



Hacking Ético

Reconocimiento

Marco Aravena Vivar

Marco Aravena Vivar
Académico Titular Escuela de Ingeniería Informática
Director General de Modernización y Transformación Digital.



Reconocimiento

Reconocimiento

Marco Aravena Vivar

Marco Aravena Vivar
Académico Titular Escuela de Ingeniería Informática
Director General de Modernización y Transformación Digital.

Reconocimiento

- El reconocimiento es la primera etapa que todo hacker debe de hacer, ya que es parte de la preparación para poder atacar el sistema.
- Se trata de recopilar la mayor cantidad de información posible del objetivo en una auditoría, a más información se obtenga, mayor posibilidad de éxito en el ataque.



Reconocimiento

Los objetivos del reconocimiento son:

- **Aprender la condición de seguridad:** analizar cómo se encuentra la seguridad del objetivo, encontrar lagunas y crear un plan de ataque.
- **Identificar el área donde se va a trabajar:** utilizar diferentes herramientas y técnicas, reducir el rango de direcciones IP.
- **Mapear la red:** representar gráficamente la red del objetivo y utilizarla como guía durante el ataque.



Reconocimiento

Tipos de reconocimiento:

- Activo
- Pasivo





Reconocimiento Pasivo

Reconocimiento

Marco Aravena Vivar

Marco Aravena Vivar
Académico Titular Escuela de Ingeniería Informática
Director General de Modernización y Transformación Digital.

Reconocimiento Pasivo

- Se consigue la información sin interacción directa con el objetivo mediante el uso de técnicas tales como:
 - La ingeniería social
 - Sniffing de red
 - Búsquedas por internet
 - Vigilancia de instalaciones para recabar información sobre empleados, accesos, infraestructura, etc.



Reconocimiento Pasivo

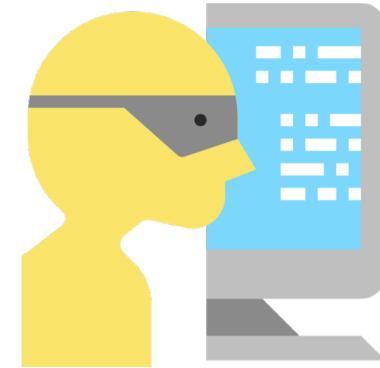
- **Ingeniería Social.** Es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.
- Algunas técnicas son:
 - Phishing
 - Redes sociales
 - Vishing



Reconocimiento Pasivo

- **¿Cómo usted aplicaría las siguientes técnicas?**

- Phishing
- Redes sociales
- Vishing



- **¿Cuál sería el público más apto para estas técnicas?**
- **¿Qué cosas cree que puede conseguir?**

Reconocimiento Pasivo

- El hacker tratar de recopilar de forma metodológica toda la información que más pueda al respecto del objetivo:
 - No se realiza ningún tipo de escaneo o contacto con la máquina objetivo.
 - Permite construir un mapa del objetivo, sin interactuar con él.
 - Existen menos herramientas informáticas que en las otras fases.
 - Se realiza recolección de información pública



5 AÑOS
ACREDITADA
NIVEL DE EXCELENCIA
Gestión Institucional, Docencia de Pregrado
Investigación, Vinculación con el Medio y
Docencia de Postgrado
HASTA MARZO DE 2020

Comisión Nacional
de Acreditación
CNA-Chile

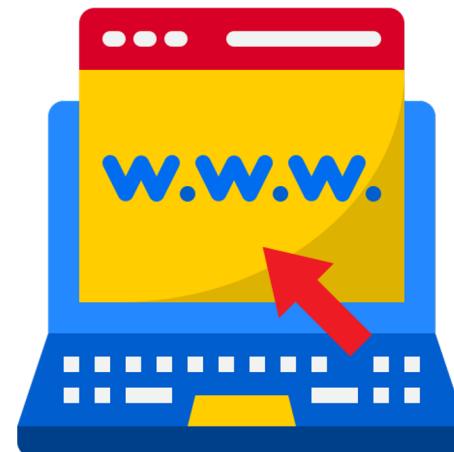
Reconocimiento Pasivo

- La recolección de información se hace desde:
 - Páginas web
 - Publicidad
 - Llamadas
 - Redes Sociales

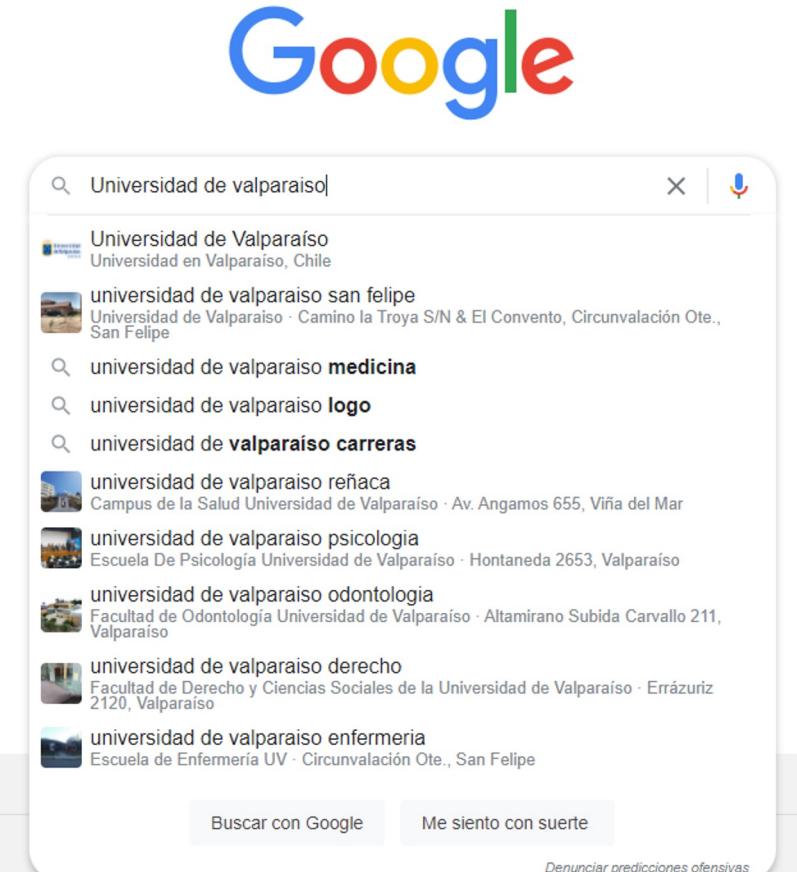


Reconocimiento Pasivo

- Para buscar la información se puede utilizar:
 - <https://www.whois.com/>
 - <https://www.google.cl/>
 - <https://nic.cl/>
 - <https://news.netcraft.com/>



Reconocimiento Pasivo



A screenshot of a Google search results page. The search query is "Universidad de valparaíso". The top result is a link to the official website of the University of Valparaíso, Chile. Below it are several other links related to the university's various faculties and departments.

- Universidad de Valparaíso - Universidad en Valparaíso, Chile
- universidad de valparaíso san felipe
Universidad de Valparaíso · Camino la Troya S/N & El Convento, Circunvalación Ote., San Felipe
- universidad de valparaíso medicina
- universidad de valparaíso logo
- universidad de valparaíso carreras
- universidad de valparaíso reñaca
Campus de la Salud Universidad de Valparaíso · Av. Angamos 655, Viña del Mar
- universidad de valparaíso psicología
Escuela De Psicología Universidad de Valparaíso · Hontaneda 2653, Valparaíso
- universidad de valparaíso odontología
Facultad de Odontología Universidad de Valparaíso · Altamirano Subida Carvallo 211, Valparaíso
- universidad de valparaíso derecho
Facultad de Derecho y Ciencias Sociales de la Universidad de Valparaíso · Errázuriz 2120, Valparaíso
- universidad de valparaíso enfermería
Escuela de Enfermería UV · Circunvalación Ote., San Felipe

At the bottom of the search results, there are buttons for "Buscar con Google", "Me siento con suerte", and "Denunciar predicciones ofensivas".

<https://www.uv.cl> ▾

Bienvenido a la Universidad de Valparaíso, Chile

PORTAL ACADÉMICO CORREO UV CONVENIOS DE DESEMPEÑO · Estudiantes de primer año de Arquitectura exponen trabajos vinculados a la temática del agua.

Portal UV

[INGRESO A SISTEMAS](#)
[INSTITUCIONALES](#). Alumnos ...

Carreras de la Universidad de ...

[Ingresar al portal de admisión UV](#)
[2020. RELACIONADOS ...](#)

Admisión 2022

[Ingresos especiales - Becas y beneficios - Medicina - Psicología](#)

[Más resultados de uv.cl »](#)

Postgrados y Postítulos

[ADMISIÓN POSTGRADO UV](#)
[2020 Doctorado, Magíster ...](#)

Visión y misión

[Facultades - Organización -](#)
[Organigrama - ...](#)

Bibliotecas

[Bases de Datos - Libros](#)
[Electrónicos - Bibliotecas - ...](#)



Reconocimiento Pasivo

<https://www.facebook.com> › ... › College & University ▾

[Universidad de Valparaíso - Chile - Home | Facebook](#)

Acreditados en docencia de pregrado, gestión institucional, investigación, docencia de postgrado y... Calle Blanco 951, 2340000 **Valparaíso**, Chile.

<https://www.youtube.com> › channel

[Universidad de Valparaíso - YouTube](#)

Canal YouTube de la **Universidad de Valparaíso**, Chile.

<https://twitter.com/uvalpochile>

[Universidad de Valparaíso \(@uvalpochile\) · Twitter](#)

Atención futuros
#MechonesUV los invitamos
a que ingresen a la web
www.uv.cl y se inscriban en
nuestro ensayo online de la
Prueba de Admisión
Transitoria, que este 23 de
octubre a las 9:00 horas se
desarrollará con las pruebas
de Ciencias y...
dlvr.it/S81Yps

Twitter · hace 2 horas

¡Conéctate y conoce
nuestra universidad!
dlvr.it/S81MnH

Twitter · hace 3 horas

Eres parte de la UV, y
queremos conocer tu
opinión, con tu participación,
y la colaboración de todas y
todos podemos convertir
este proceso en una
oportunidad de mejora y un
mayor desarrollo para
nuestra Universidad.
Contesta la Encuesta de...
dlvr.it/S81M7m

Twitter · hace 3 horas



5 AÑOS ACREDITADA
NIVEL DE EXCELENCIA
Gestión Institucional, Docencia de Pregrado
Investigación, Vinculación con el Medio y
Docencia de Postgrado

HASTA MARZO DE 2029



Reconocimiento Pasivo

- Para buscar la información se puede utilizar:
 - <https://who.is/>
 - Whois se refiere a un protocolo de consulta y respuesta que se utiliza para recuperar información sobre los recursos de Internet asignados.
 - Las bases de datos Whois contienen información personal de los propietarios de dominios y son mantenidas por los Registros Regionales de Internet.



Reconocimiento Pasivo

- Los resultados de las consultas de Whois suelen incluir:
 - Detalles del dominio.
 - Detalles del propietario del dominio.
 - Servidor de dominio.
 - Caducidad del dominio.
 - Fechas de creación y última actualización.



Reconocimiento Pasivo

Premium Domains

Transfer

Features

Login

Sign Up

whois

WHOIS Search, Domain Name, Website, and IP Tools

Domain names or IP addresses...



Your IP address is 1.1.1.1



Looking to get a website?

Web Hosting

Website Builder

SSL Certificates

**Everything you
need in one place.**

DOMAINS. HOSTING. EMAIL.
WORDPRESS. SSL. G SUITE.



Name.com

SAVE 15% ON
YOUR FIRST ORDER

USE PROMO WHOIS

New customers only. Not applicable to domain transfers, renewals, or premium registrations.



See Website Information

Search the whois database, look up domain and IP owner information, and check out dozens of other statistics.



On Demand Domain Data

Get all the data you need about a domain and everything associated with that domain anytime with a single search.



Register Domain Names

Find a domain with the best domain registrar on the web. Start your domain search at Name.com.

REREDITADA
VEL DE EXCELENCIA

ión Institucional, Docencia de Pregrado
Ingeniería, Vinculación con el Medio y
Inicia de Postgrado

ESTA MARZO DE 2029



Reconocimiento Pasivo



uv.cl

public information

Whois DNS Records Diagnostics

cache expires in 14 hours, 22 minutes and 47 seconds

refresh

Registrar Info

Name
Referral URL <https://www.nic.cl>

Status

Important Dates

Expires On 1970-01-01
Registered On 1970-01-01
Updated On

Name Servers

ns.uv.cl (200.14.68.75)
secundario.nic.cl 200.7.5.7

Similar Domains

uv.cl | uv.cloud | uv.club |

Registrar Data

We will display stored WHOIS data for up to 30 days
refresh

Make Private Now

Registrant Contact Information:

Name Universidad de Valparaíso (UNIVERSIDAD DE VALPARAISO)
Organization
Address
City
Postal Code
Country
Phone
Email

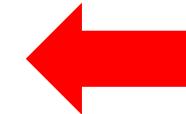
Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at **Name.com**

Site Status

Status	Active
Server Type	Apache/2.4.25 (Debian)

Suggested Domains for uv.cl



Use promo code WHOIS to save 15% on your first Name.com order.

Find the perfect domain at **Name.com**

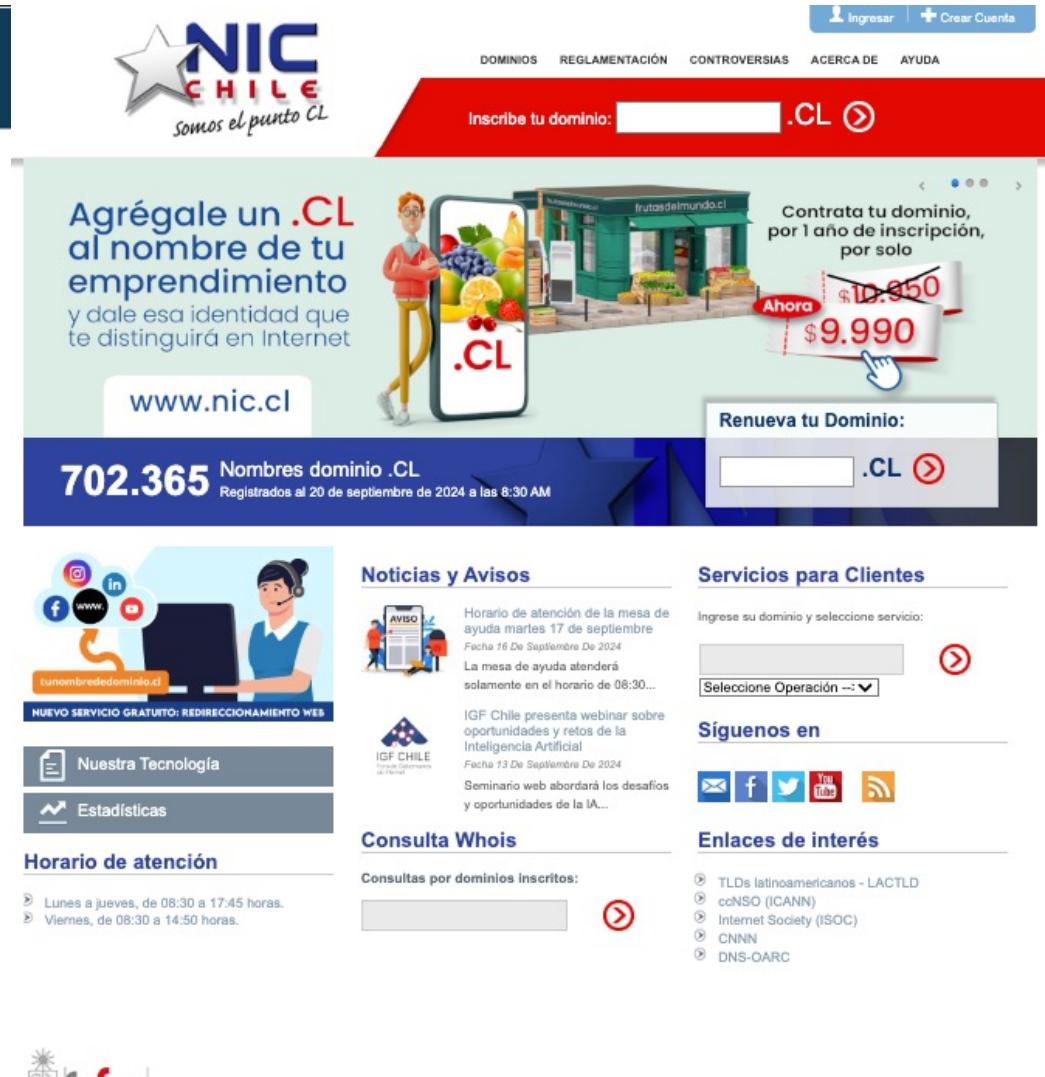
Reconocimiento Pasivo

DNS Records for uv.cl

Hostname	Type	TTL	Priority	Content
uv.cl	SOA	300		ns.uv.cl postmaster@uv.cl 2021092001 3600 600 604800 300
uv.cl	NS	300		secundario.nic.cl
uv.cl	NS	300		ns.uv.cl
uv.cl	A	300		200.14.249.53
uv.cl	MX	300	30	aspmx4.googlemail.com
uv.cl	MX	300	30	aspmx3.googlemail.com
uv.cl	MX	300	30	aspmx2.googlemail.com
uv.cl	MX	300	30	aspmx5.googlemail.com
uv.cl	MX	300	20	alt1.aspmx.l.google.com
uv.cl	MX	300	10	aspmx.l.google.com
uv.cl	MX	300	20	alt2.aspmx.l.google.com
www.uv.cl	A	300		200.14.249.53

Reconocimiento Pasivo

- Para buscar la información se puede utilizar:
 - <https://nic.cl/>
 - Es el encargado de la administración del Registro de Nombres de Dominio .CL, que identifica a Chile en la red Internet



The screenshot shows the main page of the NIC Chile website. At the top right, there are links for 'Ingresar' (Log In) and '+ Crear Cuenta' (Create Account). Below the header, there are navigation links for 'DOMINIOS', 'REGLAMENTACIÓN', 'CONTROVERSIAS', 'ACERCA DE', and 'AYUDA'. A search bar invites users to 'Inscribe tu dominio: .CL'. To the right, a promotional banner for '.CL' domains features a character holding a smartphone displaying '.CL' and a store named 'frutasdelmundo.cl'. It highlights a price reduction from '\$10.950' to '\$9.990'. Another banner below says 'Renueva tu Dominio:' followed by a renewal input field and a '.CL' button. The central part of the page displays statistics: '702.365 Nombres dominio .CL' registered on '20 de septiembre de 2024 a las 8:30 AM'. On the left, there's a section about 'REDIRECCIONAMIENTO WEB' with a person at a computer. Below it are links for 'Nuestra Tecnología' and 'Estadísticas'. On the right, sections include 'Noticias y Avisos' (with an IGF Chile webinar announcement), 'Servicios para Clientes' (with a dropdown menu for domain selection), 'Síguenos en' (social media icons), and 'Enlaces de interés' (links to various internet organizations).

