

Actividad práctica número 2:

Formato: Individual.


Asignatura: Seguridad de Sistemas

Código: INF346

Título: Reconocimiento Pasivo

A.- Búsqueda en whois

1.- Busque información del dominio usm.cl en algún sitio de whois

— Domain Profile	
Registrant	Universidad Tecnica Federico Santa Maria (UNIVERSIDAD TECNICA FEDERICO SANTA MARIA)
Registrar	NIC Chile IANA ID: — URL: https://www.nic.cl Whois Server: —
Registrar Status	
Dates	8,314 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 14,796 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

2.- Corrobore la información en el sitio del NIC

usm.cl	
Titular:	Universidad Tecnica Federico Santa Maria (UNIVERSIDAD TECNICA FEDERICO SANTA MARIA)
Agente Registrador:	NIC Chile
Fecha de creación:	1998-11-30 21:08:03 CLST
Fecha de última modificación:	2016-10-11 23:35:03 CLST
Fecha de expiración:	2021-12-26 18:08:03 CLST Renovar ahora
Servidor de Nombre:	secundario.nic.cl
Servidor de Nombre:	inti.inf.ut fsm.cl
Servidor de Nombre:	ns.usm.cl
Servidor de Nombre:	ns2.usm.cl
Servidor de Nombre:	mateo.elo.ut fsm.cl

3.- Utilice la herramienta nslookup para comprobar si coincide con la configuración de DNS

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

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

4.- Obtenga la información de whois vía comando

```
root@kali:/home/kali# whois lun.com
Domain Name: LUN.COM
Registry Domain ID: 1762462_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.register.com
Registrar URL: http://www.register.com
Updated Date: 2019-07-08T13:42:38Z
Creation Date: 1998-08-13T04:00:00Z
Registry Expiry Date: 2021-08-12T04:00:00Z
Registrar: Register.com, Inc.
Registrar IANA ID: 9
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: ok https://icann.org/epp#ok
Name Server: NS1.LUN.COM
Name Server: NS2.LUN.COM
Name Server: NS3.LUN.COM
Name Server: NS4.LUN.COM
DNSSEC: unsigned
```

B.- Google Hacking

1.- Use los siguientes dorks para buscar información

filetype:xls inurl:"email.xls"

?intitle:index.of?mp3 queen

filetype:sql "MySQL dump" (pass|password|passwd|pwd)

site:gov filetype:doc allintitle:restricted

inurl:"ViewerFrame?Mode="

2.- Utilice el sitio GHDB para encontrar lo siguiente:

- Archivos con contraseñas

- Acceso a Bases de datos

- Sitios con wordpress

C.- Netcraft

1.- Busque el historial de los siguientes sitios

URL: <https://news.netcraft.com/>

<https://www.usm.cl>

Hosting History				
Netblock owner	IP address	OS	Web server	Last seen
Universidad Tecnica Federico Santa Maria Valparaiso	200.1.30.100	Linux	Apache/2.2.15 CentOS	18-Sep-2020

<https://www.marca.com/>

<http://www.lun.com/>

<https://www.webscantest.com/>

<http://testphp.vulnweb.com>

D.- Recon-ng

1.- Inicie la aplicación recon-ng con el siguiente comando

```
-# recon-ng  
[*] Version check disabled.  
  
Sponsored by ...  
  
www.blackhillsinfosec.com  
  
PRACTISEC  
www.practisec.com  
  
[recon-ng v5.1.1, Tim Tomes (@lanmaster53)]  
  
[*] No modules enabled/installed.  
  
[recon-ng][default] >
```

2.- Busque el siguiente modulo en el Marketplace

```
[recon-ng][default] > marketplace info recon/domains-hosts/google_site_web
```

path	recon/domains-hosts/google_site_web
name	Google Hostname Enumerator
author	Tim Tomes (@lanmaster53)
version	1.0
last_updated	2019-06-24
description	Harvests hosts from Google.com by using the 'site' search operator.
required_keys	[]
dependencies	[]
files	[]
status	not installed

3.- Realice la instalación del 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] > █
```

4.- Cargue el módulo y revise los parámetros de configuración

```
[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 results.

Options:
  Name      Current Value  Required  Description
  _____
SOURCE     default            yes       source of input (see 'info' for details)
```

5.- Configure un dominio de prueba y ejecute un test

```
[recon-ng][default][google_site_web] > options set SOURCE usm.cl
SOURCE ⇒ usm.cl
[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.

Options:
  Name      Current Value  Required  Description
  _____
SOURCE     usm.cl            yes       source of input (see 'info' for details)
```

```
[recon-ng][default][google_site_web] > run

_____
USM.CL

[*] Searching Google for: site:usm.cl
[*] Country: None
[*] Host: www.did.usm.cl
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

6.- Instale el siguiente módulo y cárguelo en la herramienta

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

7.- Revise los hosts encontrados

```
[recon-ng][default][resolve] > show hosts
```

rowid	host	ip_address
1	www.did.usm.cl	
2	ciencias.usm.cl	
3	quimicaymedioambienteconcepcion.usm.cl	
4	aula.usm.cl	
5	beelab.usm.cl	
6	vinculacion.usm.cl	
7	casim.usm.cl	
8	arquitectura.usm.cl	
9	stem.usm.cl	
10	www.ec2g.usm.cl	
11	comunicaciones.usm.cl	
12	dcp.usm.cl	

8.- Busque la dirección IP de cada uno

```
[recon-ng][default][resolve] > run
[*] www.did.usm.cl ⇒ 200.1.30.30
[*] ciencias.usm.cl ⇒ 200.1.30.30
[*] quimicaymedioambienteconcepcion.usm.cl ⇒ 200.1.30.71
[*] aula.usm.cl ⇒ 158.69.169.45
[*] aula.usm.cl ⇒ 158.69.169.42
[*] beelab.usm.cl ⇒ 200.1.30.71
[*] vinculacion.usm.cl ⇒ 200.1.24.32
[*] casim.usm.cl ⇒ 200.1.30.30
[*] arquitectura.usm.cl ⇒ 200.1.30.129
[*] stem.usm.cl ⇒ 200.1.30.74
```

9.- Valide el resultado

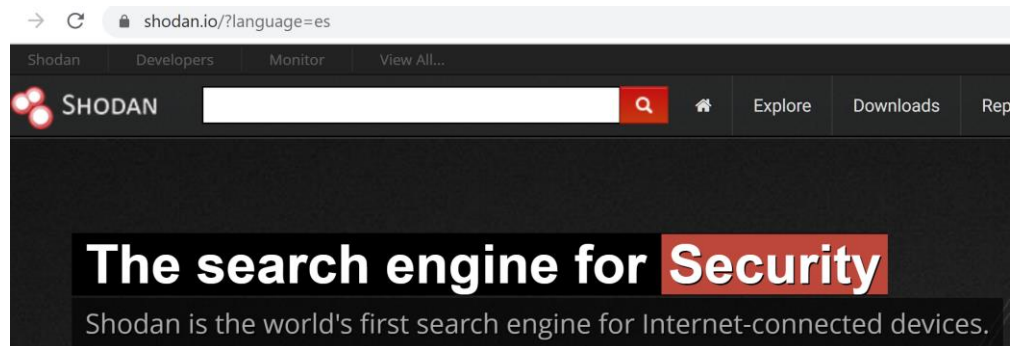
```
[recon-ng][default][resolve] > show hosts
```

rowid	host	ip_address
1	www.did.usm.cl	200.1.30.30
2	ciencias.usm.cl	200.1.30.30
3	quimicaymedioambienteconcepcion.usm.cl	200.1.30.71
4	aula.usm.cl	158.69.169.45
5	beelab.usm.cl	200.1.30.71
6	vinculacion.usm.cl	200.1.24.32
7	casim.usm.cl	200.1.30.30
8	arquitectura.usm.cl	200.1.30.129
9	stem.usm.cl	200.1.30.74

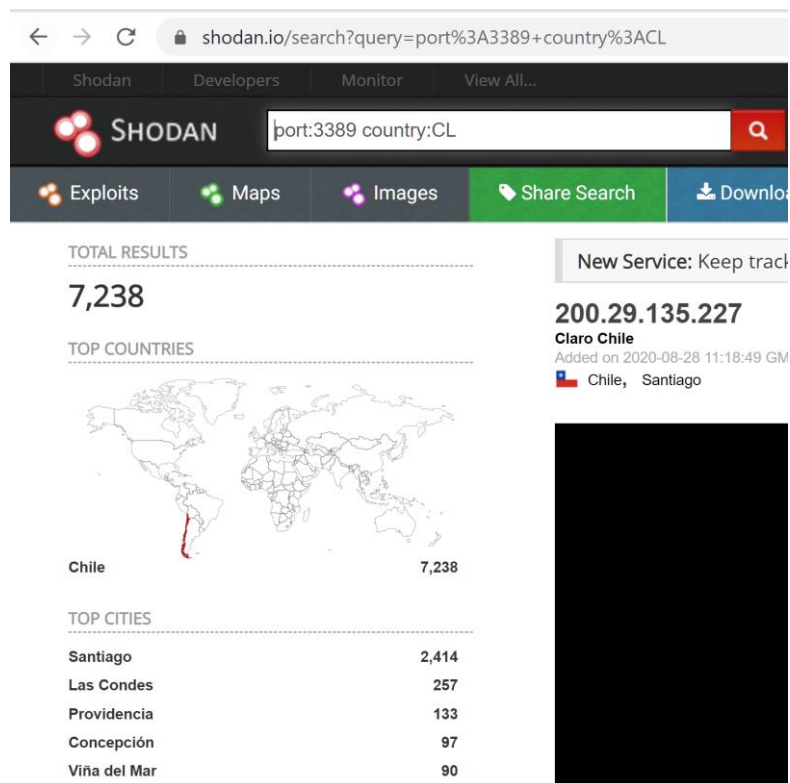
E.- Shodan

1.- Conéctese con su browser a la siguiente dirección

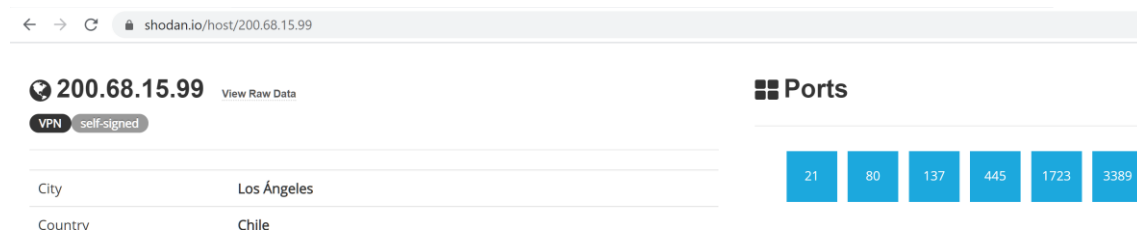
URL: <https://www.shodan.io/?language=es>



2.- Busque servidores con el puerto 3389 abierto en Chile



3.- Revise los puertos abiertos de algún host



4.- Busque los servidores públicos asociados a un dominio

The screenshot shows the Shodan search interface with the query 'ism.cl'. The results show 6 total results. The top countries are Chile and Valparaíso. The first result is for the IP address 200.130.231, which is associated with the domain 'edge02.usm.cl' and the organization 'Universidad Tecnica Federico Santa Maria'. The result also shows an SSL certificate issued by 'RapidSSL RSA CA 2018' and the organization 'Chile, Valparaíso'.

TOTAL RESULTS
6

TOP COUNTRIES

200.130.231
edge02.usm.cl
Universidad Tecnica
Federico Santa Maria
Chile, Valparaíso

SSL Certificate
Issued By:
Common Name:
RapidSSL RSA CA 2018
Organization:
Chile, Valparaíso

220 EDGE02.usm.cl Microsoft ESMTPL MAIL Service ready
250-EDGE02.usm.cl Hello [34.247.89.150]
250-SIZE 104857600
250-PIPELINING
250-DSN
250-55MMMFENETATHECODE

5.- Busque la versión de la siguiente aplicación

The screenshot shows the Shodan search interface with the query 'Apache/2.4.43 country:CL'. The results show 518 total results. The top countries are Chile and Santiago. The first result is for the IP address 190.196.7.166, which is associated with the domain 'static.190.196.7.166.gtdinternet.com' and the organization 'Gtd Internet S.A.'. The result also shows the date 'Added on 2020-08-26 05:00:51 GMT' and the location 'Chile, Santiago'.

TOTAL RESULTS
518

TOP COUNTRIES

190.196.7.166
static.190.196.7.166.gtdinternet.com
Gtd Internet S.A.
Added on 2020-08-26 05:00:51 GMT
Chile, Santiago

6.- Busque servidores web Microsoft

The screenshot shows the Shodan search interface with the query 'IIS Windows Server country:CL'. The results show 2,294 total results. The top countries are Chile and Santiago. The first result is for the IP address 131.221.32.187, which is associated with the domain 'unassigned.32.221.131.in-addr.arpa' and the organization 'Grupo Zgh SpA'. The result also shows the date 'Added on 2020-08-26 23:45:12 GMT' and the location 'Chile, Santiago'.

TOTAL RESULTS
2,294

TOP COUNTRIES

IIS Windows Server
131.221.32.187
unassigned.32.221.131.in-addr.arpa
Grupo Zgh SpA
Added on 2020-08-26 23:45:12 GMT
Chile, Santiago

7.- Busque cámaras en vivo

The screenshot shows the Shodan search interface with the query '/cgi-bin/guestimage.html'. The results show 769 total results. The top countries are Australia and Malvern. The first result is for the IP address 161.43.96.52, which is associated with the domain 'Optus' and the organization 'Optus'. The result also shows the date 'Added on 2020-08-26 23:32:45 GMT' and the location 'Australia, Malvern'.

TOTAL RESULTS
769

TOP COUNTRIES

161.43.96.52
Optus
Added on 2020-08-26 23:32:45 GMT
Australia, Malvern

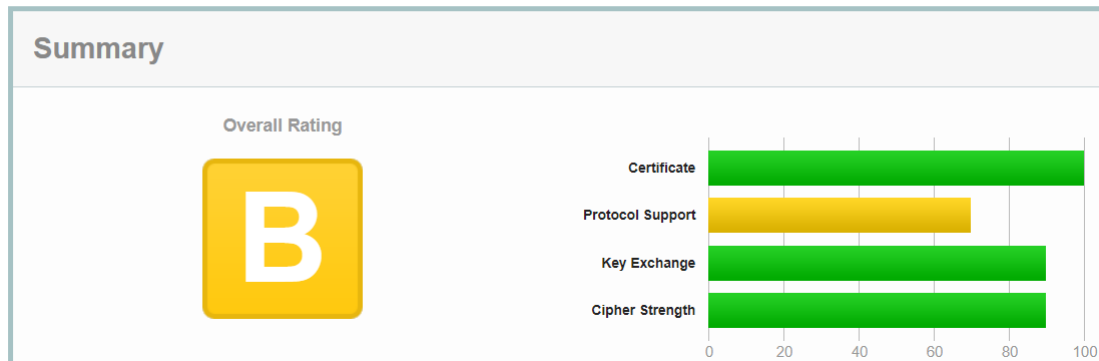
F.- Análisis SSL/TLS

1.- Realice el análisis SSL/TLS con la siguiente aplicación, en las siguientes URL

URL: <https://www.ssllabs.com/ssltest/>

SSL Report: **www.usm.cl** (200.1.30.100)

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



demo.testfire.net

media-online.ddns.net

www.bciseguros.cl

www.arrow.cl

G.- TheHarvester

1.- Busque información con el siguiente comando

```
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.

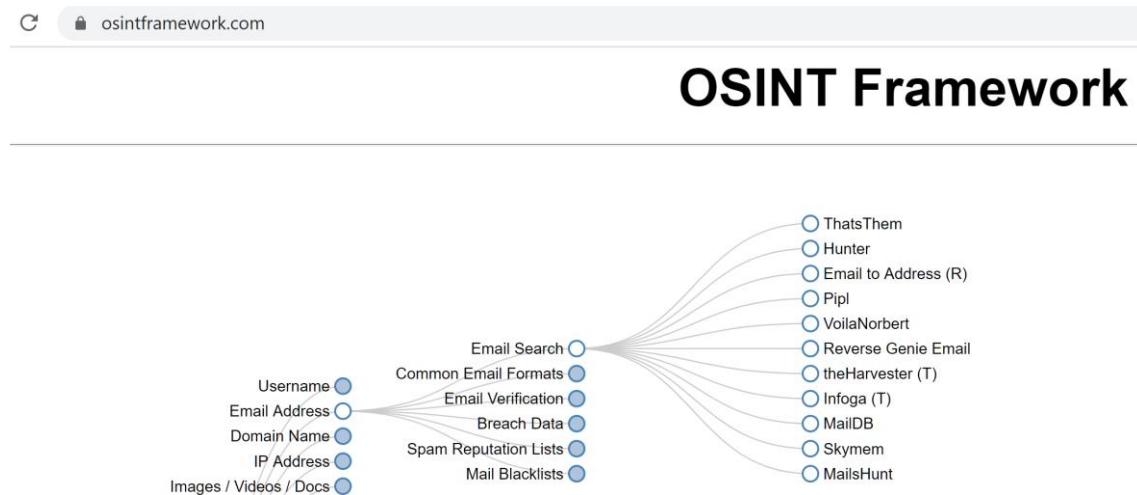
[*] No IPs found.

[*] 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
```


E.- OSINT Framework

1.- Conéctese a la siguiente aplicación

URL: <https://osintframework.com/>



F.- Búsqueda en DNS

1.- Obtenga los siguientes registros de los siguientes dominios

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

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

Altoromutual.com

Redusers.com

2.- Obtenga la IPv6 de los siguientes hosts

```
> set type=aaaa
> www.microsoft.com
Server:          200.75.0.4
Address:         200.75.0.4#53

Non-authoritative answer:
www.microsoft.com canonical name = www.microsoft.com-c-3.edgekey.net.
www.microsoft.com-c-3.edgekey.net canonical name = www.microsoft.com-c-3.
www.microsoft.com-c-3.edgekey.net.globalredir.akadns.net canonical name
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1419:9c00:194::356e
Name:   e13678.dscb.akamaiedge.net
Address: 2600:1419:9c00:18e::356e
```

www.redusers.com

www.usm.cl

3.- Obtenga el registro SOA de los siguientes dominios

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

Non-authoritative answer:
usm.cl
      origin = ns.usm.cl
      mail addr = hostmaster.usm.cl
      serial = 2021090202
      refresh = 3600
      retry = 1800
      expire = 86400
      minimum = 86400
```

Altoromutual.com

Redusers.com

4.- Valide si existe transferencia de zona en los siguientes dominios

```
root@kali:/home/kali# fierce -dns zonetransfer.me
DNS Servers for zonetransfer.me:
  nsztml.digi.ninja
  nsztml2.digi.ninja

Trying zone transfer first...
Testing nsztml.digi.ninja

Whoah, it worked - misconfigured DNS server found:
zonetransfer.me.      7200      IN      SOA      ( nsztml.
                        2019100801      ;serial
                        172800      ;refresh
                        900      ;retry
                        1209600      ;expire
                        3600      ;minimum
```

Altoromutual.com

Redusers.com

usm.cl

5.- Enumere los siguientes dominios

```
# 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.      0      IN      A      200.1.21.80
ns2.usm.cl.      0      IN      A      200.1.21.150
secundario.nic.cl. 5897      IN      A      200.7.5.7
```

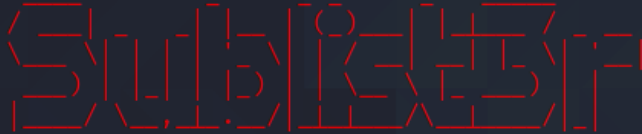
Altoromutual.com

6.- Enumere los siguientes dominios vía DNS

```
# dnsrecon -d usm.cl
[*] std: Performing General Enumeration against: usm.cl ...
[-] DNSSEC is not configured for usm.cl
[*] SOA ns.usm.cl 200.1.21.80
[*] NS ns2.usm.cl 200.1.21.150
[*] NS secundario.nic.cl 200.7.5.7
[*] NS secundario.nic.cl 2001:1398:276:0:200:7:5:7
[*] NS ns.usm.cl 200.1.21.80
[*] MX usm-cl.mail.protection.outlook.com 104.47.58.110
[*] MX usm-cl.mail.protection.outlook.com 104.47.70.110
[*] A usm.cl 200.1.30.100
```

7.- Busque los subdirectorios con la siguiente herramienta

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



```
# Coded By Ahmed Aboul-Ela - @aboul3la
```

```
cpanel.claseinvertida.usm.cl
mail.claseinvertida.usm.cl
webdisk.claseinvertida.usm.cl
webmail.claseinvertida.usm.cl
cloud.usm.cl
hpc.cmitt.usm.cl
cocim2015.usm.cl
www.cocim2015.usm.cl
comercial.usm.cl
www.comercial.usm.cl
cpanel.comercial.usm.cl
icv.comercial.usm.cl
www.icv.comercial.usm.cl
mail.comercial.usm.cl
webdisk.comercial.usm.cl
webmail.comercial.usm.cl
```