Task 9
PASSWORD POLICY CREATION

CREATE A PASSWORD POLICY FOR A COMPANY THAT ENFORCES STRONG AND UNIQUE PASSWORDS

1. Password Complexity:

- Password Length: Encourage or mandate passwords that are at least 12 characters long. Longer passwords provide greater security against brute force attacks.
- Character Types: Require a mix of uppercase and lowercase letters, numbers, and special characters (e.g., !, @, #, $). This complexity adds entropy, making it more challenging for attackers to guess or crack passwords.

2. Password Expiry:

- Regular Interval: Set a 90-day expiration period for passwords. Regularly changing passwords helps mitigate the risk of unauthorized access due to compromised credentials.
- Password History: Prohibit the reuse of the last five passwords. This prevents users from cycling through a small set of passwords, enhancing security.

Task 9
PASSWORD POLICY CREATION

3. Account Lockout:

- Failed Login Attempts: Implement an account lockout policy after five consecutive failed login attempts. This guards against brute force attacks by temporarily locking out an account.
- Lockout Duration: Choose a lockout duration, such as 30 minutes. This provides a balance between security and preventing inconvenience for users.
- Administrator Intervention: Allow for administrator intervention to unlock accounts in case of genuine issues, reducing the risk of denial-of-service attacks against user accounts.

4. Two-Factor Authentication (2FA):

- Enable or Mandate: Encourage or mandate the use of 2FA. This adds an extra layer of security, requiring users to provide a second form of authentication in addition to their passwords.
- Authentication Methods: Support various 2FA methods, such as SMS codes, authenticator apps, or hardware tokens.

Task 9
PASSWORD POLICY CREATION

5. Password Storage:

- Hashing Algorithms: Store passwords using strong cryptographic hashing algorithms (e.g., bcrypt, Argon2). Avoid older, less secure methods.
- Salting: Implement password salting to further enhance security. Salting involves adding a unique random value to each password before hashing, preventing attackers from using precomputed tables (rainbow tables) for attacks.

6. User Education:

- Regular Training: Conduct regular training sessions on password security best practices. Educate users on the importance of creating strong, unique passwords and recognizing phishing attempts.
- Simulated Attacks: Conduct simulated phishing attacks to help users identify and report potential threats.

7. Password Recovery:

- Multi-Step Process: Design a secure, multi-step password recovery process that verifies the user's identity without compromising security.
- Account Verification: Utilize secondary email addresses, mobile phone numbers, or other secure methods for account verification during the recovery process.

Task 9
PASSWORD POLICY CREATION

8. Third-Party Applications:

- Vendor Security Standards: Ensure that third-party applications and services adhere to or surpass the company's password policy. Verify that vendors follow secure coding practices and regularly update their systems to address vulnerabilities.

9. Unique Usernames:

- Avoid Predictability: Discourage the use of easily guessable usernames, such as first names or initials followed by a common surname. Unique usernames make it harder for attackers to target specific accounts.

10. Monitoring and Logging:

- Security Information and Event Management (SIEM): Implement a SIEM system to centralize and analyze log data for potential security incidents.
- Real-Time Alerts: Configure real-time alerts for suspicious login activities, including multiple failed login attempts or login attempts from unusual locations.

Task 9
PASSWORD POLICY CREATION

11. Regular Audits:

- Schedule periodic security audits to assess the effectiveness of the password policy.
- Include penetration testing and vulnerability assessments to identify and address potential weaknesses in the overall security infrastructure.

12. Password Managers:

- Encourage Adoption: Promote the use of reputable password managers to generate, store, and autofill complex passwords.
- Training and Support: Provide training and support for employees to effectively use password managers across various devices.

13. Mobile Device Security:

- Strong Password Requirements: Enforce strong password policies for mobile devices, including a mix of characters and regular password updates.
- Biometric Authentication: Encourage the use of biometric authentication features (e.g., fingerprint or facial recognition) on mobile devices for an additional layer of security.

Task 9

PASSWORD POLICY CREATION

14. Employee Departure Process:

- Access Revocation: Develop a comprehensive process for promptly revoking access when employees leave the company or change roles.
- Exit Interviews: Conduct exit interviews to remind departing employees of their responsibility to return company devices and credentials.

15. Continuous Improvement:

- Stay Informed: Regularly monitor industry trends, new cyber threats, and advancements in security technology.
- Policy Review: Schedule periodic reviews of the password policy to ensure it remains aligned with the current threat landscape and industry best practices.