Global Information Assurance Certification Paper

Slamming the Slammer worm–

Securing a database server using both a Security Template and a Checklist

Prepared by

Tim Gensler

April 2003

Prepared for the GIAC Certified Windows Security Administrator (GCWN)
Practical Assignment v 3.1 (revised April 8 2002) – Option 2

Disclaimer

No company or character in this paper is meant to represent any real person, living or dead. All names both for the company and its products were made up solely for the purposes of writing this paper. Any product names that sound like any existing products are purely coincidental. All street addresses are also fictitious. All IP addresses and other sensitive information have been sanitized for this publication. The company name used in the paper is HydrationInc. There is ***no space*** separating Hydration and Inc.

"Is it safe?"

--Szell (Laurence Olivier) to Babe (Dustin Hoffman)

Marathon Man (the movie) -theatrical release in October, 1976

Executive Summary

The Slammer worm struck the Internet and caused massive traffic problems due to unpatched Microsoft SQL Server databases. [1] Not even Microsoft with all its vast resources was immune from the Slammers victim list.[2] It is with this in mind that this paper will describe how to properly secure a Microsoft SQL Server database running under Microsoft Windows 2000 using a template for the operating system and a checklist for the database.

This paper describes a typical small company IT scenario of securing a database server on their local premises. The company is in startup mode and was created after a successful defense of a Ph.D. dissertation. The company is faced with numerous obstacles, the first being funding. With this in mind, they have purchased their IT equipment on Ebay and have contracted with us to secure the server where they are keeping their data for the only product that they sell, a reporting package describing water conditions in vines for wine growers.

The owners were successful in setting up a local network. However, with the business growing, they wish to impress upon clients and potential investors that they are stable and technically competent company. They have purchased the necessary hardware and several retail copies of Windows 2000 to outfit their meager staff. However, after reading about some of the problems with Microsoft's operating system, they wish to make sure they are doing everything correctly.

The main focus of the paper will be securing the database server for this company. Because security does not exist in a vacuum, the wishes of the owner will take precedence over what could be considered a "best practice". A standard template will be applied to the operating system to secure it. Following that, a database checklist for securing the database will be applied. Testing will be performed to verify the effectiveness of both. Lastly, recognizing that security is a vigilant readiness and not a one time fix, suggestions will be offered to prevent future problems from occurring and to keep this company running smoothly from a technical perspective.

Company background

HydrationInc is a newly formed company formed by Dr. I.M. Smart for the purposes of selling plant-water content reports to winegrowers. Based in Stanford, California, just off Lomalita Drive, Dr. Smart has set up his newly formed corporation, HydrationInc. Dr. Smart has recently completed his

dissertation proving that wine flavors change based on how much water is contained in grapevines during their growing season. The company produces, by hand, small battery operated monitoring devices called the *Wineboy gimlet*™ that are inserted into the vines and measures the amount of water in the plant. These devices transmit, on a daily basis, the amount of water contained in the vine. The information is transmitted to a radio receiver at the farmer's house. Once a week, by FTP, the farmer uploads the data to an ISP that hosts the company's FTP site and web server. The company then retrieves the files off the ISPs FTP server and loads the data into the database at the home office. Reports are created and emailed back to the farmer. The farmer can then decide scientifically whether to water the plants or not. They have chosen to keep the FTP server located at the ISP because it has a guaranteed uptime policy. The office is connected to the same ISP through a business DSL connection.

The IT situation is typical for a struggling business. Dr. Smart took over the offices of a failed Internet company. Network wiring was in place and some abandoned furniture came with the company. They have 2 servers that run Windows 2000. The first serves as the domain controller, the second server serves as a dedicated member server running the SQL Server database. They have 3 office PCs running Windows 2000 Professional that are used for creating farm reports, email and Internet browsing. Two laptops, running Windows XP, are also connected from time to time and they are taken on the road to demonstrate the system to potential clients. Contractors can bring in their laptops and plug into these connections. They company has DSL connection for Internet access. A Netgear FVL328 ProSafe High-Speed VPN Firewall is connected to the Motorola cable modem and offers DHCP to the office clients. Performance is not currently an issue. HydrationInc needs to pull down information once a day from the FTP site at its ISP. The data is uploaded to the database at the end of day. All office PCs will connect to the database for extensive analysis of the water data. The database also contains lists of potential farmers that could be future customers. Dr. Smart employs his wife and his son to help run the business. Both of these individuals have PCs on their desks. The wife is the one who pulls the FTP files, loads it into the database and massages the data for the reports. The son helps put together the *Wineboy gimlet*™ on an as needed basis. Groups of farmers that are potential customers are brought in from time to time to demonstrate the system. A desktop PC is setup in the conference room for this purpose.

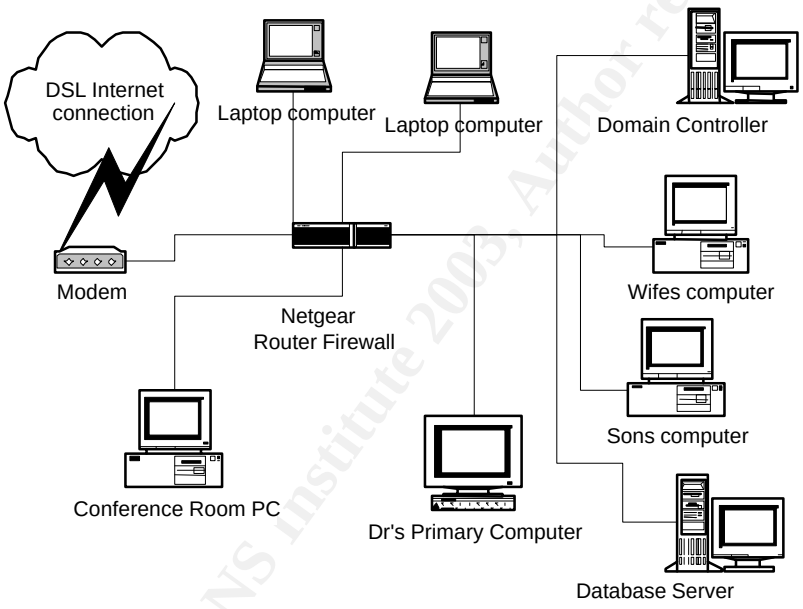
Operational needs and requirements

The company wants to secure the database from unwanted tampering. Currently the son has shown great technical aptitude and sometimes experiments with the company's equipment putting games on the various PCs, as his is the oldest and slowest PC at the company. As the business relies solely on the data captured within the database server, it is imperative that this data and the box it is on are impervious to attack or an employee's mischievous activities. Dr. Smart is

concerned after reading about the SLAMMER worm and how it affected Microsoft. He has asked to have just his database server “locked down”. They also do not want potential customers left alone in the conference room to have access to the network. This paper will only focus on providing that security through a template to lock down the operating system and checklist to lock down the database for that one server.

Network Layout of the Office

Dr. Smart’s wife buys the company equipment on Ebay to save money. The router is an 8 port Netgear connected to the Internet by a Motorola Modem. The database server is a clone running an AMD Duron 750 MHz with 512 MB of memory. It has 1 network interface card of unknown origin running at 100 MBs /full duplex. An 8GB 4mm-tape drive is internal. For storage it has 3 disk drives but they are not in any raid setup. It has 60 GB of disk storage. The domain controller is a clone as well with 128 MB of memory and a single 40 GB hard drive. The office PCs are clones with 64 MB of memory and 10-20 GB hard drives. The conference room PC has 128 MB of memory and a 10 GB hard drive.



Operational Solution

Even though HydrationInc wishes to keep costs low, physically securing the servers is a priority. To keep individuals away from the equipment, a telecom computer cabinet rack with fans was purchased on Ebay. Standing 84" tall, this cabinet houses the domain controller, the database server, the router and the modem. Because it is lockable, this was considered a wise investment. Additionally, a fireproof box was purchased to house backup tapes made on a daily basis, with the wife being tasked with performing the backup, removing the

tape, and locking the cabinet. A small uninterruptible power supply (UPS) protects the server from spikes and surges.

What are they trying to protect and what are they defending against

Dr. Smart was interviewed to determine what his concerns were to the company. His fears were:

- His son loading games on the servers.
- Outsiders browsing the network from the conference room PC and obtaining/corrupting client data in the database.
- The slammer worm and how it affected Microsoft in the papers.
- Individuals visiting from time to time to perform statistical analysis on the data to try to spot trends. These individuals are contractors who work for the farmers but require access to the data. Dr. Smart wants them only looking at the field data for the farmer who is employing them. He does not want the contractors to find out who his other customers are so that they do not undercut the services Dr. Smart is providing to them.

It was proposed to lock down the server using a security template along with the database using a checklist. Dr. Smart agreed with the assessment.
The requirements outlined were:

- Only Dr. and Mrs. Smart should be able to logon to the database server locally. All others must use the application that was developed for the purpose.
- The database should listen on a non-standard port to prevent contractors from casually finding it.
- Login and other audit logging must be enabled to make sure no one is trying to login beyond the scope of their responsibilities.
- Update services will be turned off to prevent unwanted fixes from being downloaded.

This paper will go over the steps used to secure HydrationInc's database server.

Initial Hardware and Software Setup

BIOS Setup

The BIOS was set to boot from the C: drive, followed by the CD-ROM, followed by the floppy disk. After all software was installed, this was changed to be booted from the C: drive only. A password was set on changing the BIOS configuration, to prevent the son from booting from a diskette and using the CD-

ROM. After all software was installed, the CD-ROMs IDE power cord was unplugged, as it was not deemed necessary. If a CD was needed, a share on the network could be accessed for the purposes of software installation.

Windows 2000 Installation

Because of the number of games already installed on the server, it was decided a fresh install of the operating system and database would be the best course of action. Backups were made of the production databases. The special NIC card drivers were located prior to formatting.

- The system was removed from the network and then wiped clean. Four partitions on two of the three drives were created. Windows 2000 was installed into its own partition with nothing else purposely being installed there. Windows 2000 Server was installed with the only Windows components being Accessories.
- Installed next was the Transmission Control Protocol/Internet Protocol (TCP/IP) networking and Client for Microsoft Networking.
- From a CD, Windows service pack 3 was installed.
- It was then plugged back into the office LAN behind the Netgear router/firewall.
- Windows update was connected to and all security updates were applied for the operating system.
- Internet Explorer was not updated to the latest version at this time but was left at the 5.0 default version.
- An Emergency Repair Disk (ERD) was created. The ERD will be used for disaster recovery. The disk will be stored in the fireproof box.
- The MARQUEE password-protected screen saver was set with a maximum wait time of 5 minutes. Set the text to display: ***Unauthorized Use Prohibited- All Actions will be logged and monitored. IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION. Contact a HydrationInc manager for other restrictions***. The speed was set to a slow setting.

Other application software installed was:

- *Winzip 8.1* was purchased and installed to compress the databases prior to tape backup.
- *WS-FTP Pro* was purchased and installed – to send out database backups should the tape drive fail.
- *Adobe Acrobat 5 reader* was downloaded and installed to read documents on the SQL Server CD.
- *AVG Free Edition version 6* was downloaded and installed. It provides antivirus protection for protecting against bootup viruses located on floppy disks (should the ERD disk ever get corrupted). Because none of the office PCs had current virus protection, this product was loaded on both servers as

well as the office PCs. Dr. Smart did not wish to purchase anything else at this time, and this product was free for both office and home use.

User Accounts

To minimize the possibly of break-ins, separate accounts will be created for all individuals at the company, as well as separate accounts for SQL Server. Dr. and Mrs. Smart will both have 2 accounts; one for everyday use and a second for when an administrator access to a server is needed, such as when they wish to check the event logs. The Guest account, while already disabled, will be further strengthened by having a strong password put on it and limiting the logon hours, should it ever get turned on accidentally[3].
The command line used perform this was:

Net user guest /times:Sunday,22:00 –23:00

The Syskey.exe program was run to protect passwords stored in the registry in the local Security Accounts Manager (SAM) registry key.

Operating System Template Selection

To secure the operating system that the database will be running on, group policy templates from Microsoft and the NSA were examined. Because of the dedicated nature of the database, and the fact that the only access needed would be through a custom written application, both templates would serve HydrationInc equally well. It was assumed because this was a Windows 2000/XP shop, the best template would be one with the most strict settings.

Operating System Template Settings

Microsoft's and the NSA's templates are similar in design. Microsoft provides two templates in the base install of Windows 2000 Server that would be appropriate: ***hisecdc.inf*** is designed for high security for a domain controller and securedc.inf, which is designed for domain controllers as well. The difference between Microsoft's two templates are: *'the levels of encryption and signing that are required for authentication and for the data that flows over secure channels and between SMB clients and servers'*.[4]

The NSA's template, **NSA_w2k_server.inf,** further restricts settings more than the ***hisecdc.inf*** in most instances***.*** However, in some instances, it is actually less restrictive. For example, with passwords the NSA allows the minimum password age to be 1 day while both of Microsoft's templates require a more stringent 2 days. Since the goal is to start with known template that will meet a majority of our needs, it was decided to pick the more restrictive NSA template. The primary objectives of group policy for just the database server were:

- a policy that would limit the system services running the database server

- a policy that was set to audit valid and invalid logon events
- a policy that would set permissions on keys within the registry
- Secure the various files within the filesystem. Directories such as the **winnt\repair** directory where the emergency repair disk loads backup files to must also be restricted from the curious

Extra items contained in the policy would be acceptable so long as they did not hamper the operation of the database server itself.

