

SEGURIDAD INFORMATICA

PRESENTADO POR:

CRISTHIAN MAURICIO LOZANO TROCHEZ

DOCENTE

JOSE GUERLLY LARA

CORPORACION UNIVERSITARIA AUTONOMA DEL CAUCA

FACULTAD DE INGENIERIA

POPAYAN-CAUCA

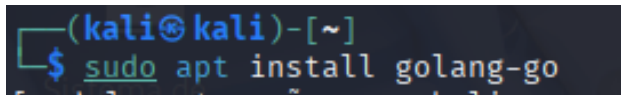
2025

1) Leer el documento HerramientasYGoogleHacking, elegir una herramienta de las que están como ejemplo, pero que no esté descrita en este documento y realizar una práctica y su respectivo tutorial.

Primero instalamos Go:

```
sudo apt update
```

```
sudo apt install golang-go
```



```
(kali@kali)-[~]  
$ sudo apt install golang-go
```

Después decargamos Subfinder:

```
go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest
```



```
(kali@kali)-[~]  
$ go install -v github.com/projectdiscovery/subfinder/v2/cmd/subfinder@latest  
go: downloading github.com/projectdiscovery/subfinder/v2 v2.7.0  
go: downloading github.com/projectdiscovery/subfinder v2.7.0+incompatible  
go: downloading github.com/projectdiscovery/gologger v1.1.44  
go: downloading github.com/projectdiscovery/fdmax v0.0.4  
go: downloading github.com/hako/durafmt v0.0.0-20210316092057-3a2c319c1acd  
go: downloading github.com/json-iterator/go v1.1.12  
go: downloading github.com/projectdiscovery/chaos-client v0.5.2  
go: downloading github.com/projectdiscovery/dnsx v1.2.2  
go: downloading github.com/projectdiscovery/goflags v0.1.72  
go: downloading github.com/projectdiscovery/utils v0.4.11  
go: downloading golang.org/x/exp v0.0.0-20230420155640-133eef4313cb  
go: downloading gopkg.in/yaml.v3 v3.0.1
```

Ahora hacemos un escaneo a un dominio:

```
(kali@kali)-[~]
$ subfinder -d hackthebox.com -o htb-subdominios.txt

projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for hackthebox.com
academy-cdn.hackthebox.com
maintenance.hackthebox.com
app.hackthebox.com
forum-staging.hackthebox.com
flock-ng.hackthebox.com
trust.hackthebox.com
proxy.hackthebox.com
affiliate.hackthebox.com
airflow.data-dev.hackthebox.com
jobs.hackthebox.com
proxy.www.hackthebox.com
academy.hackthebox.com
sso.hackthebox.com
noahbot.hackthebox.com
proxy.enterprise.hackthebox.com

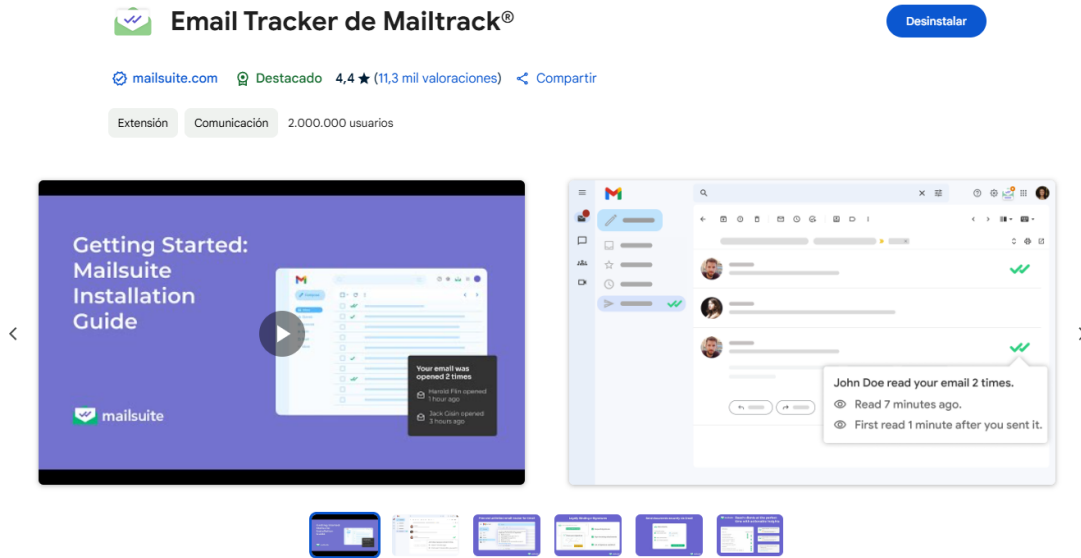
[INF] Found 57 subdomains for hackthebox.com in 5 seconds 39 milliseconds
```

2) Realizar un seguimiento huella de correo electrónico con alguna de las herramientas gratuitas descritas en el anterior documento.

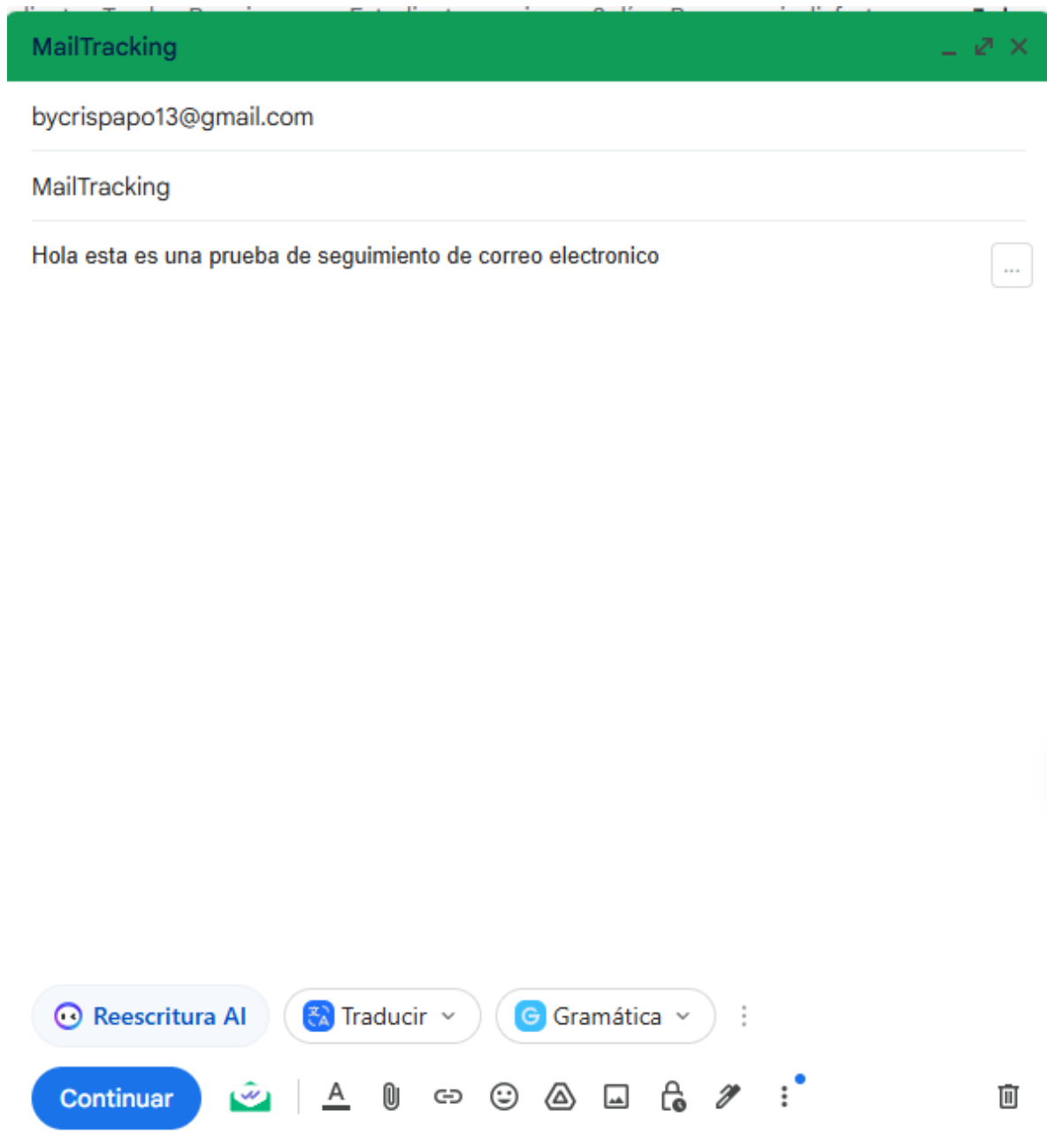
PARA HACER SEGUIMIENTO DE CORREO, UTILIZAMO MAILTRACKING.

Este programa es gratuito, pero tiene formas de paga, funciona de la siguiente manera:

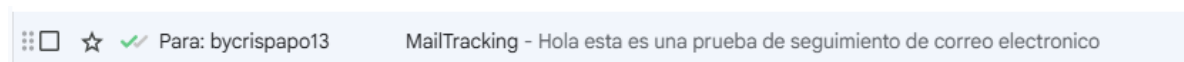
- 1) Añadimos la extensión a Google:



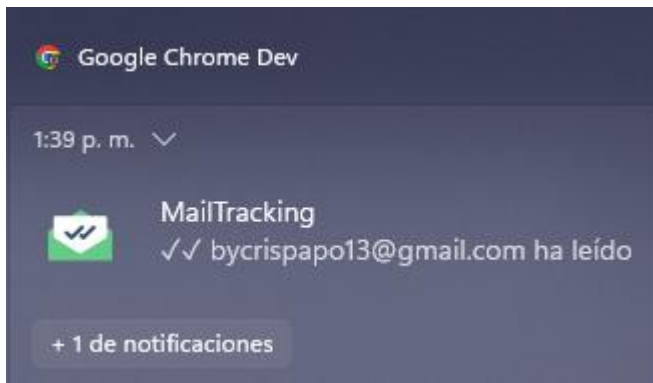
- 2) Automáticamente la aplicación nos pedirá iniciar con el correo y siempre que queramos enviar un mensaje y este la extensión activada, el programa empezará a funcionar.
- Para esta prueba vamos a enviarnos un mensaje a uno de nuestros propios correos.



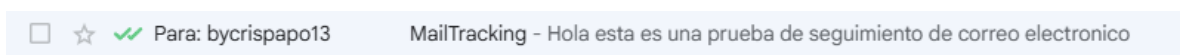
Podemos ver utilidades como por ejemplo los dos chulitos, que al momento de enviarlo se ve así:



Cuando el usuario ve el mensaje nos llega una notificación de la siguiente manera:



Y automáticamente aparecerán los dos chulitos como vistos:



También dentro de su interfaz podemos ver un resumen de las estadísticas de los correos enviados.

Email tracking

Last opened emails [Download CSV](#)

RECIPIENTS	EMAIL	ACTIVITY	ACTIONS
bycrispapo13@gmail.com	MailTracking Sent on Apr 11, 2025 at 1:38 PM	1 open First open on Apr 11, 2025 at 1:39 PM	...

Esta técnica funciona porque envían un píxel invisible el cual se carga desde un servidor cuando el destinatario abre el correo, permitiendo a Mail rack registrar esta interacción y proporcionar datos sobre cuándo y dónde se visualizó el mensaje.

3) ESCANEOS CON NMAP

Escaneo TCP SYN (-sS)

Nombre: Escaneo SYN o escaneo semi-abierto.

Descripción: Envía paquetes SYN para verificar si un puerto está abierto sin completar la conexión TCP.

```
(kali㉿kali)-[~]  
$ sudo nmap -sS 10.0.2.5  
[sudo] contraseña para kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:36 EDT  
Nmap scan report for 10.0.2.5  
Host is up (0.0019s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Escaneo UDP (-sU)

Nombre: Escaneo de puertos UDP.

Descripción: Detecta servicios que usan el protocolo UDP. Es más lento que el escaneo TCP.

```
(kali㉿kali)-[~]  
$ sudo nmap -sU 10.0.2.5  
  
[sudo] contraseña para kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:37 EDT  
Nmap scan report for 10.0.2.5  
Host is up (0.0013s latency).  
Not shown: 993 closed udp ports (port-unreach)  
PORT      STATE      SERVICE  
53/udp    open|filtered domain  
68/udp    open|filtered dhcpd  
69/udp    open|filtered tftp  
111/udp   open|filtered rpcbind  
137/udp   open|filtered netbios-ns  
138/udp   open|filtered netbios-dgm  
2049/udp  open|filtered nfs  
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap done: 1 IP address (1 host up) scanned in 1088.85 seconds
```

Escaneo TCP NULL (-sN)

Nombre: Escaneo NULL.

Descripción: Envía un paquete TCP sin ningún flag. Algunos sistemas lo interpretan como una técnica de evasión.


```

(kali㉿kali)-[~] https://nmap.org ) at 2025-04-11 23:37 EDT
└─$ sudo nmap -sN 10.0.2.5
[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:42 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00056s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2049/tcp  open|filtered nfs
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8009/tcp  open|filtered ajp13
8180/tcp  open|filtered unknown
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.97 seconds

```

Escaneo TCP FIN (-sF)

Nombre: Escaneo FIN.

Descripción: Envía paquetes con solo el flag FIN. Puede evadir algunos firewalls.

```
(kali㉿kali)-[~]  
$ sudo nmap -sF 10.0.2.5  
  
[sudo] contraseña para kali:  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:43 EDT  
Nmap scan report for 10.0.2.5  
Host is up (0.0010s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE      SERVICE  
21/tcp    open|filtered ftp  
22/tcp    open|filtered ssh  
23/tcp    open|filtered telnet  
25/tcp    open|filtered smtp  
53/tcp    open|filtered domain  
80/tcp    open|filtered http  
111/tcp   open|filtered rpcbind  
139/tcp   open|filtered netbios-ssn  
445/tcp   open|filtered microsoft-ds  
512/tcp   open|filtered exec  
513/tcp   open|filtered login  
514/tcp   open|filtered shell  
1099/tcp  open|filtered rmiregistry  
1524/tcp  open|filtered ingreslock  
2049/tcp  open|filtered nfs  
2121/tcp  open|filtered ccproxy-ftp  
3306/tcp  open|filtered mysql  
5432/tcp  open|filtered postgresql  
5900/tcp  open|filtered vnc  
6000/tcp  open|filtered X11  
6667/tcp  open|filtered irc  
8009/tcp  open|filtered ajp13  
8180/tcp  open|filtered unknown  
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```

Escaneo TCP Xmas (-sX)

Nombre: Escaneo "Xmas tree" (árbol de navidad).

Descripción: Envía paquetes con los flags FIN, URG y PSH. Se llama así porque "brillan como un árbol de navidad".

```
(kali㉿kali)-[~]
└─$ sudo nmap -sX 10.0.2.5

[sudo] contraseña para kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:45 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00039s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE      SERVICE
21/tcp    open|filtered ftp
22/tcp    open|filtered ssh
23/tcp    open|filtered telnet
25/tcp    open|filtered smtp
53/tcp    open|filtered domain
80/tcp    open|filtered http
111/tcp   open|filtered rpcbind
139/tcp   open|filtered netbios-ssn
445/tcp   open|filtered microsoft-ds
512/tcp   open|filtered exec
513/tcp   open|filtered login
514/tcp   open|filtered shell
1099/tcp  open|filtered rmiregistry
1524/tcp  open|filtered ingreslock
2049/tcp  open|filtered nfs
2121/tcp  open|filtered ccproxy-ftp
3306/tcp  open|filtered mysql
5432/tcp  open|filtered postgresql
5900/tcp  open|filtered vnc
6000/tcp  open|filtered X11
6667/tcp  open|filtered irc
8009/tcp  open|filtered ajp13
8180/tcp  open|filtered unknown
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
```

Escaneo TCP Connect (-sT)

Nombre: Escaneo TCP completo (conexión completa).

Descripción: Usa la llamada al sistema connect() del sistema operativo. No requiere privilegios de root.

```
(kali@kali)-[~]
$ nmap -sT 10.0.2.5

Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:46 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0035s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds
```

Escaneo ACK (-sA)

Nombre: Escaneo ACK.

Descripción: No identifica puertos abiertos, pero ayuda a identificar reglas de filtrado (firewalls).

```
(kali㉿kali)-[~]  
$ sudo nmap -sA 10.0.2.5  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:47 EDT  
Nmap scan report for 10.0.2.5  
Host is up (0.00035s latency).  
All 1000 scanned ports on 10.0.2.5 are in ignored states.  
Not shown: 1000 unfiltered tcp ports (reset)  
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```

Escaneo Window (-sW)

Nombre: Escaneo de ventana TCP.

Descripción: Similar al escaneo ACK, pero intenta deducir si un puerto está abierto a partir del tamaño de la ventana TCP.

