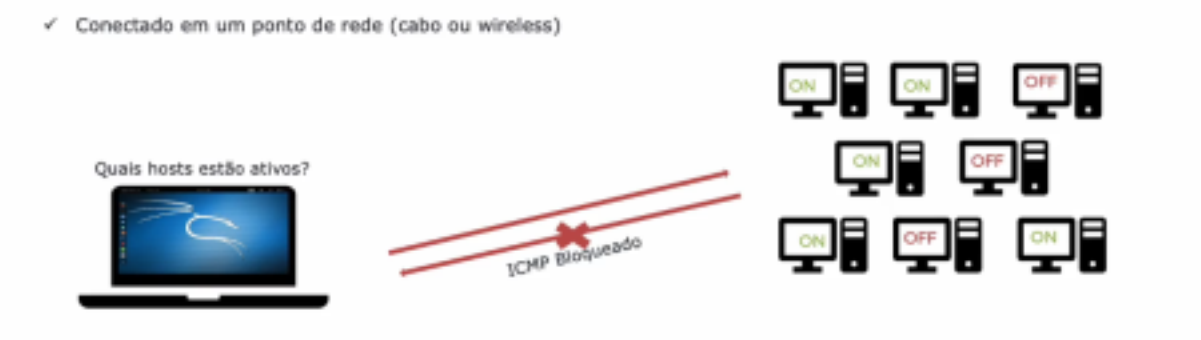
Descobrindo Hosts Ativos - Pentest Interno

+ Encontrando hosts ativos através do

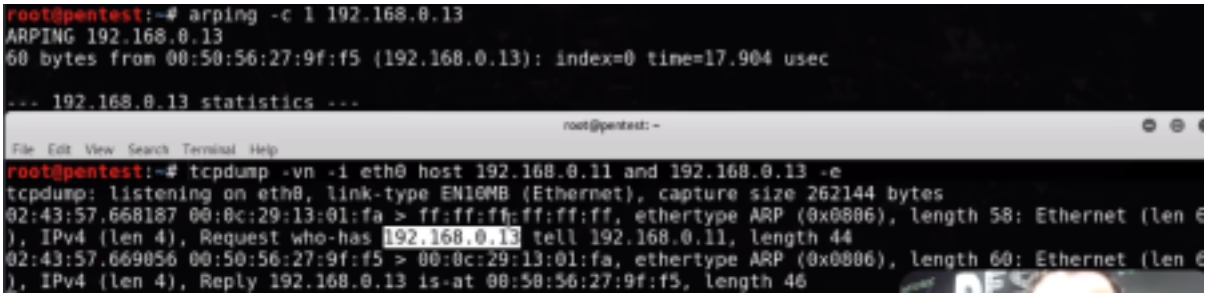
~~~~~~
Protocolo ARP
~~~~~~

+ Esse método só funciona bem quando aplicado presencialmente, foi à distância se usam ferramentas da camada 3 do modelo OSI.

+ De maneira semelhante ao ping, usaremos agr o arping para descobrir quais hosts estão ativos em uma rede



+ Veja a captura pelo tcpdump do arping



+ Para fazer um script que seja semelhante ao anterior no sentido de fazer a varredura em um range, basta trocar ping por arping e onde tinham 64 bytes que era a resposta padrão do ping, colocaremos agora 60 bytes, como se segue:

```
for ip in $(seq 10 14);do arping -c 1 192.168.0.$ip;done | grep "60 bytes"
```

+ Há uma ferramenta que executa uma varredura automática na rede interna que é o arp-scan. Veja abaixo o seu uso local

```
arp-scan -l
```

```
┌──(root㉿DESKTOP-NJHHNK6)-[/home/kali]
└─# arp-scan -l
Interface: wlan0, type: EN10MB, MAC: da:0c:03:87:86:aa, IPv4: 192.168.1.138
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1     00:6d:61:b5:d2:20       (Unknown)
192.168.1.39    24:0a:64:05:63:72       (Unknown)
192.168.1.33    28:9c:6e:6a:e2:bc       (Unknown)
192.168.1.33    28:9c:6e:6a:e2:bc       (Unknown) (DUP: 2)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.868 seconds (137.04 hosts/sec).
```