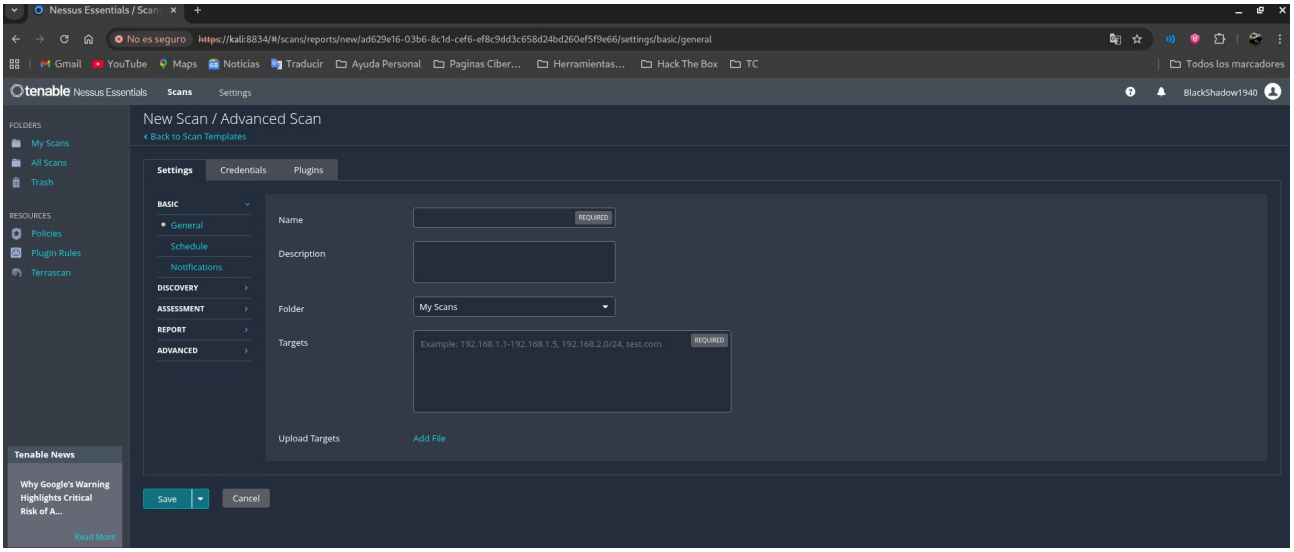
En el panel podemos ver……
Informacion del sistema…..
Actualizacion…..
Cambiar la clave…..
Licencia del producto…..



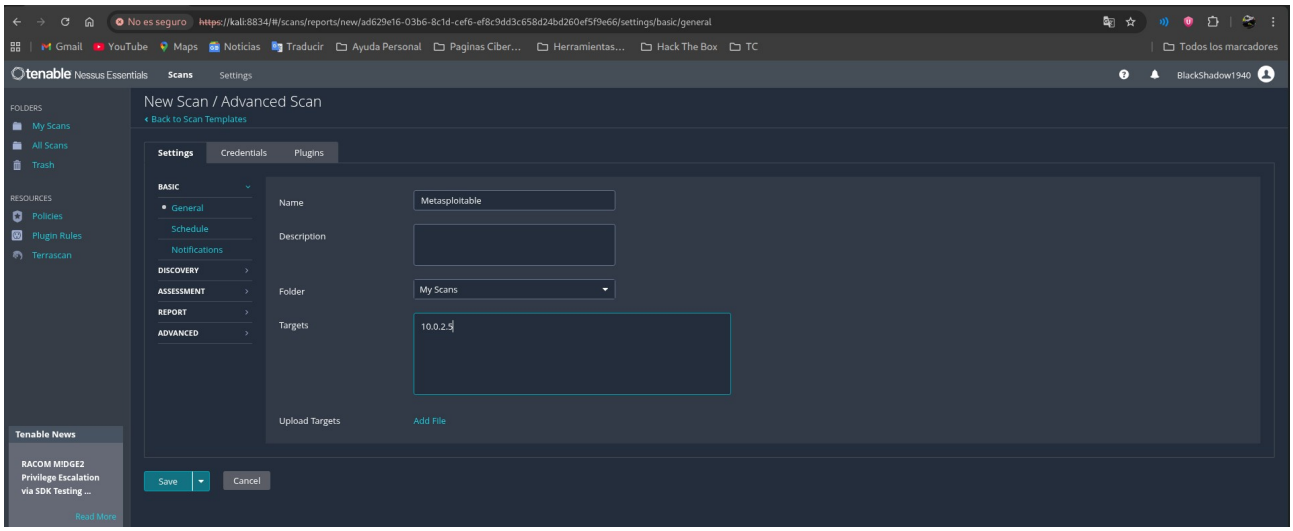
2…….Ejecucion de analisis de vulnerabilidades

