LAB - SEM 05 - Info Gathering INFRA

LAB01: 37.59.174.224-37.59.174.239
host business... → usamos o endereço (37.59.174.225) para realizar uma busca no site da ARIN → whois/rdap

LAB02: AS16276
whois 37.59.174.225

LAB03: infrasecreta.businesscorp.com.br
forçamos o zone transfer com o script dnszone.sh

```
#!/bin/bash
for server in $(host -t ns $1 | cut -d " " -f 4);
do
host -l -a $1 $server
done
```

LAB04: 37.59.174.225
Já vinha resolvido com o script anterior

LAB05: rh.businesscorp.com.br,piloto.businesscorp.com.br
o seguinte script realiza o dns reverso a partir do range de IP's encontrado no começo (dns_rev.sh)

```
#!/bin/bash
for ip in $(seq 224 239); do
host -t ptr 37.59.174.$ip | grep -v "37-59-174" | cut -d " " -f 5
done
```

LAB06: 37.59.174.229,37.59.174.230
já vinham resolvidos com o script anterior

LAB07: 0989201883299
para exibir informações acerca do host, usamos o seguinte comando

```
host -t hinfo businesscorp.com.br
```

LAB08: 9283947588214
para analisar o spf, bastou que executássemos o seguinte:

```
host -t txt businesscorp.com.br
```

LAB09: 092935999311009
Para a realização do subdomain takeover, usamos uma wordlist chamada cat.txt e o seguinte script: (subtakeover.sh)

```
#!/bin/bash
for palavra in $(cat cat.txt); do
host -t cname $palavra$1 | grep "alias for"
done
```