LESSON NOTES

CYBERSECURITY

Domain 4.0 - Security Operations

4.6.3 - Passwords

Lesson Overview:

Students will:

- Investigate common password concepts.

Guiding Question: What are some common password concepts?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

4.6 - Given a scenario, implement and maintain identity and access management

- Password concepts
  - Password best practices
    - Length
    - Complexity
    - Reuse
    - Expiration
    - Age
  - Password managers
  - Passwordless

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Passwords

Password Best Practices

The following are some common password best practices:

- *Length*: Longer passwords are generally more secure. Aim for a minimum password length and encourage users to create complex, memorable passphrases. Longer passwords provide a larger search space, making brute-force attacks more difficult.

- *Complexity*: Advocate for the use of complex passwords that include a mix of uppercase and lowercase letters, numbers, and special characters. Complex passwords increase the complexity of attacks, reducing the likelihood of successful brute-force or dictionary attacks.

- *Reuse*: Discourage password reuse across multiple accounts. Encourage users to use unique passwords for different services. Password reuse increases the risk of unauthorized access if one account is compromised.

- *Expiration*: Implement password expiration policies, requiring users to change their passwords periodically. Regularly changing passwords helps mitigate the impact of potential credential compromises.

- *Age*: Set policies to restrict the use of old passwords. Users should not be able to revert to previous passwords. Prevents the reuse of old and potentially compromised passwords.

Password Managers

Password managers are tools or applications that help users generate, store, and manage complex and unique passwords for various accounts. Password managers enhance security by eliminating the need for users to remember multiple complex passwords, and they often include features like password generation and secure storage.

Password managers generate and store strong, unique passwords for each account. Users only need to remember a master password to access their password vault. Facilitates the management of multiple passwords in a secure and organized manner.

Passwordless

Passwordless authentication eliminates the need for traditional passwords. It relies on alternative authentication methods, such as biometrics, security keys, or one-time codes. This enhances security by reducing the reliance on passwords, which can be susceptible to various attacks. This uses unique physical or behavioral characteristics for user identification (e.g., fingerprints, facial recognition). Examples of security keys include physical devices, often USB-based, used for secure authentication. One-time codes are temporary codes generated and sent to a user's device for authentication.

The elimination of passwords reduces the risk of password-related attacks, such as phishing and credential theft. The user experience sees improvement with a more convenient and user-friendly authentication process. Stronger authentication methods contribute to increased security.

While passwordless authentication provides enhanced security and user experience, organizations need to carefully evaluate and implement these methods based on their specific needs, user base, and security requirements.

Password concepts encompass best practices for creating and managing passwords, the use of password managers to enhance security, and the adoption of passwordless authentication methods to reduce reliance on traditional passwords. Implementing these concepts contributes to a more secure and user-friendly authentication environment.