2.0 Technologies and Tools

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- **Firewall**
  - ACL
  - Application-based vs. network-based
  - Stateful vs. stateless
  - Implicit deny
- **VPN concentrator**
  - Remote access vs. site-to-site
  - IPSec
    - Tunnel mode
    - Transport mode
    - AH
    - ESP
  - Split tunnel vs. full tunnel
  - TLS
  - Always-on VPN
- **NIPS/NIDS**
  - Signature-based
  - Heuristic/behavioral
  - Anomaly
  - Inline vs. passive
  - In-band vs. out-of-band
  - Rules
  - Analytics
    - False positive
    - False negative
- **Router**
  - ACLs
  - Antispoofing
- **Switch**
  - Port security
  - Layer 2 vs. Layer 3
  - Loop prevention
  - Flood guard
- **Proxy**
  - Forward and reverse proxy
  - Transparent
  - Application/multipurpose
- **Load balancer**
  - Scheduling
    - Affinity
    - Round-robin
  - Active-passive
  - Active-active
  - Virtual IPs
- **Access point**
  - SSID
  - MAC filtering
  - Signal strength
  - Band selection/width
  - Antenna types and placement
  - Fat vs. thin
  - Controller-based vs. standalone
- **SIEM**
  - Aggregation
  - Correlation
  - Automated alerting and triggers
  - Time synchronization
  - Event deduplication
  - Logs/WORM
- **DLP**
  - USB blocking
  - Cloud-based
  - Email
- **NAC**
  - Dissolvable vs. permanent
  - Host health checks
  - Agent vs. agentless
- **Mail gateway**
  - Spam filter
  - DLP
  - Encryption
- **Bridge**
- **SSL/TLS accelerators**
- **SSL decryptors**
- **Media gateway**
- **Hardware security module**

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- **Protocol analyzer**
- **Network scanners**
  - Rogue system detection
  - Network mapping
- **Wireless scanners/cracker**
- **Password cracker**
- **Vulnerability scanner**
- **Configuration compliance scanner**
- **Exploitation frameworks**
- **Data sanitization tools**
- **Steganography tools**
- **Honeypot**
- **Backup utilities**
- **Banner grabbing**
- **Passive vs. active**
- **Command line tools**
  - ping
  - netstat
  - tracert
  - nslookup/dig
  - arp
  - ipconfig/ip/ifconfig
  - tcpdump
  - nmap
  - netcat

CompTIA.

2.3 Given a scenario, troubleshoot common security issues.

- **Unencrypted credentials/clear text**
- **Logs and events anomalies**
- **Permission issues**
- **Access violations**
- **Certificate issues**
- **Data exfiltration**
- **Misconfigured devices**
  - Firewall
  - Content filter
  - Access points
- **Weak security configurations**
- **Personnel issues**
  - Policy violation
  - Insider threat
  - Social engineering
  - Social media
  - Personal email
- **Unauthorized software**
- **Baseline deviation**
- **License compliance violation (availability/integrity)**
- **Asset management**
- **Authentication issues**

2.4 Given a scenario, analyze and interpret output from security technologies.

- **HIDS/HIPS**
- **Antivirus**
- **File integrity check**
- **Host-based firewall**
- **Application whitelisting**
- **Removable media control**
- **Advanced malware tools**
- **Patch management tools**
- **UTM**
- **DLP**
- **Data execution prevention**
- **Web application firewall**

2.5 Given a scenario, deploy mobile devices securely.

- **Connection methods**
  - Cellular
  - WiFi
  - SATCOM
  - Bluetooth
  - NFC
  - ANT
  - Infrared
  - USB
- **Mobile device management concepts**
  - Application management
  - Content management
  - Remote wipe
  - Geofencing
  - Geolocation
  - Screen locks
  - Push notification services
  - Passwords and pins
  - Biometrics
  - Context-aware authentication
  - Containerization
  - Storage segmentation
  - Full device encryption
- **Enforcement and monitoring for:**
  - Third-party app stores
  - Rooting/jailbreaking
  - Sideloading
  - Custom firmware
  - Carrier unlocking
  - Firmware OTA updates
  - Camera use
  - SMS/MMS
  - External media
  - USB OTG
  - Recording microphone
  - GPS tagging
  - WiFi direct/ad hoc
  - Tethering
  - Payment methods
- **Deployment models**
  - BYOD
  - COPE
  - CYOD
  - Corporate-owned
  - VDI

2.6 Given a scenario, implement secure protocols.

- **Protocols**
  - DNSSEC
  - SSH
  - S/MIME
  - SRTP
  - LDAPS
  - FTPS
  - SFTP
  - SNMPv3
  - SSL/TLS
  - HTTPS
  - Secure POP/IMAP
- **Use cases**
  - Voice and video
  - Time synchronization
  - Email and web
  - File transfer
  - Directory services
  - Remote access
  - Domain name resolution
  - Routing and switching
  - Network address allocation
  - Subscription services