

Programa de Fundamentos de Ciberseguridad

3° Edición

Taller Módulo II Implementación de Openvas

By:

WoSEC Panamá

Comunidad DOJO



Objetivos del taller:

Armar un laboratorio de análisis de vulnerabilidades y probar su correcto funcionamiento utilizando herramientas Open Source que nos permitan conocer cómo podemos identificar vulnerabilidades en nuestros sistemas.

Disclaimer:

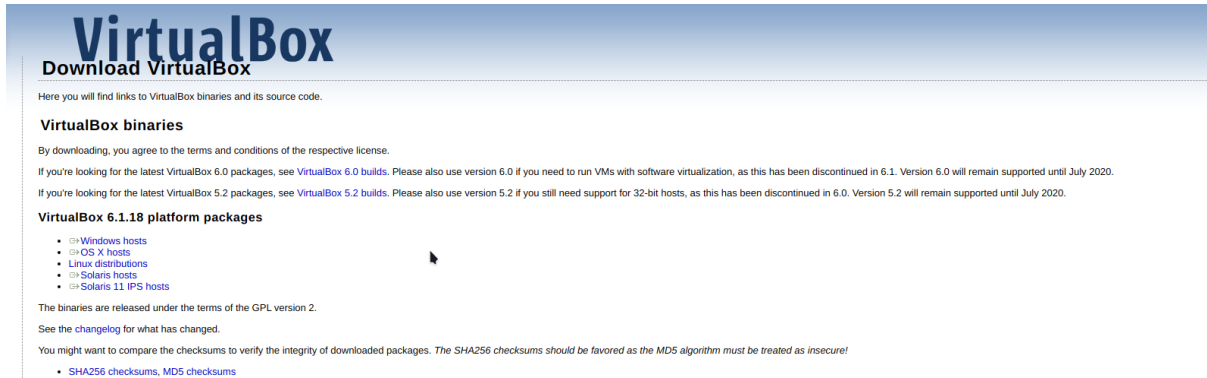
Este laboratorio se realiza sólomente con fines educativos y de aprendizaje, con el fin de brindar información que permita mejorar las defensas en ciberseguridad.

Metodología:

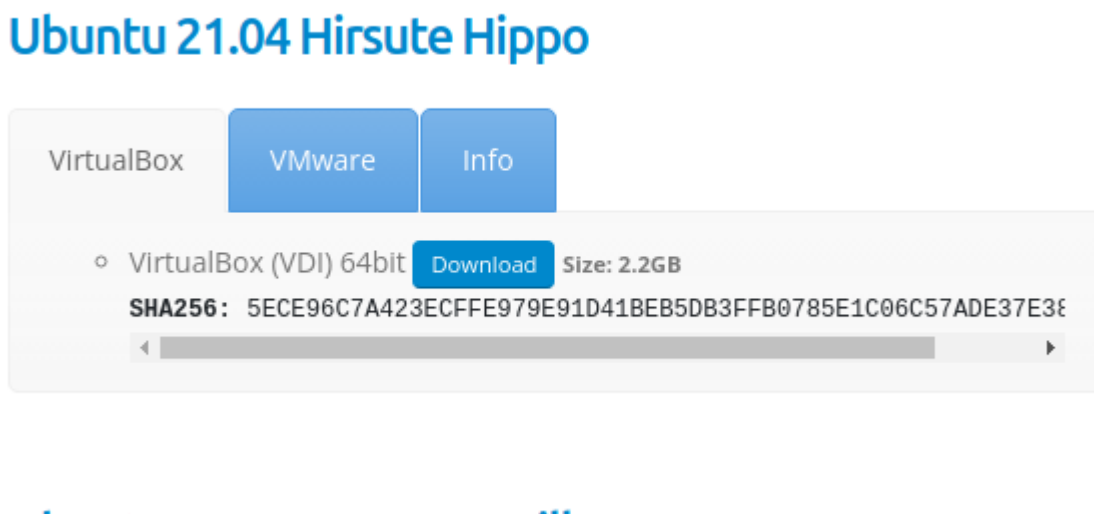
1. Se desplegará la herramienta Openvas en un entorno Linux utilizando Docker y se realizarán las configuraciones necesarias para su funcionamiento.
2. Se desplegará un entorno vulnerable por diseño DVWA y se realizará el escaneo de vulnerabilidades en este entorno, con el fin de analizar las vulnerabilidades encontradas.

Prerrequisitos:

Descargar e instalar VirtualBox: <https://www.virtualbox.org/wiki/Downloads>

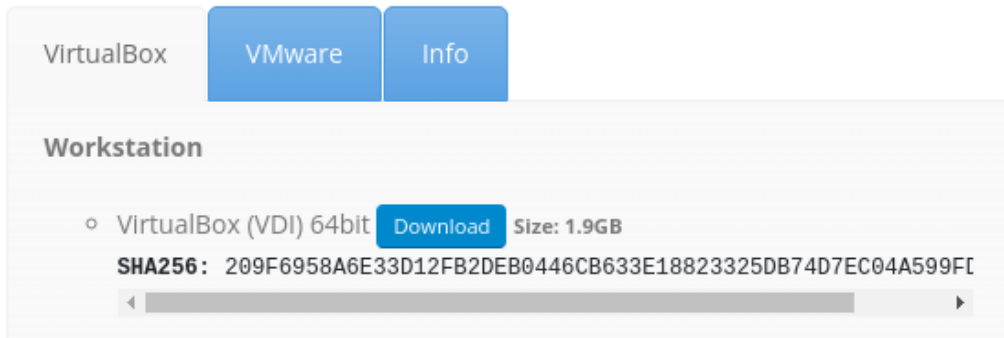


Descargar una máquina virtual con Ubuntu la cual pueden conseguir desde OSboxes: <https://www.osboxes.org/ubuntu/>



Descargar una máquina virtual con Fedora la cual pueden conseguir desde OSboxes: <https://www.osboxes.org/fedora/>

Fedora 34



Nota: La ventaja de las máquinas de OSBoxes es que ya se encuentran "listas para usar". Utilizan el siguiente usuario y contraseña por defecto: Usuario: **osboxes**
Contraseña: **osboxes.org**

Una vez descargados los archivos de OSBoxes, descomprimirlo en un subdirectorio utilizando una herramienta como p7zip:

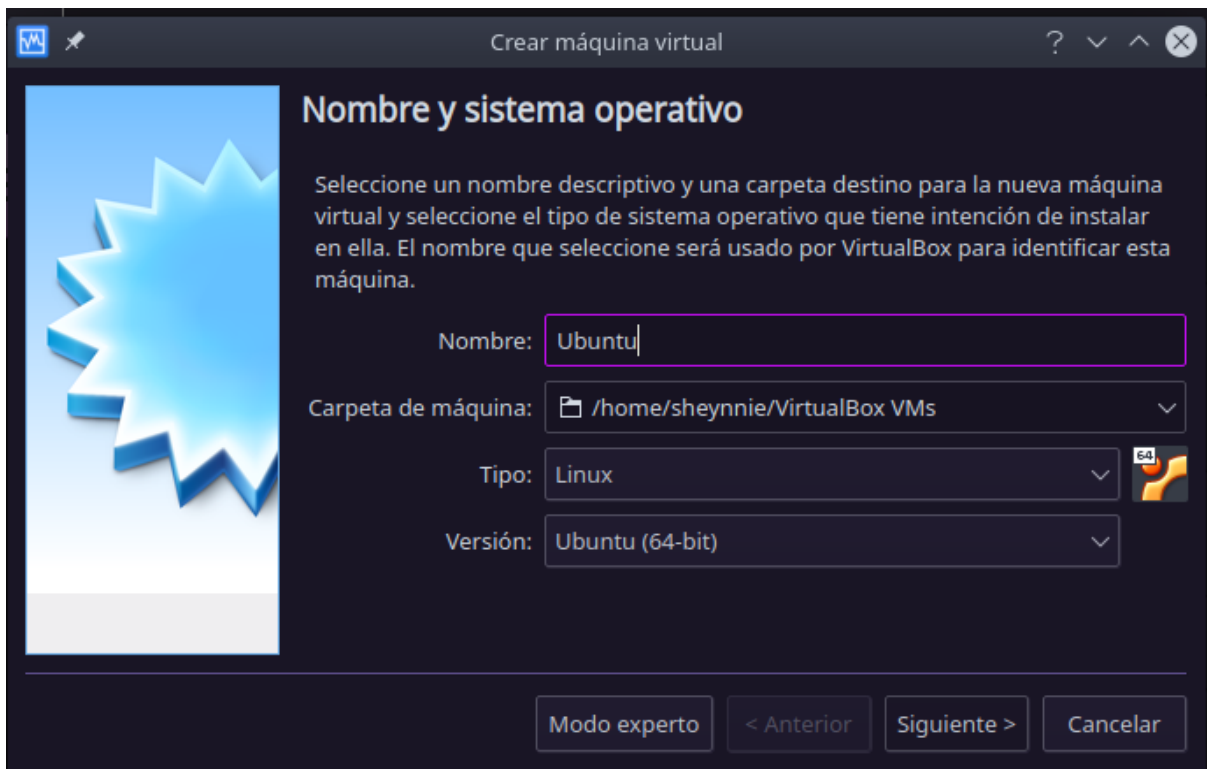
p7zip -d ubuntu_64bits.7z

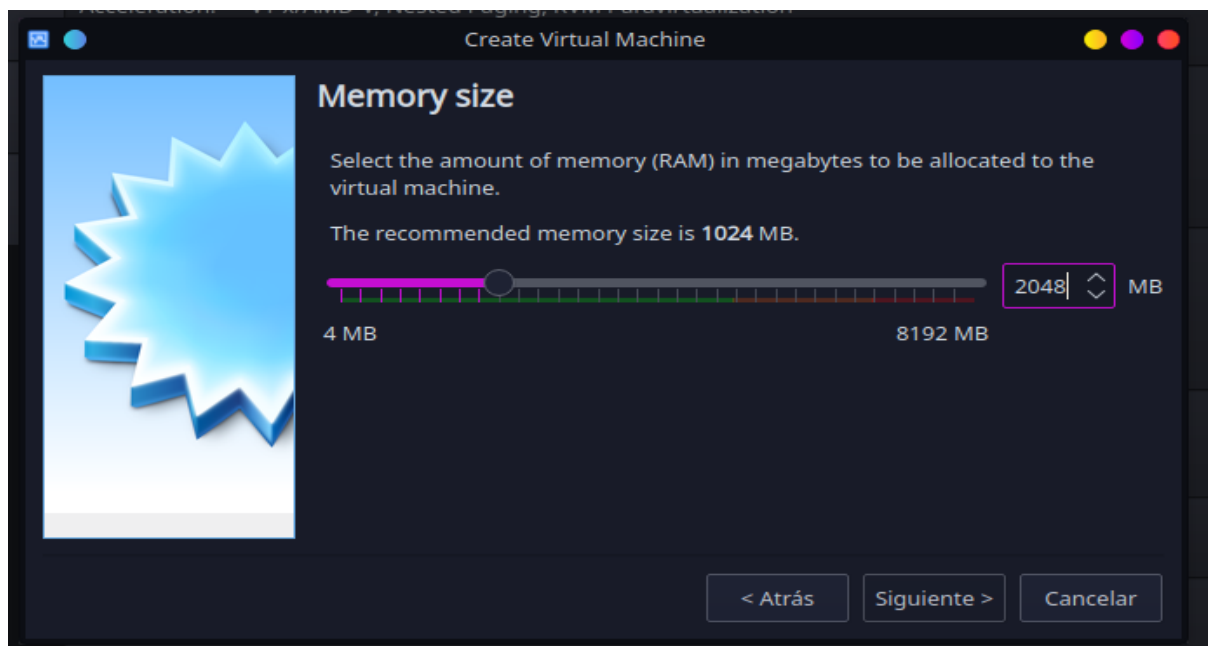
```
sheynnie@localhost:~/Downloads> p7zip -d ubuntu_64bits.7z
```

Para la máquina Ubuntu:

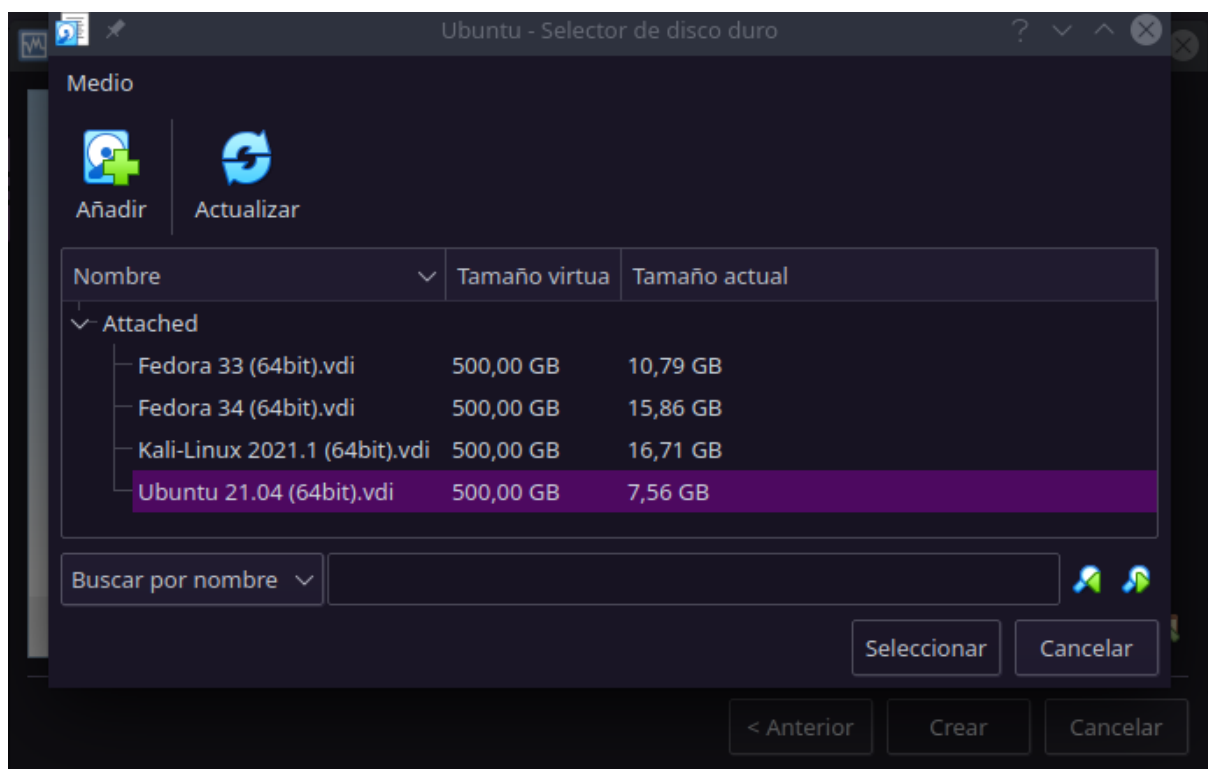
Abrir virtualbox y crear 1 máquina virtual con las siguientes características:

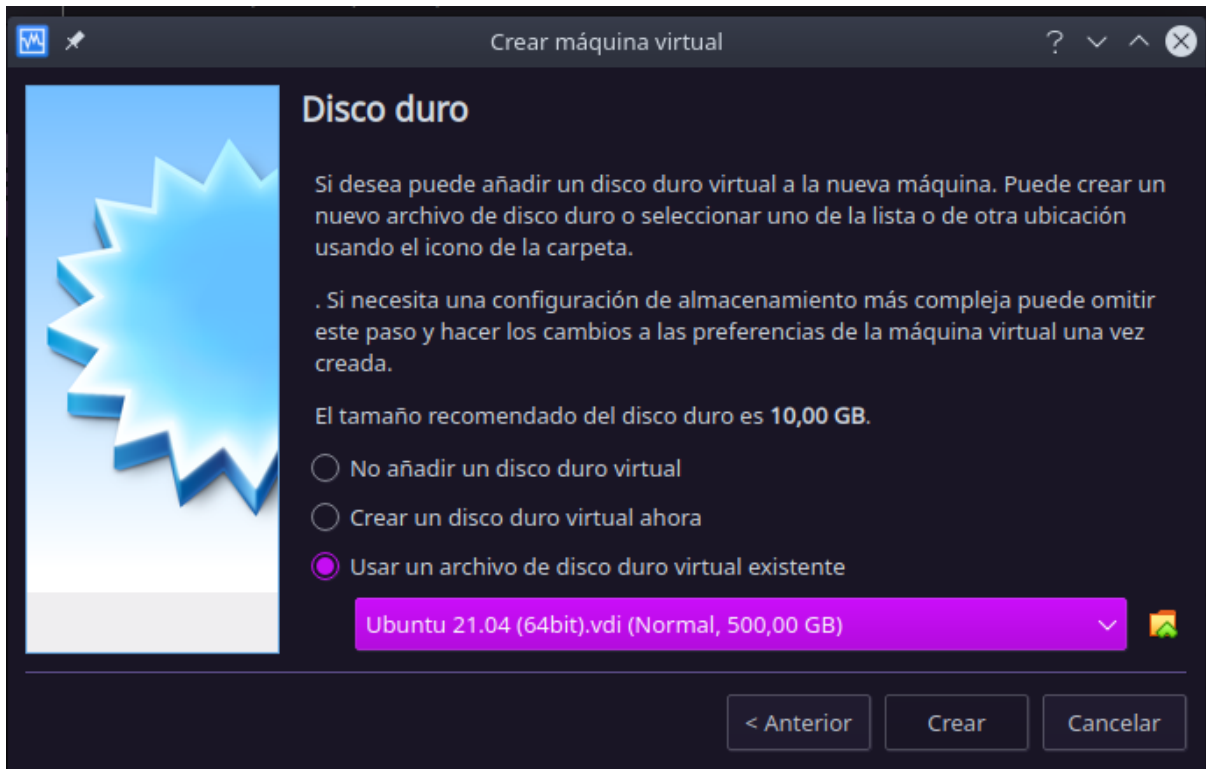
Mínimo 2048 mb de memoria





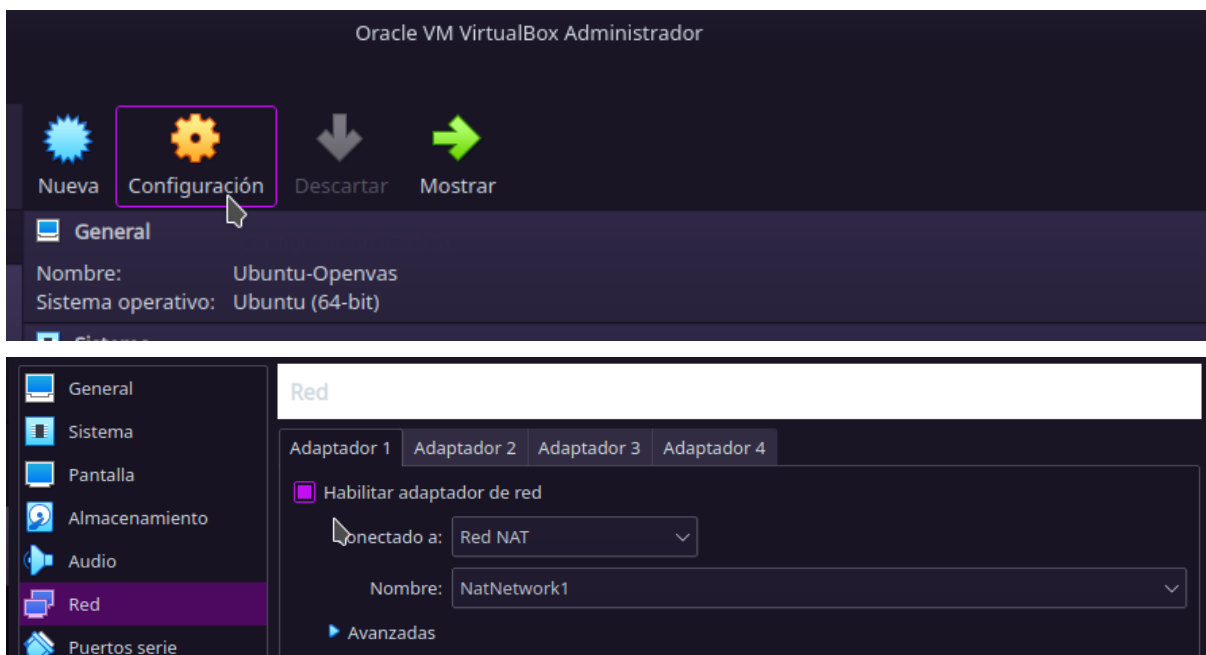
Asignar el archivo .vdi previamente extraído como disco duro existente de la máquina:





Dar click al botón crear para finalizar.

