Global Information Assurance Certification Paper

Developments in Auditing NT

Level Two Practical Requirements for Network Security 2000
Monterey, CA October 2000

Tom Robinette

GCNT

Disclaimer: This paper was written to satisfy GIAC 'Certification in NT Security' requirements. This paper is not intended for use as a comprehensive source for Windows NT Server audits. It is merely a guideline for some of the controls suitable to a medium security level network. As with all information related to Information Systems Security, timeliness is very important, and any network administrator should carefully review current information about Windows NT security.

Built-In user Accounts

Introduction:

Usernames and passwords are the keys to protection for resources accessed over the network. If an attacker is able to obtain or guess the correct username, then the password is the only thing standing between him or her and the resources in question. Since user names are often based on the users real name and or department, guessing usernames may not be difficult. Tools also exist for discovering usernames on systems even remotely. One can almost define network security in whole as the securing of user accounts and their passwords.

Risks:

The administrator and guest accounts are often the target of initial attacks, as they exist by default. The Administrator account is an attractive target because it has the most rights on the network, and as an added bonus, this account cannot be locked out by bad login attempts. If the attacker can gain Administrator privileges he or she can accomplish virtually anything on the network. The Guest account by default does not have the same level of rights on the network, but is still targeted because it often has no password, or an easily guessed password. Even this basic account can give an attacker a springboard from which he or she can launch other attacks and or attempt to escalate permissions.

Best Practice:

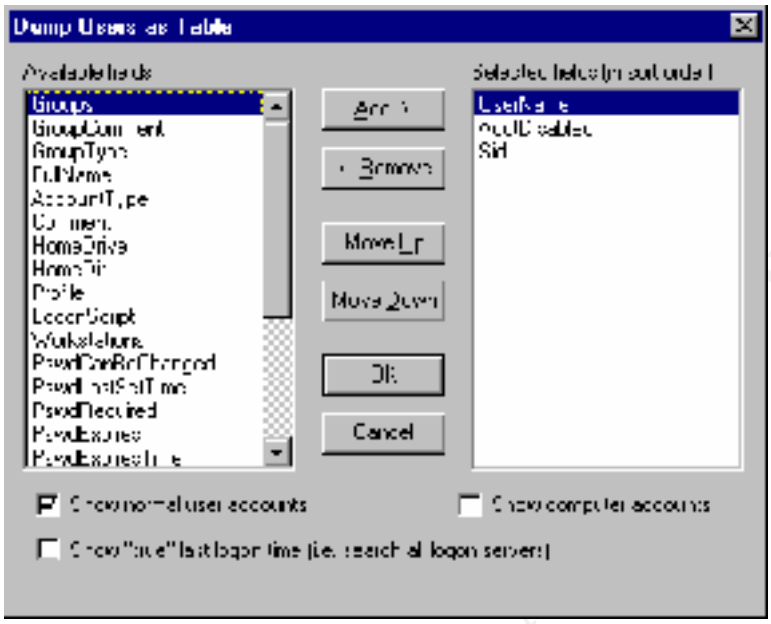
Since Windows NT Server 4.0 comes with two default accounts (Administrator and Guest), the Administrator account should be renamed to something less obvious and the Guest account should be disabled unless it will be used. In addition to disabling the Guest account it should be assigned a password.

Test work:

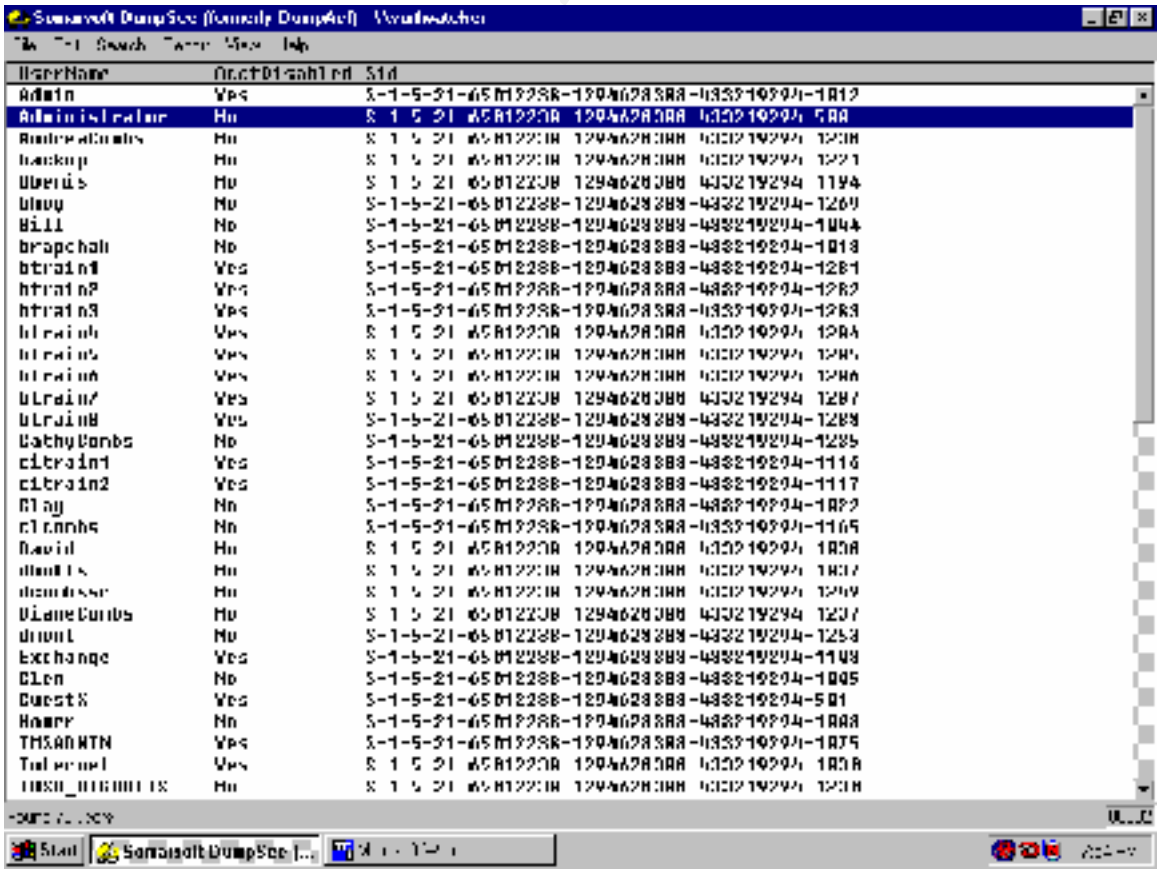
1. Through inquiry determine the status of the two built-in accounts for the domain.
   Administrator states that the Administrator account has not been renamed, but that the guest account was renamed, and disabled.

