Global Information Assurance Certification Paper

Windows NT 4.0 Auditing and Security

Eric Griswold

Practical Assignment 1.4 Option 1

Abstract
Although Windows NT 4.0 auditing and security may seem straightforward and relatively easy, there are settings that should be configured prior to bringing the server online that are often overlooked. There are many references and resources that explain and assist with administering an NT network, but finding these resources is often a daunting task. This paper will attempt to clarify some basic security elements and tools that are useful to the Windows NT administrator. Welcome, and read on.

Are you connected to a wired network?
Just say No! It's a jungle out there and they are truly out to get you. Maybe that seems a bit extreme, but Windows NT 4.0 straight out of the box is NOT secure. At the very least, you will want to refrain from connecting a network cable to the back of your server until you have applied your service pack(s), patched your system, and sufficiently locked down your operating system / file system.

All the patches and files are on the network so I absolutely HAVE to get on the net.
No, you just *THINK* you have to get on the network. The year is 2002, CD recorders are fast and inexpensive. If the CD recorder solution does not jive with your methodologies, then beg, steal, or borrow an extra hard disk. Either way, put your service pack(s), patches, hot fixes, system drivers, etc on the storage device for later use.

Okay, so where do I get these patches?
The latest service pack for Windows NT 4.0 is Service Pack 6a and can be downloaded from the Microsoft Service Pack 6a site.
http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp

For a listing of bug fixes see the following Q Articles:
Q241211 List of Bugs Fixed in Windows NT 4.0 Service Pack 6/6a (1 of 2)
Q244690 List of Bugs Fixed in Windows NT 4.0 Service Pack 6/6a (2 of 2)
Many applications and drivers will require that a minimal service pack (greater than service pack 4) be applied to the system prior to installation. Therefore, it is best to apply your service pack first, install your server applications, tools, and then reapply your service pack. Seems tedious? Yep . . .

If you intend to run IIS 4.0 on this server you will need to reapply your service pack after installing the NT 4.0 Option Pack. To be completely honest, you may as well park the service pack on the local file system, as you will need to reapply it anytime you make a system modification that requires the original NT 4.0 disk or the original i386 installation files.

After applying the service pack, it is recommended that you apply the Security Rollup Package. This can be downloaded at the following Microsoft web site:
http://www.microsoft.com/ntserver/sp6asrp.asp

Notes:
1. If you have installed the Compaq Array Controller Driver (CPQARRAY.SYS) from the Compaq Web Site, Compaq FTP Site or Compaq SmartStart, then please see the following article in the Microsoft Knowledge Base regarding Compaq Array Controllers and the Windows NT 4.0 Security Rollup Package (SRP).
Q305228 - STOP 0xA Occurs After Applying Windows NT 4.0 Security Rollup Package.

2. As of April 10th, 2002 a new IIS cumulative update has been released and is available on the Microsoft Site.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-018.asp

3. When applying any patch or update, do your research and **READ** all documentation concerning the update. Ugly and horrible things can occur if you are not aware of the issues associated with the update.

Since the service pack, IIS Cumulative Update, and the SRP were created at a single point in time, it is necessary to do your research and determine if other patches and/or updates are needed. There exist many excellent sites for providing information on Windows NT 4.0 security updates, but your first stop should be at Microsoft's Security site. http://www.microsoft.com/technet/security/default.asp

Enough with these crazy patches . . . Now what?
What's next, you ask? Hit CTRL-ALT-DEL then Enter (or Spacebar) on the keyboard and walk away from the server. Do this a few times till it becomes natural. Do it so many times that you feel icky and wrong if you ever forget to do it. An unattended server is an easily compromised server. An unattended and locked server is a good start, but if you truly want a happy server then simply log off. Besides the obvious reason of advertising your logon name to anybody that has

physical access to the device, failing to logoff a server and walking away makes you the single point of failure. Whack and unwrap, "what if you were hit by a bus?"

Since we are on the logoff and locking the workstation kick, lets hit CTRL-ALT-DEL again. . . but this time, stare at the 'Workstation Locked' message. Most likely, it will say something like, "This workstation is in use and has been locked. The workstation can only be unlocked by COMPUTERNAME\Administrator or an administrator. Press Ctrl + Alt + Delete to unlock this workstation."

