Global Information Assurance Certification Paper

Step by Step Procedures for Securing a Computer Training Lab

Introduction: During the "Windows Security" Track of SANS Network 2000 in Monterey, CA Jason Fossen and Jennifer Kolde spoke briefly about "special types of users," such as contractors, temporary employees, or guests. These users must be given special consideration when granting them access to domain resources because of their unique situations. As an NT system administrator, I have had to deal with several special types of users, and decided to expand upon this topic for my practical. This document will focus on users that must be given access to domain resources for training purposes, and the special considerations that must be given to them in order to maintain an effective but secure training environment on a network that hosts a training lab.

Background: This practical has been developed based upon an actual requirement for the establishment of a computer-training lab, which will reside on a military base. Specific requirements are outlined to illustrate the various types of unique issues that must be considered when establishing a training lab. For the purposes of this document, emphasis will be placed on three major topics:

1) Configuring the Windows NT server that controls the training lab so that it is reliable and secure, keeping in mind that the server's primary function is to control account access to the Training Lab computers.
2) Assuring that the user accounts created for this environment serve the training users adequately, but do not create or exploit security vulnerabilities.
3) Deploying the System Policy Editor to assure that the training workstations are protected from the "happy fingers" of the students who will be using them.

Types of Training Anticipated:

- Job related training, such as time and attendance, payroll, inventory, or any server based application that is used in the performance of an employee's regular duties.
- Training in the use of off-the-shelf software, such as Office 2000 or programming languages, such as Visual Basic.
- Internet based training.
- Training sponsored by the local college, which teaches a number of evening courses on base and has an arrangement with the Training Department to use the computers in the lab.

Training User Considerations:

Personnel who will be using the computers for training come from various groups, such as:

- Current employees who already have accounts on the primary domain.
- Current employees who do not have domain accounts because their job functions do not require them to have domain access.

- Local college students and instructors who do not have accounts on the domain.

Hardware and Network Considerations:

- The facility contains 15 computers with Windows NT Workstation licenses for each one.
- One Windows NT Server will be dedicated to managing and administering these machines; it is located in a secured computer facility in a separate building.
- The training lab has existing connectivity to the backbone network on the military base and an adequate number of network connections to support all the workstations in the training lab. The training lab's network segment is behind a firewall.
- To restate the previous point, the training facility is connected to an operational military network which processes Unclassified Sensitive (US2) data. For this reason, it is especially important to assure that the security requirements of the military organization are met.
- No Remote Access Services or dialup networking are permitted on the server or workstations.

Facility Considerations:

- The training lab is located in a dedicated training facility on the base; the facility also contains office spaces for Training Department employees. Additional physical controls exist to secure the training lab so that it may only be opened or made available for use by authorized personnel.
- One full time employee is assigned the duty of training coordinator for the lab. He is responsible for controlling access to the lab spaces, coordinating training schedules for lab usage, and assuring that the computers and network connections are in proper working order. He does not perform maintenance on the computers; rather, he keeps apprised of the status of the computers (before, during, and after training sessions) and notifies technical support personnel regarding any discrepancies. In the event of his absence, other personnel in the training department perform these duties as needed.

Class Format Considerations:

