# Global Information Assurance Certification Paper

# SANS Practical for the GCNT certification

# Windows 2000 Monitoring
# From Windows NT in a workgroup

## By

## Frank H. Vianzon

## May 4, 2001

## Introduction:

We are trying to use Windows NT in a workgroup environment to do performance monitoring on Windows 2000 in a domain or workgroup. Since Windows 2000 in a workgroup maintains it's own SAM (Security Account Manager) database, authorization is need to complete the monitoring. The target machine (Windows 2000) sees an attempt to access system resources from the host machine across the network. Proper access is required to compete the task. A username and password needs to be passed from the host machine (Windows NT) to the target machine. The user account that is being passed needs to exist on the target machine, and a member of the user group.

Processor and memory monitoring is successful by passing a username/password variable and creating a SMB session. Once a session has been created, the performance monitor can be launched and connected to the target machine. In the case of disk monitoring, both physical and logical, an administrator account is needed. Without administrator rights on the target machine, the counters for physical or logical disks will not appear.

Microsoft TechNet **article Q164018** (controlling remote performance monitoring access to WinNT servers) does state that monitoring is possible with just a user account. Many attempts at this have failed without having local administrator accounts. The research behind this document concerns trying to make disk monitoring possible with a user account. This situation is documented with Microsoft, **case number SRX010111605989**. There are no error codes associated with this, since when trying to monitor physical or logical disks, the option to monitor them simply does not show up.

## Audience:

Target audience is members of the SANS conference, Microsoft engineers, and company operations personnel. Some aspects of this document have been purposely removed to maintain confidential company information.

While this paper is technically accurate to the best of the author's knowledge, there is not much entertainment value. This paper could cause drowsiness, so please do not operate motor vehicles (car, motorcycles, forklifts) or those dumb little razor scooters that no one in Denver knows how to ride, while reading this paper.

Also please do not use illicit drugs while reading this paper. Illicit drugs are bad, and if you use them while reading this paper, you may think that monitoring is fun, and not the boring (but essential) procedure that it really is. Besides, imagine tripping out and saying stuff like "whoa, look at the system idle time"

## Conventions used in this paper:

**BOLD** is a filename, case number or other specific information
Anything in "quotes" is an option on a menu or a directory
***Bold italics*** are actual commands that should be typed

A glossary is also included at the end of this paper

## Theory:

Windows NT in a workgroup is configured as a member server. As a member server, versus a domain controller, accounts are created locally. This would mean that a user account would exist on the member server only, and not shared with another system. These user accounts are stored in a security accounts database, and maintained by the Security Accounts Manager (SAM) on the system trying to do the monitoring, or the "host" machine. This is commonly referred as the SAM database. Objects in the security accounts database are: User Accounts, Computer Accounts, Global Groups, and Local Groups. The focus of this problem lies in user accounts, and the permissions that the user accounts have across the network.

On the Windows 2000 system that is going to be monitored, or the "target" machine, a user account must exist. Any user account creates a SID, or security identifiers. A SID is a very long number that is similar to the following:

S-1-5-21-2087915065-388913830-1877560073-500

There are four main parts of a SID. A revision number, an authority value, a subauthority value, and a relative ID (RID). The most relevant part of the SID in context with this paper is the relative ID, which is the last section of the SID. In this case, the 500 stands for the default administrator account, or an account copied from it. A 501 is the default guest account, or an account copied from it. Non-default accounts start with 1000 and are incremented, with the exception that copied accounts maintain the RID it was copied from.

This is what the Windows 2000 system uses to access objects, including the performance counters. First the host machine (Windows NT 4/Workgroup) attempts to access the target machine, and must try to establish a SMB session to access this process.

There are four stages to this process:
Stage One: Establishing a TCP session
Stage Two: Negotiating a Dialect
Stage Three: Establishing a SMB session
Stage Four: Accessing Resources

**Stage One:** ***Establishing a TCP session*** – the host machine sends a SRB (Session Request Block) to the target server. This NETBIOS request includes both the name of the client and of the server. When the server responds, in creates (by default) a connection on TCP port 139. The server does NOT check the IP address of the host machine

**Stage Two:** ***Negotiating a Dialect*** – at this point, the host and target machine try to figure out which version of SMB to communicate on. Basically, what is the most sophisticated "language" that they can both communicate on? This is stemming from Microsoft Networks, and while there are eight "dialects", the most sophisticated one is NTLM0.12, which both Windows NT 4 and Windows 2000 "speak".

**Stage Three:** ***Establishing a SMB session*** – Once a dialect is negotiated, the client then sends a request containing a username (SID), domain name and other variable information. This username should already exist on the target server, so access should be granted. If the username is not recognized, access is either denied, or a null session is created. This is where the SID that was explained in the previous page falls in. The target machine sees a request from across the network, and since member servers do not share their SAM database, the SID ID is not recognized since the SID ID being passed is of the currently logged on user on the host machine. Here are two ways to pass a different username variable.

**PASSING A DIFFERENT USERNAME (SID):**

1. Create a session by going to START-RUN and in the command line, type the IP address or hostname of the target machine, preceded by the double- backslash (\\). Another window will come up challenging you for a username and password. ***Note:*** this window will have a habit of coming up behind all other windows

2. At a command prompt, type "*net use \\target-hostname /user:domain\username*
The system will then ask for a password. A password can also be placed at the end of the command line, but be aware that it is not encrypted, and people standing behind you can see the password

In this case, access is granted, and logged in the event log – security of the target machine (See "server hardening" later on in this paper). By viewing the security event log, we can see with event ID: 540 access is granted, and then the username is then moved to a different context with event ID: 576.

| | | | | | |
|---|---|---|---|---|---|
| 4/24/2001 | 10:24 | Security | Logon/Logoff | Success | 540 |

Successful Network Logon
User Name: Mothra
Domain: Monster Island
Logon ID: 0x0,0x11ff2
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name: \\NTSERVER

| | | | | | |
|---|---|---|---|---|---|
| 4/24/2001 | 10:24 | Security | Privilege Use | Success | 576 |

Special privileges assigned to new logon:
UserName: Mothra
Domain: Monster Island
Logon ID 0x0, 0x11ff2
Assigned: SeChangeNotifyPrivilege

SeChangeNotifyPrivilege is identifying that the user "Mothra" has the right to "bypass transverse checking". This is a user right that allows a user to bypass the permissions on a higher level directory.

