Reconocimiento DNS de una empresa

17 de Abril del 2024

Jose Almirón López

Índice

Descripción del objetivo

Audi es una empresa alemana de renombre mundial, especializada en la fabricación y venta de vehículos de alta calidad. La compañía es una subsidiaria de Volkswagen AG y es conocida por su enfoque en la innovación, el diseño y la tecnología de vanguardia.

La empresa fue fundada en 1909 por August Horch, y su nombre actual se adoptó en 1910. Desde entonces, Audi ha evolucionado hasta convertirse en un líder global en la industria automotriz, con una gama de productos que incluyen sedanes, coupés, descapotables y vehículos utilitarios deportivos (SUV).

Audi se enorgullece de su compromiso con la calidad y la ingeniería de precisión. La empresa utiliza una variedad de tecnologías avanzadas en sus vehículos, como sistemas de propulsión híbridos enchufables y eléctricos, sistemas de conducción autónoma y sistemas de información y entretenimiento de última generación.

La empresa ofrece una amplia gama de servicios a sus clientes, incluyendo servicios de mantenimiento y reparación, financiamiento y leasing, y programas de fidelidad y beneficios. Audi también tiene una fuerte presencia en las carreras de automovilismo, con equipos que compiten en las series de carreras más prestigiosas del mundo.

Dominios TLD (Top Level Domain)

Usaremos el comando '**whois**' para obtener información básica del dominio, como datos de contacto, registrador y fechas importantes como creación y expiración, además de los servidores DNS asociados opcionalmente.

```
└─$ whois audi.com
   Domain Name: AUDI.COM
   Registry Domain ID: 2530258_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.1api.net
   Registrar URL: http://www.1api.net
   Updated Date: 2024-02-09T08:01:40Z
   Creation Date: 1995-02-07T05:00:00Z
   Registry Expiry Date: 2025-02-08T05:00:00Z
   Registrar: 1API GmbH
   Registrar IANA ID: 1387
   Registrar Abuse Contact Email: abuse@1api.net
   Registrar Abuse Contact Phone: +49.68949396850
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: NS2.AUDI.DE
   Name Server: NS5.XC-NS.DE
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-20T12:17:28Z <<<

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

Domain Name: AUDI.COM
Registry Domain ID: 2530258_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.1api.net
Registrar URL: http://www.1api.net
Updated Date: 2021-01-27T09:21:24Z
Creation Date: 1995-02-07T05:00:00Z
Registrar Registration Expiration Date: 2025-02-08T05:00:00Z
Registrar: 1API GmbH
Registrar IANA ID: 1387
Registrar Abuse Contact Email: abuse@1api.net
Registrar Abuse Contact Phone: +49.68949396x850
Reseller: HEXONET GmbH http://www.hexonet.net/
Domain Status: clientDeleteProhibited - http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited - http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
```

```
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: DE
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: contact via https://www.1api.net/send-message/audi.com/registrant
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: contact via https://www.1api.net/send-message/audi.com/admin
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: contact via https://www.1api.net/send-message/audi.com/tech
Name Server: ns2.audi.de
Name Server: ns5.xc-ns.de
DNSSEC: unsigned
```

Entre las entradas destacadas se encuentra el estado del dominio (**Domain status**), indicando que no se puede borrar para evitar la pérdida accidental, y el permiso de transferencia para

prevenir el hackeo del dominio. Además, se observa que el dominio cuenta con dos servidores de nombres (**name server**), uno de los cuales es externo a Audi. Respecto a la privacidad, los datos personales restantes están ocultos

