BASTIONADO DE REDES Y SISTEMAS

Tarea 5

ESTHER CARRILLO GÁLVEZ

Índice

Apartado 1: Filtrado MAC

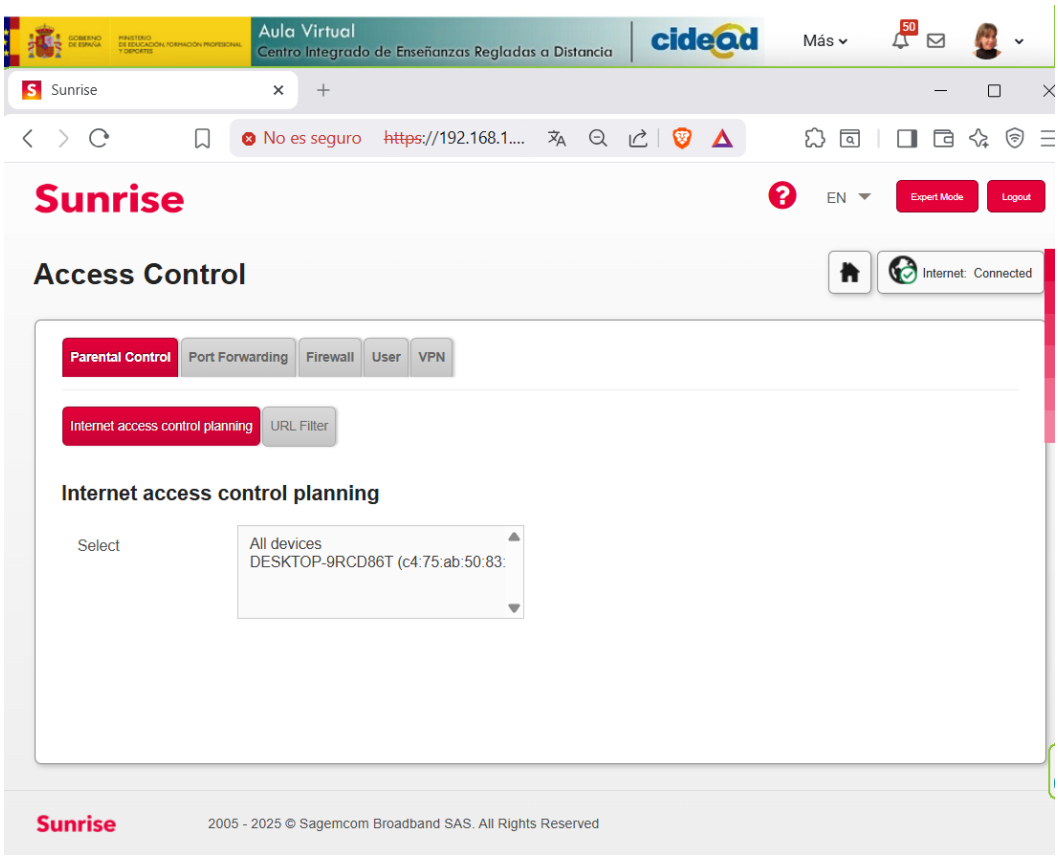
La alumna tendrá que configurar en la seguridad wifi de su router el filtrado MAC y añadir a la lista una MAC de un dispositivo que esté a su alcance (móvil, portátil, etc.). A continuación, desde una distribución Kali u otro linux, virtualizada o nativa, se hará pasar por el dispositivo autorizado modificando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

