Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

# Bastionado de redes y sistemas

UD05. Diseño de redes de computadores seguras.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

## INDICE

## 1.- Descripción de la tarea.

### Caso práctico

A lo largo de esta unidad, el alumno tendrá que llevar a cabo dos prácticas relacionadas con los temas que se tratan en esta unidad.

**Wifi**

El alumno 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 otra linux, virtualizada o nativa, se hará pasar por el dispositivo autorizado modificando su MAC con la aplicación correspondiente y comprobando que se puede conectar. El alumno evidenciará con capturas que ha conseguido conectarse a la red wifi suplantando a un cliente.

**IDS**

El alumno llevará a cabo un trabajo de investigación que consistirá en desplegar una solución de IDS opensource como SNORT y tras configurarlo, 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, el alumno tendrá que saber dónde se almacenan los logs del IDS para que, una vez lanzado el ataque con nmap, pueda interpretar los resultados.

Recursos:

- ✓ Nmap: https://nmap.org/
- ✓ Snort: https://www.snort.org/downloads
- ✓ Adicionalmente puede instalar la interfaz gráfica snorby para tener un dashboard gráfico: https://github.com/Snorby/snorby

**¿Qué te pedimos que hagas?**

- ✓ **Apartado 1: seguridad wifi**

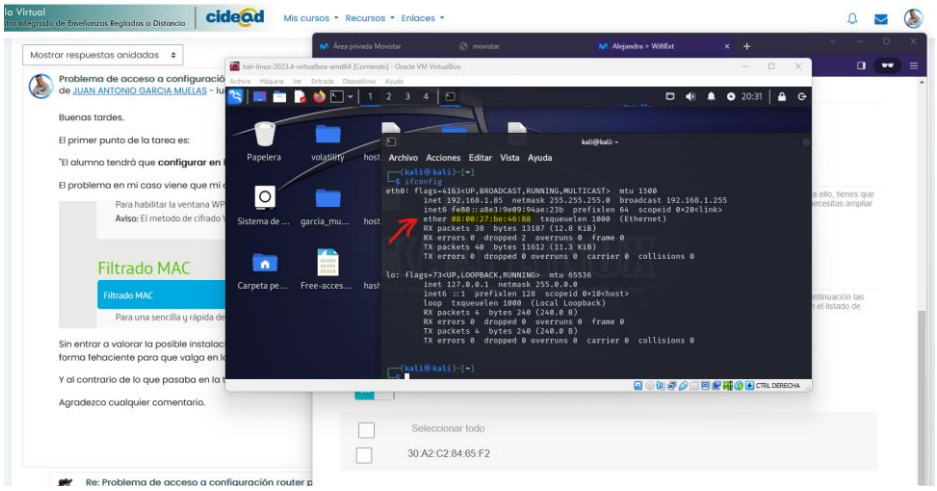
El alumno tendrá que configurar en la seguridad wifi de su router el filtrado MAC y añadir a la lista una MAC de un dispositivo que esté a su alcance (móvil, portátil, etc.). A continuación, desde una distribución Kali u otro linux, virtualizada o nativa, se hará pasar por el dispositivo autorizado modificando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

Para la realización de esta tarea voy a seguir utilizando las máquinas virtuales de Kali Linux creadas anteriormente.

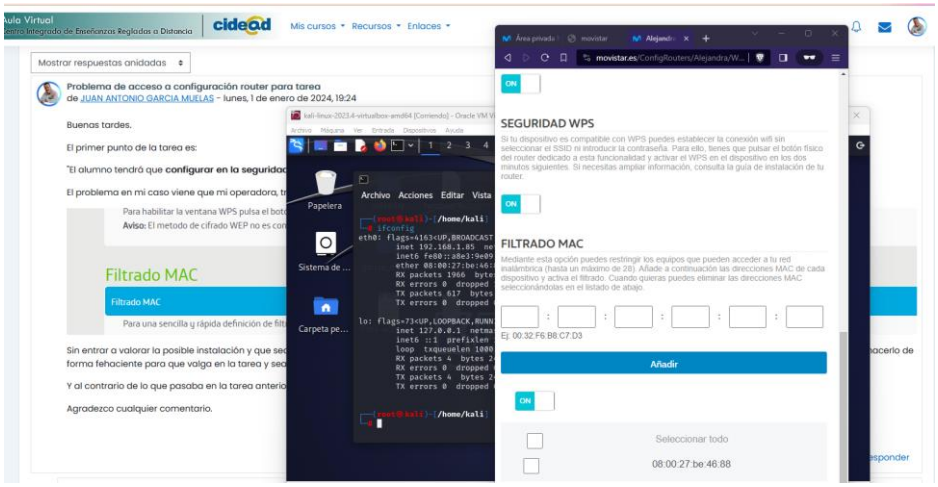
La MAC Wifi del dispositivo móvil que voy a utilizar es **`30:A2:C2.84:65:F2`**.

Abrimos una consola en Kali para comprobar la configuración de red de esta máquina.

La MAC de esta VM es **`08:00:27:be:56:88.`**




En el portal de configuración de la operadora, añadimos la MAC y dejamos activado el filtrado.

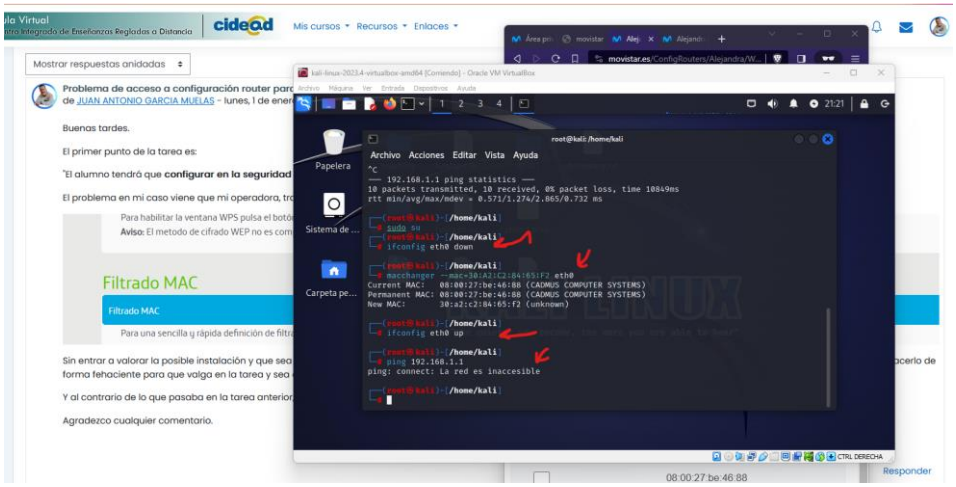



Procedo a utilizar macchanger para modificar la dirección MAC, para lo que debo deshabilitar la interfaz eth0.

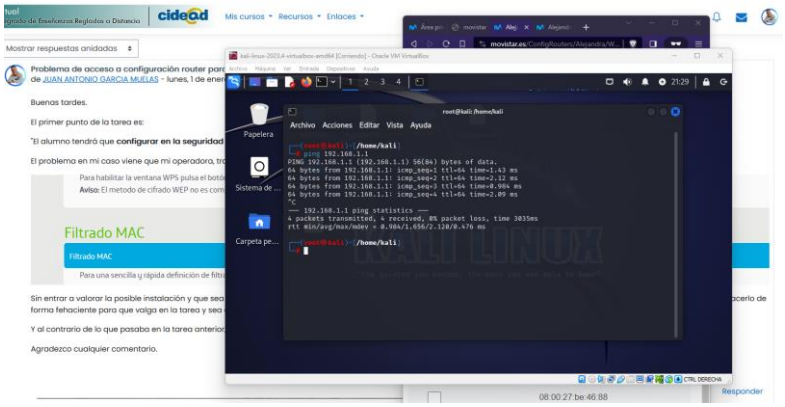
```
ifconfig eth0 down
macchanger --mac=30:A2:C3:84:65:F2 eth0
```

Tras modificarlo, volvemos a habilitar la interfaz e intentamos hacer ping

```
ifconfig eth0 up
ping 192.168.1.1
```



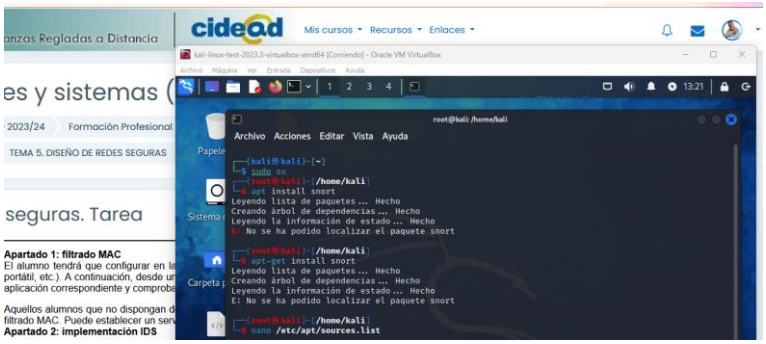
Desconecto de la red el móvil y volvemos a probar, para comprobar que funciona correctamente.



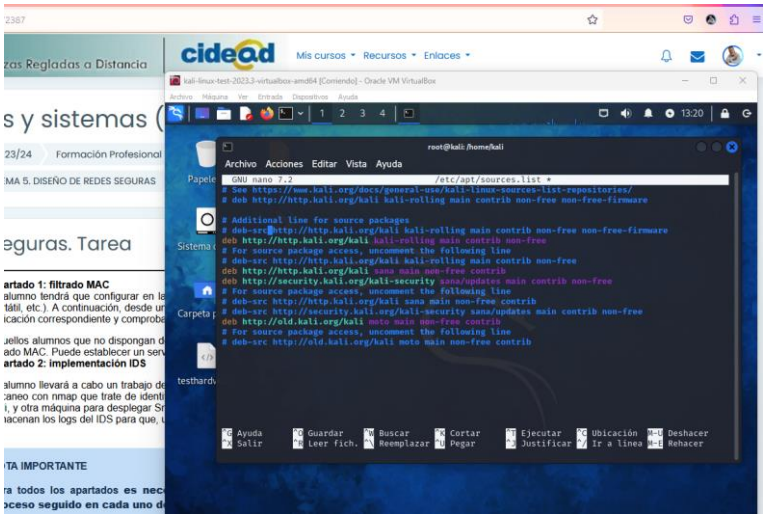
## ✓ Apartado 2: implementación IDS

El alumno 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, el alumno tendrá que saber dónde se almacenan los logs del IDS para que, una vez lanzado el ataque con nmap, pueda interpretar los resultados.

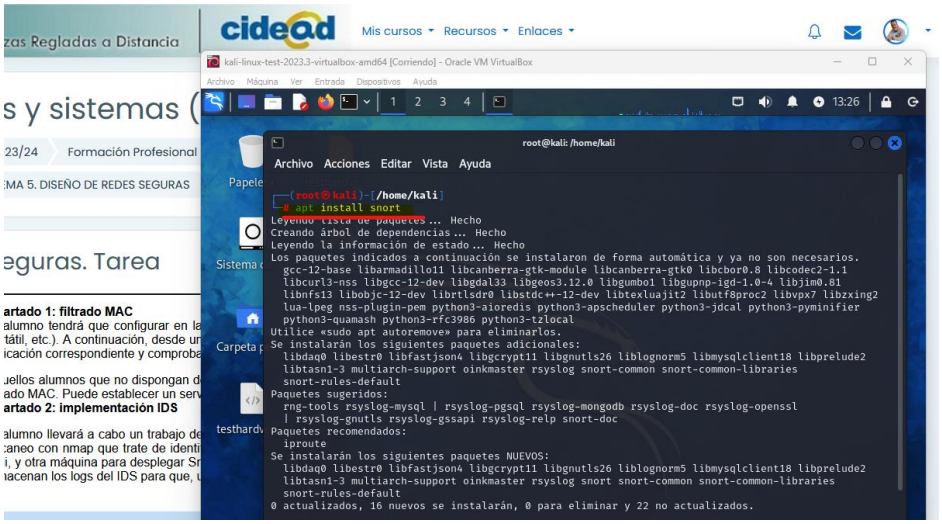
Intentamos la instalación de Snort en la primera de las máquinas Kali. Sin embargo, da problemas porque en este tipo de distribución no se incluyen esos paquetes por defecto.



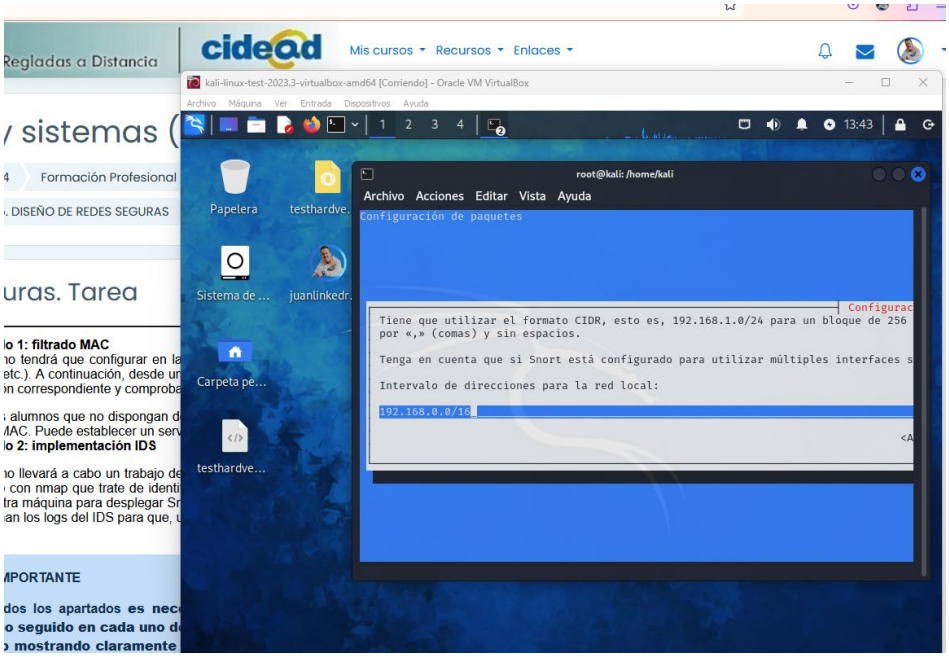
Debemos entonces añadirlos como fuentes.
**`nano /etc/apt/sources.list`**



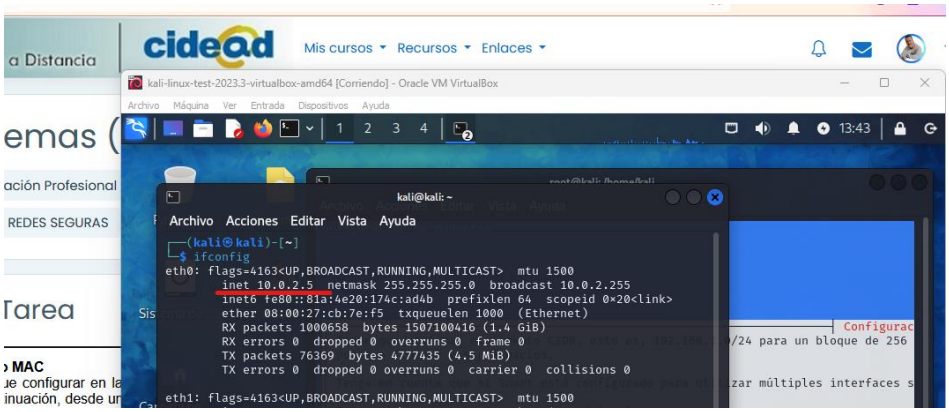
Realizamos un **`apt update`** y volvemos a intentar la instalación **`apt install snort`** o **`apt-get install snort`**

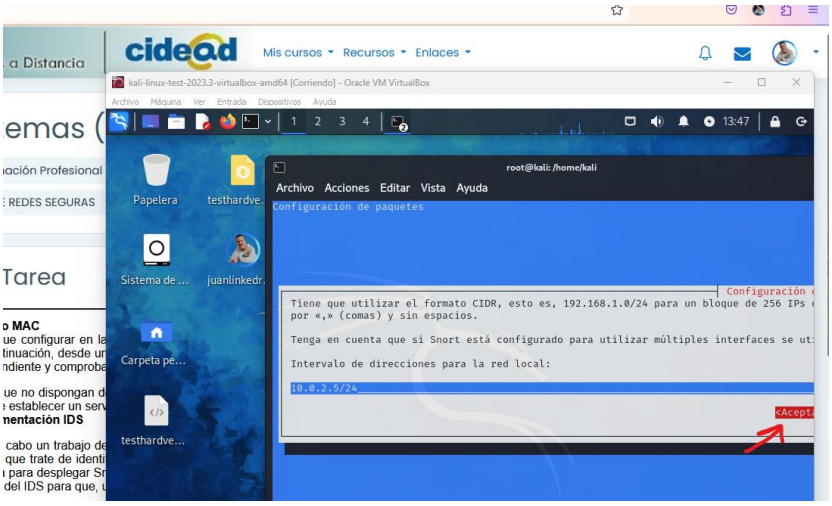



Si todo va correctamente, nos abrirá una ventana para indicarle la red local.

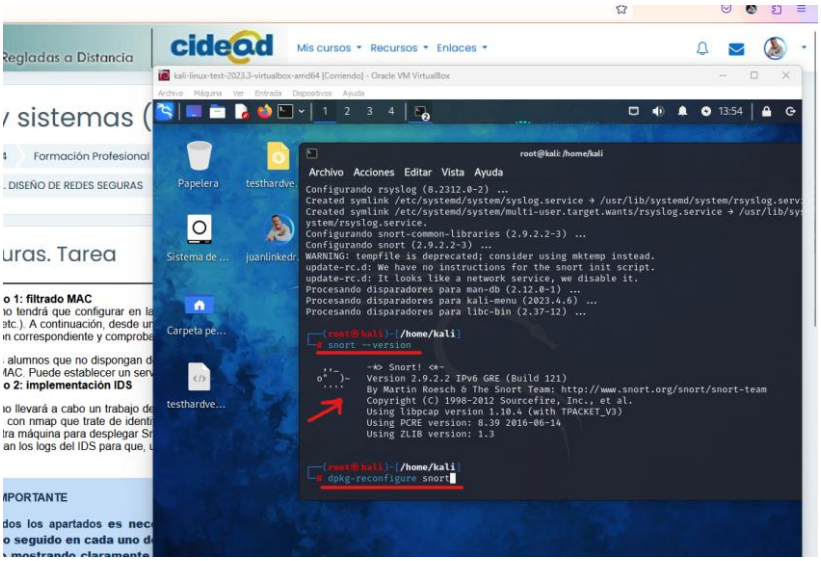



Comprobamos para añadir la IP correcta con **`ifconfig`**.

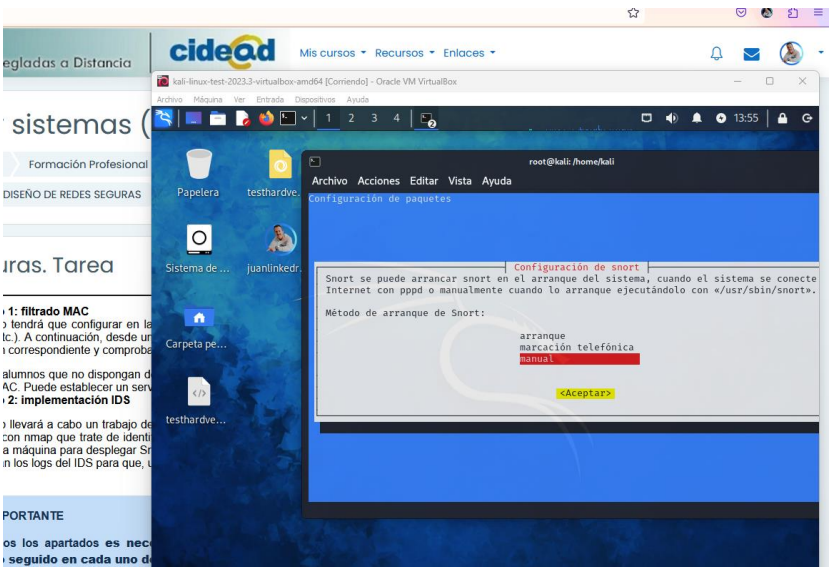




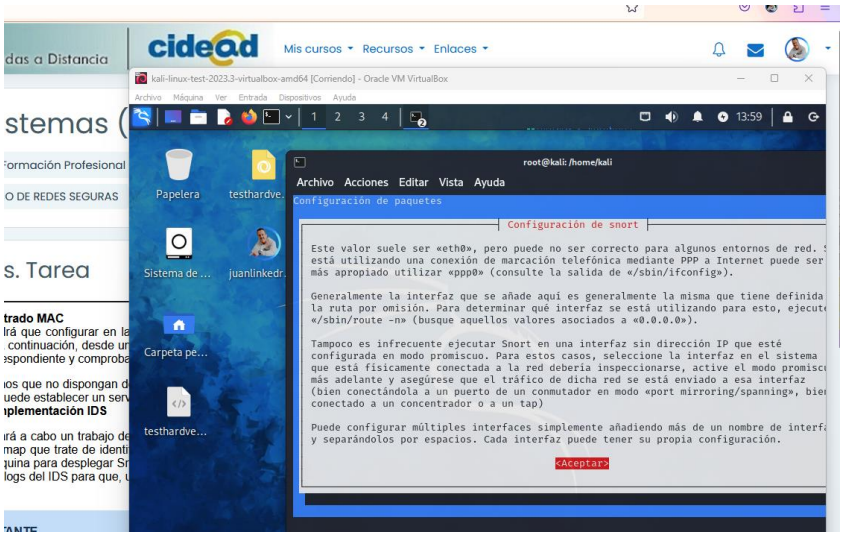

Tras aceptar, comprobamos la instalación **`snort --version`**
y comenzamos la configuración con **`dpkg-reconfigure snort`**

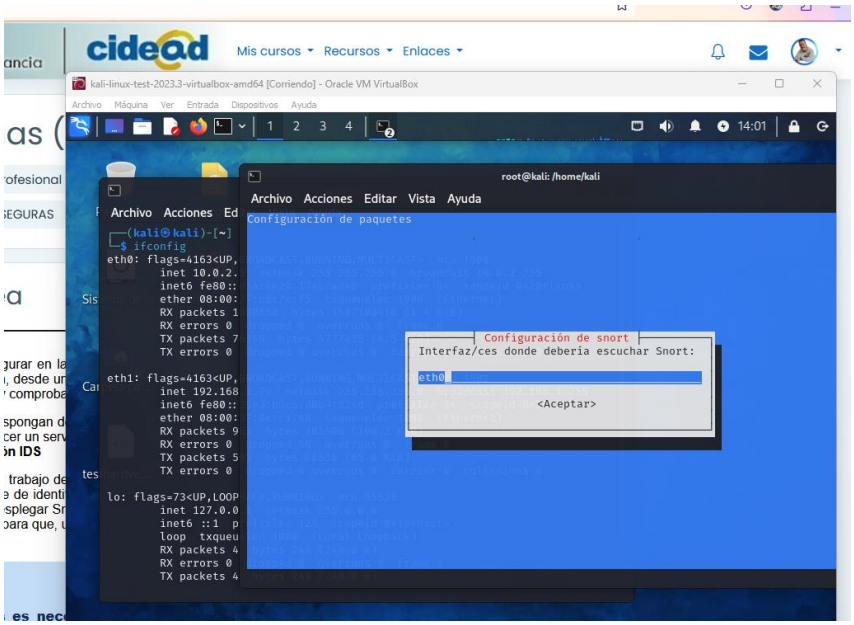



La primera ventana es para el modo de arranque, que lo dejaré en manual para poder controlar su uso.

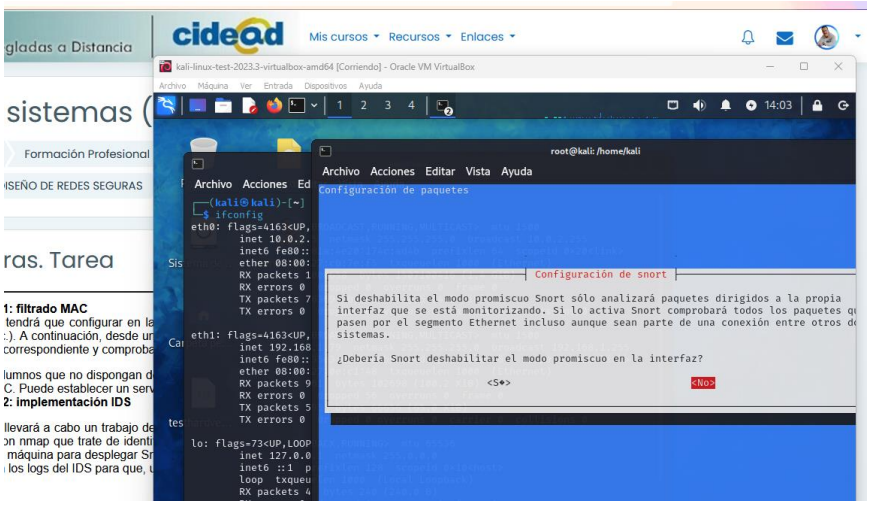


Las ventanas para la interfaz de red para la escucha, las pasamos aceptando.

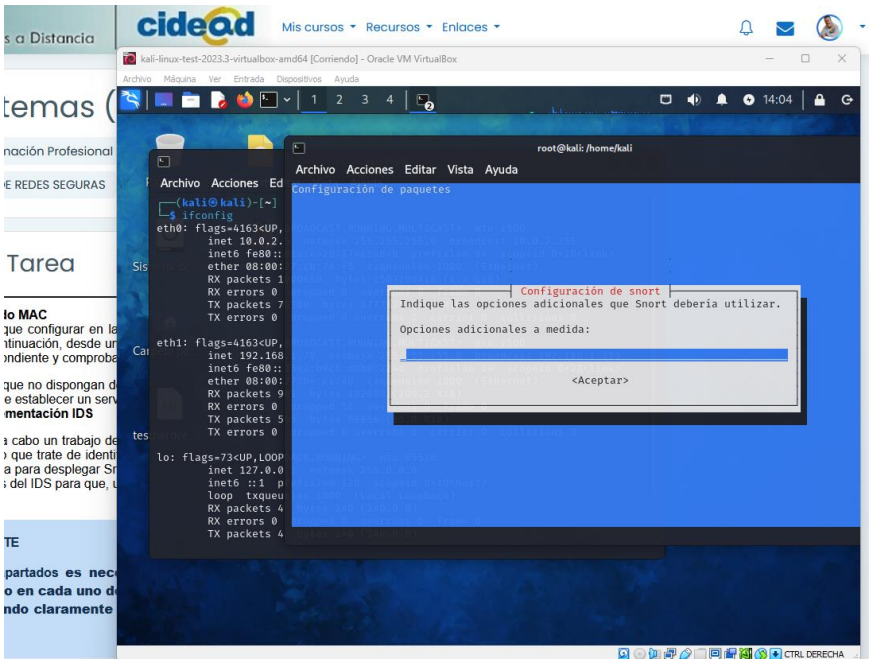


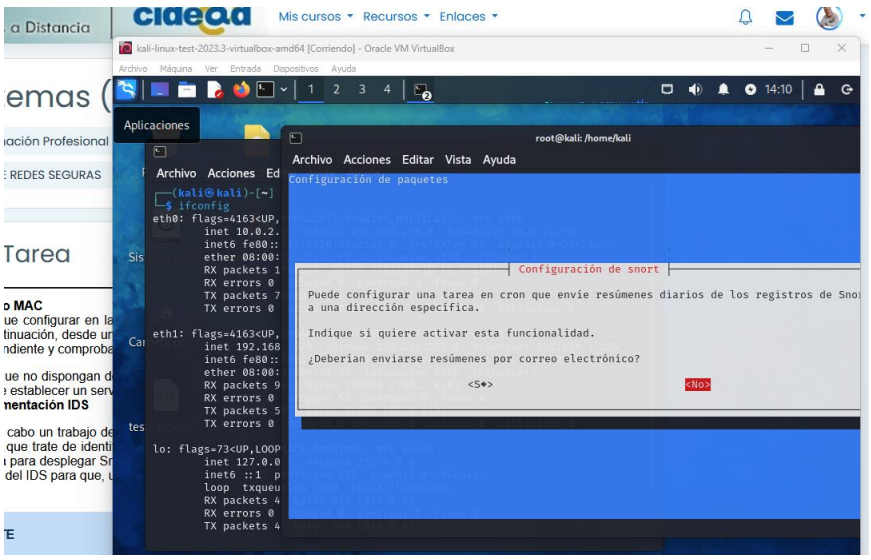




Nos puede volver a pedir el rango de IP y luego si queremos deshabilitar el modo promiscuo, que lo marcaremos con un **No**.

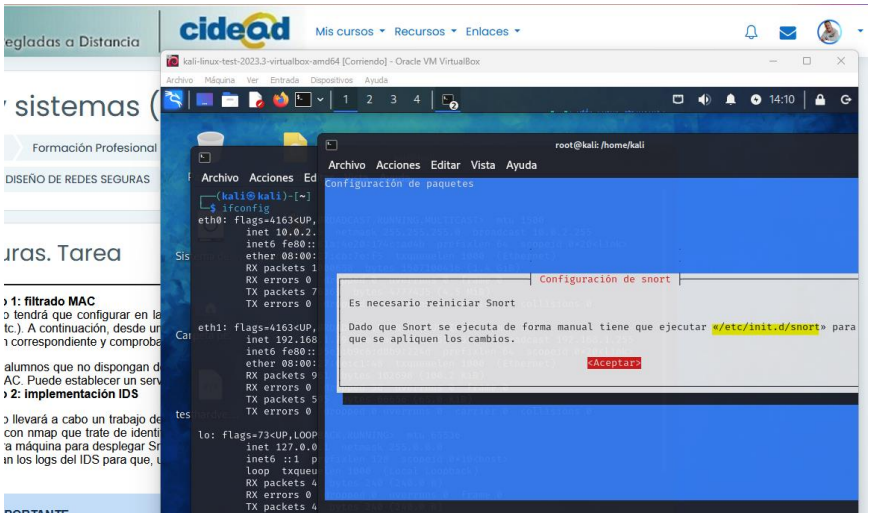


Las opciones adicionales las dejamos vacías y el envío de resúmenes lo marcamos con **No**.

