Registro de ataques con el Firewall
Práctica 10C

1. Objetivo

En esta práctica el alumno debe comprender la información que registra (o no registra) el FW en relación con diferentes tipos de ataques, escaneos, y anomalías en el tráfico que entra y sale de un computador.

En la sección 2 se explica la activación y desactivación del registro del FW de Windows y la selección de lo que registra el FW, que no es todo el tráfico de red que entra/sale del computador, sino unas acciones concretas realizadas por el FW.

En la sección 3 se presenta la herramienta Nping para generar tráfico de paquetes.

En las secciones siguientes se van explicando ataques, escaneos, etc.

Esta práctica debe realizarse con DOS MVs:
- La 1ª MV actúa como víctima/servidor defendida por su FW.
- La 2ª MV actúa como atacante/cliente que realiza ataques, escaneos, inyecta tráfico, etc.

Hay dos formas de realizar la práctica:
Entre dos alumnos: la MV de un alumno actúa como atacante y la del otro como víctima.
Un solo alumno: para usar DOS MVs puede clonar su MV, asignando a sus dos MVs 5GB de RAM.

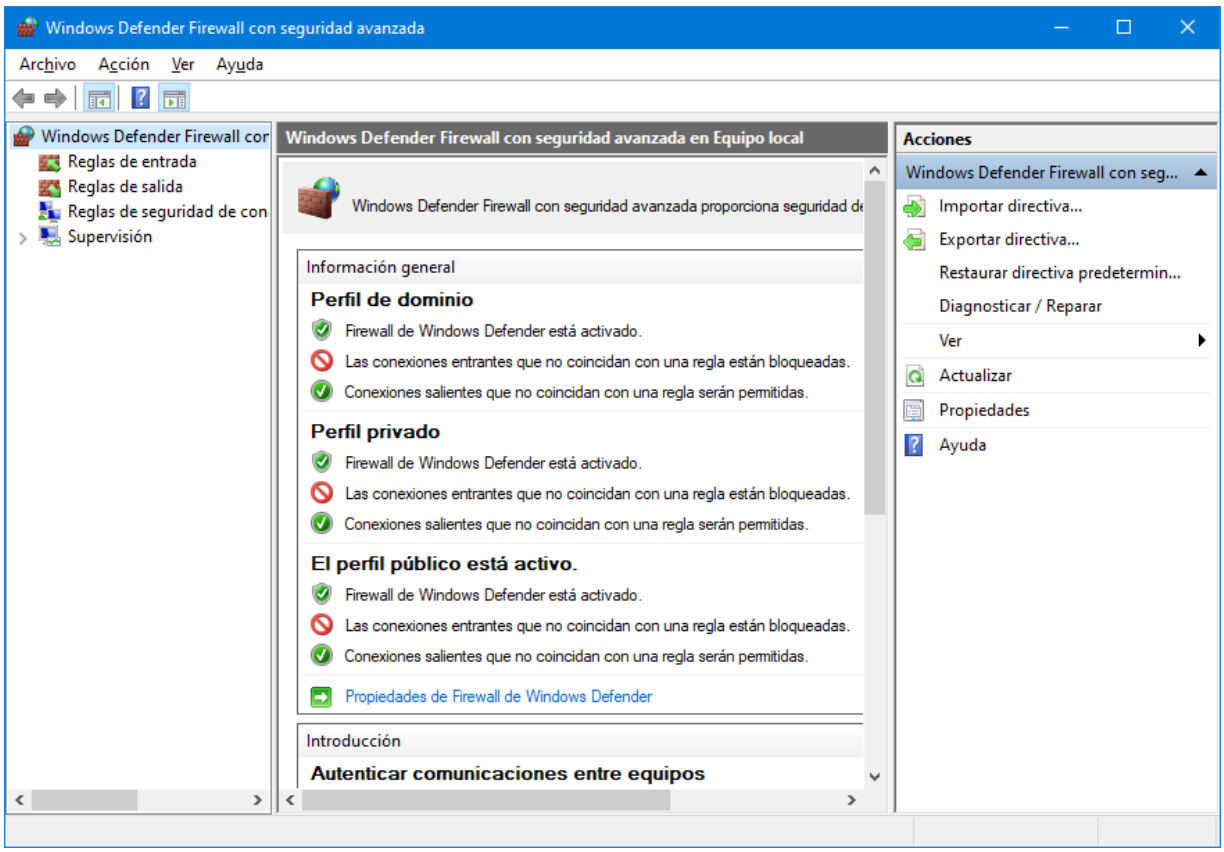
2. El registro del FW

El sistema operativo Windows registra información sobre las acciones que realiza el FW en dos formatos distintos:

- En formato de eventos en el Registro de Seguridad de Windows (explicado en una práctica posterior).
- En formato de texto en el Registro del Firewall (explicado en esta práctica).

