COMP435 In Class Practice 8/21/26 Name: _____

Question 1: Analyzing Attack Trees We will answer a few questions reasoning about attack trees.

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

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

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

Question 2: Threat Modeling the 2020 Twitter Account Takeover In 2020, attackers gained access to internal Twitter tools and used that access to take control of several high-profile accounts.

For this activity, assume the attacker's overall goal is:

Take control of a high-profile Twitter account

2.1. Construct a simple **threat model** for this scenario.

1. What assets are we trying to protect?

2. Who is the adversary? What is their motivation?

3. What capabilities or resources might the adversary have?

4. What assumptions are we making about the system or attacker?

5. Give one example of an attack that is **in scope** and one that is **out of scope** for your threat model.

2.2. Consider the following first level of an attack tree:
Choose **one** of the three branches above and expand it by at least **two additional levels**.
Your tree should:

- include at least three new nodes,
- identify whether child nodes represent an **AND** or **OR** relationship where appropriate,
- describe concrete steps an attacker might take (each node should be a subgoal).

Take control of a high-profile Twitter account

↓

Compromise the account owner | Abuse Twitter's internal access | Exploit the platform directly

2.3. Suppose the defender successfully blocks the attack path you identified above.
Does that mean the system is now secure? Why or why not?