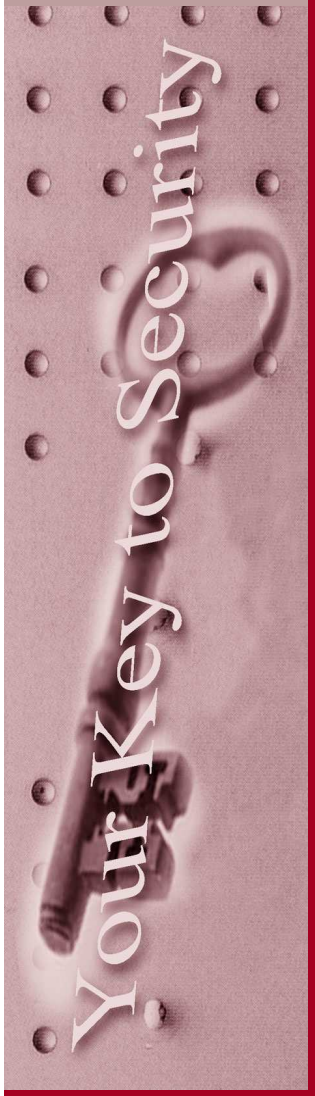


Windows XP Hardening; Part 2 of 2

Prepared for NEbraskaCERT Cyber Security Forum
October 18, 2006

Stephen M. Nugen, CISSP
Senior Research Fellow
Nebraska University Consortium for Information Assurance
College of Information Science & Technology
Peter Kiewit Institute
University of Nebraska Omaha

Meta

- Speaker: Stephen (Steve) Nugen, CISSP
  - smnugen@nucia.unomaha.edu
  - smnugen@nugensoft.com
- Approach
  - Pointers and observations to help you develop your own methods (with liberal re-use of course)
- Caveat
  - Settings in these slides reflect presenter's
    - Highly subjective opinions
    - Experiences which may not be any prediction of how these settings will work in you experience

Meta cont'd

- Caveat cont'd
  - Settings in these slides are just illustrations
  - There is no representation by the presenter or any organization he is affiliated with that these settings
    - Will be useful for your situation
    - Won't turn your system into an overpriced doorstop
  - As a courtesy: If you do encounter any problems with these settings, please tell the presenter so that he
    - Update his own knowledge
    - Spread less misinformation in subsequent presentations

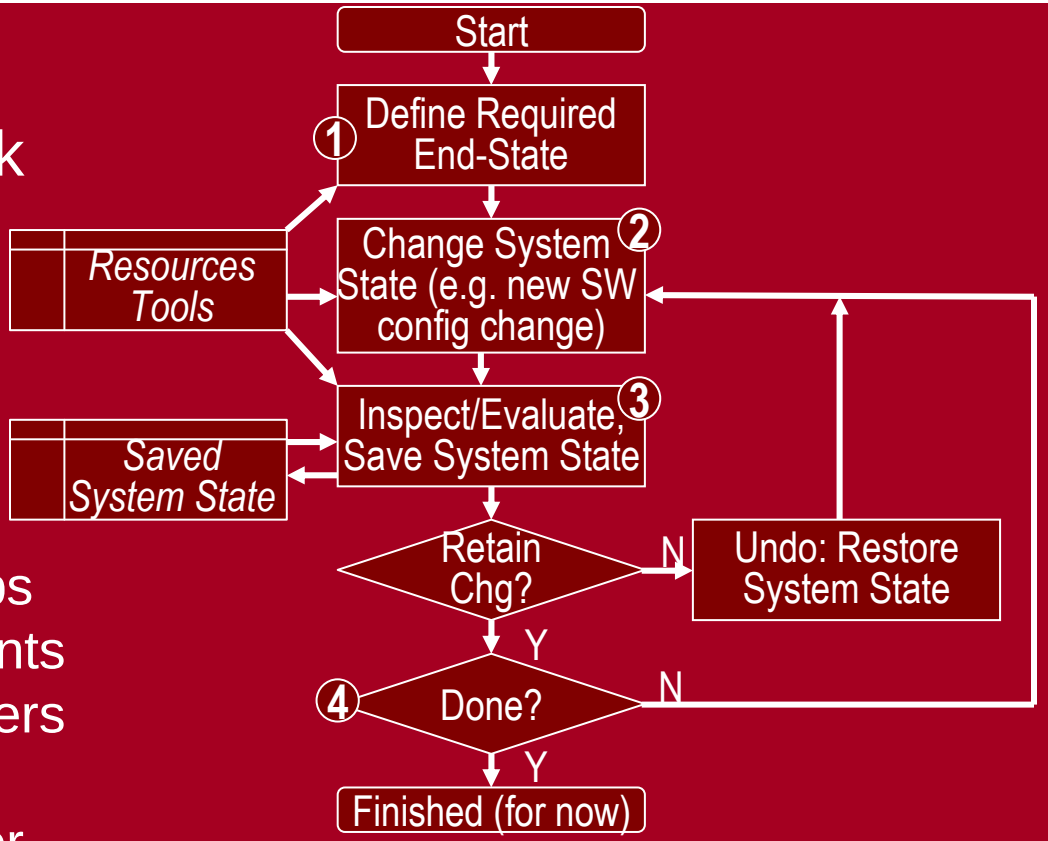
Meta cont'd

- Part-2 of 2-Part Presentation

- Part-1
  - Sep 2006 CSF
    - Slides available at http://www.nebraskacert.org/CSF/CSF-Sep2006.pdf
  - Target environment
    - Standalone laptop, not connected to any domain
    - Single trusted user
    - Windows XP Pro with SP2

Meta cont'd

- Part-1 cont'd
  - Defined this framework



① Resources from Microsoft, DISA,CIS, and others recommend specific security configurations for Win XP laptops operating in different environments

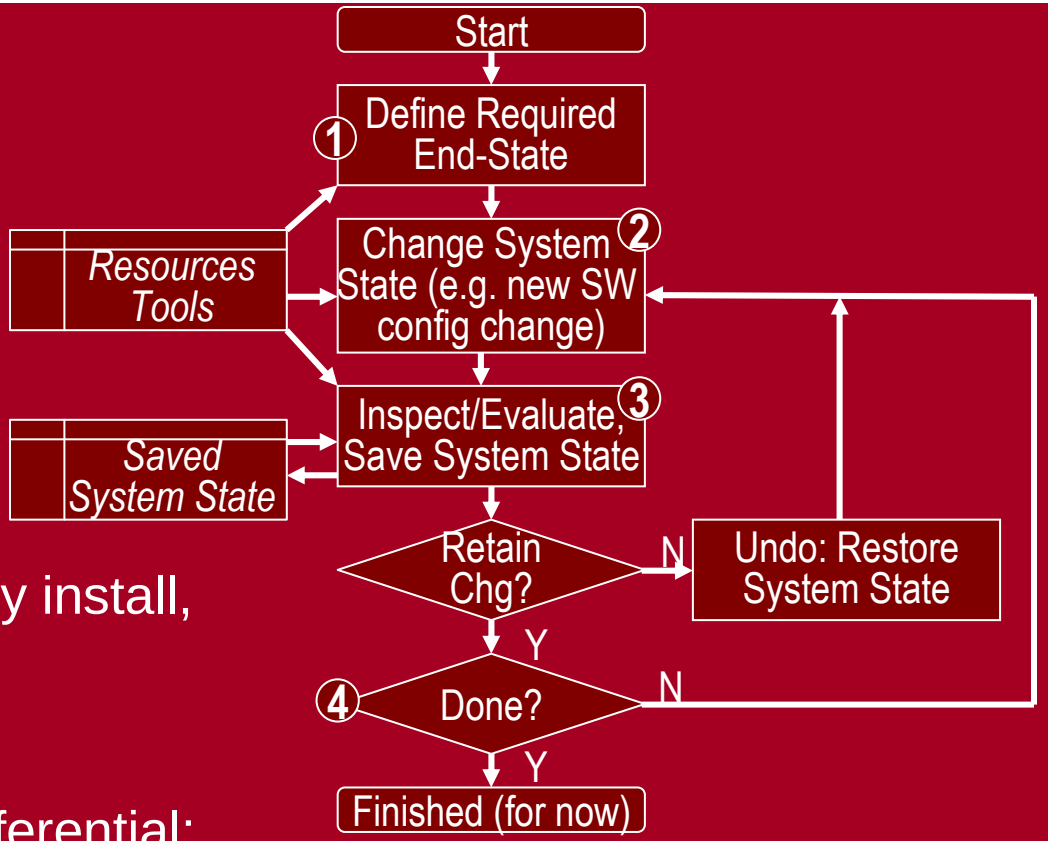
-- EC (Enterprise Client): members of Active Directory Domain

-- SA (Stand-Alone): not member of Active Directory Domain

-- SSLF (Specialized Security – Limited Functionality): Tighter security, but with significant loss of functionality and manageability

Meta cont'd

- Part-1 cont'd
  - Framework cont'd



② System state changed with every install, every configuration change

③ Evaluation of system state is differential; comparing state of system before the change to system state after the change
Saved states permit recovery ("undo")

④ Done when evaluated state matches defined end-state

Meta cont'd

- Part-2
  - Assumed state
    - End state (mostly) defined
    - Base operating system installed
    - All required device drivers and system software installed... incrementally, with saved system states
    - System not yet exposed to live Internet

Meta cont'd

- Part-2 cont'd
  - Remaining tasks, still using the incremental approach:
    - Configure/Harden, Part-1
    - Update on-line
    - Configure/Harden, Part-2
    - Configure/Harden, Part-3
    - Configure/Harden, Part-4
    - Operate securely... patch management, etc.

Config/Harden, Part-1

- Context
  - Purpose
    - Configure user interface for local system administrator visibility, control, control
    - Harden the system before connecting it to live Internet for software updates
    - Make some changes that could easily be deferred, but if already at the relevant GUI, make them now anyway
  - All of these changes are Preference (rather than Policy) settings
  - Most of these changes made with GUI, a few with command line

Config/Harden, Part-1 cont'd

- Context cont'd
  - Some changes computer-specific
  - Some changes are user-specific... naturally reflecting personal preferences
    - See references [1]..[3] for specific suggestions
    - These presentation slides reflect a subset items from presenter's personal checklist... selected for their security implications or likelihood they are less familiar than other items

Config/Harden, Part-1 cont'd

- Display Properties
  - Disable auto-start of desktop cleanup
  - Disable active content on desktop
  - Set screensaver to require password on resume
  - Configure power options for what's appropriate during configuration
    - Presenter always disables standby (but, still configures it to require a password when resuming from standby)
    - May want to defer hibernation support to Part-3... defragment the partition first... remember that hiberfil.sys will contain a persistent snapshot of memory, including cached secrets

Config/Harden, Part-1 cont'd

- Display Properties cont'd
  - There is overlap between UI settings in
    - Display Properties | Appearance | Effects
    - System Properties | Advanced | Performance Settings | Visual Effects
  - Suggestions
    - Adjust DPI before changing font sizes
    - If operating in different environments (w/ and w/o external monitor for example)
      - Changing font sizes with themes quick, no reboot
      - Changing DPI requries reboot
    - Clear type improves readability on most LCDs... for more control, use free ClearType Tuner utility from MS

Config/Harden, Part-1 cont'd

- Taskbar
  - Enable Administrative Controls on Start Menu
  - Consider disabling Personalized Menus
    - Or, adust the settings in Part-2 not to track user actions
- Recycle Bin
  - Adjust size, globally or by partition/disk
  - Configure the "Display Confirmation" option

Config/Harden, Part-1 cont'd

- Windows Explorer
  - Enable
    - Display contents of system folders
    - Show hidden files and folders
  - Disable
    - Automatically search for network folders and printers
    - Hide extensions for well-known file types
    - Hide protected operating systm files
    - Use simple file sharing
  - Offline Files: Return to this in Part-3, after disabling Fast User Switching
  - Suggestions
    - Configure one instance, than apply to all folders
    - Consider adding more columns to detailed view for creation and access times

Config/Harden, Part-1 cont'd

- Command Prompt
  - [User Pref] Create a copy of shortcut and then configure
    - Console properties for more optimal font and layout; quick edit mode
    - Shortcut properties to start cmd.exe in a different working directory (c:\temp for example)
    - Copy modified shortcut to [Start] button or quickstart
    - Remember to return this shortcut in Part-3 if using RunAs
  - File attributes
    - Four file attributes, toggled on/off independent of each other
      - R: Read-only
      - A: Archive
      - S: System
      - H: Hidden

Config/Harden, Part-1 cont'd

- Command Prompt cont'd
  - File attributes
    - Four file attributes, toggled on/off independent of each other
      - R: Read-only
      - A: Archive
      - S: System
      - H: Hidden
    - Even if (GUI) Windows Explorer configured to view all files, files with S or H attributes not visible with command line "dir" defaults

Config/Harden, Part-1 cont'd

- Command Prompt cont'd
  - File attributes cont'd
    - Even if (GUI) Windows Explorer configured to view all files, files with S or H attributes not visible with command line "dir" defaults
    - Illustration-1: dir /a
      - Doesn't hide files marked as System or Hidden
      - Can use environment variable dircmd to change default behavior... e.g. set dircmd=/a
    - Illustration-2:
      (attrib %systemdrive%*.* /s | find "A SH") > shFiles.txt
      - Writes names (and attributes) of all files stored on system drive, and marked as System and Hidden, to shFiles.txt
    - For even more visibility, use RootkitRevealer from sysinternals

Config/Harden, Part-1 cont'd

- TweakUI
  - Free utility from MS, part of WinXP Power Toys, requires installation
  - Security-related settings include
    - Explorer: disable Allow web content to be added to desktop
    - Explorer: disable Encrpt on context menu
      - Encryption good, but in-place decryption not so good (because unencrypted file still available through undelete... better practice to move files to encrypted folder)
    - My Computer | Autoplay | Types
      - Disable Autoplay for CD and DVD drives
      - Disable Autoplay for removeable drives
        - » Doesn't prevent system from detecting and configuring new USB devices

Config/Harden, Part-1 cont'd

- TweakUI cont'd
  - Security-related settings cont'd
    - Logon
      - Disable Parse Autoexec.bat at logon
      - Disable Show unread mail on welcome screen
      - Configure grace period for screen saver
  - Non-security user-preference settings to consider include
    - General: Disable unneeded frills
    - Mouse wheel: Some touchpad drivers interfere with ability to configure mouse wheel behavior through control panel, but TweakUI still gets it right
    - Explorer
      - Enable Detect accidential double clicks
      - Disable Maintain network history

Config/Harden, Part-1 cont'd

- System Properties
  - Computer Name
    - Membership in the "Workgroup" best left to honeypots and other "come and get me" targets
  - Hardware | Windows Update
    - Configure search behavior for as-desired, but never "...go without asking me."
  - System Restore
    - Configure disk space allocated to system restore points
  - Remote
    - Disable all remote assistance options

Config/Harden, Part-1 cont'd

- System Properties cont'd
  - Advanced | Performance | Settings
    - | Visual Effects: Your desired level of frilly stuff
    - | Data Execution Prevention: Enabled
      - Details depend on hardware support
    - | Startup and Recovery | System Failure
      - Enable "Write an event to the system log"
      - Disable "Send an administrative alert"
      - Disable "Automatically restart"
    - | Startup and Recovery | Error Reporting
      - Disable error reporting, but notify me...
  - Automatic Updates
    - Turn off Automatic Updates
    - Then, disable those annoying nag messages from Security Center
      - Via Security Center (systray) | Change the way Security Center alerts me

Config/Harden, Part-1 cont'd

- User Accounts
  - Ensure all user accounts are disabled unless required
  - Ensure all user accounts have reasonable passwords
    - Passwords will be required for logon after the next step...
    - Passwords will have to be changed after Part-2 to eliminate the LM hash
  - Configure logon method
    - Disable Use the welcome screen
    - Disable Use fast user switching

Config/Harden, Part-1 cont'd

- Internet Explorer
  - Home Page: Blank
  - Security
    - | Internet | Custom Level: Select High; then [reset]
    - | Intranet | Sites: Deselect everything
    - | Trusted Sites | Custom Level: Select Medium; then [reset]
    - | Trusted Sites | Sites
      - Disable Require server verification...
      - Add: microsoft.com
      - Add: <any other sites required for updates and known to be trusted for that purpose>

Config/Harden, Part-1 cont'd

- Windows Firewall
  - General
    - On
    - Don't allow exceptions
  - Exceptions: disable everything
  - Advanced: enable logging
    - Make a shortcut to logfile, place on desktop, etc.

Config/Harden, Part-1 cont'd

- Network interface properties... for every network connection
  - Disable every protocol not strictly required
    - Usually, everything except TCP/IP
    - Especially disable File and Printer Sharing
  - Configure TCP/IP
    - DNS: Disable Register this connection's address in DNS
    - WINS: Disable NetBIOS over TCP/IP
- Disable browser announcements
  - Command line: net config server /hidden:yes

Config/Harden, Part-1 cont'd

- Remove unnecessary Windows components
  - But, remember that they won't be updated
  - Presenter always uninstalls
    - Windows Messenger
    - MSN Explorer

Update Online

- Preferably
  - Using a hardware firewall in addition to software firewall
  - Still monitoring for unexpected traffic
- Windows update...
  - Takes a long while... repeat until no more
    - Anti-piracy controls need to be installed
    - Relevant updates available
  - Malware detection scan not too useful at this stage, but Windows Update and MBSA will whine later if you don't run it

Config/Harden, Part-2

- Context: Policies and Preferences
  - Policies and preferences include settings for
    - Computers
    - Users
  - Preferences
    - Reflect
      - Default choices configured at installation
      - Changes made by users, including local administrators
    - Configured through local GUIs
    - Stored in the local registry
    - Sometimes referred to as profile settings

