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

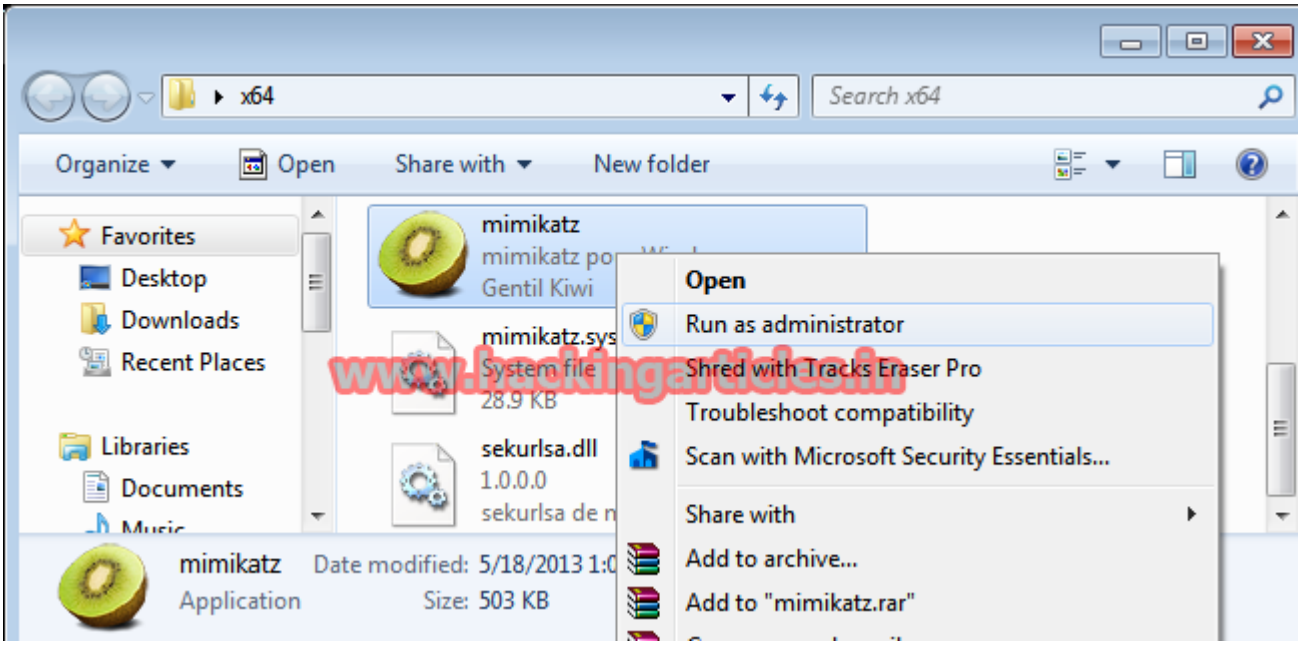
hackingarticles.in/hack-windows-password-in-clear-text-using-mimikatz-and-windows-credentials-editor

Raj December 10, 2015

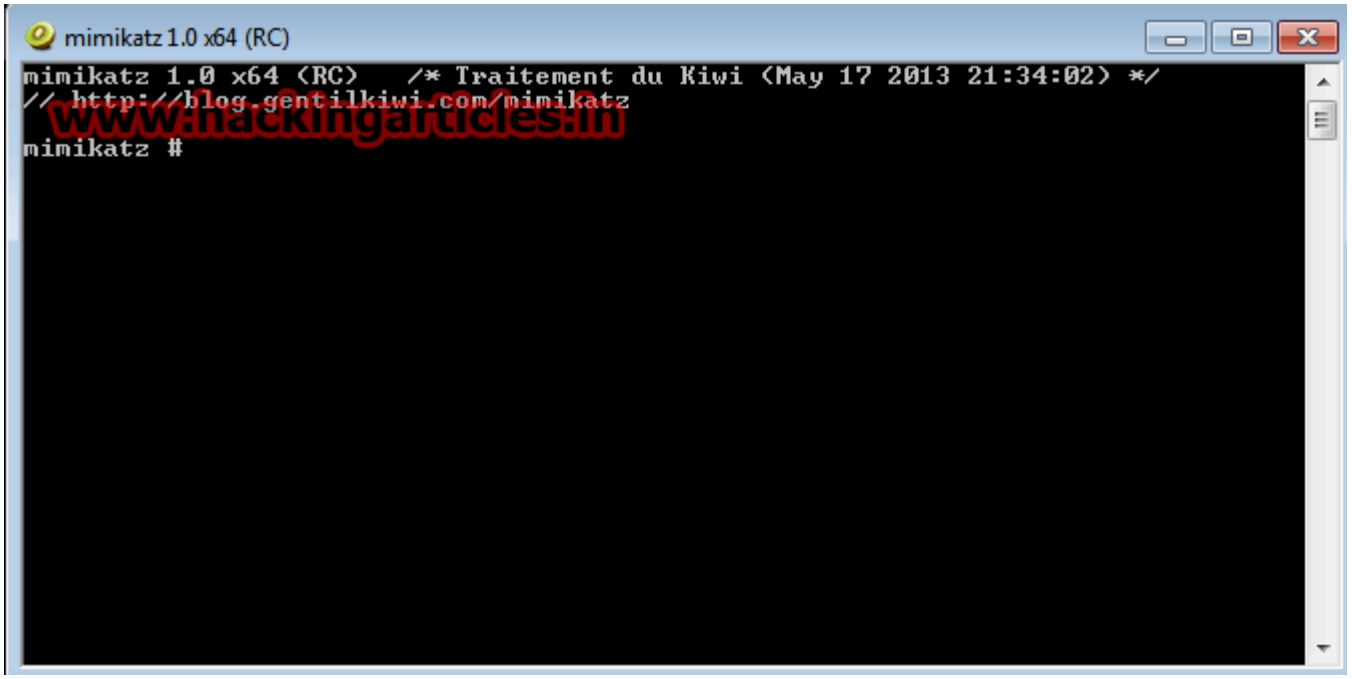
Mimikatz

mimikatz is a tool to check Windows security. It's now well known to extract plaintexts 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.

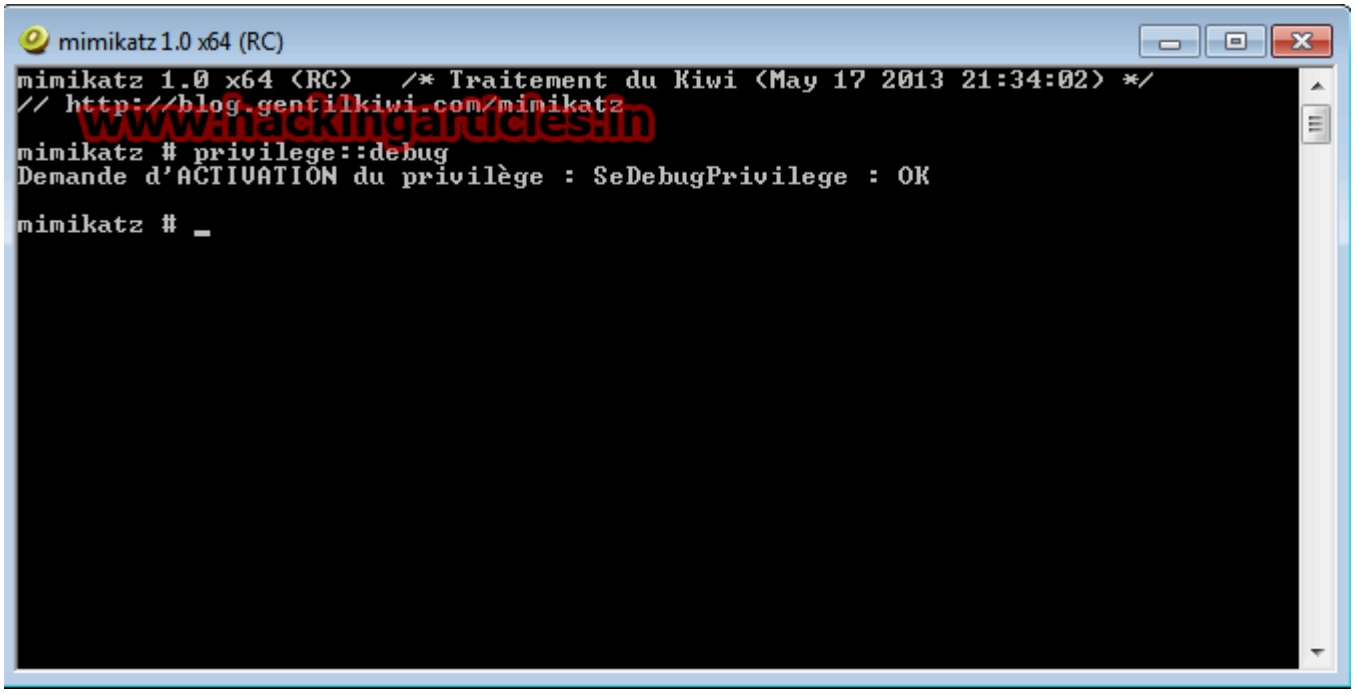


It will open mimikatz windows.



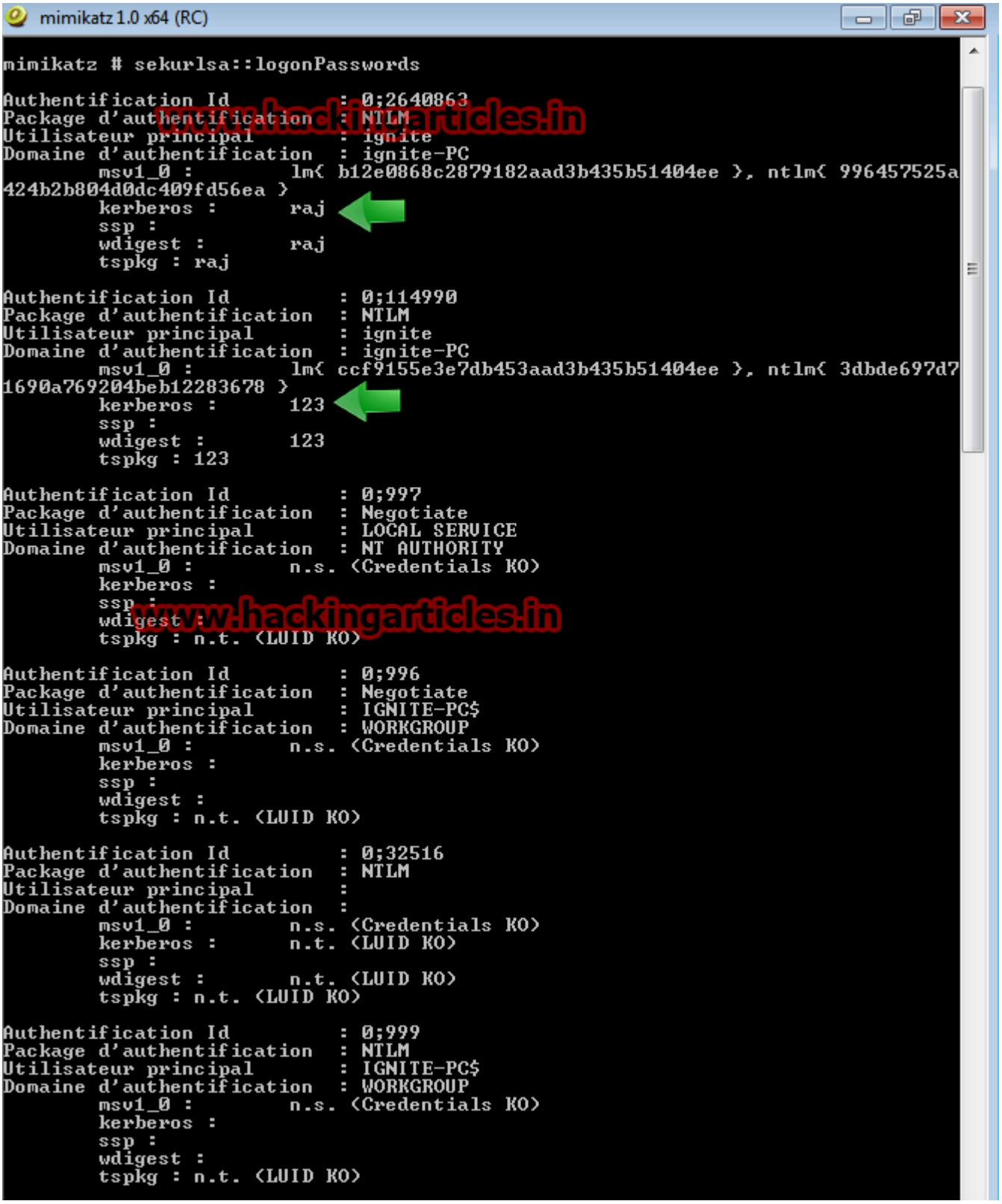
Type the following command to **check privilege**

privilege::debug



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

sekurlsa::logonPasswords



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.