

Master en Ciberseguridad - Universidad Católica de Murcia en
colaboración con Telefónica e Eleven Paths 8va Edición.



DISTRIBUCIÓN ORIENTADA A LA OBTENCIÓN DE INFORMACIÓN EN LA RED

Presenta:

JIM CÁRDENAS CRUZ

Tutores:

FELIZ BREZO FERNÁNDEZ

YAIZA RUBIO VIÑUELA

Abril – 2022

CONTENIDO

| | |
|--|----|
| RESUMEN | 6 |
| ABSTRACT..... | 7 |
| 1. INTRODUCCIÓN..... | 8 |
| 2. PROBLEMA OBJETO..... | 9 |
| 3. OBJETIVOS DEL PROYECTO..... | 10 |
| 3.1. Objetivo Principal | 10 |
| 3.2. Objetivos Secundarios..... | 10 |
| 4. ESTADO DEL ARTE | 11 |
| 5. HIPÓTESIS..... | 13 |
| 6. DEMOSTRACIÓN..... | 14 |
| 6.1. Creación e instalación mínima de la máquina virtual | 14 |
| 6.2. Uso del Script sobre una maquina limpia de Ubuntu | 15 |
| 6.3. Herramientas..... | 16 |
| 6.3.1. Herramientas que requieren instalación | 16 |
| 6.3.1.1. Recon- <i>ng</i> | 16 |
| 6.3.1.2. The Harvester | 18 |
| 6.3.1.3. Maltego | 19 |
| 6.3.1.4. Sherlock..... | 20 |
| 6.3.1.5. Nmap | 22 |
| 6.3.1.6. OSRFramework..... | 23 |
| 6.3.1.7. OSI.IG..... | 26 |
| 6.3.1.8. Twint (Twitter Intelligence Tool)..... | 28 |
| 6.3.1.9. Metagoofil | 29 |
| 6.3.1.10. Sublist3r..... | 30 |
| 6.3.1.11. Katana-ds..... | 32 |
| 6.3.1.12. DMitry | 33 |
| 6.3.1.13. Ghunt..... | 34 |
| 6.3.1.14. Infoga | 36 |
| 6.3.1.15. H8mail | 37 |
| 6.3.1.16. Dnsmap | 38 |

| | | |
|-----------|---------------------------------|----|
| 6.3.1.17. | SocialPwned | 39 |
| 6.3.1.18. | Profil3r..... | 41 |
| 6.3.1.19. | FisherMan..... | 43 |
| 6.3.2. | Herramientas web..... | 44 |
| 6.3.2.1. | Shodan..... | 44 |
| 6.3.2.2. | SpiderFoot HX..... | 46 |
| 6.3.2.3. | Robtex | 47 |
| 6.3.2.4. | Geosocial Footprint..... | 48 |
| 6.3.2.5. | Metashield Clean-up Online..... | 49 |
| 6.3.2.6. | Mr Looquer..... | 50 |
| 6.3.2.7. | Censys..... | 51 |
| 6.3.2.8. | Flightaware..... | 52 |
| 6.3.2.9. | Lampyre..... | 53 |
| 6.3.2.10. | Builtwith | 54 |
| 6.3.2.11. | Searchcode | 55 |
| 6.3.2.12. | Zoomeye..... | 56 |
| 6.3.2.13. | DnsDumpster | 57 |
| 6.3.2.14. | Wayback machine | 58 |
| 6.3.2.15. | Ipinfo | 59 |
| 6.3.2.16. | Centralops | 60 |
| 6.3.2.17. | ImgOps | 62 |
| 6.3.2.18. | Whotwi..... | 64 |
| 6.3.2.19. | Urlscan.io..... | 65 |
| 6.4. | Exportado de .ova | 66 |
| 7. | CONCLUSIONES | 68 |
| 8. | BIBLIOGRAFIA..... | 69 |

Tabla de Ilustraciones

| | |
|---|----|
| Ilustración 1 Instalación minima | 14 |
| Ilustración 2 Sistema Operativo Maquina Virtual..... | 14 |
| Ilustración 3 Instalación del Script | 15 |
| Ilustración 4 Rencon-ng | 16 |
| Ilustración 5 Ejemplo de Modulos Recon-ng | 17 |
| Ilustración 6 Modulo Interesting_files Recon-ng | 17 |
| Ilustración 7 Set url y Resultados | 18 |
| Ilustración 8 TheHarvester Ayuda | 18 |
| Ilustración 9 TheHarvester Resultado..... | 19 |
| Ilustración 10 Maltego | 19 |
| Ilustración 11 Maltego Versión Free | 20 |
| Ilustración 12 Sherlock - Ayuda..... | 21 |
| Ilustración 13 Sherlock - Resultado..... | 21 |
| Ilustración 14 Nmap | 22 |
| Ilustración 15 Nmap - Resultado..... | 23 |
| Ilustración 16 OSRFramework - Ayuda | 23 |
| Ilustración 17 OSRFramework Searchfy | 25 |
| Ilustración 18 OSRFramework Searchfy Resultado | 26 |
| Ilustración 19 OSI.IG - Ayuda..... | 26 |
| Ilustración 20 OSI.IG - Resultado..... | 27 |
| Ilustración 21 Twint - Ayuda | 28 |
| Ilustración 22 Twint - Resultado | 29 |
| Ilustración 23 Metagoofil - Ayuda | 29 |
| Ilustración 24 Metagoofil - Resultado..... | 30 |
| Ilustración 25 Sublist3r..... | 30 |
| Ilustración 26 Sublist3r - Ayuda | 31 |
| Ilustración 27 Sublist3r – Resultado..... | 31 |
| Ilustración 28 Katana - Ayuda | 32 |
| Ilustración 29 Katana - Resultado | 33 |
| Ilustración 30 DMitry - Ayuda | 33 |
| Ilustración 31 DMitry - Resultado | 34 |
| Ilustración 32 Ghunt - Ayuda | 35 |
| Ilustración 33 Ghunt - Resultado | 35 |
| Ilustración 34 Infoga - Ayuda | 36 |
| Ilustración 35 Infoga - Resultado | 37 |
| Ilustración 36 H8mail - Ayuda | 37 |
| Ilustración 37 H8mail - Resultado | 38 |
| Ilustración 38 Dnsmap - Ayuda | 39 |
| Ilustración 39 Dnsmap - Resultado | 39 |
| Ilustración 40 SocialPwned - Ayuda | 40 |
| Ilustración 41 SocialPwned – Configuración | 40 |
| Ilustración 42 SocialPwned - Resultado | 41 |
| Ilustración 43 Profil3r - Ayuda..... | 41 |

| | |
|---|----|
| Ilustración 44 Profil3r - Resultados | 42 |
| Ilustración 45 FisherMan..... | 43 |
| Ilustración 46 Marcadores en Firefox | 44 |
| Ilustración 47 Shodan..... | 45 |
| Ilustración 48 Shodan - Interbank Resultado | 45 |
| Ilustración 49 SpiderFoot HX – Username | 46 |
| Ilustración 50 FootPrint Resumen..... | 47 |
| Ilustración 51 FootPrint Resumen 2..... | 47 |
| Ilustración 52 Robtex | 48 |
| Ilustración 53 Robtex - Resultado | 48 |
| Ilustración 54 GeosocialFootprint..... | 49 |
| Ilustración 55 Metashield Clean-up Online..... | 49 |
| Ilustración 56 MetashieldClean-up - Resultado | 50 |
| Ilustración 57 Mr. Looquer..... | 51 |
| Ilustración 58 Censys..... | 51 |
| Ilustración 59 Flightaware..... | 52 |
| Ilustración 60 Flightaware - Resultado..... | 52 |
| Ilustración 61 Lampyre..... | 53 |
| Ilustración 62 Lampyre - Resultados | 53 |
| Ilustración 63 Builtwith | 54 |
| Ilustración 64 Builtwith - Resultados | 54 |
| Ilustración 65 Searchcode | 55 |
| Ilustración 66 Searchcode - Resultado..... | 56 |
| Ilustración 67 Zoomeye..... | 56 |
| Ilustración 68 Zoomeye - Resultado..... | 57 |
| Ilustración 69 DnsDumpster..... | 57 |
| Ilustración 70 DnsDumpster - Resultado | 58 |
| Ilustración 71 Wayback machine | 58 |
| Ilustración 72 Wayback Machine - Resultado..... | 59 |
| Ilustración 73 Ipinfo | 59 |
| Ilustración 74 Ipinfo - Resultado | 60 |
| Ilustración 75 Central Ops..... | 61 |
| Ilustración 76 Central Ops - Resultado..... | 62 |
| Ilustración 77 ImgOps | 63 |
| Ilustración 78 ImgOps - Resultado | 63 |
| Ilustración 79 Whotwi | 64 |
| Ilustración 80 Whotwi - Resultado..... | 64 |
| Ilustración 81 UrlScan.io | 65 |
| Ilustración 82 UrlScan.io - Resultado | 65 |
| Ilustración 83 Exportar .ova | 66 |
| Ilustración 84 Exportar .ova 2 | 66 |
| Ilustración 85 Exportar .ova 3 | 67 |
| Ilustración 86 Ova Exportado..... | 67 |

RESUMEN.

La inteligencia de código abierto (OSINT - Open Source INTeelligence), es una rama de la ciberseguridad, cuyo estudio y uso está creciendo actualmente de forma exponencial, esta rama se utiliza principalmente para obtener información, analizarla y poder tomar decisiones en función de ese análisis. En la actualidad, esta información está disponible de forma libre en la web y con la aplicación adecuada de herramientas de código abierto se puede facilitar esta tarea.

El objetivo de este trabajo es proponer una distribución en Ubuntu con las herramientas necesarias de código abierto, que en su totalidad sea utilizada para realizar búsquedas mediante el uso de herramientas OSINT. Esta propuesta se debe a que las herramientas OSINT son cada vez más numerosas, por lo que deben ser ordenadas y probadas para que su conglomerado en la distribución Ubuntu pueda facilitar la obtención de datos a través de OSINT.

Por otro lado, esta propuesta se debe al hecho de que estas herramientas crecen de acuerdo a las nuevas fuentes de información alojadas en la web a nivel mundial, también se sabe que las mismas herramientas están cambiando todo el tiempo, por lo que es necesario que se actualicen continuamente.

PALABRAS CLAVE:

Código abierto, OSINT, Herramientas OSINT, Distribución ubuntu, Exponencial, Ciberseguridad, Open Source Intelligence, La inteligencia de código abierto.

ABSTRACT.

Open Source Intelligence (OSINT), is a branch of cybersecurity, whose study and use is currently growing exponentially, this branch is mainly used to obtain information, analyze it and be able to make decisions based on that analysis. Currently, this information is freely available on the web and with the proper application of open source tools this task can be facilitated.

The objective of this work is to propose an Ubuntu distribution with the necessary open source tools, which in its entirety can be used to perform searches through the use of OSINT tools. This proposal is due to the fact that OSINT tools are more and more numerous, so they must be ordered and tested so that their conglomeration in the Ubuntu distribution can facilitate data retrieval through OSINT.

On the other hand, this proposal is due to the fact that these tools are growing according to the new sources of information hosted on the web worldwide, it is also known that the same tools are changing all the time, so it is necessary that they are continuously updated.

KEY WORDS:

Open Source, OSINT, OSINT Tools, Ubuntu Distribution, Exponential, Cybersecurity, Open Source Intelligence, Open Source Intelligence.

1. INTRODUCCIÓN

Los datos que se encuentran en la web son abundantes, al punto de que ni siquiera una persona puede llegar a imaginar todo lo que podría encontrar en la web y cada día que pasa el crecimiento de estos datos es abismal, esta información se encuentra abierta para todos los usuarios, público en general, la información que se aloja en la web es muy valiosa por lo que encontrarla, ordenarla y evaluarla siempre será una tarea complicada de realizar, esto se debe a la gran inmensidad de datos existentes, pero gracias a OSINT, las herramientas que se ofrecen y las tácticas adecuadas, se puede facilitar un poco este arduo trabajo, de este modo se pueden centrar todos los esfuerzos en áreas específicas de acuerdo a los datos que se quieran consultar y obtener buenos resultados.

Para poder realizar con éxito estas búsquedas se deberá tener un plan y/o estrategia a seguir para que de este modo los esfuerzos realizados no sean inútiles o los resultados sean poco relevantes, de modo que no conduzca al agotamiento o perdida de interés en el camino.

En el presente trabajo se propone una distribución en Ubuntu donde se recopilan herramientas de OSINT, previamente probadas y analizadas, para así poder facilitar la búsqueda inteligente en fuentes abiertas, se proporcionará un script para poder realizar la instalación en cualquier distribución limpia de Ubuntu así como la imagen OVA, estas herramientas son gratuitas aunque algunas poseen mucho mejor motor de búsqueda en su versión de paga, esto no quiere decir que sin esta paga la información es limitada para poder obtener información valiosa o menor a la prevista, ya que se podrá optar por probar más herramientas libres con los mismos o resultados parecidos.

2. PROBLEMA OBJETO

Al momento de conocer más a fondo OSINT, me pude dar cuenta de la problemática que tenía en cuanto a mi ambiente laboral, ciberseguridad para bancos en Sudamérica, esta problemática se rige en mayor nivel a la búsqueda diaria de datos sobre Cibercriminales (que realizan ataques phishing u otros tipos de ataques a los usuarios de los bancos) y toda la información que se debe analizar, lo cual conlleva al uso diario de herramientas que ofrece OSINT.

Esta problemática en mayor nivel genera la siguiente pregunta:

¿Se puede extraer todos los datos de un Cibercriminal o relacionados, sin el uso de herramientas de OSINT?

Según la investigación DIGITAL 2020: PERU de “We are Social” y “Hootsuite”, en enero de 2020 había 24 millones de usuarios de internet, mientras que los usuarios en redes sociales aumento en 1.1 millones en un año (+4.8%)

Crear perfiles falsos en las redes sociales es cada vez más común. Los ciberdelincuentes crean cuentas falsas, anuncios falsos o enlaces maliciosos para cometer fraudes, toda esta información seria casi imposible de encontrar y analizar con búsquedas simples sin el uso de OSINT y de mayor complejidad aun, sin el uso de las herramientas que se ofrecen.

3. OBJETIVOS DEL PROYECTO

3.1. Objetivo Principal

El objetivo principal a alcanzar en este proyecto final, es de poder analizar, probar y juntar las herramientas OSINT en una distribución limpia de Ubuntu y entregar un fichero .ova que facilite el uso de dichas herramientas, para para poder realizar la búsqueda de información de forma eficiente.

3.2. Objetivos Secundarios

- Proporcionar un fichero .ova basada en la distribución Ubuntu donde se pueda usar el catálogo de herramientas descritas en este proyecto.
- Brindar un script que se pueda correr sobre una distribución limpia de Ubuntu, esto permitirá la instalación de todas las herramientas del catálogo (que requieran instalación).
- Brindar información de las herramientas, como usarlas y categorizarlas por el tipo de datos que se puede obtener de cada una de ellas.

4. ESTADO DEL ARTE

Las herramientas en la web pueden llegar a ser demasiadas, por lo que se tomara de base las herramientas libres dentro del master cursado (donde se aportaron las herramientas más relevantes y más usadas), todas estas herramientas son probadas y agregadas a la distribución en Ubuntu.

A parte de esto se encontraron cuatro proyectos muy interesantes y relevantes, donde se pueden observar distribuciones con diferentes herramientas, con finalidad muy parecida al proyecto actual, a continuación, se describirá brevemente cada uno y las mejoras que se darán o cambios y la base que se tomara de estos:

4.1. Fuente 1:

El proyecto realizado por Raquel Acosta de la 7ma edición del Master en Ciberseguridad, contiene en total 27 herramientas en una máquina virtual, aunque no se logró poder observar el proyecto en su totalidad, ya que no está en la web de forma libre, sino que se debe ser alumno del “Curso de Ciberinvestigación Cibergia”, dio el punto de partida en cuanto a la problemática y se pudo redireccionar al proyecto actual.

Este proyecto no está abierto en la web por lo que se diferenciaría, además que 27 herramientas resultan un tanto escasas.

4.2. Fuente 2:

El proyecto llamado “Osintux” ofrece una ISO la cual fue actualizada por última vez el 2018, posee 34 herramientas, “Osintux” tiene muy buenas referencias, del cual se confirmarán las herramientas más usadas y también se pudo observar que posee herramientas que están obsoletas.

La importancia de este proyecto es que estas herramientas están categorizadas lo cual le da un peso añadido al proyecto, esta categorización se tomara de ejemplo para poder categorizar las herramientas del proyecto actual.

