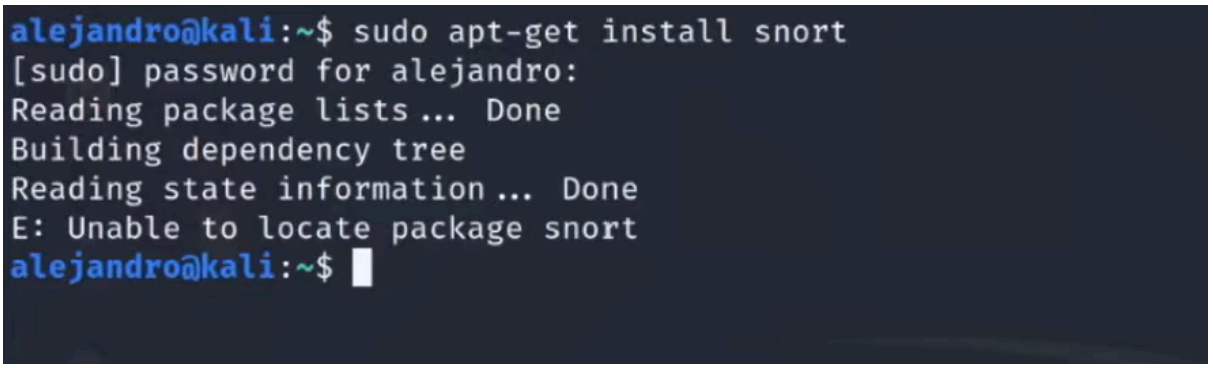
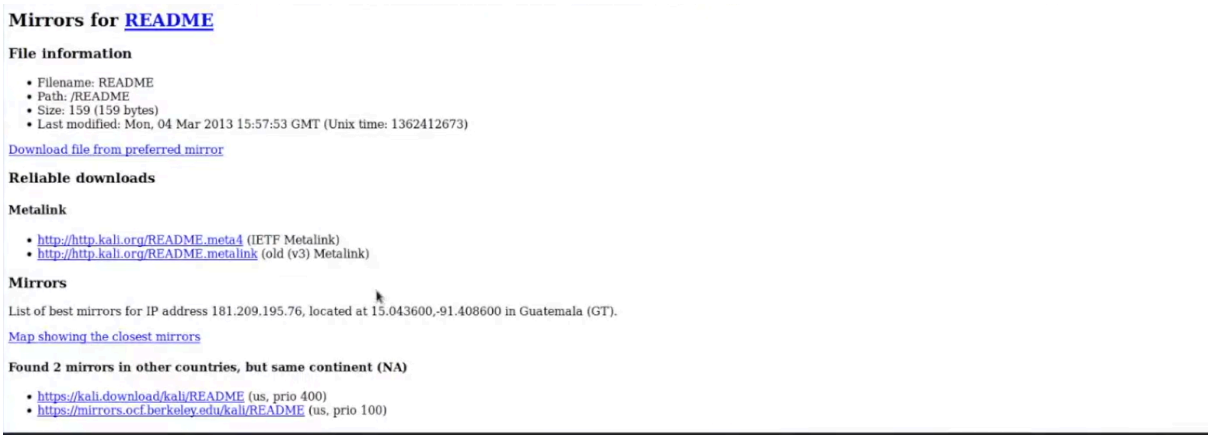
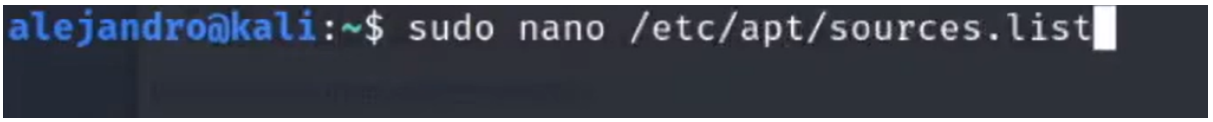
MONTANDO NIDS CON SNORT.

