

Actividad 2

INTRODUCCIÓN A GREENBONE OPENVAS

Miquel Rodríguez González

5 de mayo de 2024



Greenbone

Qué es greenbone

Greenbone Security Assistant (GSA) es una interfaz web de código abierto que forma parte del proyecto OpenVAS (Open Vulnerability Assessment System). OpenVAS es un marco de software libre que aporta herramientas de evaluación de vulnerabilidades que se utiliza para escanear redes y sistemas en busca de posibles vulnerabilidades de seguridad.

Índice

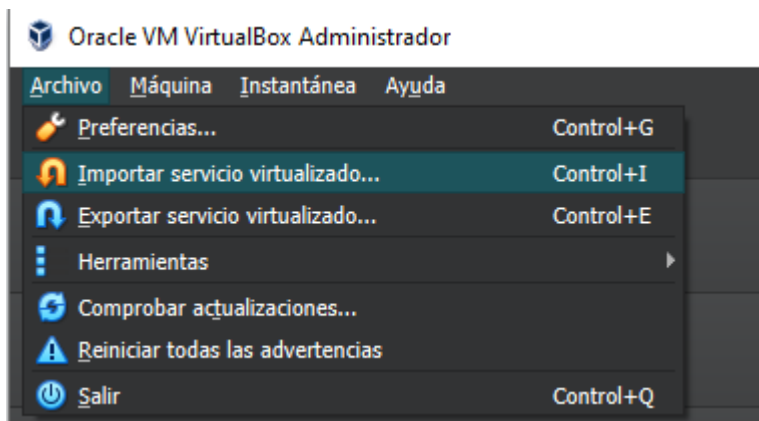
1- Preparación.....	3
2- Configuración de la máquina virtual.....	3
3- Instalación de greenBone.....	4
4- configuración de greenbone.....	6
4.1- configuración de IPs.....	6
4.2- Actualización de BBDD de Greenbone.....	8
5- Acceder a la web de Greenbone.....	9
6- Creación de una tarea.....	10

1- Preparación

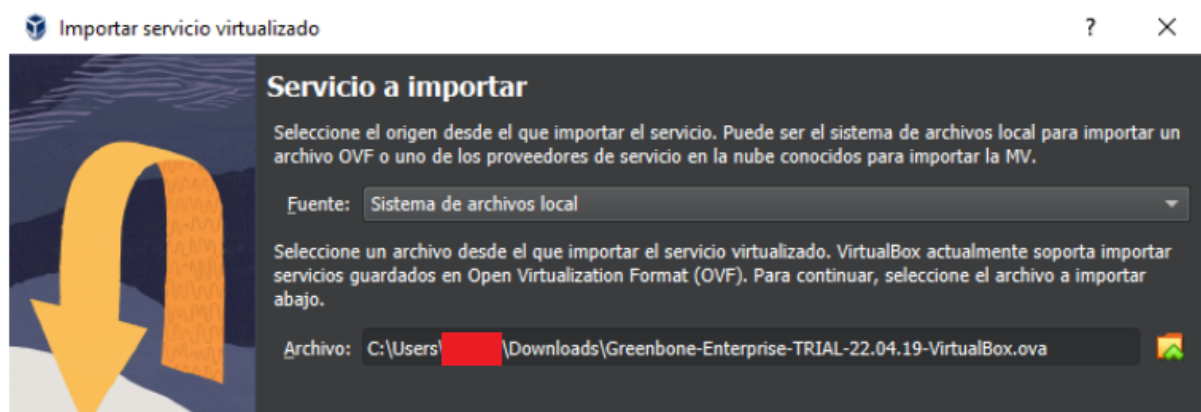
- tener un programa de virtualización
- descargar la ova de Greenbone <https://www.greenbone.net/en/testnow/>