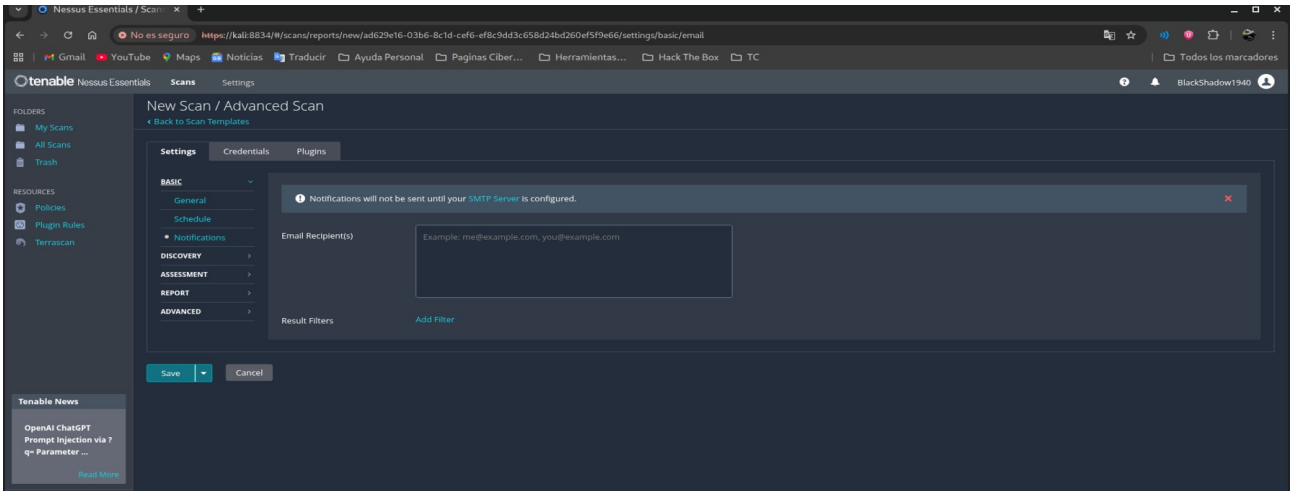
Hay que pulsar la opcion **Create New Scan.**
En Settings, pulsamos en **Advanced Scan.**
Ponemos el nonbre del proyecto y la direccion IP que queremos hacer el analisis.
En capturas posteriores, se puede apreciar, que en el panel, hay opciones, poner dia y hora que queremos programas un analisis. Los Plugins. Y muchas otras cosas que vienen por defecto. Que al principio para conocer la herramienta, conviene no tocar.

