Global Information Assurance Certification Paper

Limiting Anonymous Logon/Network Access To Named Pipes and Shares

June 8, 2000

Author: **John W. Albright**
S1399134

Table of Contents

Table of Figures

1. Introduction

Anonymity, that's what a cracker/hacker wants while they ply their trade against their target. Whereas, the target also wishes to have their resources remain out of the limelight of prying eyes while providing a dependable service to their legitimate users. But this very act of providing a service in and of itself opens up a window of opportunity that someone could exploit. Just the mere fact of using a service can give someone enough information to make an educated guess about your system's Operating System (OS), your naming standards for user identifications (IDs) or System names, or even what version of the service you are providing. So the key to someone cracking into a system is basically information. The more information an attacker has about your site, the easier it may be for them to enter your system without you knowing that they have been there.

The challenge to every systems administrator is to provide access to a system while still restricting access to and maintaining the integrity of specific data stores. Securing a system requires knowledge of each access area available to a hacker and the ability to apply a process that blocks access to specified restricted areas. The challenge for the manufacturer of the Operating System (OS), on the other hand, is to provide a generic solution to meet everyone's needs, while trying to provide backward compatibility with their previous or existing products. This backward compatibility is great for companies who don't want to lose their initial investment in what they currently have, but for the OS to support this, sometimes vulnerabilities are knowingly or unknowingly opened up in the OS.

Microsoft Windows NT 4.0 provides a would-be attacker with one of these opportunities/methods right out of the box. The method we will be discussing here is limiting the use of null sessions, as well as restricting the use of anonymous logins which can permit an anonymous user or "NULL" user from gaining access to your system.

2. Scope & Intent

The guidelines put forth in this document will describe how to make four (4) changes to the registry file in a Microsoft Windows NT 4.0 environment to help prevent null sessions from listing out user accounts or shares, limiting null access to named pipes and shares. Most publications gloss over the topic of Inter-Process Communication (IPC) mechanisms which allow an anonymous connection to a server[1]. Nor do they describe the named pipes and shares other than that the default entrees should be deleted.

There are many aspects of securing Windows NT contained within the product, as well as third-party solutions[2]. Unfortunately, security is often deferred until the latter part of a system's life cycle for a number of reasons, usually after a site has already been established and the staff becomes more technically proficient, or a system has been compromised.

Our job is to make it as difficult as possible to deter or distract an attacker from attacking our site while providing services to our users. All of which still needs to be balanced between allotted budgets, manpower, system usability, and the threat our systems face. Obviously, the decisions made depend on where the system is located and how the system is going to be used. Systems that are accessible via the Internet will require more stringent security measures than some of the systems tucked behind the corporate firewall.

An example of an internal system that may be considered a modest risk (by letting someone list out user names) is one running Microsoft Exchange server (mail server). Often some companies will use their Exchange servers to authenticate user IDs in an NT environment. Since large organizations have people spread out over a vast area, most companies provide a method to look up a person on line. The information could include how to contact them, where they are located, the hours they work, and in some cases they also provide an alias for that person. In some cases, the alias that has been assigned to a person could be a unique identifier that the company uses as a corporate logon ID. This corporate logon ID allows the user to use a single ID to log onto any of the systems the user has access to within the company or, in some cases, the company's customers systems. And typically, if a site uses this approach, then the site is probably using a software package to synchronize the user's passwords across all the systems so that the user only has to remember one password.

So the guidelines presented here are pretty straight forward and do not require anything more then what comes with Windows NT to implement. Although one of the steps presented in this document uses a command that only comes with the Microsoft Windows

[1] See [Gonc98] pp. 260 - 261 section 13.3 NT versus UNIX: A Security Perspective.

[2] There are several third-party solutions available on the market today for all budget types. An example of a well rounded product is CA's Unicenter TNG which not only provides an improved security package but will help manage your system if configured correctly. For a more intimate look at Unicenter, see [Stur98].

NT Resource Kit, it is still possible to use the commands that come with Windows NT to perform the same task.

But considerable judgment and testing should be used before implementing any of these changes in a production environment because these changes could cause some services to fail or crash the system if not done properly. This document is in no way a complete discussion on the topic of securing a system[3]. What is presented here is one small aspect of securing a system and it will only present the most rudimentary information on why the changes are being made, in this case, the limiting of null access to a Primary Domain Controller.

[3] See [TechNet] URL: http://www.microsoft.com/TechNet/security/dccklst.asp for the article entitled "Windows NT 4.0 Domain Controller Configuration Checklist".

3. Test Environment

Although each site will have its unique setup and requirements, the following exercises will show just a small sample of what an anonymous connection can reveal about a site. The testing environment will involve three (3) systems and two (2) domains. The first system will act as a Primary Domain Controller (PDC) for the domain called "Master Domain" which will be used to authenticate the user IDs at this site. The second system will be the PDC for the "Resource Domain" and will control access to all the resources contained within the resource domain. The last system will be a standalone system that is not part of either domain and will be used to probe the other systems. This "Master Domain Model" (See Figure 1) will contain a one-way trust relationship between the resource domain (Trusting Domain) and the master domain (Trusted Domain). This section will not be very verbose in any descriptions of the screen shots provided. The purpose is to show some basic techniques for gathering information about a system and it will be left up to the reader's own devices to expand their knowledge on what they see within this section.

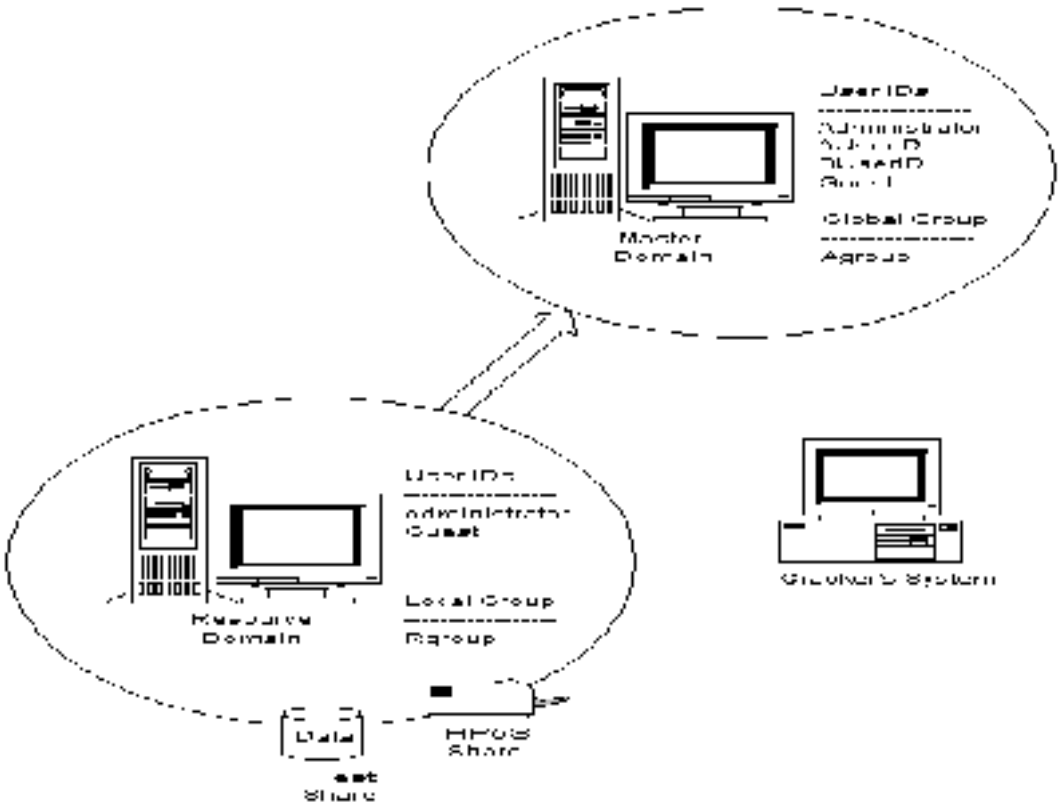

Figure 1 Master Domain Model.

Software Install

The following software was loaded on all systems with the default settings except where noted in Figures 2 through 4:

Microsoft, Windows NT Version 4.0 (Build 1381)
Microsoft, Windows NT 4.0 Service Pack 4
Microsoft, Windows NT Server Resource Kit 4.0 Supplement 3
Software Excellence By Design, Inc., "GrabIt Professional™, Version 6.02[4]
HP, HP JetAdmin, Version 3.42[5]
Pedestal Software LLC, NTUser.exe[6]

Partition Type	Format the partition using the NTFS file system
Name and Organization	Name: Sans Organization: Practical Assignment
Licensing Modes:	Per Server for: 50
Computer Name:	APDC
Server Type:	Primary Domain Controller
Administrator Account:	Password: apdc
IIS	Unchecked Install Microsoft Internet Information Server
Network Protocols	Unchecked NWLink IPX/SPX Compatible Transport
Microsoft TCP/IP Properties	IP Address: 192.168.0.1 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.0.1
Domain Controller	Domain: MASTER
Display Properties	Desktop Area: 800 by 600 pixels

Figure 2 Master Domain's Primary Domain Controller.

[4] A demo copy of "GrabIt Professional™ Version 6.02 from Software Excellence By Design, Inc. was loaded on each workstation to capture the images used within this document.
[5] The HP JetAdmin software was only loaded on the resource domain PDC to share out a printer.
[6] The command NTUser.exe was only added to the C drive of the standalone server.

Partition Type	Format the partition using the NTFS file system
Name and Organization	Name: Sans Organization: Practical Assignment
Licensing Modes:	Per Server for: 50
Computer Name:	RPDC
Server Type:	Primary Domain Controller
Administrator Account:	Password: rpdc
IIS	Unchecked Install Microsoft Internet Information Server
Network Protocols	Unchecked NWLink IPX/SPX Compatible Transport
Microsoft TCP/IP Properties	IP Address: 192.168.0.2 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.0.1
Domain Controller	Domain: RESOURCE
Display Properties	Desktop Area: 800 by 600 pixels

Figure 3 Resource Domain's Primary Domain Controller.

Partition Type	Format the partition using the NTFS file system
Name and Organization	Name: Sans Organization: Practical Assignment
Licensing Modes:	Per Server for: 50
Computer Name:	CRACKER
Server Type:	Stand-Alone Server
Administrator Account:	Password: hack
IIS	Unchecked Install Microsoft Internet Information Server
Network Protocols	Unchecked NWLink IPX/SPX Compatible Transport
Microsoft TCP/IP Properties	IP Address: 192.168.0.3 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.0.1
Domain Controller	Workgroup: HACKTHEPLANET
Display Properties	Desktop Area: 800 by 600 pixels

Figure 4 Standalone System.

User IDs

Two (2) IDs were created on the master domain. The default settings were used in the creation of the IDs "AUserID" and "BUserID". The user ID, "AuserID", was also granted access to use Remote Access Servers (RAS) in addition to the default settings. Both IDs were added to a global group called "Agroup" on the master domain. In the resource domain, a local group "Rgroup", was created; then the global group[7], "Agroup", from the master domain was added to the local group, "Rgroup".

Shares

The printer on the resource domain was shared out as "HP5Si" and a directory called "Test" was also shared out on the resource domain. Again, all default values were used in the creation of these resources. Next, the local group "Rgroup" was given the access "Full Control" on the "Test" share and the "Everyone" group was removed from the "Test" share.

Setting up auditing

The following figure shows how auditing was setup for this test on both PDCs.

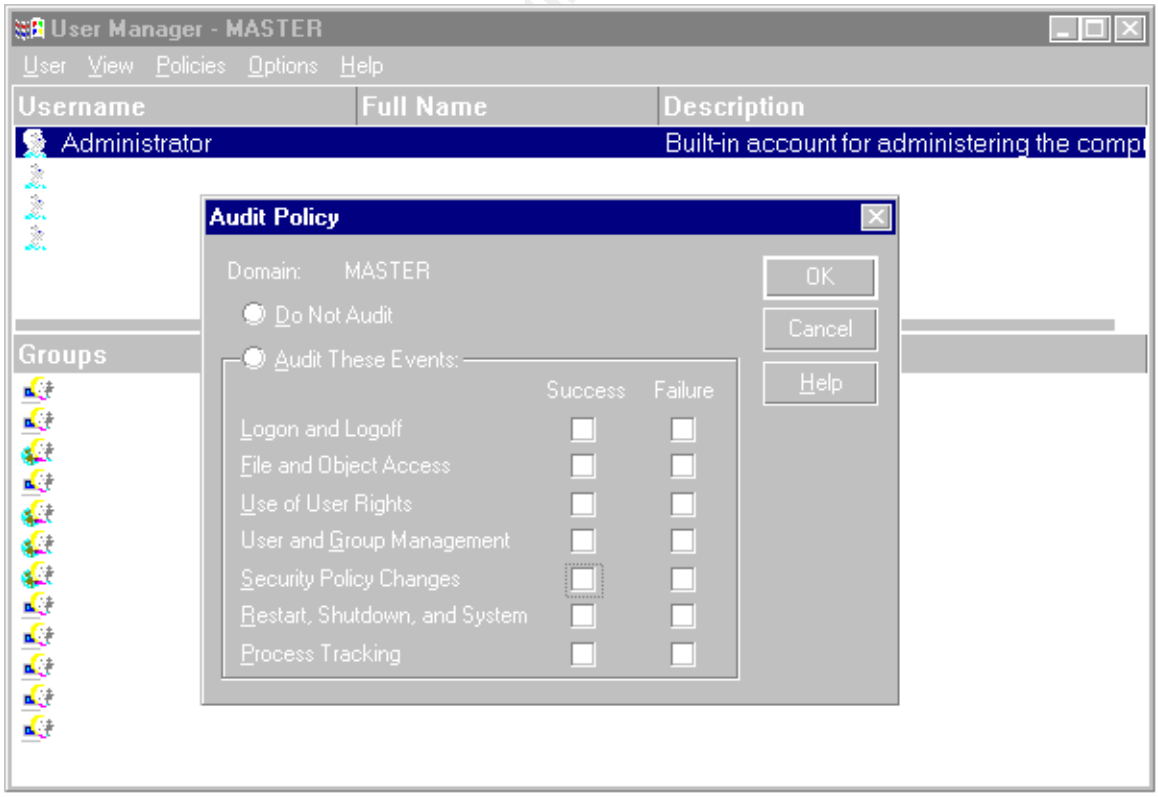

Figure 5 Enabling Auditing.

[7] See [Hadf97] pp. 147 – 151 for a description on adding local/global groups in a master domain model.

Testing Before PDC(s) are Locked Down

Using the Nbtstat Command

This will not trigger a security event.

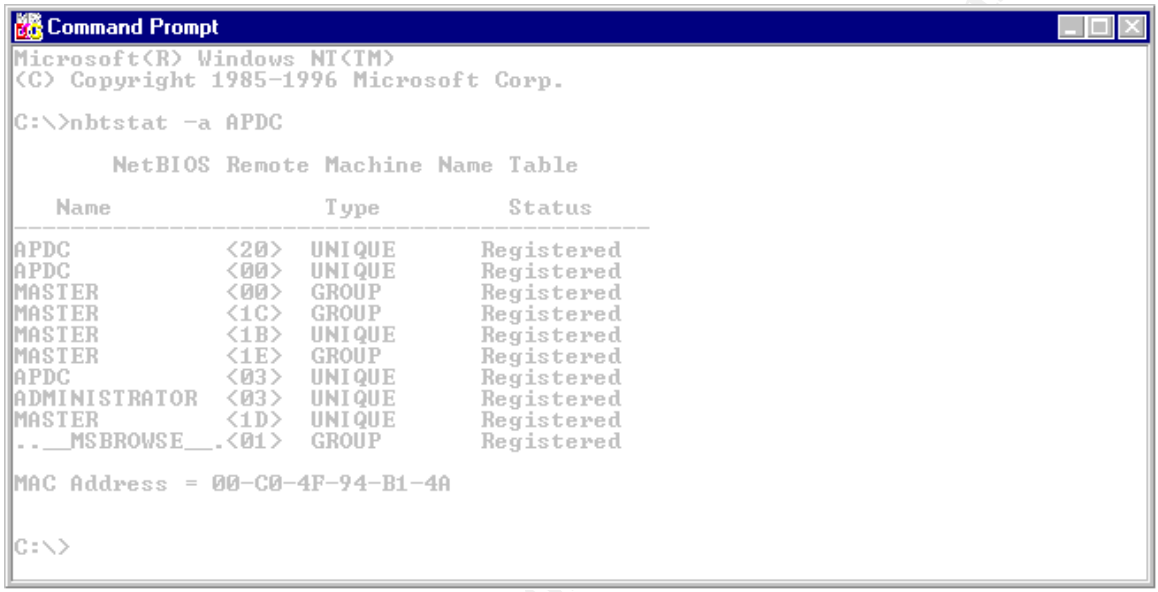

Figure 6 NetBIOS Remote Machine Name Table.

Using the Net View Command

Only the "net view" command used outside a null session will trigger a security event (See Figure 8). The null session connect/disconnect will not trigger a security event.

