Threat Modeling a Campus Service

College & University Faculty | Lesson Plan | 75 minutes

Before class: Prepare a fictional campus service diagram (for example, course registration, advising, or student-file sharing). Do not use production architecture diagrams or real credentials.

Outcome: Students will identify assets, actors, trust boundaries, abuse cases, and defensible mitigations for a fictional campus service.

Materials

- Fictional one-page service diagram
- Threat-model worksheet or whiteboard
- Sticky notes or collaborative board
- Optional MITRE ATT&CK or threat reference for extension

Learning Objectives

- Identify critical assets and trust boundaries.
- Describe plausible misuse or abuse cases without attempting real exploitation.
- Prioritize mitigations based on likelihood, impact, and feasibility.
- Explain residual risk and assumptions.

Opening (10 minutes)

- Introduce the fictional service and ask students what must be protected and who depends on it.
- Clarify that the exercise is design analysis, not an authorization to test a real system.

Model the System (15 minutes)

- Teams mark users, services, data stores, external dependencies, and trust boundaries.
- Require each team to state at least three assumptions.

Develop Abuse Cases (20 minutes)

- Each team writes four plausible misuse cases, including at least one identity or privilege problem and one data-handling problem.
- For each case, describe the precondition, affected asset, and potential consequence.

Prioritize and Mitigate (20 minutes)

- Rank the abuse cases using a simple likelihood-impact discussion.
- Choose one preventive, one detective, and one recovery-oriented mitigation.

Debrief (10 minutes)

- Which assumption mattered most?
- Which mitigation reduced the most risk for the least complexity?
- What evidence would you want before approving the design?

Evidence and Assessment

- Collect the annotated model and a one-page decision summary. Assess clarity of assumptions, quality of reasoning, connection between risk and mitigations, and acknowledgement of residual risk.

Optional Companion

- Pair this lesson with the Hub resource “Threat Model a Student Service” or a relevant Academy/Wiki topic for deeper preparation.

Source and use

The Complete Cybersecurity Educator, Dr. Jason Edwards. College & University lesson-plan extension derived from the companion course-design, lab, and assessment resources.

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 and source attribution below intact. Use fictional or appropriately authorized data where applicable.

Read online: https://educate.baremetalcyber.com/resources/threat-modeling-a-campus-service/