TODO SOBRE MI OBJETIVO

Ignacio Brihuega Rodríguez (N4xh4ck5)

EastMadH4ck 2017

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

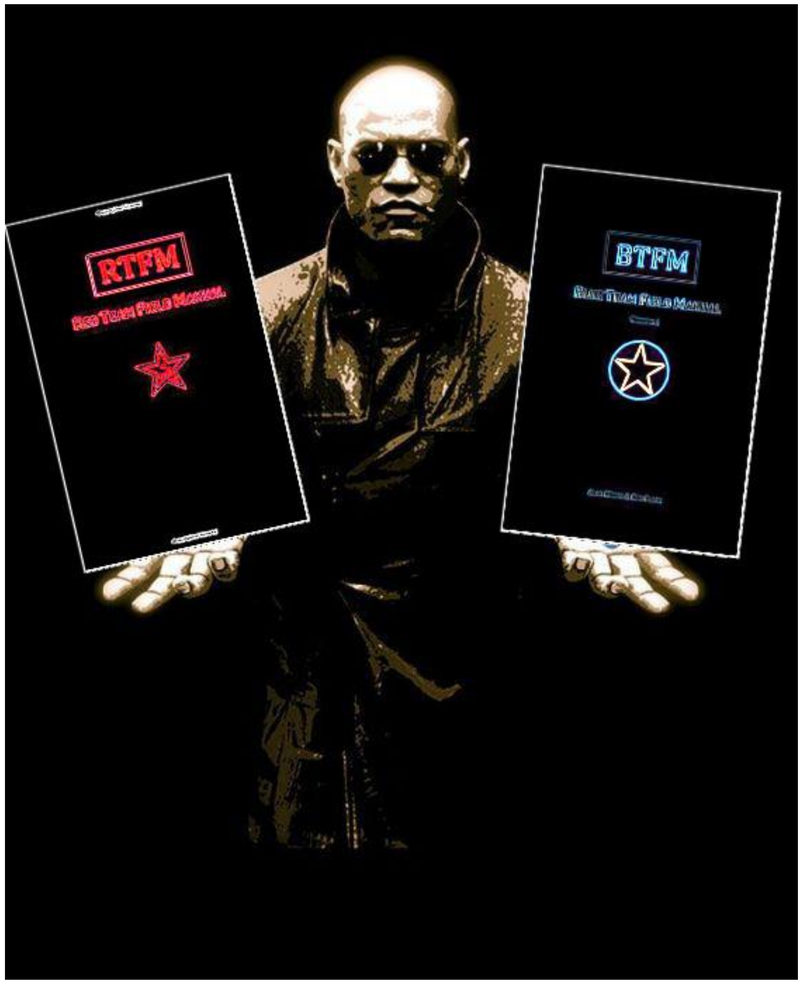
1. Whoami
2. Red Team tools
3. Blue Team tools

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
- Info contacto:
    - **Linkedin**: Ignacio Brihuega Rodríguez
    - **Twitter**: 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

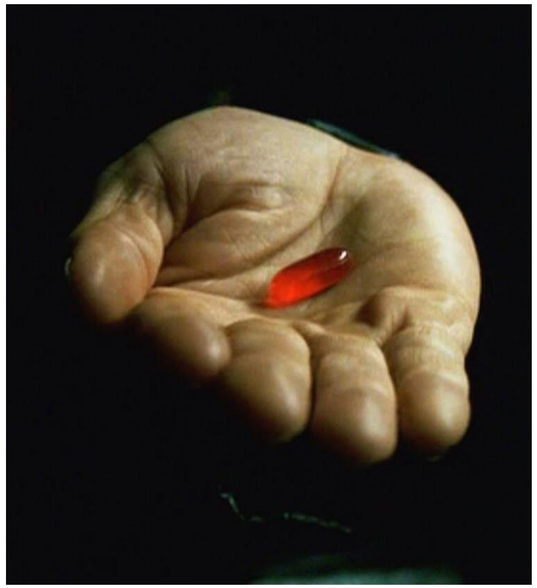
- **Tools para recoger información pública de un target con objeto de ser empleado para un test de intrusión.**

