Identity and Access Management (IAM) Solutions

Objectives:

- 2.4 - Given a scenario, you must be able to analyze indicators of malicious activity
- 4.6 - Given a scenario, you must be able to implement and maintain identity and access management

- **Identity and Access Management (IAM) Solutions**
    - *Identity and Access Management (IAM)*
        - Ensures right individuals have right access to right resources for right reasons
        - Components
            - Password Management
            - Network Access Control
            - Digital Identity Management
    - IAM Processes
        - Identification, Authentication, Authorization, and Accounting (IAAA)
        - IAM System Processes
            - *Identification*
                - Claiming identity, e.g., username, email address
            - *Authentication*
                - Verifying user, device, or system identity
            - *Authorization*
                - Determining user permissions after authentication
            - *Accounting*
                - Tracking and recording user activities

- IAM Concepts
  - Processes
    - Provisioning
    - Deprovisioning
    - Identity Proofing
    - Interoperability
    - Attestation
- *Multi Factor Authentication (MFA)*
  - Factors
    - Something you know
    - Something you have
    - Something you are
    - Something you do
    - Somewhere you are
  - Implementations
    - Biometrics
    - Hard tokens
    - Soft tokens
    - Security keys
    - Passkeys
- Password Security
  - Best Practices
    - Password policies
    - Password managers
    - Passwordless authentication

- Password Attacks
  - Types
    - Spraying Attacks
    - Brute Force Attacks
    - Dictionary Attacks
    - Hybrid Attacks
- *Single Sign-On (SSO)*
  - User authentication service using one set of credentials for multiple applications
  - Technologies
    - LDAP
    - OAuth
    - SAML
- *Federation*
  - Sharing and using identities across multiple systems or organizations
- *Privileged Access Management (PAM)*
  - Involves the following
    - Just-in-Time (JIT) Permissions
    - Password Vaulting
    - Temporal Accounts
- Access Control Models
  - Mandatory Access Control
  - Discretionary Access Control
  - Role-based Access Control
  - Rule-based Access Control
  - Attribute-based Access Control

- Assigning Permissions
  - Best practices to enhance organization security

- **Identity and Access Management (IAM)**
  - *Identity and Access Management (IAM)*
    - Critical component of enterprise security, focusing on managing access to information
    - Ensures the right individuals have access to the right resources at the right times for the right reasons
  - Four Main IAM Processes
    - *Identification*
      - User claims an identity using a unique identifier (e.g., username or email address)
      - Ensures user legitimacy and accuracy of provided information
    - *Authentication*
      - Verifies the identity of a user, device, or system
      - Typically involves validating user credentials against an authorized user database
      - Methods
        - Passwords
        - Biometrics
        - Multi-factor authentication
    - *Authorization*
      - Determines the permissions or access levels for authenticated users
      - Ensures users have access only to appropriate resources
      - Role-based access control often used

- *Accounting (Auditing)*
  - Tracks and records user activities
    - Logins
    - Actions
    - Changes
  - Helps detect security incidents, identify vulnerabilities, and provide evidence in case of breaches

- Key IAM Concepts
  - Provisioning and Deprovisioning of User Accounts
    - *Provisioning*
      - Creating new user accounts, assigning permissions, and providing system access
    - *Deprovisioning*
      - Removing access rights when no longer needed (e.g., when an employee leaves)
  - *Identity Proofing*
    - Process of verifying a user's identity before creating their account
    - May involve checking personal details or providing identification documents (e.g., driver's license or passport)
  - *Interoperability*
    - Ability of different systems, devices, and applications to work together and share information
    - In IAM, it can involve using standards like SAML or OpenID Connect for secure authentication and authorization
  - *Attestation*
    - Process of validating that user accounts and access rights are correct and

