

# **Martin Dalla Pozza**

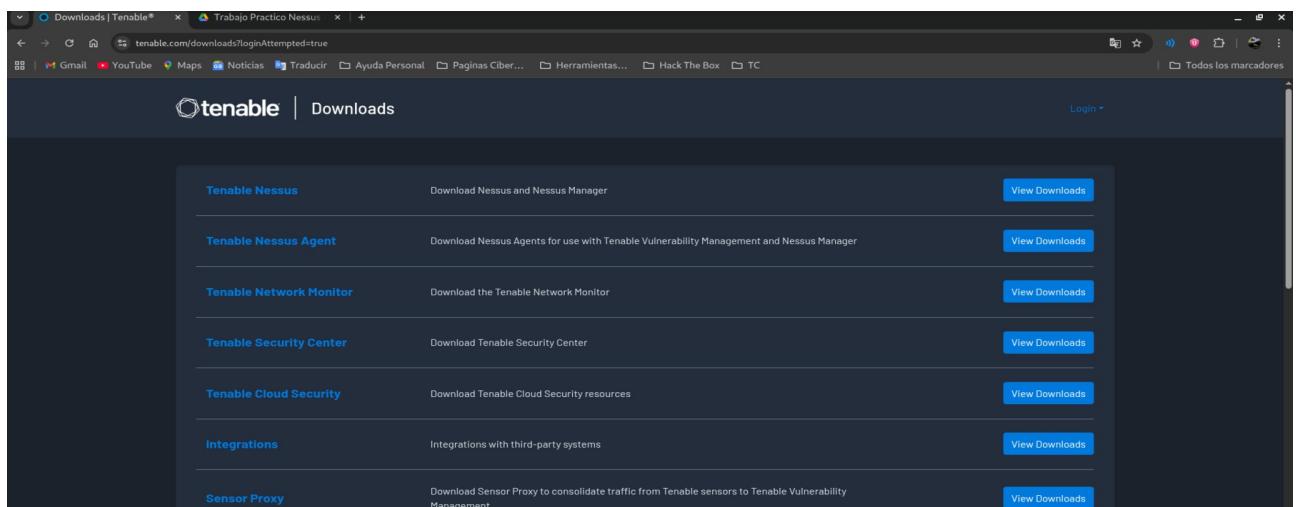
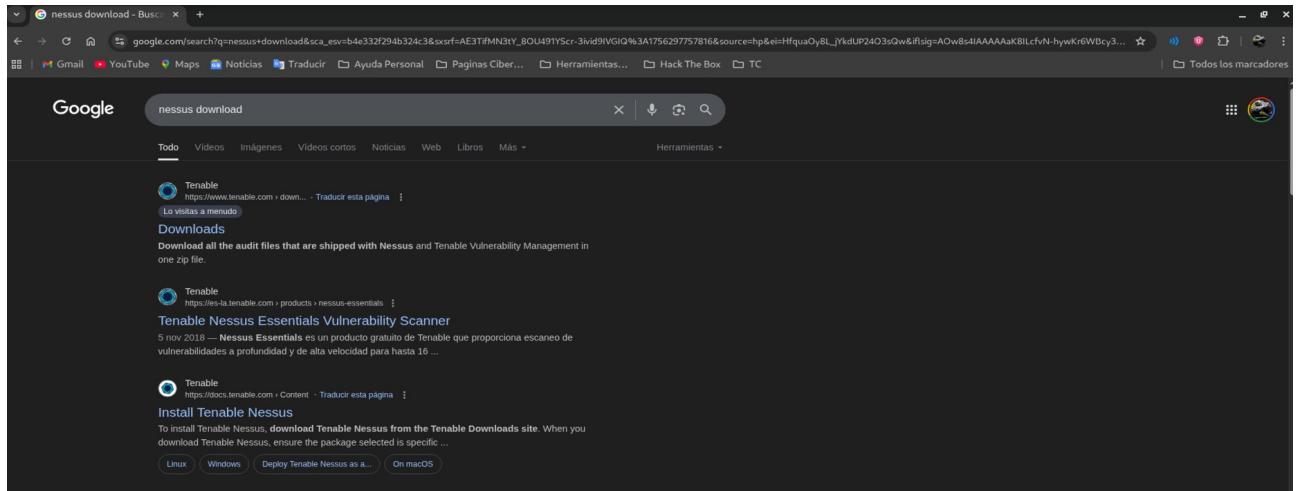
## **Trabajo practico Nessus**

