Seguridad en Redes de Ordenadores
Práctica 3: Firewall, IDS, Pentesting
Parte II

GSyC
Departamento de Teoría de la Señal y Comunicaciones y
Sistemas Telemáticos y Computación

Abril de 2017

Resumen

Esta práctica se va a realizar con la herramienta netgui-ng.sh. Es muy importante que arranques esta herramienta y no `netgui.sh` ya que la nueva versión de NetGUI tiene instalados paquetes necesarios para la realización de la práctica.

Configuración previa

Se usará una configuración de máquinas virtuales con 128MB de memoria RAM, para ello, recuerda que deberás usar el fichero `netkit.conf` que te proporcionamos en la parte I de esta práctica. Si todavía no la has hecho copia el fichero `netkit.conf` en el directorio de tu carpeta personal `.netkit`. Comprueba que lo has copiado correctamente, deberías verlo en esa carpeta:

```
miusuario@maquinaLaboratorio ~ $ ls ~/.netkit
```

Si quieres arrancar las máquinas de las prácticas anteriores deberás borrar el fichero `netkit.conf` para que se use el valor por defecto de memoria RAM.

Se usará la misma configuración de red que se utilizó en la parte I de esta práctica, direcciones IP: `X.<ID>.Z.W`.

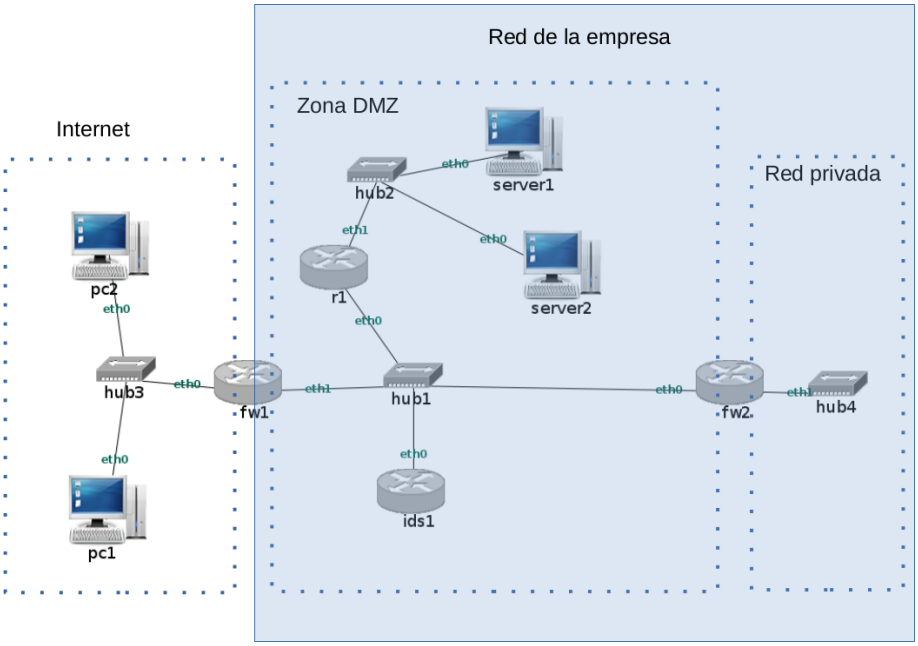

Figura 1: Escenario de red de una empresa conectada a Internet a través de una zona DMZ.

1. nmap

Lanza `snort` en la máquina `ids1` (`snort -A console -c /etc/snort/snort.conf`) para que comience a detectar tráfico potencialmente peligroso y déjalo lanzado para que te vaya mostrando las alertas que detecte en los apartados sucesivos.

Lanza un servidor de ssh en `server1`:

```
/etc/init.d/ssh start
```

Lanza algunos servicios que maneja el demonio `inetd` en `server1`. Copia primero el fichero `inetd.conf` en la carpeta `/etc/` en la máquina `server1` y a continuación ejecuta:

```
/etc/sbin/inetd
```

Lanza un servidor de web apache en `server2`:

```
/etc/init.d/apache start
```

Comprueba qué puertos están utilizándose en cada uno de estos servidores con la herramienta `netstat` y explícalo en la memoria. Si no sabes qué servicios son los que se están utilizando en determinados puertos, haz uso del fichero `/etc/services` que te da información sobre los números de puerto reservados para servicios habituales.

`nmap` es una herramienta potente que es capaz de generar muchos paquetes de sondeo para extraer información de un sistema. Desafortunadamente no podemos explotar todo el potencial de `nmap` porque tenemos la limitación de las máquinas virtuales que no pueden soportar tanto tráfico en sus interfaces.

