Snort Cheatsheet

Prepared by: Abdullah Akram

■ Introduction

Snort is an open-source Network Intrusion Detection System (NIDS) and Intrusion Prevention System (IPS). It is widely used in cybersecurity for packet analysis, traffic monitoring, and threat detection.

■ Snort Modes

- Sniffer Mode: Captures and displays packets in real-time.
- Packet Logger Mode: Logs packets to disk for later analysis.
- NIDS Mode: Detects malicious activity based on rules and signatures.

■ Snort Rule Structure

A Snort rule is composed of two parts: Rule Header and Rule Options.
Rule Format:
-> (options)

■ Example Rule

alert tcp any any -> 192.168.1.0/24 80 (msg:"Possible HTTP traffic"; sid:1000001;)

■ Common Rule Options

- msg: Message displayed when rule triggers.
- sid: Snort ID, unique identifier for rules.
- rev: Revision number of the rule.
- content: Looks for specific payload content.
- nocase: Makes content search case-insensitive.
- dsize: Checks data size of the packet.
- flags: Matches TCP flags.
- ttl: Matches packet TTL value.

■ Rule Operators & Modifiers

- -> : Unidirectional traffic.
- <> : Bidirectional traffic.
- ! : Negation operator.
- [] : Range specification.
- : : Port ranges (e.g., 1:1024).

■ Common Snort Commands

- snort -v : Run Snort in verbose mode (packet sniffer).
- snort -d : Display application layer data.

- snort -dev : Display data link, IP, and TCP/UDP headers + payload.
- snort -c snort.conf : Run Snort with a config file.
- snort -r file.pcap : Read and analyze packets from a pcap file.
- snort -l /log/path : Specify custom log directory.
- snort -T -c snort.conf : Test configuration file.

■ Output & Logging

- Fast Log: Minimal logging for alerts.
- Full Log: Complete packet dumps.
- Unified2: Binary logging format for use with analysis tools.
- Database Logging: Sending alerts to SQL databases.

■ Key Takeaways

- Snort can operate as a sniffer, logger, or NIDS.
- Rules define detection logic with headers and options.
- Efficient rule writing reduces false positives.
- Regular updates of rule sets are essential for accuracy.
- Integration with SIEM tools enhances monitoring and response.

■ Conclusion

Snort is a powerful tool for intrusion detection and prevention. By mastering rules, commands, and logging, SOC analysts can effectively use Snort to detect and prevent network attacks.