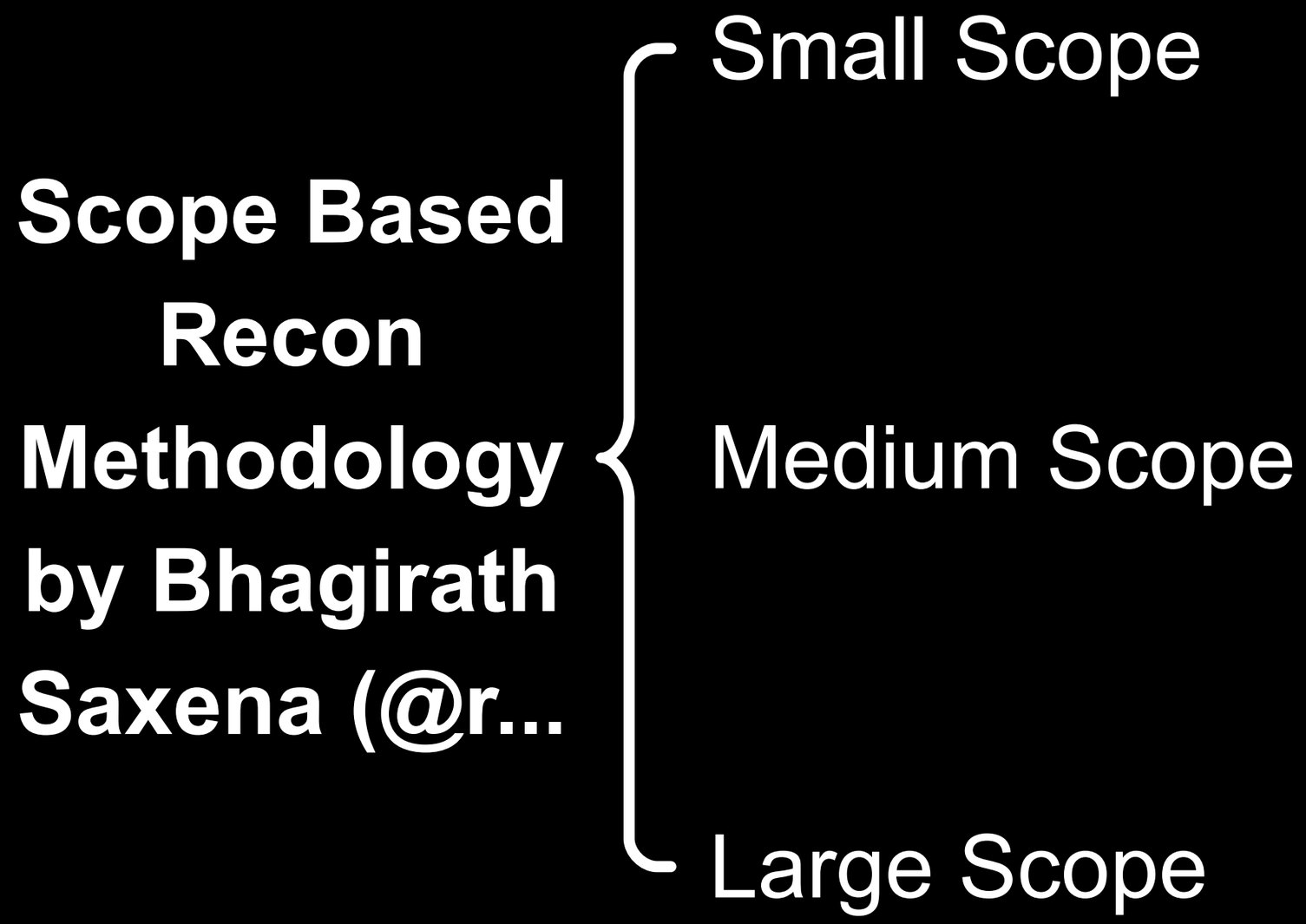
Scope Based Recon Methodology by Bhagirath Saxena (@rix4uni) For GarudRecon



Small Scope

Small Scope

Only Specific URLs are part of Scope. This usually includes staging/dev/testing or single URLs. like: support.dell.com

Only Specific URLs are part of Scope. T...

Recon To-Do

Recon To-Do

- Port Scanning & Probing
- Technology Fingerprinting
- Directory Enumeration
- Url Crawling
- Google Dorking

Recon To-Do

- Google Dorking
- JS Crawling
- Hidden Parameter
- Program Based Wordlist Generator
- Github Dorking