Activación del registro del FW

La primera tarea a realizar es indicar al Firewall que genere registros de las acciones que realiza con los paquetes de red que controla. Para ello hay que abrir la consola de gestión del "Firewall de Windows con seguridad avanzada", por ejemplo tecleando **wf.msc** en el botón inicio de Windows.

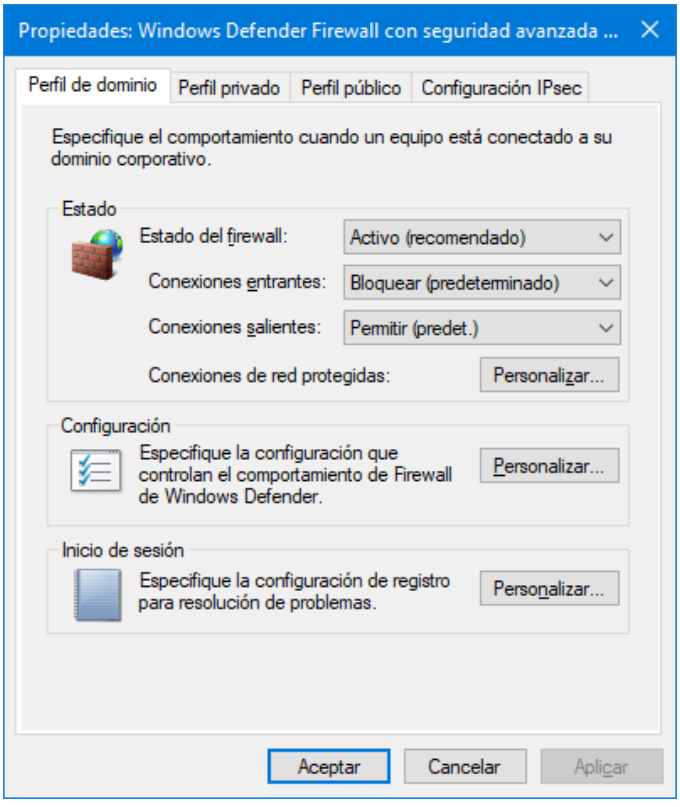


Desde esta ventana hay que acceder a la ventana de propiedades de alguna de estas formas:

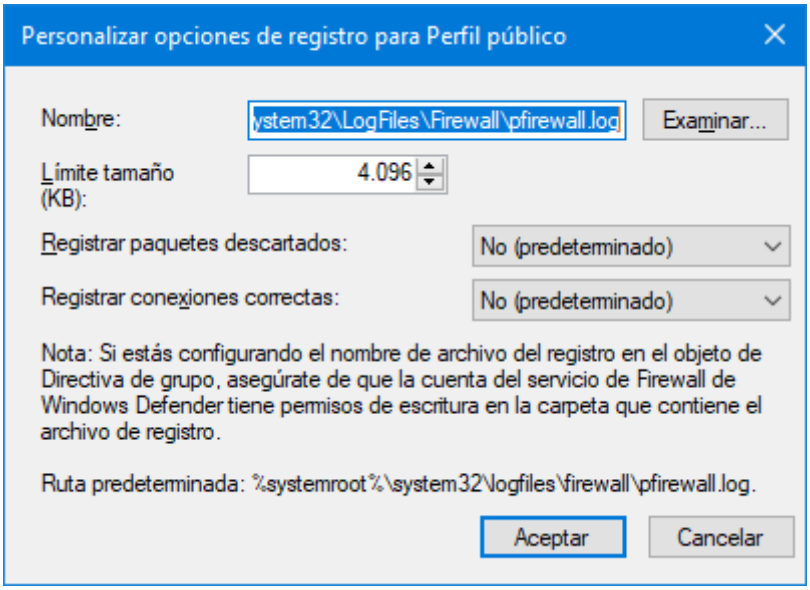
1) En el panel izquierdo coloca el puntero del ratón sobre la raíz del árbol mostrado y haz clic en el botón derecho. En el menú contextual que aparece selecciona “Propiedades”.

2) En el panel central selecciona la opción “Propiedades de Firewall de Windows Defender”.

3) En el panel derecho selecciona la acción “Propiedades”.



