Implementation Stage:

In the implementation stage I began with creating my Virtual Machine, I went to Ubuntu to get the operating system I was going to use in my virtual machine for my victim machine and use my already installed kali and Metasploit machines as my attackers. I opened the VM software and installed my Ubuntu operating system. From Here I opened the terminal and update the system and upgraded the software. I then install the net-tools this I needed to find my ip address for my virtual machine this was 10.0.2.15 and enp0s3 this is important cause Snort will require this. I then installed Snort and set up the configuration request at time of download. I then opened snort conf to setup my network the rest of the way. This led to the first test with an Nmap scan to see if Snort was working correctly. From here I created rules in the local.rules setting this where you want to set up your own rules see local rules below for rules created. Once all my rules have been created and setup scanning, internet detection and pings, and a Dos attack I when into the testing stage to see if my rule where successful along with creating a log to save scan and downloading Wireshark to view logs. See below for all coding used for installation.

snort local.rule:

1. Alert icmp any any -> $HOME\_NET any (msg:”it is done”; sid:90001; rev:1)

-This rule displays the message it is done when a ping is done on the network.

1. Alert tcp any any -> any any (msg: “GitHub is being accessed;” content: “github.com”; sid:90004;)

- “This will display the massage GitHub is being accessed when trigger.”

3. Alert tcp any any -> $HOME\_NET any (msg:”SSH Auth attempt”; sid:90002; rev:1)

-this rule will alert to an SSH attempt

4.Alert tcp any any -> $HOME\_NET 80 (msg:” DOS attack is happening”; sid:90005; rev:1)

-This will display when a DOS attack happens

Installation:

Open virtual box

Create a new machine.

Install Ubuntu operating system.

Open terminal

Type below for setup.

Sudo apt update (to update the system and security)

Sudo apt upgrade (to upgrade software)

Sudo apt install snort (install snort)

Sudo cd /etc/snort/rules (to see snort rules)

/etc/snort/rules# nano local.rules (opens local rules so you can enter alerts)

Sudo snort -l /home/log -A console -c /etc/snort/snort.conf -i enp0s3 (this starts the console)

Sudo snort -de -l /home/log/ -this runs snort in DOS mode

Sudo snort -v : this runs snort in sniffer mode.

Mkdir log (creates a log directory in the home folder)

Sudo apt install Wireshark (installs Wireshark)