2- Configuración de la máquina virtual

En VM debemos importar la ova a través de **Archivo/Importar** servicio virtualizado



seleccionamos la ova

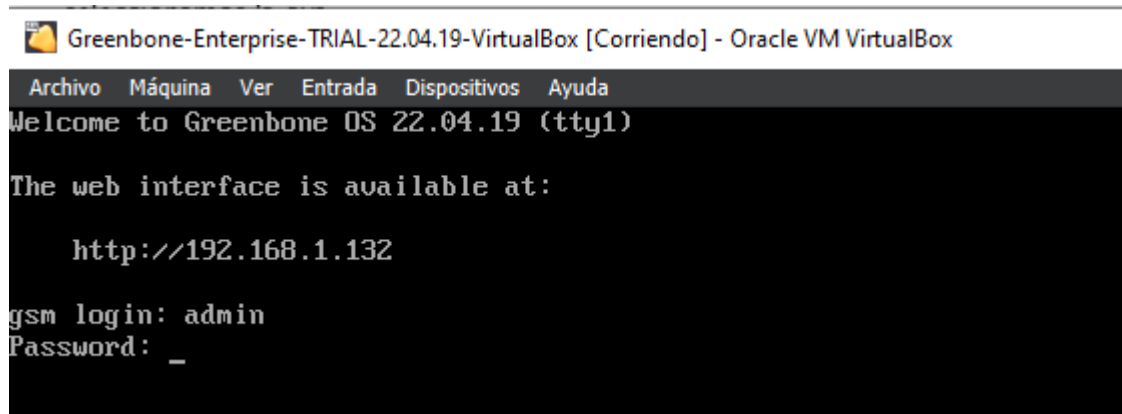


Y al final la importación la Iniciamos

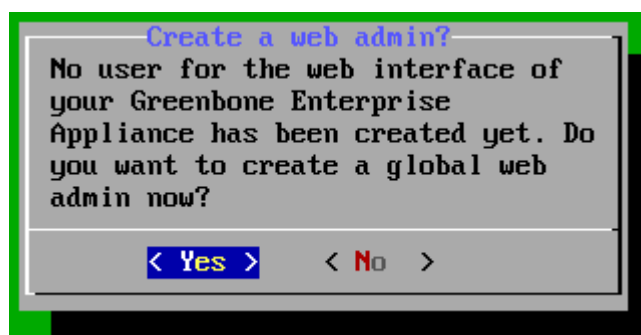
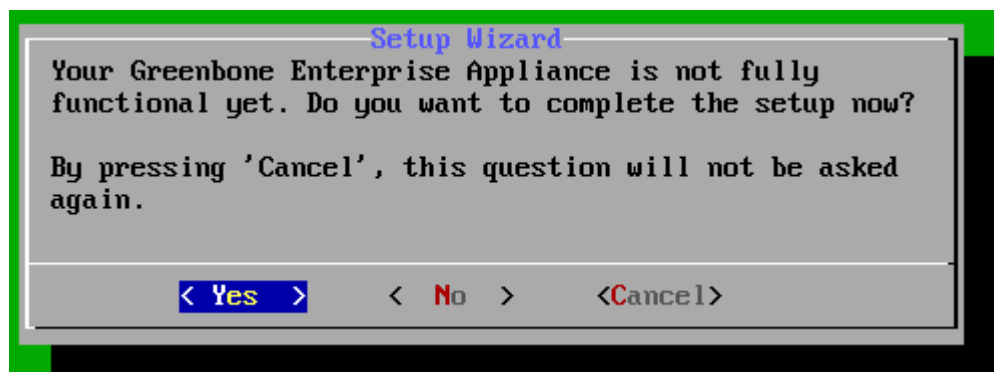
3- Instalación de greenBone

Al iniciar Greenbone nos encontraremos en la siguiente pantalla. Para poder acceder utilizaremos el usuario y contraseña por defecto

user: admin **password: admin**



Vamos siguiendo las instrucciones para hacer su configuración



Añadimos nuevo usuario y contraseñas

New Admin

Create a new global web user with the role 'Admin'.
You can create users with different roles via the web interface
of your Greenbone Enterprise Appliance.

Account name	admin
Account password	*****
Account password confirmation	*****

< OK > <Cancel>

Success

User created.

< OK >

En el siguiente paso nos pide una clave de suscripción, si no tenemos ninguna tenemos que hacer skip

Upload Subscription key now?

There is no Subscription Key for the Greenbone Enterprise Feed installed.

Either you can skip this step and continue with the Greenbone Community Feed. This feed is not as complete as the Greenbone Enterprise Feed. But all is there for an immediate start.