Comprobar que hay tres perfiles de utilización del Firewall: dominio, privado y público. Si se está trabajando en el perfil público, seleccionar su pestaña, y luego pulsar el botón "Personalizar..." en el cuadro inferior de “Inicio de sesión”. Aparece la ventana siguiente:



Para activar el registro cambiar las opciones siguientes:

- Registrar paquetes descartados: Sí
- Registrar conexiones correctas: Sí

Si no se activa al menos una de estas dos opciones, el Firewall no registra nada.

Además, cada vez que se realice un experimento (emulación de un ataque) es conveniente cambiar el Nombre del registro del FW, para que el fichero contenga solo las acciones del FW correspondientes a ese experimento.

Registro con el tráfico base

El primer experimento a realizar consiste en activar el registro del FW de un computador (físico o virtual) sin realizar ninguna generación deliberada de tráfico hacia/desde el computador. Esto permite ver qué acciones registra el FW con solo el tráfico base o de fondo que llega a la interfaz de red del computador.

Para iniciar el experimento poner las dos opciones de registro en **Si** y para terminar el experimento poner las dos opciones de registro en **No**. Después copia el fichero con el registro (pfirewall.log) a un directorio del usuario. Ahora se puede abrir el fichero pfirewall.log con cualquier editor de ficheros de texto.

Al registrar las acciones del FW durante 100 segundos en un computador conectado a la red de UniOvi se registran 580 acciones. Por tanto, el promedio es de 5,8 acciones/segundo, pero hay un segundo en el que se registraron 28 acciones. Comprueba que la mayoría de las acciones son DROP y el protocolo es UDP.

Si se realiza este mismo registro en un computador usado en el hogar y conectado a un router que usa NAT el número de acciones registrado será típicamente mucho menor.

3. La herramienta Nping

Nping es una herramienta para la generación de paquetes de red. Se distribuye conjuntamente con la herramienta de escaneo Nmap. Se puede ver la información general en:

https://nmap.org/nping/

La guía de referencia para usar Nping se puede encontrar en:

https://nmap.org/book/nping-man.html

Abre una consola y ejecuta Nping. Aparece una descripción de cómo usar Nping.

El uso normal de Nping es:

Nping [probe mode] [options] {target specifications}

Nping [modo de sondeo] [opciones] {especificación de objetivos}

Prueba el funcionamiento usando el modo --icmp con las opciones --icmp-type y –icmp-code, y especificando al final del comando la IP objetivo.

Utilizar Wikipedia como recordatorio del protocolo ICMP:

https://es.wikipedia.org/wiki/Protocolo_de_control_de_mensajes_de_Internet

Utiliza Tipo ICMP = 8 y Código ICMP = 0 para realizar una petición “Echo Request”.

Nping --icmp --icmp-type 8 --icmp-code 0 156.35.123.45

Antes de usar el comando comprueba en el computador objetivo la regla del Firewall “Archivos e impresoras compartidos (petición de eco: ICMPv4 de entrada)” está habilitada para el perfil que esté usando el adaptador de red, que típicamente será el “Privado, Público”.

Al habilitar esta regla, observar que la dirección remota está restringida a las direcciones IP de la “Subred local”. Si es necesario editar las propiedades de la regla y en la pestaña “Ámbito” asignar la Dirección IP remota a “Cualquier dirección IP”.

Observa que Nping indica los valores máximo, mínimo y promedio de RTT (Round-Trip Time) entre cada paquete enviado y su respuesta, que será de unos 1000 milisegundos, ya que Nping envía una petición cada segundo.

Si se desea generar un tráfico intenso que emule un ataque de denegación de servicio será necesario incrementar la velocidad con la que se envían paquetes.

Opciones para controlar la velocidad de envío de paquetes

Nping proporciona dos opciones para especificar la velocidad a la que se generan paquetes.

Estas opciones se denominan como temporales y de rendimiento (timing and performance):

https://nmap.org/book/nping-man-timing-performance-options.html

--delay <tiempo>

Indica el tiempo que Nping espera antes de enviar el siguiente paquete (probe). El valor por defecto es 1 segundo. El tiempo se indica por defecto en segundos, pero se pueden indicar las unidades detrás del número: ms, s, m, h.

--rate <velocidad>

Indica el número de paquetes (probes) que Nping deberá enviar por segundo.

Las dos opciones son inversas: --rate 20 es igual que --delay 0.05. Si se usan ambas opciones, Nping solo usa la última especificada en la lista de opciones.

Realiza una prueba reduciendo el tiempo entre peticiones sucesivas:

Nping --icmp --icmp-type 8 --icmp-code 0 --delay 100ms 156.35.123.45

Prueba con valores de delay menores y finalmente con cero.

