

Homework

Take your NIDS skills beyond the lab: build a rule pack, benchmark against a SOC dashboard, and automate one piece of the triage.

Task 1 — Rule Pack

Objective: Write 3 high-fidelity Suricata rules from the lab findings.

Instructions:

- One protocol-anomaly rule, one content-match rule, one flowbits rule chaining two conditions
- Each must have: sid (start from 5000000), rev, msg, classtype, metadata
- Test the logic against your baseline file from Exercise 3 — confirm no match

Deliverable: `custom-rules.rules` file with 3 commented Suricata rules.

Task 2 — Coverage Map

Objective: Produce a MITRE ATT&CK Navigator-style coverage map for network detections.

Instructions:

- List the 10 most important network-observable techniques
- For each, mark: detected / partial / missed
- Explain why the missed ones are missed

Deliverable: A markdown table with 10 techniques and an exec summary paragraph.

Task 3 — Automation Script

Objective: Write a short Python script that parses a Suricata alert JSON file and produces the exact report format you used in Exercise 1.

Instructions:

- Read JSON lines
- Group by SID and source IP
- Emit a markdown summary with top 5 clusters
- Unit test it on a fake event

Deliverable: A `nids-triage.py` script and a sample output.