Threats, Vulnerabilities, and Mitigations

Compare and contrast common threat actors and motivations

- **Threat actors**
  - **Nation-state**
    - Attributes:
      - External entities, often government-sponsored, with substantial resources and advanced capabilities
    - Motivations:
      - Engage in espionage to gather intelligence, disrupt services of rival nations, exfiltrate sensitive data, and can prepare for cyber warfare
  - **Unskilled attacker (scriptkiddy)**
    - Attributes:
      - Typically external individuals with limited technical knowledge, relying on pre-made scripts or tools.
    - Motivations:
      - Seek thrill or recognition by disrupting services, defacing websites, or causing chaos without a specific agenda
  - **Hacktivist**
    - Attributes:
      - External actors driven by ideological beliefs, possessing varying levels of technical expertise.
    - Motivations:
      - Promote political or social causes by defacing websites, leaking information, or disruption services do draw attention to their message
  - **Insider threat**
    - Attributes:
      - Individuals within an organization, such as employees or contractors, who have authorized access.
    - Motivations:
      - May act out of financial gain, revenge, or coercion, leading to data exfiltration, sabotage, unauthorized information disclosure.
  - **Organized crime**
    - Attributes:
      - External networks resembling corporate structures, equipped with significant resources and specialized skills
    - Motivations:
      - Primarily driven by financial gain through activities like ransomware attacks, data theft for sale, and financial fraud.
  - **Shadow IT**
    - Attributes:
      - Internal groups or individuals deploying unauthorized systems or applications without IT department approval
    - Motivation:
      - Often aim to enhance productivity or bypass perceived IT constraints, inadvertently introducing security vulnerabilities due to lack of oversight.

Explain common threat vectors and attack surfaces

- **Message-based**
  - **Email**
    - Attackers often use phishing emails containing malicious links or attachments to deceive recipients into revealing sensitive information or installing malware.
  - **Short Message Service (SMS)**
    - Known as **smishing**, this involves sending fraudulent SMS messages to trick individuals into disclosing personal data or clicking on harmful links.
  - **Instant Messaging (IM)**
    - Threats via IM platforms can include malicious links, file transfers containing malware, or social engineering tactics to extract information.

- **Image-based**
  - Techniques like steganography hide malicious code within images, which, when opened, can execute harmful scripts on the user's device.

- **File-based**
  - Files such as PDFs, Word documents, or spreadsheets can be embedded with malicious macros or exploits that activate upon opening.

- **Voice Call**
  - Referred as **vishing**, attackers impersonate legitimate entities over the phone to extract confidential information from victims.

- **Removable Devices**
  - USB drives and other removable media can carry malware, which automatically executes when connected to a system, leading to potential data breaches or system compromises.

- **Vulnerable software**
  - **Client-based**
    - Applications installed on user devices can have vulnerabilities that attackers exploit, especially if not regularly updated.
  - **Agentless**
    - Systems without security agents can be more susceptible to attacks due to the lack of monitoring and protection.

- **Unsupported Systems and Applications**
  - Using outdated software that no longer receives security updates exposes systems to known vulnerabilities that attackers can easily exploit

- **Unsecure Networks**
  - **Wireless**
    - Unsecured Wi-Fi networks can be intercepted by attackers, leading to data theft or unauthorized access.
  - **Wired**
    - Physical access to network cables can allow attackers to tap into communications.
  - **Bluetooth**
    - Vulnerabilities in bluetooth can be exploited for unauthorized data access or device control.

- **Open Service Ports**
    - Unnecessary open ports can serve as entry points for attackers to access or compromise a system.

- **Default Credentials**
    - Default usernames and passwords must be changed to prevent attackers from easily gaining access.

- **Supply Chain**
    - **Manage Service Providers (MSPs), Vendors, Suppliers**
        - Third-party partners with access to systems can introduce vulnerabilities, either unintentionally or through target attacks, affecting the primary organization's security.

- **Human Vectors/Social Engineering**
    - **Phishing**
        - Deceptive emails designed to trick recipients into revealing information or installing malware.
    - **Vishing**
        - Voice phishing attacks conducted over the phone.
    - **Smishing**
        - SMS-based phishing attempts.
    - **Misinformation/Disinformation**
        - Spreading false information to manipulate or deceive users.
    - **Impersonation**
        - Attackers pose as trusted individuals to gain access or information.
    - **Business Email Compromise (BEC)**
        - Fraudulent emails appear to come from legitimate business sources to trick recipients into taking harmful actions.
    - **Pretexting**
        - Creating a fabricated scenario to persuade someone to divulge information.
    - **Watering Hole**
        - Compromising a website frequented by a target group to distribute malware.
    - **Brand Impersonation**
        - Mimicking a trusted brand to deceive users.
    - **Typosquatting**
        - Registering misspelled domain names of popular sites to trick users into visiting malicious websites.

Explain various types of vulnerabilities

- **Application Vulnerabilities**
    - **Memory Injection**
        - Occurs when an attacker inserts malicious code into a program's memory space, potentially leading to unauthorized actions or data breaches.
    - **Buffer Overflow**
        - Happens when a program writes more data to a buffer than it can hold, causing data to overflow into adjacent memory. This can lead to system crashes or provide a pathway for code execution by attackers

    - **Race Conditions**
        - These arise when the system’s behavior depends on the sequence or timing of uncontrollable events.
        - **Time-of-Check (TOC)**
            - A vulnerability that occurs between the checking of a condition and the use of the result of that check.
        - **Time-of-Use (TOU)**
            - Similar to TOC, but focuses on the time between the decision to perform an action and the actual performance of that action.
    - **Malicious Update**
        - Involves attackers distributing updates that contain malicious code, compromising the application upon installation.

- **Operating System (OS)-Based Vulnerabilities**
    - These vulnerabilities are inherent weaknesses within an operating system that can be exploited to gain unauthorized access or control. They often arise from unpatched software, misconfigurations, or inherent design flaws.

- **Web-Based Vulnerabilities**
    - **Structured Query Language Injection (SQLi)**
        - An attack where malicious SQL statements are inserted into an entry field, allowing attackers to manipulate databases and access unauthorized information.
    - **Cross-Site Scripting (XXS)**
        - Occurs when attackers inject malicious scripts into content that is then delivered to users, potentially leading to data theft or session hijacking.

- **Hardware Vulnerabilities**
    - **Firmware**
        - Flaws in the low-level software that controls hardware can be exploited to gain deep system access.
    - **End-of-Life**
        - Hardware that is no longer supported with security updates becomes vulnerable to exploitation.
    - **Legacy Systems**
        - Older hardware may lack modern security features, making them susceptible to attacks.

- **Virtualization Vulnerabilities**
    - **Virtual Machine (VM) Escape**
        - An exploit where an attacker escapes from the isolated environment of a VM to access the host system or other VMs.
    - **Resource Reuse:**
        - Improper management of resources can lead to data from one VM being accessible to another, violating isolation principles.

- **Cloud-Specific Vulnerabilities**
    - These include issues like API, misconfigured storage services, and inadequate access controls, which can lead to data breaches or unauthorized access in cloud environment

- **Supply Chain Vulnerabilities**
  - **Service Provider**
    - Weakness in third-party services can be exploited to compromise the primary organization
  - **Hardware Provider**
    - Malicious components or flaws in hardware from suppliers can introduce vulnerabilities
  - **Software Provider**
    - Insecure software from vendors can serve as an entry point for attackers.

- **Cryptographic Vulnerabilities**
  - Weaknesses in cryptographic algorithms or improper implementation can lead to data being decrypted or tampered with by unauthorized parties.

- **Misconfiguration Vulnerabilities**
  - Improperly configured systems, such as default settings, unnecessary services enabled, or weak permissions, can open avenues for exploitation.

- **Mobile Device Vulnerabilities**
  - **Side Loading**
    - Installing apps from unofficial sources can introduce malicious software.
  - **Jailbreaking**
    - Removing manufacturer restrictions can expose the device to security risks by allowing unauthorized apps and services.

- **Zero-Day Vulnerabilities**
  - These are unknown vulnerabilities that attackers exploit before developers become aware and issue patches, making them particularly dangerous.

Given a scenario, analyze indicators of malicious activity

- **Malware Attacks**
  - **Ransomware**
    - Files become encrypted with demands for payment to decrypt
  - **Trojan**
    - Legitimate-looking applications that, once executed, perform malicious activities
  - **Worm**
    - Rapid replication across networks, leading to increased network traffic and system slowdowns.
  - **Spyware**
    - Unauthorized data collection, leading to information leaks.
  - **Bloatware**
    - Wanted pre-installed applications consuming system resources
  - **Virus**
    - Unexpected system behavior, frequent crashes, and data corruption
  - **Keylogger**
    - Unauthorized logging of keystrokes, potentially leading to credential theft
  - **Logic Bomb**
    - Delayed malicious actions triggered by specific conditions
  - **Rootkit**
    - Deep system infiltration, often hiding other malware and evading detection

- **Physical Attacks**
    - **Brute Force**
        - Repeated failed access attempts, potentially leading to account lockouts
    - **RFID Cloning**
        - Unauthorized duplication of RFID-enabled access devices
    - **Environmental**
        - Unexplained system shutdowns or hardware failures due to environmental tampering