Recon To-Do

- Github Dorking
- 403/401 bypass
- byp4xx
- Known Vulnerabilities

Port Scanning & Probing

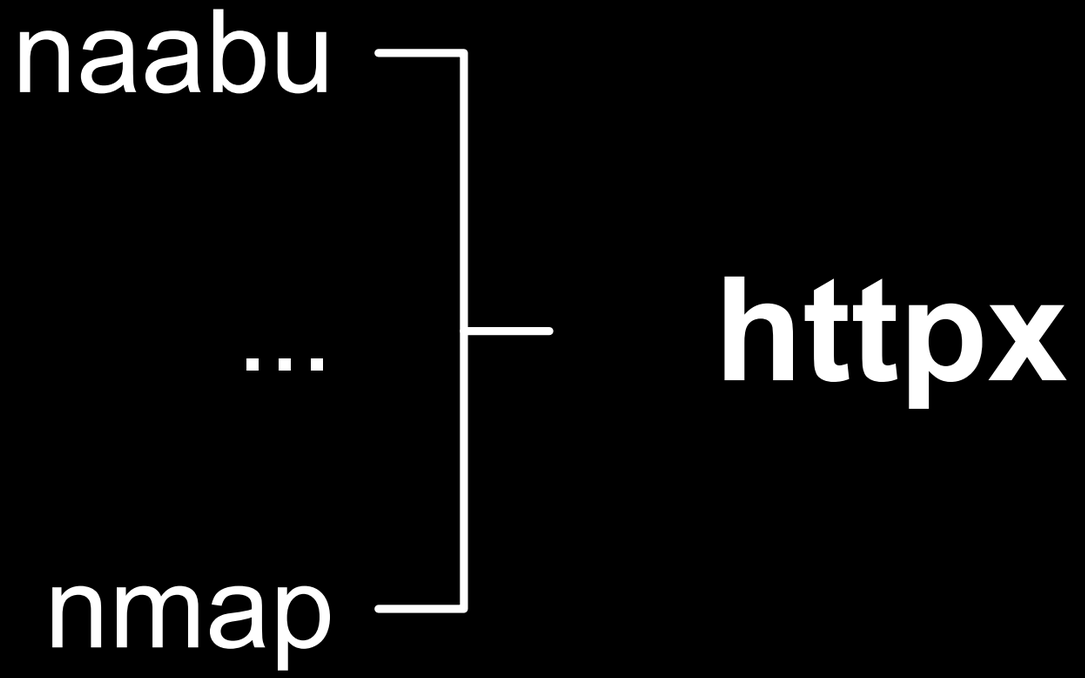
- naabu
- masscan
- rustscan
- nmap

naabu

cat subs.txt | naabu -duc -silent -o naabu.txt

(top 1000 or 65365)

Small Scope



httpx

cat naabu.txt | httpx -silent -duc -nc -nf -title -ct -sc -cl -o httpx.txt

Technology Fingerprinting

techx

techx

nucleitechx

Directory Enumeration

- ffuf
- dirsearch
- feroxbuster
- wfuzz

ffuf

ffuf -c -u https://example.com/FUZZ -w onelistforallshort.txt

https://github.com/dwyl/english-words/blob/master/words.txt
ffuf -c -u https://example.com/FUZZ.zip -w words.txt -mc 200,302
ffuf -c -u https://example.com/FUZZ.php -w words.txt -mc 200,302

default fuzzing 403, 404 domains

ffuf

ffuf -c -u https://example.com/FUZZ -w onelistforallshort.txt

https://github.com/dwyl/english-words/blob/master/words.txt
ffuf -c -u https://example.com/FUZZ.zip -w words.txt -mc 200,302
ffuf -c -u https://example.com/FUZZ.php -w words.txt -mc 200,302

default fuzzing 403, 404 domains

ffuf

ffufPostprocessing

Url Crawling

- waymore
- hakrawler
- waybackurls
- gau
- katana

Url Crawling

- katana
- gospider
- uforall
- github-endpoints
- crawley

Url Crawling

- urlgrab
- GoLinkFinder
- cariddi
- Burp 1.7 spider urls

Google Dorking

- Automated
- Manual

Automated

- xnldorker
- uDork
- GooFuzz
- dorks_hunter

Manual

- https://pentestingdorks.netlify.app/google/
- BulkURLOpener

https://pentestingdorks.netlify.app/google/

Do you want to add your manually google dorks output in google-dorks-output.txt or do you want to skip or wait 30 minites: Y/N/wait