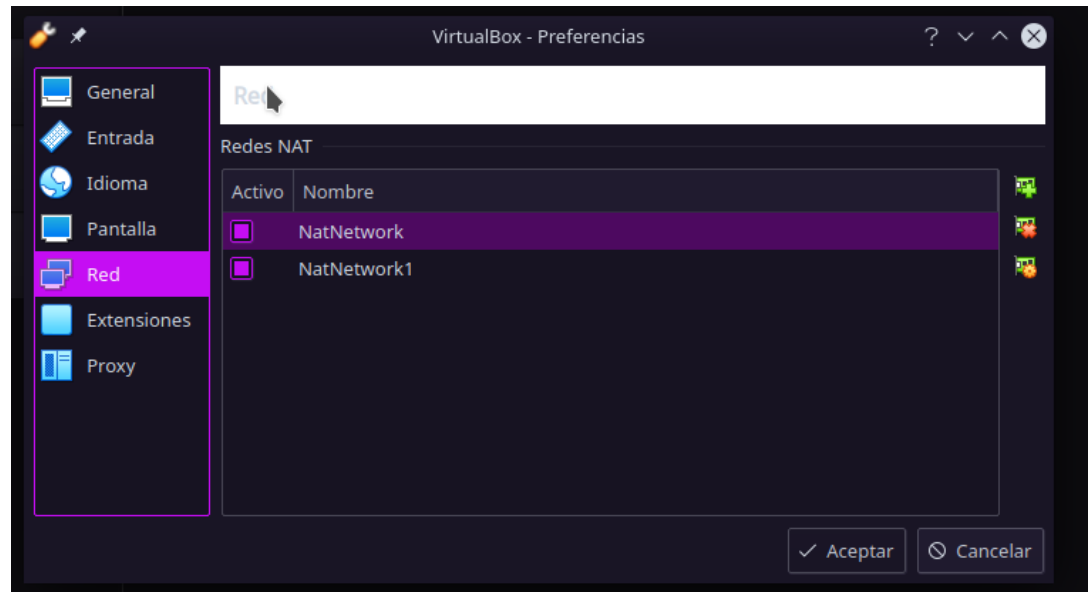
Posteriormente, nos dirigimos a la máquina creada y damos click al botón configuración->red y en la sección del primer adaptador, asigne la opción "Red NAT" y seleccione una red NAT previamente creada.



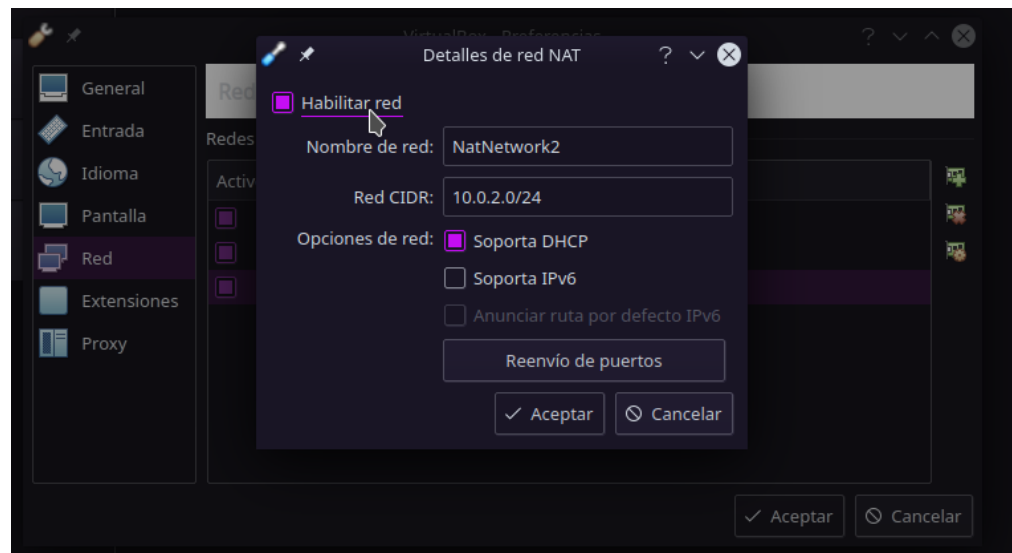
Con esta configuración ya podemos iniciar la máquina.

Notas:

- Si no tiene una red NAT creada previamente, puede realizarlo de la siguiente forma:
 - Desde la opción “**Archivo->Preferencias->red**” de VirtualBox



- Donde, con el botón + puede agregar una nueva red y con el botón de **configuración** puede cambiar el nombre, rango de red y opciones como DHCP, IPV6 y reenvío de puertos. Para fines de este laboratorio solo necesitamos especificar el rango de red y la opción de DHCP para la asignación de IP automática.



- Se recomienda actualizar la máquina:
 - Para Ubuntu, desde la terminal ingrese el comando “**sudo apt-get update**”.

Para la máquina Fedora:

Repetimos el mismo procedimiento utilizado para la máquina de Ubuntu.

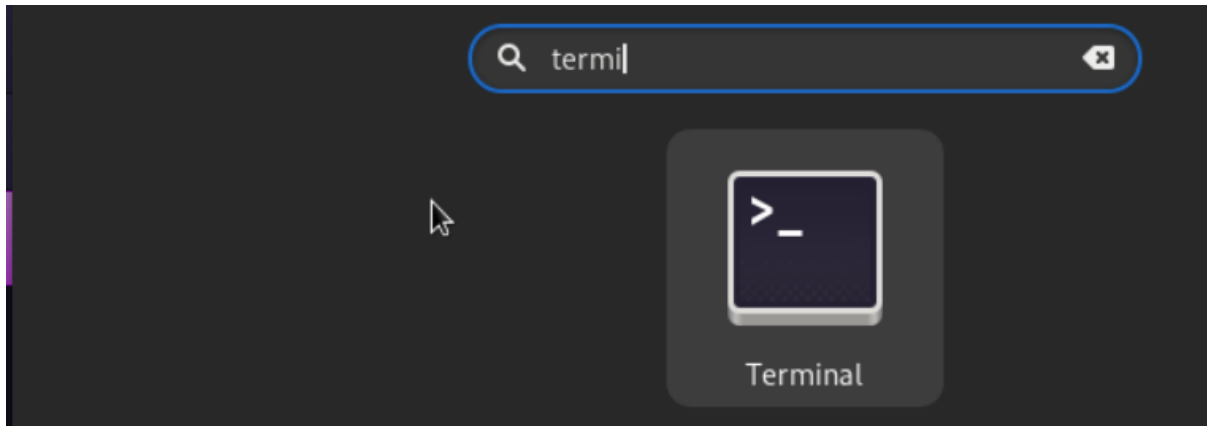
Notas:

- Ambas máquinas deben quedar bajo la misma red NAT para que puedan visualizarse entre sí.
- Se recomienda actualizar la máquina:
 - Desde la terminal ingrese el comando: “***sudo dnf update***”.