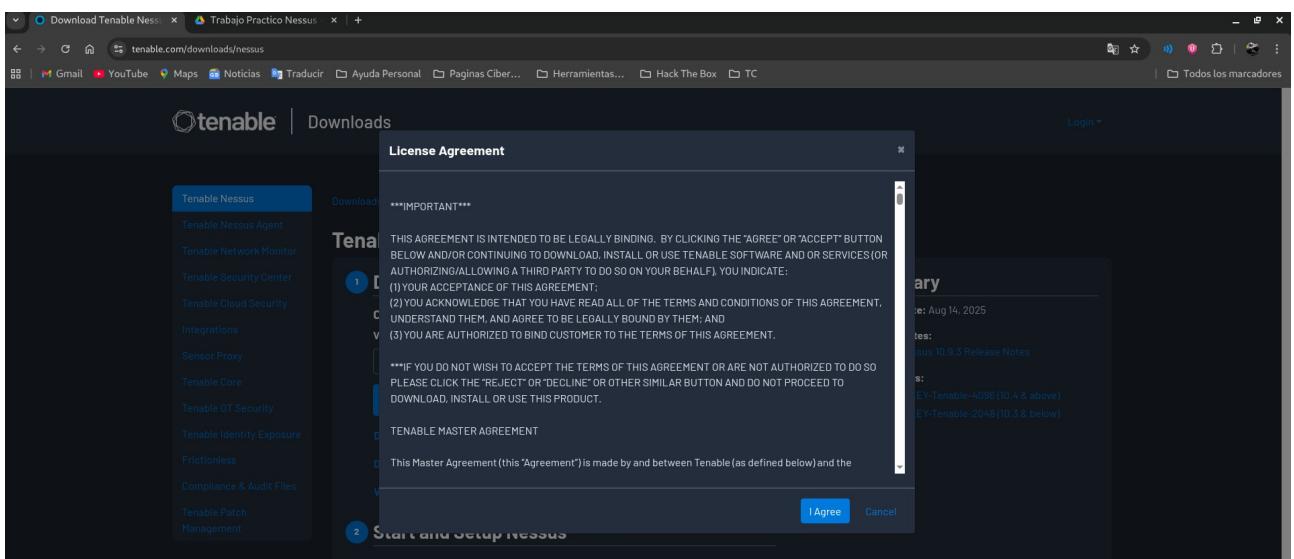
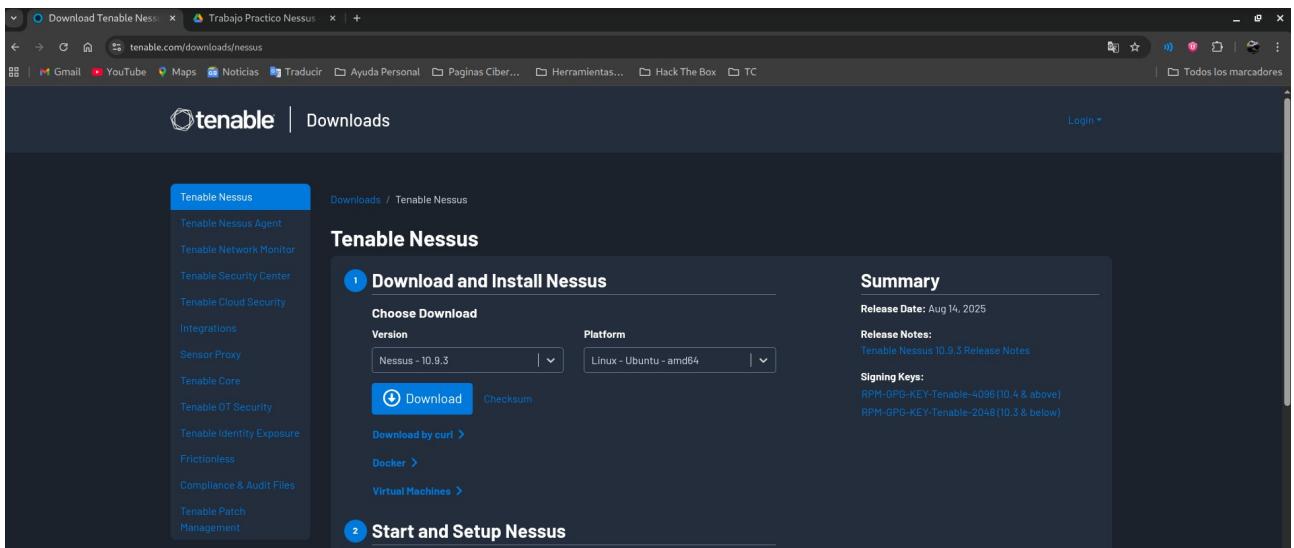
- 1.....Instalacion de Nessus**
- 2.....Ejecucion de analisis de vulnerabilidades**
- 3.....Vulnerabilidades encontradas**
- 4.....Explicacion del alumno**

## 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 aparece 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:[~]
Archivo Acciones Editar Vista Ayuda
└─(kali㉿kali)-[~]
$ cd Descargas
└─(kali㉿kali)-[~/Descargas]
└─$ ls
Nessus-10.9.3-ubuntu1604_amd64.deb
└─(kali㉿kali)-[~/Descargas]
└─$ ┌─[

Dispositivos
└─ Sistema de archivos
Red
└─ Navegar por la red
```

```
kali@kali:[~]
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 ┌─[

Dispositivos
└─ Sistema de archivos
Red
└─ Navegar por la red
```

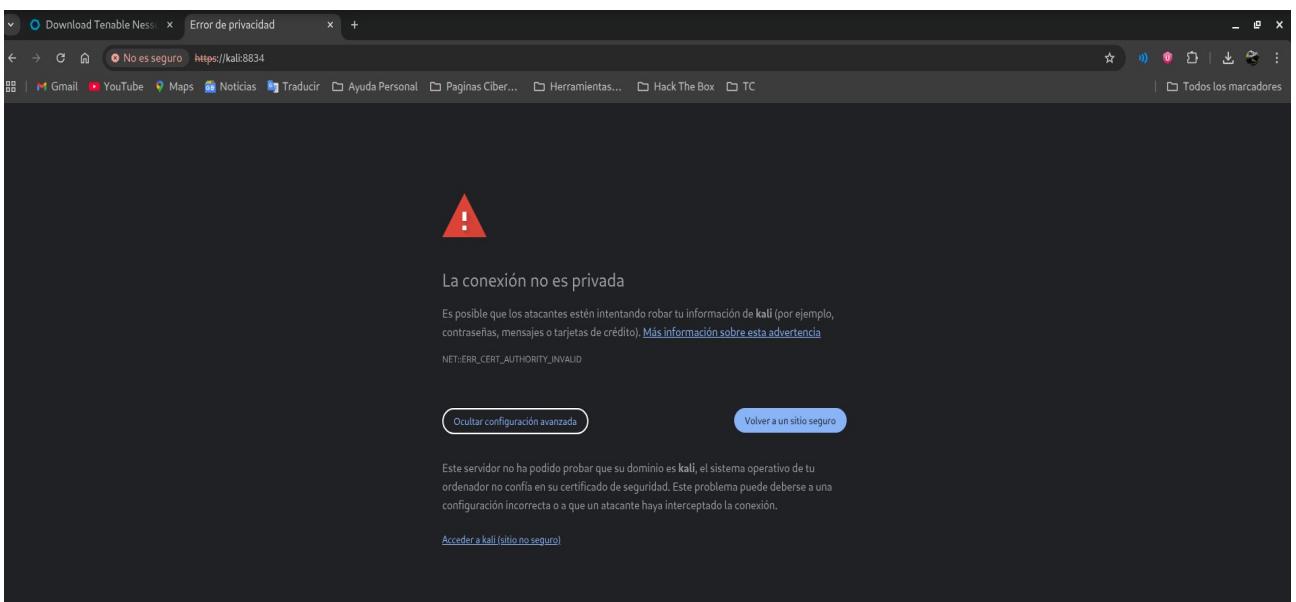
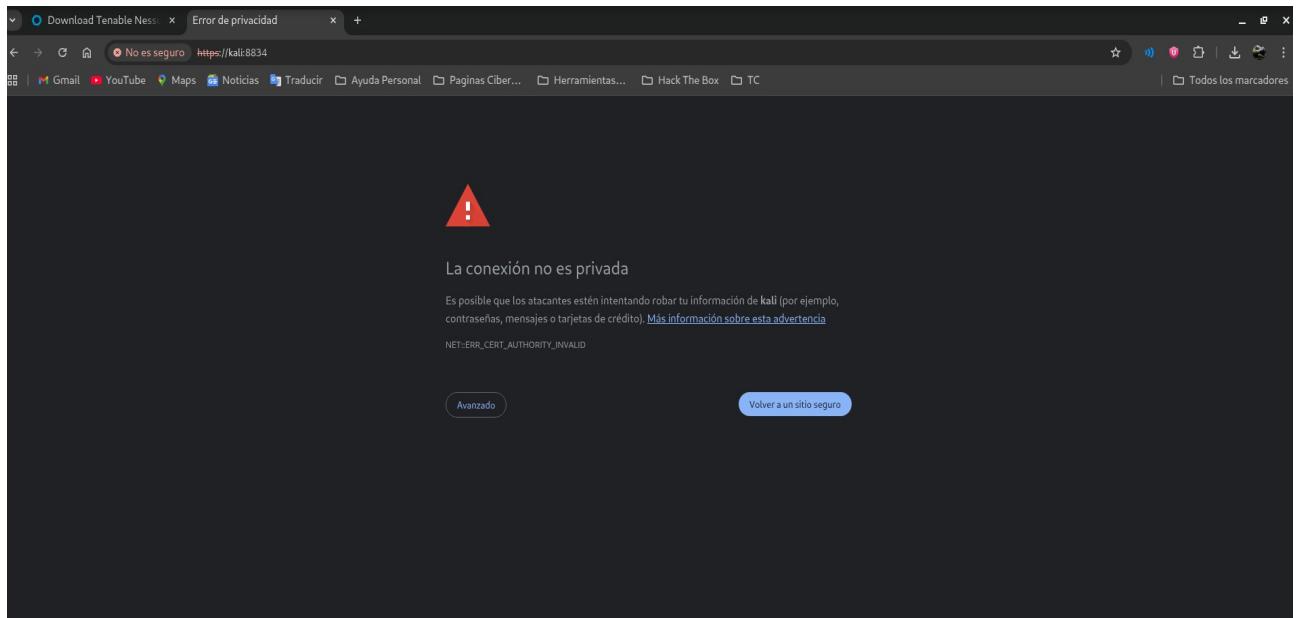
```
kali@kali:[~]
Archivo Acciones Editar Vista Ayuda
└─(kali㉿kali)-[~]
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : 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
```

