Automating the recon process... FTW!

> whoami

- six2dez

> uname -a

- Alexis Fernández
- Madrid, Spain
- Pentester & Bug Hunter SynAck RT
- pentestbook.six2dez.com
- reconFTW

> startx

> which recon

Definición y Objetivos

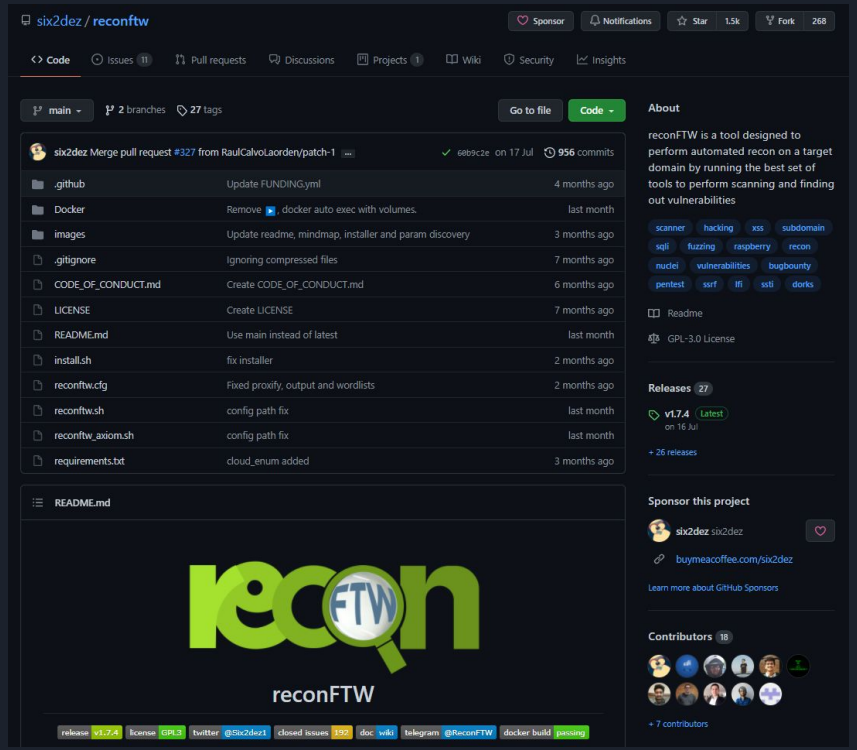
Fase de recopilación de información previa al ataque.

- Recolectar información útil
- Ampliar superficie de ataque
- Descubrir vectores de explotación
- Filtrar resultados potencialmente vulnerables
- Eliminar ruido de la superficie expuesta
- Almacenar toda la información recolectada
- Ahorrar tiempo

> git clone reconftw

reconFTW info

- Bash + 2500 líneas
- 1,5K GitHub
- Casi 1000 commits
- Casi 200 issues cerrados
- 143 PR
- 1er commit 7 Enero 2021
- +50 herramientas integradas



https://github.com/six2dez/reconftw

Principales fases

- OSINT
- Subdominios
- IP/Host
- Webs
- Urls

OSINT

- Información del target (whois, registrants, etc)
- Dorking
- Emails & leaks
- Usuarios y/o empleados
- Metadatos en documentos indexados

SUBDOMINIOS

- Pasivos (SecurityTrails, PassiveRecon, Censys, etc...) + resolución DNS
- Transparencia de certificados
- Fuerza Bruta + Permutaciones
- Registros DNS
- Crawling + JS
- Analytics IDs
- Recursividad
- Transferencias de zona
- Takeovers

HOSTS

- Pertenencia CDN/WAF
- Escaneo de puertos pasivo y activo
- Searchsploit
- Password Spraying
- Detección proveedor Cloud

WEB

- Web probing de subdominios + puertos inusuales
- Web screenshot
- Detección de WAF
- Nuclei
- Fuzzing
- Detección CMS
- Análisis JS
- CORS
- Extracción urls (pasiva y activa)
- Robots wayback

URLs

- Generación de Wordlists
- Urls por extensión
- Análisis por patrones
- Múltiples ataques automatizados
  - XSS
  - SQLi
  - SSRF
  - LFI
  - etc...

Extras

- Instalador/Actualizador
- Fichero de configuración
- Notificaciones vía Slack, Discord o Telegram
- Múltiples modos
- Carga de trabajo distribuida
- Interfaz web, API y BD
- Pull Request bienvenidos :)

Agradecimientos

Mindmap

Demo instalación

Demo configuración

Demo ejecución normal

Demo ejecución distribuida

Demo visualización bbrf

> help

Referencias y repos

Dorks
https://github.com/six2dez/degoogle_hunter
https://github.com/obheda12/GitDorker

Favicon
https://github.com/pielco11/fav-up

Subdominios
https://github.com/projectdiscovery/subfinder
https://github.com/tomnomnom/assetfinder
https://github.com/OWASP/Amass
https://github.com/Findomain/Findomain
https://github.com/cgboal/sonarsearch
https://github.com/tomnomnom/waybackurls
https://github.com/eslam3kl/crtfinder
https://tls.bufferover.run/dns?q=.whatever.com
https://dns.bufferover.run/dns?q=.whatever.com
https://github.com/projectdiscovery/shuffledns
https://github.com/ProjectAnte/dnsgen
https://github.com/hakluke/hakrawler
https://github.com/projectdiscovery/dnsx

Puertos y resolución web
https://github.com/nmap/nmap
https://github.com/projectdiscovery/httpx
https://github.com/drwetter/testssl.sh
https://github.com/projectdiscovery/nuclei
https://github.com/projectdiscovery/nuclei-templates
https://cli.shodan.io/
https://github.com/dwisiswant0/cf-check

Análisis Web
https://github.com/maaaaz/webscreenshot
https://github.com/ffuf/ffuf
https://github.com/Tuhinshubhra/CMSeeK
https://gist.githubusercontent.com/KathanP19
https://github.com/m4ll0k/Bug-Bounty-Toolz
https://github.com/lc/gau
https://github.com/gwen001/github-endpoints
https://github.com/s0md3v/Corsy

Análisis URLs
https://github.com/devanshbatham/ParamSpider
https://github.com/s0md3v/Arjun
https://github.com/m4ll0k/SecretFinder/blob/master/SecretFinder.py
https://github.com/tomnomnom/gf
https://github.com/1ndianl33t/Gf-Patterns
https://github.com/tomnomnom/unfurl
https://github.com/tomnomnom/qsreplace
https://github.com/s0md3v/XSStrike
https://gist.github.com/h4ms1k/adcc340495d418fcd72ec727a116fea2
https://github.com/devanshbatham/OpenRedireX
https://github.com/dwisiswant0/crlfuzz
https://github.com/sqlmapproject/sqlmap

Wordlists / Diccionarios
https://github.com/six2dez/OneListForAll/blob/main/onelistforallmicro.txt
https://raw.githubusercontent.com/xmendez/wfuzz/master/wordlist/vulns/dirTraversal-nix.txt
https://gist.githubusercontent.com/six2dez/ffc2b14d283e8f8eff6ac83e20a3c4b4/raw/137bb6b60c616552c705e93a345c06cec3a2cb1f/permutations_list.txt
https://raw.githubusercontent.com/BBerastegui/fresh-dns-servers/master/resolvers.txt
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/DNS/sortedcombined-knock-dnsrecon-fierce-reconng.txt
https://gist.githubusercontent.com/jhaddix/86a06c5dc309d08580a018c66354a056/raw/96f4e51d96b2203f19f6381c8c545b278eaa0837/all.txt

> shutdown now