- Filename: eccouncil-ceh31250-v10-2-1-1-footprinting.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Footprinting
- Description: In this episode, Daniel and Zach discuss the concept and practice of Footprinting. Here they will define Footprinting as it pertains to penetration testing as well as demonstrate passive reconnaissance techniques to gather info from sources like web sites, job listings, search engines, and social media.

==========

Footprinting

- What is footprinting, and how does it relate to reconnaissance?
    - Gathering of target info
        - User names
        - Email addresses
        - Systems
            - Services
            - Operating Systems
                - Vulnerabilities
        - General lay of the land
    - Pentester then uses that info to gain access into the target's systems
- How does one go about the business of footprinting?
    - Passive recon
        - Gathering freely available and distributed target info
            - Target's web sites
                - About Us
                - Contact Us
            - Job Listings
            - Social Media sites
                - Company
                - Users/Employees
            - Search engines
                - Google Dorks
                    - `site`: Only return results from given domain
                    - `inurl`: Must contain X in the url
                    - `intitle`: Results includes X in title of the webpage
                    - Google Hacking Database
                        - https://www.exploit-db.com/google-hacking-database/
            - Social Media
            - Tools
                - The Harvester
                    - Gathers target info
                        - Subdomain names
                        - Employee names
                        - Email Addresses
                        - PGP keys
                        - Open ports and service banners

1. `/usr/bin/theharvester` gets the help
2. `theharvester -d itpro.tv -l 500 -b all`

- Sublist3r