Global Information Assurance Certification Paper

Securing Windows GCWN
Practical Assignment v3.1

Securing A Windows 2000 Domain Controller That Is Also The Schema Master

Prepared by Doug Adams
September 2002

Table Of Contents

Introduction

This paper was written to discuss in detail the steps I took to build a secure Windows 2000 Domain Controller that is also the Schema Master, by making use of a security template. [1]The base Schema that ships in Microsoft 2000 contains all the necessary directory definitions used by Windows 2000, and Windows 2000 components. For most organizations, the base Schema is all that will ever be needed. For the purpose of this paper, I will use the scenario of a small Government agency that would like to add and store additional employee information in Active Directory. I will be configuring the server to be able to accept changes to the Schema, while taking the appropriate measures to keep it secure, without impeding the functionality of the system. The Domain Controller will be one of three Domain Controllers on a small network that will also be using Microsoft Exchange 2000 and Norton Antivirus Corporate Edition.

System Information

Server Role

The server is going to be a Windows 2000 server with Active Directory installed. Because this is the first domain controller in an initial domain, it will by default retain all the Flexible Single Master Operation roles, which are Schema Master, Domain Naming Master, PDC Emulator, Relative ID Master, and the Infrastructure Master. The Schema Master makes changes to the schema database. The changes are made on the Schema Master then replicated to the other Domain Controllers. Changes can be made remotely but the changes actually take place on the Schema Master. The Domain Naming Master adds or removes domains to or from the forest. Because it verifies the name of a new object by querying the Global Catalog Server, the Global Catalog must run on the same domain controller as the one holding the Domain Naming Master role. The Infrastructure Master updates group membership information when users from other domains are moved or renamed. This role should not be on the same domain controller as the Global Catalog server or the Infrastructure Master will not work because it will not contain any references to objects that it does not hold. The global catalog runs on the forest root domain controller by default. I will keep the Schema Master, and Domain Naming Master on this server, and move the other roles to another domain controller. These roles can be transferred as needed from one domain controller to another. If a server holding an operation role should

[1] David Rice, Guide To Securing Microsoft Windows 2000 Schema Version 1.0 National Security Agency – March 6, 2001

happen to become disabled, the roles can be seized from any other domain controller in the domain.

The physical location for the server will be a secured floor, with an access control system installed. Only network personnel will have access to this floor, and the server room where the domain controllers reside.

Server Hardware

The server hardware consists of a Dell PowerEdge 6450/700 with dual Pentium III processors. It will contain 1G of physical RAM. The system will contain 2 20GB hard drives configured in a RAID 1 as 2 logical drives. Logical partition C: will be set to 10GB and labeled “system” and logical partition D: will be set to 10GB and will be labeled as “programs”. After the operating system installation the D: partition will be formatted with NTFS. After formatting the partition, I will be sure to go into the NTFS permissions and remove the “Everyone” group. I will then add “Administrators” and “System” and give them Full Control. There will be a CD-ROM drive, and there will also be a standard 1.44MB floppy drive.

Operating System

Windows 2000 Server version 5.0.2195 Service Pack 1 Build 2195 was installed from CDROM. On the disk configuration screen I made sure the disk was partitioned into at least two different partitions, one for the operating system, and one for the data files. It was installed using default locations to a NTFS formatted drive. Once installation was finished I ran dcpromo to promote the server to a Domain Controller for a new Domain. Next I wanted to make sure I had all the available and necessary service packs installed. I downloaded and installed the latest service pack available from Microsoft which was Service Pack 3, available for download at:

http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/default.asp

I also downloaded and installed the latest version of Internet Explorer, which is Internet Explorer 6 available from:

http://www.microsoft.com/windows/ie/downloads/ie6/default.asp

Once that was installed, I downloaded and installed Internet Explorer 6 Service Pack 1 from:

http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/download.asp

Next I went to Add/Remove Windows Components and uninstalled IIS since there will be no need for it on this server, and there are numerous vulnerabilities associated with it. To see if there are any patches that need installed that were not

included in the Service Packs, I downloaded and ran the [2]Microsoft Security Hotfix Checker (HFNetChk) Version 3.3, which is a command-line tool that administrators can use to centrally determine if a computer, or group of computers are lacking security patches. It can be used to assess patch status for computers that are running Windows NT 4.0, Windows 2000, and Windows XP, as well as hotfixes for IIS 4.0/5.0, SQL Server 7.0/2000, and Internet Explorer 5.01 or later. It is available for download at:

http://www.microsoft.com/downloads/release.asp?releaseid=31154&area=featured&ordinal=2

By running hfnetchk with the –v switch to, I obtained the following results:

* WINDOWS 2000 SP3

NOTE MS01-022 Q296441
Please refer to Q306460 for a detailed explanation.

Patch NOT Found MS02-008 Q318203
File C:\WINNT\system32\msxml3.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS02-042 Q326886
File C:\WINNT\system32\netman.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS02-045 Q326830
File C:\WINNT\system32\xactsrv.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS02-048 Q323172
The registry key **SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility\{43F8F289-7A20-11D0-8F06-00C04FC295E1}** does not exist. It is required for this patch to be considered installed.

* Internet Explorer 6 Gold

Patch NOT Found MS02-009 Q318089
File C:\WINNT\system32\vbscript.dll has an invalid checksum and its file version is equal to or less than what is expected.

Patch NOT Found MS02-047 Q323759
File C:\WINNT\system32\mshtml.dll has an invalid checksum and its

[2] Microsoft, Microsoft Security Hotfix Checker Tool is Available
Microsoft Knowledge Base Article – Q303215

file version is equal to or less than what is expected.

