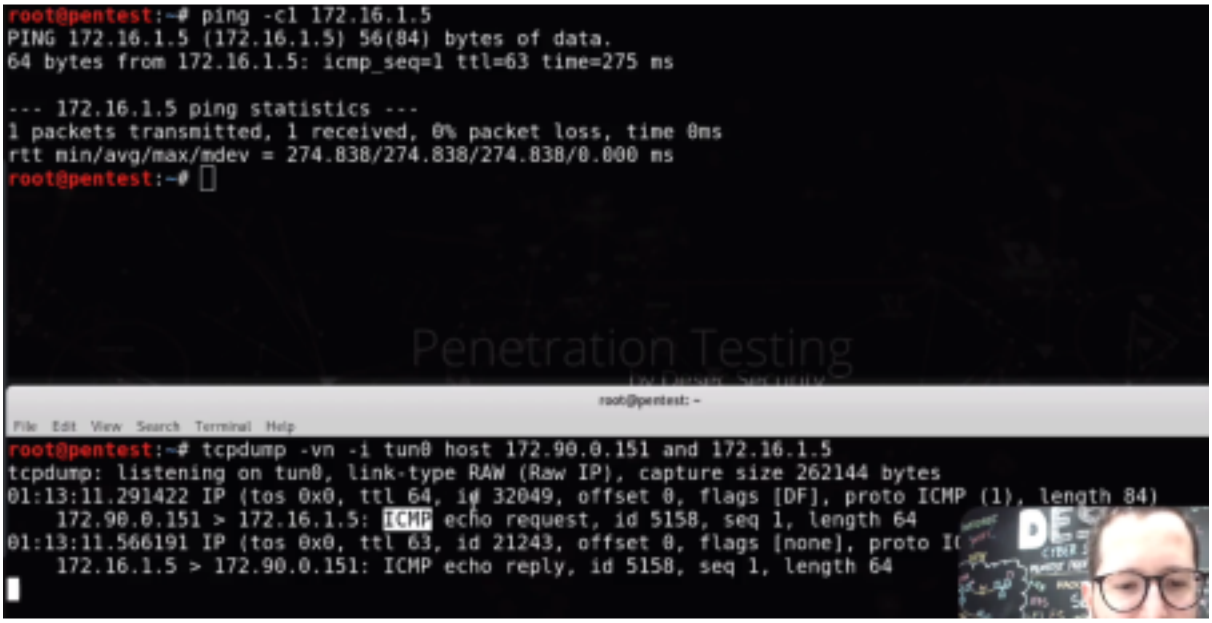
Estudo Técnico: Ping Sweep

+ Alguns hosts podem estar ativos, mas não responder ao ping por ter algum firewall que bloqueie o protocolo icmp.

+ O objetivo dessa aula foi fazer a captura [com o tcpdump] e análise do envio de pacotes icmp setados pelo ping numa rede interna.

+ Basicamente, quando o host está com as regras de firewall desligadas, podemos ver a resposta do protocolo icmp

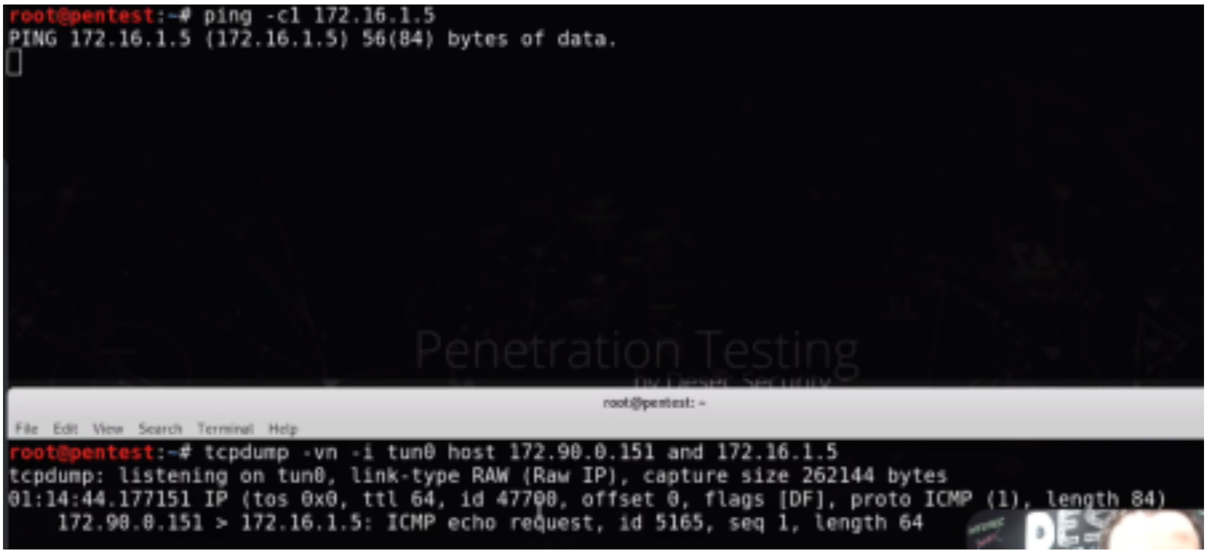


```
root@pentest:~# ping -c1 172.16.1.5
PING 172.16.1.5 (172.16.1.5) 56(84) bytes of data.
64 bytes from 172.16.1.5: icmp_seq=1 ttl=63 time=275 ms

--- 172.16.1.5 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 274.838/274.838/274.838/0.000 ms
root@pentest:~# 
```

```
root@pentest:~# tcpdump -vn -i tun0 host 172.90.0.151 and 172.16.1.5
tcpdump: listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
01:13:11.291422 IP (tos 0x0, ttl 64, id 32049, offset 0, flags [DF], proto ICMP (1), length 84)
    172.90.0.151 > 172.16.1.5: ICMP echo request, id 5158, seq 1, length 64
01:13:11.566191 IP (tos 0x0, ttl 63, id 21243, offset 0, flags [none], proto I(
    172.16.1.5 > 172.90.0.151: ICMP echo reply, id 5158, seq 1, length 64
```

