



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:

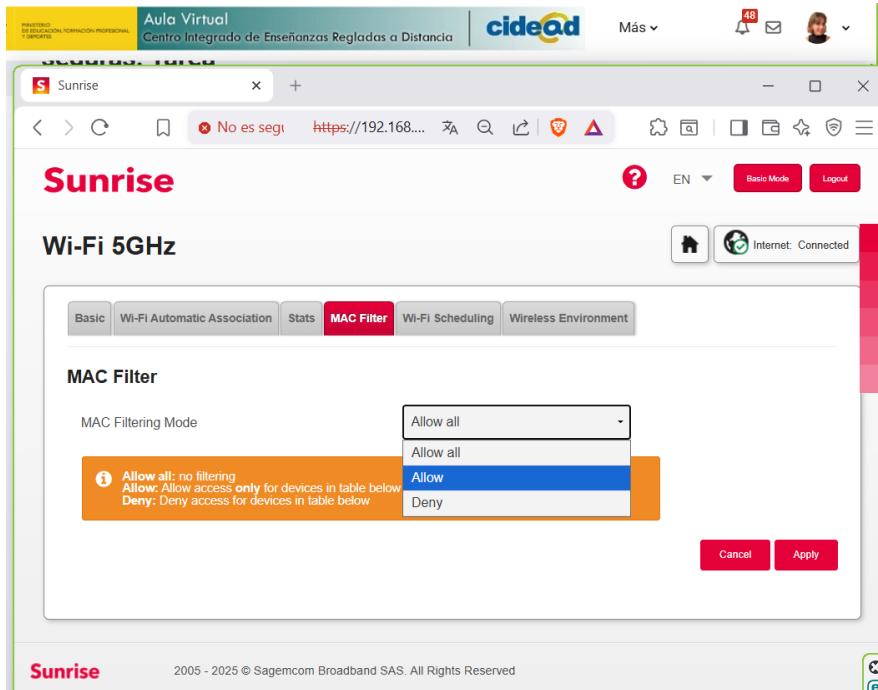
c4:75:ab:50:83:31 (para el portátil)

The screenshot shows the Sunrise Access Control interface. At the top, there are tabs for Parental Control, Port Forwarding, Firewall, User, and VPN. The Parental Control tab is highlighted with a red border. Below the tabs, there are two buttons: Internet access control planning (highlighted with a red border) and URL Filter. The main area is titled "Internet access control planning" and contains a dropdown menu labeled "Select" which shows "All devices DESKTOP-9RCD86T (c4:75:ab:50:83)". At the bottom left, it says "Sunrise" and at the bottom right, it says "2005 - 2025 © Sagemcom Broadband SAS. All Rights Reserved".

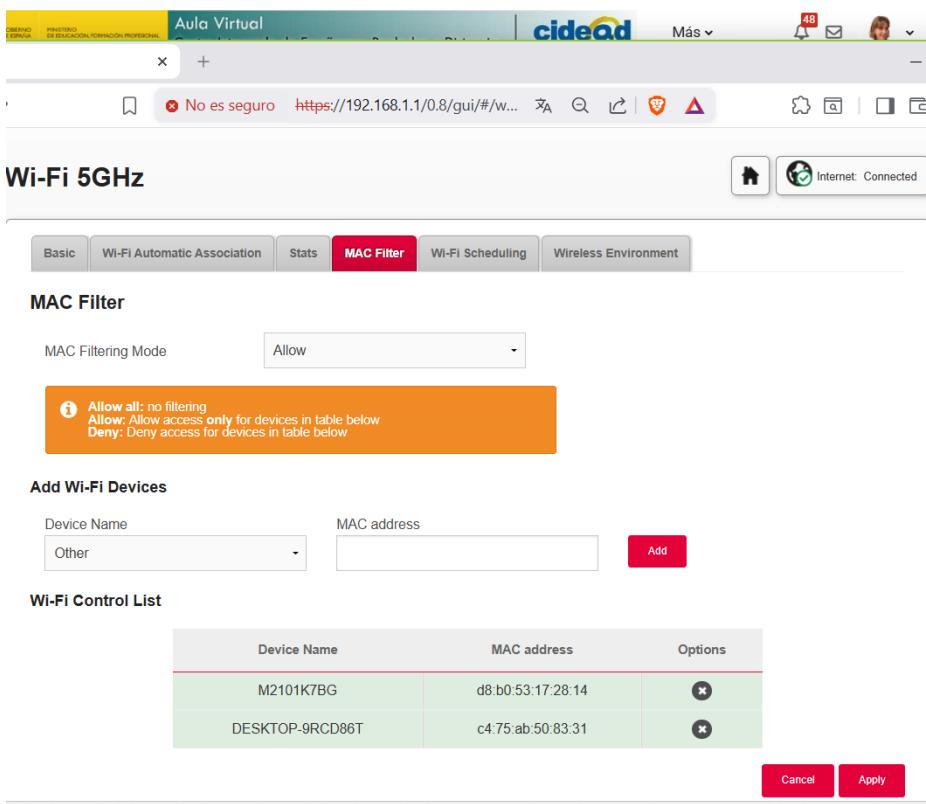
Se selecciona la red específica Wifi 5GHz.

The screenshot shows the Sunrise Internet Box interface. It features several cards: My Sunrise Internet Box (Configure DHCP, NTP, DynDNS), Access Control (Configure Parental Control, Firewall, DMZ, Remote Access), Internet Connectivity (Status: Connected, DS: 476.3, US: 98.8), My Media, Phonebook, Answering Machine, Ethernet (There are no connected devices), USB (There are no connected devices), Wi-Fi 2.4GHz (SSID Name: Sunrise_2.4GHz_CD1..., Speed: 450 Mbit/s, listing devices: Xiaomi-12 and Galaxy-S24), and Wi-Fi 5GHz (SSID Name: Sunrise_5GHz_CD1A58, Speed: 1733 Mbit/s, listing device: DESKTOP-9RC...). The Wi-Fi 5GHz card is highlighted with a red box.

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.



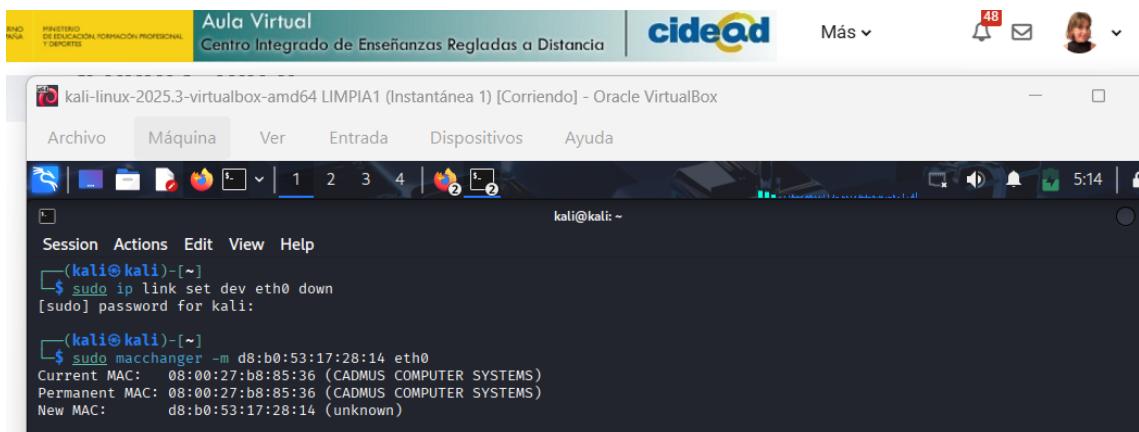
Añadir las direcciones MAC del primer paso. Tanto la MAC del móvil, como la MAC del portátil para no perder el acceso al router.



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`



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.



