2025

2.1-Footprinting con WHOIS

PRACTICA 2

IZAN NAVARRO LUJAN

INDICE

1- Introducción:

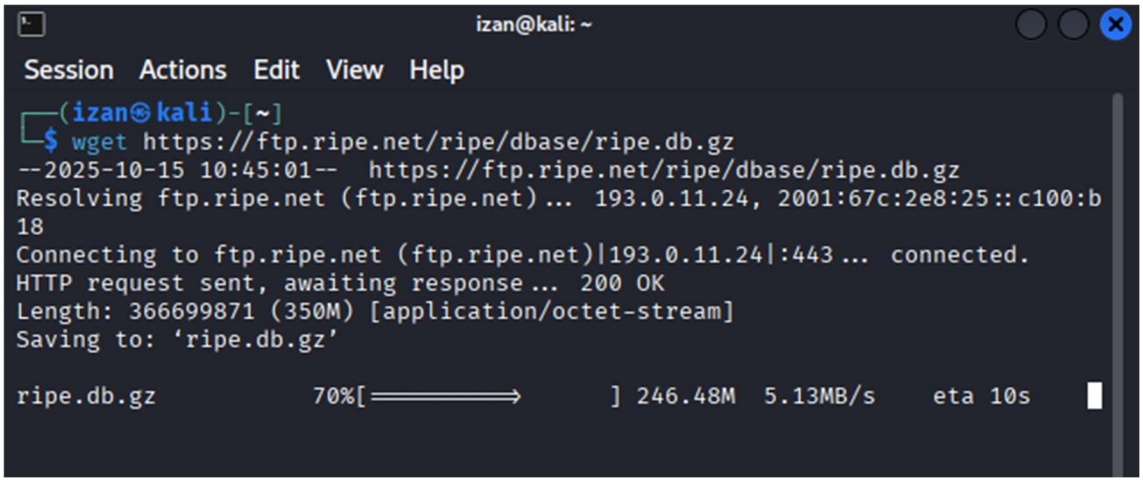
El objetivo de esta práctica es que el alumno conozca las herramientas whois y cómo utilizarla en la fase de footprinting para recabar información de fuentes públicas sobre el propietario de un dominio o el rango de redes usado por una organización.

WHOIS es un protocolo de aplicación que utiliza el puerto 43/TCP y que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet. Las consultas WHOIS se han realizado tradicionalmente usando una interfaz de línea de comandos, pero actualmente existen multitud de páginas web que permiten realizar estas consultas. Estas páginas siguen dependiendo internamente del protocolo WHOIS para conectar a un servidor WHOIS y hacer las peticiones. Los clientes de línea de comandos siguen siendo muy usados por los administradores de sistemas.

