



**Certificado de Profesionalidad en  
Seguridad Informática  
IronHack - SOC**

**Módulo 2  
Práctica 2 - GreenBone OpenVas**

**Alumno: Julián Gordon**

# Indice

<b>Introducción</b>	<b>3</b>
<b>Descarga e Instalación de OpenVAS</b>	<b>4</b>
<b>Configuración de OpenVAS</b>	<b>11</b>
<b>Realización del Análisis sobre máquina Kali Linux</b>	<b>12</b>
<b>Análisis sobre Máquina Metasploitable</b>	<b>15</b>
<b>Conclusiones</b>	<b>16</b>

# Introducción

En el actual panorama de ciberseguridad, donde las amenazas evolucionan constantemente, es fundamental contar con herramientas efectivas para evaluar la seguridad de los sistemas de información (SI) y prevenir posibles vulnerabilidades. Una de estas herramientas es Greenbone OpenVAS (Open Vulnerability Assessment System), una solución de software libre ampliamente reconocida por su capacidad para identificar y analizar vulnerabilidades en redes y dispositivos.

El presente trabajo se centra en la introducción y exploración de Greenbone OpenVAS, con el objetivo de proporcionar una comprensión fundamental de su instalación, configuración y uso en la evaluación de la seguridad de los sistemas de información. A través de una serie de pasos prácticos, explicaremos el proceso de preparación del entorno virtual, la instalación de OpenVAS, su configuración inicial y la realización de un análisis de vulnerabilidades en un entorno controlado.

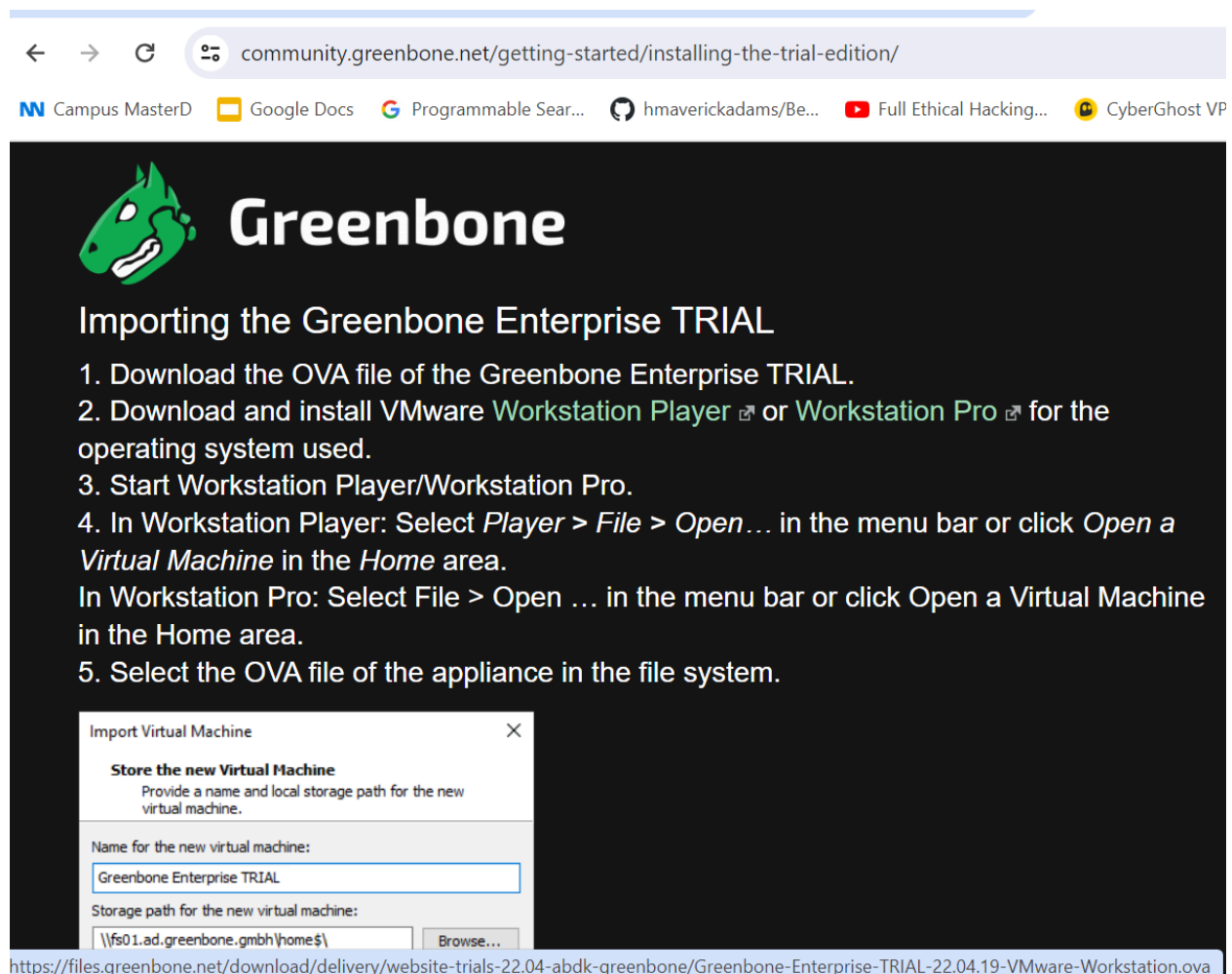
Durante el desarrollo de esta actividad, se abordarán conceptos clave relacionados con la ciberseguridad, como la importancia de la evaluación proactiva de las vulnerabilidades, la configuración adecuada de herramientas de seguridad y la comprensión de los resultados obtenidos a través de los escaneos de vulnerabilidades.

Mediante este trabajo práctico, se busca dotarnos de los conocimientos y habilidades necesarios para utilizar Greenbone OpenVAS como una herramienta efectiva en la identificación y mitigación de riesgos de seguridad en los sistemas de información, contribuyendo así a fortalecer la postura de seguridad de las organizaciones ante las amenazas cibernéticas.

## Descarga e instalación de la herramienta OpenVAS

Es importante destacar que este ejercicio lo realizaremos en Virtual Box, que es un software de virtualización que nos permite crear y ejecutar máquinas virtuales en un entorno de escritorio, facilitando el desarrollo y prueba de sistemas operativos y aplicaciones en diferentes configuraciones de hardware. Ya tenemos creada nuestra máquina virtual de Kali Linux y haremos nuestras pruebas desde allí. Lo siguiente que debemos hacer es crear una máquina virtual de Greenbone OpenVAS en nuestro VirtualBox.

