Global Information Assurance Certification Paper

Securing Windows 2000 Server

Cory Bys
MCSE, MCP+I, CCSE, CCSA, TCP, CNST

May 20, 2001
Version 1.2d

Introduction

This document intends to outline the steps required to harden a default Windows 2000 Server installation. While additional measures can be taken to further secure the installation, implementation of the following will sufficiently protect your system from all currently known attacks – at least all of those known by ISS's Internet Scanner.

Please note that you may need to modify this procedure for your specific needs. This process has always worked for my installations but may render your server inoperable. Think before you click.

Installation

First and foremost is use the NTFS file system - especially for the boot partition. Yes, it is possible to secure a FAT partition from a remote users perspective, but the use of FAT increases risk considerably.

Another issue that needs to be corrected during installation is the default directory. Do not install system files in the \WINNT directory. Rename the directory anything else you like -- \REDHAT and \MITNICK are two popular examples. I'll refer to the system directory as \SIOUXSIE for the remainder of this paper. This step will prevent attacks hard coded to refer to files in the \WINNT directory.

NTFS Permissions

After the installation has completed you will need to correct the NTFS permissions. The primary goal is to get rid of all occurrences of "EVERYONE". Try the following, in your test environment first of course:

- Reset permissions at the logical drive level for all of your drives as shown below. Apply the settings to all child objects and enable propagation of inheritable permissions.

Administrators	Full Control
Authenticated Users	Modify
	Read and Execute
	List Folder Contents
	Read
	Write
CREATOR OWNER	Full Control

SYSTEM Full Control

- After this has been done remove all permissions for Authenticated Users from \SIOUXSIE (the system directory) and its child objects.

- Allow Authenticated Users Modify, Read and Execute, List Folder Contents, Read and Write to the following directories and all of their child objects:
  \Documents and Settings
  \SIOUXSIE\Installer (Note: It's hidden…)
  \SIOUXSIE\System32\Spool
  \SIOUXSIE\System32\Config
  \SIOUXSIE\Repair

- Allow Authenticated Users Read and Execute, List Folder Contents and Read to \SIOUXSIE\System32\Spool\Drivers. This is an important step as it prevents users from uploading trojaned drivers that would be distributed to other users.

- Set the appropriate permissions on your user directories.

Share Permissions

We have already locked down the file system, but you should still check your share permissions if applicable. It is a little extra work, but I never turn down the opportunity to add a layer of security to my servers.

Services

Now is a good time to disable any unnecessary services. These are the ones I typically do not require to be running on a server:

DHCP Client
Fax Service
Internet Connection Sharing
Intersite Messaging
Remote Registry Service
RunAs Service
Simple TCP/IP Services
Telnet
Terminal Services
Utility Manager

If your server is destined to be an intrusion detection box it would be wise to disable services like Computer Browser and Server as well.

Protocols

Unbind protocols like IPX and NetBIOS from interfaces where they are not required. They love to broadcast, and broadcasts are evil.

User Accounts

Next we will secure the local user accounts.

- Disable the Guest account and give it a very strong password.

- Disable the TsInternetUser account and give it a very strong password. Create the account if it does not exist. Do not delete the account even if it is not being used, since when you later upgrade the OS the account will be created if it does not exist.

I am assuming you already created a very strong password for the Administrator account during the installation.

Registry

Now we will need to fire up REGEDT32 and add or edit the following values. Most of them are intended to defend against Denial of Service attacks, while the others help prevent such things as the enumeration of accounts by unauthenticated users.

Under HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services add or modify the following values:

Key: Tcpip\Parameters
Value: SynAttackProtect
Value Type: REG_DWORD
Parameter: 2

Key: Tcpip\Parameters
Value: TcpMaxHalfOpen
Value Type: REG_DWORD
Parameter: 100

Key: Tcpip\Parameters
Value: TcpMaxHalfOpenRetried
Value Type: REG_DWORD
Parameter: 80

Key: Tcpip\Parameters
Value: EnablePMTUDiscovery
Value Type: REG_DWORD
Parameter: 0

Key: Tcpip\Parameters
Value: EnableDeadGWDetect

Value Type: REG_DWORD
Parameter: 0

Key: Tcpip\Parameters
Value: KeepAliveTime
Value Type: REG_DWORD
Parameter: 300000

Key: Tcpip\Parameters
Value: EnableICMPRedirect
Value Type: REG_DWORD
Parameter: 0

Key: Tcpip\Parameters\Interfaces\
Value: PerformRouterDiscovery
Value Type: REG_DWORD
Parameter: 0

Key: Netbt\Parameters
Value: NoNameReleaseOnDemand
Value Type: REG_DWORD
Parameter: 1

Under HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Control add or modify the following value:

Key: Lsa
Value: RestrictAnonymous
Value Type: REG_DWORD
Parameter: 1

You may have noticed that I failed to have you fix the known flaws in the registry key permissions. Since we disabled the Remote Registry Service earlier it is not really necessary to do so.

If you're like me and wear suspenders and a belt (even when wearing coveralls), another neat trick is changing the file association for the .REG extension to something like NOTEPAD.EXE. This will prevent malicious web sites from adding registry keys without your knowledge. But since we're talking about servers here, the only site you are likely to visit from the console is a trusted one like http://windowsupdate.microsoft.com -- so I guess we don't really need to worry about that issue…

Console

Enable a screen saver, password protect it, and set it for some short interval like 5 minutes. This will protect you in the rare occurrence in which you forget to lock the computer before walking away from it.

Auditing

Next we will enable Auditing. This may be configured at the domain level, so you may not need to configure this for every server. I typically configure the Auditing settings as shown:

Audit Account Logon Events	Success and Failure
Audit Account Management	Success and Failure
Audit Directory Access	No Auditing
Audit Logon Events	Success and Failure
Audit Object Access	Success
Audit Policy Change	Success and Failure
Audit Privilege Use	Success and Failure
Audit Process Tracking	No Auditing
Audit System Events	Success and Failure

Now we need to change the log settings so they have the potential to serve some purpose. Keeping the settings at their defaults may cause the server to crash when a log gets full. Increase the maximum size of the Application, Security and System logs to at least 10,048 KB each. Configure them to overwrite events as needed.

Security Policy

The local security policy is configured rather well in a default installation, but I usually change the following settings:

Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign server communication (when possible)	Enabled
Shut down system immediately if unable to log security audits	Enabled

Telnet

Now we have to worry about telnet to Windows boxes. Create a group named “TelnetClients”. Leave it empty if you are not using the service. If you are using the service, add your users to this group.

Trojans

This step is most helpful on workstations, but you will learn to like it on your servers as well.

Many, if not most of the trojans currently circulating take advantage of the Windows feature of hiding the extensions of known file types. This is what makes the executable script CLICKONME.BMP.VBS appear to be the bitmap file CLICKONME.BMP. This behavior makes it simple to trick people into executing files they believe are benign.

To fix the problem navigate to My Computer – Tools – Folder Options – View. Deselect "Hide file extensions for known file types". While you are here, you might want to deselect "Hide protected operating system files" as well. Being able to see the protected OS files doesn't benefit security much, but it will assist you in future troubleshooting.

If you have no need for Visual Basic or other scripts on your server, you can protect yourself further by preventing the scripts from executing by default. Simply change the file associations for some or all of the following file extensions to NOTEPAD.EXE:

.JS
.JSE
.VBE
.VBS
.WSF

Service Packs

You know the drill. New vulnerabilities are found in computing products every day. Keep an eye out for applicable Service Packs and Hotfixes and apply them as soon as possible.

Other Measures

There are a few other steps you can take to lock down a Windows 2000 Server, like implementing TCP/IP Filters and IPSec filtering. In practice though these features are difficult to maintain so I typically use them sparingly. Try filtering on your routers instead.

Conclusion

This procedure outlines the steps required to secure a default Windows 2000 Server installation. After applying these modifications to your servers you will be free to resume your game of Half-Life – at least until the release of the next CERT advisory.

References

"BackOrifice2K.Trojan", Symantec Corporation, http://www.symantec.com/avcenter/venc/data/back.orifice.2000.trojan.html

Cox, Philip, “Hardening Windows 2000”, http://www.sys-exp.com/tutors/HardenW2K101.pdf

“Creating a Local Group Can Restrict Other Users from Gaining Access to a Windows 2000-Based Computer Through Telnet”, Microsoft Corporation, http://support.microsoft.com/support/kb/articles/Q250/9/08.ASP?LN=EN-US&SD=gn&FR=0&qry=create%20telnetclients&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=WIN2000

Dodds, Tom and Kerby, Warren and Howard, Michael, “Data Security and Data Availability for End Systems”, http://www.microsoft.com/technet/security/datavail.asp

Dodds, Tom and Pfeil, Kenneth, “Security Considerations for End Systems”, http://www.microsoft.com/TechNet/security/sconsid.asp

“Locking Down an NT Server”, http://www.iis-resources.com/Build_Docs/lockdown.html

“NetBIOS Vulnerability May Cause Duplicate Name on the Network Conflicts”, Microsoft Corporation, http://support.microsoft.com/support/kb/articles/Q269/2/39.ASP?LN=EN-US&SD=gn&FR=0&qry=nonamereleaseondemand&rnk=1&src=DHCS_MSPSS_gn_SRCH&SPR=WIN2000

Pfeil, Kenneth, “Data Security and Data Availability in the Administrative Authority”, http://www.microsoft.com/technet/security/datasec.asp

Robichaux, Paul, “Robichaux on Security – December 1999”, http://www.microsoft.com/technet/security/ro1299.asp

“Securing Windows 2000 Network Resources”, Microsoft Corporation, http://www.microsoft.com/technet/win2000/netres.asp#d