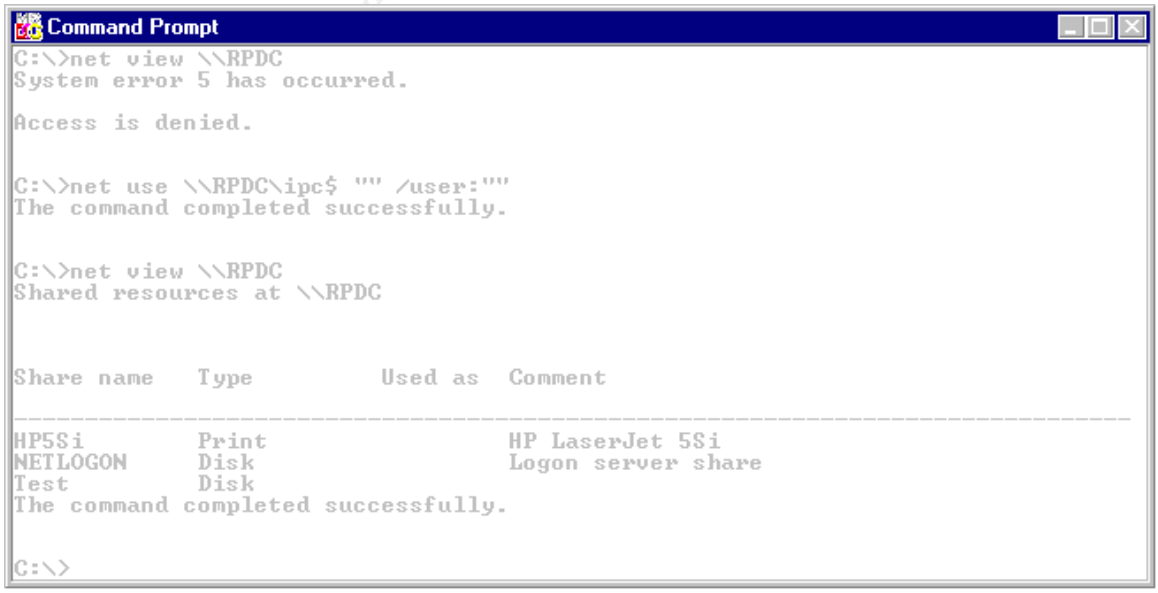

Figure 7 Resources Being Shared on a Computer.

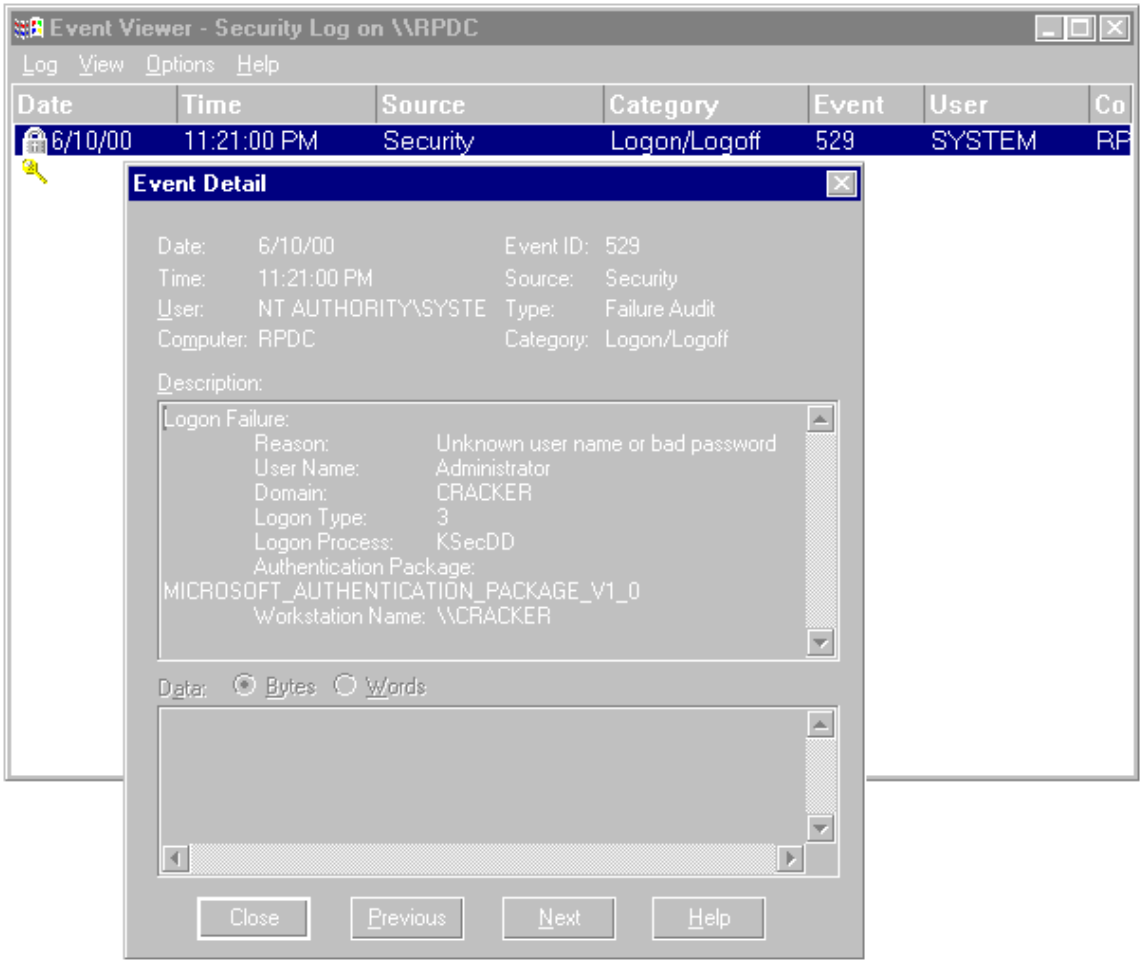

Figure 8 Security event for net view command used outside the null session.

Using the RasUsers Command

The command "RasUsers" will trigger a security event (See Figure 10).

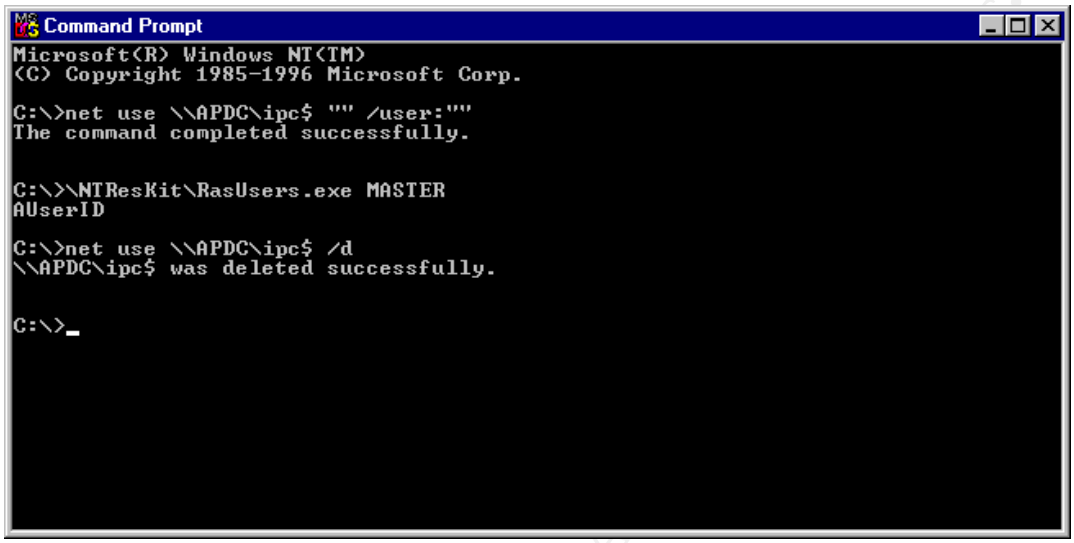

Figure 9 List Users with Remote Access Permission.

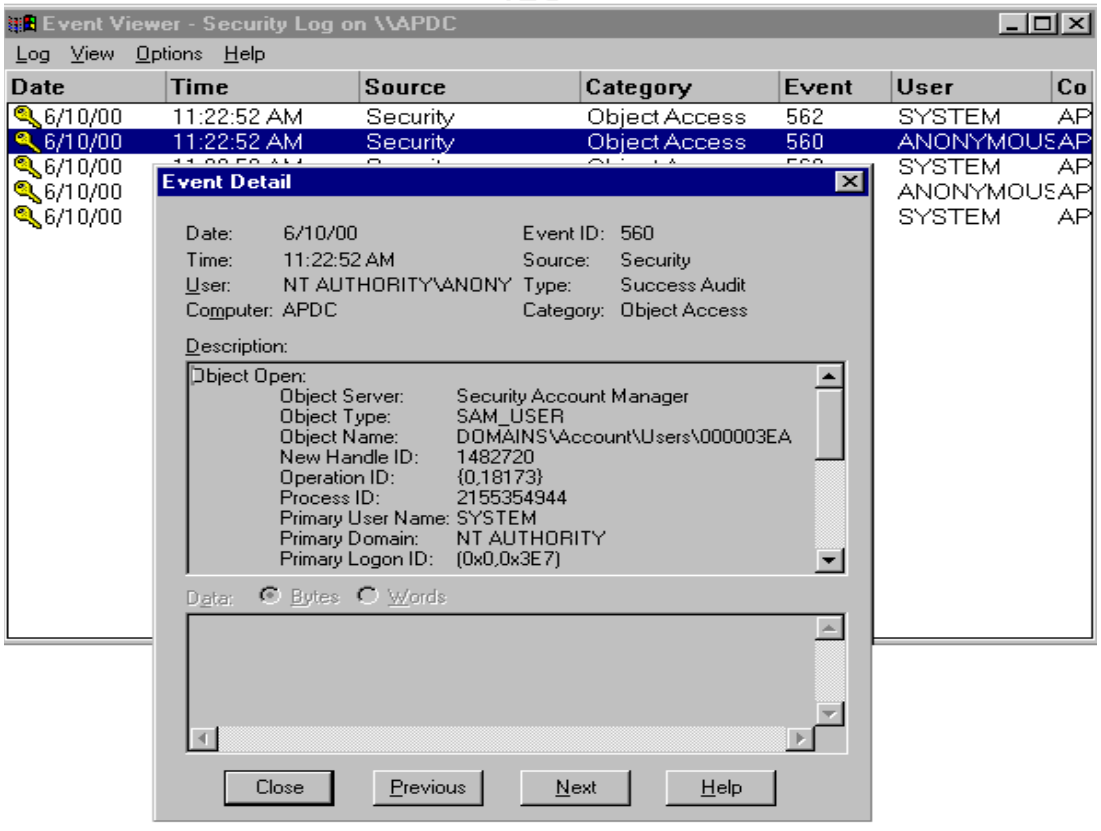

Figure 10 Security event for RasUsers command.

Using the NTUser to Generate a User List

In this context, the command "NTUser" will not trigger a security event.

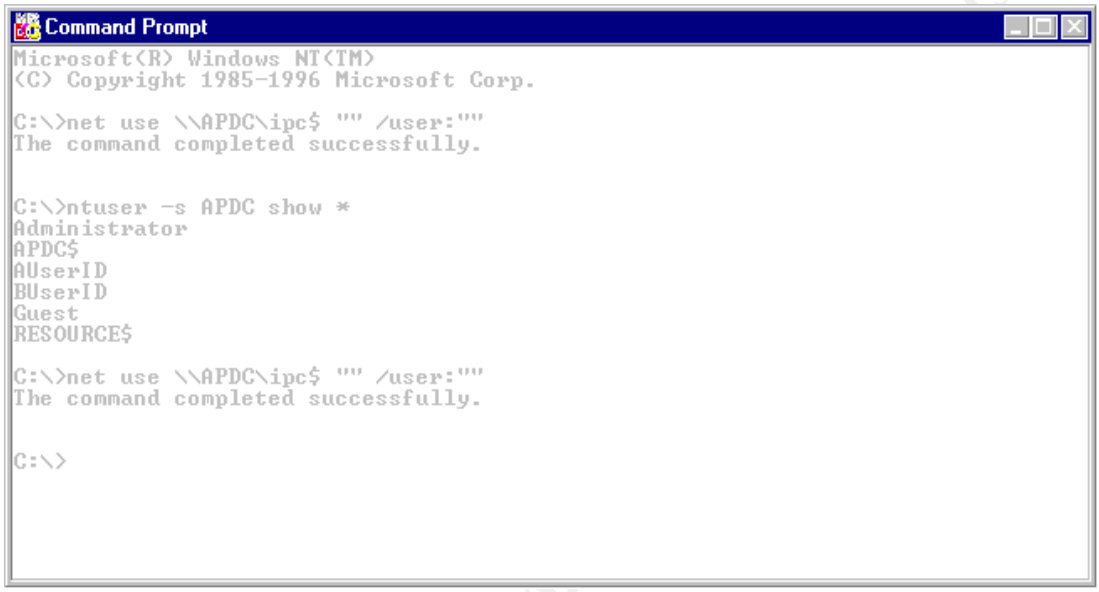

Figure 11 List User IDs.

Using the NTUser to List a Users Policies

This will cause a security event to trigger (See Figure 13).

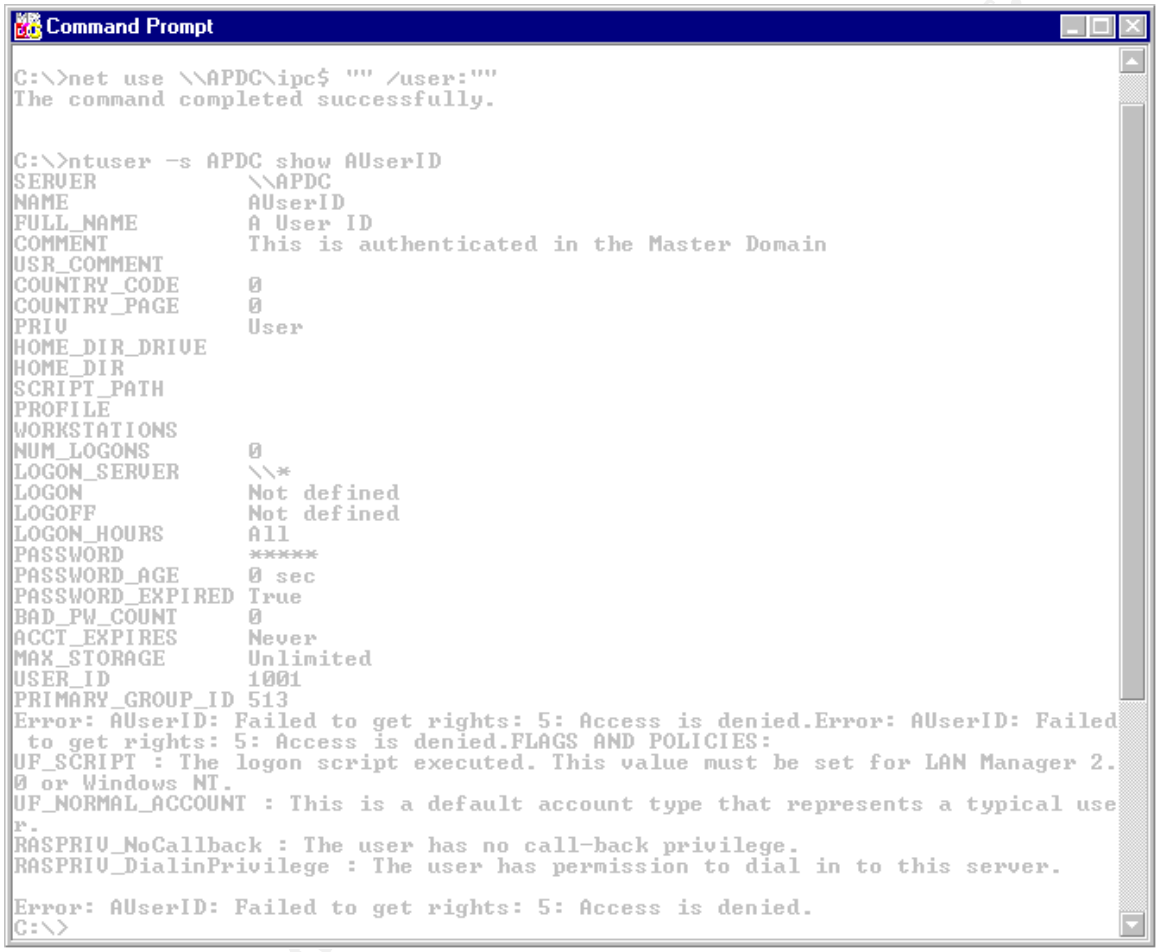

Figure 12 Listing the Password Policy for a user.

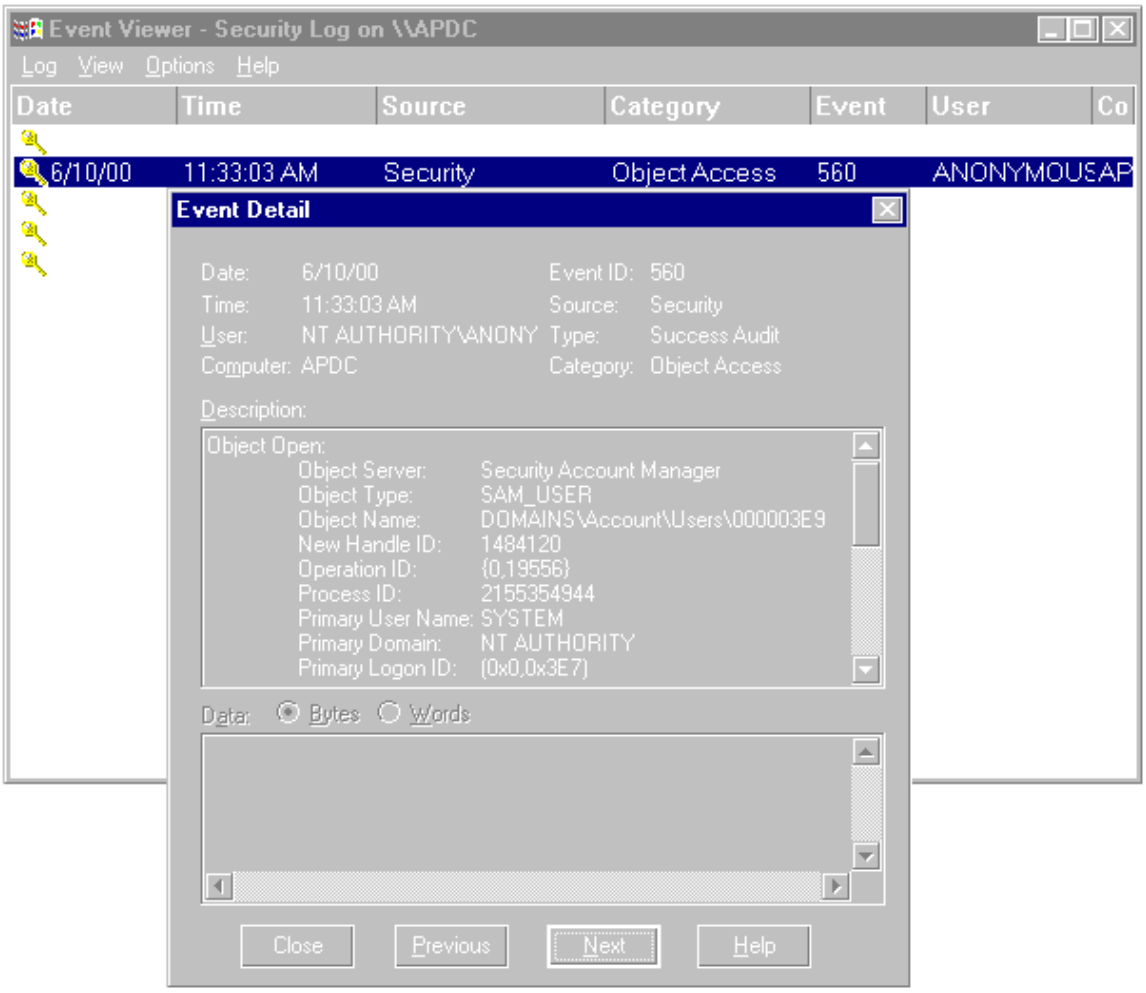

Figure 13 Security event for NTUser command.

