



EuskalHack Security Congress VI





ReconFTW: a framework...



> WHOAMI?

- Padre
- Bash lover
- Open source dev
- [@six2dez / \[@six2dez1\]\(https://twitter.com/six2dez1\)](https://twitter.com/six2dez)
- Red Teamer en [Visma](#)
- pentestbook.six2dez.com
- Bug bounty hunter & pentester
- Speaker en Disobey, H-cOn, BitUp, DragonJarCOn, HacktivityCon...





ReconFTW: a framework...



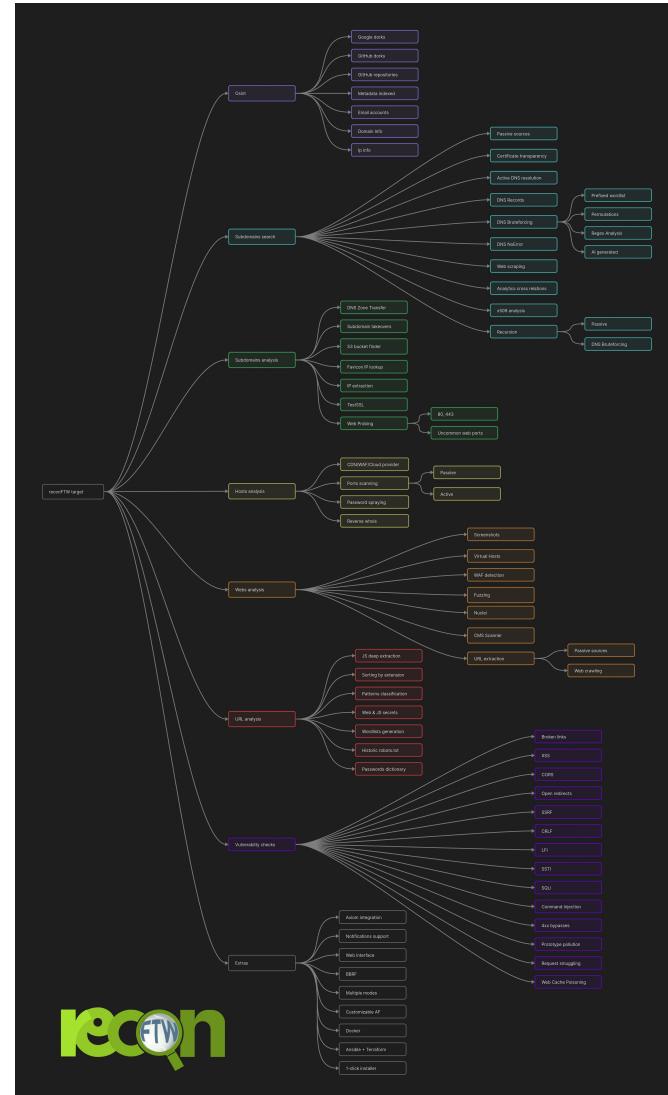


ReconFTW: a framework...



> QUÉ ES RECONFTW?

- **Framework de reconocimiento**
 - **Flujo de trabajo fijo pero muy configurable**
 - **Basado en herramientas FOSS**
 - **Inspirado en metodología @jhaddix [TBHM](#)**
 - **En constante actualización y cambio**
 - **Adaptable a diferentes entornos y requisitos**





ReconFTW: a framework...



> QUÉ ES RECONFTW?

```
~/Tools/reconftw | on dev !1
./reconftw.sh

RECONFTW
by @six2dez

dev-v2.6-80-g145164c

Usage: ./reconftw.sh [-d domain.tld] [-m name] [-l list.txt] [-x oos.txt] [-i in.txt]
                   [-r] [-s] [-p] [-a] [-w] [-n] [-i] [-h] [-f] [--deep] [-o OUTPUT]

TARGET OPTIONS
-d domain.tld      Target domain
-m company          Target company name
-l list.txt         Targets list (One on each line)
-x oos.txt          Exclude subdomains list (Out Of Scope)
-i in.txt           Include subdomains list

MODE OPTIONS
-r, --recon        Recon - Perform full recon process (without attacks)
-s, --subdomains   Subdomains - Perform Subdomain Enumeration, Web probing and check for sub-tko
-p, --passive       Passive - Perform only passive steps
-a, --all           All - Perform all checks and active exploitations
-w, --web           Web - Perform web checks from list of subdomains
-n, --osint          OSINT - Check for public intel data
-c                 Launches specific function against target
-h                 Help - Show help section
```

- +4K ★
- + 700 forks
- 1,6K commits
- +300 issues
- + 45 releases
- +2K clones/semana
- +8K visitantes/semana
- +75 herramientas
- 7 modos distintos
- 3 tipos de inputs
- Instalador
- Licencia MIT



ReconFTW: a framework...



> OBJETIVOS Y NECESIDADES

- Proyecto personal
- Entornos pentesting, BB o RT
- AutomatizaFTW
- Técnicas actualizadas
- Output listo para analizar
- Escalable
- Proyecto vivo
- Contribución a la comunidad
- Mejorar el panorama de recon





ReconFTW: a framework...



Jason Haddix

A lot of people ask me about recon.sh, my homegrown hunting script.

Just use reconFTW by [@Six2dez1](#) it's vastly su
#bugbountytips

[Traducir Tweet](#)

Snifer@L4b's Acerca de Archivo Recomendaciones Biblioteca

[Snifer@L4b's / Posts / Automatiza las tareas de Reconocimiento Web con ReconFTW](#)

Automatiza las tareas de Reconocimiento Web con ReconFTW Labs About us

Jan 27, 2022 · Jan 29, 2022 · 4 min read · Autor - Snifer #Docker

> What's on this Page

La herramienta que veremos en esta entrada corresponde a automatizada.

Herramientas ReconFTW

reconftw A collection of 3 posts

reconftw Reconnaissance like a cyber scout - Part 3. Final. The final part of the reconnaissance like a cyber scout series. Feb 21, 2023 · 5 min read

reconftw Reconnaissance like a cyber scout - Part 2. Salutations fellas! I'm back for the second part of our series on perimeter reconnaissance.... Feb 8, 2023 · 23 min read

reconftw Reconnaissance like a cyber scout - Part 1. Greetings dear readers, how are you? May the god of hacking be present in your lives! All kidding... Jan 26, 2023 · 6 min read

STÖK @stokfredrik · 14 may. 2021

Lol. got my ip banned again, def need to distribute my **reconftw** scans with axiom and smash my nmaps using unimap .. Oh and here's a fresh **#bountythursdays** video for you! Good times!

[youtu.be/w0AMcX0odOI](#)

#C4PACHT | _secpro

Darkbyte

- Inicio
- Archivo
- Sobre mí
- Colabora

ReconFTW – A swiss Army Knife for Recon and Web Pentesting

By Indrajeet Bhuyan

In the last few articles, I shared about different Burp suite tools and how you can use each tool to your advantage. In this article, we will learn about ReconFTW, a python-based framework which can be used for web pentesting. It has various modules for performing tasks such as port scanning, subdomain enumeration, etc.

28 de febrero de 2021

Automatizando el reconocimiento web con reconFTW

kinomakino @kinomakino · 3 dic. 2021

Conoces **ReconFTW** para enumeración de objetivos?

blogvisionarios.com Reconocimiento De Dominios Con ReconFtw: La ... Nuestro compañero Joaquín Molina nos habla en este artículo del reconocimiento de dominios con...



ReconFTW: a framework...