Para realizar este procedimiento, lo primero que vamos a hacer será visitar la página oficial de Greenbone Security y descargar la OVA que luego importaremos en VirtualBox. <https://community.greenbone.net/getting-started/installing-the-trial-edition/>



The screenshot shows a web browser window with the address bar displaying [community.greenbone.net/getting-started/installing-the-trial-edition/](https://community.greenbone.net/getting-started/installing-the-trial-edition/). The browser's tab bar shows several open tabs: 'Campus MasterD', 'Google Docs', 'Programmable Sear...', 'hmaverickadams/Be...', 'Full Ethical Hacking...', and 'CyberGhost VP'. The main content area of the browser displays the Greenbone logo (a green dragon head) and the title 'Greenbone'. Below the logo, the heading 'Importing the Greenbone Enterprise TRIAL' is followed by a list of five numbered steps: 1. Download the OVA file of the Greenbone Enterprise TRIAL. 2. Download and install VMware Workstation Player or Workstation Pro for the operating system used. 3. Start Workstation Player/Workstation Pro. 4. In Workstation Player: Select Player > File > Open... in the menu bar or click Open a Virtual Machine in the Home area. In Workstation Pro: Select File > Open ... in the menu bar or click Open a Virtual Machine in the Home area. 5. Select the OVA file of the appliance in the file system. Below the list, there is a screenshot of the 'Import Virtual Machine' dialog box in VMware. The dialog box has a title bar 'Import Virtual Machine' and a close button. It contains the text 'Store the new Virtual Machine' and 'Provide a name and local storage path for the new virtual machine.' There are two input fields: 'Name for the new virtual machine:' with the text 'Greenbone Enterprise TRIAL' and 'Storage path for the new virtual machine:' with the text '\\fs01.ad.greenbone.gmbh\home\$'. A 'Browse...' button is next to the storage path field. At the bottom of the browser window, the URL <https://files.greenbone.net/download/delivery/website-trials-22.04-abdk-greenbone/Greenbone-Enterprise-TRIAL-22.04.19-VMware-Workstation.ova> is visible.

1. Download the OVA file of the Greenbone Enterprise TRIAL.
2. Download and install VMware Workstation Player or Workstation Pro for the operating system used.
3. Start Workstation Player/Workstation Pro.
4. In Workstation Player: Select *Player* > *File* > *Open...* in the menu bar or click *Open a Virtual Machine* in the *Home* area.  
In Workstation Pro: Select *File* > *Open ...* in the menu bar or click *Open a Virtual Machine* in the *Home* area.
5. Select the OVA file of the appliance in the file system.

Import Virtual Machine


Store the new Virtual Machine  
Provide a name and local storage path for the new virtual machine.

Name for the new virtual machine:  
Greenbone Enterprise TRIAL

Storage path for the new virtual machine:  
\\fs01.ad.greenbone.gmbh\home\$ Browse...

<https://files.greenbone.net/download/delivery/website-trials-22.04-abdk-greenbone/Greenbone-Enterprise-TRIAL-22.04.19-VMware-Workstation.ova>

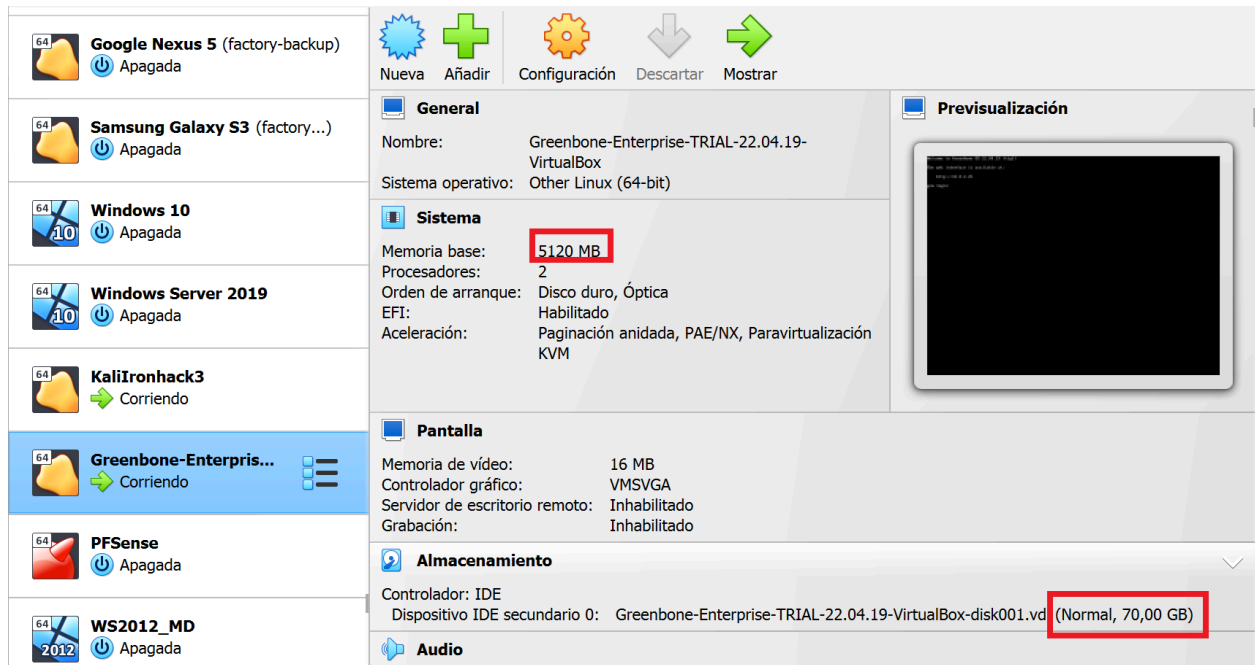
## Importing the Greenbone Enterprise TRIAL

1. Download the OVA file of the Greenbone Enterprise TRIAL.
2. Download and install Oracle VirtualBox for the operating system used.
3. Start VirtualBox.
4. Select *File > Import Appliance ...* in the menu bar.
5. Click  and select the OVA file of the appliance in the file system.

