Snort

## 📓 **Notes – Snort**

**Lab Name:** Snort  
**Category:** Network Security & Traffic Analysis – Notes

### **Snort Capabilities**

1. **Use Configuration Files & Rules**
   * Snort uses a **config file** (e.g., snort.conf) that loads all the rules.
   * Rules define **what traffic to alert on, log, or drop**.
   * You can customize or update rules from sources like **Emerging Threats** or **Snort community rules**.
2. **Traffic Monitoring Modes**
   * **Sniffer Mode** → Show real-time packets on console (-v option).
   * **Packet Logger Mode** → Save packets to log files for later review.
   * **NIDS/NIPS Mode** → Detect or **actively block** packets that match rules.
3. **Log Handling**
   * Logs can be:
     + Displayed on the **console**.
     + Saved to **local log files**.
     + Sent to a **remote log server** or via **email**.
   * Logs can be stored in plain text or in **unified2** format for use with other tools.
4. **Network Protection**
   * In IPS mode, Snort can **drop packets** that match rules **in real time**.
   * Useful for stopping malware, exploits, and unauthorized access.
5. **PCAP File Investigation**
   * Snort can analyze previously captured **PCAP files** (-r option).
   * Great for **incident investigation** and **offline forensic analysis**.

### **1. Introduction**

Snort is an **open-source network intrusion detection/prevention system (NIDS/NIPS)** developed by Cisco.  
It analyzes network packets in real time and detects malicious activity using a **signature/rule-based** approach.

### **2. Modes of Operation**

1. **Sniffer Mode**
   * Displays packet information directly to the console.
   * Command example:

bash

CopyEdit

snort -v

1. **Packet Logger Mode**
   * Saves packet data to a log file for later analysis.
   * Command example:

bash

CopyEdit

snort -dev -l /var/log/snort

1. **IDS/IPS Mode**
   * Detects and alerts on suspicious packets based on rule sets.
   * Can drop or modify traffic when used inline (IPS).
   * Example:

bash

CopyEdit

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

1. **PCAP Investigation Mode**
   * Reads and analyzes previously captured network traffic from .pcap files.
   * Example:

bash

CopyEdit

snort -r file.pcap

### **3. Snort Rule Structure**

A Snort rule has two main parts:

java

CopyEdit

action protocol src\_ip src\_port -> dest\_ip dest\_port (options)

Example:

css

CopyEdit

alert tcp any any -> 192.168.1.0/24 80 (msg:"Possible HTTP Exploit"; content:"/etc/passwd"; sid:1000001;)

* **Action:** alert, log, pass, drop, reject.
* **Protocol:** tcp, udp, icmp, ip.
* **Options:** conditions like msg, content, sid, rev.

### **4. Snort2 Operation Logic – Points to Remember**

* Packet capture → Decoding → Preprocessing → Detection engine → Output plugins.
* Preprocessors handle protocol normalization and anomaly detection.
* Detection engine matches packets to rule conditions.

### **5. Key Takeaways**

* Snort is versatile for **real-time monitoring** and **offline analysis**.
* Rules can be custom-written or loaded from community/professional rule sets.
* In SOC environments, Snort is often integrated with SIEM tools for correlation.