En el siguiente paso, emplearemos el comando **'dnsrecon'** para identificar otros dominios de primer nivel que contengan una cadena específica en su nombre de dominio.

```
└─$ dnsrecon -t tld -d audi
[*] tld: Performing TLD Brute force Enumeration against audi...
[*] The operation could take up to: 00:08:13
[+]      A audi.cymru 64.190.63.222
[+]      A audi.live 198.148.126.56
[+]      A site.my.box 34.232.152.68
[+]      A site.my.box 52.20.143.163
[+]      A site.my.box 3.221.134.22
[+]      A site.my.box 18.215.42.147
[+]      A audi.barcelona 31.214.178.54
[+]      A audi.krd 104.21.75.33
[+]      A audi.krd 172.67.210.154
[+]      AAAA audi.krd 2606:4700:3035::ac43:d29a
[+]      AAAA audi.krd 2606:4700:3030::6815:4b21
[+]      A audi.paris 185.43.62.20
[+]      A audi.yokohama 150.95.255.38
[+]      A audi.stream 213.155.69.214
[+]      AAAA audi.stream 2001:780:205:0:213:155:69:214
[+]      A audi.link 44.227.76.166
[+]      A audi.link 44.227.65.245
[+]      A audi.kaufen 192.166.192.19
[+]      A 77980.bodis.com 199.59.243.225
[+]      A audi.video 46.23.69.44
[+]      A audi.fashion 15.197.162.184
[+]      A audi.yoga 3.33.130.190
[+]      A audi.yoga 15.197.148.33
[+]      A audi.xyz 76.223.54.146
[+]      A audi.xyz 13.248.169.48
[+]      A audi.vegas 15.197.148.33
[+]      A audi.vegas 3.33.130.190
[+]      A audi.fun 98.124.224.17
[+]      A audi.ceo 45.87.158.7
[+]      A audi.music 127.0.53.53
[+]      A audi.tokyo 150.95.255.38
[+]      A audi.one 192.64.119.80
[+]      A audi.arab 127.0.53.53
```

```
[+]       A audi.xn--ngbrx 127.0.53.53
[+]       A audi.bar 91.189.114.22
[+]       A audi.nyc 52.33.207.7
[+]       A audi.nyc 44.230.85.241
[+]       A audi.org 3.33.130.190
[+]       A audi.org 15.197.148.33
[+]       A audi.sexy 109.234.111.119
[+]       A audi.jobs 143.164.101.227
[+]       A audi.ovh 144.217.153.176
[+]       A audi.global 3.64.163.50
[+]       A audi.xn--kput3i 47.57.12.156
[+]       A audi.swiss 37.153.81.16
[+]       A audi.com 143.164.101.69
[+]       A audi.wales 64.190.63.222
[+]       A audi.xn--mxtq1m 127.0.53.53
[+]       A audi.party 3.64.163.50
[+]       A audi.haus 199.83.62.140
[+]       A audi.motorcycles 3.64.163.50
[+]       A audi.ruhr 217.160.0.61
[+]       AAAA audi.ruhr 2001:8d8:100f:f000::290
[+]       A audi.ing 64.190.63.222
[+]       A audi.cyou 172.67.197.153
[+]       A audi.cyou 104.21.36.169
[+]       AAAA audi.cyou 2606:4700:3033::6815:24a9
[+]       A audi.tel 195.253.75.107
[+]       A audi.tech 76.223.54.146
[+]       A audi.tech 13.248.169.48
[+]       A audi.cat 216.185.152.151
[+]       A audi.miami 3.33.130.190
[+]       A audi.miami 15.197.148.33
[+]       A audi.cam 162.144.4.132
[+]       A audi.xn--vuq861b 45.120.243.27
[+]       AAAA audi.xn--vuq861b 2402:7d80:fffc::27
[+]       A audi.best 104.21.24.11
[+]       A audi.best 172.67.215.72
[+]       AAAA audi.best 2606:4700:3033::6815:180b
[+]       AAAA audi.best 2606:4700:3037::ac43:d748
[+]       A audi.asia 143.164.100.183
[+]       A audi.click 217.160.0.171
[+]       AAAA audi.click 2001:8d8:100f:f000::214
[+]       A audi.melbourne 202.124.241.178
[+]       A audi.monster 172.67.182.203
[+]       A audi.monster 104.21.32.42
[+]       AAAA audi.monster 2606:4700:3033::ac43:b6cb
[+]       AAAA audi.monster 2606:4700:3030::6815:202a
```

```
[+]       A audi.moscow 194.58.112.165
[+]       AAAA audi.moscow 2a00:f940:4::152
[+]       A audi.alsace 143.164.101.227
[+]       A audi.dev 217.70.184.38
[+]       A audi.repair 109.234.111.119
[+]       A audi.ac 143.164.101.227
[+]       A audi.af 143.164.101.227
[+]       A audi.ag 143.164.101.227
[+]       A audi.ai 143.164.101.227
[+]       A audi.al 212.183.88.29
[+]       A audi.al 212.183.88.30
[+]       A audi.am 143.164.101.67
[+]       A audi.as 143.164.101.227
[+]       A audi.au 165.160.13.20
[+]       A audi.au 165.160.15.20
[+]       A audi.at 212.183.88.30
[+]       A audi.at 212.183.88.29
[+]       A audi.az 104.21.30.171
[+]       A audi.az 172.67.173.119
[+]       AAAA audi.az 2606:4700:3035::ac43:ad77
[+]       AAAA audi.az 2606:4700:3035::6815:1eab
[+]       A audi.ba 212.183.88.30
[+]       A audi.ba 212.183.88.29
[+]       A audi.bb 143.164.101.173
[+]       A audi.be 193.53.139.84
[+]       A audi.bg 212.183.88.29
[+]       A audi.bg 212.183.88.30
[+]       A audi.bi 143.164.101.227
[+]       A audi.bo 143.164.101.67
[+]       A audi.bs 143.164.101.227
[+]       A audi.by 143.164.101.67
[+]       A audi.ca 143.164.101.67
[+]       A audi.cc 3.33.152.147
[+]       A audi.cc 15.197.142.173
[+]       A audi.bz 143.164.101.227
[+]       A audi.cd 143.164.101.227
[+]       A audi.cg 143.164.101.227
[+]       A audi.cf 143.164.101.227
[+]       A audi.ch 143.164.101.67
[+]       A audi.ci 143.164.101.227
[+]       A audi.cl 212.183.88.29
[+]       A audi.cl 212.183.88.30
[+]       A audi.cm 143.164.101.227
[+]       A audi.co 212.183.88.29
[+]       A audi.co 212.183.88.30
```

```
[+]       A audi.cu 143.164.101.227
[+]       A audi.cw 184.28.224.43
[+]       A audi.cx 143.164.101.227
[+]       A audi.cz 212.183.88.30
[+]       A audi.cz 212.183.88.29
[+]       A audi.de 143.164.101.67
[+]       A audi.dj 143.164.101.227
[+]       A audi.dk 143.164.101.67
[+]       A audi.dm 143.164.101.227
[+]       A audi.ee 143.164.101.67
[+]       A audi.es 143.164.101.67
[+]       A audi.fi 143.164.101.67
[+]       A audi.fm 143.164.101.227
[+]       A audi.fr 143.164.101.67
[+]       A audi.gd 143.164.101.227
[+]       A audi.gf 143.164.101.67
[+]       A audi.ge 91.212.213.32
[+]       A audi.gg 143.164.101.227
[+]       A audi.cn 123.56.6.133
[+]       A audi.gp 143.164.101.67
[+]       A audi.gr 143.164.101.67
[+]       A audi.gs 143.164.101.227
[+]       A audi.gy 143.164.101.227
[+]       A audi.hn 143.164.101.67
[+]       A audi.hr 212.183.88.30
[+]       A audi.hr 212.183.88.29
[+]       A audi.gm 143.164.101.227
[+]       A audi.hu 195.228.75.127
[+]       A audi.ie 143.164.101.67
[+]       A audi.im 143.164.101.227
[+]       A audi.in 143.164.101.67
[+]       A audi.io 143.164.101.227
[+]       A audi.is 143.164.101.67
[+]       A audi.it 143.164.101.67
[+]       A audi.ir 143.164.101.227
[+]       A audi.je 143.164.101.227
[+]       A audi.jo 143.164.101.227
[+]       A audi.kg 143.164.101.227
[+]       A audi.hm 143.164.101.227
[+]       A audi.ki 143.164.101.227
[+]       A audi.kn 143.164.101.227
[+]       A audi.la 143.164.101.227
[+]       A audi.ky 107.180.100.15
[+]       A audi.lc 143.164.101.67
[+]       A audi.kz 194.39.65.2
```

```
[+]       AAAA audi.kz 2a00:5da0:1000::151
[+]       A audi.lk 143.164.101.67
[+]       A audi.lt 143.164.101.67
[+]       A audi.lu 143.164.101.67
[+]       A audi.jp 52.198.232.1
[+]       A audi.ly 143.164.101.227
[+]       A audi.lv 143.164.101.67
[+]       A audi.ma 143.164.101.67
[+]       A audi.md 143.164.101.67
[+]       A audi.mg 143.164.101.227
[+]       A audi.me 212.183.88.29
[+]       A audi.me 212.183.88.30
[+]       A audi.mk 212.183.88.30
[+]       A audi.mk 212.183.88.29
[+]       A audi.mn 143.164.101.227
[+]       A audi.ml 143.164.101.227
[+]       A audi.ms 143.164.101.227
[+]       A audi.mq 143.164.101.227
[+]       A audi.mu 143.164.101.227
[+]       A audi.mp 143.164.101.227
[+]       A audi.my 185.116.31.150
[+]       A audi.mw 162.210.102.212
[+]       A audi.mx 143.164.100.200
[+]       A audi.nf 143.164.101.227
[+]       A audi.no 143.164.101.67
[+]       A audi.nl 143.164.101.67
[+]       A audi.ng 143.164.101.227
[+]       A audi.mv 143.164.101.227
[+]       A audi.ph 143.164.101.67
[+]       A audi.pk 143.164.101.67
[+]       A audi.pl 143.164.101.67
[+]       A audi.pm 143.164.101.227
[+]       A audi.pn 143.164.101.227
[+]       A audi.ps 143.164.101.227
[+]       A audi.pt 212.183.88.30
[+]       A audi.pt 212.183.88.29
[+]       A audi.nr 143.164.101.227
[+]       A audi.pw 143.164.101.227
[+]       A audi.pr 143.164.101.227
[+]       A audi.re 213.186.33.5
[+]       A audi.rs 212.183.88.29
[+]       A audi.rs 212.183.88.30
[+]       A audi.ro 212.183.88.29
[+]       A audi.ro 212.183.88.30
[+]       A audi.ru 143.164.101.67
```

```
[+]       A audi.sa 143.164.101.227
[+]       A audi.sc 143.164.101.227
[+]       A audi.rw 143.164.101.227
[+]       A audi.sd 143.164.101.227
[+]       A audi.si 212.183.88.30
[+]       A audi.si 212.183.88.29
[+]       A audi.se 143.164.101.67
[+]       A audi.sh 143.164.101.227
[+]       A audi.sk 212.183.88.30
[+]       A audi.sk 212.183.88.29
[+]       A audi.so 143.164.101.227
[+]       A audi.sl 143.164.101.227
[+]       A audi.sn 143.164.101.227
[+]       A audi.sr 143.164.101.227
[+]       A audi.td 143.164.101.227
[+]       A audi.tf 143.164.101.227
[+]       A audi.st 143.164.101.227
[+]       A audi.tj 143.164.101.227
[+]       A audi.tl 143.164.101.227
[+]       A audi.tk 143.164.101.227
[+]       A audi.tc 143.164.101.227
[+]       A audi.to 143.164.101.227
[+]       A audi.tn 143.164.101.173
[+]       A audi.tm 143.164.101.227
[+]       A audi.tg 143.164.101.227
[+]       A audi.tt 143.164.101.67
[+]       A audi.tv 143.164.101.227
[+]       A audi.ug 143.164.101.227
[+]       A audi.uk 3.33.139.32
[+]       A audi.us 67.199.248.13
[+]       A audi.vc 143.164.101.227
[+]       A audi.uz 80.80.218.172
[+]       A audi.tw 61.221.12.104
[+]       A audi.vg 143.164.101.227
[+]       A audi.vu 143.164.101.227
[+]       A audi.ua 212.183.88.30
[+]       A audi.ua 212.183.88.29
[+]       A audi.vn 143.164.101.67
[+]       A audi.xn--node 188.93.95.11
[+]       A audi.fi.fit 3.64.163.50
[+]       A audi.la.tips 13.248.169.48
[+]       A audi.la.tips 76.223.54.146
[+]       A 77980.bodis.com 199.59.243.225
[+]       A audi.ls.mortgage 91.195.240.94
[+]       A audi.my.catering 72.52.179.175
```

```
[+]       A audi.pr.health 3.64.163.50
[+]       A audi.us.center 3.64.163.50
[+]       A audi.vc.whoswho 82.196.14.243
[+] 265 Records Found
```

Al intentar obtener información de uno de los dominios encontrados, como por ejemplo audi.es, no obtendremos los resultados esperados.

```
┌──(jose㉿kali)-[~]
└─$ whois audi.es
Este TLD no dispone de servidor whois, pero puede acceder a la base de datos de whois en
https://www.dominios.es/en
```

Esto ocurre porque el comando 'whois' no almacena la información de los registros regionales. Por lo tanto, debemos dirigirnos al sitio web del registrador oficial correspondiente, como en el caso de los dominios .es, que podemos encontrar en www.dominios.es. En mi caso no he obtenido ninguna ip

DATOS DEL TITULAR

Nombre del Dominio	audi.es
Estado	Activado
Identificador	184FA1D-ESNIC-F5
Titular	AUDI AG
Fecha de Alta	02-07-2001
Fecha de Caducidad	02-07-2024
Agente Registrador	1API

PERSONA DE CONTACTO ADMINISTRATIVO

Identificador	184FA1E-ESNIC-F5
Nombre	Kai Brandt

PERSONA DE CONTACTO TECNICO

Identificador	184FA1E-ESNIC-F5
Nombre	Kai Brandt

PERSONA DE CONTACTO DE FACTURACION

SERVIDORES DNS

Nombre Servidor	IP
ns2.audi.de	
ns5.xc-ns.de	

Una vez que hemos obtenido las direcciones IP, podemos avanzar en nuestra investigación consultándolas en la base de datos de RIPE. Sin embargo, reservaremos esta tarea para un apartado posterior. Por el momento, podemos verificar si obtenemos información utilizando el comando WHOIS con las otras direcciones de dominio.

```
┌──(jose@kali)-[~]
└─$ whois audi.fr
 %%
 %% This is the AFNIC Whois server.
 %%
 %% complete date format: YYYY-MM-DDThh:mm:ssZ
 %%
 %% Rights restricted by copyright.
%%                                                                                See
https://www.afnic.fr/en/domain-names-and-support/everything-there-is-to-know-about-domain-name
s/f  ind-a-domain-name-or-a-holder-using-whois/
 %%
 %%

 domain:                       audi.fr
 status:                       ACTIVE
 eppstatus:                    clientTransferProhibited
 hold:                         NO
 holder-c:                     GVFS34-FRNIC
 admin-c:                      SC5114-FRNIC
 tech-c:                       G768-FRNIC
 registrar:                    GANDI
 Expiry Date:                  2024-11-14T15:18:27Z
 created:                      2000-08-27T22:00:00Z
 last-update:                  2023-11-18T13:22:25.337459Z
 source:                       FRNIC

 nserver:                      ns-2-c.gandi.net
 nserver:                      ns-44-b.gandi.net
 nserver:                      ns-79-a.gandi.net
 source:                       FRNIC

 registrar:                    GANDI
 address:                      63-65 boulevard Massena
 address:                      75013 PARIS
 country:                      FR
 phone:                        +33.170377661
 fax-no:                       +33.143731851
```

```
e-mail:                         support@support.gandi.net
website:                        https://www.gandi.net/fr/tlds/fr/
anonymous:                      No
registered:                     2004-03-08T00:00:00Z
source:                         FRNIC

nic-hdl:                        GVFS34-FRNIC
type:                           ORGANIZATION
contact:                        VOLKSWAGEN GROUP FRANCE
address:                        11 avenue de Boursonne - B.P. 62
address:                        02601 Villers-Cotterets
country:                        FR
phone:                          +33.323735703
e-mail:                         d8fdbb0ca87ef55ce26f63511798aa24-1324835@contact.gandi.net
registrar:                      GANDI
changed:                        2022-04-08T16:17:03Z
anonymous:                      NO
obsoleted:                      NO
eppstatus:                      associated
eppstatus:                      active
eligstatus:                     not identified
reachstatus:                    not identified
source:                         FRNIC

nic-hdl:                        G768-FRNIC
type:                           ORGANIZATION
contact:                        GANDI
address:                        GANDI
address:                        63-65 Boulevard MASSENA
address:                        75013 Paris
country:                        FR
phone:                          +33.143737851
fax-no:                         +33.143731851
e-mail:                         noc@gandi.net
registrar:                      GANDI
changed:                        2024-04-20T12:42:45.582888Z
anonymous:                      NO
obsoleted:                      NO
eppstatus:                      associated
eppstatus:                      active
eligstatus:                     not identified
reachstatus:                    not identified
source:                         FRNIC

nic-hdl:                        SC5114-FRNIC
```

```
type:                           ORGANIZATION
contact:                        Shiva Communication
address:                        8 rue Lavoisier
address:                        75008 Paris
country:                        FR
phone:                          +33.663356254
fax-no:                         +33.141060936
e-mail:                         c649d1a9954afe1e11ee273fd3d8f72e-162274@contact.gandi.net
registrar:                      GANDI
changed:                        2021-08-28T16:34:50Z
anonymous:                      NO
obsoleted:                      NO
eppstatus:                      associated
eppstatus:                      active
eligstatus:                     not identified
reachstatus:                    not identified
source:                         FRNIC

>>> Last update of WHOIS database: 2024-04-21T12:20:26.58658Z <<<
```

