Global Information Assurance Certification Paper

Ratish Pillai
Thursday, March 11, 2004
GSEC Practical Assignment 1.4b Option 1

A PRIMER FOR WINDOWS 2000 SECURITY MAINTENANCE

TABLE OF CONTENTS

1. SETTING THE SCOPE

1.1 Abstract

Windows 2000 is widely deployed in many corporations, homes, and in various organization data networks today. This paper is meant to be a guide to individuals responsible for maintaining stability, security, and confidentiality of network systems for their organization. By using a combination of tools, and information I hope to show that they are many aspects to be aware of in maintaining security in a Windows 2000 network.

1.2 Background

Windows 2000 Professional and Windows 2000 Server is now deployed in thousand of locations around the world. It is an astounding improvement from the days of Microsoft Windows for Workgroups, and Microsoft Windows NT 4.0. Microsoft was finally able to supply the consumers with a reliable network operating system. Windows 2000 features amazing improvements in performance, stability, features, and most importantly security. None the less the out of the box setup and the supplied tools is not enough to secure your environment. Furthermore Active Directory, NTFS permissions, Kerberos etc. do require strong understanding of various areas for you to be successful. If you really want to be able to sleep at night you have to spend a lot of time, and invest in resources to do so. This paper will not only solely focus on only extremely technical details of hacking utilities, firewall rules etc.. Instead the focus will be an overall broader approach to securing a Windows 2000 environment. We cannot depend on any one program, person or piece of hardware to ensure the safety of our systems. Therefore having the proper foundation, being diligent with periodic security tasks, being rational and good problem solving skills is imperative. Having the right state of mind is just as important as mastering ones technical abilities. I feel with those basic “street smarts” individuals can succeed, that may lack the highest level of security training. A lot of IT’s function stems down to making the right decision given the situation. Therefore having the right attitude and mindset will help you deal with a crisis or better yet prevent one!

1.3 Disclaimer and Assumptions of audience

- By no means is this a complete guide to securing a Windows 2000 environment ,
    - Please, consult multiple sources to have a iron clad solution
- Always try to stay current with latest exploits, and tool with sites mentioned in this guide
    - This information will get outdated, but the concepts will probably remain about the same
- Your or your team should possess experience building systems with
    - Microsoft Windows 2000 Server, Advanced Server
    - Microsoft Windows 2000 Professional
- Strong knowledge of Active Directory, and experience with group policies
- Active Directory is running in Native mode on your network
- Good grasp of TCP/IP, and network protocols
- Your organization must be committed to funding and backing up your findings in order to secure your organization
- You have access to adequate test labs, which match the configuration of you productions system at your organization
- Authorization from your organization to use network monitoring, password cracking tools, and network reconnaissance tools

1.4 The focus

The operability of network systems is no easy task, and it only seems to get harder. But, the key is to work smarter not harder with the adversities you will no doubt face as an admin in a Windows 2000 environment. Most organizations have cut back on IT staff or currently in a hiring freeze, but still expect their environment to be secure for all employees. This pressure can be mitigated with proper planning, resources, and calm mind to deal with the bombardment of events present in your environment. My goal is to focus on tasks required on frequent basics to ensure operability of Windows 2000 systems.

1.4.1 Focus Points

We will focus on key areas that a network administrator or authorized individuals should pay special attention to. Always keep in mind hackers, and users with malicious internet are always developing new techniques to penetrate your network. That is why it is important to stay up to date with the latest scanning tools, hot fixes, and to subscribe to multiple vulnerability mailing lists. Government and security organizations like NIST, NSA, Microsoft, Security Focus and Neohapsis are a few great resources to consult.

Our main focus with be on the following topics

1. A secured Windows 2000 environment
2. Patch, and Exploit management
3. Auditing your environment with the right tools
    a. The importance of a Syslog server, and Event ID

2. SECURED ENVIRONMENT

2.1 Where do I find the required Information?

Windows 2000 is highly configurable in many aspects. You can change settings in the registry, Group Policy, Local security Policy, use security templates, OU Units in Active Directory etc. We are lucky enough that NIST (National Institute of Standards and Technology) has made available unclassified document available to the public. In some respect gives you free information to secure your systems to government standards! You can download security templates from NIST @ http://csrc.nist.gov/itsec/NIST_Win2KPro_R1.2.3.zip , and the comprehensive guide from http://csrc.nist.gov/itsec/NIST_Win2KPro.zip.

If you prefer Microsoft official guide it is available for Windows 2000 at http://www.microsoft.com/downloads/details.aspx?familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56&displaylang=en

Labmice.net guide to securing Windows 2000 is quicker read guide available at http://labmice.techtarget.com/articles/securingwin2000.htm.

