



BASTIONADO DE REDES Y SISTEMAS

Tarea 5

ESTHER CARRILLO GÁLVEZ

Índice

Apartado 1: Filtrado MAC	3
Apartado 2: Implementación IDS	7
Webgrafía	12

Apartado 1: Filtrado MAC

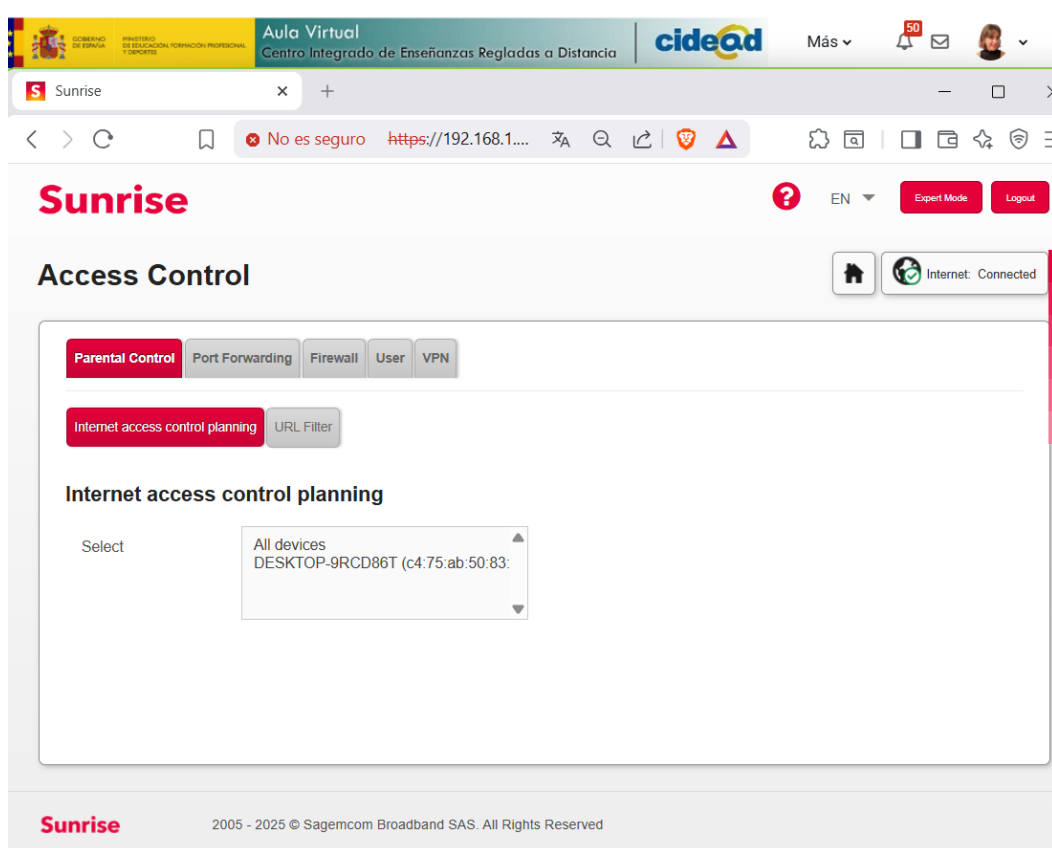
La alumna tendrá que configurar en la seguridad wifi de su router el filtrado MAC y añadir a la lista una MAC de un dispositivo que esté a su alcance (móvil, portátil, etc.). A continuación, desde una distribución Kali u otro linux, virtualizada o nativa, se hará pasar por el dispositivo autorizado modificando su MAC con la aplicación correspondiente y comprobando que se puede conectar.

Aquellos alumnos que no dispongan de un router donde poder implementar el filtrado MAC, puede crear una MV con Linux y mediante iptables puede realizar el filtrado MAC. Puede establecer un servicio como ssh y realizar el filtrado MAC hacia ese servicio.

