- Filename: eccouncil-ceh31250-v11-2-1-1-footprinting-concepts.md
- Show Name: CEHv11 (312-50)
- Topic Name: Footprinting and Recon
- Episode Name: Footprinting Concepts

==

Footprinting Concepts

Objectives:

- Define Footprinting and Footprinting types and describe its objectives in the attack process
- Explain types of information gathered during the Footprinting phase
- Explore Footprinting as a Methodology

- What is Footprinting?
    - Passive
        - No direct interaction with target
            - Kind of like 'eavesdropping' on a conversation
            - Looking for freely available/public info
                - May get lucky and find unsecured sensitive info
        - Difficult/impossible to detect
    - Active
        - Direct interaction with target
            - Interrogation vs eavesdropping
        - Detection possible
- What kinds of information are attackers looking for?
    - System Info
        - OS type
        - Services
        - Usernames/Passwords
    - Network Info
        - DNS
        - Domain/Sub-domains
        - Firewall rules
    - Organizational Info
        - Contact info
        - Employee info
        - Location info
- How does this information help attackers?
    - May reveal security controls
    - Helps them focus on live targets
    - Vulnerability identification
- So does Footprinting directly lead to target compromise?

  - Usually not directly, but it is a crucial step towards those ends
  - It supports compromise attacks like
    - Social Engineering
    - Sensitive Data Exposure
    - System/Network Hacking

...