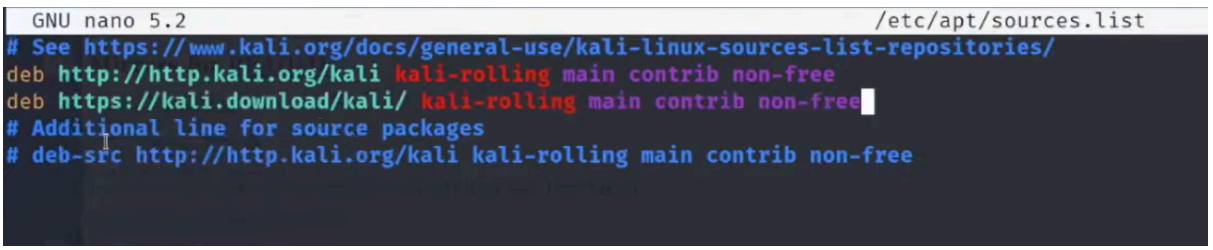
1.INSTALAR SNORT



Antes de instalar snort es necesario actualizar las fuentes de kali

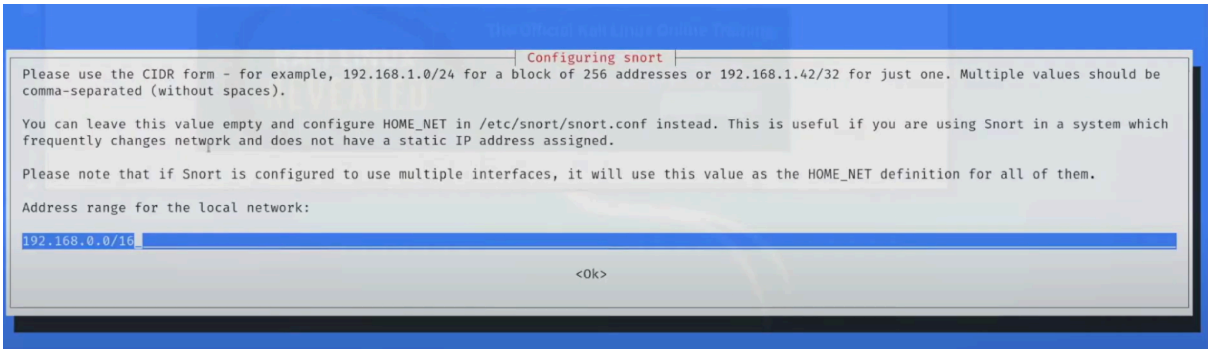






Ahora ya es posible instalar snort

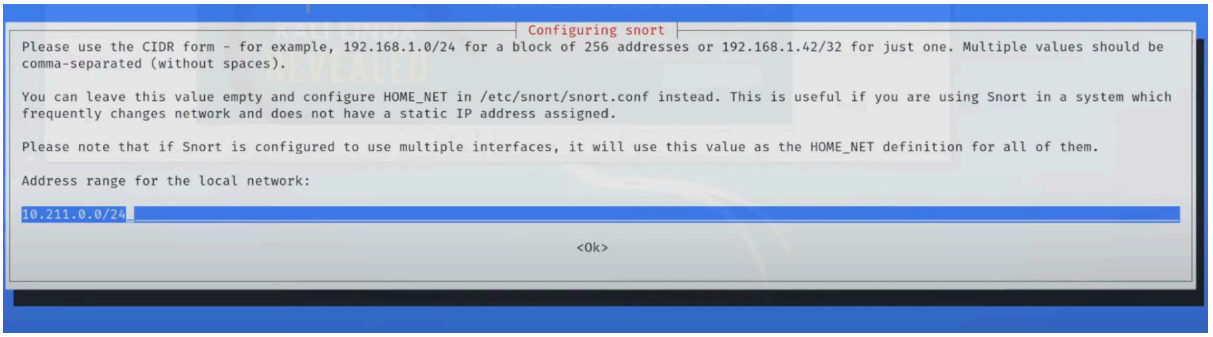
```
alejandro@kali:~$ sudo apt-get install snort
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
E: Unable to locate package snort
alejandro@kali:~$ sudo apt-get update
Get:2 https://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:3 https://kali.download/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
Get:4 https://kali.download/kali kali-rolling/contrib amd64 Packages [109 kB]
Get:5 https://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Packages [17.7 MB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Packages [109 kB]
Get:8 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Fetched 36.1 MB in 5s (7,102 kB/s)
Reading package lists ... Done
alejandro@kali:~$ sudo apt-get install snort
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libcdio18 libcfitsio8 libmpdec2 libobjc-9-dev libpoppler82 libprotobuf22 libtsk13 libx264-155 libx264-159 openjdk-
  python3-grequests python3-mimeparse python3-mimerender
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdaq2 libdumbnet1 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
```



