

# New Windows tool - PWDumpX v1.0

Wednesday, 29 November 2006

## Description:

The PWDumpX v1.0 tool allows a user with administrative privileges to retrieve the encrypted password hashes and LSA secrets from a Windows system. This tool can be used on the local system or on one or more remote systems.

If an input list of remote systems is supplied, PWDumpX will attempt to obtain the encrypted password hashes and the LSA secrets from each remote Windows system in a multi-threaded fashion (up to 64 systems simultaneously).

The encrypted password hash information and the LSA secret information from remote Windows systems is encrypted as it is transferred over the network. No data is sent over the network in clear text.

This tool is a completely re-written version of PWDump3e and LSADump2 which integrates suggestions/bug fixes for PWDump3e and LSADump2 found on various web sites, etc.

Source code included.

## Credits:

My intent with including the source code along with this tool is to give something back to the I.T. security community. I learned a lot while creating PWDumpX but I could not have done it without the original source code for PWDump2, PWDump3e, and LSADump2. So...thanks to the creators of these tools for being generous enough to include the source code with these tools so that hungry minds can learn new things.