Tracking the route - Aula Prática

+ Quando fazemos o ping em uma rede, a diferença entre o ttl default
e o ttl apresentado representa a quantidade de hosts na rota

+ Veja o seguinte default para os sistemas operacionais:
  - Windows - 128
  - Linux - 64
  - Unix - 255

+ Enviaremos 1 pacote ping para a businesscorp:

```
ping -c 1 businesscorp.com.br
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# ping -c 1 businesscorp.com.br
PING businesscorp.com.br (37.59.174.225) 56(84) bytes of data.
64 bytes from ip225.ip-37-59-174.eu (37.59.174.225): icmp_seq=1 ttl=50 time=189 ms

--- businesscorp.com.br ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 188.660/188.660/188.660/0.000 ms
```

Veja que o ttl encontrado foi de 50, o que nos mostra que, como
está próximo do 64, possivelmente o sistema alvo é um Linux,
e nossa distância à ele é de 64 - 50 = 14 hosts

+ Para descobrir cada um dos hosts desse caminho, faremos pings
consecutivos incrementando uma unidade ao ttl

+ O parâmetro que nos permite controlar o valor do ttl é o -t

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# ping -c 1 -t 1 businesscorp.com.br
PING businesscorp.com.br (37.59.174.225) 56(84) bytes of data.
From 192.168.1.1 (192.168.1.1) icmp_seq=1 Time to live exceeded

--- businesscorp.com.br ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms


┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# ping -c 1 -t 2 businesscorp.com.br
PING businesscorp.com.br (37.59.174.225) 56(84) bytes of data.
From 100.90.0.1 (100.90.0.1) icmp_seq=1 Time to live exceeded

--- businesscorp.com.br ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms


┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# ping -c 1 -t 3 businesscorp.com.br
PING businesscorp.com.br (37.59.174.225) 56(84) bytes of data.
From 172.31.250.6 (172.31.250.6) icmp_seq=1 Time to live exceeded

--- businesscorp.com.br ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

~~~~~~
~~~~~~

Aprendendo a usar o traceroute

~~~~~~

+ É uma ferramenta que realiza pings e nos devolve a rota e os tempos de resposta de cada roteador

+ Principais parâmetros:

→ `traceroute businesscorp.com.br`

Modo comum de uso, que por paadrão, agurda resposta de até 3s e utiliza o protocolo UDP
Quando apresenta mais de um endereço de IP em uma linha, significa que houve um balanceamento de carga
Quando aparece um * * *, significa que o host local não aceitou o protocolo UDP, e quando vemos apenas 1 *, significa que o tempo de espera foi excedido (>3s)

→ `traceroute businesscorp.com.br -w 1`

Indica que mudamos o tempo padrão de espera que era 3s, e agora será de apenas 1s

→ `traceroute businesscorp.com.br -m 1`

Indica que mudamos o ttl, que era 30 e passou a ser apenas 1

→ `traceroute businesscorp.com.br -m 20 -f 15`

Agora teremos 20 saltos (hops) e só serão exibidos a partir do 15

→ `traceroute businesscorp.com.br -A`

Com esse parâmetro, serão exibidos os ASN's

→ `traceroute businesscorp.com.br -n`

Essa opção não diz o host. Traz uma saída mais limpa mostrando apenas os IP's.

+ Para mudar os portocolos enviados, basta executar os seguintes parâmetros

- I → ICMP
- T → TCP
- U → UDP (vem como padrão, mas quando executamos assim, ele mira na porta 53.

+ Para mudar a porta de ataque, bas executar o parâmtro -p 43
[nesse caso muda a porta para 43]
~~~~~~