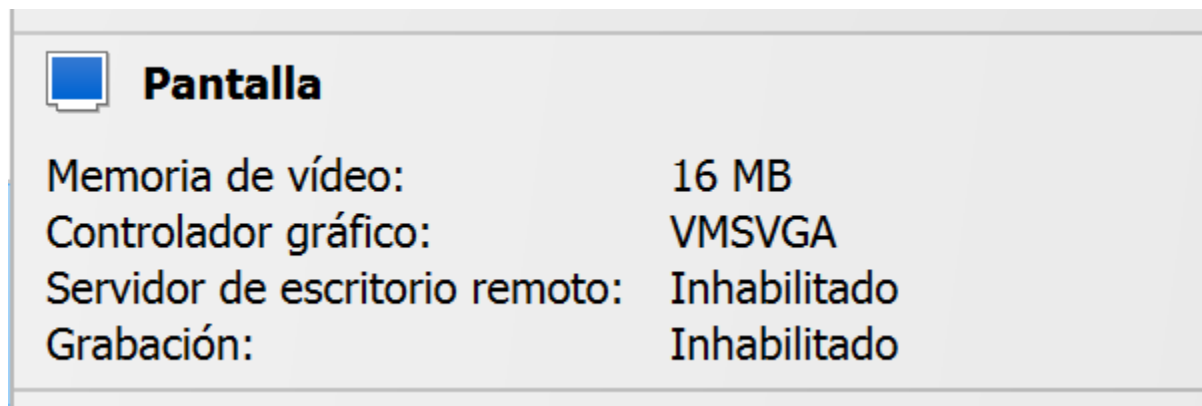
Desde VirtualBox importamos la OVA que nos descargamos.



Una vez importada la OVA debemos asegurarnos de darle al menos 4 GB de RAM y 40GB de espacio en disco disponible para la máquina virtual, ya que la instalación de Greenbone OpenVAS requiere recursos significativos para operar eficientemente.

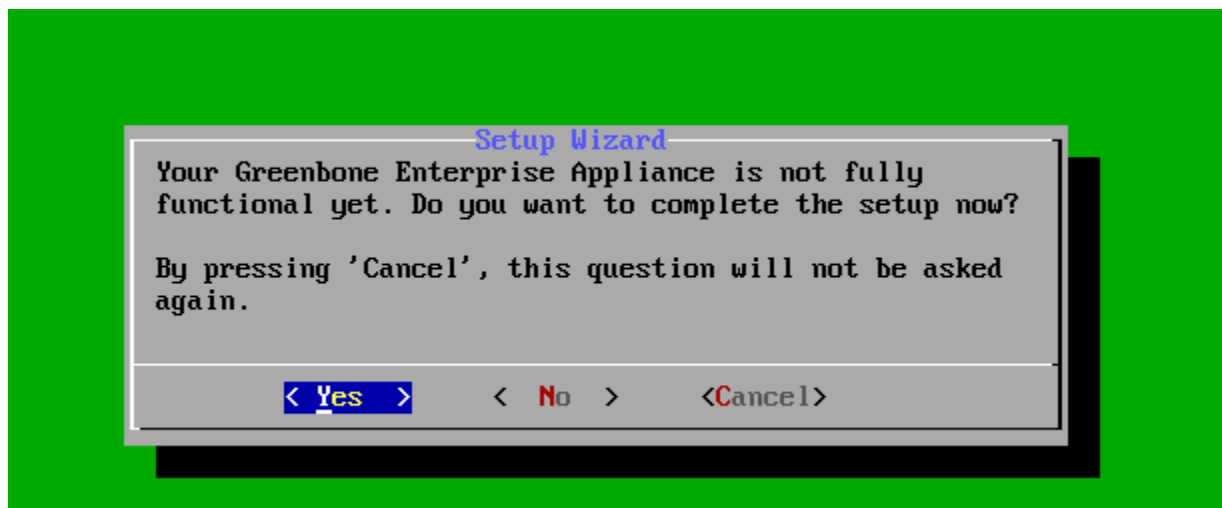
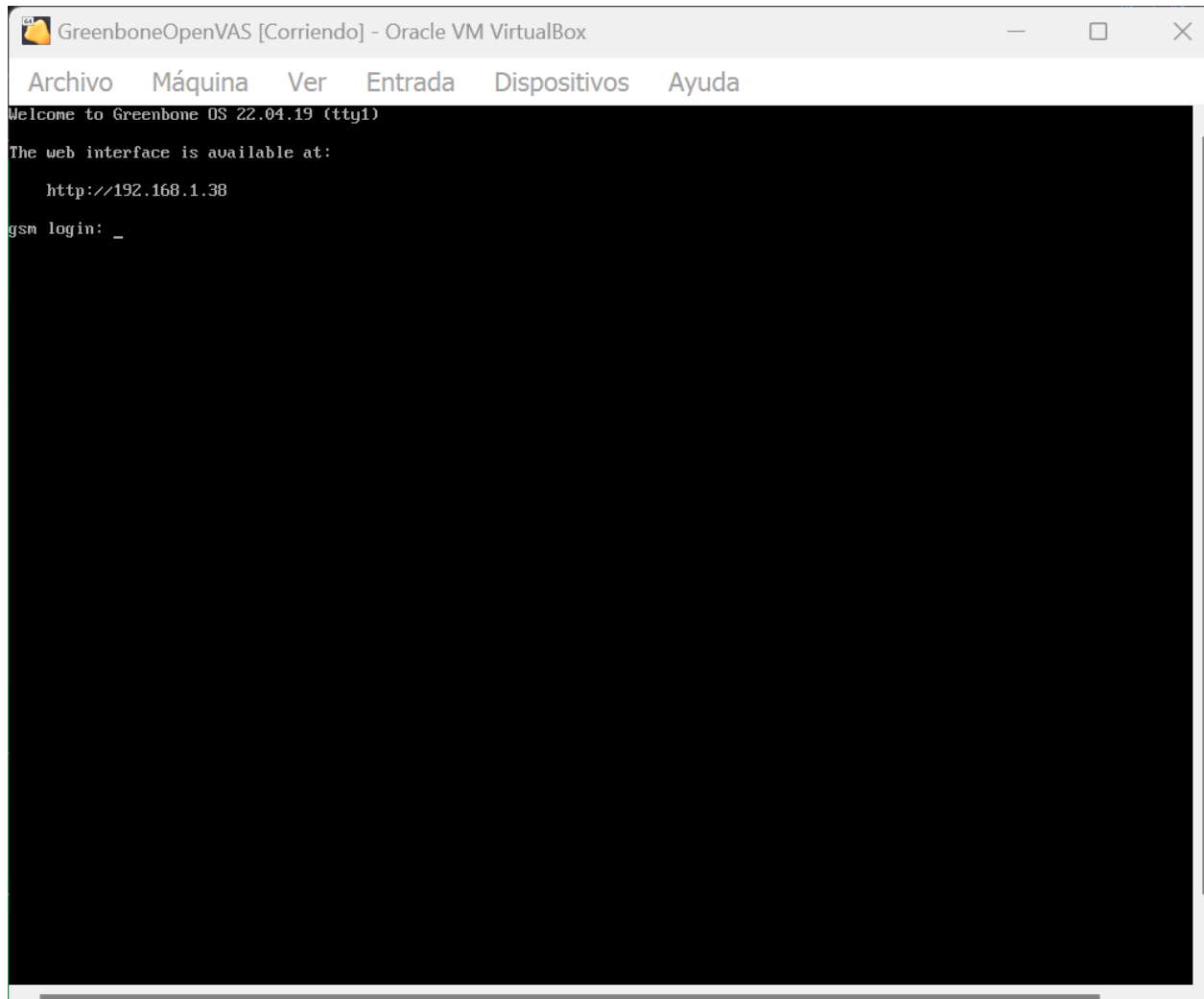


En nuestro caso para el ejercicio le dimos 5g de RAM y 70gb de disco duro.