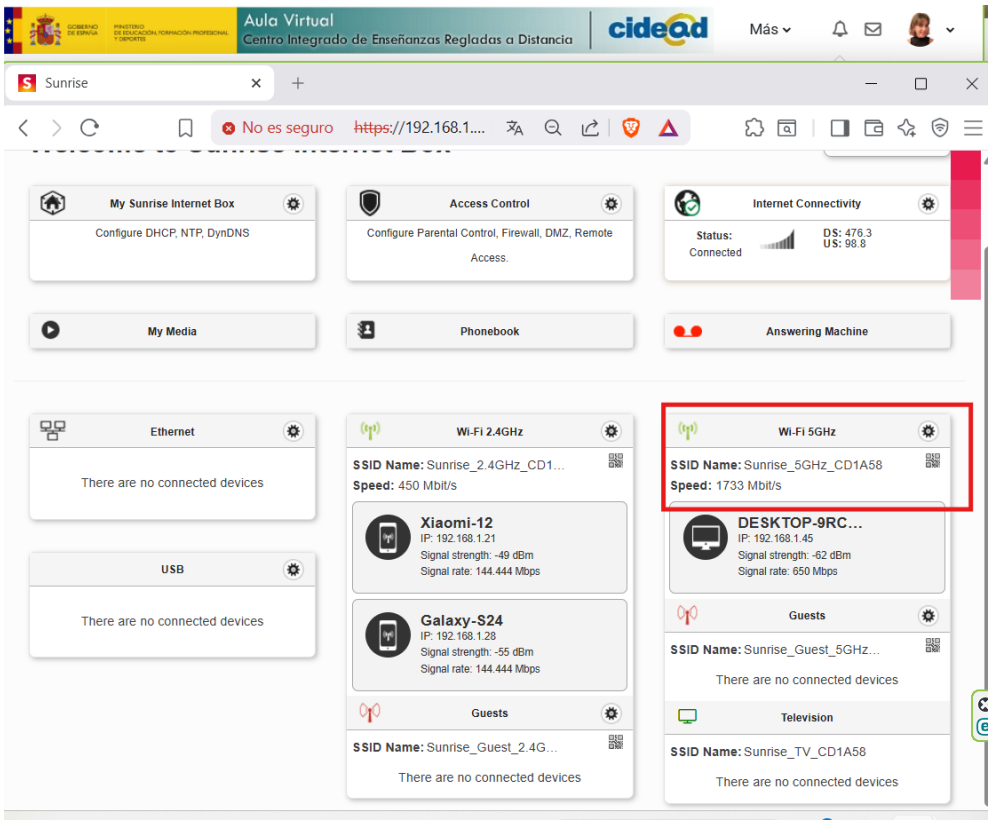
Para comenzar con la práctica, se accede a la configuración del router desde 192.168.1.1 y desde el modo *Expert Mode*, se selecciona *Access Control* donde se podrán ver las direcciones MAC registradas en el momento de la captura.

La dirección MAC existente:

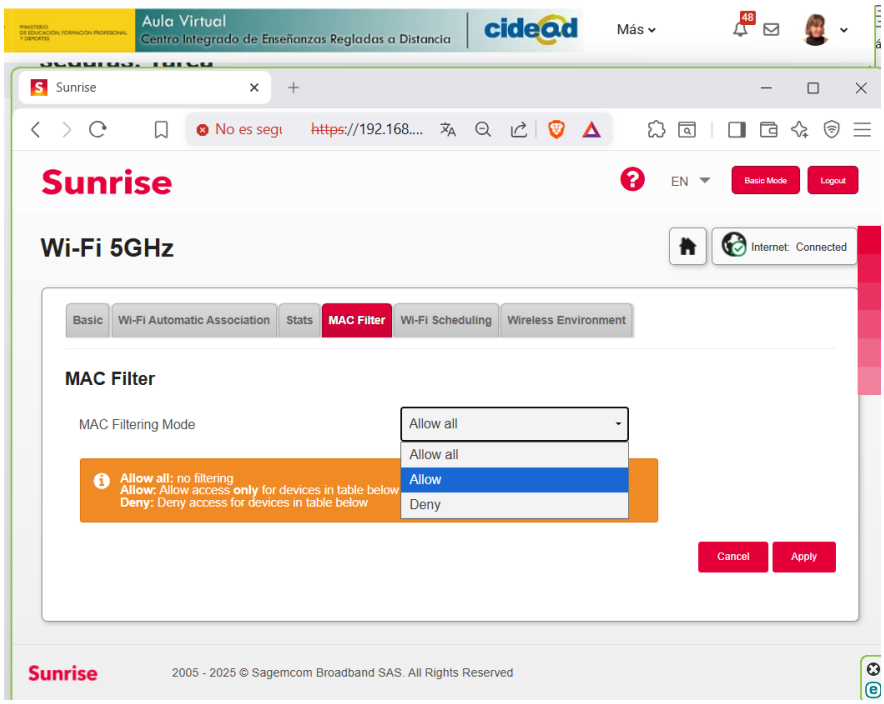
c4:75:ab:50:83:31 (para el portátil)



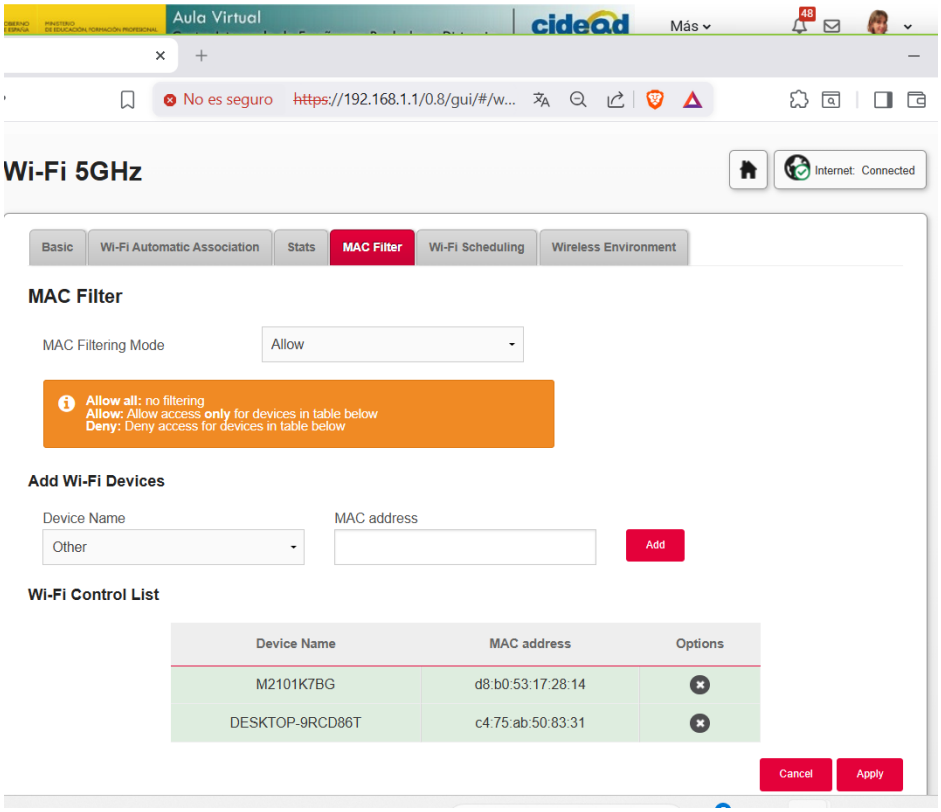
Se selecciona la red específica *Wifi 5GHz*.



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.

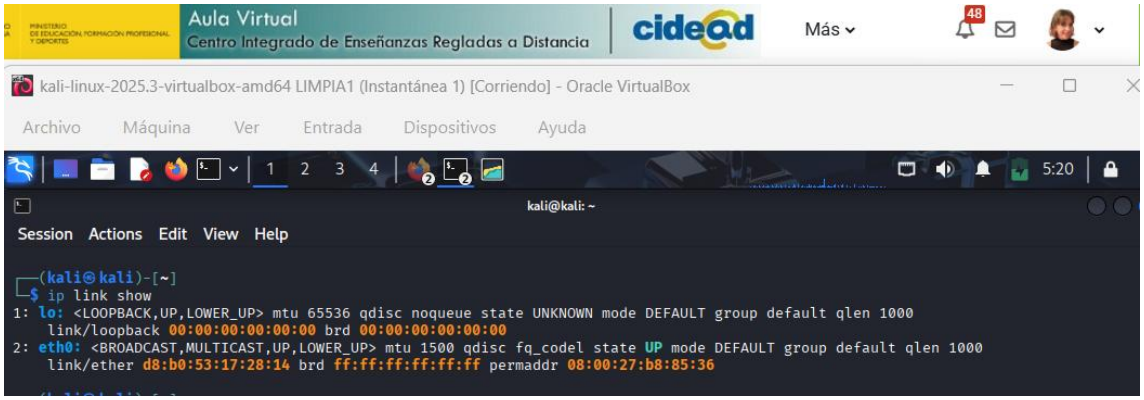


Desde la terminal de la máquina virtual Kali Linux, se procede al cambio de la dirección física por la MAC de mi móvil. En primer lugar, se apaga la tarjeta para cambiarle el nombre mediante el comando sudo ip link set dev eth0 down

