**Scanning**

## 

## 

**MARCO BATISTA Y ENRIQUE GONZÁLEZ**

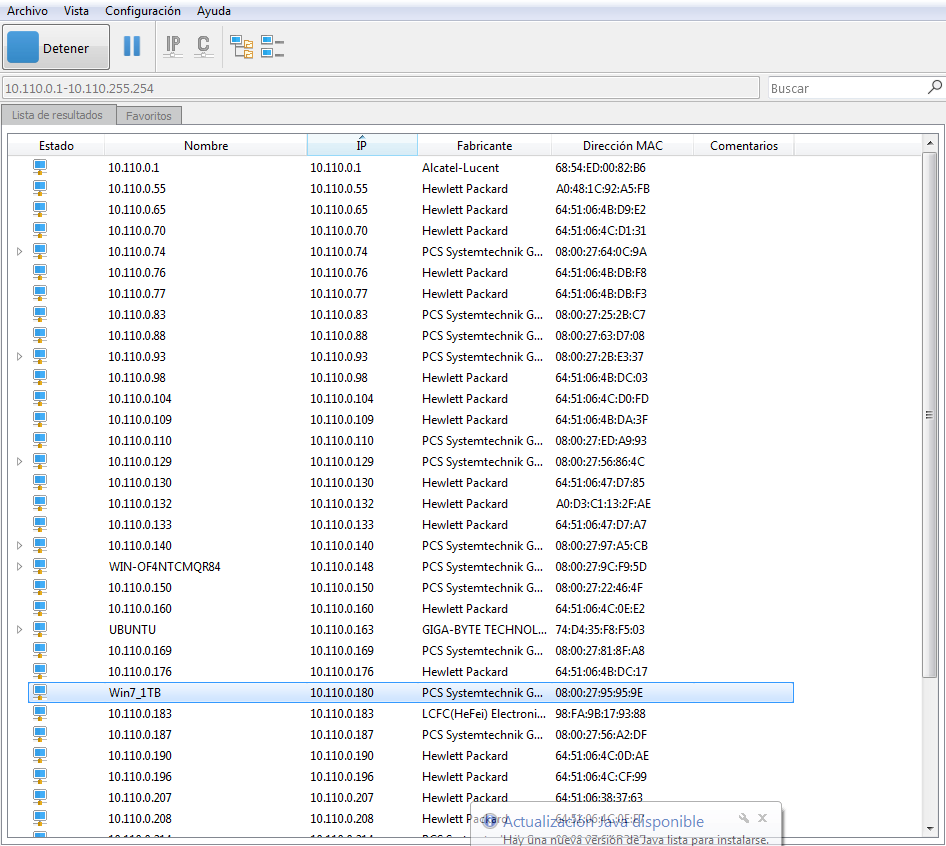
**Definición:** El término escáner de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuegos.

Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos. (Wikipedia)

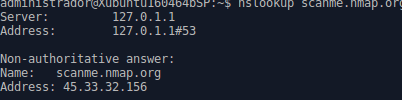
En algunos países esta actividad puede considerarse un delito informático.

**Ejercicios:**

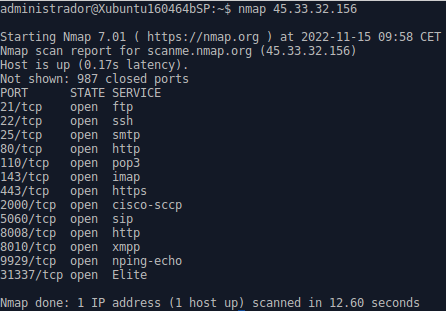
1. Realizar un análisis de red con el programa Advanced IP Scanner para Windows.



2. Nmap

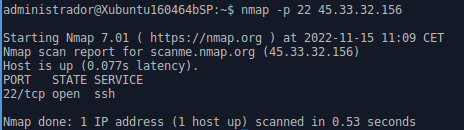


2.1. Realizar varias pruebas de escaneo con la página http://scanme.nmap.org/

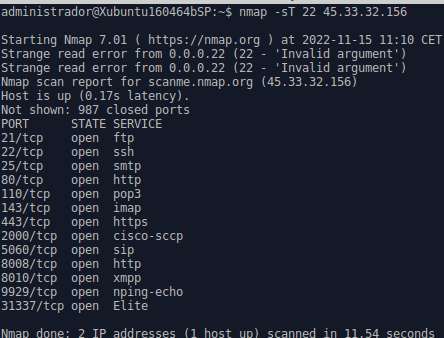


**nmap *[ip]* ->Puertos abiertos**

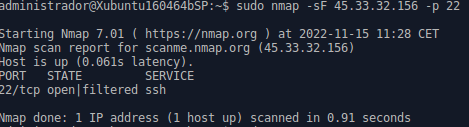
***nmap -p 22 45.33.32.156 ->puerto en concreto, ver si está abierto***