Subdominios (DNS Bruting)

Para obtener los subdominios, podemos utilizar fuerza bruta mediante un diccionario para encontrar coincidencias. Estos subdominios se dividen en dos tipos:

- **Público**: publicados en internet y accesibles desde el exterior
- **Privados**: pertenecen a la red interna y se define en servidores

Ahora intentaremos obtener los datos de los subdominios de Audi utilizando el comando **dnsenum**. En la sección de fuerza bruta (brute forcing), podremos observar los subdominios encontrados.

```
└─$ dnsenum audi.com
dnsenum VERSION:1.2.6

-----   audi.com   -----


Host's addresses:
__________________
```

```
audi.com.                               3600     IN    A        143.164.101.69


Name Servers:
_____________

ns2.audi.de.                            260      IN    A        143.164.100.254
ns5.xc-ns.de.                           15495    IN    A        194.50.187.172


Mail (MX) Servers:
__________________

mg5.vw.com.                             300      IN    A        199.5.47.161
mg11.vw.com.                            300      IN    A        199.5.47.226
mg9.vw.com.                             300      IN    A        199.5.47.230
mg4.vw.com.                             300      IN    A        199.5.47.158
mg7.vw.com.                             300      IN    A        199.5.47.203
mg8.vw.com.                             300      IN    A        199.5.47.204
mg6.vw.com.                             300      IN    A        199.5.47.197
mg10.vw.com.                            300      IN    A        199.5.47.223
mg12.vw.com.                            300      IN    A        199.5.47.250


Trying Zone Transfers and getting Bind Versions:
________________________________________________

Use of uninitialized value $size in integer subtraction (-) at
/usr/share/perl5/Net/DNS/Resolver/Base.pm line 832.

Trying Zone Transfer for audi.com on ns5.xc-ns.de ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for audi.com on ns2.audi.de ...
AXFR record query failed: REFUSED


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

access.audi.com.                        3600     IN    A        199.5.50.33
access.audi.com.                        3600     IN    A        199.5.50.36
aco.audi.com.                           3600     IN    CNAME    dns.aco.webapps.audi.io.
```

```
 dns.aco.webapps.audi.io.                300       IN    CNAME
fp32e1.wpc.1eddbe.epsiloncdn.net.
 fp32e1.wpc.1eddbe.epsiloncdn.net.       3600      IN    CNAME    fp32e1.wpc.epsiloncdn.net.
 fp32e1.wpc.epsiloncdn.net.              3600      IN    A        192.229.202.87
 av.audi.com.                            3600      IN    A        199.5.50.38
 av.audi.com.                            3600      IN    A        199.5.50.35
 blog.audi.com.                          3600      IN    A        195.93.201.191
 communication.audi.com.                 3600      IN    A        161.71.33.242
 europe.audi.com.                        3600      IN    CNAME    www.audi.com.
 www.audi.com.                           282       IN    CNAME
fp31f8.wpc.1bfd67.iotacdn.net.
 fp31f8.wpc.1bfd67.iotacdn.net.          2931      IN    CNAME    fp31f8.wpc.iotacdn.net.
 fp31f8.wpc.iotacdn.net.                 510       IN    A        192.229.202.3
 extranet.audi.com.                      3600      IN    CNAME    dvinnie.vw.com.
 dvinnie.vw.com.                         300       IN    A        199.5.55.142
 mail.audi.com.                          3600      IN    A        13.111.18.27
 survey.audi.com.                        3600      IN    CNAME    external.umfrageonline.com.
 external.umfrageonline.com.             60        IN    A        34.241.212.106
 external.umfrageonline.com.             60        IN    A        52.210.148.238
 trends.audi.com.                        3600      IN    A        80.190.116.67
 www.audi.com.                           235       IN    CNAME
fp31f8.wpc.1bfd67.iotacdn.net.
 fp31f8.wpc.1bfd67.iotacdn.net.          2884      IN    CNAME    fp31f8.wpc.iotacdn.net.
 fp31f8.wpc.iotacdn.net.                 463       IN    A        192.229.202.3


 audi.com class C netranges:
 ___________________________

 13.111.18.0/24
 80.190.116.0/24
 143.164.101.0/24
 161.71.33.0/24
 195.93.201.0/24
 199.5.50.0/24


 Performing reverse lookup on 1536 ip addresses:
 ________________________________________________


 0 results out of 1536 IP addresses.
 Could not open audi.com_ips.txt file: Permission denied
```