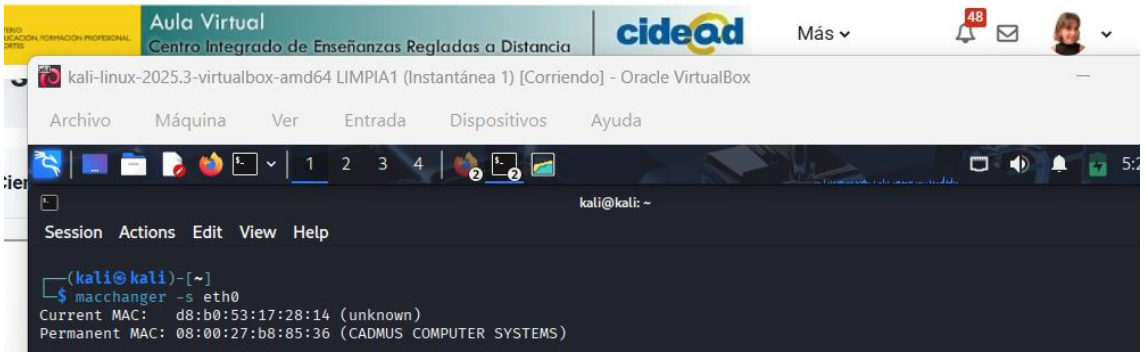
A continuación, con el comando sudo macchanger -m d8:b0:53:17:28:14 eth0, cambiar la MAC de la máquina Kali por la MAC del móvil.

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



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*.