- **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

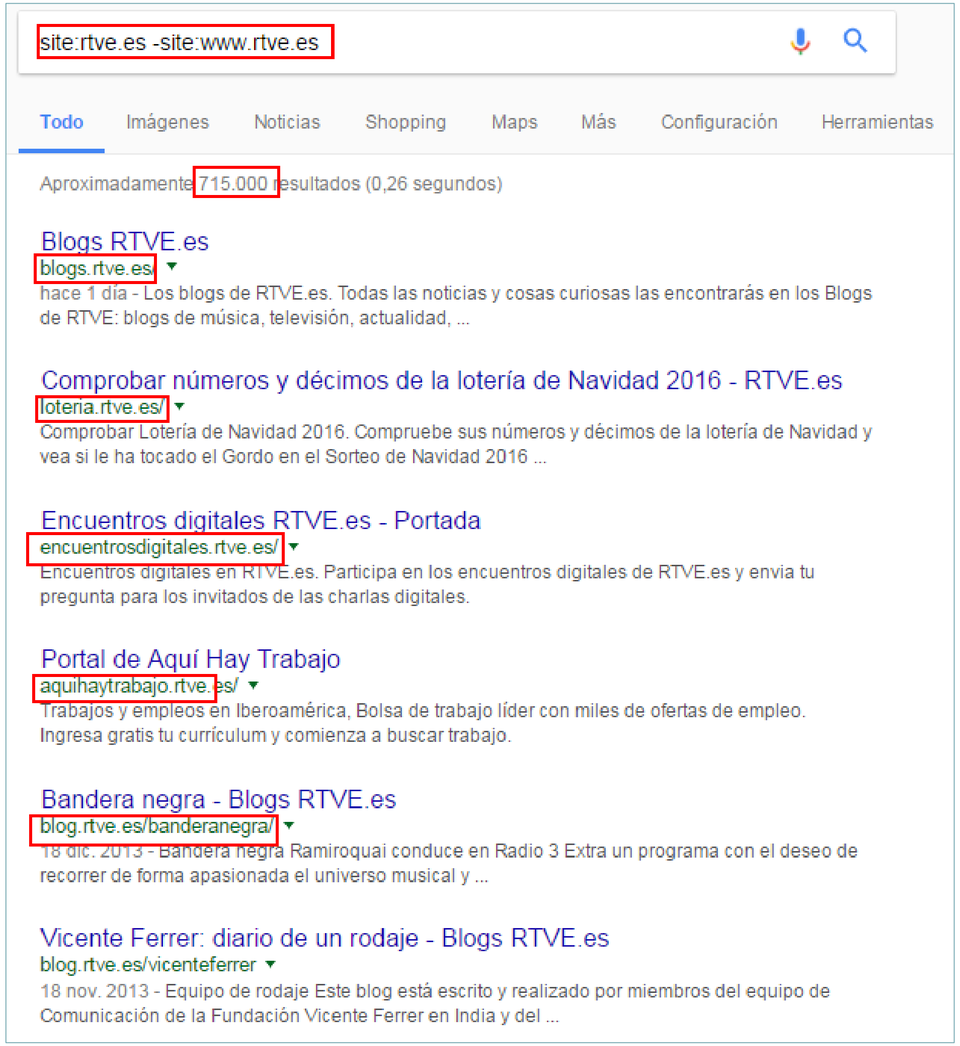
- Th4sD0m
- N4xD0rk
- n0d0M
- CMsSc4n
- RastLeak

Read Team Tools

Google

¿Por dónde empezamos?

site:rtve.es –site:www.rtve.es



Read Team Tools

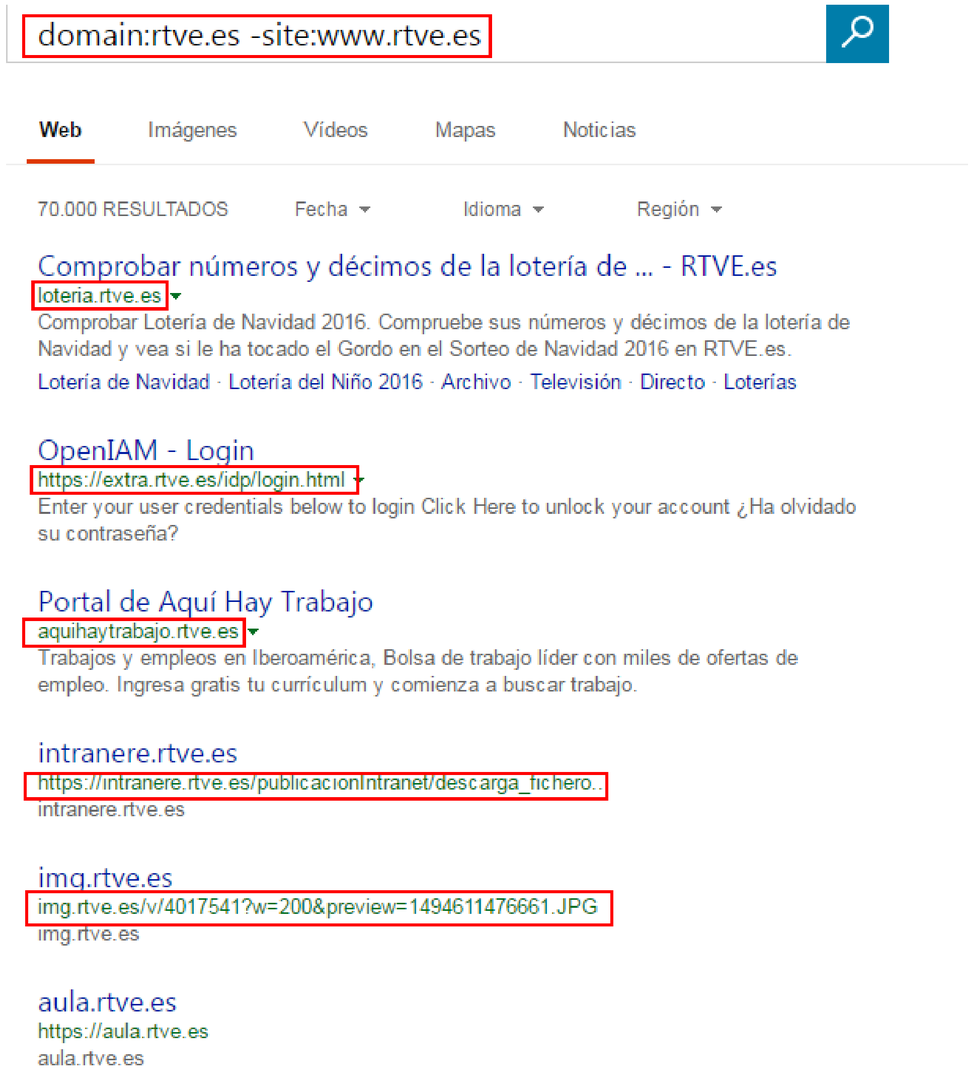
¿subdominios? -> **Bing: domain:rtve.es**

-> Automatizando: **N4xD0rk**

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

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

bing



Read Team Tools

Th4sD0m

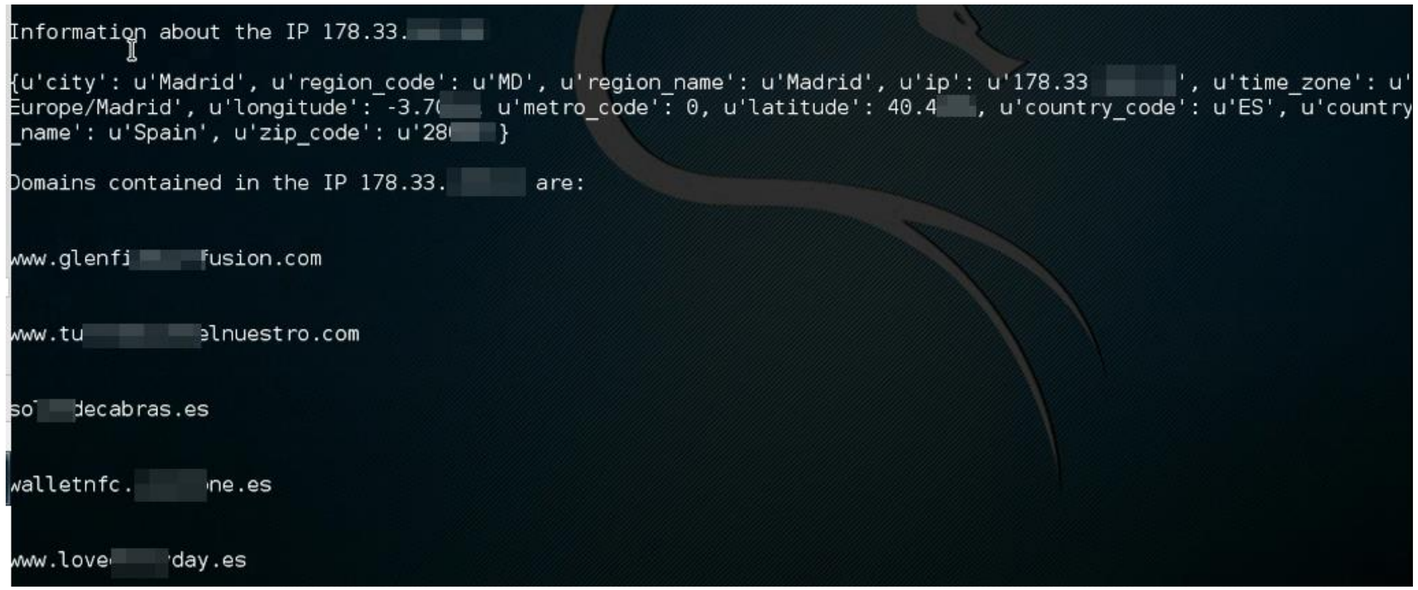
- Python 2.7
- Listar dominios contenidos en una IP de manera anónima.

```
 _____ _  _  ___  ___  ___  _ __
|_  / | || |/ __|/ _ \/ _ \| '_ \
 / /| | || |\__ \ (_) | (_) | | | |
/___|_|_||_||___/\___/ \___/|_| |_|

** Tool to identify all domains contained in an IP
    ** Author: Ignacio Brihuega Rodriguez a.k.a N4xh4ck5
    ** DISCLAMER 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: th4sd0m.py [-h] -i IP -n NUM [-e EXPORT]

This script identifies all domains contained in an IP

optional arguments:
  -h, --help            show this help message and exit
  -i IP, --ip IP        The IP which wants to search
  -n NUM, --num NUM     Indicate the number of the search which you want to do
  -e EXPORT, --export EXPORT
                        Export the results to a json file (Y/N)
```

