Global Information Assurance Certification Paper

Locking Down Your Windows NT Server
Angelo Giambra
Version 1.2f
GSEC
Angelo_001
1/8/02

Introduction:

When Windows NT was first released, it was touted as a highly secure system. Hackers were not as predominant as today and UNIX systems were still their prime target. Since then, a lot has changed. Internet Explorer has become a key component in Windows NT. Most users in large organizations can access the Internet directly from their desk. Because of its popularity, Windows NT has become one of the primary targets of Internet hackers.

Microsoft's recent announcement of a two-phased initiative dubbed the Strategic Technology Protection Program (STPP) is evidence of this. The first phase of this program promises to provide short-term fixes to security problems. During the second phase, called Stay Secure, Microsoft will perform a rewrite of its key software in an effort to make it more secure and resilient.

A rewrite of key software is a major undertaking and, until Microsoft completes this phase, it is important that system administrators make every effort to secure NT systems the old fashioned way. This document will explain some of the key elements in locking down an NT system.

The NTFS File System:

Unless one specifically chooses to install the NTFS file system, there is no file security whatsoever. Anyone with a system password is free to access, even delete, critical files. The first, most important step in locking down your system is to implement the strong file and directory security afforded by the NTFS File System. NTFS can be installed during the initial install of Windows NT, or the existing FAT file system can be converted to NTFS using the following command at the DOS command prompt:

Convert <Drive>: /FS:NTFS

Substitute the drive letter you are converting. During the next reboot of your system, Windows will automatically convert your FAT file system to NTFS. When security is a concern, always install the NTFS file system. Installing NTFS is not enough, however, to fully protect your system.

The Security Configuration Manager:

Beginning with Service Pack 4, Microsoft has provided a utility that greatly simplifies the process of setting system security, the Microsoft Security Configuration Manager. You can download MSCM at:
http://www.microsoft.com/ntserver/nts/downloads/recommended/scm/default.asp

MSCM, while easy to use, has many features and options. It is not the intent of this paper to instruct you in its use. An excellent white paper explaining MSCM and how to use it to configure system security can be found at:

http://www.microsoft.com/NTServer/techresources/security/securconfig.asp

Note that you must have Service Pack 4 or later installed to use MSCM. Once installed, MSCM uses template files (called INF files) to automatically configure security settings for several security configuration areas. MSCM will allow you to configure account policies, local policies, event log settings, restricted groups, system services, the registry and certain file system settings.

The installation includes several INF files that are pre-configured. These files define four levels of security, basic, compatible, secure and high secure. Different INF files exist for the various flavors of Windows NT (PDC, Member Server and Workstation).

Configuration File	Security Level	Platform
Basicwk.inf	Default	NT4 Wksta
Basicsv.inf	Default	NT4 Server
Basicdc.inf	Default	NT4 DC
Compws4.inf	Compatible	NT4 Wksta\Server
Compdc4.inf	Compatible	NT4 DC
Securws4.inf	Secure	NT4 Wksta\Server
Securdc4.inf	Secure	NT4 DC
Hisecws4.inf	High Security	NT4 Wksta\Server
Hisecdc4.inf	High Security	NT4 DC

Using MSCM, you can analyze and configure your system security settings. This is done by loading one of the template files and choosing either the Analyze or Configure functions. Analyze will compare settings in the template with the settings on your system and display the differences. You can then choose the Configure option, which will apply the settings in the INF file to your system.

An improvement over the default security settings, the compatible configuration errs on the side of applications when making a tradeoff between functionality and security. A better choice is the secure configuration, which errs on the side of security when making a tradeoff between functionality and security. The use of the high secure INF files is not recommended since most existing application will not function adequately.

Of course, you should never apply the INF files directly to a production system. Create a test environment that duplicates your production environment. Apply the INF settings to your test system and thoroughly test all applications to ensure that you have not lost functionality.

If the pre-configured INF files do not meet your specific needs, you may also configure your own INF files using MSCM. The tool uses a GUI which displays significant file and directory settings and allows you to modify them as needed. Modification are stored in the INF file and applied when you choose the Configure option.

