



# TODO SOBRE MI OBJETIVO

Ignacio Brihuega Rodríguez (N4xh4ck5)  
EastMadH4ck 2017

1. Whoami
2. Red Team tools
3. Blue Team tools

1. Whoami
2. Red Team tools
3. Blue Team tools

# Whoami



- Security Consultant – Tiger Team SIA
- Máster de Seguridad Informática en la Universidad de La Rioja (UNIR)
- Grado en Ingeniería en Tecnologías de la Telecomunicación, especialidad en ingeniería telemática en la Universidad de Alcalá de Henares (UAH)
- Coautor del blog “Follow the White Rabbit” – [fwhibbit.es](http://fwhibbit.es)
- Info contacto:
  - **Linkedin:** Ignacio Brihuega Rodríguez
  - **Twitter:** [twitter.com/@nachoo\\_91](https://twitter.com/@nachoo_91)



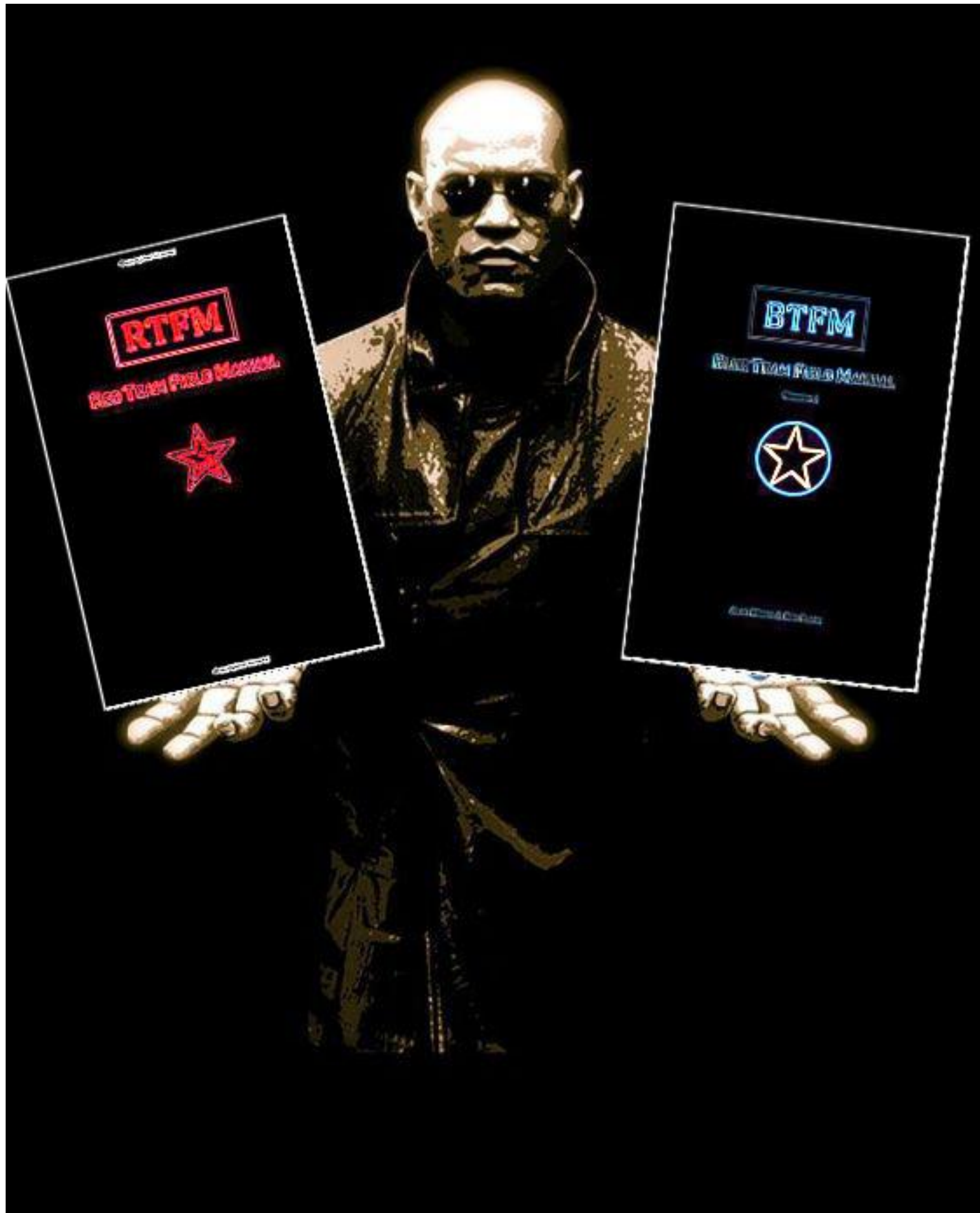


# Disclamer



- La información que se va a mostrar es de carácter público.
- Las técnicas demostradas son para fines académicos, no me hago responsable de su uso para otro fin.





## Read Team vs Blue Team

- Tools para recoger información pública de un target con objeto de ser empleado para un test de intrusión.
- Tools para buscar de manera proactiva posibles fugas de información y detección de posible fraude.

1. Whoami
2. Red Team tools
3. Blue Team tools

# Red Team Tools

Tools para recoger información pública de un target con objeto de ser empleado para un test de intrusión externo.