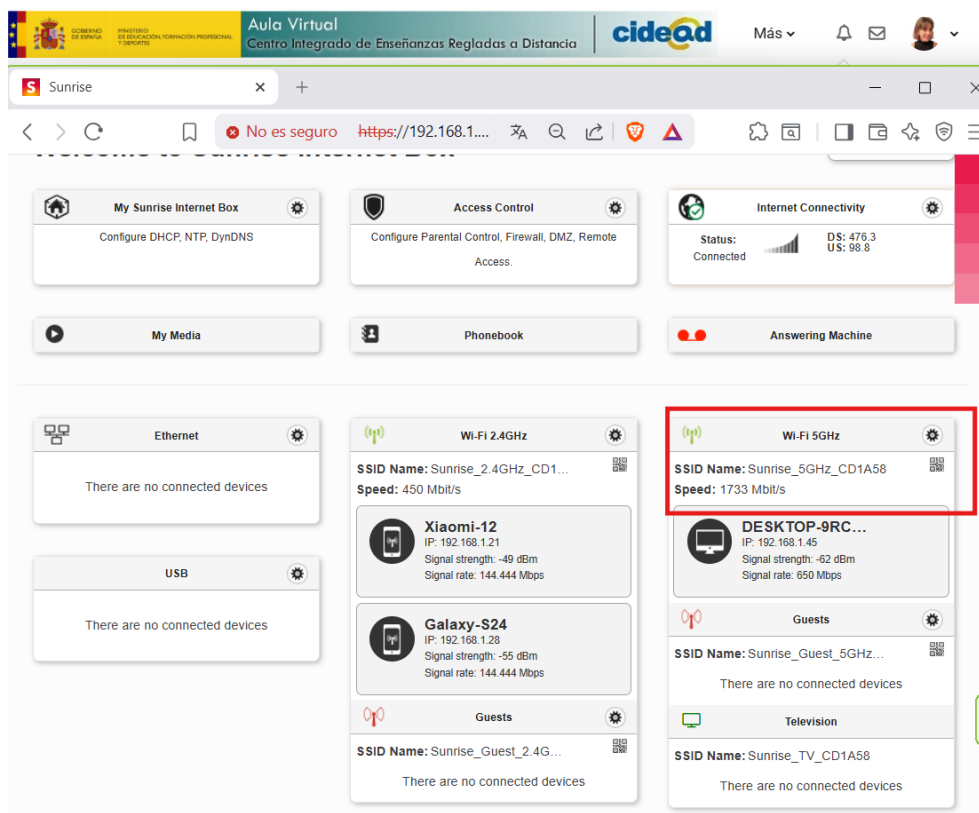
Para comenzar con la práctica, se accede a la configuración del router desde 192.168.1.1 y desde el modo *Expert Mode*, se selecciona *Access Control* donde se podrán ver las direcciones MAC registradas en el momento de la captura.

La dirección MAC existente:

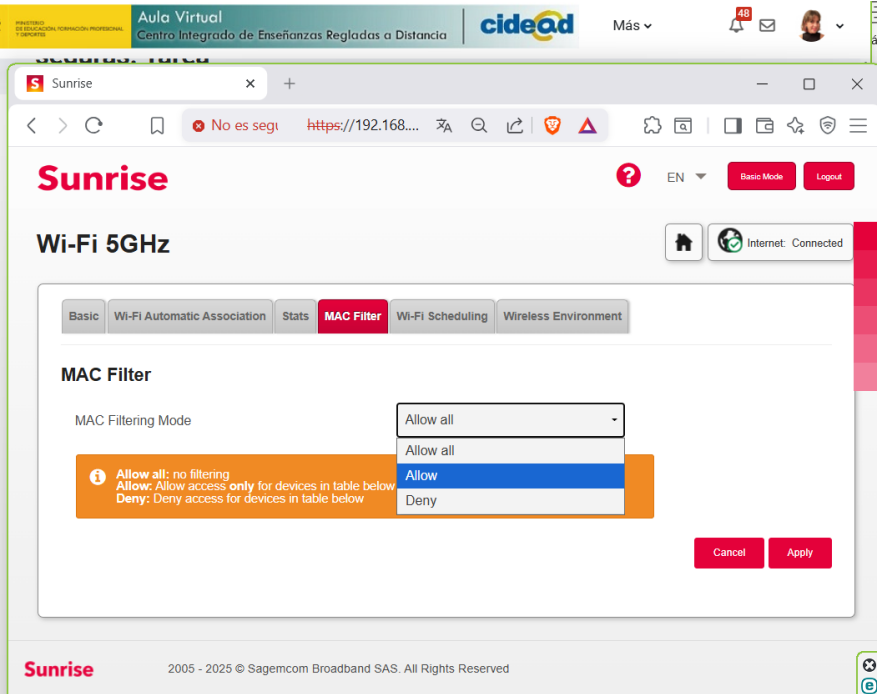
c4:75:ab:50:83:31 (para el portátil)



