Estudio de los flags TCP para detección de firewalls

Práctica 02

Gonzalo Tudela Chavero

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

INTRODUCCION

Para realizar esta práctica serán necesarias máquinas virtuales que se comuniquen entre sí. Aquellas máquinas que tengan el rol de servidor tendrán una configuración de red estática. Las máquinas para utilizar son:

- Kali Linux: tendrá el rol de máquina ofensiva para comprobar el estado de los puertos del servidor, firewall del servidor, etc...
- Windows Server 2016: tendrá el rol de servidor.

Para comprobar el estado de los puertos del servidor se utilizará una máquina Kali Linux con las siguientes herramientas:

- Nmap: `https://nmap.org/`
- Hping: `http://www.hping.org/`

CONFIGURACIÓN

Configura las dos máquinas a nivel de red para que se puedan comunicar. Envía un mensaje de tipo ICMP al servidor e interpreta de manera minuciosa qué es lo que está ocurriendo. ¿Llegan realmente las peticiones de tipo ICMP al servidor?

Configuramos Windows Server 2016 con una IP estática mediante el correspondiente panel.

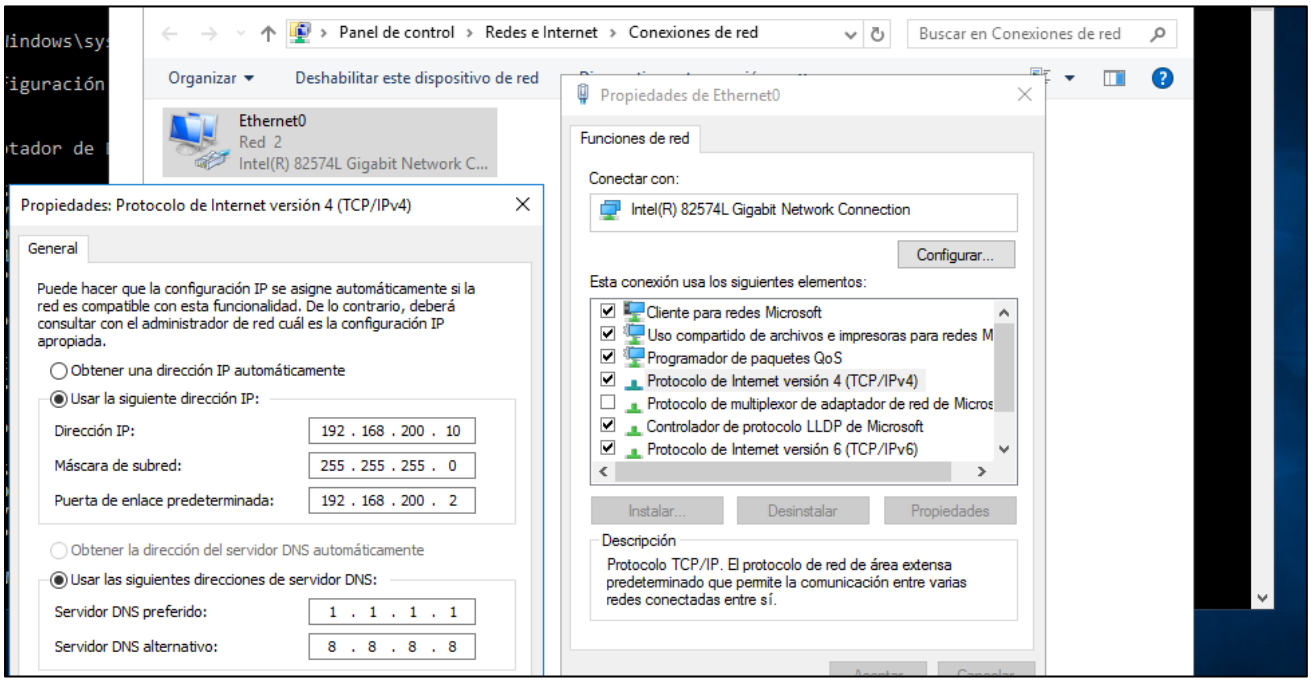

Ilustración 1 - Configuración IP estática en Windows Server.

Configuración permanente de Kali Linux mediante DHCP.

```
nano /etc/network/interfaces
```

```
  GNU nano 4.3                                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```

Ilustración 2 - Configuración DHCP para Kali Linux

Comprobamos mediante Hping3 enviando peticiones ICMP tipo 8 (echo) (-C 8) al servidor.