# Red Team Tools

- Th4sD0m
- N4xD0rk
- n0d0M
- CMsSc4n
- RastLeak



# Read Team Tools



¿Por dónde empezamos?

site:rtve.es -site:www.rtve.es

site:rtve.es -site:www.rtve.es

Todo Imágenes Noticias Shopping Maps Más Configuración Herramientas

Aproximadamente 715.000 resultados (0,26 segundos)

**Blogs RTVE.es**  
blogs.rtve.es ▼  
hace 1 día - Los blogs de RTVE.es. Todas las noticias y cosas curiosas las encontrarás en los Blogs de RTVE: blogs de música, televisión, actualidad, ...

**Comprobar números y décimos de la lotería de Navidad 2016 - RTVE.es**  
loteria.rtve.es ▼  
Comprobar Lotería de Navidad 2016. Compruebe sus números y décimos de la lotería de Navidad y vea si le ha tocado el Gordo en el Sorteo de Navidad 2016 ...

**Encuentros digitales RTVE.es - Portada**  
encuentrosdigitales.rtve.es/ ▼  
Encuentros digitales en RTVE.es. Participa en los encuentros digitales de RTVE.es y envía tu pregunta para los invitados de las charlas digitales.

**Portal de Aquí Hay Trabajo**  
aquihaytrabajo.rtve.es/ ▼  
Trabajos y empleos en Iberoamérica, Bolsa de trabajo líder con miles de ofertas de empleo. Ingresa gratis tu currículum y comienza a buscar trabajo.

**Bandera negra - Blogs RTVE.es**  
blog.rtve.es/banderanegra/ ▼  
18 dic. 2013 - Bandera negra Ramiroquai conduce en Radio 3 Extra un programa con el deseo de recorrer de forma apasionada el universo musical y ...

**Vicente Ferrer: diario de un rodaje - Blogs RTVE.es**  
blog.rtve.es/vicenteferrer ▼  
18 nov. 2013 - Equipo de rodaje Este blog está escrito y realizado por miembros del equipo de Comunicación de la Fundación Vicente Ferrer en India y del ...

# Read Team Tools

¿subdominios? -> **Bing: domain:rtve.es**

-> Automatizando: **N4xD0rk**

*!!!Pero esto no es una ponencia de Hacking  
con buscadores!!!*

¿ Es un servidor dedicado o se encuentra en un  
hosting? -> tool: **Th4sD0m**



The screenshot shows a Bing search interface with the query 'domain:rtve.es -site:www.rtve.es' entered in the search bar. Below the search bar, there are tabs for 'Web', 'Imágenes', 'Vídeos', 'Mapas', and 'Noticias'. The 'Web' tab is selected. The search results show 70,000 results. The first result is 'Comprobar números y décimos de la lotería de ... - RTVE.es' with the subdomain 'loteria.rtve.es' highlighted. The second result is 'OpenIAM - Login' with the URL 'https://extra.rtve.es/idp/login.html' highlighted. The third result is 'Portal de Aquí Hay Trabajo' with the subdomain 'aquihaytrabajo.rtve.es' highlighted. The fourth result is 'intranere.rtve.es' with the URL 'https://intranere.rtve.es/publicacionIntranet/descarga\_fichero...' highlighted. The fifth result is 'img.rtve.es' with the URL 'img.rtve.es/v/4017541?w=200&preview=1494611476661.JPG' highlighted. The sixth result is 'aula.rtve.es' with the URL 'https://aula.rtve.es' highlighted.



[illegible]



# Read Team Tools

Th4sD0m



- Determinar el alcance de la intrusión.
- Conocer si el target se encuentra en un hosting o es un servidor dedicado

```
Information about the IP 178.33.██████████
{u'city': u'Madrid', u'region_code': u'MD', u'region_name': u'Madrid', u'ip': u'178.33.██████████', u'time_zone': u'Europe/Madrid', u'longitude': -3.7(██████████ u'metro_code': 0, u'latitude': 40.4██████████, u'country_code': u'ES', u'country_name': u'Spain', u'zip_code': u'28(██████████)}

Domains contained in the IP 178.33.██████████ are:

www.glenfi██████████fusion.com
www.tu██████████alnuestro.com
so██████████decabras.es
walletnfc.██████████ne.es
www.love██████████day.es
```



# Read Team Tools



## N4xd0rk

- Python 2.7
- Listar subdominios de un dominio de manera anónima.
- Integración de Th4D0m

```
python n4xd0rk.py -h
usage: n4xd0rk.py [-h] [-d DOMAIN] [-i IP] -o OPTION -n SEARCH -e EXPORT
                  [-l LANGUAGE]

This script searches the subdomains about a domain using the results indexed of Bing search.

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        The domain which wants to search.
  -i IP, --ip IP        The IP which to kown the domains to contain.
  -o OPTION, --option OPTION
                        Select an option:
                        1. Searching the subdomains about a domain using the results indexed.
                        2. Searching the domains belong to an IP.
  -n SEARCH, --search SEARCH
                        Indicate the number of the search which you want to do.
  -e EXPORT, --export EXPORT
                        Export the results to a json file (Y/N)
                        Format available:
                        1.json
                        2.xlsx
  -l LANGUAGE, --language LANGUAGE
                        Indicate the language of the search
                        (es) -Spanish(default)
                        (en) -English
```



# Read Team Tools



N4xd0rk

- Descubrimiento subdominios
- Obtención direccionamiento IP del target

```
Searching subdomains...

Subdomains rtve.es are:

loteria.rtve.es 77.2[REDACTED].64

www.rtve.es 77.[REDACTED].64

aquihaytrabajo.rtve.es 93.189.[REDACTED].5

loteria-nino.rtve.es [REDACTED].227.57

foroaguileroja.rtve.es 3.[REDACTED].0.56.118

lab.rtve.es 8.[REDACTED].126

juegocarlos.rtve.es 54.2[REDACTED].10

vocesdelamemoria.rtve.es 34.24[REDACTED].108

generation-what.rtve.es 77.2[REDACTED].41
```

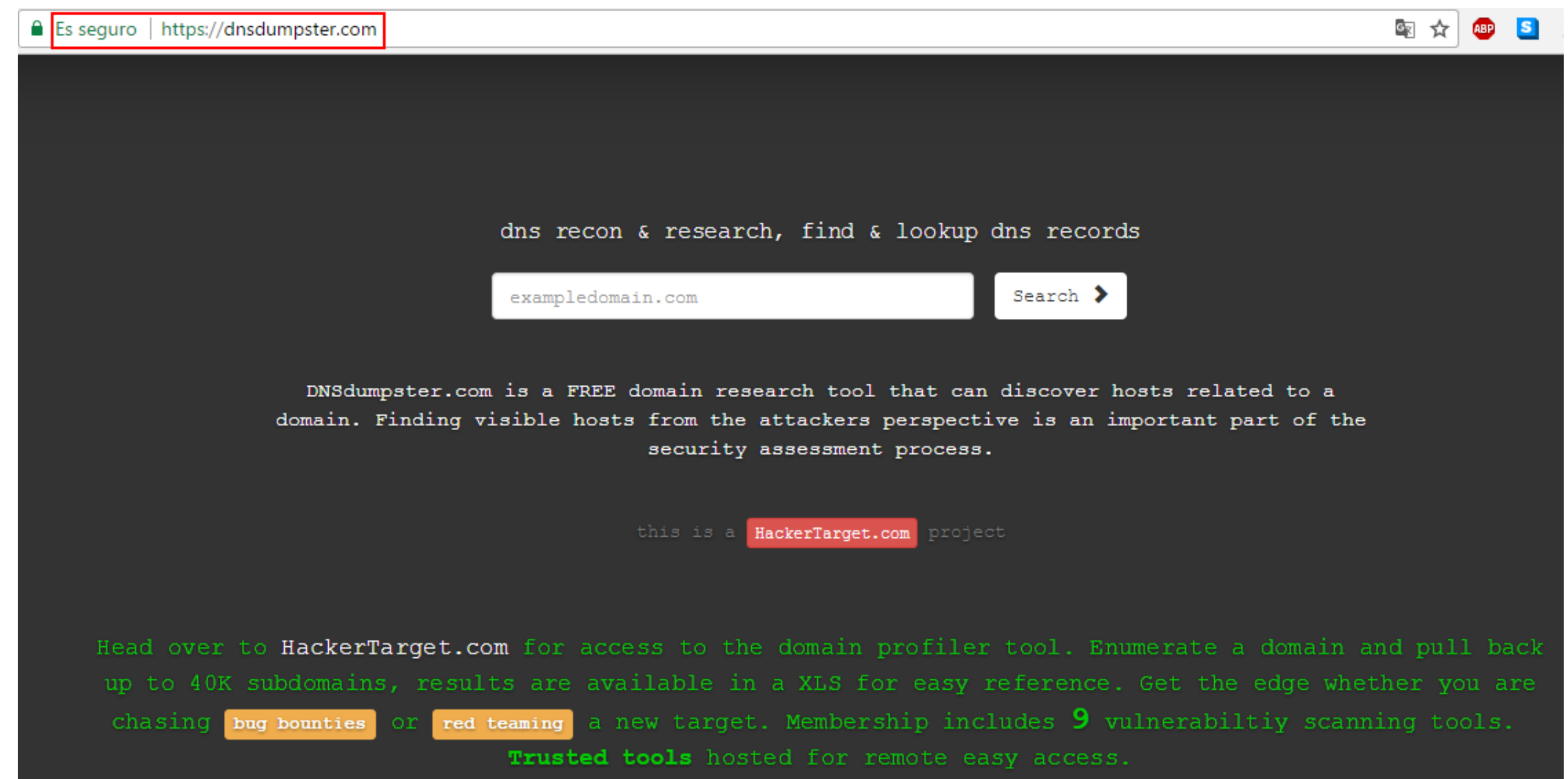
# Read Team Tools

Y empleando servicios online:

Manualmente ;(

Para listar dominios y subdominios:

**dnsdumper**





# Read Team Tools

## Sublist3r de about3la

Enumera subdominios de servicios web como Netcraft, Virustotal, ThreatCrowd, DNSdumpster y PassiveDNS. Posee el modulo subbrute para realizar fuerza bruta a través de un diccionario.

```
/Sublist3r# python sublist3r.py -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]]
                  [-t THREADS] [-e ENGINES] [-o OUTPUT]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file

Example: python sublist3r.py -d google.com
```



# Read Team Tools

## Herramientas listar subdominios

Sublist3r o Subbrute -> footprinting.

Knock -> activa: fingerprinting

Un gran inconveniente:

- ¿Los dominios/subdominios siguen vivos?
- ¿Comprobación manual? -> **NoDOM**

```
/n0D0m# python nod0m.py -h
NoDOM
** Tool to know the status code about a domain
** Author: Ignacio Brihuega Rodriguez a.k.a N4xh4ck5
** DISCLAIMER This tool was developed for educational goals.
** The author is not responsible for using to others goals.
** A high power, carries a high responsibility!
** Version 1.0
usage: nod0m.py [-h] -e EXPORT -i INPUT

This script verifies the domain status and exports the result in standar format

optional arguments:
  -h, --help            show this help message and exit
  -e EXPORT, --export EXPORT
                        Indicate the type of format to export results.
                        1.json (by default)
                        2.xlsx
  -i INPUT, --input INPUT
                        File in json format which contains the domains want to know their status
```





# Read Team Tools

## NoDOM



- Identificar dominios/subdominio “vivos”
- Identificar posibles redirección, necesidad de autenticación o no accesibles.

```
NoDOM

** Tool to know the status code about a domain
** Author: Ignacio Brihuega Rodriguez a.k.a N4xh4ck5
** DISCLAIMER This tool was developed for educational goals.
** The author is not responsible for using to others goals.
** A high power, carries a high responsibility!
** Version 1.0

{'200': [u'http://loteria.rtve.es/', u'http://www.rtve.es/', u'http://aquihaytrabajo.rtve.es/', u'http://loteria-nino.rtve.es/', u'http://foroaguilaroja.rtve.es/', u'http://www.rtve.es/lab/', u'http://juegocarlos.rtve.es/', u'http://vocesdelamemoria.rtve.es/', u'http://generation-what.rtve.es/', u'http://foroeltiempo.rtve.es/'], '300': [u'lab.rtve.es'], '404': [], '403': [], '401': [], '500': []}
Exporting the results in an excel
-----STADISTICS-----
Domains Up: 10
Domains Moved: 1
Domains Required Authorization: 0
Domains Forbidden: 0
Domains Not Found: 0
Domains Down: 0
```

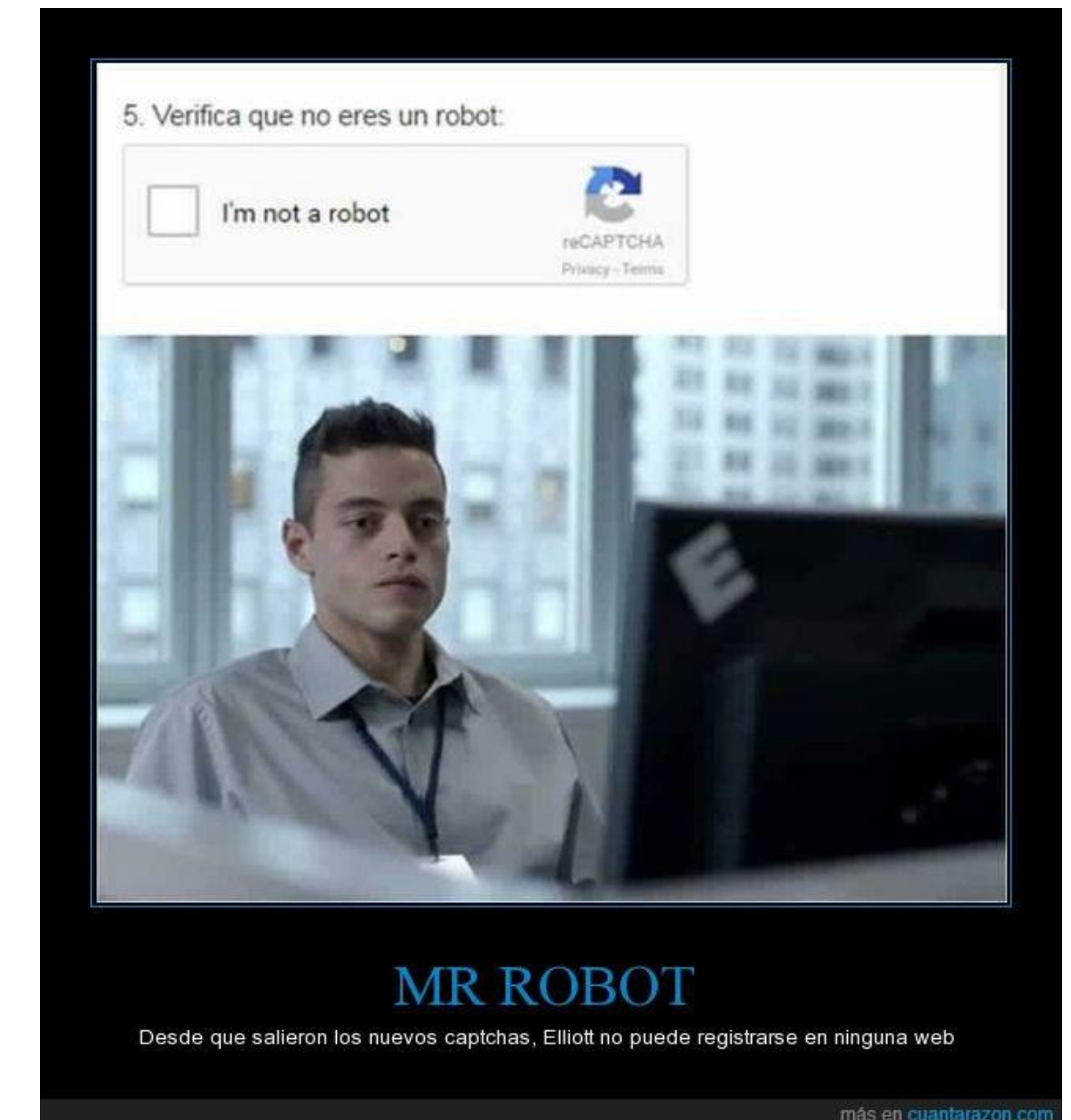


# Read Team Tools

## RastLeak



- Búsqueda de documentos ofimáticos.
- Site:TARGET (ext:pdf OR ext:doc OR ext:docx OR ext:xlsx OR ext:ppt)
- Necesidad de automatización **Rastleak**





