Security audit: user plaintext passwords in OS Windows

Passcape Software

1 Security audit: user plaintext passwords in Windows OS

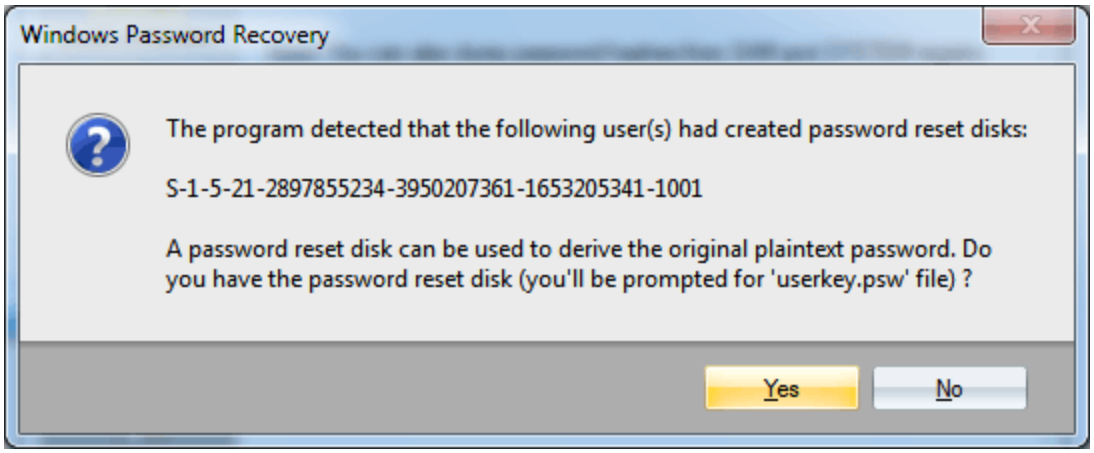
Is your Windows logon password 30 characters long? Sorry to break it to you, but it's useless. Any intruder with physical access to your account can get his hands on your password without too much trouble.

The Windows operating system was originally designed not to store user passwords openly, but to use one-way functions (OWF), also known as hash functions. For example, the password **test** produces a 16-symbol string **0CB6948805F797BF2A82807973B89537** or, more precisely, a hash that is additionally encrypted using the SYSKEY utility and stored in the SAM registry file that is accessible to the system only. If you know the password, you can generate its hash; but you cannot restore the password from the hash. This is why the hashing functions are also known as one-way functions. When the user logs into the system, the password is verified thusly:

- The user enters a text password that is then hashed.
- The resulting hash is compared against the reference hash stored in the SAM registry.
- If the hashes match, the password entered is considered correct.

What is the most effective way to restore the original password from its hash? We will devote a separate series of articles to this vast subject. We will now discuss a somewhat different issue. Namely: Is there any way to get the original text password of a user who has logged into his account? The answer to this question has always been academically definitive: There is not, because the text password entered by the user is wiped after being verified, and only its hash is used after that. This is what theory would have us believe. Yet this theory is not all that watertight in practice, as it turns out that the original password can be restored ... wait for it ... from several different locations in the system! For example, arguably the most powerful password audit application, Windows Password Recovery, can restore and decrypt original text passwords using various methods:

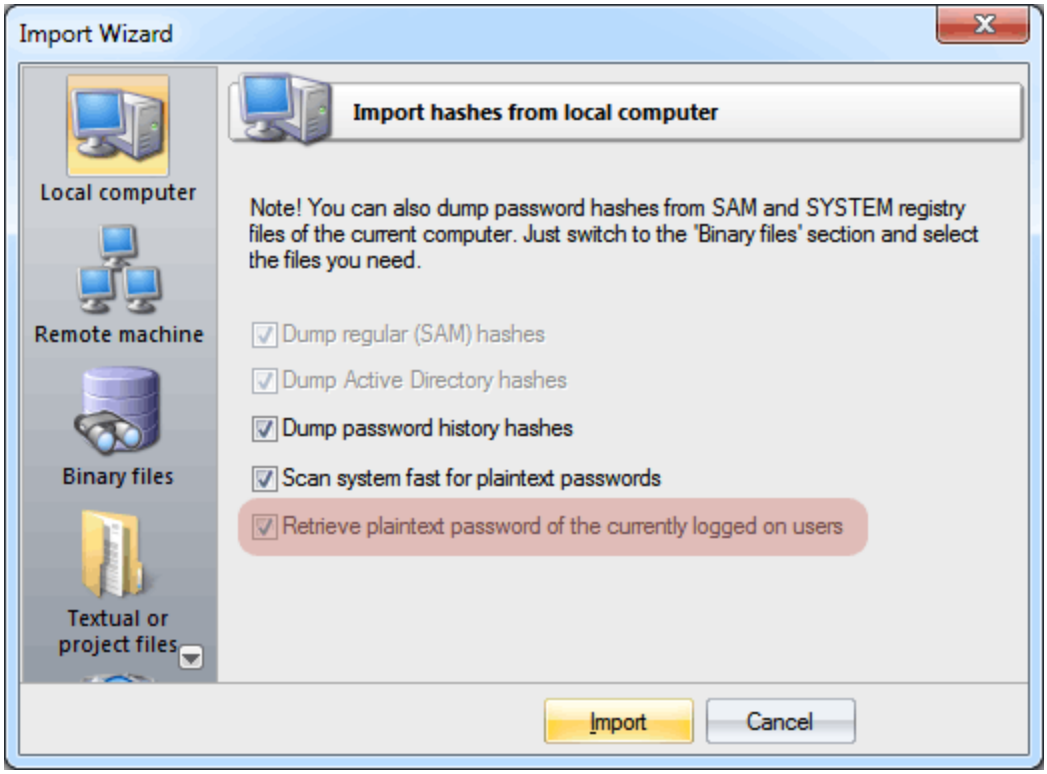
- An unobfuscated user password in Windows 2000 can be easily retrieved by generating a simple system memory dump.
- In the HKLM registry tree, old Windows versions used to store passwords for automatic system logon if the relevant option was enabled.
- LSA secrets. It's an open secret (excuse the tautology) that LSA secrets also store personal data for automatic logon. In some cases, the original plaintext password is saved to the secrets even if the automatic system logon option is NOT enabled. This is a known issue which Microsoft has been struggling with for many years now. Our team has found that it is also present in the beta version of Windows 8.
- The secrets store text passwords of some system accounts as well as those of services that are launched.
- Plaintext user passwords can be stored in a domain if the reverse encryption option is enabled.
- In the beta version of Windows 8, the plaintext user password can be easily extracted out of the Windows Vault. Let us hope that password security will be enhanced in the final version of Windows 8.
- A password reset disk (if one has been created) can be used to decrypt (specifically decrypt, not reset) the user password, which in this case is stored in the registry in encrypted form, while the decryption key is stored on the reset disk.



Pic 1. Decrypting user plaintext password using Password Reset Disk

We now get to the most important part. It turns out that in all Windows versions beginning with Windows XP, the text password of the logged-in user, which is used by certain authentication protocols, such as WDigest or TsPkg, is encrypted in system memory using a block cypher, and therefore can be decrypted! The new version of Windows Password Recovery can cope with this non-trivial albeit realistic mission. To run an ordinary security audit of your system, it suffices for the computer administrator to launch the application and attempt to perform a local import of passwords, and draw the appropriate conclusions based on its results.

Recovering Windows plaintext password



Pic 2. Recovering user logon passwords

To enhance the security of your PC, we recommend enabling the option whereby the SYSKEY is stored on the startup disk or using the SYSKEY bootup password. While this will not render the decryption of the password of an already logged-in user impossible, this will prevent physical access to your computer even if a potential intruder manages to get his hands on your logon password.