

Setup:

Windows como hospedeiro, rodando uma VM do kali, com rede conectada a placa em modo bridge.

```
Connection-specific DNS Suffix . :  
IPv6 Address. . . . . : 2804:18:803:7b75:f5b8:1a0a:c50d:103f  
Temporary IPv6 Address. . . . . : 2804:18:803:7b75:b577:d8e2:42e1:816  
Link-local IPv6 Address . . . . . : fe80::f5b8:1a0a:c50d:103f%16  
IPv4 Address. . . . . : 192.168.43.157  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . : fe80::7e03:5eff:febd:2f4f%16  
192.168.43.1
```

Ipconfig no windows

```
kali@kali:~/Desktop$ /sbin/ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.43.18 netmask 255.255.255.0 broadcast 192.168.43.255  
    inet6 fe80::270e:bcca:c7c2:c6a6 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:10:13:24 txqueuelen 1000 (Ethernet)  
    RX packets 572 bytes 46766 (45.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 2407 bytes 156205 (152.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

/sbin/ifconfig no kali

Com o comando */sbin/ifconfig*, foi possível descobrir o ip da rede e o submask, que são necessários para o primeiro exercício.

Exercício 1.1.a: Descubra qual ip do seu alvo

Comando utilizado: *sudo nmap -sn 192.168.43.0/24* . Com esse comando foi possível listar todos os IPs sendo utilizados na redes e todos os MAC address dos respectivos IPs. Por exclusão (192.168.43.1 é o roteador; 192.168.43.157 é o hospedeiro; 192.168.43.18 é o próprio), o IP do alvo é 192.168.43.205, e seu MAC address é 08:00:27:B4:A6:BB.

```
kali@kali:~/Desktop$ sudo nmap -sn 192.168.43.0/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-20 12:10 UTC  
Nmap scan report for 192.168.43.1  
Host is up (0.097s latency).  
MAC Address: 7C:03:5E:FD:2F:4F (Xiaomi Communications)  
Nmap scan report for 192.168.43.157  
Host is up (0.00071s latency).  
MAC Address: 34:E1:2D:81:DE:3B (Intel Corporate)  
Nmap scan report for 192.168.43.205  
Host is up (0.0015s latency).  
MAC Address: 08:00:27:B4:A6:BB (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.43.18  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.91 seconds
```

Exercício 1.1.b: reconhecendo serviços e portas abertas do alvo.

Comando utilizado: *nmap 192.168.43.205 -p 21* . A porta 21 do alvo está aberta e rodando o serviço *ftp*.

```
kali@kali:~/Desktop$ nmap 192.168.43.205 -p 21  
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-20 12:25 UTC  
Nmap scan report for 192.168.43.205  
Host is up (0.00053s latency).  
  
PORT      STATE SERVICE  
21/tcp    open  ftp  
  
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

```
kali@kali:~/Desktop$ sudo nmap 192.168.43.205
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-20 18:15 UTC
Nmap scan report for 192.168.43.205
Host is up (0.00013s latency).
Not shown: 994 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
MAC Address: 08:00:27:B4:A6:BB (Oracle VirtualBox virtual NIC)
```

```
Not shown: 993 closed ports
PORT      STATE SERVICE
68/udp    open|filtered dhcp
111/udp    open      rpcbind
137/udp    open      netbios-ns
138/udp    open|filtered netbios-dgm
626/udp    open|filtered serialnumberd
5353/udp   open      zeroconf
44190/udp  open|filtered unknown
MAC Address: 08:00:27:B4:A6:BB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1086.39 seconds
kali@kali:~/Desktop$
```

Exercício 1.1.c: fingerprint.

Comando utilizado: `nmap -A 192.168.43.205`. Esse comando deu um monte de informação.

```
kali@kali:~/Desktop$ nmap -A 192.168.43.205
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-20 12:54 UTC
Nmap scan report for 192.168.43.205
Host is up (0.00034s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.7p1 Debian 5+deb8u7 (protocol 2.0)
|_ ssh-hostkey:
|_   1024 38:1c:57:f5:7f:71:8f:b8:84:96:41:75:37:a2:d1:d8 (DSA)
|_   2048 28:43:35:c6:a1:d1:9b:59:0e:76:cb:c2:fb:eb:31:78 (RSA)
|_   256  ad:98:ca:f7:3a:20:cc:83:3f:df:c4:2c:3c:70:3a:45 (ECDSA)
|_   256  88:ff:f9:47:b3:1e:cf:56:a7:b5:c8:98:d5:38:13:63 (ED25519)
80/tcp    open  http         Apache httpd 2.4.10 ((Debian))
|_ http-server-header: Apache/2.4.10 (Debian)
|_ http-title: Site doesn't have a title (text/html).
111/tcp   open  rpcbind      2-4 (RPC #100000)
|_ rpcinfo:
|_   program version  port/proto  service
|_   100000  2,3,4    111/tcp     rpcbind
|_   100000  2,3,4    111/udp     rpcbind
|_   100000  3,4      111/tcp6    rpcbind
|_   100000  3,4      111/udp6    rpcbind
|_   100024  1        35519/tcp   status
|_   100024  1        38435/tcp6  status
|_   100024  1        40680/udp   status
|_   100024  1        58241/udp6  status
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
Service Info: Host: DEBIAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```

Host script results:
  _clock-skew: mean: 1h00m00s, deviation: 1h43m55s, median: 0s
  _nbstat: NetBIOS name: DEBIAN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
  smb-os-discovery:
    OS: Windows 6.1 (Samba 4.2.14-Debian)
    Computer name: debian
    NetBIOS computer name: DEBIAN\X00
    Domain name: \x00
    FQDN: debian
    System time: 2020-02-20T09:54:14-03:00
  smb-security-mode:
    account_used: guest
    authentication_level: user
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
  smb2-security-mode:
    2.02:
      Message signing enabled but not required
  smb2-time:
    date: 2020-02-20T12:54:14
    start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.23 seconds
kali@kali:~/Desktop$

```

Exercício 1.1.d: criação de Escaneamento de Portas com Python.

Url do git: https://github.com/LiuSeeker/tech_hack

Exercício 1.1.e: utilização do Escaneador de Portas.

```

D:\7o-semester\hack\tech_hack\roteiro1-1>python scanner.py
Escolha a rede:
(0) 192.168.1.0
(1) 192.168.56.0
(2) 192.168.43.0
(3) 127.0.0.0
>> 2
Digite o range de ips a serem scaneados com traco (ex: 10-20)
>> 205-206
Scan de portas TCP (1) ou UDP (2):
>> 1
Digite as portas a serem scaneadas separadas por
      virgulas ou espaco e com traco em caso de range (ex: 1,3,10-20,30)
>> 20-25

Scaneando host 192.168.43.205
Port 20 (ftp-data) : Closed
Port 21 (ftp) : Open
Port 22 (ssh) : Open
Port 23 (telnet) : Closed
Port 24 : Closed
Port 25 (smtp) : Closed
Tempo scan: 0:00:08.015957

Scaneando host 192.168.43.206
Nao foi possivel conectar ao host
Tempo scan: 0:00:21.002363

D:\7o-semester\hack\tech_hack\roteiro1-1>_

```

Ao scanear o alvo apenas nas portas 20 a 25 como exemplo, o resultado foi como esperado, tendo apenas as portas 21 e 22 abertas.

Ao tentar scanear um host não existente, tenta-se fazer uma conexão com o host, porém há um timeout.