

Homework

Three take-home tasks that extend the lab into a full recon methodology you can reuse in future engagements.

Complete the lab exercises before attempting the homework. All tasks build on the outputs you generated in the lab. Check your answers against [answer.html](#) only after you finish.

Task 1 — Build a Reusable OSINT Prompt Library

Objective

Turn the ad-hoc prompts you wrote in the lab into a versioned prompt library you could use on any future engagement.

Instructions

1. For each of the five OSINT sources (WHOIS, DNS, CT logs, social profiles, paste dumps) rewrite your best prompt so it is:
 - Reusable (no hard-coded company names)
 - Self-contained (output format specified)
 - Defensive (includes a sanity-check clause: "flag low-confidence findings")
2. Save them as `osint-prompts.md` with one H2 section per source.
3. Include a short "when to use" note for each prompt.

Deliverable

A single `osint-prompts.md` file you could hand to a junior analyst on day one.

Task 2 — AI vs. Manual Benchmark

Objective

Quantify where AI-assisted OSINT beats manual work and where it fails.

Instructions

1. Pick **one** of the five lab files (your choice).
2. Do a manual analysis of it in 10 minutes — no AI. Write down every finding you can extract by hand.
3. Now run the same file through your best AI prompt from Task 1.
4. Compare the two lists: findings only in manual, findings only in AI, findings in both.
5. Write a 200-word summary titled "Where AI helped and where it missed."

Deliverable

A comparison table plus your written summary.

Task 3 — Defender's Mirror Exercise

Objective

Flip the lab and think like the defender who would see your recon.

Instructions

1. Take the top 5 findings from your final recon report in Exercise 6.
2. For each finding, answer:
 - Which defensive control should have prevented the leak?
 - Which detection source could catch an attacker who used this finding next?
 - What is the cost to remediate vs. the cost of the breach it enables?

3. Rank the five remediations by ROI (impact divided by effort) and recommend the top 2 for sprint 1.

Deliverable

A remediation plan formatted as a 1-page defender briefing.