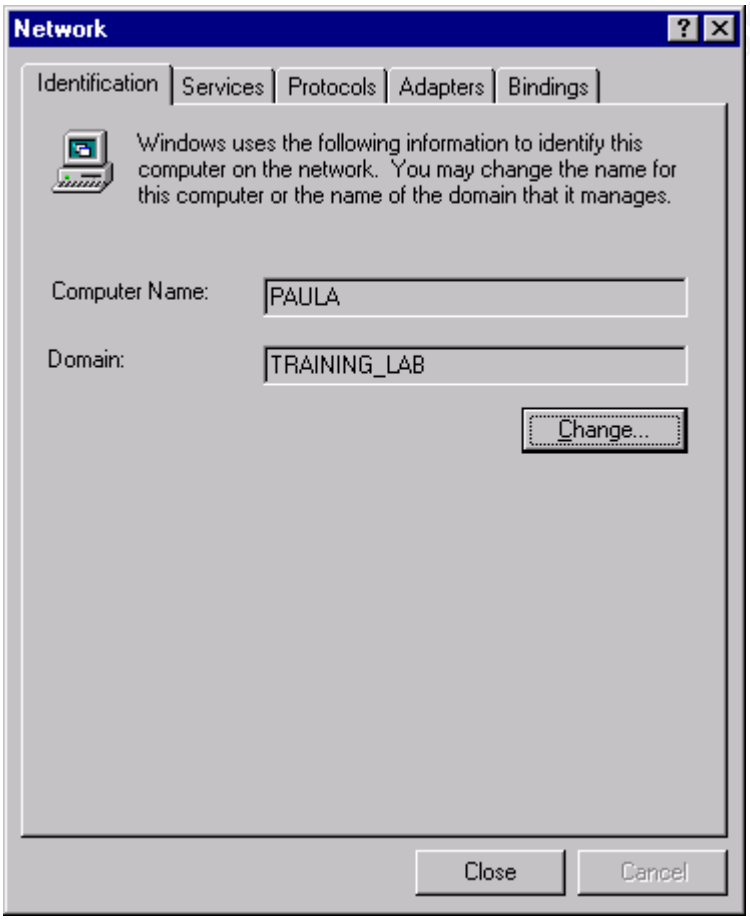
- Organized classes for employees generally take place during work hours (between 8:00 AM and 5:00 PM), and run from one day to a couple of weeks.
- Organized classes for college students take place at a specific day and time (for example Tuesdays from 7:00 to 10:00 PM) and run for a period of several weeks to a few months.
- There is no "open lab time" available in the training lab; it is used solely for organized class meetings. College students who require additional computer time must use the computer lab that is located at the local campus.

Additional Note: This document is by no means intended to be comprehensive in all aspects of securing a Windows NT environment. It is simply meant to illustrate some of the unique issues facing administrators who must deal with "special users" on the network. Although this document is specific in many aspects to a training lab environment, many of the same concepts could be applied to other special types of users, such as contractors or subcontractors, temporary employees, official visitors who require network or workstation access, or foreign nationals. The intention is to highlight some of the basic security issues and steps that may be taken to minimize their impact to the organization.

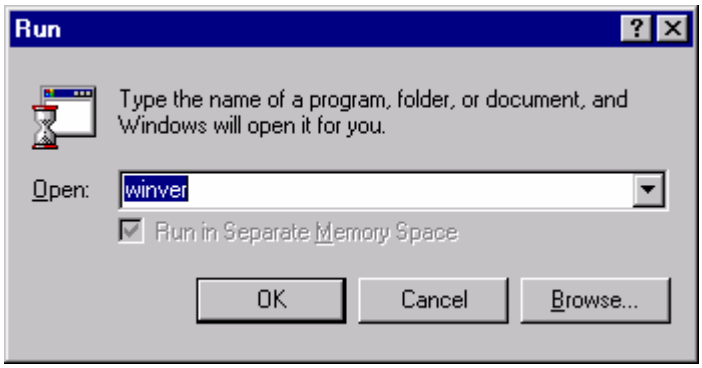
Part One
Securing the NT Server Environment

1. Install Windows NT Server 4.0 on the computer that will control the 15 NT workstations in the lab. The server will be loaded using standard installation procedures "out of the box"; therefore, the actual software installation procedure will not be covered in detail.

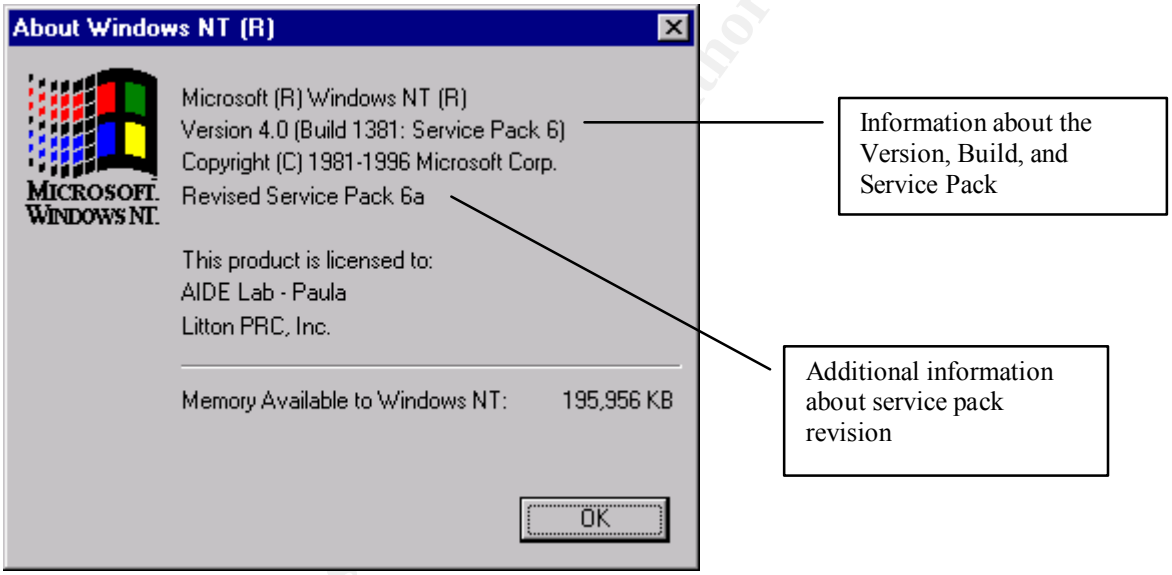
2. Since the training lab resides on an existing operational network for a military base, it is crucial to assure that there are no security vulnerabilities introduced into this network as a result of the addition of the lab. Therefore, as a first step, the Windows NT Server and the fifteen workstations will reside on their own separate, non-trusted domain on the network. This domain will be called "TRAINING_LAB."



3. Assure the latest service packs are loaded on the server. Check for current build and service pack by clicking START, RUN, WINVER.



The following screen will be displayed:



Service Pack 6a is the most current as of the creation of this document; therefore, we have assured that the latest Service Pack is indeed installed. The latest Service Pack is always available at windowsupdate.microsoft.com.

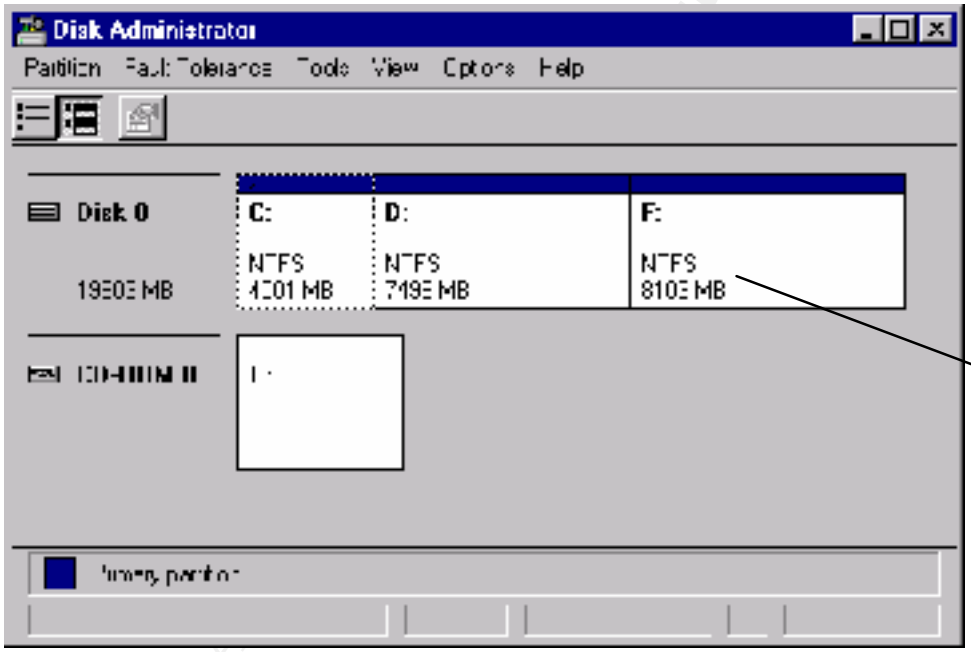
A note about hotfixes: Although often necessary to fix important system problems or plug dangerous security holes, they are not always thoroughly regression tested and often not "supported" by Microsoft. When considering whether to implement the latest hotfixes, it is important to decide if a particular fix is necessary. If so, it is crucial to load and test the hotfix on a non-production system, and to make a complete backup before loading it into a production environment. If the hotfix is not necessary, it is often better to wait until the next Service Pack, when hotfixes and other new features have been more thoroughly tested before inclusion. It is still important to perform system backups before loading new Service Packs and/or hotfixes to any system.