Para añadir el address range tenemos que comprobar cuál es nuestra red interna y máscara de red

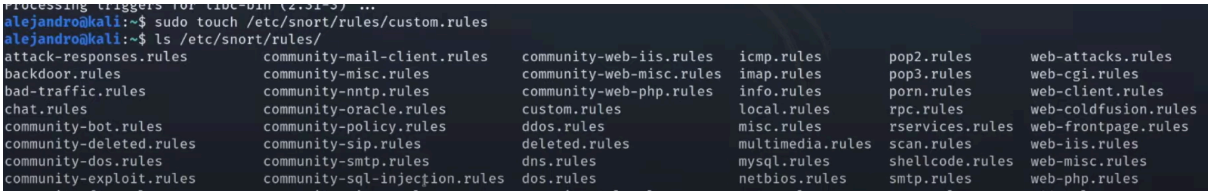
```
alejandro@kali:~$ sudo ifconfig
[sudo] password for alejandro:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.211.55.12  netmask 255.255.255.0  broadcast 10.211.55.255
        inet6 fdb2:2c26:f4e4:0:21c:42ff:fe5b:df7d  prefixlen 64  scopeid 0x0<global>
        inet6 fdb2:2c26:f4e4:0:984c:9ff5:8e95:704b  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::21c:42ff:fe5b:df7d  prefixlen 64  scopeid 0x20<link>
        ether 00:1c:42:5b:df:7d  txqueuelen 1000  (Ethernet)
        RX packets 41515  bytes 44594971 (42.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 19905  bytes 1757411 (1.6 MiB)
        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 3142  bytes 128568 (125.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3142  bytes 128568 (125.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Como se puede observar nuestra red interna es 10.211.55.12 y la máscara de red es 255.255.255.0. Por tanto añadimos 10.211.0.0/24

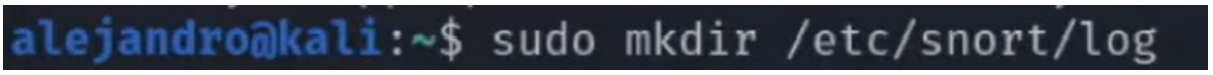


2. CONFIGURACIÓN DE SNORT Y CREACIÓN DE REGLAS

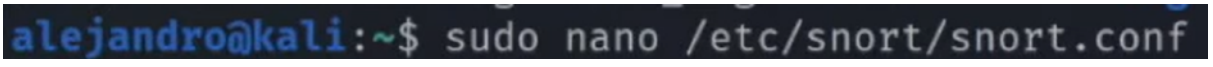