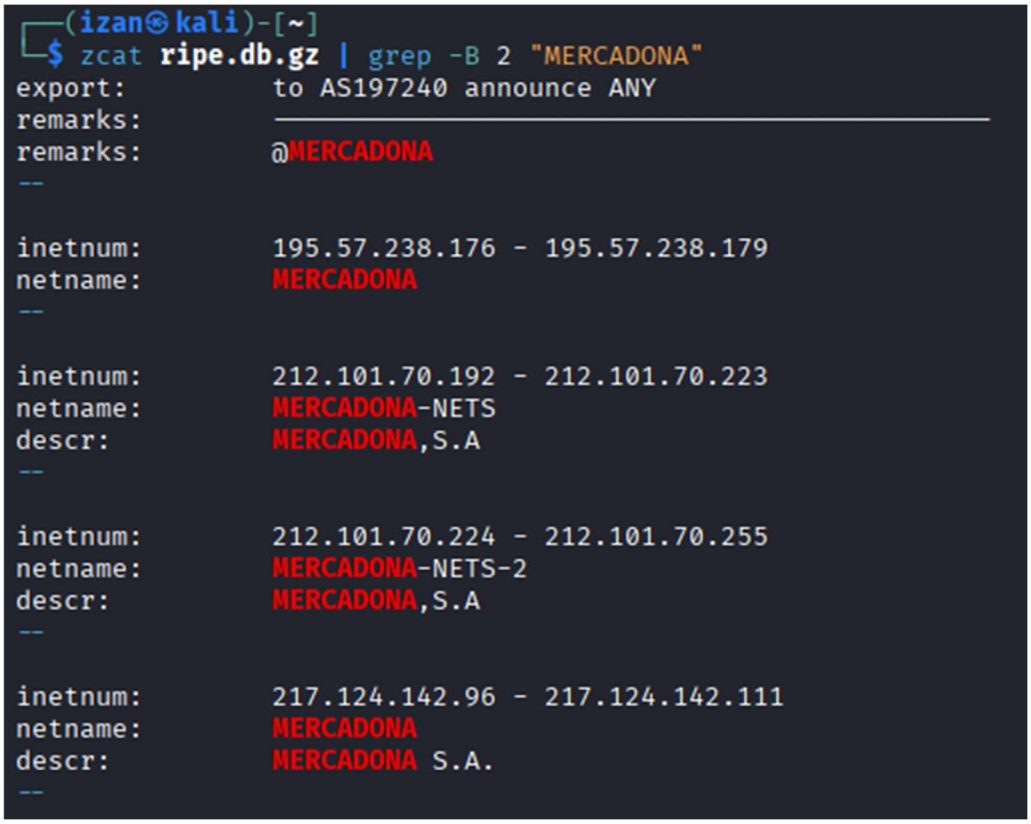
En esta práctica vamos a simular el proceso de footprinting de una determinada compañía objetivo a la que queremos descubrir sus redes IP. Este proceso es el que haríamos como pentesters en una auditoría de caja blanca contratada por la empresa o bien el proceso que seguiría un ciberdelincuente que se ha marcado como objetivo una organización por los beneficios que tiene en un determinado sector.

2- Ejercicio 1

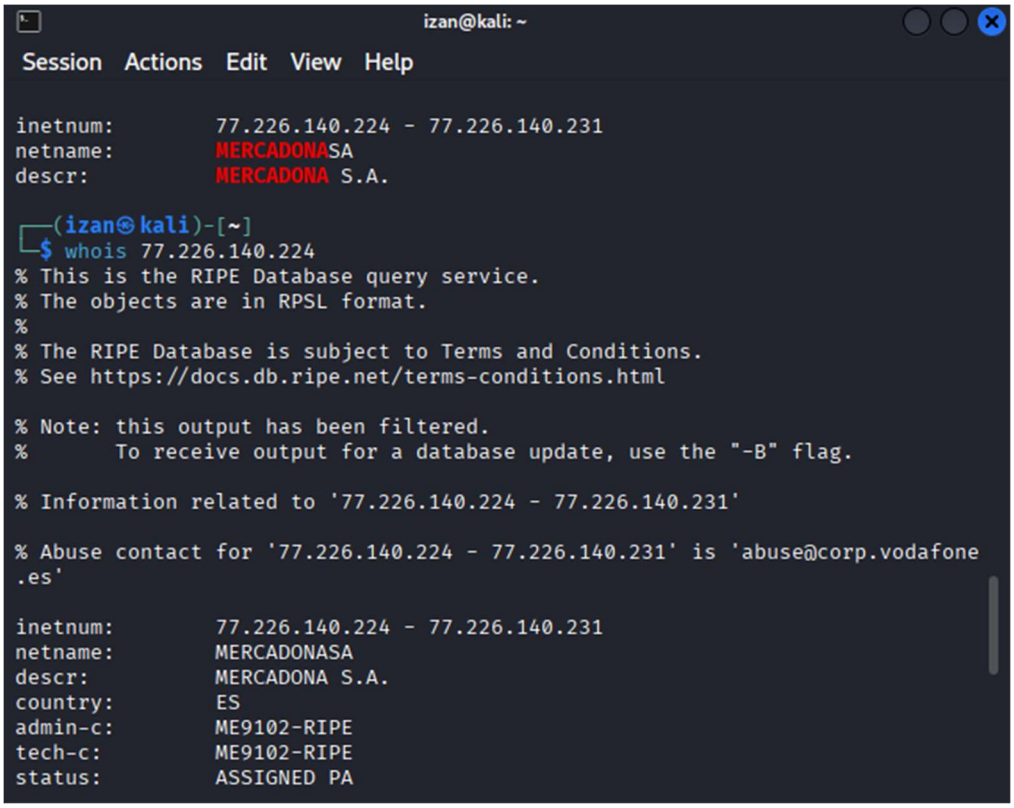
-Comando para extraer la BBDD ripe de la web proporcionada mediante “wget”:



- Buscar “Mercadona” dentro de la BBDD ripe y mostrar las 2 lineas anteriores:

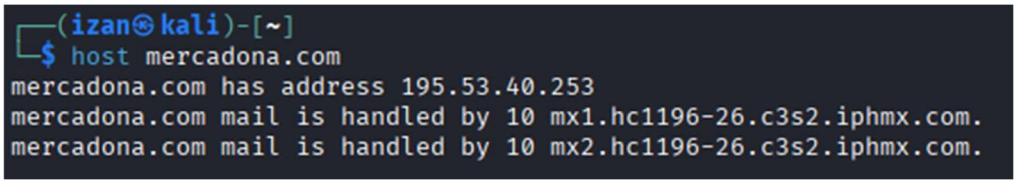


- Verifico un inetnum proporcionado por la bbdd ripe mediante el comando “whois”:

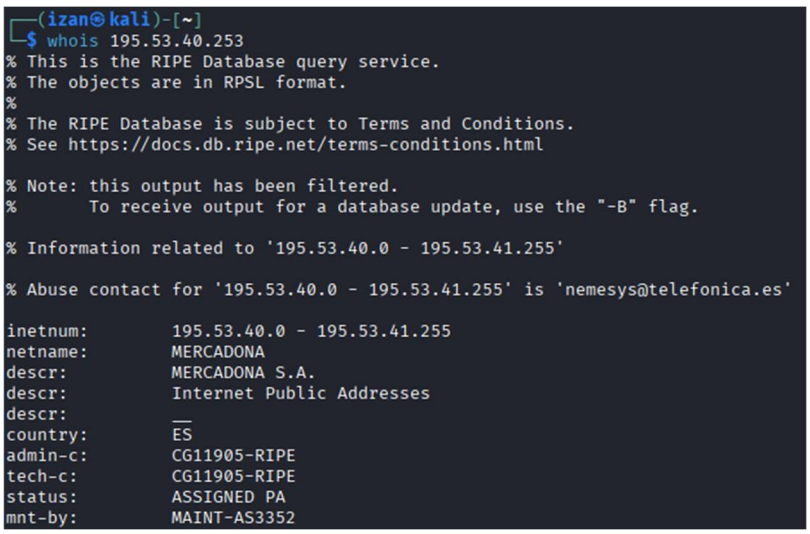


3- Ejercicio 2

- Averiguar la dirección de Servidores Web de “Mercadona.com”:



- Verificación de la IP obtenida mediante “Whois”:



Sí coincide con los rangos extraídos del ejercicio 1.

Si tratásemos con empresas con servicios como **CDN, Cloudflare, AWS en la nube**, entonces puede NO COINCIDIR porque usan proveedores externos

4- Ejercicio 3

-Búsqueda de servidores de correo (registro MX) mediante DNS con el comando “nslookup -type=MX (organización)”.

```
┌──(izan㉿kali)-[~]
└─$ nslookup -type=MX mercadona.com
Server:         100.100.1.1
Address:        100.100.1.1#53

Non-authoritative answer:
mercadona.com   mail exchanger = 10 mx2.hc1196-26.c3s2.iphmx.com.
mercadona.com   mail exchanger = 10 mx1.hc1196-26.c3s2.iphmx.com.

Authoritative answers can be found from:
```

- Obtención de IP de los “mx” mediante HOST:

```
┌──(izan㉿kali)-[~]
└─$ host mx1.hc1196-26.c3c2.iphmx.com
Host mx1.hc1196-26.c3c2.iphmx.com not found: 3(NXDOMAIN)
```

```
┌──(izan㉿kali)-[~]
└─$ dig mx2.hc1196-26.c3c2.iphmx.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> mx2.hc1196-26.c3c2.iphmx.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 44412
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 818d802d860e18d60100000068efb920faf5281b6cdf88dd (good)
;; QUESTION SECTION:
;mx2.hc1196-26.c3c2.iphmx.com.  IN      A

;; AUTHORITY SECTION:
iphmx.com.              3600    IN      SOA     ns1-93.akam.net. stbu-hostmas
ter\@cisco.com. 1760534265 3600 900 2419200 3600

;; Query time: 63 msec
;; SERVER: 100.100.1.1#53(100.100.1.1) (UDP)
;; WHEN: Wed Oct 15 11:09:22 EDT 2025
;; MSG SIZE  rcvd: 167
```

Significa que ese registro **MX existe**, pero el **nombre de host que aparece no tiene una IP asociada (registro A o AAAA)** en el DNS.

