Implement and IDS/IPS with Snort

1. Install Snort

```
dsalgado@dsalgado-VirtualBox:~$ sudo apt-get install snort -y
```

2. Checking that the installation was correct.

```
dsalgado@dsalgado-VirtualBox:~$ snort --version

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.15.1 GRE (Build 15125)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.1 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.2.11
```

3. Opening the configuration file to include my network and my own rules for the Snort to take into account:

```
  GNU nano 6.2                    /etc/snort/snort.conf
# network interface) and adjust the valuse 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.variabl>
###################################################

# Setup the network addresses you are protecting
#
# Note to Debian users: this value is overriden when starting
# up the Snort daemon through the init.d script by the
# value of DEBIAN_SNORT_HOME_NET s defined in the
# /etc/snort/snort.debian.conf configuration file
#
ipvar HOME_NET 10.0.2.0/24

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

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

4. Proving that the changes in the configuration file where ok, and that it works:

```
dsalgado@dsalgado-VirtualBox:~$ sudo snort -T -i enp0s3 -c /etc/snort/snort.conf
[sudo] password for dsalgado:
Running in Test mode

Snort successfully validated the configuration!
Snort exiting
```

5. Running the Snort on IDS mode:

```
dsalgado@dsalgado-VirtualBox:~$ sudo snort -A console -q -c /etc/snort/snort.con
f -i enp0s3
```

6. Analyzing the different logs that it can create because of the detection and prevention system:

```
dsalgado@dsalgado-VirtualBox:~$ ls -la /var/log/snort
total 12
drwxr-s---  2 snort adm    4096 ene 20 16:29 .
drwxrwxr-x 16 root  syslog 4096 ene 20 14:13 ..
-rw-------  1 root  adm       0 ene 20 16:29 snort.alert
-rw-r--r--  1 root  adm     163 ene 20 14:16 snort.alert.fast
-rw-------  1 root  adm       0 ene 20 16:29 snort.log
-rw-------  1 root  adm       0 ene 20 16:22 snort.log.1737408123
-rw-------  1 root  adm       0 ene 20 16:28 snort.log.1737408486
```