

RECONOCIMIENTO DNS



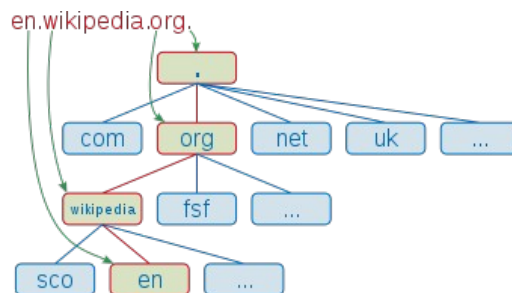
José Luis Berenguel Gómez – IES Zaidín-Vergeles

Sumario

1. Introducción a DNS.....	3
2. Comandos y herramientas para obtener información.....	5
Protocolo whois.....	5
TLD (Top Level Domain).....	5
Registros Regionales de Internet (RIR).....	7
Registros MX y NS.....	7
Obtención de subdominios (DNS Brutting).....	7
Transferencia de zona.....	9
DNS Cache Snooping.....	10
3. Caso práctico guiado.....	11
5. Herramientas visuales.....	32
Herramientas web.....	32
Transformadas de Maltego.....	33
6. Bibliografía.....	34

1. Introducción a DNS

La resolución de nombres de dominio permite traducir las direcciones IP a nombres de la forma www.dominio.com. Esta estructura de nombres de dominio se conoce como FQDN (*Fully Qualified Domain Name*).



Recurso [ENG]

Información sobre FQDN en Wikipedia.

https://en.wikipedia.org/wiki/Fully_qualified_domain_name

El protocolo DNS establece las reglas de comunicación entre el servidor de nombres de dominio y los clientes. Se encuentra descrito en numerosos RFC, aunque un punto de comienzo puede ser el RFC 6195, que revisa el estado y realiza recomendaciones de buenas prácticas en la implementación del protocolo.

Recurso [ENG]

RFC 6895. Domain Name System (DNS) IANA Considerations

<https://tools.ietf.org/html/rfc6895>

No es posible hacer una revisión completa del funcionamiento detallado del protocolo. Es importante saber que la información DNS se guarda en **registros de distinto tipo**:

- **A (Address)**. Registro para traducir nombres de hosts a direcciones IPv4.
- **AAAA (Address)**. Similar al anterior, pero para traducir nombres a direcciones IPv6.
- **CNAME (Canonical Name)**. Se usa para crear nombres de hosts adicionales, o alias, para los host de un dominio. Empleado cuando se corren múltiples servicios (ftp, http...) en un servidor con una sola IP. Cada servicio tiene su propia entrada DNS (ftp.ejemplo.com y www.ejemplo.com). También se utiliza cuando hay múltiples servidores HTTP en el mismo host, con diferentes nombres.
- **NS (Name Server)**. Establece la asociación entre un nombre de dominio y el servidor o servidores de nombres que almacenan la información de ese dominio.

- MX (*Mail eXchange*). El registro de intercambio de correo asocia el nombre de dominio a los servidores de correo disponibles para ese dominio.
- PTR (*PoinTeR*). También conocido como registro inverso, ya que su funcionamiento es lo opuesto al registro A, traduciendo direcciones IP a nombres de dominio.
- SOA (*Start Of Authority*). Proporciona información sobre el servidor DNS primario de la zona.
- HINFO (*Host Information*). Descripción del host. Permite conocer información del tipo de máquina y sistema operativo.
- TXT (*Text*). Información textual, permite a los dominios identificarse de modo arbitrario.
- LOC (*Location*). Permite indicar las coordenadas GPS del dominio.
- WKS. Obsoleto en favor de SRV.
- SRV (*Services*). Permite indicar los servicios que ofrece el dominio (definido en el [RFC 2782](https://tools.ietf.org/html/rfc2782) y actualizado posteriormente en RFC 6335 y 8553).
- SPF (*Sender Policy Framework*). Este registro especifica los hosts que están autorizados a enviar correo desde el dominio dado. Se utiliza para identificar correos falsificados y/o spam.



Ilustración 1: Fuente: https://en.wikipedia.org/wiki/Domain_Name_System

2. Comandos y herramientas para obtener información

Protocolo whois

Protocolo que permite consultar y almacenar información de un nombre de dominio ([RFC 3912](#)). Almacena información de los dominios, datos de contacto administrativo y técnico, correo electrónico, registrador, fecha de creación y expiración, y opcionalmente los servidores DNS donde está alojado. Hoy en día, gran parte de los datos personales no se muestra como medida de protección de privacidad. Herramientas:

- Comando *whois*. Aplicación en línea de comandos que permite realizar consultas al servicio de directorio DNS.
- [Robtex.com](#). Servicio web que permite investigar IPs y registros DNS. Obtiene la información de consultas a numerosas fuentes abiertas.

General	
FQDN	ieszaidinvergeles.org
Host Name	
Domain Name	ieszaidinvergeles.org
Registry	org
TLD	org
DNS	
IP numbers	2001:8d8:1001:11e8:b170:b203:e9c2:301e 2001:8d8:100f:f000::20d 217.160.0.64 217.160.196.206
Name servers	ns1074.ui-dns.biz ns1020.ui-dns.com ns1025.ui-dns.de ns1022.ui-dns.org
Mail servers	aspmx.l.google.com alt1.aspmx.l.google.com alt2.aspmx.l.google.com alt3.aspmx.l.google.com alt4.aspmx.l.google.com

Ilustración 2: Información obtenida en Robtex.com para el dominio ieszaidinvergeles.org

TLD (Top Level Domain)

Son los dominios de nivel superior. Existen distintos tipos:

- **Organizaciones genéricas** (gTLD – *Generic Top Level Domain*). Se conocen como genéricos por razones históricas y la lista ha sufrido cambios a lo largo de los años. En la actualidad se

consideran dominios gTLD a *.com*, *.org*, *.net*, *.info*, *.name* y *.pro*.

- **Localizados geográficamente** (ccTLD – *Country Code Top Level Domain*). Pertenecen a países o regiones, están definidos por [ISO 3166-1](https://www.iso.org/standard/51020.html)) : *.es*, *.pt*, *.fr*, ...
- **Dominios patrocinados** (sTLD – *Sponsored Top Level Domain*). Son dominios propuestos por alguna agencia o fundación independiente (*.aero*, *.mobi*, *.cat*, *.edu*, *.gov*). Los dominios patrocinados *.edu*, *.gov*, *.mil*, y *.int* inicialmente pertenecían a la categoría gTLD.
- **Dominios para pruebas** (tTLD – *Test Top Level Domain*): Son dominios *.test* empleados para pruebas en el desarrollo de los protocolos. No se encuentran accesibles en los directorios raíz.

Los dominios geográficos son gestionados, normalmente, por cada país. En España se encarga el **organismo REDES** (*red.es*) a través de **dominios.es** (<https://www.dominios.es>).

Algunas herramientas para obtener esta información:

- Comando *dnsrecon*. Herramienta escrita en Python que permite realizar comprobaciones de transferencia de zona, realizar fuerza bruta mediante diccionario para el descubrimiento de subdominios, etc.

```
(kali@kali)-[~]
$ dnsrecon --domain ieszaidinvergeles.org
[*] std: Performing General Enumeration against: ieszaidinvergeles.org ...
[-] All nameservers failed to answer the DNSSEC query for ieszaidinvergeles.org
[*] SOA ns1025.ui-dns.de 217.160.80.25
[*] SOA ns1025.ui-dns.de 2001:8d8:fe:53:0:d9a0:5019:100
[*] NS ns1022.ui-dns.org 217.160.83.22
[*] NS ns1022.ui-dns.org 2001:8d8:fe:53:0:d9a0:5316:100
[*] NS ns1020.ui-dns.com 217.160.82.20
[*] NS ns1020.ui-dns.com 2001:8d8:fe:53:0:d9a0:5214:100
[*] NS ns1025.ui-dns.de 217.160.80.25
[*] NS ns1025.ui-dns.de 2001:8d8:fe:53:0:d9a0:5019:100
[*] NS ns1074.ui-dns.biz 217.160.81.74
[*] NS ns1074.ui-dns.biz 2001:8d8:fe:53:0:d9a0:514a:100
[*] MX alt3.aspmx.l.google.com 74.125.200.26
[*] MX aspmx.l.google.com 142.251.5.26
[*] MX alt1.aspmx.l.google.com 142.251.9.26
[*] MX alt4.aspmx.l.google.com 142.250.157.27
[*] MX alt2.aspmx.l.google.com 142.250.150.26
[*] MX alt3.aspmx.l.google.com 2404:6800:4003:c00::1a
[*] MX aspmx.l.google.com 2a00:1450:400c:c00::1a
[*] MX alt1.aspmx.l.google.com 2a00:1450:4025:c03::1a
[*] MX alt4.aspmx.l.google.com 2404:6800:4008:c13::1a
[*] MX alt2.aspmx.l.google.com 2a00:1450:4010:c1c::1b
[*] A ieszaidinvergeles.org 217.160.0.64
[*] AAAA ieszaidinvergeles.org 2001:8d8:100f:f000::20d
[*] TXT ieszaidinvergeles.org MS=ms19225252
[*] TXT ieszaidinvergeles.org v=spf1 include:_spf.google.com ~all
[*] TXT ieszaidinvergeles.org v=DMARC1; p=none; rua=mailto:webmaster@ieszaidinvergeles.org
[*] Enumerating SRV Records
[+] 0 Records Found
```

Ilustración 3: Empleo de la herramienta *dnsrecon* sobre el dominio *ieszaidinvergeles.org*

Recurso

Repositorio oficial de *dnsrecon*: <https://github.com/darkoperator/dnsrecon>
Ayuda del comando en Kali: <https://www.kali.org/tools/dnsrecon/>

Registros Regionales de Internet (RIR)

Estas organizaciones están encargadas de la gestión (venta, distribución) de direcciones IP. Ofrecen información útil para identificar rangos de IP de una entidad y sistemas autónomos (AS, los routers de direccionamiento IP en la red pública).

- Localizadas geográficamente: APNIC (Asia), [RIPE](#) (Europa), ARIN (América), AfricNIC (África) y LacNIC (Lationamérica y Caribe).
- Se consulta mediante el protocolo *whois* y vía web.
- Son bases de datos que se pueden descargar.