up-to-date

- Involves regular reviews and audits of user accounts and their access rights

- **Multi-factor Authentication**
  - *Multi-factor Authentication (MFA)*
    - A security system requiring multiple methods of authentication from independent categories of credentials
    - Enhances security by creating a layered defense against unauthorized access
  - Five Categories of Authentication for MFA
    - *Something You Know (Knowledge-Based Factor)*
      - Authentication based on information the user knows, like a password, PIN, or answers to secret questions
    - *Something You Have (Possession-Based Factor)*
      - Authentication based on physical possession of an item
        - Smart card
        - Hardware token (key fob)
        - Software token on a device
    - *Something You Are (Inherence-Based Factor)*
      - Authentication based on biometric characteristics unique to individuals
        - Fingerprints
        - Facial recognition
        - Voice recognition
    - *Somewhere You Are (Location-Based Factor)*
      - Authentication based on the user's location, determined through IP address, GPS, or network connection

- Geographical location restrictions can be applied

- *Something You Do (Behavior-Based Factor)*
  - Authentication based on recognizing unique patterns associated with user behavior
    - Keystroke patterns
    - Device interaction
  - Rarely used as a primary factor but can provide an additional layer of security

- Authentication Types
  - *Single Factor Authentication*
    - Uses one authentication factor to access a user account
  - *Two Factor Authentication (2FA)*
    - Requires two different authentication factors to gain access
  - *Multi-factor Authentication (MFA)*
    - Uses two or more factors to authenticate a user
    - MFA can involve 2, 3, 4, or 5 factors depending on the chosen configuration
      - Generally, using more authentication types makes a system safer, but is less convenient for the end user
  - Knowledge-based factors like passwords and PINs are the most common authentication methods
    - Password managers can generate different long, strong, and complex passwords for each website or application
  - *Passkeys (Passwordless Authentication)*
    - An alternative to traditional passwords for authentication
    - Involves creating a passkey secured by device authentication methods like

fingerprint or facial recognition
    - Provides a more secure and user-friendly authentication method
    - Passkeys utilize public key cryptography

- **Password Security**
    - *Password Security*
        - Measures the effectiveness of a password in resisting guessing and brute-force attacks
        - Estimates the number of attempts needed to guess a password correctly
    - Group Policy Editor for Password Policies
        - Used to create password policies in Windows
        - Available for local machines, and global policy orchestrator can be used in domain environments
    - Five Characteristics of Password Policies
        - Password Length
            - Longer passwords are harder to crack
            - Strong passwords should be at least 12 to 16 characters
            - Longer passwords increase security exponentially
        - Password Complexity
            - Combines uppercase and lowercase letters, numbers, and special characters
            - Complexity makes passwords resistant to brute force attacks
            - The more character choices, the more secure the password
        - Password Reuse
            - Avoid using the same password for multiple accounts
            - Reusing passwords increases vulnerability

- Password Expiration
  - Requires users to change passwords after a specific period
  - Overemphasis on expiration can lead to poor password choices
- Password Age
  - Password age refers to the time a password has been in use
  - Older passwords have a higher risk of being compromised

- *Password Managers*
  - Tools for storing and managing passwords securely
  - Features
    - Password generation
      - Password managers create unique strong passwords for accounts to prevent reuse and enhance security
    - Auto-fill
      - Password managers autofill login details, sparing users the need to recall or input information manually
    - Secure sharing
      - Password managers provide secure methods to share passwords without directly disclosing the password itself
    - Cross-platform access
      - Password managers offer cross-device compatibility, allowing access to passwords from any location or device
  - Promote password complexity, prevent reuse, and offer easy access to strong, unique passwords
- Passwordless Authentication Methods
  - Provide a higher level of security and better user experience

- Methods
  - *Biometric Authentication*
    - Uses unique biological characteristics
  - *Hardware Token*
    - Generate ever-changing login codes
  - *One-Time Passwords (OTP)*
    - Sent to email or phone for one-time use
  - *Magic Links*
    - One-time links sent via email for automatic login
  - *Passkeys*
    - Rely on device screen lock for authentication