> INSTALACIÓN

- Script instalación
 - Dependencias de sistema
 - Instalación de herramientas
 - Descarga de archivos
- Docker / DockerHub
- Despliegue Terraform + Ansible
- Uso de API keys
- Archivo de configuración
 - GOPATH
 - Directorio de tools

```
RECONFTW
dev-v2.6-82-gdd119a1
reconFTW installer/updater script
Choose one of the following options:
1. Install/Update ReconFTW (without Web Interface)
2. Install/Update ReconFTW + Install Web Interface
3. Setup Web Interface (User Interaction needed!)
4. Exit
#####
Insert option: 1
#####
This may take time. So, go grab
Running: Looking for new reconFTW
Running: Downloading required files
Running: Double check for installed tools
Running: Performing last configurations
Remember set your api keys:
- amass (~/.config/amass/config.ini)
- subfinder (~/.config/subfinder/provider-config.yaml)
- GitLab (~/.Tools/.gitlab_tokens)
- SSRF Server (COLLAB_SERVER in reconftw.cfg or env var)
- Blind XSS Server (XSS_SERVER in reconftw.cfg or env var)
- notify (~/.config/notify/provider-config.yaml)
- WHOISXML API (WHOISXML_API in reconftw.cfg or env var)
- subgpt_cookies.json (subgpt_cookies.json file, follow instr
Finished!
#####
reconFTW is already up to date!
Running: Installing system packages
Running: Installing/Updating Golang
Running: Installing requirements
Running: Installing Golang tools (40)
inscope installed (1/40)
hakip2host installed (2/40)
puredns installed (3/40)
interactsh-client installed (4/40)
nuclei installed (5/40)
analyticsrelationships installed (6/40)
crt installed (7/40)
ghauri installed (18/31)
cloud_enum installed (19/31)
testssl installed (20/31)
Web-Cache-Vulnerability-Scanner installed (21/31)
Oralyzer installed (22/31)
fav-up installed (23/31)
massdns installed (24/31)
xlinkFinder installed (25/31)
gf installed (26/31)
commix installed (27/31)
urless installed (28/31)
pwndb installed (29/31)
interlace installed (30/31)
GF-Patterns installed (31/31)
Running: Looking for new reconFTW
Running: Double check for installed tools
Running: Performing last configurations
Remember set your api keys:
- amass (~/.config/amass/config.ini)
- subfinder (~/.config/subfinder/provider-config.yaml)
- GitLab (~/.Tools/.gitlab_tokens)
- SSRF Server (COLLAB_SERVER in reconftw.cfg or env var)
- Blind XSS Server (XSS_SERVER in reconftw.cfg or env var)
- notify (~/.config/notify/provider-config.yaml)
- WHOISXML API (WHOISXML_API in reconftw.cfg or env var)
- subgpt_cookies.json (subgpt_cookies.json file, follow instr
Finished!
#####
reconFTW is already up to date!
Running: Installing system packages
Running: Installing/Updating Golang
Running: Installing requirements
Running: Installing Golang tools (40)
inscope installed (1/40)
hakip2host installed (2/40)
puredns installed (3/40)
interactsh-client installed (4/40)
nuclei installed (5/40)
analyticsrelationships installed (6/40)
crt installed (7/40)
ghauri installed (18/31)
cloud_enum installed (19/31)
testssl installed (20/31)
Web-Cache-Vulnerability-Scanner installed (21/31)
Oralyzer installed (22/31)
fav-up installed (23/31)
massdns installed (24/31)
xlinkFinder installed (25/31)
gf installed (26/31)
commix installed (27/31)
urless installed (28/31)
pwndb installed (29/31)
interlace installed (30/31)
GF-Patterns installed (31/31)
Running: Looking for new reconFTW
Running: Double check for installed tools
Running: Performing last configurations
Remember set your api keys:
- amass (~/.config/amass/config.ini)
- subfinder (~/.config/subfinder/provider-config.yaml)
- GitLab (~/.Tools/.gitlab_tokens)
- SSRF Server (COLLAB_SERVER in reconftw.cfg or env var)
- Blind XSS Server (XSS_SERVER in reconftw.cfg or env var)
- notify (~/.config/notify/provider-config.yaml)
- WHOISXML API (WHOISXML_API in reconftw.cfg or env var)
- subgpt_cookies.json (subgpt_cookies.json file, follow instr
Finished!
#####
reconFTW is already up to date!
Running: Installing system packages
Running: Installing/Updating Golang
Running: Installing requirements
Running: Installing Golang tools (40)
inscope installed (1/40)
hakip2host installed (2/40)
puredns installed (3/40)
interactsh-client installed (4/40)
nuclei installed (5/40)
analyticsrelationships installed (6/40)
crt installed (7/40)
ghauri installed (18/31)
cloud_enum installed (19/31)
testssl installed (20/31)
Web-Cache-Vulnerability-Scanner installed (21/31)
Oralyzer installed (22/31)
fav-up installed (23/31)
massdns installed (24/31)
xlinkFinder installed (25/31)
gf installed (26/31)
commix installed (27/31)
urless installed (28/31)
pwndb installed (29/31)
interlace installed (30/31)
GF-Patterns installed (31/31)
Running: Looking for new reconFTW
Running: Double check for installed tools
Running: Performing last configurations
Remember set your api keys:
- amass (~/.config/amass/config.ini)
- subfinder (~/.config/subfinder/provider-config.yaml)
- GitLab (~/.Tools/.gitlab_tokens)
- SSRF Server (COLLAB_SERVER in reconftw.cfg or env var)
- Blind XSS Server (XSS_SERVER in reconftw.cfg or env var)
- notify (~/.config/notify/provider-config.yaml)
- WHOISXML API (WHOISXML_API in reconftw.cfg or env var)
- subgpt_cookies.json (subgpt_cookies.json file, follow instr
Finished!
#####
reconFTW is already up to date!
Running: Installing system packages
Running: Installing/Updating Golang
Running: Installing requirements
Running: Installing Golang tools (40)
inscope installed (1/40)
hakip2host installed (2/40)
puredns installed (3/40)
interactsh-client installed (4/40)
nuclei installed (5/40)
analyticsrelationships installed (6/40)
crt installed (7/40)
ghauri installed (18/31)
cloud_enum installed (19/31)
testssl installed (20/31)
Web-Cache-Vulnerability-Scanner installed (21/31)
Oralyzer installed (22/31)
fav-up installed (23/31)
massdns installed (24/31)
xlinkFinder installed (25/31)
gf installed (26/31)
commix installed (27/31)
urless installed (28/31)
pwndb installed (29/31)
interlace installed (30/31)
GF-Patterns installed (31/31)
Running: Looking for new reconFTW
Running: Double check for installed tools
Running: Performing last configurations
Remember set your api keys:
- amass (~/.config/amass/config.ini)
- subfinder (~/.config/subfinder/provider-config.yaml)
- GitLab (~/.Tools/.gitlab_tokens)
- SSRF Server (COLLAB_SERVER in reconftw.cfg or env var)
- Blind XSS Server (XSS_SERVER in reconftw.cfg or env var)
- notify (~/.config/notify/provider-config.yaml)
- WHOISXML API (WHOISXML_API in reconftw.cfg or env var)
- subgpt_cookies.json (subgpt_cookies.json file, follow instr
Finished!
#####
reconFTW is already up to date!
Running: Installing system packages
Running: Installing/Updating Golang
Running: Installing requirements
Running: Installing Golang tools (40)
inscope installed (1/40)
hakip2host installed (2/40)
puredns installed (3/40)
interactsh-client installed (4/40)
nuclei installed (5/40)
analyticsrelationships installed (6/40)
crt installed (7/40)
ghauri installed (18/31)
cloud_enum installed (19/31)
testssl installed (20/31)
Web-Cache-Vulnerability-Scanner installed (21/31)
Oralyzer installed (22/31)
fav-up installed (23/31)
massdns installed (24/31)
xlinkFinder installed (25/31)
gf installed (26/31)
commix installed (27/31)
urless installed (28/31)
pwndb installed (29/31)
interlace installed (30/31)
GF-Patterns installed (31/31)
Running: Looking for new reconFTW
Running: Double check for installed tools
Running: Performing last configurations
Remember set your api keys:
- amass (~/.config/amass/config.ini)
- subfinder (~/.config/subfinder/provider-config.yaml)
- GitLab (~/.Tools/.gitlab_tokens)
- SSRF Server (COLLAB_SERVER in reconftw.cfg or env var)
- Blind XSS Server (XSS_SERVER in reconftw.cfg or env var)
- notify (~/.config/notify/provider-config.yaml)
- WHOISXML API (WHOISXML_API in reconftw.cfg or env var)
- subgpt_cookies.json (subgpt_cookies.json file, follow instr
Finished!
#####
reconFTW is already up to date!
Running: Installing system packages
Running: Installing/Updating Golang
Running: Installing requirements
Running: Installing Golang tools (40)
inscope installed (1/40)
hakip2host installed (2/40)
puredns installed (3/40)
interactsh-client installed (4/40)
nuclei installed (5/40)
analyticsrelationships installed (6/40)
crt installed (7/40)
ghauri installed (18/31)
cloud_enum installed (19/31)
testssl installed (20/31)
Web-Cache-Vulnerability-Scanner installed (21/31)
Oralyzer installed (22/31)
fav-up installed (23/31)
massdns installed (24/31)
xlinkFinder installed (25/31)
gf installed (26/31)
commix installed (27/31)
urless installed (28/31)
pwndb installed (29/31)
interlace installed (30/31)
GF-Patterns installed (31/31)
Running: Looking for new reconFTW
Running: Double check for installed tools
Running: Performing last configurations
Remember set your api keys:
- amass (~/.config/amass/config.ini)
- subfinder (~/.config/subfinder/provider-config.yaml)
- GitLab (~/.Tools/.gitlab_tokens)
- SSRF Server (COLLAB_SERVER in reconftw.cfg or env var)
- Blind XSS Server (XSS_SERVER in reconftw.cfg or env var)
- notify (~/.config/notify/provider-config.yaml)
- WHOISXML API (WHOISXML_API in reconftw.cfg or env var)
- subgpt_cookies.json (subgpt_cookies.json file, follow instr
Finished!
```