this will automatically choose N if no output provide within 30minutes

JS Crawling

- subjs
- getJS
- jscrawler
- linkfinder
- xnLinkFinder

JS Crawling

- xnLinkFinder
- getjswords
- gowitness
- sourcemapper
- linx

JS Crawling

- sourcemapper
- linx
- other tools
- js moniter

gowitness

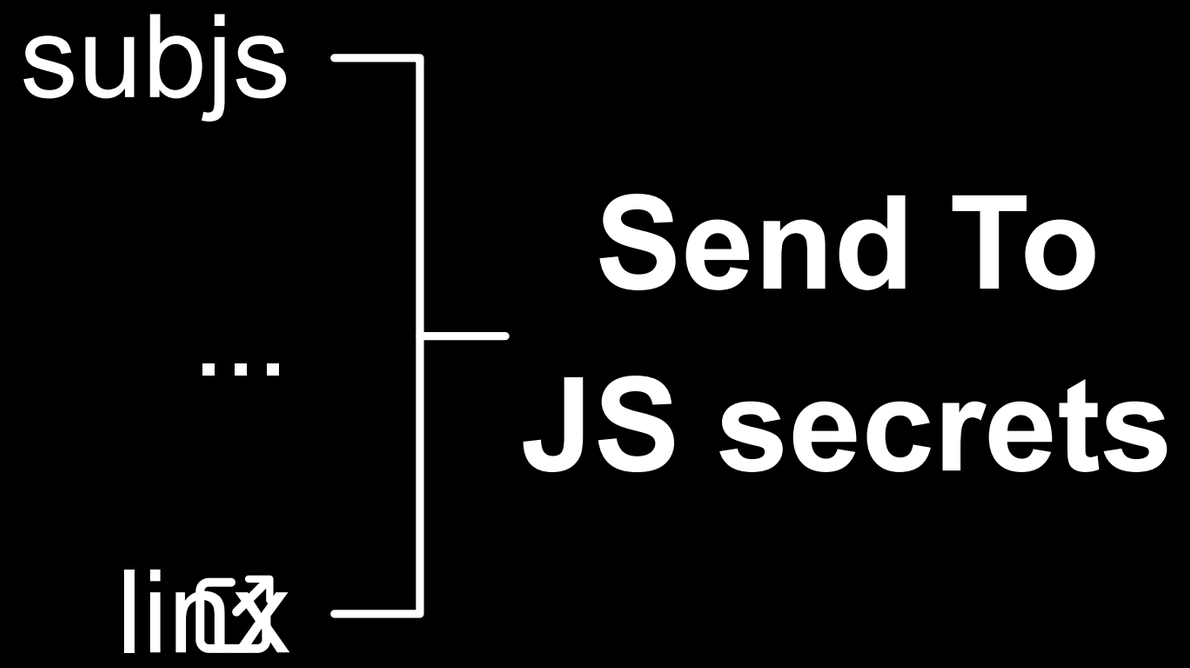
collect js links in gowitness network logs, gives exta links because it's DOM based data

sourcemapper

sourcemapper -insecure -output sourcemapper -url https://www.cga.ct.gov/aspx/cgabilltracking/pub/Scripts/js/pdfmake.min.js.map

interlace -tL js_links.txt -threads 10 -c "sourcemapper -insecure -url _target_ -output _output_/_cleantarget_" -o .tmp/sourcemapper

Small Scope



Hidden Parameter

- paramfinder
- msarjun (arjun)
- x8

Program Based Wordlist Generator

- cewl
- unfurl
- roboxtractor
- Password Generation

Password Generation

pydictor

Github Dorking

gitrob

403/401 bypass

These tools only can bypass 403 endpoints not 403 domain

403/401 bypass

- byp4xx
- 4-ZERO-3

Known Vulnerabilities

1st check vulnerability on hidden urls then exclude those hidden urls you already checked in gf urls, and check gf parameters then exclude hidden and gf urls because you already checked those urls and check all parameters

this way you can avoid getting blocked/getting temprary website down

Known Vulnerabilities

- xss (knoxnl with knoxss, dalfox, pyxss)
- error based sqli (nuclei template)
- blind sqli (gosqli with ghauri and sqlmap)
- lfi (nuclei template)
- rce (nuclei template)

Known Vulnerabilities

- rce (nuclei template)
- Dot Git
- Hardcoded Information in JavaScript (nuclei exposures template)
- technology based vuln (nucleitechx)
- Sensitive PDFs

Known Vulnerabilities

- technology based vuln (nucleitechx)
- Sensitive PDFs
- URLs Secrets
- JS secrets

Dot Git

goop

Sensitive PDFs

pdftotext

pdftotext

https://ott3rly.com/mass-hunting-for-leaked-sensitive-documents/

interlace -tL urls.txt -threads 10 -c "curl -s _target_ | pdftotext - _output_/_cleantarget_.txt" 2>/dev/null" -o ~/pdf &>/dev/null

find ~/pdf -type f -print0 | xargs --null grep -Z -L -Eai 'internal use only|confidential' | xargs --null rm

pdftotext

https://ott3rly.com/mass-hunting-for-leaked-sensitive-documents/

interlace -tL urls.txt -threads 10 -c "curl -s _target_ | pdftotext - _output_/_cleantarget_.txt" 2>/dev/null" -o ~/pdf &>/dev/null

find ~/pdf -type f -print0 | xargs --null grep -Z -L -Eai 'internal use only|confidential' | xargs --null rm

URLs Secrets

- back-me-up
- linkinspector

JS secrets

- nuceli exposures
- trufflehog
- secretfinder
- mantra

Medium Scope

Medium Scope

Usually the scope is wild card scope where all the subdomains are part of scope. like:
Scope: *.dell.com

Usually the scope is wild card scope whe...