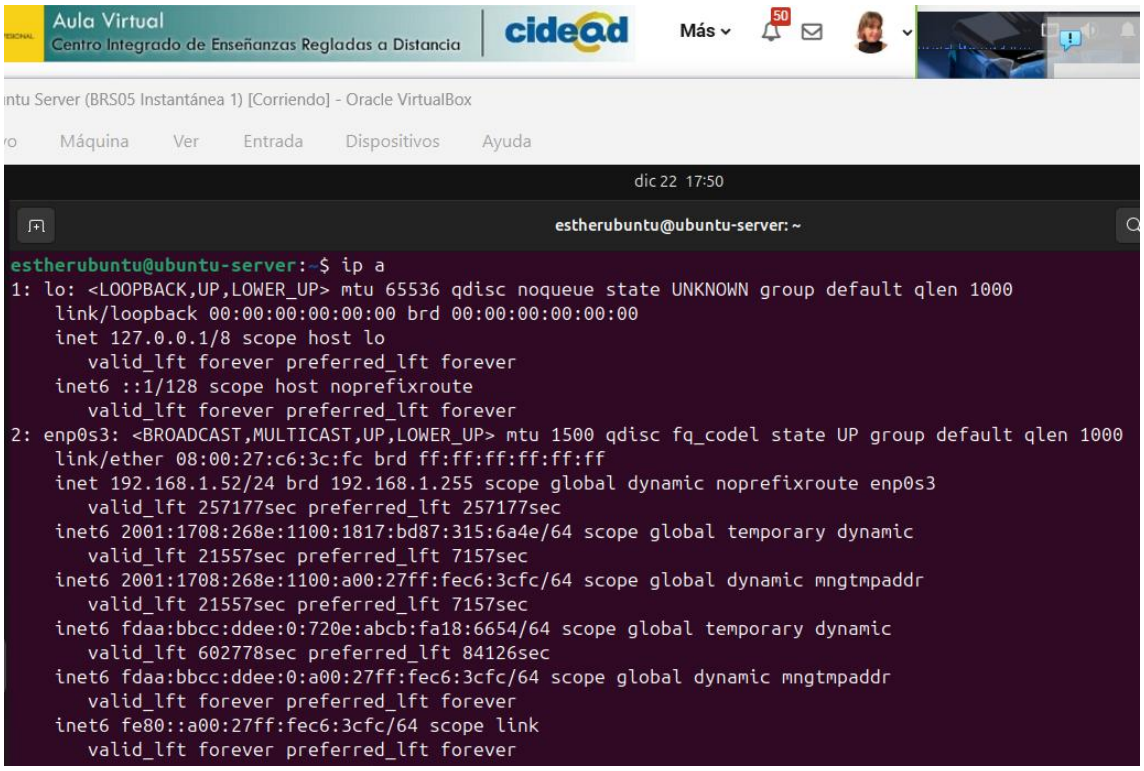


Apartado 2: Implementación IDS

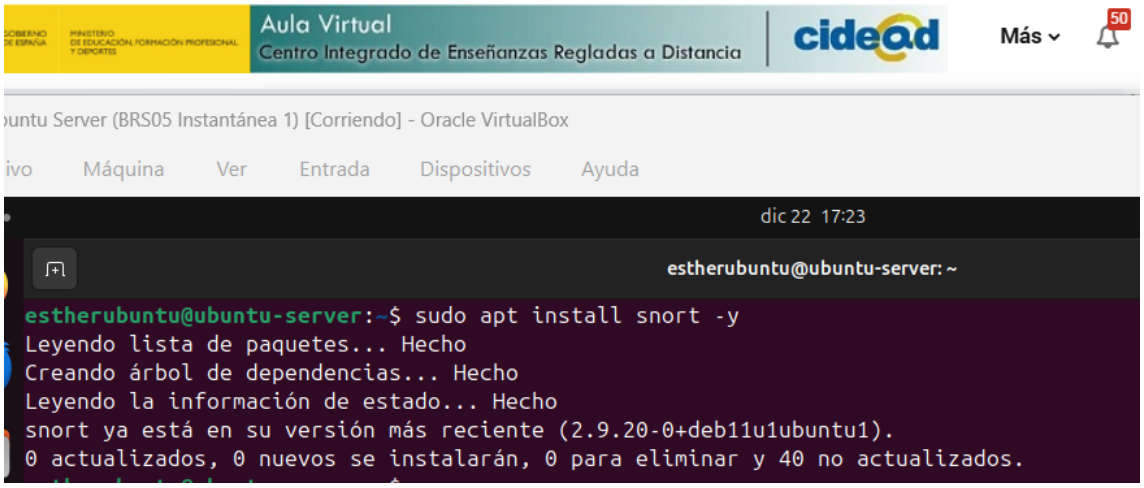
La alumna llevará a cabo un trabajo de investigación que consistirá en desplegar una solución de IDS opensource como SNORT y tras configurarla, realizará un escaneo con nmap que trate de identificar los servicios para ver cómo se comporta la herramienta. Para ello necesitará una máquina de ataque que 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.

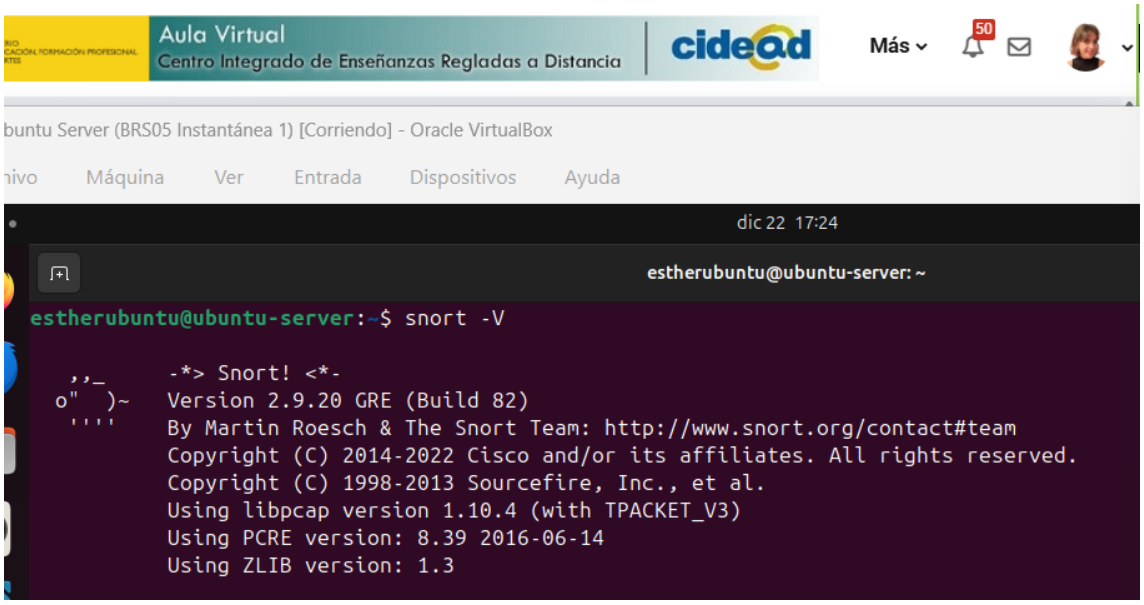
En primer lugar, con el comando ip a, se observa la ip para la máquina servidor Linux Ubuntu. La dirección IP es 192.168.1.52



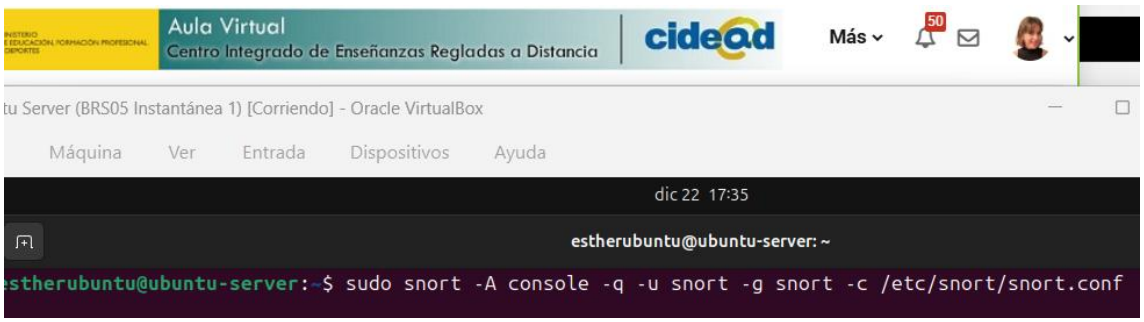
Se procede a la instalación de *Snort* con el comando sudo apt install snort -y