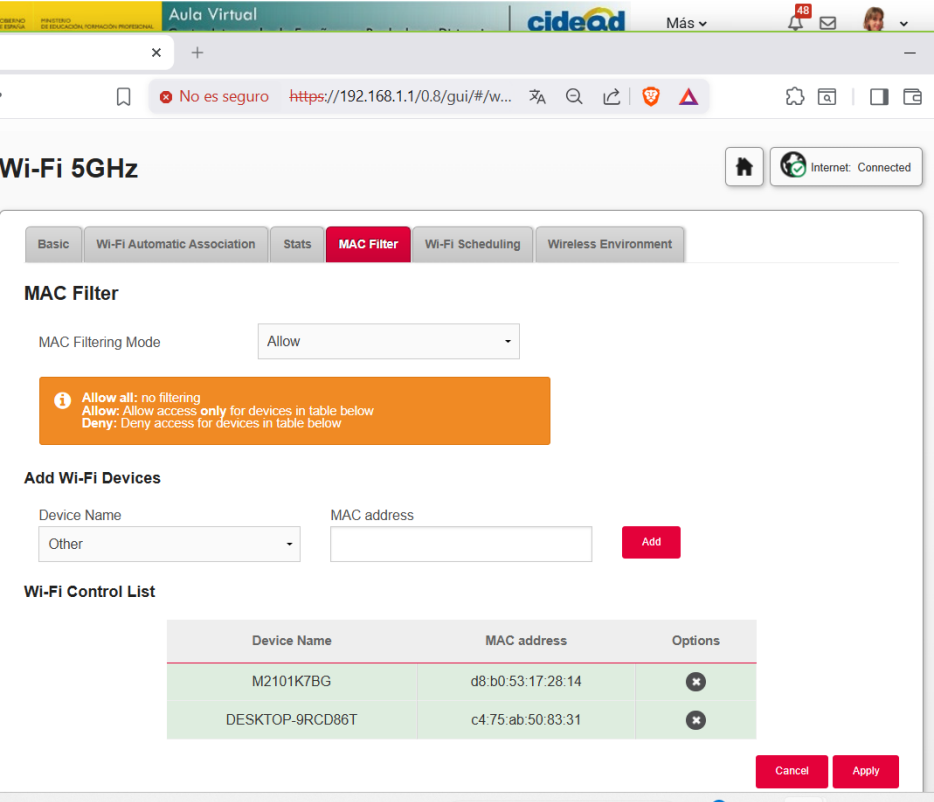
Se selecciona la red específica *Wifi 5GHz*.



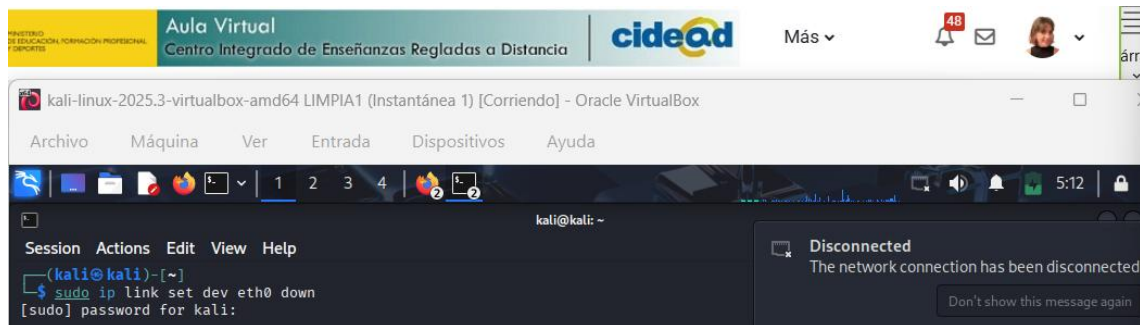
Una vez dentro de la red, se selecciona la pestaña MAC Filter y cambiar el MAC Filtering Mode *Allow all* a *Allow*. Esto significa que el router bloqueará a cualquier dispositivo que intente conectarse, a menos que su MAC esté en esa lista verde de abajo.



Añadir las direcciones MAC del primer paso. Tanto la MAC del móvil, como la MAC del portátil para no perder el acceso al router.

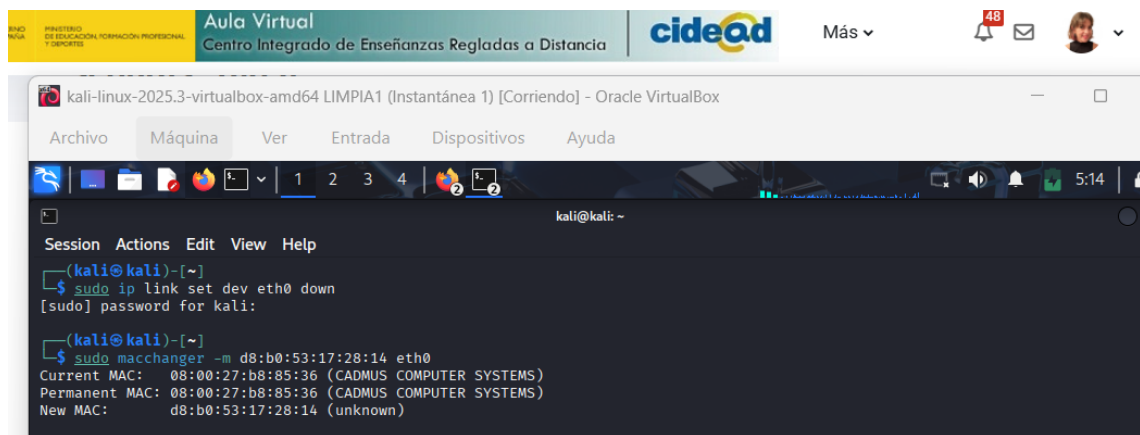


Desde la terminal de la máquina virtual Kali Linux, se procede al cambio de la dirección física por la MAC de mi móvil. En primer lugar, se apaga la tarjeta para cambiarle el nombre mediante el comando `sudo ip link set dev eth0 down`



```
kali@kali: ~  
$ sudo ip link set dev eth0 down  
[sudo] password for kali:
```

A continuación, con el comando `sudo macchanger -m d8:b0:53:17:28:14 eth0`, cambiar la MAC de la máquina Kali por la MAC del móvil.



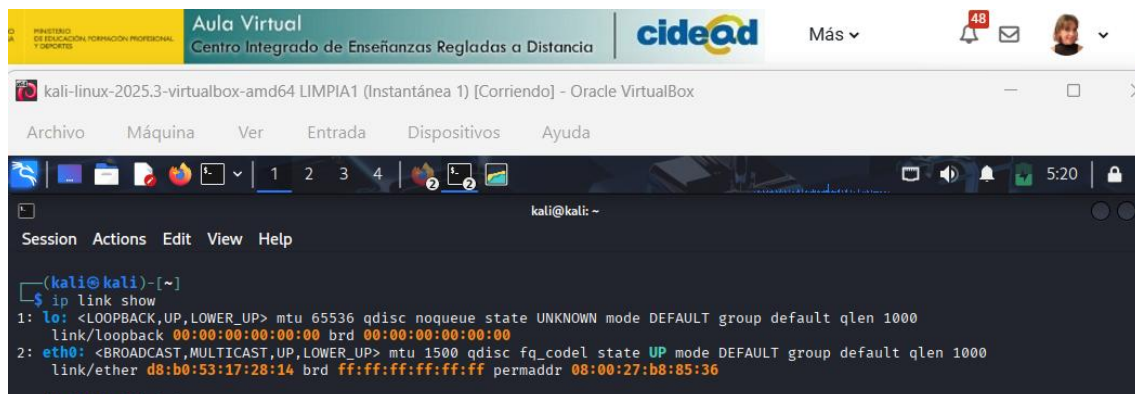
```
kali@kali: ~  
$ sudo ip link set dev eth0 down  
[sudo] password for kali:  
  
$ sudo macchanger -m d8:b0:53:17:28:14 eth0  
Current MAC: 08:00:27:b8:85:36 (CADMUS COMPUTER SYSTEMS)  
Permanent MAC: 08:00:27:b8:85:36 (CADMUS COMPUTER SYSTEMS)  
New MAC: d8:b0:53:17:28:14 (unknown)
```

Encender la tarjeta con la nueva dirección física mediante el comando `sudo ip link set dev eth0 up`




```
kali@kali: ~  
$ sudo ip link set dev eth0 up
```

Se comprueba que la MAC de Kali Linux sea `d8:b0:53:17:28:14` con el comando `ip link show`



```
kali@kali: ~  
$ ip link show  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000  
    link/ether d8:b0:53:17:28:14 brd ff:ff:ff:ff:ff:ff permaddr 08:00:27:b8:85:36
```

El comando `macchanger -s eth0` sirve para visualizar el estado actual de la dirección MAC de la interfaz `eth0`. Se muestran la *current* MAC y la *Permanent* MAC.



