

Actividad 2 – Módulo 2

Introducción a Greenbone OpenVAS

Diego Mucci

04/05/2024

Seguridad Informática

Introducción a Greenbone OpenVAS

Greenbone OpenVAS (Open Vulnerability Assessment System) es una solución de software libre para la evaluación de seguridad de redes, que proporciona un escáner de vulnerabilidades completo y un gestor de vulnerabilidades. OpenVAS es reconocido por su capacidad para detectar vulnerabilidades en sistemas y dispositivos de red mediante una amplia base de datos de pruebas de vulnerabilidad actualizada regularmente.

Objetivo de la Actividad

Esta actividad está diseñada como introducción en el proceso de instalación y configuración de Greenbone OpenVAS. Aprenderemos cómo utilizar esta poderosa herramienta para realizar un análisis de vulnerabilidades en un entorno controlado, configurando y ejecutando un escaneo de red.

Pasos de la Actividad

1. Preparación del Entorno Virtual:

- Instalar un software de virtualización, como Oracle VM VirtualBox o VMware Workstation, en tu ordenador.
- Asegurarse de contar con al menos 4 GB de RAM y 40 GB de espacio en disco disponible para la máquina virtual, dado que OpenVAS requiere recursos significativos para operar eficientemente.

Este primer paso lo tenemos ya realizado debido al trabajo previo que venimos haciendo con las máquinas virtuales. Por lo tanto, el entorno virtual está correcto. En mi caso uso un Windows 10, así que me descargué Oracle VM VirtualBox para Windows 10 en su momento.

2. Descarga e Instalación de Greenbone OpenVAS:

- Visitar la página oficial de Greenbone Security (<https://www.greenbone.net>) y descargar la imagen de Greenbone Security Manager TRIAL (GSM TRIAL), que incluye OpenVAS, o en su defecto la OVA que importaremos en el hypervisor de máquinas virtuales.



Greenbone

Greenbone Cloud Service TRIAL Greenbone Enterprise TRIAL Buy Here Contact Blog  

Products Cyber Resilience Customer Services About Greenbone 

VMware Workstation Player/Pro

1. Instruction

2. Note

3. Download

Here you can download the Greenbone Enterprise TRIAL and use it for free:

[Download for VMware Workstation Player/Pro now](#)

Version:
22.04.19

SHA256 checksum:
c5902fbc862f6ae09f1c3d80b7ffe3451c82315f54c6fd1324c398ae
aaffed73

Oracle VirtualBox

1. Instruction

Requirements

- Compatibility: Oracle VirtualBox 6.1 or higher
- Minimum requirements: 2 CPUs, 5 GB RAM
- Virtual network adapter with direct Internet connection

Note: With default settings, the Greenbone Enterprise TRIAL uses bridged networking and expects an IP address from a DHCP server. This may be reconfigured.

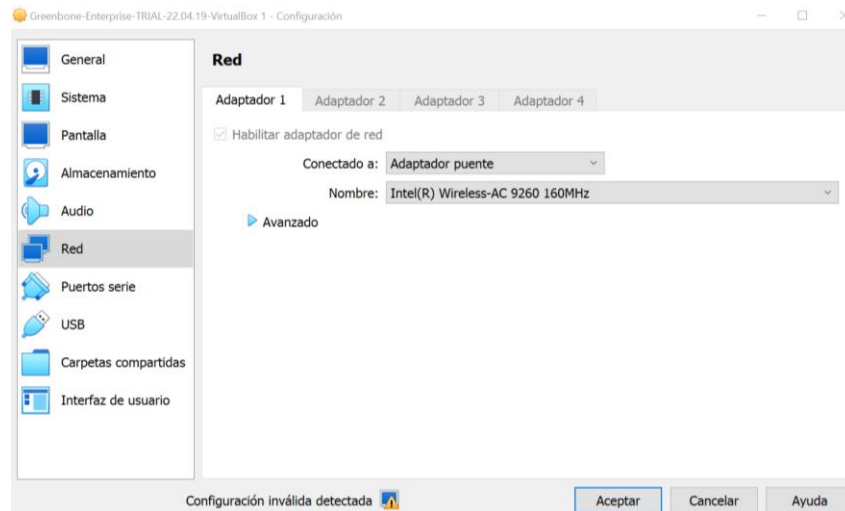
Importing the Greenbone Enterprise TRIAL

1. [Download](#) the OVA file of the Greenbone Enterprise TRIAL.

