- Filename: eccouncil-ceh31250-v10-2-1-2-footprinting_pt2.md
- Show Name: CEHv10 (312-50)
- Topic Name: Information Gathering and Vulnerability Identification
- Episode Name: Footprinting Pt.2
- Description: In this episode, Daniel and Zach continue their exposition on Footprinting. They pick back up by looking into using specific tools for the gathering of information on your target. This includes performing online searches using Shodan, Netcraft, and Censys, using a website spidering tool like Burp Suite, and directory fuzzing with tools like Dirb.

==

Footprinting Pt.2

- We've seen some great tools that run on the OS, but what about web-based reconnaissance tools?
    - Online Recon Tools
        - Netcraft
        - Shodan
            - Searches for specific types of Internet connected devices
            - Looks for specific banner content
                - Search for: "default password"
        - Censys
            - Search for
                - itpro.tv
                - 443.https.heartbleed.heartbleed_vulnerable: true
- Now that we've discovered our client's web presence, should we now turn to exploring their site or sites?
    - Website Recon
        - Focus on the target site(s) and info you can gather from them
            - "Spidering" or "Crawling" the site
                - Use a proxy like Burp or ZAP
            - Directory fuzzing
                - Dirb, gobuster, dirbuster(ZAP),
            - Look at source code
                - Comments
                - Files/dirs that may be of interest
                - Names
                - Technologies
                - Firebug > Security