**Snort Challenge - Live Attacks**

Snort Challenge - Live Attacks

Scenario 1 | Brute-Force – Proof of Concept

1. Run snort in logger mode

sudo snort -dev -l .

run this for couple of minutes and stop the snort

By analyzing the snort.log generated

sudo snort -r snort.log.1687057444

we can find there most of the connection is on port 80 and port 22.

Further analyses

sudo snort -r snort.log.1687057444 'port 80'

sudo snort -r snort.log.1687057444 'port 22'

sudo snort -r snort.log.1687057444 'port 22' -n 10

shows there is to-fro communication in port 22 -ssh port

1. Write snort rules in

sudo vim /etc/snort/rules/local.rules

rule- drop any 22 <> any any (msg: "ssh" ; sid:1000001; rev:1;)

1. running snort in IPS mode

sudo snort -c /etc/snort/snort.conf -q -Q --daq afpacket -i eth0:eth1 -A full

This generated a falg.txt on the desktop with the required flag

A screenshot of a computer

Description automatically generated