4. Assure that all partitions are formatted NTFS (NT File System). This provides for file level security via the use of ACLs (Access Control Lists), which is not available in FAT (File Allocation Table) formatted partitions. In addition to the its security advantages, NTFS also provides for file compression in Windows NT as well as support for large disk partitions (greater than 4GB). If any partitions are formatted FAT, they may be converted to NTFS using the CONVERT.EXE utility which is included with Windows NT. The syntax is as follows:

   CONVERT drive: /FS:NTFS [/V]

drive	Specifies the drive to convert to NTFS. Note that the current drive may not be converted
/FS:NTFS	Specifies to convert the volume to NTFS
/V	Specifies that Convert should be run in verbose mode

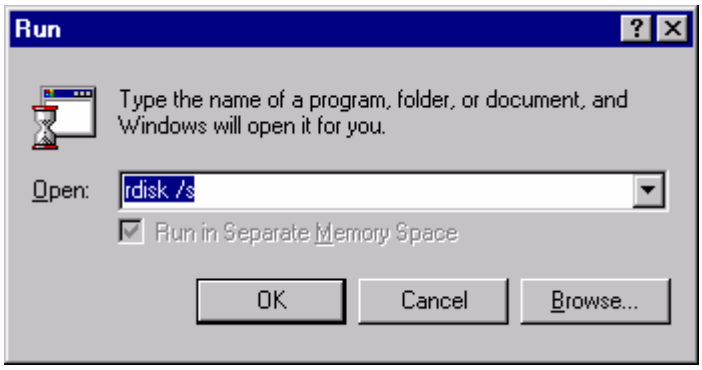
To verify that partitions are formatted NTFS, click on Start, Programs, Administrative Tools (Common), Disk Administrator. The display will be similar to the following:



There are some situations where FAT partitions are necessary. For example, if an NT machine will also boot to a disk using any other operating system such as DOS, Windows 9x, Novell, Linux or OS/2, it must be formatted FAT. However, in our scenario, all disks will be partitioned NTFS.

5. Create an Emergency Repair Disk (ERD) for the server, and update it often. An option to create an ERD is given during the initial setup process; it may also be created or updated in the following manner:

Click Start, Run on the computer. At the command line, type in RDISK /S



Note that by default, the RDISK command does not copy the current user account database (SAM) to the ERD. The "/S" must be added to copy the current SAM. Add a minus "-" sign after the "S" (RDISK /S-) to eliminate dialog boxes and copy the ERD files to the \winnt\repair folder instead of a floppy.