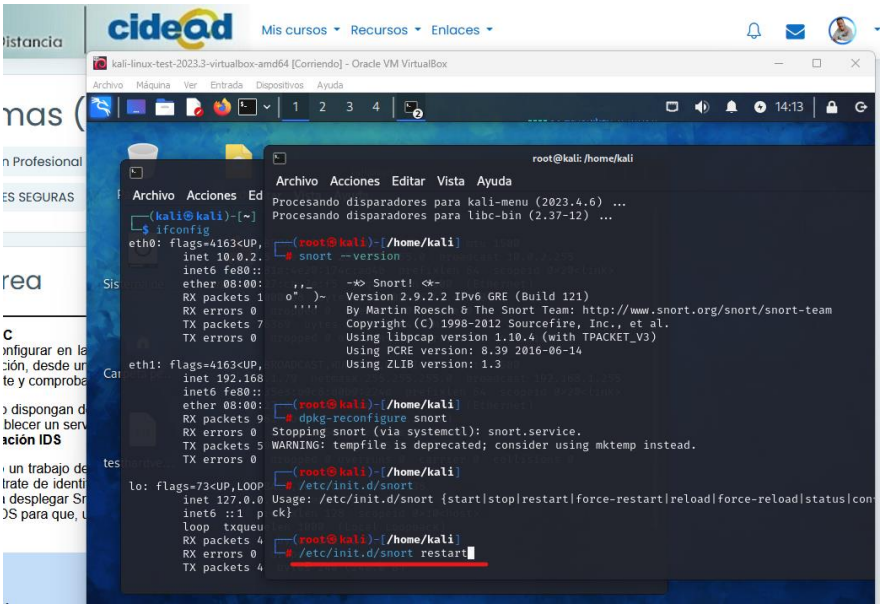



Nos pide reiniciar para aplicar la configuración.

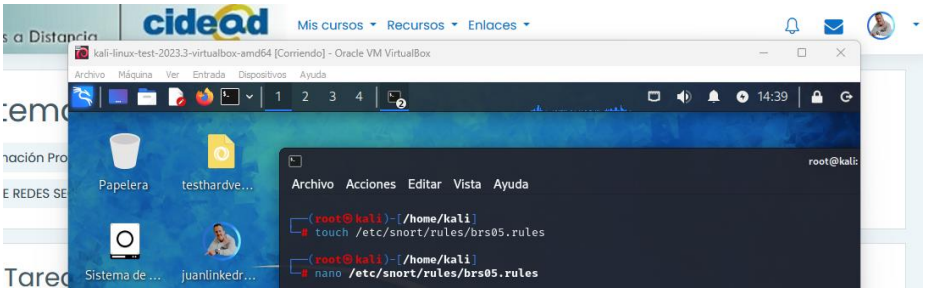


Podemos por curiosidad ver las opciones y tras comprobarlo: **`/etc/init.d/snort restart`**

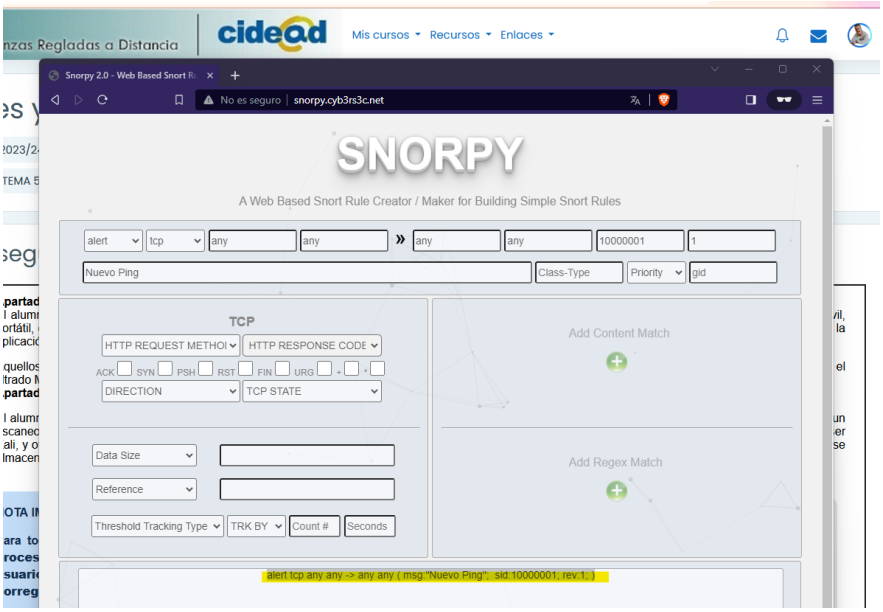



Necesitamos crear el archivo con las reglas que utilizará nmap.