Parte I: Configuración de DVWA en Fedora

Instalar las librerías necesarias desde la terminal:

Activities → terminal



Ingresamos el siguiente comando para instalar los prerequisites necesarios: ***sudo dnf install docker***

```
osboxes@fedora:~ — sudo dnf install docker
[osboxes@fedora ~]$ sudo dnf install docker
[sudo] password for osboxes:
Last metadata expiration check: 0:02:51 ago on Wed 06 Apr 2022 11:26:55 PM EDT.
Dependencies resolved.
=====
Package                Architecture Version                Repository             Size
=====
Installing:
moby-engine             x86_64             20.10.12-1.fc34        updates                33 M
Installing dependencies:
containerd              x86_64             1.6.1-1.fc34           updates                39 M
runc                    x86_64             2:1.1.0-1.fc34         updates                3.1 M
=====
Transaction Summary
=====
Install 3 Packages

Total download size: 75 M
Installed size: 317 M
Is this ok [y/N]: y
Downloading Packages:
(1/3): runc-1.1.0-1.fc34.x86_64.rpm          921 kB/s | 3.1 MB    00:03
(2/3): moby-engine-20.10.12-1.fc34.x86_64.rpm 3.4 MB/s | 33 MB    00:09
(3/3): containerd-1.6.1-1.fc34.x86_64.rpm    3.7 MB/s | 39 MB    00:10
```

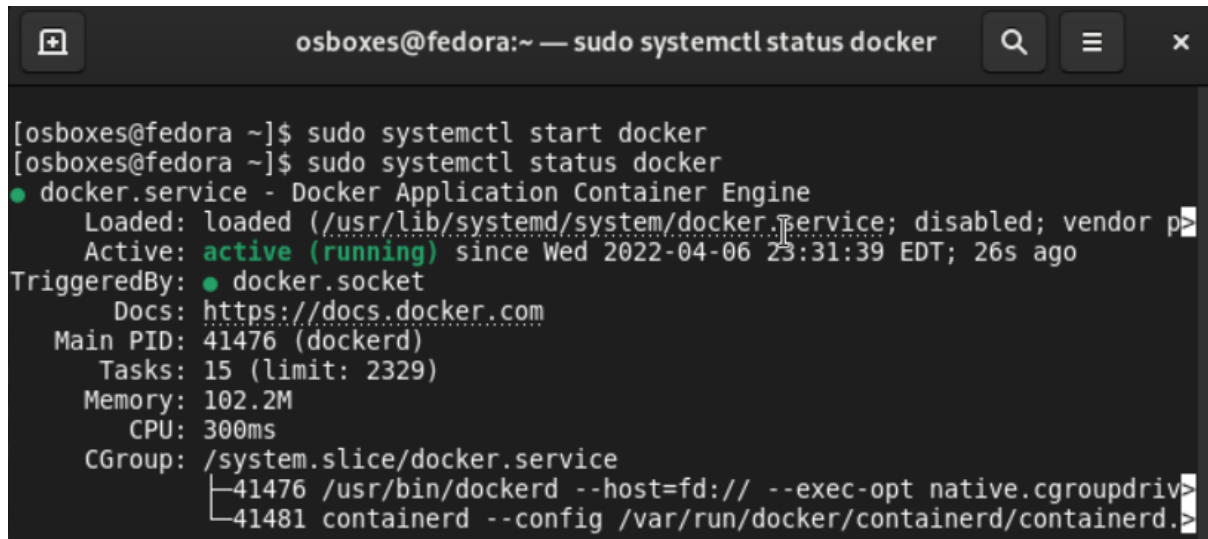
Iniciamos el servicio de docker

sudo systemctl start docker

```
[osboxes@fedora ~]$ sudo systemctl start docker
```

Revisamos que se encuentre en ejecución:

`sudo systemctl status docker`

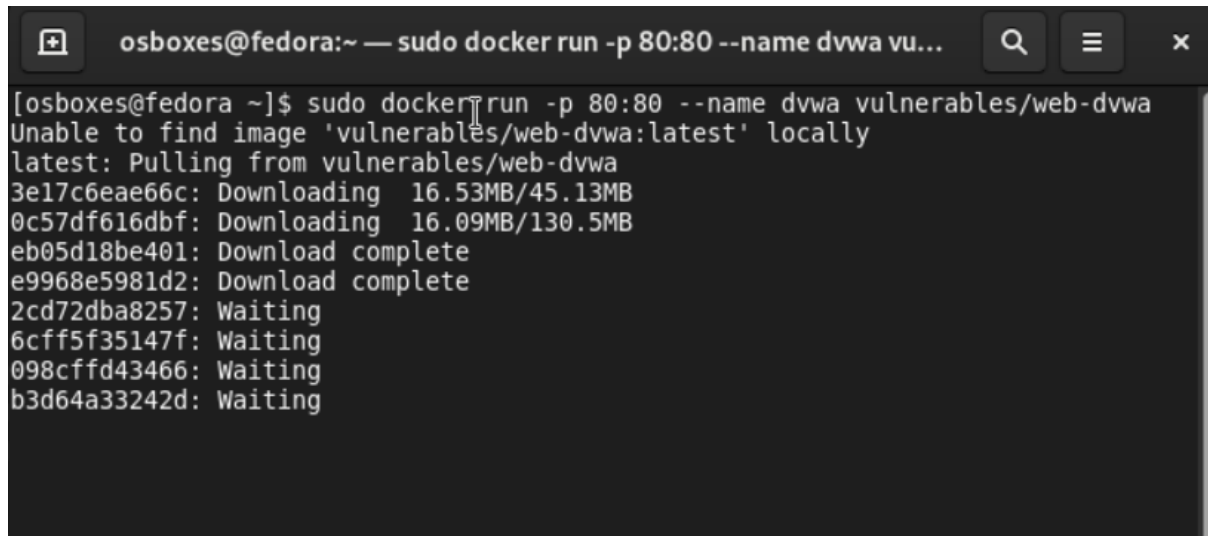


```
osboxes@fedora:~ — sudo systemctl status docker

[osboxes@fedora ~]$ sudo systemctl start docker
[osboxes@fedora ~]$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; disabled; vendor p
   Active: active (running) since Wed 2022-04-06 23:31:39 EDT; 26s ago
   TriggeredBy: ● docker.socket
     Docs: https://docs.docker.com
    Main PID: 41476 (dockerd)
      Tasks: 15 (limit: 2329)
     Memory: 102.2M
        CPU: 300ms
    CGroup: /system.slice/docker.service
            └─41476 /usr/bin/dockerd --host=fd:// --exec-opt native.cgroupdriv
              └─41481 containerd --config /var/run/docker/containerd/containerd.
```

Ahora, pasaremos a ejecutar DVWA:

`sudo docker run -p 80:80 --name dvwa vulnerables/web-dvwa`




```
osboxes@fedora:~ — sudo docker run -p 80:80 --name dvwa vu...

[osboxes@fedora ~]$ sudo docker run -p 80:80 --name dvwa vulnerables/web-dvwa
Unable to find image 'vulnerables/web-dvwa:latest' locally
latest: Pulling from vulnerables/web-dvwa
3e17c6eae66c: Downloading 16.53MB/45.13MB
0c57df616dbf: Downloading 16.09MB/130.5MB
eb05d18be401: Download complete
e9968e5981d2: Download complete
2cd72dba8257: Waiting
6cff5f35147f: Waiting
098cffd43466: Waiting
b3d64a33242d: Waiting
```

Una vez finalizada la descarga, podemos abrir el navegador web y dirigirnos a <https://127.0.0.1> para visualizar la interfaz de DVWA.

