“HOW TO” make a new password on Windows 7, when the old is lost

In Windows 7, Microsoft has been so "smart" to give access to a BAGDOR, so anyone can get on a PC if you sit with the keyboard in front of them. This certainly applies to Windows 8, and maybe other versions of Windows. This is NOT a question of HACKING this PC in any way, but solely and only re-establishes a lost connection.

When the PC starts up and asks for password, there should be at least 2 choices,

1. Administrator
2. Standard user

Default user is usually named by a name. Both accounts should be protected with a strong password to maintain security against 90% of VIRUS and MALWARE trying to intercept the Internet.

Most users have probably not detected that in the lower left corner of this LOGIN image there is an ICON that shows "Increased availability" when you move the mouse over it and pressing it will display a nice menu with Different choices. One of these options is the selection of the SCREEN KEYBOARD, which is started by the OSK.EXE program, located in **c: \ windows \ system32>**.

Now, the idea is that we need this command OSK.exe to start another command instead of CMD.EXE or COMMANDPROMPT, and this is done by Rename CMD.EXE to OSK.EXE.

If COMMANDPROMPT is started before anyone is logged on to the computer, it receives SYSTEM ADMINISTRATOR rights, and may Change user access codes, with some DOS commands.

(DOS = Disk Operating System, is an old Microsoft system that still exists in the latest Windows versions.)

Then we start:

BOOT PC from your Recovery CD, as follows:

Insert RecoveryBOOT CD and REBOOT PC - Press F12 to select BOOT from CD.

Select: "**Windows Setup [EMS Enabled]"**

Under "**System Recovery and Language Selection**" press "**Next**".

The system will now search for recovery files and the system to be restored.

Select the option:

"**Restore your computer using a system image you previously created.**" and press "**NEXT**".

For the next pictures, press "CANCEL" until the "**System Restore Settings**" screen, where "Command **Prompt**" can be selected at the bottom of the image.

CommandPrompt is in old days also called DOS PROMPT, and a black background image will show:

x: \ windows \ system32>

This must be changed to:

C: \ windows \ system32>

Thus:

X: \ windows \ system32> **cd c: \ windows \ system32 ** <enter>

DOS answers:

x: \ windows \ system32>

And you add: c: <enter>

DOS answers:

C: \ windows \ system32>

Make sure you are in the correct directory: ..> **DIR OSK.EXE**

If you are landed correctly, something will look like:

"The volume in drive C has no label
The volume Serial Number is 0051-c054
Directory of c: \ windows \ system32 \ OSK.exe
07/14/09 01: 39a -a ------ 692736 osk.exe
Xxxxxxxxxx bytes free "

Make sure you have **CMD.exe** in the same catalog by typing: ..> **DIR CMD.EXE** <enter>

If you are landed correctly, something will look like:

"The volume in drive C has no label
Thw Volume Serial Number is 0051-c054
Directory of c: \ windows \ system32 \ CMD.exe
07/14/09 03: 23a -a ------ 345088 cmd.exe
Xxxxxxxxxx bytes free "

OSK.exe must be saved in **OSK.EXE.OLD** so we can re-establish it to its original name again later, so we rename the original OSK.exe to name OSK.exe.Old.

DOS command REN = Rename = Rename

..> **RENE OSK.EXE OSK.EXE.OLD** <ENTER>

Display Keyboard Command Change to Command Prompt:

..> **REN CMD.EXE OSK.EXE** <ENTER>

Now the PC must be restarted.

In the LOGIN picture, the ICON is shown in the bottom left corner (Increased availability), press it and select:

"Write without keyboard (on-screen keyboard)"

Select the square field in front of the line and press "**OK**".

Now, **CMD.exe** is started and a black square will appear with CommandPROMPT showing:

C: \ windows \ system32>

Test to see who you are:

..> **whoami** <ENTER> This is a DOS-command

DOS answers:

Nt authority \ system that is SYSTEM administrator in Windows 7
c: \ windows \ system32> _

This means you have about 70% authority on your Windows system, where only SUPER administrator has more powers.

Now you have access to change the password for a user, whether it's an administrator or a default user, with the command:

C: \ windows \ system32> **net user <Default user> <New password>**

Instead of STANDARD USERS, you could have chosen to change the Administratoracount - the command, both apply because you are Administrator, or you could create a completely new user with the command:

C: \ windows \ system32> **net user <NewStandardUser> <New Password> / add**

THAT IS IT

Now you can log on to the machine using the Default User Name and its new password.

As a result of this story, you must return files to their original names, so you must restart the machine with the Recovery CD as mentioned at the beginning.

The commands are now the opposite way:

> **REN OSK.EXE CMD.EXE** <ENTER> Restore Command Prompt

> **REN OSK.EXE.OLD OSK.EXE** <ENTER> Restore SCREEN KEYBOARD

It's astonishingly easy and straightforward to cheat a WindowsPC and access it without knowing a password and it's no wonder when burglars go for laptops that can quickly break the security and that's Easily negotiable.

If you solved a problem on your PC by reading this document, both you and I have achieved something.

Sincerely
Palle A. Andersen
HAMRadioamateur OZ6YM