UT01: Adopción de pautas de seguridad informática – Amenazas 3 – Ataques de Reconocimiento

Nombre: Francisco Jesús García – Uceda Díaz – Albo y Alex Valdepeñas
Curso: 2º ASIR.

Índice

Introducción

En está práctica aprenderemos a realizar un ataque de reconocimiento a un equipo. Está práctica la hemos realizado con el compañero Alex Valdepeñas el cuál él es la víctima y yo el que realiza el ataque de reconocimiento. En la práctica aprenderemos también ha realizar un Man In The Middel e intentaremos interceptar a este.

Desde el ordenador atacante (PC1-Windows/Linux): (Va todo en conjunto).

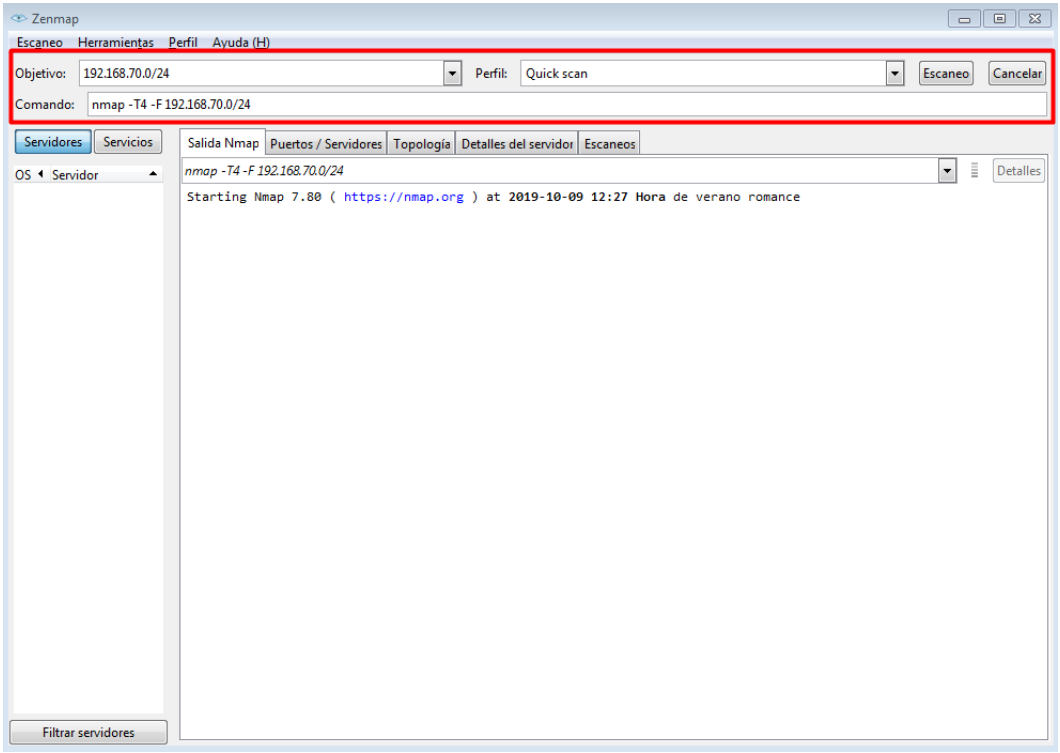
a) Barrido de pings y detectar el sistema operativo de los equipos activos en la red (comando o herramientas: Superscan, IP Scanner, etc).

b) Visualizar o escanear los puertos que tiene abiertos el ordenador amenazado (PC3).

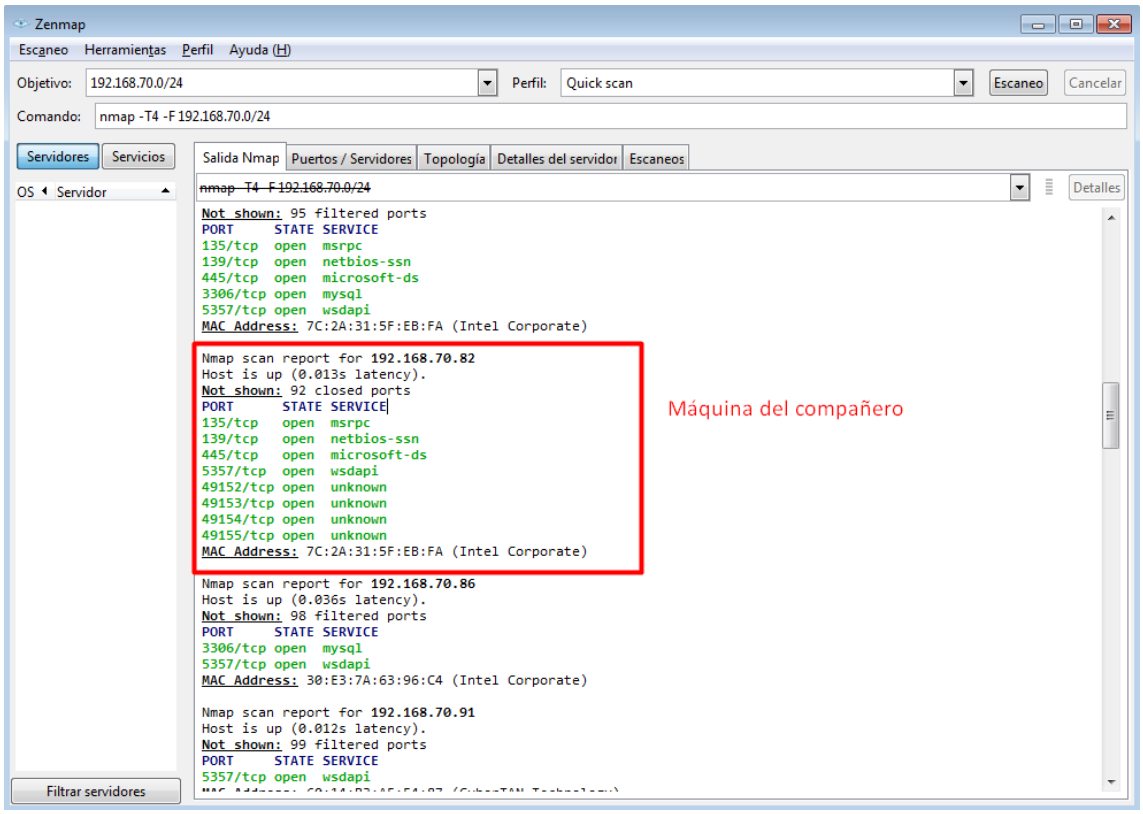
c) Captura los paquetes de la red desde "Man in the Midle" situado en PC2 (Windows/Linux).

El barrido de ping es utilizado para contabilizar las máquinas disponibles en una red, o monitorizar servidores. Es más fiable que hacer ping a la dirección de broadcast, ya que algunos equipos no responden a ese tipo de consultas.

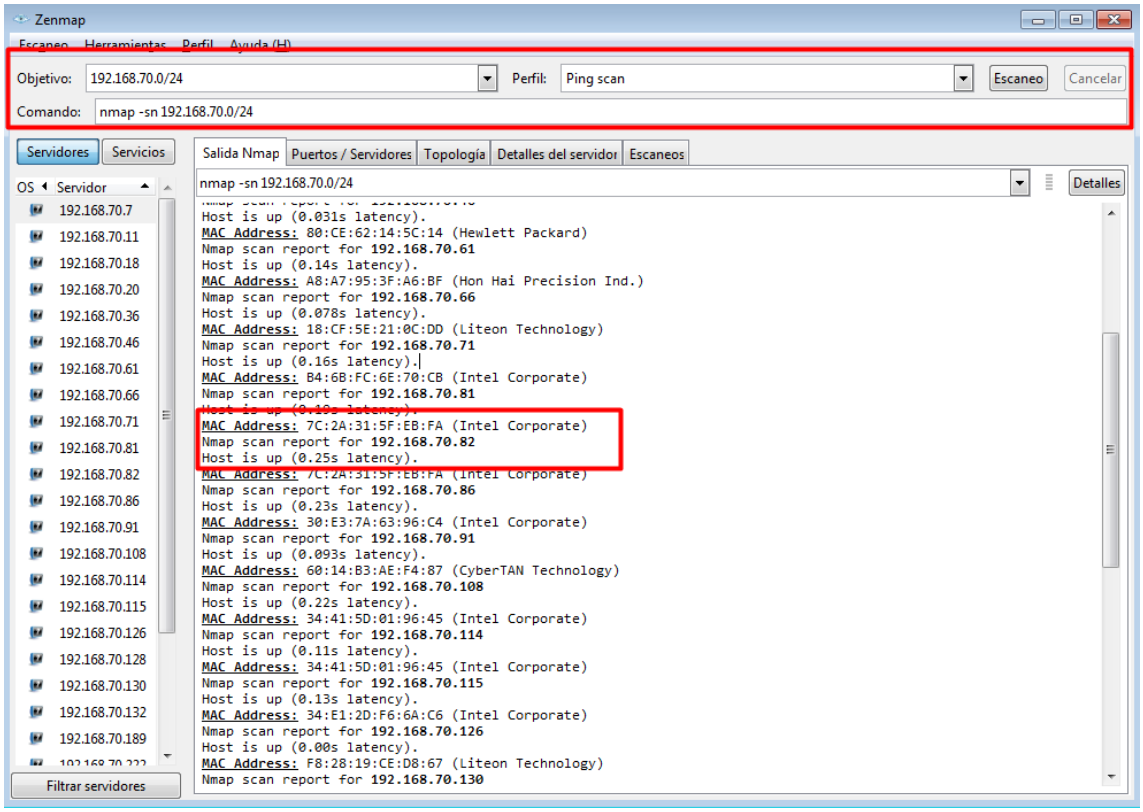
Primero lo haremos con NMAP el escaneo, usaremos un escaneo rápido sobre la red 192.168.70/24 para encontrar el equipo que buscamos.



