Recon

Acquistions (Finding Seeds/Roots)

- Crunchbase
  - We can investigate a company's acquisition on sites like https://crunchbase.com, wikipedia, and Google.
- ASN Enumeration
  - Autonomous System Numbers are given to large enough networks. These ASN's will help us track down some semblance of an entity's IT infrastructure. The most reliable way to get these is manually through Hurricane Electric's free-form search:
    http://bgp.he.net
- ASN Enumeration (CMD line)
  - https://github.com/yassineaboukir/Asnlookup
  - python asnlookup.py -o <Organization>
- ASN Enumeration with AMASS
  - amass intel -asn <asn number>
- Reverse WHOIS (with Whoxy.com)
  - Every website has some registration info on file with the registrars. Two key pieces of data we can use are Organization name and any emails in the WHOIS data. To do this you need access to a large WHOIS database. WHOXY.com is one such database. You can use whoxy.com in this fashion, after you register and your free API key:
    http://api.whoxy.com/?key=APIkeyHERE
    &reverse=whois&name=Twitch+Hostmaster
- Reverse WHOIS (with DOMLink)
  - https://github.com/vysecurity/DomLink
  - python domLink.py -D target.com -o target.out.txt
- Ad/Analytics Relationships (builtwith.com)
  - You can also glean related domains and subdomains by looking at a target's ad/analytics tracker codes. Many sites use the same codes across all their domains. Google analytics and New Relic codes are the most common. We can look at these "relationships" via a site called BuiltWith. Builtwith also has a Chrome and Firefox extension to do this on the fly.
  - https://builtwith.com/relationships/twitch.tv
  - CMD Line - https://raw.githubusercontent.com/m4ll0k/Bug-Bounty-Toolz/master/getrelationship.py
- Google FU
  - Copyright text
  - Terms of service text
  - Privacy policy text
- Shodan
  - https://www.shodan.io/search?query=twitch.tv

