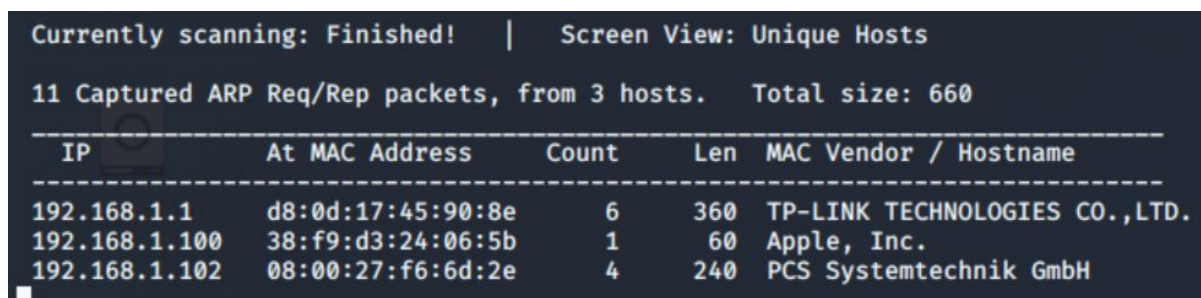


Roteiro 1 - Diário de bordo

Gabriel Monteiro

1.1A

Utilizando o comando “ifconfig” foi possível descobrir em qual subrede nossa máquina estava. Depois disso foi usado o comando “sudo netdiscover -r 192.168.1.0/24 -i eth0” para encontrar as máquinas presentes nesta subrede, como visto na imagem 1:

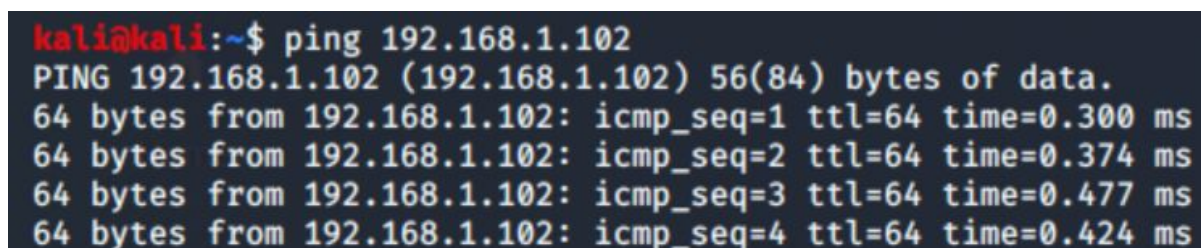


```
Currently scanning: Finished! | Screen View: Unique Hosts
11 Captured ARP Req/Rep packets, from 3 hosts. Total size: 660
```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	d8:0d:17:45:90:8e	6	360	TP-LINK TECHNOLOGIES CO.,LTD.
192.168.1.100	38:f9:d3:24:06:5b	1	60	Apple, Inc.
192.168.1.102	08:00:27:f6:6d:2e	4	240	PCS Systemtechnik GmbH

Imagem 1

Ao analisar as máquinas encontradas, é de nossa informação que o nosso alvo se trata de uma máquina com SO GNU/Linux, logo dos IPs encontrados um se trata de um dispositivo Apple com MacOS e 1 dispositivo se trata do roteador da minha casa da marca TP-LINK. Com isso dito, o provável IP do alvo é **192.168.1.102**. Apenas como medida de comprovação, é realizado o comando ping no provável alvo para se garantir que seu SO trata-se GNU/Linux. E como visto na imagem 2, é possível se comprovar isso pois seu TTL(Time-To-Live) é 64, valor característico deste SO:



```
kali@kali:~$ ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 192.168.1.102: icmp_seq=1 ttl=64 time=0.300 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=64 time=0.374 ms
64 bytes from 192.168.1.102: icmp_seq=3 ttl=64 time=0.477 ms
64 bytes from 192.168.1.102: icmp_seq=4 ttl=64 time=0.424 ms
```

Imagem 2

1.1B

Para reconhecer o nome e a versão do processo executado na porta 21 do alvo, foi necessário executar o comando “telnet 192.168.1.102 21”. O resultado está na imagem 3 abaixo:

```
kali@kali:~$ telnet 192.168.1.102 21
Trying 192.168.1.102 ...
Connected to 192.168.1.102.
Escape character is '^]'.
220 ProFTPD 1.3.5 Server (Debian) [::ffff:192.168.1.102]
```

Imagem 3

Como observado, a porta 21 é responsável por um servidor ProFTPD de versão 1.3.5.

1.1C

Para coletar mais informações sobre o SO foi utilizada a ferramenta nmap. O comando “sudo nmap -O -v 192.168.1.102” trouxe informações do SO(no modo verbose) como é possível ver na imagem 4:

```
Scanning 192.168.1.102 [1 port]
Completed ARP Ping Scan at 14:21, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:21
Completed Parallel DNS resolution of 1 host. at 14:21, 0.02s elapsed
Initiating SYN Stealth Scan at 14:21
Scanning 192.168.1.102 [1000 ports]
Discovered open port 139/tcp on 192.168.1.102
Discovered open port 21/tcp on 192.168.1.102
Discovered open port 22/tcp on 192.168.1.102
Discovered open port 111/tcp on 192.168.1.102
Discovered open port 80/tcp on 192.168.1.102
Discovered open port 445/tcp on 192.168.1.102
Discovered open port 15000/tcp on 192.168.1.102
Completed SYN Stealth Scan at 14:21, 0.09s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.1.102
Nmap scan report for 192.168.1.102
Host is up (0.00026s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
15000/tcp open  hydap
MAC Address: 08:00:27:F6:6D:2E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Uptime guess: 0.094 days (since Wed Feb 26 12:06:44 2020)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/./share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
Raw packets sent: 1023 (45.806KB) | Rcvd: 1015 (41.306KB)
```

Imagem 4

1.1E

As imagens 5 e 6 mostram as portas TCP e UDP abertas no alvo:

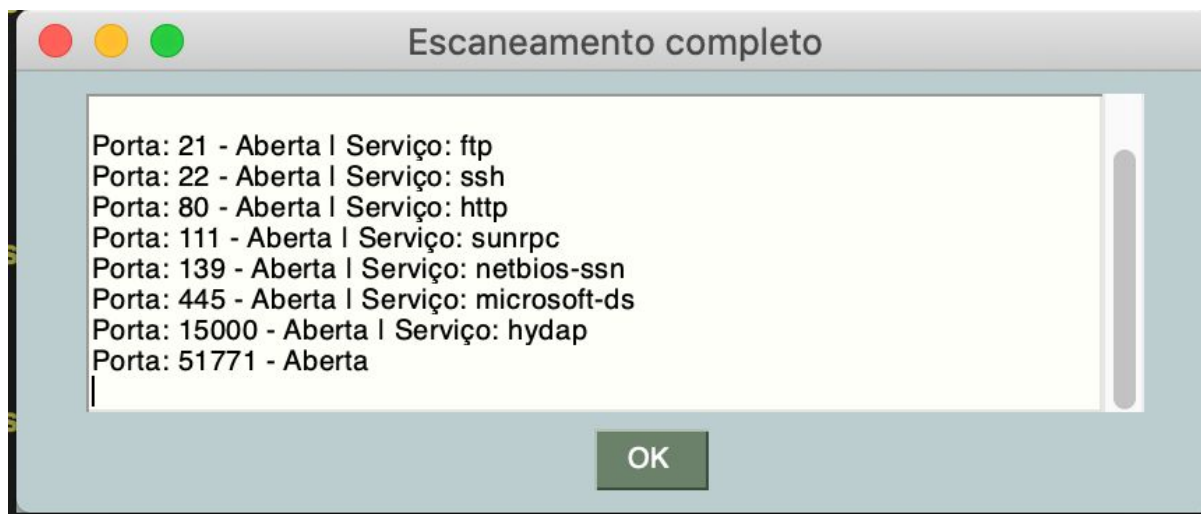


Imagem 5 - Portas TCP abertas no alvo

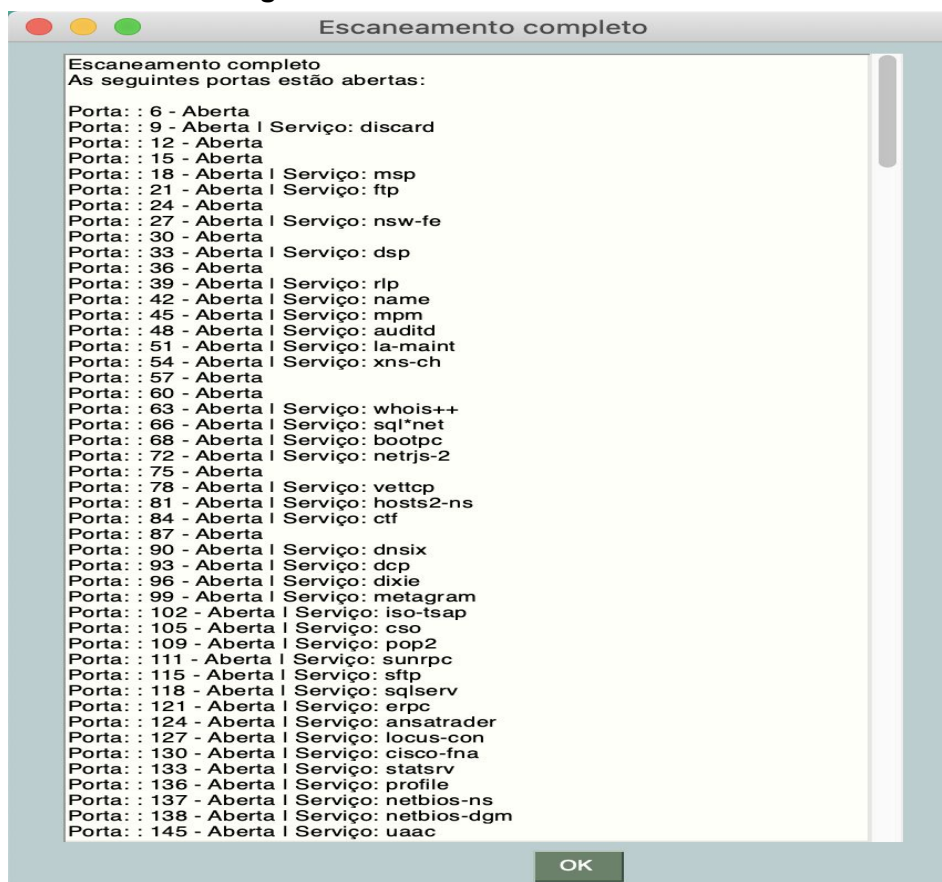


Imagem 6 - Portas UDP abertas no alvo(Muitas não couberam no print)

O serviço FTP trata-se de um protocolo de transferência de arquivos entre computadores onde a segurança é um dos seus principais problemas. Ao ter essa porta aberta, os dados trocados via esse protocolo estão sujeitos ataques dos tipos sniffing, spoofing, and brute force attack pelo simples fato de usar métodos de autenticação não criptografados.