Testing and Documentation

## Intrusion and Detection system setup and Tuning

After Creating downloading and creating rules and log now is the time to test my rules and see if they work and will detect the signatures of my attacker machines. I began with the easy scans with a Nmap scan. This showed the active and was logged and then opened in Wireshark and displayed the data. This let me know my first rule had worked. I then went on to test my other rule by using the ping command on my kali machine and to stop it after a few pings with control C. On my Ubuntu it displayed the message It is done this was the first rule and the message was there to show that this rule worked and picked up the intrusion. I did the next with the SSH rule and got the same results, the GitHub rule was next this did not work because I did not know about the content needed but this help from YouTube, I got this rule to work. Then came the final test the DOS attack, I started by switching both machines to promiscuous mode to allow the attack to happen, at first nothing register and got an unable to exploit on my Metasploit I realized that port 80 wasn’t open I tried on another port still nothing, I then realized that I was on the incorrect mode and switch to the DOS mode and ran the exploit this time it show the data and got my message at this time I new my IDS/IPS was up and running and work as it should I then went and check the data that was log after each attempt in Wireshark for logs had to run command to unlock since only admins can open. Below are the commands used.

Commands Ubuntu:

Sudo snort -l /home/log/ -c snort.conf -A console -I enp0s3

-This command was used for the Nmap, Ping, ssh, and GitHub attempts

Sudo snort -de -l /home/log/

* This was used to put snort in DOS mode and record the date to the log when the dos attack accorded.

Sudo Wireshark

-open Wireshark

Sudo chmod -v -R 777 home/log/log name

Open Firefox and went to GitHub for internet exploit.

Kali:

Ping 10.0.2.15

Nmap 10.0.2.15

Metasploit:

Use auxiliary/dos/tcp/synflood.

Show options.

Set RHOST <10.0.2.15>

Exploit

CTRL C