



# Dev-Pentest

Ignacio Brihuega / Álvaro Macías



# ÍNDICE

- Whoami
- Motivación
- Pasando al ataque
- Reconocimiento y recolección de información.
- Explotación y postexplotación
- Referencias

# ÍNDICE

- Whoami
- Motivación
- Pasando al ataque
- Reconocimiento y recolección de información.
- Explotación y postexplotación
- Referencias

# Whoami: Nacho Brihuega

- Coordinador técnico de hacking en ElevenPaths Cybersecurity Professional Service en Telefónica.
- Graduado en Ingeniería en Tecnologías de la Telecomunicación, especialidad en ingeniería telemática (UAH)
- Máster en Seguridad Informática (UNIR).
- Coautor en blog “Follow the White Rabbit”.
- @n4xh4ck5 / @naxhack5

*Telefónica*



## *Whoami: Álvaro Macías*

- Técnico superior en administración de sistemas en red.
- Co-fundador del blog “Follow the White Rabbit”. @naivenom
- Offensive Security Certified Professional (OSCP).
- Reverse engineer en mi tiempo libre.



# DISCLAIMER

- La información que se va a mostrar es de carácter público.
- Se ofuscará la mayor parte de las ocasiones para no mostrar el origen de la información.
- Las técnicas demostradas son para fines académicos, no nos hacemos responsables de su uso para otros fines.
- Hack&Learn&Share



# ÍNDICE

- Whoami
- Motivación
- Pasando al ataque
- Reconocimiento y recolección de información.
- Explotación y postexplotación
- Referencias

# MOTIVACIÓN

El objetivo del taller Dev-Pentest es describir el proceso de un pentesting desde la recolección de información hasta el compromiso y post-explotación de una máquina aplicando herramientas de desarrollo propio. El enfoque que se quiere transmitir a los asistentes son las ventajas de programar sus propias herramientas como mecanismo de aprendizaje y no depender exclusivamente de desarrollos de terceros.

En la segunda parte del taller, se profundizará en tareas de ingeniería inversa de software vulnerable en busca de algún bug y su posterior explotación.





# ÍNDICE

- Whoami
- Motivación
- Pasando al ataque
- Reconocimiento y recolección de información.
- Explotación y postexplotación
- Referencias

# PASANDO AL ATAQUE

- Escenario: Realizar un Pentesting dentro de un servicio de Red Team
- Seleccionar target.
- Fases:
  - Reconocimiento y recolección de información.
  - Explotación
  - Postexplotación

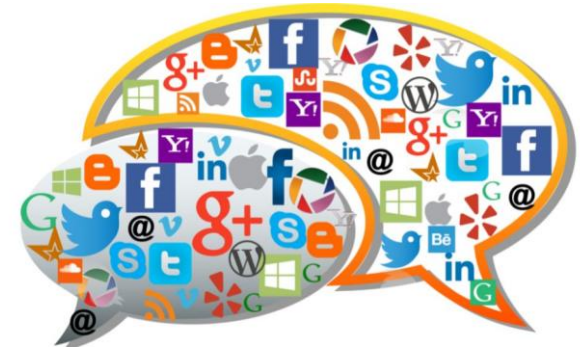


# ÍNDICE

- Whoami
- Motivación
- Pasando al ataque
- Reconocimiento y recolección de información.
- Explotación y postexplotación
- Referencias

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN

- Se divide en dos fases:
  - Reconocimiento pasivo: **Footprinting**. Obtención de información de forma pasiva.
  - Reconocimiento activo: **Fingerprinting**. Escaneo o enumeración de forma activa, es decir, existe interacción directa con el target.
- Objetivo: Obtener un mapa de red y visibilidad para **perfilar la superficie de ataque**



Fuente:

<http://www.expansion.com/economia-digital/innovacion/2016/01/03/5682714e22601da00f8b4635.html>

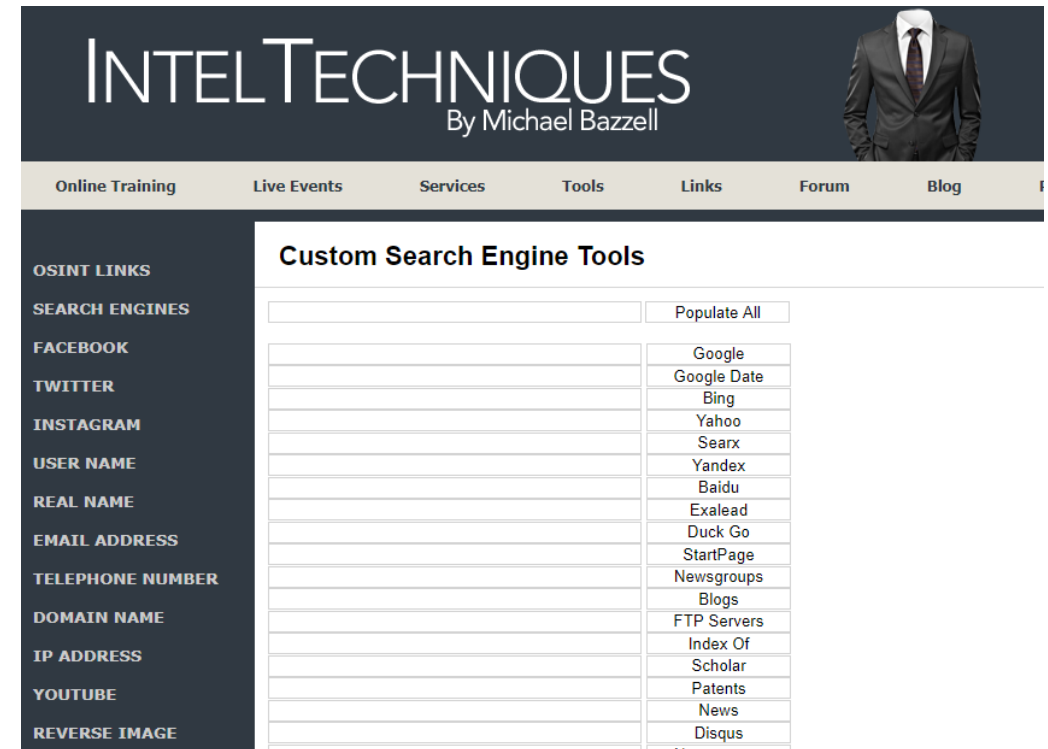
# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN

- Identificar IP's
- Identificar dominios para esas IP's.
- Identificar subdominios.
- Descubrimiento de puertos y servicios.
- Análisis e identificación de tecnología.
- Búsqueda de resultados indexados...
- Descubrimiento de contenidos: rutas por defecto, usuarios, formularios de login,..