Recon To-Do

Recon To-Do

- Passive Subdomain Enumeration
- Certificate Transperency
- Content Security Policy
- Subdomain Permutations
- Subdomain DNS Enumeration

Recon To-Do

- Subdomain DNS Enumeration
- Cloud Recon
- Subdomain Analytics Enumeration
- Port Scanning & Probing
- Subdomain Probing

Recon To-Do

- Subdomain Bruteforcing
- VHOST Dicovery
- Screenshotting
- Directory Enumeration
- Email Enumeration

Recon To-Do

- Email Enumeration
- IP Information Enumeration
- Url Crawling
- Google Dorking
- JS Crawling

Recon To-Do

- JS Crawling
- Hidden Parameter
- Program Based Wordlist Generator
- Github Dorking
- 403/401 bypass
- Favicon Lookup

Recon To-Do

- Favicon Lookup
- Internet Search Engine Discovery (Shodan, Censys, FOFA, Hunter How, Spyse, etc.)
- Misconfigured Cloud Storage
- IP Range Enumeration (If in Scope)

Recon To-Do

- Misconfigured Cloud Storage
- IP Range Enumeration (If in Scope)
- Testing TLS/SSL encryption
- Vulnerability Scanning

Passive Subdomain Enumeration

- BugBountyData
- subfinder
- amass
- subdog
- findomain

Passive Subdomain Enumeration

- findomain
- chaos
- github-subdomains
- bbot
- oneforall
- shosubgo

Passive Subdomain Enumeration

- bbot
- oneforall
- shosubgo
- assetfinder
- SubDomainizer

Certificate Transperency

- certinfo
- rcert
- cero

Content Security Policy

csprecon 

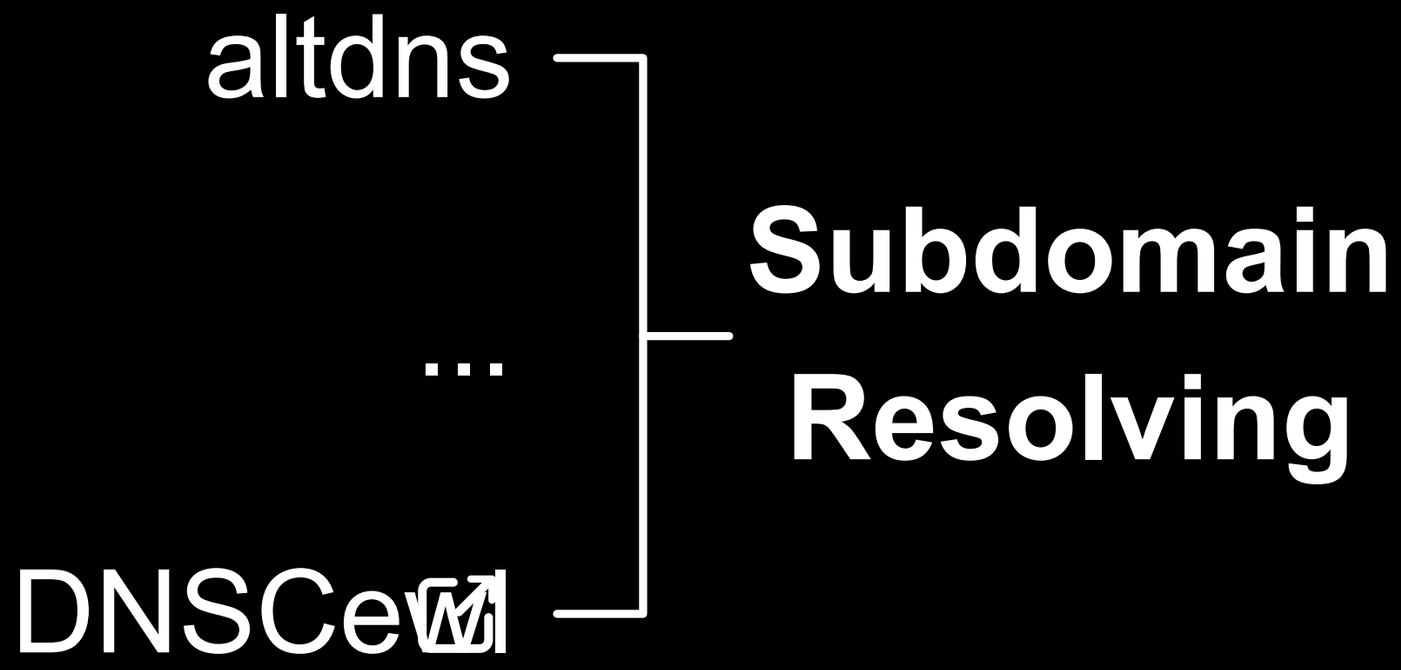
Subdomain Permutations

- altdns
- puredns
- alterx
- gotator
- dnsgen

Subdomain Permutations

- dnsgen
- goaltdns
- ripgen
- DNSCewl

Medium Scope



Subdomain Resolving

- puredns
- shuffleDNS
- massdns

Subdomain DNS Enumeration

dnsx

Cloud Recon

- Cloudrecon
- http://kaeferjaeger.gay
- CIDR Ranges

Cloudrecon

https://github.com/g0ldencybersec/CloudRecon

Tool

Ip ranges

https://raw.githubusercontent.com/lord-alfred/ipranges/main/all/ipv4_merged.txt

CloudRecon scrape -i ipv_merged.txt | grep 'target.com'

