

Homework

Apply firewall design principles in your own network: build a baseline, audit a cloud tenant, and automate drift detection.

Task 1 — Personal Network Baseline

Objective: Document the expected traffic baseline for your home or lab network.

Instructions:

- List every device and the services it should talk to
- Produce an allow matrix
- Identify rules you cannot justify

Deliverable: A zone matrix + narrative of any surprises you found.

Task 2 — Cloud SG Audit

Objective: If you have a cloud account, export your security groups and audit them. If not, re-audit the lab's `aws-security-groups.txt` with stricter rules.

Instructions:

- Flag every 0.0.0.0/0 finding
- Propose the least-privilege replacement
- Estimate the business impact of the change

Deliverable: A CSV or markdown table of findings with fixes.

Task 3 — Drift Detector

Objective: Write a short shell or python script that compares `iptables-save` output to a baseline file and alerts on drift.

Instructions:

- Reads baseline from file
- Diffs current state
- Prints added / removed rules
- Exit code non-zero if drift

Deliverable: A `drift.sh` or `drift.py` script.