

Part 1 — Lab Answers

Reference solutions for the lab exercises. Use these only after attempting the exercises yourself.

Exercise 1 — SSH Config Audit

Key fixes: `PermitRootLogin no`, `PasswordAuthentication no`, `MaxAuthTries 3`, `AllowGroups sshusers`, modern `KexAlgorithms` (curve25519, diffie-hellman-group16), strong `Ciphers` (chacha20-poly1305, aes256-gcm). Rollout risk: removing password auth breaks users without keys — stage first.

Exercise 2 — Linux System Audit

Critical: UID 0 duplicates, EoL kernel, sshd on 0.0.0.0 with password auth. High: NOPASSWD sudo, missing auditd. Medium: missing sysctl hardening. Map each to CIS control numbers (e.g., 5.2.x for SSH).

Exercise 3 — Windows GPO Review

Top finding: SMBv1 or LM hash storage enabled. Fix via `Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options`. Next: weak password policy, missing script block logging.

Exercise 4 — Dockerfile Hardening

```
FROM node:20-alpine@sha256:... AS build
WORKDIR /app
COPY package*.json ./
RUN npm ci --only=production
```

```
FROM gcr.io/distroless/nodejs20
COPY --from=build /app /app
USER 10001
EXPOSE 8080
CMD ["/app/server.js"]
```

Run with `--read-only --cap-drop=ALL --security-opt=no-new-privileges`.

Final Exercise — Rollout Plan

Day 1: SSH + sysctl (low risk, instant). Day 2-3: pilot OU for GPO (5% of fleet).
Day 4: rebuild containers with hardened Dockerfile. Day 5: full rollout with monitoring + rollback script ready.

Part 2 — Homework Answers

Model answers for the homework tasks. Your solution may differ and still be correct.

Task 1 — Personal Hardening Checklist

Expect 10 items with verification commands like `sudo ufw status` or `defaults read com.apple.screensaver askForPassword`. Bonus: rollback per item.

Task 2 — Dockerfile Lint

Linters should catch: latest tags, root user, apt without `rm -rf /var/lib/apt/lists/*`, COPY . ., hardcoded secrets. Output in severity order.

Task 3 — CIS Gap Analysis

A real gap report should cite exact CIS control numbers and document WHY an item cannot be fixed (e.g., legacy client dependency) with a compensating control.