Secure Authentication Models

4.3 Given a Scenario, Implement Identity and Access Management

Description

- In this episode, we will look over the common authentication methods for cloud environements. This includes Federated Single Sign-On(SSO), SAML, OIDC, OATH, Hardware Tokens, and Directory Based.

Resources

- https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html
- https://cloud.google.com/iam/docs/workforce-identity-federation
- https://store.google.com/us/product/titan_security_key?pli=1&hl=en-US
- https://www.hidglobal.com/product-mix/crescendo

Learning Objectives

- Describe Federated Single-Sign-On
- Describe SAML, OATH, and OIDC
- Describe Directory Based systems used for authentication in cloud systems
- Define Hardware Tokens and explain how they are used for secure authentication

Notes

- Authentication models
    - Federation
        - SSO:
            - Allows users to log in once and gain access to multiple applications without needing to separately authenticate for each
        - Federated SSO:
            - Extends SSO by allowing users to authenticate across multiple domains|organizations using a central Identity Provider
        - Can authenticate Federated users using...
            - Security Assertion Markup Language (SAML)
                - XML-based standard
                - Relies on Identity Providers(IdP) like Okta for Authentication and Authorization
                    - IdP authenticates user to the Service Provider(SP) like SalesForce,M365,Google Workspaces,etc...
                        - Does this through the use of **Authentication Assertions**
            - OpenID Connect/OAuth 2.0
                - OAuth 2.0
                    - Provides **Authorization** for 3rd-parties(Clients) to act on behalf of Resource Owner
                - OpenID Connect (OIDC)
                    - Extension of OAuth 2.0
                    - JSON-based standard
                    - Utilizes Tokens (JWTs)
                    - This is the part that provides the Federated SSO authentication
        - Federated SSO in AWS
            - AWS (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp.html)
            - GCP (https://cloud.google.com/iam/docs/workforce-identity-federation)
    - Hardware Tokens

        - FIDO Key
            - Titan Security Key (https://store.google.com/us/product/titan_security_key?pli=1&hl=en-US)
        - Smart cards
            - HID Crescendo (https://www.hidglobal.com/product-mix/crescendo)
        - TOTP (Time-Based One Time Password)
            - Like an authenticator app
        - Other MFA
            - SMS
            - Email
    - Directory-based
        - MS AD
        - Entra ID (Formally Azure AD)
        - AWS Directory Service
        - Google Cloud Directory Sync