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting - OSINT

Búsqueda del target en motores de  
búsqueda

<https://inteltechniques.com/menu.html>



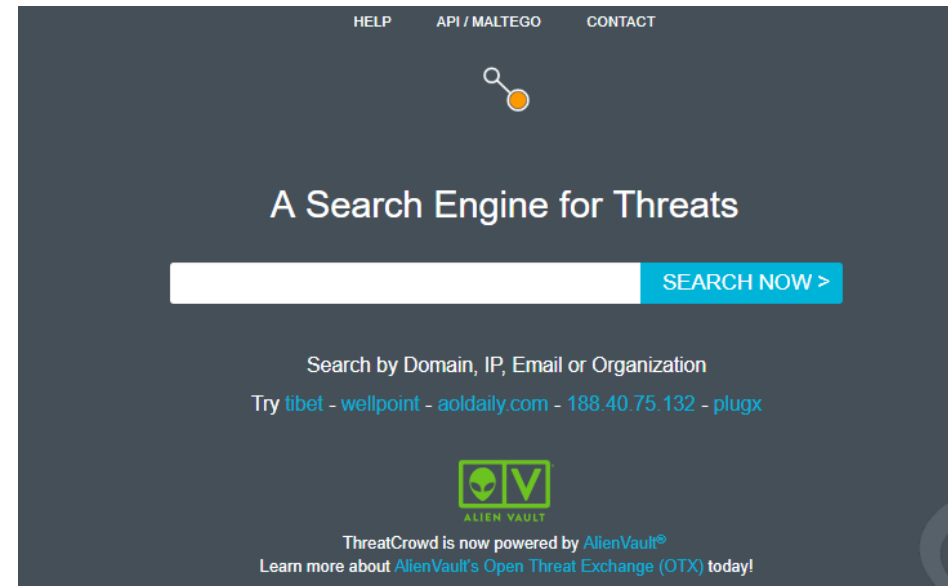
The screenshot shows the IntelTechniques website header with the title "INTELTECHNIQUES By Michael Bazzell" and a navigation menu including "Online Training", "Live Events", "Services", "Tools", "Links", "Forum", and "Blog". Below the header is a sidebar with "OSINT LINKS" and a main content area titled "Custom Search Engine Tools". The sidebar lists various search categories: SEARCH ENGINES, FACEBOOK, TWITTER, INSTAGRAM, USER NAME, REAL NAME, EMAIL ADDRESS, TELEPHONE NUMBER, DOMAIN NAME, IP ADDRESS, YOUTUBE, and REVERSE IMAGE. The "Custom Search Engine Tools" section features a table with a search input field and a "Populate All" button. The table lists various search engines and services:

Search Engine	Populate All
	Google
	Google Date
	Bing
	Yahoo
	Searx
	Yandex
	Baidu
	Exalead
	Duck Go
	StartPage
	Newsgroups
	Blogs
	FTP Servers
	Index Of
	Scholar
	Patents
	News
	Disqus



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting - OSINT

- Búsqueda de dominios, IP's, nombre de la compañía,...en los principales servicios online:
  - **Robtex** - <https://www.robtex.com>
  - **Reverse Report** - <https://reverse.report/>
  - **Ipv4info** - <http://ipv4info.com/>
  - **Crowd** - <https://www.threatcrowd.org/>



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting - OSINT

- **Servicios online de geolocalización o histórico**
  - Domain Tools - <http://domaintools.com/> - captcha
  - MX Toolbox: <http://mxtoolbox.com/>
  - Ultra tools - <https://www.ultratools.com/>
  - GeoIP - <http://freegeoip.net>
  - DB-IP - <https://db-ip.com/>
  - Archive - <https://archive.org/>
  - ViewDNS - <http://viewdns.info/>
  - Virustotal – IP [www.virustotal.com/en/ip-address/](http://www.virustotal.com/en/ip-address/)





# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting - OSINT

- Boletín oficial del Estado (BOE): <https://www.boe.es>
- Boletín Oficial de Registro Mercantil (BORME):  
<https://libreborme.net/>
- **Redes profesionales:** LinkedIn – Listado de empleados, clientes, cuentas de correo, ...
- **Redes sociales:** Facebook, Twitter, Instagram,...
- **Foros de desarrolladores:** Stackoverflow, canales telegram ,...
- **Foros privados:** Pastebin, Reddit, Forocoches, ...



Telegram



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN:

## Footprinting - OSINT

### Tools específicas para

- InSpy
- LinkedIn2username
- ScapedIn

```
/InSpy# python InSpy.py -h
usage: InSpy.py [-h] [-v] [--techspy [file]] [--limit int] [--empspy [file]]
               [--emailformat string] [--html file] [--csv file]
               [--json file]
               company

InSpy - A LinkedIn enumeration tool by Jonathan Broche (@g0jhony)

positional arguments:
  company                Company name to use for tasks.

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         show program's version number and exit

Technology Search:
  --techspy [file]     Crawl LinkedIn job listings for technologies used by
                       the company. Technologies imported from a new line
                       delimited file. [Default: tech-list-small.txt]
  --limit int          Limit the number of job listings to crawl. [Default:
                       50]

Employee Harvesting:
  --empspy [file]      Discover employees by title and/or department. Titles
                       and departments are imported from a new line delimited
                       file. [Default: title-list-small.txt]
  --emailformat string Create email addresses for discovered employees using
                       a known format. [Accepted Formats: first.last@xyz.com,
                       last.first@xyz.com, firstl@xyz.com, lfirst@xyz.com,
                       flast@xyz.com, lastf@xyz.com, first@xyz.com,
                       last@xyz.com]

Output Options:
  --html file          Print results in HTML file.
  --csv file           Print results in CSV format.
  --json file          Print results in JSON.
```

# **RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Hacking con buscadores**

Hacking con buscadores: Deja que Google y cia hagan el trabajo sucio.

- Google: Conocidos Google Dorks
- Bing: Dorks interesante como “ip” y “domain”
- Baidu: [www.baidu.com](http://www.baidu.com)
- Yandex: [www.yandex.com](http://www.yandex.com)
- Yaci: <https://yaci.net>
- Startpage: [www.startpage.com](http://www.startpage.com)
- DuckDuckGo: <https://duckduckgo.com/>
- Exalead: <https://www.exalead.com/search/>

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Hacking con buscadores

Google Hacking – Referencia: <https://www.exploit-db.com/google-hacking-database/>

- site: web específica
- inurl: Aparece en la url – exclusivo de Google
- intitle: título
- intext: Aparezca en el texto
- filetype/ext: extensión.
- info: información
- cache: info cacheada en Google
- ip (bing): Listar dominios de una IP
- link: enlaces contenido sitio web
- Domain (Bing): listar subdominios.

## Operadores lógicos

- OR: |
- AND: +
- Comillas dobles: "" - Buscar frase exacta
- \*: Cualquier cosa
- "-": Descarta de la búsqueda
- "?": Puede estar o no.



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Hacking con buscadores

## Metalocalización de archivos:

- ext: pdf intitle: c users
- ext:pdf intitle: “c documents and settings”
- ext:pdf “file home”

The screenshot shows a search engine interface with the query "ext:pdf intitle: c users" entered in the search bar. The search results are displayed in a list format. The first result is a PDF file located at "C:\Users\MÓNICA\AppData\Local\MicrosoftWindows ..." with a title "Emprendelo". The second result is a PDF file located at "C:\Users\admin\Desktop\2015\_04\_23\_u\_m.htm" with a title "1 1 of 74 file:". The third result is a PDF file located at "C:\Users\sesa60911\AppData\Local\Temp\hhA391.htm" with a title "Page 1 of 13 Diagnostics 12-08-2014 file:". The fourth result is a PDF file located at "C:\Users\lamilo\Documents\FERNANDO\QDatos\CARRETERA ..." with a title "contratos-publicos/1354398228874/.../1354398241245.pdf". The fifth result is a PDF file located at "C:\Users\ccbarit\Documents\Republic of the.tif" with a title "Webs y buscadores en ciencias de la salud. 2.ª edición - Inicio". The sixth result is a PDF file located at "C:\Users\ccbarit\Documents\Republic of the.tif" with a title "Intitle index of mp3 andy - WordPress.com".