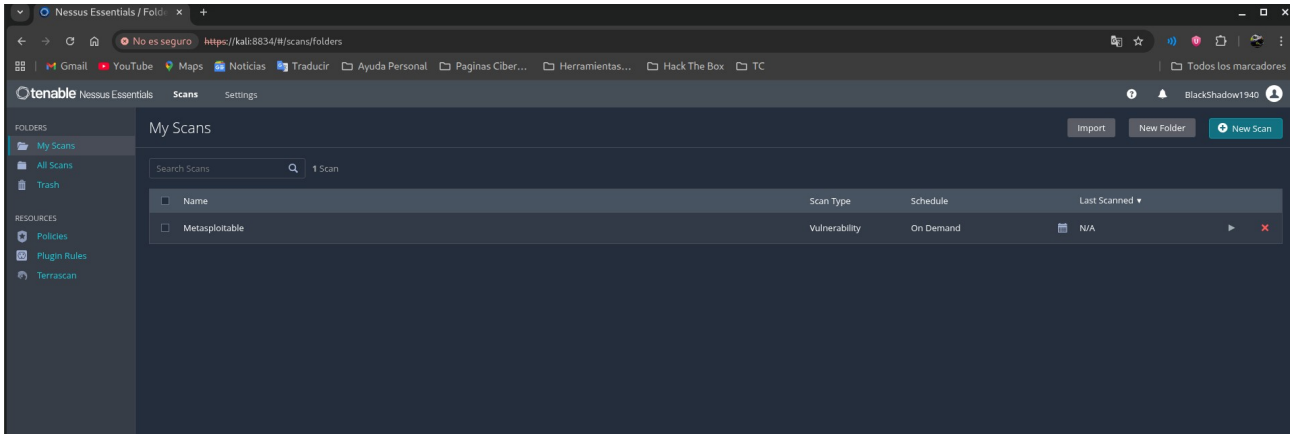


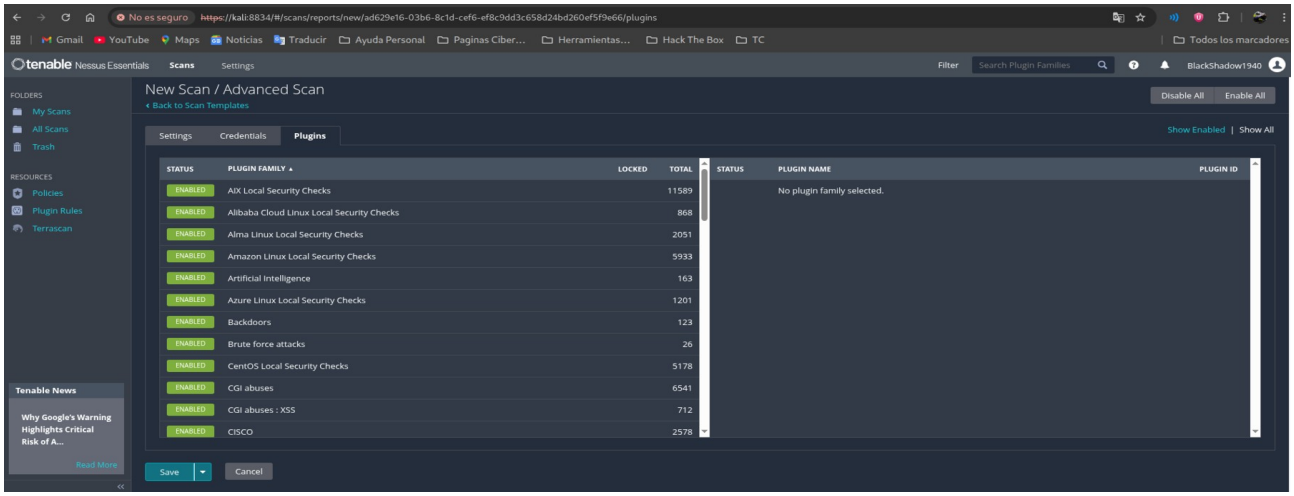


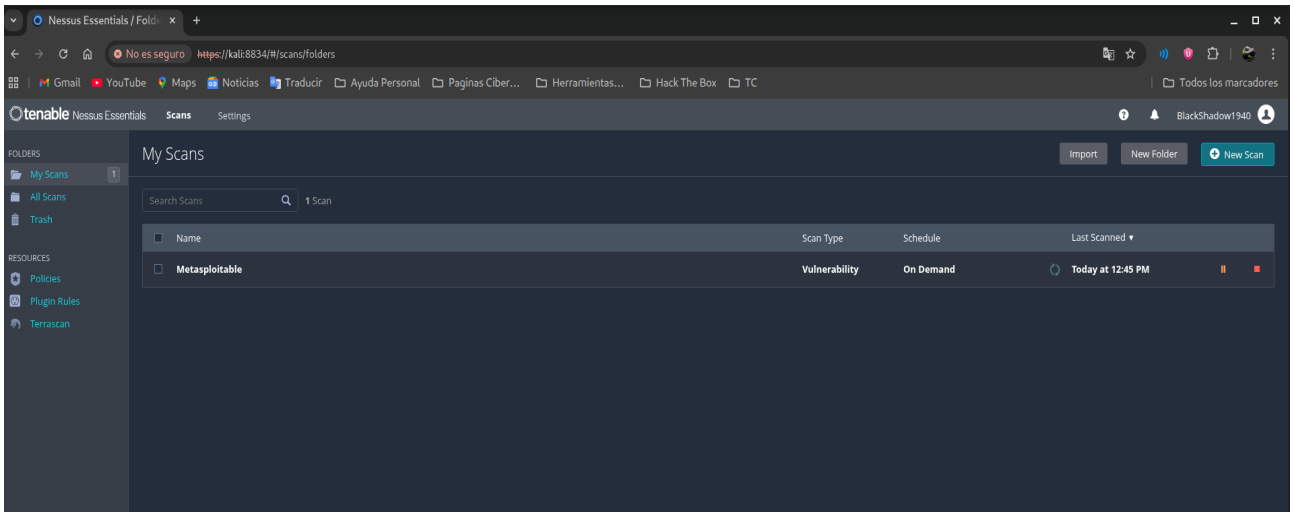
Pulsamos salvar y luego arriba a la izquierda pulsamos **launch** para iniciar el analisis.

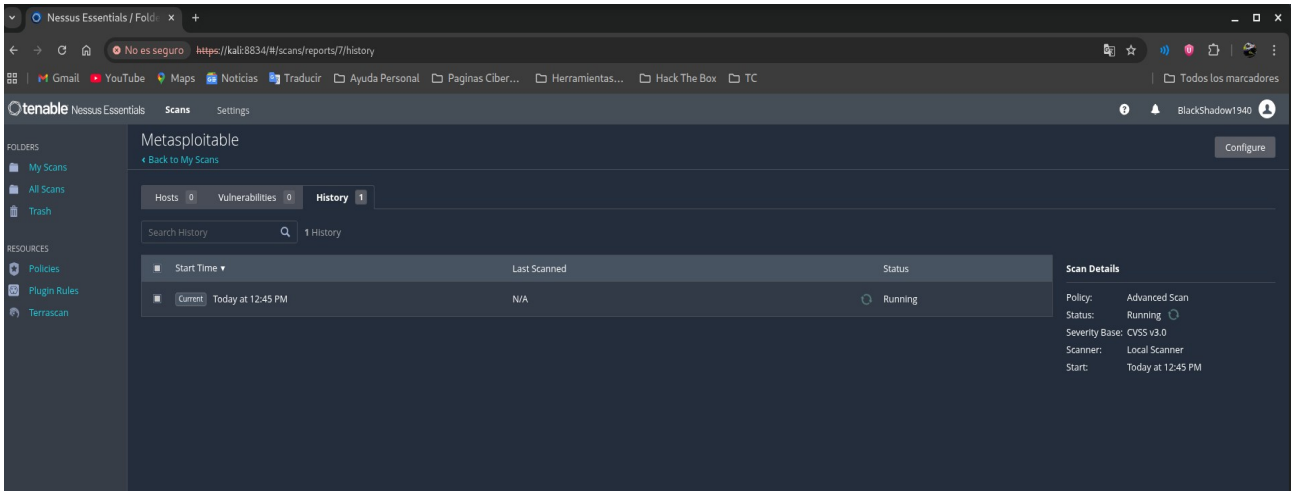


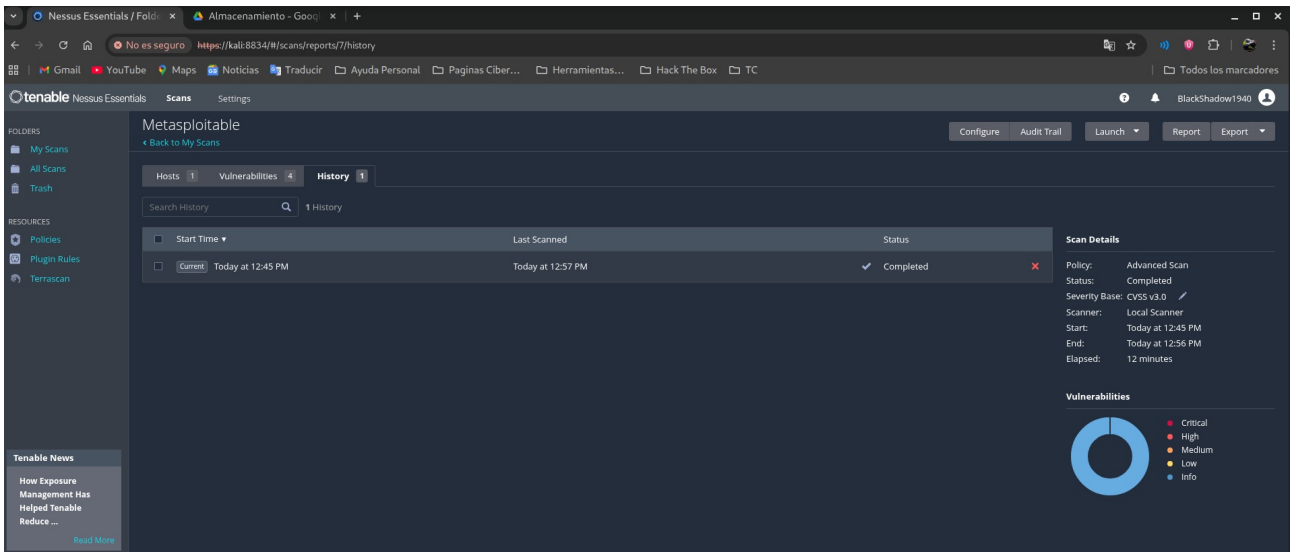


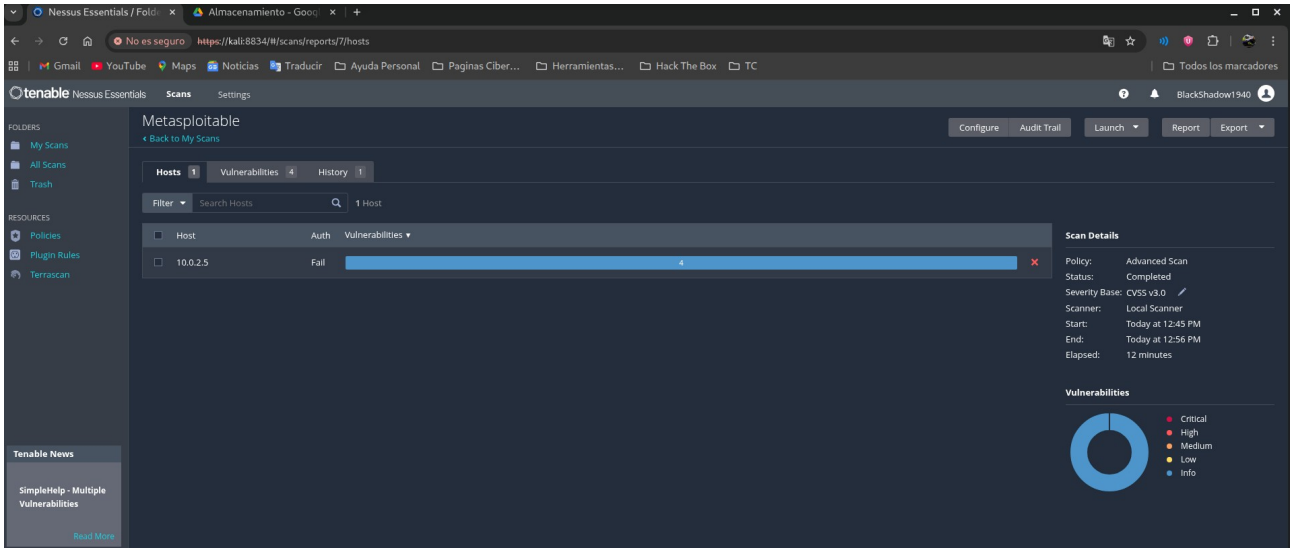


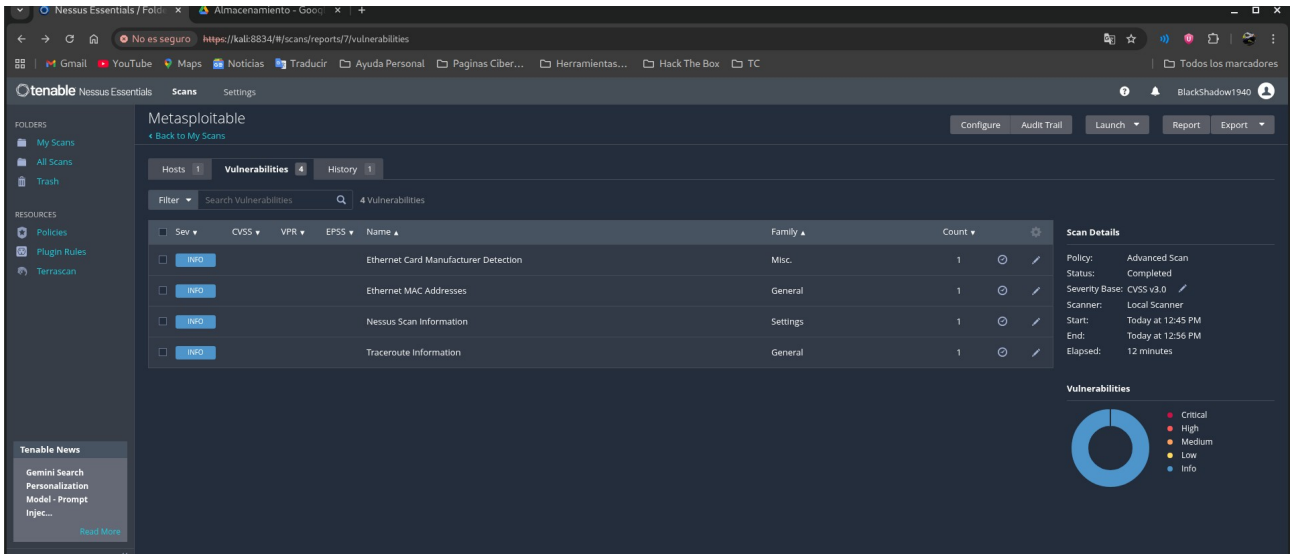

New Scan / Advanced Scan
Back to Scan Templates
Settings
Credentials
Plugins
Disable All
Enable All
Show Enabled | Show All
STATUS
PLUGIN FAMILY
LOCKED
TOTAL
PLUGIN NAME
PLUGIN ID
No plugin family selected.
ENABLED
AIX Local Security Checks 11589
Alibaba Cloud Linux Local Security Checks 868
Alma Linux Local Security Checks 2051
