

MONTANDO NIDS CON SNORT.

1.INSTALAR SNORT

```
alejandro@kali:~$ sudo apt-get install snort
[sudo] password for alejandro:
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package snort
alejandro@kali:~$
```

Antes de instalar snort es necesario actualizar las fuentes de kali

Mirrors for [README](#)

File information

- Filename: README
- Path: /README
- Size: 159 (159 bytes)
- Last modified: Mon, 04 Mar 2013 15:57:53 GMT (Unix time: 1362412673)

[Download file from preferred mirror](#)

Reliable downloads

Metalink

- <http://http.kali.org/README.meta4> (IETF Metalink)
- <http://http.kali.org/README.metalink> (old (v3) Metalink)

Mirrors

List of best mirrors for IP address 181.209.195.76, located at 15.043600,-91.408600 in Guatemala (GT).

[Map showing the closest mirrors](#)

Found 2 mirrors in other countries, but same continent (NA)

- <https://kali.download/kali/README> (us, prio 400)
- <https://mirrors.ocf.berkeley.edu/kali/README> (us, prio 100)

```
alejandro@kali:~$ sudo nano /etc/apt/sources.list
```

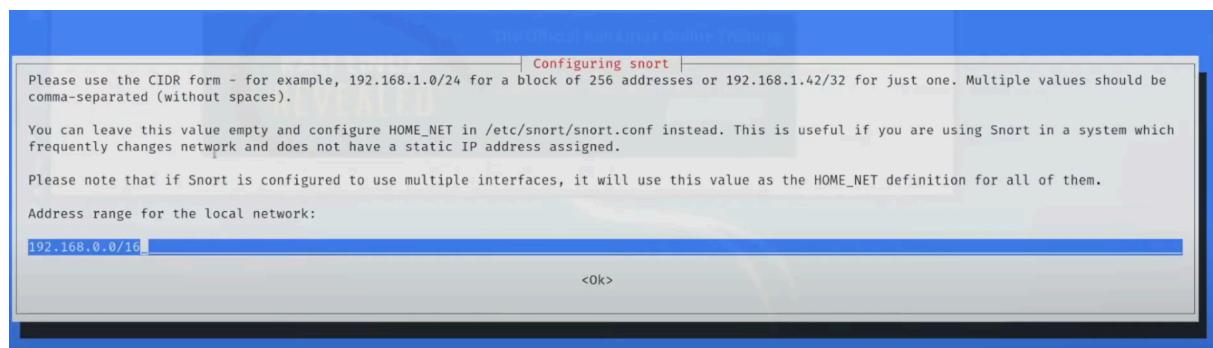
```
GNU nano 5.2                                     /etc/apt/sources.list
# See https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
deb http://http.kali.org/kali kali-rolling main contrib non-free
deb https://kali.download/kali/ kali-rolling main contrib non-free
# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free
```

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-requests 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

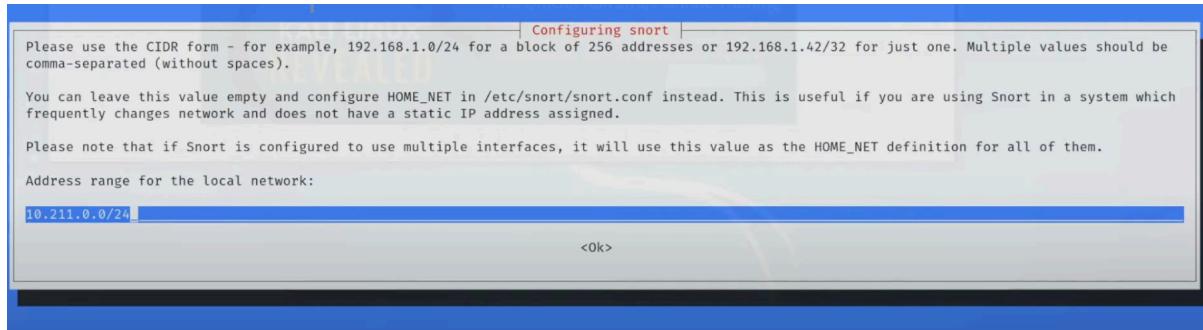
```

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

```
processing triggers for tloc-bin (2.51-5) ...
alejandro@kali:~$ sudo touch /etc/snort/rules/custom.rules
alejandro@kali:~$ ls /etc/snort/rules/
attack-responses.rules      community-mail-client.rules    community-web-iis.rules  icmp.rules      pop2.rules      web-attacks.rules
backdoor.rules                community-misc.rules        community-web-misc.rules  imap.rules      pop3.rules      web-cgi.rules
bad-traffic.rules             community-nntp.rules       community-web-php.rules  info.rules      porn.rules      web-client.rules
chat.rules                   community-oracle.rules     custom.rules            local.rules     rpc.rules      web-coldfusion.rules
community-bot.rules           community-policy.rules    ddos.rules            misc.rules      rservices.rules  web-frontpage.rules
community-deleted.rules      community-sip.rules       deleted.rules         multimedia.rules  scan.rules      web-iis.rules
community-dos.rules           community-smtp.rules      dns.rules            mysql.rules    shellcode.rules  web-misc.rules
community-exploit.rules      community-sql-injection.rules dos.rules            netbios.rules   smtp.rules      web-php.rules
```

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

```
alejandro@kali:~$ sudo mkdir /etc/snort/log
```

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

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

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.

```
#####
## Step #0: (Debian specific) Create a configuration
##          for a specific interface
#####
#
# If you want to run Snort in Debian using different
# instances each handling a different interface and
# a different configuration you can copy this file to
# /etc/snort/snort.$interface.conf (where '$interface' is the name of your
# network interface) and adjust the values there.
#
# The Debian init.d script is defined in such a way
# that you can run multiple instances.

#####
# Step #1: Set the network variables. For more information, see README.variable
#####

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overridden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET as defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 10.211.55.12

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET
# If HOME_NET is defined as something other than "any", alternative, you can
# use this definition if you do not want to detect attacks from your internal
# IP addresses:
#ipvar EXTERNAL_NET !$HOME_NET
```

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

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

Una vez dentro añadimos la siguiente regla/alerta

```
GNU nano 5.2                                     /etc/snort/rules/custom.rules
#Nuestras reglas customizadas

alert tcp $EXTERNAL_NET any → $HOME_NET 22 (msg:"Incoming SSH traffic"; flags:S; sid:10000;)
```

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

```
alejandro@kali:~$ sudo cat /etc/snort/log/snort.  
snort.alert      snort.alert.fast    snort.log.1613058011  
alejandro@kali:~$ sudo cat /etc/snort/log/snort.alert.fast  
02/11-09:40:44.793845  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::  
ff9:9c2a  
02/11-09:40:44.793846  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::  
ff9:9c2a  
02/11-09:40:44.793846  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::  
f14:8cb  
02/11-09:40:44.793846  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::  
f1c:6e53  
02/11-09:40:45.430625  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:  
.255.255:67  
02/11-09:40:45.431340  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:  
.255.255:67  
02/11-09:41:27.654067  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:  
.255.255:67  
02/11-09:41:27.664686  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::  
02/11-09:41:27.784673  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::  
02/11-09:41:28.022397  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {IPV6-ICMP} ::
```

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

```
02/11-09:42:04.586306  [**] [1:10000:0] Incoming SSH traffic [**] [Priority: 0] {TCP} 10.211.55.6:36798 → 10.211.55.12:22
```