

# Lab 4 - Monitoring Traffic With Snort

The objective of this lab is to develop an understanding of methods of detecting network events via developing Snort signatures.

## Preparing for the lab

In order to properly perform this lab you will need a working installation of snort on your virtual servers. You can easily install snort via the terminal with:

```
sudo apt-get install snort
```

## Helpful Hints and Resources

There are quite a few resources available to help work with snort, a few notable ones are:

- The Snort homepage
- The Snort Manual - Writing Snort Rules
- Intrusion Detection with Snort (Rafeeq Ur Rehman) - Sample Chapter - Working with Snort Rules - Click on Sample Chapter
- The previous class lectures

Snort command line options:

```
-d          - Show Application Data
-e          - Show Ethernet Information
-v          - Show Verbose Information (View data on the console)
-l <directory> - Save information to a specific directory for later processing
-r <file>    - Reprocess information from a specific file
-i <interface> - Specify interface from which to collect
-c <file>    - Specify rule definition file
```

Example of running snort using the device ens160

```
sudo snort
```

Or

```
sudo snort -dev -i ens160
```

If you need help finding the networking device that you are using try:

```
ifconfig -a | grep -i ethernet
```

```
Tilix: Default
1: orr@orr-virtual-machine: ~
orr@orr-virtual-machine:~$ ifconfig -a | grep -i ethernet
ether 00:0c:29:4a:99:93 txqueuelen 1000 (Ethernet)
```

If that doesn't work, try running

```
dmesg | grep -i eth
```

```
Tilix: Default
1: orr@orr-virtual-machine: ~
orr@orr-virtual-machine:~$ dmesg | grep -i eth
[ 1.273382] vmxnet3 0000:03:00.0 eth0: NIC Link is Up 10000 Mbps
[ 1.297888] vmxnet3 0000:03:00.0 ens160: renamed from eth0
```

**Note:** In Ubuntu, the Snort install may start up a Snort daemon by default, to ensure that only one instance of Snort is running, before you start the lab run the following from the command line to stop any other occurrences of Snort.

```
sudo service snort stop
```

**Instructor Note:** Snort should work out of the box for them within the virtual environment

## Thoughts on Testing

Snort will allow you to test the configuration file, a nice way to verify that you haven't broken things. **Note:** In this lab we are editing the local.rules file, but if you review the main snort.conf file you will see that there are many settings that you should pay attention to.

```
sudo snort -Tc /etc/snort/snort.conf
```

```
Tilix: Default
1: orr@orr-virtual-machine: ~
Using ZLIB version: 1.2.11

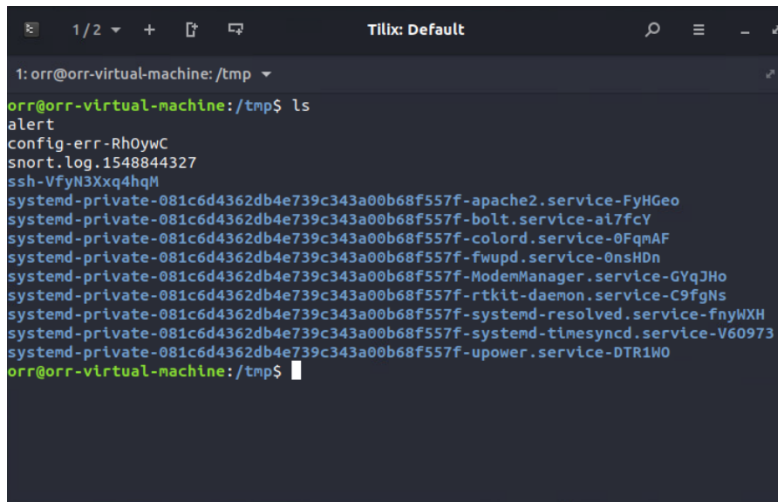
Rules Engine: SF_SNORT_DETECTION_ENGINE Version 2.4 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_DCERPC2 Version 1.0 <Build 3>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_SDF Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>

Snort successfully validated the configuration!
Snort exiting
```

To run snort so that the alerts and capture are stored to /tmp, run:

```
sudo snort -l /tmp/ -b -c /etc/snort/snort.conf
```

