Name: Ram Haygrev S Roll no:231901039

EX 3: Identity And Access Management

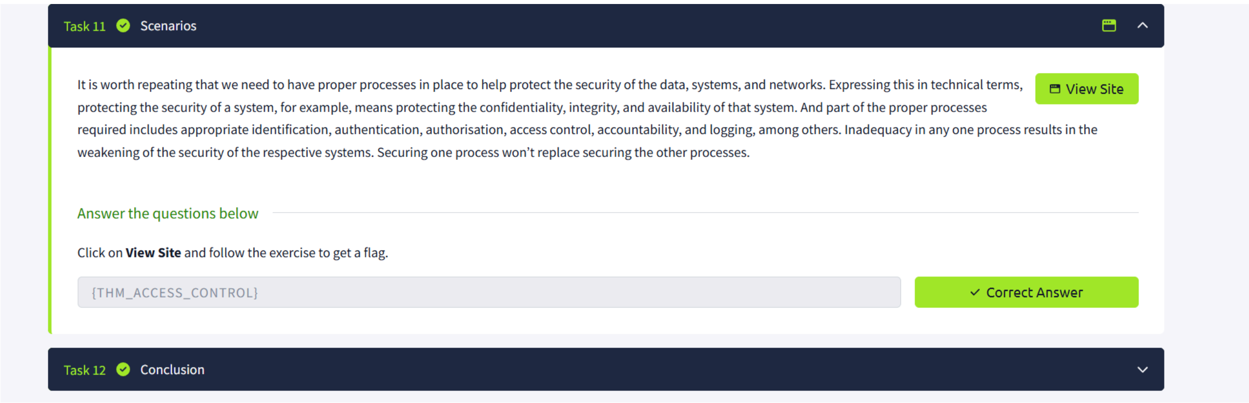
Date:

Aim:-

To learn about identity and access management.

ALGORITHM : N/A

Exercises:-



Task 11 ✓ Scenarios

It is worth repeating that we need to have proper processes in place to help protect the security of the data, systems, and networks. Expressing this in technical terms, protecting the security of a system, for example, means protecting the confidentiality, integrity, and availability of that system. And part of the proper processes required includes appropriate identification, authentication, authorisation, access control, accountability, and logging, among others. Inadequacy in any one process results in the weakening of the security of the respective systems. Securing one process won't replace securing the other processes.

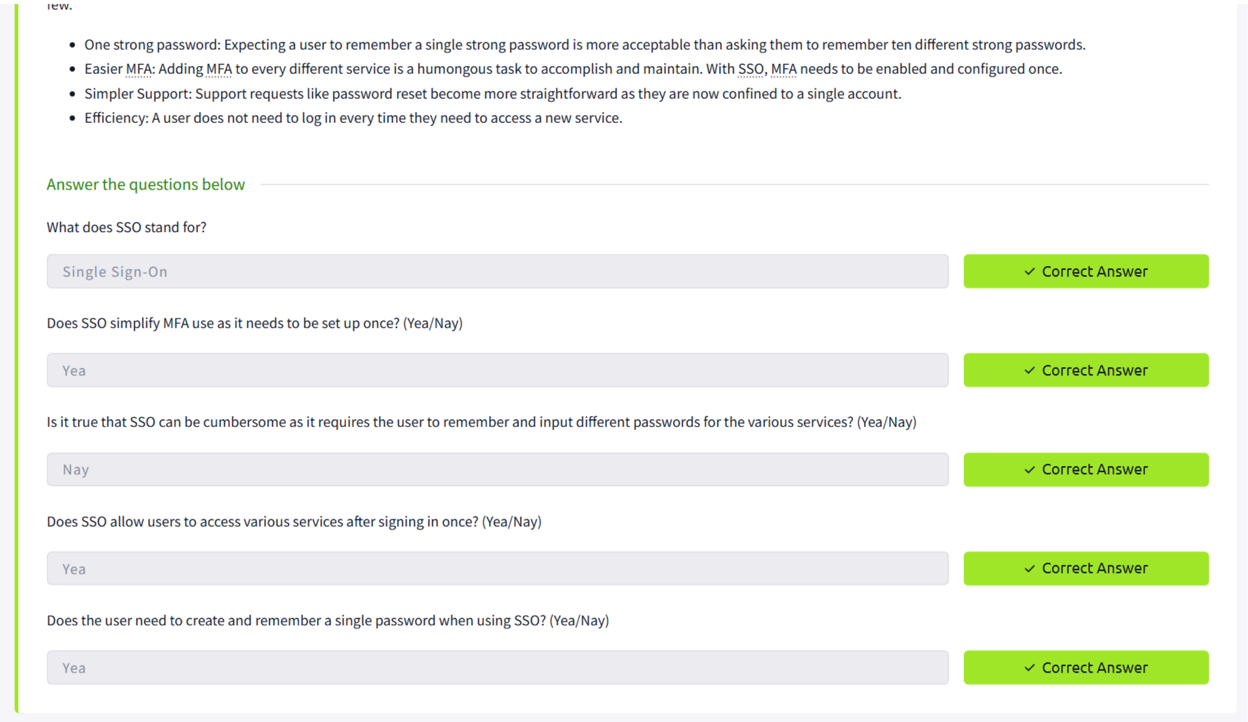
Answer the questions below

Click on **View Site** and follow the exercise to get a flag.

{THM_ACCESS_CONTROL}

Task 12 ✓ Conclusion

Name: Ram Haygrev S Roll no:231901039



few.

- One strong password: Expecting a user to remember a single strong password is more acceptable than asking them to remember ten different strong passwords.
- Easier MFA: Adding MFA to every different service is a humongous task to accomplish and maintain. With SSO, MFA needs to be enabled and configured once.
- Simpler Support: Support requests like password reset become more straightforward as they are now confined to a single account.
- Efficiency: A user does not need to log in every time they need to access a new service.

Answer the questions below

What does SSO stand for?

Single Sign-On

Does SSO simplify MFA use as it needs to be set up once? (Yea/Nay)

Yea

Is it true that SSO can be cumbersome as it requires the user to remember and input different passwords for the various services? (Yea/Nay)

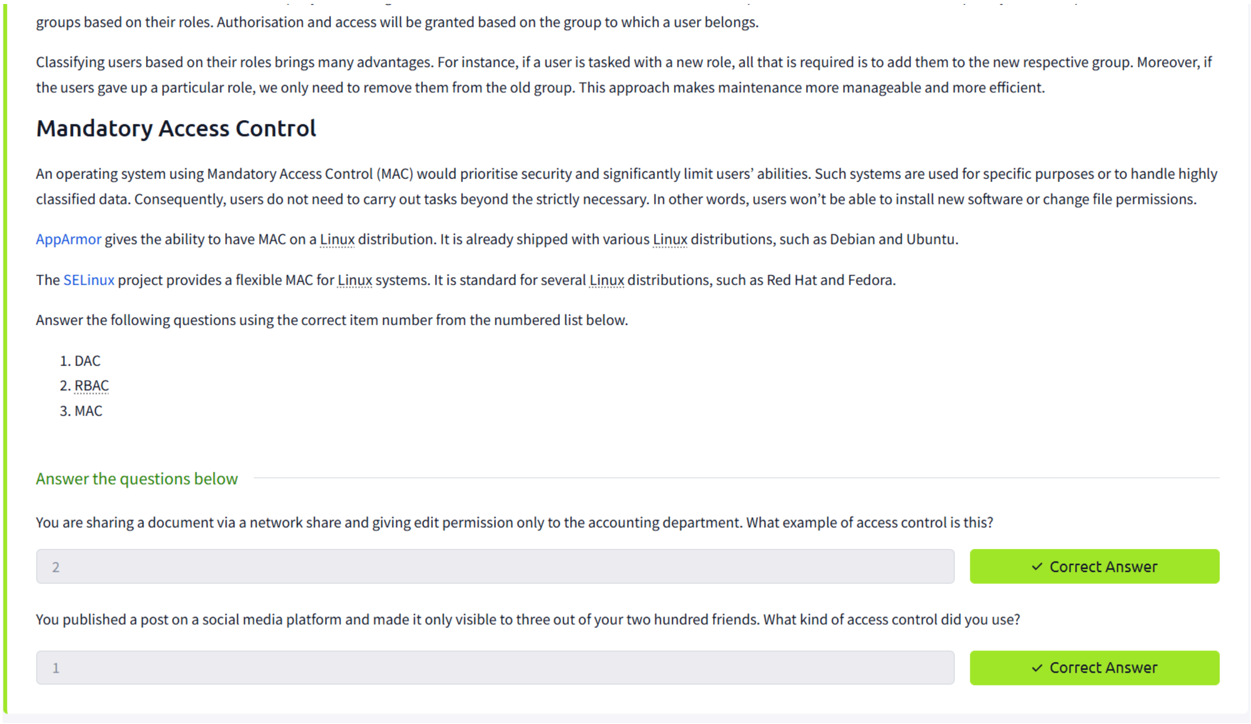
Nay

Does SSO allow users to access various services after signing in once? (Yea/Nay)

Yea

Does the user need to create and remember a single password when using SSO? (Yea/Nay)

Yea



groups based on their roles. Authorisation and access will be granted based on the group to which a user belongs.

Classifying users based on their roles brings many advantages. For instance, if a user is tasked with a new role, all that is required is to add them to the new respective group. Moreover, if the users gave up a particular role, we only need to remove them from the old group. This approach makes maintenance more manageable and more efficient.

Mandatory Access Control

An operating system using Mandatory Access Control (MAC) would prioritise security and significantly limit users' abilities. Such systems are used for specific purposes or to handle highly classified data. Consequently, users do not need to carry out tasks beyond the strictly necessary. In other words, users won't be able to install new software or change file permissions.

AppArmor gives the ability to have MAC on a Linux distribution. It is already shipped with various Linux distributions, such as Debian and Ubuntu.

The SELinux project provides a flexible MAC for Linux systems. It is standard for several Linux distributions, such as Red Hat and Fedora.

Answer the following questions using the correct item number from the numbered list below.

1. DAC
2. RBAC
3. MAC

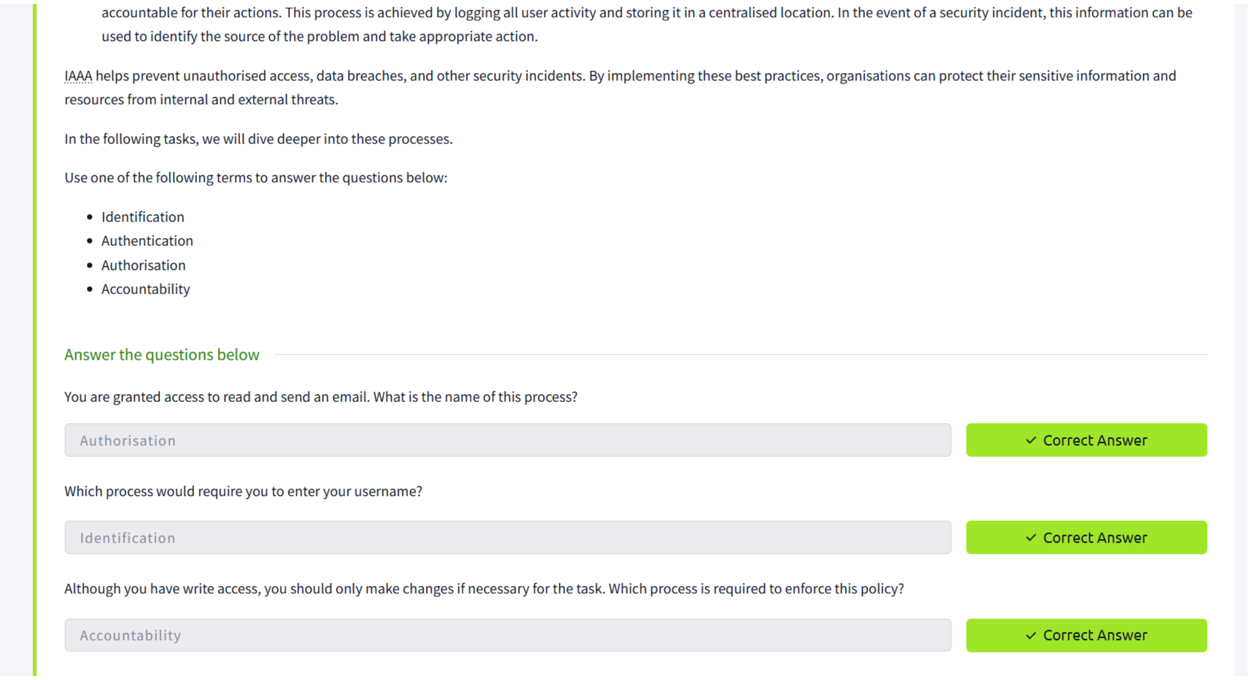
Answer the questions below

You are sharing a document via a network share and giving edit permission only to the accounting department. What example of access control is this?

2

You published a post on a social media platform and made it only visible to three out of your two hundred friends. What kind of access control did you use?

1



accountable for their actions. This process is achieved by logging all user activity and storing it in a centralised location. In the event of a security incident, this information can be used to identify the source of the problem and take appropriate action.

IAAA helps prevent unauthorised access, data breaches, and other security incidents. By implementing these best practices, organisations can protect their sensitive information and resources from internal and external threats.

In the following tasks, we will dive deeper into these processes.

Use one of the following terms to answer the questions below:

- Identification
- Authentication
- Authorisation
- Accountability

Answer the questions below

You are granted access to read and send an email. What is the name of this process?

Authorisation

Which process would require you to enter your username?

Identification

Although you have write access, you should only make changes if necessary for the task. Which process is required to enforce this policy?

Accountability

Result: Hence the exercises were completed successfully