

Part 1 — Lab Answers

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

Exercise 1 — Web Access Log Triage

Primary attacker: a single source IP hammering the login endpoint with 4xx responses, then suddenly returning 200s after hitting an admin path — classic credential-stuffing → admin panel access. Look for `sqlmap`, `nikto`, or `gobuster` user-agents, and any `../` / `%2e%2e` sequences. MITRE: T1110.003 (password spray), T1083 (file discovery), T1190 (exploit public-facing app).

Sigma rule sketch:

```
title: Web Login Brute Force Followed by Success
logsource: {product: apache, service: access}
detection:
  spray:
    cs-method: POST
    cs-uri-stem: '/login'
    sc-status: 401
  success:
    cs-method: POST
    cs-uri-stem: '/login'
    sc-status: 200
  condition: spray | count(c-ip) > 20 near success
fields: [c-ip, cs-uri-stem, sc-status]
level: high
tags: [attack.credential_access, attack.t1110]
```

Exercise 2 — Linux Syslog Analysis

Narrative: repeated SSH failures from one external IP, eventual success, then immediate `sudo su -`, then a new cron job in `/etc/cron.d/` calling `curl | sh`.

That is T1110.001 → T1078 → T1548 → T1053.003. The killer evidence is the cron entry: persistence is a one-line giveaway.

Top 3: (1) successful SSH after brute force, (2) sudo to root, (3) new cron job pulling remote code.

Exercise 3 — Windows Security Events

Look for Event 4624 type 3 (network logon) from a workstation IP to the DC with a service account — that is often lateral movement. Pair with 4672 (special privileges) to confirm privilege escalation. 4769 with RC4_HMAC = Kerberoasting. A single user showing 4624s across many hosts in minutes = lateral movement. Map to T1021.002, T1558.003, T1078.

Exercise 4 — Cloud Audit Log Review

Root cause: typically a `CreateAccessKey` on an existing IAM user, followed by `AttachUserPolicy` granting `AdministratorAccess`, followed by `PutBucketAcl` making an S3 bucket public. The first suspicious call is the key creation from an unusual source IP. MITRE cloud: T1098.001, T1562.008, T1537.

Containment: delete the key immediately, detach the policy, revoke any active sessions.

Final Exercise — Cross-Log Correlation

The web log attacker IP often appears in CloudTrail (source IP of the API call) and in syslog (same IP doing SSH). One shared indicator across 3 sources collapses 4 separate alerts into 1 incident. Earliest sign: the web login spray, because it pre-dates credential capture by minutes to hours.

Part 2 — Homework Answers

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

Task 1 — Detection Pack

Expect a 5-rule pack with clean metadata, tuned FPs, and MITRE tags. Grade on: uniqueness per source, realistic FP notes, and that each rule has a specific string/field match (not just severity filtering).

Task 2 — Detection Benchmark

Typical result: AI is 3-5x faster on the first pass but misses 1-2 subtle findings that a human analyst catches by cross-referencing memory. Human wins on context; AI wins on volume.

Task 3 — Personal SIEM Notebook

A good prompt library has one prompt per source, each parameterized with "paste log here" and each specifying desired output format. Bonus if the learner includes a "confidence" column in outputs.