Snort - TryHackMe
Snort

Intrusion Detection System

IDS is a passive monitoring solution for detecting possible malicious activities/patterns, abnormal incidents, and policy violations. It is responsible for generating alerts for each suspicious event.

There are two main types of IDS systems:

- **Network Intrusion Detection System (NIDS)** - NIDS monitors the traffic flow from various areas of the network. The aim is to investigate the traffic on the entire subnet. If a signature is identified, **an alert is created**.
- **Host-based Intrusion Detection System (HIDS**) - HIDS monitors the traffic flow from a single endpoint device. The aim is to investigate the traffic on a particular device. If a signature is identified, **an alert is created**.

Intrusion Prevention System (IPS)

IPS is an active protecting solution for preventing possible malicious activities/patterns, abnormal incidents, and policy violations. It is responsible for stopping/preventing/terminating the suspicious event as soon as the detection is performed.

There are four main types of IPS systems;

- **Network Intrusion Prevention System (NIPS)** - NIPS monitors the traffic flow from various areas of the network. The aim is to protect the traffic on the entire subnet. If a signature is identified, **the connection is terminated**.
- **Behaviour-based Intrusion Prevention System (Network Behaviour Analysis - NBA)** - Behaviour-based systems monitor the traffic flow from various areas of the network. The aim is to protect the traffic on the entire subnet. If a signature is identified, **the connection is terminated.**
- **Wireless Intrusion Prevention System (WIPS)** - WIPS monitors the traffic flow from of wireless network. The aim is to protect the wireless traffic and stop possible attacks launched from there. If a signature is identified, **the connection is terminated.**
- **Host-based Intrusion Prevention System (HIPS)** - HIPS actively protects the traffic flow from a single endpoint device. The aim is to investigate the traffic on a particular device. If a signature is identified, **the connection is terminated.**

Detection/Prevention Techniques

There are three main detection and prevention techniques used in IDS and IPS solutions;

Technique	Approach

Technique	Approach
Signature-Based	Relies on rules that identify the specific patterns of the known malicious behaviour. This model helps detect known threats.
Behaviour-Based	Identifies new threats with new patterns that pass through signatures. The model compares the known/normal with unknown/abnormal behaviours. This model helps detect previously unknown or new threats.
Policy-Based	compares detected activities with system configuration and security policies. This model helps detect policy violations.

SNORT is an open-source, rule-based Network Intrusion Detection and Prevention System (NIDS/NIPS). It was developed and still maintained by Martin Roesch, open-source contributors, and the Cisco Talos team.

Capabilities of Snort:

- Live traffic analysis
- Attack and probe detection
- Packet logging
- Protocol analysis
- Real-time alerting
- Modules & plugins
- Pre-processors
- Cross-platform support! (Linux & Windows)

Snort has three main use models;

- Sniffer Mode - Read IP packets and prompt them in the console application.
- Packet Logger Mode - Log all IP packets (inbound and outbound) that visit the network.
- NIDS (Network Intrusion Detection System) and NIPS (Network Intrusion Prevention System) Modes - Log/drop the packets that are deemed as malicious according to the user-defined rules.

> **snort.conf:** *Main configuration file.*
> **local.rules:** *User-generated rules file.*

check for validity of Snort config file located in /etc/snort.conf

```
sudo snort -c /etc/snort/snort.conf -T
```

Various Parameters

- **-c** - Identifying the configuration file
- **-T** - Self-test parameter. Used for testing your configsnort config.
- **-q** - quiet mode.
- **-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 helps to define a specific network interface to listen/sniff. Once you have multiple interfaces, you can choose a specific interface to sniff.
- **-l** - Logger mode, target **log and alert** output directory. Default output folder is **/var/log/snort**.The default action is to dump as tcpdump format in **/var/log/snort**
- **-K ASCII** - Log packets in ASCII format.
- **-r** - Reading option, read the dumped logs in Snort.
- **-n** - Specify the number of packets that will process/read. Snort will stop after reading the specified number of packets.
- **-D** - Background mode.
- **-A** - Alert modes:
  - **full:** Full alert mode, providing all possible information about the alert. This one also is the default mode; once you use -A and don't specify any mode, snort uses this mode.
  - **fast:** Fast mode shows the alert message, timestamp, source and destination IP, along with port numbers.
  - **console:** Provides fast style alerts on the console screen.
  - **cmg:** CMG style, basic header details with payload in hex and text format.
  - **none:** Disabling alerting.

> For using snort in IDS/IPS modes run commands this:
> `sudo snort -c /etc/snort/snort.conf [params]`

Investigating PCAP files with Snort:

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.

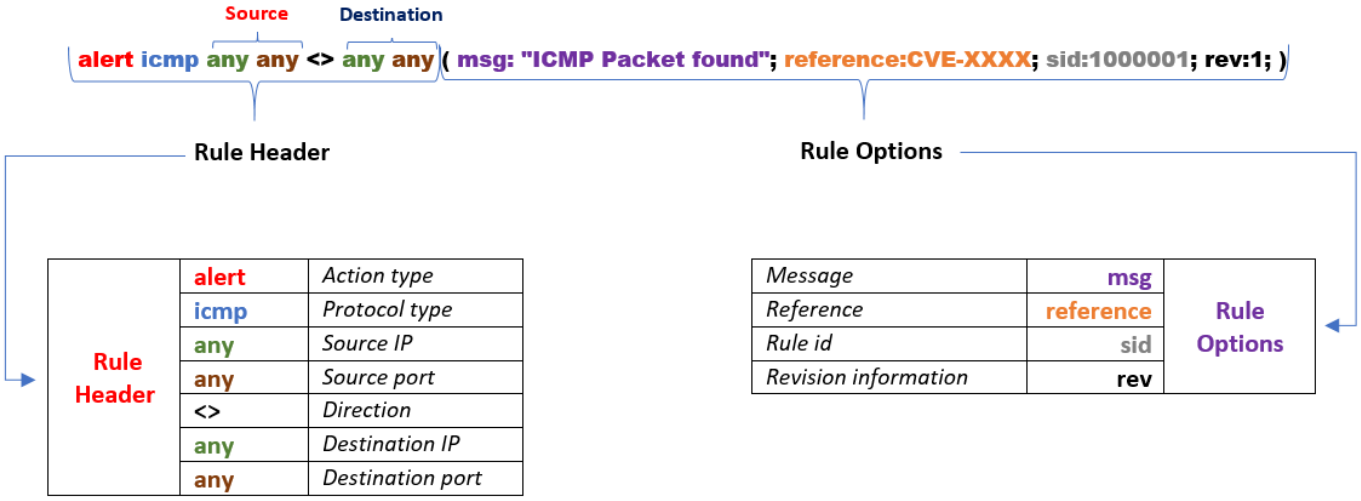
> **Example:** sudo snort -c /etc/snort/snort.conf -A full -l . --pcap-list="mx-2.pcap mx-3.pcap"

Snort Rules:

General Structure:

Action	Protocol	Source IP	Source Port	Direction	Destination IP	Destination Port	Options
Alert Drop Reject	TCP UDP ICMP	ANY	ANY	<>	ANY	ANY	Msg Reference Sid Rev
Rule Header							Rule Options

- The following rule will generate an alert for each ICMP packet processed by Snort;



Example Rules:

IP Filtering - `alert icmp 192.168.1.56 any <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

IP Range Filtering- `alert icmp 192.168.1.0/24 any <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

Filter multiple IP ranges: `alert icmp [192.168.1.0/24, 10.1.1.0/24] any <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

Exclude IP addresses/ranges - `alert icmp !192.168.1.0/24 any <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

> This rule will create alerts for each ICMP packet not originating from the 192.168.1.0/24 subnet.

Port Filtering - `alert tcp !192.168.1.0/24 21 <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

Exlcluding specific Port - `alert tcp !192.168.1.0/24 !21 <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

> This rule will create alerts for each TCP packet not originating from port 21.

Filter Port Range (Type 1) - `alert tcp !192.168.1.0/24 1:1024 <> any any  (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

Filter Port Range (Type 2) - `alert icmp any :1024 <> any any  (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

> This rule will create alerts for each TCP packet originating from ports less than or equal to 1024.

Filter Port Range (Type 3) - `alert icmp any 1024: <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

Filter Port Range (Type 4) - `alert icmp any 80,1024: <> any any (msg: "ICMP Packet Found"; sid: 100001; rev:1;)`

> This rule will create alerts for each TCP packet originating from a source port 80 and higher than or equal to 1024.

Payload Detection Rule Options:

Content: Following rules will create an alert for each HTTP packet containing the keyword "GET". This rule option is case sensitive!

- **ASCII mode** - `alert tcp any any <> any 80  (msg: "GET Request Found"; content:"GET"; sid: 100001; rev:1;)`
- **HEX mode** - `alert tcp any any <> any 80  (msg: "GET Request Found"; content:"|47 45 54|"; sid: 100001; rev:1;)`

NoCase: - Disabling case sensitivity. Used for enhancing the content searches.
`alert tcp any any <> any 80  (msg: "GET Request Found"; content:"GET"; nocase; sid: 100001; rev:1;)`

Fast_pattern: - Prioritise content search to speed up the payload search operation.
The following rule has two content options, and the fast_pattern option tells to snort to use the first content option (in this case, "GET") for the initial packet match.
`alert tcp any any <> any 80  (msg: "GET Request Found"; content:"GET"; fast_pattern; content:"www";  sid:100001; rev:1;)`

Non-Payload Detection Rule Options

ID: Filtering the IP ID Field.
`alert tcp any any <> any any (msg: "ID TEST"; id:123456; sid: 100001; rev:1;)`

Flags: Filtering the TCP flags.

- F - FIN
- S - SYN

- R - RST
- P - PSH
- A - ACK
- U - URG

```
alert tcp any any <> any any (msg: "FLAG TEST"; flags:S;  sid: 100001; rev:1;)
```

DSize: Filtering the packet payload size

- dsize:min<>max;
- dsize:>100
- dsize:<100

```
alert ip any any <> any any (msg: "SEQ TEST"; dsize:100<>300;  sid: 100001; rev:1;)
```

Sameip: Filtering the source and destination IP addresses for duplication.

```
alert ip any any <> any any (msg: "SAME-IP TEST";  sameip; sid: 100001; rev:1;)
```

> snort rules are located under /etc/snort/local.rules