Seguridad en Redes de Ordenadores
Práctica 6: Seguridad Perimetral
Parte 1: snort, nmap

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

Abril de 2018

Resumen

Esta práctica se va a realizar con el uso de 2 raspberry pi en las que hay que instalar una distribución kali y utilizar herramientas de sondeo de equipos y detección de intrusos.

1. Configuración previa

Se desea configurar un escenario como el que se muestra en la siguiente figura 1.

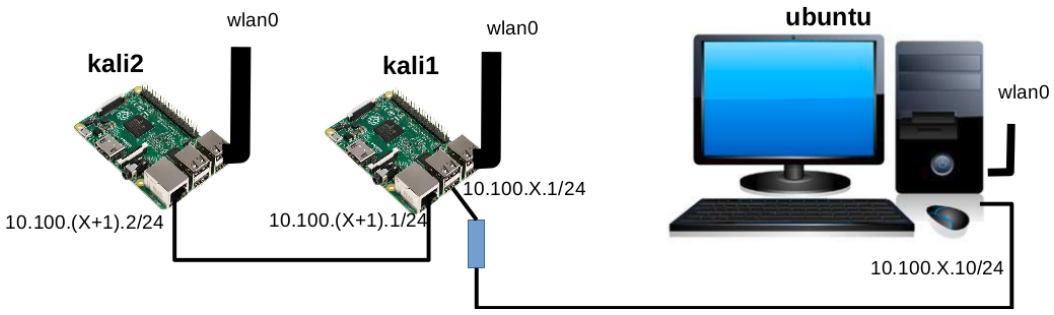

Figura 1: Configuración de red para realizar la práctica.

Donde tendremos 3 máquinas:

- Tu ordenador con una distribución **ubuntu** que debe estar conectado a 2 interfaces de red. La interfaz cableada estará directamente conectada a la raspberry pi `kali1` dentro de la subred 10.100.X.0/24. Además deberá tener conexión a Internet a través de la tarjeta inalámbrica. El ordenador tendrá configurada una ruta a la subred 10.100.(X+1).0/24 a través de 10.100.X.1 (`kali1`).
- La raspberry pi **kali1** que tendrá 3 interfaces de red. Una de ellas conectada a tu ordenador dentro de la subred 10.100.X.0/24 , otra de ellas conectada a la raspberry pi `kali2` dentro de la subred 100.100.(X+1).0/24 y la interfaz inalámbrica que deberá tener conexión a Internet. `kali1` estará configurada como router entre las subredes 10.100.X.0/24 y 10.100.(X+1).0/24.
- La raspberry pi **kali2** que tendrá 2 interfaces de red. Una de ellas conectada a la raspberry pi `kali1` dentro de la subred 100.200.(X+1).0/24 y la interfaz inalámbrica que deberá tener conexión a Internet. El `kali2` tendrá configurada una ruta a la subred 10.100.X.0/24 a través de 10.100.(X+1).1 (`kali1`).

Todas las pruebas de detección y sondeo en la red que realizaremos en esta práctica serán sobre las redes privadas 10.100.(X+1).0/24 y 10.100.X.0/24.

1.1. Copia la distribución kali en 2 tarjetas de memoria

Vamos a copiar la imagen de la distribución `kali` que se llama `kali-linux-2018.1a-rpi3-nexmon.img.xz` en tu portátil, se encuentra en las máquinas del laboratorio en la carpeta `/var/lib/vms` o también la puedes descargar de:

`https://images.offensive-security.com/arm-images/kali-linux-2018.1a-rpi3-nexmon.img.xz`

Una vez copiada en tu portátil, descomprime esta imagen con el siguiente comando:

```
xz -d kali-linux-2018.1a-rpi3-nexmon.img.xz
```

Mete la tarjeta microSD en tu portátil. Para saber el nombre del dispositivo que se corresponde con la tarjeta miniSD en tu ordenador ejecuta el siguiente comando:

```
df -h
```

