

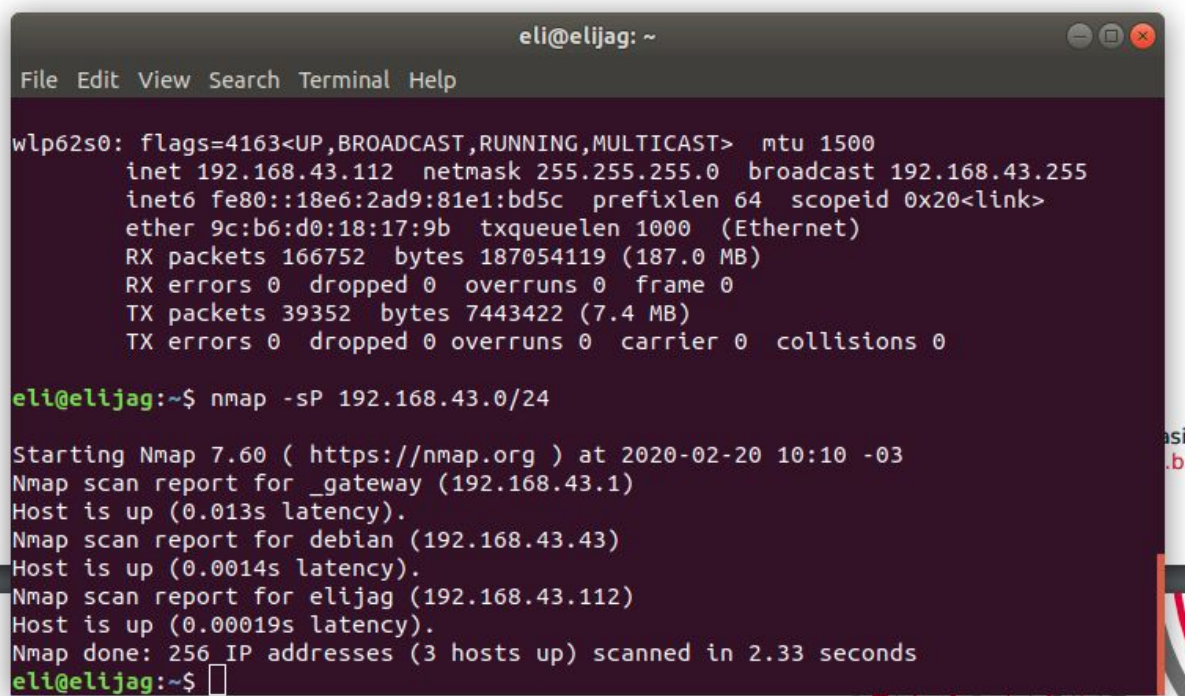
# Roteiro 1

## Eli Jose Abi Ghosn

**Exercício 1.1.a:** Descubra qual ip do seu alvo. Depois de importar a maquina virtual para o seu sistema descubra o endereço que este host recebeu em sua rede. Você já pode utilizar neste momento outra instância de máquina virtual com o Kali Linux e a partir dele utilizar as ferramentas e scripts que permitiram você executar os demais exercícios deste roteiro. Registre em seu diário de bordo, qual a técnica utilizada para resolver este exercício (print de tela com o comando, ferramenta ou script utilizado)

```
$ ifconfig
$ nmap -sP 192.168.43.0/24
```

Obs: *ifconfig* utilizado para descobrir a SubRede (192.168.43.0/24) na qual minha maquina esta.



```
eli@elijag: ~
File Edit View Search Terminal Help

wlp62s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.43.112 netmask 255.255.255.0 broadcast 192.168.43.255
    inet6 fe80::18e6:2ad9:81e1:bd5c prefixlen 64 scopeid 0x20<link>
    ether 9c:b6:d0:18:17:9b txqueuelen 1000 (Ethernet)
    RX packets 166752 bytes 187054119 (187.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39352 bytes 7443422 (7.4 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eli@elijag:~$ nmap -sP 192.168.43.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-02-20 10:10 -03
Nmap scan report for _gateway (192.168.43.1)
Host is up (0.013s latency).
Nmap scan report for debian (192.168.43.43)
Host is up (0.0014s latency).
Nmap scan report for elijag (192.168.43.112)
Host is up (0.00019s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.33 seconds
eli@elijag:~$
```

**\_gateway** - Roteador da sub rede

**elijag** - Host do meu computador

**debian (192.168.43.43)** - Host da máquina alvo

**Exercício 1.1.b:** Reconhecendo serviços e portas abertas do alvo. SEM utilizar uma ferramenta de escaneamento de portas e serviços descubra qual o nome e versão do processo que está executando na porta 21 do alvo. Evidencie o comando e sua saída no diário de bordo.

```
eli@elijag:~$ telnet 192.168.43.43 21
Trying 192.168.43.43...
Connected to 192.168.43.43.
Escape character is '^]'.
220 ProFTPD 1.3.5 Server (Debian) [::ffff:192.168.43.43]
ls
500 LS not understood

```

**Processo:** ProFTPD 1.3.5 Server

**Exercício 1.1.c:** Fingerprint é o nome dado a fase dentro de um pentest com o objetivo de identificar o sistema operacional do host alvo. Neste exercício você deverá descobrir o maior número de informações sobre o Sistema Operacional do host alvo como versão, distribuição e arquitetura. Registre no diário de bordo os comandos, ferramentas e scripts utilizados. Obrigatoriamente esta informações devem ser acessadas a partir do host do atacante (Kali).

```
$ ping 192.168.43.43
```

ttl = 64

Linux	64
Windows	128
Unix	255

```
$ nmap -A 192.168.43.43
```

```
eli@elijag: ~  
File Edit View Search Terminal Help  
|_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  
|   100024  1            37011/udp  status  
|_  100024  1            41591/tcp  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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Host script results:  
|_clock-skew: mean: -1s, deviation: 0s, median: -1s  
|_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: 2020-02-20T11:45:22-03:00  
|_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: 2020-02-20 11:45:22  
|_  start_date: 1600-12-31 20:53:32  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 11.87 seconds  
eli@elijag:~$
```

```
$ nmap -O 192.168.43.43
```

```

QUITTING!
eli@elijag:~$ sudo nmap -O 192.168.43.43
[sudo] password for eli:

Starting Nmap 7.60 ( https://nmap.org ) at 2020-02-20 11:53 -03
Nmap scan report for debian (192.168.43.43)
Host is up (0.00061s 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:A7:FB:7A (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 - 4.8
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.61 seconds
eli@elijag:~$ █

```

## Tarefa:

Você deverá realizar uma pesquisa dos módulos e bibliotecas que permitem o desenvolvimento de uma ferramenta para o escaneamento de portas TCP de acordo com as premissas a seguir:

- Ser em linguagem Python;
- Deverá possuir uma interface amigável e de fácil utilização (user-friendly interface);
- Permitir o escaneamento de um host ou uma rede;
- Permitir selecionar o Protocolo TCP ou UDP;
- Permitir inserir o range (intervalo) de portas a serem escaneadas;
- Além da função de escaneamento, espera-se que seu código relacione as portas Well-Know Ports e seus serviços, e apresente em sua saída (imprimir) o número da porta e o nome do serviço associado.

Github: <https://github.com/elijose55/Port-Scan>



```

eli@elijag:~/Desktop/TechHack/roteiro1$ python3 port_scanner.py -h
usage: port_scanner.py [-h] [-tcp] [-udp] [-port PORT] target

Simple Port Scanner by Eli

positional arguments:
  target          Specify target host to be scanned

optional arguments:
  -h, --help      show this help message and exit
  -tcp            Flag to select TCP Protocol (default = tcp)
  -udp            Flag to select UDP Protocol (default = tcp)
  -port PORT      Port range to scan (default = 0-65535). Expected forms like
                  0-65535 or 5000

eli@elijag:~/Desktop/TechHack/roteiro1$ python3 port_scanner.py 192.168.0.20
-----
Please wait, scanning remote host 192.168.0.20
-----
**Couldn't connect to port: 59552
PORT      STATE      SERVICE
-----
21/tcp    open      ftp
22/tcp    open      ssh
80/tcp    open      http
111/tcp   open      sunrpc
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds

TCP Scanning Completed in: 3.152 seconds

```

Arquivo port\_scanner.py com interface com -help, seleção de protocolo (TCP ou UDP) e seleção da faixa das portas.

**Exercício 1.1.e:** Utilizando sua ferramenta (port scan) descubra quais portas TCP e UDP estão abertas no alvo, bem como os serviços que estão associados nestes. Pesquise e anote em seu diário de bordo as vulnerabilidades comuns conhecidas (CVE) do processo que está gerenciando a porta 21. Observação: é obrigatório o uso da ferramenta desenvolvida no exercício anterior para a conclusão deste exercício. Evidencie por meio de prints e insira no diário de bordo.

```

eli@elijag:~/Desktop/TechHack/roteiro1$ python3 port_scanner.py 192.168.0.20
-----
Please wait, scanning remote host 192.168.0.20
-----
**Couldn't connect to port: 59552
PORT      STATE      SERVICE
-----
21/tcp    open      ftp
22/tcp    open      ssh
80/tcp    open      http
111/tcp   open      sunrpc
139/tcp   open      netbios-ssn
445/tcp   open      microsoft-ds

TCP Scanning Completed in: 3.152 seconds

```

Scan TCP

## Scan UDP

## Network Scan

## Vulnerabilidades Comuns Conhecidas (CVE)

[illegible]

Fonte: [https://www.cvedetails.com/vulnerability-list/vendor\\_id-2/FTP.html](https://www.cvedetails.com/vulnerability-list/vendor_id-2/FTP.html)

Fontes para o desenvolvimento do port\_scanner.py:

- <https://stackoverflow.com/questions/6512280/accept-a-range-of-numbers-in-the-form-of-0-5-using-pythons-argparse>
- <https://www.pythonforbeginners.com/code-snippets-source-code/port-scanner-in-python/>
- <https://pythonprogramming.net/python-port-scanner-sockets/>
- <https://docs.python.org/3/library/argparse.html>
- <https://docs.python.org/3/library/ipaddress.html>
- [https://www.python-course.eu/python\\_network\\_scanner.php](https://www.python-course.eu/python_network_scanner.php)
- <https://johanneskinzig.de/index.php/it-security/2-python-network-scanner>