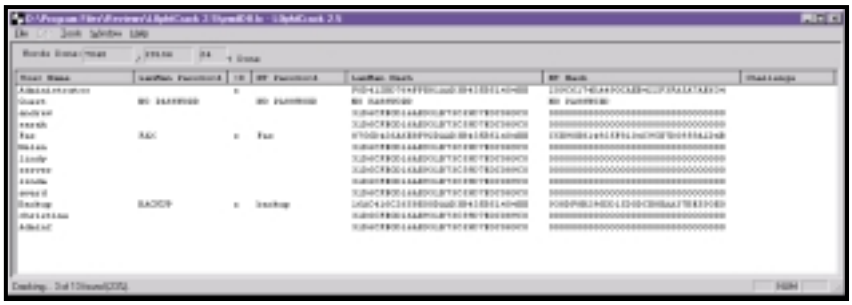
Packs, cracks and hacks

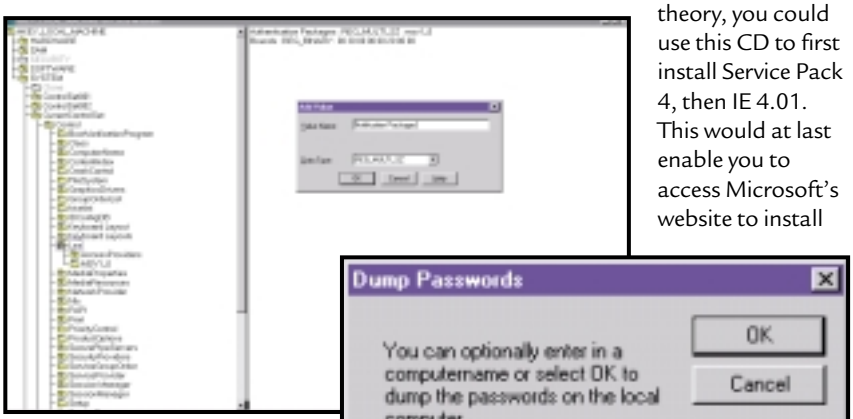
Andrew Ward recommends having the latest service pack CD handy and cracks a few passwords.

If you work with Windows NT systems, make sure that you always have a CD containing the latest service pack, because if you ever have to install or reinstall Windows NT4 and you only have the original release CD, you'll be in trouble. This may seem pretty obvious, but when you're faced with an emergency situation and only have the Windows NT4 CD, the facility to install a service pack over the Internet might seem to be a useful way out. It isn't.

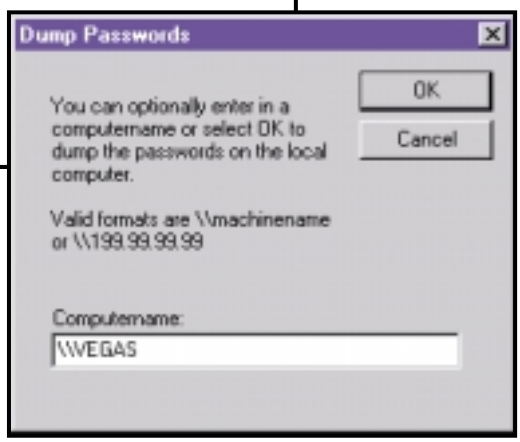
In the past, I've used the version of Internet Explorer that comes with Windows NT to go to Microsoft's website in order to download the current service pack. However, the Microsoft website is now one of the few sites on the Internet that you can't access at all with IE 2.0 – the version that shipped on the NT4 CD. Netscape, Novell and AOL are fine – although amusingly, Oracle's website will be just as inaccessible to you as Microsoft's.



L0phtCrack cracked these rather obvious passwords almost immediately



You can add a password filter to stop users choosing passwords that are too easy to guess



L0phtCrack will even retrieve passwords from a remote registry

Even if you could somehow gain access to Microsoft's website in order to upgrade to the latest version of IE, you wouldn't be able to install it, since IE5 requires Service Pack 3 or higher. The other alternative that might occur to you is to download the service pack from Microsoft's FTP site – but unfortunately, all that you'll find there is a text file referring you back to the website.

There are a number of other CDs you might have in your possession that include intermediate versions of IE, and service packs prior to 6A. For example, there is a CD that includes Service Pack 4 and IE 4.01 with Service Pack 1. In theory, you could use this CD to first install Service Pack 4, then IE 4.01. This would at last enable you to access Microsoft's website to install Service Pack 6, and finally upgrade IE 4.01 SP1 to IE5. However, by the time you'd done all that, the system would probably be in the sort of unstable mess that caused you to reinstall the operating system in the first place.

More lost passwords

A reader who wishes to remain anonymous suggests alternative methods in the saga of retrieving lost administrative passwords. He recommends the use of tools that work out Windows NT passwords for you, by using a variety of different cracking techniques. These tools can be surprisingly good, in these days of fast processors. For example, his colleagues in the IT department apparently still use numeric-only passwords – these take less than three minutes to crack.

Of course, passwords are never going to be a particularly good security solution, but for most of us, we have to make the best of a bad job. One of the first things we can do to try to encourage a better choice of password by users is to install the password filter that's been included with Windows NT since Service Pack 2. This helps to address the problem that many users opt for standard English words, which are easily guessed by humans or machines.

