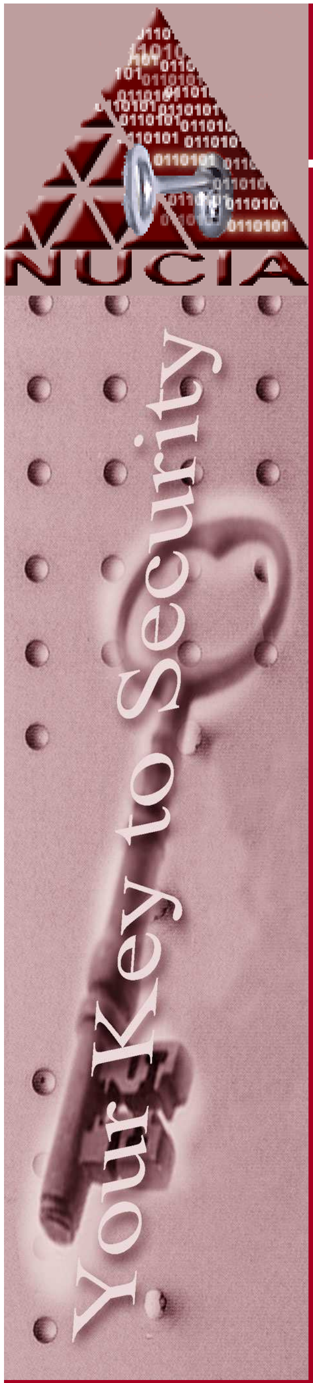


# Windows XP Hardening;
# Part 1 of 2

Prepared for NEbraskaCERT Cyber Security Forum
September 20, 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

# Speaker

- Stephen (Steve) Nugen, CISSP
  - Affiliations (biases)
    - UNO; IS&T; NUCIA
    - NEbraskaCERT Board of Directors
    - InfraGard Exec Board
    - NuGenSoft, LLC
  - Not offended when asked to mumble slower or with more articulation
  - Email welcome: smnugen@nucia.unomaha.edu;<br>smnugen@nugensoft.com

# Overview

- Approach
  - Not a tutorial or a step-by-step process
  - Pointers and observations to help you develop your own methods (with liberal re-use of course)
  - Slide contents reflect presenter's subjective views and experiences... your mileage may vary
  - Part-1 (today)
    - Laptop Challenges
    - Planning Resources
    - Tools - with focus on analysis
    - References
    - Limited Demos

# Overview

- Approach cont'd
  - Part-2 (update:  Scheduled for Oct CSF, lunch meeting)
    - Tools - with focus on configuration
    - Configuration demos
  - Caveat
    - These inspection methods and tools are meant for use on healthy systems
    - Forensic analysis and malware detection are different topics

# Laptop Challenges

- These challenges defined by
  - Assessment findings
  - Discussions with senior executives visiting NUCIA
  - Presenter's own experiences (frustrations) as a user

# Laptop Challenges cont'd

- Challenge-1: Laptops only secure when operated inside the protected enclave/domain
  - Laptops within your enclave protected and managed with
    - Documented policies
    - Defense-in-depth countermeasures such as
      - Perimeter firewalls
      - Professional installations and configurations
      - Group security policy settings
    - Secure operations

# Laptop Challenges cont'd

- Challenge-1 cont'd
    - Life is good... until some unfeeling user
        - Tears the laptop out of its protected domain, severing its connection to all that is good
        - Joins that laptop to vile unsanitary networks... collecting filthy viruses, spyware, device drivers, and other executables of dubious or unknown value
        - Rejoins that laptop to your domain... where it energetically shares its newly-acquired gifts from the wild side with all the other computers
            - Sometimes, this is nearly the only chance desktops have to experience a wider variety of executables

# Laptop Challenges cont'd

- Challenge-2: Unwashed laptops connect to your internal network
  - Clueless or unfeeling visitors (e.g., consultants, visitors, security assessors) connect their laptop of questionable *(or, at least unknown)* pedigree to your network
    - Just to check their email, or to print, or to access a shared folder, or...
    - Bypass perimeter firewall without the benefit of applying your domain policies to their laptop

# Laptop Challenges cont'd

- Challenge-3: You are the owner/operator of a mobile laptop *(but not clueless or unfeeling)*
  - You normally operate standalone, not part of any workgroup or domain
  - You sometimes connect your computer to multiple networks of questionable *(or, at least unknown)* trustworthiness
    - WiFi hotspots
    - Campus LANs... wired or wireless
    - Customer LANs... wired or wireless

# Laptop Challenges cont'd

- Challenge-3 cont'd
  - – You know better, but use a local Administrator account anyway because
    - It's a single-user laptop and you are both the user and the Administrator
    - Some security software (e.g. antivirus) won't run unless you run it as Administrator

# Laptop Challenges cont'd

- The underlying problems in these challenges aren't new
  - From 1993 NSA study [1]
    - Every component in a system must operate in a security environment that is a subset of its specified security environment
    - A component should not be asked to respond to events for which it was not designed and evaluated

