EuskalHack Security Congress VI

> WHOAMI?

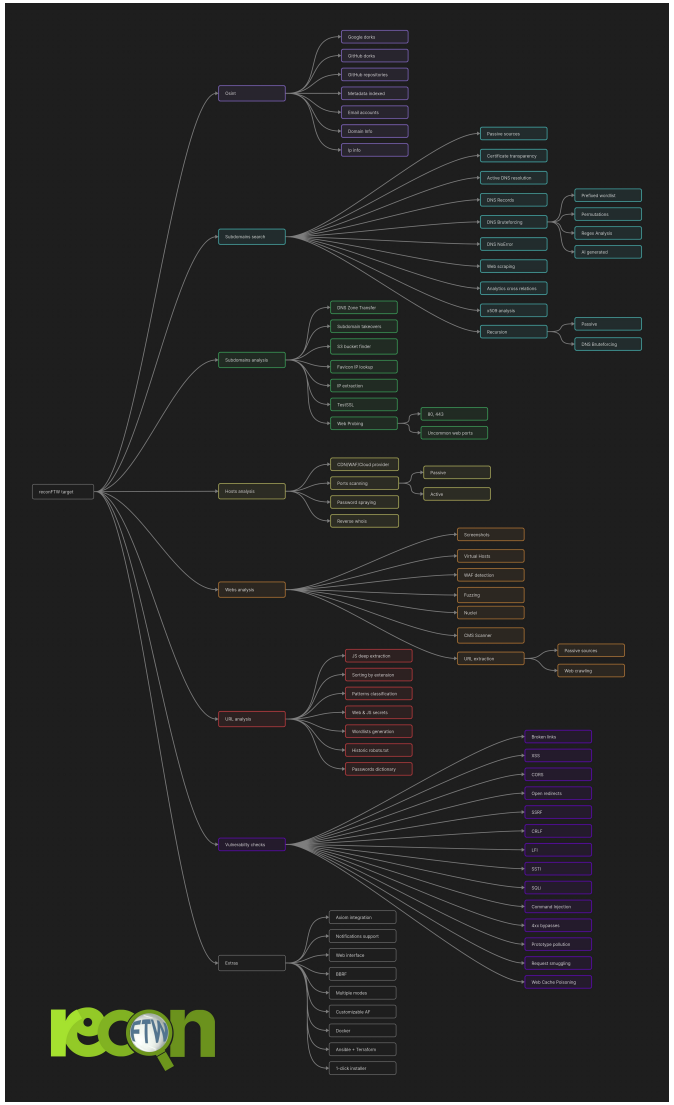
- Padre
- Bash lover
- Open source dev
- @six2dez / @six2dez1
- Red Teamer en Visma
- pentestbook.six2dez.com
- Bug bounty hunter & pentester
- Speaker en Disobey, H-c0n, BitUp, DragonJarCOn, HacktivityCon...

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
```

```
dev-v2.6-80-g145164c                                    by @six2dez

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
```

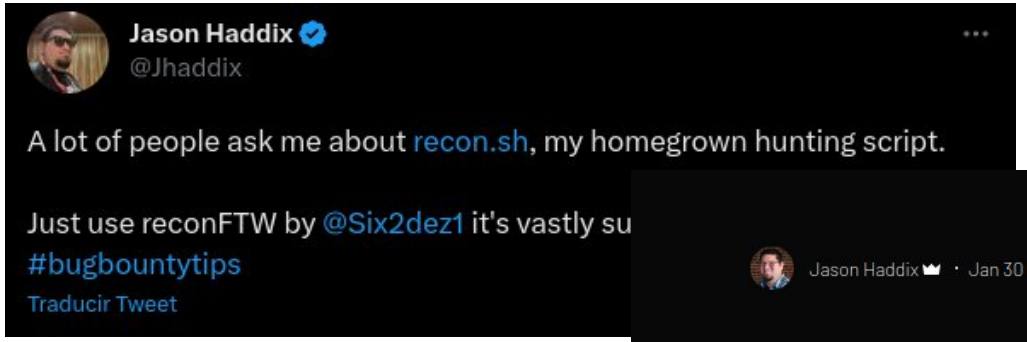
- +4K ★
- + 700 forks
- 1,6K commits
- +300 issues
- + 45 releases
- +2K clones/semana
- +8K visitantes/semana
- +75 herramientas
- 7 modos distintos
- 3 tipos de inputs
- Instalador
- Licencia MIT

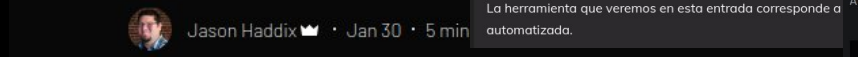
ReconFTW: a framework...

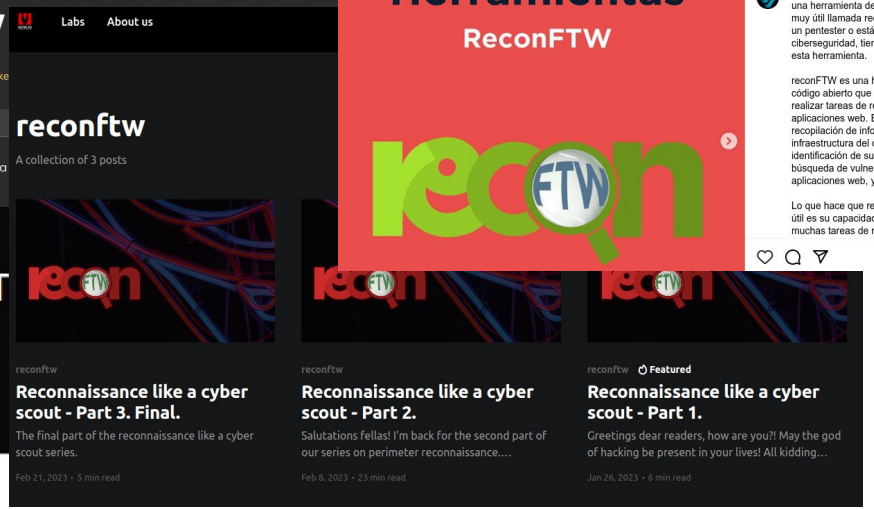
> OBJETIVOS Y NECESIDADES

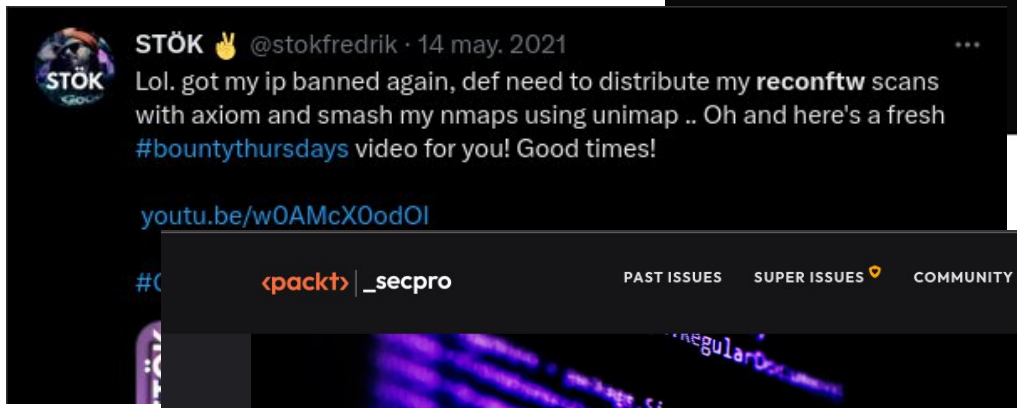
- Proyecto personal
- Entornos pentesting, BB o RT
- AutomatizaFTW
- Técnicas actualizadas
- Output listo para analizar
- Escalable
- Proyecto vivo
- Contribución a la comunidad
- Mejorar el panorama de recon

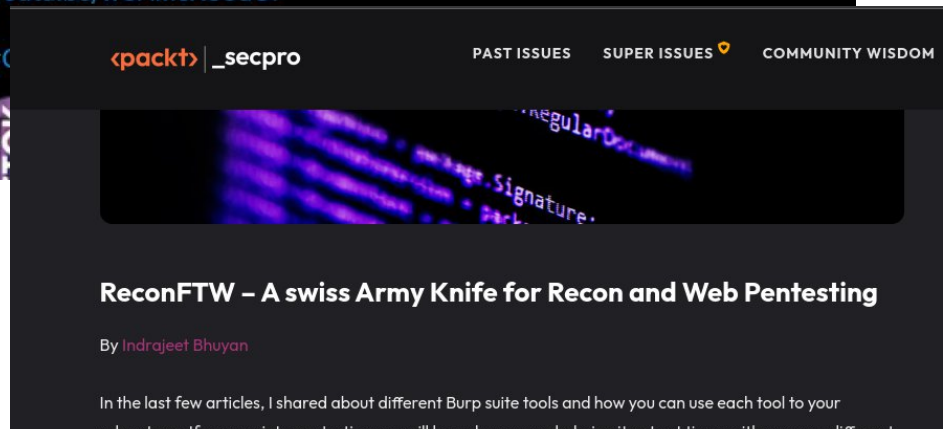
ReconFTW: a framework...

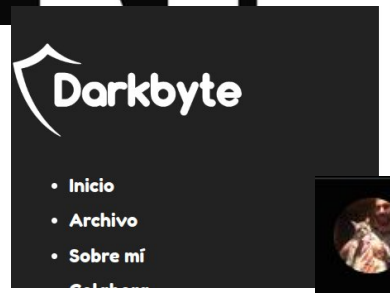


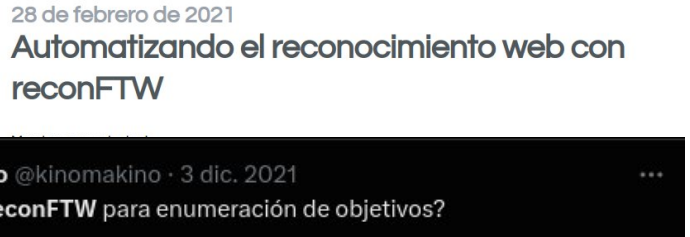












ReconFTW: a framework...

> 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: a framework...

> MÓDULOS - OSINT

Dominio

- Google Dorks predefenidos