To implement the password filter, copy the file passfilt.dll into the %systemroot%\system32 directory, usually \winnt\system32. You then need to do some registry editing, and this must be done in regedt32 rather than regedit, since it requires creating a value of type REG_MULTI_SZ, something that regedit doesn't support.

Using regedt32, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa and there create a new value (using Edit / New value) called 'Notification Packages' of type REG_MULTI_SZ. This value

contains a list of DLL notification packages (and you may find that there is already one or more installed). Set the value to 'PASSFILT' – if there is already something installed, add 'PASSFILT' beneath it.

The filtering function only takes place on the computer that houses the updated account. You should, therefore, normally install the filter on the PDC and every BDC for a domain, or every system in a workgroup.

Notification packages include (among others) a PasswordFilter function, which is called whenever a password change has been requested. This could be activated at account creation, administrative password override or simply when the user is changing the password. However, if you still have 16bit Windows clients, these do not generate password notification events when users change passwords.

If PasswordFilter returns TRUE, the password is considered valid. You can write your own password filter if you don't think the standard one is good enough – details and sample code are provided in the Microsoft Knowledge Base (search for 'passfilt').

The standard password filter that comes with the service packs implements the following rules: Passwords must be at least six characters long and must contain characters from at least three of four classes. These classes are English upper case letters, lower case letters, numerals and non-alphanumeric characters such as punctuation symbols. Passwords may also not contain your user name or any part of your full name.

When Service Pack 2 was released, it was believed that passwords corresponding to these rules would be secure from a dictionary attack and would take several days to crack by brute force. Of course, times have changed. With L0phtCrack and a modern system – even if you don't yet have a 1GHz processor – you can sometimes even do the job overnight. In addition to setting up a password filter, you could therefore consider using L0phtCrack to ensure that your user passwords really do require an all-night run, and that they aren't guessable within seconds.

L0phtCrack computes NT user passwords using the hashed values stored by NT. L0phtCrack can recover passwords directly from the registry, from the file system and backup tapes, from repair disks or even by recovering the passwords as they travel across the network.

Once L0phtCrack has extracted the hashed values, it works out the passwords using three different methods, the fastest of which is a dictionary attack. L0phtCrack tests all the words in a dictionary or word file against the hashed passwords. Although L0phtCrack does ship with a small word file, you can do better with a larger file – easily found on the Internet.

Finally, L0phtCrack uses the brute force method, which will always recover the password

Then, L0phtCrack moves on to the hybrid crack method, which builds upon the dictionary method by adding numeric and symbol characters to dictionary words, since many users choose passwords that are really just dictionary words slightly modified with additional numbers and symbols. This shows up the weakness of the standard password filter supplied by Microsoft – many passwords will pass the filter, but will give way to a hybrid crack in seconds.

Finally, L0phtCrack uses the brute force method, which of course will always recover the password, whatever it happens to be. The secret here is to ensure that your password policy expiration time is set to be shorter than the time it takes to crack the passwords that your users choose! Using a tool such as L0phtCrack is really the only method of finding out what is a sensible expiration time to choose.

L0phtCrack is available from www.l0pht.com (note that that is a figure zero, not a letter O).

Resource kit query

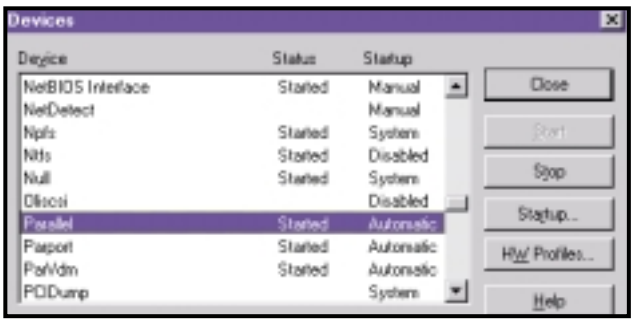
There is always interest in the resource kit, and from time to time people write in to ask whether it is downloadable from Microsoft's website. I'm afraid I might have misled one or two people by suggesting that it is.

In fact, what is downloadable is a subset of the tools to be found in the resource kit, that are either new or have been updated from previous releases. See: www.microsoft.com/ntserver/nts/downloads/recommended/ntkit/default.asp.

Failed printing

L Michael Hohmann writes in to ask what could cause the error message 'The system cannot find the file specified' when trying to print. Unable to solve the problem for the parallel port, he had to resort to a serial to parallel converter in order to continue to work.

This error occurs if the parallel port driver parallel.sys is not started for some reason. Usually, this is because NTDETECT failed to find a valid parallel port. The first thing to do is use the Devices control panel to see if the driver has started or not. If not, try starting it manually. If you receive error 20 (hardware not detected), then you know it couldn't find the port.



Ensure that the parallel printer device driver is actually running

Windows NT4 doesn't support EPP or ECP bi-directional communication ports, and so the cause could simply be the port is set in the wrong mode. Otherwise, there could be a variety of system BIOS settings that result in the problem – such as moving the port to a non-standard address.

CONTACTS

PCW welcomes your comments on the Windows NT column. Contact us via the *PCW* editorial office or email **nt@pcw.co.uk**