Windows XP: Surviving the First Day

SANS Institute Internet Storm Center

Since its release, a number of severe security vulnerabilities have been discovered in Windows XP. These vulnerabilities are used by worms and viruses, making it impossible to connect an unsecured, unpatched system to the Internet for any amount of time without risking exposure and infection. Users of new computers are faced with the dilemma of being infected by these worms before being able to download the necessary patches.

This guide will show how to install Windows XP securely, without being infected by these worms during the patching process.

Introduction

The target audience for this guide are home users and small businesses without a firewall, who rely on downloading patches from Microsoft directly. This guide is not a “Windows hardening” guide. See the reference section at the end for more details regarding hardening Windows. Steps outlined in this guide should be seen as minimum due diligence to make it through the first day of using Microsoft Windows XP.

Screen-shots are from Windows XP Professional Edition. However, all steps outlined here apply to the 'Home' edition as well.

The guide assumes a new Windows XP install 'from scratch' using the Windows XP CD. If you buy a computer with Windows XP pre-installed, some of these steps may already have been performed for you. Please see the guide for details. If you are already logged in, skip to the 'Verify Settings' section.

To keep this guide short, only critical steps are shown. All other settings can be left in their default state or should be selected in accordance with your preferences (e.g. language, time zone).

Preparations

Unpack your new PC according to the manufacturer's instructions. DO NOT CONNECT THE PC TO ANY NETWORK OR PHONE LINE. If the computer includes a wireless network card, turn off any wireless access points within range if possible. Follow the manufacturers instructions to disable the wireless network card.

Once you take these precautions, turn the system on. If Windows XP is not pre-installed, boot from your Windows XP install CD.

Install

Administrator Password

Early in the setup process, you will be given the option to configure an Administrator account password. Use a strong password. Characteristics of a good password:

- at least 8 characters long
- contains letters, numbers and other characters
- not a dictionary word
- not easily guessed (e.g. pet names, birthdays ...)

Figure 1Setup Administrator password.

You may want to adjust the computer name to reflect your naming scheme. The computer name may be visible to others, so don't use your password or social security number.

Network Settings

You have to select 'custom' network settings in order to gain access to the network component dialog.

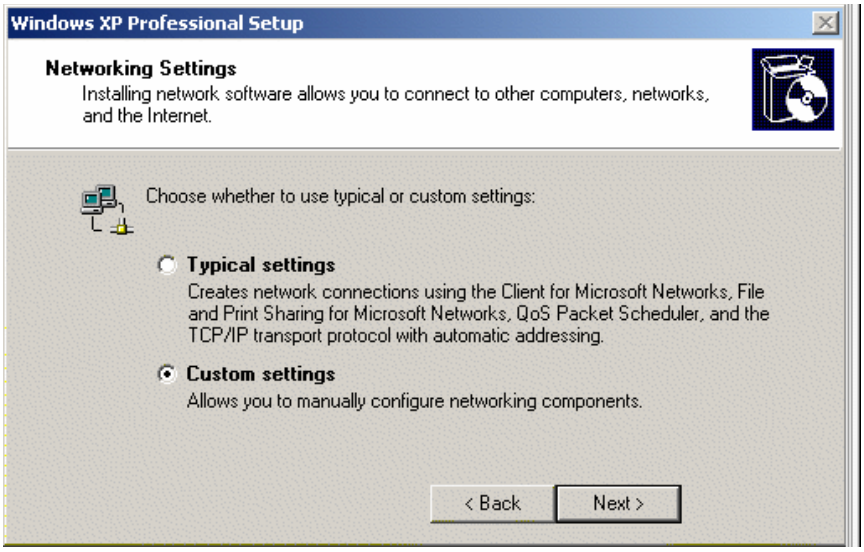

Figure 2Select custom network settings.

Next, you will arrive at the Networking Components dialog. Unselect the “Client for Microsoft Networks” and the “File and Printer Sharing for Microsoft Networks”. If you require these components for your network, you will be able to enable them later after you have patched the system.

