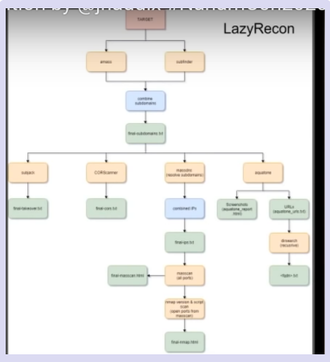
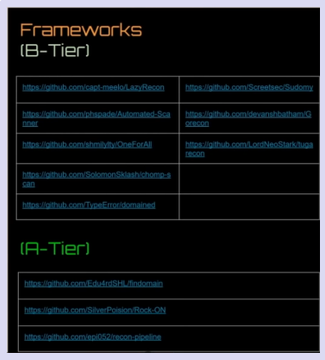
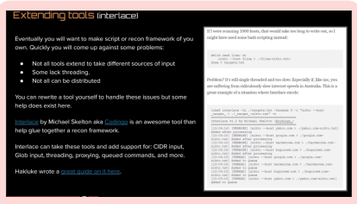
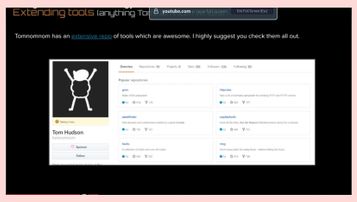
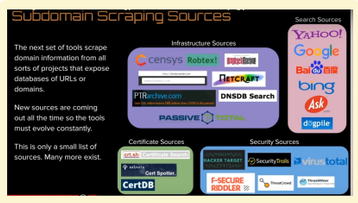
TOOLS

- frameworks
  - 

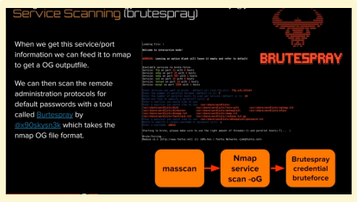
    Layrecon
  - 

    links imp
- people
  - TomNomNom
  - samwcyo
  - bitk_
  - defparam
  - jcran
  - jeff_foley
  - secrinti
  - chloemessdaghi
  - mdisec
  - snyff
  - _johnhammond
  - jhaddix
- wordlists
  - tailored wordlists
  - massive wordlists
  - commonspeak V lateset for a very big massive list
- Automated tools
  - extending tools
    - 

      interlace
    - Subtopic 2
  - 

    tomnomnom has an extensive repo
- sites
- manual tools
  - link subdomain emumeration
    - gospider
    - hakrawler
    - subdomainizer
    - amass
    - subfinder
    - Gwendal Le Coguic (made him alot of money)
    - Masscan
  - subdomains recursion
    - subscraper
  - subdomain scraping sources
    - 

      tools for subdomain scrapping
  - subdomain bruteforcing
    - Massdns
    - Amass -rf
    - shuffledns
    - Subtopic 4
  - Alteration Scanning
    - altdns
    - amass
  - Port Scanning
    -

      masscan faster than nmap
    - nmap
  - Port Analysis
    - dnmasscan
  - service scanning
    - 

      brutespray
  - github Dorking
    -

      manual
    - gdorkslinks
  - screen shotting links
    - eyewitness
    - aquatone
    - httpscreenshot
  - subdomain takeover
    - can-i-take-over-xyz
    - subover
    - nuclei

Presented with xmind