Config/Harden, Part-2 cont'd

- Context: Policies and Preferences cont'd
  - Policies
    - Reflect settings specified by the (domain) administrator
    - Configured by Group Policy Editor
    - Policy settings also stored in the local registry
      - But in a different area than preference settings
      - With ACLs that deny changes by users
    - Policy settings take precedence over preference settings

Case		Behavior Configured By ____
Policy Present?	Preference Present?	
N	N	Default settings
N	Y	Preference settings
Y	N	Policy Settings
Y	Y	Policy Settings

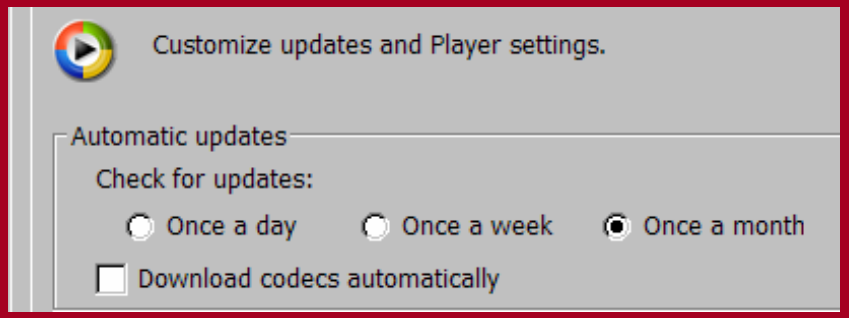
    - If a conflicting policy setting is removed, original user preference setting is restored

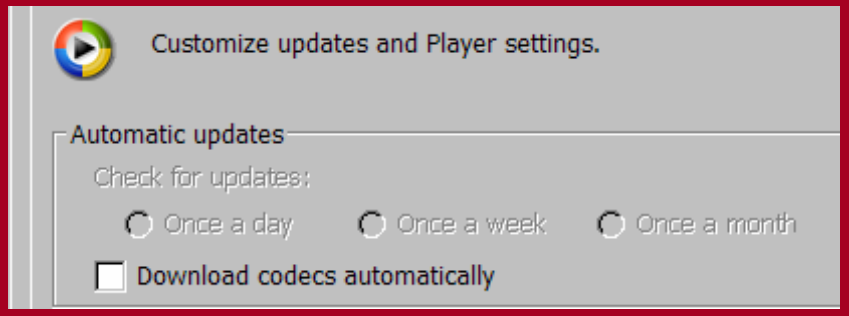
Config/Harden, Part-2 cont'd

- Context: Policies and Preferences cont'd
  - Domain motivation for using Policies
    1. Help administrators manage and increase security of their desktop computers
    2. To hide or disable a user interface that can lead users into a situation in which they must call the helpdesk for support
    3. To hide or disable new behavior that might confuse users
    4. To hide settings and options that might take up too much of users' time
  - Standalone motivation for using Policies
    1. Assume domain reasons 2-4 not relevant to these discussions
    2. Policies expose settings not configureable through preferences

Config/Harden, Part-2 cont'd

- Context: Policies and Preferences cont'd
  - Standalone motivation for using Policies cont'd
    - Illustration-1: Media Player
      - GUI-interface preferences constrain user choices to just how frequently media player should check for updates...
        No option for never
      - But, we can use group policy to disable all automatic updates





Config/Harden, Part-2 cont'd

- Context: Policies and Preferences cont'd
  - Standalone motivation for using Policies cont'd
    - User preference settings can be silently changed by an program, including installation programs
    - Illustration-2: Printer install
      - When Windows firewall configured just with preferences, installer running with admin privileges can silently change firewall configuration to perhaps open up an port for external inbound connections
      - When Windows firewall configured with group policy, installer attempt to modify firewall settings fails
        - » Local administrator can then evaluate... optionally making changes to policy so that installer doesn't puke over its failure to sneak a backdoor into the host computer

Config/Harden, Part-2 cont'd

- Context: Security Templates
  - Text files (*.inf) that contain security setting values
  - Can be modified and applied in domain environments using mmc snap-in: Group Policy Object Editor
  - Can be modified and applied in standalone environments using mms snap-ins:
    - Security Templates
    - Security Configuration and Analysis
  - Windows XP Security Guide describes how to use security templates for
    - Windows XP clients in an Active Directory Domain
    - Standalone XP clients

Config/Harden, Part-2 cont'd

- Context: Security Templates cont'd
  - Security templates
    - Provided by Microsoft and others for different environments and external requirements
    - Can be modular... can apply multiple templates to single DB used to analyze and configure
    - Can (and should be) edited for each role/system as-requried, considering
      - Advice from MS, DISA, and others
        - » See references [4]..[7] for background, context
        - » See references [8]..[13] for specifics
      - The (incremental) As-Is state of the target system
      - Special needs, experience, etc.