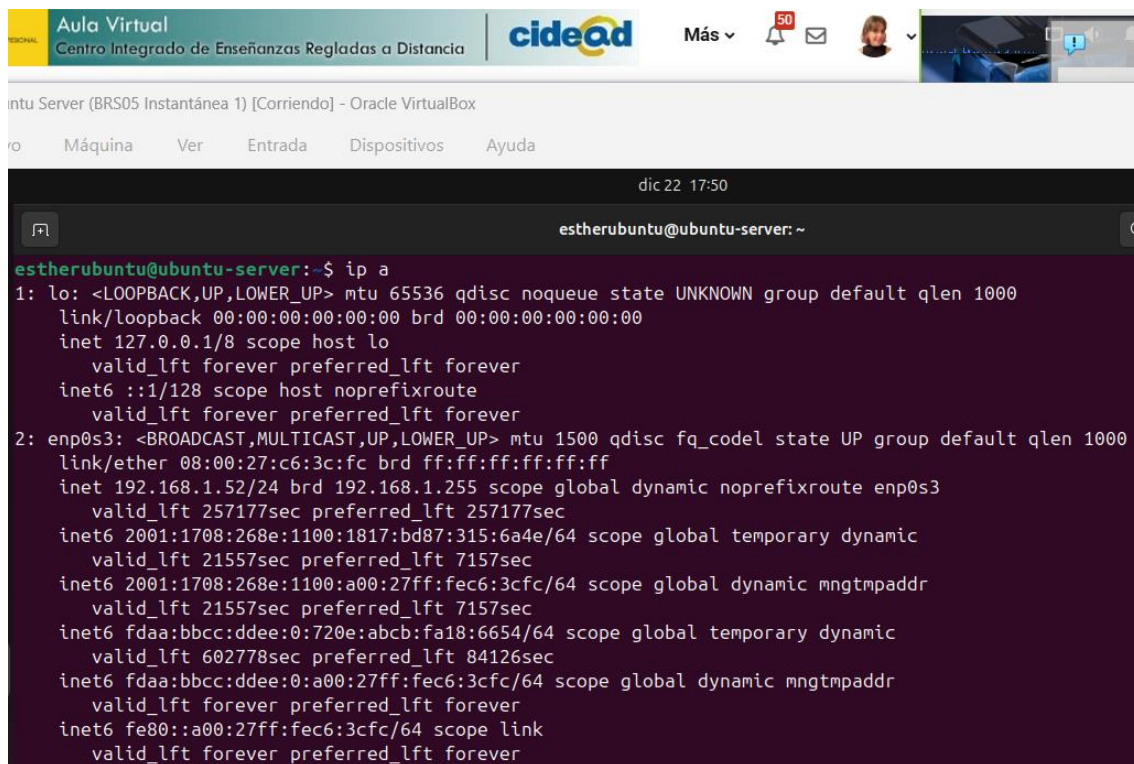
```
kali@kali: ~  
$ macchanger -s eth0  
Current MAC: d8:b0:53:17:28:14 (unknown)  
Permanent MAC: 08:00:27:b8:85:36 (CADMUS COMPUTER SYSTEMS)
```

Apartado 2: Implementación IDS

La alumna llevará a cabo un trabajo de investigación que consistirá en desplegar una solución de IDS opensource como SNORT y tras configurarla, realizará un escaneo con nmap que trate de identificar los servicios para ver cómo se comporta la herramienta. Para ello necesitará una máquina de ataque que puede ser Kali, y otra máquina para desplegar Snort (puede ser otra distribución Linux o un Windows). Tras desplegar la herramienta, la alumna tendrá que saber dónde se almacenan los logs del IDS para que, una vez lanzado el ataque con nmap, pueda interpretar los resultados.