Medium Scope

Cloudrecon

https://github.com/g0ldencybersec/CloudRecon

Tool

Ip ranges

https://raw.githubusercontent.com/lord-alfred/ipranges/main/all/ipv4_merged.txt

CloudRecon scrape -i ipv_merged.txt | grep 'target.com'

CIDR Ranges

https://whois.arin.net/ui/query.do

prips 23.228.128.0/18 | certinfo | jq -r '.Certificate_Subject_Alternative_Name // empty | .[]'

and

prips 23.228.128.0/18 | hakip2host | awk '{print $3}' | tee -a hakip2host-output.txt

Medium Scope

CIDR Ranges

https://whois.arin.net/ui/query.do

prips 23.228.128.0/18 | certinfo | jq -r '.Certificate_Subject_Alternative_Name // empty | .[]'

and

prips 23.228.128.0/18 | hakip2host | awk '{print $3}' | tee -a hakip2host-output.txt

Medium Scope

Subdomain Analytics Enumeration

analyticsrelationships

Port Scanning & Probing

- naabu
- masscan
- rustscan
- nmap

naabu

cat subs.txt | naabu -duc -silent -o naabu.txt

(top 1000 or 65365)

Subdomain Probing

httpx

httpx

cat naabu.txt | httpx -silent -duc -nc -nf -title -ct -sc -cl -o httpx.txt

Medium Scope

httpx

dlevel

dlevel

sort subdomains high level to bottom level, this way you can avoid duplicate if do google dorking and fuzzing like this, because not many people touch high level subdomain

https://github.com/rix4uni/dlevel

Subdomain Bruteforcing

ffuf

Screenshotting

- gowitness
- aquatone
- EyeWitness
- httpx

gowitness

cat httpx.txt | awk '{print $1}' | unew -el -i -t -q only_httpx_urls.txt && time cat only_httpx_urls.txt | gowitness file -f - --fullpage --timeout 30 --threads 4 --screenshot-db-store

don't use nuclei of httpx for screenshotting, i see big difference

I see screenshot on same input

gowitness: 19

```
cat httpx.txt | awk '{print $1}' | unew -el -i -t -q only_httpx_urls.txt && time cat only_httpx_urls.txt | gowitness file -f - --fullpage --timeout 30 --threads 4 --screenshot-db-store
```

don't use nuclei of httpx for screenshotting, i see big difference

I see screenshot on same input
gowitness: 19
nuclei: 11
httpx: 2

Directory Enumeration

- ffuf
- dirsearch
- feroxbuster
- wfuzz

ffuf

ffuf -c -u https://example.com/FUZZ -w onelistforallshort.txt

https://github.com/dwyl/english-words/blob/master/words.txt
ffuf -c -u https://example.com/FUZZ.zip -w words.txt -mc 200,302
ffuf -c -u https://example.com/FUZZ.php -w words.txt -mc 200,302

default fuzzing 403, 404 domains

ffuf

ffuf -c -u https://example.com/FUZZ -w onelistforallshort.txt

https://github.com/dwyl/english-words/blob/master/words.txt
ffuf -c -u https://example.com/FUZZ.zip -w words.txt -mc 200,302
ffuf -c -u https://example.com/FUZZ.php -w words.txt -mc 200,302

default fuzzing 403, 404 domains

ffuf

ffufPostprocessing

Email Enumeration

- emailfinder
- LeakSearch

Url Crawling

- waymore
- hakrawler
- waybackurls
- gau
- katana

Url Crawling

- katana
- gospider
- uforall
- github-endpoints
- crawley

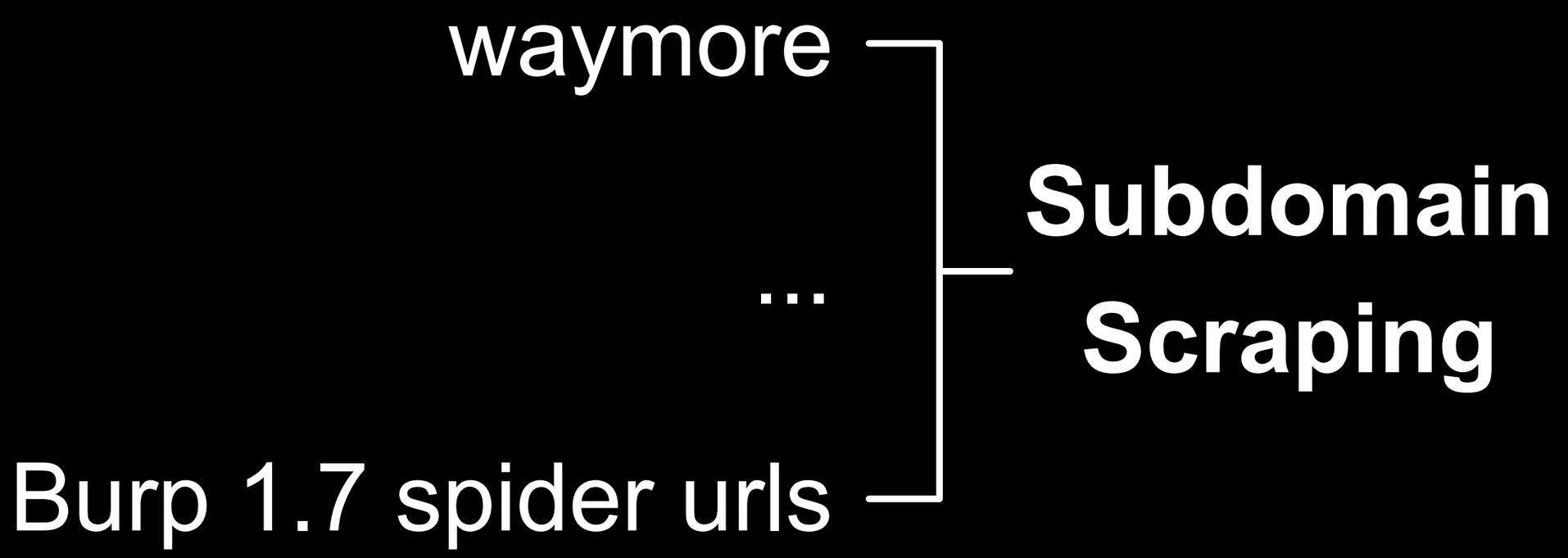
Url Crawling

- galer
- roboxtractor
- urlgrab
- GoLinkFinder
- cariddi

Url Crawling

- urlgrab
- GoLinkFinder
- cariddi
- Burp 1.7 spider urls

Medium Scope



Subdomain Scraping

```
cat urls.txt | cut -d"/" -f1-3 | unew subs.txt | tee scrape-subs.txt
```

Google Dorking

- Automated
- Manual

Automated

- xnldorker
- uDork
- GooFuzz
- dorks_hunter
- go-dork

Automated

- xnldorker
- uDork
- GooFuzz
- dorks_hunter
- go-dork

Manual

- https://pentestingdorks.netlify.app/google/
- BulkURLOpener
- Bulk URL Opener Extension

JS Crawling

- subjs
- getJS
- jscrawler
- linkfinder
- xnLinkFinder

JS Crawling

- xnLinkFinder
- getjswords
- gowitness
- sourcemapper
- linx

JS Crawling

- sourcemapper
- linx
- other tools
- js moniter

gowitness

collect js links in gowitness network logs, gives exta links because it's DOM based data

sourcemapper

sourcemapper -insecure -output sourcemapper -url https://www.cga.ct.gov/aspx/cgabilltracking/pub/Scripts/js/pdfmake.min.js.map

interlace -tL js_links.txt -threads 10 -c "sourcemapper -insecure -url _target_ -output _output_/_cleantarget_" -o .tmp/sourcemapper

Hidden Parameter

- paramfinder
- msarjun (arjun)
- x8

Medium Scope

Program Based Wordlist Generator

- cewl
- unfurl
- cook
- Password Dictionary Generation

cewl

cewl -d 2 -m 5 https://example.com | sed '1d'

interlace -tL httpx.txt -threads 100 -c "proxychains cewl -d 2 -m 5 _target_ | sed '1d' | unew -q _output_/_cleantarget_.txt" -o cewlwordlist &>/dev/null

Password Dictionary Generation

pydictor

Github Dorking

- gitrepoenum
- gitrob
- gitleaks
- trufflehog
- code-review

Github Dorking

- gitleaks
- trufflehog
- code-review
- gitdorks_go

403/401 bypass

These tools only can bypass 403 endpoints not 403 domain

403/401 bypass

- byp4xx
- 4-ZERO-3
- 403jump
- BypassFuzzer
- nomore403

403/401 bypass

- bypass

- 4-ZERO-3
- 403jump
- BypassFuzzer
- nomore403

Favicon Lookup

- favinfo
- favirecon

Internet Search Engine Dis...

- uncover
- karma_v2
- shodan

Misconfigured Cloud Storage

S3 buckets

S3 buckets

S3Scanner

Testing TLS/SSL encryption

testssl.sh

Vulnerability Scanning

- Subdomain Takeover
- MX Takeover
- DNS takeover
- Zone Transfer
- ftpx

Vulnerability Scanning

- ftpx
- SSHBruteForce
- vulntechx
- XSS
- SQLI

Vulnerability Scanning

- LFI
- RCE
- AEM
- Grafana
- Jenkins

Vulnerability Scanning

- Jenkins
- JIRA
- Swagger UI
- Symfony
- PHPMYADMIN

Vulnerability Scanning

- Dependency Confusion
- Dot Git
- Hardcoded Information in JavaScript (nuclei exposures template)
- IIS Windows Server

Vulnerability Scanning

- IIS Windows Server
- fuzzuli
- Sensitive PDFs
- Prototype Pollution
- HTTP Request Smuggling

Vulnerability Scanning

- Web Cache Poisoning
- URLs Secrets
- Password Spraying
- JS secrets

Subdomain Takeover

- subjack
- subzy
- tko-subs
- subsnipe
- nuclei

Subdomain Takeover

- subjack
- subzy
- tko-subs
- subsnipe
- nuclei

Medium Scope

nuclei

nuclei -tags takeover

MX Takeover

mxtakeover

Medium Scope

DNS takeover

dnstake

Zone Transfer

dig

XSS

- Reflected XSS
- Blind XSS
- DOM XSS

Reflected XSS

- xsschecker
- knoxnl
- dalfox
- XSpear

xsschecker

pyxss

knoxnl

knoxnl uses knoxss api

Blind XSS

- ezxss
- xss.report

Medium Scope

DOM XSS

domscan

SQLI

- Error Based SQLI
- Blind Time Based SQLI

Medium Scope

Error Based SQLI

nuclei template

Blind Time Based SQLI

gosqli

gosqli

- ghauri
- sqlmap

LFI

nuclei template

RCE

nuclei template

Dot Git

goop

IIS Windows Server

Collect iis domains in "Technology Fingerprinting" and "httpx"

cat techx-output.txt httpx.txt | unew -q iis_sites.txt

interlace -tL iis_sites.txt -threads 100 -c "shortscan _target_ -F -s -p 1 > _output_/_cleantarget_.txt" -o ~/iis &>/dev/null

find ~/iis -type f -print0 | xargs --null grep -Z -L 'Vulnerable: Yes' | xargs --null rm

Medium Scope

IIS Windows Server

Collect iis domains in "Technology Fingerprinting" and "httpx"

cat techx-output.txt httpx.txt | unew -q iis_sites.txt

interlace -tL iis_sites.txt -threads 100 -c "shortscan _target_ -F -s -p 1 > _output_/_cleantarget_.txt" -o ~/iis &>/dev/null

find ~/iis -type f -print0 | xargs --null grep -Z -L 'Vulnerable: Yes' | xargs --null rm

Sensitive PDFs

pdftotext

pdftotext

https://ott3rly.com/mass-hunting-for-leaked-sensitive-documents/

interlace -tL urls.txt -threads 10 -c "curl -s _target_ | pdftotext - _output_/_cleantarget_.txt" 2>/dev/null" -o ~/pdf &>/dev/null

find ~/pdf -type f -print0 | xargs --null grep -Z -L -Eai 'internal use only|confidential' | xargs --null rm

pdftotext

https://ott3rly.com/mass-hunting-for-leaked-sensitive-documents/

interlace -tL urls.txt -threads 10 -c "curl -s _target_ | pdftotext - _output_/_cleantarget_.txt" 2>/dev/null" -o ~/pdf &>/dev/null

find ~/pdf -type f -print0 | xargs --null grep -Z -L -Eai 'internal use only|confidential' | xargs --null rm

Prototype Pollution

ppmap

Medium Scope

HTTP Request Smuggling

smuggler

Web Cache Poisoning

Web-Cache-Vulnerability-Scanner

URLs Secrets

- linkinspector
- back-me-up

Password Spraying

brutespray

JS secrets

- nuceli exposures
- trufflehog
- secretfinder
- mantra

Large Scope

Large Scope

Everything related to the Organization is a part of Scope. This includes child companies, subdomains or any labelled asset owned by organization.

Everything related to the Organization is a...

Recon To-Do

Recon To-Do

- Tracking & Tracing every possible signatures of the Target Application (Often there might not be any history on Google related to a scope target, but you can still crawl it.)
- Subsidiary & Acquisition Enumeration (Depth – Max)
- Reverse Lookup
- ASN & IP Space Enumeration and Service Identification

Recon To-Do

- ASN
- Acquistions
- Google Dorking to find Acquistions
- Cloud Recon
- Certificate Transperency

Recon To-Do

- Certificate Transperency
- Ad and Analytics
- Subdomain Enumeration
- Subdomain Takeover
- Probing & Technology Fingerprinting
- Port Scanning

Recon To-Do

- Port Scanning
- Known Vulnerabilities
- Template Based Scanning (Nuclei/Jeales)
- Broken Link Hijacking
- Directory Enumeration
- Hardcoded Information in JavaScript

Recon To-Do

- Hardcoded Information in JavaScript
- GitHub Reconnaissance
- Google Dorking
- Data Breach Analysis
- Parameter Fuzzing
- Internet Search Engine Discovery (Shodan, Censys, Spyse, etc.)

Recon To-Do

- Internet Search Engine Discovery (Shodan, Censys, Spyse, etc.)
- IP Range Enumeration (If in Scope)
- Wayback History
- Potential Pattern Extraction with GF and automating further for XSS, SSRF, etc.
- Heartbleed Scanning

Recon To-Do

SSRF, etc.

- Heartbleed Scanning
- General Security Misconfiguration Scanning
- And any possible Recon Vector (Network/Web) can be applied.
- code-review

ASN

- asnlookup
- metabigor
- org2asn

Acquistions

- crunchbase
- wikipedia
- https://www.startupranking.com/startup/google/acquisitions
- aleph.occrp.org

crunchbase

https://pentestingdorks.netlify.app/crunchbase

```
site:crunchbase.com google acquisitions
```

```
cat tmp.txt | grep -E "https://www.crunchbase.com/organization/|https://www.crunchbase.com/acquisition/" | sed 's/acquisition/organization/' | sed 's|.*/\(.*\)-acquires-\(.*\)--.*|https://www.crunchbase.com/organization/\2|'
```

wikipedia

site:wikipedia.org google acquisitions

aleph.occrp.org

https://aleph.occrp.org/entities/7b7d09a2d8dc6ba480655a79953630f61331cf60.da69c7367a0c0d85c10efa72076cb762c2884eda

Google Dorking to find Ac...

- Trademark
- Twitter
- Apex Domains
- TLD
- ORG Name / Subsidiaries

Google Dorking to find Ac...

- TLD
- ORG Name / Subsidiaries
- Wildcard Domains
- Favicon

Trademark

- intext:"Copyright © 2024 Google LLC"
- intext:"Copyright © 2024 google"
- intext:"2024 Google LLC"
- intext:"Google LLC. All rights reserved."

change different year also like 2023, 2022

Twitter

https://twitter.com/search?q=google&src=typed_query&f=user

this will give Appex Domains and TLD

Apex Domains

- intext:"2024 google"
- site:google

change different year also like 2023, 2022

TLD

- site:*.google.* -site:google.com
- site:*.*.google -site:google.com
- site:google.*
- intext:@google.com
- intext:@google
- curl -s "https://crt.sh/?q=google&output=json" | jq -r '.[].common_name' | grep "*" | unew -p

TLD

- site:*.google.* -site:google.com
- site:*.*.google -site:google.com
- site:google.*
- intext:@google.com
- intext:@google
- curl -s "https://crt.sh/?q=google&output=json" | jq -r '.[].common_name' | grep "*" | unew -p

TLD

tldscan

tldscan

bash tldscan -q google

ORG Name / Subsidiaries

```
curl -s 'https://www.google.com/search?
q=Google+Inc.+subsidiaries&sourceid=chrome&ie=UTF-8' -H 'user-agent:
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/53
7.36 (KHTML, like Gecko) Chrome/128.0.0.0 Safari/537.36' | grep -oP 'role="tab"
title="\K[^"]+' | unew
```

Wildcard Domains

Do with all apex domains like this with 10 *.

site:*.withgoogle.com
site:*.*.withgoogle.com
site:*.mandiant.com
site:*.*.mandiant.com

Favicon

- FOFA
- FavFreak

Cloud Recon

- Cloudrecon
- http://kaeferjaeger.gay
- CIDR Ranges

Cloudrecon

https://github.com/g0ldencybersec/CloudRecon

Tool

Ip ranges

https://raw.githubusercontent.com/lord-alfred/ipranges/main/all/ipv4_merged.txt

CloudRecon scrape -i ipv4_merged.txt | grep 'target.com'

Large Scope

Cloudrecon

https://github.com/g0ldencybersec/CloudRecon

Tool

Ip ranges

https://raw.githubusercontent.com/lord-alfred/ipranges/main/all/ipv4_merged.txt

CloudRecon scrape -i ipv_merged.txt | grep 'target.com'

CIDR Ranges

https://whois.arin.net/ui/query.do

prips 23.228.128.0/18 | certinfo | jq -r '.Certificate_Subject_Alternative_Name // empty | .[]'

and

prips 23.228.128.0/18 | hakip2host | awk '{print $3}' | tee -a hakip2host-output.txt

CIDR Ranges

https://whois.arin.net/ui/query.do

prips 23.228.128.0/18 | certinfo | jq -r '.Certificate_Subject_Alternative_Name // empty | .[]'

and

prips 23.228.128.0/18 | hakip2host | awk '{print $3}' | tee -a hakip2host-output.txt

Certificate Transperency

- certinfo
- rcert
- cero

rcert

bash rcert.sh google.com

or

bash rcert.sh domains.txt

Ad and Analytics

Builtwith

Builtwith

Firefox Extension:
https://addons.mozilla.org/en-US/firefox/addon/builtwith

Chrome Extension:
https://chromewebstore.google.com/detail/builtwith-technology-prof/dapjbgnjinbpoindlpdmhochffioedbn?hl=en&pli=1

Using CLI tool:
python3 getrelationship.py apigee.com

Large Scope

Firefox Extension:
https://addons.mozilla.org/en-US/firefox/addon/builtwith

Chrome Extension:
https://chromewebstore.google.com/detail/builtwith-technology-prof/dapjbgnjinbpoindlpdmhochffioedbn?hl=en&pli=1

Using CLI tool:
python3 getrelationship.py apigee.com FgMABMLf4RoJrjFXjTBT1/13WHxgNxUwCJmvd0Urq2gzhAVVXcQBcVTITfkZXcqVoyhEbYgRK+mQLAAJ5vej8jGtt0f0lzFtQ1N/gy9qDXU= | tee -a output.txt

Thank you