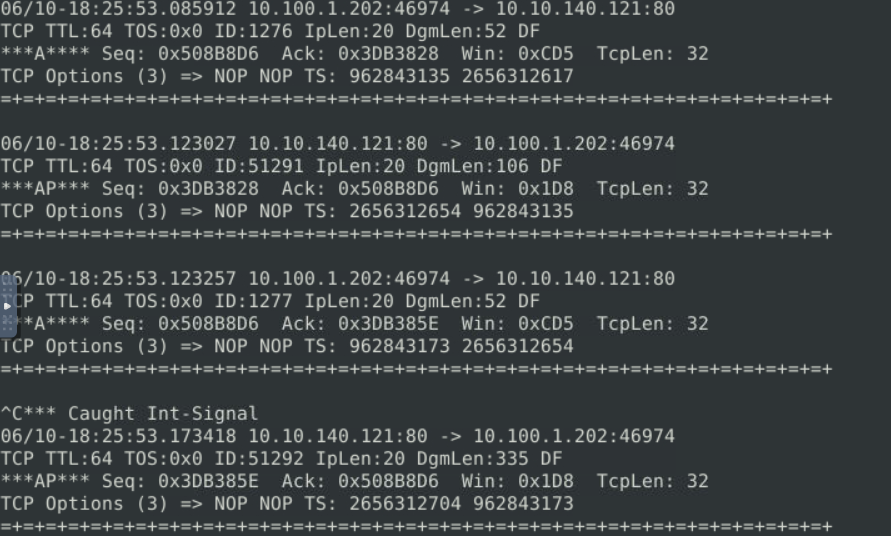
**A guide to using open-source tool Snort**

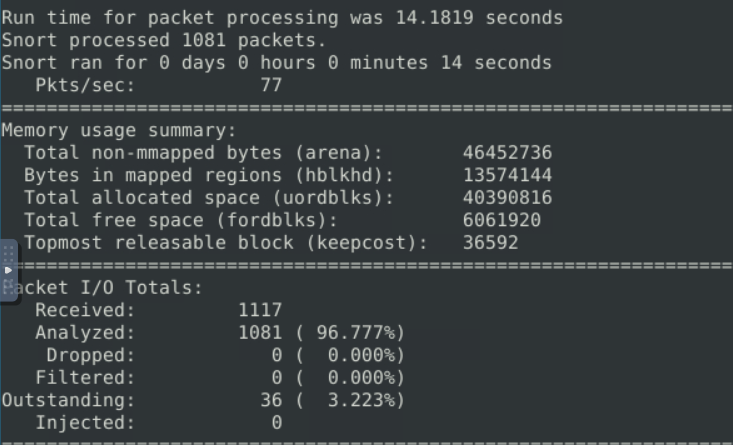
Snort is an open source, Linux tool that allows you to monitor/log network traffic, and/or be used as an IDS (intrusion detection system). The packet sniffer tool is helpful if you want to watch the traffic on the network, similar to Tcpdump. The IDS is similar to a firewall, but only sends alerts based on preconfigured or custom rules. Snort has different parameters you can use depending on the output you want such as -v for verbose, -e to display link layer headers, and -d to display packet data (use command man snort for more information)

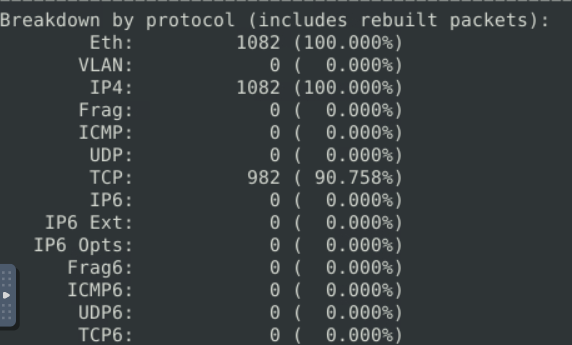
**Packet Sniffer Mode**

Snort in Packet Sniffer mode after running the command snort -v -c /etc/snort/snort.conf



It gives the source and destination IP address with ports, an ID number, and other packet information for network traffic.

Here is an example of the results from running Snort in Packet Sniffer mode.

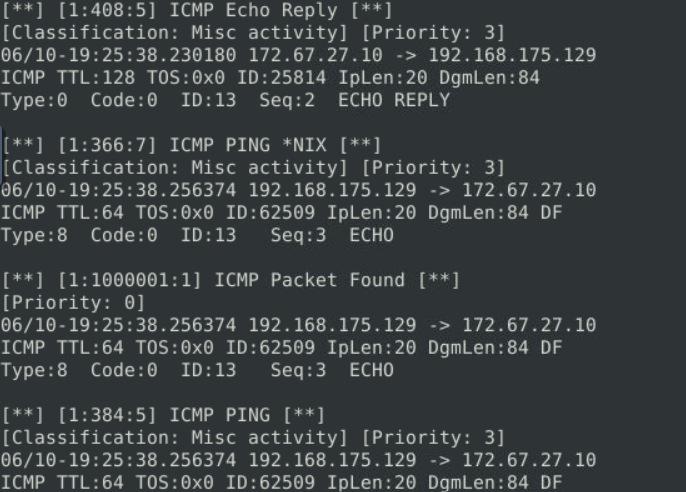
Snort breaks down results from Packet Sniffer mode by protocol.

Here we can see Ethernet was used with IPv4 and 90% Transmission Control Protocol.

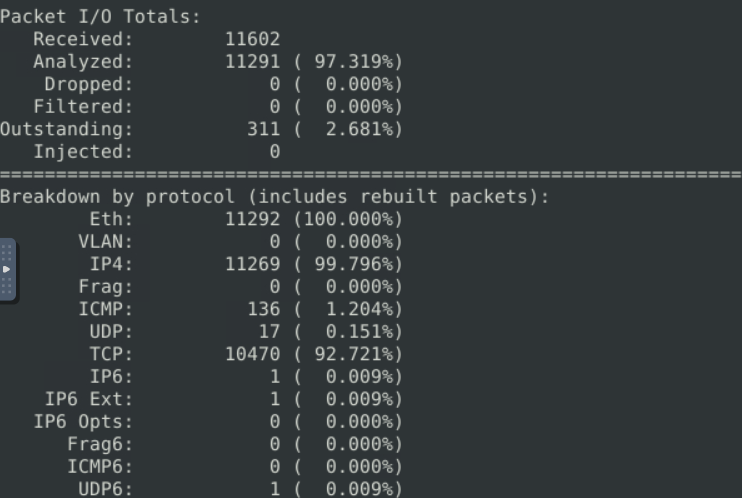
You can then send those results into a file you can create and name with the parameter -l. Logs can be found in the /var/log/snort folder. Opening the file with Wireshark allows you to filter traffic based on communication type or information in the packets (keywords, websites, etc).

**IDS Mode**

Running Snort in IDS mode will monitor network traffic and send alerts based on preconfigured rules (you can also create custom rules). These alerts are then sent to /var/log/snort. Priority is ranked from 1-4 with 1 being the most severe alert.

Snort in IDS mode after running: sudo snort -c /etc/snort/snort.conf -A full

Here we have the source and destination IP addresses, protocols (ICMP) with low priority alerts.

Snort in IDS mode gives packet statistics after running similar to Packet Sniffer modeHere we have a mix of TCP, UDP, and ICMP.

Snort in IDS mode provides alerts statics, and allows everything (DETECTION only).