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 ...)

Windows XP Pr	ofessional Setup	X		
Computer N You mus	Name and Administrato at provide a name and an A	r Password dministrator password for your computer.		
	Setup has suggested a n network, your network ad	ame for your computer. If your computer is on a Iministrator can tell you what name to use.		
	Computer name:	ISC-SANS3948		
.	Setup creates a user acc yoggeed full access to yo	ount called Administrator. You use this account when our computer.		
	Type an Administrator password.			
	Administrator password:	•••••		
	Confirm password:	••••••		
		< Back Next >		

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.

Windows XP Professional Setup
Networking Components Click on the checkbox to enable a networking component for this device. To add a component, click Install.
For device: AMD PCNET Family PCI Ethernet Adapter Components checked are used by this connection:
Install Uninstall Properties Quality of Service Packet Scheduler. This component provides network traffic control, including rate-of-flow and prioritization services.
< Back Next >

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.

Will this computer connect to the Internet directly, or through a network?

You can set up this computer to connect to the Internet directly, or through a network of connected computers, if you have one. In either case, the Internet Connection Firewall in Windows protects your computer from unauthorized access over the Internet.

Will this computer connect to the Internet through a network?

- Yes, this computer will connect through a local area network or home network
- No, this computer will connect directly to the Internet

If you're not sure whether your computer is on a network, select No above. You can always change this option after you finish setting up Windows. Just click **Control Panel** on the **Start** menu, and then click **Network and Internet Connections**.

If you don't want this computer to connect to the Internet now, click Skip.

Figure 4Select network connection

Activation

Ready to activate Windows?

To help reduce software piracy, please activate your copy of Windows now.

You don't need to give your name or other personal information when you activate Windows.

If you wait to activate, you can still use Windows, but you will receive periodic reminders. After 30 day(s), you must activate Windows before you can continue to use it.

Microsoft is committed to your privacy. For more information, read the Windows Product Activation Privacy Statement.

Do you want to activate Windows now?

- Yes, activate Windows over the Internet now
- No, remind me every few days

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

Who will use this computer?

Type the name of each person who will use this computer. Windows will create a separate user account for each person so you can personalize the way you want Windows to organize and display information, protect your files and computer settings, and customize the desktop.

Your name:	SANS User	
<u>2</u> nd User:		
<u>3</u> rd User:		
<u>4</u> th User:		
<u>5</u> th User:		
These names will appear on the Welcon click your name on the Welcome screen each user, or add more user accounts a Start menu, and then click User Accoun	ne screen in alphabetical order to begin. If you want to set pass fter you finish setting up Windov ts .	When you start Windows, simply words and limit permissions for vs, just click Control Panel on the

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'



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.

🕹 Local Area Connection Properties	?×
General Authentication Advanced	
Connect using:	
B AMD PCNET Family PCI Ethernet Adapter	
Configure.	
This connection uses the following items:	
 Client for Microsoft Networks File and Printer Sharing for Microsoft Networks QoS Packet Scheduler Treinternet Protocol (TCP/IP) 	
Install Uninstall Properties	
Description	
Allows your computer to access resources on a Microsoft network.	
	:
Show icon in notification area when connected	
OK Ca	ncel

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.

Control Panel	۲			
🚱 Switch to Classic View				
See Also	۲			
 Windows Update Help and Support 				

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.

Welcome to Windows Update

Get the latest updates available for your computer's operating system, software, and hardware.

Windows Update scans your computer and provides you with a selection of updates tailored just for you.





Note Windows Update does not collect any form of personally identifiable information from your computer. Read our privacy statement

Figure 15Welcome to Windows Update

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

Pick updates to install

Windows Update has found 46 critical updates for your computer.

Review and install updates

Windows Update has also found other updates for your computer. To browse I select the ones you want to install, click a category title in the list.

Figure 16Pick updates

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



Figure 17Security Warning

Next, select 'Install Now'

Total Selected Updates

Review and install your selected updates

Your total selected updates include an exclusive item that must be installed separately from other updates. To install the exclusive item, click **Install Now**. If you wish to install other critical updates, remove the exclusive item by clicking **Remove**.



Total (including prerequisites): 47 = 49.4 MB

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

- i Microsoft Security Guide: http://www.microsoft.com/security/protect/.
- T 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.
- ^T 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
- T 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

Microsoft, Windows, Windows XP are trademarks or registered trademarks of Microsoft Corporation. This document may be copied and shared freely in its original form without alteration. Please do not offer copies online, but instead link to the original at <u>http://isc.sans.org</u> to avoid distributing outdated versions. This document may contain errors. In no event shall the SANS Institute be liable for any damages resulting from the application of procedures outlined in this document.

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 \rightarrow Control Panel \rightarrow Windows Update \rightarrow Scan for Updates