- 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

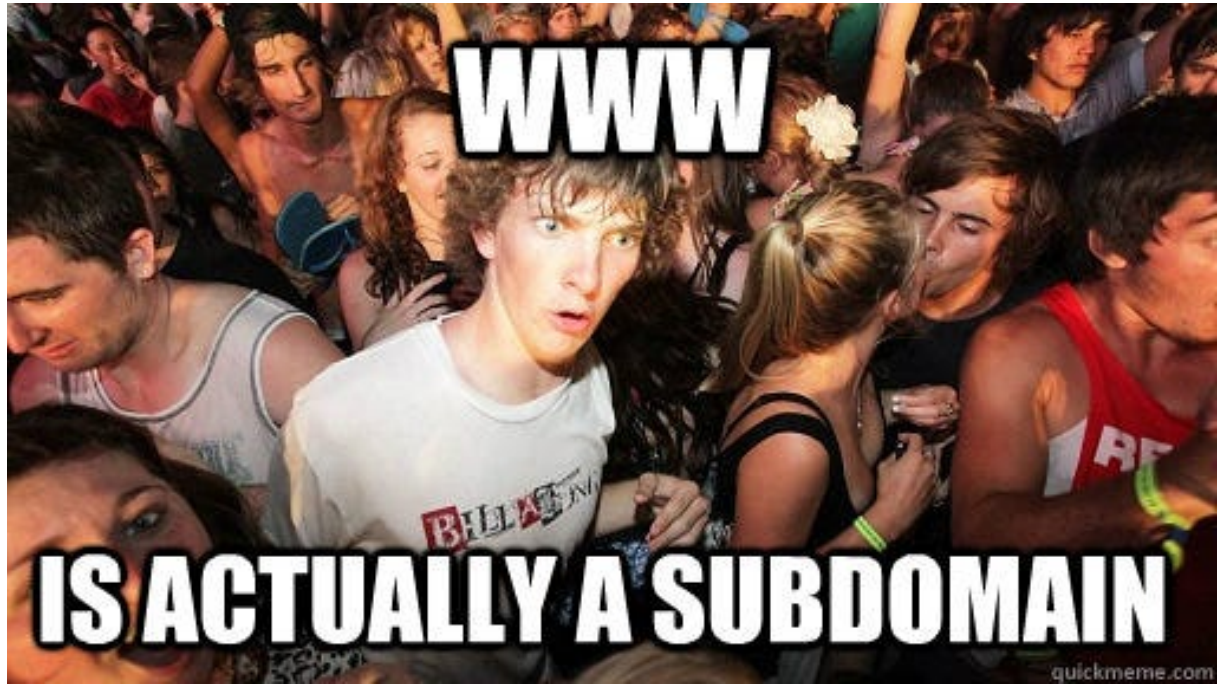
IP *

- 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 screenshooting
- 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

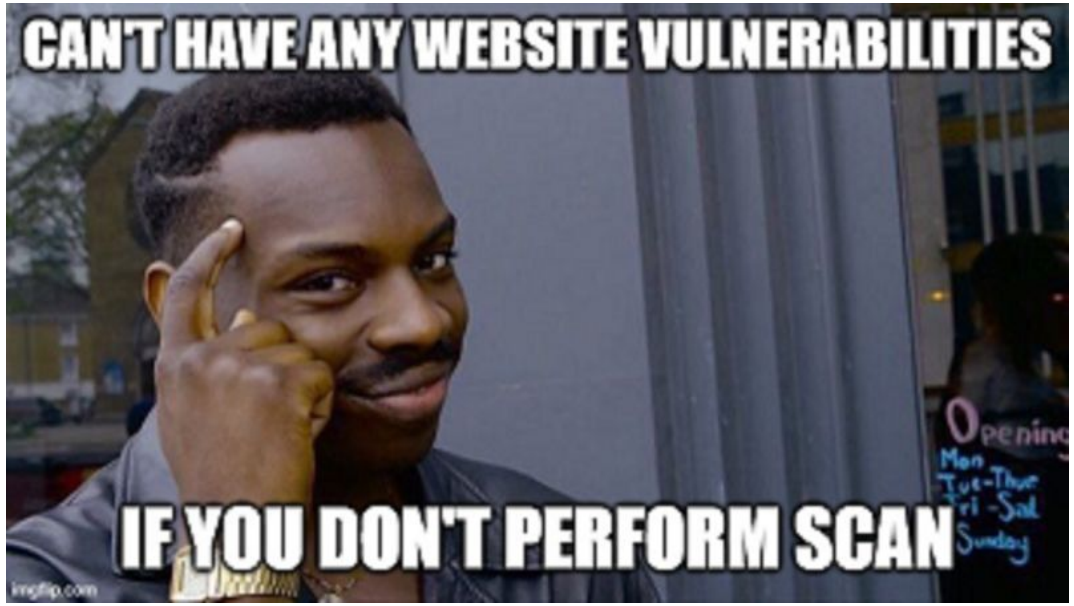
Wordlists

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

ReconFTW: a framework...

> MÓDULOS - VULNERABILIDADES

- Broken Links
- XSS
- CORS
- Open redirect
- CRLF
- LFI
- SSTI
- 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

> 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.
```