- Crear una nueva máquina virtual utilizando la imagen descargada y configurarla siguiendo las instrucciones específicas para la instalación.

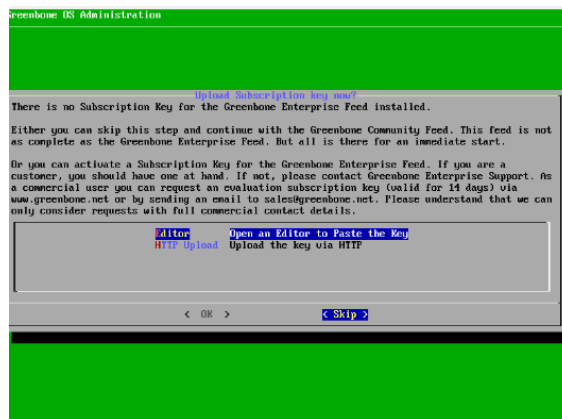
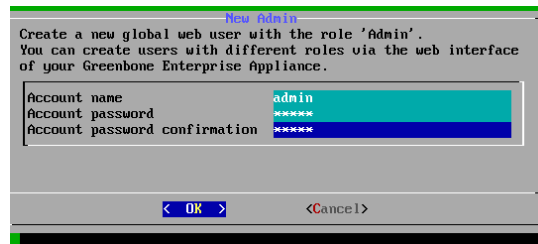
En VirtualBox vamos a archivo, importar servicio virtualizado, seleccionamos la OVA que nos hemos descargado anteriormente



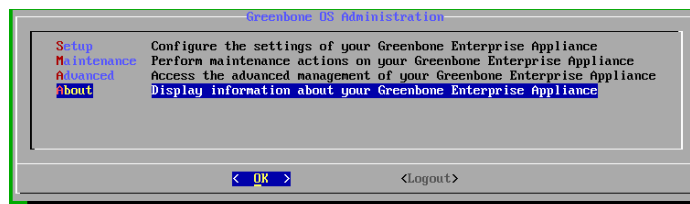


En configuración de red seleccionamos Adaptador puente.

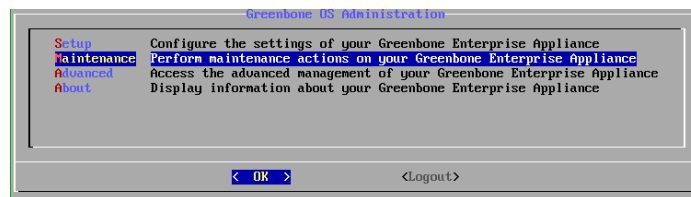
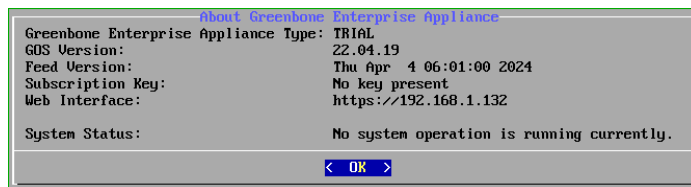
Iniciamos la máquina virtual e introducimos admin tanto para usuario como para la contraseña que nos pide.