Registros MX y NS

Contienen información de los servidores de nombres y de correo.

- MX: Identifica los nombres de los servidores de correo y puede ser más de uno. Utilizan pesos para priorizar y balancear la carga (máximo 0, mínimo 50). Suelen estar **balanceados y utilizar filtros/servidores antispam**.
- NS: Encargados de identificar los nombres de los servidores DNS de un dominio y puede ser uno o más.
- Herramientas: *nslookup*, *dig*, *host*.
 - *host -t mx <dominio>*

Obtención de subdominios (*DNS Brutting*)

Queremos descubrir los nombres de host de un determinado dominio. Se puede emplear fuerza bruta a través de un diccionario para obtener coincidencias. Hay dos tipos de subdominios:

- **Públicos:** publicados en Internet y accesibles desde el exterior. ← Objetivo.
- **Privados:** pertenecen a la red interna y se definen en servidores DNS internos.
- Herramientas: *fierce*, *dnsenum*, *dnsdict6*, *dnsmap*.
 - *fierce --domain <dominio>*
 - *dnsenum <dominio> -f <diccionario>*
 - *dnsdict6 <dominio> / dnsdict6 <dominio> <diccionario>*
 - *dnsmap <dominio> / dnsmap <dominio> -w <diccionario>*
 - *dnsrecon -d <dominio> -D <diccionario>*


```
(kali㉿kali)-[/usr/share/seclists]
$ dnsrecon -domain ieszaidinvergeles.org -D /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[*] std: Performing General Enumeration against: ieszaidinvergeles.org ...
[-] All nameservers failed to answer the DNSSEC query for ieszaidinvergeles.org
[*] SOA ns1025.ui-dns.de 217.160.80.25
[*] SOA ns1025.ui-dns.de 2001:8d8:fe:53:0:d9a0:5019:100
[*] NS ns1074.ui-dns.biz 217.160.81.74
[*] NS ns1074.ui-dns.biz 2001:8d8:fe:53:0:d9a0:514a:100
[*] NS ns1025.ui-dns.de 217.160.80.25
[*] NS ns1025.ui-dns.de 2001:8d8:fe:53:0:d9a0:5019:100
[*] NS ns1020.ui-dns.com 217.160.82.20
[*] NS ns1020.ui-dns.com 2001:8d8:fe:53:0:d9a0:5214:100
[*] NS ns1022.ui-dns.org 217.160.83.22
[*] NS ns1022.ui-dns.org 2001:8d8:fe:53:0:d9a0:5316:100
[*] MX aspmx.l.google.com 108.177.15.26
[*] MX alt4.aspmx.l.google.com 142.250.157.27
[*] MX alt3.aspmx.l.google.com 74.125.200.27
[*] MX alt2.aspmx.l.google.com 142.250.150.26
[*] MX alt1.aspmx.l.google.com 142.251.9.26
[*] MX aspmx.l.google.com 2a00:1450:400c:c01::1a
[*] MX alt4.aspmx.l.google.com 2404:6800:4008:c13::1b
[*] MX alt3.aspmx.l.google.com 2404:6800:4003:c00::1b
[*] MX alt2.aspmx.l.google.com 2a00:1450:4010:c1c::1b
[*] MX alt1.aspmx.l.google.com 2a00:1450:4025:c03::1b
[*] A ieszaidinvergeles.org 217.160.0.64
[*] AAAA ieszaidinvergeles.org 2001:8d8:100f:f000::20d
[*] TXT ieszaidinvergeles.org MS=ms19225252
[*] TXT ieszaidinvergeles.org v=spf1 include:_spf.google.com ~all
[*] TXT ieszaidinvergeles.org v=DMARC1; p=none; rua=mailto:webmaster@ieszaidinvergeles.org
[*] Enumerating SRV Records
[*] 0 Records Found
```

Ilustración 4: Enumeración de subdominios con la herramienta *dnsrecon*

Otra forma de obtener subdominios es mediante los certificados digitales emitidos para un determinado dominio. La herramienta **ct-exposer** desarrollada en Python utiliza el protocolo experimental *Certification Transparency* creado para auditar de forma pública los certificados emitidos por una CA para un determinado dominio. No está en los repositorios de Kali pero se puede instalar desde la página oficial de GitHub.

```
$ cd /opt
$ git clone https://github.com/chris408/ct-exposer.git
$ cd ct-exposer
$ pip3 install -r requirements.txt
$ sudo chmod +x ct-exposer.py
$ ./ct-exposer.py
usage: ct-exposer.py [-h] -d DOMAIN [-u] [-m]
ct-exposer.py: error: the following arguments are required: -d/--domain
```

Recurso

Repositorio oficial en GitHub de ct-exposer.
<https://github.com/chris408/ct-exposer>

La lista de subdominios que obtenemos con esta herramienta para el dominio *bmw.com* es cuantiosa por lo que se expone una brevísima muestra..

```
$ /opt/ct-exposer/ct-exposer.py -d bmw.com
[+]: Downloading domain list from crt.sh...
[+]: Download of domain list complete.
[+]: Parsed 1392 domain(s) from list.

[+]: Domains found:
170.34.100.20 3gio-app-us.bmw.com
160.46.228.213 72h-radar-intl.bmw.com
```



```
77.95.83.42    Parknow-ltr.com
114.66.81.70   SSA-P.BMW.COM.CN
192.109.190.85 UCP14RP.bmw.de
160.46.240.174 a3.bmw.com
192.109.190.82 access14.bmw.de
160.46.229.14  access21.bgmtest.info
160.46.226.83  accessories.bmw.com
160.46.244.19  acscat.bmw.com
160.46.250.163 aem-author-inta1.bmw.com
160.46.251.175 aem-author-inta2.bmw.com
160.46.250.189 aem-author-inta3.bmw.com
160.46.224.37  aem-author-inta4.bmw.com
160.46.227.46  aem-author-inta5.bmw.com
....

[+]: Domains with no DNS record:
none    360portal-int.bmw.com
none    4bo-test-s.bmw.com
none    72h-radar-int2.bmw.com
none    72h-radar.bmw.com
none    CnGuestWlan@bmw.com
none    ConnectedDrive-Zertifikate@list.bmw.com
none    FZ-222HISSLCertificateAdmin@list.bmw.com
none    FZ-444Z-WLAN@list.bmw.com
none    SF3-CN-ITservice@bmw.com
none    SF3-JP-ServerAdmin@list.bmw.com
none    SF4-US-Insurance@list.bmw.com
none    SF5-CN-IT@bmw.com
none    SF5-JP-ServerAdmin@list.bmw.com
none    SRA-operation@list.bmw.com
none    ZA-SF-SoftwareMaintenance-Support@list.bmw.com
none    a2mac1-i.bmw.com
none    a2mac1-inti.bmw.com
none    a3-int.bmw.com
none    admin.meetmini@list.bmw.com
none    aem-author-inti2.bmw.com
none    aem-author-pocaka-inta6.bmw.com
none    alpheradealerpoint.bmwgroupfinance.jp
none    amab-i.bmw.com
none    amb-int.bmw.com
none    amc.bmw.com
none    aos-osp.bmw.com
none    apac.helpde
....
```

Transferencia de zona

Es el proceso por el cual se copia el contenido de un servidor DNS principal en un servidor DNS secundario. También se conoce como AXFR, que es el nombre de la consulta o petición en el protocolo DNS para realizar esta acción. Las peticiones AXFR siempre son iniciadas por el servidor DNS secundario y el servidor DNS principal simplemente responde. El servidor principal debe filtrar la dirección IP de los servidores secundarios que pueden realizar dichas acciones, de lo contrario sería posible obtener todos los datos del servidor primario, incluidos los registros DNS de la red interna.

- Herramientas: *dnsenum*, *fierce*, *dnsrecon*.
 - *dnsenum* <dominio>
 - *dnsrecon -a --domain* <dominio>

```
(kali㉿kali)-[~]  
$ dnsrecon -a --domain ieszaidinvergeles.org  
[*] std: Performing General Enumeration against: ieszaidinvergeles.org ...  
[*] Checking for Zone Transfer for ieszaidinvergeles.org name servers  
[*] Resolving SOA Record  
[-] Error while resolving SOA record.  
[*] Resolving NS Records  
[*] NS Servers found:  
[*] Removing any duplicate NS server IP Addresses ...  
[*] Checking for Zone Transfer for ieszaidinvergeles.org name servers  
[*] Resolving SOA Record  
[-] Error while resolving SOA record.  
[*] Resolving NS Records  
[*] NS Servers found:  
[*] Removing any duplicate NS server IP Addresses ...
```

Ilustración 5: Prueba de transferencia de zona con el comando dnsrecon

DNS Cache Snooping

Consiste en consultar al servidor DNS si un determinado dominio está almacenado en la caché. Se emplea un diccionario de todos los sitios web que queremos probar. De este modo podríamos averiguar los sitios por los que los usuarios de la organización navegan. Esta información podría ser útil para diseñar ataques con el [Framework Evilgrade](#) para inyectar actualizaciones de software maliciosas (para ello, previamente se ha debido realizar un MitM).

- Herramientas: *dnsrecon*.
 - *dnsrecon -d <dominio> -n <name_server> -t snoop -D <diccionario>*

```
(kali㉿kali)-[~]  
$ dnsrecon --domain ieszaidinvergeles.org -n 217.160.80.25 -t snoop -D /usr/share/dnsrecon/snoop.txt  
[*] Using the dictionary file: /usr/share/dnsrecon/snoop.txt (provided by user)  
[*] snoop: Performing Cache Snooping against NS Server: 217.160.80.25 ...  
[*] Name: google.com. TTL: 178 Address: 142.250.185.238 Type: A  
[*] Name: yahoo.com. TTL: 317 Address: 98.137.11.164 Type: A  
[*] Name: yahoo.com. TTL: 317 Address: 74.6.143.25 Type: A  
[*] Name: yahoo.com. TTL: 317 Address: 98.137.11.163 Type: A  
[*] Name: yahoo.com. TTL: 317 Address: 74.6.231.21 Type: A  
[*] Name: yahoo.com. TTL: 317 Address: 74.6.143.26 Type: A  
[*] Name: yahoo.com. TTL: 317 Address: 74.6.231.20 Type: A
```

Ilustración 6: Intento de DNS Cache Snooping con dnsrecon al dominio ieszaidinvergeles.org

Recurso

Usar DNS Cache Snooping para hacer DNS fingerprinting

<https://www.elladodelmal.com/2016/04/usar-dns-cache-snooping-para-hacer-dns.html>

3. Caso práctico guiado

Se ha elegido el dominio de la empresa BMW para realizar la recopilación de información.

