UT.2.

Ataque y defensa en entorno de pruebas, de redes y sistemas para acceder a sistemas de terceros:

Fase 1: Reconocimiento (Footprinting):

¿Cómo te ven desde fuera de tu empresa?
¿Eres un objetivo para un hacker de sombrero negro?
¿Qué información está expuesta en Internet sobre tu empresa?

OBJETIVO: Buscar la mayor información posible sobre la empresa a auditar en fuentes abiertas. Descubrir el perímetro de una red corporativa (rango IPs de redes), Servidores DNS, IPs de la organización, dominios y subdominios, servidores de correo, correos electrónicos, teléfonos, nombres de empleados, documentos, …

Herramientas para esta fase:

- De líneas de comando (CLI: *Command Line Interface*)
  `whois, nslookup, host, dig, …`
- Búsquedas automáticas
  `subfinder, dnsrecon, fierce, dnsenum, sublist3r, theHarvester, …`
- De todo en uno
  `spiderfoot, maltego, …`

- **Infocif**: Si eres una empresa española, podemos empezar a buscar información sobre tu empresa en https://www.infocif.es/

  a. Buscar información sobre algunas empresas:
     i. **Aguas de Teror S.L.**
     ii. **ETSA S.L.**

- **WHOIS**: Whois es un protocolo basado en petición y respuesta que se utiliza para efectuar **consultas en una base de datos**, la cual nos permite determinar el propietario de un nombre de dominio o una dirección IP en Internet. Lo primero que haremos será obtener toda la información posible de un dominio de internet. Para ello utilizaremos el comando **whois**, herramienta que permite consultar los datos de registro de un dominio.

  - Para el ejemplo del whois utilizaremos los dominios:
    - bmw.com
    - ulpgc.es
    - etsa.es
    - cock.li
    - aguasdeteror.com
    - aguasdefirgas.com
    - camaramurcia.es

Realizamos la consulta al dominio **bmw.com** (ARIN)

```
# whois bmw.com
# whois aguasdeteror.com
# whois camaramurcia.es ¿?
# whois ulpgc.es ¿?
```

De toda la información que muestra el comando, lo más relevante de la salida de este comando serían los **servidores de nombre** y direcciones de **correo electrónico**.

Nota: intenta buscar un dominio con el TLD `.li`

```
Whois cock.li
Whois quepasa.li
Whois quepasa.ar → ahora sí
```

Top level domains: .es, .it, .de, .li, .uk, …

Vienen definidos en una iso y nos van a permitir hacer consultas para saber si los dominios están registrados o no. Para hacer la consulta de estos dominios podríamos ir consultando todos los dominios mediante un ***whois*** pero es más fácil utilizar una herramienta que nos haga la tarea de forma automática.

Es decir, por ejemplo, podríamos ir probando todos los ***tops level domains*** de **bmw** mediante un whois y ver si existen.

Con el comando **dnsrecon** vamos ir haciendo una consulta ***dns*** para ver si tienen una dirección ip o no.

El comando va mostrando las distintas ips de todos los dominios que encuentra. De todos los dominios tendremos que hacer un whois para saber si los dominios pertenecen a la misma compañía o en cambio pertenecen a otra.

```
# dnsrecon -t tld -d bmw
# dnsrecon –d aguasdeteror.com
# dnsrecon –d camaramurcia.es
```

```
root@kali:/home/kali# dnsrecon -t tld -d bmw
[*] Performing TLD Brute force Enumeration against bmw
[*] The operation could take up to: 00:01:35
[+] {'type': 'A', 'name': 'bmw.museum', 'address': '160.46.244.54'}
[+] {'type': 'A', 'name': 'bmw.xyz', 'address': '137.74.127.233'}
[+] {'type': 'A', 'name': 'bmw.jobs', 'address': '62.245.246.210'}
[+] {'type': 'A', 'name': 'bmw.info', 'address': '160.46.244.131'}
[+] {'type': 'A', 'name': 'bmw.xxx', 'address': '49.12.41.238'}
[+] {'type': 'A', 'name': 'bmw.xxx', 'address': '116.203.29.187'}
```

NOTA: Probar consultar un dominio **.es** para que nos salga información de ir a la página de dominios.es (www.nic.es)
Por ejemplo, si intentamos sacar la información de un dominio .es nos informará que tenemos que ir a una página.

```
# whois www.camaramurcia.es
# whois www.ulpgc.es
```

```
root@kali:/home/kali# whois camaramurcia.es
This TLD has no whois server, but you can access the whois database at
https://www.nic.es/
root@kali:/home/kali#
```

```
└─# whois www.ulpgc.es
This TLD has no whois server, but you can access the whois database at
https://www.nic.es/
```

- Para los dominios **.es** hay que dirigirse a la página https://dominios.es

➢ Otra manera de buscar información relevante es **comprobar el direccionamiento ip** para saber si estas ips están registradas a nombre de bmw o hay un proveedor de servicios intermedio. Para nuestro ejemplo de bmw podemos consultarla en la página web de ripe.

