

Homework

Three tasks to harden your infrastructure-audit methodology.

Complete the lab first.

Task 1 — AWS Privesc Playbook

Objective

Build a reusable IAM-privesc checklist.

Instructions

1. Document the privesc path you identified in Exercise 5 as a 5-step runbook.
2. For each step: AWS CLI command, expected output, failure mode.
3. Add a "detection" column: which CloudTrail event would fire if a defender had logging enabled?

Deliverable

Runbook as markdown.

Task 2 — Hardening Diff

Objective

Produce fixes a developer can merge.

Instructions

1. Pick the most dangerous finding from each of the five artifacts.

2. For each, produce a unified diff showing the exact change (YAML, conf, policy).
3. Verify each diff does not break the service's core functionality.

Deliverable

Five patches in one file.

Task 3 — Policy-as-Code Rule

Objective

Prevent the bad config from returning.

Instructions

1. Pick one k8s or Docker finding.
2. Write an OPA/Rego policy or kube-linter rule that would have rejected the manifest at CI time.
3. Test it mentally: would it fire on the lab file? Would it fire on a safe manifest?

Deliverable

Policy file plus a two-sentence rationale.