En este paso seleccionamos skip



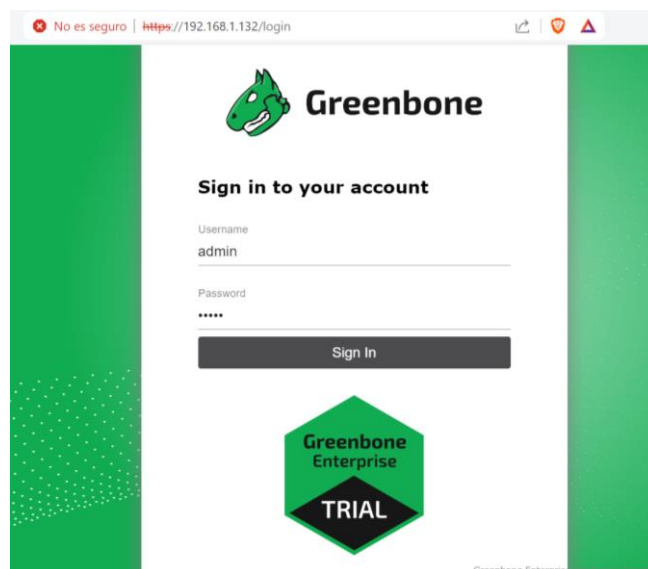
Seleccionamos *about* para saber la IP de Greenbone y esta la introduciremos en el navegador de mi ordenador físico porque estamos trabajando en nuestra red física.



Para apagar la máquina lo haremos siempre desde el menú de mantenimiento y nunca de un modo brusco.

3. Configuración Inicial de OpenVAS:

- Acceder a la consola de administración de OpenVAS a través de la interfaz web proporcionada, usando la dirección IP asignada a la máquina virtual.



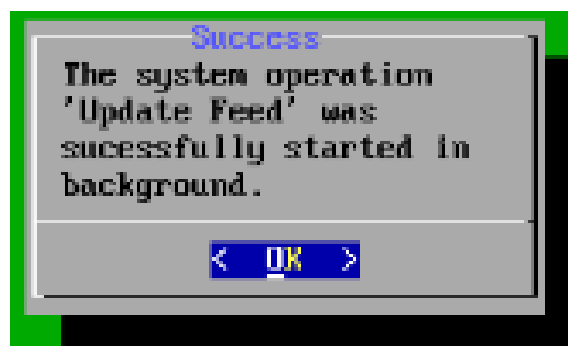
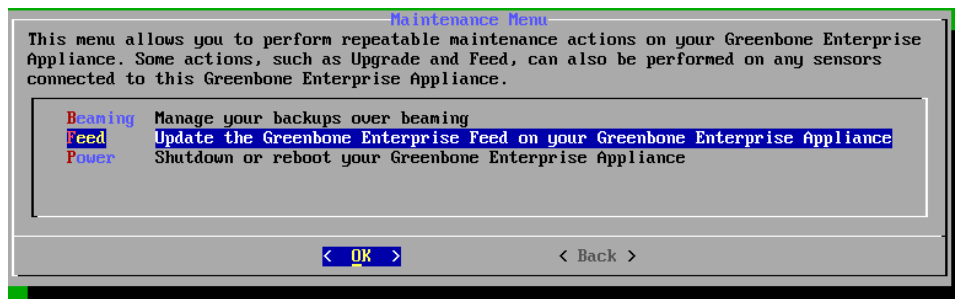
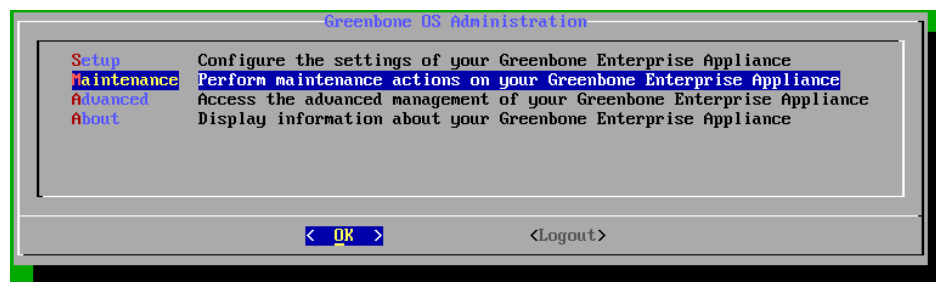
Introducimos *admin* tanto para el usuario como para la contraseña.

- Realizar la configuración inicial, incluyendo la configuración de la red y la actualización de la base de datos de vulnerabilidades para asegurar que el sistema está actualizado.

