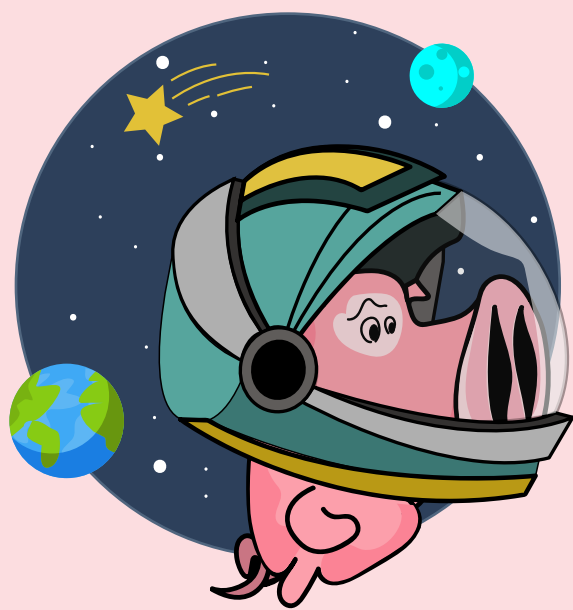


SNORT 101

10 10
1110
0101 01
01 010

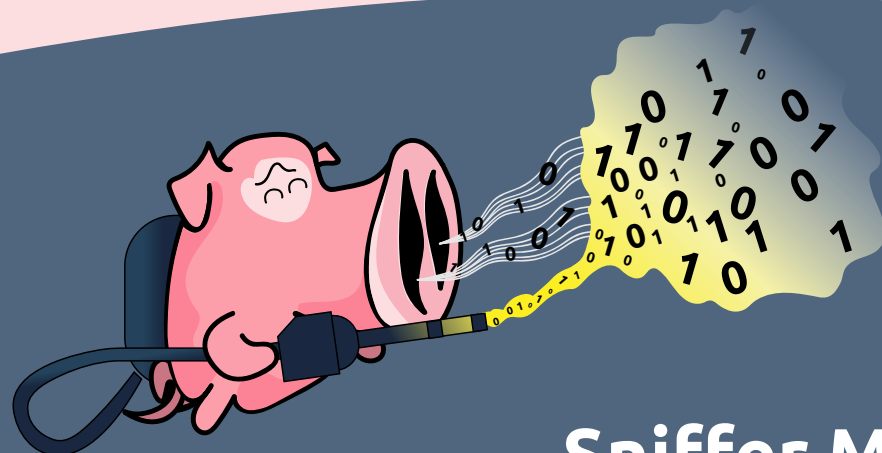


Global Commands

Display version:
Snort -V
Snort -version

Do not display the version banner:
Snort -q

Use specific inetrface:
Snort -i eth0



Sniffer Mode

Verbose mode:
Snort -v

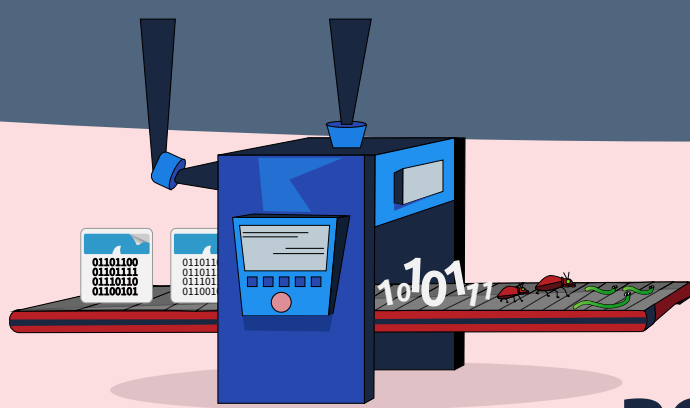
Display link-layer headers:
Snort -e

Display data payload:
Snort -d

Display full packet details in HEX:
Snort -X

Multiple flag usage. Display all packet details:
Snort -eX

Sniff "N" number of packets:
Snort -v -n 10



PCAP Processing

Process single pcap file:
Snort -c /etc/snort/snort.conf -q -r file.pcap -A console

Process multiple pcap files:
Snort -c /etc/snort/snort.conf -q --pcap-list="file1.pcap file2.pcap" -A console