Encender la tarjeta con la nueva dirección física mediante el comando `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`



A screenshot of a terminal window titled "kali-linux-2025.3-virtualbox-amd64 LIMPIA1 (Instantánea 1) [Corriendo] - Oracle VirtualBox". The terminal shows the command `ip link show` being run, and its output indicates two interfaces: `lo` (loopback) and `eth0`. The `eth0` interface has the MAC address `d8:b0:53:17:28:14`.

```
(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*.



A screenshot of a terminal window titled "kali-linux-2025.3-virtualbox-amd64 LIMPIA1 (Instantánea 1) [Corriendo] - Oracle VirtualBox". The terminal shows the command `macchanger -s eth0` being run. It displays the current MAC address (`d8:b0:53:17:28:14`) and the permanent MAC address (`08:00:27:b8:85:36`).

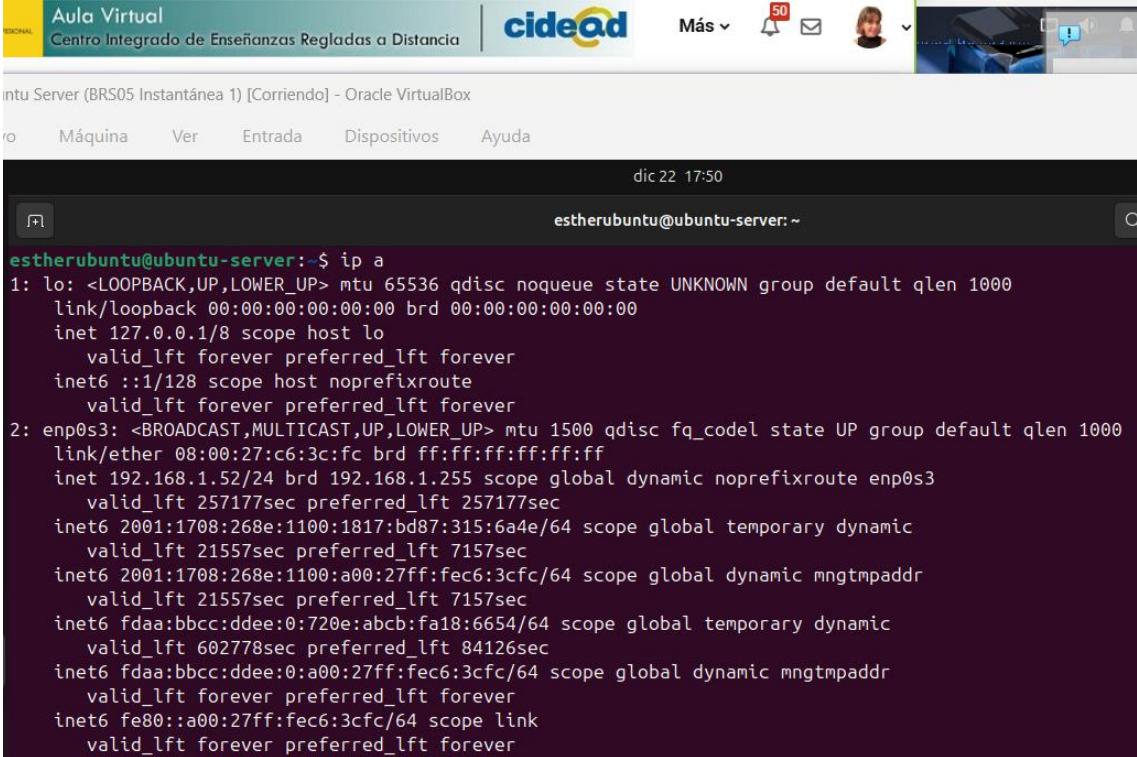
