4. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

HERRAMIENTAS DEL SISTEMA OPERATIVO TIPO PING, TRACEROUTE, ETC.

Los comandos tanto de Windows como de Linux en general el uso de la consola de comandos, no eres nadie, ya que no todo es Metasploit, y los comandos son muy importantes tanto es las fases de recopilación de información sobre nuestro objetivo como en el momento en que ya tenemos acceso al equipo comprometido. Por otra parte, también **es importante un gran conocimiento a cerca del funcionamiento de los protocolos, sus cabeceras y en general de redes**.

Ping

Ping (Packet Internet Groper) Permite comprobar el estado de la comunicación del host local con uno o varios equipos remotos de una red. Por medio del envío de paquetes ndel protocolo **ICMP**, diagnostica el estado, conectividad, velocidad y calidad de una red determinada.

Ping es un comando del protocolo de **capa 3** del modelo **OSI ICMP**, que son las siglas de **Internet Control Message Protocol**, que se encarga de revisar y notificar si hay errores en la comunicación entre dos hosts y/o redes. Para ello, **ICMP** envía 3 paquetes al destino, y en base a lo que suceda en el origen obtendrá una respuesta.

Dentro de la cabecera de **ICMP** hay una serie de campos que contienen código y tipo de respuesta, y según el valor que tengan tendremos un diagnóstico.

	Bit 0–7	Bit 8–15	Bit 16–23	Bit 24–31
0	Tipo	Código	Suma de verificación	
32	Datos sobre la cabecera			

Para simplificar, cuando hacemos un ping a un equipo, enviamos 4 paquetes, y esperamos recibir la confirmación por parte del destino de la recepción de esos cuatro paquetes, con lo que establecemos que tenemos conectividad con el equipo, como ves en el siguiente ejemplo:

```
C:\Users\silvia.menendez>ping google.com

Haciendo ping a google.com [172.217.168.174] con 32 bytes de datos:
Respuesta desde 172.217.168.174: bytes=32 tiempo=3ms TTL=54
Respuesta desde 172.217.168.174: bytes=32 tiempo=4ms TTL=54
Respuesta desde 172.217.168.174: bytes=32 tiempo=3ms TTL=54
Respuesta desde 172.217.168.174: bytes=32 tiempo=3ms TTL=54

Estadísticas de ping para 172.217.168.174:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 3ms, Máximo = 4ms, Media = 3ms
```

Las respuestas de **ICMP** pueden indicar otros estados, como por ejemplo host de destino inaccesible, host inalcanzable, etc.

Este campo puede tomar los siguientes valores cuyo significado es:

- 0 Respuesta de eco (**Echo Reply**).
- 3 Destino inaccesible (**Destination Unreachable**).
- 4 Disminución del tráfico desde el origen (**Source Quench**).
- 5 Redireccionar (cambio de ruta) (**Redirect**).
- 8 Solicitud de eco (**Echo**).
- 11 Tiempo excedido para un datagrama (**Time Exceeded**).
- 12 Problema de Parámetros (**Parameter Problem**).
- 13 Solicitud de marca de tiempo (**Timestamp**).
- 14 Respuesta de marca de tiempo (**Timestamp Reply**).
- 15 Solicitud de información (obsoleto) (**Information Request**).
- 16 Respuesta de información (obsoleto) (**Information Reply**).
- 17 Solicitud de máscara (**Addressmask**).
- 18 Respuesta de máscara (**Addressmask Reply**).

En color verde están marcados los que habitualmente te vas a encontrar más a menudo.

Ping también dispone de algunos parámetros interesantes que podemos obtener solicitando la ayuda en la consola de comandos como puedes observar a continuación. En Linux tendrías que poner **ping -h.**

Es muy común el uso de **-t**, con el que haremos un ping continuo hasta que queramos pararlo pulsando las teclas CTRL+C, en Linux no es necesario porque esta es la opción por defecto, pero en Windows como ya vimos por defeco se envían sólo 4 paquetes ICMP. Esta opción es útil cuando se quieren observar fallos intermitentes en la red y latencias.

Ping -t Google.es

Otra opción es enviar un número concreto de paquetes por ejemplo 100, con el modificador **-n** y el número de paquetes a enviar que oscila entre los valores 0-4.294.000.000

Ping -n 100 google.es

Con **-l** modificamos el tamaño del paquete que enviamos, siendo el nº máximo 65500, al enviar paquetes más grandes ponemos a prueba la tarjeta de red.

Con el parámetro **-i** modificamos el TTL, tiempo de vida (time to live) del paquete, los valores permitidos son de 0 a 255.

Ping -i 200 google.es

Otro de los parámetro o modificador interesante es **-f**, que establece que no se debe fragmentar el paquete.

Ping -f Google.es

En el siguiente enlace se explica el protocolo:

Protocolo de control de mensajes de Internet

Tracert

Tracert nos permite conocer la ruta que siguen los paquetes hasta llegar a su destino y también es un comando del protocolo **ICMP**.

También obtenemos una estadística del RTT, tiempos de ida y vuelta o latencia de red de esos paquetes, que corresponden al envío de 3 paquetes ICMP, ofreciendo una estimación de la distancia en saltos, o routers por los que se pasa, a la que están los extremos de la comunicación.

Esta utilidad de diagnóstico de red determina la ruta a un destino mediante el envío de paquetes de eco de Protocolo de mensajes de control de Internet (ICMP) al destino.

En estos paquetes, TRACERT usa valores de período de vida, conocido como TTL por sus siglas en inglés Time to Live. Dado que los enrutadores de la ruta deben disminuir el TTL del paquete como mínimo una unidad antes de reenviar el paquete, el TTL es, en realidad, un contador del número de saltos o routers por los que vamos pasando.

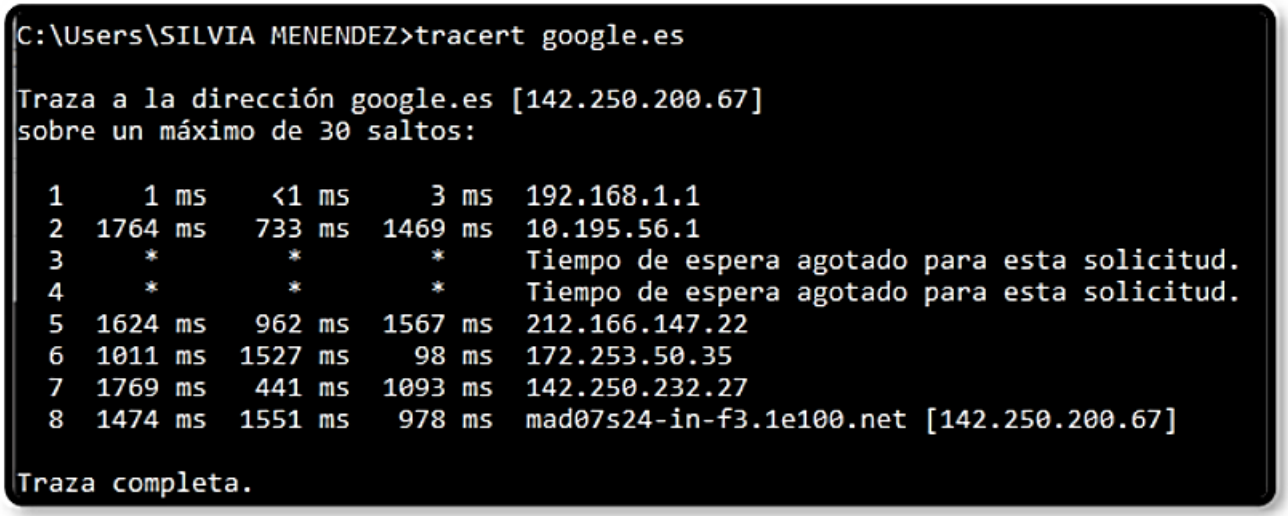
Cuando el TTL de un paquete alcanza el valor cero, el router devuelve al equipo de origen un mensaje ICMP de “Tiempo agotado para esta solicitud”, ya que el paquete no ha podido llegar a su destino y ha expirado en tránsito.

Con tracert /? Obtenemos la ayuda del comando.

El modificador **-d** le indica a TRACERT que no haga la resolución DNS de forma que nos devuelve la dirección IP de los routers por los que paso.

TRACERT es útil a la hora de solucionar problemas en redes propias donde tengamos varios routers y se pueden tomar varias rutas para llegar a un destino, de forma que podemos observar dónde podemos tener un problema en la red.

En la siguiente imagen puedes observar un tracert hecho a Google, donde podemos observar que hecha la solicitud al dominio Google.es nos devuelve mediante la resolución DNS su dirección IP, posteriormente nos indica que va a realizar la traza sobre un máximo de 30 saltos, o router por los que como máximo va a pasar, luego propiamente encontramos la traza realizada siendo el primer salto nuestro propio router, como observas nos dice en cada línea el nº de salto, después los tiempo de ida y vuelta RTT o latencias y a continuación la dirección IP del router por el que pasamos.



En el salto nº 8 vemos que ya hemos llegado a nuestro destino ya que la IP que nos muestra es la misma que nos daba la resolución DNS al principio.

En la traza anterior también puedes observar que en los saltos 3 y 4 los RTT se marcan con un asterisco, esto no es sinónimo de un error, sino que por seguridad muchos servidores y routers tienen deshabilitado el protocolo ICMP, para evitar ataques de denegación de servicio mediante este protocolo.

Pathping

Pathping es una mezcla de **ping** y **tracert**.

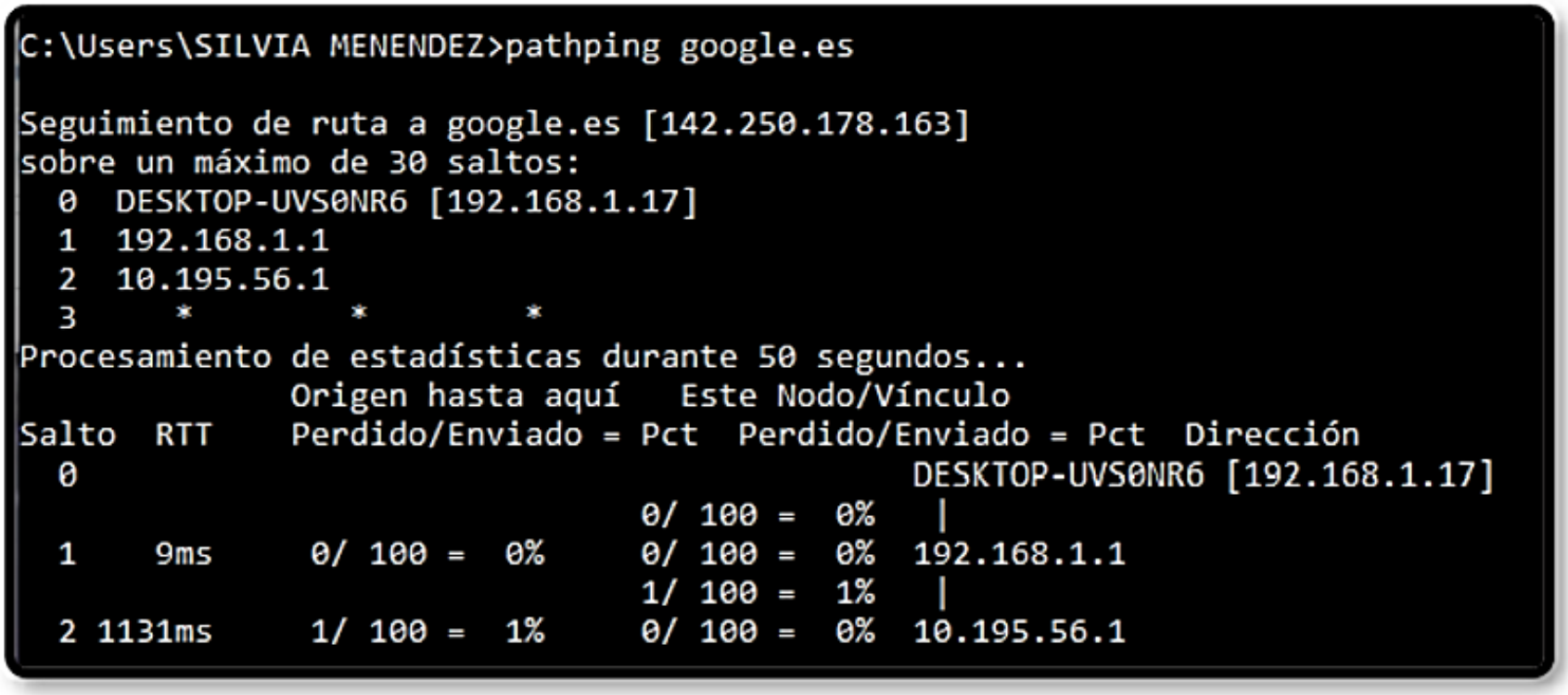
Es más informativo, ya que nos devuelve también una serie de estadísticas, por lo que tarda más tiempo para ejecutar. Después de enviar los paquetes a un destino determinado, se analiza la ruta tomada y se calcula la pérdida de paquetes, proporcionando detalles entre dos hosts.