All templates provide for the following sections:

Security area	Description
Account Policies	Password , Account Lockout, and Kerberos Policy
Local Policies	Audit Policy, User Rights Assignment, and Security Options
Event Log	Event Log settings and Event Viewer settings
Restricted Groups	Policies pertaining to default system groups such as power users
System Services	Startup and permissions for all services running on the server
Registry	Registry security keys permission and audit settings
File System	Permissions for file/directory security settings

The Security Configuration and Analysis MMC snap in was used to examine the NSA security template. To use it, start the MMC by using the Start menu, Run command, and open *mmc.exe.* Add the Security Templates snap-in and the Security Configuration and Analysis snap-in to the MMC by selecting Console, Add/Remove Snap-in, Add, and scrolling down and locating them. Highlight each and press the Add button. Press Close and then OK.
Each section of the template will be reviewed and explained.

Account Policies

Password Policies

Enforce password history - 24 passwords remembered
This setting ensures that when new passwords are created, they will be unique from the ones used previously. If a user tries to change his password several times in a row, they would have to do this 24 times before they could get back to the one they wanted. However, the Minimum Password Age would prevent them from doing this at one time.

Maximum password age -90 days
In days, the time that a password can be used to logon before having to change it.

Minimum password age - 1 day
In days, the time that must pass before a user can change it to something else.

Minimum password length - 12 characters
This is least number of characters that a password must contain. On one hand, longer passwords are considered stronger. On the other hand, longer passwords tend to be written down which can lead to a breach of security.

Passwords must meet complexity requirements – Enabled
The Microsoft requirements for a complex password are that it is at least 6 characters in length and should contain a combination of uppercase, lowercase, numerical digits and possibly non-alphanumeric characters ***!$#%.***

Store password using reversible encryption - Disabled
If, for legacy applications, the password must be stored so that it can be decrypted easily. This is a very poor practice and such applications must be upgraded if the environment is to be considered secure. Fortunately for HydrationInc, this will not be a problem as it has no legacy applications.

Account Lockout Policies

Account lockout duration -15 minutes
Once a user has entered in the incorrect password '*Account lockout threshold'* times, the account will lock and stay locked this amount of minutes and then become unlocked. If someone is running a password-guessing program, setting this value high will prevent him or her from trying a large number of passwords. However, for legitimate users with typing problems, a high number means more frequent helpdesk calls.

Account lockout threshold - 3 invalid logon attempts
This is the number of failed logon attempts that can occur before an account will be locked out. This occurs on initial logon and not when unlocking from a password protected screen saver.

Reset account lockout counter after - 15 minutes
This is the number of minutes to wait after a failed logon attempt before the bad logon attempt counter is reset to 0.

Local Policies

Audit Policies

Audit account logon events -Success, Failure
This records a user logging on and/or logging off of a computer on the network

Audit account management - Success, Failure

This logs when a user account is created, changed, deleted, renamed, disabled, or enabled. It also logs when a password is set or changed.

Audit directory service access - No auditing
This records when a user accesses the Active Directory

Audit logon events- Success, Failure
This records a user logging on, logging off, or making a network connection to this computer

Audit object access- Failure
This records when a user accesses any file, folder, registry key, printer or any other object in the system.

Audit policy change -Success, Failure
This logs when user rights are changed on assignment policies, audit policies and trust policies.

Audit privilege use – Failure
This logs when a user exercises one of his user rights.
Backup and Restore files are some of the rights not included in this setting.

Audit process tracking - No auditing
This records events such as program activation and process exit. This is useful If rouge PCs are straying into the building or people are upgrading the OS without consent.

Audit system events -Success, Failure
This records when a user restarts or shuts down the computer.

User Rights Assignment Policies

Access this computer from the network – Administrators, Users
Defines which users and groups are allowed to make connections to the computer over the network.

Act as part of the operating system- Not defined in template

Add workstations to domain - Not defined in template

Back up files and directories – Administrators
This allows the individual to bypass permissions and read and backup files and directories. This could be a potential abuse of power.

Bypass traverse checking - Users

This allows a user to bypass security for the purposes of going though a directory. This does not allow one to retrieve a list of files from any directory that one is traversing through.

Change the system time - Administrators
Only the Administrator should change the system time. This is crucial for file time stamps and database timestamps.

Create a pagefile – Administrators
This defines who should be able to create and change the size of a pagefile(s) for the system. Setting this to low can cause performance problems.

Create a token object- Not defined in template

Create permanent shared objects - Not defined in template

Debug programs - Not defined in template

Deny access to this computer from the network - Not defined in template

Deny logon as a batch job - Not defined in template

Deny logon as a service - Not defined in template

Deny logon locally - Not defined in template

Enable computer and user accounts to be trusted for delegation - Not defined in template

Force shutdown from a remote system - Administrators
This lists the users and groups who should be able to shut down the server remotely.

Generate security audits - Not defined in template

Increase quotas – Administrators
This shows which accounts can use 1 process to access another process and increase processor quota. While possibly useful for system tuning, the Windows 2000 Resource Kit states it can be abused as in a denial-of-service attack[5]

Increase scheduling priority – Administrators
This is similar to above where 1 process to access another process and change the seconds scheduling priority.

Load and unload device drivers- Administrators

This lists who can dynamically load device drivers.

Lock pages in memory - Not defined in template

Log on as a batch job - Not defined in template

Log on as a service - Not defined in template

Log on locally –Administrators
This defines who can log on at the computer console. This is a critical privilege and restricting this will help prevent problems. Dr. and Mrs. Smart will each have a separate administrative account for when they need to logon to the database server locally.

Manage auditing and security log - Administrators
This defines who can set auditing options for specific resources.

Modify firmware environment values - Administrators
This defines who can modify system environment variables such as the path.

Profile single process - Administrators
This defines who can run performance monitor for observing application processes.

Profile system performance – Administrators
This defines who can run performance monitor for observing system processes.

Remove computer from docking station - Not defined in template

Replace a process level token - Not defined in template

Restore files and directories -Administrators
This right allows the individual to bypass permissions and restore files and directories. This could be a potential abuse of power.

Shut down the system - Administrators
This defines whom, when logged on locally, can shut down the computer.

Synchronize directory service data - Not defined in template

Take ownership of files or other objects - Administrators
This shows who may take ownership of any securable object in the system.

Security Options
Policy - Computer Setting
Additional restrictions for anonymous connections
(No access without explicit anonymous permissions)
Prevent anonymous connections from finding out domain accounts and shares.

Allow server operators to schedule tasks - Not defined in template

Allow system to be shut down without having to log on Disabled
This causes the **Shut Down** button to appear on the Windows logon screen. This should be disabled to prevent unauthorized users or authorized users from casually clicking a button to shut down the server with no audit trail of who did it. Authorized users may make the mistake of not reading the buttons and accidentally choose it.

Allowed to eject removable NTFS media - Administrators
This lists who is allowed to eject NTFS formatted media. CD-RWs are not NTFS media.

Amount of idle time required before disconnecting session - 30 minutes
This is the number of idle minutes that must pass in a Server Message Block session before the session is disconnected due to inactivity.

Audit the access of global system objects – Enabled
When enabled, system objects such as semaphores, and DOS Devices will be created with a default system access control list (SACL) that will record when accessed.

Audit use of Backup and Restore privilege - Enabled
When enabled, use of just the Backup and Restore rights will be written to the security log.

Automatically log off users when logon time expires (local) – Enabled
If logon hours are set for an account, this setting will cause client sessions with the SMB server to be forcibly disconnected when users exceed those hours.

Clear virtual memory pagefile when system shuts down – Enabled
This will clears all pagefiles at shutdown preventing someone from reading old data contained therein if booted with a floppy or other operating system.

Digitally sign client communication (always) - Disabled
This will prevent man-in-the-middle attacks. It does this by providing authentication using a digital signature in each SMB. However, it does cause CPU overhead.

Digitally sign client communication (when possible) – Enabled
If both the client and server can support SMB packet signing, then they will.

Digitally sign server communication (always) – Disabled
On the server, only allow the SMB server to use SMB packet signing.

Digitally sign server communication (when possible) – Enabled
On the server, allow the SMB server to use SMB packet signing if the client supports it.

Disable CTRL+ALT+DEL requirement for logon –Disabled
Asks if the user should be required to press CTRL+ALT+DEL before a user can log on. This will prevent back door programs from stealing logon ids and passwords.

Do not display last user name in logon screen – Enabled
When enabled, the name of the last user to successfully logon is not displayed in the **Log On to Windows** dialog box. This is good for security in that a person trying to break in will have to first find the user account and then the password.

LAN Manager Authentication Level – (Send NTLMv2 response only\refuse LM & NTLM)
Prevent the weaker challenge/response protocols of LM & NTLM.

Message text for users attempting to log on - Not defined in template
We will set this to be the same as the screen saver.

Message title for users attempting to log on- Not defined in template

Number of previous logons to cache (in case domain controller is not available) - 0 logons
In case a domain controller cannot be located, this setting would store a previous user's logon information locally to allow them to logon. A value of 0 disables all caching.

Prevent system maintenance of computer account password – Disabled
When enabled, a new computer account password will not be generated every week. The default setting is disabled so that a new account password will be generated every week.

Prevent users from installing printer drivers – Enabled
When enabled, this policy will prevent users from installing print drivers, which may cause system problems.

Prompt user to change password before expiration - 14 days
Windows 2000 will warn users that their password will expire. They will begin receiving this message this many days prior to the expiration.

Recovery Console: Allow automatic administrative logon –Disabled
When enabled, the recovery console will not ask for an administrative password to log on the system. Disabling this will cause the recovery console to ask for a password.

Recovery Console: Allow floppy copy and access to all drives and all folders - Disabled
This allows the setting of 4 different environment variables that could compromise the server. **AllowAllPaths** is one of those variables that when set would allow access to all files and folders. This should be disabled.

Rename administrator account - Not defined in template

Rename guest account - Not defined in template

Restrict CD-ROM access to locally logged-on user only – Enabled
When enabled, the user who is logged on locally can use the CD-ROM and prevent network users from using it. However, after they logoff, the CD-ROM may be shared over the network. This setting may come into use if the CD-ROM's power connector is plugged back in. The power connector was removed from the CD-ROM drive after installing the operating system.

Restrict floppy access to locally logged-on user only – Enabled
When enabled, the user who is logged on locally can use the floppy and prevent network users from using it.

Secure channel: Digitally encrypt or sign secure channel data (always) – Disabled
When disabled, signing and encryption are negotiated with the domain controller. This option should only be enabled when all domain controllers in all trusted domains support encrypted and signed data.

Secure channel: Digitally encrypt secure channel data (when possible) - Enabled
When enabled, all outgoing secure channel traffic *should be* encrypted.

Secure channel: Digitally sign secure channel data (when possible) – Enabled
When enabled, all outgoing secure channel traffic should be signed.

Secure channel: Require strong (Windows 2000 or later) session key – Disabled
When disabled, they key strength will be negotiated with the domain controller authenticating it.

Send unencrypted password to connect to third-party SMB servers – Disabled

If there are third-party SMB servers, send passwords to them in cleartext.
This is disabled to stop this practice.

Shut down system immediately if unable to log security audits – Enabled
This setting has the benefit of keeping an excellent audit trail. However, the event logs must be properly sized or someone attempting to logon could create a denial of service attack by forcing the computer to blue-screen.

Smart card removal behavior - Lock Workstation
If a smart card is used, and if it is removed, the computer will lock.

Strengthen default permissions of global system objects (Symbolic Links) - Enabled
When enabled, the default DACL is stronger, preventing the non-admin users from modifying shared objects but allowing them to read them.

Unsigned driver installation behavior -Warn but allow installation
This is how installing an unsigned driver is treated.

Unsigned non-driver installation behavior - Warn but allow installation
This is how installing an unsigned non-driver is treated.

Event Log

Policy - Setting
Maximum application log size 4194240 kilobytes
4GB is the maximum size for the application event log to grow to.
Be aware that performance problems could result if the event log fills the entire disk that the boot files are on.

Maximum security log size 4194240 kilobytes
4GB is the maximum size for the security event log to grow to.
Be aware that performance problems could result if the event log fills the entire disk that the boot files are on.

Maximum system log size 4194240 kilobytes
4GB is the maximum size for the system event log to grow to.
Be aware that performance problems could result if the event log fills the entire disk that the boot files are on.

Restrict guest access to application log - Enabled
When enabled, guests cannot access the application log.

Restrict guest access to security log - Enabled
When enabled, guests cannot access the security log.

Restrict guest access to system log - Enabled
When enabled, guests cannot access the system log.

Retain security log – Not defined in template
The number of days to keep the security log before it is overwritten with newer events.

Retention method for application log - Manually
When the log is full, how should new events be handled?
Overwrite events as needed, overwrite events by days, do not overwrite – clear the log manually.

Retention method for security log – Manually
When the log is full, how should new events be handled?
Overwrite events as needed, overwrite events by days, do not overwrite – clear the log manually.

Retention method for system log – Manually
When the log is full, how should new events be handled?
Overwrite events as needed, overwrite events by days, do not overwrite – clear the log manually.

Shut down the computer when the security audit log is full – Enabled
This will prevent a hacker from covering their tracks by shutting the operating system down upon filling up the log.