Read Team Tools

Th4sD0m

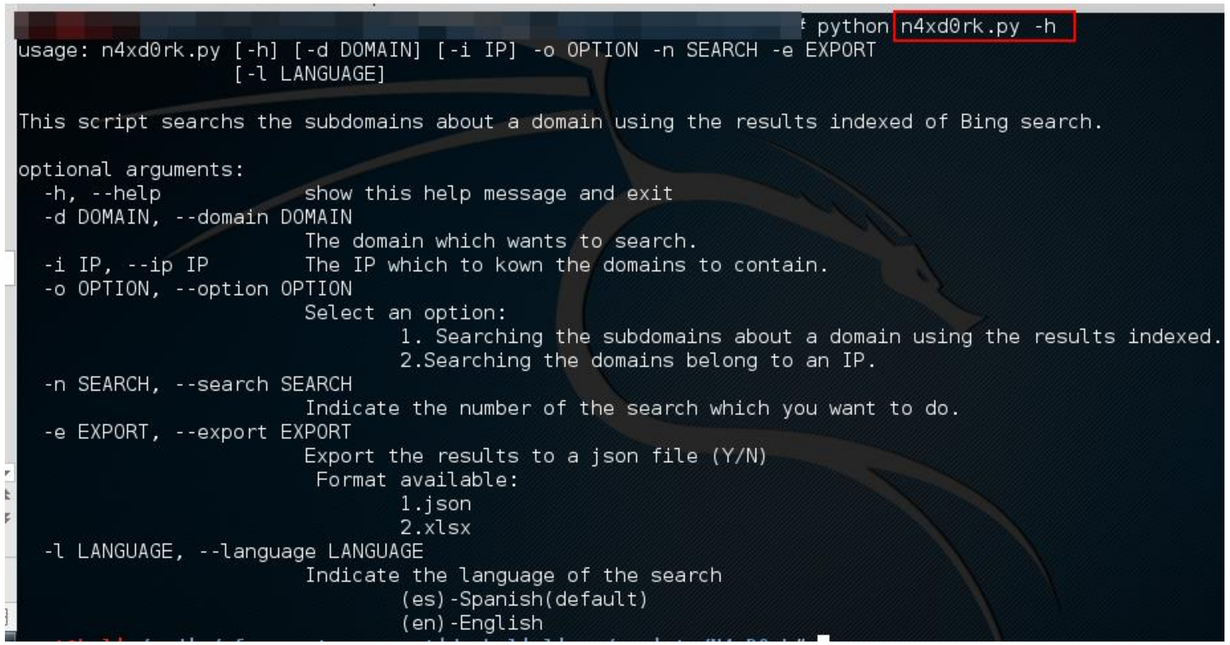
- Determinar el alcance de la intrusión.
- Conocer si el target se encuentra en un hosting o es un servidor dedicado



Read Team Tools

N4xd0rk

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



Read Team Tools

N4xd0rk

- Descubrimiento subdominios
- Obtención direccionamiento IP del target

```
Searching subdomains...

Subdomains rtve.es are:

loteria.rtve.es 77.1      .64

www.rtve.es 77.1      .64

aquihaytrabajo.rtve.es 93.189.      5

loteria-nino.rtve.es      .227.57

foroaguilaroja.rtve.es 3      0.56.118

lab.rtve.es 8.1      .126

juegocarlos.rtve.es 54.2      .10

vocesdelamemoria.rtve.es 34.24      .108

generation-what.rtve.es 77.2      .41
```