```
(kali㉿kali)-[~]  
$ sudo nmap -sW 10.0.2.5  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:48 EDT  
Nmap scan report for 10.0.2.5  
Host is up (0.00039s latency).  
All 1000 scanned ports on 10.0.2.5 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

Escaneo Maimon (-sM)

Nombre: Escaneo Maimon.

Descripción: Envía un paquete TCP con los flags FIN/ACK. Es una técnica más inusual de evasión.

```
(kali㉿kali)-[~]  
$ sudo nmap -sM 10.0.2.5  
  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 23:52 EDT  
Nmap scan report for 10.0.2.5  
Host is up (0.0010s latency).  
All 1000 scanned ports on 10.0.2.5 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
MAC Address: 08:00:27:83:CC:02 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

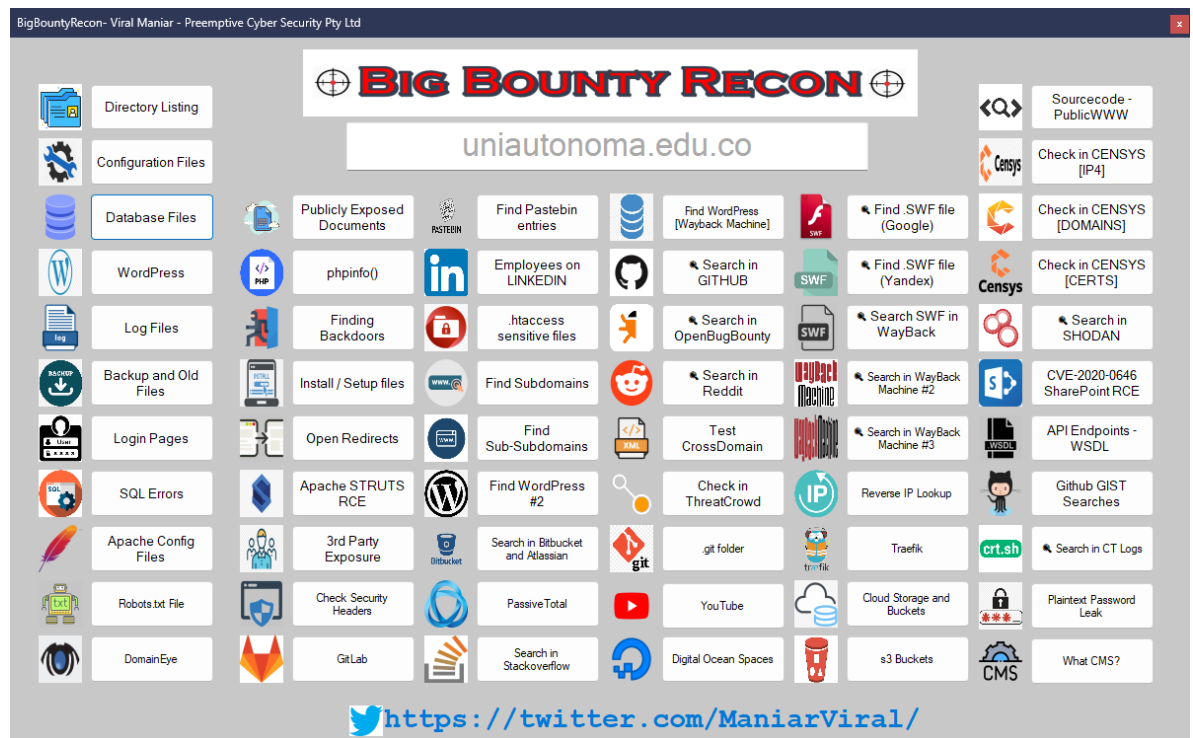
4) Investigar sobre el funcionamiento de la herramienta BigBountyRecon y realizar un ejemplo.

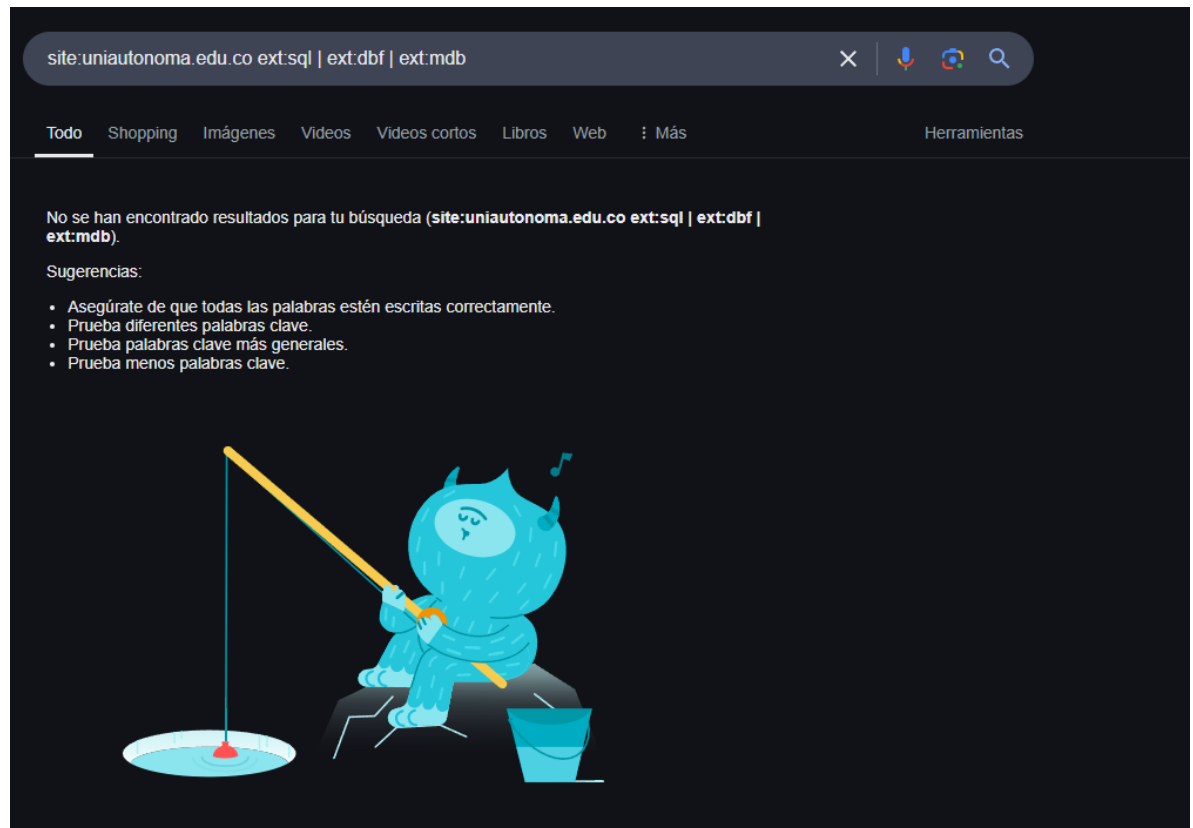
BigBountyRecon es una herramienta automatizada diseñada para facilitar la recolección de información de forma masiva sobre dominios y subdominios. Está enfocada especialmente en ayudar a bug bounty hunters a encontrar vulnerabilidades en programas públicos o privados de forma eficiente.

BigBountyRecon ejecuta una serie de herramientas de recolección bajo un solo flujo, lo que permite automatizar tareas como:

- Enumeración de subdominios.
- Resolución de DNS.

- Detección de subdominios vivos (HTTP/S).
- Screenshots de los subdominios (via aquatone o similar).
- Recolección de URLs con herramientas como waybackurls o gau.
- Verificación de vulnerabilidades comunes (ej: subdomain takeover, SSRF, etc.).





5) Investigar sobre un caso reconocido a nivel mundial sobre ingeniería social y socializarlos con sus compañeros.

Kevin Mitnick fue un famoso hacker estadounidense que durante los años 80 y 90 se convirtió en el criminal informático más buscado por el FBI. Lo más impresionante de su historia es que gran parte de sus ataques no los hizo con herramientas tecnológicas complejas, sino usando ingeniería social: manipular a personas para obtener información sensible.

Llamaba a empleados de grandes empresas (como Motorola, Nokia y Sun Microsystems) haciéndose pasar por compañeros de trabajo o técnicos de soporte.

Les pedía contraseñas, accesos remotos o información interna.

Con eso, accedía a los sistemas, copiaba software propietario y espiaba comunicaciones.

Todo esto sin romper literalmente puertas digitales, sino convenciendo a la gente.

Fue arrestado en 1995 y sentenciado por varios cargos de fraude informático y acceso no autorizado.

Estuvo cinco años en prisión, ocho meses en confinamiento solitario porque se decía que era tan peligroso que "podía iniciar una guerra nuclear silbando en un teléfono".

Luego se convirtió en consultor de seguridad, autor de libros y conferencista. Hoy es una figura clave en la concienciación sobre ciberseguridad.

PRUEBAS DE RECONOCIMIENTO:

Usas Dmitry para hacer una prueba a la ip de metasploitable:

```
(kali㉿kali)-[~]  
$ dmitry -p -b 10.0.2.5  
Deepmagic Information Gathering Tool  
"There be some deep magic going on"  
  
ERROR: Unable to locate Host Name for 10.0.2.5  
Continuing with limited modules  
HostIP:10.0.2.5  
HostName:  
  
Gathered TCP Port information for 10.0.2.5  
-----  
  
Port          State  
21/tcp        open  
>> 220 (vsFTPd 2.3.4)  
  
22/tcp        open  
>> SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1  
  
23/tcp        open  
>> ♦♦♦♦♦ ♦♦#♦♦♦  
  
25/tcp        open  
>> 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)  
  
53/tcp        open  
  
Portscan Finished: Scanned 150 ports, 144 ports were in state closed  
  
All scans completed, exiting  
  
(kali㉿kali)-[~]  
$
```

Recolectamos información de un DNS, mediante dnsenum:

```
(kali@kali)-[~]  
$ dnsenum scanme.org  
dnsenum VERSION:1.3.1
```

```
----- scanme.org -----
```

Host's addresses:

scanme.org.	3600	IN	A	45.33.32.156
-------------	------	----	---	--------------

Name Servers:

ns2.linode.com.	300	IN	A	92.123.94.3
ns3.linode.com.	46	IN	A	92.123.95.3
ns4.linode.com.	32	IN	A	92.123.95.4
ns5.linode.com.	300	IN	A	92.123.95.2
ns1.linode.com.	300	IN	A	92.123.94.2

Mail (MX) Servers:

mail.titan.net.	3600	IN	A	64.13.134.2
-----------------	------	----	---	-------------

Trying Zone Transfers and getting Bind Versions:

```
Trying Zone Transfer for scanme.org on ns2.linode.com ...  
AXFR record query failed: corrupt packet
```

```
Trying Zone Transfer for scanme.org on ns3.linode.com ...  
AXFR record query failed: corrupt packet
```

```
Trying Zone Transfer for scanme.org on ns4.linode.com ...  
AXFR record query failed: corrupt packet
```

```
Trying Zone Transfer for scanme.org on ns5.linode.com ...  
AXFR record query failed: corrupt packet
```

```
Trying Zone Transfer for scanme.org on ns1.linode.com ...  
AXFR record query failed: corrupt packet
```

Usamos Nikto para capturar vulnerabilidades de un servidor web:

```
--(kali@kali):~$
$ nikto -h 10.0.2.5
Nikto v2.5.8

+-----+
+ Target IP:      10.0.2.5
+ Target Hostname: 10.0.2.5
+ Target Port:    80
+ Start Time:     2025-04-11 01:32:37 (GMT-4)
+-----+

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The x-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'len' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698bdc59d15_https://exchange4force.blob.core.windows.net/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active, which suggests the host is vulnerable to XST. See: https://cwsap.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /%PMP%P568F36-D428-11D2-A769-00AA001ACFA2: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /%PMP%P568F36-D428-11D2-A769-00AA001ACFA2: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /%PMP%P568F36-D428-11D2-A769-00AA001ACFA2: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /%PMP%P568F36-D428-11D2-A769-00AA001ACFA2: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/changelog: Server may leak inodes via ETags: header found with file /phpMyAdmin/changelog. inode: 52459, size: 40548, etime: Tue Dec 9 12:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CVE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /wp-config.php: wp-config.php file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:     2025-04-11 01:33:25 (GMT-4) (48 seconds)
```

MALTEGO

TUVE UN ERROR CON EL PROGRAMA Y NO LO PUDE UTILIZAR A TIEMPO...