Comenzamos utilizando el comando whois. El cuadro siguiente muestra los resultados ofrecidos en la ejecución del comando (se ha eliminado información irrelevante y advertencias legales).

```
$ whois bmw.com
Domain Name: BMW.COM
Registry Domain ID: 43804_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: http://cscdbs.com
Updated Date: 2019-11-14T15:31:22Z
Creation Date: 1996-01-29T05:00:00Z
Registry Expiry Date: 2029-01-30T05:00:00Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: 8887802723
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS.BMW.DE
Name Server: NS2.M-ONLINE.NET
Name Server: NS3.M-ONLINE.NET
Name Server: NS4.M-ONLINE.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-02-08T10:07:48Z <<<
```

The Registry database contains ONLY .COM, .NET, .EDU domains and Registrars.

```
Domain Name: bmw.com
Registry Domain ID: 43804_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2020-10-02T12:05:03Z
Creation Date: 1996-01-29T00:00:00.000-05:00
Registrar Registration Expiration Date: 2029-01-30T05:00:00.000-05:00
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Not Disclosed
Registrant Organization: Not Disclosed
Registrant Street: Not Disclosed
Registrant City: Munich
Registrant State/Province:
Registrant Postal Code: 80788
Registrant Country: DE
Registrant Phone: +Not Disclosed
Registrant Phone Ext:
Registrant Fax: +Not Disclosed
Registrant Fax Ext:
Registrant Email: Not Disclosed
```

```
Registry Admin ID:  
Admin Name: Not Disclosed  
Admin Organization: Not Disclosed  
Admin Street: Not Disclosed  
Admin City: Munich  
Admin State/Province:  
Admin Postal Code: 80788  
Admin Country: DE  
Admin Phone: +Not Disclosed  
Admin Phone Ext:  
Admin Fax: +Not Disclosed  
Admin Fax Ext:  
Admin Email: Not Disclosed  
Registry Tech ID:  
Tech Name: Not Disclosed  
Tech Organization: Not Disclosed  
Tech Street: Not Disclosed  
Tech City: Munich  
Tech State/Province:  
Tech Postal Code: 80788  
Tech Country: DE  
Tech Phone: +Not Disclosed  
Tech Phone Ext:  
Tech Fax: +Not Disclosed  
Tech Fax Ext:  
Tech Email: Not Disclosed  
Name Server: ns2.m-online.net  
Name Server: ns.bmw.de  
Name Server: ns3.m-online.net  
Name Server: ns4.m-online.net  
DNSSEC: unsigned
```

Destacan las entradas **Domain Status**, donde podemos observar que el dominio no se puede borrar, transferir o actualizar. Permite evitar el hackeo del dominio.

Recurso [ENG]

Códigos de estado de un dominio.

<https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en>

Podemos observar también que dispone de 4 servidores de nombres (**name server**), tres de ellos externos al dominio de BMW. El resto de datos personales aparecen ocultos.

En el siguiente paso utilizaremos el comando **dnsrecon** para obtener otros dominios de primer nivel que contengan una cadena en su nombre de dominio. Posteriormente, deberemos usar whois con los dominios obtenidos para comprobar si pertenecen o no al objetivo. Esto es útil para saber si la empresa, además de un dominio .com, tiene registrados otros dominios (.es, .fr, etc.), en el caso de grandes empresas será lo habitual.

```
$ dnsrecon -t tld -d bmw  
[*] Performing TLD Brute force Enumeration against bmw  
[*] The operation could take up to: 00:01:07  
[*] A bmw.net.ag 34.102.136.180  
[*] CNAME bmw.ai park.io  
[*] A park.io 54.235.69.41  
[*] A park.io 50.19.236.14  
[*] A bmw.org.ag 34.102.136.180  
[*] A bmw.al 184.25.179.45  
[*] A bmw.al 184.31.3.43  
[*] A bmw.al 184.31.10.46
```

```
[*] A bmw.al 104.109.12.39
[*] A bmw.al 104.109.11.39
[*] A bmw.al 23.1.106.46
...
[*] A bmw.co.uk 160.46.226.165
[*] A bmw.uk 160.46.244.54
[*] A bmw.us 64.29.204.16
[*] A bmw.org.uk 85.233.160.22
[*] A bmw.org.ua 159.69.35.8
[*] A bmw.co.uy 69.162.126.13
[*] A bmw.com.uy 160.46.226.165
[*] A bmw.uz 160.46.231.95
[*] CNAME bmw.biz.uz biz.uz
[*] A biz.uz 144.76.162.245
[*] A bmw.vc 133.242.70.66
[*] A bmw.co.vg 88.198.29.97
[*] A bmw.com.vg 88.198.29.97
[*] A bmw.com.ve 160.46.226.165
[*] A bmw.net.vg 166.62.28.147
[*] A bmw.biz.vg 89.31.143.20
[*] A bmw.vn 160.46.226.165
[*] A bmw.vu 160.46.244.131
[*] A bmw.wf 165.160.15.20
[*] A bmw.wf 165.160.13.20
[*] A bmw.ws 64.70.19.203
[*] A bmw.org.ws 202.4.48.211
[*] A bmw.net.ws 202.4.48.211
[*] CNAME bmw.co.ws suhao.github.io
[*] A suhao.github.io 185.199.110.153
[*] A suhao.github.io 185.199.108.153
[*] A suhao.github.io 185.199.111.153
[*] A suhao.github.io 185.199.109.153
[*] A bmw.com.ws 202.4.48.211
[*] A bmw.biz.wf 46.166.184.113
[*] A bmw.biz.wf 185.206.180.119
[*] AAAA bmw.biz.wf 2a00:1768:2001:63::46:113
[*] AAAA bmw.biz.wf 2a0b:1640:1:1:1:1:c45:4c4f
[*] A bmw.net.vn 112.213.89.3
[*] A bmw.co.za 160.46.226.165
[+] 340 Records Found
```

Las opciones del comando son las siguientes: *dnsrecon -t tld -d bmw*

- -t (*type*). Indica el tipo de dominio a buscar, en nuestra caso tld.
- -d (*domain*). Nombre base del dominio a buscar.

La información obtenida debería ser almacenada y posteriormente analizada para buscar vulnerabilidades en cada una de ellas.

Recurso [ENG]

Footprinting with dnsrecon

<https://laptrinhx.com/footprinting-with-dnsrecon-2994369622/>

Si intentamos obtener información de alguno de los dominios obtenidos, por ejemplo bmw.es no obtendremos la información esperada.

```
$ whois bmw.es
Este TLD no dispone de servidor whois, pero puede acceder a la base de datos de whois en
https://www.nic.es/
```

En este caso, **whois no almacena la información de los registros regionales**, por lo que tenemos que ir a la página del registrador oficial, en el caso de los dominios .es en www.dominios.es. La imagen siguiente muestra los dominios registrados y disponibles.

Dominios disponibles			
DOMINIO	DISPONIBLE	REGISTRAR CON ...	
bmw.es	✗	Registrado. Ver datos	
bmw.com.es	✗	Registrado. Ver datos	
bmw.nom.es	✓	<input type="text"/>	Agente Registrador Dominios.es
bmw.org.es	✗	Registrado. Ver datos	
bmw.gob.es	✓	<input type="text"/>	Agente Registrador Dominios.es
bmw.edu.es	✓	<input type="text"/>	Agente Registrador Dominios.es

DATOS DEL TITULAR	
Nombre del Dominio	bmw.es
Estado	Activado
Identificador	6D8A-MIG1
Titular	BMW Iberica S.A.
Fecha de Alta	07-11-1995
Fecha de Caducidad	07-11-2021
Agente Registrador	INTERDOMINIOS
PERSONA DE CONTACTO ADMINISTRATIVO	
Identificador	960909-ESNIC-F5
Nombre	Javier Casanova
PERSONA DE CONTACTO TECNICO	
Identificador	96090A-ESNIC-F5
Nombre	Javier Casanova
SERVIDORES DNS	
Nombre Servidor	IP
dns.bmw.es	194.106.16.134
dns3.bmw.es	194.106.16.135
dns2.bmw.es	217.118.113.111

Podemos acceder a los datos de [bmw.es](#) pinchando en el **enlace ver datos**, tras superar un *captcha*. En este caso, obtenemos datos de la persona de contacto técnico y administrativo. Esta la podríamos relacionar con otros datos obtenidos en otros procesos de recolección de información, por ejemplo, si

hemos obtenido su dirección de correo.

```
person:      Bernd-Rainer Kottke
address:     Bernd-Rainer Kottke
address:     BMW Group
address:     Internationales Netzwerk (FI-40)
address:     80788 Muenchen
phone:       +49 89 382 47065
fax-no:      +49 89 382 41749
e-mail:      bernd-rainer.kottke@bmw.de
nic-hdl:     BK173-RIPE
mnt-by:      BMW-MNT
created:     2001-11-22T16:53:57Z
last-modified: 2001-11-22T16:53:57Z
source:      RIPE
```

El siguiente paso será **buscar en ripe.net una de las IPs obtenidas en el listado anterior** de dominios

```
inetnum:      160.46.0.0 - 160.46.255.255
status:       LEGACY
remarks:      **** INFORMATION FROM ARIN OBJECT ****
remarks:      netname: BER-NET
descr:        BMW AG, Berlin production plant
descr:        BMW AG, FI-13
descr:        Postfach 400240
descr:        D-W-8000 Muenchen 40
remarks:      country: DE
admin-c:      KK699-RIPE
tech-c:       BK173-RIPE
remarks:      changed: hostmaster@arin.net 19920521
remarks:      changed: hostmaster@arin.net 19920521
remarks:      **** INFORMATION FROM RIPE OBJECT ****
netname:      BER-NET
descr:        BMW AG, Berlin production plant
country:      DE
mnt-by:       BMW-MNT
mnt-lower:    BMW-MNT
mnt-domains:  BMW-MNT
mnt-routes:   BMW-MNT
mnt-routes:   AS8590-MNT
created:      1970-01-01T00:00:00Z
last-modified: 2019-12-04T13:01:21Z
source:      RIPE
```

```
route:        160.46.240.0/20
descr:        Route Object BMW
origin:        AS8590
mnt-routes:    CW-RR
mnt-routes:    AS8590-MNT
mnt-by:        CW-RR
created:       2007-04-24T07:51:19Z
last-modified: 2007-04-24T07:51:19Z
source:      RIPE
```

TLD de bmw. Elegiremos la IP del **dominio bmw.uk (160.46.244.54)**. En la imagen podemos observar que la IP pertenece a un rango de direcciones IP (*inetnum*) y los datos de contacto administrativo y técnico que sí son accesibles. Por ejemplo, los datos de contacto técnico. También podemos observar los datos del mantenedor (*mnt*) y del router o AS.

