

SEMINARIO 1

HERRAMIENTAS PARA INVESTIGAR EN INTERNET



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



JOSÉ MANUEL REDONDO LÓPEZ PROYECTO "S-81 ISAAC PERAL" v4.0



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

Logo: @creative_vanesa (Instagram)

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

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

● Vamos a hacer algo que no requiere mucha pericia técnica 😊

- **OSINT (Open Source INTelligence)**
- Algunas de estas herramientas las usaremos en prácticas
- Pero, sobre todo, explotaremos más esta rama en el **Trabajo en Grupo** de la asignatura

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

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



ÍNDICE

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

[< Ir al Índice](#)

OSINT CONTRA MÁQUINAS

Investigando máquinas usando solo información pública



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

● Motor de búsqueda de máquinas (no web)

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

● Busca hasta 10 dispositivos

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

● Tutoriales

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

Web Technologies

 MOODLE

 PHP

 REQUIREJS

Vulnerabilities

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

CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ("/), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38. a bug in mod_ssl when using per-location

Apache httpd 2.4.38

HTTP/1.1 200 OK
Date: Mon, 21 Feb 2022 02:36:16 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: MoodleSession=j25o9m0cman8dkarptfvspemup; path=/; secure
Expires:
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Content-Language: es
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-UA-Compatible: IE=edge
Accept-Ranges: none
X-Frame-Options: sameorigin
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

03:b7:b4:45:4c:85:40:a2:1d:c9:b0:fd:06:bf:c0:61:e8:f3

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=Let's Encrypt, CN=R3

Validity

Not Before: Jan 12 04:06:45 2022 GMT

Not After : Apr 12 04:06:44 2022 GMT

Subject: CN=virtual.ingenieriainformatica.uniovi.es

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:df:4c:d6:9c:50:19:04:39:96:05:61:cb:0d:2b:

ab:4f:cd:0a:9f:66:33:3b:66:07:a8:61:8a:ac:25:

c7:ab:08:38:d9:36:05:de:2d:43:58:d5:eb:0c:e1:

55:04:5f:70:79:f5:f4:44:1a:fa:d2:77:e4:38:75:

4c:51:3a:3e:f7:02:95:c6:cd:96:f7:3a:2d:ae:48:

fe:8a:5a:df:cb:d5:52:eb:e3:d1:b3:87:b2:35:67:

5f:0d:e1:44:05:3b:c1:3f:a0:43:62:86:9b:3f:ea:

The search engine for Webcams

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

Create a Free Account | Getting Started

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

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

See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform

56% of Fortune 100
Shodan is used around the world by researchers, security pros

Busca los banners de estos servicios

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

SHODAN apache

Exploits | Maps

TOTAL RESULTS
14,301,988

TOP COUNTRIES

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

TOP SERVICES

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

RELATED TAGS: web servers

72.29.75.120
72-29-75-120 static.hostdime.com
HostDime.com
Added on 2017-12-04 15:19:36 GMT
United States, Orlando
Details

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache
Last-Modified: Wed, 20 Jul 2016 05:39:00 GMT
ETag: "6f-5380a3e498500"
Accept-Ranges: bytes
Content-Length: 111
Connection: close
Content-Type: text/html

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

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

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

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

General

- all
- asn
- city
- country
- cpe
- device
- geo
- has_ipv6
- has_screenshot
- has_ssl
- has_vuln
- hash
- hostname
- ip
- isp
- link
- net
- org
- os

HTTP

- http.component
- http.component_category
- http.favicon.hash
- http.headers_hash
- http.html
- http.html_hash
- http.robots_hash
- http.securitytxt
- http.status
- http.title
- http.waf

Bitcoin

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

SSL

- ssl
- ssl.alpn
- ssl.cert.alg
- ssl.cert.expired
- ssl.cert.extension
- ssl.cert.fingerprint
- ssl.cert.issuer.cn
- ssl.cert.pubkeybits
- ssl.cert.pubkeytype
- ssl.cert.serial
- ssl.cert.subject.cn
- ssl.chain_count
- ssl.cipher.bits
- ssl.cipher.name
- ssl.cipher.version
- ssl.ja3s
- ssl.jarm
- ssl.version

SHODAN CLI

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



Seguridad de Sistemas
Informáticos

- **Biblioteca de Python que proporciona las capacidades de Shodan desde comandos**
 - Útil en contextos sin GUI
- **Permite integrar las capacidades de Shodan en nuestros propios scripts o programas**
 - O automatizar tareas de pentesting usando Shodan
 - La web oficial tiene ejemplos de uso
- **Sus capacidades son equivalentes a las de la interfaz web**
- **Conjunto de búsquedas útiles:**
 - <https://github.com/jakejarvis/awesome-shodan-queries>

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

● Como Shodan, pero con información estructurada

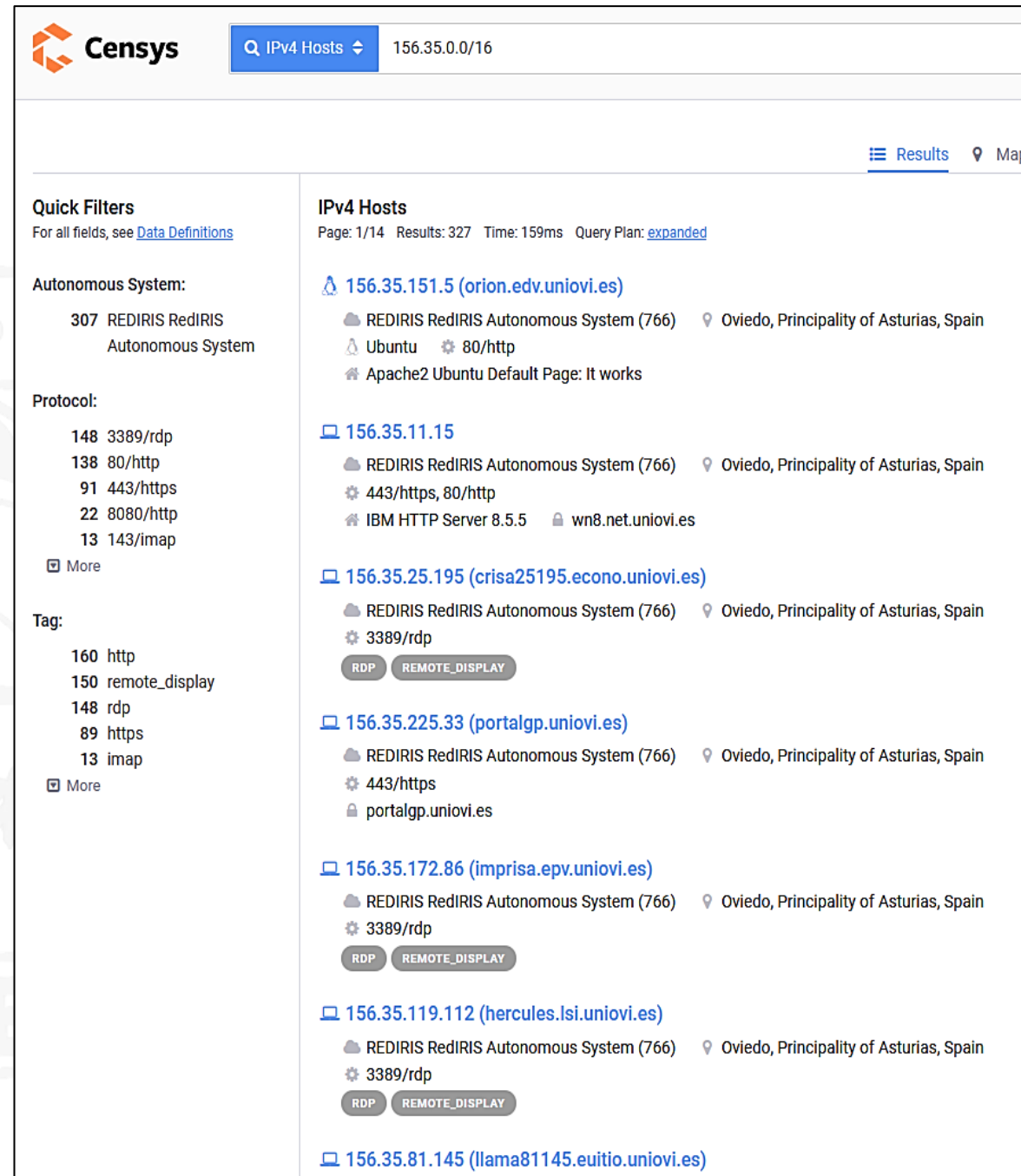
- Busca características de servidores: servicios interesantes en ejecución (RDP), banners de SO servidores web...
- Varios criterios de búsqueda
 - IP (solo v4) y redes: <https://censys.io/ipv4/>
 - Nombres de dominio del sitio web: <https://censys.io/domain?q>
 - Certificados: <https://censys.io/certificates?q>

● Tutorial de búsqueda

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

● Una herramienta similar es Onhype.io

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



The screenshot shows the Censys search results page for IPv4 Hosts. The search query is "156.35.0.0/16". The results are displayed in a list format, showing the IP address, the Autonomous System (AS), and the location. The results are filtered by "Quick Filters" and "Tags".

Quick Filters
For all fields, see [Data Definitions](#)

Autonomous System:
307 REDIRIS RedIRIS Autonomous System

Protocol:
148 3389/rdp
138 80/http
91 443/https
22 8080/http
13 143/imap
[More](#)

Tag:
160 http
150 remote_display
148 rdp
89 https
13 imap
[More](#)

IPv4 Hosts
Page: 1/14 Results: 327 Time: 159ms Query Plan: [expanded](#)

[156.35.151.5 \(orion.edv.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
Ubuntu 80/http
Apache2 Ubuntu Default Page: It works

[156.35.11.15](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
443/https, 80/http
IBM HTTP Server 8.5.5 wn8.net.uniovi.es

[156.35.25.195 \(crisa25195.econo.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
3389/rdp
[RDP](#) [REMOTE_DISPLAY](#)

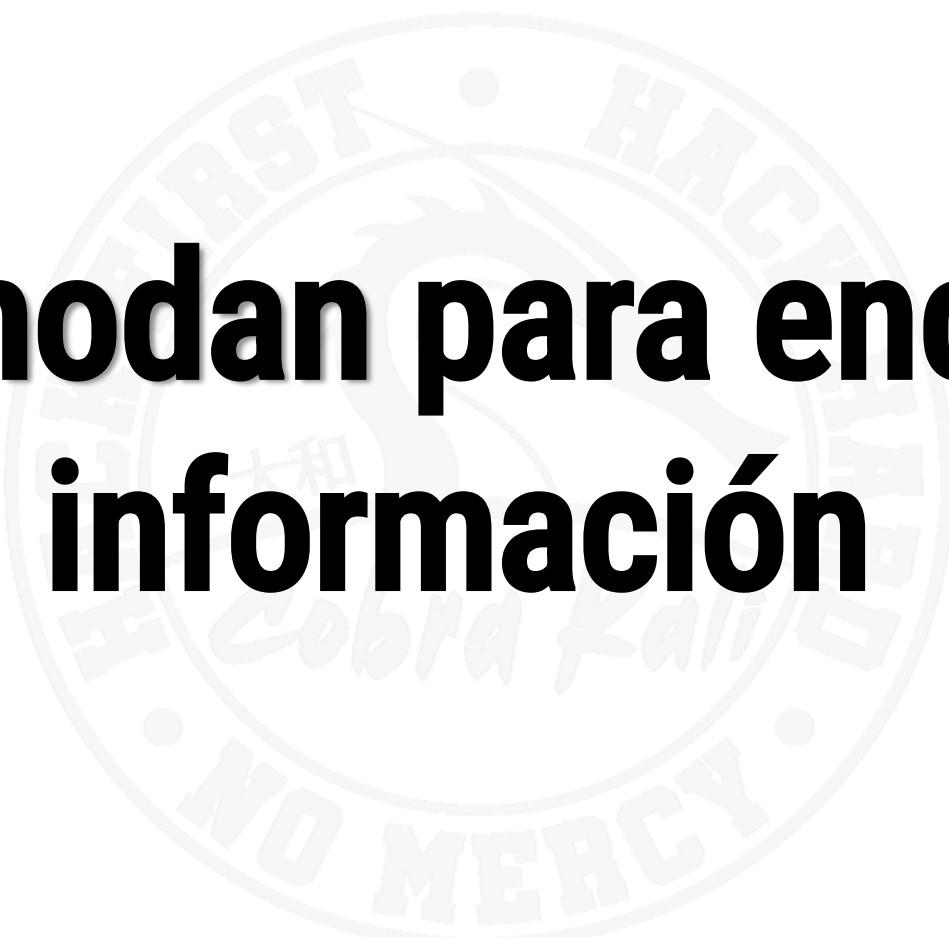
[156.35.225.33 \(portalgp.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
443/https
portalgp.uniovi.es

[156.35.172.86 \(imprisa.epv.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
3389/rdp
[RDP](#) [REMOTE_DISPLAY](#)

[156.35.119.112 \(hercules.lsi.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
3389/rdp
[RDP](#) [REMOTE_DISPLAY](#)

[156.35.81.145 \(llama81145.eutio.uniovi.es\)](#)

Usar Shodan para encontrar información



GOOGLE HACKING O “GOOGLE DORKING”



Seguridad de Sistemas
Informáticos

- **Capacidad de realizar búsquedas que revelan información comprometedor**
 - Usando motores de búsqueda (normalmente dirigidas a un dominio con el operador `site:`)
 - Las búsquedas tratan de encontrar información de vulnerabilidades, problemas de configuración o facilite un ataque
 - También se puede hacer en otros motores de búsqueda (aunque Google es el más usado)
- **Hay una BD de búsquedas preconstruidas clasificadas: Google Hacking Database**
 - Se llaman “Google Dorks”: <https://www.exploit-db.com/google-hacking-database>
 - Elige la categoría de búsqueda correcta: ¡cada categoría representa una posible vulnerabilidad!
 - Busca en el destino con la consulta elegida (`site:`)
- **El “Dorking” puede usarse con otros productos**
 - <https://github.com/cipher387/Dorks-collections-list>
- **Ejemplos**
 - <https://wifibit.com/google-hacking/>
 - <https://ciberpatrulla.com/osint-con-google/>
 - <https://ciberpatrulla.com/buscar-google/>
 - https://medium.com/@logicbomb_1/one-misconfig-jira-to-leak-them-all-including-nasa-and-hundreds-of-fortune-500-companies-a70957ef03c7

GOOGLE HACKING: PROCESO



EXPLOIT DATABASE

Google Hacking Database

Show 15

Date Added	Dork	Category	Author
2020-01-17	intitle:"WS02 Management Console"	Various Online Devices	Alfie
2020-01-10	intitle:"webview login" alcatel lucent	Pages Containing Login Portals	Bruno Schmid
2020-01-09	intitle:"LAS VANTAGE Login"	Pages Containing Login Portals	Reza Abasi
2020-01-09	site:"cgi/domadmin.cgi"	Pages Containing Login Portals	Reza Abasi
2020-01-09	inurl:"8080/login.jsp?os_destination="	Pages Containing Login Portals	Reza Abasi
2020-01-09	intitle:"index of" "wp-security-audit-log"	Files Containing Juicy Info	Reza Abasi
2020-01-09	intext:"powered by codoforum" inurl:"/user/login"	Pages Containing Login Portals	Prasanth
2020-01-06	inurl:"/index.php?enter=guest"	Various Online Devices	Reza Abasi
2020-01-06	intitle:"Zabbix" intext:"username" intext:"password" inurl:"/zabbix/index.php"	Pages Containing Login Portals	Reza Abasi

Category: Any

Author: Begin typing...

Filters

Search

intitle:"Apache2 Ubuntu Default Page: It works"

GHDB-ID: 5311

Author: REZA ABASI

Published: 2019-07-31

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

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

web server detection: intitle:"Apache2 Ubuntu Default Page: It works"

Reza Abasi(Turku)

EXPLOIT DATABASE

Google Hacking Database

Show 15

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

intitle:"Apache2 Ubuntu Default Page: It works"

Aproximadamente 27.000 resultados (0,40 segundos)

Traducir esta página

Apache2 Ubuntu Default Page: It works Annex02!

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

Traducir esta página

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

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

Traducir esta página

Apache2 Ubuntu Default Page: It works

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

Traducir esta página

Apache2 Ubuntu Default Page: It works

it works !

FINAL RECON

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



- **Script de Python para reconocimiento web**

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

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

- **Tutorial**

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

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

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

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

positional arguments:

url Target URL

optional arguments:

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

Extra Options:

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



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

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

● Tutorial:

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

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

Target: nasa.gov

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

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

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

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

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

https://bocachica.arc.nasa.gov/HAVE/nmc_rh_omega_plots.html.old
https://echo.jpl.nasa.gov/asteroids/1988TA/1988TA_planning.html.old
https://echo.jpl.nasa.gov/asteroids/1998QE2/1998QE2_planning.html.old
https://echo.jpl.nasa.gov/asteroids/2014J025/2014J025_planning.html.old
https://echo.jpl.nasa.gov/asteroids/goldstone_asteroid_schedule.html.old
https://fits.gsfc.nasa.gov/users_guide/users_guide.ps.old
https://image.msfc.nasa.gov/ChrisDocs/UDFInstall/uLibInstall.old
https://seawifs.gsfc.nasa.gov/OCEAN_PLANET/HTML/titanic.html.old
https://umbra.nascom.nasa.gov/soho/hqa/history.html.old
```

[< Ir al Índice](#)

Fuente: Bing Chat AI

[Redes sociales >](#)

[Integración de datos >](#)

OSINT CONTRA PERSONAS

Investigando gente usando solo información pública



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

Redes sociales

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



LA PROBLEMÁTICA DE LAS HERRAMIENTAS QUE TRABAJAN CON RRSS



Seguridad de Sistemas
Informáticos

- A las RRSS no les gustan las herramientas que extraen información de sus perfiles 😊
 - Y eso nos mete en una carrera del “gato y el ratón”
 - Obligándonos a buscar herramientas que sigan funcionando
- Puedes encontrar muchas en Ciberpatrulla
- Twitter (ahora X) es un ejemplo de ello
 - El acceso a la API se hizo de pago, lo que mató a muchas herramientas de investigación
 - Esto dejó operativas (algunas) de las que hacen scraping
 - Es decir, **procesar los contenidos que se muestran por pantalla**, actuando como si fueran usuarios normales
 - Algunas son (pero no descartes que dejen de funcionar)
 - <https://github.com/tweepy/tweepy>
 - <https://github.com/dataquestio/twitter-scrape>

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

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

Facebook

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

Otras RRSS

- ⌚ Busca en RRSS menos importantes

Instagram

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

- Sitio web que permite descubrir direcciones de correo electrónico relacionadas con un dominio / empresa
- Con ellas se pueden iniciar ataques OSINT, intentos de phishing o APTs (Advanced Persistent Threats)
- No es un servicio gratuito
 - El registro gratuito permite un uso limitado de sus características
 - Resultados completos
 - Descargas CSV
 - Hasta 50 búsquedas/mes

The screenshot displays the Hunter.io web application. At the top, there's a navigation bar with the 'hunter' logo, 'Product' dropdown, and 'Pricing' link. The main content area is divided into sections: 'Domain Search' (Find the email addresses of a company), 'Email Finder' (Find the email address of a professional), and 'Email Verifier' (Verify any email address). The 'Email Finder' section is active, showing a search for 'uniovi.es' with a 'Find email addresses' button. Below this, the 'Email Verifier' section shows the most common pattern: '{last}{first}@uniovi.es' with 2,672 email addresses. A list of found email addresses is displayed, each with a source count:

Email Address	Source Count
s rezfaustino@uniovi.es	1 source
b tranjose@uniovi.es	5 sources
p lina@uniovi.es	3 sources
s isjaime@uniovi.es	2 sources
g zalezcristian@uniovi.es	3 sources

At the bottom, it indicates '2,667 more results for "uniovi.es"'. A large, faint watermark of the University of the Basque Country logo is visible in the background of the screenshot.

PROJECT SHERLOCK

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



- Encuentra nombres de usuario en muchas RRSS o webs diferentes
 - ¡Más de 320!
- Es muy común encontrar usuarios con el mismo nombre en diferentes redes sociales y sitios
 - Y, de esta manera, recopilar información de diferentes fuentes sobre la misma persona
 - O utilizar fuentes secundarias si encontramos perfiles cerrados en algunas redes sociales...
- El uso básico es sencillo
 - `python3 pherlock.py <nombre de usuario>`

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

Integración de reconocimiento de usuarios / de varias fuentes

Agregando datos de usuarios

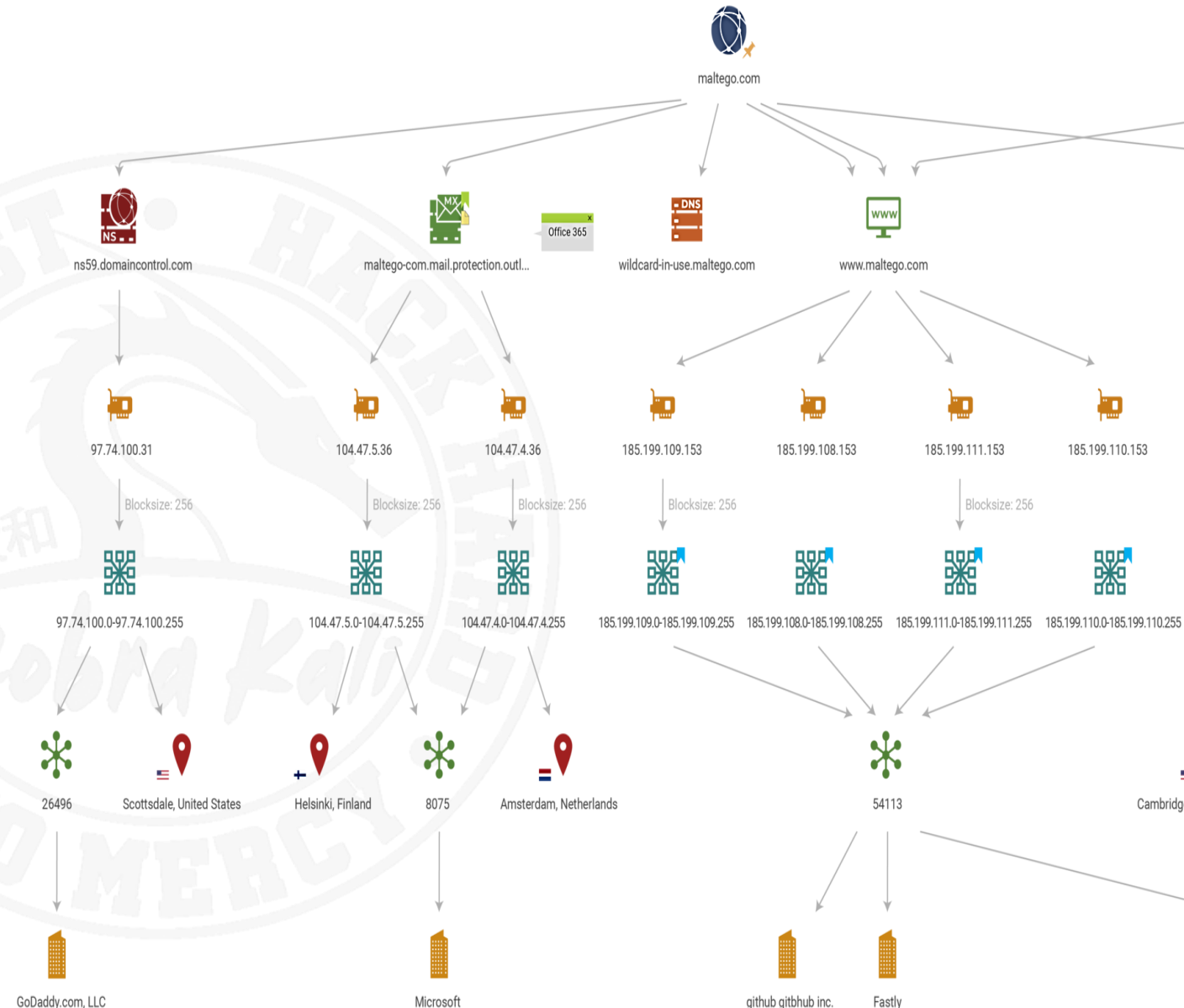


● Recopila información de entidades de internet

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

● Tutoriales

- <https://www.fwhibbit.es/introduccion-a-maltego>
- <https://ciberpatrulla.com/maltego/>
- www.elladodelmal.com/2010/08/mineria-de-datos-con-maltego-1-de-2.html
- Veremos más sobre ella en los **Trabajos en Grupo**



THE HARVESTER

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

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

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

- Utiliza motores de búsqueda conocidos para diferentes tipos de información
 - baidu, bing, bingapi, censys, Comodo Certificate search, dnsdumpster, dogpile, duckduckgo, github-code, Google (Google dorking opcional), google-certificates, hunter, intelx, Linkedin, Netcraft Data Mining, securityTrails (información histórica DNS), Shodan, threatcrowd, trello, Twitter, Bing virtual hosts search, Virustotal, y Yahoo search engine

- baidu, bing, bingapi, censys, Comodo Certificate search, dnsdumpster, dogpile, duckduckgo, github-code, Google (Google dorking opcional), google-certificates, hunter, intelx, LinkedIn, Netcraft Data Mining, securityTrails (información histórica DNS), Shodan, threatcrowd, trello, Twitter, Bing virtual hosts search, Virustotal, y Yahoo search engine

● También información de servidores DNS

- Fuerza bruta, búsqueda inversa, expansión TLD

● Tutorial

- <https://www.welivesecurity.com/la-es/2015/04/08/the-harvesterriesgo-nformacion-publica/>

SCRUMMAGE

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



Seguridad de Sistemas
Informáticos

● Centraliza los análisis OSINT

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

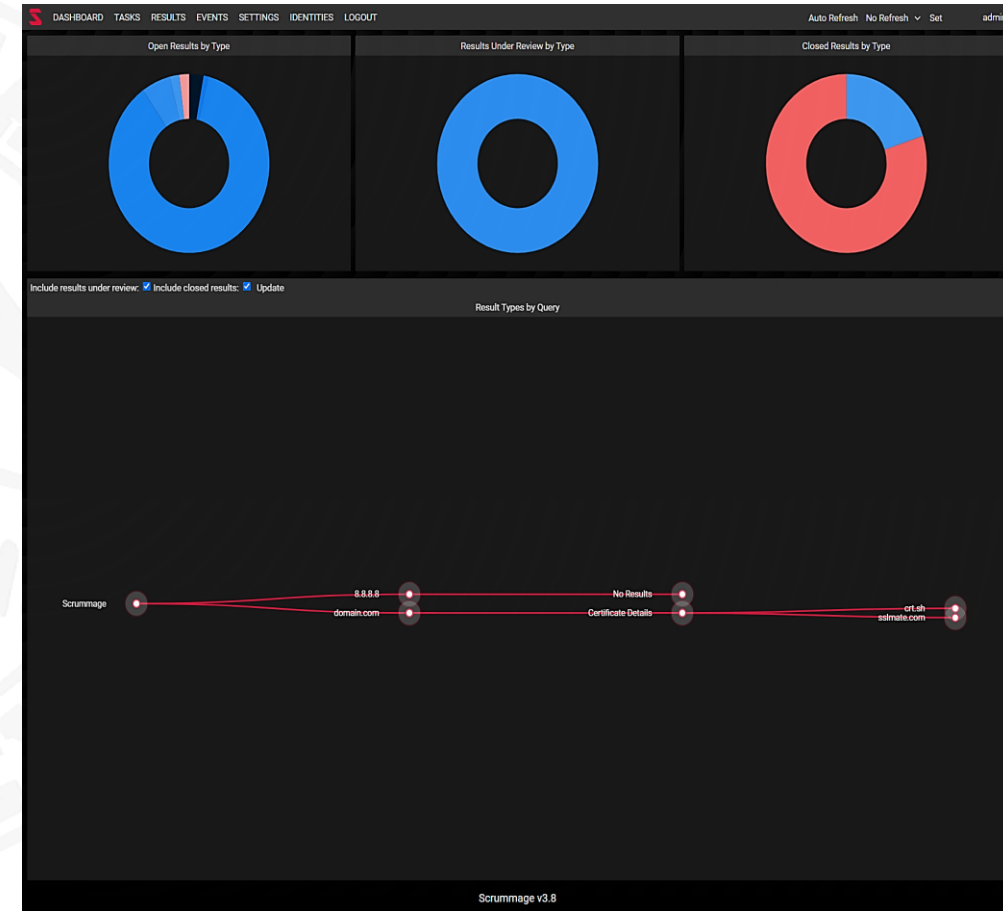
● Implementa plugins para personalizar el tipo de escaneos y optimizar el uso de recursos

● Estos plugins le dan diversas capacidades

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

● Herramientas similares

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



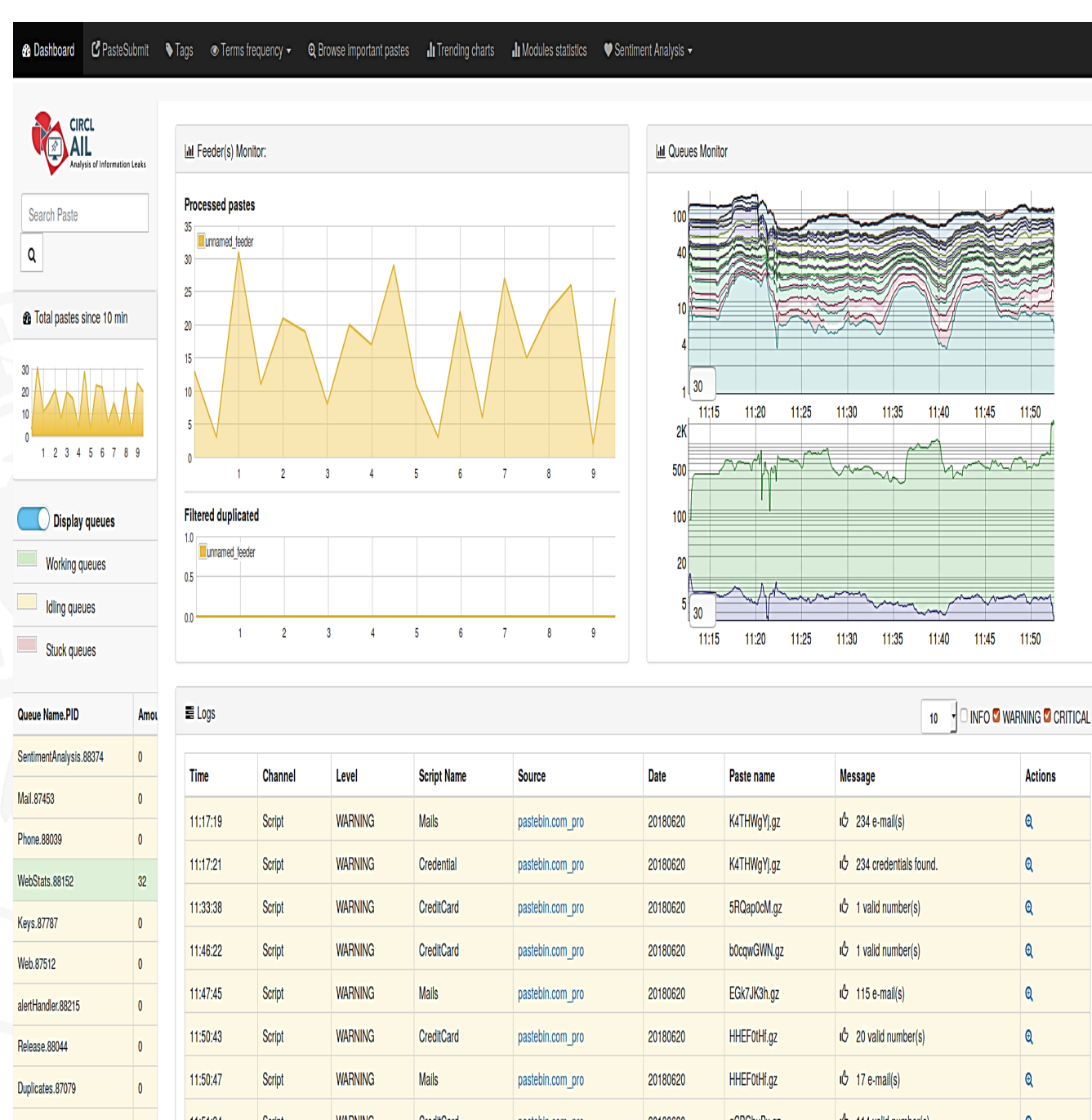
AIL FRAMEWORK

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



Seguridad de Sistemas
Informáticos

- **Framework muy modular que analiza la información filtrada**
 - De fuentes no estructuradas
 - Un origen de datos popular es Pastebin
- **Su alta modularidad permite ampliarla**
 - Y usarla para extraer y procesar información privada de diferentes tipos
 - Y por lo tanto detectar y prevenir la fuga de información
- **Para obtener más información**
 - <https://www.kitploit.com/2019/08/ail-frameworkframework-for-analysis-of.html>



MÁS HERRAMIENTAS OSINT...



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

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

● Recuerda: Hay una lista clasificada de herramientas: <https://ciberpatrulla.com/links/>

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

Recon Tools for Web Application Pentesting

Proxy

- Burpsuite
- Zap Proxy

Webspidering

- Gospider
- Gau
- Linkfinder
- Waybackurls
- Hakrawler
- Paramspider

Fingerprinting

- Wappalyzer
- Builtwith
- Netcraft
- Whatweb
- Wafw0f

Email

- Mxtoolbox
- Emkei
- Anonymailer
- Thunderbird

Sensitive data

- Trufflehog
- Gitsecrets

Payloads / Wordlists

- Swisskeyrepo
- Seclists

SSL

- SSLscan
- SSLhopper

Searchengines

- Shodan
- Censys
- Zoomeye
- Google

Subdomain

- Subfinder
- Amass
- Dig
- Assetfinder
- Sublist3r
- Chaos

Directory / Fuzzing

- Ffuf
- Wfuzz
- Gobuster
- Dirbuster

Vulnerability

- Nuclei
- Wpscan
- Nikto

Exploit

- Searchsploit
- Exploitdb

Api

- Postman
- GraphQLmap

Ports

- Nmap
- Masscan
- Zmap
- Smap
- Hackertarget

Misc

- HTTPx
- Metasploit
- DNSDumpster
- HTTPPrope
- Recon-ng
- Securitytrails

¿TIENES EJEMPLOS?

- Con esta cantidad de herramientas disponibles, es muy fácil perderse al iniciar una investigación OSINT
- Por lo tanto, es mejor ver ejemplos de cómo hacer una
- Como guía se puede seguir este tutorial de cinco partes
 - <https://navisec.io/a-pentesters-guide-part-1-osint-passive-recon-and-discovery-of-assets/>
 - <https://navisec.io/a-pentesters-guide-part-2-osint-linkedin-is-not-just-for-jobs/>
 - <https://navisec.io/a-pentesters-guide-part-3-osint-breach-dumps-password-spraying/>
 - <https://navisec.io/a-pentesters-guide-part-4-grabbing-hashes-and-forging-external-footholds/>
 - <https://navisec.io/a-pentesters-guide-part-5-unmasking-wafs-and-finding-the-source/>
- 0 esta guía OSINT
 - <https://www.hackers-arise.com/osint>
- Podemos encontrar además más herramientas en esta web
 - Extracción de metadatos, geolocalización, extracción de subdominios, etc.
 - <https://derechodelared.com/herramientas-osint-recopilatorio/>
- 0 en el material que te vamos a dar para los **Trabajos en Grupo** 😊

Usar Google Hacking para encontrar recursos de Uniovi



[< Ir al Índice](#)

OSINT CONTRA CÓDIGO FUENTE

El código fuente también puede ser una amenaza OSINT



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

```
https://github.com/intel/pa-biliu/blob/98565fea6e44a40fac3901b8d4bdc0029c708032/LayoutTests/fast/url/script-tests/segments.js
["http://example.com/", ["http:", "example.org", "", "", "example.com/", "", "", ""],
["ftp://example.com/", ["ftp:", "example.com", "", "", "", ""],
["https://example.com/", ["https:", "example.com", "", "", "", ""],
["madeupscheme://example.com/", ["madeupscheme:", "", "", "example.com/", "", "", ""],
["file://example.com/", ["file:", "", "", "", "example.com/", "", "", ""],
["ftps://example.com/", ["ftps:", "", "", "", "example.com/", "", "", ""],
["gopher://example.com/", ["gopher:", "example.com", "", "", "", ""],
["ws://example.com/", ["ws:", "example.com", "", "", "", ""],
["wss://example.com/", ["wss:", "example.com", "", "", "", ""],
["data://example.com/", ["data:", "", "", "", "example.com/", "", "", ""],
["javascript://example.com/", ["javascript:", "", "", "example.com/", "", "", ""],
["mailto://example.com/", ["mailto:", "", "", "", "example.com/", "", "", ""],
["http://example.com/", ["http:", "example.org", "", "", "foo/example.com/", "", "", ""],
["ftp://example.com/", ["ftp:", "example.com", "", "", "", ""],
["https://example.com/", ["https:", "example.com", "", "", "", ""],
["madeupscheme://example.com/", ["madeupscheme:", "", "", "example.com/", "", "", ""],
["file://example.com/", ["file:", "", "", "", "example.com/", "", "", ""],
["ftps://example.com/", ["ftps:", "", "", "", "example.com/", "", "", ""],
["gopher://example.com/", ["gopher:", "example.com", "", "", "", ""],
["ws://example.com/", ["ws:", "example.com", "", "", "", ""],
["wss://example.com/", ["wss:", "example.com", "", "", "", ""],
["data://example.com/", ["data:", "", "", "", "example.com/", "", "", ""],
["javascript://example.com/", ["javascript:", "", "", "example.com/", "", "", ""],
["mailto://example.com/", ["mailto:", "", "", "", "example.com/", "", "", ""],
End of Matches
(Result 12/1000+)=== Ignore similar [c]ontents/[u]ser/[r]epo/[f]ilename, [p]rint contents, [s]ave state, [a]dd to log, search
```

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

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

[i] Github query : https://api.github.com/search/code?q=yahoo access_key&sort=indexed&o=desc
[i] Status code : 200
[!] POSSIBLE AWS TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-09-10T13:40:08Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/[REDACTED]/cmd_bash.md
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]
[i] Github query : https://api.github.com/search/code?q=yahoo access_token&sort=indexed&o=desc
[i] Status code : 200
[!] POSSIBLE GOOGLE_FIREBASE_OR_MAPS TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-09-11T20:12:28Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/connectApp/[REDACTED]/app.js
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]
[!] POSSIBLE TWILIO TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-07-30T06:28:32Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/[REDACTED]/project.html
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]
```

¡EL PROPIO GITHUB!



- La opción de búsqueda de GitHub se puede usar para encontrar información privada en repositorios públicos
- Es una función muy potente que permite buscar por muchos términos
 - Como Google Hacking (Google Dorks), pero para código
 - ¡De hecho, mucha gente llama a esto **GitHub Dorks**!
- La imagen muestra varias búsquedas populares como ejemplo



Anton

@therceman



www.therceman.dev

GitHub Dorks for Finding Files

filename:manifest.xml
filename:travis.yml
filename:vim_settings.xml
filename:database
filename:prod.exs
filename:prod.secret.exs
filename:.npmrc_auth
filename:.dockercfg
filename:WebServers.xml
filename:.bash_history
filename:sftp-config.json
filename:sftp.json
filename:secrets.yml
filename:.esmtprc
filename:passwd
filename:LocalSettings.php

filename:config.php
filename:config.inc.php
filename:prod.secret.exs
filename:configuration.php
filename:.sh_history
filename:shadow
filename:proftpdpasswd
filename:pgpass
filename:idea14.key
filename:hub
filename:.bash_profile
filename:.env
filename:wp-config.php
filename:credentials
filename:id_rsa
filename:id_dsa

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

GitHub Dorks for Finding API Keys, Tokens and Passwords

api_key
authorization_bearer:
oauth
auth
authentication
client_secret
api_token:
client_id

OTP
HOMEBREW_GITHUB_API_TOKEN
SF_USERNAME
HEROKU_API_KEY
JEKYLL_GITHUB_TOKEN
shodan_api_key
api.forecast.io

password
user_password
user_pass
passcode
client_secret
secret
password hash
user auth

GitHub Dorks Automation Tools

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

LISTA DE LOGROS PARA AUTOEVALUACIÓN: SEMINARIO 1

?

- Entender el concepto OSINT
- Entender qué tipos de dispositivos podemos encontrar en Internet
- Saber qué tipo de información no debe poner en el código fuente
- Saber cómo usar las herramientas OSINT Shodan y Censys para encontrar máquinas de un objetivo
- Saber cómo usar Google Hacking para encontrar información de un objetivo
- Conocer múltiples herramientas OSINT que trabajan con información personal de individuos / empresas
- Conocer herramientas para estudiar el código en repositorios públicos
- Saber cómo estudiar un objetivo con Google Hacking
- Saber cómo estudiar a una persona por RRSS y el problema que hay con las herramientas que hacen este tipo de actividades

SEMINARIO 1

HERRAMIENTAS PARA INVESTIGAR EN INTERNET

