Recon

* Asset Discovery
  + Subdomain Bruceforce
    - Tools
      * sublist3r
      * enumall
      * massdns
      * atldns
      * brucesubs
      * dns-parallel-prober
      * dnscan
      * knockpy
      * tko-subs
      * HostileSubBruceforce
    - Different permutation
    - Google Dorks: site.com +inurl:dev -cdn
    - Different enviroment
      * dashboard.dev.site.com
      * dashboard-dev.site.com
  + Certificate transparency
    - How to find more?
      * Censys
        + Look for SSL certificate
      * Shodan
        + Search for hostname
        + Filter

Port

Tile

Product

Org

Hostname

ssl

* + - * Certspotter
        + make bash alias
        + automate
        + win
* OSINT
  + ARIN
    - Defication
      * American Registry for Internet Numbers
  + Acquisitions
    - Usually in Scope (after 6 months)
    - Geared towards bigger company
* Vender Services
  + Leak Credentials
    - Paste Site
    - Online Repositories
  + CDN and Cloud Services
    - Misconfigurations
* Defication
  + Understand how application is built
  + Understand how application process data
  + Finding possible "entry" points or company assest
  + Finding files, folder, endpoints
* Automation

Contain Discovery

* Visual Identification
* Port Scanning
* Directory Bruceforce
* Javascript Files