Set Policies to Meet Security Requirements. Microsoft's Security Configuration Manager (SCM), available in Service Pack 4 or later, provides an array of templates to assist in configuring the security of NT servers and workstations. It is provided as a snap-in to the Microsoft Management Console (MMC). With the SCM, policies and ACL requirements may be easily and conveniently established. [1]

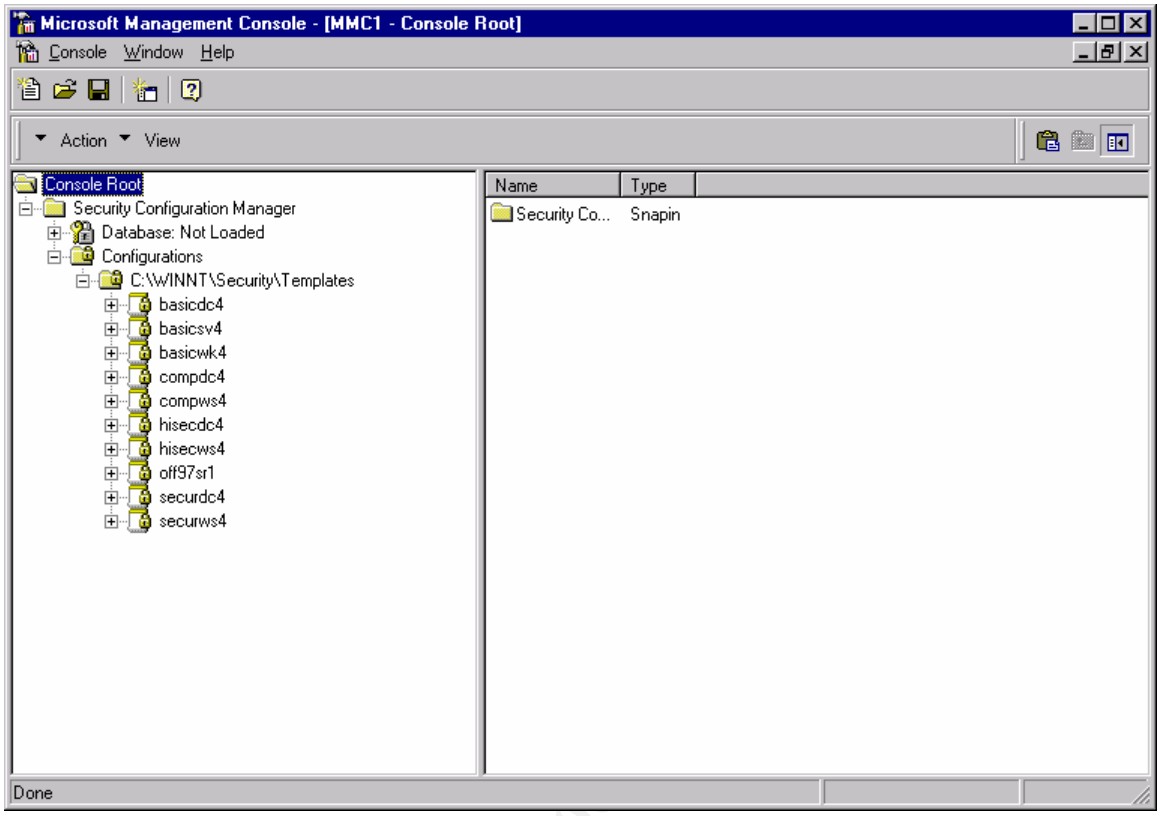
To open Security Configuration Manager (assuming it has been installed from a Service Pack 4 or later CD):

Click Start, Run. At the command prompt, type, "MMC.EXE".

When the Microsoft Management Console window is displayed, click Console, Add/Remove Snap-in, Add, Security Configuration Manager. Click OK.

Expand the "Security Configuration Manager" folder, then the "Configurations" folder, and finally the "Templates" folder (will look something like C\:Winnt\Security\Templates). Notice that there are several templates available for use.

[1] The SANS Institute, Windows NT Security Step-by-Step, SANS Network Security 2000, pp.321-325.