- **Password Attacks**
  - *Password Attacks*
    - Methods used by attackers to crack or recover passwords
    - Types of password attacks
      - Brute Force
      - Dictionary
      - Password Spraying
      - Hybrid
  - *Brute Force Attack*
    - Tries every possible character combination until the correct password is found
    - Effective for simple passwords but time-consuming for complex ones
    - Mitigation
      - Increasing password complexity and length
      - Limiting login attempts

        - Using multi factor authentication
        - Employing CAPTCHAS
    - *Dictionary Attack*
        - Uses a list of commonly used passwords (a dictionary) to crack passwords
        - May include variations with numbers and symbols
        - Effective against common, easy-to-guess passwords
        - Mitigation
            - Increase password complexity and length, limit login attempts, use multifactor authentication, and employ CAPTCHAS
    - *Password Spraying*
        - A form of brute force attack that tries a few common passwords against many usernames or accounts
        - Effective because it avoids account lockouts and targets weak passwords
        - Mitigation
            - Use unique passwords and implement multi-factor authentication
    - *Hybrid Attack*
        - Combines elements of brute force and dictionary attacks
        - May include variations, such as adding numbers or special characters to passwords
        - Can use a static dictionary or dynamically create variations
        - Effective for discovering passwords following specific patterns

- **Single Sign-On (SSO)**
    - *Single Sign-On (SSO)*
        - Authentication process allowing users to access multiple applications with one set of credentials

- Simplifies the user experience and enhances productivity
- Trusted relationship between applications and Identity Providers (IdP)

- How SSO Works
  - User logs into the primary identity provider (IdP)
  - Accesses a secondary application or website configured for SSO
  - The secondary application verifies the user's identity with the IdP's assertion
  - Once authenticated, access to the secondary application is granted
- Benefits of SSO
  - Improved user experience
  - Increased productivity
  - Reduced IT support costs
  - Enhanced security, encouraging stronger passwords
- Protocols for SSO
  - *LDAP (Lightweight Directory Access Protocol)*
    - Used to access and maintain distributed directory information
    - Can share user information across network resources
    - Supports central repository for authentication and authorization
    - Can be secured using LDAPS (LDAP over SSL or StartTLS)
    - LDAP stores user data for authorization, like group memberships and roles
  - *OAuth (Open Authorization)*
    - Open standard for token-based authentication and authorization
    - Allows third-party services to access user account information without exposing passwords
    - Often used in RESTful APIs for secure sharing of user profile data
      - The client app or service registers with the authorization server,

provides a redirect URL and gets an ID and secret

- Uses JSON Web Tokens (JWT) for data transfer

- *SAML (Security Assertion Markup Language)*
  - Standard for logging users into applications based on sessions in another context
  - Redirects users to an identity provider for authentication
  - Eliminates the need for services to authenticate users directly
  - Decouples services from identity providers, enhancing security and flexibility

- **Federation**
  - *Federation*
    - Links electronic identities and attributes across multiple identity management systems
    - Enables users to use the same credentials for login across systems managed by different organizations
    - Based on trust relationships between systems
    - Federation extends beyond an organization's boundaries
      - Partners
      - Suppliers
      - Customers
    - Simplifies user access to various services
    - Ensures security through trust relationships between networks
  - Federation Process
    - Login Initiation
      - User accesses a service or application and chooses to log in

- Redirection to Identity Provider
  - Service Provider (SP) redirects the user to their Identity Provider (IdP) for authentication
- Authentication of the user
  - IdP validates the user's identity using stored credentials
  - Validates the user's identity
- Generation of Assertion
  - IdP creates an assertion (token) with user identity and authentication status in a standardized format
- Return to Service Provider
  - User returns to the original service or application with the assertion from the IdP
- Verification and Access
  - Service Provider verifies the assertion and grants access based on the information it contains
- Login Complete
  - User gains access to the service or application and potentially others within the federation without additional logins