To install the remaining patches that were not found on the system, I used [3]Qchain.exe, which is a command line utility released from Microsoft that gives system administrators the ability to safely chain hotfixes together. Hotfix chaining involves installing multiple hotfixes without rebooting between each installation. This increases uptime for servers, and allows for faster installations of hotfixes on a single computer. Qchain is available for download and documented at:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861

To use qchain, I downloaded the needed hotfixes into a directory along with the qchain.exe file. I then created the following batch file to do the installs:

```
@echo off
setlocal
set PATHTOFIXES= c:\que

%PATHTOFIXES%\Q318203_MSXML30_x86.exe –z -m
%PATHTOFIXES%\Q323172_w2k_sp4_x86_EN.exe -z -m
%PATHTOFIXES%\Q326830_w2k_sp4_x86_EN.exe -z -m
%PATHTOFIXES%\Q326886_w2k_sp4_x86_EN.exe -z -m
%PATHTOFIXES%\Q323759.exe /q:1 /r:n
%PATHTOFIXES%\vbs56nen.exe /q:1 /r:n
%PATHTOFIXES%\qchain.exe
```

Even though the batch file ran, and didn't return any error messages, I wanted to ensure the hotfixes installed properly, so I ran hfnetchk.exe once again, and received the following results:

```
* WINDOWS 2000 SP3

    NOTE            MS01-022    Q296441
    WARNING         MS02-008    Q318203

    * Internet Explorer 6 SP1

    INFORMATION
    All necessary hotfixes have been applied
```

The NOTE for MS01-022 is explained in Microsoft's Knowledge Base article Q306040, and can be verified by making sure that you are using version 8.103.4004.0 or later of the file Msdaipp.dll.

[3] Microsoft, Use Qchain.exe to Install Multiple Hotfixes with Only One Reboot Microsoft Knowledge Base Article – Q296861

The warning for MS02-008 is because the file Msxm13.dll has a file version greater than what is expected.

Installed Software

I have installed Norton AntiVirus Corporate Edition version 7.6. I configured this as a client to be managed by a parent server to insure virus definition updates occur on a regular scheduled basis.

Security Template

Selection

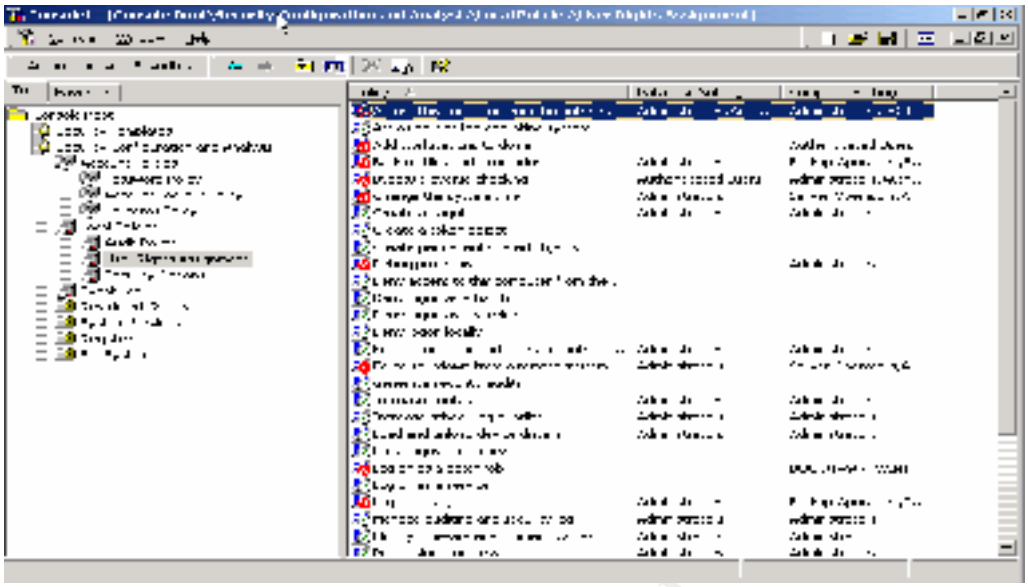
I have decided to use the w2k_dc.inf template available for download, and documented at:

http://nsa1.www.conxion.com/win2k/download.htm

The reason I have decided to use this template as a starting point is mainly for trust in the way it was developed. It was developed by the NSA with the cooperation of the other government agencies and industry partners who provided their expertise and extensive technical review. They also provide extensive configuration guides and supporting documents. Another reason is because it was designed especially for Domain Controllers. For example the options that a domain controller pulls from the Group Policy Object of the domain are not defined in this template.

Template Settings

When I downloaded the template, I saved it to the %SystemRoot%\security\templates folder. This is the default location for security templates. To review and edit the template settings and compare them to the default settings on the machine, I opened a MMC console and added in the Security Templates and the Security Configuration and Analysis snap-ins. With the Security Templates snap-in, I was able to view the templates in the templates folder. By expanding the nodes I was able to view the settings on the various options within the templates. This is also where I made any changes to the w2k_dc.inf template before loading it into the Security Configuration and Analysis snap-in. I did this by right clicking on the node, and clicking on Open database. By naming the database and clicking open, it creates a new database, and then asks you which template you want to import. I selected the w2k_dc template, and clicked open. Next I did a right click on the Security Configuration and Analysis node, and clicked Analyze Computer Now. The following is a sample of the output:



By doing this, I was able to compare the template settings with the current computer settings and be able to see any consistencies and differences. A red X indicates a difference from the base configuration, and a green check indicates consistency with the base configuration. No icon at all indicates that attribute was not included in the template used, and therefore not analyzed. This also lets me see if there are any other changes I would like to make to the template before I import it. Again, the changes would be made in the Security Template snap-in.

Account Policies

There are no account policies defined in the template that I chose to use, which is not a problem as I will be applying this template to the Domain Controllers container, and the account policies for the domain will be defined at the domain level. It is very important to address these options though, as I will discuss later.

Local Policies

Audit Policy

Audit Account logon events Success, Failure

This tracks user logon events on other computers in which the local computer was used to authenticate the account. Used to track local logons on other machines.

Audit account management Success, Failure

This tracks changes to the Security Account Database. Used to track when accounts are created, deleted, or changed. This could be used to discover misuse of privileges.

Audit directory service access Failure

This audit's user's access to Active Directory Objects that have their system access control list (SACL) defined. Used to track access to objects in Active Directory.

Audit logon events Success, Failure

This tracks users who have logged on or off, or made a network connection. It also records the type of logon requested which is helpful in knowing how and where the user logged on, or attempted to logon from. This option differs from "Audit Account Logon Events" in that it records where the logon occurred versus where the logged-on account lives. The auditing of both successful and failed logons generates a large amount of data. Network, service, and user logons are all recorded. Auditing of success events is important for tracking users logged on during potential attacks. However, if log space is at a premium, at a minimum, failure of logon events should be recorded.

