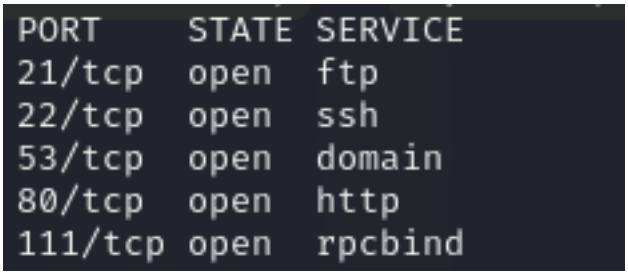
LAB - SEM 06 - SCANNING

LAB01: 21,22,53,80,111

Executamos o nmap varrendo em todas as portas com pacotes TCP

```
nmap -v -sT -p- businesscorp.com.br --open
```

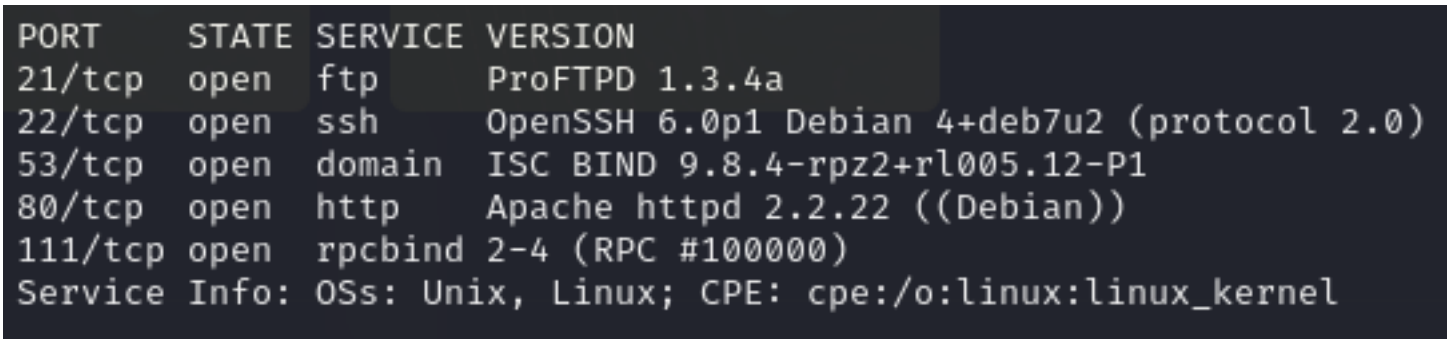


```
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
```

LAB02: bind9.8.4

Agora pedimos para o nmap interagir com os serviços

```
nmap -v -sTV -p 21,22,53,80,111 businesscorp.com.br
```



```
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     ProFTPD 1.3.4a
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
53/tcp  open  domain  ISC BIND 9.8.4-rpz2+rl005.12-P1
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
111/tcp open  rpcbind 2-4 (RPC #100000)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

LAB03: proftpd1.3.4a

Segue do lab passado

LAB04: vinteedois

Primeiramente usamos a ferramenta fping, que já automatiza
o exato processo solicitado: verificar quais host respondem ping

```
fping -a -g 172.30.0/24 > ativos_na172_30_0.txt
```

-a para verificar apenas os hosts que respondem
-g para designar o range
Em seguida, contamos as linhas do arquivo com o comando wc

```
wc ativos_na172_30_0.txt
```

LAB05: vinteetres

Usamos o nmap para fazer essa investigação com os seguintes parâmetros

```
nmap -sn 172.30.0.0/24 -oG hostativos_172_30
```

-o de output
-G de grepable
o último argumento é o nome do diretório que queremos que ele salve

Em seguida, fizemos um cut para limpar a resposta e encaminhamos
para o arquivo hostativos_172_30.txt

```
cat hostativos_172_30 | cut -d " " -f 2 > hostativos_172_30.txt
```

Por default, o arquivo vinha com os nomes "nmap" no topo e no fim
Retiramos com o editor nano e por fim contamos as linhas como feito anteriormente com o comando wc

LAB06: 172.30.0.103
Tentamos o filtro do ttl, mas todos tinham ttl de 63 ou 64
Tentamos o filtro do nmap mas tb n tivemos sucesso
Por fim, com o rdesktop obtivemos sucesso

```
for ip in $(cat hostativos_172_30.txt); do echo "tentando no $ip";
timeout 2s rdesktop $ip ; done
```

Verificamos que apenas o ip 130 ofereceu uma conexão disponível, o que indica a presença do windows

O teste do nmap, embora demorado, também acusou o OS

```
for ip in $(cat hostativos_172_30.txt); do nmap -v -O $ip -Pn; done
```

```
Nmap scan report for 172.30.0.103
Host is up (0.17s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8080/tcp open  http-proxy
Warning: OSScan results may be unreliable because we could not find at least 1
 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012 (86%)
```

LAB07: 135,139,445,2810,5985,8080
Executamos o teste mais demorado possível (pq eu ía lavar a louça)

```
nmap -v -sTV 172.30.0.103 --open
```

```
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2
 - 2012 microsoft-ds (workgroup: DHC17)
2810/tcp open  netsteward?
5985/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSD
P/UPnP)
8080/tcp open  http         Apache Tomcat/Coyote JSP engine
1.1
Service Info: Host: SRV01; OS: Windows; CPE: cpe:/o:microsof
t:windows
```

LAB08: 172.30.0.128

Pesquisamos no chatgpt quais as portas mais comuns para o serviço de email. A partir disso, fizemos a varredura usando o nmap:

```
nmap -p 25,587,110,143,465,993,995 172.30.0.0/24 --open
```

```
Nmap scan report for 172.30.0.128
Host is up (0.17s latency).
Not shown: 6 closed tcp ports (reset)
PORT   STATE SERVICE
25/tcp open  smtp
```

Apenas esse host foi setado.

LAB09: postfix

Identificamos o serviço utilizando o nmap na porta especificada no host achado no lab passado

```
nmap -v -sV -p 25 172.30.0.128
```

-v de verbose
-s de scan
-V de para saber o serviço/versão

```
PORT   STATE SERVICE VERSION
25/tcp open  smtp    Postfix smtpd
Service Info: Host:  ubuntu.bloi.com.br
```

LAB10: ubuntu

Segue do lab passado

LAB11: 172.30.0.20,172.30.0.104

Pesquisamos no chatgpt as portas mais comuns para execução do MySql e descobrimos que é a 3306 e a 1186. A partir disso, fizemos a varredura com o nmap:

```
nmap -v -p 3306,1186 172.30.0.0/24 --open
```

```
Nmap scan report for 172.30.0.20
Host is up (0.17s latency).
Not shown: 1 closed tcp port (reset)
PORT     STATE SERVICE
3306/tcp open  mysql

Nmap scan report for 172.30.0.104
Host is up (0.17s latency).
Not shown: 1 closed tcp port (reset)
PORT     STATE SERVICE
3306/tcp open  mysql
```

LAB12: 172.30.0.15

A porta padrão para execução do webmin é a 10000
Proesseguimos da mesma maneira do lab passado e apenas um host foi setado

```
nmap -v -p 10000 172.30.0.0/24
```