Como podemos apreciar, este dominio usa proveedores externos como es el caso de “akam.net”.

También podría darse el caso que el dominio redirija el correo a otro subdominio o a otro dominio interno que no está visible públicamente.

-Consulta de los registros TXT de la organización:

```
┌──(izan㉿kali)-[~]
└─$ nslookup -type=TXT mercadona.com
;; Truncated, retrying in TCP mode.
Server:         100.100.1.1
Address:        100.100.1.1#53

Non-authoritative answer:
mercadona.com   text = "yahoo-verification-key=F0jizlkjAphLWL90i93h6CncVO1o0z
0YUe1qIvPqqko="
mercadona.com   text = "MS=ms15589025"
mercadona.com   text = "Lb5z8z0wJ+h4fDTNGgK+ZD89/s5SgvAMXevUn/Wk9knFsKvnh5a5e
4FCi8JRSQBippGlYm/LHmCYdQFtiRYH9g=="
mercadona.com   text = "MS=ms95143477"
mercadona.com   text = "MS=ms40717057"
mercadona.com   text = "atlassian-domain-verification=a6W57an/bQEt37FKZ7H5eKW
S4MBUeSBwL9AcOoUyvO6n7z4sV3F94CXESOXc9Q8U"
mercadona.com   text = "openai-domain-verification=dv-KUXCTS0iI9lP8jVuWxZhvuD
r"
mercadona.com   text = "webexdomainverification.4C675B8917F0B136E053AB06FC0A3
F65=d2842f8d-291d-44b9-ad78-94aeec967fc7"
mercadona.com   text = "atlassian-domain-verification=hvVtneTaG701A0XGwc9otDZ
U9EURkStXsI59IVGQzP1GNVpqqjhYa693L/C5oBFJ"
mercadona.com   text = "v=spf1 mx include:spf.mercadona.es -all"
mercadona.com   text = "teamviewer-sso-verification=cbdaf292327843f6824bdbcee
cce6fd9"
mercadona.com   text = "adobe-idp-site-verification=c29ca8c0f6ce2ade12dd965f9
217c1678293486ec5a0718368157d7029d77d97"
mercadona.com   text = "google-site-verification=7mSD7qq8VxOgAOUUoVG8NhuYb8k0
rXk9WLKKvy3fM1s"
mercadona.com   text = "google-site-verification=uhxloKx3IH2Bw3ZCAZgyRcekge8W
```

El registro que empieza con v=spf1 es un **registro SPF (Sender Policy Framework)**.
Este tipo de registro DNS se utiliza para **indicar qué servidores están autorizados a enviar correos electrónicos** en nombre de un dominio, con el objetivo de prevenir el **spoofing** o suplantación de identidad en el correo electrónico.

```
mercadona.com   text = "v=spf1 mx include:spf.mercadona.es -all"
```

· v=spf1 → Indica la versión del protocolo SPF.

· mx → Autoriza a los servidores de correo definidos en los registros **MX** del dominio mercadona.com a enviar correo electrónico legítimo.

