

Answers

Reference answers for Lesson 07.

Part 1 — Lab Answers

Exercise 1 — Nmap Scan Analysis

Expected findings

- A host running an outdated service with a known CVE.
- A database or admin panel exposed directly to the network.
- At least one host with an unusual combination (Windows exposing SSH, or Linux exposing RDP).

Exercise 2 — Kubernetes Pod Spec

Expected findings

- `privileged: true` or a `hostPath` volume mounting the host filesystem.
- Missing `securityContext` with `runAsNonRoot`.
- A service account with cluster-wide RBAC.
- Image using `:latest` or no digest.

A realistic escape primitive: `hostPath` write to `/var/spool/cron` or to a kubelet config.

Exercise 3 — Docker Compose

Expected findings

- A secret in `environment:` block.
- A volume mounting `/var/run/docker.sock`.
- A database on the same network as an internet-exposed service with no firewall.

Exercise 4 — Nginx Config

Expected findings

- An alias path traversal (missing trailing slash).
- A `proxy_pass` with user-controlled upstream enabling SSRF.
- Missing auth on `/admin` or `/status`.
- Weak TLS protocols or ciphers.

Exercise 5 — AWS IAM Policy

Expected findings

- `iam:PassRole` + `lambda:CreateFunction` = classic privesc.
- `"*": "*"` pattern on write actions.
- Missing `Condition` blocks for MFA or source IP.

Final Exercise — Kill Chain

Expected chain

External nmap finding → web exploit via nginx misconfig → container access → docker.sock escape OR k8s service account → AWS metadata credentials → IAM privesc via PassRole.

Part 2 — Homework Answers

Task 1 — AWS Privesc Playbook

Expected detections

CloudTrail events like `CreateFunction`, `PassRole`, `AttachRolePolicy` are the defender's best signals. A good runbook notes that attackers who disable CloudTrail leave their own fingerprint via `StopLogging`.

Task 2 — Hardening Diff

Expected patch quality

Each diff should change the root cause (remove the wildcard, drop the capability, add the Condition) without removing legitimate functionality. Tests: does the app still start? Does traffic still flow?

Task 3 — Policy-as-Code Rule

Expected rule

A Rego rule matching `input.spec.containers[_].securityContext.privileged == true` or equivalent kube-linter check. Should fire on the lab manifest and ignore compliant ones.