# Laptop Challenges cont'd

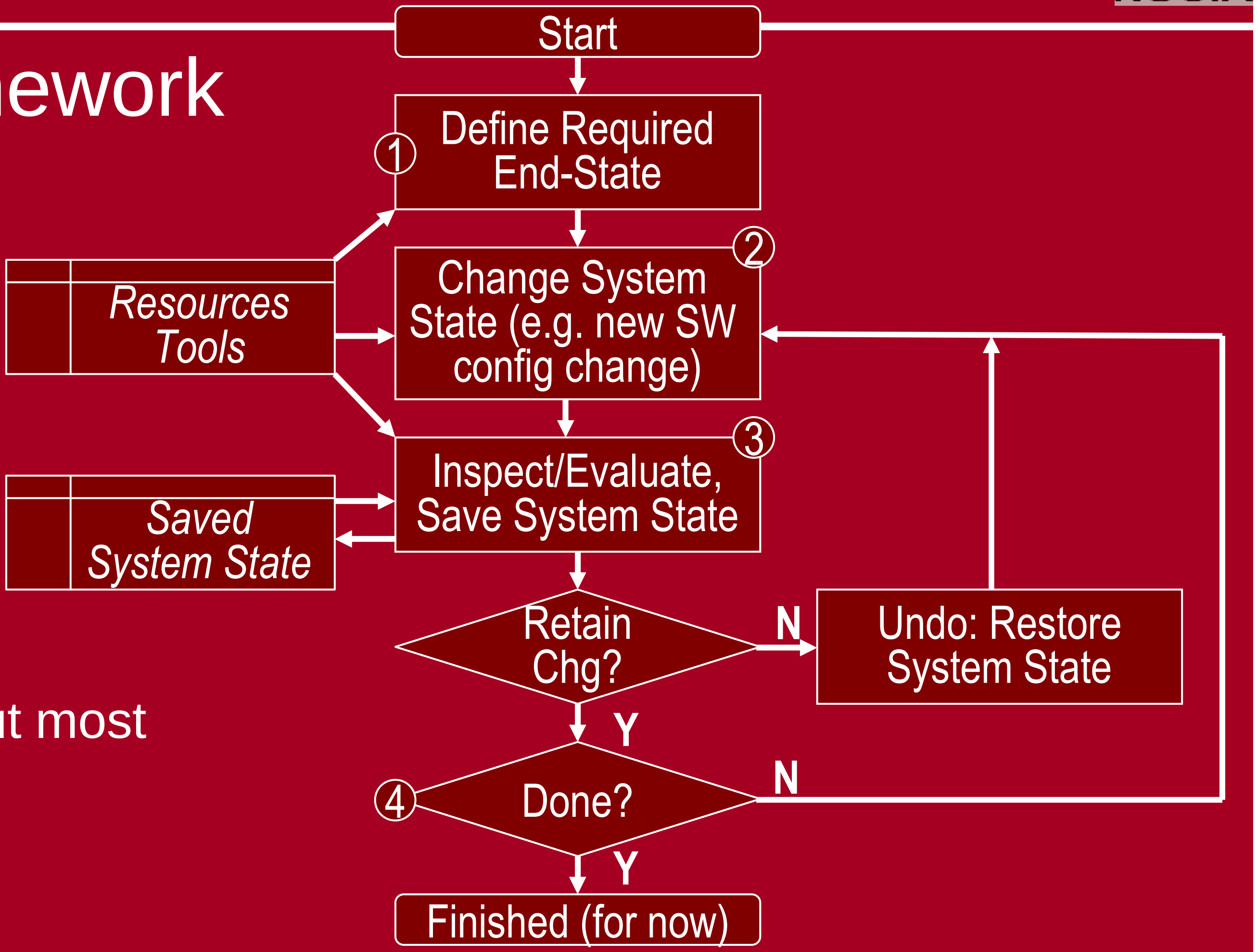
- Underlying problems aren't new cont'd
  - From 2004 DARPA study [2] commenting on [1]
    - This is a gross oversimplification, particularly for systems relying on other components on the Internet
    - It would be preferable to require that each component check that the environment in which it executes is a subset of its specified environment

# Laptop Challenges cont'd

- Underlying problems aren't new cont'd
  - Common practice
    - Pervert the meaning of [1] and [2] which define environments by what operations are permitted
    - Instead, define the environment to be the set of protective mechanisms... then nearly every set, including the null set, is a subset of the specified environment
  - Better practice
    - Implement sufficient protections on the host (laptop) itself so that they are always present

# Resources

- Context Framework


Start
1
Define Required End-State
2
Change System State (e.g. new SW config change)
3
Inspect/Evaluate, Save System State
Resources Tools
Saved System State
Retain Chg?
N
Undo: Restore System State
Y
4
Done?
N
Y
Finished (for now)

