SEMINARIO 1
HERRAMIENTAS PARA INVESTIGAR EN INTERNET

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

José Manuel Redondo López Proyecto *"S-81 Isaac Peral"* v4.0

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

Logo: @creative_vanesa (*Instagram*)

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
  - Pero, sobre todo, explotaremos más esta rama en el **Trabajo en Grupo** de la asignatura
- **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

OSINT CONTRA MÁQUINAS

Investigando máquinas usando solo información pública

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

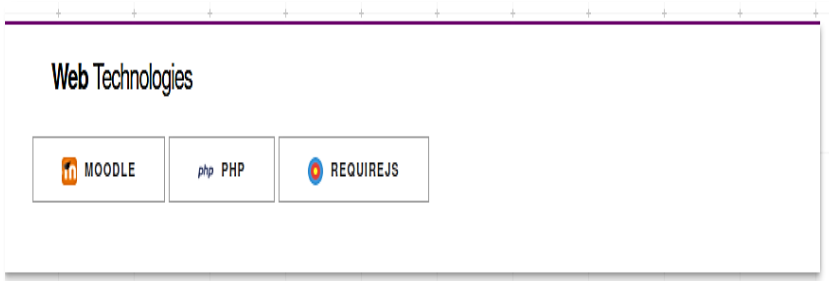
Universidad de Oviedo

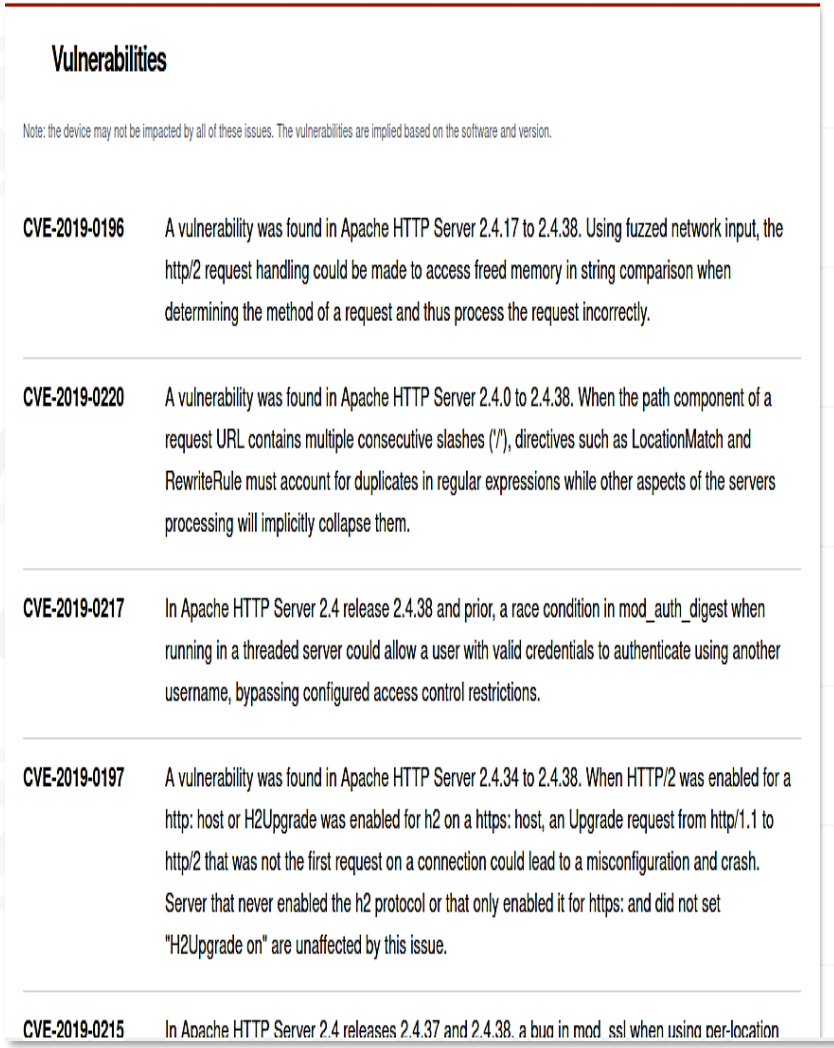
SHODAN

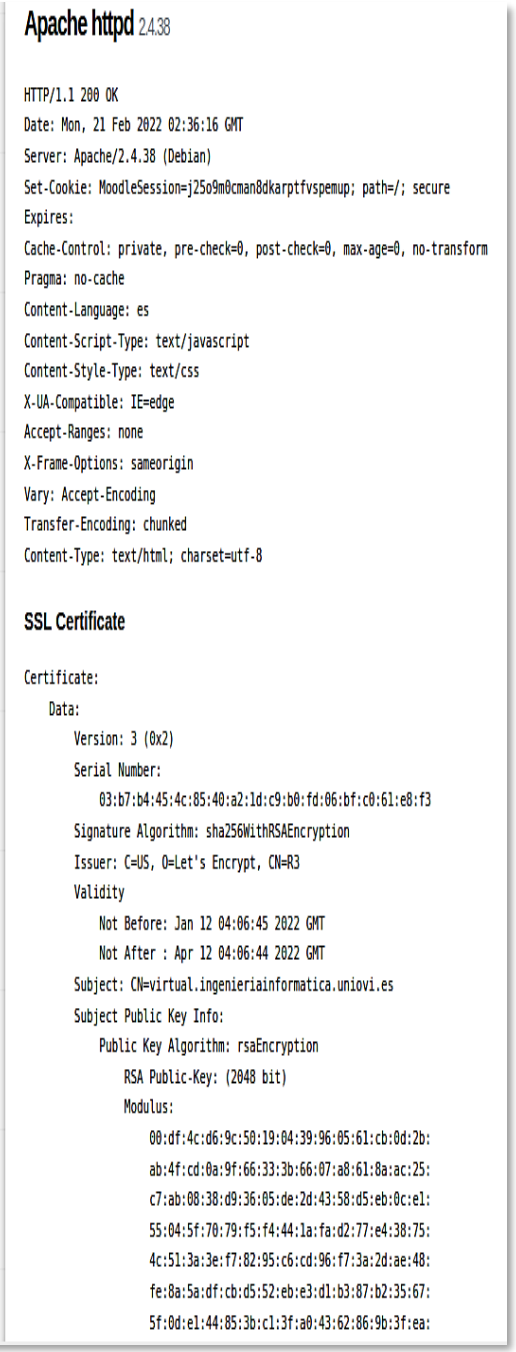
http://www.shodanhq.com/

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/



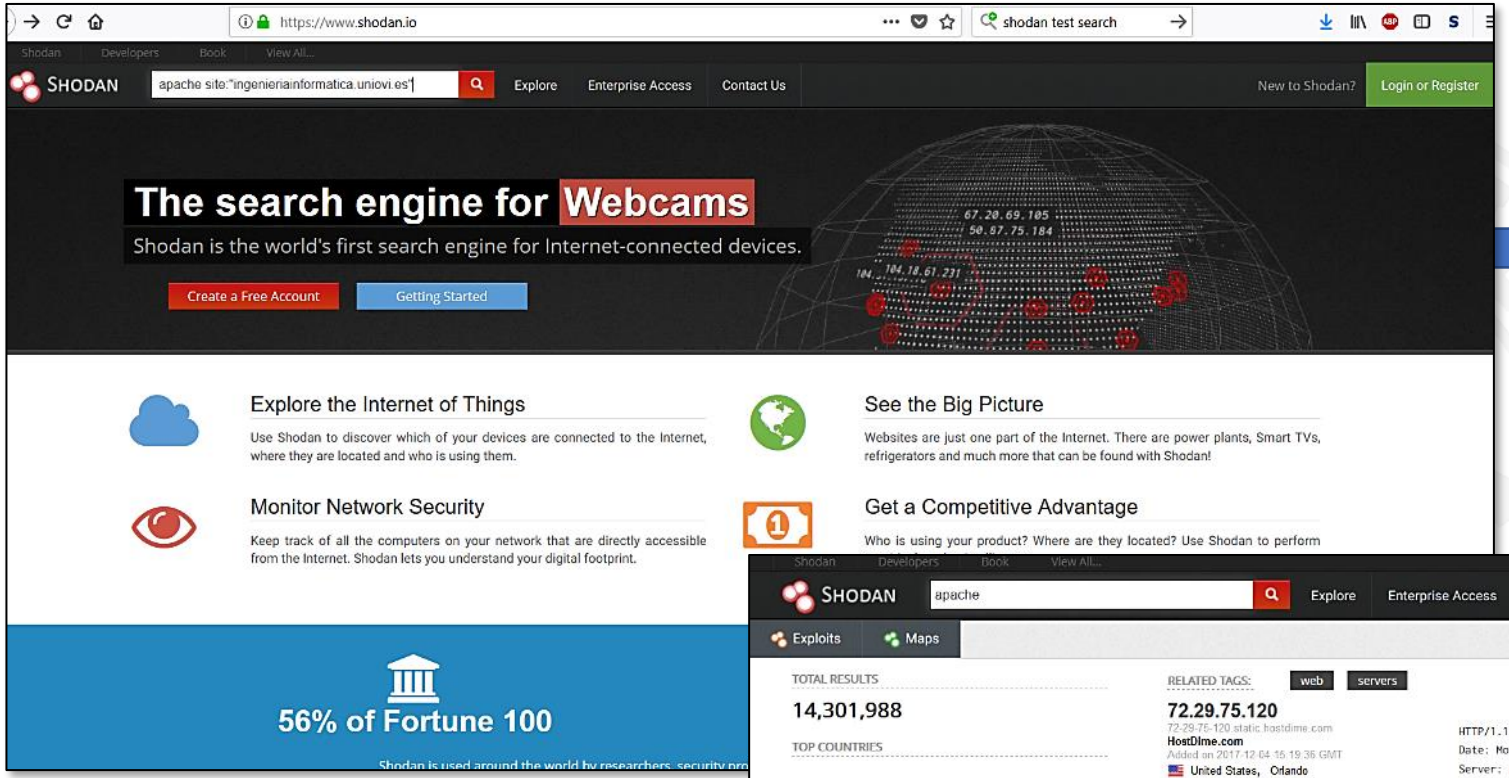


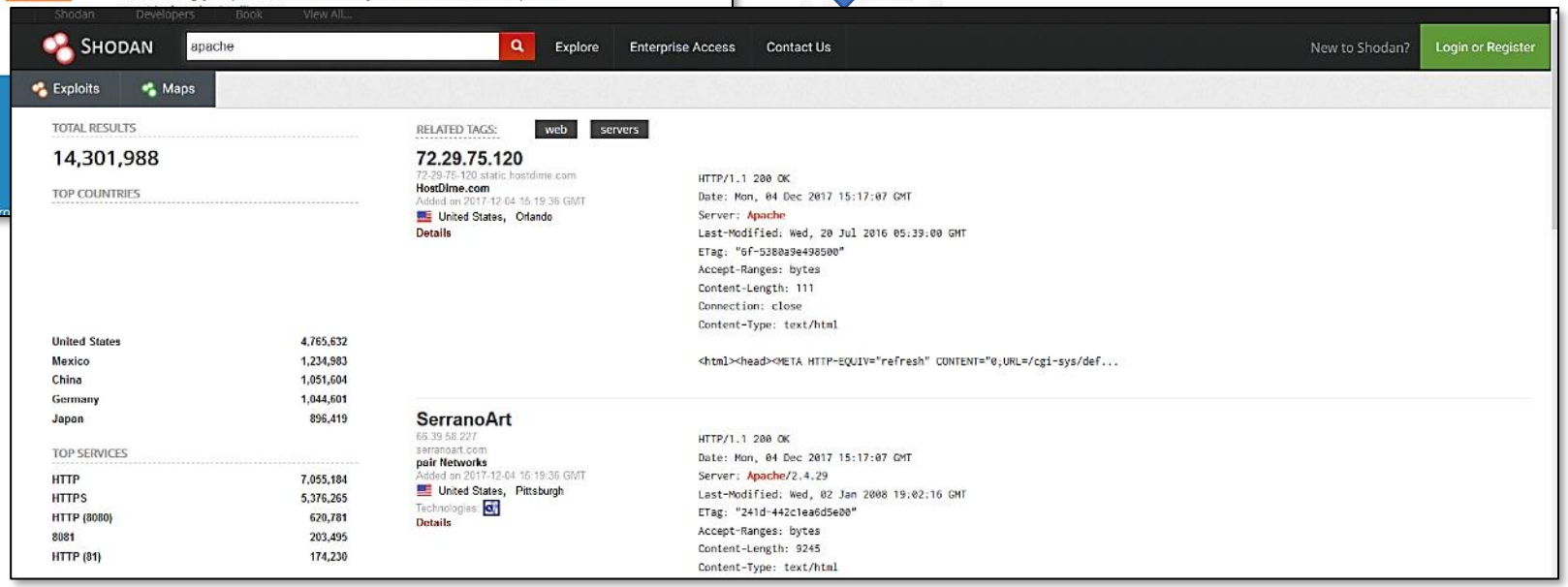


SHODAN

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.cipher.version
