1.0 Threats, Attacks, and Vulnerabilities

1.1 Compare and contrast different types of social engineering techniques.

- **Phishing**
- **Smishing**
- **Vishing**
- **Spam**
- **Spam over instant messaging (SPIM)**
- **Spear phishing**
- **Dumpster diving**
- **Shoulder surfing**
- **Pharming**
- **Tailgating**
- **Eliciting information**
- **Whaling**
- **Prepending**
- **Identity fraud**
- **Invoice scams**
- **Credential harvesting**
- **Reconnaissance**
- **Hoax**
- **Impersonation**
- **Watering hole attack**
- **Typosquatting**
- **Pretexting**
- **Influence campaigns**
  - Hybrid warfare
  - Social media
- **Principles (reasons for effectiveness)**
  - Authority
  - Intimidation
  - Consensus
  - Scarcity
  - Familiarity
  - Trust
  - Urgency

1.2 Given a scenario, analyze potential indicators to determine the type of attack.

- **Malware**
  - Ransomware
  - Trojans
  - Worms
  - Potentially unwanted programs (PUPs)
  - Fileless virus
  - Command and control
  - Bots
  - Cryptomalware
  - Logic bombs
  - Spyware
  - Keyloggers
  - Remote access Trojan (RAT)
  - Rootkit
  - Backdoor
- **Password attacks**
  - Spraying
  - Dictionary
  - Brute force
    - Offline
    - Online
  - Rainbow table
  - Plaintext/unencrypted
- **Physical attacks**
  - Malicious Universal Serial Bus (USB) cable
  - Malicious flash drive
  - Card cloning
  - Skimming
- **Adversarial artificial intelligence (AI)**
  - Tainted training data for machine learning (ML)
  - Security of machine learning algorithms
- **Supply-chain attacks**
- **Cloud-based vs. on-premises attacks**
- **Cryptographic attacks**
  - Birthday
  - Collision
  - Downgrade

1.3 Given a scenario, analyze potential indicators associated with application attacks.

- **Privilege escalation**
- **Cross-site scripting**
- **Injections**
  - Structured query language (SQL)
  - Dynamic-link library (DLL)
  - Lightweight Directory Access Protocol (LDAP)
  - Extensible Markup Language (XML)
- **Pointer/object dereference**
- **Directory traversal**
- **Buffer overflows**
- **Race conditions**
  - Time of check/time of use
- **Error handling**
- **Improper input handling**
- **Replay attack**
  - Session replays
- **Integer overflow**
- **Request forgeries**
  - Server-side
  - Cross-site
- **Application programming interface (API) attacks**
- **Resource exhaustion**
- **Memory leak**
- **Secure Sockets Layer (SSL) stripping**
- **Driver manipulation**
  - Shimming
  - Refactoring
- **Pass the hash**

1.4 Given a scenario, analyze potential indicators associated with network attacks.

- **Wireless**
  - Evil twin
  - Rogue access point
  - Bluesnarfing
  - Bluejacking
  - Disassociation
  - Jamming
  - Radio frequency identification (RFID)
  - Near-field communication (NFC)
  - Initialization vector (IV)
- **On-path attack (previously known as man-in-the-middle attack/ man-in-the-browser attack)**
- **Layer 2 attacks**
  - Address Resolution Protocol (ARP) poisoning
  - Media access control (MAC) flooding
  - MAC cloning
- **Domain name system (DNS)**
  - Domain hijacking
  - DNS poisoning
  - Uniform Resource Locator (URL) redirection
  - Domain reputation
- **Distributed denial-of-service (DDoS)**
  - Network
  - Application
  - Operational technology (OT)
- **Malicious code or script execution**
  - PowerShell
  - Python
  - Bash
  - Macros
  - Visual Basic for Applications (VBA)

1.5 Explain different threat actors, vectors, and intelligence sources.

- **Actors and threats**
  - Advanced persistent threat (APT)
  - Insider threats
  - State actors
  - Hacktivists
  - Script kiddies
  - Criminal syndicates
  - Hackers
    - Authorized
    - Unauthorized
    - Semi-authorized
  - Shadow IT
  - Competitors
- **Attributes of actors**
  - Internal/external
  - Level of sophistication/capability
  - Resources/funding
  - Intent/motivation
- **Vectors**
  - Direct access
  - Wireless
  - Email
  - Supply chain
  - Social media
  - Removable media
  - Cloud
- **Threat intelligence sources**
  - Open-source intelligence (OSINT)
  - Closed/proprietary
  - Vulnerability databases
  - Public/private information-sharing centers
  - Dark web
  - Indicators of compromise
  - Automated Indicator Sharing (AIS)
    - Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)
  - Predictive analysis
  - Threat maps
  - File/code repositories
- **Research sources**
  - Vendor websites
  - Vulnerability feeds
  - Conferences
  - Academic journals
  - Request for comments (RFC)
  - Local industry groups
  - Social media
  - Threat feeds
  - Adversary tactics, techniques, and procedures (TTP)

1.6 Explain the security concerns associated with various types of vulnerabilities.

- **Cloud-based vs. on-premises vulnerabilities**
- **Zero-day**
- **Weak configurations**
  - Open permissions
  - Unsecure root accounts
  - Errors
  - Weak encryption
  - Unsecure protocols
  - Default settings
  - Open ports and services
- **Third-party risks**
  - Vendor management
    - System integration
    - Lack of vendor support
  - Supply chain
  - Outsourced code development
  - Data storage
- **Improper or weak patch management**
  - Firmware
  - Operating system (OS)
  - Applications
- **Legacy platforms**
- **Impacts**
  - Data loss
  - Data breaches
  - Data exfiltration
  - Identity theft
  - Financial
  - Reputation
  - Availability loss

1.7 Summarize the techniques used in security assessments.

- **Threat hunting**
  - Intelligence fusion
  - Threat feeds
  - Advisories and bulletins
  - Maneuver
- **Vulnerability scans**
  - False positives
  - False negatives
  - Log reviews
  - Credentialed vs. non-credentialed
  - Intrusive vs. non-intrusive
  - Application
  - Web application
  - Network
  - Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS)
  - Configuration review
- **Syslog/Security information and event management (SIEM)**
  - Review reports
  - Packet capture
  - Data inputs
  - User behavior analysis
  - Sentiment analysis
  - Security monitoring
  - Log aggregation
  - Log collectors
- **Security orchestration, automation, and response (SOAR)**

1.8 Explain the techniques used in penetration testing.

- **Penetration testing**
  - Known environment
  - Unknown environment
  - Partially known environment
  - Rules of engagement
  - Lateral movement
  - Privilege escalation
  - Persistence
  - Cleanup
  - Bug bounty
  - Pivoting
- **Passive and active reconnaissance**
  - Drones
  - War flying
  - War driving
  - Footprinting
  - OSINT
- **Exercise types**
  - Red-team
  - Blue-team
  - White-team
  - Purple-team