******

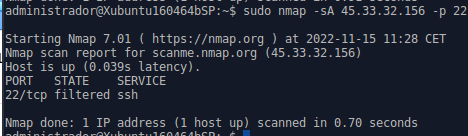
***nmap -sT 45.33.32.156 ->tcp full, es el que hace por defecto***

******

***sudo nmap -sF 45.33.32.156 -> envias la señal de finalización.***

******

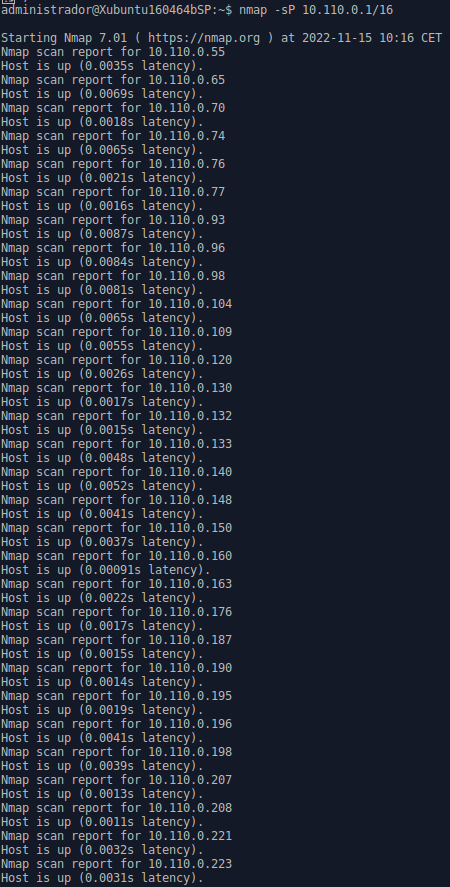
***sudo nmap -sA 45.33.32.156 -> envias la señal sin que te la pida.***

***filtered suele ser por firewall***

2.2. Realizar un barrido ping para averiguar los hosts activos en la red local.

**nmap -sP**

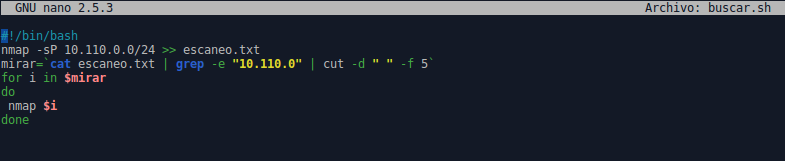
[**Barridos de pings (Ipscan y Nmap) | Christian Romero**](https://christianromero.es/blog/2010/08/02/barridos-de-pings-ipscan-y-nmap/)

****

2.3. Para los hosts activos del apartado anterior realizar un escaneo TCP completo para averiguar los puertos abiertos.

**lo metemos en un fichero > escaneo.txt**

**Y ahora creamos un script que coja IP a IP y realice un escaneo de puertos, se puede poner -sT, pero lo hace por defecto.**