Este comando mostrará todas las particiones que hay montadas en la máquina, hay que localizar la que se corresponde con la memoria miniSD. En particular, en Linux será algo como: `/dev/sdX1` montada en `/media/nombreUsuario`. Si la tarjeta ya tenía grabado algo previamente, pueden aparecer varios puntos de montaje: `/dev/sdX1`, `/dev/sdX2`, etc. Primero es necesario desmontar todas ellas, por ejemplo:

```
umount /dev/sdX1
```

Para copiar esta distribución ejecuta en tu portátil el siguiente comando, teniendo en cuenta que `<DIR>` es el nombre de la carpeta donde está almacenada la imagen de kali y `<DEV>` es el nombre del dispositivo `sdX` en tu ordenador **sin el número**. Es importante que seas especialmente cuidadoso con estas instrucciones para no borrar alguna de las particiones de tu ordenador:

```
sudo dd bs=4M if=<DIR>/kali-linux-2018.1a-rpi3-nexmon.img of=/dev/<DEV>
```

Mete la segunda tarjeta microSD y repite los pasos anteriores para copiarla: desmonta los puntos de montaje de la tarjeta microSD y realiza la copia.

1.2. Configuración inicial kali1

Arranca la primera raspberry, a la que vamos a llamar `kali1`. La raspberry tiene conectado un cable TTL serial que permite tener una consola a través de su puerto serie conectado a un puerto USB de tu ordenador, véase la figura 1.2.

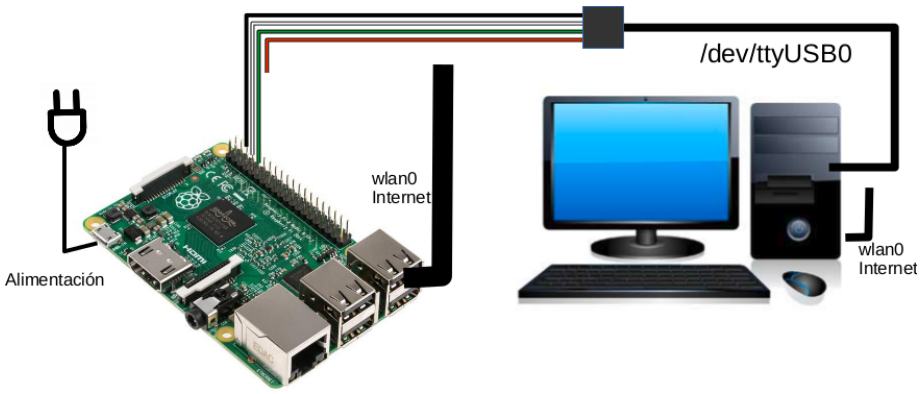

Figura 2: Conexión de la raspberry pi con un ordenador a través del cable TTL serial al puerto USB.

Para tener una consola serie necesitas usar el programa `screen` en tu portátil (instálalo si no lo tienes) y ejecuta el siguiente comando:

```
sudo screen  /dev/ttyUSB0 115200
```

Este programa abrirá una consola serie con la raspberry pi, entra con nombre de usuario `root`, contraseña `toor`.

Es necesario configurar las direcciones IP de `kali1`: puertos `eth0` y `eth1` en el fichero `/etc/network/interfaces` variando los valores de X por los que se te asignaron en las prácticas anteriores:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
   address 10.200.X.1
   netmask 255.255.255.0

auto eth1
iface eth1 inet static
```

```
   address 10.200.X+1.1
   netmask 255.255.255.0

allow-hotplug wlan0
iface wlan0 inet dhcp
wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
```

Además, se desea que la raspberry pi tenga acceso a través de la configuración de la red inalámbrica de la universidad y para ello hay que configurar el fichero `/etc/wpa_supplicant/wpa_supplicant.conf`:

```
network={
    ssid="eduroam"
    scan_ssid=1
    key_mgmt=WPA-EAP
    pairwise=CCMP
    group=CCMP TKIP
    eap=PEAP
    ca_cert="/etc/ssl/certs/ca.pem"
    identity="alumno@alumnos.urjc.es"
    domain_suffix_match="urjc.es"
    phase1="peaplabel=0"
    phase2="auth=MSCHAPV2"
    password="PASS"
}
```

Ten en cuenta que hay que dejar el fichero `ca.pem` con el certificado de la autoridad de certificación en la carpeta `/etc/ssl/certs/`. Descarga el fichero en tu ordenador desde el aula virtual y con el ratón copia exactamente el contenido en el fichero `/etc/ssl/certs/ca.pem`.

Para usar la red inalámbrica de tu casa, dependerá de la configuración que tengas, pero es habitual que funcione este fichero de configuración `/etc/wpa_supplicant/wpa_supplicant.conf`:

```
network={
    ssid="nombreDeLaRedEnTuCasa"
    psk="contraseña"
    key_mgmt=WPA-PSK
}
```

Cambia el nombre a la raspberry para que la indentifiquemos como `kali1`:

```
hostname kali1
```

Además como en el caso de kali1 se desea que funcione como router es necesario activar el reenvío:

```
sysctl -w net.ipv4.ip_forward=1
```

Cambia el passwd de `root`, ya que tiene el valor por defecto a `toor` y lo vas a conectar a Internet.

Hay un problema con la hora, la distribución kali tiene configurada la hora en la que se creó la distribución, diciembre de 2017 y el certificado para conectarse a la red inalámbrica aún no es válido en esa fecha, por tanto hay que cambiar la hora a `kali1`. Para ello vamos a configurar que cada vez que se reinicie la máquina se configure una hora más actual:

```
crontab -e

@reboot date --set "04/17/2018 11:00"
```

Ejecuta `reboot` para que la configuración tenga efecto y vuelve a entrar a través del puerto serie. La raspberry se habrá conectado a la red inalámbrica eduroam, en su interfaz `wlan0`. Apunta la dirección IP que te han asignado por DHCP. Esta dirección IP te permitirá conectarte a la raspberry pi, de forma más cómoda y con tantos terminales como necesites, a través de `ssh` desde tu portátil que también deberá estará conectado a la red eduroam. Ten en cuenta que cada vez que inicies la raspberry le podrán asignar una dirección IP diferente a su interfaz inalámbrica.

Ahora que ya tienes conectada kali1 a Internet, ejecuta:

```
apt-get update
apt-get install tcpdump
apt-get install snort
apt-get install netcat
apt-get install nmap
```

1.3. Configuración inicial kali2

Arranca la segunda raspberry pi y conéctate también utilizando el cable TTL serial. Edita su fichero `/etc/network/interfaces` con la siguiente configuración, para que tenga una dirección IP en la misma subred de `kali1` y además utilice a `kali1` para alcanzar la subred 10.100.X.0/24:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
   address 10.100.X+1.2
   netmask 255.255.255.0

allow-hotplug wlan0
iface wlan0 inet dhcp
wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf

up route add -net 10.100.X.0/24 gw 10.100.X+1.1
```

Realiza la misma configuración en `/etc/wpa_supplicant/wpa_supplicant.conf` que en `kali1`.

Cambia el nombre a esta segunda raspberry pi para identificarla como `kali2`. Cambia el passwd de `root` y la hora.

Ejecuta `reboot` para que la configuración tenga efecto y vuelve a entrar a través del puerto serie. La raspberry se habrá conectado a la red inalámbrica eduroam, en su interfaz `wlan0`. Apunta la dirección IP que te han asignado por DHCP. Esta dirección IP te permitirá conectarte a la raspberry pi, de forma más cómoda y con tantos terminales como necesites, a través de `ssh` desde tu portátil que también deberá estará conectado a la red eduroam. Ten en cuenta que cada vez que inicies la raspberry le podrán asignar una dirección IP diferente a su interfaz inalámbrica.

1.4. Configuración en tu ordenador

Configura la dirección IP 10.100.X.10/24 en tu ordenador a través de la interfaz cableada que tendrás conectada a `kali1`. También debes configurar una ruta a la subred 10.100.(X+1).0/24 a través del router 10.100.X.1 (`kali1`), esta ruta te permitirá alcanzar la máquina `kali2`. Comprueba que puedes hacer un ping a la máquina `kali2`.

2. Snort

La máquina `kali1` va a ejecutar una herramienta IDS, `snort`, que detecta accesos potencialmente maliciosos y los registra en un fichero de log. Cuando `snort` descubra tráfico potencialmente malicioso escribirá una alerta en un fichero de logs y almacenará el tráfico malicioso en un fichero de captura. Estos ficheros se encontrarán en la carpeta `/var/log/snort`.

2.1. Reglas Snort

En la carpeta `/etc/snort/rules/` se describen reglas predefinidas en `snort` para la inspección de tráfico. Dependiendo de la configuración del fichero `/etc/snort/snort.conf` se podrán cargar las reglas que se desean aplicar al tráfico que el IDS examine.

A continuación responde a las siguientes preguntas en la memoria de la práctica:

1. El fichero `/etc/snort/snort.conf` es el que contiene la configuración de snort. Este fichero está dividido en varias partes, las líneas que comienzan por # son comentarios. Nosotros nos vamos a fijar en la parte de la configuración de variables (parte 1 ó *Step #1*) y en la parte de configuración de reglas (parte 7 ó *Step #7*). Escribe en la memoria el contenido de las variable `HOME_NET` y `EXTERNAL_NET` y explica qué crees que significa ese valor.
2. En la sección *Step #7* se incluyen la reglas escritas en diversos ficheros que se encuentran en la carpeta `/etc/snort/rules`, en particular comprueba que se inlcuye el fichero `/etc/snort/rules/icmp.rules`. Abre este fichero. Las líneas que comienzan por # son comentarios, las reglas están escritas cada una en una única línea. Incluye la última regla de ese fichero en la memoria y explica el contenido [1].

[1] Puedes consultar la información sobre classtype en la sección 3.4.6 del manual: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

3. Busca en el fichero `icmp.rules` la regla que es una alerta que escribe el mensaje `"ICMP PING NMAP"`[2], inclúyela en la memoria y explica todo lo que puedes saber de su contenido.
4. Busca en el fichero `icmp-info.rules` la regla que es una alerta que escribe el mensaje `ICMP PING *NIX"`, inclúyela en la memoria y explica todo lo que puedes saber de su contenido.
5. Explica cuál es la diferencia entre ambas reglas y el nivel de prioridad de cada una de ellas. ¿Por qué una tiene mayor prioridad que otra?
6. Lanza `snort` en la máquina `kali1` (`snort -A console -c /etc/snort/snort.conf -i eth1`) para que comience a detectar tráfico potencialmente peligroso y déjalo lanzado para que te vaya mostrando las alertas que detecte en los apartados sucesivos. Una vez arrancado informará de que la inicialización se ha completado e indicará el número de proceso (pid), apúntalo para que, en caso de que sea necesario, puedas matar el proceso.

2.2. Alertas Snort

Vamos a realizar algunas pruebas sencillas para ver cómo se activan las notificaciones en snort.

1. Desde `kali2` ejecuta un `ping a 10.100.X.10` con el envío de un único paquete. Observa las alertas que muestra snort y ve al fichero de definición de esa/s regla/s, copia la/s regla/s y explica qué condiciones se han cumplido para que se activen.
2. Desde `kali2` vuelve a ejecutar el mismo ping pero con tamaño de paquete 1000 bytes (`-s 1000`). Observa las alertas que muestra snort y ve al fichero de definición de esa/s regla/s, copia la/s regla/s y explica qué condiciones se han cumplido para que se activen.
3. Desde `kali2` vuelve a ejecutar el mismo ping pero con tamaño de paquete 0 bytes (`-s 0`). Observa las alertas que muestra snort y ve al fichero de definición de esa/s regla/s, copia la/s regla/s y explica qué condiciones se han cumplido para que se activen.
4. En la carpeta `/var/log/snort` se quedan almacenados ficheros `snort.log.*`. Estos ficheros contienen los paquetes que han generado las alertas que se han mostrado en snort. Interpreta estos ficheros cargándolos con tcpdump y la opción `-r <nombreFichero>`.

