4.0 Identity and Access Management

4.1 Compare and contrast identity and access management concepts

- **Identification, authentication, authorization and accounting (AAA)**
- **Multifactor authentication**
  - Something you are
  - Something you have
  - Something you know
  - Somewhere you are
  - Something you do
- **Federation**
- **Single sign-on**
- **Transitive trust**

4.2 Given a scenario, install and configure identity and access services.

- **LDAP**
- **Kerberos**
- **TACACS+**
- **CHAP**
- **PAP**
- **MSCHAP**
- **RADIUS**
- **SAML**
- **OpenID Connect**
- **OAUTH**
- **Shibboleth**
- **Secure token**
- **NTLM**

4.3 Given a scenario, implement identity and access management controls.

- **Access control models**
  - MAC
  - DAC
  - ABAC
  - Role-based access control
  - Rule-based access control
- **Physical access control**
  - Proximity cards
  - Smart cards
- **Biometric factors**
  - Fingerprint scanner
  - Retinal scanner
  - Iris scanner
  - Voice recognition
  - Facial recognition
  - False acceptance rate
  - False rejection rate
  - Crossover error rate
- **Tokens**
  - Hardware
  - Software
  - HOTP/TOTP
- **Certificate-based authentication**
  - PIV/CAC/smart card
  - IEEE 802.1x
- **File system security**
- **Database security**

4.4 Given a scenario, differentiate common account management practices.

- **Account types**
  - User account
  - Shared and generic accounts/credentials
  - Guest accounts
  - Service accounts
  - Privileged accounts
- **General Concepts**
  - Least privilege
  - Onboarding/offboarding
  - Permission auditing and review
  - Usage auditing and review
  - Time-of-day restrictions
  - Recertification
  - Standard naming convention
  - Account maintenance
  - Group-based access control
  - Location-based policies
- **Account policy enforcement**
  - Credential management
  - Group policy
  - Password complexity
  - Expiration
  - Recovery
  - Disablement
  - Lockout
  - Password history
  - Password reuse
  - Password length

CompTIA