Esto mismo se puede realizar con el comando *whois*.

- `whois -h whois.ripe.net <ip>`
- `whois -r --sources RIPE <ip>`

```
$ whois -r --sources RIPE 160.46.244.54

% 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
descr:           D-W-8000 Muenchen 40
remarks:          country: DE
admin-c:         KK699-RIPE
tech-c:          BK173-RIPE
remarks:          changed: hostmaster@arin.net 19920521
remarks:          changed: hostmaster@arin.net 19920521
remarks:          **** INFORMATION FROM RIPE OBJECT ****
netname:          BER-NET
descr:           BMW AG, Berlin production plant
country:         DE
mnt-by:          BMW-MNT
mnt-lower:        BMW-MNT
mnt-domains:     BMW-MNT
mnt-routes:      BMW-MNT
mnt-routes:      AS8590-MNT
created:         1970-01-01T00:00:00Z
last-modified:    2019-12-04T13:01:21Z
source:          RIPE

% Information related to '160.46.240.0/20AS8590'

route:           160.46.240.0/20
descr:           Route Object BMW
origin:          AS8590
mnt-routes:      CW-RR
mnt-routes:      AS8590-MNT
mnt-by:          CW-RR
created:         2007-04-24T07:51:19Z
last-modified:    2007-04-24T07:51:19Z
source:          RIPE

% This query was served by the RIPE Database Query Service version 1.99 (ANGUS)
```

Otra opción de búsqueda interesante es buscar por **netname**. En lugar de introducir la IP en el buscador de RIPE, podemos introducir el dato obtenido del **netname**. Podríamos intentar hallar una IP de BMW en España para obtener su **netname**, y posteriormente realizar una búsqueda de más IPs en esa misma red. Por ejemplo, la IP 194.106.16.157, nos sirve para este propósito.

```
$ whois -r --sources RIPE 194.106.16.157

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
```

Probaremos con el *netname* BMW_IBERICA. Podríamos ahora sí, ver los datos de contacto técnico y administrativo que antes vimos en la consulta a dominios.es. El comando alternativo en *whois* sería el siguiente:

```
$ whois -r --sources RIPE BMW_IBERICA
```

Responsible organisation: [VODAFONE ONO, S.A.](#)

Abuse contact info: 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-ONO
created:    2003-11-26T12:46:23Z
last-modified: 2014-05-07T08:32:45Z
source:     RIPE# Filtered
```

Login to update 


[RIPEstat](#) 

Responsible organisation: [VODAFONE ONO, S.A.](#)

Abuse contact info: abuse@corp.vodafone.es

```
inetnum:    194.149.197.0 - 194.149.197.63
netname:    BMW_IBERICA
descr:      BMW IBERICA, S.A.
country:    ES
admin-c:    JC1699-RIPE
tech-c:     JC1699-RIPE
status:     ASSIGNED PA
mnt-by:     MNT-PROV-ONO
created:    2005-03-08T15:29:55Z
last-modified: 2014-05-07T08:33:15Z
source:     RIPE# Filtered
```

Login to update 

[RIPEstat](#) 

El siguiente objetivo será obtener nombres de dominio de máquinas. Podemos usar el comando *host* con dos opciones diferentes:

- *host -t a <dominio>*. Obtiene los registros A del dominio indicado.
- *host -t ptr <ip>*. Obtiene los registros PTR de la IP indicada.

Para probar el primer comando, usaremos el **servidor de nombres primario** obtenido con *whois*: *ns.bmw.de*

```
$ host -t a ns.bmw.de
ns.bmw.de has address 192.109.190.2
```

Si hacemos el inverso:

```
$ host -t ptr 192.109.190.2
2.190.109.192.in-addr.arpa domain name pointer ns.bmw.de.
```

¿Cómo podemos usar el comando *host* con rangos de IP grandes? Partimos de la dirección IP 192.109.190.2 y realizamos un *whois*.

```
$ whois 192.109.190.2

NetRange:          192.109.121.0 - 192.109.241.255
CIDR:              192.109.128.0/18, 192.109.121.0/24, 192.109.192.0/19, 192.109.240.0/23,
192.109.124.0/22, 192.109.122.0/23, 192.109.224.0/20
NetName:           RIPE-ERX-192-109-121-0
NetHandle:         NET-192-109-121-0-1
Parent:            NET192 (NET-192-0-0-0-0)
NetType:           Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:     RIPE Network Coordination Centre (RIPE)
RegDate:           2005-01-31
Updated:           2009-10-20
Comment:           These addresses have been further assigned to users in
Comment:           the RIPE NCC region. Contact information can be found in
Comment:           the RIPE database at http://www.ripe.net/whois
Ref:               https://rdap.arin.net/registry/ip/192.109.121.0

ResourceLink:      https://apps.db.ripe.net/search/query.html
ResourceLink:      whois.ripe.net

OrgName:           RIPE Network Coordination Centre
OrgId:             RIPE
Address:           P.O. Box 10096
City:              Amsterdam
StateProv:
PostalCode:        1001EB
Country:           NL
RegDate:
Updated:           2013-07-29
Ref:               https://rdap.arin.net/registry/entity/RIPE

ReferralServer:    whois://whois.ripe.net
ResourceLink:      https://apps.db.ripe.net/search/query.html

OrgAbuseHandle:    ABUSE3850-ARIN
OrgAbuseName:      Abuse Contact
OrgAbusePhone:     +31205354444
OrgAbuseEmail:     abuse@ripe.net
OrgAbuseRef:       https://rdap.arin.net/registry/entity/ABUSE3850-ARIN

OrgTechHandle:     RN029-ARIN
OrgTechName:       RIPE NCC Operations
OrgTechPhone:      +31 20 535 4444
```

```
OrgTechEmail: hostmaster@ripe.net
OrgTechRef: https://rdap.arin.net/registry/entity/RN029-ARIN

Se ha encontrado una referencia a whois.ripe.net.

% 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 '192.109.190.0 - 192.109.190.255'

% Abuse contact for '192.109.190.0 - 192.109.190.255' is 'ripe-contact@list.bmw.com'

inetnum: 192.109.190.0 - 192.109.190.255
netname: BMW-NET
descr: 80788 Muenchen
descr: Germany
country: DE
org: ORG-BMWA1-RIPE
admin-c: BN04-RIPE
tech-c: BN04-RIPE
status: ASSIGNED PI
mnt-by: RIPE-NCC-END-MNT
mnt-by: BMW-MNT
mnt-by: AUTO-1BMW
created: 1970-01-01T00:00:00Z
last-modified: 2017-10-20T09:50:08Z
source: RIPE
```

Encontramos el *netname* BMW-NET. Ahora vamos a obtener todos los rangos de IP (*inetnum*) de este *netname*.

```
$ 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
inetnum: 88.217.174.184 - 88.217.174.191
inetnum: 192.109.190.0 - 192.109.190.255
inetnum: 193.23.32.0 - 193.23.45.255
inetnum: 194.185.176.64 - 194.185.176.95
inetnum: 195.67.91.0 - 195.67.91.63
inetnum: 195.149.159.176 - 195.149.159.183
inetnum: 212.114.130.0 - 212.114.130.15
```

Seguidamente, podemos hacer una resolución inversa de cada IP de un determinado rango. El comando

dnsrecon permite realizar esto. Mostraremos el resultado con el rango 192.109.190.0-192.109.190.255.

- *-r <range>*. Rango de direcciones IP.
- *-t rvl*. Indicamos el tipo reverso.
- *-d <domain>*. El nombre base del dominio a buscar.

