Classroom Exercise: Threat Modeling with OWASP Threat Dragon

Learning Outcome

Participants will understand how to:

- Use OWASP Threat Dragon
- Apply the STRIDE threat modeling methodology
- Create and document a threat model with real-world relevance.

Pre-requisites

You will need:

- Internet browser (Google Chrome / Edge)
- OWASP Threat Dragon (https://owasp.org/www-project-threat-dragon/)
- Optional: GitHub account
- Sample use case for modeling

Step 1: Introduction to OWASP Threat Dragon

OWASP Threat Dragon is an open-source tool for modeling threats visually.

Interface Overview:

- Home Screen: View models
- Top Menu: New, Load, Export
- Diagram Toolbar: Add elements
- Properties Panel: Edit items
- Threats Panel: Manage STRIDE threats

Step 2: Creating a New Threat Model

1. Click 'New Threat Model'
2. Name: Online Banking Login System
3. Owner: Your name
4. Description: A login page linked to authentication service and DB
5. Click 'Create Model'

Classroom Exercise: Threat Modeling with OWASP Threat Dragon

Step 3: Designing the System Diagram

Add components:

- External Entity: User
- Processes: Login Web Page, Authentication Service
- Data Store: User Database
- Trust Boundary around the system

Data Flows:

- User -> Login Web Page: Enter credentials
- Login Web Page -> Auth Service: Send credentials
- Auth Service <-> DB: Validate user
- Auth Service -> Login Page -> User: Result

Step 4: Applying STRIDE

Right-click each element and select 'Threats', then click 'Auto-generate threats using STRIDE'.

STRIDE:

- S: Spoofing
- T: Tampering
- R: Repudiation
- I: Information Disclosure
- D: Denial of Service
- E: Elevation of Privilege

Step 5: Example Threats (STRIDE)

1. Spoofing (Auth Service): Brute-force credentials
   - Mitigation: Rate-limiting, MFA
2. Tampering (Data Flow): Intercepted credentials
   - Mitigation: HTTPS

3. Repudiation (Login Page): User denies login
   - Mitigation: Logging
4. Information Disclosure (Data Flow): Leaked data
   - Mitigation: Encryption
5. Denial of Service (Auth Service): Flooding
   - Mitigation: IP throttling
6. Elevation of Privilege (User): Gains admin
   - Mitigation: RBAC, session validation

Step 6: Review and Export

Review all threats added.

Click 'Export Model' and save as PDF or JSON.

Suggested filename: OnlineBanking_ThreatModel.pdf

Instructor Notes

Duration: 1.5 - 2 hours

Walkthrough: Demonstrate the tool live

Hands-On: Students model a new system

Review: Peer-review threat models

Optional Homework

Task:

- Choose a system (e.g., Online Ticket Booking)
- Create a new model
- Add at least 2 threats per STRIDE category