- Filename: eccouncil-ceh31250-v11-11-1-1-session-hijacking-concepts.md
- Show Name: CEHv11 (312-50)
- Topic Name: Network and Perimeter Hacking: Session Hijacking
- Episode Name: Session Hijacking Concepts
  ==

Session Hijacking Concepts

Objectives:

- Define Session Hijacking
- Explain why session hijacking is successful
- List and define the common session hijacking types

- What is session hijacking?

  - Take over of a TCP coversation
  - Impersonate an authenticated user

    - HTTP
    - TCP

      - MitM

- Why does this work?

  - Sessions that never time out
  - IDs are easily guessed
  - No security around IDs
  - No lockouts for invalid session IDs

- Types

  - Passive

    - Hijack session and just sniff network traffic

  - Active

    - Session take-over

      - Attacker becomes the user and is actively doing things as them

  - Application Layer Hijacking

    - Taking over web-app user session

      - Session IDs = gold!

  - Network Layer Hijacking

    - Intercepting and taking over TCP/UDP sessions

      - ARP Spoofing MitM