```
(kali㉿kali)-[~]
$ macchanger -s eth0
Current MAC:  d8:b0:53:17:28:14 (unknown)
Permanent MAC: 08:00:27:b8:85:36 (CADMUS COMPUTER SYSTEMS)
```

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.

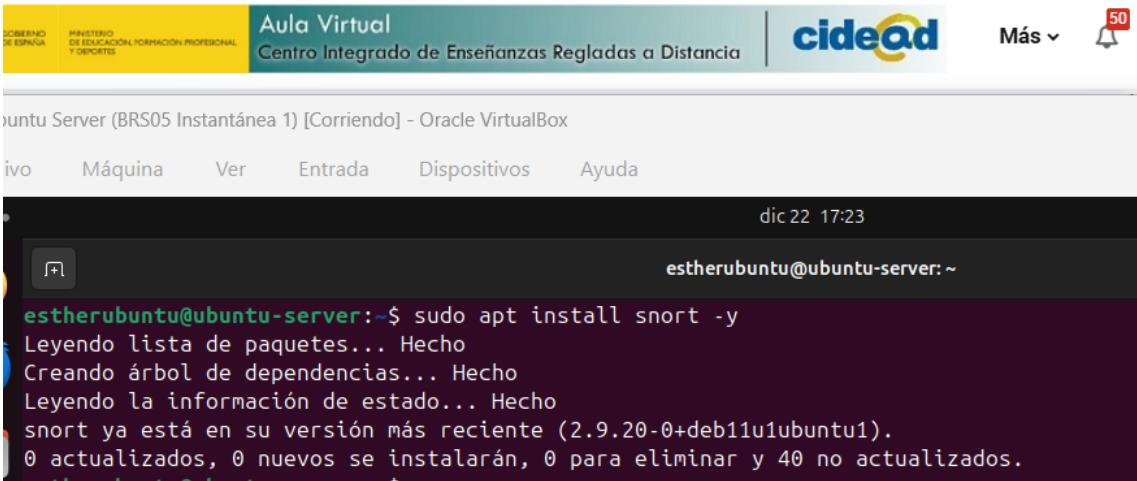
En primer lugar, con el comando `ip a`, se observa la ip para la máquina servidor Linux Ubuntu. La dirección IP es 192.168.1.52



The screenshot shows the Oracle VM VirtualBox Manager interface. At the top, there's a header with the Aula Virtual logo and navigation links like 'Máquina', 'Ver', 'Entrada', 'Dispositivos', and 'Ayuda'. The date 'dic 22 17:50' is displayed. Below the header, a terminal window is open with the command `ip a`. The output shows network interfaces: 'lo' (loopback) and 'enp0s3' (ethernet). The 'enp0s3' interface has an IP address of 192.168.1.52/24, which is highlighted in yellow.

