2019

IDS - SNORT

SEMINARIO LINUX

HAROL HERNAN TORRES NEUTA

INSTALACIÓN SNORT

1. Instalar fuentes de librerias para la instalación de SNORT.

sudo apt install -y gcc libpcre3-dev zlib1g-dev libluajit-5.1-dev libpcap-dev openssl libssl-dev libnghttp2-dev libdumbnet-dev bison flex libdnet

```
Leyendo la información de estado... Hecho
zlib1g-dev ya está en su versión más reciente (1:1.2.11.dfsg-0ubuntu2).
gcc ya está en su versión más reciente (4:7.4.0-1ubuntu2.3).
fijado gcc como instalado manualmente.
openssl ya está en su versión más reciente (1.1.1-1ubuntu2.1~18.04.5).
Se instalarán los siguientes paquetes adicionales:
  libbison-dev libfl-dev libfl2 libluajit-5.1-2 libluajit-5.1-common libpcap0.8-dev libpcre16-3 libpcre32-3 libpcrecpp0v5 m4 pkg-config
Paquetes sugeridos:
  bison-doc flex-doc dnet-common libnghttp2-doc libssl-doc m4-doc
Se instalarán los siguientes paquetes NUEVOS:
  bison flex libbison-dev libdnet libdumbnet-dev libfl-dev libfl2 libluajit-5.1-2 libluajit-5.1-common libluajit-5.1-dev libnghttp2-dev libpcap-dev libpcap0.8-dev libpcre16-3 libpcre3-dev libpcre32-3 libpcrecpp0v5 libssl-dev m4
  pkg-config
0 actualizados, 20 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 4.530 kB de archivos.
Se utilizarán 18,0 MB de espacio de disco adicional después de esta operación.
Des:1 http://archive.ubuntu.com/ubuntu bionic/main amd64 m4 amd64 1.4.18-1 [197 kB]
Des:2 http://archive.ubuntu.com/ubuntu bionic/main amd64 flex amd64 2.6.4-6 [316 kB]
Des:3 http://archive.ubuntu.com/ubuntu bionic/main amd64 libdumbnet-dev amd64 1.12-7build1 [56,2 kB]
Des:4 http://archive.ubuntu.com/ubuntu bionic/main amd64 libbison-dev amd64 2:3.0.4.dfsg-1build1 [339 kB]
Des:5 http://archive.ubuntu.com/ubuntu bionic/main amd64 bison amd64 2:3.0.4.dfsg-1build1 [266 kB]
Des:6 http://archive.ubuntu.com/ubuntu bionic/main amd64 libfl2 amd64 2.6.4-6 [11,4 kB]
Des:7 http://archive.ubuntu.com/ubuntu bionic/main amd64 libfl-dev amd64 2.6.4-6 [6.320 B]
Des:8 http://archive.ubuntu.com/ubuntu bionic/universe amd64 libluajit-5.1-common all 2.1.0~beta3+dfsg-5.1 [44,3 kB]
