**Day 6**  
**Threat Modeling for a University’s Learning Management System**

**1. Assets**

* Student Data
* Course Materials
* Grades and Feedback
* System Infrastructure

**2. Potential Threats**

* Unauthorized Access: Someone might try to gain access to the LMS to alter grades or steal sensitive student data.
* Data Breach: Personal and academic data could be exposed due to vulnerabilities in the system.
* Phishing Attacks: Students or faculty might be tricked into giving away their login credentials through fake emails or websites.
* Denial of Service (DoS) Attacks: An attacker could try to overload the system, making it unavailable during critical times like exam periods.

**3. Vulnerabilities**

* Weak Passwords
* Outdated Software

**4. Possible Attacks**

* Brute Force Attack: An attacker might try to guess users' passwords to gain unauthorized access to the LMS.
* SQL Injection
* Phishing

**5. Risks and Exploits**

* Grade Tampering: Unauthorized changes to grades could affect the integrity of the university’s academic records.
* Loss of Privacy: A data breach could expose sensitive student information, leading to identity theft or other privacy violations.
* Operational Disruption: A DoS attack during critical periods could disrupt exams, assignments, or access to course materials.

**6. Impact**

* Academic Integrity: Altering grades or course content could damage the university’s reputation and trust in its academic processes.
* Student Trust: If student data is compromised, it could lead to a loss of trust in the university’s ability to protect their personal information.
* Operational Costs: Recovering from a successful attack could be costly in terms of both time and resources.