Reconocimiento Pasi

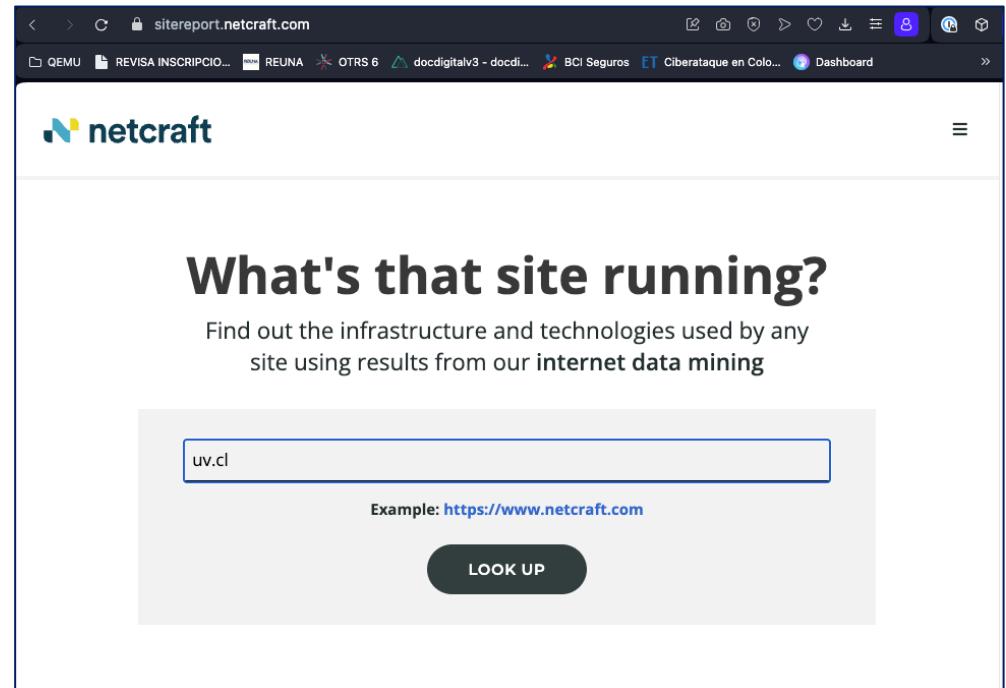
The screenshot shows the NIC Chile website interface. At the top, there is a navigation bar with links for 'DOMINIOS' and 'REGISTRA'. Below the navigation, the NIC Chile logo is displayed with the tagline 'Somos el punto CL'. A large blue button labeled 'Inscribe tu dominio' is prominent. In the center, there is a form for domain registration with fields for 'Nombre de dominio' (containing 'uv.cl') and 'Consultar información dominio'. Below the form, there is a section for 'Realizar una nueva búsqueda' with a search bar and radio buttons for 'Exacta' or 'Contenga'. The background features a light gray gradient.



The screenshot shows the NIC Chile Whois search results for the domain 'uv.cl'. The results are presented in a clean, white card-like format. At the top, it says 'uv.cl'. Below that, the 'Titular' is listed as 'Universidad de Valparaíso (UNIVERSIDAD DE VALPARAISO)'. The 'Agente Registrador' is 'NIC Chile'. The 'Fecha de creación' is 'Anterior a 1997-09-09'. The 'Fecha de última modificación' is '2022-06-07 10:02:23 CLST'. The 'Fecha de expiración' is '2026-01-15 17:37:13 CLST', with a green 'Renovar ahora' (Renew now) button next to it. The 'Servidor de Nombre' is 'secundario.nic.cl' and 'ns.uv.cl'. The 'Sitio web' is 'www.uv.cl'. At the bottom, a yellow banner states: 'IMPORTANTE: NIC Chile ya no entrega domicilio, teléfonos ni direcciones de email de los contactos del dominio. En su lugar, provee un servicio para hacerles llegar un mensaje a través de [este formulario web](#)'.

Reconocimiento Pasivo

- Para buscar la información se puede utilizar:
 - <https://sitereport.netcraft.com>
 - Netcraft es una empresa de servicios de Internet que proporciona, entre otros servicios de seguridad, pruebas de aplicaciones y escaneo automatizado de vulnerabilidades.



The screenshot shows a browser window with the URL sitereport.netcraft.com in the address bar. The page header features the Netcraft logo. Below it, the main heading reads "What's that site running?". A subtext explains: "Find out the infrastructure and technologies used by any site using results from our internet data mining". A search input field contains the text "uv.cl". Below the input field is a "LOOK UP" button. At the bottom of the page, there is sample text: "Example: <https://www.netcraft.com>".

Reconocimiento Pasivo

netcraft

[LEARN MORE](#) [REPORT FRAUD](#)

Background

Site title	Not Present	Date first seen	June 1997
Site rank	957013	Primary language	Not Present
Description	Not Present		

Network

Site	http://uv.cl	Domain	uv.cl
Netblock Owner	Telmex Chile Internet S.A.	Nameserver	ns.uv.cl
Hosting company	America Movil	Domain registrar	Unknown
Hosting country	CL	Nameserver organisation	Unknown
IPv4 address	200.14.246.253 (VirusTotal)	Organisation	Unknown
IPv4 autonomous systems	AS6429	DNS admin	postmaster@uv.cl
IPv6 address	Not Present	Top Level Domain	Chile (.cl)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Enabled
Reverse DNS	Unknown		

IP delegation

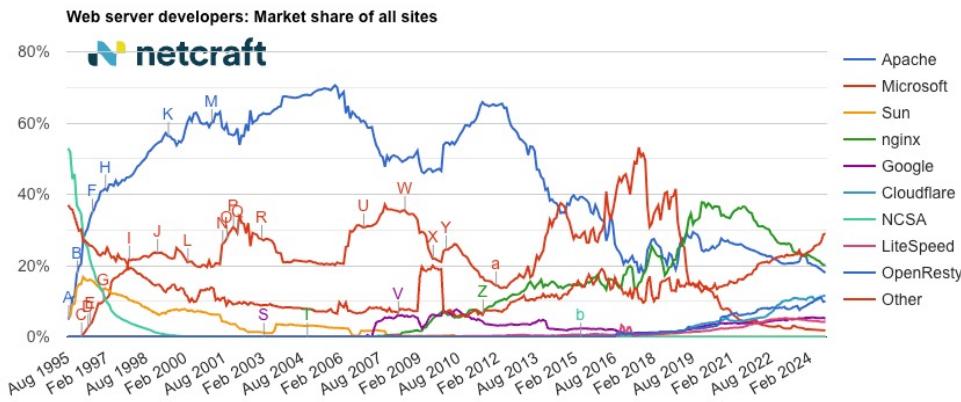
IPv4 address (200.14.246.253)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
4 200.0.0.0-200.255.255.255	Uruguay	LACNIC-200	Latin American and Caribbean IP address Regional Registry
4 200.14.192.0-200.14.255.255	Chile	LACNIC-200-14-192-18	Telmex Chile Internet S.A.
4 200.14.246.253	Chile	LACNIC-200-14-192-18	Telmex Chile Internet S.A.

CHILE



Reconocimiento Pasivo



Developer	August 2024	Percent	September 2024	Percent	Change
nginx	223,025,645	20.13%	225,640,032	20.16%	0.03
Apache	203,825,341	18.40%	201,390,151	18.00%	-0.40
Cloudflare	127,028,522	11.47%	130,093,325	11.63%	0.16
OpenResty	108,954,196	9.84%	111,723,893	9.98%	0.15

Reconocimiento Pasivo

Los atacantes utilizan el reconocimiento para recopilar la siguiente información:

- Información de la red
 - Dominios
 - Subdominios
 - Direcciones IP
 - Whois y registros DNS

URL : Uniform Resource Locator



Reconocimiento Pasivo

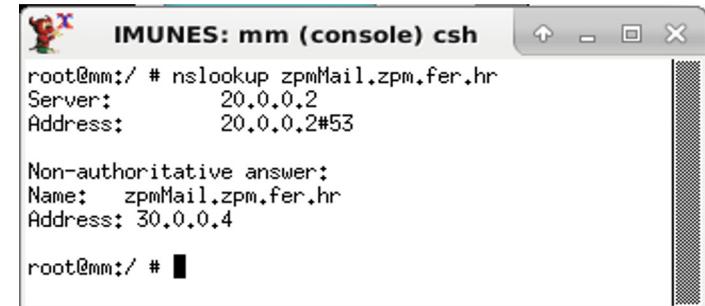
DNS Footprinting

- Es técnica utilizada para recopilar información sobre los sistemas informáticos y las entidades a las que pertenecen.
- Para buscar información sobre DNS Footprinting se puede usar lo siguiente:
 - Nslookup
 - <https://network-tools.com/>
 - <https://www.dnsstuff.com/>



Reconocimiento Pasivo

- **Nslookup**
 - Es una herramienta de línea de comandos.
 - Su función básica es encontrar la dirección IP de un equipo determinado o realizar una búsqueda DNS inversa (encontrar el nombre de dominio de una determinada dirección IP).
 - **Es especialmente importante a la hora de resolver errores de DNS, pues permite consultar información diversa de un dominio o IP correspondiente**



```
root@mm:/ # nslookup zpmMail.zpm.fer.hr
Server:      20.0.0.2
Address:     20.0.0.2#53

Non-authoritative answer:
Name:  zpmMail.zpm.fer.hr
Address: 30.0.0.4

root@mm:/ #
```

Reconocimiento Pasivo

- <https://www.broadbandsearch.net/network-tools>

- Búsqueda de DNS
- Comprobador de correo electrónico
- Encabezados HTTP
- Ping en línea
- Comprobador de lista negra de spam
- Codificación y decodificación de URL

The screenshot shows the homepage of broadbandsearch.net. At the top, there is a navigation bar with the logo 'BroadbandSearch' on the left and links for 'Home', 'Find Provider', and 'Search' on the right. A blue header bar below the navigation bar contains the text 'Internet Providers / Network Tools'. The main content area features a section titled 'Internet Tools: Trusted Free Online Internet Tools' with a sub-section title '20 Years Of Free Tools For Network Geeks'. Below this, there is a paragraph of text followed by a bulleted list of ten network tools: DNS Lookup, Email Checker, HTTP Headers, IDN & Punycode Conversion, NS Lookup, Online Ping, Spam Blacklist Checker, Traceroute, URL Encode & Decode, and WHOIS Search.



Reconocimiento Activo

Reconocimiento

Marco Aravena Vivar

Marco Aravena Vivar
Académico Titular Escuela de Ingeniería Informática
Director General de Modernización y Transformación Digital.

