COURSE: SECURITY+ SY0-401

MODULE 5: ACCESS CONTROL AND IDENTITY MANAGEMENT
Overview

• Explain the importance of application security controls and techniques
• Compare and contrast the function and purpose of authentication services
• Given a scenario, select the appropriate authentication, authorization or access control
• Install and configure security controls when performing account management, based on best practices
Authentication Services

- RADIUS
- TACACS+
- Kerberos
- LDAP
- XTACACS
- SAML
- Secure LDAP
Authentication, Authorization and Access

- Identification vs. authentication vs. authorization
- Authorization
  - Least privilege
  - Separation of duties
  - ACLs
  - Mandatory access
  - Discretionary access
  - Rule-based access control
  - Role-based access control
  - Time of day restrictions
Authentication, Authorization and Access

- Authentication
  - Tokens
  - Common access card
  - Smart card
  - Multifactor authentication
  - TOTP
  - HOTP
  - CHAP
  - PAP
  - Single sign-on
  - Access control
  - Implicit deny
  - Trusted OS
Authentication, Authorization and Access

• Authentication factors
  • Something you are
  • Something you have
  • Something you know
  • Somewhere you are
  • Something you do

• Identification
  • Biometrics
  • Personal identification verification card
  • Username

• Federation

• Transitive trust/authentication
Account Management

• Mitigate issues associated with users with multiple account/roles and/or shared accounts

• Account policy enforcement
  • Credential management
  • Group policy
  • Password complexity
  • Expiration
  • Recovery
  • Disablement
  • Lockout
Account Management

Account policy enforcement

• Password history
• Password reuse
• Password length
• Generic account prohibition

• Group based privileges
• User assigned privileges
• User access reviews
• Continuous monitoring
THANK YOU