This is an ugly message that should be fixed ASAP. Let's unlock the server, go to Start>Run, type: usrmgr \\computername, then hit Enter. This should fire up User Manager application. Highlight the administrator user account. Click the user menu item and select rename. Rename the Administrator account to something other than administrator, admin, root, etc. . . It is common for the administrator, setting up the server, to create a placebo account on the system called 'administrator' after the original account is renamed. This account will either be disabled or have useless permissions that are tracked and audited.

Even though it is relatively trivial to determine the renamed administrator account based on the security identifier of the account this may help thwart the script kid. Just in case you were curious, the SID will end with '–500' if it is the administrator account.

SANS trainers and security professionals will advise against *Security though Obscurity* type of solutions. While renaming the administrator account can be considered by some administrators to be a STO type of solution, when the account renaming practice is combined with routine password changes, audit logging, and audit monitoring this solution can be seen as a being a component of another concept that SANS trainers and security professional will beat into you. This concept is called *Defense in Depth*.

Death to the guest!

The next order of business is to rename the *Guest* account, set a complex password for the account, and verify that it is disabled. Merely leaving the account disabled is not sufficient. A complex password, one that is inclusive of capitals letters, numeric, and shift-numeric characters, should be set on the account.

Death to the administrator, Long live the user!
Next, we should create local user account(s) for everyday usage. It is an extremely poor practice to use the Administrator account or an account that is a member of the Administrators groups as your regular logon account.

If you are new to Windows NT 4.0, you may wish to create individual user accounts for the default groups. The default groups are Administrators, Backup Operators, Guests, Power Users, Replicator, and Users. Even if you are not new to Windows NT 4.0 it is often useful to have a test account that is a member of the Users group to observe and correct behavior(s) that your typical end user may experience.

Tightening the grip
Within the User Manager application there exist useful security features, other than the ability to create user accounts, that should be reviewed. These features include the ability to manage account policies, user rights, and trust relationships.

The Account Policy applet is logically separated into two functions. The first function is to enable and configure user password restrictions. The second function is to define a user account lockout policy.

I've said it once and I'm sure I will say it a few more times before we get to the, "*. . .and they lived happily ever after"* section of this paper. Windows NT 4.0, straight out of the box is NOT secure. So far we have seen this with the need to patch the operating system, the need to rename default user accounts, and apply strong password to the guest account even though, by default, it was disabled.

Below is a screen capture of the default account policy for Windows NT 4.0. I have circled items in red that should concern the security conscientious administrator.

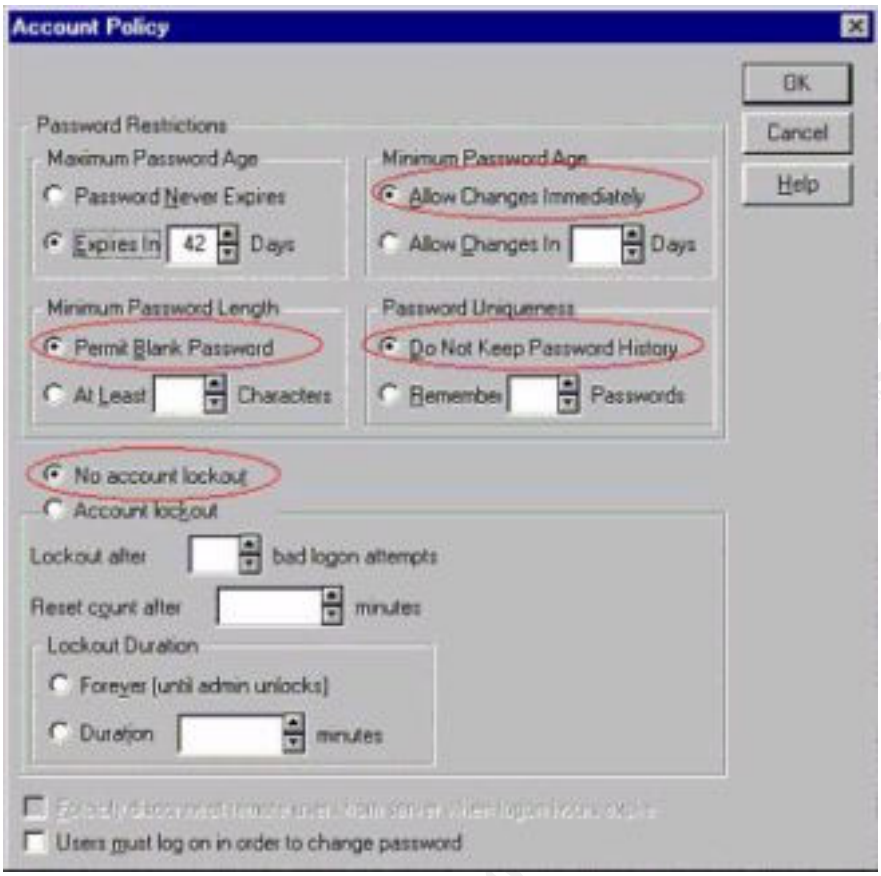

Figure 1: Default Account Policy for Windows NT 4.0

Nothing gets you nothing

The most disturbing default account policy setting might be that '*Permit Blank Password*' is enabled by default. This should be changed to something a little more challenging than nothing. I would recommend that you consider a minimum of six to eight characters.

Even though it is possible to set the minimum password length to 14 characters, I would strongly advise against doing this. Not only would you annoy the end users of your server with this logon requirement, you would advertise to a potential password cracker a major piece of your server's password anatomy. Since the maximum character length allowed on a Windows NT 4.0 server is 14 characters, setting the minimum to 14 characters would create a policy that ALL passwords on the system are 14 characters.

Although I didn't circle it, the '*Maximum Password Age*' should be reviewed and customized for your network environment. A number of at least one day or greater should be configured. Do not even consider choosing the '*Never Expire Password*' radio button. Passwords that do not expire should only be limited to the (now renamed) administrator account or accounts that log on as a service.

Don't allow users to change password: *password* to *password*

Another default setting I will raise an issue with is the '*Password Uniqueness*' option. Since we have accepted the default, in our example, that passwords need to be changed every 42 days, we should protect against users reusing passwords they have used in the recent past. Used in conjunction with the '*Minimum Password Age*' an administrator can make it difficult for users to recycle their expired passwords and reuse a favorite password over and over again.

It is better to have an account locked out than to have the account cracked

Next we should look at the '*Account Lockout*' policy. By default there isn't one. A password cracker would be able to use brute force, dumb luck, educated guesses, or tools such as John the Ripper without the penalty or inconveniences of locking the user(s) account.

It is advised that an account lockout be defined on your server. The settings are fairly intuitive, so I will not get too granular here. Before we hit our next topic I would like to mention a couple of points on the issue of account lockout policies.

If the administrator configures the account lockout duration to 'forever (until admin unlocks)', it is would be extremely easy for an attacker to launch a denial of service against your user accounts by locking the accounts with bogus password attempts.

- The administrator account cannot be *locally* locked out.
- There is a Windows NT 4.0 Resource Utility called Passprop.exe that is used to limit password cracking attempts initiated over a network connection.

Right or Wrong?

Next we will take a look at the *User Rights Policy* for Windows NT 4.0. The User Rights Policy is located in the 'Policies' menu and is called 'User Rights'.

This is one of the reasons we are not yet plugged into a network. The 'Everyone' group has no business accessing the server from the network. Also, the administrator account should not be able to access the server from the network. The administrator should perform their administrative functions while physically present at the server console.