Otro comando útil para intentar obtener una lista de subdominios es '**fierce**'. Esta herramienta está diseñada para buscar IPs y nombres de host contiguos a un dominio o subdominio específico

```
└─$ fierce --domain audi.com
NS: ns2.audi.de. ns5.xc-ns.de.
SOA: ns2.audi.de. (143.164.100.254)
Zone: failure
Wildcard: failure
Found: access.audi.com. (199.5.50.33)
Nearby:
 {'199.5.50.33': 'sip.audi.ca.',
 '199.5.50.34': 'webconf.electrifyamerica.com.',
 '199.5.50.35': 'av.vw.com.',
 '199.5.50.36': 'access.gtb-procurement.com.',
 '199.5.50.37': 'webconf.gtb-procurement.com.',
 '199.5.50.38': 'av.volkswagen.ca.'}
Found: akamai.audi.com. (143.164.100.213)
Found: av.audi.com. (199.5.50.35)
Nearby:
 {'199.5.50.39': 'access.audi.ca.'}
Found: blog.audi.com. (195.93.201.191)
Nearby:
 {'195.93.201.193': 'secure.gil.kundenserver42.de.'}
Found: commerce.audi.com. (207.173.193.19)
Found: contact.audi.com. (161.71.33.242)
Nearby:
 {'161.71.33.237': 'gx237.mta.exacttarget.com.',
 '161.71.33.238': 'gx238.mta.exacttarget.com.',
 '161.71.33.239': 'gx239.mta.exacttarget.com.',
 '161.71.33.240': 'gx240.mta.exacttarget.com.',
 '161.71.33.241': 'gx241.mta.exacttarget.com.',
 '161.71.33.242': 'reply.s50.exacttarget.com.',
 '161.71.33.243': 'manage.s50.exacttarget.com.',
 '161.71.33.244': 'cloud.straps1-sfmctest.com.',
 '161.71.33.245': 'gx245.mta.exacttarget.com.',
 '161.71.33.246': 'mon-s50.monitor.marketingcloud.com.',
 '161.71.33.247': 'user-content.s50.sfmc-content.com.'}
Found: crs.audi.com. (199.5.55.137)
Found: dc.audi.com. (63.140.62.27)
Nearby:
 {'63.140.62.22': 'ip-63-140-62-22.data.adobedc.net.',
 '63.140.62.23': 'ip-63-140-62-23.data.adobedc.net.',
```

```
 '63.140.62.24': 'ip-63-140-62-24.data.adobedc.net.',
 '63.140.62.25': 'ip-63-140-62-25.data.adobedc.net.',
 '63.140.62.26': 'ip-63-140-62-26.data.adobedc.net.',
 '63.140.62.27': 'ip-63-140-62-27.data.adobedc.net.',
 '63.140.62.28': 'ip-63-140-62-28.data.adobedc.net.',
 '63.140.62.29': 'ip-63-140-62-29.data.adobedc.net.',
 '63.140.62.30': 'ip-63-140-62-30.data.adobedc.net.',
 '63.140.62.31': 'ip-63-140-62-31.data.adobedc.net.',
 '63.140.62.32': 'ip-63-140-62-32.data.adobedc.net.'}
Found: developer.audi.com. (121.36.157.125)
Nearby:
 {'121.36.157.120': 'ecs-121-36-157-120.compute.hwclouds-dns.com.',
 '121.36.157.121': 'ecs-121-36-157-121.compute.hwclouds-dns.com.',
 '121.36.157.122': 'ecs-121-36-157-122.compute.hwclouds-dns.com.',
 '121.36.157.123': 'ecs-121-36-157-123.compute.hwclouds-dns.com.',
 '121.36.157.124': 'ecs-121-36-157-124.compute.hwclouds-dns.com.',
 '121.36.157.125': 'ecs-121-36-157-125.compute.hwclouds-dns.com.',
 '121.36.157.126': 'ecs-121-36-157-126.compute.hwclouds-dns.com.',
 '121.36.157.127': 'ecs-121-36-157-127.compute.hwclouds-dns.com.',
 '121.36.157.128': 'ecs-121-36-157-128.compute.hwclouds-dns.com.',
 '121.36.157.129': 'ecs-121-36-157-129.compute.hwclouds-dns.com.',
 '121.36.157.130': 'ecs-121-36-157-130.compute.hwclouds-dns.com.'}
Found: download.audi.com. (18.198.83.150)
Nearby:
 {'18.198.83.145': 'ec2-18-198-83-145.eu-central-1.compute.amazonaws.com.',
 '18.198.83.146': 'ec2-18-198-83-146.eu-central-1.compute.amazonaws.com.',
 '18.198.83.147': 'ec2-18-198-83-147.eu-central-1.compute.amazonaws.com.',
 '18.198.83.148': 'ec2-18-198-83-148.eu-central-1.compute.amazonaws.com.',
 '18.198.83.149': 'ec2-18-198-83-149.eu-central-1.compute.amazonaws.com.',
 '18.198.83.150': 'ec2-18-198-83-150.eu-central-1.compute.amazonaws.com.',
 '18.198.83.151': 'ec2-18-198-83-151.eu-central-1.compute.amazonaws.com.',
 '18.198.83.152': 'ec2-18-198-83-152.eu-central-1.compute.amazonaws.com.',
 '18.198.83.153': 'ec2-18-198-83-153.eu-central-1.compute.amazonaws.com.',
 '18.198.83.154': 'ec2-18-198-83-154.eu-central-1.compute.amazonaws.com.',
 '18.198.83.155': 'ec2-18-198-83-155.eu-central-1.compute.amazonaws.com.'}
Found: ecommerce.audi.com. (199.5.47.123)
Nearby:
 {'199.5.47.125': 'st_qa.vw.com.', '199.5.47.126': 'vwcourtsettlements.com.'}
Found: europe.audi.com. (192.229.202.3)
Found: extranet.audi.com. (199.5.55.142)
Found: feedback.audi.com. (81.169.188.180)
Nearby:
 {'81.169.188.176': 'concept-rs.de.',
 '81.169.188.177': 'h2928748.stratoserver.net.',
 '81.169.188.179': 'h2809758.stratoserver.net.',
```

```
 '81.169.188.181': 'vps000.niemann.com.de.',
 '81.169.188.182': 'h3003773.stratoserver.net.',
 '81.169.188.183': 'h2992689.stratoserver.net.',
 '81.169.188.184': 'h2834229.stratoserver.net.',
 '81.169.188.185': 'mail-lines.com.'}
Found: login.audi.com. (108.157.125.93)
Nearby:
 {'108.157.125.88': 'server-108-157-125-88.mad53.r.cloudfront.net.',
 '108.157.125.89': 'server-108-157-125-89.mad53.r.cloudfront.net.',
 '108.157.125.90': 'server-108-157-125-90.mad53.r.cloudfront.net.',
 '108.157.125.91': 'server-108-157-125-91.mad53.r.cloudfront.net.',
 '108.157.125.92': 'server-108-157-125-92.mad53.r.cloudfront.net.',
 '108.157.125.93': 'server-108-157-125-93.mad53.r.cloudfront.net.',
 '108.157.125.94': 'server-108-157-125-94.mad53.r.cloudfront.net.',
 '108.157.125.95': 'server-108-157-125-95.mad53.r.cloudfront.net.',
 '108.157.125.96': 'server-108-157-125-96.mad53.r.cloudfront.net.',
 '108.157.125.97': 'server-108-157-125-97.mad53.r.cloudfront.net.',
 '108.157.125.98': 'server-108-157-125-98.mad53.r.cloudfront.net.'}
Found: mail.audi.com. (13.111.18.27)
Nearby:
 {'13.111.18.22': 'orionims.s10.exacttarget.com.',
 '13.111.18.23': 'orionsmtp.s10.exacttarget.com.',
 '13.111.18.24': 'orionimsw.s10.exacttarget.com.',
 '13.111.18.25': 'pages.s10.exacttarget.com.',
 '13.111.18.26': 'ej26.mta.exacttarget.com.',
 '13.111.18.27': 'ej27.mta.exacttarget.com.',
 '13.111.18.28': 'ej28.mta.exacttarget.com.',
 '13.111.18.29': 'ej29.exacttarget.com.',
 '13.111.18.30': 'pub.s10.sfmctest.com.',
 '13.111.18.31': 'sock.s10.exacttarget.com.',
 '13.111.18.32': 'view.s10.exacttarget.com.'}
Found: marketplace.audi.com. (13.224.115.80)
Nearby:
 {'13.224.115.75': 'server-13-224-115-75.mad50.r.cloudfront.net.',
 '13.224.115.76': 'server-13-224-115-76.mad50.r.cloudfront.net.',
 '13.224.115.77': 'server-13-224-115-77.mad50.r.cloudfront.net.',
 '13.224.115.78': 'server-13-224-115-78.mad50.r.cloudfront.net.',
 '13.224.115.79': 'server-13-224-115-79.mad50.r.cloudfront.net.',
 '13.224.115.80': 'server-13-224-115-80.mad50.r.cloudfront.net.',
 '13.224.115.81': 'server-13-224-115-81.mad50.r.cloudfront.net.',
 '13.224.115.82': 'server-13-224-115-82.mad50.r.cloudfront.net.',
 '13.224.115.83': 'server-13-224-115-83.mad50.r.cloudfront.net.',
 '13.224.115.84': 'server-13-224-115-84.mad50.r.cloudfront.net.',
 '13.224.115.85': 'server-13-224-115-85.mad50.r.cloudfront.net.'}
Found: media.audi.com. (96.16.88.157)
```

```
Nearby:
 {'96.16.88.152': 'a96-16-88-152.deploy.static.akamaitechnologies.com.',
  '96.16.88.153': 'a96-16-88-153.deploy.static.akamaitechnologies.com.',
  '96.16.88.154': 'a96-16-88-154.deploy.static.akamaitechnologies.com.',
  '96.16.88.155': 'a96-16-88-155.deploy.static.akamaitechnologies.com.',
  '96.16.88.156': 'a96-16-88-156.deploy.static.akamaitechnologies.com.',
  '96.16.88.157': 'a96-16-88-157.deploy.static.akamaitechnologies.com.',
  '96.16.88.158': 'a96-16-88-158.deploy.static.akamaitechnologies.com.',
  '96.16.88.159': 'a96-16-88-159.deploy.static.akamaitechnologies.com.',
  '96.16.88.160': 'a96-16-88-160.deploy.static.akamaitechnologies.com.',
  '96.16.88.161': 'a96-16-88-161.deploy.static.akamaitechnologies.com.',
  '96.16.88.162': 'a96-16-88-162.deploy.static.akamaitechnologies.com.'}
Found: my.audi.com. (108.157.125.93)
Found: nokia.audi.com. (143.164.6.159)
```

Una alternativa para obtener subdominios es a través de los certificados digitales emitidos para un dominio específico. La herramienta '[ct-exposer]' utiliza el protocolo experimental de Transparencia de Certificación, creado para auditar públicamente los certificados emitidos por una Autoridad de Certificación para un dominio determinado.

```
└─$ ./ct-exposer.py -d audi.com
 [+]: Downloading domain list from crt.sh...
 [+]: Download of domain list complete.
 [+]: Parsed 650 domain(s) from list.

 [+]: Domains found:
199.5.50.47 Dialin.audi.com
109.232.173.209 E-AUCTION.AUDI.COM
199.5.50.47 Join.audi.com
199.5.50.47 Lyncdiscover.audi.com
199.5.50.47 Revproxypool1.vw.com
143.164.101.163 ac-cxs.audi.com
199.5.50.33 access.audi.com
199.5.50.36 access.vw.com
192.229.202.87  aco.audi.com
143.164.101.130 acoidx.audi.com
143.164.101.132 acorep.audi.com
- - - - - - - - - - - - - - - - - - - -

 [+]: Domains with no DNS record:
none    *.aat.eu-west-1.apps.msi.audi.com
none    *.admin.collaboration.msi.audi.com
none    *.audi.com
none    *.collaboration.msi.audi.com
```

```
none    *.dev.eu-west-1.apps.msi.audi.com
none    *.dev.mobility-tools.msi.audi.com
none    *.elb.dev.mobility-tools.msi.audi.com
none    *.elb.mobility-tools.msi.audi.com
none    *.eu-west-1.apps.msi.audi.com
none    *.eu-west-1.data.msi.audi.com
none    *.eu-west-1.stage.apps.msi.audi.com
none    *.internal.cn.cn-northwest-1.cfcr.msi.audi.com
none    *.internal.emea.eu-west-1.cfcr.msi.audi.com
none    *.internal.eu-west-1.apps.msi.audi.com
none    *.internal.us-west-2.apps.msi.audi.com
none    *.live.eu-west-1.apps.msi.audi.com
none    *.mobility-tools.msi.audi.com
- - - - - - - - - - - - - - - - - - - -
```

Servidores NS y MX

Estos servidores almacenan información sobre los servidores de nombres y los servidores de correo asociados.

- **MX**: Identifica los nombres de los servidores de correo, los cuales pueden ser múltiples. Estos servidores utilizan pesos para priorizar y balancear la carga (con un rango máximo de 0 y mínimo de 50). Normalmente, están equilibrados y utilizan filtros o servidores antispam.
- **NS**: Estos registros identifican los nombres de los servidores DNS responsables de un dominio, y puede haber uno o varios de ellos.