Amazon Linux Local Security Checks 5933
Artificial Intelligence 163
Azure Linux Local Security Checks 1201
Backdoors 123
Brute force attacks 26
CentOS Local Security Checks 5178
CGI abuses 6541
CGI abuses : XSS 712
CISCO 2578
Save
Cancel
Tenable News
Why Google's Warning Highlights Critical Risk of A...
Read More

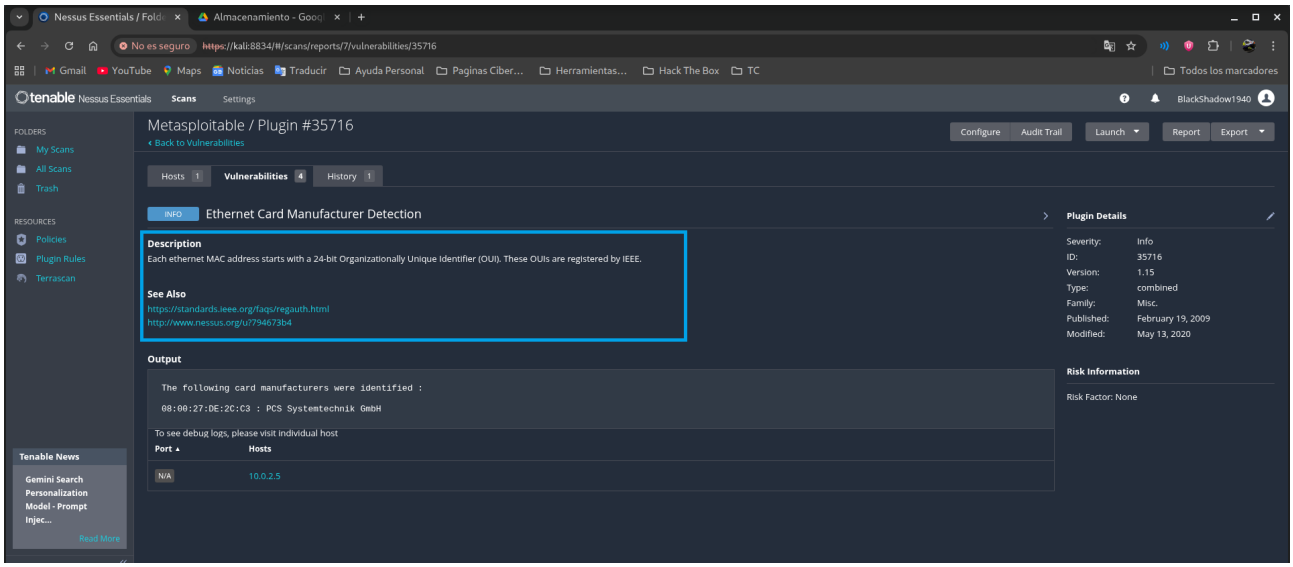

My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Scan Type
Schedule
Last Scanned
Metasploitable
Vulnerability
On Demand
Today at 12:45 PM


