

# 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
```

```
root@pentesting:/home/desec/Desktop#  
Enter ORIONSCORP2\mfernanda's password:  
rpcclient $> enumdomusers  
user:[Administrador] rid:[0x1f4]  
user:[Convidado] rid:[0x1f5]  
user:[krbtgt] rid:[0x1f6]  
user:[Egabriel] rid:[0x452]  
user:[Abeatriz] rid:[0x455]  
user:[Jvitor] rid:[0x456]  
user:[MFernanda] rid:[0x45a]  
user:[ACosta] rid:[0x45d]  
user:[SQLService] rid:[0x460]
```

→ enumera os usuários

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

→ Traz informações mais detalhadas do usuário

```
Account Name: MFernanda, Authority Name: ORIONSCORP2  
rpcclient $> queryuser  
queryuser          queryuseraliases queryusergroups  
rpcclient $> queryuser 0x45a  
User Name       : MFernanda  
Full Name       : Maria Fernanda  
Home Drive      :  
Dir Drive       :  
Profile Path    :  
Logon Script    :  
Description     :  
Workstations    :  
Comment         :  
Remote Dial     :  
Logon Time      : Tue, 31 Mar 2020 16:44:55 -03  
Logoff Time     : Wed, 31 Dec 1969 21:00:00 -03  
Kickoff Time    : Wed, 13 Sep 30828 23:48:05 -03  
Password last set Time : Wed, 19 Feb 2020 16:55:23 -03  
Password can change Time : Thu, 20 Feb 2020 16:55:23 -03  
Password must change Time: Wed, 13 Sep 30828 23:48:05 -03  
unknown_2[0..31]...  
user_rid       : 0x45a  
group_rid      : 0x201  
local_auth_info : 0x00000210
```

```
enumdomgroups
```

```
logon_hrs[0..21]...  
rpcclient $> enumdomgroups  
group:[Controladores de Domínio de Empresa Somente Leitura] rid:[0x1f2]  
group:[Administradores do Domínio] rid:[0x200]  
group:[Usuários do Domínio] rid:[0x201]  
group:[Convidados do Domínio] rid:[0x202]  
group:[Computadores do domínio] rid:[0x203]  
group:[Controladores de domínio] rid:[0x204]  
group:[Administradores de esquema] rid:[0x206]  
group:[Administradores de empresa] rid:[0x207]  
group:[Proprietários criadores de diretiva de grupo] rid:[0x208]  
group:[Controladores de Domínio Somente Leitura] rid:[0x209]
```

→ enumera os grupos e controladores de domínio

```
rpcclient $> querygroup 0x200
Group Name:      Administradores do Domínio
Description:     Administradores designados do domínio
Group Attribute: 7
Num Members: 3
rpcclient $> querygroupmem 0x200
rid:[0x1f4] attr:[0x7]
rid:[0x452] attr:[0x7]
rid:[0x460] attr:[0x7]
```

→ 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 :)