Since MSCM cannot add registry keys, there are still some manual changes to the registry which are necessary to fully lock down your system. The most important modifications are listed below.

Registry Modifications:

The Guide to Securing Microsoft Windows Networks, published by the National Security Agency, makes the following recommendations for registry settings:

Note: Use Regedt32.exe to make the following modifications to the registry. Not all of the keys listed will exist; you will have to add them.

Enforce the strongest level of authentication. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\LMCompatibilityLevel=5.

Disable the CDROM autorun feature. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Cdrom\Autorun=0.

Prevent users from gaining access to base objects through DLLs. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\AdditionalBaseNamedObjectsProtectionMode=1.

Restrict remote registry access. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg\Restrict GuestAcess=1.

Allow only Administrators to schedule tasks. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\Submit Control=0.

Allow only Adminstrators to add print drivers. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers\AddPrintDrivers=1.

Disable auto-generation of 8.3 file names. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3Name Creation=1. **Warning: Setting this registry value may break 16-bit applications or other applications requiring the use of 8.3 name. Test this thoroughly.**

Disable automatic logon of Administrator. Modify HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon\AutoAdminLogon=0.

Protect kernel object attributes. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=1.

If you are not using Netware, remove the Netware DLL authentication. Modify HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\Notification Packages. Remove the FPNWCLNT entry from this key. Do not delete the key or remove any other entries you may find.

Remove OS2 and Posix subsystems by deleting all keys which refer to them. Delete the following keys.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session manager\Environment\Os2LibPath.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session manager\Subsystems\Optional.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session manager\Subsystems\OS2.

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session manager\Subsystems\POSIX.

Folder and File Permissions:

Certain folder permissions must be manually set. Also, several files related to OS/2 and POSIX must be removed.

LDER OR FILE	**r Groups**	**ommended Permissions**
stemRoot%\Profiles	inistrators	Control
	ATOR OWNER	Control
	TEM	Control
	enticated Users	l,Execute,Create Folders
stemRoot%\Profiles\Administrator	inistrators	Control
	TEM	Control
stemRoot%\Profiles\All Users	inistrators	Control
	enticated Users	l, Execute
	TEM	Control
stemRoot%\Profiles\Default User	inistrators	Control
	enticated Users	l, Execute
	TEM	Control

Remove the following files from %SystemRoot%\system32:

Os2.exe
Os2ss.exe
Os2srv.exe
Psxss.exe
Psxdll.dll
Posix.exe

Remove the following folder from %SystemRoot%\system32:

Os2

NT Service Packs and hotfixes:

The final step in locking down your system is to apply the latest service pack and hotfixes to your system. As of this writing, the latest service pack available for Windows NT is Service Pack 6a. Use the high-encryption version, available at http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/128bitX86/default.asp

Once this is applied, you should obtain and install the latest hotfixes. The Post-Windows NT 4 Service Pack 6a Security Rollup Package (SRP) is the best method for accomplishing this. Previous hotfixes had to be installed individually, requiring a reboot after each install. The Security Rollup Package includes all these hotfixes in one, simple to install package. You can obtain the SRP from at http://www.microsoft.com/ntserver/nts/downloads/critical/q299444/default.asp

IIS Server:

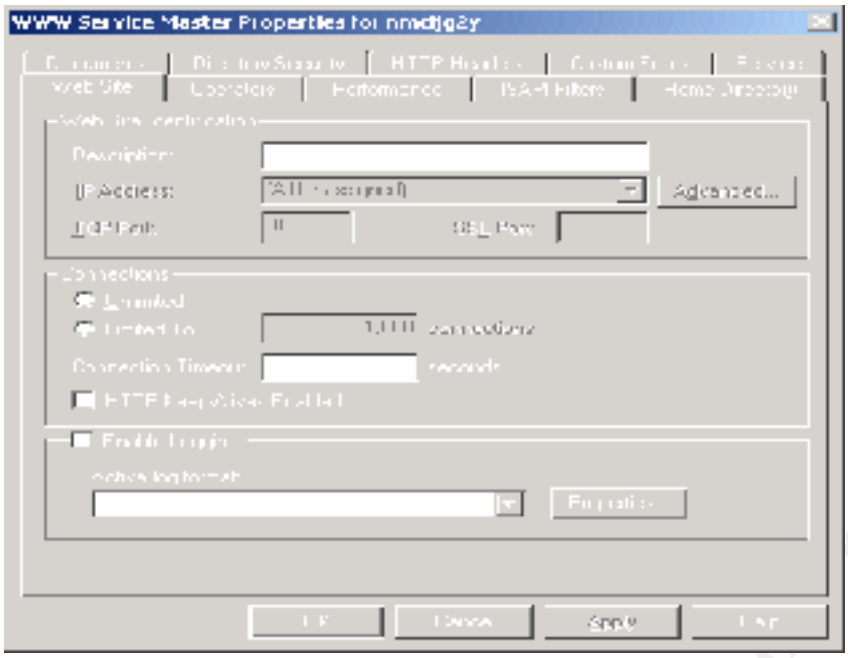
If you have installed the IIS server component of Windows NT, there are additional tasks which must be performed.

Install the latest IIS hotfixes. If you applied the SRP, these are included. Otherwise, you can obtain them at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp?productid=16&servicepackid=0&submit1=go

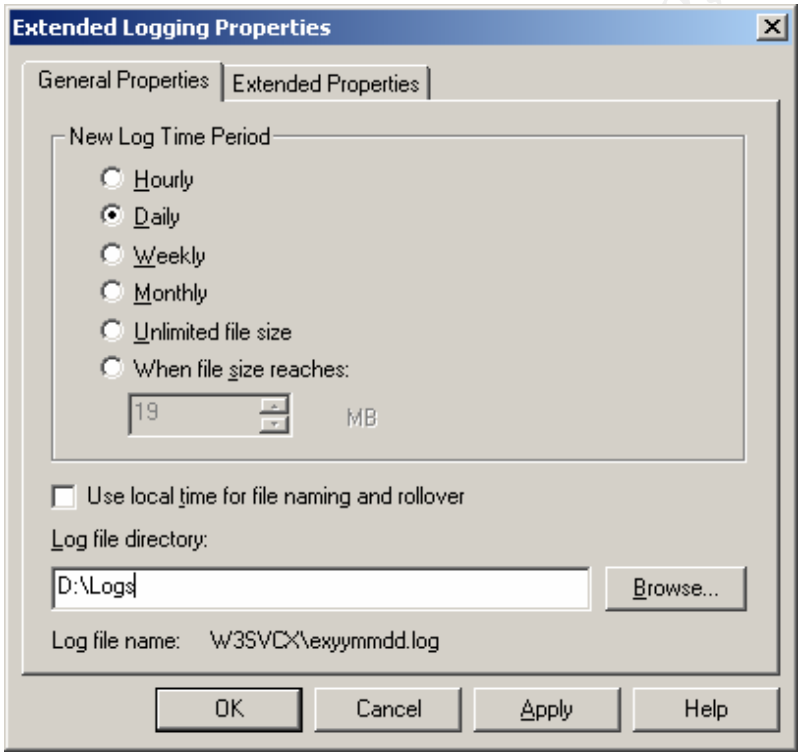
Move the Winnt\System32\LogFiles to a different location. Be sure to stop the World Wide Web Service before moving the directory.

Delete all directories containing samples, such as inetpub\iissamples.