**Stage Four:** ***Accessing Resources*** – Once a SMB session is established, the target machine then locates a point to which access is granted, depending on the access that is given by the account that was passed.

At this point, a SMB session is made, and a layer seven protocol called "named pipes" is now the access point for performance monitoring. Named pipes exist on layer seven of the OSI model. Please see the glossary at the end of this paper for more information.

## The Question

When trying to monitor disk space from Windows NT to Windows 2000, it is only possible when a local administrator account is used. If a user account is used, the counters are not visible. No error codes are associated with this since is seems to be an access issue.

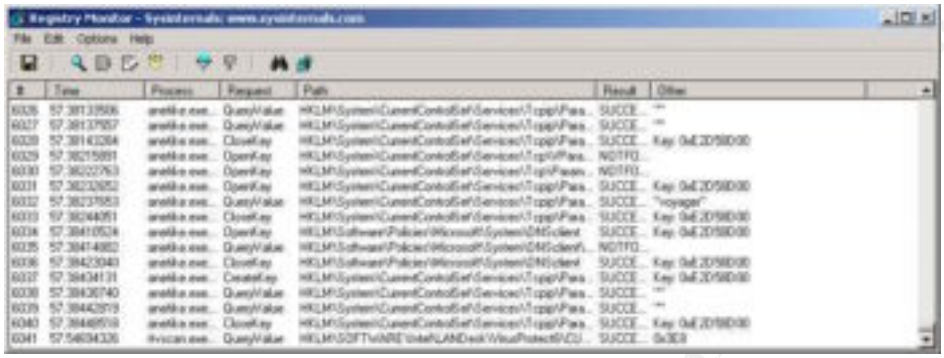
When logged on locally to the Windows 2000 machine, disk monitoring is possible with either a user account or an administrator account. This is due to the fact that when monitoring the local machine, the context used is the system account.

While the process that is described in the following section shows that explicit access to objects is given, all attempts to make it work have failed. *The question now is, what permission does an admin account have that a standard user does not?*

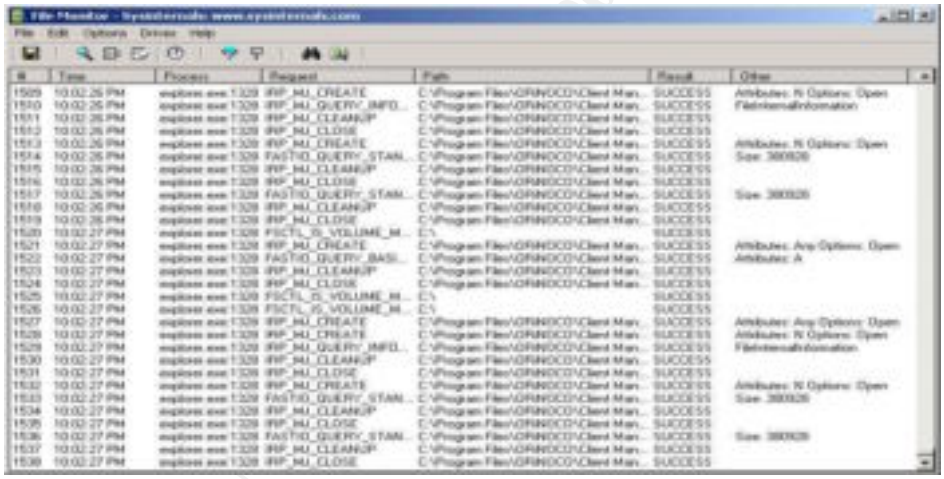
## Third Party Tools

There are two tools from SysInternals (www.sysinternals.com) that have proven useful in this case. These tools allow us to see which registry and files are being accessed.

RegMon is a registry-monitoring tool that shows access to registry entries. It lists a sequential entry including which registry key is being access, the result, and the process trying to access it.



FileMon is similar to RegMon that is shows which files are being accessed, the result, and the process trying to access it



Each tool was used on the target machine twice, once when accessed with a user account, and once with an administrator account. Within a two-minute time frame, each tool captured over 50,000 entries. A program was run to compare the files (administrator versus user), and find the differences. After 36 hours of intensive crunching by a Pentium III system, the list was cut down to just under 5,000 entries. A manual comparison is necessary to analyze this.

## Setting Up the Environment:

Hardware:
Windows NT is running on a Dell Pentium II with 512 MB RAM, with a PERC RAID (Redundant Array of Inexpensive Disks) controller. The system contains four SCSI drives, two 9GB and two 18GB drives. The drives are configured in two RAID ONE (drive mirrors) arrays. Windows NT is running on service pack 6 with two different NIC's (Network Interface Cards). Network card one is dubbed the "public side" and carries a IP address as follows:

IP Address: 192.168.184.2
Subnet Mask: 255.255.255.
Gateway: 192.168.184.1

As stated in **RFC 1918**, an IP address of 192.168.0.0 is a private network that is not routable through the Internet. The IP address of this NIC is natted through an external device, like a firewall or router.

Network card two is dubbed the private side, and is configured:
IP Address: 10.99.1.1
Subnet Mask: 255.255.255.224
No default gateway

While the private NIC does not have a gateway, there needs to be a route off that network. Windows NT has this ability built into the operating system by adding a static route. This will tell the server to send all packets that are destined for a particular network, in this case the 10.99 networks, out of a particular interface. To complete this, a command line option for a static route is entered.