```
$ dnsrecon -r 192.109.190.0-192.109.190.255 -t rvl -d bmw
[*] Reverse Look-up of a Range
[*] Performing Reverse Lookup from 192.109.190.0 to 192.109.190.255
[*] PTR ns.bmw.de 192.109.190.2
[*] PTR proxy7.bmw.de 192.109.190.8
[*] PTR gw01-d.bmwgroup.com 192.109.190.1
[*] PTR codisprod.bmwgroup.com 192.109.190.13
[*] PTR ibpdmz-ns-n1.bmw.de 192.109.190.10
[*] PTR e2e-b2b-webeamnext-swl-sec2-admin.bmw.com 192.109.190.12
[*] PTR proxy8.bmw.de 192.109.190.15
[*] PTR efinance-directentry.bmwbank.de 192.109.190.19
[*] PTR sgate-o.bmwgroup.com 192.109.190.24
[*] PTR extranet-sgate-premium.bmwgroup.com 192.109.190.30
[*] PTR sfhexa-neu.bmw.de 192.109.190.33
[*] PTR ns-cache-2-old.bmw.de 192.109.190.25
[*] PTR shop-80.mini.de 192.109.190.18
[*] PTR webappt6.bmw.com 192.109.190.29
[*] PTR ibpdmz-nsb.bmwgroup.net 192.109.190.20
[*] PTR dop-o.bmwgroup.com 192.109.190.57
[*] PTR asprb2b-o.bmw.com 192.109.190.60
[*] PTR spweb1.bmw.com 192.109.190.64
[*] PTR sync-test1.bmw.de 192.109.190.69
[*] PTR sync-test2.bmw.de 192.109.190.70
[*] PTR wcmstraining.bmwgroup.com 192.109.190.72
[*] PTR enterpriseenrollment.bmwgroup.com 192.109.190.74
[*] PTR mdm.bmwgroup.com 192.109.190.75
[*] PTR sync.bmwgroup.com 192.109.190.76
[*] PTR mdm-int.bmwgroup.com 192.109.190.79
[*] PTR mag.bmwgroup.com 192.109.190.77
[*] PTR webcon14.bmw.de 192.109.190.83
[*] PTR av14.bmw.de 192.109.190.84
[*] PTR access14.bmw.de 192.109.190.82
[*] PTR ucpl4rp.bmw.de 192.109.190.85
[*] PTR proxy6.bmw.de 192.109.190.87
[*] PTR uct14rp.bmw.de 192.109.190.86
[*] PTR vproxy01.bmwgroup.com 192.109.190.88
[*] PTR emm-idm-int.bmwgroup.net 192.109.190.90
[*] PTR b2dpapp5.bmwgroup.com 192.109.190.91
[*] PTR b2dpapp6.bmwgroup.com 192.109.190.92
[*] PTR erfxt.bmw.de 192.109.190.108
[*] PTR b2b-o.bmw.com 192.109.190.115
[*] PTR webappt.bmw.com 192.109.190.143
[*] PTR wcminter-3.bmwgroup.com 192.109.190.151
[*] PTR wcminter-4.bmwgroup.com 192.109.190.152
[*] PTR contenteditor.bmwgroup.com 192.109.190.153
[*] PTR spwww1.bmw.com 192.109.190.160
[*] PTR spwww2.bmw.com 192.109.190.161
[*] PTR famos-uk-old.bmw.com 192.109.190.171
[*] PTR spoa-prod-o.bmwgroup.com 192.109.190.176
[*] PTR jetstream.bmw.com 192.109.190.184
[*] PTR pdm-o.bmw.com 192.109.190.200
[*] PTR n1.bmw.de 192.109.190.201
[*] PTR n2.bmw.de 192.109.190.202
[*] PTR www.press-neu.bmwgroup.com 192.109.190.205
[*] PTR wartungsinfo.bmwgroup.com 192.109.190.206
[*] PTR cs-i-n.bmwgroup.com 192.109.190.221
[*] PTR sbnk0023.bmwbank.de 192.109.190.226
```

```
[*] PTR cs-p-alt.bmwgroup.com 192.109.190.230
[*] PTR sbnk0024.bmwbank.de 192.109.190.232
[*] PTR dd-o.bmwgroup.com 192.109.190.234
[*] PTR spweb2.bmw.com 192.109.190.235
[*] PTR www2.bmwbank.de 192.109.190.240
[*] PTR www-t.bmwbank.de 192.109.190.241
[*] PTR www.plant.bmwgroup.com 192.109.190.247
[+] 61 Records Found
```

Pasamos ahora a averiguar los servidores de correo. Utilizamos el comando *host* con la opción *-t mx*.

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

El resultado muestra dos servidores de correo, uno con un peso de 20 (*mx2*) y otro con un peso de 10 (*mx1*). ¿Realmente son solo dos servidores de correo? También destaca el dominio, que no tiene que ver con BMW.

Averigüemos algo más de estos equipos con el comando *host*.

```
$ host mx1.hc324-48.eu.iphmx.com
mx1.hc324-48.eu.iphmx.com has address 207.54.71.48
mx1.hc324-48.eu.iphmx.com has address 207.54.69.27
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 207.54.68.120
mx1.hc324-48.eu.iphmx.com has address 207.54.69.24
mx1.hc324-48.eu.iphmx.com has address 207.54.69.29
mx1.hc324-48.eu.iphmx.com has address 207.54.69.30
mx1.hc324-48.eu.iphmx.com has address 207.54.68.119
mx1.hc324-48.eu.iphmx.com has address 207.54.72.35
mx1.hc324-48.eu.iphmx.com has address 207.54.68.121
mx1.hc324-48.eu.iphmx.com has address 207.54.65.242
mx1.hc324-48.eu.iphmx.com has address 207.54.71.126
mx1.hc324-48.eu.iphmx.com has address 207.54.72.34
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2012:300::3f9
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3fa
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2012:300::3ff
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3fb
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3fd
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3fc
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3fe
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2012:300::3fe
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2012:300::3fc
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2012:300::3fd
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2012:300::3fa
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::3ff
mx1.hc324-48.eu.iphmx.com has IPv6 address 2620:101:2011:300::3f9
```

Podemos ver que esa dirección URL, tiene 14 direcciones IP asociadas, que pueden ser los propios servidores de correo, servidores antispam, etc. Obtengamos el *whois* de uno de ellos.

```
$ whois 207.54.71.48
NetRange:      207.54.64.0 - 207.54.95.255
CIDR:          207.54.64.0/19
NetName:       CISL-7
```

```
NetHandle: NET-207-54-64-0-1
Parent: NET207 (NET-207-0-0-0-0)
NetType: Direct Assignment
OriginAS: AS16417, AS30238, AS30214, AS30215
Organization: Cisco Systems Ironport Division (CISL-7)
RegDate: 2018-11-30
Updated: 2019-04-23
Ref: https://rdap.arin.net/registry/ip/207.54.64.0

OrgName: Cisco Systems Ironport Division
OrgId: CISL-7
Address: 170 West Tasman Drive
City: San Jose
StateProv: CA
PostalCode: 95134
Country: US
RegDate: 2010-11-09
Updated: 2020-01-29
Ref: https://rdap.arin.net/registry/entity/CISL-7
```

Podemos observar que el rango de IPs coincide con las IPs de los servidores de correo y pertenecen a **Cisco System Ironport Division**, una empresa que adquirió Cisco, dedicada a servicios de protección de spam.

Recurso [ENG]

Entrada en la Wikipedia de IronPort
<https://en.wikipedia.org/wiki/IronPort>

Continuemos consultando los servidores de nombres de BMW con la opción `-t ns` del comando `host`. Estos datos coinciden con los obtenidos inicialmente con `whois`.

```
$ host -t ns bmw.com
bmw.com name server ns2.m-online.net.
bmw.com name server ns.bmw.de.
bmw.com name server ns4.m-online.net.
bmw.com name server ns3.m-online.net.
```

El comando ***dig*** (*Domain Information Groper*) es otra herramienta poderosa para realizar consultas DNS. El comando `dig` hace la consulta por defecto a nuestro servidor DNS que podemos consultar en el fichero `/etc/resolv.conf`

```
$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 10.0.2.3
```

Ejecutando `dig` sobre el dominio `bmw.com` obtenemos información de los registros A del dominio.

```
$ dig bmw.com

; <<>> DiG 9.16.15-Debian <<>> bmw.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12460
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
```



```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 65494
;; QUESTION SECTION:
;bmw.com.                IN      A

;; ANSWER SECTION:
bmw.com.                300     IN      A      160.46.226.165

;; Query time: 72 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Tue Nov 16 12:18:57 EST 2021
;; MSG SIZE rcvd: 52
```

Podemos realizar la consulta de modo que solo obtengamos el registro PTR con **+short**.

```
$ dig bmw.com +short
160.46.226.165
```

Podemos mostrar como resultado solo la sección ;ANSWER con el comando **+noall +answer**.

```
$ dig bmw.com +noall +answer
bmw.com.                8        IN      A      160.46.226.165
```

Podemos cambiar el servidor al que queremos realizar la consulta con el símbolo **@** seguido de la dirección IP. A continuación se muestra la información obtenida si hacemos la consulta al servidor DNS de Google. La opción **ANY** añade todos los registros DNS del dominio indicado, no solo los registros A. Podemos observar los registros TXT donde aparece información para la verificación del dominio de BMW en diferentes sitios (Google, Facebook, Microsoft, etc.).

```
$ dig @8.8.8.8 bmw.com ANY

; <<>> DiG 9.16.15-Debian <<>> @8.8.8.8 bmw.com ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53837
;; flags: qr rd ra; QUERY: 1, ANSWER: 19, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;bmw.com.                IN      ANY

;; ANSWER SECTION:
bmw.com.                3600    IN      NS      ns2.m-online.net.
bmw.com.                3600    IN      NS      ns3.m-online.net.
bmw.com.                3600    IN      NS      ns.bmw.de.
bmw.com.                3600    IN      NS      ns4.m-online.net.
bmw.com.                3600    IN      TXT     "v=spf1 exists:%{i}.spf.bmwgroup.com
include:servers.mcsv.net ~all"
bmw.com.                3600    IN      TXT     "MS=ms55083425"
bmw.com.                3600    IN      TXT     "IjFiuU0j36RbwT08cBQddNhQgCOFQ9ZWYisbdZ4T9aI="
bmw.com.                3600    IN      TXT     "google-site-verification=y48_Huwdcv0YgVAv4d-
hd7WFAjJtr_tn9FH-vjUu34"
bmw.com.                3600    IN      TXT     "facebook-domain-
```

```
verification=7qshqm5nhxp077vc3pjczh8prtzzf"
bmw.com.          3600    IN      TXT      "swisssign-
check=XhWTI8XD2rKnZho3xuYlG98B7Zf14pGigehhwkQMEI"
bmw.com.          3600    IN      TXT      "Dynatrace-site-verification=b7c1e591-49bf-46db-aea0-
4ba1064710cc__h9acrql0pl6aodc853ofh936se"
bmw.com.          3600    IN      TXT      "google-site-
verification=7qhHl1QEE0eXqplmX6Fyvn6NlQMkSeN4ScxwyjqSNM8"
bmw.com.          3600    IN      TXT      "MS=ms60515415"
bmw.com.          3600    IN      TXT      "globalsign-domain-
verification=jzdviERoHIp4wRVQiFh0tL0sRFjdFptn_P5T5m5zj8"
bmw.com.          3600    IN      TXT      "adobe-sign-
verification=15bb0cf14bab7e7f78038ee6a1fcdb9"
bmw.com.          300     IN      MX       10 mx1.hc324-48.eu.iphmx.com.
bmw.com.          300     IN      MX       20 mx2.hc324-48.eu.iphmx.com.
bmw.com.          300     IN      A        160.46.226.165
bmw.com.          3600    IN      SOA      ns.bmw.de. domadm.bmw.de. 2011126921 10800 3600
2592000 900

;; Query time: 68 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Tue Nov 16 12:25:53 EST 2021
;; MSG SIZE rcvd: 995
```

Podríamos limitar la consulta solo para obtener los datos de los registros MX.

