

SEMINARIO 1

HERRAMIENTAS PARA INVESTIGAR EN INTERNET



Obtener información acerca de máquinas, personas y código fuente!



PROYECTO "S-81 ISAAC PERAL" v4.2

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

Logo: @creative_vanesa
(Instagram)



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo



ACERCA DEL USO DE CONTENIDO GENERADO POR IA



- En esta presentación se usan algunas imágenes generadas por IA
 - Salvo error, cualquier imagen a la que no se le atribuya una fuente u origen expreso
- La IA generativa usada para ello es Microsoft Copilot
 - <https://copilot.microsoft.com/>
- Se ha restringido el uso de estas imágenes a la ilustración de los conceptos explicados en algunas de las páginas
 - Es decir, como refuerzo visual a lo explicado en algunas transparencias
 - El procedimiento ha sido describirle a la IA con toda la precisión posible los elementos que quería que apareciesen en la imagen (**prompt**)
 - Y la selección del mejor resultado obtenido, a juicio del autor de esta presentación
 - No se ha mencionado ni indicado que se copie el estilo a ningún autor, ni que se plagien obras concretas
- El autor declara expresamente su apoyo al trabajo de los artistas, ilustradores y creadores, de extrema importancia en la actualidad
 - El uso de estas técnicas se ha hecho solo con fines de mejora de las explicaciones, y cuando la alternativa era no contar con refuerzos visuales por restricciones de tiempo y presupuesto

INTRODUCCIÓN

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

- Incluso sin conocimientos técnicos se puede obtener mucha información de personas/entidades
 - Que puede ser explotada para obtener ventajas
 - Todo lo que está en Internet puede averiguarse.... 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
- Pero, sobre todo, explotaremos más esta rama en el **Trabajo en Grupo** de la asignatura



EGOSURFING: ¿ESTOY EXPUESTO?

● Con estas herramientas es posible que veas que estás exponiendo mucha información

- Buscarse a sí mismo en Internet se llama "egosurfing"
- **Hay formas de recuperar tu privacidad**
 - Puedes seguir esta guía: <https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954?gi=57af4dc583d>
- También damos más consejos sobre cómo manejarse en Internet y las redes sociales en los siguientes cursos gratuitos
 - Están en: https://github.com/jose-r-lopez/Formacion_-Seguridad_Joven/wiki
 - Redes sociales: F-31 "Descubierta"
 - Ataques sobre las personas: P-74 "Atalaya"

● Más información

- <https://www.lisainstitute.com/blogs/blog/que-es-el-egosurfing-y-como-puede-ayudarnos>
- <https://www.incibe.es/ciudadania/blog/egosurfing-que-information-hay-sobre-mi-en-internet>

ÍNDICE



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



🔍💻 OSINT CONTRA MÁQUINAS

Investigando máquinas usando solo información pública



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

SHODAN

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

● Motor de búsqueda de máquinas (no de webs)

- Routers, servidores, cámaras... (IoT)
- 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/>



Seguridad de Sistemas
Informáticos

Web Technologies

MOODLE PHP REQUIREJS

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

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. Server 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=j25o9m0cman0dkarptfvspemup; 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:e1:
55:04:f5:70:79:f4:44:1a:fa:d2:77:e4:38:75:
4c:51:3a: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:0d: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

shodan test search

New to Shodan? Login or Register

Exploits Maps

TOTAL RESULTS: 14,301,988

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: "6f-5380a934e98500"

Accept-Ranges: bytes

Content-Length: 111

Connection: close

Content-Type: text/html

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

TOP COUNTRIES

Country	Count
United States	4,765,632
Mexico	1,234,983
China	1,051,604
Germany	1,044,601
Japon	896,419

