Task 1:

Give an example Role-Based Access Control (RBAC) specification that cannot be expressed using Discretionary Access Control (DAC).

An example could be assigning a user as a custodian or an end-user. Assigning the user as an owner would not be an example because DAC assigns an owner to every object, making it the least restrictive.

Task 2:

Assume you need to develop an RBAC policy for the class materials in an online course. Briefly describe the components of RBAC using an example of an online course you have taken in the past.

For an RBAC policy for an online class, a role could be given to students in the class and professors for the class. The students should be given access to read all notes, assignments, assessments, announcements, discussion posts, and other materials and information designed for student use in the course. Moreover, for assignments and assessments, students should be given write access in order to submit answers and work. Not only that, students may also need write access for discussion posts. However, students should not have access to read or write privileges in folders that contain information intended only for professors, like answer keys and the grades of other students. Additionally, no student should be able to have write access to edit anything that the professor can only create, specifically notes, assignment and assessment information and dropboxes, and class announcements. Lastly, students should not have write access to edit over the work or discussion posts of other students in the course. On the professor's side, there should be read and write access for all previously mentioned resources for only the class or classes that he or she is teaching. The only things the professor should not have write access for is editing answers, work, and discussion posts from students.

Task 3:

Describe a potential misuse of the resources from your example from Task 2 by one of the users (for instance, another faculty/student) that the access control model prevents.

The access control model example from task 2 would help prevent any and all users who are either not taking the class as students or instructing the class as professors from entering the online class due to the RBAC policy. The only potential concerns would be if users outside the online class either obtain the login credentials of approved users or they steal the devices the approved users access the online class on. These situations are best avoidable with two-factor

authentication, very strong passwords, and refraining from using any devices near crowded areas when possible.

Task 4:

Consider the scenario where an organization allows its employees to access confidential customers' data via a web site. To login to the website, employees use their last name and a password. For simplicity, the same password is assigned to all employees, and then delivered via unencrypted email. Describe a misuse of the web application by a malicious attacker. Explain the:

- Motivation
- Opportunity
- Method

What security technologies would you recommend mitigating the above misuse and why?

One of the primary system security concerns for this organization is that all of the passwords are initially assigned to be the same for every user. This attacking opportunity is also tempting because default passwords are oftentimes easy to come across and may not require any hacking experience. All the attacker would have to do is locate websites that are known to hold many default passwords, like the one being used to function the dpl4hydra command, which is part of the Hydra Kali Linux tool. If the default password used by the organization gets discovered, then all computers in the organization are at extreme risk because the attacker could harmfully modify or delete customer or organization data. Not only that, there is also the situation of no encryption being performed on email services, which once again lowers the security of customer and organization data. On top of these harmful impacts, attackers could jeopardize the organization's network by transferring malicious software via methods like phishing, especially if an email is accidently sent to the wrong recipient. Motivators for an attack on this system could also include anything from a fired worker wanting revenge by deleting essential files to an unknown attacker desiring to load ransomware onto the system in order to demand a massive amount of money.

To solve the password problem, users should first be allowed to make their own passwords, but with password policy settings that enforce a minimum length requirement, preferably of at least 12 characters, and complexity to make them as unguessable as possible. Not only that, an additional password policy should be set that ensures passwords are changed approximately every 90 days as an extra security measure in case any of the employee's passwords were found in recent data breaches. Secondly, the unencrypted email issue should be solved with an asymmetric cryptography algorithm to provide five layers of security to the organization's system, including confidentiality, integrity, availability, authenticity, and non-repudiation. A convenient way to apply this plan for all computers in the network is to use an asymmetric

cryptography system, like Pretty Good Privacy and GNU Privacy Guard, which both encrypt files and email messages.

Task 5:

Indicate the read/write privileges for the following scenario of university departments: Let

- F1, F2 be faculty at Computer Science (CS); F3 Faculty at Electrical Engineering (EE); F4 Faculty at Human Computer Interaction (HCI); F5 faculty of all three departments.
- Resources r1 belong to CS; r2 to EE; r3 to HCI;
- Students s1, s2, s3, s4 belong to CS; s5, s6, s7 to EE; s8, s9 to HCI

- Students s1, s2, s3, and s4:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the CS courses that they are taking, presuming that they are made available by one of the CS faculty members and do not contain confidential information intended only for the faculty of the CS department.
    - Write access for assignments, assessments, and discussion posts for the CS courses they are taking.

- Faculty F1 and F2:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the CS courses that F1 and F2 are teaching.
    - Write access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the CS courses that F1 and F2 are teaching, with the exception of submitted assignments, assessments, and discussion posts from the CS students.

- Resource r1:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for all CS courses.
    - Write access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for all CS courses, specifically in the event where any of these sources do not submit properly when used by CS students and/or faculty.

- Students s5, s6, and s7:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the EE courses that they are taking, presuming that they are made available by one of the EE faculty members and do not contain confidential information intended only for the faculty of the EE department.

    - Write access for assignments, assessments, and discussion posts for the EE courses they are taking.

- Faculty F3:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the EE courses that F3 is teaching.
    - Write access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the EE courses that F3 is teaching, with the exception of submitted assignments, assessments, and discussion posts from the EE students.

- Resource r2:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for all EE courses.
    - Write access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for all EE courses, specifically in the event where any of these sources do not submit properly when used by EE students and/or faculty.

- Students s8 and s9:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the HCI courses that they are taking, presuming that they are made available by one of the HCI faculty members and do not contain confidential information intended only for the faculty of the HCI department.
    - Write access for assignments, assessments, and discussion posts for the HCI courses they are taking.

- Faculty F4:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the HCI courses that F4 is teaching.
    - Write access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the HCI courses that F4 is teaching, with the exception of submitted assignments, assessments, and discussion posts from the HCI students.

- Resource r3:
    - Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for all HCI courses.
    - Write access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for all HCI courses, specifically in the event where any of these sources do not submit properly when used by HCI students and/or faculty.

- Faculty F5

- Read access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the CS, EE, and HCI courses that F5 is teaching.
- Write access to all folders, files, notes, announcements, assignments, assessments, and discussion posts for the CS, EE, and HCI courses that F5 is teaching, with the exception of submitted assignments, assessments, and discussion posts from the CS, EE, and HCI students.

Task 6:

Build an RBAC model to enforce the question 5 BLP (Bell–LaPadula model, [5]) rules. Note that the BLP model is another implementation of MAC.

All initial read/write privileges will still apply to this model. However, to enforce BLP rules, students will only be allowed to create new discussion posts and not folders, files, notes, announcements, assignments, or assessments in any and all courses. Additionally, these sources that are isolated to a single course should only be allowed to be sent to students taking that course. Lastly, students should not be able to modify any sources beyond their privileges to write discussion posts and answer questions for assignments and assessments. For example, faculty and resources can create and update online assignments and assessments for their corresponding course and department, but the students should not be allowed to change the questions or the correct answers.