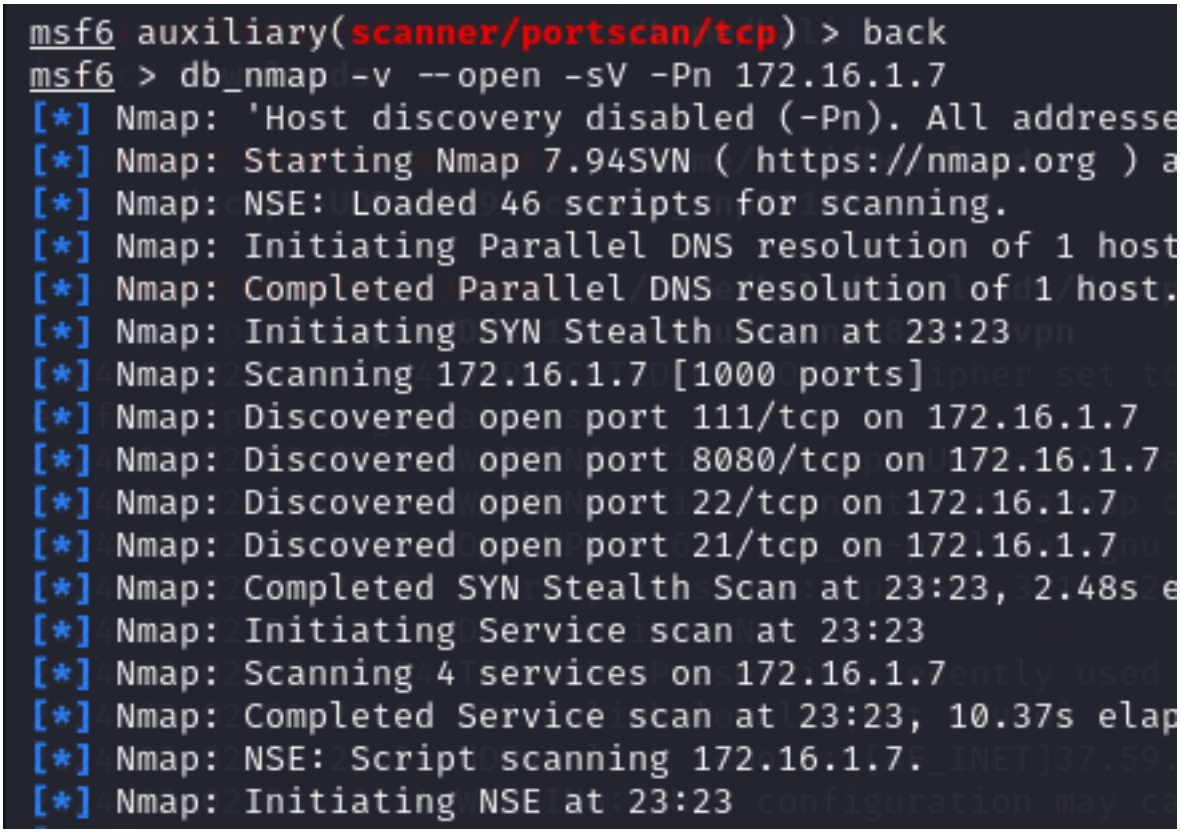
Trabalhando com a Base de Dados

+ Podemos usar o nmap da mesma maneira que usávamos fora do metasploit, com a única diferença que agora começa com db_nmap



+ Podemos também realizar a varredura fora do metasploit e depois importar o resultado pra dentro dele. Basta que durante a realização nmap, salvemos seu output em um arquivo xml

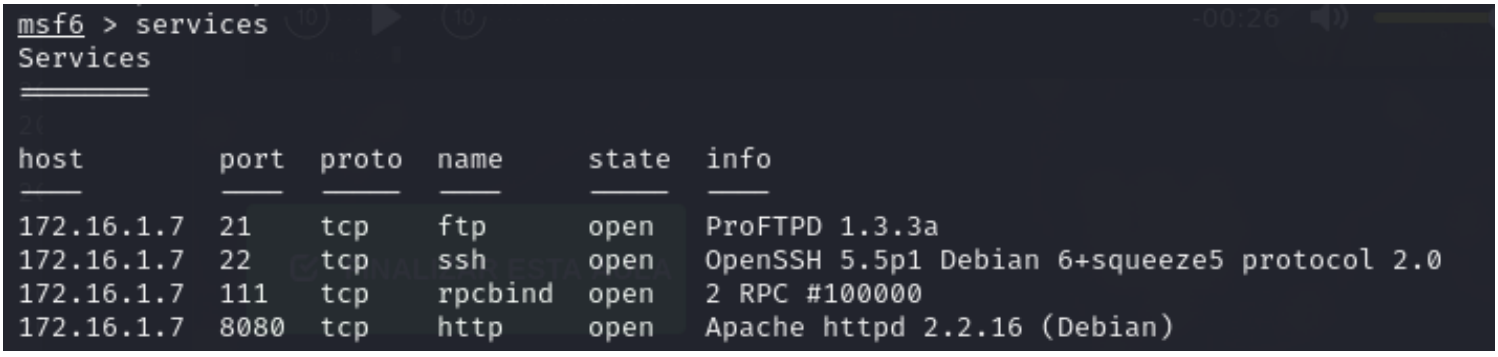
```
nmap -v --open -sV -Pn 172.16.1.4 -oX /opt/host4.xml
```

Agora, no metasploit:

```
db_import /opt/host4.xml
```

+ Para vermos o que já foi salvo de nossas varreduras, executamos

```
services
```



+ Para explorar vulnerabilidades de maneira automática, fazemos

```
vulns
```

→ Claro, os resultados só vão ser mais efetivos conforme formos

enumerando os serviços