- ssl.ja3s
- ssl.jarm
- ssl.version

SHODAN CLI

https://cli.shodan.io/

Seguridad de Sistemas Informáticos

- **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

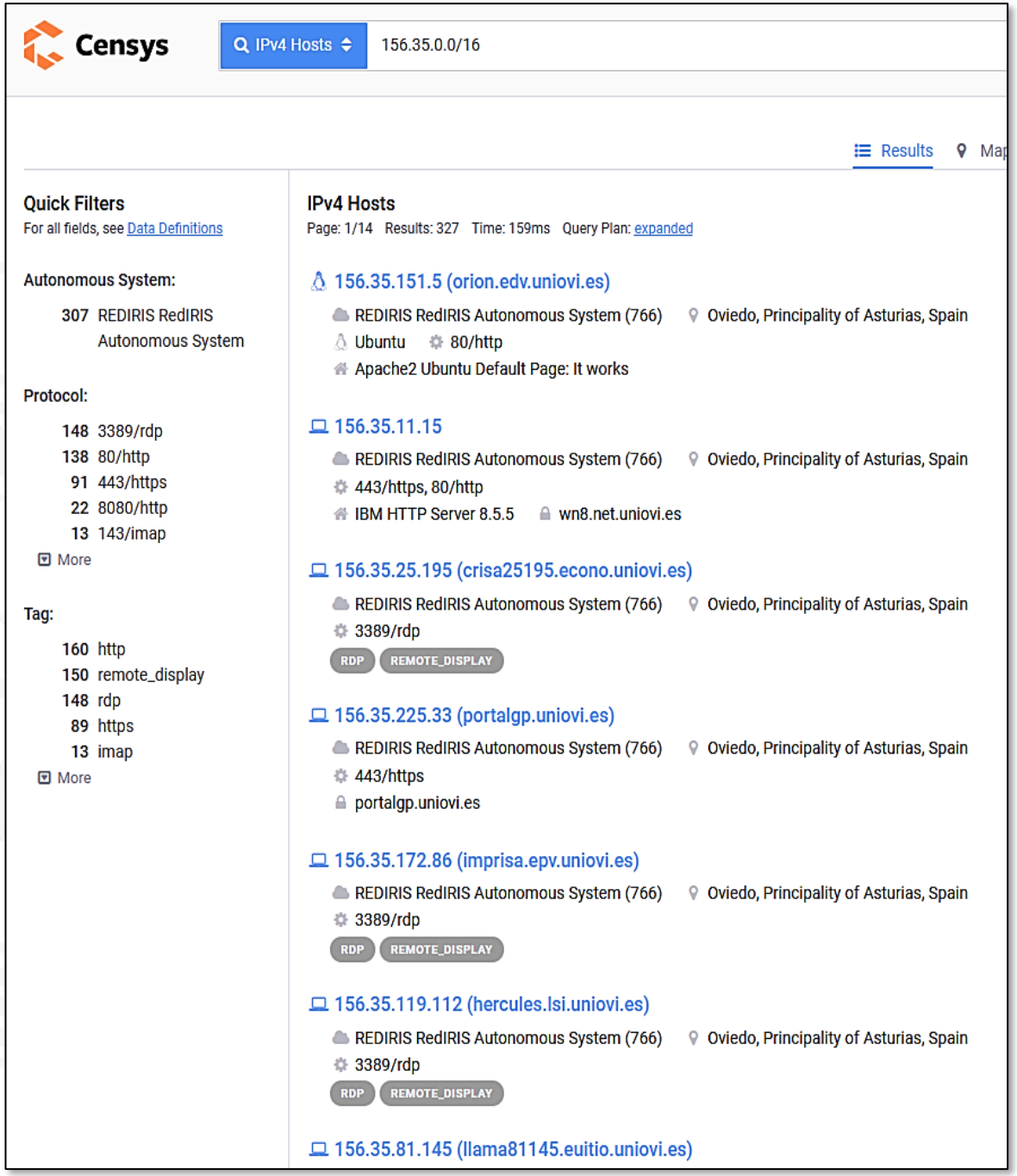
```
81.171.175.68   80    Star Technology Services Limited
178.73.238.43   80    Portlane Networks AB
113.245.76.199  5900  China Telecom HUNAN
149.210.160.163 80    Transip B.V.    nowarkrengelink.com
23.92.216.117   80    Res.pl Isp S.c. mailingrolout.com
