



CURSO DE HACKING ÉTICO

RECOLECCIÓN DE INFORMACIÓN

“The more information you have about the target, the more is the chance of successful exploitation “

- **Al respecto de Information Gathering**

RECOLECCIÓN DE INFORMACIÓN

Tipos

- ☐ WHOIS
- ☐ Ubicar el objetivo
- ☐ DNS enumeration
- ☐ Mails enumeration
- ☐ METADATOS
- ☐ Maltego, Hyena

Tipos

En general podemos clasificar la recolección de información (Information Gathering) en dos categorías.

❑ Active Information Gathering:



En active information gathering, interactuamos directamente con el objetivo, por ejemplo realizando un escaner del objetivo para detectar puertos abiertos o qué el Sistema operativo se está utilizando. Este tipo de técnicas genera mucho "ruido" en la parte del objetivo y pueden ser fácilmente detectadas por IDS, IPS o Firewalls. En cuyo caso nos conviene "camuflar nuestra identidad " siempre que sea posible " (VPN, red Thor ...)

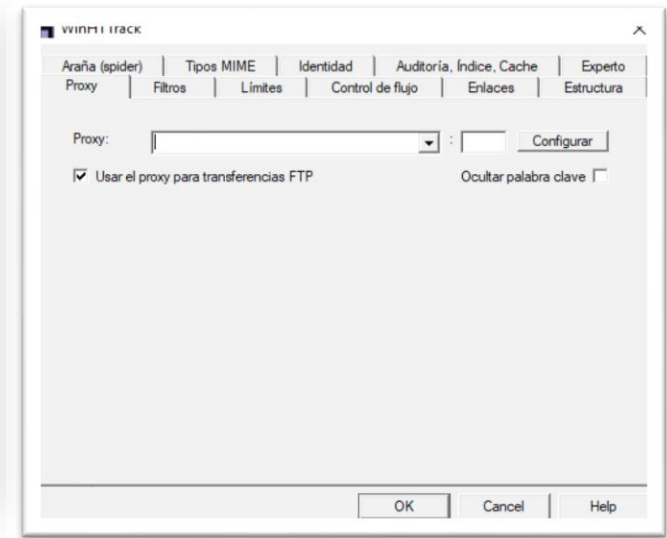
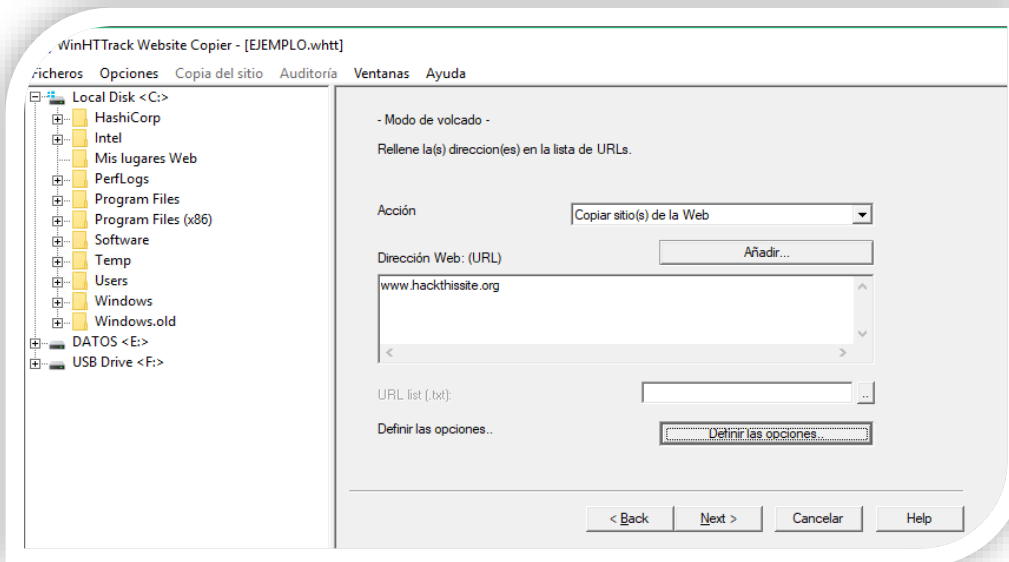
❑ Passive Information Gathering :



Con éste método no interactuamos con el objetivo, sino que utilizamos motores de búsqueda, redes sociales u otras websites para obtener información sobre el objetivo. No genera "ruido" en el objetivo. Un ejemplo común es utilizar Facebook, Linkedin, etc. Éste método es muy útil cuando queremos aplicar técnicas de phishing, keylogging, browser exploitation y otras técnicas desde el lado del cliente.

Copiar una web localmente

Hay muchas herramientas que pueden ser usadas para copiar websites. Una de las más intuitivas es [HTTrack](#). Una vez copiada, la podemos utilizar para examinarla. Por ejemplo, si los permisos de un fichero de configuración no están bien configurados, podremos obtener información muy interesante como cuentas de usuario y passwords.



Whois

Whois mantiene una enorme base de datos que contiene información sobre cada website que está en la Web. Información como puede ser el propietario de la web, su correo electrónico, persona técnica de contacto, teléfonos, etc. Podemos utilizar dicha información para realizar ataques de redes sociales.

La base de datos de Whois es accesible en whois.domaintools.com.

```
root@educait:~# whois hackthissite.org
Domain Name: HACKTHISSITE.ORG
Registry Domain ID: D99641092-LROR
Registrar WHOIS Server: whois.enom.com
Registrar URL: http://www.enom.com
Updated Date: 2018-03-06T11:59:39Z
Creation Date: 2003-08-10T15:01:25Z
Registry Expiry Date: 2018-08-10T15:01:25Z
Registrar Registration Expiration Date:
Registrar: eNom, Inc.
Registrar IANA ID: 48
Registrar Abuse Contact Email: abuse@enom.com
Registrar Abuse Contact Phone: +1.4252982646
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#
Registry Registrant ID: C203613481-LROR
Registrant Name: Whois Agent
Registrant Organization: Whois Privacy Protection Service, Inc
```



The screenshot shows the homepage of the 'domini.es' website, which is the official portal for the Spanish domain registry. The header includes the Spanish flag, the coat of arms of Spain, and logos for the 'GOBIERNO DE ESPAÑA', 'MINISTERIO DE ENERGÍA, TURISMO Y AGENCIA DIGITAL', and 'domini.es'. There is also a logo for '@dministración electrónica'. A navigation bar contains links for 'INICIO', 'BUSCA Y REGISTRA TU DOMINIO', 'AGENTES REGISTRADORES', 'TODO LO QUE NECESITAS SABER', 'GESTIONA TU DOMINIO', 'ACTUALIDAD Y NOTICIAS', and 'SOBRE NOSOTROS'. Below the navigation bar, there is a section titled 'Información de Dominio' with a search bar labeled 'Introduce el nombre de Dominio a buscar:'. The search bar has a dropdown menu showing various domain extensions: '.es', '.com.es', '.nom.es', '.org.es', '.gob.es', and '.edu.es'. The search bar contains the text 'Nombre del Dominio www.danone.es'. At the bottom right, there are buttons for 'Limpiar Campos' and 'Buscar'.