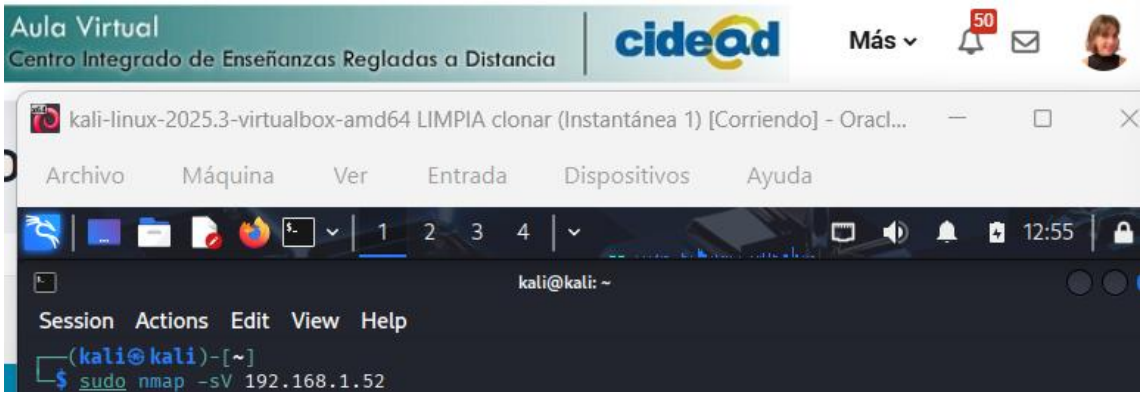
El comando snort -V comprueba que Snort se ha instalado correctamente y no tiene errores de configuración.



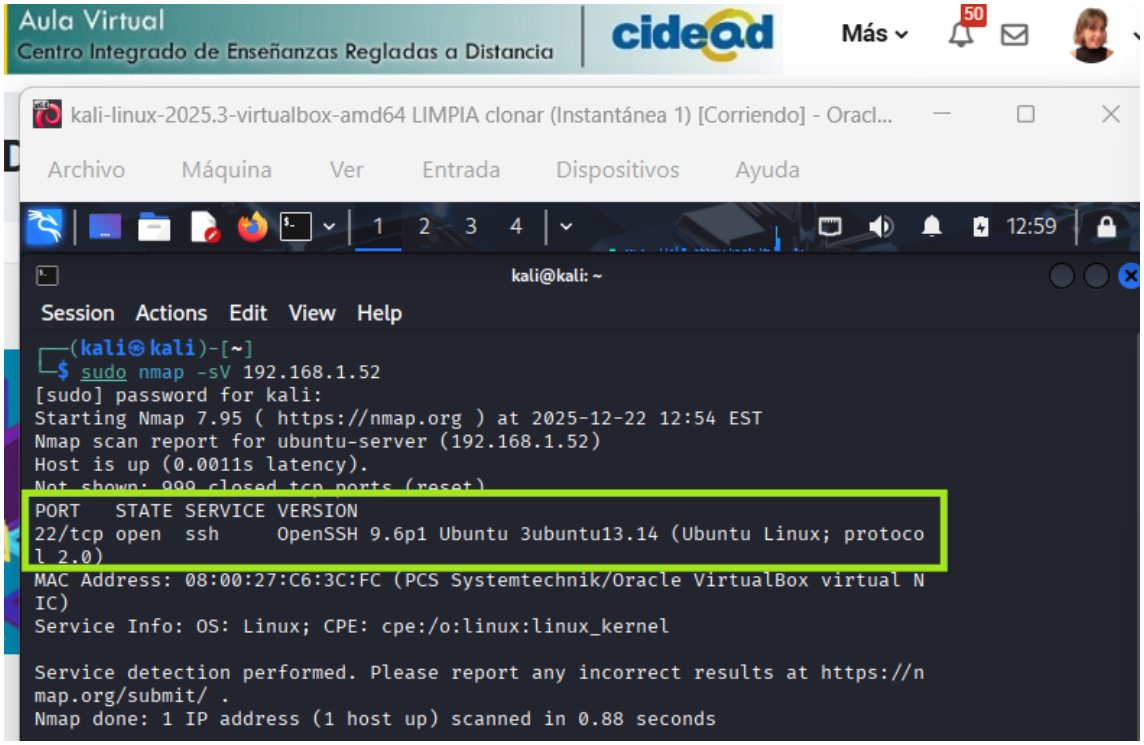
Se pone a Snort en modo para que escuche la red mediante el comando sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf.