Restricted Groups

Group Name	Members	Member Of
Administrators	Not defined	Not defined
Backup Operators	Not defined	Not defined
Guests	Not defined	Not defined
Power Users	OK	OK
Replicator	Not defined	Not defined
Users	Not defined	Not defined

This section of the template allows for the management of groups into two categories Members and Members of. Members refers to those users that are supposed to be included in the group. If an account was in a restricted group prior to the policy, but is not listed in the restricted group's member list in the policy, he/she will removed when group policy is refreshed. Thus membership is maintained.

System Services

No services are defined in the template. It was described in the documentation that this was done on purpose so that this could be customized on a case by case basis. Stefan Norberg's book Securing Windows NT/2000 Servers[6] Chapter 3 – "Building a Windows 2000 Bastion Host" lists the bare minimum number of services that need to run to host an application such as a database or IIS. However, when told that shutting down the 'server service' would prevent Mrs. Smart from attaching to a share and copying backups, the idea of disabling a number of these services was turned down.

Registry

The template does further strengthen the access control to certain registry settings to further strengthen the IP stack as well as other objects.

File System

The template includes 58 lines to further strengthen the default settings of the various files and directories on the server including but not limited to: Regedt32, ntbackup, regedit, along with a number of files in the root directory of the system drive

Deployment

There are two ways to deploy the NSA security template, either through the Security Configuration and Analysis MMC snapin or with a command line program. The command line program was chosen because of the easy log trail it can create. The program is called SECEDIT.EXE. It can be called from within a windows scripting host program or from within a command file. The syntax can be obtained by opening up a command prompt and typing in SECEDIT /? and following the link for HOW TO. To apply the NSA template, a command file was written to analyze and configure the template settings as per the documentation. The command file looked like this:

```
@echo off
rem ********
rem
rem this command file will apply the NSA server template
rem to the database server
rem
rem see the .log files for results
rem
rem ********
echo Analyzing...
secedit /analyze /DB test.db /CFG C:\WINNT\security\templates\NSA_w2k_server.inf /log
%computername%_nsa_anal.log  /verbose

echo Configuring...
secedit /configure /DB test.db /CFG C:\WINNT\security\templates\NSA_w2k_server.inf /log
%computername%_nsa_config.log  /verbose
```

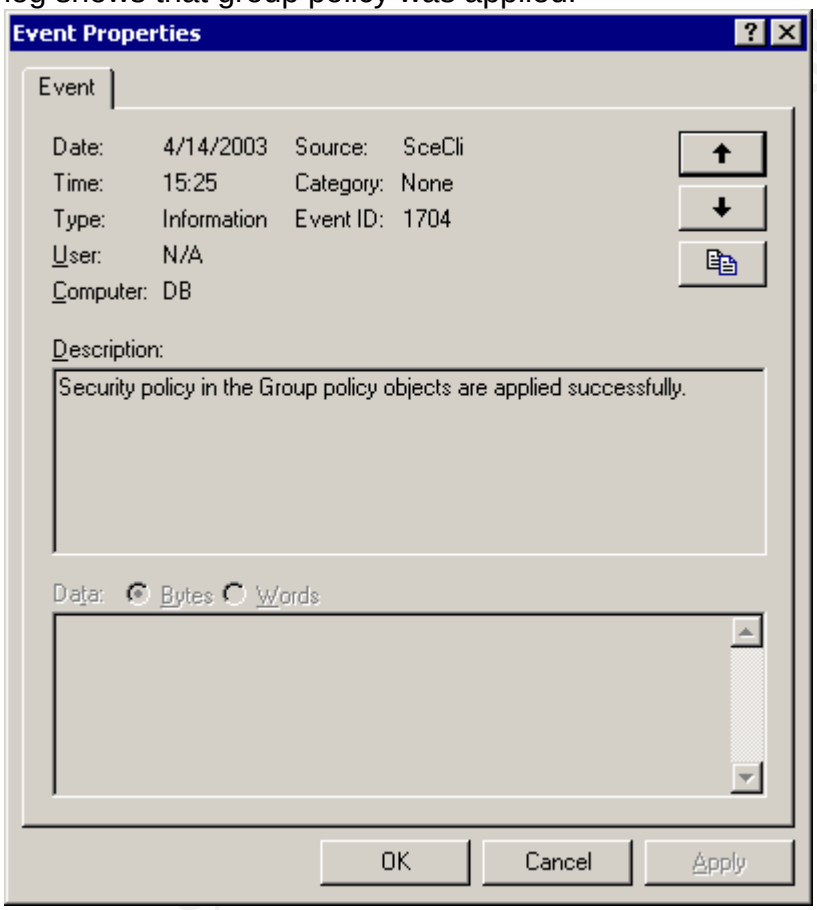
```
echo Done.
```

The two logs were reviewed for errors.

Testing the OS template

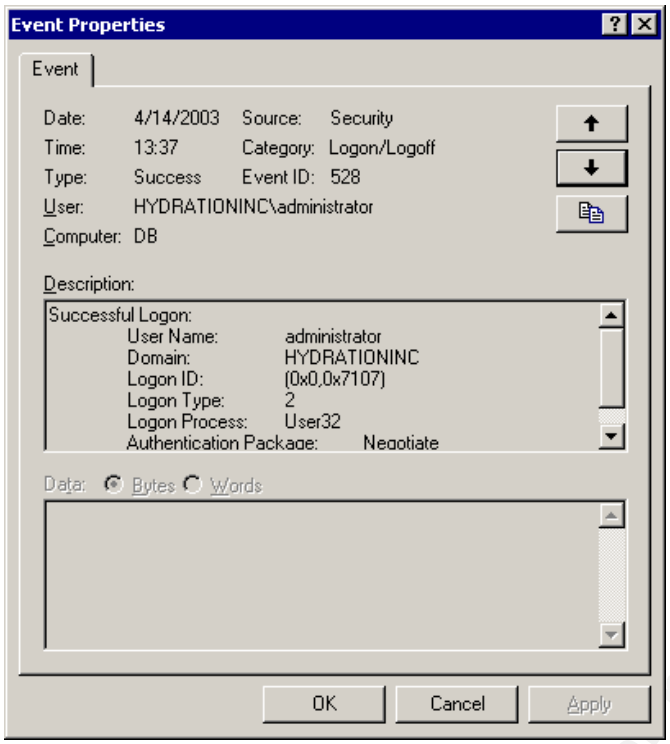
An important feature of this template is that it rejects local logons. This prevents Dr. Smart's son from logging on the server and installing games. Unfortunately the screen shot for this could not be obtained due to the need to logon to run the program.

The group policy template is believed to have been applied because the event log shows that group policy was applied.

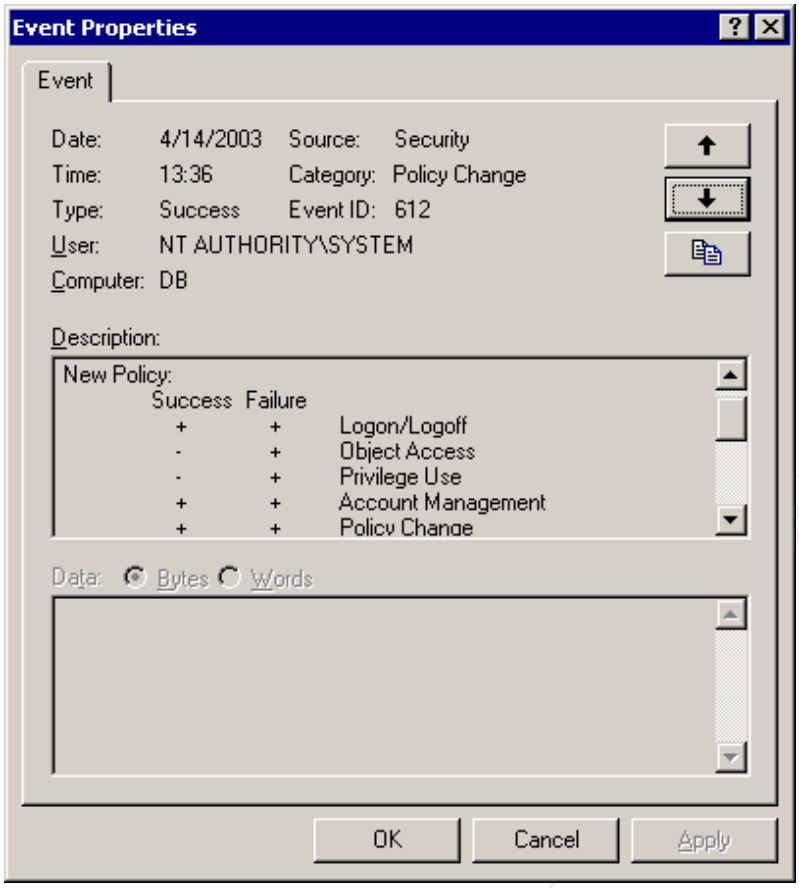


Local Policies

To verify that local policies have been processed, the event log was checked to see to see if the administrator logon and logoff events were captured. They were.

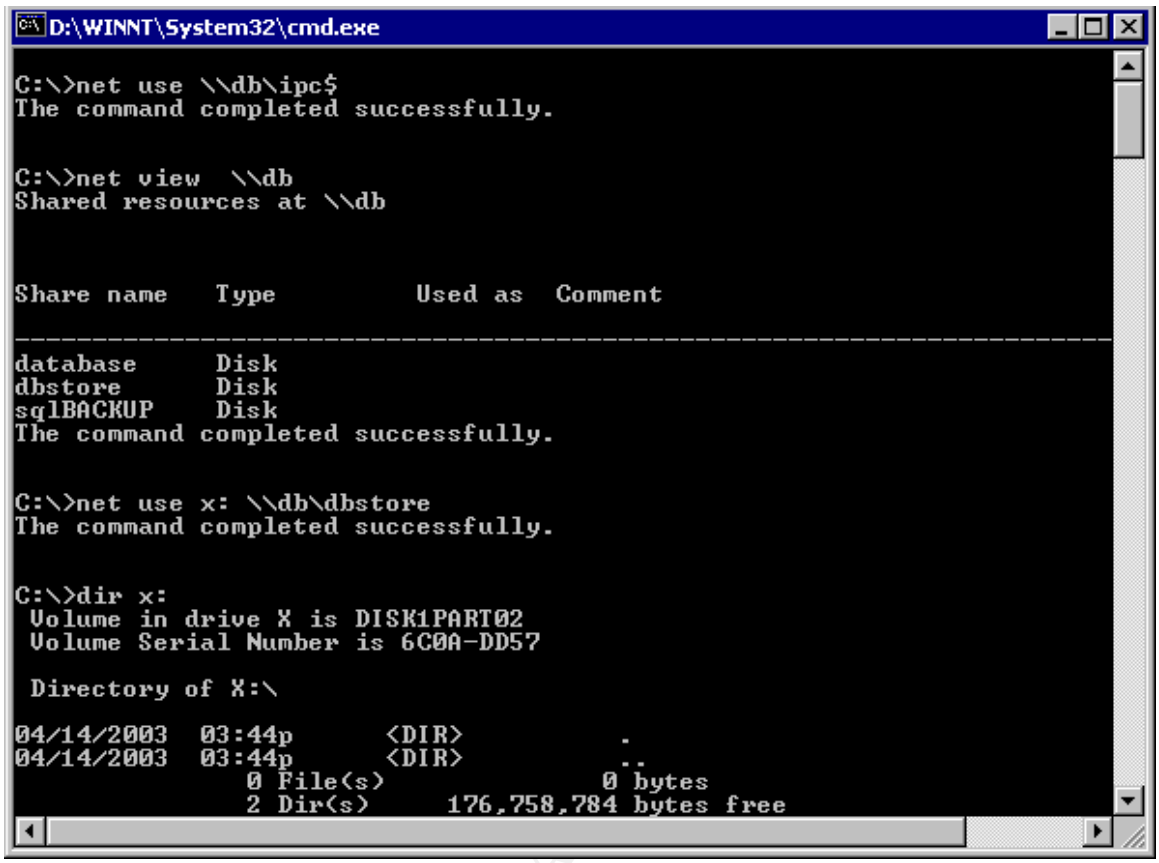


Reapplying the template is also logged.

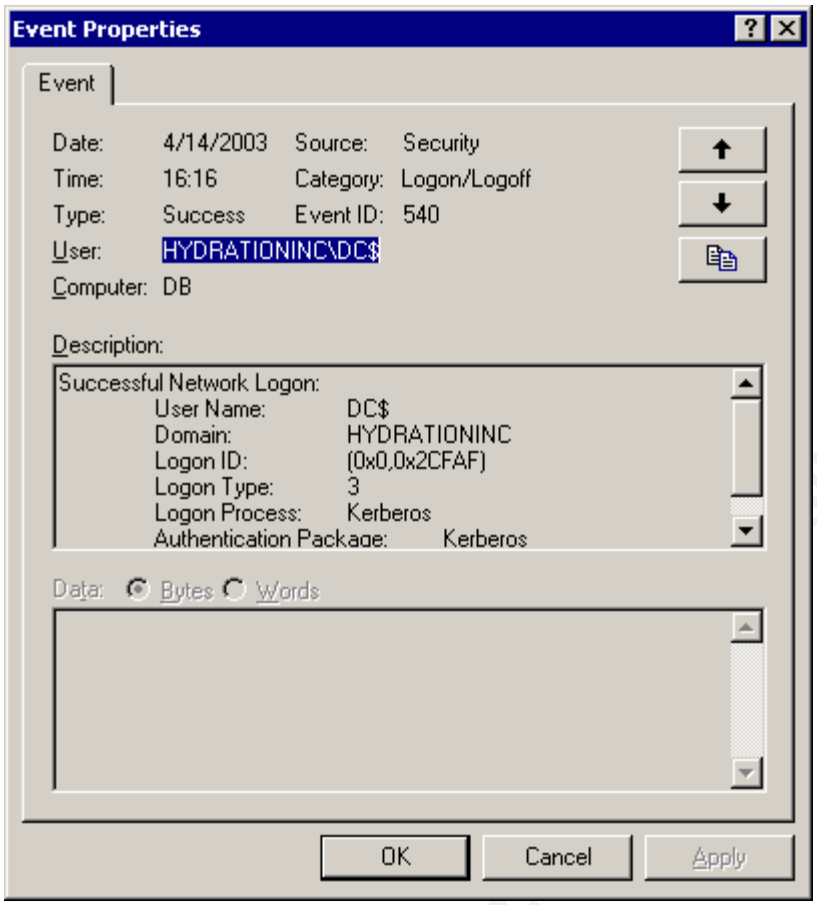


Audit Policies

1. To check if network connections are being audited, Mrs. Smart logged in and connected to the database server's backup directory share.