# Read Team Tools

- **RastLeak:**



- Python 2.7
- Búsqueda de documentos ofimáticos indexados empleado Google y Bing.
- Extracción y análisis de metadatos.
- Reporte de resultados.

```
/RastLeak# python rastleak.py -h
usage: rastleak.py [-h] -d DOMAIN -o OPTION -n SEARCH -e EXT [-f EXPORT]

This script searches files indexed in the main searches of a domain to detect a possible leak information

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        The domain which it wants to search
  -o OPTION, --option OPTION
                        Indicate the option of search
                        1.Searching leak information into the target
                        2.Searching leak information outside target
  -n SEARCH, --search SEARCH
                        Indicate the number of the search which you want to do
  -e EXT, --ext EXT      Indicate the option of display:
                        1-Searching the domains where these files are found
                        2-Searching ofimatic files
  -f EXPORT, --export EXPORT
                        Indicate the type of format to export results.
                        1.json (by default)
                        2.xlsx
```





# Read Team Tools

- **RastLeak:**



- Obtención de posibles usuarios.
- Obtención SSOO y software
- Obtención licencias de código -> Auditoría de licencias

## METADATA RESULTS BY CATEGORY

#####

Users - Documents Author  
Mov [REDACTED]

Administrador  
cristian. [REDACTED] a  
blancab

#####

### Producer

Microsoft® Word 2010  
Mac OS X 10.12.1 Quartz PDFContext

Microsoft® Office Word 2007  
doPDF Ver 8.0 Build 908  
Acrobat Distiller 10.1.7 (Windows)

#####

### Creator

Microsoft® Word 2010  
Chrome

Microsoft® Office Word 2007  
PScript5.dll Version 5.2.2



# Read Team Tools

## CMSsc4n:



- Python 2.7
- Identificación de CMS: Wordpress, Moodle, Drupal, Joomla y Prestashop
- Orientada fingerprinting
- CMS tienen numerosas vulnerabilidades potenciales si no se encuentran actualizados

```
/CMSs4cn# python cmssc4n.py -h

CMSsc4n

** Tool to scan if a domain is a CMS (Wordpress , Drupal, Joomla, Prestashop or Moodle) and return the version
** Author: Ignacio Brihuega Rodriguez a.k.a N4xh4ck5
** Version 1.0
** DISCLAIMER This tool was developed for educational goals.
** The author is not responsible for using to others goals.
** A high power, carries a high responsibility!
usage: cmssc4n.py [-h] -e EXPORT -i INPUT

This tool verifies if the domain is a CMS (Wordpress , Drupal, Joomla, Prestashop or Moodle) and returns the version

optional arguments:
  -h, --help            show this help message and exit
  -e EXPORT, --export EXPORT
                        Indicate the type of format to export results.
                        1.json (by default)
                        2.xlsx
  -i INPUT, --input INPUT
                        File in json format which contains the domains want to know if they are a CMS
```



# Read Team Tools

# CMSSc4n:



- **Categorización de dominios que sean CMS.**
- **Identificación de versión de CMS siempre que sea posible.**

```
gtgeneration.com
*****Checking if the CMS is a Wordpress*****
wp-content detected in main webpage. Trying to detect the wordpress version
Version Wordpress detected in source font => 4.7.5
gtgeneration.com is wordpress

thehackingfactory.com
*****Checking if the CMS is a Wordpress*****
wp-content detected in main webpage. Trying to detect the wordpress version
Version Wordpress detected in source font => 4.7.5
thehackingfactory.com is wordpress

fwhibbit.es
*****Checking if the CMS is a Wordpress*****
wp-content detected in main webpage. Trying to detect the wordpress version
It can't detect the wordpress version
fwhibbit.es is wordpress
```

# Read Team Tools

## Objetivos:

- Identificación de dominios y subdominios.
- Identificación direccionamiento IP.
- Obtención de dominios/subdominios en hosting
- Identificación dominios que son CMS -> Vulnerabilidades, exploits, ...
- Obtención de posibles usuarios -> Intruder, Hydra, Medusa,...
- Obtención de SSOO, software, correos electrónicos, ...