Whois

EL RGPD Obliga a Whois a dejar de Funcionar en Europa



Reverse IP lookup, Simlink bypassing

Symlink bypassing permite a un atacante utilizar un website para comprometer a otro que esté en el mismo servidor.

Yougetsignal.com permite realizar una búsqueda IP inversa de un webserver para detectar otros.



The screenshot shows a web application titled "Reverse IP Domain Check". It features a sidebar with icons for various functions. The main area contains a form with a "Remote Address" field containing "techlotips.com" and a "Check" button. Below the form, a message states: "Found 97 domains hosted on the same web server as techlotips.com (50.22.81.62)". A list of domains is displayed in two columns.

Domain	Domain
123learntoplayguitar.com	absoluteohd.com
advancedlimo.net	apolloent.com
arkofsafetycenter.com	awarenews.info
battlerapup.com	bestofbostonma.com
bing.com	brantscheifler.com
brucebirdantlercarving.com	buscamores.com
clawson.com	calderon.com

Ubicar el objetivo

Podemos utilizar un simple ping para obtener la IP de un determinado objetivo. Con esa IP podemos visitar múltiples páginas en Internet donde nos indica la localización de dicho servidor. Un tema interesante es observar el TTL de la respuesta...

```
C:\>ping www.salesianssarria.com
```

Haciendo ping a www.salesianssarria.com [178.33.113.169] con 32 bytes de datos:

```
Respuesta desde 178.33.113.169: bytes=32 tiempo=36ms TTL=51
```

```
Respuesta desde 178.33.113.169: bytes=32 tiempo=72ms TTL=51
```

```
Respuesta desde 178.33.113.169: bytes=32 tiempo=36ms TTL=51
```

```
Respuesta desde 178.33.113.169: bytes=32 tiempo=38ms TTL=51
```

Estadísticas de ping para 178.33.113.169:

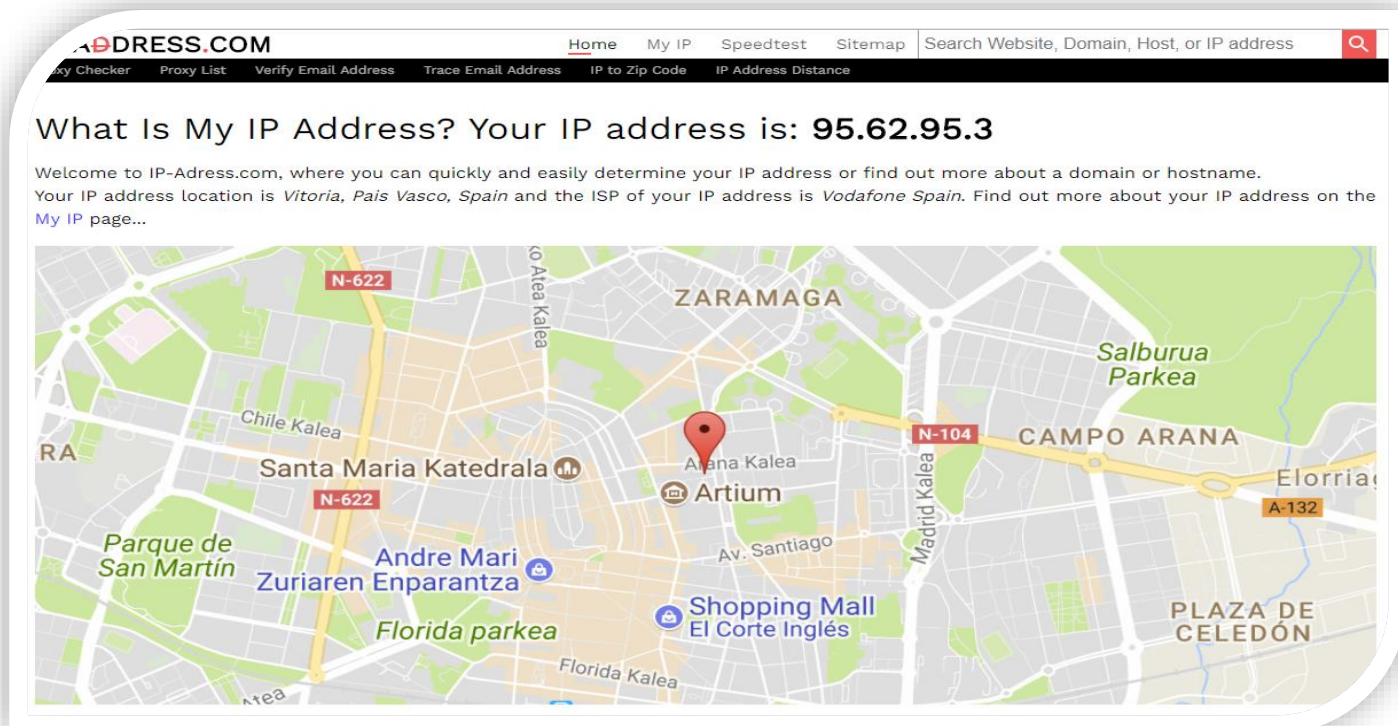
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 36ms, Máximo = 72ms, Media = 45ms

Ubicar el objetivo

En la página <https://www.ip-adress.com/> se nos dará información de la ubicación de la IP. Interesante tener presente que las IP's son asignadas por Internet [Assigned Numbers Authority](#), IANA



Traceroute / Tracert

Traceroute es una utilidad muy popular que funciona tanto en Windows como en Linux. Nos proporciona información de la topología de la red al informarnos de la ruta de un paquete IP desde el origen al destino.

Hay tres tipos diferentes de traceroutes:

1. ICMP traceroute
2. TCP traceroute
3. UDP traceroute

```
C:\>tracert www.google.com
```

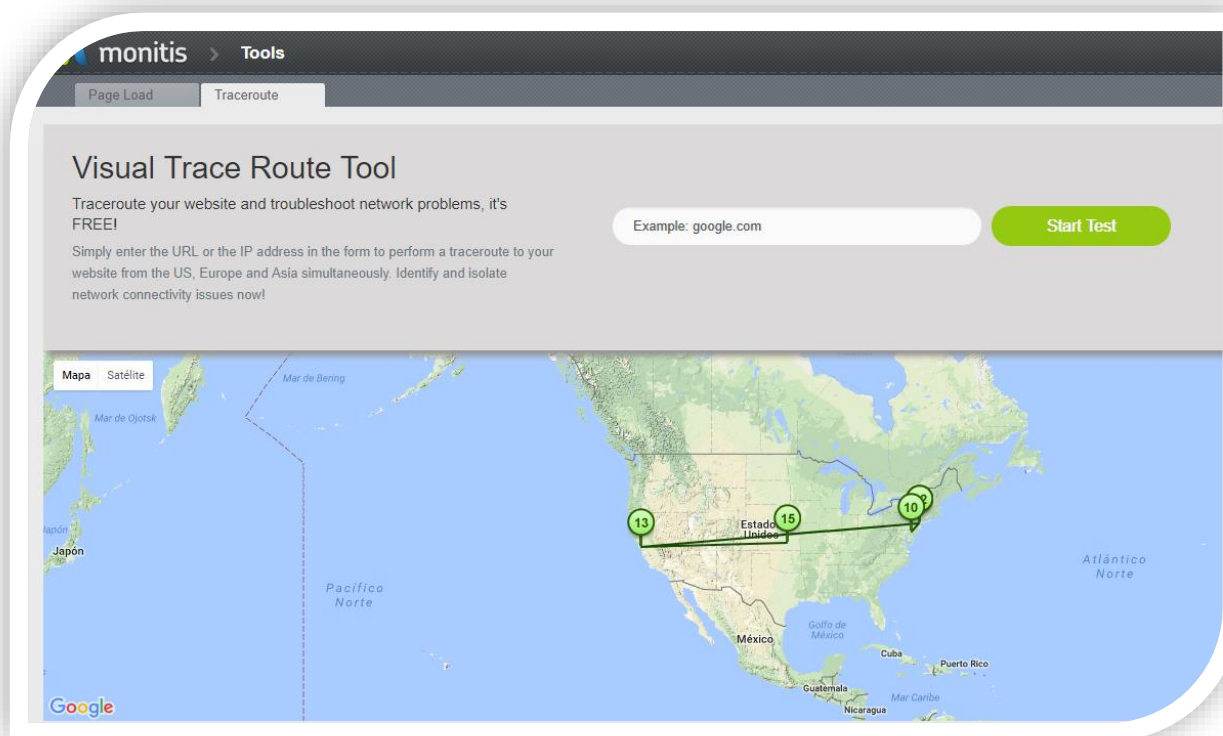
```
Traza a la dirección www.google.com [216.58.211.36]  
sobre un máximo de 30 saltos:
```