Also do not forget the all powerful Google.com, and Google groups search engines, my personal favorites.

2.2 Key areas that must be hardened

As I mentioned earlier the best security solution should be tailored to your environment and most probably combine all available security resources to lead to a secure system. Some of the fixes that will be mentioned are detailed to setup. We could focus on this topic alone, but my goal is too point you in the right direction. This section may take time to complete depending on the state of your servers, but once complete you have a more sterile environment to monitor, and audit. The areas discussed below revolve around NIST's free security templates made by security experts in various branches of the government. Probably one of the best freebies, you can find. Since these changes are lengthy, therefore a shortened version with page numbers has been supplied. I suggest you print out the NIST Win2k document and place in a 3 ring binder for your department, and copy the templates to an admin share on your network. Furthermore using NIST as resource is a good example of working smart! If you had to make the polices form scratch, you would have wasted time better spent managing your network, and sleeping.

2.2.1 Customize a secure Windows 2000 security template from NIST/NSA

- See NIST guide for details (Souppaya, et. All, 4-1 – 4-5)
- Export current settings into a backup template
- Import NISTWIN2KPRO.INF mentioned above in section 2.1
- Customize the policy to the need of your environment
- TEST THOUROUGLY in test lab or on non business critical machines
- Roll out to your environment slowly from least important to business critical in a staggered fashion
- Export the file to a custom file name for Internet use
- Enable IPSEC between servers, and Use 3DES in between servers for communication

2.2.2 Use new policy to import into GPO for use current OU units

- See NIST guide for details (Souppaya, et. All, 4-5 – 4-10)
- You can push the GPO to any OU contain in your forest
- Be very careful in pushing security changes, because it may critical applications or processes
    - Again testing in a test lab, and rolling out changes slowly say department by department is key, during off peak or after hours

2.2.3 Turning ON auditing via the NISTWIN2KPRO.inf

- You can adjust the settings further to track certain files changes, or changes in an OU that are important to you or your organization (Souppaya, et all 5-3 – 5-4)
- Use secedit.exe to enable system wide auditing for all required servers (Souppaya, et all 5-1 – 5-3)

2.2.4 Removing unneeded Windows servers from startup

- Extra windows services slow down boot times, and can cause clutter in the event logs
    - If you take care you can disable unnecessary services to reclaim system resources
- Black Viper runs a web site, and has a section dedicated to this topic.
    - For safety purposes his information may be better suited for workstations then servers.
    - http://www.blackviper.com/WIN2K/win2kservice411.htm
    - All services he recommends disabling are well documented
- Another resource is from NIST guidelines for disabling services. The chart below outlines services NIST feels could be disabled (Souppaya, et all 8-18)

Service	Description
DHCP Client	Contacts a DHCP server to obtain a DHCP lease for network connection configuration. Disable this if network connections are statically configured.
Distributed Link Tracking Client	Provides configured notifications of NTFS networked file activity within a Windows 2000 domain. Disable this service if running a stand-alone machine.
Messenger	Sends alerts of various events to the console; useful within a Windows 2000 domain.
Remote Registry Service	Allows remote manipulation of Windows 2000 Professional registry. Disable this unless determined to be absolutely necessary.
RunAs Service	Enables programs to execute under a specified alias—for example, an Administrator can log on to a system as an unprivileged user as recommended and can execute administrative programs using the RunAs service. NIST recommends the use of this service.
Server Service	The SA should disable this service unless the Windows 2000 Professional workstation must share files. It is present if the File and Printer Sharing for Microsoft Network service is installed.

Alerter	Can send a network popup message and/or run a program when one of the Performance Monitor counters exceeds a preset threshold. Disable if you do not require this functionality.
Fax Service	Allows faxes to be sent and received; disable if not necessary.
Indexing Service	Indexes the entire all files on the system for rapid searching. Disable if you do not want this functionality.
Infrared Monitor	Enables infrared ports to function. Disable if infrared capability is not desired.
Logical Disk Manager Administrative Service	Service is started only when a disk is configured or partitioned. It is used to provide Administrative functions for Logical Disk Manager. Required to use the Disk Management user interface.
Net Logon	Used in Domain Member configurations. Do not disable if in a Domain.
Netmeeting Remote Desktop Sharing	Allows authorized remote users to connect to your desktop. Disable if this functionality is not required.
Performance Logs and Alerts	Used to configure Performance Logs and Alerts; also used to collect log and alert information. Disable if Performance Logging is not desired.
Remote Access Auto Connection Manager	Starts when no network connection is available and offers to dial up to connect when an application attempts to access the internet. Disable if this functionality is not required.
Remote Procedure Call (RPC) Locater	Provides name services for RPC clients. Disable if no third-party programs require this functionality.
Smart Card	Manages and controls access to smart cards. Disable if smart cards are not used in your system.
Smart Card Helper	Provides support for non-plug and play smart card readers. Disable if no non-plug and play readers will be installed on the system.
Uninterruptible Power Supply (UPS)	Manages serial communications with a UPS. Disable if not required.
Windows Management Instrumentation (WMI)	Provides system management information used by internal and external partners. Disabling this service will prevent management information applications from running.
WMI Driver Extensions	Tracks drivers that have WMI information to publish. Disable if WMI is disabled.
Windows Time	Used to access Network Time Protocol services. Disable if you do not require an external time source.
Utility Manager	Used to provide rapid access to accessibility tools: Magnifier, Narrator, and On-Screen Keyboard. Disable if rapid access to these tools is not required.