Observa los tiempos RTT y la pérdida de paquetes.

4. Ataque con mensajes ICMP

El objetivo es emular un ataque de denegación de servicio por inundación de mensajes ICMP del tipo Petición eco (Echo Request), con Tipo ICMP = 8 y Código ICMP = 0.

Preparación del comando de ataque

Para maximizar el ratio de peticiones/segundo enviadas, utiliza la opción --delay 0.

Además es necesario enviar un número total de paquetes grande, para que el ataque emulado tenga una duración apreciable. Para ello utiliza la opción --count 20 para enviar 20 peticiones.

Nping --icmp --icmp-type 8 --icmp-code 0 --count 20 --delay 0ms 156.35.123.45

Al utilizar un número de peticiones elevado es necesario reducir el nivel de verbosidad (cantidad) de la información de salida visualizada. Utiliza la opción –vN, donde N es el número 0 para tener una verbosidad normal, números positivos para incrementarla y negativos para disminuirla. Por ejemplo, utiliza el siguiente comando:

Nping --icmp --icmp-type 8 --icmp-code 0 --count 1000 --delay 0ms -v-1 156.35.123.45

Comprobación de la efectividad del ataque

Con una pareja de computadores operando uno como cliente y otro como servidor, el comando realiza las 1000 peticiones y recibe las respuestas en un tiempo de 0,4 segundos. Esto supone una frecuencia de 2500 peticiones+respuestas/segundo.

Esta frecuencia de peticiones no es suficiente para saturar los recursos del computador atacado. Para comprobarlo, arranca el Administrador de Tareas en el computador atacado y selecciona la pestaña Rendimiento. Después, ejecuta el comando Nping pero usando –count 30000 para que dé tiempo a observar la utilización de la CPU y la RED del computador atacado en el Administrador de Tareas. Sería necesario usar múltiples atacantes.

Análisis del registro por el FW de la inundación de mensajes ICMP

En el computador atacado abre una ventana del Administrador de Archivos y colócate en el directorio C:\Windows\System32\LogFiles\Firewall\ que es donde el FW guarda los registros. Si contiene un fichero denominado pfirewall.log bórralo, para partir de un fichero nuevo vacío.

Si incluso aplicando permisos de administrador, no se puede borrar el fichero porque un componente de Windows tiene abierto el archivo, tendrás que poner al FW en su perfil público en estado inactivo. Después borrar el fichero y seguidamente volver a activar el FW.

Realiza los dos experimentos que se describen a continuación.

EXPERIMENTO ICMP 1: Enviar mensajes con una regla del FW existente y **SI** habilitada en el perfil privado y público.

Borra el fichero pfirewall.log si existe.

Habilita la regla: Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada).

(También puede haber otra regla igual deshabilitada para el perfil dominio).

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

Nping --icmp --icmp-type 8 --icmp-code 0 --count 1000 --delay 0ms -v-1 156.35.123.45

El envío de los 1000 paquetes se realiza en menos de 1 segundo y hay casi 1000 respuestas.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el FW registra 1000 líneas como la siguiente:

aaaa-mm-dd hh:mm:ss ALLOW ICMP 156.35.163.82 156.35.123.45 - - 0 - - - - 8 0 - RECEIVE

EXPERIMENTO ICMP 2: Enviar mensajes con una regla del FW existente y **NO** habilitada en el perfil privado y público.

Borra el fichero pfirewall.log si existe.

Deshabilita la regla: Archivos e impresoras compartidos (petición eco: ICMPv4 de entrada).

(También puede haber otra regla igual deshabilitada para el perfil dominio).

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

Nping --icmp --icmp-type 8 --icmp-code 0 --count 1000 --delay 0ms -v-1 156.35.123.45

El envío de los 1000 paquetes se realiza en menos de 1 segundo y no hay ninguna respuesta.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el FW registra 1000 líneas como la siguiente:

aaaa-mm-dd hh:mm:ss DROP ICMP 156.35.163.82 156.35.123.45 - - 28 - - - - 8 0 – RECEIVE

¿Cuál es la capacidad del FW para registrar ataques con mensajes ICMP?

Copia el texto blanco del cuadro en notepad para ver la solución.

Mejorar la efectividad del ataque

El ataque denominado “ping de la muerte” consiste en enviar una petición de eco ICMP pero con una carga (payload) grande en el paquete IP. El comando Nping puede ser:

Nping --icmp --icmp-type 8 --icmp-code 0 --data-length 1000 --count 100 --delay 1s 156.35.123.45

Con este comando Nping envía peticiones de eco a un mensaje de 1000 bytes generados aleatoriamente en el primer envío y luego reutilizados en los envíos siguientes.

