

Part 1 — Lab Answers

Reference solutions for the lab exercises. Use these only after attempting the exercises yourself.

Exercise 1 — Snort Alert Triage

Noise examples: policy-info rules like "ET INFO Observed DNS Query", GPL ICMP echo rules, TLS self-signed alerts on development subdomains. Real alerts: any rule flagging a known exploit CVE, rules with `established` flow to an internal asset, or ET MALWARE rules correlating with a known C2 IP. Cluster by `src_ip` + `classtype`. Top 5 should each have a specific asset and a MITRE technique.

Exercise 2 — PCAP Summary Analysis

Look for periodic HTTP POSTs of identical size (beacon), DNS queries with high-entropy subdomains (tunnel), and TLS with SNI not matching cert CN (MITM or malware). A beacon interval around 60s with 5s jitter is classic Cobalt Strike default. Map to T1071.001 (web protocols), T1071.004 (DNS), T1573 (encrypted channel).

Exercise 3 — Baseline vs Anomaly

Expect new destinations to IP ranges never in the baseline, a 10x DNS volume spike, and port 4444 or 8080 that were not in the baseline at all. Off-hours activity (02:00-05:00) from a workstation is highly suspect.

Exercise 4 — Write the Detection Rule

Sample Suricata rule:

```
alert http any any -> $EXTERNAL_NET any (msg:"BEACON Suspicious 60s peric
```

Final Exercise — Coverage Gap Analysis

NIDS detects initial-access and discovery stages. It misses: endpoint-local actions (credential theft from LSASS), fully encrypted C2 with valid certs, and DNS exfil below threshold volumes. Coverage improvement: EDR for endpoint, TLS decrypt or JA3 fingerprints, DNS sinkhole for known-bad domains.

Part 2 — Homework Answers

Model answers for the homework tasks. Your solution may differ and still be correct.

Task 1 — Rule Pack

Expect 3 rules that actually test against the baseline without firing. Bonus: flowbits-chained rule correlating scan + exploit attempts.

Task 2 — Coverage Map

Typical gaps: T1048 (exfil over alt protocol), T1572 (protocol tunneling), T1090.002 (external proxy). These are hard for NIDS alone and usually need a proxy/DNS sensor.

Task 3 — Automation Script

A 40-line Python script reading Suricata eve.json, using

`collections.defaultdict` keyed on `(src_ip, signature_id)`, emitting a markdown table. Unit test with a fake event dict.