# Operation Mode 2: Packet Logger Mode

-l : Logger mode, target Log, and alert output directory

-K ASCII : Log packets in ASCII format

-r : Reading option: Review the logged events in Snort

-n : Specify the number of packets to be processed or read. Snort will stop after reading the specified numbes of packets.

Snort needs root right to sniff the traffic

sudo snort -dev -l ← tells Snort where to write log output

runs the command as root

-d -e -v ← verbose

display the packet data

display the link-layer headers (TCP/IP/UDP/ICMP)

sudo snort -dev -K ASCII -l

Same but:

write logs as readable text files

sudo snort -r ###

read and handle Binary log output
if we create logs with -K Ascii, Snort will not read them!!!

-r parameter allows filter

sudo snort -r ###.log icmp
tcp
-X
'udp and port 53'

Questions

1) what is the source port used to connect port 53?

3009

2) Read to snort log file with Snort, what is the IP ID of the 10th packet?

sudo snort -r snort.log -n 10

3) what is the referrer of the 4th packet?

sudo snort -r snort.log -n 4

4) what is the Ack number of the 8th packet?

sudo snort -r snort.log -n 8

5) what is the numbes of the "TCP port 80" packets?

sudo snort -r snoft.log "tcp and port 80"

# Operation Mode 3: IDS/IPS

-c: Defining the configuration file

-T: Testing the ~~cof~~ configuration file

-N: Disable logging

-D: Background Mode

-A: Alert Modes:

Full → all possible information about the alert

Console → fast style alerts on the console screen

cmg → CMG style, Basic header details with payload in hex and text format

None → Disabling Alert

-D: Background mode means:

→ Snort detaches from the terminal
→ We get our shell prompt back immediately
→ Snort continues running until stopped
→ Output usually goes to log files, not in our screen

Once we are in background mode, and want to check the corresponding process.

```
ps -e -f | grep snort
```

- `ps` — shows running processes
- `-e` — include all processes on the system
- `-f` — show full format details
- `| grep snort` — filter snort

To stop the background mode.

```
sudo kill -9 <pid>
```

- `-9` — hard stop (optional)

-A:

-A console : fast style alerts on the console screen

-A cmg: Basic headers details with payload in hex and text format

-A full: all possible information about the alert.

-A fast: fast mode, shows the alert message, timestamp, source, destination IP, port number

-A none: disabling alerting

# Operation Mode 4 : Pcap Investigation

-r/--pcap-single= : Read single pcap

--pcap-list="" : Read pcaps provided in command

--pcap-show : Show pcap name on console during processing

```
sudo snort -c snort.conf -q -r icmp-test.pcap
                            -A console -n 10

sudo snort -c snort.conf -q --pcap-list="icmp-test.pcap
                                         http2.pcap"
```

# Snort Rule Structure

| Action | Protocol | Source IP | Source Port | Direction | Dest IP | Dest Port | Option |
|---|---|---|---|---|---|---|---|
| Alert<br>Drop<br>Reject | TCP<br>UDP<br>ICMP<br>... | Any | Any | <> | Any | Any | Msg<br>Reference<br>Sid<br>Rev |

alert icmp any any <> any any (Msg: "ICMP Packet found"; reference: sid:####; rev:1;)

Action : alert, log, drop, reject

FTP: ~~Port~~ Protocol : TCP port 21

Filtes multiple IP ranges : [192.168.1.0/24, 10.1.1.0/24]

Exclude will get "!" in front

→ Source to destination flow
<> Bidirectional flow

SID
- <100 Reserved Rules
- 100 - 999,999 Rules came with the Build
- >=1000,000 Rules created by users

# Payload detection Rule Options

Content : specific pattern match features we create

Nocase : Disabling case sensitivity

Fast-pattern : speed up the payload search operation

## Non-Payload

ID : filtering the IP ID field

Flags : filtering the TCP flags  flags:S

F-FIN S-SYN R-RST P-PSH A-ACK U-URG

Dsize : filtering the packet payload size.

~~dest~~ dsize: min<>max;

dsize: >100

dsize: <100

sameip : filtering same source and destination ip

## Questions

1) Write a rule to filter IP ID "35369"

alert ip any any <> any any (msg: "IP ID 35369 Detected";
id:35369; sid:1000001; rev:1;)

2) Create a rule to filter packet with syn flag

alert tcp any any <> any any (msg: "SYN flag detected"; flags:S;
sid: 1000002; rev: 1;)

3) Create a rule to filter packets with Push-Ack flags

alert tcp any any <> any any (msg: "Push-Ack flag Detected";
flags: PA; sid: 1000003; rev: 1;)

4) Create a rule to filter UDP packets with the same source and destination IP

alert udp any any <> any any (msg: "same src ip and dst ip"; sameip; sid: 1000004; rev: 1;)

5) An analyst modified an existing rule. Which rule option must the analyst change the implementation?

rev

# Snort 2 operation Logic: Points to Remember

Main components of Snort:

Packet Decoder - Packet collector component. It collects and prepare the packets for preprocessing

Pre-processors - A component that arranges and modifies the packets for the detection ~~page~~ engine

Detection-Engine - The primary component that processes, dissects, and analyzes the packet by applying the rules

Logging and Alerting

Output and plugins

~~Snort Rules~~

Home_Net : where we are protecting
External_Net : external network, so we need to keep it set to 'any' or "!$HOME_NET"

Rule-Path : hardcode rule path
So_Rule-Path : rules are accompanied by registered and subscribed rules
$RULE_PATH/so_rules

PREPROC_RULE_PATH rules accompanied by registered and subsriber rules $Rule-Path/plugin_rules

IPS model works best with 'afpacket' mode

Config tags:

config daq: afpacket
→ Collects Data Acquisition Modules (DAQs) (packet in and out engine)
→ This tells Snort how to receive/send packets

config daq_mode: incline
→ Turns on incline behaviour (IPS Mode)
without incline, snort is generally passive (IDs)

config logdir: /var/log/snort
→ sets where snort writes logs/alerts

Data Acquisition Modules list:

pcap → passive sniffing

afpacket → Linux high-performance capture

ipq/nfq → Linux Netfilter queue-based incline paths

ipfw → BSD firewall/divert-based path

dump → test/replay style module

DAQ → packet in and out layer

↳ It answers "How does Snort get packets and drop"

Think DAQ as the adapter between Snort and the network

mechanism/path for packet access

Incline Mode → Snort is placed in the traffic path and can enforce actions in real time

Operating mode where Snort can block traffic

~~Configuration~~