- Benefits
  - Simplified user experience
  - Reduced administrative overhead
  - Increased security through reduced password reuse and improved management

- **Privileged Access Management (PAM)**
  - *Privileged Access Management (PAM)*
    - Solution that restricts and monitors privileged access within an IT environment

        - The policies, procedures, and technical controls that are used to prevent malicious abuse of privileged accounts
        - Crucial for preventing data breaches and ensuring the least privileged access is granted for specific tasks or roles
    - Components of Privileged Access Management
        - *Just-In-Time Permissions (JIT Permissions)*
            - Security model that grants administrative access only when needed for a specific task
            - Reduces the risk of unauthorized access or misuse of privileges
            - Access rights are given when the task begins and revoked once the task is completed
        - *Password Vaulting*
            - Technique that stores and manages passwords securely, often in a digital vault.
            - Requires multi-factor authentication for accessing stored passwords
            - Tracks access to privileged credentials, providing an audit trail
        - *Temporal Accounts*
            - Temporary accounts used for time-limited access to resources
            - Created for specific purposes and automatically disabled or deleted after a predefined period

- **Access Control Models**
    - Different Types of Access Control Models
        - *Mandatory Access Control (MAC)*
            - Uses security labels to authorize resource access
            - Requires assigning security labels to both users and resources

- Access is granted only if the user's label is equal to or higher than the resource's label

- *Discretionary Access Control (DAC)*
  - Resource owners specify which users can access their resources
  - Access control based on user identity, profile, or role
  - Allows resource owners to grant access to specific users
- *Role-Based Access Control (RBAC)*
  - Assigns users to roles and assigns permissions to roles
  - Roles mimic the organization's hierarchy
  - Enforces minimum privileges
  - Effective for managing permissions based on job roles and turnover
- *Rule-Based Access Control*
  - Uses security rules or access control lists
  - Policies can be changed quickly and frequently
  - Applied across multiple users on a network segment
- *Attribute-Based Access Control (ABAC)*
  - Considers various attributes like
    - *User Attributes*
      - User’s name, role, organization ID, or security clearance
    - *Environment Attributes*
      - Time of access, data location, and current organization’s threat level
    - *Resource Attributes*
      - File creation date, resource owner, file name, and data sensitivity
  - Access decisions are based on the combination of attributes

        - Provides fine-grained control and dynamic access decisions
    - Access Control Extensions
        - *Time-of-Day Restrictions*
            - Limits access based on specific time periods
            - Often used to complement other access control models
            - Helps prevent unauthorized access during non-working hours
        - *Principle of Least Privilege*
            - Users are granted the minimum access required to perform their job functions
            - Reduces the risk of misuse or accidental damage
            - Regularly review and adjust permissions to prevent authorization creep

- **Assigning Permissions**
    - *Privileges*
        - Define the levels of access that users have
        - Local Administration Account
            - High level of access
            - Allows administrator to
                - change system settings
                - install softwares
                - perform a variety of managerial tasks
        - Standard User Accounts
            - Can’t change system settings
            - Can store files in their designated area only
    - *Principle of Least Privilege*
        - A user should only have the minimum access rights needed to perform their job

functions and tasks, and nothing additional or extra

- *Microsoft Account*
  - Free online account that you can use to sign in to a variety of Microsoft services
- *User Account Control (UAC)*
  - A mechanism designed to ensure that actions requiring administrative rights are explicitly authorized by the user
  - Access is limited to what the user needs to do a job
  - Purpose is to minimize the risk of users gaining access to administrative privileges
- Access control and permissions can also apply to groups of users
- File and Folder Permissions
  - Setting permissions at the folder level applies those permissions to all files within that folder
  - In Windows, these file and folder permissions are accessed by
    - Right-click on a file or folder
    - Select ‘Properties’
    - Navigate to the ‘Security’ tab
- Always ensure to only give out the necessary permissions