4.0 Security Operations

4.1 Given a scenario, apply common security techniques to computing resources.

- **Secure baselines**
  - Establish
  - Deploy
  - Maintain
- **Hardening targets**
  - Mobile devices
  - Workstations
  - Switches
  - Routers
  - Cloud infrastructure
  - Servers
  - ICS/SCADA
  - Embedded systems
  - RTOS
  - IoT devices
- **Wireless devices**
  - Installation considerations
    - Site surveys
    - Heat maps
- **Mobile solutions**
  - Mobile device management (MDM)
  - Deployment models
    - Bring your own device (BYOD)
    - Corporate-owned, personally enabled (COPE)
    - Choose your own device (CYOD)
  - Connection methods
    - Cellular
    - Wi-Fi
    - Bluetooth
- **Wireless security settings**
  - Wi-Fi Protected Access 3 (WPA3)
  - AAA/Remote Authentication Dial-In User Service (RADIUS)
  - Cryptographic protocols
  - Authentication protocols
- **Application security**
  - Input validation
  - Secure cookies
  - Static code analysis
  - Code signing
- **Sandboxing**
- **Monitoring**

4.2 Explain the security implications of proper hardware, software, and data asset management.

- **Acquisition/procurement process**
- **Assignment/accounting**
  - Ownership
  - Classification
- **Monitoring/asset tracking**
  - Inventory
  - Enumeration
- **Disposal/decommissioning**
  - Sanitization
  - Destruction
  - Certification
  - Data retention

4.3 Explain various activities associated with vulnerability management.

- **Identification methods**
  - Vulnerability scan
  - Application security
    - Static analysis
    - Dynamic analysis
    - Package monitoring
  - Threat feed
    - Open-source intelligence (OSINT)
    - Proprietary/third-party
    - Information-sharing organization
    - Dark web
  - Penetration testing
  - Responsible disclosure program
    - Bug bounty program
  - System/process audit
- **Analysis**
  - Confirmation
    - False positive
    - False negative
  - Prioritize
  - Common Vulnerability Scoring System (CVSS)
  - Common Vulnerability Enumeration (CVE)
  - Vulnerability classification
  - Exposure factor
  - Environmental variables
  - Industry/organizational impact
  - Risk tolerance
- **Vulnerability response and remediation**
  - Patching
  - Insurance
  - Segmentation
  - Compensating controls
  - Exceptions and exemptions
- **Validation of remediation**
  - Rescanning
  - Audit
  - Verification
- **Reporting**

4.4 Explain security alerting and monitoring concepts and tools.

- **Monitoring computing resources**
  - Systems
  - Applications
  - Infrastructure
- **Activities**
  - Log aggregation
  - Alerting
  - Scanning
  - Reporting
  - Archiving
  - Alert response and remediation/validation
    - Quarantine
    - Alert tuning
- **Tools**
  - Security Content Automation Protocol (SCAP)
  - Benchmarks
  - Agents/agentless
  - Security information and event management (SIEM)
  - Antivirus
  - Data loss prevention (DLP)
  - Simple Network Management Protocol (SNMP) traps
  - NetFlow
  - Vulnerability scanners

4.5 Given a scenario, modify enterprise capabilities to enhance security.

- **Firewall**
  - Rules
  - Access lists
  - Ports/protocols
  - Screened subnets
- **IDS/IPS**
  - Trends
  - Signatures
- **Web filter**
  - Agent-based
  - Centralized proxy
  - Universal Resource Locator (URL) scanning
  - Content categorization
  - Block rules
  - Reputation
- **Operating system security**
  - Group Policy
  - SELinux
- **Implementation of secure protocols**
  - Protocol selection
  - Port selection
  - Transport method
- **DNS filtering**
- **Email security**
  - Domain-based Message Authentication Reporting and Conformance (DMARC)
  - DomainKeys Identified Mail (DKIM)
  - Sender Policy Framework (SPF)
  - Gateway
- **File integrity monitoring**
- **DLP**
- **Network access control (NAC)**
- **Endpoint detection and response (EDR)/extended detection and response (XDR)**
- **User behavior analytics**

4.6 Given a scenario, implement and maintain identity and access management.

- **Provisioning/de-provisioning user accounts**
- **Permission assignments and implications**
- **Identity proofing**
- **Federation**
- **Single sign-on (SSO)**
  - Lightweight Directory Access Protocol (LDAP)
  - Open authorization (OAuth)
  - Security Assertions Markup Language (SAML)
- **Interoperability**
- **Attestation**
- **Access controls**
  - Mandatory
  - Discretionary
  - Role-based
  - Rule-based
  - Attribute-based
  - Time-of-day restrictions
  - Least privilege
- **Multifactor authentication**
  - Implementations
    - Biometrics
    - Hard/soft authentication tokens
    - Security keys
  - Factors
    - Something you know
    - Something you have
    - Something you are
    - Somewhere you are
- **Password concepts**
  - Password best practices
    - Length
    - Complexity
    - Reuse
    - Expiration
    - Age
  - Password managers
  - Passwordless
- **Privileged access management tools**
  - Just-in-time permissions
  - Password vaulting
  - Ephemeral credentials

4.7 Explain the importance of automation and orchestration related to secure operations.

- **Use cases of automation and scripting**
  - User provisioning
  - Resource provisioning
  - Guard rails
  - Security groups
  - Ticket creation
  - Escalation
  - Enabling/disabling services and access
  - Continuous integration and testing
  - Integrations and Application programming interfaces (APIs)
- **Benefits**
  - Efficiency/time saving
  - Enforcing baselines
  - Standard infrastructure configurations
  - Scaling in a secure manner
  - Employee retention
  - Reaction time
  - Workforce multiplier
- **Other considerations**
  - Complexity
  - Cost
  - Single point of failure
  - Technical debt
  - Ongoing supportability

4.8 Explain appropriate incident response activities.

- **Process**
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Eradication
  - Recovery
  - Lessons learned
- **Training**
- **Testing**
  - Tabletop exercise
  - Simulation
- **Root cause analysis**
- **Threat hunting**
- **Digital forensics**
  - Legal hold
  - Chain of custody
  - Acquisition
  - Reporting
  - Preservation
  - E-discovery

4.9 Given a scenario, use data sources to support an investigation.

- **Log data**
  - Firewall logs
  - Application logs
  - Endpoint logs
  - OS-specific security logs
  - IPS/IDS logs
  - Network logs
  - Metadata
- **Data sources**
  - Vulnerability scans
  - Automated reports
  - Dashboards
  - Packet captures