Como vemos, nos ha hecho un análisis con todas las máquinas que hay en la red, nosotros nos fijaremos en la .70.82 que es la máquina del compañero y de la cual podemos actuar.



Podemos también hacer un *<<Ping scan>>* en toda la red.

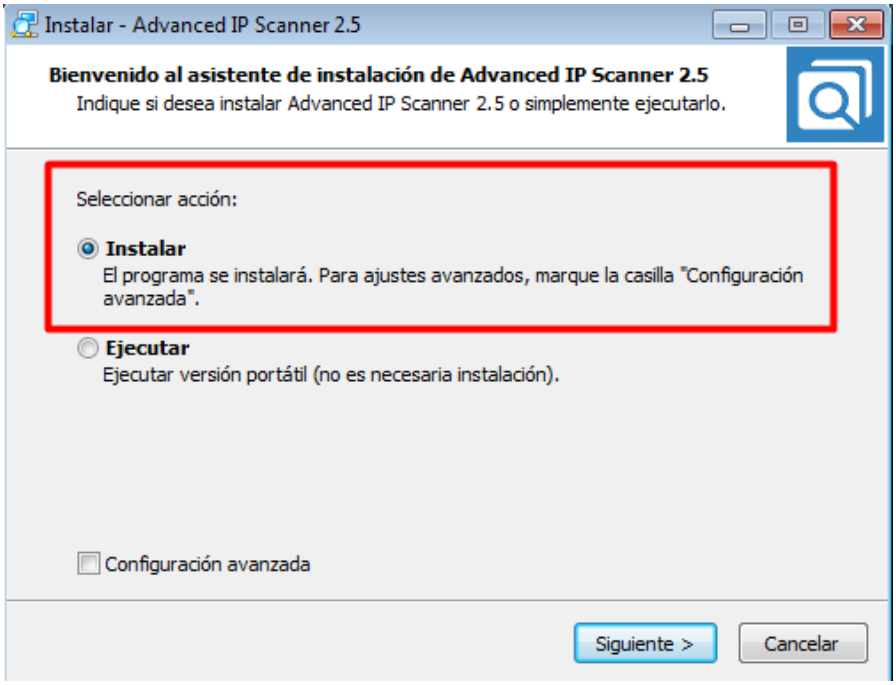


Podemos realizar un escaneo con la versión ligera de nmap también:

nmap -T4 -F 192.168.70.0/24

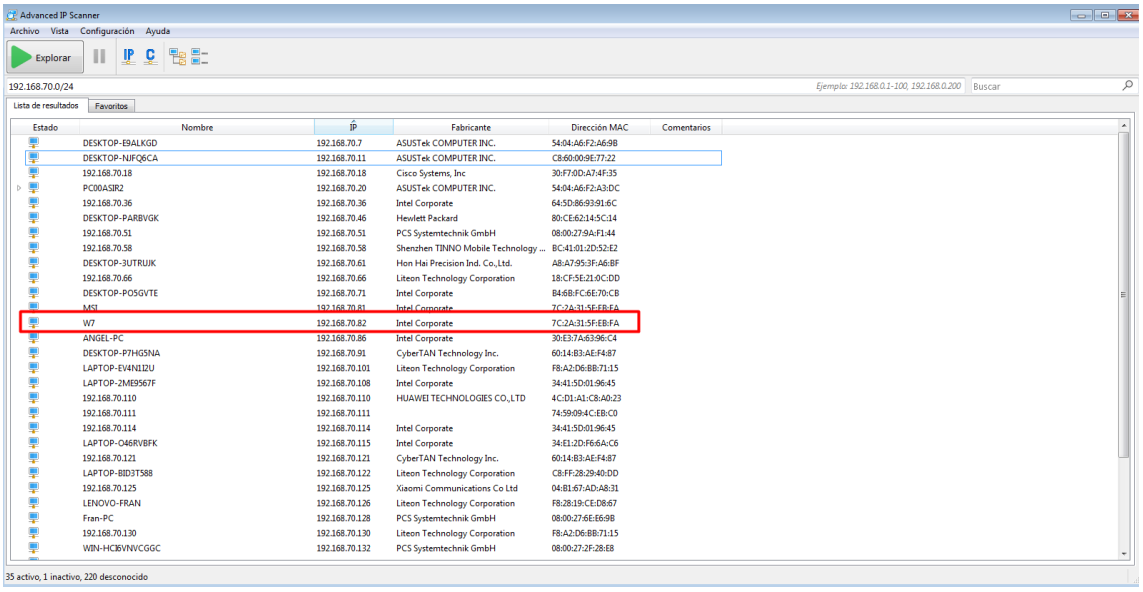
Lo siguiente que haremos es descargar *Advamnced IP Scanner* para realizar un escaneo a la red con este programa. Puedes descargarlo pulsando aquí.

Podemos elegir instalarlo o su versión portable.

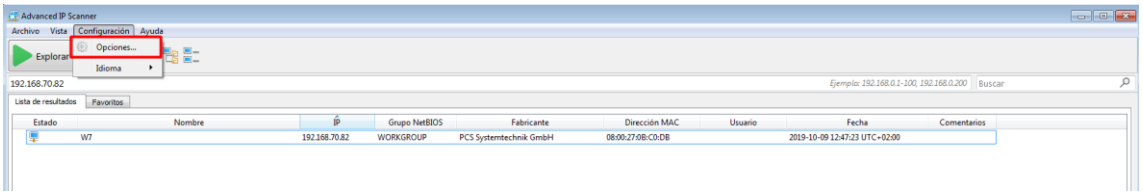


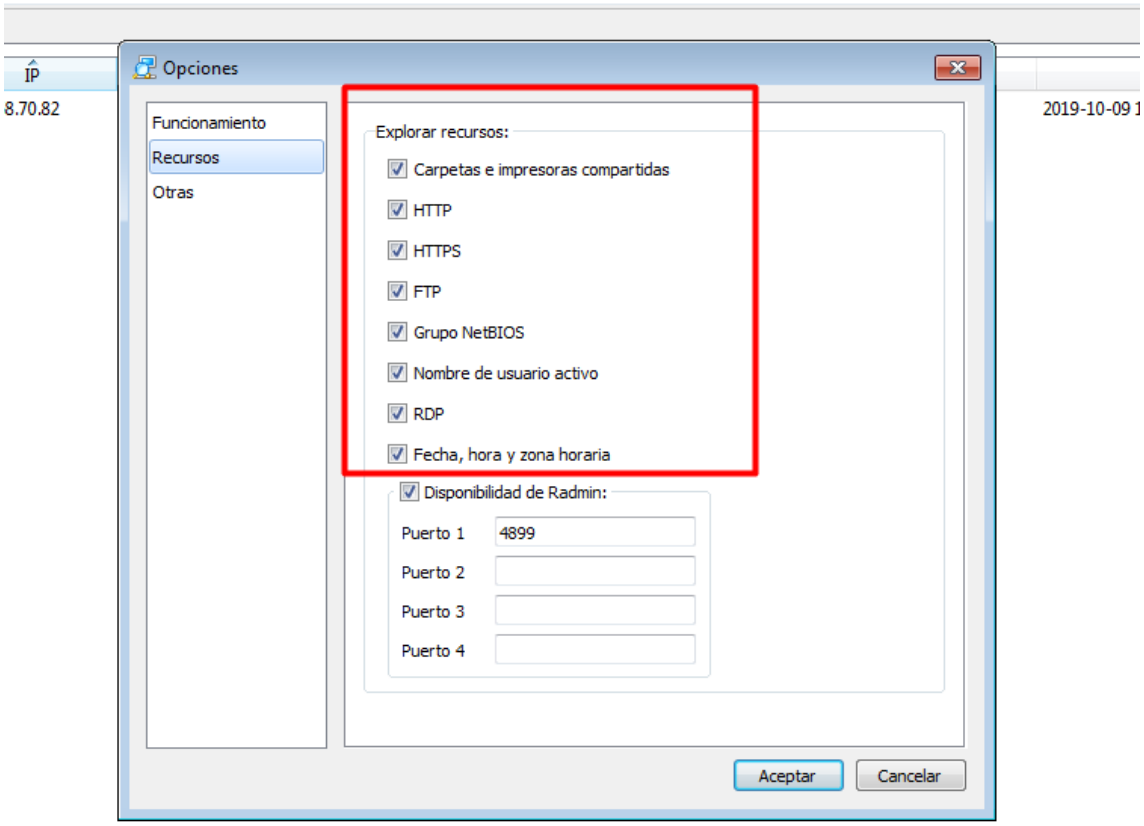
Aceptaremos los términos y condiciones.