Con un delay de 1 segundo entre peticiones sucesivas Nping recibe el eco de todas las peticiones enviadas hasta un –data-length 1400. Por encima de este valor Nping genera un WARNING:

“Payload exceeds the maximum recommended payload (1400)”

Y no se recibe ninguna respuesta o eco.

Nping permite un tamaño máximo de payload de 65400 bytes.

Un comando más agresivo podría ser:

Nping --icmp --icmp-type 8 --icmp-code 0 --data-length 65400 --count 50000 --delay 0s 156.35.123.45

Pero este comando no satura ni la red ni la CPU del computador destino.

Realiza experimentos para determinar cuál es el ataque más efectivo que se puede realizar con esta técnica.

5. Ataque a un servidor TCP

El objetivo es emular un ataque de denegación de servicio por inundación de peticiones a un servidor TCP. El ataque desde un solo cliente nunca será realista ni efectivo, pero servirá para aprender los conceptos básicos sobre ataques y su registro por el FW.

Preparación del servidor TCP

Utiliza el programa pServidor, pero como el programa Nping solo establece conexiones, comenta la parte de recepción de la petición, procesamiento, y envío de la respuesta. En el bucle infinito de procesamiento de peticiones solo se debe usar: (1) la aceptación de una conexión, (2) mostrar la dirección IP y el puerto remotos, (3) el cierre de la conexión.

Una vez que se ejecuta en la MV servidora se crean automáticamente dos reglas para permitir el acceso, una para UDP y otra para TCP. En las reglas, la dirección IP local puede ser cualquiera.

Preparación del comando de ataque

Nping proporciona dos modos para generar paquetes TCP:

Modo --tcp-connect: establece una conexión con un servidor TCP completando los tres mensajes del Handshake TCP. La conexión la establece usando la función connect() de la API de Sockets.

Modo --tcp: se puede crear y enviar cualquier clase de paquete TCP. Por ejemplo, para descubrir puertos abiertos, enviando un paquete TCP SYN sin completar los tres mensajes del Handshake. Una respuesta SYN/ACK indica que el puerto está abierto y una respuesta RST indica que está cerrado.

Inicialmente usar el modo –tcp-connect.

Nping --tcp-connect --dest-port 2459 156.35.151.51

Este comando realizará cinco conexiones un intervalo de un segundo entre cada conexión. Si Nping muestra las peticiones y la confirmación del establecimiento de cada conexión, todo es correcto.

Realiza los dos experimentos que se describen a continuación.

EXPERIMENTO TCP 1: Enviar mensajes a un puerto IP en el que **SI escucha** un servicio y en el FW **SI hay una regla habilitada** en el perfil público.

Borra el fichero pfirewall.log si existe. Activa el FW.

Habilita la regla: pServidor.

Arranca el servicio pServidor.exe

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

Nping --tcp-connect --dest-port 2459 --count 100 --delay 0ms -v-1 156.35.123.45

El envío de los 1000 paquetes se realiza en menos de 1 segundo y hay 100 conexiones correctas.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el **FW registra** 100 líneas como la siguiente:

aaaa-mm-dd hh:mm:ss ALLOW TCP 156.35.163.29 156.35.123.45 53845 2459 0 - 0 0 0 - - - RECEIVE

EXPERIMENTO TCP 2: Enviar mensajes a un puerto IP en el que **SI escucha** un servicio y en el FW **SI hay una regla deshabilitada** en el perfil público.

Borra el fichero pfirewall.log si existe. Activa el FW.

Deshabilita la regla: pServidor.

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

Nping --tcp-connect --dest-port 2459 --count 100 --delay 0ms -v-1 156.35.123.45

El envío de los 100 paquetes se realiza en unos 4 segundos y no hay conexiones correctas.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el **FW registra** más de 200 líneas como la siguiente:

aaaa-mm-dd hh:mm:ss DROP TCP 156.35.163.29 156.35.123.45 53897 2459 52 S 2624628890 0 64240 - - - RECEIVE

Parece que cada conexión se reintenta varias veces antes de desistir.

EXPERIMENTO TCP 3: Enviar mensajes a un puerto IP en el que **NO escucha** un servicio y en el FW **NO hay una regla** en el perfil público para el puerto.

Borra el fichero pfirewall.log si existe. Activa el FW.