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Hacking con buscadores

## Política de contraseñas: Usuarios y contraseñas por defecto.

- “ tu contraseña inicial”
- “your initial password”
- “username consists of the” password

### Ayuda - Biblioteca Central - Universidad Tecnológica de Panamá

Si existe, **tu contraseña inicial es 12345** debes cambiar de contraseña. Si no existe, Regístrate. Presentate por nuestra biblioteca para autenticar tus datos.

### Biblioteca Central - Universidad Tecnológica de Panamá

Si ya existes, **tu contraseña inicial es 12345** es necesario que la cambies. 2. Si no existes es necesario que te registres en la opción "Regístrate" del portal ...

### MANUAL DE USO DEL OPAC - absysnet

absysnet\_Docs/Manual\_opac1.pdf - Archivo PDF

**Tu contraseña inicial** está formada por los ocho primeros caracteres de tu documento de identidad. A continuación, pulsa el botón Conectar. 2

### Cómo obtengo el usuario y contraseña de Alquilerdeviviendas.es

www.alquilerdeviviendas.es/acceso\_alquileres.php

... puedes enviarnos tus datos de contacto y te enviaremos un usuario y el código de cliente que será **tu contraseña inicial** para que tú mismo puedas insertar las ...

### contraseña - Microsoft Community

answers.microsoft.com/es-es/outlook\_com/forum/oemail-oapps...

... de 30 a 72 días para generar nuevamente el cambio, en ocasiones debe realizar un tercer cambio para que reconozca **tu contraseña inicial**. ...

### Archivo de Categoría de "03. Registro e ingreso" | Facto

https://www.facto.cl/manuales/manual-para-usuarios/registro-e-ingreso

Cambiar **tu contraseña inicial** después de ingresar. Si quieres cambiar la contraseña inicial por otra más fácil de recordar, ...

### PLATAFORMA MOODLE - plataforma-moodle

plataforma-moodle

**Tu contraseña inicial** es como tu usuario, tu DNI con 0 delante, salvo que ya hayas utilizado alguna vez la plataforma Moodle de la Conselleria d'Educació, ...

### Correo UNY by on Prezi

https://prezi.com/...

30 may. 2014 - Haz clic en el boton de lo contrario. Haz clic. HCP-012-000001. Debes ingresar tu expediente. **Tu contraseña inicial es: V-tuCédula** Ejemplo: ...

### [PDF] Preguntas frecuentes - Belcorp

https://www.somosbelcorp.com/.../Preguntas%20frecuentes%20Portal%20Consultora...

a) Si es la primera vez que ingresas o no has cambiado **tu contraseña inicial**, por favor ve a la pregunta 4. b) Si ya cambiaste tu contraseña y has confirmado tu ...

### Ayuda Migración - ech/pro/app/detalle?ID=132465

www.ech.pro/app/detalle?ID=132465

Así, si **tu contraseña inicial** era abc, ahora es abc2006. Desde luego, puedes cambiar esta contraseña ingresando a la opción Modificar datos en el Menú de ...



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Hacking con buscadores

## Política de contraseñas: Usuarios y contraseñas por defecto.

- “your password in the same”
- “your password is the same” site:edu
- “tu contraseña es la misma”

Acceder al área de clientes Fibra / ADSL - [redacted]  
<https://ayuda.queens.edu/particulares/adsl-y-fibra/mi-adsl/1894...>  
[redacted] tu contraseña es la misma para tu área de clientes y para tu app Mi [redacted]. No recuerdo mi contraseña. Si has olvidado tu contraseña clic en la opción ...

Ranking de Notas - puedes ingresar a un simulador  
[redacted].cl  
[redacted] Tu contraseña es la misma que utilizaste para el proceso de Inscripción PSU  
INGRESAR. Recuperar contraseña de acceso

[redacted] Corporation Online Courses Traducir esta página  
[redacted] edu  
... login on the left side of this page using your full FCSL email as your login ID. Your password is the same one utilized to login to the FCSL network and email

[redacted] - Login Traducir esta página  
[redacted] edu/Login.aspx  
\*Your password is the same as your JagMail or USAonline/Sakai password. For USA Health System employees: \*If you do not already have a USA online/Sakai account ...

Moodle @ Mac Traducir esta página  
[redacted] edu/my  
Your password is the same one you use to access your MacMurray email. Site News. Subscribe to the Site News forum below for updates on scheduled Moodle downtime, ...

Login :: [redacted] Traducir esta página  
[redacted] edu/[redacted] balance  
Home > [redacted]. Please log in with your UMass Lowell email address, ... Your password is the same as your email password Email: Password: UCard, ...

How to use the Zone [redacted]  
[redacted] finaid/PDFdocs/1011/How to use the Zone... - Archivo PDF  
How to use the Zone to check your Financial Aid Information. Your password is the same password used for your Zone login FYI: If you can't find your Financial Aid

Home - [redacted] Traducir esta página  
[redacted] edu/[redacted] /default.aspx  
In tandem with our new website, Queens College has launched its intranet, [redacted]. Your password is the same password you adopted for your QC Username account

YOU Portal Login Traducir esta página  
[redacted] edu  
Enter your Username and Password. U sername: P assword: ... Your password is the same as the password you use to access your WesternU e-mail account



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Hacking con buscadores

## Indexación de ficheros ofimáticos

*site:\*rtve.es site:rtve.\* (ext:pdf OR ext:doc OR  
ext:docx OR ext:xls OR ext:ppt)*

site:\*rtve.es site:rtve.\* (ext:doc OR ext:docx OR ext:pdf OR ext:xls OR ext:ppt)

Todo Imágenes Noticias Shopping Maps Más Configuración Herramientas

Aproximadamente 88.700 resultados (0,65 segundos)

[PDF] [k - RTVE.es](#)  
extra.rtve.es/ugt/0194/normadirectivos.pdf  
Page 1. RadioTelevisión Española. INSTRUCCIÓN 112004, DE 30 DE SEPTIEMBRE, DE LA DIRECCIÓN GENERAL. DE RADIOTELEVISIÓN ESPAÑOLA...

[PDF] [Reglamento de la OSCRTVE - RTVE.es](#)  
extra.rtve.es/ugt/roc.pdf  
Page 1. Portada. Reglamento de la. Orquesta y Coro. EDICIÓN ELECTRÓNICA EN FORMATO PDF. [Revisión 27 de febrero de 2014]. PUBLICADO POR UGT ...

[PDF] [capitulo octavo - RTVE.es](#)  
extra.rtve.es/ccoo/.../250611/Propuesta\_retribucion\_complementos\_CCOO\_UGT.pdf  
Page 1. CAPÍTULO OCTAVO. SISTEMA RETRIBUTIVO. Artículo 57.- Retribuciones. 1. Se considera salario la totalidad de las percepciones económicas de ...

[PDF] [perfiles para cubrir 25 puestos por adscripción - sirtve.com](#)  
extra.rtve.es/.CONVOCATORIA\_PERSONAL\_FIJO\_PARA\_LA\_MANANA\_DE\_L...  
Page 1. COMUNICADO DE INTERÉS PARA EL PERSONAL FIJO (\*) DE LA CORPORACIÓN RTVE. (\*) Con una antigüedad mínima de seis (6) meses en ...

[PDF] [Catálogo de Ayudas 2015 - RTVE.es](#)  
extra.rtve.es/ugt/201506/catalogo-ayudas-crtve.pdf  
Page 1. Catálogo de Ayudas 2015. Convocatorias y prestaciones 2015. Pólizas colectivas de seguros para los trabajadores. Aprobado por la Comisión de ...

