Attack Profile and Potential Damage Assessment for the University’s Online Learning Platform

Introduction

The university’s Learning Management System (LMS) is a critical platform for course delivery, student assessments, and academic collaboration. It stores sensitive data such as grades, exam materials, and personal information. This assessment identifies high-risk attack vectors, analyzes attacker profiles, and evaluates potential damages based on real-world tactics.

List of Attack Vectors

1. **Phishing Attacks**
2. **Exploitation of LMS Vulnerabilities**
3. **Denial of Service (DoS) Attacks**
4. **Unauthorized API Access**
5. **Credential Stuffing**

ATTACK PROFILE 1: Phishing Attacks

**1. Motivation & Capabilities of Potential Attackers**

* **Cybercriminals: Seek credentials for financial gain (e.g., selling stolen data).**
* **Disgruntled Students: Aim to alter grades or disrupt classes.**
* **Capability Level: Low to Moderate — phishing kits are widely available.**

**2. Potential Damage Assessment**

**Best-Case Scenario**

* **Description: Phishing email reported by a trained faculty member; no compromise.**
* **Risk: Low**
* **Cost: Minimal (time for triage).**
* **Probability of Spread: Very low**

**Most Likely Scenario**

* **Description: Credentials stolen but blocked by MFA; account locked.**
* **Risk: Moderate**
* **Cost: Moderate (password resets, investigations).**
* **Probability of Spread: Low**

**Worst-Case Scenario**

* **Description: Multiple accounts compromised, grades altered, data leaked.**
* **Risk: High**
* **Cost: High (legal penalties, reputational damage).**
* **Probability of Spread: Moderate**

**3. Recommended Countermeasures**

* **Mandatory MFA for all accounts.**
* **Quarterly phishing simulations.**
* **Email filtering with spoofed domain detection.**

ATTACK PROFILE 2: Exploitation of LMS Vulnerabilities

**1. Motivation & Capabilities**

* **Hacktivists: Target unpatched systems for fame/political reasons.**
* **Cybercriminals: Exploit bugs for ransomware or data theft.**
* **Capability Level: Moderate to High (requires technical skills).**

**2. Potential Damage Assessment**

**Best-Case Scenario**

* **Vulnerability patched before exploitation.**
* **Risk: Low**
* **Cost: Minimal (patching effort).**

**Most Likely Scenario**

* **Partial system breach; antivirus halts payload.**
* **Risk: Moderate**
* **Cost: Moderate (cleanup, scans).**

**Worst-Case Scenario**

* **Full system compromise; data encrypted/deleted.**
* **Risk: Critical**
* **Cost: Severe (downtime, recovery costs).**

**3. Recommended Countermeasures**

* **Regular penetration testing.**
* **Automated patch management.**
* **Network segmentation.**

ATTACK PROFILE 3: Denial of Service (DoS) Attacks

**1. Motivation & Capabilities**

* **Hacktivists: Disrupt exams for publicity.**
* **Capability Level: Moderate (botnet tools available).**

**2. Potential Damage Assessment**

* **Best-Case: Traffic blocked by WAF; minimal downtime.**
* **Worst-Case: LMS offline during exams; academic delays.**

**3. Recommended Countermeasures**

* **Deploy Web Application Firewall (WAF).**
* **Rate-limiting and traffic filtering.**

ATTACK PROFILE 4: Unauthorized API Access

1. Motivation & Capabilities

* **Insiders/Students**: Abuse weak API permissions for grade changes.
* **Capability Level**: Low to Moderate.

2. Potential Damage Assessment

* **Worst-Case**: Mass grade tampering; legal repercussions.

3. Recommended Countermeasures

* API gateway with strict permissions.
* Monitor anomalous API calls.

ATTACK PROFILE 5: Credential Stuffing

1. Motivation & Capabilities

* **Cybercriminals**: Reuse leaked passwords for account takeovers.
* **Capability Level**: Low (automated tools).

2. Potential Damage Assessment

* **Worst-Case**: Unauthorized access to admin accounts.

3. Recommended Countermeasures

* Enforce password complexity.
* Monitor login attempts (geo-blocking).