



## Actividad de SNORT

Santiago Aillón Prada

Marzo 2024

### Ajustes de la configuración

Una vez descargado SNORT con sus dependencias, lo primero que toca hacer es modificar el archivo `snort.conf`. Una vez en el archivo, la línea `ipvar HOME_NET xxx.xxx.x.x` tiene que ser modificada, cambiando las equis por la dirección IP de la red/maquina que se quiere proteger.

Entonces, primero se utilizó el comando `ifconfig` para saber la dirección IP.

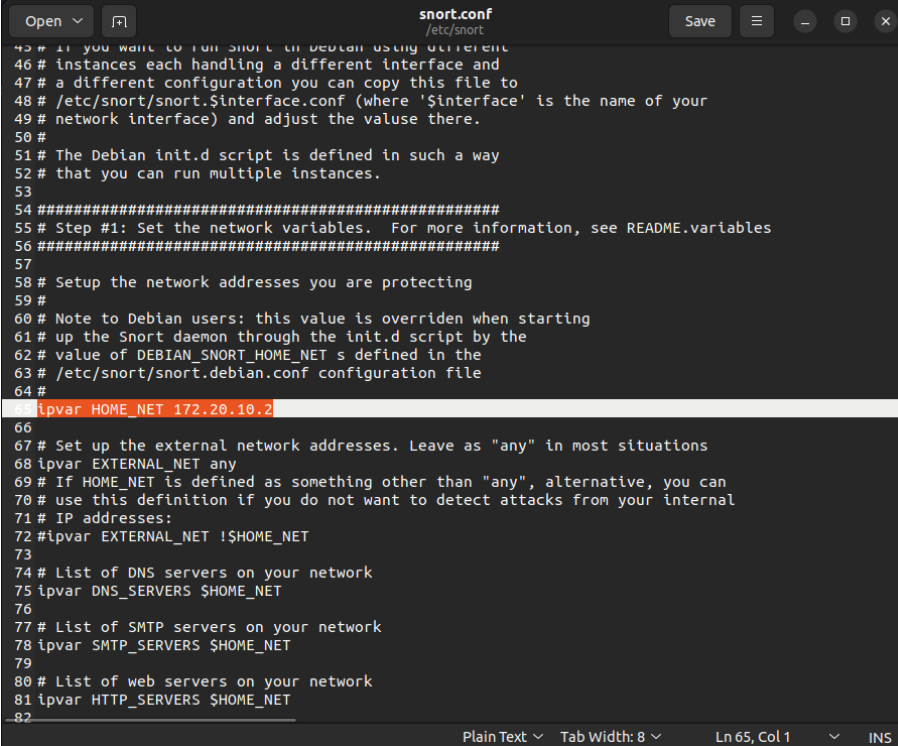
```
~ took 8m8s
> ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:32:c2:ef:1f txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    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 77933 bytes 103138428 (103.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 77933 bytes 103138428 (103.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 192.168.122.1 netmask 255.255.255.0 broadcast 192.168.122.255
    ether 52:54:00:ec:89:79 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp0s20f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.2 netmask 255.255.255.240 broadcast 172.20.10.15
    inet6 fe80::8146:5e43:be9b:e05f prefixlen 64 scopeid 0x20<link>
    ether 8c:f8:c5:12:56:24 txqueuelen 1000 (Ethernet)
    RX packets 404247 bytes 391436251 (391.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 101959 bytes 17734895 (17.7 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

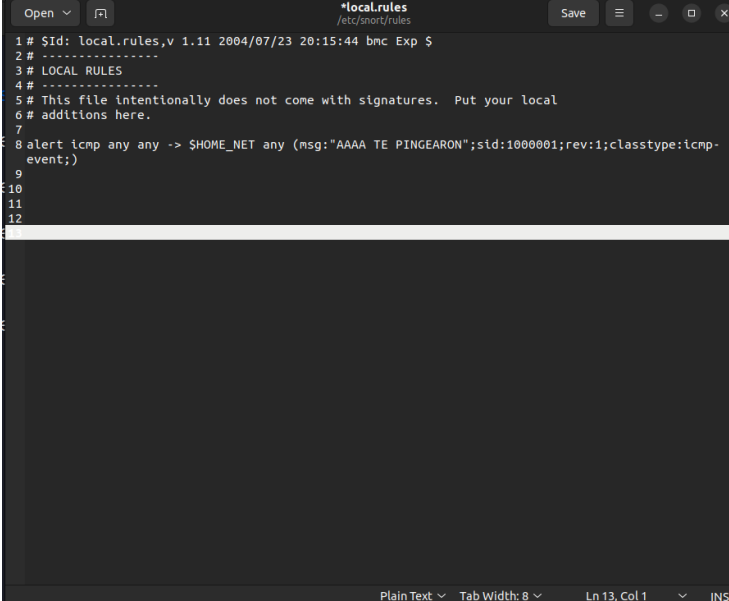
Luego, utilizando el comando `sudo gedit /etc/snort/snort.conf`, se modificó la línea mencionada anteriormente en el archivo `snort.conf`