TOP SERVICES

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

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



Filter Reference

- **Tener una cuenta en Shodan da**
 - La potencia de sus **filtros de búsqueda**
 - ¡Es como un **Google** de máquinas!
 - Puedes buscar máquinas usando gran cantidad de criterios
 - **Una API Key** para integrarlo en tus programas (**Shodan CLI**)
 - <https://cli.shodan.io/>
- **Puede encontrar muchos datos útiles de dispositivos expuestos**
 - Incluidos aspectos avanzados de servicios HTTP y SSL
 - Cualquier clase de servidor, dispositivo IoT...expuesto a Internet
 - <https://github.com/jakejarvis/awesome-shodan-queries>

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.securitytxt
- 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
- sslChain_count
- sslCipher.bits
- sslCipher.name
- sslCipherversion
- sslJa3s
- sslJarm
- sslVersion

Bitcoin

- bitcoin.ip
- bitcoin.ip_count
- bitcoin.port
- bitcoin.version

CENSYS

<https://censys.io/>



Seguridad de Sistemas
Informáticos

● 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: <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/>

● En el A-21 “Poseidón” (Trabajo en Grupo) encontrarás más motores similares

The screenshot shows the Censys search interface with the query "IPv4 Hosts" and the result "156.35.0.0/16". The interface includes a sidebar with "Quick Filters" for fields like Autonomous System and Protocol, and a main area displaying a list of hosts. Each host entry includes its IP address, name, service details (e.g., port, protocol), and location.

Host IP	Host Name	Protocol	Location
156.35.151.5	(orion.edv.uniovi.es)	80/http	Oviedo, Principality of Asturias, Spain
156.35.11.15		80/http	Oviedo, Principality of Asturias, Spain
156.35.25.195	(crisa25195.econo.uniovi.es)	443/https, 80/http	Oviedo, Principality of Asturias, Spain
156.35.225.33	(portalgp.uniovi.es)	443/https	Oviedo, Principality of Asturias, Spain
156.35.172.86	(imprisa.epv.uniovi.es)	3389/rdp	Oviedo, Principality of Asturias, Spain
156.35.119.112	(hercules.lsi.uniovi.es)	3389/rdp	Oviedo, Principality of Asturias, Spain
156.35.81.145	(llama81145.euitio.uniovi.es)		

!? Usar Shodan / Censys para
encontrar información

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 que 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

GOOGLE HACKING: PROCESO

EXPLOIT DATABASE

Google Hacking Database

Show 15 Dork

Date Added	Dork
2020-01-17	intitle:'WS02 Management Console'
2020-01-10	intitle:'webView login' alcatel lucent
2020-01-09	intitle:'LABVANTAGE Logon'
2020-01-09	site:/cgi/domadmin.cgi
2020-01-09	inurl:'8080/login.jsp?os_destination='
2020-01-09	intitle:index.of "wp-security-audit-log"
2020-01-09	intext:"powered by codoforum" inurl:"user/login"
2020-01-06	inurl:index.php?enterguest"
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

Author

Begin typing... GET CERTIFIED

Filters

Google Dork Description:
intitle:"Apache2 Ubuntu Default Page: It works"

GHDB-ID: 5311 **Author:** REZA ABASI

Published: 2019-07-31

web server detection:
intitle:"Apache2 Ubuntu Default Page: It works"
Reza Abasi (Turku)

Google Search: intitle:"Apache2 Ubuntu Default Page: It works"

Google Hacking Database

Show 15 Dork

Date Added	Dork	Category
2019-09-24	site:/server-status intext:"Apache server status for"	Web Server Detection
2019-09-02	inurl:iisstart.htm intitle:IIS7	Web Server Detection
2019-08-30	inurl:phpmyadmin/changelog.php -github -gitlab	Web Server Detection
2019-08-12	inurl:WebPortal?bankir	Web Server Detection
2019-07-31	intitle:"Apache2 Ubuntu Default Page: It works"	Web Server Detection
2019-07-31	intitle:"IIS Windows Server"-inurl:"IIS Windows Server"	Web Server Detection
2019-07-29	inurl:server-status + "Server MPM."	Web Server Detection
2019-06-24	inurl:phpinfo.php intext:build 2600	Web Server Detection
2019-06-17	inurl:OrganizationChart.cc	Web Server Detection
2019-06-17	intext:"Brought to you by eVetSites"	Web Server Detection
2019-06-06	intext:"Powered by GetSimple" -site:get-simple.info	Web Server Detection
2019-05-20	inurl:icool.php	Web Server Detection

Google Search: intitle:"Apache2 Ubuntu Default Page: It works"

Aproximadamente 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]

GooFuzz

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



Seguridad de Sistemas
Informáticos



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

- Sin hacer peticiones directas al servidor web concreto
- Ficheros, directorios, subdominios...

● Tutorial:

- <https://www.youtube.com/watch?v=DY8k-WEravY>

```
> ./GooFuzz -t nasa.gov -e pdf,bak,old -d 10
*****
* GooFuzz 1.2.2 - The Power of Google Dorks *
*****
```

Target: nasa.gov

```
=====
Extension: pdf
=====
```

https://history.nasa.gov/alsj/a11/A11_PressKit.pdf
https://history.nasa.gov/alsj/a13/A13_PressKit.pdf
https://history.nasa.gov/alsj/a14/A14_PressKit.pdf
https://history.nasa.gov/alsj/a15/A15_PressKit.pdf
https://history.nasa.gov/alsj/a410/A07_PressKit.pdf
https://history.nasa.gov/alsj/a410/A09_PressKit.pdf
<https://history.nasa.gov/monograph15.pdf>
https://www.hq.nasa.gov/alsj/LLRV_Monograph.pdf

```
=====
Extension: bak
=====
```

https://bocachica.arc.nasa.gov/ATTREX_2013/rh/rh_omega_oct3.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2013/rh/rh_omega_sep30.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2014/attrex2014_satmap.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2014/schom/schomfigures_20140126.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2014/schom/schomfigures_20140226.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2014/trajfigures/trajfigures.html.bak
<https://bocachica.arc.nasa.gov/POSIDON/posidon.html.bak>
https://hesperia.gsfc.nasa.gov/hessi/solar_install/installation.bak
<https://ndeaa.jpl.nasa.gov/nasa-nde/outreach/outreach.html.bak>
<https://ndeaa.jpl.nasa.gov/nasa-nde/yosi/yosi.htm.bak>

```
=====
Extension: old
=====
```

https://bocachica.arc.nasa.gov/HAVE/nmc_rh_omega_plots.html.old
https://echo.jpl.nasa.gov/asteroids/1988TA/1988TA_planning.html.old
https://echo.jpl.nasa.gov/asteroids/1998QE2/1998QE2_planning.html.old
https://echo.jpl.nasa.gov/asteroids/2014J025/2014J025_planning.html.old
https://echo.jpl.nasa.gov/asteroids/goldstone_asteroid_schedule.html.old
https://fits.gsfc.nasa.gov/users_guide/users_guide.ps.old
<https://image.msfc.nasa.gov/ChrisDocs/UDFInstall/uLibInstall.old>
https://seawifs.gsfc.nasa.gov/OCEAN_PLANET/HTML/titanic.html.old
https://umhra.nascom.nasa.gov/sohn/bga_history.html.old



🔍 🧑 OSINT CONTRA PERSONAS

Investigando gente usando solo información pública



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo



Redes sociales

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





LA PROBLEMÁTICA DE LAS HERRAMIENTAS QUE TRABAJAN CON RRSS

● A las RRSS no les gustan las herramientas que extraen información de sus perfiles ☺

- Y eso nos mete en una carrera del “gato y el ratón”
- Obligándonos a buscar herramientas que sigan funcionando

● Puedes encontrar muchas en Ciberpatrulla

- Y en el OSINT Framework: <https://osintframework.com/>

● Twitter (ahora X) es un ejemplo de ello

- El acceso a la API se hizo de pago, lo que mató a muchas herramientas de investigación
- Esto dejó operativas (algunas) de las que hacen scraping
 - Es decir, **procesar los contenidos que se muestran por pantalla**, actuando como si fueran usuarios normales
- Algunas son (pero no descartes que dejen de funcionar)
 - <https://github.com/tweepy/tweepy>
 - <https://github.com/dataquestio/twitter-scrape>

Ciberpatrulla es un enorme repositorio de herramientas OSINT, entre las que hay muchas que trabajan en redes sociales:

<https://ciberpatrulla.com/links/>

Facebook

- ⌚ Descargar videos de Facebook
- ⌚ Whopostedwhat - Busca por fechas
- ⌚ Exportador de comentarios a CSV
- ⌚ Socialfy - Exportar comentarios a CSV
- ⌚ FB-Search - Búsqueda en Facebook
- ⌚ Intelx - Búsqueda en Facebook
- ⌚ URLs personalizadas para buscar en Facebook
- ⌚ Obtener ID perfil de Facebook

Instagram

- ⌚ Buscar en google por frase concreta
- ⌚ Cuidado con los avisos de capturas!
- ⌚ Picodash - Búsqueda en Instagram
- ⌚ Exportador de comentarios a CSV
- ⌚ Tucktools - Descargar Videos de Instagram
- ⌚ Instafollowers - Obtener ID de Instagram
- ⌚ Buyinstagramfollowers - Obtener ID de Instagram
- ⌚ Allsmo - Obtener ID de Instagram
- ⌚ Otzberg - Obtener ID de Instagram
- ⌚ Instagram - Buscar por localización
- ⌚ Obtener usuario desde la ID

Otras RRSS

- ⌚ Busca en RRSS menos importantes

HUNTER.IO

<https://hunter.io/>



Seguridad de Sistemas
Informáticos

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

- *¿Qué ataques se pueden realizar contra el correo electrónico de una determinada persona en un alto cargo en una empresa?*

- 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 homepage with a search bar at the top. Below it, there's a section titled "Email Finder" where the domain "uniovi.es" has been entered. A red button labeled "Find email addresses" is visible. The main area displays a list of found email addresses:

Email Address	Sources
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

At the bottom of the list, a link reads "2,667 more results for 'uniovi.es'".

PROJECT SHERLOCK

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



Seguridad de Sistemas
Informáticos

- Encuentra nombres de usuario en muchas RRSS o webs diferentes

- ¡Más de 320!

- *¿Cómo usarás una herramienta como esta para adivinar información sobre las personas?*

- 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 información de usuarios desde varias fuentes

Agregando datos de usuarios



MALTEGO

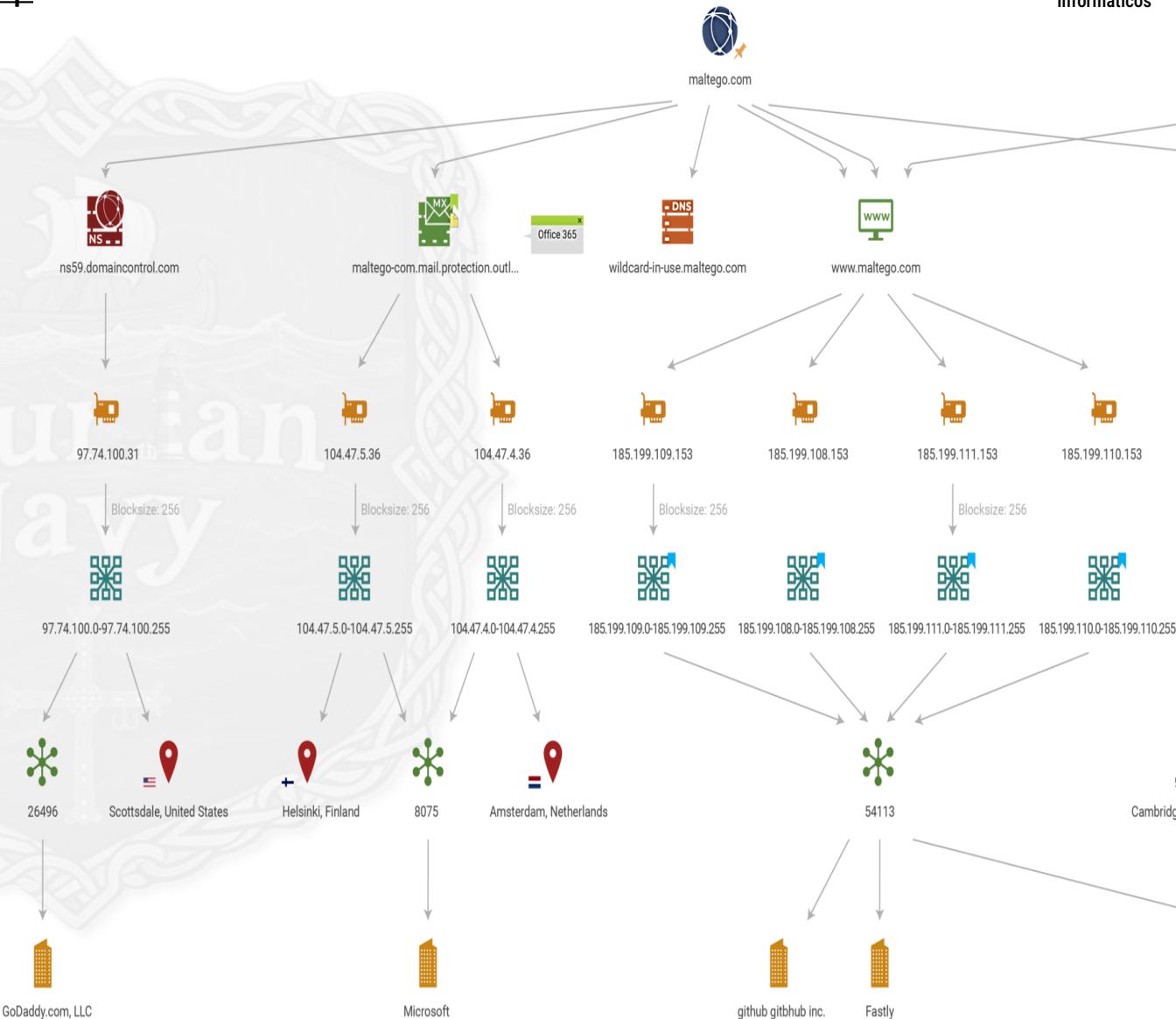
<https://www.paterva.com/buy/maltego-clients/maltego-ce.php>

● Recopila información de entidades de internet

- Crea entidades personalizadas que representan cualquier información
- Se especializa en encontrar relaciones entre ellas
 - Redes sociales, redes de ordenadores, dominios...
- Utiliza como fuentes DNS, registros **whois**, buscadores, RRSS, 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
- Descrita en el **A-21 “Poseidón” (Trabajos en Grupo)**



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

RECON-NG

<https://github.com/lanmaster53/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 (**Tema 7**) para las personas que ya están familiarizados con él

● Tutoriales

 - <https://hackertarget.com/recon-ng-tutorial/>
 - <https://noticiasseguridad.com/tutoriales/recon-ng-herramienta-para-recoleccion-de-informacion/>

```
carlos@NoSoloHacking:~/recon-ng$ sudo ./recon-ng

Sponsored by ...
          ^ 
         / \ \ ^ 
        ^ \ / \ \ \ \ \ 
       / \ \ / \ \ \ \ \ \ \ 
      // \ \ BLACK HILLS V \ \
      www.blackhillsinfosec.com

PRACTISE
www.practise.com

[*] No modules enabled/installed.

[recon-ng][default] > |
```

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

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, buscadores...
 - 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-harvesterriesgo-nformacion-publica/>

SCRUMMAGE

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

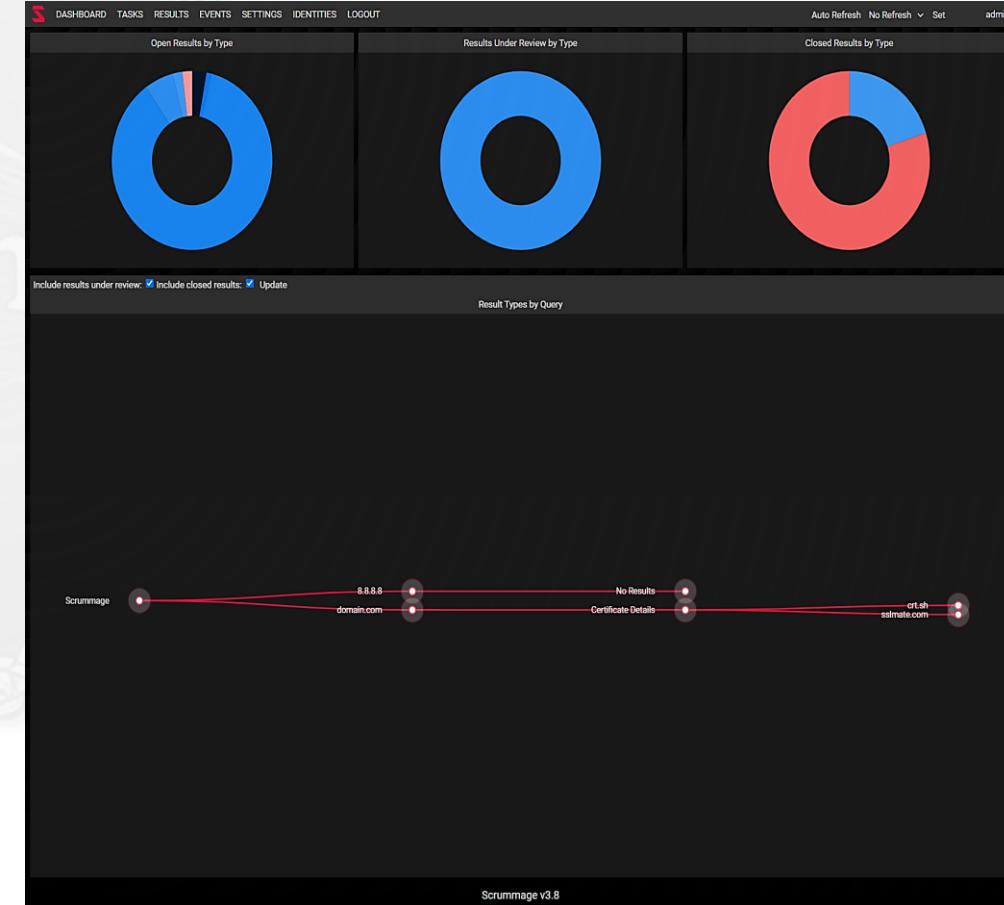
● Centraliza los análisis OSINT

- 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/>)
 - **Lab 2**, por si se ha filtrado alguna identidad de cuenta
- ...



AIL FRAMEWORK

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



Seguridad de Sistemas
Informáticos

● Framework muy modular que analiza la información filtrada

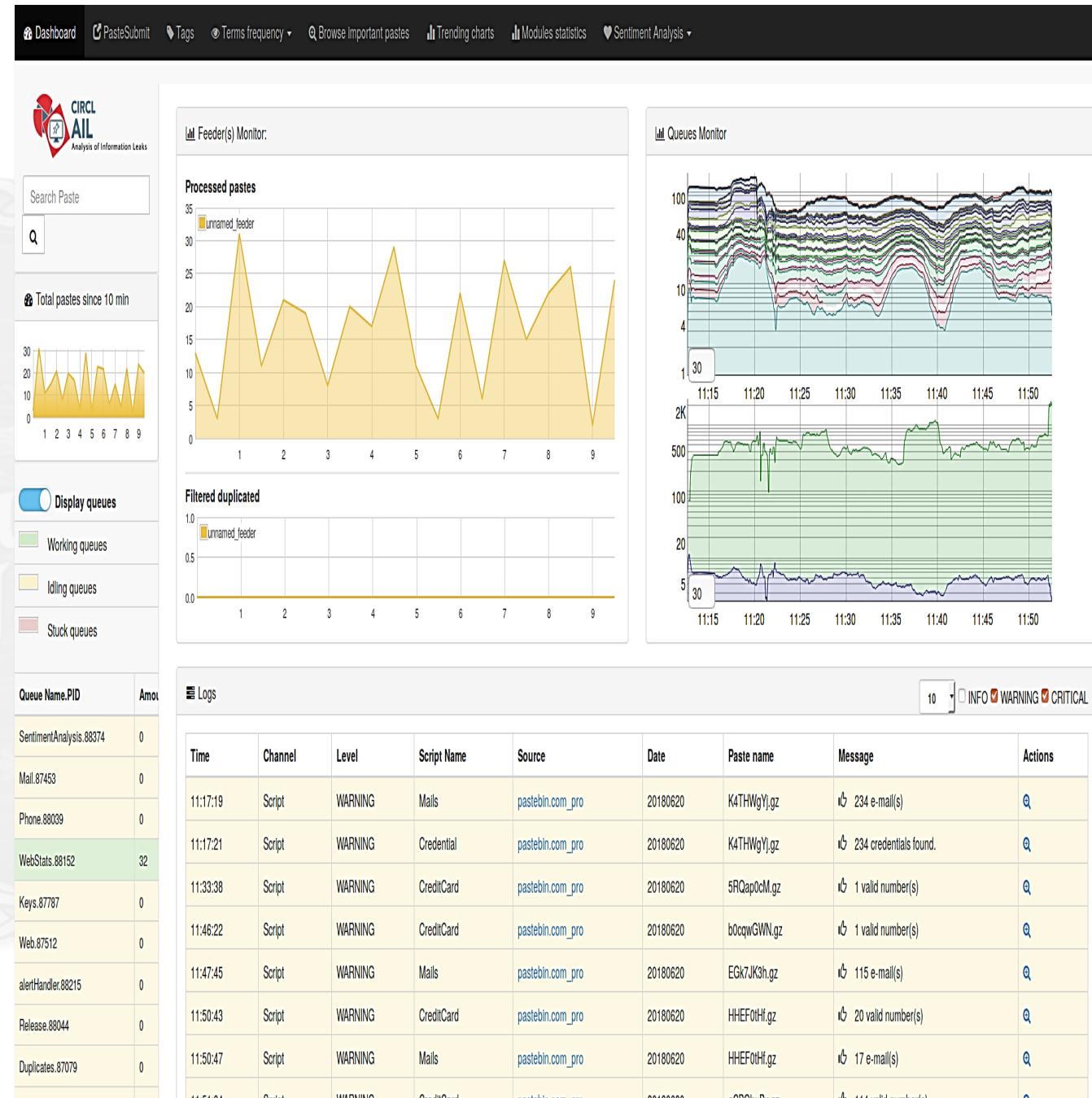
- De fuentes no estructuradas
- Un origen de datos popular es Pastebin

● 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>





¿TIENES EJEMPLOS?

• Como guía se puede seguir este tutorial de cinco partes

- <https://navisec.io/a-pentesters-guide-part-1-osint-passive-recon-and-discovery-of-assets/>
- <https://navisec.io/a-pentesters-guide-part-2-osint-linkedin-is-not-just-for-jobs/>
- <https://navisec.io/a-pentesters-guide-part-3-osint-breach-dumps-password-spraying/>
- <https://navisec.io/a-pentesters-guide-part-4-grabbing-hashes-and-forging-external-footholds/>
- <https://navisec.io/a-pentesters-guide-part-5-unmasking-wafs-and-finding-the-source/>

• 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/>

• O en el material que te vamos a dar para los Trabajos en Grupo ☺



Usar Google Hacking para encontrar recursos de Uniovi



OSINT CONTRA CÓDIGO FUENTE

El código fuente también puede ser una amenaza
OSINT



GITGOT

<https://github.com/BishopFox/GitGot>

● 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/", ["madeupscheme:", "", "", "/example.com/", "", "", ""], ["file:", "", "", "/example.com/", "", "", ""], ["ftps:/example.com/", ["ftps:", "", "", "/example.com/", "", "", ""], ["gopher:/example.com/", ["gopher:", "example.com", "", "/", "", "", ""], ["ws:/example.com/", ["ws:", "example.com", "", "/", "", "", ""], ["wss:/example.com/", ["wss:", "example.com", "", "/", "", "", ""], ["data:/example.com/", ["data:", "", "", "/example.com/", "", "", ""], ["javascript:/example.com/", ["javascript:", "", "", "/example.com/", "", "", ""], ["mailto:/example.com/", ["mailto:", "", "", "/example.com/", "", "", ""], ["http:example.com/", ["http:", "example.org", "", "/foo/example.com/", "", "", ""], ["ftp:/example.com/", ["ftp:", "example.com", "", "/", "", "", ""], ["https:/example.com/", ["https:", "example.com", "", "/", "", "", ""], ["madeupscheme:/example.com/", ["madeupscheme:", "", "", "/example.com/", "", "", ""], ["file:/example.com/", ["file:", "", "", "/example.com/", "", "", ""], ["ftps:/example.com/", ["ftps:", "", "", "/example.com/", "", "", ""], ["gopher:/example.com/", ["gopher:", "example.com", "", "/", "", "", ""], ["ws:/example.com/", ["ws:", "example.com", "", "/", "", "", ""], ["wss:/example.com/", ["wss:", "example.com", "", "/", "", "", ""], ["data:/example.com/", ["data:", "", "", "/example.com/", "", "", ""], ["javascript:/example.com/", ["javascript:", "", "", "/example.com/", "", "", ""], ["mailto:/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]ack, [q]uit, next [<Enter>]==: ]
```

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

- 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 como ejemplo

- Puedes encontrar más en:
<https://github.com/techgaun/github-dorks>



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	- https://github.com/dxa4481/truffleHog
Github-Dorks	- https://github.com/techgaun/github-dorks
GitGot	- https://github.com/BishopFox/GitGot
GitMonitor	- https://github.com/Talkaboutcybersecurity/GitMonitor
GitRob	- https://github.com/michenriksen/gitrob
GitHound	- https://github.com/tillson/git-hound
GittyLeaks	- https://github.com/kootenpv/gitleaks
GitSecrets	- https://github.com/awslabs/git-secrets
Watchtower	- https://radar.nightfall.ai



LISTA DE LOGROS PARA AUTOEVALUACIÓN: SEMINARIO 1



● Este seminario debería permitirte...

- 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
- Conocer múltiples herramientas OSINT que trabajan con información personal de individuos / empresas
- Conocer herramientas para estudiar el código en repositorios públicos
- Saber cómo estudiar un objetivo con Google Hacking
- Saber cómo estudiar a una persona por RRSS y el problema que hay con las herramientas que hacen este tipo de actividades

SEMINARIO 1



HERRAMIENTAS PARA INVESTIGAR EN INTERNET



Departamento de Informática
Universidad de Oviedo



34
Universidad de Oviedo