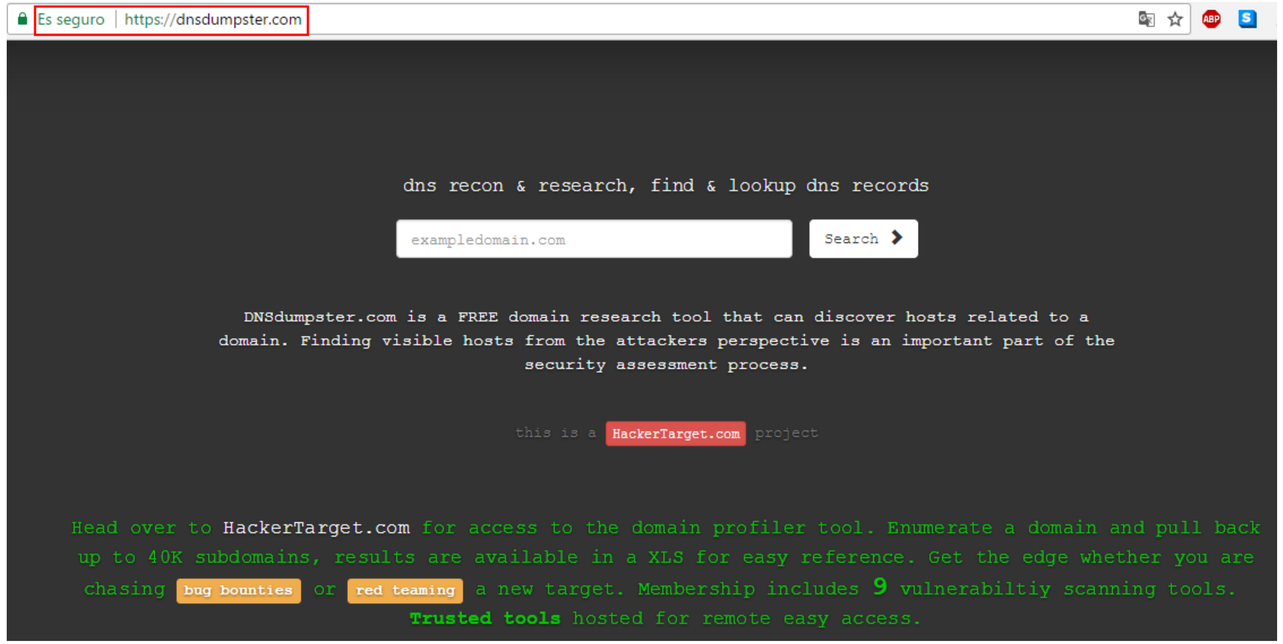
Read Team Tools

Y empleando servicios online:

Manualmente ;(

Para listar dominios y subdominios:

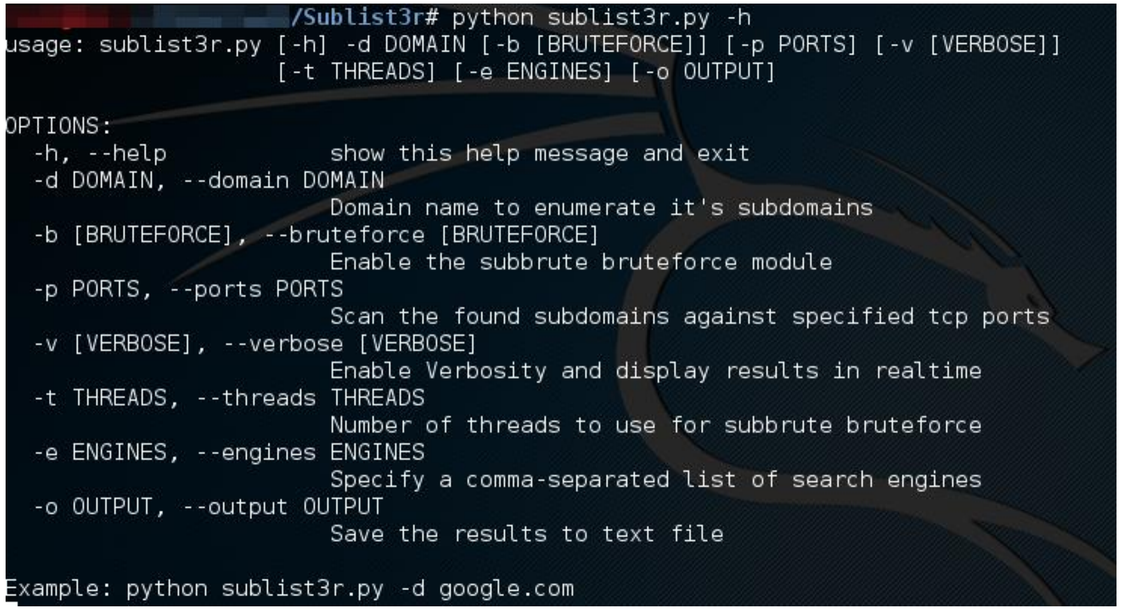
dnsdumpter



Read Team Tools

Sublist3r de aboul3la

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.