1	5 ms	6 ms	6 ms	www.adsl.vf [192.168.1.1]
2	13 ms	10 ms	13 ms	static-10-0-235- 87.ipcom.comuitel.net
3	9 ms	8 ms	8 ms	10.183.73.21
4	*	*	8 ms	172.29.104.109
5	*	*	*	Tiempo de espera agotado
6	17 ms	16 ms	18 ms	212.166.147.46
7	18 ms	16 ms	17 ms	216.239.50.150
8	17 ms	15 ms	16 ms	209.85.251.219
9	17 ms	16 ms	18 ms	muc03s14-in-f4.1e100.net

```
Traza completa.
```

Visual Trace Route Tool

Existen páginas web donde de forma visual se nos proporciona una información similar gráficamente. Una de ellas es: <http://www.monitis.com/traceroute/>



Enumerar WebServers, WhatWeb

WhatWeb es un paquete instalado en la distribución de Kali Linux por defecto, que mediante técnicas activas sobre una WebSite, y más de 900 plug-ins es capaz de darnos mucha información: versión del servidor, mails, errores de SQL, etc.

Su uso es muy sencillo, solo se necesita ejecutar.









whatweb salesianssarria.com


```
root@educait:~# whatweb salesianssarria.com
http://salesianssarria.com [301 Moved Permanently] Apache[2.4.10], Country[FRANCE][FR], HTTPServer[Debian Linux][Apache/2.4.10 (Debian)], IP[178.33.113.169], RedirectLocation[https://salesianssarria.com/], Title[301 Moved Permanently]
https://salesianssarria.com/ [301 Moved Permanently] Apache[2.4.10], Country[FRANCE][FR], HTTPServer[Debian Linux][Apache/2.4.10 (Debian)], IP[178.33.113.169], RedirectLocation[https://www.salesianssarria.com/], Title[301 Moved Permanently]
https://www.salesianssarria.com/ [301 Moved Permanently] Apache[2.4.10], Cookies[96fe45008ef4a0ef45c0584e032ec01b], Country[FRANCE][FR], HTTPServer[Debian Linux][Apache/2.4.10 (Debian)], HttpOnly[96fe45008ef4a0ef45c0584e032ec01b], IP[178.33.113.169], RedirectLocation[https://www.salesianssarria.com/ca/], Strict-Transport-Security[max-age=31536000; includeSubDomains]
https://www.salesianssarria.com/ca/ [200 OK] Apache[2.4.10], Cookies[96fe45008ef4a0ef45c0584e032ec01b], Country[FRANCE][FR], Email[salesians.sarria@salesians.cat], HTML5, HTTPServer[Debian Linux][Apache/2.4.10 (Debian)], HttpOnly[96fe45008ef4a0ef45c0584e032ec01b], IP[178.33.113.169], JQuery, Open-Graph-Protocol, Script[application/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[Formació Professional Dual i Batxillerats - Barcelona - Salesians Sarrià], X-UA-Compatible[IE=edge]
root@educait:~#
```

Enumerar WebServers, Netcraft


Netcraft contiene una amplia base de datos online con información muy valiosa sobre WebSites, y puede ser utilizada como método **pasivo** para examinar el objetivo. (<https://www.netcraft.com/>).
 Dispone de extensiones para [Firefox](#) y [Chrome](#).

Share:      

Background

Site title	Formació Professional Dual i Batxillerats - Barcelona - Salesians Sarrià	Date first seen	February 2018
Site rank		Primary language	Catalan
Description	Escola de Batxillerat, Batxillerat Internacional i Formaci303263 Professional FP amb Cicles formatius de Grau Mitj303240 i Cicles formatius de Grau Superior a Barcelona amb m303251s de 130 anys d342200231experi303250ncia, treballem per donar resposta a les necessitats educatives actuals dels joves, en un ambient familiar i amb un tracte proper i directe. En aquesta l303255nia i seguint l342200231estil de Sant Joan Bosco, posem cura en construir una relaci303263 educativa de confian303247a.		
Keywords	Not Present		
Netcraft Risk Rating [FAQ]	1/10 		

Network

Site	https://www.salesianssarria.com	Netblock Owner	OVH Hispano
Domain	salesianssarria.com	Nameserver	dns1.nominalia.com
IP address	178.33.113.169	DNS admin	root@dns1.nominalia.com
IPv6 address	Not Present	Reverse DNS	178-33-113-169.ovh.net
Domain registrar	unknown	Nameserver organisation	unknown
Organisation	unknown	Hosting company	OVH
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	 ES		

Google Hacking

Las búsquedas en Google pueden ser todo un Tesoro para un pentester, si las utiliza correctamente. Con las búsquedas en Google, un atacante puede obtener mucha información incluyendo incluso cuentas y passwords de acceso del objetivo.