4.3. Fuente 3:

El proyecto llamado “HURON” posee 27 herramientas, el cual al igual que el proyecto anterior está un poco pasado, ya que su última actualización fue del 2019 y aun el umbral de uso es bastante positivo, esta herramienta fue probada y se pudo dar con las herramientas más útiles y que aún están en uso, de este proyecto se tomó la base del uso de herramientas más importantes, mas no su categorización ya que no la posee.

4.4. Fuente 4:

Por último, se tiene el proyecto de Miguel Navarro publicado en ENIIT, el alumno del 7mo Master en Ciberseguridad, pudo realizar un proyecto muy completo en cuanto a la cantidad y utilidad de herramientas, son 42 herramientas que se brindan en dicha distribución, son categorizadas de mejor manera, lo cual hace mucho más entendible el proyecto, y también la actualización de esta distribución no es mayor a 1 año de antigüedad lo cual asegura el funcionamiento actual de todas las herramientas.

Se tomo de base muchas herramientas de este proyecto, pero se dio con la sorpresa que, aunque el proyecto es muy parecido, la cantidad de herramientas que se diferencian con este es bastante elevado, de las 42 herramientas que se proponen en el proyecto 26 se diferenciaran de la presente distribución, lo cual es muy importante ya que en muy poco tiempo las herramientas más usadas cambian y que aparecen muchas más herramientas, por lo cual la actualización constante es muy necesaria.

5. HIPÓTESIS

La distribución que poseerá las herramientas de OSINT, por su entendimiento y su fácil instalación, como finalidad tendrá que poder facilitar el trabajo a los usuarios (estos usuarios no necesariamente deben poseer mucho conocimiento en ciberseguridad), que requieran el uso de herramientas OSINT y así poder usar esta distribución de manera efectiva y eficaz.

6. DEMOSTRACIÓN

6.1. Creación e instalación mínima de la máquina virtual.

La distribución usada para esta instalación fue la de “ubuntu-20.04.4-desktop-amd64”

A continuación, se observan las evidencias de la instalación de la maquina limpia.

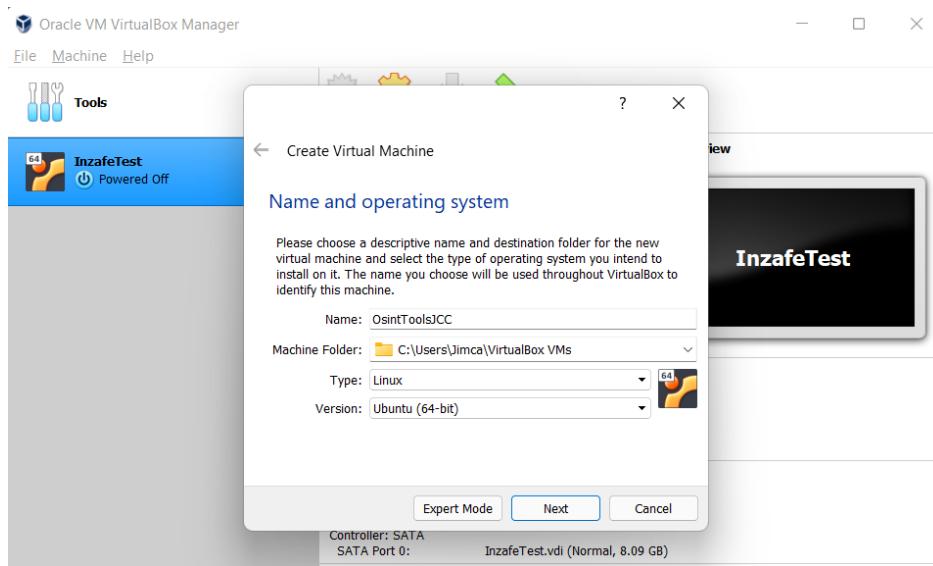


Ilustración 2 Sistema Operativo Maquina Virtual

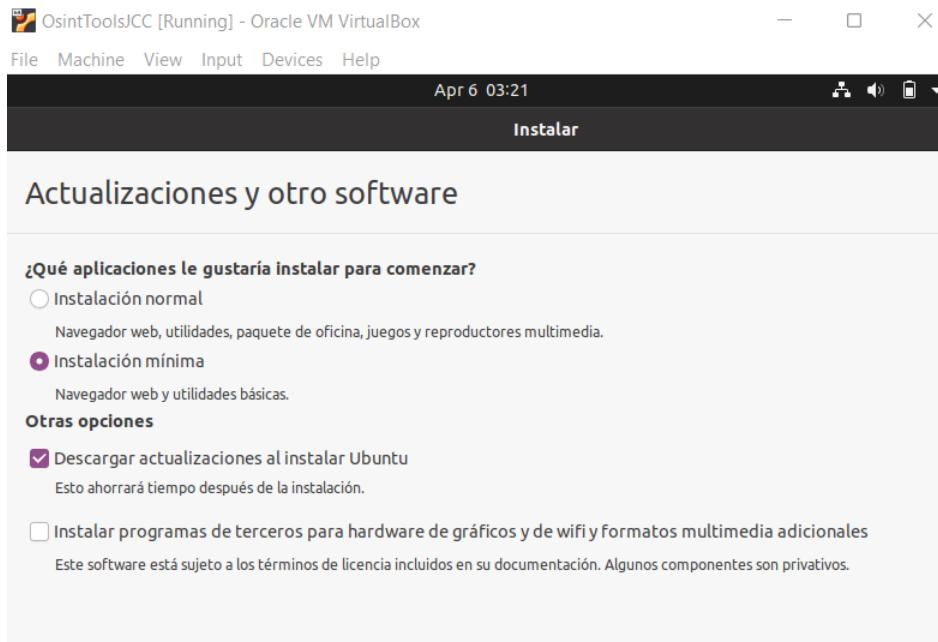


Ilustración 1 Instalación minima

6.2.Uso del Script sobre una maquina limpia de Ubuntu

Solo se requiere descargar el archivo “osintToolsScript.sh” y hacer correr las siguientes instrucciones en el path de archivo en la terminal:

- sudo su (contraseña: osint)
- sudo chmod +x osintToolsScript.sh
- sudo bash osintToolsScript.sh

Lo cual procederá con la instalación como se muestra a continuación

```
root@lordmadness:/home/lordmadness/Escritorio# sudo bash osintToolsScript.sh
Obj:1 http://security.ubuntu.com/ubuntu focal-security InRelease
Obj:2 http://pe.archive.ubuntu.com/ubuntu focal InRelease
Des:3 http://pe.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Des:4 http://pe.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Des:5 http://pe.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages [629 kB]
Des:6 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [1.712 kB]
Des:7 http://pe.archive.ubuntu.com/ubuntu focal-updates/main Translation-en [320 kB]
Des:8 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata [278 kB]
Ign:8 http://pe.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11 Metadata
Ign:16 http://pe.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP-11 Metadata
Ign:17 http://pe.archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 DEP-11 Metadata
0% [7 Translation-en store 0 B] [Esperando las cabeceras]
```

Ilustración 3 Instalación del Script

Solo se debe proceder a esperar que la instalación termine y se tendrán las herramientas instaladas, para su uso se seguirá el siguiente apartado de Herramientas.

6.3. Herramientas

Las herramientas propuestas estarán categorizadas como sigue a continuación:

- Herramientas que requieren instalación
 - Herramientas web

Dentro de los detalles de cada herramienta se dará una categorización más sobre el tipo de datos que se puede obtener.

6.3.1. Herramientas que requieren instalación

6.3.1.1. Recon-ng

Para el uso de Recon-**ng** solo basta texpear **recon-*ng*** en la terminal como se muestra a continuación.

Ilustración 4 Rencon-ng

Para recibir ayuda de todos los modulos que se pueden consultar se escribe `marketplace info all` dando todos los modulos disponibles.

```
[recon-ng][default] > marketplace info all

+---+-----+
| path      | discovery/info_disclosure/cache_snoop
| name      | DNS Cache Snooper
| author    | thrapt (thrapt@gmail.com)
| version   | 1.1
| last_updated | 2020-10-13
| description | Uses the DNS cache snooping technique to check for visited domains
| required_keys | []
| dependencies | []
| files     | ['av_domains.lst']
| status    | not installed
+---+-----+


+---+-----+
| path      | discovery/info_disclosure/interesting_files
| name      | Interesting File Finder
| author    | Tim Tomes (@lanmaster53), thrapt (thrapt@gmail.com), Jay Turla (@shipcod3), and Mark Jeffery
| version   | 1.2
| last_updated | 2021-10-04
| description | Checks hosts for interesting files in predictable locations.
| required_keys | []
| dependencies | []
| files     | ['interesting_files_verify.csv']
| status    | not installed
+---+-----+
```

Ilustración 5 Ejemplo de Modulos Recon-ng

Datos disponibles: En caso de Recon-ng se puede realizar la búsqueda de muchos tipos de datos, solo hace falta leer cada uno de los modulos disponibles, como ejemplo a continuación se instala y carga el módulo que utiliza de entrada una url para descubrir “archivos interesantes”

```
[recon-ng][default] > marketplace install discovery/info_disclosure/interesting_files
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Reloading modules...
[recon-ng][default] > modules
Interfaces with installed modules

Usage: modules <load|reload|search> [...]
[recon-ng][default] > modules load discovery/info_disclosure/interesting_files
[recon-ng][default][interesting_files] > █
```

Ilustración 6 Modulo Interesting_files Recon-ng

Luego se realiza el SET de la url y se hace correr como se muestra a continuación con los resultados.

```
[recon-ng][default][interesting_files] > options set SOURCE ucam.edu  
SOURCE => ucam.edu  
[recon-ng][default][interesting_files] > run  
[*] http://ucam.edu:80/robots.txt => 200. 'robots.txt' found!  
[*] http://ucam.edu:80/sitemap.xml => 200. 'sitemap.xml' found!  
[*] http://ucam.edu:80/sitemap.xml.gz => 404  
[*] http://ucam.edu:80/crossdomain.xml => 404  
[*] http://ucam.edu:80/phpinfo.php => 404  
[*] http://ucam.edu:80/test.php => 404  
[*] http://ucam.edu:80/elmah.axd => 404  
[*] http://ucam.edu:80/server-status => 404  
[*] http://ucam.edu:80/jmx-console/ => 404  
[*] http://ucam.edu:80/admin-console/ => 404  
[*] http://ucam.edu:80/web-console/ => 404  
[*] 2 interesting files found.  
[*] Files downloaded to '/root/.recon-ng/workspaces/default/'  
[recon-ng][default][interesting_files] > █
```

Ilustración 7 Set url y Resultados

6.3.1.2. The Harvester

Para el uso de The Harvester, se debe entrar a la carpeta con nombre “theHarvester” se puede lograr ubicando el path de escritorio y a continuación `cd theHarvester/`, luego para iniciar se hará correr el siguiente comando `python3 theHarvester.py -h` para obtener de inicio la ayuda que se proporciona.

```
root@lordmadness:/home/lordmadness/Escritorio/theHarvester# python3 theHarvester.py -h
*****
*          _ _ _ _ _          *
*         [ ] [ ] [ ] [ ] [ ]  *
*        / \ / \ / \ / \ / \ / \ *
*       [ ] [ ] [ ] [ ] [ ] [ ] *
*      / \ / \ / \ / \ / \ / \ / \ *
*     [ ] [ ] [ ] [ ] [ ] [ ] [ ] *
*    / \ / \ / \ / \ / \ / \ / \ / \ *
*   [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] *
*  / \ / \ / \ / \ / \ / \ / \ / \ / \ *
* [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] *
* / \ / \ / \ / \ / \ / \ / \ / \ / \ / \ *
* [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] *
*  _ _ _ _ _          *
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
* ****

usage: theHarvester.py [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [--screenshot S]
                      [-f FILENAME] [-b SOURCE]
```

Ilustración 8 TheHarvester Ayuda

Datos disponibles: theHarvester se utiliza para recopilar inteligencia de fuente abierta (OSINT) en una empresa o dominio.

Para poner un ejemplo se pone el siguiente comando `python3 theHarvester.py -d ucam.edu -b bing`, donde “-d” significa el dominio y “-b” el motor de búsqueda.

Ilustración 9 TheHarvester Resultado

6.3.1.3. Maltego

Para el uso de Maltego se iniciará como una aplicación común (buscar manualmente Maltego y se mostrará la aplicación) y ya estará instalada lista para ser usada.



Ilustración 10 Maltego

Una vez iniciada la herramienta se podrá observar la primera configuración donde se puede escoger versiones de pago y gratuitas, se recomienda seguir un pequeño curso de cómo usar Maltego y las diferencias entre la versión pagada y la gratuita.

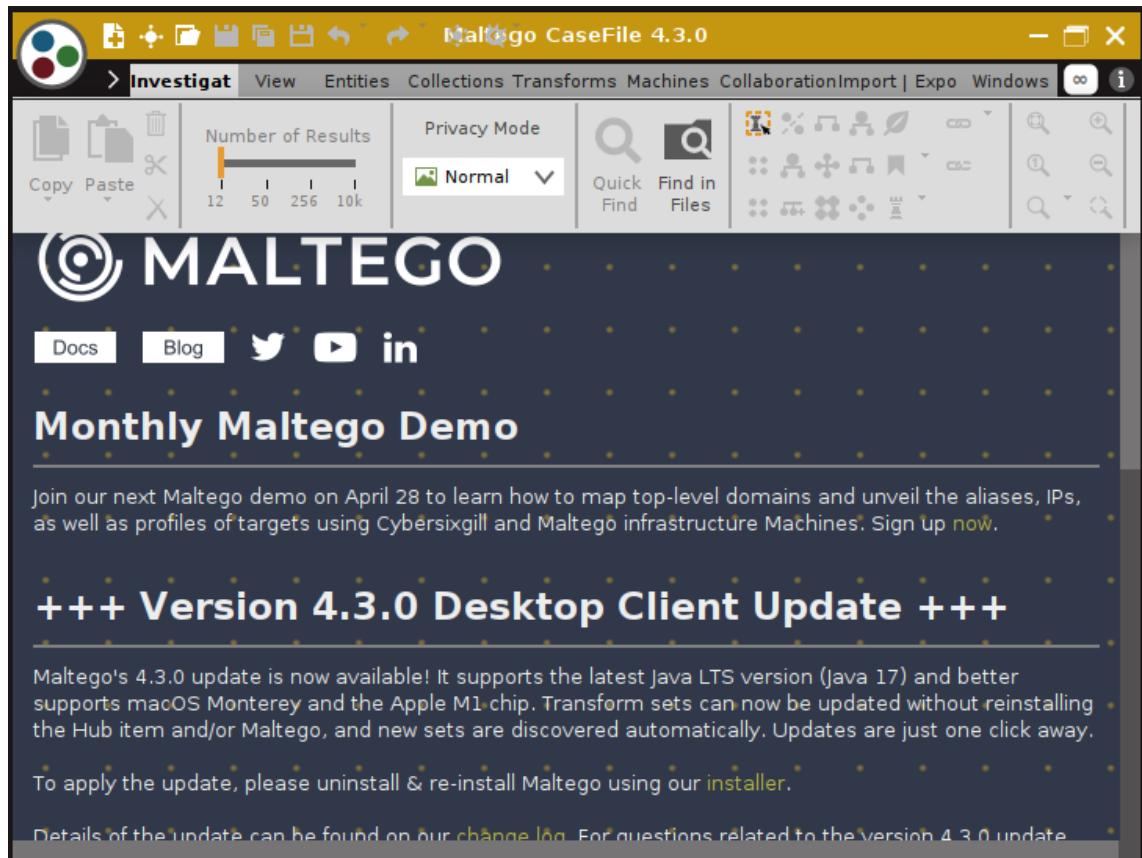


Ilustración 11 Maltego Versión Free

Datos disponibles: Maltego es una herramienta muy potente que permite búsquedas como por ejemplo de usuarios, alias, imágenes, personas, números de teléfono, frases, documentos, correos y muchos otros más.

Su versión instalada en esta distribución permite su uso de modo intuitivo.