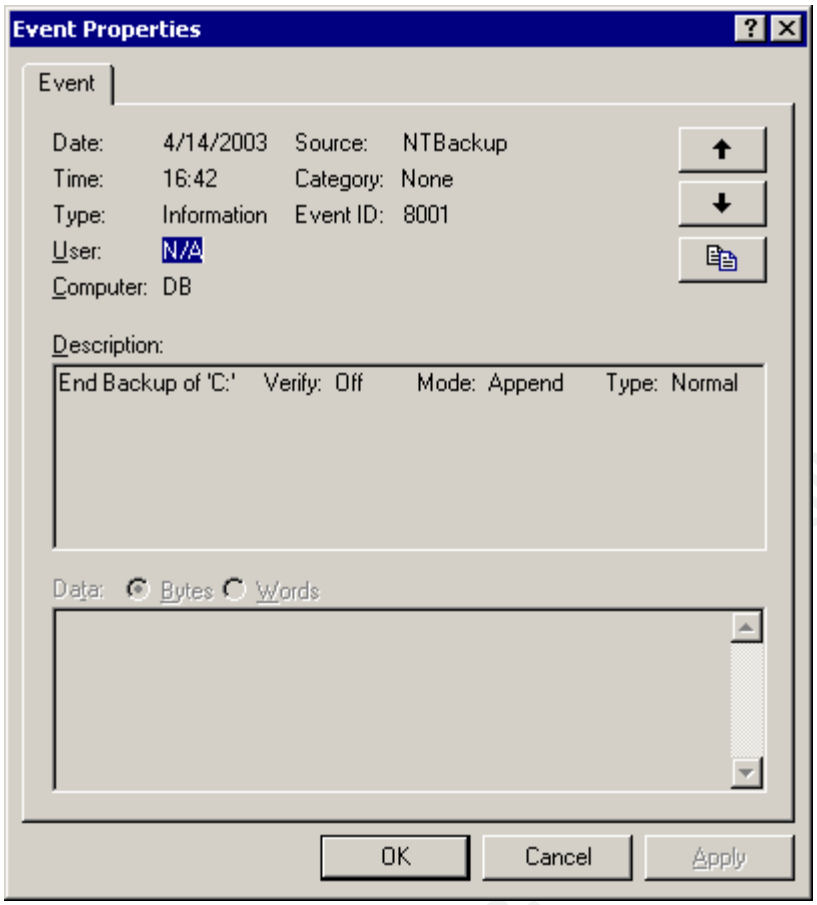


2. The event log on the database server was then examined to see if the access was recorded.



3. It should be noted that Mrs. Smart was on the Domain Controller at the time.

Because the use of backup and restore privileges is audited, the NTBACKUP program was run to create an emergency repair disk as well as to backup files. Surprisingly, the creation of the repair disk did not show up in the event log – the backup did as the template indicates.



Evaluation of OS Template

The NSA server template provides a good starting point in securing a server. However, it should be noted that it still needs to be enhanced. Specifically, certain services should be disabled if they are not needed. The OS/2 and Posix subsystems will not be used and should be dropped both in the registry and the DLLs that make them up. Default administrative shares can also be removed. As this server will only be used on the internal network, either IP filters or IPSEC should be loaded to limit the ports that are listened to.

However, success must be measured by on two counts: Did it satisfy the owner who was paying us to secure his system and will it stand up to those threats we were trying to defend against? On the first point, the answer is yes. On the second, the answer is only a maybe. The reason being that every avenue of exploitation was not pursued in tightening down the server. Automated tools could have been brought in to help as well. More file and registry tweaking could have done to prevent not just authorized users but specific users on an individual basis. However, as this is not a server that is left as a honeypot on the open

internet but is behind a firewall, the settings using the NSA template are reasonable.

Database Checklist Selection

To insure that the database holding the company's data is secure, the checklist created by Chip Andrews from his website at http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4 and the corresponding SQL script written by him will be used to secured the SQL Server 2000 database. Both the script and checklist are considered a valuable tool as they present in a concise form the steps needed to secure a database. Mr. Andrew's checklist was picked over several other checklists due to his extensive background in database security. Mr. Andrews has given several talks on SQL Security at the Black Hat briefings[7] and has also contributed the SQL Server chapter to the recently released book "Hacking Exposed: Windows 2000" (Scambray, McClure) by Osborne Press[8].

However, like the operating system templates, his is not the only one available. Other smaller checklists on the Internet exist such as the one by Brian Knight http://www.sqlservercentral.com/columnists/bknight/10securingyoursqlserver.asp (free registration required)
A larger one written by Chris Kempster is found at, http://www.sqlservercentral.com/columnists/ckempster/sql_server_security.asp and another short one written by Stephen V. Arehart is found here: http://www.zone-h.org/files/13/sql_security.htm.
Of course, Microsoft has a very detailed and exhaustive one written by Richard Waymire and Ben Thomas at http://www.microsoft.com/sql/techinfo/administration/2000/2000SecurityWP.doc
Mr. Andrews checklist provides an excellent starting point and includes a SQL script to help implement it.

Installation of SQL Server 2000 database

Installing SQL Server is easy. Installing it securely in a domain is more difficult. This portion of the paper will outline the steps needed to install and secure the database. Two accounts will need to be created for database service to use. The software will need to be installed under one of those accounts. SQL Server Service Pack 3 is the most current service pack at the time of this writing and will need to be applied. Then the lock-down script will be run. Finally, the log on locally user right will be removed from the SQL Server account that is needed for installation only. Testing will then be performed to insure that everything works and is secure.

Pre installation steps

Because SQL Server is an application running as a service under Windows 2000, it needs to run under an account with the appropriate permissions. Because it must be installed while logged on either as the administrator or with and account in the administrator group, some people choose to run it under the administrator group. However, this could be considered inappropriate in that it violates the principle of least privilege. One could also run it under the local system account, but this would prevent using replication or having it perform database backups across the network. By installing it under a domain account, you have the benefit of utilizing replication to other servers as well as backup to other servers if necessary.

The initial premise was that after installation, the SQL Server service account could be removed from the administrators group. While the service ran perfectly well in this mode, the lockdown script could not write to the registry. This could be construed as a good thing as you normally don't want to write to the registry. However, in order to fully test the lockdown script, the SQL Server service account was left as a member of the local administrators group. Further investigation must be made as why this needed to be.

For this installation, two accounts will be used: one for SQL Server itself, and the other for SQL Agent – a valuable add-on that performs job scheduling similar to Task Scheduler but is highly integrated with SQL Server.

To create both accounts, on a domain controller, go to Start, Programs, Administrative Tools, Active Directory Users and Computers. Right click on Users, select New, and pick User. Type in the name you wish for the SQL Server service account. Type in the name "S Smith" for the SQL Server Service and "B Smith" for the SQL Server Agent service. This way, people will not be able to guess which accounts are used to run the SQL Server service.

Remove the check box for "User must change password at next logon". Check the two boxes "User cannot change password" and "Password never expires". This will be the account that SQL Server will logon with. Press the Create Button.

Although the accounts used are automatically assigned the appropriate privileges during the installation process, the SQL Server account should be granted the following user rights according to Microsoft knowledge base article Q283811:

1. Act as Part of the Operating System = SeTcbPrivilege
2. Bypass Traverse Checking = SeChangeNotify
3. Increase Quotas = SeIncreaseQuotaPrivilege
4. Lock Pages In Memory = SeLockMemory
5. Log on as a Batch Job = SeBatchLogonRight
6. Log on as a Service = SeServiceLogonRight

7. Replace a Process Level Token = SeAssignPrimaryTokenPrivilege

Because this is part of a domain, and we want the functionality of backing up to and restoring from network drives, it must be a domain account and not a local system account.

The SQL Agent only needs these 5 user rights:

1. Act as Part of the Operating System = SeTcbPrivilege
2. Increase Quotas = SeIncreaseQuotaPrivilege
3. Log on as a Batch Job = SeBatchLogonRight
4. Log on as a Service = SeServiceLogonRight
5. Replace a Process Level Token = SeAssignPrimaryTokenPrivilege

A point needs to be made here on what domain. Typically, the database server should not be part of the same network as the users but segregated into a network DMZ. It should then make up its own domain. Because of the small size of this company, this concession to best security practices will be made and it will not be segregated.

To set these permissions, go to Start, Programs, Administrative Tools, and Domain Security Policy. Expand the Local Policies, and click on User Rights Assignment.

Grant the SQL Server service account the above 7 user rights and the SQL Server Agent the 5 user rights. For HydrationInc, those accounts will be Ssmith for SQL Server and Bsmith for SQL Agent.

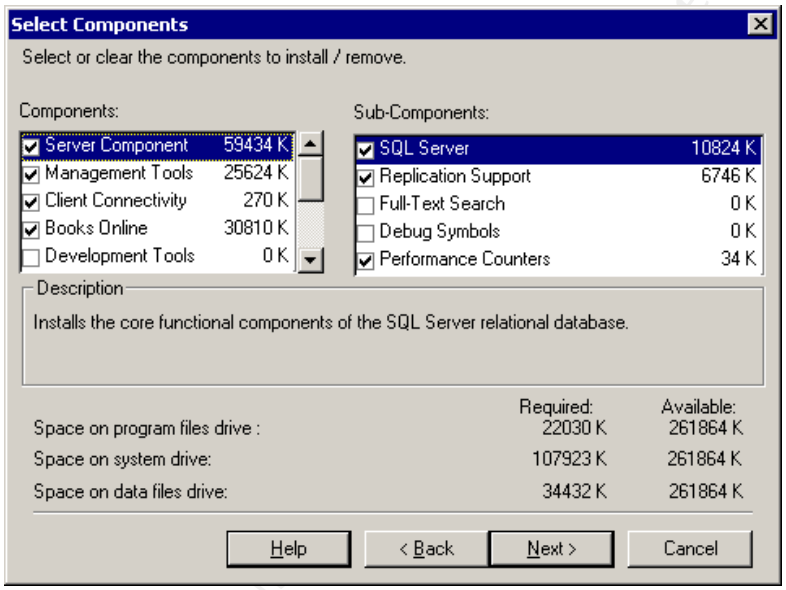
Temporarily, two other steps need to be taken. SQL Server can only be installed if the logged on user is an administrator either of the local machine or of the domain. Therefore, on the local machine, open up Computer Management from the Administrative Tools folder and add both accounts to local Administrators group. Also, grant the Log On Locally right to it as well. After everything is installed, the log on locally right will be removed.

Logon to the database server with the account that will run the SQL Server service. In our case, that would be SSmith.

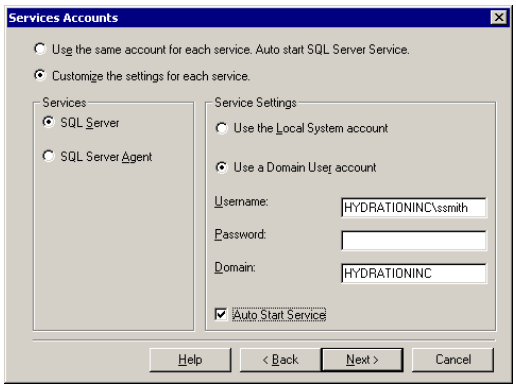
SQL Server installation steps

1. Insert the SQL Server CD-ROM.
2. Choose to install SQL Server 2000 Components.
3. Click on install the Database Server.
4. Choose to install to a local computer from the computer name screen.

5. From the Installation Selection, choose to create a new instance of SQL Server.
6. At the User information screen, enter an appropriate name and company name.
7. Select Yes on the license agreement screen.
8. On the Installation Definition screen, choose to install both Server and Client tools.
9. On the Instance Name Screen, choose to install to the Default instance.
10. At the Setup Type Screen, choose the Custom installation option button.
    - There will be two buttons for the Destination Folders
    - Press the Program Files button and change the drive letter off of the boot disk. For HydrationInc, this will be drive E:.
    - Press the Data Files button and change it to F:\dbstore or some innocuous name that won't draw attention
11. On the Select component screen, uncheck development tools and uncheck Full-text Search and Debug Symbols.



12. Use the two accounts created earlier for running the services under. Below is a screen shot of how to type in the account.



