Operating Systems - Week 7

Khaula Molapo

1. Scenario Analysis

A good security setup for an IT system like a cloud operating system should focus on protecting data, users, and resources. The setup should include firewalls, antivirus software, and intrusion detection systems to monitor network traffic and block harmful actions. User accounts must have strong passwords and two-factor authentication for extra protection. The system should use encryption to protect data during transfer and storage, making it unreadable to unauthorized people. Access to resources must be limited by user roles, so only specific users can perform certain actions. Regular updates and patches are important to close security gaps. Administrators should perform regular backups and store them safely to recover data in case of an attack or failure. Security logs should be checked often to find any strange activities. This setup ensures that even if one part fails, the rest of the system stays safe and working properly.

2. Concept Research

RBAC, or Role-Based Access Control, is a security model used to control who can access what in a computer system. Instead of giving permissions directly to users, the system gives them roles such as admin, editor, or viewer. Each role has a specific set of permissions, and users get access based on their role. This makes managing permissions easier and reduces the risk of mistakes. For example, an admin can change system settings, while a viewer can only read information. RBAC improves security by preventing unauthorized users from accessing sensitive data and simplifies user management in large systems.

3. Tool Practice

In VirtualBox, encryption can be configured to protect virtual machine data from unauthorized access. To do this, you go to the settings of a virtual machine, select the encryption tab, and set a password with an encryption algorithm like AES. Once activated, VirtualBox encrypts the virtual disk, making it unreadable without the correct password. This ensures that even if someone copies the VM file, they cannot open it without permission. Using encryption helps keep sensitive information safe, especially when running operating systems that handle private data. It adds a layer of protection that is easy to set up but very effective in practice.

4. Application Practice

A security policy is a set of rules that guide how users and systems should protect data and resources. It defines what users can and cannot do, how passwords should be created, and how data should be stored and shared. A good policy also includes steps to handle security breaches and backup plans for emergencies. Its purpose is to make sure everyone follows the same safety rules to prevent data loss, hacking, or misuse. For example, the policy may require regular password changes or restricted use of USB drives. By having a clear policy, an organization can reduce risks and create a safer working environment.