+ Quando o host está ativo mas o firewall impede o input de icmp, não conseguiremos ver a ICMP echo reply

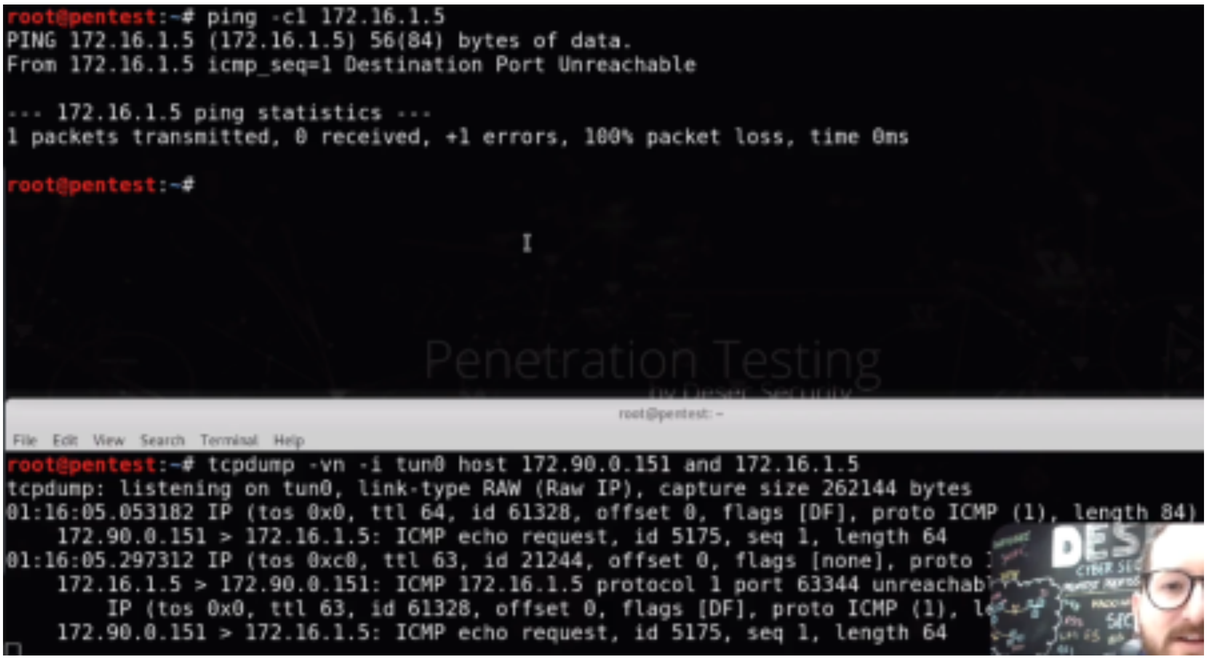


```
root@pentest:~# ping -c1 172.16.1.5
PING 172.16.1.5 (172.16.1.5) 56(84) bytes of data.
```

```
root@pentest:~# tcpdump -vn -i tun0 host 172.90.0.151 and 172.16.1.5
tcpdump: listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
01:14:44.177151 IP (tos 0x0, ttl 64, id 47700, offset 0, flags [DF], proto ICMP (1), length 84)
    172.90.0.151 > 172.16.1.5: ICMP echo request, id 5165, seq 1, length 64
```

+ Quando o firewall estiver configurado para rejeitar (nem aceitar [accept], nem bloquear [drop]), poderemos ver uma echo reply dizendo que a porta está fechada

```
iptables -A INPUT -p icmp -j REJECT
```



```
root@pentest:~# ping -c1 172.16.1.5
PING 172.16.1.5 (172.16.1.5) 56(84) bytes of data.
From 172.16.1.5 icmp_seq=1 Destination Port Unreachable

--- 172.16.1.5 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms

root@pentest:~#
```

```
root@pentest:~# tcpdump -vn -i tun0 host 172.90.0.151 and 172.16.1.5
tcpdump: listening on tun0, link-type RAW (Raw IP), capture size 262144 bytes
01:16:05.053182 IP (tos 0x0, ttl 64, id 61328, offset 0, flags [DF], proto ICMP (1), length 84)
    172.90.0.151 > 172.16.1.5: ICMP echo request, id 5175, seq 1, length 64
01:16:05.297312 IP (tos 0xc0, ttl 63, id 21244, offset 0, flags [none], proto I
    172.16.1.5 > 172.90.0.151: ICMP 172.16.1.5 protocol 1 port 63344 unreachab
        IP (tos 0x0, ttl 63, id 61328, offset 0, flags [DF], proto ICMP (1), le
    172.90.0.151 > 172.16.1.5: ICMP echo request, id 5175, seq 1, length 64
```