13. The authentication method must now be chosen. SQL Server offers the legacy mixed mode or Windows Authentication. With mixed mode, you have to assign and control passwords. SQL has no method to force users to change passwords in this mode however. This is also the source of attacks on SQL Server. Since there are no legacy programs in use at HydrationInc, it will not be needed. Windows Authentication Mode will be picked.
14. Accept the default collation set.
15. On the Network Libraries screen, it will ask you what network libraries to allow clients to connect to the database with. The defaults of Named Pipes and TCP/IP are fine. Change the default port on the IP sockets to be anything but 1433, the default. This won't stop the dedicated hacker but will impede the casual browser from using some automated tools.
16. For the licensing Mode, choose the model that the company paid for, either per processor or per seat.

After installation, the directories where SQL Server was installed are secured. The program files directory, "E:\Program Files\Microsoft SQL Server\MSSQL" has on its directory permissions, Administrators (DB\Administrators), B smith (Bsmith@HydrationInc.US), and s smith(ssmith@HydrationInc.US). This is secure.

From the database server, shutdown, restart and log in as the administrator. Remove the user right: "Logon Locally" from SSmith.

After SQL installs, the SQL Server service account has access to the directories. You should also remove the "everyone" group privilege from the SQL Server program directories E:\Program Files\Microsoft SQL Server.

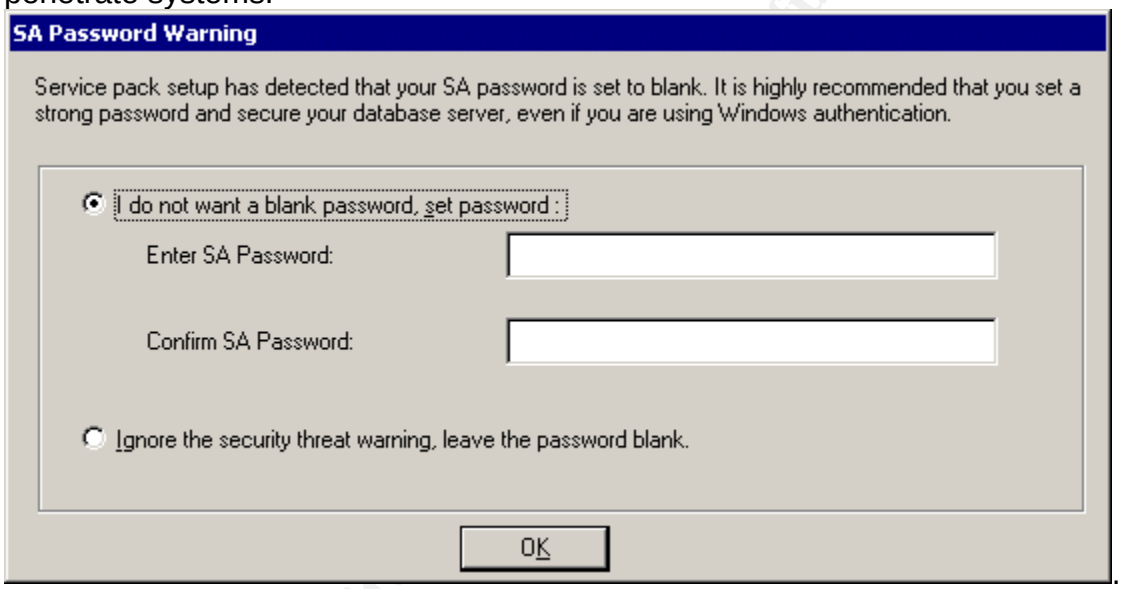
To see that the database is installed correctly, from a command prompt type in:

```
ISQL.EXE  –E –S127.0.0.1
1> select getdate()
2> go
```

After typing in the word go and pressing enter, you should see the current date displayed. Type in Exit to quit.

```
1>exit
```

At this point there is a tremendous security hole. There exists 1 account called 'SA' that has god-like powers. By default after install, it has no password. Some exploits rely on the fact that the password is not set on install. However, SQL Server service pack 3 remedies this by prompting you to enter a password if one is not already assigned. This is how the 'Spida' or SQLworm[9] was able to penetrate systems.



Service pack 3 for SQL Server 2000 should now be applied and the server rebooted.

At this point, the database is ready to be used. However, further steps can be taken to insure a more secure environment, the following document was obtained from http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=3&tabid=4
The lock down transact-sql script was obtained from
http://www.sqlsecurity.com/scripts/lockdown.sql

The lockdown transact-sql script is the implementation of the steps recommended in the document. Please note that the following 11 pages are a duplicate from Chip Andrews SQLSECURITY.COM website and is not the work of the author.

Beginning of Document
****

Database Checklist Settings

SQLSecurity Checklist by Chip Andrews

http://www.sqlsecurity.com

1. **Make sure the latest OS and SQL Server Service Packs/Hot-Fixes are applied.** This goes without saying but I'll say it anyway for completeness. The following table should help you track down the out-of-date servers. Simply perform a "select @@version" on your SQL Server and compare the results to this table.

Version	Patch Level
8.00.760	2000 SP3
8.00.679	2000 SP2+Q316333
8.00.667	2000 SP2+8/14 fix
8.00.665	2000 SP2+8/8 fix
8.00.655	2000 SP2+7/24 fix (Q323875) *SQLSlammer worm vuln fixed here
8.00.650	2000 SP2+Q322853
8.00.608	2000 SP2+Q319507
8.00.604	2000 SP2+3/29 fix
8.00.578	2000 SP2+Q317979
8.00.561	2000 SP2+1/29 fix
8.00.534	2000 SP2.01
8.00.532	2000 SP2
8.00.475	2000 SP1+1/29 fix
8.00.452	2000 SP1+Q308547
8.00.444	2000 SP1+Q307540/307655
8.00.443	2000 SP1+Q307538
8.00.428	2000 SP1+Q304850
8.00.384	2000 SP1
8.00.287	2000 No SP+Q297209
8.00.250	2000 No SP+Q291683
8.00.249	2000 No SP+Q288122
8.00.239	2000 No SP+Q285290
8.00.233	2000 No SP+Q282416
8.00.231	2000 No SP+Q282279
8.00.226	2000 No SP+Q278239
8.00.225	2000 No SP+Q281663
8.00.223	2000 No SP+Q280380
8.00.222	2000 No SP+Q281769
8.00.218	2000 No SP+Q279183
8.00.217	2000 No SP+Q279293/279296
8.00.211	2000 No SP+Q276329
8.00.210	2000 No SP+Q275900
8.00.205	2000 No SP+Q274330
8.00.204	2000 No SP+Q274329
8.00.194	2000 No SP
8.00.190	2000 Gold, no SP
8.00.100	2000 Beta 2
8.00.078	2000 EAP5
8.00.047	2000 EAP4

(entries deleted for earlier SQL versions)
(Special Thanks to Ken Klaft for maintaining this list)

2. **Evaluate and choose a network protocol library that allows for maximum security but doesn't break functionality.** Since SQL Server 2000 it's becoming increasingly obvious that Microsoft intends TCP/IP to be the net-lib of choice. The question now is really whether to use SSL for SQL Server access or not.
3. **Secure the "sa" and "probe" (SQL 6.5) accounts with strong passwords.** Assign a strong password and lock away the password in a secure location. Note: The probe account is used for performance analysis and distributed transactions. Assigning a password to this account can break functionality when used in standard security mode.
4. **Use a low-privilege user account for SQL Server service rather than LocalSystem or Administrator.** This account should only have minimal rights (note that Run as a Service Right will be required) and should help contain (but not stop) an attack to the server in case of compromise. Notice that when using Enterprise Manager to make this change, the ACLs on files, the registry, and user rights are done for you automatically.
5. **Make sure all SQL Server data and system files are installed on NTFS partitions and the appropriate ACLs are applied.** If someone should gain access to the OS, make sure that the necessary permissions are in place to prevent a catastrophe.
6. **Restrict to sysadmins-only access to stored procedures and extended stored procedures that you believe could pose a threat.** There are quite a few of them, and this could take some time. Be careful not to do this on a production server first. Test on a development machine so you don't break any functionality. Below is a list of the ones we recommend you assess:

sp_sdidebug	xp_perfend
xp_availablemedia	xp_perfmonitor
xp_cmdshell	xp_perfsample
xp_deletemail	xp_perfstart
xp_dirtree	xp_readerrorlog
xp_dropwebtask	xp_readmail
xp_dsninfo	xp_revokelogin
xp_enumdsn	xp_runwebtask
xp_enumerrorlogs	xp_schedulersignal
xp_enumgroups	xp_sendmail
xp_enumqueuedtasks	xp_servicecontrol
xp_eventlog	xp_snmp_getstate
xp_findnextmsg	xp_snmp_raisetrap
xp_fixeddrives	xp_sprintf
xp_getfiledetails	xp_sqlinventory
xp_getnetname	xp_sqlregister
xp_grantlogin	xp_sqltrace
xp_logevent	xp_sscanf
xp_loginconfig	xp_startmail
xp_logininfo	xp_stopmail
xp_makewebtask	xp_subdirs
xp_msver	xp_unc_to_drive
xp_regread	xp_dirtree

7. **Disable Default Login under "Security Options" in Enterprise Manager (SQL 6.5 only).** When using Integrated security, this keeps unauthorized users from accessing the server without a valid entry in the syslogins table.
8. **Remove the Guest user from databases to keep unauthorized users out.** The exception to this is the master and tempdb databases as the guest account is required.
9. **Disable SQL Mail capability unless absolutely necessary.** Leaving it open gives a potential attacker another means of delivering potential trojans, viruses, or simply launching a particularly nasty denial of service attack.
10. **Check master..Sp_helpstartup for trojan procedures.** Make sure no one has placed a backdoor here. Use Sp_unmakestartup to remove any rogue procedures.
11. **Check master..Sp_password for trojan code.** Compare your production scripts to the default script on a fresh installation and keep that code handy.

12. **Enable logging of all user access. Do this from Enterprise Manager or by entering the following into the Query Analyzer as a SQL system administrator:**

xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer',N'AuditLevel', REG_DWORD,3

Before the drop the procedure of course ;-]

13. **Rewrite applications to use more user-defined stored procedures and views so general access to tables can be removed.** You should also see some performance improvement here as query execution plans won't be performed as often.
14. **Remove unneeded network protocol libraries.**
15. **Physically secure the SQL Server.** Lock it behind a door and lock away the key while you're at it. Someone sitting in front of the server will always find a way.
16. **Set up a scheduled task to run:**

findstr /C:"Login Failed" \your_sql_path\log*.*'

and redirect to the output to a text file or email so you can monitor failed login attempts. This also provides a good way for administrators to document attacks. There are also many third-party tools for analyzing NT event logs. Note: You may need to change the path for the log files based on your installation and SQL Server version.

17. **Set alerts to log failed object access and logins.** Go to "Manage SQL Server Messages" in Enterprise Manager and search for any messages relating to permission denial (start by searching for "Login Failed" or "denied"). Make sure any messages you're interested in are logged to the event log. Next, set up an alert on that message or severity level 14 to send an email or page to an operator who can quickly react to the issue.
18. **Make sure roles at the server and database levels are only assigned to the users who need them.** While the SQL Server 7 security model has many enhancements, it also adds the extra layer of permissions that we must monitor to make sure no one has been given more access than they need or that they've already circumvented security to elevate themselves.
19. **Frequently check group or role memberships and make sure to assign permissions by group so your auditing tasks can be simplified.** Make sure the public group can't issue SELECT statements against system tables while you're at it.

20. **Take the time to audit for logins with null passwords.** Use the following code to check for null passwords:

```
Use master
Select name,
Password
from syslogins
where password is null
order by name
```

21. **Make use of Windows Authentication Mode for security if feasible in your organization.** By using integrated security, you can greatly simplify administration by relying on the OS security and saving yourself from maintaining two separate security models. This also keeps passwords out of connection strings.
22. **Regularly check access permissions for all non-"sa"s on stored procs and extended stored procs.** Use the following query to periodically query which procedures have public access: (Use "type" instead of "xtype" for SQL 6.5):

```
Use master
Select sysobjects.name
From sysobjects, sysprotects
Where sysprotects.uid = 0
AND xtype IN ('X','P')
AND sysobjects.id = sysprotects.id
Order by name
```

23. **Use integrated security when accessing Enterprise Manager.** In the past, Enterprise Manager has been found to store the “sa” password in plaintext in the registry when in standard security mode. Note: Even if you change modes, the password remains in the registry. Use regedit and check this key:

    HKEY_CURRENT_USER\SOFTWARE\Microsoft\ MSSQLServer\SQLEW\Registered Server\ SQL 6.5

Currently the data is buried (and apparently encrypted although I have not taken a long hard look) in

HKEY_USERS\{yourSID}\Software\Microsoft\Micro soft SQL Server\80\Tools\SQLEW\Registered Servers X\SQL Server Group

(The "SQL Server Group" is the default but you may have created custom groups so change the location accordingly)

24. **Develop an audit plan and make monthly security reports available to IT administration that includes any new exploits, successful attacks, backup storage protection, and object access failure statistics.**
25. **Never allow users to log on to the SQL Server interactively.** This tip goes for any server. Once a user can interactively log into a server, there are myriad of privilege escalation attacks that can be used to obtain Administrative access.
26. **Do your best to limit ad-hoc access to the SQL Server.** There are many things a user can query inside the SQL Server even with minimal privileges. Don't give them the chance if you don't have to.

End of document

To help implement the checklist, the following is a set of Transact-SQL statements that are from the Chip Andrews site as well.[10] The font has been changed to indicate that this is Transact-SQL code.

