iLab Tools

Modules :-

1. Footprinting and Reconnaissance

a. Through Search engines
   i. Advanced Google hacking techniques
   ii. Video search engine - https://mattw.io/youtube-metadata/
   iii. FTP search engine - **https://www.searchftps.net/**
   iv. IoT search engine - **shodan.io and censys.io**

b. Through web services and tools
   i. Netcraft, Sublist3r, **Pentest-Tools Find Subdomains** (https://pentest-tools.com)
   ii. PeekYou, Spokeo, pipl, Intelius, BeenVerified
   iii. theHarvester,theHarvester -d [domain] -l [Result] -b [source]
   iv. Sherlock, **Social Searcher** (https://www.social-searcher.com), **UserRecon** (https://github.com)
   v. Deep Dive with Tor Browser, **ExoneraTor (https://metrics.torproject.org)**, **OnionLand (https://onionlandsearchengine.com)**

c. Perform website footprinting
   i. Photon [python3 photon.py -u www.certifiedhacker.com]
   ii. Central Ops, Website Informer (https://website.informer.com), Burp Suite (https://portswigger.net), Zaproxy (https://www.zaproxy.org)
   iii. Web data extractor, **ParseHub** (https://www.parsehub.com), **SpiderFoot** (https://www.spiderfoot.net)
   iv. HTTrack website copier, **Cyotek WebCopy** (https://www.cyotek.com)
   v. GRecon [python3 grecon.py]
   vi. CeWL [cewl -d 2 -m 5 https://www.certifiedhacker.com]

d. Perform email footprinting
   i. eMailTrackerPro, **Infoga** (https://github.com), **Mailtrack** (https://mailtrack.io)

e. Perform whois and DNS footprinting
   i. Whois Lookup, **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com)
   ii. Nslookup, **DNSdumpster** (https://dnsdumpster.com), **DNS Records** (https://network-tools.com)
   iii. Reverse Ip domain check
   iv. DNSRecon [./dnsrecon.py **-r 162.241.216.0-162.241.216.255**]
   v. Security Trail, **DNSChecker** (https://dnschecker.org), and **DNSdumpster** (https://dnsdumpster.com)

f. Through Network footprinting
   i. Tracert(windows), Traceroute(Parrot), **VisualRoute** (http://www.visualroute.com), **Traceroute NG** (https://www.solarwinds.com)

g. Through footprinting tools
   i. Recon-ng
      - Marketplace install all
      - Modules search
      - Workspaces
      - Workspaces create CEH
      - Workspace list
      - Db insert domains
      - Give name of the domain
      - Show domain
      - Modules load brute
      - Modules load recon/domains-hosts/brute_hosts
      - Run
   ii. Maltego
   iii. OSRFramework
      1. **domainfy -n [domain_name] -t all** (existing domains using words and nicknames)
      2. **Searchfy -q [target user name]** (user details on different social networking platforms)
      3. **usufy** - Gathers registered accounts with given usernames.
      4. **mailfy** – Gathers information about email accounts
      5. **phonefy** – Checks for the existence of a given series of phones
      6. **entify** – Extracts entities using regular expressions from provided URLs

iv. FOCA

v. Billcipher [python3 billcipher.py]

vi. OSINT Framework

{

Recon-Dog (https://www.github.com), **Grecon** (https://github.com), **Th3Inspector** (https://github.com), **Raccoon** (https://github.com), **Orb** (https://github.com)

}