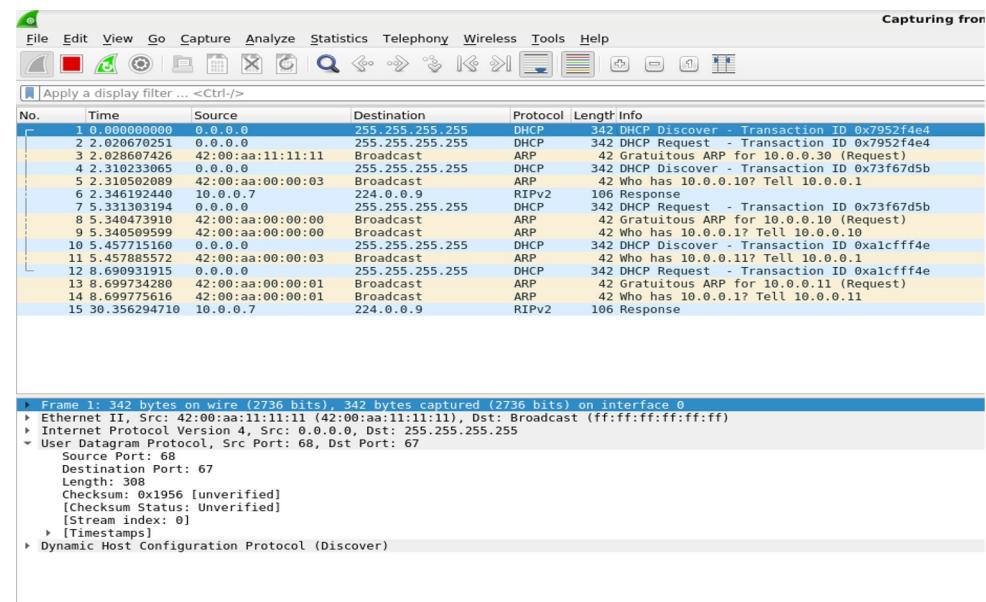
Reconocimiento Activo

- Estudio de la red para descubrir los equipos individuales, las direcciones IP y los servicios que se prestan.
- Implica **más riesgo de detección** que el reconocimiento pasivo porque hay que **interactuar con el objetivo**.
- Algunos de sus objetivos son:
 - Identificación y Estado de Puertos.
 - Identificar Servicios.
 - Identificar Sistemas operativos.
 - Contacto directo y enumeración de Objetivo.



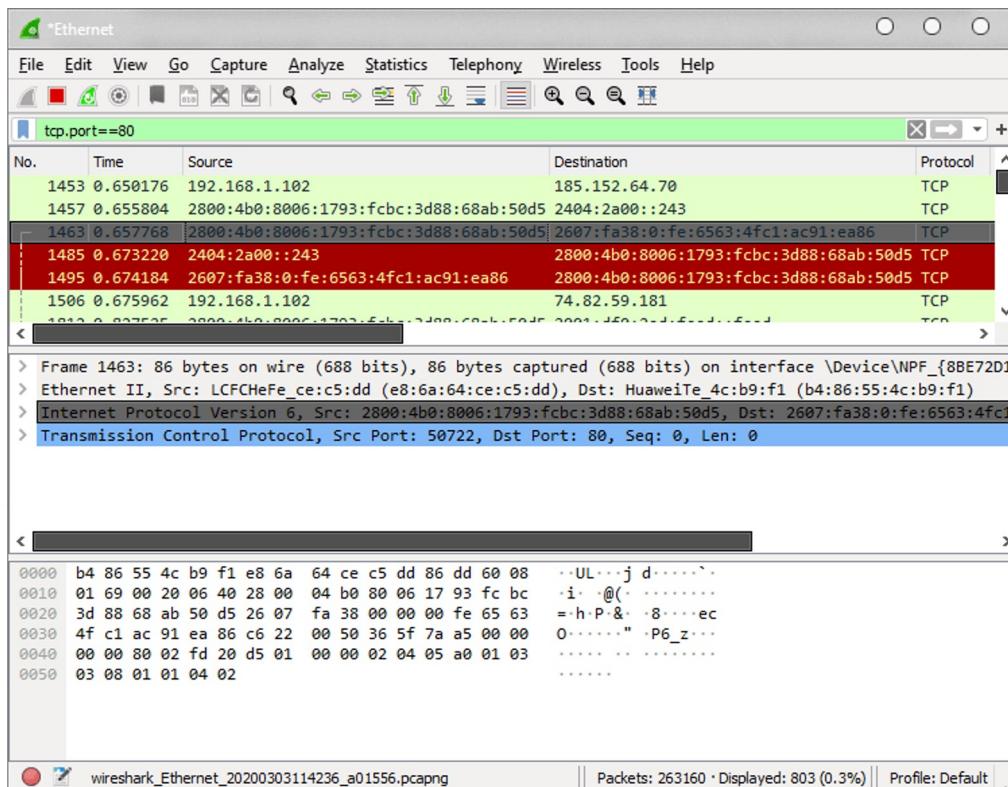
Reconocimiento Activo: Sniffer

- Un sniffer es un programa informático diseñado para controlar y analizar el tráfico red de un punto a otro de la misma.
- Las herramientas de sniffing son relativamente fáciles de usar y proporcionan una ingente cantidad de información útil.
- Ejemplo:
 - Wireshark
 - Tcpdump
 - Microsoft Message Analyzer
 - Nmap



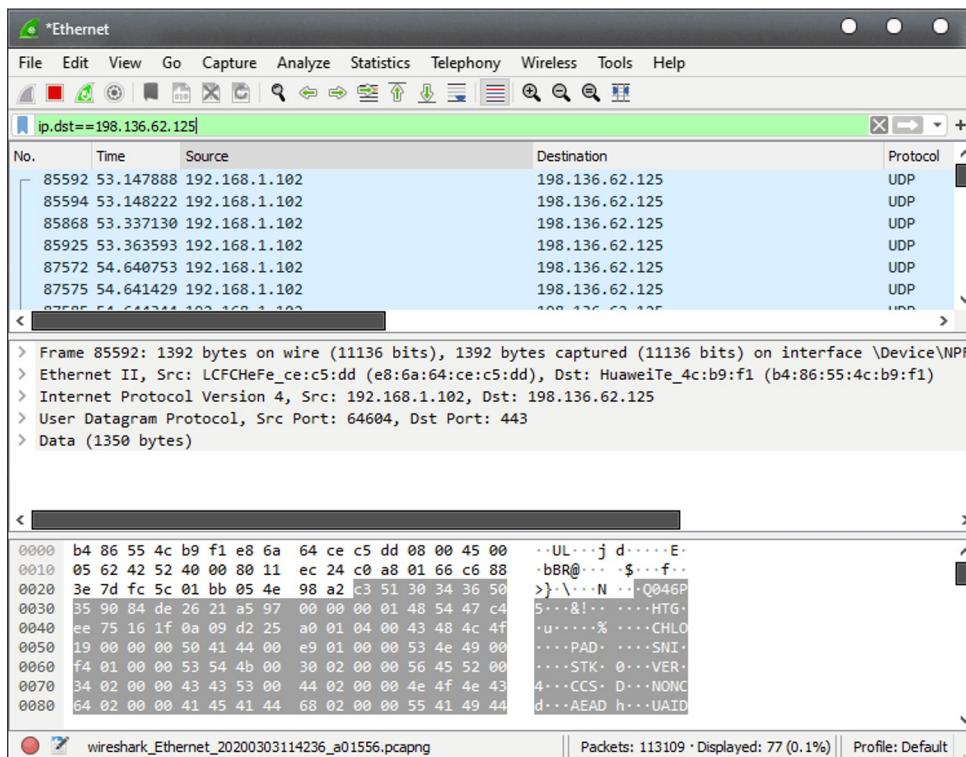
Sniffer

- **Wireshark.**
- Filtro por puerto: se puede filtrar a través de un puerto TCP



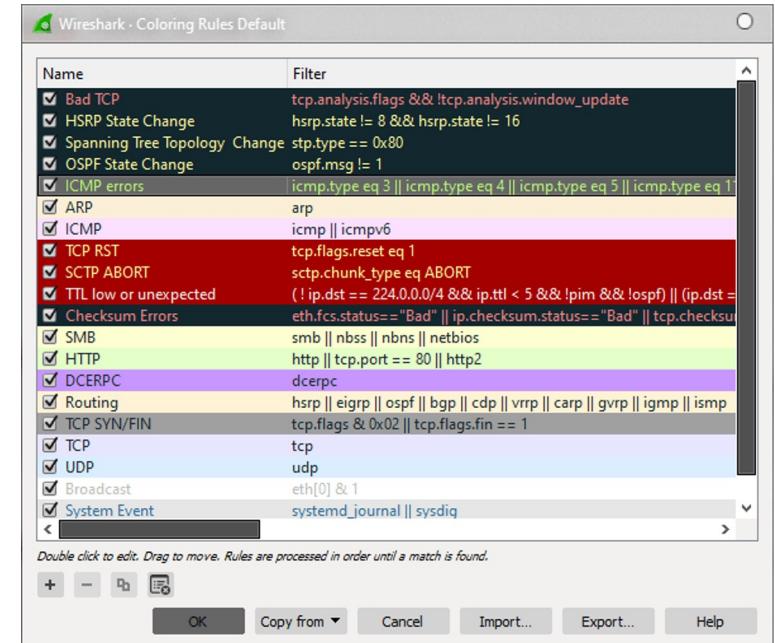
Sniffer

- **Wireshark**.
- Filtrar por IP: Se puede buscar por dirección de origen (ip.src) y dirección de destino (ip.dst)



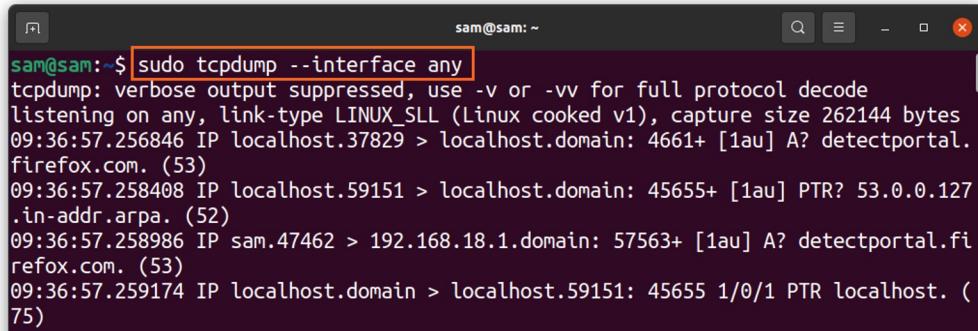
Sniffer

- **Wireshark.**
- Se tiene un esquema de colores para diferenciar cada protocolo. Esquema de color completo del Wireshark, View-> Coloring Rules.
- **Verde:** HTTP
- **Morada claro:** TCP
- **Azul claro:** UDP, DNS
- **Negro:** segmentos TCP problemáticos



TCPDUMP

- **TCPDUMP.** Es una herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red. Permite al usuario capturar y mostrar en tiempo real los paquetes transmitidos y recibidos en la red a la cual el ordenador está conectado.

