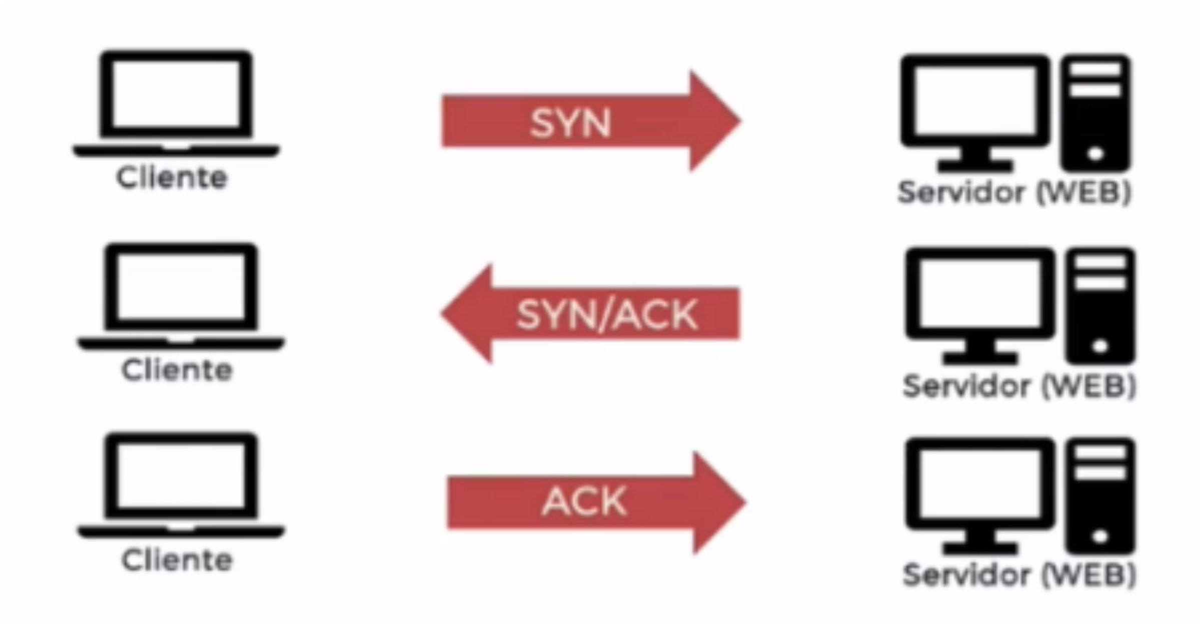
Diferenças entre os tipos de Scan

~~~~~~
Diferenças entre o TCP Connect e o SYN Scan
~~~~~~

+ TCP Connect
  ◇ Completa o #WHS
  ◇ Facilmente detectável e "barulhento"
  ◇ Consumo maior de tráfego na rede
  ◇ Após estabelecer o 3WHS, envia um RESET para encerrar a conexão



+ Half Open / SYN Scan
  ◇ Não completa o three-way handshake
  ◇ É mais furtivo que o TCP Connect
  ◇ Consome menos tráfego na rede

+ Veja que ambos os testes fornecem o mesmo resultado, que é o de

indicar que a porta 80 está aberta

```
root@pentest:~/Desktop# nmap -sT -p 80 -Pn 172.16.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-19 23:58 -03
Nmap scan report for 172.16.1.5
Host is up (0.33s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds
root@pentest:~/Desktop#
```

root@pentest: ~/Desktop

File Edit View Search Terminal Help

```
root@pentest:~/Desktop# nmap -sS -p 80 -Pn 172.16.1.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-19 23:58 -03
Nmap scan report for 172.16.1.5
Host is up (0.29s latency).

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.47 seconds
root@pentest:~/Desktop#
```

→ Mas a diferença repousa sobre o lado do servidor atacado, que não detecta tão facilmente o log via netcat

+ Segue abaixo o resultado do listening no servidor:

```
root@pentest:~/Desktop# nc -vnlp 5555
listening on [any] 5555 ...
connect to [192.168.0.11] from (UNKNOWN) [192.168.0.12] 38892
root@pentest:~/Desktop# nc -vnlp 5555
listening on [any] 5555 ...
```

→ Repare que no primeiro método (TCP Connect), pudemos visualizar quem logou na rede. Já no segundo, não.

+ Existe também uma maneira de fazer o teste com a flag FYN. Pode não ser tão efetivo

```
nmap -sF -p 80 -Pn 172.16.1.5
```