Configuration Review and Change Plan

Secondary, higher ed, professional | Runbook | 60-90 minutes

Before class: This is an instructor preparation runbook. Assemble the fictional scenarios, messages, or data it specifies before use; it does not provision a lab or include a ready-made dataset.

Lab ID: CONFIG-REVIEW-01 Outcome: Identify weaknesses in an approved configuration and propose testable, reversible changes. Environment: Invented text configuration or isolated lab. Time: 60-90 minutes.

Required Finding Fields

Finding ID: _____

Evidence: _____

Risk relationship: _____

Recommendation: _____

Operational consequence: _____

Test: _____

Rollback: _____

Priority: _____

Instructor Preparation

Create six to ten findings across identity, logging, network rules, updates, backups, ownership, and recovery. Include at least one setting that appears weak but is justified by a documented dependency so learners must ask questions rather than mechanically harden everything.

Stop Conditions

Stop if the environment reaches an unapproved network, uses real credentials, or affects a service outside the exercise. Preserve evidence and notify the lab owner.

Debrief

- Which recommendation reduced risk but created the largest operational consequence?
- Which change required sequencing or a compensating control?
- How would the team verify success and detect regression?

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Editable companion - Runbook 4 - Configuration Review and Change Plan.

Sharing and reuse: Please do not resell this resource. You may repost or share it with other educators. Please leave the Bare Metal Cyber Educators Hub URL below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/configuration-review-and-change-plan/