2.0 Security

2.1 Summarize various security measures and their purposes.

- **Physical security**
  - Access control vestibule
  - Badge reader
  - Video surveillance
  - Alarm systems
  - Motion sensors
  - Door locks
  - Equipment locks
  - Guards
  - Bollards
  - Fences
- **Physical security for staff**
  - Key fobs
  - Smart cards
  - Keys
  - Biometrics
    - Retina scanner
    - Fingerprint scanner
    - Palmprint scanner
  - Lighting
  - Magnetometers
- **Logical security**
  - Principle of least privilege
  - Access control lists (ACLs)
  - Multifactor authentication (MFA)
  - Email
  - Hard token
  - Soft token
  - Short message service (SMS)
  - Voice call
  - Authenticator application
- **Mobile device management (MDM)**
- **Active Directory**
  - Login script
  - Domain
  - Group Policy/updates
  - Organizational units
  - Home folder
  - Folder redirection
  - Security groups

2.2 Compare and contrast wireless security protocols and authentication methods.

- **Protocols and encryption**
  - WiFi Protected Access 2 (WPA2)
  - WPA3
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- **Authentication**
  - Remote Authentication Dial-In User Service (RADIUS)
  - Terminal Access Controller Access-Control System (TACACS+)
  - Kerberos
  - Multifactor

CompTIA.

2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.

- **Malware**
  - Trojan
  - Rootkit
  - Virus
  - Spyware
  - Ransomware
  - Keylogger
  - Boot sector virus
  - Cryptominers

- **Tools and methods**
  - Recovery mode
  - Antivirus
  - Anti-malware
  - Software firewalls
  - Anti-phishing training
  - User education regarding common threats
  - OS reinstallation

2.4 Explain common social-engineering attacks, threats, and vulnerabilities.

- **Social engineering**
  - Phishing
  - Vishing
  - Shoulder surfing
  - Whaling
  - Tailgating
  - Impersonation
  - Dumpster diving
  - Evil twin

- **Threats**
  - Distributed denial of service (DDoS)
  - Denial of service (DoS)
  - Zero-day attack
  - Spoofing
  - On-path attack
  - Brute-force attack
  - Dictionary attack
  - Insider threat
  - Structured Query Language (SQL) injection
  - Cross-site scripting (XSS)

- **Vulnerabilities**
  - Non-compliant systems
  - Unpatched systems
  - Unprotected systems (missing antivirus/missing firewall)
  - EOL OSs
  - Bring your own device (BYOD)

2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

- **Defender Antivirus**
  - Activate/deactivate
  - Updated definitions
- **Firewall**
  - Activate/deactivate
  - Port security
  - Application security
- **Users and groups**
  - Local vs. Microsoft account
  - Standard account
  - Administrator
  - Guest user
  - Power user
- **Login OS options**
  - Username and password
  - Personal identification number (PIN)
  - Fingerprint
  - Facial recognition
  - Single sign-on (SSO)
- **NTFS vs. share permissions**
  - File and folder attributes
  - Inheritance
- **Run as administrator vs. standard user**
  - User Account Control (UAC)
- **BitLocker**
- **BitLocker To Go**
- **Encrypting File System (EFS)**

2.6 Given a scenario, configure a workstation to meet best practices for security.

- **Data-at-rest encryption**
- **Password best practices**
  - Complexity requirements
    - Length
    - Character types
  - Expiration requirements
  - Basic input/output system (BIOS)/ Unified Extensible Firmware Interface (UEFI) passwords
- **End-user best practices**
  - Use screensaver locks
  - Log off when not in use
  - Secure/protect critical hardware (e.g., laptops)
  - Secure personally identifiable information (PII) and passwords
- **Account management**
  - Restrict user permissions
  - Restrict login times
  - Disable guest account
  - Use failed attempts lockout
  - Use timeout/screen lock
- **Change default administrator's user account/password**
- **Disable AutoRun**
- **Disable AutoPlay**

2.7 Explain common methods for securing mobile and embedded devices.

- **Screen locks**
  - Facial recognition
  - PIN codes
  - Fingerprint
  - Pattern
  - Swipe
- **Remote wipes**
- **Locator applications**
- **OS updates**
- **Device encryption**
- **Remote backup applications**
- **Failed login attempts restrictions**
- **Antivirus/anti-malware**
- **Firewalls**
- **Policies and procedures**
  - BYOD vs. corporate owned
  - Profile security requirements
- **Internet of Things (IoT)**

2.8 Given a scenario, use common data destruction and disposal methods.

- **Physical destruction**
  - Drilling
  - Shredding
  - Degaussing
  - Incinerating

- **Recycling or repurposing best practices**
  - Erasing/wiping
  - Low-level formatting
  - Standard formatting

- **Outsourcing concepts**
  - Third-party vendor
  - Certification of destruction/ recycling

2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

- **Home router settings**
  - Change default passwords
  - IP filtering
  - Firmware updates
  - Content filtering
  - Physical placement/secure locations
  - Dynamic Host Configuration Protocol (DHCP) reservations
  - Static wide-area network (WAN) IP
  - Universal Plug and Play (UPnP)
  - Screened subnet

- **Wireless specific**
  - Changing the service set identifier (SSID)
  - Disabling SSID broadcast
  - Encryption settings
  - Disabling guest access
  - Changing channels

- **Firewall settings**
  - Disabling unused ports
  - Port forwarding/mapping

2.10 Given a scenario, install and configure browsers and relevant security settings.

- **Browser download/installation**
  - Trusted sources
    - Hashing
  - Untrusted sources
- **Extensions and plug-ins**
  - Trusted sources
  - Untrusted sources

- **Password managers**
- **Secure connections/sites – valid certificates**

- **Settings**
  - Pop-up blocker
  - Clearing browsing data
  - Clearing cache
  - Private-browsing mode
  - Sign-in/browser data synchronization
  - Ad blockers

CompTIA.