ReconFTW: a framework...



> MÓDULOS - OSINT

Dominio

- Google Dorks predefinidos
- GitHub Dorks predefinidos
- Análisis de repos de la org
- Metadatos indexados en buscadores
- Emails indexados en buscadores
- Whois info
- IP → Whois reverso
- Dominios del mismo tenant de Azure

IP *

- Relaciones de IP reversas
- Whois reverso
- Geolocalización IP



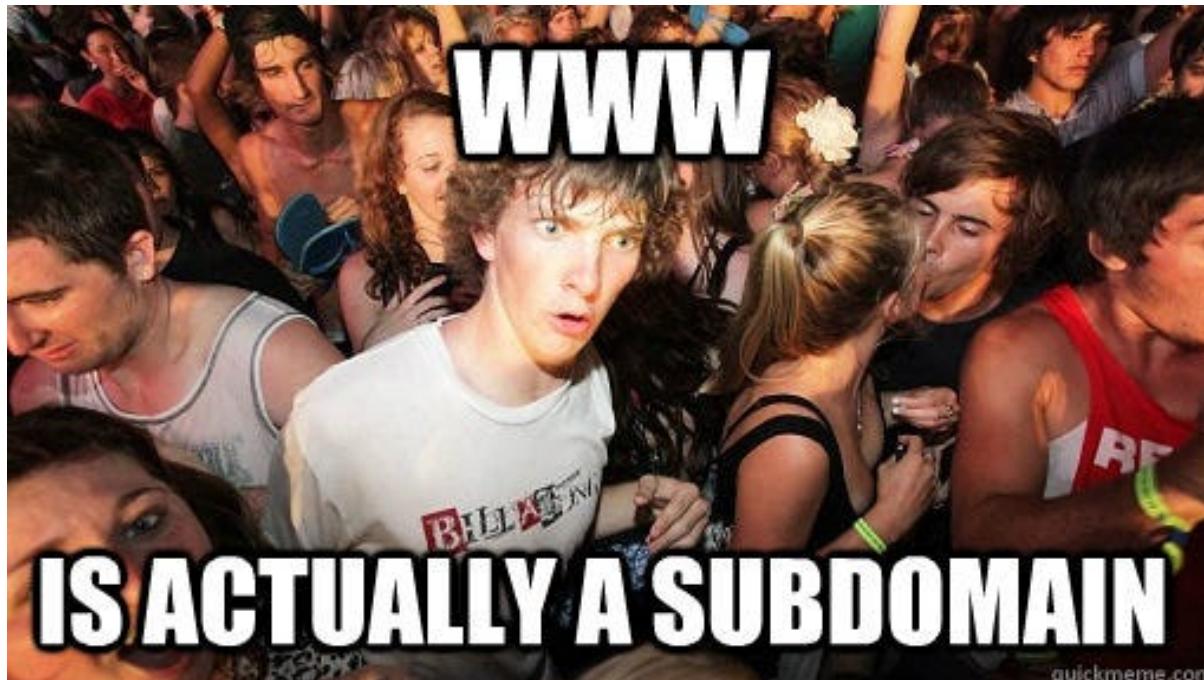
*Requiere API de whoisxmlapi



ReconFTW: a framework...



