Exam Cram Notes: Indicators of Malicious Activity

1. What are Indicators of Malicious Activity?

Indicators of Malicious Activity (IMAs) are signs or traces that suggest a system, network, or application may have been compromised or is under attack. These indicators are often used in incident detection, forensics, and mitigation efforts to identify attacks or intrusions in progress.

---

2. Types of Indicators of Malicious Activity

1. **Network Traffic Anomalies**
    - **Description**: Unusual patterns or spikes in network traffic that may signal malicious activity.
    - **Examples**:
        - **Unusual Outbound Traffic**: High volume of data being sent outside the network, especially to external servers, which could indicate data exfiltration or a botnet connection.
        - **Port Scanning**: Repeated attempts to connect to various ports on a device, often a precursor to an attack (e.g., a port scan).
        - **Unexpected Protocols**: Detection of non-standard protocols running in the network, possibly due to malware or unauthorized communication.
        - **Denial of Service (DoS)**: A sudden and sustained increase in traffic aimed at overwhelming a server or network, which could indicate a DDoS attack.
    - **Mitigation**: Implementing network monitoring systems, intrusion detection systems (IDS), and firewalls.
2. **File System Modifications**
    - **Description**: Malicious activity often results in changes to files, directories, or the file system structure.
    - **Examples**:
        - **Unauthorized File Access**: Detection of unusual access to sensitive files or folders, such as system configuration files or sensitive user data.
        - **File Integrity Changes**: Files that have been altered or replaced without proper authorization (e.g., tampered configuration files or logs).
        - **Ransomware**: Detection of encrypted files, which may be a sign of ransomware activity.
        - **Creation of Unknown Files**: Unusual or unauthorized file creation, often linked to malware installation.
    - **Mitigation**: Implementing file integrity monitoring, anti-malware tools, and enforcing access controls.
3. **Log Anomalies**

- **Description**: Logs can provide crucial insights into activities occurring within a system or network, and anomalies in these logs often indicate malicious actions.
- **Examples**:
  - **Failed Login Attempts**: Multiple failed login attempts from different locations, often an indication of a brute force attack or credential stuffing.
  - **Log Clearing**: Logs being cleared or deleted, especially after successful exploitation, could indicate an attacker is attempting to cover their tracks.
  - **Unexpected Login Locations**: Logins from locations or IP addresses that deviate from normal patterns (e.g., logins from foreign countries when the user typically logs in locally).
  - **Privilege Escalation**: Logs showing unusual user actions, such as changing user privileges or accessing restricted areas.
- **Mitigation**: Regular log reviews, centralized log management, and setting up alerts for suspicious log entries.

4. **User Behavior Anomalies**
   - **Description**: User activity that deviates from the norm may indicate account compromise or malicious intent.
   - **Examples**:
     - **Abnormal Account Logins**: A user logging in at unusual times or from unfamiliar devices or locations.
     - **Unusual File Access**: A user accessing files or systems outside their normal job functions or permissions.
     - **Unexpected Privilege Escalation**: A user gaining higher levels of access without the appropriate permissions or approval.
     - **Mass File Deletions**: A user deleting a large number of files, which could indicate a data wipe, possibly from malware or a malicious insider.
   - **Mitigation**: Implementing user behavior analytics (UBA), restricting access based on roles, and using multi-factor authentication (MFA).
5. **Malware Indicators**
   - **Description**: Malicious software leaves distinctive traces when it infects a system.
   - **Examples**:
     - **Unknown Processes**: Processes running in the background with suspicious names or that are consuming a high amount of system resources.
     - **Unexpected Network Connections**: Malware may open unauthorized network connections to external servers or command-and-control centers.
     - **High CPU Usage**: Malware often consumes excessive CPU or memory, which can affect system performance.
     - **Fileless Malware**: Malware that resides solely in memory without creating files on the disk, making it harder to detect.

        - **Persistence Mechanisms**: Malware often creates or modifies registry entries, scheduled tasks, or services to maintain persistence even after system reboot.
    - **Mitigation**: Use of anti-malware solutions, endpoint detection and response (EDR) tools, and routine system scans.
6. **Suspicious Process Behavior**
    - **Description**: Processes that exhibit abnormal or unexpected behavior often indicate malicious activity.
    - **Examples**:
        - **Unusual Parent-Child Process Relationships**: Processes spawning other processes that are unrelated or suspicious in nature.
        - **Command Line Arguments**: Processes with unusual or suspicious command-line arguments, such as encoded or obfuscated commands.
        - **Excessive Resource Usage**: Processes that consume an abnormal amount of system resources (CPU, memory, disk), which could be indicative of a malware infection.
        - **Unauthorized Code Execution**: Detection of unauthorized or unknown code being executed on the system (e.g., reverse shells).
    - **Mitigation**: Monitoring system processes, using endpoint detection solutions, and restricting execution permissions.
7. **Indicator of Compromise (IOC)**
    - **Description**: Specific artifacts or traces of an attack that have been identified in one or more affected systems.
    - **Examples**:
        - **File Hashes**: The unique hash values of malicious files detected in a system.
        - **IP Addresses**: Known malicious IP addresses used by attackers for command-and-control or exfiltration.
        - **Domain Names**: Malicious domains or URLs contacted by malware.
        - **Malicious Files**: Identified files that are known to be malicious (e.g., based on a virus signature).
    - **Mitigation**: Use of threat intelligence feeds, IOC-based detection tools, and blocking malicious IPs or domains.
8. **Phishing or Social Engineering Attacks**
    - **Description**: Phishing and other forms of social engineering often serve as a starting point for further malicious activity.
    - **Examples**:
        - **Deceptive Emails or Messages**: Malicious emails or texts designed to trick users into revealing sensitive information or downloading malware.
        - **Malicious Links**: URLs or links that direct the user to phishing websites or sites hosting malware.
        - **Spoofed Email Addresses**: Emails from addresses that closely resemble legitimate ones but are slightly altered to deceive the recipient.
    - **Mitigation**: User education, phishing detection systems, email filtering, and multi-factor authentication (MFA).

---

3. Key Exam Tips

✅ **Recognize network traffic patterns** that could indicate an ongoing attack or intrusion, such as unusual ports or excessive traffic.
✅ **Understand malware indicators**, like abnormal processes, file changes, or unauthorized network connections.
✅ **Know the common signs of social engineering** attacks, including phishing and pretexting, and how they relate to indicators of malicious activity.
✅ **Be familiar with IOC** and how they are used in detecting and responding to malicious activities.