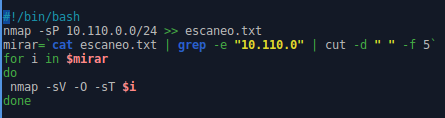
****

2.4. Repetir la prueba pero averiguando el sistema operativo y la versión de los servicios utilizados

**Opción -O: sistema operativo**

**-sV: version**

**-sT: distintos tipos de escaneo**

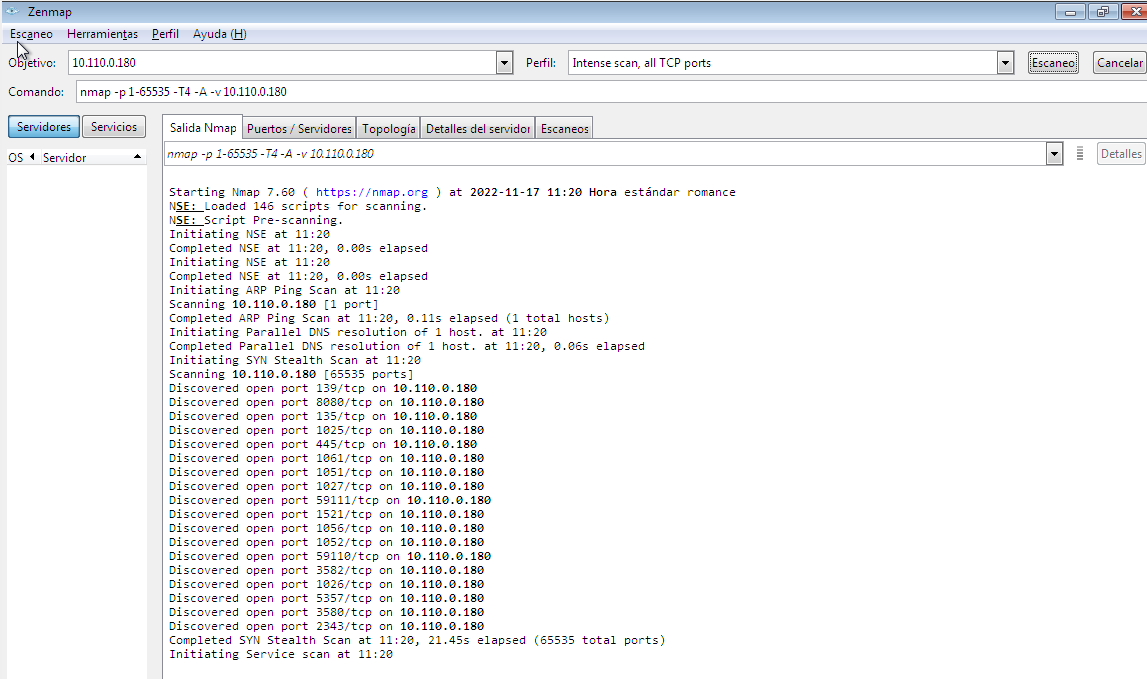
/24 para que tarde menos

el script se tiene que ejecutar con sudo

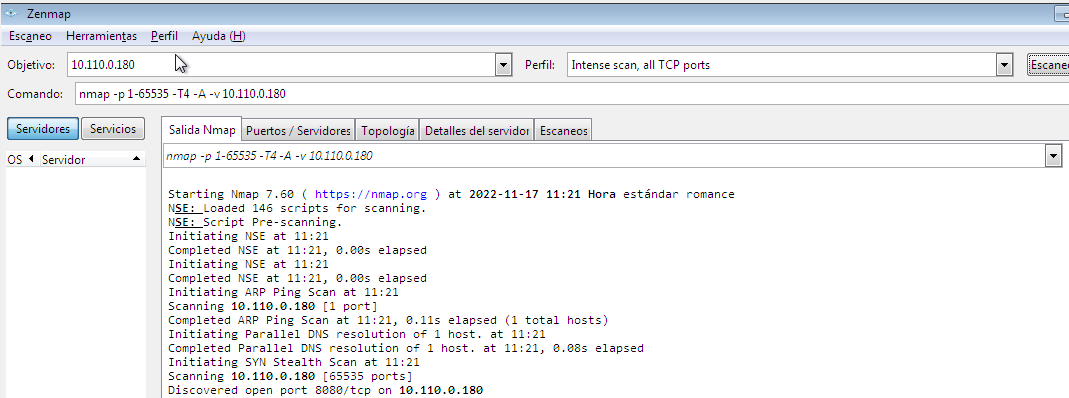