User Manager

Using the "User Manager" tool before restricting anonymous logons.

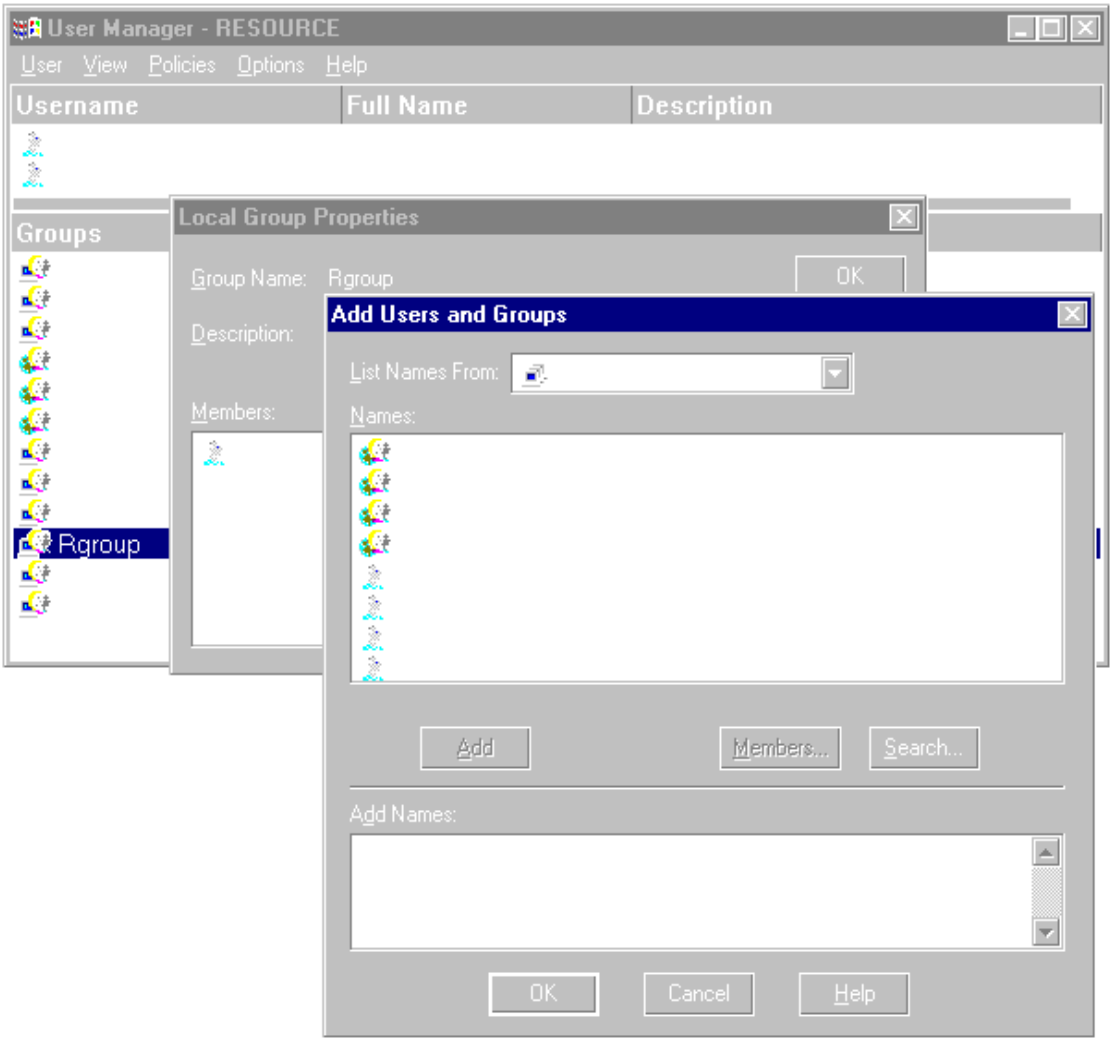

Figure 14 Viewing the User List before restricting anonymous logon.

After Null Login/Access has been implemented

Using the Nbtstat Command

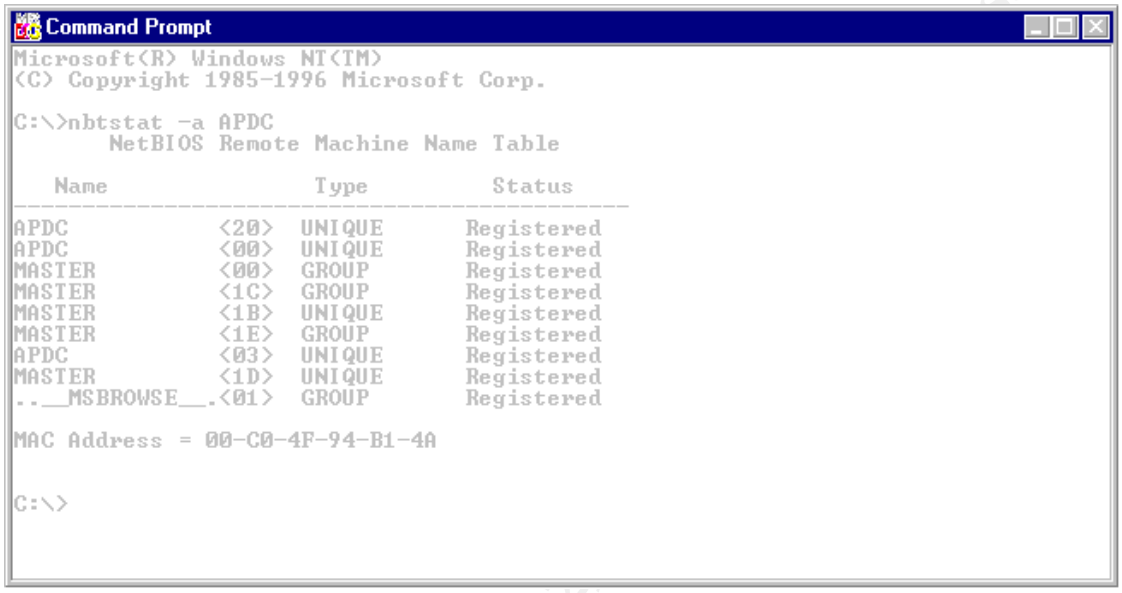

Figure 15 NetBIOS Remote Machine Name Table.

Using the Net View Command

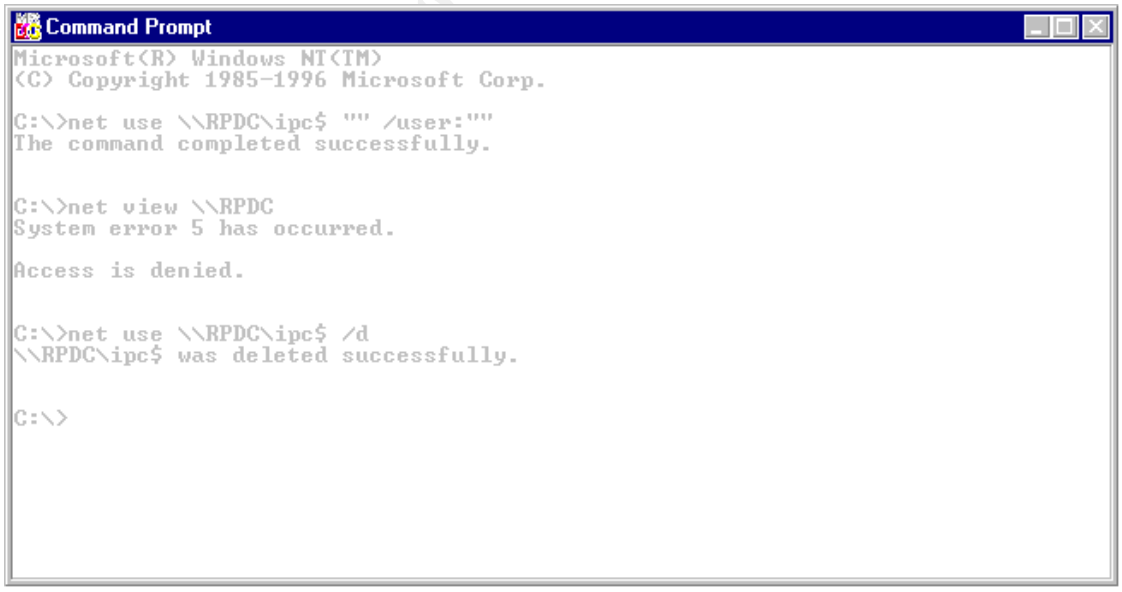

Figure 16 Listing Resources Being Shared on a Computer Fails.

Using the RasUsers Command

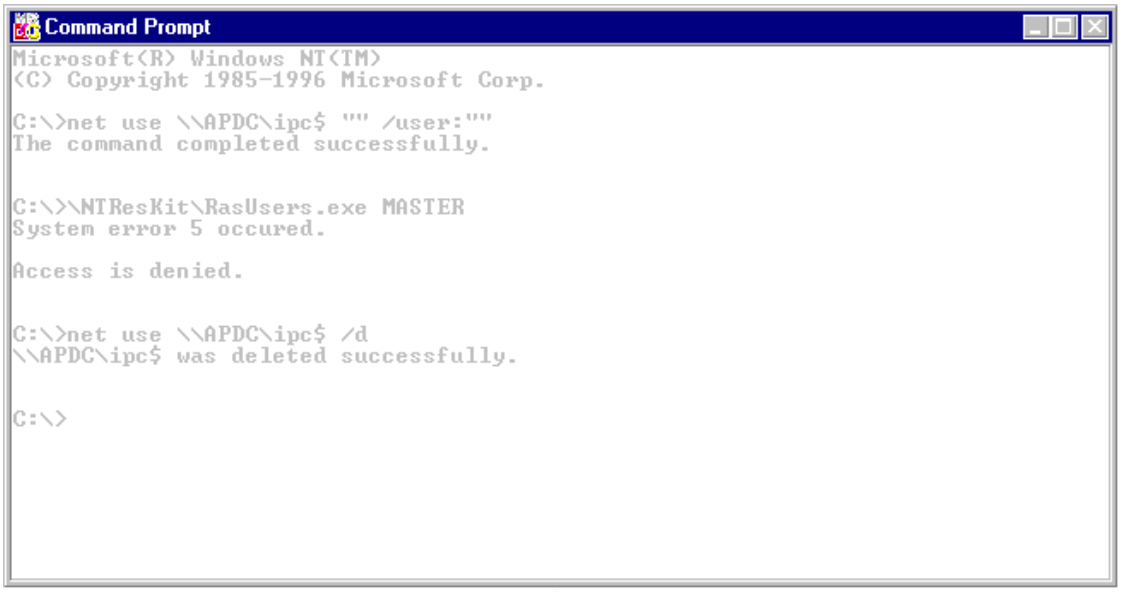

Figure 17 List Users with Remote Access Permission Fails.

Using NTUser to Generate a User List

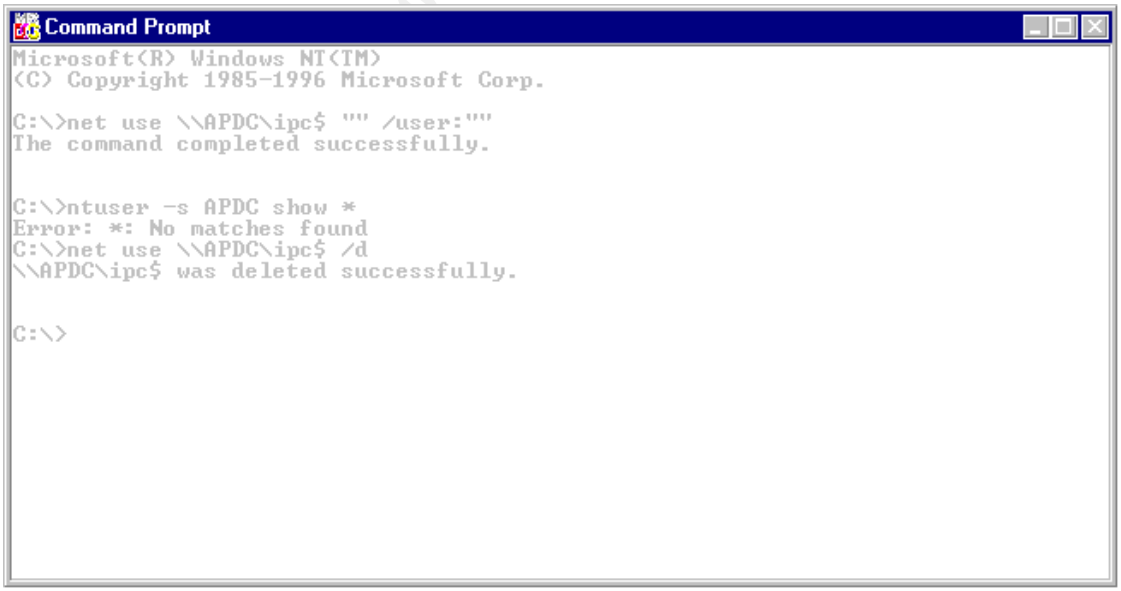

Figure 18 Listing User IDs Fails.

Using NTUser to List a Users Policies

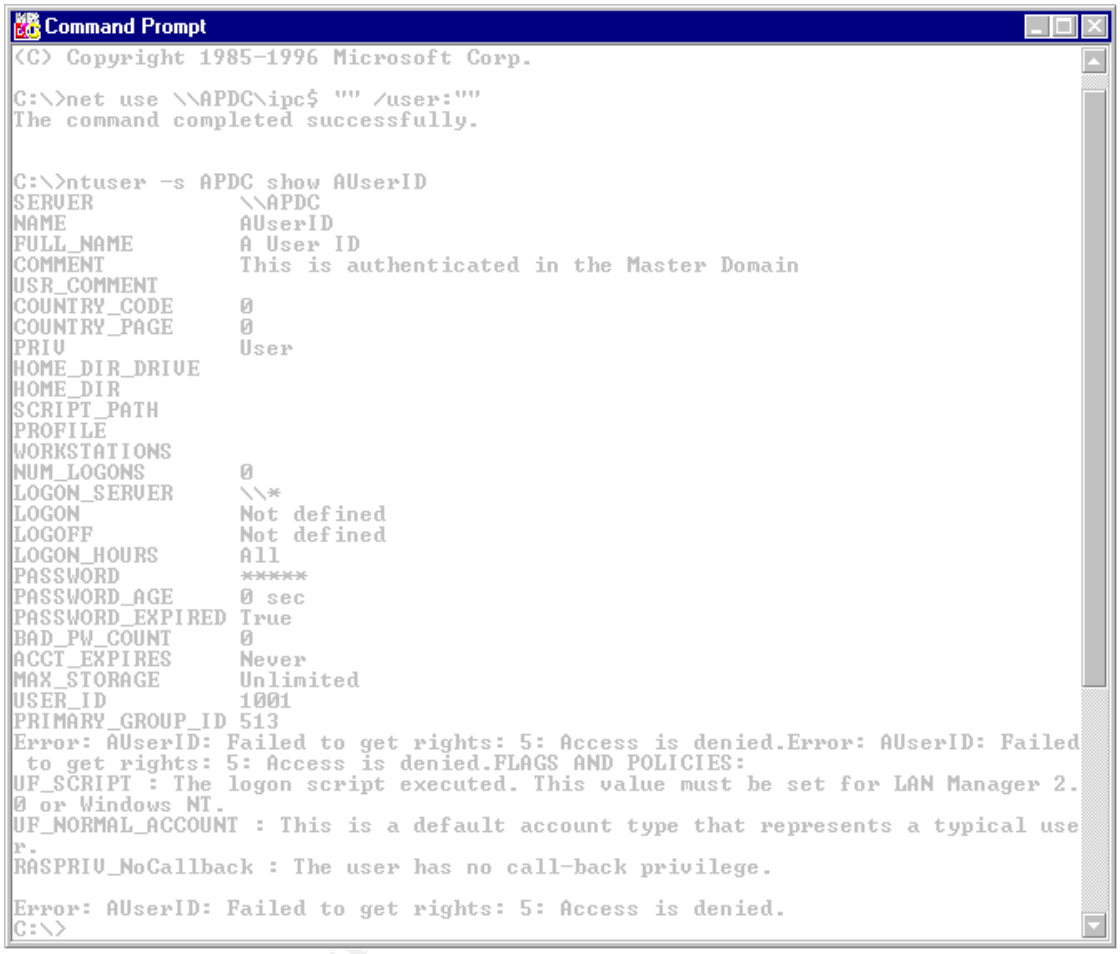

Figure 19 Listing the Password Policy for a user does not fail.

User Manager

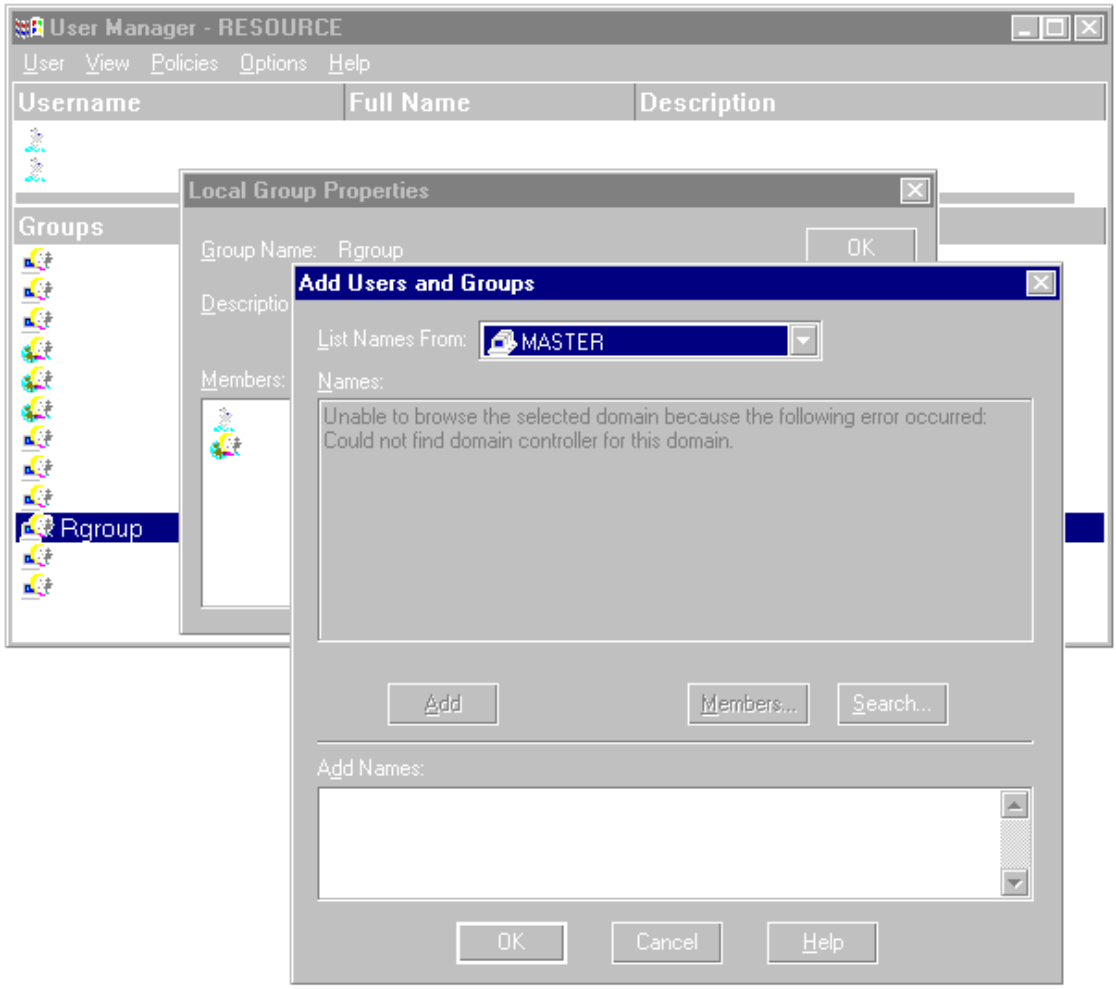

Figure 20 Access Denied to View the User List on the Master Domain.

4. Steps Involved in Modifying the Registry to restrict Null Sessions/Login

Developing an Implementation Plan

Develop a step-by-step plan for implementing, testing, and backing out any changes to be made to the system(s). This may entail generating change control documentation, coordinating your efforts with other departments or regions, developing contingency plans, notifying users of an upcoming server maintenance, or any other items that may be unique or standard to your organization.

System Testing

Perform all systems modifications and testing on a test system that mimics your current environment, if at all possible, before making any changes in a production environment. Usually, this step will provide feedback to the Implementation Plan and the process is repeated until all parties involved agree with the changes being made and are aware of the possible consequences these changes can have on the services running on the server(s).

Logging Onto the System

Log onto the system to be modified with an account that has the rights to edit the registry and reboot the system.

Check Viability of Backup(s) on Production Systems

If on a production machine, verify that a full set of backups has been performed on the system prior to implementing any changes to the system and that you have the capability to recover the system from the backup media if the need arises.

Updating The Emergency Repair/Boot Disks

Updating NT 4.0 Setup Disks

Insure that you have a set of Windows NT 4.0 Setup disks[8] available and that Disk Number Two of the NT Setup disk contains an updated copy of Setupdd.sys[9] from the current Service Pack that was last installed on the system. If after expanding the service pack files and the file "Setupdd.sys" could not be found, see [KBase] Q236158 on how to obtain the missing file(s)[10].

[8] [KBase] Q131735 – How to Create Windows NT Boot Floppy Disks.
[9] [KBase] Q168015 - Files Not Replaced When Running Emergency Repair on X86 Intel Systems.
[10] In case the system your working on becomes unavailable, you my also whish to insure that you have access to any software, utility programs and/or setup documents on hand before modify the system.

Updating the Emergency Repair Disk (ERD)

1. For each machine that is to be modified, open a "Command Prompt" window and type in the following command[11] at the prompt:

   %SystemRoot%\System32\Rdisk.exe /S

   This will update the system's Emergency Repair Disk, as well as the SAM database. Also make sure you are familiar with the procedures for repairing the Windows NT System[12] or have a contingency plan if something goes amiss after editing the registry[13].

Updating Disk Configuration Files

Depending on your hardware configuration and setup, the following steps may not be needed or they may need to be modified to fit your environment.

1. Bring up the "Disk Administration" tool by left clicking on the "Start" button on the "Task Bar" and following the path "Programs\Administrative Tools (Common)\Disk Administrator".

2. Once the "Disk Administration" tool is open save the disk configuration information by selecting the "Partition" menu, then point to "Configuration", and then click "Save".

3. Follow the instructions that appear in the pop up message box and, once completed, close the application.

[11] [KBase] Q156328 - Description of Windows NT Emergency Repair Disk and [KBase] Q122857 - RDISK /S and RDISK /S- Options in Windows NT.

[12] An example of repairing a Windows NT System can be found in [KBase] Q196603 - Windows NT after installation of Service Pack 4.

[13] In almost any documentation from Microsoft that deals with modifying the registry you will see the following quote.

"*WARNING: Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.*

For information about how to edit the registry, view the "Changing Keys And Values" Help topic in Registry Editor (Regedit.exe) or the "Add and Delete Information in the Registry" and "Edit Registry Data" Help topics in Regedt32.exe. Note that you should back up the registry before you edit it. If you are running Windows NT, you should also update your Emergency Repair Disk (ERD)."

Backing Up the Registry Keys

This is an optional step. But my personal preference is to backup the parts of the registry that will be changed, this includes both before and after the registry changes have been made. This step enables one to quickly recover from some types of errors in editing the registry while providing a record of the changes that were made.

Windows NT comes with a set of tools to modify, dump, and import the registry; but there are also other tools available from Microsoft, as well as other third-party tools to perform the same function. In this document, we will be using the Windows NT 4.0 Server Resource Kit tools. The Microsoft Windows NT Resource Kit is typically bundled within the TechNet subscription or the Resource Kit can be purchased separately.

The tools that are provided with the standard NT operating system for manipulating the registry are:

Regedt32.exe:	Export or import the registry through hives and text files.
RegEdit.exe:	Although this command can export or import the registry through .REG files. If the exported files contain values of data types REG_MULTI_SZ, REG_EXPAND_SZ, or REG_BINARY, then the RegEdit.exe[14] command cannot be use to import the registry file back into the registry database. Because of this limitation, RegEdit.exe should only be used for its expanded searching capabilities.

The Windows NT Resource Kit[15] provides the following commands to backup, restore, and or modify the registry:

RegBack.exe:	Backup open registry hives to disk.
RegRest.exe:	Restore registry data saved with RegBack.exe.
SaveKey.exe:	Save individual registry values to disk.
RestKey.exe:	Restore registry values saved with SaveKey.exe.
RegDmp.exe:	Dumps the registry to screen unless redirected to disk.
RegIni.exe:	Uses the output of RegDmp.exe to modify the registry.

[14] [KBase] Q186146 - Double-Clicking .reg File Will Not Add Extended ANSI Values and pp. XXV of [Osbo98].

[15] Refer to the Windows NT Resource Kit documentation set for instructions on how to use the commands mentioned in this document.

All the changes we will be making to the registry in this document fall under the following two registry keys:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Dumping The Registry Key(s)

Use the following steps and the RegDmp.exe[16] program from the Windows NT 4.0 Server Resource Kit to dump the registry keys and pipe the output into a text file.

1. Bring up the "Command Prompt" by left clicking on the "Start" button on the "Task Bar" and follow the path "Programs\Command Prompt".

Dumping The Registry Key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

1. Enter the following command[17] in the "Command Prompt" window:

```
C:\NTResKit\RegDmp.exe HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Control\Lsa > HKLM_SYS_CCS_Lsa_0006031415.txt
```

See Appendix A for an example of the text file that was created in this step.

Dumping The Registry Key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

1. Enter the following command in the "Command Prompt" window:

```
C:\NTResKit\RegDmp.exe HKEY_LOCAL_MACHINE\SYSTEM\
CurrentControlSet\Services\LanmanServer\Parameters >
HKLM_SYS_CCS_Ser_LS_P_0006031415.txt
```

See Appendix B for an example of the text file that was created in this step.

[16] The location of the command "RegDmp.exe" may be in a different location at your site depending on how the product was installed.
[17] Due to space limitations the length of some commands within this document may be continued on another line.

Starting The Registry Editor.

Although the RegEdit.exe[18] program is a good tool for searching the registry, it cannot perform all the functions needed to make the changes within this document. So the Regedt32.exe command will be used.

1. While the "Command Prompt" is still open, enter the following command:

   %SystemRoot%\System32\Regedt32.exe

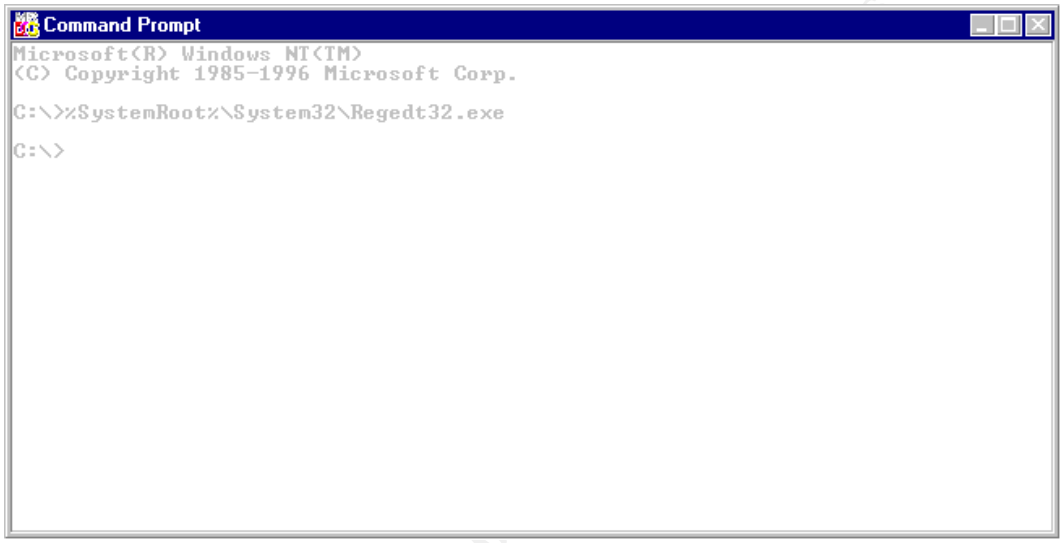

Figure 21 Opening the Registry Editor (Regedt32.exe).

The window entitled "Registry Editor" should appear on the desktop. You should keep this window open until all the registry modifications in this document have been completed (See Figure 22).

[18] See [Osbo98] pp. xx - xxvi, in the introduction for a description of the registry data types and editors.

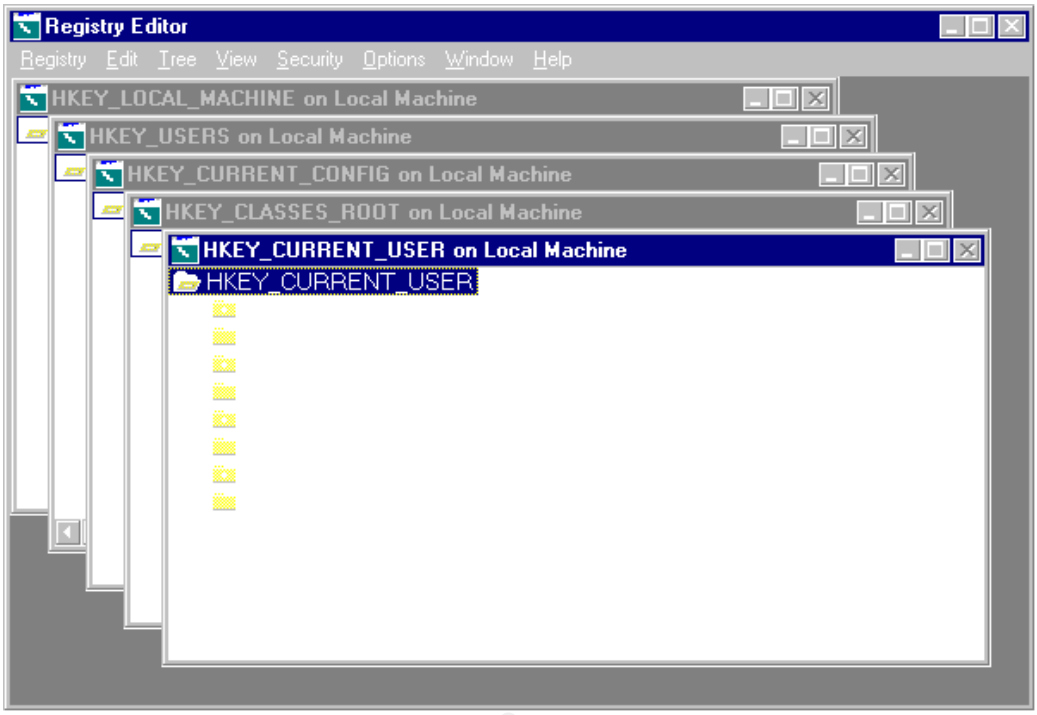

Figure 22 The Registry Editor (Regedt32.exe).

Restricting Anonymous Logon.

Window's NT allows a type of logon known as a Null Credentials logon that attaches to a system via the Named Pipes share:

Inter-Process Communications[19] (IPC$)

A very basic description of an anonymous logon (a null user session) means a person or a service is allowed to connect to a system without credentials, which is synonymous to no user name, no domain name, and no password. Once connected, a potential intruder[20] can obtain a listing of the user account names, group memberships, password properties, user Security Identifiers, account policy details, share names and permissions. To restrict anonymous logon to a Microsoft's Internet Information (IIS) server is beyond the scope of this text.

[19] The security concerns of the IPC mechanisms are beyond the scope of this paper. See [MSED689] pp. 467 for the definitions of the following IPC Mechanisms: Named Pipes (NPFS), Mailslots (MSFS), NetBIOS, Windows Sockets, Remote Procedure Calls (RPC), Network Dynamic Data Exchange (NetDDE), and Distributed Component Object Model (DCOM) or [TechNet] at the following URL: http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/winbase/ipc_57qr.htm for additional information on the topic of Inter-Process Communications. Or [MSDN] topic on Inter-Process Communications at URL: http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/winbase/services_11tg.htm .

[20] See [Jume98] pp.197 on how to connect to the IPC$ share using the Null Credentials logon in the section entitled "Null Credentials Logon". Chapter 11 also describes other registry modifications you might want to explore to secure you system(s).

The following is an excerpt from Microsoft Knowledge Base article Q143474[21] last reviewed on March 28, 2000:

> *"It should be noted that even with the value of RestrictAnonymous set to 1, although the user interface tools with the system will not list account names, there are Win32 programming interfaces to support individual name lookup that do not restrict anonymous connections."*

From the above statement made by Microsoft (and [TRS99][22]), as well as the problems with restricting anonymous access, it would sound as though limiting null access is a mute point. In some cases it may be, but currently not every exploit for NT is known; plus, it also depends on what you are trying to protect. There's another caveat to all of this, which is, limiting null user access via the "RestrictAnonymous" key. If you restrict anonymous access on a domain controller, then you must also restrict the anonymous access on all the domain controllers contained within that domain group that you want to protect for this step to work.

