Suricata Commands Explained

This document explains the key commands used in the Suricata lab exercise. Suricata is an open-source intrusion detection and prevention system (IDS/IPS) that can inspect network traffic based on custom rules and generate alerts. The commands below demonstrate how to load rules, process packet captures, and analyze logs.

Command: cat custom.rules

Explanation: Displays the content of the custom.rules file, which contains user-defined Suricata rules.

Command: sudo suricata -r sample.pcap -S custom.rules -k none

Explanation: Runs Suricata to process packets from 'sample.pcap' using rules from 'custom.rules'. -r sample.pcap → Reads packets from the specified pcap file. -S custom.rules → Loads rules from the custom.rules file. -k none → Disables checksum validation (useful for pcap testing).

Command: cat /var/log/suricata/fast.log

Explanation: Displays quick, human-readable alerts generated by Suricata.

Command: jq . /var/log/suricata/eve.json | less

Explanation: Formats and displays the eve.json log in a human-readable way using jq and less. jq . → Pretty-prints JSON. less → Allows scrolling through the output.

Command: jq -c "[.timestamp,.flow_id,.alert.signature,.proto,.dest_ip]" /var/log/suricata/eve.json

Explanation: Extracts specific fields from the eve.json log for easier analysis.

Command: jq "select(.flow_id==X)" /var/log/suricata/eve.json

Explanation: Displays all events in eve.json related to a specific flow_id (replace X with actual ID).