Config/Harden, Part-2 cont'd

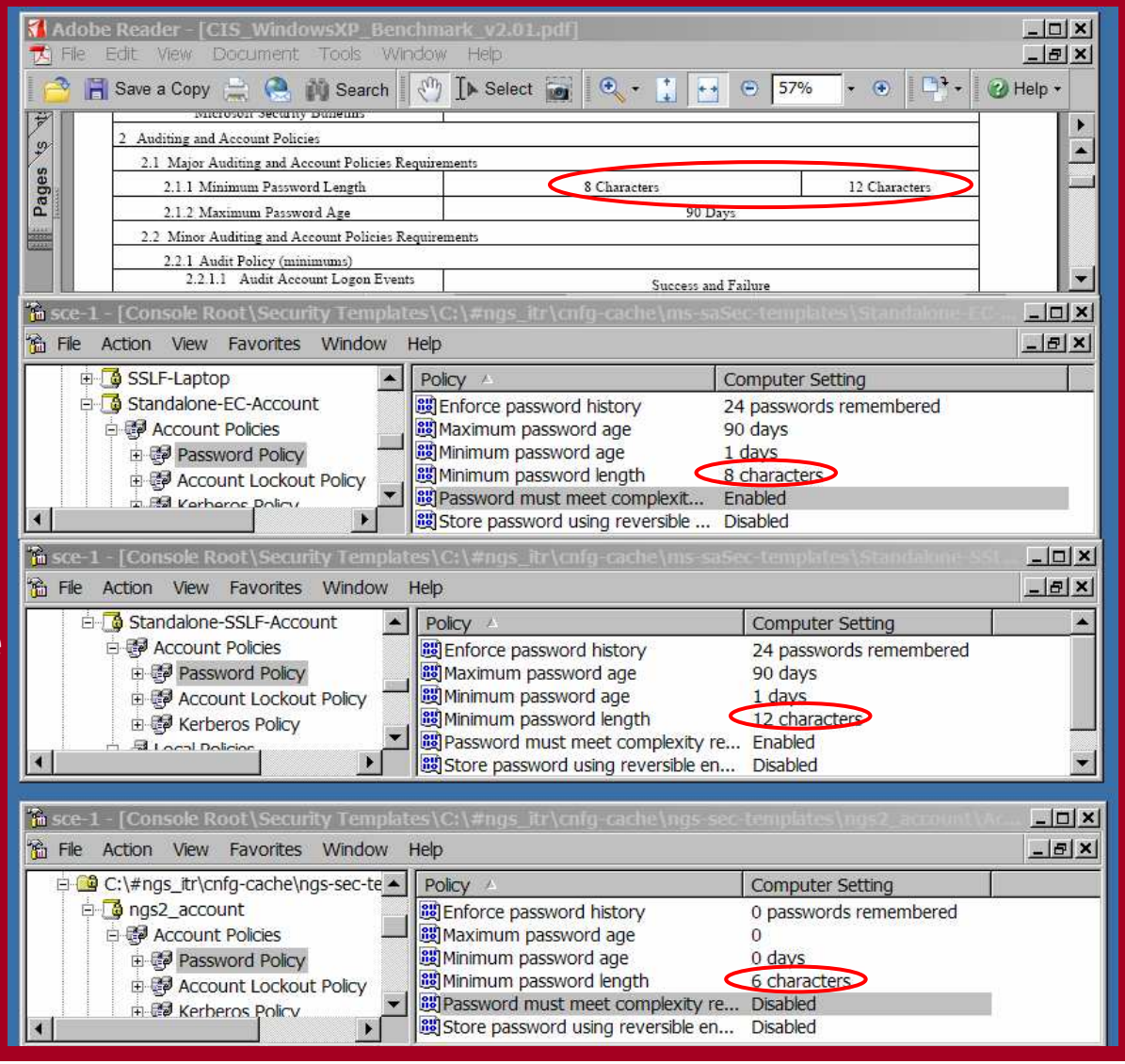
- Context: Security Templates cont'd | Illustration-1

CIS WinXP Benchmark Reference

MS Standalone EC-Account

MS Standalone SSLF-Account

Template being edited



Config/Harden, Part-2 cont'd

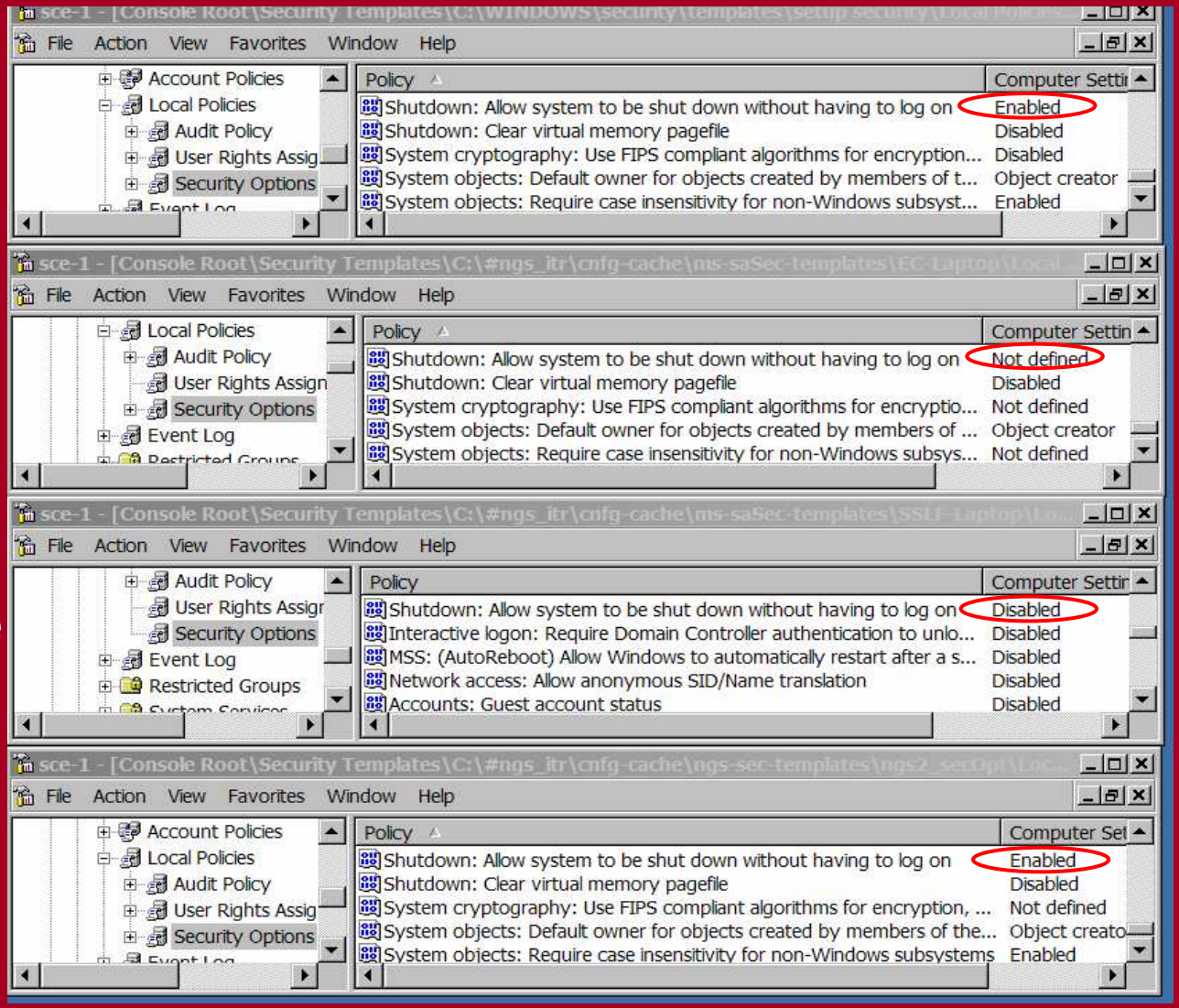
- Context: Security Templates cont'd | Illustration-2