2.2.4 Physical security

- Enable BIOS password on system startup in cases user gains physical access, if system has chassis alarm use that as well
  - A Hacker may try to clear the CMOS to by pass BIOS password

- Consider using token Cards for 2 Factor authentication on for all Domain administrators

- Install security cameras, and card reader in and around data center if not already in place

2.2.5 Account and System security

- Rename administrator account to something that sounds like a regular user name (Labmice,2)

- NTFS is a must for all servers, and desktops with EFS on with 128 bit 3DES encryption (Cole, Et. All, 1197)
  - Use the Hi Encryption pack from Microsoft to allow this feature
  - http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp

- Clear the page files at shutdown of the PC
  - Edit the Registry key below AFTER making a backup
  - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management and changing the data value of the ClearPageFileAtShutdown value to 1 (Labmice,8)

- Disable auto run so malicious user cannot use CD's labeled Mp3 , game etc.. and fool users into loaded malicious software
  - Backup registry and edit following value
  - **HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services Cdrom** subkey and set the **AutoRun** value to 0

2.3 Summary of "Secured Environment "

Assuming that all the servers are patched to the latest level, and appropriate hot fixes are installed we have a relatively secure system.

- We saw that using the templates supplied freely by NIST was an amazing time saver
- They was no need to worry about the effectiveness of templates
    - It was hardened for Government organizations like the DOD and the NSA
- A fresh Windows 2000 server would need an amazing amount of patches, hot fixes, policies etc. before it should even connect to the domain.
- Realized there are many resource to user when hardening the environment
    - NIST, Microsoft, Google, and other individual web sites
    - The Default installation of Window 2000 is not secure by nature
    - Furthermore auditing of required logs, has to be manually initiated or pushed via GPO

3. PATCH AND EXPLOIT MANAGEMENT

3.1 Be proactive and stop the exploits before they hit!

Let the information come to you! This section will relatively short, but nevertheless important. New exploits, viruses, vulnerabilities and hot fixes are available on a daily basis. Obviously on one really has the time to monitor web sites for vulnerabilities that affect their environments. Therefore the best course of action is to be proactive and subscribe to well know organizations, and trusted sources for the latest exploits (Cole, 1288-9) If you have custom or specialized applications for your company, you may want to subscribe to that as well.

If your organization stays on tops of patching servers, applications, routers, and well know exploits they should not affect your company. It is when you expect your network to patch, and heal it self is when the trouble starts. Neglecting to apply patches, and react fast enough to exploits can be a devastating. Emails would stop, people would head home, thousands even millions could be lost. Do you really want your whole network down when patches were released a week ago my Microsoft? I think not, and the same would go for your users. Furthermore many applications may have built in mechanisms for updates via the Internet. Keep a list of these applications so that other engineeres have a clue what to expect on unque computers.

Name	URL	Specialty
Bugtraq mailing list	http://www.ntbugtraq.com	Mailing list of bugs and exploits
Symantec	http://nct.symantecstore.com/virusalert/	Notification of Dangerous viruses
Microsoft	http://register.microsoft.com/subscription/subscribeme.asp?id=166	Security alerts for Microsoft applications
Neohapsis	http://www.neohapsis.org	Well respected Chicago security firm
KB ALertz	http://www.kbalertz.com/	Notifies you of new Microsoft KB articles
Network World	http://www.nwwsubscribe.com/Default.aspx?keycode=foc54	Network World – Multiple subscriptions
CERT	http://www.cert.org	Carnegie Mellon security reporting cente
NIST	http://www.nist.gov	Government agency in charge of securit standards for DOD, and NSA

3.2 Reacting to Vulnerabilities

Once vulnerabilities are found testing must take place immediately in a test lab environment. If no serious issues arise it should be rolled out to production n for machines that are most affected. If you skeptical about that patch apply it to less critical system and department first before testing with the Payroll department.