[PDF] [en La Primera de TVE - RTVE.es](#)  
www.rtve.es/files/1013-22-FICHERO/TVE\_Ankawa\_050606.pdf?do  
6 jun. 2005 - Page 1. Page 2. Ankawa es un nuevo espacio de entretenimiento, presentado por Bertín Osborne, que se estrena el viernes, 10 de junio..

[PDF] [gente de primera - RTVE.es](#)  
www.rtve.es/files/1013-25-FICHERO/TVE\_GentedePrimera\_050526.pdf?..



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Hacking con buscadores

Indexación de ficheros ofimáticos fuera del  
target

*intext:rtve intitle:rtve –site:rtve.es –*

*site:www.rtve.es (ext:pdf OR ext:doc OR ext:docx*

*OR ext:xls OR ext:ppt)*



intext:rtve intitle:rtve -site:www.rtve.es -site:rtve.es (ext:pdf OR ext:doc (

Todo Noticias Vídeos Maps Imágenes Más Configuración Herramientas

Aproximadamente 1.050 resultados (0,52 segundos)

[PDF] 2.225 PROFESIONALES DE RTVE EXIGEN INDEPENDENCIA Y ...  
www.infolibre.es/uploads/documentos/2017/02/16\_tve\_7bd3a402.pdf  
16 feb. 2017 - Los Consejos de Informativos de RTVE (TVE, RNE, Interactivos) hemos recogido. 2.225 firmas de profesionales de la Corporación en apoyo al ...

[PDF] TESIS DOCTORAL LA TRANSFORMACIÓN DE RTVE DESDE LA V...  
www.tesisenred.net/bitstream/handle/10803/117461/ammf1de1.pdf?sequence=1...y  
Bajo la dirección del Catedrático D. José Manuel Pérez Tomero. Mayo de 2012. LA TRANSFORMACIÓN DE RTVE DESDE LA VIII. LEGISLATURA: Legislación ...

[PDF] @ RTVE.ES - IMIM  
https://intranet.imim.cat/esdeveniments/22394/fixers/17571/download  
3 Noviembre, 2014. @ RTVE.ES. 4 min. TMV: 539300. TVD: 406000. UUD: 5603000. UUM:  
www.rtve.es/noticias. TARIFA: PAÍS: URL: 5393 €. España ...

[PDF] EL RÉGIMEN JURÍDICO DE LA NUEVA CORPORACIÓN RTVE  
e-spacio.uned.es/fez/eserv/bibliuned:revistaDFD-2009-1-5080/Documento.pdf  
de AM Ruiz de Apodaca Espinosa - 2009 - Citado por 2 - Artículos relacionados  
Administración. b) El Director General de RTVE. c) Los Consejos Asesores. B. ... Obligaciones derivadas de la condición de servicio público para RTVE. B. El.

[PDF] La crisis de RTVE - E-Prints Complutense  
eprints.ucm.es/8052/1/rtve2.pdf  
de S López-Pavillard - 1992 - Citado por 3 - Artículos relacionados  
Santiago.lopez@rtve.es. Junio de 1992. Índice. 1. La televisión pública en Europa. 2. Organización, control y financiación de RTVE. 3. Cronología de una crisis.

[PDF] La documentación audiovisual en RTVE  
https://revistas.ucm.es/index.php/DCIN/article/download/.../19961  
de SL Pavillard - 1995 - Citado por 8 - Artículos relacionados  
prestación a terceros de los fondos audiovisuales de RTVE, es la primera ... Radiotelevisión Española, sobre la Documentación en RTVE y sus sociedades..

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Hacking con buscadores

- Puertos de administración:

*“allinurl:.com:8080”*

- Encontrar info de usuarios en errores

*intext:"Access denied for user" intext:"using password" intext:"on line“*

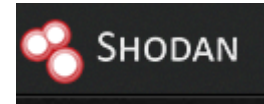
- Búsqueda de subdominios:

- *site:dominio.com –site:www.dominio.com*

- *(bing) domain:dominio.com*

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Servicios análisis servicios

- Servicios online que “analizan” IP’s -> identificar servicios y puertos de manera anónima:
  - Shodan [www.shodan.io](http://www.shodan.io)
  - Censys: censys.io (API ya es de pago)
  - Zoomeye - [www.zoomeye.org](http://www.zoomeye.org)
  - Fofa - fofa.so



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Servicios análisis servicios

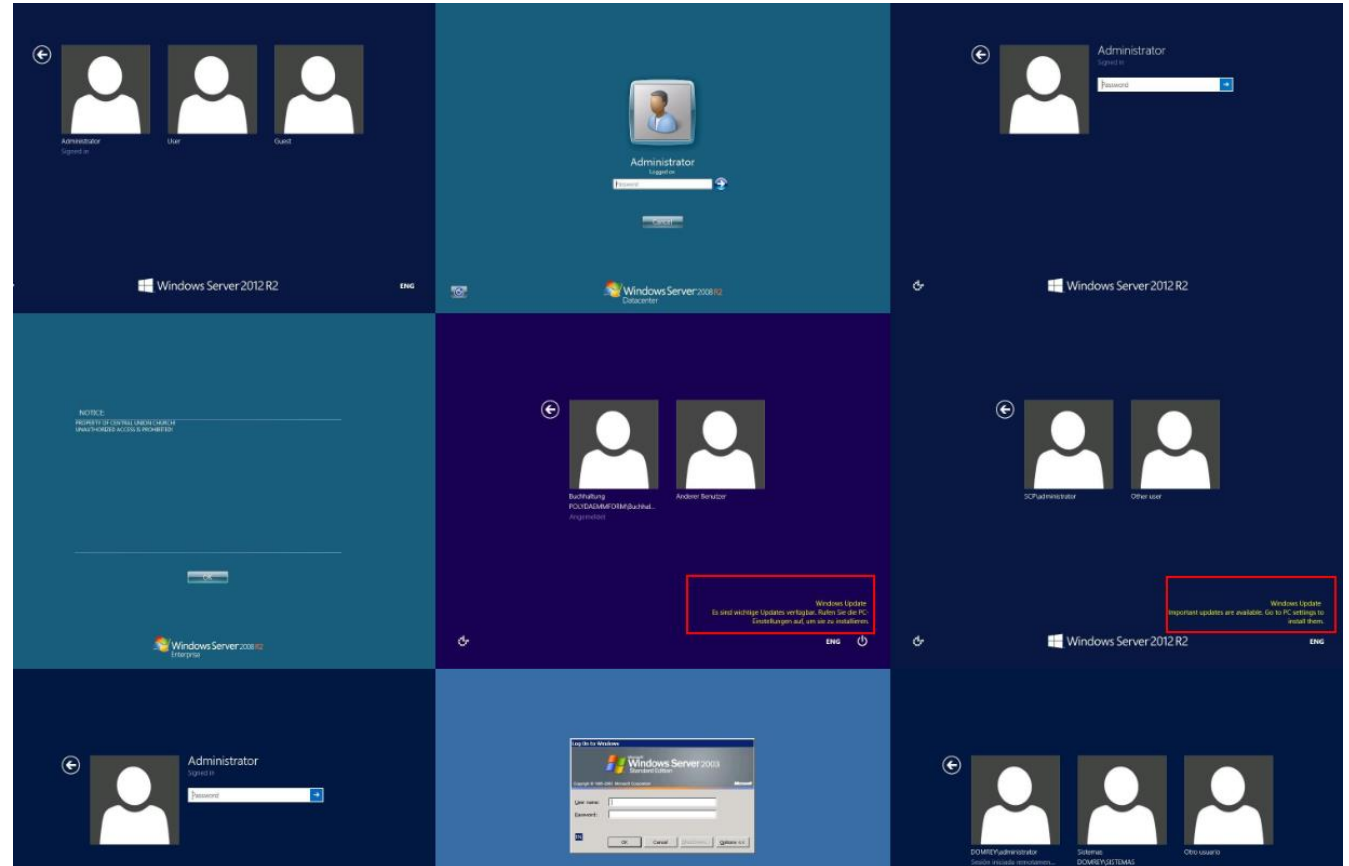
- Shodan [www.shodan.io](http://www.shodan.io)
- Propios filtros: (requiere autenticación):
  - City
  - Country
  - Geo
  - Port
- Funcionalidad “Explore” enfocado a dispositivos IoT: gasolineras, SCADA, barcos, cámaras IP,...
- API free y premium.

