

Bastionado de redes y sistemas

Tarea 5: Diseño de redes seguras

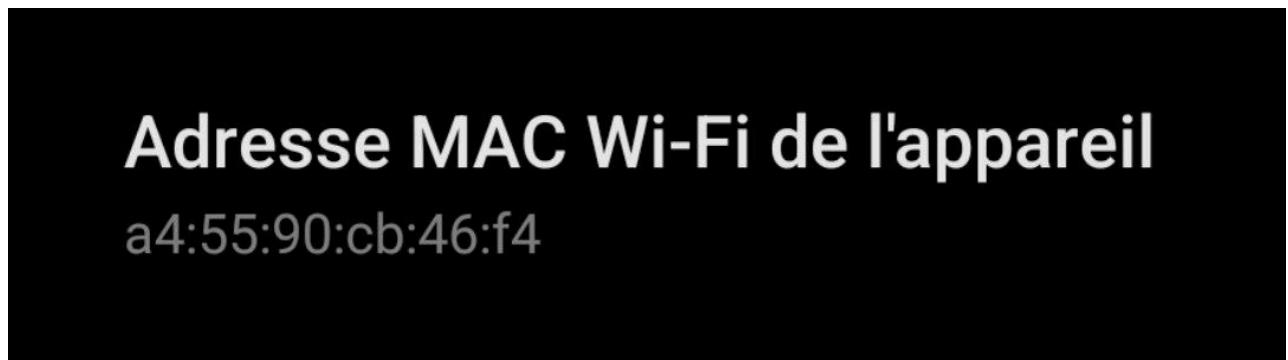
Índice

Índice.....	1
Seguridad Wi-Fi.....	2
Configura en la seguridad Wi-Fi del router el filtrado MAC y añade a la lista la dirección MAC de un dispositivo que esté a tu alcance (móvil, portátil, etc.).....	2
Desde una distribución Kali u otra de Linux, ya sea en un entorno virtualizado o nativo, suplanta el dispositivo autorizado modificando su dirección MAC (MAC spoofing) con la aplicación adecuada y demuéstralos con capturas de pantalla.....	5
Implementación IDS.....	8
Despliega una solución de IDS de código abierto, como Snort, y configúrala.....	8
Realiza un escaneo con Nmap que trate de identificar los servicios para ver cómo se comporta la herramienta. Para ello, se requiere una máquina de ataque, que puede ser Kali, y otra máquina para desplegar Snort (puede ser otra distribución Linux o Windows).....	10
Interpreta los resultados de los logs del IDS tras lanzar el ataque con Nmap.....	13
Bibliografía.....	16

Seguridad Wi-Fi

Configura en la seguridad Wi-Fi del router el filtrado MAC y añade a la lista la dirección MAC de un dispositivo que esté a tu alcance (móvil, portátil, etc.).

En primer lugar, tenemos que averiguar la dirección MAC del dispositivo que queremos añadir a la lista. En este caso, es un dispositivo Android, por lo que vamos a **Ajustes > Acerca del teléfono > Estado > Dirección MAC Wi-Fi**.



Dirección MAC del dispositivo Android, el cual está en francés

Una vez obtenida, tenemos que ir a los ajustes de la red y cambiar los ajustes de privacidad para que se utilice la dirección MAC del dispositivo en lugar de una aleatoria.

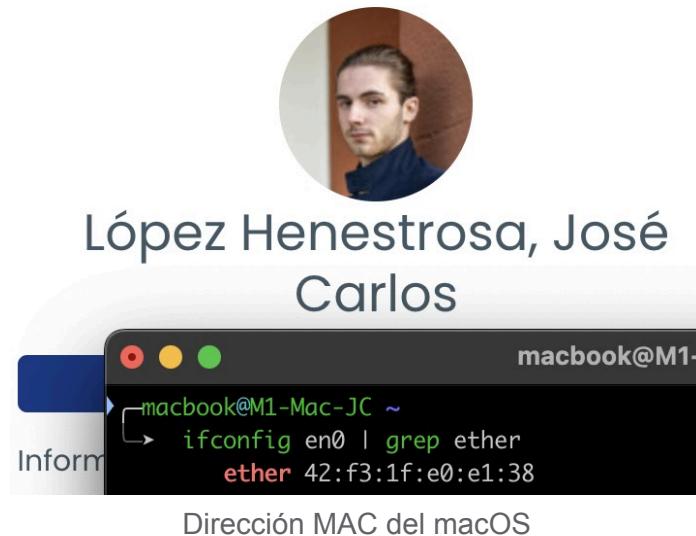
Tras esto, tenemos que obtener la dirección IP del router, por lo que ejecutamos arp -a y tomamos como referencia la primera IP obtenida.

A screenshot of a Windows command prompt window. It shows a user profile picture and name 'López Henestrosa, José Carlos'. Below that, it displays system information: 'Símbolo del sistema' and 'Microsoft Windows [Versión 10.0.22000.739] (c) Microsoft Corporation. Todos los derechos reservados.' Then, it runs the command 'C:\Users\Gunze>arp -a'. The output shows a table of network interfaces and their MAC addresses. The first entry, '192.168.18.1', is highlighted with a red box. The table columns are 'Interfaz', 'Dirección de Internet', 'Dirección física', and 'Tipo'. The highlighted row shows the IP 192.168.18.1 with the MAC address 1c-43-63-a9-81-64 and the type 'dinámico'. Other static entries include 192.168.18.255, 224.0.0.22, 224.0.0.251, 224.0.0.252, 239.255.255.250, and 255.255.255.255.