En las ejecuciones de `nmap`, se intentará realizar resoluciones inversas al DNS de las direcciones IP, sin embargo, como no está configurado el servicio de DNS, se mostrará un mensaje de aviso indicando que no se puede utilizar ningún servidor de DNS. Esto no es problemático para el desarrollo de la práctica.

1.1. Descubrimiento de equipos

Existen diversas técnicas para el descubrimiento de equipos utilizando `nmap`. El objetivo es mostrar si la máquina se encuentra activa o no. A continuación se muestran algunas formas de sondeo utilizando `nmap`:

1.1.1. Sondeo de equipos Ping Scan

Para el sondeo de equipos `nmap` trata de contactar con las máquinas objetivo de formas diferentes dependiendo de si la máquina se encuentra en la misma subred que el atacante o en diferentes subredes. Por eso se va a probar este sondeo con `pc2` y `server2`, desde `pc1`.

Realiza una captura en `fw1(eth0)` y guarda el contenido en un fichero `nmap-01.cap`.
Ejecuta `nmap` para que se envíen varios paquetes de sonda:

```
nmap -sn <dirIPpc2>, <dirIPServer2>
```

1. Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta.
2. ¿Cuál es la diferencia que encuentras entre el sondeo a la máquina `pc2` y a la máquina `server2`?
3. Explica si `snort` ha detectado alertas e indica cuáles y por qué.

1.1.2. Sondeo de protocolos

Realiza una captura en `r1(eth1)` y guarda el contenido en un fichero `nmap-02.cap`. Utiliza `nmap` desde `pc1` de la siguiente forma para que se envíen paquetes de diferentes protocolos a una determinada máquina y comprobar si la máquina responde a este tipo de paquetes. Los protocolos que se usan por defecto son IGMP, ICMP e IP encapsulado en IP:

```
nmap -sn -PO <dirIPServer1>
```

1. Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta.
2. Explica si `snort` ha detectado alertas e indica cuáles y por qué.

1.1.3. Sondeo TCP SYN

Realiza una captura en `r1(eth1)` y guarda el contenido en un fichero `nmap-03.cap`. Utiliza `nmap` desde `pc1` de la siguiente forma para que se envíe un paquete TCP con el flag de SYN activo con el objetivo de determinar si hay un servicio esperando recibir paquetes (se pueden sondear varios puertos a la vez utilizando un rango, por ejemplo, del puerto 80 al 82):

```
nmap -sn -PS80-82 <dirIPServer2>
```

1. Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta y el tipo de respuesta obtenida.
2. Explica si `snort` ha detectado alertas e indica cuáles y por qué.

1.1.4. Sondeo UDP

Realiza una captura en `r1(eth1)` y guarda el contenido en un fichero `nmap-04.cap`. Utiliza `nmap` desde `pc1` de la siguiente forma para que se envíe un paquete UDP con el objetivo de determinar si hay un servicio esperando recibir paquetes (se pueden sondear varios puertos a la vez utilizando un rango, por ejemplo, del puerto 7 al 13):

```
nmap -sn -PU7-13 <dirIPServer1>
```

1. Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta y el tipo de respuesta obtenida.
2. Explica si coincide con los servicios UDP que hay arrancados en `server1` y que examinaste con `netstat`.
3. Explica si `snort` ha detectado alertas e indica cuáles y por qué.

1.2. Escaneo de puertos

Con las siguientes técnicas se desea obtener información de si un puerto tiene un servicio arrancado o no. El resultado de la ejecución de `nmap` mostrará los puertos sondeados y el estado en el que se encuentran `open/close`.

1.2.1. Sondeo TCP SYN

Este sondeo es sigiloso porque implementa un escaneo en el que el atacante no finaliza las conexiones.

Realiza una captura en `r1(eth1)` y guarda el contenido en un fichero `nmap-05.cap`. Utiliza `nmap` desde `pc1` de la siguiente forma para que se envíe un paquete TCP con el flag SYN con el objetivo de determinar si hay un servicio esperando recibir paquetes (se pueden sondear varios puertos a la vez utilizando un rango, por ejemplo, del puerto 20 al 25):

```
nmap -Pn -sS -p 20-25 -v <dirIPServer1>
```

1. Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta y el tipo de respuesta obtenida.
2. Fíjate en la salida de `nmap` y la diferencia con el apartado 2.1.3 donde sólo se deseaba conocer si la máquina estaba activa. Con esta prueba se desean conocer los servicios TCP. Incluye esta salida en la memoria.
3. Explica si `snort` ha detectado alertas e indica cuáles y por qué.

