Configure Snort

For extra insight on flags: Read the Man's..

```
man snort
```

Rule Syntax

Headers + Options:

```
! Rule Header !

action      : alert
Protocol    : icmp
SrcAddr     : <IP_addr>
SrcPort     : <port_#>
Direction   : -> / <-
DestAddr    : <IP_addr>
DestPort     : <port_#>
```

eg.

```


alert icmp any any -> any any  (msg: "[ICMP]: "; sid: 100004;)

^                           ^  ^                             ^

|_______Rule__Header________|  |________Rule__Options________|
```

Snort Tree

in the `/etc/snort/` dir, you will find

```
 classification.config
 community-sid-msg.map
 gen-msg.map
 reference.config
 rules/
 snort.conf
 snort.debian.conf
 threshold.conf
 unicode.map
```

snort.conf

Run:

```
sudo vim /etc/snort/snort.conf
```

First great thing to take note of in the snort.conf file, is a given ToDo List:

```
###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################
```

Second: It's not a bad idea to make a backup file of `snort.conf`

```
sudo cp /etc/snort/snort.conf /etc/snort/snort_backup.conf
```

ˆ Kinda ike with the apt list file..

Step 1

$HOME_NET variable

The `$HOME_NET` variable will be set to `any` by default.. lets change that to our own "ip addr":

Run:

```
ip addr
```

or

```
iwconfig
```

and you should see something like: (I will be giving fake values on mine.. so that git-guardian doesn't complain)

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
```

```
2: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen
    link/ether f8:8a:d3:5a:42:19 brd ff:ff:ff:ff:ff:ff
3: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1
    link/ether 82:5b:f4:02:42:23 brd ff:ff:ff:ff:ff:ff

   inet 192.168.0.107/24 brd 192.168.0.255 scope global dynamic noprefixroute wlan0
! ! !      ^ this is what you are looking for

       valid_lft 70698sec preferred_lft 70698sec
    inet6 fa81::b1c3:e42f:7b37:83ea/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Now we can set:

```
ipvar HOME_NET 192.168.0.107/24
```

! Note: It’s not a good idea to play with the rest of variables..

So, we’re going to skip to Step 7.. and start working on the RULES.. Which is where the fun stuff lies..

Step 7

Customize Rule Set

From line:570 to line:696 you will find a list of multiple predefined rules.. some are commented out, soe are not.. But, Know This: They are ALL outdated.. .. LoL/K3k

Test Config

We will use `-T` to first test for syntax errors (as we have made changes..)

For ‘interface’ we use `-i wlan0` (you can use whichever has the connection)

To specify the ‘rules-file’ we `-c /etc/snort/snort.conf`

Since it’s going to be interacting directly with the hardware, we will require `sudo`

```
sudo snort -T -i wlan0 -c /etc/snort/snort.conf
```

It will generate a lot of output.. but if all goes well, you will see an ASCII pig and the last 2 lines:

```
   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.7.0 GRE (Build 149)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team

    ...
    ...
```

```
Snort successfully validated the configuration!
Snort exiting
```

Don't panic when you see all the `Warning`s & `Error`s -We'll deal with that just now..

Clean Rules

For sanity sake, we are going to comment out all the community/predefined rules…

since I'm lazy.. let's use the vim built-in functions

! First make sure you hit ESC, and :w…

Now:

```
:578,696s/^/#
```

Then those lines should all be commented out..

Now, `:wq` once again, to 'write' the changes and quit vim

Again Run:

```
sudo snort -T -i wlan0 -c /etc/snort/snort.conf
```

And you shall see much cleaner outputs :)

End-Of-Doc

Next Doc is "make_rules.md"