Setup Security

MS Standalone EC Laptop

MS Standalone SSLF Laptop

Template being edited



Config/Harden, Part-2 cont'd

- Context: Security Templates cont'd
  - Selecting the most-useful value for customized template is inexact, debatable, very time-consuming, etc.
    - Quote from MS XP Security Guide: "The settings that should be included in this list could be debated extensively. In fact, this topic was discussed at great length by a group of security experts within Microsoft."
    - MS XP Security Guide, Appendix A identifies settings considered especially important... a good starting point
    - Some shortcuts used by presenter
      - Safe bets: Settings whose recommended value is the:
        - » Same from multiple sources for comporable environments
        - » Same across multiple environments
        - » Same across multiple revisions of the guidance documents

Config/Harden, Part-2 cont'd

- Context: Security Templates cont'd
  - Selecting the most-useful value cont'd
    - Some shortcuts used by presenter cont'd
      - More interesting settings:
        - » Any settings that fails any part of the safe bet criteria
        - » Any setting whose protective value is influenced by other factors
    - Illustration-3
      - The recommended values for password-related settings consider the risk of remote logons
      - If the laptop is configured to deny all remote logons, then consider adjustments to password length, duration, complexity, etc.

Config/Harden, Part-2 cont'd

- Context: Security Templates cont'd
  - Selecting the most-useful value cont'd
    - Illustration-4
      - If the choice is made to run with non-Administrator account, may want to grant some rights normally reserved for Administrators to non-Administrator group or account
        - » Example: Ability to disable a (wiredless) network connection from desktop icon... The risk of an unauthorized disruption of service might be less than the risk of unathorized access

Config/Harden, Part-2 cont'd

- Context: Administrative Templates
  - Text (Unicode) files (*.adm) used to expose registry-based policy settings
    - Administrative templates do not set the registry values, but rather expose the registry values as policy settings in the group policy editor
    - Must be used with group policy editor mmc snap-in (or, run gpedit.msc) to create local GPO that can be applied with gpupdate /force
  - Windows XP Security Guide describes how to use administrative templates
    - Only for Windows XP clients in an Active Directory Domain
    - Not for Standalone XP clients (but, some settings exposed only in the administrative templates)

Config/Harden, Part-2 cont'd

- Context: Administrative Templates cont'd
  - Microsoft's administrative templates for WinXP SP2
    - Include more 1,300 Administrative Template policy settings
      - Windows XP Security Guide only describes security-related policy settings
    - Located in %systemroot%\inf directory:
      - System.adm: Policy settings to configure the operating system
      - Inetres.adm: Policy settings to configure Internet Explorer.
      - Wuau.adm: Policy settings to configure Windows Update
      - Wmplayer.adm: OPolicy settings to configure Windows Media Player.
      - Conf.adm: Policy settings to configure NetMeeting
    - Should not be edited

Config/Harden, Part-2 cont'd

- Context: Administrative Templates cont'd
  - And...
    - Administrators and developers can add their own custom settings... which could also be used to configure registry-based preference settings
    - Separate templates are available for Office 2003
  - See reference [14]

- Context: Software Restriction Policies
  - Outside the scope of this discussion

Config/Harden, Part-2 cont'd

- Process: For reasons forgotten, or just nonsensical superstition, presenter's usual sequence for Part-2
  - 2-1: Review and adjust security templates
  - 2-2: Create group policy
  - 2-3: Apply security templates
  - 2-4: Make additional, manual, changes

Config/Harden, Part-2 cont'd

- 2-1: Review and adjust security templates
  - Using
    - Security configuration editor in Security Templates snap-in
      - After updating it for additional settings using scripts/instructions in Win XP Security Guide
    - Security Configuration and Analysis snap-in to always know the delta between as-is and as-specified
  - Note: These templates aren't applied immediately
    - But reviewing and editing them in Step 2-1 helps with the identification of settings that have to be made in Step 2-2

Config/Harden, Part-2 cont'd

- 2-1: Review and adjust security templates cont'd
  - Illustration-1: Presenter's security templates organized into five files to cover:
    1. User accounts
    2. Audit
    3. User Rights
    4. Security Options
    5. Services

<Snippet from Audit.inf>

```
MaximumLogSize = 4096
AuditLogRetentionPeriod = 0
[Security Log]
MaximumLogSize = 4096
AuditLogRetentionPeriod = 0
[Application Log]
MaximumLogSize = 4096
AuditLogRetentionPeriod = 0
[Event Audit]
AuditSystemEvents = 1
AuditLogonEvents = 3
AuditObjectAccess = 2
<snip>
```

Just changes from default, i.e., what auditing to enable

<Snippet from Audit.inf>

```
1="alerter", 4, ""
2="browser", 4, ""
3="cisvc", 4, ""
4="clipsrv", 4, ""
5="messenger", 4, ""
6="mnmsrvc", 4, ""
7="rdsessmgr", 4, ""
8="remoteaccess", 4, ""
9="schedule", 4, ""
a="ssdpsrv", 4, ""
b="termservice", 4, ""
c="tlntsvr", 4, ""
d="upnphost", 4, ""
```

Just changes from default, i.e., which services to disable

Config/Harden, Part-2 cont'd

- 2-2: Create group policy
  - Use Administrative Templates with Group Policy Editor for settings that
    - Can't be done otherwise
    - Are better expressed as policy rather than preference
  - Note: The language used to describe the options is sometimes convoluted, occasionally amusing
    - It's not just you...
  - When done, apply with gpupdate /force

