- Filename: eccouncil-ceh31250-v11-1-3-1-attack-classifications.md
- Show Name: CEHv11 (312-50)
- Topic Name: Intro to Ethical Hacking
- Episode Name: Attack Classifications

==

Attack Classifications

Objectives:

- List and define the different attack classifications
- Associate specific attacks types with the attack classifications

---

- Can we start off by listing Attack Classifications we'll need to be aware of?
    - Passive Attacks
    - Active Attacks
    - Close-In Attacks
    - Insider Attacks
    - Distribution Attacks
- Let's dig into Passive Attacks
    - Gathering info by inspecting network traffic
        - Clear-text passwords
        - Other sensitive info (in the clear)
        - Difficult/impossible to detect
- Any Passive Attack examples?
    - Packet Sniffing
    - Network traffic analysis
    - Decryption
- How about Active Attacks? What are they and how do they differ from Passive?
    - Manipulation of data
    - Disruption of services
    - Breaking into systems and compromising networks
    - Can be detected
- A few examples of Active Attacks?
    - DoS
    - Password Attacks
    - Session Hijacking
    - Priv Esc
    - SQLi
    - RCE
- What are we talking about with regards to Close-in Attacks?
    - These attacks are possible through close proximity
        - Being physically near the target could provide opportunity to glean actionable intel
    - Could also be through any type of personal contact with target
- What are some examples of Close-In Attacks?

  - Social engineering
  - Shoulder surfing
  - Dumpster Diving
  - Eavesdropping

- I've heard that Insider Attacks can be very catastrophic. What do we mean by 'Insider Attack' and why is it so dangerous?

  - Assumed level of trust

    - Physical access
    - Computer access
    - Attacker is already beyond many/all safeguards

- Examples of Insider Attacks?

  - Intellectual Property
  - Customer PII

    - Pod Slurping

  - Stolen devices
  - Installing malware and keyloggers
  - Close-in Attacks

    - Social Engineering

  - https://www.k2e.com/articles/insider-threats/

- Difficult but devastating, we have the Distribution Attack. What's this all about?

  - aka Supply-Chain Attack
  - Compromising software and/or hardware before customer installation

- Examples of Distribution Attacks

  - Solarwinds

    - https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/