

Homework

Three capstone tasks that cement your full red team workflow.

Complete the capstone lab first. These tasks build directly on your engagement output.

Task 1 — Engagement Rules of Engagement (ROE) Template

Objective

Build a reusable scope/ROE template.

Instructions

1. Using the lab scope as a starting point, produce a generic ROE template with clearly labeled placeholders.
2. Include sections for: in-scope, out-of-scope, techniques permitted, blackouts, emergency contacts, legal authorization language.
3. Add a "red flags" checklist: ambiguities that must be resolved before engagement start.

Deliverable

`roe-template.md`.

Task 2 — Blue Team Debrief

Objective

Deliver the post-engagement handoff from the defender's perspective.

Instructions

1. Take your attack timeline from Exercise 4.
2. For each step, identify: detection source that should have fired, detection source that actually fired (if any), and the specific rule or log query that would catch it next time.
3. Rank the gaps by "how much earlier in the kill chain would this have stopped the attack?"

Deliverable

A defender-facing handoff document.

Task 3 — AI Workflow Retrospective

Objective

Reflect on the course.

Instructions

1. For each of the 10 lessons, write one sentence: "the AI was most useful for X in this lesson."
2. For each lesson, write one sentence: "the AI was least reliable for Y in this lesson."
3. Conclude with a 200-word personal policy: how will you use AI in your next real engagement, and where will you NOT trust it?

Deliverable

`ai-retrospective.md`.