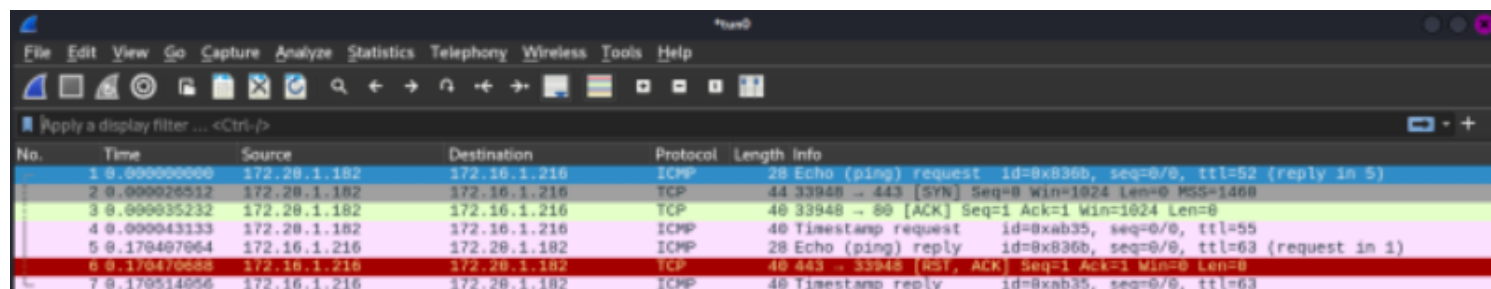


Descobrimos Hosts Ativos - NMAP

+ Indicado para pentests externos quando o icmp for bloqueado

+ O nmap realiza outros testes que não somente os do protocolo icmp para verificar se um host está ativo ou não. Veja a seguinte captura de tráfego:



The image shows a Wireshark packet capture interface. The packet list on the left shows seven packets. The packet details pane on the right shows the selected packet (No. 6) as an Echo (ping) reply from 172.16.1.216 to 172.20.1.182. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.20.1.182	172.16.1.216	ICMP	28	Echo (ping) request id=8x836b, seq=0/0, ttl=52 (reply in 5)
2	0.0000026512	172.20.1.182	172.16.1.216	TCP	44	33948 → 443 [SYN] Seq=8 Win=1024 Len=0 MSS=1460
3	0.0000035232	172.20.1.182	172.16.1.216	TCP	40	33948 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
4	0.0000043133	172.20.1.182	172.16.1.216	ICMP	40	Timestamp request id=8xab35, seq=0/0, ttl=55
5	0.170407064	172.16.1.216	172.20.1.182	ICMP	28	Echo (ping) reply id=8x836b, seq=0/0, ttl=63 (request in 1)
6	0.170408568	172.16.1.216	172.20.1.182	TCP	40	443 → 33948 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	0.170514096	172.16.1.216	172.20.1.182	ICMP	40	Timestamp reply id=8xab35, seq=0/0, ttl=63

+ Fizemos um filtro para que o wireshark capturasse apenas pela tun0, pois estamos usando a VPN.

+ Nessa captura, veja que o nmap tentou o ICMP, TCP na porta 443, TCP na porta 80, ICMP novamente e outros. Veja que o protocolo TCP na porta 443 não obteve sucesso, mas o ICMP sim, pois teve uma reply mostrando que o host está ativo.

+ `nmap -sn 172.16.1.216`

```
(root@DESKTOP-NJHHNK6)-[/home/kali]
# nmap -sn 172.16.1.216
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 18:20 -03
Nmap scan report for 172.16.1.216
Host is up (0.17s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

+ `nmap -sn 172.16.1.0/24 -oG hostsativos`

-o indica o output

N → normal

X → xml

G → greppable (em que se pode aplicar o grep)

hostsativos é o nome do diretório em que a resposta será guardada

```
cat hostsativos | cut -d " " -f 2 > ips
```

A indicação de que o host estava ativo é a saída "host up"