Creamos archivo custom.rules en la carpeta rules. Visualizamos también la carpeta rules para ver todas las reglas que vienen ya configuradas por defecto en snort



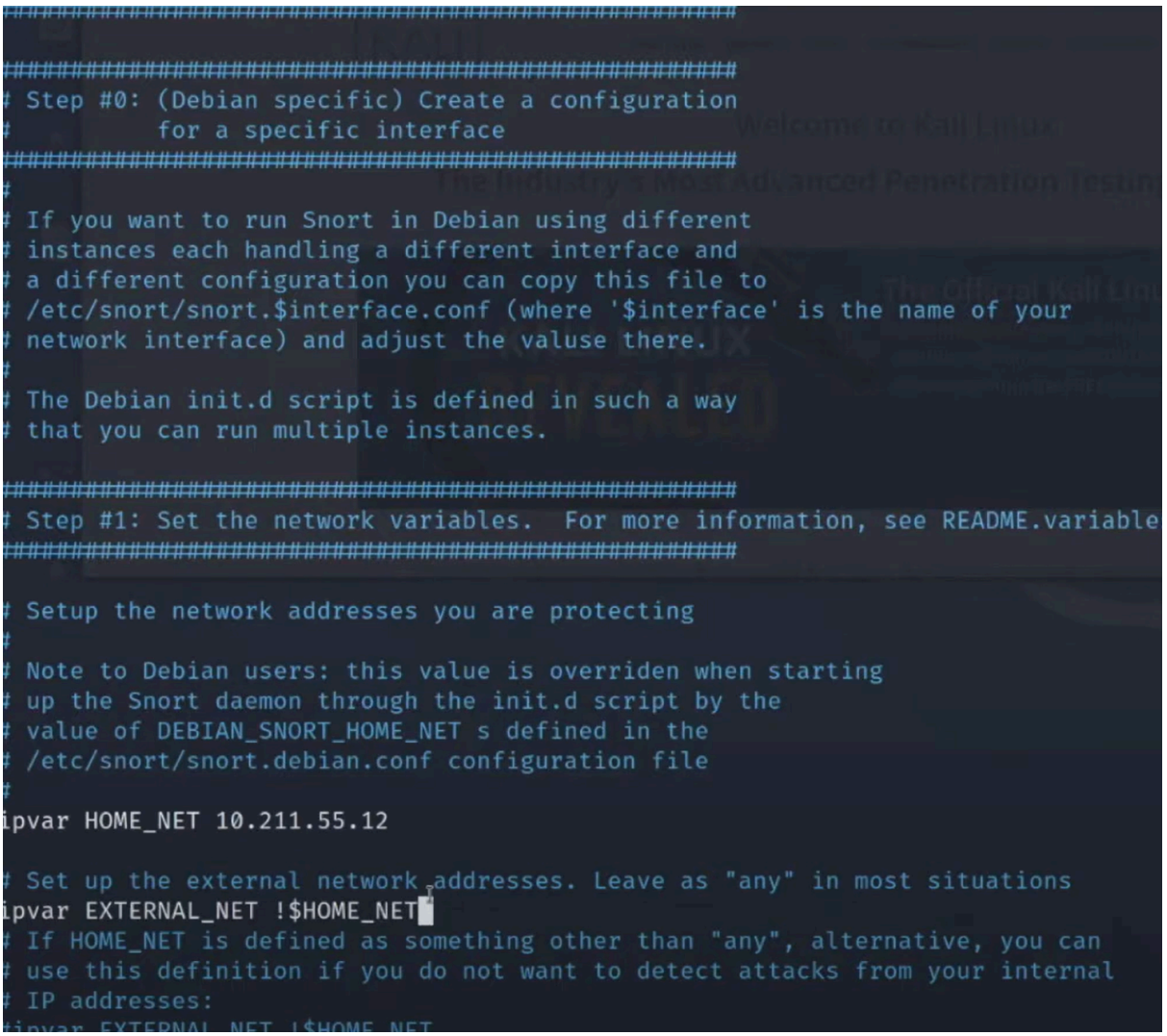
Creamos carpeta log para guardar nuestros logs en caso de que salten alertas



Vamos a definir 2 variables muy importantes que son HOME_NET y EXTERNAL_NET, es decir la red en la que snort está situado y la red externa. Para ello tenemos que entrar en el archivo de configuración de snort

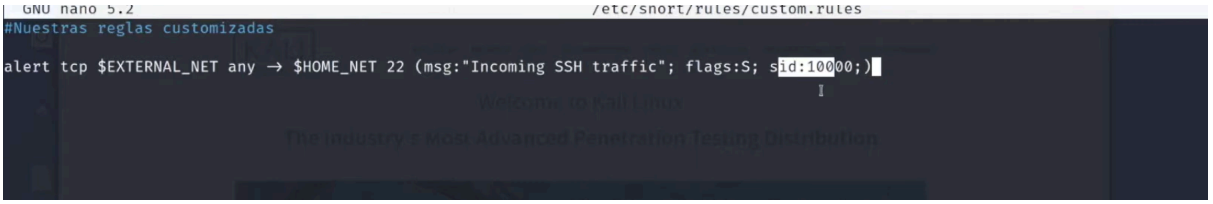


Una vez dentro del archivo definimos estas 2 variables. En mi caso la HOME_NET sera 10.211.55.12 y EXTERNAL_NET será !&HOME_NET, que quiere decir cualquier cosa que no sea la HOME_NET.



Ahora si vamos a escribir nuestra primera regla. Primero entramos en el archivo custom.rules creado anteriormente

Una vez dentro añadimos la siguiente regla/alerta



Con esta regla le decimos a snort que alerte todo el tráfico tcp que venga de la red externa desde cualquier puerto hacia la red interna al puerto 22. Para alertar lanzará el mensaje: ‘Incoming SSH traffic’

Para incluir la regla hay que entrar en el archivo de configuración de snort e incluirla junto con el resto de la misma forma