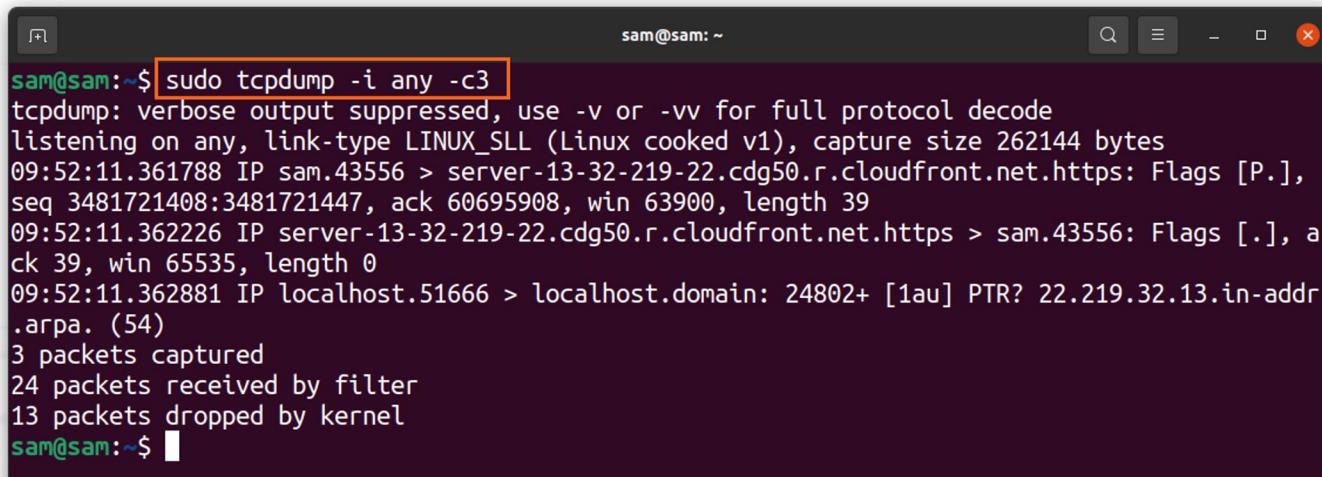


```
sam@sam:~$ sudo tcpdump --interface any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
09:36:57.258486 IP localhost.37829 > localhost.domain: 4661+ [1au] A? detectportal.
firefox.com. (53)
09:36:57.258408 IP localhost.59151 > localhost.domain: 45655+ [1au] PTR? 53.0.0.127
.in-addr.arpa. (52)
09:36:57.258986 IP sam.47462 > 192.168.18.1.domain: 57563+ [1au] A? detectportal.fi
refox.com. (53)
09:36:57.259174 IP localhost.domain > localhost.59151: 45655 1/0/1 PTR localhost. (75)
```

El comando rastrea paquetes de todas las interfaces activas. Los paquetes serán capturados continuamente hasta que el usuario los interrumpe

TCPDUMP

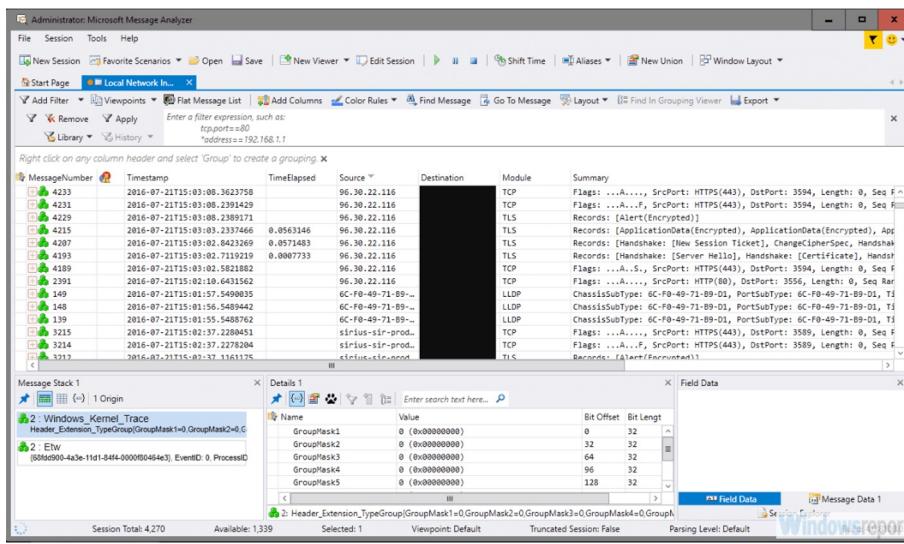
- **TCPDUMP.** Este comando es útil para filtrar un paquete específico. Además, la resolución de problemas de conectividad requiere solo la captura de unos pocos paquetes iniciales. Podemos limitar la cantidad de paquetes a capturar usando la bandera "-c" que significa el "recuento".



```
sudo tcpdump -i any -c3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bytes
09:52:11.361788 IP sam.43556 > server-13-32-219-22.cdg50.r.cloudfront.net.https: Flags [P.], seq 3481721408:3481721447, ack 60695908, win 63900, length 39
09:52:11.362226 IP server-13-32-219-22.cdg50.r.cloudfront.net.https > sam.43556: Flags [.], ack 39, win 65535, length 0
09:52:11.362881 IP localhost.51666 > localhost.domain: 24802+ [1au] PTR? 22.219.32.13.in-addr.arpa. (54)
3 packets captured
24 packets received by filter
13 packets dropped by kernel
```

Microsoft Message Analyzer

- **Microsoft Message Analyzer.** Es una aplicación orientada a los expertos de redes y administradores de sistemas desarrollada para permitir a los usuarios capturar los paquetes de su red local en tiempo real (incluso de forma remota), listarlos y analizar el tráfico según los diferentes protocolos. Además, la aplicación permite cargar capturas de tráficos realizadas previamente para un análisis en detalle.



Nmap

- **Nmap.** Es una herramienta utilizada para el descubrimiento de redes. Utiliza paquetes de IP sin procesar para determinar los hosts disponibles en la red, los servicios ofrecidos por esos hosts, los sistemas operativos que están ejecutando, los tipos de firewall que se utilizan y otras características importantes.
- Las características de Nmap incluyen la capacidad de escanear redes grandes, así como de mapear redes.

```
notwist@notwist:~$ nmap localhost
Starting Nmap 4.20 ( http://insecure.org ) at 2007-04-02 15:50 CEST
Interesting ports on localhost (127.0.0.1):
Not shown: 1691 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql

Nmap finished: 1 IP address (1 host up) scanned in 0.213 seconds
notwist@notwist:~$
```

Nmap

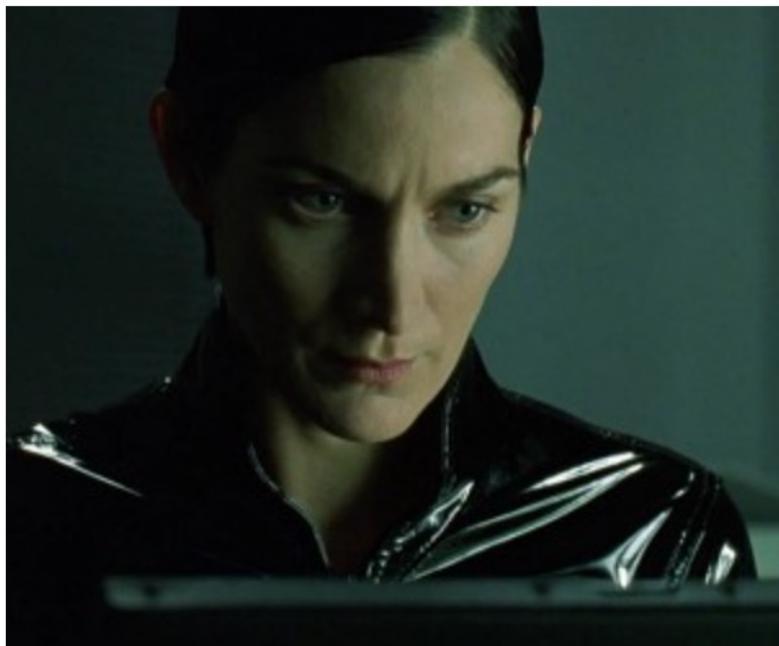
- **Nmap.**
- Escanear una sola IP: Si se detecta una actividad extraña proveniente de un host desconocido, un escaneo de IP puede permitir ver por donde puede estar ocurriendo estos ataques.

```
root@EthicalHaks:~# nmap 192.168.0.9
Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-19 08:19 PDT
Nmap scan report for 192.168.0.9
Host is up (0.0000030s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
111/tcp    open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

Nmap

- Nmap en películas <https://nmap.org/movies/>



A composite image. On the left is a terminal window showing Nmap scan results for IP 10.2.2.2. The output includes port 80/tcp (http) and 22/tcp (ssh) as open. It also shows an OS detection attempt and a successful SSH exploit attempt. On the right is a smaller window titled "REF CONTROL" with the message "ACCESS GRANTED".

```
80/tcp      open     http  
81/tcp      open  
10.2.2.2   [ nmap ]  
11 $ nmap -v -sS -O 10.2.2.2  
11  
13 Starting nmap 0.2.54BETA25  
13 Insufficient responses for TCP sequencing (3). OS detection is  
13 accurate.  
14 Interesting ports on 10.2.2.2:  
44 (The 1539 ports scanned but not shown below are in state: cl  
51 Port      State       Service  
51 22/tcp    open        ssh  
58  
68 No exact OS matches for host  
68  
24 Nmap run completed -- 1 IP address (1 host up) scanned  
50 $ sshnuke 10.2.2.2 -rootpw="Z10N0101"  
Connecting to 10.2.2.2:ssh ... successful.  
Re-Attempting to exploit SSHv1 CRC32 ... successful.  
IP Resetting root password to "Z10N0101".  
System open: Access Level <9>  
Hn $ ssh 10.2.2.2 -l root  
root@10.2.2.2's password: ■
```

Traceroute

- **Traceroute.** Sirve para trazar la ruta que hace un paquete entrante que viene desde un host o punto de red hasta el computador.
- El computador envía un paquete al destino, en el camino el computador le solicita a cada enrutador el tiempo de respuesta de cada uno cuando pasa por ahí el paquete
- Se trata de una herramienta de diagnóstico de red, ya que cuando envías estos paquetes obtienes estadísticas del RTT o la latencia de red.