➢ Ir a www.ripe.net y en el buscador meter la ip de uno de los registros tipo A bmw, por ejemplo, para bmw.it ponemos (160.46.226.165)

También podemos hacer la consulta con el comando whois especificando que le pregunte a ripe

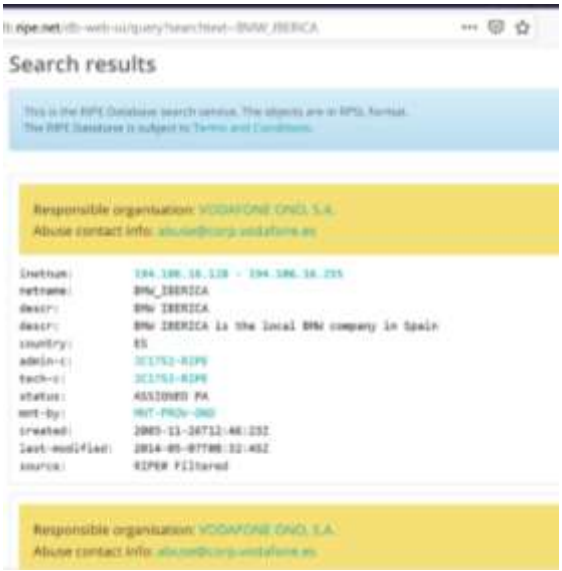
```
# whois -h whois.ripe.net 160.46.226.165
```

```
root@kali:/home/kali# whois -h whois.ripe.net 160.46.226.165
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '160.46.0.0 - 160.46.255.255'

% No abuse contact registered for 160.46.0.0 - 160.46.255.255

inetnum:        160.46.0.0 - 160.46.255.255
status:         LEGACY
remarks:
remarks:        **** INFORMATION FROM ARIN OBJECT ****
remarks:        netname: BER-NET
descr:          BMW AG, Berlin production plant
descr:          BMW AG, FI-13
descr:          Postfach 400240
```

- Otra de las ventajas que tiene Ripe es que nos permite buscar por **netname**, no solo por direcciones ip. **Netname** es el nombre de un rango de direcciones ips definidos por un objeto creado en la base de datos de ripe. Ejemplo para el netname **BMW_IBERICA**

```
# whois -h whois.ripe.net BMW_IBERICA
```

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '194.106.16.128 - 194.106.16.255'

% Abuse contact for '194.106.16.128 - 194.106.16.255' is 'abuse@corp.vodafone.es

inetnum:        194.106.16.128 - 194.106.16.255
netname:        BMW_IBERICA
descr:          BMW IBERICA
descr:          BMW IBERICA is the local BMW company in Spain
country:        ES
admin-c:        JC1752-RIPE
tech-c:         JC1752-RIPE
status:         ASSIGNED PA
mnt-by:         MNT-PROV-DNO
created:        2003-11-26T12:46:23Z
last-modified:  2014-05-07T08:32:45Z
source:         RIPE # Filtered

person:         Javier Casanova
address:        Avda de Castilla, 27
address:        28830
address:        San Fernando (Madrid)
```



- De esta forma hacemos una búsqueda inversa y podemos saber qué rangos de ips están registrados para ese ***netname***. En este caso es el rango **194.106.16.128-255** y vemos que pertenece a Vodafone.

- ENUMERACIÓN: Consultas dns (comando **host**)

Para continuar haciendo nuestra identificación de activos de una organización es importante saber cómo funcionan los dns.

Para hacer consultas de registros dns utilizamos el comando **host.** Ejemplo de consulta de búsqueda de registro **tipo A**, es decir, sabemos el nombre de un dominio y queremos saber la ip asociada.

Tipos de registros DNS

- A = Dirección (address).
- AAAA = Dirección (address).
- CNAME = Nombre canónico (canonical Name).
- NS = Servidor de nombres (name server).
- MX = Intercambio de correo (mail exchange).
- PTR = Indicador (pointer).
- SOA = Autoridad de la zona (start of authority).
- SRV = Service record (SRV record).