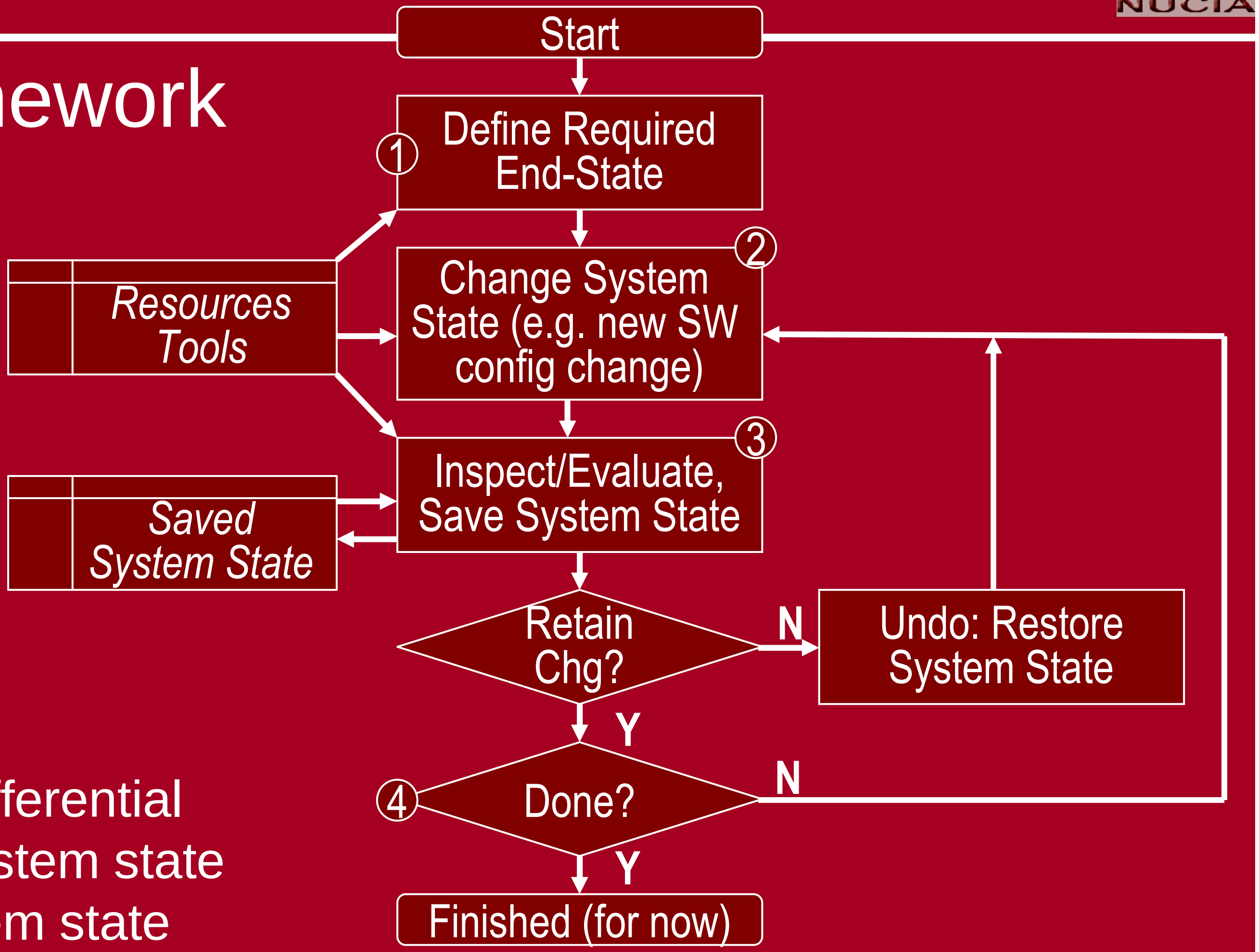
Ref (1): Hardest part, but most important

Ref (4): This test of "doneness" is really: Does the evaluated system state match the defined end-state?

# Resources cont'd

- Context Framework cont'd

Ref (2): Inspect/Eval once before making any changes... establish a baseline



Start

1 Define Required End-State

*Resources Tools*

2 Change System State (e.g. new SW config change)

3 Inspect/Evaluate, Save System State

*Saved System State*

Retain Chg?

N

Undo: Restore System State

Y

4 Done?

N

Y

Finished (for now)

Ref (3): Evaluation of system state includes differential analysis... comparing system state after the change to system state before the change... especially useful when loading device drivers and other software incrementally, measuring the impact of each new component

# Planning Resources

- Used to help define the required end-state
- MS Planning Guides
  - Security Risk Management Guide [3]
    - Four-phase process to measure and mitigate security risks to an acceptable level
    - Includes analysis tools
  - Regulatory Compliance Planning Guide [4]
    - Identifies MS software and guidance that can be used to address regulatory compliance issues

# Planning Resources cont'd

- MS Planning Guides cont'd
  - Administrator Accounts Security Planning Guide [5]
    - Plan your strategy for securing administrator-level accounts  [not so hard for single-user laptop]
  - Services and Service Accounts Security Planning Guide [6]
    - Addresses common problem of Windows services set to run with the highest possible privileges

# Planning Resources cont'd

- MS Planning Guides cont'd
  - Security Monitoring and Attack Detection Planning Guide [7]
    - Plan how to use Windows Security Event logs for security monitoring and detecting attacks... induces requirements for how to configure auditing and event logs

# Planning Resources cont'd

- MS Guidelines and checklists
  - Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP [8]
    - 355 pages describing different threats, potential countermeasures, and the potential impact of configuring these settings
    - Referenced by Windows XP Security Guide [9]
    - Includes tools and templates
      - Updates for Security Configuration toolset
      - Describes default security policy
    - Read the release notes for changed settings...
  - msThreat-and-Countermeasures

# Planning Resources cont'd

- MS Guidelines and checklists cont'd
  - Windows XP Security Guide [9]
    - Collaborative effort of NIST (National Institute of Standards and Technology); DHS (Department of Homeland Security); DISA (Defense Information Systems Agency); NSA (National Security Agency); CIS (Center for Internet Security)
    - Last updated in April, 2006
    - 172-pages recommending security settings to harden desktop and laptop client computers
    - Includes tools and templates, including definitions update for MS Security Configuration Toolset

# Planning Resources cont'd

- MS Guidelines and checklists cont'd
  - Windows XP Security Guide [9] cont'd
    - Considers three different environments
      - EC (Enterprise Client)
        - Client computers in an Active Directory domain
        - Managed through Group Policy
      - SA (Stand-Alone)
        - Client computers not members of an Active Directory domain
        - But, may need to communicate with systems that run Windows NT
        - *A looser definition than presenter is using for Standalone*

# Planning Resources cont'd

- MS Guidelines and checklists cont'd
  - – Windows XP Security Guide [9] cont'd
    - Considers three different environments cont'd
      - – SSLF (Specialized Security – Limited Functionality)
        - » Tighter security at a cost of significant loss of functionality and manageability
        - » Applies only to a few systems at a very small number of organizations, such as military and intelligence agencies
        - » "In other words, the SSLF settings are not a good choice for most organizations."