Or you can activate a Subscription Key for the Greenbone Enterprise Feed. If you are a customer, you should have one at hand. If not, please contact Greenbone Enterprise Support. As a commercial user you can request an evaluation subscription key (valid for 14 days) via www.greenbone.net or by sending an email to sales@greenbone.net. Please understand that we can only consider requests with full commercial contact details.

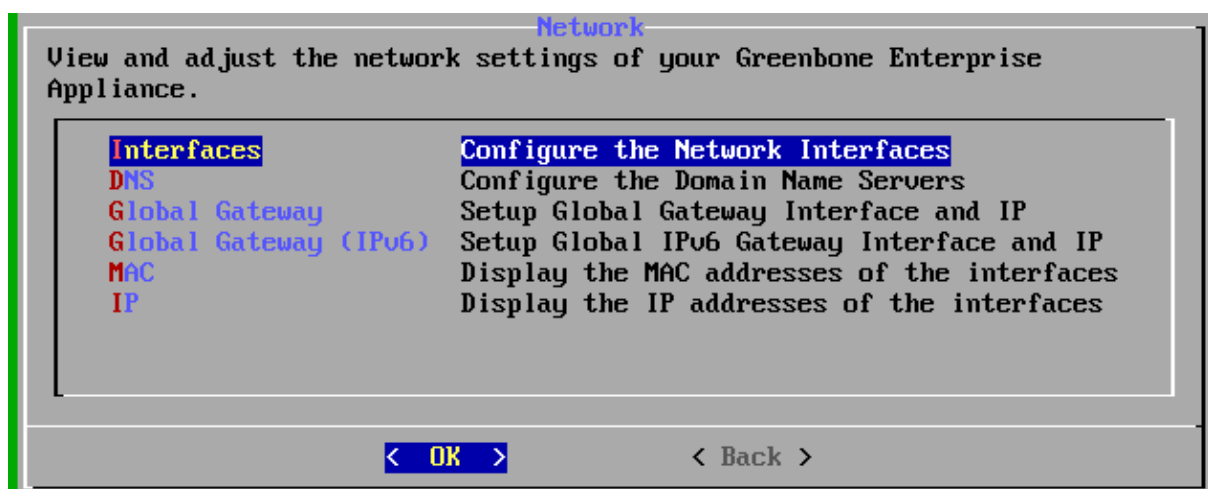
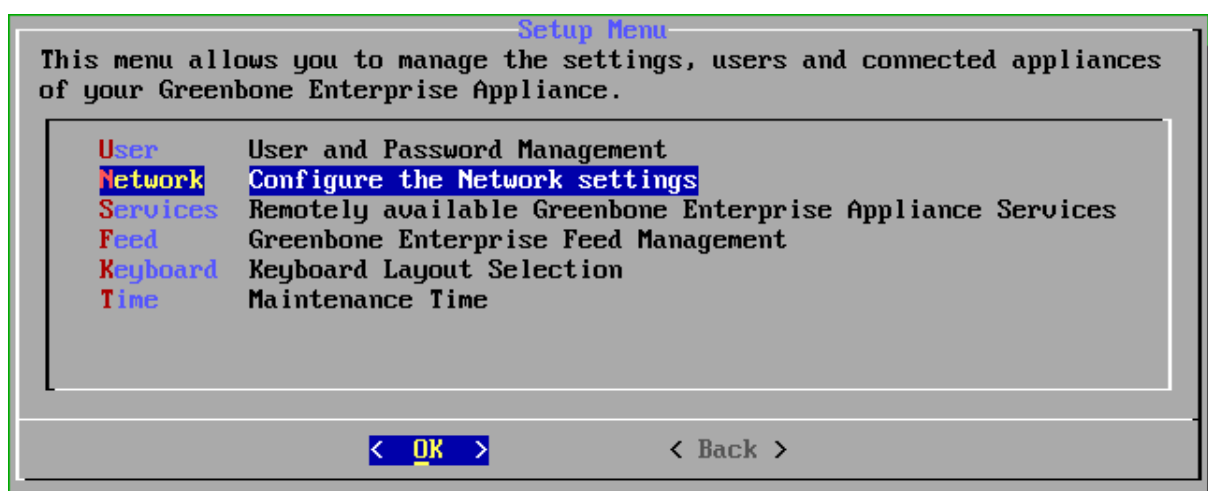
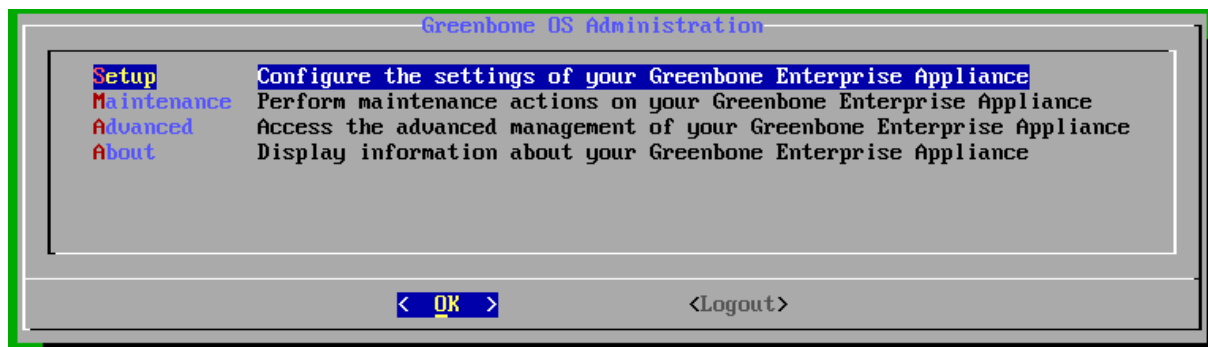
Editor	Open an Editor to Paste the Key
HTTP Upload	Upload the key via HTTP