Muestra la ruta a un host TCP/IP y las pérdidas de paquetes en cada enrutador del camino, además de información acerca de la latencia de red y pérdidas en saltos intermedios entre origen y destino.

Pathping envía varios mensajes de solicitud de eco mediante el protocolo **ICMP** a cada enrutador entre un origen y destino durante un período de tiempo y, a continuación, calcula los resultados en función de los paquetes devueltos desde cada enrutador.

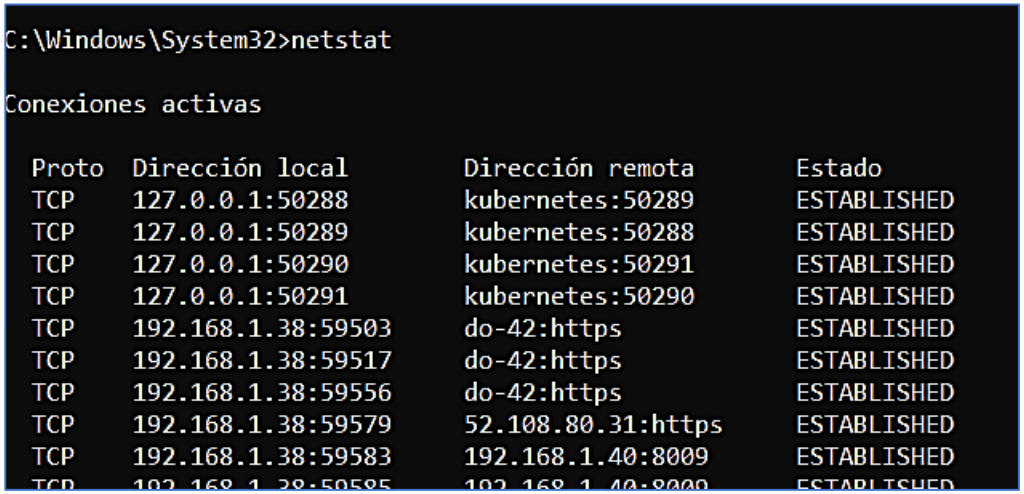
El **modificador -n** Impide la resolución DNS de las direcciones IP, lo que acelera la presentación de los resultados.

Con **-h** especificamos el número máximo de saltos para llegar al destino, el valor predeterminado es 30 saltos.



Netstat

Netstat me permite conocer las conexiones establecidas en el momento de su ejecución, indicando protocolo (TCP), direcciones en formato socket de origen y destino y el estado de la conexión.



Añadiendo el modificador **-b** podemos ver el ejecutable asociado.

Con el modificador de netstat “Interval”, podemos especificar un intervalo en segundos en que netstat se ejecute de nuevo con lo que la información se refresca y nos muestra los nuevos datos, ya que por este comando sólo muestra el resultado en el momento que se realiza, así que sería una forma de hacerlo más “en tiempo real” cuando queremos observar que sucede con determinadas conexiones.

Whois

Whois es un protocolo de comunicación entre los" regional internet registries", que almacenan información de registro sobre direcciones ip o dominios. Es un protocolo TCP.

A través de whois podemos obtener cierta información sobre la organización, aunque a día de hoy poquito debido a la protección de datos, aunque en algunos casos con suerte puedes encontrar información sobre quien ha registrado un dominio, correos, teléfono, etc.

Podemos hacer whois a una ip o a un dominio, y son cosas totalmente distintas, una es el registro del dominio y otra es el registro de la IP.

El comando whois ya no funciona en Windows, si en Linux, pero existen multitud de aplicaciones online que nos facilitan esta tarea.

Aplicaciones web para hacer whois:

- Netcraft: https://www.netcraft.com/
- Domaintools.com: https://whois.domaintools.com/
- ICANN: https://whois.icann.org/es

Nslookup

Se emplea para conocer si el DNS está resolviendo correctamente los nombres de dominio y las IPs. También nos permite averiguar la dirección IP detrás de un determinado nombre de dominio.

Puedes obtener la ayuda del comando una vez estás dentro de nslookup con help.

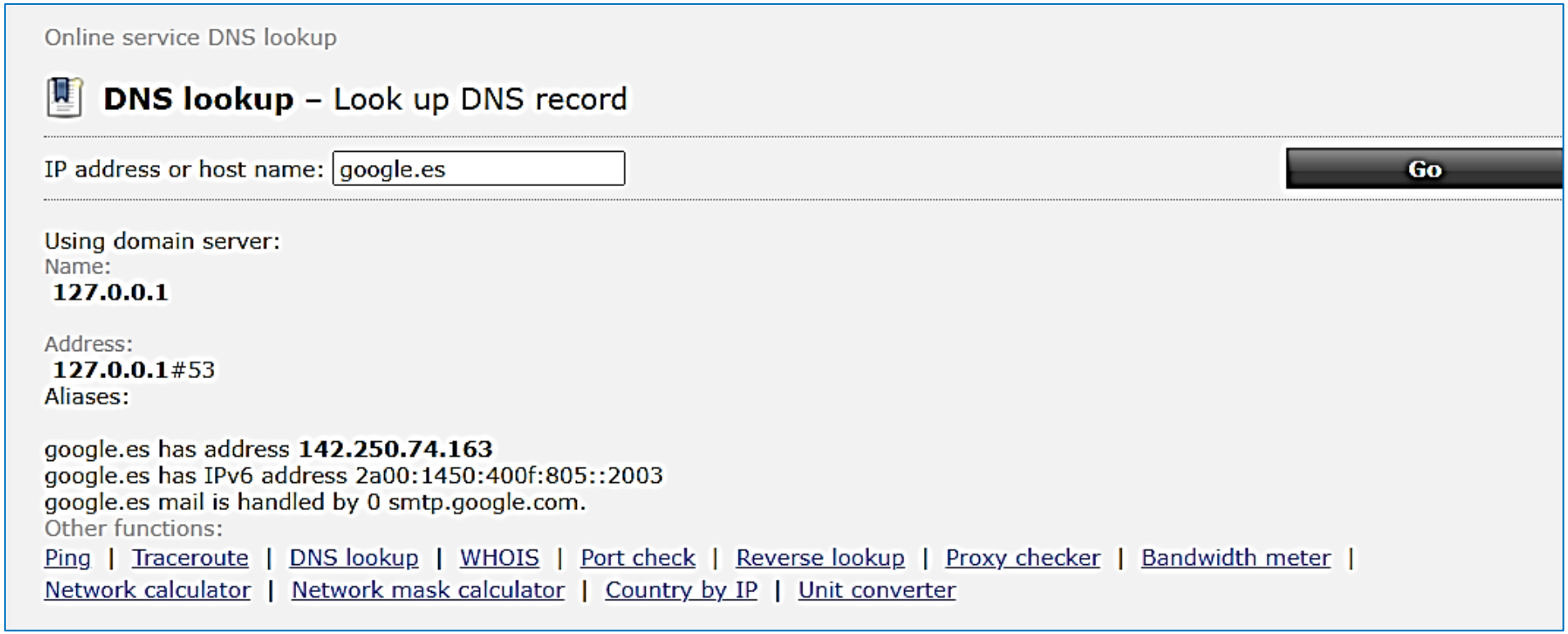
En principio, nslookup está pensado para las consultas de direcciones IPv4 e IPv6. Sin embargo, también nos permite conocer información de otros tipos registros DNS, para ello, una vez dentro de la aplicación escribimos set type y el registro que se quiere conocer sobre el nombre de dominio indicado en la segunda línea.

La sintaxis de este comando de nslookup muestra el esquema que sigue:

set type=TIPODEREGISTRO

En la parte “TIPODEREGISTRO” se introduce el tipo de petición que se desea, entre los que se pueden encontrar:

Disponemos de herramientas nslookup online como ping.eu y centralops.net, además ambas ofrecen herramientas de red adicionales como Traceroute y Whois.



Dig

El comando que puedes usar en Linux es **Dig (Domain information groper).**

Ejemplos de uso con DIG:

Dig xxx.com

Nos muestra las IP, de tipo A.

Dig mx xxx.com

Muestra direcciones ip de servidores Mx (de correo).

Dig ns xxx.com

Muestra ip, servidores de nombre de servidor principal y subdominios.

NS =servidor de nombre.

A= IP

Enumeración de sistemas mediante DNS.

Dig @8.8.8.8 xxx.com A.

@8.8.8.8 servidor al que se pregunta, resuelve sólo direcciones de tipo A usando un determinado DNS

Obtener distintos tipos de registro DNS.

Dig @208.67.222.222 Google.com A.

Obtener los servidores de nombres.

Dig @208.67.222.222 Google.com NS.

Obtener registros MX (de correo).

Dig @208.67.222.222 Google.com MX.

Obtener todos los tipos de registros en 1 misma consulta.

Dig any Google.com

Realizar una consulta inversa.

Dig –x 173.194.34.233

Transferencia de zona con DIG

Dig @ns1.midominio.net axfr midominio.net

Ipconfig

Con **ipconfig** podemos realizar varias cosas mediante sus modificadores, pero lo más habitual es usarlo para conocer la configuración TCP/IP de una forma simple solo escribiendo **ipconfig**, nos devuelve nuestra IP, la máscara de red y puerta de enlace del router, y **con ipconfig /all** vemos una configuración más completa.

También nos permite liberar y renovar las direcciones ip que han sido asignadas mediante un servidor dhcp con los modificadores **/release**, y **/renew** para todos los adaptadores de red o para uno específico.

Ejemplos:

ipconfig

Muestra información TCP/IP de todos los adaptadores de red.

ipconfig /all

Muestra información TCP/IP detallada de todos los adaptadores de red.

ipconfig /renew.

Renueva la IP de todos los adaptadores asignada mediante dhcp.

ipconfig /renew EL*

Renueva cualquier conexión cuyo nombre comience con EL.

ipconfig /release *Con*

Libera todas las conexiones coincidentes, por ejemplo: “Conexión cableada Ethernet 1” o “Conexión cableada Ethernet 2”. Solo para direcciones IP asignadas mediante dhcp.

Windows almacena la cache de resolución DNS, es decir la relación que existe entre las direcciones IP y los sitios visitados con sus nombres de dominio, de forma predeterminada se renueva cada 24 minutos.

IPCONFIG /displaydns: muestra el contenido de la caché de resolución DNS.

IPCONFIG /flushdns: vacía la memoria caché de resolución DNS.

IPCONFIG /registerdns: actualiza todas las concesiones DHCP y vuelve a registrar los nombres DNS.

Getmac

Getmac obtiene la MAC del equipo donde se ejecuta.

La dirección MAC es un identificador único para cada dispositivo de red de 48 bits conocida también como dirección física y que es única para cada dispositivo. Sus siglas vienen del inglés, y significan Media Access Control.

Las direcciones MAC están formadas por 48 bits representados generalmente por dígitos hexadecimales, como cada hexadecimal equivale a cuatro binarios (48:4=12), la dirección acaba siendo formada por 12 dígitos agrupados en seis parejas separadas generalmente por dos puntos, aunque también puede haber un guion o nada en absoluto.

De esta manera, un ejemplo de dirección MAC podría ser 00:1e:c2:9e:28:6b.

Otra cosa que tienes que tener en cuenta, es que la mitad de los bits de una dirección MAC, tres de las seis parejas, identifican al fabricante, y la otra mitad al modelo.

Por ejemplo, los números 00:1e:c2 del ejemplo de dirección pertenecen siempre al fabricante (OUI) Apple Inc, mientras que los últimos seis determinan el ID de dispositivo.

La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos.

Hay buscadores especializados para saber el fabricante de un dispositivo dependiendo de los primeros seis dígitos de su MAC.

COFFER

MACVENDORS

Como son identificadores únicos, las MAC pueden ser utilizadas por un administrador de red para permitir o denegar el acceso de determinados dispositivos a una red.

En teoría son fijas para cada dispositivo, aunque existen maneras de cambiarlas, inicialmente no porque la MAC se encuentra grabada en una memoria ROM en el hardware del dispositivo, pero al iniciar el equipo, el firmware pasa esta información a la memoria RAM, y por tanto ya es la podemos tratar como algo lógico en lugar de físico, y es aquí donde podemos modificarla, para que nuestro equipo no sea reconocible, esto también se conoce como suplantar la dirección MAC o MAC Spoofing.

Arp -a

El comando **ARP** resulta útil para visualizar la caché de resolución de direcciones, conocida como caché arp, que son básicamente los equipos con los que se ha comunicado mi equipo en la red (LAN).

Muestra y modifica las tablas de traducción de direcciones **IP** a direcciones físicas usadas por el protocolo de resolución de direcciones **ARP**.

El Address Resolution Protocol se describe en la RFC 826 donde explica cómo se lleva a cabo la resolución de direcciones IPv4 en direcciones MAC.

ARP es imprescindible para la transmisión de datos en redes Ethernet por dos razones: por un lado, las tramas de datos (también tramas Ethernet) de los paquetes IP solo pueden enviarse con ayuda de una dirección de hardware a los hosts de destino, pero el protocolo IP no puede obtener estas direcciones físicas por sí mismo.

En caso de querer añadir la combinación de direcciones de un host o eliminarla de la **usaremos -s** y **-d**. Se puede crear una nueva entrada estática con el siguiente comando:

arp -s 10.0.2.15 00-aa-00-62-c6-09

También se puede eliminar esta información de la caché arp con -d (delete)

arp -d 10.0.2.15

Netsh

Netsh significa shell de red, permite modificar, administrar y diagnosticar la configuración de una red. Tenemos que ejecutarlo con permisos de administrador en la consola de comandos (CMD).

Netsh, es una aplicación muy extensa, que nos permite configurar el firewall, especificar rangos de puertos dinámicos tanto para UDP como para TCP, ver claves WIFI almacenadas, configurar el protocolo TCP/IP, entre otras muchas acciones.

En el siguiente ejemplo, podemos ver las interfaces de red del equipo.

netsh interface show interface

Asignar ip estática a una interfaz de red

netsh interface ipv4 set address “Wi-Fi”static 192.168.1.40 255.255.255.0 192.168.1.1

Donde:

Interface IPv4 indica el tipo de interfaz a configurar.

Set address «Wi-Fi»: selecciona la dirección IP de la interfaz llamada en este caso «Wi-Fi».

Static: indicamos que la dirección IP se asignará de forma fija o estática aportando los valores de IP, máscara y puerta de enlace del router.

Configuración de red de la interfaz Wi-Fi dinámica mediante DHCP

netsh interface ipv4 set address “Wi-Fi” dhcp
netsh interface ipv4 set dnsservers “Wi-Fi” dhcp

Mostrar la configuración solo para el interfaz de nombre Wi-Fi:

netsh interface ipv4 show address Wi-Fi
netsh interface ipv4 show dns Wi-Fi

Ver perfiles de red Wi-Fi

netsh wlan show profiles

Desplegar los perfiles de una sola interfaz.
netsh wlan show profiles interface=”nombre_**interfaz”**

CONOCER LA CONFIGURACIÓN DEL ADAPTADOR WI-FI

Conocer en detalle la configuración del controlador es importante en tareas de soporte ya que nos permiten saber con el soporte necesario. Podemos ver detalles específicos tales como nombre, dirección MAC, tipo de red, versión Wi-Fi, canal actual, porcentaje de la señal, velocidad de recepción, etc.

netsh wlan show interfaces

Recuperar claves de seguridad de perfiles almacenados

En algunas situaciones es posible que hayamos olvidado la clave de seguridad de un perfil WIFI:

netsh wlan show profile name=”Perfil” key=clear

Borrar un perfil de red Wi-Fi

Si tenemos almacenados diversos perfiles a los que ya no nos conectamos, una solución es eliminarlos para evitar conexiones fallidas.

netsh wlan delete profile name=”nombre de perfil”.

Hostname

El comando hostname es muy simple y no tiene modificadores, nos muestra el nombre del host, o lo que es lo mismo el nombre del equipo.

Route

El comando Route permite ver y modificar la tabla de rutas.

Route print muestra todo el contenido de la tabla de enrutamiento IP.

Route add se utiliza para añadir rutas a la tabla, y route delete se utiliza para borrar rutas de la tabla.

Nbtstat

Muestra estadísticas del protocolo y conexiones TCP/IP actuales utilizando NBT (NetBIOS sobre TCP/IP). NBTStat es una herramienta que resulta de utilidad para solucionar problemas con la resolución de nombres llevada a cabo por NetBIOS.

Nbtstat se puede usar en redes WiFi públicas para recopilar todas las direcciones IP y utilizarlas en la fase de recopilación de información llamada footprinting o en un ataque a cualquier dirección IP pública, se pueden usar para enumerar todas las conexiones TCP/IP en la máquina de Windows y para solucionar problemas con la resolución de nombres.

-n: muestra nombres locales NetBIOS.

HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS: NMAP

En este apartado, nos vamos a centrar en el uso de un escáner de puertos, como es **NMAP**, uno de los más usados, aunque no el único.

Nmap es una herramienta con la que podemos escanear puertos y redes para comprobar que puertos están abiertos, servicios que corren tras esos puertos, si está el host detrás de un cortafuegos, el Sistema Operativo de los hosts en la red, las versiones de las aplicaciones que están detrás de los puertos, identificar equipos activos en la red, y obtener sus direcciones MAC, entre otras muchas más posibilidades.

Tenemos una versión gráfica y una de comandos, Zenmap y Nmap, ambas tanto para Windows como para Linux, en el framework Kali Linux ya la tienes instalada, pero quizás no uses Kali, y tal vez te hayas creado tu propio framework con las herramientas que te interesan en un entorno Ubuntu, por ejemplo, en ese caso tendrás que instalarla.

La instalación en Windows es igual de sencilla que para cualquier otra aplicación, puedes dejar los valores que vienen por defecto.

En el caso de Linux:

Instalar Zenmap: sudo apt-get install zenmap.

Actualizar e instalar nmap: apt-get update && apt-get install nmap.

Para ejecutar nmap o zenmap:

Sudo nmap.

Sudo zenmap.

Encontrarás la aplicación para descargar en la web de nmap.org.

Enlace Web a descarga NMAP: https://nmap.org/download.html

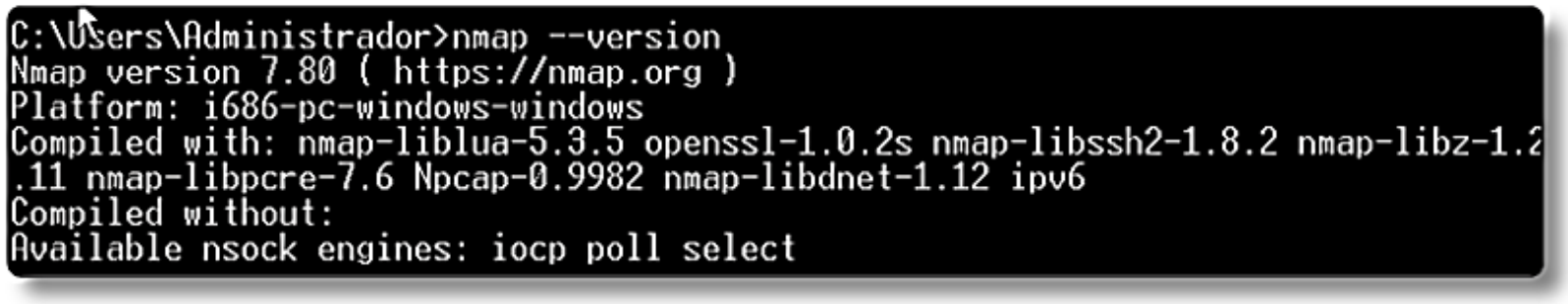
Antes de nada, una ADVERTENCIA, realizar escaneos de red, así como el uso de otras herramientas de hacking ético sin autorización expresa de la empresa, es decir, sólo si vas a realizar una auditoría con permiso, ES ILEGAL.

Puedes practicar el uso de Nmap con máquinas virtuales, en tu propia red, con máquinas y webs especialmente diseñadas para que practiques con ellas, o en el enlace para tal efecto proporcionado por Nmap: scanme.nmap.org.

Ahora sí, entremos en materia:

Como ya hemos dicho existen dos versiones, la gráfica y la de consola de comandos, que es la que vamos a usar aquí.

Una vez instalado Nmap, puedes comprobar que todo ha ido bien ejecutando la consola de comandos en Windows o el Terminal en Linux y simplemente escribiendo Nmap, lo que te aparecerá será la ayuda de Nmap, que también aparece si escribimos nmap - -help, igualmente podemos ejecutar nmap - -version para comprobar las versiones del propio programa y las librerías.

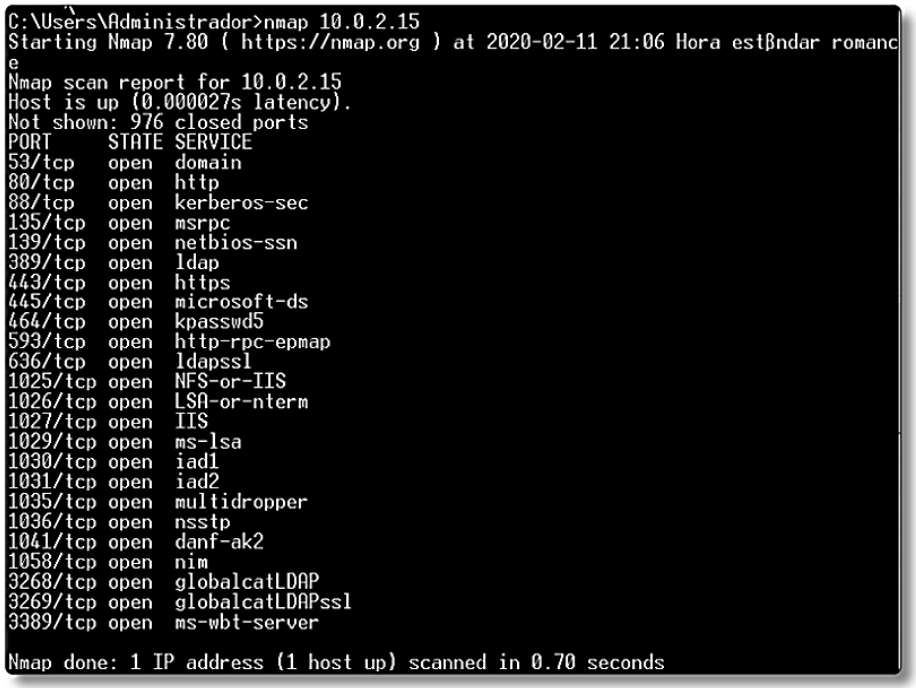


Es importante conocer la versión de los programas con los que trabajamos, ya que en una auditoría o en un análisis forense debemos especificarla, ya que según la versión que usemos podríamos obtener unos resultados u otros, y además garantiza que cualquiera que use esa misma versión puede llegar a los mismos resultados que nosotros.

Escaneo básico con NMAP

El escaneo más básico que podemos hacer con Nmap, es poner nmap junto con el nombre de dominio a escanear, dirección ip o rango de direcciones o el nombre de equipo.

Este escaneo nos devuelve la versión de nmap, fecha y hora del escaneo, internamente realiza una resolución de nombre de dominio, un Ping Arp Scan, para comprobar que el equipo está activo, y el escaneo donde se indica, puerto, estado del puerto (abierto, cerrado o filtrado) y servicio/protocolo que corre tras ese puerto.



Podemos escanear un dominio, o varios, lo mismo con las direcciones ip y los nombres de equipo.

- Escanear una IP: nmap 10.0.0.2
- Escanear varias IP no contiguas: nmap 10.0.0.2 10.0.0.10
- Escanear varias IP no contiguas separadas por comas: nmap 10.0.0.2,10,20
- Escanear un rango de direcciones IP: nmap 10.0.0.2-100
- Escanear una red completa con rangos de IP: nmap 192.168.1.1-255
- Escanear una red completa indicando la máscara de red: 192.168.1..0/24
- Escanear red completa:192.168.1.*

Generalmente la mayoría de los escaneos de nmap se hacen a los 1000 puertos más importantes, si queremos especificar un puerto o varios en concreto usamos la opción -p. veamos las distintas posibilidades.

- Escanear un único puerto: Nmap -p 80 google.es
- Escanear varios puertos no contiguos separados por comas: Nmap -p 80,443 google.es
- Escanear un rango de puertos: Nmap -p 80-3000 google.es
- Escanear todos los puertos: nmap -p- Google.es
- Escanear todos los puertos especificando el rango: nmap -p 1-65535 google.es
- Escanear rango completo de puertos: nmap -p- Google.es
- Escanear puertos UDP (implica escaneo UDP): Nmap -sU -p U:53 google.es
- Escanear puertos TCP (implica escaneo TCP): Nmap -sT -p T:80

Podemos esperar a que nmap nos muestre el resultado del escaneo o ver lo que hace en cada momento usando el modo verboso -v o con -vv para mayor información.