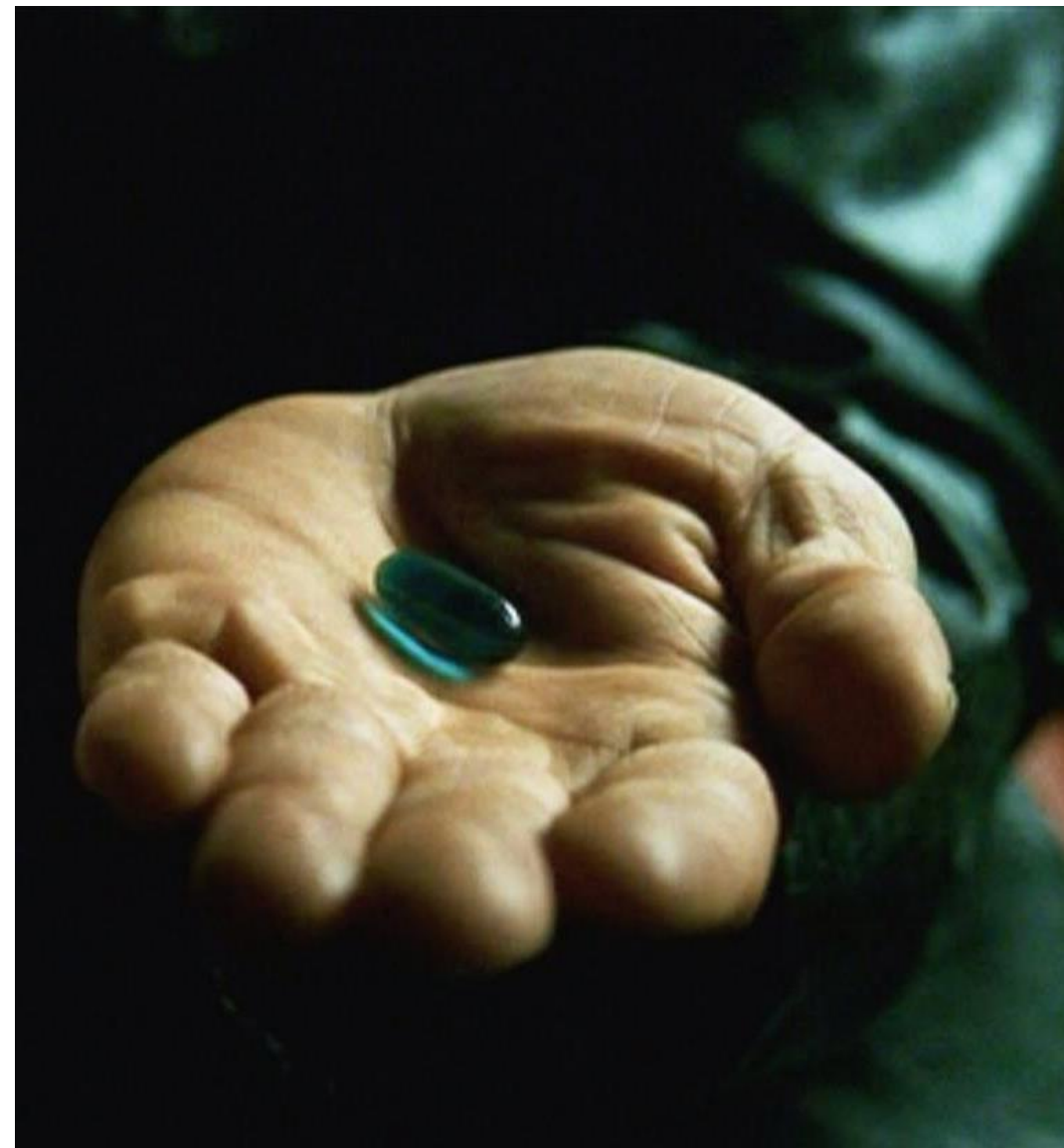


1. Whoami
2. Red Team tools
- 3 .Blue Team tools



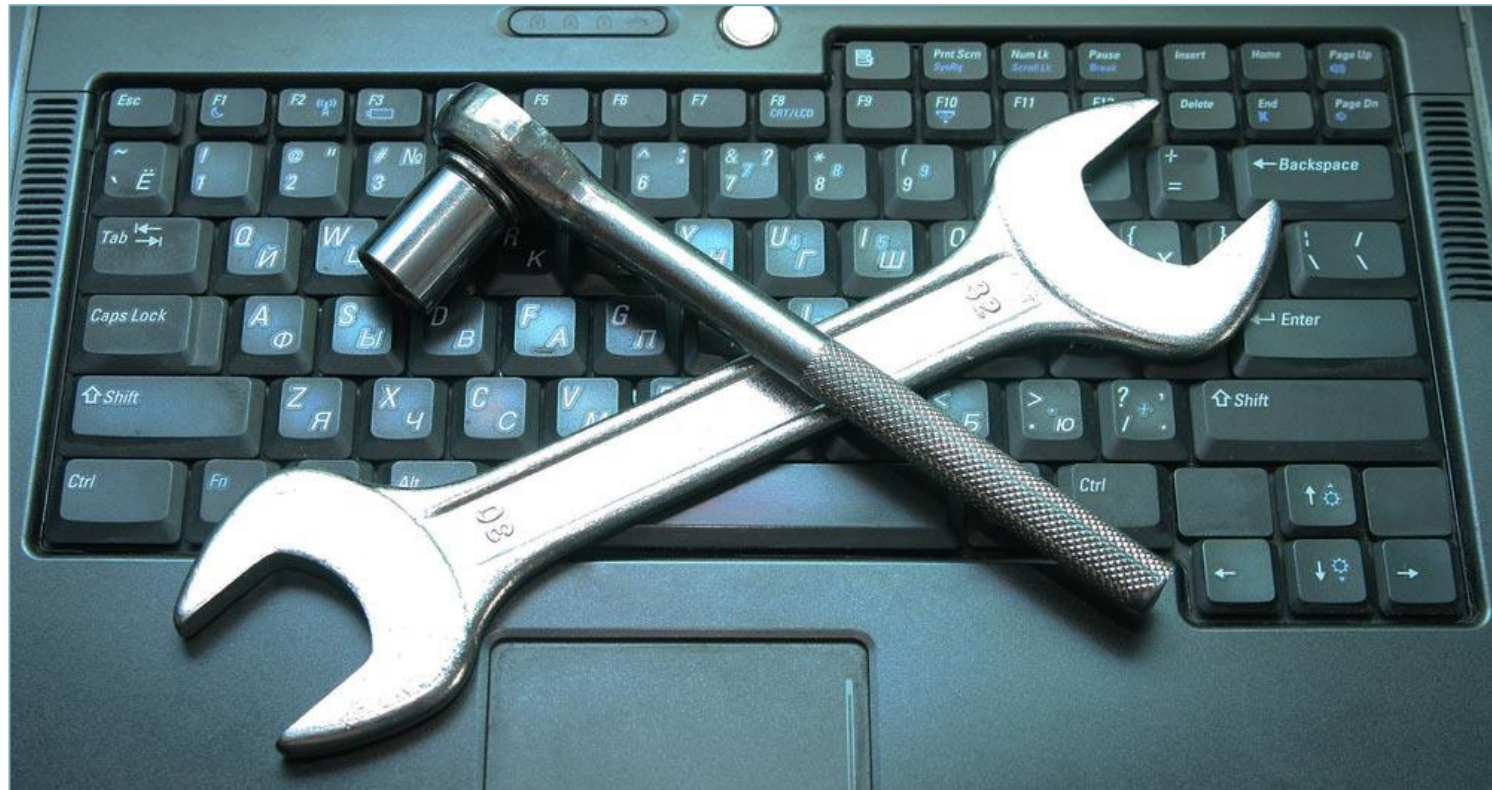
# Blue Team Tools

Automatización de tools para prevenir fraude online,  
identificar recursos expuestos en Internet



# Blue Team Tools

## Objetivos:



## Tools para:

- Detectar los recursos disponible en Internet.
- Identificar fuga de información: Indexación de documentos
- Identificar de manera proactiva fraude online: phishing, abuso de marca y ciber/typosquatting



## Blue Team Tools

- N4xD0rk
- RastLeak
- Find0



## RastLeak



## Blue Team Tools

- Python 2.7
- Opción 2 -> Identificar ficheros indexados en dominios que no pertenece a target -> Posible fuga de info indexada