3. Pentesting con nmap

Si has interrumpido la ejecución de `snort` en la máquina `kali1` vuelve a lanzarlo:

```
snort -A console -c /etc/snort/snort.conf -i eth1
```

para que comience a detectar tráfico potencialmente peligroso y déjalo lanzado para que te vaya mostrando las alertas que detecte en los apartados sucesivos.

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`:

3.1. Sondeo de equipos

1. Desde `kali2` ejecuta `nmap` para sondear qué equipos están activos en la subredes 10.100.(X+1).0/24. Realiza una captura en `kali2(eth0)` con la opción `-n`[3] y guarda el contenido en un fichero `nmap-01.cap` y después arranca el sondeo en `kali2`.
   a) Explica la salida que muestra nmap.
   b) Interrumpe la captura y explica qué paquetes se han enviado y cuáles tienen respuesta.
   c) ¿Se muestra alguna alerta en snort? Explica tu respuesta.
2. Desde `kali2` ejecuta `nmap` para sondear un único equipo de su misma subred, `kali1`. Realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-02.cap` y después arranca el sondeo en `kali2`.
   a) Explica la salida que muestra nmap.
   b) Interrumpe la captura y explica qué paquetes se han enviado y cuáles tienen respuesta.
   c) ¿Se muestra alguna alerta en snort? Explica tu respuesta.

[2] Nmap es una aplicación que realiza escaneo de redes, aplicaciones y servicios. Se utiliza para Pentesting.

[3] Esta opción se utiliza para que tcpdump no envíe paquetes de DNS para solicitar la resolución de direcciones IP a nombres y mostrar la información de forma más legible. Como en el escenario de pruebas no tenemos servidor de DNS para las máquinas involucradas, es mejor utilizar esta opción.

3. Desde `kali2` ejecuta `nmap` para sondear un único equipo de otra subred diferente, tu máquina. Realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-03.cap` y después arranca el sondeo en `kali2`.

   a) Explica la salida que muestra nmap.

   b) Interrumpe la captura y explica qué paquetes se han enviado y cuáles tienen respuesta.

   c) ¿Se muestra alguna alerta en snort? Explica tu respuesta.

3.2. Sondeo TCP SYN

Realiza una captura en `lkali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-04.cap`. Utiliza `nmap` desde `kali2` de la siguiente forma para que se envíen segmentos TCP con el flag de SYN activo con el objetivo de determinar si hay un servicio esperando recibir paquetes entre los puertos 1 a 50 de `kali1`.

1. Explica la salida que muestra nmap.
2. Interrumpe la captura y explica los paquetes intercambiados. Explica las diferencias del sondeo del puerto 22 y el resto de puertos.
3. Explica si `snort` ha detectado alertas e indica cuáles y por qué.
4. Consulta los servicios TCP activos (los servidores que se encuentran esperando paquetes TCP) en la máquina `kali1` a la que estabas realizando el sondeo, utilizando el comando `netstat -nt4l`. Relaciona el resultado de la ejecución de este comando con el resultado del sondeo.
5. Una vez encontrado un puerto abierto, puede ser útil obtener información de la versión del servicio que se está ejecutando. Prueba a realizar el sondeo anterior únicamente en el puerto que has encontrado abierto y añadiendo la opción `-sV`. Previamente a realizar el sondeo realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-05.cap`. Estudia el resultado de nmap y el contenido de la captura y explícalos.
6. Vamos a arrancar un servidor de web en la máquina `kali1` escuchando peticiones HTTP en el puerto 80. Para que este servidor sólo use IPv4 hay que modificar el siguiente fichero `/etc/apache2/ports.conf` y cambiar la línea `Listen 80` por `Listen 0.0.0.0:80`. Inicia el servidor con el siguiente comando:
   ```
   /etc/init.d/apache2 start
   ```
   Ejecuta `netstat` igual que antes para comprobar que se encuentra arrancado este servicio en el puerto 80. ¿Qué crees que ocurrirá si se sondea nuevamente la máquina con el rango de puertos 20-100?
7. Prueba a realizar el sondeo anterior en el puerto 80 añadiendo la opción `-sV`. Previamente a realizar el sondeo realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-06.cap`. Estudia el resultado de nmap y el contenido de la captura y explícalos.