> MÓDULOS - SUBDOMINIOS



- Pasivo, 3rd parties y crtsh
- Resolución DNS
- TLS handshake x.509
- Técnica DNS NOERROR
- Recopilación de registros DNS
- Fuerza bruta DNS
 - Wordlist
 - Permutaciones
 - Wordlist x2
 - Regex
 - BingGPT
- Recursividad, pasivo y BF
- Web scraping
- Analytics

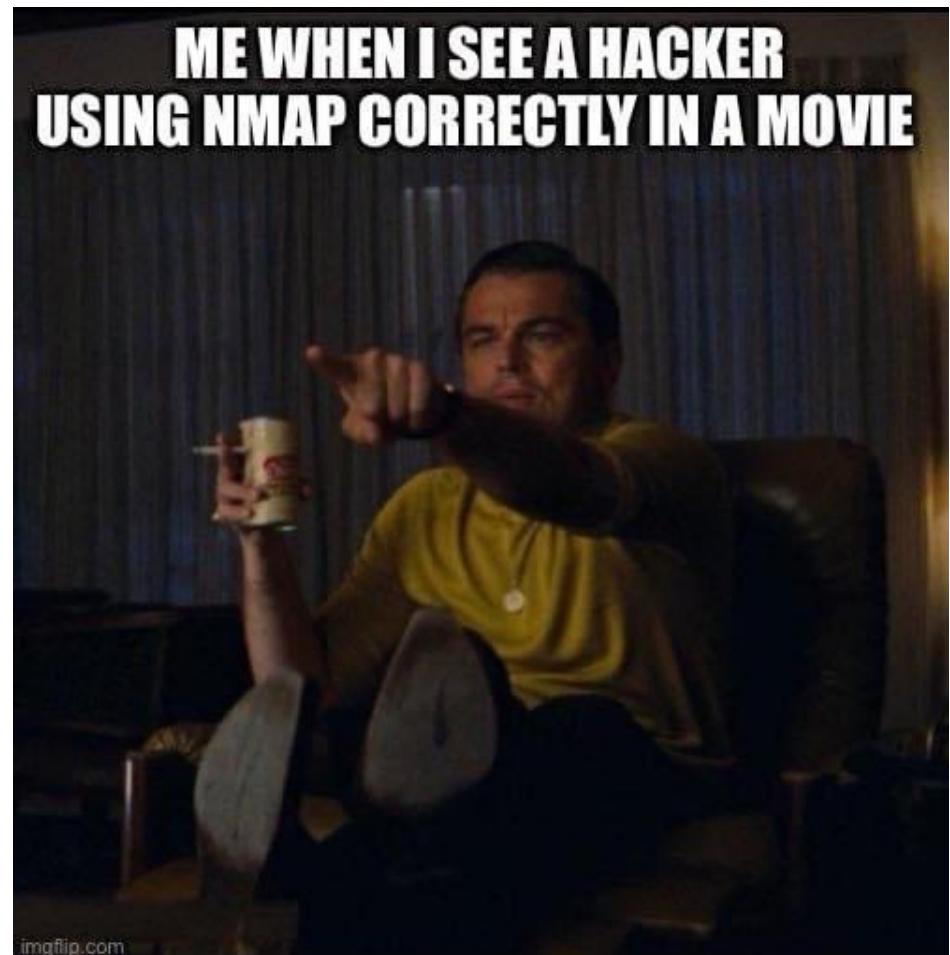


ReconFTW: a framework...



> MÓDULOS - HOSTS

- Filtrado IPs Cloud/CDN/WAF
- Escaneo de puertos pasivo via Shodan
- Escaneo de puertos activo
 - top 200
 - fingerprinting
 - vulners





ReconFTW: a framework...



> MÓDULOS - WEBS && URLs

- Web probing
 - Standard 80,443,8080...
 - +100 puertos no comunes
 - Incluye fingerprinting
- Web screenshots
- VHosts
- Favicon lookup
- Recolección URLs
 - Pasiva, 3rd parties
 - Activa, web crawling
- Categorización vulns
- Análisis JS
- Búsqueda recursiva
- Extracción endpoints
- Detección secretos



ReconFTW: a framework...



> MÓDULOS - ESCANEOS && WORDLISTS

Escaneo básico

- Detección WAFs
- Nuclei
- Web fuzzing
- CMS, detección y fingerprint
- S3 Buckets
- TestSSL

Wordlists

- Por extensión
- Endpoints
- Parámetros
- Valores
- Rutas
- Histórico de robots
- Contraseñas

