

## Securing Windows XP Professional

How to quickly secure a Windows XP Professional PC out of the box

## Goals of Security

- Confidentiality
- Availability
- Reliability
- Manageability
- Accountability
- Responsibility

## Methods of Security

- Physical security
- Account security
- Network security
- Data security
- Security by obscurity
- Protect against malware
- Patch and update
- Be aware

## Physical Security

- Set BIOS password
- Disable boot from floppy/CD
- Restrict physical access
- Secure from theft
- Protect with UPS (or at least a surge protector)

## Account Security

- Establish secure password policy
- Set secure passwords on all accounts
- Delete or disable unused accounts
- Don't send passwords unencrypted

## Network Security

- Turn on secure file sharing
- Turn off unnecessary services
  - Messenger, Computer Browser, etc.
- Turn off “dangerous” services
  - Remote Registry, IIS, ftp, telnet, snmp, etc.
- Don't confuse a workstation with a server
- Use IPSec filtering

## Data Security

- Use NTFS file system
- Set reasonable file and share permissions
- Perform regular backups (and test)
  - Copy data to CD-R/CD-RW
  - Windows backup
  - Departmental services
  - CITES TSM service
  - Whatever works for you

## Security by Obscurity

- Hide machine from browsing
- Use classic logon screen
- Disable anonymous enumeration of accounts and shares

## Protect Against Malware

- Install anti-virus software, and keep up-to-date, preferably automatically
- Show all file extensions
- Link script extensions to notepad
- Don't use Outlook or Outlook Express, unless committed to keeping it secure
- Use Office macro security

## Patch and Update

- Use Windows Update
- Use Office Update
- Don't rely solely on Windows Update
- Use Microsoft's "HotFix & Security Bulletin Service"

## Be Aware

- Turn on auditing
- Regularly check system logs
- Occasionally look for suspicious accounts or services
- Subscribe to security mailing lists
  - NTBugtrak
  - Microsoft Security notification

## Interesting URLs

- The Ten Immutable Laws of Security
  - <http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/columns/security/essays/10imlaws.asp>
- Security Administration Operations Guide
  - <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/opsguide/secadmog.asp>
- RestrictAnonymous registry key setting
  - <http://support.microsoft.com/default.aspx?scid=kb;en-us;q246261>
- Using IPSec to Lock Down a Server
  - [http://www.microsoft.com/serviceproviders/columns/using\\_ipsec.asp](http://www.microsoft.com/serviceproviders/columns/using_ipsec.asp)
- Windows Update
  - <http://v4.windowsupdate.microsoft.com/en/default.asp>

## Interesting URLs - continued

- Microsoft Office Update (also available from Windows Update page)
  - <http://office.microsoft.com/productupdates/>
- Security Bulletin Search
  - <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp>
- Microsoft Security Home
  - <http://www.microsoft.com/security>
- BISS Security Page
  - <http://biss.beckman.uiuc.edu/security/>
- CITES Security Page
  - <http://www.cio.uiuc.edu/security/>

## Tools and Resources

- Hfnetchk (3.86, not 3.2. See hfnetchk issues.txt)
- Windows XP Professional Resource Kit
- Security Configuration Manager
  - MMC snap-in, security templates, secedit.exe
- UIUC Technet DVD
  - \\technet\technet\technet DVD\Technical Information and Utilities, run setup.exe
- Google

## IPSec Filtering

- Policy is a set of IP Security Rules
- Rule consists of a filter list associated with a filter action
- Filter list a list of IP address and port source/destination combinations
- Filter actions:
  - Permit
  - Block
  - Negotiate security
- Rules applied from most general to most specific
- Command line interface available: IPsecPol.exe

## IPSec example

- This example allows full access from a single machine, allows access to any port except TCP 80 for 128.174.0.0, blocks all else (action protocol sourceIP:port destIP:port)
  - Block Any Me:Any Any:Any
  - Permit Any Me:Any 128.174.0.0/16:Any
  - Block TCP Me:80 128.174.0.0/16:Any
  - Permit Any Me:Any 128.174.208.254:Any

# Securing Windows XP Professional

v. 2.0 4/8/2003

## Preliminaries:

- Set computer name.
- Set time, time zone, and daylight savings.
- Set up IP information.
- Install latest video and network drivers.
- Show My Computer on desktop.
- Do NOT attach to network.

## Security Settings:

### Secure BIOS:

- Set BIOS to boot from hard drive first. This will prevent accidental boot from an infected floppy or CD.
- Set BIOS password

### Install Service Pack 1

### Configure User Accounts:

- Start -> Settings -> Control Panel-> User Accounts
  - Set administrator password:
    - Click on "Computer administrator".
    - Click "Create a password", set complex password.
  - Verify Guest account is off:
    - Under Guest it should say "Guest account is off".
  - Turn off Fast User Switching and the Welcome Screen:
    - Click on "Change the way users log on or off".
    - Uncheck "Use the Welcome Screen" and "Use Fast User Switching".

### Set Local Security Policy:

- Start -> Settings -> Control Panel -> Administrative Tools -> Local Security Policy
- Change the following, all else default:

#### Account Policies:

- Password Policy
  - Maximum password age, set to 0 (does not expire)
  - Minimum password length, set to 6 (8 is better)
  - Set "Password must meet complexity requirements" to Enabled
  - Verify "Store password using reversible encryption" is set to Disabled.
- Account Lockout Policy
  - Threshold -> 10 attempts (maximum)
  - Duration -> 30 minutes (minimum)
  - Reset after -> 30 minutes (minimum)

#### Local Policies:

- Audit Policy
  - Account logon events -> failure
  - Account management -> success, failure
  - Directory service access -> none
  - Logon events -> failure
  - Object access -> none (can be verbose, but useful for troubleshooting)
  - Policy change -> success, failure
  - Privilege use -> none (can be very verbose)
  - Process tracking -> none
  - System events -> success, failure
- User Rights Assignment
  - Access this computer from the network: change Everyone to Authenticated Users
  - Log on locally: remove Guest

## Security Options

Accounts: Rename administrator account: set to desired name (anything but “administrator”)

Microsoft network client: Send unencrypted password to third-party SMB servers: Disabled

Network access: Do not allow anonymous enumeration of SAM accounts: Enabled

Network access: Do not allow anonymous enumeration of SAM accounts and shares: Enabled

Network access: Sharing and security model for local accounts: Guest only -> Classic

(This also turns off “simple file sharing” and sets

HKLM\System\CurrentControlSet\Control\LSA\forceguest to “0”)

### **Enable network lockout of administrator account:**

From command line: passprop.exe /adminlockout (Obtain from Resource Kit. 2000 version ok.)

### **Disable and/or stop unnecessary or dangerous services:**

Right-click My Computer -> Manage -> Services and Applications -> Services

Verify the following dangerous services are stopped and disabled, if they exist, unless you have a very good reason:

IIS, ftp, smtp, lpd, snmp, Terminal Services, Remote Registry

You probably want to stop and disable (or set to manual) these services:

Messenger, SSDP, Universal Plug and Play, Indexing Service, Help and Support

Any other junk added by OEM

### **Set “hidden” attribute, to keep machine from appearing in browse lists:**

Using regedit:

Create new dword HKLM\system\currentcontrolset\services\lanmanserver\parameters\Hidden.

Set value to 1.

### **Create dummy administrator account, set complex password, disable:**

Right-click My Computer -> Manage -> Local Users and Groups -> Users

Right-click -> New User, create Administrator account.

Set complex password, select “Account is disabled”.

Set complex password for Guest account.

### **Increase size of event log files:**

Right-click My Computer -> Manage -> Event Viewer

Right-click Application -> Properties

Set “Maximum log size” to at least 5120 KB

Repeat for Security and System

[attach to network here]

### **Install any post-SP1 security patches:**

Use Windows Update.

Make sure Windows Update does the following:

Patch Internet Explorer to current level.

Patch Media Player to current level.

Use Office Update, if Office is installed.

Patch Office to current level.

Check MS Security Bulletin web site.

### **Install and configure anti-virus software:**

Install

Update

Make sure that an update method is arranged, with either auto-update or management software.

Configure:

Check for macros, use heuristics, scan all files, exclude appropriate folders

Disable “floppy on shutdown”. Do not disable on-access scanner.

### **Ask for ISS scan of machine to verify installation and settings.**

## **Optional Security Settings:**

(These could possibly break things, so test when done.)

### **Secure file extensions:**

Disable file associations for .hta, .wsh files and set to notepad.exe

Explorer -> Tools -> Folder Options -> File Types

Highlight "HTA File", click "Change", highlight "Notepad" (browse if necessary), click "OK".

Repeat for "WSH File".

Disable "Hide extensions for known file types":

Explorer -> Tools -> Folder Options -> View:

Deselect "Hide extensions for known file types".

Remove "NeverShowExt" registry settings for ConferenceLink, DocShortcut, piffile, SHCmdFile, xnkfile:

Open regedit, Edit -> Find. Search for "NeverShowExt" and delete from those keys listed above.

Set "Always show extension" for: Desklink, Mapimail, SHS, HTA, WSH, LNK (optional):

Explorer -> Tools -> Folder Options -> File Types

Highlight Desklink, click "Advanced", select "Always show extension", click "OK".

Repeat for remaining file types listed above.

### **Set IP Security Policies:**

Start -> Control Panel -> Administrative Tools -> Local Security Policy -> IP Security Policies on Local Machine:

Create new policy:

Right-click -> Create IP Security Policy

Enter name for new policy, click "Next".

Accept default on "Requests for Secure Communication", click "Next".

Accept default on "Default Response Rule Authentication Method", click "Next".

Click "Yes" on Warning box, click "Finish".

Create new rule:

Click "Add"

Create new filter list if necessary:

Click "Add".

Create filter

Repeat until done.

Assign action to filter list to create rule.

Create more rules as necessary to complete the policy

Assign policy:

Right-click on policy -> assign

**Consider using campus firewall.**