The screenshot displays the 'Explore' section of the Shodan search engine. At the top, it says 'Explore' and 'Discover the Internet using search queries shared by other users.' Below this, there are three columns: 'Featured Categories', 'Top Voted', and 'Recently Shared'. The 'Featured Categories' column shows three categories: 'Industrial Control Systems', 'Databases', and 'Video Games'. The 'Top Voted' column shows five search results with their respective counts and titles: 'Webcam' (9,933), 'Cams' (3,921), 'Netcam' (2,191), 'default password' (1,479), and 'dreambox' (1,073). The 'Recently Shared' column shows three search results: 'Cam-Webs', 'Password Not Set', and 'GoAhead country:"kr"', each with a count of 1.



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Servicios análisis servicios

- Screenshot Shodan [images.shodan.io](https://images.shodan.io)
- Muchos Leak: RDP (3389) -  
<https://images.shodan.io/?query=port:3389>



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Servicios análisis servicios

- Shodan presenta “HUNDIR LA FLOTA”
- <https://shiptracker.shodan.io/>



Fuente - <https://www.bleepingcomputer.com/news/security/to-nobodys-surprise-ships-are-just-as-easy-to-hack-as-anything-else/>

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Servicios análisis servicios

- Esto está muy bien pero hacerlo a mano.... Las API's son tus amigas - ¡LARGA VIDA A LAS API'S!
- Uso de scripts que interactúen con las API para obtener los servicios, puertos abiertos y banner.
- Herramientas propias:
  - Wh01p -  
<https://github.com/n4xh4ck5/wh01p>
  - Sh4d0m



**DEMO**

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Búsqueda infraestructura

Búsqueda de dominios y subdominios de forma pasiva. Uso de tools propias para automatizar:

- **N4xD0rk** – Indexación Bing y Google - <https://github.com/n4xh4ck5/N4xD0rk>
- **DorkGo0** – Indexación Google - <https://github.com/n4xh4ck5/D0rkGo0>
- **V1D0m** – API virustotal - <https://github.com/n4xh4ck5/V1D0m>
- **Cr0wd** – API ThreatCrowd - <https://github.com/n4xh4ck5/cr0wd>
- **T1pf0** – API IPv4info - <https://github.com/n4xh4ck5/t1pf0>





# **RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN:**

## **Footprinting – Búsqueda infraestructura**

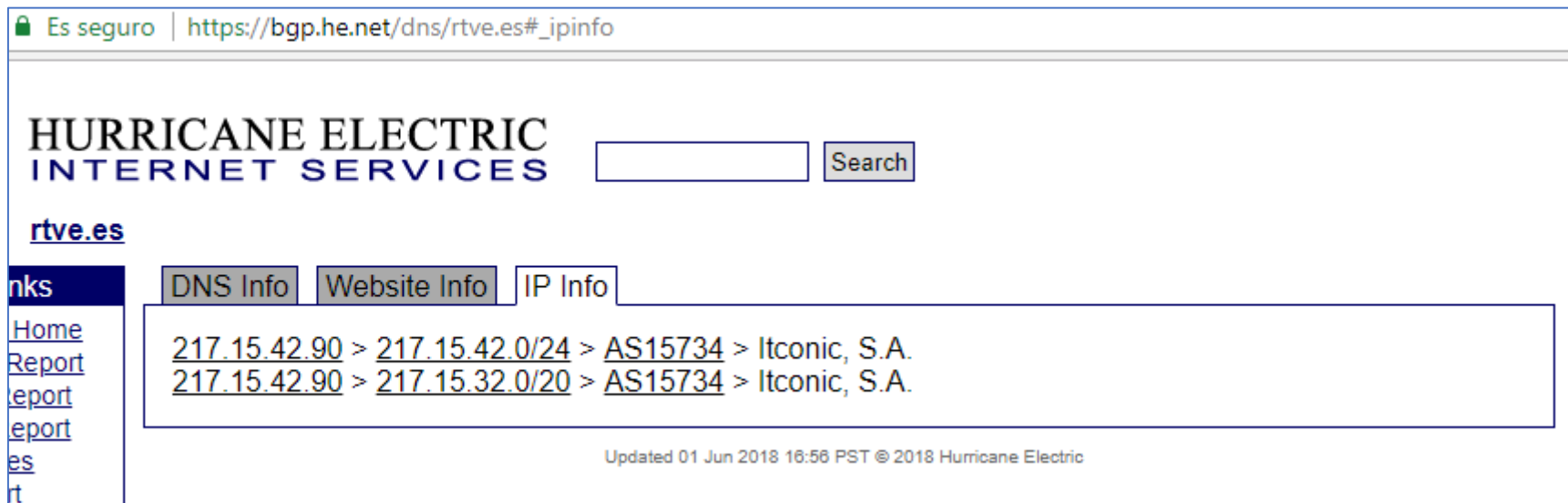
Búsqueda de dominios y subdominios de forma pasiva. Uso de tools de terceros para automatizar:

- **Aquatone** – <https://github.com/michenriksen/aquatone>
- **CTFR** (@UnaPibaGeek) – Certificados SSL - <https://github.com/UnaPibaGeek/ctfr>
- **Sublist3r** - <https://github.com/aboul3la/Sublist3r>
- **SubBrute** - <https://github.com/TheRook/subbrute>
- **DNSRecon** - <https://github.com/darkoperator/dnsrecon>



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Búsqueda infraestructura

- Identificar Rango de IP's:
- Servicio online: <https://bgp.he.net/>



The screenshot shows a web browser window with the address bar displaying "Es seguro | https://bgp.he.net/dns/rtve.es#\_ipinfo". The main content area features the "HURRICANE ELECTRIC INTERNET SERVICES" logo, a search input field, and a "Search" button. Below the logo, the domain "rtve.es" is entered. A navigation menu includes "Links", "DNS Info", "Website Info", and "IP Info". The "IP Info" tab is active, displaying the following information:

```
217.15.42.90 > 217.15.42.0/24 > AS15734 > Itconic, S.A.  
217.15.42.90 > 217.15.32.0/20 > AS15734 > Itconic, S.A.
```

At the bottom of the page, it says "Updated 01 Jun 2018 16:56 PST © 2018 Hurricane Electric".

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Metadatos

- Datos que describen otros datos.
- Ficheros ofimáticos, imágenes,...
  - Indexación resultados buscadores.
  - Repositorios abiertos: Drive, Mega, Dropbox,...
  - Propias web's de la empresa.
- ¿Qué info se obtiene?
  - Usuarios (Nombre, apellidos, sintaxis usuario el DA)
  - Cuentas de correo.
  - Carpetas compartidas.
  - Impresoras.
  - Versiones de software y SSOO.