Empezaremos obteniendo los servidores de correo MX.

```
┌──(jose㉿kali)-[~]
└─$ host -t mx audi.com
audi.com mail is handled by 10 mg2.vw.com.
audi.com mail is handled by 10 mg10.vw.com.
audi.com mail is handled by 10 mg7.vw.com.
audi.com mail is handled by 10 mg9.vw.com.
audi.com mail is handled by 10 mg11.vw.com.
audi.com mail is handled by 10 mg1.vw.com.
audi.com mail is handled by 10 mg5.vw.com.
audi.com mail is handled by 10 mg12.vw.com.
audi.com mail is handled by 10 mg6.vw.com.
audi.com mail is handled by 10 mg8.vw.com.
audi.com mail is handled by 50 mg3.vw.com.
audi.com mail is handled by 10 mg4.vw.com.
```

Ahora procederemos a obtener la dirección IP de cada servidor.

```
┌──(jose㉿kali)-[~]
└─$ host mg2.vw.com
Host mg2.vw.com not found: 3(NXDOMAIN)

┌──(jose㉿kali)-[~]
└─$ host mg10.vw.com
mg10.vw.com has address 199.5.47.223

┌──(jose㉿kali)-[~]
└─$ host mg7.vw.com
mg7.vw.com has address 199.5.47.203

┌──(jose㉿kali)-[~]
└─$ host mg9.vw.com
mg9.vw.com has address 199.5.47.230

┌──(jose㉿kali)-[~]
└─$ host mg11.vw.com
mg11.vw.com has address 199.5.47.226

┌──(jose㉿kali)-[~]
└─$ host mg1.vw.com
Host mg1.vw.com not found: 3(NXDOMAIN)
```

```
┌──(jose㉿kali)-[~]
└─$ host mg5.vw.com
mg5.vw.com has address 199.5.47.161

┌──(jose㉿kali)-[~]
└─$ host mg12.vw.com
mg12.vw.com has address 199.5.47.250

┌──(jose㉿kali)-[~]
└─$ host mg6.vw.com
;; communications error to 100.100.1.1#53: timed out
mg6.vw.com has address 199.5.47.197

┌──(jose㉿kali)-[~]
└─$ host mg8.vw.com
mg8.vw.com has address 199.5.47.204

┌──(jose㉿kali)-[~]
└─$ host mg3.vw.com
Host mg3.vw.com not found: 3(NXDOMAIN)

┌──(jose㉿kali)-[~]
└─$ host mg4.vw.com
mg4.vw.com has address 199.5.47.158
```

Se observa que todas las direcciones IP pertenecen al segmento de red 199.5.47. Ahora procederemos a obtener el **whois** de una de estas direcciones para verificar si coinciden con nuestro objetivo

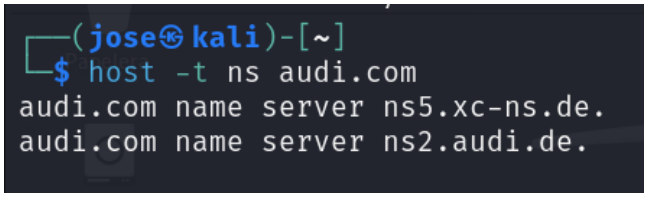
```
└─$ whois 199.5.47.223

 #
 # ARIN WHOIS data and services are subject to the Terms of Use
 # available at: https://www.arin.net/resources/registry/whois/tou/
 #
 # If you see inaccuracies in the results, please report at
 # https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
 #
 # Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
 #


 NetRange:       199.5.32.0 - 199.5.63.255
 CIDR:           199.5.32.0/19
```

```
NetName:        NETBLK-NET-VWNA
NetHandle:      NET-199-5-32-0-1
Parent:         NET199 (NET-199-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Volkswagen Group of America, Inc. (VOLKSW-1)
RegDate:        1994-01-05
Updated:        2021-12-14
Ref:            https://rdap.arin.net/registry/ip/199.5.32.0

OrgName:        Volkswagen Group of America, Inc.
OrgId:          VOLKSW-1
Address:        3800 Hamlin Rd
City:           Auburn Hills
StateProv:      MI
PostalCode:     48326
Country:        US
RegDate:        1994-01-05
Updated:        2021-11-23
Ref:            https://rdap.arin.net/registry/entity/VOLKSW-1

OrgAbuseHandle: NETWO5018-ARIN
OrgAbuseName:   Network Operations
OrgAbusePhone:  +1-248-754-4500
OrgAbuseEmail:  VWGoAITSTSNetworkTeam@vw.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/NETWO5018-ARIN

OrgTechHandle: MTC9-ARIN
OrgTechName:   Cummins, Marty Thomas
OrgTechPhone:  +1-248-754-4333
OrgTechEmail:  marty.cummins@vw.com
OrgTechRef:    https://rdap.arin.net/registry/entity/MTC9-ARIN

OrgTechHandle: NETWO5018-ARIN
OrgTechName:   Network Operations
OrgTechPhone:  +1-248-754-4500
OrgTechEmail:  VWGoAITSTSNetworkTeam@vw.com
OrgTechRef:    https://rdap.arin.net/registry/entity/NETWO5018-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
```

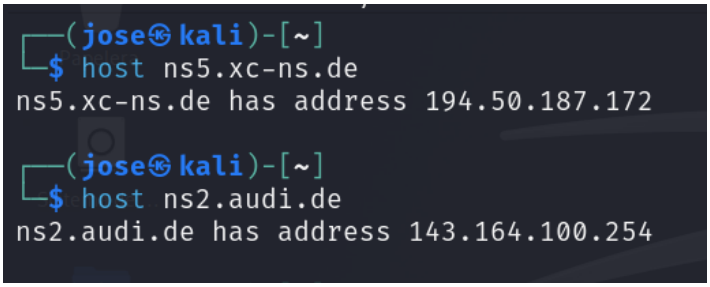
```
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
```

Como podemos ver en el campo **'orgName'**, estos servidores pertenecen a Volkswagen, que como vimos en la primera sección, está asociado con Audi. Por lo tanto, podemos confirmar que estos servidores son parte de nuestro objetivo.

Ahora procederemos a obtener información de los nombres de los nombres.



Como podemos observar, nos proporciona los dos servidores que obtuvimos inicialmente con el comando '**whois audi.com**'. Recordemos que teníamos dos servidores, y uno de ellos era externo a Audi. Ahora procederemos a obtener la dirección IP de estos servidores.



Vamos a analizar mas detalladamente cada ip

```
└─$ whois 194.50.187.172
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

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

```
% Information related to '194.50.187.0 - 194.50.187.255'

% Abuse contact for '194.50.187.0 - 194.50.187.255' is 'info@1api.net'

inetnum:        194.50.187.0 - 194.50.187.255
netname:        CentralNic-Anycast-J
descr:          CentralNic
descr:          CentralNic Anycast-J IPv4 Allocation
country:        DE
org:            ORG-GA152-RIPE
admin-c:        CNO4-RIPE
tech-c:         CNO4-RIPE
status:         ASSIGNED PI
mnt-by:         RIPE-NCC-END-MNT
mnt-by:         ONEAPI-MNT
mnt-by:         CENTRALNIC-MNT
created:        2006-04-25T09:26:13Z
last-modified:  2020-12-07T09:27:53Z
source:         RIPE # Filtered

organisation:   ORG-GA152-RIPE
org-name:       1api GmbH
country:        DE
org-type:       LIR
address:        Kaiserstraße 172-174
address:        66386
address:        St. Ingbert
address:        GERMANY
phone:          +4968949396760
fax-no:         +4968416984299
abuse-c:        AR14484-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-ref:        ISPAPI-M
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         ISPAPI-M
admin-c:        CH3108-RIPE
tech-c:         CH3108-RIPE
created:        2008-01-29T12:34:34Z
last-modified:  2024-01-26T09:17:47Z
source:         RIPE # Filtered

role:           CentralNic Network Operations
address:        CentralNic Ltd
address:        4th Floor, Saddlers House
address:        44 Gutter Lane
```

```
address:        London
address:        EC2V 6BR
address:        United Kingdom
org:            ORG-CL213-RIPE
admin-c:        DNS53
admin-c:        CACH3
admin-c:        KA4521-RIPE
admin-c:        JH30387-RIPE
tech-c:         DNS53
nic-hdl:        CNO4-RIPE
mnt-by:         CENTRALNIC-MNT
created:        2013-04-08T09:10:27Z
last-modified:  2023-01-25T14:22:39Z
source:         RIPE # Filtered

% Information related to '194.50.187.0/24AS1921'

route:          194.50.187.0/24
origin:         AS1921
mnt-by:         CENTRALNIC-MNT
created:        2023-09-18T09:19:53Z
last-modified:  2023-09-18T09:19:53Z
source:         RIPE

% Information related to '194.50.187.0/24AS207021'

route:          194.50.187.0/24
origin:         AS207021
mnt-by:         CENTRALNIC-MNT
created:        2023-09-18T09:20:09Z
last-modified:  2023-09-18T09:20:09Z
source:         RIPE

% Information related to '194.50.187.0/24AS212390'

route:          194.50.187.0/24
origin:         AS212390
mnt-by:         CENTRALNIC-MNT
created:        2020-12-07T09:28:30Z
last-modified:  2020-12-07T09:28:30Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.111 (SHETLAND)
```

En este caso, podemos observar que la dirección 194.50.187.172 está asociada a la organización CentralNic, una plataforma de reventa de dominios. Esta dirección pertenece a 1api GmbH, un proveedor de servicios de Internet con sede en Homburg, Alemania. Es posible que esta dirección IP se utilice para servicios relacionados con la gestión de dominios y otros servicios en línea.