3. Zenmap

3.1. Realizar un escaneo TCP completo a una máquina Windows 7 sin firewall

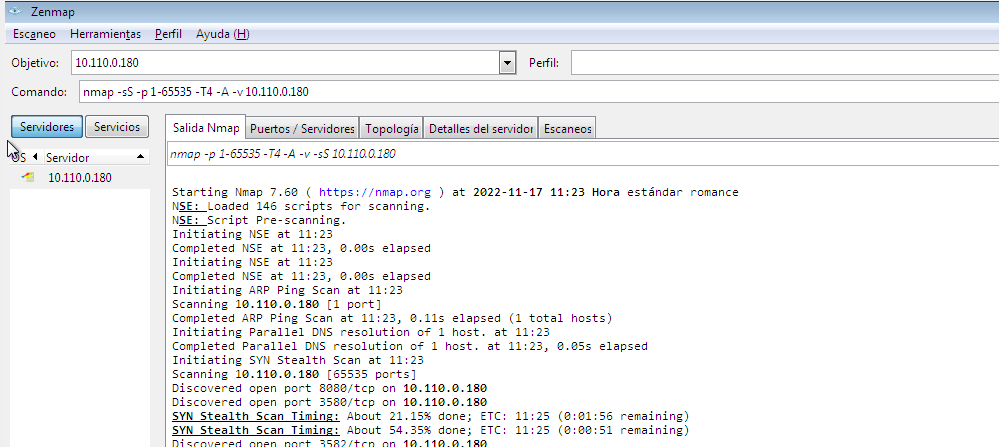


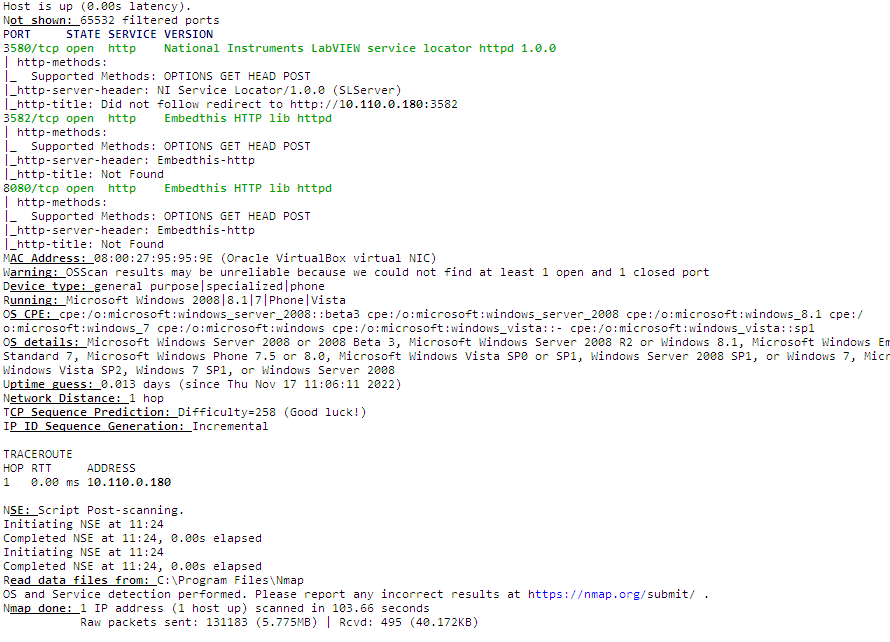
3.2. Habilitar el firewall de Windows y repetir la prueba



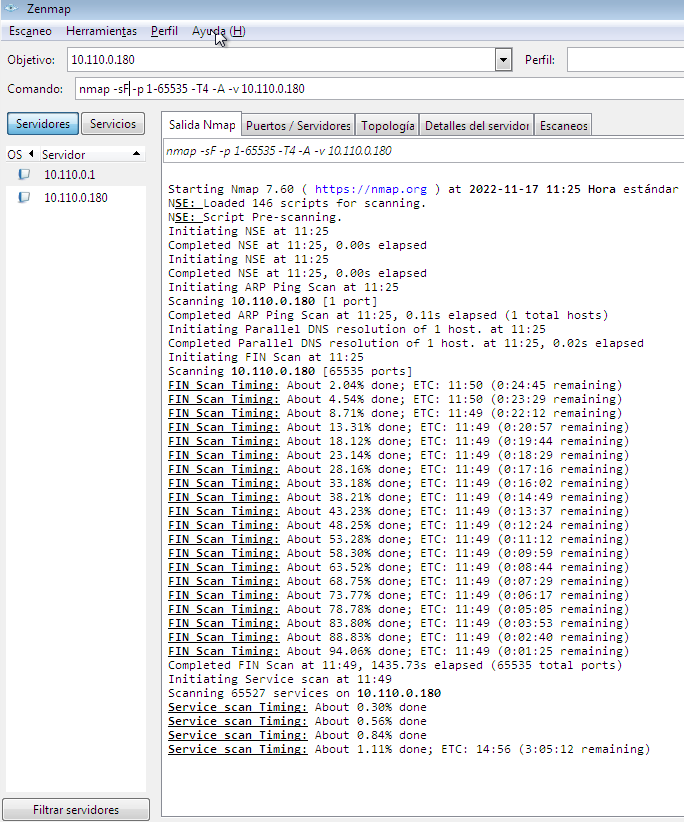
3.3. Con el firewall activo hacer distintos tipos de escaneo a esa máquina (syn, fin, null, xmas,ack)

