



EuskalHack Security Congress VI





ReconFTW: a framework...



> WHOAMI?

- **Padre**
- **Ba\$h lover**
- **Open source dev**
- [@six2dez](#) / [@six2dez1](#)
- **Red Teamer en [Vi\\$ma](#)**
- [pentestbook.six2dez.com](#)
- **Bug bounty hunter & pentester**
- **Speaker en Di\$obey, H-con, BitUp, DragonJarCon, HacktivityCon...**





ReconFTW: a framework...



euskalhack2023.reconftw.com:8000



- [illegible]



ReconFTW: a framework...



> QUÉ ES RECONFTW?

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

RECONFTW

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...



Jason Haddix
@Jhaddix

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

Snifer@L4b's / Posts / Automatiza las tareas de Reconocimiento Web con ReconFTW

Automatiza las tareas de Reconocimiento Web con ReconFTW

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



securiters · Seguir

securiters Hoy quiero hablaros de una herramienta de reconocimiento muy útil llamada reconFTW. Si eres un pentester o estás interesado en la ciberseguridad, tienes que conocer esta herramienta.

reconFTW es una herramienta de código abierto que se utiliza para realizar tareas de reconocimiento en aplicaciones web. Esto incluye la recopilación de información sobre la infraestructura del objetivo, la identificación de subdominios, la búsqueda de vulnerabilidades en aplicaciones web, y mucho más.

Lo que hace que reconFTW sea tan útil es su capacidad para automatizar muchas tareas de reconocimiento.

Jason Haddix · Jan 30 · 5 min

The Anti-Recon Recon Club (using ReconFTW)



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/wOAMcX0odOI

<packt> | _secpro

PAST ISSUES

SUPER ISSUES

COMMUNITY WISDOM

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



- Inicio
- Archivo
- Sobre mí

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 reconF

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)
haki2host 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)
xnLinkFinder 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: 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: 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



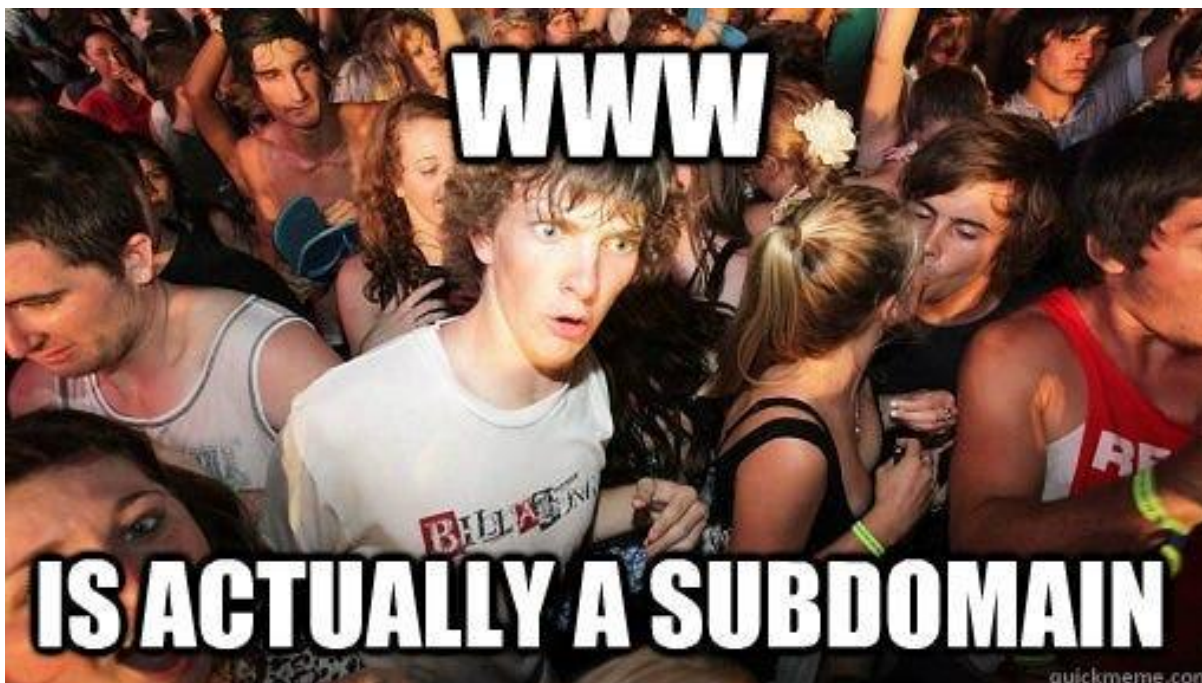
*Requiere API de whoisxmlapi



ReconFTW: a framework...



➤ MÓDULOS - SUBDOMINIOS



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



ReconFTW: a framework...



> MÓDULOS - HOSTS

- **Filtrado IP, Cloud/CDN/WAF**
- **Escaneeo de puertos pasivo via Shodan**
- **Escaneeo de puertos activo**
 - **top 200**
 - **fingerprinting**
 - **vulner**





ReconFTW: a framework...



> **MÓDULOS - WEBS && URLS**

- **Web probing**
 - **Standard 80,443,8080...**
 - **+100 puertos no comunes**
 - **Incluye fingerprinting**
- **Web screenshoting**
- **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**
- **\$3 Buckets**
- **TestSSL**

Wordlists

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

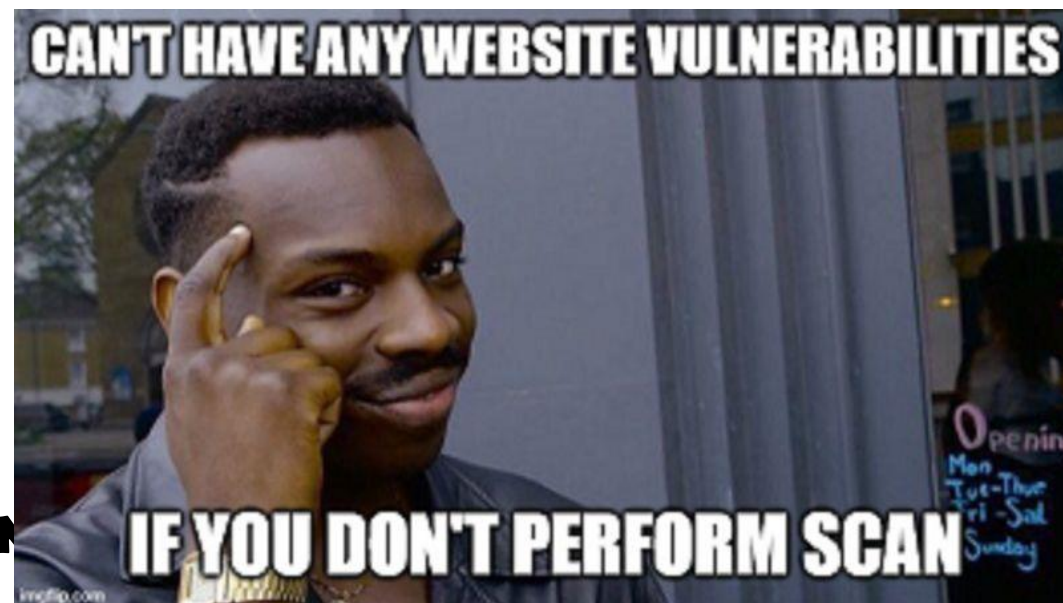


ReconFTW: a framework...



> MÓDULOS - VULNERABILIDADES

- Broken Link\$
- XSS
- CORS
- Open redirect
- CRLF
- LFI
- SSTI
- SQLi
- Nuclei Fuzzing
- SSRF
- Password \$praying
- Command injection
- 4xx bypass
- Prototype pollution
- Request \$muggling
- Web cache deception
- Trans\$ferencia de zona DMZ





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

Workflow\$ predefinido\$ usando diferente\$ módulos\$

- **O\$INT\$**: Solo información de Intel, indexado\$, dorking, VC\$, metadato\$.
- **Pa\$ivo\$**: 3rd parties\$, sin interacción directa con el objetivo (sí DN\$).
- **\$ub\$**: descubrimiento de subdominio\$.
- **Recon\$**: enumeración completa, dominio -> sub\$ -> host\$ -> web\$ -> url\$ -> vuln\$ 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	?



```
#####
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.
```

```

//      ) )
//____//
//____( //____) ) //____) ) //____) ) //____) ) //____
//      | | //      //      //      //      //      //      //
//      | | ((____ ((____ ((____//      //      //      //      //
dev-v2.6-113-g91b8d54                                     by @six2dez
Web Interface      by @lur1el, @d3vchac, @mx61tt and @dd4n1b0y

```



ReconFTW: a framework...



> INTERFAZ WEB

← → ↻ 🏠 ⚠ Not secure | 192.168.1.38:8001/projects/

recon

🔄 SCANS PERFORMED

⌵ VERSION ⚙ TARGET 🌐 DC

NEW SCAN ✕

TARGET OPTIONS

☒ Single ☐ List

euskalhack.org

MODE OPTIONS

<input checked="" type="checkbox"/> Recon	<input type="checkbox"/> All
<input type="checkbox"/> Subdomains	<input type="checkbox"/> Web
<input type="checkbox"/> Passive	<input type="checkbox"/> OSINT

GENERAL OPTIONS

<input checked="" type="checkbox"/> Deep Scan	<input checked="" type="checkbox"/> Axiom
---	---

COMMAND: ./reconftw.sh -d euskalhack.org -r --deep -v

Cancel Submit



ReconFTW: a framework...



