Lab 5 - Monitoring Traffic II

The objective of this lab is to develop snort signatures that will trigger an action.

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

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 occurances of Snort.

```
sudo service snort stop
```

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
```

Note: if you receive an afpacket error, this is ok, you should still be able to use the daq features.

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**.

DAQ issues?

If you experience any issues with DAQ (which is used for processing PCAP and inline operations) then perform the following. To install DAQ,

```
sudo apt-get install build-essential libpcap0.8-dev libpcre3-dev bison g++ flex ruby make au
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
tar xpf daq-2.0.6.tar.gz
cd daq-2.0.6
./configure
make
sudo make install
```

And make the appropriate changes in **/etc/snort/snort.conf**, add the following to the appropriate section (around line 168):

```
config daq: afpacket
config daq_mode: passive
config daq_dir: /usr/local/lib/daq
```

Note: Perform these actions **only** if you are experiencing issues with error messages specifying daq.

Problems

1. Read Intrusion Detection with Snort (Rafeeq Ur Rehman) - Sample Chapter - **Working with Snort Rules - Click on Sample Chapter**

2. Read Chapter 2 of the **Guide to Intrusion Detection and Prevention Systems** NIST Special Publication 800-94. Discuss the differences between the three *Common Detection Methodologies*.

3. Edit your snort.conf file, configuring all of the necessary parameters, such as **HOME_NET** and define the servers for which you already know the types.

4. Using the default rules that came with the snort install, have a neighbor scan your machine using the following nmap commands. Review the alerts that are created. Were the nmap scans detected?

```
nmap -sP 10.10.2.xx
nmap -A 10.10.2.xx
nmap -O 10.10.2.xx
nmap -sV 10.10.2.xx
```

5. Now add the Emerging Threats scan rules to your local rules file. and perform the same actions, Which of the Emerging Threat Rules were triggered?

- **Instructor Note: The following question was removed in 2018**

  Since we are not using our virtual machines as routers, we do not use snort in an *in-line* fashion where we could easily drop packets as they move between interfaces. **But** we do have these nice logs, and ubuntu does have a firewall... Write a script that reads the alerts file and creates a firewall rule (ubuntu uses the **ufw** firewall) to block all traffic from the hosts that initiate a scan against the machine. **Note:** while not required for this assignment, I would recommend that you code your program so that it unblocks hosts after approximately 15 minutes.

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 5: Monitoring II). 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 and snort.conf
2. (Attach) the output of any requested search and your answers to the above questions (as a .txt file)