**-sS: sincronización**

****

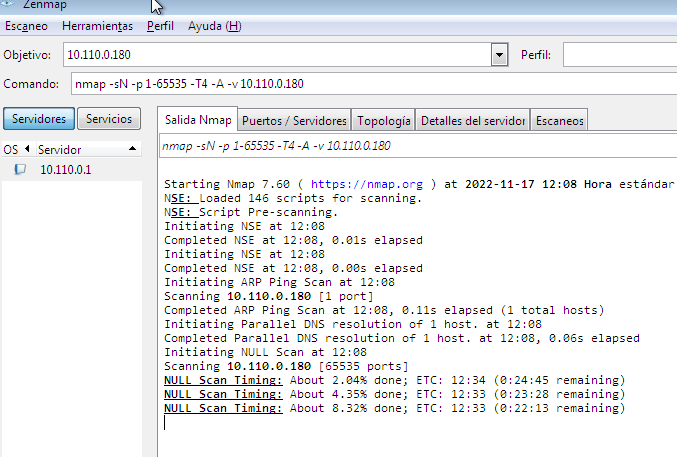
****

**-sF**

****

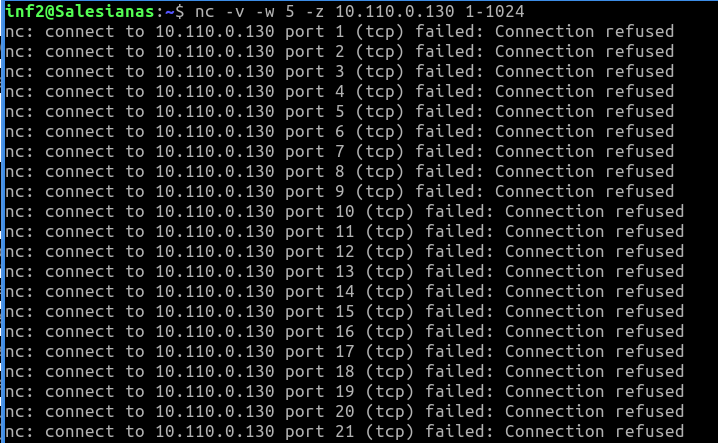
**-sN**

**-sX**

****

4. En Linux probar el siguiente comando de Netcat contra una máquina Linux normal y contra la máquina Linux metaesploitable2: nc -v -w 5 -z ip 1-1024 (ip es la dirección de la máquina a atacar)

**CONTRA OTRA LINUX:**  no esta ninguno abierto, o no salen.



**CONTRA METAESPLOITABLE2:**



5. Buscar en Internet alguna vulnerabilidad conocida que se pueda explotar para los siguientes protocolos: netbios, ssh, ftp y http

**Netbios:** es frecuente que los routers o switches que son utilizados por usuarios domésticos, señuelos de ciberseguridad (honeypots) o servicios de vigilancia, sean vulnerables al no contar con una configuración adicional de seguridad para el servicio de NetBIOS.

**SSH:** La nueva vulnerabilidad grave del momento se llama [CVE-2018-10933](https://www.libssh.org/security/advisories/CVE-2018-10933.txt). Se trata de una vulnerabilidad crítica en una librería de código abierto llamada libssh.

El problema es más que grave, es aterrador, ya que en teoría permite a un atacante conectarse a un servidor protegido con libssh sin tener que introducir ninguna contraseña.

Es aterrador porque SSH es probablemente el protocolo de acceso remoto más utilizado en todo el mundo. Casi todos los servidores Unix y Linux emplean SSH para la administración remota y hay un montón de enormes granjas de servidores por lo que SSH está implementado en infinidad de lugares.

**FTP:** Se ha reportado una vulnerabilidad en el FTP de Microsoft IIS que podría permitir a un atacante remoto la ejecución de código arbitrario en el equipo atacado. El usuario autenticado puede enviar comandos FTP especialmente diseñados para provocar un desbordamiento de pila, obteniendo.

El código con los parámetros manipulados se puede conseguir en el siguiente enlace: <http://www.milw0rm.com/exploits/9541>

Aunque esta vulnerabilidad sólo se ha probado con usuarios anónimos con permiso de escritura, no significa que el resto de usuarios con estos permisos estén exentos de poder ser utilizados por el atacante como vía de acceso mediante el exploit.

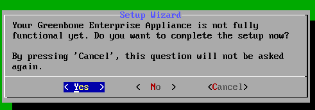
Se recomienda encarecidamente eliminar los permisos de escritura de los usuarios del FTP hasta que salga el parche que solucione la vulnerabilidad.

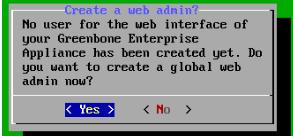
Microsoft aún no ha publicado ningún parche que solucione el problema, aunque se espera que, debido a la gravedad de la vulnerabilidad, lo haga pronto.

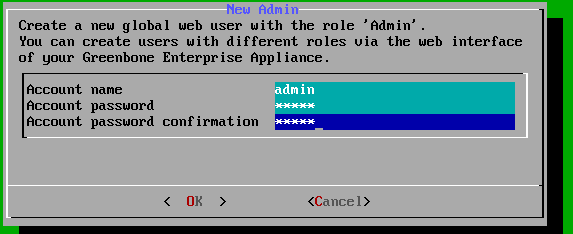
**HTTP:** Tal es el caso, como hemos podido saber, con [la vulnerabilidad CVE-2022-21907](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907), que afecta a la pila de red de HTTP de [Windows](https://www.muyseguridad.net/tag/windows/). Esto es lo que podemos leer en la página publicada por Microsoft para informar de esta vulnerabilidad y, al tiempo, ofrecer las medidas necesarias para mitigar el riesgo:

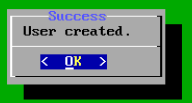
«El componente vulnerable está vinculado a la pila de red y el conjunto de posibles atacantes se extiende más allá de las otras opciones enumeradas, hasta e incluyendo todo Internet. Una vulnerabilidad de este tipo suele denominarse «explotable de forma remota» y puede considerarse como un ataque explotable a nivel de protocolo a uno o más saltos de red (por ejemplo, a través de uno o más routers).»