Process pcaps from folder:
Snort -c /etc/snort/snort.conf -q --pcap-dir=/home/pcap-folder -A console

Show processed pcap name:
Snort -c /etc/snort/snort.conf -q --pcap-list="file1.pcap file2.pcap" -A console --pcap-show

Logger Mode

Default log path :
/var/log/snort

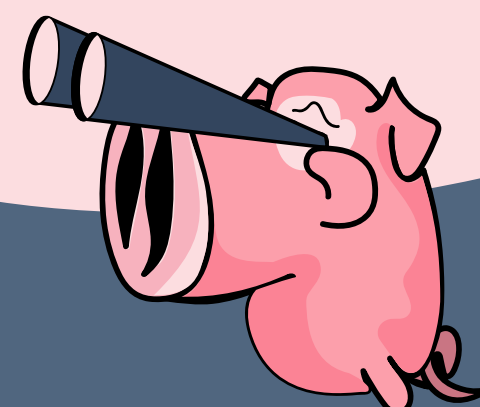
Use alternative log path:
Snort -v -l /home/username/Desktop

Log in ASCII format:
Snort -v -K ASCII

Read snort files:
Snort -v -r snort.log

Read "N" number of packets:
Snort -v -r snort.log -n 10

Filter packets with "Berkeley Packet Filters" (BPF):
Snort -v -r snort.log tcp
Snort -v -r snort.log 'udp and port 53'



Default Log path ->
/var/log/snort

IDS/IPS Mode

Use configuration file:
Snort -c /etc/snort/snort.conf

Test instance and configuration file:
Snort -c /etc/snort/snort.conf -T

Disable logging:
Snort -c /etc/snort/snort.conf -N

Run Snort in background:
Snort -c /etc/snort/snort.conf -D

Alert mode 1 | No output:
Snort -c /etc/snort/snort.conf -v -A none

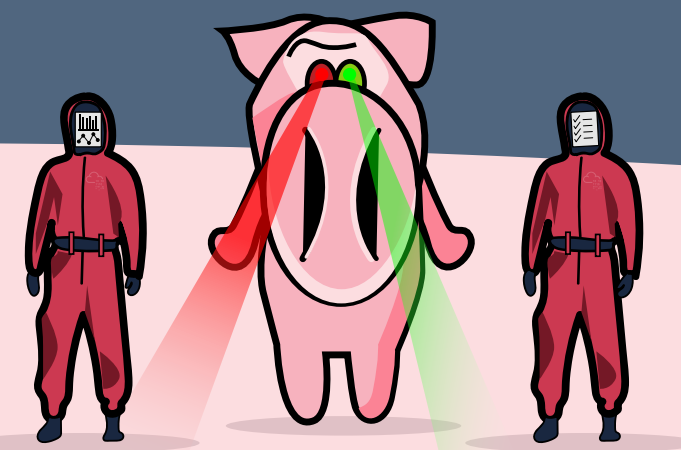
Alert mode 2 | Console output 1:
Snort -c /etc/snort/snort.conf -v -A console

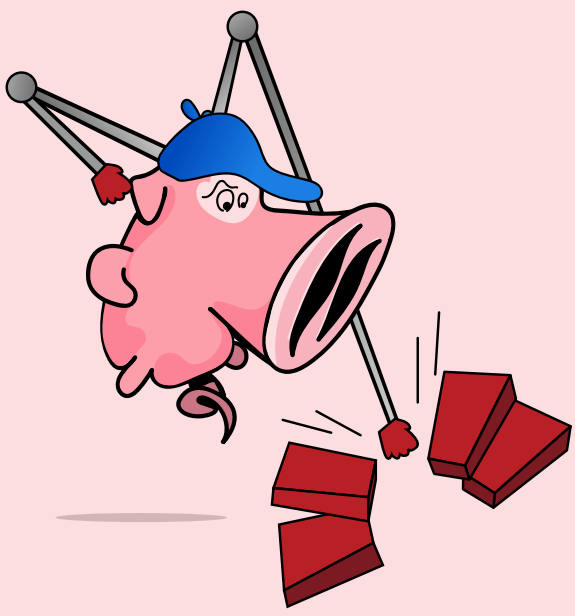
Alert mode 2 | Console output 2:
Snort -c /etc/snort/snort.conf -v -A cmg