< OK > < Skip >

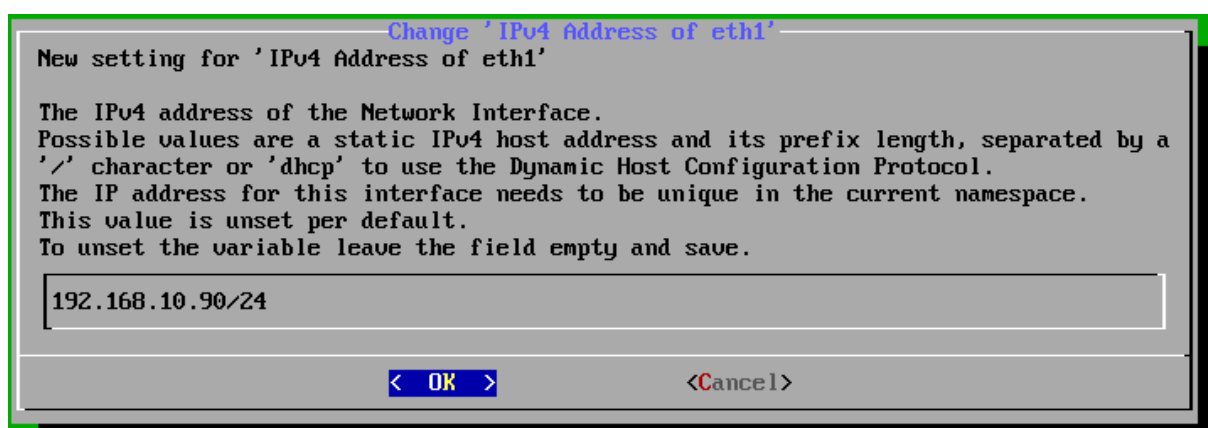
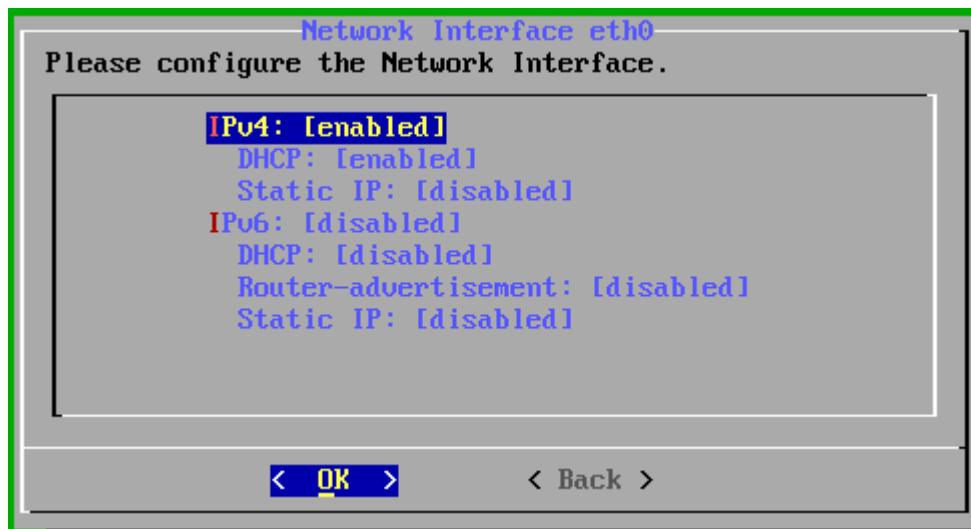
4- configuración de greenbone