6.3.1.4. Sherlock

Para el uso de Sherlock, se debe entrar a la carpeta con nombre “sherlock” se puede lograr ubicando el path de escritorio y a continuación `cd`

`sherlock/sherlock/`, luego para iniciar se hará correr el siguiente comando
`python3 sherlock.py -h` para obtener de inicio la ayuda que se proporciona.

```
root@lordmadness:/home/lordmadness/Escritorio/sherlock/sherlock# python3 sherlock.py -h
usage: sherlock.py [-h] [--version] [--verbose] [--folderoutput FOLDEROUTPUT]
                   [--output OUTPUT] [--tor] [--unique-tor] [--csv] [--site SITE_NAME]
                   [--proxy PROXY_URL] [--json JSON_FILE] [--timeout TIMEOUT]
                   [--print-all] [--print-found] [--no-color] [--browse] [--local]
                   USERNAMES [USERNAMES ...]

Sherlock: Find Usernames Across Social Networks (Version 0.14.0)

positional arguments:
  USERNAMES           One or more usernames to check with social networks.

optional arguments:
  -h, --help          show this help message and exit
  --version          Display version information and dependencies.
  --verbose, -v, -d, --debug
                      Display extra debugging information and metrics.
  --folderoutput FOLDEROUTPUT, -fo FOLDEROUTPUT
                      If using multiple usernames, the output of the results will be
                      saved to this folder.
  --output OUTPUT, -o OUTPUT
                      If using single username, the output of the result will be saved
                      to this file.
  --tor, -t           Make requests over Tor; increases runtime; requires Tor to be
                      installed and in system path.
  --unique-tor, -u    Make requests over Tor with new Tor circuit after each request;
                      increases runtime; requires Tor to be installed and in system
                      path.
```

Ilustración 12 Sherlock - Ayuda

Datos disponibles: Sherlock es una herramienta que recibe de entrada una cadena de texto de nombres de usuarios y busca perfiles en redes sociales por nombre de usuario.

Luego de poder visualizar todas las opciones que ofrece Sherlock para su configuración se muestra el siguiente ejemplo.

```
root@lordmadness:/home/lordmadness/Escritorio/sherlock/sherlock# python3 sherlock.py lordmadness
[*] Checking username lordmadness on:

[+] Archive.org: https://archive.org/details/@lordmadness
[+] AskFM: https://ask.fm/lordmadness

[+] Blogger: https://lordmadness.blogspot.com
[+] CapFriendly: https://www.capfriendly.com/users/lordmadness
[+] Chaturbate: https://chaturbate.com/lordmadness
[+] Chess: https://www.chess.com/member/lordmadness
[+] Codecademy: https://www.codecademy.com/profiles/lordmadness
[+] Countable: https://www.countable.us/lordmadness
```

Ilustración 13 Sherlock - Resultado

6.3.1.5. Nmap

Para el uso de Nmap solo se tendrá que escribir desde cualquier path “nmap” y así se accederá a toda la ayuda que posee nmap

```
root@lordmadness:/home/lordmadness/Escritorio# nmap
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
      -iL <inputfilename>; Input from list of hosts/networks
      -iR <num hosts>; Choose random targets
      --exclude <host1[,host2][,host3],...>; Exclude hosts/networks
      --excludefile <exclude_file>; Exclude list from file
HOST DISCOVERY:
      -sL: List Scan - simply list targets to scan
      -sn: Ping Scan - disable port scan
      -Pn: Treat all hosts as online -- skip host discovery
      -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
      -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
      -PO[protocol list]: IP Protocol Ping
      -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
      --dns-servers <serv1[,serv2],...>; Specify custom DNS servers
      --system-dns: Use OS's DNS resolver
      --traceroute: Trace hop path to each host
```

Ilustración 14 Nmap

Datos disponibles: Nmap es una herramienta cuya funcionalidad es la de escanear puertos, para poder realizar este escaneo se recibe de datos de entrada Nombres de dominio, IPs, DNS.

A continuación, se realiza un ejemplo de un escaneo a un dominio con el siguiente comando `nmap ucam.edu`.

```

root@lordmadness:/home/lordmadness/Escritorio# nmap ucam.edu
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-15 04:28 -05
Nmap scan report for ucam.edu (193.147.26.228)
Host is up (0.24s latency).
rDNS record for 193.147.26.228: ucamonline.net
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8080/tcp  closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 16.96 seconds

```

Ilustración 15 Nmap - Resultado

6.3.1.6. OSRFramework

Para obtener ayuda de OSRFramework solo es necesario ingresar el comando `osrf`, en cualquier path, dando de resultado lo siguiente:

```

root@Lordmadness:/home/lordmadness/Escritorio# osrf
usage: osrf [-h] [--license] [--version] <sub_command> <sub_command_options> ...

OSRFramework CLI. Collection of tools included in the framework.

SUBCOMMANDS:
  List of available commands that can be invoked using OSRFramework CLI.

  <sub_command> <sub_command_options>
    alias_generator      Generates a list of candidate usernames based on known information.
    checkfy              Verifies if a given email address matches a pattern.
    domainfy             Checks whether domain names using words and nicknames are available.
    mailfy               Gets information about email accounts.
    phonefy              Looks for information linked to spam practices by a phone number.
    searchfy             Performs queries on several platforms.
    usufy                Looks for registered accounts with given nicknames.
    upgrade              Updates the module.

ABOUT ARGUMENTS:
  Showing additional information about this program.

  -h, --help            shows this help and exists.
  --license            shows the GPLv3+ license and exists.
  --version            shows the version of the program and exists.

```

Ilustración 16 OSRFramework - Ayuda

Datos disponibles: Para el uso de OSRFramework se debe tener en cuenta los siguientes modulos incluidos.

alias_generator: Genera apodos de candidatos basados en información conocida sobre el objetivo. Entrada: información sobre el objetivo. Salida: lista de posibles apodos.

checkfy: Adivina posibles correos electrónicos basándose en una lista de apodos de candidatos y un patrón. Entrada: lista de apodos y un patrón de correo electrónico. Salida: lista de correos electrónicos que coinciden con el patrón.

domainfy: Encuentra dominios que actualmente se resuelven usando una palabra o apodo dado. Entrada: lista de palabras. Salida: dominios que usan esa palabra.

mailfy: Encuentre más información sobre los correos Entrada: lista de apodos o correos electrónicos. Salida: información encontrada sobre el correo electrónico.

phonefy: Recupera información sobre teléfonos móviles. Entradas: lista de teléfonos. Salidas: Teléfonos vinculados a spam.

searchfy: Encuentra perfiles vinculados a un nombre completo. Entradas: lista de perfiles. Salidas: Perfiles conocidos vinculados a la consulta.

usufy: Identifica perfiles de redes sociales usando un apodo dado. Entradas: lista de apodos. Salidas: Perfiles conocidos en las redes sociales que usan esos apodos.

A continuación, se muestra un ejemplo con el código `searchfy -q chema alonso`

```
root@lordmadness:/home/lordmadness/Escritorio# searchfy -q chema alonso
```

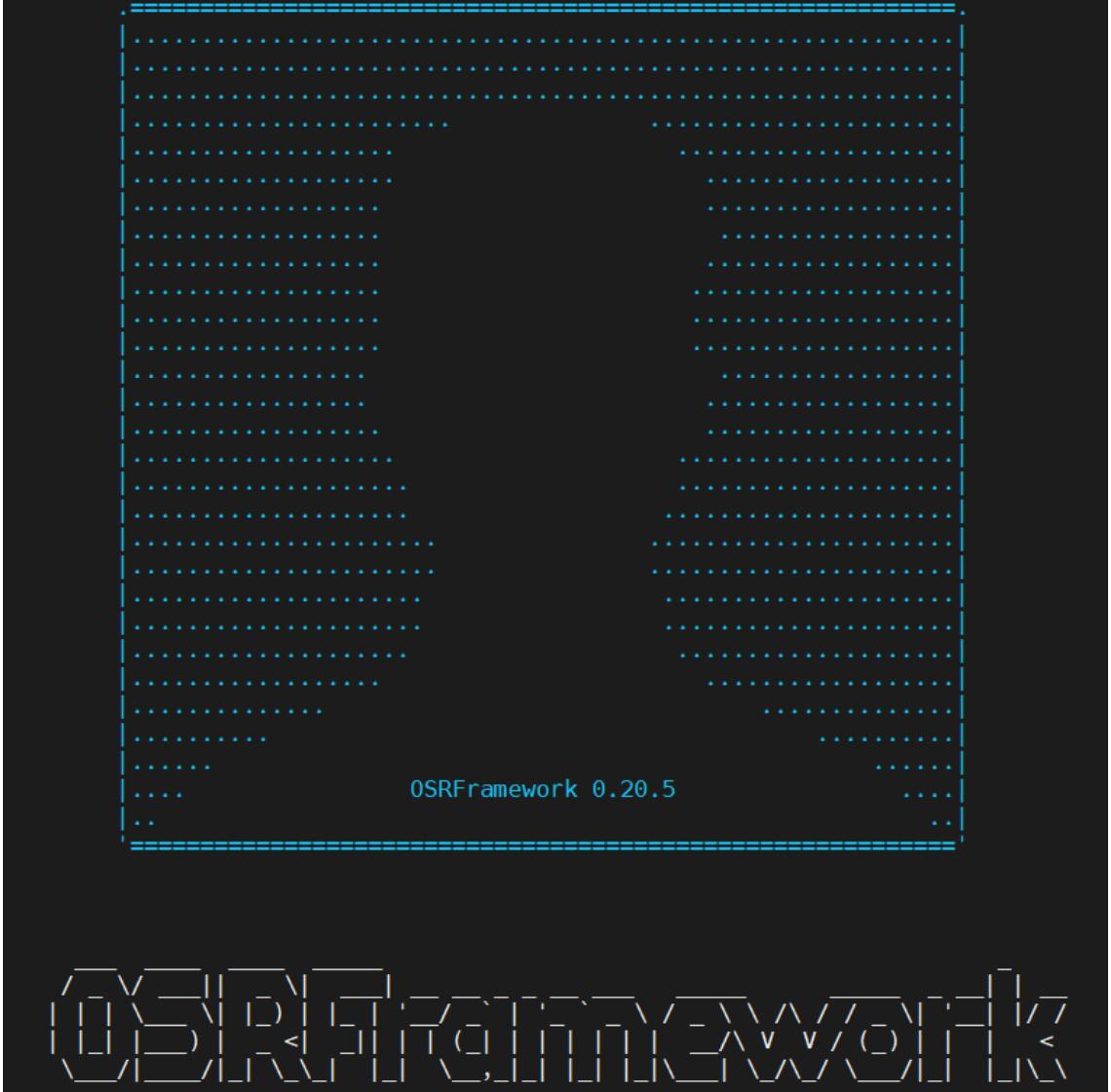


Ilustración 17 OSRFramework Searchfy

```

Coded with ❤ by Yaiza Rubio & Félix Brezo

-- Use 'osrf upgrade --only-check' to check for newer versions in PyPI. --

Searchfy | Copyright (C) Yaiza Rubio & Félix Brezo (i3visio) 2014-2021

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit <https://www.gnu.org/licenses/agpl-3.0.txt>.

2022-04-15 04:40:55.105681      Starting search in different platform(s)... Relax!
Press <Ctrl + C> to stop...

[*] Launching search using the Github module...
[*] Launching search using the Instagram module...
[*] Launching search using the KeyServerUbuntu module...
[*] Launching search using the Github module...
[*] Launching search using the Instagram module...
[*] Launching search using the KeyServerUbuntu module...

2022-04-15 04:41:11.554560      Results obtained:

sheet Name: Objects recovered (2022-4-15_4h41m).
+-----+
| com.i3visio.Platform | com.i3visio.Alias | com.i3visio.Domain | com.i3visio.URI |
+-----+
|           |           |           |           |
|           |           |           |           |
|           |           |           |           |
+-----+
| Github   | chema     | https://github.com/chema | N/A          |
|           | | N/A       | | N/A        |           |
|           |           |           |           |
|           |           |           |           |
| Github   | neo22s    | https://github.com/neo22s | N/A          |
|           | | N/A       | | N/A        |           |
|           |           |           |           |
|           |           |           |           |
| Github   | durbon    | https://github.com/durbon | N/A          |
|           | | N/A       | | N/A        |           |
|           |           |           |           |
+-----+

```

Ilustración 18 OSRFramework Searchfy Resultado

6.3.1.7. OSI.IG

Para el uso de OSI.IG, se debe entrar a la carpeta con nombre “osi.ig” se puede lograr ubicando el path de escritorio y a continuación `cd osi.ig/`, luego para iniciar se hará correr el siguiente comando `python3 main.py -h` para obtener de inicio la ayuda que se proporciona.

```

root@lordmadness:/home/lordmadness/Escritorio/osi.ig# python3 main.py -h
usage: main.py [-h] -u USER [-p]

optional arguments:
  -h, --help            show this help message and exit
  -u USER, --user USER  username of account to scan
  -p, --post             image info of user uploads

```

Ilustración 19 OSI.IG - Ayuda

Datos disponibles: OSI.IG es una herramienta que busca perfiles de Instagram y saca toda la información posible, a continuación, se muestra un ejemplo del uso del código `python3 main.py -u skinnyflakk`

The screenshot shows the output of the OSI.IG tool. At the top, it displays the logo "OSI.IG". Below the logo, it says "Code By : youtube.com/UCnknCgg_3pVXS27ThLpw3xQ". The main output is a JSON-like structure representing a user profile:

```
[+] user info
username : skinnyflakk
user id : 310361533
name : Rels B 🇲🇽
followers : 2829992
following : 769
posts img : 21
posts vid : 4
reels : 2
bio : tickets
external url : https://linktr.ee/relsbtour
private : False
verified : True
profile img : https://tinyurl.com/y67wlrwh
business account : False
joined recently : False
business category : None
category : None
has guides : False

[+] most used tags :
flakkstour2022 : 1
186 : 1

[+] most used mentions :
richboywest : 6
_eladiocarrion : 5
khea.yf : 5
snowthaproduct : 4
mxalemanmx : 4
```

Ilustración 20 OSI.IG - Resultado

6.3.1.8. Twint (Twitter Intelligence Tool)

Para el uso de Twint, solo se debe estar en cualquier path y escribir en comando `twint -h` para así acceder a todas las opciones que ofrece, como se muestra una parte de la ayuda a continuación:

```
root@lordmadness:/home/lordmadness/Escritorio# twint -h
usage: python3 twint [options]

TWINT - An Advanced Twitter Scraping Tool.

optional arguments:
  -h, --help            show this help message and exit
  -u USERNAME, --username USERNAME
                        User's Tweets you want to scrape.
  -s SEARCH, --search SEARCH
                        Search for Tweets containing this word or phrase.
  -g GEO, --geo GEO    Search for geocoded Tweets.
  --near NEAR           Near a specified city.
  --location            Show user's location (Experimental).
  -l LANG, --lang LANG Search for Tweets in a specific language.
  -o OUTPUT, --output OUTPUT
                        Save output to a file.
```

Ilustración 21 Twint - Ayuda

Datos disponibles: Twint es una herramienta que busca información de Twitter que permite analizar los tweets de perfiles de los usuarios, a continuación, se muestra un ejemplo del uso del código `twint -u Master_CIBERSG`, donde regresara los tweets que realizo ese usuario.

```

root@lordmadness:/home/lordmadness/Escritorio# twint -u Master_CIBERSG
1514538199648858112 2022-04-14 04:37:00 -0500 <Master_CIBERSG> ¿Conoces el #talento de nuestros #alumnos? Hoy os presentamos el post de Alejandro Martínez Colombo, alumno de la 7ª edición del #Máster en #Ciberseguridad sobre filitrado por #DNS ¡Es un todo un placer leerlo! https://t.co/NLefOMPnDK https://t.co/3bauw92aeX
151417556020050645 2022-04-13 04:36:00 -0500 <Master_CIBERSG> ¿Quieres saber qué tipos de #Vulnerabilidades existen en #Ciberseguridad? ¿Cómo te afectan si eres una empresa o usuario? ¡No te pierdas el vídeo! https://t.co/4s1iy9l8rS
1513812921062617088 2022-04-12 04:35:00 -0500 <Master_CIBERSG> La #Mentorización de #Chema Alonso ¿Qué es, en qué consiste? Su labor consiste en ayudar a definir los contenidos formativos con sus conocimientos, experiencia, valores y habilidades en el área de #Seguridad Informática ...Descubre más ↗ https://t.co/8YPoPgWR61
1513536930042073093 2022-04-11 10:18:18 -0500 <Master_CIBERSG> ¡Comenzamos con los #Ciberdesayunos! ¿Quieres pasar un ratito por la mañana charlando sobre #Ciberseguridad? No te pierdas el primero, el 21 de abril a las 11:00 con @_JuanjoSalvador. https://t.co/L6MxlfAtPL https://t.co/gaS1aBTkxV
1512361607581470722 2022-04-08 04:28:00 -0500 <Master_CIBERSG> ¡#Sabiasque que con el #Máster en #Fundamentos de #Ciberseguridad tendrás una serie de libros de la Oxford entre otras muchas cosas? ¿A qué esperas? Aprende ciberseguridad desde cero. Comienza el próximo día 12 de abril ¡Te esperamos! https://t.co/WZciOXs9NX https://t.co/EkwmV2VktD
1512345659688554503 2022-04-08 03:24:37 -0500 <Master_CIBERSG> Hoy iniciamos el día con una buena noticia ↗ ¡Comenzamos con los #Ciberdesayunos! ¿Quieres pasar un ratito por la mañana charlando sobre #Ciberseguridad? No te pierdas el primero, el 21 de abril a las 11:00 con @_JuanjoSalvador. https://t.co/L6MxlfAtPL https://t.co/z0YD30jJoC