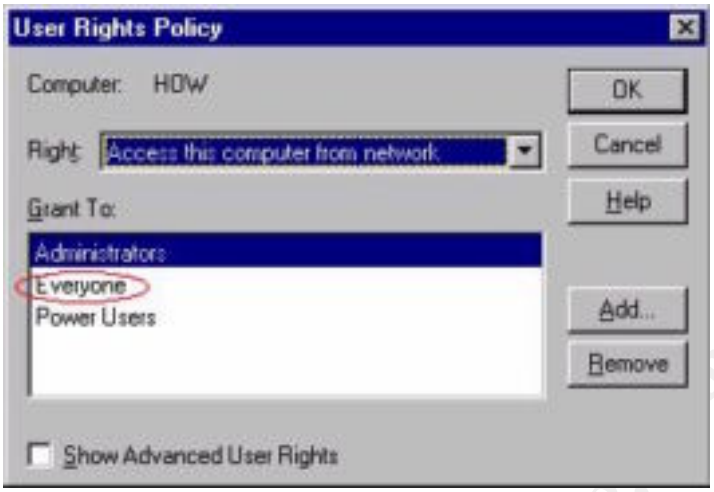

Figure 2: Default Rights Policy for Windows NT 4.0

The Basic rights are listed below with their recommended settings[1]:

Access this computer from the network	Domain Users, Server Operators, Account Operators, Print Operators, Backup Operators
Add workstations to the domain	Administrators
Backup files and directories	Administrators, Backup Operators
Force shutdown from a remote system	None
Load and unload device drivers	Administrators, Server Operators
Log on Locally	Administrator, Server Operators, Backup Operators
Manage auditing and security log	Administrators
Restore files and directories	Administrators, Backup Operators
Shutdown the system	Administrator, Server Operators
Take ownership of files or other objects	Administrators

[1] User rights information can be found in, e.g., *Windows NT 4.0 Security, Audit, and Control*, or directly from the User Rights Policy dialog in User Manager

The Advanced User Rights with their recommended settings:

Act as part of the operating system	None
Bypass traverse checking	Administrators, Server Operators, Backup Operators
Create a page file	Administrators
Create a token object	None
Create permanent shared objects	None
Debug programs	Administrators
Generate security audits	None
Increase quotas	Administrators
Increase scheduling priority	Administrators
Lock pages is memory	None
Log on as a batch job	None
Log on as a service	Replicators, (Others as needed)
Modify firmware environment	Administrators, Server Operators, Backup Operators
Profile single process	Administrators
Profile system performance	Administrators
Replace a process level token	None

Wouldn't you like to know?

Before we exit out the User Manager application, we should make one final stop in the Audit Policy applet. This is located in the 'Policies' menu and is simply called 'Audit'.

By default, the 'Do Not Audit' option is selected. Since our focus is to **secure** Windows NT 4.0, leaving this option as-is should not be acceptable.

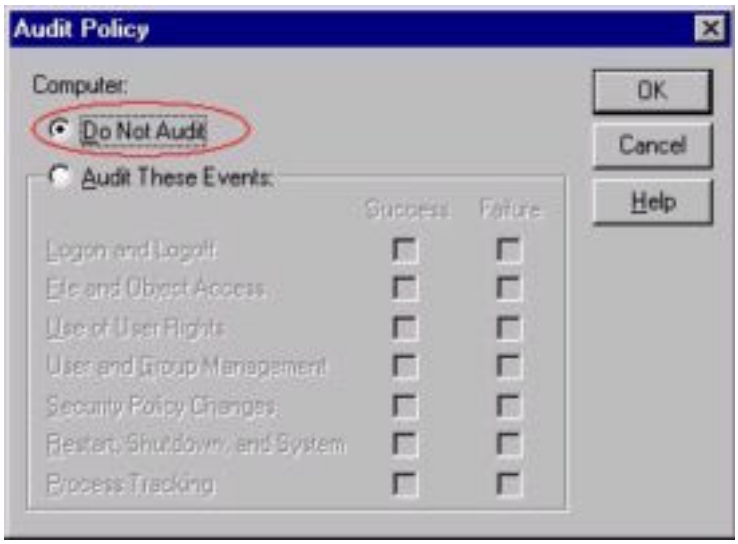

Figure 3: Default Audit Policy for Windows NT 4.0

The options you set for auditing will depend on the role the server will perform.

