🐍 Snort Cheat Sheet for SOC (1)

Reference ⇒ https://upcloud.com/resources/tutorials/install-snort-ubuntu/

📘 What is Snort?

Snort is a **Network Intrusion Detection System (NIDS)** used to detect and log malicious network traffic.

📁 Important Snort Files

Path	Purpose
`/etc/snort/snort.conf`	Main config file
`/etc/snort/rules/local.rules`	Custom user rules
`/etc/snort/rules/`	All rule files stored here
`/var/log/snort/`	Logs, alerts, and packet captures

⚙️ Snort Operating Modes

Mode	Command	Use
Sniffer	`snort -i eth0`	Shows packets in real-time
Packet Logger	`snort -i eth0 -l /var/log/snort/`	Saves traffic logs
NIDS (Detection)	`snort -c /etc/snort/snort.conf -i eth0`	Uses rules to alert

🛡️ Basic Snort Commands

Task	Command
Test config	`snort -T -c /etc/snort/snort.conf`
Run in alert mode	`snort -A console -q -i eth0 -c /etc/snort/snort.conf`
Read PCAP	`snort -r file.pcap -c /etc/snort/snort.conf`

Save pcap	`tcpdump -i eth0 -w out.pcap`
Analyze pcap	`snort -r out.pcap -c /etc/snort/snort.conf` -q -A console

✍️ How to Write a Custom Rule

Rule format:

```
css
CopyEdit
alert <protocol> <src_ip> <src_port> → <dst_ip> <dst_port> (msg:"messag
e"; content:"text"; sid:id; rev:rev;)
```

Example rule (detect HTTP GET):

```
snort
CopyEdit
alert tcp $HOME_NET any → $EXTERNAL_NET $HTTP_PORTS (
    msg:"HTTP GET Detected";
    flow:to_server,established;
    content:"GET "; http_method;
    sid:1001; rev:1;
)
```

➡️ Save it to: `/etc/snort/rules/local.rules`

➡️ Restart Snort after rule update.

📊 SOC Real-World Flow

1. **Capture packet**

   `tcpdump -i eth0 -w suspicious.pcap`

2. **Analyze pcap with Snort**

   `snort -r suspicious.pcap -c /etc/snort/snort.conf`

3. **Write rule in** **`local.rules`**

4. **Restart Snort and monitor**

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

🧠 Tips for SOC

- Focus on `HTTP`, `FTP`, `DNS`, `SSH` traffic.
- Regularly **tune rules** to reduce false positives.
- Keep an eye on **outbound traffic** (data exfiltration).
- Combine with SIEM (like Splunk) for alert correlation.