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Metadatos

- Herramientas para automatizar el proceso:
- Búsqueda y extracción
  - FOCA - <https://github.com/ElevenPaths/FOCA>
  - Metagoofil -  
<https://github.com/laramies/metagoofil>
  - RastLeak - <https://github.com/n4xh4ck5/RastLeak>
  - PoweMeta -  
<https://github.com/dafthack/PowerMeta>
- Extracción:
  - Exiftool -  
<https://www.sno.phy.queensu.ca/~phil/exiftool>



**DEMO**



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Repositorios

- Búsqueda de proyectos con info sensible
  - Credenciales y API's hardcodeadas.
  - Comentarios con info.
  - Código fuente de aplicaciones web.
- Dispone de un buscador propio (Requiere autenticación). Búsqueda por keywords: nombre empresa, aplicación web, fabricante, nickname. Ej: API\_key, secret\_key, token, private, password, aws, login, hashes,..
- Tool para automatizar: GitMiner -  
<https://github.com/UnkL4b/GitMiner>



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – ¿He sido juankeado?

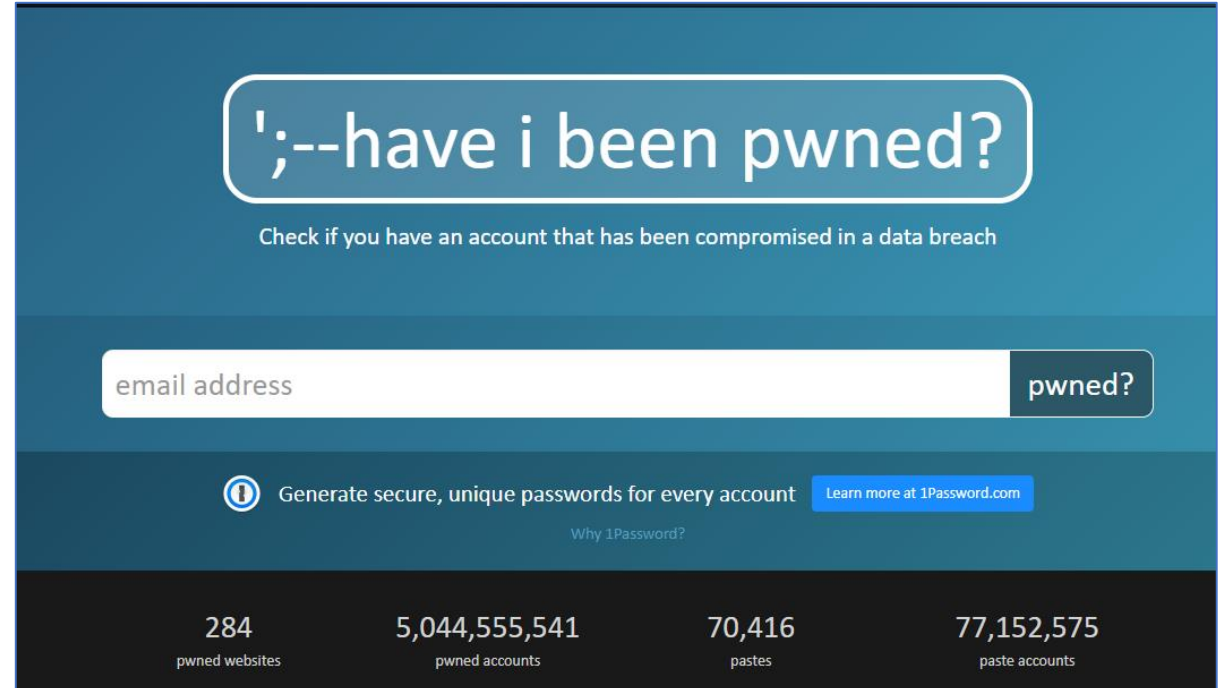
- Búsqueda de correos indexados en buscadores: Infoga-  
<https://github.com/m4ll0k/Infoga>
- Búsqueda de correos encontrados por la tool “the harvester” –  
haveIBeenHarvested - <https://github.com/depthsecurity/haveIBeenHarvested>



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – ¿He sido juankeado?

Búsqueda de emails del target en bases de datos de compromiso:

- <https://hacked-emails.com>
- <https://haveibeenpwned.com>
- <https://isleaked.com>
- <https://breachalarm.com/>



The screenshot shows the homepage of the 'have i been pwned?' website. The main heading is 'have i been pwned?' in a large, white, rounded font. Below it, a subtitle reads 'Check if you have an account that has been compromised in a data breach'. There is a search input field labeled 'email address' and a button labeled 'pwned?'. Below the search area, there is a promotional banner for 1Password: 'Generate secure, unique passwords for every account' with a link 'Learn more at 1Password.com' and the text 'Why 1Password?'. At the bottom, there are four statistics: '284 pwned websites', '5,044,555,541 pwned accounts', '70,416 pastes', and '77,152,575 paste accounts'.

Category	Count
pwned websites	284
pwned accounts	5,044,555,541
pastes	70,416
paste accounts	77,152,575

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – ¿He sido juankeado?

Y de nuevo API' => tool **check\_hacked**

- Interactúa con las API's de *hacked-emails* y *haveibeenpwned*.
- *Fail* -> *GDPR* eliminó API *hacked-emails* y protección *cloudfare* en la API de *haveibeenpwned*

```
check_hacked# python check_hacked.py -h
usage: check_hacked.py [-h] [-a ADDRESS] [-i INPUT] [-e EXPORT]

https://haveibeenpwned.com/

optional arguments:
  -h, --help            show this help message and exit
  -a ADDRESS, --address ADDRESS
                        Account email which you would like to search
  -i INPUT, --input INPUT
                        File in .txt or json which the email accounts
  -e EXPORT, --export EXPORT
                        File in xlsx format which the results(y/n)
```



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: *Fingerprinting – Escáner de red*

*¡Larga vida a nmap!*

- Por defecto en Kali Linux.
- Multitud de scripts, especialmente de reconocimiento y enumeración.
- Verificación vulnerabilidades (netapi o eternalblue)
- Obtener puertos abiertos y servicios.
- Complementar resultados encontrados pasivamente en Shodan, Censys,...

```
nmap -sSV -A -open -v -oN RESULTADOS
```



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Fingerprinting – Fichero robots.txt

- Consultar el fichero **robots.txt**
  - Información de directorios
  - Identificar directorios que revelan un CMS: wp-admin

```
← → ↻ Es seguro | https://podemos.info/robots.txt

User-agent: *
Disallow: /wp-login
Disallow: /wp-admin
Disallow: //wp-includes/
Disallow: /*/feed/
Disallow: /*/trackback/
Disallow: /*/attachment/
Disallow: /author/
Disallow: /*/page/
Disallow: /*/feed/
Disallow: /tag/*/page/
Disallow: /tag/*/feed/
Disallow: /page/
Disallow: /comments/
Disallow: /xmlrpc.php
Disallow: /*?s=
Disallow: /*/*/*/*feed.xml
Disallow: /?attachment_id*
Disallow: /procesos-autonomicos-extraordinarios/candidaturas/*
Disallow: /procesos-autonomicos-extraordinarios/resultados/andalucia/
```

```
← → ↻ Es seguro | https://www.loteriasypuestas.es/robots.txt

User-Agent: *
###
Disallow: /portal/site/
Disallow: /es/paginas-informativas/trabaja-con-nosotros*
Disallow: /*.json$
Disallow: /*.formatoRSS$
Disallow: /*.corporativa
Disallow: /*.info
Disallow: /*.info2
Disallow: /index.php/
Disallow: /*/noticias/
Disallow: /*/red-comercial
Disallow: /*/botes
Disallow: /*/escrutinios
Disallow: /*/resultados
```



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Fingerprinting – Identificar tecnología

- Identificar tecnología (PHP, JSP, ASP,...), servidor web o CMS empleado.
  - Cabeceras respuesta: “**server**”, “**X-Powered-by**”
  - Nombre de la propia cookie: **PHPSessionID**.
  - Forzando un error.
  - Analizar código fuente
  - Conexión vía telnet puede revelar banner

## Not Found

The requested URL /home.html was not found on this server.