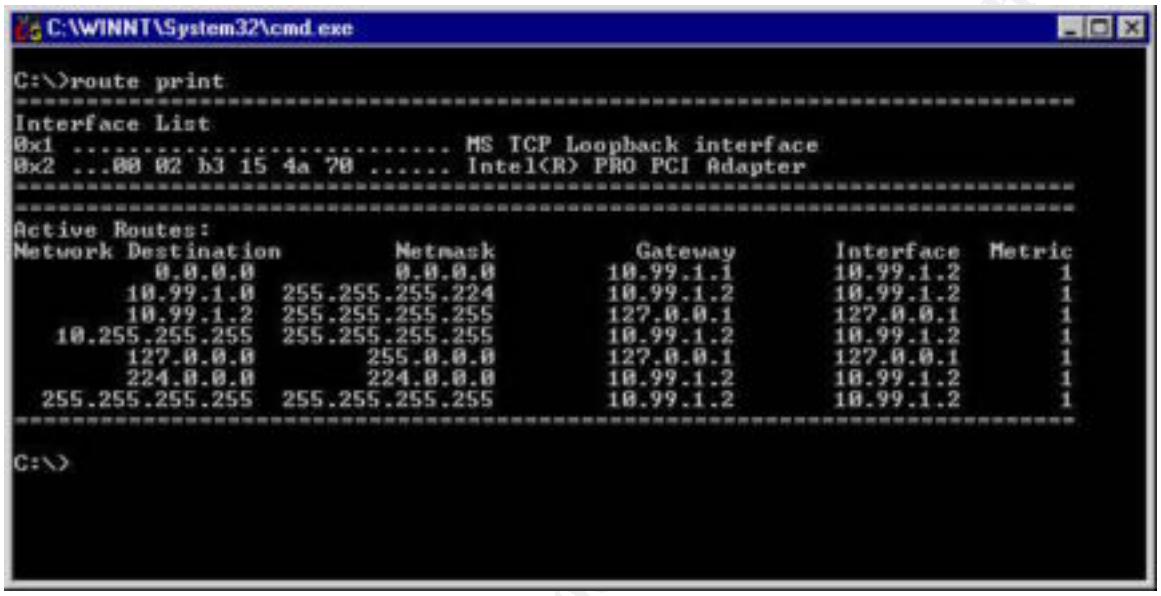
***"route add 10.99.1.0 mask 255.255.255.224 10.99.1.1 –p***

route add is adding a static route
10.991.1 and "255.255.255.224 is identifying the network to route from
10.99.1.1 is IP address of the router that is directly connected to that interface
The "-p" is for persistence, so when the system is rebooted, the route is permanent.

To see all the routes that a system has, type the following statement:

***"route print"***

The following window will display




1. The first line displays the default route
2. The second line displays the subnet on which the network resides
3. The third line displays the host route for the local host. Note that the gateway is the loopback address as defined in **RFC 1933, section 3.1.1**
4. The fourth line shows the broadcast address for the network that the system is on.
5. The fifth line is for the loopback address, as defined in **RFC 1933, section 3.1.1**
6. The sixth line is for IP multicasting. IP multicasting is used to provide multicast services to clients that may not be on the same network. For example, media broadcast.
7. The seventh and final entry is for a limited broadcast. This will most likely affect only the subnet on which the system resides, since most routers by default stop broadcasts

This should define how packets are routed out of the NIC's and to the correct devices

## Preparing the Host machine:

The host machine is defined as the Windows NT server that is doing the monitoring. This machine is part of a workgroup environment and configured as a member server. A member server is defined as a server that contains it's own SAM database. While these servers can be joined to a domain, it this case it stands alone

The target machine is seeing a request from a foreign server, and unless permission has been given to the "everyone" group or the "guest" account, an authorized username needs to be given.

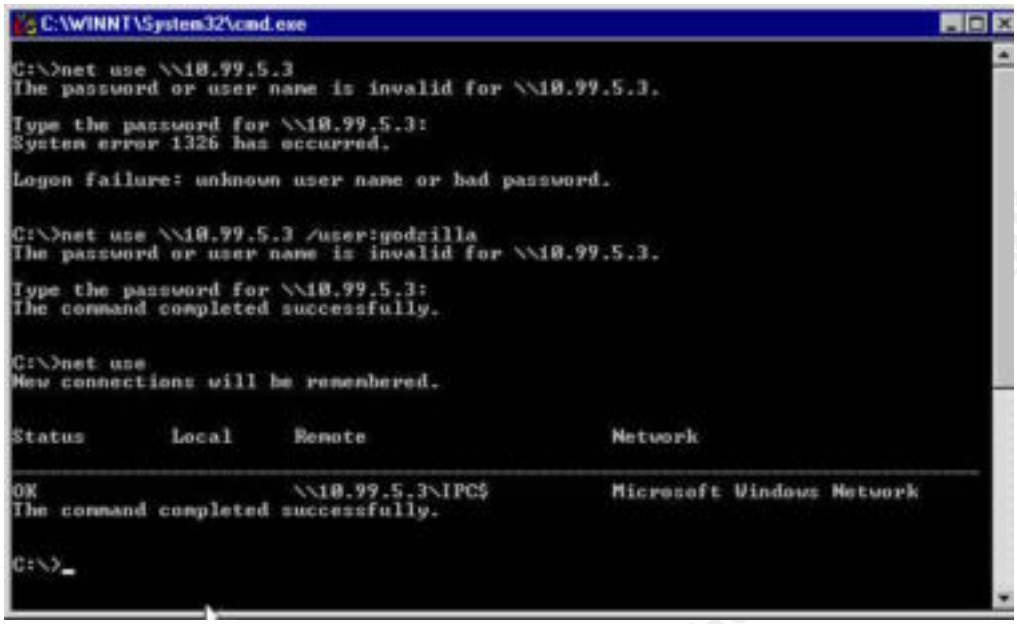
The most typically way to accomplish this is to open a NETBIOS session to the machine, which is sometimes called an IPC session. To make a connection, from the run box in the start menu, type the hostname or NETBIOS name, preceded by the double backslash (\\). For example: \\computername. This will bring up an explorer window to non-hidden shares on the target machine. If the currently logged in user on the host machine does not have a proper access, a dialog box will open request a proper username and password. This can also be done at a command line with the "net use" command. The computer name can be replaced with the IP address

***net use \\computername***

To pass a username variable that is different from the currently logged on user on the host machine

