More Rules

ICMP

In /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.


# Any WebReturn..
alert icmp any any -> $HOME_NET any (msg: "[ANY]:[ICMP]: "; sid: 10000014; rev: 1;)
```

SSH

Add this to the /etc/snort/rules/local.rules..

```
alert tcp any any -> $HOME_NET 22 (msg: "[SSH-Auth]: ", sid: 1000002; rev: 1;)
```

The file will automatically link the new rules to the config

ˆ Now to test this, You will need to set up your own ssh, and connect to it via some other machine.. You can read these steps in 'docs/install/install_ssh.md'

If you got it right, (and figured out the ufw) you should have seen something like:

```
04/29-08:13:08.602737  [**] [1:1000002:1] [SSH-Auth]:  [**] [Priority: 0] {TCP} 192.168.0.10
04/29-08:13:09.544379  [**] [1:1000002:1] [SSH-Auth]:  [**] [Priority: 0] {TCP} 192.168.0.10
04/29-08:13:09.662606  [**] [1:1000002:1] [SSH-Auth]:  [**] [Priority: 0] {TCP} 192.168.0.10
04/29-08:13:09.669397  [**] [1:1000002:1] [SSH-Auth]:  [**] [Priority: 0] {TCP} 192.168.0.10
04/29-08:13:09.669767  [**] [1:1000002:1] [SSH-Auth]:  [**] [Priority: 0] {TCP} 192.168.0.10
04/29-08:13:09.670168  [**] [1:1000002:1] [SSH-Auth]:  [**] [Priority: 0] {TCP} 192.168.0.10
04/29-08:13:09.670547  [**] [1:1000002:1] [SSH-Auth]:  [**] [Priority: 0] {TCP} 192.168.0.10
```

HTTP

In /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.


# Any WebReturn..
alert icmp any any -> $HOME_NET any (msg: "[ANY]:[ICMP]: "; sid: 10000014; rev: 1;)

# FTP/SSH Connection Attempt: (Regardless of Success)
alert tcp any any -> $HOME_NET $SSH_PORTS (msg: "[SSH-Auth]: "; sid: 1000002; rev: 1;)

# HTTPS..
# Request:
alert tcp $HOME_NET any -> any $HTTP_PORTS ( msg: "[HTTP_REQUEST]: "; flow: to_server,estabL

# Response:
alert tcp $HOME_NET any -> any $HTTP_PORTS (msg: "[HTTP_RESPONSE]: "; flow: to_server, estab
```

^ If you have better rules than this.. plz help..

Any way, from here you can run:

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

And after opening a webpage, you should get something like this:

```
04/29-14:24:47.408912  [**] [1:100000003:0] [HTTP_REQUEST]:  [**] [Priority: 0] {TCP} 192.16
04/29-14:24:50.878577  [**] [1:100000003:0] [HTTP_REQUEST]:  [**] [Priority: 0] {TCP} 192.16
```

End-Of-Doc

Next: Implement this on a Django Project... "add-to-django.md"