COMP435 WA1 Name: ____________________

Question 1: Building an Attack Tree Build an attack tree. The goal of the attack is to reset the victim's passwrod to their UNC email account to a password of the attacker's choosing.

The tree must include at least one root-to-leaf path that is at least 3 nodes deep. The tree must have at least one AND set and at least one OR set. Use the correct notation to label the AND and OR sets. Make sure each node, including the root node, is clearly labeled. In addition, point out which node is the root node and which are the leaf nodes.

Finally, there are many attacks you might come up with, imagine reading your answer out loud in front of someone whose respect you would like to earn, maybe a supervisor – don't be lewd and don't include graphic depictions of violence.

Question 2: Security Primitives For each of the following system requirements, identify the security primitive being described (confidentiality, integrity, availability, accountability).

2.1. The system must ensure that all registered IoT devices can reliably connect even during peak hours.

2.2. TLS ensures that sensitive data in transit between client and server cannot be read by eavesdroppers

2.3. A version-control system (e.g., Git) prevents force-pushing rewritten history without administrator approval.

2.4. Audit logs must record the exact user ID and timestamp for every configuration change.

Question 3: Security Policies The computer science department allows faculty to use Google Drive to store course information, including students' names and grades. We must use our @cs.unc.edu accounts, which are backed and maintained by Google. (I.e., our @cs.unc.edu email accounts are actually gmail accounts.) Federal law lays out strict confidentiality requirements around student information, including enrollment status and grades. List two reasonable security policies that our department expects of Google Drive in order to ensure we remain in compliance with federal law. For each policy, describe why or how a violation of that policy could be harmful. Finally, for each policy, describe what an attacker's motivation might be for violating the policy. Write your answer using complete sentences and be specific in your answers. (For example, an answer that says only "provide confidentiality" will not receive much credit.)

3.1. Policy (1):

3.2. How a violation might be harmful (1):

3.3. Attacker's Motivation (1):

3.4. Policy (2):

3.5. How a violation might be harmful (2):

3.6. Attacker's Motivation (2):