```

Ilustración 22 Twint - Resultado

6.3.1.9. Metagoofil

Para el uso de Metagoofil, se debe entrar a la carpeta con nombre “metagoofil” se puede lograr ubicando el path de escritorio y a continuación `cd metagoofil/`, luego para iniciar se hará correr el siguiente comando `python3 metagoofil.py -h` para obtener de inicio la ayuda que se proporciona.

```

root@lordmadness:/home/lordmadness/Escritorio/metagoofil# python3 metagoofil.py -h
usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f [SAVE_FILE]] [-i URL_TIMEOUT] [-l SEARCH_MAX] [-n DOWNLOAD_FILE_LIMIT] [-o SAVE_DIRECTORY]
                     [-r NUMBER_OF_THREADS] [-t FILE_TYPES] [-u [USER_AGENT]] [-w]

Metagoofil v1.1.0 - Search Google and download specific file types.

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN             Domain to search.
  -e DELAY              Delay (in seconds) between searches. If it's too small Google may block your IP, too big and your search may take a while. Default: 30.0
  -f [SAVE_FILE]         Save the html links to a file.
                        no -f = Do not save links
                        -f = Save links to html_links-<TIMESTAMP>.txt
                        -f SAVE_FILE = Save links to SAVE_FILE
  -i URL_TIMEOUT        Number of seconds to wait before timeout for unreachable/stale pages. Default: 15
  -l SEARCH_MAX          Maximum results to search. Default: 100
  -n DOWNLOAD_FILE_LIMIT
                        Maximum number of files to download per filetype. Default: 100
  -o SAVE_DIRECTORY      Directory to save downloaded files. Default is current working directory, "."
  -r NUMBER_OF_THREADS   Number of downloader threads. Default: 8
  -t FILE_TYPES          file_types to download (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx). To search all 17,576 three-letter file extensions, type "ALL"
  -u [USER_AGENT]         User-Agent for file retrieval against -d domain.
                        no -u = "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
                        -u = Randomize User-Agent
                        -u "My custom user agent 2.0" = Your customized User-Agent
  -w                     Download the files, instead of just viewing search results.

```

Ilustración 23 Metagoofil - Ayuda

Datos disponibles: Metagoofil es una herramienta que extrae metadatos de documentos públicos, como ingreso tiene un dominio.

A continuación, se realiza un ejemplo con el siguiente comando `python3 metagoofil.py -d ucam.edu -t pdf` que da como resultado los metadatos en formato .pdf del dominio indicado

```
root@lordmadness:/home/lordmadness/Escritorio/metagoofil# python3 metagoofil.py -d ucam.edu -t pdf
[*] Searching for 100 .pdf files and waiting 30.0 seconds between searches
[*] Results: 100 .pdf files found
http://go.ucam.edu/ventaja-ubereats
https://campus.ucam.edu/web/faqs.pdf
https://ccd.ucam.edu/index.php/revista/article/download/184/174
https://ccd.ucam.edu/index.php/revista/article/download/171/162
https://www.ucam.edu/sites/default/files/estudios/postgrados/docs/alfredo_rodriguez_gomez.pdf
https://ccd.ucam.edu/index.php/revista/article/download/178/169/351
https://ccd.ucam.edu/index.php/revista/article/download/93/86/185
https://ccd.ucam.edu/index.php/revista/article/download/92/85/183
https://ccd.ucam.edu/index.php/revista/article/download/95/88/189
https://ccd.ucam.edu/index.php/revista/article/download/90/84/181
https://api0.ucam.edu/citrix/Xenapp/Resolucion_problemasCA3.pdf
https://www.ucam.edu/sites/default/files/estudios/postgrados/docs/pena_vela_jose_luis.pdf
https://www.ucam.edu/sites/default/files/estudios/postgrados/docs/arturo_merayo.pdf
https://www.ucam.edu/sites/default/files/estudios/postgrados/docs/hernandez_martinez_salvador.pdf
https://www.ucam.edu/sites/default/files/documentos/curriculum-profesor/arnaiz_marina_alejo-cv.pdf
https://www.ucam.edu/sites/default/files/estudios/postgrados/docs/carmen_campos.pdf
https://www.ucam.edu/sites/default/files/estudios/postgrados/docs/jose_rocamora_tora.pdf
http://repositorio.ucam.edu/bitstream/handle/10952/957/Tesis.pdf?sequence=1&isAllowed=y
http://repositorio.ucam.edu/bitstream/handle/10952/703/Tesis.pdf?sequence=1&isAllowed=y
http://repositorio.ucam.edu/bitstream/handle/10952/167/pag94_101.pdf?sequence=1&isAllowed=y
https://lavoz.ucam.edu/documentos/lavoz-marzo-2021.pdf
http://repositorio.ucam.edu/bitstream/handle/10952/996/Tesis.pdf?sequence=1&isAllowed=y
http://repositorio.ucam.edu/bitstream/handle/10952/1675/Tesis.pdf?sequence=1&isAllowed=y
https://lavoz.ucam.edu/documentos/lavoz-junio-2019.pdf
https://lavoz.ucam.edu/documentos/lavoz-noviembre-2016.pdf
https://lavoz.ucam.edu/documentos/lavoz-noviembre-2015.pdf
https://lavoz.ucam.edu/documentos/lavoz-marzo-2018.pdf
```

Ilustración 24 Metagoofil - Resultado

6.3.1.10. Sublist3r

Para el uso de Sublist3r, se debe entrar a la carpeta con nombre “Sublist3r” se puede lograr ubicando el path de escritorio y a continuación `cd Sublist3r/`, luego para iniciar se hará correr el siguiente comando `python3 sublist3r.py` y para obtener ayuda `python3 sublist3r.py -h`

Ilustración 25 Sublist3r

```

root@lordmadness:/home/lordmadness/Escritorio/Sublist3r# python3 sublist3r.py -h
usage: sublist3r.py [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES] [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python sublist3r.py -d google.com

```

Ilustración 26 Sublist3r - Ayuda

Datos disponibles: Sublist3r es una herramienta que nos permite enumerar subdominios de un sitio web usando OSINT.

A continuación, se muestra un ejemplo de su uso con el comando `python3 sublist3r.py -d elevenpaths.com -p 80,443`

```

root@lordmadness:/home/lordmadness/Escritorio/Sublist3r# python3 sublist3r.py -d elevenpaths.com -p 80,443
[!] Error: Virustotal probably now is blocking our requests

[!] Total Unique Subdomains Found: 18
[-] Start port scan now for the following ports: 80,443
latch.elevenpaths.com - Found open ports: 80, 443
autodiscover.elevenpaths.com - Found open ports: 80
www.elevenpaths.com - Found open ports: 80, 443
sandals.elevenpaths.com - Found open ports: 80, 443
community.elevenpaths.com - Found open ports: 80, 443
focamarket.elevenpaths.com - Found open ports: 80, 443
latchcontest.elevenpaths.com - Found open ports: 80, 443
partners.elevenpaths.com - Found open ports: 80, 443
securityinnovationday.elevenpaths.com - Found open ports: 80, 443
metashieldwebservices.elevenpaths.com - Found open ports: 80, 443
metashieldanalyzer.elevenpaths.com - Found open ports: 80, 443

```

Ilustración 27 Sublist3r – Resultado

6.3.1.11. Katana-ds

Para el uso de Katana-ds, se debe entrar a la carpeta con nombre “Katana” se puede lograr ubicando el path de escritorio y a continuación `cd Katana/`, luego para iniciar se hará correr el siguiente `python3 kds.py -h` el cual mostrara la ayuda que se obtiene de Katana.

```
root@lordmadness:/home/lordmadness/Escritorio/Katana# python3 kds.py -h

          |
          T
  |-----|
  |G|o|o|g|l|e|_|j|_0|-----|
  |R|                           |
  |                               / V1.5.3

Katana Dork Scanner (Katana-DS) coded by adnane-X-tebbaa
please use -h to see help

usage: katana-ds.py [-h] [-g] [-s] [-t] [-p]

optional arguments:
  -h, --help    show this help message and exit
  -g, --google  google mode
  -s, --scada   scada mode
  -t, --tor     Tor mode
  -p, --proxy   Proxy mode
```

Ilustración 28 Katana - Ayuda

Datos disponibles: Katana-ds es una herramienta que nos permite automatizar Google Hacking / Dorking.

Se tiene estos modos de búsqueda:

-g: para el modo Google

-s: para el modo scada

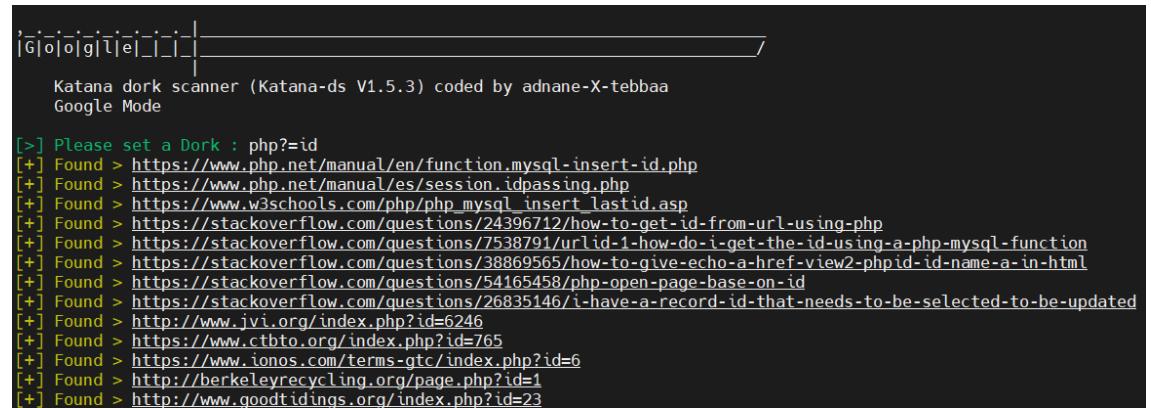
-t: para modo tor

-p: para modo proxy

Para su uso solo se deberá escoger el modo es en comando poner `python3 kds.py "modo escogido"`

A continuación, se muestra un ejemplo de su uso con el comando `python3`

```
kds.py -g
```



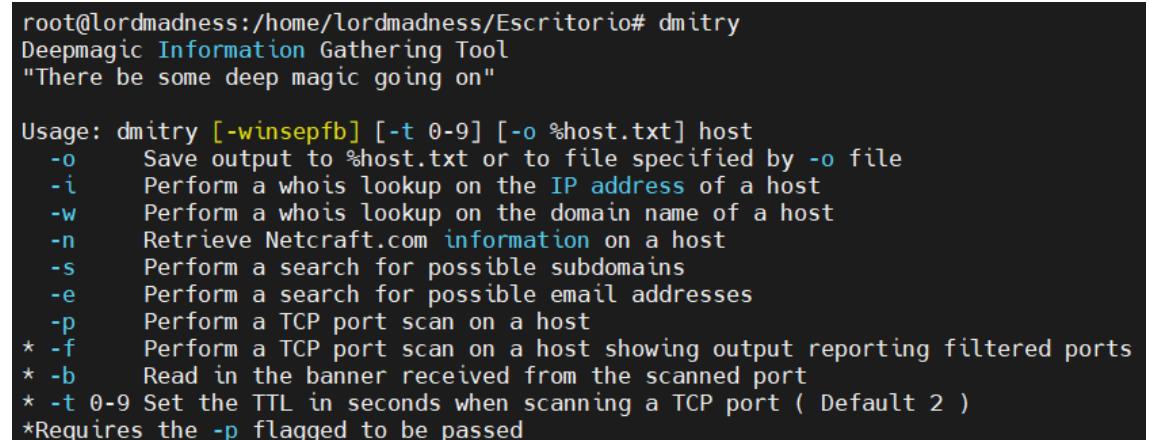
Katana dork scanner (Katana-ds V1.5.3) coded by adnane-X-tebbaa
Google Mode

[>] Please set a Dork : php?id
[+] Found > <https://www.php.net/manual/en/function.mysql-insert-id.php>
[+] Found > <https://www.php.net/manual/es/session.idpassing.php>
[+] Found > https://www.w3schools.com/php/php_mysql_insert_lastid.asp
[+] Found > <https://stackoverflow.com/questions/24396712/how-to-get-id-from-url-using-php>
[+] Found > <https://stackoverflow.com/questions/7538791/urlid-1-how-do-i-get-the-id-using-a-php-mysql-function>
[+] Found > <https://stackoverflow.com/questions/38869565/how-to-give-echo-a-href-view2-phpid=id-name-a-in-html>
[+] Found > <https://stackoverflow.com/questions/54165458/php-open-page-base-on-id>
[+] Found > <https://stackoverflow.com/questions/26835146/i-have-a-record-id-that-needs-to-be-selected-to-be-updated>
[+] Found > <http://www.jvi.org/index.php?id=6246>
[+] Found > <https://www.ctbto.org/index.php?id=765>
[+] Found > <https://www.ionos.com/terms-gtc/index.php?id=6>
[+] Found > <http://berkeleyrecycling.org/page.php?id=1>
[+] Found > <http://www.goodtidings.org/index.php?id=23>

Ilustración 29 Katana - Resultado

6.3.1.12. DMitry

Para el uso de DMitry, solo se debe estar en cualquier path y escribir en comando `dmitry` para así acceder a todas las opciones que ofrece, como se muestra una parte de la ayuda a continuación:



```
root@lordmadness:/home/lordmadness/Escritorio# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o      Save output to %host.txt or to file specified by -o file
  -i      Perform a whois lookup on the IP address of a host
  -w      Perform a whois lookup on the domain name of a host
  -n      Retrieve Netcraft.com information on a host
  -s      Perform a search for possible subdomains
  -e      Perform a search for possible email addresses
  -p      Perform a TCP port scan on a host
  * -f    Perform a TCP port scan on a host showing output reporting filtered ports
  * -b    Read in the banner received from the scanned port
  * -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

Ilustración 30 DMitry - Ayuda

Datos disponibles: DMitry es una herramienta que está enfocada en obtener la mayor cantidad de información de un host, tiene la capacidad de recolectar información de subdominios, direcciones de correo, tiempo de

funcionamiento, hacer un escaneo de puertos TCP, consultas Whois y otras opciones más.

A continuación, se muestra un ejemplo de uso usando el comando `dmitry -winsepf mountainplanet.com`

```
root@lordmadness:/home/lordmadness/Escritorio# dmitry -winsepf mountainplanet.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:138.201.49.134
HostName:mountainplanet.com

Gathered Inet-whois information for 138.201.49.134
-----
inetnum:      138.201.49.128 - 138.201.49.191
netname:      HETZNER-fsn1-dc8
descr:        Hetzner Online GmbH
descr:        Datacenter fsn1-dc8
country:      DE
admin-c:      HOAC1-RIPE
tech-c:       HOAC1-RIPE
status:       LEGACY
remarks:      INFRA-AW
mnt-by:       HOS-GUN
mnt-lower:    HOS-GUN
mnt-routes:   HOS-GUN
created:     2018-03-15T14:19:50Z
last-modified: 2018-03-15T14:19:50Z
source:       RIPE
```

Ilustración 31 DMitry - Resultado

6.3.1.13. Ghunt

Para el uso de Ghunt, se debe entrar a la carpeta con nombre “ghunt” se puede lograr ubicando el path de escritorio y a continuación `cd ghunt/`, luego para iniciar se hará correr el siguiente `python3 ghunt.py` el cual mostrara la ayuda que se obtiene de Ghunt.

Con los modulos que se muestran a continuación

```
root@lordmadness:/home/lordmadness/Escritorio/ghunt# python3 ghunt.py
Please choose a module.