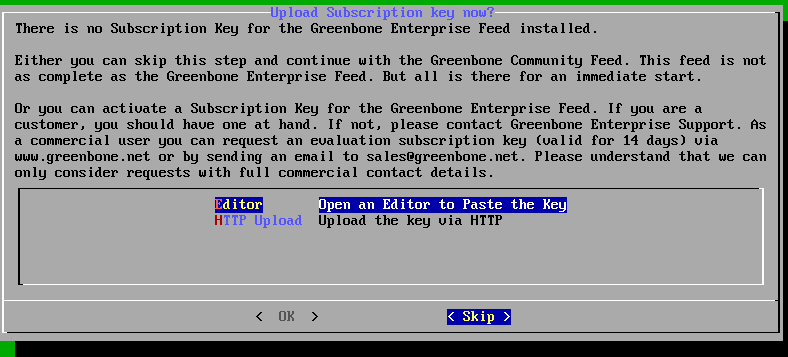
6. Realizar un análisis de vulnerabilidades con OpenVAS (https://www.openvas.org/) En Linux: sudo apt-get install openvas, openvas-setup, openvas-start



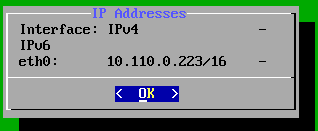


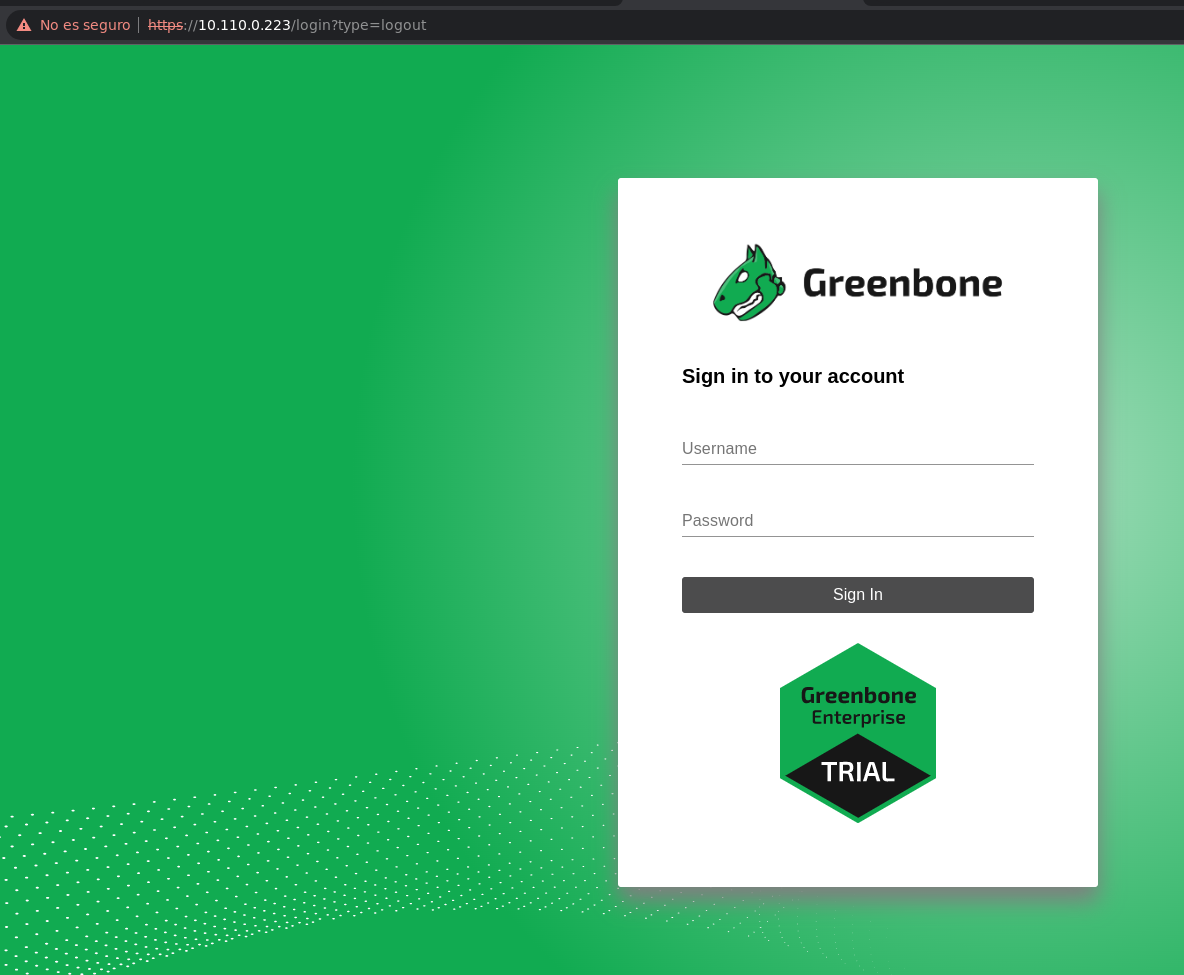


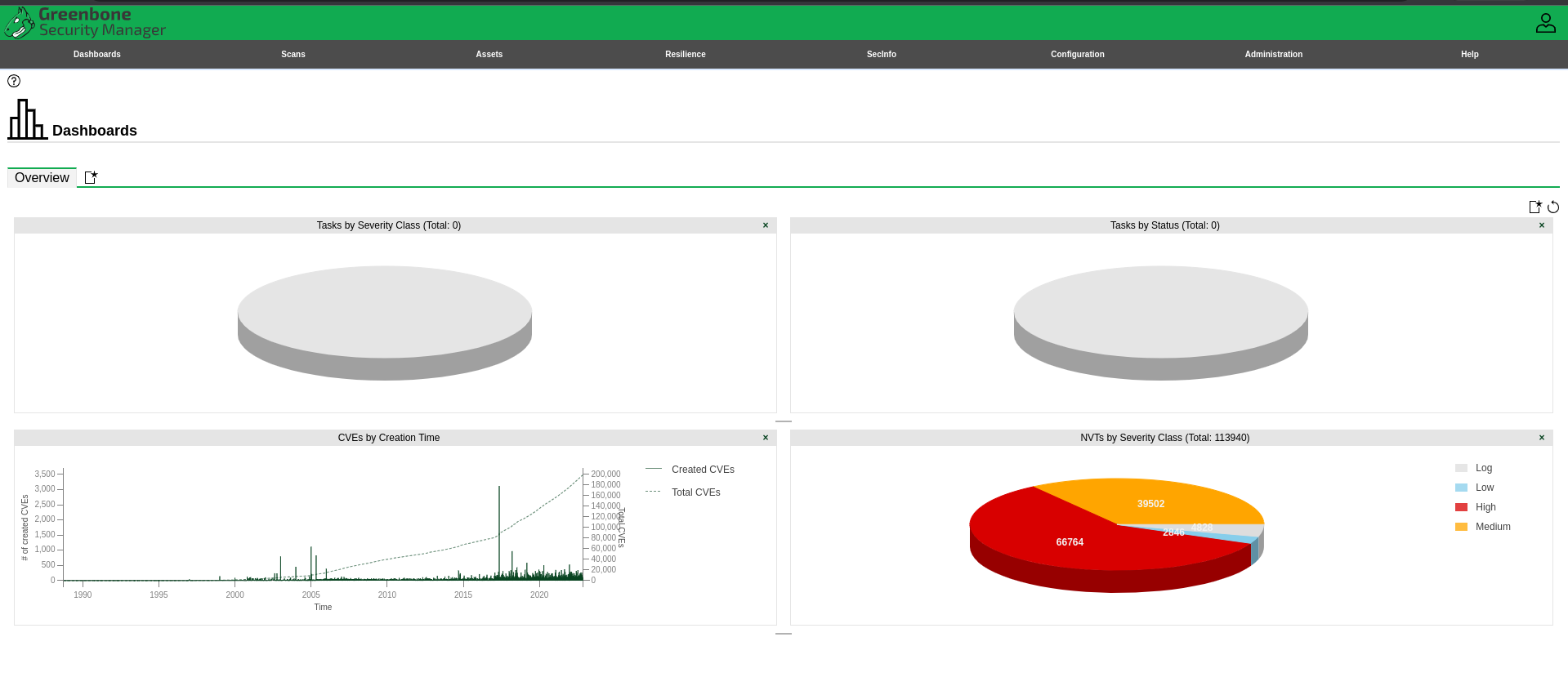




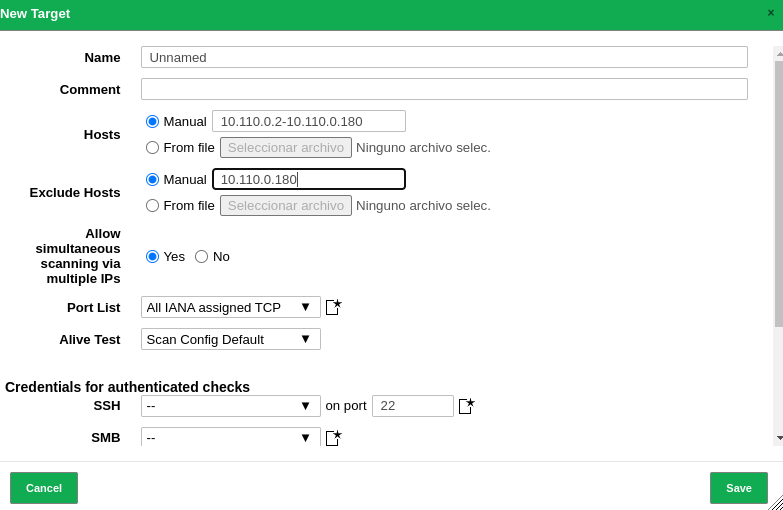
**SETUP>NETWORK>IP**

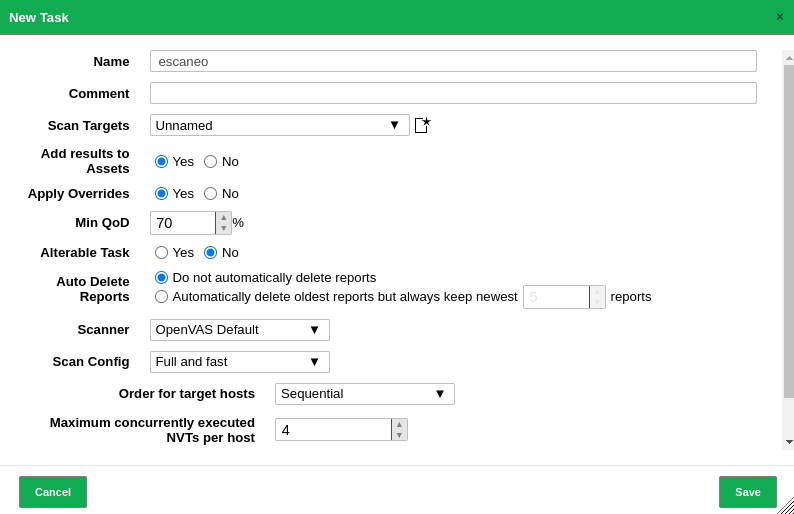