```
hping3 192.168.200.10 -C 8
```

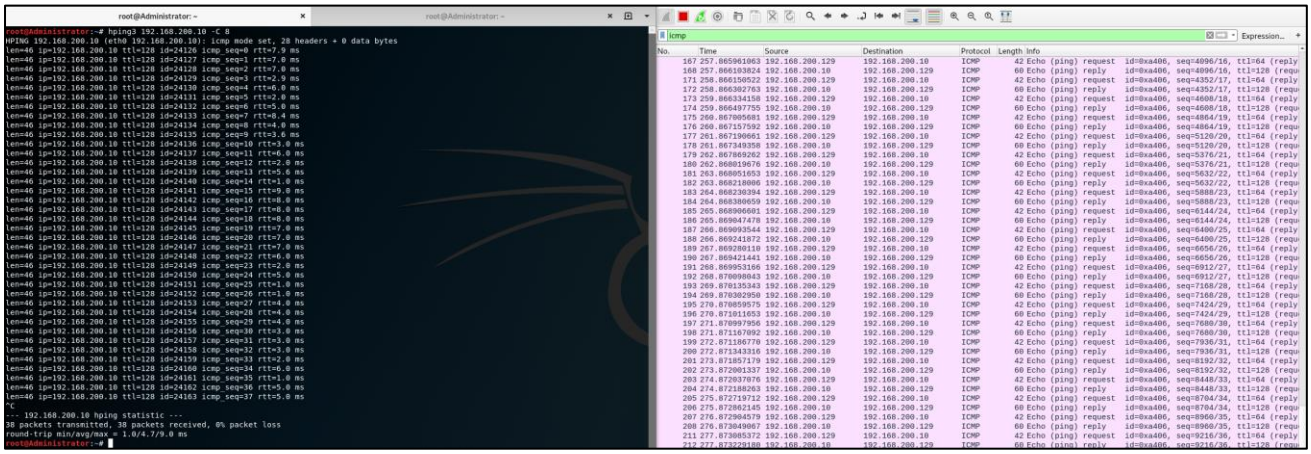

Ilustración 3 - Comprobación de las peticiones ICMP entre Kali y Servidor.

Comprobamos mediante ping enviando peticiones ICMP tipo 8 (echo) a Kali Linux.

```
ping 192.168.200.129
```

```
Administrador: Símbolo del sistema

C:\Windows\system32>ping 192.168.200.129

Haciendo ping a 192.168.200.129 con 32 bytes de datos:
Respuesta desde 192.168.200.129: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.200.129: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.200.129: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.200.129: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.200.129:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Windows\system32>
```

Ilustración 4 - Comprobación de Ping con Kali Linux.

ESCANEO

Realiza un escaneo con nmap a los puertos TCP del servidor Windows. Obtén la versión de cada uno de los servidores por defecto que trae la máquina después de la instalación. Indica qué parámetros has utilizado con nmap para obtener el estado real de todos los puertos TCP del servidor.

Escaneo preliminar completo.

Realizamos un primer escaneo rápido de los puertos (-T 5) sin resolver nombres (-n) del puerto 0 al 65535 (-p 0-65535) con el siguiente comando: (la velocidad T 5 puede dar falsos resultados en entornos reales)

nmap 192.168.200.10 -n -p 0-65535 -T 5

```
root@Administrator:~# nmap 192.168.200.10 -n -p 0-65535 -T 5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-21 23:21 CEST
Nmap scan report for 192.168.200.10
Host is up (0.00012s latency).
Not shown: 65530 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
49666/tcp open  unknown
49667/tcp open  unknown
MAC Address: 00:0C:29:22:AE:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 53.86 seconds
root@Administrator:~#
```

Ilustración 5 - Escaneo preliminar para descubrir puertos abiertos.

Escaneo dirigido.

Ahora realizamos un escaneo que comprueba que servicio esta tras cada puerto mediante (-sV):

nmap 192.168.200.10 -n -p 135,139,445,5985,49666,49667 -sV

```
root@Administrator:~# nmap 192.168.200.10 -n -p 135,139,445,5985,49666,49667 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-21 23:23 CEST
Stats: 0:00:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 23:23 (0:00:11 remaining)
Nmap scan report for 192.168.200.10
Host is up (0.00016s latency).

PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: WORKGROUP)
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:22:AE:66 (VMware)
Service Info: Host: WIN-ATDR3AC0U0D; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 53.94 seconds
root@Administrator:~#
```

Ilustración 6 - Escaneo en profundidad para obtener versión de los servicios.

HPING3

Utilizando la herramienta Hping3, realiza un escaneo de tipo "SYN" y de tipo "ACK" a uno de los puertos TCP (puedes usar el [445/TCP] e interpreta los resultados. Realiza lo mismo con la herramienta "nmap". ¿Influye el estado del firewall en el escaneo de los puertos?

El firewall de Windows Server está activo por defecto al arrancar, no se han realizado ningún tipo de modificación de su configuración.

Escaneo hping3 enviando SYN al puerto 445:

```
hping3 192.168.200.10 -c 1 -S -p 445
```

```
root@Administrator:~# hping3 192.168.200.10 -p 445 -S -c 1
HPING 192.168.200.10 (eth0 192.168.200.10): S set, 40 headers + 0 data bytes
len=46 ip=192.168.200.10 ttl=128 DF id=24411 sport=445 flags=SA seq=0 win=8192 rtt=8.0 ms

--- 192.168.200.10 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 8.0/8.0/8.0 ms
root@Administrator:~#
```

Ilustración 7 - Enviamos un paquete SYN al puerto 445 con hping3.

La respuesta es el siguiente paso en el HANDSHAKE, un SYN+ACK. El puerto esta abierto ya que desea establecer conexión.

Escaneo hping3 enviando ACK al puerto 445:

```
Hping3 192.168.200.10 -p 445 -A -c 1
```

```
root@Administrator:~# hping3 192.168.200.10 -p 445 -A -c 1
HPING 192.168.200.10 (eth0 192.168.200.10): A set, 40 headers + 0 data bytes

--- 192.168.200.10 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Administrator:~#
```

Ilustración 8 - El envío de un paquete ACK no devolvió ninguna respuesta.

No existe respuesta lo que nos indica que existe algo que esta capturando esas peticiones en concreto y no las contesta.

Escaneo nmap al puerto 445 mediante SYN:

```
nmap 192.168.200.10 -sS -p 445
```

```
root@Administrator:~# nmap 192.168.200.10 -sS -p 445
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-21 23:50 CEST
Nmap scan report for 192.168.200.10
Host is up (0.00013s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:22:AE:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@Administrator:~#
```

Ilustración 9 - Escaneo NMAP al 445 TCP con SYN.

Escaneo nmap al puerto 445 mediante ACK:

```
nmap 192.168.200.10 -sA -p 445
```

```
root@Administrator:~# nmap 192.168.200.10 -sA -p 445
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-21 23:56 CEST
Nmap scan report for 192.168.200.10
Host is up (0.00013s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:0C:29:22:AE:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
root@Administrator:~#
```

Ilustración 10 - Escaneo nmap al puerto 445 mediante ACK.

Podemos ver que nmap determina un puerto como filtrado cuando no recibe respuesta, es decir puede haber un firewall o no haber ningún servicio escuchando, este tipo de escaneos ACK tienen sentido en conjunto con un SYN para ver diferencias según sus mecánicas.

Desactivamos el firewall en Windows Server 2016 y repetimos las pruebas.

Configurado el firewall como se ve en la siguiente imagen procedemos a repetir las pruebas con hping3 y nmap.

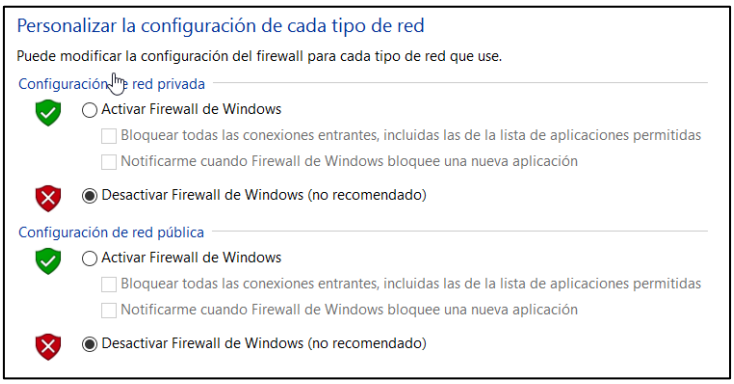

Ilustración 11 - Firewall desactivado.

Escaneo Hping3 SYN sin firewall.

