Enhanced User Acess and Password Policy Enforcement with PAM

Monday, November 18, 2024 1:14 PM

This project focuses on securing the Dunder Mifflin network by implementing user-specific access controls and enforcing a robust password policy across all Linux machines using the **PAM (Pluggable Authentication Module)**. These changes address security concerns and ensure compliance with organizational policies.

Key Features

1. **User-Specific Login Restrictions**:
    - Configured **PAM access control** to restrict logins to specific users based on the machine:
        - **All Machines**: Only root, the system administrator, Michael Scott, and Dwight Schrute can log in.
        - **Machine E**: All users are allowed to log in.
        - **Machines C and D**: Limited to Pam Beesly, Andy Bernard, Kelly Kapoor, and the users in (1).
        - **Machine F**: Access restricted to members of the accounting group and the users in (1).
2. **Centralized User Accounts**:
    - Ensures consistency by synchronizing /etc/passwd and /etc/shadow files across all Linux machines.
3. **Robust Password Policy**:
    - Enforced through **PAM pwquality module**:
        - Minimum password length: **10 characters**.
        - At least **2 digits**, **2 uppercase letters**, and **1 non-alphanumeric character**.
        - Length credit is not granted for lowercase characters.
    - Applies the policy to password changes without expiring existing passwords.
    - Explicitly defined all parameters in /etc/security/pwquality.conf for consistency across systems.
4. **Time-Based Access Control:**
    Configured PAM to restrict logins for all users (except root, the system administrator, and Dwight Schrute) on **Machines C and D** to weekdays between **9 AM and 5 PM**.

This project enhances security by combining user-specific access controls, time-based restrictions, and strict password requirements, ensuring a safer and more controlled DMZ environment for Dunder Mifflin.