This will create a `/tmp/alert` and `/tmp/snort.log.XXXXXX`. If your alert successfully works it will be visible in `/tmp/alert`.



```
1: orr@orr-virtual-machine: /tmp ▾
orr@orr-virtual-machine:/tmp$ ls
alert
config-err-Rh0ywc
snort.log.1548844327
ssh-VfyN3Xxq4hqM
systemd-private-081c6d4362db4e739c343a00b68f557f-apache2.service-FyHGeo
systemd-private-081c6d4362db4e739c343a00b68f557f-bolt.service-a17fcY
systemd-private-081c6d4362db4e739c343a00b68f557f-colord.service-0FqmAF
systemd-private-081c6d4362db4e739c343a00b68f557f-fwupd.service-0nsHDn
systemd-private-081c6d4362db4e739c343a00b68f557f-ModemManager.service-GYqJHo
systemd-private-081c6d4362db4e739c343a00b68f557f-rtkit-daemon.service-C9fgNs
systemd-private-081c6d4362db4e739c343a00b68f557f-systemd-resolved.service-fnyWXH
systemd-private-081c6d4362db4e739c343a00b68f557f-systemd-timesyncd.service-V60973
systemd-private-081c6d4362db4e739c343a00b68f557f-upower.service-DTR1W0
orr@orr-virtual-machine:/tmp$
```

## Questions

For all problems below, provide the respective answers to all questions asked, the Snort Rule you created, and a copy of the alert that was produced.

1 What does the following Snort rule do?

```
alert tcp any any -> any any (msg:"FoundIt!";content:"Search Phrase";sid:2000001;rev:1;)
```

- **Note:** Snort requires that a Snort ID (sid) be declared in the rule, and a rule revision (rev) is suggested.

2. Edit the file `/etc/snort/rules/local.rules` and create a rule that will trigger when someone views your webpage **from within of 10.10.x.x**. Lets install and use lynx to surf the web from within the terminal:

```
sudo apt-get install lynx
```

Use lynx to visit the web pages of other students in the class, When your page is visited your alert should trigger. Alerts and logs will be stored to `/tmp` if you run the line above described in testing , otherwise expect alerts to appear in `/var/log/snort`.

- **Note:** If you are using the default rule set, you probably will not see the alert triggered when you visit the website yourself, have your neighbor check.
- **Note:** If you are not receiving any alerts add the **-k none** option on the command line.
- **Note:** For your rule numbering, use your alpha as the basis, so 7999901 would be a good name for m209999 and rule #01, this will allow you to share rules later on.

3. Make a second web traffic rule that triggers on web traffic coming from outside of 10.10.x.x.

4. Snort has installed a large number of community rules in `/etc/snort/rules`. Take a look at the **telnet.rules** files. Describe what the first rule is doing?

5. Look through the rules in `/etc/snort/rules`, this is the standard snort ruleset that is provided for free, and probably forms the basis of many Network Intrusion Detection Systems. Knowing this, if you were an attacker why would you want to track the free, community, and paid editions of Snort rules?

6. Since you have an ssh server on your virtual machine create an alert that is triggered when someone attempts to connect.
7. Review the ICS-CERT (Heartbleed) website and implement their signatures. Why is it important to look for current hot topic vulnerabilities?
8. Create a rule that will detect a ping from targeted at your the virtual machine, ensure that it only detects inbound pings! **What is your rule**, and **what was logged?**. Work with another student and run nmap scans across the network, do you see their scans, what alerts are triggered? Is it possible to make snort rules that would detect scanning in the fashion that we did in the last lab with tcpdump?

## What to submit

When you have completed the lab **post all requested materials to your webpage**. Then, submit the link via email to your Professor.

The email subject line should be SY402 [Section Number] Lab [X]: Title of Lab (e.g., SY402 1111 Lab 4: Monitoring Traffic With Snort). Email sent with a different subject line will reduce the overall grade by 5 points.

The web page link(s) should include:

1. (Attach) your local.rules file (this is the file you should have been editing...)
2. (Attach) the output of any requested search and your answers to the above questions (as a .txt file)