```
root@Administrator:~# hping3 192.168.200.10 -S -c 1 -p 445
HPING 192.168.200.10 (eth0 192.168.200.10): S set, 40 headers + 0 data bytes
len=46 ip=192.168.200.10 ttl=128 DF id=12507 sport=445 flags=SA seq=0 win=8192 rtt=4.1 ms

--- 192.168.200.10 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 4.1/4.1/4.1 ms
root@Administrator:~#
```

Ilustración 12- Resultado Hping3 SYN al 445 sin firewall.

La respuesta es exactamente igual que con firewall solo que esta vez se produjo en la mitad de tiempo 8ms a 4ms.

Escaneo Hping3 ACK sin firewall.

```
root@Administrator:~# hping3 192.168.200.10 -A -c 1 -p 445
HPING 192.168.200.10 (eth0 192.168.200.10): A set, 40 headers + 0 data bytes
len=46 ip=192.168.200.10 ttl=128 DF id=12512 sport=445 flags=R seq=0 win=0 rtt=12.2 ms

--- 192.168.200.10 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.2/12.2/12.2 ms
root@Administrator:~#
```

Ilustración 13 - Resultado Hping3 ACK sin firewall.

En este caso el servidor si contesta, nos envía un reset, por lo que podemos deducir que el firewall estaba bloqueando este tipo de mensajes.

Escaneo Nmap SYN sin firewall.

```
root@Administrator:~# nmap 192.168.200.10 -n -sS -p 445
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-22 11:40 CEST
Nmap scan report for 192.168.200.10
Host is up (0.00028s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:50:54:9A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
root@Administrator:~#
```

Ilustración 14 - Escaneo Nmap SYN sin firewall.

Escaneo Nmap ACK sin firewall.

```
root@Administrator:~# nmap 192.168.200.10 -n -sA -p 445
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-22 11:45 CEST
Nmap scan report for 192.168.200.10
Host is up (0.00031s latency).

PORT    STATE      SERVICE
445/tcp unfiltered microsoft-ds
MAC Address: 00:0C:29:50:54:9A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.18 seconds
root@Administrator:~#
```

Ilustración 15 - Escaneo Nmap ACK sin firewall.

Ahora podemos ver como Nmap que sabe que un ACK no es modo de iniciar un handshake, y como ha recibido un RESET sabe que no hay un firewall filtrando (en este caso elimina comunicaciones que se salen de la regla) y nos etiqueta el puerto como Unfiltered, lo que suele ser habitual ya que Nmap se comporta de esta manera por defecto.

WINDOWS SERVER FIREWALL

Configura el firewall de Windows Server para que acepte una conexión TCP al puerto 12000 del servidor. Realiza los pasos del apartado anterior e interpreta los resultados.

Desactiva el firewall de los tres perfiles (perfil de dominio, público y privado) y repite al apartado anterior. ¿Qué conclusiones obtienes?

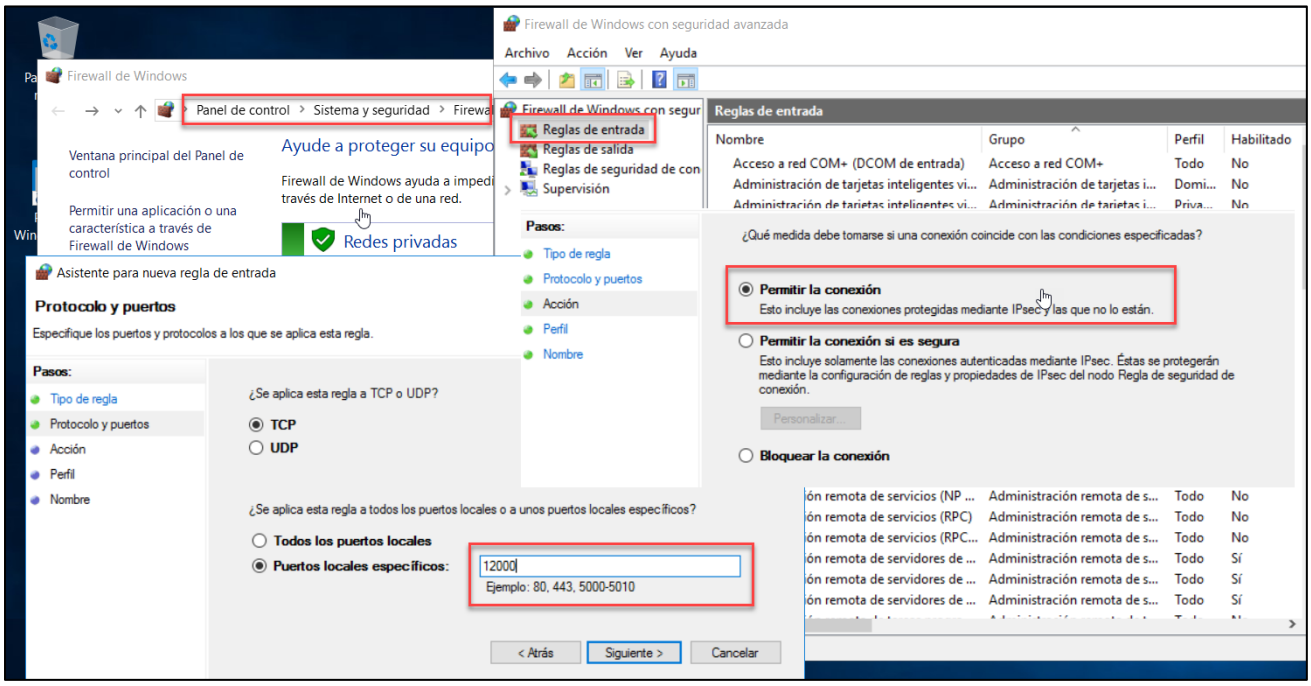

Ilustración 16 - Firewall Windows Server, puerto 12000

Una vez configurado el firewall para que acepte peticiones entrantes via TCP en el puerto 12000 procedemos a realizar las pruebas del apartado anterior.

Hping3 SYN con firewall permitiendo entrantes en 12.000 TCP:

```
root@Administrator:~# hping3 192.168.200.10 -c 1 -S -p 12000
HPING 192.168.200.10 (eth0 192.168.200.10): S set, 40 headers + 0 data bytes

--- 192.168.200.10 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Administrator:~#
```

Ilustración 17 - Hping3 flag SYN al puerto 12.000 TCP, firewall habilitado y permitiendo entrantes.

Hping3 informa de que no hubo respuesta.

Hping3 ACK con firewall permitiendo entrantes en 12.000 TCP:

```
root@Administrator:~# hping3 192.168.200.10 -c 1 -A -p 12000
HPING 192.168.200.10 (eth0 192.168.200.10): A set, 40 headers + 0 data bytes

--- 192.168.200.10 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@Administrator:~#
```

Ilustración 18 - Hping3 flag ACK al puerto 12.000 TCP, firewall habilitado y permitiendo entrantes.

Hping3 informa de que no hubo respuesta.

Nmap SYN con firewall permitiendo entrantes en 12.000 TCP:

```
root@Administrator:~# nmap 192.168.200.10 -sS -n -p 12000
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-22 15:46 CEST
Nmap scan report for 192.168.200.10
Host is up (0.00013s latency).

PORT      STATE    SERVICE
12000/tcp filtered cce4x
MAC Address: 00:0C:29:22:AE:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
root@Administrator:~#
```

Ilustración 19 - Nmap SYN al puerto 12.000 con firewall habilitado y permitiendo entrantes.

Nmap informa de que el puerto puede estar filtrado o que no hubo respuesta.

Nmap ACK con firewall permitiendo entrantes en 12.000 TCP:

```
root@Administrator:~# nmap 192.168.200.10 -sA -n -p 12000
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-22 15:48 CEST
Nmap scan report for 192.168.200.10
Host is up (0.00014s latency).