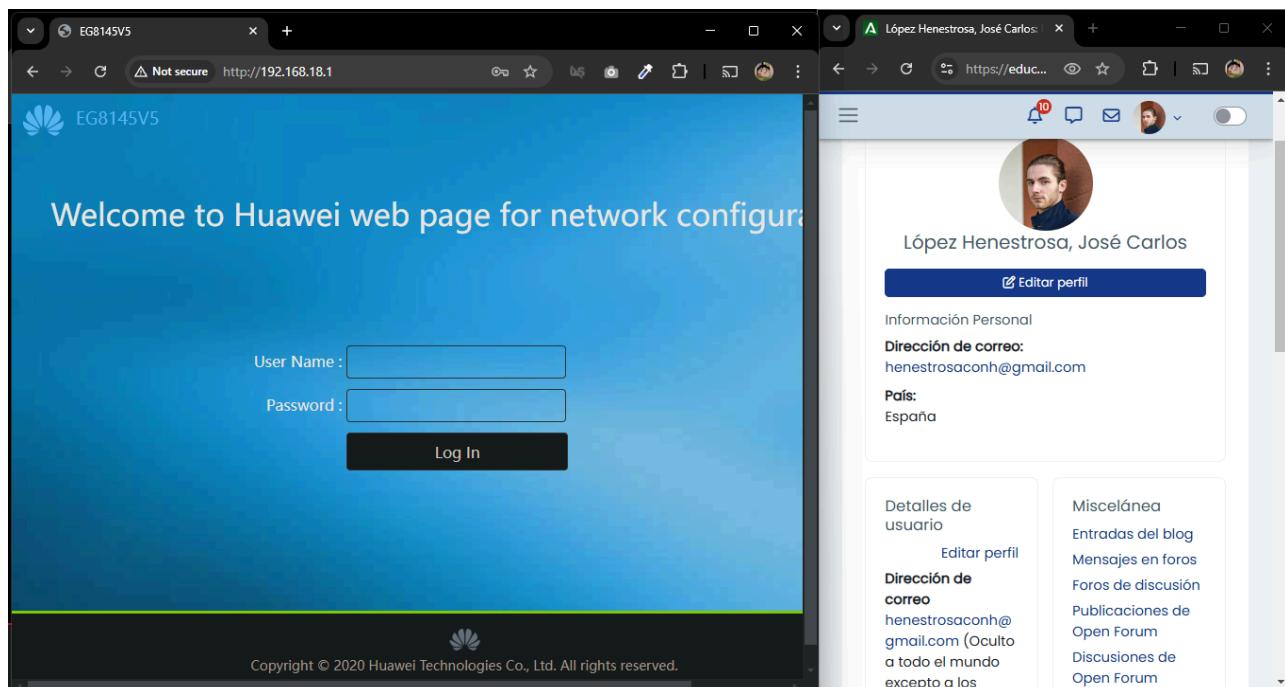
IP del router señalado en rojo

También tenemos que hallar la dirección MAC del ordenador desde el que modificamos la configuración del router para poder tener acceso a Internet. Mi equipo macOS está conectado por Wi-Fi, por lo que ejecutamos este comando:

```
ifconfig en0 | grep ether
```



Acto seguido, vamos a la configuración del router introduciendo la IP obtenida anteriormente. En nuestro caso, la dirección es 192.168.18.1.



Pantalla de login para acceder a la configuración del router

Introducimos el usuario y contraseña establecidos para acceder. Si no hay ninguno configurado, podemos consultar la página web del fabricante para ver las credenciales por defecto. En el caso de Huawei, las predeterminadas son `Epuser / userEp`.

Una vez dentro, vamos a **Advanced > Security > Wi-Fi MAC Filtering** y activamos la opción **Enable MAC Filter**. También tenemos que cambiar el **Filter Mode** de Blacklist a **Whitelist**, ya que queremos que sólo los dispositivos con una determinada dirección MAC puedan conectarse al router.

Tras ello, añadimos las direcciones MAC del dispositivo Android y el equipo macOS para que tengan acceso a la red. Tenemos que configurarlas tanto para los **índices 1** (frecuencia 2.4GHz) y **5** (5.2GHz) del **SSID (Service Set Identifier)**.

Configuración de filtro por MAC en modo *whitelist*

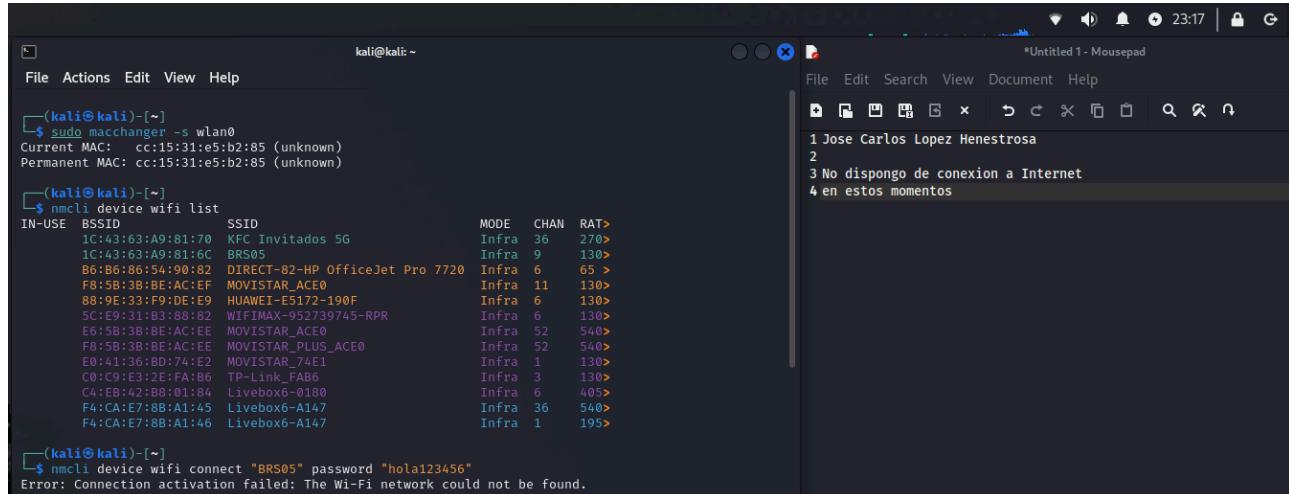
Con esto, ya tendríamos el filtro de conexión por dirección MAC listo.

Desde una distribución Kali u otra de Linux, ya sea en un entorno virtualizado o nativo, suplanta el dispositivo autorizado modificando su dirección MAC (**MAC spoofing**) con la aplicación adecuada y demuéstralos con capturas de pantalla.

Antes de entrar en detalles sobre cómo realizar la suplantación de MAC, conviene señalar que este proceso es un tanto complicado en un entorno virtualizado, ya que al suplantar la MAC, la máquina virtual pierde la red y no puede conectar de nuevo al router. Como solución, he creado un Live USB con Kali Linux para que se ejecute de forma nativa con ayuda de [esta guía](#).

Hay que tener en cuenta que, para que el sistema arranque a partir del Live USB, hay que acceder a la BIOS de la máquina y cambiar el orden de arranque, poniendo el dispositivo USB como la opción principal.

Después de completar este paso, iniciamos Kali Linux e intentamos conectarnos a la red Wi-Fi. Sin embargo, aunque ingresamos la contraseña correctamente, vemos que no podemos establecer la conexión.



The screenshot shows a Kali Linux desktop environment. On the left, a terminal window titled 'kali@kali: ~' displays the command 'nmcli device wifi list' and its output, which includes a list of available wireless networks. On the right, a 'Mousepad' application window titled '*Untitled 1 - Mousepad' shows a text document with the following content:

```
1 Jose Carlos Lopez Henestrosa
2
3 No dispongo de conexión a Internet
4 en estos momentos
```

Conexión fallida con el punto de acceso

Como podemos ver, el filtro por dirección MAC está funcionando correctamente, por lo que procedemos a realizar el MAC *spoofing*. Para ello, Kali cuenta con la herramienta `macchanger`, la cual nos permitirá cambiar la dirección MAC.

El proceso se desglosa en los siguientes pasos:

1. Verificar la interfaz de red

Ejecutamos `ip` a para mostrar las interfaces de red disponibles. Para la conexión Wi-Fi, como es nuestro caso, nos interesa fijarnos en `wlan0`.

2. Desactivar la interfaz de red antes de cambiar la MAC

Para evitar errores al cambiar la MAC, tenemos que desactivar la interfaz:

```
sudo ip link set wlan0 down
```

3. Cambiar la dirección MAC

Para suplantar una MAC de un dispositivo autorizado, como por ejemplo la del teléfono móvil, ejecutamos el comando:

```
sudo macchanger -m a4:55:90:cb:46:f4 wlan0
```

Y verificamos el cambio realizado con:

```
macchanger -s wlan0
```

4. Reactivar la interfaz de red

Ahora que tenemos la MAC suplantada, activamos de nuevo la interfaz:

```
sudo ip link set wlan0 up
```

5. Conectar a la red manualmente

Podemos hacerlo a través de la GUI o de la terminal. Para que esté en consonancia con el resto del proyecto, vamos a realizarlo desde la terminal mediante la ejecución del siguiente comando:

```
nmcli device wifi connect "BRS05" password "hola123456"
```

Si el cambio se ha realizado correctamente, la máquina tiene que conectarse sin problemas a la red, tal y como podemos apreciar en la siguiente captura de todo el proceso.

```

kali㉿kali:~/Desktop
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 08:bb:c1:cf:53:00 brd ff:ff:ff:ff:ff:ff
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether cc:15:31:e5:b2:85 brd ff:ff:ff:ff:ff:ff
4: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether 62:7e:c9:50:98:79 brd ff:ff:ff:ff:ff:ff

kali㉿kali:~/Desktop
$ sudo macchanger -s wlan0
Current MAC: cc:15:31:e5:b2:85 (unknown)
Permanent MAC: cc:15:31:e5:b2:85 (unknown)
New MAC: a4:55:90:cb:46:f4 (unknown)

kali㉿kali:~/Desktop
$ sudo ip link set wlan0 down
kali㉿kali:~/Desktop
$ sudo ip link set wlan0 up
kali㉿kali:~/Desktop
$ sudo ip link show wlan0
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN mode DORMANT group default qlen 1000
    link/ether a4:55:90:cb:46:f4 brd ff:ff:ff:ff:ff:ff permaddr cc:15:31:e5:b2:85
kali㉿kali:~/Desktop
$ nmcli device wifi connect "BRS05" password "holal23456"
Device 'wlan0' successfully activated with 'bd8f08dc-5381-4b8e-8315-6d9c2ae58049'.

```

Proceso de MAC *spoofing* completo

Como última prueba, podemos hacer un `ping` para comprobar que la conexión con la red funciona correctamente.

```

kali㉿kali:~/Desktop
$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=120 time=18.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=120 time=19.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=120 time=18.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=120 time=19.0 ms

```

— 8.8.8.8 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 18.742/19.137/19.947/0.474 ms

Realizando conexión vía `ping` para comprobar que funciona correctamente

Tal y como podemos comprobar, el proceso de spoofing se ha llevado a cabo con éxito. Como podemos ver, es bastante sencillo lanzar este tipo de ataques, por lo que esta capa de seguridad no es suficiente para proteger un punto de acceso. Para incrementar su seguridad, es necesario configurar el router para que use el protocolo de seguridad WPA2/3 con una contraseña fuerte en lugar de depender solo del filtrado MAC. Además, es conveniente establecer un IDS (Sistema de Detección de Intrusiones) y, si fuese necesario, un IPS (Sistema de Prevención de Intrusiones).

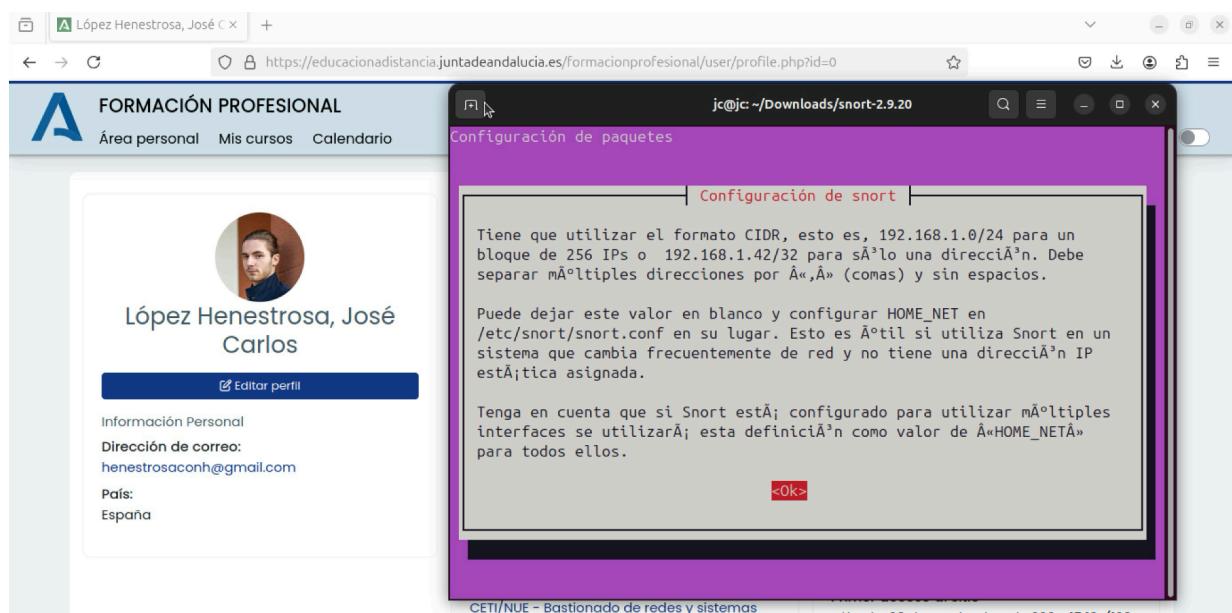
Implementación IDS

Despliega una solución de IDS de código abierto, como Snort, y configúrala.

Vamos a instalar Snort en Ubuntu con este comando:

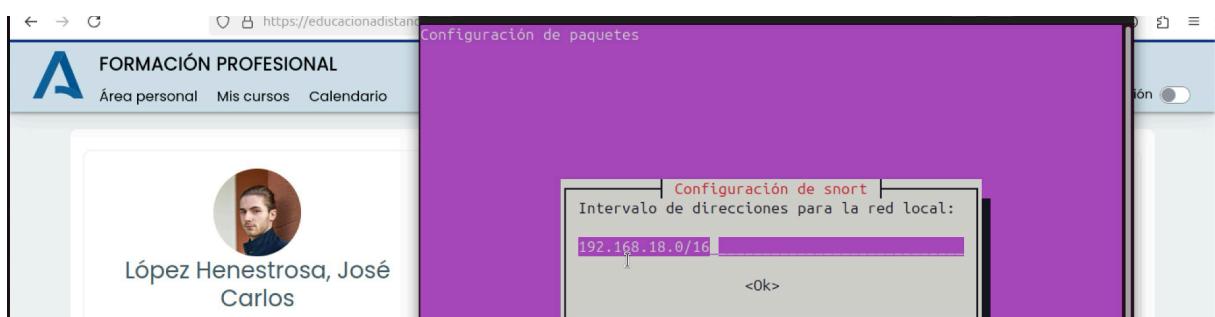
```
sudo apt-get install snort
```

Tras ejecutarlo, veremos la siguiente pantalla para configurar la herramienta:



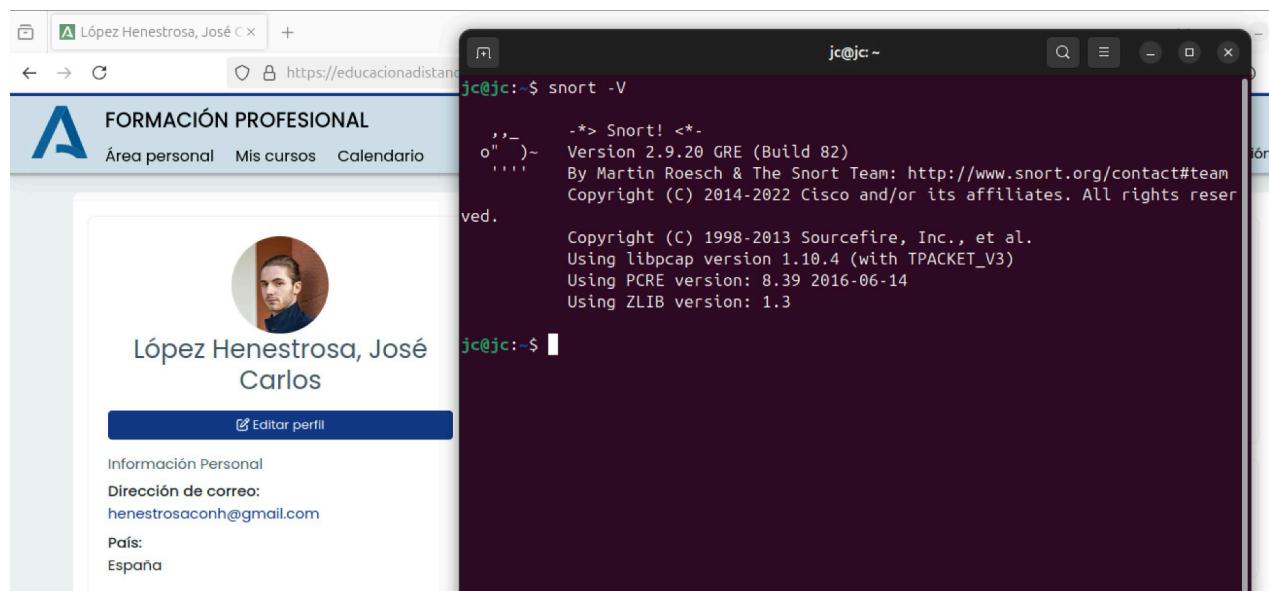
Primera pantalla de configuración de Snort

Al continuar, nos pedirá introducir el intervalo de direcciones IP para la red local. La IP de mi router es 192.168.18.1, lo cual significa que mi red local usa el rango 192.168.18.0/24, lo que abarca las direcciones 192.168.18.1 - 192.168.18.254.



Configuración del intervalo de direcciones IP para la red local

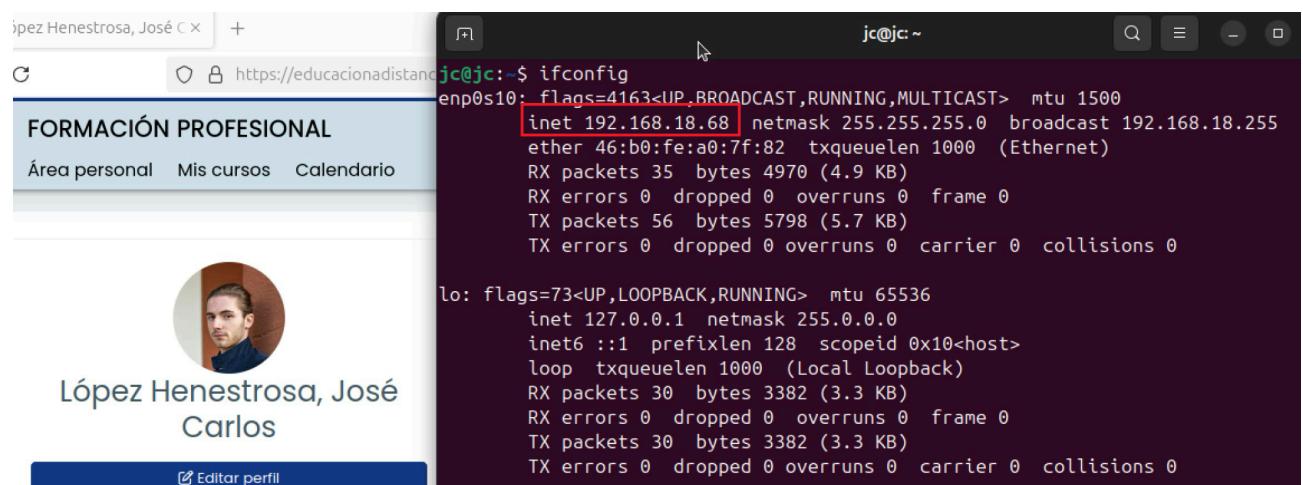
Al aceptar, la instalación se completará correctamente. Para comprobar que, efectivamente, Snort está disponible en el sistema, ejecutamos `snort -V`, lo cual debe mostrar el número de versión instalada.



La versión de Snort aparece, lo que indica que ha sido instalado con éxito

Realiza un escaneo con Nmap que trate de identificar los servicios para ver cómo se comporta la herramienta. Para ello, se requiere una máquina de ataque, que puede ser Kali, y otra máquina para desplegar Snort (puede ser otra distribución Linux o Windows).

Para realizar el ataque con Nmap, primero tenemos que identificar la IP de la máquina virtual con Ubuntu, el cual tiene instalado Snort. Para ello, ejecutamos el comando `ifconfig` en ella:



```
jc@jc:~$ ifconfig
enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
          inet 192.168.18.68 netmask 255.255.255.0 broadcast 192.168.18.255
                  ether 46:b0:fe:a0:7f:82 txqueuelen 1000 (Ethernet)
                  RX packets 35 bytes 4970 (4.9 KB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 56 bytes 5798 (5.7 KB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 30 bytes 3382 (3.3 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 30 bytes 3382 (3.3 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ejecución del comando `ifconfig` con la IP de la máquina virtual marcada en rojo

Como podemos ver, la IP de la máquina virtual es `192.168.18.68` y está conectada a través de la interfaz de red `enp0s10`, el cual es un dato relevante para desplegar Snort.

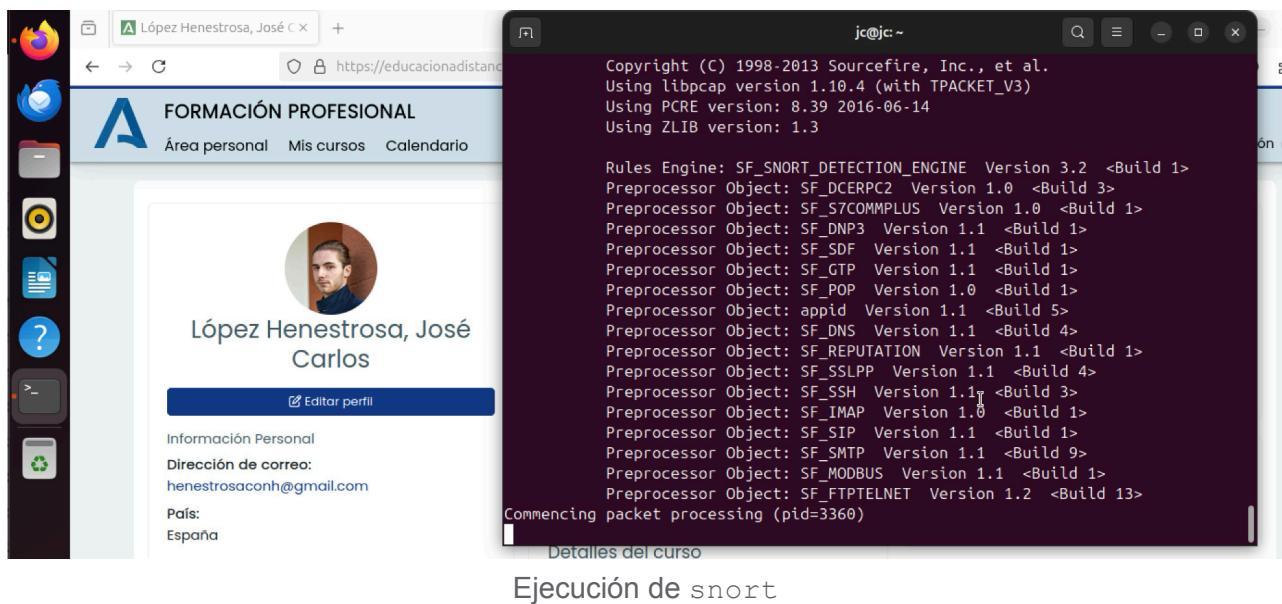
Una vez hallada la IP, ejecutaremos el siguiente comando para lanzar Snort con el fin de registrar alertas y analizar el tráfico de la interfaz de red a la que está conectada la máquina virtual.

```
sudo snort -l /var/log/snort/ -c /etc/snort/snort.conf -i enp0s10
```

Donde:

- `sudo`: Ejecuta Snort con privilegios de administrador, ya que requiere acceso a la interfaz de red y a archivos de configuración.
- `snort`: Llama al programa Snort.
- `-l /var/log/snort/`: Indica el directorio donde Snort almacenará los logs y las alertas generadas.
- `-c /etc/snort/snort.conf`: Especifica el archivo de configuración que Snort usará. Define las reglas, filtros y configuraciones del IDS.

- `-i enp0s10`: Define la interfaz de red en la que Snort monitoreará el tráfico. En este caso, `enp0s10`, ya que el ataque con Nmap se lanzará a la red Wi-Fi a la que también está conectada la máquina virtual donde hemos instalado Snort.



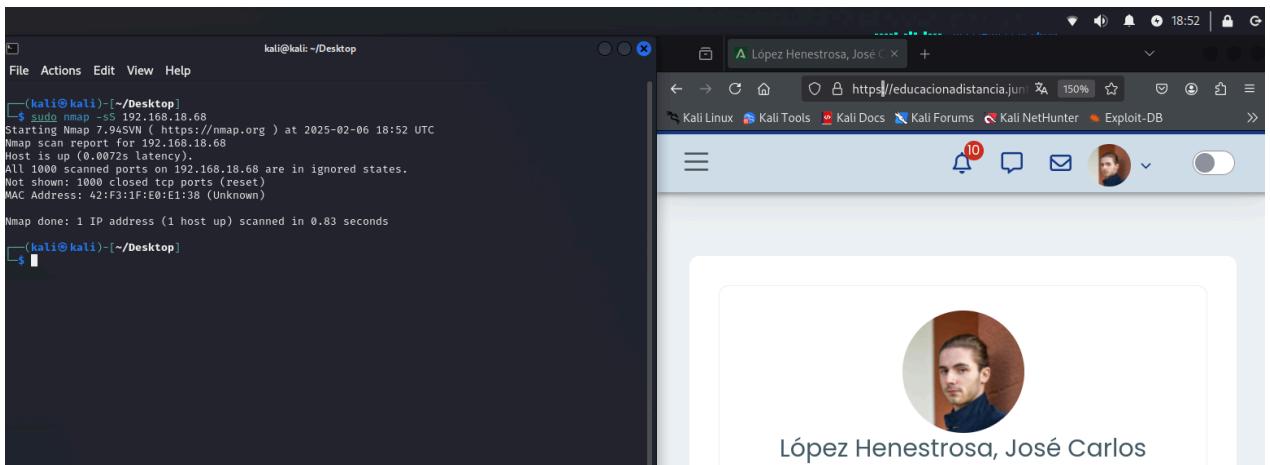
Ejecución de snort

Ahora que Snort está registrando y analizando el tráfico de la red, vamos al equipo con Kali Linux para lanzar el escaneo con Nmap. Para ello, ejecutamos el siguiente comando:

```
sudo nmap -sS 192.168.18.68
```

Donde:

- `sudo`: Ejecuta Snort con privilegios de administrador, ya que requiere acceso a la interfaz de red y a archivos de configuración.
- `nmap`: Llama al programa Nmap.
- `-sS`: Indica a Nmap que realice un **escaneo SYN** para identificar los puertos abiertos de manera rápida y sigilosa, sin establecer una conexión TCP completa. Este tipo de escaneo es ideal para descubrir servicios en ejecución en una máquina remota sin dejar huellas claras.
- `192.168.18.68`: IP de la máquina que va a recibir el ataque.

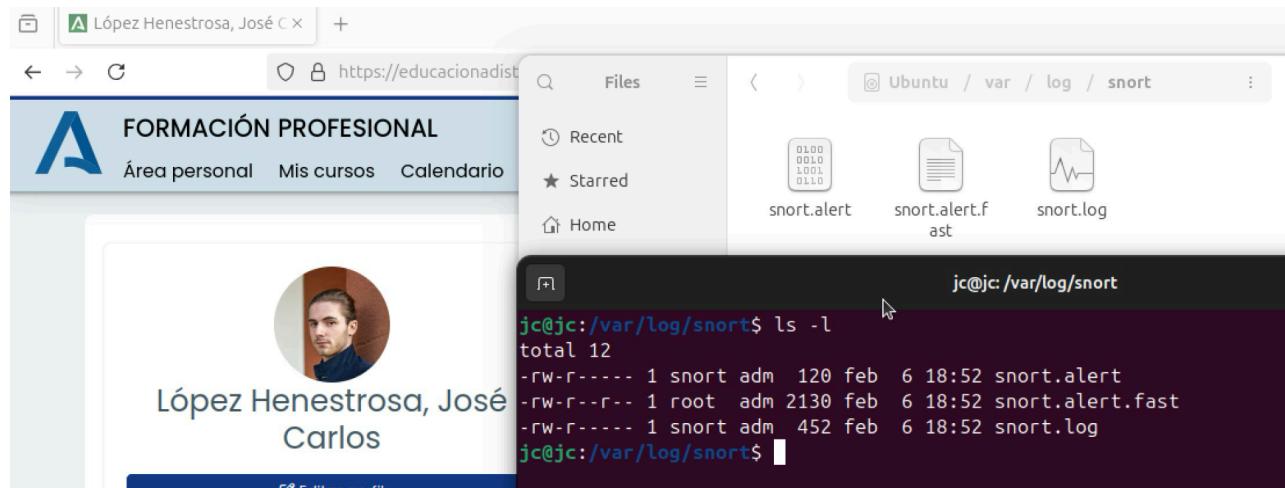


Lanzamiento de rastreo con Nmap

Como podemos ver, el ataque se ha ejecutado correctamente.

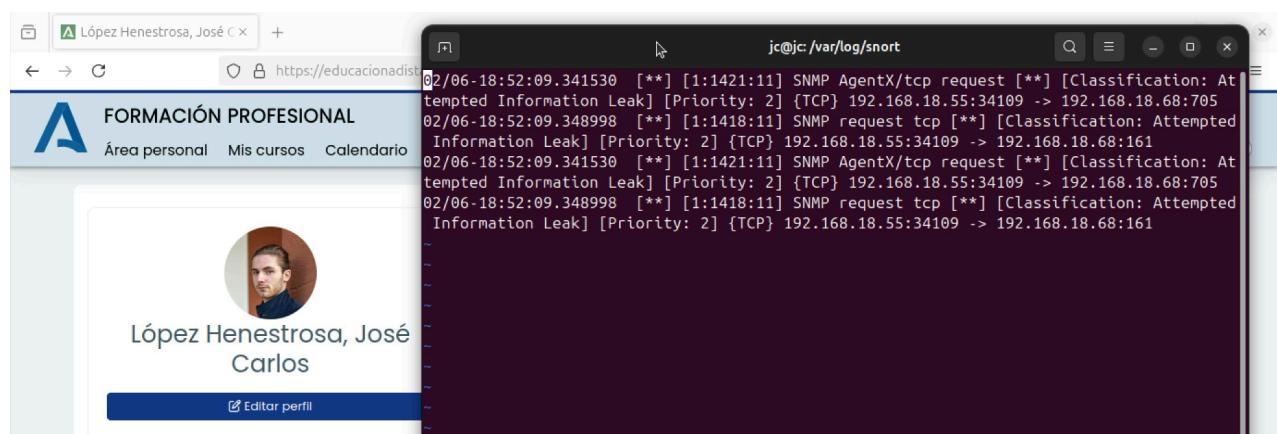
Interpreta los resultados de los logs del IDS tras lanzar el ataque con Nmap.

Para comprobar la respuesta de Snort ante el ataque con Nmap, volvemos a la máquina virtual con Ubuntu para comprobar los logs, los cuales se encuentran en el directorio `/var/log/snort/`, tras y como indicamos al ejecutar el programa. Ahí encontraremos tres archivos: `snort.alert`, `snort.alert.fast` y `snort.log`.



Archivos generados por Snort almacenados en el directorio `/var/log/snort/`

Abrimos el archivo `snort.alert.fast`, el cual contiene alertas simplificadas con un formato más conciso que otros archivos de logs completos, como `snort.alert`. Para ello, ejecutamos el comando `vim snort.alert.fast`:



Contenido del archivo `/var/log/snort/snort.alert.fast`

He aquí el contenido del archivo:

```
02/06-18:52:09.341530  [**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.18.55:34109 -> 192.168.18.68:705
02/06-18:52:09.348998  [**] [1:1418:11] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.18.55:34109 -> 192.168.18.68:161
02/06-18:52:09.341530  [**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.18.55:34109 -> 192.168.18.68:705
02/06-18:52:09.348998  [**] [1:1418:11] SNMP request tcp [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.18.55:34109 -> 192.168.18.68:161
```

Como podemos apreciar, las alertas generadas por Snort nos informan de que ha habido actividad relacionada con escaneo o recopilación de información a través de SNMP. Para entrar en más profundidad sobre lo que revelan los datos, analizaremos la estructura de la primera alerta:

```
02/06-18:52:09.341530  [**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP}
192.168.18.55:34109 -> 192.168.18.68:705
```

Donde:

- **Fecha y hora en la que se notificó la alerta:** 02/06-18:52:09.341530
- **ID de la alerta:** [1:1421:11]
 - 1: ID de la familia de reglas (en este caso, podría referirse a una familia como "ET" o "Snort").
 - 1421: ID de la regla específica de Snort que disparó la alerta.
 - 11: Indica cuántas veces ha sido actualizada dicha regla.
- **Descripción de la alerta:** SNMP AgentX/tcp request
 - Esta alerta está asociada con una *request* (petición) de SNMP AgentX sobre el protocolo TCP.
 - **SNMP (Simple Network Management Protocol)** es un protocolo utilizado para gestionar y monitorizar dispositivos de red.
 - **AgentX** es un protocolo para que los agentes SNMP se comuniquen con otros procesos de gestión.
- **Clasificación de la alerta:** [Classification: Attempted Information Leak]. Indica que ha detectado un intento de fuga de información (Attempted Information Leak), lo cual sugiere que la alerta está relacionada con un comportamiento potencialmente malicioso o sospechoso, como la filtración de información de configuración o datos del sistema.
- **Prioridad de la alerta:** [Priority: 2]. El 2 indica que es una alerta de baja a media gravedad. No es crítica, pero aún así requiere atención.

- **Protocolo de transporte utilizado en el ataque:** {TCP} (Transmission Control Protocol).
- **IP de la máquina atacante:** 192.168.18.55:34109.
- **IP de la máquina víctima:** 192.168.18.68:705. El puerto 705 es generalmente utilizado para AgentX.

Observamos, en definitiva, que las alertas almacenadas en el log están relacionadas con **intentos de consulta SNMP** desde la máquina 192.168.18.55 hacia la máquina 192.168.18.68. Como ya hemos comentado, en uno de los registros se utiliza el puerto 705, que es usado para AgentX (un protocolo para la extensión de SNMP), y en el otro se utiliza el puerto estándar 161 para SNMP.

La clasificación de ambas alertas es "Attempted Information Leak" (Intento de fuga de información), lo que sugiere que estas solicitudes pueden estar intentando acceder a información sensible o configuración de la máquina de destino sin autorización.

Bibliografía

- Documentación de Kali Linux. (2024, 6 de marzo). *Making a Kali Bootable USB Drive on Windows.* <https://www.kali.org/docs/usb/live-usb-install-with-windows/>
- Documentación de Kali Linux. (2024, 17 de noviembre). *macchanger.* <https://www.kali.org/tools/macchanger/>
- 0x00sec. (2016, 31 de mayo). *Macchanger - Spoofing your MAC Address.* <https://0x00sec.org/t/macchanger-spoofing-your-mac-address>
- Hacklido. (2024, 11 de julio). *Getting started with Snort IPS - A QuickStart Guide.* <https://hacklido.com/blog/873-getting-started-with-snort-ips-a-quickstart-guide>
- Manual Snort. <http://manual-snort-org.s3-website-us-east-1.amazonaws.com/>
- Blue Hosting. (2016, 23 de julio). *¿Cómo usar Nmap para escanear los puertos de un VPS?* <https://docs.bluehosting.cl/tutoriales/servidores/como-usar-nmap-para-escanear-los-puertos-de-un-vps.html>