3.3. Sondeo UDP

Realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-07.cap`. Utiliza `nmap` desde `kali2` de la siguiente forma para que se envíen paquetes UDP con el objetivo de determinar si hay un servicio esperando recibir paquetes entre los puertos 60 a 70 de `kali1`.

1. Explica la salida que muestra nmap.
2. Interrumpe la captura y explica los paquetes intercambiados. Explica las diferencias del sondeo del puerto 68 y el resto de puertos.
3. Explica si `snort` ha detectado alertas e indica cuáles y por qué.
4. Consulta los servicios UDP activos (los servidores que se encuentran esperando paquetes UDP) en la máquina `kali1` a la que estabas realizando el sondeo, utilizando el comando `netstat -nu4l`. Relaciona el resultado de la ejecución de este comando con el resultado del sondeo.

3.4. Sondeo TCP FIN, Xmas

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

- FIN: únicamente flag FIN (`-sF` en vez de `-sS`)
- Xmas: activa FIN, PSH y URG (`-sX` en vez de `-sS`)

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.

1. Desde `kali2` ejecuta `nmap` para realizar un ataque FIN TCP. Realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-08.cap` y después arranca el sondeo en `kali2` para los puertos 20-25.
   a) Explica la salida que muestra nmap.
   b) Interrumpe la captura y explica qué paquetes se han enviado y cuáles tienen respuesta.
   c) ¿Se muestra alguna alerta en snort? Explica tu respuesta.
2. Desde `kali2` ejecuta `nmap` para realizar un ataque XMAS TCP. Realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-09.cap` y después arranca el sondeo en `kali2` para los puertos 20-25.
   a) Explica la salida que muestra nmap.
   b) Interrumpe la captura y explica qué paquetes se han enviado y cuáles tienen respuesta.
   c) ¿Se muestra alguna alerta en snort? Explica tu respuesta.

3.5. Sondeos exhaustivos

Los sondeos anteriores aportan información concreta sobre un determinado aspecto de la máquina. Sin embargo, nmap permite realizar sondeos más agresivos que aportan información exhaustiva de una máquina. Esto requiere enviar muchos mensajes más para detectar toda la información posible. Generalmente llevan más tiempo y pueden alertar a los sistemas IDS. Para activar este tipo de sondeo se arranca `nmap -A -n <dirIP>`.

1. Desde `kali2` vamos a realizar un análisis exhaustivo de `kali1`. Realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-10.cap` y después arranca el sondeo en `kali2` hacia la máquina `kali1`. Explica el resultado que muestra nmap. Carga la captura y comenta algún aspecto relevante que veas.
2. Desde `kali2` vamos a realizar un análisis exhaustivo de tu ordenador en la interfaz `10.100.X.10`. Realiza una captura en `kali2(eth0)` con la opción `-n` y guarda el contenido en un fichero `nmap-11.cap` y después arranca el sondeo en `kali2` hacia tu máquina. Explica el resultado que muestra nmap. Carga la captura y comenta algún aspecto relevante que veas.

4. Normas de entrega

Deberás subir al `aulavirtual` un fichero `snort-nmap.tgz` que contenga los siguientes archivos:

- La memoria en formato pdf.
- Un archivo `nmap-caps.tgz` que contenga los ficheros con las capturas de `nmap-01.cap` y `nmap-11.cap`.