202.69.233.212  443   Verio Web Hosting   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

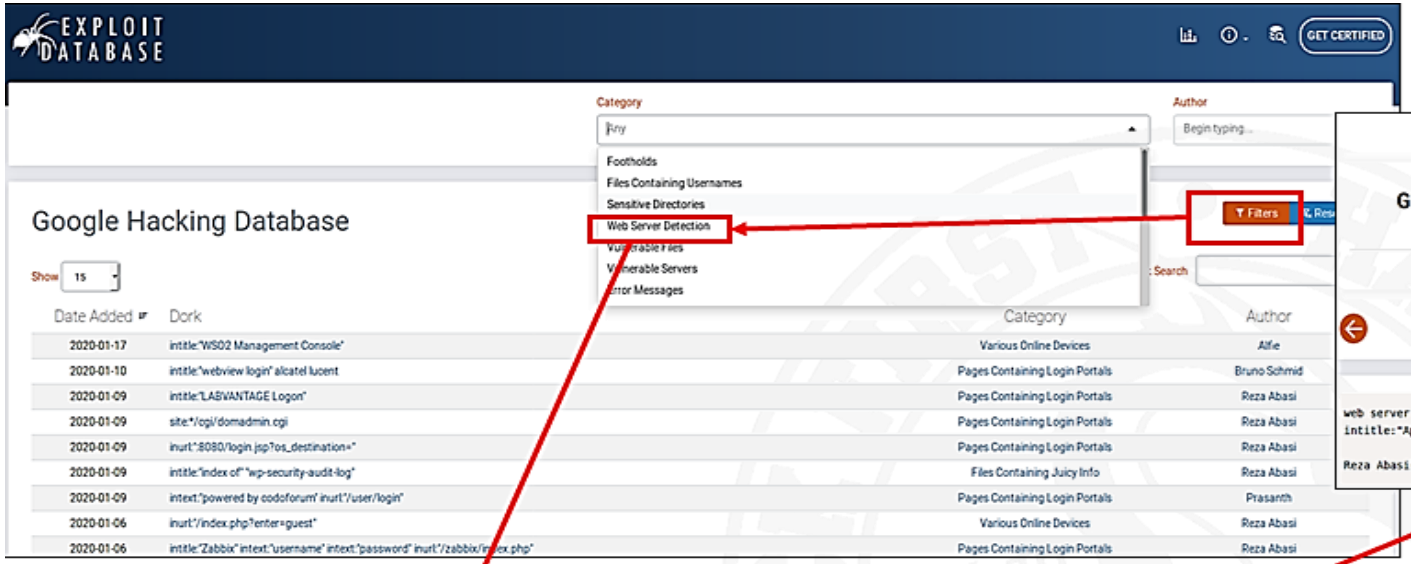


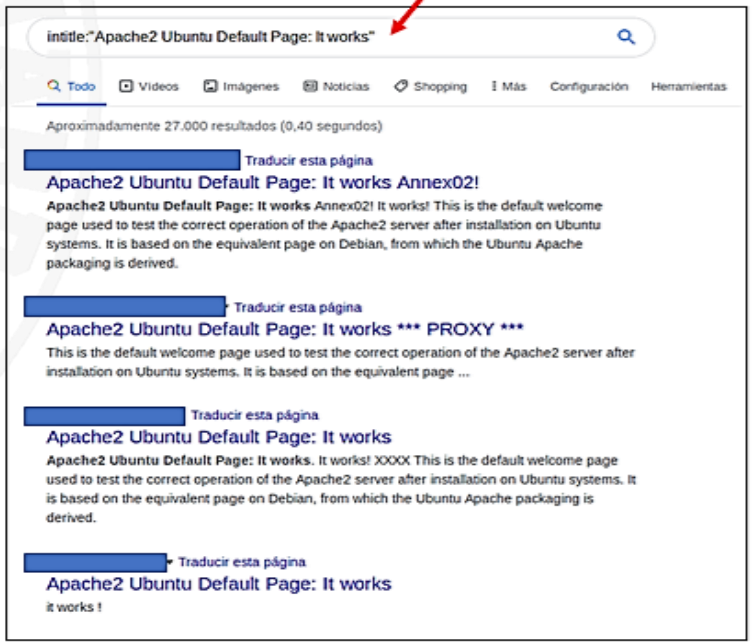
Usar Shodan para encontrar información

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 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

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/2014JO25/2014JO25_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://umbra.nascom.nasa.gov/sobo/bga_history.html.old
```