127.0.0.1/login.php




Username

Password

Login

Puedes ingresar con el usuario **admin** y contraseña **password**

127.0.0.1/setup.php



Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: `/var/www/html/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.0.30-0+deb9u1**

Web Server SERVER_NAME: **127.0.0.1**

PHP function display_errors: **Disabled**
PHP function safe_mode: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: **Enabled**
PHP function magic_quotes_gpc: **Disabled**
PHP module gd: **Installed**
PHP module mysql: **Installed**
PHP module pdo_mysql: **Installed**

MySQL username: **app**
MySQL password: *********
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

Parte II: Configuración de Openvas en Ubuntu

Instalar las librerías necesarias desde la terminal:

Aplicaciones → buscador→terminal

Ingresamos el siguiente comando para instalar los prerequisites necesarios:

***sudo apt-get install apt-transport-https ca-certificates curl
software-properties-common***

```
osboxes@osboxes:~$ sudo apt-get install apt-transport-https ca-certificates curl  
software-properties-common git  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done
```

Añadimos la llave PGP para el repositorio oficial de docker:

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

```
osboxes@osboxes:~$ curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -  
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).  
OK
```

Agregamos el repositorio de docker a los paquetes del sistema:

***sudo add-apt-repository "deb [arch=amd64]
https://download.docker.com/linux/ubuntu bionic stable"***

```
osboxes@osboxes:~$ sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu bion  
ic stable"  
Repository: 'deb [arch=amd64] https://download.docker.com/linux/ubuntu bionic stable'  
Description:  
Archive for codename: bionic components: stable  
More info: https://download.docker.com/linux/ubuntu  
Adding repository.  
Press [ENTER] to continue or Ctrl-c to cancel.  
Adding deb entry to /etc/apt/sources.list.d/archive_uri-https_download_docker_com_linux_ubuntu-hirsute.lis  
t
```

Actualizamos nuevamente el sistema para leer los nuevos paquetes

sudo apt-get update

```
osboxes@osboxes:~$ sudo apt-get update  
Hit:1 http://us.archive.ubuntu.com/ubuntu hirsute InRelease  
Hit:2 http://us.archive.ubuntu.com/ubuntu hirsute-updates InRelease  
Hit:3 http://us.archive.ubuntu.com/ubuntu hirsute-backports InRelease  
Hit:4 http://security.ubuntu.com/ubuntu hirsute-security InRelease  
Hit:5 https://download.docker.com/linux/ubuntu bionic InRelease  
Reading package lists... Done
```

Instalamos docker con el siguiente comando:

sudo apt install docker-ce

```
osboxes@osboxes:~$ sudo apt install docker-ce
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  containerd.io docker-ce-cli docker-ce-rootless-extras docker-scan-plugin libslirp0 pigz slurp4netns
Suggested packages:
  aufs-tools cgroupfs-mount | cgroup-lite
The following NEW packages will be installed:
  containerd.io docker-ce docker-ce-cli docker-ce-rootless-extras docker-scan-plugin libslirp0 pigz
```

Revisamos que se encuentre en ejecución:

`sudo systemctl status docker`

```
osboxes@osboxes:~$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/lib/systemd/system/docker.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-10-01 01:08:10 EDT; 38s ago
     TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
      Main PID: 23906 (dockerd)
         Tasks: 7
        Memory: 30.2M
         CGroup: /system.slice/docker.service
                 └─23906 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock
```

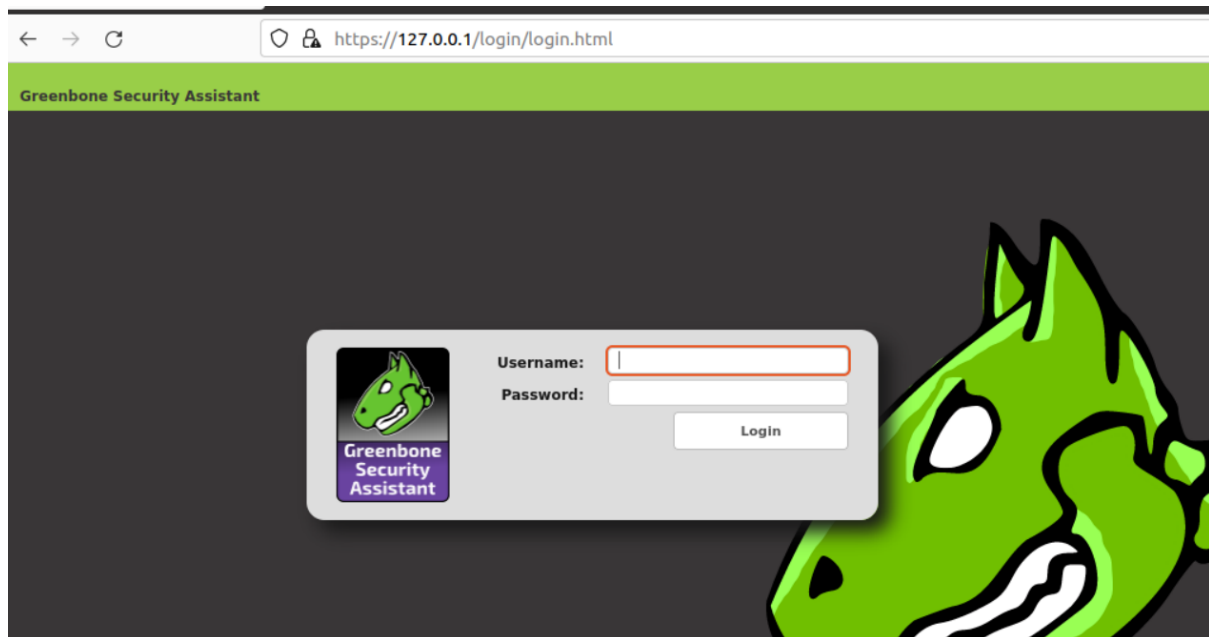
Ahora, pasaremos a ejecutar Openvas:

`sudo docker run -d -p 443:443 --name openvas mikesplain/openvas`

```
osboxes@osboxes:~$ sudo docker run -d -p 443:443 --name openvas mikesplain/openvas
Unable to find image 'mikesplain/openvas:latest' locally
latest: Pulling from mikesplain/openvas
34667c7e4631: Pull complete
d18d76a881a4: Pull complete
119c7358fbfc: Pull complete
2aaf13f3eff0: Pull complete
67b182362ac2: Pull complete
c878d3d5e895: Pull complete
ec12cc49fe18: Pull complete
c4c454aeebef: Pull complete
27d3410150b2: Pull complete
e08d578dc278: Pull complete
44951337cd32: Pull complete
8c7fe885e62a: Pull complete
a4f833680e45: Pull complete
Digest: sha256:23c8412b5f9f370ba71e5cd3db36e6f2e269666cd8a3e3e7872f20f8063b2752
Status: Downloaded newer image for mikesplain/openvas:latest
5d4ff6d74dc5c0fe90d268aafc0c0f82f27ed2206eddd7db8f19788db3aaa6ec
osboxes@osboxes:~$
```

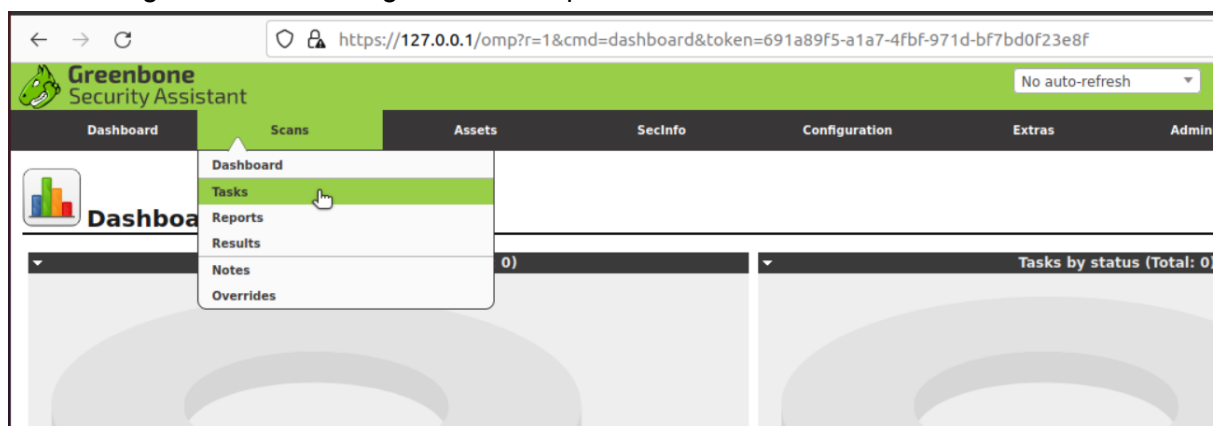
Una vez finalizada la descarga, podemos abrir el navegador web y dirigirnos a

<https://127.0.0.1> para visualizar la interfaz de Openvas.

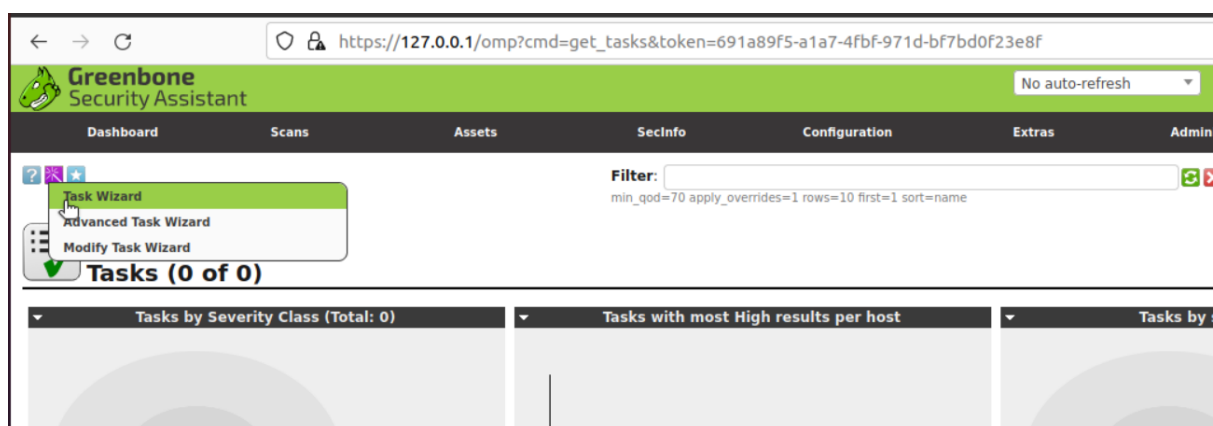


Puedes ingresar con el usuario **admin** y contraseña **admin**

Una vez ingresamos, nos dirigiremos a la opción **Scans -> Tasks**




Ahora, nos posicionamos en el segundo botón ubicado a mano izquierda y damos click en **Task Wizard** para iniciar el asistente de ejecución de tareas.



Ingresamos la ip de nuestra máquina DVWA y damos click al botón “Start Scan” para iniciar el escaneo de vulnerabilidades.

Task Wizard



Quick start: Immediately scan an IP address


IP address or hostname:
192.168.1.18

The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:

1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

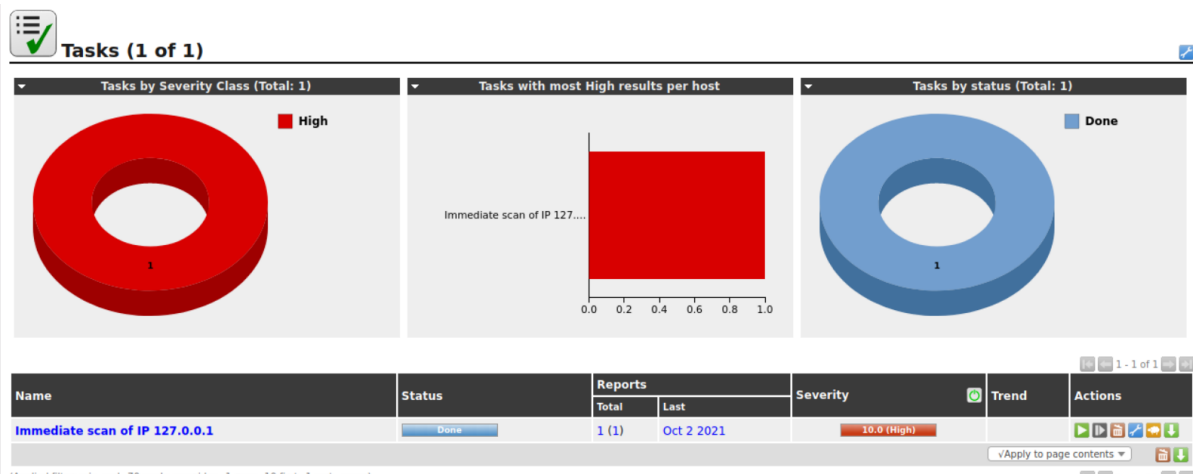
In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the defaults as configured in "My Settings".

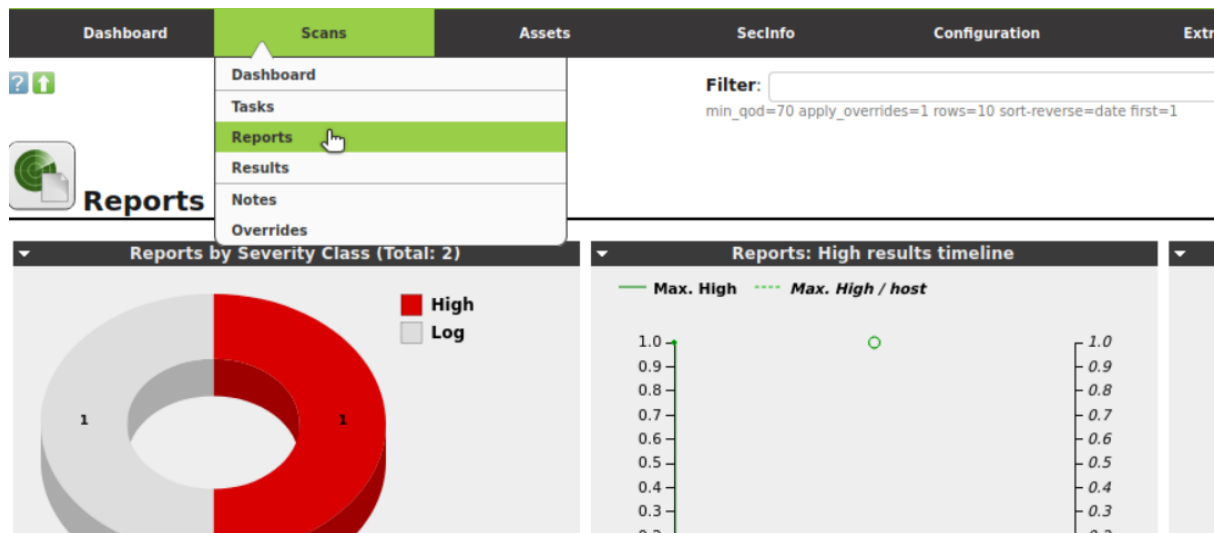
By clicking the New Task icon  you can create a new Task yourself.

Start Scan

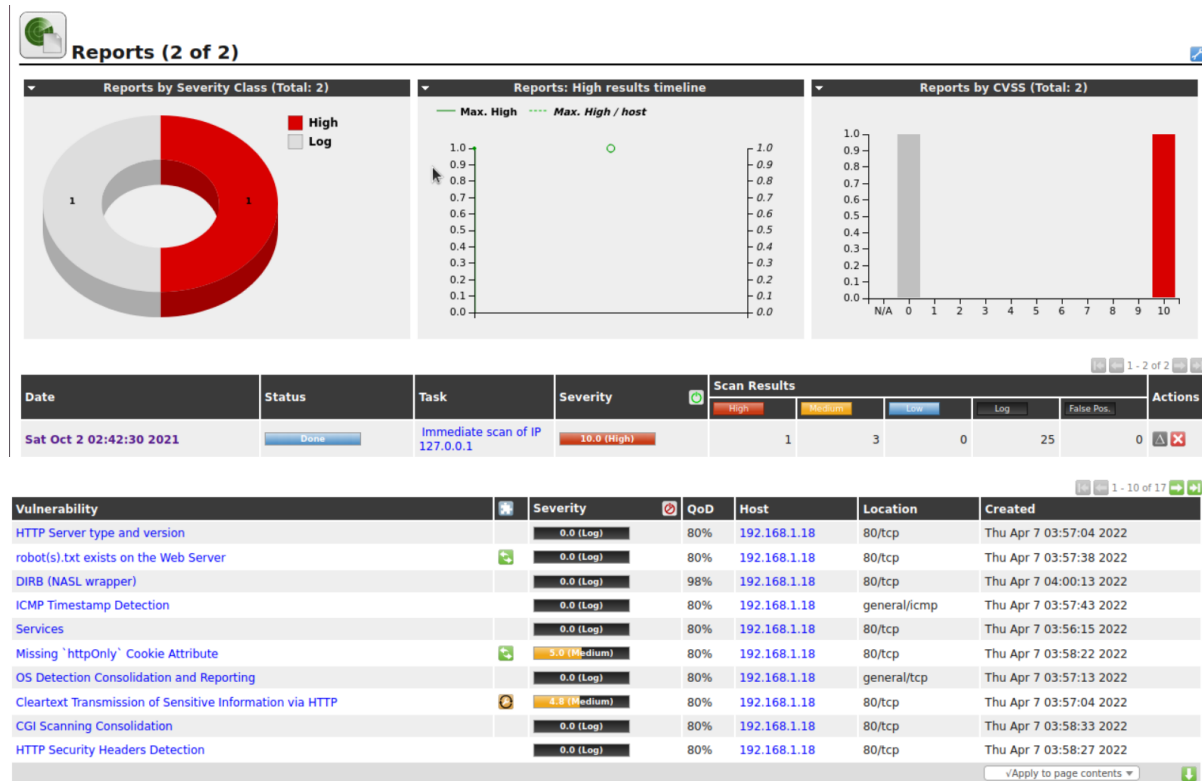
Una vez finalice el scan se mostrará en status “Done”



Ahora, ingresamos a **Scan -> Reports**



Y seleccionamos el reporte previamente generado para conocer las vulnerabilidades encontradas.



Ya con esto, podemos seleccionar cada una de las vulnerabilidades para visualizar el reporte detallado.

**Result: OpenVAS / Greenbone Vulnerability Manager Default Credentials**

Groups	401fa9e65
Roles	
LDAP	
Radius	

Vulnerability	Severity	QoD	Host	Location	Actions
OpenVAS / Greenbone Vulnerability Manager Default Credentials	10.0 (High)	100%	127.0.0.1	9390/tcp	
Summary The remote OpenVAS / Greenbone Vulnerability Manager is installed/configured in a way that it has account(s) with default passwords enabled.					
Vulnerability Detection Result It was possible to login using the following credentials (username:password:role): admin:admin:Admin					
Impact This issue may be exploited by a remote attacker to gain access to sensitive information or modify system configuration.					
Solution Solution type: Workaround Change the password of the mentioned account(s).					
Vulnerability Insight It was possible to login with default credentials: admin/admin, sadmin/changeme, observer/observer or admin/openvas.					
Vulnerability Detection Method Try to login with default credentials via the OMP/GMP protocol. Details: OpenVAS / Greenbone Vulnerability Manager Default Credentials (OID: 1.3.6.1.4.1.25623.1.0.108554)					