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

Nping --tcp-connect --dest-port 2460 --count 100 --delay 0ms -v-1 156.35.123.45

El envío de los 100 paquetes se realiza en unos 4 segundos y no hay conexiones correctas.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el FW **NO registra** ni uno de los intentos de conexión TCP fallidos.

EXPERIMENTO TCP 4: Enviar mensajes a un puerto IP en el que **NO escucha** un servicio y en el FW **SI hay una regla habilitada** en el perfil público para el puerto.

Crea y habilita una regla que permita el tráfico entrante al puerto 2640. Denomínala SINservicio.

Borra el fichero pfirewall.log si existe. Activa el FW.

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

Nping --tcp-connect --dest-port 2460 --count 100 --delay 0ms -v-1 156.35.123.45

El envío de los 100 paquetes se realiza en unos 4 segundos y no hay conexiones correctas.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el FW **NO registra** ni uno de los intentos de conexión TCP fallidos.

EXPERIMENTO TCP 5: Enviar mensajes a un puerto IP en el que **NO escucha** un servicio y en el FW **SI hay una regla deshabilitada** en el perfil público para el puerto.

Deshabilita la regla que permite el tráfico entrante al puerto 2640.

Borra el fichero pfirewall.log si existe. Activa el FW.

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

Nping --tcp-connect --dest-port 2460 --count 100 --delay 0ms -v-1 156.35.123.45

El envío de los 100 paquetes se realiza en unos 4 segundos y no hay conexiones correctas.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el FW **NO registra** ni uno de los intentos de conexión TCP fallidos.

Los experimentos TCP 4 y TCP 5 se han realizado también con una regla para permitir el tráfico. Puedes comprobar que si la regla se crea para bloquear el tráfico, el resultado es el mismo. El FW no registra ninguno de los intentos de conexión fallidos.

¿Cuál es la capacidad del FW para registrar ataques a servidores TCP?

Copia el texto blanco del cuadro en notepad para ver la solución.

Ahora debes comprobar como registra el FW las comunicaciones entre pCliente y pServidor, como paso previo para realizar un ataque de denegación de servicio a un puerto TCP usando un cliente desarrollado y programado personalmente.

En la MV, borra el fichero pfirewall.log si existe. Activa el FW.

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

En la MF, ejecuta pCliente, que realiza 10 conexiones sucesivas y envía/recibe un mensaje.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el FW **SI registra** diez líneas como ésta:

aaaa-mm-dd hh:mm:ss ALLOW TCP 156.35.151.71 156.35.123.45 52680 2459 0 - 0 0 0 - - - RECEIVE

(Busca con el editor del notepad el puerto de destino 2459).

Hay que comprobar el comportamiento en condiciones de ataque, esto es, aumentando la frecuencia de envío de peticiones y su tamaño.

6. Escaneo de un servidor TCP

El objetivo de esta sección es aprender a trabajar con Nping con el modo --tcp, que se usa típicamente para escanear un puerto concreto de un computador en el que se supone que escucha un servidor TCP. También se compara el funcionamiento de Nping con Nmap. Para ello se realizan varios experimentos.

Preparación del comando de escaneo

Habilita en el FW la regla que permite el tráfico TCP entrante al puerto 2459 o a la aplicación pServidor.exe.

Arranca el programa pServidor.exe que solo consume conexiones TCP.

Nping --tcp --dest-port 2459 --flags SYN --count 1 -delay 1s 156.35.123.45

Observa en la consola de Nping:

Se envía un paquete con el flag S (SYN) y se reciben dos paquetes con los flags SA (SYN/ACK). Parece que el servidor, tras enviar la primera respuesta SYN/ACK a Nping y no recibir la respuesta ACK para completar el handshake TCP, envía una segunda respuesta SYN/ACK y tras no recibir respuesta se aborta la conexión.

Observa en la consola de pServidor:

No se muestra ninguna conexión entrante, pues al no completarse la conexión el socket de escucha no retorna de la llamada al método Accept().

Detén el programa pServidor.exe que solo consume conexiones TCP.

Nping --tcp --dest-port 2459 --flags SYN --count 1 -delay 1s 156.35.123.45

Observa en la consola de Nping:

Se envía un paquete con el flag S (SYN) y NO se recibe respuesta.

Este mismo comportamiento se obtiene si se envía el paquete a un puerto en el que no escucha ningún servidor TCP, por ejemplo el puerto 2460.

Una vez que se controla el funcionamiento del comando de escaneo, se procede a realizar los experimentos de escaneo activando el registro del FW.

Comprueba si el FW registra el escaneo a un puerto específico

Borra el fichero pfirewall.log si existe. Activa el FW.

Habilita la regla: pServidor.

