

Forum:[Hack Forums](#)

Thread: [Resetting a windows user's password](#)

GuestPass - June 20, 2015, 7:35 pm

This method uses the "Patched" sticky-keys-backdoor to gain Kernel Access to windows.
(I use the quotation marks for "Patched" because methods like this still allow it to be used?)

Things you'll need:

USB/CD with alternate boot installed (i.e. Hiren's Boot, Knoppix, Ultimate boot, etc.)

Basic understanding of how to operate a computer.

Step 1.

Boot the computer up with alternate boot of choice and select an operating system like Windows, Linux, mac, etc.

Step 2.

Ignoring the various tools loaded with the operating system, open the file browser and locate the local disc used for the computer's operating system.

Step 3.

Navigate to "c:\windows\system32" and rename the file "Sethc.exe" something you can remember for cleanup, like "panda.exe".

Step 4.

make a copy of "cmd.exe" and rename it "Sethc.exe"

Step 5.

Shut down the system and remove alternative boot disk.

Step 6.

Turn on computer and wait for login screen.

Step 7.

Press Shift five (5) times to bring up Kernel Access Command Prompt.

Step 8.

Find the username for the user by typing in "Net User". Should be one of the names that are not either "Administrator" or "Guest". For the sake of the tutorial let's say the username is "Ninja".

Step 9.

Type "Net user [Username here] *" (Should look like "Net user Ninja *" no quotes) and press enter three times to remove the password.

Alternatively after typing "Net user Ninja *" and pressing enter. Type the password in and hit enter and repeat to change the password to something new.

Step 10. (Optional)

Hide the trail. Repeat steps 1 & 2. Delete the current "Sethc.exe" and rename "Panda.exe" to replace it.

Tested on Laptops and Desktops running Windows XP/Vista/7/8/8.1/10

Jinu - June 20, 2015, 9:47 pm

Hiren's Boot is the easiest method I have ever seen. Anyway, thanks for this tutorial. I learned something from this tutorial.

GuestPass - June 21, 2015, 6:43 pm

(Jun 20, 2015 09:47 PM)Jinu Wrote: [\[CITE\]](#) Hiren's Boot is the easiest method I have ever seen. Anyway, thanks for this tutorial. I learned something from this tutorial.

No problem, glad I could help. ?