Audit object access Failure

This tracks unsuccessful attempts to access objects. This can be used to track access to specific files. In order to use this you must first enable auditing in the properties of the individual object you would like to audit. If you select success or failure here, and an object has auditing enabled on it, every time an audit fulfills your requirements, an event will be written to the security event log.

Audit policy change Success, Failure

This tracks changes in security policy, such as assignment of privileges or changes in the audit policy.

Audit privilege use Failure

This tracks unsuccessful attempts to use privileges. Privileges would indicate rights assigned to Administrators or other power users. Tracks all user rights except Bypass Traverse Checking, Debug Programs, Create a Token Object, Replace Process Level Token, Generate Security Audits, Back Up Files and Directories, and Restore Files and Directories. To audit those rights excluded, enable auditing on the "Audit use of all user rights including Backup and Restore" under Security Options.

Audit process tracking No auditing

This provides detailed tracking information for events such as program executions and exits. This would create a large event log very quickly with a lot of data that is more or less useless unless you are tracking a specific behavior. You could enable auditing of success and failure to record specific events if you thought you were under attack.

Audit system events Success, Failure

This tracks events that effect the entire system, or the Audit log, such as restart, shutdown, or other security related events.

User Rights Assignment

Access this computer from the network — Administrators, Authenticated users, Enterprise Domain Controllers

This allows users to connect to the computer over the network. This will be needed for users to access the Domain Controller for authentication. It is sometimes recommended to remove the Administrators group because it would allow a stolen administrator account to be used over the network. By removing Administrators, it would force them to have physical access to access the resources on it.

Act as part of the operating system

Allows a process to perform as a secure, trusted part of the operating system. Some subsystems are granted this right. This overrides all other rights and privileges.

Add workstations to domain

Allows users to add workstations to a particular domain. This right is only meaningful on Domain Controllers. [4]Administrators and Account Operators groups have this ability and need not be given this right. This right can be very dangerous, because a user could add another domain controller to the network to get a copy of the SAM database. It is often necessary to create a group for Desktop personnel who would legitimately need to add PCs to the domain, and assign them this right.

Back up files and directories — Administrators

Allows a user to back up files and directories. This takes precedence over file and directory permissions. If this right is combined with Restore Files and Directories right, a user would be able to get a copy of any critical files they desired.

Bypass traverse checking — Authenticated users

Allows a user to change directories and access files and subdirectories even if the user has no permission to access parent directories. This prevents the user from inheriting permissions.

Change the system time — Administrators

Allows a user to set the time for the internal clock of the computer. By changing the system time, a user could alter or destroy audit trails.

Create a pagefile — Administrators

[4] Julie M. Haney, Guide To Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Kit Version 1.1.1 National Security Agency – July 22, 2002

Allows a user to create new pagefiles for virtual memory swapping and change the size of the pagefile

Create a token object

Allows a process to create access tokens that can be used to access local resources. Only the LSA should be able to create this object.

Create permanent shared objects

Allows a user to create special permanent directory objects that are used within the Windows 2000 object manager.

Debug programs

Allows a user to debug various low-level objects such as threads. This could let a user change a program to be able to rum malicious code. This right can be assigned as needed.

Deny access to this computer from the network

This right will prevent anyone from being able to access the system from across the network. If you are going to force Administrators to log on locally to make administrative changes, you could add them here to enforce that.

Deny logon as a batch job

Prevents specific users or groups to log on as a batch job, and will supercede "Logon as batch job" setting if account is subject to both policies.

Deny logon as a service

Prevents specific user accounts from registering a process as a service, and will supercede the "Log on as a service" setting if the account is subject to both policies.

Deny logon locally

Prevents specific users or groups to log on directly to the computer, and will supercede the "Log on locally" setting if the account is subject to both policies.

Enable computer and user accounts to be trusted… Administrators

Allows a user to set the "Trusted for Delegation" setting on a user or computer object. User granted this right, must also have write access to the account control flags on the user or object.

Force shutdown from a remote system Administrators

Allows a user to shut down a Windows 2000 system remotely over the network.

Generate security audits
Allows a process to generate security audit log entries.

Increase quotas Administrators
Allows a user to increase the processor quota assigned to a process.

Increase scheduling priority Administrators
Allows a user to boost the execution priority of a process, which can be done in Task Manager. If a user was able to set a process's priority to high, it could consume system resources and cause a denial of service attack.

Load and unload device drivers Administrators
Allows a user to install and remove device drivers. This could allow for a Trojan Horse device driver to be loaded.

Lock pages in memory
Allows a user to lock page in memory so they cannot be paged out to a backing store such as pagefile.sys. Could be used to launch a denial of service attack.

Log on as batch job
Allows a user to log on by means of a batch-queue facility. This is automatically granted as needed in Windows 200 by Task Scheduler.

Log on as service
Allows a process to register as a service with the system. This could allow a user to log on as a service with full control of the system. Often times certain accounts need this right, and should be monitored closely.

Log on locally Administrators
Allows a user to log on at a system's console. There are known security bugs such as GetAdmin that can escalate a users' privileges if run from the console.

Manage audit and security log Administrators
Allows a user to view and clear the security log and specify what types of object access should be audited. An attacker, to alter or clear the security log to get rid of evidence of an attack, could use this right.

Modify firmware environment rules Administrators
Allows users to modify system environment variables stored in nonvolatile RAM on systems that support this type of configuration. These variables could be modified to point to a malicious program.

Profile single process Administrators
Allows a user to perform profiling on a process.

Profile system performance — Administrators
Allows a user to perform profiling on the system.

Remove computer from docking station
Allows a user to undock a laptop from a docking station.

Replace a process level token
Allows a user to modify a process's security access token. This is a powerful right used only by the system.

Restore files and directories — Administrators
Allows a user to restore backed-up files and directories, and will supercede file and directory permissions. To overwrite a file with a malicious file, a user could use this right. In a very high security environment the Backup and Restore rights should not be given to the same user, but this is usually not a good solution in most cases.

Shut down system — Administrators
Allows a user to shut down the system.

Synchronize directory service data
This right has no effect in the initial release of Windows 2000.

