

Re: Storing passwords

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.win2000.security/2002-10/10286.html>

From: Karl Levinson [x y] MVP (jamescagney90210@excite.com)

Date: 10/27/02

From: "Karl Levinson [x y] MVP" <jamescagney90210@excite.com>

Date: Sun, 27 Oct 2002 07:30:13 -0500

"Lem Lo" <lemlo@yahoo.com> wrote in message
news:ee0e01c27d84\$6fdd14b0\$36ef2ecf@tkmsftngxa12...
> *Hello. I was wondering if anyone knew how the user and*
> *administrator passwords are stored? Is there a danger of*
> *someone being able to read them from a hard disk?*

Yes, absolutely, though it probably requires special tools, the Windows passwords themselves are generally not stored in plaintext unless you have set the computer to log in as you automatically or you are using third party software that uses passwords.

The passwords for Windows 2000 / XP / NT are stored encrypted in a file called SAM [unless the computer is joined to a Windows 2000 Active Directory domain, in which case some of the passwords are stored elsewhere]. L0phtcrack from www.l0pht.com is one of the more common cracking tools, though there are other free ones. [along with PWDUMP / PWDUMP3 which is used to dump the contents of the SAM] NTFSDOS from www.winternals.com can be used for free to read the SAM file from an NTFS formatted hard drive if someone has physical access to your computer [or if the hard drive is formatted in FAT instead of NTFS, you just boot to a regular DOS boot floppy to get the file]. There are also a number of boot disks that can be used to blank out the administrator password to be able to log into your computer without knowing the password.

On the other hand, depending on your environment, this may or may not be the security issue you need to worry about most. Generally a lot of hacking is done because a machine is missing the latest microsoft security patches or is not configured securely.

More information can be found by searching www.google.com for SAM or any of the other keywords here. The book Hacking Exposed 3rd edition is a good introduction to a variety of security issues affecting Windows. There are also a number of checklists on how to secure or harden Windows computers at www.microsoft.com/technet/security, www.nsa.gov, <http://rr.sans.org>, www.google.com, etc. Be sure to also secure IIS if IIS is installed.

microsoft.public.win2000.security: Re: Storing passwords

Here's too much information, in case i