Descobrindo Hosts Ativos - Ping Sweep

+ Depois da etapa passada de descobrir os ranges de endereços de IP, vamos agora descobrir quais desses endereços estão ativos e respondendo.

~~~~~~

Ping Sweep

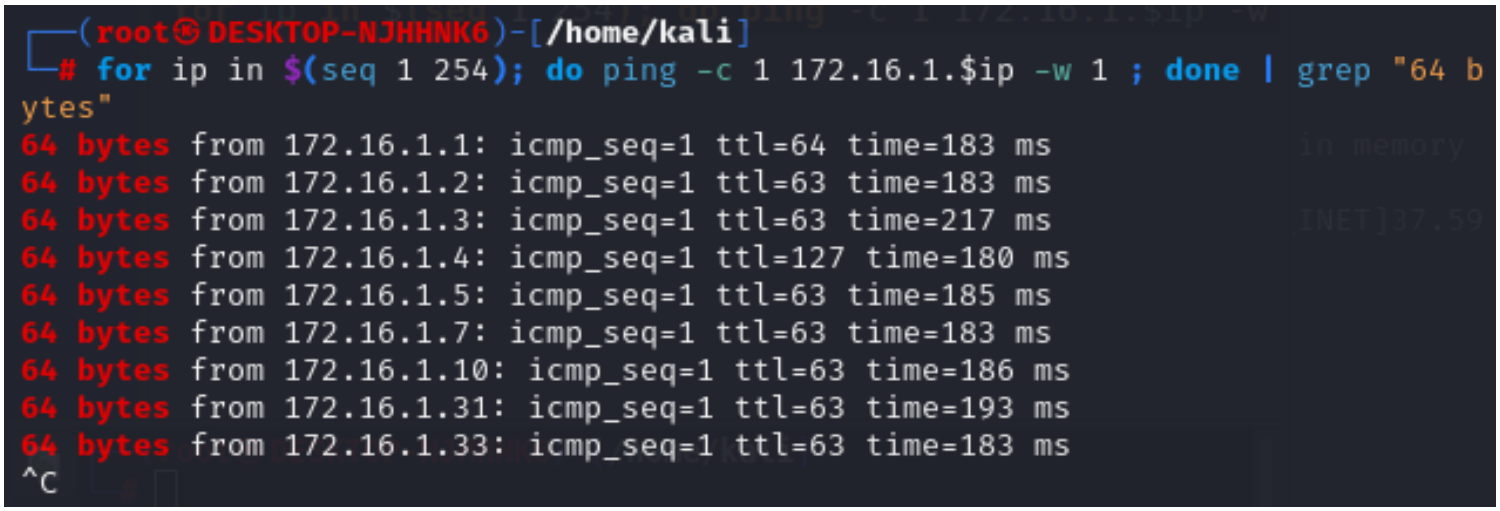
~~~~~~

+ Basicamente vamos usar o utilitário do ping e ver quais endereços mandam respostas

+ Quando n há resposta do ping, n podemos afirmar diretamente que o host está inativo. Pode ser que haja um Firewall impedindo o ping.

+ Conectamos na VPN da desec e fizemos uma varredura interna na rede com o ping

```
for ip in $(seq 1 254); do ping -c 1 172.16.1.$ip -w 1 ; done | grep "64 bytes"
```



+ O parâmetro -w serve para indicar o tempo de espera, no caso -w 1 indica espera de apenas 1s pela resposta e o -c 1 indica que enviamos apenas um pacote ping.

+ Para simular o ping sweep numa rede externa, vamos executar o seguinte (no ambiente da businesscorp)

```
for ip in $(seq 224 239); do ping -c 1 37.59.174.$ip -w 1 ; done | grep "64 byte
```

```
└─# for ip in $(seq 224 239); do ping -c 1 37.59.174.$ip -w 1 ; done | grep "6
4 bytes"
64 bytes from 37.59.174.225: icmp_seq=1 ttl=50 time=188 ms
64 bytes from 37.59.174.226: icmp_seq=1 ttl=50 time=190 ms
64 bytes from 37.59.174.227: icmp_seq=1 ttl=50 time=187 ms
64 bytes from 37.59.174.228: icmp_seq=1 ttl=50 time=192 ms
64 bytes from 37.59.174.229: icmp_seq=1 ttl=50 time=184 ms
64 bytes from 37.59.174.231: icmp_seq=1 ttl=50 time=186 ms
64 bytes from 37.59.174.232: icmp_seq=1 ttl=50 time=190 ms
64 bytes from 37.59.174.239: icmp_seq=1 ttl=50 time=185 ms
```

Ele retorna os hosts que identificou como ativos (no caso, que respondem icmp)

\+ Existem ferramentas que fazem isso de maneira automatizada, como o fping

```
fping -a -g 172.16.1.0/24
```

-a para verificar apenas os hosts q respondem
-g para passarmos o range