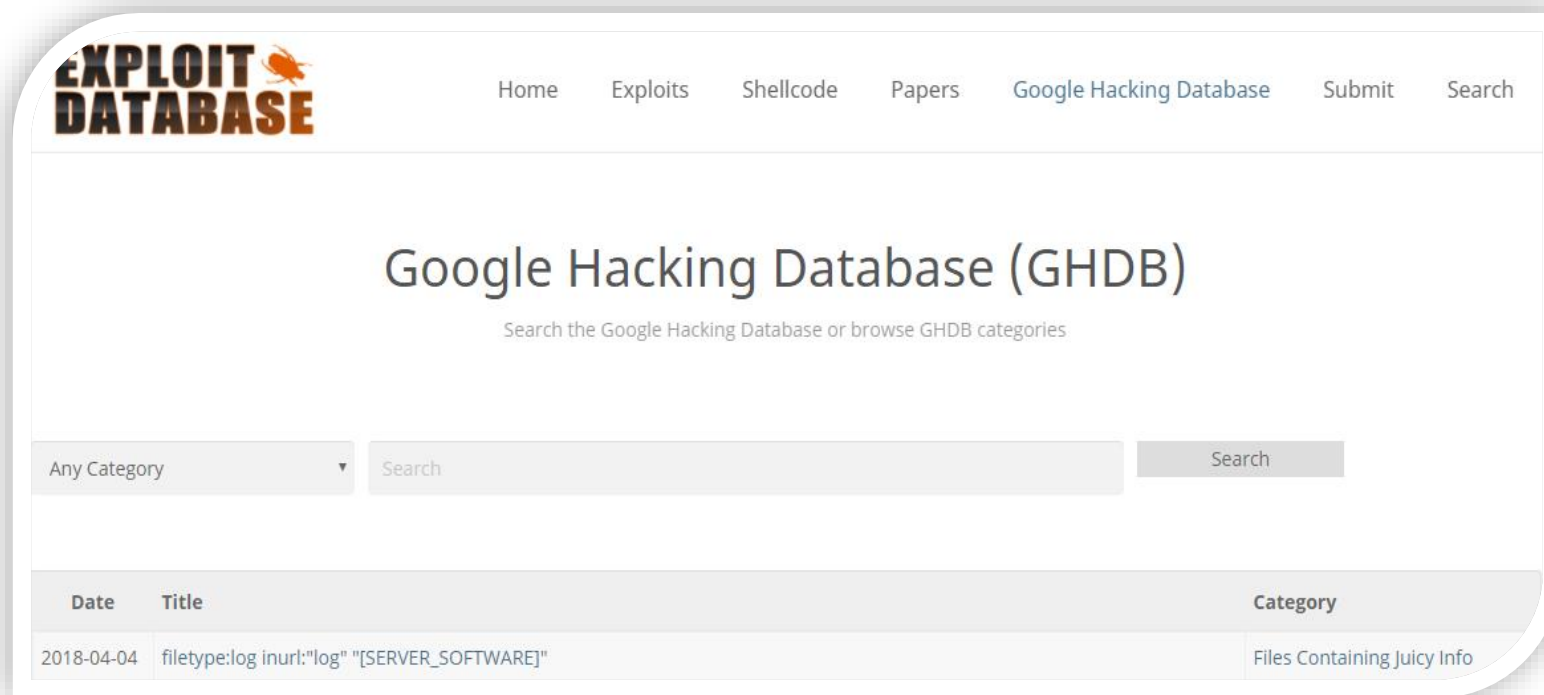
Google ha desarrollado unos pocos parámetros de búsqueda para mejorar las búsquedas. Como suele pasar, son utilizadas de forma masiva por los hackers para obtener información sensible de una organización.

- Operadores avanzados:
- ☐ Permiten afinar las búsquedas
 - ☐ Están incluidas como parte de una consulta estándar de Google.
 - ☐ Tienen la siguiente sintaxis: **operator: search term**
 - ☐ NO hay espacio entre el operador, los dos puntos y el término a buscar.
 - ☐ Se conocen también como Google Dorks



Google Hacking Database

[Google hacking database](#) tiene una lista de muchos Google dorks que pueden ser usados para encontrar nombres de usuario, password, listas de correo electrónico, [hashes](#) de passwords y más información relevante.



The screenshot shows the Google Hacking Database (GHDB) website. At the top, there is a navigation bar with links: Home, Exploits, Shellcode, Papers, Google Hacking Database (highlighted), Submit, and Search. The main heading is "Google Hacking Database (GHDB)" with a subtitle "Search the Google Hacking Database or browse GHDB categories". Below this, there is a search interface with a dropdown menu for "Any Category", a search input field, and a "Search" button. At the bottom, there is a table with the following data:

Date	Title	Category
2018-04-04	filetype:log inurl:"log" "[SERVER_SOFTWARE]"	Files Containing Juicy Info



TheHarvester - Listas de E-Mail y +

La recolección de información sobre e-mails de empleados de una organización puede proporcionarnos un buen vector de ataque contra el objetivo. Este método puede ser clasificado como pasivo ya que no interactúa directamente con el objetivo, sino con motores de búsqueda.

El objetivo del programa **TheHarvester** es recopilar mails, subdominios, hosts, nombres de empleados, puertos abiertos, PHP Keys y ordenadores de la base de datos [SHODAN](#). En definitiva es una buena aproximación de la información que desde el exterior tienen de nuestra organización.

- ☐ All sources search
- ☐ Virtual host verifier
- ☐ Active enumeration (DNS enumeration, Reverse lookups, TLD expansion)
- ☐ Integration with SHODAN computer database, to get the open ports and banners.
- ☐ Save to XML and HTML
- ☐ Basic graph with stats
- ☐ New sources

TheHarvester - Ejemplos

```
# theharvester -d hackthissite.org -l 500 -b google
```

```
# theharvester -d hackthissite.org -l 500 -b all
```

```
# theharvester -d hackthissite.org -l 500 -b all -f test
```



```
root@educait:~# theharvester -d hackthissite.org -l 300 -b google
*****
*                                     *
*  theHarvester                      *
*  theHarvester                      *
*                                     *
* TheHarvester Ver. 2.7              *
* Coded by Christian Martorella      *
* Edge-Security Research             *
* cmartorella@edge-security.com      *
*****

[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...
    Searching 300 results...

[+] Emails found:
-----
No emails found

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
198.148.81.138:www.hackthissite.org
185.24.222.13:irc.hackthissite.org
137.74.187.133:mirror.hackthissite.org
198.148.81.167:tor.hackthissite.org
185.24.222.13:wolf.irc.hackthissite.org
198.148.81.139:www.hackthissite.org
```

PIPL, buscando personas



Buscar Más 3,166,875,147 Personas

Con el motor de búsqueda de personas más grande del mundo, Pipl es el lugar adecuado para encontrar a la persona que hay detrás de la dirección de correo electrónico, el nombre de usuario social o el número de teléfono.



Scanning for SSL Version

```
# sslscan www.hackthissite.org
```

```
educait:~# sslscan www.hackthissite.org
Version: 1.11.11-static
OpenSSL 1.0.2-chacha (1.0.2g-dev)

Connected to 198.148.81.137

Testing SSL server www.hackthissite.org on port 443 using SNI name www.hackthissite.org

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.0 128 bits ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted TLSv1.0 256 bits ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted TLSv1.0 128 bits DHE-RSA-AES128-SHA            DHE 4096 bits
Accepted TLSv1.0 256 bits DHE-RSA-AES256-SHA            DHE 4096 bits
Accepted TLSv1.0 128 bits AES128-SHA
Accepted TLSv1.0 256 bits AES256-SHA
Accepted TLSv1.0 256 bits DHE-RSA-CAMELLIA256-SHA       DHE 4096 bits
Accepted TLSv1.0 256 bits CAMELLIA256-SHA
Accepted TLSv1.0 128 bits DHE-RSA-CAMELLIA128-SHA       DHE 4096 bits
Accepted TLSv1.0 128 bits CAMELLIA128-SHA
Accepted TLSv1.0 112 bits DES-CBC3-SHA

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength: 4096
```