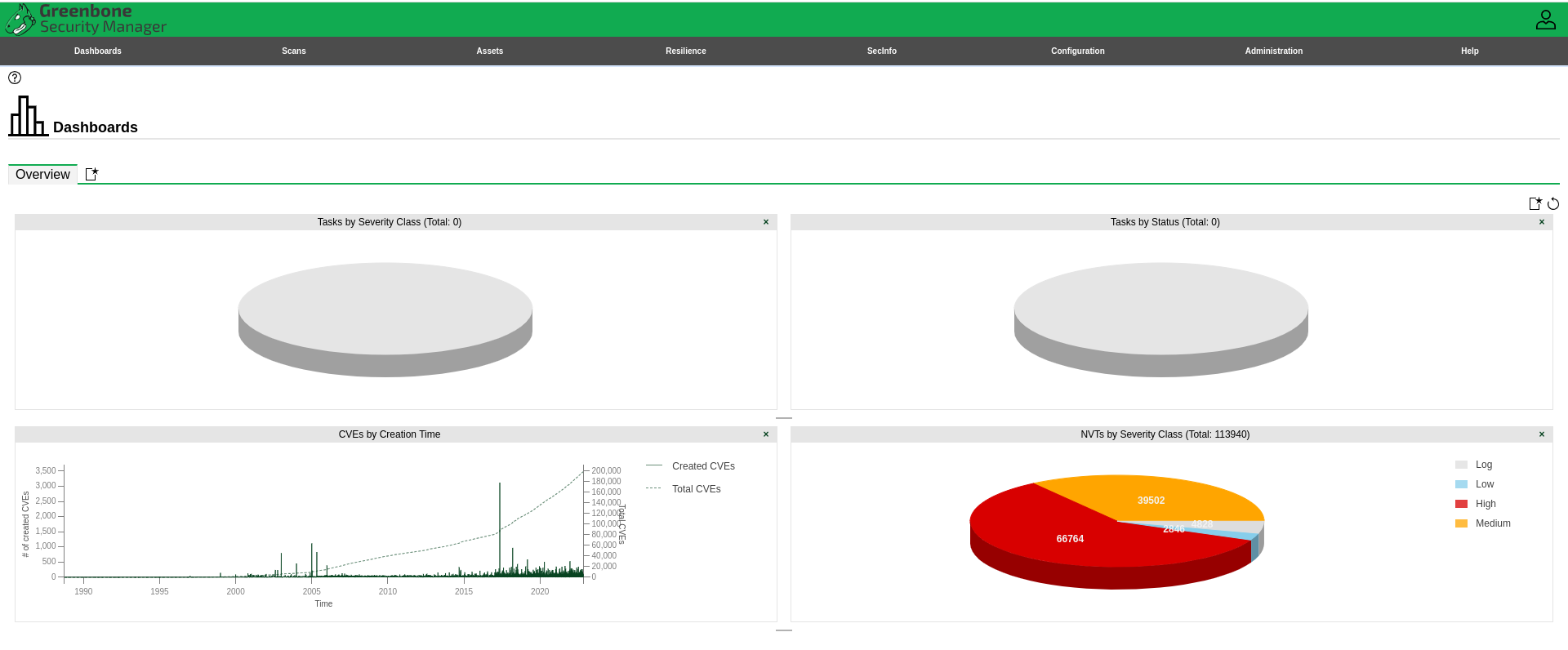




**Crear una scans-task y poner las opciones que queremos:**







7. (opcional) Utilizando Netcap conseguir abrir remotamente una consola cmd en un Windows sin necesidad de autenticación.