2. On a domain controller install Somarsoft's DumpSec tool, available from www.somarsoft.com the tool is free. Open DumpSec and choose Report, then

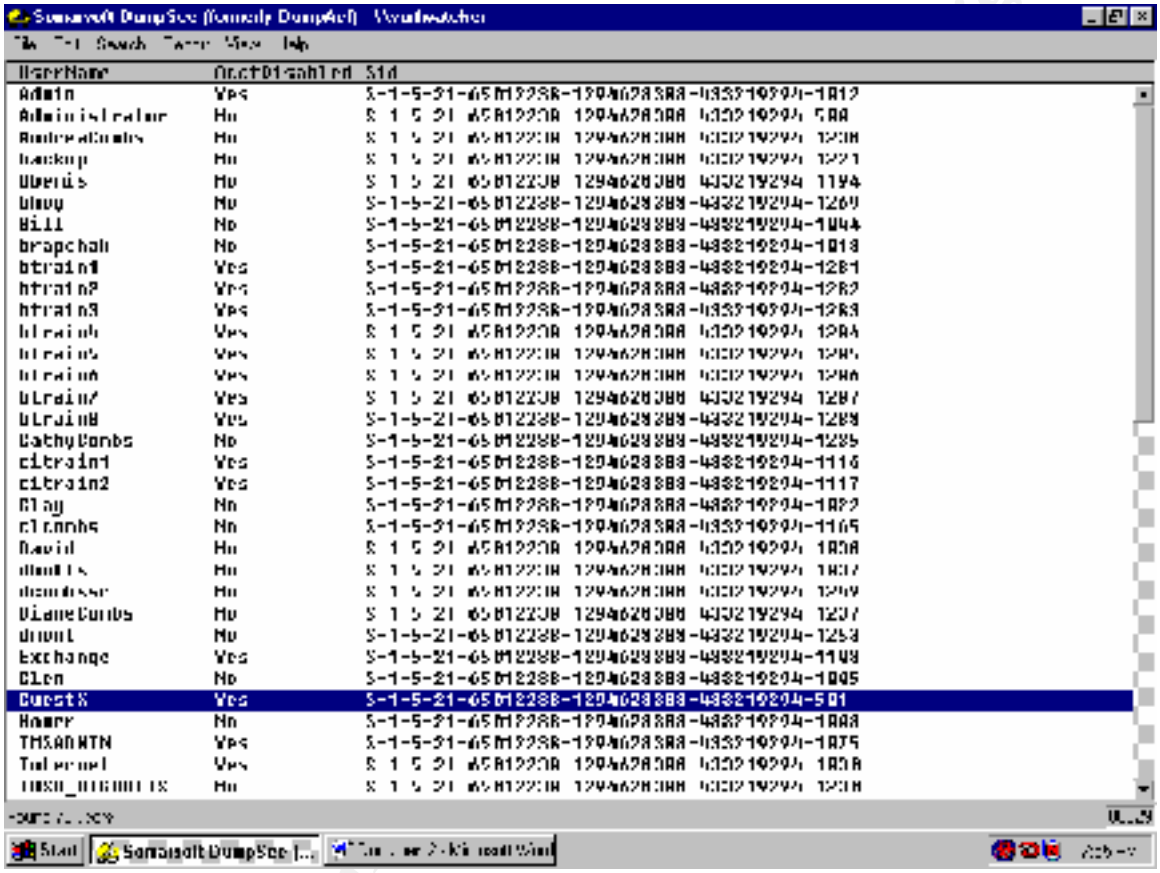
Dump Users as a Table. From the list of Available fields select UserName, AcctDisabled, and SID as shown in the screen shot next:



After clicking on the OK button (In the lower center of the screen above) a report like the following will be generated:



We can tell by looking at this report that the Administrator account (Note that the SID ends with 500) has not been renamed, and has not been disabled. On the other hand if we look lower down to find the built-in Guest account, we see that it has been renamed to GuestX and that it has in fact been disabled. We are able to know which account is the built-in Guest account because its SID ends with 501, as shown in the screenshot below:



Built-In Account	Renamed (Yes or No)	Disabled (Yes or No)	Meets Best Practice Standards (Yes or No)
Administrator	No	No	No
Guest	Yes	Yes	Yes

Conclusion:

Administrator reports that the Administrator password is changed on a regular basis, and that many tools exist to determine the username for the Administrator account even when it has been renamed. While this is true we still recommend renaming the Administrator account. We also verified through the use of L0phtCrack (Discussed in the next section) that the Guest account has a password in addition to being disabled.