- **Network Attacks**
    - **Distributed Denial-of-Service (DDoS):**
        - Overwhelming network traffic causing service disruptions
        - **Amplified**
            - Small requests resulting in large responses to flood targets
        - **Reflected**
            - Spoofed requests causing response to be send to the target
    - **Domain Name System (DNS) Attacks**
        - Redirection to malicious sites or DNS service disruptions
    - **Wireless**
        - Unauthorized access point or interception of wireless communications
    - **On-Path (Man-in-the-Middle)**
        - Interception and potential alteration of communication between parties
    - **Credential Replay**
        - Unauthorized use of captured credentials to gain access
    - **Malicious Code**
        - Injection of harmful scripts or code into applications or websites

- **Application Attacks**
    - **Injection**
        - Insertion of malicious code into applications, leading to unauthorized actions
    - **Buffer Overflow**
        - Exploiting memory management flaws to execute arbitrary code
    - **Replay**
        - Capturing and reusing valid data transmissions to impersonate users.
    - **Privilege Escalation**
        - Gaining higher access levels than permitted
    - **Forgery**
        - Creation of counterfeit requests or data to deceive systems
    - **Directory Transversal**
        - Accessing restricted directories and files outside the web root

- **Cryptographic Attacks**
    - **Downgrade**
        - Forcing systems to use weaker encryptions methods
    - **Collision**
        - Finding two different inputs that produce the same hash value
    - **Birthday**
        - Exploiting the mathematics behind hash functions to find collisions

- **Password Attacks**
    - **Spraying**
        - Attempting common passwords across many accounts to avoid detection
    - **Brute Force**
        - Systematic trail of all possible passwords until the correct one is found

- **Common Indicator of Malicious Activity**
    - **Account lockout**
        - Multiple failed login attempts leading to account suspension
    - **Current Session Usage**
        - Same account accessed simultaneously within a short time frame
    - **Resource Consumption**
        - Unexplained spikes in CPU, memory, or network usage
    - **Resource Inaccessibility**
        - Inability to access files or services
    - **Out-of-Cycle Logging**
        - Unexpected log entries outside normal operational hours
    - **Published/Documented**
        - Public disclosure of vulnerabilities or exploits affecting the system
    - **Missing Logs**
        - Absence of expected log entries, possibly indicating tampering

Explain the purpose of mitigation techniques used to secure the enterprise

- **Segmentation**
    - Dividing a network into smaller, isolated segments limits the spread of potential breaches and restricts unauthorized access to sensitive data. This approach enhances security by containing threats within specific areas.

- **Access Control**
    - **Access Control List (ACL)**
        - Defines permissions for users or system processes, specifying who can access specific resources and the actions they can perform
    - **Permissions**
        - Assigning appropriate access rights ensures users can only interact with data and systems necessary for their roles, reducing the risk of unauthorized activities

- **Application Allow List**
    - Permitting only pre-approved applications to run on systems prevents the execution of unauthorized or malicious software, thereby reducing the attack surface

- **Isolation**
    - Separating critical systems or applications from the main network minimizes exposure to threats and limits potential damage from compromised components

- **Patching**
    - Regularly updating software and systems addresses known vulnerabilities, preventing attackers from exploiting outdated components

- **Encryption**
  - Encoding data in transit and at rest ensures that even if intercepted or accessed without authorization, the information remains unreadable and secure

- **Monitoring**
  - Continuous observation of network activities and system behavior enables the early detection of anomalies or unauthorized actions, facilitating prompt incident response

- **Least Privilege**
  - Granting users minimum level of access necessary for their tasks reduces the potential impact of accidental or malicious activities

- **Configuration Enforcement**
  - Implementing standardized security configurations across systems ensures consistency and reduces the likelihood of misconfigurations that could be exploited

- **Decommissioning**
  - Properly retiring outdated or unused systems includes securely removing data and disconnecting them from networks to prevent unauthorized access through obsolete assets

- **Hardening Techniques**
  - **Encryption**
    - Protects data confidentiality and integrity by converting information into a secure format
  - **Installation of Endpoint Protection**
    - Deploying antivirus and anti-malware solutions on devices safeguards against malicious software
  - **Host-Based Firewall**
    - Monitor and controls incoming and outgoing network traffic on individual devices, providing an additional security layer
  - **Host-Based Intrusion Prevention System (HIPS)**
    - Detects and prevents malicious activities on host systems by monitoring system behavior and blocking suspicious actions
  - **Disabling Ports/Protocols**
    - Turning off unused network ports and protocols reduces potential entry points for attackers
  - **Default Password Changes**
    - Replacing default credentials with strong, unique passwords prevents unauthorized access through commonly known defaults
  - **Removal of Unnecessary Software**
    - Eliminating unused applications reduces vulnerabilities and minimizes the attack surface.