

Re: Gaining Administrator Access to Windows XP Professional SP2 Sy

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-02/msg00868.html

- *From:* "Steven L Umbach" <n9rou@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 24 Feb 2006 18:04:15 -0600
-

That was true in Windows 2000 but not in Windows XP. If a local user account password is reset an attacker will NOT be able to logon with the reset password and access the EFS encrypted files. Now an attacker could logon as an administrator, install a password hash cracking program to try and recover a user's password and then logon with the correct password to access the files. If you use complex passphrase of at least 15 characters [which also disables it from being stored with lm hash] then it will become almost impossible to recover your password. If you export and delete your EFS private key and assuming non other can decrypt the files then the files are safe from opening and the only possibility would be to try and brute force AES 256 encryption which is not going to happen anytime soon. Ideally for maximum confidentiality you want to run cipher /w after deleting the EFS private key to overwrite free disk space to eliminate any traces of the private key or clear copies of the EFS files if any existed. Users that logon with cached domain credentials have there passwords stored very securely and they are not stored in the local sam. I have yet to hear of a verified successful attempt to recover such though an atacker could resort to simple guessing and maybe get lucky. --- Steve

"stephen-robertson" <stephenrobertson@xxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message <news:D6EE89C6-5E5E-4620-A269-DB0DFD39E4FE@xxxxxxxxxxxxxxxxxxxx>

I do encrypt my data, and I did not create any Designated Recovery Agent for EFS. Otherwise, if I did lose the laptop and someone gained Administrator access to the system, that person could then decrypt my data. Even if the Administrator account is not a Designated Recovery Agent, someone could simply change the passwords of every user account on the system, log in to each one, and attempt to decrypt the data. If another user account was a Designated Recovery Agent, eventually the encrypted data would become accessible.

Stephen

Re: Gaining Administrator Access to Windows XP Professional SP2 Sy