Config/Harden, Part-2 cont'd

- 2-2: Create group policy cont'd
  - Illustration-1: Just snippets
    - Computer Config | Admin Templates | Windows Components | Netmeeting | Disable remote Desktop Sharing : enable (set)
      - No brainer
    - Computer Config | Admin Templates | Windows Components | Internet Explorer | Disable Periodic Check for Internet Explorer software updates
      - This removes the option for user preference, all users of this computer
      - Alternative: Configure as user preference
    - Computer Config | Admin Templates | Windows Components | Windows Messenger | Do not allow Windows Messenger to be run : enable
      - Defense in depth.. also prevents users (or malicious software) from using MSN Messenger

Config/Harden, Part-2 cont'd

- 2-2: Create group policy cont'd
  - Illustration-1: Just snippets
    - Computer Config | Admin Templates | Windows Components | Windows Media Player | Prevent Automatic Updates: enable
    - Computer Configuration | Administrative Templates | System | Turn off Autoplay: for all drives
      - Alternative registry edit:
        - » Path: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft \Windows\CurrentVersion\Policies\Explorer\
        - » Key: NoDriveTypeAutoR: DWORD; 0: Disable autoplay
      - Alternative: Use Tweak UI, but that changes a preference rather than a policy

Config/Harden, Part-2 cont'd

- 2-2: Create group policy cont'd
  - Illustration-1 cont'd
    - Computer Configuration | Administrative Templates | System | User Profiles | Maximum retries to unload and update user profile: 5
      - Determines how many times system tries to unload and update registry portion of user profile. (Does not affect system attemnpts to update files in user profile. When # tries exhausted, system stops trying... so user profile might not be current and local and roaming profiles might not match.
        - » Rate is not configurable: 1 try/second.
        - » Default value: 60 (So, takes one minute.)
      - Decrease this value for faster logoff/shutdowns... also consider MS UPHClean tool/service

Config/Harden, Part-2 cont'd

- 2-2: Create group policy cont'd
  - Illustration-1 cont'd
    - Computer Configuration | Administrative Templates | System | Internet Communication Management | Internet Communication Settings | ... <Disable most of this information leakage by enabling following restrictions:
      - Turn off the Publish to Web task for files and folders
      - Turn off Internet download for Web publishing and online ordering wizards
      - Turn off the "Order Prints" picture task
      - Turn off the Windows Messenger Customer Experience Improvement Program
      - Turn off Help and Support Center "Did you know?" content
      - <snip>
      - Turn off Search Companion content file updates
      - <snip>

Config/Harden, Part-2 cont'd

- 2-2: Create group policy cont'd
  - Illustration-1 cont'd
    - Computer Configuration | Administrative Templates | Network | Network Connections | Windows Firewall | Domain Profile | Windows Firewall | ...
      - <snip>
      - Windows Firewall: Allow remote administration exception: disabled
      - <sniop>
      - Windows Firewall: Allow UPnP framework exception: disabled
        - » Unless you trust everyone on your network and need this protocol traffic
        - » Allowing this traffic permits non-solicited traffic on tcp/2869 and udp/1900
    - Repeat for ... | Windows Firewall | Standard Profile |

Config/Harden, Part-2 cont'd

- 2-2: Create group policy cont'd
  - Illustration-1 cont'd
    - User Configuration | Administrative Templates | Start Menu and Taskbar
      - Turn off user tracking: set
      - Turn off personalized menus: set
  - When done, apply with gpupdate /force

Config/Harden, Part-2 cont'd

- 2-3: Apply security templates
  - Incrementally via Security Configuration and Analysis
  - For each template
    - Import template into DB
    - Analyze
      - If changes required... make them to template... restart
    - Configure
    - Analyze
  - Note: Templates can be addititive

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes...
  - Illustration-1: Set/confirm no autoplay, all drives
    - Via registry:
      - Keypath: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\
      - Key
        - » Name: NoDriveTypeAutoRun
        - » Value: 255
    - Via registry, just for CDROM
      - Keypath: HKLM\SYSTEM\CurrentControlSet\Services\CDRom
      - Key
        - » Name: Autorun
        - » Value: 0

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Illustration-2: Confirm MSN Messenger disabled
    - Via registry
      - Keypath: HKLM\SYSTEM\SOFTWARE\Policies\Microsoft\Messenger\Client
      - Key
        - » Name: PreventRun
        - » Value: 1

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Illustration-3: Confirm/set no instrumentation
    - Via registry
      - Keypath: HKCU\Software\Microsoft\Windows \CurrentVersion\Policies\Explorer
      - Key
        - » Name: NoInstrumentation
        - » Type: DWORD
        - » Value: 0 (or missing): Enable user tracking;
          1: Disable user tracking... disables customized menus, etc

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Illustration-4: Confirm/set Search Companion auto content updates and auto searches disabled
    - Via: Start | Search | Change Prefs | On the Internet | Change Preferences | With Classic Search
    - Via registry
      - Keypath: HKCU\Software\Microsoft\Internet Exporer\Main
      - Key
        - » Name: Use Search Asst
        - » Type: REG-SZ
        - » Value: "no"
    - Help and Support Center
      - Confirm auto searches disabled

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Illustration-5: Configure Media Player
    - Confirm auto updates disabled by GPO
    - Disable all other chedks
    - Disable script execution inside of IE
  - Illustration-6: Administrative shares
    - Context
      - Identified by "$" suffix on share name
      - Not visible via "net view"; but visible via "net share"
      - Created automaticially by windows to enable remote management

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Illustration-6: Administrative shares cont'd
    - Prevent default admin shares from being created
      - Via registry hack (ref MS KB 314984)
      - Keypath: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters
      - Key
        - » Name: AutoShareWks
        - » Type: DWORD
        - » Data: 0
      - *Or, use .reg file*

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Services to {evaluate, confirm-effect of security template, configure} include
    - Indexing
    - Remote Desktop
    - Windows Messenger
    - Alerter
    - Clipboard
    - SSDP Remote Discovery
      - To close listening UDP Port 1900
    - Windows Time
      - To close listening UDP port 123 (Network Time Protocol)