PORT      STATE    SERVICE
12000/tcp filtered cce4x
MAC Address: 00:0C:29:22:AE:66 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
root@Administrator:~#
```

Ilustración 20 - Nmap SYN al puerto 12.000 con firewall habilitado y permitiendo entrantes.

Nmap informa de que el puerto puede estar filtrado o que no hubo respuesta.

Desactivamos el firewall de Windows Server 2016 y repetimos las pruebas del puerto 12.000 TCP:

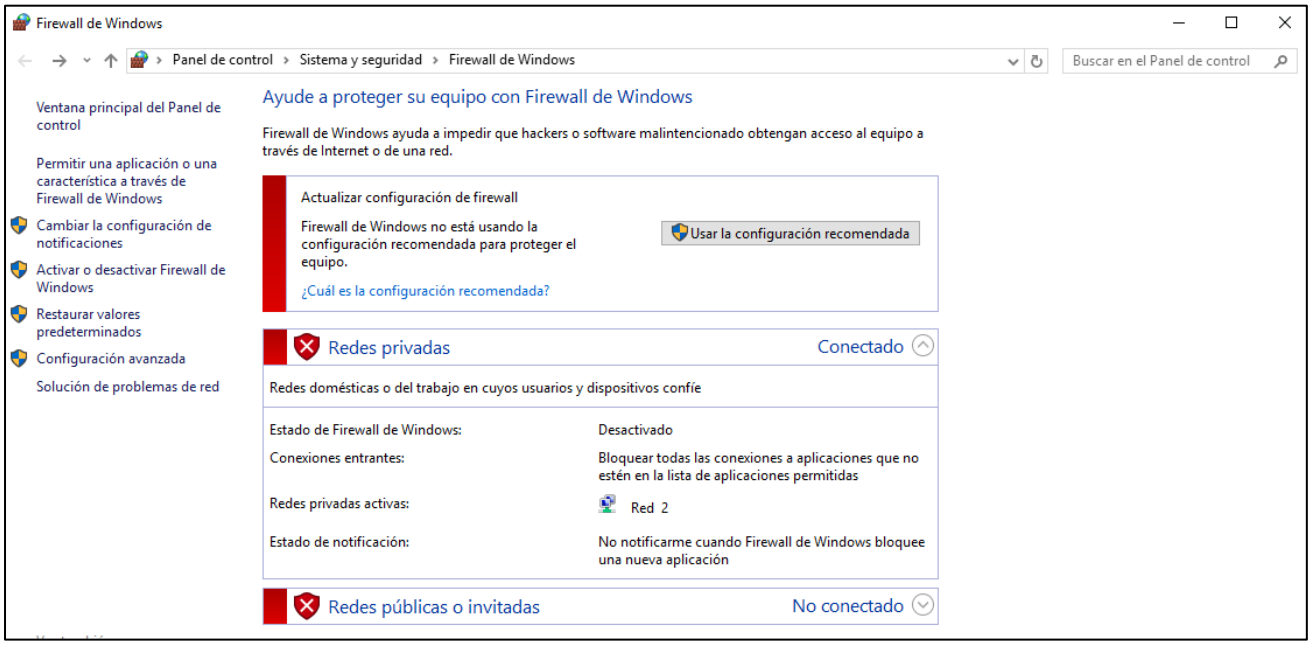

Ilustración 21 - Firewall desactivado.

Hping3 SYN sin firewall activado:

```
root@Administrator:~# hping3 192.168.200.10 -c 1 -S -p 12000
HPING 192.168.200.10 (eth0 192.168.200.10): S set, 40 headers + 0 data bytes
len=46 ip=192.168.200.10 ttl=128 DF id=0 sport=12000 flags=RA seq=0 win=0 rtt=7.9 ms

--- 192.168.200.10 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 7.9/7.9/7.9 ms
root@Administrator:~#
```

Ilustración 22 - Hping3 flag SYN al puerto 12.000 TCP, firewall desactivado.

Hping3 a pesar de que no hay ningún servicio escuchando en ese puerto, recibimos un paquete de vuelta, esta vez una respuesta RESET+ACK que podemos interpretar como un rechazo cortés de la conexión.

Hping3 ACK sin firewall activado:

```
root@Administrator:~# hping3 192.168.200.10 -c 1 -A -p 12000
HPING 192.168.200.10 (eth0 192.168.200.10): A set, 40 headers + 0 data bytes
len=46 ip=192.168.200.10 ttl=128 DF id=1 sport=12000 flags=R seq=0 win=0 rtt=3.9 ms