# Planning Resources cont'd

- MS Guidelines and checklists cont'd
  - Windows XP Security Guide [9] cont'd
    - Does not include settings which are not specifically recommended for one of the three environments... f
      - But, all the settings are described in Threats and Countermeasures... [8]
    - Read the release notes for changed settings... (but, don't assume every intended change is actually implemented...)
      - Example: Prevent the creation of (any new) 8.3 names in NTFS?
  - msXP-securityGuide

# Planning Resources cont'd

- CIS (Center for Internet Security)
  - A consensus security benchmark for Microsoft Windows XP Professional
    - Reflects input from NIST (National Institute of Standards and Technology); DISA (Defense Information Systems Agency); NSA (National Security Agency); GSA (General Services Administration); SANS; CIS (Center for Internet Security)
      - *Compared MS WinXP Guide contributors:  Replaced DHS with GSA and SANS*

# Planning Resources cont'd

- CIS cont'd
  - Different security settings for different operating environments
    - Legacy for systems that need to operate with older systems such as Windows NT, or in environments where older third party applications required
      - Security settings designed not to impact function or performance of the OS or applications already running

# Planning Resources cont'd

- CIS cont'd
  - Different security settings cont'd
    - Enterprise Desktop for clients operating in a in a managed environment where interoperability with legacy systems is not required
      - Security settings unlikely to affect the function or performance of the OS, but may impact applications
    - Enterprise Mobile  for clients that operate both on and away from the corporate network
    - Specialized Security – Limited Functionality for clients operating in very specialized domains
      - See MS WinXP Guide

# Planning Resources cont'd

- CIS cont'd
  - Document:  Windows XP Professional Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Baseline Security Settings [10]
    - Last update:  Aug, 2005
    - Focuses on local security policy settings
    - Summary checklists very nice... show the associated registry settings for the different security settings
    - Section 2 describes the security settings and the impacts of changing them (self-contained, but with less detail, than MS 2-book approach)

# Planning Resources cont'd

- CIS cont'd
  - Document cont'd
    - Appendix C lists some of the settings that are known to cause problems, and what types of problems may arise
    - Read the changes in Appendix E
    - cis-xpBenchmarkDoc
  - Scoring tool
    - Not generally free... read the license

# Planning Resources cont'd

- DISA (Defense Information Systems Agency)
  - – Document:  Windows 2003/XP/2000 Addendum [11]
    - Focus on exceptions or additions to the requirements described in other Microsoft or NSA documents, which include:
      - – Microsoft “Solutions for Security, Threats and Countermeasures: Security Settings in Windows 2003 and Windows XP,” 2003
      - – Microsoft Windows 2003 and XP Specialized Security – Limited Functionality Templates
      - – NSA Guide to Securing Windows XP, Dec 2003, Version 1.1
      - – *And, other Microsoft and NSA documents focused on Windows 2000 and Server 2003*

# Planning Resources cont'd

- DISA cont'd
  - Document: Windows XP Security Checklist [12]
    - Latest release: May 26, 2006; multiple documents
    - Describes compliance checks developed from DISA and NSA guidelines as well as the Windows Server 2003/XP security guides and security templates published by the Microsoft Corporation
    - More detailed than the other references
  - disa-xpSecChklst

# Planning Resources cont'd

- DISA cont'd
  - Gold Disk [13]
    - Documents folder includes [11] and [12]
    - A lot of knowledge and policy encoded in the XML files
    - For Windows XP Professional, automates 209 of the 238 required checks
    - disa-xpGoldDisk

# Planning Resources cont'd

- Other sources
  - The Tweaking Guides Tweaking Companion
    - Updated June 2006
    - Less-rigorous than DISA (well, duh), but describes usability settings related to security not included in the other references... another point of view [14]
    - tweakingCompanion

# Planning Resources cont'd

- Other sources cont'd
  - The Elder Geek Services Guide for Windows XP [15]
    - Focus is on performance
    - Recommendations differ from other sources... another point of view
  - Services are especially problematic
    - MMC services console doesn't report some functional dependencies
    - Ex:  Host firewall depends on NLA to determine which profile to use... if NLA not running, makes its own determination (which could be spoofed?)

# Planning Resources cont'd

- Using these planning resources
  - Different planning guides provide different consensus recommendations from different points of view
    - Have to reconcile the differences yourself
    - Multiple and/or really big monitors helpful for this task...

# Planning Resources cont'd

- Using these planning resources cont'd
  - Have to consider your own special needs
    - Illustration
      - Some of the recommendations address rights and privileges for users accessing laptop resources via network
      - But, if policy is to: (1) Share nothing and (2) Deny all external access to the laptop, then some of these settings may not apply

# Planning Resources cont'd

- Using these planning resources cont'd
  - Have to consider your own special needs cont'd
    - Long, complex, limited-duration passwords for local accounts are recommended to mitigate the risk of compromise from
      - Remote access to laptop *[may not apply]*
      - Theft *[not much protection]*
      - Non-theft snooping
    - Counterargument (to deciding some security settings don't apply)
      - Defense in depth
      - Things change

# Tools

- Tools used to inspect/evaluate; and to change the configuration
  - All tools are built-in (included with standard install of WinXP Pro) unless otherwise noted
  - Many of the built-in tools are accessed through Computer Management console... started by:
    - Run compmgmt.msc /s
    - Control Panel | Administrative Tools | Computer Management
    - Right-Click My Computer (if-enabled)
    - Programs | Administrative Tools | Computer Management (Note: May not be visible in program list until taskbar is configured)

# Tools cont'd

- Event logs
  - – Inspect/manage via Computer Management | System Tools | Event Viewer
  - – Three logs:  System, Application, Security
    - Security event log will be empty or nearly-so until auditing is configured
  - – Interesting entries can be copied to clipboard and then pasted into a system log (e.g., using notepad) along with observations, etc.... all part of documenting system state "snapshots"
  - – compMgt-evLogs

# Tools cont'd

- Device Manager
  - Via Computer Management | System Tools | Device Management
  - Configure environment to force Device Manager to display all devices
    - One time (to enable view of hidden ghost devices)
      - Set System Environment Variable: devmgr_show_nonpresent_devices=1
    - Every time, in devmgr: View | Show hidden devices