If the server's role will be a domain controller or Remote Access Server that handles authentication requests, then you will want to configure the applet, at a minimum, to audit the following events:

Logon and Logoff	Failure
File and Object Access	Failure
Use of User Rights	Success and Failure
User and Group Management	Success and Failure
Security Policy Changes	Success and Failure
Restart, Shutdown, and System	Success and Failure

If the server's role will be a file and/or print server then you will not need to audit on authentication related events. The following events are the minimal events you will want to audit for a file and/or print server:

File and Object Access	Failure
Restart, Shutdown, and System	Success and Failure

Note for file servers: Instead of the 'Domain Users Audit Policy' applet, you will want to consider using the directory or file auditing tools to log directory and/or file access tracking. We will discuss this in greater detail later, but for now let's keep the focus on the options within the 'User Manager' application.

It's a server so let's audit everything
That would be a bad idea for a few reasons. The first reason would be the performance hit the server would suffer from auditing processor intensive events such as '**Process Tracking**'. Another reason would be the collecting of useless data and having to sift through this data. Or worse, having your salient data overwritten by insignificant or useless audit events.

The important thing to keep in mind is the *role* the server will be performing and only audit on these events. If the server will process logons then audit account related events. If the server contains sensitive database files then you might want to consider auditing '**File and Object**' events for success and failure accesses. In any case, experiment with these audit settings and verify that you are capturing the intended events in the Event Viewer.

File and Directory Auditing 101
Here is another example of a useful Windows NT 4.0 security feature that is disabled by default. Unlike the last few examples, this option makes sense to be disabled by default, as these options should be customized for each server's role and the files or directories that it contains.

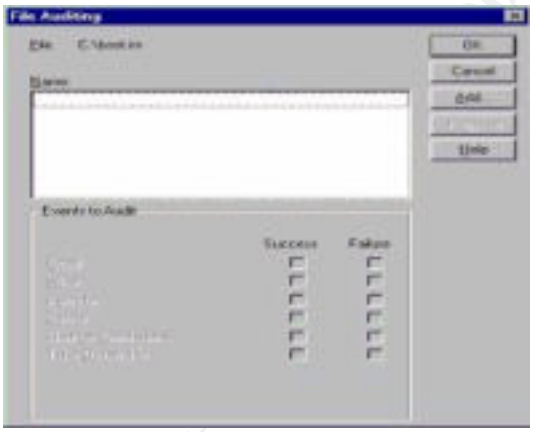

Figure 4: File Auditing applet

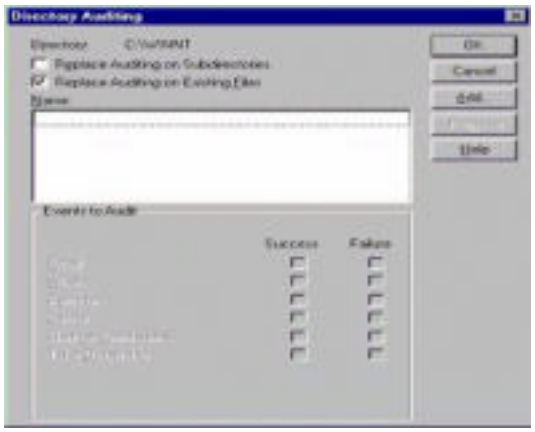

Figure 5: File Auditing applet

File and directory auditing allows the administrator to monitor successful and/or failed attempts to modify or access items that reside on the server's file system.

To enable file and/or directory auditing for a file system resource drill down to the file or folder, right-click the item (Shift-F10 for the keyboard users out there), select properties, select the security tab, then select the 'Auditing' button.

You will not be able to modify these audit events until you select the 'Add' button and choose user group(s) and/or user(s) accounts. Although there is not a, "one size fits all" recommendation for file and directory auditing, there are some things you should consider when enabling auditing controls. Details should include:

- What are you required to audit?
- What groups and/or users are allowed access to these files or directories?
- How often will event log files be reviewed?

Auditing can be resource intensive in regard to CPU cycles, disk storage space, and the administrator's time. It is important to note that if your audit policy is defined properly you can minimize the impact on your company's resources. Take the time now to get it right. You will be glad you did.

Whack! What happened?

