1.0 Threats, Attacks and Vulnerabilities

1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.

- **Viruses**
- **Crypto-malware**
- **Ransomware**
- **Worm**
- **Trojan**
- **Rootkit**
- **Keylogger**
- **Adware**
- **Spyware**
- **Bots**
- **RAT**
- **Logic bomb**
- **Backdoor**

1.2 Compare and contrast types of attacks.

- **Social engineering**
  - Phishing
  - Spear phishing
  - Whaling
  - Vishing
  - Tailgating
  - Impersonation
  - Dumpster diving
  - Shoulder surfing
  - Hoax
  - Watering hole attack
  - Principles (reasons for effectiveness)
    - Authority
    - Intimidation
    - Consensus
    - Scarcity
    - Familiarity
    - Trust
    - Urgency
- **Application/service attacks**
  - DoS
  - DDoS
  - Man-in-the-middle
  - Buffer overflow
  - Injection
  - Cross-site scripting
  - Cross-site request forgery
  - Privilege escalation
  - ARP poisoning
  - Amplification
  - DNS poisoning
  - Domain hijacking
  - Man-in-the-browser
  - Zero day
  - Replay
  - Pass the hash
  - Hijacking and related attacks
    - Clickjacking
    - Session hijacking
    - URL hijacking
    - Typo squatting
  - Driver manipulation
    - Shimming
    - Refactoring
  - MAC spoofing
  - IP spoofing
- **Wireless attacks**
  - Replay
  - IV
  - Evil twin
  - Rogue AP
  - Jamming
  - WPS
  - Bluejacking
  - Bluesnarfing
  - RFID
  - NFC
  - Disassociation
- **Cryptographic attacks**
  - Birthday
  - Known plain text/cipher text
  - Rainbow tables
  - Dictionary
  - Brute force
    - Online vs. offline
  - Collision
  - Downgrade
  - Replay
  - Weak implementations

1.3 Explain threat actor types and attributes.

- **Types of actors**
  - Script kiddies
  - Hacktivist
  - Organized crime
  - Nation states/APT
  - Insiders
  - Competitors
- **Attributes of actors**
  - Internal/external
  - Level of sophistication
  - Resources/funding
  - Intent/motivation
- **Use of open-source intelligence**

1.4 Explain penetration testing concepts.

- **Active reconnaissance**
- **Passive reconnaissance**
- **Pivot**
- **Initial exploitation**
- **Persistence**
- **Escalation of privilege**
- **Black box**
- **White box**
- **Gray box**
- **Penetration testing vs. vulnerability scanning**

1.5 Explain vulnerability scanning concepts.

- **Passively test security controls**
- **Identify vulnerability**
- **Identify lack of security controls**
- **Identify common misconfigurations**
- **Intrusive vs. non-intrusive**
- **Credentialed vs. non-credentialed**
- **False positive**

1.5 Explain the impact associated with types of vulnerabilities.

- **Race conditions**
- **Vulnerabilities due to:**
  - End-of-life systems
  - Embedded systems
  - Lack of vendor support
- **Improper input handling**
- **Improper error handling**
- **Misconfiguration/weak configuration**
- **Default configuration**
- **Resource exhaustion**
- **Untrained users**
- **Improperly configured accounts**
- **Vulnerable business processes**
- **Weak cipher suites and implementations**
- **Memory/buffer vulnerability**
  - Memory leak
  - Integer overflow
  - Buffer overflow
  - Pointer dereference
  - DLL injection
- **System sprawl/undocumented assets**
- **Architecture/design weaknesses**
- **New threats/zero day**
- **Improper certificate and key management**