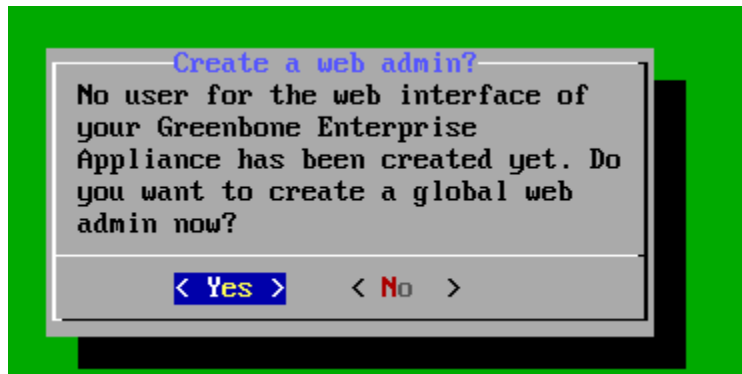


Ajustamos el controlador gráfico para que esté en VMSVGA.

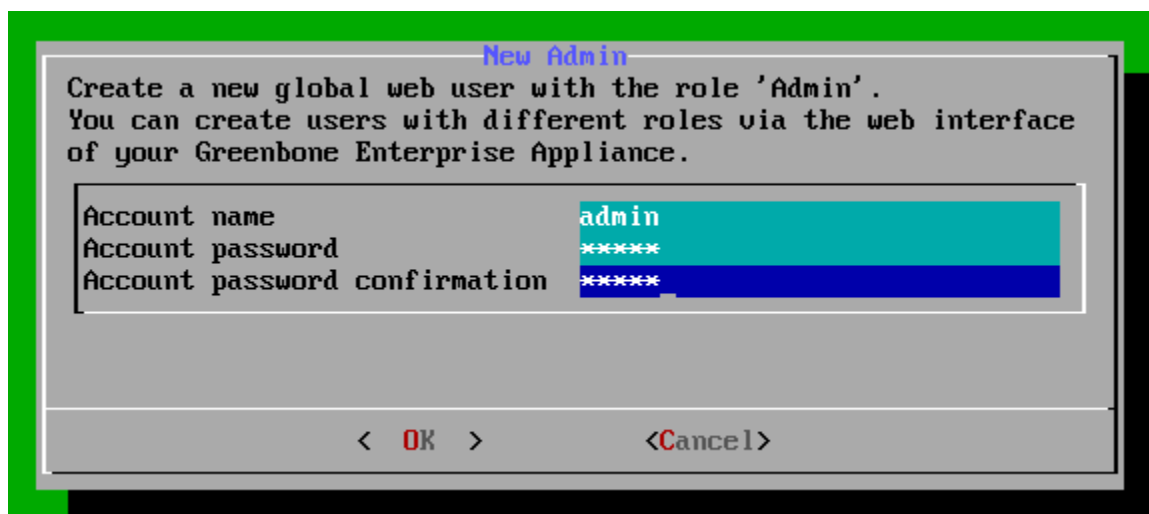
Ahora pasaremos a la instalación de OpenVAS. Arrancamos la máquina y ponemos usuario admin contraseña admin.



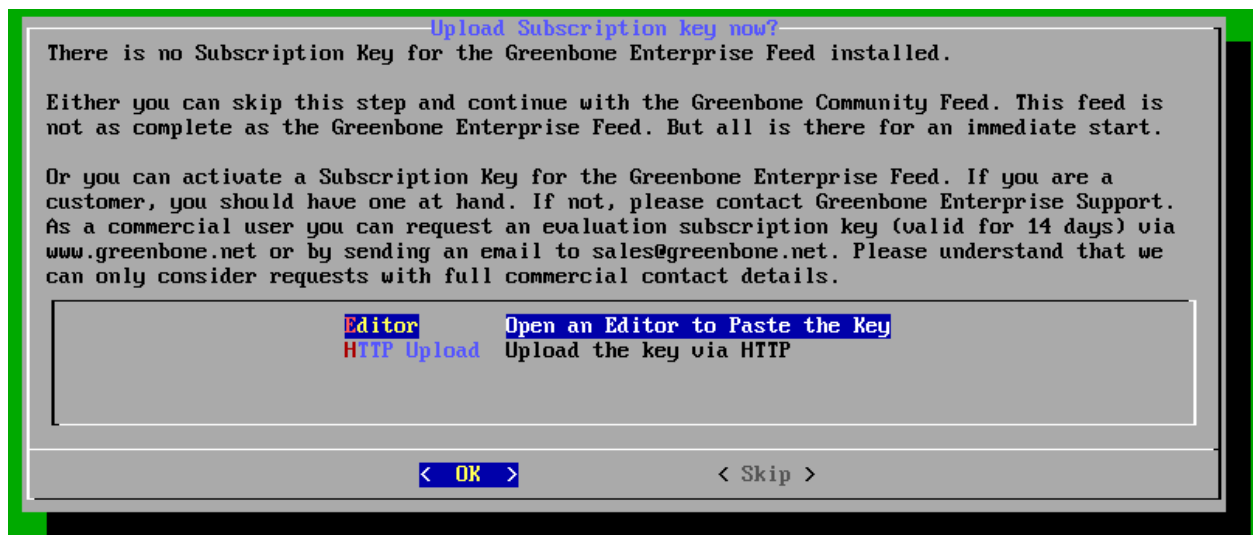
Le damos a Yes. Y nos pedirá crear un usuario.



Creamos usuario admin.

