

TCP Host Scan

+ Da aula passada, aprendemos que o nmap realiza a varredura padrão nas 1000 portas mais comuns com o seguinte comando

```
nmap -v -sS -Pn 192.168.0.11
```

+ Porém, podemos realizar a mudança da porta de um serviço

→ Exemplo disso é o ssh, cujas configurações se encontram em /etc/ssh/sshd_config

→ Ao abrirmos elas com o nano, podemos mudar sua porta de funcionamento de 22 para outra qualquer, digamos 22999.



```
GNU nano 7.2 /etc/ssh/sshd_config
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
Include /etc/ssh/sshd_config.d/*.conf
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
```

→ Essa porta não seria mais capturada pelo nmap na configuração setada inicialmente

→ Para que a captura dessa porta possa ser feita mesmo depois de modificada, executamos

```
nmap -v -sS -p- -Pn 192.168.0.11
```