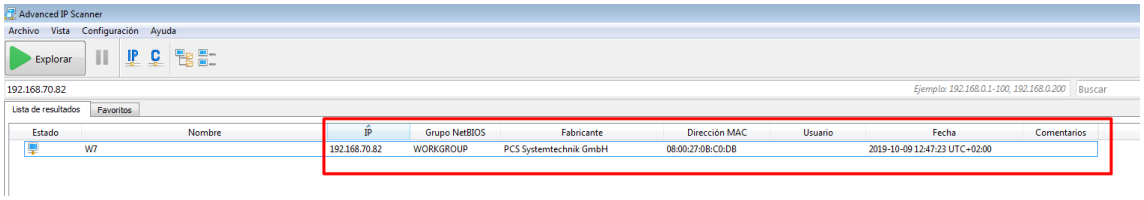
Para hacer un escaneo de la red basta con poner la IP de la red y darle explorar.



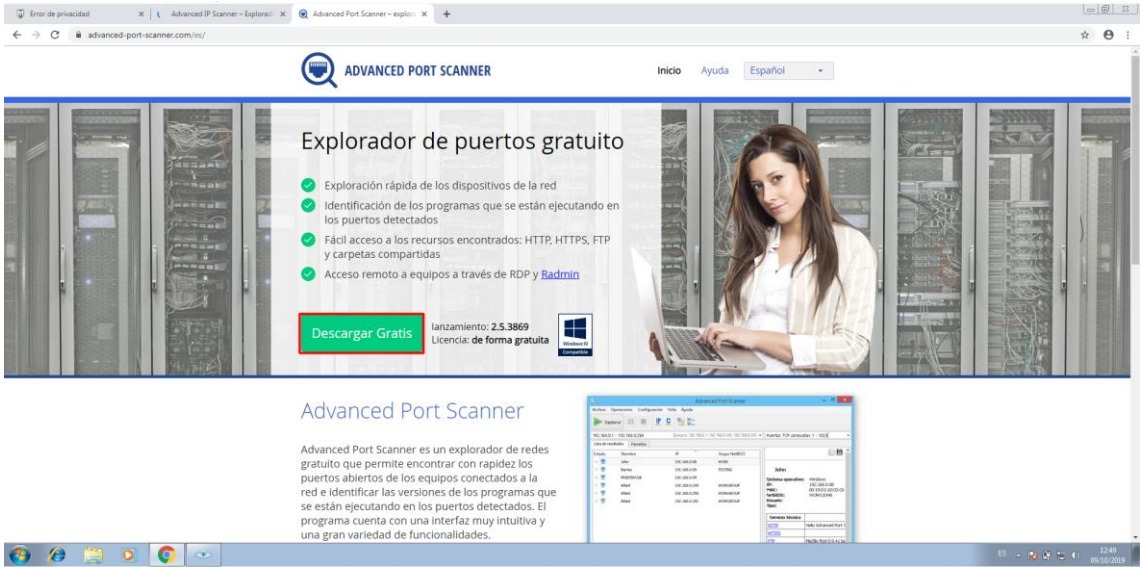
Podemos activar en las opciones más opciones para que nos de más información.



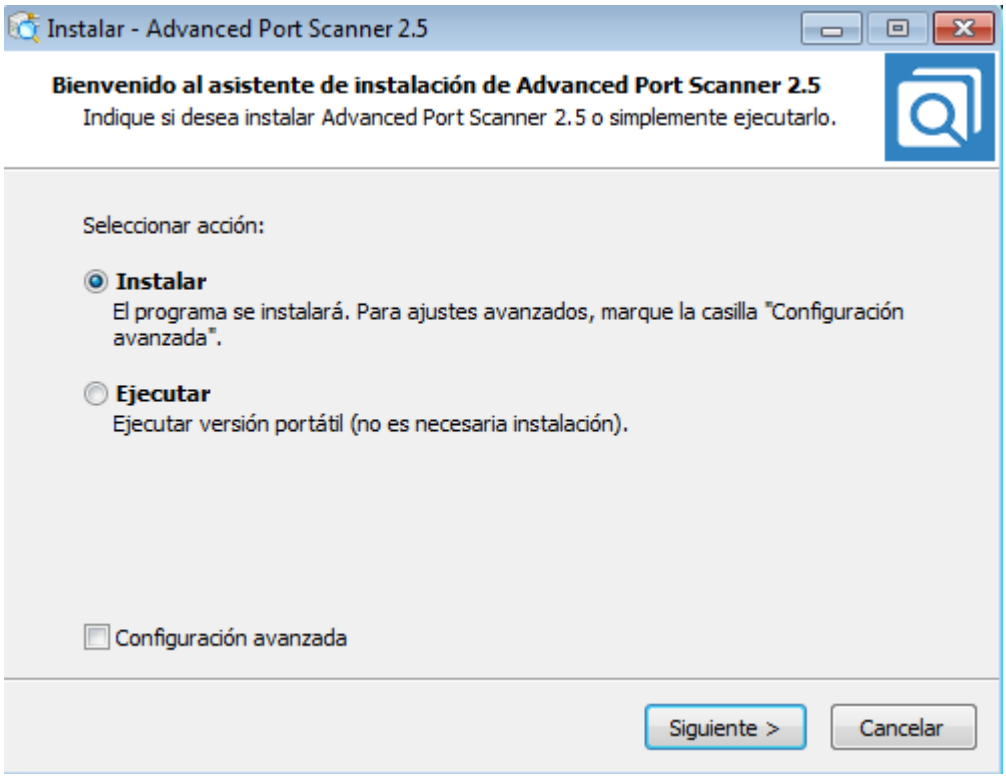




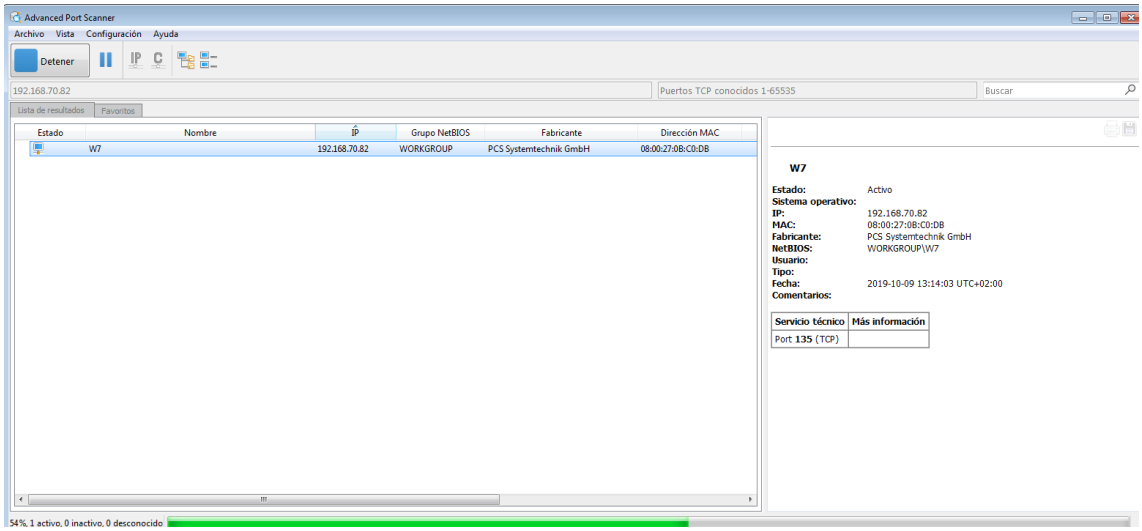
Lo siguiente que haremos es descargar *Advanced Port Scanner,* un programa de la misma compañía, con este realizaremos un escaneo de puertos. Lo podemos descargar desde aquí.



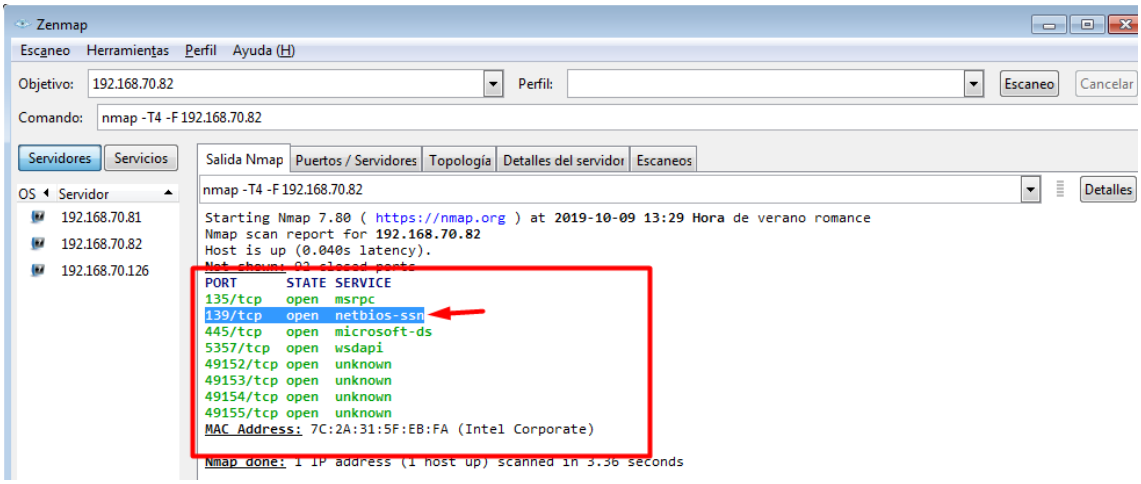
Lo podremos de igual forma instalar o ejecutar en la versión portable.