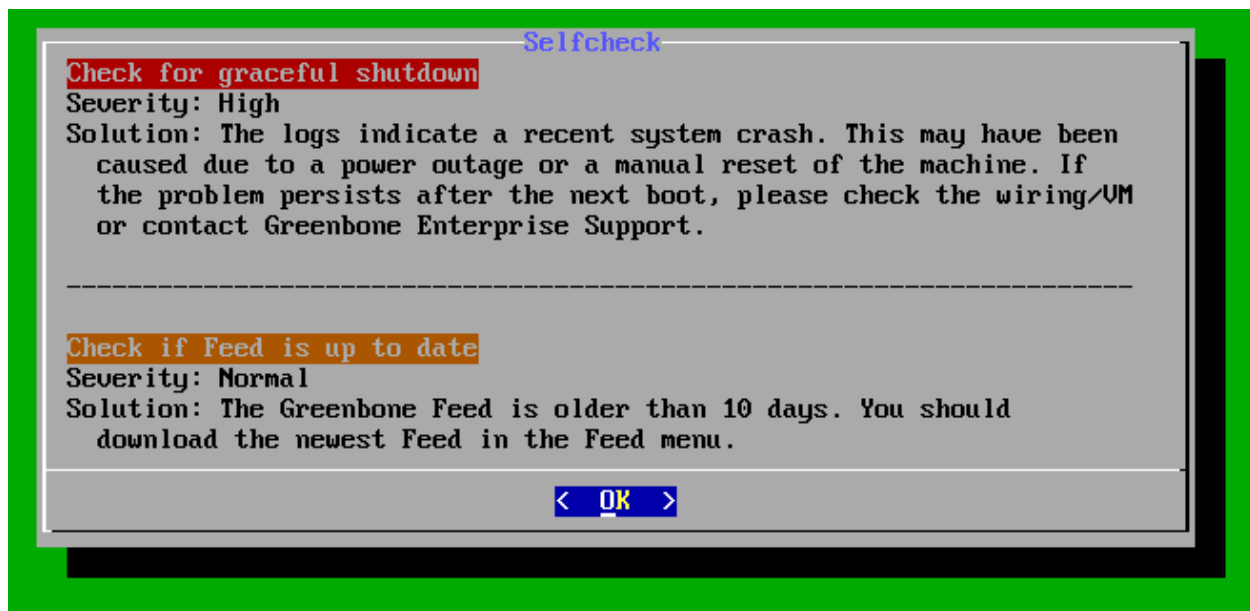


Nos pedirá Subscription Key, no la tenemos entonces le daremos a 'skip'.

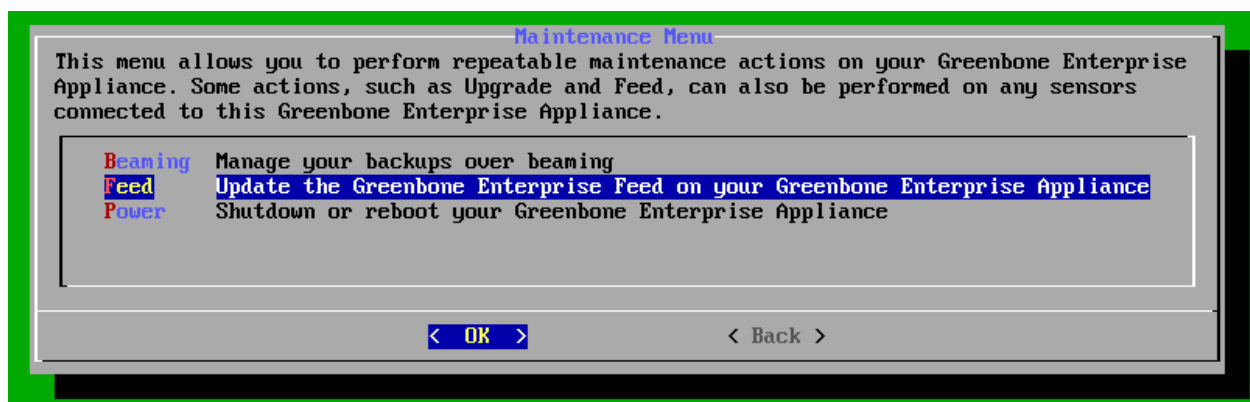
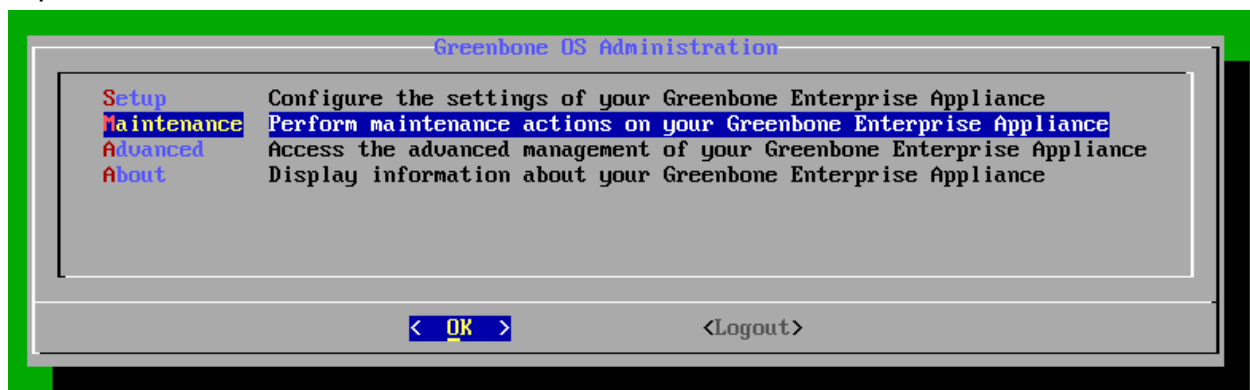




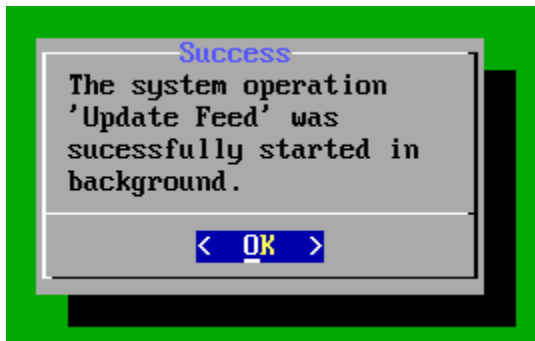
A continuación nos muestra un autochequeo que se realiza esta máquina.