--- 192.168.200.10 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.9/3.9/3.9 ms
root@Administrator:~#
```

Ilustración 23 - Hping3 flag ACK al puerto 12.000 TCP, firewall desactivado.

Hping3 recibe un paquete de respuesta con el flag RESET, comportamiento típico de que el puerto no está cerrado, pero rechaza ese inicio del handshake (espera un SYN).

Nmap SYN sin firewall activado:

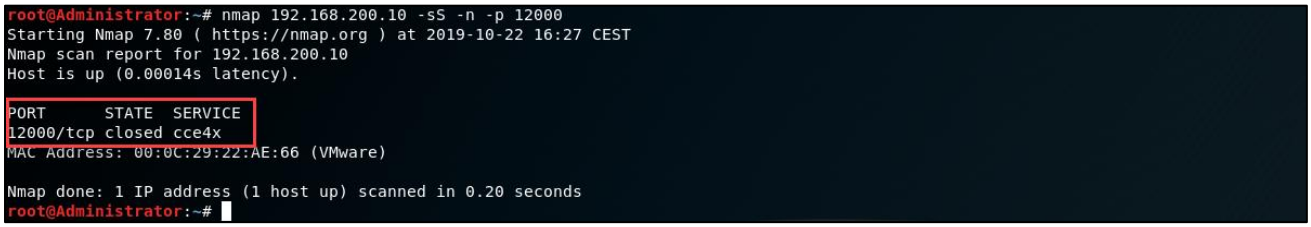

Ilustración 24 - Nmap SYN al puerto 12.000 con firewall desactivado.

Nmap informa de que el puerto está cerrado, lo que me da que pensar, ya que el estado abierto o cerrado de un puerto parece tener que ver con si existe un servicio escuchando o no.

Nmap ACK sin firewall activado:

Ilustración 25 - Nmap ACK al puerto 12.000 con firewall desactivado.

Nmap informa de que el puerto no está filtrado, ya que ha recibido respuesta, pero no hay nadie escuchando.

TABLA RESUMEN DE LOS RESULTADOS

HPING 3

	FIREWALL DENEGANDO		FIREWALL PERMITIENDO		SIN FIREWALL	
FLAG	SERVICIO ESCUHANDO	SIN SERVICIO	SERVICIO ESCUHANDO	SIN SERVICIO	SERVICIO ESCUCHANDO	SIN SERVICIO
SYN	packet loss	packet loss	Syn+Ack	packet loss	Syn+Ack	Reset+Ack
ACK	packet loss	packet loss	packet loss	packet loss	Reset	Reset

NMAP

	FIREWALL DENEGANDO		FIREWALL PERMITIENDO		SIN FIREWALL	
FLAG	SERVICIO ESCUHANDO	SIN SERVICIO	SERVICIO ESCUHANDO	SIN SERVICIO	SERVICIO ESCUCHANDO	SIN SERVICIO
SYN	filtered	filtered	Open	filtered	Open	Closed
ACK	filtered	filtered	filtered	filtered	Unfiltered	Unfiltered

Ilustración 26 - Tabla resumen de los resultados.

PERFILES DEL FIREWALL

Explica con tus palabras qué diferencia existe en el firewall de Windows Server entre los siguientes perfiles: perfil de dominio, perfil público y perfil privado. Por un ejemplo.

Los perfiles de Firewall en Windows server son diferentes conjuntos de reglas dependiendo del ámbito de la red, para una red organizada en un dominio, una red considerada como publica (reglas mas estrictas) o redes privadas en las que podríamos configurar un conjunto de reglas más permisivas.

Por ejemplo, podríamos tener un adaptador de red que conecta con una red publica como internet que estuviese sujeto a las reglas de redes publicas ofreciendo una seguridad mayor y otras reglas para la red local en la que se supone una confianza en los hosts que la pueblan y por tanto aplicaríamos unas reglas mas flexibles en el firewall.

Ejemplo de creación de una regla, en un paso del asistente se nos pregunta por el ámbito en el que se aplicará.

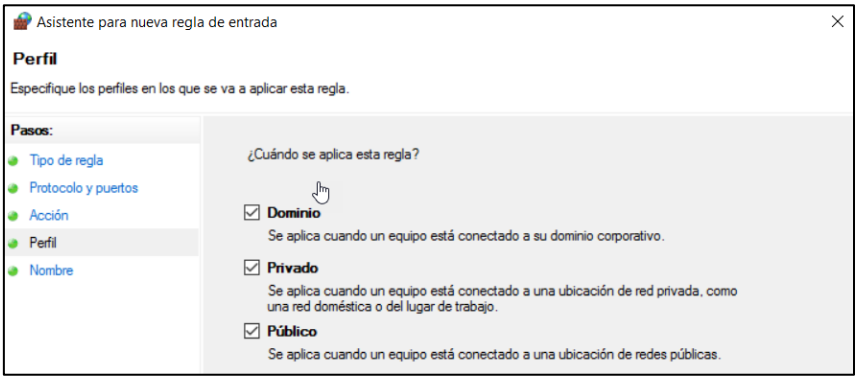

Ilustración 27 - Perfil de aplicación para una regla de firewall.