***net use \\computername /user:domain\username password***

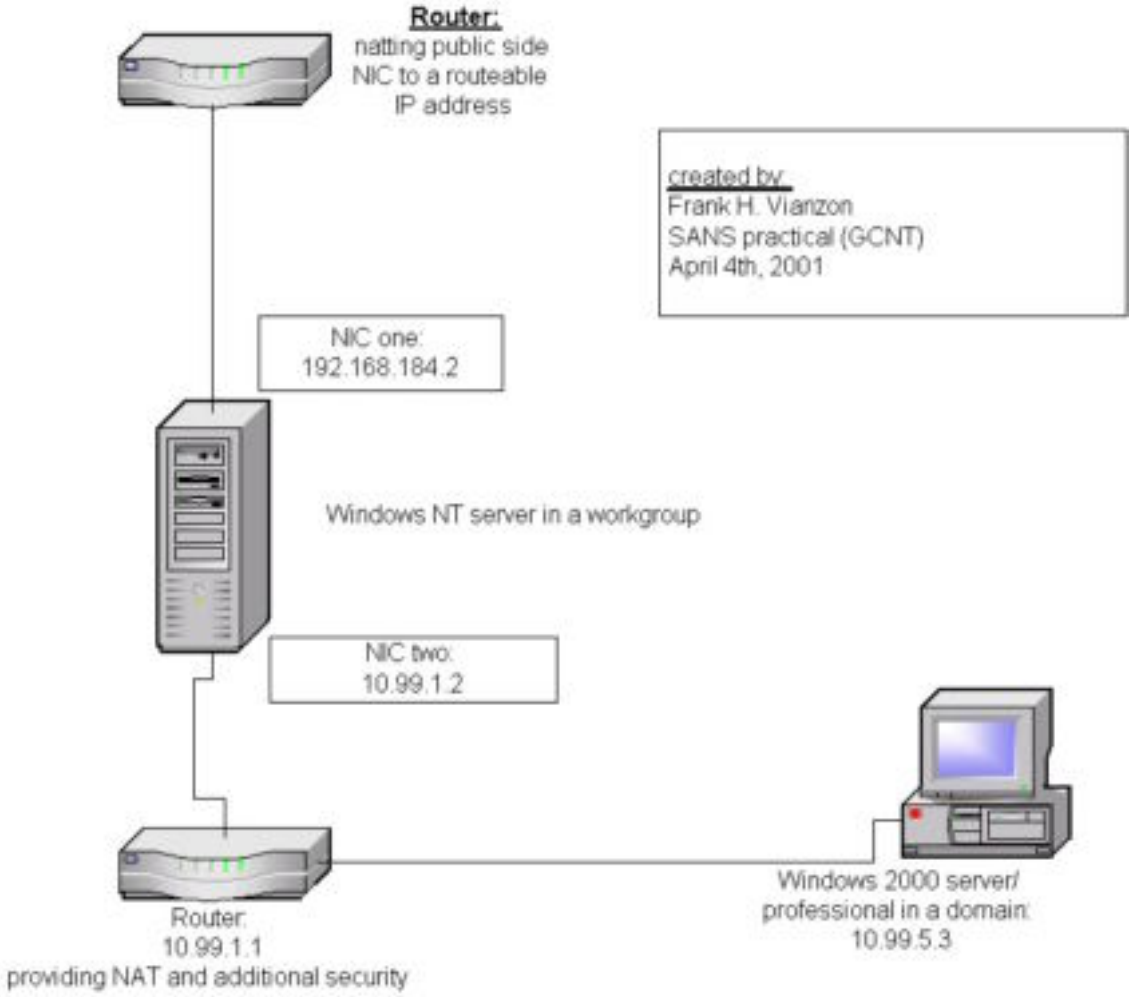
The forward-slash user defines that a different user name is to be used. If the username to be used is not in the domain, the domain option can be omitted. The password that is passed in plain-text. To avoid this possible security risk, do not enter a password. The system will then prompt for a password as seen below:




As you can see above, the password is not displayed when omitted from the end of the "/user" option. There are other ways to make a connection, through a third party tool such as SiteScope from Freshwater (http://www.freshwater.com), which is discussed later in this paper.

A connection has not been made to the target machine. Windows explorer can be launched to view the contents of the target machine. At this point, performance monitor can be launched on the host machine, and processor and memory monitoring can be accomplished. Disk monitoring is not possible unless the account that is used is a local administrator account on the target machine. Without service pack one for Windows 2000, disk monitoring can be used with a user account by modifying specific user rights. Service pack one for Windows 2000 adds a new PERFMON.DLL which does not make disk monitoring possible without a local administrator account.

The following diagram shows a logical overview of the network once it leaves the server

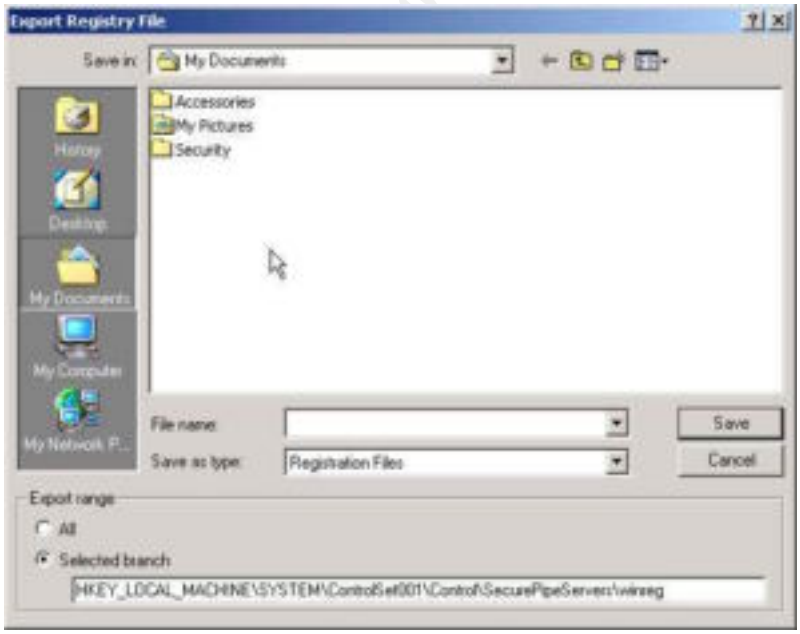



By watching the syslog from the router, we can identify the packets are reaching the intended host. We can also audit the security log on the target machine to see that access has been granted. Further proof is by being able to do processor and memory monitoring.