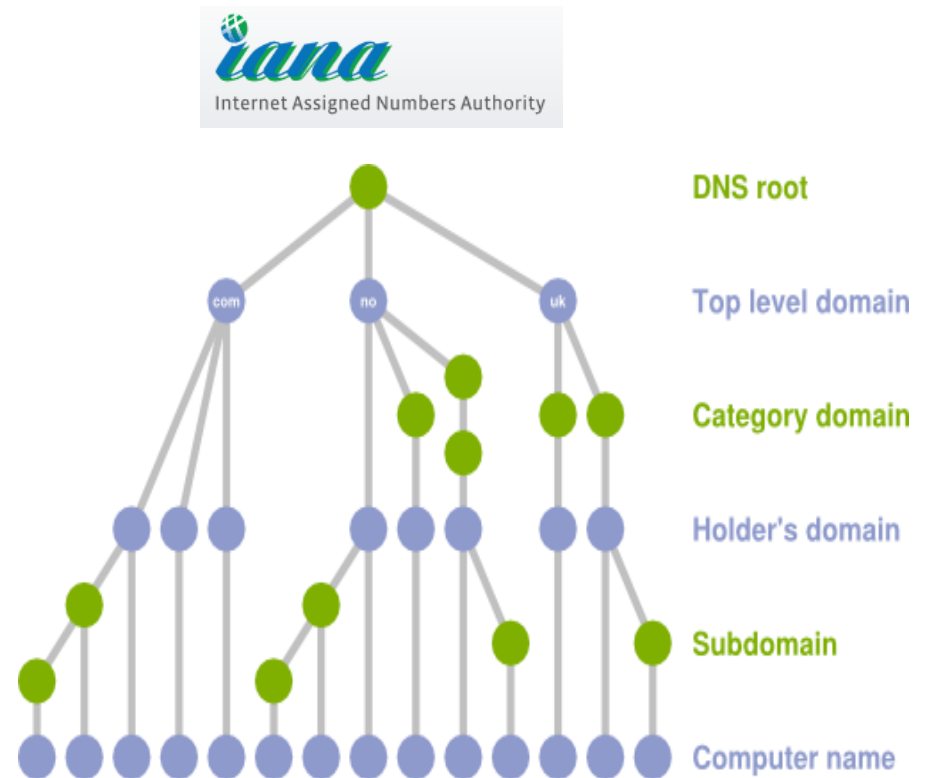


DNS Enumeration

Domain Name System es un servicio de red que permite traducciones de nombres lógicos en su correspondiente IP física:

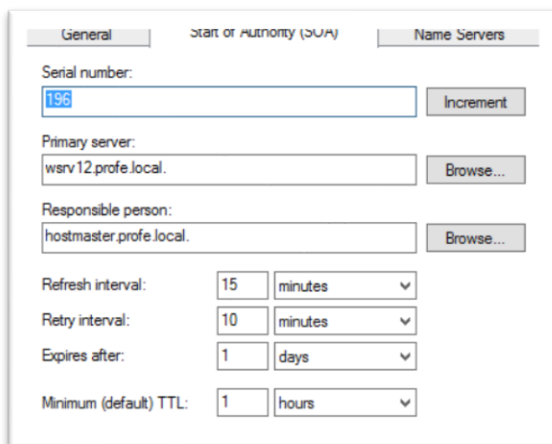
www.mytcpip.com → 146.66.85.161

Su función no solamente es esa, la más conocida, sino que hoy en día es una fuente inagotable de información para obtener datos de servidores y servicios de una determinada organización.



DNS: Tipos de registros

Un archivo de zona mantiene la información de los servidores y servicios asociados a un dominio, o al menos los que el administrador desea que puedan ser localizados por nombres. DNS mantiene un tipo de registro para cada función. Por ejemplo el registro tipo SOA tiene los parámetros globales de configuración de un dominio.



General Start of Authority (SOA) Name Servers

Serial number: 185 Increment

Primary server: wsr12.profe.local. Browse...

Responsible person: hostmaster.profe.local. Browse...

Refresh interval: 15 minutes

Retry interval: 10 minutes

Expires after: 1 days

Minimum (default) TTL: 1 hours

DNS Record Types

Types	DESCRIPTION
A	Address Record
CNAME	Canonical Record Name
MX	Mail Exchange Record
AAAA	IPv6 Address Record
TXT	Text Record
PTR	Pointer Record
SRV	Service locator
SPF	Sender policy framework
NS	Name Server Record
SOA	Start of authority Record

DNS: nslookup / dig

```
root@kali:~# host
www.hackthissite.org
root@kali:~# host -t ns
hackthissite.org
root@kali:~# host -t mx
hackthissite.org
root@kali:~# host -l
hackthissite.org
```

ZoneTransfer.me

```
dig axfr
@nsztn1.digi.ninja
zonetransfer.me
```

```
root@kprofe:~# nslookup
```

```
> set type=mx
```

```
> salesians.cat
```

```
Server:          192.168.1.1
```

```
Address:         192.168.1.1#53
```

```
Non-authoritative answer:
```

```
salesians.cat    mail exchanger = 30 ALT2.ASPMX.L.GOOGLE.COM.
```

```
salesians.cat    mail exchanger = 40 ASPMX2.GOOGLEMAIL.COM.
```

```
> set type=a
```

```
> www.salesians.cat
```

```
Server:          192.168.1.1
```

```
Address:         192.168.1.1#53
```

```
Non-authoritative answer:
```

```
Name: www.salesians.cat
```

```
Address: 89.140.86.154
```



DNS: DNSENUM

```
root@kprofe:~# dnsenum --enum hackthissite.org
```

```
dnsenum VERSION:1.2.4
```

```
----- hackthissite.org -----
```

```
Host's addresses:
```

hackthissite.org.	3600	IN	A	198.148.81.135
hackthissite.org.	3600	IN	A	198.148.81.138
hackthissite.org.	3600	IN	A	198.148.81.136



DNS: DNSRECON / nmap

```
# dnsrecon -d hackthissite.org
```

```
# root@educait:~# dnsrecon -d hackthissite.org -D  
/usr/share/dnsrecon/namelist.txt -t brt
```

```
# nmap -Pn -sU -p 53 --script=dns-recursion 192.168.1.1  
|_dns-recursion: Recursion appears to be enabled
```

```
# nmap --script dns-srv-enum --script-args "dns-srv-  
enum.domain='google.com'"
```

Starting Nmap 7.60 (<https://nmap.org>) at 2018-04-07 09:08 CEST

Pre-scan script results:

| dns-srv-enum:

| LDAP

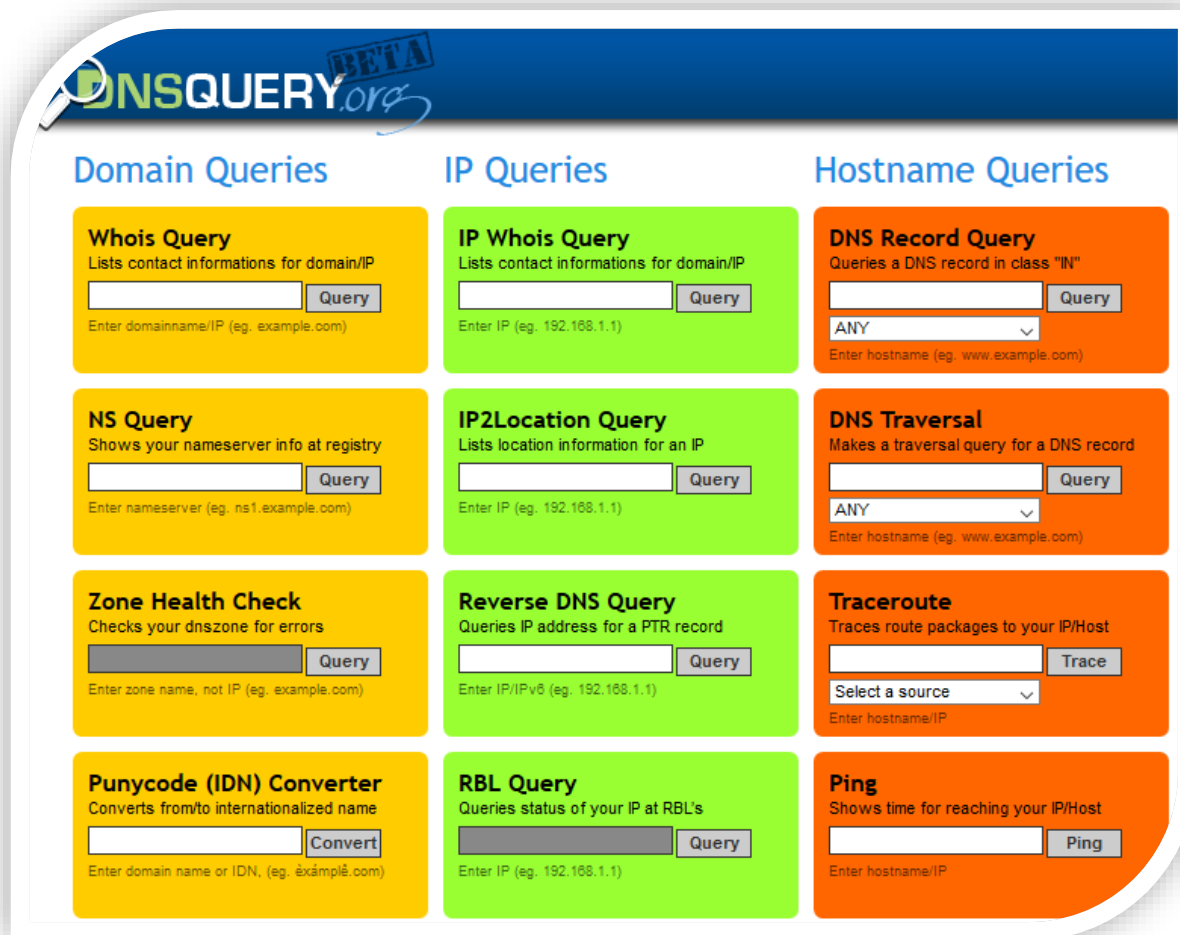
service	prio	weight	host
389/tcp	5	0	ldap.google.com

| XMPP client-to-server

service	prio	weight	host
5222/tcp	5	0	xmpp.1.google.com



DNS: Herramientas ONline



DNSQUERY.org BETA

Domain Queries	IP Queries	Hostname Queries
Whois Query Lists contact informations for domain/IP <input type="text"/> Enter domainname/IP (eg. example.com) <input type="button" value="Query"/>	IP Whois Query Lists contact informations for domain/IP <input type="text"/> Enter IP (eg. 192.168.1.1) <input type="button" value="Query"/>	DNS Record Query Queries a DNS record in class "IN" <input type="text"/> ANY <input type="button" value="Query"/> Enter hostname (eg. www.example.com)
NS Query Shows your nameserver info at registry <input type="text"/> Enter nameserver (eg. ns1.example.com) <input type="button" value="Query"/>	IP2Location Query Lists location information for an IP <input type="text"/> Enter IP (eg. 192.168.1.1) <input type="button" value="Query"/>	DNS Traversal Makes a traversal query for a DNS record <input type="text"/> ANY <input type="button" value="Query"/> Enter hostname (eg. www.example.com)
Zone Health Check Checks your dnszone for errors <input type="text"/> Enter zone name, not IP (eg. example.com) <input type="button" value="Query"/>	Reverse DNS Query Queries IP address for a PTR record <input type="text"/> Enter IP/IPv6 (eg. 192.168.1.1) <input type="button" value="Query"/>	Traceroute Traces route packages to your IP/Host <input type="text"/> Select a source <input type="button" value="Trace"/> Enter hostname/IP
Punycode (IDN) Converter Converts from/to internationalized name <input type="text"/> Enter domain name or IDN, (eg. example.com) <input type="button" value="Convert"/>	RBL Query Queries status of your IP at RBL's <input type="text"/> Enter IP (eg. 192.168.1.1) <input type="button" value="Query"/>	Ping Shows time for reaching your IP/Host <input type="text"/> Enter hostname/IP <input type="button" value="Ping"/>

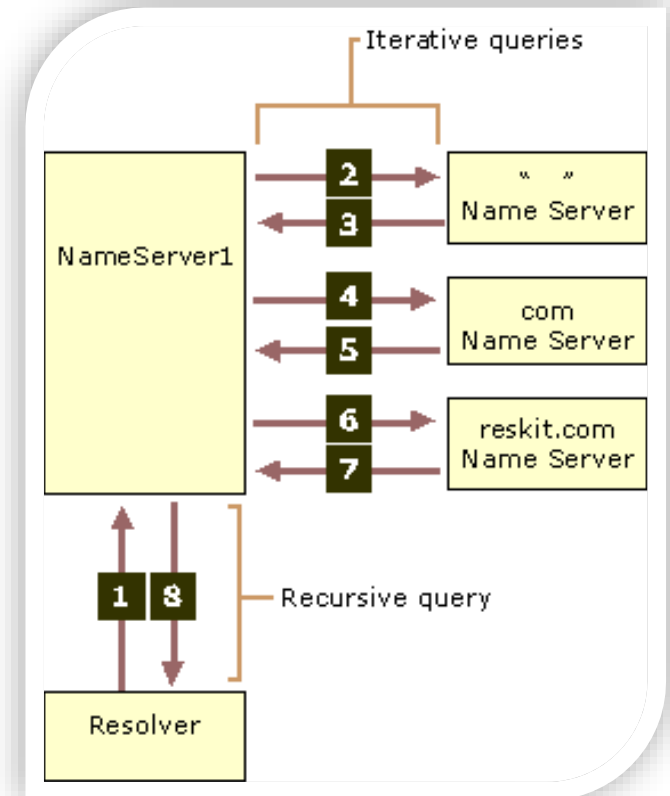
POC: DNS Cache Snooping

Un ataque DNS cache snooping permite realizar consultas DNS a un determinado servidor para determinar si un determinado registro DNS está en cache. Los registros pueden ser de tipo A, CNAME o TXT.

Esto nos permite saber las páginas Web a las que se conectan nuestros usuarios, y por lo tanto utilizar dicha información para un ataque posterior, como por un ejemplo MiTM (Man in the Middle) y alguna utilidad de SEA (Social Engineering Attacks).

