Threat Modeling (intermediate)

Learning Objectives

Learners will:

- Apply threat modeling to a hypothetical situation.

Prerequisites

- Learners have completed the beginning part of this module.

Ratio

Instructor: Learners
It's okay to do this lecture-style, and then break learners into breakout groups for activities.

Recommended Reading

Assessing Your Risks

Lesson Content

ACTIVITY

Break learners up into groups of even-numbered people—one has a particular asset to protect, the other are adversaries trying to get to that asset. Give them a specific scenario and have them spend 15 minutes discussing how they would protect the asset or attack the asset, then have them report back.

The best scenarios are the ones that are specific to your audience. Some examples include:

- For a group of journalists, the asset could be a story from an anonymous source. How would you protect the anonymity of your source? Or, if the story

were then published and you were unhappy about it, how would you try to unmask the anonymous source.

- For a group of activists in an urban U.S. setting, the asset could be communications among a group or collective. What precautions would you take to make sure that the messages you send to each other stay among you? Or, if you were a [law enforcement, university, etc] official, how would you try to find out what subject members of the group were talking about?
- For students concerned about online bullying, the asset could be social media identity and information. How would you make sure that what you share online goes only to the people you intend? Or, if you were a bully, how would you try to find that information?

Scenarios can also be silly! Some include:

- One group is the Joker, and one is Batman.
- One group is a jewelry store owner, and the other is an international jewel thief.

If you have more than an hour:

This threat modeling module segues nicely into specific modules about tools that address participants' concerns. Based on the concerns participants have voiced before and during the threat modeling session, you might teach, for example, passwords and password managers, phishing protections, social media security, anonymous browsing and Tor, etc.