Beginning of lockdown script
****

```
--SQL Server 2000 Lockdown Script
```

```
--by Chip Andrews (www.sqlsecurity.com)
--12/23/2002
--
--The purpose of this script is to provide administrators (SQL Server or otherwise) a baseline
--lockdown configuration for new installations.  These settings should disable potentially dangerous
--functionality while leaving the server operational and still capabable of Service Pack and hotfix
--installations.  Feel free to provide feedback at www.sqlsecurity.com if you find any issues or
--have any suggestions for improvement.
--
--Project Goals:
--    * Must support named instances
--    * Must not break future Service Pack and hotfixes installations
--    * Must strive to disable rarely used functionality but not break common applications (80-20 rule)
--    * Must be easily runnable from the command prompt for mass distribution
--
--Notes:
--
--*You will note that no Extended Stored Procedures have been dropped in the script.  This is due to several reasons:
--  1.  It causes some problems with Service Packs and hotfix installations when certain functions are disabled
--  2.  Blocking access to non-sysadmin users is more easily achieved by dropping execute permissions
--  3.  Sysadmins can easily add them back so dropping them really serves no real purpose
--*The last script item has been commented out because it effectively blocks all network access to the SQL Server
--  and thus violates the 80-20 rule.  Feel free to enable it for local-only SQL Server installs.
--
--
SET NOCOUNT ON
PRINT '*** Begin SQL Server 2000 Lockdown Script v1.0 ***'
PRINT ''
PRINT 'SERVER NAME : ' + @@SERVERNAME
PRINT ''
--
--
--Check SQL Server Service Account for LocalSystem Authority - Send warning
--It should be noted that it may be possible to create a local account if LocalSystem is found
--and alter the service account here in the script.  However, since there are also file ACL and registry
--permissions to deal with then its probably best left to the Enterprise Manager to do this.
CREATE TABLE #user (value VARCHAR(50), data VARCHAR(50))
IF (charindex('\',@@SERVERNAME)=0)
        INSERT #user EXEC master..xp_regread 'HKEY_LOCAL_MACHINE'
,'SYSTEM\CurrentControlSet\Services\MSSQLSERVER','ObjectName'
ELSE
        BEGIN
                PRINT 'Note: SQL Server was determined to be a named instance'
                PRINT ''
                DECLARE @RegistryPath varchar(200)
                SET @RegistryPath = 'SYSTEM\CurrentControlSet\Services\MSSQL$' +
RIGHT(@@SERVERNAME,LEN(@@SERVERNAME)-CHARINDEX('\',@@SERVERNAME))
                INSERT #user EXEC master..xp_regread 'HKEY_LOCAL_MACHINE' ,@RegistryPath,'ObjectName'
        END
SELECT TOP 1 DATA AS [SQL Server Service Account] FROM #USER
IF (SELECT TOP 1 DATA FROM #user)='LocalSystem'
        PRINT '*** ALERT LOCALSYSTEM AUTHORITY BEING USED FOR SQL SERVER SERVICE ACCOUNT IS
NOT RECOMMENDED. ***'
DROP TABLE #user
PRINT ''
--
-- Confirm the latest service pack and hotfixes have been applied by selecting
-- the server version and comparing it to the most current SQL Server
-- version (at the time of writing that was 8.00.665 for SQL Server 2000).
-- (Although we are not applying the latest patch in this script, we can still
--  output a message warning the user of the script to apply the needed patches as long as you capture the output.)
SELECT @@version as [SQL Server Version]
IF NOT (charindex('8.00.665',@@version)>0)
BEGIN
print '*** WARNING - SQL Server NOT PROPERLY PATCHED! ***'
END
GO
--
```

```
-- Enable Windows Authentication as the only login method to prevent against 'sa'
-- account attacks and the weak internal SQL Server authentication model.
IF (charindex('\',@@SERVERNAME)=0)
	EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\MSSQLServer',N'LoginMode',N'REG_DWORD',1
ELSE
	BEGIN
		DECLARE @RegistryPath varchar(200)
		SET @RegistryPath = 'Software\Microsoft\Microsoft SQL Server\' +
RIGHT(@@SERVERNAME,LEN(@@SERVERNAME)-CHARINDEX('\',@@SERVERNAME)) + '\MSSQLServer'
		EXECUTE master..xp_regwrite
'HKEY_LOCAL_MACHINE',@RegistryPath,N'LoginMode',N'REG_DWORD',1
	END
GO
--
-- Set strong 'sa' account password (in this case a concatenation of two
-- unique identifiers).  This password can easily be reset later by using a
-- trusted connection while logged in as a local administrator or any user
-- who is a member of the System Administrator role.
DECLARE @pass char(72)
SELECT @pass=convert(char(36),newid())+convert(char(36),newid())
EXECUTE master..sp_password null,@pass,'sa'
GO
--
-- Enable full auditing to monitor both successful and failed access to the
-- SQL Server.  You may want to scale this back to failed-only is log space
-- is a problem.
IF (charindex('\',@@SERVERNAME)=0)
	EXECUTE master.dbo.xp_regwrite N'HKEY_LOCAL_MACHINE',
N'Software\Microsoft\MSSQLServer\MSSQLServer',N'AuditLevel',N'REG_DWORD',3
ELSE
	BEGIN
		DECLARE @RegistryPath varchar(200)
		SET @RegistryPath = 'Software\Microsoft\Microsoft SQL Server\' +
RIGHT(@@SERVERNAME,LEN(@@SERVERNAME)-CHARINDEX('\',@@SERVERNAME)) + '\MSSQLServer'
		EXECUTE master..xp_regwrite
'HKEY_LOCAL_MACHINE',@RegistryPath,N'AuditLevel',N'REG_DWORD',3
	END
GO
--
-- Disable SQLAgent, Microsoft Distributed Transaction Coordinator (MSDTC), and MSSEARCH
-- since they may potentially represent unnecessary services.  There are no multiple instances of these services.
EXECUTE msdb..sp_set_sqlagent_properties  @auto_start = 0
GO
EXECUTE master..xp_instance_regwrite N'HKEY_LOCAL_MACHINE', N'SYSTEM\CurrentControlSet\Services\MSDTC',
N'Start', N'REG_DWORD', 3
GO
EXECUTE master..xp_instance_regwrite N'HKEY_LOCAL_MACHINE',
N'SYSTEM\CurrentControlSet\Services\MSSEARCH', N'Start', N'REG_DWORD', 3
GO
--
--Diable adhoc queries for each data provider since this functionality is ripe for abuse.  Once again, if
--your application requires this you can add the functionality back on a per provider basis.
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\SQLOLEDB',N'DisallowAdhocAccess',N'REG
_DWORD',1
GO
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\Microsoft.Jet.Oledb.4.0',N'DisallowAdhocAcc
ess',N'REG_DWORD',1
GO
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\MSDAORA',N'DisallowAdhocAccess',N'REG
_DWORD',1
GO
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\ADSDSOObject',N'DisallowAdhocAccess',N'
REG_DWORD',1
```

```
GO
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\DB2OLEDB',N'DisallowAdhocAccess',N'REG
_DWORD',1
GO
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\MSIDXS',N'DisallowAdhocAccess',N'REG_D
WORD',1
GO
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\MSQLImpProv',N'DisallowAdhocAccess',N'R
EG_DWORD',1
GO
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\MSSEARCHSQL',N'DisallowAdhocAccess',N
'REG_DWORD',1
GO
EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\Providers\MSDASQL',N'DisallowAdhocAccess',N'REG_
DWORD',1
GO
--
--Remove the pubs and northwind sample databases since they represent known targets with minimal
--permissions for potential attackers.
USE master
DROP DATABASE northwind
DROP DATABASE pubs
GO
--
--Tighten permissions on jobs procedures in case the SQL Agent service is ever activated to prevent low
--privilege users from submitting or managing jobs.
USE msdb
REVOKE execute on sp_add_job to public
REVOKE execute on sp_add_jobstep to public
REVOKE execute on sp_add_jobserver to public
REVOKE execute on sp_start_job to public
GO
--
--Tighten permissions on web tasks table to keep malicious users from creating or altering tasks.
USE msdb
REVOKE update on mswebtasks to public
REVOKE insert on mswebtasks to public
GO
--
--Tighten permissions on DTS package connection table so that malicious users cannot affect DTS packages.
USE msdb
REVOKE select on RTblDBMProps to public
REVOKE update on RTblDBMProps to public
REVOKE insert on RTblDBMProps to public
REVOKE delete on RTblDBMProps to public
GO
--
--Tighten permissions on extended procedures that require heavy use but should not be allowed public access.
USE master
REVOKE execute on sp_runwebtask to public
REVOKE execute on sp_readwebtask to public
REVOKE execute on sp_MSSetServerProperties to public
REVOKE execute on sp_MScopyscriptfile to public
REVOKE execute on sp_MSsetalertinfo to public
REVOKE execute on xp_regread to public
REVOKE execute on xp_instance_regread to public
GO
--
--Revoke guest access to msdb in order to keep any non system administrators from accessing the database without
explicit permissions.
USE msdb
EXECUTE sp_revokedbaccess guest
GO
```

```
--
--Turn off allow remote access to keep other SQL Servers from connecting to this server via RPC.
EXECUTE sp_configure 'remote access', '0'
GO
RECONFIGURE WITH OVERRIDE
GO
--
--Verify that the capability to allow access to system tables is disabled.
EXECUTE sp_configure 'allow updates', '0'
GO
RECONFIGURE WITH OVERRIDE
GO
--
--Increase SQL Server log history threshold in order to maintain logs for a longer amount of time.
IF (charindex('\',@@SERVERNAME)=0)
        EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'Software\Microsoft\MSSQLServer\MSSQLServer',N'NumErrorLogs',N'REG_DWORD',365
ELSE
        BEGIN
                DECLARE @RegistryPath varchar(200)
                SET @RegistryPath = 'Software\Microsoft\Microsoft SQL Server\' +
RIGHT(@@SERVERNAME,LEN(@@SERVERNAME)-CHARINDEX('\',@@SERVERNAME)) + '\MSSQLServer'
                EXECUTE master..xp_regwrite
'HKEY_LOCAL_MACHINE',@RegistryPath,N'NumErrorLogs',N'REG_DWORD',365
        END
GO
--
--Remove any residual setup files (\sqldir\setup.iss - \winnt\setup.iss - \winnt\sqlstp.log) that may be
--lingering on the file system. These scripts now include system variables thanks to Carlos Moran
EXECUTE master.dbo.xp_cmdshell 'if exist %windir%\setup.iss del %Windir%\setup.iss'
GO
EXECUTE master.dbo.xp_cmdshell 'if exist %windir%\sqlstp.log del %Windir%\sqlstp.log'
GO
EXECUTE master.dbo.xp_cmdshell 'if exist "%ProgramFiles%\microsoft sql server\mssql\install\setup.iss" del
"%ProgramFiles%\microsoft sql server\mssql\install\setup.iss"'
GO
--
--Remove any un-used network libraries. Since this is a hardened server, all netlibs can be removed until
--external connectivity requirements are identified.  Connections to the local server are still possible
--using the Shared Memeory netlib which is always in effect by specifiying '(local)' or (a period) as
--the server name.  The other netlibs can easily be restored using the Server Network Utility.
--(You must stop and restart the SQL Server for this change to go into effect)
--This step effectively blocks all network access to this SQL Server.  Please be advised of this before
--applying this step.
--NOTE: This step has been removed by default.  Feel free to add it when applying to local-only installations
--such as MSDE applications or Visual Studio.NET/.NET SDK installs
--
--EXECUTE master.dbo.xp_regwrite
N'HKEY_LOCAL_MACHINE',N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib',
N'ProtocolList',N'REG_SZ',''
--GO
--
--
PRINT '*** Please Stop and Start the SQL Server Service Instance in order to implement changes ***'
PRINT ''
PRINT '*** End SQL Server 2000 Lockdown Script ***'
```

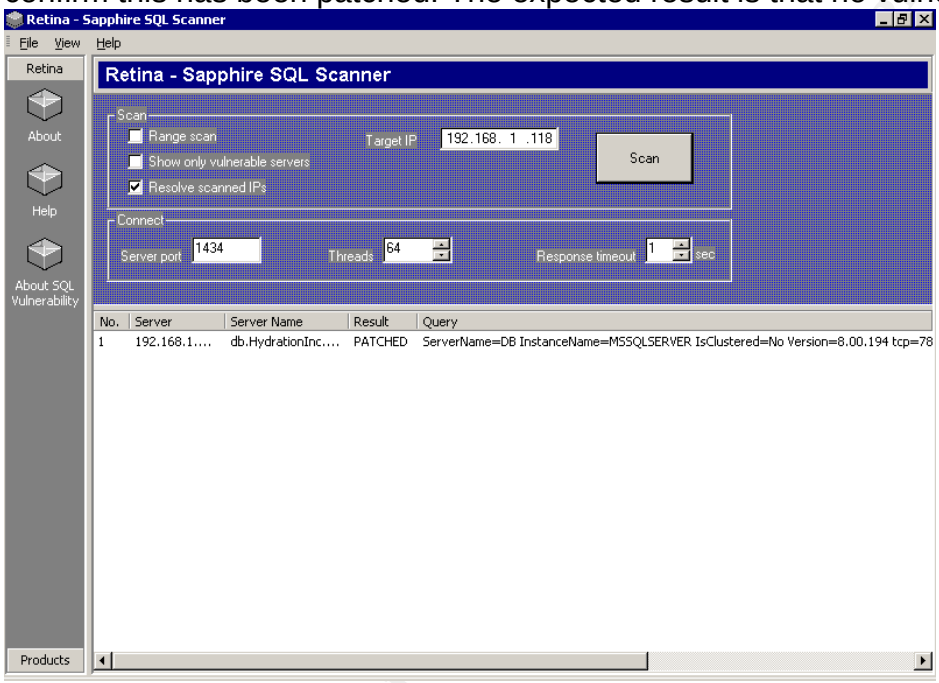
End of Lockdown script

Applying the database lockdown script

From the database server, while logged in as the administrator, the lockdown script was downloaded and saved on the desktop. The Query Analyzer (Start, Programs, Microsoft SQL Server, Query Analyzer) was use to load and run the script.