```
# host -t a ns.bmw.de
```

```
root@kali:/home/kali# host -t a ns.bmw.de
ns.bmw.de has address 192.109.190.2
root@kali:/home/kali#
```

Si quisiéramos consultar el registro **PTR** de una ip. Ahora justo lo contrario, sabemos la ip de un dominio y queremos saber su nombre asociado. A

```
# host -t ptr direccionip
```

```
root@kali:/home/kali# host -t ptr 192.109.190.2
2.190.109.192.in-addr.arpa domain name pointer ns.bmw.de.
root@kali:/home/kali#
```

Con la combinación de comandos vistos hasta ahora y las opciones que tienen podríamos sacar mucha información.

- Obtener el rango de direccionamiento y el **netname** al que pertenece.

```
# whois 192.109.190.2
```

```
inetnum:        192.109.190.0 - 192.109.190.255
netname:        BMW-NET
descr:          80788 Muenchen
```

Obtenemos el netname BMW-NET que tendríamos que ir guardando en nuestro fichero de texto junto toda la información recopilada.

- Si quisiéramos obtener todos los rangos de direcciones ip asociados a ese netname

```
# whois BMW-NET -h whois.ripe.net | grep inetnum
```

```
root@kali:/home/kali# whois BMW-NET -h whois.ripe.net | grep inetnum
inetnum:        62.245.187.96 - 62.245.187.127
inetnum:        62.245.228.72 - 62.245.228.79
inetnum:        62.245.239.68 - 62.245.239.71
inetnum:        62.245.239.240 - 62.245.239.247
inetnum:        80.81.23.240 - 80.81.23.247
inetnum:        80.81.27.96 - 80.81.27.103
inetnum:        82.135.5.232 - 82.135.5.239
inetnum:        82.135.5.240 - 82.135.5.247
inetnum:        82.135.6.104 - 82.135.6.111
inetnum:        82.135.7.24 - 82.135.7.31
inetnum:        82.135.25.128 - 82.135.25.159
inetnum:        82.135.37.80 - 82.135.37.87
```

- Si ahora por ejemplo utilizo el rango que estamos usando de prueba con el comando **dnsrecon** podría realizar una búsqueda PTR de este tipo:

-r : especificar que es un rango
-t: especificar tipo de rango en este caso **rvl** (reverse lookup o PTR)

```
# dnsrecon -r 192.109.190.0-192.109.190.255 -t rvl -d bmw
```

```
root@kali:/home/kali# dnsrecon -r 192.109.190.0-192.109.190.255 -t rvl
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 192.109.190.0 to 192.109.190.255
[+] {'type': 'PTR', 'name': 'gw01-d.bmwgroup.com', 'address': '192.109.190.1'}
[+] {'type': 'PTR', 'name': 'proxy7.bmw.de', 'address': '192.109.190.8'}
[+] {'type': 'PTR', 'name': 'ibpdmz-ns-n1.bmw.de', 'address': '192.109.190.10'}
[+] {'type': 'PTR', 'name': 'e2e-b2b-webeamnext-swl-sec2-admin.bmw.com', 'address': '192.109.190.12'
[+] {'type': 'PTR', 'name': 'codisprod.bmwgroup.com', 'address': '192.109.190.13'}
[+] {'type': 'PTR', 'name': 'proxy8.bmw.de', 'address': '192.109.190.15'}
[+] {'type': 'PTR', 'name': 'efinance-directentry.bmwbank.de', 'address': '192.109.190.19'}
[+] {'type': 'PTR', 'name': 'shop-80.mini.de', 'address': '192.109.190.18'}
[+] {'type': 'PTR', 'name': 'ibpdmz-nsb.bmwgroup.net', 'address': '192.109.190.20'}
[+] {'type': 'PTR', 'name': 'ns-cache-2-old.bmw.de', 'address': '192.109.190.25'}
[+] {'type': 'PTR', 'name': 'sgate-o.bmwgroup.com', 'address': '192.109.190.24'}
[+] {'type': 'PTR', 'name': 'webappt6.bmw.com', 'address': '192.109.190.29'}
[+] {'type': 'PTR', 'name': 'extranet-sgate-premium.bmwgroup.com', 'address': '192.109.190.30'}
[+] {'type': 'PTR', 'name': 'sfhexa-neu.bmw.de', 'address': '192.109.190.33'}
[+] {'type': 'PTR', 'name': 'dop-o.bmwgroup.com', 'address': '192.109.190.57'}
[+] {'type': 'PTR', 'name': 'asprb2b-o.bmw.com', 'address': '192.109.190.60'}
```

Otros registros muy importantes son los registros **MX** y **NS** de los dominios.
Ahora sacamos información de los registros MX del dominio