```
$ dig bmw.com MX

; <<>> DiG 9.16.15-Debian <<>> bmw.com MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 9503
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 65494
;; QUESTION SECTION:
;bmw.com.          IN      MX

;; ANSWER SECTION:
bmw.com.          300     IN      MX       20 mx2.hc324-48.eu.iphmx.com.
bmw.com.          300     IN      MX       10 mx1.hc324-48.eu.iphmx.com.

;; Query time: 68 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Tue Nov 16 12:27:28 EST 2021
;; MSG SIZE rcvd: 94
```

Con el comando *dig* también podemos comprobar si está disponible la transferencia de zona con **axfr**.

```
$ dig bmw.com axfr

; <<>> DiG 9.16.15-Debian <<>> bmw.com axfr
;; global options: +cmd
; Transfer failed.
```

Recurso [ENG]

Información de cómo usar el comando dig.

<https://phoenixnap.com/kb/linux-dig-command-examples>

Por último, vamos a intentar obtener los datos de los **subdominios de los que dispone BMW** con el comando *dnsenum*. También comprobamos que la **transferencia de zona** se encuentra correctamente configurada y no es posible realizarla. La información ofrecida por este comando es bastante exhaustiva.

```
$ dnsenum bmw.com

dnsenum VERSION:1.2.6

-----  bmw.com  -----

Host's addresses:
-----
bmw.com.                300      IN      A       160.46.226.165

Name Servers:
-----
ns.bmw.de.              6803     IN      A       192.109.190.2
ns3.m-online.net.       41661    IN      A       217.160.41.67
ns4.m-online.net.       83454    IN      A       212.114.171.64
ns2.m-online.net.       172800   IN      A       212.18.3.8

Mail (MX) Servers:
-----
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.68.121
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.71.60
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.69.27
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.69.29
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.65.242
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.68.119
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.72.35
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.71.69
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.69.24
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.71.48
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.68.120
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.72.34
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.69.30
mx2.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.71.126
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.68.119
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.65.242
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.69.27
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.68.120
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.69.29
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.68.121
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.71.48
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.72.35
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.69.30
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.72.34
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.71.126
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.69.24
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.71.60
mx1.hc324-48.eu.iphmx.com. 3600     IN      A       207.54.71.69
```

Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for bmw.com on ns.bmw.de ...
AXFR record query failed: timed out

Trying Zone Transfer for bmw.com on ns3.m-online.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for bmw.com on ns4.m-online.net ...
AXFR record query failed: REFUSED

Trying Zone Transfer for bmw.com on ns2.m-online.net ...
AXFR record query failed: REFUSED

Brute forcing with /usr/share/dnsenum/dns.txt:

asc.bmw.com.	86400	IN	A	160.46.240.170
beta.bmw.com.	3600	IN	CNAME	bmwprod.b.edgekey.net.
bmwprod.b.edgekey.net.	7199	IN	CNAME	e25631.dscb.akamaiedge.net.
e25631.dscb.akamaiedge.net.	19	IN	A	2.21.24.208
e25631.dscb.akamaiedge.net.	19	IN	A	2.21.25.49
fr.bmw.com.	86400	IN	A	160.46.247.181
ftp.bmw.com.	86400	IN	A	195.27.218.60
mobility.bmw.com.	300	IN	A	18.184.157.205
nic.bmw.com.	28800	IN	A	185.16.184.143
search.bmw.com.	86400	IN	A	62.67.62.32
secure.bmw.com.	300	IN	A	160.46.244.143
shop.bmw.com.	28800	IN	A	160.46.226.63
vpn.bmw.com.	300	IN	A	193.23.38.30
vpn2.bmw.com.	300	IN	A	193.23.33.6
www.bmw.com.	258	IN	CNAME	bmwprod.b-ion.edgekey.net.
bmwprod.b-ion.edgekey.net.	7199	IN	CNAME	e25631.dsca.akamaiedge.net.
e25631.dsca.akamaiedge.net.	19	IN	A	2.21.25.49
e25631.dsca.akamaiedge.net.	19	IN	A	2.21.24.208
www2.bmw.com.	600	IN	CNAME	www2.bmw.com.c.footprint.net.
www2.bmw.com.c.footprint.net.	299	IN	CNAME	g-cc.b.c.footprint.net.
g-cc.b.c.footprint.net.	229	IN	A	8.254.226.125

bmw.com class C netranges:

18.184.157.0/24
62.67.62.0/24
160.46.226.0/24
160.46.240.0/24
160.46.244.0/24
160.46.247.0/24
185.16.184.0/24
193.23.33.0/24
193.23.38.0/24
195.27.218.0/24

Performing reverse lookup on 2560 ip addresses:

19.226.46.160.in-addr.arpa.	28800	IN	PTR	tssbapac-prod.bmw.com.
44.226.46.160.in-addr.arpa.	28800	IN	PTR	etk-webservices.bmw.com.
44.226.46.160.in-addr.arpa.	28800	IN	PTR	webetk.bmw.com.
45.226.46.160.in-addr.arpa.	28800	IN	PTR	exdprod.bmw.com.
58.226.46.160.in-addr.arpa.	3600	IN	PTR	c2b-services.bmw.com.
59.226.46.160.in-addr.arpa.	28800	IN	PTR	cct-dev-test.bmw.com.
83.226.46.160.in-addr.arpa.	28800	IN	PTR	accessories.bmw.com.
84.226.46.160.in-addr.arpa.	28800	IN	PTR	piaoportal.bmw.com.
141.226.46.160.in-addr.arpa.	28800	IN	PTR	b2b-wen-new.bmw.com.

234.226.46.160.in-addr.arpa.	28800	IN	PTR	faas20nsf-prod.bmw.com.
15.240.46.160.in-addr.arpa.	28800	IN	PTR	opendxm.bmw.com.
17.240.46.160.in-addr.arpa.	28800	IN	PTR	b2b.bmw.com.
18.240.46.160.in-addr.arpa.	28800	IN	PTR	b2biff.bmw.com.
19.240.46.160.in-addr.arpa.	28800	IN	PTR	b2bpapp6.bmw.com.
20.240.46.160.in-addr.arpa.	28800	IN	PTR	b2bpapp8.bmw.com.
24.240.46.160.in-addr.arpa.	28800	IN	PTR	pars2.bmw.com.
29.240.46.160.in-addr.arpa.	28800	IN	PTR	emcq.bmw.com.
32.240.46.160.in-addr.arpa.	28800	IN	PTR	au.bmw.com.
37.240.46.160.in-addr.arpa.	28800	IN	PTR	spetros.bmw.com.
43.240.46.160.in-addr.arpa.	28800	IN	PTR	ldb.bmw.com.
45.240.46.160.in-addr.arpa.	28800	IN	PTR	efaplus.bmw.com.
46.240.46.160.in-addr.arpa.	28800	IN	PTR	rplan-b2b.bmw.com.
49.240.46.160.in-addr.arpa.	28800	IN	PTR	itms.bmw.com.
50.240.46.160.in-addr.arpa.	28800	IN	PTR	ppeapneu.bmw.com.
...				

Otro comando disponible para tratar de obtener una lista de subdominios es **fierce** que está disponible en Kali. Esta herramienta trata de encontrar IPs y hostnames contiguos a un dominio o subdominio dado. El inconveniente de esta herramienta es que puede ser muy lenta.

```
$ fierce --domain ieszaidinvergeles.org
2 x
NS: ns1020.ui-dns.com. ns1074.ui-dns.biz. ns1025.ui-dns.de. ns1022.ui-dns.org.
SOA: ns1025.ui-dns.de. (217.160.80.25)
Zone: failure
Wildcard: failure
Found: ftp.ieszaidinvergeles.org. (217.160.0.64)
Nearby:
{'217.160.0.59': '217-160-0-59.elastic-ssl.ui-r.com.',
 '217.160.0.60': '217-160-0-60.elastic-ssl.ui-r.com.',
 '217.160.0.61': '217-160-0-61.elastic-ssl.ui-r.com.',
 '217.160.0.62': '217-160-0-62.elastic-ssl.ui-r.com.',
 '217.160.0.63': '217-160-0-63.elastic-ssl.ui-r.com.',
 '217.160.0.64': '217-160-0-64.elastic-ssl.ui-r.com.',
 '217.160.0.65': '217-160-0-65.elastic-ssl.ui-r.com.',
 '217.160.0.66': '217-160-0-66.elastic-ssl.ui-r.com.',
 '217.160.0.67': '217-160-0-67.elastic-ssl.ui-r.com.',
 '217.160.0.68': '217-160-0-68.elastic-ssl.ui-r.com.',
 '217.160.0.69': '217-160-0-69.elastic-ssl.ui-r.com.'}
...
```

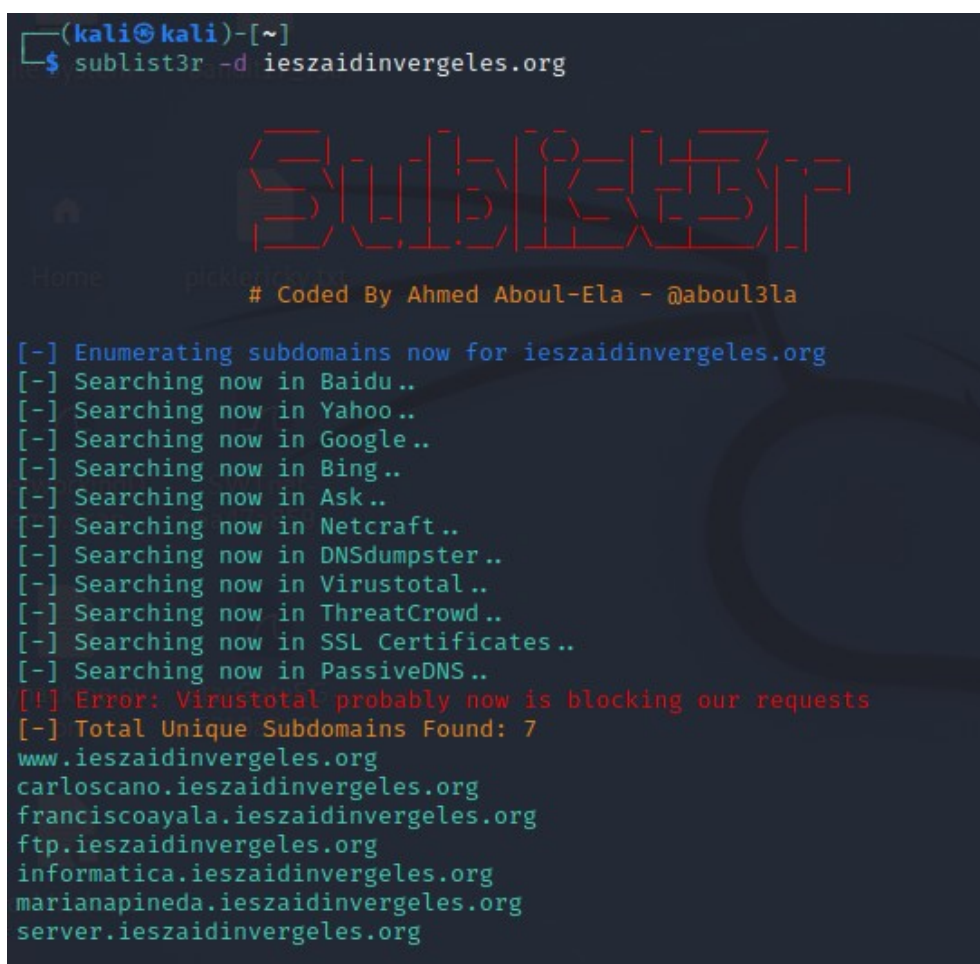
Con toda la información recopilada se puede proseguir la investigación en esta misma fase de reconocimiento (*footprinting*) o de la fase posterior (*fingerprinting*).

4. Herramientas de automatización

Existen multitud de scripts que automatizan el proceso de reconocimiento DNS. Solo mencionaremos dos, *sublist3r* y *spiderfoot*.

Sublist3r

Es un script escrito en python que utiliza OSINT para enumerar un dominio. Utiliza los buscadores de Google, Yahoo, Bing, Baidu y Ask. También emplea Netcraft, Virustotal, ThreatCrowd, DNSdumpster y ReverseDNS. Se puede instalar en Kali desde los repositorios con *apt*.