The following two items are examples of the known problems with disabling the anonymous logon:

> The first example is with Microsoft's User Manager[23] tool because the User Manager requires an anonymous user logon to list account information. Similar situations occur with Windows NT Explorer and the ACL editor. This poses a problem in a multiple domain[24] environment where the resource domain has a one-way trust relationship with the account domain. If the administrator in the resource domain wants to grant access to a resource in their domain for a user from the account domain, then it would be convenient to be able to obtain the list of users and groups from the account domain. Once the list was displayed, the resource domain administrator could then select the user(s)/group(s) to grant the access rights to use the resource. Due to the one-way trust relationship, the account domain does not trust the resource domain, thus the resource administrator's request to obtain the list of user names and/or group names from the resource domain cannot be authenticated because the resource domain was trying to connect to the account domain via a null user session.
>
> To get around this problem, the administrator from the account domain would have to send the resource domain administrator the information they needed so that the data could be inputted manually; or the resource administrator could have two accounts, one in each domain. Once rights have been assigned on the

[21] See [TRS99] pp. 32 "User & Share Names Available to Unauthenticated Uses", [Okun] pp.243 "Writing spy programs", and the code to write an API spy program can be obtained from [MSJDec94].
[22] On pp. 32 see the section entitled "User & Share Names Available to Unauthenticated Users".
[23] See [KBase] Q178640 - Could Not Find Domain Controller When Establishing a Trust and [KBase] Q143474 - Restricting Information Available to Anonymous Logon Users.
[24] To get a better understanding of Windows NT domain concepts see chapter 4 in [Hadf97].

resource domain, users from the account domain can authenticate and access resources in the resource domain based on the one-way trust.

The other example of a problem in restricting anonymous login, would be with Novell's "NDS for Windows NT". (See the [KBase] Q184018 entitled "Novell NDS for Windows NT Does Not Support Restrict Anonymous Security" for more information.)

To restrict anonymous logons you will need to create the registry entry shown in the table below:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Control\Lsa
Value Name	RestrictAnonymous
Type	REG_DWORD
Value	1

Figure 23 Settings to restrict anonymous logons (RestrictAnonymous).

Locating The Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA

To locate the keys in the steps below may require use of the scroll bar in the Registry Editor's window. To find the keys listed in the steps may require expanding the key by double-clicking the key in the previous step (See Figures 24).

1. Select the "Window" menu, then point to the line that starts with "HKEY_LOCAL_MACHINE".

2. Under the hive "HKEY_LOCAL_MACHINE", locate the key "SYSTEM".

3. Locate the sub-key "CurrentControlSet" under the key "HKEY_LOCAL_MACHINE\SYSTEM".

4. Locate the sub-key "Control" under the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet".

5. Locate the sub-key "Lsa" under the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control".

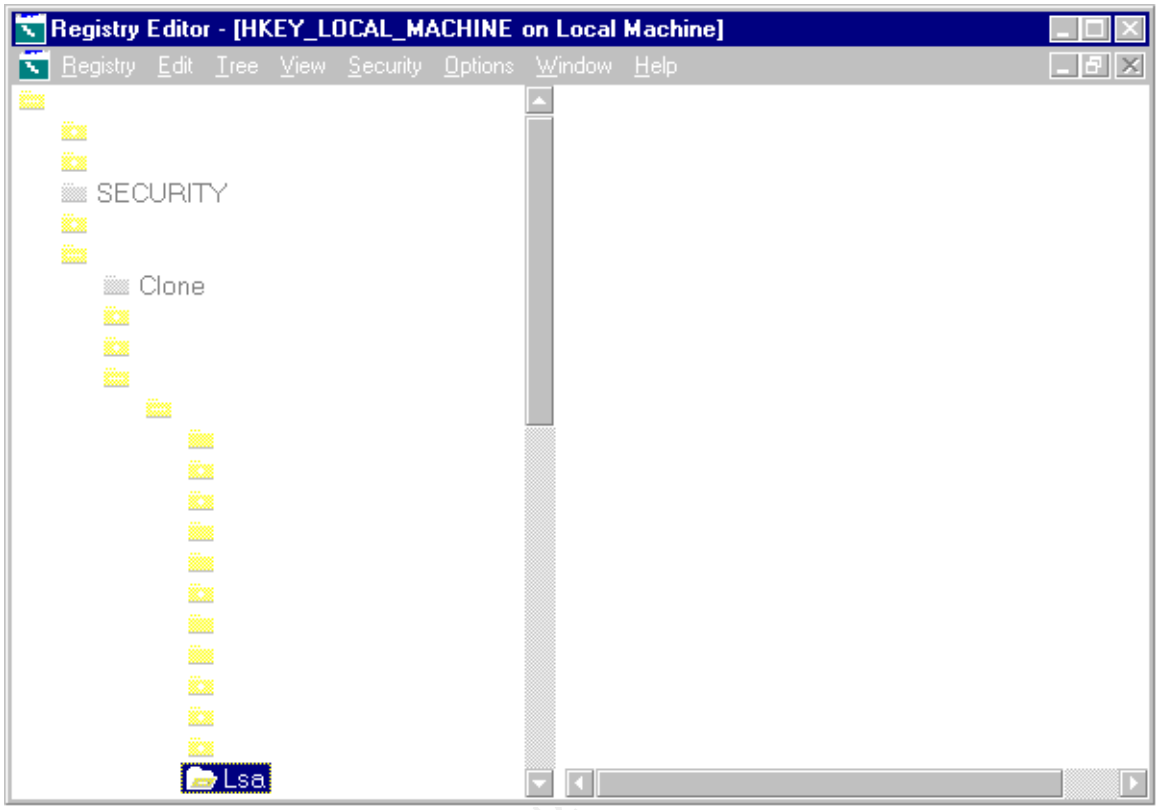

Figure 24 Registry Settings Before Restricting Anonymous Logon.

Adding The RestrictAnonymous Value

1. With the "Lsa" key highlighted, select the "Edit" menu, then point to "Add Value…",

2. When the "Add Value" windows appears, enter the following word in the "Value Name" text box:

   RestrictAnonymous

3. Change the "Data Type" value to REG_DWORD

4. Click on the "OK" button on the "Add Value" windows (See Figure 25).

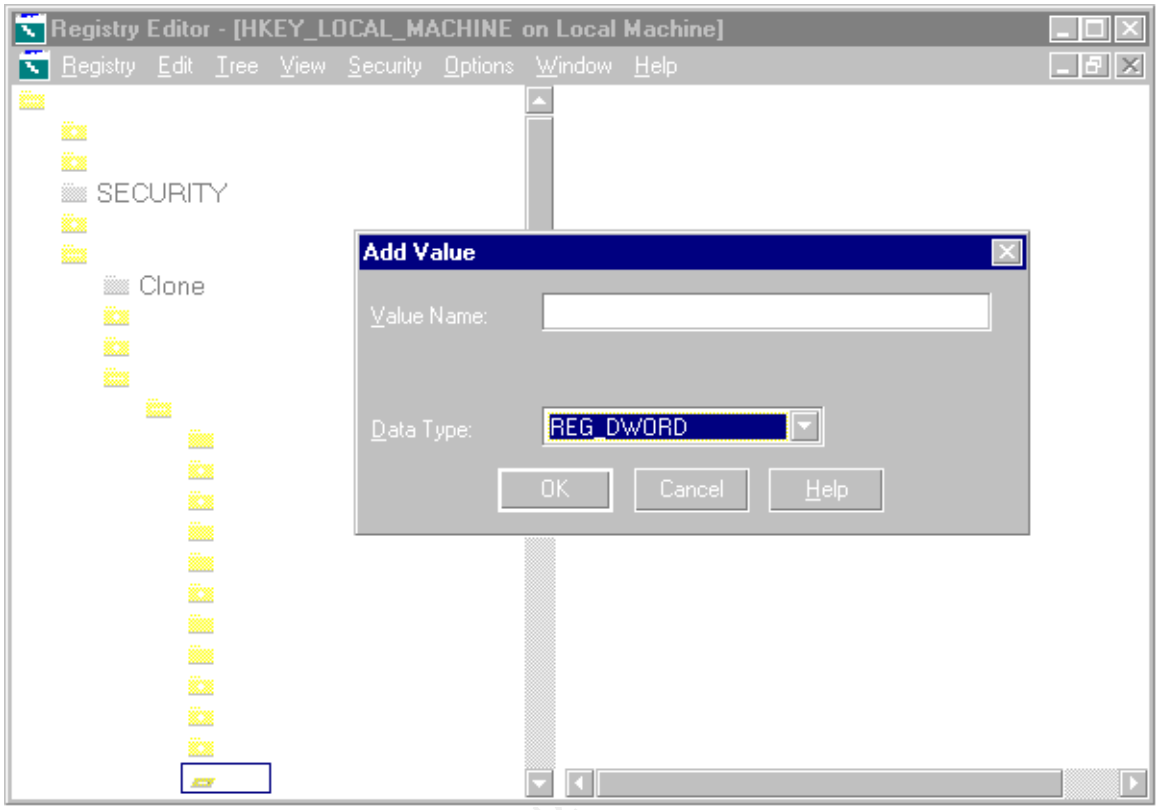

Figure 25 Adding The RestrictAnonymous Value.

Setting The Value For RestrictAnonymous

Entering a 1 disables anonymous logon and a 0 enables anonymous login to list out usernames, groups, and share names.

1. When the "DWORD Editor" window appears, enter the following value in the "Data" text box:

   1

2. Ensure that the "Hex" radio button is selected.

3. Click on the "OK" button on the "DWORD Editor" window (See Figure 26).

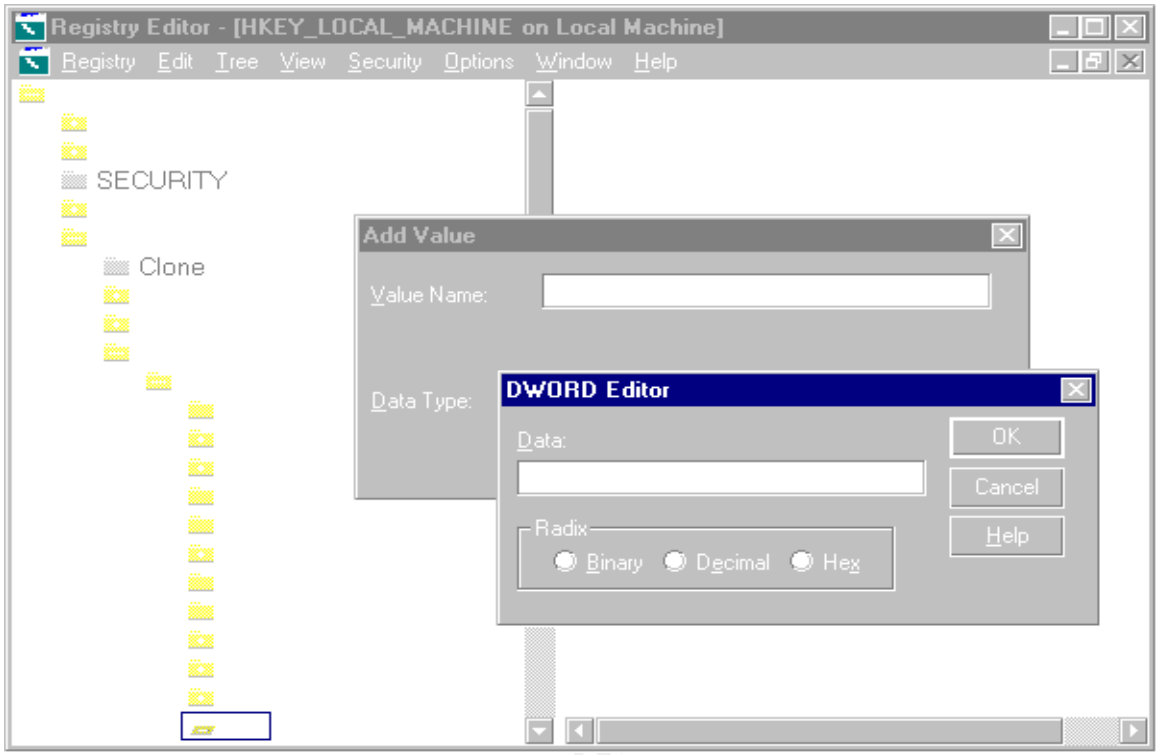

Figure 26 Setting The Value of RestrictAnonymous to Disable Anonymous Logon.

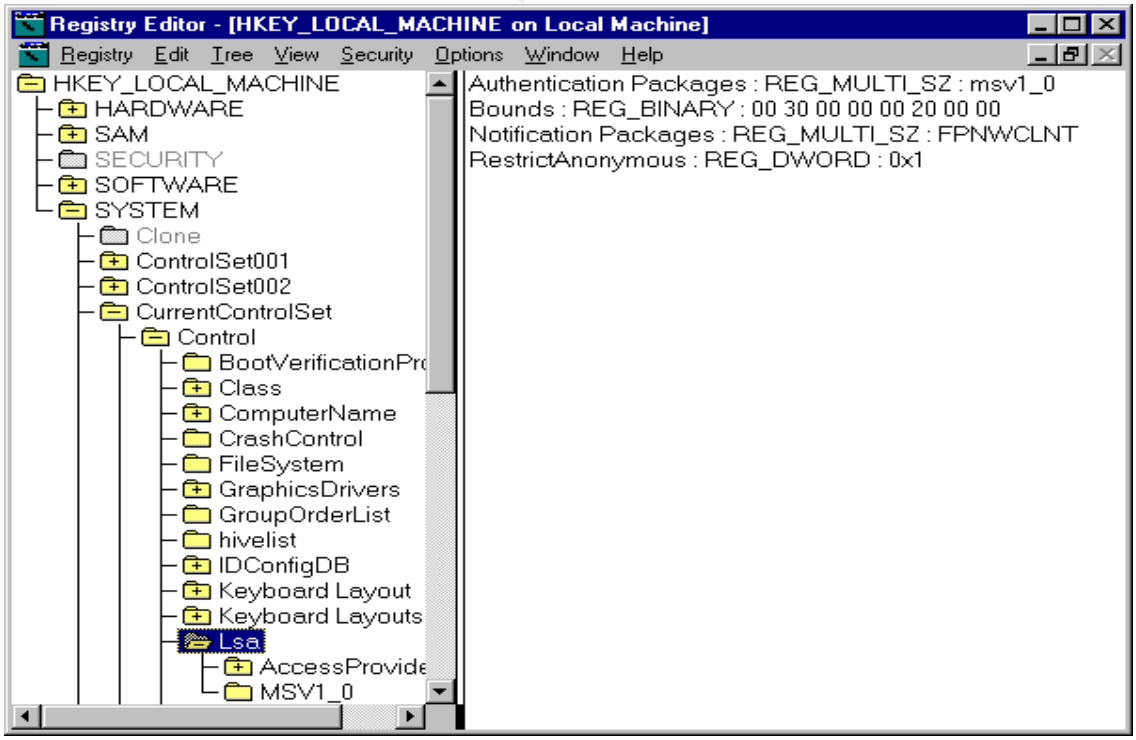

Figure 27 The registry after anonymous login has been disabled.

Restricting Null Session Access To Named Pipes and Shares

By default, when Windows NT is loaded onto a system, the registry key "RestrictNullSessAccess" does not exist. The registry key will be added and set to disallow null access to ensure limiting access to named pipes and shares. Although the system[25] account has limited access to any of these network resources, such as shares and pipes, the context that is used to access them on a remote machine is as follows:

Default Owner:	Everyone	
User:	Everyone	
Groups:	AnonymousLogin	pseudo group - local group scope
	Network	pseudo group - local group scope

Figure 28 Context of the System account running on a remote machine.

The context[26] that the System account runs on the local machine, better known as the operating system is:

Default Owner:	Administrators	local group
User:	System	pseudo group - local group scope
Groups	Administrators	local group
	Everyone	pseudo group - local group scope

Figure 29 Context of the System account running on the local machine.

The default owners of these two contexts (as well as their default DACLs) are different. So any files created in the contexts (Figure 29) above will be owned by the Administrators; however, any files created through a null session (Figure 28) will be owned by "Everyone". Unless otherwise configured differently, most services run, by default, as the System account[27] which happens to be a member in both the "Everyone" group and the Administrators group. In some aspects, the System account is more powerful than the Administrator ID due to the fact that it is configured to have six privileges[28] which the Administrator ID does not have. In addition, the System account has two privileges[29] enabled by default, whereas the same privileges for the Administrator's ID are disabled by default

[25] See [MSDN] documentation on "The LocalSystem Account" for more information on null sessions see URL: http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/winbase/services_11tg.htm
[26] See [KBase] Q132679 - Local System Account and Null Sessions in Windows NT
[27] See [Fris98] pp. 60 for a brief description of the System account.
[28] In [Okun] pp. 223 the book states that the Administrator account does not contain the following privileges where as the System account does: SetcbPrivilege, SeCreateTokenPrivilege, SeLockMemoryPrivilege, SeAssignPrimaryTokenPrivilege, SetCreatePermanentPrivilege, and SeAuditPrivilege.
[29] In [Okun] pp. 223, the book states that the following two privileges are enabled by default in the System account but not in the Administrator's account: SeCreatePageFilePrivilege and SetIncreaseBasePriorityPrivilege.

Therefore, depending on what services a server will be running, the following factors will help determine if disabling the null access to named pipes or shares may or may not cause a problem at your site.

- Whether or not a service is setup to use the System account or a Domain[30] account.
- How well the service was written[31].
- How the File/Sharing permissions are setup.
- What the group "Everyone" has access to on the system, as well as within the registry.

Wherever possible, all services that are not required should be disabled; and any services that need to be running on the server should be started with a domain account instead of the system account. Most issues with disabling the null access to named pipes or shares [32] will have to be dealt with by a trial and error approach.

To restrict null sessions, you will need to create the registry entry shown in table below:

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Services\LanmanServer\Parameters
Value Name	RestrictNullSessAccess
Type	REG_DWORD
Value	1

Figure 30 Settings to restrict null sessions (RestrictNullSessAccess).

Even though the RestrictNullSessAccess has been enabled, any named pipes contained within the registry key NullSessionPipes or any shares contained within the registry key NullSessionShares will still be accessible by a null session. In the later sections, we will look at how to resolve this problem.

[30] There are many examples available on setting up a Service to run under an account other then the System account but [Jume98] deals with an example of setting up directory replication quite nicely on pages 169 through 174

[31] See [Okun] pp. 243 in the section entitled "Writing spy programs" or [MSJDec94] for the article "Learn System-Level Win32® Coding Techniques by Writing and API Spy Program."

[32] With the advent of Service Pack 4, Microsoft introduced a new group known as "Authenticated Users." The Authenticated Users group is similar to the "Everyone" group, except anonymous logon users (or NULL session connections) are never members of the Authenticated Users group. So in some cases the Authenticated Users group may be able to replace the "Everyone" group.

Locating The Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

To locate the keys in the steps below may require closing any previously opened keys and using the scroll bar (See Figure 31).

1. Select the "Window" menu, then point to the line that starts with "HKEY_LOCAL_MACHINE".

2. Under the hive "HKEY_LOCAL_MACHINE", locate the key "SYSTEM".

3. Locate the sub-key "CurrentControlSet" under the key "HKEY_LOCAL_MACHINE\SYSTEM".

4. Locate the sub-key "Services" under the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet".

5. Locate the sub-key "LanmanServer" under the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services".

6. Locate the sub-key "Parameters" under the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer.

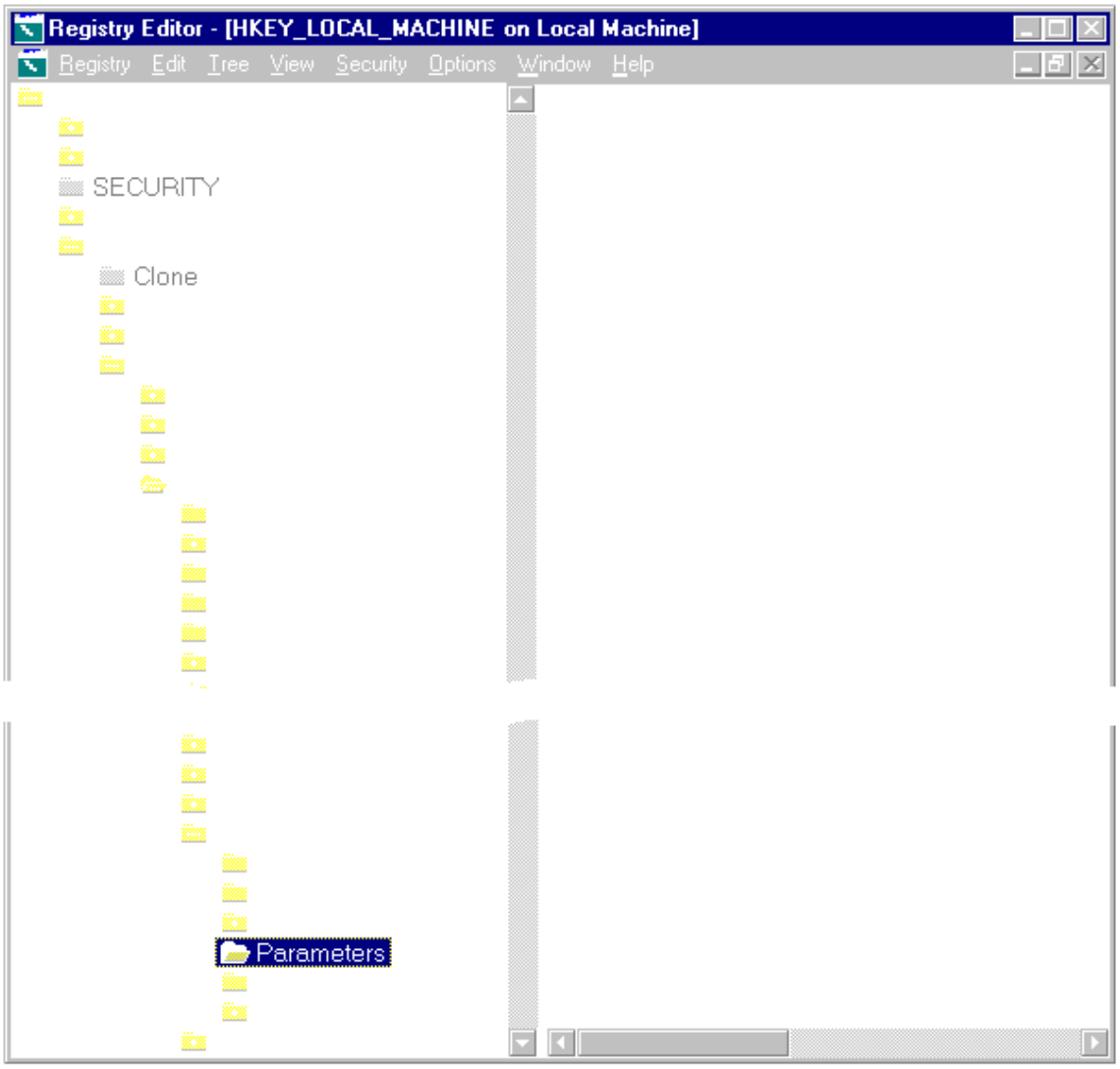

Figure 31 Before view of registry before disabling null sessions access.

Adding The RestrictNullSessAccess Value

1. Select the "Edit" menu, then point to "Add Value…",
2. When the "Add Value" windows appears enter the following word in the "Value Name" text box

   RestrictNullSessAccess

3. Change the "Data Type" value to REG_DWORD.
4. Click on the "OK" button on the "Add Value" window (See Figure 32).

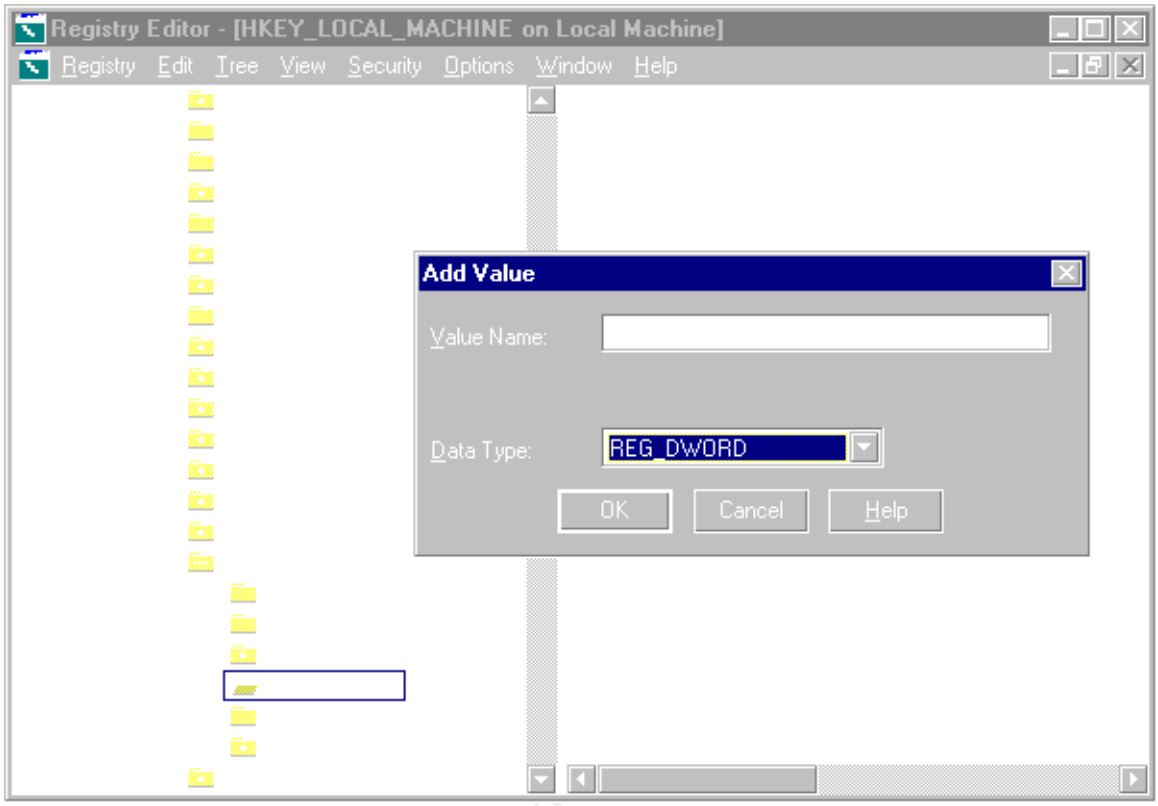

Figure 32 Adding the value RestrictNullSessAccess.

Setting The Value For RestrictNullSessAccess

Entering a 1 disables null session access, except to the items listed in "NullSessionShares" and "NullSessionPipes"; whereas a 0 does not limit the null session access to any of the named pipes or shares on the system.

1. When the "DWORD Editor" windows appears enter the following value in the "Data" text box:

   1

2. Ensure that the "Hex" radio button is selected.

3. Click on the "OK" button on the "DWORD Editor" window (See Figure 33).

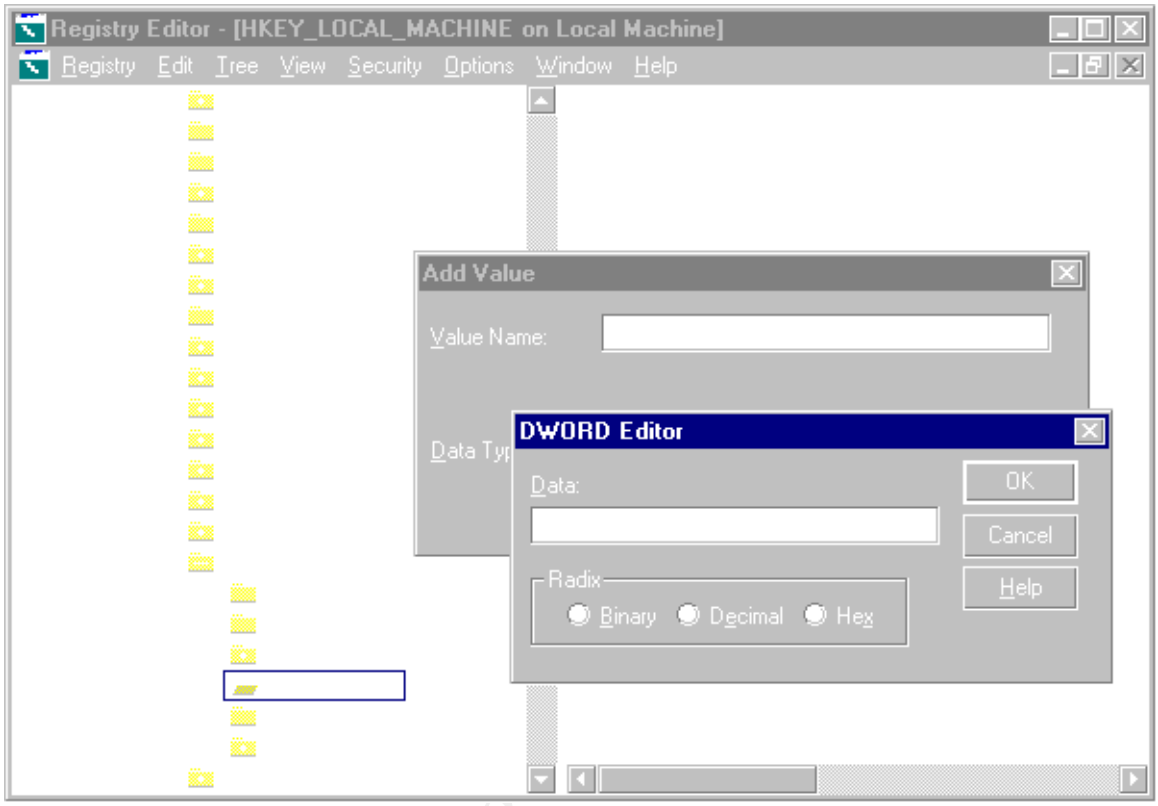

Figure 33 Setting the value of RestrictNullSessAccess to disable null session access.

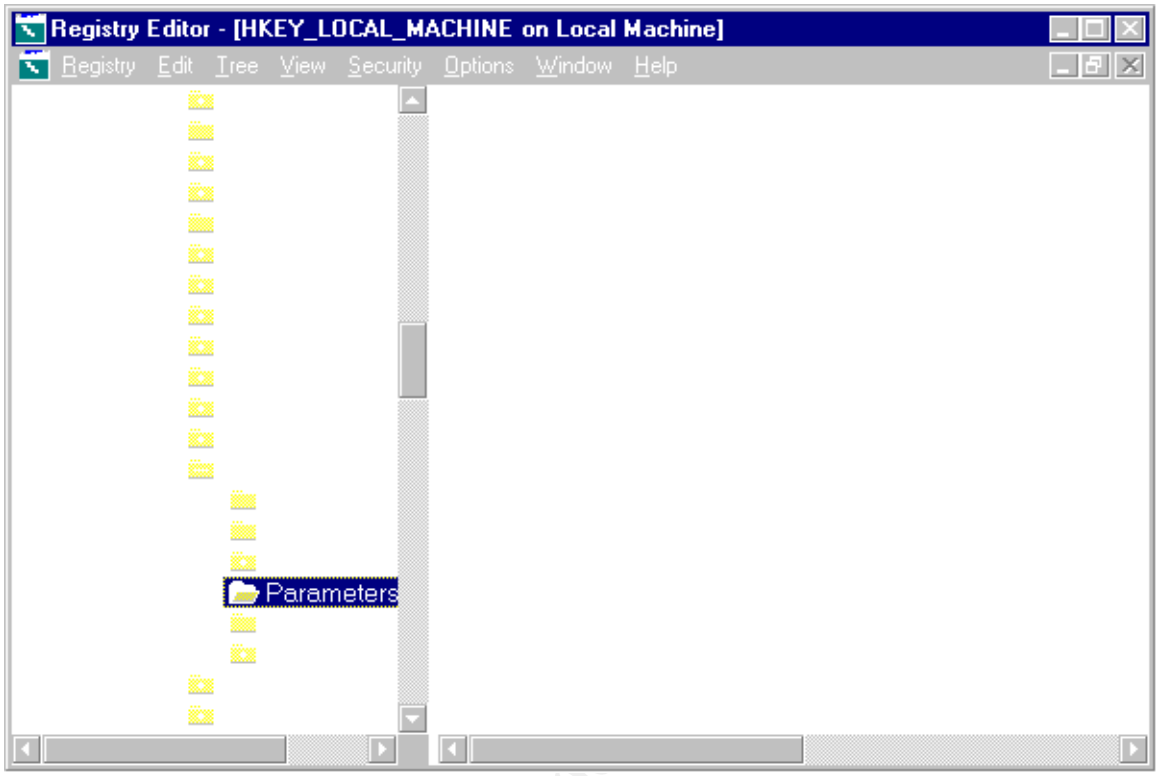

Figure 34 The view of the registry after the value RestrictNullSessAccess was added.

Controlling Null Session Access to Shares

The following shares are placed in the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionShares" by default when NT 4.0 is loaded.

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Services\LanmanServer\Parameters
Value Name	NullSessionShares
Type	REG_MULTI_SZ
Value	COMCFG DFS$

Figure 35 Default settings for NullSessionShares.

Because some applications can only connect to a share via a null connection, Microsoft provided a way to allow some shares to be accessed in this fashion while blocking this access to all the other shares on the system. The way this is done is by placing only the shares that require a null session into the NullSessionShares key. Depending on how some sites are laid out and the security options that are put into place, a few problems could arise. The following articles describe a small sample of some of the things that could go wrong or applications that would need access to a null session share.

The [KBase] Q174296 article demonstrates how an application like Microsoft's Personalization System (MPS) can be affected by the method of authentication that is in place (Windows NT Challenge Response (NTML)) and from where the HTTP client is in relation to the MPS server if null sessions are enabled or disabled.

The [KBase] Q118501 deals with the topic of trouble shooting products like SQL Server 4.2x, SQLMail and SQL Server version 6.x. Part of the document describes how to add the necessary null share "WGPO" if it was not in the NullSessionShares key.

As you can see, the function of the server and the interaction between the other servers/clients can have a great impact on the layout of the security that is implemented at a site and the amount of effort to support a security policy. The following will provided a brief description of the default shares.

COMCFG

The COMCFG share is used to support Microsoft's SNA server. If you are running Microsoft's SNA server, listed below are some additional resources relating to the named pipes and shares.

[KBase] Q140556 - Securing SNA Server to Not Require Everyone: Read Access

[KBase] Q161048 - SNA Server Cannot Find the Share COMCFG or file COM.CFG

[KBase] Q220871 - SNA Server LUs Assigned To Authenticated Users Group Do Not Work Properly

[KBase] Q140556 - Securing SNA Server to Not Require Everyone: Read Access.

DFS$

The purpose of the DFS$ hidden share point is, I believe, associated with the Windows NT Directory File System[33] (DFS) service. So far I have not been able to find any documentation that specifically referenced the DFS$ share.

Locating The Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

1. The key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" should still be displayed in the registry editor from the last step, but if it is not, repeat the previous steps shown in section 9A to locate the key again before continuing.

[33] See [MSED922] pp. 271 – 272 for a brief description about the Distributed File System.

Removing the Data Contained Within The Sub-Key Value NullSessionShares

1. The value "NullSessionShares" is located in the right-hand window of the registry editor. Double-clicking on the sub-key value will bring up a window so that the contents of the value can be edited.