# Tools cont'd

- Device Manager cont'd
  - Ghost devices could be relevant
    - When trying to understand a log entry
    - To determine what devices the laptop connected to outside the enclave
  - Look for problem devices
    - Illustration: Intel wireless choices
      - (1) Use insecure drivers that don't leak resources
      - (2) Use secure drivers that leak memory
      - (3) Don't install the driver... get worried if wireless not detected as a problem device
  - compMgt-devMgr

# Tools cont'd

- Log files
  - Look in (%windir%) for*.log *.txt
    - Sort by creation time and access time (customize columns in windows explorer)
    - Logs of potential interest just after install include (assuming c:\windows): c:\windows\setuperr.log; c:\windows\setuplog.txt; c:\windows\setupapi.log; c:\windows\setupact.log
  - Also examine c:\windows\system32\wbem\logs
    - Can control the logging level through WMI
    - compMgt-WMI

# Tools cont'd

- System Information tool
  - Run msinfo32; or access through Help | Tools | Advanced System Information; or via Programs | Accessories | System Tools | System Information
  - View | Current Information
  - View Components | Problem Devices
  - View Software Environment | Startup Programs
    - This list won't be complete

# Tools cont'd

- System Information tool cont'd
  - Save everything via File | Export
    - Useful when trying to figure out when (in connection with what change to the system) a device driver changed
    - Useful when trying to understand terse log file entries
  - msinfo32

# Tools cont'd

- DirectX Diagnostic
  - Run dxdiag
  - Multimedia-focused system information, diagnostic tools
  - Can save snapshots... compare to later snapshots

# Tools cont'd

- System Configuration tool
  - Run msconfig
  - Check Startup Programs at Startup Tab
    - Different results than from System Information Tool
  - Check running services
  - Can also use to configure restrictions on startup... to recover after a bad change

  - msconfig

# Tools cont'd

- Sigverif:  Verify digital signatures on operating system files
  - Run sigverif;
    or launch from System Information | Tools
  - Configure before starting the scan
    - Advanced | Search
      - Look for other files not digitally signed
      - Search in %windir% and subfolders
    - Advanced | Logging
      - Save results to log file
      - If scanned before, copy existing file before overwriting; use a different log file; or append

# Tools cont'd

- Sigverif cont'd
  - Scan... not a very quick process
  - Inspect results
    - Sort by clicking on column titles
    - Change width of columns
  - Save the log file
    - Advanced | Logging | View Log | Save As
  - sigverif

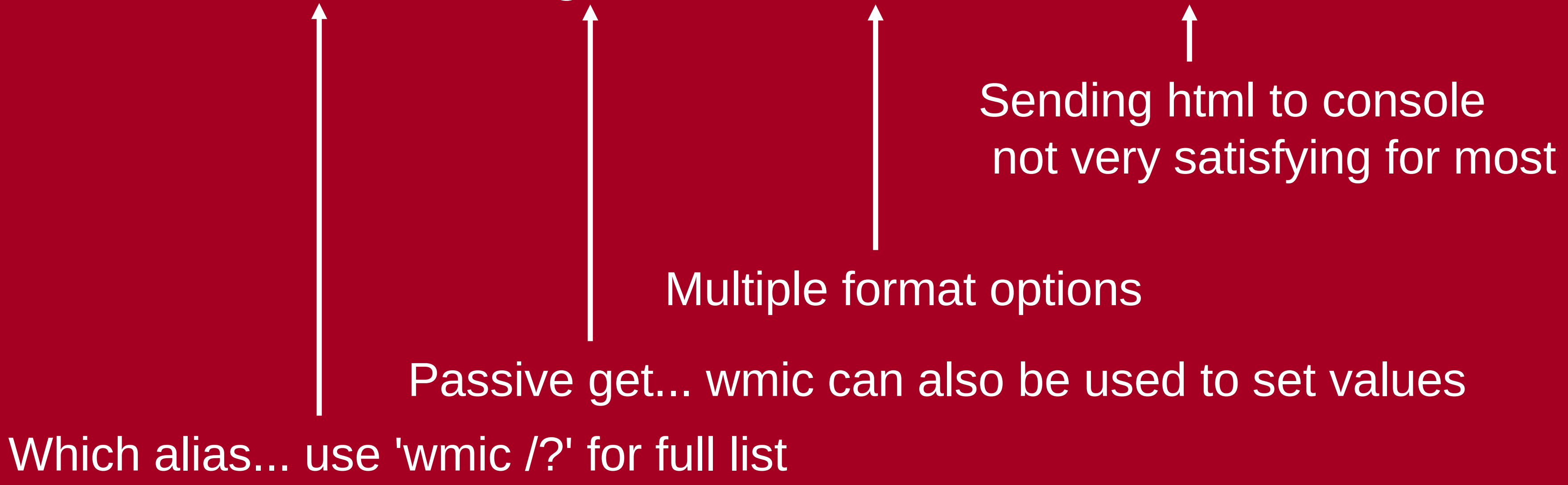
# Tools cont'd

- Determine if software install caused creation of a system restore point
  - – Via System Configuration Tool; or via <Help>

# Tools cont'd

- Query WMI via wmic
  - A method of querying the WMI database from the command line, scriptable
  - Included with WinXP, but not well-known or well-documented
  - Illustration-1:

```
wmic service get /format:hform > service.htm
```