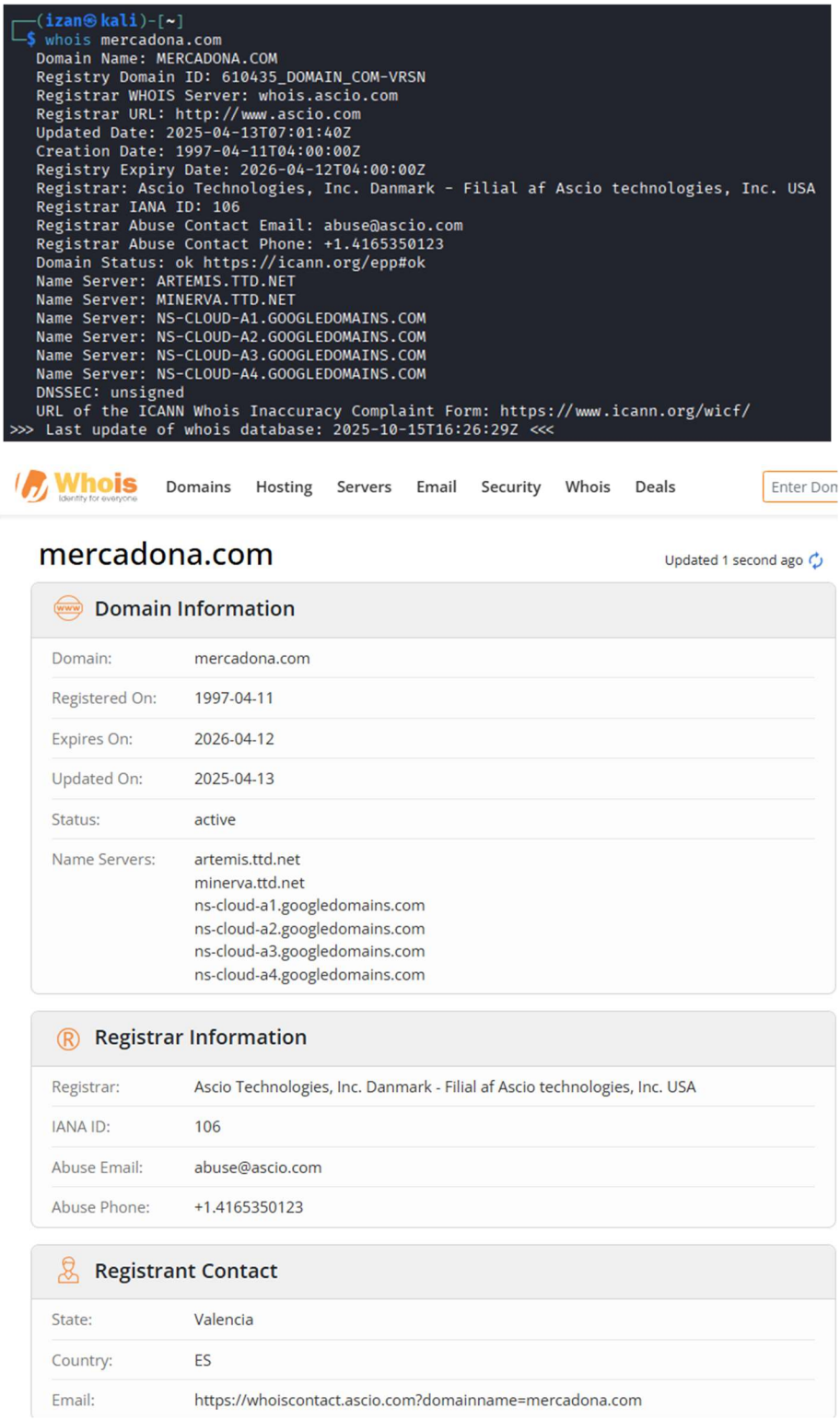
· include:spf.mercadona.es → Permite también el envío desde los servidores que estén definidos en el registro SPF del subdominio spf.mercadona.es.

· -all → Establece una política estricta: **solo** los servidores mencionados (directamente o incluidos) pueden enviar correo.
Cualquier otro servidor no listado será rechazado por los receptores.

Tras comprobar los registros MX del dominio y las IPs que incluyen, **se verifica** que las direcciones IP de los servidores de correo coinciden con las que autoriza el registro SPF, ya que **el parámetro mx incluye explícitamente a los servidores de correo principales del dominio**.

-Comparación de los resultados que obtienes con el comando whois por consola y los que puedes obtener con cualquier servicio whois vía web

Vía Comandos:



El comando whois en consola ofrece información más técnica, directa y sin formato, mientras que las páginas web WHOIS presentan los mismos datos de forma más amigable y complementada con información adicional (como localización del servidor,

gráficos o registros históricos).
En ambos casos, la información principal del dominio mercadona.com coincide, ya que procede de la misma base de datos pública WHOIS.