```
kali@kali: ~/Descargas
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
```

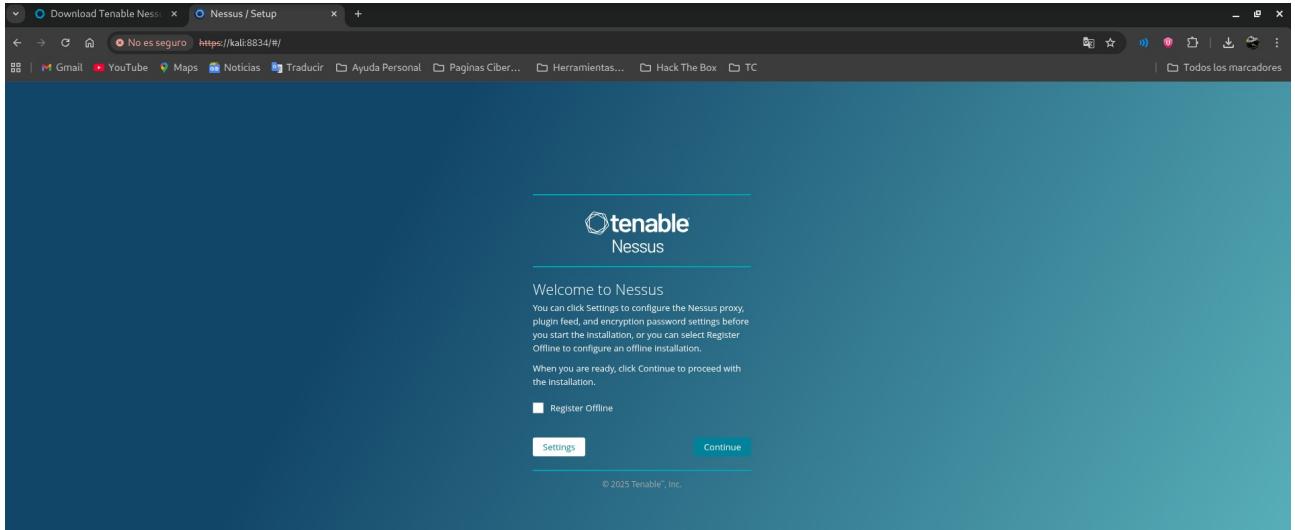
```
kali@kali: ~/Descargas
Archivo Acciones Editar Vista Ayuda
└─(kali㉿kali)-[~/Descargas]
$ /bin/systemctl start nessusd.service
└─(kali㉿kali)-[~/Descargas]
$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
    Loaded: loaded (/usr/lib/systemd/system/nessusd.service; 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 inicua Nessus se pone en el buscador <https://kali:8834>

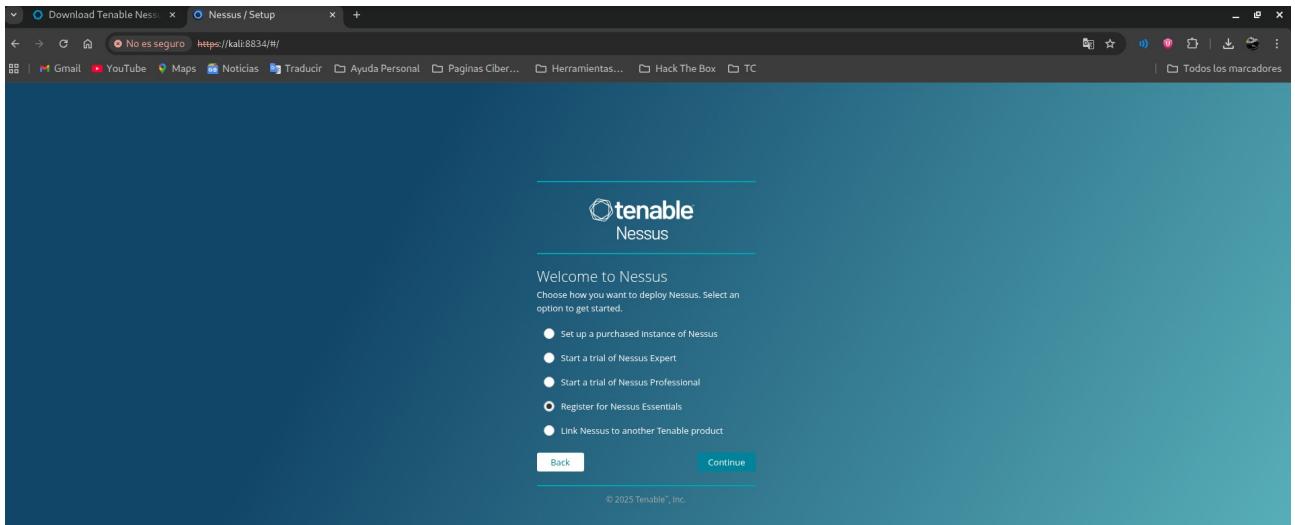
Nos pondrá una advertencia, pero avanzamos y entramos en la página.