2. Highlight the items shown below in the "Data" window and press the "Delete" key on the keyboard.

   COMCFG
   DFS$

3. Click on the "OK" button on the "Multi-String Editor" windows.

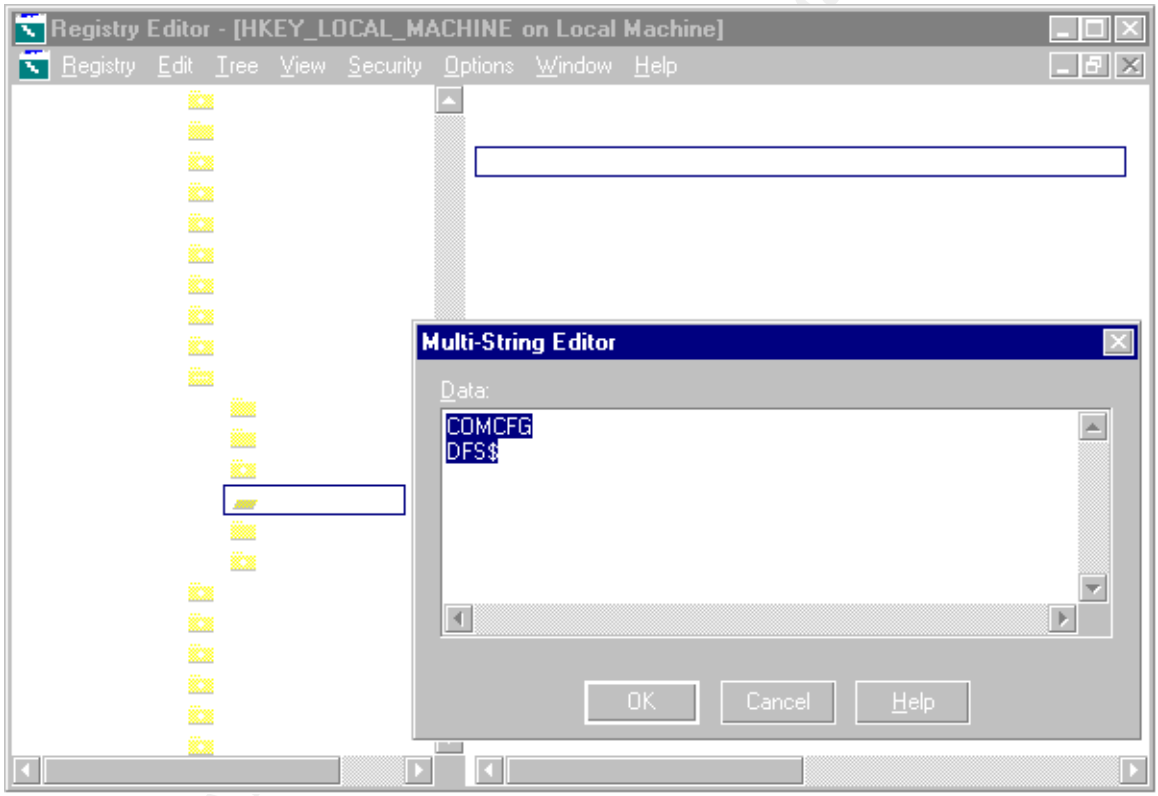

Figure 36 Selecting the data within NullSessionShares.

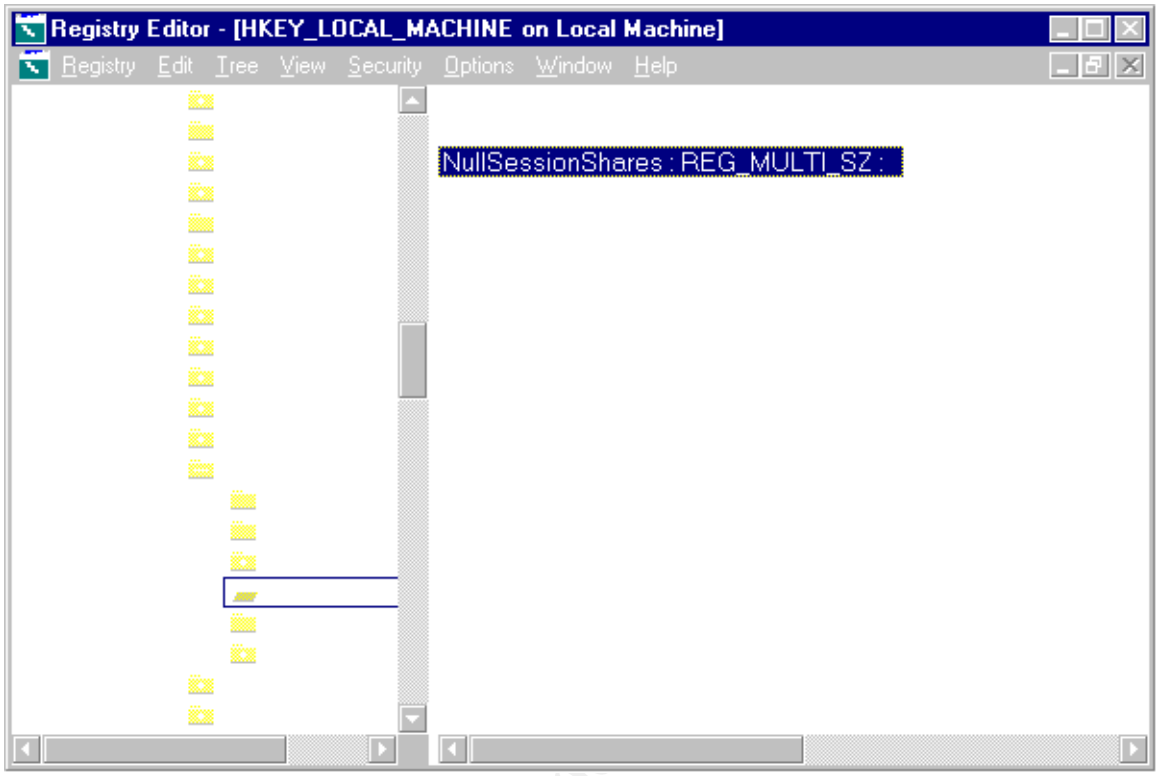

Figure 37 A view of the registry after the values within NullSessionShares has been removed.

Controlling Null Session Access to Named Pipes

The following seven named pipes are placed in the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters\NullSessionPipes" by default when Windows NT 4.0 is loaded.

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Services\LanmanServer\Parameters
Value Name	NullSessionPipes
Type	REG_MULTI_SZ
Value	COMNAP COMNODE SQL\QUERY SPOOLSS LLSRPC EPMAPPER LOCATOR

Figure 38 Default settings for NullSessionPipes.

Because some named pipes will only work via null connections, Microsoft provided a way to allow some named pipes to be accessed via a null connection while blocking this access to all other named pipes on the system. The way this is done is by placing only the named pipes that require a null session into the NullSessionPipes key. Therefore, any service that is listed within the NullSessionPipes key can be connected via a null session. If possible, try to avoid running a service as the LocalSystem account and disable all services that are not needed. Jumes ([Jume98] pp.179 – 180) shows a list of recommended services to run on a variety of servers.

The COMNAP/COMNODE Entries

The COMNAP and COMNODE named pipes are used for SNA sessions with certain clients (OS/2, Win95, Windows 3.x and LanMan 2.2c) who are trying to connect to a Microsoft SNA Server (service) running on a Windows NT 4.0 box.

It appears that the SNA Server is made up of three parts, SnaServer, SnaBase, and the SnaDMO services. A client will connect initially to the SnaBase service to find a list of valid SNA servers. This is done using the COMNAP null connection (no authentication is needed). Once the client chooses a server, it will then connect using the COMNODE null session. After the initial connection, the client will authenticate itself to the SNA server, but the initial connection is still done via a null session.

The SQL\QUERY Entry

The SQL\QUERY named pipe provides null connectivity to Microsoft's SQL Server running on a Windows NT 4.0 box. Most site installations of SQL usually require

users to be authenticated to access a database. Therefore, even on the SQL server, this service can typically be deleted. But an example of a situation where the named pipe is still needed is where the SQL Server is on a different system than the Internet Mail Service server. See the [KBase] Q182228 entitled "XFOR: Error Message: Cannot Get List of Local Domains" for a more complete description of the problem. The following is an excerpt from [KBase] Q182228 which briefly states how the Internet Mail Service server connects to an SQL Server:

> *"Internet Mail Service runs under the Inetinfo process. Inetinfo starts in the context of the system account. When Internet Mail Service needs to query the SQL database, it uses the system account, which uses null credentials to access a SQL pipe on the SQL Server computer."*

The SPOOLSS Entry

The SPOOLSS named pipe provides null connectivity to the Spooler service (Print Server). Typically SPOOLSS can be removed even from the Print Server without causing too many problems. An example of a problem that could crop up is when a third-party software package adds entries into the following registry keys:

> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services\LanmanServer\Parameters\NullSessionShares
>
> -and-
>
> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlset\Services\LanmanServer\Parameters\NullSessionPipes

The [KBase] Q162695 article entitled "SMSINST: 'Access Denied' Message When Connecting to a Printer" outlines the type of problem as shown below:

> *"Although printing is still possible, users of computers running Windows NT Workstation that connect to a network printer share see "access denied" in the printer window caption when they do the following:*
>
> 1. *On the Start menu, point to Settings, and click Printers.*
> 2. *Double-click the shared network printer icon.*
>
> *Therefore, the printer queue that is displayed is empty and the user cannot control (for example, delete or cancel) his or her own print jobs."*

The LLSRCP Entry

The LLSRPC named pipe provides null connectivity to the RPC Interface of the License Logging Service (License server[34]).

The EPMAPPER Key

The EPMAPPER named pipe provides null connectivity to the Endpoint Mapper which can list all the applications that are using RPC[35] (Remote Procedure Call). This service defines ports to the applications. See [RkitS] pp. 44 – 46 of the "Microsoft Windows NT Server Networking Guide" for a description of the Remote Procedure Call.

The LOCATOR Entry

The LOCATOR named pipe provides null connectivity to the name-service provider service. The default name-service provider on Windows NT 4.0 is the Microsoft Locator. See [RkitS] pp. 49 – 51 of the "Microsoft Windows NT Server Networking Guide" for a description of the Multiple Universal Naming Convention Provider (MUP) and the Multi-provider Router (MPR) or [MSED922] pp. 269 for a description of MUP and MPR.

Locating The Key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

1. The key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" should still be displayed in the registry editor from the last step, but if it is not, repeat the previous steps shown for Figure 31 to locate the key again before continuing.

Removing the Data Contained Within The Sub-Key Value NullSessionPipes

The value "NullSessionPipes" is located in the right-hand window of the registry editor. Double-clicking on the sub-key value, NullSessionPipes, will bring up a window so that the contents of the value can be edited (See Figure 39).

[34] See [KBase] Q193218 entitled "Configuring License Service Replication in Windows NT Server 4.0" and [KBase] Q185953 entitled "How License Service Keeps Track of License Usage" for more details.
[35] See [KBase] Q142024 - How to Configure the Windows NT RPC Name Service Provider.

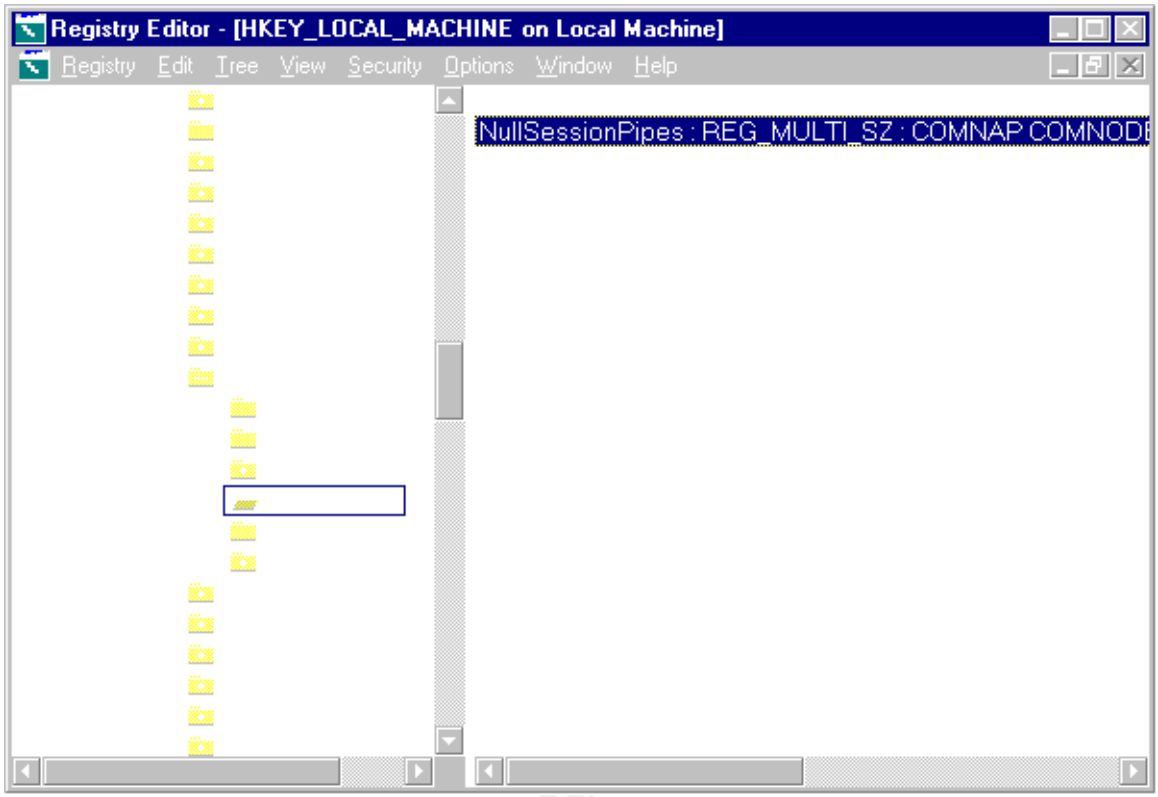

Figure 39 The view of the registry before removing the values within NullSessionPipes.

1. Highlight the items shown below in the "Data" window (See Figure 40) and press the "Delete" key on the keyboard.

   COMNAP
   COMNODE
   SQL\QUERY
   SPOOLSS
   LLSRPC
   EPMAPPER
   LOCATOR

2. Click on the "OK" button on the "Multi-String Editor" window.

3. Close the "Registry Editor" window.

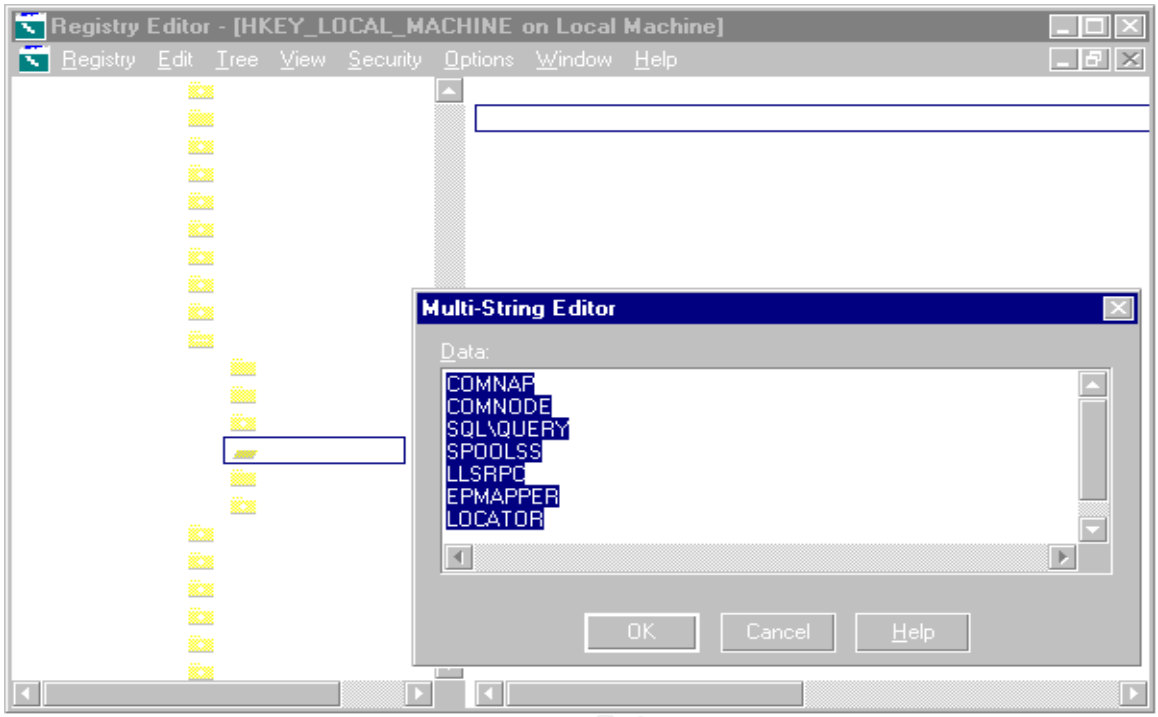

Figure 40 Deleting the values within NullSessionPipes.

