

# Estudo Técnico: Port Scanning

+ Vamos usar o **hping3**, que é um utilitário que nos permite enviar pacotes personalizados.

```
hping3 -c 1 --syn -p 80 businesscorp.com.br
```

→ o --syn é pra enviar uma flag SYN

```
(root@DESKTOP-NJHHNK6) - [/home/kali]
# hping3 -c 1 --syn -p 80 businesscorp.com.br
HPING businesscorp.com.br (wlan0 37.59.174.225): S set, 40 headers + 0 data bytes
len=44 ip=37.59.174.225 ttl=50 DF id=0 sport=80 flags=SA seq=0 win=14600 rtt=179.9 ms

--- businesscorp.com.br hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 179.9/179.9/179.9 ms
```

→ A resposta no campo flag=SA significa SYN / ACK, o que indica que completou o 3WS e, portanto, o serviço está ativo e a porta aberta

→ Caso a resposta fosse RA ( de RESET / ACK ), a porta estaria fechada

+ Podemos executar isso também usando o **nmap**, que é um scan conhecido de portas

```
nmap -sS -p 80 -Pn businesscorp.com.br
```

→ -s é de scan e -sS é de syn-scan (enviando pacotes SYN)

→ -Pn serve para que ele ignore se o host está ativo ou não

```
(root@DESKTOP-NJHHNK6) - [/home/kali]
# nmap -sS -p 80 -Pn businesscorp.com.br
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 19:35 -03
Nmap scan report for businesscorp.com.br (37.59.174.225)
Host is up (0.17s latency).
rDNS record for 37.59.174.225: ip225.ip-37-59-174.eu

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.63 seconds
```

→ Ele identificou a porta 80 como aberta

→ Caso executássemos na 81, ela seria dada como fechada

+ Há o caso de que a porta seja identificada como filtrada, conforme mostramos a seguir

```
File Edit View Search Terminal Help
root@pentest:~/Desktop# nmap -sS -p 23,80,8055 -Pn 172.16.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-19 19:57 -03
Nmap scan report for 172.16.1.5
Host is up (0.24s latency).

PORT      STATE SERVICE
23/tcp    filtered telnet
80/tcp    open  http
8055/tcp   closed  senomix04
```

+ Geralmente, as portas são dadas como fechadas se a resposta padrão for RST,

mas isso pode ocorrer de duas formas:

- ◇ A porta realmente está fechada
- ◇ Há um firewall agindo na porta que envia essa resposta

+ A porta é dada como filtrada (existe um firewall protegendo) se não vier resposta da flag SYN

Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.90.0.151	172.16.1.5	TCP	44	33545 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2	0.000221203	172.90.0.151	172.16.1.5	TCP	44	33545 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000369512	172.90.0.151	172.16.1.5	TCP	44	33545 → 8055 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	0.242477596	172.16.1.5	172.90.0.151	TCP	44	80 → 33545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1358
5	0.242504779	172.90.0.151	172.16.1.5	TCP	40	33545 → 80 [RST] Seq=1 Win=0 Len=0
6	0.242519079	172.16.1.5	172.90.0.151	TCP	40	8055 → 33545 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
7	1.971891767	172.90.0.151	172.16.1.5	TCP	44	33546 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

→ Nesse caso acima, veja que um pacote TCP SYN foi enviado duas vezes à porta 23, mas não houve resposta. Isso indica a ação de um firewall

+ Há um parâmetro no nmap que nos permite saber a razão da resposta que ele deu sobre o resultado do scanearmento, é o --reason

```
root@pentest:~/Desktop# nmap -sS -p 80 -Pn 172.16.1.5 --reason
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-19 20:02 -03
Nmap scan report for 172.16.1.5
Host is up, received user-set (0.27s latency).

PORT      STATE      SERVICE REASON
80/tcp    filtered  http    port-unreach ttl 63
```

+ Como resumo:

RESPOSTAS	
PORTA ABERTA	RESPONDE COM SYN / ACK (SA)
PORTA FECHADA	RESPONDE COM RST / ACK (RA)
PORTA COM FILTRO DE FIREWALL EM DROP	SEM RESPOSTA
PORTA COM FILTRO DE FIREWALL EM REJECT	RESPONDE COM UM ICMP PORT UNREACHABLE
PORTA COM FILTRO DE FIREWALL EM REJECT COM RST	RESPONDE COMO PORTA FECHADA (RST)