

# Seguridad de Sistemas

## **Clase 2: Reconocimiento pasivo**

# Contenidos



- Conocer las diferentes técnicas de búsqueda de información en fuentes abiertas (OSINT)
- Conocer las principales herramientas para reconocimiento pasivo
- Conocer las técnicas de análisis de seguridad web y DNS

# Introducción

- La recopilación de información pasiva (también conocida como Open Source Intelligence u **OSINT**) es el proceso de recopilar información abiertamente disponible sobre un objetivo, generalmente sin ninguna interacción directa con ese objetivo.
- Hay una variedad de recursos y herramientas que podemos utilizar para recopilar esta información.
- Dado que cada herramienta o recurso puede generar cualquier número de resultados variados, puede resultar difícil definir un proceso estandarizado. El objetivo final de la recopilación pasiva de información es obtener información que aclare o amplíe una superficie de ataque.

# Introducción

- Este proceso puede iniciar simplemente buscando información de las personas que trabajan en una empresa en el sitio web o LinkedIn.

## MEET OUR TEAM

---



**Joe Sheer**  
**CHIEF EXECUTIVE OFFICER**

Email: [joe@megacorpone.com](mailto:joe@megacorpone.com)

Twitter: [@Joe\\_Sheer](https://twitter.com/Joe_Sheer)

---



**Tom Hudson**  
**WEB DESIGNER**

Email: [thudson@megacorpone.com](mailto:thudson@megacorpone.com)

Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)

---



**Tanya Rivera**  
**SENIOR DEVELOPER**

Email: [trivera@megacorpone.com](mailto:trivera@megacorpone.com)

Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)

---



**Matt Smith**  
**MARKETING DIRECTOR**

Email: [msmith@megacorpone.com](mailto:msmith@megacorpone.com)

Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)

---

# Whois

- Es un servicio TCP, una herramienta y un tipo de base de datos que puede proporcionar información sobre un nombre de dominio, como el servidor de nombres y el registrador. Esta información suele ser pública ya que los registradores cobran una tarifa por el registro privado.
- Puede ser ejecutado como un comando de Sistema Operativo o bien a través de aplicaciones online



# Whois

```
# whois usm.cl
%%
%% This is the NIC Chile Whois server (whois.nic.cl).
%%
%% Rights restricted by copyright.
%% See https://www.nic.cl/normativa/politica-publicacion-de-datos-cl.pdf
%%

Domain name: usm.cl
Registrant name: Universidad Tecnica Federico Santa Maria (UNIVERSIDAD TECNICA FEDERICO SANTA MARIA)
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 1998-11-30 21:08:03 CLST
Expiration date: 2021-12-26 18:08:03 CLST
Name server: ns.usm.cl (200.1.21.80)
Name server: ns2.usm.cl (200.1.21.150)
Name server: inti.inf.utfsm.cl
Name server: mateo.elo.utfsm.cl
Name server: secundario.nic.cl
```

# Whois

- También es posible obtener datos de una IP pública

```
root@kali:/home/kali# whois 200.54.26.251

% Joint Whois - whois.lacnic.net
% This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net

% Copyright LACNIC lacnic.net
% The data below is provided for information purposes
% and to assist persons in obtaining information about or
% related to AS and IP numbers registrations
% By submitting a whois query, you agree to use this data
% only for lawful purposes.
% 2020-08-25 18:46:50 (-03 -03:00)

inetnum:      200.54.26.0/24
status:       reallocated
aut-num:      N/A
owner:        CL-TEMSR-LACNIC
ownerid:      CL-CLTE-LACNIC
responsible:  Technical Contact
address:      Providencia, 111, 11
address:      1 - Santiago -
country:      CL
phone:        +56 2 6912678
owner-c:      ALS17
```

# Whois



## — Domain Profile

Registrant	Universidad Tecnica Federico Santa Maria (UNIVERSIDAD TECNICA FEDERICO SANTA MARIA)
Registrar	NIC Chile IANA ID: — URL: <a href="https://www.nic.cl">https://www.nic.cl</a> Whois Server: —
Registrar Status	
Dates	8,313 days old Created on 1998-11-30 Expires on 2021-12-26
Name Servers	INTI.INF.UTFSM.CL (has 33 domains) MATEO.ELO.UTFSM.CL (has 33 domains) NS.USM.CL (200.1.21.80) (has 13 domains) NS2.USM.CL (200.1.21.150) (has 13 domains) SECUNDARIO.NIC.CL (has 14,774 domains)
Tech Contact	—
IP Address	200.1.30.100 - 1 other site is hosted on this server
IP Location	 - Valparaiso - Valparaiso - Universidad Tecnica Federico Santa Maria



# Google Hacking

- El término "Google Hacking" fue popularizado por Johnny Long en 2001. A través de varias charlas y un libro extremadamente popular (Google Hacking for Penetration Testers), describió cómo los motores de búsqueda como Google podrían usarse para descubrir información crítica, vulnerabilidades y sitios web mal configurados.
- En el corazón de esta técnica había cadenas de búsqueda inteligentes y operadores que permitieron el refinamiento creativo de las consultas de búsqueda, la mayoría de las cuales funcionan con una variedad de motores de búsqueda. El proceso es iterativo, comenzando con una búsqueda amplia, que se reduce con operadores para tamizar resultados irrelevantes o poco interesantes.

# Google Hacking

## Algunos comandos de Google Hacking

- link: busca sitios relacionados con el argumento
- intitle: busca sitios cuyo título es el indicado
- allintitle: busca sitios cuyo título contiene todas las palabras de la búsqueda
- inurl: busca sitios cuya URL contenga la palabra buscada
- allinurl: busca sitios donde todas las palabras estén la URL
- filetype: busca archivos con la extensión indicada
- allintext: busca un sitio específico en el sitio

# Google Hacking

site:inacap.cl filetype:pdf



All



Books



Images



Shopping



Videos



More

Tools

About 2,830 results (0.24 seconds)

<http://www.inacap.cl> › web › acreditacion › Dictamen\_N\_...

## AGENCIA DE ACREDITACIÓN Y EVALUACIÓN DE ... ✓

Lo dispuesto en la Ley 20.129 que establece un sistema de aseguramiento de la calidad de la educación superior; el reglamento para la autorización de las ...

<http://www.inacap.cl> › web › acreditacion › Acuerd... PDF

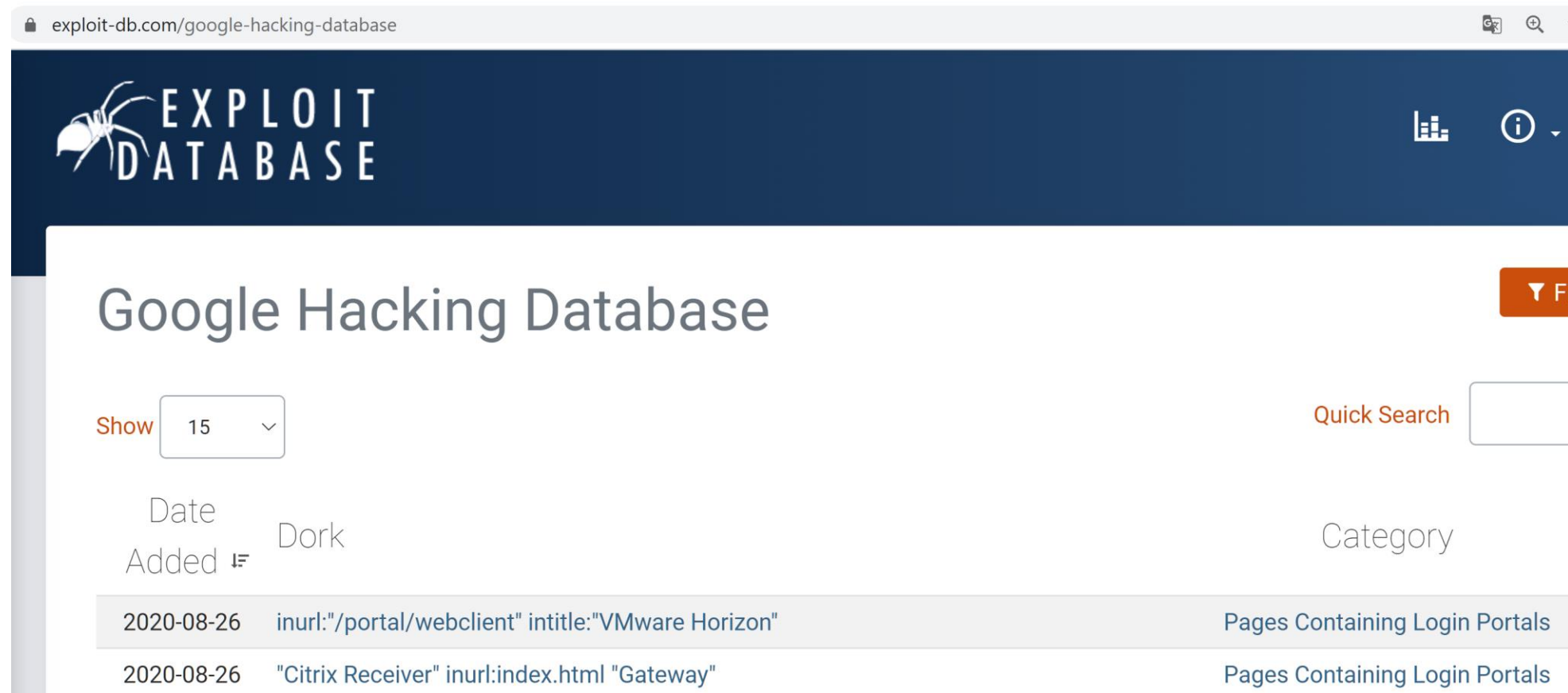
## AGENCIA DE ACREDITACIÓN Y EVALUACIÓN DE ... ✓

Lo dispuesto en la Ley 20.129 que establece un sistema de aseguramiento de la calidad de la educación superior; el reglamento para la autorización de las ...

6 pages

# Google Hacking

- Google Hacking Database



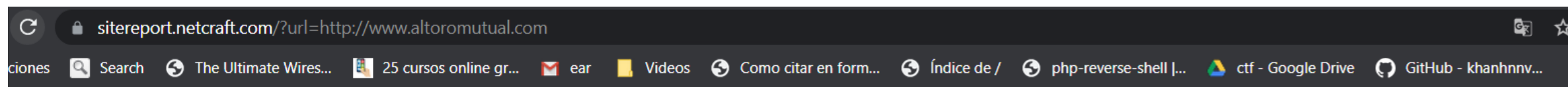
The screenshot shows the Exploit-DB Google Hacking Database interface. The browser address bar displays `exploit-db.com/google-hacking-database`. The page header features the Exploit-DB logo (a spider) and the text "EXPLOIT DATABASE". Below the header, the title "Google Hacking Database" is prominently displayed. On the right side of the header, there are icons for a bar chart and an information symbol. Below the title, there is a "Show" button next to a dropdown menu set to "15". To the right of the title, there is a "Quick Search" input field and a "Category" dropdown menu. Below these, there is a table of search results. The first two results are visible, both dated "2020-08-26". The first result is for a search query `inurl:"/portal/webclient" intitle:"VMware Horizon"` and the second is for `"Citrix Receiver" inurl:index.html "Gateway"`. Both results are categorized as "Pages Containing Login Portals".

Date Added	Dork	Category
2020-08-26	<code>inurl:"/portal/webclient" intitle:"VMware Horizon"</code>	Pages Containing Login Portals
2020-08-26	<code>"Citrix Receiver" inurl:index.html "Gateway"</code>	Pages Containing Login Portals

# Netcraft

- Netcraft es una empresa de servicios de Internet con sede en Inglaterra que ofrece un portal web gratuito que realiza diversas funciones de recopilación de información. El uso de servicios como los que ofrece Netcraft se considera una técnica pasiva, ya que nunca interactuamos directamente con nuestro objetivo.
- Netcraft también proporciona pruebas de seguridad, y publica comunicados de prensa sobre el estado de las diversas redes que conforman Internet.
- La compañía también es conocida por su barra de herramientas anti-phishing gratuita para el explorador Firefox e Internet Explorer.

# Netcraft



Services ▾ Solutions ▾ News Company ▾ Resources ▾ [Report Fraud](#) [Request](#)

## Hosting History

Netblock owner	IP address	OS	Web server	Last seen
▶ Rackspace Backbone Eng...	65.61.137.117	Windows Server 2008	Apache-Coyote/1.1	26-Aug-2021
▶ Rackspace Backbone Eng...	65.61.137.117	Windows Server 2008	unknown	30-Apr-2020
▶ Rackspace Backbone Eng...	65.61.137.117	Windows Server 2008	Apache-Coyote/1.1	29-Apr-2020
▶ Rackspace Backbone Eng...	65.61.137.117	Windows Server 2012	Microsoft-IIS/8.0	13-Dec-2018
▶ Rackspace Backbone Eng...	65.61.137.117	Windows Server 2008	Microsoft-HTTPAPI/2.0	15-Feb-2018

# Archive

- El Internet Archive (Archivo de Internet) es una biblioteca digital gestionada por una organización sin ánimo de lucro dedicada a la preservación de archivos, capturas de sitios públicos de la Web, recursos multimedia y también software.
- Creada el 12 de mayo de 1996 esta organización existe con el apoyo de Alexa Internet y de otros colaboradores que han donado materiales y colecciones como la Biblioteca del Congreso y otras muchas bibliotecas públicas y privadas.
- Alberga una gran cantidad de archivos de muchos tipos como audio, vídeo y texto, la gran mayoría de ellos en dominio público.

# Archive

INTERNET ARCHIVE

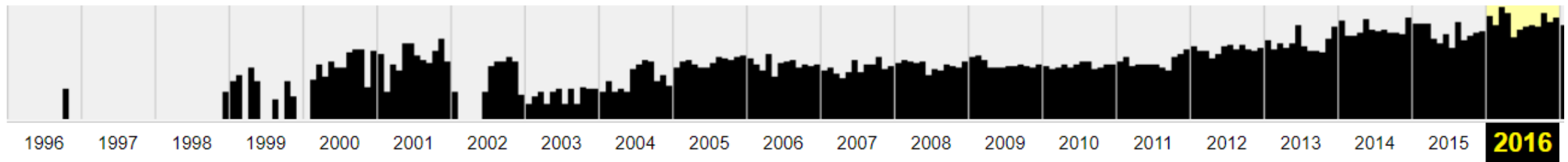
[DONATE](#) **WayBack Machine**

Explore more than 607 billion [web pages](#) saved over time

Results: 50 [100](#) [500](#)

[Calendar](#) · [Collections](#) <sup>beta</sup> · [Changes](#) <sup>beta</sup> · [Summary](#) · [Site Map](#)

Saved **183.064 times** between [October 20, 1996](#) and [September 4, 2021](#).



Registro histórico del sitio [www.Microsoft.com](http://www.microsoft.com)



# Recon-ng

- Recon-ng es un framework de reconocimiento web escrito en Python. Entre sus características principales se enumeran los módulos independientes, interacción con base de datos, construcción con funciones confortables, ayuda interactiva, y completado de comandos. Recon-ng proporciona un poderoso entorno en el cual se puede realizar reconocimiento open source basado en web de manera rápida y total.
- Recon-ng no tiene la intención de competir con los frameworks existentes, ha sido diseñado exclusivamente para reconocimiento basado en web open source

# Recon-ng



# USM

UNIVERSIDAD TECNICA  
FEDERICO SANTA MARIA

[illegible]

# Recon-ng

- Instalación de módulo

```
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules...
[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > info

Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0


Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.
```

# Shodan

- Shodan es un motor de búsqueda que rastrea dispositivos conectados a Internet, incluida, entre otras, la World Wide Web. Esto incluye los servidores que ejecutan sitios web, pero también dispositivos como enrutadores y dispositivos IoT.
- Aunque no se requiere que Shodan complete ningún material en este módulo o los laboratorios, vale la pena explorar un poco. Antes de usar Shodan debemos registrar una cuenta gratuita, que brinda acceso limitado.




# Shodan


 SHODAN

Explore

Downloads

Pricing 

hostname:usm.cl



TOTAL RESULTS

144

TOP COUNTRIES



View Report




Download Results



View on Map


**New Service:** Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

 **Electrónica USM** Participa en nuestras actividades de las Jornadas

200.1.17.61

vhost.elo.usm.cl

Universidad Tecnica  
Federico Santa Maria

 Chile, Santiago



HTTP/1.1 200 OK

Date: Sat, 04 Sep 2021 01:25:32 GMT

Server: Apache/2.4.6 (CentOS) PHP/7.4.11

X-Powered-By: PHP/7.4.11

X-UA-Compatible: IE=edge

Link: <http://semanaelectronica.elo.usm.cl/wp-json/>; rel="https://api.w.org/"

Link: <http://semanaelectronica.elo.usm.cl/wp-json/wp/v2/pages/37>; r...

# Shodan

←

→

↺

shodan.io/search?query=port%3A3389+country%3ACL

Shodan

Developers

Monitor

View All...

SHODAN

port:3389 country:CL

Q

🏠

Explore

Downloads

Reports

Pricing

Enterprise Access

🔥 Exploits

🗺 Maps

🖼 Images

🔗 Share Search


📄 Download Results

📊 Create Report

TOTAL RESULTS

7,592

TOP COUNTRIES



Chile

7,592

TOP CITIES

Santiago	2,545
Las Condes	272
Providencia	161
Concepción	108
Nunoa	97

TOP ORGANIZATIONS

Entel Chile	1,407
Gtd Internet S.A.	693
Telefonica Empresas	604
VTR Banda Ancha S.A.	562
Telefonica del Sur S.A.	373

TOP PRODUCTS


OpenSSH	1
Dropbear sshd	1

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

200.68.15.104


Ctc. Corp S.A. (telefonica Empresas)


Added on 2020-08-25 21:50:25 GMT

 Chile, Los Ángeles


self-signed

EN






Administrador



byb

# Shodan

← → ↻  shodan.io/host/200.68.15.104

 **200.68.15.104** [View Raw Data](#)

self-signed

City	Los Ángeles
Country	Chile
Organization	Ctc. Corp S.A. (telefonica Empresas)
ISP	Ctc. Corp S.A. (telefonica Empresas)
Last Update	2020-08-26T08:20:07.008151
ASN	AS16629

## Ports

21

80

137

3389

5985

## Services

21

tcp

ftp

220-FileZilla Server version 0.9.  
220-written by Tim Kosse (Tim.Kos  
220 Please visit http://sourcefor  
530 Login or password incorrect!

# Análisis SSL/TLS

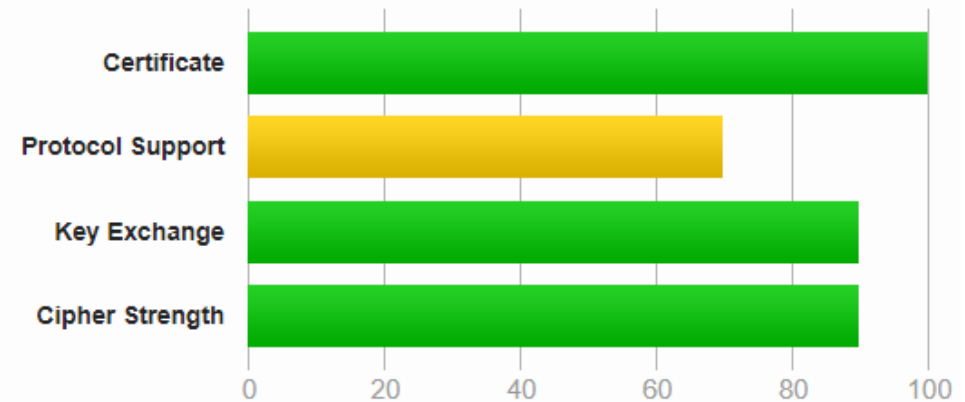
## SSL Report: [www.usm.cl](http://www.usm.cl) (200.1.30.100)

Assessed on: Sun, 05 Sep 2021 03:13:32 UTC | [Hide](#) | [Clear cache](#)



### Summary

#### Overall Rating





# Análisis SSL/TLS

- Protocolos soportados en el análisis

## Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

# Información de usuarios

- Además de recopilar información sobre los recursos de nuestra organización objetivo, también podemos recopilar información sobre los empleados de la organización.
- Nuestro propósito al recopilar esta información es compilar listas de usuarios o contraseñas, crear pretextos para la ingeniería social, aumentar las campañas de phishing o los ataques del lado del cliente, ejecutar el relleno de credenciales y mucho más.
- Algunas pruebas de penetración pueden limitarse a pruebas puramente técnicas sin ningún aspecto de ingeniería social. Otros compromisos pueden tener pocas o ninguna restricción.

# The Harvester

- El objetivo de este programa es recopilar correos electrónicos, subdominios, hosts, nombres de empleados, puertos abiertos y banners de diferentes fuentes públicas como motores de búsqueda, servidores de claves PGP y base de datos informática SHODAN.
- Esta herramienta está destinada a ayudar a los probadores de penetración en las primeras etapas de la prueba de penetración para comprender la huella del cliente en Internet. También es útil para cualquiera que quiera saber qué puede ver un atacante sobre su organización.

# The Harvester

```
# theHarvester -d usm.cl -b google -l 50

*****
*                                     *
* theHarvester                       *
*                                     *
* theHarvester 3.2.3                 *
* Coded by Christian Martorella       *
* Edge-Security Research              *
* cmartorella@edge-security.com       *
*                                     *
*****

[*] Target: usm.cl

        Searching 0 results.
[*] Searching Google.

[*] No IPs found.

[*] Emails found: 5
-----
alfredo.gallegos.14@sansano.usm.cl
camila.lopezm@sansano.usm.cl
info.mii@usm.cl
nicol.ormeno@usm.cl
santiago.geywitz@usm.cl
```

# Búsqueda en RRSS

usm.cl

SEARCH SETTINGS

Sentiment: 4:1

**SEARCH TIPS**

Select language for more relevant results.

Select 

[www.usm.cl](http://www.usm.cl)  
Posted 02:23 04 Sep 2021

CarrerasEstudia en la USM:  
Carreras de Pregrado. Presentes  
en la ...SIGA USMIngrese al sitio  
<https://siga.usm.cl/spe/index.html>  
· Circular Plan ...Admisión  
2022Carreras - Admisión  
Especial - Carreras Vespertinas -  
...Admisión USMPostulaciones -  
Iniciar sesión - Carreras  
Vespertinas - ...Campus y Sed ...

[Universidad Técnica Federico Santa MaríaCarrerasSIGA USMAdmisión 2022Admisión USMCampus y](#)

[es.wikipedia.org](https://es.wikipedia.org)  
Posted 02:23 04 Sep 2021

Universidad Técnica Federico  
Santa María -  
Wikipedia[https://es.wikipedia.org  
> wiki >  
Universidad\\_Técnica\\_...https://es.w  
ikipedia.org > wiki >  
Universidad\\_Técnica\\_...En cachéSi  
milares](https://es.wikipedia.org/wiki/Universidad_Técnica_Federico_Santa_María)  
[Universidad Técnica Federico Santa María - Wikipedia](#)

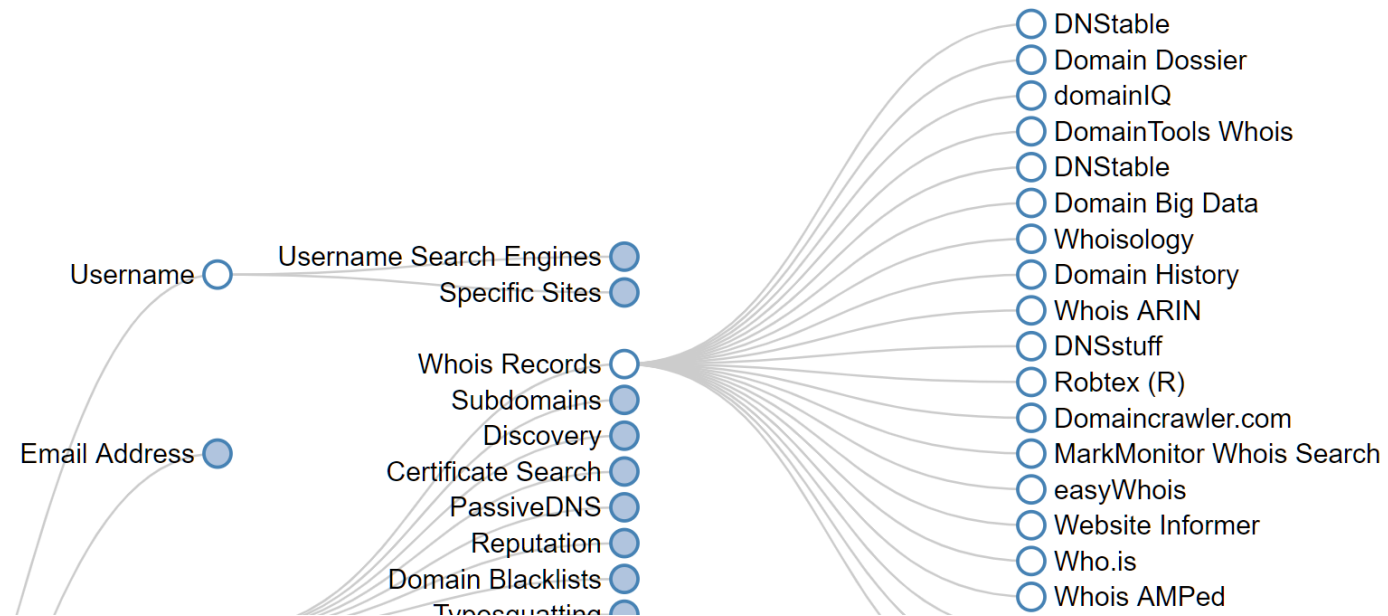
 link 

# OSINT Framework



osintframework.com

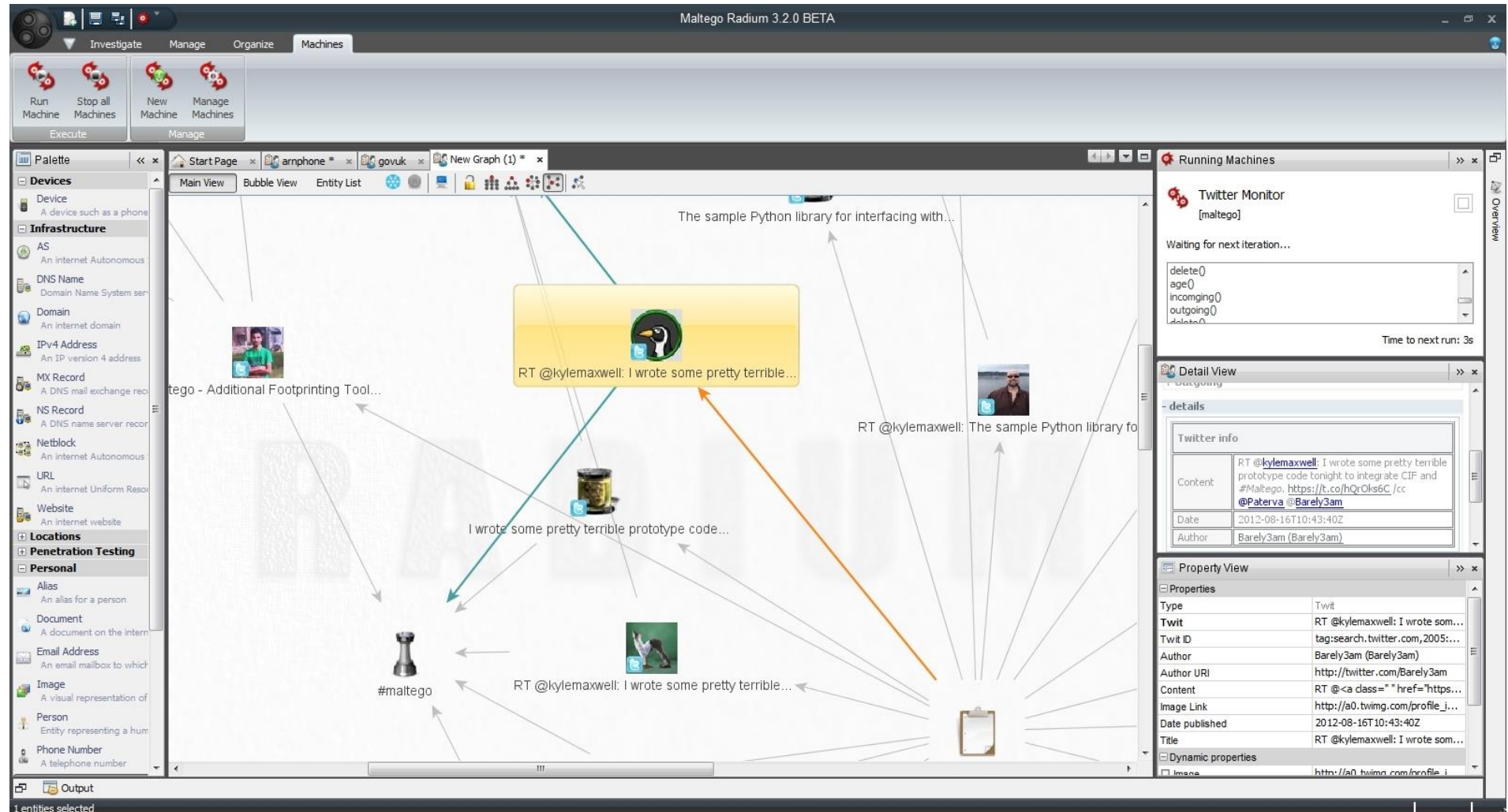
## OSINT Framework



# Maltego

- Es una herramienta de minería de datos muy poderosa que ofrece una combinación infinita de herramientas y estrategias de búsqueda. La curva de aprendizaje para él puede ser empinada y, francamente, es excesivo para este módulo, pero su impresionante capacidad merece una introducción.
- Maltego busca en miles de fuentes de datos en línea y utiliza “transformaciones” extremadamente inteligentes para convertir una información en otra. Por ejemplo, si estamos realizando una campaña de recopilación de información del usuario, podríamos enviar una dirección de correo electrónico y, a través de varias búsquedas automáticas, "transformarla" en un número de teléfono o una dirección postal asociados. Durante un ejercicio de recopilación de información organizacional, podríamos enviar un nombre de dominio y "transformarlo" en un servidor web, luego en una lista de direcciones de correo electrónico, luego en una lista de cuentas de redes sociales asociadas y luego en una lista de posibles contraseñas para esa cuenta de correo electrónico.

# Maltego





# Búsqueda en DNS

- Existe una serie de comandos para consultas DNS y obtener información así como validar si existen fallas de seguridad en el servicio.
- Nslookup: permite obtener registros del servidor DNS
- Fierce: permite validar si existe transferencia de zona y la seguridad del servidor DNS
- Dnsenum: permite obtener todos los registros DNS de un dominio