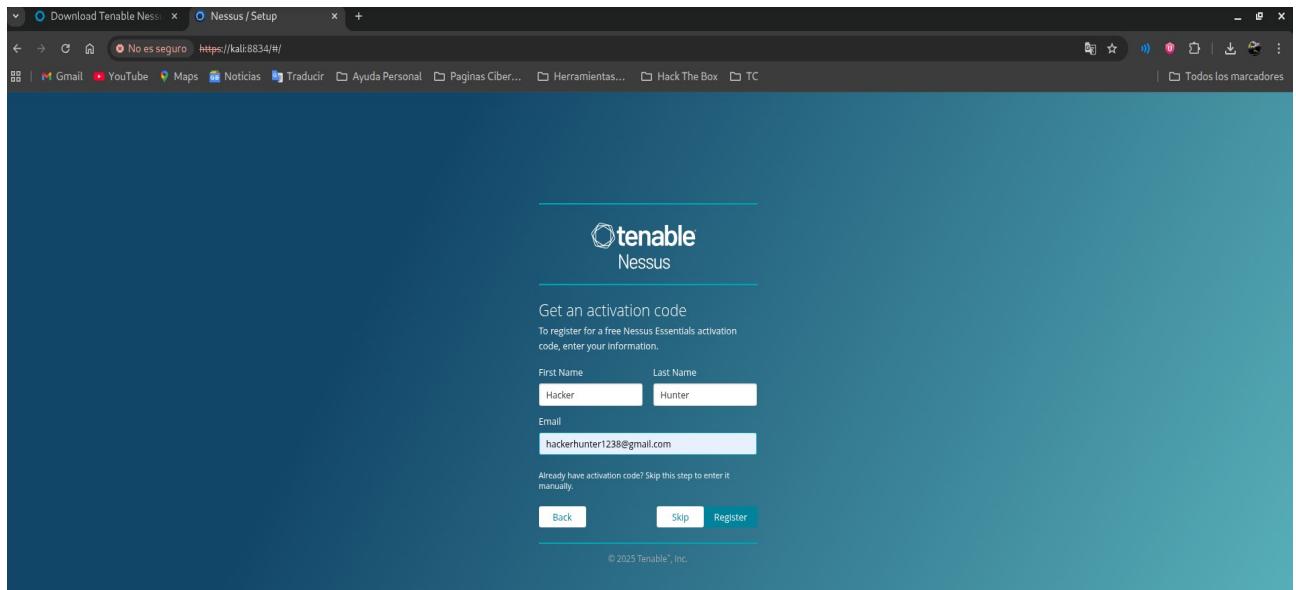
Pulsamos en continuar.....



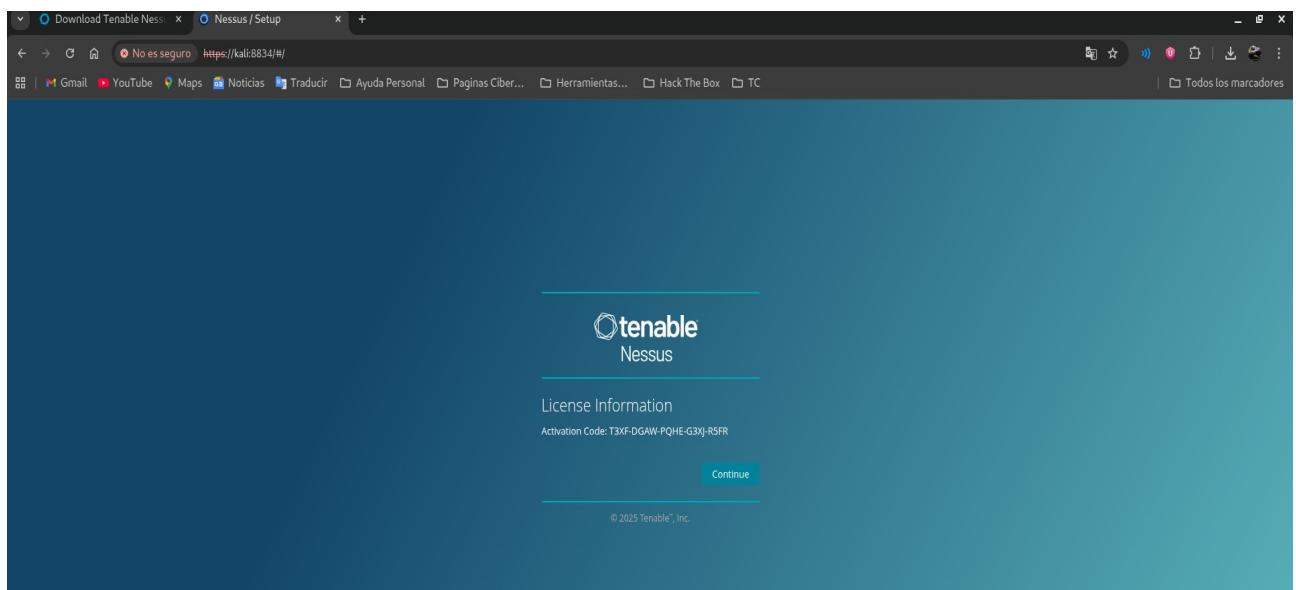
Marcamos la opcion **Register Nessus Essentials**.



