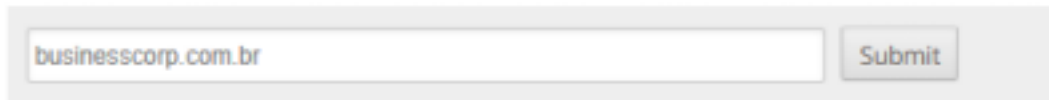


Coletando Info com o Whois

+ Primeiramente, devemos buscar o Whois da IANA:

iana.org/whois



```
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object
```

```
refer:      whois.registro.br
```

```
domain:     BR
```

```
organisation: Comit  Gestor da Internet no Brasil
address:     Av. das Na  es Unidas, 11541, 7. andar
address:     S o Paulo SP 04578-000
address:     Brazil
```

```
contact:     administrative
name:        Demi Getschko
organisation: Comit  Gestor da Internet no Brasil
address:     Av. das Na  es Unidas, 11541, 7. andar
address:     S o Paulo SP 04578-000
address:     Brazil
phone:       +55 11 5509 3505
fax-no:      +55 11 5509 3501
e-mail:      demi@registro.br
```

→ Veja que o campo "refer" aponta para o whois.registro.br

+ Faremos a busca mais detalhada no whois.registro.br

Domínio **businesscorp.com.br**

TITULAR

Desec Security Segurança da Informação LTDA

DOCUMENTO

23.019.510/0001-06

RESPONSÁVEL

Desec Security

PAÍS

BR

CONTATO DO TITULAR

JORLO47

CONTATO TÉCNICO

JORLO47

SERVIDOR DNS

ns1.businesscorp.com.br 37.59.174.225 ~

SERVIDOR DNS

ns2.businesscorp.com.br 37.59.174.226 ~

→ a busca no registro.br nos apontou um endereço de ip:
37.59.174.225

→ Isso permite uma nova consulta no registro.br



→ A pesquisa nos aponta para o whois.lacnic.net, o qual faremos a busca

+ inetnum: 37.59.174.224 - 37.59.174.239 [range de IP's]

+ origin: AS16276

~~~~~

Whois no terminal

~~~~~

+ No terminal do kali, o whois também começa a pesquisa pelo site da IANA

```
whois businesscorp.com.br
```

```
root@pentest:~/Desktop# whois businesscorp.com.br

% Copyright (c) Nic.br
% The use of the data below is only permitted as described in
% full by the terms of use at https://registro.br/termo/en.html ,
% being prohibited its distribution, commercialization or
% reproduction, in particular, to use it for advertising or
% any similar purpose.
% 2019-11-12T16:04:13-03:00

domain:      businesscorp.com.br
owner:       Desec Security Segurança da Informação LTDA
ownerid:      23.019.510/0001-06
responsible: Desec Security
country:     BR
owner-c:      JORLO47
admin-c:      JORLO47
tech-c:       JORLO47
billing-c:    JORLO47
nserver:     ns1.businesscorp.com.br 37.59.174.225
```

+ Para aparecer o refer, basta que forcemos o processo com o seguinte comando:

```
whois -h whois.iana.org businesscorp.com.br
```

```
root@pentest:~/Desktop# whois -h whois.iana.org businesscorp.com.br

% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:       whois.registro.br
domain:      BR
organisation: Comitê Gestor da Internet no Brasil
address:     Av. das Nações Unidas, 11541, 7º andar
address:     São Paulo SP 04578-000
address:     Brazil
contact:     administrative
name:        Demi Getschko
organisation: Comitê Gestor da Internet no Brasil
address:     Av. das Nações Unidas, 11541, 7º andar
address:     São Paulo SP 04578-000
address:     Brazil
phone:       +55 11 5509 3505
fax-no:      +55 11 5509 3501
e-mail:      demi@registro.br
```