Des:9 http://archive.ubuntu.com/ubuntu bionic/universe amd64 libluajit-5.1-2 amd64 2.1.0~beta3+dfsg-5.1 [227 kB]
Des:10 http://archive.ubuntu.com/ubuntu bionic/universe amd64 libluajit-5.1-dev amd64 2.1.0~beta3+dfsg-5.1 [243 kB]
Des:11 http://archive.ubuntu.com/ubuntu bionic/main amd64 pkg-config amd64 0.29.1-0ubuntu2 [45,0 kB]
Des:12 http://archive.ubuntu.com/ubuntu bionic/main amd64 libnghttp2-dev amd64 1.30.0-1ubuntu1 [95,4 kB]
Des:13 http://archive.ubuntu.com/ubuntu bionic/main amd64 libpcap0.8-dev amd64 1.8.1-6ubuntu1 [217 kB]
Des:14 http://archive.ubuntu.com/ubuntu bionic/main amd64 libpcap-dev amd64 1.8.1-6ubuntu1 [3.480 B]
Des:15 http://archive.ubuntu.com/ubuntu bionic/main amd64 libpcre16-3 amd64 2:8.39-9 [147 kB]
Des:16 http://archive.ubuntu.com/ubuntu bionic/main amd64 libpcre32-3 amd64 2:8.39-9 [138 kB]
Des:17 http://archive.ubuntu.com/ubuntu bionic/main amd64 libpcrecpp0v5 amd64 2:8.39-9 [15,3 kB]
Des:18 http://archive.ubuntu.com/ubuntu bionic/main amd64 libpcre3-dev amd64 2:8.39-9 [537 kB]
Des:19 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libssl-dev amd64 1.1.1-1ubuntu2.1~18.04.5 [1.566 kB]
Des:20 http://archive.ubuntu.com/ubuntu bionic/universe amd64 libdnet amd64 2.65 [60,1 kB]
Descargados 4.530 kB en 17s (273 kB/s)
Seleccionando el paquete m4 previamente no seleccionado.
(Leyendo la base de datos ... 77179 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../00-m4_1.4.18-1_amd64.deb ...
Desempaquetando m4 (1.4.18-1) ...
Seleccionando el paquete flex previamente no seleccionado.
Preparando para desempaquetar .../01-flex_2.6.4-6_amd64.deb ...
Desempaquetando flex (2.6.4-6) ...
Seleccionando el paquete libdumbnet-dev previamente no seleccionado.
Preparando para desempaquetar .../02-libdumbnet-dev_1.12-7build1_amd64.deb ...
Desempaquetando libdumbnet-dev (1.12-7build1) ...
Progreso: [  7%] [############..........................................................................................................................]
```