3.3 Patch Management

The best "free" patch management solution is a combination of SUS, Microsoft Base. Security Analyzer (MBSA), and paying close attention to late breaking hot fixes. When you combine all three ways to avoid exploits, you will have a network that hums while others die.

3.3.1 SUS

When the SUS services are configured properly, an admin has a console to manage the updates pushed to your clients. Using an Intranet site an admin will choose the exact patches he or she wishes to download for use in the network. He or she can then schedule the updates to install at any time, and slowly slip down the data to intended clients via GPO (Microsoft, 1-3). It makes effective use on LAN bandwidth, Chain installations, and detect requires patches to get system at desired level without manual intervention.

In effect it can replace HFNETchk, QCHAIN, and complicated scripting.

3.3.2 Microsoft Base Security Analyzer (MBSA)

MBSA is an improvement to HFNETCHK, and a much easier to use GUI with report making capabilities. The tool can scan any given PC or an IP range for vulnerabilities, improper or dangerous settings that exists on the system. MBSA can find issues such a blank password on an administrator account, or hot fixes that may be required.

3.3.3 Email alerts for hot fixes

As a last resort any hot fix or patch that slips thru the Microsoft applications will arrive via email. It is then up to the admin to determine the scope of the exploit to determine if patch must be run manually on all affected servers, and desktops. You may want the subscription email to page your phone, so their no way you can miss an important patch.

3.4 Syslog server and Network monitoring

The Microsoft Event, Security, and application log record important event about the servers they resides on. The event long is typically the best spot to look for, when trouble shooting errors. The event ID's you see, combined with a site known as Eventid.net, will help a user solve many obscure problems. Unfortunately Microsoft has no built in way pooling the entire set event ID's of multiple servers into one "syslog server: for further analysis. This is can be a problem for an administrator that is trying to maintain 100% reliability of his or her servers

Therefore we use an article written by Rainer Gerhards on http://sysadminnews.com/sysadminnews-32-20040105CentrallyMonitoringWindowsNT2000XP2003.html

3.4.1 Syslog Basics

Hardware one can build a reliable syslog server.
Windows does not have the built in capability for centralized system event og auditing. The tools are were used below to build a syslog environment :

- EventReporter - data collector
- WinSyslog - storage engine and alert notification
- MoniLog - console and reporting tool

3.4.2 Event Report

Event Report is used to query the days from different servers. This application has to be installed on each server who information eventually ends up in the syslog server. Aftter the information is queried about every 30 seconds it is transferred to a storage engine, in this case WinSysLog.

3.4.3 Win Sys Log

This utility can detect configured rules, changes in environment to email or phones. It has the ability to filter certain event Id's, and escalate message to administrator if need by.

Can also be used to analyze WAN links over the VPN etc.

3.4.1 Analyzing the Events

For reporting purposes and application know as MoniLog running to provide daily reports. It takes gathered from Win Sys log into smaller sections for reporting purposes. .

3.4.2 SysLog Conclusion

Especially with low man power a tool like this is required to ensure no one server cries for help are missed. When a good monitoring service is setup an administrator can rest assured the he or she is aware of very single minute event log error on all servers. Again the tool used are mentioned below

The following tools were used to build the monitoring system:

- EventReporter - data collector
- WinSyslog - storage engine and alert notification
- MoniLog - console and reporting tool

5. CONCLUSION

5.1 Closing thoughts

Multiple views of security are essential for an admin to have. You should be able to look at your network the way hacker would, understand his or her mindset, look into the latest tools available to them. After which see if your network is vulnerable to such tools, and harden the environment so it is immune to such scans. Window 2000 has many areas that be hardened ranging from the operating system, Active Directory, and group policy. It is important to say abreast of new findings in all areas of Windows 2000 to keep the network healthy

6. WORKS CITED

Cole, Fossen, Northcutt, Pomeranz. "SANS Security Essentials with CISSP CBK" USA: April 2003

Gerhards, Rainer. "Centrally Monitoring Windows NT/2000/XP/2003". January 2004 URL: http://sysadminnews.com/sysadminnews-32-20040105CentrallyMonitoringWindowsNT2000XP2003.html

Labmice editors. "Windows 2000 Security Checklist" Dec 2003 URL: http://labmice.techtarget.com/articles/securingwin2000.htm

Microsoft. "Software Update Services Overview White Paper" January 19, 2004 URL: http://www.microsoft.com/windowsserversystem/sus/suscomponents.mspx

Souppaya, Harris, McLarnon, Selimis. "Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System: Recommendations of the National Institute of Standards and Technology. Special Publication 800-43. 11-19-2002. URL: http://csrc.nist.gov/itsec/NIST_Win2KPro.zip

Last Updated: July 27th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event