Kubernetes Security Lab Workbook

A practical, hands-on guide to securing Kubernetes clusters

Phase 1 — Cluster & API Hardening Fundamentals

- Enable RBAC: microk8s enable rbac
- Create ServiceAccounts, Roles, and RoleBindings.
- Use 'kubectl auth can-i' to test permissions.
- Create namespaces (dev/prod) and restrict via RBAC.
- Enable audit logs and observe denied requests.

Phase 2 — Pod & Workload Security

- Experiment with privileged vs. restricted SecurityContexts.
- Apply PodSecurityAdmission labels and enforce 'restricted'.
- Install Kyverno and enforce a policy (e.g., disallow ':latest' images).

Phase 3 — Network & Runtime Security

- Install Calico/Cilium; create NetworkPolicies for isolation.
- Install Falco and trigger a detection (e.g., exec into pod).

Phase 4 — Supply Chain & Secrets

- Scan images with Trivy.
- Enable encryption at rest for secrets.
- Integrate with an external secrets manager (Vault or External Secrets Operator).

Phase 5 — Assessment & Attack Simulation

- Run kube-bench for CIS benchmark compliance.
- Run kube-hunter to identify open surfaces.
- Run Kubescape for posture assessment.

Recommended References & Resources

- Kubernetes official docs: https://kubernetes.io/docs/concepts/security/
- OWASP Kubernetes Security Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Kubernetes_Security_Cheat_Sheet.html
- Falco Runtime Security: https://falco.org/docs/
- Kyverno Policy Engine: https://kyverno.io/
- Trivy Image Scanner: https://aquasecurity.github.io/trivy/
- Kube-bench & Kube-hunter: https://github.com/aquasecurity/

Created by ChatGPT (GPT-5) — 2025