Recon Phase

- ^_^
  - Company
    - Domains
      - Subdomains
        - Subdomain Enumeration
          - Bruteforce
            - gobuster dns -d Domain.com -w subdomains.txt
          - Third Parties
            - amass enum -passive -d Domain_name
            - knockpy.py
            - crt.sh
            - assetfinder
            - virus total
            - netcraft
            - search engine
              - google dorking
                - site:
                - intext:
                - inurl:
          - Github
            - github-subdomains.py
            - github-endpoints.py
          - httpx
          - eyewitness
        - Fingerprint Techs
          - Shodan
            - Query using CIDR
              - net:CIDR,CIDR,CIDR
            - Query using Org name
              - org:oragnization_name
            - Query using SSL certs
              - ssl:organization_name
          - Cencys
          - Nmap (for small set of IPs)
          - Masscan (for large set of IPs)
          - Webapplication fingerprinting
            - Wappalyzer (browser ext)
              - Wappylyzer (command line)
                - https://github.com/vincd/wappylyzer
                - python3 main.py analyze -u URL
            - Firewall
              - WAF detection
                - https://github.com/EnableSecurity/wafw00f
              - WAF bypass
                - https://github.com/0xInfection/Awesome-WAF#known-bypasses
        - Content Discovery
          - Self Crawl
            - https://github.com/ghostlulzhacks/crawler/tree/master
            - python3 crawler.py -d <URL> -l <Levels Deep to Crawl>
          - Wayback machine crawl data
            - web.archive.org
          - Common Crawl
            - commoncrawl.org
            - https://github.com/ghostlulzhacks/commoncrawl
          - Directory bruteforce
            - gobuster
              - gobuster dir -k -w <wordlist> -u <url>
          - google dork
            - ext:
        - Javascript files discovery
          - Link Finder
            - https://github.com/GerbenJavado/LinkFinder
            - python linkfinder.py -i <JavaScript File> -o cli
          - JSsearch
            - https://github.com/incogbyte/jsearch
            - python3.7 jsearch.py -u https://starbucks.com -n Starbucks
        - Google Dorks
          - https://www.exploit-db.com/google-hacking-database
          - https://gbhackers.com/latest-google-dorks-list/
            - intitle:
              inurl:
              intext:
              define:
              site:
              phonebook:
              maps:
              book:
              info:
              movie:
              weather:
              related:
              link: