Questo sito utilizza cookie di Google per erogare i propri servizi e per analizzare il traffico. Il tuo indirizzo IP e il tuo user agent sono condivisi con Google, unitamente alle metriche sulle prestazioni e sulla sicurezza, per garantire la qualità del servizio, generare statistiche di utilizzo e rilevare e contrastare eventuali abusi.

ULTERIORI INFORMAZIONI OK

Reconftw - Simple Script For Full Recon

9 MONTHS AGO 5:30 PM | POST SPONSORED BY FARADAYSEC | MULTIUSER PENTEST ENVIRONMENT

ZION3R

This is a simple script intended to perform a full recon on an objective with multiple subdomains

tl;dr

- Requires Go
- Run ./install.sh before first run (apt, rpm, pacman compatible)

```
r00t@r00t-KitPloit: ~
git clone https://github.com/six2dez/reconftw
cd reconftw
chmod +x *.sh
./install.sh
./reconftw.sh -d target.com -a
```

Features

- Tools checker
- Google Dorks (based on deggogle_hunter)
- Subdomain enumeration (passive, resolution, bruteforce and permutations)
- Sub TKO (subjack and nuclei)
- Web Prober (httpx)
- Web screenshot (aquatone)
- Template scanner (nuclei)

FOLLOW US!

Your Email

Subscribe to our Newsletter

POPULAR

FUSE - A Penetration Testing Tool For Finding File Upload Bugs

FUSE is a penetration testing system designed to identify Unrestricted Executable File Upload (UEFU) vulnerabilities. The details of the...

SharpML - Machine Learning Network Share Password Hunting Toolkit

SharpML is a proof of concept file share data mining tool using Machine Learning in Python and C#. The tool is discussed in more detai...

Qu1cksc0pe - All-in-One Static Malware Analysis Tool

This tool allows you to statically analyze Windows, Linux, OSX executables and APK files. You can get : What DLL files are used. Functio...

PowerShx - Run Powershell Without Software Restrictions

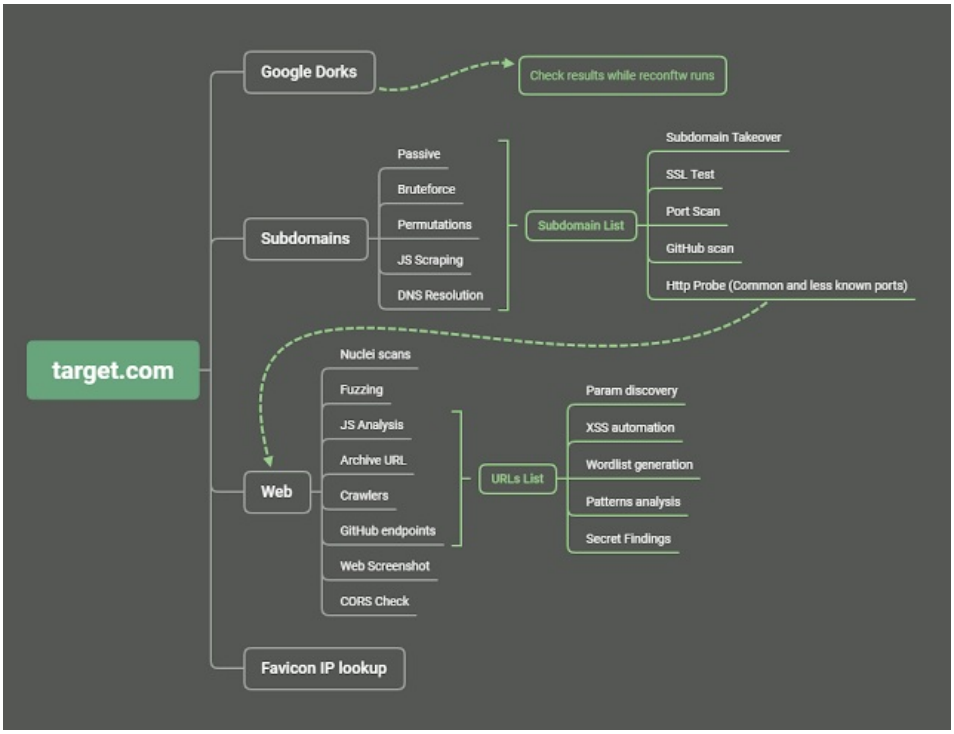
Unmanaged PowerShell execution using DLLs or a standalone executable. Introduction PowerShx is a rewrite and expansion on the PowerSh...

Rdesktop - Open Source Client for Microsoft's RDP protocol

rdesktop is an open source client for Microsoft's RDP protocol. It is known to work with Windows versions ranging from NT 4 Terminal...

- Port Scanner (naabu)
- Url extraction (waybackurls, gau, hakrawler, github-endpoints)
- Pattern Search (gf and gf-patterns)
- Param discovery (paramspider and arjun)
- XSS (Gxss and dalfox)
- Github Check (git-hound)
- Favicon Real IP (fav-up)
- JS Checks (LinkFinder, SecretFinder, scripts from JSFScan)
- Fuzzing (ffuf)
- Cors (Corsy)
- SSL Check (testssl)
- Interlace integration
- Custom output folder (default under Recon/target.com/)
- Run standalone steps (subdomains, subtko, web, gdorks...)
- Polished installer compatible with most distros

Mindmap/Workflow



Requirements

- Golang > 1.14 installed and env vars correctly set ($GOPATH,$GOROOT)
- Run ./install.sh

> *Installer is provided as is. Nobody knows your system better than you, so nobody can debug your system better than you. If you are experiencing some issues with the installer script I can help you out, but keep in mind that is not my main priority.*

- It is highly recommended, and in some cases essential, set your api keys:
  - amass (~/.config/amass/config.ini)
  - subfinder (~/.config/subfinder/config.yaml)
  - git-hound (~/.githound/config.yml)
  - github-endpoints.py (GITHUB_TOKEN env var)
  - favup (shodan init SHODANPAIDAPIKEY)
- This script uses dalfox with blind-xss option, you must change to your own server, check xsshunter.com.

Usage examples

Full scan:

```
r00t@r00t-KitPloit: ~
./reconftw.sh -d target.com -a
```

Subdomains scan:

```
r00t@r00t-KitPloit: ~
./reconftw.sh -d target.com -s
```

Web scan (target list required):

```
r00t@r00t-KitPloit: ~
./reconftw.sh -d target.com -l targets.txt -w
```

Dorks:

```
r00t@r00t-KitPloit: ~
./reconftw.sh -d target.com -g
```

Improvement plan:

- Notification support (Slack, Discord and Telegram)
- CMS tools (wpscan, drupwn/droopescan, joomscan)
- Add menu option for every feature
- Any other interesting suggestion
- Open Redirect with Oralyzer
- Enhance this Readme
- Customize output folder
- Interlace usage
- Crawler
- SubDomainizer
- Install script
- Apt,rpm,pacman compatible installer

Thanks

For their great feedback, support, help or for nothing special but well deserved:

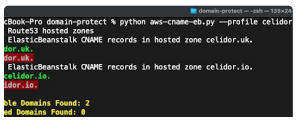
- @detonXX
- @cyph3r_asr
- @h4ms1k

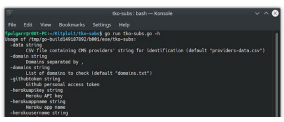
Download Reconftw

TAGS

BRUTEFORCE X BUGBOUNTY X DALFOX X DORKS X ENUMERATION X OPEN REDIRECT X RECONFTW X SCANNER X SUBDOMAIN

Facebook





Domain-Protect - Protect Against Subdomain Takeover

Wordlistgen - Quickly Generate Context-Specific Wordlists For Content Discovery From Lists Of URLs Or Paths

Tko-Subs - A Tool That Can Help Detect And Takeover Subdomains With Dead DNS Records

PREVIOUS

MobileHackersWeapons - Mobile Hacker's Weapons / A Collection Of Cool Tools Used By Mobile Hackers

NEXT

CDK - Zero Dependency Container Penetration Toolkit

POST COMMENT FACEBOOK DISQUS

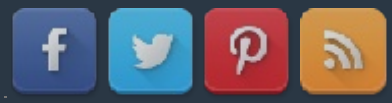
BLOG ARCHIVE

Blog Archive

RECOMMENDED

1. SSD cloud server on DigitalOcean
2. Exploit Collector
3. BlackPloit
4. Hacking Reviews
5. Hacking Land

SOCIAL



Your Email

Subscribe to our Newsletter

BY FEEDBURNER