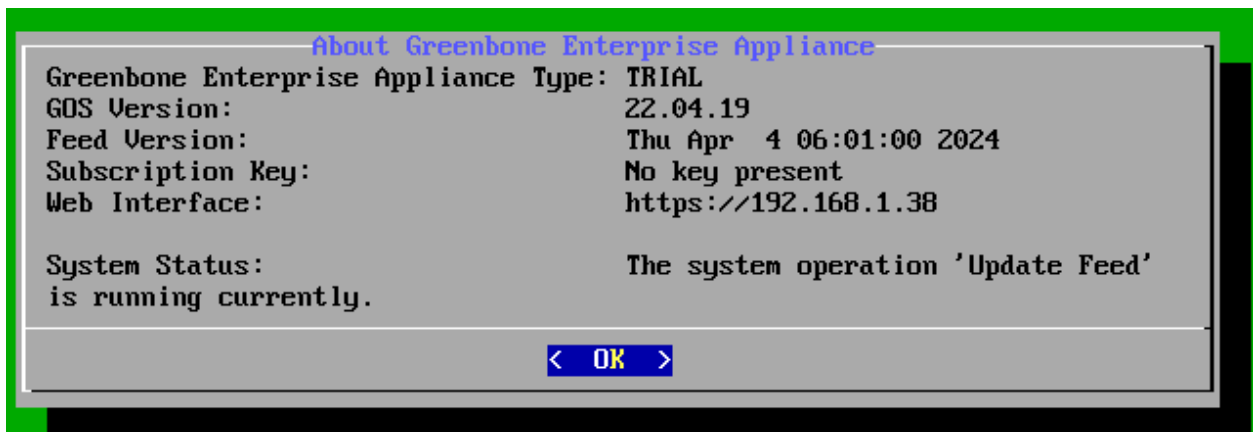
Ahora iremos a Maintenance y actualizaremos el Feed, que es la base de datos donde está almacenada toda la información sobre vulnerabilidades, exploits, amenazas y es muy importante tenerla actualizada.



Este proceso se queda funcionando en Background, quiere decir que no lo vemos pero que se está actualizando.

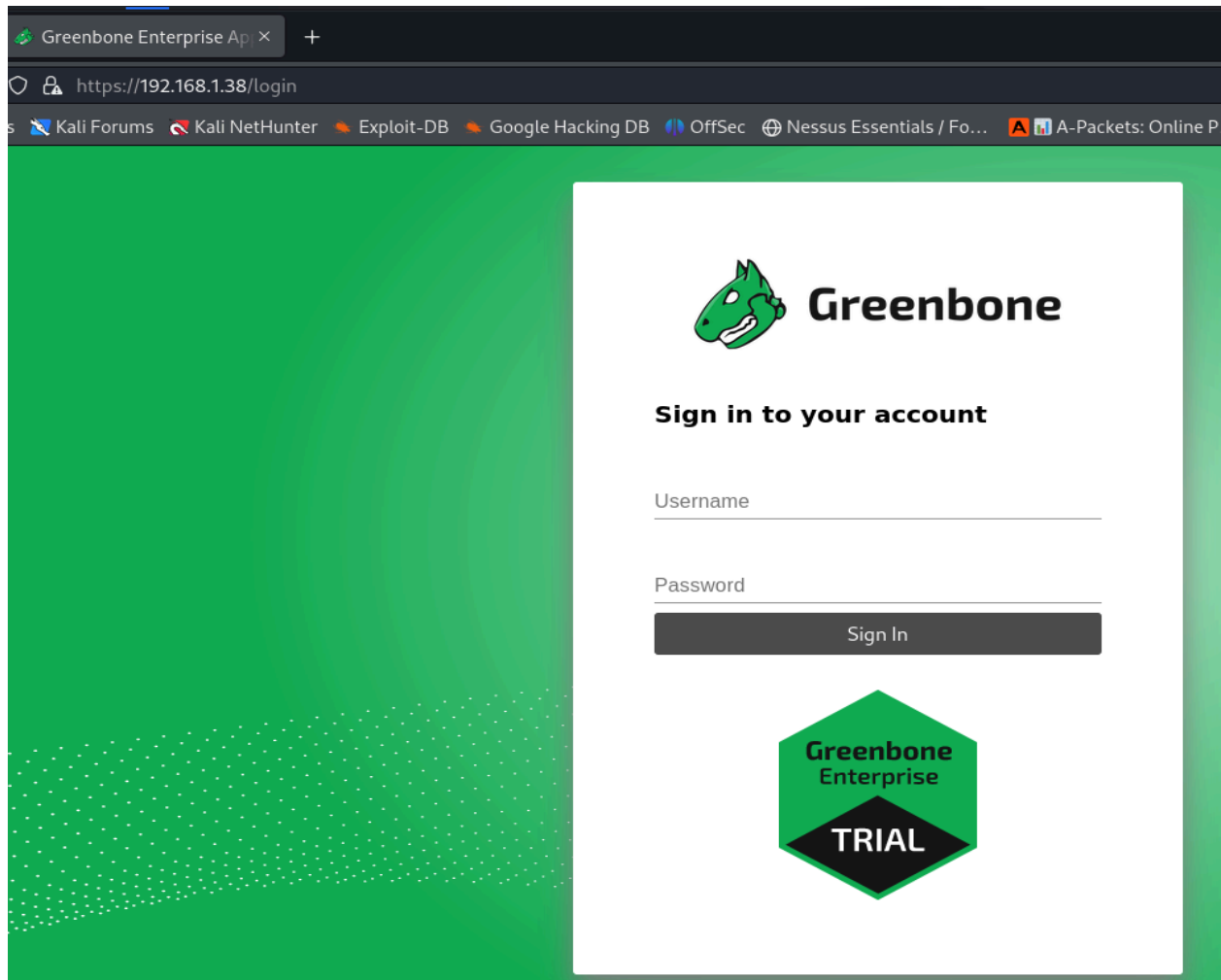


Ahora volveremos atrás e iremos a About Display Information y luego esto nos dará la IP de la máquina que creamos y accederemos a ella desde nuestro Kali Linux.