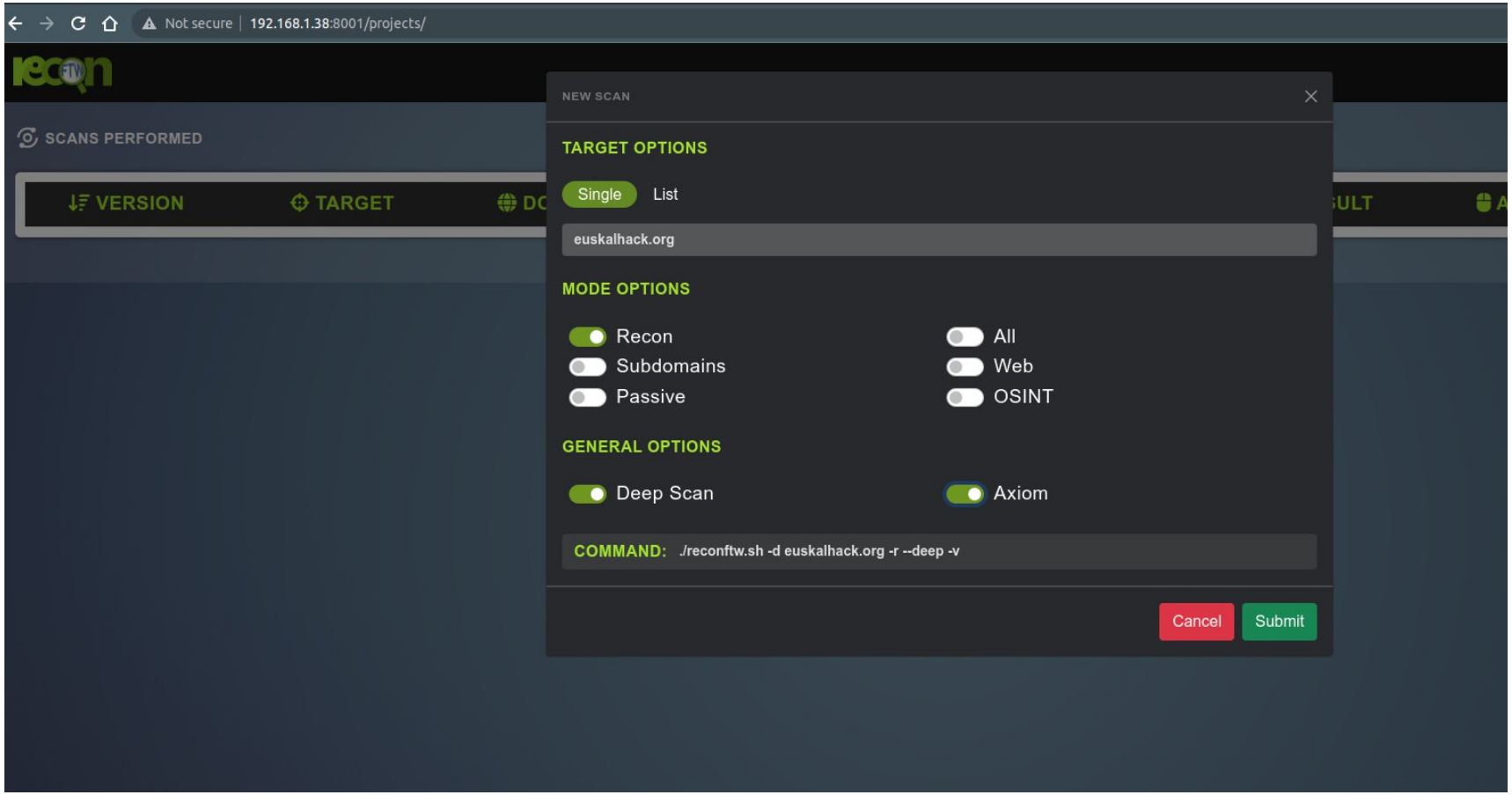
```
~/Tools/reconftw | on dev !49 ?1 ····· 1 ✘ | took 17s | at 17:15:06
./reconftw.sh --web-server start

dev-v2.6-113-g91b8d54                                    by @six2dez
Web Interface    by @lur1el, @d3vchac, @mx61tt and @dd4n1b0y

Starting web server...
Web server started!
Service Address: http://192.168.1.38:8001
```

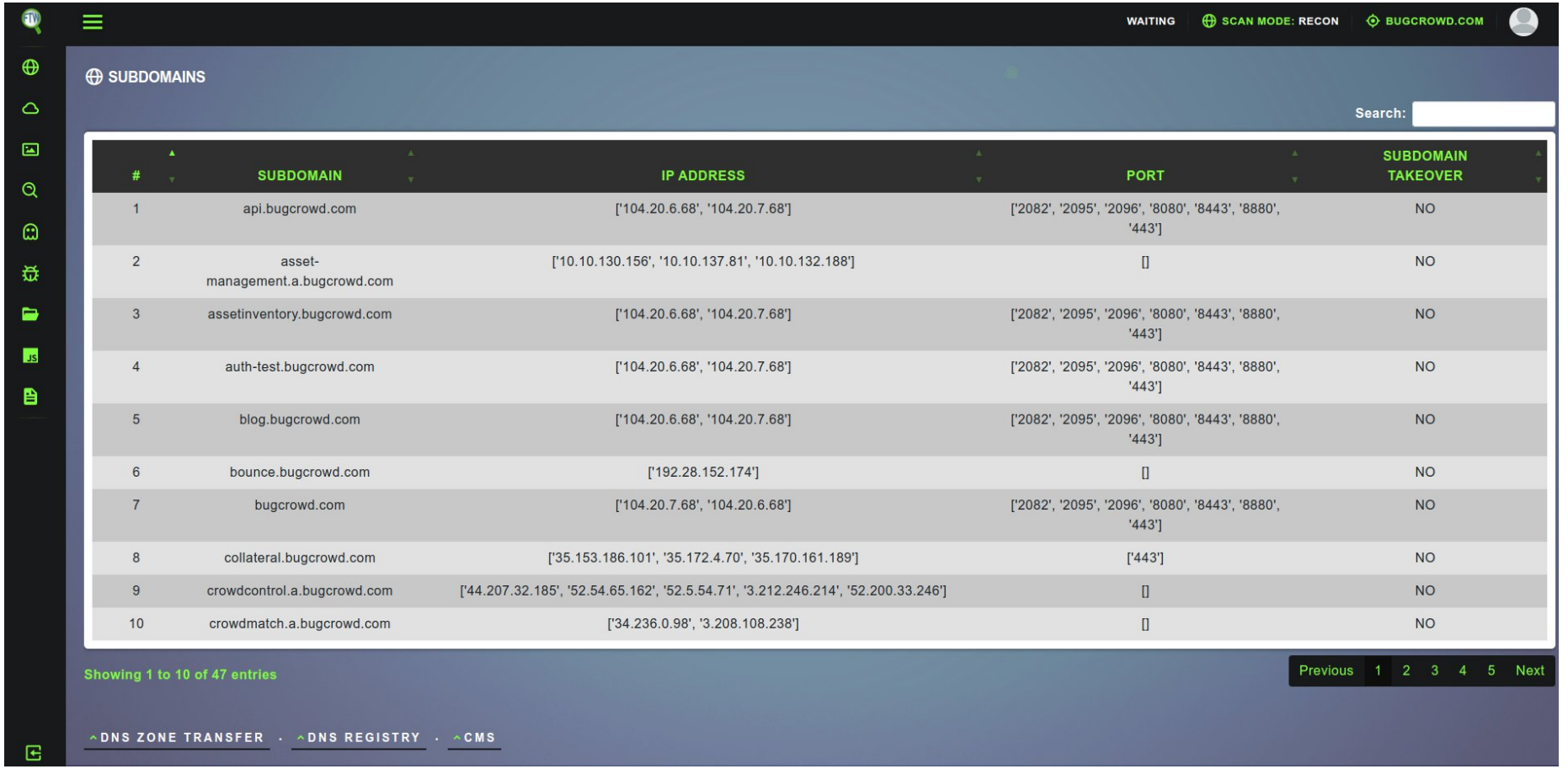
ReconFTW: a framework...