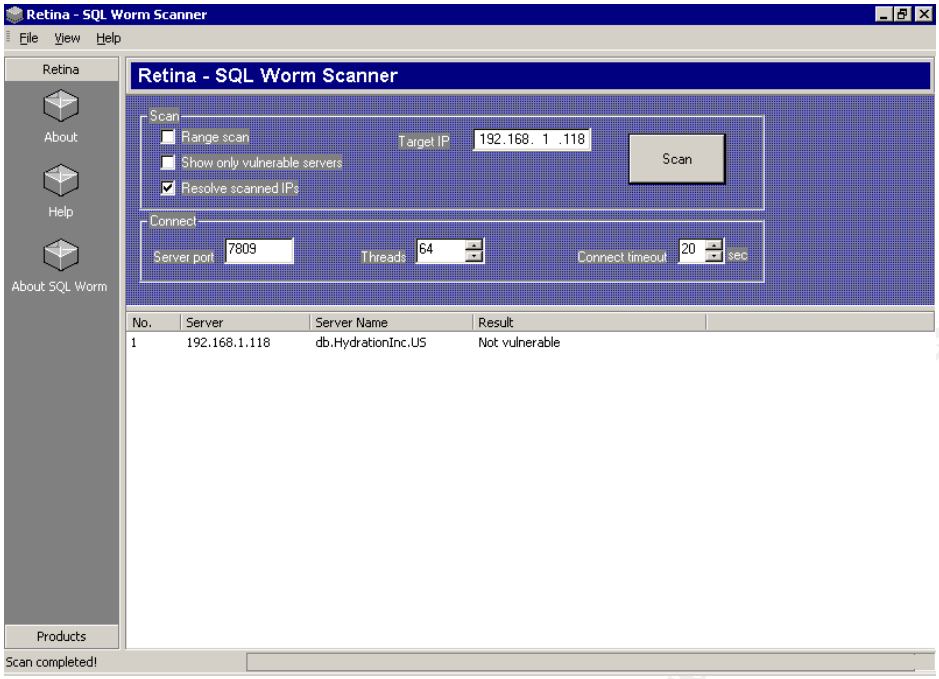
Testing the script

The first test is to determine if the database is vulnerable to the Slammer or Sapphire worm. To determine eEye's vulnerability scanner Retina[11] will be run to confirm this has been patched. The expected result is that no vulnerability exists.



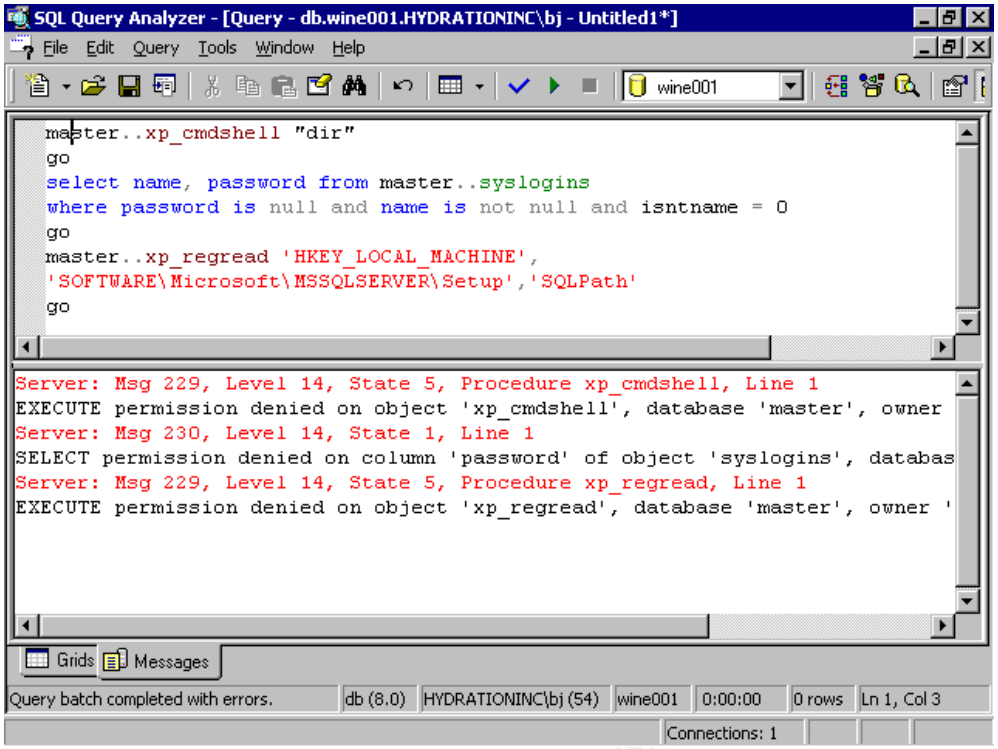
The result column in the screenshot shows patched so this is not vulnerable.

Another test was to verify that this is was not vulnerable to the SQL Spida Worm. The expected result is that no vulnerability exists.



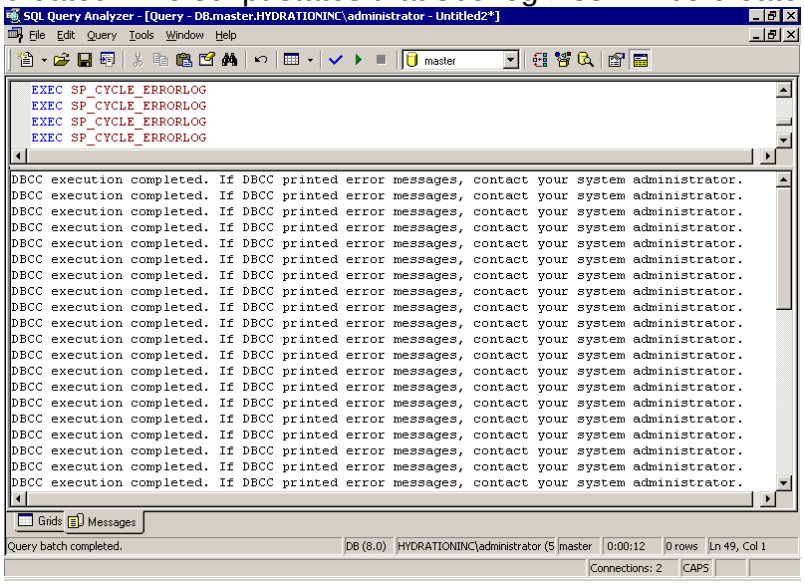
The result column in the screenshot shows 'Not vulnerable' so this server is secure.

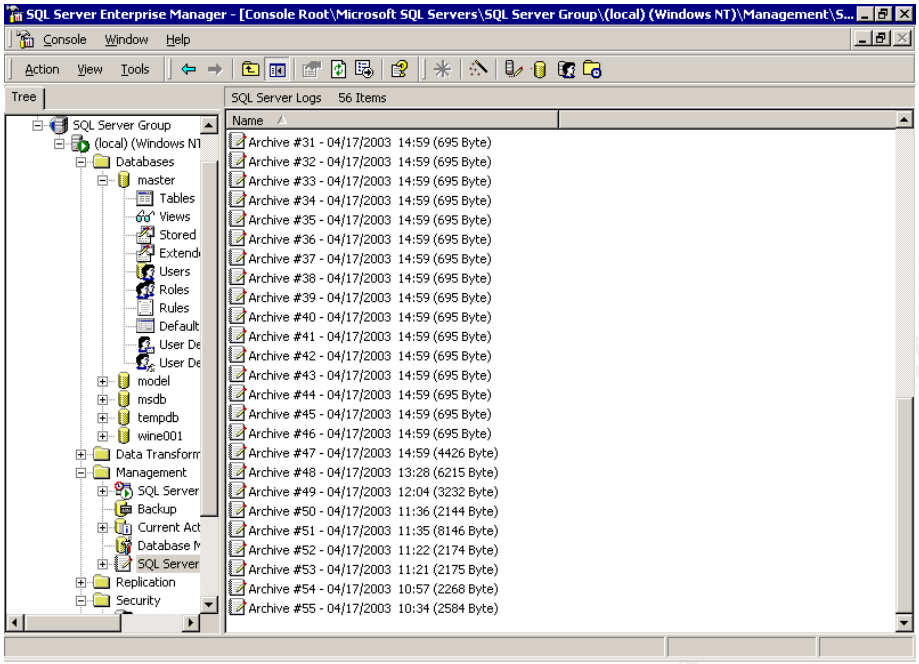
A third test will be to see if a legitimate user can do nefarious things. The expected result is that no one, apart from the system administrators, should be able to shell out to a command prompt. BJ from Napa Valley will attempt to run the xp_cmdshell procedure, find out users with blanks passwords and read the registry. The expected result is that he will be denied on all attempts.



Execution was denied on all three attempts.

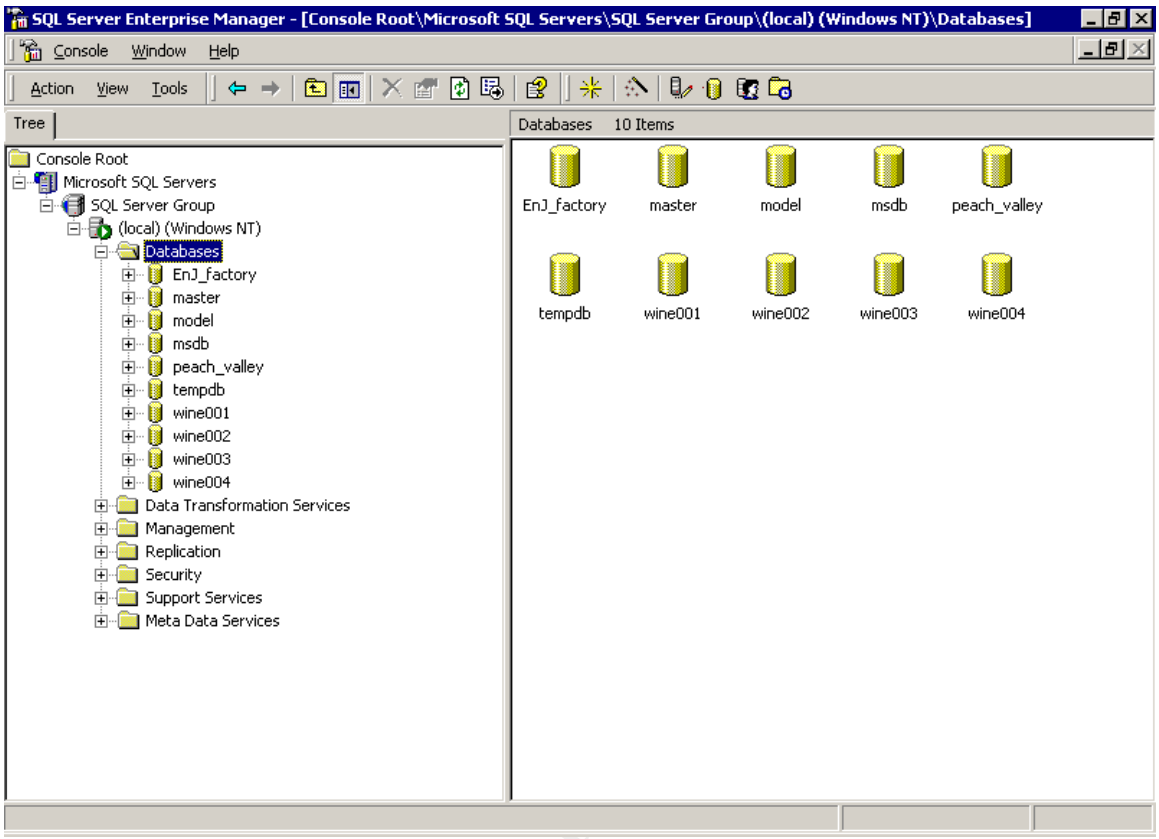
A fourth test will be to cycle the errorlog 50 times and to see if 50 log files are created. The script states that 365 log files will be created.





Within Enterprise Manager, 55 log files are available to be viewed. The default setting is six.

A fifth test will be to see if the PUBS or NORTHWIND databases are present. The expected result is that they are gone.



Both databases are missing from the system.

Evaluation of the database script

Like the NSA's OS template, some things can be strengthened outright while others must be implemented as the situation arises. For the database, the template does several things well. The template did a good job of removing obvious targets of default databases. Like the OS template, by increasing the number of SQL Server log files, a record of who did what will be maintained. Auditing of both failed and successful logins will be recorded in case someone tries to attack the SA account. This is a good starting point. If the logs become too full, this may have to be scaled back to only capture failed logins.

The script also does a nice job of protecting DTS packages. By default, anyone with a login to the server can create packages. This could lead to a denial of service by filling up the database where packages are held. The script revokes public access to the RtblDBMProps table.

For job system lockdown, the script revokes access on sp_add_job. It misses sp_delete_job and sp_purge_jobhistory. However, there are a very large number

of these stored procedures and the checklist does say to review and add more as they are found.

