Computer Security Week 7

Khaula Molapo

Scenario Analysis

In an IT system like a cloud platform, access control is very important to keep things safe. The setup includes different user levels such as admin, staff, and clients. Each level can only access what they need. For example, admins can manage servers and data, staff can update customer info, and clients can only see their own data. The system uses passwords, two-step verification, and sometimes biometrics to make sure the right person is logging in. Roles are managed through a central database. Permissions are reviewed often to prevent abuse. Logging and monitoring tools record every action in the system, helping detect strange behavior early. This makes the setup secure and efficient while keeping users' data safe.

Concept Research

ABAC (Attribute-Based Access Control) is a method that gives or denies access based on user attributes like role, time, or location. Instead of using just roles like in RBAC, ABAC looks at multiple conditions to decide access. For example, an employee can access a file only during work hours and from a company device. This makes it flexible and secure for big organizations. It's mostly used in systems that need strong data protection, such as cloud services and government databases. ABAC helps reduce mistakes by automatically applying rules instead of relying only on human decisions.

Tool Practice

In VirtualBox, I configured SELinux to control what processes and users can do inside the system. It was a bit tricky at first, but once I understood the basics, it made sense. SELinux uses rules called policies to decide who can access what. It's like a strict security guard inside Linux that checks every action. During the setup, I learned to switch between enforcing, permissive, and disabled modes. Enforcing mode blocks actions that break rules. This tool is great because it adds another layer of defense if something gets compromised. It's a must for anyone serious about system security.

Application Practice

An access control policy helps manage who can use what inside an organization’s IT system. I designed one where users are grouped by role — admins, managers, and regular staff. Each group has certain rights, and sensitive data is protected with extra verification. The policy also says how passwords are created, how long sessions last, and how to handle failed logins. There’s also a rule that access rights must be reviewed every three months. This policy keeps systems organized and reduces the risk of data leaks or unauthorized access. It helps build trust and protects company data from being misused.