Exam Cram Notes: Mitigation Techniques

1. What are Mitigation Techniques?

Mitigation techniques are strategies and methods implemented to reduce or eliminate the risk of security threats and vulnerabilities. These techniques focus on minimizing the impact of potential security incidents, preventing attacks, and addressing the weaknesses in systems and processes.

---

2. Types of Mitigation Techniques

1. **Firewalls**
   - **Description**: Firewalls control incoming and outgoing network traffic based on predetermined security rules. They help block unauthorized access and prevent certain types of attacks.
   - **Example Techniques**:
     - **Network Firewalls**: Filter traffic based on IP addresses, ports, and protocols to prevent unauthorized access.
     - **Application Firewalls**: Protect specific applications by monitoring and filtering HTTP traffic, preventing attacks like SQL injection.
   - **Mitigation**: Use firewalls to prevent unauthorized access to sensitive systems, especially in areas like perimeter security.
2. **Encryption**
   - **Description**: Encryption is the process of converting plaintext data into unreadable ciphertext to prevent unauthorized access. It ensures confidentiality and protects data integrity.
   - **Example Techniques**:
     - **Symmetric Encryption**: Uses the same key for both encryption and decryption (e.g., AES).
     - **Asymmetric Encryption**: Uses a pair of keys (public and private) for encryption and decryption (e.g., RSA).
     - **End-to-End Encryption (E2EE)**: Protects data as it travels across a network, ensuring that only the sender and receiver can decrypt the data.
   - **Mitigation**: Use encryption to protect sensitive data both at rest (on storage devices) and in transit (across networks).
3. **Access Control**
   - **Description**: Access control mechanisms ensure that only authorized users can access specific resources or perform specific actions within a system.
   - **Example Techniques**:
     - **Role-Based Access Control (RBAC)**: Assigns permissions based on user roles, ensuring users only access resources relevant to their job functions.
     - **Least Privilege**: Users and systems are granted only the minimum permissions needed to perform their tasks.

        - **Mandatory Access Control (MAC)**: Restricts access based on predefined security policies, often enforced by the operating system.
    - **Mitigation**: Implement strong access control policies to reduce the risk of unauthorized access and privilege escalation.

4. **Multi-Factor Authentication (MFA)**
    - **Description**: MFA requires users to provide multiple forms of identification (e.g., password, fingerprint, SMS code) before gaining access to a system, making it more difficult for attackers to gain unauthorized access.
    - **Example Techniques**:
        - **Something You Know**: A password or PIN.
        - **Something You Have**: A mobile phone, security token, or smart card.
        - **Something You Are**: Biometric data like fingerprints or facial recognition.
    - **Mitigation**: Enforce MFA across critical systems and applications to significantly reduce the likelihood of unauthorized access due to stolen credentials.
5. **Security Patches and Updates**
    - **Description**: Keeping software and hardware systems up to date by applying patches and updates ensures that known vulnerabilities are addressed before attackers can exploit them.
    - **Example Techniques**:
        - **Regular Patch Management**: Schedule and automate updates for software, operating systems, and applications to mitigate vulnerabilities.
        - **Vulnerability Scanning**: Regularly scan systems for known vulnerabilities and apply patches as they are released.
    - **Mitigation**: Ensure systems are always up to date to prevent exploits based on outdated software and known vulnerabilities.
6. **Intrusion Detection and Prevention Systems (IDPS)**
    - **Description**: IDPS monitors network and system activities for signs of potential intrusions or attacks, providing both detection and prevention capabilities.
    - **Example Techniques**:
        - **Intrusion Detection Systems (IDS)**: Detect suspicious activities, generate alerts, and notify administrators.
        - **Intrusion Prevention Systems (IPS)**: Actively block identified threats in real time by dropping malicious packets or blocking IP addresses.
    - **Mitigation**: Implement IDPS to detect and prevent attacks, minimizing the impact of intrusions and reducing response time.
7. **Security Information and Event Management (SIEM)**
    - **Description**: SIEM solutions aggregate and analyze logs and security events from various sources to identify anomalies and potential security incidents.
    - **Example Techniques**:
        - **Log Aggregation**: Collect logs from various sources (e.g., firewalls, servers, workstations) for centralized analysis.
        - **Real-Time Analysis**: Use SIEM tools to detect and respond to threats in real time based on log and event data.

        - **Incident Correlation**: Correlate data from different systems to identify patterns that may indicate a security incident.
    - **Mitigation**: Use SIEM to get real-time visibility into security events, enabling faster detection and response to malicious activity.
8. **Network Segmentation**
    - **Description**: Network segmentation divides a larger network into smaller, isolated subnets to limit the spread of attacks and better control access to sensitive resources.
    - **Example Techniques**:
        - **Firewalled Segments**: Use firewalls to create isolated network segments for critical systems.
        - **Virtual LANs (VLANs)**: Use VLANs to segment network traffic, ensuring that only authorized users can access specific areas of the network.
    - **Mitigation**: Segment networks to prevent lateral movement by attackers, isolating critical systems and reducing the risk of full network compromise.
9. **Anti-Malware Software**
    - **Description**: Anti-malware software protects systems from various types of malware, including viruses, worms, ransomware, and spyware.
    - **Example Techniques**:
        - **Real-Time Scanning**: Scans files, emails, and web traffic in real time to detect and block malware before it infects the system.
        - **Heuristic Analysis**: Detects unknown malware by analyzing the behavior of programs and files.
        - **Signature-Based Detection**: Compares files to known malware signatures for detection.
    - **Mitigation**: Use anti-malware solutions to detect, block, and remove malicious software from systems.
10. **Backup and Disaster Recovery Planning**
    - **Description**: Having proper backup and recovery procedures in place ensures that critical data and systems can be restored in the event of a security incident.
    - **Example Techniques**:
        - **Regular Backups**: Perform regular backups of important data, including system configurations, databases, and user files.
        - **Offsite/Cloud Backups**: Store backups in offsite or cloud environments to protect against physical damage (e.g., fire or flood).
        - **Recovery Testing**: Periodically test recovery procedures to ensure they work effectively when needed.
    - **Mitigation**: Use backup and recovery strategies to minimize data loss and downtime during security incidents such as ransomware attacks.
11. **Security Awareness Training**
    - **Description**: Educating users and employees about security best practices can help prevent human error, which is often a key factor in security breaches.
    - **Example Techniques**:
        - **Phishing Simulations**: Conduct simulated phishing attacks to test employee awareness and response.

        - **Social Engineering Awareness**: Teach employees to recognize and report social engineering tactics such as pretexting and baiting.
        - **Security Best Practices**: Provide training on password hygiene, secure browsing, and data protection.
    - **Mitigation**: Invest in security awareness programs to reduce the risk of successful attacks exploiting human error.

---

3. Key Exam Tips

✅ **Understand how firewalls, encryption, and access control** can mitigate network and data breaches.
✅ **Know how multi-factor authentication (MFA)** significantly enhances security and helps prevent unauthorized access.
✅ **Regular patching, updating software, and using SIEM solutions** are essential for keeping systems secure and detecting attacks.
✅ **Apply the principle of least privilege and network segmentation** to limit the damage of any potential attack.
✅ **Recognize the importance of anti-malware tools** and the need for a solid disaster recovery plan to respond to data loss incidents.