🧠 “Hack or Be Hacked: Types of Security Attacks You Should Know”

Attacks are primarily categorized by the attacker's **intent** and the resulting **impact** on the three core cybersecurity principles: **Confidentiality, Integrity, and Availability (the CIA Triad)**.

---

1. 👓 Passive Attack

This category is defined by **covert surveillance** and a lack of direct interaction that would alter the system.

- **Key Action:** Observes data traffic silently.
    - *Explanation:* The attacker's presence is difficult to detect because they are not modifying system state or transmitting unusual data; they are only *listening*.
- **Goal: Steal information** (violates **Confidentiality**).
    - *Explanation:* The sole purpose is **information gathering** to exploit the victim later or use the data for unauthorized purposes.
- **Example:** Packet sniffing, traffic analysis (eavesdropping).
    - *Detail:* **Traffic Analysis** involves examining the *patterns* of communication (who talks to whom, and how often) even if the content is encrypted, to infer sensitive relationships or activities.
- **Detection:** Harder to detect (no system change).
    - *Mitigation Focus:* Since detection is difficult, the primary defense must be **prevention**.
- **Defense:** Strong **encryption** (to make collected data useless).
    - *Mechanism:* Encryption scrambles the data, ensuring that even if the attacker successfully intercepts the information, they cannot read it without the proper decryption key.

---

2. ⚔️ Active Attack

This category involves the attacker directly interacting with the target system to cause damage or unauthorized changes.

- **Key Action:** Alters or disrupts data.
    - *Explanation:* Unlike a passive attack, an active attack involves the transmission of new, unauthorized, or modified data, which inherently causes a change in system state.
- **Goal: Modify or destroy data** (violates **Integrity** or **Availability**).
    - *Impact:* An attack on **Integrity** changes data content (e.g., a bank transfer amount); an attack on **Availability** blocks access to the resource (e.g., DoS).
- **Example:** DoS (Denial-of-Service), session hijacking, Masquerade.

  - *Detail:* **Session Hijacking** is a sophisticated attack where an attacker steals a legitimate user's session token to take over their active connection to an application.
- **Detection:** Easier to detect (causes noticeable system changes).
  - *Defense Focus:* Since the attack is disruptive, the defense goal is **rapid detection and response**.
- **Defense:** Firewalls, Intrusion Detection/Prevention Systems (**IDS/IPS**).
  - *Mechanism:* **IPS** actively blocks malicious traffic based on known signatures or behavioral anomalies, preventing the attack from reaching its target.

---

3. 🕵 Insider Attack

This is a risk factor originating from privileged access and trust within an organization.

- **Key Action:** Comes from **within** the organization.
  - *Context:* This attacker already has authorized access to network resources, bypassing perimeter security like firewalls.
- **Goal: Abuse access privilege** (often to leak or destroy data).
  - *Motivation:* Can be malicious (disgruntled employee), negligent (accidental data leak), or compromised (an account taken over by an external threat).
- **Example:** Disgruntled employee leaking data, misuse of legitimate credentials.
  - *Detail:* **Misuse of credentials** is common; the employee may not have malicious intent initially but uses their access to view sensitive data they shouldn't.
- **Mitigation: Principle of Least Privilege (PoLP)**, strict access controls, user monitoring.
  - *Mechanism:* **PoLP** ensures users only have the bare minimum access required to do their job, limiting the potential damage they can inflict, intentionally or accidentally.

---

4. 📦 Distribution Attack

This specifically targets the **supply chain** before a product even reaches the end-user.

- **Key Action:** Corrupts hardware/software **during distribution**.
  - *Process:* The malicious code is inserted into a legitimate product's development, build, or update process.
- **Goal: Spread malicious code** to end-users/systems.
  - *Scope:* This is highly scalable, as a single compromise can infect thousands of end-users who trust the original vendor (known as a **Supply Chain Attack**).
- **Example:** Tampered firmware or updates, infecting software libraries (Supply Chain Attack).
  - *Detail:* The attacker might target a **third-party library** that is widely used, and when developers download the compromised library, the malicious code is incorporated into their own software.

- **Mitigation: Code signing**, checking cryptographic hashes, secure supply chain vetting.
    - *Mechanism:* **Code Signing** uses digital signatures to verify that software has not been tampered with since the developer signed it, alerting the user to any unauthorized modification.