

Securing WinXP Pro (with what win-xp has to offer)

Note: These are just notes of the changes i made to win-xp pro using win-xp options after my default install. These changes will not secure your box 100% but they make a good couple of 1st steps. They are in no specific order other than the order that I performed them. I have only spent a couple of hours working on this operating system at the time of this text so please bare with me and understand that there is much more to securing your box than this.

1. NTFS Partition.
2. Disable Error Reporting
3. Disable Automatic Updates (only if your XP copy is pirated)
4. Disable "Recent Documents" Viewed
5. Setup XP Firewall
6. Setup screensaver password
7. Setup BIOS password
8. Setup "AfterBios" login password
9. Account Modifications
 - Rename Admin Account
 - Disable Guest Account
 - Disable Help_Assistant Account
 - Disable Support Account
10. Install a virus scanner.
11. Change Login Screen (default shows usernames)
12. Disable Remote Registry (and other services)
13. Disable/Change Auto-Search settings in IE.

1. ----- NTFS Partition (I like being God over system users) -----

Be sure to install XP onto an NTFS partition so that you (the admin) can take advantage of file permissions. You want this option so that "you" can decide who reads, writes, executes what files.

If you didnt install XP onto an NTFS partition. Convert It. To convert to NTFS follow the instructions below.

Open a command prompt and type "convert c: /FT:NTFS /v"

This command will convert your c: partition from FAT to NTFS in verbose mode.

2. ----- Disable Error Reporting - we dont want microsoft to know everytime we fuck up. especially if we didnt pay for winxp. -----

control panel >> performance and maintenance >> system >> advanced >> error reporting
(disable all)

right click "my computer" >> manage >> services and applications >> services >> " stop
and disable" Error Reporting.

3. -----

Disable automatic updates - to update, they must know what we have. thats a NO NO!

NOTE: DO THIS ONLY IF YOUR COPY OF XP IS PIRATED!! I suggest "auto update" if your copy of XP is legal. If your copy is pirated then i suggest that you stay updated with the latest fixes and patches manually.

control panel >> performance and maintenance >> system >> automatic updates
(disable updates)

right click "my computer" >> manage >> services and applications >> services >> " stop
and disable" Automatic Updates.

4. -----

Quit listing most recent documents opened under the start button - Dont want the girlfriend or the parents to find that pr0n you being viewing.

control panel >> appearance and themes >> task bar and start menu >> start menu >>
customize >> advanced

remove the checkmark next to "List my most recently opened documents".

5. -----

Block incoming traffic to your winxp box. - Before this change, i scanned my xp box and found it to have many ports wide open. After this change, I found nothing and xp logged the attempts in c:\windows\pfirewall.log.

control panel >> network connections >> right click "local area connection" >> properties
>> advanced >> check the box under "Internet Connection Firewall" then choose "settings".

Services Tab - leave all unchecked unless there is a service you are running that people must be able to access.

Logging Options - Log everything.

ICMP - I left all these unchecked for the time being. (allowing nothing)

(this does not protect you from "Spy Ware". This only stops traffic from coming into your win-xp box (not all traffic). It does not stop traffic from going out.) If you need to stop traffic from going out and need a more secure firewall then download a real firewall like "zone alarm or black ice".

6. -----

Setting a screensaver password incase you leave some of that secret pr0n open when you walk away.

right click on the desktop >> properties >> screen saver >> check the box next to " On
Resume, Password Protect."

If you dont have a password set on your user account, you can do so in control panel >>
user accounts >> change account.

7. -----

Setting a BIOS password - We dont want anyone rebooting the computer or trying to sneak into our pr0n while we are away at school or work.

I cant explain to one how this is done due to the differences between all computers and how the BIOS settings are entered. If you know what Im talking about then do it. If you dont know what Im talking bout then learn how to do it. A screensaver password is useless unless you setup a BIOS password.

8. -----

Setting up the "AfterBios" password. Sometimes bios passwords are easily cracked. This password will add extra local login security incase your bios pass is crax0red. I dont know bout you but i love having to type in 3 passwds and a username to login to my box.

Start >> run >> type "syskey" >> choose "update" >> choose "Password Startup" >> enter a password and choose ok.

9. -----

Renaming and Disabling Accounts for administrator, guest, help_assistant and support.

Right click my_computer >> manage >> local users and groups

rename administrator account
disable guest account
disable help_assistant account
disable support account

10. -----

Install Virus Protection..... (We like our uncorrupted data and trojan free system)

Install a virus scanner. Your firewall might protect your system from unwanted hackers but what about an unwanted virus or trojan?. I recommend installing a virus scanner such as "Nortons" or "McAfee".

11. -----

Change Default Login Screen..... (why do we want to share usernames with anyone?)

Xp uses the "welcome screen" by default. This screen has the names of all accounts on the system so that the user only has to click on their name and type a password. Come on now.... We arent that damn lazy. If we change this screen to the normal login, then prying eyes will have to know a username and password to get in. Follow the instruction below to change this.

control panel >> user accounts >> change the way users log on or off

uncheck the box next to "Use Welcome Screen" and choose "apply options".

12. -----

Disable Remote Registry.....(why would I need to edit my registry remotely anyway?)

right click "my computer" >> manage >> services and applications >> services >> " stop
and disable" Remote Registry.

NOTE: disable any services running in this area that you arent using.

13. -----

Disable/Change Auto-search in Internet Explorer. This is not really a security risk but it
is important to some people that prefer to keep their internet surfing to themselves and
away from microsoft.

Open Internet Explorer >> Click the "search" button >> click the "customize" button >> click
"autosearch settings" >> FOLLOW INSTRUCTIONS BELOW.....

DISABLE: In the "When Searching" drop down menu, select "Do not search from the address bar".
>> click "ok" >> "ok". Type an invalid address in your address bar and see if it
takes you to the msn search page or if it gives a "page not found" error. In this
case, the "page not found" error is what we want.

CHANGE: If you wish not to disable, but you wish to change it to your favorite "google.com"
search page. Instead of following the "DISABLE" instructions, follow the instructions
below. Choose "Google Sites (or whatever you prefer)" from the "choose a search provider
to search from address bar" drop down menu >> click "ok" >> "ok"