Recon workflow

Horizontal & vertical Correlations

https://mxtoolbox.com/asn.aspx

https://viewdns.info/reversewhois

https://domaineye.com/

```
amass intel -org <company name here>
amass intel -asn <ASN Number Here>
amass intel -cidr <CIDR Range Here>
amass intel -whois -d <Domain Name Here>
amass enum -passive -d <Domain Name Here>
```

https://github.com/danielmiessler/SecLists

Subdomain bruteforcing - https://gist.github.com/jhaddix/86a06c5dc309d08580a018c66354a056

https://github.com/internetwache/CT_subdomains

https://crt.sh/?q=%25.facebook.com

https://github.com/ghostlulzhacks/CertificateTransparencyLogs

```
gobuster dns -d starbucks.com -w subdomains.txt
```

https://github.com/infosec-au/altdns

A small list of these

resources can be found below:

- Virus Total
- Netcraft
- DNSdumpster
- Threat crowed
- Shodan
- Cencys
- DNSdb
- Pastebin

```
knockpy.py <Domain Name Here>
```

https://github.com/blechschmidt/massdns

finding aws endpoints, awskeys, urls, upload fields

https://github.com/incogbyte/jsearch

Google dorks

site:<Third Party Vendor> <Company Name>

site:pastebin.com “Company Name”

site:*.atlassian.net “Company Name”

site:bitbucket.org “Company Name”

Inurl:gitlab “Company Name”

https://pentest-tools.com/information-gathering/google-hacking#

Shodan dorks

net:<”CIDR,CIDR,CIDR”>

org:<”Organization Name”>

ssl:<”ORGANIZATION NAME”>

Censys - https://censys.io/ipv4

waf - https://github.com/EnableSecurity/wafw00f

Wafw00f <URL HERE>

wafbypass - https://github.com/0xInfection/Awesome-WAF#known-bypasses

subdomaintakeover - https://github.com/haccer/subjack

https://github.com/EdOverflow/can-i-take-over-xyz

github dorks - https://github.com/techgaun/github-dorks/blob/master/github-dorks.txt

Aws s3

s3bucket dorks - site:.s3.amazonaws.com "Starbucks"

https://github.com/ghostlulzhacks/s3brute

python amazon-s3-enum.py -w BucketNames.txt -d <Domain Here>

Google cloud storage

https://github.com/RhinoSecurityLabs/GCPBucketBrute

```
python3 gcpbucketbrute.py -k <Domain Here> -u
```

Digital ocean spaces

site:digitaloceanspaces.com <Domain Here>

https://github.com/appsecco/spaces-finder

Unauthenticated Elasticsearch DB

port "9200" elastic [;shodan query]

Exposed Docker api

product:docker [;shodan query]

Kubernetes API

unauthenticated REST API on port 10250

product:"kubernetes"

Gitdumper (.git) - https://github.com/internetwache/GitTools/tree/master/Dumper

Subversion (.svn)- https://github.com/anantshri/svn-extractor

Exploitation CMS

Wordpress - https://github.com/wpscanteam/wpscan

Joomla - https://github.com/rezasp/joomscan

Drupal - https://github.com/droope/droopescan

adobe aem - https://github.com/0ang3el/aem-hacker

Magento - https://github.com/steverobbins/magescan

URLSCAN

https://urlscan.io/

https://rapiddns.io

https://sitereview.bluecoat.com/#/

Security Tools

https://tools.tldr.run/

Awesome Shodan Queries for Recon

https://github.com/jakejarvis/awesome-shodan-queries

https://www.osintme.com/index.php/2021/01/16/ultimate-osint-with-shodan-100-great-shodan-queries/

Simple Recon Workflow

Subdomain scan - amass enum -brute -active -d domain.com-o amass-output.txt

httprobe - cat amass-output.txt | httprobe -phttp:81 -p http:3000 -p https:3000 -p http:3001 -phttps:3001 -p http:8000 -phttp:8080 -p https:8443 -c 50 | tee online-domains.txt

anew - cat new-output.txt| anew old-output.txt |httprobe

dnsgen - catamass-output.txt | dnsgen - | httprobe

Aquatone- catdomains-endpoints.txt | aquatone

files/directory bruteforcing - ffuf -ac -v -u https://domain/FUZZ -wwordlist.txt