2.0 Threats, Vulnerabilities, and Mitigations

2.1 Compare and contrast common threat actors and motivations.

- **Threat actors**
  - Nation-state
  - Unskilled attacker
  - Hacktivist
  - Insider threat
  - Organized crime
  - Shadow IT
- **Attributes of actors**
  - Internal/external
  - Resources/funding
  - Level of sophistication/capability
- **Motivations**
  - Data exfiltration
  - Espionage
  - Service disruption
  - Blackmail
  - Financial gain
  - Philosophical/political beliefs
  - Ethical
  - Revenge
  - Disruption/chaos
  - War

2.2 Explain common threat vectors and attack surfaces.

- **Message-based**
  - o Email
  - o Short Message Service (SMS)
  - o Instant messaging (IM)
- **Image-based**
- **File-based**
- **Voice call**
- **Removable device**
- **Vulnerable software**
  - o Client-based vs. agentless
- **Unsupported systems and applications**
- **Unsecure networks**
  - Wireless
  - Wired
  - Bluetooth
- **Open service ports**
- **Default credentials**
- **Supply chain**
  - Managed service providers (MSPs)
  - Vendors
  - Suppliers
- **Human vectors/social engineering**
  - Phishing
  - Vishing
  - Smishing
  - Misinformation/disinformation
  - Impersonation
  - Business email compromise
  - Pretexting
  - Watering hole
  - Brand impersonation
  - Typosquatting

2.3 Explain various types of vulnerabilities.

- **Application**
  - Memory injection
  - Buffer overflow
  - Race conditions
    - Time-of-check (TOC)
    - Time-of-use (TOU)
  - Malicious update
- **Operating system (OS)-based**
- **Web-based**
  - Structured Query Language injection (SQLi)
  - Cross-site scripting (XSS)
- **Hardware**
  - Firmware
  - End-of-life
  - Legacy
- **Virtualization**
  - Virtual machine (VM) escape
  - Resource reuse
- **Cloud-specific**
- **Supply chain**
  - Service provider
  - Hardware provider
  - Software provider
- **Cryptographic**
- **Misconfiguration**
- **Mobile device**
  - Side loading
  - Jailbreaking
- **Zero-day**

2.4 Given a scenario, analyze indicators of malicious activity.

- **Malware attacks**
  - Ransomware
  - Trojan
  - Worm
  - Spyware
  - Bloatware
  - Virus
  - Keylogger
  - Logic bomb
  - Rootkit
- **Physical attacks**
  - Brute force
  - Radio frequency identification (RFID) cloning
  - Environmental
- **Network attacks**
  - Distributed denial-of-service (DDoS)
    - Amplified
    - Reflected
  - Domain Name System (DNS) attacks
  - Wireless
  - On-path
  - Credential replay
  - Malicious code
- **Application attacks**
  - Injection
  - Buffer overflow
  - Replay
  - Privilege escalation
  - Forgery
  - Directory traversal
- **Cryptographic attacks**
  - Downgrade
  - Collision
  - Birthday
- **Password attacks**
  - Spraying
  - Brute force
- **Indicators**
  - Account lockout
  - Concurrent session usage
  - Blocked content
  - Impossible travel
  - Resource consumption
  - Resource inaccessibility
  - Out-of-cycle logging
  - Published/documented
  - Missing logs

2.5 Explain the purpose of mitigation techniques used to secure the enterprise.

- **Segmentation**
- **Access control**
  - Access control list (ACL)
  - Permissions
- **Application allow list**
- **Isolation**
- **Patching**
- **Encryption**
- **Monitoring**
- **Least privilege**
- **Configuration enforcement**
- **Decommissioning**
- **Hardening techniques**
  - Encryption
  - Installation of endpoint protection
  - Host-based firewall
  - Host-based intrusion prevention system (HIPS)
  - Disabling ports/protocols
  - Default password changes
  - Removal of unnecessary software