```
# python find0.py -h
usage: find0.py [-h] -t TARGET

This script gets domains in sold about a target

optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        The keyword which it wants to search
```



## Blue Team Tools

### find0

- Python 2.7
- Listar dominios registrados en venta.
- Identificar posible abuso de marca a través de parking de dominios



```
# python find0.py -h
usage: find0.py [-h] -t TARGET

This script gets domains in sold about a target

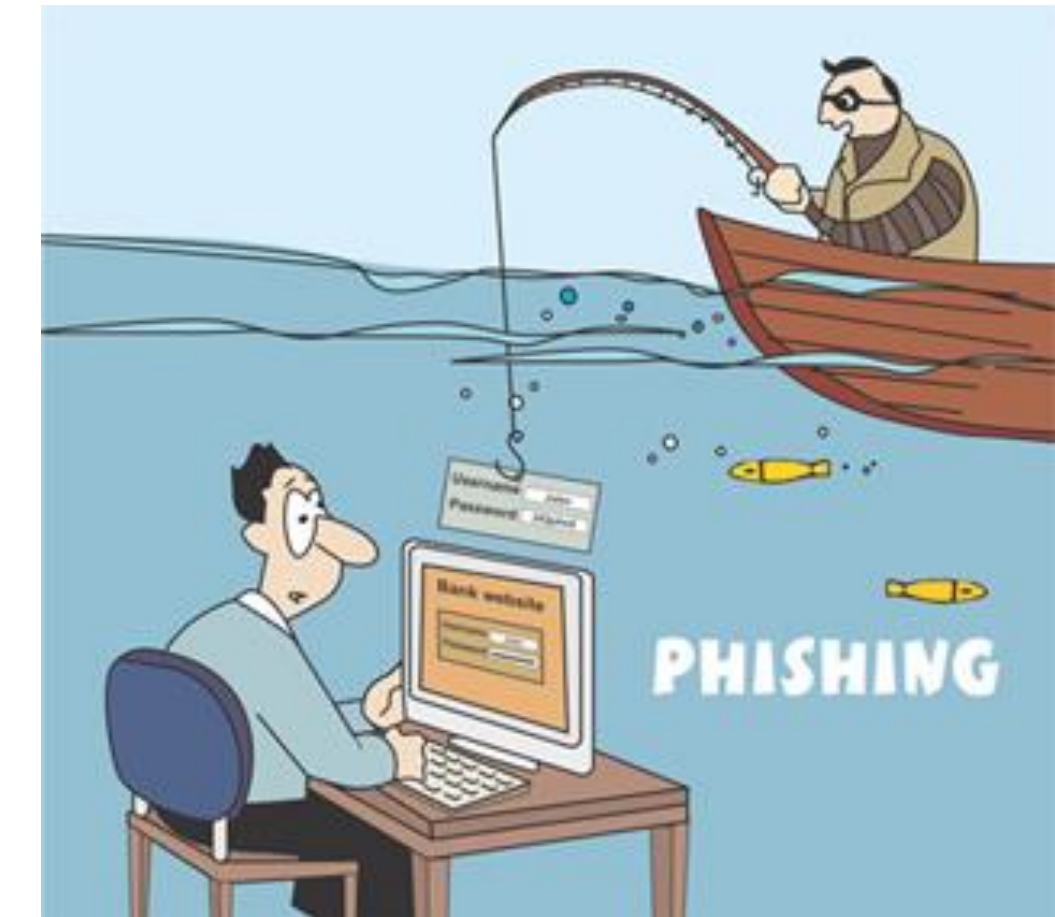
optional arguments:
  -h, --help            show this help message and exit
  -t TARGET, --target TARGET
                        The keyword which it wants to search
```



