

Part 1 — Lab Answers

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

Exercise 1 — Network Diagram Review

Expected zones: Internet → DMZ → App → DB → Admin. Violations: admin jump host reachable from user net, DB directly reachable from DMZ, backup path that bypasses firewall. Principle violated most often: flat internal network (no segmentation past the edge firewall).

Exercise 2 — ACL Audit

Collapse catch-alls, remove shadowed rules, add explicit deny with log at the end. Group rules by purpose: "inbound web", "outbound DNS", "management". Each rule gets a one-line comment.

Exercise 3 — iptables Review

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p tcp --dport 22 -s 10.0.0.0/24 -m limit --limit 10/min -j ACCEPT
-A INPUT -p tcp --dport 443 -j ACCEPT
COMMIT
```

Exercise 4 — AWS Security Groups

Flag any rule with `0.0.0.0/0` on 22, 3306, 5432, 3389. Fix: reference the specific admin-jump SG by ID, not CIDR. CLI example: `aws ec2 revoke-security-group-ingress --group-id sg-xxx --protocol tcp --port 22 --cidr 0.0.0.0/0`.

Final Exercise — Unified Policy

One page: zone model + default-deny + per-zone allow matrix + change-control workflow + quarterly audit command. Fits on a single printed sheet as a reference.

Part 2 — Homework Answers

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

Task 1 — Personal Network Baseline

Inventory devices, list expected protocols per device, and explain any rule you cannot justify (often IoT devices calling home).

Task 2 — Cloud SG Audit

Typical finding: legacy `0.0.0.0/0 22` rule from a contractor. Replace with a specific SG reference or bastion-only access via SSM.

Task 3 — Drift Detector

Expected: `iptables-save | diff baseline.rules -` wrapped in a script with timestamped logging and non-zero exit on drift.