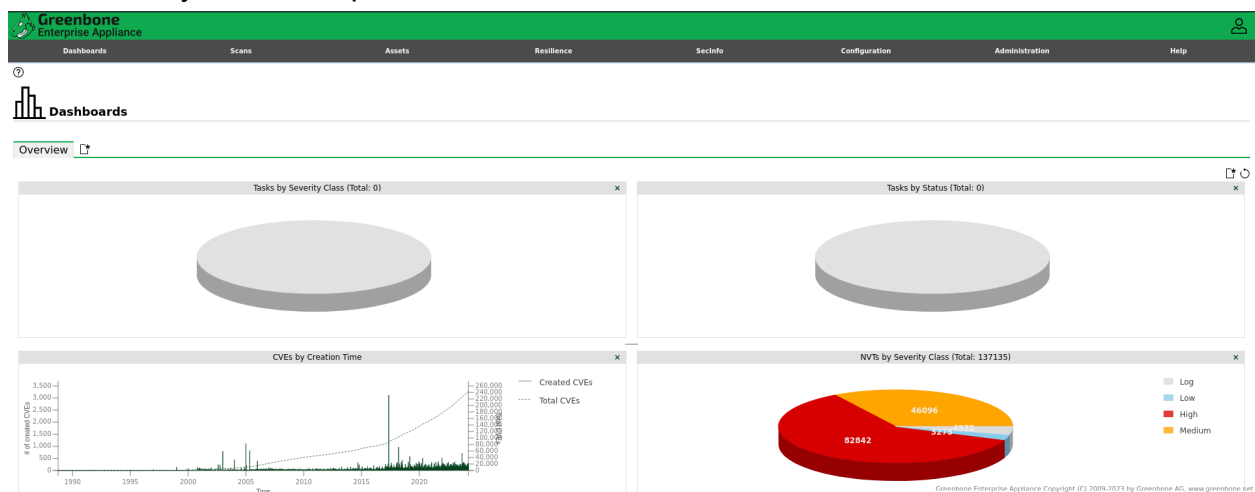


## Configuración de Greenbone OpenVAS para análisis de vulnerabilidades

Entramos a la IP 192.168.1.38 en nuestro navegador de Kali Linux y nos pedirá información de Log in, pondremos admin admin nuevamente.

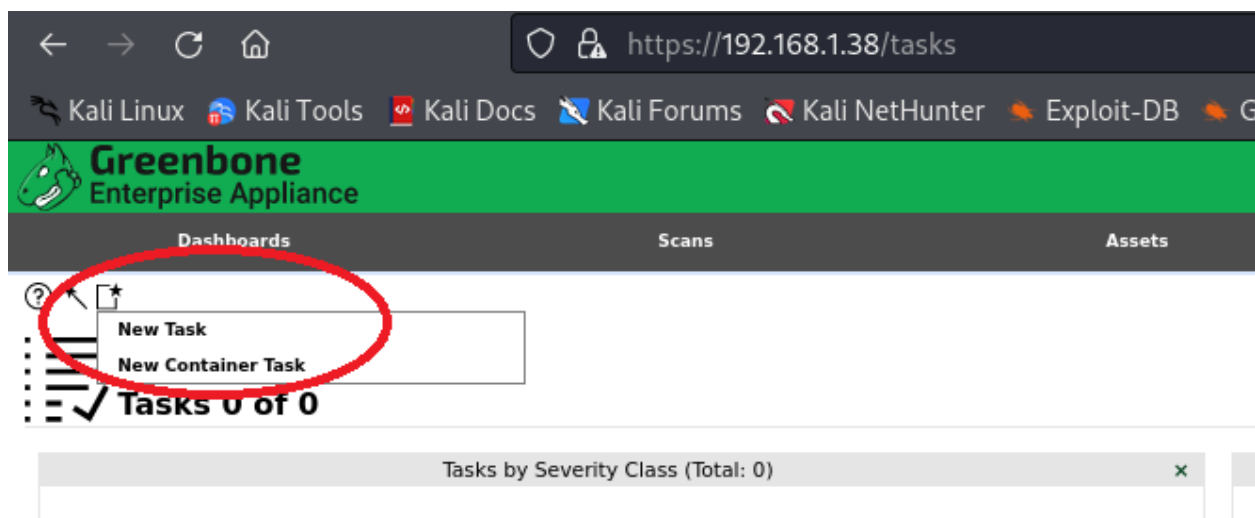


Accedemos y esta es la pantalla inicial.



## Realización de un Análisis de Vulnerabilidades con OpenVAS

Ahora vamos a configurar el análisis, para ello vamos a la pestaña Scans y veremos la opción New task.



Dentro de este apartado nos pedirá el objetivo al cual queremos realizar el análisis.

En nuestro caso lo haremos sobre nuestra máquina de Kali Linux.

New Task

Name

Nuestra máquina de Kali Linux

Comment

Haremos un análisis de vulnerabilidades sobre nuestra máquina de Kali Linux

Scan Targets

Add results to Assets

☒ Yes ☐ No

Apply Overrides

☒ Yes ☐ No

Min QoD

70 %

Alterable Task

☐ Yes ☒ No

Auto Delete Reports

☒ Do not automatically delete reports  
☐ Automatically delete oldest reports but always keep newest 

0

 reports

Scanner

OpenVAS Default

Scan Config

Full and fast

Order for target hosts

Sequential

Maximum concurrently executed NVTs per host

4

Cancel

Save

New Target

Name

Kali Linux

Comment

Hosts

☒ Manual 

192.168.56.109

  
☐ From file 

Browse...

 No file selected.

Exclude Hosts

☒ Manual   
☐ From file 

Browse...

 No file selected.

Allow simultaneous scanning via multiple IPs

☒ Yes ☐ No

Port List

All IANA assigned TCP

Alive Test

Scan Config Default

Credentials for authenticated checks

SSH

--

on port

22

SMB

--

ESXi

--

SNMP

--

Reverse Lookup Only

☐ Yes ☒ No

Reverse Lookup Unify

☐ Yes ☒ No

Cancel

Save

Le debemos dar la IP de nuestra máquina de Kali Linux.

Ahora ya tenemos configurado el análisis y lo podemos ver creado en el panel.

Name	Status	Reports	Last Report	Severity	Trend	Actions
Kali Linux (Análisis sobre nuestra máquina de Kali)	Queued	1				

Target

kali Linux red nat

Scanner

Name

OpenVAS Default

Type

OpenVAS Scanner

Scan Config

Full and fast

Order for target hosts

sequential

Maximum concurrently executed NVTs per host

4

Maximum concurrently scanned hosts

20

Assets

Add to Assets

Yes

Apply Overrides

Yes

Min QoD

70 %

Scan

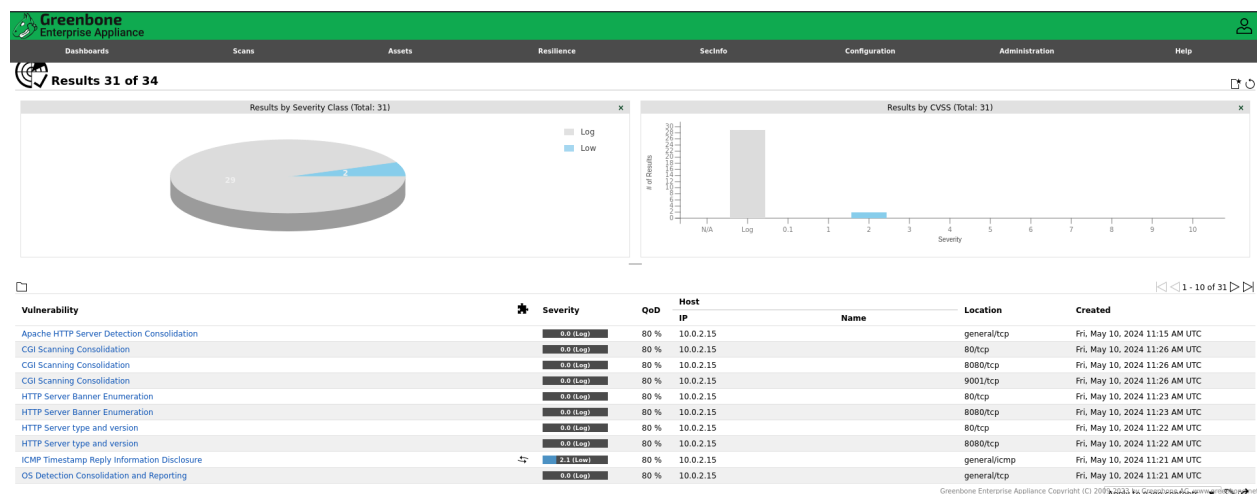
Duration of last Scan

No scans yet

Auto delete Reports

Do not automatically delete reports

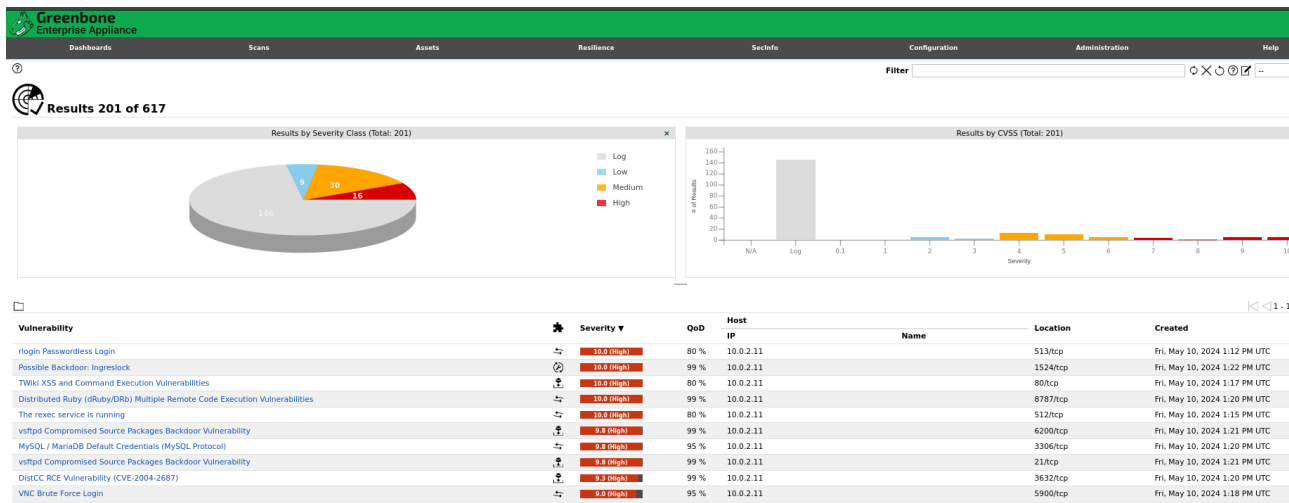
Una vez haya terminado el escaneo podremos ver los resultados de forma legible en la interfaz gráfica.



Podemos observar que no encontró vulnerabilidades, apenas 1 ICMP Timestamp Reply Information Disclosure. Esta vulnerabilidad permite a un atacante obtener información sensible sobre la hora del sistema de un host remoto a través de respuestas ICMP Timestamp, lo que puede facilitar ataques posteriores.

# Análisis sobre máquina de Metasploitable

Para hacer un análisis más exhaustivo, pondremos como objetivo la máquina de Metasploitable que tenemos también en nuestro laboratorio de VirtualBox. Seguiremos los mismos pasos que con nuestra máquina de Kali Linux. A continuación podemos ver que la cantidad de vulnerabilidades encontradas es mucho mayor.



Si abrimos la vulnerabilidad específica nos brinda mayor información sobre la misma.



# Conclusiones

Durante la realización de esta práctica de introducción a Greenbone OpenVAS, hemos explorado los fundamentos de esta poderosa herramienta de evaluación de vulnerabilidades. A través de la instalación y configuración de OpenVAS en una máquina virtual, hemos adquirido experiencia práctica en su uso, lo que nos ha permitido comprender mejor su funcionamiento y su papel en la evaluación de la seguridad de los sistemas de información.

Al seguir los pasos detallados para la preparación del entorno virtual, la descarga e instalación de OpenVAS, y la realización de un análisis de vulnerabilidades, hemos sido capaces de identificar y comprender los procesos clave involucrados en la ejecución de escaneos de seguridad y la interpretación de los resultados obtenidos. Esto nos ha proporcionado una valiosa experiencia práctica que podemos aplicar en entornos reales para mejorar la postura de seguridad de las organizaciones.

Además, al enfrentarnos a la detección de una vulnerabilidad específica, como ICMP Timestamp Reply Information Disclosure, hemos aprendido sobre la importancia de la identificación y comprensión de las vulnerabilidades reportadas, así como sobre las posibles implicaciones para la seguridad de los sistemas. Esta experiencia nos ha sensibilizado sobre la necesidad de mantenernos actualizados sobre las amenazas y vulnerabilidades emergentes, y nos ha motivado a seguir explorando y aprendiendo en el campo de la ciberseguridad.

Esta práctica nos ha brindado una valiosa introducción a Greenbone OpenVAS y nos ha equipado con los conocimientos y habilidades necesarios para utilizar esta herramienta de manera efectiva en la evaluación y mejora de la seguridad de los sistemas de información, contribuyendo así a fortalecer la resiliencia de las organizaciones ante las crecientes amenazas cibernéticas.