Available modules :
- email
- doc
- gaia
- youtube
```

Ilustración 32 Ghunt - Ayuda

Datos disponibles: Ghunt es una herramienta que permite a los usuarios extraer información de cualquier cuenta de Google mediante un correo electrónico.

A continuación el uso con el comando de ejemplo `python3 ghunt.py youtube https://www.youtube.com/channel/UCfEE7VQC9xLMzNssS7y3APA`

```
.d8888b. 888 888 888
d88P Y88b 888 888 888
888 888 888 888
888 8888888888 888 888 88888b. 888888
888 8888 888 888 888 888 "88b 888
888 888 888 888 888 888 888 888 888
Y88b d88P 888 888 Y88b 888 888 888 Y88b.
"Y8888P88 888 888 "Y88888 888 888 "Y888

► [Youtube channel]
[+] Channel name : Clara Luciani
[+] Snapshot : 04/07/2019
[+] GaiaID => 101027053727652826750
[+] Email on profile : available !
[+] Country : France

Description : Nouvel album "Coeur" maintenant disponible ❤
https://claraluciani.lnk.to/CoeurID
Clara Luciani en concert en 2021 : https://tix.to/ClaraTour21YD
S'abonner à la chaîne Youtube de Clara : https://lnk.to/ClaraYTAbonnementYD
Instagram : https://www.instagram.com/jesuisclaraluciani
Facebook : https://www.facebook.com/claralucianimusique
Actus, shop en ligne : http://www.claraluciani.com
Total views : 113,411,961
Joined date : Dec 24, 2013

[+] Primary links (5 found)
- "Cœur" => https://claraluciani.lnk.to/Coeur
- Dates de concerts => https://tix.to/ClaraTour21YD
- Instagram => https://www.instagram.com/jesuisclaraluciani
- Facebook => https://www.facebook.com/claralucianimusique
- Shop => https://claraluciani.store/
```

Ilustración 33 Ghunt - Resultado

6.3.1.14. Infoga

Para el uso de Infoga, se debe entrar a la carpeta con nombre “Infoga” se puede lograr ubicando el path de escritorio y a continuación `cd Infoga/`, luego para iniciar se hará correr el siguiente `python3 infoga.py` el cual mostrara la ayuda que se obtiene de Infoga.

```
root@lordmadness:/home/lordmadness/Escritorio/Infoga# python3 infoga.py
=====
-[ Infoga - Email OSINT
-[ Momo (m4ll0k) Outaadi
-[ https://github.com/m4ll0k

=====
Usage: infoga.py [OPTIONS]

      -d --domain    Target URL/Name
      -s --source     Source data, default "all":
                      all   Use all search engine
                      google Use google search engine
                      bing  Use bing search engine
                      yahoo Use yahoo search engine
                      ask   Use ask search engine
                      baidu Use baidu search engine
                      dogpile Use dogpile search engine
                      exalead Use exalead search engine
                      pgp   Use pgp search engine

      -b --breach    Check if email breached
      -i --info      Get email informations
      -r --report    Simple file text report
      -v --verbose   Verbosity level (1,2 or 3)
      -H --help      Show this help and exit

Example:
infoga.py --domain site.gov -v 3
infoga.py --info admin@site.gov -v 3
infoga.py --domain site.gov --source pgp --breach -v 1
infoga.py --domain site.gov --source google --breach --report site.gov.txt -v 3
```

Ilustración 34 Infoga - Ayuda

Datos disponibles: Infoga es una herramienta que recopila información de cuentas de correo electrónico y verifica mediante la API haveibeenpwned.com si los correos electrónicos han sido filtrados.

A continuación, se muestra un ejemplo de uso usando el comando `python3 infoga.py -d ucam.edu --source all`

```
root@lordmadness:/home/lordmadness/Escritorio/Infoga# python3 infoga.py -d ucam.edu --source all
--=[ Infoga - Email OSINT
--=[ Momo (m4ll0k) Outaadi
--=[ https://github.com/m4ll0k

[*] Searching "ucam.edu" in Ask...
[i] Found 0 emails in Ask
[*] Searching "ucam.edu" in Baidu...
[i] Found 5 emails in Baidu
[*] Searching "ucam.edu" in Bing...
[i] Found 0 emails in Bing
[*] Searching "ucam.edu" in DogPile...
[i] Found 0 emails in Dogpile
[*] Searching "ucam.edu" in Exalead...
[*] Searching "ucam.edu" in Google...
[i] Found 24 emails in Google
[*] Searching "ucam.edu" in PGP...
[i] Found 0 emails in PGP
[*] Searching "ucam.edu" in Yahoo...
[i] Found 1 emails in Yahoo
[+] Email: -campuscartagena@ucam.edu ()
[+] Email: pweitichan@ucam.edu ()
[+] Email: admissions@ucam.edu ()
[+] Email: info-asia@ucam.edu ()
[+] Email: zguanghao@ucam.edu ()
[+] Email: info@ucam.edu ()
[+] Email: fisiologia@ucam.edu ()
[+] Email: dpd@ucam.edu ()
[+] Email: japellicer@ucam.edu ()
[+] Email: campuscartagena@ucam.edu ()
[+] Email: presidencia@ucam.edu ()
[+] Email: ucam dental@ucam.edu ()
[+] Email: afrutos@pas.ucam.edu ()
```

Ilustración 35 Infoga - Resultado

6.3.1.15. H8mail

Para el uso de h8mail, solo se debe estar en cualquier path y escribir en comando `h8mail -h` para así acceder a todas las opciones que ofrece, como se muestra una parte de la ayuda a continuación:

Ilustración 36 H8mail - Ayuda

Datos disponibles: H8mail es una herramienta que busca por api en varias aplicaciones webs que contienen variedad de información, los datos de entrada pueden ser correo electrónico, usuarios, ip o url.

A continuación, se muestra un ejemplo de uso usando el comando `h8mail -t example@gmail.com -c h8mail_config.ini`

Ilustración 37 H8mail - Resultado

6.3.1.16. Dnsmap

Para el uso de dnsmap, solo se debe estar en cualquier path y escribir en comando `dnsmap` para así acceder a todas las opciones que ofrece, como se muestra una parte de la ayuda a continuación:

```
root@lordmadness:/home/lordmadness/Escritorio# dnsmap
dnsmap 0.35 - DNS Network Mapper

usage: dnsmap <target-domain> [options]

options:
-w <wordlist-file>
-r <regular-results-file>
-c <csv-results-file>
-d <delay-millisecs>
-i <ips-to-ignore> (useful if you're obtaining false positives)

e.g.:
dnsmap example.com
dnsmap example.com -w yourwordlist.txt -r /tmp/domainbf_results.txt
dnsmap example.com -r /tmp/ -d 3000
dnsmap example.com -r ./domainbf_results.txt
```

Ilustración 38 Dnsmap - Ayuda

Datos disponibles: Dnsmap es una herramienta utilizada para recopilar información de subdominios para un host de destino.

El dato de entrada será un dominio, como se muestra en el siguiente ejemplo de uso `dnsmap elevenpaths.com`

```
root@lordmadness:/home/lordmadness/Escritorio# dnsmap elevenpaths.com
dnsmap 0.35 - DNS Network Mapper

[+] searching (sub)domains for elevenpaths.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

help.elevenpaths.com
IP address #1: 104.16.53.111
IP address #2: 104.16.51.111
```

Ilustración 39 Dnsmap - Resultado

6.3.1.17. SocialPwned

Para el uso de SocialPwned, se debe entrar a la carpeta con nombre “SocialPwned” se puede lograr ubicando el path de escritorio y a continuación `cd SocialPwned/`, luego para iniciar se hará correr el siguiente `python3 socialpwned.py` el cual mostrara la ayuda que se obtiene de SocialPwned.

Ilustración 40 SocialPwned - Ayuda

Datos disponibles: SocialPwned es una herramienta que recolecta datos de cuatro posibles modulos: Instagram, Twitter, LinkedIn y PwnBD.

Su propósito fundamental es facilitar la búsqueda de objetivos vulnerables.

Lo primero que se debe hacer es crear un archivo .json en este caso lo llamaremos `configuracion.json`, con las credenciales que se usaran para cada red social con el formato se muestra a continuación.

```
{
    "instagram": {
        "username": "username",
        "password": "password"
    },
    "linkedin": {
        "email": "email",
        "password": "password"
    }
}
```

Ilustración 41 SocialPwned – Configuración

Luego se usará el archivo creado como se muestra en el siguiente ejemplo

```
python3 socialpwned.py --credentials configuracion.json --linkedin --search-companies "Target"
```

```
#####
Author: @MrTuxx
DISCLAIMER: This is only for testing purposes and can only be used where strict consent has been given.

[+] Successful login to LinkedIn!

[-] Searching companies... :)
[+] Name: Target company ID: 1512 Number of employees: 10,001+ employees
[+] Name: Target Recruitment & HR Solutions company ID: 1445528 Number of employees: 51-200 employees
[+] Name: Target Group company ID: 31624 Number of employees: 1,001-5,000 employees
[+] Name: Target Australia company ID: 1092686 Number of employees: 10,001+ employees
[+] Name: Target Engineering Construction Co LLC company ID: 435462 Number of employees: 5,001-10,000 employees
[+] Name: Target Corporation (Electronics Manufacturing Services) company ID: 2608152 Number of employees: 11-50 employees
[+] Name: Target Distributing company ID: 1454319 Number of employees: 51-200 employees
[+] Name: Target River company ID: 7950907 Number of employees: 11-50 employees
[+] Name: Target Hospitality company ID: 28995138 Number of employees: 201-500 employees
[+] Name: Target Test Prep company ID: 1054372 Number of employees: 11-50 employees
[+] Name: Target Logistics Management LLC company ID: 1075542 Number of employees: 201-500 employees
[+] Name: Luxottica company ID: 1614240 Number of employees: 10,001+ employees
[+] Name: Target Integration company ID: 343800 Number of employees: 51-200 employees
[+] Name: Target Specialty Products company ID: 1465287 Number of employees: 201-500 employees
[+] Name: Target Optical company ID: 3480281 Number of employees: 5,001-10,000 employees
[+] Name: Target RWE Health Evidence Solutions company ID: 15161585 Number of employees: 51-200 employees
[+] Name: Target Distribution Ctr company ID: 5491342 Number of employees: 11-50 employees
[+] Name: Consensus, a Target company company ID: 2746891 Number of employees: 51-200 employees
[+] Name: Target Data company ID: 1129587 Number of employees: 11-50 employees
[+] Name: Target Human Resources Solutions company ID: 2533827 Number of employees: 201-500 employees
[+] Name: Target Marketing Digital company ID: 2987047 Number of employees: 11-50 employees
[+] Name: Target Media Partners company ID: 77495 Number of employees: 501-1,000 employees
[+] Name: Target Global company ID: 3358953 Number of employees: 51-200 employees
[+] Name: Target HR company ID: 233077 Number of employees: 11-50 employees
[+] Name: TARGET DDI company ID: 1008681 Number of employees: 51-200 employees
[+] Name: Target Engineering Group company ID: 6071796 Number of employees: 51-200 employees
[+] Name: Target Sistemas company ID: 513158 Number of employees: 51-200 employees
[+] Name: Drug Target Review company ID: 5220086 Number of employees: 51-200 employees
```

Ilustración 42 SocialPwned - Resultado

6.3.1.18. Profil3r

Para el uso de Profil3r, se debe entrar a la carpeta con nombre “Profil3r” se puede lograr ubicando el path de escritorio y a continuación `cd Profil3r/`, luego para iniciar se hará correr el siguiente `python3 profil3r.py` el cual mostrara la ayuda que se obtiene de Profil3r.

```
root@lordmadness:/home/lordmadness/Escritorio/Profil3r# python3 profil3r.py
[.]>[-]>/[.]-[<]>[<]>
[<]>[<]>/[<]>
v1.0.4
You can buy me a coffee at : https://www.buymeacoffee.com/givocefo
```

Ilustración 43 Profil3r - Ayuda

Datos disponibles: Profil3r es una herramienta que puede Encontrar cuentas en redes sociales, dominios y correos electrónicos.

Los datos de entrada son nombres de usuario, nombres personales o nombres de usuarios de correos electrónicos, como se muestra en el siguiente ejemplo a continuación `python3 profil3r.py -p lordmadness`.

```
root@lordmadness:/home/lordmadness/Escritorio/Profil3r# python3 profil3r.py -p lordmadness
[. ]>(. )<(. )>(. )<(. )>
[. ]>(. )<(. )>(. )<(. )>

v1.0.4

You can buy me a coffee at : https://www.buymeacoffee.com/givocefo

└─ EMAIL ✓
  └─ -p@gmail.com [SAFE]
    └─ lordmadness@gmail.com [SAFE]
    └─ plordmadness@gmail.com [SAFE]
    └─ lordmadness-p@gmail.com [SAFE]
    └─ p.lordmadness@gmail.com [SAFE]
    └─ lordmadness.-p@gmail.com [SAFE]
    └─ -p@yahoo.com [SAFE]
    └─ lordmadness@yahoo.com [SAFE]
    └─ plordmadness@yahoo.com [SAFE]
    └─ lordmadness-p@yahoo.com [SAFE]
    └─ p.lordmadness@yahoo.com [SAFE]
    └─ lordmadness.-p@yahoo.com [SAFE]
    └─ -p@hotmail.com [SAFE]
    └─ lordmadness@hotmail.com [SAFE]
    └─ plordmadness@hotmail.com [SAFE]
    └─ lordmadness-p@hotmail.com [SAFE]
    └─ p.lordmadness@hotmail.com [SAFE]
    └─ lordmadness.-p@hotmail.com [SAFE]
```

Ilustración 44 Profil3r - Resultados

6.3.1.19. FisherMan

Para el uso de FisherMan, se debe entrar a la carpeta con nombre “FisherMan” se puede lograr ubicando el path de escritorio y a continuación `cd FisherMan/`, luego para iniciar se hará correr el siguiente `python3 fisherman.py` el cual mostrara la ayuda que se obtiene de FisherMan y para obtener ayuda el comando `python3 fisherman.py --help`

Ilustración 45 FisherMan

Datos disponibles: Profil3r es una herramienta que busca perfiles de usuarios de Facebook.

Donde su uso es del siguiente modo:

```
python3 fisherman.py --username user user.name user2.name2
```

El nombre de usuario lo encontramos en el perfil público:

<https://www.facebook.com/user.name>

También es posible cargar múltiples nombres de usuario desde un archivo .txt, puede ser útil para un ataque de fuerza bruta:

```
python3 fisherman.py --use-txt fichero.txt
```

Puedes enviar si lo deseas la salida a un .txt también usando:

```
python3 fisheman.py --username name --file-output
```

6.3.2. Herramientas web

Estas herramientas están en el navegador Firefox ya agregadas como marcadores.

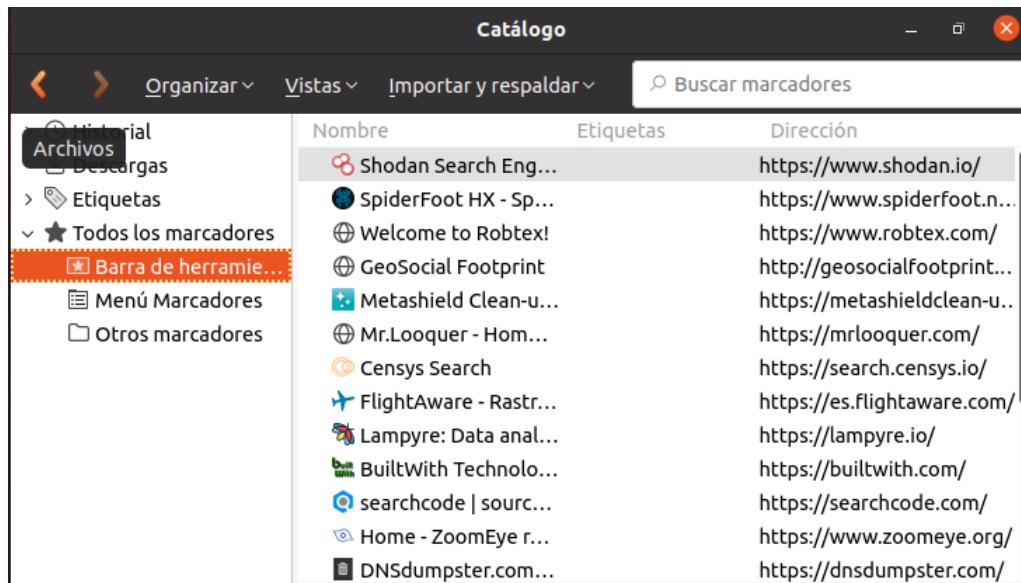


Ilustración 46 Marcadores en Firefox

6.3.2.1. Shodan

Shodan es un motor de búsqueda que tiene como principal objetivo ubicar y descubrir todos los dispositivos posibles conectados a internet (todo tipo de dispositivos), solo es necesario acceder a la web y empezar a realizar búsquedas. (<https://www.shodan.io/>)

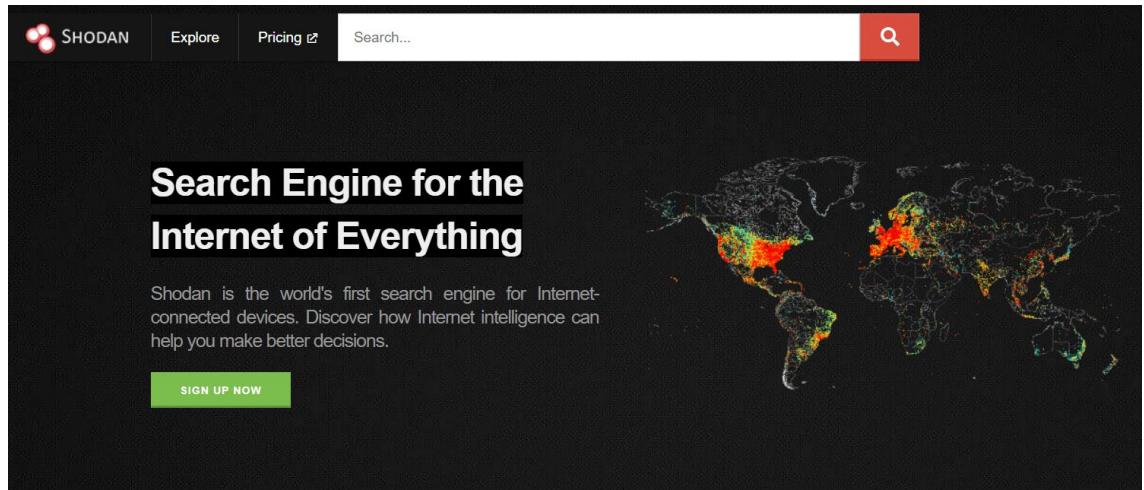


Ilustración 47 Shodan

Como, por ejemplo, se busca la organización “Interbank” y se encuentran muchas conexiones.

| TOP COUNTRIES | COUNT |
|--------------------|-------|
| Azerbaijan | 2 |
| United States | 2 |
| Hong Kong | 1 |
| Netherlands | 1 |
| Russian Federation | 1 |

| TOP PORTS | COUNT |
|-----------|-------|
| 443 | 2 |
| 3389 | 2 |
| 5984 | 2 |
| 8880 | 1 |

| TOP ORGANIZATIONS | COUNT |
|-------------------|-------|
| rabitabank.com | 2 |
| Caspel LLC | 2 |

Ilustración 48 Shodan - Interbank Resultado

6.3.2.2. SpiderFoot HX

SpiderFoot HX es un escaner de multitud de fuentes, puede buscar dominios, usuarios, correos, ASNs, personas, Bitcoin address, subnets, teléfonos, hostnames e IPs. (<https://www.spiderfoot.net/>)



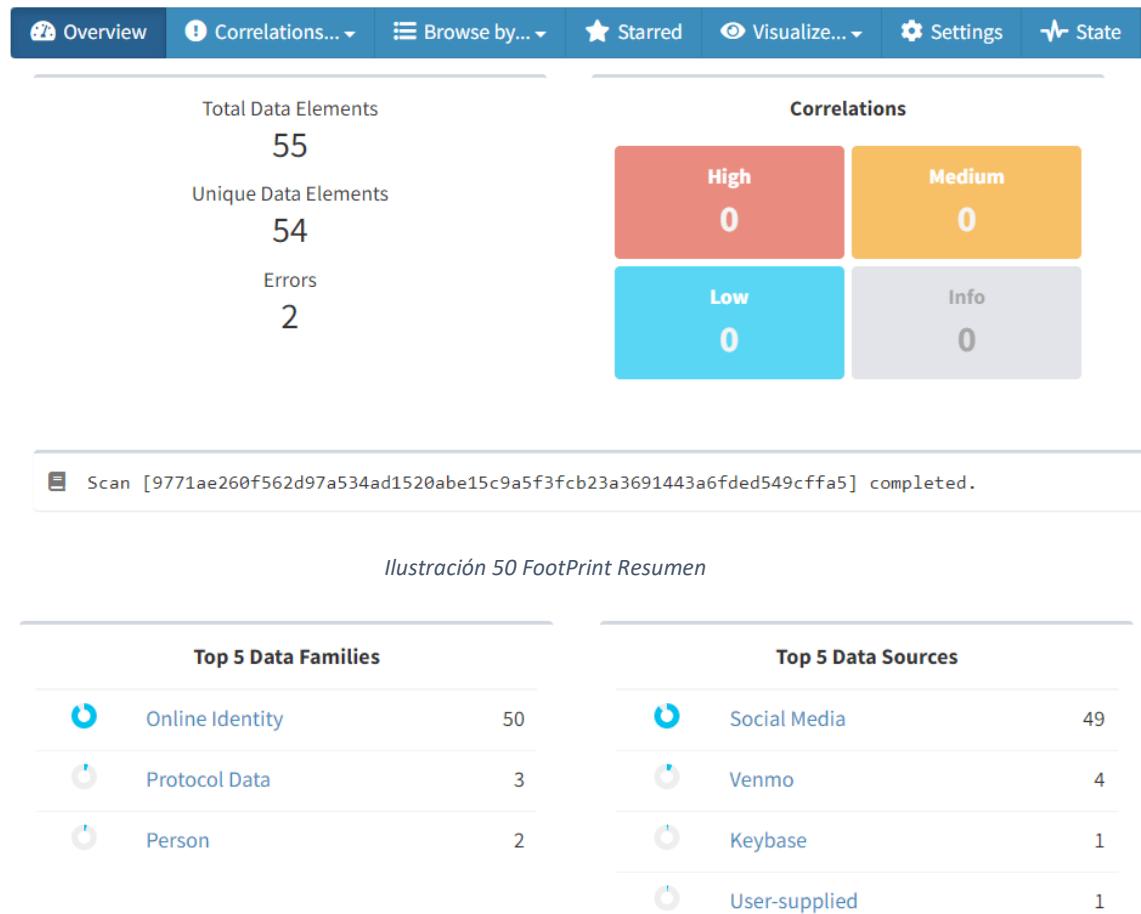
Para poder empezar a escanear es necesario crear una cuenta con un correo luego para realizar un escaneo es bastante intuitivo como se muestra a continuación.

En este caso se buscó un username

A screenshot of the "New Scan" page in SpiderFoot HX. The page has a light gray background with several sections. At the top, there is a header "New Scan". Below it is a section titled "Scan Name & Targets" with a sub-section "Test" containing the text "lordmadness". There are also "Help", "Import", and "Iteration" buttons. Further down are sections for "Modules" (with a warning icon) and "Options". At the bottom are buttons for "Run Scan Now", "Save as Scan Profile...", and "Apply Scan Profile...".

Ilustración 49 SpiderFoot HX – Username

A continuación, se verán los resultados del escaneo.



6.3.2.3. Robtex

Robtex es un buscador que da información relacionada a la búsqueda de Dominios (Hostnames, IP, Numero AS, Route).

Es necesario entrar a la web y realizar las consultas requeridas. (<https://www.robtex.com/>).

Welcome to Robtex!

hostname, ipnumber, route or AS-number

What is Robtex used for?

Robtex is used for various kinds of research of IP numbers, Domain names, etc

Are you a normal IT guy doing data forensics, investigating competitors, tracking spammers or hackers or a virus, or just curious? No matter what, this should be the first place to go

What does Robtex do?

Robtex uses various sources to gather public information about IP numbers, domain names, host names, Autonomous systems, routes etc. It then indexes the data in a big database and We aim to make the fastest and most comprehensive free DNS lookup tool on the Internet.

Our database now contains billions of documents of internet data collected over more than a decade.

Ilustración 52 Robtex

A continuación, se muestra un ejemplo.

The screenshot shows the Robtex search interface. At the top, there is a green header bar with the text "ibaiscanbit.com" and "Robtex >> D". Below the header is a search bar containing the text "ibaiscanbit.com". Underneath the search bar is a horizontal menu bar with several buttons: ANALYSIS, QUICK INFO, REVERSE (NEW!), RECORDS, SEO, WOT, ALEXA, THREATMINER, SHARED, and GRAPH. The "WHOIS" button is highlighted with a green border. To the right of the menu bar, there are three sections: "DNSBL" and "GRAPH(oid)".

Ilustración 53 Robtex - Resultado

Donde cada apartado tiene información interesante en cuanto al dominio.

6.3.2.4. Geosocial Footprint

Geosocial Footprint, se trata de una página web que nos permite rastrear la “huella” que todo usuario deja tras de sí al utilizar redes sociales.

(<http://geosocialfootprint.com/#>)

Para los usuarios de Twitter.com, esta huella se crea a partir de tweets habilitados para GPS.

rmapalacios Retrieve Tweets Download Tweets Clear Tweets Toggle HeatMap Give Feedback

Alerts

Areas of concern:

Risk

Retrieve your tweets and we'll analyze the results and calculate your Geosocial risk:

Suggestions

After you've submitted your twitter username, we'll make suggestions on how to cut down on your personal Geosocial footprint:

 Tweet



Ilustración 54 GeosocialFootprint

También nos permite tratar de ocultar nuestra ubicación o identidad.

6.3.2.5. Metashield Clean-up Online

Se trata de una herramienta que nos ayuda con la obtención de metadatos

Analyze your files with Metashield Clean-up Online.

To analyze the metadata in a file, choose the file below and click on "Analyze". Once you accept the [Terms and Conditions of Use for Metashield Clean-up Online service](#) a screen will appear with the summary of metadata found.

No file selected [Select](#) [Analyze](#)

Analysis and cleaning of metadata without complications.
Extensions

| | |
|---|--|
| Open Office .odt .ods .odg .odp .sxw .odf .ott .oth .odm .otg .otp .ots | Image .jpg .jpeg .raw .png .tif .tiff .svg .svgz .cr2 .crw |
| Microsoft .docx .doc .pptx .ppt .ppsx .pps .xlsx .xls .xlsm .xlt .xslb .tmp .xar .asd .wbk .xlk .xlt .wpd | Audio/Video .mp3 .avi .mp4 |
| iWorks⁽¹⁾ .pages .key .numbers | Compressed⁽²⁾ .zip .tar |
| | Others .pdf .rtf .wnry .wry .indd .rdp .ica |

Ilustración 55 Metashield Clean-up Online

Para utilizar esta herramienta simplemente se debe abrir la web (<https://metashieldclean-up.elevenpaths.com/#>), subir el archivo que se quiera analizar y presionar el botón “Analize” y esperar los metadatos de ese archivo, obteniendo resultados como se muestran a continuación.

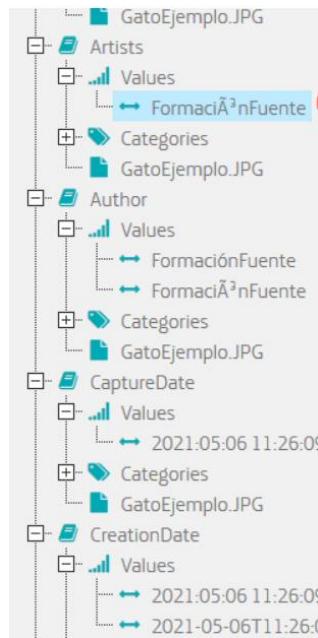


Ilustración 56 MetashieldClean-up - Resultado

6.3.2.6. Mr Looquer

Se trata de un metabuscador parecido a Shodan, en el cual también se puede ingresar dominios, IPs o rango de IPs también se pueden utilizar operadores booleanos dentro de las búsquedas.

Para utilizar esta herramienta simplemente se debe abrir la web (<https://mrlooquer.com/>) y crear una cuenta.



Ilustración 57 Mr. Looquer

Se puede observar el dashboard intuitivo donde se podrá realizar las consultas requeridas.

6.3.2.7. Censys

Censys al igual que los anteriores metabuscadores también se puede ingresar dominios, IPs o rango de IPs, certificados, hosts, también se pueden utilizar operadores booleanos dentro de las búsquedas.

Para poder usar el metabuscador solo es necesario ingresar a la web (<https://search.censys.io/>) y empezar a realizar las búsquedas requeridas.

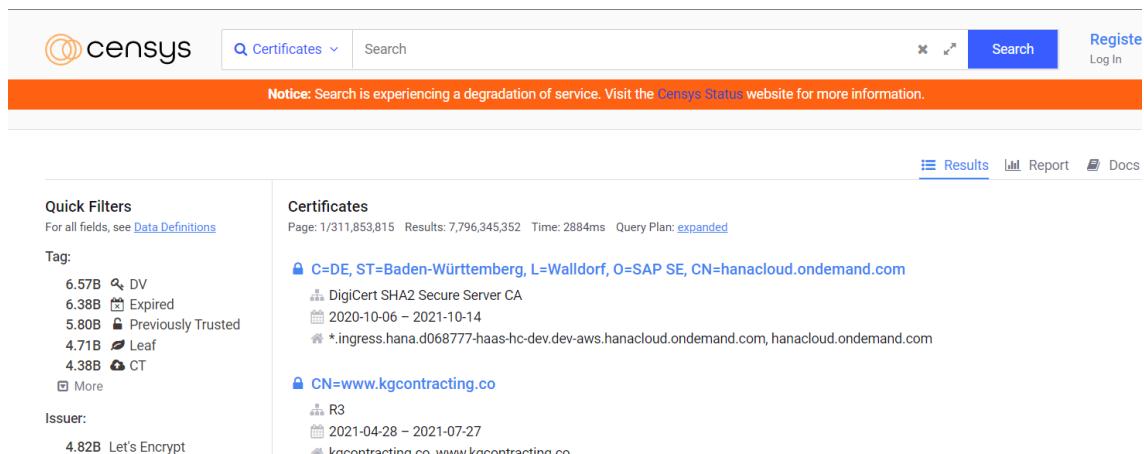


Ilustración 58 Censys

6.3.2.8. Flightaware

Flightaware se trata de un buscador de vuelos actuales, sirve para dar seguimiento a nivel mundial los vuelos y poder rastrearlos.

Para su uso solo es necesario entrar a la web (<https://es.flightaware.com/>) y buscar por número de vuelo o por destinos, ahí saldrán todos los vuelos que se pueden rastrear.



Ilustración 59 Flightaware

Ejemplo de búsqueda.

This screenshot shows the search results page on FlightAware. The search criteria are set to 'ORIGEN: SPZO' and 'DESTINO: SPJC'. The results table is titled 'Resultados de vuelos: (CUZ) Int'l Alejandro Velasco Astete - (LIM) Jorge Chávez Int'l'. The table has columns for 'Línea aérea', 'Ident', 'Aeronave', 'Estado', 'Salida', and 'Llegada'. There are 48 results listed, all belonging to LATAM Peru A320 aircraft, programmed for departure at 10:19AM-05 and arrival at 11:50AM-05. The sidebar on the left contains filters for 'Estado' (Programado, Arribado), 'Línea aérea' (LATAM Peru, Sky Airline, VIVA PERU), and 'Hora de llegada' (12am-12am).

Ilustración 60 Flightaware - Resultado

6.3.2.9. Lampyre

Lampyre es un buscador web, que saca información de los contactos deseados, puede recibir de parámetro de entrada: emails, números de teléfono, usernames, IP address, dominios e imágenes



Ilustración 61 Lampyre

Para su uso es necesario entrar a la web (<https://lampyre.io/>), crearse una cuenta y empezar con las búsquedas en el apartado de “Data Lookup”. Cada cuenta, posee una cantidad limitada de búsquedas, luego habrá que pagar una membresía para recargar las búsquedas o crear una cuenta nueva. Se realiza un ejemplo a continuación de la búsqueda por correo.

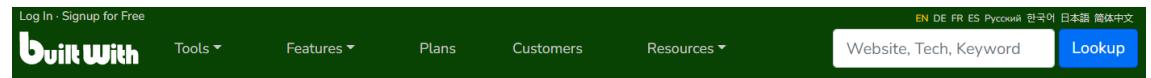


A screenshot of the Lampyre search results page. The results are presented in three separate cards. Each card contains an icon, a field name, a value, a date, and a more options icon. Card 1: Icon user, Field 'Username', Value 'yaspalugo', Date '04.04.2022'. Card 2: Icon envelope, Field 'Email', Value 'yaspalugo@hotmail.com', Date '04.04.2022'. Card 3: Icon envelope, Field 'Email', Value 'yaspalugo@gmail.com', Date '04.04.2022'. Each card also indicates '3 results'.

Ilustración 62 Lampyre - Resultados

6.3.2.10. Builtwith

Se trata de una herramienta que extrae información técnica de una web, extrae las diferentes tecnologías que la web está usando, desde servidores, frameworks, motores de publicidad, etc.



Find out what websites are Built With

Enter a website address, a technology name or a keyword

Lookup

Ilustración 63 Builtwith

Para su uso es necesario entrar a la web (<https://builtwith.com/>) e ingresar el dominio que requiera ser analizado.

The screenshot shows the search results for 'University or College'. It includes a 'Frameworks' section with a 'View Global Trends' link, a 'University or College' section with a 'View Global Trends' link, and a 'PHP' section with a 'View Global Trends' link. The 'University or College' section contains a link to 'University or College Usage Statistics' and a download link for 'Download List of All Websites using University or College'. The 'PHP' section contains a link to 'PHP Usage Statistics' and a download link for 'Download List of All Websites using PHP'. The 'Organization Schema' section contains a link to 'Organization Schema Usage Statistics' and a download link for 'Download List of All Websites using Organization Schema'.

The screenshot shows the search results for 'Content Delivery Network'. It includes a 'Content Delivery Network' section with a 'View Global Trends' link and an 'AJAX Libraries API' section with a 'View Global Trends' link. The 'AJAX Libraries API' section contains a link to 'AJAX Libraries API Usage Statistics' and a download link for 'Download List of All Websites using AJAX Libraries API'. Below this, there is a brief description: 'The AJAX Libraries API is a content distribution network and loading architecture for the most popular, open source JavaScript libraries.'

Ilustración 64 Builtwith - Resultados

6.3.2.11. Searchcode

Es una herramienta que como su nombre indica sirve para buscar código fuente, que puede buscar entre más de 75 mil millones de líneas de código, las búsquedas son sugeridas incluyendo nombre de usuarios, fallas de seguridad y caracteres especiales que son usados para inyección de código.

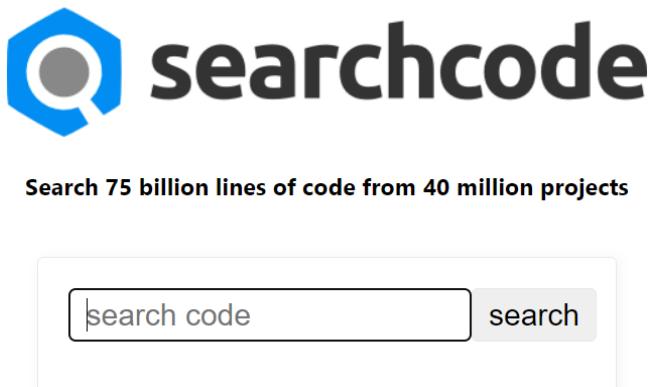


Ilustración 65 Searchcode

Para su uso es simplemente acceder a la web (<https://searchcode.com/>) y empezar con la búsqueda de código, como se muestra en el siguiente ejemplo.

searchcode

eval \$_GET

4,262 results for 'eval \$_GET' (620 ms)

apply filters

Source

- Github (2,679)
- Bitbucket (1,180)
- GitLab (204)
- Google Code (94)
- Fedora Project (53)
- CodePlex (35)
- repo.or.cz (6)
- Sourceforge (3)
- codeberg (1)

Language

- JavaScript (2,935)
- PHP (371)
- Perl (219)

GET.js https://github.com/pipifuyj/global.git | JavaScript | 39 lines

