Helper Document

sudo password:

kali

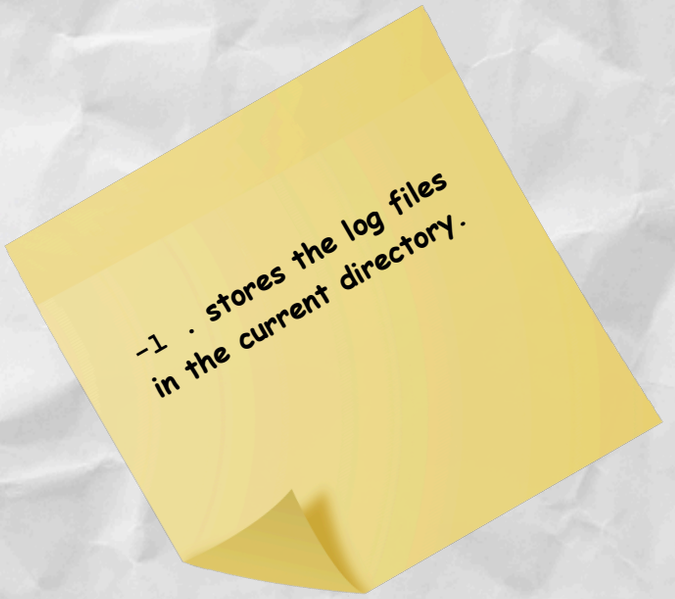
What is Snort?

Snort is an open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) used to monitor network traffic for suspicious or malicious activity. It uses rule-based analysis to detect attacks and unusual behavior.

Key Features

- Packet Sniffer – reads network packets in real time.
- Packet Logger – records network traffic for later analysis.
- Intrusion Detection / Prevention – uses rules to detect and optionally block threats.
- Flexible Rule Language – customizable rules for specific security needs.

You will be using sudo in this task.
Sudo is a Linux command that allows a permitted user to temporarily execute commands with elevated privileges, typically those of the superuser (root). Use password *kali*.



Snort Commands

Global commands

-V	This parameter provides information about your instance version.
-c	Identifying the configuration file
-T	Snort's self-test parameter allows you to test your setup with this parameter.
- q	Quiet mode prevents Snort from displaying the default banner and initial information about your setup.

PCAP Processing

-r / --pcap-single=	Read a single pcap
--pcap-list=""	Read pcaps provided in command (space separated).
--pcap-show	Show pcap name on console during processing

IDS/IPS Mode

-c	Defining the configuration file.
-T	Testing the configuration file.
-N	Disable logging.
-A	Alert modes; **full**: Full alert mode, providing all possible information about the alert. **console**: Provides fast style alerts on the console screen **fast**: Fast mode, shows the alert message, timestamp, source, and destination ip along with port numbers. **cmg**: CMG style, basic header details with payload in hex and text format. **None**: Disabling alerting.
-Q --daq afpacket	Activate IPS mode.