4.1- configuración de IPs

Podemos acceder a la configuración de ips para darle una estática o cambiarla. lo haremos a través de **Setup/Network/Interfaces**



Aquí podemos configurar la ip (y poner la máquina en nuestra red interna, en caso necesario)

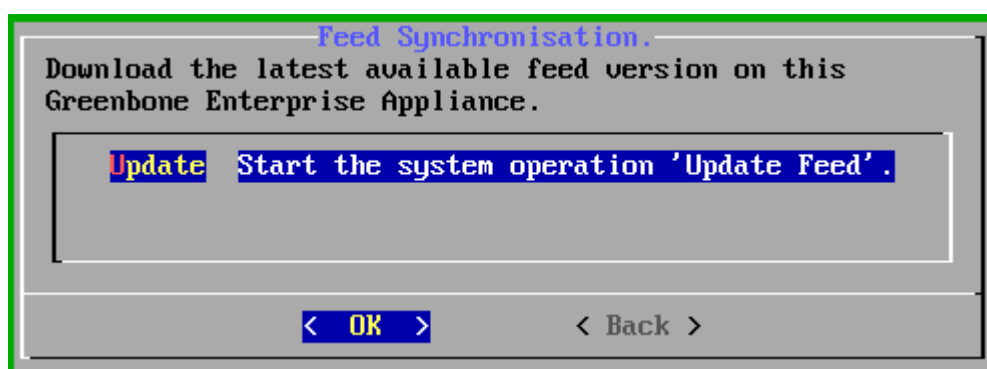
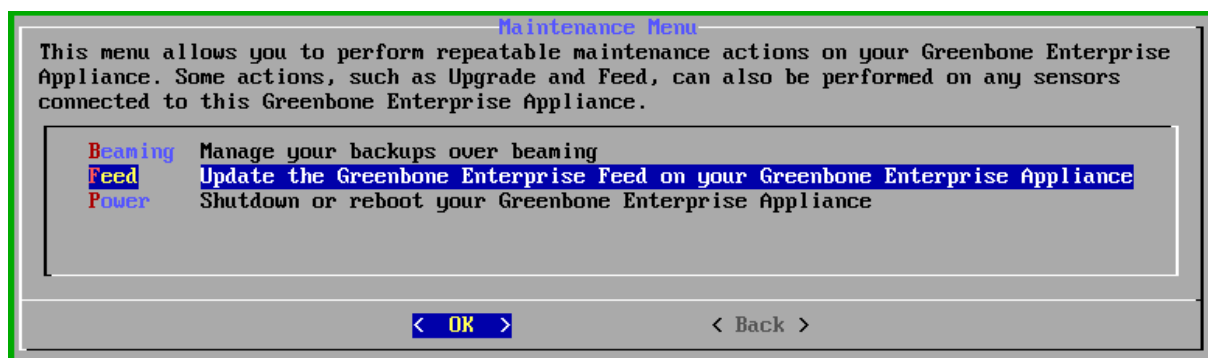
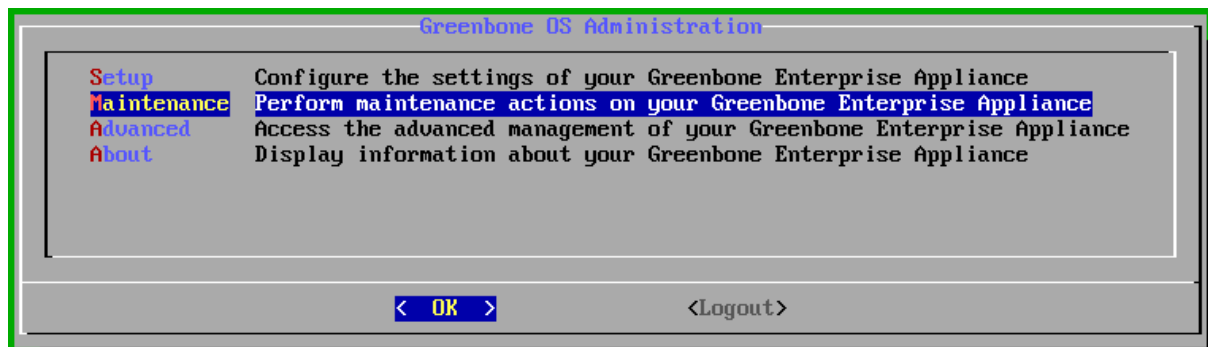