2. Ir a la ruta de fuentes de SNORT

mkdir ~/snort_src && cd ~/snort_src

```
adminserver@padilla:~$ mkdir ~/snort_src && cd ~/snort_src
adminserver@padilla:~/snort_src$
```

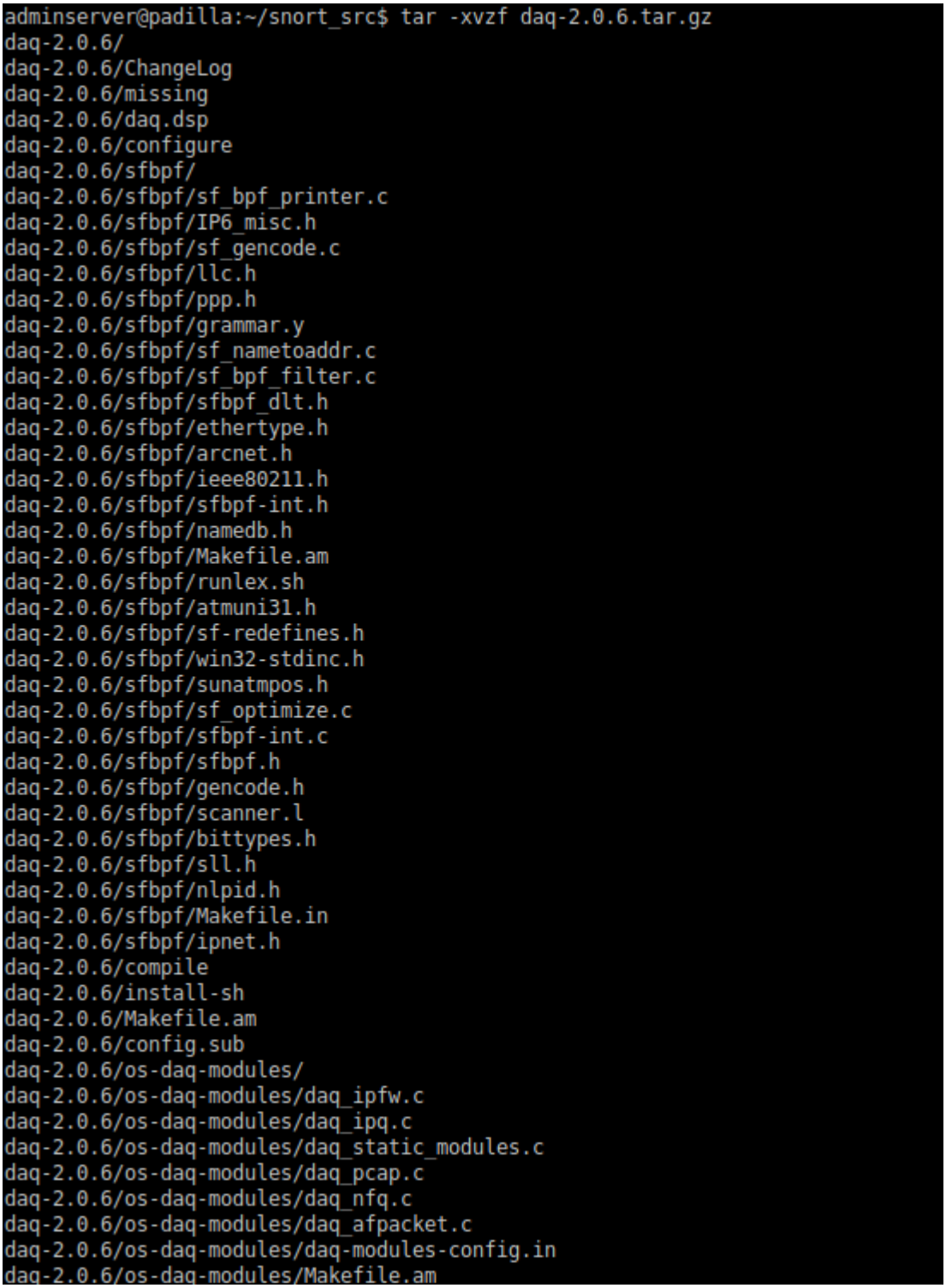
3. Obtener Fuentes

wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz

```
adminserver@padilla:~/snort_src$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2019-11-22 13:15:17--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8b09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/803/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191122%2Fus-east-1%2Fs3%2Faws4_requ
est&X-Amz-Date=20191122T131518Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=10ee36b3e19c4553451fc2a511b0e566774ff20253f7b5c14d6329d737970436 [following]
--2019-11-22 13:15:18--  https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/803/original/daq-2.0.6.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191122%2Fus-east-1%2
Fs3%2Faws4_request&X-Amz-Date=20191122T131518Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=10ee36b3e19c4553451fc2a511b0e566774ff20253f7b5c14d6329d737970436
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.101.43
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.101.43|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 518013 (506K) [binary/octet-stream]
Saving to: 'daq-2.0.6.tar.gz'

daq-2.0.6.tar.gz                                    100%[=============================================================================================================================>] 505,87K  1007KB/s    in 0,5s

2019-11-22 13:15:19 (1007 KB/s) - 'daq-2.0.6.tar.gz' saved [518013/518013]

adminserver@padilla:~/snort_src$
```

