**Lab Exercise: Threat Modeling for a File Upload Web Application**

**🎯 Objective**

By the end of this lab, you will be able to:

* Design a system diagram (DFD) for a web application
* Use Microsoft Threat Modeling Tool to identify threats using STRIDE
* Propose realistic mitigations
* Export and interpret threat reports

**🧰 Pre-requisites**

* Installed: Microsoft Threat Modeling Tool
* Windows OS or VM
* Internet connection (optional for reading docs)

**📘 Scenario**

You are developing a **File Upload Web App** where users can:

* **Register/Login**
* **Upload files**
* **Download their previously uploaded files**

The system includes:

* Frontend (web browser)
* Web server (business logic)
* Azure Blob Storage
* Azure SQL Database
* Authentication service (Azure AD B2C or custom)

**🏗️ Step-by-Step Instructions**

**✅ Step 1: Launch Tool and Create New Model**

1. Open the **Microsoft Threat Modeling Tool**.
2. Click **File > New Model**.
3. Choose **"Blank Template"**.
4. Save the file as FileUploadAppThreatModel.tmt.

**✅ Step 2: Build the Data Flow Diagram (DFD)**

**🔹 2.1 Add Elements**

From the left-hand toolbox:

| **Element Type** | **Label** |
| --- | --- |
| External Interactor | User |
| Process | Web Frontend |
| Process | Application Server |
| Data Store | Azure SQL DB |
| Data Store | Azure Blob Storage |
| External Interactor | Identity Provider (Azure AD B2C) |

**🔹 2.2 Connect Elements with Data Flows**

Use **“Data Flow”** arrows for each communication:

| **From** | **To** | **Data Flow Label** |
| --- | --- | --- |
| User | Web Frontend | HTTP Request (Login/Register) |
| Web Frontend | User | HTTP Response |
| Web Frontend | Identity Provider | Auth Request |
| Identity Provider | Web Frontend | Auth Token |
| Web Frontend | Application Server | Upload File |
| Application Server | Azure Blob Storage | Store File |
| Application Server | Azure SQL DB | Save File Metadata |
| Application Server | Web Frontend | File Upload Response |
| Web Frontend | User | Confirmation/Download Link |

💡 **Tip**: Right-click each component to rename. Use "Properties" panel to give detailed descriptions.

**✅ Step 3: Auto-Analyze Threats**

1. Click **“Analyze > Analyze Model”**.
2. The tool will automatically identify threats based on **STRIDE** per component and data flow.
3. Click the **Threats** tab to see the list.

**🔍 Step 4: Review Example Threats and Add Mitigations**

Here are 3 **sample threats** you might see (or manually add):

**🛑 Threat 1: Spoofing Identity**

* **Target**: Web Frontend
* **Description**: An attacker may spoof identity by injecting forged credentials.
* **STRIDE Category**: Spoofing
* **Mitigation**:
  + Use OAuth2 with Azure AD B2C
  + Validate JWT tokens on the server
  + Implement IP throttling and rate-limiting

**🛑 Threat 2: Information Disclosure**

* **Target**: Data Flow – App Server → Blob Storage
* **Description**: File content may be intercepted if sent over unencrypted channels.
* **STRIDE Category**: Information Disclosure
* **Mitigation**:
  + Use HTTPS (TLS 1.2+)
  + Store files encrypted at rest in Azure Blob Storage
  + Avoid exposing direct blob URLs to clients

**🛑 Threat 3: Elevation of Privilege**

* **Target**: Application Server
* **Description**: A normal user might gain admin access due to insecure role validation.
* **STRIDE Category**: Elevation of Privilege
* **Mitigation**:
  + Enforce role-based access control (RBAC)
  + Validate permissions server-side
  + Log and alert unusual access attempts

**✅ Step 5: Generate and Export the Report**

1. Click **Reports > View Report**.
2. Review threat details, mitigations, and DFD snapshot.
3. Click **File > Export > HTML** or **PDF**.
4. Save as ThreatModelReport\_FileUploadApp.pdf.

**📤 Submission Instructions**

Submit the following:

| **Item** | **Description** |
| --- | --- |
| Screenshot | Completed DFD in Threat Modeling Tool |
| Screenshot | At least 3 reviewed threats |
| PDF | Exported Threat Report |
| Summary | Brief text (150–200 words) of top 2 threats + mitigations |

**🧠 Additional Tips**

* You can add **custom threats** manually if you want to explore more.
* Explore “Properties” on each component to add descriptions.
* Use the **STRIDE-per-element** guide to understand expected threats for each type.

👉 STRIDE threat guidance: <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats>