SEMINARIO 1
HERRAMIENTAS PARA INVESTIGAR EN INTERNET

Obtener información acerca de máquinas, personas y ¡código fuente!

Fuente: zona-militar.com

PROYECTO "*S-81 ISAAC PERAL*" V3.1

¿LOCALIZASTE ALGUNA ERRATA O PROBLEMA? POR FAVOR, NOTIFÍCALA A JOSÉ MANUEL REDONDO LÓPEZ (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 puedas 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 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 INTelligence)**
  - 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-doxyourself-on-the-internet-d2892b4c5954?gi=57af4dc583d

ÍNDICE

< Ir al Índice

Fuente: zona-militar.com

OSINT CONTRA MÁQUINAS

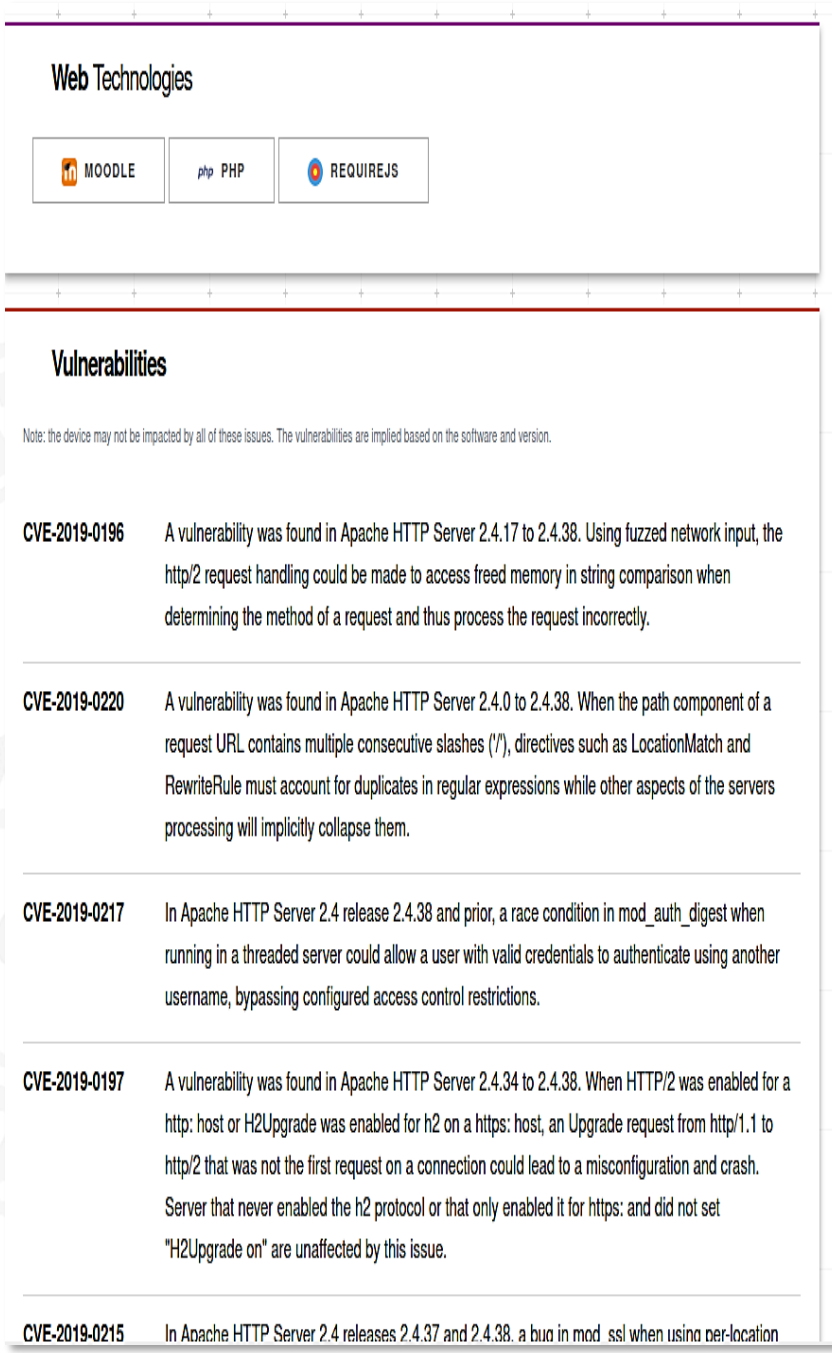
Investigando máquinas usando solo información pública

SHODAN

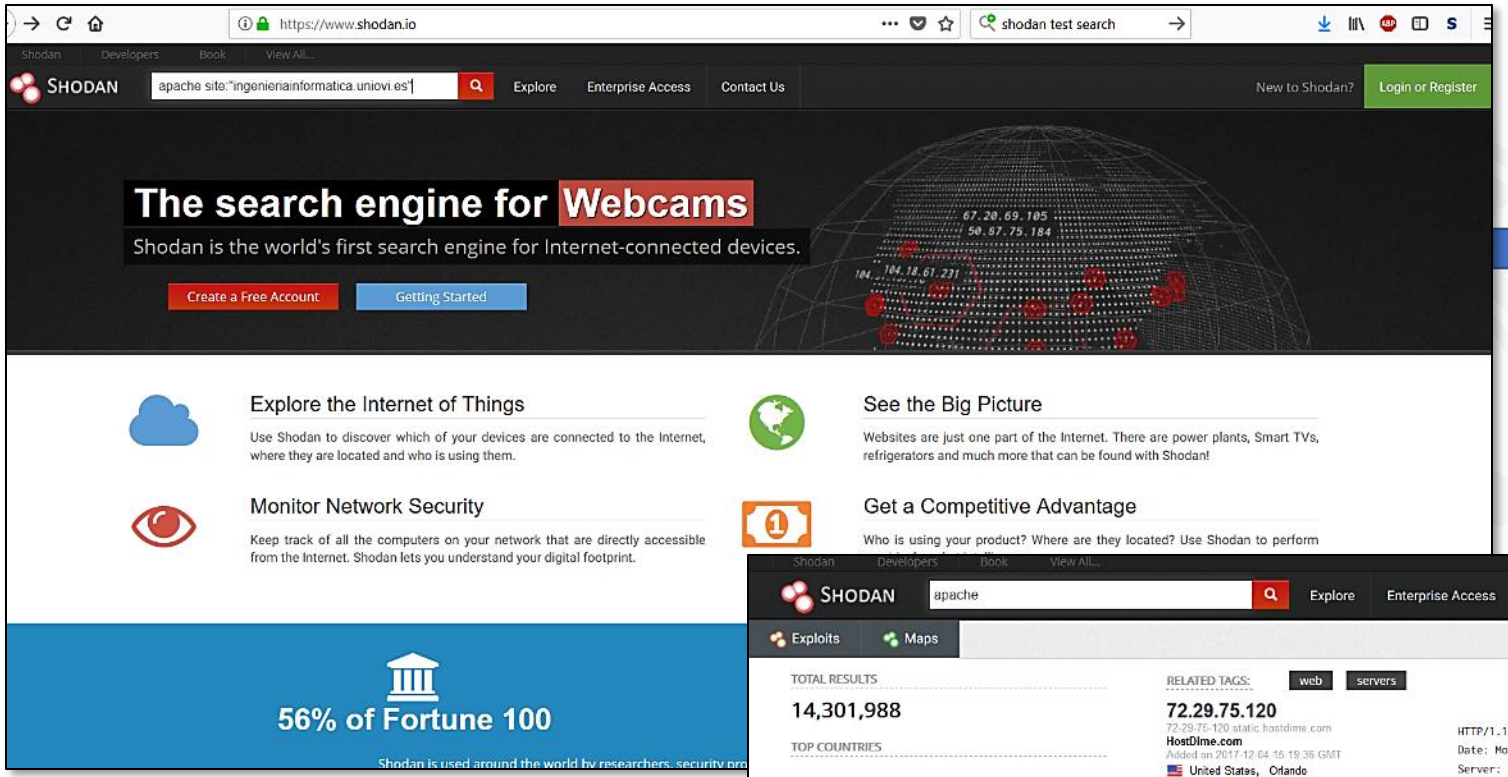
http://www.shodanhq.com/

Seguridad de Sistemas Informáticos

- **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/

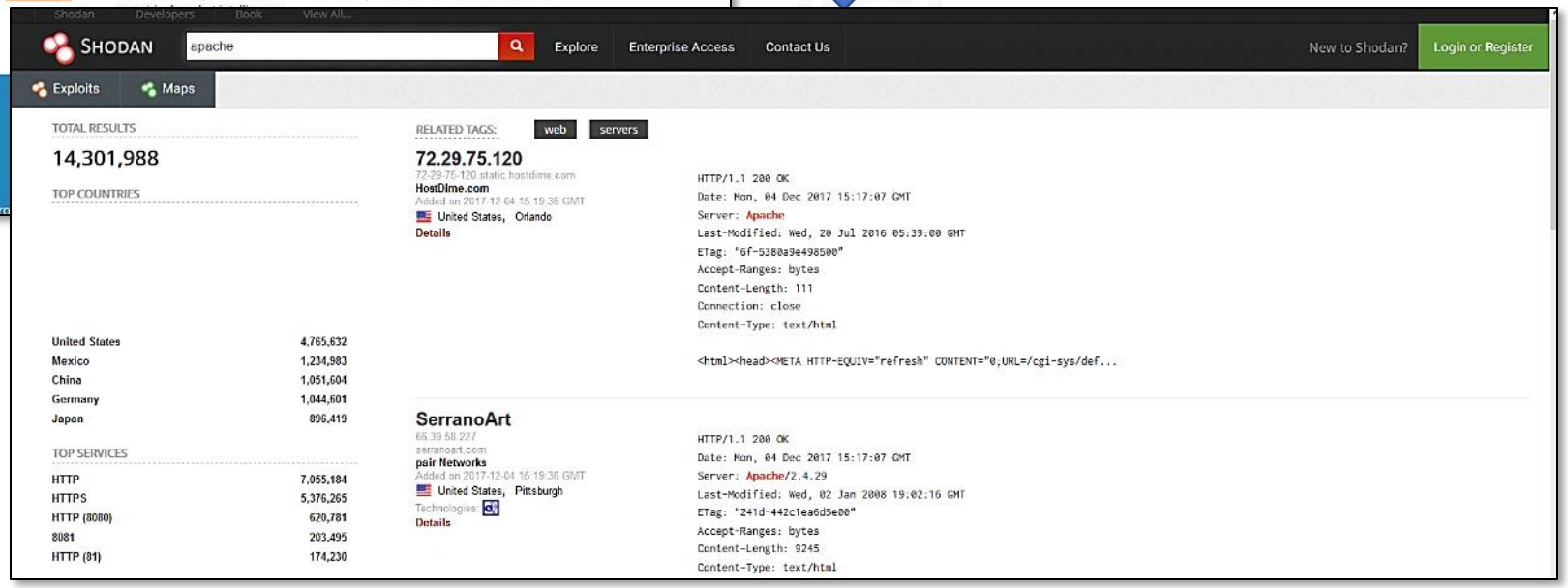


SHODAN



Busca los banners de estos servicios

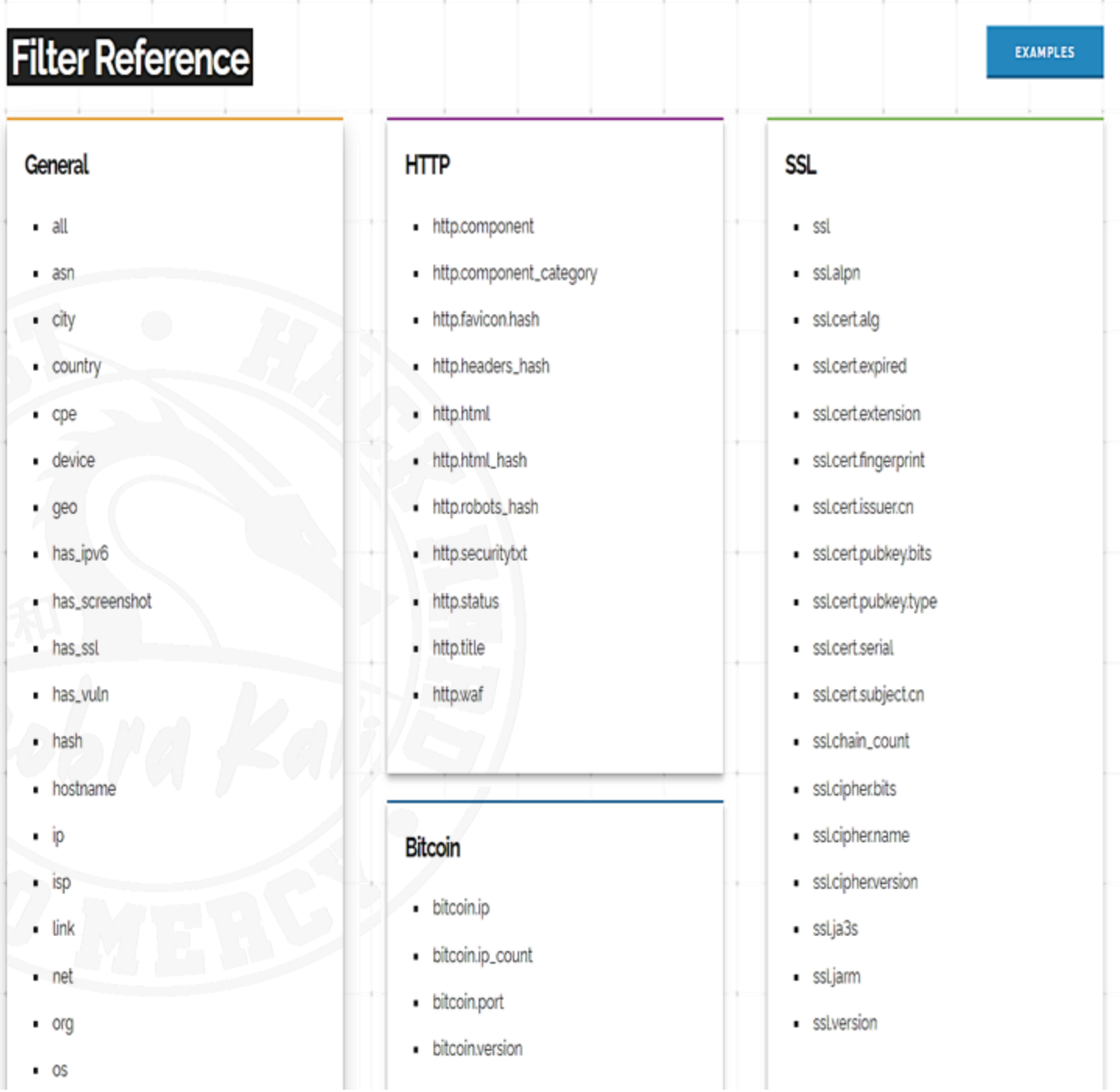
- HTTP/HTTPS
- FTP
- SSH
- Telnet
- SNMP
- SIP (telefonía IP)
- RTSP (streaming de video y webcams)
- …



SHODAN

Seguridad de Sistemas Informáticos

- **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

EXAMPLES

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
- http.waf

Bitcoin

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

SSL

- ssl
- ssl.alpn
- ssl.cert.alg
- ssl.cert.expired
- ssl.cert.extension
- ssl.cert.fingerprint
- ssl.cert.issuer.cn
- ssl.cert.pubkey.bits
- ssl.cert.pubkey.type
- ssl.cert.serial
- ssl.cert.subject.cn
- ssl.chain_count
- ssl.cipher.bits
- ssl.cipher.name
- ssl.cipherversion
- ssl.ja3s
- ssl.jarm
- ssl.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

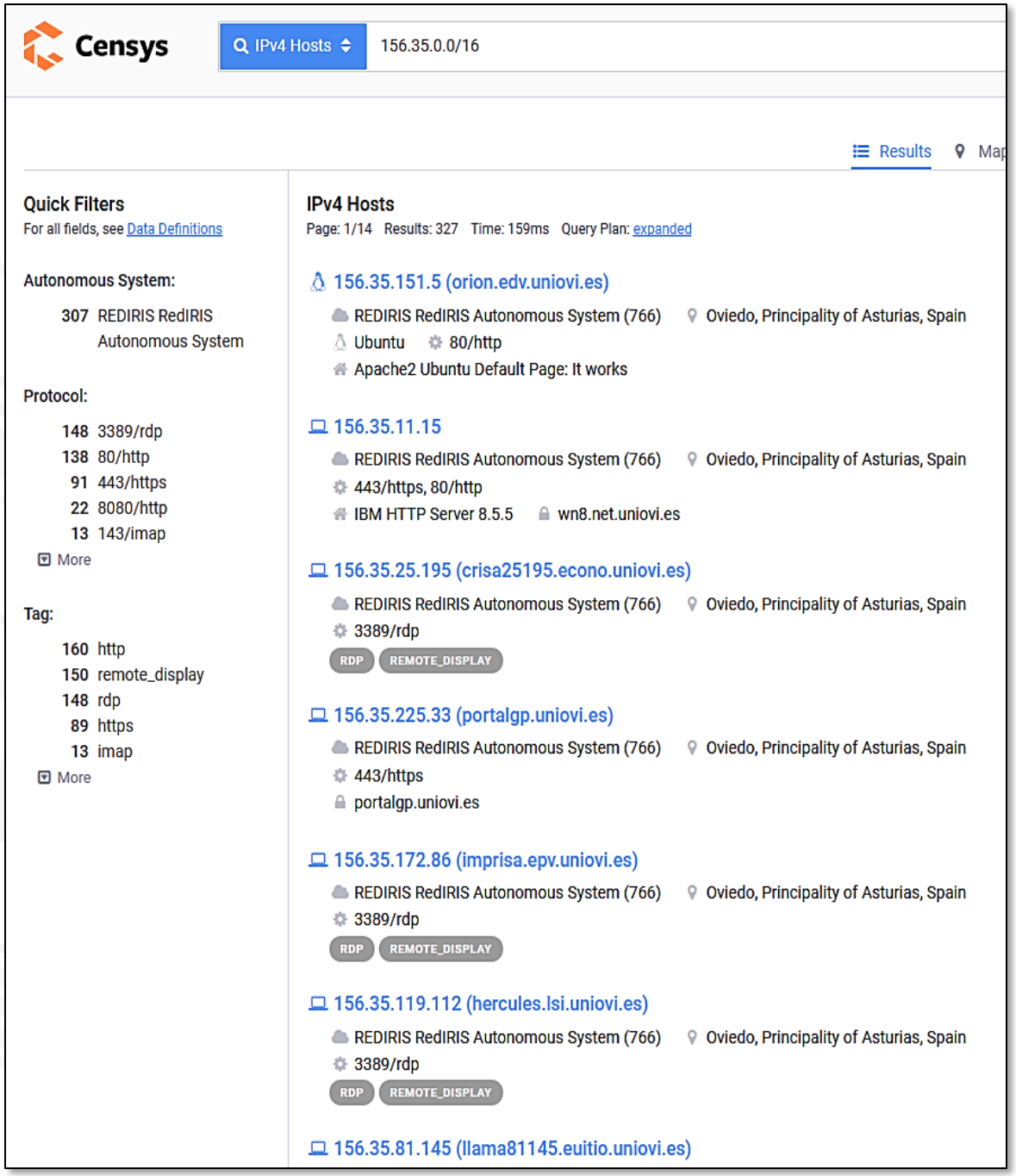
```
81.171.175.68   80      Star Technology Services Limited
178.73.238.43   80      Portlane Networks AB
113.245.76.199  5900    China Telecom HUNAN
149.210.160.163 80      Transip B.V.    nowarkrengelink.com
23.92.216.117   80      Res.pl Isp S.c. mailingrolout.com
202.69.233.212  443     Verio Web 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-ll-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/

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 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-onyphe-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

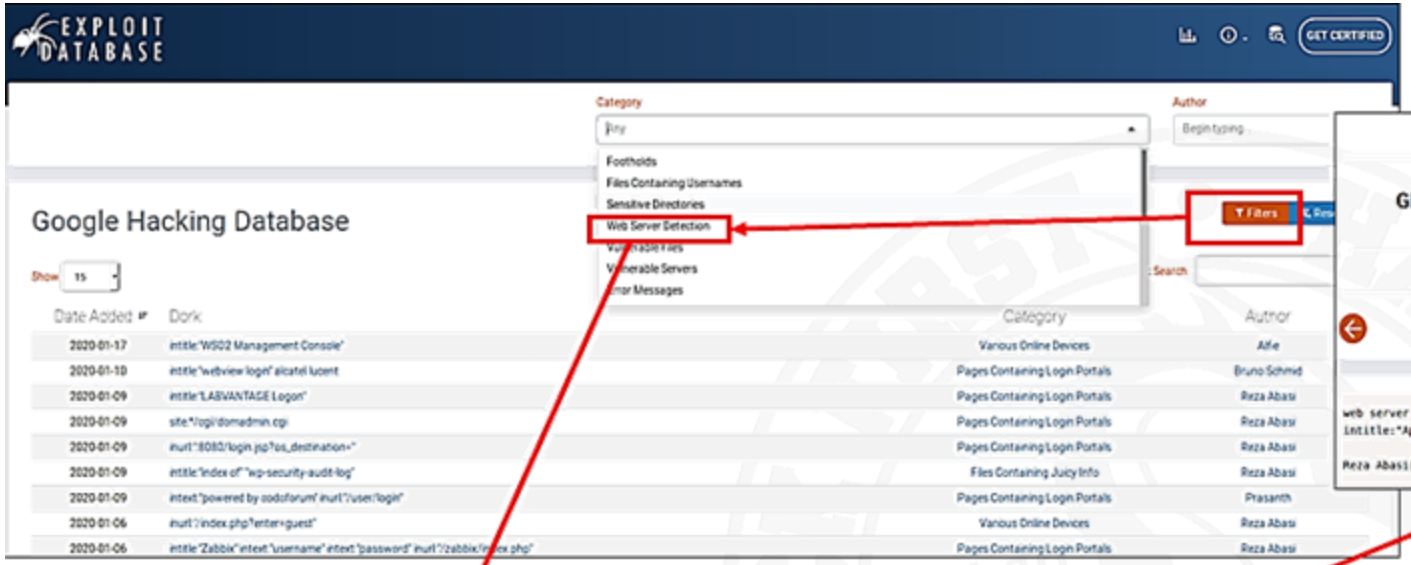


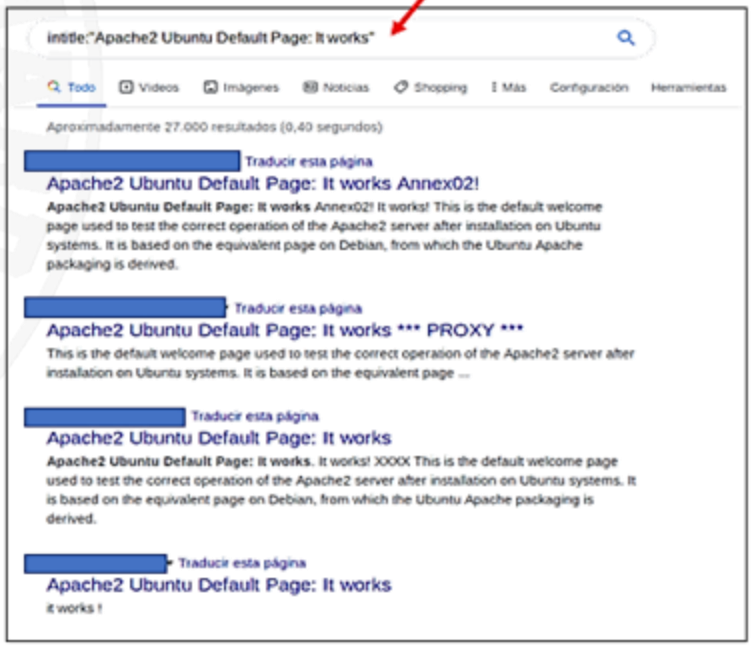
(1) Usar Shodan para encontrar recursos pertenecientes a Uniovi

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

GOOGLE HACKING: PROCESO





Final Recon

https://github.com/thewhiteh4t/FinalRecon

- **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

Seguridad de Sistemas Informáticos

- **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/

```
      _____           _
     |  __ \         | |
_   _| |  | | ___  _ __| | __
| | | | |  | |/ _ \| '__| |/ /
| |_| | |__| | (_) | |  |   <
 \__,_|_____/ \___/|_|  |_|\_\ v.2.0
       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 >

Fuente: zona-militar.com

OSINT CONTRA PERSONAS

Investigando gente usando solo información pública

Redes sociales

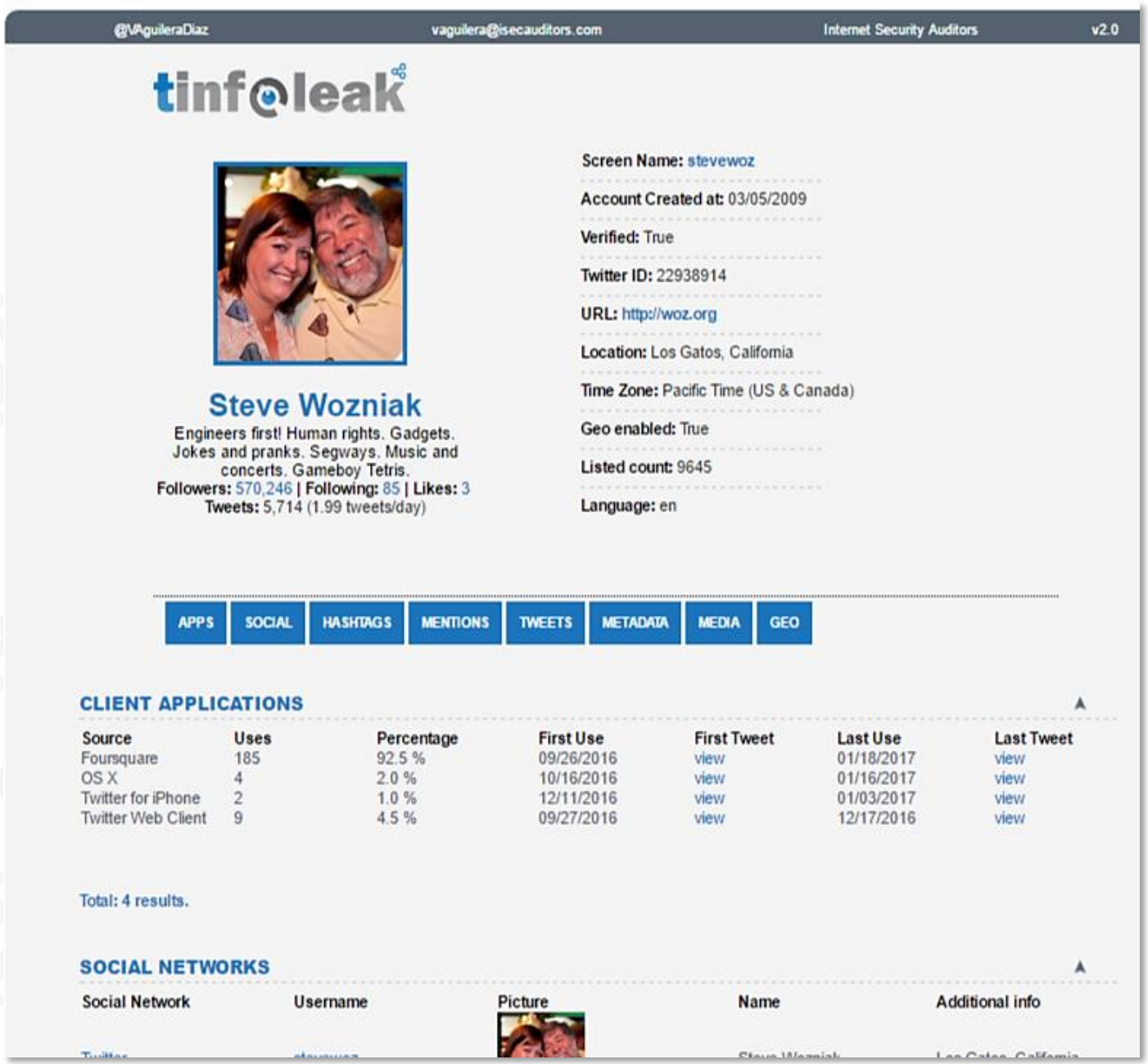
Saber lo que la gente hace...y escribe ☺

TINFOLEAK

https://github.com/vaguileradiaz/tinfoleak

Seguridad de Sistemas Informáticos

- **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…



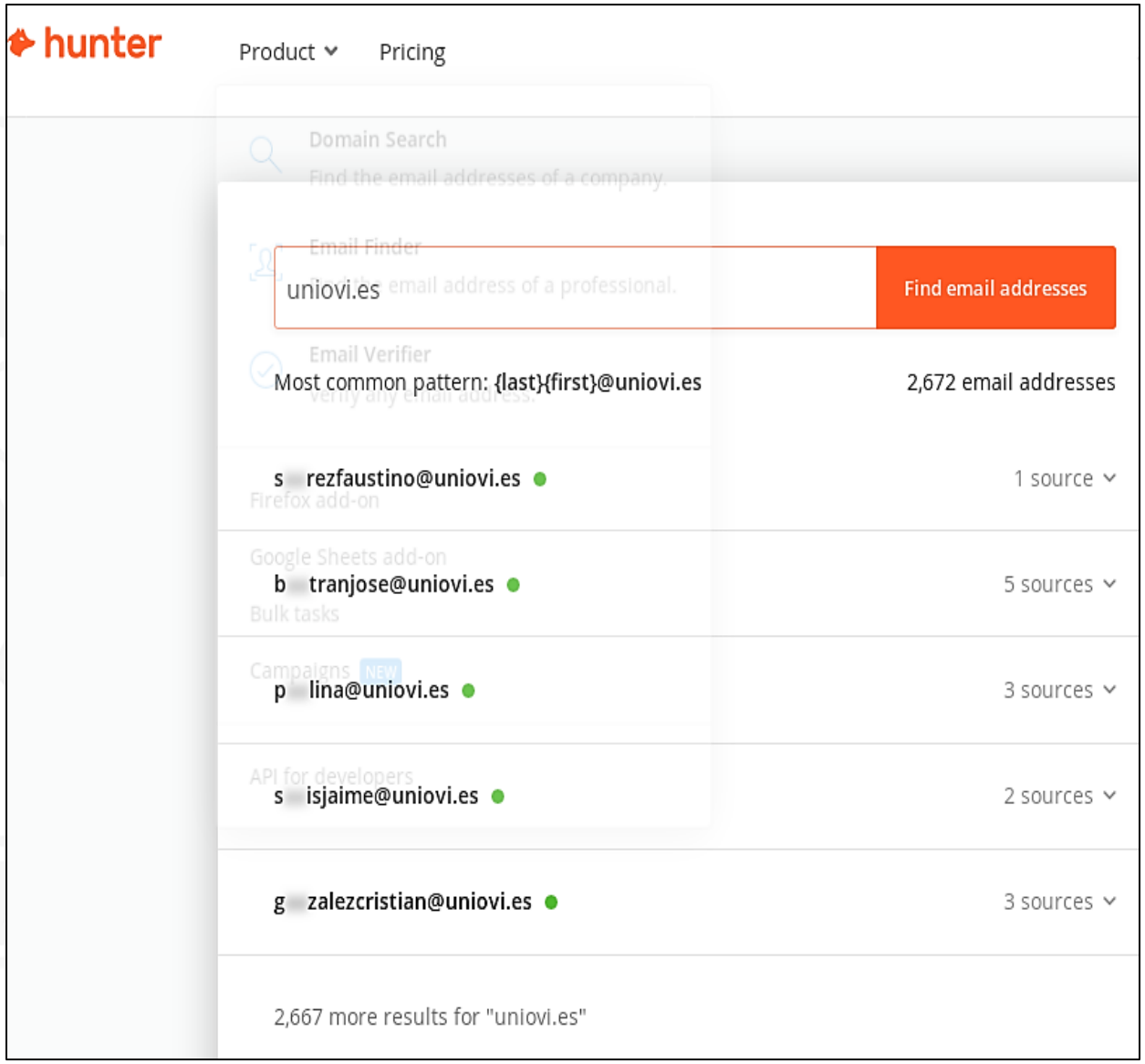
Fuente: https://www.redeszone.net/2017/10/08/tinfoleak-recopilar-informacion-usuarios-twitter/

HUNTER.IO

https://hunter.io/

Seguridad de Sistemas Informáticos

- **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



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=Ib
aiLlanos
[+] 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

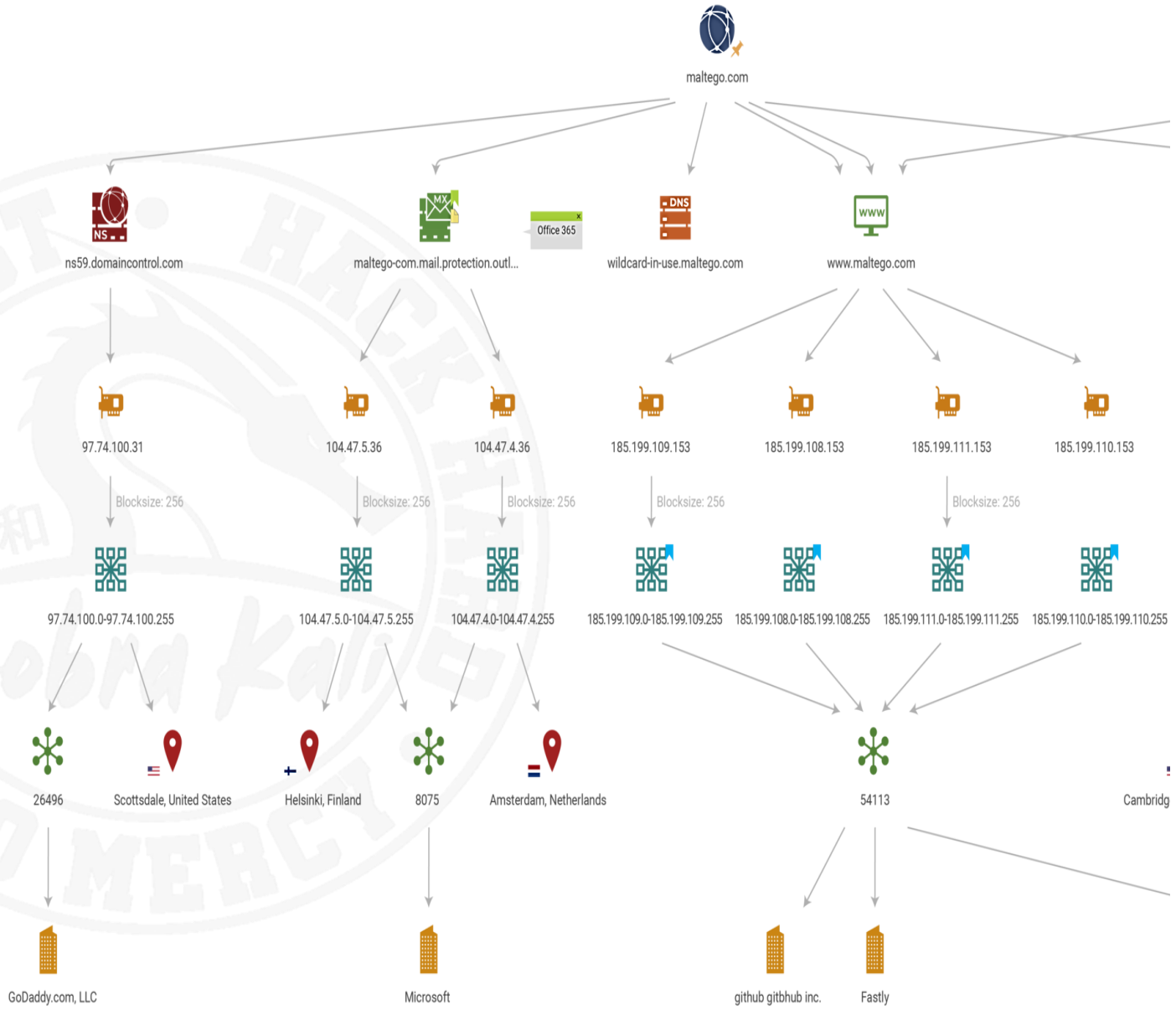
MALTEGO

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

Seguridad de Sistemas Informáticos

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

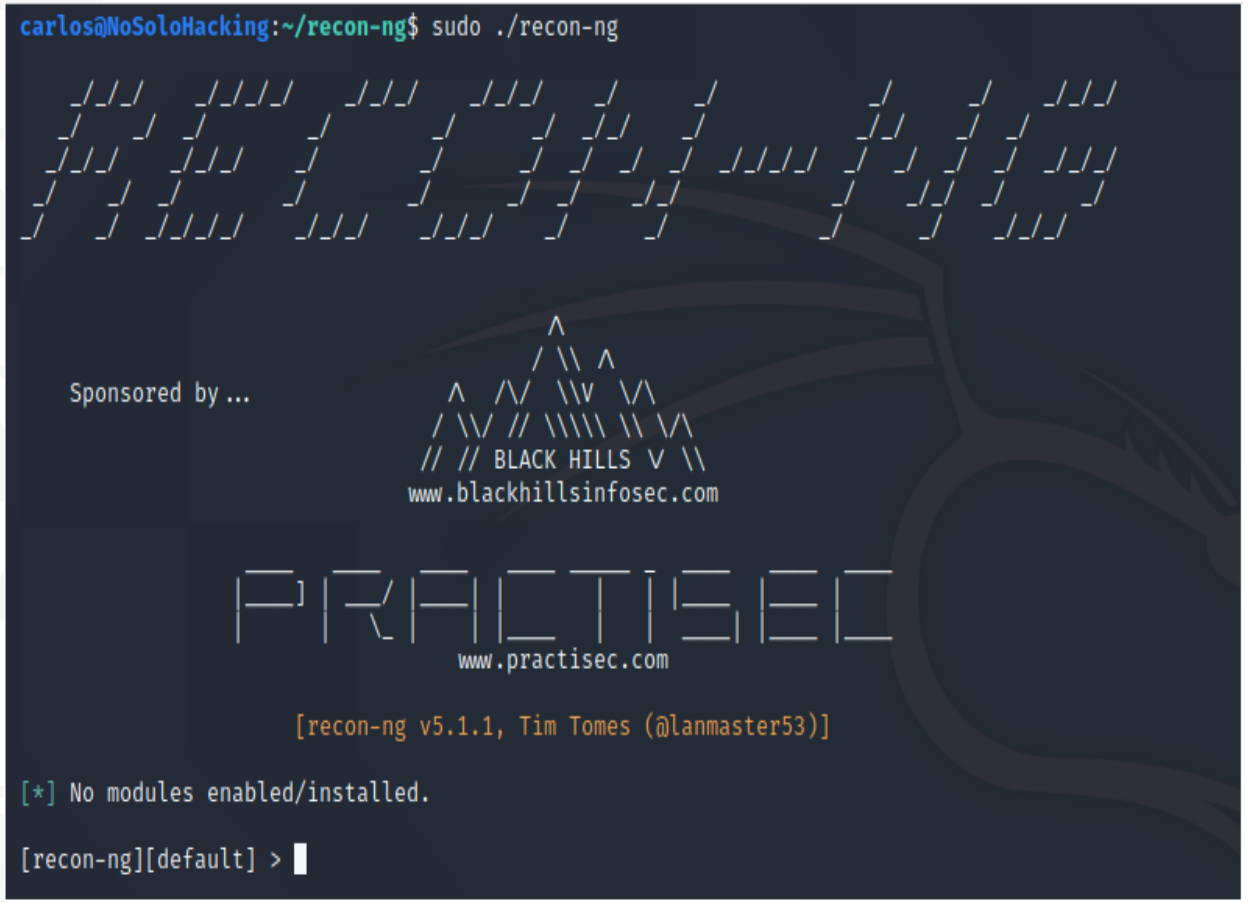
- **Recopila información de entidades de internet**
  - Crea entidades personalizadas que representan cualquier tipo de información
  - Se especializa en encontrar relaciones entre ellas
    - Redes sociales, redes de ordenadores, dominios...
  - Utiliza como fuentes DNS, registros `whois`, motores de 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