4. Descomprimir paquetes descargados

tar -xvzf daq-2.0.6.tar.gz



5. ir a carpeta con archivos extraídos

cd daq-2.0.6

```
adminserver@padilla:~/snort_src$ cd daq-2.0.6
adminserver@padilla:~/snort_src/daq-2.0.6$ ll
total 1116
drwxr-xr-x 6 adminserver adminserver   4096 jul 16  2015 ./
drwxrwxr-x 3 adminserver adminserver   4096 nov 22 13:17 ../
-rw-r--r-- 1 adminserver adminserver  42353 jul 15  2015 aclocal.m4
drwxr-xr-x 2 adminserver adminserver   4096 jul 16  2015 api/
-rw-r--r-- 1 adminserver adminserver    446 jul 16  2015 ChangeLog
-rwxr-xr-x 1 adminserver adminserver   7333 jul 15  2015 compile*
-rwxr-xr-x 1 adminserver adminserver  42938 jul 15  2015 config.guess*
-rw-r--r-- 1 adminserver adminserver   6280 jul 15  2015 config.h.in
-rwxr-xr-x 1 adminserver adminserver  35987 jul 15  2015 config.sub*
-rwxr-xr-x 1 adminserver adminserver 497485 jul 15  2015 configure*
-rw-r--r-- 1 adminserver adminserver  11296 jul 15  2015 configure.ac
-rw-r--r-- 1 adminserver adminserver  21007 sep  6  2012 COPYING
-rwxr-xr-x 1 adminserver adminserver   7121 jun  8  2011 daq.dsp*
-rwxr-xr-x 1 adminserver adminserver  23566 jul 15  2015 depcomp*
-rwxr-xr-x 1 adminserver adminserver  14675 jul 15  2015 install-sh*
-rw-r--r-- 1 adminserver adminserver 324089 jul 15  2015 ltmain.sh
drwxr-xr-x 2 adminserver adminserver   4096 jul 16  2015 m4/
-rw-r--r-- 1 adminserver adminserver    168 may  6  2010 Makefile.am
-rw-r--r-- 1 adminserver adminserver  25594 jul 15  2015 Makefile.in
-rwxr-xr-x 1 adminserver adminserver   6872 jul 15  2015 missing*
drwxr-xr-x 2 adminserver adminserver   4096 jul 16  2015 os-daq-modules/
-rw-r--r-- 1 adminserver adminserver  13381 jun 19  2014 README
drwxr-xr-x 2 adminserver adminserver   4096 jul 16  2015 sfbpf/
adminserver@padilla:~/snort_src/daq-2.0.6$
```

6. Compilar librerías

./configure && make && sudo make install

```
adminserver@padilla:~/snort_src/daq-2.0.6$ ./configure && make && sudo make install
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking whether make supports nested variables... yes
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... GNU
checking dependency style of gcc... gcc3
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
checking for a sed that does not truncate output... /bin/sed
checking for grep that handles long lines and -e... /bin/grep
checking for egrep... /bin/grep -E
checking for fgrep... /bin/grep -F
checking for ld used by gcc... /usr/bin/ld
checking if the linker (/usr/bin/ld) is GNU ld... yes
checking for BSD- or MS-compatible name lister (nm)... /usr/bin/nm -B
checking the name lister (/usr/bin/nm -B) interface... BSD nm
checking whether ln -s works... yes
checking the maximum length of command line arguments... 1572864
checking how to convert x86_64-unknown-linux-gnu file names to x86_64-unknown-linux-gnu format... func_convert_file_noop
checking how to convert x86_64-unknown-linux-gnu file names to toolchain format... func_convert_file_noop
checking for /usr/bin/ld option to reload object files... -r
checking for objdump... objdump
```

7. Ir a la carpeta de instalación.

cd ~/snort_src

```
adminserver@padilla:~/snort_src/daq-2.0.6$ cd ~/snort_src
adminserver@padilla:~/snort_src$ pwd
/home/adminserver/snort_src
adminserver@padilla:~/snort_src$
```

8. Descargar Snort desde las fuentes oficiales.

sudo wget https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz

```
adminserver@padilla:~/snort_src$ sudo wget https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
--2019-11-22 13:25:52--  https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8b09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/796/original/snort-2.9.15.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191122%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191122T132554Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=84695f549ed6c478406dba74ec221e7d58d37f6dbe8686663dfbac0a26ac0170 [following]
--2019-11-22 13:25:53--  https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/011/796/original/snort-2.9.15.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191122%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191122T132554Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=84695f549ed6c478406dba74ec221e7d58d37f6dbe8686663dfbac0a26ac0170
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.114.227
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.114.227|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6704763 (6,4M) [binary/octet-stream]
Saving to: 'snort-2.9.15.tar.gz'

snort-2.9.15.tar.gz                 100%[=============================================================================================================>]   6,39M  1,31MB/s    in 5,0s

2019-11-22 13:25:59 (1,27 MB/s) - 'snort-2.9.15.tar.gz' saved [6704763/6704763]

adminserver@padilla:~/snort_src$
```

