- Filename: eccouncil-ceh31250-v12-2-4-1-sub-domain-enumeration.md
- Show Name: CEHv12 (312-50)
- Topic Name: Footprinting and Recon
- Episode Name: Sub-Domain Enumeration

==

Sub-Domain Enumeration

Objectives:

- Search for a target's subdomains by utilizing common hacking tools to properly footprint their attack surface

---

- What is a sub-domain?
  - Domains
    - Main web presence
      - Domain name
        - aka 2nd Level Domain
      - gTLD (Generic Top-Level Domain)
        - Catch-all for specific areas
          - .com
          - .net
  - Sub-Domains
    - Secondary web presence
      - Used to organize web sites that are big enough to need their own space
        - Same idea as a Sub-directory in a file system
- How do we do subdomain enumeration and why is it important to ethical hacking?
  - It's important because...
    - It's apart of the attack surface
  - We can find them a couple of ways
    - Manual searching (demo)
      - Google
        - site:itpro.tv
      - Page source code
- That seems a bit tedious. Can we automate that process?
  - Automation (demo)
    - netcraft
    - sublist3r

https://hover.blog/whats-a-domain-name-subdomain-top-level-domain/
...