COMP435 In Class Practice 8/24/26 Name: _____

Question 1: Exploring Risk with MITRE ATT&CK Go to the **MITRE ATT&CK Enterprise Matrix**:

`https://attack.mitre.org/matrices/enterprise/`

Choose **one technique** that seems interesting to you.

1.1. Research your technique and record:

- **Technique name + ID:** _____
- **Tactic:** _____
- In your own words, **what does the attacker do?**

- What **asset or security property** could be harmed?

1.2. Imagine you are responsible for security in a typical university computing environment.
Rate the risk posed by this technique:

Likelihood: Low Medium High

Impact: Low Medium High

Overall Priority: Low Medium High

Briefly explain your reasoning and any assumptions you made.

1.3. Now compare with your group.
Find someone who researched a **different technique**. Compare your priority ratings and decide:

If you could defend against only one of your group's techniques first, which would you prioritize and why?

Question 2: Calculating Risk Exposure Hospitals are vulnerable to ransomware attacks: the hospital's medical records are encrypted by the attacker and inaccessible to the hospital administration, staff, or doctors. To recover their records, hospitals must pay the requested ransom, typically around $1,200,000. There is a 1% probability of HealthyHospital being the subject of a $1.2M ransomware attack in any given year. Calculate the hospital's annual risk exposure

Question 3: Calculating Costs Calculating Costs Suppose the HealthyHospital administrators are considering how best to protect against such attacks. One option is to maintain a duplicate database of records. Maintaining this independent set of records would cost $10,000 per year. In the event of a ran- somware attack, the hospital would not have to pay the $1.2M ransom, but it would cost the hospital $20,000 to restore service from the back-up database. Considering only costs, should the hospital take the option?