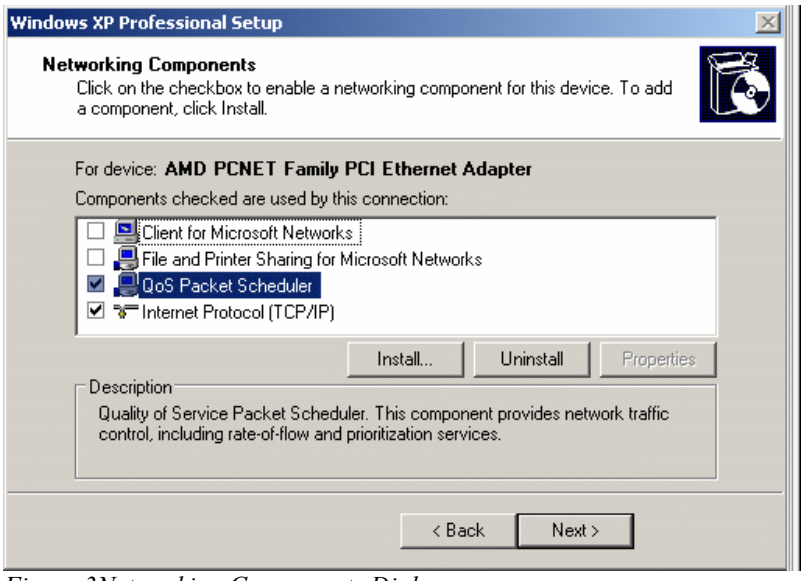

Figure 3Networking Components Dialog

Internet Connection

After a few more dialogs, Windows will switch to a higher resolution and ask you for your network connection. Most likely, you will select 'connect directly to the Internet', unless you have a Local Area Network and use one host on the network as a gateway. Select whichever option is appropriate for your network, even though you are not currently connected to it.

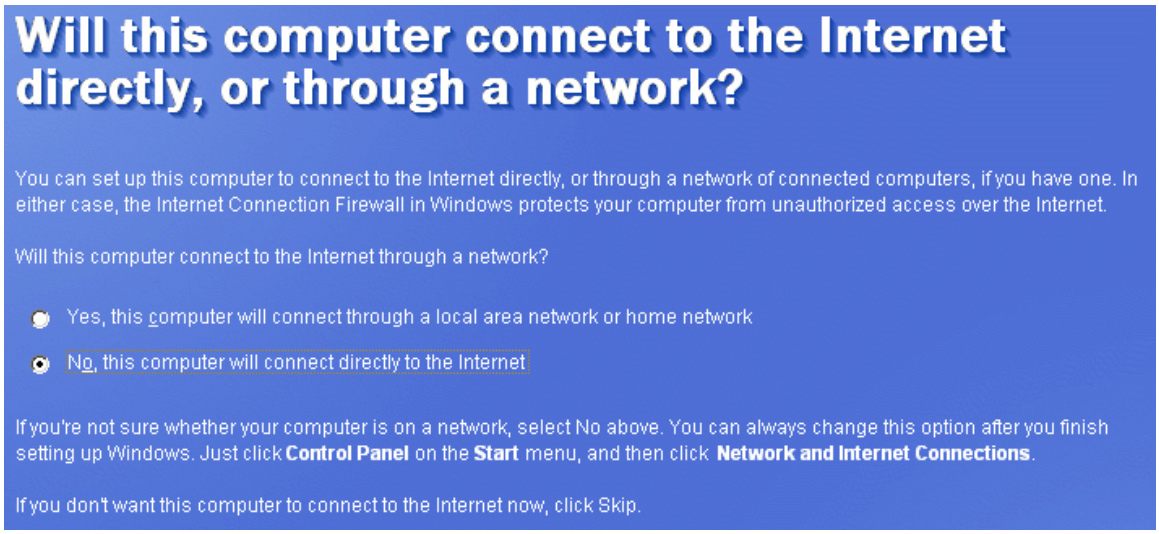

Figure 4Select network connection

Activation

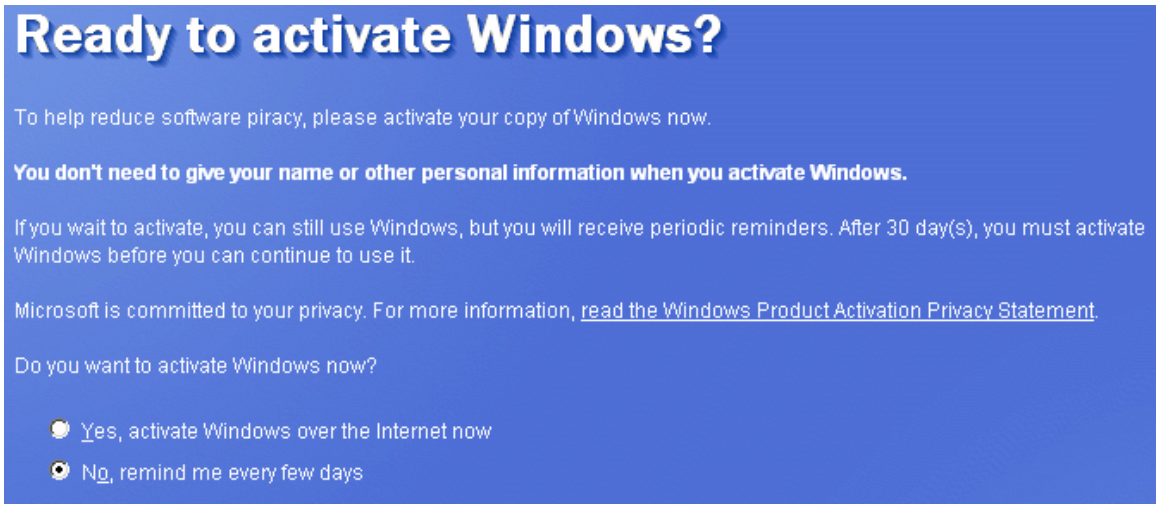

Figure 5Windows Activation

You will not be able to activate Windows XP at this point. Select 'No, remind me every few days'. You will have to register your copy of Windows XP within 30 days.

User Setup

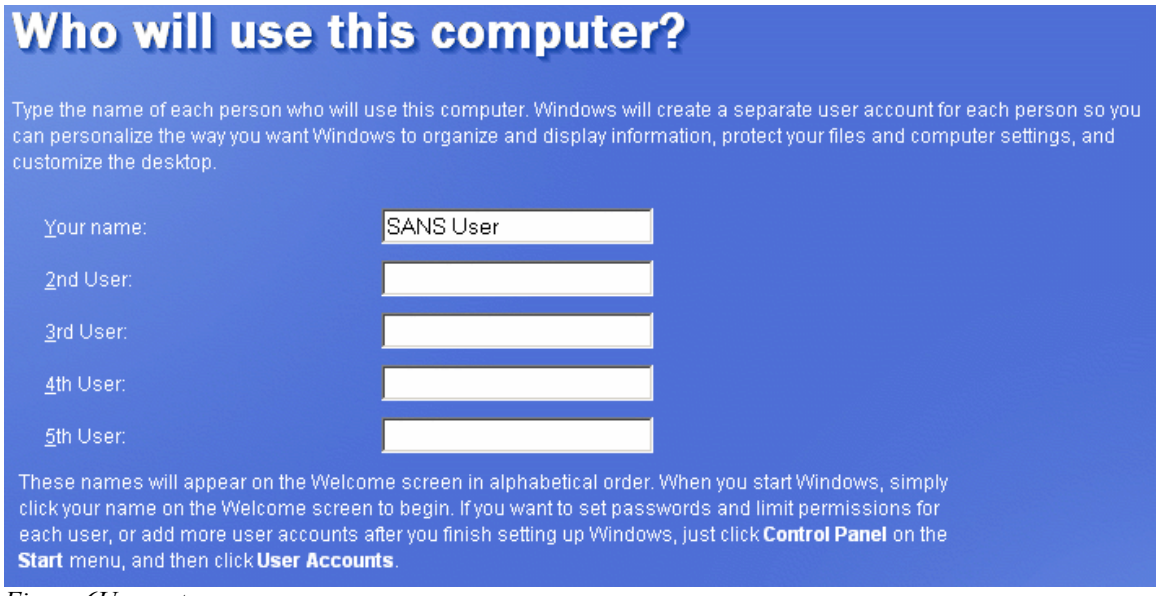

Figure 6User setup.

Important:

Users you setup here will have “Administrator” access and no password. This is a bad combination if unauthorized users will have access to this system. However, by default, Windows XP prevents network access using accounts without password. As a result, these accounts will not expose you to network based attacks.

Review your Windows XP documentation to learn how to limit these accounts.

Verify Network Settings

After completing the installation, you will be able to log in to your system. In particular if Windows XP was pre-installed on your system, you should check the network settings.

First, launch the control panel from the 'Start' menu:

Figure 7Windows XP Start Menu

In the control panel, select 'Network and Internet Connections'

Figure 8Control Panel

Next, select 'Network Connections'

Figure 9Select Network Connection

Select your network connection. There should be only one at this point. If you have more than one network connection, you have to repeat these steps for each connection.

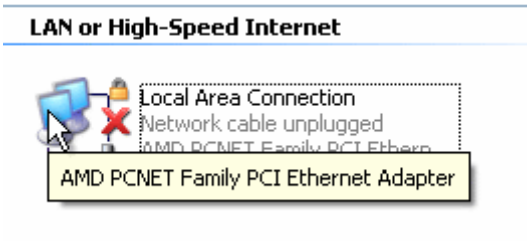

Figure 10Network Connection

The “Local Area Connection Properties” dialog should show the “Client for Microsoft Networks” and the “File and Printer Sharing for Microsoft Networks” unchecked. If they are checked, uncheck them now.