```
(kali㉿kali)-[~]
$ sublist3r -d ieszaidinvergeles.org

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for ieszaidinvergeles.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 7
www.ieszaidinvergeles.org
carloscano.ieszaidinvergeles.org
franciscoayala.ieszaidinvergeles.org
ftp.ieszaidinvergeles.org
informatica.ieszaidinvergeles.org
marianapineda.ieszaidinvergeles.org
server.ieszaidinvergeles.org
```

Ilustración 7: Enumeración con *sublist3r* para *ieszaidinvergeles.org*

Incorpora además el script **subbrute** para la búsqueda de subdominios mediante fuerza bruta usando diccionario, que se ha incorporado a la herramienta *sublist3r* mediante la opción **--bruteforce**. Esta opción puede ser bastante lenta.

Repositorio oficial de sublist3r
<https://github.com/aboul3la/Sublist3r>

Spiderfoot

Otra herramienta desarrollada en python que emplea OSINT para el reconocimiento DNS. Está disponible en la instalación base de Kali. Los scripts se encuentran en el directorio `/usr/share/spiderfoot` y en Kali disponemos de los comandos ***spiderfoot*** y ***spiderfoot-cli***, ya que es una herramienta que funciona en modo cliente-servidor.

Con ***spiderfoot -l ip:puerto*** arrancamos el servicio de *spiderfoot*.

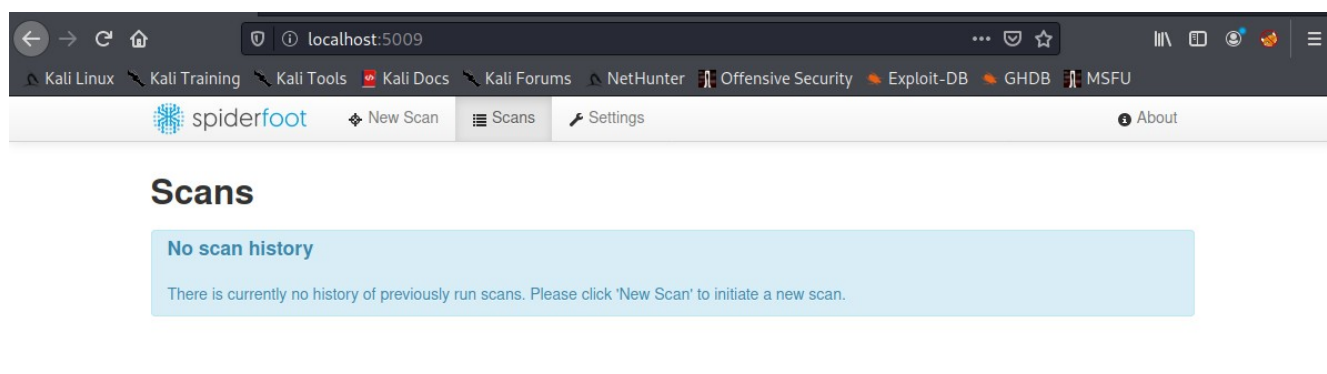
Arrancamos el servidor en nuestra máquina local y abrimos el navegador en el puerto indicado.

```
$ spiderfoot -l localhost:5009
Starting web server at http://localhost:5009 ...

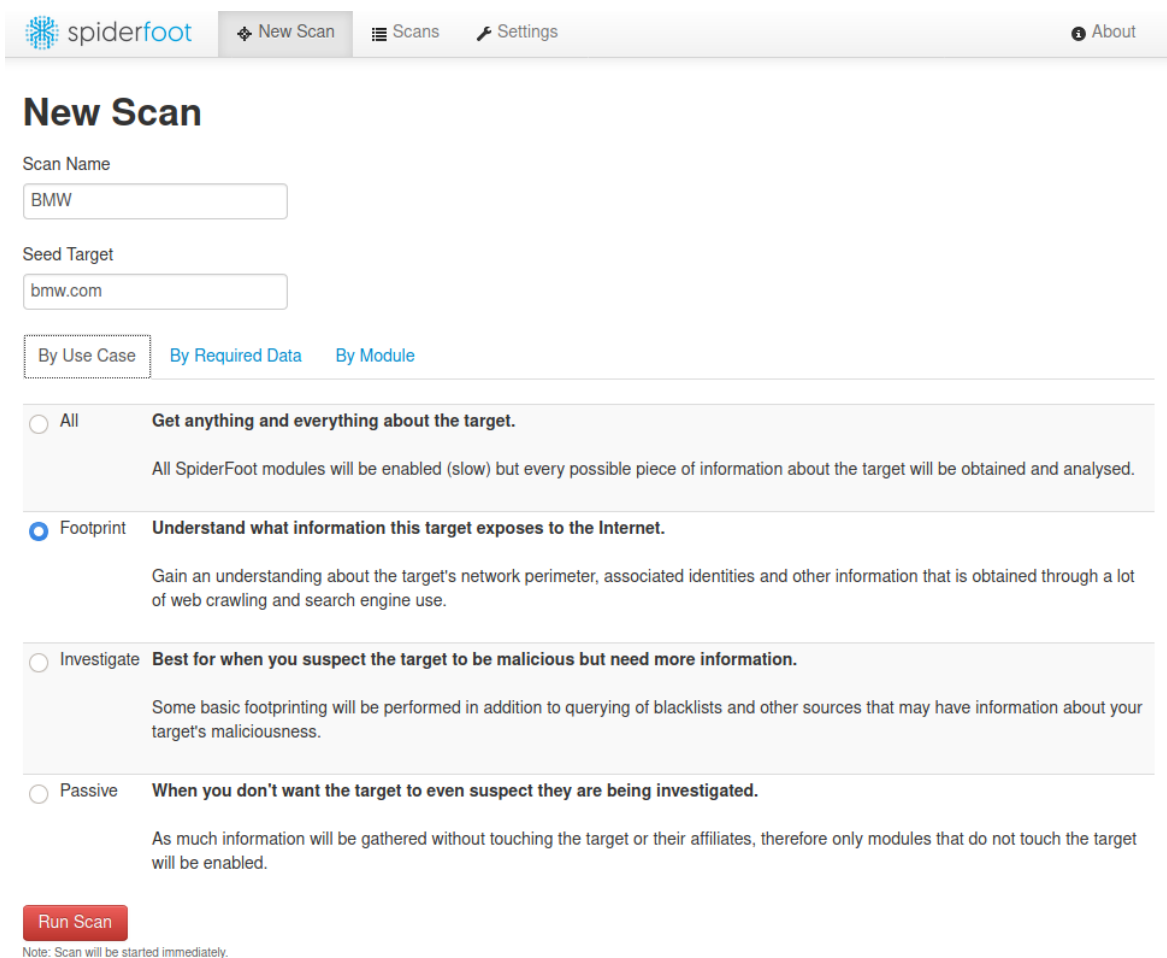
*****
Use SpiderFoot by starting your web browser of choice and
browse to http://localhost:5009
*****

[08/Oct/2021:04:43:35] ENGINE Listening for SIGTERM.
[08/Oct/2021:04:43:35] ENGINE Listening for SIGHUP.
[08/Oct/2021:04:43:35] ENGINE Listening for SIGUSR1.
[08/Oct/2021:04:43:35] ENGINE Bus STARTING
CherryPy Checker:
The use of 'localhost' as a socket host can cause problems on newer systems, since 'localhost' can map
to either an IPv4 or an IPv6 address. You should use '127.0.0.1' or ':::1' instead.