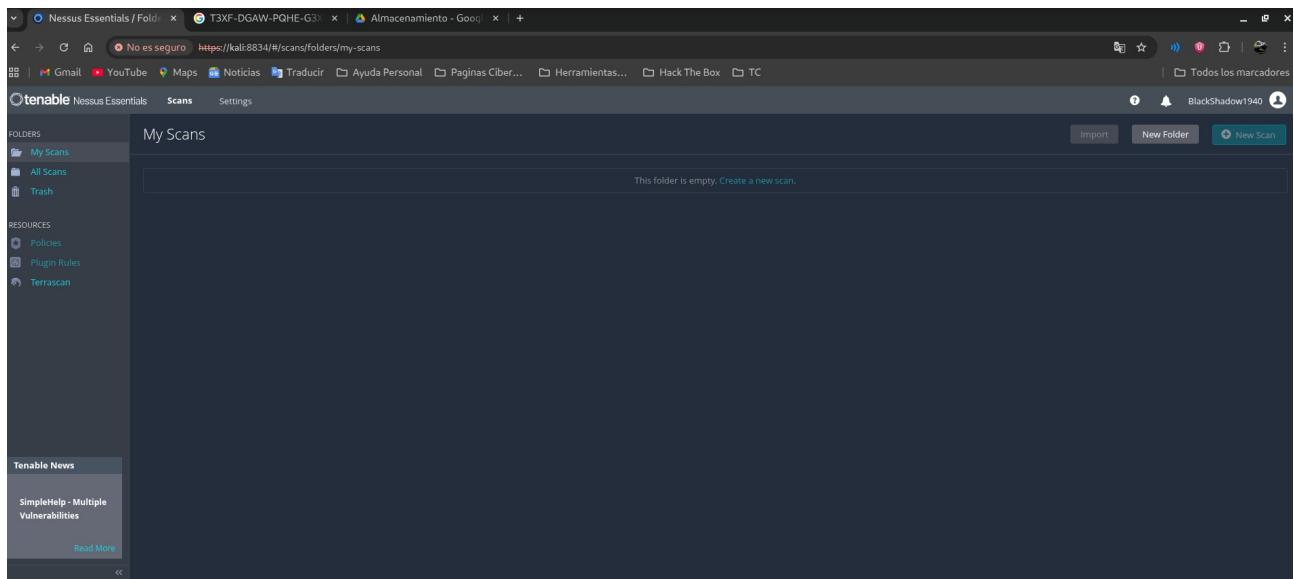
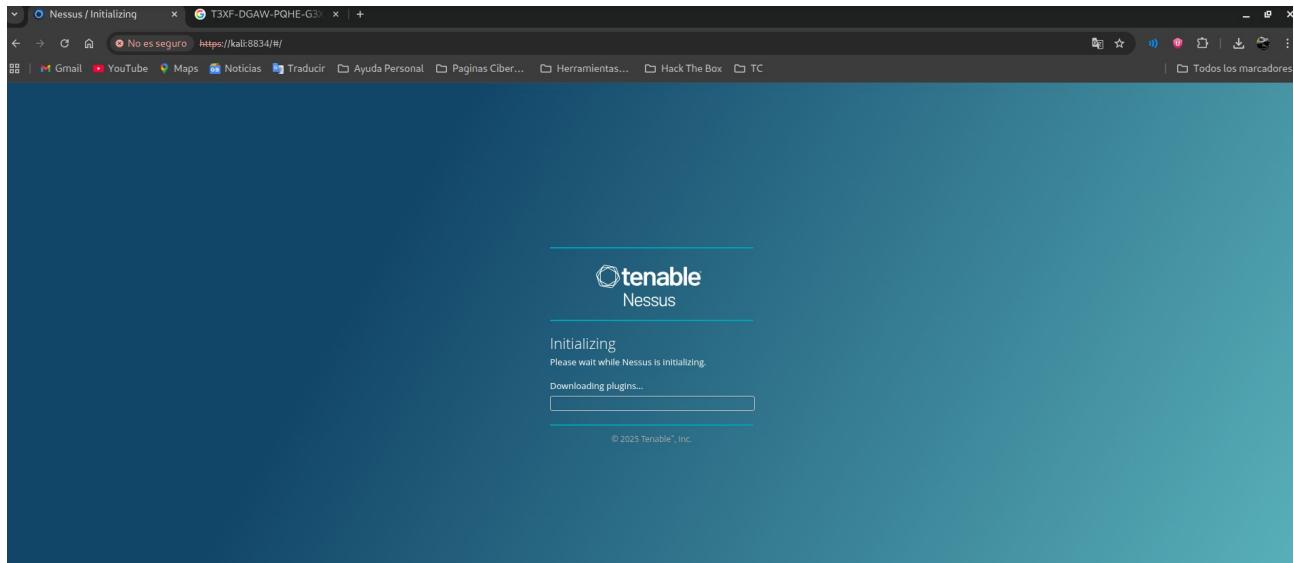
Llenamos los casilleros con Nombre y Apellido (puede ser cualquiera) y ponemos un correo electronico.



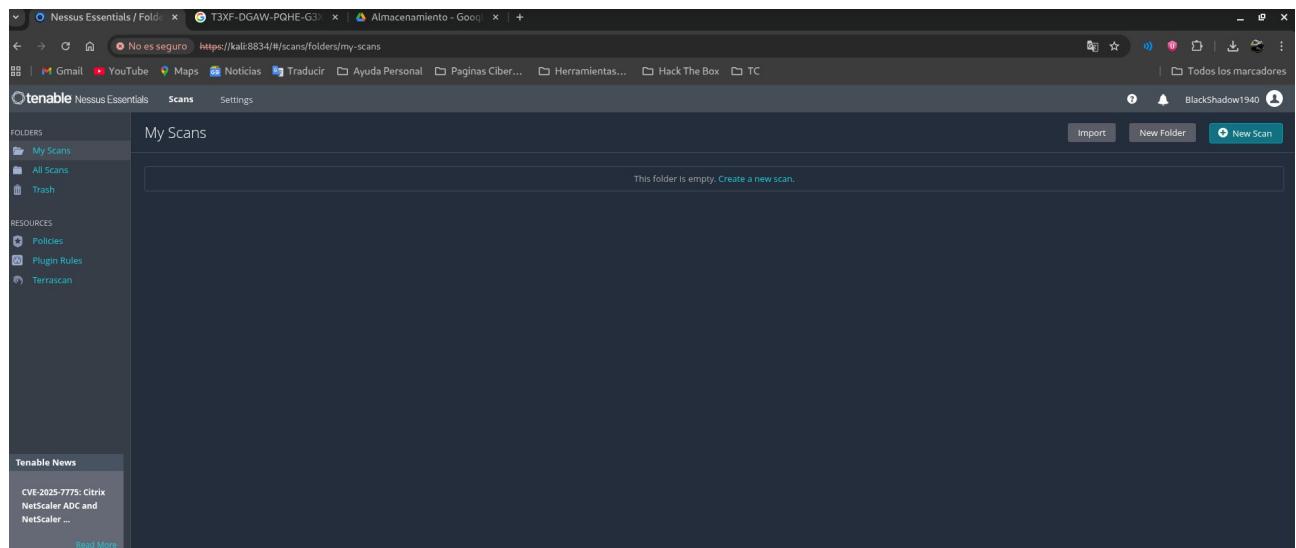
Aca veremos la informacion de licencia y el numero.