Passwords

Introduction:

Assuming that the NetBIOS Session service, has not been disabled, then the single most effective method of attacking Windows NT Server is plain old remote password guessing. In other words, connecting to an enumerated share and trying a username/password combination, until one is found that grants access (Source: Hacking Exposed, Second Edition, Network Security Secrets and Solutions)

Risks:

Unauthorized access to system resources and data, including tampering with or destroying the information on your network.

Best Practice:

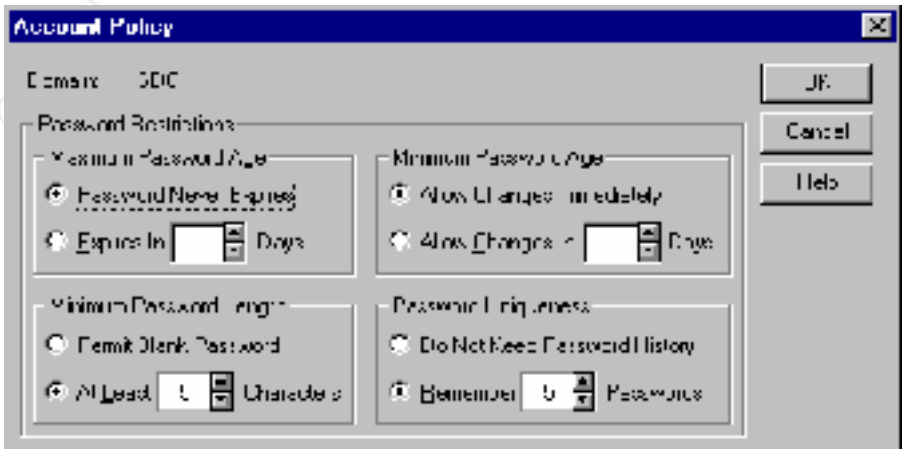
A password policy should be developed implemented and verified. This policy should include rules for minimum password length, password complexity and maximum password age. Windows NT 4.0 SP3 and later includes an optional password filter which can require complex passwords, and other third party tools are also available.

Test work:

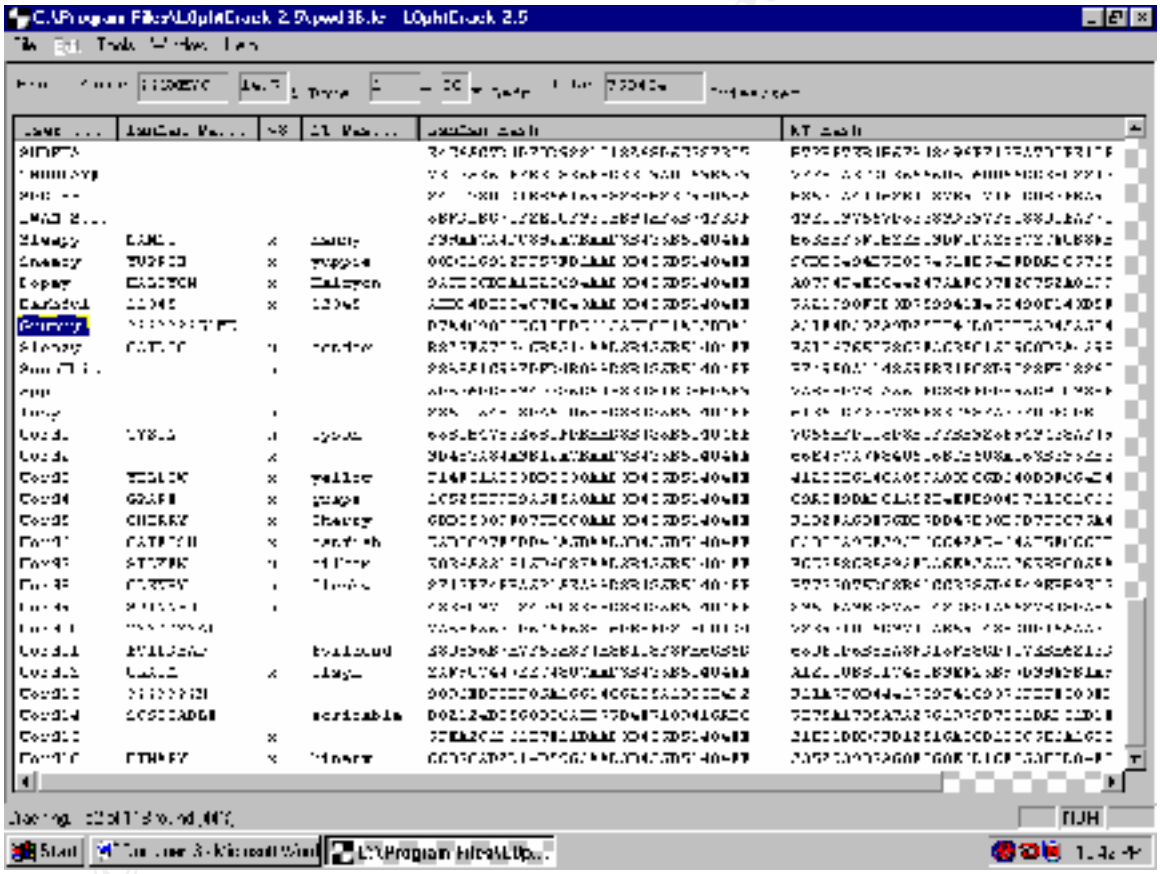
1. Through inquiry determine if a password policy exists and what the details are of this policy with respect to password length, complexity, and age.