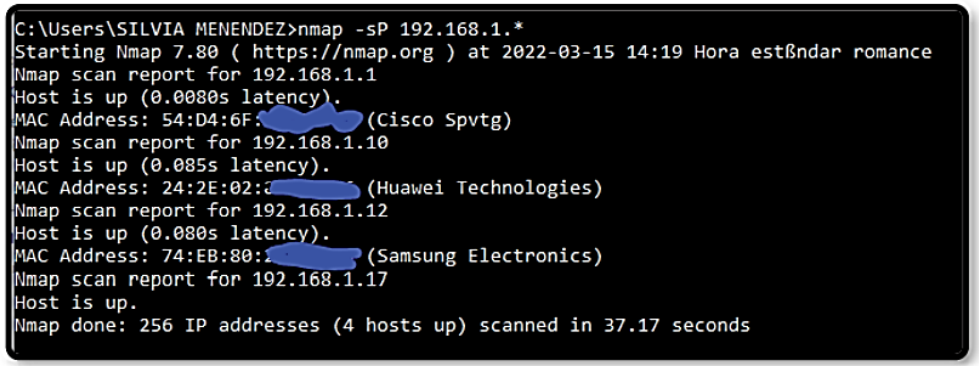
```
C:\Users\SILVIA MENENDEZ>nmap -v google.es
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-15 14:09 Hora estßndar romance
Initiating Ping Scan at 14:09
Scanning google.es (142.250.178.163) [4 ports]
Completed Ping Scan at 14:09, 0.87s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:09
Completed Parallel DNS resolution of 1 host. at 14:09, 1.41s elapsed
Initiating SYN Stealth Scan at 14:09
Scanning google.es (142.250.178.163) [1000 ports]
Discovered open port 443/tcp on 142.250.178.163
Discovered open port 80/tcp on 142.250.178.163
Completed SYN Stealth Scan at 14:09, 10.07s elapsed (1000 total ports)
Nmap scan report for google.es (142.250.178.163)
Host is up (0.062s latency).
rDNS record for 142.250.178.163: mad41s08-in-f3.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds
           Raw packets sent: 2009 (88.372KB) | Rcvd: 31 (1.364KB)
```

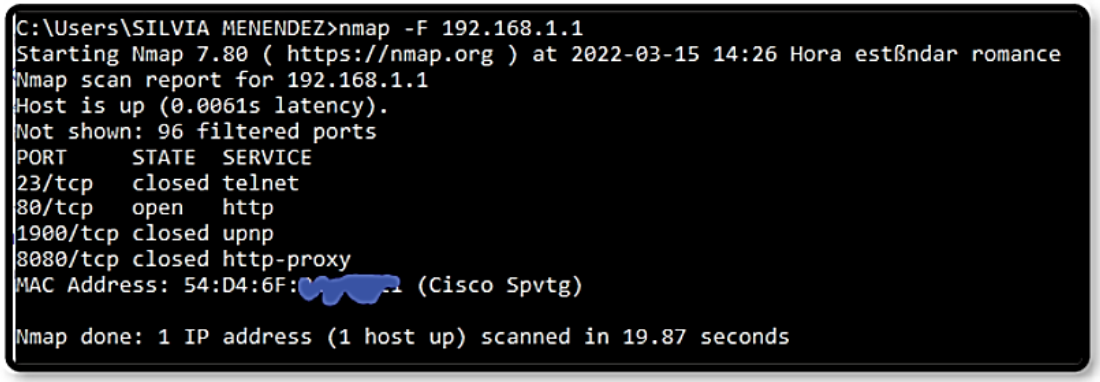
Con la opción -vv nos muestra la razón por la que los puertos están abiertos, que es porque ha recibido un SYN-ACK.

```
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT    STATE SERVICE REASON
80/tcp  open  http    syn-ack ttl 123
443/tcp open  https   syn-ack ttl 123
```

Ahora podemos comprobar los equipos que están conectados en la red haciendo un escaneo ping. En la siguiente imagen puedes observar que nos muestra los equipos activos, un equipo y dos móviles con sus respectivas direcciones MAC.



Con -F podemos realizar un Fast Scan, es decir un escaneo rápido, este tiene la particularidad de hacerlo sólo a los 100 puertos más habituales.



Con nmap - - iflist podemos listar todas las interfaces de red.

```
C:\Users\Administrador>nmap --iflist
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-11 21:07 Hora estßndar romanc
e
************************INTERFACES************************
DEV  (SHORT) IP/MASK                          TYPE        UP   MTU  MAC
lo0  (lo0)   ::1/128                          loopback    up   1500
lo0  (lo0)   127.0.0.1/8                      loopback    up   1500
eth0 (eth0)  fe80::d40d:1823:975b:2b96/64     ethernet    up   1500 08:00:27:28:48
:3B
eth0 (eth0)  10.0.2.15/24                     ethernet    up   1500 08:00:27:28:48
:3B
tun0 (tun0)  fe80::5efe:10.0.2.15/128         point2point down 1280
tun1 (tun1)  fe80::5efe:169.254.160.229/128   point2point down 1280

DEV    WINDEVICE
lo0    \Device\NPF_{3BBF4EAB-E31A-4F9C-9A34-994735361569}
lo0    \Device\NPF_{3BBF4EAB-E31A-4F9C-9A34-994735361569}
eth0   \Device\NPF_{1B3FA0D7-0BAF-444E-A03C-EB0D4B728AD9}
eth0   \Device\NPF_{1B3FA0D7-0BAF-444E-A03C-EB0D4B728AD9}
tun0   <none>
tun1   <none>
<none> \Device\NPF_NdisWanIpv6
<none> \Device\NPF_{26B3A979-9D29-46C7-A2BF-ED49D03898E1}
<none> \Device\NPF_{57B78A29-B37D-4C4E-BB9F-7CA4341A3D5E}
<none> \Device\NPF_NdisWanBh
<none> \Device\NPF_NdisWanIp

************************ROUTES************************
DST/MASK                      DEV  METRIC GATEWAY
255.255.255.255/32            eth0 266
10.0.2.255/32                 eth0 266
10.0.2.15/32                  eth0 266
169.254.160.229/32            lo0  286
169.254.255.255/32            lo0  286
255.255.255.255/32            lo0  286
255.255.255.255/32            eth0 306
127.0.0.1/32                  lo0  306
127.255.255.255/32            lo0  306
10.0.2.0/24                   eth0 266
169.254.0.0/16                lo0  286
127.0.0.0/8                   lo0  306
224.0.0.0/4                   eth0 266
224.0.0.0/4                   lo0  286
224.0.0.0/4                   eth0 306
```

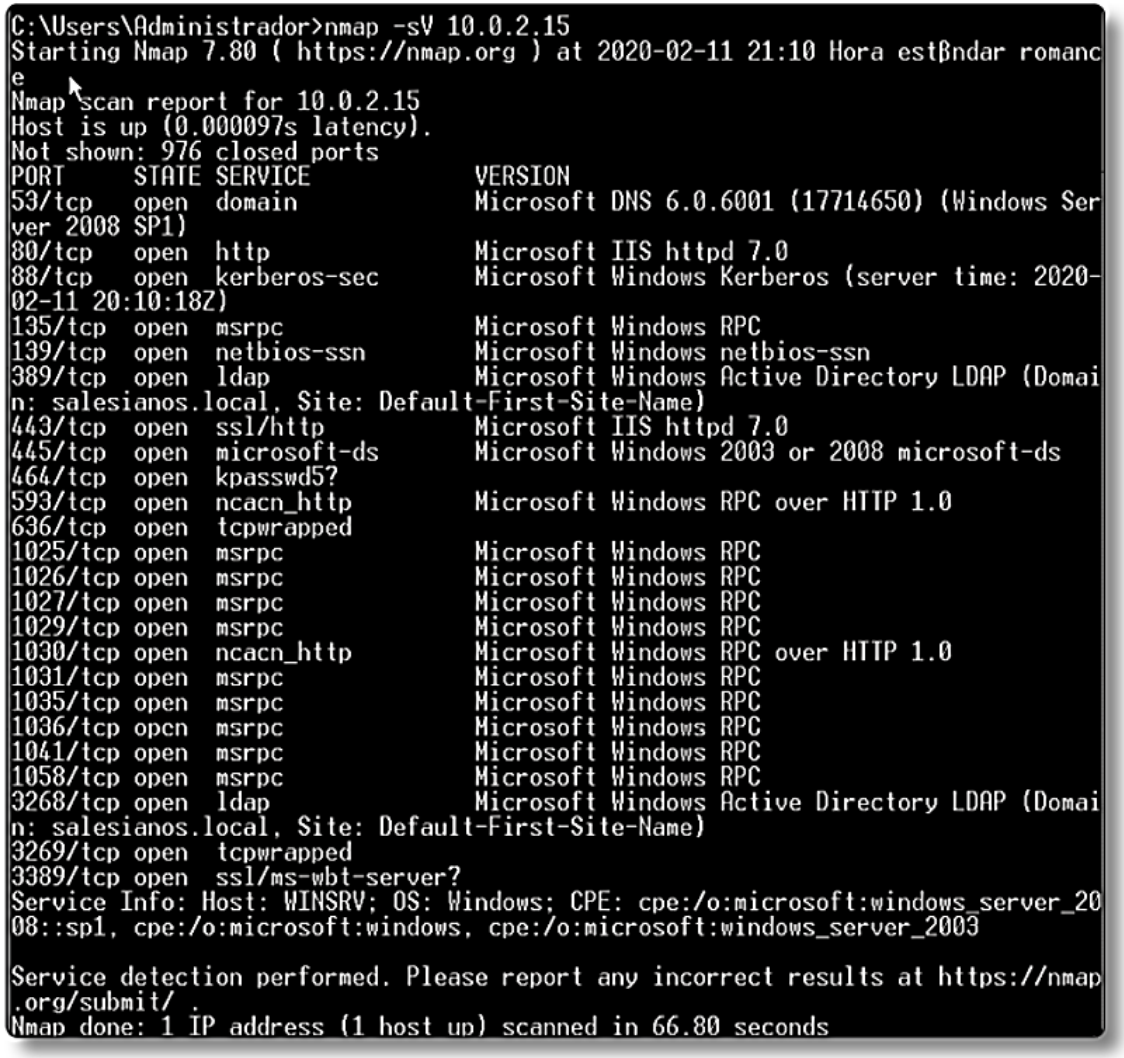
Existen varias opciones para detectar el sistema operativo del equipo remoto, una de ellas es usando -O.

```
C:\Users\SILVIA MENENDEZ>nmap -O 192.168.1.1
Starting Nmap 7.80 ( https://nmap.org ) at 2022-03-15 14:35 Hora estßndar romance
Nmap scan report for 192.168.1.1
Host is up (0.0095s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
23/tcp   closed telnet
80/tcp   open   http
1900/tcp closed upnp
8080/tcp closed http-proxy
MAC Address: 54:D4:6F:[redacted] (Cisco Spvtg)
Device type: broadband router
Running: eCosCentric eCos 2.X, Cisco embedded, Motorola embedded, Scientific Atlanta embedded
OS CPE: cpe:/o:ecoscentric:ecos:2.0 cpe:/h:cisco:epc3925 cpe:/h:cisco:dpc2320 cpe:/h:motorola:sb5101e cpe:/h:scientific_
atlanta:epc2203
OS details: Cisco EPC3925, DPC2320, Motorola SURFboard SB5101E, or Scientific Atlanta EPC2203 cable modem (eCos 2.0)
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.98 seconds
```

SI a este escaneo anterior le añadimos - -osscan-guess, obtendremos mejores resultados.

Para detectar las versiones de los servicios que corren tras los puertos, usamos -sV.



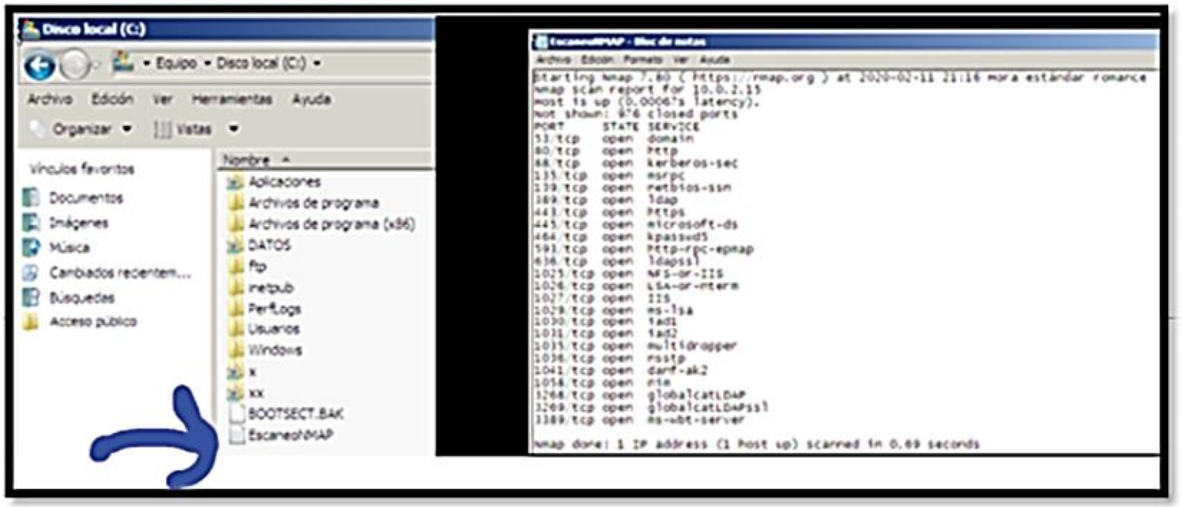
En el escaneo anterior podemos obtener más información usando - -verion-intensity pero deja más rastro en el sistema y logs de firewalls. Podemos poner valores de 0 a 5 siendo 0 un escaneo más ligero y 5 más ruidoso.