> INTERFAZ WEB

WAITING SCAN MODE: RECON BUGCROWD.COM

SUBDOMAINS

Search:

#	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

^ 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)**

```
six2dez Create mantra.json (#721) 
```

```
Code Blame 4 lines (4 loc) · 84 Bytes
```

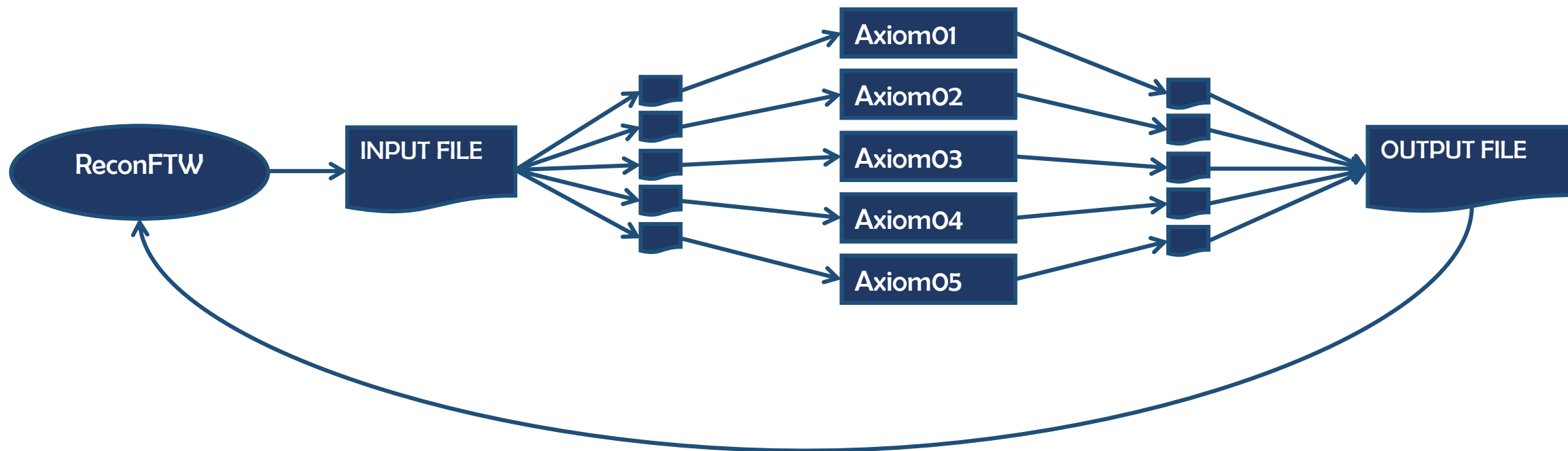
```
1  [{
2    "command": "cat input | /home/op/go/bin/Mantra -s | tee output",
3    "ext": "txt"
4  }]
```



ReconFTW: a framework...



> INTEGRACIÓN AXIOM





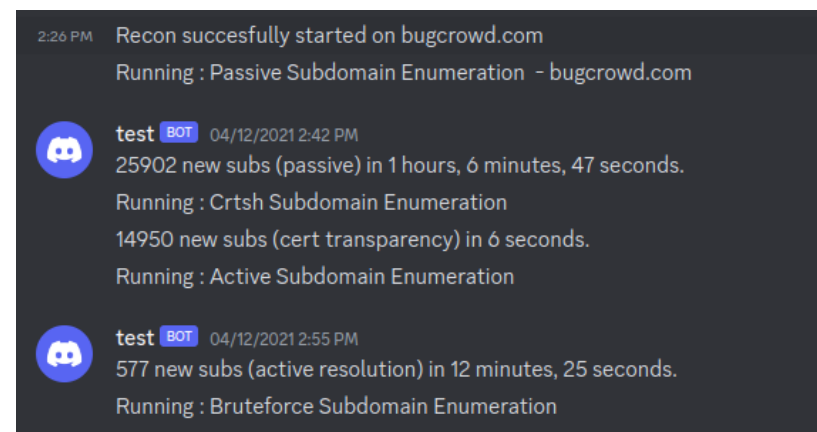
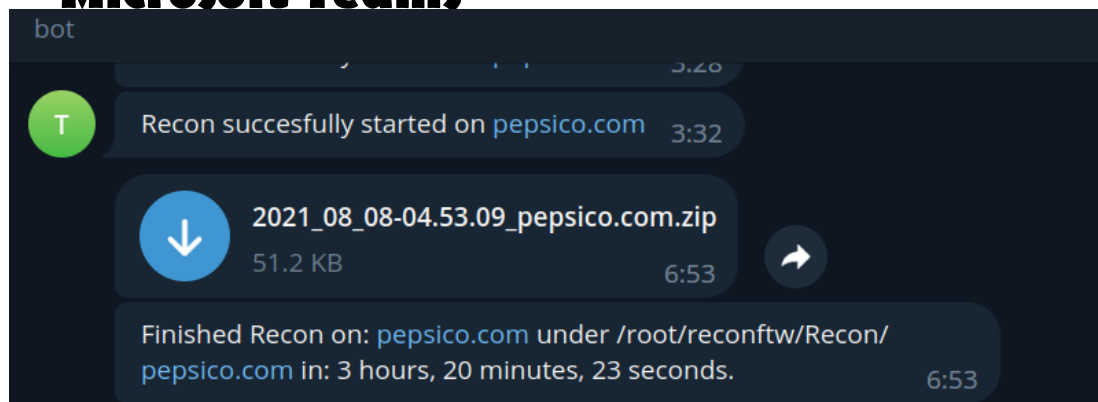
ReconFTW: a framework...



➤ 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





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 PROXIFY 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!**