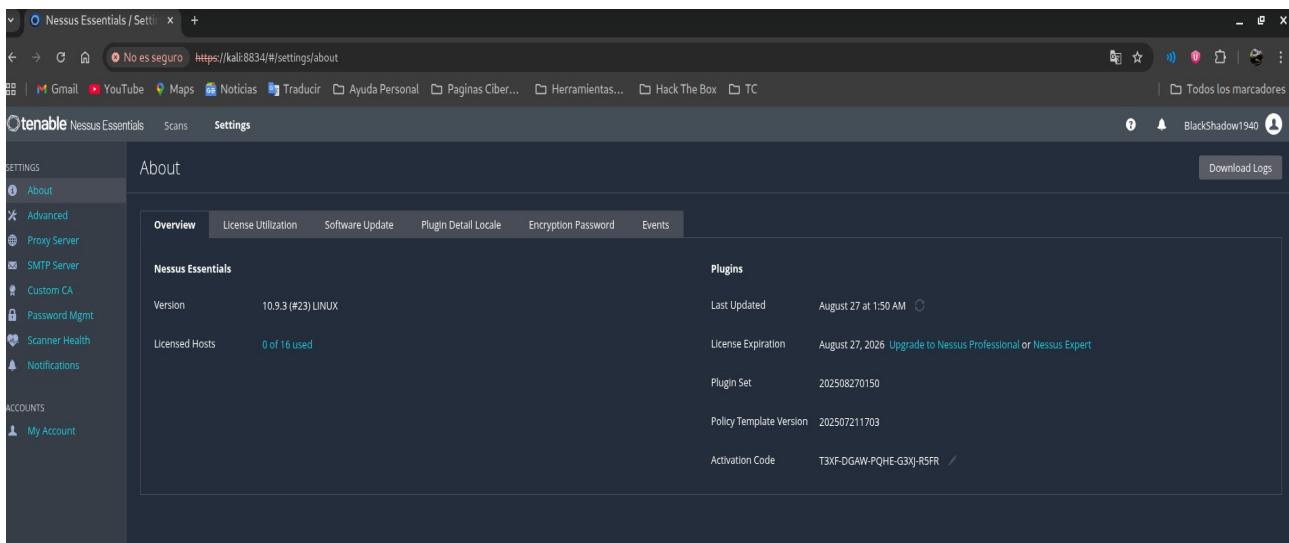
Se empiezan a cargar los plugins.



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**.

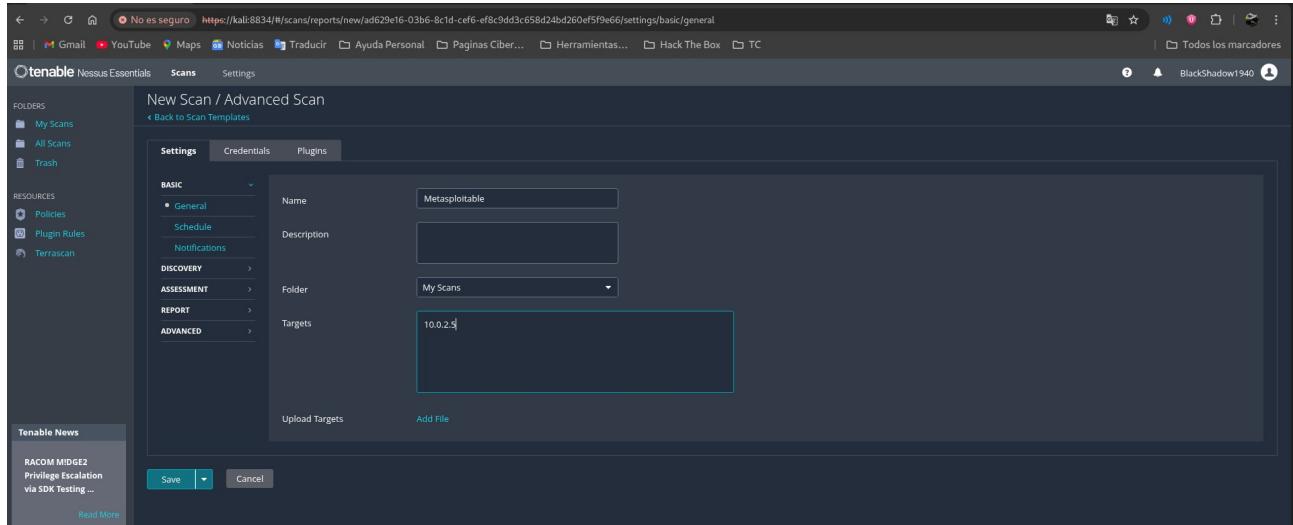
Ponemos el nombre del proyecto y la direccion IP que queremos hacer el analisis.

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

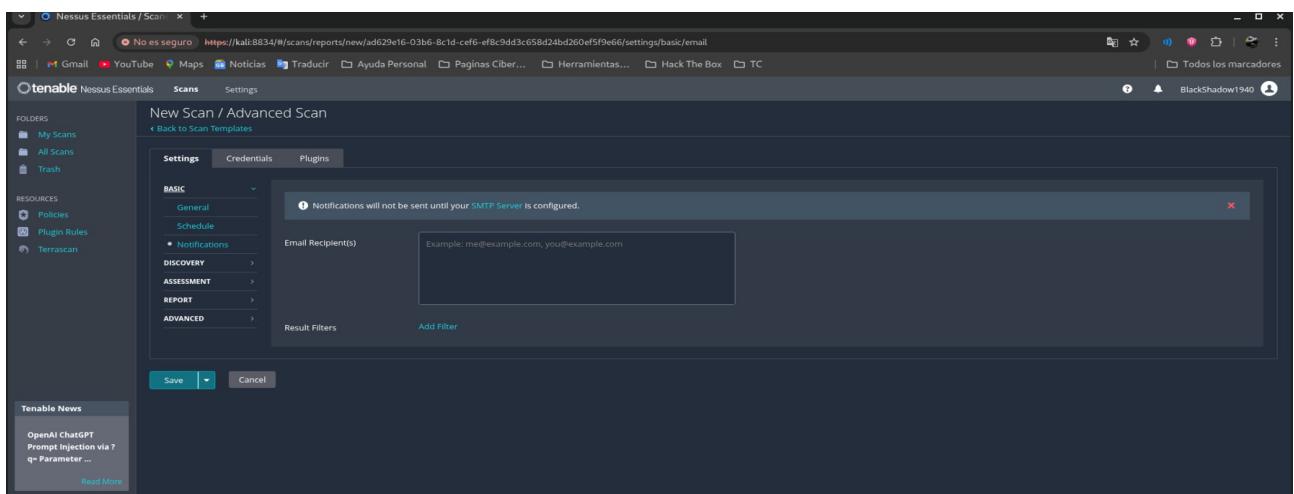
The screenshot shows the 'Scan Templates' section of the Nessus Essentials interface. On the left, there's a sidebar with 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (RACOM MIDDLE2 Privilege Escalation via SDK Testing...). The main area is titled 'Scan Templates' and has tabs for 'Scanner' and 'Discovery'. Under 'DISCOVERY', there are two cards: 'Host Discovery' (a simple scan to discover live hosts and open ports) and 'Ping-Only Discovery' (a simple scan to discover live hosts with minimal network traffic). Under 'VULNERABILITIES', there are eight cards: 'Basic Network Scan' (a full system scan suitable for any host), 'Credential Validation' (verifies credentials for hosts & Unix successfully), 'Advanced Scan' (configures a scan without using any recommendations), 'Advanced Dynamic Scan' (configures a dynamic plugin scan without recommendations), 'Malware Scan' (scans for malware on Windows and Unix systems), 'Nessus 10.8.0 / 10.8.1 Agent Reset' (scans to find and update agents), and 'Mobile Device Scan' (accesses mobile devices via Microsoft Exchange or an MDM). A 'Search Library' input field is at the top right.

The screenshot shows the 'New Scan / Advanced Scan' configuration page. The left sidebar includes 'Folders' (My Scans, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and 'Tenable News' (Why Google's Warning Highlights Critical Risk of A...). The main form is titled 'New Scan / Advanced Scan' and has tabs for 'Settings', 'Credentials', and 'Plugins'. The 'Settings' tab is active, showing fields for 'Name' (required), 'Description', 'Folder' (set to 'My Scans'), and 'Targets' (with an example value: '192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com'). There are also 'Upload Targets' and 'Add File' buttons. At the bottom are 'Save' and 'Cancel' buttons.

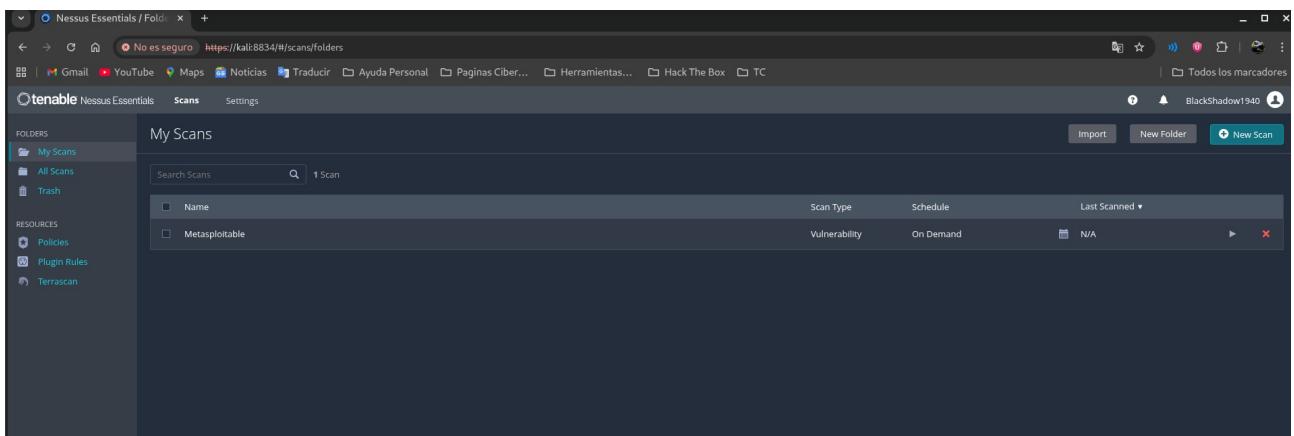
Pulsamos salvar y luego arriba a la izquierda pulsamos **launch** para iniciar el análisis.



The screenshot shows the 'New Scan / Advanced Scan' dialog in the Nessus Essentials interface. The 'Targets' field is populated with '10.0.2.5'. The 'Save' button at the bottom left is highlighted in blue. The sidebar on the left shows 'My Scans' selected under 'FOLDERS'.



The screenshot shows the 'New Scan / Advanced Scan' dialog with a notification message: 'Notifications will not be sent until your SMTP Server is configured.' The 'Email Recipient(s)' field is empty. The sidebar on the left shows 'My Scans' selected under 'FOLDERS'.



The screenshot shows the 'My Scans' list in the Nessus Essentials interface. A single scan named 'Metasploitable' is listed. The 'New Scan' button is located at the top right of the main content area. The sidebar on the left shows 'My Scans' selected under 'FOLDERS'.

New Scan / Advanced Scan

Back to Scan Templates

Settings Credentials Plugins

Show Enabled | Show All

STATUS	PLUGIN FAMILY	LOCKED	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	AIX Local Security Checks		11589		No plugin family selected.	
ENABLED	Alibaba Cloud Linux Local Security Checks		868			
ENABLED	Alma Linux Local Security Checks		2051			
ENABLED	Amazon Linux Local Security Checks		5933			
ENABLED	Artificial Intelligence		163			
ENABLED	Azure Linux Local Security Checks		1201			
ENABLED	Backdoors		123			
ENABLED	Brute force attacks		26			
ENABLED	CentOS Local Security Checks		5178			
ENABLED	CGI abuses		6541			
ENABLED	CGI abuses : XSS		712			
ENABLED	CISCO		2578			

Save Cancel

My Scans

Import New Folder New Scan

Name	Scan Type	Schedule	Last Scanned
Metasploitable	Vulnerability	On Demand	Today at 12:45 PM

Metasploitable

Back to My Scans

Hosts 0 Vulnerabilities 0 History 1

Search 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 / Folders | Almacenamiento - Google Drive | +

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

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

Tenable Nessus Essentials Scans Settings

Metasploitable Back to My Scans

Hosts 1 Vulnerabilities 4 History 1

Search 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 / Folders | Almacenamiento - Google Drive | +

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

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

Tenable Nessus Essentials Scans Settings

Metasploitable Back to My Scans

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 / Folders | Almacenamiento - Google Drive | +

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

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

Tenable Nessus Essentials Scans Settings

Metasploitable Back to My Scans

Hosts 1 Vulnerabilities 4 History 1

Filter ▾ Search Vulnerabilities 4 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count	Configure
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](#)

**Metasploitable / Plugin #35716**

**Description**  
Each ethernet MAC address starts with a 24-bit Organizational Unique Identifier (OUI). These OUs are registered by IEEE.