Take ownership of files or other objects — Administrators
Allows a user to take ownership of files, directories, printers, and other objects on the computer. This will supercede any permissions already protecting files. A user who could take ownership of a file could then change the permissions to give them full access.

Security options

Additional restrictions for anonymous connections — No access without explicit anonymous permissions
Places restrictions on anonymous users. By setting it to "No access without explicit permissions" it will require "Anonymous" to have explicit permissions to access resources by removing the "Everyone" and "Network" groups from the anonymous users token. Keep in mind that this will disable older programs that make use of this account

Allow server operators to schedule tasks — Disabled
Allows server operators to use the scheduling service. On Domain Controllers, only Administrators have permissions to access the Task Scheduler. This could be enabled to delegate tasks to Server Operators.

Allow system to be shut down without having to log on Disabled

This is disabled by default which requires users to be able to log on to the system to be able to shut it down.

Allowed to eject removable NTFS media Administrators

Allows users to eject removable NTFS media and is set to administrators by default.

Amount of idle time required before disconnecting session 30 minutes

Sets the amount of continuous idle time in a SMB session before a session is disconnected. It is automatically reestablished if the user resumes activity after a disconnect.

Audit the access of global system objects Enabled

When enabled, this option will assign a default SACL to system objects such as mutexes, events, semaphores, and DOS devices. In order for these system objects to be audited, Audit Object Access must be enabled under auditing.

Audit use of backup and restore privilege Enabled

This enables auditing of all user rights in conjunction with Audit Privilege Use auditing being enabled. If this option were disabled, the Backup and Restore rights will not be audited.

Automatically log off users when logon time expires Not defined

This forcibly disconnects users SMB sessions when their logon hours expire. Should be set in domain level policy.

Automatically log off users when logon time expires (local) Enabled

Same as above only for the local system.

Clear virtual memory pagefile when system shuts down Enabled

Clears the system pagefile when the system shuts down. This will ensure any information that may have been in the pagefile will not be available to malicious users.

Digitally sign client communication (always) Disabled

Forces an SMB client to always digitally sign SMB communications. This option must be enabled on the client and the server in order to work.

Digitally sign client communication (when possible) Enabled

Enables an SMB client to perform digital packet signing when communicating with an SMB server that also supports packet signing.

Digitally sign server communication (always) Disabled

Forces a SMB server to always digitally sign SMB communications. This must be enabled on both client and server to work.

Digitally sign server communication (when possible) Enabled

Enables an SMB server to perform digital packet signing when communicating with a SMB client that also supports packet signing.

Disable CTRL+ALT+DEL requirement for logon Disabled

If this is enabled, a user would not be required to press CTRL+ALT+DEL to log on.

Do not display last user name in log on screen Enabled

By default Windows 2000 displays the name of the last user to logon to the system in the logon dialog box. By not enabling this, you could provide a malicious user with a username to try brute force cracking against.

LAN Manager Authentication Level Send NTLMv2 only/ refuse LM & NTLM

This parameter specifies the type of challenge/response authentication to be used for network logons with non Windows 2000 Windows clients. The template option was set to level 5, "Send NTLMv2 only/refuse LM & NTLM", the most secure.

Message text for users attempting to log on Not defined

This will be defined in our domain level policy. Legally an intruder on a network or computer is not an intruder unless they have been warned that they are not welcome on that system, and that by entering the system is agreeing that they accept that, and they know their actions may be monitored. It is very important to have a banner here for that reason.

Message title for users attempting to log on Not defined

This goes along with the message text, and should be anything as long as it does not sound like you are welcoming anyone. This will be defined in our domain level policy.

Number of previous logons to cache 0 logons

By default Windows 2000 caches the 10 last logon credentials for users who logged on interactively to a system. This should be set to zero so users will not be able to log on to the domain unless connected to the network. This can slow down the authentication process, but will prevent a malicious user from logging on to a cached account.

Prevent system maintenance of computer account password Disabled

By default, computer account passwords are changed every seven days. Enabling this option will prevent machines from requesting a weekly password change.

Prevent users from installing print drivers Enabled

This prevents members of the users group from being able to install printer drivers on the local machine. It is possible to disguise Trojan Horse types of programs as printer drivers that actually do something other than what the user thought it was going to do. They will still be able to connect to printer shares to which they have permissions.

Prompt user to change password before expiration 14 days

This sets how far in advance users are warned that their password will expire. Fourteen days is the default setting, and is also recommended, but at least seven days are required.

Recovery Console: Allow automatic administrative logon Disabled

If this option is enabled, the recovery console will not ask for an Administrators password, and will automatically log onto the system. The only time this should be enabled is if the physical security of the machine is tightly controlled. Do keep in mind though that if this is enabled, and the machine is stolen, the contents could be easily compromised.

Recovery Console: Allow floppy copy and access to all drives and folders Disabled

Recovery Console is restricted to the root folder of each volume, and the Windows system folders by default. By enabling this option, you would allow unrestricted access to an entire system.

Rename Administrator account Not defined

This will let you rename the built in Administrator account. It will be renamed, configured locally. Hackers know this is the default name of the account and it should be renamed anything other than Administrator. This is not however a guarantee against finding the Administrator account but will defiantly help defend against scripted attacks. Renaming this account can also interfere with some applications and should be tested before implemented.

Rename guest account Not defined

This will let you rename the built in Guest account. It will be renamed, configured locally. This should not be an issue if you keep the Guest account disabled, but is a good idea anyway.

Restrict CD-ROM access to locally logged-on users only Enabled

Allows only locally logged on users to access the CD-ROM. This will prevent users from sharing the CD-ROM drive.

Restrict floppy access to locally logged-on users only Enabled

Allows only locally logged on users to access the floppy.

Secure channel:
Digitally encrypt or sign secure channel data (always) Disabled
Forces a computer to always digitally encrypt or sign secure channel data.

Secure channel:
Digitally encrypt secure channel data (when possible) Enabled
Enables a computer to digitally encrypt secure channel data.

Secure channel:
Require strong (Windows 2000 or later) session key Disabled
Requires strong encryption keys for all outgoing secure channel communications.

Secure system partition (for RISC platforms only) Not defined
Not a RISK platform

Send unencrypted password to connect to third-party SMB servers Disabled
This should not be enabled, to avoid being able to send clear text password exchanges during authentication on some Non-Microsoft servers.

Shut down system immediately if unable to log security audits Enabled
If events cannot be written to the security log, the system is halted immediately. If this is the result of a full log, an Administrator must log onto the system and clear the log.

Smart card removal behavior Lock workstation
Determines what action to take when a smart card for a logged on user is removed from the smart card reader. By using the "Lock Workstation" option, user will be able to remove their card and walk away, then later return to their same session.

Strengthen default permissions of global system objects Enabled
Strengthens the DACLs on the global list of shared system resources so that non-administrative users can read, but not modify shared objects they did not create.

Unsigned driver installation behavior Warn but allow Installation
This determines the action to take when a device driver that has not been certified for Windows 2000 attempts to load. This should be set to anything except silent success. If a user or an administrator is going to install unauthenticated drivers, they should at least receive a warning.

Unsigned non-driver installation behavior — Warn but allow Installation

This determines the action to take when non-device driver software that has not been certified for Windows 2000 attempts to load. This is much like the setting above, and should be set the same

Event log

Maximum application log size — 4194240 kilobytes

This is the maximum setting for the log and will allow the log file to equal the amount of space available on the hard drive, or up to 4 GB.

Maximum security log size — 4194240 kilobytes

This is the maximum setting for the log and will allow the log file to equal the amount of space available on the hard drive, or up to 4 GB.

Maximum system log size — 4194240 kilobytes

This is the maximum setting for the log and will allow the log file to equal the amount of space available on the hard drive, or up to 4 GB.

Restrict guest access to application log — Enabled

Restrict guest access to security log — Enabled

Restrict guest access to system log — Enabled

Default configuration allows guests and null logons the ability to view event logs (system and application logs). While the security log is protected from guest access by default, it is viewable by users with the Manage Audit Logs user right. This option disallows guests and null logons from viewing any of the event logs.

Retain application log — Not defined

Retain security log — Not defined

Retain system log — Not defined

These options control how long the event logs will be retained before they are overwritten. Since it is not recommended to overwrite any event logs, this option should not be configured.

Retention method for application log — Manually

Retention method for security log — Manually

Retention method for system log — Manually

This is how the operating system handles event logs that have reached their maximum size. To ensure that no important data is lost, especially in the event of a

security breach, the event logs should not be overwritten. I have set it to be cleared manually.

Shut down the computer when the security audit log is full Enabled

If events cannot write to the security log, the system should be halted immediately. If it stops because of a full log, an administrator must log on locally and clear the log.

Restricted Groups

The chosen template did not have any restricted groups defined, but since we are concerned about the Schema Master, I have decided to restrict the Schema Admins group with Administrator as the only member. To do this by using the Security Templates MMC snap-in, right click on Restricted Groups in the left pane, then select Add Group, which will open a window to allow you to type in, or browse to select the group desired.

System Services

It is recommended to always disable all unused, or unneeded services. This can be very hard to, as Microsoft has poor documentation of each services complete function, and it's dependencies. It is usually easier to decide what services are needed for the basic functionality of the system. If you are uncertain about a service, disable it and test your system for functionality. Be sure to only do this to one service at a time so you will be able to determine which service it is if there becomes a problem with your systems functionality. Once it is determined what all services are needed, you can disable the rest.

Here is a list of the services I kept enabled, and I disabled all the rest.

- DNS Client
- DNS Server
- Event Log
- File Replication Service
- Kerberos Key Distribution Center
- Logical Disk Manager
- Net Logon
- Network Connections
- Norton AntiVirus Client
- NT LM Security Support Provider
- Plug And Play
- Protected Storage
- Remote Procedure Call
- Remote Procedure Call Locator
- Security Accounts Manager
- Server
- TCP/IP NetBIOS helper

- Windows Time
- Workstation (when connecting to resources)

Registry Settings

I have left the registry settings in the template as they are with the exception of the key \MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg. This key defines which users and groups can connect to the system for remote registry access. If the key did not exist, anyone would be able to connect remotely to the registry. Since we will not be using the Backup Operators group, I have removed it. I have added Exchange Domain Servers group with full access because we are using Microsoft Exchange 2000, and it requires remote registry access.

Applying The Template

Since I will be applying the template to the Default Domain Controllers container, I will need to import it into it's Group Policy Object. To do this I opened Active Directory Users and Computers, and right clicked on the Domain Controllers container, then clicked on properties. Inside the Domain Controllers Properties window, I clicked on the Group Policy Tab. The Default Domain Controllers Policy is already highlighted, so I clicked on Edit. Next I navigated to the Computer Configuration\Windows Settings\Security Settings node, and right clicked on Security Settings. Then I selected Import Policy. When the Import Policy From window opened, it initially displayed all the files in the %SystemRoot%\security\templates folder. I then double clicked the w2k_dc.inf file, which imported the template settings into the Security Settings node.

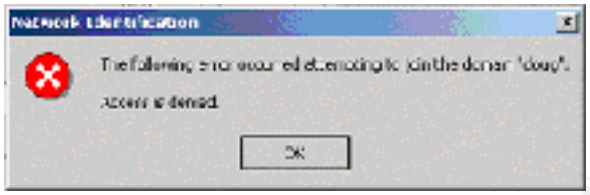
[5]Within Active Directory, computers refresh GPO settings at established intervals. The default Group Policy refresh intervals are 90 minutes for computers running Windows 2000 Professional, and for member servers running Windows 2000 Server, and every 5 minutes for domain controllers. Since I have applied the template to the Domain Controllers container, I can be assured the security settings will be refreshed every 5 minutes. Any domain controllers added to the domain will also receive these settings since they are added to this container by default. I could also use the Security Configuration and Analysis tool to occasionally audit the system to make sure the policy hasn't changed.

