Bug Hunter Methodology V4 (@jhaddix)

Tools

Syntax

- Finding Seeds
  - Crunchbase
    - Add Acquisition Domains to Seeds
- ASN Enumeration
  - bgp.he.net
    - Amass Intel
      - ASN from bgp.he.net
        - amass intel -asn 46489
  - metabigor
  - asnlookup
- Reverse Whois
  - whoxy.com
  - Domlink
- Shodan
  - Check SSL Cert Names
- Linked & JS Discovery
  - Content Discovery in Burp
  - GoSpider
  - Hakrawler
  - Subdomainizer (JS)
- Subdomain Scraping
  - Amass
  - Subfinder
  - git-subdomains.py
  - Shosubgo
  - Scan Cloud Ranges
    - curl 'https://tls.bufferover.run/dns?q=.twitch.tv' 2>/dev/null | jq .Results
- Subdomain Bruteforcing
  - Amass
    - all.txt
  - Shuffledns
- Alteration Scanning
  - Naming Patterns
    - dev1.twitch.tv
      dev2.twitch.tv
      devx.twitch.tv
      etc
- Port Scanning
  - dnsmasscan
    - dnmasscan example.txt dns.log -p80,443 -oG masscan.log
  - masscan
    - masscan -p1-65535 -iL $ipFile --max-rate 1800 -oG $outPutFile.log
- Service Scanning
  - Brutespray
- Github Dorking
  - https://gist.github.com/jhaddix/1fb7ab2409ab579178d2a79959909b33
  - github-search
  - th3g3ntlemans full module on github and sensitive data exposure
- Screenshotting
  - Eyewitness
  - Gowitness
- Subdomain Takeover
  - can-i-take-over-xyz
  - nuclei
- Automation
  - Interlace (Hakkluke Article)
  - ultimate_recon.sh