Podemos utilizar dos métodos:

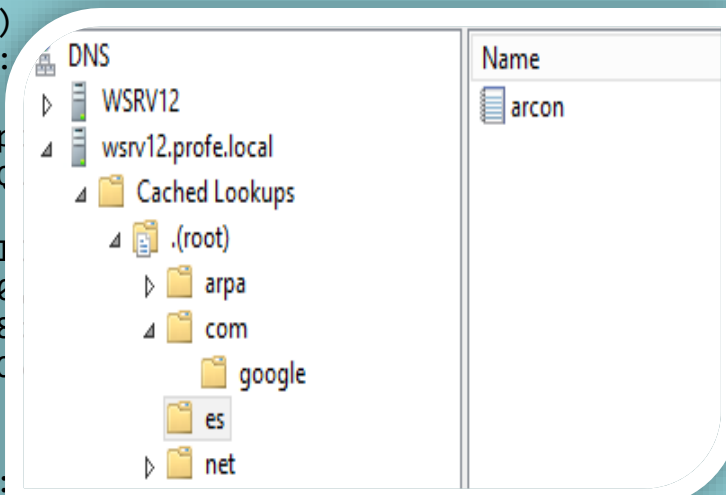
- ☐ Nonrecursive method
- ☐ Recursive method



POC: DNS Cache Snooping

```
root@educait:~# dig @192.168.1.106 arcon.es A +norecurse
```

```
; <>> DiG 9.11.2-P1-1-Debian <>> @192.168.1.106 arcon.es A +norecurse
; (1 server found)
;; global options:
;; Got answer:
;; ->>HEADER<<- op
;; flags: qr ra; C
;; OPT PSEUDOSECTION:
; EDNS: version: 0
; COOKIE: 7d8e2f38
;; QUESTION SECTION:
;arcon.es.
;; ANSWER SECTION:
arcon.es.                43139      IN      A       77.240.114.52
;; Query time: 0 msec
;; SERVER: 192.168.1.106#53(192.168.1.106)
;; WHEN: Sat Apr 07 09:30:47 CEST 2018
;; MSG SIZE rcvd: 65
```



```
C:\>nslookup
```

```
Servidor predeterminado:
adsl.vf
Address: 192.168.1.1
```

```
> server 192.168.1.106
```

```
Servidor predeterminado:
[192.168.1.106]
Address: 192.168.1.106
```

```
> set type=A
```

```
> set norecurse
```

```
> arcon.es
```

```
Servidor: [192.168.1.106]
Address: 192.168.1.106
```

```
Respuesta no autoritativa:
```

```
Nombre: arcon.es
```

```
Address: 77.240.114.52
```



METADATOS: FOCA

El concepto de **metadatos** se refiere a aquellos datos que hablan de los datos, es decir, describen el contenido de los archivos o la información de los mismos.

**Foca**
OPEN SOURCE

Foca Market >

Descripción

Funcionalidad

Características

5/10/17. Versión Open Source

F FOCA

FOCA (Fingerprinting Organizations with Collected Archives) es una herramienta utilizada principalmente para encontrar metadatos e información oculta en los documentos que examina. Estos documentos pueden estar en páginas web, y con FOCA se pueden descargar y analizar.

Los documentos que es capaz de analizar son muy variados, siendo los más comunes los archivos de Microsoft Office, Open Office, o ficheros PDF, aunque también analiza ficheros de Adobe InDesign, o svg por ejemplo.

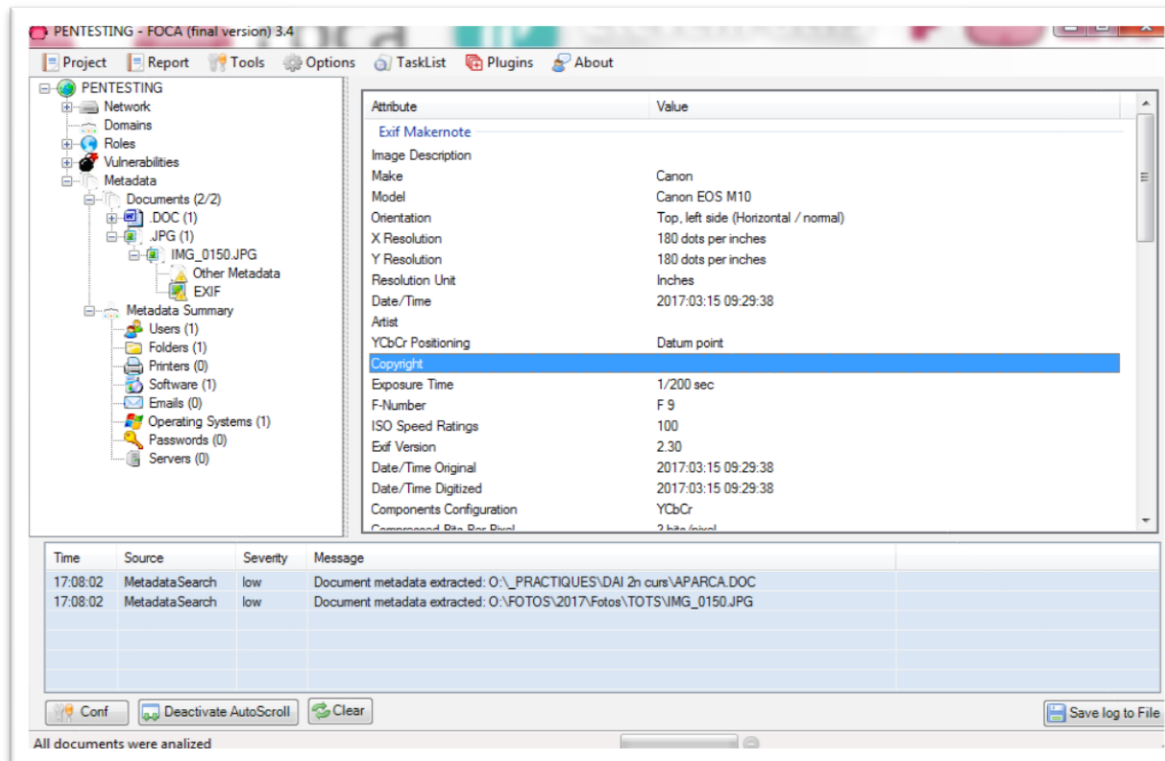
Estos documentos se buscan utilizando tres posibles buscadores que son Google, Bing y DuckDuckGo. La suma de los tres buscadores hace que se consigan un gran número de documentos. También existe la posibilidad de añadir ficheros locales para extraer la información EXIF de archivos gráficos, y antes incluso de descargar el fichero se ha realizado un análisis completo de la información descubierta a través de la URL.

Con todos los datos extraídos de todos los ficheros, FOCA va a unir la información, tratando de reconocer qué documentos han sido creados desde el mismo equipo, y qué servidores y clientes se pueden inferir de ellos.



METADATOS: EXIF

El concepto de **metadatos** se refiere a aquellos datos que hablan de los datos, es decir, describen el contenido de los archivos o la información de los mismos.



EXIF son las abreviaturas de Exchangeable image file format. Es un estándar creado para almacenar metadatos de las fotos hechas con cámaras digitales.

