Hacking Into Your Own PC

From Fred Langa (Langa Plus)

It's an adage among computer security professionals: If someone has unlimited electronic or physical access to your PC, then given enough time, money, talent and effort, they can break in. This is true for any OS, bar none: Windows, Linux, Mac, whatever.

But the reverse also is true: If you limit easy electronic and physical access to your PC, you can keep essentially all casual hackers at bay, and seriously impede even professional-level data thieves. For example, you can help control electronic access to the system with good firewalling and network practices (see Firewall Feedback

http://www.informationweek.com/story/IWK20020412S0009 and How Much Security Is Enough? http://www.informationweek.com/840/langa.htm), and you can control physical access through simple expedients such as locking your office door; or, if that's not an option, through BIOS-level passwords, security access keys, "dongles" and the like. (Examples: http://www.google.com/search?q=usb+security+access+key)

However, all that security can come back to haunt you if you forget your password(s), or if you legitimately need to access someone else's password-protected PC. This happens fairly frequently in totally above-board circumstances such as when a worker or family member has become ill or incapacitated, and has left behind a password-protected PC; in cases where simple user-error has caused someone to forget his or her own password; and so on.

If you have a legitimate need to access a password-protected PC, then you probably also have unhindered physical access to that system. That means that for you--- unlike the hackers and crackers who should not have easy access to the system--- it's not that hard to hack into the system and reset or otherwise bypass the passwords.

In the article now posted at InformationWeek.Com (http://www.informationweek.com/story/showArticle.jhtml?articleID=13100343), we'll sample some of the very best tools available to solve the most common types of OS- and application-level password problems in XP. Then we'll also discuss resources for an enormous range of tools that can solve almost any password-related problem.

Click on over to http://www.informationweek.com/story/showArticle.jhtml?articleID=13100343 , and you may never have to worry about lost passwords again!

Langa Letter: Managing Your Windows XP Passwords

Lightweight Approaches: Resetting User Account Passwords
First, if you have access to any XP admin-level account on the machine in question, and need to gain entry to any other user account, the simplest method is via XP's built-in "userpasswords2" function: Click Start/Run, and in the Run box, type "control userpasswords2" without the quotes. A window will open showing you all accounts on the system. You can then use the "reset password" button to change any or all of the passwords on the system, even if you don't know the current password.

In some XP systems joined to Domains, and in some versions of XP Home, the direct approach of using "Control Userpasswords2" won't work. In these instances you have to edit the accounts conventionally via the Control Panel "User Accounts" applet, accessed from an admin-level account. This is less convenient, but still works fine.

The XP Help system and the Microsoft Knowledgebase both contain abundant additional information on this simplest form of resetting passwords. See these articles at Microsoft Service and Support".

Heavy-Duty Password-Resetting Tools
Ironically, Linux offers perhaps the easiest way to reset any XP account's password, including the Administrator account. (In XP Home, the Administrator account is normally so well hidden that many XP Home users don't even know that their system has an Administrator account, but it does.)

The very best tool I've found is the free "Offline NT Password & Registry Editor Bootdisk." Even though its name says "NT," it actually works fine on NT, Win2K, XP Pro, and XP Home.

The tool can run from a floppy or CD, and is a series of highly automated scripts that lets you easily change the password of any user account on an NT/2K/XP box. You don't have to know the existing password to make the change, and the tool will even detect locked or disabled accounts and offer to unlock or re-enable them.

The "Offline NT Password & Registry Editor Bootdisk" is so well done that using it is often just a matter of accepting the defaults and hitting Enter when asked. But it's also flexible enough that you can break out of the automated process to accommodate whatever machine-specific idiosyncrasies you may encounter. Although the tool is almost two years old, the Web page still describes it as "very alpha," which I have to assume is the author's extreme programmatic conservatism because the software's never even hiccupped when I've used it. It's worked smoothly every time.

If the main site above doesn't have enough how-to information for you to use the "Offline NT Password & Registry Editor Bootdisk," this independent site has additional information.

A similar Linux-based tool is the Trinity Rescue Kit http://trinityhome.org/trk/index.html , based on Mandrake 9.1. Broader in scope than the "Offline NT Password & Registry Editor Bootdisk," the Trinity Rescue Kit "... is designed to rescue/repair/prepare dead or damaged systems, be it Linux or Windows. It has networking capabilities like SSH, samba, and FTP and supports about every network card, disk controller, and USB controller. You can use it to repair a Windows 2000 or Windows XP system by setting the chkdisk flag or editing the registry or just reset the administrator password (or any other user). You can even undelete files from an ntfs, ext2, or fat partition ..."

Both the above tools are self-contained: You boot to the tool's own environment and work from there on the affected system. A somewhat less-direct option is the LAN-based freeware "NT Toolkit", a small suite of utilities optimized for password administration via a local network. The tools of primary interest are ServiceSecure ("allows you to reset service passwords by specifying the username and password rather than having to specify the service names themselves or changing the password manually"), and Password Assistant ("a GUI application that lets you update passwords of user accounts on multiple

Windows NT, Windows 2000, or Windows XP machines. A good example is updating the Administrator password on all of your network workstations.")

Password Recovery Tools, Especially For Applications
At the applications level, it's usually simpler and easier to reveal or recover an existing, forgotten password than to use a brute-force method to reset or delete the password.

The simplest form of password revealers show you what's behind the asterisks or black circles that some software uses to hide typed-in passwords: The password-revealer software turns the asterisks or black circles back into plain text, so you can see and copy down what the password is, simple as that.

One of the most popular tools is the free, oddly-named "SnadBoy Revelation." http://www.snadboy.com/ I've used this tool several times with excellent results. For example, I recently set up a new PC for a user who wasn't physically present to tell me her passwords for services she needed, such as Dial-Up Networking. I installed SnadBoy's Revealer on her old PC, grabbed the passwords, and used them to set up her new PC so it would work identically to her old system, minimizing her relearning/rekeying time.

There are many similar tools, too, some more sophisticated, others even simpler. For a sampling, see Iopus' commercial password recovery tool, or its simpler, free version ; or try this Google search.

Tool To Prevent Password Problems
All the above deal with after-the-fact problems: Cases where a password was lost, forgotten, or is otherwise unavailable.

But XP offers a preventive measure that, if used beforehand and with extreme care, can avoid most or all of these kinds of problems with user-account passwords. It's the "Password Reset Disk," a floppy you can make via XP's "Forgotten Password Wizard." This tool creates a small file called userkey.psw on a floppy; this file can later be read by the Forgotten Password Wizard to reset the password for whatever account originally created the psw key.

This is very handy--and very dangerous. Anyone with access to the Password Reset Disk can use it as a kind of skeleton key to access whatever account created the disk. In a way, it's much the same as if you posted your password on a sticky note attached to your monitor.

So, if you're going to create a Password Reset Disk, you need to ensure that the floppy is stored securely and away from the PC that created it, and, ideally, is labeled with an obscure, nonobvious name--not "Password Reset Disk!"

It's easy to create a Password Reset Disk; the process is well documented in the XP help files and on the Microsoft site.
https://www.microsoft.com/technet/prodtechnol/winxppro/proddocs/windows_password_resetdisk_overviewW.asp

http://www.informationweek.com/security/mra**Myriad Additional Resources** The tools we've discussed so far are among the best of the best, but there's an entire universe of additional tools out there that can help you solve almost any kind of password-related problem.

For example, "Password Recovery Resources" lists some 80 password tools and sites, many of which offer still more tools and links to other sites. One such link of special note is "Cmos, LILO, NT passwords - Data recovery" which contains a nicely focused selection of tools for the purposes suggested by the page's name.

A bulletin-board system discussion called "Lost windows XP Home edition Password" lists numerous sites and tools specific to that purpose; an article called "Fixing Your Admin Password (Windows XP Home Edition)" covers similar ground in a more do-it-yourself manner.

A Google search will lead you to many tools for XP Pro and XP Office.

The "Ultimate Boot CD" comes with a copy of the "Offline NT Password & Registry Editor" mentioned earlier, and many other tools besides.

The "Linux NT Toolkit" is a free bootable floppy image you can use to reset the passwords on an NT/2K/XP box, but it's a bare-bones tool that requires a fair amount of prior knowledge to use.

In contrast to the above, the "Windows XP/2000/NT Key" is far more polished and easier to use--but it costs $195. You can try it for free to reset a "demo" password only, but you have to pay full price to make changes on real accounts.

For unusual and narrower kinds of password problems, try the Microsoft Knowledgebase. For example, you may get an error message stating "The Password Is Not Valid" when you log onto the XP Recovery Console, even when you know that the password is OK: That error is covered in this article.

Finally, and most generally, you'll find links to an enormous array of "Security Resources for Administrators" here.

Your Turn

What password-recovery sites or resources do you use? Which tools have you found to be particularly useful, powerful, or easy to use? Do you know of tools that are better than the ones Fred suggests? Please join in the discussion!