```
└─$ whois 143.164.100.254

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#


NetRange:       143.163.0.0 - 143.164.255.255
CIDR:           143.163.0.0/16, 143.164.0.0/16
NetName:        RIPE-ERX-143-163-0-0
NetHandle:      NET-143-163-0-0-1
Parent:         NET143 (NET-143-0-0-0-0)
NetType:        Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:   RIPE Network Coordination Centre (RIPE)
RegDate:        2003-11-12
Updated:        2003-11-12
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/143.163.0.0

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: RNO29-ARIN
OrgTechName:   RIPE NCC Operations
OrgTechPhone:  +31 20 535 4444
OrgTechEmail:  hostmaster@ripe.net
OrgTechRef:    https://rdap.arin.net/registry/entity/RNO29-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#



Found a referral to 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 https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

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

```
% Information related to '143.164.0.0 - 143.164.255.255'

% No abuse contact registered for 143.164.0.0 - 143.164.255.255

inetnum:        143.164.0.0 - 143.164.255.255
netname:        NET-AUDI
descr:          Audi AG, Ingolstadt
country:        DE
admin-c:        AD1626-RIPE
tech-c:         AD1626-RIPE
status:         LEGACY
mnt-by:         AS12331-MNT
created:        2002-01-02T11:06:54Z
last-modified:  2019-12-04T13:10:29Z
source:         RIPE

role:           Audi Domainservice
address:        Audi AG
address:        D-85045 Ingolstadt
address:        Germany
admin-c:        RZ3093-RIPE
tech-c:         MR2740-RIPE
tech-c:         CS17416-RIPE
nic-hdl:        AD1626-RIPE
mnt-by:         AS12331-MNT
created:        2003-08-11T11:33:12Z
last-modified:  2023-02-22T11:57:47Z
source:         RIPE # Filtered

% Information related to '143.164.0.0/16AS12331'

route:          143.164.0.0/16
descr:          AUDI
origin:         AS12331
mnt-by:         AS12331-MNT
created:        2002-01-02T13:01:38Z
last-modified:  2002-01-02T13:01:38Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.111 (SHETLAND)
```

La dirección 143.164.100.254 efectivamente corresponde a la organización de Audi. A simple vista, podemos notar que esta dirección IP se encuentra dentro del rango de direcciones IP que obtuvimos previamente utilizando DNSRecon para los TLD asociados con Audi

Testeo de vulnerabilidades

Transferencia de zona

La transferencia de zona, también conocida como **AXFR**, es el proceso de copiar el contenido de un servidor DNS principal a un servidor DNS secundario. Las solicitudes AXFR son iniciadas por el servidor secundario y el principal responde. Para seguridad, el servidor principal debe filtrar las direcciones IP de los servidores secundarios autorizados para evitar la exposición de datos sensibles

```
└─$ dnsrecon -a -d audi.com
[*] std: Performing General Enumeration against: audi.com...
[*] Checking for Zone Transfer for audi.com name servers
[*] Resolving SOA Record
[+]     SOA ns2.audi.de 143.164.100.254
[*] Resolving NS Records
[*] NS Servers found:
[+]     NS ns5.xc-ns.de 194.50.187.172
[+]     NS ns2.audi.de 143.164.100.254
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 194.50.187.172
[+] 194.50.187.172 Has port 53 TCP Open
[-] Zone Transfer Failed ()
[*]
[*] Trying NS server 143.164.100.254
[+] 143.164.100.254 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[*] Checking for Zone Transfer for audi.com name servers
[*] Resolving SOA Record
[+]     SOA ns2.audi.de 143.164.100.254
```

```
[*] Resolving NS Records
[*] NS Servers found:
[+]     NS ns5.xc-ns.de 194.50.187.172
[+]     NS ns2.audi.de 143.164.100.254
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 194.50.187.172
[+] 194.50.187.172 Has port 53 TCP Open
[-] Zone Transfer Failed ()
[*]
[*] Trying NS server 143.164.100.254
[+] 143.164.100.254 Has port 53 TCP Open
[-] Zone Transfer Failed (Zone transfer error: REFUSED)
[-] DNSSEC is not configured for audi.com
[*]     SOA ns2.audi.de 143.164.100.254
[*]     NS ns5.xc-ns.de 194.50.187.172
[*]     Bind Version for 194.50.187.172 "reg-lhr1"
[*]     NS ns2.audi.de 143.164.100.254
[*]     Bind Version for 143.164.100.254 "*hidden*"
[*]     MX mg8.vw.com 199.5.47.204
[*]     MX mg5.vw.com 199.5.47.161
[*]     MX mg6.vw.com 199.5.47.197
[*]     MX mg11.vw.com 199.5.47.226
[*]     MX mg4.vw.com 199.5.47.158
[*]     MX mg10.vw.com 199.5.47.223
[*]     MX mg7.vw.com 199.5.47.203
[*]     MX mg12.vw.com 199.5.47.250
[*]     MX mg9.vw.com 199.5.47.230
[*]     A audi.com 143.164.101.69
[*]     TXT audi.com 9h35s1h847t8fdmwy1w1g17p7qjz59gq
[*]     TXT audi.com mmpxfqrlnr1rdg5f1hfj5cfkhd0dtrk9
[*]     TXT audi.com onetrust-domain-verification=8fee23d4a46d4df6b41d6d00e1c94a56
[*]     TXT audi.com onetrust-domain-verification=b0d32161c9544b16989c5e3aa4286e54
[*]     TXT audi.com 6w9m6dz73w9bk38kvc4j8pwmbwlr762k
[*]     TXT audi.com d5d9pkqkjz69yxy3njmdr6dvwtqtww11
[*]     TXT audi.com sdgnplnp27c0mx6cjtccgd4f4mvysvmm
[*]     TXT audi.com x4xn71kf072jkd1hd5z53mpqrhg4fds1
[*]     TXT audi.com E5C2CC6C-53C2-433D-891D-EA790B310D7A_30.10.2018
[*]     TXT audi.com QuoVadis=6a4e6d2a-eb05-4a91-8f88-bfa4aae58c6d
[*]     TXT audi.com
atlassian-domain-verification=TNcQgmSfT9rTwIinUauwy3r1oCoMJRIJm8F4Inf5qpprHwO/HMMWa7LaakG1LR34
[*]     TXT audi.com qm3tht3cwhvn8gd28md5zbjfhdwpk3m5
[*]     TXT audi.com
mds4WZIcsgf4QrIXBaS5wrL5S7pU7W8UGIEyUkByt8rXQw//xyDKs3C2yOaiZMw1LxaKEcTf7JfrAkWJd6YyRg==
[*]     TXT audi.com onetrust-domain-verification=bfc51da3d9c146a3b31970c84f3d4268
```

```
[*]     TXT audi.com google-site-verification=OFcxdsChGILZTgW99eHqq9l0XD6oTb3eSLShvo6Nruc
[*]     TXT audi.com pxy1tsygj3m1r2dch1bd4bk2pqk08s1c
[*]     TXT audi.com t3b0ldv7t0nzkr1gcvspxwntn95xncdh
[*]     TXT audi.com QuoVadis=6c56a19d-becb-44c4-8a16-576559c033b2
[*]     TXT audi.com MS=ms42598126
[*]     TXT audi.com miro-verification=768da25e0f20267ec0679b4f8ed36e8e56aaaa21
[*]     TXT audi.com x1mf91c3t49rwkq53gvv03xb4g9s5sg1
[*]     TXT audi.com frdv68l96gnwvjfsp1hxtxkn8w8tsjwv
[*]     TXT audi.com rkvx285z6n9k2jn0mqghlp76904b3nk0
[*]     TXT audi.com g1448cdl77b067lf2fbvp6cbd863s5m7
[*]     TXT audi.com twpddrvvjxtk5xqnt3qfc3qdvvl3lj8j
[*]     TXT audi.com QuoVadis=7c9b1377-11cd-452e-8933-44aff4389e87
[*]     TXT audi.com QuoVadis=8238d75d-d8e0-47a4-98ea-3feab274af8a
[*]     TXT audi.com v=spf1 include:cust-spf.exacttarget.com include:spf.constantcontact.com
ip4:199.5.47.0/24 ip4:199.5.50.176/28 ip4:199.5.51.2 ip4:91.198.139.136/31 -all
[*]     TXT audi.com bh0lxx9492t136ms988x9lvj04mgg2hc
[*]     TXT audi.com logmein-verification-code=18b1bac6-b901-4da7-a781-6fb5ce06afb5
[*]     TXT audi.com w9nv9b7ly1jb7z73973y0n0m2qvm41xk
[*]     TXT audi.com m62jdgqkl4q70f9807z055ph5kzxsjjn
[*]     TXT audi.com
adobe-idp-site-verification=799f7407b5ca168c7cfad993ade1d9259654b04d8a7cc5f1f427b253294be507
[*]     TXT audi.com google-site-verification=vDFU6sYZej2mOuf-DknoKJLAIJhHPJ9qlQh3dDYTs20
[*]     TXT _dmarc.audi.com
v=DMARC1;p=none;rua=mailto:dmarc_rua@audi.com;ruf=mailto:dmarc_ruf@audi.com;fo=1
[*] Enumerating SRV Records
[+]     SRV _sip._tls.audi.com access.audi.com 199.5.50.33 443
[+]     SRV _sip._tls.audi.com access.audi.com 199.5.50.36 443
[+]     SRV _sipfederationtls._tcp.audi.com access.audi.com 199.5.50.33 5061
[+]     SRV _sipfederationtls._tcp.audi.com access.audi.com 199.5.50.36 5061
[+] 4 Records Found
```

El comando dnsrecon intenta obtener información sobre el dominio audi.com, pero no logra una transferencia de zona. Proporciona detalles sobre los servidores DNS, direcciones IP, registros MX, A, TXT y SRV encontrados para el dominio, ofreciendo una visión general de su configuración de DNS.

Una alternativa para verificar la disponibilidad de la transferencia de zona es mediante el comando dig.

```
┌──(jose㉿kali)-[~]
└─$ dig audi.com axfr

; <<>> DiG 9.19.21-1-Debian <<>> audi.com axfr
;; global options: +cmd
; Transfer failed.
```

DNS Cache Snooping

Este proceso implica la consulta al servidor DNS para verificar si un dominio específico está almacenado en la caché. Se utiliza un diccionario que contiene todos los sitios web que se desean examinar. De esta manera, se puede identificar los sitios que los usuarios de la organización están visitando.

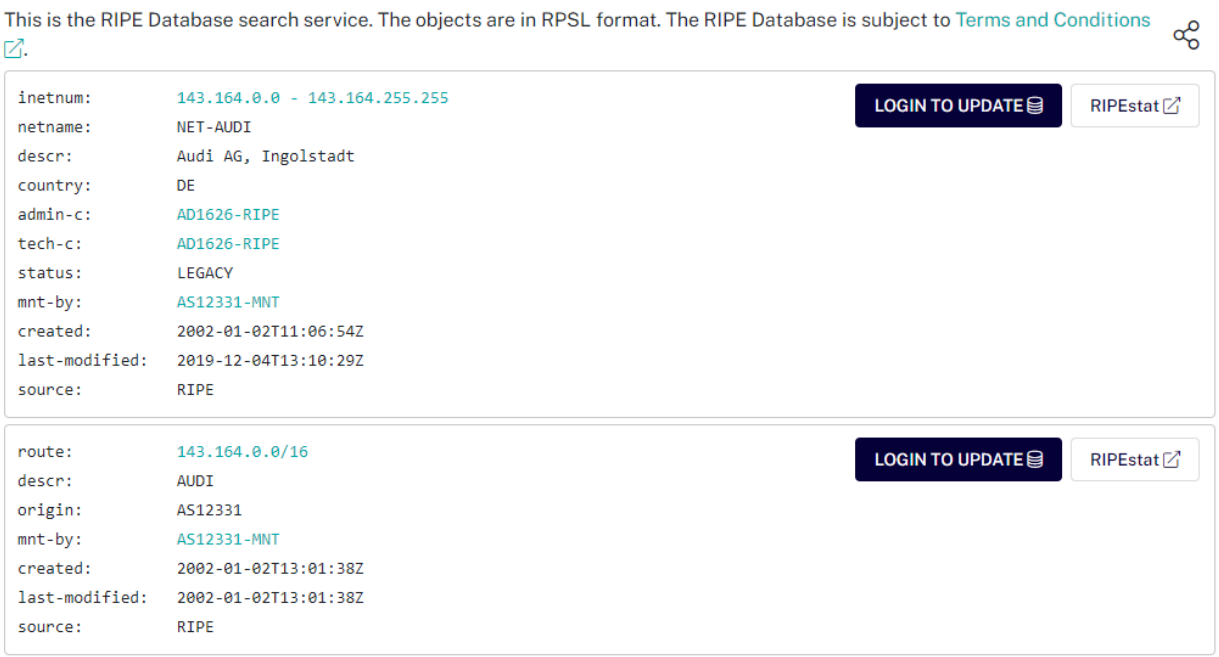
```
┌──(jose㉿kali)-[~]
└─$ dnsrecon -d audi.com -n 143.164.100.254 -t snoop -D /usr/share/dnsrecon/snoop.txt
[*] Using the dictionary file: /usr/share/dnsrecon/snoop.txt (provided by user)
[*] snoop: Performing Cache Snooping against NS Server: 143.164.100.254 ...
```

Rangos de IP y netnames

Podemos obtener esta información consultando los **registros regionales de Internet (RIR)**. Estas organizaciones son responsables de gestionar la asignación y distribución de direcciones IP. Los RIR proporcionan datos valiosos para identificar los rangos de direcciones IP asociados con una entidad específica y los sistemas autónomos (AS), que son los bloques de enrutamiento en la infraestructura de Internet.

- Localizadas geográficamente: APNIC (Asia), RIPE (Europa), ARIN (América), AfricNIC (África) y LacNIC (Lationamérica y Caribe).

Utilizando la lista de dominios TLD que obtuvimos al principio de la práctica, podemos consultar las diversas direcciones en el sitio web de ripe.net.

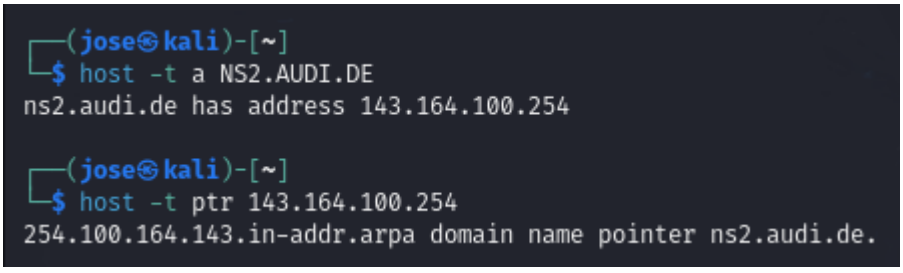


Utilizando el comando whois, podemos obtener información sobre la dirección IP seleccionada, 143.164.101.67, la cual está asociada al dominio audi.fr. La consulta revela que esta dirección IP se encuentra dentro del rango de direcciones IP (**inetnum**) de **143.164.0.0 a 143.164.255.255**, y está vinculada al **netname NET-AUDI**.

```
└─$ whois -r --sources RIPE 143.164.101.67
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

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

% Information related to '143.164.0.0 - 143.164.255.255'
```

```
% No abuse contact registered for 143.164.0.0 - 143.164.255.255

inetnum:        143.164.0.0 - 143.164.255.255
netname:        NET-AUDI
descr:          Audi AG, Ingolstadt
country:        DE
admin-c:        AD1626-RIPE
tech-c:         AD1626-RIPE
status:         LEGACY
mnt-by:         AS12331-MNT
created:        2002-01-02T11:06:54Z
last-modified:  2019-12-04T13:10:29Z
source:         RIPE

% Information related to '143.164.0.0/16AS12331'

route:          143.164.0.0/16
descr:          AUDI
origin:         AS12331
mnt-by:         AS12331-MNT
created:        2002-01-02T13:01:38Z
last-modified:  2002-01-02T13:01:38Z
source:         RIPE

% This query was served by the RIPE Database Query Service version 1.111 (DEXTER)
```

El siguiente paso consistiría en obtener nombres de dominio a partir de rangos de direcciones IP. Para ello, primero obtendremos la dirección IP del servidor, aunque esta dirección ya la habíamos obtenido previamente y le habíamos realizado una búsqueda whois



.

Al realizar un whois al nombre de red (**netname**) que hemos obtenido, también obtendremos el rango de direcciones IP que ya conocemos.

```
┌──(jose㉿kali)-[~]
└─$ whois NET-AUDI -h whois.ripe.net | grep inetnum
inetnum:        143.164.0.0 - 143.164.255.255
```

Una vez tengamos el rango de direcciones IP, podemos realizar una resolución inversa de cada dirección IP dentro de ese rango.

```
└─$ dnsrecon -r 143.164.0.0-143.164.255.255 -t rvl -d audi
[*] Performing Reverse Lookup from 143.164.0.0 to 143.164.255.255
[+]      PTR dataproxy3.dev2.audi.de 143.164.47.49
[+]      PTR dataproxy4.dev2.audi.de 143.164.47.50
[+]      PTR dataproxy1.dev2.audi.de 143.164.47.47
[+]      PTR dataproxy5.dev2.audi.de 143.164.47.51
[+]      PTR dataproxy2.dev2.audi.de 143.164.47.48
[+]      PTR kafka2.prod1.audi.de 143.164.47.72
[+]      PTR kafka3.prod1.audi.de 143.164.47.73
[+]      PTR kafka1.prod1.audi.de 143.164.47.71
[+]      PTR kafka4.prod1.audi.de 143.164.47.74
[+]      PTR kdc1.prod1.audi.de 143.164.47.80
[+]      PTR kdc2.prod1.audi.de 143.164.47.81
[+]      PTR kafka2.preprod1.audi.de 143.164.47.104
[+]      PTR kafka1.preprod1.audi.de 143.164.47.103
[+]      PTR kafka3.preprod1.audi.de 143.164.47.105
[+]      PTR kdc1.preprod1.audi.de 143.164.47.111
[+]      PTR kdc2.preprod1.audi.de 143.164.47.112
[+]      PTR a57u1weblb01.audi.de 143.164.97.1
[+]      PTR irfwweb01.audi.de 143.164.97.3
[+]      PTR n10h1weblb01.audi.de 143.164.97.2
[+]      PTR irfwweb02.audi.de 143.164.97.4
[+]      PTR irfwweb02n10-9.audi.de 143.164.97.6
[+]      PTR irfwweb01a57-9.audi.de 143.164.97.5
[+]      PTR aria.audi.de 143.164.97.215
[+]      PTR shop.audi.de 143.164.97.213
[+]      PTR shop-prelive.audi.de 143.164.97.212
[+]      PTR extranet.audi.de 143.164.97.216
[+]      PTR is0544.audi.de 143.164.97.217
[+]      PTR is0542.audi.de 143.164.97.219
[+]      PTR gebrauchtwagen.audi.de.164.143.in-addr.arpa 143.164.97.222
[+]      PTR www.audi-a4.com 143.164.97.218
[+]      PTR is0550.audi.de 143.164.97.221
[+]      PTR is0548.audi.de 143.164.97.223
[+]      PTR www.audi-fan.com 143.164.97.220
```

```
[+]       PTR www.do-not-open.com 143.164.97.224
[+]       PTR is0389.audi.de 143.164.97.228
[+]       PTR is0532.audi.de 143.164.97.225
[+]       PTR is0390.audi.de 143.164.97.227
[+]       PTR www.audi-fan.de.164.143.in-addr.arpa 143.164.97.226
[+]       PTR is0388.audi.de 143.164.97.229
[+]       PTR is0387.audi.de 143.164.97.230
[+]       PTR is0386.audi.de 143.164.97.231
[+]       PTR is0385.audi.de 143.164.97.232
[+]       PTR is0383.audi.de 143.164.97.234
[+]       PTR is0384.audi.de 143.164.97.233
[+]       PTR www.audi-tt.com 143.164.97.235
[+]       PTR www.audi-partner.de 143.164.97.239
[+]       PTR www.audi.hu 143.164.97.237
[+]       PTR www.audi-servicenet.de 143.164.97.238
[+]       PTR is0374.audi.de 143.164.97.241
[+]       PTR www.audi.com 143.164.97.240
[+]       PTR www.audi-marketing.com 143.164.97.236
[+]       PTR is0369.audi.de 143.164.97.246
[+]       PTR www-prelive.audi.de 143.164.97.247
[+]       PTR is0370.audi.de 143.164.97.245
[+]       PTR is0371.audi.de 143.164.97.244
[+]       PTR is0372.audi.de 143.164.97.243
[+]       PTR is0373.audi.de 143.164.97.242
[+]       PTR konfigurator.audi.de 143.164.97.250
[+]       PTR listen.audi.de 143.164.97.248
[+]       PTR wap.audi.de 143.164.97.252
[+]       PTR www.audi-allroad-quattro.com 143.164.97.251
[+]       PTR www.audi-a2.com 143.164.97.249
[+]       PTR www.sommerkonzerte.de 143.164.97.253
[+]       PTR www.audi.de 143.164.97.254
[+]       PTR irfwweb01a57-7.audi.de 143.164.98.3
[+]       PTR irfwweb01.audi.de 143.164.98.1
[+]       PTR irfwweb02.audi.de 143.164.98.2
[+]       PTR irfwweb02n10-7.audi.de 143.164.98.4
[+]       PTR irfwweb07.audi.de 143.164.98.5
[+]       PTR is0353.audi.de 143.164.98.117
[+]       PTR is0569.audi.de 143.164.98.116
[+]       PTR is0352.audi.de 143.164.98.118
[+]       PTR is0596.audi.de 143.164.98.120
[+]       PTR is0595.audi.de 143.164.98.121
[+]       PTR is0335.audi.de 143.164.98.123
[+]       PTR is0597.audi.de 143.164.98.119
[+]       PTR is0591.audi.de 143.164.98.122
[+]       PTR is0334.audi.de 143.164.98.124
```

```
[+]       PTR is0333.audi.de 143.164.98.125
[+]       PTR irfwweb01.audi.de 143.164.98.129
[+]       PTR is0332.audi.de 143.164.98.126
[+]       PTR irfwweb07.audi.de 143.164.98.133
[+]       PTR irfwweb02.audi.de 143.164.98.130
[+]       PTR irfwweb01a57-8.audi.de 143.164.98.131
[+]       PTR irfwweb02n10-8.audi.de 143.164.98.132
[+]       PTR ihwc01.audi.de 143.164.98.139
[+]       PTR ihwc02.audi.de 143.164.98.140
[+]       PTR ihwc03.audi.de 143.164.98.141
[+]       PTR ihwc04.audi.de 143.164.98.142
[+]       PTR is0347.audi.de 143.164.98.249
[+]       PTR mailgate.audi.de 143.164.98.252
[+]       PTR is0394.audi.de 143.164.98.251
[+]       PTR is0346.audi.de 143.164.98.250
[+]       PTR mail.ve-carnect.audi-online.de 143.164.99.67
[+]       PTR ve-carnect.audi-online.de 143.164.99.66
[+]       PTR irwebn10.audi.de 143.164.99.130
[+]       PTR irweba57.audi.de 143.164.99.129
[+]       PTR inzurt02a57--hsa.audi.de 143.164.99.131
[+]       PTR irfwweb01.audi.de 143.164.99.133
[+]       PTR irwebn10-5.audi.de 143.164.99.132
[+]       PTR irfwweb01a57-6.audi.de 143.164.99.135
[+]       PTR irfwweb02n10-6.audi.de 143.164.99.136
[+]       PTR irfwweb02.audi.de 143.164.99.134
[+]       PTR vpn-test-1.audi.de 143.164.99.167
[+]       PTR vpn-test-2.audi.de 143.164.99.169
[+]       PTR inzurt02a57-ql-ge0-3-0.audi.de 143.164.99.217
[+]       PTR irwebn10.audi.de 143.164.99.218
[+]       PTR irviag.audi.de 143.164.99.225
[+]       PTR irweba57.audi.de 143.164.99.226
[+]       PTR irviag.audi.de 143.164.99.233
[+]       PTR irwebn10.audi.de 143.164.99.234
[+]       PTR inzurt02a57--hsp.audi.de 143.164.99.239
[+]       PTR irwebn10.audi.de 143.164.99.242
[+]       PTR iruunet.audi.de 143.164.99.241
[+]       PTR iruunet.audi.de 143.164.99.249
[+]       PTR irweba57.audi.de 143.164.99.250
[+]       PTR pre-akamai-www.audi.com 143.164.100.160
[+]       PTR pre-akamai-cms.audi.com 143.164.100.162
[+]       PTR www.audi-mynet.de 143.164.100.179
[+]       PTR ak-edit.audi.de 143.164.100.195
[+]       PTR ak4-es.audi.de 143.164.100.203
[+]       PTR ns.audi.de 143.164.100.253
[+]       PTR ns2.audi.de 143.164.100.254
```

```
[+]       PTR webprx1.audi.de 143.164.102.13
[+]       PTR mailin3.audi.de 143.164.102.17
[+]       PTR webprx2.audi.de 143.164.102.14
[+]       PTR mailin4.audi.de 143.164.102.18
[+]       PTR mailin7.audi.de 143.164.102.23
[+]       PTR mailin8.audi.de 143.164.102.24
[+]       PTR mailin5.audi.de 143.164.102.19
[+]       PTR mailin6.audi.de 143.164.102.20
[+]       PTR mailin11.audi.de 143.164.102.58
[+]       PTR mailin10.audi.de 143.164.102.59
[+]       PTR mailin12.audi.de 143.164.102.57
[+]       PTR mailin14.audi.de 143.164.102.55
[+]       PTR mailin13.audi.de 143.164.102.56
[+]       PTR www.audi-partner.de 143.164.247.2
[+]       PTR www.audi.hu 143.164.247.1
[+]       PTR www.sommerkonzerte.de 143.164.247.3
[+]       PTR shop.audi.de 143.164.247.5
[+]       PTR www.audi-tt.com 143.164.247.4
[+]       PTR www.audi.de 143.164.247.7
[+]       PTR www.audi-tt.de 143.164.247.6
[+]       PTR web10.audi.de 143.164.247.10
[+]       PTR www.audi.com 143.164.247.8
[+]       PTR web11.audi.de 143.164.247.11
[+]       PTR extranet.audi.de 143.164.247.12
[+]       PTR www.audi-marketing.com 143.164.247.9
[+]       PTR aria.audi.de 143.164.247.13
[+]       PTR web17.audi.de 143.164.247.17
[+]       PTR www.audi-a2.com 143.164.247.14
[+]       PTR web18.audi.de 143.164.247.18
[+]       PTR web16.audi.de 143.164.247.16
[+]       PTR www.audi-a4.com 143.164.247.21
[+]       PTR web22.audi.de 143.164.247.22
[+]       PTR web31.audi.de 143.164.247.31
[+]       PTR web30.audi.de 143.164.247.30
[+]       PTR web32.audi.de 143.164.247.32
[+]       PTR www.audi-servicenet.de 143.164.247.53
[+]       PTR www.audi-allroad-quattro.com 143.164.247.51
[+]       PTR konfigurator.audi.de 143.164.247.54
[+]       PTR wap.audi.de 143.164.247.52
[+]       PTR www.do-not-open.com 143.164.247.57
[+]       PTR gate5.audi.de 143.164.248.5
[+]       PTR gate4.audi.de 143.164.248.4
[+]       PTR gate2.audi.de 143.164.249.1
[+]       PTR gate3.audi.de 143.164.249.2
[+]       PTR gate15.audi.de 143.164.249.66
```

```
[+]       PTR gate16.audi.de 143.164.249.67
[+]       PTR gate1.audi.de 143.164.249.254
[+] 170 Records Found
```

Resumen y conclusiones

El análisis exhaustivo de la empresa Audi a través del reconocimiento DNS ha proporcionado una visión detallada de su infraestructura de red. Durante este proceso, se identificaron diversos elementos clave, incluyendo dominios TLD, subdominios, servidores de nombres (como **NET-AUDI**), servidores de correo (por ejemplo, **mgxx.vw.com**) y rangos de IPs (desde **143.164.0.0 hasta 143.164.255.255**). Además, se llevó a cabo una evaluación de vulnerabilidades en los servidores DNS de Audi para determinar posibles debilidades en su seguridad. Estos datos recopilados son fundamentales para guiar las próximas fases del test de intrusión, permitiendo así fortalecer proactivamente la ciberseguridad de la empresa.

Con la información obtenida en la fase de footprinting, las siguientes etapas serían:

- **Escaneo (Scanning)**: Esta fase implica utilizar herramientas y técnicas para descubrir activos de red, identificar puertos abiertos, servicios en ejecución y posibles vulnerabilidades. Se busca obtener una comprensión más profunda de la topología de la red y los sistemas involucrados.
- **Enumeración (Enumeration)**: Aquí se recopila información más detallada sobre los sistemas y servicios descubiertos durante el escaneo. Esto puede incluir información sobre usuarios, grupos, recursos compartidos, y más, dependiendo de los servicios y protocolos disponibles.
- **Obtención de acceso (Gaining Access)**: Una vez que se han identificado las vulnerabilidades, se procede a explotarlas para obtener acceso no autorizado a los sistemas. Esto puede implicar el uso de exploits, ataques de fuerza bruta, o ingeniería social, entre otros métodos.

- **Mantenimiento del acceso (Maintaining Access)**: Después de obtener acceso inicial, el objetivo es mantener ese acceso de manera persistente para poder continuar explorando la red y recopilando información sensible.
- **Escalada de privilegios (Privilege Escalation)**: En esta etapa, se busca aumentar los privilegios obtenidos inicialmente para acceder a información más confidencial o sistemas de mayor importancia dentro de la red.
- **Movimiento lateral (Lateral Movement)**: Consiste en expandir la presencia en la red, buscando otros sistemas vulnerables o puntos de entrada adicionales para obtener un mayor control sobre la infraestructura.
- **Exfiltración de datos (Data Exfiltration)**: Finalmente, si el objetivo del atacante es robar información confidencial, se llevará a cabo la transferencia no autorizada de datos fuera de la red comprometida.