   Administrator states that there is no maximum password age, that each password is required to be at least 5 characters in length and that he uses L0phtCrack to periodically test for password complexity.

2. On a Domain Controller open User Manager for Domains and click on Policies. Screenshot next:



3. On a Domain Controller install the L0phtCrack NT password Cracker available from www.l0pht.com . This tool allows an administrator to evaluate the strength of passwords on the Domain. While logged on as the Domain Administrator or equivalent you can dump the password Hashes directly from the registry and then begin cracking them. It should be noted that there are other ways to obtain the password hashes, and this tool could be used by malicious individuals to obtain passwords for accounts they are not authorized to use. The L0phtCrack tool takes advantage of weaknesses in the older LANMAN hashes. First it splits each password into two 7 character passwords and attacks each one individually. Also the LANMAN hash does not allow for lowercase characters and this reduces the number of combinations that must be attempted during a brute force attack. Screenshot of L0phtCrack below:

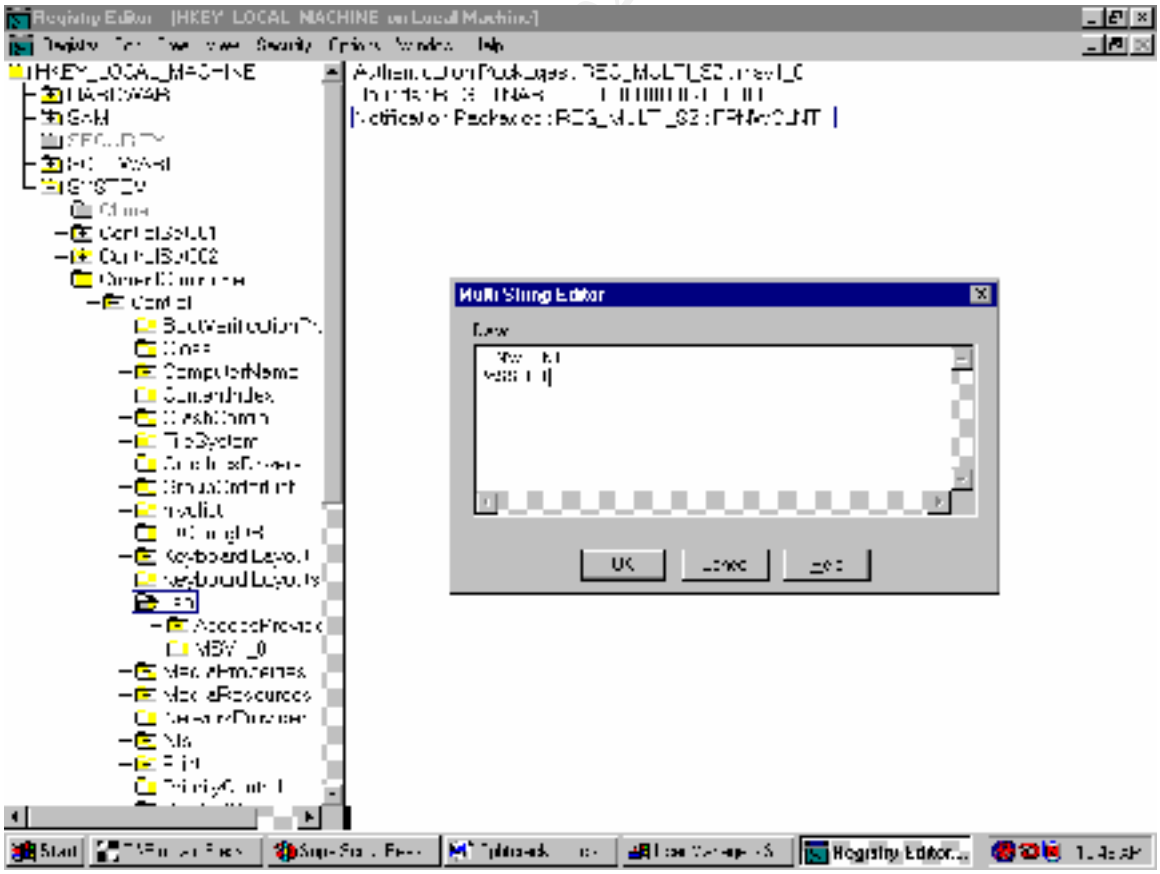


As you can tell from the screenshot, a tool like L0phtCrack can make very quick work of simple passwords. After running for only a few seconds it has found nearly half the passwords in the domain and will have finished a brute force attack in less than 3 hours.

Domain Name	Minimum Password Length	Minimum Password Complexity	Maximum Password Age	Compensating Controls present
SDGI	5 Characters	Stated Policy does not meet Best Practice	None	L0phtCrack is used to test Password complexity on an approximately monthly basis

Conclusion:

While L0phtCrack is a very useful tool for testing the strength of NT passwords, a tool such as PASSFILT.DLL available on Windows NT SP 3 and higher gives a network administrator the ability to manage password policies in a much more structured manner. This is especially important on larger networks. In order to install PASSFILT.DLL you should open REGEDT32 on the Domain Controller and browse to the Notification Packages shown below: Add the Value PASSFILT, close REGEDT32 and reboot.



Further recommendations include: Increasing the password length to 8 characters and setting passwords to expire in 45 days. These setting can be changed on a Domain Controller by opening User Manager for Domains and then clicking on Policies, and then clicking on Account. It should be noted that simply installing PASSFILT.DLL does not affect the passwords already in existence on the Domain, and unless those passwords are set to expire they will not be affected by the installation of PASSFILT.DLL until the next time the passwords are changed (Source: Heckendorn, Sherri, SANS GCNT Certification Practical).

Service Packs

Introduction:

"Service packs are the means by which Windows NT product updates are distributed. Service packs keep the product current, and extend and update your computer's functionality. Service packs include updates, system administration tools, drivers, and additional components. ... Service packs are cumulative – each new service pack contains all the fixes in previous service packs, as well as any new fixes. You do not need to install a previous service pack before you install the latest one." (Source: How to Obtain the Latest Windows NT 4.0 Service Pack, Microsoft Knowledge Base Article ID Q152734)

Risks:

Microsoft publishes fixes to security holes, and Denial of Service attacks, and then bundles them together into Service packs along with other components. Because of Windows NT's complexity these ongoing updates; which occur as the OS is exposed to attack over a period of time, are perhaps the second best way (after installing a perimeter Firewall) to protect your system from Known Security Vulnerabilities and Denial of Service attacks.

Best Practices:

Your NT servers should all be brought up to the most recently available Service Pack level as soon as possible, but it is very important that these new Service Pack's be tested in a Non-Production environment first, to ensure that they will not cause unforeseen problems on the network.

Test work:

1. For the Domain Controllers on the network run the Winver.exe program located in the \\systemroot\system32 subdirectory. Click on Start, then run, then type winver.exe and press enter. A screen similar to the one shown below should appear. Note that the Service Pack level along with the version number of the Operating System and the Memory available to the Operating System are all shown on this screen. Screenshot next:

At the time of this writing, Service pack 6a was the most up to date Service Pack available for Windows NT 4.0 Server.

Server Name	Service Pack Installed	Control in Place to Monitor new Service Pack Releases?
SURFWATCHER	Revised Service Pack 6a	Administrator receives TechNet Subscription from Microsoft Corporation, which includes new Service Packs upon release.

Conclusion:

A policy of testing the Service packs on non-production machines was not well defined, and the Administrator knew of times when installing the latest available service pack had cause unforeseen problems. With this knowledge we recommend that all new Service Packs be tested on non-production machines before being placed into production environments.

Modems

Introduction:

When users connect modems to their workstations, they have created another avenue into the network, which may completely bypass all the other security controls in place on a network.

Risks:

Attackers can use wardialers to search for and identify modems attacked to computers. Once these modem numbers are identified the attacker will have another way to attack the system.

Best Practices:

Define a company wide policy on the use of Modems on individual workstations, and whenever possible do not allow individual modems on the network. In the cases where a demonstrable need exists, do not use phone numbers within the same block as published phone numbers for the company and leave the modems turned off or unplugged unless they are actually in use, or need to be in use.

Test work:

1. Determine through inquire which workstations need modems.
   Administrator states, that the only modems on network client machines are on laptop computers and than none of them should be connected to an analog phone line at any time. Administrator further states that he controls access to the only analog phone lines in the company and only connects them when a specific need arises. He is aware of cellular technology which would allow users to connect to the Internet without the use of an analog line but this risk is deemed miniscule.

2. Visually inspect workstations to determine which if any have modems and whether they are attached to phone lines.

Domain username for Primary User	Machine Serial Number	Is Modem Present (Yes/No)	Is Modem attached to functioning phone line (Yes/No)
Papa	6822BW27L333	No	No
Smurfette	6822BW27L346	No	No
Brainy	6822BW27L291	No	No
Grouchy	6822BW27J462	Yes	No

Gargamel	6822BW27L398	No	No
Happy	6822BW27L316	Yes	No
Azrial	6822BW27J461	No	No

Conclusion:

While controls are not in place to ensure that the stated policy remains in effect, the stated policy does conform to best practices, and no further action is necessary other than periodically verifying that users with modems do not have easy access to phone lines that the Administrator is unaware of.

Audit Logs

Introduction:

One of the most important steps in detecting intruders or other unauthorized activity is to enable audit logs within NT 4.0. Auditing is not enabled by default in NT server and must be enabled. Of course merely turning auditing on is not sufficient; there must also be a mechanism in place for reviewing the logs.

Risks:

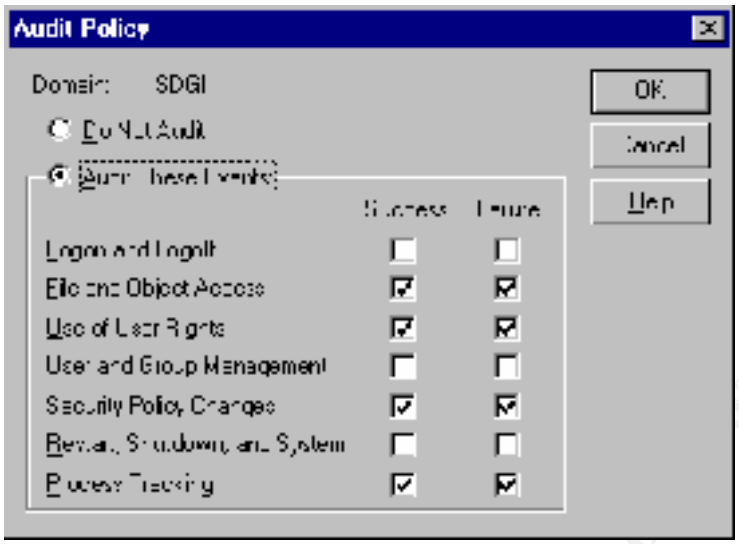
First you have to decide which events to audit and then whether to audit success or failure or both for each event. If you choose too many events, you may lose valuable information under a sea of unnecessary events. If on the other hand you do not audit enough events, then the useful information may never be recorded in the first place. Another risk lies in how well you can protect the logs after they have been generated. An attacker may attempt to fill the log files up in order to cause your system to hang or stop responding, or if the attacker gains sufficient rights on your network, he or she may attempt to change or delete individual entries or the entire log file.

Best Practices:

See table below (In Test work Section) for best practices for Medium Security Network. (Source: Windows Security Step-by-Step. The SANS Institute)

Test work:

On a domain controller (Logged in as Administrator or equivalent) open User Manager for Domains, click on Polices, and then Audit. The next Screenshot shows the result:

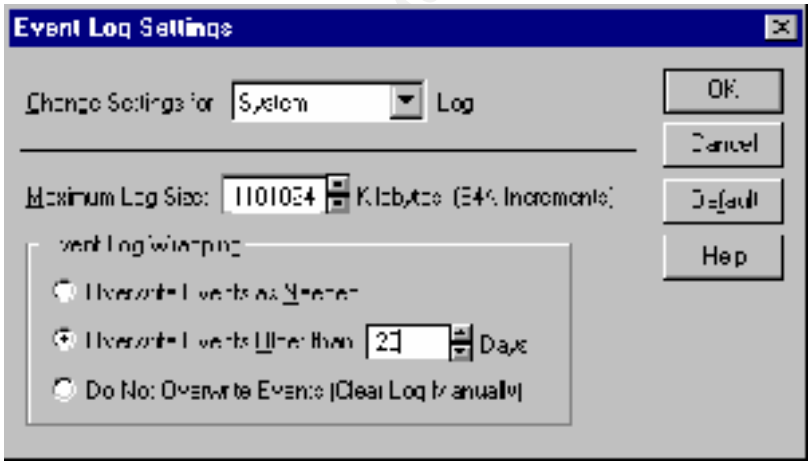


Event to be Audited	Stated Policy from Inquiry to Network Administrator	Best Practice from SANS Windows NT Security Step-by-Step	Value discovered in Testing	Comments
Logon and Logoff Success	Disabled	Enabled	Disabled	Complies with stated policy but the stated policy does not meet Best Practice.
Logon and Logoff Failure	Disabled	Enabled	Disabled	Complies with stated policy but the stated policy does not meet Best Practice.
File and Object Access Success	Enabled	Disabled	Enabled	Complies with stated policy but the stated policy does not meet Best Practice.
File and Object Access Failure	Enabled	Enabled	Enabled	
Use of User Rights Success	Enabled	Disabled	Enabled	Exceeds Best Practice
Use of User Rights Failure	Enabled	Enabled	Enabled	
User and Group Management Success	Disabled	Disabled	Disabled	
User and Group Management Failure	Disabled	Disabled	Disabled	
Security Policy	Enabled	Enabled	Enabled	

Changes Success				
Security Policy Changes Failure	Enabled	Enabled	Enabled	
Restart, Shutdown, and System Success	Disabled	Enabled	Disabled	Complies with stated policy but the stated policy does not meet Best Practice.
Restart, Shutdown, and System Failure	Disabled	Enabled	Disabled	Complies with stated policy but the stated policy does not meet Best Practice.
Process Tracking Success	Enabled	Disabled	Enabled	Exceeds Best Practice
Process Tracking Failure	Enabled	Disabled	Enabled	Exceeds Best Practice

Conclusion:

The Audit events which are not being monitored to the level suggested as Best Practice for a medium security network should be escalated to that minimum level. Policies should also be in place for how large these logs are allowed to grow, and what happens when the log reaches its maximum size. If the log overwrites older data you may lose log entries before they can be reviewed, but if you don't allow the log entries to wrap, then an attacker may use this as a denial of service attack. The recommendation is to have sufficient space for log entries to give you time to move them to a more permanent storage device. In order to set the configuration options for the size and wrapping of the logs open the event viewer from the Administrative Tools folder. Click on Log, and then click on Log Settings. Screenshot below:



Hotfixes

Introduction:

While the subject of Hotfixes is undeniably related to Service packs discussed above, there are key differences which warrant individual attention. Hotfixes, are released by Microsoft in order to fix bugs, or close security holes which cannot wait for the next Service pack release. Typically many of these Hotfixes are bundled together to form a service pack.

Risks:

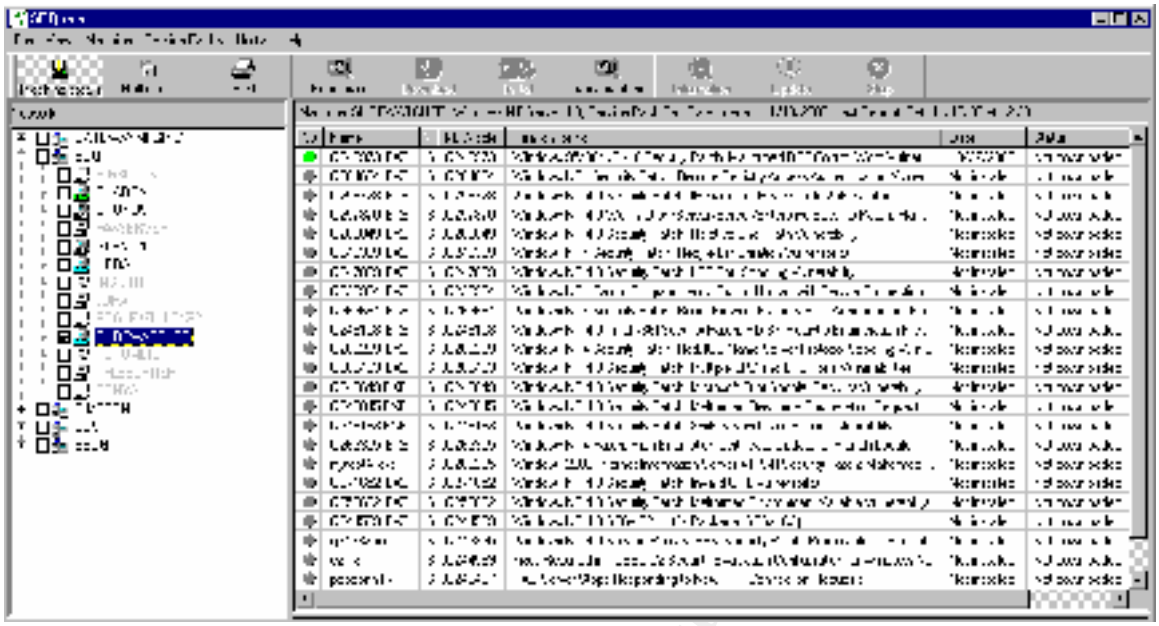
Hotfixes are not nearly as thoroughly tested as Service packs, and even Service packs sometimes have unexpected results. Consider the following statement from a Microsoft Hotfix: (This is typically found on virtually all Hotfixes, especially when they first come out) 'Emphasis added'

> A supported fix that corrects this problem is now available from Microsoft, but it has not been fully regression tested and should be applied only to computers that are experiencing this specific problem. If you are not severely affected by this specific problem, Microsoft recommends that you wait for the next Windows NT 4.0 service pack that contains this fix.

As you can tell from the statement, you should be very cautious about applying Hotfixes, and only apply them after they have been tested on non-production machines. The network administrator must then make a decision about whether to apply Hotfixes based on the perceived threat the Hotfix is patching.

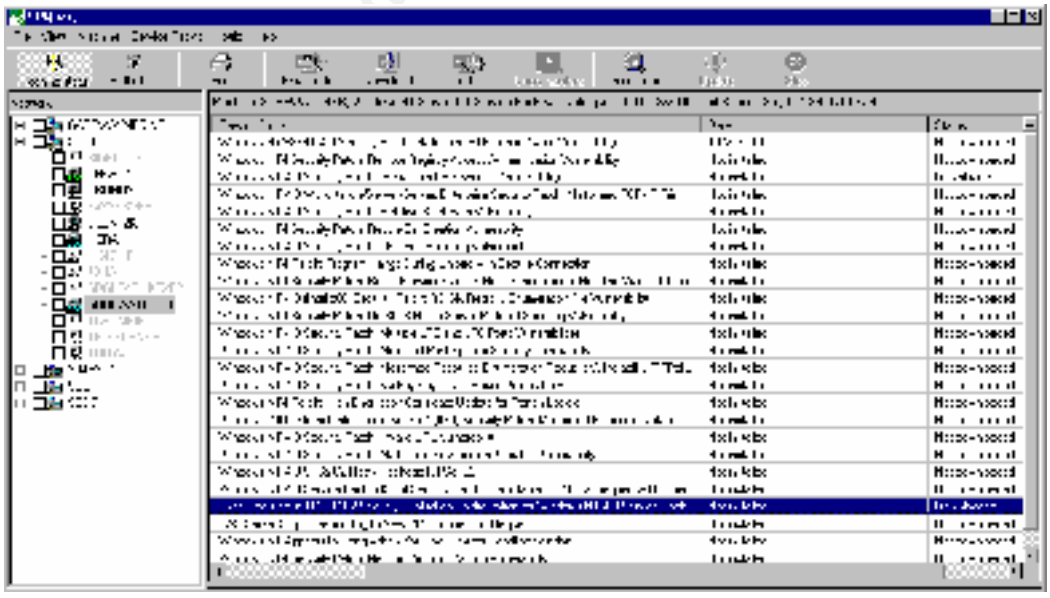
Best Practices:

Many Hotfixes fix security vulnerabilities that should be addressed as quickly as possible, so it may not be possible to wait for the Service pack release to apply the patch to your system. Therefore the best practice is to review all the Hotfixes available for the current Service pack release you have in Production and decide which if any of them should be applied immediately. Third party tools are available to help Administrators track, research and apply Hotfixes to NT servers. One such tool is called SPQuery, and is available from St. Bernard Software (http://www.stbernard.com). This tool allows administrators to remotely check which hotfixes are applied on servers, research hotfixes on Microsoft's website, and even download and apply the hotfixes to remote servers. After installing the product on the management workstation, you merely select the domain and then the specific machine or group of machines you are interested in then click the Query Machine button. The output which is generated (shown below) lists all the available Hotfixes for the service pack level running on the machine, and whether or not that particular Hotfix has been applied. In the example below only the first Hotfix has been applied. Highlighting any of the Hotfixes and clicking the Hotfix Info button opens a window to Microsoft's technical support database which contains the most current information about the hotfix.