[View and remove Exif online](#)



Windows Enumeration

Entendemos por Windows Enumeration el acceso a sistemas Windows para obtener una lista de sus recursos de red, listas de usuarios y grupos así como otra información sensible de poder ser utilizada para un acceso no autorizado en el sistema. Muchas de estas técnicas se basan en el acceso anónimo al sistema, aunque esta técnica ya es complicada al estar protegida en los sistemas (GPO's)

```
C:\temp>net use \\192.168.1.106\ipc$ "" /
```

Se ha completado el comando correctamente

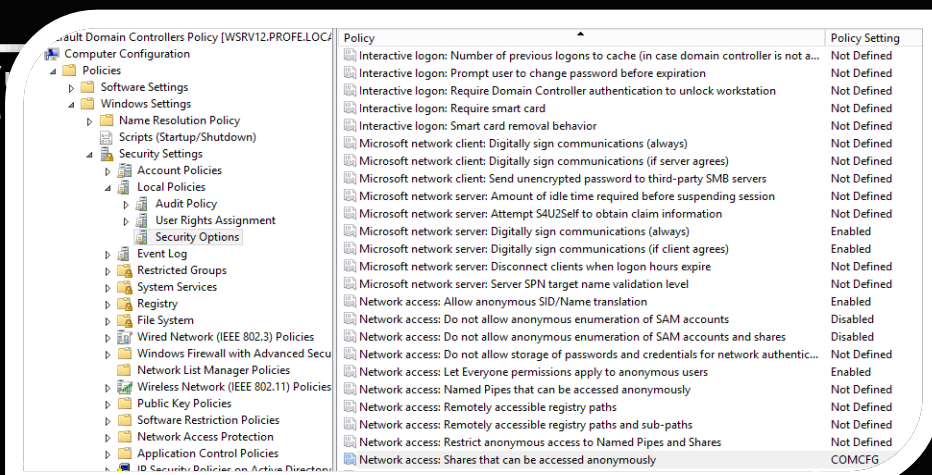
```
C:\temp>net use
```

Se registrarán las nuevas conexiones.

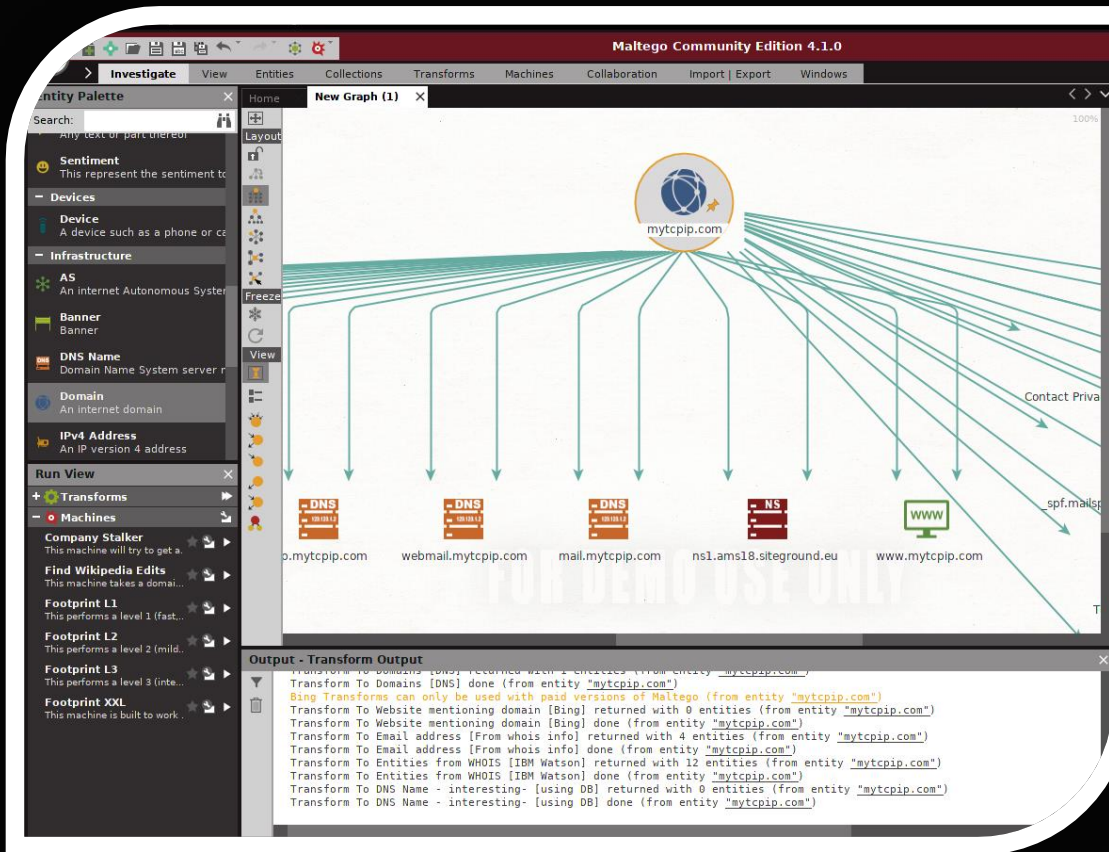
Estado	Local	Remoto
--------	-------	--------

Conectado	\\192.168.1.106\ipc\$	Microsoft Windows Network
-----------	-----------------------	---------------------------

```
C:\temp>nbtstat -a 192.168.1.106
```



Maltego CE



Maltego es una programa que **recopila información** de internet y la representa de forma gráfica para que sea sencilla de analizar, es una herramienta muy potente, llena de opciones que pueden ser muy útiles para investigar empresas, sitios, personas y mucho más.

Permite iniciar búsquedas a partir de dominios, IPs, ubicaciones geográficas, correos, nombres, teléfonos e incluso frases. Viene con Kali Linux

**MALTEGO**

Enum4Linux

Herramienta Linux que permite enumerar los diferentes recursos de un sistema Windows.

```
root@mytcpip:~# enum4linux -a -u "demo" -p "12345aA" 192.168.1.106
```

```
root@mytcpip:~# enum4linux -a -u "demo" -p "12345aA" 192.168.1.106
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Apr  8 08:40:06 2018
```

```
=====
| Target Information |
=====
Target ..... 192.168.1.106
RID Range ..... 500-550,1000-1050
Username ..... 'demo'
Password ..... '12345aA'
Known Usernames .. administrator, guest, krbtgt, domain admins, root,
```

```
=====
| Enumerating Workgroup/Domain on 192.168.1.106 |
=====
[+] Got domain/workgroup name: PROFE
```

```
=====
| Nbtstat Information for 192.168.1.106 |
=====
```

Looking up status of 192.168.1.106

PROFE	<00>	-	<GROUP>	B	<ACTIVE>	Domain/
WSRV12	<00>	-		B	<ACTIVE>	Workstat
PROFE	<1c>	-	<GROUP>	B	<ACTIVE>	Domain
WSRV12	<20>	-		B	<ACTIVE>	File Ser
PROFE	<1b>	-		B	<ACTIVE>	Domain

```
=====
Users on 192.168.1.106 |
=====
```

```
=====
Groups on 192.168.1.106 |
=====
```

```
[+] Getting builtin groups:
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
```

```
nt: a.perez
nt: Administrator
nt: demo Name:
nt: fj.paris
nt: Guest Name:
nt: j.serradell
nt: jl.sanchez
nt: krbtgt Name:
nt: M1J01 Name:
nt: M1J02 Name:
nt: M1K01 Name:
nt: M1K02 Name:
```

Hyena

Herramienta Windows que permite enumerar los diferentes recursos de un sistema Windows.