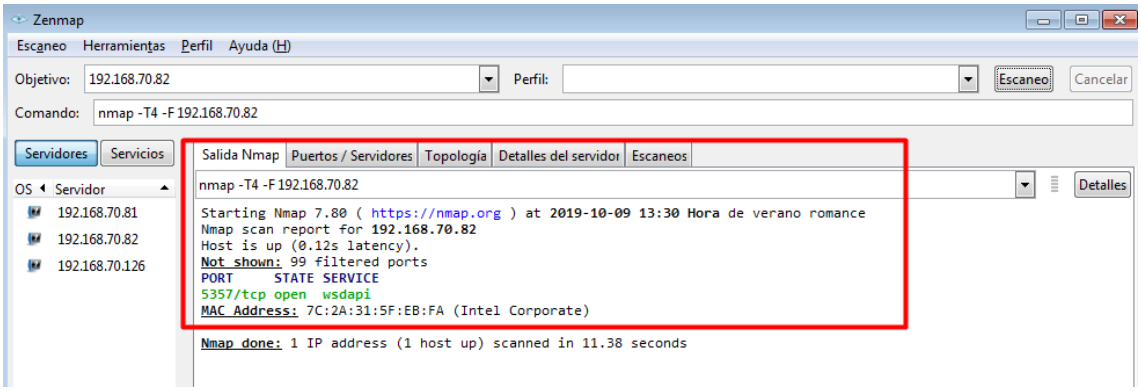
Vemos como según los puertos que encuentra en tiempo real lo va indicando, buscaremos directamente por la IP del equipo.



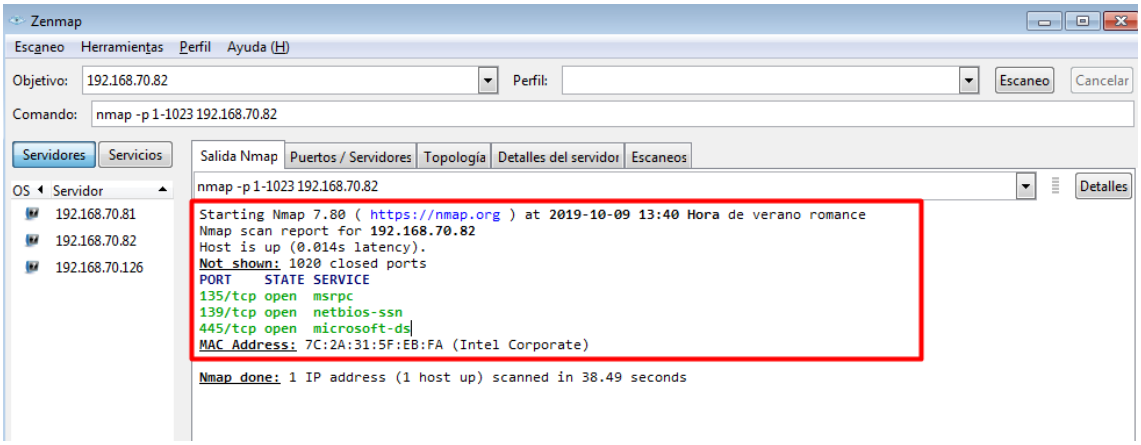
Con un escaneo rápido en ZENMAP también podremos ver los puertos abiertos del equipo que buscamos, vemos como tiene varios puertos abiertos, en este caso cerraremos el puerto NetBIOS (Podremos ver como se hace en la segunda parte sección A de este ejercicio).



Una vez cerrado podemos ver que ya no nos aparece.

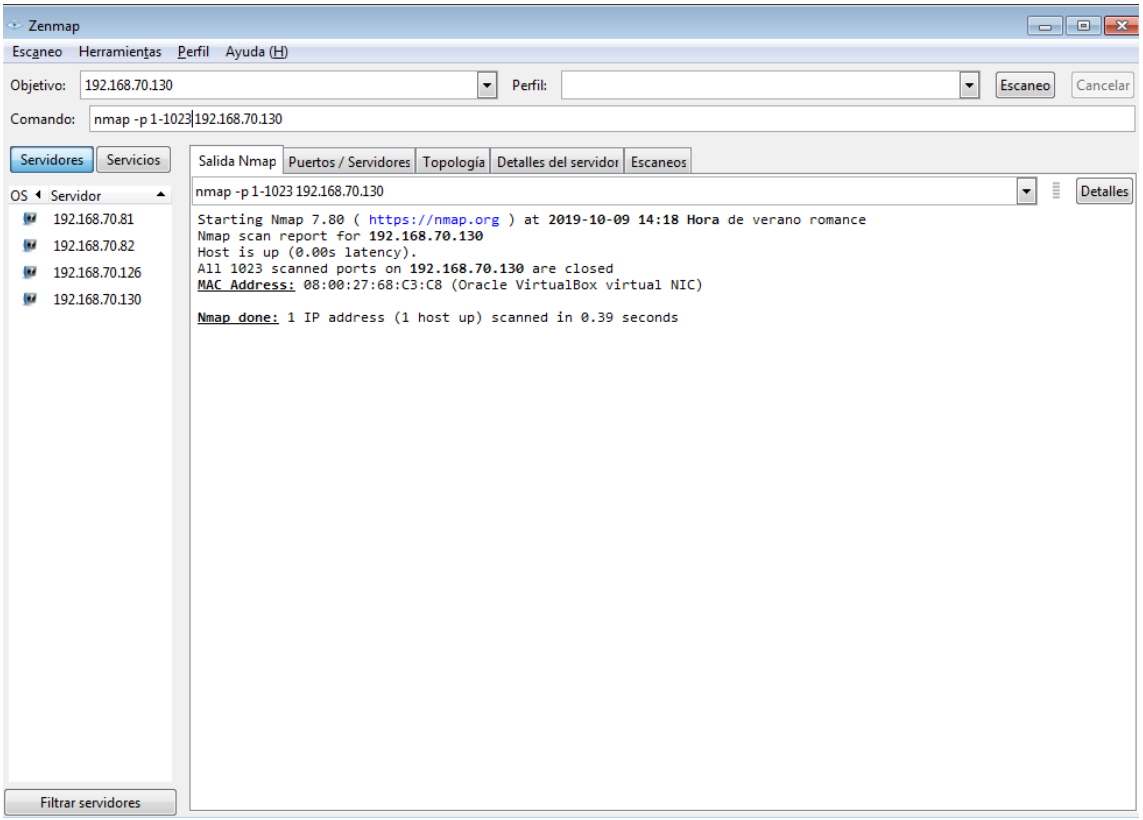


Si eliminamos la regla y reiniciamos el equipo de la victima podemos ver como se vuelve a abrir.



A partir de esta parte lo hemos realizado en una máquina con Ubuntu 18 instalado, como vemos esta máquina no tiene ningún puerto abierto.

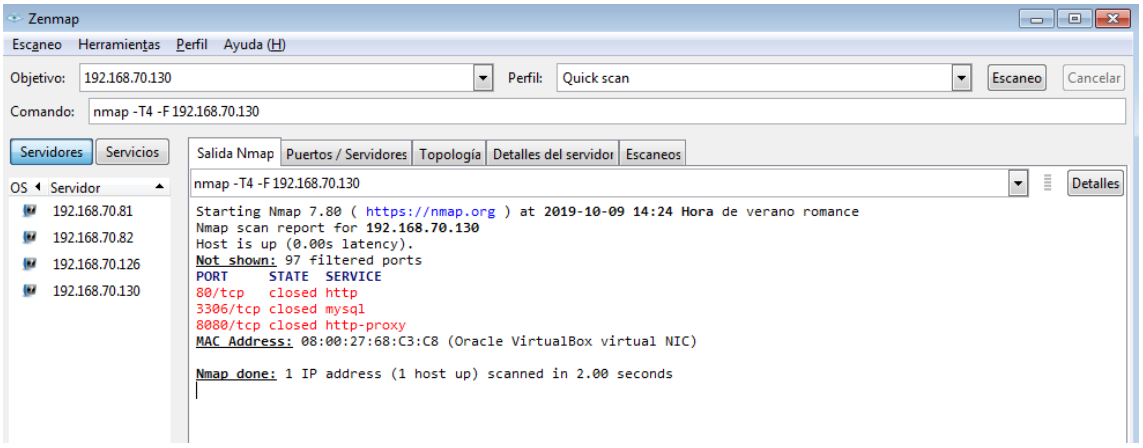
Con *nmap -p [rango puertos] [IP]* podremos buscar por rango de puertos.