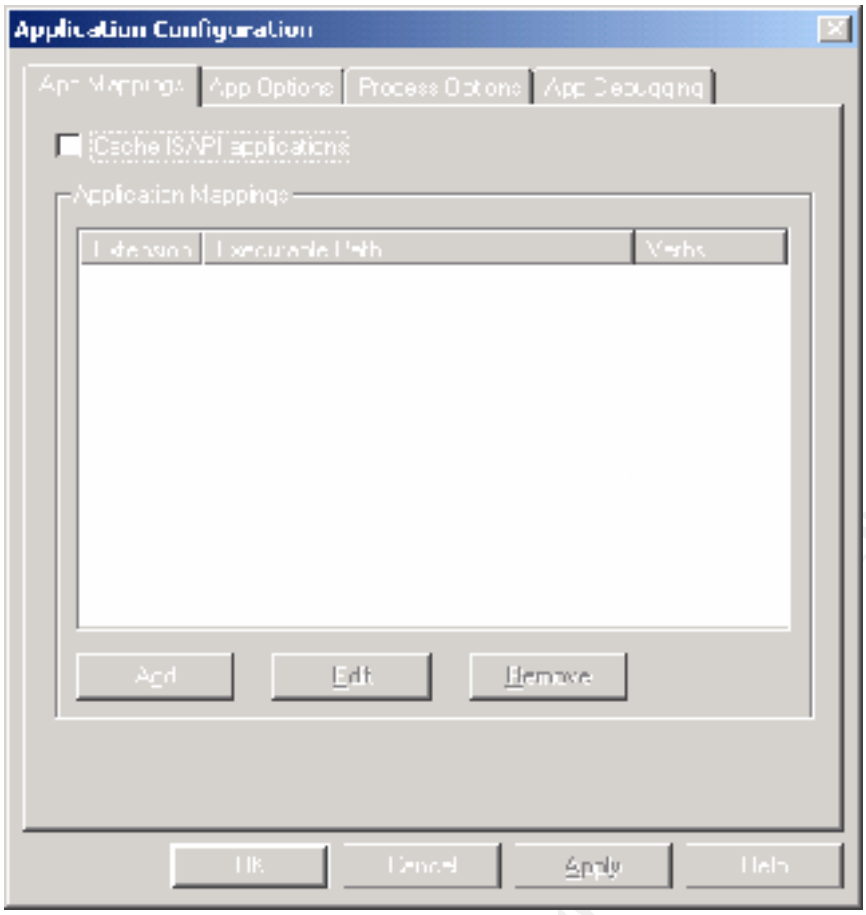
Using the Internet Services Manager, highlight the server name and choose **Properties**. Click on the **EDIT** button, then the **Web Site** tab.



Ensure **Enable Logging** is checked. In the **Active Log Format** window, select the **W3C Extended Log File Format** option from the pull-down menu, then click the **Properties** button.



In the **log file directory** window, key in the location of the log file directory. Click **OK**. Next, select the **Home Directory** tab and click the **Configuration** button.



Under **App Mappings**, highlight the .htr, .idc, and .printer extensions and click the **Remove** button.

These steps will close the most obvious Internet vulnerabilities.

Conclusion:

Several techniques for locking down Windows NT have been outlined in this document. To summarize, locking down NT involves the following steps.

- Install the NTFS file system
- Use the Security Configuration Manager to apply the appropriate INF file
- Use Regedt32 to manually configure important registry keys
- Apply the latest service pack
- Apply the latest security hotfixes
- If running IIS server, lock down known vulnerabilities

If these steps are adhered to, you can be assured that your system will be resistant to hacker attempts to compromise it. While there is never any guarantee that a system will be hacker proof, locking down NT and constant vigilance are your best protection.

References:

"Microsoft Promises to Stay Secure", Windows & Net Magazine. January, 2002
URL: http://www.winntmag.com/Articles/Index.cfm?ArticleID=23201 (December 20, 2001).

Microsoft Corporation, "Security Configuration Editor". 1998
URL: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/readme.txt (December 20, 2001).

Bartok, Paul F., "Guide To Securing Microsoft Windows NT Networks". September 18,2001
URL: http://nsa1.www.conxion.com/winnt/guides/wnt-1.pdf (December 30, 2001)

Mahmud, Luqman, "Procedures For Hardening Microsoft Windows NT Workstation".
URL: http://www.users.fast.net/~lmahmud/index4.html (January 5, 2002)

Proctor, Paul, "Hardening Windows NT Against Attack". January, 1999
URL: http://secinf.net/info/nt/hard/hard.html (January 5, 2002)

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
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