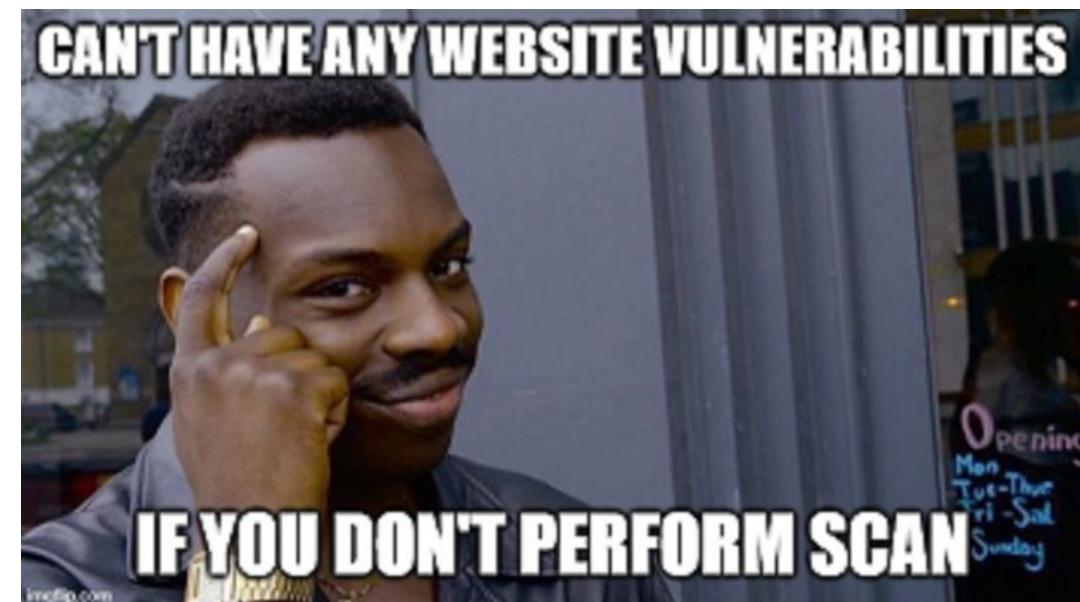


ReconFTW: a framework...



> MÓDULOS - VULNERABILIDADES

- Broken Links
- XSS
- CORS
- Open redirect
- CRLF
- LFI
- STI
- SQLi
- Nuclei Fuzzing
- SSRF
- Password spraying
- Command injection
- 4xx bypass
- Prototype pollution
- Request smuggling
- Web cache deception
- Transferencia de zona DNS





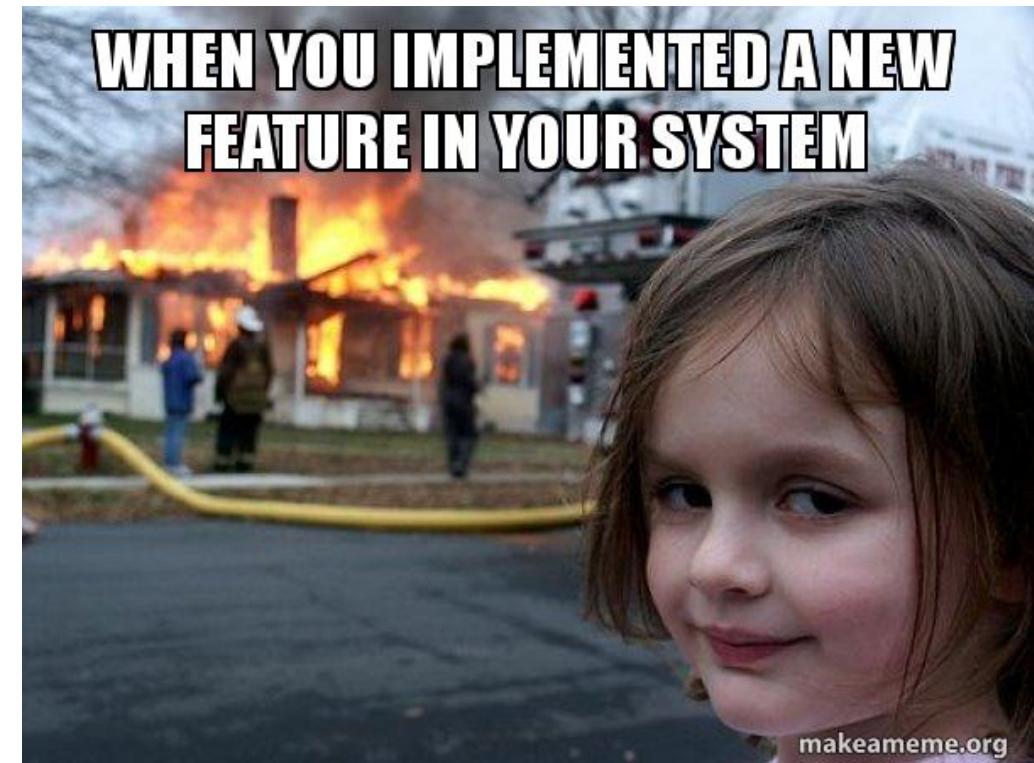
ReconFTW: a framework...



> MÓDULOS - EXTRAS

Extras

- Control scope
- Notificaciones
- Enviar zip con resultados
- Actualización de resolvers
- Detección y expansión de CIDR
- Axiom, auto arranque y limpieza
- Modo -multi
 - Disponible para osint y recon
 - Reduce requests para el mismo target
- Auto update
- Interfaz web





ReconFTW: a framework...