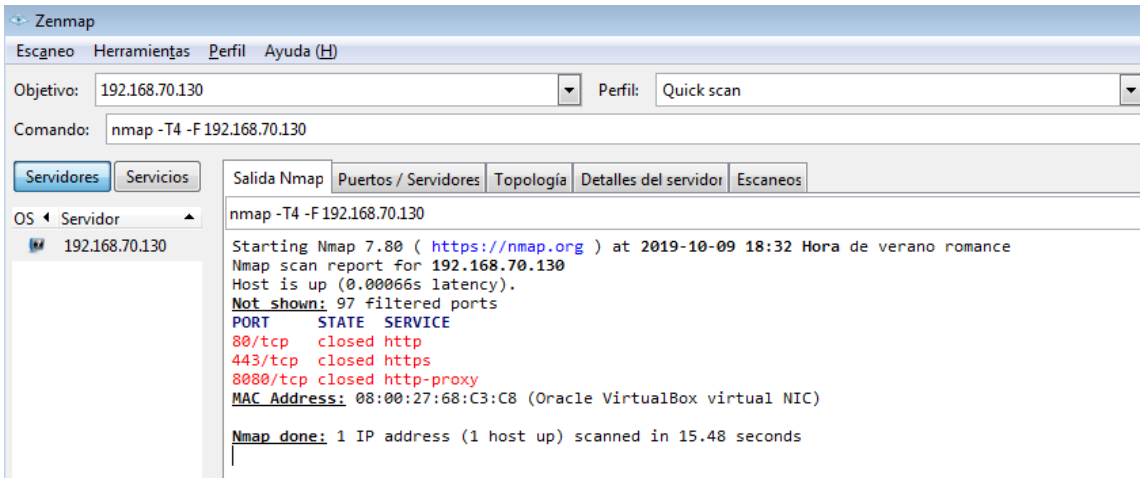
Lo que hemos realizado y que veremos en la segunda parte sección a es como abrir puertos, vemos que en *State* aparece como *Closed,* esto ocurre porque en Ubuntu, todos los puertos se abren a menos que tenga un firewall o una aplicación que lo esté bloqueando. En circunstancias normales, la aplicación que se ejecuta en el puerto es para escuchar.

Un puerto generalmente se considera abierto cuando hay un programa ejecutándose y escuchando en el puerto.

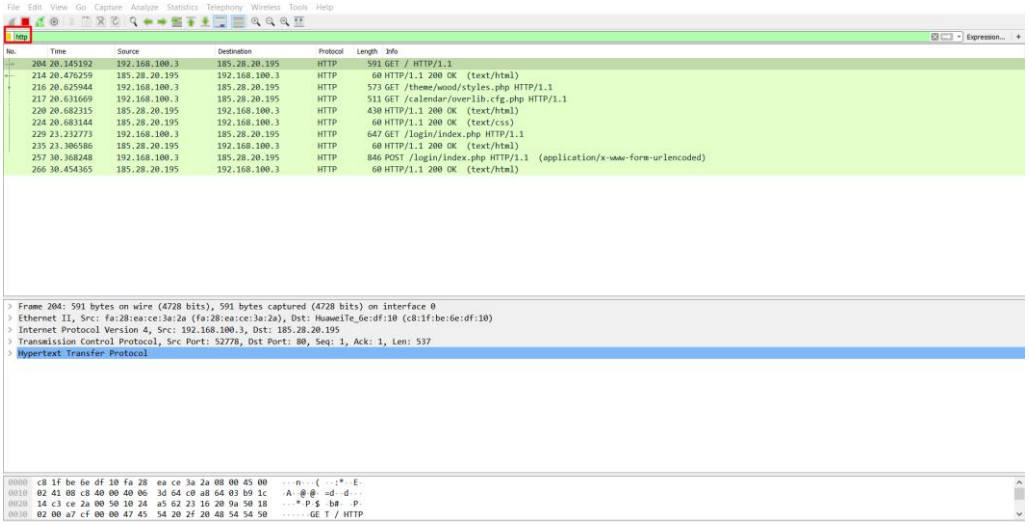
Como vemos hemos abierto el puerto http, MySQL y http-proxy.

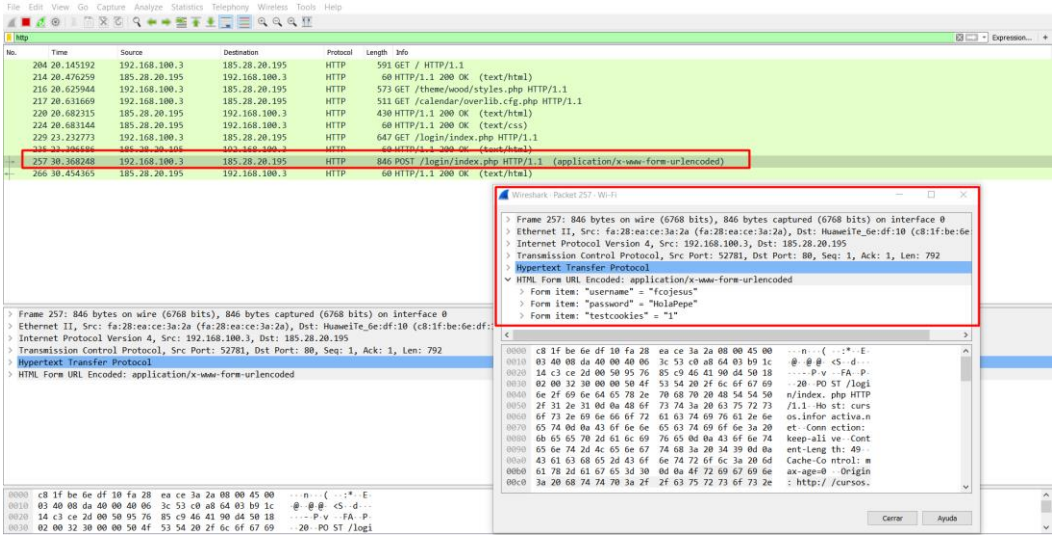


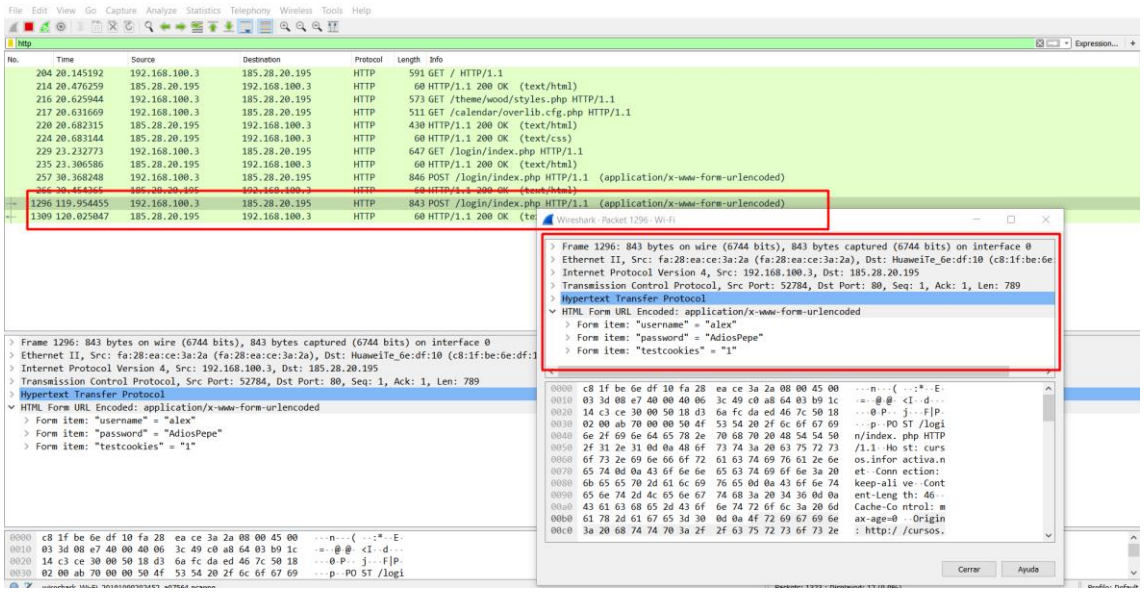
Hemos cerrado el puerto MySQL y hemos abierto el https (443).

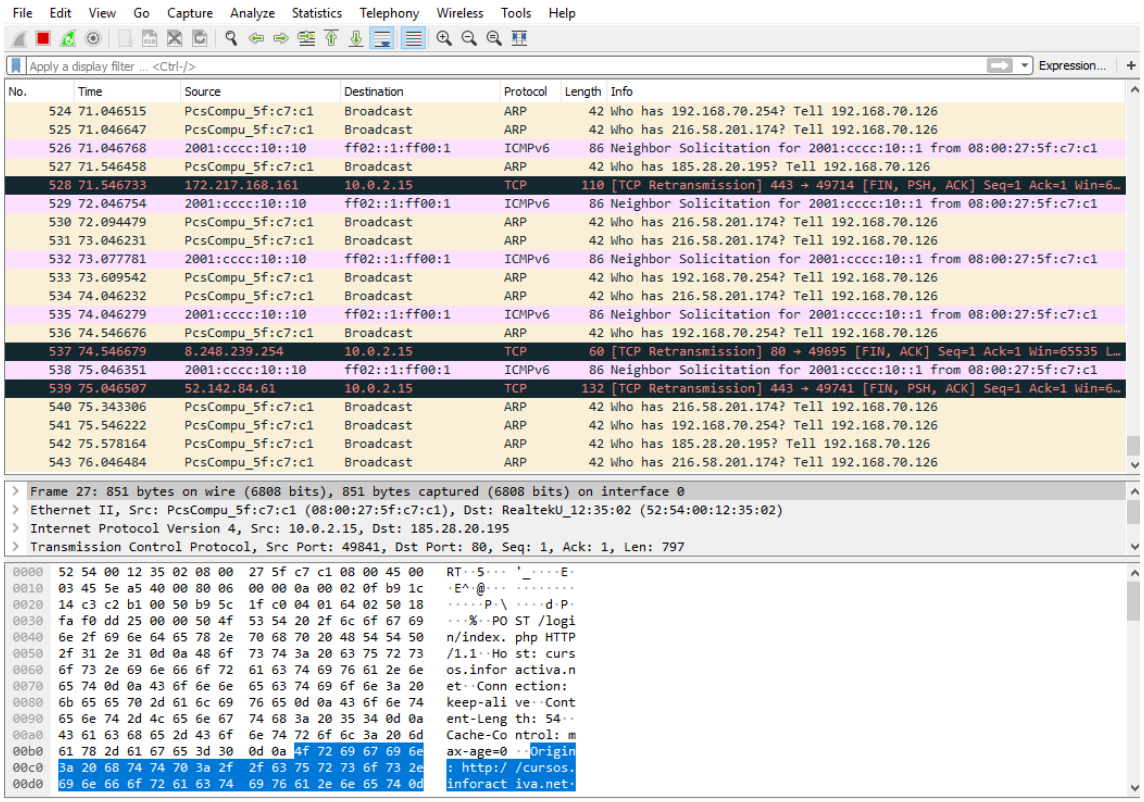


La siguiente fase será realizar un Man In The Middel en los equipos, podemos ver el escenario. Para realizar el MiNT utilizaremos Wireshark. Capturaremos la clave de usuario de una página http.







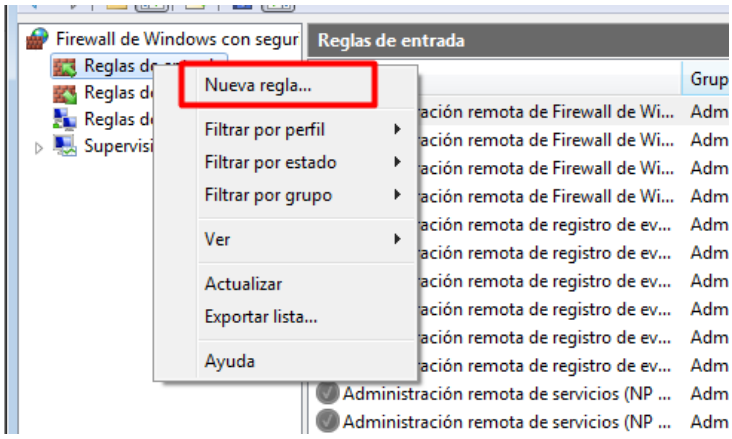


Desde el ordenador amenazado (PC3 –Windows/Linux):

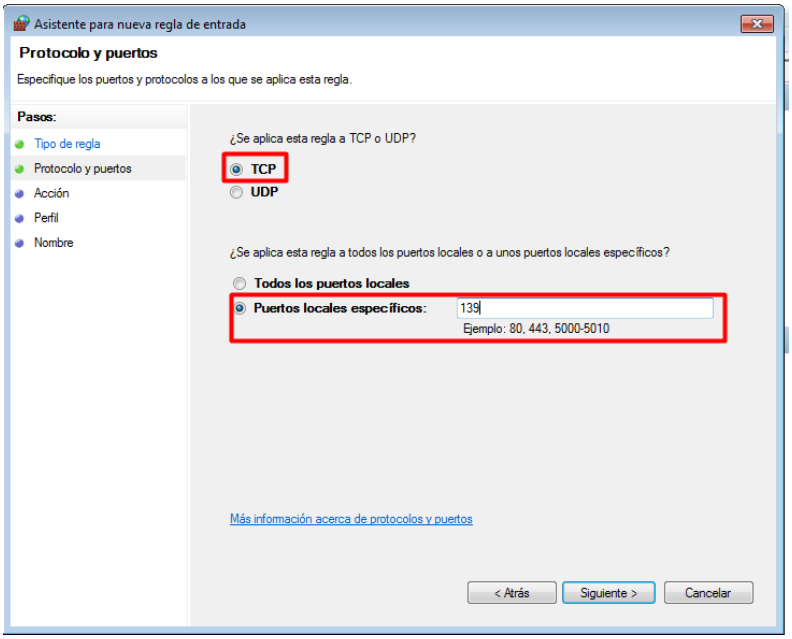
a) Cerrar o abrir puertos (Windows y Linux).

b) Realiza un informe sobre software anti-sniffers Y SI LO CONSIDERAS NECESARIO UTILIZA EL MISMO para detectar desde PC3 sniffers situados en la red.

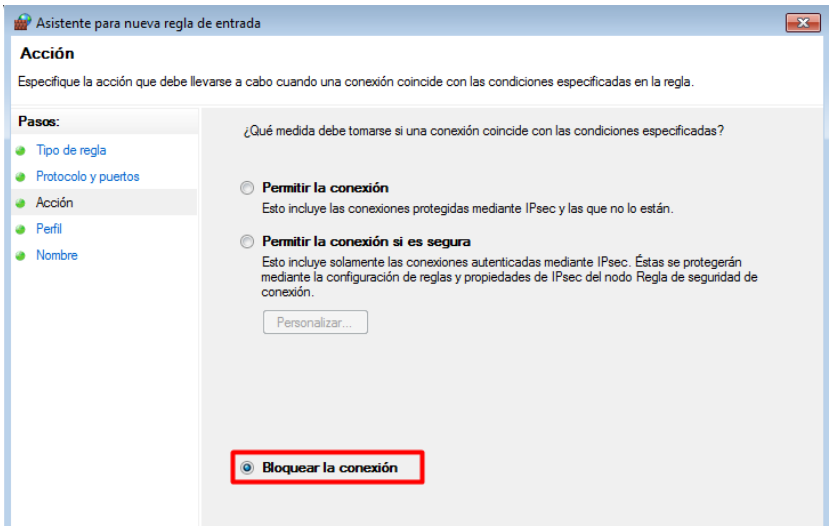
Vamos a bloquear el puerto 139 para ver si el equipo atacante no consigue localizarlo. Para ello crearemos una nueva regla de entrada y de salida bloqueado el puerto.

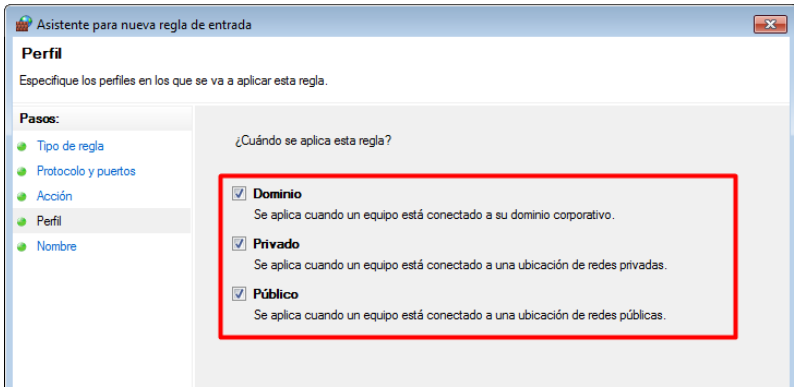


Escogemos TCP y el puerto.

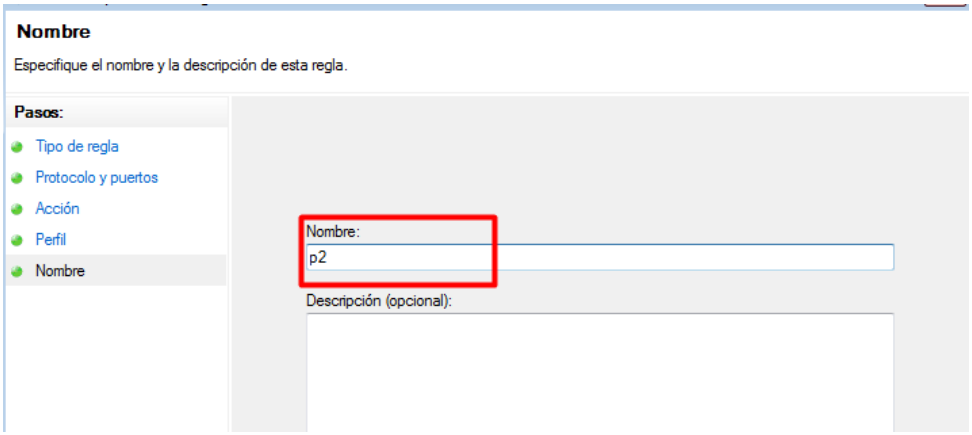


Lo bloquearemos.

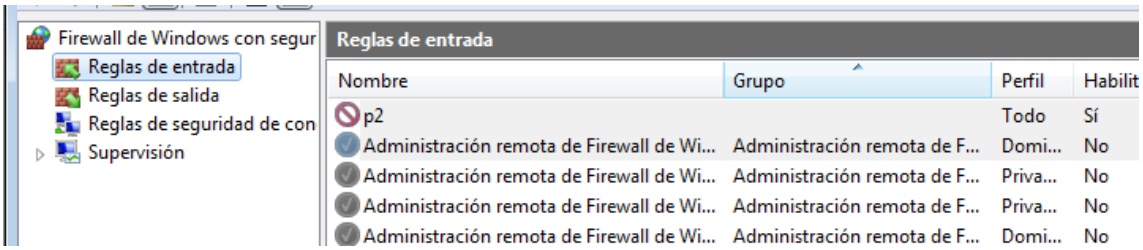


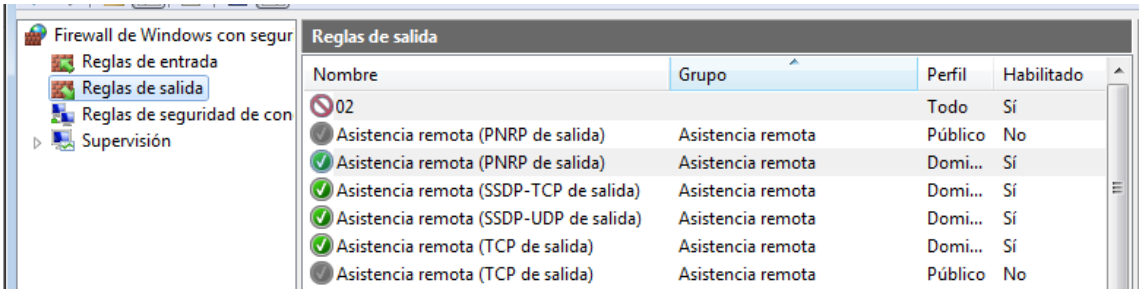


Le pondremos un nombre.

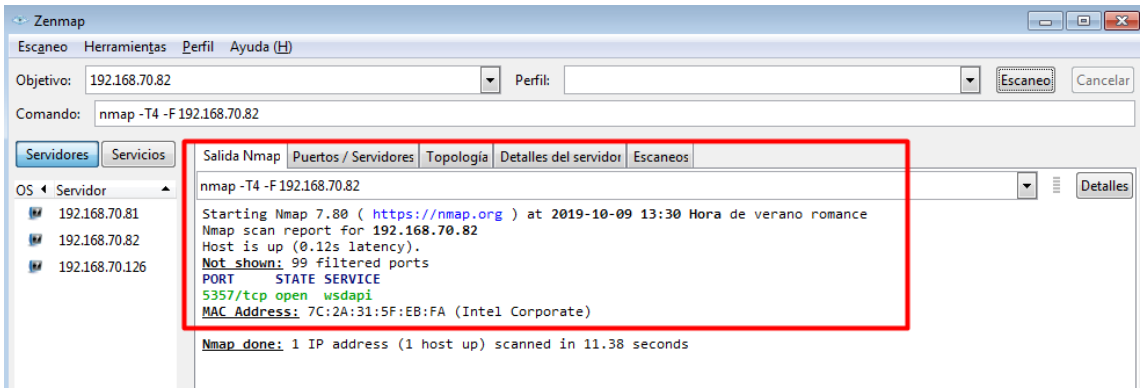


Nos deberá quedar una cosa tal que así:

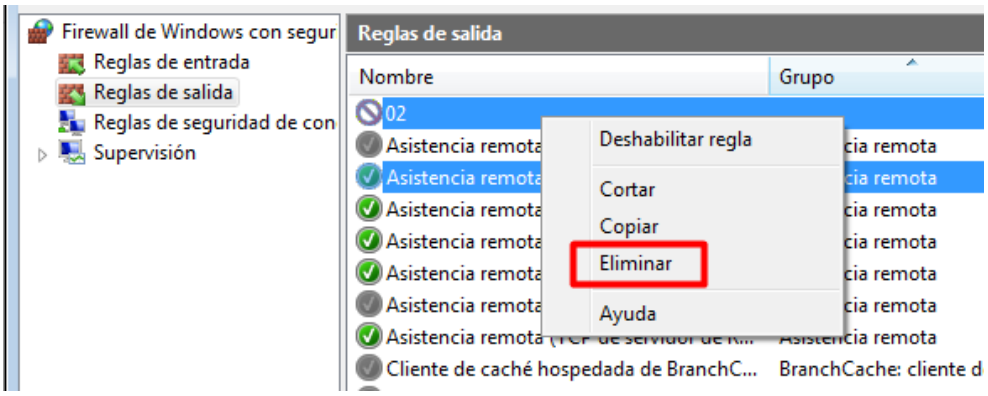




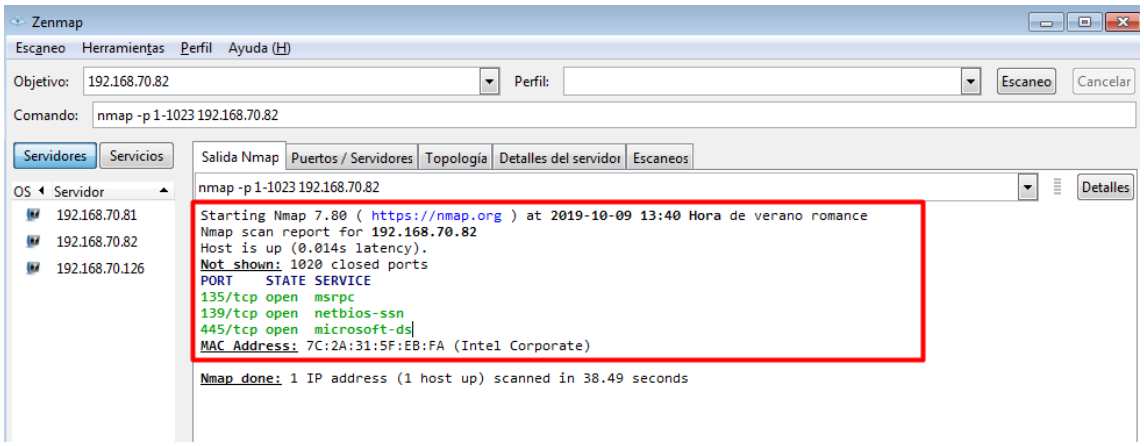
Vemos como dicho puerto ya no aparece abierto.



Para volver a abrirlo solo tendremos que eliminar la regla.

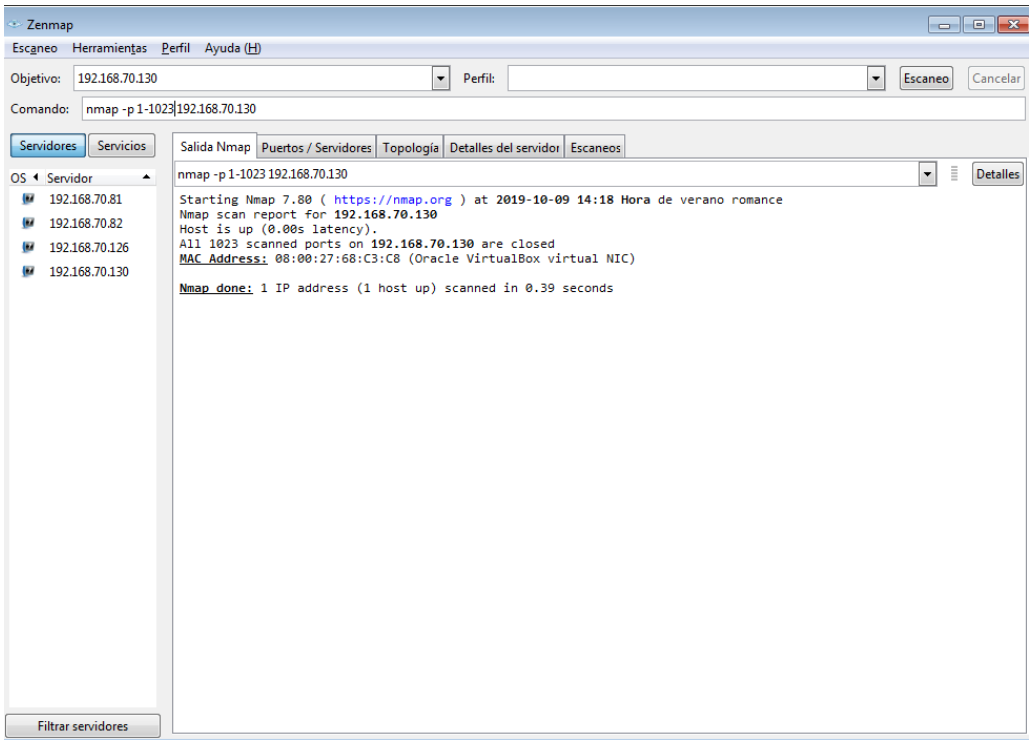


Después de eliminar la regla volveremos a ver como aparece de nuevo el puerto abierto.



Lo siguiente será realizar lo mismo, pero en Ubuntu. Abriremos el puerto 80 y 8080.

Con *nmap -p [rango puertos] [IP]* podremos buscar por rango de puertos. Vemos que no hay ningún puerto abierto.



Abriremos el puerto 80 y 8080.

sudo ufw allow 80

sudo ufw allow 8080

```
franciscojesus@sri-ubuntu18-practicas:~$ sudo ufw allow 80
[sudo] contraseña para franciscojesus:
Regla añadida
Regla añadida (v6)
franciscojesus@sri-ubuntu18-practicas:~$ sudo ufw allow 8080
Regla añadida
Regla añadida (v6)
```

```
franciscojesus@sri-ubuntu18-practicas:~$ sudo ufw reload
El cortafuegos se ha recargado
franciscojesus@sri-ubuntu18-practicas:~$ sudo ufw allow 443
Regla añadida
Regla añadida (v6)
```

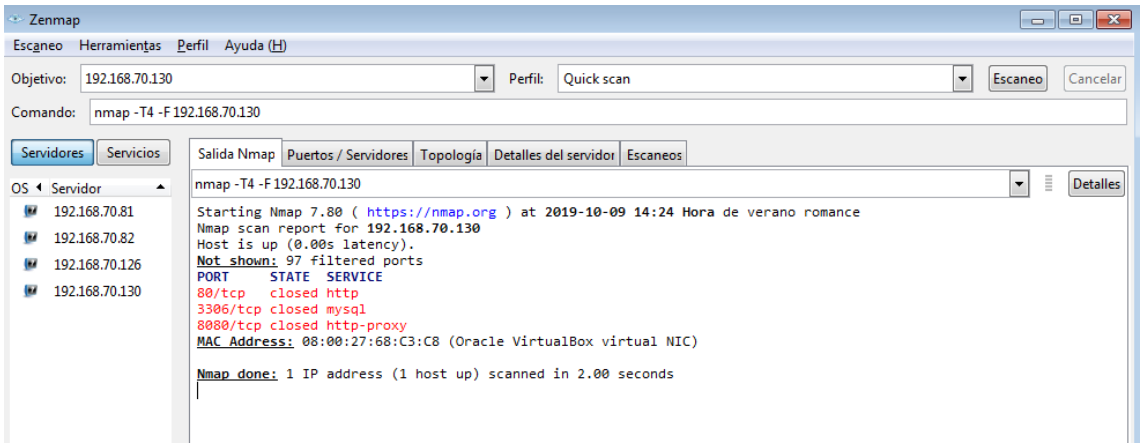
También lo podremos hacer con IPTables.

```
franciscojesus@sri-ubuntu18-practicas:~$ sudo iptables -A INPUT -p tcp -d 0/0 -s 0/0 --dport 8080 -j ACCEPT
```

Vemos que en *State* aparece como *Closed,* esto ocurre porque en Ubuntu, todos los puertos se abren a menos que tenga un firewall o una aplicación que lo esté bloqueando. En circunstancias normales, la aplicación que se ejecuta en el puerto es para escuchar.

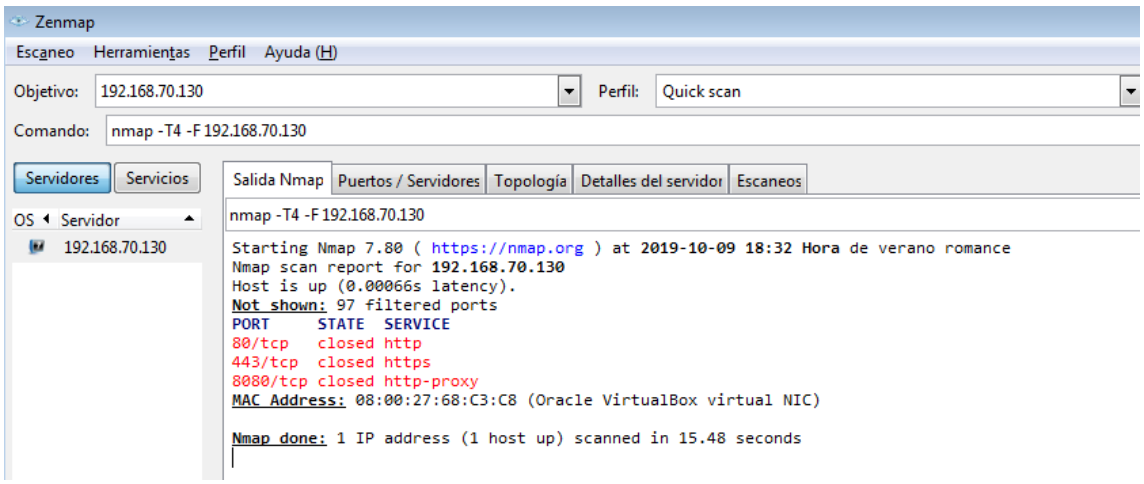
Un puerto generalmente se considera abierto cuando hay un programa ejecutándose y escuchando en el puerto.

Como vemos hemos abierto el puerto http y http-proxy.



Hemos cerrado el puerto MySQL y hemos abierto el https (443).

sudo ufw dwny 3306



**Nota: Puede que en algún momento tengamos que reiniciar UFW o IPTABLES.

sudo ufw disable

sudo ufw enable

sudo service iptables restart

Informe sobre Anti-Sniffer

¿Qué es y para qué sirve ARP?

En una red Ethernet cuando queremos enviar un paquete IP entre dos hosts conectados las únicas direcciones válidas son las MAC y lo que circula son tramas Ethernet. Entonces y volviendo al ejemplo de antes cuando queremos enviar un paquete IP lo que se hace es meter el paquete dentro de una trama Ethernet y enviar.

¿Cuál es el problema entonces?

El problema radica en que sabemos la dirección IP del host de destino, pero no su dirección MAC.

¿Cómo se soluciona esto?

La solución está en que antes de enviar el paquete IP se debe usar ARP para averiguar cuál es la dirección MAC del host destino de la conexión que pretendemos realizar.

Las técnicas de detección.

El test DNS

En este método, la herramienta de detección en sí misma está en modo promiscuo. Creamos numerosas conexiones TCP falsas en nuestro segmento de red, esperando un sniffer pobremente escrito para atrapar estas conexiones y resolver la dirección IP de los inexistentes hosts. Algunos sniffers realizan búsquedas inversas DNS en los paquetes que capturan. Cuando se realiza una búsqueda inversa DNS, una utilidad de detección de sniffers "huele" la petición de las operaciones de búsqueda para ver si el objetivo es aquel que realiza la petición del host inexistente.

El Test del Ping

Este método confía en un problema en el núcleo de la máquina receptora. Podemos construir una petición tipo "ICMP echo" con la dirección IP de la máquina sospechosa de hospedar un sniffer, pero con una dirección MAC deliberadamente errónea. Enviamos un paquete "ICMP echo" al objetivo con la dirección IP correcta, pero con una dirección de hardware de destino distinta. La mayoría de los sistemas desatenderán este paquete ya que su dirección MAC es incorrecta. Pero en algunos sistemas Linux, NetBSD y NT, puesto que el NIC está en modo promiscuo, el sniffer asirá este paquete de la red como paquete legítimo y responderá, por consiguiente.

Si el blanco en cuestión responde a nuestra petición, sabremos que está en modo promiscuo. Un atacante avanzado puede poner al día sus sniffers para filtrar tales paquetes para que parezca que el NIC no hubiera estado en modo promiscuo.

El Test ICMP

En este método, hacemos ping al blanco y anotamos el Round Trip Time (RTT, retardo de ida y vuelta o tiempo de latencia). Creamos centenares de falsas conexiones TCP en nuestro segmento de red en un período de tiempo muy corto. Esperamos que el sniffer esté procesando estos paquetes a razón de que el tiempo de latencia incremente. Entonces hacemos ping otra vez, y comparamos el RTT esta vez con el de la primera vez. Después de una serie de tests y medias, podemos concluir o no si un sniffer está realmente funcionando en el objetivo o no.

El test ARP

Podemos enviar una petición ARP a nuestro objetivo con toda la información rápida excepto con una dirección hardware de destino errónea. Una máquina que no esté en modo promiscuo nunca verá este paquete, puesto que no era destinado a ellos, por lo tanto, no contestará. Si una máquina está en modo promiscuo, la petición ARP sería considerada y el núcleo la procesaría y contestaría. Por la máquina que contesta, la sabemos estamos en modo promiscuo.

El test Etherping

Enviamos un "ping echo" al host a testear con una IP de destino correcta y dirección MAC falseada. Si el host responde, es que su interfaz está en modo promiscuo, es decir, existe un sniffer a la escucha y activo.

Protegerse contra la acción de los sniffers

A grandes rasgos para protegernos de los sniffers y para que éstos no cumplan sus objetivos de olfateo de contraseñas y en general nos "lean datos sensibles" en texto plano -sin cifrado fuerte, podemos hacer uso de diversas técnicas o utilizar sistemas como:

- Redes conmutadas (no siempre es efectivo)
- PGP
- SSL
- SSH
- VPN
- etc.

Conclusión

La práctica ha sido muy entretenida en conjunto con mi compañero Alex Valdepeñas, ha sido muy curioso ser uno el atacante y otro la victima y realizar el ataque mint. Prácticas así se aprende y entretiene uno realmente. En la práctica hemos podido realizar muchas cosas interesantes también como abrir y cerrar puertos en Windows y Linux o ataques de reconocimiento. Muy chula está práctica en grupos de 2.