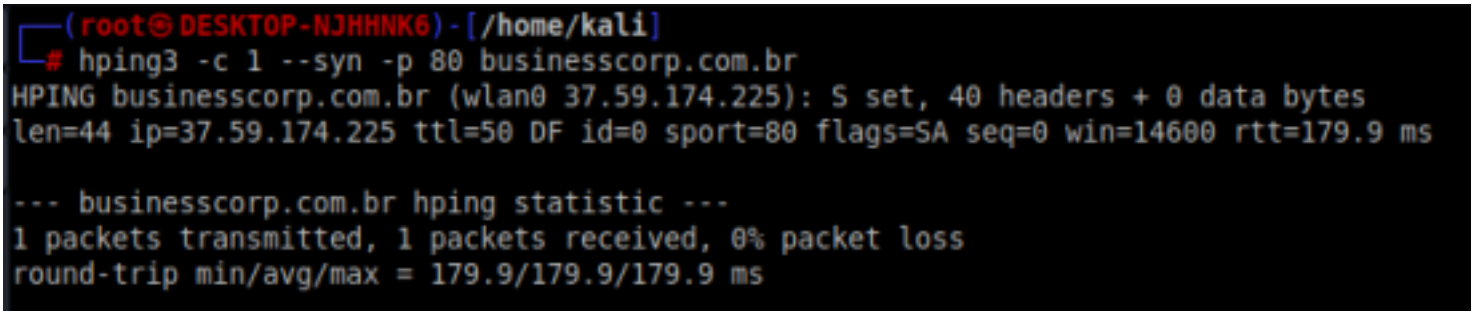
Estudo Técnico: Port Scanning

+ 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

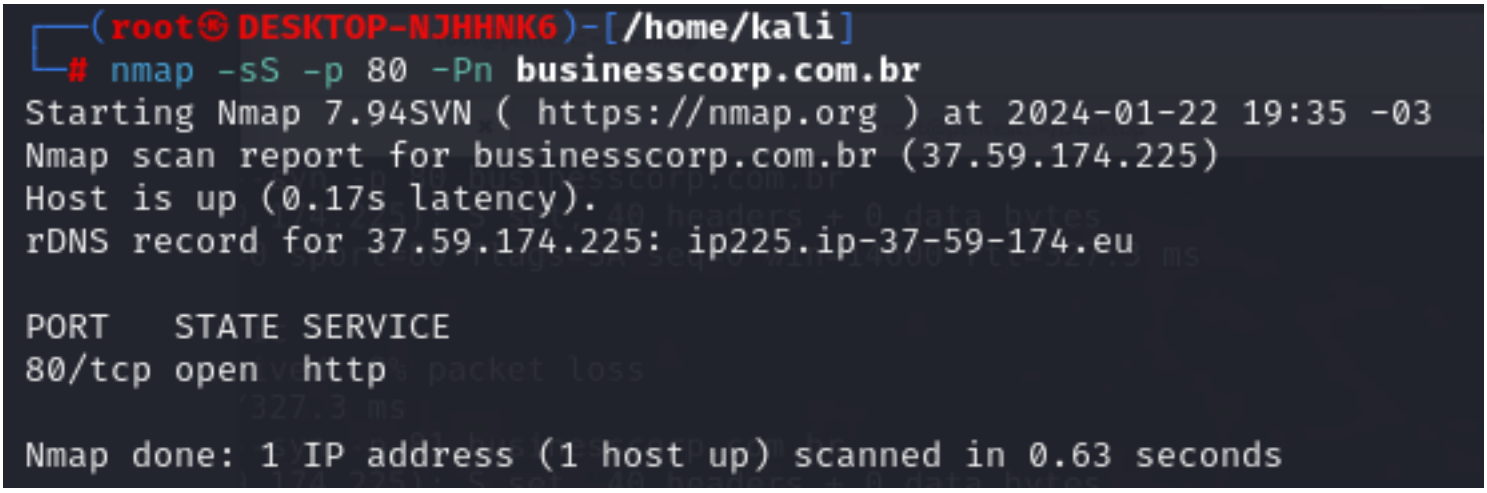


→ A resposta no campo flag=SA significa SYN / ACK, o que indica que completou o 3WHS e, portanto, o serviço está ativo e a porta aberta
→ Caso a resposta fosse RA (de RESET / ACK), a porta estaria fechada

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

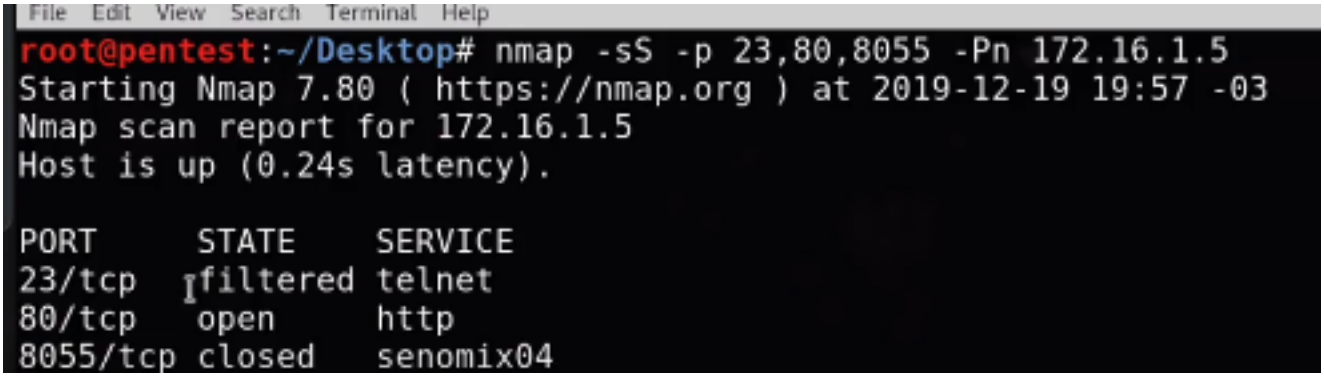
```
nmap -sS -p 80 -Pn businesscorp.com.br
```

→ -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



→ 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



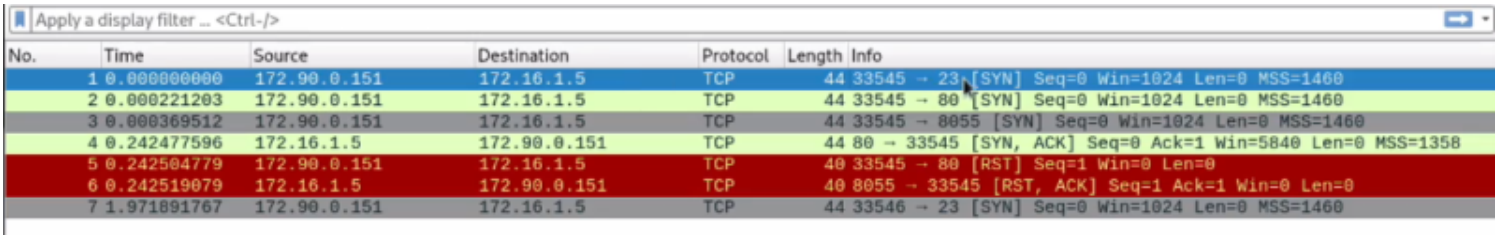
+ Geralmente, as portas são dadas como fechadas se a resposta padrão for RST,

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



→ 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 scaneamento, 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)