The built-in templates (in the order displayed on the screen) are as follows:

Template	Platform	Security
Basicdc4	NT 4 Domain Controller	Default
Basicsv4	NT 4 Server	Default
Basicwk4	NT 4 Workstation	Default
Compdc4	NT 4 Domain Controller	Somewhat Secure
Compws4	NT 4 Workstation or Server	Somewhat Secure
Hisecdc4	NT 4 Domain Controller	Highly Secure
Hisecws4	NT 4 Workstation or Server	Highly Secure
Off97sr1	NT 4 Workstation or Server	Somewhat Secure
Securdc4	NT 4 Domain Controller	Secure
Securws4	NT 4 Workstation or Server	Secure

The settings provided in the "High Security Domain Controller" (Hisecdc4) template are an excellent choice for securing accounts, the file system, and the registry. The following policies, which are based upon this template, provide a good basis for securing user accounts, performing auditing, and assignment of user rights.[2]

[2] Kapp, Justin, "Securing Windows NT," PC Network Advisor, Issue 115 (February 2000), pp. 11-12.

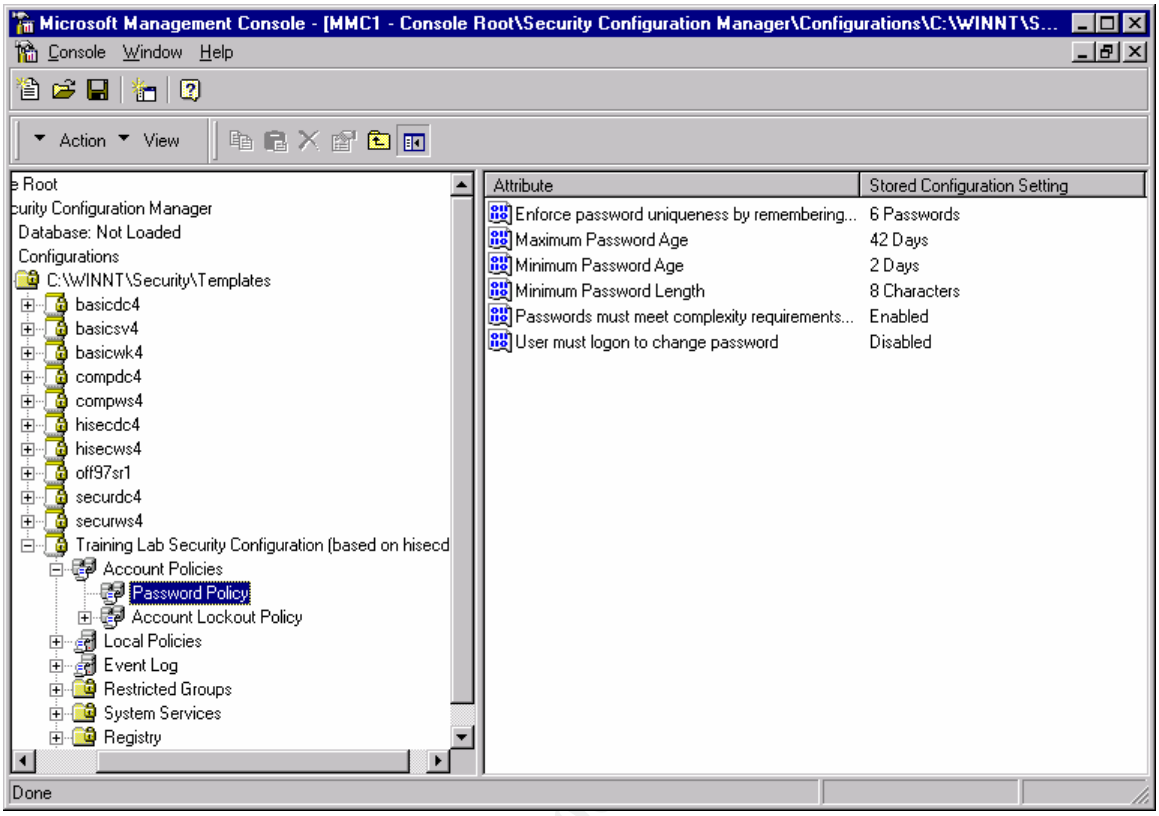
Password and Account Lockout Policies

Password Policy	
Enforce password uniqueness by remembering X number of passwords	6
Minimum password age	2 days
Maximum password age	42 days
Minimum password length	8
Complex passwords (passfilt.dll)	Enabled
User must logon to change password	Disabled
Account Lockout Policy	
Account lockout count	5
Lockout account time	Forever
Reset lockout count after	720 min.