Also while the checklist mentions to “Restrict to sysadmins-only access to stored procedures and extended stored procedures that you believe could pose a threat. There are quite a few of them, and this could take some time.”
The script only revoked access on 17 of the list.

I would also add to the list to revoke access on those stored procedures that can create objects:

Revoke execute on sp_OACreate to public
Revoke execute on sp_OADestroy to public
Revoke execute on sp_OAGeErrorInfo to public
Revoke execute on sp_OAGetProperty to public
Revoke execute on sp_OAMethod to public
Revoke execute on sp_OASetProperty to public
Revoke execute on sp_OAStop to public

To finish up the task of security, the underlying dlls to these extended stored procedures should be deleted off the system as well.

It was mentioned to Dr. Smart that if wished to use a third party product, he could encrypt his data within the database very easily[12]. Third party products also exist that compress and through the compression provide a mild form of obfuscation of the backup files if he was so inclined to use them[13]. Dr. Smart decided to keep costs to a minimum and declined.

Conclusion

The Windows 2000 operating system was secured using a nationally recognized group policy template. The operating system’s settings were changed from factory defaults to a more stringent standard. SQL Server 2000 was installed and secured using a database script that will prevent customers from straying beyond what is required.

Mr. Smart was presented with summary of what was done, the settings that were changed and the reasons they were changed. We then presented Mrs. Smart with the final bill. When Mrs. Smart asked “So, is it safe now?” Mr. Smart answered for us: “It is both safe and secure!”.

Appendix 1

NSA server template W2k Server.INF

http://www.nsa.gov/snac/win2k/guides/inf/w2k_server.inf

```
; (c) Microsoft Corporation 1997-2000
;
; Security Configuration Template for Security Configuration Editor
;
; Template Name:        W2k Server.INF
; Template Version:     05.00.DR.0000
;
; Revision History
; 0000  -       Original
; May 2001 - SNAC version 1.01a
; November 2001 -
;       Changed the line "RequireLogonToChangePassword = 1" to
;       "RequireLogonToChangePassword = 0" under the [System Access]
;       section. This line is an artifact from Windows NT 4.0 templates and could
have
;       adverse effects on a user's ability to change password at first logon. If you
have
;       experienced this problem, please reapply this corrected inf file, or, via a
;       text editor, create and apply an inf file with only the following lines:
;       [Unicode]
;       Unicode=yes
;       [System Access]
;       RequireLogonToChangePassword = 0

;
;       NOTE: This setting does NOT appear when the template file is viewed
graphically in
;       the MMC.
;
; July 2002 -
;       In the Registry section, corrected the
;       MACHINE\System\CurrentControlSet\Control\Wmi\Security to grant
Administrators Full
;       Control on the key and subkeys
;
;  Nov. 2002 -
;       In the Registry section, corrected the
MACHINE\Software\Microsoft\WindowsNT\
```

; CurrentVersion\Perflib to give Creator Owner Full Control on Subkeys only.

; Warning : Care should be exercise When using this template on Exchange Server platform.
; Additional settings and modification to these settings are required, which are site specific.
; No general .INF templates are available for Exchange Server on Windows 2000 at this time.

[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 12
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 3
ResetLockoutCount = 15
LockoutDuration = 15
RequireLogonToChangePassword = 0
ClearTextPassword = 0
[System Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Application Log]
MaximumLogSize = 4194240
AuditLogRetentionPeriod = 2
RetentionDays = 7
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 2
AuditPrivilegeUse = 2
AuditPolicyChange = 3

```
AuditAccountManage = 3
AuditProcessTracking = 0
AuditDSAccess = 0
AuditAccountLogon = 3
CrashOnAuditFull = 1
[Version]
signature="$CHICAGO$"
Revision=1
[Privilege Rights]
seassignprimarytokenprivilege =
seauditprivilege =
sebackupprivilege = *S-1-5-32-544
sebatchlogonright =
sechangenotifyprivilege = *S-1-5-32-545
secreatepagefileprivilege = *S-1-5-32-544
secreatepermanentprivilege =
secreatetokenprivilege =
sedebugprivilege =
sedenybatchlogonright =
sedenyinteractivelogonright =
sedenynetworklogonright =
sedenyservicelogonright =
seenabledelegationprivilege =
seincreasebasepriorityprivilege = *S-1-5-32-544
seincreasequotaprivilege = *S-1-5-32-544
seinteractivelogonright = *S-1-5-32-544
seloaddriverprivilege = *S-1-5-32-544
selockmemoryprivilege =
semachineaccountprivilege =
senetworklogonright = *S-1-5-32-545,*S-1-5-32-544
seprofilesingleprocessprivilege = *S-1-5-32-544
seremoteshutdownprivilege = *S-1-5-32-544
serestoreprivilege = *S-1-5-32-544
sesecurityprivilege = *S-1-5-32-544
seservicelogonright =
seshutdownprivilege = *S-1-5-32-544
sesyncagentprivilege =
sesystemenvironmentprivilege = *S-1-5-32-544
sesystemprofileprivilege = *S-1-5-32-544
sesystemtimeprivilege = *S-1-5-32-544
setakeownershipprivilege = *S-1-5-32-544
setcbprivilege =
seundockprivilege =
[Group Membership]
*S-1-5-32-547__Memberof =
```

```
*S-1-5-32-547__Members =
[Profile Description]
Description=NSA Enhanced Security for Windows 2000 Member/Stand-alone
Servers
[File Security]
"%SystemDrive%\Program Files\Resource
Kit",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\security",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)"
"%SystemDrive%\Documents and Settings\Default
User",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\ntldr",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\config.sys",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;
0x1200a9;;;BU)"
"%SystemDrive%\ntdetect.com",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\boot.ini",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OI
CI;0x1200a9;;;BU)"
"%SystemRoot%\$NtServicePackUninstall$",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;F
A;;;SY)"
"c:\boot.ini",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntdetect.com",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntldr",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\ntbootdd.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)"
"c:\autoexec.bat",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;
BU)"
"c:\config.sys",2,"D:PAR(A;;FA;;;BA)(A;;FA;;;SY)(A;;0x1200a9;;;BU)"
"%ProgramFiles%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;S
Y)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)
(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\CSC",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;F
A;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\Registration",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OIC
I;FR;;;BU)"
"%SystemRoot%\repair",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\Tasks",1,"D:AR"
"%SystemRoot%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;F
A;;;SY)(A;CI;0x100026;;;BU)"
"%SystemDirectory%",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;
;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\appmgmt",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OI
CI;0x1200a9;;;BU)"
```

"%SystemDirectory%\DTCLog",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\GroupPolicy",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
"%SystemDirectory%\NTMSData",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Setup",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\ReinstallBackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\repl",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\import",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1301bf;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\repl\export",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;RE)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDirectory%\spool\printers",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DCLCSWWPLO;;;BU)"
"%SystemDirectory%\config",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDirectory%\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"%SystemDrive%\Documents and Settings",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\My Download Files",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1201bf;;;BU)"
"%SystemDrive%\System Volume Information",1,"D:PAR"
"%SystemDrive%\Temp",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;CI;DCLCWP;;;BU)"
"%SystemDrive%\",0,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\IO.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\MSDOS.SYS",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemRoot%\regedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rcp.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\Ntbackup.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rexec.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\rsh.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDirectory%\regedt32.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemRoot%\debug\UserMode",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;;CCDCWP;;;BU)(A;OIIO;DCLC;;;BU)"

"%SystemDrive%\Documents and
Settings\Administrator",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OI
CI;FA;;;SY)(A;OICIIO;DCLCWP;;;BU)(A;OICI;CCSWWPLORC;;;BU)"
"%SystemDirectory%\secedit.exe",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)"
"%SystemDrive%\Inetpub",1,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;FA;;;CO)(A;OICI;
FA;;;SY)(A;OICI;0x1200a9;;;BU)"
"%SystemDrive%\Documents and Settings\All
Users\Documents\DrWatson\drwtsn32.log",2,"D:PAR(A;OICI;FA;;;BA)(A;OICIIO;
FA;;;CO)(A;OICI;FA;;;SY)(A;OICI;0x1301bf;;;BU)"
"%SystemRoot%\Offline Web Pages",1,"D:AR(A;OICI;FA;;;WD)"
"%SystemDrive%\Documents and Settings\All
Users",0,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)(A;OICI;0x1200a9;;;BU)"
[Registry Keys]
"MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AsrCommands",2,"D:PAR(A;CI;KA;;;BA)(A;CI;CCDCLCSWR
PSDRC;;;BO)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for
NT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"machine\software",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI
;KR;;;BU)"
"machine\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)"
"machine\software\microsoft\protected storage system provider",1,"D:AR"
"machine\software\microsoft\windows
nt\currentversion\perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CII
O;KA;;;CO)"
"machine\software\microsoft\windows\currentversion\group
policy",0,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\software\microsoft\windows\currentversion\installer",0,"D:PAR(A;CI;KA
;;;BA)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\software\microsoft\windows\currentversion\policies",0,"D:PAR(A;CI;KA;
;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\system",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;
KR;;;BU)"
"machine\system\clone",1,"D:AR"
"machine\system\controlset001",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset002",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset003",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset004",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;K
A;;;SY)(A;CI;KR;;;BU)"

"machine\system\controlset005",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset006",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset007",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset008",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset009",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\controlset010",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:PAR(A;CI;KA;;;BA)(A;;KR;;;BO)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\control\wmi\security",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\enum",1,"D:PAR(A;CI;KA;;;BA)(A;CI;KR;;;AU)(A;CI;KA;;;SY)"
"machine\system\currentcontrolset\hardware profiles",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"users\.default",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"users\.default\software\microsoft\netdde",2,"D:PAR(A;CI;KA;;;BA)(A;CI;KA;;;SY)
"
"users\.default\software\microsoft\protected storage system provider",1,"D:AR"
"CLASSES_ROOT",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)(A;CI;KR;;;BU)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
"MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities",2,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)(A;CI;KA;;;SY)"
[Registry Values]
MACHINE\System\CurrentControlSet\Control\Session Manager\EnhancedSecurityLevel=4,1
MACHINE\System\CurrentControlSet\Services\Eventlog\Security\WarningLevel=4,90
MACHINE\System\CurrentControlSet\Services\MrxSmb\Parameters\RefuseReset=4,1
MACHINE\System\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand=4,1
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0

MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\PerformRouterDiscovery=4,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,2
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen=4,200
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpenRetired=4,160
MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun=4,255
MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon=4,0
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,0
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,0
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpassword=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignature=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,30
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\print\providers\lanman print services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5

machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,1
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,1
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,1
machine\software\microsoft\windows\currentversion\policies\system\shutdownwithoutlogon=4,0
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername=4,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,1
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\non-driver signing\policy=3,1
machine\software\microsoft\driver signing\policy=3,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableForcedLogOff=4,1

References

The Center for Internet Security. Lockdown Scripts and Checklists for Windows 2000 https://www.cisecurity.org/tools2/win2000/W2K-Srv.pdf

National Security Agency http://www.nsa.gov/snac/index.html

Lewis, Morris SQL Server Security Distilled. Curlingstone. December 2002.

Andrews, Chip. http://www.sqlsecurity.com/DesktopDefault.aspx

Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet. O'Reilly & Associates. November 2000.

Port Assignments and Protocol Numbers from Microsoft for SQL Server – table 3 http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/cnfc/cnfc_por_zqyu.asp

Registry keys for SQL Server Account and access permissions http://support.microsoft.com/default.aspx?scid=kb;en-us;Q283811

SQL Server C2 configuration checklist http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/sql/maintain/security/sqlc2.asp

Waymire, Richard and Ben Thomas. SQL Security whitepaper. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/sql/maintain/security/sqlc2.asp

INF: TCP Ports Needed for Communication to SQL Server through a Firewall. http://support.microsoft.com/default.aspx?scid=kb;EN-US;q287932

Antivirus software. http://www.grisoft.com/html/us_index.htm

Changing the logon hours of an account (such as guest) using Active Directory or the command line. http://support.microsoft.com/default.aspx?scid=kb;en-us;318714

Endnotes

[1] http://www.theregister.co.uk/content/56/29040.html
http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html

[2] http://www.cnn.com/2003/TECH/biztech/01/28/microsoft.worm.ap/

[3] http://support.microsoft.com/default.aspx?scid=kb;en-us;318714

[4]
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/sag_SCEdefaultpols.asp

[5] http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/gp/507.asp

[6] Securing Windows NT/2000 Servers for the Internet O'Reilly & Associates; 1st edition (November 2000) Stefan Norberg

[7] http://www.blackhat.com/html/win-usa-02/win-usa-02-spkrs.html#Chip%20Andrews
was his 2002 presentation and
http://www.blackhat.com/html/bh-usa-01/bh-usa-01-speakers.html#Chip Andrews was his 2001 presentation on SQL Server security where he presented the SQLPing.exe Utility.

[8] McClure, Scambray, and Kurtz. *Hacking Exposed: Windows 2000*. Osborne, 2001

[9] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-1209
Spida worm is documented here.

[10] http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=4&tabid=12

[11] Download the Retina Sapphire SQL Worm Scanner here:
http://www.eeye.com/html/Research/Tools/Download.asp?file=RetinaSapphireSQL
Note the download will require you to register prior to download. The program is free. Microsoft has recently released the Slammer Vulnerability Assessment Tool found at
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/SVAtool.asp

[12] http://www.protegrity.com
http://www.informnavigator.com/index.asp?ap=xp_crypto&am=about#xp_crypto

[13] http://www.sqlzip.com/