

# SEMINARIO 1

## HERRAMIENTAS PARA INVESTIGAR EN INTERNET

Obtener información acerca de  
máquinas, personas y código fuente!



PROYECTO "S-81 ISAAC PERAL" v3.1

¿LOCALIZASTE ALGUNA ERRATA O PROBLEMA? POR FAVOR, NOTIFÍCALA A JOSÉ MANUEL REDONDO  
LÓPEZ ([REDONDOJOSE@UNIOVI.ES](mailto:REDONDOJOSE@UNIOVI.ES)) ¡GRACIAS POR AYUDARNOS A MEJORAR LA ASIGNATURA!



Departamento de Informática  
Universidad de Oviedo



Universidad de Oviedo

Logo: @creative\_vanesa (Instagram)



# AVISO

- Este material forma parte de la asignatura “**Seguridad de Sistemas Informáticos**”, impartida en la Escuela de Ingeniería Informática de la Universidad de Oviedo
- Es fruto del trabajo continuado de elaboración, soporte, mejora, actualización y revisión del siguiente equipo de profesores desde el año 2019
  - Enrique Juan de Andrés Galiana
  - Fernando Cano Espinosa
  - Miguel Riesco Albizu
  - José Manuel Redondo López
  - Luís Vinuesa Martínez
- **Te pedimos por favor que NO lo compartas públicamente en Internet**
- No obstante, entendemos que puedes considerar este material interesante para otras personas
- Por ese motivo, hemos creado una versión del mismo adaptada para que pueda cursarse de forma online, **disponible gratuitamente para todo el mundo**
  - <https://ocw.uniovi.es/course/view.php?id=109>
  - A diferencia de esta versión, **la versión libre puedes promocionarla todo lo que quieras**, para eso está ☺

**GRACIAS POR TU COLABORACIÓN**

# INTRODUCCIÓN

## ● ¿Por qué hay tanto interés actualmente en la seguridad?

- Incluso sin tener conocimientos técnicos se puede conseguir mucha información sobre personas o compañías que puede ser explotada para obtener ventajas
- Todo lo que está en Internet puede averiguar.... si se sabe dónde (y cómo) mirar
- Este seminario enseñará herramientas que hacen esto
- Pero, si te interesa el uso (y el mal uso) de la información en Internet, deberías considerar cursar la asignatura optativa **Sistemas de Información para la Web (SIW)**
  - Si contactas con Daniel Gayo, ¡te podrá incluso dar acceso a los materiales del curso y los videos!

## ● Vamos a hacer algo que no requiere mucha pericia técnica ☺

- **OSINT (Open Source INTeelligence)**
- Algunas de estas herramientas las usaremos en prácticas

## ● **Nota: si al usar estas herramientas encuentras que tú mismo estás exponiendo demasiada información en internet, siempre hay formas de recuperar la privacidad**

- Sigue esta guía: <https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954?gi=57af4dc583d>

# ÍNDICE



- ▶ **OSINT contra máquinas**
- ▶ **OSINT contra personas**
  - Redes sociales
  - Reconocimiento desde varias fuentes
- ▶ **OSINT contra código fuente**

< Ir al Índice

# OSINT CONTRA MÁQUINAS

Investigando máquinas usando solo información pública



# SHODAN

<http://www.shodanhq.com/>



## ● Motor de búsqueda de máquinas (no web)

- Routers, servidores, cámaras... (IoT)
- Informa del tipo de servicio encontrado, versión, etc.
- Encuentra dispositivos SCADA (Supervisory Control And Data Acquisition)
  - Dispositivos industriales

## ● Busca hasta 10 dispositivos

- El registro gratuito permite más cosas y usar operadores
- Usado para ver dispositivos expuestos a internet y si representan un peligro
  - Tienen software de gestión al que acceder y por tanto atacar

## ● Tutoriales

- <https://danielmiessler.com/study/shodan/>
- <https://hacking-etico.com/2016/02/12/4979/>

The screenshot shows a Shodan search result for an Apache HTTP Server 2.4.38 device. At the top, it lists "Web Technologies" and identifies the server as using Moodle, PHP, and RequireJS. Below this, the "Vulnerabilities" section lists several CVE entries:

- CVE-2019-0196: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
- CVE-2019-0220: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
- CVE-2019-0217: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod\_auth\_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
- CVE-2019-0197: A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Servers that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
- CVE-2019-0215: In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod\_ssl when using per-location

Apache httpd 2.4.38

HTTP/1.1 200 OK  
Date: Mon, 21 Feb 2022 02:36:16 GMT  
Server: Apache/2.4.38 (Debian)  
Set-Cookie: MoodleSession=j25o9m0cmn8dkarptfvspemup; path=/; secure  
Expires:  
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform  
Pragma: no-cache  
Content-Language: es  
Content-Script-Type: text/javascript  
Content-Style-Type: text/css  
X-UA-Compatible: IE=edge  
Accept-Ranges: none  
X-Frame-Options: sameorigin  
Vary: Accept-Encoding  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=utf-8

SSL Certificate

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
03:b7:b4:45:4c:85:40:a2:1d:c9:b0:fd:06:bf:c0:61:e8:f3  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C=US, O=Let's Encrypt, CN=R3  
Validity  
Not Before: Jan 12 04:06:45 2022 GMT  
Not After : Apr 12 04:06:44 2022 GMT  
Subject: CN=virtual.ingenieriainformatica.uniovi.es  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public-Key: (2048 bit)  
Modulus:  
00:df:4c:d6:9c:50:19:04:39:96:05:61:cb:0d:2b:  
ab:4f:cd:0a:9f:66:33:3b:66:07:a8:61:8a:ac:25:  
c7:ab:08:38:d9:36:05:de:2d:43:58:d5:eb:0c:el:  
55:04:5f:70:79:f5:f4:44:1a:fa:d2:77:e4:38:75:  
4c:51:5a:3e:f7:82:95:c6:cd:96:f7:3a:2d:ae:48:  
fe:8a:5a:df:cb:d5:52:eb:e3:d1:b3:87:b2:35:67:  
5f:00:e1:44:85:3b:c1:3f:a0:43:62:86:9b:3f:ea:

# SHODAN

The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account      Getting Started

**Explore the Internet of Things**

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

**Monitor Network Security**

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

**56% of Fortune 100**

Shodan is used around the world by researchers, security pros

**TOTAL RESULTS**  
14,301,988

**TOP COUNTRIES**

United States	4,765,632
Mexico	1,234,583
China	1,051,604
Germany	1,044,601
Japan	896,419

**TOP SERVICES**

HTTP	7,055,184
HTTPS	5,376,265
HTTP (8080)	620,781
8081	203,495
HTTP (81)	174,230

**RELATED TAGS:** web servers

**72.29.75.120**  
72.29.75.120 static.hostdime.com  
HostDime.com  
Added on 2017-12-04 15:19:36 GMT  
United States, Orlando  
Details

```

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache
Last-Modified: Wed, 20 Jul 2016 05:39:00 GMT
ETag: "gf-5280a93e498500"
Accept-Ranges: bytes
Content-Length: 111
Connection: close
Content-Type: text/html

<html><head><META HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/def...

```

**SerranoArt**  
66.39.58.227  
serranoart.com  
pair Networks  
Added on 2017-12-04 15:19:36 GMT  
United States, Pittsburgh  
Technologies: Details

```

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache/2.4.29
Last-Modified: Wed, 02 Jan 2008 19:02:16 GMT
ETag: "241d-442c1ea6d5e00"
Accept-Ranges: bytes
Content-Length: 9245
Content-Type: text/html

```

## Busca los banners de estos servicios

- HTTP/HTTPS
- FTP
- SSH
- Telnet
- SNMP
- SIP (telefonía IP)
- RTSP (streaming de video y webcams)
- ...