Es importante acordarnos de guardar los cambios siempre que nos lo pida

4.2- Actualización de BBDD de Greenbone

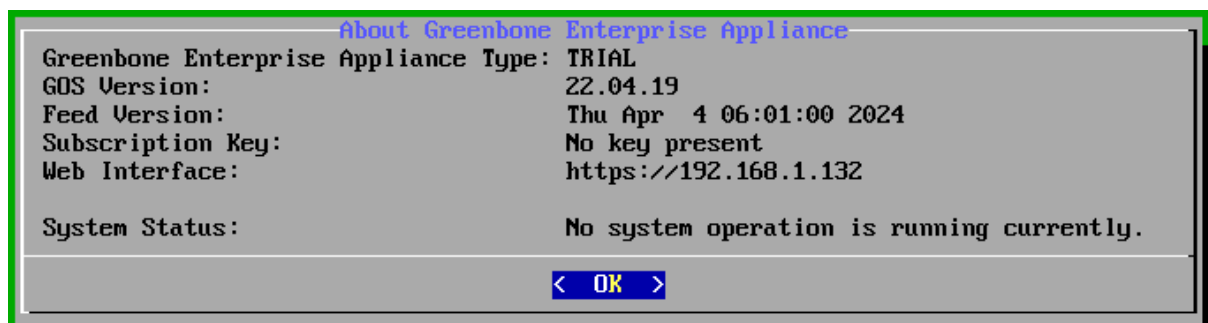
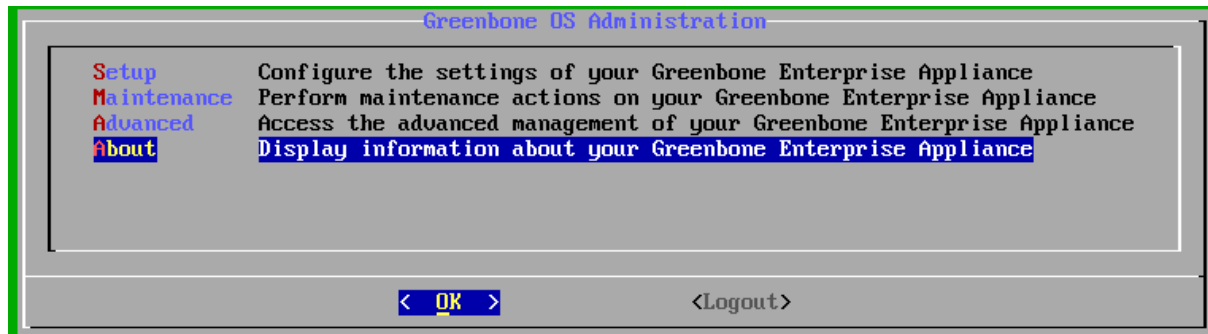
Siguiendo los siguientes pasos podemos actualizar la base de datos de amenazas de Greenbone.

