

Snort Cheat Sheet

Sniffer Mode	
Sniff packets and send to standard output as a dump file	
-v (verbose)	Display output on the screen
-e	Display link layer headers
-d	Display packet data payload
-x	Display full packet with headers in HEX format

Packet Logger Mode	
Input output to a log file	
-r	Use to read back the log file content using snort
-l (directory name)	Log to a directory as a tcpdump file format
-k (ASCII)	Display output as ASCII format

Snort Rules Format	
Rule Header + (Rule Options)	
Action - Protocol - Source/Destination IP's - Source/Destination Ports - Direction of the flow	
Alert Example	<code>alert udp !10.1.1.0/24 any -> 10.2.0.0/24 any</code>
Actions	alert, log, pass, activate, dynamic, drop, reject, sdrop
Protocols	TCP, UDP, ICMP, IP

Snort Rule Example	
<code>log tcp !10.1.1.0/24 any -> 10.1.1.100 (msg: "ftp access");</code>	

Output Default Directory	<code>/var/snort/log</code>
--------------------------	-----------------------------

NIDS Mode	
Use the specified file as config file and apply rules to process captured packets	
-c	Define configuration file path
-T	Use to test the configuration file including rules

Logger Mode command line options	
-l logdir	Log packets in tcp dump
-K ASCII	Log in ASCII format

NIDS Mode Options	
Define a configuration file	-c (Configuration file name)
Check the rule syntax and format for accuracy	-T -c (Configuration file name)
Alternate alert modes	-A (Mode : Full, Fast, None ,Console)
Alert to syslog	-s
Print alert information	-v
Send SMB alert to PC	-M (PC name or IP address)
ASCII log mode	-K
No logging	-N
Run in Background	-D
Listen to a specific network interface	-i