```
45 # If you want to run snort on Debian using different
46 # instances each handling a different interface and
47 # a different configuration you can copy this file to
48 # /etc/snort/snort.$interface.conf (where '$interface' is the name of your
49 # network interface) and adjust the value there.
50 #
51 # The Debian init.d script is defined in such a way
52 # that you can run multiple instances.
53
54 #####
55 # Step #1: Set the network variables. For more information, see README.variables
56 #####
57
58 # Setup the network addresses you are protecting
59 #
60 # Note to Debian users: this value is overridden when starting
61 # up the Snort daemon through the init.d script by the
62 # value of DEBIAN_SNORT_HOME_NET s defined in the
63 # /etc/snort/snort.debian.conf configuration file
64 #
65 ipvar HOME_NET 172.20.10.2
66
67 # Set up the external network addresses. Leave as "any" in most situations
68 ipvar EXTERNAL_NET any
69 # If HOME_NET is defined as something other than "any", alternative, you can
70 # use this definition if you do not want to detect attacks from your internal
71 # IP addresses:
72 #ipvar EXTERNAL_NET !$HOME_NET
73
74 # List of DNS servers on your network
75 ipvar DNS_SERVERS $HOME_NET
76
77 # List of SMTP servers on your network
78 ipvar SMTP_SERVERS $HOME_NET
79
80 # List of web servers on your network
81 ipvar HTTP_SERVERS $HOME_NET
82
```

## Definición de reglas

Una vez configurado SNORT, se procederá a definir las reglas necesarias para el NIDS. Para esto se utilizó el comando `sudo gedit /etc/snort/rules/local.rules`, y se configuró la siguiente regla.



```
1 # $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
2 # -----
3 # LOCAL RULES
4 # -----
5 # This file intentionally does not come with signatures. Put your local
6 # additions here.
7
8 alert icmp any any -> $HOME_NET any (msg:"AAAA TE PINGEARON";sid:1000001;rev:1;classtype:icmp-
9 event;)
10
11
12
```

## Descripción de la regla

Esta regla hace que el SNORT mande una alerta cuando detecta cualquier conexión mediante el protocolo icmp junto con el mensaje "AAAA TE PINGEARON"

- **alert:** Le decimos a SNORT que muestre una alarma.
- **icmp any any:** Cuando se detecte una conexión desde cualquier dirección a cualquier dirección con el protocolo icmp.
- **\$HOME.NET:** IP de destino (Esta fue la misma variable que definimos anteriormente)
- **msg:** Mostrar un mensaje junto con la alarma
- **sid:** Esta es la manera de SNORT para identificar cada regla. El sid es un identificador único, sin embargo, SNORT por defecto ya tiene registradas las reglas 100 - 1,000,000 entonces, se necesita utilizar un número mayor a este.
- **rev:** El rev es otro identificador de reglas de SNORT, solamente que este, identifica las revisiones/modificaciones de cada regla.
- **classtype:icmp-event:** Aunque ya se le declaro a SNORT que esta regla va a tener en cuenta todas las conexiones icmp, SNORT tiene ciertas categorías predefinidas las cuales son convenientes de utilizar, pues ayuda para la organización y categorización de las reglas.

## Evaluación de la regla

Para la evaluación de la regla, como la regla detecta cualquier conexión mediante el protocolo icmp, se realizó un ping desde otra máquina a la dirección IP de la máquina a proteger.

```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Windows\system32> ping 172.20.10.2

Haciendo ping a 172.20.10.2 con 32 bytes de datos:
Respuesta desde 172.20.10.2: bytes=32 tiempo=735ms TTL=64
Respuesta desde 172.20.10.2: bytes=32 tiempo=105ms TTL=64
Respuesta desde 172.20.10.2: bytes=32 tiempo=24ms TTL=64
Respuesta desde 172.20.10.2: bytes=32 tiempo=37ms TTL=64

Estadísticas de ping para 172.20.10.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 24ms, Máximo = 735ms, Media = 225ms
PS C:\Windows\system32>
```

Una vez realizado el ping desde la otra maquina, se ejecuto el comando `sudo snort -A console -q -c /etc/snort/snort.conf -i wlp0s20f3`. El cual permite ver las alarmas que manda SNORT en tiempo real.

```
root@kali:~# sudo snort -A console -q -c /etc/snort/snort.conf -i wlp0s20f3
03/16-16:59:02.563026  [**] [1:1000001:1] AAAA TE PINGEARN [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 172.20.10.14 -> 172.20.10.2
03/16-16:59:02.946094  [**] [1:1000001:1] AAAA TE PINGEARN [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 172.20.10.14 -> 172.20.10.2
03/16-16:59:03.878126  [**] [1:1000001:1] AAAA TE PINGEARN [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 172.20.10.14 -> 172.20.10.2
03/16-16:59:04.902004  [**] [1:1000001:1] AAAA TE PINGEARN [**] [Classification: Generic ICMP event] [Priority: 3] {ICMP} 172.20.10.14 -> 172.20.10.2
03/16-16:59:34.599467  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
03/16-17:01:58.258566  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
03/16-17:02:26.518861  [**] [1:527:8] BAD-TRAFFIC same SRC/DST [**] [Classification: Potentially Bad Traffic] [Priority: 2] {UDP} 0.0.0.0:68 -> 255.255.255.255:67
```

Finalmente, se puede ver que SNORT está detectando correctamente el ping desde la otra maquina y está mandando la alerta y el mensaje correctamente.