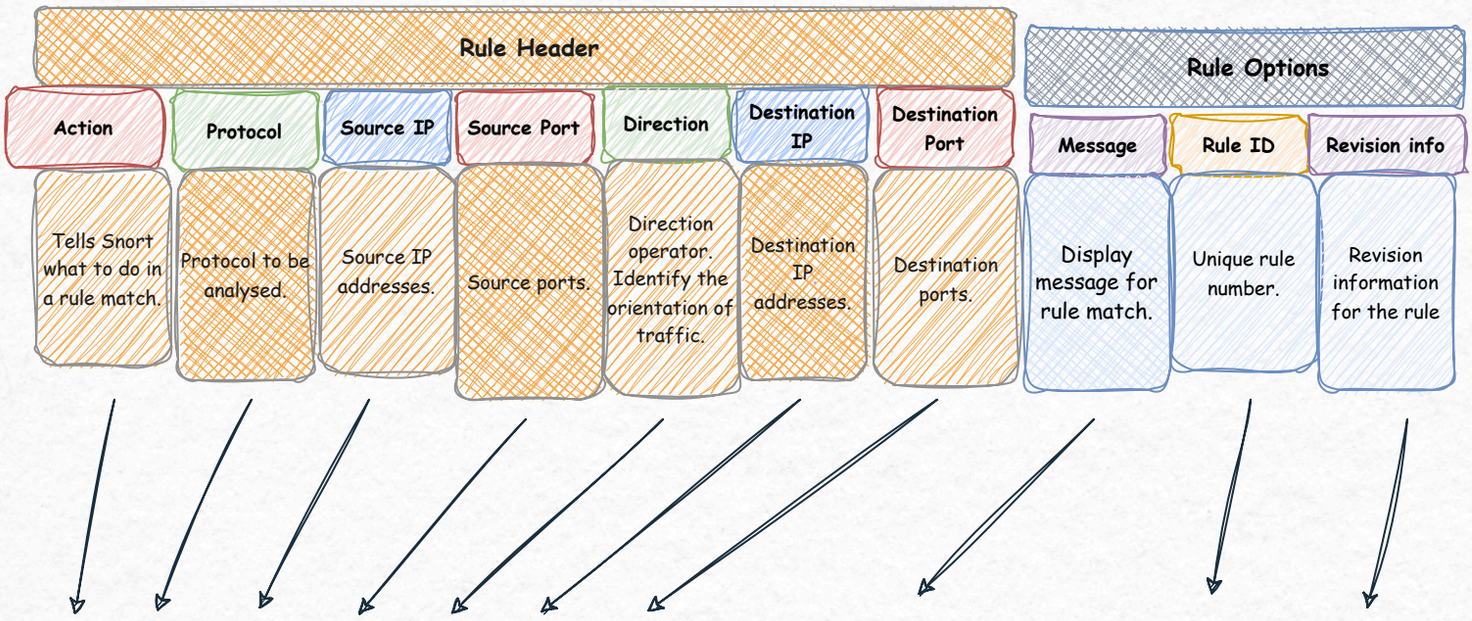
Sniffer Mode

-v	Verbose. Display the TCP/IP output in the console.
-d	Display the packet data (payload).
-e	Display the link-layer (TCP/IP/UDP/ICMP) headers.
-X	Display the full packet details in HEX.
-i	This parameter specifies which network interface Snort should listen on. If the system has multiple interfaces, it allows you to select the exact one to capture traffic from.

Logger Mode

-l	Logger mode, target log, and alert output directory. Default output folder is /var/log/snort
-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 number of packets.

Snort Rules



alert tcp any any <> any any (msg: "Hello!"; sid: 10001; rev:1;)

Run your rule like this:

Run in sudo mode

Path to .rule file

To use IPS you have to be between two network interfaces.

Print to console

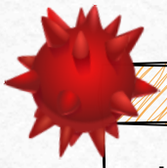
```
sudo snort -c /home/kali/Desktop/snort.rules -Q --daq afpacket -i br0:eth0 -A console
```

Snort IPS mode is activated with the -Q- - daq afpacket parameters.

Note!

Snort can be run using only rules, without a configuration file. This mode is useful for testing user-created rules, but it may result in reduced performance.

```
sudo snort -c /etc/snort/rules/local.rules -A console
```



Action	
alert	Generate an alert and log the packet.
log	Log the packet
drop	Block and log the packet
reject	Block the packet, log it, and terminate the packet session.

Protocol	
IP	Internet Protocol: responsible for addressing and routing packets across networks.
TCP	Transmission Control Protocol: used by higher-level protocols such as HTTP, POP3, IMAP, and SMTP.
UDP	User Datagram Protocol: used by services like DNS and by real-time applications such as audio/video conferencing and broadcast traffic.
ICMP	Internet Control Message Protocol: used for diagnostics and network control tasks, such as ping and traceroute.

Direction	
->	Source to destination flow.
<>	Bidirectional flow
	Note that there is no "<-" operator in Snort.

Rule Options	
msg	Once the rule is triggered, the message will appear.
sid	Snort rule ID. (must be unique)
rev	The ' Rev' option is only an indicator of how many times the rule has undergone revisions.

You can enter any number here, but remember that sid must be unique.

(msg: "ICMP Packet Found"; **sid: 100001**; **rev:1**;)

IP address	
IP	A numerical label such as 192.0.2.1 that is assigned to a device connected to a computer network.
any	Matches any IP address or port.

Port	
port	A numerical identifier used in networking to specify a particular service or application on a device.
any	Matches any IP address or port.

If Snort crashes or becomes unresponsive, open a new terminal and stop it using the `kill` command:

sudo kill -9 <PID>