```
# host -t mx bmw.com
```

```
└─# host -t mx bmw.com
bmw.com mail is handled by 10 mx1.hc324-48.eu.iphmx.com.
bmw.com mail is handled by 20 mx2.hc324-48.eu.iphmx.com.
```

¿Qué raro que solo tenga dos servidores de correo? Además, es un subdominio externo, no pertenece a bmw. El correo no puede ser auditado. Vemos que los servidores de correo aparentemente están externalizados mediante una empresa que tiene el dominio **iphmx.com.**

Podríamos obtener la ip de uno de ellos con el comando host.

```
# host mx1.hc324-48.eu.iphmx.com
```

```
└─# host mx1.hc324-48.eu.iphmx.com
mx1.hc324-48.eu.iphmx.com has address 207.54.69.30
mx1.hc324-48.eu.iphmx.com has address 207.54.72.35
mx1.hc324-48.eu.iphmx.com has address 207.54.69.29
mx1.hc324-48.eu.iphmx.com has address 207.54.71.48
mx1.hc324-48.eu.iphmx.com has address 207.54.65.242
mx1.hc324-48.eu.iphmx.com has address 207.54.69.24
mx1.hc324-48.eu.iphmx.com has address 207.54.71.126
mx1.hc324-48.eu.iphmx.com has address 207.54.71.69
mx1.hc324-48.eu.iphmx.com has address 207.54.71.60
mx1.hc324-48.eu.iphmx.com has address 207.54.68.121
mx1.hc324-48.eu.iphmx.com has address 207.54.72.34
mx1.hc324-48.eu.iphmx.com has address 207.54.68.120
mx1.hc324-48.eu.iphmx.com has address 207.54.68.119
mx1.hc324-48.eu.iphmx.com has address 207.54.69.27
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3fd
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2012:300::3fb
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3fe
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3ff
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2012:300::3fd
```

Vemos que aparecen varias ips para el mismo nombre de host. Esto se suele utilizar por ejemplo cuando se balancea un servicio de correo por internet.

Si hacemos un whois a una de estas ips

```
# whois 207.54.69.30
```

```
NetName:        IRONPORT-DH
NetHandle:      NET-68-232-128-0-1
Parent:         NET68 (NET-68-0-0-0-0)
NetType:        Direct Assignment
OriginAS:       AS16417, AS30238, AS25605, AS30214, AS30215
Organization:   Cisco Systems Ironport Division (CISL-7)
```

Vemos que se trata de un servicio de correo de cisco llamado IRONPORT.

Vamos a fijarnos ahora en los servidores de nombres de bmw.

En el caso de los servidores de nombre podríamos realizar una consulta de dns con el siguiente comando.

```
# host -t ns bmw.com
```

```
root@kali:/home/kali# host -t ns bmw.com
bmw.com name server ns4.m-online.net.
bmw.com name server ns3.m-online.net.
bmw.com name server ns2.m-online.net.
bmw.com name server ns.bmw.de.
```

Comando dig: hace algo parecido a lo que estamos haciendo

```
# dig bmw.com
# dig bmw.com +short
# dig bmw.com +noall +answer
# dig 8.8.8.8 bmw.com -> preguntamos sevidor dns de google.
# dig 8.8.8.8 bmw.com ANY
# dig 8.8.8.8 bmw.com MX
# dig @8.8.8.8 bmw.com +answer -x 67.227.189.142 -> consultamos registro PTR
# dig TXT bmw.com
```

Vemos que parece que también tienen externalizado el servicio de dns. No se puede auditar.

Comando dnsenum

```
# aguasdeteror.com
```

Comando nslookup: respuesta dns a una consulta tanto directa como inversa.