**Apache/2.2.22 (Debian) Server** at 192.168.1.7 Port 80



```
Request  Response
Raw  Headers  Hex
-----
HTTP/1.1 301 Moved Permanently
Date: Tue, 04 Oct 2016 20:20:45 GMT
Server: Apache/2.2.15 (Oracle)
Location: /es/
Connection: close
Vary: Accept-Encoding, User-Agent
Content-Type: text/html; charset=UTF-8
Set-Cookie: cookieSession=1212DD040A2G0LE07LJ04MBAFEF61C42; Path=/; HttpOnly
Set-Cookie: FGTServe=5195ECC22E7FEC288B00CD0948D27D58F7176E8E1712105885588F; Version=1; Max-Age=3600
Content-Length: 0
```

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN:

## Fingerprinting – Enumeración directorios – fuzzing

- *Especificar las extensiones en función de la tecnología identificada (.asp,.php,.jsp,.aspx,.txt,.html,.do,.action,...)*
- *Uso de diccionarios preestablecidos:*
  - **SecLists:** <https://github.com/danielmiessler/SecLists>
  - **FuzzDB:** <https://github.com/fuzzdb-project/fuzzdb>
  - Propios de **BurpPro**
- Herramientas específicas: **Dirb/dirbuster**
- **Dirsearch:** <https://github.com/maurosoria/dirsearch>
- **Cansina:** <https://github.com/deibit/cansina>
- **photon:** <https://github.com/s0md3v/Photon>
- **Dirhunt:** <https://github.com/Nekmo/dirhunt>



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Fingerprinting – Identificación CMS

- Notable número de CMS empleados en aplicaciones web.
- Enumeración e identificación =>

**CMSsc4n -**

<https://github.com/n4xh4ck5/CMSs>

[c4n.git](#)

```
cmssc4n# python cmssc4n.py -i test.txt -e y

  O M S S C 4 N
  O M S S C 4 N
  O M S S C 4 N

*** 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 2.0
** DISCLAIMER: This tool was developed for educational goals.
** Github: https://github.com/n4xh4ck5/
** The author is not responsible for using to others goals.
** A high power, carries a high responsibility!

Tool to scan if a domain is a CMS (Wordpress , Drupal, Joomla, Prestashop or Moodle) and return the version

Example of usage: python cmssc4n.py -i input.json

Obtaining the CMS last versions...
wordpress version: 4.9.1
moodle version: 3.4
joomla version: 3.8.3
drupal version: 8.4.3
prestaShop version: 1.7.2.4
```

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Fingerprinting – Nikto

- **Nikto** para automatizar fingerprint - <https://github.com/sullo/nikto>
  - Seguridad en cabeceras de respuesta.
  - Listado de directorios y rutas por defecto.
  - Identificación del fichero robots.txt
  - Identificación de versión
  - Identificación de paneles de login.
- Contra: Es muy ruidoso!!!

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Fingerprinting – Interfaz de administración

- Identificación panel de administrador: wp-login.php, /administrator/,...
  - <https://github.com/pwnwiki/webappdefaultsdb>
  - <https://github.com/danielmiessler/SecLists>
- Realizar técnicas de enumeración de usuarios y fuerza bruta.
- Búsqueda de tutoriales y manuales que faciliten descubrir rutas, credenciales...***Al loro con las capturas de pantalla sin ofuscar.***

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Fingerprinting – vectores de compromiso

- Inyección de código SQLi o JavaScript.
  - Formularios de registro, login, búsqueda,... Sqlmap
  - XSS almacenados para robo de cookies o tokens -  
<https://github.com/s0md3v/Striker>
- Bypass login mediante SQLi o modificación cabeceras. (location)
- Incorrectos controles de autorización.
- Identificación subida ficheros:
  - Web.config en asp
  - Uso de php3, php5, pHP,...
  - Fuxploider - <https://github.com/almandin/fuxploider>





# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Fingerprinting – 0d1n

- Automatizar el proceso de visibilidad de un target.
  - Descubrimiento dominios y subdominios.
  - Identificación direccionamiento IP.
  - Identificación rangos de IP
  - Descubrimiento de activos no indexados.
  - Identificación tecnología.
  - Descubrimiento puertos abiertos.
  - Identificación CMS's
  - Screenshot de resultados
  - Exportación resultados en formato excel



# ÍNDICE

- Whoami
- Motivación
- Pasando al ataque
- Reconocimiento y recolección de información.
- **Explotación y postexplotación**
- Referencias

## ***EXPLOTACIÓN – Enumeración red interna***

- Sniffer de red: Identificar segmentos de red de servidores, token, tráfico no cifrado,...
- Escaneo y enumeración de red:
  - Identificación base de datos: mssql, Oracle, mysql,...
  - Identificación servidores de aplicaciones: tomcat, phpmyadmin, struts, ...
  - Identificación SSOO¿XP, Microsoft Server 2003 o 2005?
  - Identificación servicios y puertos: SSH(22),SMB (445), RDP (3389),...



## ***EXPLOTACIÓN – Enumeración de red interna***

- Sniffer de passwords, token, usuarios,...
- Uso de contraseñas por defecto (tomcat/tomcat, admin/admin, sa/sa...).
- Explotación servicio -> subida webshell -> ¿admin? -> creación usuario administrador. ¿No admin? -> Escalada de privilegios

# EXPLOTACIÓN

- Identificación de software vulnerable: XP -> netapi, EternalBlue
- Explotación servicio -> subida webshell -> ¿admin? -> creación usuario administrador. ¿No admin? -> Escalada de privilegios.
- Casos de uso:
  - Apache Tomcat
  - Netapi
  - EternalBlue

# POSTEXPLOTACIÓN EN WINDOWS

- Obtención hashes Windows: hashdump, cachedump
- Escalada de privilegios mediante vuln: Windows-Suggester-exploit
- Cracking de hashes: John, hashcat,...
- Pass the hash.
- Búsqueda de info sensible: ficheros de config, passwords en txt, backup, bases de datos, interfaces de red, tareas programadas, unidades de red, keepass,...
- Buscar las máquinas DC
- Objetivo: capturar hash cacheado de DC => Ser domain admin

## ***POSTEXPLOTACIÓN EN Linux***

- Identificación software vulnerable: Versión kernel,...
- Revisión tareas periódicas, permisos, (sudo -l), puertos locales, cron:  
LinEnum, linux-suggester-exploit,...
- Búsqueda de info sensible: ficheros de config, passwords en txt, backup, bases de datos, interfaces de red, tareas programadas, unidades de red, ...
- Objetivo: Ser root

# Dudas

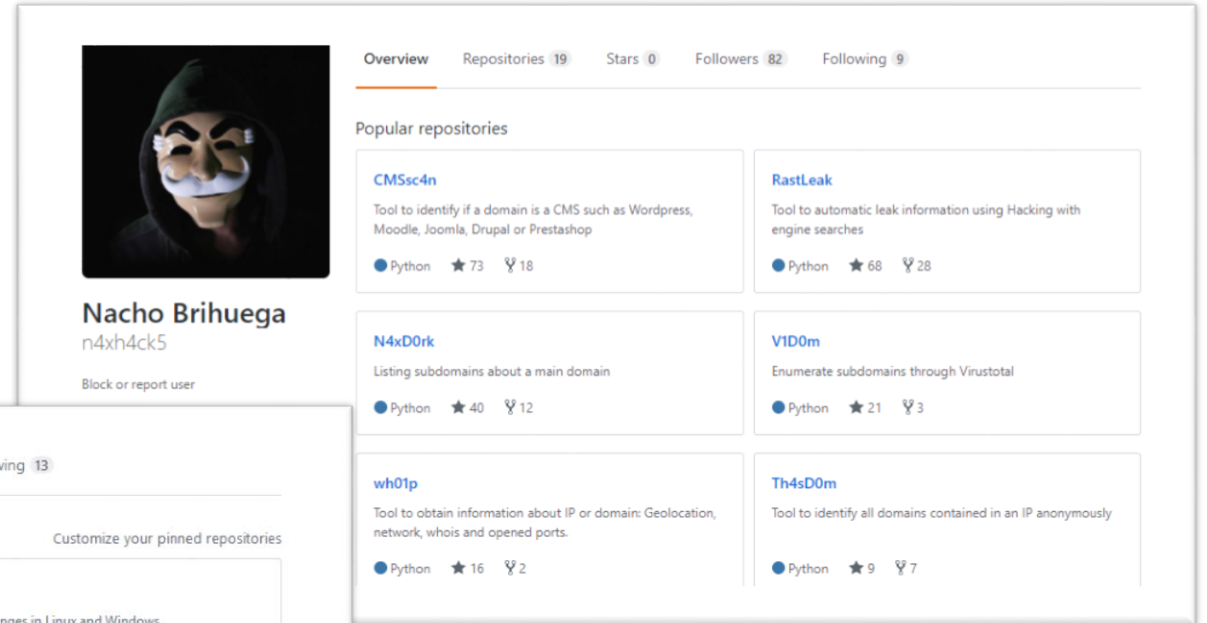




# REFERENCIAS

<https://github.com/n4xh4ck5>

<https://github.com/naivenom>

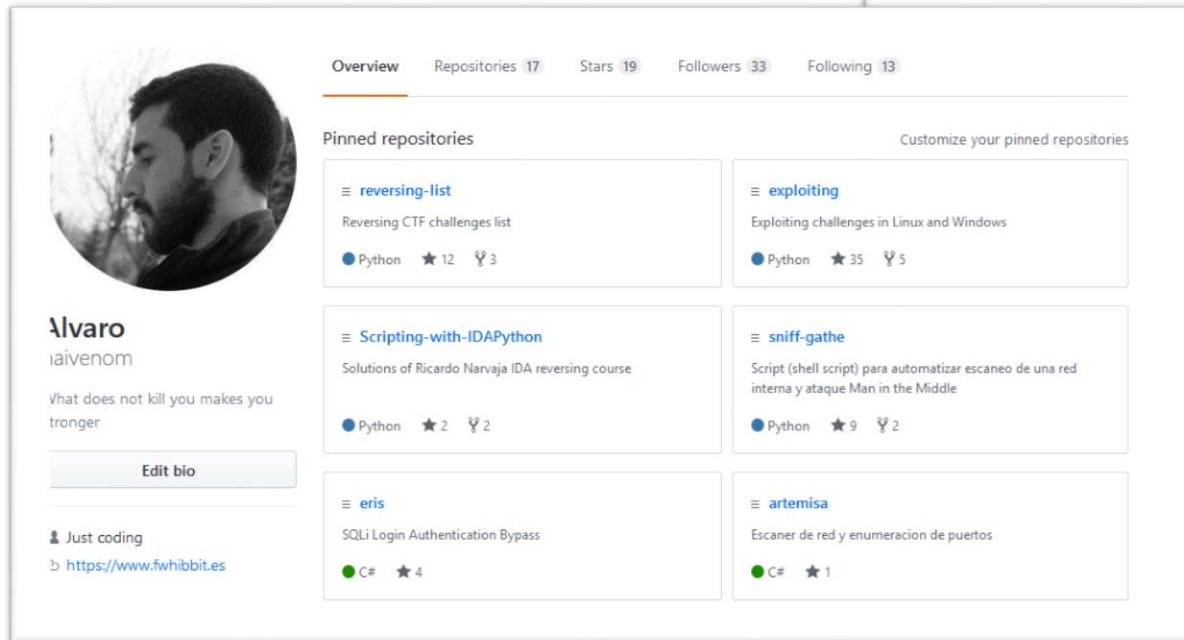


**Nacho Brihuega**  
n4xh4ck5  
Block or report user

Overview Repositories 19 Stars 0 Followers 82 Following 9

Popular repositories

- CMSsc4n**  
Tool to identify if a domain is a CMS such as Wordpress, Moodle, Joomla, Drupal or Prestashop  
Python ★ 73 🍴 18
- RastLeak**  
Tool to automatic leak information using Hacking with engine searches  
Python ★ 68 🍴 28
- N4xD0rk**  
Listing subdomains about a main domain  
Python ★ 40 🍴 12
- VID0m**  
Enumerate subdomains through Virustotal  
Python ★ 21 🍴 3
- wh01p**  
Tool to obtain information about IP or domain: Geolocation, network, whois and opened ports.  
Python ★ 16 🍴 2
- Th4sD0m**  
Tool to identify all domains contained in an IP anonymously  
Python ★ 9 🍴 7



**Alvaro**  
laivenom  
What does not kill you makes you stronger  
Edit bio

Overview Repositories 17 Stars 19 Followers 33 Following 13

Pinned repositories

- reversing-list**  
Reversing CTF challenges list  
Python ★ 12 🍴 3
- exploiting**  
Exploiting challenges in Linux and Windows  
Python ★ 35 🍴 5
- Scripting-with-IDAPython**  
Solutions of Ricardo Navaja IDA reversing course  
Python ★ 2 🍴 2
- sniff-gathe**  
Script (shell script) para automatizar escaneo de una red interna y ataque Man in the Middle  
Python ★ 9 🍴 2
- eris**  
SQLi Login Authentication Bypass  
C# ★ 4
- artemisa**  
Escaner de red y enumeracion de puertos  
C# ★ 1



# REFERENCIAS

Blogs o repositorios de referencia\_

- <https://www.fwhibbit.es/>
- <https://www.hackplayers.com/>
- <https://www.kitploit.com/>
- <https://ciberpatrulla.com/links/>
- <http://www.elladodelmal.com/>
- <https://blog.elevenpaths.com/>



# REVERSE ENGINEERING & PWN

- Requisitos:
  - (2) VM Ubuntu 16.04 LTS de 32 y 64 bit.
  - Framework radare2 y r2pipe. <https://github.com/radare/radare2>
  - Pwntools lib para el exploit.

## Released Version

pwntools is available as a `pip` package.

```
$ apt-get update
$ apt-get install python2.7 python-pip python-dev git libssl-dev libffi-dev build-essential
$ pip install --upgrade pip
$ pip install --upgrade pwntools
```

## Install

The easiest way to install radare2 from git is by running the following command:

```
$ sys/install.sh
```

## Installation

```
$ pip install r2pipe
```

or

```
$ pip3 install r2pipe
```