Inevitably, something is going to bring your server down. Maybe a power failure, maybe a hardware failure, bad memory, a failed application, or the evil script kid. Whatever it is, you will want a few things to happen 'automagically'. At the very least, you will want to write an event to the system log. AMAZING! This was actually enabled by default.

You will probably want to send an 'administrative alert' to your administrator's workstation, just in case the administrator happens to be staring at their monitor and wants the pop-up message. In order for these administrative alerts to be sent to the administrator's workstation, the *Alerter* service must be enabled on the server and the Messenger server must be enabled on both the server sending the message and the workstation receiving the alert.

Next you should decide if you will be auditing your dump files. If you will, then check the checkbox. You can change the location of the dump file, but be advised that the system needs to have write or change (if you select the 'overwrite any existing file' option) permissions to the target location. Also note that the dump file will be equal in size to the amount of system memory. (E.g., If you have 2GB of RAM you will need to allow for 2GB of space for your dump file.)

The next option is to 'Automatically Reboot'. This is enabled by default. Depending on your environment, you may wish to require manual interaction with any crashed servers.

Boot.ini . . . The wizard behind the curtain

It is within this applet that you can change the system startup options that are defined in %SystemDrive%\Boot.ini. If multiple boot options are defined, such as VGA Mode or another operating system, these will show up in the 'Startup' dropdown list.

If your server crashes and you would like the server configured to reboot, perform the BIOS POST, and wait at the boot menu screen for somebody to physically make a selection or touch the keyboard, you will need to manually modify the %SystemDrive%\Boot.ini and set the TIMEOUT value to TIMEOUT=-1. If you want your server to boot immediately into Windows NT 4.0, then set the TIMEOUT=0.

Another tidbit of value. . . If you would like see a listing of system variables, fire up a CMD prompt and type: **set <Enter>**

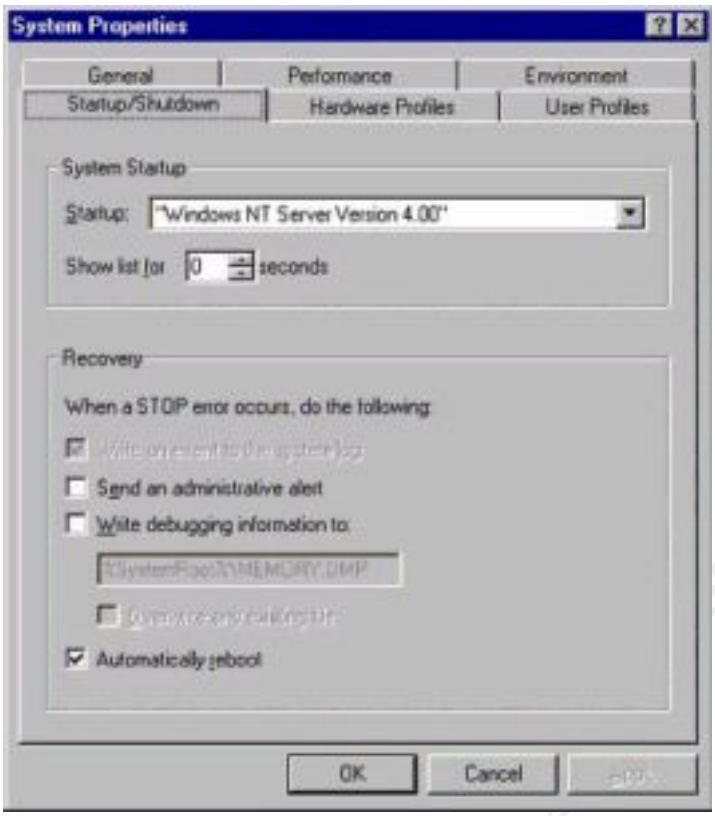

Figure 6: Default System Properties

Oh, so that's where it all goes . . .
Now that we have configured auditing, maybe we should check out where our audit logs are stored. To view the logs, go to Start, Select Programs, drill down to '*Administrative Tools (Common)*', and select *Event Viewer*. If I were nice, I would have had you go to Start→Run, and type: **eventvwr <Enter>**
Anyhow, now that you have it cracked open, check it out.

