Identificando Vulnerabilidades

+ Identificados os serviços e as versões, podemos agora fazer a pesquisa por exploits.

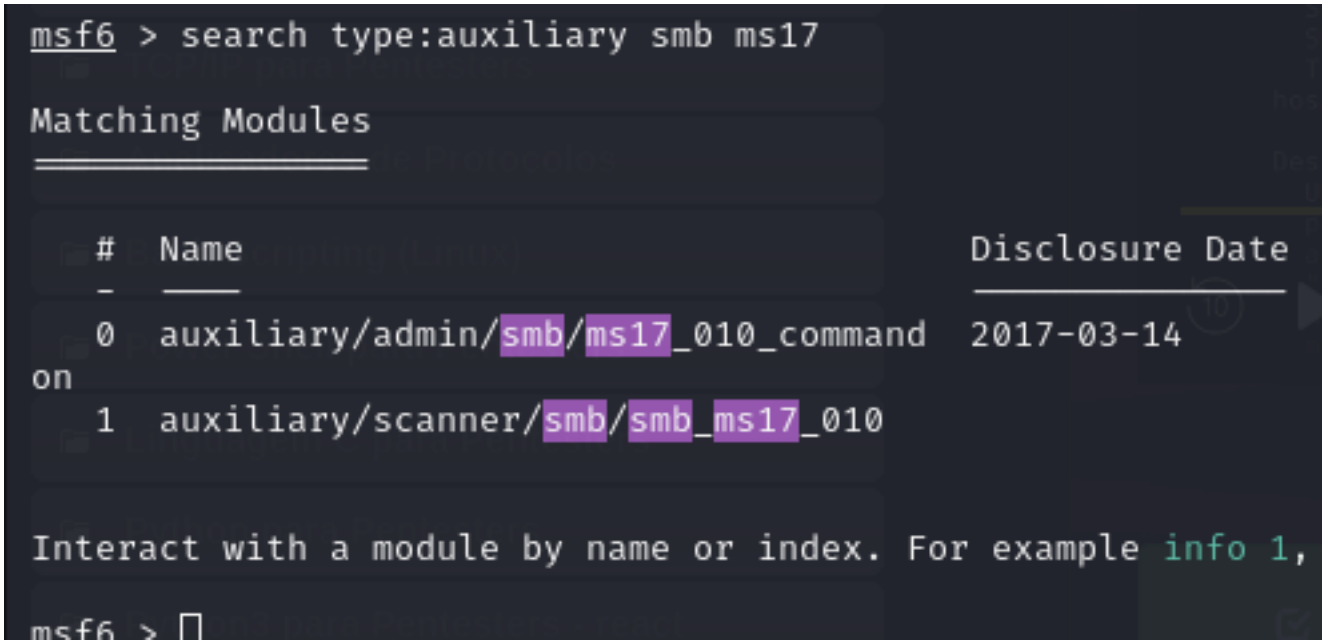
+ Invés de dar um info em cada um dos exploits relacionados, podemos pesquisar dentro das informações de cada exploit de maneira mais incisiva

+ Por exemplo, se queremos um exploit específico para o Samba 3.0.20

```
search type:exploit fullname:"Samba 3.0.20"
```

+ Se quisermos, por exemplo, um módulo auxiliar que busque pela falha ms17 (reportada pela Microsoft) em serviços smb, podemos

```
search type:auxiliary smb ms17
```



+ Para varrer os hosts já identificados em services que tenham essa falha

```
use auxiliary/smb/smb_ms17_010
```

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

+ Podemos verificar a inclusão do arquivo com os IPs no rhosts por meio do

```
show options
```

+ Por fim, damos o run