Your Own Custom Rules

First off..

```
sudo vim /etc/snort/rules/local.rules
```

You should find a file containing: well, not much..

```
sudo cat /etc/snort/rules/local.rules
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.
```

Here you will write your rules

Syntax

! Note: Please read prior docs for basic view of Headers+Options

Now let's add:

```
alert icmp any any -> $HOME_NET any (msg: "[ICMP]:[ping detected]: "; sid: 10000014; rev: 1;
```

Headers

alert is our action icmp is the first `any any` is the Src Host & Port.. The `->` is the direction of the traffic.. second `$HOME_NET any` is the Dest Host & Port..

Options

For `msg: " some kind of flag/indecation ";` You can make the `sid: <iterally-any-number>` ^ (it works on 'jobs', so bigger is better..) And `rev:1` is our 'revision 1'

Test New Rule

-A : Alert Mode

Without the -A flag, the `alert`s in our rules, means nothing..

```
-A console
```

^ So it alerts to the console.. not some other random place..

Logs/

We will need to use:

`-l /var/log/snort/`

to save all our logs

Sshhh

`sudo snort -q`

^ So we don't get whacked with banners & pigs...

Interface

`-i wlan0`

^ For me.. maybe different for you..

Run This

CleanSnort

`sudo snort -q -l /var/log/snort -i wlan0 -A console -c /etc/snort/snort.conf`

If no output is given, we are on the right track..

though, it may hang.. if

`Ctrl+C`

Doesn't work..

Try using

`Ctrl+Z`

..

after which, run `jobs`...

You might find something like :

```
$ jobs
[1]  + suspended  sudo snort -q -l /var/log/snort -i wlan0 -A console -c /etc/snort/snort.co
```

^ This means It's still running in the background.. so kill it..

`kill -9 %%`

Once again, run `jobs`, and you will be pleased to find it gone.. :)

Now Run the $ CleanSnort $ Again.. and just leave it one side.. open a new terminal to the side..

PING Google :P

In the new terminal, Run:

```
ping 8.8.8.8
```

You should now see your first terminal poping output In sync with you ping output...

```
04/29-07:18:28.282442  [**] [1:10000014:1] [ICMP]:  [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192
04/29-07:18:29.115078  [**] [1:10000014:1] [ICMP]:  [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192
04/29-07:18:29.718609  [**] [1:10000014:1] [ICMP]:  [**] [Priority: 0] {ICMP} 8.8.8.8 -> 192
```

ˆ Date : ˆ Time IKD ˆ rev ˆ: ˆ pid msg ˆ ˆIDK ˆU can Read Typeˆ Srcˆ Dircˆ Destˆ (Me..)

You can also Ping websites.. however, do not use “http(s)://” or “www.”

End-Of-Doc

Coming Soon: -> Displaying output to local webhost (Flask/Django) -> Changing Filters from local webhost -> Creating profile of ‘Target IP’