< Ir al Índice

Redes sociales >

Integración de datos >

Fuente: Bing Chat AI

OSINT CONTRA PERSONAS

Investigando gente usando solo información pública

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

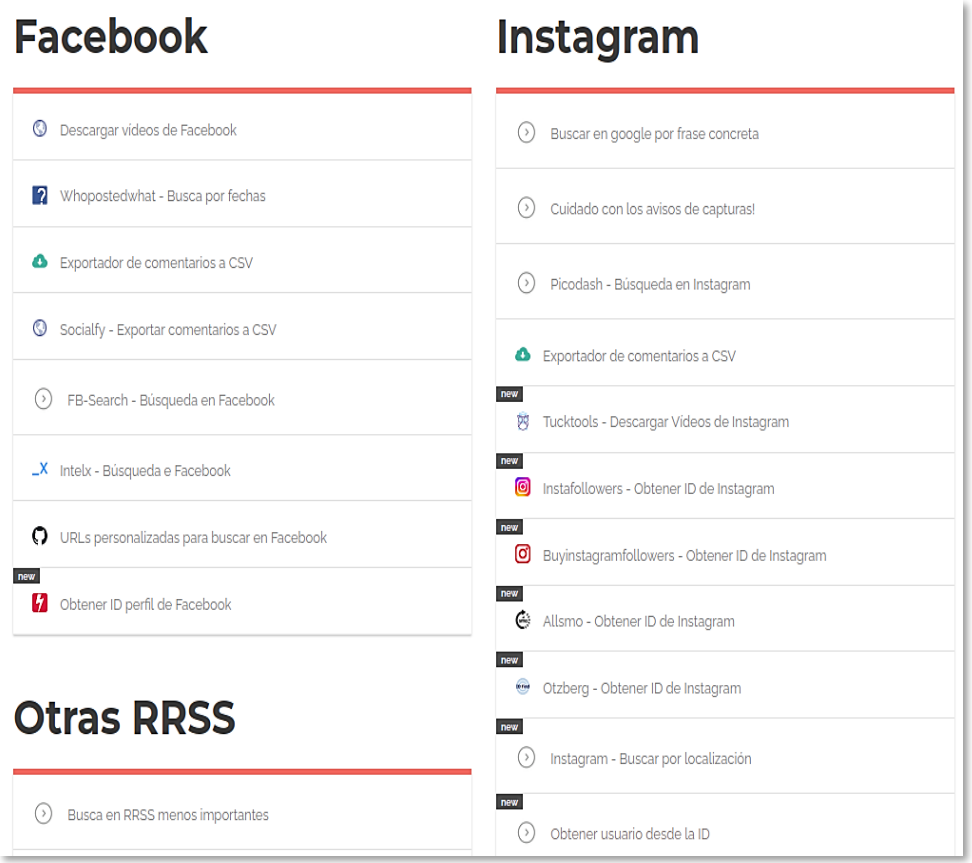
Redes sociales

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**
- **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 dejo 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/

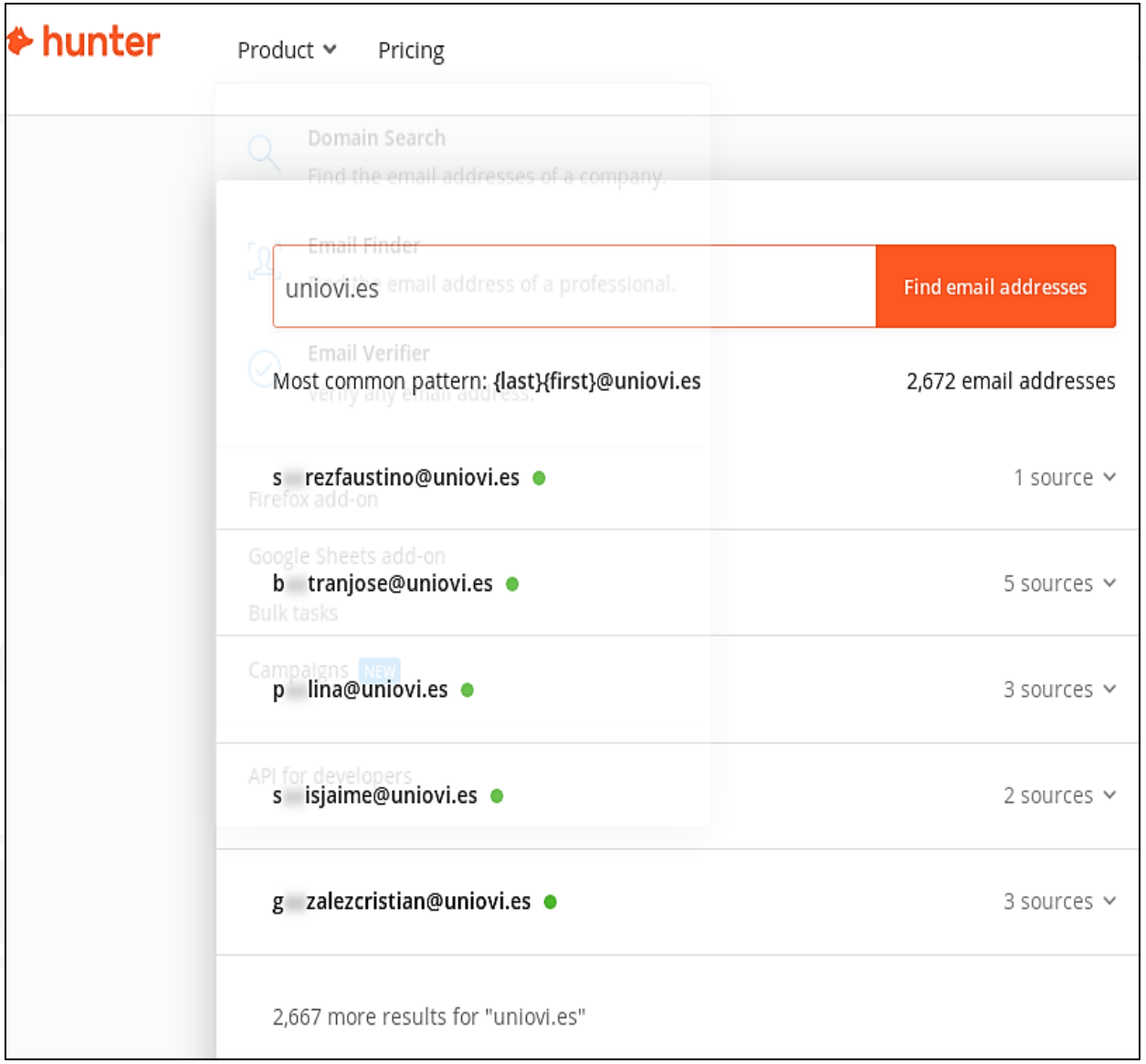


HUNTER.IO

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



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!
- **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

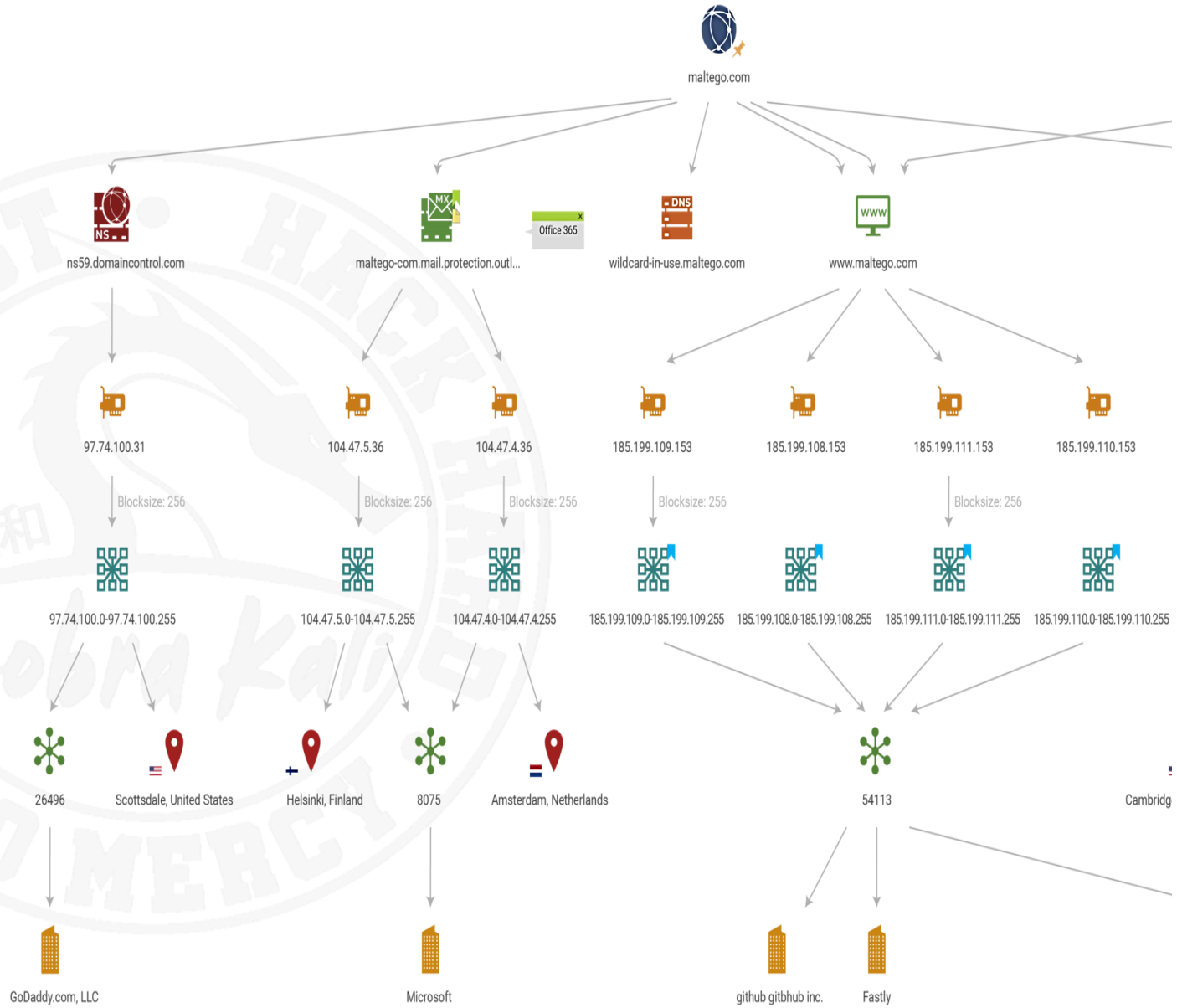
https://www.paterva.com/buy/maltego-clients/maltego-ce.php

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...



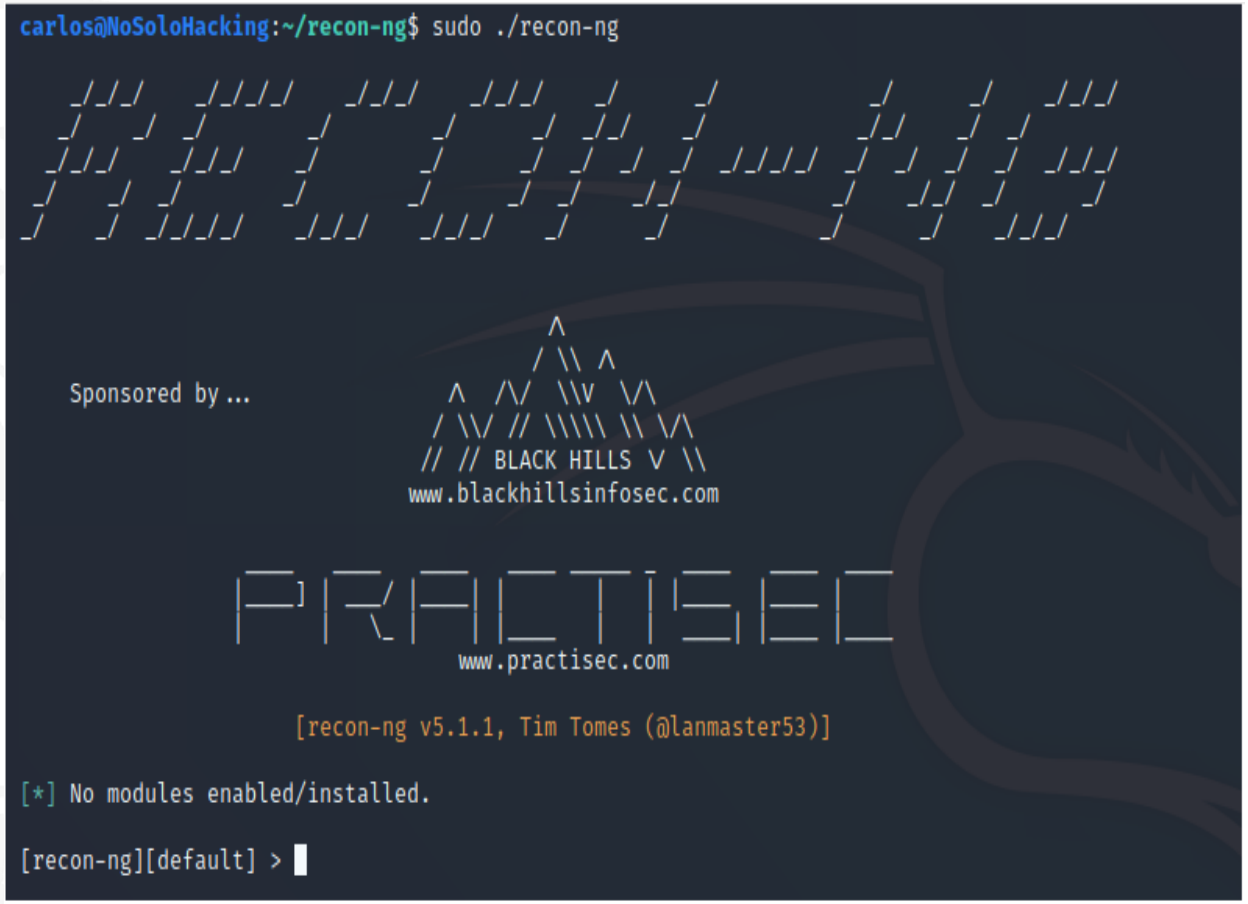
Tutoriales

- 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
- Veremos más sobre ella en los **Trabajos en Grupo**