- DNSRecon: permite validar si existe transferencia de zona y obtener registros del servidor DNS

# Búsqueda en DNS

- nslookup

```
# nslookup
> set type=ns
> usm.cl
Server:          200.75.0.4
Address:         200.75.0.4#53

Non-authoritative answer:
usm.cl  nameserver = ns2.usm.cl.
usm.cl  nameserver = ns.usm.cl.
usm.cl  nameserver = secundario.nic.cl.
```

```
> set type=mx
> usm.cl
Server:          200.75.0.4
Address:         200.75.0.4#53

Non-authoritative answer:
usm.cl  mail exchanger = 0 usm-cl.mail.protection.outlook.com.
```

# Búsqueda en DNS

- Fierce

```
root@kali:/home/kali# fierce -dns megacorpone.com
DNS Servers for megacorpone.com:
    ns3.megacorpone.com
    ns2.megacorpone.com
    ns1.megacorpone.com

Trying zone transfer first...
    Testing ns3.megacorpone.com
        Request timed out or transfer not allowed.
    Testing ns2.megacorpone.com

Whoah, it worked - misconfigured DNS server found:
megacorpone.com.      259200  IN      SOA      ( ns1.megacorpone.com. admin.megacorpone.com.
                        202007073      ;serial
                        28800      ;refresh
                        7200       ;retry
                        2419200    ;expire
                        86400      ;minimum
                        )
megacorpone.com.      259200  IN      TXT      "Try Harder"
megacorpone.com.      259200  IN      TXT      (
                        google-site-verification=U7B_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA )
megacorpone.com.      259200  IN      MX       10 fb.mail.gandi.net.
megacorpone.com.      259200  IN      MX       20 spool.mail.gandi.net.
```

# Búsqueda en DNS

- dnsenum

```
└─# dnsenum usm.cl
dnsenum VERSION:1.2.6

┌─── usm.cl ──┐
└─┘
```

**Host's addresses:**

---

usm.cl.	60	IN	A	200.1.30.100
---------	----	----	---	--------------

**Name Servers:**

---

ns.usm.cl.	60	IN	A	200.1.21.80
ns2.usm.cl.	60	IN	A	200.1.21.150
secundario.nic.cl.	9976	IN	A	200.7.5.7

# Búsqueda en DNS

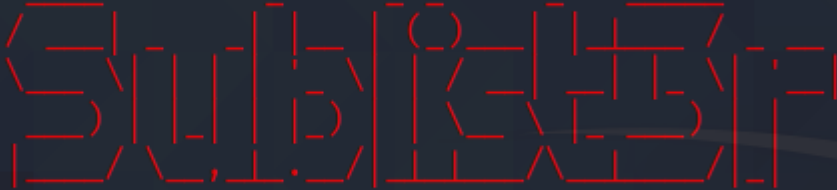
- dnsrecon

```
root@kali:/home/kali# dnsrecon -d megacorpone.com -t axfr
[*] Testing NS Servers for Zone Transfer
[*] Checking for Zone Transfer for megacorpone.com name servers
[*] Resolving SOA Record
[+]      SOA ns1.megacorpone.com 3.220.61.179
[*] Resolving NS Records
[*] NS Servers found:
[*]      NS ns2.megacorpone.com 3.211.51.86
[*]      NS ns1.megacorpone.com 3.220.61.179
[*]      NS ns3.megacorpone.com 3.212.85.86
[*] Removing any duplicate NS server IP Addresses ...
[*]
[*] Trying NS server 3.220.61.179
[+] 3.220.61.179 Has port 53 TCP Open
```

# Búsqueda de sub-dominios

- Sublist3r

```
# sublist3r -d usm.cl
```

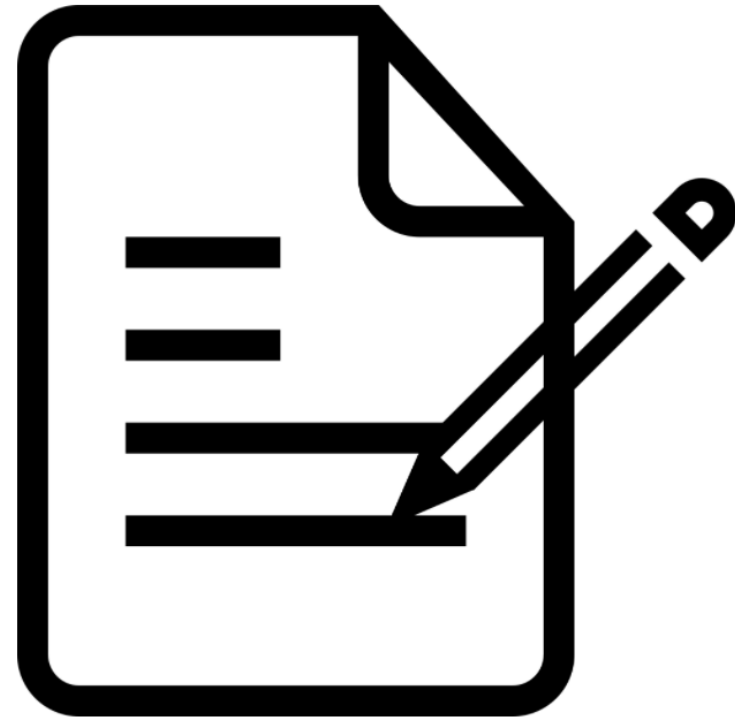


# Coded By Ahmed Aboul-Ela - @aboul3la

```
vader.usm.cl  
valposolar.usm.cl  
www.valposolar.usm.cl  
vc.usm.cl  
vcrate.usm.cl  
vespertinos.usm.cl  
www.vespertinos.usm.cl  
cpanel.vespertinos.usm.cl  
mail.vespertinos.usm.cl  
webdisk.vespertinos.usm.cl  
webmail.vespertinos.usm.cl  
vinadelmar.usm.cl  
www.vinadelmar.usm.cl  
www.rree.vinadelmar.usm.cl  
www.vitacura.usm.cl  
voluntariado.usm.cl  
vplab.usm.cl  
www.vplab.usm.cl  
cpanel.vplab.usm.cl  
mail.vplab.usm.cl  
webdisk.vplab.usm.cl
```

# Resumen

- Búsqueda de Información en fuentes abiertas (OSINT)
- whois
- google hacking
- netcraft
- recon-ng
- shodan
- análisis web (cabecera y SSL/TLS)
- theHarvester
- Maltego
- Búsqueda en DNS







# USM

UNIVERSIDAD TECNICA  
FEDERICO SANTA MARIA