Full Mini-Lab, Logic, and CTF Activity Library

Secondary, higher ed, professional | Reference

These activities are deliberately bounded. Each numbered I.x entry is a separate activity or reusable form; labels such as Setup, Learner Task, Evidence, Assessment Focus, Scoring, and Debrief are components of that entry. No activity requires testing public systems, real accounts, or live targets. Review each activity against the lab controls in Chapter 10 and Appendix F before use.

I.1 Mini-Lab: Suspicious Message Triage

Audience: Grades 4-6 through adult, with language adjusted Time: 25 to 40 minutes Outcome: Identify evidence in a fictional message and choose a safe verification and reporting action.

Setup

Create three fictional messages: one legitimate, one deceptive, and one ambiguous. Use invented organizations, links, names, and phone numbers. Provide screenshots or printed cards so no one can click or reply.

Learner Task

For each message, record:

- Claimed sender and purpose
- Requested action
- Pressure or emotion used
- Information or access at risk
- Evidence that can be checked independently
- Safest next action
- Reporting path

Evidence

A completed triage sheet and a two-sentence explanation of the most uncertain case.

Debrief

A professional appearance, encrypted connection, familiar logo, or correct name can coexist with deception. The goal is not to memorize one visual cue but to verify identity, purpose, and action through a trusted path.

I.2 Mini-Lab: Account Recovery Map

Audience: Grades 7-12, postsecondary, or professional Time: 35 minutes Outcome: Analyze how an approved fictional service proves identity and restores access without exposing actual credentials.

Setup

Provide a fictional account with these recovery elements:

- Primary password or passkey
- Registered device
- Backup authentication method
- Recovery code
- Support process
- Session revocation
- Notification to the account owner

Learner Task

1. Draw the normal sign-in path.
2. Draw the lost-device or forgotten-credential path.
3. Identify two ways an attacker might abuse recovery.
4. Recommend safeguards for proofing, notifications, rate limits, support staff, and session revocation.
5. Identify one accessibility or continuity concern.

Evidence

An annotated recovery diagram and prioritized recommendations.

Boundary

Do not inspect or change real account recovery settings during the activity. A supervised extension may use institutionally approved test accounts.

I.3 Mini-Lab: Log Triage Without Exploitation

Audience: Grades 9-12, postsecondary, or professional Time: 45 to 60 minutes Outcome: Build an event timeline from sanitized logs and distinguish confirmed evidence from hypotheses.

Setup

Provide a small text or spreadsheet data set containing:

- Successful and failed sign-ins
- One unusual source location or device
- File-access events
- Administrative change
- Benign background activity
- Incomplete or missing fields

All data must be invented or thoroughly sanitized.

Learner Task

1. Normalize timestamps and sort events.
2. Identify the five events most relevant to the investigation.
3. Label each statement as fact, inference, or unknown.
4. Develop two competing hypotheses.
5. Identify the next evidence needed to distinguish them.
6. Prepare a one-minute status update.

Evidence

Timeline, hypothesis table, and status update.

Assessment Focus

Reward evidence discipline, not dramatic conclusions. A learner who says “insufficient evidence” with a strong next step may demonstrate better judgment than a learner who names an attacker without support.

I.4 Logic Challenge: Sequence the Incident

Cut the following events into cards and ask teams to create the most defensible sequence. Some events may remain uncertain.

- User reports an unfamiliar authentication prompt.
- Monitoring records a successful sign-in from an unusual device.
- A help-desk ticket requests a password reset.
- A privileged group membership changes.
- A shared file is downloaded.
- The user confirms the prompt was not expected.
- Security revokes active sessions.
- The team preserves authentication and administrative logs.

Challenge Questions

- Which events are observations, actions, or interpretations?
- What sequence is supported by timestamps?
- What alternative sequence remains possible?
- Which containment action might destroy useful evidence?
- What should be communicated to the affected user?

I.5 Logic Challenge: Choose the Control Portfolio

A fictional organization has limited funds and these conditions:

- Shared administrator accounts
- Incomplete device inventory

- Reliable backups that have not been restored recently
- Frequent phishing reports
- A critical public service with little downtime tolerance
- Several unsupported applications

Teams receive a fixed budget of ten points. Possible actions cost one to four points. Examples include inventory improvement, privileged account redesign, restore testing, phishing-report workflow, network segmentation, emergency patching, application retirement, logging improvement, and awareness training.

Learner Task

Select a portfolio, explain the sequence, identify residual risk, and state what evidence would cause the priorities to change. There is no single correct portfolio; scoring focuses on risk relationships, dependencies, feasibility, and justification.

I.6 Beginner CTF: Metadata and Evidence Hunt

Audience: Grades 7-12 or introductory postsecondary Time: 45 minutes Format: Offline evidence challenge Outcome: Inspect approved files and records for clues without exploiting a system.

Challenge Design

Prepare a folder with fictional documents, images, and text files. Embed flags in safe locations such as:

- Document properties
- File names and timestamps
- Image metadata created specifically for the exercise
- A text file encoded with a simple substitution
- A log entry requiring correlation with a provided timeline

Rules

- Only the supplied folder may be examined.
- No external upload or public decoding service may be used unless explicitly approved.
- Files may be copied within the lab but not modified if evidence preservation is part of the outcome.
- Learners record the method and evidence for every flag.

Scoring

Award points for the flag, method, evidence, and explanation. A guessed flag without method evidence earns little or no credit.

Debrief

Discuss metadata reliability, chain of custody, tool limitations, and the difference between a clue and a conclusion.

I.7 Beginner CTF: Configuration Review

Audience: Grades 9-12, postsecondary, or professional Time: 60 minutes Format: Sanitized configuration analysis Outcome: Identify weaknesses in an invented configuration and recommend prioritized fixes.

Challenge Design

Provide an approved text configuration containing several issues, such as:

- Excessive permissions
- Unused account that remains active
- Logging disabled for a critical action
- Broad network rule
- Unprotected backup location
- Default or insecure setting
- Missing owner or review date

Flags correspond to issue identifiers, not exploitation steps.

Learner Task

For each issue:

1. Identify the evidence.
2. Explain the risk.

3. Recommend a proportional change.
4. State a possible operational consequence.
5. Describe how the change should be tested and rolled back.

Scoring

Use technical accuracy, prioritization, consideration of consequences, and verification plan.

I.8 Activity Evidence Template

Activity ID	
Outcome	_____
Evidence collected	_____
Learner explanation	_____
Instructor finding	_____
Revision or follow-up	_____

Vertical planning form

I.9 Post-Activity Debrief

- What was the intended capability?
- Which action or clue produced the strongest evidence?
- Where did the environment encourage guessing or unsafe shortcuts?
- Which assumptions proved wrong?
- What would a professional document or communicate differently?
- What should be changed before the activity is offered again?

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. Online public appendices - Appendix I.

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/activities/