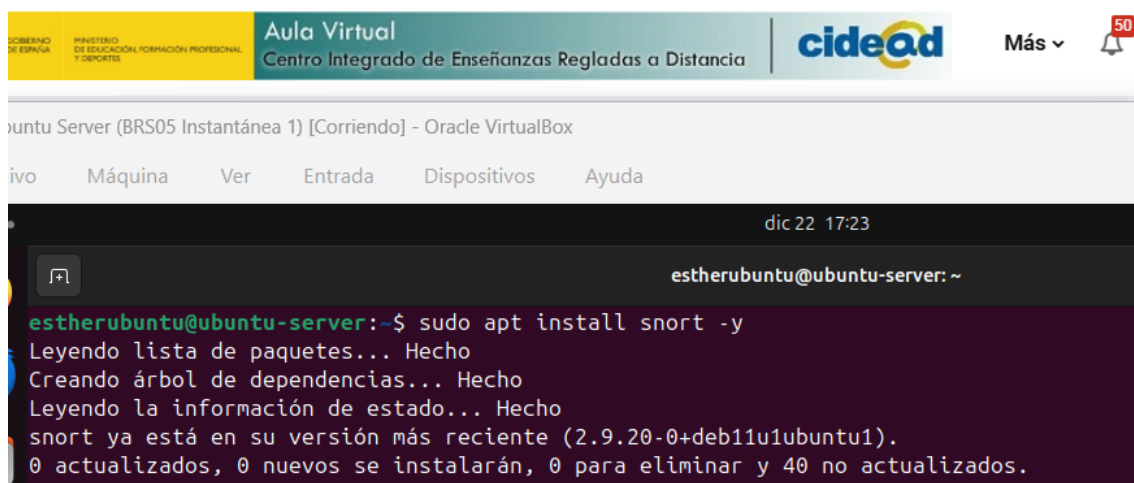
Para este segundo apartado, se utilizará una máquina virtual Kali Linux que actuará como atacante y una máquina virtual Ubuntu Linux que actuará como el servidor donde se va a desplegar Snort.

En primer lugar, con el comando `ip a`, se observa la ip para la máquina servidor Linux Ubuntu. La dirección IP es 192.168.1.52



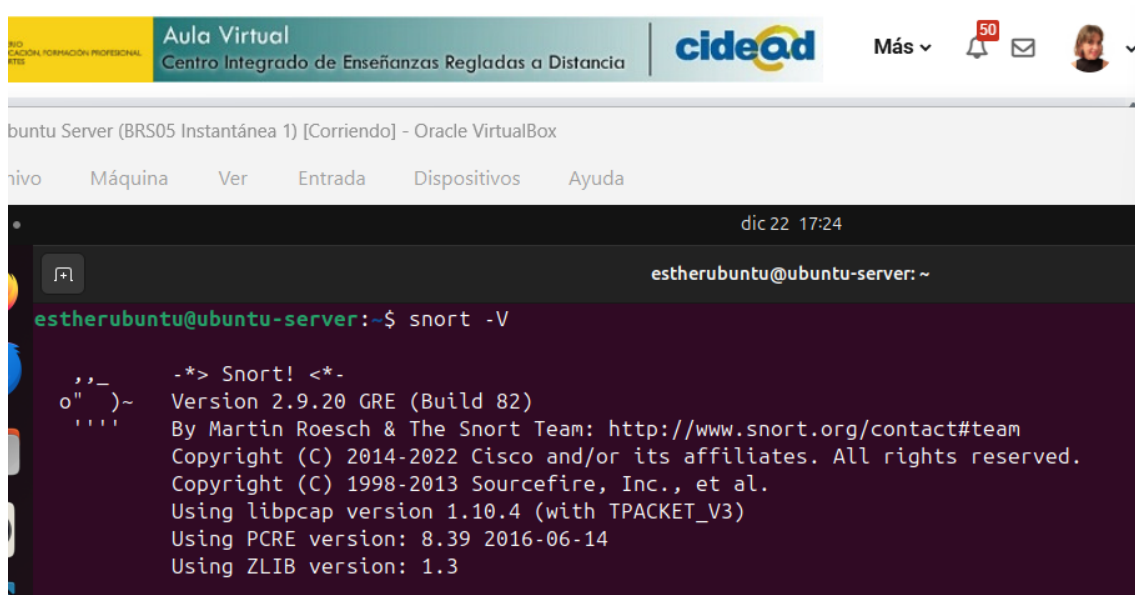
```
dic 22 17:50
estherubuntu@ubuntu-server: ~
estherubuntu@ubuntu-server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c6:3c:fc brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.52/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 257177sec preferred_lft 257177sec
    inet6 2001:1708:268e:1100:1817:bd87:315:6a4e/64 scope global temporary dynamic
        valid_lft 21557sec preferred_lft 7157sec
    inet6 2001:1708:268e:1100:a00:27ff:fec6:3cfc/64 scope global dynamic mngtmpaddr
        valid_lft 21557sec preferred_lft 7157sec
    inet6 fd0a:bbcc:ddee:0:720e:abcb:fa18:6654/64 scope global temporary dynamic
        valid_lft 602778sec preferred_lft 84126sec
    inet6 fd0a:bbcc:ddee:0:a00:27ff:fec6:3cfc/64 scope global dynamic mngtmpaddr
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec6:3cfc/64 scope link
        valid_lft forever preferred_lft forever
```