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-recoleccion-de-informacion/



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

ODIN

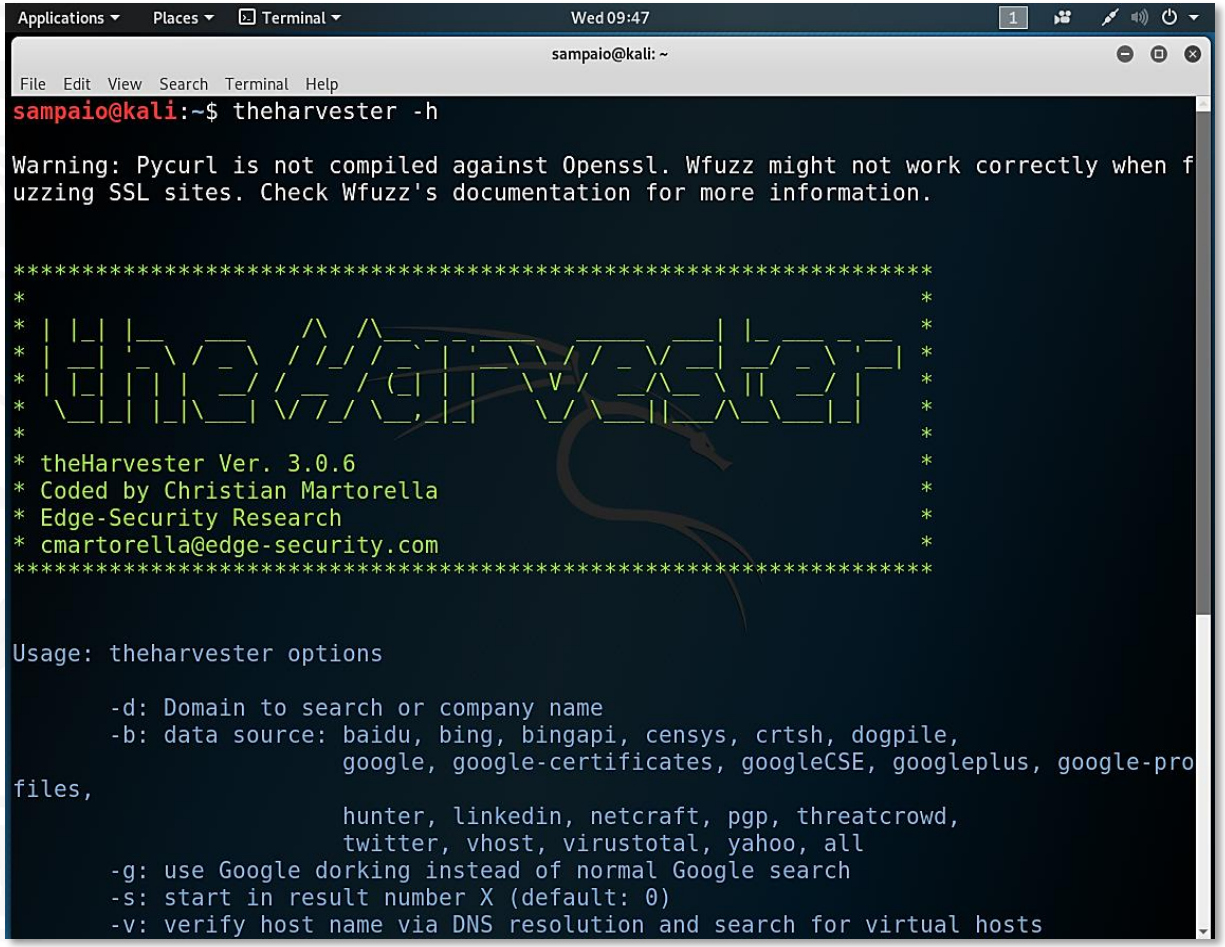
https://github.com/chrismaddalena/ODIN

- **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

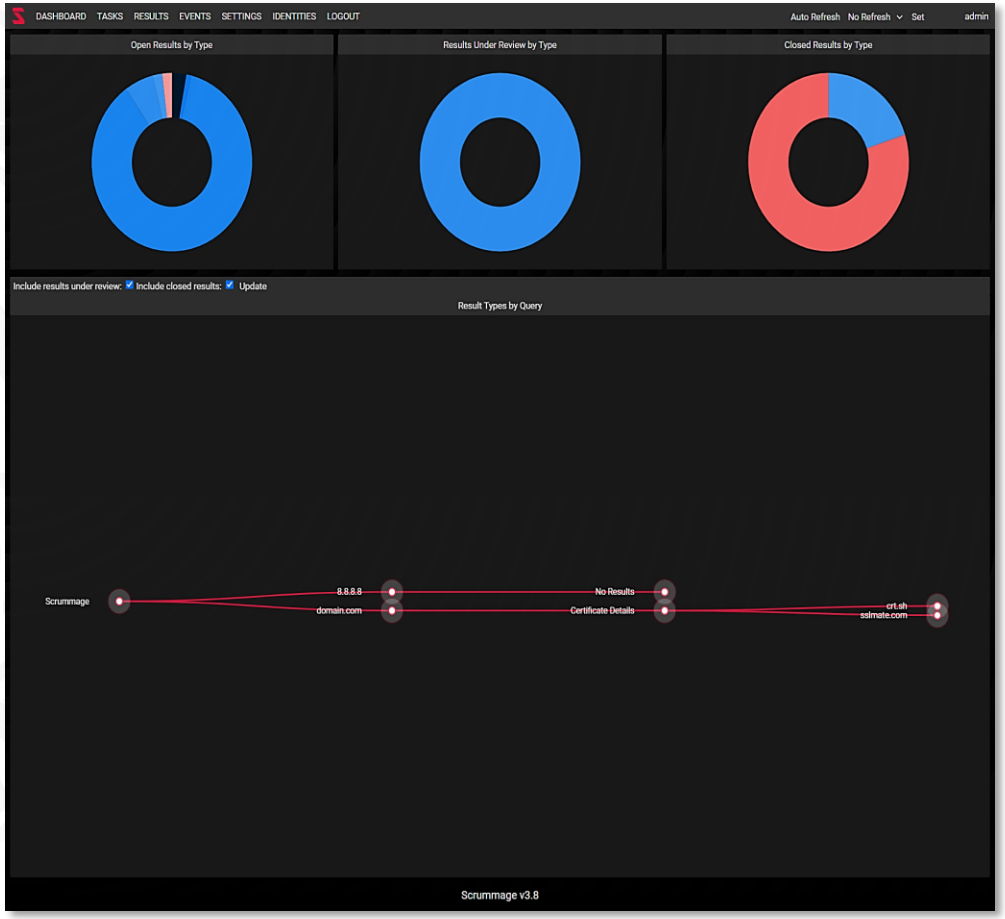
- **Obtiene datos de un objetivo usando muchos sitios diferentes como fuentes**
  - Obtiene mucha información de fuentes de datos públicas: correos electrónicos, nombres, subdominios, IP, URLs...
  - Utiliza motores de búsqueda conocidos para diferentes tipos de información
    - baidu, bing, bingapi, 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-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/)
    - 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

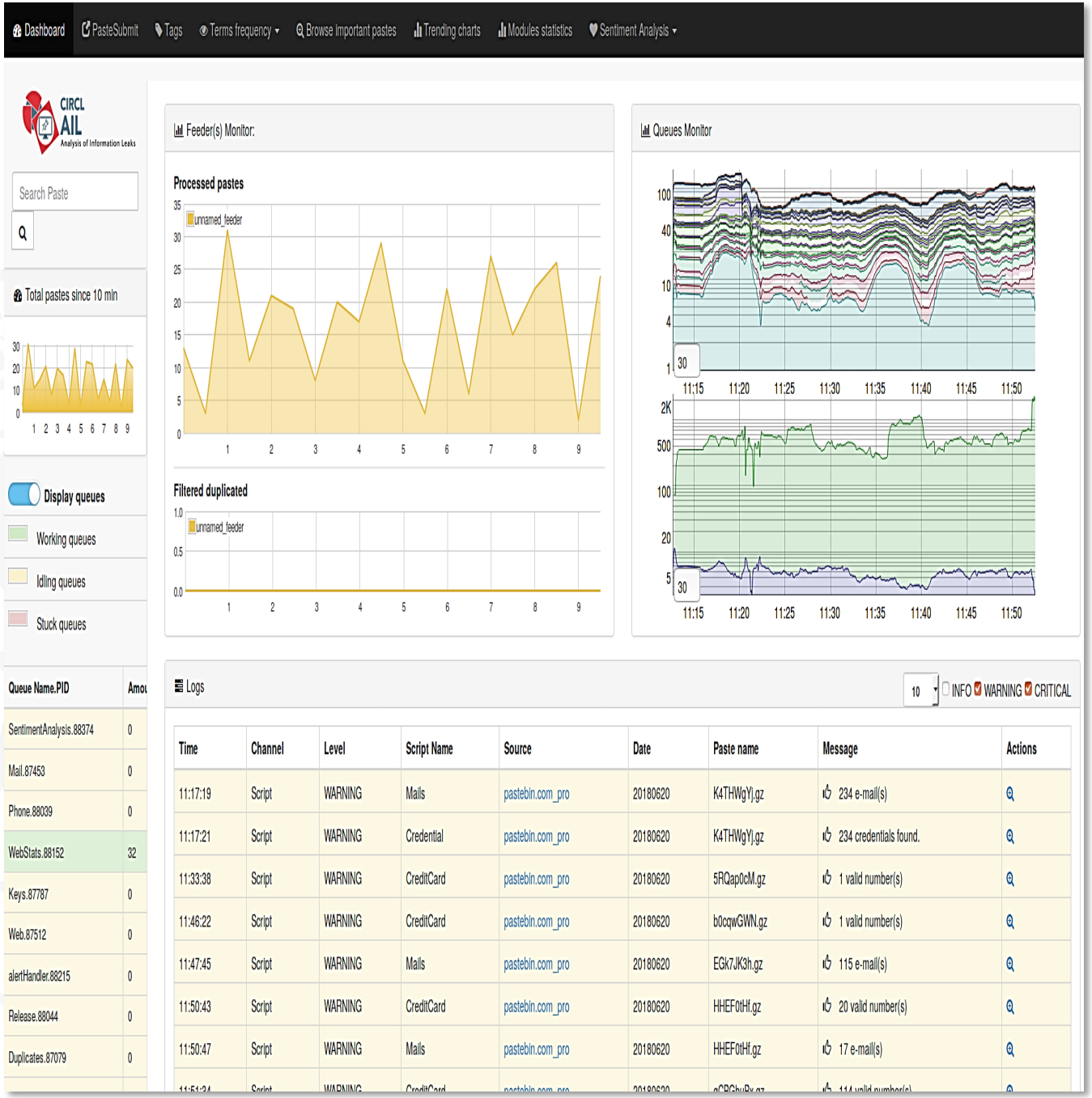


AIL Framework

https://github.com/CIRCL/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-frameworkframework-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!

¿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/

(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

Fuente: zona-militar.com

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

GitRob

https://github.com/michenriksen/gitrob

- **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/

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

¡El propio GitHub!

- **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**

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**
	**Animal Social**: Ser capaz de localizar información de máquinas, usuarios y código fuente en Internet

SEMINARIO 1. HERRAMIENTAS PARA INVESTIGAR EN INTERNET

Fuente: zona-militar.com