Scenario 2 | Reverse Shell

1. run snort in logger mode

sudo snort -dev -l .

1. analyze the snort.log

sudo snort -r snort. snort.log.1687060965

Further on deep analyze we can find there is a lot of connection on port 444

1. write snort rules

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

snort rule – drop tcp any 4444 -> any any (msg: “reverse shell” ; sid:1000001; rev:1;)

1. run snort in IPS mode

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

This generated a flag.txt on the desktop with the required flag 2

Screens screenshot of a computer

Description automatically generated with medium confidence