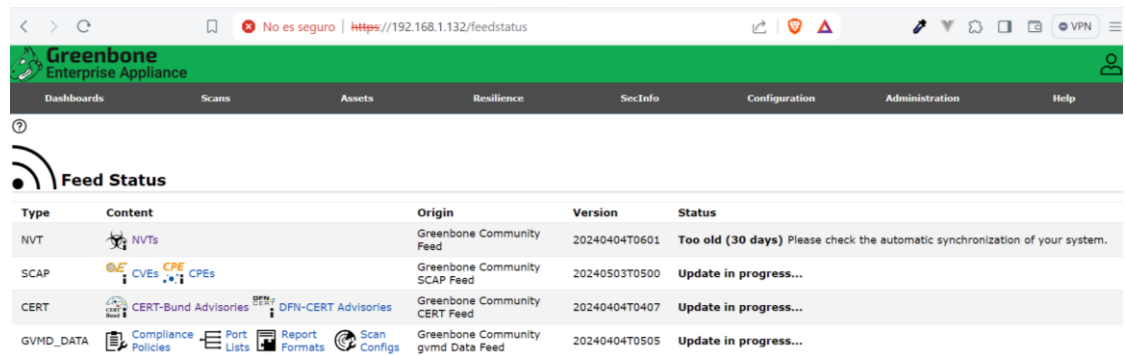
Si vamos al apartado de Adeministration – Feed Status veremos que nos aparecen las siguientes bases de datos como demasiado antiguas (30 días).

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20240404T0601	Too old (30 days) Please check the automatic synchronization of your system.
SCAP	CVEs CPE CPEs	Greenbone Community SCAP Feed	20240404T0500	Too old (30 days) Please check the automatic synchronization of your system.
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone Community CERT Feed	20240404T0407	Too old (30 days) Please check the automatic synchronization of your system.
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Community gvmd Data Feed	20240404T0505	Too old (30 days) Please check the automatic synchronization of your system.

Para actualizarlas tendremos que ir a la máquina virtual y seleccionar *Maintenance – Feed – Update*.



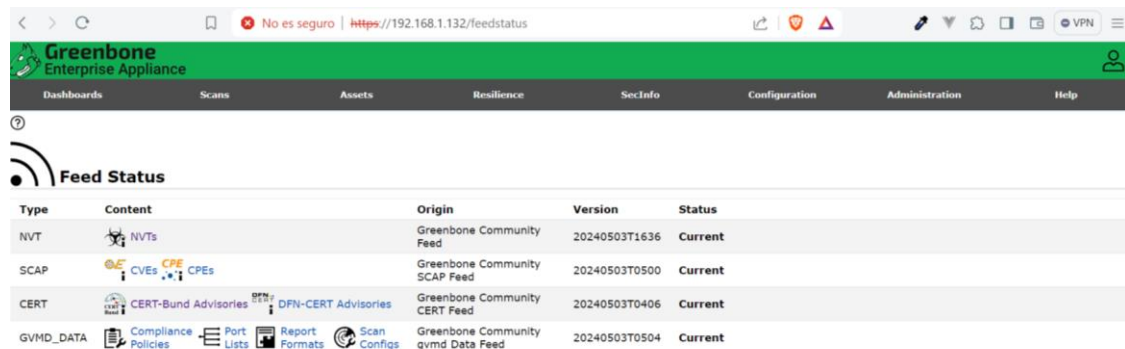
Ahora si volvemos al *Feed Status* veremos como la actualización se está realizando.



The screenshot shows the Greenbone Enterprise Appliance interface. The top navigation bar includes: Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. The main section is titled "Feed Status" and contains a table with the following data:

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20240404T0601	Too old (30 days) Please check the automatic synchronization of your system.
SCAP	CVEs, CPEs	Greenbone Community SCAP Feed	20240503T0500	Update in progress...
CERT	CERT-Bund Advisories, DFN-CERT Advisories	Greenbone Community CERT Feed	20240404T0407	Update in progress...
GVMD_DATA	Compliance Policies, Port Lists, Report Formats, Scan Configs	Greenbone Community gvmd Data Feed	20240404T0505	Update in progress...

Esta actualización puede tardar varios minutos. Una vez finalice, volvemos a entrar y vemos que el estado de todas ellas ha cambiado, ahora aparece como "current".