**See Also**  
<https://standards.ieee.org/faqs/regauth.html>  
<http://www.nessus.org/u7794073b4>

**Output**  
The following card manufacturers were identified :  
08:00:27:DE:2C:C3 : PCS Systemtechnik GmbH  
To see debug logs, please visit individual host

Port	Hosts
N/A	10.0.2.5

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.

**Autoridad de Registro IEEE: Asignaciones**

El IEEE ofrece programas o registros de Autoridades de Registro que mantienen listas de identificadores únicos conforme a estándares y los emiten a quienes deseen registrarse. La Autoridad de Registro del IEEE asigna nombres inequívocos a los objetos, de modo que la asignación esté disponible para los interesados.

**INICIAR SESIÓN**

**CREAR UNA CUENTA**

Si actualmente no tiene una cuenta existente, inicie sesión en el sistema de la Autoridad de Registro para verificar el estado de un pedido pendiente, ver su historial de pedidos y realizar un nuevo pedido.

Si actualmente no tiene una cuenta para acceder al sistema de Autoridad de Registro que le permita ver su historial de pedidos y realizar un nuevo pedido, haga clic en crear una cuenta.

Debido al alto volumen de consultas sospechosas a los servidores de descarga de asignaciones de la Autoridad de Registro IEEE, se están bloqueando varias direcciones. Se recuerda a los usuarios que las descargas de asignaciones de la Autoridad de Registro IEEE están limitadas a una por día. Si su acceso está bloqueado, por favor, contacte con la Autoridad de Registro IEEE en [ieee-registration-authority@ieee.org](mailto:ieee-registration-authority@ieee.org) para resolver el problema.

Busque en el listado público para determinar si su organización ya ha recibido una cesión.

**Por favor seleccione un producto**

**RESULTADOS DE LA BÚSQUEDA**

**DESCARGAR**

**PREGUNTAS FRECUENTES SOBRE LA AUTORIDAD DE REGISTRO DEL IEEE**

**Sobre nosotros** | **Normas** | **Productos y programas** | **Prácticas y enfoques** | **Comprometer** | **Recursos** | **DIRECCIÓN MAC**

**Herramientas electrónicas** | **IEEE**

**Realidad aumentada**

**Concentración en Banca e Información Financiera**

**Preguntas frecuentes sobre derechos de autor para los participantes**

**SUSCRIBIR**

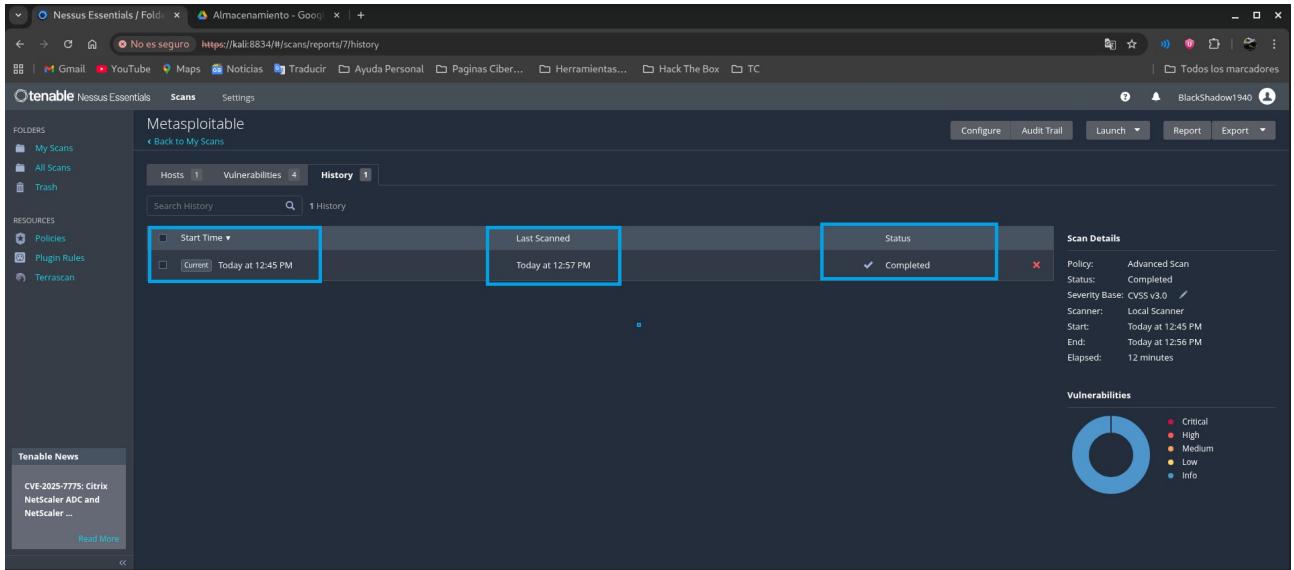
**El IEEE ofrece programas o registros de Autoridades de Registro que mantienen listas de identificadores únicos conforme a estándares y los emiten a quienes deseen registrarse. La Autoridad de Registro del IEEE asigna nombres inequívocos a los objetos, de modo que la asignación esté disponible para los interesados.**

**¿Qué son un EUI-48 y un EUI-64?**

**¿Cómo puedo obtener una dirección MAC/Ethernet universalmente única?**

**Necesito números únicos en mi estándar, ¿cuáles son mis opciones?**

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



The screenshot shows the Nessus Essentials interface with a scan report for 'Metasploitable'. The report details the following information:

- 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:** A pie chart indicates the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), and Info (blue).

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 parecen 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.

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

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

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

- <http://www.nessus.org/udf39b8b3>
- <http://technet.microsoft.com/en-us/library/cc731957.aspx>
- <http://www.nessus.org/u74b80723>
- <http://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>
- <http://www.nessus.org/u/a3cac4ea>

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

CVSS v3.0 Base Score:	5.3
CVSS v3.0 Vector:	CVSS3.0:AV:N/AC:L/PR:N/U:N/S:U/C:N/I:L/A:N
CVSS v3.0 Temporal Vector:	CVSS3.0:TE:R/L/D/R/C/C
CVSS v2.0 Temporal Score:	4.6
CVSS v2.0 Base Score:	5.0
CVSS v2.0 Vector:	CVSS2:AV:N/AC:L/Au:N/C/N/I/P/A:N
CVSS v2.0 Temporal Vector:	CVSS2:TE:R/L/D/R/C/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.