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** 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/

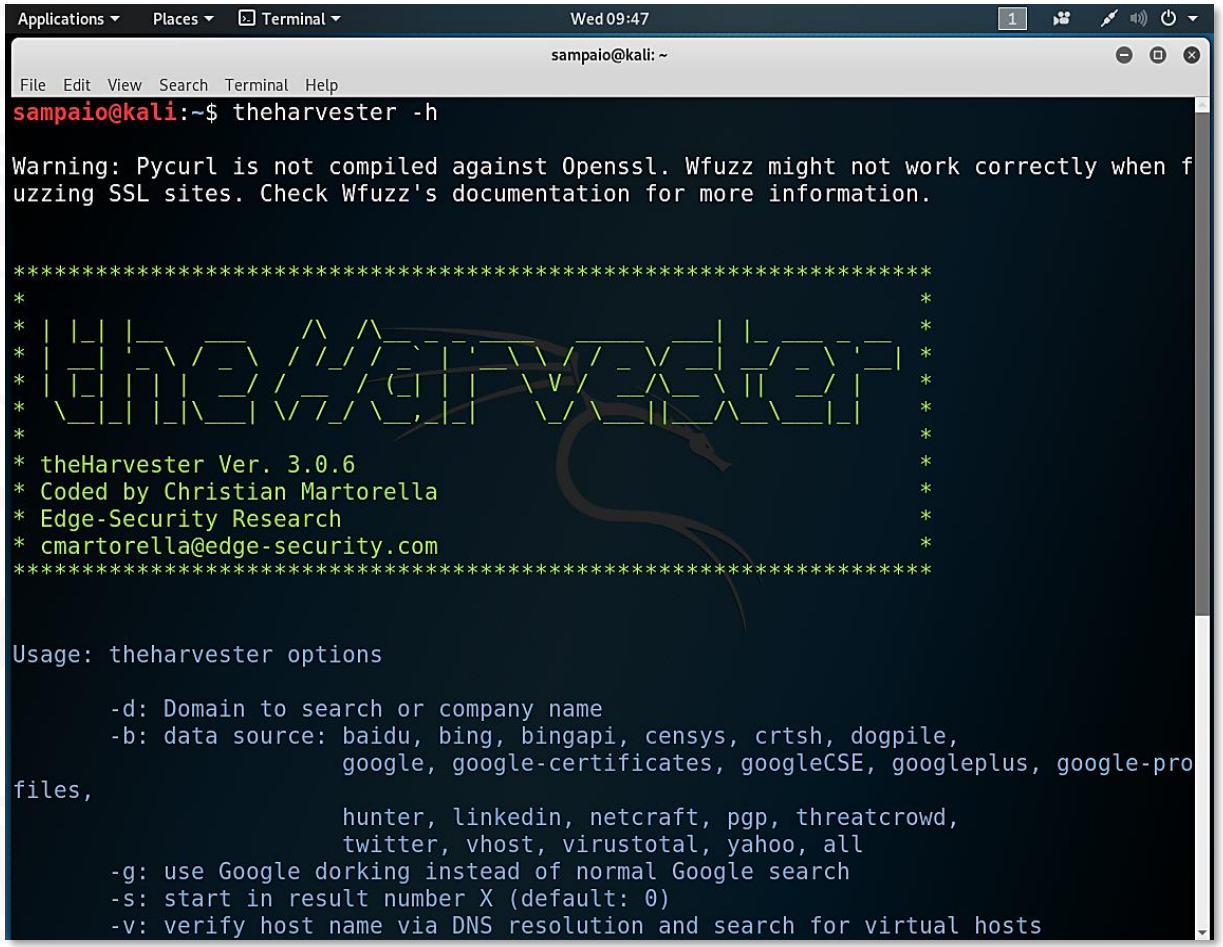


Fuente: https://www.nosolohacking.info/recon-ng-instalacion/

The Harvester

https://github.com/laramies/theHarvester

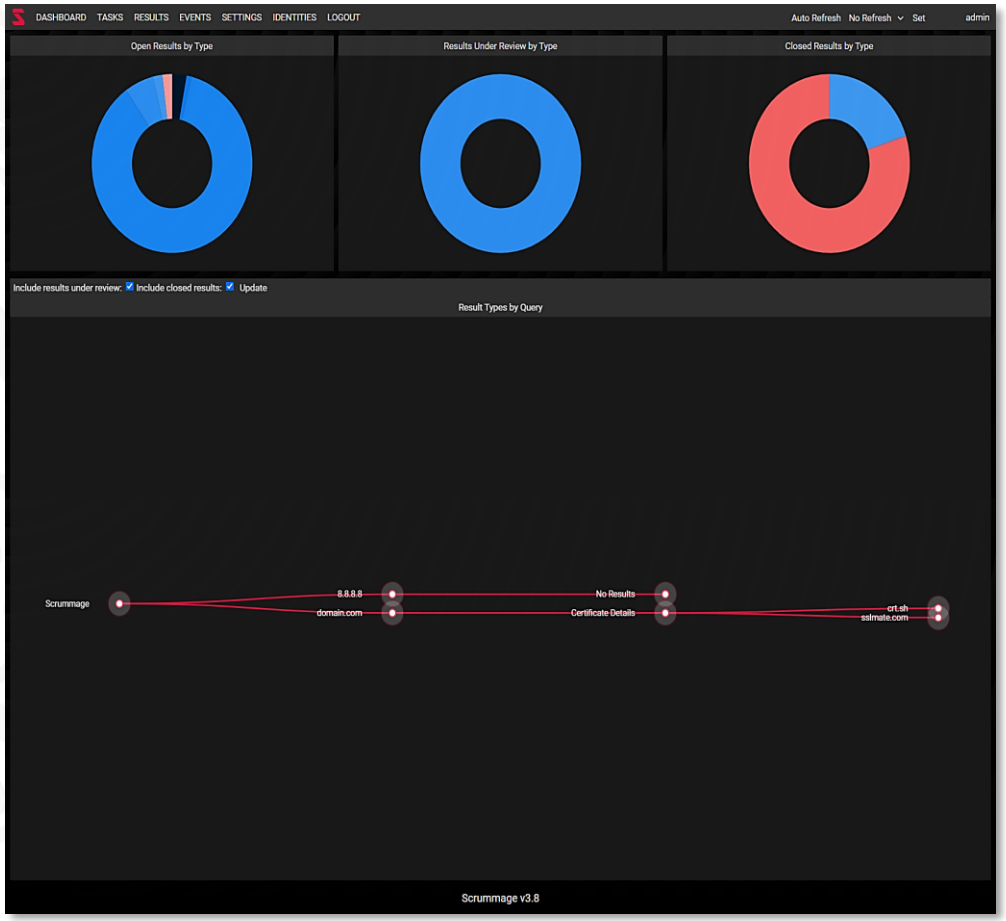
- **Obtiene datos de un objetivo usando muchos sitios diferentes como fuentes**
  - Obtiene mucha información de fuentes de datos públicas: correos electrónicos, nombres, subdominios, IP, URLs...
  - Utiliza motores de búsqueda conocidos para diferentes tipos de información
    - baidu, bing, bingapi,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

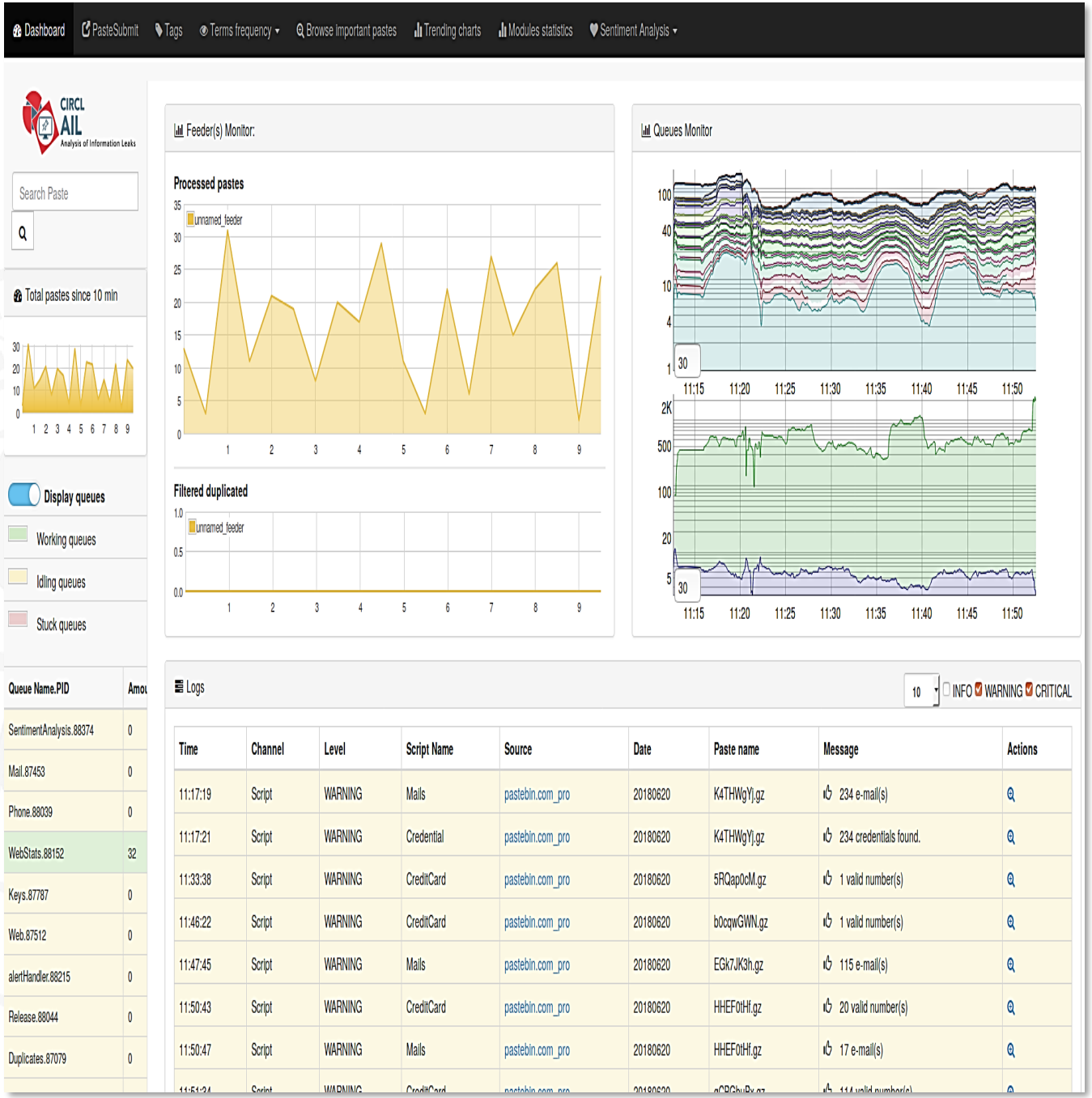


AIL Framework

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…

Seguridad de Sistemas Informáticos

- **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
- **Recuerda: 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...

¿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 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

< Ir al Índice

OSINT CONTRA CÓDIGO FUENTE

El código fuente también puede ser una amenaza OSINT

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

GitGot

https://github.com/BishopFox/GitGot

Seguridad de Sistemas Informáticos

- **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

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

?

- 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

Fuente: Bing Chat AI

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo