Enumerando as contas do AD

+ Nós temos duas credenciais com níveis diferentes de acesso

+ A partir disso, vamos interagir com os serviços usando o rpcclient

```
rpcclient -W orionscorp2 -U mfernanda 172.16.1.243
```

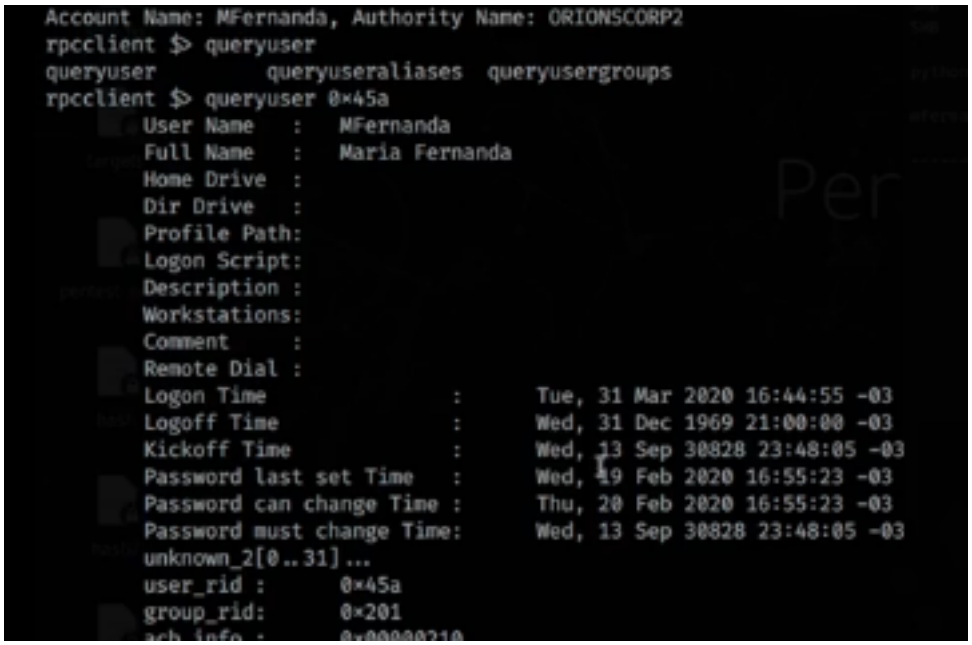
→ <passamos a senha >

```
enumdomusers
```

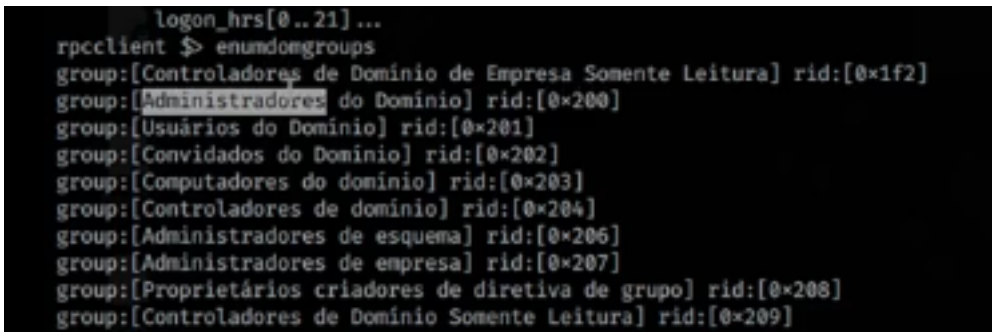
→ enumera os usuários

```
queryuser <rid do user>
```

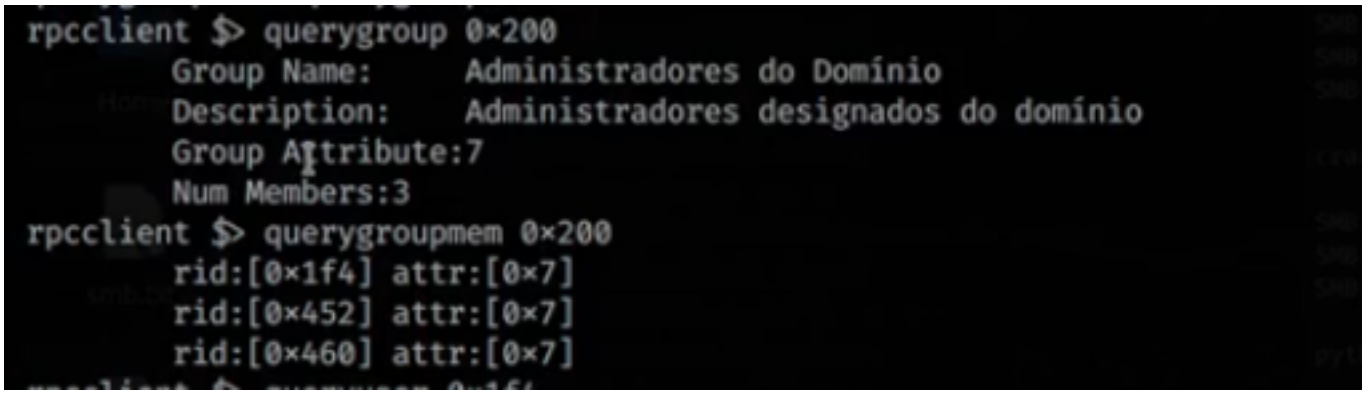
→ Traz informações mais detalhadas do usuário




```
enumdomgroups
```



→ enumera os grupos e controladores de domínio



→ Quando damos um querygroup 0x200 e depois querygroupmem, podemos ver quais os users de cada grupo por meio do seu rid

+ Todo esse processo tbm pode ser feito pela conta do jvitor :)