Read Team Tools

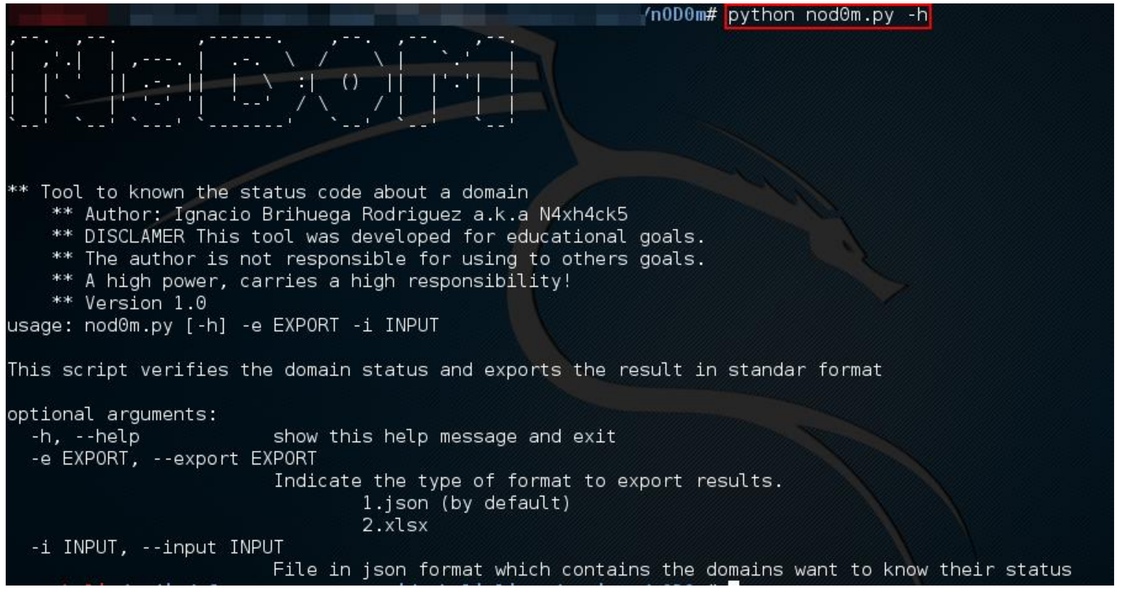
Herramientas listar subdominios

Sublist3r o Subbrute -> footprinting.

Knock -> activa: fingerprinting

Un gran inconveniente:

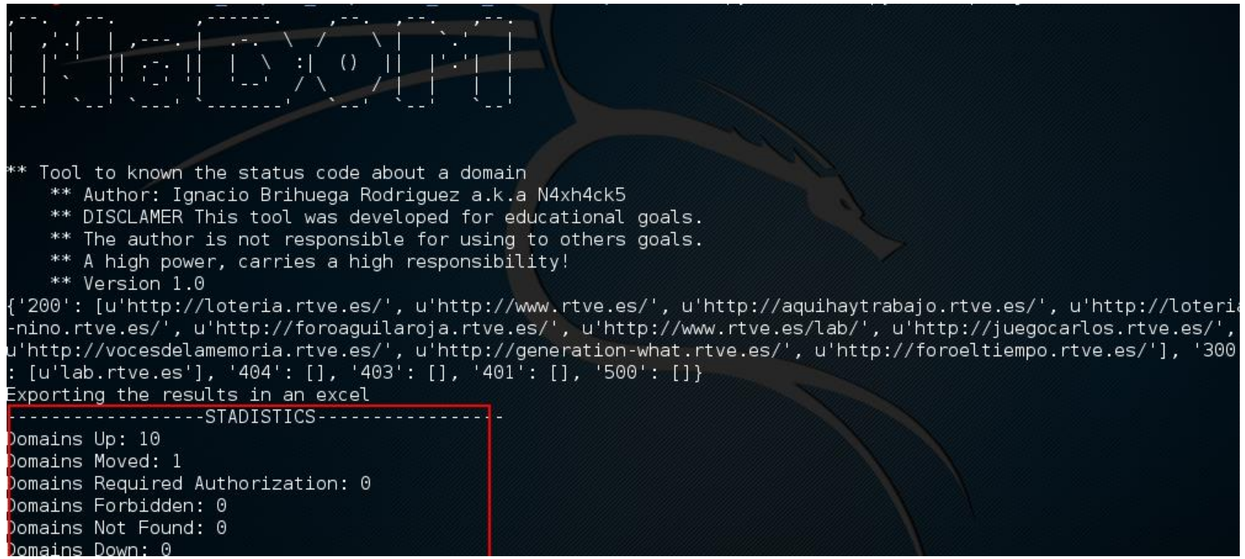
- **¿Los dominios/subdominios siguen vivos?**
- **¿Comprobación manual? -> NoDOM**