9, Descomprimir SNORT

tar -xvzf snort-2.9.15.tar.gz

```
adminserver@padilla:~/snort_src$ tar -xvzf snort-2.9.15.tar.gz
snort-2.9.15/
snort-2.9.15/snort.8
snort-2.9.15/install-sh
snort-2.9.15/snort.pc.in
snort-2.9.15/aclocal.m4
snort-2.9.15/config.guess
snort-2.9.15/compile
snort-2.9.15/config.h.in
snort-2.9.15/missing
snort-2.9.15/LICENSE
snort-2.9.15/config.sub
snort-2.9.15/COPYING
snort-2.9.15/templates/
snort-2.9.15/templates/sp_template.c
snort-2.9.15/templates/sp_template.h
snort-2.9.15/templates/spp_template.c
snort-2.9.15/templates/Makefile.in
snort-2.9.15/templates/Makefile.am
snort-2.9.15/templates/spp_template.h
snort-2.9.15/verstuff.pl
snort-2.9.15/Makefile.in
snort-2.9.15/etc/
snort-2.9.15/etc/file_magic.conf
```

10. ir a la carpeta de instalación.

cd snort-2.9.15

```
adminserver@padilla:~/snort_src$ cd snort-2.9.15
adminserver@padilla:~/snort_src/snort-2.9.15$ pwd
/home/adminserver/snort_src/snort-2.9.15
adminserver@padilla:~/snort_src/snort-2.9.15$
```

11. instalación y configuración de snort.

./configure --enable-sourcefire && make && sudo make install

CONFIGURACIÓN SNORT

1. Actualizar Librerías

sudo ldconfig

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo ldconfig
adminserver@padilla:~/snort_src/snort-2.9.15$
```

2. Genera enlace de la carpeta

sudo ln -s /usr/local/bin/snort /usr/sbin/snort

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo ln -s /usr/local/bin/snort /usr/sbin/snort
adminserver@padilla:~/snort_src/snort-2.9.15$
```

3. Adicionar usuario de servicio a grupos y configuracion nologin

sudo groupadd snort

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo groupadd snort
adminserver@padilla:~/snort_src/snort-2.9.15$
```

sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
adminserver@padilla:~/snort_src/snort-2.9.15$
```

4. Creación de carpetas de estructura de configuraciones.

sudo mkdir -p /etc/snort/rules
sudo mkdir /var/log/snort
sudo mkdir /usr/local/lib/snort_dynamicrules

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo mkdir -p /etc/snort/rules
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo mkdir /var/log/snort
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo mkdir /usr/local/lib/snort_dynamicrules
adminserver@padilla:~/snort_src/snort-2.9.15$
```

5. Permisos en carpetas

sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
sudo chown -R snort:snort /etc/snort
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo chmod -R 5775 /etc/snort
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo chmod -R 5775 /var/log/snort
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo chown -R snort:snort /etc/snort
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo chown -R snort:snort /var/log/snort
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

6. Creacion de listas blancas y negras para snort.

sudo touch /etc/snort/rules/white_list.rules
sudo touch /etc/snort/rules/black_list.rules
sudo touch /etc/snort/rules/local.rules

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo touch /etc/snort/rules/white_list.rules
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo touch /etc/snort/rules/black_list.rules
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo touch /etc/snort/rules/local.rules
adminserver@padilla:~/snort_src/snort-2.9.15$
```

7. Copia de archivos de configuracion

sudo cp ~/snort_src/snort-2.9.15/etc/*.conf* /etc/snort
sudo cp ~/snort_src/snort-2.9.15/etc/*.map /etc/snort

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo cp ~/snort_src/snort-2.9.15/etc/*.conf* /etc/snort
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo cp ~/snort_src/snort-2.9.15/etc/*.map /etc/snort
adminserver@padilla:~/snort_src/snort-2.9.15$
```

REGLAS POR COMUNIDADES

1. Descargar archivos de configuración.

wget https://www.snort.org/rules/community -O ~/community.tar.gz

```
adminserver@padilla:~/snort_src/snort-2.9.15$ wget https://www.snort.org/rules/community -O ~/community.tar.gz
--2019-11-22 15:52:15--  https://www.snort.org/rules/community
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8b09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/012/216/original/community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191122%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191122T155216Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=146f0977b2f4c05b705d1119f343d663a83e7186510d27a0816104f40e580c79 [following]
--2019-11-22 15:52:16--  https://snort-org-site.s3.amazonaws.com/production/release_files/files/000/012/216/original/community-rules.tar.gz?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191122%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191122T155216Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Signature=146f0977b2f4c05b705d1119f343d663a83e7186510d27a0816104f40e580c79
Resolving snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)... 52.216.8.171
Connecting to snort-org-site.s3.amazonaws.com (snort-org-site.s3.amazonaws.com)|52.216.8.171|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 331032 (323K) [application/gzip]
Saving to: '/home/adminserver/community.tar.gz'

/home/adminserver/community.tar.gz                  100%[=============================================================================================================================>] 323,27K   791KB/s    in 0,4s

2019-11-22 15:52:17 (791 KB/s) - '/home/adminserver/community.tar.gz' saved [331032/331032]

adminserver@padilla:~/snort_src/snort-2.9.15$
```

2. extraer y copiar archivos de configuración.

sudo tar -xvf ~/community.tar.gz -C ~/

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo tar -xvf ~/community.tar.gz -C ~/
[sudo] password for adminserver:
community-rules/
community-rules/community.rules
community-rules/VRT-License.txt
community-rules/LICENSE
community-rules/AUTHORS
community-rules/snort.conf
community-rules/sid-msg.map
adminserver@padilla:~/snort_src/snort-2.9.15$
```

sudo cp ~/community-rules/* /etc/snort/rules

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo cp ~/community-rules/* /etc/snort/rules
adminserver@padilla:~/snort_src/snort-2.9.15$
```

3. Actualizar reglas a aplicar

sudo sed -i 's/include \$RULE_PATH/#include \$RULE_PATH/' /etc/snort/snort.conf

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo sed -i 's/include \$RULE\_PATH/#include \$RULE\_PATH/' /etc/snort/snort.conf
adminserver@padilla:~/snort_src/snort-2.9.15$
```

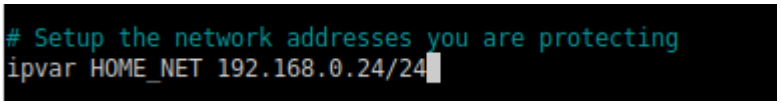
ARCHIVO DE CONFIGURACIÓN

1. Editar archivo de configuracion.

sudo nano /etc/snort/snort.conf

2. llaves a editar

 # Setup the network addresses you are protecting
ipvar HOME_NET server_public_ip/32



 # Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

 # Path to your rules files (this can be a relative path)
var RULE_PATH /etc/snort/rules
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

 # Set the absolute path appropriately
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules

 # unified2
 # Recommended for most installs
output unified2: filename snort.log, limit 128

include $RULE_PATH/local.rules

include $RULE_PATH/community.rules

Guardar cambios en el archivo de configuración.

```
adminserver@padilla:~/snort_src/snort-2.9.15$ sudo nano /etc/snort/snort.conf
adminserver@padilla:~/snort_src/snort-2.9.15$
```

3. Validar configuraciones

sudo snort -T -c /etc/snort/snort.conf

```
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15 GRE (Build 7)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.8.1
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>

Snort successfully validated the configuration!
Snort exiting
adminserver@padilla:/etc/snort/rules$ sudo snort -T -c /etc/snort/snort.conf
```