Metasploitable
Back to My Scans
Configure
Hosts 0
Vulnerabilities 0
History 1
Search History
1 History
Start Time
Last Scanned
Status
Current
Today at 12:45 PM
N/A
Running
Scan Details
Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 12:45 PM

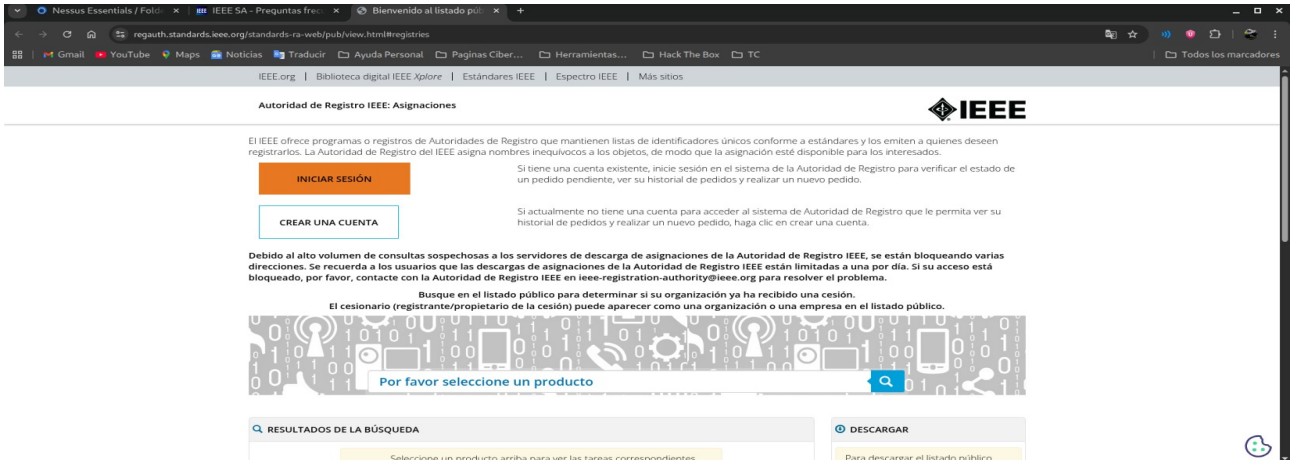

Nessus Essentials / Folde
Almacenamiento - Goog
No es seguro
https://kali:8834/#/scans/reports/7/history
Gmail
YouTube
Maps
Noticias
Traducir
Ayuda Personal
Paginas Ciber...
Herramientas...
Hack The Box
TC
Todos los marcadores
tenable Nessus Essentials
Scans
Settings
BlackShadow1940
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
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
Tenable News
How Exposure Management Has Helped Tenable Reduce ...
Read More

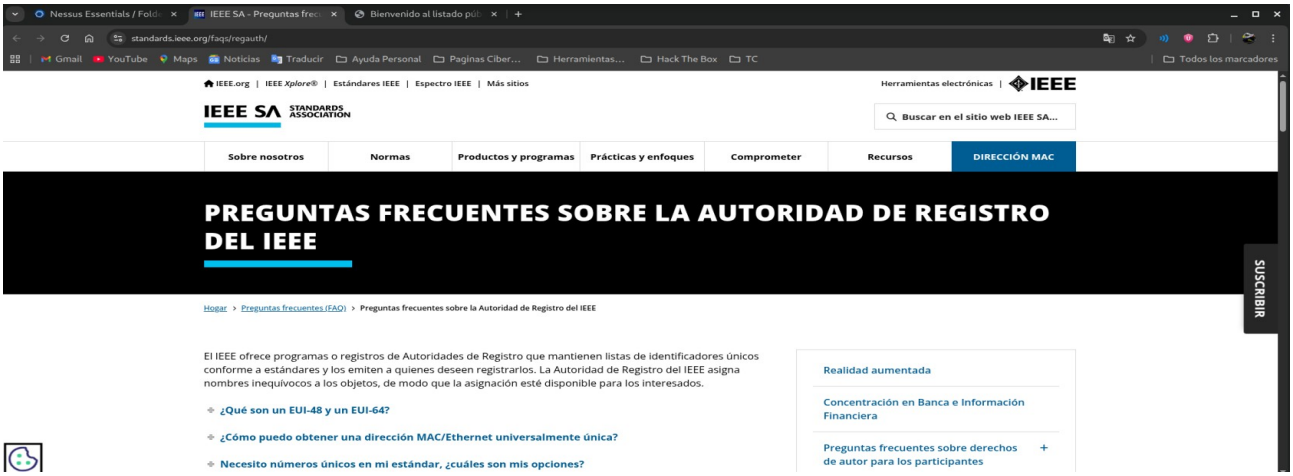

Nessus Essentials / Folde
Almacenamiento - Goog
No es seguro
https://kali:8834/#/scans/reports/7/hosts
Gmail
YouTube
Maps
Noticias
Traducir
Ayuda Personal
Paginas Ciber...
Herramientas...
Hack The Box
TC
Todos los marcadores
tenable Nessus Essentials
Scans
Settings
BlackShadow1940
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
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
Tenable News
SimpleHelp - Multiple Vulnerabilities
Read More