Read Team Tools

NoD0M

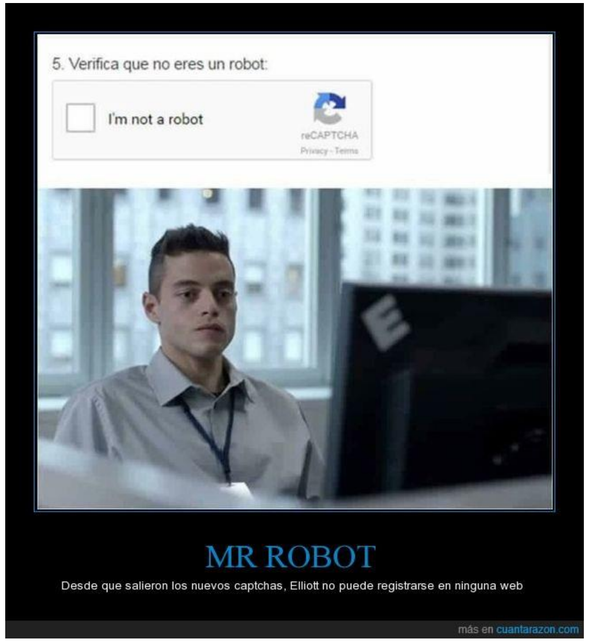
- Identificar dominios/subdominio “vivos”
- Identificar posibles redirección, necesidad de autenticación o no accesibles.



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 searchs 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**:

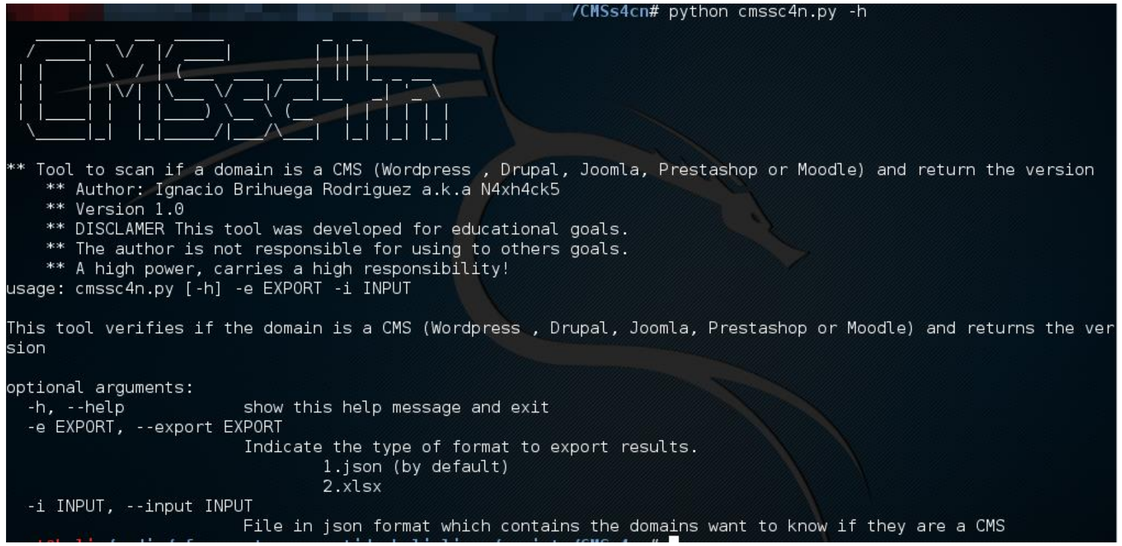
- Obtención de posibles usuarios.
- Obtención SSOO y software
- Obtención licencias de código -> Auditoría de licencias

```
METADATA RESULTS BY CATEGORY

##############################################

Users - Documents Author
        Mo[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



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:

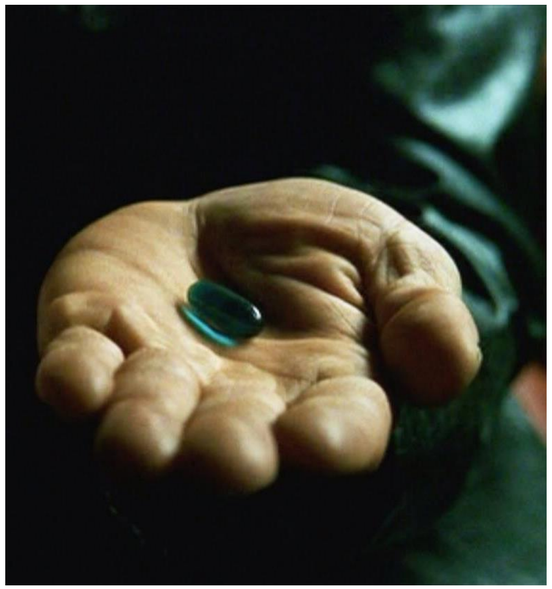
- Identificación de dominios y subdominios.
- Identificación direccionamiento IP.
- Obtención de dominios/subdominios en hosting
- Identificación dominios que son CMS -> Vulnerabilidades, exploits, …
- Obtención de posibles usuarios -> Intruder, Hydra, Medusa,…
- Obtención de SSOO, software, correos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

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

Blue Team Tools

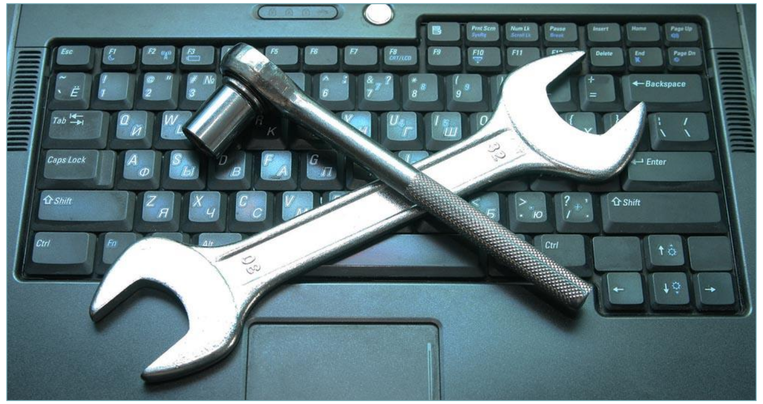
Automatización de tools para prevenir fraude online,

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/typosquating**

Blue Team Tools

- N4xD0rk
- RastLeak
- Find0

Blue Team Tools

RastLeak

- 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:

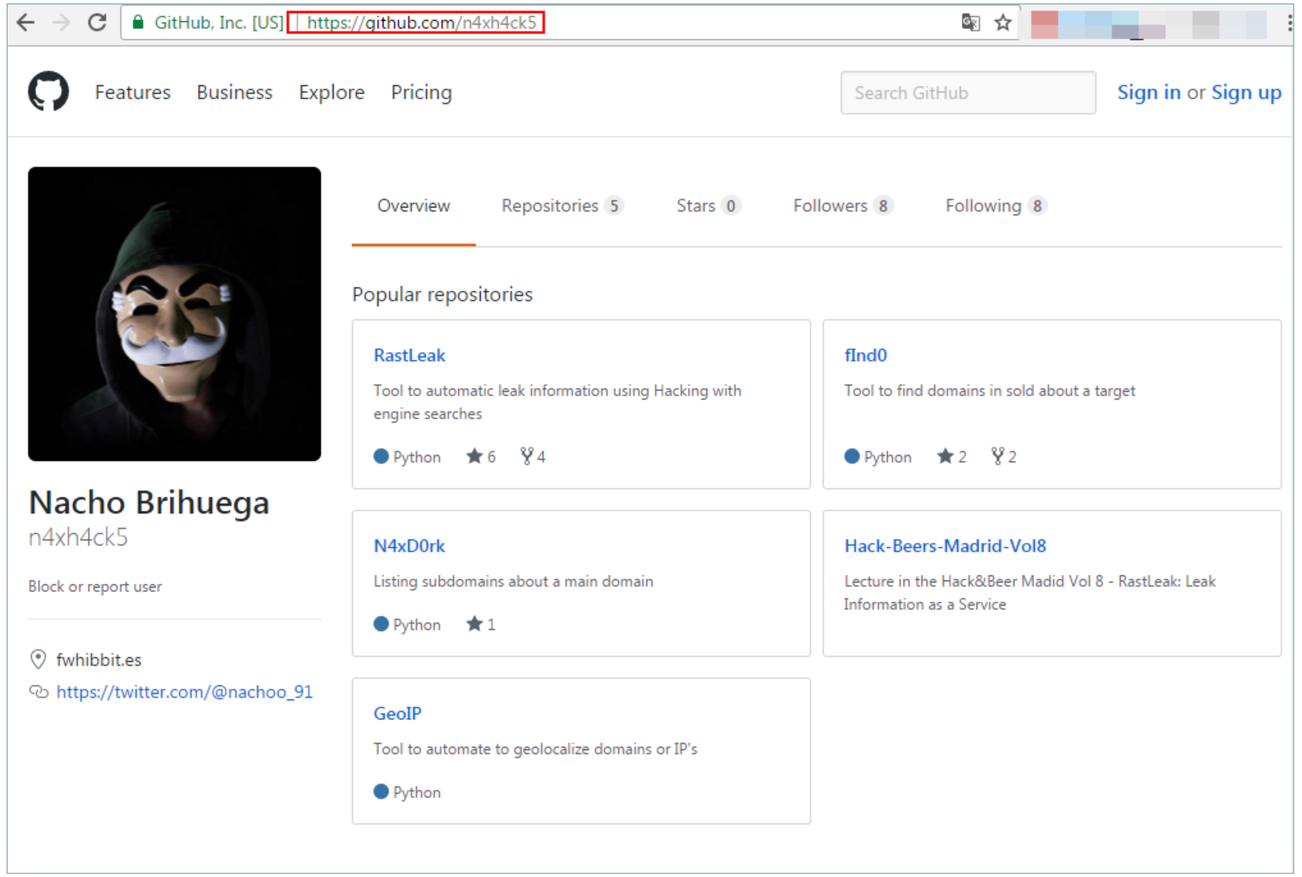
Heimdal – Motor de detección de fraude temprano (Heimdal) – Track A 18-19h

Cybersquating (es) - http://cyber.squatting.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