Snort Process

Install Snort

1. Snort was not available for install on the Fullstack Kali distribution, so Kali 2020 was needed for the install.
2. In the command line, type (without quotes) “apt install snort”
3. Snort will download, and will be available for use afterwards

Set up Rules

1. In Kali command line, type (without quotes) “touch fullstack.rules”
2. Further, type “nano fullstack.rules”
3. In the text editor, insert the snort rules to alert for pings:
    - First field is “alert” to generate an alert
    - Second field is external network, which for this example is set to “any”
    - Third field is external port, which for this example is set to “any”
    - Type in an arrow “->” to point to the home network
    - Fourth field is the home IP address, which I specified
    - Fifth field is home port, which for this example is set to “any”
    - The sixth field, the message and rule ID are set in parenthesis - It reads (msg: “Kali has been pinged;sid:1000001)
    - The rule should ultimately read as “alert any any -> 192.168.56.108 any (msg:”Kali has been pinged”;sid:1000001)”
4. Exit the text editor and save the file

Set up Wireshark on Kali machine

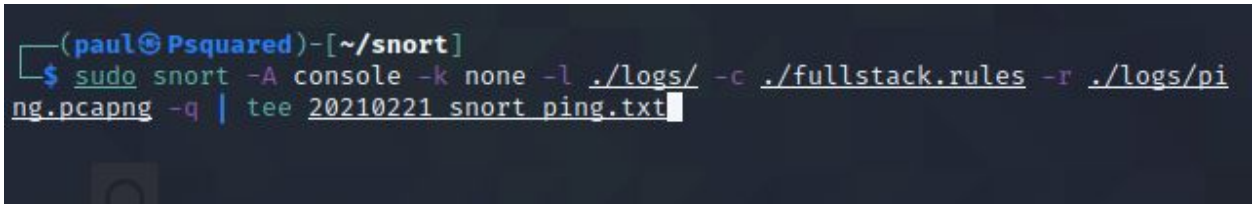
1. Set up Wireshark to listen for packet traffic on the eth1 network, as the ping will come from metaspolitable2, which is on the Host Only network.
2. Start listening for packet traffic before proceeding to ping from metasploitable2

Ping from metaspolitable2

1. In the command line in metasploitable2, type “ping 192.168.56.108”
2. After some pings have completed, ^C to end the process

Capture and Save Traffic

1. In Kali, stop the listening in Wireshark, and save the file as the filename of your choice in /snort/logs as a pcapng file.
2. From the command line, run snort to obtain log of the network traffic and any alerts that came through:



- Snort should be running, for this example, on console.
- Set -k to none, as a checksum mode is not being specified
- The log folder is ./logs
- The rule document is called out with -c
- Snort should read ./logs/ping.pcapng, called out using -r operator
- The output is condensed using -q

The output is expected to display all of the alerts resulting from the ping. See reference screenshot below.