# Blue Team Tools

Tools para identificar phishing de manera proactiva:

Heimdal – Motor de detección de fraude temprano (Heimdal) – Track A 18-19h



Cybersquatting (es) -

<http://cyber.squatting.es/>

Cybersquatting [ es ] [SOBRE EL PROYECTO](#)

Introduce el nombre dominio a analizar (sin TLD .es)

Distancia entre letras ▼

Porcentaje de similitud ▼

De 1 a 10 caracteres similares

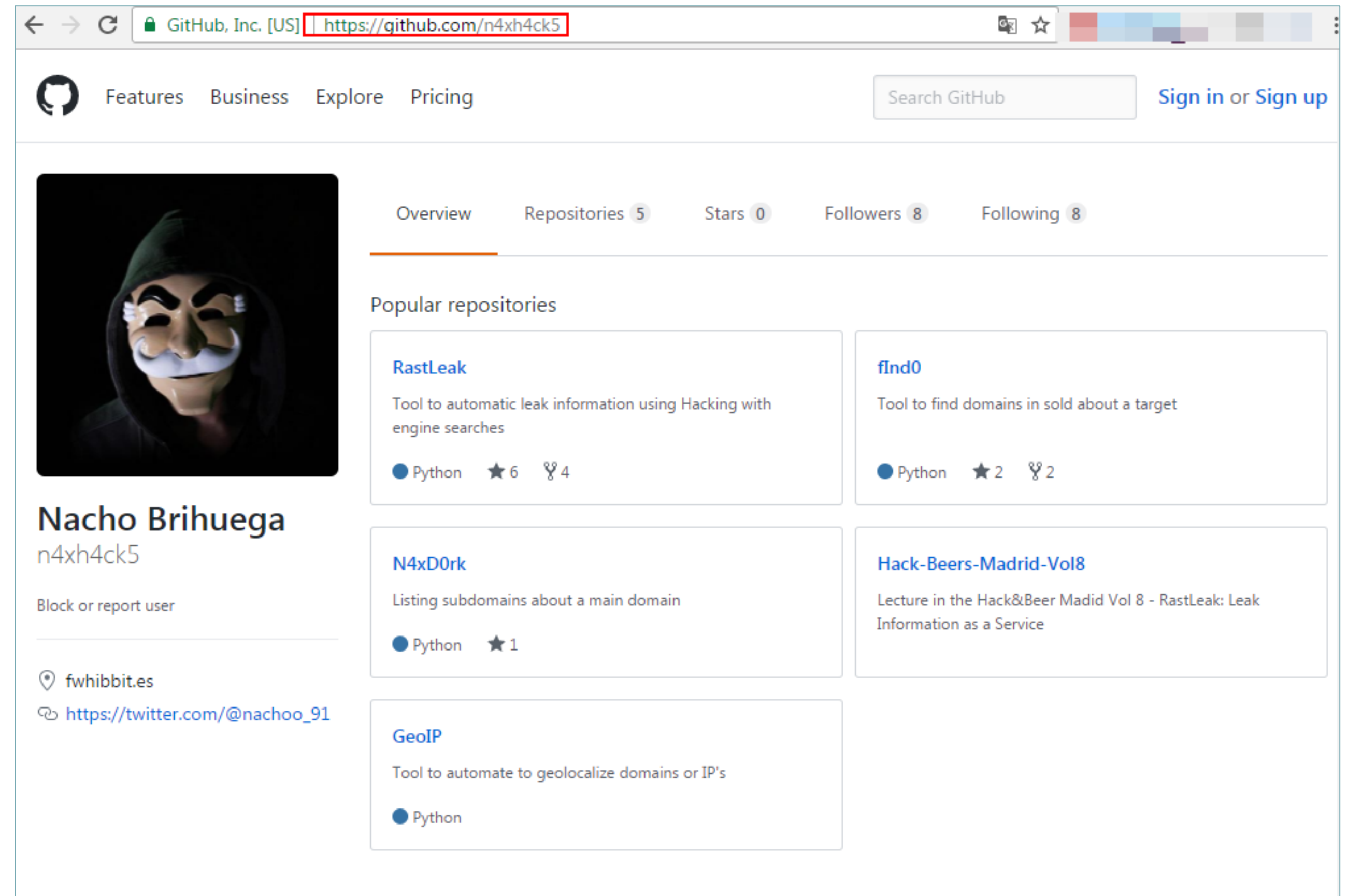


Copyright © 2016 Cybersquatting.es - Servicio gratuito de análisis de Cybersquatting en TLD .es

# Referencias

Las tools de desarrollo propio mostradas están o estarán en mi github:

<https://github.com/n4xh4ck5>



# Referencias

<https://github.com/n4xh4ck5>

<https://github.com/aboul3la/Sublist3r>

<https://www.fwhibbit.es/n4xd0rk-anonimizando-el-descubrimiento-de-subdominios>

<http://www.hackplayers.com/2017/02/recopilatorio-para-descubrimiento-subdominios.html>

<http://cyber.squatting.es/>



# RUEGOS Y PREGUNTAS





# MUCHAS GRACIAS