Nmap -sV - -version-intensity 5 10.0.2.15

Se hace interesante volcar los resultados del escaneo en un archivo de texto, nmap dispone de formas de hacerlo, pero una muy sencilla es redireccionar la salida del comando a un archivo de texto, puedes escribir nmap 192.168.1.17> c:\NmapEscaneo.txt, tienes que indicar la ruta donde quieres guardar el archivo.

```
C:\Users\Administrador>nmap 10.0.2.15>c:\EscaneoNMAP.txt

C:\Users\Administrador>
```



Otros escaneos interesantes son:

Lanzar un escaneo TCP SYN (opción por defecto)

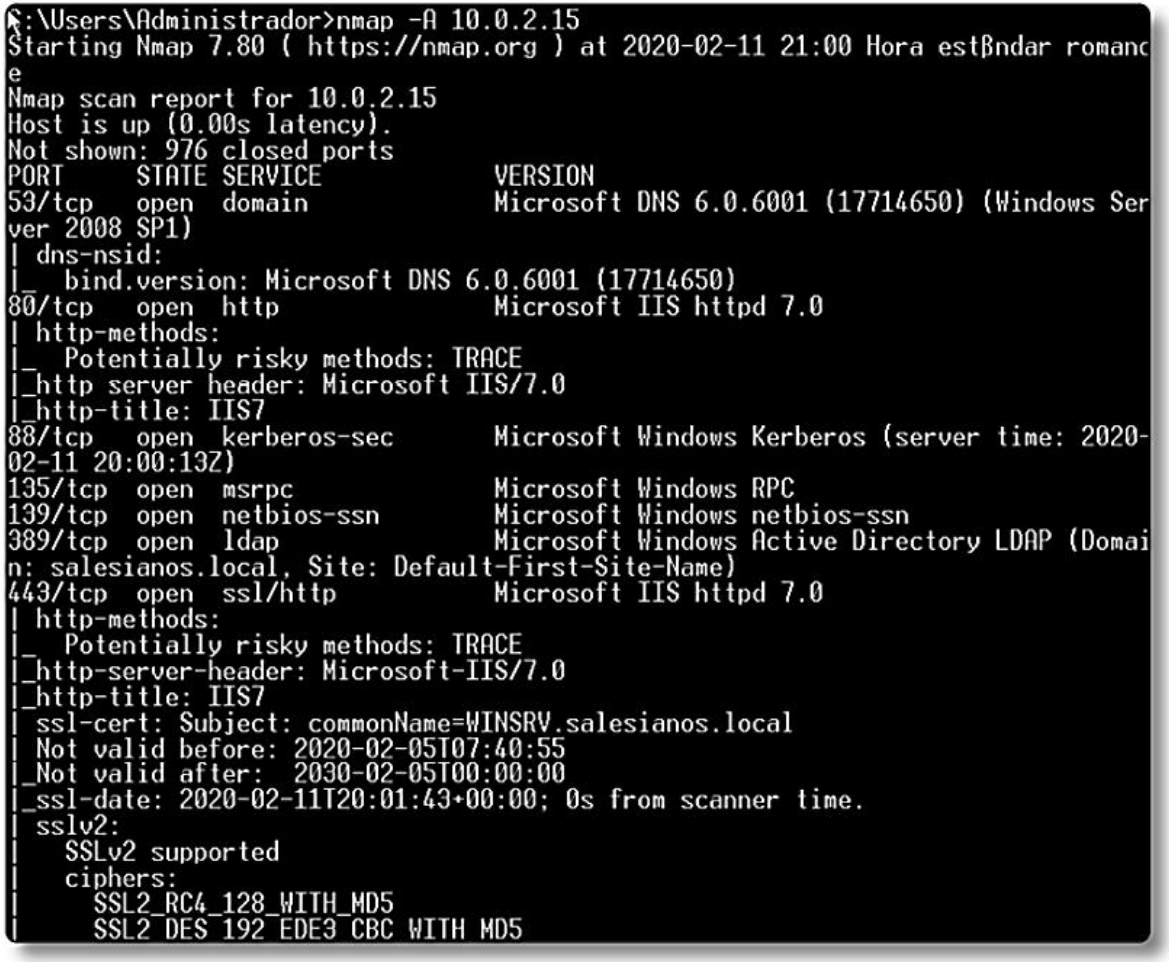
Este comando determina si el puerto remoto está abierto, conocido como escaneo half-opening, porque comienza como una conexión normal, pero no llega a establecerse un handshake por ambas partes, sino que enviamos un único paquete SYN y esperamos la respuesta.

Si nmap recibe una respuesta SYN/ACK, el puerto está abierto, y RST (reset) si está cerrado, pero no se llega a completa del 3 way handshake, es decir, nmap no envía el ACK correspondiente.

Escaneo de Sistema Operativo y servicios: modo agresivo

Este escaneo, además, lanza una serie de scripts, descubre versiones y el sistema operativo.

nmap -sS 192.168.1.17



Mostrar los puertos TCP usados más comunes utilizando TCP SYN Scan

- TCP Maimon scan

  nmap -sM 192.168.1.1

- TCP Window scan

  nmap -sW 192.168.1.1

- TCP ACK scan:

  nmap -sA 192.168.1.1

- Stealthy scan:

  nmap -sS 192.168.1.1

- Mostrar los puertos TCP usados más comunes utilizando TCP connect scan

nmap -sT 192.168.1.1

Finalmente, ya que no podemos abarcar aquí todos los escaneos de nmap, decirte que existen técnicas específicas para evadir cortafuegos y dispositivos como IDS e IPS, además de poder

realizar MAC Spoofing de tu IP para realizar el escaneo e IP Spoofing, con el fin de no ser detectados como origen del escaneo.

Escanear haciendo MAC address spoofing

nmap --spoof-mac [MAC-AQUÍ] 192.168.1.1

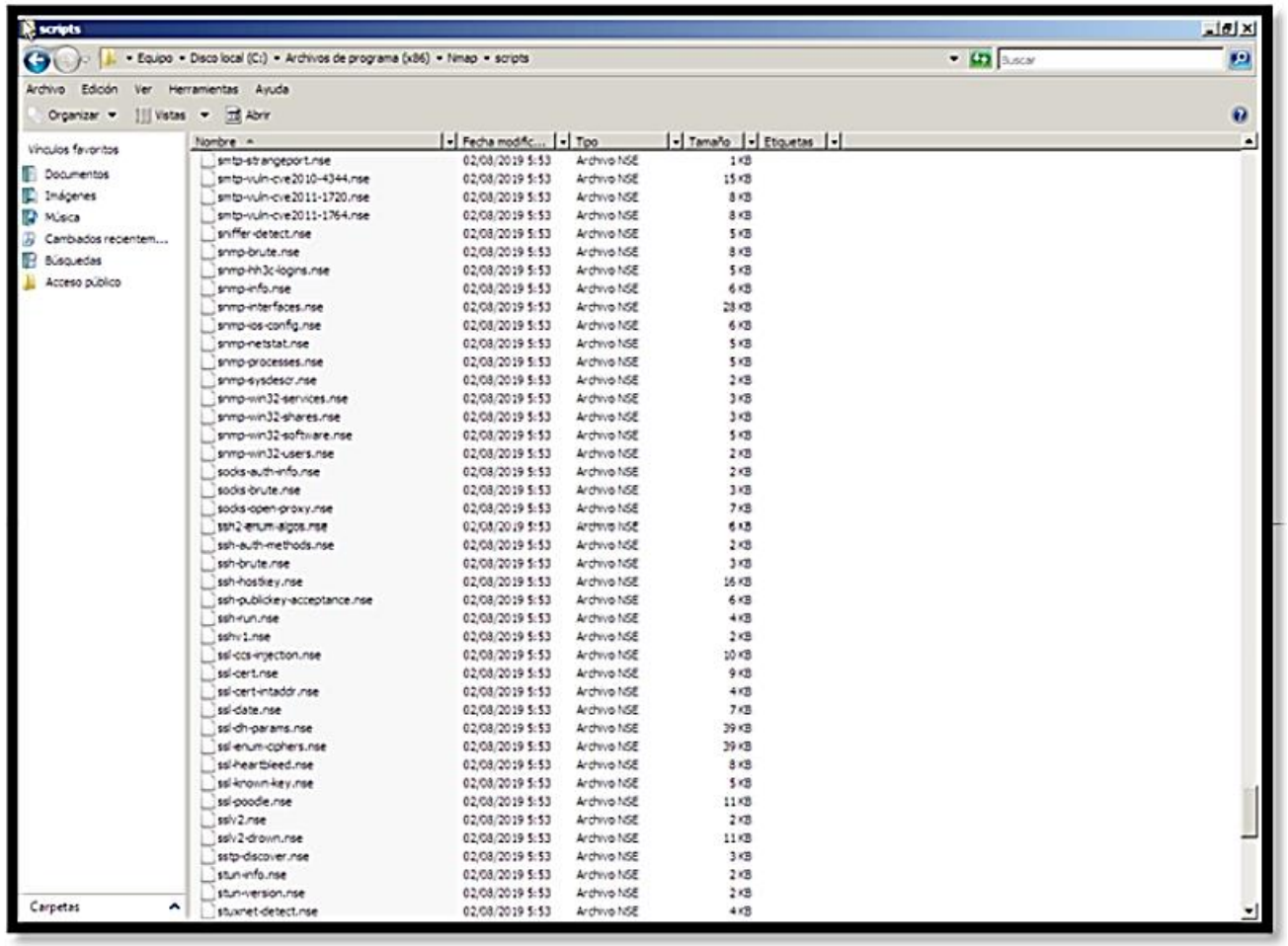
Usar una MAC aleatoria. El 0 indica que nmap escoge la MAC:

nmap -v -sT -PN --spoof-mac 0 192.168.1.1

Para finalizar comentarte la existencia de multitud de Scripts que puedes ejecutar para diferentes fines, como por ejemplo comprobar alguna vulnerabilidad específica, entre otras cosas, la sintaxis para poner un script es la siguiente:

Nmap - -script= NOMBRE SCRIPT

Los scripts los puedes encontrar en la carpeta de scripts de Nmap.



Veamos un ejemplo de un script que actualiza la base de datos de scripts de Nmap.

```
nmap --script-updatedb
```

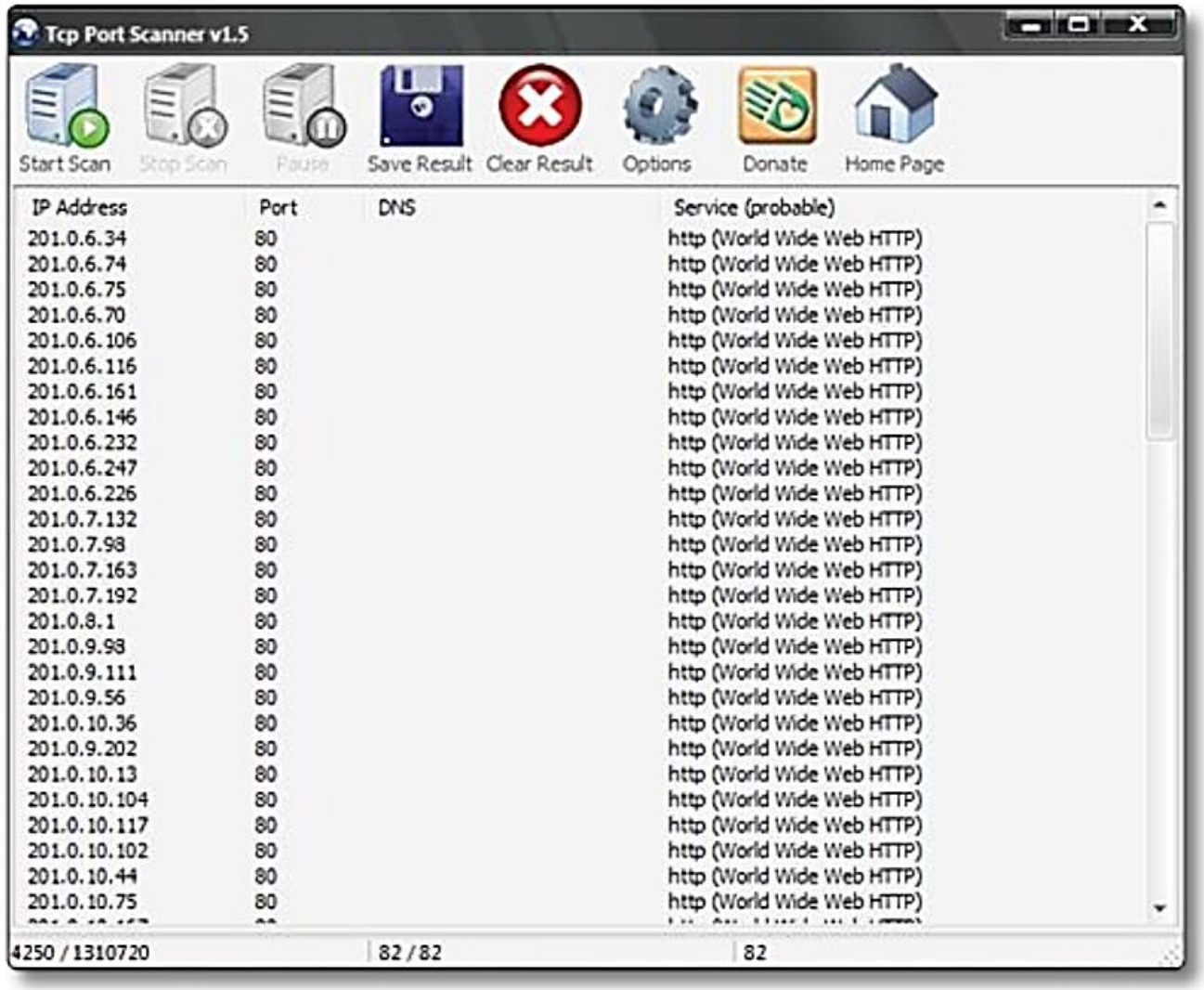
En el siguiente ejemplo, un script, que busca ataques de tipo heartbleed:

```
nmap -sV -p 443 --script=ssl-heartbleed 192.168.1.17
```

Si quieres obtener ayuda sobre los scripts puedes poner nmap - -script-help= NOMBRE SCRIPT

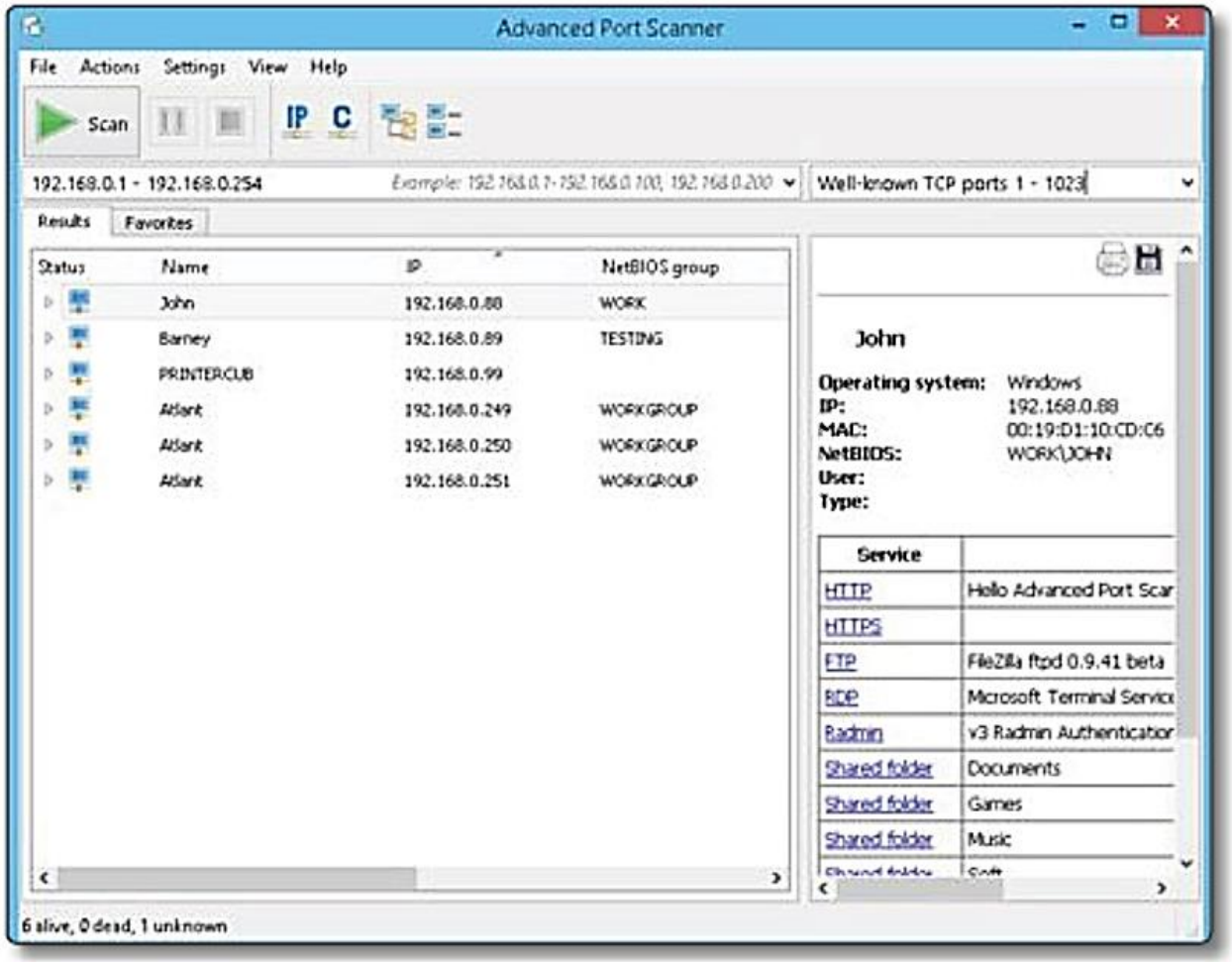
Otras herramientas que también puedes probar para el mismo fin son:

TCP Port Scanner: que sólo escanea puertos TCP mediante el método SYN.



Netcat: herramienta multipropósito, también llamada la “Navaja suiza” que tiene una función de escaneo de puertos, y que también se puede usar para establecer conexiones inversas o reversas con el equipo remoto.

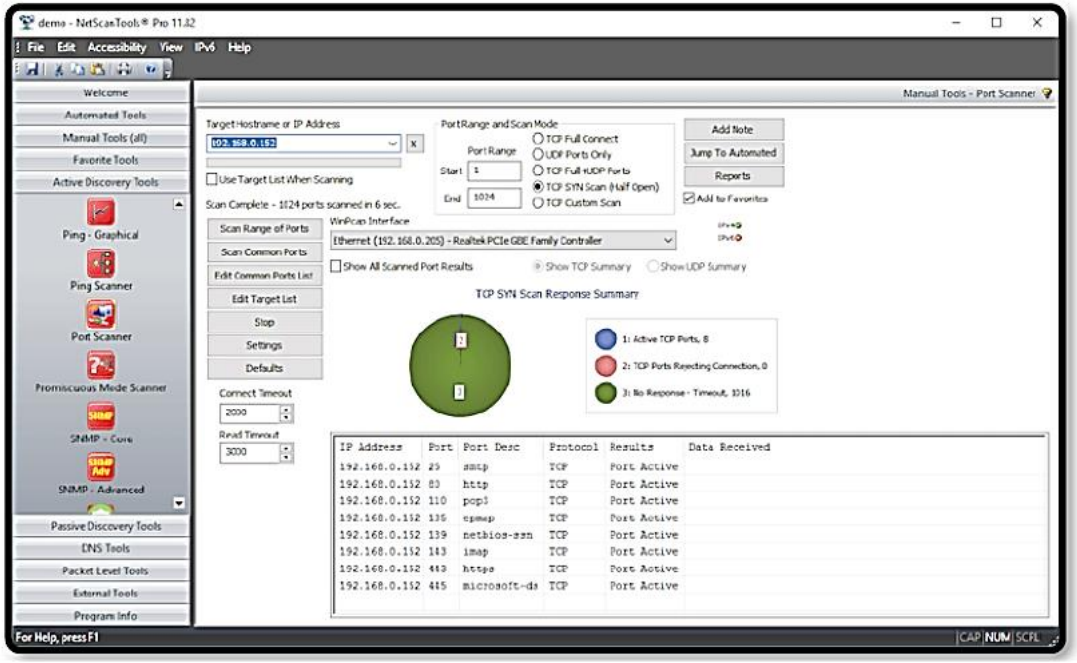
Advanced Port Scanner: escáner que verifica puertos abiertos con sus servicios.



NetScanTools: una herramienta con múltiples utilidades para diferentes protocolos, ICMP, ARP, SNMP, DNS, entre otros.

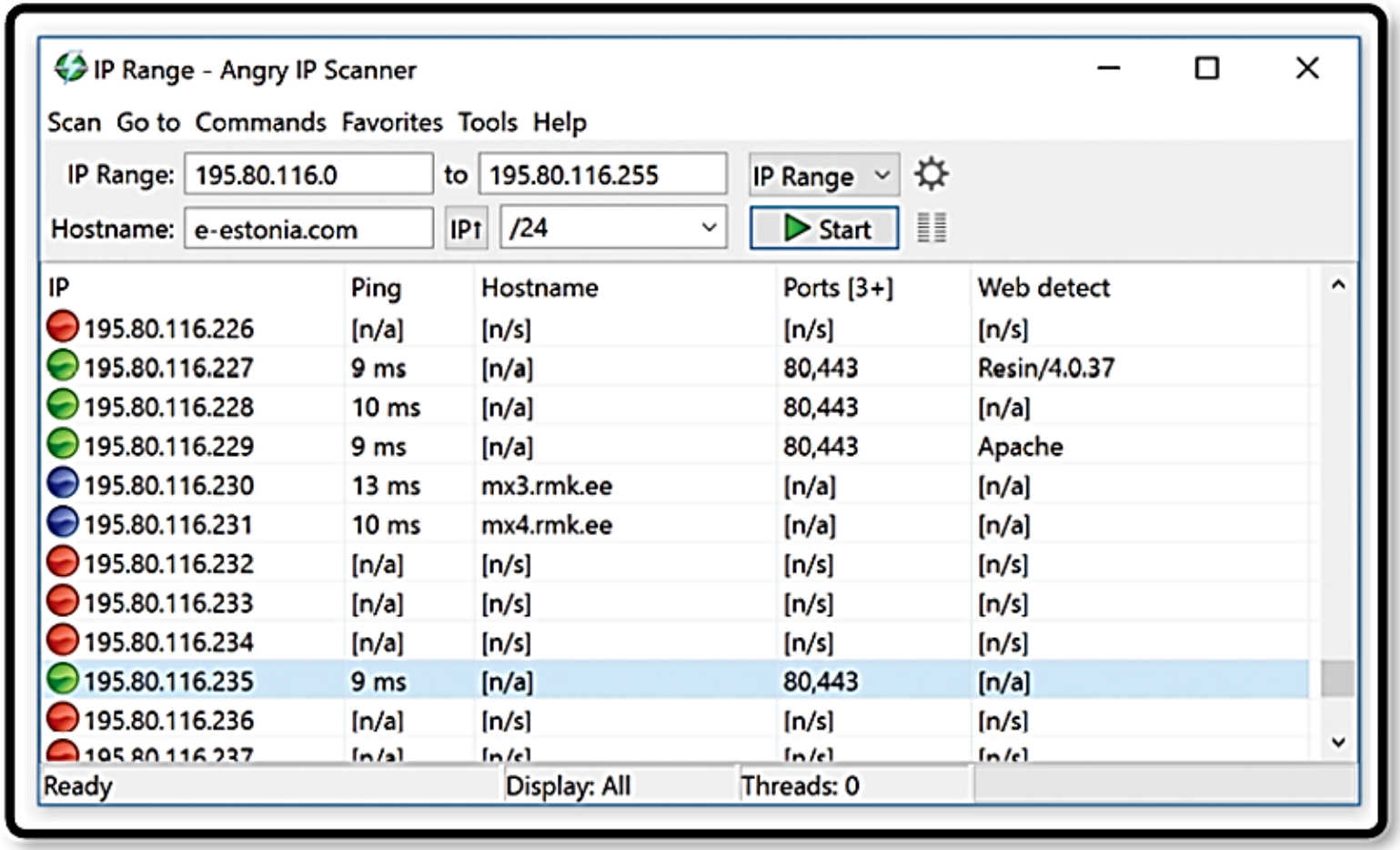
Escanea puertos usando diferentes métodos:

- Conexión completa TCP.
- TCP SYN semiabierto.
- UDP ICMP.
- TCP / UDP ICMP.
- Combinando las flags SYN, URG, PSH, FIN, ACK, RST.



Angry IP Scanner: que además de escanear puertos también es capaz de buscar información NetBIOS, direcciones IP, detectar servidores web, etc.

Los resultados del escaneo se pueden guardar en CSV, TXT o XML.



HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS: NMAP

Durante el proceso de auditoría y de Hacking ético se usan herramientas automáticas de escaneo de vulnerabilidades, que nos permiten hacer distintos tipos de análisis por ejemplo escaneo de vulnerabilidades de aplicaciones y sistemas operativos, malware, algún tipo concreto de Malware, aplicaciones web entre otras.

Estas herramientas tienen la ventaja además de generar reportes en los que figuran el CVE de la vulnerabilidad encontrada, así como otros códigos de vulnerabilidad, el riesgo en métrica CVSS y enlaces a documentación que nos puede ofrecer más información sobre las vulnerabilidades y su posible remediación.

Un análisis de vulnerabilidades nos ayuda a:

- Identificar y clasificar fallos del software que comprometen la disponibilidad, integridad y confidencialidad.
- Ayuda a tomar decisiones a la hora de reemplazar, reparar o sustituir el hardware y software de la infraestructura tecnológica.
- Favorece la implementación de correctas configuraciones de software.
- Apoya la mejora continua de los controles de seguridad.
- Permite documentar los niveles de seguridad alcanzados con fines a la auditoría y el cumplimiento de las leyes, reglamentos y políticas que tiene que seguir la empresa...

Nessus

Nessus es posiblemente una de las aplicaciones para analizar sistemas en busca de vulnerabilidades más conocida.