```

19         }
20         eval("if(typeof _GET"+t+"==\"undefined\"){_GET"+t+"={};")
21     }
21     }
22     eval("_GET"+t+"='"+value+"\n");
23 }

```

anagrams.m4 https://gitlab.com/dlucenap/RosettaCodeData.git | m4 | 46 lines

```

4     [ifelse($#,0,[[$0]],]
5     [ifelse(eval($2<=$3),1,
6     [pushdef([[$1],$2]$4[popdef([[$1]$0([[$1],incr($2,$3,[4]]))])])
8     define([eachline],),
9     [ifelse(eval($2>0),1,
10    [$3(substr([[$1],0,$2)])]eachline(substr([[$1],incr($2)),[$3])))])
15     define([checkfirst],
16     [ifelse(eval(index([$2],substr([[$1],0,1))<0),1,
17        0,
21        [ifelse([[$1],[[$2],1,
22        eval(len([[$1]])!=len([[$2]])),1,0,
23        len([[$1]],0,0,
29        define([matchj],
30        [_set([count],$2,incr(_get([count],$2))][ifelse(eval(_get([count],$2)> max),
31            1,[define([_max],incr(_max))][_set([list],$2,_get([list],$2 '$1))])])

```

anagrams.m4 https://github.com/aayushKumarJarvis/RosettaCodeData.git | m4 | 46 lines

```

4     [ifelse($#,0,[[$0]],]
5     [ifelse(eval($2<=$3),1,

```

Ilustración 66 Searchcode - Resultado

6.3.2.12. Zoomeye

Se trata de un motor de búsqueda bastante potente comparable a Shodan o Censys y al igual que estos este metabuscador obtiene información de dispositivos conectados a internet.



Ilustración 67 Zoomeye

Para su uso es simplemente acceder a la web (<https://www.zoomeye.org/>) y empezar con la búsqueda, como se muestra en el siguiente ejemplo.

| Banner | SSL | Data update |
|-------------|---|-------------|
| mail.amp... | HTTP/1.1 301 Moved Permanently Date: Fri, 15 Apr 2022 16:09:05 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Fri, 15 April 2022 17:09:05 GMT Location: https://mail.amplificadorwifi.xyz/ Report-To: {"endpoints": [{"url": "https://a.ne1.cloudflare.com/report"}], "NEL": {"success_fraction": 0, "report_to": "cf-ne1", "max_age": 604800}} Vary: Accept-Encoding Server: cloudflare CF-RAY: 6fc5f18f1def00bf-AMS alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400 | |

SEARCH TYPE

| | |
|----------|-----------|
| Devices | 3,235,698 |
| Ipv4 | 3,235,122 |
| Ipv6 | 576 |
| Websites | 128,061 |

YEAR

| | |
|------|---------|
| 2022 | 418,466 |
|------|---------|

Ilustración 68 Zoomeye - Resultado

6.3.2.13. DnsDumpster

Se trata de una herramienta que analiza dominios, esta herramienta recopila información de diferentes motores de búsqueda (Google, Bing, etc), plataformas como Alexa Top 1 Million, Common Crawl, Certificate Transparency, Max Mind, Team Cymru, Shodan y scans.io, entre otros.

dns recon & research, find & lookup dns records

exampledomain.com

DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

this is a [HackerTarget.com](#) project

Ilustración 69 DnsDumpster

Para poder usar este buscador solo se requiere ingresar a la web (<https://dnsdumpster.com/>) e ingresar el dominio que se quiere analizar y empezar a buscar, a continuación, se muestra una parte del resultado.

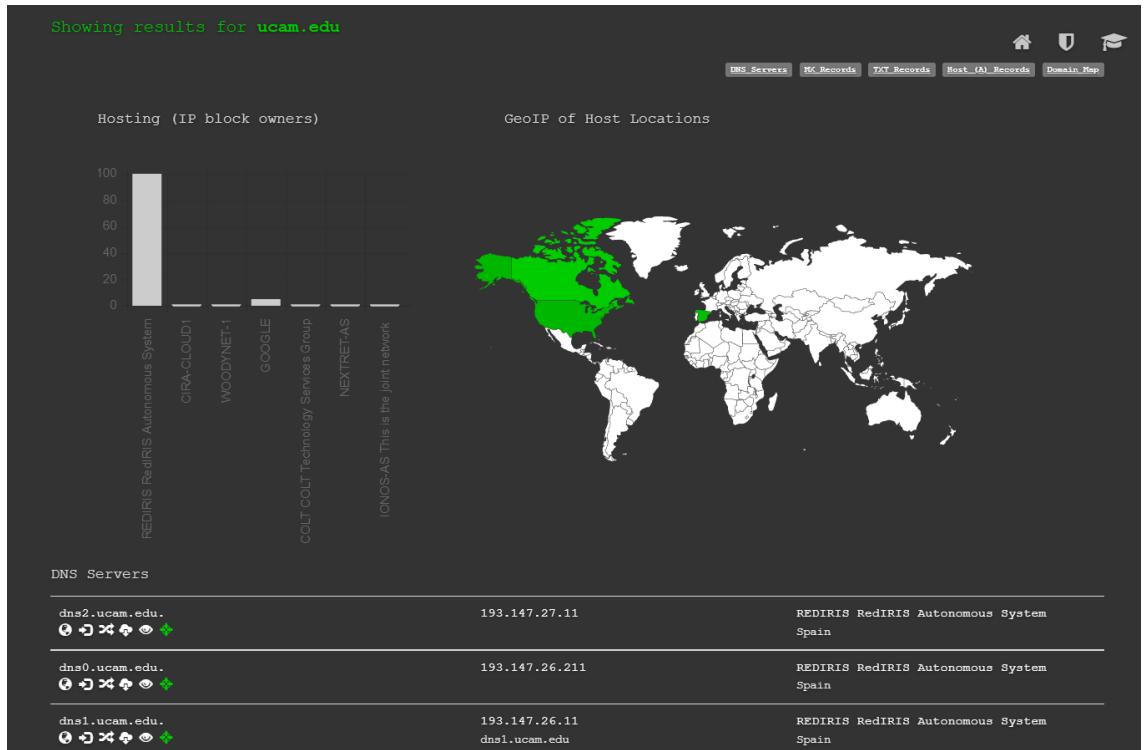


Ilustración 70 DnsDumpster - Resultado

6.3.2.14. Wayback machine

Se trata de un buscador que tiene como parámetros de entrada direcciones URL, metadatos, nombres y apellidos, esta herramienta consulta de versiones antiguas de páginas web y consulta de información sobre medios digitales o digitalizados.

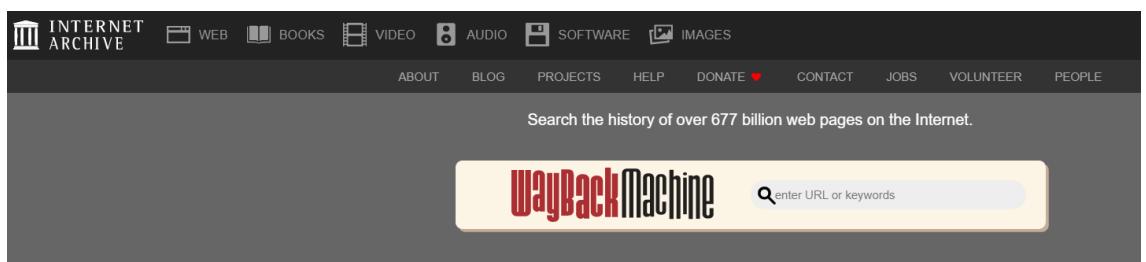


Ilustración 71 Wayback machine

Para poder usar este buscador solo se requiere ingresar a la web (<https://archive.org/>) e ingresar la url o las palabras de los usuarios, como se muestra a continuación.

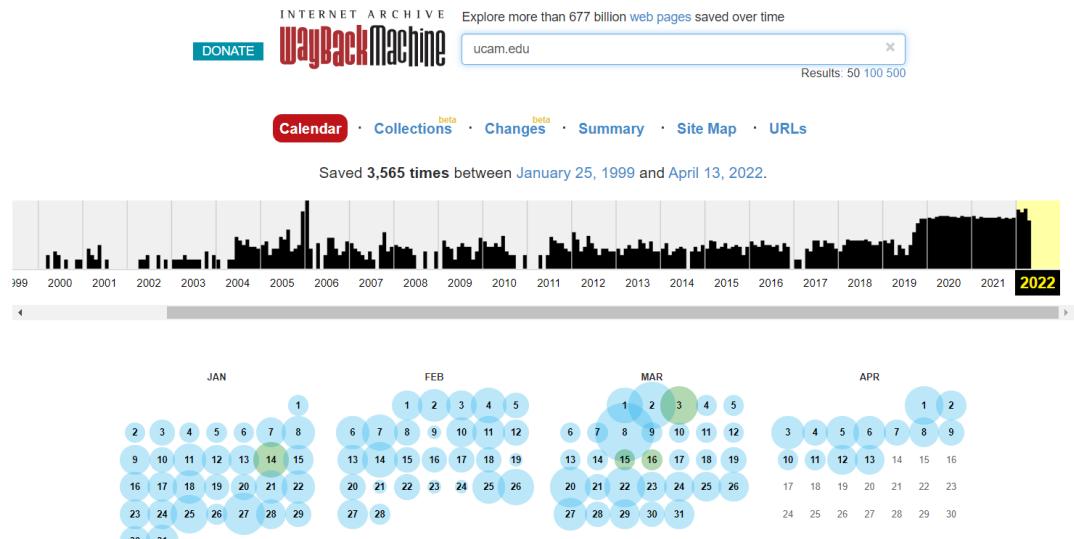


Ilustración 72 Wayback Machine - Resultado

6.3.2.15. Ipinfo

Se trata de un analizador de direcciones IP o ASN (Autonomous System Number).

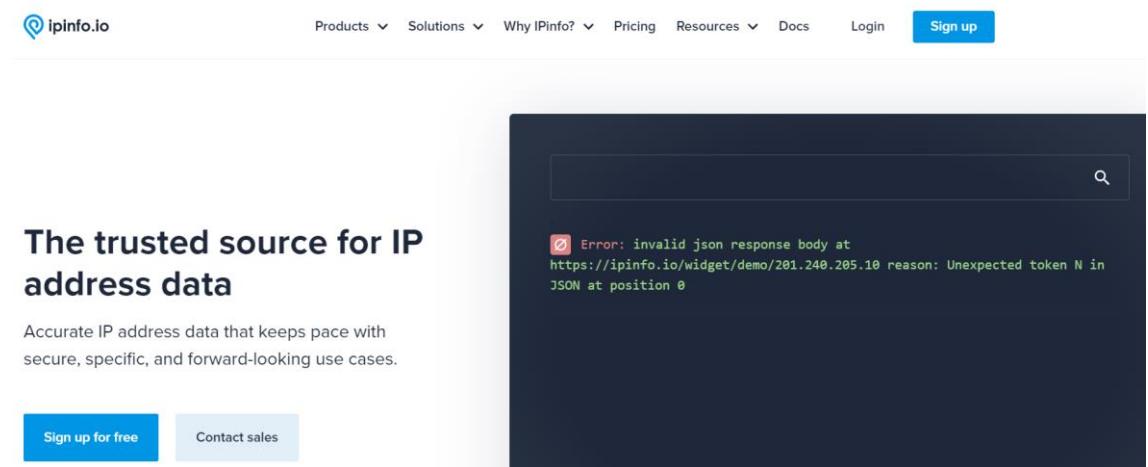


Ilustración 73 Ipinfo

Para poder usar este buscador solo se requiere ingresar a la web (<https://ipinfo.io/>) e ingresar la ip o ASN, como se muestra a continuación.

The screenshot shows a dark-themed web interface for ipinfo.io. At the top, there is a search bar containing the IP address "201.240.205.10" and a magnifying glass icon. Below the search bar, the results are displayed in a JSON-like format:

```
  "asn": "AS6147",
  "name": "Telefonica del Peru S.A.A.",
  "domain": "telefonica.com.pe",
  "route": "201.240.205.0/24",
  "type": "isp",
  {} company: Object,
    "name": "Telefonica del Peru S.A.A.",
    "domain": "telefonica.com.pe",
    "type": "isp",
```

At the bottom of the results section, there are several buttons with links: "Your IP", "8.8.4.4", "AS15169", "1.1.14", "AS45194", and "68.87.41.40".

Ilustración 74 Ipinfo - Resultado

6.3.2.16. Centralops

Esta herramienta permite investigar dominios y direcciones IP, gracias a esta herramienta se puede obtener la información del registrante, registros de DNS y más, todo en un solo reporte.

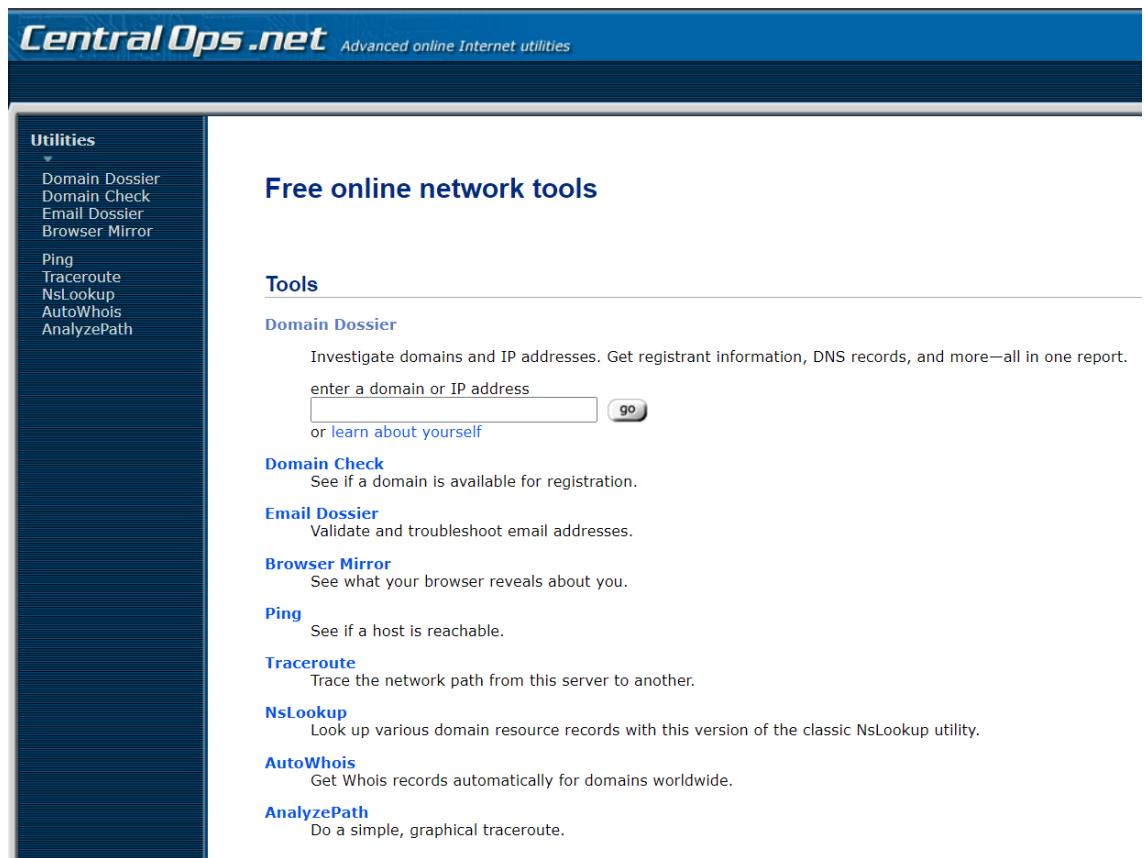


Ilustración 75 Central Ops

Para poder usarla solo es necesario entrar a la web (<https://centralops.net/co/>) y poner el dominio o la ip que se quiera analizar, como a continuación se muestra.

Address lookup

canonical name [ucam.edu.](#)

aliases

addresses [193.147.26.228](#)

Domain Whois record

Queried [whois.educause.net](#) with "ucam.edu"...

Domain Name: UCAM.EDU

Registrant:

Universidad Catolica San Antonio de Murcia
Avda. Los Jeronimos, S/N
Guadalupe, MURCIA 30107
Spain

Administrative Contact:

Sergio Leon
Universidad Catolica San Antonio de Murcia
Avenida de Los Jeronimos 135
Guadalupe, MU 30107
Spain
+34.968278835
sleon@ucam.edu

Technical Contact:

Sergio Leon
Universidad Catolica San Antonio de Murcia
Avenida de Los Jeronimos 135
Guadalupe, MU 30107
Spain
+34.968278835
sleon@ucam.edu

Name Servers:

DNS1.UCAM.EDU
DNS2.UCAM.EDU

Domain record activated: 07-Jul-1998

Domain record last updated: 25-Feb-2022

Domain expires: 31-Jul-2024

Ilustración 76 Central Ops - Resultado

6.3.2.17. ImgOps

Esta página web recopila distintas herramientas que permiten obtener información interesante para realizar OSINT sobre imágenes.



Ilustración 77 ImgOps

Para poder utilizar esta herramienta solo es necesario entrar a la web (<https://imgops.com/>) y poner la url de la imagen que se desea analizar, como se muestra a continuación.

| Operations | Links |
|---------------------|---|
| reverse / similar | google • bing • tineye • reddit • yandex • baidu • so.com • sogou |
| quick view | fit-zoom • zoom-pan • left 90 • right 90 • 180 • mirror |
| edit | ours • pixlr • picmonkey • lunapic • annotate |
| host | beeimg • imgur |
| hidden data | exif / xmp / gps • metapicz • view/remove exif • http headers • error level |
| effects | meme • text • ancient • ASCII |
| special | optimize • waifu2x • tester • what the font • what font is • OCR • OCR2 • QR de-code • color palette • palette2 • css borders • 3-way view • wiggle |
| specialized reverse | reddit [KD] • reddit [RS] • igdb (anime) • saucenao (anime+) • ascii2d (anime2) • trace.moe (anime) • pictrev (faces) |
| animated GIFs | add sound • gif-explode • big gif • crop / optimize / split |
| convert | base 64 • HTML • JPG • GIF • PNG • BMP • ICO • PDF • TIFF • EPS • HDR/EXR • SVG • TGA • WBMP |
| custom | edit personal links |

Ilustración 78 ImgOps - Resultado

6.3.2.18. Whotwi

Esta página nos permite analizar las cuentas de usuario de Twitter que deseemos, pudiendo ver toda su actividad desglosada en distintos gráficos tras introducir la ID correspondiente al usuario en la página.



Ilustración 79 Whotwi

Para usar esta herramienta solo es necesario entrar a la web (<https://es.whotwi.com/>) y poner el ID de Twitter que se quiera analizar, como se muestra a continuación.

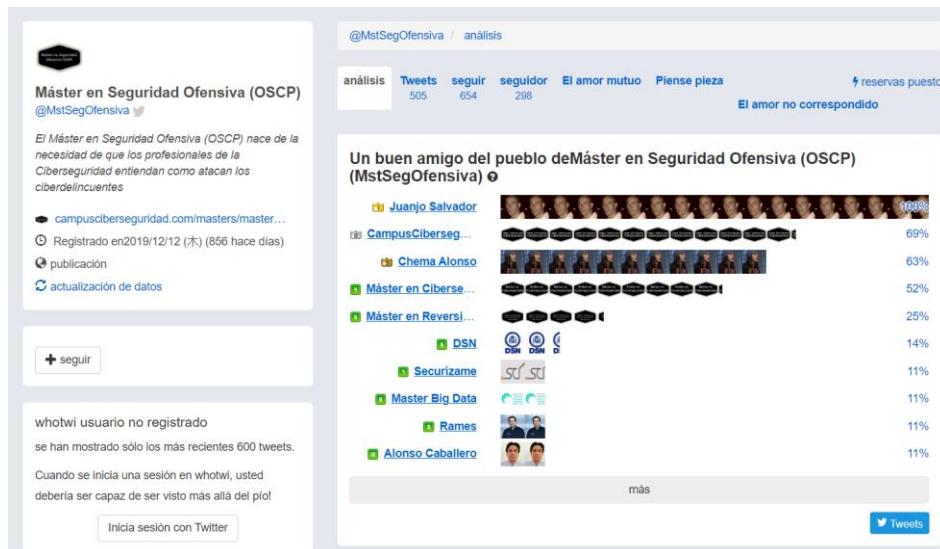


Ilustración 80 Whotwi - Resultado

6.3.2.19. Urlscan.io

Urlscan.io provee un servicio gratuito de escaneo y análisis de dominios/URLs.

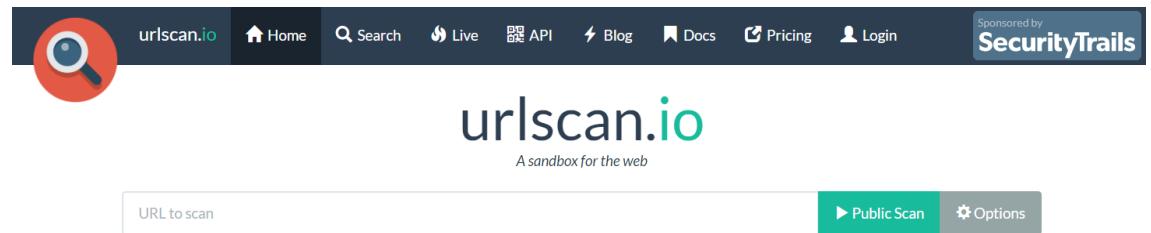


Ilustración 81 UrlScan.io

Para utilizar este escaner se tiene que entrar a la web (<https://urlscan.io/>) donde se pondrá la url o dominio a escanear, obteniendo el siguiente resultado.

A detailed screenshot of the UrlScan.io analysis results for the domain www.ucam.edu. The page shows the URL submitted (www.ucam.edu) and its IP address (193.147.26.228, Spain). It provides a summary of the scan, including 11 IPs from 10 domains over 29 HTTP transactions. The main IP is 193.147.26.228, located in Guadalupe, Spain, belonging to REDIRIS RedIRIS Autonomous System, ES. The TLS certificate is valid until December 14th, 2021. The page also displays a screenshot of the UCAM website, showing the university's building at dusk. Other sections include 'Live information' (Google Safe Browsing: No classification), 'Page URL History' (listing the URL with an HTTP 301 redirect to https://www.ucam.edu), and various analysis tabs like Summary, HTTP, Redirects, Links, Behaviour, Indicators, Similar, DOM, Content, API, and Verdicts.

Ilustración 82 UrlScan.io - Resultado

6.4. Exportado de .ova

Al finalizar la instalación del script con todas las herramientas y el agregado de los marcadores de todas las herramientas anteriormente mencionadas, se procede a exportar.

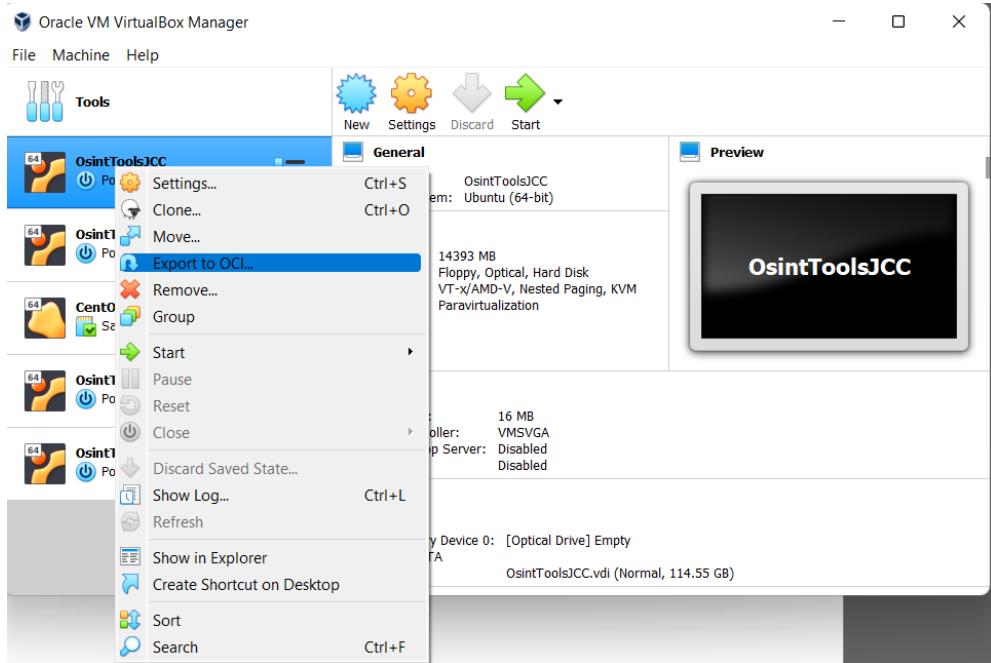


Ilustración 83 Exportar .ova

Se sigue los pasos que pide para poder exportar la máquina virtual en un .ova

Appliance settings

Please choose a format to export the virtual appliance to.

The **Open Virtualization Format** supports only **.ovf** or **.ova** extensions. If you use the **.ovf** extension, several files will be written separately. If you use the **.ova** extension, all the files will be combined into one Open Virtualization Format archive.

The **Oracle Cloud Infrastructure** format supports exporting to remote cloud servers only. Main virtual disk of each selected machine will be uploaded to remote server.

Format: **Open Virtualization Format 1.0**

Please choose a filename to export the virtual appliance to. Besides that you can specify a certain amount of options which affects the size and content of resulting archive.

File: **C:\Users\Jimca\OneDrive\Documents\OsintToolsJCC.1.ova**

MAC Address Policy: **Include only NAT network adapter MAC addresses**

Additionally: **Write Manifest file**

Include ISO image files

Ilustración 84 Exportar .ova 2

Y finalmente se espera para que se exporte de forma correcta, obteniendo lo siguiente.

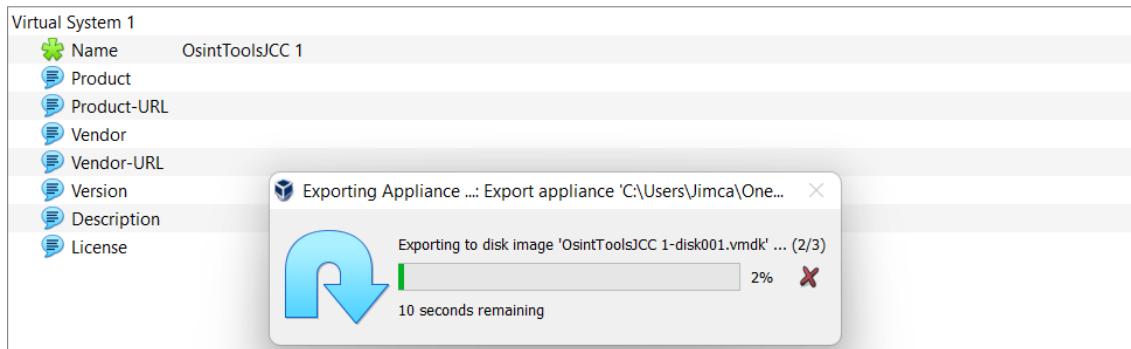


Ilustración 85 Exportar .ova 3



Ilustración 86 Ova Exportado

7. CONCLUSIONES

Las herramientas fueron probadas y todas funcionan correctamente, por tanto también se logró construir el fichero .ova con todas las herramientas descritas.

Se pudo crear el script de instalación y probarlo, de modo que las herramientas se instalan de forma satisfactoria, por lo que se logró completar satisfactoriamente el catálogo del presente proyecto.

Se brindo la información básica para el entendimiento y uso de cada una de las herramientas y donde se encuentran dentro del fichero creado.

8. BIBLIOGRAFIA

- Acosta, R. (2021, Marzo 20). *Distribución orientada a la obtención de información en la red.* Retrieved from Cibergia: <https://www.cibergia.com/distribucion-orientada-a-la-obtencion-de-informacion-en-la-red/>
- Blanco, A. G. (2022, Marzo 21). *¿Para qué quieren tus datos los ciberdelincuentes?* Retrieved from BBVA: <https://www.bbva.com/es/para-que-quieren-tus-datos-los-ciberdelincuentes/>
- Fernández, L. (2020, Marzo 07). *¿Conocías Shodan? Todo sobre este motor de búsqueda orientado al hacking.* Retrieved from Redes Zone: <https://www.redeszone.net/tutoriales/seguridad/shodan-busqueda-hacking/>
- Frias, M. (2021, Julio 26). *OSINT: Qué es, técnicas y herramientas.* Retrieved from Open Webinars: <https://openwebinars.net/blog/osint-que-es-tecnicas-y-herramientas/>
- HuronOsint. (2019, Julio 30). *HuronOsint DistroV2.* Retrieved from Github: https://github.com/HuronOsint/Distro_Osint_v2
- Kemp, S. (2020, Febrero 18). *DIGITAL 2020: PERU.* Retrieved from Data Reportal: <https://datareportal.com/reports/digital-2020-peru?rq=peru>
- Navarro, M. (2021). *Distro Linux/OSINT.* Retrieved from ENIIT: <https://eniit.es/distro-linux-osint/>
- Pastorino, C. (2019, Octubre 07). *Técnicas y herramientas OSINT para la investigación en Internet.* Retrieved from Welivesecurity: <https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/>
- Torre, P. d. (2018, Julio 06). *OSINTUX.* Retrieved from Osintux.org: <https://www.osintux.org/blog/usb-booteable-osintux>