```
# nslookup etsa.es
```

```
└─# nslookup etsa.es
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   etsa.es
Address: 82.98.132.86
```

set type = [NS | MX | PTR | TXT]: Establece el tipo de consulta

```
└─# nslookup
> set type=MX
> etsa.es
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
etsa.es mail exchanger = 10 etsa-es.mail.protection.outlook.com.
```

- **Descargar Base de datos RIPE**

Nos podemos descargar la Base de datos de RIPE, y hacer las consultas en local. Luego podemos comprobar con whois.

```
# wget https://ftp.ripe.net/ripe/dbase/ripe.db.gz
```

```
# zcat ripe.db.gz| grep -i "ayuntamiento" -B 3
```

Y probamos con el de Sevilla:

```
# whois 195.77.241.240
```

Identificación de subdominios

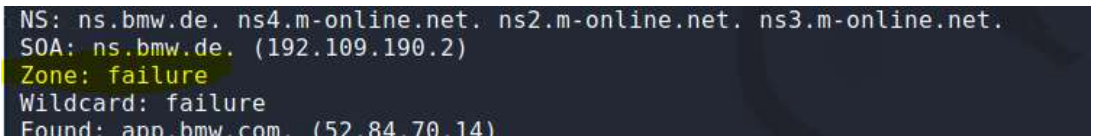
Existen dos tipos de subdominios, los **públicos** y los **privados**. Un ejemplo de subdominio público puede ser por ejemplo ***formación.dominio.com*** o ***tienda.dominio.com*** y en cambio un subdominio privado es un subdominio que solamente está disponible para uso interno de empleados o administradores por ejemplo ***admin.dominio.com***

Los subdominios privados no suelen ser publicados en los dns y muchas veces no están tan securizados como los subdominios visibles. Para sacar los subdominios podemos utilizar la herramienta **fierce** que hace uso de un diccionario de palabras de tal forma que irá probando si existen los subdominios.

```
# fierce --domain bmw.com
```

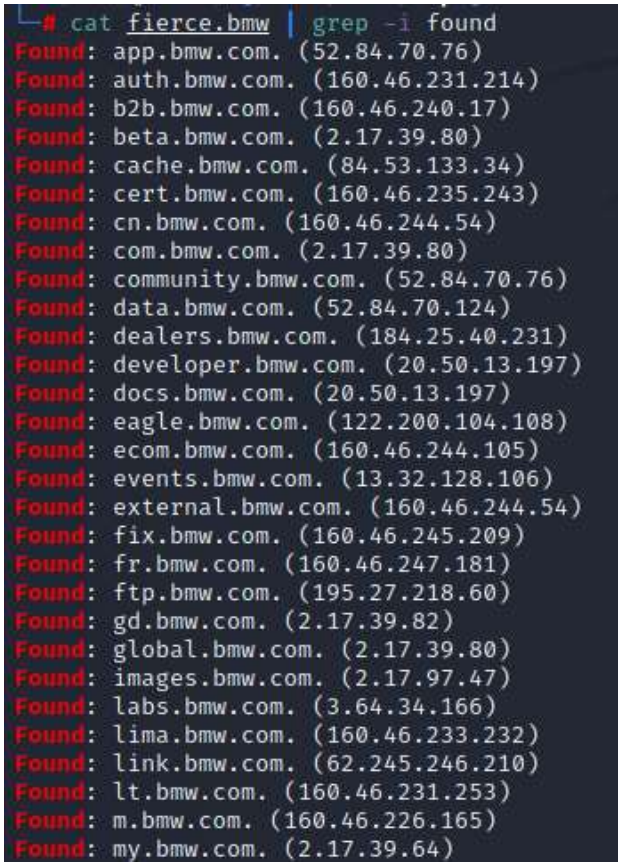
Primero prueba a ver si está habilitada la **transferencia de zona** del dominio en los servidores dns. En este caso sería muy fácil conseguir todos los registros dns de la zona bmw.com

Lo primero que intenta es hacer una transferencia de zona. Si lo consigue, por mala configuración, tendríamos acceso a todos los subdominios de la organización. Lo normal es que no esta transferencia falle.




```
# fierce --domain bmw.com > fierce.bmw
```

```
# cat fierce-dns.bmw | cut -d: -f2
```



Para automatizar el proceso de enumeración existen multitud de recursos online vía web:

Recursos web

https://dnsdumpster.com/

https://www.robtex.com/

http://ipinfo.io/

https://www.netcraft.com/: consultar qué subdominios existen para un dominio concreto.

https://searchdns.netcraft.com

https://www.virustotal.com/gui/home/search

Generar alertas para detectar resoluciones DNS sospechosas (y otras alertas):

https://canarytokens.org/generate

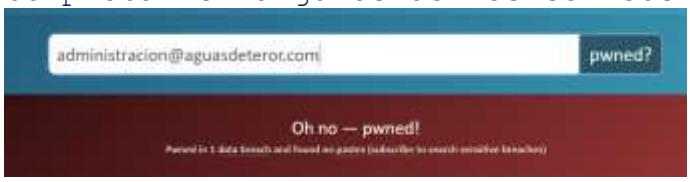
Herramientas todo en uno

Para evitar tener que ir copiando toda la información que vamos procesando en las páginas web existen herramientas como **theHarvester, sublist3r o spiderfoot** que nos permiten la automatización.

theHarvester

```
# theHarvester -h
# theHarvester -d etsa.es -l 100 -b google
# theHarvester -d aguasdeteror.com  -l 100 -b google
```

Comprobar si algunos de los correos han sido comprometidos.



sublist3r

```
sudo apt install sublist3r
sudo sublist3r -d bmw.es -o bmw.es.txt
```

Spiderfoot

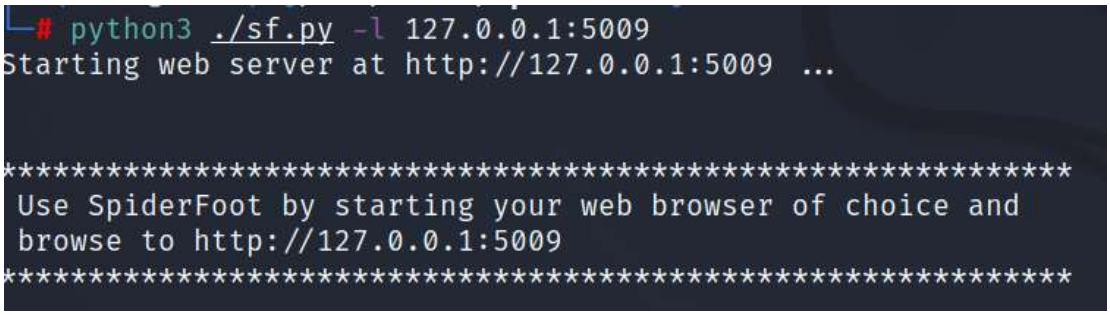
- Accedemos al directorio donde está spiderfoot:

```
# cd /usr/share/spiderfoot
```

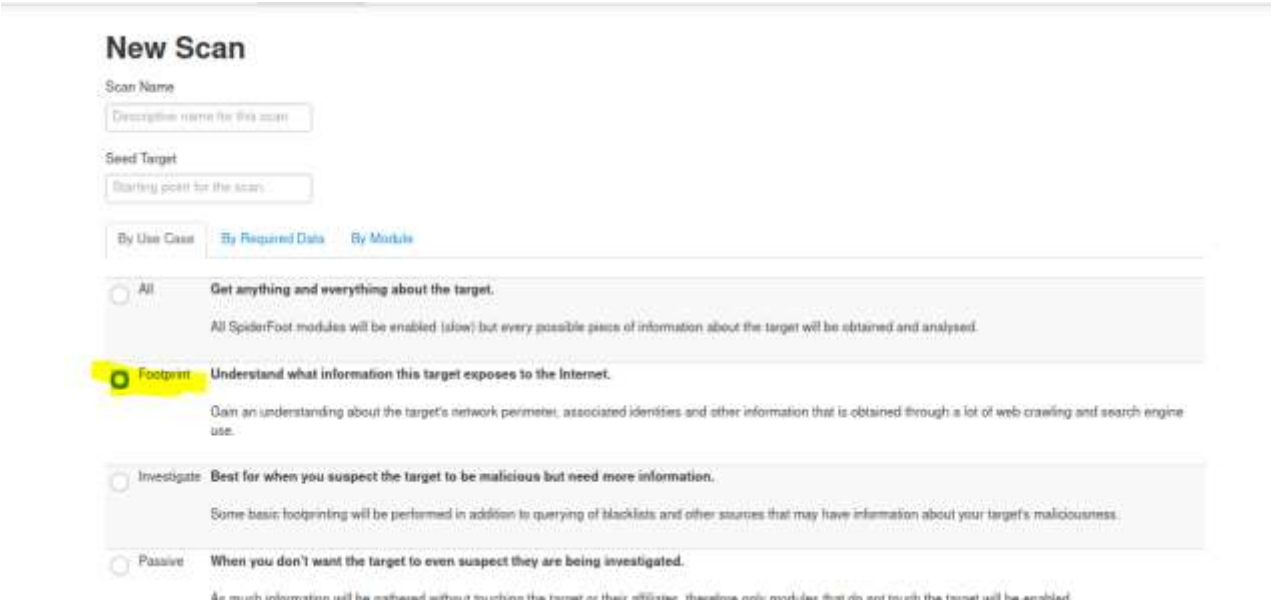
- Ejecutamos

```
# python3 ./sf.py -l 127.0.0.1:5009
```

- Hemos lanzado un servicio web en el puerto **5009**. Abrimos un explorador y navegamos a la dirección **http://127.0.0.1:5009**



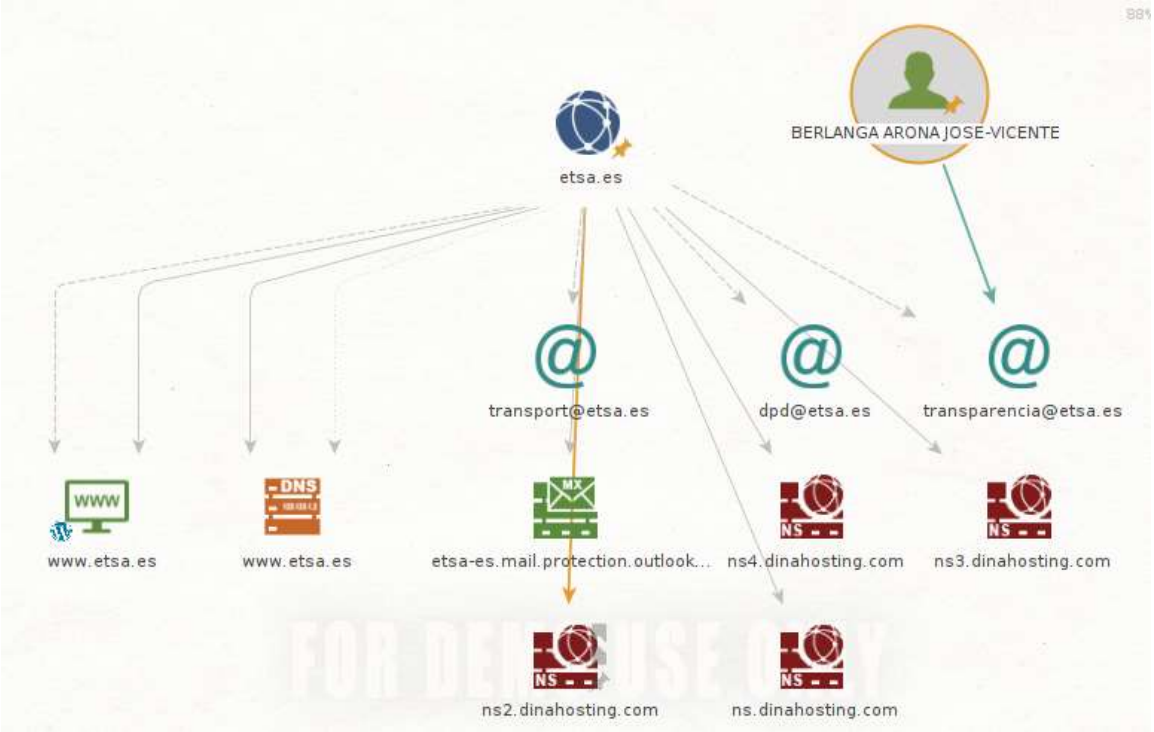
Vamos a lanzar un escaneo nuevo pulsando sobre “New scan”. Y lo configuramos para hacer un Footprint

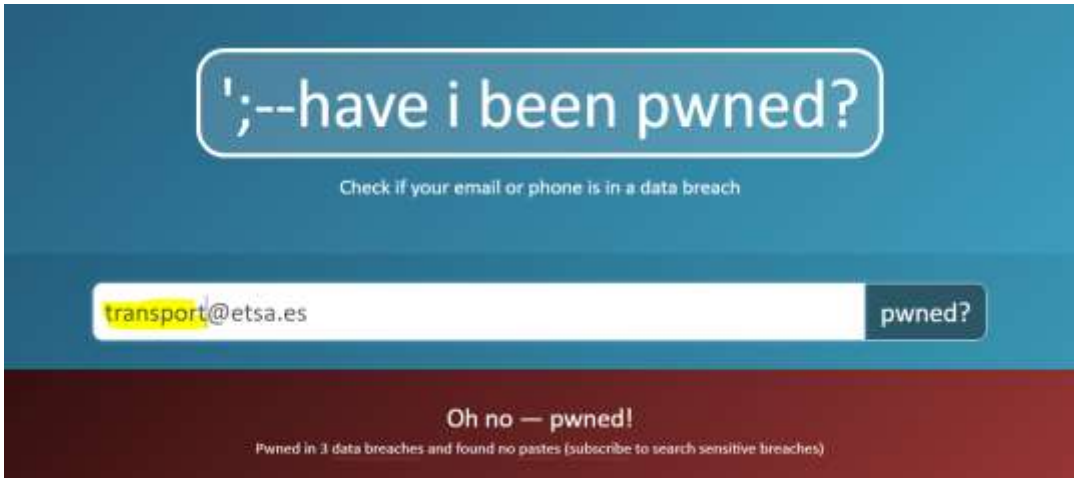


Maltego:

- Maltego es una herramienta que permite recabar datos sobre una organización de forma sencilla, a través del uso de objetos gráficos y menús contextuales que permiten aplicar "transformaciones" a dichos objetos, a través de las cuales se obtiene a su vez mayor información.

- Usando Maltego no sólo ahorraremos tiempo durante la fase de reconocimiento, sino que además podremos visualizar la relación existente entre las diferentes piezas de información recolectadas y disponerla de forma ordenada, lo cual será de gran utilidad al momento de escribir el informe de auditoría.





Google Hacking

Filter	Description	Example
allintext	Searches for occurrences of all the keywords given.	allintext:"keyword"
intext	Searches for the occurrences of keywords all at once or one at a time.	intext:"keyword"
inurl	Searches for a URL matching one of the keywords.	inurl:"keyword"
allinurl	Searches for a URL matching all the keywords in the query.	allinurl:"keyword"
intitle	Searches for occurrences of keywords in title all or one.	intitle:"keyword"
allintitle	Searches for occurrences of keywords all at a time.	allintitle:"keyword"
site	Specifically searches that particular site and lists all the results for that site.	site:"www.google.com"
filetype	Searches for a particular filetype mentioned in the query.	filetype:"pdf"