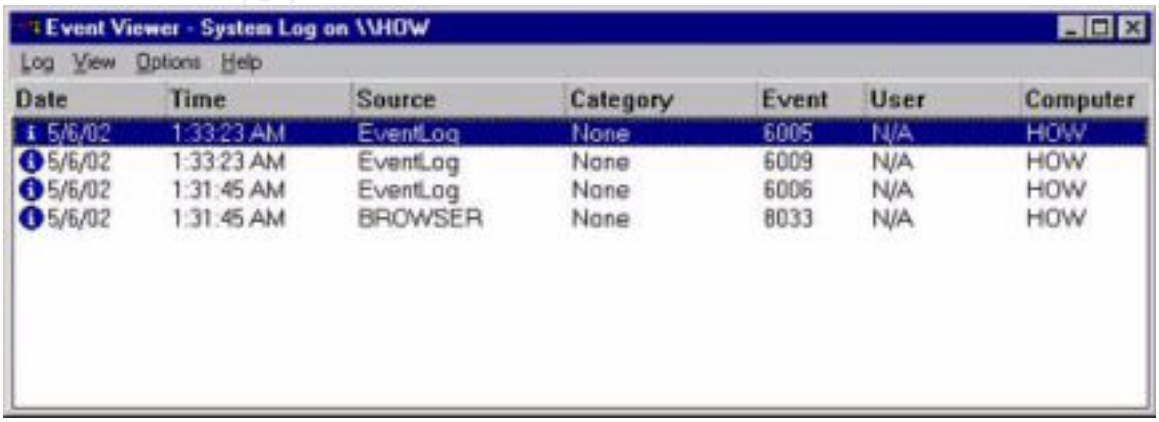

Figure 7: Windows NT 4.0 Event Viewer

If you select the 'Log' menu you will see that you can toggle between the three types of logs. These types are System, Security, and Application. Within the '*Log*' menu, you can select a remote computer's logs, save logs to the file system, or configure the log sizes and their behavior when they reach their thresholds.

Depending upon the auditing and the size of your server, you may need to increase the log settings to accommodate the role of your server. Again, this can be achieved by tweaking the 'Maximum Log Size' for each log type.

Another cool feature of the Event Viewer is the ability to filter for username, computer name, or event IDs. It would be nice if you could perform string queries within this application, but no such luck . . .

Until recently, the Microsoft Knowledge Base was practically useless when querying for event IDs that correlated to Windows NT 4.0 Event Viewer. More recently, they have updated their KB with useful data that simplifies troubleshooting and minimizes headaches. I only mention this because, prior to Microsoft updating their data, a website at http://www.jsiinc.com/reghacks was the most useful site I have found that provided extremely useful data regarding Windows NT 4.0 event IDs.

The Event Log files reside in the %SystemRoot%\Winnt\System32\Config directory and are named Appevent.evt, SecEvent.evt, and SysEvent.evt. These files should be protected with proper *Access Control Lists* and backed up regularly to protect against unauthorized modification or deletion.

Scripting the lockdown, old style . . .

It used to be that grunts, much like myself, had to manually modify the permissions for both the registry and the file system using *regedt32* and *Explorer.* As a matter of fact, I still do when I modify a preexisting server. In the past, I have generated scripts using XCACLS. If you dislike yourself enough to want to do this, check out Article Q135268 at http://support.microsoft.com. Also grab yourself a copy of DumpSec from http://www.systemtools.com/somarsoft which will allow you to generate reports in text format of your system permissions so you don't have to manually script every directory path and registry hive.

Even if you don't intend to perform any scripting, you should still grab a copy of DumpSec. Try it, you will like it. Did I mention that it's free?

If you need to reset the Windows NT 4.0 permissions back to their default settings, you can download the NT Resource Kit utility called FIXACLS.exe from ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/nt40/i386/

Fixacls.exe requires the ability to read %SystemRoot%\Inf\Perms.inf, as this is the location of the default permissions for Windows NT 4.0. If you ever have a chance you should give it a read. It made me smile and laugh a few months ago.