Sending html to console not very satisfying for most

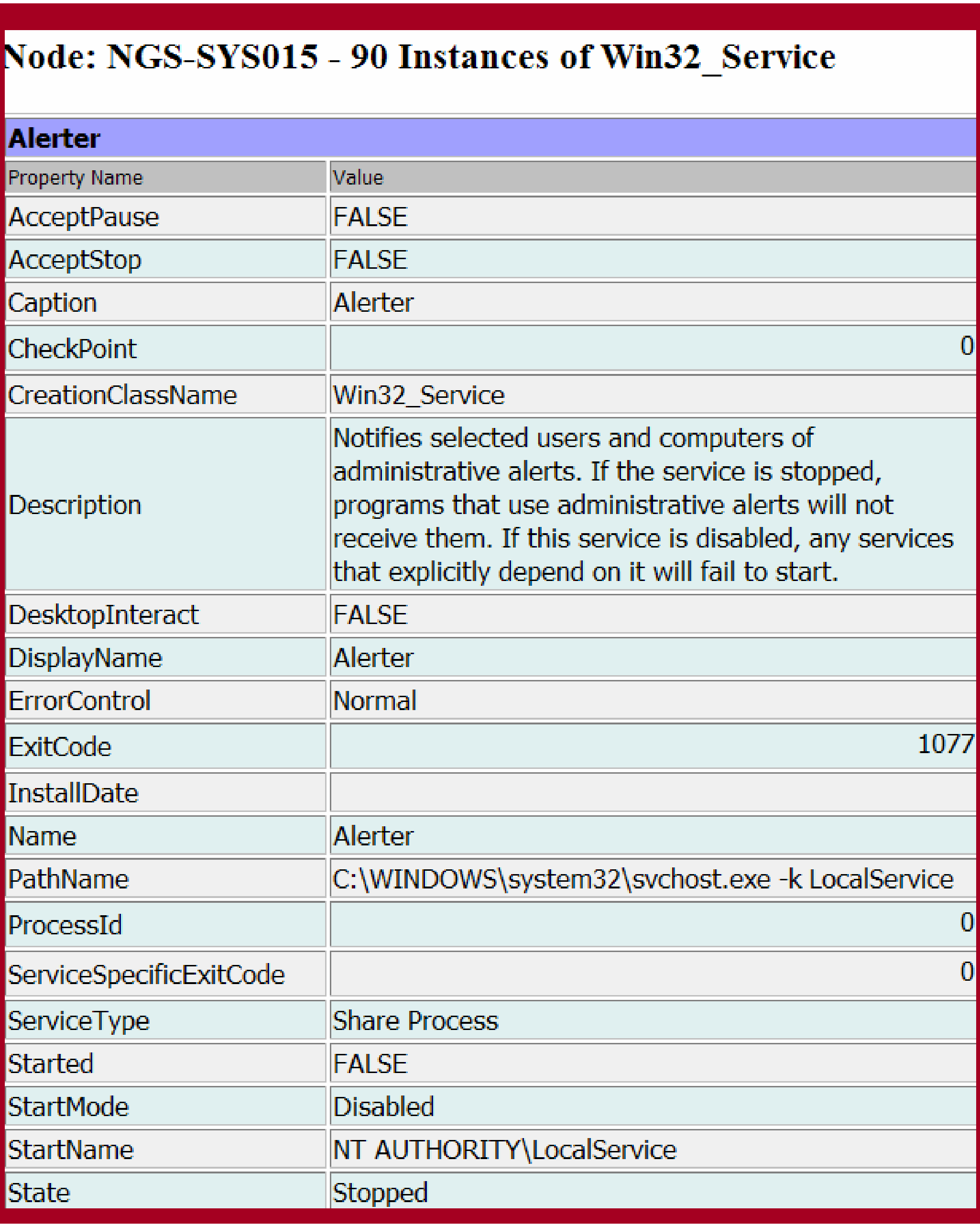
Multiple format options

Passive get... wmic can also be used to set values

Which alias... use 'wmic /?' for full list

# Tools cont'd

- wmic cont'd
  - snippet



**Node: NGS-SYS015 - 90 Instances of Win32_Service**

**Alerter**

| Property Name | Value |
|---|---|
| AcceptPause | FALSE |
| AcceptStop | FALSE |
| Caption | Alerter |
| CheckPoint | 0 |
| CreationClassName | Win32_Service |
| Description | Notifies selected users and computers of administrative alerts. If the service is stopped, programs that use administrative alerts will not receive them. If this service is disabled, any services that explicitly depend on it will fail to start. |
| DesktopInteract | FALSE |
| DisplayName | Alerter |
| ErrorControl | Normal |
| ExitCode | 1077 |
| InstallDate | |
| Name | Alerter |
| PathName | C:\WINDOWS\system32\svchost.exe -k LocalService |
| ProcessId | 0 |
| ServiceSpecificExitCode | 0 |
| ServiceType | Share Process |
| Started | FALSE |
| StartMode | Disabled |
| StartName | NT AUTHORITY\LocalService |
| State | Stopped |

# Tools cont'd

- wmic cont'd
  - Snippet from script Nugen uses
    - echo getting information about groups
    - wmic group get /format:hform > group.htm
    - echo.
    - echo getting information about useraccounts
    - wmic useraccount get /format:hform > useraccount.htm
    - echo.
    - echo getting information about systemaccounts
    - wmic sysaccount get /format:hform > sysaccount.htm

# Tools cont'd

- Autoruns:  Inspect autostarts
  - From www.sysinternals.com  (get it while you can)
  - Can deselect Microsoft entries from the display to reduce clutter
  - Save results at every step... can use them for later comparisons where Autoruns flags new entries by with a green background
  - autoruns

# Tools cont'd

- Filemon: Inspect level of file activity
  - From www.sysinternals.com
  - What level of file activity when the system is "quiet"?
  - If there is recurring activity, which processes are accessing which files?
  - Good for detecting "noisy" drivers, utilities, applications
  - Useful in debugging programs... what files are they trying to access?