> MODOS

Workflows predefinidos usando diferentes módulos:

- **OSINT:** Solo información de Intel, indexados, dorking, VCS, metadatos.
- **Pasivo:** 3rd parties, sin interacción directa con el objetivo (sí DNS).
- **Subs:** descubrimiento de subdominios.
- **Recon:** enumeración completa, dominio -> subs -> hosts -> webs -> urls -> vulns comunes
- **Web:** enumeración web + vulnerabilidades
- **All:** YOLO mode, recon completo + vulnerabilidades



ReconFTW: a framework...



> MODOS

	-n osint	-p passive	-s subs	-r recon	-w web	-a all	-c custom
osint	x	x		x		x	?
subdomains		x	x	x		x	?
cloud			x	x		x	?
hosts		x		x		x	?
web			x	x		x	?
url				x	x	x	?
vulns						x	?



ReconFTW: a framework...



> INTERFAZ WEB

Requiere pasos adicionales en la instalación

```
#####
# Insert option: 3

#####
# Running: Installing web reconfTw

Installing python libraries...
python virtualenv install...

Activating virtualenv...
Installing Requirements...
Installing tools...
Creating WEB User...

Username (leave blank to use 'six2dez'): test
Email address:
Password:
Password (again):
The password is too similar to the username.
This password is too short. It must contain at least 8 characters.
This password is too common.
Bypass password validation and create user anyway? [y/N]: y
Superuser created successfully.
```



ReconFTW: a framework...



> INTERFAZ WEB

The screenshot shows a web browser window with the URL `192.168.1.38:8001/projects/`. The main page has a header "recon" and a table with columns "VERSION", "TARGET", and "D". A modal dialog box titled "NEW SCAN" is open, containing the following fields:

- TARGET OPTIONS:** Single (selected), List
- Target:** euskalhack.org
- MODE OPTIONS:**
 - Recon (selected)
 - Subdomains
 - Passive
 - All
 - Web
 - OSINT
- GENERAL OPTIONS:**
 - Deep Scan (selected)
 - Axiom (selected)
- COMMAND:** `./reconftw.sh -d euskalhack.org -r --deep -v`
- Buttons:** Cancel (red), Submit (green)



ReconFTW: a framework...



> INTERFAZ WEB

The screenshot shows the ReconFTW web interface with the following details:

Header: WAITING | SCAN MODE: RECON | BUGCROWD.COM | User icon

Section: SUBDOMAINS

Table Headers: #, SUBDOMAIN, IP ADDRESS, PORT, SUBDOMAIN TAKEOVER

Table Data:

#	SUBDOMAIN	IP ADDRESS	PORT	SUBDOMAIN TAKEOVER
1	api.bugcrowd.com	['104.20.6.68', '104.20.7.68']	['2082', '2095', '2096', '8080', '8443', '8880', '443']	NO
2	asset-management.a.bugcrowd.com	['10.10.130.156', '10.10.137.81', '10.10.132.188']	[]	NO
3	assetinventory.bugcrowd.com	['104.20.6.68', '104.20.7.68']	['2082', '2095', '2096', '8080', '8443', '8880', '443']	NO
4	auth-test.bugcrowd.com	['104.20.6.68', '104.20.7.68']	['2082', '2095', '2096', '8080', '8443', '8880', '443']	NO
5	blog.bugcrowd.com	['104.20.6.68', '104.20.7.68']	['2082', '2095', '2096', '8080', '8443', '8880', '443']	NO
6	bounce.bugcrowd.com	['192.28.152.174']	[]	NO
7	bugcrowd.com	['104.20.7.68', '104.20.6.68']	['2082', '2095', '2096', '8080', '8443', '8880', '443']	NO
8	collateral.bugcrowd.com	['35.153.186.101', '35.172.4.70', '35.170.161.189']	['443']	NO
9	crowdcontrol.a.bugcrowd.com	['44.207.32.185', '52.54.65.162', '52.5.54.71', '3.212.246.214', '52.200.33.246']	[]	NO
10	crowdmatch.a.bugcrowd.com	['34.236.0.98', '3.208.108.238']	[]	NO

Pagination: Showing 1 to 10 of 47 entries | Previous | 1 | 2 | 3 | 4 | 5 | Next

Footer: DNS ZONE TRANSFER . DNS REGISTRY . CMS



ReconFTW: a framework...



> INTEGRACIÓN AXIOM

Framework para distribución y paralelización de procesos ([vídeo](#))

- Disponible para Azure, AWS, DO, Linode, IBM Cloud y GCP (parcialmente)
- Despliega múltiples instancias de una snapshot creada previamente
- Divide la carga de entrada en partes iguales
- Une las diferentes salidas en un solo fichero/directorio
- Más de 80 herramientas disponibles
- Permite multi-region
- Incluye comandos para la gestión de las instancias (ssh, scp, on/off, proxy, vpn, backup)

The screenshot shows a GitHub code editor interface. At the top, there's a header with a user icon, the repository name 'six2dez Create mantra.json (#721)', and a 'Code' tab which is currently selected. Below the header, the code editor displays the following JSON content:

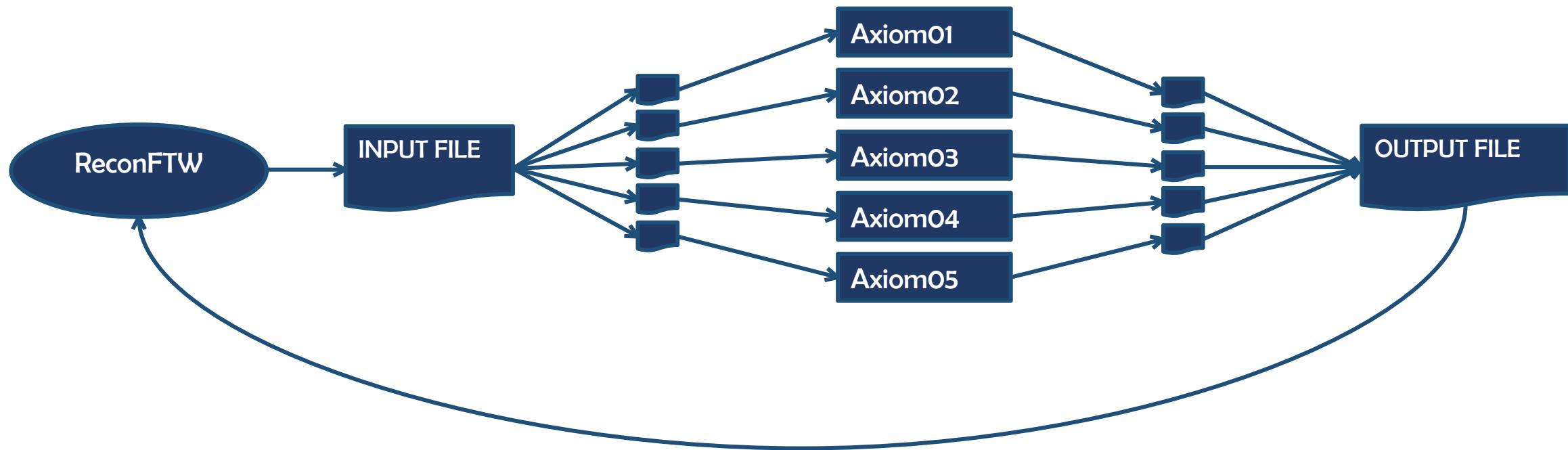
```
1  [{  
2      "command": "cat input | /home/op/go/bin/Mantra -s | tee output",  
3      "ext": "txt"  
4  }]
```



ReconFTW: a framework...



> INTEGRACIÓN AXIOM





ReconFTW: a framework...



> INTEGRACIÓN NOTIFICACIONES

- 2 modos:
 - Inicio / Fin escaneo por dominio
 - Inicio / Fin de cada módulo
- Envío de resultados vía zip
 - Si el zip pesa más de 8Mb se envía link vía [transfer.sh](#)

Disponible para Slack / Discord / Telegram / Email / Google Chat / Microsoft Teams

bot
Recon successfully started on pepsico.com 3:32
2021_08_08-04.53.09_pepsico.com.zip 51.2 KB 6:53
Finished Recon on: pepsico.com under /root/reconftw/Recon/pepsico.com in: 3 hours, 20 minutes, 23 seconds. 6:53

2:26 PM Recon successfully started on bugcrowd.com
Running : Passive Subdomain Enumeration - bugcrowd.com
test BOT 04/12/2021 2:42 PM
25902 new subs (passive) in 1 hours, 6 minutes, 47 seconds.
Running : Crtsh Subdomain Enumeration
14950 new subs (cert transparency) in 6 seconds.
Running : Active Subdomain Enumeration
test BOT 04/12/2021 2:55 PM
577 new subs (active resolution) in 12 minutes, 25 seconds.
Running : Bruteforce Subdomain Enumeration



ReconFTW: a framework...



> TRUCOS Y CONSEJOS

- Abre los resultados en un editor de código
- Velocidad de escaneos
 - No escanees un ISP o algo como Google sin pensar qué estás haciendo
 - El modo DEEP solo si sabes lo que implica
 - Pasivo -> Subdominios -> Recon
- En caso de fallos o cero resultados
 - Chequear el directorio .log
 - Te han baneado?
 - Relanzar el proceso concreto que falló
 - Enviar un PR :)
- Relanzar procesos
 - En la carpeta .called_fn eliminar la función que queremos relanzar
 - La opción DIFF del fichero de config relanzará todos los procesos
- Combina con Burp activando PROXY en la config



ReconFTW: a framework...



> TRUCOS Y CONSEJOS

- Recuerda que puedes crear ficheros de configuración distintos por modos o targets
- Cambia de wordlists
- Con axiom
 - Usa el script post-arranque para personalizar los VPS
 - Si puedes usa multiregion
 - Reconstruye el snapshot periódicamente
- Riesgos
 - Tirar ese DNS montado en una RPI
 - Ruido
 - Baneos
- Relanzar distintos modos contra el mismo objetivo para escanear por fases
- Aprender a usar el modo sin documentar “-c”
- Genera tus propios resolvers



ReconFTW: a framework...



> PRÓXIMOS PASOS

- Refactorización y modularización
 - Funciones en scripts independientes
 - reconftw.sh solo será un orquestador
 - Entorno propio
 - Accesibles a nivel de sistema
- Wiki
- Mejorar la monitorización continua
- Continuar con el desarrollo de la interfaz web



ReconFTW: a framework...



> DUDAS?





ReconFTW: a framework...



**¡MUCHAS GRACIAS!
ESKERRIK ASKO!**