

Descobrimos Hosts Ativos - Pentest Interno

+ Encontrando hosts ativos através do

~~~~~

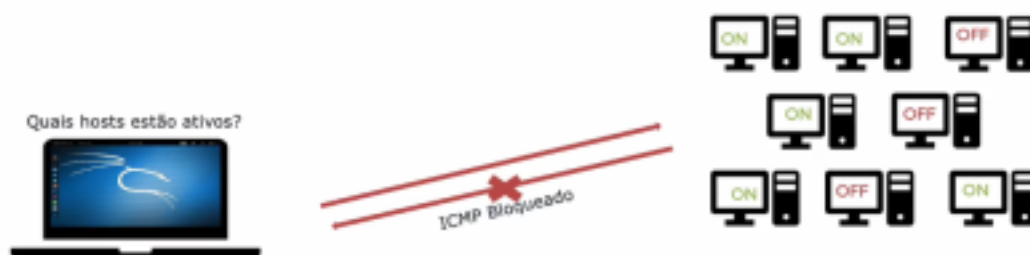
## Protocolo ARP

~~~~~

+ 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

✓ Conectado em um ponto de rede (cabo ou wireless)



+ Veja a captura pelo tcpdump do arping

```
root@pentest:~# arping -c 1 192.168.0.13
ARPING 192.168.0.13
60 bytes from 00:50:56:27:9f:f5 (192.168.0.13): index=0 time=17.904 usec
--- 192.168.0.13 statistics ---

root@pentest:~# tcpdump -vn -i eth0 host 192.168.0.11 and 192.168.0.13 -e
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
02:43:57.668187 00:0c:29:13:01:fa > ff:ff:ff:ff:ff:ff, ethertype ARP (0x0806), length 58: Ethernet (len 6
), IPv4 (len 4), Request who-has 192.168.0.13 tell 192.168.0.11, length 44
02:43:57.669056 00:50:56:27:9f:f5 > 00:0c:29:13:01:fa, ethertype ARP (0x0806), length 60: Ethernet (len 6
), IPv4 (len 4), Reply 192.168.0.13 is-at 00:50:56:27:9f:f5, length 46
```

+ 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).

```