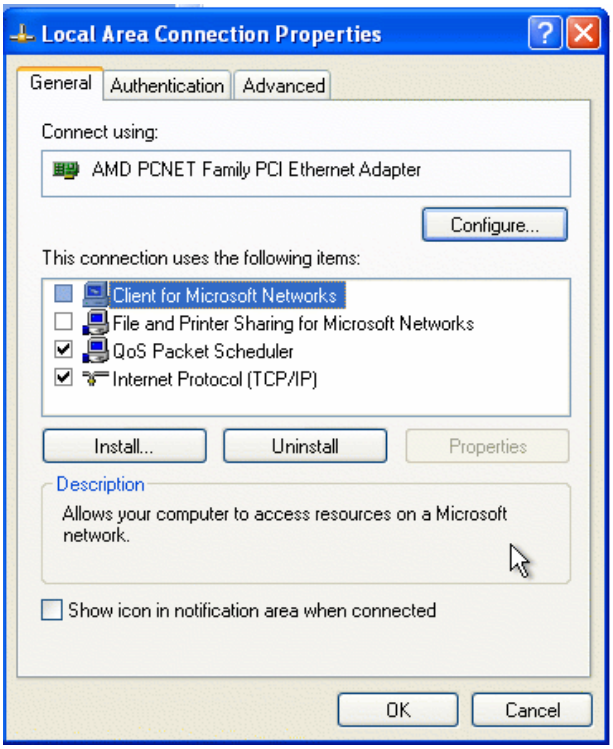

Figure 11Network connection properties

Next select the “Advanced” tab in this dialog

Figure 12Advanced LAN Connection Properties

Make sure the Internet Connection Firewall is enabled.

Close all dialogs and reboot the system.

Windows Update (1st Pass)

At this point, your system should be secure enough to connect it to the Internet. If you made any changes in the last step, you may want to review that they are still active after the reboot. Next, connect your system to the network.

Once the system is connected to the network, enter the “Control Panel” again, and select “Windows Update” from the small menu at the left hand side.

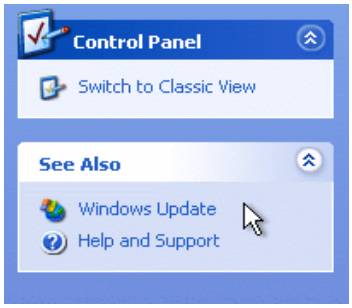

Figure 13Control Panel, left hand side

This will launch Internet Explorer and open the windows update web site. A dialog will ask you for permission to install the latest version of Windows Update. Click 'Yes'. You may select “Always trust content from Microsoft Corporation” if you don't want to be confronted with this dialog in the future. This implies that you trust the Windows code signing procedures.

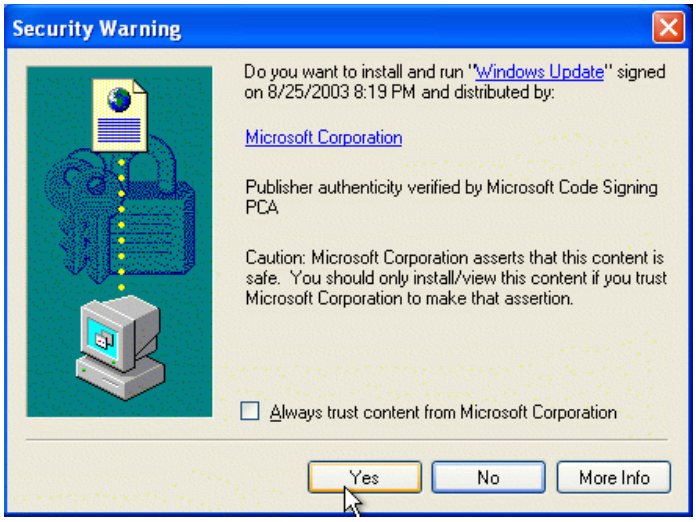

Figure 14Signature verification.

After the latest version of the Windows Update software is installed, you will have to reboot your system.

IMPORTANT: At this point, your system is not yet patched. Only the update software is updated.

Windows Update (2nd Pass)

After the system reboots, start Windows Update again. This time, you will be asked to scan for updates.

