1.0 Enterprise Security

1.1 Given a scenario, select appropriate cryptographic concepts and techniques.

- **Techniques**
  - Key stretching
  - Hashing
  - Code signing
  - Pseudorandom number generation
  - Perfect forward secrecy
  - Transport encryption
  - Data-at-rest encryption
  - Digital signature
- **Concepts**
  - Entropy
  - Diffusion
  - Confusion
  - Non-repudiation
  - Confidentiality
  - Integrity
  - Chain of trust, root of trust
  - Cryptographic applications and proper/improper implementations
  - Advanced PKI concepts
    - Wild card
    - OCSP vs. CRL
    - Issuance to entities
    - Users
    - Systems
    - Applications
    - Key escrow
  - Steganography
  - Implications of cryptographic methods and design
    - Stream
    - Block
    - Modes
    - ECB
    - CBC
    - CFB
    - OFB
    - Known flaws/weaknesses
    - Strength vs. performance vs. feasibility to implement vs. interoperability
- **Implementations**
  - DRM
  - Watermarking
  - GPG
  - SSL
  - SSH
  - S/MIME

1.2 Explain the security implications associated with enterprise storage.

- **Storage types**
  - Virtual storage
  - Cloud storage
  - Data warehousing
  - Data archiving
  - NAS
  - SAN
  - vSAN
- **Storage protocols**
  - iSCSI
  - FCoE
  - NFS, CIFS
- **Secure storage management**
  - Multipath
  - Snapshots
  - Deduplication
  - Dynamic disk pools
  - LUN masking/mapping
  - HBA allocation
  - Offsite or multisite replication
  - Encryption
    - Disk
    - Block
    - File
    - Record
    - Port

CompTIA

1.3 Given a scenario, analyze network and security components, concepts and architectures.

- **Advanced network design (wired/wireless)**
  - Remote access
    - VPN
    - SSH
    - RDP
    - VNC
    - SSL
  - IPv6 and associated transitional technologies
  - Transport encryption
  - Network authentication methods
  - 802.1x
  - Mesh networks
- **Security devices**
  - UTM
  - NIPS
  - NIDS
  - INE
  - SIEM
  - HSM
  - Placement of devices
  - Application and protocol aware technologies
    - WAF
    - NextGen firewalls
    - IPS
    - Passive vulnerability scanners
    - DAM
- **Virtual networking and security components**
  - Switches
  - Firewalls
  - Wireless controllers
  - Routers
  - Proxies
- **Complex network security solutions for data flow**
  - SSL inspection
  - Network flow data
- **Secure configuration and baselining of networking and security components**
  - ACLs
  - Change monitoring
  - Configuration lockdown
  - Availability controls
- **Software-defined networking**
- **Cloud-managed networks**
- **Network management and monitoring tools**
- **Advanced configuration of routers, switches and other network devices**
  - Transport security
  - Trunking security
  - Route protection
- **Security zones**
  - Data flow enforcement
  - DMZ
  - Separation of critical assets
- **Network access control**
  - Quarantine/remediation
- **Operational and consumer network-enabled devices**
  - Building automation systems
  - IP video
  - HVAC controllers
  - Sensors
  - Physical access control systems
  - A/V systems
  - Scientific/industrial equipment
- **Critical infrastructure/Supervisory Control and Data Acquisition (SCADA)/ Industrial Control Systems (ICS)**

1.4 Given a scenario, select and troubleshoot security controls for hosts.

- **Trusted OS (e.g., how and when to use it)**
- **Endpoint security software**
  - Anti-malware
  - Antivirus
  - Anti-spyware
  - Spam filters
  - Patch management
  - HIPS/HIDS
  - Data loss prevention
  - Host-based firewalls
  - Log monitoring
- **Host hardening**
  - Standard operating environment/ configuration baselining
    - Application whitelisting and blacklisting
  - Security/group policy implementation
  - Command shell restrictions
  - Patch management
  - Configuring dedicated interfaces
    - Out-of-band NICs
    - ACLs
    - Management interface
    - Data interface
  - Peripheral restrictions
    - USB
    - Bluetooth
    - Firewire
  - Full disk encryption
- **Security advantages and disadvantages of virtualizing servers**
  - Type I
  - Type II
  - Container-based
- **Cloud augmented security services**
  - Hash matching
    - Antivirus
    - Anti-spam
    - Vulnerability scanning
  - Sandboxing
    - Content filtering
- **Boot loader protections**
  - Secure boot
  - Measured launch
  - Integrity Measurement Architecture (IMA)
  - BIOS/UEFI
- **Vulnerabilities associated with co-mingling of hosts with different security requirements**
  - VM escape
  - Privilege elevation
  - Live VM migration
  - Data remnants
- **Virtual Desktop Infrastructure (VDI)**
- **Terminal services/application delivery services**
- **TPM**
- **VTPM**
- **HSM**

1.5 Differentiate application vulnerabilities and select appropriate security controls.

- **Web application security design considerations**
  - Secure: by design, by default, by deployment
- **Specific application issues**
  - Cross-Site Request Forgery (CSRF)
  - Click-jacking
  - Session management
  - Input validation
  - SQL injection
  - Improper error and exception handling
  - Privilege escalation
  - Improper storage of sensitive data
  - Fuzzing/fault injection
  - Secure cookie storage and transmission
  - Buffer overflow
  - Memory leaks
  - Integer overflows
  - Race conditions
    - Time of check
    - Time of use
  - Resource exhaustion
  - Geo-tagging
  - Data remnants
- **Application sandboxing**
- **Application security frameworks**
  - Standard libraries
  - Industry-accepted approaches
  - Web services security (WS-security)
- **Secure coding standards**
- **Database Activity Monitor (DAM)**
- **Web Application Firewalls (WAF)**
- **Client-side processing vs. server-side processing**
  - JSON/REST
  - Browser extensions
    - ActiveX
    - Java Applets
    - Flash
  - HTML5
  - AJAX
  - SOAP
  - State management
  - JavaScript