📘 Snort – Intrusion Detection and Prevention System

🔹 Overview

- **Snort** is an open-source **Intrusion Detection System (IDS)** and **Intrusion Prevention System (IPS)**.
- Developed by **Martin Roesch** and maintained by **Cisco Talos**.
- Works by analyzing network traffic in real-time to detect malicious activities such as:
  - Attacks
  - Scans
  - Probes
  - Exploits

🔹 Key Features

- **Packet Sniffer** (like tcpdump).
- **Packet Logger** (saves network packets for later analysis).
- **Network Intrusion Detection System (NIDS)**.
- **Intrusion Prevention System (IPS)**.
- Uses a **rule-based language** to detect anomalies and attacks.
- Supports **real-time alerting** (console, log files, syslog, database).
- Cross-platform (Linux & Windows).

🔹 Snort Modes of Operation

1. **Sniffer Mode** → Reads network traffic and displays it on the console.

   `snort -v`

   (Verbose output of packet headers).

---

2. **Packet Logger Mode** → Logs packets to a file for offline analysis.

   ```
   snort -dev -l ./log
   ```

---

3. **Network Intrusion Detection Mode (NIDS)** → Uses rules to analyze traffic and generate alerts.

   ```
   snort -c /etc/snort/snort.conf -i eth0
   ```

---

4. **Inline Mode (IPS)** → Drops malicious packets in real-time.

- **Important Snort Commands**

Command	**Description**
snort.exe -V	Shows Snort version and build info
snort.exe -W	Lists available network interfaces on Windows
snort.exe -i 5 -c "C:\Snort\etc\snort.conf" -T	Tests configuration file on interface 5
snort.exe -i 5 -c "C:\Snort\etc\snort.conf" -A console	Runs Snort with alerts displayed on console
snort -l /var/log/snort	Specifies log directory
snort -A fast	Outputs alerts in fast mode
snort -A full	Outputs detailed alerts
snort -A console	Alerts directly to console
snort -c /etc/snort/snort.conf	Runs Snort using a config file

---

🔹 Snort Rule Structure

A Snort rule has **two parts**:

1. **Rule Header** → Defines action, protocol, source, destination.
2. **Rule Options** → Provides detailed conditions (content matching, flags, messages).

General Rule Syntax:

```
action protocol src_ip src_port -> dst_ip dst_port (options)
```

Example:

```
alert tcp any any -> 192.168.1.10 80 (msg:"Possible Web Attack"; content:"/etc/passwd"; sid:1000001; rev:1;)
```

- **alert** → Action (generate alert).
- **tcp** → Protocol.
- **any any** → Source IP & Port.
- **192.168.1.10 80** → Destination IP & Port.
- **msg** → Custom alert message.
- **content** → String to search in packet.
- **sid** → Snort Rule ID.
- **rev** → Revision number.

🔹 Snort Actions

- **alert** → Generate alert and log packet.
- **log** → Log the packet.
- **pass** → Ignore the packet.
- **drop** → Block & log (IPS mode).
- **reject** → Block and send TCP RST/ICMP error.
- **sdrop** → Block silently without logging.

🔹 Snort Configuration File

- Location: C:\Snort\etc\snort.conf (Windows) or /etc/snort/snort.conf (Linux).
- Contains:
  - Network variables (HOME_NET, EXTERNAL_NET).
  - Rule path.
  - Preprocessors.
  - Output plugins.
  - Included rulesets.

🔹 Example Usage

1. **Sniffer Mode**

   snort -v -i eth0

---

2. **Packet Logger Mode**

   snort -dev -l ./log

---

3. **Testing Configuration**

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

---

4. **Running IDS with Rules**

   snort -A console -q -c /etc/snort/snort.conf -i eth0

🔹 Snort Preprocessors

Preprocessors normalize and preprocess packets before rule-checking. Examples:

- **frag3** → Handles IP fragmentation.

- **stream5** → Handles TCP streams.
- **http_inspect** → Analyzes HTTP traffic.
- **ssl_preproc** → Monitors SSL traffic.

🔹 Snort Logging & Alerts

- Logs can be stored in:
  - Console
  - File (/var/log/snort)
  - Syslog
  - Unified2 format (for SIEM/IDS tools)

🔹 Real-World Use Cases

- Detecting port scans.
- Detecting brute-force login attempts.
- Monitoring suspicious HTTP requests.
- Detecting malware communication.
- Preventing SQL injection or XSS attacks.

🔹 Advantages of Snort

- Open-source & free.
- Highly customizable with rules.
- Active community support.
- Lightweight compared to enterprise IDS/IPS.

🔹 Limitations of Snort

- Can be resource-intensive on large networks.
- Signature-based (may miss zero-day attacks).
- Needs frequent rule updates.

References

- Official Site: https://www.snort.org
- Snort Manual: https://www.snort.org/documents
- Cisco Talos Rules: https://talosintelligence.com