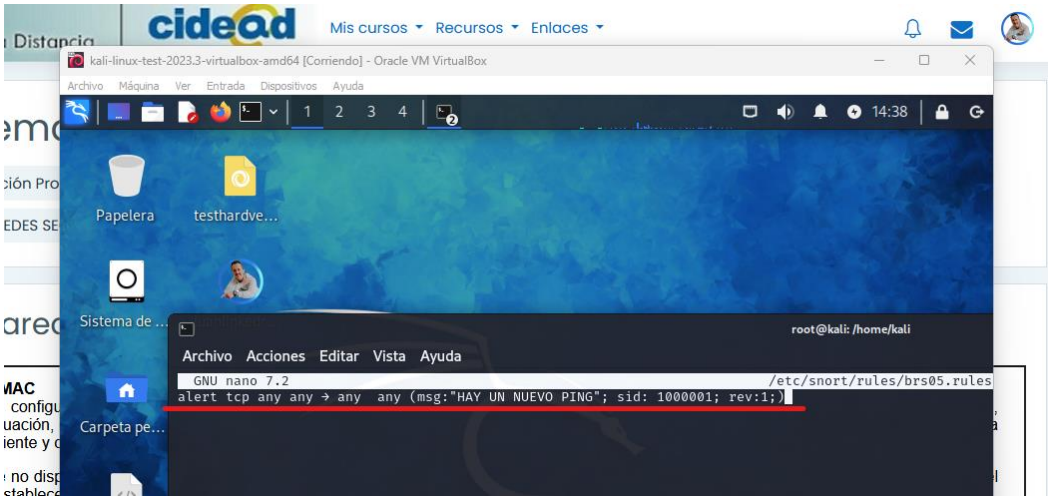
Lo creamos con **`touch /etc/snort/rules/brs05.rules`** y abrimos **`nano /etc/snort/rules/brs05.rules`**




El sitio **`snorpy.cyb3s3c.net`** nos ayuda con la tarea. En este caso, un **`alert`** para el protocolo **`TCP`**, desde y hacia cualquier red, con el mensaje **`"Nuevo Ping".`** El SID viene definido por como creamos la regla y en revisión:**`1`**.

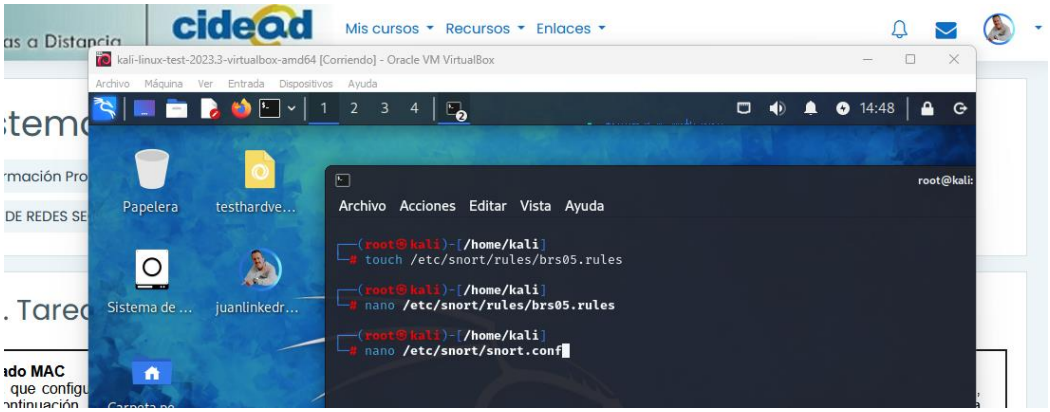


Lo copiamos en el archivo, y guardamos.

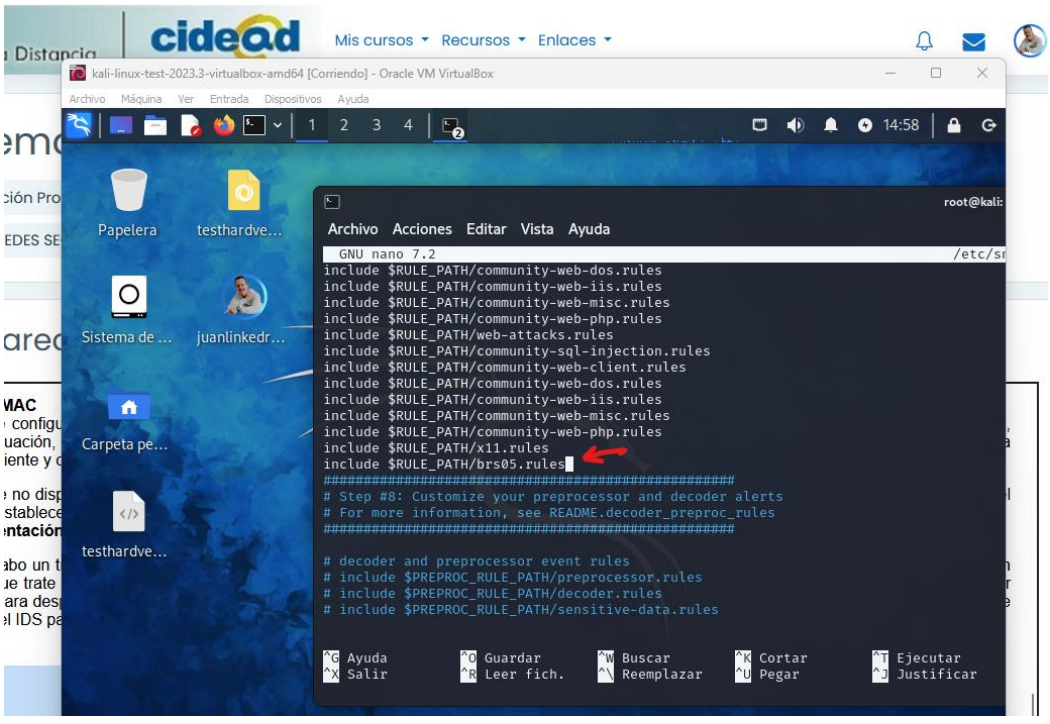



Vamos a añadir el nuevo archivo a la configuración.