```
alejandro@kali:~$ sudo nano /etc/snort/snort.conf
```

```
  GNU nano 5.2                                  /etc/snort/snort.conf
include $RULE_PATH/snmp.rules
#include $RULE_PATH/specific-threats.rules
#include $RULE_PATH/spyware-put.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/telnet.rules
include $RULE_PATH/tftp.rules
include $RULE_PATH/virus.rules
#include $RULE_PATH/voip.rules
#include $RULE_PATH/web-activex.rules
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/web-cgi.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/web-coldfusion.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-php.rules
include $RULE_PATH/x11.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/community-sql-injection.rules
include $RULE_PATH/community-web-client.rules
include $RULE_PATH/community-web-dos.rules
include $RULE_PATH/community-web-iis.rules
include $RULE_PATH/community-web-misc.rules
include $RULE_PATH/community-web-php.rules
include $RULE_PATH/custom.rules
```

3. INICIAR SNORT Y COMPROBAR QUE FUNCIONA Y EFECTIVAMENTE NOS ALERTA ANTE POSIBLES ATAQUES

Iniciamos snort

```
alejandro@kali:~$ sudo snort -d -l /etc/snort/log/ -b -c /etc/snort/snort.conf
Running in IDS mode

        --== Initializing Snort ==--
```

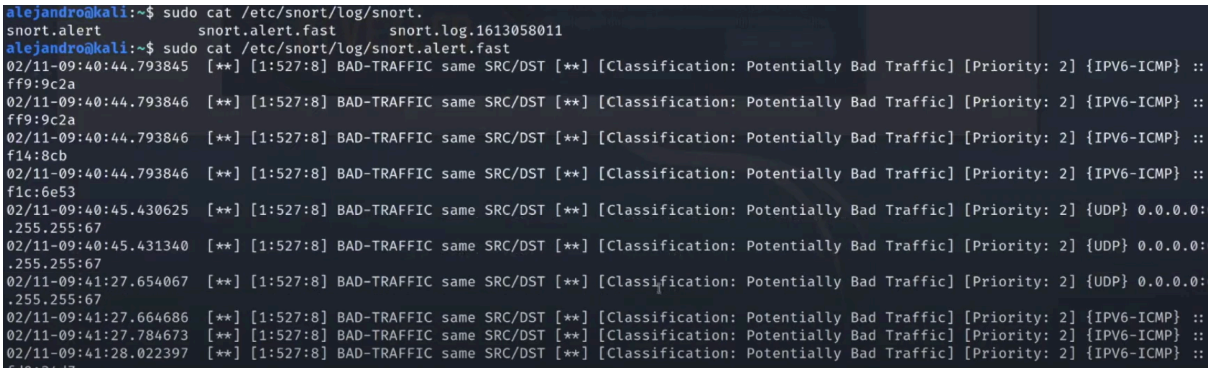
Levantamos servicio ssh

```
alejandro@kali:~$ sudo service ssh start
```

Accedemos desde otra máquina a la máquina kali

```
alejandro@ubuntu:~$ ssh alejandro@10.211.55.12
alejandro@10.211.55.12's password:
Linux kali 5.8.0-kali1-amd64 #1 SMP Debian 5.8.7-1kali1 (2020-09-14) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
alejandro@kali:~$
```

Para comprobar si se generó alerta entramos en la carpeta log creada anteriormente



Como se puede observar efectivamente se han generado distintas alertas, ya que snort ya venía con otras reglas predefinidas, y entre estas alertas se encuentra la alerta que hace referencia a la regla que nosotros creamos