Mapeando a INFRA - Pesquisa por IP

+ Pesquisa pelo IP do site:

```
host businesscorp.com.br
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# host businesscorp.com.br
businesscorp.com.br has address 37.59.174.225
businesscorp.com.br mail is handled by 10 mail.businesscorp.com.br.
```

→ estamos buscando descobrir se o cliente tem um netblock ou um ASN
→ em alguns casos, o cliente usa um proxy ou outra ferramenta para ocultar seu real endereço de IP

+ Podemos então fazer a pesquisa no site da ARIN (American Registry for Internet Numbers)

https://search.arin.net/rdap

+ De maneira análoga, podemos pesquisar por meio do terminal

```
whois 37.59.174.225 | egrep "inetnum|aut-num"
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# whois 37.59.174.225 | egrep "inetnum|aut-num"
inetnum:        37.59.174.224 - 37.59.174.239
```

→ não retorna um aut-num pois o cliente n tem um ASN

+ Para o caso de empresas maiores, como é o caso do Itaú, o endereço apresentado é o de outra empresa. No nosso caso, a Akamai:

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# host itau.com.br
itau.com.br has address 23.73.216.51
```

→ Ao consultar o whois desse endereço, obtemos:

```
NetRange:       23.72.0.0 - 23.79.255.255
CIDR:           23.72.0.0/13
NetName:        AKAMAI
NetHandle:      NET-23-72-0-0-1
Parent:         NET23 (NET-23-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Akamai Technologies, Inc. (AKAMAI)
```

+ A solução para isso é então resolver os outros nomes que decorrem do host itau.com.br