Arranca el servicio pServidor.exe

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

Nping --tcp --dest-port 2459 --flags SYN --count 100 --delay 0ms 156.35.123.45

El envío de los 100 paquetes se realiza en poco más de 1 segundo y solo hay 2 respuestas.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el FW **NO registra** ni uno de los intentos de conexión TCP.

En la consola de Nping se puede observar que solo hay una o dos respuestas de pServidor al primer paquete TCP SYN enviado por Nping. El programa pServidor al recibir los paquetes TCP SYN tan rápidamente no llega a enviar las confirmaciones TCP SYN/ACK.

Compara los resultados de Nping con Nmap. Arranca pServidor y en el FW habilita la regla que permite el acceso. Luego ejecuta estos comandos:

Nmap -sS -p T:2459 -v 156.35.123.45 // TCP SYN Stealth Scan

No hay respuesta y recomienda usar –Pn, para eliminar el ping inicial de 4 mensajes.

Nmap -sS -p T:2459 –v -Pn 156.35.123.45

Indica que el puerto tcp 2459 está open.

En la consola de pServidor NO se muestra una nueva conexión.

Nmap -sT -p T:2459 -v 156.35.123.45 // TCP Connect Scan

No hay respuesta y recomienda usar -Pn.

Nmap –sT –p T:2459 –v –Pn 156.35.123.45

Parece que Nmap v7.94 se bloquea.

Pero Nmap v7.92 indica que el puerto tcp 2459 está open.

En la consola de pServidor SI se muestra una nueva conexión.

Comprueba si el FW registra el escaneo a un conjunto de puertos

Aprovecha la capacidad de Nping para enviar paquetes a un rango de puertos destino.

Borra el fichero pfirewall.log si existe. Activa el FW.

En FW Perfil público, selecciona Registrar: **SI** paquetes descartados y **SI** conexiones correctas.

nping --tcp --dest-port 1-4096 --flags SYN --count 1 -delay 10ms 156.35.123.45

El envío de los 4096 paquetes se realiza en poco más de 45 segundos y solo hay 9 respuestas.

En FW Perfil público, selecciona Registrar: **NO** paquetes descartados y **NO** conexiones correctas.

(Para parar el registro y evitar que continúe creciendo el fichero).

Copia el fichero pfirewall.log a un directorio donde se pueda editar sin restricciones.

Comprueba que el FW **NO registra todos** los intentos de conexión TCP.

(Tan solo ha registrado tres DROP a los puertos: 135, 139 y 445).

Compara los resultados de Nping con Nmap. Arranca pServidor y en el FW habilita la regla que permite el acceso. Luego ejecuta estos comandos:

Nmap -sS -p T:1-4096 -v -Pn 156.35.123.45 // TCP SYN Stealth Scan

Descubre que los puertos tcp 2459 y 3389 están open.

El FW registra dos DROP para cada uno de los siguientes puertos: 135, 139, 445.

En la consola de pServidor NO se muestran nuevas conexiones.

Nmap -sT -p T:2459 -v -Pn 156.35.123.45 // TCP Connect Scan

Parece que Nmap v7.94 se bloquea.

Pero Nmap v7.92 indica que los puertos tcp 2459 y el 3389 están open.

El FW registra dos DROP para cada uno de los siguientes puertos: 135, 139, 445. También registra un ALLOW para el puerto 2459 y muchísimos ALLOW para el puerto 3389.

En la consola de pServidor SI se muestra una nueva conexión cuando Nmap descubre el puerto 2459 en estado abierto.

¿Cuál es la capacidad del FW para registrar escaneos a puertos TCP?

Copia el texto blanco del cuadro en notepad para ver la solución.

7. Ataque a un servidor UDP

El objetivo es realizar experimentos de ataque basados en el envío intenso (anómalo) de paquetes UDP a un computador durante un pequeño período de tiempo. Hay que determinar si el FW registra el envío anómalo dependiendo de dos aspectos: (1) la forma de enviar los paquetes y (2) la configuración de reglas del FW.

Experimentos con servicios del sistema

Enviar mensajes a un puerto con una regla del FW existente y NO habilitada en el perfil público.

Regla: Compartir archivos e impresoras (Nombre NB de entrada) usa puerto 138

Regla: Detección de redes (Nombre NB de entrada) usa puerto 138

Pero hay una regla habilitada para el perfil privado.