Testing the security settings

By default, authenticated users are given the right to add workstations to the domain. Our template had removed authenticated users, leaving no one defined for this right. Administrators and Account Operators automatically have this right, and it need not be defined for them. To make sure authenticated users could not add workstations to the domain I created a user account on the domain with the

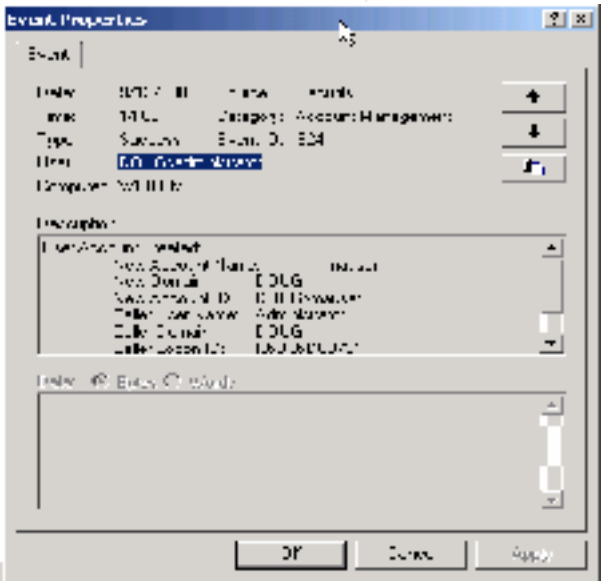
[5] Julie M. Haney Securing Microsoft Windows 2000 Group Policy Version 1.1 National Security Agency - September 13, 2001

logon name of tttester, making sure it was only a member of the Domain Users group. Next I tried to add a workstation to the domain using the credentials of the created account. I was unable to add the account as an authenticated user, as seen in the error window below.

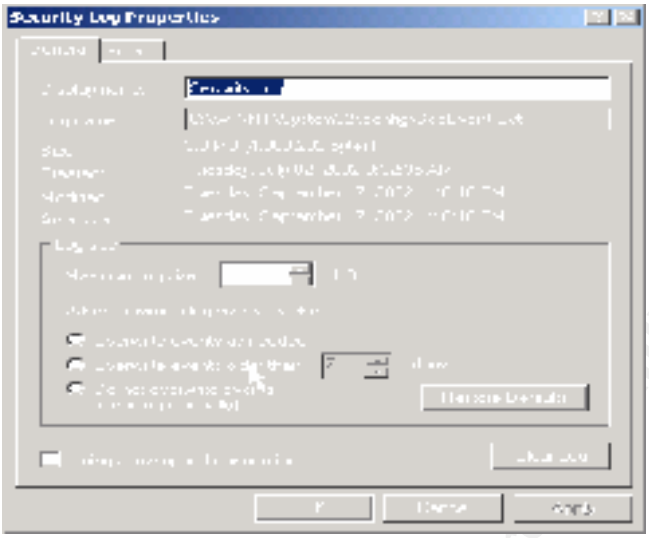


I next tried adding the machine using the credentials of an administrator, and was able to add the computer to the domain.

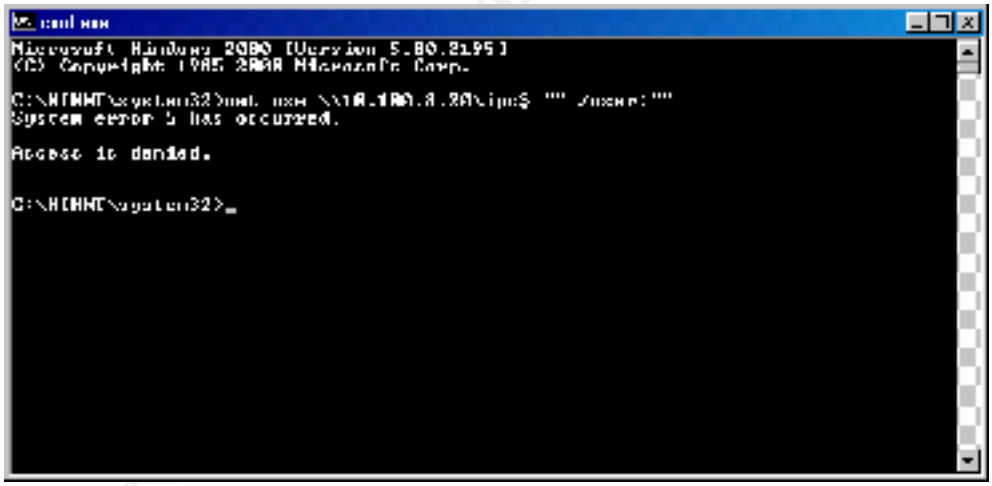
I also wanted to audit Account Management to be able to tell of any new unexpected accounts being created. To test this, I created a new user, then opened Event Viewer and selected the security log and looked for event ID 624 which is a success audit of User Account Created. The following entry showed up in the log:



While I had Event Viewer open, I right clicked on the security node and clicked properties to check to see if my Event Log settings such as log size, and retention methods are defined as they were in the template. By looking at the security log properties screenshot below, I see that the log size is changed from the default setting of 512 KB to the maximum of 4194240 KB, and Do not overwrite events (clear log manually) is selected.



I also wanted to restrict anonymous connections, to prevent anyone from getting a full dump of all your usernames, groups, shares, permissions, policies, services and more using the Null user. To test this I tried making a null user connection by running the net use *ip_address*\ipc$ "" /user: "" command from a command prompt. I was denied access as seen in the screenshot below:



Another good test for the security of your system is to use the Microsoft Security Baseline Analyzer (MBSA). This is a tool that was developed for Microsoft by Shavlik Technologies LLC. [6]Version 1.0 of MBSA includes a graphical and command line interface that can perform local or remote scans of Windows systems. MBSA runs on Windows 2000 and Windows XP systems and will scan for missing hotfixes and vulnerabilities in the following products: Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server (IIS) 4.0 and 5.0, SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000 and 2002. MBSA creates and stores individual XML security reports for each computer