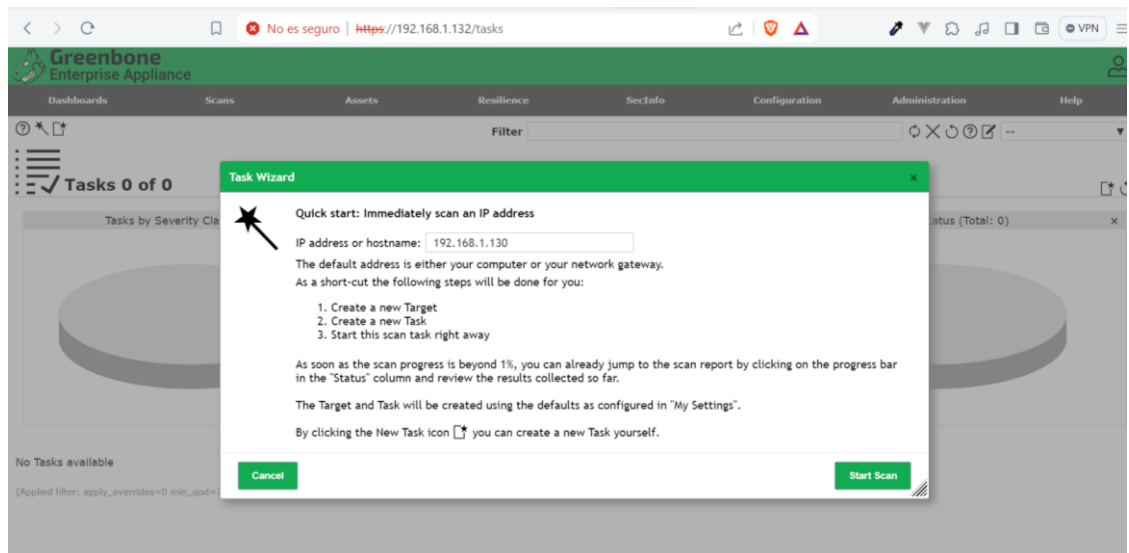
The screenshot shows the Greenbone Enterprise Appliance interface after the update. The top navigation bar is the same. The main section is titled "Feed Status" and contains a table with the following data:

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20240503T1636	Current
SCAP	CVEs, CPEs	Greenbone Community SCAP Feed	20240503T0500	Current
CERT	CERT-Bund Advisories, DFN-CERT Advisories	Greenbone Community CERT Feed	20240503T0406	Current
GVMD_DATA	Compliance Policies, Port Lists, Report Formats, Scan Configs	Greenbone Community gvmd Data Feed	20240503T0504	Current

4. Realización de un Análisis de Vulnerabilidades:

- Configurar un objetivo de escaneo dentro de la red de la máquina virtual o una dirección IP específica designada para pruebas.

Si seleccionamos *Scans* y luego clicamos en el icono de la varita mágica (*Task Wizard*) automáticamente va a detectar la IP del equipo sobre el cual está trabajando, en este caso la de mi ordenador físico. Después le damos a *Start Scan* y se escaneará de manera rápida las vulnerabilidades de este equipo que pueden ser alcanzadas.