Accedemos a **Maintenance/Feed/Update**, la actualización se hará en segundo plano



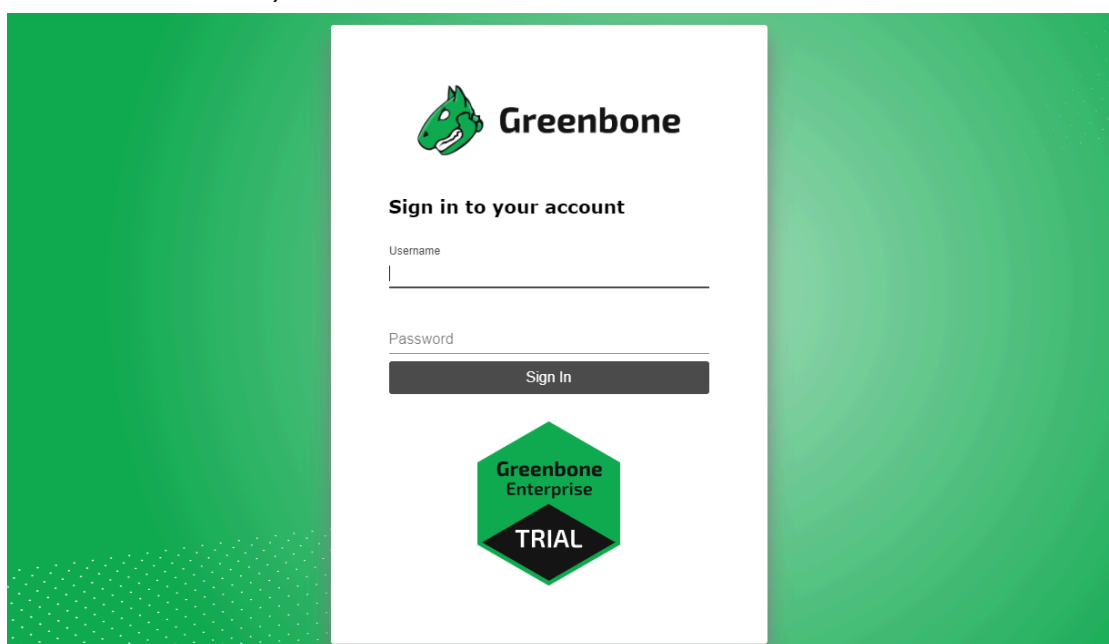
5- Acceder a la web de Greenbone

Para poder acceder a la página web debemos utilizar la IP que encontramos en **About** con el nombre de **Web interface**



Con esta IP solo debemos abrir un navegador desde un equipo que tenga acceso a la red interna y poner la URL indicada.

Una vez entremos nos pedirá usuario y contraseña (serán las por defecto si no se han cambiado): **User: admin** **Password: admin**



6- Creación de una tarea

Para hacer un escaneo primero crearemos un target (opcional) a través de **Configuration/Targets**. Aquí podemos definir sobre qué ordenador/es hacer el escaneo y cómo queremos hacerlo.

En este caso se hará un análisis sobre un kali que se encuentra en la misma red interna.

New Target [X]

Name:

Comment:

Hosts: ☒ Manual
☐ From file Ninguno archivo selec.

Exclude Hosts: ☒ Manual
☐ From file Ninguno archivo selec.

Allow simultaneous scanning via multiple IPs: ☒ Yes ☐ No

Port List: [v] [★]

Alive Test: [v]

Credentials for authenticated checks

SSH: [v] on port [★]

SMB: [v] [★]

Después creamos una task a través de **Scan/tasks**. Aquí podemos escoger el target creado con anterioridad (kali es el nombre del target creado con anterioridad)

New Task

Name

kali

Comment

kali red interna

Scan Targets

kali

▲

✱

Add results to Assets

kali

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

Scanner

OpenVAS Default

▼

Scan Config

Full and fast

▼

Order for target hosts

Sequential

▼

Maximum concurrently executed NVTs per host

4

▲

▼

Cancel

Save

Con la tarea configurada ya la podremos iniciar dándole al botón de pay

Trend Actions

<input type="text" value="Apply to page contents"/> ▼

1 - 1 of 1

Des de **Scan/reports** podem veure com va el escaneig