# Tools cont'd

- Filemon cont'd
  - Useful in debugging slowdowns... what file accesses are timing out?
  - Results can be saved
  - filemon

# Tools cont'd

- Regmon: Inspect level of registry activity
  - From www.sysinternals.com
  - What level of registry activity when the system is "quiet"?
    - Running Regmon itself causes a flurry of activity
    - Some installations finish after next reboot; wait for that to finish before measuring baseline activity
    - Suggestion: After initial activity, clear display, then capture for 10 sec to determine registry operations/sec

# Tools cont'd

- Regmon cont'd
  - If there is recurring activity, which processes are accessing which registry keys?
  - Results can be saved
  - Useful for detecting all sorts of activity related to polling
    - "Hot Key" utilities
    - "Show [network] icon in notification area when connected"
    - VMWare
  - regmon

# Tools cont'd

- Process Explorer
  - From www.sysinternals.com
  - Provides much more information than built-in task manager
    - Shows details by process (memory sizes, I/O, CPU, command line, which services it's hosting, open files, etc.
    - Very useful when trying to map activity or open network port by PID when PID just resolves to one of six 'svchost' processes
      - If process explorer not avail, use 'netstat -anb'
  - processExplorer

# Tools cont'd

- TCPView
  - From www.sysinternals.com
  - Can save results
  - tcpView

# Tools cont'd

- netstat
  - Command-line, scriptable, can redirect output
  - netstat -an (report open ports)
  - netstat -nab (adds process information)
  - netstat -s (statistics by protocol... look for errors)
  - netstat -r (reports host routing table)
    - Look for new networks (added by Mare for example)

# Tools cont'd

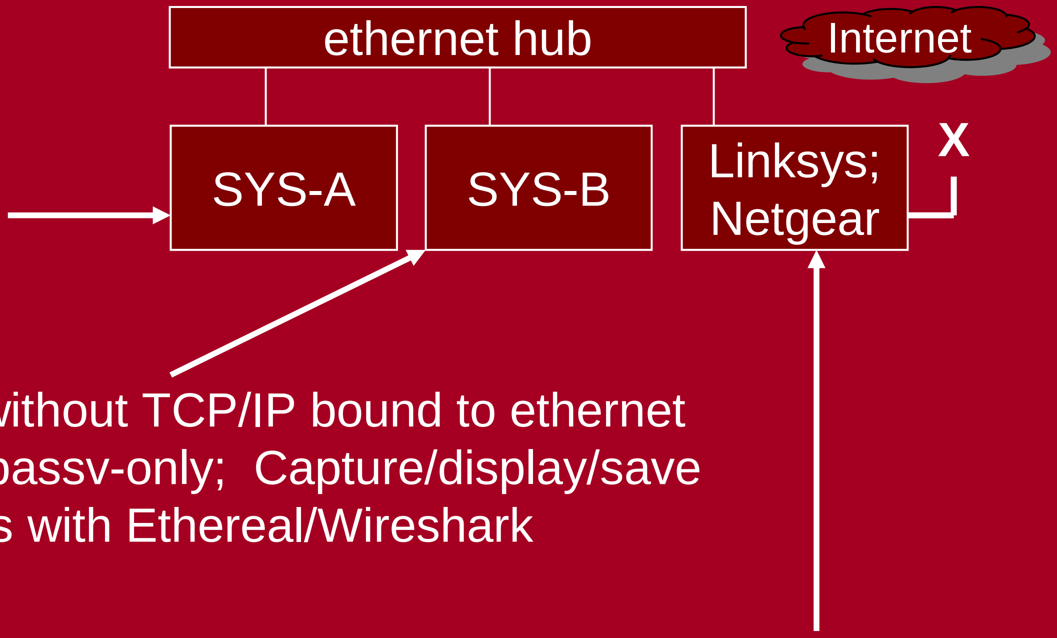
- netsh
  - Command-line, scriptable, can redirect output
  - Useful commands, always redirecting output to file (or paginate)
    - netsh firewall show config verbose = ENABLE
    - netsh firewall show state verbose = ENABLE
    - netsh diag show all /v
  - Netsh allows view and sets to firewall attributes for both domains (standard and domain)... not available through the GUI

# Tools cont'd

- netsh cont'd
  - Illustration (presenter's experience)
    - Installed network printer for <Vendor-Withheld> All-In-One device
    - Installer silently reconfigured the host firewall...
      - If running as admin, then change was silent, detected afterwards with netsh
      - If policy prohibited exceptions, installer complains and fails... better than a silent change
    - Same installer tries to map memory card slot on printer to local drive letter... detected by FileMon when Office Save As operations slowed