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Services to {evaluate, confirm-effect of security template, configure} cont'd
    - IPSec Policy Agent
      - To close listening UDP port 500 (ISAKMP)
      - To close listening UDP port 4500
      - Reenable if want to use IPSec packet filtering
    - Task Scheduler
      - To disable automatic virus runs, downloads, etc.
      - Note: Disabling Task Scheduler also disables application prefetching
    - NetBIOS helper service

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Note: Not all service dependencies obvious
    - Server seems like a good candidate to disable, but then some tools like MBSA fail to run
    - Lots of sources recommend disabling NLA... but, Windows Firewall uses NLA to determine which profile to use... if NLA isn't running, WFW uses a less-robust scheme...
  - Other areas of potential interest include
    - Disable Automatic Execution of Dr. Watson System Debugger
    - Delete shared folder (from MS-supplied cmd-files for hardening)
      - Command line: reg delete "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace\DelegateFolders\{59031a47-3f72-44a7-89c5-5595fe6b30ee}" /f
      - Confirm via registry...

Config/Harden, Part-2 cont'd

- 2-4: Make additional, manual, changes cont'd
  - Other areas of potential interest cont'd
    - Disable or configure UserAssist... definitely not described-by, recommended-by, or supported-by MS (or any of the other sources)
      - Details in 2005 NEbraskaCERT Conference Presentation
      - Options
        - » Clear tracking history
        - » Disable encryption of new entries
        - » Disable tracking
  - Reset all user account passwords to remove the stored LM hash
    - Applying the security template changed the setting, but LM hash (the weak 7+7 hash) is retained until the password is changed
  - Tweak host firewall... see references [15]..[16]

Config/Harden, Part-3

- Focus: Configure Applications and Utilities

- Illustration-1: Configure MSIE
  - Set start page: Blank is good
  - Privacy | Cookies
    - Accept first-party cookies
    - Block third-party cookies
    - Accept session cookies
  - Content | Personal Information
    - | AutoComplete
      - Uncheck all AutoComplete options
      - Clear saved forms, saved passwords
    - myProfile: None

Config/Harden, Part-3 cont'd

- Illustration-1: Configure MSIE cont'd
  - LAN Settings
    - Disable auto detect/config
    - Disable protocols that aren't needed
  - Programs
    - Internet Explorer should check to see whether it is the default browser: disable
    - Manage Add-ons
      - Show: Add-ons currently loaded...
      - Disable anything not required
  - Advanced... too many to discuss... some of them connected to zone settings

Config/Harden, Part-3 cont'd

- Illustration-2: Configure MSOE
  - Disable all previews
  - Plaintext only
- Illustration-3: Configure Firefox
  - Disable Headlines bookmark
  - Configure settings for automatic updates, personal information, etc.
- Illustration-X: Configure X for
  - Automatic updates, script behaviors, personal information, etc... X includes Acrobat Reader, MSO, etc.

Config/Harden, Part-4

- Configure User and Program Rights
  - Approach-1: RunAs
    - Normal user account is not an Admin account
    - Use pre-configured RunAs when non-Admin needs perform some task requiring elevated privileges
    - For details, see Bob McCoy's recent CSF Presentation (Reference [17])
  - Approach-2: DropMyRights and Software Restrictions
    - Normal user account is an Admin account
    - Run higher-risk programs like web browser with non-Admin rights
    - For details (scant), see Michael Howard's blog postings at MSDN (References [18]..[19])

References

- [1] TweakGuides Tweaking Companion; v3.10
  - www.tweakguides.com
  - Date: 200606
- [2] How can I customize a new Windows XP installation?
  - http://www.petri.co.il/customize_a_new_xp_installation.htm
- [3] Windows XP Security Checklist
  - http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm
  - Date: 20060817

References cont'd

- [4] The Administrator Accounts Security Planning Guide; v1.0
  - Microsoft
  - Date: 20060630
- [5] Regulatory Compliance Planning Guide Release Notes; v1.0;
  - Microsoft
  - Date: 20060707
- [6] The Security Monitoring and Attack Detection Planning Guide; v1.0
  - Microsoft
  - Date: 20050630
- [7] The Services and Service Accounts Security Planning Guide; v1.0
  - Microsoft
  - Date: 20050531
  - May 31, 2005

References cont'd

- [8] Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP; Version 2.0;
  - Microsoft
  - Date: 20051227
- [9] Windows XP Security Guide; v2.2
  - Microsoft
  - Date: 20060413
- [10] Windows XP Professional Operating System Legacy, Enterprise,and Specialized Security Benchmark Consensus Baseline Security Settings; Version 2.01
  - Center for Internet Security
  - Date: 200508
  - http://www.cisecurity.org (registration required)

References cont'd

- [11] WINDOWS XP SECURITY CHECKLIST; Version 5, Release 1.4
  - DISA
  - Date: 20060526
  - http://iase.disa.mil/stigs/iadocs.html
- [12] Windows 2003/XP/2000 Addendum V5R1; DISA Field Security Operations
  - DISA
  - Date: 20050829
  - http://iase.disa.mil/stigs/iadocs.html
- [13] Windows XP Gold Disk (public)
  - DISA
  - http://iase.disa.mil/stigs/SRR/winxp.zip

References cont'd

- [14] Using Administrative Template Files with Registry-Based Group Policy
  - Microsoft
  - Published: 200409
- [15] Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2;
  - Microsoft
  - Published 200408; Updated 200504
- [16] Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2
  - Microsoft
  - Published 200403; Updated 200411

References cont'd

- [17] Non Admin Today on Windows XP
  - Bob McCoy, CISSP/ISSAP, MCSE
  - http://www.nebraskacert.org/CSF/CSF-Jun2006.pdf
- [18] Browsing the Web and Reading E-mail Safely as an Administrator
  - MSDN Blog by Michael Howard
  - Date: 20041115
- [19] Browsing the Web and Reading E-mail Safely as an Administrator, Part 2
  - MSDN Blog by Michael Howard
  - Date: 20050113

Questions?

Contributions?