Figure 15Welcome to Windows Update

Once the scan is completed, click 'Review and install updates'

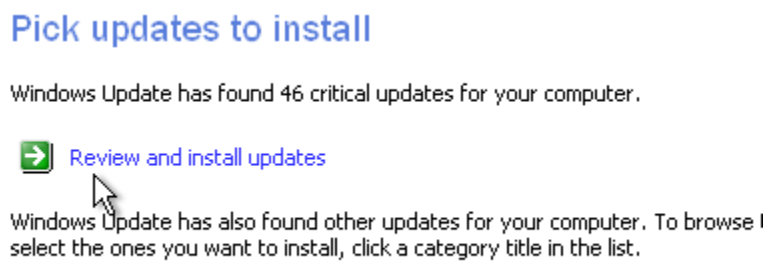

Figure 16Pick updates

if you are asked to send information over the Internet, click “Yes”

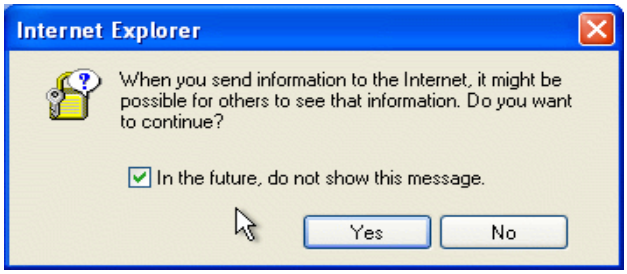

Figure 17Security Warning

Next, select 'Install Now'

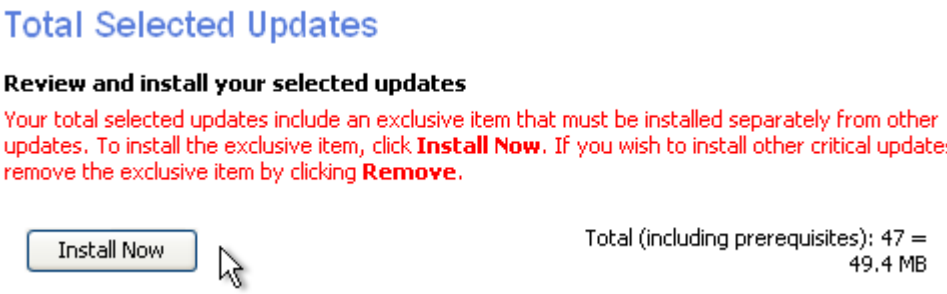

Figure 18Selected Updates

Depending on which version of Windows XP you install, it may not be possible to install all available updates at the same time. In particular service packs, which include a large number of patches, will have to be installed first. The next dialog will advise you of such a case. Click 'Ok'

Figure 19Service Pack notice

The following screens will ask you to accept the license agreement and the updates will be installed once you accept the agreement.

After the update finishes, reboot the system and run Windows Update again until no more critical updates are available.

Additional Tips

Please check the “References” section for more detailed guides. Also, if you are installing any additional software, like Microsoft Office, or if you are enabling any server functions (file sharing, Internet Information Server), consult specific hardening guides.

Aside from keeping your system up to date, running a virus checker is probably one of the best things you can do. Again, review the “References” section for details.

References

- Microsoft Security Guide: http://www.microsoft.com/security/protect/.
- Microsoft Security Page: http://www.microsoft.com/security.
- Participating in the Internet Storm Center: http://www.dshield.org/clients/windows_xp_firewall_setup.php. http://www.dshield.org/howto.php.
- SANS Reading Room: http://www.sans.org/rr.
- SANS Track 5: Securing Windows. http://www.sans.org/conference/bytrack.php#t5
- NSA Security Guides: http://nsa.gov/snac/index.html
- Center for Internet Security: http://www.cisecurity.org.

Acknowledgments

I would like to thank our Internet Storm Center “Handler” team for valuable input. In particular: Scott Fendley, Deb Hale, Marcus Sachs, Donald Smith. Other contributors: David Hart, Wayne Larmon, Bjorn Stromberg.

Disclaimers

Contact for suggestions/questions: isc@sans.org

Windows XP: Surviving the First Day (Checklist)

- ❑ Disconnect Network Connection.
- ❑ Setup a secure administrator password.
- ❑ Disable Client for Microsoft Networks

  To verify: Start ➔ Control Panel ➔ Internet and Network Connections ➔ Network Connection ➔ select your network connection
- ❑ Disable File and Printer sharing

  verify using the same dialog as 'Client for Microsoft Networks'
- ❑ Enable Internet Connection Firewall

  same dialog as 'Client for Microsoft Networks'. Select 'Advanced' tab.

Connect Network

- ❑ Run Windows Update until there are no more critical updates.

  Start ➔ Control Panel ➔ Windows Update ➔ Scan for Updates