Es una aplicación de pago, pero puedes usar una versión un poquito más limitada que puedes obtener desde su web (Tenable), Nessus Essentials, es necesario que para descargar Nessus te registres y recibas un correo para obtener código de acceso, que a veces puede demorarse un poco. Esta versión gratuita te permite analizar hasta 16 equipos y está disponible tanto para Windows como para Linux.

Ahora bien, cuando descargues la aplicación, y la instales, tendrás que esperar un buen rato, ya que se descarga e instala online y tiene que descargar bastantes plugins, por lo que el proceso puede durar hasta un par de horas, dependiendo de tu equipo e internet.

Para abrir Nessus tendrás que ir al navegador y poner lo siguiente:

- En Linux: https://unix-deb:88341
- En Windows: https://127.0.0.1:8834

En Linux tendrás que levantar el servicio para que funcione para ello copia en el terminal lo siguiente:

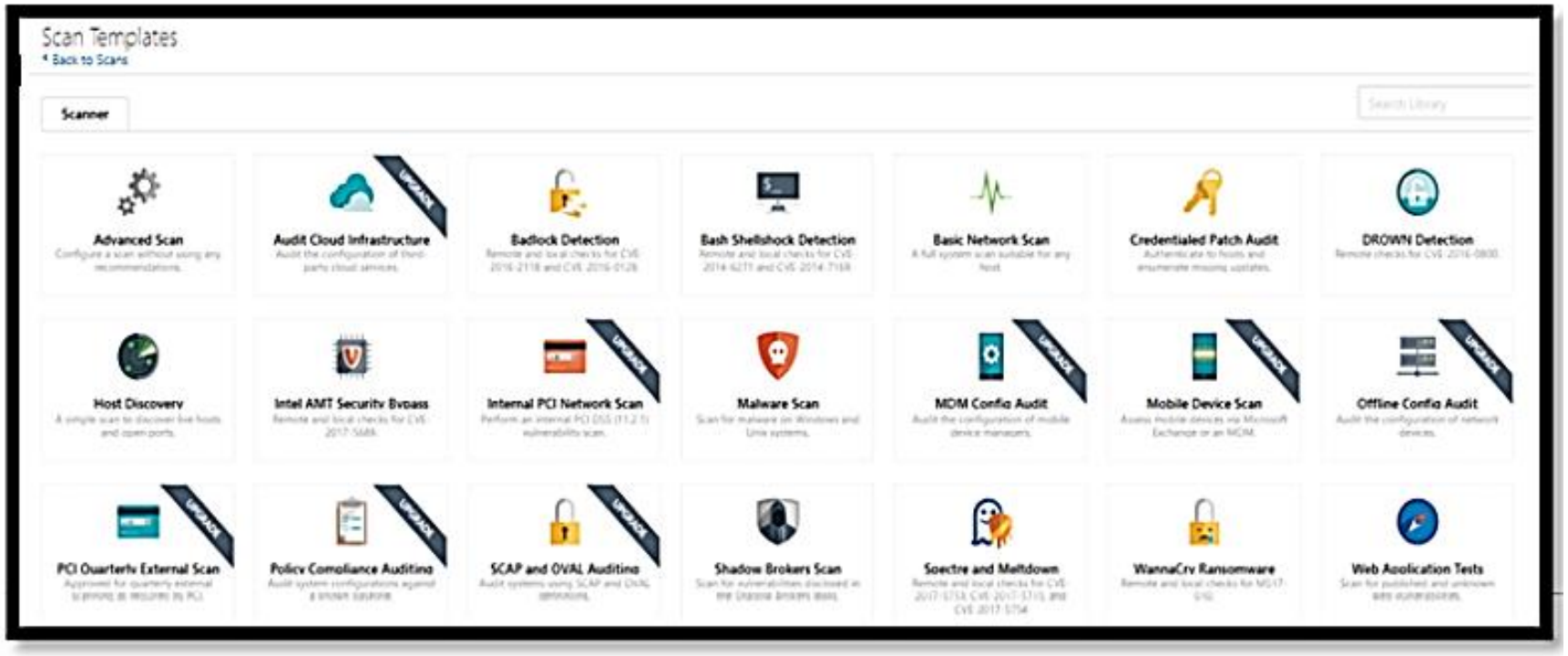
- /etc/init.d/nessusd start
- Service nessusd start
- Service nessusd status

Una vez levantado el servicio insertamos el usuario y la contraseña, y es aquí, en el primer inicio donde verdaderamente comienza la instalación, que como te comentaba tarda bastante tiempo.

Ahora ya podrás ejecutar tu primer escaneo, en la pantalla inicial, encontrarás una serie de escaneos por defectos y otros con una banda que pone “Upgrade” estos últimos son para la versión de pago, no obstante, dispones de unos cuantos escaneos en la versión gratuita.

Basic Network Scan, es uno de los escaneos más comunes que enumerará servicios y verá las vulnerabilidades, donde debemos indicar:

- Dirección ip a escanear.
- Name WINDOWS 7 (x.ej: a quien realizamos el escaneo).
- Targets: indicar ip a escanear.
- Save: guarda escaneo para lanzarlo más tarde.
- Launch: lanza directamente el escaneo.



Una vez terminado el escaneo, pinchando sobre él vemos las diferentes vulnerabilidades detectadas en colores:

- Rojo: crítico
- Amarillo: Media
- Verde: bajo
- Azul: informativas

Podemos pinchar sobre el equipo o dar a vulnerabilidades

Pinchando sobre alguna de las vulnerabilidades, vemos su información:

- Título
- Descripción
- Solución y referencias externas.

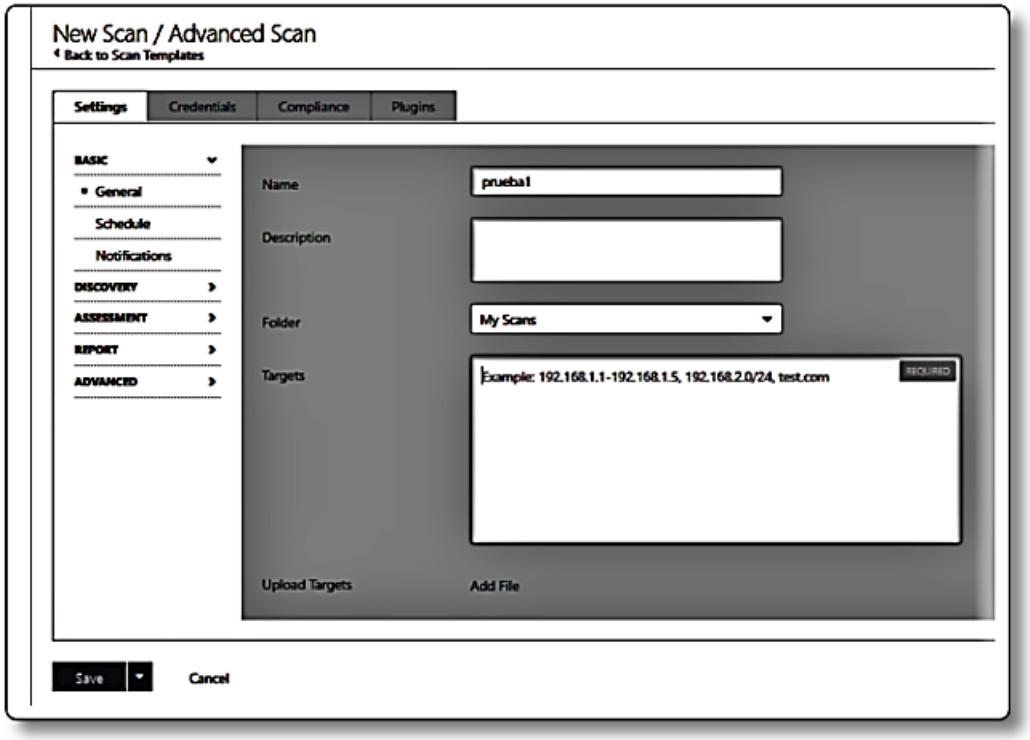
En el panel de la derecha indica:

- Plugin details: detalles vulnerabilidad y del plugin usado para identificar la vulnerabilidad.
- Risk information: riesgo asociado a una vulnerabilidad, calculado en base al cvss (common vulnerability scoring system)
- Métrica con la que medir el impacto que una vulnerabilidad tiene de ser explotada. Http://www.first.org/cvss/cvss-guide.html
- Vulnerability information: indica si hay vulnerabilidad pública
    - Parches
    - Fecha
- Exploitable with:
    - Indica si existe un exploit con el qué explotar la vulnerabilidad (Metasploit).
- Reference information
    - CVE: código único de vulnerabilidad.

Veamos un ejemplo con Advance Scan

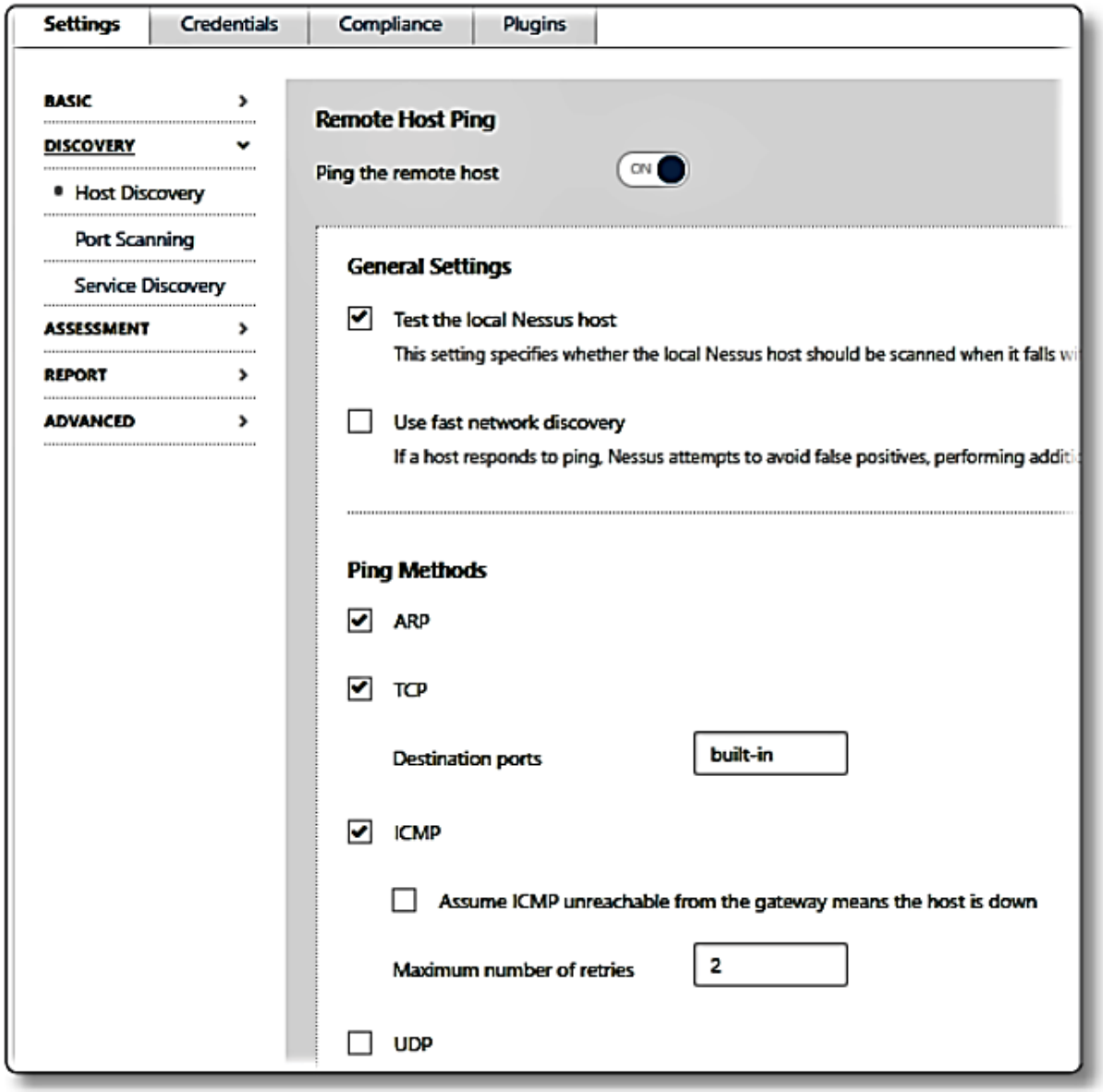
En settings debemos especificar el/los targets:

- IP
- Rango
- Varias IP
- Dominio



En las siguientes opciones del panel de la derecha podemos realizar más configuraciones:

- Schedule: programación escaneo.
- Notifications: poner email y que nos llegue el resultado.
- Discovery: indicar si hay que hacer ping al host remoto (ver si el equipo está vivo o no).
- Métodos: ping, arp, tcp, icmp, udp.
- Test rápido o lento.
- Escanear dispositivos frágiles a los que es posible realizar un ataque DoS durante el escaneo, ya que tienen poca memoria, como por ejemplo las impresoras.