Nping --udp --dest-port 138 --count 100 --delay 100ms 156.35.123.45

El FW SI REGISTRA muchas líneas como la siguiente:

aaaa-mm-dd hh:mm:ss DROP UDP 156.35.163.82 156.35.123.45 53 138 28 - - - - - - - RECEIVE

Nping siempre utiliza el mismo puerto origen: 53

Enviar mensajes a un puerto con una regla del FW existente y NO habilitada en el perfil Todo.

Regla: Enrutamiento y acceso remoto (L2TP de entrada) usa puerto 1701

Nping --udp --dest-port 1701 --count 1000 --delay 10ms 156.35.123.45

El FW NO REGISTRA ninguno de los paquetes enviados.

Se habilita la regla y se repite el envío de paquetes y el FW NO REGISTRA ningún paquete enviado.

Regla: Servicio de uso compartido en red del Reproductor de Windows Media, usa puerto 1900

Nping --udp --dest-port 1900 --count 1000 --delay 10ms 156.35.123.45

El FW SI REGISTRA muchas líneas como la siguiente:

aaaa-mm-dd hh:mm:ss DROP UDP 156.35.163.29 156.35.151.20 53 1900 28 - - - - - - - RECEIVE

Realiza pruebas adicionales con los puertos udp 68 y 7680.

¿Cuál es la capacidad del FW para registrar ataques a puertos UDP de servicios del sistema?

Copia el texto blanco del cuadro en notepad para ver la solución.

Experimentos con servidor programado

Para experimentar con un servidor o servicio UDP programado (no del sistema) se proporcionan tres programas descargables del CV:

- pUdpSer: Programa Udp Servidor.
- pUdpCli1: Programa Udp Cliente – Usa 1 socket para enviar N mensajes.
- pUdpCliN: Programa Udp Cliente – Usa N sockets para enviar N mensajes.

Arranca el pUdpSer en la MV servidora y crea una regla su FW para permitir el acceso.

Arranca el pUdpCliN en la MV cliente y comprueba que se envían y reciben los mensajes.

Pruebas con pUdpCliN

Comprueba realizando experimentos el siguiente comportamiento:

Servicio ejecutándose Y Regla habilitada → FW registra muchos eventos ALLOW:

aaaa-mm-dd hh:mm:ss ALLOW UDP 156.35.163.29 156.35.151.20 60540 9050 0 - - - - - - - RECEIVE

Pero NO REGISTRA TODAS las comunicaciones permitidas. Comprueba que cada comunicación usa un puerto origen diferente.

Servicio ejecutándose Y Regla deshabilitada → FW registra 1 evento DROP:

aaaa-mm-dd 20:09:07 DROP UDP 156.35.163.29 156.35.123.45 50728 9050 38 - - - - - - - RECEIVE

El registro de 1 único evento DROP se debe a que el cliente se bloquea esperando la respuesta a la primera petición que envió y ya no vuelve a realizar más peticiones. Comenta con /* ··· */ el código del cliente que recibe y muestra las respuestas y vuelve a realizar el experimento. Comprueba que el FW REGISTRA muchos eventos DROP aunque no todos.

Servicio parado Y Regla habilitada → FW NO registra eventos

Servicio parado Y Regla deshabilitada → FW NO registra eventos

Cuando un servicio está ejecutándose y NO hay regla (porque se borró después de arrancar el servicio, caso rarísimo) → FW registra gran parte de los eventos DROP, pero no todos

Cuando un servicio está parado y NO hay regla → FW NO registra eventos

Pruebas con pUdpCli1

Comprueba realizando experimentos el siguiente comportamiento:

Servicio ejecutándose Y Regla habilitada → FW registra 1 evento ALLOW:

aaaa-mm-dd hh:mm:ss ALLOW UDP 156.35.163.29 156.35.123.45 53 9050 0 - - - - - - - RECEIVE

Servicio ejecutándose Y Regla deshabilitada → FW registra 1 evento DROP:

aaaa-mm-dd hh:mm:ss DROP UDP 156.35.163.29 156.35.151.20 51525 9050 38 - - - - - - - RECEIVE

Prueba con Nping

Comando Nping utilizado:

Nping --udp --dest-port 9050 --data-length 10 --count 100 --delay 10ms 156.35.123.45

Con la opción --data-length 10 Nping genera 10 bytes aleatorios que luego envía como datos en todos los paquetes UDP.

El comportamiento es similar al observado con pUdpCli1.

Se supone que Nping crea un socket y elije un puerto que utiliza para enviar todos los paquetes. Con esta técnica no se establecen múltiples "conexiones" diferentes para enviar paquetes.

¿Cuál es la capacidad del FW para registrar ataques a servidores UDP?

Copia el texto blanco del cuadro en notepad para ver la solución.