```
Command Prompt
C:\Users\Johel>tracert www.youtube.com

Tracing route to youtube-ui.l.google.com [216.58.192.110]
over a maximum of 30 hops:

 1   5 ms    2 ms    2 ms  192.168.1.1
 2   26 ms   25 ms   24 ms  mbo-03-lo65.bras.cantv.net [190.36.64.1]
 3   23 ms   23 ms   24 ms  172.16.26.1
 4   26 ms   27 ms   27 ms  10.150.0.21
 5   29 ms   26 ms   26 ms  10.150.0.2
 6   27 ms   30 ms   27 ms  10.150.0.202
 7   85 ms   88 ms   88 ms  pos15-1-0.miami2.mia.seabone.net [195.22.199.110]
 8   90 ms   90 ms   84 ms  et10-3-0.miami15.mia.seabone.net [89.221.41.177]
 9   215 ms  218 ms   *     et9-3-0.miami15.mia.seabone.net [195.22.199.179]
10   79 ms   77 ms   78 ms  google.miami15.mia.seabone.net [89.221.41.18]
11   77 ms   77 ms   78 ms  209.85.253.118
12   78 ms   78 ms   77 ms  216.239.42.79
13   77 ms   77 ms   77 ms  mia07s35-in-f110.1e100.net [216.58.192.110]

Trace complete.
```

Sniffer

- **Traceroute.**

```
[marco@MacBook-de-Marco ~ % traceroute www.uv.cl
traceroute to www.uv.cl (200.14.249.53), 64 hops max, 52 byte packets
 1  192.168.100.1 (192.168.100.1)  19.580 ms  2.064 ms  3.205 ms
 2  100.66.32.1 (100.66.32.1)  8.794 ms  8.975 ms  6.606 ms
 3  172.31.232.141 (172.31.232.141)  12.472 ms  8.066 ms  18.354 ms
 4  172.31.215.94 (172.31.215.94)  8.613 ms  10.917 ms  17.229 ms
 5  172.31.213.18 (172.31.213.18)  7.966 ms  12.696 ms  13.715 ms
 6  172.31.215.69 (172.31.215.69)  15.039 ms  32.660 ms  15.334 ms
 7  192.168.104.146 (192.168.104.146)  11.787 ms  9.108 ms  24.153 ms
 8  190.208.1.78 (190.208.1.78)  12.493 ms  14.006 ms  12.206 ms
 9  190.54.112.5 (190.54.112.5)  28.118 ms  61.290 ms  65.818 ms
10  190.54.112.18 (190.54.112.18)  19.182 ms  13.808 ms  10.620 ms
```

Traceroute

- **Traceroute. ¿Cuándo usarlo?**
- Imagine que quiere conectarse a www.uv.cl, pero no puede y no sabe que puede estar pasando.
- Puede que este fallando el servidor o puede que la falla este dentro de nuestra red.
- Se puede mandar un mensaje a www.uv.cl que va a ir rebotando por cada etapa hasta llegar al destino.
- Así se puede saber si la conexión se pierde en algún punto y donde.



Reconocimiento Mail

Reconocimiento

Marco Aravena Vivar

Marco Aravena Vivar
Académico Titular Escuela de Ingeniería Informática
Director General de Modernización y Transformación Digital.

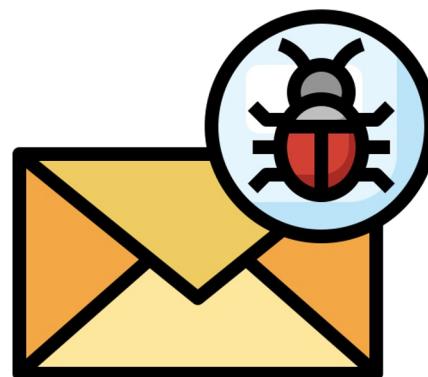
Reconocimiento de correo electrónico

- La huella de correo electrónico se refiere a la recopilación de información de los correos electrónicos mediante el seguimiento de la entrega del correo electrónico y la inspección de los encabezados.
- La información recopilada a través de la huella del correo electrónico incluye:
 - Dirección IP del destinatario
 - Geolocalización del destinatario
 - Información de entrega
 - Enlaces visitados
 - Información del navegador y del sistema operativo
 - Tiempo de lectura



Reconocimiento de correo electrónico

- Los encabezados de correo electrónico contienen información sobre el remitente, el asunto y el destinatario. Toda esta información es valiosa para los piratas informáticos cuando planean atacar a su objetivo.
- La información contenida en los encabezados de los correos electrónicos incluye:
 - Nombre del remitente
 - IP / dirección de correo electrónico del remitente
 - Servidor de correo
 - Sistema de autenticación del servidor de correo
 - Sello de envío y entrega



Reconocimiento de correo electrónico

- Un ejemplo de herramienta para reconocimiento de correo electrónico:
- <https://mailheader.org>

Analyze my mail header

About

This tool will make your email header legible by parsing each record. Email headers are present on every email you receive via the Internet, the email header is generated by the client mail program that first sends it and by all the mail servers en route to the destination.

Each node adds more text, including from/to addresses, subject, content type, time stamp and identification data. You can trace the path of the message from source to destination by reviewing the email header text.

Analyze my mail header

Please paste the mail header into the text box below and click submit.

Note, privacy is important to us and your data is secure with us, we will not store or forward any information provided; please refer to our privacy policy. If you just want to view a example mail header then click here: [Show Sample](#) or another - more complex [Sample](#)