Alert mode 3 | File output 1:
Snort -c /etc/snort/snort.conf -v -A fast

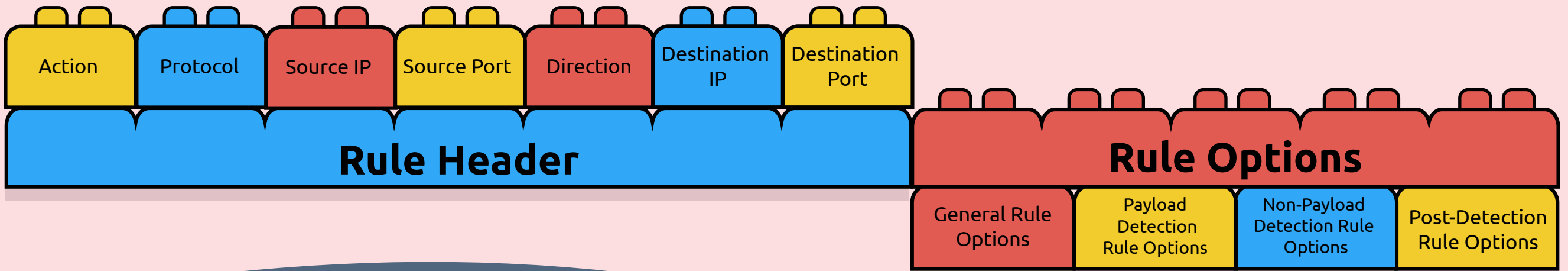
Alert mode 3 | File output 2:
Snort -c /etc/snort/snort.conf -v -A full

Use rules without configuration file:
Snort -c /etc/snort/rules/local.rules -v -A console





Snort Rule Breakdown



★ Snort rules are composed of two logical parts;

Rule Header:

This part contains network-based information; action, protocol, source and destination IP addresses, port numbers, and traffic direction.

Rule Options:

This part contains packet-based investigation details; message, reference, flow and content.

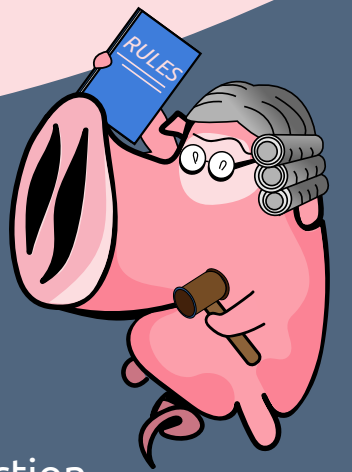
Example Rule

Alert rule for possible "Directory Traversal Attempt" detection.

```

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (
msg:"Directory Traversal Attempt!";
flow:established;
nocase; content:"HTTP"; fast_pattern; content:"| 2E 2E 2F|"; content:"/..";
session:all;
reference:CVE,XXX;
sid:100001; rev:1;)

```



RULE HEADER		Field	Value	Description
RULE HEADER		Action	alert	Action, this option tells Snort what to do in a rule match
		Protocol	tcp	Protocol to be analysed. Supported protocols: TCP, UDP, ICMP, IP.
		Source IP	\$EXTERNAL_NET	Source IP addresses.
		Source Port	any	Source ports.
		Direction	->	Direction operator. Identify the orientation of traffic.
		Destination IP	\$HOME_NET	Destination IP addresses.
		Destination Port	\$HTTP_PORTS	Destination ports.
RULE OPTIONS	GENERAL RULE OPTIONS	Message	msg	Display message for rule match.
		Reference	reference	Provide additional information or reference for the rule.
		Rule id	sid	Unique rule number.
		Revision info	rev	Revision information for the rule.
	PAYLOAD DETECTION RULE OPTIONS	Flow	flow	TCP stream direction.
		Nocase	nocase	Disable case sensitivity to enhance the content match.
		Content	content	Filter the payload data and look for an exact match.
	POST-DETECTION RULE OPTIONS	Fast-pattern	fast-pattern	Prioritise the content search to speed up the payload search. This option is required when using multiple "content" options.
		Session	session	Extract user data from TCP sessions.