1.2.2. Sondeo UDP

Realiza una captura en `r1(eth1)` y guarda el contenido en un fichero `nmap-06.cap`. Utiliza `nmap` desde `pc1` de la siguiente forma para que se envíe un paquete UDP con el objetivo de determinar si hay un servicio esperando recibir paquetes (se pueden sondear varios puertos a la vez utilizando un rango, por ejemplo, del puerto 7 al 13):

```
nmap -Pn -sU -p 7-13 <dirIPServer1>
```

1. Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta y el tipo de respuesta obtenida.
2. Fíjate en la salida de `nmap` y la diferencia con el apartado 2.1.4 donde sólo se deseaba conocer si la máquina estaba activa. Con esta prueba se desean conocer los servicios UDP. Incluye esta salida en la memoria.
3. Explica si `snort` ha detectado alertas e indica cuáles y por qué.

1.2.3. Sondeo TCP Null, FIN, Xmas

Este sondeo consiste en enviar diferentes segmentos TCP que tengan activos determinados flags:

- Null: ningún flag (`-sN`)
- FIN: únicamente flag FIN (`-sF`)
- Xmas: activa FIN, PSH y URG (`-sX`)

La RFC de TCP (RFC-793) no está totalmente definida para ciertas ocasiones inesperadas, como por ejemplo la activación de flags inesperados en determinados momentos. Dependiendo de los SO se pueden responder diferentes tipos de paquetes.

Los siguientes sondeos ejecútalos siempre desde la máquina `pc1`.

1. Realiza una captura en `r1(eth1)` y guarda el contenido en un fichero `nmap-07.cap`. Utiliza `nmap`:

   ```
   nmap -Pn -sN -p 20-25 -v <dirIPServer1>
   ```

   Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta y el tipo de respuesta obtenida.
2. Explica si `snort` ha detectado alertas e indica cuáles y por qué.
3. Realiza una captura en `r1(eth1)` y guarda el contenido en un fichero `nmap-08.cap`. Utiliza `nmap`:

   ```
   nmap -Pn -sF -p 20-25 -v <dirIPServer1>
   ```

   Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta y el tipo de respuesta obtenida.
4. Explica si `snort` ha detectado alertas e indica cuáles y por qué.
5. Realiza una captura en `r1(eth1)` y guarda el contenido en un fichero `nmap-09.cap`. Utiliza `nmap`:

   ```
   nmap -Pn -sX -p 20-25 -v <dirIPServer1>
   ```

   Interrumpe la captura y observa qué paquetes se han enviado y explica cuáles tienen respuesta y el tipo de respuesta obtenida.
6. Explica si `snort` ha detectado alertas e indica cuáles y por qué.

2. firewall

Vamos a utilizar el script `fw1.sh` que deberás copiar en la máquina `fw1`, por ejemplo en la carpeta personal del usuario root: `/root`. Estudia su contenido, cambia las direcciones IP incluidas en el fichero para que reflejen las direcciones IP que hay configuradas en tu escenario y ejecútalo (recuerda darle permisos de ejecución: `chmod 700 /root/fw1.sh`).

- Inicia una captura en `fw1(eth0)` (`nmap-10.cap`). Ejecuta los sondeos NULL, FIN y Xmas con `server1` (puertos 20-25) desde `pc1`. A continuación interrumpe la captura.
- Inicia una captura en `fw1(eth0)` (`nmap-11.cap`). Ejecuta los sondeos NULL, FIN y Xmas con `server2` (puertos 80-82) desde `pc1`. A continuación interrumpe la captura.

1. Explica las diferencias entre la regla que permite las conexiones entrantes TCP puerto 80 hacia la máquina `server2` y la regla que permite las conexiones entrantes TCP puerto 22 hacia la máquina `server1`.
2. Consulta el fichero `fw1.sh` y explica qué paquetes se van trazar en el fichero `/var/log/kern.log`.
3. Consulta los mensajes del final del fichero `/var/log/kern.log` para ver las trazas que se han generado en `fw1.log` como consecuencia de la configuración de `iptables`. Inclúyelos en la memoria. ¿Qué ha hecho la máquina `fw1` con esos paquetes?
4. Explica las capturas que has obtenido.
5. Explica los resultados obtenidos de `nmap`.

3. Normas de entrega

Deberás subir al `aulavirtual` un fichero `analisis.tgz` que contenga los siguientes archivos:

- La memoria en formato pdf que incluya las dos partes de la práctica 3.
- Un archivo `analisis-caps.tgz` que contenga los ficheros con las capturas de `analisis-01.cap` y `analisis-02.cap`.
- Un archivo `nmap-caps.tgz` que contenga los ficheros con las capturas de `nmap-01.cap` a `nmap-11.cap`