**`nano /etc/snort/snort.conf`**

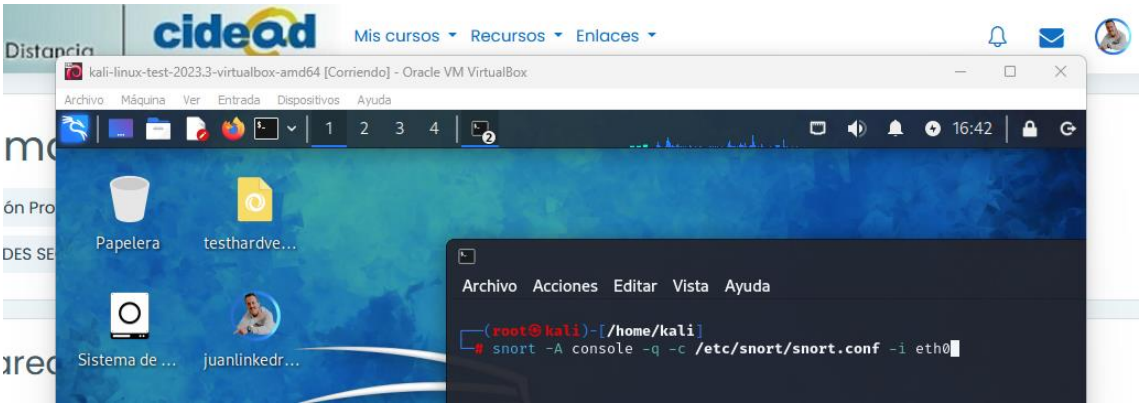



Lo añadimos al final de las reglas, con el mismo formato.



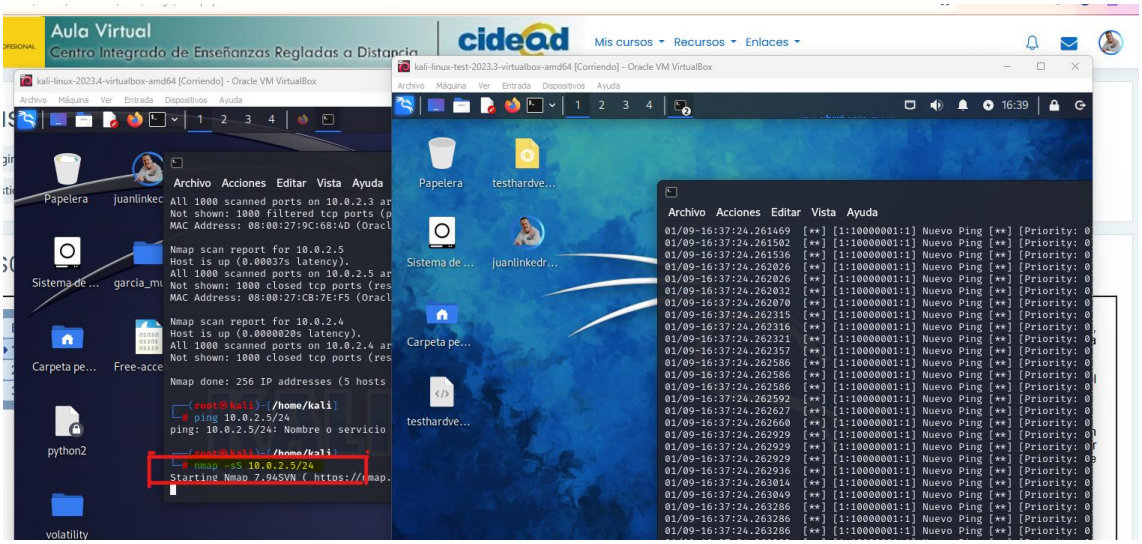
Iniciamos la consola de **snort**

**snort -A console -q -c /etc/snort/snort.conf -i eth0**

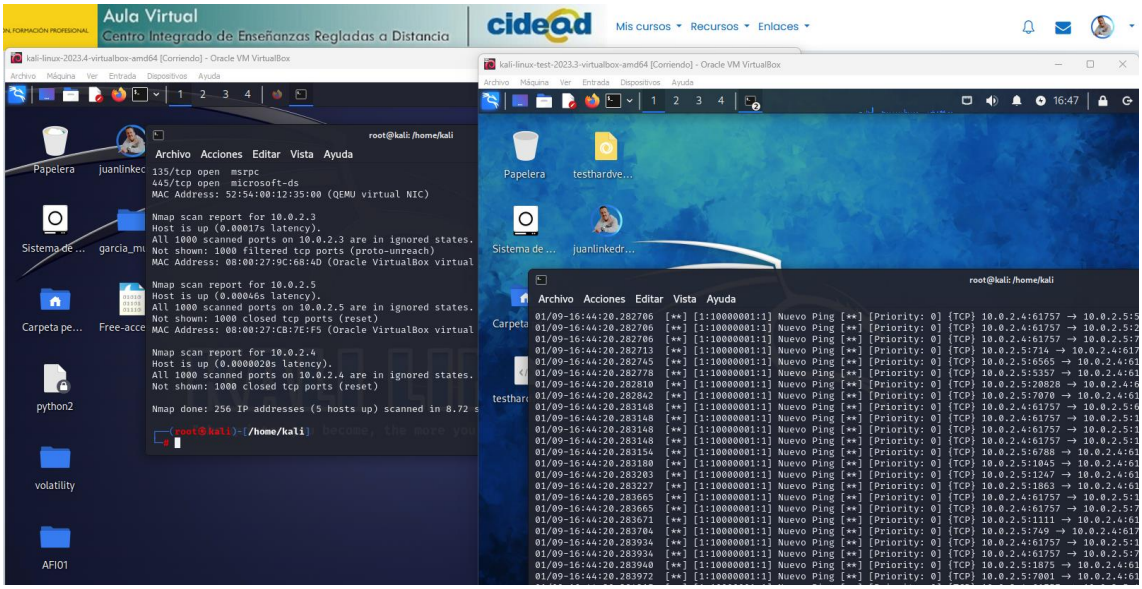



Abrimos una consola en la otra máquina Kali y con **nmap** comprobamos el funcionamiento de SNORT.

**nmap -sS 10.0.2.5/24**




Vemos que la respuesta es la esperada.



## Webgrafía.

https://www.movistar.es/particulares/internet/adsl-fibra-optica/clientes/configuracion-routers-portal-alejandra/

https://www.snort.org/

https://nmap.org/man/es/

https://www.youtube.com/watch?v=nYXWsrXPafA

https://www.youtube.com/watch?v=cD-DoKLzq2s