```
Delivered-To: marco.aravena@gmail.com
Received: by 2002:a:b3:72d3:8:b0:27b:247d:7958 with SMTP id p19csp1027671lrf;
Fri, 20 Sep 2024 11:22:10 -0700 (PDT)
X-Google-Sntp-Source:
AGHT+HmzbB3xLPz2n...0x8e0HEp008kFCV1L+S/gmuPZ7HMYoNDbaezGs1BnXJ8VmKkoF2JZ
X-Received: by 2002:a:b3:72d3:8:b0:27b:247d:7958 with SMTP id ffacd0b85a97d-
37a42277desm/314505718f; Fri, 20 Sep 2024 11:22:09 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1726856529; cv=none;
d=google.com; s=arc-20240605;
a=rsa-sha256; c=relaxed/relaxed; d=google.com;
h=list-unsubscribe:list-unsubscribe-post:mime-version:subject:to:from
:date:message-id:dkim-signature;
```

Submit

Mail header analysis

Address Details

Mail From:	news@iknewsletter.com	Mail To:	marco.aravena@gmail.com
Mail From Name:	IK Multimedia Newsletter	Reply To:	

Message Details

Subject:	Un órgano real en sol o \$39.99	Content-Type:	multipart/alternative boundary== ==AGNITASOUTER164240059B29003BC1==
Date:	Fri, 20 Sep 2024 18:16:26 GMT	UTC Date:	Fri Sep 20 18:16:26 2024
MessageID:	20240920180450-1.1.bsx.12man.0.1708dcfr15@iknewsletter.com		

Message Transfer Agent (MTA) - Transfer Details

Mail Server From:	iknewsletter.com	Mail Server To:	iknewsletter.com
Mail Server From IP:	5.135.235.172	Mail Server To IP:	5.135.235.172
Mail Country From:	France	Mail Country To:	France
AS Name From:	OVH SAS	AS Name To:	OVH SAS
AS Number From:	AS16276	AS Number To:	AS16276
Distance (All Hops/Summary):	0/0.00 KM	Hops (All/Public):	5 / 1
MTA Encryption	Poor (*)	Delivery Time:	0 days, 0 hours, 5 min, 44 sec
Your IP:	181.42.20.133	Your GeoLoc:	Lat:-33.4521 Lon:-70.6536

Reconocimiento de correo electrónico

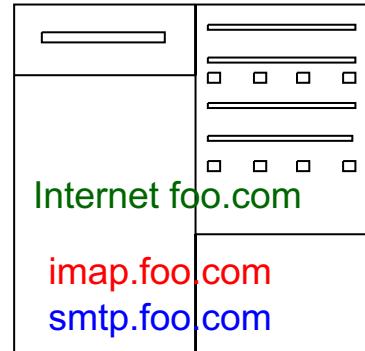
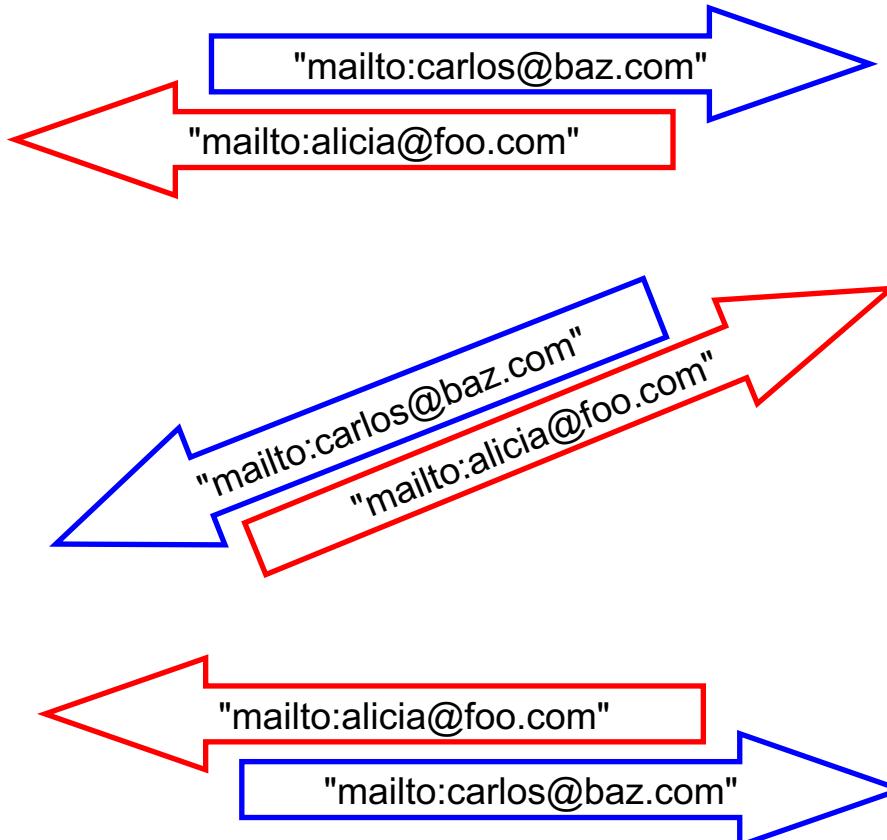
- También es posible rastrear correos electrónicos usando varias herramientas de rastreo. Las herramientas de seguimiento de correo electrónico tienen la capacidad de rastrear correos electrónicos e inspeccionar sus encabezados para extraer información útil.
- Se notifica al remitente que el destinatario ha entregado y abierto el correo electrónico. Un ejemplo: correos de tiendas comerciales para ver el alcance de las campañas que realizan.

Enviar

Reconocimiento de correo electrónico



alicia@foo.com



Responder



Universidad de Valparaíso
Hasta marzo de 2010
Acreditación CNA-Chile

Reconocimiento de correo electrónico

Mensaje original

ID de mensaje	<CAKNmkX6hgKW8aDQUN+LjZsFocFX5KRck7nH_gpr7dBb2dexuPA@mail.gmail.com>
Creado a las:	19 de noviembre de 2020, 9:59 (entregado en 12 segundos)
De:	Victor Ibaceta <victor.ibaceta@uv.cl>
Para:	marco aravena <marco.aravena@uv.cl>
Asunto:	Prueba de Correo
SPF:	PASS con la IP 209.85.220.41 Más información
DKIM:	'PASS' con el dominio uv.cl Más información
DMARC:	'PASS' Más información



[Descargar original](#)

CHILE

[Copiar en el portapapeles](#)



Investigación, Vinculación con el Medio y
Docencia de Postgrado
HASTA MARZO DE 2020



Reconocimiento de correo electrónico

Delivered-To: marco.aravena@uv.cl
Received: by 2002:a19:c08c:0:0:0:0:0:0 with SMTP id y12csp3206811ff;
Thu, 19 Nov 2020 04:59:38 -0800 (PST)
X-Received: by 2002:a4d:47b0:: with SMTP id a16m10566195qvz.22.1605790778180;
Thu, 19 Nov 2020 04:59:38 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1605790778; cv=none;
d=google.com; s=arc-20160816;
b=UvShdem0/xubyizXtL6n+37OwefZ0E0B009rPCKEF733mHDorEBjhzddmoReR2RYvT
K911K9tYGVY1E2eokst0Taav0jInqH0lW9x1Rdbva0/TQE10nV1k1mkOurAOPIGV
VP0eCCKMq1snFhMqI31omvggn8iuM+2ET2rVnW/mhn19eEjU7G7jgjn1BCKghR4x4Et
BYBwLqlSgpnexSXx_KmmHSBRnCH+43V/B99f9FTp2GmAT0U0le6ub8fbk1mPVfb5h
OFKGXBx1+Hnnqavav1wQBRN4H40xNMFxblgbnzz/uUh/q1s1bqaqRrTnzA5n61nkp
g8mew=
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
h-to:subject:message-id:date:from:mime-version:dkim-signature;
bh=cpk94G4BeYvhpuzCIAJ/EmT0k1iwszN0MTe0d8L1=;
b=TycPM44/YuFip0ed1eJASmdq140LzNtDGrnTUgtV1W4nQhULBtzbYQgkAoAwx
b73Taly9u04s1lfyChu23XQxbuL0t0h2v0lrSAAHXQh1ZhPcDsy9meX136QD
bockhafVyuzejlaVFjNgQT8wysyk619Kp1ZA+h0hdmpBuQpn1Q0w335wq10Yhf
pvG0nn1N863Y1R1PBkWlpmpH70Ok/Kv+o9qf8r7fj82kp8UonuzQx53gXx8dpqb
1/1kuGKt40lp6m3JzW6k+22BAZDXIA/DccGHDqulEJwiagABnCF44G3qw+pByX6sJ6R
jDmew=
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@uv.cl header.s=google header.b=qTSC0DON;
spf=pass (google.com: domain of victor.ibaceta@uv.cl designates 209.85.220.41 as permitted sender)
smtp.mailfrom=victor.ibaceta@uv.cl;
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=uv.cl
Return-Path: <victor.ibaceta@uv.cl>
Received: from mail-sor-f41.google.com (mail-sor-f41.google.com. [209.85.220.41])
by mx.google.com with SMTPS id k1sor13387764qtm.31.2020.11.19.04.59.38
for <marco.aravena@uv.cl>
(Google Transport Security);
Thu, 19 Nov 2020 04:59:38 -0800 (PST)
Received-SPF: pass (google.com: domain of victor.ibaceta@uv.cl designates 209.85.220.41 as permitted sender) client-ip=209.85.220.41
Authentication-Results: mx.google.com;
dkim=pass header.i=@uv.cl header.s=google header.b=qTSC0DON;
spf=pass (google.com: domain of victor.ibaceta@uv.cl designates 209.85.220.41 as permitted sender)
smtp.mailfrom=victor.ibaceta@uv.cl;
dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=uv.cl
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=uv.cl; s=google;
h=mime-version:from:date:message-id:subject:to;
bh=cpk94G4BeYvhpuzCIAJ/EmT0k1iwszN0MTe0d8L1=;
b=qTSC0DONHEgmP0b4p015+vYHejTSp59Y1tD/wdCEaAMividvSt/HlmJ1jzkD
4zcgfJ06/72t1N1qj0qf9UUA6NaNsqja1oQ92Q5ZL1cIP2+lXQ2bucuj3/r/c+zIt
nBNKwN7td+ioF32wXnrGL6yxrBrz/w/9j4y=
X-Google-OKIM-Signature: v=1 a=sa-sha256 c=relaxed/relaxed;
d=1e180.net; s=20161025;
h=x-gm-magic-signature-date-version:from:date:message-id:subject:to;
bh=cpk94G4BeYvhpuzCIAJ/EmT0k1iwszN0MTe0d8L1=;
b=j9WzqGv5lMGDU1qsdh2j3jHTSGCdqj203105G0Cs1khe3N3pJPT5FCNk
dvcX3HpnufFSDVwvh/TncKLoJu1U5hK5qEo0lE16G67B8g8CVe03GrtMcJrmdt36
TUTuRhQ1x+xE15U3hB78nckpdqh86NqC81E1122X1Nkwzsr60s3QUhjdh1pa0853
avF7QuQ+kmtGge7oI8eXfmhxt3Mlag/hz5f3y7VRChW0FxzCbm11i5nw1LBAX+23G
pp0F11uallXehbu41w+yic+1xoD/ps1ZNj724jogjt4EXd41TgdH+c7toikTAf2esRtSzR
3kbA==
X-Gm-Message-State: AOA5321XE185gwcaFcJp0apJYckA/jxjocV2gnlw+Tdsvo0d1kdiqg
s@vt3r2BrlzUFhZ99+6RKhCo+jBnPz/BXP2zKmfb52qms2wRPI5
X-Google-Smtph-Source: ABdnP3wpC4rrCwTBewJvrLat4uCfogBtfUeb080ZsT0IcmcyXgFifqjHIEm02816G2gfz1XUzr0d9H60c4uYIm4=
X-Received: by 2002:a8:221b:: with SMTP id o27mr1029217qto.54.1605790777384; Thu, 19 Nov 2020 04:59:37 -0800 (PST)
MIME-Version: 1.0
From: Victor Ibaceta <victor.ibaceta@uv.cl>
Date: Thu, 19 Nov 2020 04:59:26 -0300
Message-ID: <CAKNmX6hgKWBabQUN+ljzfocFX5KRck7nh_gpr7dBb2dexuA@mail.gmail.com>
Subject: Prueba de Correo
To: marco aravena <marco.aravena@uv.cl>
Content-Type: multipart/alternative; boundary="00000000000debb0f05b4754c0"



Acreditada
NIVEL DE EXCELENCIA
Gestión Institucional, Docencia de Pregrado
Investigación, Vinculación con el Medio y
Docencia de Postgrado

HASTA MARZO DE 2020



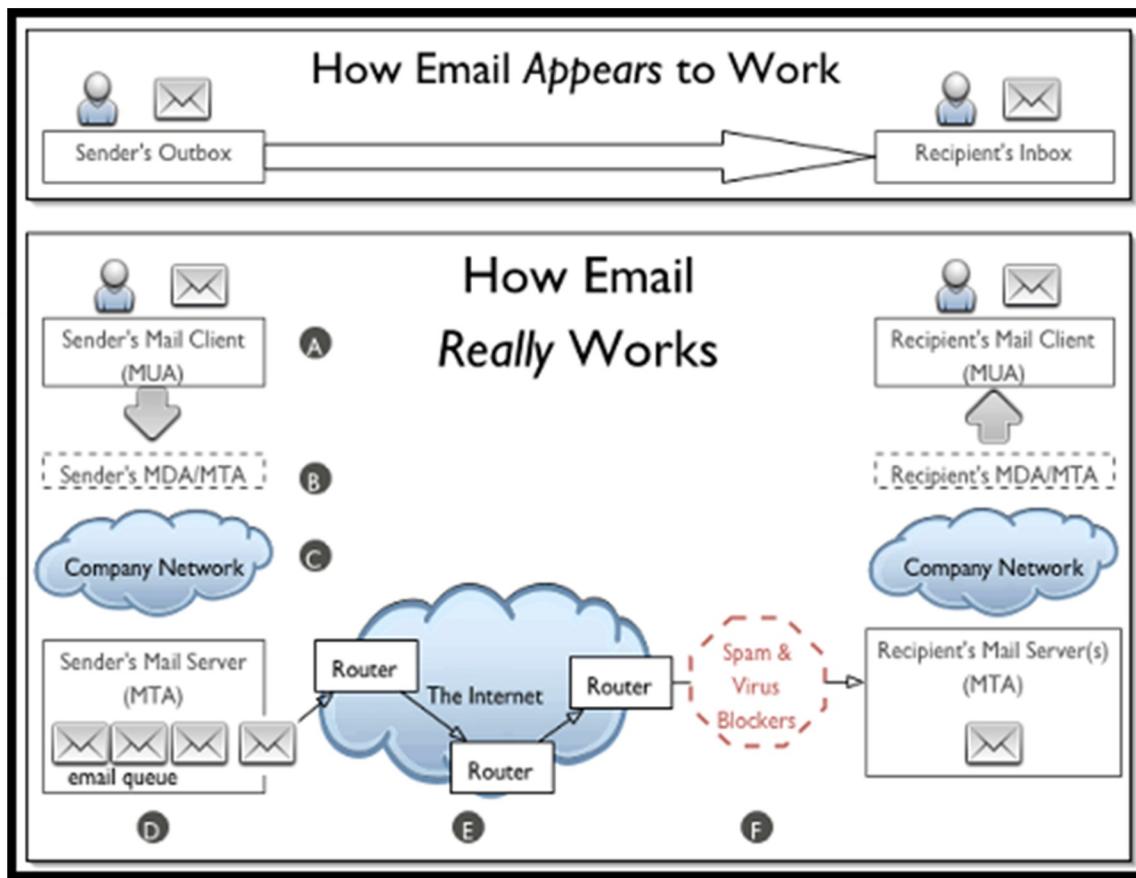
Reconocimiento de correo electrónico



**ACREDITADA
NIVEL DE EXCELENCIA**



Reconocimiento de correo electrónico





Reconocimiento Sitio Web

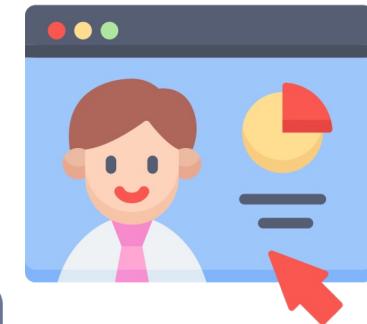
Reconocimiento

Marco Aravena Vivar

Marco Aravena Vivar
Académico Titular Escuela de Ingeniería Informática
~~Ingeniería Civil~~
Director General de Modernización y Transformación Digital.

Reconocimiento de sitio web

- La huella del sitio web es una técnica en la que se recopila información sobre el objetivo mediante el seguimiento del sitio web del objetivo. Los hackers pueden mapear todo el sitio web del objetivo sin que se den cuenta.
 - La huella del sitio web brinda información sobre:
 - Software.
 - Sistema operativo.
 - Subdirectorios.
 - Información del contacto.
 - Plataforma de scripting.
- Detalles de consulta.



Reconocimiento de sitio web

- Al examinar los encabezados del sitio web, es posible obtener información sobre los siguientes encabezados:
 - Tipo de contenido.
 - Estado de conexión.
 - Información modificada por última vez.
 - Información del servidor web.



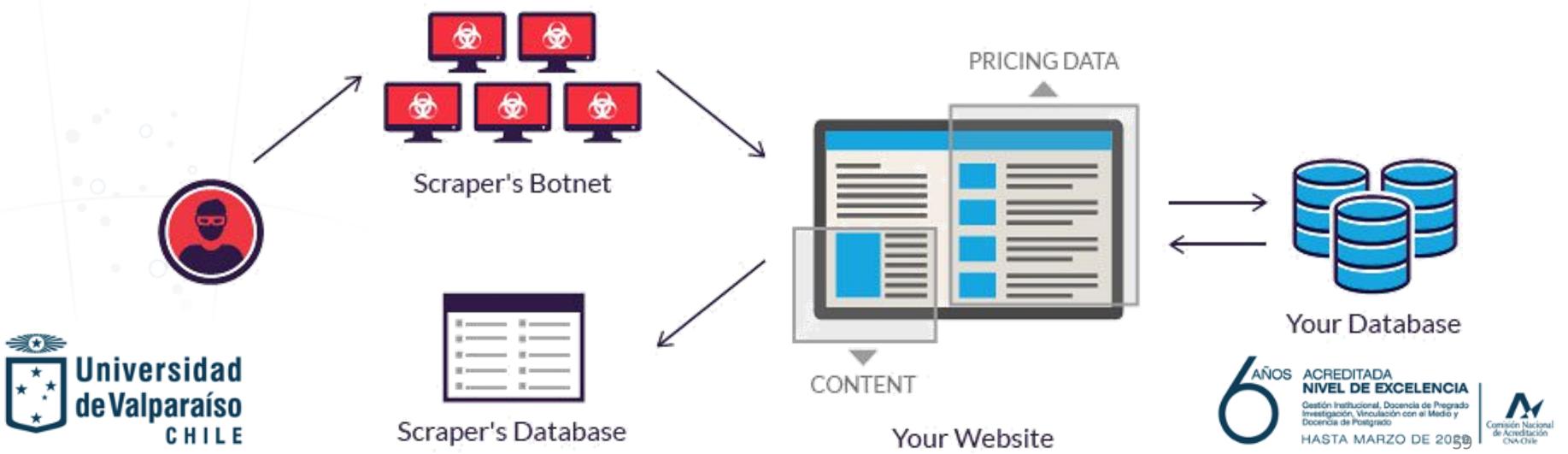
Reconocimiento de sitio web

- Las formas adicionales de recopilar información son a través del código fuente HTML y las cookies. Al examinar el código fuente HTML, es posible extraer información de los comentarios en el código, así como obtener información sobre la estructura del sistema de archivos mediante la observación de los enlaces y las etiquetas de las imágenes.
- Las cookies también pueden revelar información importante sobre el software que se ejecuta en el servidor y su comportamiento. Además, al inspeccionar las sesiones, es posible identificar las plataformas de scripting.



Reconocimiento de sitio web

- Hay programas diseñados para ayudar en la huella del sitio web y estos programas se denominan arañas web que navegan metódicamente por un sitio web en busca de información específica.
- La información recopilada de esta manera puede ayudar a los atacantes a realizar ataques de ingeniería social.
- Esta técnica es conocida como scraping.





Para finalizar

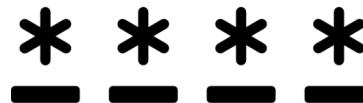
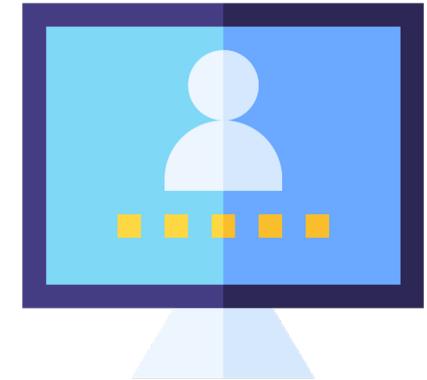
Reconocimiento

Marco Aravena Vivar
Académico Titular Escuela de Ingeniería Informática
~~Ingeniería Civil~~
Director General de Modernización y Transformación Digital.

Reconocimiento

Los atacantes utilizan el reconocimiento para recopilar la siguiente información:

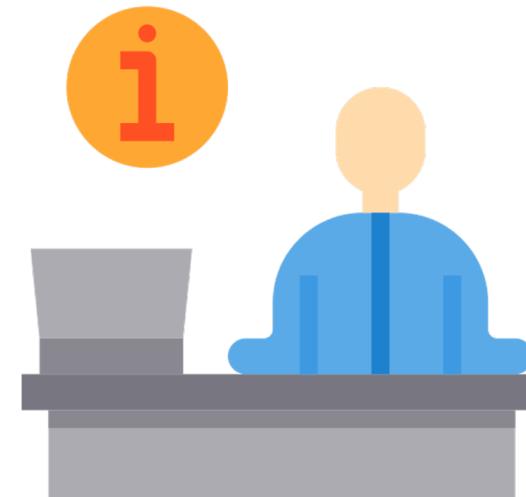
- Información del sistema
 - Sistemas operativos de servidor (web, correo, dns.....)
 - Ubicaciones del servidor
 - Puertos...
 - Propietario de dominio
 - IP's....



Reconocimiento

Los atacantes utilizan el reconocimiento para recopilar la siguiente información:

- Información de la organización
 - Información del empleado
 - Antecedentes de la organización
 - Números de teléfono
 - Ubicaciones



Ataque de reconocimiento

Consultas a través de internet



Barridos de ping



Escaneo de puertos



Programas detectores de paquetes

Reconocimiento

- **Consultas a través de internet.** <https://www.whois.com/whois/uv.cl> .

uv.cl Updated 56 days ago 