The Security Configuration Manager

The administrators asked for it and finally got it. The *Microsoft Security Configuration Manager* enables the administrator to configure account policy settings, user rights assignments, registry permissions, and file permissions. Proof that whining does pay off . . .

The Security Configuration Manager can be downloaded from http://www.microsoft.com/ntserver/nts/downloads/recommended/scm/default.asp and include sample INF files for testing and tweaking.

The NSA has made available a security paper dedicated to securing Windows NT 4.0 using the SCM. http://nsa1.www.conxion.com/winnt/guides/wnt-1.pdf. This paper covers everything from installation of the SCM, to custom settings, registry tweaks, and files lockdowns. Give it a read. I hope you will enjoy it as much as I did.

Is my server now secure?

From a networking standpoint, the answer is yes. Absolutely! Unfortunately, as soon as you plug the network cable into the server all bets are off!

It doesn't make you feel so warm and fuzzy? Sorry, I truly am . . . Network security is icky and the more you learn the less comfortable you feel. They are out there to get you. The good news is the box is more secure than the default Windows NT 4.0 installation, but keep in mind that network security is an ongoing process that includes securing, monitoring, testing, improving, rinsing, and repeating.

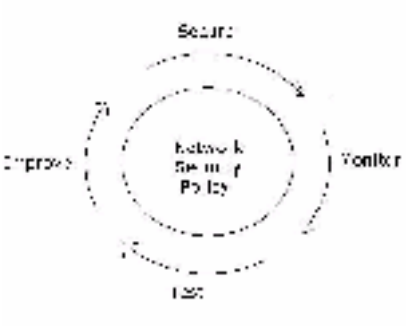

Figure 8: Cisco Security Wheel

Hopefully, this introduction has given you a chance to investigate some elements of Windows NT 4.0 that has you pondering the state of the server in the corner. Can you afford to have the data on the server corrupted, destroyed, copied, or stolen?

References

Cisco Systems
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/idpg/design.htm#1012071

Google (The best search engine ever created on this planet)
http://www.google.com

JSIINC
http://www.jsiinc.com/reghacks

Microsoft
Windows NT 4.0 Server White Papers
http://www.microsoft.com/ntserver/techresources/WpGlobal.asp
Windows NT 4.0 Security Services
http://www.microsoft.com/ntserver/techresources/security/default.asp
Windows NT 4.0 Security Checklists
http://www.microsoft.com/technet/security/tools/chklist/default.asp
Windows NT 4.0 Server Baseline Security
http://www.microsoft.com/technet/security/tools/chklist/nt4svrcl.asp
Domain Controller
http://www.microsoft.com/technet/security/tools/chklist/dccklst.asp
Member Server
http://www.microsoft.com/technet/security/tools/chklist/mbrsrvcl.asp

Security Updates and Tools
http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp
http://www.microsoft.com/ntserver/sp6asrp.asp
http://www.microsoft.com/ntserver/nts/downloads/recommended/scm/default.asp
ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/nt40/i386

Network Windows & .NET Magazine
http://www.ntfaq.com

National Security Agency
http://nsa1.www.conxion.com/winnt/guides/wnt-1.pdf

NT Security
http://www.ntsecurity.net

SystemTools.com
http://www.systemtools.com/somarsoft

The Terry's Chocolate Orange Company
http://www.candystand.com/terrys
-The people who brought us, "Whack and unwrap" and good chocolate!

Jumes, Cooper, Chamoun, and Feinman, **Microsoft Technical Reference: Windows NT 4.0, Security, Audit, and Control**
Microsoft Press, ISBN 1-57231-818-X, 1999

Minasi, Mark, **Master Windows NT Server 4, Sixth edition**
Sybex Inc, ISBN 0-7821-2445-3, 1999

Norberg, Stefan, Russell, Deborah; **Securing Windows NT/2000 Servers**
O'Reilly & Associates; ISBN 1-56592-768-0, copyright 2000

Microsoft Windows NT Network Administration
Microsoft Press, ISBN 1-57231-439-7, 1998

Supporting Microsoft Windows NT Server in the Enterprise
Microsoft Press, ISBN 1-57231-710-8, 1998