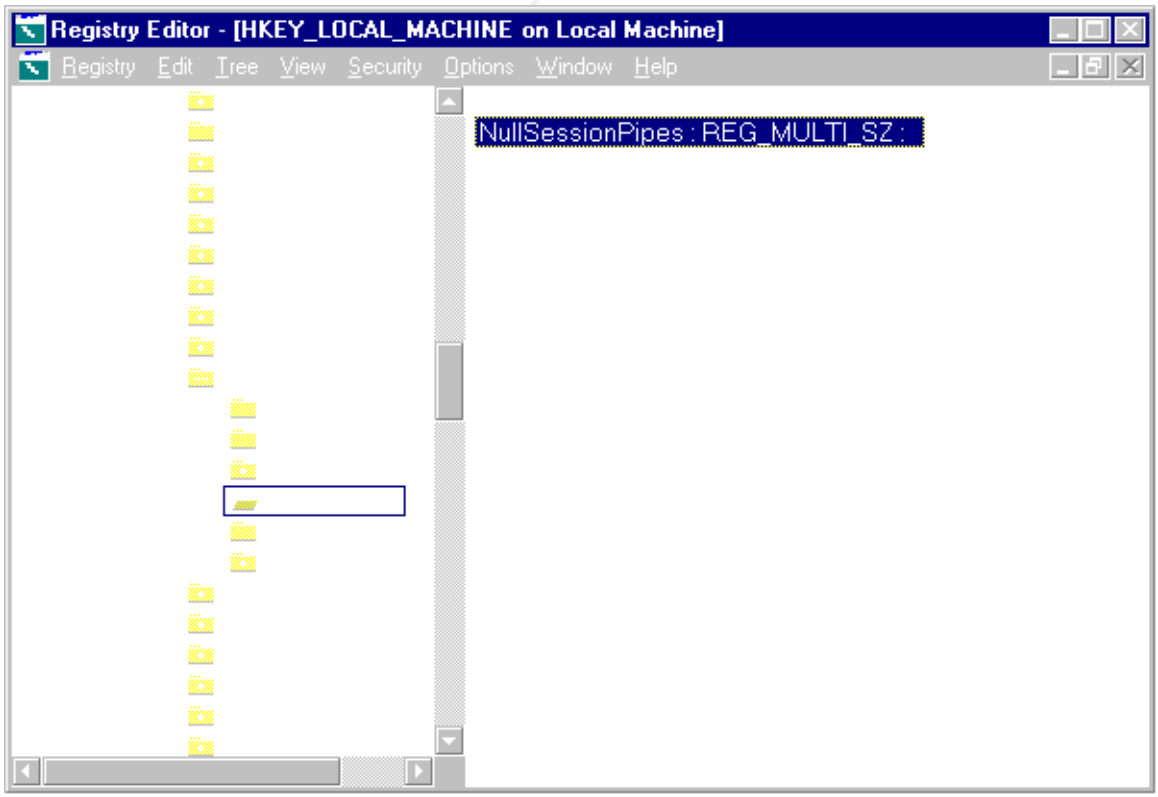

Figure 41 The view after the values within NullSessionPipes have been removed.

Enabling The Changes Made To The Registry

To enable the changes that were made to the registry, the system will need to be rebooted.

1. Close all open applications/windows.

2. Bring up the "Shut Down Windows" window by left clicking on the "Start" button on the "Task Bar" and select "Shut Down…".

3. After the window "Shut Down Windows" appears, select the radio button labeled "Restart the computer?" then click on the "Yes" button.

Logging Onto the System

If the system rebooted successfully, then log onto the system with an account that has the rights to edit the registry and reboot the system. If the system fails to reboot or crashes while trying to log onto the system, then you may need to take appropriate steps to recover your system. If you have been able to log onto the system, proceed to the next step.

Updating The Emergency Repair Disk

Checking the Modifications Made to the Registry

Use the "%SystemRoot%\System32\Regedt32.exe" program to verify that the changes you have made to the registry are correct and close the registry editor once verified.

Updating the Emergency Repair Disk (ERD)

1. Archive the previous copy of the SAM and Security database files located in the directory "%SystemRoot%\Repair" along with the previous set of ERD disks.

2. Using a new set of diskettes, create a new ERD disk with the command:

   "%SystemRoot%\System32\Rdisk.exe /S".

3. Store the new ERD disk in a secure location.

Backing Up The Registry Keys

Dumping The Registry Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

1. Enter the following command[36] at the "Command Prompt" (See Figure 42):

   C:\NTResKit\RegDmp.exe HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Control\Lsa > HKLM_SYS_CCS_Lsa_0006031625.txt

See Appendix A for an example of the text file that was created in this step.

Dumping The Registry Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

1. Enter the following command in the "Command Prompt":

   C:\NTResKit\RegDmp.exe HKEY_LOCAL_MACHINE\SYSTEM\
   CurrentControlSet\Services\LanmanServer\Parameters >
   HKLM_SYS_CCS_Ser_LS_P_0006031625.txt

See Appendix B for an example of the text file that was created in this step.

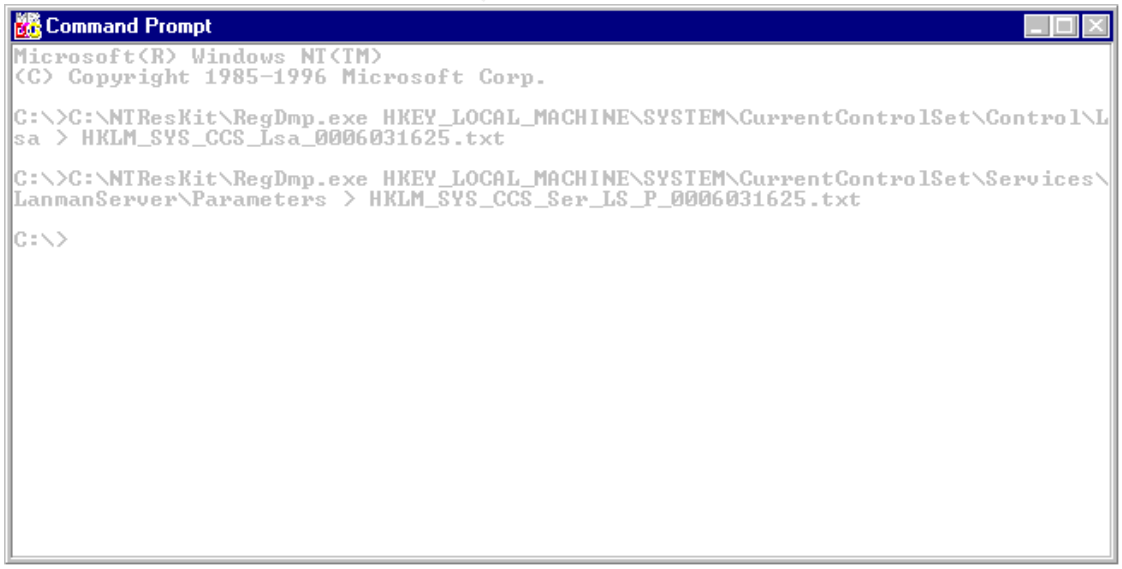

Figure 42 Backing up the registry keys that were changed.

[36] Due to space limitations the length of some commands within this document may be continued on another line.

5. Conclusion

The information that was presented here is just a very small part of securing a system. Yet, just making the four (4) changes to the registry, presented here, can have a profound effect on how your systems operate. Before you make any changes to your system, you have to know where the server/workstation will be located, who might have access to the server, what the server will be used for, and what services you will be running or might be running in the near future.

To avoid creating opportunities for someone you don't want in your system, you should load the bare minimum on the system in question that you can get away with. Do you really need games on the corporate PDC? Also, if a service or socket is not needed on the system, then disable them. If a service is needed, then see if the service will support running under a specific domain ID. If the service does require null credentials, then you may want to rethink where you run the service.

Now some sites may not be able to or want to implement the changes shown here, the type of security measures you enact at your site has to be weighed by the resources you have at hand versus their benefits. And once you put a security measure in place, it will always be an on-going task, because every time a software package is added or a service patch is applied, you will need to verify that your security system is still viable.

6. Appendix A

HKLM_SYS_CCS_LSA_0006031415.txt

The following is how the registry key for HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA appears before anonymous login was disabled.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA [8 1 17 5]
    Authentication Packages = REG_MULTI_SZ "msv1_0"
    Bounds = REG_BINARY 0x00000008 0x00003000 0x00002000
    Notification Packages = REG_MULTI_SZ "FPNWCLNT"
    AccessProviders
        ProviderOrder = REG_MULTI_SZ "Windows NT Access Provider"
        Windows NT Access Provider
            ProviderPath = REG_EXPAND_SZ
%SystemRoot%\system32\ntmarta.dll
    MSV1_0
        Auth1 = FPNWCLNT
```

HKLM_SYS_CCS_LSA_0006031625.txt

The following is how the registry key for HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA appears after anonymous login was disabled.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa [8 1 17 5]
    Authentication Packages = REG_MULTI_SZ "msv1_0"
    Bounds = REG_BINARY 0x00000008 0x00003000 0x00002000
    Notification Packages = REG_MULTI_SZ "FPNWCLNT"
    RestrictAnonymous = REG_DWORD 0x00000001
    AccessProviders
        ProviderOrder = REG_MULTI_SZ "Windows NT Access Provider"
        Windows NT Access Provider
            ProviderPath = REG_EXPAND_SZ
%SystemRoot%\system32\ntmarta.dll
    MSV1_0
         Auth1 = FPNWCLNT
```

7. Appendix B

HKLM_SYS_CCS_Ser_LS_P_0006031415.txt

The following is how the registry key for HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters appears before null session access to named pipes and shares was disabled. Or before the default name pipes or shares were removed.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
            NullSessionPipes = REG_MULTI_SZ "COMNAP"  \
                                            "COMNODE"  \
                                            "SQL\QUERY"  \
                                            "SPOOLSS"  \
                                            "LLSRPC"  \
                                            "EPMAPPER"  \
                                            "LOCATOR"
            NullSessionShares = REG_MULTI_SZ "COMCFG"  \
                                             "DFS$"
            Size = REG_DWORD 0x00000003
            Lmannounce = REG_DWORD 0x00000000
```

HKLM_SYS_CCS_Ser_LS_P_0006031625.txt

The following is how the registry key for HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters appears after null session access to named pipes and shares was disabled and the default named pipes and shares have been removed.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
    NullSessionPipes = REG_MULTI_SZ
    NullSessionShares = REG_MULTI_SZ
    Size = REG_DWORD 0x00000003
    Lmannounce = REG_DWORD 0x00000000
    RestrictNullSessAccess = REG_DWORD 0x00000001
```

8. References

The following material was drawn upon in the creation of this document:

[Fris98] Essential Windows NT System Administration, by Aeleen Frisch, O'Reilly & Associates, ISBN: 1-56592-274-3, (February, 1998)

[Gonc98] Windows NT 4.0 Server Security Guide (Prentice Hall Series on Microsoft Technologies), by Marcus Goncalves, Marcus Gonsalves, Prentice Hall PTR, ISBN: 0-13-679903-5, (May 1998)

[Hadf97] Windows NT Server Security Handbook, by Lee Hadfield, Que Corporation, ISBN: 0-7897-1213-X, (July 1, 1997)

[Jume98] Microsoft Windows NT 4.0 Security, Audit, and Control (Microsoft Technical Reference), by James G. Jumes, Microsoft Press, ISBN: 1-57231-818-X, (December 1998)

[KBase] Microsoft's Knowledge Base, is available in several forms, including [TechNet], and at URL: http://www.microsoft.com/ via the search function. Knowledge Base articles are given a unique access code number, for example doing a search of "Q131735" on the Microsoft's web site will retrieve all articles referencing Q131735 as well as a URL link to "Q131735 - How to Create Windows NT Boot Floppy Disks" which is the document in question.

Q118501 - INF: Troubleshooting SQLMail with Post Offices, Last Reviewed: March 20, 1999, URL: http://support.microsoft.com/support/kb/articles/Q118/5/01.asp

Q122857 - RDISK /S and RDISK /S- Options in Windows NT, Last Reviewed: December 8, 1999, URL: http://support.microsoft.com/support/kb/articles/Q122/8/57.ASP

Q126726 - INF: Using SQLMail with a NetWare Post Office, Last Reviewed: April 16, 1999, URL: http://support.microsoft.com/support/kb/articles/Q126/7/26.asp

Q131735 - How to Create Windows NT Boot Floppy Disks, Last Reviewed: September 17, 1999, URL: http://support.microsoft.com/support/kb/articles/Q131/7/35.asp

Q132679 - Local System Account and Null Sessions in Windows NT, Last Reviewed: February 17, 1999, URL: http://support.microsoft.com/support/kb/articles/Q132/6/79.asp

Q140556 - Securing SNA Server to Not Require Everyone: Read Access, Last Reviewed: April 5, 2000, URL: http://support.microsoft.com/support/kb/articles/Q140/5/56.asp

Q142024 - How to Configure the Windows NT RPC Name Service Provider, Last Reviewed: February 3, 1999, URL: http://support.microsoft.com/support/kb/articles/Q142/0/24.asp

Q143474 - Restricting Information Available to Anonymous Logon Users, Last Reviewed: March 28, 2000, URL: http://support.microsoft.com/support/kb/articles/Q143/4/74.asp

Q156328 - Description of Windows NT Emergency Repair Disk, Last Reviewed: July 28, 1999, URL: http://support.microsoft.com/support/kb/articles/Q156/3/28.asp

Q161048 - SNA Server Cannot Find the Share COMCFG or file COM.CFG, Last Reviewed: February 29, 2000, URL: http://support.microsoft.com/support/kb/articles/Q161/0/48.asp

Q162695 - SMSINST: "Access Denied" Message When Connecting to a Printer, Last Reviewed: September 2, 1999, URL: http://support.microsoft.com/support/kb/articles/Q162/6/95.asp

Q168015 - Files Not Replaced When Running Emergency Repair on X86 Intel Systems, Last Reviewed: February 28, 2000, URL: http://support.microsoft.com/support/kb/articles/Q168/0/15.ASP

Q174296 - Writes to User Property Database Do Not Occur, Last Reviewed: July 20, 1999, URL: http://support.microsoft.com/support/kb/articles/Q174/2/96.ASP

Q178640 - Could Not Find Domain Controller When Establishing a Trust, Last Reviewed: January 30, 1999, URL: http://support.microsoft.com/support/kb/articles/Q178/6/40.ASP

Q182228 - XFOR: Error Message: Cannot get list of local domains, Last Reviewed: September 7, 1999, URL: http://support.microsoft.com/support/kb/articles/Q182/2/28.ASP

Q184018 - Novell NDS for Windows NT Does Not Support Restrict Anonymous Security, Last Reviewed: February 5, 1999, URL: http://support.microsoft.com/support/kb/articles/Q184/0/18.ASP

Q185953 - How License Service Keeps Track of License Usage, Last Reviewed: January 20, 2000, URL: http://support.microsoft.com/support/kb/articles/Q185/9/53.ASP

Q186146 - Double-Clicking .reg File Will Not Add Extended ANSI Values, Last Reviewed: February 9, 1999, URL: http://support.microsoft.com/support/kb/articles/Q186/1/46.ASP

Q193218 - Configuring License Service Replication in Windows NT Server 4.0, Last Reviewed: January 25, 2000, URL: http://support.microsoft.com/support/kb/articles/Q193/2/18.ASP

Q196603 - Windows NT after installation of Service Pack 4, Last Reviewed: August 16, 1999, URL: http://support.microsoft.com/support/kb/articles/Q196/6/03.ASP

Q220871 - SNA Server LUs Assigned To Authenticated Users Group Do Not Work Properly, Last Reviewed: March 11, 1999, URL: http://support.microsoft.com/support/kb/articles/Q220/8/71.ASP

Q236158 - Winnt32.exe and Setupdd.sys Are Not Included with Downloadable Versions of SP4, SP5, and SP6, Last Reviewed: December 17, 1999, URL: http://support.microsoft.com/support/kb/articles/Q236/1/58.ASP

[Okun] Windows NT Security Programming Easy-to-Use Security Options, by Nik Okuntseff, R & D Books, ISBN: 0879304731

[Osbo98] Windows NT Registry a Settings Reference, by Sandra Osborne, New Riders, ISBN 1-56205-941-6, (September 18, 1998)

[MSDN] MSDN Online Library, Microsoft, URL: http://msdn.microsoft.com/default.asp

[MSED689] Supporting Microsoft Windows NT Server 4.0 Enterprise Technologies Student Workbook, by Microsoft Corporation, Microsoft Education and Certification Course Number: 689, (December, 1996)

[MSED922] Supporting Microsoft Windows NT 4.0 Core Technologies Delivery Guide, by Microsoft Corporation, Microsoft Education and Certification Course Number: 922, (May, 1997)

[MSJDec94] Learn System-Level Win32® Coding Techniques by Writing and API Spy Program, by Matt Pietrek, MSJ Vol. 9 No. 9 (December 17th, 1994), URL: http://www.microsoft.com/MSJ/backissues96.asp

Topic – Registry Entries, URL: http://msdn.microsoft.com/library/default.asp?URL=/library/tools/catapult/prereg.htm

Topic – Interprocess Communications, URL: http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/winbase/services_11tg.htm

Topic - The LocalSystem Account, URL: http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/winbase/services_11tg.htm

[RkitS] Microsoft's Resource Kit for Windows NT Server 4.0. This product is typically included in [TechNet] or the product can be purchased separately

[Stur98] Working with Unicenter TNG, by Rick Sturm, Que. ISBN 0-7897-1765-4, (August 1998)

[TechNet] Microsoft's Technet information service is available by subscription from Microsoft and is distributed monthly on CD-ROM

Windows NT 4.0 Domain Controller Configuration Checklist, Last Reviewed: March 29, 2000, URL: http://www.microsoft.com/TechNet/security/dccklst.asp

[TRS99] Windows NT Security Guidelines Considerations & Guidelines for Securely Configuring Windows NT in Multiple Environments A Study for NSA Research, by Trusted Systems Services, URL: http://www.trustedsystems.com, (June 3rd, 1999)

The following books were reviewed in the preparation of this text, but none were made reference to within this document:

[Heyw98] Inside Windows Nt Server 4 (Second Edition), by Drew Heywood, New Riders Publishing, ISBN: 1-56205-860-6, (February 1998)

[Mcln99] Windows NT Security, by Michael McInerney, Prentice Hall PTR, ISBN: 0-13-083990-6, (September 14, 1999)

[Ruts97] Windows NT Security: A Practical Guide to Securing Windows NT Servers and Workstations (McGraw-Hill Ncsa Guides), by Charles B. Rutstein, McGraw-Hill, ISBN: 0-07-057833-8, (April 1997)

[Solo98] Inside Windows NT (Microsoft Programming Series), by David A. Solomon, Microsoft Press, ISBN: 1-57231-677-2, (May 1998)

Last Updated: October 19th, 2017

Upcoming Training

SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**vLive**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
Univ. of California - SEC505: Securing Windows and PowerShell Automation	**Los Angeles, CA**	**Jan 29, 2018 - Feb 03, 2018**	**vLive**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS Security West 2018	**San Diego, CA**	**May 11, 2018 - May 18, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**