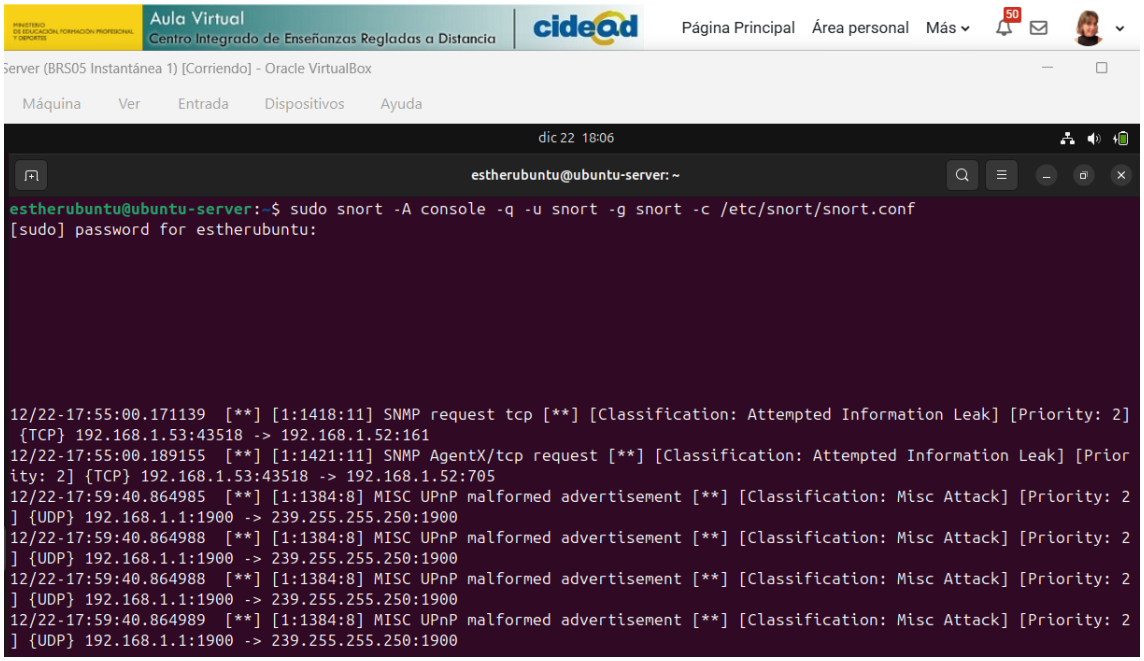
El siguiente paso es lanzar el ataque en Kali Linux con el comando sudo nmap -sV 192.168.1.52 que le dice a Kali que ejecute Nmap con privilegios de administrador (*s* viene de *Scan* y *V* de *Version Detection*) y realizar un escaneo de la red más profundo.



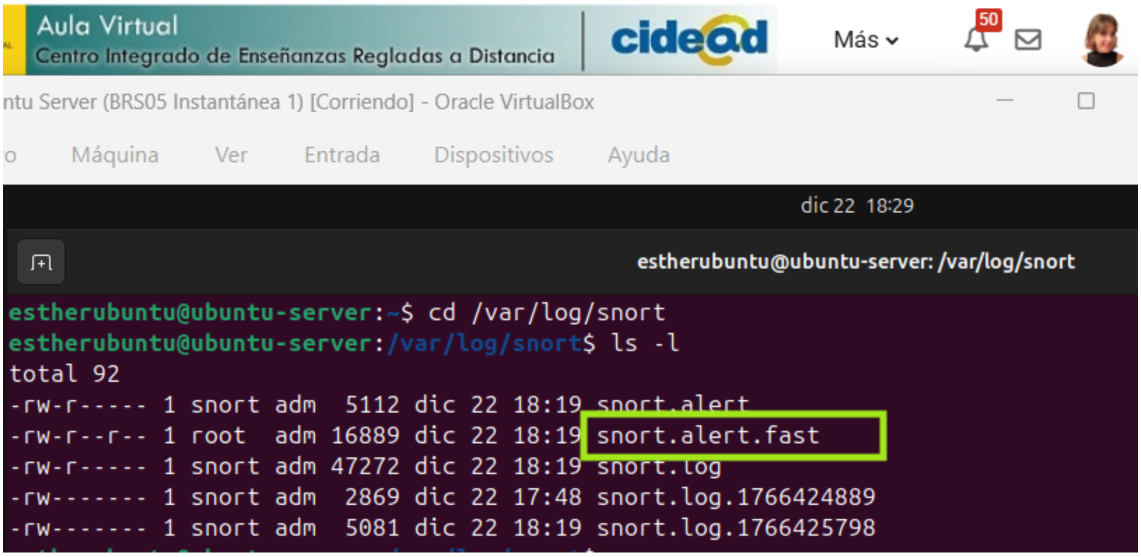
Según se indica en la columna de PORT STATE SERVICE VERSION, indica que el puerto 22, que es SSH, está abierto.