```
%%
%% 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: uv.cl
Registrant name: Universidad de Valparaíso (UNIVERSIDAD DE VALPARAISO)
Registrant organisation:
Registrar name: NIC Chile
Registrar URL: https://www.nic.cl
Creation date: 1996-04-29 14:37:37 CLST
Expiration date: 2022-01-15 17:37:13 CLST
Name server: ns.uv.cl (200.14.68.75)
Name server: secundario.nic.cl

%%
%% For communication with domain contacts please use website.
%% See https://www.nic.cl/registry/Whois.do?d=uv.cl
%%
```

Reconocimiento

- **Barrios de ping**

Iniciando nmap V. 3.00 (www.insecure.org/nmap)

Host aus1.cinko.com (10.10.10.2) appears to be up.
Host aus2.cinko.com (10.10.10.3) appears to be up.
Host aus3.cinko.com (10.10.10.4) appears to be up.
Host aus4.cinko.com (10.10.10.5) appears to be up.

Reconocimiento

- Escaneo de puertos.

Barrido del puerto NMAP

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 3.5p1 (p)
53/tcp	open	domain	ISC Bind 9.2.1
111/tcp	open	rpcbind	2 (rpc #100000)
631/tcp	open	ipp	CUPS 1.1
953/tcp	open	rndc?	

Reconocimiento

- Programa detectores de paquetes.

Wireshark

HTTP	GET / HTTP
TCP	80 > 1242 [ACK] Seq - 366161510
TCP	1242 > 80 [FIN, ACK] Seq-1404
TCP	HTTP/1.1 403 Forbidden (text/HHTTP)
HTTP	1242 > 80 [RST] Seq - 1404511235
TCP	1244 > 135 [SYN] Seq - 141445223
TCP	135 > 1244 [SYN, ACK] Seq-3672
TCP	1244 > 135 [ACK] Seq-141445223
DCERPC Bind:	call_id: 57 UUID:IOXIDP

Reconocimiento

- Algunas de las medidas que se pueden tomar para mitigar el reconocimiento son:
 - Restringir el acceso a las redes sociales.
 - Hacer cumplir las políticas de seguridad.
 - Educar a los empleados sobre las amenazas a la seguridad.
 - Cifrar información sensible.
 - Deshabilitar protocolos que no son necesarios.
 - Configuración de servicio adecuada (hardening)

Para concluir

- El reconocimiento pasivo NO implica interacción con el objetivo y la información que se obtiene es general. Tiene menos riesgo de detección y es un aporte para delimitar el reconocimiento activo (IP por ejemplo).
- El reconocimiento activo le puede brindar al atacante información sobre las políticas de seguridad que se adoptan en el lugar (servicios/puertos abiertos, por ejemplo), pero este proceso también aumenta la posibilidad de ser descubierto o al menos despertar sospechas.



Marco Aravena Vivar
Académico Titular Escuela de Ingeniería
Director General de Modernización y Transformación Digital.