# Tools cont'd

- Sniff traffic... even if only DNS queries
  - Physical



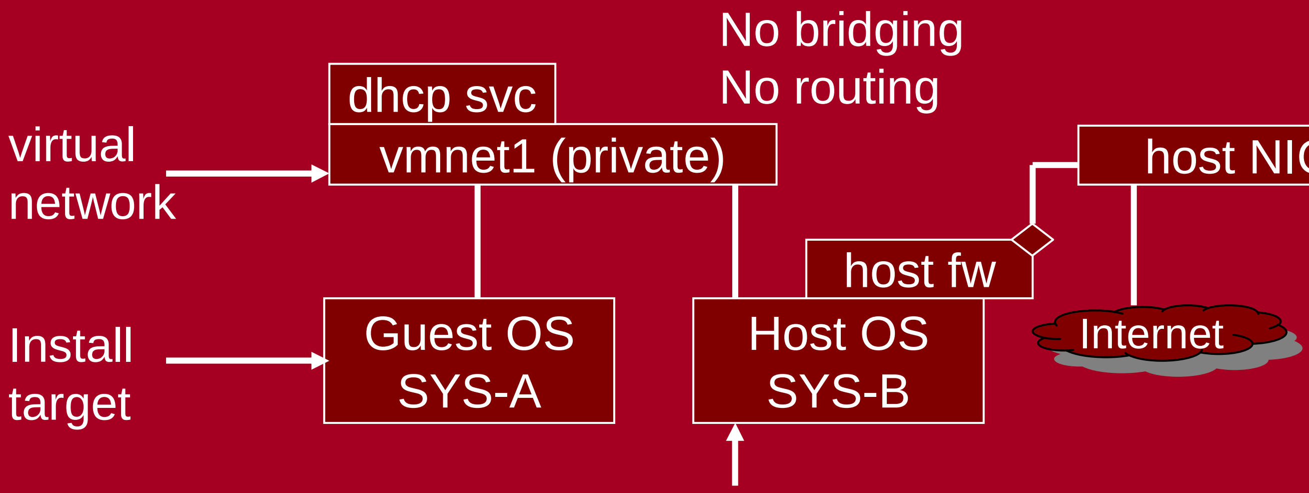
Install target

Win2K/XP without TCP/IP bound to ethernet adapter so passv-only; Capture/display/save network pkts with Ethereal/Wireshark

Cheap cable modem router/firewall with DHCP server;
LAN configured; WAN configured with DNS server addresses,
but no WAN connection to Internet

# Tools cont'd

- Sniff traffic... even if only DNS queries
  - Virtual



No bridging
No routing

virtual network

dhcp svc

vmnet1 (private)

host NIC

host fw

Install target

Guest OS
SYS-A

Host OS
SYS-B

Internet

use "normal" or special VMware tools
to monitor traffic on self-contained network

Watch applications contacting (or trying to contact) their web sites without warning during or afterwards... even if you instruct them not to register and/or never to check for updates... including (in presenter's experience): Zone Alarm, HP, Roxio, Winpcap, Powerlink, etc.

# Preview of Part-2

- Using Security Configuration Toolset (built-in) and templates to
  - Save the system state of a computer as a template
  - Change the state of a computer to match the template
- Using administrative templates with GPO to further configure the host

# Preview of Part-2 cont'd

- Coolness
  - Microsoft, DISA, and others provide templates you can use as starting point for your own
  - Templates aren't hardware-specific, so can be shared across hosts from different vendors (unlike Ghost images)
  - GPO offers more control over settings than is possible otherwise
    - Illustration:  User GUI to media player doesn't provide an option for no automatic checks for updates... but that setting is available through administrative templates

# Preview of Part-2 cont'd

- Two different approaches to running as Admin
  - Don't
    - Use RunAs instead
    - Consider assigning some rights normally reserved for Administrators to non-Administrator group for routine maintenance
  - Run as Admin, but use software restrictions (DropMyRights) when using applications like browsers and email clients
    - Not well-documented (or supported)

# References

- [1] NSA ISSO INFOSEC Systems Engineering study on rules of system composition
  - P. Boudra, Jr. Report on rules of system composition: Principles of secure system design
  - Technical report, National Security Agency, Information Systems Security Organization, Office of Infosec Systems Engineering, I9 Technical Report 1-93, Library No. S-240, 330, March 1993.
- [2] DARPA CHATS Report
  - Neumann, Peter G.  Principled Assuredly Trustworthy Composable Architectures:
  - Final Report, December 26, 2004; http://www.csl.sri.com/neumann/chats4.html

# References cont'd

- [3] Security Risk Management Guide; v1.2; March 15, 2006
  - Licensed under the Creative Commons Attribution-Non Commercial License
  - TechNet: http://go.microsoft.com/fwlink/?linkid=30794
  - Download: http://go.microsoft.com/fwlink/?linkid=32050
- [4] Regulatory Compliance Planning Guide Release Notes; v1.0; July 7, 2006
  - Licensed under the Creative Commons Attribution-Non Commercial License
  - TechNet: http://go.microsoft.com/fwlink/?linkid=56114
  - Download: http://go.microsoft.com/fwlink/?linkid=56419

# References cont'd

- [5]  The Administrator Accounts Security Planning Guide; Version 1.0; June 30, 2005
  - TechNet:  http://go.microsoft.com/fwlink/?LinkId=41315
  - Download: http://go.microsoft.com/fwlink/?LinkId=41316
- [6]  The Security Monitoring and Attack Detection Planning Guide;  Version 1.0; June 30, 2005
  - TechNet:  http://go.microsoft.com/fwlink/?LinkId=41309
  - Download: http://go.microsoft.com/fwlink/?LinkId=41310
- [7]  The Services and Service Accounts Security Planning Guide; Version 1.0; May 31, 2005
  - TechNet:  http://go.microsoft.com/fwlink/?LinkId=41311
  - Download: http://go.microsoft.com/fwlink/?LinkId=41312

# References cont'd

- [8] Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP; Version 2.0; December 27, 2005
  - TechNet:  http://go.microsoft.com/fwlink/?LinkId=15159
  - Download: http://go.microsoft.com/fwlink/?LinkId=15160
- [9]  Windows XP Security Guide; v2.2; April 13, 2006
  - Licensed under the Creative Commons Attribution-Non Commercial License
  - TechNet: http://go.microsoft.com/fwlink/?linkid=14839
  - Download: http://go.microsoft.com/fwlink/?linkid=14840

# References cont'd

- [10] Windows XP Professional Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Baseline Security Settings; Version 2.01; August, 2005
  - http://www.cisecurity.org (registration required)
- [11] Windows 2003/XP/2000 Addendum V5R1; DISA Field Security Operations; 29 August 2005
  - http://iase.disa.mil/stigs/iadocs.html
- [12] WINDOWS XP SECURITY CHECKLIST; Version 5, Release 1.4; May 26, 2006
  - http://iase.disa.mil/stigs/iadocs.html
- [13] Publicly available Windows XP Gold Disk
  - http://iase.disa.mil/stigs/SRR/winxp.zip

Questions?

Contributions?