```
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:1100:0:0:27ff:fec6:3cfc/64 scope global dynamic mngtmpaddr
        valid_lft 21557sec preferred_lft 7157sec
    inet6 fd8a:bbcc:ddee:0:720e:abcb:fa18:6654/64 scope global temporary dynamic
        valid_lft 602778sec preferred_lft 84126sec
    inet6 fd8a: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
```

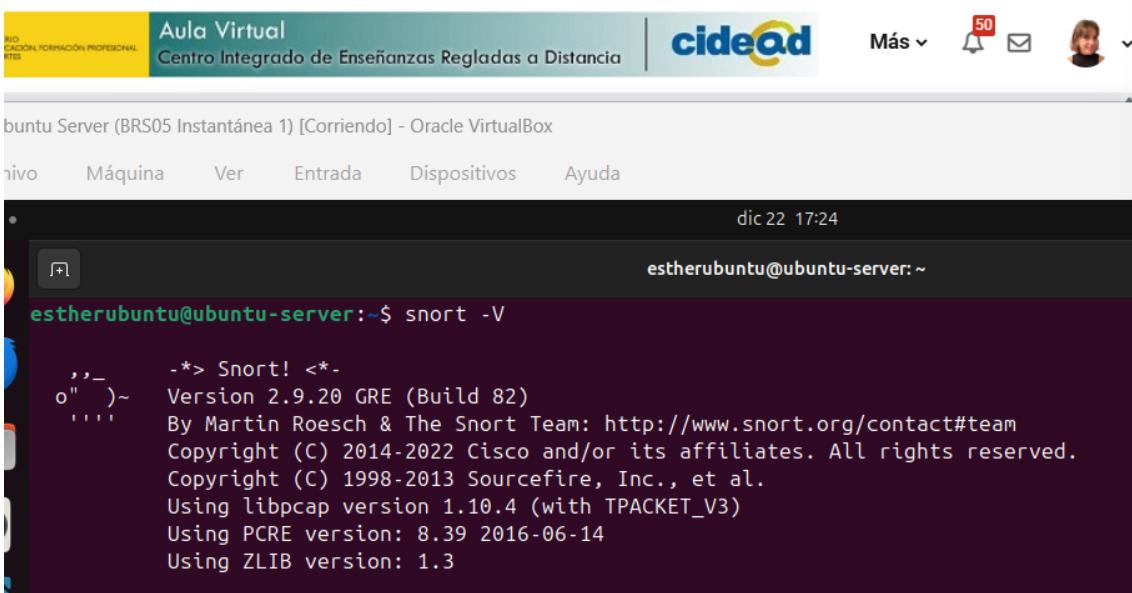
Se procede a la instalación de *Snort* con el comando `sudo apt install snort -y`



The screenshot shows the Oracle VM VirtualBox Manager interface. At the top, there's a header with the Aula Virtual logo and navigation links like 'Máquina', 'Ver', 'Entrada', 'Dispositivos', and 'Ayuda'. The date 'dic 22 17:23' is displayed. Below the header, a terminal window is open with the command `sudo apt install snort -y`. The output shows the process of installing Snort, including reading package lists, creating dependency trees, and checking state information. It also indicates that Snort is already at its latest version (2.9.20-0+deb11u1ubuntu1) and that no updates are available.

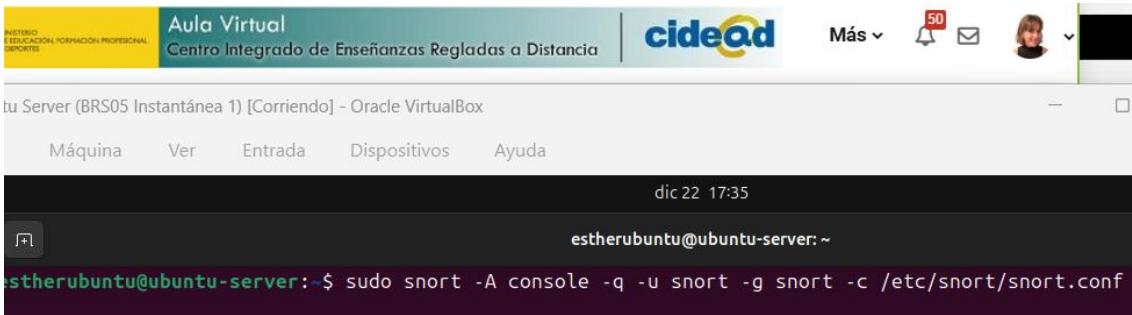
```
estherubuntu@ubuntu-server:~$ sudo apt install snort -y
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
snort ya está en su versión más reciente (2.9.20-0+deb11u1ubuntu1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y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