[6] Microsoft – Microsoft Security Baseline Analyzer

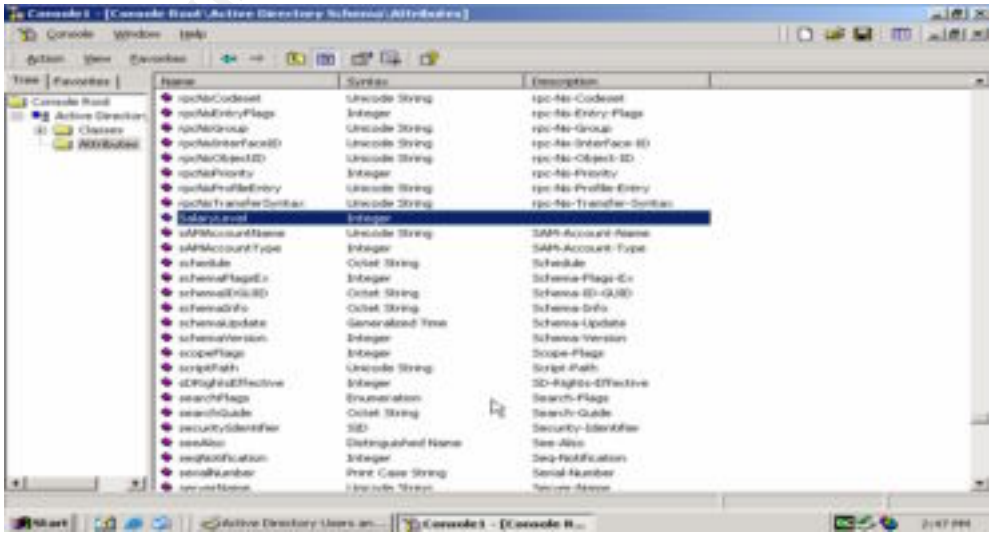
scanned and will display the reports in the graphical user interface in HTML.). It is available for download and documented at:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp

After running the tool, it reported that I was missing 4 security Hotfixes on the machine, yet when I built the machine, I made certain I had all available patches applied. The reason for the need for more patches is because Microsoft had released more patches in between the time I had applied the previous patches and the time I ran the Microsoft Baseline Security Analyzer. This is why it is very important to subscribe to an e-mail newsgroup of some sort that will keep you notified of new security patches as soon as the are available. The best way to keep current on Microsoft patches is to sign up for the Microsoft Security Notification Service. This is a free service from Microsoft to provide security information about their products. You can subscribe at http://register.microsoft.com/regsys/pic.asp. Another free tool available to test your security settings is the Webscan tool by Security Expressions. The difference is the Webscan tool will also let you check your user rights assignment, registry permissions, and file permissions against a Microsoft White Paper for NT, or against NSA guidelines. The tool along with more documentation about it and how it works is available at http://www.pedestalsoftware.com/secexp/webscan/scan.htm.

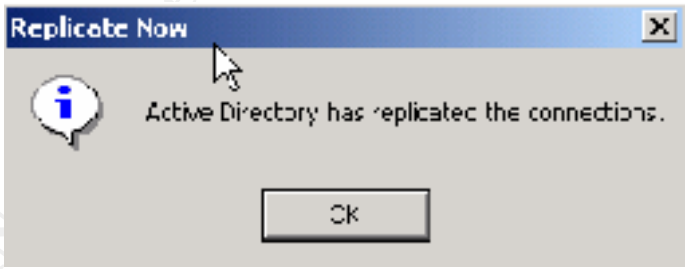
Testing Functionality

Since this will be the Schema Master, the first test I want to do is to make sure I am able to make changes to the Schema when they are deemed necessary. I logged on locally to the Domain Controller as an administrator and, following the directions in Microsoft's Step-by-Step Guide to Using Active Directory Schema and Display Specifiers, I was able to add the SalaryLevel attribute to the Schema as seen in the screen-shot below.



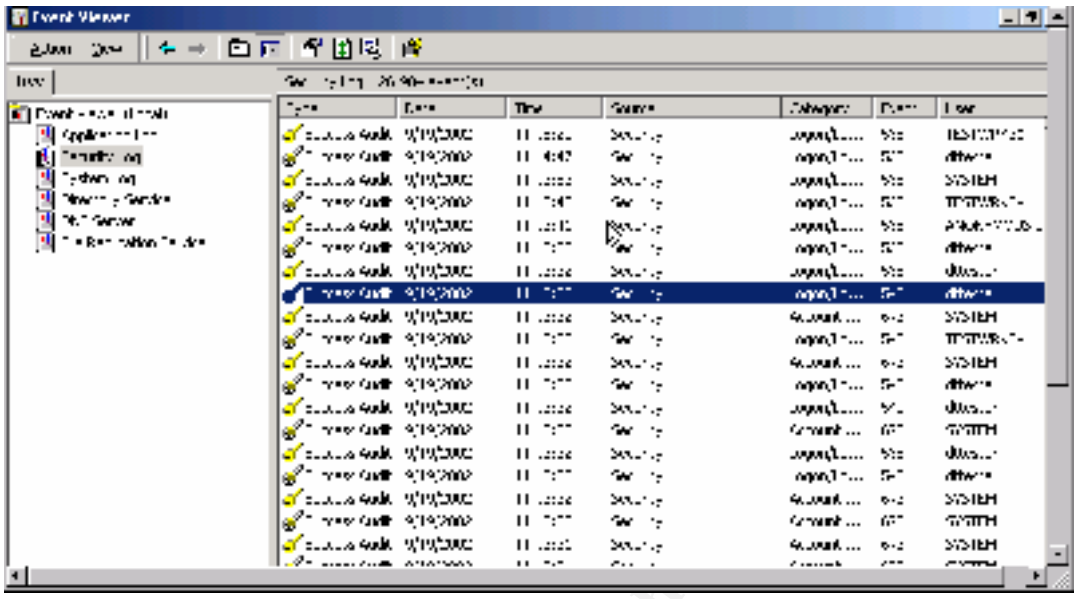
[7]In order to write to the Schema you must create new DWORD registry entry called *Schema Update Allowed* under the key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\parameters. A value of 1 will enable write access to the Schema. It is imperative that the Schema Update Allowed value is set back to 0 (disable write-access) after any changes have been made to the Schema. Failure to do so may leave the Schema vulnerable. There are some programs that will need to write to the Schema as part of their installation. Sometimes they are not coded well enough to set the value back to 0, so you should manually check this after any installation that you would suspect as writing to the Schema. Keep in mind that adding a new attribute to the global catalog causes a full synchronization of all of object attributes stored in the global catalog (for all of the domains in the forest). In a large, multi-domain forest, this one-time synchronization can cause significant network traffic.

