3.0 Security Engineering

3.1 Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment.

- **Subject access control**
  - User
  - Process
  - Device
  - Service
- **Biometrics**
- **Secrets management**
  - Tokens
  - Certificates
  - Passwords
  - Keys
  - Rotation
  - Deletion
- **Conditional access**
  - User-to-device binding
  - Geographic location
  - Time-based
  - Configuration
- **Attestation**
- **Cloud IAM access and trust policies**
- **Logging and monitoring**
- **Privilege identity management**
- **Authentication and authorization**
  - Security Assertions Markup Language (SAML)
  - OpenID
  - Multifactor authentication (MFA)
  - SSO
  - Kerberos
  - Simultaneous authentication of equals (SAE)
  - Privileged access management (PAM)
  - Open Authorization (OAuth)
  - Extensible Authentication Protocol (EAP)
  - Identity proofing
  - Institute for Electrical and Electronics Engineers (IEEE) 802.1X
  - Federation

3.2 Given a scenario, analyze requirements to enhance the security of endpoints and servers.

- **Application control**
- **Endpoint detection response (EDR)**
- **Event logging and monitoring**
- **Endpoint privilege management**
- **Attack surface monitoring and reduction**
- **Host-based intrusion protection system/host-based detection system (HIPS/HIDS)**
- **Anti-malware**
- **SELinux**
- **Host-based firewall**
- **Browser isolation**
- **Configuration management**
- **Mobile device management (MDM) technologies**
- **Threat-actor tactics, techniques, and procedures (TTPs)**
  - Injections
  - Privilege escalation
  - Credential dumping
  - Unauthorized execution
  - Lateral movement
  - Defensive evasion

3.3 Given a scenario, troubleshoot complex network infrastructure security issues.

- **Network misconfigurations**
  - Configuration drift
  - Routing errors
  - Switching errors
  - Insecure routing
  - VPN/tunnel errors
- **IPS/IDS issues**
  - Rule misconfigurations
  - Lack of rules
  - False positives/false negatives
  - Placement
- **Observability**
- **Domain Name System (DNS) security**
  - Domain Name System Security Extensions (DNSSEC)
  - DNS poisoning
  - Sinkholing
  - Zone transfers
- **Email security**
  - Domain Keys Identified Mail (DKIM)
  - Sender Policy Framework (SPF)
  - Domain-based Message Authentication Reporting & Conformance (DMARC)
  - Secure/Multipurpose Internet Mail Extension (S/MIME)
- **Transport Layer Security (TLS) errors**
- **Cipher mismatch**
- **PKI issues**
- **Issues with cryptographic**
- **implementations**
- **DoS/distributed denial of service (DDoS)**
- **Resource exhaustion**
- **Network access control list (ACL) issues**

3.4 Given a scenario, implement hardware security technologies and techniques.

- **Roots of trust**
  - Trusted Platform Module (TPM)
  - Hardware Security Module (HSM)
  - Virtual Trusted Platform Module (vTPM)
- **Security coprocessors**
  - Central processing unit (CPU) security extensions
  - Secure enclave
- **Virtual hardware**
- **Host-based encryption**
- **Self-encrypting drive (SED)**
- **Secure Boot**
- **Measured boot**
- **Self-healing hardware**
- **Tamper detection and countermeasures**
- **Threat-actor TTPs**
  - Firmware tampering
  - Shimming
  - Universal Serial Bus (USB)-based attacks
  - Basic input/output system/Unified Extensible Firmware Interface
  - (BIOS/UEFI)
  - Memory
  - Electromagnetic interference (EMI)
  - Electromagnetic pulse (EMP)

3.5 Given a set of requirements, secure specialized and legacy systems against threats.

- **Operational technology (OT)**
  - Supervisory control and data acquisition (SCADA)
  - Industrial control system (ICS)
  - Heating ventilation and air conditioning (HVAC)/environmental
- **Internet of Things (IoT)**
- **System-on-chip (SoC)**
- **Embedded systems**
- **Wireless technologies/ radio frequency (RF)**
- **Security and privacy considerations**
  - Segmentation
  - Monitoring
  - Aggregation
  - Hardening
  - Data analytics
  - Environmental
  - Regulatory
  - Safety
- **Industry-specific challenges**
  - Utilities
  - Transportation
  - Healthcare
  - Manufacturing
  - Financial
  - Government/defense
- **Characteristics of specialized/ legacy systems**
  - Unable to secure
  - Obsolete
  - Unsupported
  - Highly constrained

3.6 Given a scenario, use automation to secure the enterprise.

- Scripting
  - PowerShell
  - Bash
  - Python
- Cron/scheduled tasks
- Event-based triggers
- Infrastructure as code (IaC)
- Configuration files
  - Yet Another Markup Language (YAML)
  - Extensible Markup Language (XML)
  - JavaScript Object Notation (JSON)
  - Tom's Obvious, Minimal Language (TOML)
- Cloud APIs/software development kits (SDKs)
  - Web hooks
- Generative AI
  - Code assist
  - Documentation
- Containerization
- Automated patching
- Auto-containment
- Security orchestration, automation, and response (SOAR)
  - Runbooks
  - Playbooks
- Vulnerability scanning and reporting
- Security Content Automation Protocol (SCAP)
  - Open Vulnerability Assessment Language (OVAL)
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Common Platform Enumeration (CPE)
  - Common vulnerabilities and exposures (CVE)
  - Common Vulnerability Scoring System (CVSS)
- Workflow automation

3.7 Explain the importance of advanced cryptographic concepts.

- Post-quantum cryptography (PQC)
  - Post-quantum vs. Diffie-Hellman and elliptic curve cryptography (ECC)
  - Resistance to quantum computing decryption attack
  - Emerging implementations
- Key stretching
- Key splitting
- Homomorphic encryption
- Forward secrecy
- Hardware acceleration
- Envelope encryption
- Performance vs. security
- Secure multiparty computation
- Authenticated encryption with associated data (AEAD)
- Mutual authentication

3.8 Given a scenario, apply the appropriate cryptographic use case and/or technique.

- Use cases
  - Data at rest
  - Data in transit
    - Encrypted tunnels
  - Data in use/processing
  - Secure email
  - Immutable databases/blockchain
  - Non-repudiation
  - Privacy applications
  - Legal/regulatory considerations
  - Resource considerations
  - Data sanitization
  - Data anonymization
  - Certificate-based authentication
  - Passwordless authentication
  - Software provenance
  - Software/code integrity
  - Centralized vs. decentralized key management
- Techniques
  - Tokenization
  - Code signing
  - Cryptographic erase/obfuscation
  - Digital signatures
  - Obfuscation
  - Serialization
  - Hashing
  - One-time pad
  - Symmetric cryptography
  - Asymmetric cryptography
  - Lightweight cryptography