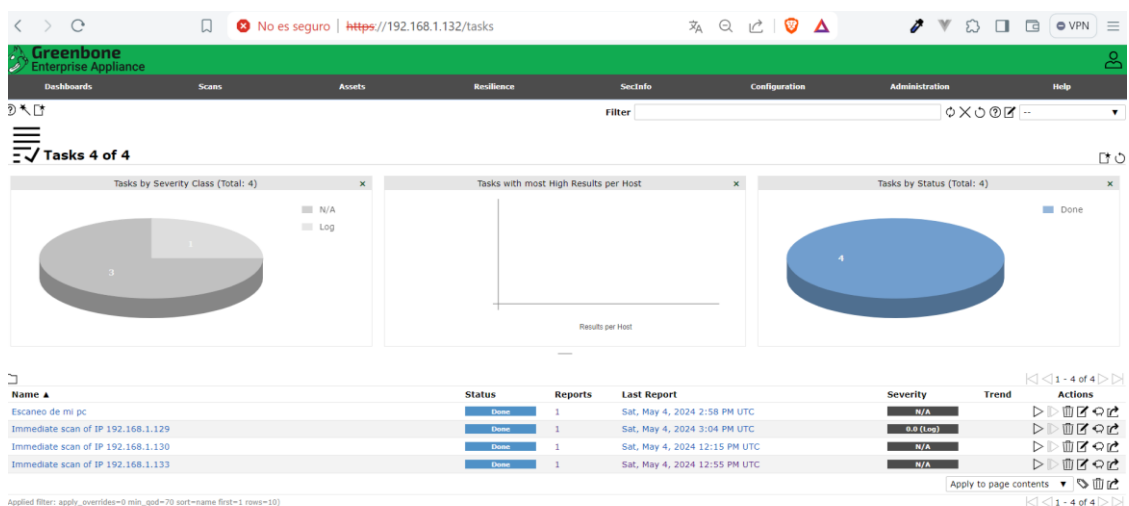


- Crear y configurar una tarea de escaneo vinculada al objetivo, seleccionando el tipo de escaneo y las preferencias de profundidad y exactitud.

Para un escaneo más preciso, nos dirigimos al icono de la hoja con una estrella (al lado de la varita mágica), seleccionamos “New Task” y se nos abrirá la siguiente ventana:

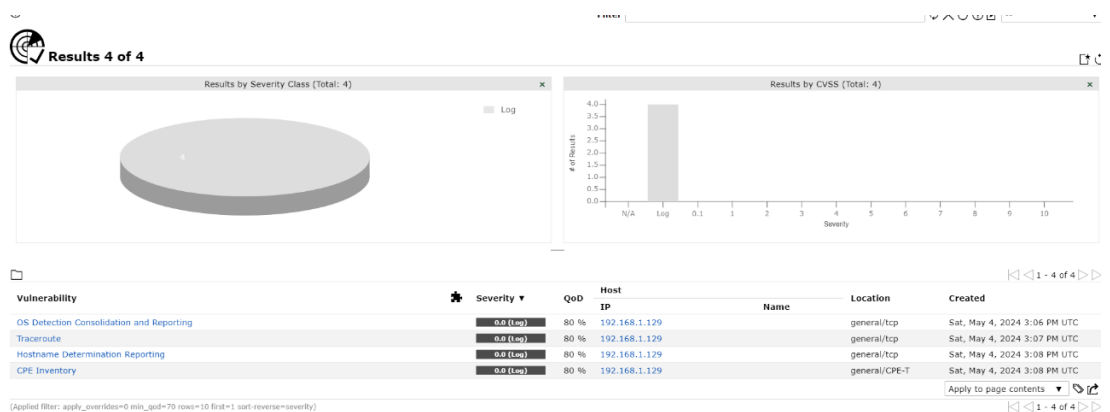
Aquí podremos especificar diferentes valores, como por ejemplo:

- Min QoD: es un valor entre 0 % y 100 % que describe la confiabilidad de la detección de vulnerabilidad o de producto ejecutada. Por defecto aparece 70%. Si vamos a la tabla de especificaciones podemos observar que significa cada valor:



Se ha realizado el escaneo tanto para mi ordenador personal como para mi teléfono móvil y no se ha encontrado ninguna vulnerabilidad.

Después hemos efectuado dicho escaneo para otro dispositivo de la red, un robot aspiradora (IP: 192.168.1.129), y sí se han encontrado algunas vulnerabilidades de tipo log tal y como podemos observar en la siguiente captura:



A este dispositivo en concreto le podrían hacer un *nmap* para saber qué equipo es, también pueden hacerle un *traceroute*, el hostname lo pueden reportar y pueden hacer un inventario.

Conclusión

Greenbone OpenVAS es una herramienta poderosa y esencial para cualquier equipo de seguridad informática que busque identificar y mitigar vulnerabilidades en su infraestructura, contribuyendo así a fortalecer la postura de seguridad y proteger los activos críticos de una organización.

dos herramientas poderosas, jajajajaj!!!!

Buen trabajo

10/10