Exam Cram Notes: Threat Vectors and Attack Surfaces

1. What are Threat Vectors?

A **threat vector** is the **path or method** used by a threat actor to gain unauthorized access to a system or network. It is how an attack is delivered, propagated, or initiated.

---

2. Types of Threat Vectors

Understanding the different types of threat vectors helps in designing comprehensive security defenses.

1. **Network-Based Threat Vectors**
    - **Description**: Exploits weaknesses in the network infrastructure to gain unauthorized access or disrupt services.
    - **Examples**:
        - **DDoS (Distributed Denial of Service) –** Overloading a network with traffic to make it unavailable.
        - **Man-in-the-Middle (MitM)** – Intercepting and altering communication between two parties.
        - **Eavesdropping –** Capturing network traffic to steal sensitive data (e.g., Wi-Fi sniffing).
2. **Application-Based Threat Vectors**
    - **Description**: Target vulnerabilities in applications or web services.
    - **Examples**:
        - **SQL Injection** – Inserting malicious SQL code into a web application.
        - **Cross-Site Scripting (XSS)** – Injecting scripts into webpages viewed by others.
        - **Buffer Overflow –** Exploiting an application to overwrite memory.
3. **Social Engineering Threat Vectors**
    - **Description**: Manipulating individuals into divulging confidential information or performing actions that compromise security.
    - **Examples**:
        - **Phishing –** Sending fraudulent emails or messages to deceive the recipient.
        - **Pretexting –** Pretending to be someone else to gain access to information.
        - **Vishing –** Voice phishing, where attackers use phone calls to trick users into revealing information.
4. **Physical Threat Vectors**
    - **Description**: Exploits vulnerabilities in physical security to gain access to systems or data.
    - **Examples**:
        - **USB Drops –** Dropping infected USB drives to be found and inserted into systems.

        - **Theft of Hardware –** Stealing laptops, hard drives, or other devices with sensitive data.
        - **Tailgating –** Gaining physical access to restricted areas by following an authorized person.
5. **Email-Based Threat Vectors**
    - **Description**: Exploits vulnerabilities in email systems or uses email as a delivery mechanism for malicious payloads.
    - **Examples**:
        - **Malicious Attachments** – Infected files (e.g., malware or ransomware) sent via email.
        - **Email Spoofing –** Sending fraudulent emails appearing to come from trusted sources.
        - **Phishing Emails –** Deceptive emails designed to steal credentials or install malware.
6. **Cloud-Based Threat Vectors**
    - **Description**: Vulnerabilities that exist in cloud environments or services.
    - **Examples**:
        - **Misconfigured Cloud Services –** Exposing data due to improper cloud configuration.
        - **Cloud Account Compromise –** Gaining unauthorized access to cloud-hosted data or applications.

---

3. What is an Attack Surface?

The **attack surface** refers to the **total points** in a system, network, or application where unauthorized access can occur. A **larger attack surface** means there are more potential entry points for attackers.

---

4. Types of Attack Surfaces

Understanding the various attack surfaces helps in mitigating threats by securing these points of access.

1. **Network Attack Surface**
    - **Description**: Refers to vulnerabilities in the network infrastructure.
    - **Components**:
        - Routers, switches, firewalls, wireless access points, etc.
        - Open ports, unprotected protocols (e.g., Telnet), and insecure network services.
    - **Mitigation**:
        - Network segmentation, firewall configuration, intrusion detection systems (IDS), and proper encryption.
2. **Application Attack Surface**
    - **Description**: Refers to vulnerabilities within applications (both web-based and installed) that attackers can exploit.

    - **Components**:
        - Input fields, user authentication, APIs, and third-party libraries.
    - **Mitigation**:
        - Secure coding practices, input validation, vulnerability testing, and regular patching of software.
3. **User Interface Attack Surface**
    - **Description**: Refers to the points where users interact with systems, including websites and mobile apps.
    - **Components**:
        - Login forms, user account management, and access controls.
    - **Mitigation**:
        - Multi-factor authentication (MFA), session management, and proper user access controls.
4. **Physical Attack Surface**
    - **Description**: The physical points where unauthorized users can gain access to devices, servers, or networks.
    - **Components**:
        - Devices (laptops, smartphones), server rooms, and data centers.
    - **Mitigation**:
        - Physical access controls (e.g., locks, card access), security cameras, and employee training on security policies.
5. **Cloud Attack Surface**
    - **Description**: Refers to vulnerabilities in cloud infrastructures and services.
    - **Components**:
        - Cloud storage, cloud applications, and third-party integrations.
    - **Mitigation**:
        - Proper cloud configurations, encryption, identity management, and periodic security audits.

---

5. Reducing Attack Surface

- **Minimize open ports –** Disable unnecessary services or ports that could be exploited.
- **Patch management –** Regularly update software to close vulnerabilities.
- **Segmentation and isolation** – Isolate sensitive systems to reduce exposure.
- **Principle of least privilege –** Ensure users and systems only have the minimum access necessary.

Key Exam Tips

✅ Understand the **difference between threat vectors** (paths used by attackers) and **attack surfaces** (points of potential vulnerability).
✅ Be familiar with **common types of attack vectors** like **social engineering, physical security**, and **network-based attacks**.

✅ Recognize the **mitigation strategies** for reducing both attack vectors and attack surfaces.
✅ Expect **scenario-based questions** on how to defend against specific threat vectors or reduce attack surfaces in real-world environments.