Settings
Credentials
Compliance
Plugins
BASIC
DISCOVERY
Host Discovery
Port Scanning
Service Discovery
ASSESSMENT
REPORT
ADVANCED
Remote Host Ping
Ping the remote host
ON
General Settings
Test the local Nessus host
This setting specifies whether the local Nessus host should be scanned when it falls
Use fast network discovery
If a host responds to ping, Nessus attempts to avoid false positives, performing addi
Ping Methods
ARP
TCP
Destination ports
built-in
ICMP
Assume ICMP unreachable from the gateway means the host is down
Maximum number of retries
2
UDP

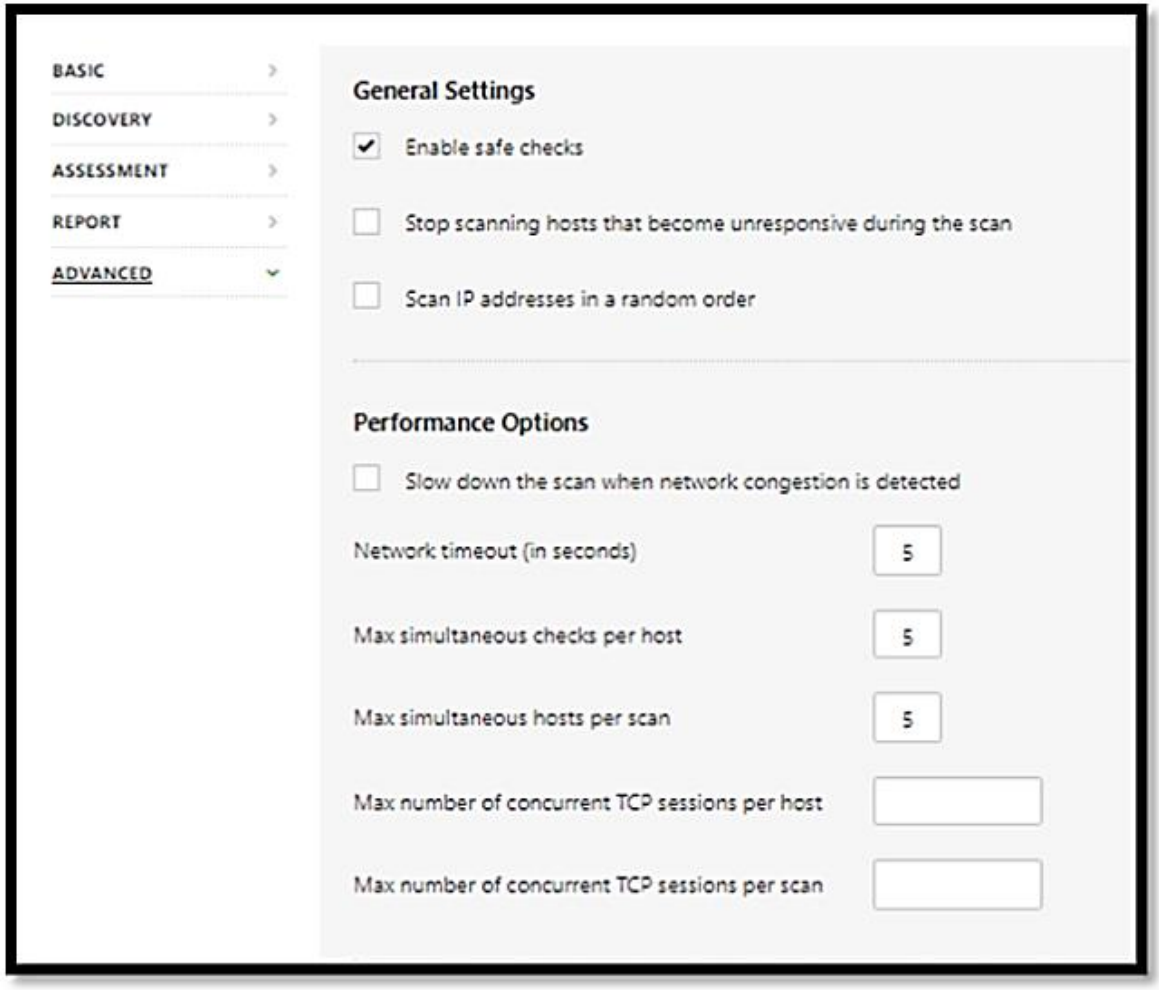
En la opción del panel derecho Discovery, en Port scanning: rango de puertos a escanear puedes realizar la siguiente configuración:

- Tcp Y SYN son los más recomendados.
    - UDP es más lento.
- Service Discovery: dejar por defecto.
- Assesment: fuerza bruta.
- App web, escaneo app web no es fiable.
- Enumeración Windows.
- Reportes.
- Avanzado.

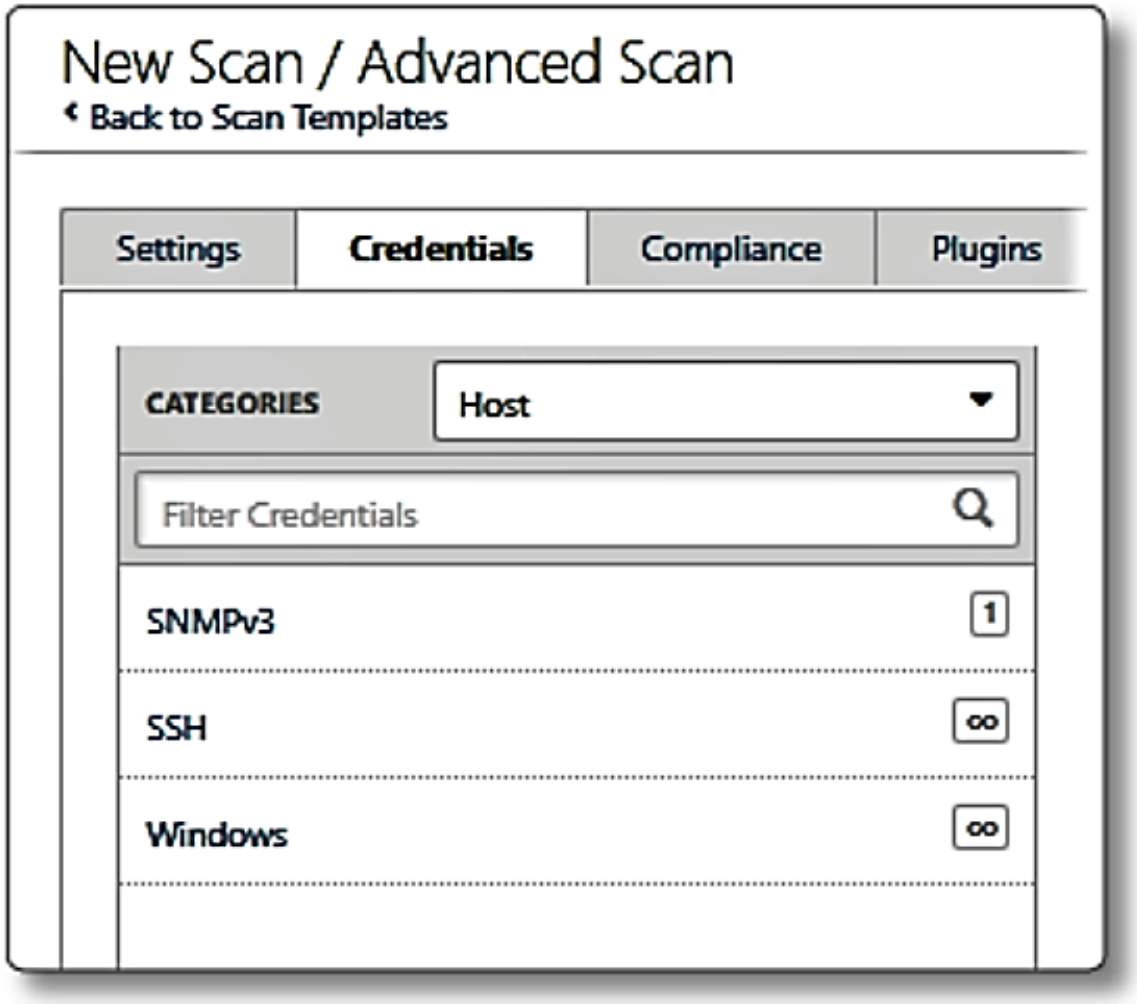
En las opciones avanzadas del escaneo, tenemos alguna configuración importante de cara a no hacer un DoS, si sabemos que el sistema que estamos auditando tiene unas capacidades limitadas, en este caso no debemos lanzar un escaneo muy potente.

- Máx simultaneous checks per host: cantidad de comprobaciones simultáneas que vamos a hacer.
- Max simultaneous host x scan, cuantos hosts de forma simultánea, un número menor si estamos ante una red con limitaciones, o si estamos haciendo ejercicio de red team y no queremos ser detectados.

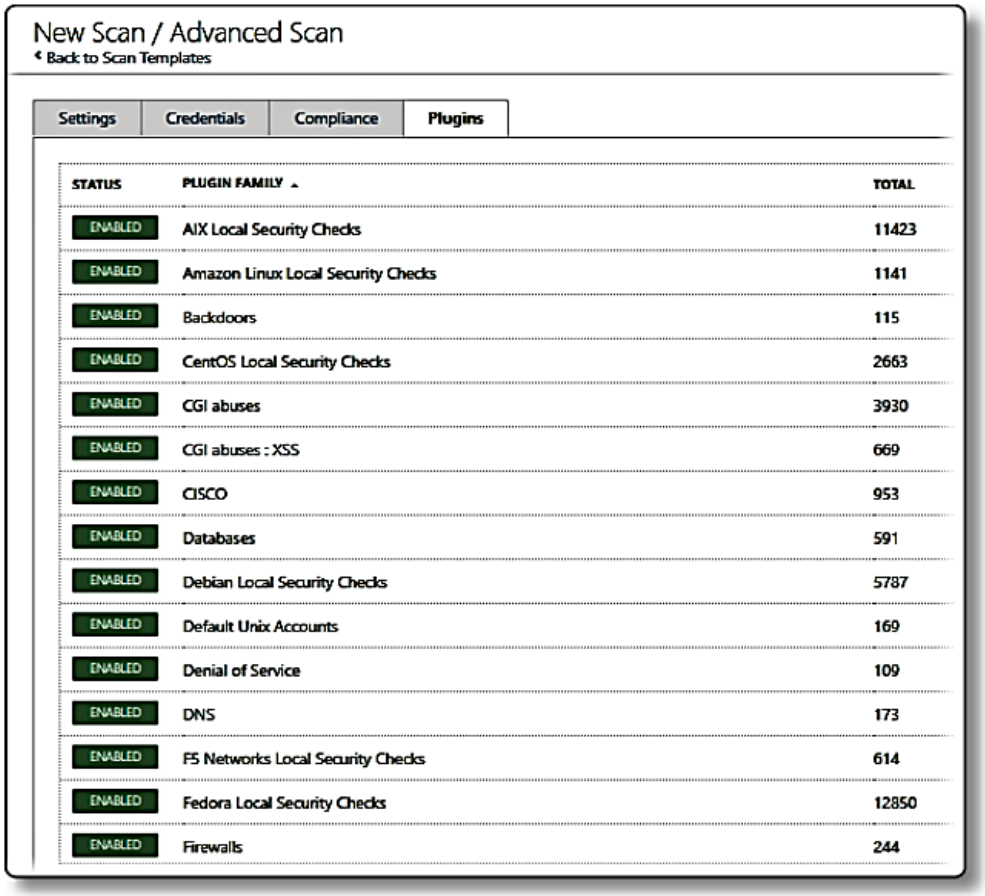
- Shown downs the scan when the network congestion is detected: evita congestión de red.



En Credentials podemos especificar credenciales para diferentes sistemas, de forma que Nessus accede al sistema y realiza verificaciones con sus credenciales.



En la última pestaña podrás escoger los plugins necesarios para hacer más liviano el escaneo, por ejemplo, no vamos a realizar análisis contra un servidor Web si no lo tenemos o contra Wordpress si no está instalado.



En el apartado donde aparecen las vulnerabilidades Export, podemos exportar los resultados en pdf, html y formato Nessus.

CVSS, QUÉ ES Y CÓMO USARLO

Hasta el momento he nombrado varias veces el CVSS, pero no te he explicado en concreto que es.

El CVSS es un sistema de puntuaje que Estima el impacto derivado de vulnerabilidades.

Vulnerabilidad= debilidad explotada por una o más amenazas= riesgo de seguridad.

Es un estándar FIRST (Forum of Incident Response and Security Teams) y se usa en bases de datos de vulnerabilidades como.

- NVDB (National vulnerability database).
- CVE (Common vulnerabilities and expoxures).
- OSVDB (Open source vulnerability database).

Actualmente coexisten 2 versiones de CVSS que clasifican la severidad del riesgo de 0 a 10 de la siguiente forma:

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	**Base Score Range**	**Severity**	**Base Score Range**
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

Enlace a Web NVD y métricas CVSS: https://nvd.nist.gov/vuln-metrics/cvss

Extraído de Auditoría de la seguridad informática. Silvia Clara Menéndez Arante. Editorial RAMA