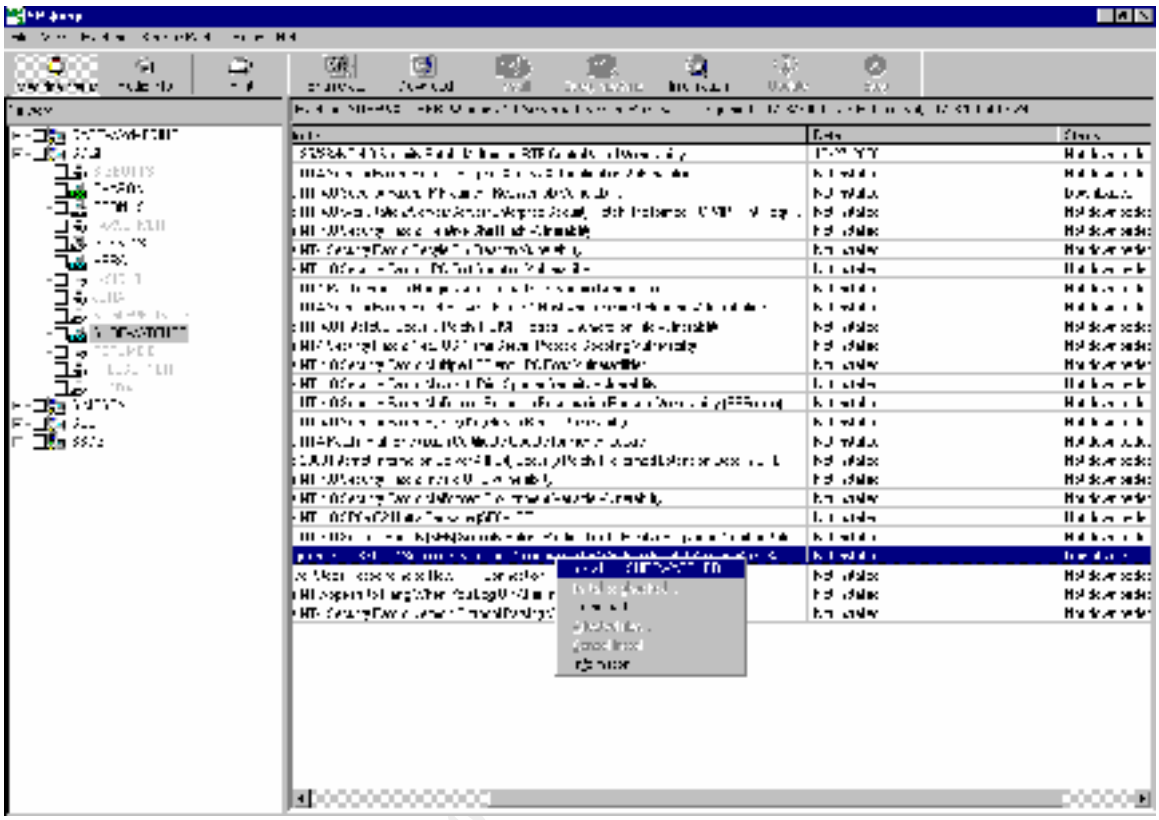


After gathering the information on the Hotfix, you can elect to download it into the SPQuery database, at which time it will be available to install on any of the remote machines. SPQuery is also updated automatically so its list of available hotfixes remains current.

In order to install a hotfix on a remote machine you must first download the hotfix in question. This is accomplished by right clicking on the Hotfix and choosing download. SPQuery automatically downloads the hotfix from the Microsoft FTP site, and places it in its download database. It then shows that the Hotfix is downloaded:



When you are ready to apply the hotfix to a remote machine simply click on the machine in the left pane, and then right click on the hotfix in the right pane, and then choose "Install to..[machine_name]" as shown in the screenshot below:



Test work:

Generate Report from SPQuery and compare it to the list the Administrator keeps of Hotfixes which should be applied to the NT servers. The Administrator generates his list of Hotfixes to apply based on researching the available hotfixes listed in SPQuery and reading his subscription to the Microsoft Security Bulletin. You can subscribe to this service by following these steps: (The following taken from the Microsoft Website, http://www.microsoft.com/technet/security/notify.asp)

1. **Compose an e-mail to microsoft_security-subscribe-request@announce.microsoft.com. The subject line and the message body are not used to process the subscription request, and can be anything you like.**
2. **Send the e-mail.**
3. **You'll receive a response, asking you to verify that you really want to subscribe. Compose a reply, and put "OK" in the message body. (Without the quotes). Send the reply**
4. **You'll receive two e-mails, one telling you that you've been added to the subscriber list, and the other with more information on the notification the**

service and its purpose. You'll receive security notifications whenever we send them.

Conclusion:

Once a hotfix is identified as one that should be applied to a server, it is then tested on a Non-Production machine, and only then placed on the list to be applied to the Production machines, using SPQuery. The Microsoft Security Bulletin is an excellent way to keep up to date with the Hotfixes available for a particular Service Pack. The stated policy for this section is above and beyond the best practice recommendation and is working as intended.

References

Fossen, Jason; Kolde, Jennifer. Securing Windows NT, Step-by-Step, Parts 1-3. The SANS Institute GIAC Training 2000.

Heckendorn, Sherri, SANS GCNT Practical. The SANS Institute. Available Online at http://www.sans.org/y2k/practical/Sherri_Heckendorn.doc

"How to Obtain the Latest Windows NT 4.0 Service pack." Microsoft Knowledge Base Article ID: Q152734. Available Online at http://support.microsoft.com

McDowall, Tracey. Developments in Auditing NT. SANS GCNT Practical. The SANS Institute. Available Online at http://www.sans.org/y2k/practical/Tracey_McDowall.doc

Scambray, Joel; McClure, Stuart; Kurtz, George. Hacking Exposed, Second Edition, Network Security Secrets & Solutions. Osborne/McGraw-Hill, 2001.

Schultz, E. Eugene. Windows NT/2000 Network Security. Macmillan Technical Publishing. 2000.

Windows Security Step-by-Step. The SANS Institute, 1999. Available online at http://www.sans.org