COMP435 In Class Practice 8/17/26 Name: _____

Question 1: Attackers and Defenders Suppose COMP 435 has a class website featuring **Milton the Virtual Cat**.

The site has the following security policy:

- Anyone may view Milton.
- Each student may feed Milton **once per day**.
- Students may only change **their own** feeding preferences.
- Only course staff may rename Milton.
- The site should remain available for legitimate users.

An adversary is a student whose goal is to cause harmless chaos or become the *#1 Milton feeder*. The adversary has a normal student account, a web browser, and knowledge of how the site behaves.

1.1. For each of the following, identify one example.

1. An **asset** the system is protecting:

2. A **security policy** the adversary might try to violate:

3. A possible **harm** caused by violating that policy:

1.2. The attacker's first idea is to repeatedly click the `Feed Milton` button.
The defender responds by requiring users to log in before feeding Milton.
What might the attacker try next?

1.3. Continue the attacker–defender game with your group.
For each round:

- The **defender** proposes a countermeasure.
- The **attacker** proposes a new technical way to violate *any one* of the policies.

Do not use physical threats or attacks on people. Focus on the technical system.

Defender: Countermeasure	**Attacker: New Attack**
Require login before feeding Milton.	Create or use multiple accounts.
2.	2.
3.	3.
4.	4.
5.	5.

1.4. Suppose the defender eventually prevents all of the attacks your group has proposed.
Now the instructor adds a new feature:

> Students may upload a profile picture of their own cat.

How might this change the attack surface? Give one new attack or security concern that the defender now needs to consider.

1.5. Compare the goals of the attacker and defender.

1. What does the attacker need to accomplish to "win"?

2. What does the defender need to accomplish to "win"?

3. Which job seems easier? Why?

1.6. Based on this activity, complete the following statement in your own words:

> Security is challenging because an attacker only needs to _____,
> while a defender must _____.

Question 2: Analyzing Attack Trees We will answer a few questions reasoning about attack trees.

2.1. Given the tree on the board, what is the cheapest attack an attacker could launch?

2.2. Will AND nodes labeled "requires collusion" propagate upwards?

2.3. Will OR nodes labeled "requires collusion" propagate upwards?