

Part 1 — Lab Answers

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

Exercise 1 — Vuln Scanner Triage

Top 10 should be dominated by: internet-facing services with CISA KEV entries, followed by authenticated-exploit RCEs on high-value hosts. A CVSS 9.8 on an offline dev VM ranks below a CVSS 7.5 KEV entry on a public-facing app.

Exercise 2 — SBOM Review

Typical findings: transitive dep with known CVE (e.g., old `log4j`, old `openssl`), abandoned package 3+ years without release, GPL license mixed into MIT-only product.

Exercise 3 — Dependency Audit

Decision matrix: patch-now for semver-patch fixes, this-sprint for minor bumps with release-note review, risk-accept for major versions blocked by breaking changes (with compensating controls documented).

Exercise 4 — Patch Inventory

Flag EoL hosts (Win7, Server 2012) and name the replacement. Coverage heatmap: by OS and criticality, target >95% for critical, >90% for high.

Final Exercise — Weekly Patch Plan

Patch list with owner, change window, rollback method, verification query per patch. A tier-1 ops engineer executes without asking questions.

Part 2 — Homework Answers

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

Task 1 — Prioritizer Prompt

Must incorporate KEV list, public PoC, and asset value multiplier. Output in rank order with rationale per item.

Task 2 — Personal SBOM

Real output from `cyclonedx-bom` or `syft`. Enrichment via `osv-scanner` is a bonus.

Task 3 — CI Gate

```
#!/bin/bash
pip-audit --format json | jq -e ' [.vulnerabilities[] | select(.aliases[]?
    echo "High severity CVE found"; exit 1;
}
```