Hardening Windows 2000 Server

Warning: This document is still a work in progress. Although to the best of my knowledge it is factually accurate and complete, the depth is variable. It is intended to be a step-by-step hardening guide for administrators with only basic technical skills. Right now about 2/3 of the document is at that level, and the remaining third leaves exercises to the reader.

This is a basic step-by-step hardening instruction intended for creating a stand-alone (i.e. not part of a domain) Windows 2000 Server bastion host. In other words an application server that will run only one or a small number of applications for a very specific purpose.

The basic methodology used in this paper is to install a basic Windows 2000 Server image with only the required components installed, install the application and then doing the hardening. I have tried to do it the other way, which is to install the application on an already hardened image, and have had nothing but grief with most applications.

This is an iterative process, which is slightly different for each application. A good understanding of the installed application will greatly aid this process.

What do I need?

You should ensure you have the following before you start:
- a copy of Windows 2000 Server. Not Windows 2000 Desktop or Windows 2000 Professional. Although these instruction will work with either of these, a few modifications will be required.
- All the required Windows Service Packs. Check the application documentation. Not all applications will run with the highest Service Pack available. Grab the highest Service Pack the application will support.
- The Application CD and license.
- Any application Service Packs, patches, or hotfixes.

I would like to give credit right up front. This document borrows heavily from Phil Cox's Hardening Windows 2000 (http://www.systemexperts.com/). I don't agree with everything he says, and I have added a bunch of my own ideas, but the man does good work, and without him this document wouldn't exist.

Tools Required

Three tools are required. The two primary tools required are built into Windows 2000 Server; the Windows Services Tool, and the Windows Event Viewer. The third tool is a port scanner or vulnerability scanner.

Services Tool

The Services tool is used to view which service are running on a server, and is used to enable or disable services. It is accessed through the following menus:

Start -> Programs -> Administrative Tools -> Services

Event Viewer

The Event Viewer is used to view system and startup and some operational events created by applications. This is where errors will show up if applications have dependencies or other problems as a result of the hardening. The Event Viewer is accessible through the following menus:

Start -> Programs -> Administrative Tools -> Event Viewer

Port or Vulnerability Scanner

The other required tool is some sort of port scanner or VA tool. This will be used to validate the external view of the server once the hardening is completed. I usually use nmapwin (http://sourceforge.net/projects/nmapwin) because it is easy to use, and best of all it is free. But any commercial port scanner or vulnerability scanner capable of doing TCP and UDP scans is fine.

Local Security Settings
The Local Security Settings Tool is used to configure individual security settings for the server.

Start -> Programs -> Administrative Tools -> Local Security Settings

Step 1:Install the image

Install the Windows 2000 image. Minimize the components installed.

Step 2: Install Service Packs

Install all O/S Service Packs required or permitted by the application. For example if the application works on Service Pack 2 or higher install the highest service pack available.

Step 3: Record Existing Services

Essential tool: Services Tool Start -> Programs -> Administrative Tools -> Services

Step 4: Install the Application

Be sure to install any application service packs, patches, or hotfixes.

Step 5: Determine which services are new

Step 6: Determine Dependencies for New Services

Step 7: Remove Services

Essential tool: Event Viewer Start -> Programs -> Administrative Tools -> Event Viewer
Iterative process. Do 10-15 at once and reboot.
If you are unsure about a service. Set it to manual and see if anything starts it

Check the application and system logs after every reboot.
In my experience, it is possible to remove a couple of these services, but in most cases this is the minimum set of services required:

- DNS Client
- EventLog
- Logical Disk Manager
- Network Connections Manager
- Plug & Play
- Protected Storage
- Remote Procedure Call
- Remote Registry Service
- RunAs service
- Security Accounts Manager

If unsure about a service…set it to manual and do a reboot, and start up the application. If it is required it will have started up.

Step 8: Modify Security Policies

Using the Local Security Settings Tool (Start -> Programs -> Administrative Tools -> Local Security Settings) set the following security policies. The headings describe the menu each set of settings can be found under. This is a bit of a crap shoot, but I find these settings will usually work. Documentation for some of these settings is fairly scarce, but if you are unsure search Microsoft's support site for more info.

This section does not touch on all the security settings, just a minimum set. It is assumed that the others will remain as set.

Account Policies

Password Policies

Enforce Password History Enabled: 5
Maximum Password Age Enabled : 45
Minimum Password Age Enabled: 2
Passwords Must Meet Complexity Requirements: Enabled
Store Password Using Reversible Encryption: Disabled

Account Lockout Policies

Account Lockout Threshold: Enabled: 5
Account Lockout Duration: Enabled: 15
Reset Account Lockout Counter After: 30 minutes

Local Policies

Audit Policy

Audit Account Logon Events: Enabled
Audit Account Management: Enabled
Audit Logon Events: Enabled
Audit Policy Change: Enabled
Audit System Events: Enabled

User Rights Assignment

Act as Part of the Operating System: Administrator
Access This Computer From the Network: Administrator
Back Up Files and Directories: Administrator
Change the System Time: Administrator
Create a Token Object: Administrator
Debug Programs: Administrator
Force Shutdown From a Remote System: Administrator
Increase Scheduling Priority
Load and Unload Device Drivers
Log On as a Service
Log On Locally
Manage Auditing and Security Log
Modify Firmware Environment Values
Profile Single Process
Profile System Performance
Replace a Process Level Token
Restore Files and Directories
Shut Down the System
Deny Access to this Computer from the Network
Deny Logon Locally
Take Ownership of Files or Other Objects