> INTERFAZ WEB



ReconFTW: a framework...

> INTERFAZ WEB



#	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

Showing 1 to 10 of 47 entries

Previous 1 2 3 4 5 Next

ReconFTW: a framework...

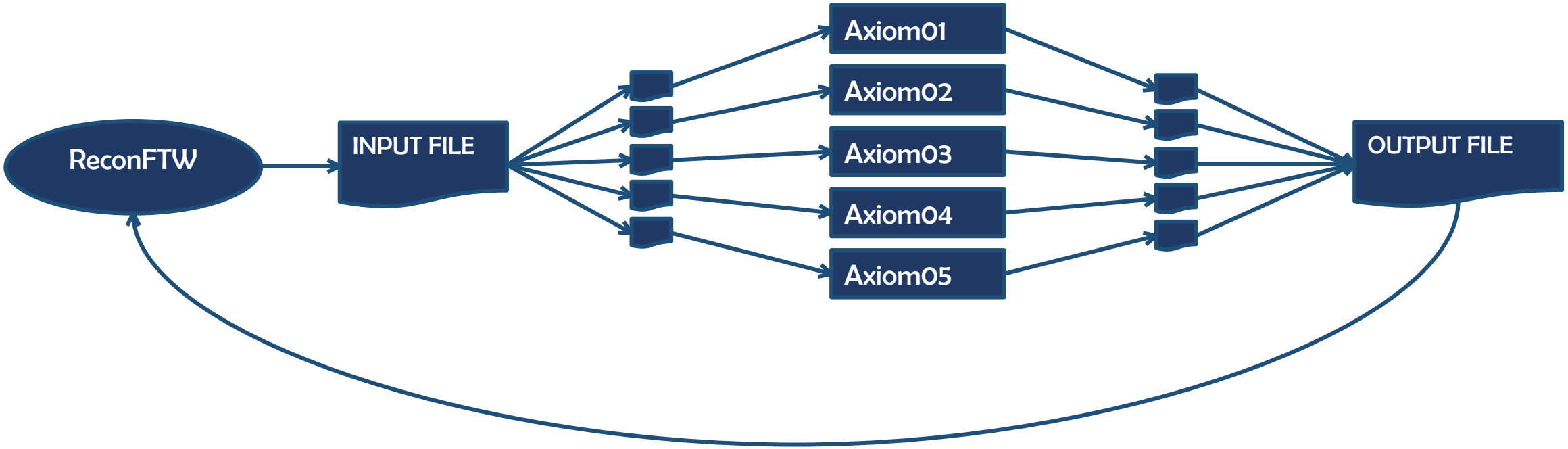
> INTEGRACIÓN AXIOM

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)

ReconFTW: a framework...

> INTEGRACIÓN AXIOM

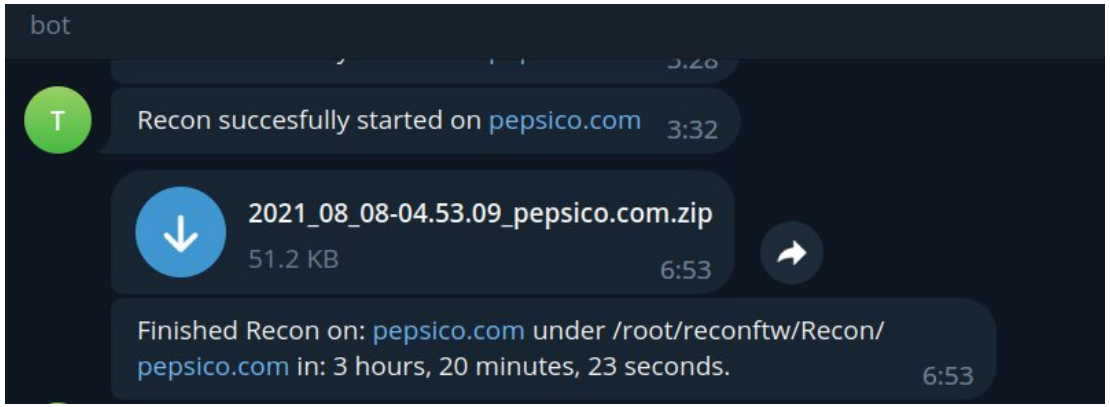


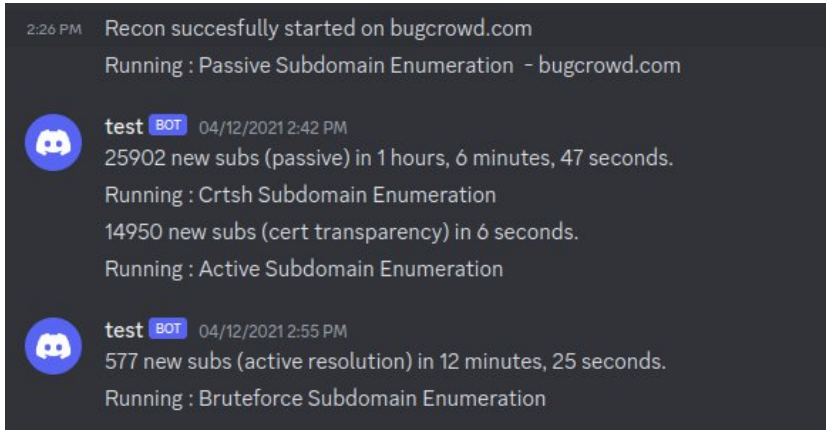
ReconFTW: a framework...

> 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





> 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 PROXIFY en la config

> 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

> 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!