Nessus Essentials / Folde
Almacenamiento - Goog
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
Metasploitable
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 4
History 1
Filter
Search Vulnerabilities
4 Vulnerabilities
Sev
CVSS
VPR
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
Tenable News
Gemini Search Personalization Model - Prompt Injec...
Read More

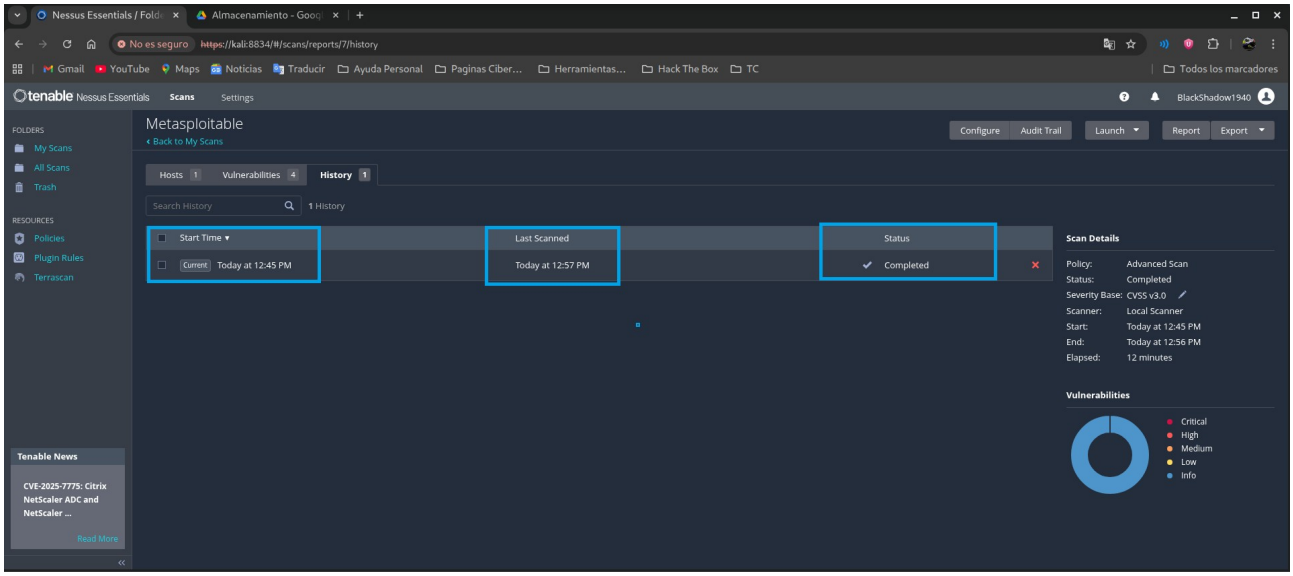


Aca esta finalizado el analisis. Se encontraron 4 vulnerabilidades.
En la captura que tiene marcado un recuadro, nos informa la descripcion y abajo dos enlaces relaciones a post con informacion de la vulnerabilidad.





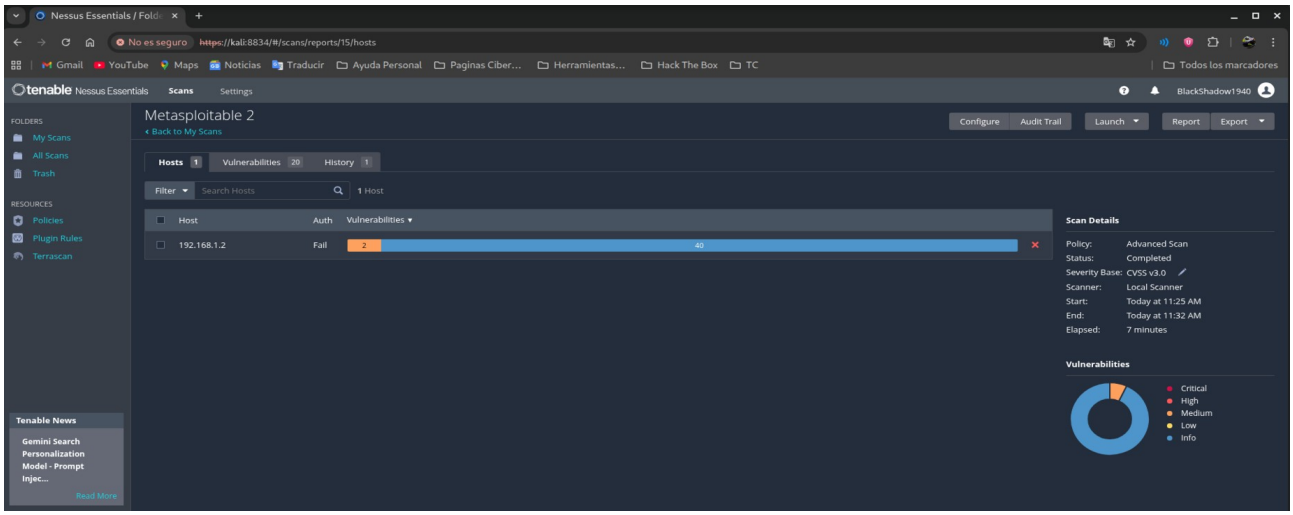
Aca estan los dos enlaces, ahi podremos encontrar informacion mas amplia, como comente antes.

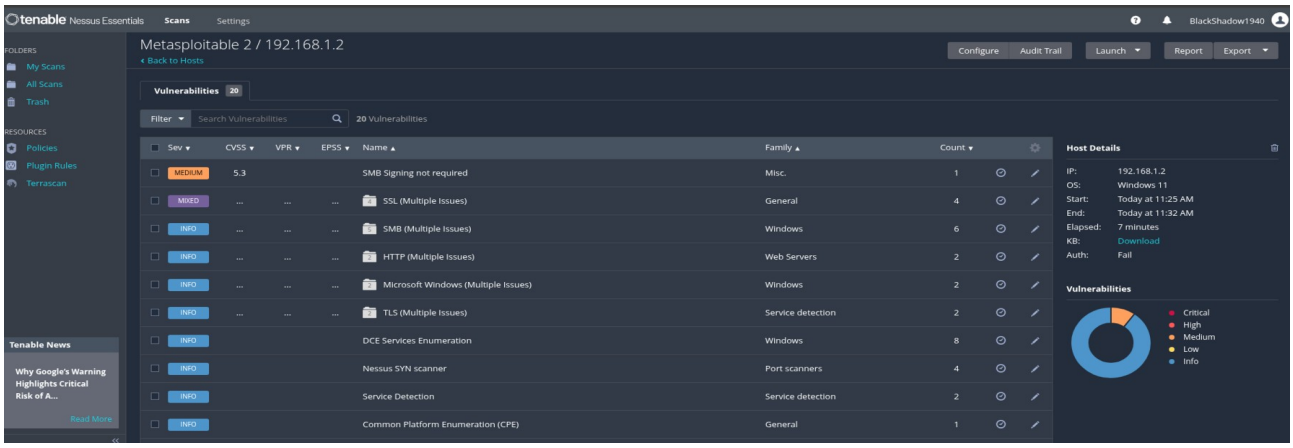


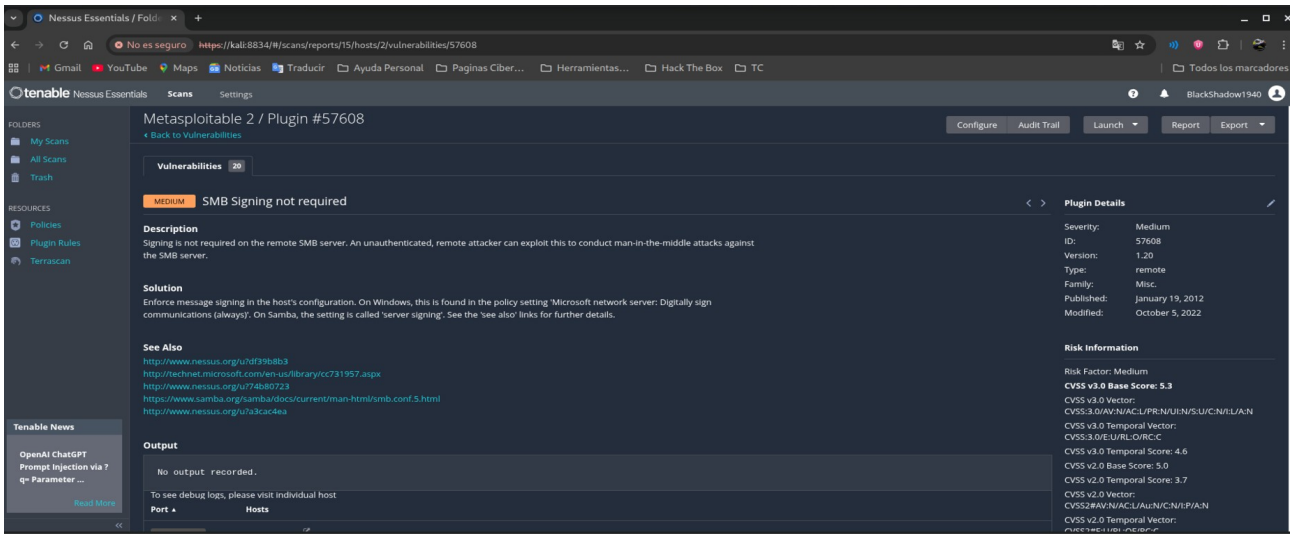
Esta ultima captura nos muestra la hora del inicio y la finalizacion del analisis. Y el ultimo recuadro, que esta completa.
Esto esta hecho con la IP del Windows10 instalado en Virtual Box.
El siguiente va a ser con la IP de Windows11 en mi PC personal.

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.







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.