SEMINAR 1
TOOLS FOR INTERNET RESEARCH

Getting information about machines, people and...source code!

JOSÉ MANUEL REDONDO LÓPEZ *"S-81 ISAAC PERAL"* PROJECT V3.0

Source: zona-militar.com

Logo: @creative_vanesa (*Instagram*)

Departamento de Informática
Universidad de Oviedo

Universidad de Oviedo

INTRODUCTION

José Manuel
Redondo López

- **You may wonder why all current focus on security these days…**
  - Even with no technical knowledge, you can have a lot of information about people / companies that can be exploited to obtain advantages
  - All is over the Internet for you to pick up…if you know where (and how) to look
  - This seminar will show you tools explaining how to do it
  - If you are serious about uses (and misuses) of the information over the Internet, you should enroll in the optional course Web Information Systems (SIW)
    - If you contact Daniel Gayo, he can give you access to the course materials and videos for you to check!
- **Let's do something that does not require a lot of technical skill ☺**
  - **OSINT (Open-Source INTelligence)**
  - Some of these applications will be used in laboratories
- **NOTE: If, using these tools, you find yourself exposing too many information on Internet ("egosurfing"), there are ways of recovering your privacy**
  - You can follow this guide: https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954?gi=57af4dc583d

INDEX

< Go to Index

Source: zona-militar.com

OSINT AGAINST THE MACHINE

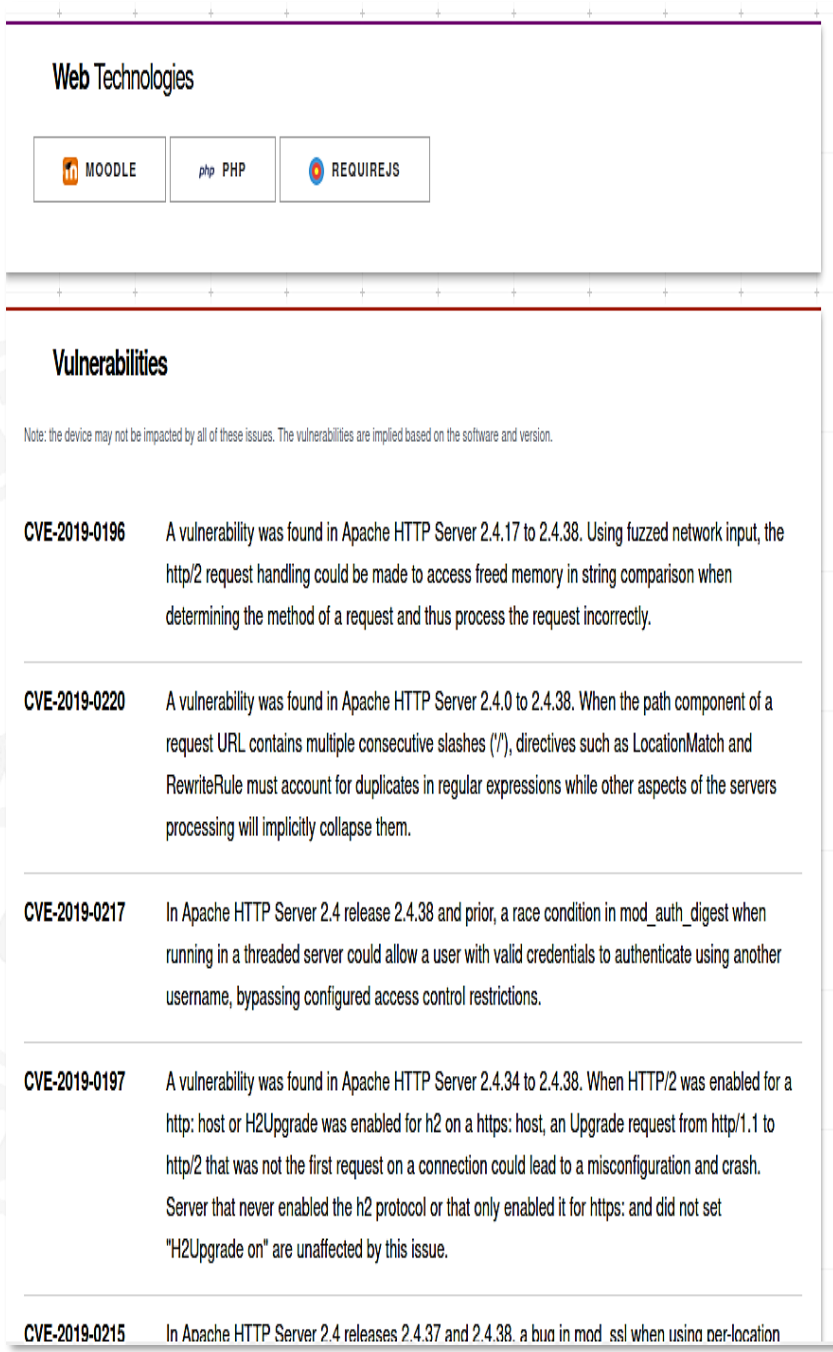
Investigating machines using only public information

SHODAN

http://www.shodanhq.com/

José Manuel
Redondo López

- **Machine (not web) search engine**
  - Routers, servers, cameras... (IoT)
  - Reports the type of service found, version, etc.
  - Finds SCADA (Supervisory Control And Data Acquisition)
    - Industrial engineering devices
- **Search for up to 10 devices**
  - Free registration allows more and using logical operators
  - Used to view devices exposed to the Internet and if they pose a danger
    - They have management software that can be accessed, and attacked
- **Tutorials**
  - 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 http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

CVE-2019-0220 A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

CVE-2019-0217 In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

CVE-2019-0197 A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.

CVE-2019-0215 In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location

Apache httpd 2.4.38

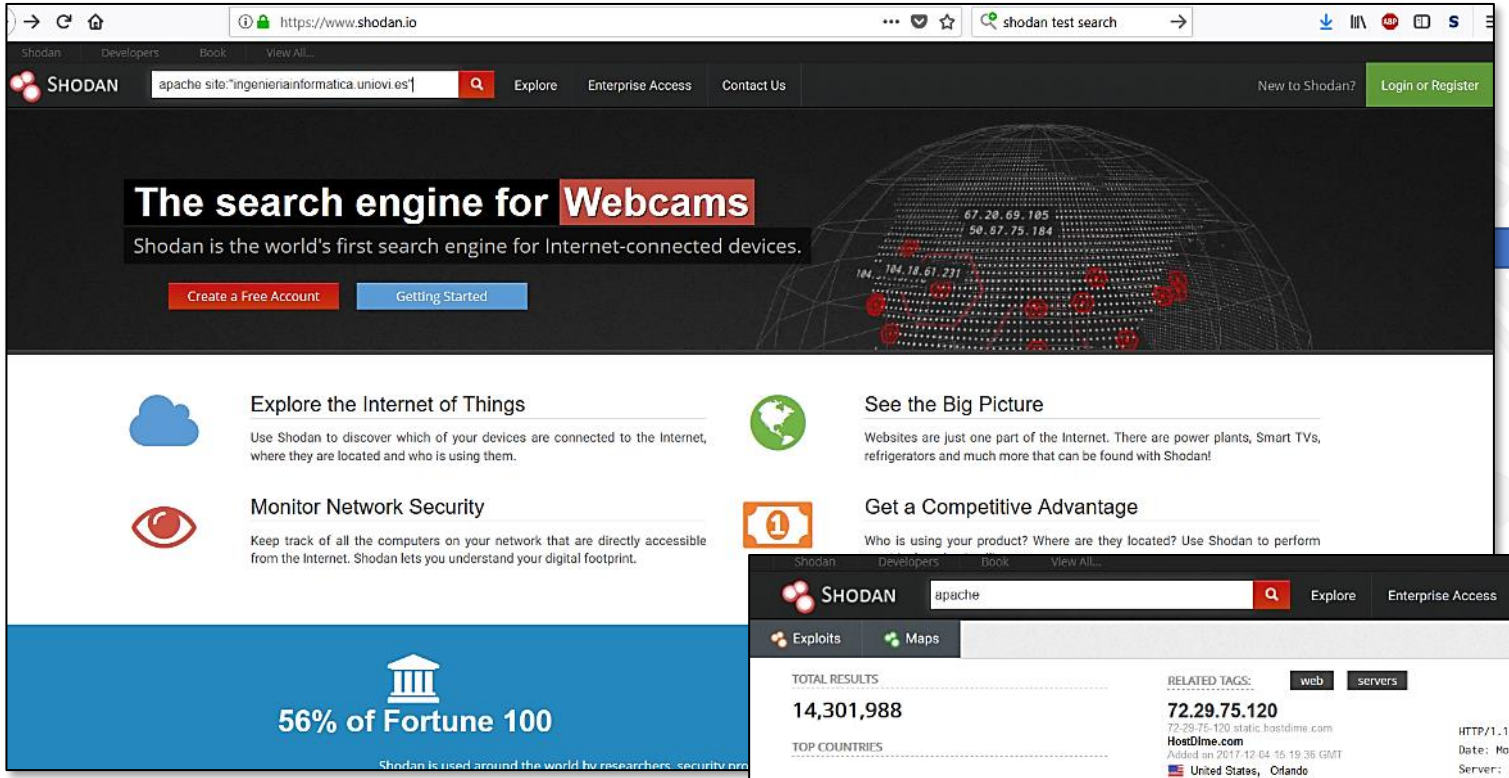
```
HTTP/1.1 200 OK
Date: Mon, 21 Feb 2022 02:36:16 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: MoodleSession=j25o9m0cman8dkarptfvspemup; path=/; secure
Expires:
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Content-Language: es
Content-Script-Type: text/javascript
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
```

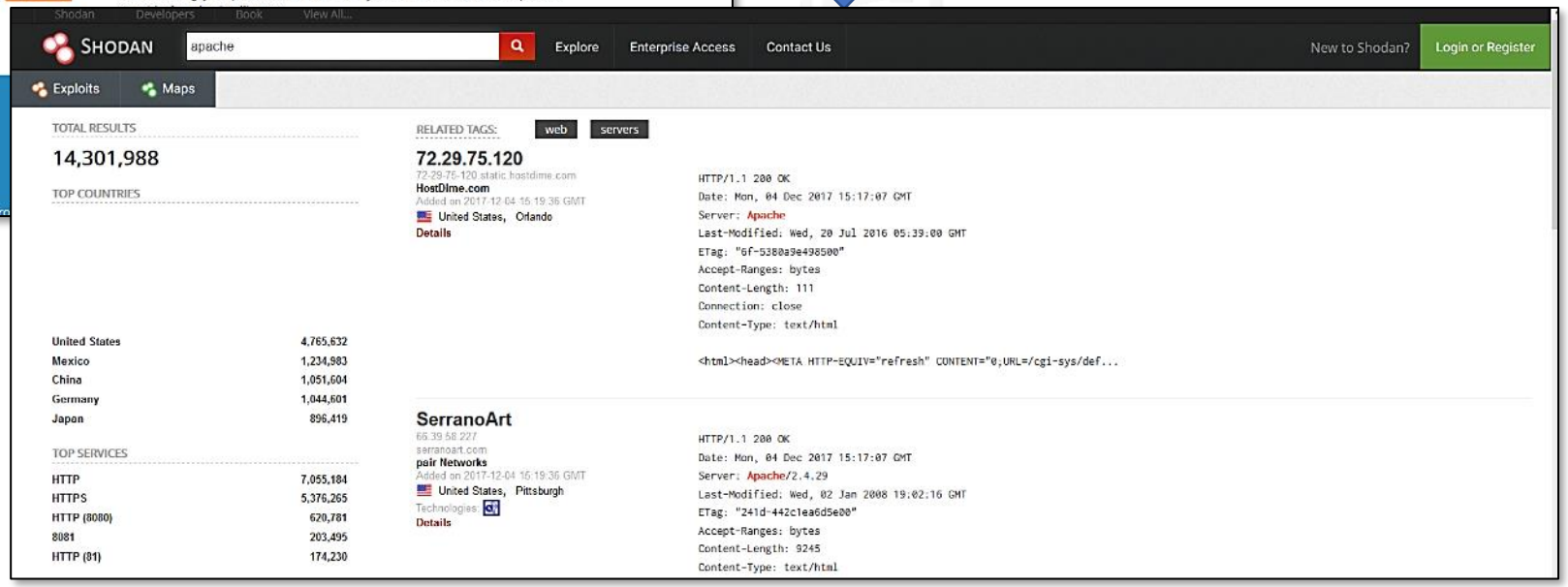
SSL Certificate

```
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:f7:82:95:c6:cd:96:f7:3a:2d:ae:48:
                    fe:8a:5a:df:cb:d5:52:eb:e3:d1:b3:87:b2:35:67:
                    5f:0d:e1:44:85:3b:c1:3f:a0:43:62:86:9b:3f:ea:
```

SHODAN

José Manuel
Redondo López





Search these service's banners

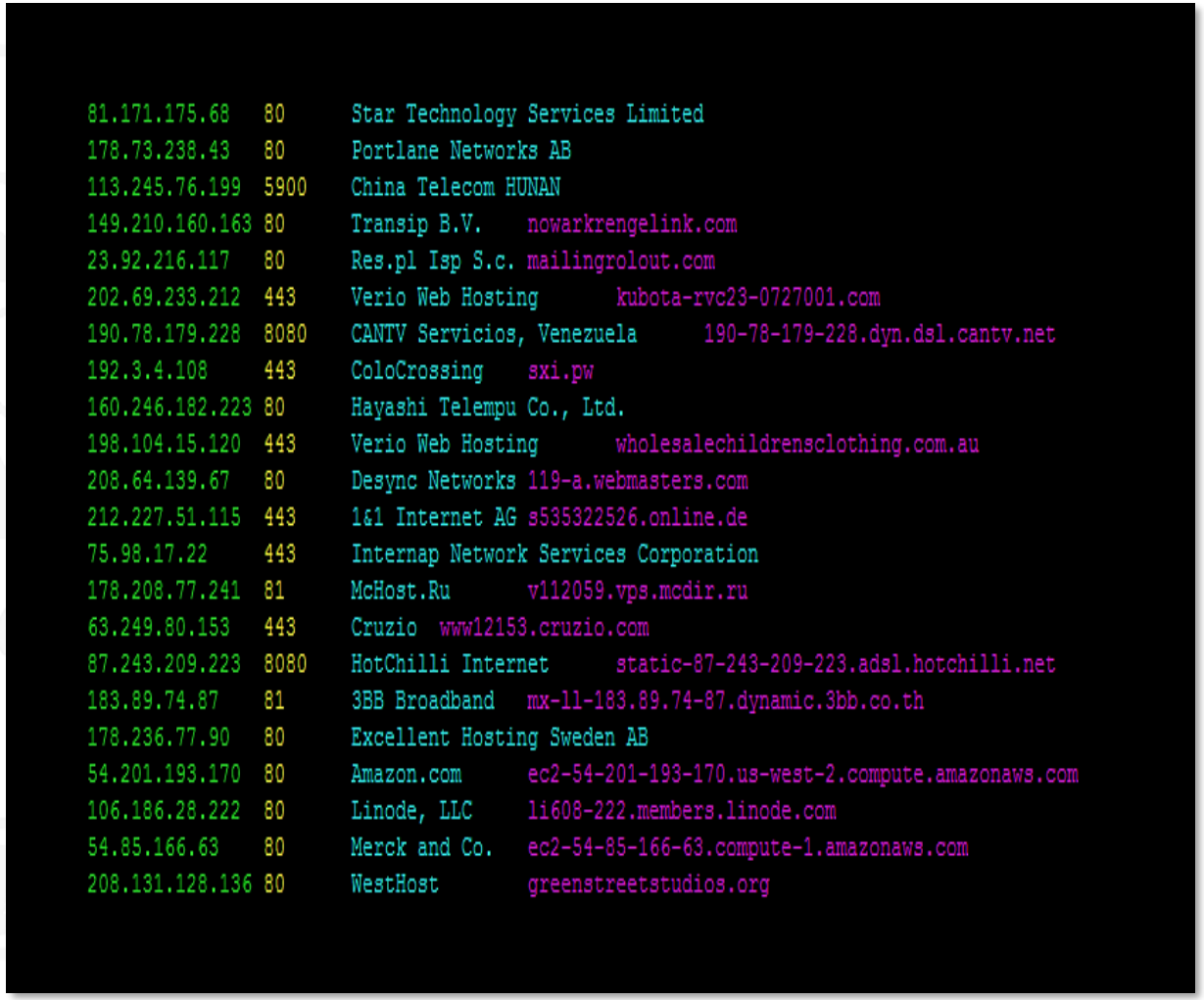
- HTTP/HTTPS
- FTP
- SSH
- Telnet
- SNMP
- SIP (IP telephony)
- RTSP (video *streaming* and webcams)
- …

SHODAN CLI

https://cli.shodan.io/

José Manuel
Redondo López

- **Python library providing Shodan's capabilities from the command line**
  - Useful in GUI-less contexts
- **Allows to integrate Shodan's features into our own scripts or programs**
  - Or automate pentesting tasks including Shodan
  - The official website has usage examples
- **Its capabilities are equivalent to the web interface**
- **Set of useful searches**
  - https://github.com/jakejarvis/awesome-shodan-queries



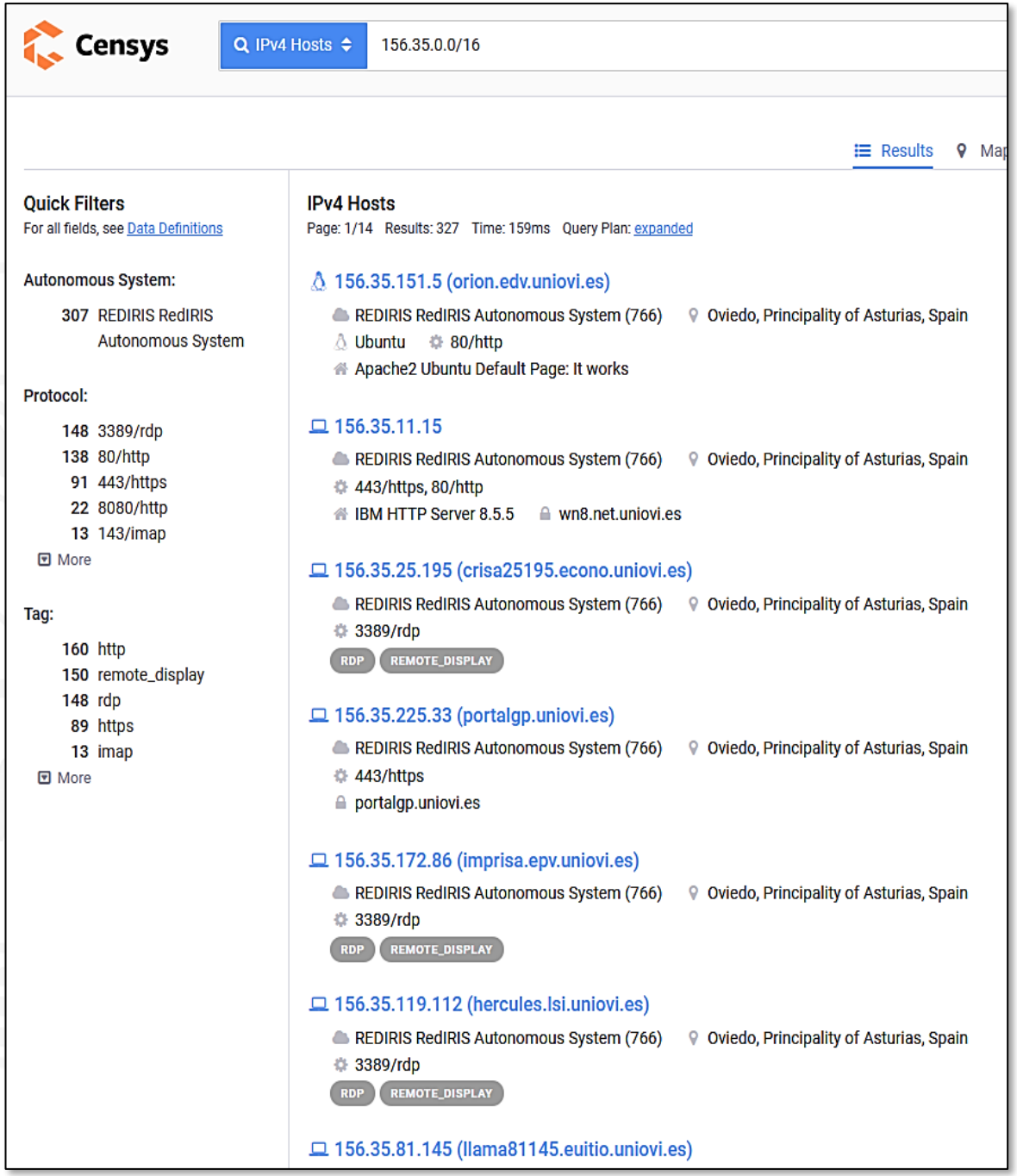
```
81.171.175.68   80     Star Technology Services Limited
178.73.238.43   80     Portlane Networks AB
113.245.76.199  5900   China Telecom HUNAN
149.210.160.163 80     Transip B.V.    nowarkrengelink.com
23.92.216.117   80     Res.pl Isp S.c. mailingrolout.com
202.69.233.212  443    Verio Web Hosting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

CENSYS

https://censys.io/

José Manuel
Redondo López

- **Like Shodan, but with structured info**
  - Searches server features: interesting running services (RDP), OS/web server banners…
  - Multiple search criteria
    - IP (v4 only) and networks: https://censys.io/ipv4/
    - Website domain names: https://censys.io/domain?q=
    - Certificates: https://censys.io/certificates?q=
- **Search Tutorial**
  - https://developerinsider.co/censys-find-and-analyze-any-server-and-device-on-the-internet/
- **A similar tool is Onhype.io:**
  - https://fwhibbit.es/descubrimiento-y-recopilacion-de-activos-con-onyphe-io
  - Comparison with other tools (ZMap, Mr Looquer)
    - https://www.dragonjar.org/shodan-vs-scans-io-vs-censys-io-vs-zmap-vs-mr-looquer.xhtml



José Manuel
Redondo López

(1) Using Shodan to find Uniovi-bound resources

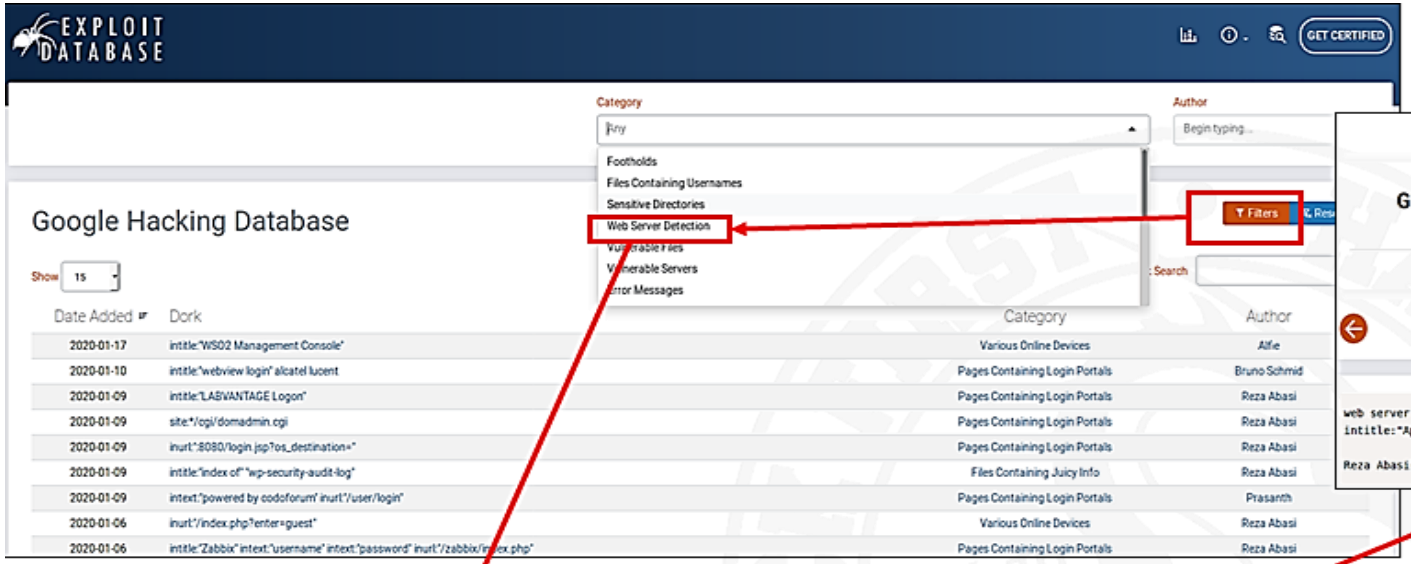
Google hacking or "Google dorking"

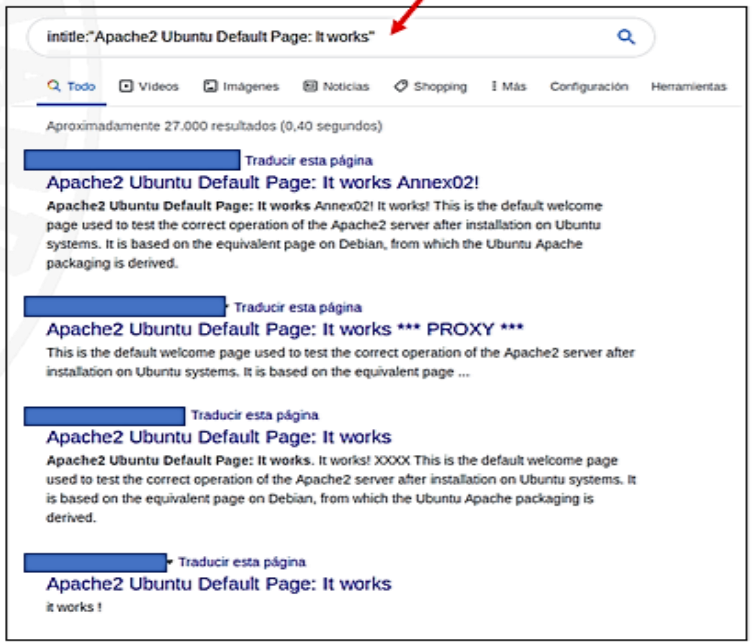
José Manuel
Redondo López

- **Ability of doing certain searches that reveal compromising information**
  - Using standard search engines (normally targeting a concrete domain with the `site:` operator)
  - These queries find information leading to vulnerabilities, configuration issues, or facilitate an attack
  - It can be done in other search engines too (although Google is the most used one)
- **There is a database of organized prebuilt searches: Google Hacking Database**
  - These are called "Google Dorks" : https://www.exploit-db.com/google-hacking-database
  - Choose the right search category: each one represents a possible vulnerability!
  - Search the target with the chosen query (`site:`)
- **"Dorking" can also be used with other products**
  - https://github.com/cipher387/Dorks-collections-list
- **Examples**
  - 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: PROCESS

José Manuel
Redondo López





FINAL RECON

https://github.com/thewhiteh4t/FinalRecon

José Manuel
Redondo López

- **Python script for web reconnaissance**
- **Implements a lot of features to create a full profile of a web page server and its contents**
  - DNS and WHOIS information
  - Full crawler
  - Traceroute
  - Directory search
  - Port scanning the server
- **Tutorial:**
  - https://hakin9.org/final-recon-osint-tool-for-all-in-one-web- reconnaissance/

```
python3 finalrecon.py -h

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

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

positional arguments:
  url         Target URL

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

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

uDork

https://github.com/m3n0sd0n4ld/uDork

José Manuel
Redondo López

- **Bash script that uses Google Hacking to obtain various types of sensitive information**
  - Files or directories
  - Find IoT devices
  - Web application framework / CMS versions
  - …
- **Tutorial**
  - https://www.enhacke.com/2020/03/21/udork-google-hacking-tool/

```
 _____                _
|  __ \              | |
| |  | | ___  _ __ | | __
| |  | |/ _ \| '__| |/ /
| |__| | (_) | |  |   <
|_____/ \___/|_|  |_|\_\ v.2.0
       by M3n0sD0n4ld - (@David_Uton)

-------------------------------------------------------------------------
[!] The results will appear below. This may take several minutes, please wait ...

Domain/IP: nasa.gov
Find links with: pdf
-------------------------------------------------------------------------
https://www.sti.nasa.gov/thesvol2.pdf
https://www.sti.nasa.gov/thesvol1.pdf
https://oig.nasa.gov/docs/MC-2018.pdf
https://www.nasa.gov/centers/dryden/pdf/88798main_srfcs.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A10_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A14_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A07_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A15_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A09_PressKit.pdf
https://www.nasa.gov/specials/apollo50th/pdf/A08_PressKit.pdf
-------------------------------------------------------------------------
Files pdf found: 10

Domain/IP: nasa.gov
Find links with: xml
-------------------------------------------------------------------------
https://www.nasa.gov/sitemap.xml
-------------------------------------------------------------------------
Files xml found: 1

Domain/IP: nasa.gov
Find links with: xls
-------------------------------------------------------------------------
https://airbornescience.nasa.gov/instrument/all/export
-------------------------------------------------------------------------
Files xls found: 1

Domain/IP: nasa.gov
Find links with: txt
-------------------------------------------------------------------------
https://www.nasa.gov/378571main_0728NASAMeeting.txt
https://seabass.gsfc.nasa.gov/archive/INIDEP_LPPB/EPEA/archive/pigments/EPEA_PD2012-03_HPLC.txt
https://seabass.gsfc.nasa.gov/archive/MLI/larouche/optique_st_laurent/2000_15/archive/SPMR0015104_CASTB.txt
-------------------------------------------------------------------------
```

< Go to Index

Source: zona-militar.com

Social Networks >

Data Integration >

OSINT AGAINST THE PEOPLE

Investigating people using public information only

Social networks

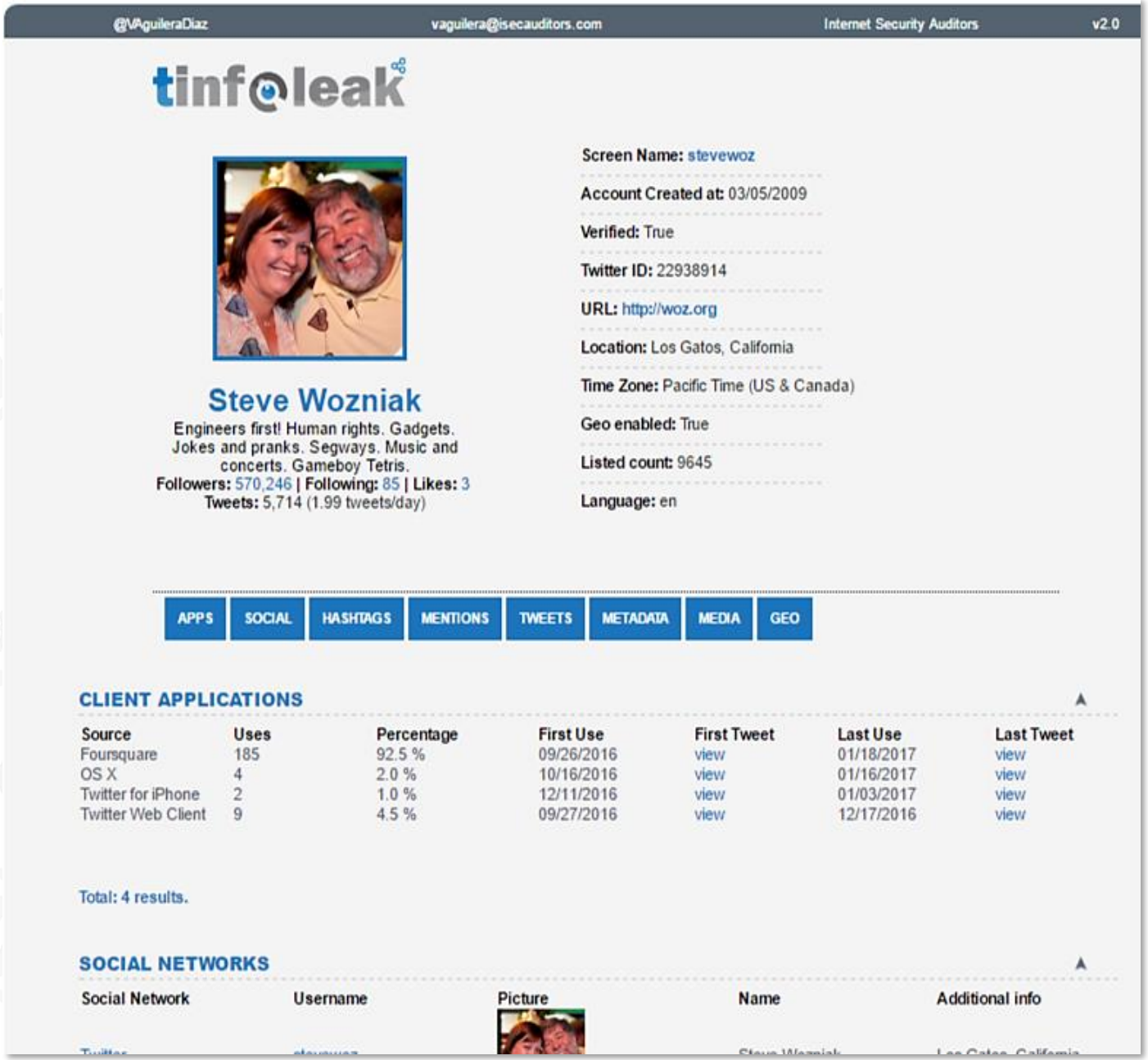
Know what the people do...and post ☺

TINFOLEAK

https://github.com/vaguileradiaz/tinfoleak

José Manuel Redondo López

- **Analyzes / extracts information from open Twitter accounts**
  - Searches messages using terms
  - Has multiple actions to find data
  - Typical tool to search "compromising" tweets of public personalities
    - Very frequent nowadays…
- **Requires a Twitter API key**
  - Hence an active Twitter account
- **Links (installation, help)**
  - https://ciberpatrulla.com/tutorial-tinfoleak/
  - https://www.isecauditors.com/herramientas-tinfoleak
  - http://www.noise-sv.com/tutorial-de-tinfoleak/



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

TWINT

https://github.com/twintproject/twint

José Manuel
Redondo López

- **Python script**
  - Hence usable from our own code!
- **Like Tinfoleak, but uses web scrapping techniques**
  - Instead of the Twitter API: **No need of a Twitter API key / account!**
  - No rate-limited
  - Maximum of around 3200 tweets per query, due to scroll limitations
  - Very easy to set up and use
- **Similar tools exist for other social networks**
  - Facebook, LinkedIn, Instagram…

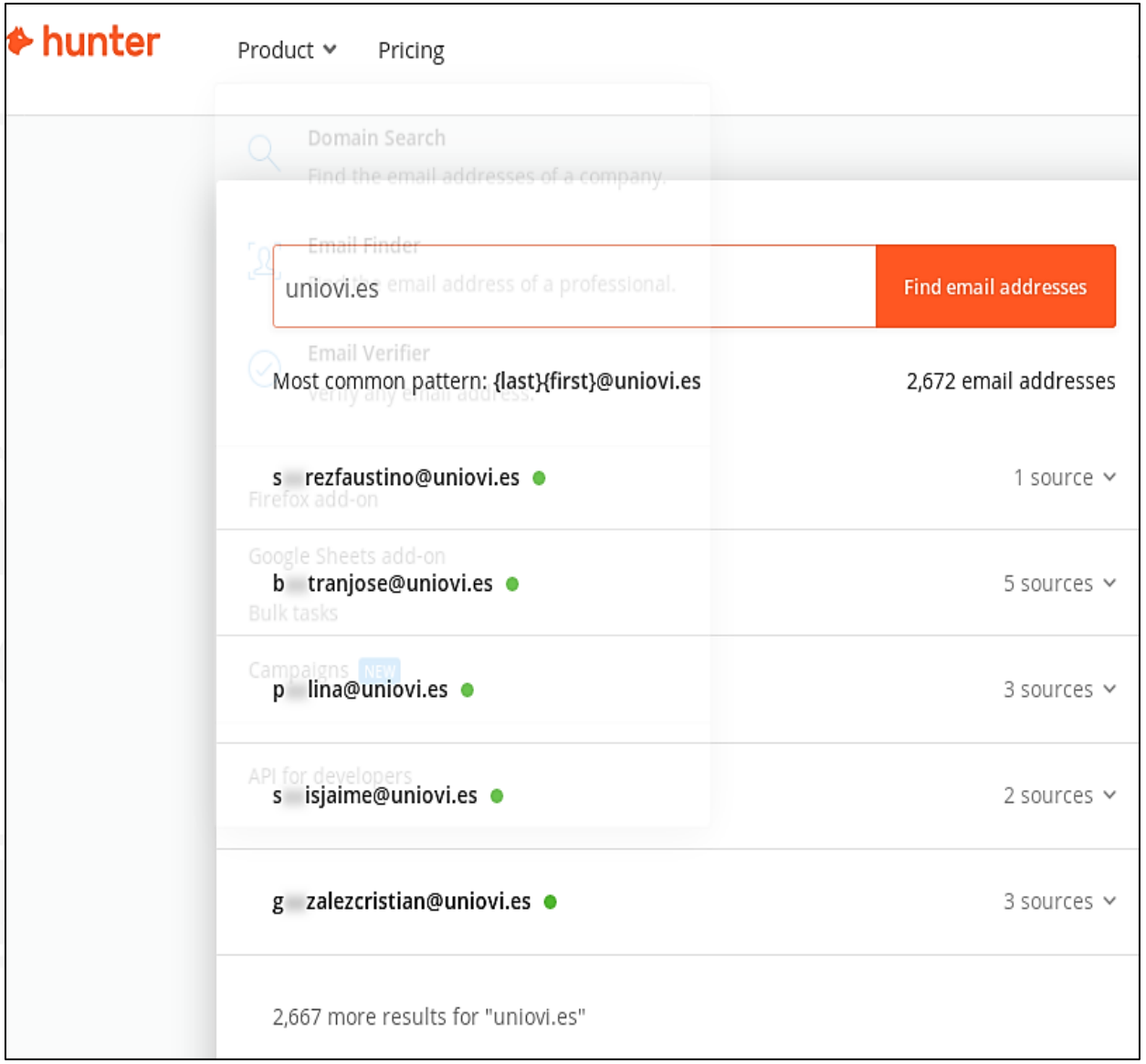
```
twint -u <username> - Scrape all the Tweets from user's timeline.
twint -u <username> -s pineapple - Scrape all Tweets from the user's timeline containing pineapple.
twint -s pineapple - Collect every Tweet containing pineapple from everyone's Tweets.
twint -u <username> --year 2014 - Collect Tweets that were tweeted before 2014.
twint -u <username> --since "2015-12-20 20:30:15" - Collect Tweets that were tweeted since 2015-12-20 20:30:15.
twint -u <username> --since 2015-12-20 - Collect Tweets that were tweeted since 2015-12-20 00:00:00.
twint -u <username> -o file.txt - Scrape Tweets and save to file.txt.
twint -u <username> -o file.csv --csv - Scrape Tweets and save as a csv file.
twint -u <username> --email --phone - Show Tweets that might have phone numbers or email addresses.
twint -s "Donald Trump" --verified - Display Tweets by verified users that Tweeted about Donald Trump.
twint -g="48.880048,2.385939,1km" -o file.csv --csv - Scrape Tweets from a radius of 1km around a place in Paris and export them to a csv file.
twint -u <username> -es localhost:9200 - Output Tweets to Elasticsearch
twint -u <username> -o file.json --json - Scrape Tweets and save as a json file.
twint -u <username> --database tweets.db - Save Tweets to a SQLite database.
twint -u <username> --followers - Scrape a Twitter user's followers.
twint -u <username> --following - Scrape who a Twitter user follows.
twint -u <username> --favorites - Collect all the Tweets a user has favorited (gathers ~3200 tweet).
twint -u <username> --following --user-full - Collect full user information a person follows
twint -u <username> --profile-full - Use a slow, but effective method to gather Tweets from a user's profile (Gathers ~3200 Tweets, Including Retweets).
twint -u <username> --retweets - Use a quick method to gather the last 900 Tweets (that includes retweets) from a user's profile.
twint -u <username> --resume resume_file.txt - Resume a search starting from the last saved scroll-id.
```

HUNTER.IO

https://hunter.io/

José Manuel
Redondo López

- **Website that allows you to discover email addresses related to domains / companies**
- **With them, OSINT attacks, phising attempts or APTs (Advanced Persistent Threats) can be started**
- **It is not a free service, but a free registration enable a limited usage of its features**
  - Complete results
  - CSV downloads
  - Up to 50 searches/month



Social Mapper

https://github.com/Greenwolf/social_mapper

José Manuel Redondo López

- **This Python script correlates users in different social media using facial recognition**
  - Can be used to locate fake users that use the same profile image in different social networks
  - It has other usages for Red Team operations
- **Accepts different input types**
  - An organization's name, searching via LinkedIn
  - A folder of named images
  - A CSV with names and URLs to online images
  - Works with Facebook, Instagram, Twitter, LinkedIn, VKontakte (Russian “Facebook”), Weibo, Douban…
- **Results can be used with Maltego**
  - Seen later

```
4 parameters must be provided. 3 are an input format, the input file or folder and the basic running mode:
-f, --format      : Specify if the -i, --input is a 'name', 'csv', 'imagefolder' or 'socialmapper' resume file
-i, --input       : The company name, a CSV file, imagefolder or Social Mapper HTML file to feed into Social
Mapper
-m, --mode        : 'fast' or 'accurate' allows you to choose to skip potential targets after a first likely
match is found, in some cases potentially speeding up the program x20

Additionally, at least one social media site to check must be selected:
-a, --all                         : Selects all of the options below and checks every site that Social Mapper
has credentials for
-fb, --facebook                   : Check Facebook
-tw, --twitter                    : Check Twitter
-ig, --instagram                  : Check Instagram
-li, --linkedin                   : Check LinkedIn
-gp, --googleplus                 : Check Google Plus
-vk, --vkontakte                  : Check VKontakte
-wb, --weibo                      : Check Weibo
-db, --douban                     : Check Douban

Additional optional parameters can also be set:
-t, --threshold    : Customizes the facial recognition threshold for matches, this can be seen as the match
accuracy. Default is 'standard', but can be set to 'loose', 'standard', 'strict' or 'superstrict'. For example
'loose' will find more matches, but some may be incorrect. While 'strict' may find less matches but also contain
less false positives in the final report.
-cid, --companyid : Additional parameter to add in a LinkedIn Company ID for if name searches are not picking the
correct company.
-s, --showbrowser : Makes the Firefox browser visible so you can see the searches performed. Useful for debugging.
-w, --waitafterlogin : Wait for user to press Enter after login to give time to enter 2FA codes. Must use with -s
-v, --version : Display current version.
-vv, --verbose : Verbose Mode (Useful for Debugging)
-e, --email : Provide a fuzzy email format like "<f><last>@domain.com" to generate additional CSV files for each
site with firstname, lastname, fullname, email, profileURL, photoURL. These can be fed into phishing frameworks
such as Gophish or Lucy.

Example Runs
* A quick run for Facebook and Twitter on some targets you have in an imagefolder, that you plan to manually
review and don't mind some false positives: python3 social_mapper.py -f imagefolder -i ./Input-
Examples/imagefolder/ -m fast -fb -tw
* The same as above but with the browser showing, and waiting enabled to allow a user to enter 2FA codes and
manually rectify changed login processes: python3 social_mapper.py -f imagefolder -i ./Input-Examples/imagefolder/
-m fast -fb -tw -s -w
* An exhaustive run on a large company where false positives must be kept to a minimum:
python3 social_mapper.py -f company -i "Evil Corp LLC" -m accurate -a -t strict
* A large run that needs to be split over multiple sessions due to time, the first run doing LinkedIn and
Facebook, with the second resuming and filling in Twitter, Google Plus and Instagram:
python3 social_mapper.py -f company -i "Evil Corp LLC" -m accurate -li -fb
python3 social_mapper.py -f socialmapper -i ./Evil-Corp-LLC-social-mapper-linkedin-facebook.html -m accurate -tw -
gp -ig
* A quick run (~5min) without facial recognition to generate a CSV full of names, email addresses, profiles and
photo links from up to 1000 people pulled out of a LinkedIn company, where the email format is known to be
"firstname.lastname": python3 social_mapper.py -f company -i "Evil Corp LLC" -m accurate -li -e
"<first>.<last>@evilcorpllc.com"
```

Project Sherlock

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

José Manuel Redondo López

- **Finds a username on lots of different social networks and webpages**
  - More than 320!
- **It is very common to find users with the same name on different social networks**
  - We can use it to collect information from different sources about the same person
  - This may reveal data about people with closed profiles only in a network, but an open profile in another one
- **Basic usage is simple**
  - `python3 pherlock.py <username>`

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

User reconnaissance integration / from multiple sources

Aggregating user data

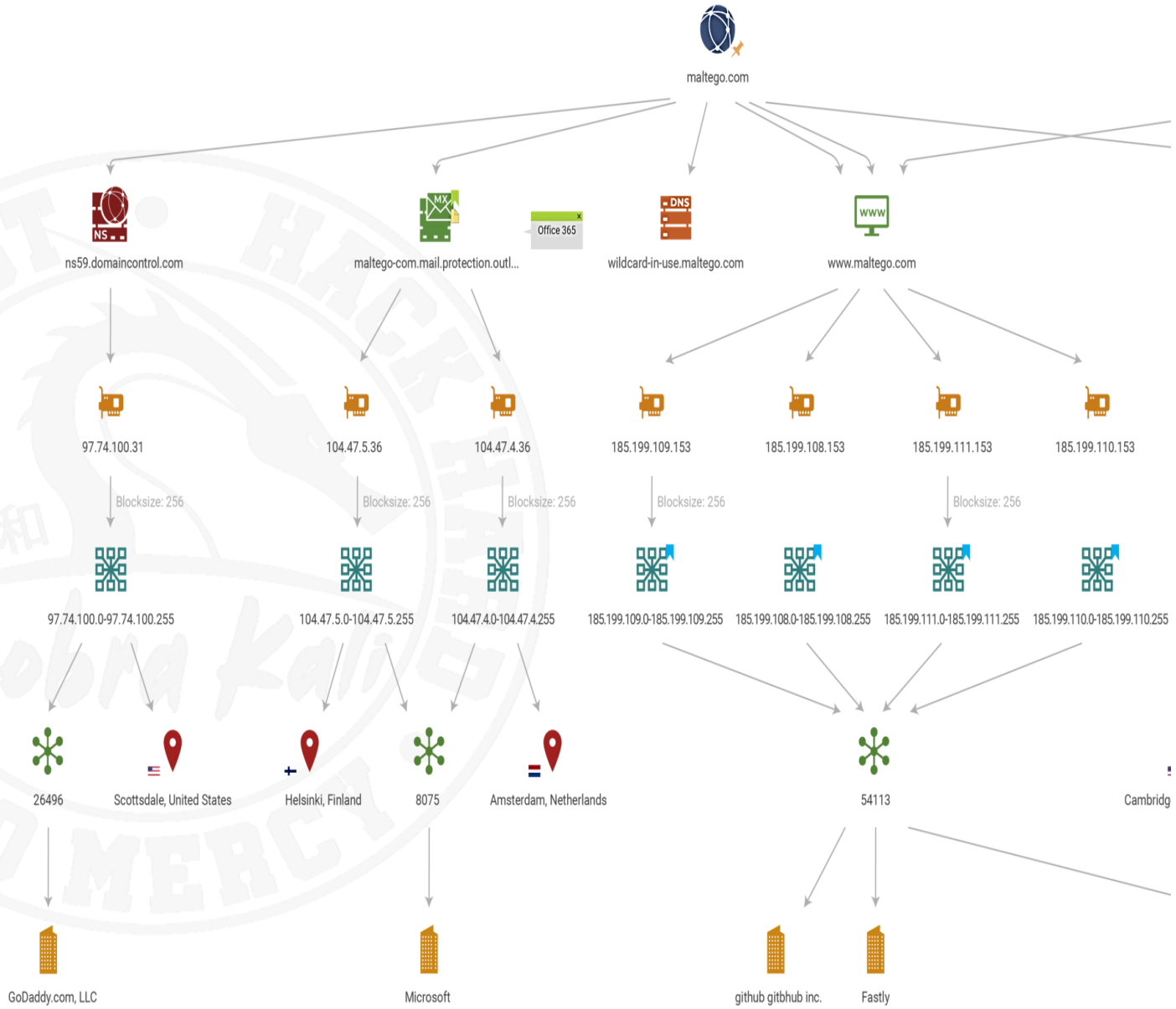
MALTEGO

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

José Manuel Redondo López

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

- **Collects information from Internet entities**
  - Creates custom entities that represent any kind of information
  - Specializes in finding relationships between them
    - Social networks, computer networks, domains...
  - Uses DNS and `whois` records, search engines, known social networks, APIs... as sources
- **Tutorials**
  - https://www.fwhibbit.es/introduccion-a-maltego
  - https://ciberpatrulla.com/maltego/
  - www.elladodelmal.com/2010/08/mineria-de-datos-con-maltego-1-de-2.html

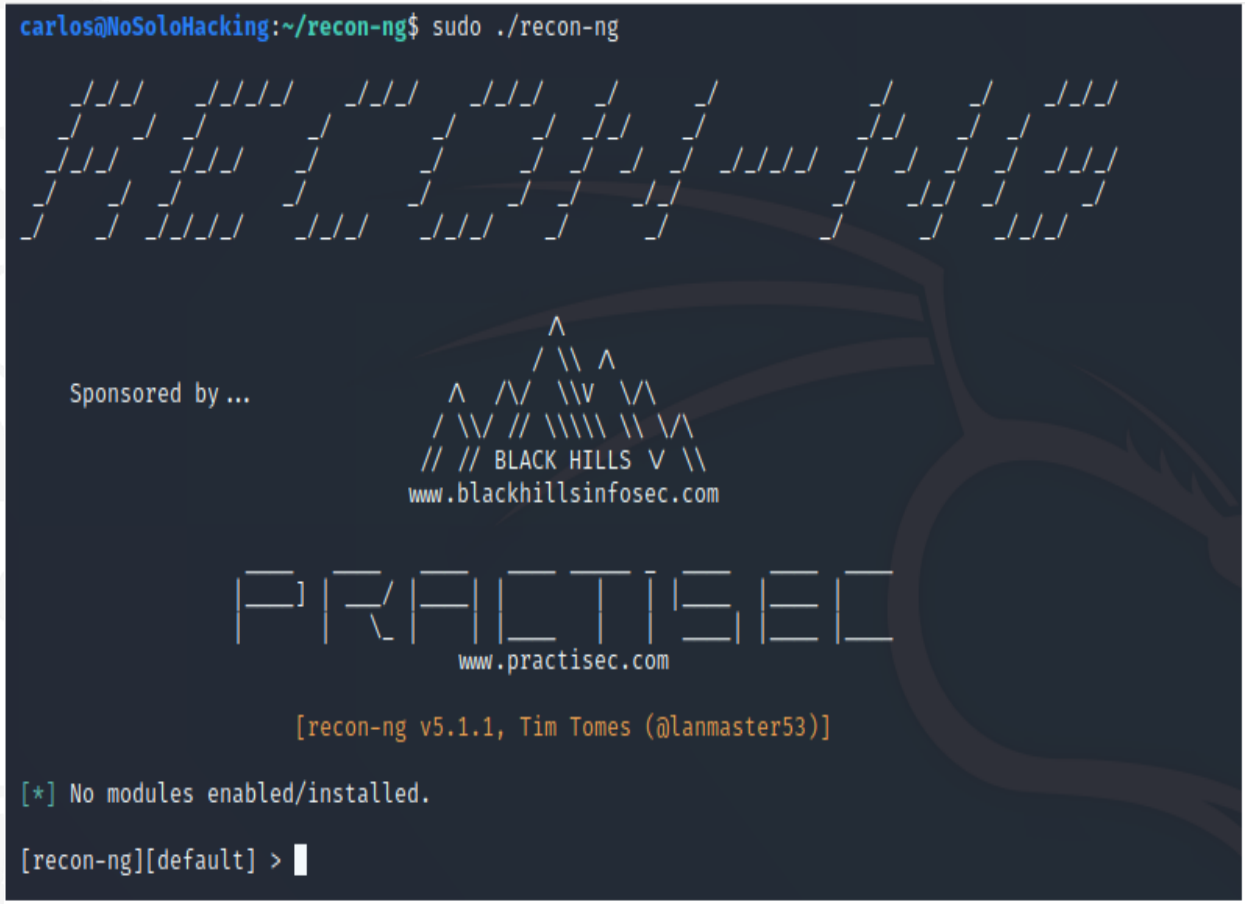


RECON-NG

https://kali-linux.net/article/recon-ng/

José Manuel
Redondo López

- **Used for recollecting information about users from different sources**
- **It has modules to search on different sources of information**
  - Search engines, APIs...
- **Copies Metasploit UI to make it easier for people who are already familiar with it**
- **Tutorials**
  - https://hackertarget.com/recon-ng-tutorial/
  - https://noticiasseguridad.com/tutoriales/recon-ng-herramienta-para-recoleccion-de-informacion/



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

ODIN

https://github.com/chrismaddalena/ODIN

José Manuel
Redondo López

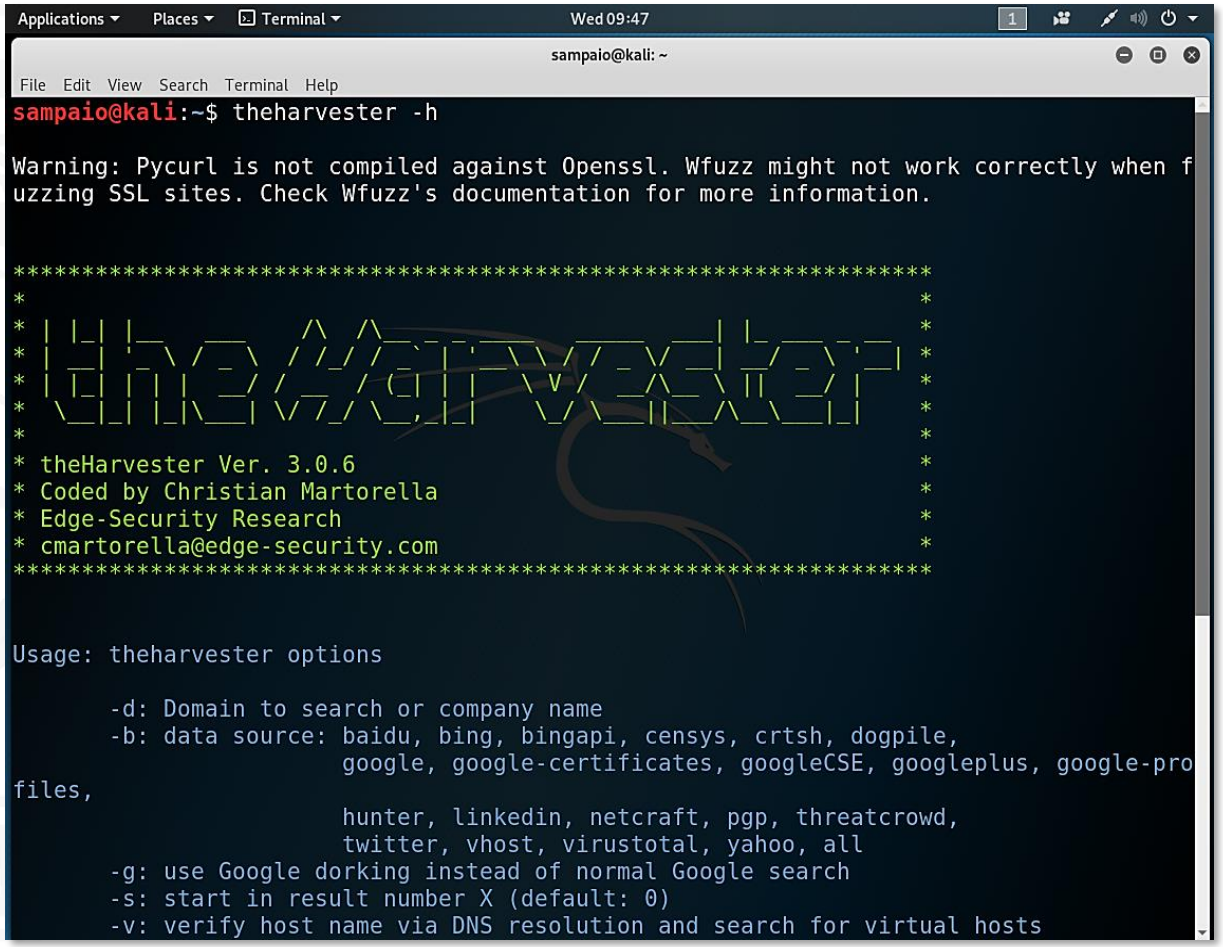
- **Automated discovery and cataloging tool for network, email and social media assets**
- **Includes employees / assets on cloud platforms**
- **Creates reports that can be saved in a BBDD for further research**
- **More information**
  - https://www.gurudelainformatica.es/2019/05/descubrimiento-y-catalogacion.html
- **Similar applications**
  - https://blog.segu-info.com.ar/2019/05/aplicaciones-para-osint.html?m=0

The Harvester

https://github.com/laramies/theHarvester

José Manuel
Redondo López

- **Obtains data of a certain target using many different sites as sources**
  - You get a lot of information from public sources: emails, names, subdomains, IPs, URLs...
  - Uses known search engines for different kinds of information
    - baidu, bing, bingapi, censys, Comodo Certificate search, dnsdumpster, dogpile, duckduckgo, github-code, Google (optional Google dorking), google-certificates, hunter, intelx, Linkedin, Netcraft Data Mining, securityTrails (DNS history information), Shodan, threatcrowd, trello, Twitter, Bing virtual hosts search, Virustotal, and Yahoo search engine
- **Also, information from DNS**
  - Brute force, reverse lookup, TLD expansion…
- **Tutorial**
  - https://www.welivesecurity.com/la-es/2015/04/08/the-harvester-riesgo-nformacion-publica/

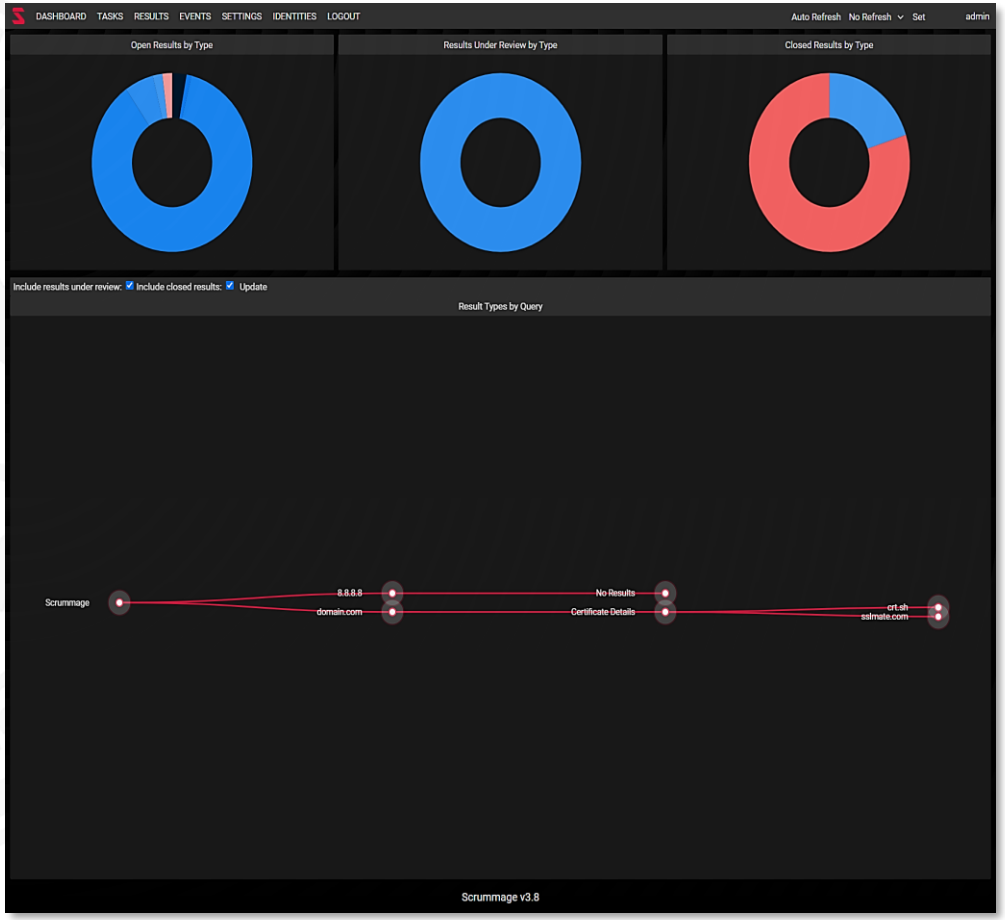


SCRUMMAGE

https://github.com/matamorphosis/Scrummage

José Manuel
Redondo López

- **Centralizes OSINT scans**
  - Provides a high-level view of sites with information about a target
- **Implements plugins to customize the type of scans and optimize resource usage**
- **Such plugins provide diverse capabilities**
  - Blockchain search
  - Domain fuzzing
  - Twitter analytics
  - Instagram search
  - Search on Have I Been Pwned? (https://haveibeenpwned.com/)
    - In case any account identities have been leaked …
- **Similar tools**
  - OSINT Framework: https://github.com/lockfale/osint-framework
  - Scumblr: https://portunreachable.com/automated-osint-with-scumblr-a4d81a048e54?gi=ae6ebac43a92

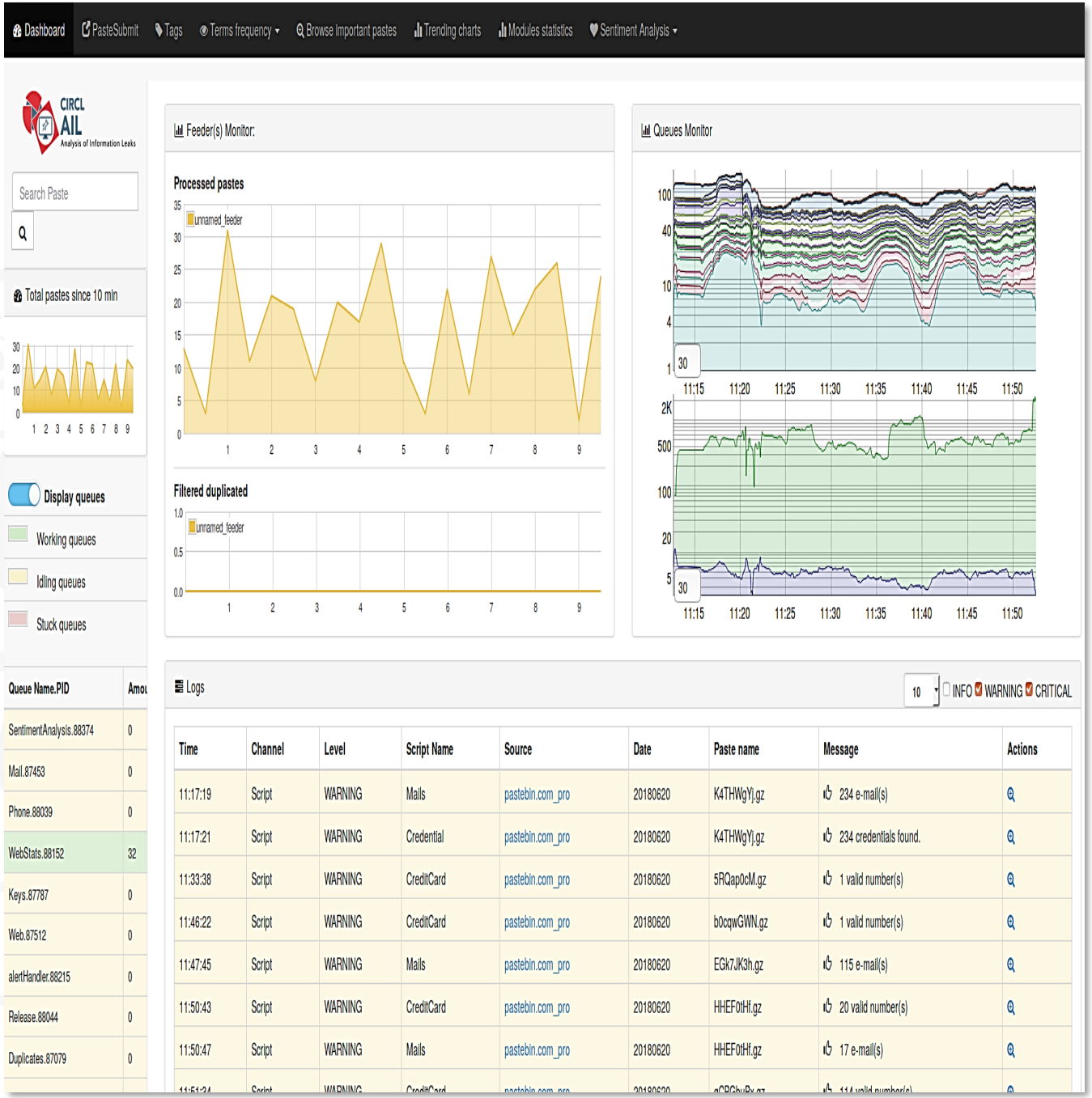


AIL Framework

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

José Manuel
Redondo López

- **Highly modular framework that analyzes filtered information**
  - From unstructured sources
  - A popular source is Pastebin
- **Its highly modular so it could be extended**
  - And used to mine and process private information of different kinds
  - And therefore, detect and prevent information leakage
- **To find out more**
  - https://www.kitploit.com/2019/08/ail-framework-framework-for-analysis-of.html



More OSINT tools...

José Manuel
Redondo López

- **OSINT's techniques are very popular and powerful due to the information they can find**
  - There are a huge number of tools that get information from different media and social networks on Internet
  - It's very difficult to list them all
- **There's a classified list of tools available: https://ciberpatrulla.com/links/**
  - This web is probably the most complete repository on OSINT tools
  - It contains hundreds of tools classified for its basic usefulness in one of the operations that contemplates the discipline of OSINT
  - Social networks, vehicles, phones, documents... 38+ categories of tools!

Do you have examples?

José Manuel
Redondo López

- **With such a number of tools available, it is very easy to get lost when starting an OSINT research**
- **Therefore, it is best to see examples of how to make one**
- **You can follow this four-part tutorial**
  - https://delta.navisec.io/osint-for-pentesters-part-1-passive-recon-and-asset-discovery/
  - https://delta.navisec.io/osint-for-pentesters-part-2-linkedin-is-not-just-for-jobs/
  - https://delta.navisec.io/osint-for-pentesters-part-3-password-spraying-methodology/
  - https://delta.navisec.io/a-pentesters-guide-part-4-grabbing-hashes-and-forging-external-footholds/
- **Or this OSINT guide**
  - https://www.hackers-arise.com/osint
- **We can find more tools in this web page**
  - Metadata extraction, geolocation, subdomain extraction…
  - https://derechodelared.com/herramientas-osint-recopilatorio/

José Manuel
Redondo López

(1) Using Google Hacking to find Uniovi-bound resources

(2) Using Tinfoleak

How to obtain a Twitter API Key & tutorial: http://www.noise-sv.com/tutorial-de-tinfoleak/

< Go to Index

Source: zona-militar.com

OSINT AGAINST THE SOURCE

Source code can be an OSINT threat too

GitGot

https://github.com/BishopFox/GitGot

José Manuel
Redondo López

- **Finding private information is, disgracefully, common in source code**
  - Connection strings, usernames, keys, API Keys (with which to request services on behalf of the application), DB server addresses, unprotected Amazon buckets...
  - When code is uploaded to GitHub, this information is an OSINT target!
- **GitGot allows searching for sensitive data in code hosted on GitHub**
  - General searches, search for a particular purpose, or only for certain types of sensitive information
  - A similar tool, but specialized in finding API Keys, is GitHound: https://www.kitploit.com/2019/07/git-hound-find-exposed-keys-across.html?m=1

GitRob

https://github.com/michenriksen/gitrob

José Manuel
Redondo López

- **Tool used to find files with sensitive information in public GitHub repos**
  - You can clone repositories belonging to the indicated target
  - Cloning has a configurable depth, to control resource usage
  - Once cloned, it will go through the repo files searching those it believes relevant
  - The result is presented in a web report for further analysis
- **Tutorial**
  - https://michenriksen.com/blog/gitrob-putting-the-open-source-in-osint/

Source: https://blog.segu-info.com.ar/2018/06/gitrob-herramienta-de-reconocimiento-de.html?m=0

GitGraber

https://github.com/hisxo/gitGraber

José Manuel
Redondo López

- Tool to find sensitive data in GitHub repositories
- Includes data from various sources that may have been left in repository files
- Among other information sources it includes
  - Google
  - Amazon (AWS)
  - Paypal
  - Github
  - Facebook
  - Twitter
  - …

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

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

Self-evaluation achievement list: Seminar 1

José Manuel
Redondo López

Rank	Concept
	Understand the OSINT concept
	Understand what types of devices we can find on the internet
	Know what type of information you should not put into source code
	Know how to use **Shodan** and **Censys** OSINT tools to find machines of a concrete target
	Know how to use **Google Hacking** to find information of a concrete target
	Know multiple OSINT tools that work with personal information of individuals / companies
	Know tools to study source code in public repositories
	Know how to study a target using **Google Hacking**
	Know how to study a person using **Tinfoleak**
	**Social Animal**: Be able to locate information about machines, users, and source code on Internet

SEMINAR 1. TOOLS FOR INTERNET RESEARCH

Source: zona-militar.com