- Lo bueno de tener una cuenta en Shodan es la potencia de sus filtros de búsqueda
  - ¡Es como un Google de máquinas!
- Puedes buscar máquinas por una cantidad enorme de criterios
- Incluidos aspectos avanzados de servicios HTTP y SSL
  - Es decir, especialmente contra servidores web y máquinas remotamente accesibles desde Internet

## Filter Reference

### General

- all
- asn
- city
- country
- cpe
- device
- geo
- has\_ipv6
- has\_screenshot
- has\_ssl
- has\_vuln
- hash
- hostname
- ip
- isp
- link
- net
- org
- os

### HTTP

- http.component
- http.component\_category
- http.favicon.hash
- http.headers\_hash
- http.html
- http.html\_hash
- http.robots\_hash
- http.security\_bit
- http.status
- http.title
- httpwaf

### SSL

- ssl
- sslalpn
- sslcert.alg
- sslcert.expired
- sslcert.extension
- sslcert.fingerprint
- sslcert.issuer.cn
- sslcert.pubkey.bits
- sslcert.pubkey.type
- sslcert.serial
- sslcert.subject.cn
- ssllchain\_count
- sslcipher.bits
- sslcipher.name
- sslcipherversion
- sslijas
- sslijarm
- sslyversion

### Bitcoin

- bitcoin.ip
- bitcoin.ip\_count
- bitcoin.port
- bitcoin.version

# SHODAN CLI

<https://cli.shodan.io/>

- **Biblioteca de Python que proporciona las capacidades de Shodan desde comandos**

- Útil en contextos sin GUI

- **Permite integrar las capacidades de Shodan en nuestros propios scripts o programas**

- O automatizar tareas de pentesting usando Shodan
- La web oficial tiene ejemplos de uso

- **Sus capacidades son equivalentes a las de la interfaz web**

- **Conjunto de búsquedas útiles:**

- <https://github.Com/jakejarvis/awesome-shodan-queries>

81.171.175.68	80	Star Technology Services Limited
178.73.238.43	80	Portlane Networks AB
113.245.76.199	5900	China Telecom HUNAN
149.210.160.163	80	Transip B.V. nowarkrengelink.com
23.92.216.117	80	Res.pl Isp S.c. mailingrolout.com
202.69.233.212	443	Verio Web Hosting kubota-rvc23-0727001.com
190.78.179.228	8080	CANTV Servicios, Venezuela 190-78-179-228.dyn.dsl.cantv.net
192.3.4.108	443	ColoCrossing sxi.pw
160.246.182.223	80	Hayashi Telempu Co., Ltd.
198.104.15.120	443	Verio Web Hosting wholesalechildrensclothing.com.au
208.64.139.67	80	Desync Networks 119-a.webmasters.com
212.227.51.115	443	1&1 Internet AG s535322526.online.de
75.98.17.22	443	Internap Network Services Corporation
178.208.77.241	81	McHost.Ru v112059.vps.mcdir.ru
63.249.80.153	443	Cruzio www12153.cruzio.com
87.243.209.223	8080	HotChilli Internet static-87-243-209-223.adsl.hotchilli.net
183.89.74.87	81	3BB Broadband mx-11-183.89.74-87.dynamic.3bb.co.th
178.236.77.90	80	Excellent Hosting Sweden AB
54.201.193.170	80	Amazon.com ec2-54-201-193-170.us-west-2.compute.amazonaws.com
106.186.28.222	80	Linode, LLC li608-222.members.linode.com
54.85.166.63	80	Merck and Co. ec2-54-85-166-63.compute-1.amazonaws.com
208.131.128.136	80	WestHost greenstreetstudios.org

# CENSYS

<https://censys.io/>



## ● Como Shodan, pero con información estructurada

- Busca características de servidores: servicios interesantes en ejecución (RDP), banners de SO, servidores web...
- Varios criterios de búsqueda
  - IP (solo v4) y redes: <https://censys.io/ipv4/>
  - Nombres de dominio del sitio web: <https://censys.io/domain?q>
  - Certificados: <https://censys.io/certificates?q>

## ● Tutorial de búsqueda

- <https://developerinsider.co/censys-find-and-analyze-any-server-and-device-on-the-internet/>

## ● Una herramienta similar es Onhype.io

- <https://fwhibbit.es/descubrimiento-y-recopilacion-de-activos-con-onhyphe-io>
- Comparación con otras herramientas (Zmap, Mr looquer)
  - <https://www.dragonjar.org/shodan-vs-scans-io-vs-censys-io-vs-zmap-vs-mr-looquer.xhtml>

The screenshot shows the Censys search interface with the query "IPv4 Hosts" and the result "156.35.0.0/16". The interface includes sections for "Quick Filters" (with a link to "Data Definitions") and "Autonomous System" (listing 307 REDIRIS RedIRIS Autonomous System). It also shows a "Protocol" section with various ports and services (e.g., 148 3389/rdp, 138 80/http, 91 443/https, 22 8080/http, 13 143/imap) and a "Tag" section with common tags like http, remote\_display, rdp, https, and imap. The main area displays a list of IPv4 hosts, each with a summary of its services, location (Oviedo, Principality of Asturias, Spain), and specific details like the operating system (Ubuntu) and port numbers. Each host entry is preceded by a small icon representing the service or protocol.

Host IP	Autonomous System	Protocol	Tags	Location
156.35.151.5 (orion.edv.uniovi.es)	REDIRIS RedIRIS Autonomous System (766)	80/http	http, RDP, REMOTE_DISPLAY	Oviedo, Principality of Asturias, Spain
156.35.11.15	REDIRIS RedIRIS Autonomous System (766)	80/http, 443/https	http, RDP, REMOTE_DISPLAY	Oviedo, Principality of Asturias, Spain
156.35.25.195 (crisa25195.econo.uniovi.es)	REDIRIS RedIRIS Autonomous System (766)	3389/rdp	RDP, REMOTE_DISPLAY	Oviedo, Principality of Asturias, Spain
156.35.225.33 (portalgp.uniovi.es)	REDIRIS RedIRIS Autonomous System (766)	443/https	http, RDP, REMOTE_DISPLAY	Oviedo, Principality of Asturias, Spain
156.35.172.86 (imprisa.epv.uniovi.es)	REDIRIS RedIRIS Autonomous System (766)	3389/rdp	RDP, REMOTE_DISPLAY	Oviedo, Principality of Asturias, Spain
156.35.119.112 (hercules.lsi.uniovi.es)	REDIRIS RedIRIS Autonomous System (766)	3389/rdp	RDP, REMOTE_DISPLAY	Oviedo, Principality of Asturias, Spain
156.35.81.145 (llama81145.eutio.uniovi.es)				

# EJEMPLO

**(1) Usar Shodan para encontrar recursos pertenecientes a Uniovi**



# GOOGLE HACKING O “GOOGLE DORKING”

- **Capacidad de realizar búsquedas que revelan información comprometedora**

- Usando motores de búsqueda (normalmente dirigidas a un dominio con el operador `site:`)
- Las búsquedas tratan de encontrar información de vulnerabilidades, problemas de configuración o facilite un ataque
- También se puede hacer en otros motores de búsqueda (aunque Google es el más usado)

- **Hay una BD de búsquedas preconstruidas clasificadas: Google Hacking Database**

- Se llaman “Google Dorks”: <https://www.exploit-db.com/google-hacking-database>
- Elige la categoría de búsqueda correcta: ¡cada categoría representa una posible vulnerabilidad!
- Busca en el destino con la consulta elegida (`site:`)

- **El “Dorking” puede usarse con otros productos**

- <https://github.com/cipher387/Dorks-collections-list>

- **Ejemplos**

- <https://wifibit.com/google-hacking/>
- <https://ciberpatrulla.com/osint-con-google/>
- <https://ciberpatrulla.com/buscar-google/>
- [https://medium.com/@logicbomb\\_1/one-misconfig-jira-to-leak-them-all-including-nasa-and-hundreds-of-fortune-500-companies-a70957ef03c7](https://medium.com/@logicbomb_1/one-misconfig-jira-to-leak-them-all-including-nasa-and-hundreds-of-fortune-500-companies-a70957ef03c7)

# GOOGLE HACKING: PROCESO

The diagram illustrates the Google Hacking process flow:

- Exploit Database:** Shows the "Google Hacking Database" interface with various search filters and categories. A red arrow points from the "Web Server Detection" filter in the sidebar to the search results table.
- Search Results:** Shows Google search results for the query "intitle:'Apache2 Ubuntu Default Page: It works'". A red arrow points from the search bar to the results page.
- Exploit Page:** Shows a detailed view of a specific exploit entry: "intitle:'Apache2 Ubuntu Default Page: It works'". It includes fields like GHDB-ID, Author, Published date, and a "Google Dork Description". A red arrow points from the "Google Search" link in the exploit entry to the search results page.
- Second Search Results:** Shows Google search results for the same query, with a red arrow pointing from the search bar to the results page.
- Third Search Results:** Shows Google search results for the same query, with a red arrow pointing from the search bar to the results page.

**Google Hacking Database (Top Left):**

Date Added	Dork
2020-01-17	intitle:'W500 Management Console'
2020-01-10	intitle:'webview login' alcatel lucent
2020-01-09	intitle:'LABVANTAGE Logon'
2020-01-09	site:'log/domedmin.cgi'
2020-01-09	inurl:'8080/login.jsp?es_destination='
2020-01-09	intitle:'index of "/wp-security-audit-log"
2020-01-09	intext:'powered by codiforum' inurl:'user/login'
2020-01-06	inurl:'index.php?enter+guest'
2020-01-06	intitle:'Zabbix' intext:'username' intext:'password' inurl:'zabbix/index.php'

**Category:** Footholds, Files Containing Usernames, Sensitive Directories, Web Server Detection, Vulnerable Files, Vulnerable Servers, Error Messages.

**Google Dork Description:** intitle:'Apache2 Ubuntu Default Page: It works'

**Google Search Result (Top Right):**

intitle:'Apache2 Ubuntu Default Page: It works'

**Google Dork Description:** intitle:'Apache2 Ubuntu Default Page: It works'

**Google Search Result (Bottom Right):**

intitle:'Apache2 Ubuntu Default Page: It works'

Aproxadamente 27.000 resultados (0,40 segundos)

Traducir esta página

**Apache2 Ubuntu Default Page: It works Annex02!**

Apache2 Ubuntu Default Page: It works Annex02! It works! This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived.

Traducir esta página

**Apache2 Ubuntu Default Page: It works \*\*\* PROXY \*\*\***

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page ...

Traducir esta página

**Apache2 Ubuntu Default Page: It works**

Apache2 Ubuntu Default Page: It works. It works! XXXX This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived.

Traducir esta página

**Apache2 Ubuntu Default Page: It works**

It works! ?

# FINAL RECON

<https://github.com/thewhiteh4t/FinalRecon>



Seguridad de Sistemas  
Informáticos

- Script de Python para reconocimiento web

- Tiene muchas características para crear un perfil completo de un servidor web y su contenido

- Información de DNS y Whois
- Recolector (crawler) completo
- Traceroute
- Búsqueda de directorios
- Escaneo de puertos del servidor

- Tutorial

- <https://hakin9.Org/final-recon-osinttool-for-all-in-one-web-reconnaissance/>

```
python3 finalrecon.py -h
```

```
usage: finalrecon.py [-h] [--headers] [--sslinfo] [--whois] [--crawl] [--dns] [--sub] [--trace] [--dir] [--ps] [--full] [-t T] [-T T] [-w W] [-r] [-s] [-d D] [-e E] [-m M] [-p P] [-tt TT] [-o O] url
```

```
FinalRecon - The Last Recon Tool You Will Need | v1.0.7
```

positional arguments:

url Target URL

optional arguments:

-h, --help	show this help message and exit
--headers	Header Information
--sslinfo	SSL Certificate Information
--whois	Whois Lookup
--crawl	Crawl Target
--dns	DNS Enumeration
--sub	Sub-Domain Enumeration
--trace	Traceroute
--dir	Directory Search
--ps	Fast Port Scan
--full	Full Recon

Extra Options:

-t T	Number of Threads [ Default : 30 ]
-T T	Request Timeout [ Default : 30.0 ]
-w W	Path to Wordlist [ Default : wordlists/dirb_common.txt ]
-r	Allow Redirect [ Default : False ]
-s	Toggle SSL Verification [ Default : True ]
-d D	Custom DNS Servers [ Default : 1.1.1.1 ]
-e E	File Extensions [ Example : txt, xml, php ]
-m M	Traceroute Mode [ Default : UDP ] [ Available : TCP, ICMP ]
-p P	Port for Traceroute [ Default : 80 / 33434 ]
-tt TT	Traceroute Timeout [ Default : 1.0 ]
-o O	Export Output [ Default : txt ] [ Available : xml, csv ]

# uDORK

<https://github.com/m3n0sd0n4ld/uDork>



## ● Script bash que utiliza Google hacking para obtener varios tipos de información sensible

- Ficheros o directorios
- Encuentra dispositivos IoT
- Frameworks de aplicaciones WEB / versiones de CMS
- ...

## ● Tutorial:

- <https://www.enhacke.com/2020/03/21/udork-google-hackingtool/>

```
v2.0
by M3n0sd0n4ld - (@David_Uton)

[!] The results will appear below. This may take several minutes, please wait ...

Domain/IP: nasa.gov
Find links with: pdf
-----
https://www.sti.nasa.gov/thesvol2.pdf
https://www.sti.nasa.gov/thesvol1.pdf
https://oig.nasa.gov/docs/MC-2018.pdf
https://www.nasa.gov/centers/dryden/pdf/88798main_srfcs.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A10_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A14_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A07_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A15_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A09_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A08_PressKit.pdf
-----
Files pdf found: 10

Domain/IP: nasa.gov
Find links with: xml
-----
https://www.nasa.gov/sitemap.xml
-----
Files xml found: 1

Domain/IP: nasa.gov
Find links with: xls
-----
https://airbornescience.nasa.gov/instrument/all/export
-----
Files xls found: 1

Domain/IP: nasa.gov
Find links with: txt
-----
https://www.nasa.gov/378571main_0728NASAMeeting.txt
https://seabass.gsfc.nasa.gov/archive/INIDEP_LPPB/EPEA/archive/pigments/EPEA_PD2012-03_HPLC.txt
https://seabass.gsfc.nasa.gov/archive/MLI/larouche/optique_st_laurent/2000_15/archive/SPMR0015104_CASTB.txt
```

< Ir al Índice

Redes sociales >

Integración de datos >

# OSINT CONTRA PERSONAS

Investigando gente usando solo información pública



[Índice](#) -> [OSINT contra personas](#)

# Redes sociales

Saber lo que la gente hace...y escribe ☺



# TINFOLEAK

<https://github.com/vaguileradiaz/tinfoleak>



## ● Analiza y extrae información de cuentas de Twitter

- Busca mensajes usando términos
- Varias opciones para encontrar datos
- Herramienta típica para buscar tweets “comprometedores” de personalidades
  - Muy típico hoy día... ☺

## ● Necesita una API key de Twitter

- Y por tanto una cuenta de Twitter activa

## ● Enlaces (instalación, ayuda)

- <https://ciberpatrulla.com/tutorial-tinfoleak/>
- <https://www.isecauditors.com/herramientas-tinfoleak>
- <http://www.noise-sv.com/tutorial-de-tinfoleak/>

## ● Hay herramientas similares para otras redes sociales

- Facebook, LinkedIn, Instagram...

@VaguilaDiaz vaguila@isecauditors.com Internet Security Auditors v2.0

# tinfoleak



**Steve Wozniak**  
Engineers first! Human rights. Gadgets. Jokes and pranks. Segways. Music and concerts. Gameboy Tetris.  
Followers: 570,246 | Following: 85 | Likes: 3  
Tweets: 5,714 (1.99 tweets/day)

Screen Name: stevewoz  
Account Created at: 03/05/2009  
Verified: True  
Twitter ID: 22938914  
URL: <http://woz.org>  
Location: Los Gatos, California  
Time Zone: Pacific Time (US & Canada)  
Geo enabled: True  
Listed count: 9645  
Language: en

APPS SOCIAL HASHTAGS MENTIONS TWEETS METADATA MEDIA GEO

### CLIENT APPLICATIONS

Source	Uses	Percentage	First Use	First Tweet	Last Use	Last Tweet
Foursquare	185	92.5 %	09/26/2016	view	01/18/2017	view
OS X	4	2.0 %	10/16/2016	view	01/16/2017	view
Twitter for iPhone	2	1.0 %	12/11/2016	view	01/03/2017	view
Twitter Web Client	9	4.5 %	09/27/2016	view	12/17/2016	view

Total: 4 results.

### SOCIAL NETWORKS

Social Network	Username	Picture	Name	Additional info
Twitter	stevewoz		Steve Wozniak	Los Gatos, California

Fuente: <https://www.redeszone.net/2017/10/08/tinfoleak-recopilar-informacion-usuarios-twitter/>

# HUNTER.IO

<https://hunter.io/>

- Sitio web que permite descubrir direcciones de correo electrónico relacionadas con un dominio / empresa

- Con ellas se pueden iniciar ataques OSINT, intentos de phishing o APTs (Advanced Persistent Threats)

- No es un servicio gratuito

- El registro gratuito permite un uso limitado de sus características
- Resultados completos
- Descargas CSV
- Hasta 50 búsquedas/mes

The screenshot shows the Hunter.io interface. At the top, there's a navigation bar with the logo, 'Product', and 'Pricing'. Below it is a search bar labeled 'Domain Search' with the placeholder 'Find the email addresses of a company.' and a magnifying glass icon. Underneath the search bar is a section titled 'Email Finder' with a blue icon. A search input field contains 'uniovi.es' and a button labeled 'Find email addresses' in orange. To the right of this section, the text '2,667 email addresses' is visible. Below this, several email addresses are listed with their source count:

- s rezfaustino@uniovi.es • 1 source
- b tranjose@uniovi.es • 5 sources
- p lina@uniovi.es • 3 sources
- s isjaime@uniovi.es • 2 sources
- g zalezcristian@uniovi.es • 3 sources

A note at the bottom indicates '2,667 more results for "uniovi.es"'.

# SOCIAL MAPPER

[https://github.com/Greenwolf/social\\_mapper](https://github.com/Greenwolf/social_mapper)



Seguridad de Sistemas  
Informáticos

## ● Script de Python que correlaciona usuarios en diferentes RRSS utilizando reconocimiento facial

- Se usa para localizar usuarios falsos en RRSS usando la misma imagen de perfil
- Tiene otros usos para operaciones de red team

## ● Acepta diferentes tipos de entrada

- El nombre de una organización, buscando a través de LinkedIn
- Una carpeta con imágenes con nombres
- Un CSV con nombres y URLs a imágenes online
- Funciona con Facebook, Instagram, Twitter, LinkedIn, VKontakte (“Facebook” ruso), Weibo, Douban...

## ● Maltego admite sus resultados

- Herramienta que veremos más adelante

4 parameters must be provided. 3 are an input format, the input file or folder and the basic running mode:  
-f, --format : Specify if the -i, --input is a 'name', 'csv', 'imagefolder' or 'socialmapper' resume file  
-i, --input : The company name, a CSV file, imagefolder or Social Mapper HTML file to feed into Social Mapper  
-m, --mode : 'fast' or 'accurate' allows you to choose to skip potential targets after a first likely match is found, in some cases potentially speeding up the program x20

Additionally, at least one social media site to check must be selected:

-a, --all	: Selects all of the options below and checks every site that Social Mapper has credentials for
-fb, --facebook	: Check Facebook
-tw, --twitter	: Check Twitter
-ig, --instagram	: Check Instagram
-li, --linkedin	: Check LinkedIn
-gp, --googleplus	: Check Google Plus
-vk, --vkontakte	: Check VKontakte
-wb, --weibo	: Check Weibo
-db, --douban	: Check Douban

Additional optional parameters can also be set:

-t, --threshold	: Customizes the facial recognition threshold for matches, this can be seen as the match accuracy. Default is 'standard', but can be set to 'loose', 'standard', 'strict' or 'superstrict'. For example 'loose' will find more matches, but some may be incorrect. While 'strict' may find less matches but also contain less false positives in the final report.
-cid, --companyid	: Additional parameter to add in a LinkedIn Company ID for if name searches are not picking the correct company.
-s, --showbrowser	: Makes the Firefox browser visible so you can see the searches performed. Useful for debugging.
-w, --waitafterlogin	: Wait for user to press Enter after login to give time to enter 2FA codes. Must use with -s
-v, --version	: Display current version.
-vv, --verbose	: Verbose Mode (Useful for Debugging)
-e, --email	: Provide a fuzzy email format like "<f><last>@domain.com" to generate additional CSV files for each site with firstname, lastname, fullname, email, profileURL, photoURL. These can be fed into phishing frameworks such as Gophish or Lucy.

### Example Runs

\* A quick run for Facebook and Twitter on some targets you have in an imagefolder, that you plan to manually review and don't mind some false positives: python3 social\_mapper.py -f imagefolder -i ./Input-Examples/imagefolder/ -m fast -fb -tw

\* The same as above but with the browser showing, and waiting enabled to allow a user to enter 2FA codes and manually rectify changed Login processes: python3 social\_mapper.py -f imagefolder -i ./Input-Examples/imagefolder/ -m fast -fb -tw -s -w

\* An exhaustive run on a Large company where false positives must be kept to a minimum: python3 social\_mapper.py -f company -i "Evil Corp LLC" -m accurate -a -t strict

\* A Large run that needs to be split over multiple sessions due to time, the first run doing LinkedIn and Facebook, with the second resuming and filling in Twitter, Google Plus and Instagram: python3 social\_mapper.py -f company -i "Evil Corp LLC" -m accurate -li -fb python3 social\_mapper.py -f socialmapper -i ./Evil-Corp-LLC-social-mapper-linkedin-facebook.html -m accurate -tw -gp -ig

\* A quick run (~5min) without facial recognition to generate a CSV full of names, email addresses, profiles and photo links from up to 1000 people pulled out of a LinkedIn company, where the email format is known to be "firstname.lastname": python3 social\_mapper.py -f company -i "Evil Corp LLC" -m accurate -li -e "<first>.<last>@evilcorpllc.com"

# PROJECT SHERLOCK

<https://github.com/sherlock-project/sherlock>



- Encuentra nombres de usuario en muchas RRSS o webs diferentes

- ¡Más de 320!

- Es muy común encontrar usuarios con el mismo nombre en diferentes redes sociales y sitios

- Y, de esta manera, recopilar información de diferentes fuentes sobre la misma persona
  - O utilizar fuentes secundarias si encontramos perfiles cerrados en algunas redes sociales...

- El uso básico es sencillo

- `python3 pherlock.py <nombre de usuario>`

```
(vagrant㉿kali)-[~]
$ sherlock Ibaillanos
[*] Checking username Ibaillanos on:
[+] Academia.edu: https://independent.academia.edu/Ibaillanos
[+] CapFriendly: https://www.capfriendly.com/users/Ibaillanos
[+] Chaturbate: https://chaturbate.com/Ibaillanos
[+] Coil: https://coil.com/u/Ibaillanos
[+] DeviantART: https://Ibaillanos.deviantart.com
[+] Duolingo: https://www.duolingo.com/profile/Ibaillanos
[+] F3.cool: https://f3.cool/Ibaillanos/
[+] Facebook: https://www.facebook.com/Ibaillanos
[+] Fiverr: https://www.fiverr.com/Ibaillanos
[+] FortniteTracker: https://fortnitetracker.com/profile/all/Ibaillanos
[+] Giphy: https://giphy.com/Ibaillanos
[+] GitHub: https://www.github.com/Ibaillanos
[+] Gumroad: https://www.gumroad.com/Ibaillanos
[+] Instagram: https://www.instagram.com/Ibaillanos
[+] LeetCode: https://leetcode.com/Ibaillanos
[+] Lichess: https://lichess.org/@Ibaillanos
[+] Linktree: https://linktr.ee/Ibaillanos
[+] Minecraft: https://api.mojang.com/users/profiles/minecraft/Ibaillanos
[+] PSNProfiles.com: https://psnprofiles.com/Ibaillanos
[+] Pinterest: https://www.pinterest.com/Ibaillanos/
[+] Pokemon Showdown: https://pokemonshowdown.com/users/Ibaillanos
[+] Pornhub: https://pornhub.com/users/Ibaillanos
[+] Quizlet: https://quizlet.com/Ibaillanos
[+] Reddit: https://www.reddit.com/user/Ibaillanos
[+] Roblox: https://www.roblox.com/user.aspx?username=Ibaillanos
[+] RuneScape: https://apps.runescape.com/runemetrics/profile/profile?user=Ibaillanos
[+] Scratch: https://scratch.mit.edu/users/Ibaillanos
[+] SlideShare: https://slideshare.net/Ibaillanos
[+] Smule: https://www.smule.com/Ibaillanos
[+] Spotify: https://open.spotify.com/user/Ibaillanos
[+] Telegram: https://t.me/Ibaillanos
[+] Tenor: https://tenor.com/users/Ibaillanos
[+] TikTok: https://tiktok.com/@Ibaillanos
[+] TradingView: https://www.tradingview.com/u/Ibaillanos/
[+] Trello: https://trello.com/Ibaillanos
[+] Twitch: https://www.twitch.tv/Ibaillanos
[+] Twitter: https://twitter.com/Ibaillanos
[+] Venmo: https://venmo.com/u/Ibaillanos
[+] Wattpad: https://www.wattpad.com/user/Ibaillanos
[+] WordPress: https://Ibaillanos.wordpress.com/
[+] Xbox Gamertag: https://xboxgamertag.com/search/Ibaillanos
[+] YouNow: https://www.younow.com/Ibaillanos/
[+] mercadolivre: https://www.mercadolivre.com.br/perfil/Ibaillanos
[+] osu!: https://osu.ppy.sh/users/Ibaillanos
[+] xHamster: https://xhamster.com/users/Ibaillanos
```

# Integración de reconocimiento de usuarios / de varias fuentes

Agregando datos de usuarios



# MALTEGO

<https://www.paterva.com/buy/maltego-clients/maltego-ce.php>



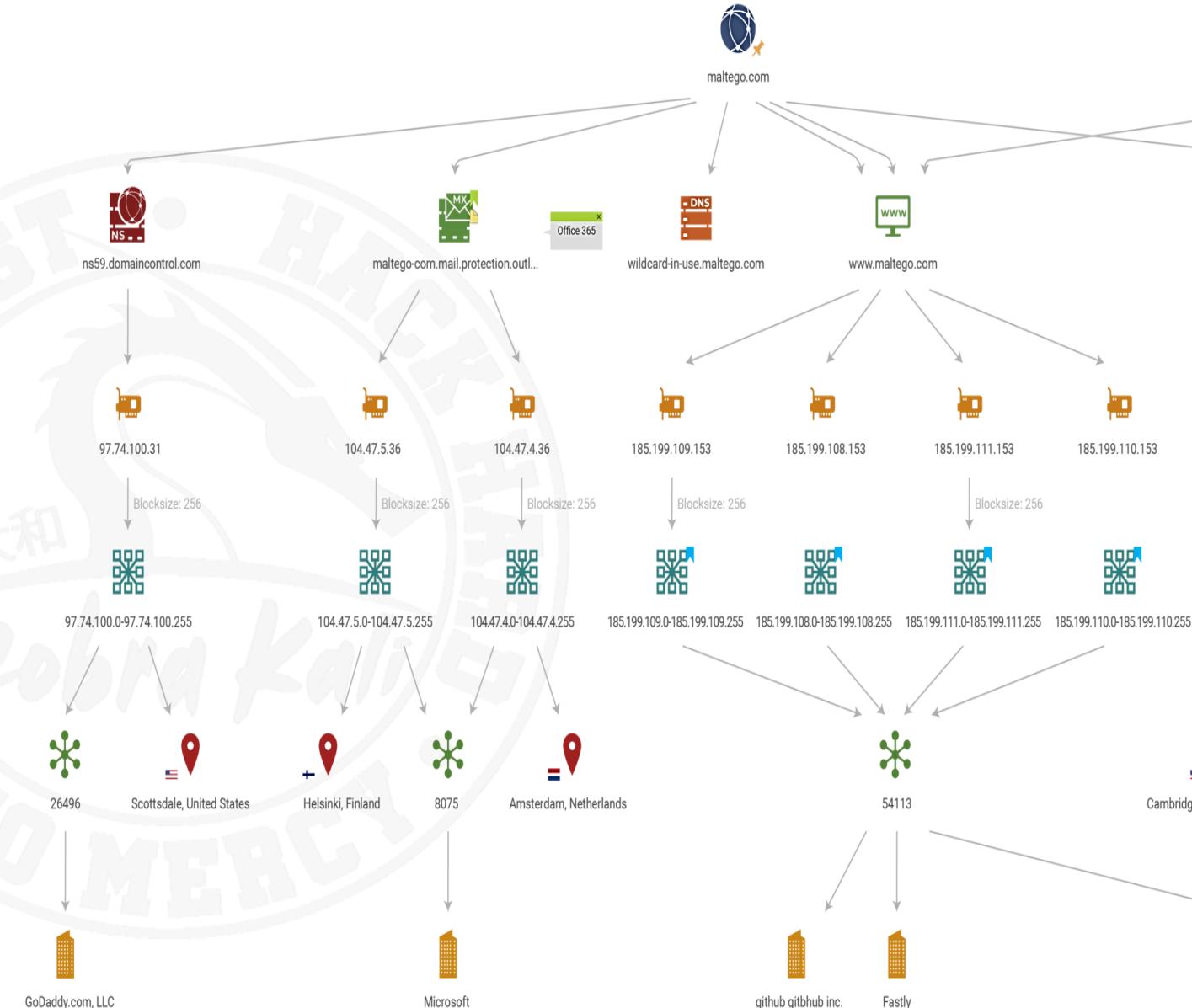
Fuente: <https://en.wikipedia.org/wiki/Maltego>

## ● Recopila información de entidades de internet

- Crea entidades personalizadas que representan cualquier tipo de información
- Se especializa en encontrar relaciones entre ellas
  - Redes sociales, redes de ordenadores, dominios...
- Utiliza como fuentes DNS, registros [whois](#), motores de búsqueda, redes sociales conocidas, APIs...

## ● Tutoriales

- <https://www.fwhibbit.es/introduccion-a-maltego>
- <https://ciberpatrulla.com/maltego/>
- [www.elladodelmal.com/2010/08/mineria-de-datos-con-maltego-1-de-2.html](http://www.elladodelmal.com/2010/08/mineria-de-datos-con-maltego-1-de-2.html)



# RECON-NG

<https://kali-linux.net/article/recon-ng/>

- Se usa para recopilar información sobre usuarios de distintas fuentes
- Cuenta con una serie de módulos que permiten buscar en diferentes fuentes de información
  - Motores de búsqueda, API...
- Copia la interfaz de Metasploit para que sea más fácil para las personas que ya están familiarizados con él
- Tutoriales
  - <https://hackertarget.com/recon-ng-tutorial/>
  - <https://noticiasseguridad.com/tutoriales/recon-ng-herramienta-para-recolección-de-informacion/>

```
carlos@NoSoloHacking:~/recon-ng$ sudo ./recon-ng
Sponsored by ...
^   ^
^ / \ \W \V \
/ \ // \VV\ \V \
// / \ BLACK HILLS V \ \
www.blackhillsinfosec.com

PRACTISEC
www.practise.com

[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installed.

[recon-ng][default] > ■
```

Fuente: <https://www.nosolohacking.info/recon-ng-instalacion/>

# ODIN

<https://github.com/chrismaddalena/ODIN>

- **Herramienta automatizada de descubrimiento y catalogación para activos de redes, correo electrónico y redes sociales**
- **Incluye empleados / activos en plataformas en la nube**
- **Crea informes que se pueden guardar en una BBDD para ser procesados**
- **Más información**
  - <https://www.gurudelainformatica.es/2019/05/descubrimiento-y-catalogacion.html>
- **Aplicaciones similares**
  - <https://blog.segu-info.com.ar/2019/05/aplicaciones-paraosint.html?m=0>

# THE HARVESTER

<https://github.com/laramies/theHarvester>

- **Obtiene datos de un objetivo usando muchos sitios diferentes como fuentes**

- Obtiene mucha información de fuentes de datos públicas: correos electrónicos, nombres, subdominios, IP, URLs...
- Utiliza motores de búsqueda conocidos para diferentes tipos de información
  - baidu, bing, bingapi, censys, Comodo Certificate search, dnsdumpster, dogpile, duckduckgo, github-code, Google (Google dorking opcional), google-certificates, hunter, intelx, Linkedin, Netcraft Data Mining, securityTrails (información histórica DNS), Shodan, threatcrowd, trello, Twitter, Bing virtual hosts search, Virustotal, y Yahoo search engine

- **También información de servidores DNS**

- Fuerza bruta, búsqueda inversa, expansión TLD

- **Tutorial**

- <https://www.welivesecurity.com/la-es/2015/04/08/the-harvester-riesgo-informacion-publica/>

```
sampaio@kali:~$ theharvester -h
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

*****
*          THE HARVESTER          *
*          v3.0.6                  *
*          Coded by Christian Martorella   *
*          Edge-Security Research           *
*          cmartorella@edge-security.com    *
*****


Usage: theharvester options

-d: Domain to search or company name
-b: data source: baidu, bing, bingapi, censys, crtsh, dogpile,
     google, google-certificates, googleCSE, googleplus, google-pro
     files,
     hunter, linkedin, netcraft, pgp, threatcrowd,
     twitter, vhost, virustotal, yahoo, all
-g: use Google dorking instead of normal Google search
-s: start in result number X (default: 0)
-v: verify host name via DNS resolution and search for virtual hosts
```

# SCRUMMAGE

<https://github.com/matamorphosis/Scrummage>

## ● Centraliza los análisis OSINT

- Nos da una vista de alto nivel de los sitios con información de un objetivo

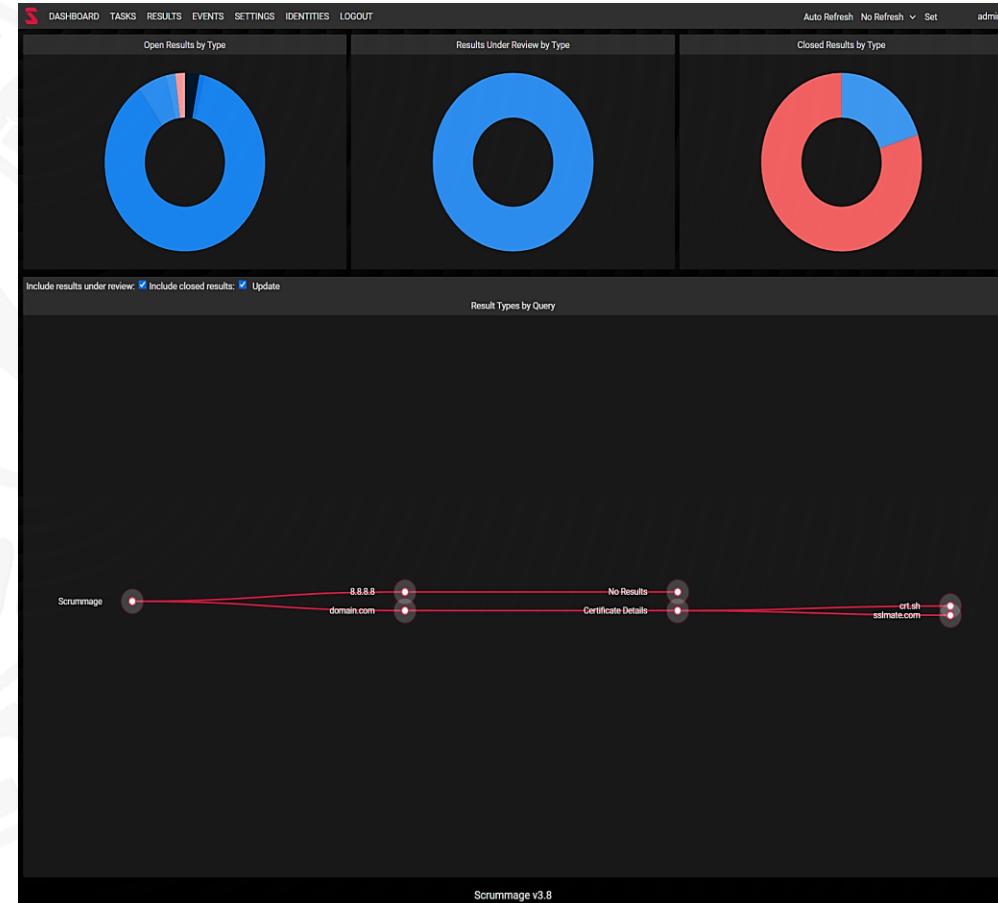
## ● Implementa plugins para personalizar el tipo de escaneos y optimizar el uso de recursos

## ● Estos plugins le dan diversas capacidades

- Búsqueda en blockchain
- Domain fuzzing
- Análisis de Twitter
- Búsqueda en Instagram
- Buscar en Have I Been Pwned? (<https://haveibeenpwned.com/>)
  - En caso de que se haya filtrado alguna identidad de cuenta
- ...

## ● Herramientas similares

- OSINT Framework: <https://github.com/lockfale/osint-framework>
- Scumblr: <https://portunreachable.com/automated-osint-withscumblr-a4d81a048e54?gi=ae6ebac43a92>



# AIL FRAMEWORK

<https://github.com/CIRCL/AI-framework>



Seguridad de Sistemas  
Informáticos

## ● Framework muy modular que analiza la información filtrada

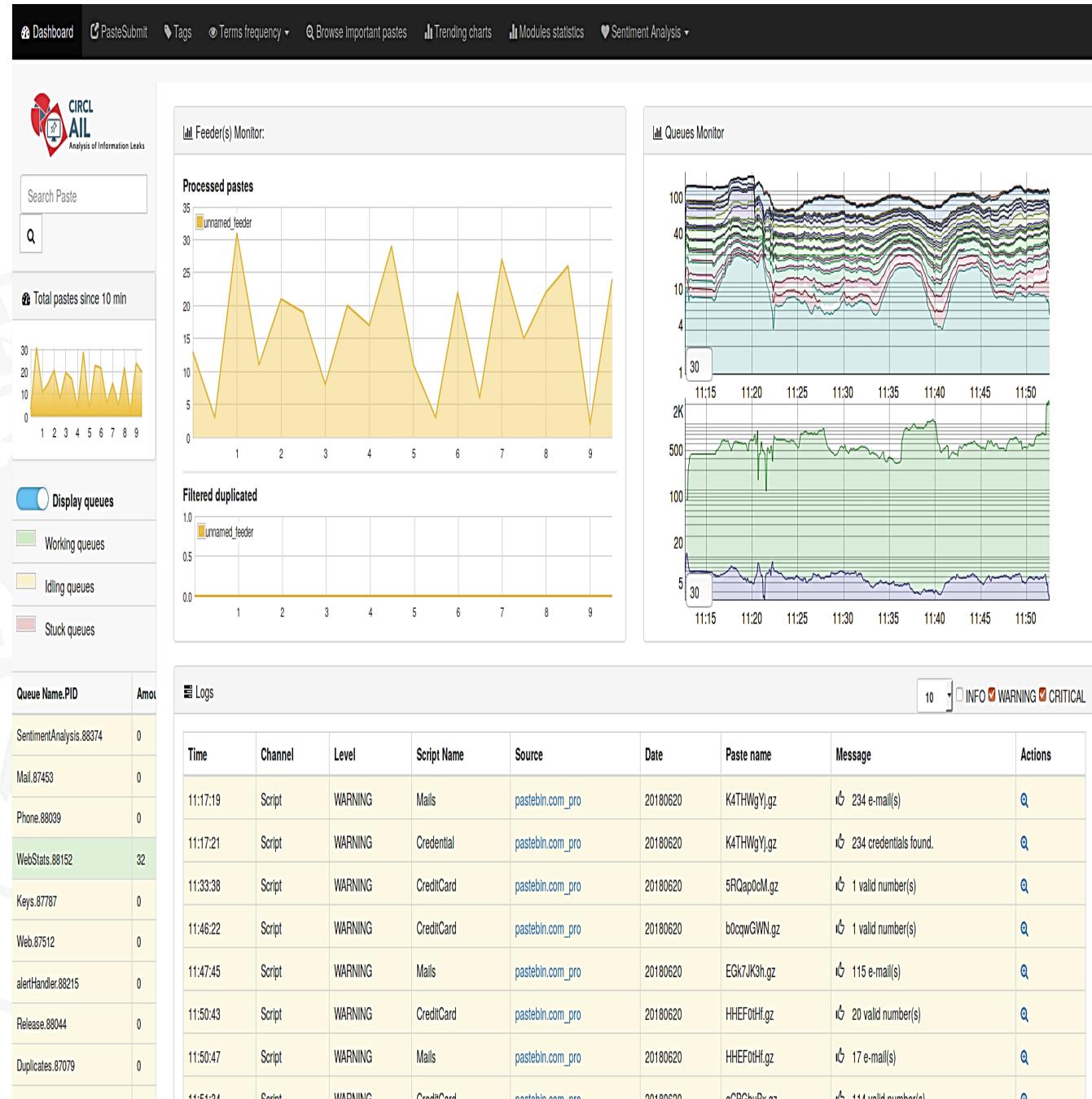
- De fuentes no estructuradas
- Un origen de datos popular es Pastebin

## ● Su alta modularidad permite ampliarla

- Y usarla para extraer y procesar información privada de diferentes tipos
- Y por lo tanto detectar y prevenir la fuga de información

## ● Para obtener más información

- <https://www.kitploit.com/2019/08/ail-framework-for-analysis-of.html>



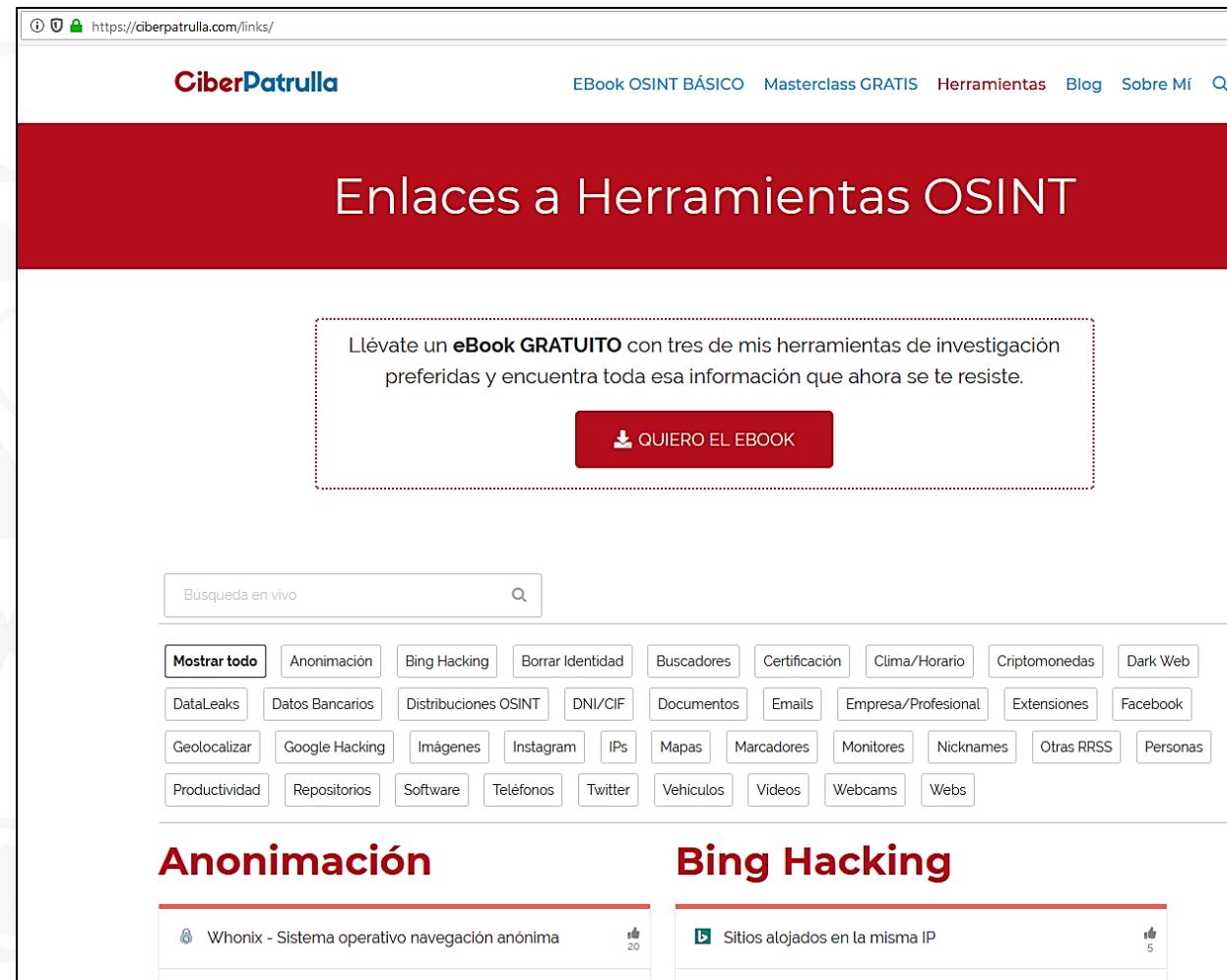
# MÁS HERRAMIENTAS OSINT...

- **Las técnicas OSINT son populares y potentes debido a la información que pueden encontrar**

- Hay una gran cantidad de herramientas que obtienen información de diferentes medios de comunicación y redes sociales en Internet
- Es muy difícil enumerarlas a todas

- **Hay una lista clasificada de herramientas:** <https://ciberpatrulla.com/links/>

- Esta web es probablemente el repositorio más completo en herramientas OSINT
- Contiene cientos de herramientas clasificadas por su uso en el mundo OSINT
- Redes sociales, vehículos, teléfonos, documentos... ¡hasta 38 categorías diferentes de herramientas!



The screenshot shows the homepage of CiberPatrulla with a red header bar containing the title "Enlaces a Herramientas OSINT". Below the header is a call-to-action box for an "eBook GRATUITO". The main content area features a search bar labeled "Búsqueda en vivo" and a grid of 38 categories. Two specific sections are highlighted: "Anonimación" and "Bing Hacking".

**CiberPatrulla**

EBook OSINT BÁSICO Masterclass GRATIS Herramientas Blog Sobre Mí

Enlaces a Herramientas OSINT

Llévate un **eBook GRATUITO** con tres de mis herramientas de investigación preferidas y encuentra toda esa información que ahora se te resiste.

QUIERO EL EBOOK

Búsqueda en vivo

Mostrar todo Anonimación Bing Hacking Borrar Identidad Buscadores Certificación Clima/Horario Criptomonedas Dark Web DataLeaks Datos Bancarios Distribuciones OSINT DNI/CIF Documentos Emails Empresa/Profesional Extensiones Facebook Geolocalizar Google Hacking Imágenes Instagram IPs Mapas Marcadores Monitores Nicknames Otras RSS Personas Productividad Repositorios Software Teléfonos Twitter Vehículos Videos Webcams Webs

**Anonimación**

Whonix - Sistema operativo navegación anónima

**Bing Hacking**

Sitios alojados en la misma IP

# ¿TIENES EJEMPLOS?

- **Con esta cantidad de herramientas disponibles, es muy fácil perderse al iniciar una investigación OSINT**
- **Por lo tanto, es mejor ver ejemplos de cómo hacer una**
- **Como guía se puede seguir este tutorial de cuatro partes**
  - <https://delta.navisec.io/osint-for-pentesters-part-1-passive-recon-and-asset-discovery/>
  - <https://delta.navisec.io/osint-for-pentesters-part-2-linkedin-is-not-just-for-jobs/>
  - <https://delta.navisec.io/osint-for-pentesters-part-3-password-spraying-methodology/>
  - <https://delta.navisec.io/a-pentesters-guide-part-4-grabbing-hashes-and-forging-external-footholds/>
- **O esta guía OSINT**
  - <https://www.hackers-arise.com/osint>
- **Podemos encontrar además más herramientas en esta web**
  - Extracción de metadatos, geolocalización, extracción de subdominios, etc.
  - <https://derechodelared.com/herramientas-osint-recopilatorio/>

# EJEMPLOS

**(1) Usar Google Hacking para encontrar recursos de Uniovi**

**(2) Uso de Tinfoleak**

Tutorial de cómo obtener una API Key de Twitter: <http://www.noise-sv.com/tutorial-de-tinfoleak/>

< Ir al Índice

# OSINT CONTRA CÓDIGO FUENTE

El código fuente también puede ser una amenaza OSINT



## ● Encontrar información privada es, por desgracia, común en el código fuente

- Cadenas de conexión, nombres de usuario, claves, API Keys (con las que solicitar servicios en nombre de la aplicación), direcciones de servidor BBDD, Amazon buckets desprotegidos (almacenamiento en nube)...
- Cuando se carga código en GitHub, esta información es un objetivo OSINT

## ● GitGot permite buscar datos confidenciales en código alojado en GitHub:

- Búsquedas generales, de un propósito particular, o para ciertos tipos de información confidencial
- Una herramienta similar, pero especializada en encontrar API Keys, es GitHound:  
<https://www.kitploit.com/2019/07/git-hound-find-exposed-keys-across.html?m=1>

```
https://github.com/intel/pa-blink/blob/98565fea6e44a40fac3901b8d4bcd0029c708032/LayoutTests/fast/url/script-tests/segments.js
["http://example.com/", ["http:" "example.org" "", "/example.com/", "", ""], ["ftp:" 'example.com', "", "/"], ["https:" "example.com", "", "/"], ["madeupscheme:" "", "", '/example.com', "", ""], ["file:" "", "", "/example.com/", "", ""], ["ftps:" "", "", "/example.com/", "", ""], ["gopher:" "example.com", "", "", ""], ["ws:" "example.com", "", "/"], ["wss:" "example.com", "", "/"], ["data:" "example.com", "", ""], ["javascript:" "example.com", "", ""], ["mailto:" "example.com", "", ""], ["http:example.com/", ["http:" "example.org" "", "/foo/example.com/", "", ""], ["ftp:" "example.com", "", "/"], ["https:" "example.com", "", "/"], ["madeupscheme:" "", "", 'example.com', "", ""], ["file:" "", "", "/example.com/", "", ""], ["ftps:" "", "", "example.com", "", ""], ["gopher:" "example.com", "", "", ""], ["ws:" "example.com", "", "/"], ["wss:" "example.com", "", "/"], ["data:" "example.com", "", ""], ["javascript:" "", "", "example.com/", "", ""], ["mailto:" "", "", "example.com/", "", ""], End of Matches
(Result 12/1000)==== Ignore similar [c]ontents/[u]ser/[r]epo/[f]ilename, [p]rint contents, [s]ave state, [a]dd to log, search [/findme], [b]lack, [q]uit, next [<Enter>]==: ]
```

- **Herramienta utilizada para encontrar archivos con información sensible en repositorios públicos de GitHub**

- Puede clonar repositorios que pertenezcan al objetivo indicado
- La clonación tiene una profundidad configurable para controlar el uso de recursos
- Una vez clonado, recorrerá los archivos del repositorio buscando aquellos que considera relevantes
- El resultado se presenta en un informe web para su posterior análisis

- **Tutorial**

- <https://michenriksen.com/blog/gitrob-putting-the-open-source-in-osint/>



```
[*] Starting Gitrob version 0.0.1 at 2015-01-06 08:46 CST
[*] Loading configuration... done
[*] Preparing SQL database... done
[*] Loading file patterns... done
[*] Collecting organization repositories... done
[*] Collecting organization members... done
[*] Collecting member repositories...
[>] Collected 1 repository from aden
[>] Collected 12 repositories from adelcambre
[>] Collected 11 repositories from achiu
[>] Collected 6 repositories from alanjrogers
[>] Collected 3 repositories from amateurhuman
[>] Collected 16 repositories from alysonla
[>] Collected 6 repositories from ammeep
[>] Collected 13 repositories from arfon
[>] Collected 13 repositories from antonio
[>] Collected 5 repositories from aroben
[>] Collected 6 repositories from arrbee
[>] Collected 17 repositories from atmos
[>] Collected 6 repositories from azizshamim
[>] Collected 5 repositories from balevine
[>] Collected 19 repositories from benbalter
[*] 14/199 [=====  
]
```

Fuente: <https://blog.segu-info.com.ar/2018/06/gitrob-herramienta-de-reconocimiento-de.html?m=0>

# GITGRABER

<https://github.com/hisxo/gitGraber>

- Herramienta para encontrar datos confidenciales en repositorios de GitHub
- Incluye datos de varias fuentes que pueden haber quedado en archivos del repositorio
- Entre otras fuentes, incluye
  - Google
  - Amazon (AWS)
  - Paypal
  - Github
  - Facebook
  - Twitter
  - ...

```
root@bugbounty# python3 gitGraber.py -k wordlists/keywords.txt -q "yahoo" -s

[i] Github query : https://api.github.com/search/code?q=yahoo access_key&sort=indexed&o=desc
[i] Status code : 200
[!] POSSIBLE AWS TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-09-10T13:40:08Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/[REDACTED]/[REDACTED]/cmd_bash.md
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]

[i] Github query : https://api.github.com/search/code?q=yahoo access_token&sort=indexed&o=desc
[i] Status code : 200
[!] POSSIBLE GOOGLE_FIREBASE_OR_MAPS TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-09-11T20:12:28Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/connectApp/[REDACTED]/app.js
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]

[!] POSSIBLE TWILIO TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-07-30T06:28:32Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/[REDACTED]/[REDACTED]/project.html
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]
```

# ¡EL PROPIO GITHUB!



Seguridad de Sistemas  
Informáticos

- La opción de búsqueda de GitHub se puede usar para encontrar información privada en repositorios públicos

- Es una función muy potente que permite buscar por muchos términos

- Como Google Hacking (Google Dorks), pero para código
- ¡De hecho, mucha gente llama a esto GitHub Dorks!

- La imagen muestra varias búsquedas populares como ejemplo



Anton

@therceman

filename:manifest.xml  
filename:travis.yml  
filename:vim\_settings.xml  
filename:database  
filename:prod.exs  
filename:prod.secret.exs  
filename:.npmrc\_auth  
filename:dockercfg  
filename:WebServers.xml  
filename:.bash\_history  
filename:sftp-config.json  
filename:sftp.json  
filename:secrets.yml  
filename:.esmtprc  
filename:passwd  
filename:LocalSettings.php

## GitHub Dorks for Finding Files

filename:config.php  
filename:config.inc.php  
filename:prod.secret.exs  
filename:configuration.php  
filename:.sh\_history  
filename:shadow  
filename:proftpdpasswd  
filename:pgpass  
filename:idea14.key  
filename:hub  
filename:.bash\_profile  
filename:.env  
filename:wp-config.php  
filename:credentials  
filename:id\_rsa  
filename:id\_dsa

filename:.ovpn  
filename:.cscfg  
filename:.rdp  
filename:.mdf  
filename:.sdf  
filename:.sqlite  
filename:.psafe3  
filename:secret\_token.rb  
filename:carrierwave.rb  
filename:database.yml  
filename:.keychain  
filename:.kwallet  
filename:.exports  
filename:config.yaml  
filename:settings.py  
filename:credentials.xml

## GitHub Dorks for Finding API Keys, Tokens and Passwords

api\_key  
authorization\_bearer:  
oauth  
auth  
authentication  
client\_secret  
api\_token:  
client\_id

OTP  
HOMEBREW\_GITHUB\_API\_TOKEN  
SF\_USERNAME  
HEROKU\_API\_KEY  
JEKYLL\_GITHUB\_TOKEN  
shodan\_api\_key  
api.forecast.io

password  
user\_password  
user\_pass  
passcode  
client\_secret  
secret  
password hash  
user auth

## GitHub Dorks Automation Tools

TruffleHog	- <a href="https://github.com/dxa4481/truffleHog">https://github.com/dxa4481/truffleHog</a>
Github-Dorks	- <a href="https://github.com/techgaun/github-dorks">https://github.com/techgaun/github-dorks</a>
GitGot	- <a href="https://github.com/BishopFox/GitGot">https://github.com/BishopFox/GitGot</a>
GitMonitor	- <a href="https://github.com/Talkaboutcybersecurity/GitMonitor">https://github.com/Talkaboutcybersecurity/GitMonitor</a>
GitRob	- <a href="https://github.com/michenriksen/gitrob">https://github.com/michenriksen/gitrob</a>
GitHound	- <a href="https://github.com/tillson/git-hound">https://github.com/tillson/git-hound</a>
GittyLeaks	- <a href="https://github.com/kootenpv/gittyleaks">https://github.com/kootenpv/gittyleaks</a>
GitSecrets	- <a href="https://github.com/awslabs/git-secrets">https://github.com/awslabs/git-secrets</a>
Watchtower	- <a href="https://radar.nightfall.ai">https://radar.nightfall.ai</a>

[www.therceman.dev](#)



# LISTA DE LOGROS PARA AUTOEVALUACIÓN: SEMINARIO 1

Nivel	Concepto
	Entender el concepto OSINT
	Entender qué tipos de dispositivos podemos encontrar en Internet
	Saber qué tipo de información no debe poner en el código fuente
	Saber cómo usar las herramientas OSINT Shodan y Censys para encontrar máquinas de un objetivo
	Saber cómo usar Google Hacking para encontrar información de un objetivo concreto
	Conocer múltiples herramientas OSINT que trabajan con información personal de individuos / empresas
	Conocer herramientas para estudiar el código fuente en repositorios públicos
	Saber cómo estudiar un objetivo con Google Hacking
	Saber cómo estudiar a una persona usando Tinfoleak
	<b>Animal Social:</b> Ser capaz de localizar información de máquinas, usuarios y código fuente en Internet

# SEMINARIO 1. HERRAMIENTAS PARA INVESTIGAR EN INTERNET