link	Searches for external links to pages.	link:"keyword"
numrange	Used to locate specific numbers in your searches.	numrange:321-325
before/after	Used to search within a particular date range.	filetype:pdf & (before:2000-01-01 after:2001-01-01)
allinanchor (and also inanchor)	This shows sites which have the keyterms in links pointing to them, in order of the most links.	inanchor:rat
allinpostauthor (and also inpostauthor)	Exclusive to blog search, this one picks out blog posts that are written by specific individuals.	allinpostauthor:"keyword"
related	List web pages that are “similar” to a specified web page.	related:www.google.com
cache	Shows the version of the web page that Google has in its cache.	cache:www.google.com
OPERADORES		

Filter	Description	Example
+	Incluir palabras	La Laguna
-	Excluir palabras	Bancos -muebles
OR (|)	site:facebook.com | site:twitter.com	
AND (&)	site:facebook.com & site:twitter.com	
~	Sinónimos	~empresa
Combinación	(site:facebook.com | site:twitter.com) & intext:"login" (site:facebook.com | site:twitter.com) (intext:"login")	

Algunos dorsks interesantes

intext:"Real-time IP Camera Monitoring System" intext:"ActiveX Mode (For IE Browser)"
inurl:console/login.jsp
intitle:"index of" "/products"
site:*.ng intitle:index of
site:drive.google.com "*.pdf" → **muy interesante: cambiar .pdf por .xls, .doc, .jpg**
intitle:"index of" "admin*.txt"
intext:"Index of" intext:"users.zip"
intitle:"index of" "Apache/2.4.41 (Ubuntu) Server"
intext:"index of" "ftp"
site:pastebin.com "*@gmail.com password"
filetype:sql «MySQL dump» (pass|password|passwd|pwd)

intitle:»index of» «Index of /» password.txt

Buscadores de dispositivos conectados a Internet

https://www.shodan.io/

https://www.zoomeye.org/