Se procede a la instalación de *Snort* con el comando `sudo apt install snort -y`



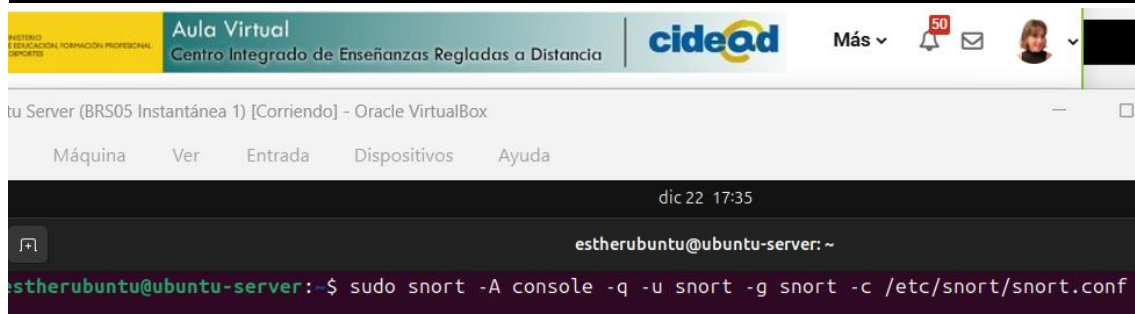
```
dic 22 17:23
estherubuntu@ubuntu-server: ~
estherubuntu@ubuntu-server:~$ sudo apt install snort -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
snort ya está en su versión más reciente (2.9.20-0+deb11u1ubuntu1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 40 no actualizados.
```


El comando **snort -V** comprueba que Snort se ha instalado correctamente y no tiene errores de configuración.



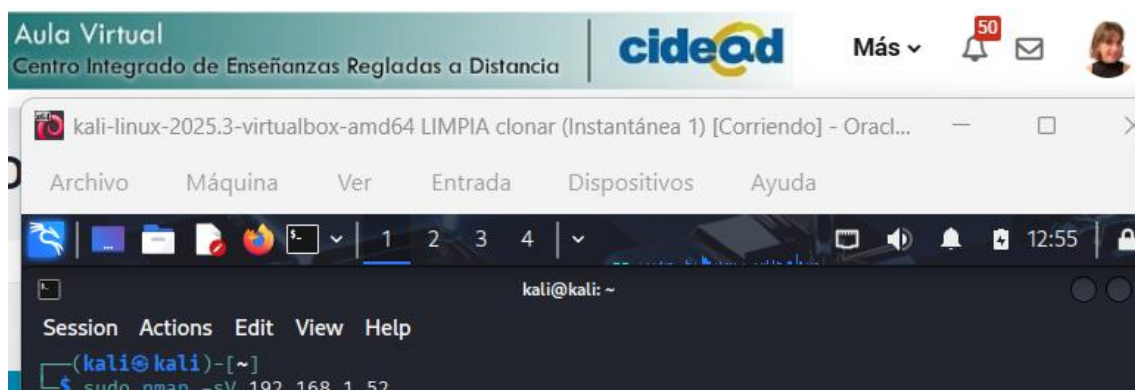
```
dic 22 17:24
estherubuntu@ubuntu-server: ~
estherubuntu@ubuntu-server:~$ snort -V
_*> Snort! <*_
o" )~
' _
' _
' _
' _
Version 2.9.20 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap version 1.10.4 (with TPACKET_V3)
Using PCRE version: 8.39 2016-06-14
Using ZLIB version: 1.3
```

Se pone a Snort en modo para que escuche la red mediante el comando **sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf**.



```
dic 22 17:35
estherubuntu@ubuntu-server: ~
estherubuntu@ubuntu-server:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf
```

El siguiente paso es lanzar el ataque en Kali Linux con el comando **sudo nmap -sV 192.168.1.52** que le dice a Kali que ejecute Nmap con privilegios de administrador (s viene de *Scan* y V de *Version Detection*) y realizar un escaneo de la red más profundo.



```
kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sV 192.168.1.52
```

Según se indica en la columna de PORT STATE SERVICE VERSION, indica que el puerto 22, que es SSH, está abierto.

```

kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sV 192.168.1.52
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-22 12:54 EST
Nmap scan report for ubuntu-server (192.168.1.52)
Host is up (0.0011s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
MAC Address: 08:00:27:C6:3C:FC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds
  
```

Ahora se vuelve a la máquina Ubuntu donde está desplegado Snort para saber dónde se almacenan los logs del IDS. Snort arroja estas alertas de seguridad en tiempo real generadas por el sistema de detección de intrusos.

```

dic 22 18:06
estherubuntu@ubuntu-server: ~
estherubuntu@ubuntu-server:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf
[sudo] password for estherubuntu:

12/22-17:55:00.171139  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2]
{TCP} 192.168.1.53:43518 -> 192.168.1.52:161
12/22-17:55:00.189155  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Priority: 2]
{TCP} 192.168.1.53:43518 -> 192.168.1.52:705
12/22-17:59:40.864985  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2]
{UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-17:59:40.864988  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2]
{UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-17:59:40.864988  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2]
{UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-17:59:40.864989  [**] [1:1384:8] MISC UPnP malformed advertisement [**] [Classification: Misc Attack] [Priority: 2]
{UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
  
```

The image shows a terminal window from a virtual machine. The title bar at the top indicates it's an 'Aula Virtual' (Virtual Classroom) from 'cideon' (Centro Integrado de Enseñanzas Regladas a Distancia). The terminal shows the user 'estherubuntu' at the 'ubuntu-server' machine, in the directory '/var/log/snort'. They have run the command 'ls -l', which lists several files. The file 'snort.alert.fast' is highlighted with a red rectangular box. The files listed are: 'snort.alert' (5112 bytes, Dec 22 18:19), 'snort.alert.fast' (16889 bytes, Dec 22 18:19), 'snort.log' (47272 bytes, Dec 22 18:19), 'snort.log.1766424889' (2869 bytes, Dec 22 17:48), and 'snort.log.1766425798' (5081 bytes, Dec 22 18:19). The total size of the files is 92 bytes.

Aula Virtual

Centro Integrado de Enseñanzas Regladas a Distancia

Más ▾

ntu Server (BR505 Instantánea 1) [Corriendo] - Oracle VirtualBox

MáquinaVerEntradaDispositivosAyuda

dic 22 18:54

estherubuntu@ubuntu-server: /var/log/snort

```
estherubuntu@ubuntu-server:/var/log/snort$ sudo cat /var/log/snort/snort.alert.fast
12/22-16:39:49.324868 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:39:49.324869 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:39:49.324940 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:39:49.324940 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:47:43.108852 [[**] [1:1917:6] SCAN UPnP service discover attempt [[**] [Classification: Detection of a Network Scan] [Priority: 3]] {UDP} 192.168.1.45:54316 -> 239.255.255.250:1900
12/22-16:47:46.109439 [[**] [1:1917:6] SCAN UPnP service discover attempt [[**] [Classification: Detection of a Network Scan] [Priority: 3]] {UDP} 192.168.1.45:54316 -> 239.255.255.250:1900
12/22-16:47:49.110409 [[**] [1:1917:6] SCAN UPnP service discover attempt [[**] [Classification: Detection of a Network Scan] [Priority: 3]] {UDP} 192.168.1.45:54316 -> 239.255.255.250:1900
12/22-16:49:47.721343 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:49:47.721343 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:49:47.721343 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:49:47.721343 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:59:46.811017 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:59:46.811017 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:59:46.811017 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
12/22-16:59:46.811017 [[**] [1:1384:8] MISC UPnP malformed advertisement [[**] [Classification: Misc Attack] [Priority: 2]] {UDP} 192.168.1.1:1900 -> 239.255.255.250:1900
```

Webgrafía

<https://www.snort.org/>

<https://www.youtube.com/watch?v=MwqdKevOas0&t=170s>

<https://www.fortinet.com/lat/resources/cyberglossary/snort>