Security Options

Additional Restrictions for Anonymous Connections: No access without explicit anonymous permissions
Allow System to Be Shut Down Without Having to Log On: Disabled
Audit Use of Backup and Restore Privilege: Enabled
Clear Virtual Memory Pagefile When System Shuts Down: Enabled
Digitally Sign Client Communication (Always): Enabled (for high security)
Digitally Sign Client Communication (When Possible): Enabled (for medium security)
Digitally Sign Server Communication (Always): Enabled (for high security)
Digitally Sign Server Communication (When Possible): Enabled (for medium security)
Disable CTRL-ALT-DEL Requirement for Logon: Disabled
Do Not Display Last User Name in Logon Screen: Enabled (for multiuser systems)
LAN Manager Authentication Level: Send NTLMv2 responses only/refuse LM & NTLM
Number of Previous Logons to Cache (In Case Domain Controller Is Not Available): 0
Prevent Users From Installing Printer Drivers: Enabled
Recovery Console: Allow Automatic Administrative Logon: Disabled
Rename Administrator Account: (Provide a good name)
Restrict CD-ROM Access to Locally Logged-On User Only: Enabled
Restrict Floppy Access to Locally Logged-On User Only: Enabled
Secure Channel: Digitally Encrypt or Sign Secure Channel Data (Always): Enabled (for high security)
Secure Channel: Digitally Encrypt Secure Channel Data (When Possible): Enabled (for medium-high security)
Secure Channel: Digitally Sign Secure Channel Data (When Possible): Enabled (for medium security)

Secure Channel: Require Strong (Windows 2000 or Later) Session Key: Enabled (for ultra-high security)
Send Unencrypted Password to Connect to Third-Party SMB Servers: Disabled
Shut Down System Immediately If Unable to Log Security Audits: Enabled
Strengthen Default Permissions of Global System Objects (e.g. Symbolic Links): Enabled
Unsigned Driver Installation Behavior: Do not allow
Unsigned Non-Driver Installation Behavior: Do not allow

Audit Log Size

Ensure that there is adequate space in the audit logs for the audits that will be generated. This is especially important if you enabled "Shut Down System Immediately If Unable to Log Security Audits". A good technique is to measure your audit logs for one day and then round that number up to the nearest 100 MB and triple it. This should allow you to log even if the server cannot access the log server for an extended period of time.

The rotation policy will also need to be set. I recommend rotating the logs daily.

Login Message

The value for *Message Text for Users Attempting to Log On* should be changed to something similar to the below (from CERT Advisory CA-1992-19). This one has the advantage of being nice and generic

This system is for the use of authorized users only. Individuals using this computer system with authority, without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Or if you want something less heavyweight I usually use this one. Some people don't like this one because it gives away your company name. In my opinion if the hacker has gotten to this point, they have already done the research to know what company they are hacking. YMMV

Access to this network and the information on it are lawfully available only for approved purposes by employees of <Insert your company name here> and other users authorized by <Your company name>. If you are not an employee of <Your company name> or an authorized user, DO NOT ATTEMPT TO LOG ON. Other than where prohibited by law and subject to legal requirements, <Your company name> reserves the right to review any information in any form on this network at any time.

Step 9: Disable Unused Hardware

On a server the following peripheral ports should not be in, and should be disabled in the BIOS:
- Parallel port
- Serial Port(s)

- USB ports
- Infrared ports

After the operating system is installed, there should be no need to use the floppy or CD. Disable them from the BIOS.:
- Booting from a floppy
- Booting from a CD

Step 10: Password Protect the BIOS

Now that you have made the BIOS changes. It is a good idea to password protect the BIOS so nobody can undo your changes.

Step 11: Screen Saver

Make sure a password-protected screen saver is installed and set to automatically lock the server console, only allowing the currently logged-in user, or a member of the Administrators group to unlock it. It is a good practice to always logout of a server when not using it, but inevitably somebody will walk away and leave it logged in. The screensaver ensures that the console is inaccessible except to valid users when this happens.

I like to configure the screen saver to start automatically after two minutes. Be sure you enable password protection.

Step 12: CD-ROM Autorun

Windows 2000 has a feature that permits a CD to be configured to autorun when it is inserted into the drive. A server should not need this feature, and disabling it prevents malicious code from being introduced by the autorun..

Disable the Autorun feature by editing the following registry key, setting the AutoRun value to 0:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom

if this key does not exist, it will have to be created.

Step 13: Scan the machine

Reboot the machine and then scan it from the same subnet using the port scanner of your choice. This machine should be solidly hardened. If any ports show up that are not essential to the operation of the server they should be investigated and if not needed disabled.

It is always good to understand what a scan of the server looks like when it is hardened. Patching and hotfixes will often disable some of the hardening, and without a baseline and a clear understanding how will you know it changed.

References

Cox, Phil, Hardening Windows 2000**,** Version 1.3, March 14**,** 2002,
http://www.systemexperts.com/

Souppaya, M., Harris, A., McLarnon, M., Selimis, N, System Administration Guidance for Securing Microsoft Windows 2000 Professional System, NIST, Version 2002.01.28, http://www.nist.org/

For information contact cerberus@whitehats.ca or rwanner@pobox.com