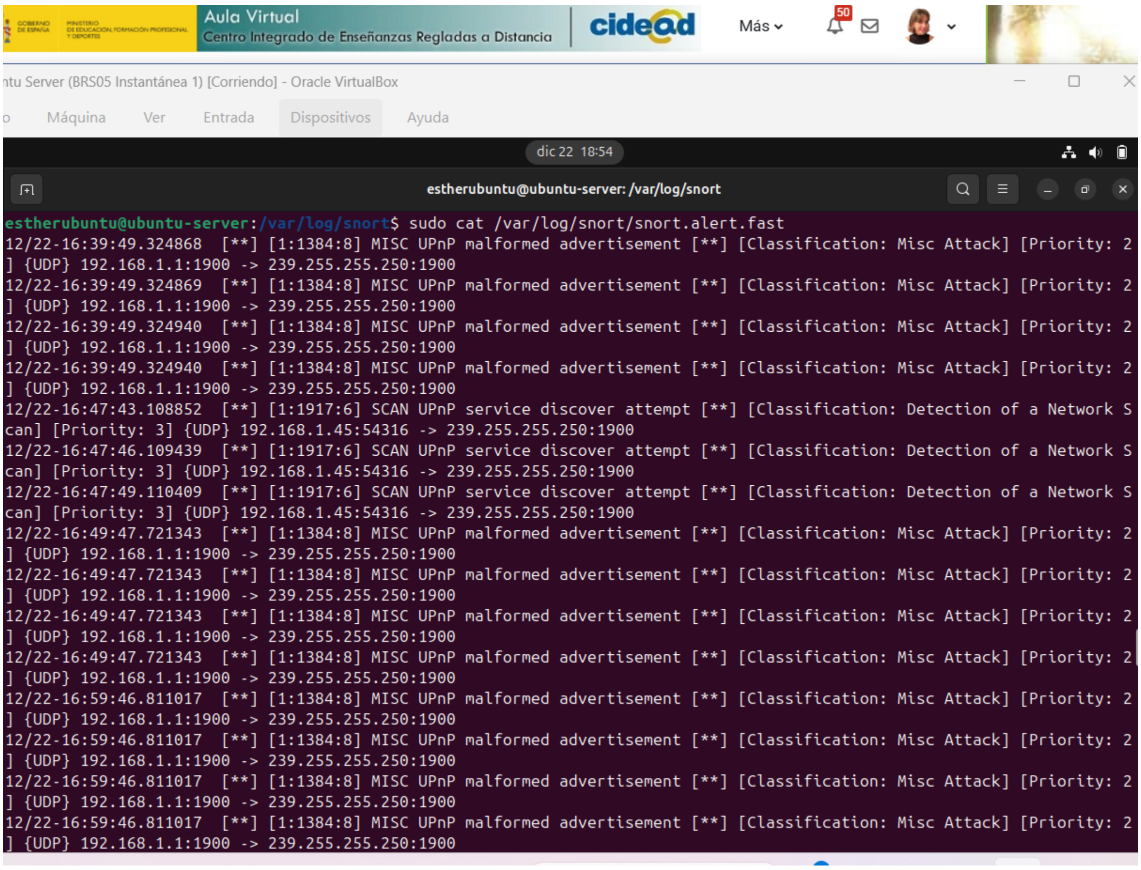
Ahora se vuelve a la máquina Ubuntu donde está desplegado Snort para saber dónde se almacenan los logs del IDS. Snort arroja estas alertas de seguridad en tiempo real generadas por el sistema de detección de intrusos.



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.



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.



Webgrafía

https://www.snort.org/

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

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