Levantamento de Informações

+ O objetivo aqui é fazer uma varredura com o nmap do metasploit nos hosts com a porta 139 e 445 de toda a rede que estão abertas e, em seguida, identificar o sistema operacional que está funcionando neles

+ Para pesquisar módulos auxiliares que ajudem na detecção do smb, podemos:

```
search type:auxiliary smb
```

+ Vamos escolher o módulo que nos permite ver o serviço e a versão que estão rodando na máquina:

```
use auxiliary/scanner/smb/smb_version
```

+ Como temos muitos hosts scaneados, pra não passar cada um dos endereços de ip à mão, podemos

```
services -p 445 --rhosts
```

→ Isso irá armazenar todos os endereços desse ip em um arquivo que automaticamente será setado no nosso RHOSTS. Então, basta que apliquemos o run

+ Quando dermos o comando hosts (ou o services), veremos as versões dos serviços rodando por trás das portas