

Homework

Three tasks to turn log analysis from a reactive exercise into a repeatable detection pipeline.

Complete the lab before starting. Check [answer.html](#) only after submitting.

Task 1 — Detection Rule Pack

Objective

Convert your lab findings into a deployable detection ruleset.

Instructions

1. For the 3 highest-value findings across the four logs, write one Sigma rule each.
2. Each rule must include: title, ID, description, logsource, detection, falsepositives, level.
3. Test your rules conceptually: would they fire on the lab data? Would they fire on benign admin activity?

Deliverable

A `detection-pack.yml` file with 3 Sigma rules.

Task 2 — Blind-Spot Analysis

Objective

Identify what the logs you analyzed CANNOT see.

Instructions

1. List five attack techniques a defender would miss even with perfect coverage of the four lab log sources.
2. For each, name the additional log source (EDR, DNS, sysmon, cloudtrail, etc.) that would catch it.
3. Rank the five by "dwell time extension" — which blind spot would let an attacker stay longest?

Deliverable

A markdown table: Technique / Blind spot / Required source / Dwell time extension.

Task 3 — Correlation Script

Objective

Automate the cross-log correlation you did manually in Exercise 5.

Instructions

1. Write a Python script that reads all four log files and extracts every IP address, username, and timestamp.
2. The script should output any IP or username that appears in 2+ files — these are high-confidence pivot points.
3. Bonus: cluster timestamps into 1-hour buckets and show the activity timeline in ASCII.

Deliverable

A single-file Python script `correlate.py` plus its output when run against the lab files.