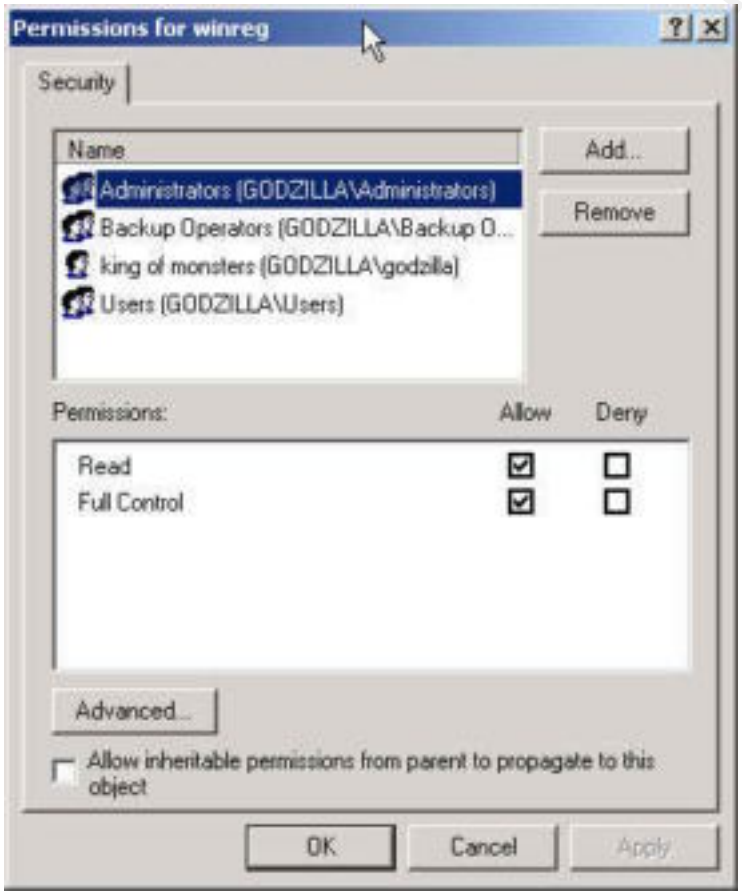
## Setting up a user account on the target machine:

When the NT Server tries to monitor the target machine, it needs to open a NetBIOS session with the target machine. Since it is coming from outside of the network, it needs to have an account in the target machine's SAM database. Below are the steps in creating an account and allowing the correct security access.

1. From the MMC (Microsoft Management Console) open the "local users and groups (local)" snap-in, or if part of a domain, the "active directory users and groups" snap-in
2. Create a new user and make them a member of "users". Fill in the appropriate name and description. Set the password appropriately.
3. Back up the registry. Run the NT backup utility, NTBACKUP.EXE; make sure that the option "system state" is checked. Otherwise the registry will not be backed up.
4. For additional safety, backup the specific key. (Two backups are better than one?) Open the "regedit" (not regedt32, since it cannot export keys) tool from the "run" box in the start menu. From the menu bar, choose "registry" and "export registry file", save this in a secure place. Run this on two keys
    a. HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\SECUREPIPESERVERS\WINREG
    b. HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\PERFLIB
    c. Note that there is a number variable under this key. This is for the language that is chosen. For example, English is 009
5. Note on the bottom of screen is a selected branch

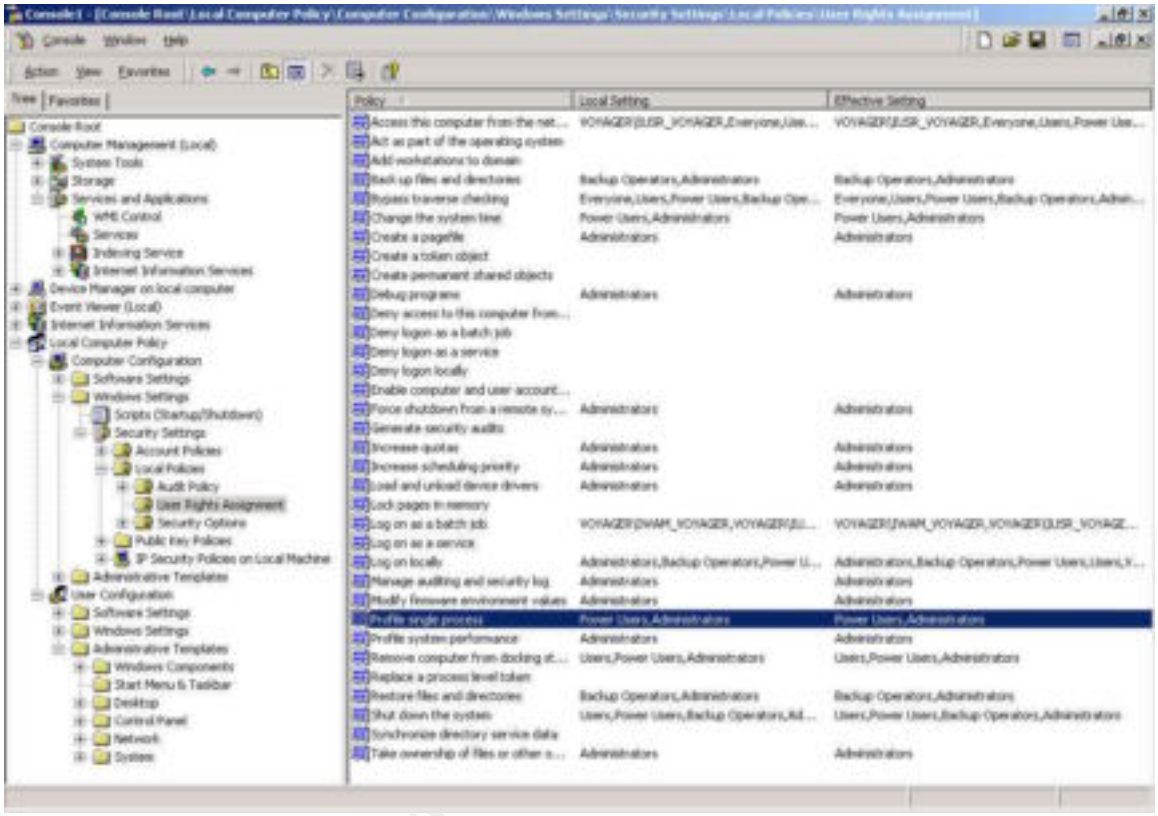


6. Exit the "regedit" tool, and start the "regedt32" tool. Regedt32 is needed, because "regedit" cannot assign security permissions. Start the tool by typing "regedt32" in the run box of the start menu
7. Go to the keys that were just exported
    a. HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\SECUREPIPESERVERS\WINREG
8. Highlight the key, and click on "security" on the menu bar, and select the only option, "permissions"
9. This will bring up the ACL (Access Control List) for that key. Click on the add button, and select the user that was created in step two.
10. Give that user read access to this key, because full control is not needed. Uncheck the box "allow inheritable permissions from parent to propagate to this object". This will make sure that later changes to the registry will not effect monitoring




11. Repeat steps 7 through 10 with:
    a. HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\PERFLIB
12. Access to two files is also required for disk monitoring. These files are PERFC009.DAT and PERFH009.DAT, assuming that the language is English. (009 is for English)

13. These two files are located in the %systemroot%\system 32 directory, which by default is C:\WINNT\SYSTEM32. To apply the permissions, use explorer to open up the C:\ drive and drill down to C:\WINNT\SYSTEM32
14. Use the CTRL key and mouse to highlight the two files
    *NOTE: holding control down allows multiple selects, while SHIFT allows a range*
15. Right-click on the files, and select properties. Then choose the "security" tab. Click on "add" which will bring up the ACL for those files. Add the user that was created in step two. Click OK to apply the permissions
16. Start the hard disk counters by typing "diskperf " at a command prompt. *A variable to this is needed*. Diskperf turns on the disk counters, while the –y turns on both logical and physical counters. Only the disk counters that are going to be used should be turned on, since there is a slight performance hit, but also with the base rule of "less is best".
    a. diskperf –yd will start the counters for physical drives. To turn off the physical disk counters, used the option -nd
    b. diskperf -yv will start the counters for logical drives. To turn off the logical disk counters, used the option –nv
    c. diskperf –y turns on both logical and physical disk counters. –n turns off both physical and logical disk counters
17. Access the security policy from the MMC snap-in "group policy". Open the local computer policy, go to computer configuration, windows settings, security settings, local policies, and user rights assignment. Assign the user created in step two the rights to the policies:
    a. profile a single process
    b. profile system performance



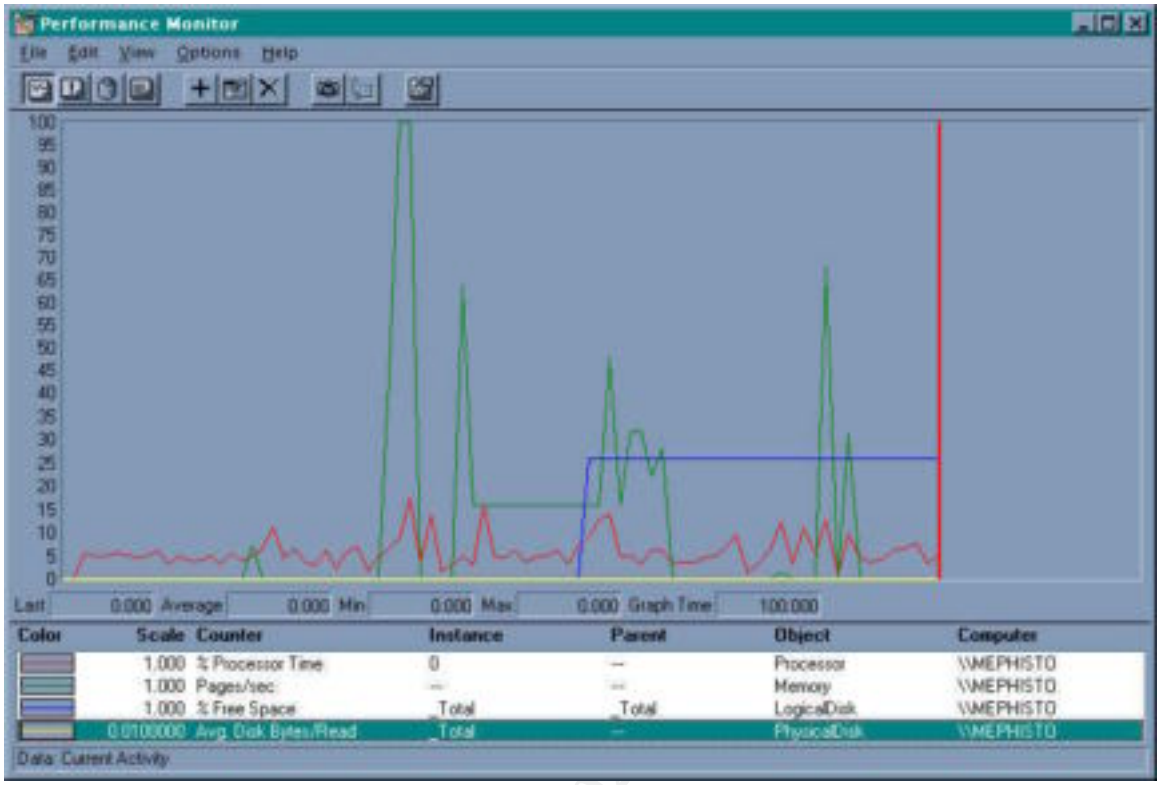
18. This concludes the security preparation for monitoring. Since monitoring in this situation is from a outside party, other security measures, or "server hardening should be taken. Some very basic steps are discussed later in this paper

## Windows NT Performance Monitor

Once a connection has been made from the host machine (Window NT in workgroup doing the monitoring) has been made to the target machine (Windows 2000 in a domain/workgroup) and all preparations have been made, performance monitoring can be done. Start the performance monitor tool from the run box on the start menu or from the command prompt by typing:

***perfmon***

The following tool will open.




1. Click on the plus (+) button to add a monitor.
2. By default, the host machine will come up. Change this in the dialog box, ensuring that the computer name or IP address is proceeded with a (\\). You can also browse for the target machine by clicking on the "….." at the end of the computer line.
3. Select the type of monitor. There is a wide range of choice, but the most popular are:
   - Processor
   - Memory
   - Logical disk
   - IIS Global (if running a web server)
   - Web Service (if running a web server)

While this type of monitoring is efficient over a single point in time, there are better tools to monitor with that can give statistics. One example is SiteScope by Freshwater.

## Third Party Tools - Monitoring

The "company" is using a product called "SiteScope" by Freshwater (http://www.freshwater.com). SiteScope is a Java application that runs on top of the Windows NT operating system for monitoring. It is extremely easy to use, and can be very robust

There are approximately thirty types of monitors available, and can be extremely easy or complex. Some of the monitors are as simple as PING (Packet InterNet Groper) or URL monitoring.

SiteScope runs as an NT service, and can be run under a different context. Since it is written in Java, a most web browsers view the interface. A ten-day trial copy can be downloaded from their web site.

Once installed, SiteScope will open a web browser and build some initial default monitors. One big advantage of this is that the management console can be opened on a web browser of any machine.

SiteScope uses a configuration file to pass username variables. This allows the host machine to make multiple connections with different target machines, without having a person making a connection to each machine manually. In a directory called located under SiteScope called the groups directory is a file called MASTER.CONFIG (C:\SITESCOPE\GROUPS\MASTER.CONFIG). This file contains some of the configuration variable for SiteScope, including a line "_remoteNTMachine". This line can be used to pass a username and password variable that was discussed earlier in this paper "preparing the host machine". The entire line looks like:

*remoteNTMachine*=_host=\\hostname _username=username _password=password

Filled in for testing, it looks like:

remoteNTMachine=_host=\\10.99.5.3 _username=godzilla _password=stompsmashcrush

The master.config files are not encrypted, so NTFS permissions should be applied to the file as to not allow unauthorized access. To apply NTFS permissions to this file, right-click on the file and select properties. Choose the security tab and select only the appropriate users. When assigning permissions to any file, remember the basic rule of "less is best".

SiteScope service can run as a specified user. This can help because then the service is not running as the local system, and gives a little more control over the application. To have a service run as a specified user, open the services applet in the control panel. Choose the "SiteScope" service, and open up the property page.


By default, the service will run as the system account. Change the radial button to "this account" and select the proper user account. Be sure to enter in the password, or "error 1057 – The account name does not exist" will occur. While the account exist, it is invalid since a password is not entered. More information on this can be found in Microsoft TechNet article Q159925.

Go to the directory that SiteScope is located in, and find the MASTER.CONFIG. By default, this should be located in C:\SITESCOPE\GROUPS\MASTER.CONFIG. Apply the change permission to the proper user account. Remove any permission that is not necessary.

Adding Monitors

1. From the top level of the SiteScope interface, click on "create group". Name the group for the system that you are trying to monitor. Click on "add monitor"
2. Select "add ping monitor" under network monitors
3. Enter the host name or IP address. Go to advance options and check "verify error"
4. Click the button "add" monitor. A ping monitor will appear under the newly created group
5. Add a processor monitor. Choose "CPU Monitor" under server monitors
6. Select the appropriate servers. If the correct server is not in the browse list, choose "other" and in the dialog box below, type the computer name or IP address preceded by the double-backslash (\\)
7. Check the verify error button, and click the button "add" monitor. A monitor to watch the processor will appear.
8. Add another monitor. Choose "memory monitor" under server monitors. Repeat steps 6 and 7
9. Add another monitor. Choose disk space monitor. Repeat step 6. Then use the drop down box and select the drive that you would like to monitor. If an administrator account is not given, this box will be blank
10. Check the verify error button, and click the button "add" monitor


11. Create a composite monitor for easy alerts. Choose "composite monitors" under advance monitors. Select the group that all the monitors reside under next to "items". Under the "error if" dialog box at the bottom of the screen, change the default to "items in error" for the first field, greater than or equals to (>=) in the second field, and 3 in the last field. This will cause an alert if three or more monitors fail. Set the error if parameters the same except set the number of monitors to 1


12. Alerts can also be set up to warn administrators. From the main SiteScope page, click on "alerts" button on the top of the screen. Select add new alert.
13. Select the radial button "error" under "on"
14. Select e-mail alert, and then the button "define alert"
15. Select the composite monitor that was set up in step 11. Select the e-mail that the alert needs to be sent to, and the frequency (when)

## Testing Scenario #1:

April 2, 2001 – Windows NT Server in a workgroup monitoring Windows 2000 Professional with an IDE drive. Windows 2000 install is an out of the box, base install with no service packs.

After applying the modifications to the target machine previously discussed in this paper, (registry hack, file permissions, and group policy), the testing was successful. Microsoft TechNet article Q164018 does not mention anything about the group policy modification. Performance monitor did see the drive, and setting up a monitor from SiteScope was also successful. There is an error in the application log on the target machine: **Event ID: 1008 coming from Source: Perflib.** Description of error is:

The Open Procedure for service "perfdisk" in DLL "C:\WINNT\SYSTEM32\PERFDISK.DLL" failed. Performance data for this service will not be available. Status code returned is data DWORD 0

We applied Windows 2000 SP1 and rebooted the system as required. After the reboot, there was an instant alarm from SiteScope stating that there was no data. After verifying the results of SiteScope with performance monitor, we found that a monitoring was not possible.

Microsoft has three TechNet articles (Q259524, Q259525, Q259524) that describe a list of bugs that Windows 2000 service pack one fixes, but does not list specifics.

While analyzing the registry, a key directly linked to performance was found. HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\PERFDISK and the key below it, PERFORMANCE. Permission was given to this key, but no effect on the monitoring.

Auditing the security log on both instances does not show a difference, and does not give any clues to where the error may have occurred:

| Date: 4/24/2001 | Time: 10:24 | Source: Security | Type: Logon/Logoff | Success | Event ID: 540 |
|---|---|---|---|---|---|

Successful Network Logon
User Name: Mothra
Domain: Godzilla
Logon ID: 0x0,0x11ff2
Logon Type: 3
Logon Process: NtLmSsp
Authentication Package: NTLM
Workstation Name: \\NTSERVER

| 4/24/2001 | 10:24 | Security | Privilege Use | Success | 576 |
|---|---|---|---|---|---|

Special privileges assigned to new logon:
UserName:
Domain:
Logon ID 0x0, 0x11ff2
Assigned: SeChangeNotifyPrivilege

## Server Hardening on the Target Machine:

In the last section, securities for performance monitoring steps were taken. Assuming the scenario that monitoring is coming from an outside or third party, certain basic security measures should be taken. This is certainly not an absolute, and the below steps should be review carefully with the system admin responsible for these machines. The last section left off with accessing the user rights assignment under the group policy – local computer policy. Let's review some of the default user rights assignments, and how to modify them. These are not all the policies, but some of the most dangerous ones.

| Policy | Default Access | Suggestion |
|---|---|---|
| Access this computer from the network. | • Backup Operators,<br>• Power Users,<br>• Users,<br>• Everyone,<br>• computer name\IWAM_computername, administrators, computername\IUSR_computername | • Remove the "everyone" access. Everyone is a dangerous group. Everyone is a special group that is not controlled by administrators, but rather any system that can access the system via the network or internet.<br>• If this is not a web server, the accounts "IWAM" & "IUSR" followed by the computer name should not exist. |
| Log on locally | • Administrators<br>• computername\IUSR_computername<br>• Backup Operators<br>• Power Users<br>• Users<br>• Guest | This account can be a security risk because anyone that can log on locally can bypass share permissions, although NTFS permissions are still in effect. Also, many processes<br>• Restrict access to only the people that need it. For example, if this is a server, remove the users/power users if not needed<br>• Remove access for the guest account. Guest account should be disabled if not needed |
| | | |
| | | |

Here are some other very basic tips.

- Verify that the guest account is disabled. This is disabled by default.
- Remove access to the "everyone" group. For example, file permissions and share permissions
- Protect the boot and system partitions by removing the "everyone group" that has full control. Consider replacing this with the "authenticated users" or "domain users" with only read, write and execute permissions.

## Turn on Auditing

Turn on Auditing by adding the "local computer policy" snap-in to the MMC (Microsoft Management Console)

Under Local Computer Policy – Windows Settings – Local Policies – Audit Policy, there are several options for security.

Audit Account Logon Events
Audit Account Management
Audit Directory Service Access
Audit Logon Events
Audit Object Access
Audit Policy Change
Audit Privilege Use
Audit Process Tracking
Audit System Events

These options should be selected carefully, since auditing can be CPU and memory intensive. Audit only events that are necessary. There are two categories on each audit, success and failure. Information from this is recorded in the security section of the event viewer.

The most important part to remember is that the logs should be reviewed periodically. Audits are not helpful if not reviewed in some manner

## Conclusion

Currently, after all our efforts, we are still unable to connect to a Windows 2000 system and perform disk monitoring without administrator rights. While we did find a solution by modifying some group policies, it is clear that Windows 2000 service pack one breaks it. It certainly cannot be acceptable to say that we can perform monitoring as long as we never service pack the system.

Our efforts will continue with the assistance of Microsoft, the analysis of the data from RegMon and FileMon, and we will also attach a system with Microsoft's Network Monitor and try to identify the issue at a packet level.

On the larger scale, it is another reason why most companies have waited to deploy Windows 2000 at an enterprise level. While monitoring from NT4 to Windows 2000 cannot be considered critical, it does prove how little we still know about Microsoft's latest operating system.

## Glossary of Terms:

**ACL – Access Control List** – list used by routers and Windows NT/2000 to determine authorized users and the permissions that each user or account has

**BDC – Backup Domain Controller (BDC)** – works in conjunction with a Primary Domain Controller (PDC). The PDC keeps a master list of accounts that are shared in the domain, and the data is replicated to the BDC

**MMC (Microsoft Management Console)** – a tool introduced in Internet Information Server 4 (IIS4) that provides a single, customizable tool to control the application. This has been adapted to serve all functions of Windows 2000

**Nat/Natted – Network Address Translation** – This is the process of taking a IP address and converting it to another. Typical use of this is taking a non-routable address (10.x.x.x) and changing it to a routable IP address

**NETBIOS – Network Basic Input/Output System** – typically called the computer name, this is a layer 5 protocol of the OSI that helps Windows NT resolve a name to a IP address

**Null Sessions** – Null session, sometimes called a IPC session, is a connection from one system to another without a valid user account

**PDC – Primary Domain Controller (PDC)** – works in conjunction with a Backup Domain Controller (BDC). The PDC keeps a master list of accounts that are shared in the domain, and the data is replicated to the BDC

**PING – Packet InterNet Grouper** – a basic utility to see used to see if a network device is responding.

**RAID – Redundant Array of Inexpensive Disks** – a series of hard drives that are linked together, typically transparent to the system

**RFC – Request for comments** – an international standard

**SAM – Security Accounts Manager** – database used by Windows NT to keep accounts. On a Windows NT in a workgroup, each local machine keeps it's own database. In a domain environment, the SAM is kept on the PDC (Primary Domain Controller) and replicated to the BDC (backup domain controller). Changes can only be made on the PDC.

**SRB – Session Request Block** – A layer six protocol of the OSI that Microsoft Networks use to connect to each other

References:

Microsoft TechNet DVD version, March 2001: MS Windows 2000 TCP/IP Implementation Details

Microsoft TechNet article Q259524: List of Bugs Fixed in Windows 2000 Service Pack 1

Mastering Windows 2000 registry by Peter D. Hipson. Sybex 2000.
ISBN # 0-7821-2615-4

Inside Windows NT Server 4: Certified Administrator's Resource Edition.
ISBN # 1-56205-789-8

Windows NT/2000 Network Security: Eugene Schultz August 2000
ISBN # 1-578870-253-4

Windows 2000 Server Study Guide: (Exam 70-215): Global Knowledge Certification Press
ISBN # 7-83254-03286-6