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



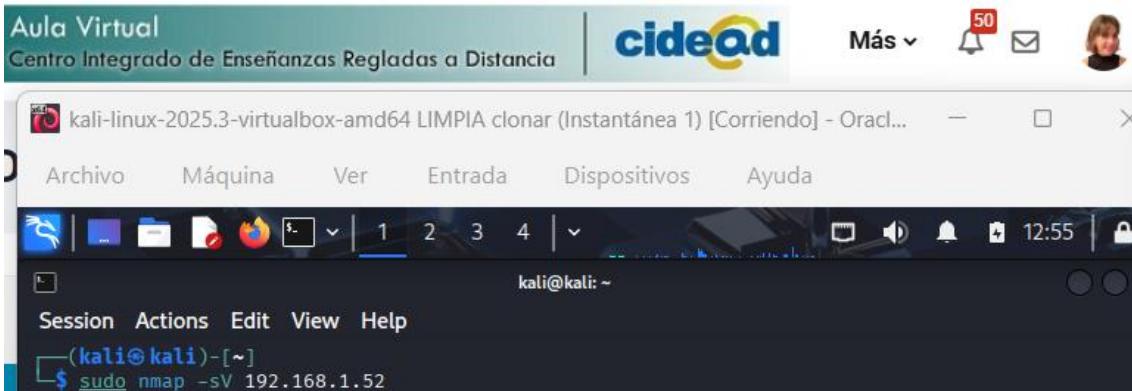
```
estherubuntu@ubuntu-server:~$ snort -V
,,-> Snort! <-
o" )~ Version 2.9.20 GRE (Build 82)
'.' By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using libpcap 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`.



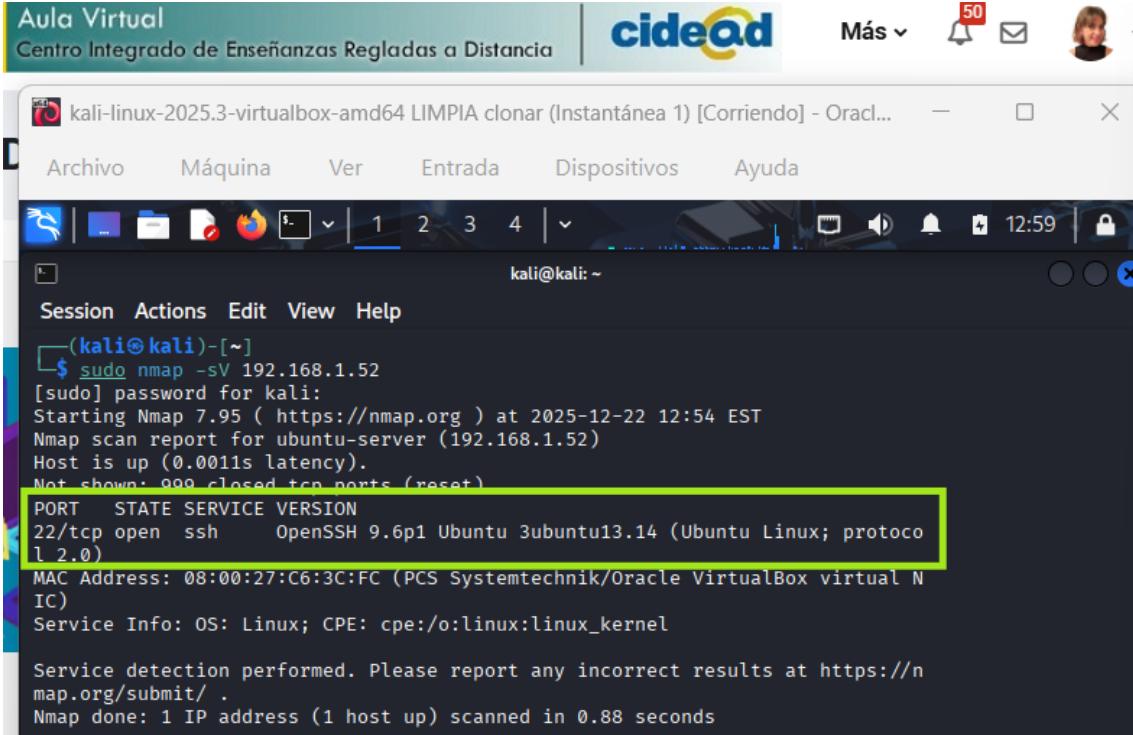
```
estherubuntu@ubuntu-server:~$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf
```

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: ~
└─$ sudo nmap -sV 192.168.1.52
```

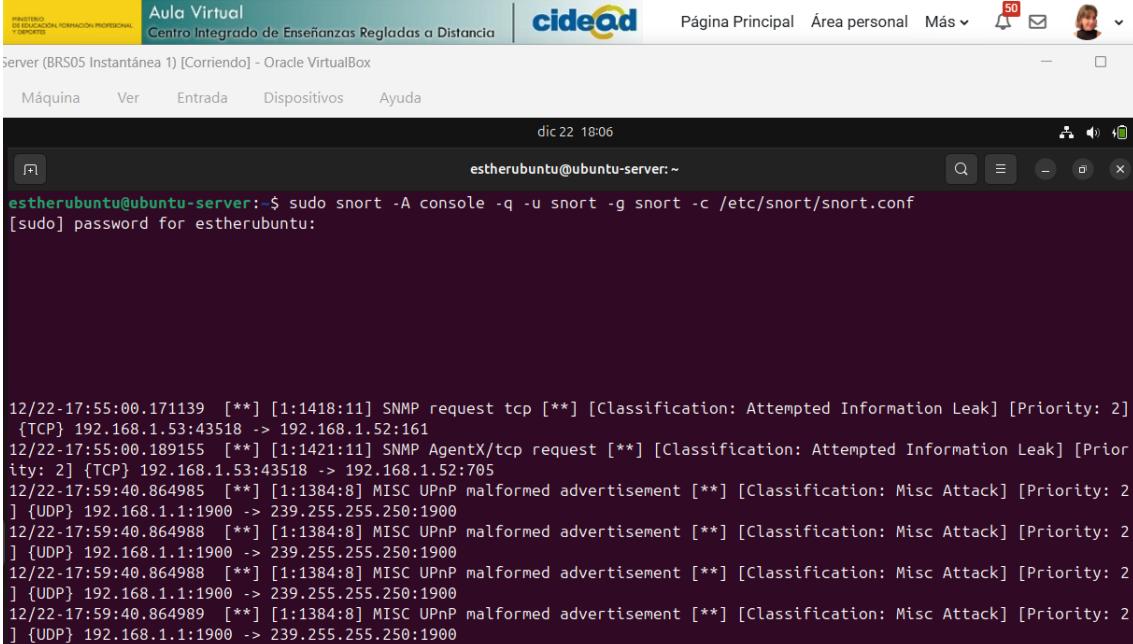
Según se indica en la columna de PORT STATE SERVICE VERSION, indica que el puerto 22, que es SSH, está abierto.



```
kali@kali:~$ 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
MAC Address: 08:00:27:C6:3C:FC (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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

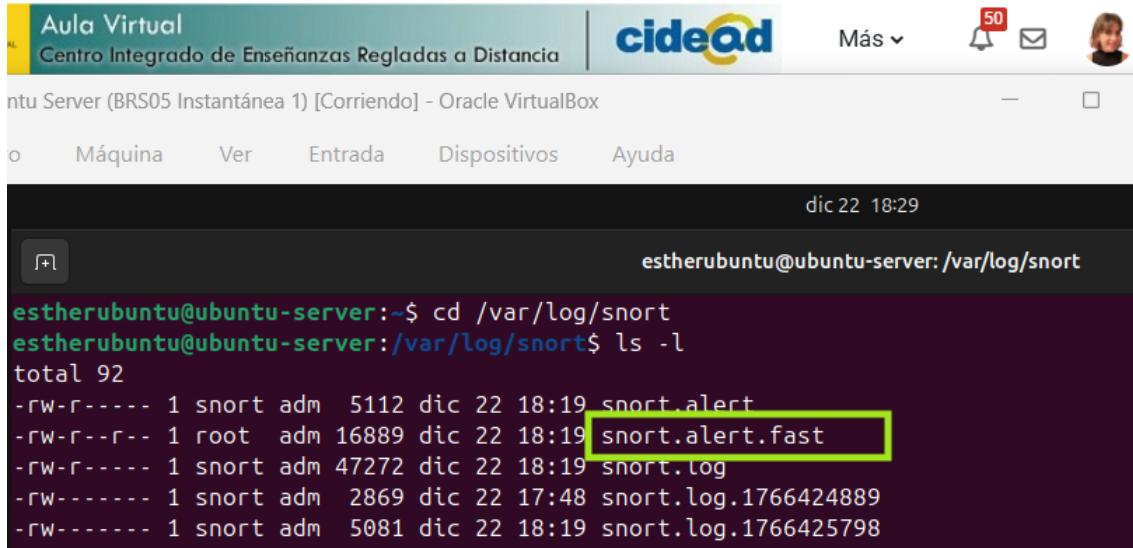
Ahora se vuelve a la máquina Ubuntu donde está desplegado Snort para saber dónde se almacenan los logs del IDS. Snort arroja estas alertas de seguridad en tiempo real generadas por el sistema de detección de intrusos.



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

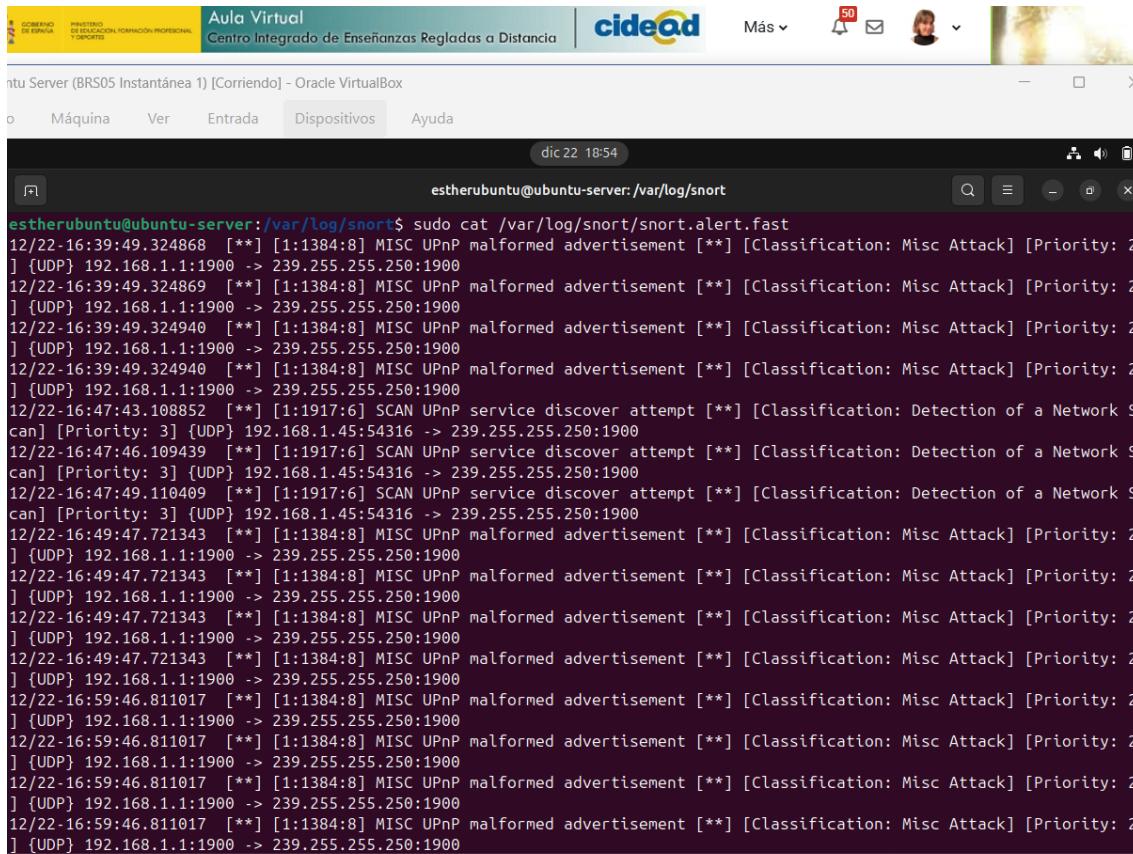
12/22-17:55:00.171139  [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2]
{TCP} 192.168.1.53:43518 -> 192.168.1.52:161
12/22-17:55:00.189155  [**] [1:1421:11] SNMP AgentX/tcp request [**] [Classification: Attempted Information Leak] [Prior
ity: 2] {TCP} 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
```

Sin embargo, es necesario acceder a la carpeta para ver dónde se almacenan todas estas alertas y su lectura sea más fácil para la persona administradora. De modo que se accede a la carpeta con el comando `cd /var/log/snort` y se ven los archivos que contiene con el comando `ls -l`. El archivo que nos interesa es `snort.alert.fast` que es el que Snort usa por defecto para escribir las alertas de manera legible.



```
estherubuntu@ubuntu-server:~$ cd /var/log/snort
estherubuntu@ubuntu-server:/var/log/snort$ ls -l
total 92
-rw-r----- 1 snort adm 5112 dic 22 18:19 snort.alert
-rw-r--r-- 1 root adm 16889 dic 22 18:19 snort.alert.fast
-rw-r----- 1 snort adm 47272 dic 22 18:19 snort.log
-rw----- 1 snort adm 2869 dic 22 17:48 snort.log.1766424889
-rw----- 1 snort adm 5081 dic 22 18:19 snort.log.1766425798
```

Finalmente, con el comando `sudo cat /var/log/snort/snort.alert.fast` se arroja el registro histórico de los logs de la herramienta. Este registro queda grabado en el disco duro permanentemente.



```
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
12/22-16:59:46.811017 [**] [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>