[08/Oct/2021:04:43:35] ENGINE Started monitor thread '_TimeoutMonitor'.
[08/Oct/2021:04:43:35] ENGINE Serving on http://localhost:5009
[08/Oct/2021:04:43:35] ENGINE Bus STARTED
```



Para iniciar un escaneo pinchamos en el menú ***New Scan*** y tendremos un formulario donde indicamos el *seed target* sobre el que queremos realizar la búsqueda y el motivo del escaneo.



spiderfoot New Scan Scans Settings About

New Scan

Scan Name
BMW

Seed Target
bmw.com

By Use Case By Required Data By Module

☐ All **Get anything and everything about the target.**
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

☒ Footprint **Understand what information this target exposes to the Internet.**
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

☐ Investigate **Best for when you suspect the target to be malicious but need more information.**
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

☐ Passive **When you don't want the target to even suspect they are being investigated.**
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan

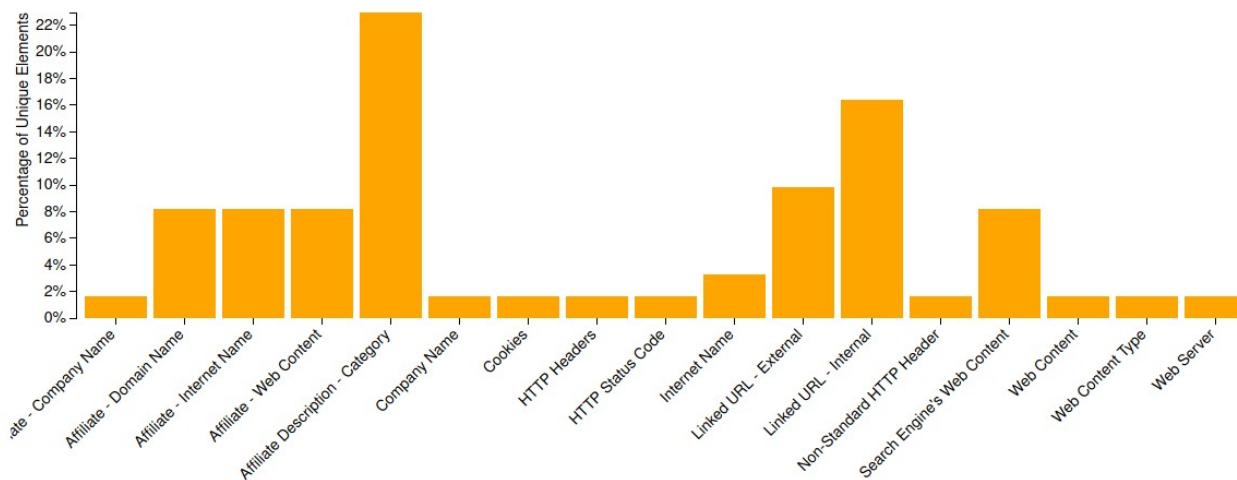
Note: Scan will be started immediately.

Pulsamos en **Run Scan** y esperamos a que comiencen a llegar los resultados al servicio web. En la terminal donde arrancamos *spiderfoot* podemos observar cómo se están realizando las peticiones y se obtienen las respuestas. El escaneo es lento y puede durar horas.

BMW

Status Browse Graph Scan Settings Log

Total 65 Unique 61 Status RUNNING Errors 7



Web oficial de spiderfoot

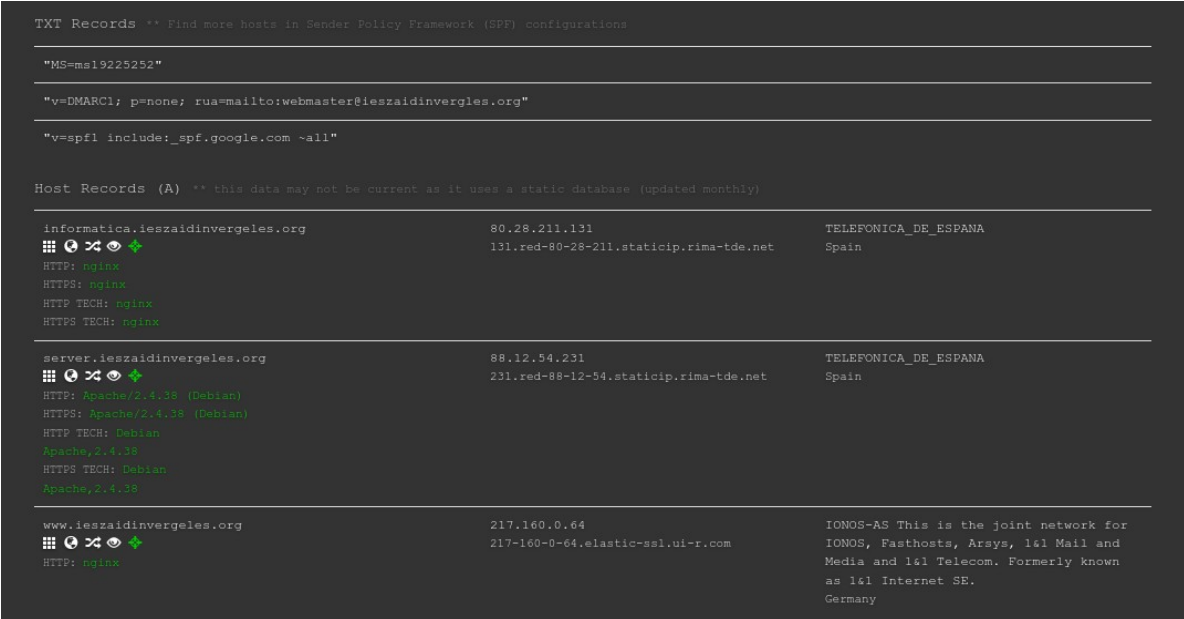
<https://www.spiderfoot.net/>

5. Herramientas visuales

Herramientas web

Además de las herramientas en línea de comandos que hemos utilizado, se pueden emplear páginas web que ofrecen esta información:

- www.domaintools.com. Ofrece servicios avanzados y de pago para Threat Intelligence.
- www.robtex.com. Esta web recopila información de IPs, DNS y AS de fuentes públicas y con una sola consulta.
- www.netcraft.com. Enfocada al ámbito empresarial para la protección de servicios. En la sección de recursos (*resources*) tiene herramientas para la búsqueda DNS, entre otras.
- www.virustotal.com. Enfocada a la detección de malware, tiene una sección de Intelligence donde utiliza Google y Facebook y una API para obtener información de todo tipo.
- <https://dnsdumpster.com/>. A través de una consulta sencilla de un dominio devuelve toda la información relativa al mismo: servidores de nombres, de correo, y otros hosts asociados, incluyendo información del software, por ejemplo tipo y versión de los servidores empleados. Quizás, lo más interesante sea que elabora un mapa de relación entre los diferentes equipos descubiertos.



The screenshot shows the results of a DNS query for the domain ieszaidinvergeles.org on the dnsdumpster.com website. It is divided into two sections: TXT Records and Host Records (A).

TXT Records (Find more hosts in Sender Policy Framework (SPF) configurations):

- "MS=ms19225252"
- "v=DMARC1; p=none; rua=mailto:webmaster@ieszaidinvergeles.org"
- "v=spf1 include:_spf.google.com ~all"

Host Records (A) (this data may not be current as it uses a static database (updated monthly)):

Host	IP	AS
informatica.ieszaidinvergeles.org	80.28.211.131	TELEFONICA_DE_ESPANA
131.red-80-28-211.staticip.rima-tde.net Spain		
HTTP: nginx		
HTTPS: nginx		
HTTP TECH: nginx		
HTTPS TECH: nginx		
server.ieszaidinvergeles.org	88.12.54.231	TELEFONICA_DE_ESPANA
231.red-88-12-54.staticip.rima-tde.net Spain		
HTTP: Apache/2.4.38 (Debian)		
HTTPS: Apache/2.4.38 (Debian)		
HTTP TECH: Debian		
Apache/2.4.38		
HTTPS TECH: Debian		
Apache/2.4.38		
www.ieszaidinvergeles.org	217.160.0.64	IONOS-AS This is the joint network for
217-160-0-64.elastic-ssl.ui-r.com IONOS, Fasthosts, Arsys, 1&1 Mail and		
Media and 1&1 Telecom. Formerly known		
as 1&1 Internet SE.		
Germany		

Ilustración 8: Resultados de la sección host records obtenidos para el dominio ieszaidinvergeles.org en dnsdumpster.com

Ejercicio propuesto

Explora las herramientas visuales presentadas en este epígrafe y compara los resultados obtenidos en el caso práctico.

Transformadas de Maltego

También es posible emplear las **transformadas de Maltego** para obtener información sobre DNS.

- *DNS from Domain > Other transforms > Domain using MX (mail server)*. Transformada encargada de obtener los servidores de correo asociados al dominio.
- *DNS from Domain > Other transforms > Domain using NS (name server)*. Transformada para obtener los servidores de nombres asociados al dominio.
- Se selecciona el conjunto de servidores obtenidos (MX y NS) y se ejecuta *Resolve IP* sobre ellos.
- Se vuelven a agrupar, esta vez sobre las direcciones IP y se ejecuta *Resolve IP > IP owner detail*.

Una vez se obtiene información básica se puede obtener más información con otras transformadas:

- *Other transforms > To website where IP appear*. Se realizan búsquedas por las direcciones IP en los principales buscadores.

6. Bibliografía

Recursos y enlaces utilizados para elaborar el documento.

- Pentesting con Kali. Silver Edition (3ª Edición). Pablo González et al. Ed. 0xWORD (2020).
- Ethical Hacking (2ª Edición). Pablo González. Ed. 0xWORD (2020).
- Guía de Seguridad en servicios DNS. INCIBE 2014. <https://www.incibe-cert.es/blog/guia-dns>
- Guía de implantación y buenas prácticas de DNSSEC. INCIBE 2018. <https://www.incibe-cert.es/guias-y-estudios/guias/guia-implantacion-y-buenas-practicas-dnssec>
- DNS Cache Poisoning Attack. Dan Kaminsky. <https://youtu.be/7Pp72gUYx00>
- La vulnerabilidad de DNS de Dan Kaminsky. Gabriel Verdejo. https://www.cs.upc.edu/~gabriel/files/DNS_Kaminsky.pdf
- Resurrections of DNS Cache Poisoning Attack with Side Channels. ArsTechnia 2021. <https://arstechnica.com/gadgets/2021/11/dan-kaminskys-dns-cache-poisoning-attack-is-back-from-the-dead-again/>