Once I have made the changes that are needed, I want to make sure I am able to replicate these changes to the other domain controllers. To test to see if I am able to replicate, I used Active Directory Sites and Services from Administrative tools. Once opened, I expanded the sites container in the left hand pane. Next I expanded the container that represents the site that holds the target that needs to be synchronized. Next I expanded the servers container, then expanded the target server to display the NTDS Settings object, which represents settings for the domain controller. Click on the NTDS settings to show the connection objects in the right pane that represent the replication partners. Now I right click on the connection object in the right plane and click Replicate Now. This will initiate replication of any changes from the source server represented by the connection object, to the target server. Once doing this, I received the following window letting me know the replication has occurred:



I also want to make sure users are able to log on, and authenticate properly. To test this, I tried to logon using the credentials of my test user from the computer I had added to the domain. By looking in the security log, using Event Viewer, I am able to see where my test user 'dttester' logged event ID number 540, which is a success audit for a successful network logon. This can be seen in the screen shot pictured below.

[7] David Rice Guide To Securing Microsoft Windows 2000 Schema Version 1.0 National Security Agency – March 6, 2001



This also assures me that option to Audit Logon Events, which was set to audit both success and failure attempts in the template, is auditing successful logon events.

Template Evaluation

Overall, I would say the template I chose was designed for general use for domain controllers only. If using this template, you must be aware that no Account Policies are defined. This template was designed for Domain Controllers and Domain Controllers by default pull some security settings only from the group policy objects linked to the domain. These settings include Account Lockout, Password, and Kerberos policies, plus the rename administrator account, rename guest account, and the automatically log off users when logon time expires security options. The reason for this is in case a Domain Controller is moved to another Organizational Unit it will still get the same settings it had before. It also helps make certain these settings are consistent on all domain controllers, since all Domain Controllers share the same account database for the domain. This ensures that members of the domain have a consistent experience no matter what Domain Controller they log on to. Also, settings defined in the default Domain Controllers Group Policy Object have higher precedence than settings defined in the default domain Group Policy Object. This ensures that a setting at the domain level will not override a setting on the Domain Controllers container that may be critical to the functionality of the Domain Controller.

These options should definitely be addressed, as the default settings are much to weak. I have included my recommendations for the settings, with a brief description in the table listed below.

Policy	Effective Setting	Recommended Setting	Explanation
Enforce password history	1 passwords remembered	6 passwords remembered	User cannot use any of their past 6 passwords
Maximum password age	42 days	90 days	This would require a user to change their password every 90 days.
Minimum password age	0days	1 days	By remembering the last 6 passwords, and having the minimum password age set to 1 day, a user would have to wait a week to try to cycle back to an original password by changing their password.
Minimum password length	0 characters	8 characters	Passwords must be at least 8 characters long.
Passwords must meet complexity requirements.	Disabled	Enabled	Passwords must contain characters from 3 of 4 classes: upper case letters, lower case letters, numbers, and special characters. Using strong passwords will help prevent brute force attacks.
Store password using reversible encryption	Disabled	Disabled	This is to provide password information to some applications, and the passwords are stored with a two-way hash. Storing

			passwords should NOT be permitted.
Account lockout duration	Not defined	30 minutes	Sets the number of minutes the account will be locked out.
Account lockout threshold	0 invalid logon attempts	5 invalid logon attempts	Specifies the number of invalid logon attempts that can be made before the account is locked out. This also helps prevent brute force password cracking.
Reset account lockout counter after	Not defined	30 minutes	Sets the number of minutes until the invalid logon count is reset.

You must consider all these settings carefully and decide how they should be applied to best suit your environment. Since this is a Government agency they would be able to use the enhanced password complexity filter enpasflt.dll in place of the passfilt.dll filter provided by Microsoft. Enpasfilt.dll is available from the NSA, and only provided to Government agencies. The difference between the two filters is that enpasfilt.dll enforces passwords of at least eight characters in length, and must contain a character from all four classes of characters that are upper case, lower case, numerals, and special characters. In addition the it will prevent the use of the user logon name, or full name in the password. If you believe you want more secure settings, such as longer passwords, and shorter password ages, or using a password filter, keep in mind that the harder it is for a user to remember and manage their password, the greater the chance they will write it down and stick it under their keyboard, or to their monitor, which defeats the purpose entirely.

I would definitely rename the administrator and guest accounts locally. Be sure to change the description also. Create a new account with no privileges, and name it Administrator. This Account should be audited for logon attempts. A hacker could still locate the true Administrator or Guest account by looking for the right SID ending, but it does add yet another layer of protection to your system.

The Services section was very weak, with no options defined at all. I assume the reasoning for this is to make the template practical for generic use. The services that are needed on a Domain Controller can vary from environment to environment, and a service that is critical in one environment might not be needed at all in another. It is also recommended to disable services very cautiously as they may be critical to your system. By going through them and disabling them one at a time, it will be easier to tell what services are needed, and what are not.

I would highly recommend going through the services and changing the template settings to disable any unused or unneeded services to suit your environments needs.

The template's file system security settings included settings that are only applicable to domain controllers, such as %SystemRoot%\NTDS for Active Directory logs, %SystemRoot%\SYSVOL for the default Active Directory location for files that must be shared throughout a domain, and %SystemRoot%\SYSVOL\domain\Policies that contains group policy objects. I also like the fact that they have removed the "Everyone" group from the permissions and replaced it with "Authenticated Users". The important difference between the two is that anonymous logon users (or NULL session connections) are never members of the Authenticated Users group.

From looking at the results from the testing, the template settings provide the security settings needed and recommended for a secure domain controller that also holds the role of Schema Master, yet it is generic enough that it did not interfere with the domain controller's functionality. I think this is a very well designed template and is very appropriate to this environment.

References

David Rice, Guide To Securing Microsoft Windows 2000 Schema Version 1.0 National Security Agency – March 6, 2001

Microsoft, Microsoft Security Hotfix Checker Tool is Available Microsoft Knowledge Base Article – Q303215

Microsoft, Use Qchain.exe to Install Multiple Hotfixes with Only One Reboot Microsoft Knowledge Base Article – Q296861

Julie M. Haney, Guide To Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Kit Version 1.1.1 National Security Agency – July 22, 2002

Microsoft – Microsoft Security Baseline Analyzer