Finding Subdomains

- Linked and JS Discovery
  - Linked Discovery with Burp Suite Pro
    1. Turn off passive scanning
    2. Set forms auto to submit (if you're feeling frisky)
    3. Set scope to advanced control and use "keyword" of target name (not a normal FQDN)
    4. Walk+browse main site, then spider all hosts recursively!
    5. Profit
  - Linked Discovery (with GoSpider or hakrawler)
    - https://github.com/jaeles-project/gospider
    - gospider -q -s "https://google.com/"
    - https://github.com/hakluke/hakrawler
    - cat urls.txt | hakrawler
  - Subdomain Enumeration (with SubDomainizer)
    1. Find subdomains referenced in js files
    2. Find cloud services referenced in js files
    3. Use the Shannon Entropy formula to find potentially sensitive items in js files
    - https://github.com/nsonaniya2010/SubDomainizer
    - python3 SubDomainizer.py -u https://example.com
- Subdomain Scraping
  - Google
    1. site:twitch.tv -www.twitch.tv
    2. site:twitch.tv -www.twitch.tv -watch.twitch.tv
    3. site:twitch.tv -www.twitch.tv -watch.twitch.tv -dev.twitch.tv
  - Amass
    - amass -d twitch.tv
  - Subfinder
    - https://github.com/projectdiscovery/subfinder
    - subfinder -d hackerone.com -v
  - GitHub-subdomains.py
    - https://github.com/gwen001/github-search
    - python3 github-subdomains.py -t "github token" -d twitch.tv > twitch.tv
  - shosubgo
    - https://github.com/d3fx/shosubgo
    - go run main.go -d target.com -s YourAPIKEY
  - Cloud Ranges
    - https://www.daehee.com/scan-aws-ip-ssl-certificates/
    - curl 'https://tls.bufferover.run/dns?q=.twitch.tv' 2>/dev/null | jq .Results
- Subdomain Bruteforce
  - Amass
    - Amass offers bruteforcing via the "enum" tool using the "brute" switch.
      - amass enum -brute -d twitch.tv -src
    - You can also specify any number of resolvers
      - amass enum -brute -d twitch.tv -rf resolvers.txt -w bruteforce.list
  - Async DNS Brute
    - https://github.com/blark/aiodnsbrute
  - shuffleDNS
    - https://github.com/projectdiscovery/shuffledns
    - shuffledns -d hackerone.com -w words.txt -r resolvers-excellent.txt
  - Sundomain bruting lists
    - https://gist.github.com/jhaddix/86a06c5dc309d08580a018c66354a056
    - A multi resolver, threaded subdomain bruter is only as good as it's wordlist.
      There are two trains of thought here:
      - Tailored wordlists
      - Massive wordlists
  - Alteration Scanning
    - https://github.com/infosec-au/altdns
    - altdns -i subdomains.txt -o data_output -w words.txt -r -s results_output.txt
- Other
  - Favicon analysis
    - https://github.com/devanshbatham/FavFreak
    - cat urls.txt | python3 favfreak.py -o output
  - Port Analysis (masscan)
    - masscan -p1-65535 -iL $ipFile --max-rate 1800 -oG $outPutFile.log
    - https://danielmiessler.com/study/masscan/
  - Port Analysis (dnmasscan)
    - dnmasscan example.txt dns.log -p80,443 -oG masscan.log
  - Service Scanning
    - When we get this service/port information we can feed it to nmap to get a OG outputfile.
    - https://github.com/x90skysn3k/brutespray
    - python brutespray.py --file nmap.gnmap
  - GitHub Dorking Manual
    - https://gist.github.com/jhaddix/1fb7ab2409ab579178d2a79959909b33
    - bash Gdorkslinks.sh twitch.tv
  - Screenshotting (Eyewitness, Aquatone, httpscreenshot)
    - https://github.com/michenriksen/aquatone
    - cat urls.txt | aquatone
    - https://github.com/breenmachine/httpscreenshot
    - ./httpscreenshot.py -i \<gnmapFile\> -p -w 40 -a -vH
    - https://github.com/FortyNorthSecurity/EyeWitness
    - ./EyeWitness -f urls.txt --web
  - Subdomain takeover
    - https://github.com/EdOverflow/can-i-take-over-xyz
    - https://github.com/Ice3man543/SubOver
    - ./SubOver -l subdomains.txt
    - Nuclei
      https://github.com/projectdiscovery/nuclei

Automation++

- Interlace
  - https://github.com/codingo/Interlace
  - Guide - https://hakluke.medium.com/interlace-a-productivity-tool-for-pentesters-and-bug-hunters-automate-and-multithread-your-d18c8137fd5d
- Tomnomnom
  - https://github.com/tomnomnom
- Frameworks
  - C Tier
    - https://github.com/AdmiralGaust/bountyRecon
      https://github.com/offhourscoding/recon
      https://github.com/Samba10x/Recon-tools
      https://github.com/JoshuaMart/AutoRecon
      https://github.com/yourbuddy25/Hunter
      https://github.com/venom26/recon/blob/master/ultimate_recon.sh
      https://gist.github.com/dwisiswant0/5f647e3d406b5e984e6d69d3538968cd
  - B Tier
    - https://github.com/capt-meelo/LazyRecon
      https://github.com/Screetsec/Sudomy
      https://github.com/phspade/Automated-Scanner
      https://github.com/devanshbatham/Gorecon
      https://github.com/shmilylty/OneForAll
      https://github.com/LordNeoStark/tugarecon
      https://github.com/SolomonSklash/chomp-scan
      https://github.com/s0md3v/photon
      https://github.com/TypeError/domained
  - A Tier
    - https://github.com/Edu4rdSHL/findomain
      https://github.com/SilverPoision/Rock-ON
      https://github.com/epi052/recon-pipeline
  - S Tier
    - https://www.intrigue.io/
      https://assetnote.io/
      https://www.spiderfoot.net/
      https://projectdiscovery.io/#/
      https://github.com/jaeles-project/jaeles
      https://github.com/j3ssie/Osmedeus
      https://huntersuite.io/
      https://github.com/yogeshojha/rengine
  - Nuclei
    - nuclei -t dot-env.yaml -l targets.txt