Windows PWDUMP tools

Hash Suite by Alain Espinosa
Windows 7 to 11 (64-bit), shareware, free or $39.95+

Hash Suite is a very efficient auditing tool for Windows password hashes (LM, NTLM, and Domain Cached Credentials also known as DCC and DCC2). It is very fast, yet it has modest memory requirements even when attacking a million of hashes at once. The GUI is simple, yet uses modern features offered by Windows 7 and above. Besides the password security auditing program itself, there's an included reports engine that generates reports in multiple formats, including PDF. (The reports engine requires free Java VM from Oracle to be installed.)

pwdump by Jeremy Allison
Windows NT, free (permissive BSD and GPL-compatible Open Source license)
Download local copy of pwdump (49 KB)

This handy utility dumps the password database of an NT machine that is held in the NT registry (under HKEY_LOCAL_MACHINE\SECURITY\SAM\Domains\Account\Users) into a valid smbpasswd format file (which is understood by practically all Windows password security auditing tools).

This is the original pwdump program. It is mostly of historical value these days. You will likely want to use a newer reimplementation such as pwdump6 instead. You might also be interested in our file archive with local copies of many pwdump-like and pwdump-related programs.

pwdump2 by Todd Sabin of Bindview
Windows NT/2000, free (GPL v2)
Download local copy of pwdump2 (46 KB)

This is an application which dumps the password hashes from NT's SAM database, whether or not SYSKEY is enabled on the system. NT Administrators can now enjoy the additional protection of SYSKEY, while still being able to check for weak users' passwords. The output follows the same format as the original pwdump (by Jeremy Allison) and can be used as input to password crackers. You need the SeDebugPrivilege for it to work. By default, only Administrators have this right, so this program does not compromise NT security.

pwdump3 and pwdump3e by Phil Staubs and Erik Hjelmstad of PoliVec, Inc.
Windows NT/2000, free (GPL v2)
Download local copies of pwdump3 version 2 (87 KB) and pwdump3e (217 KB)

pwdump3 enhances the existing pwdump and pwdump2 programs developed by Jeremy Allison and Todd Sabin, respectively. pwdump3 works across the network and whether or not SYSKEY is enabled. Like the previous pwdump utilities, pwdump3 does not represent a new exploit since administrative privileges are still required on the remote system. One of the largest improvements with pwdump3 over pwdump2 is that it allows network administrators to retrieve hashes from a remote NT system.

pwdump3e provides enhanced protection of the password hash information by encrypting the data before it is passed across the network. It uses Diffie-Hellman key agreement to generate a shared key that is not passed across the network, and employs the Windows Crypto API to protect the hashes.

pwdump4 by bingle
Windows NT/2000, free (GPL v2)
Download local copy of pwdump4 (72 KB)

pwdump4 is an attempt to improve upon pwdump3. It might work in cases when pwdump3 fails (and vice versa).

pwdump5 by AntonYo!
Windows NT/2000/XP/2003, free
Download local copy of pwdump5 (28 KB)

pwdump5 is an application that dumps password hashes from the SAM database even if SYSKEY is enabled on the system. If SYSKEY is enabled, the program retrieves the 128-bit encryption key, which is used to encrypt/decrypt the password hashes.

pwdump6 by fizzgig
Windows 2000/XP/2003/Vista, free (GPL v2)
Download local copy of pwdump6 1.7.2 in ZIP (1268 KB) or tar.bz2 format (1103 KB)

pwdump6 is a significantly modified version of pwdump3e. This program is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether SYSKEY is enabled. It is also capable of displaying password histories if they are available. Currently, data transfer between the client and target is NOT encrypted, so use this at your own risk if you feel eavesdropping may be a problem.

pwdump7 by Andres Tarasco Acuna
Windows NT family (up through XP or Vista?), free
Download local copy of pwdump7 revision 7.1 (505 KB)

pwdump7 works with its own filesytem driver (from rkdetector.com technology) so users with administrative privileges are able to dump directly from disk both SYSTEM and SAM registry hives. Once dumped, the SYSKEY key will be retrieved from the SYSTEM hive and then used to decrypt both LanMan and NTLM hashes and dump them in pwdump like format.

Quarks PwDump originally by Sebastien Kaczmarek of Quarkslab
Windows XP/2003/Vista/7/2008/8, free (GPL v3)
Original source code on GitHub (no pre-compiled binary, outdated) by Quarkslab
Revised source code on GitHub (with pre-compiled binary in Releases) by red canari
Download local copy of Quarks PwDump 0.3a by red canari (369 KB) or its source code (5.6 MB including a prerequisite library)

Quarks PwDump extracts local accounts NT/LM hashes + history, domain accounts NT/LM hashes + history, cached domain password, Bitlocker recovery information (recovery passwords & key packages). It requires administrator privileges.

pwdump8 by Fulvio Zanetti and Andrea Petralia of blackMath
Windows 2000/XP/Vista/7/2008/8/8.1/10/2012/2016/2019, free
Download local copy of pwdump8 8.2 (529 KB)

pwdump8 supports AES-128 encrypted hashes and thus works on Windows 10 v1607 and later, where the previous pwdump tools fail. pwdump8 works with the local Windows system, as well as with dumped SAM and SECURITY reg hives. Version 8.2 adds support for domain cached account. pwdump8 requires administrative privileges, just like the previous tools did.

mimikatz by Benjamin DELPY `gentilkiwi`
Windows (up to latest builds of Windows 10), free (CC BY 4.0)

mimikatz is a well-known advanced tool 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*. mimikatz is an actively maintained Open Source project.

Offline NT Password & Registry Editor by Petter Nordahl-Hagen
Windows NT to 8.1 (32- and 64-bit), freeware

This is an utility (available in the form of bootable floppy and CD images) to reset the password of any user that has a valid (local) account on your NT system, by modifying the password hash in the registry's SAM file. You do not need to know the old password to set a new one.

The editor works offline, that is, you have to shutdown your computer and boot off a floppy disk or a CD. The boot disks use Linux as the OS and include stuff to access NTFS partitions and scripts to glue the whole thing together.

This will also work with SYSKEY, including the option to turn it off.

3804804