Auditing and User Rights Assignment Policies

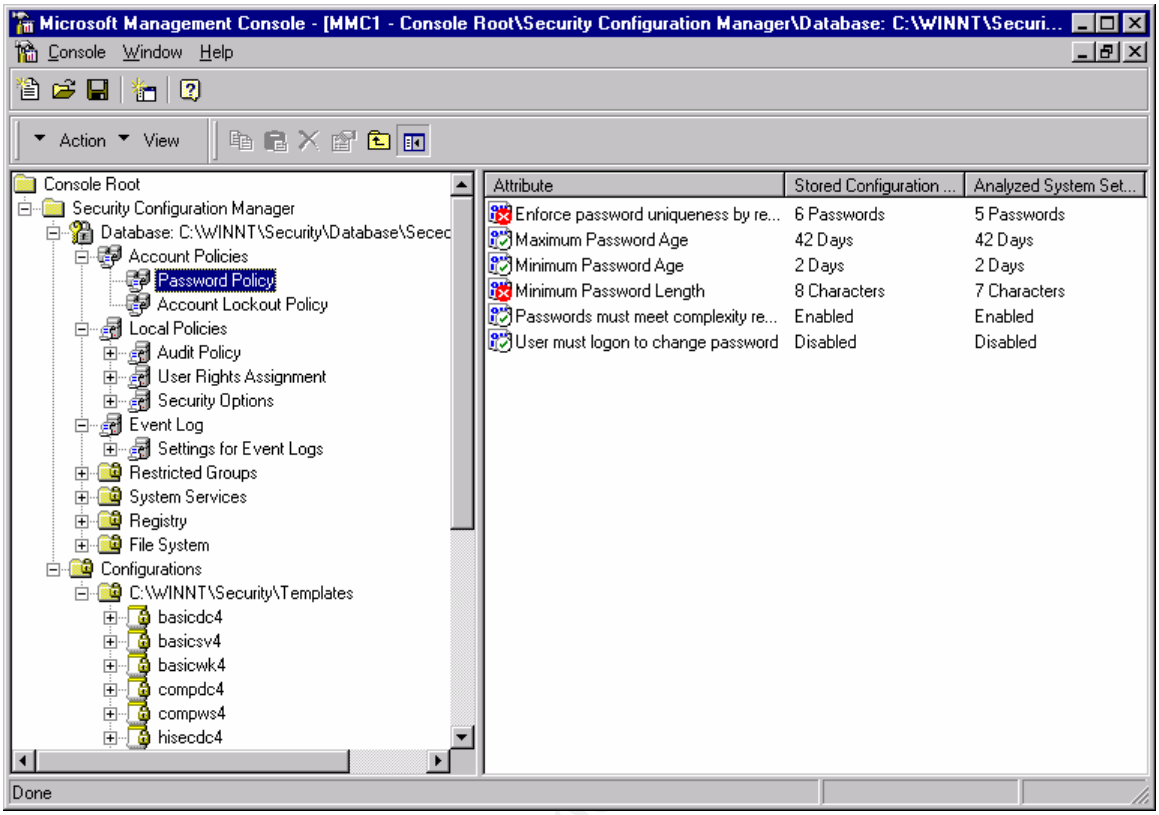
Audit Policy	
Audit account management	Success, Failure
Audit logon events	Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	None
Audit system events	Success, Failure

We will create a custom template based upon the Hisecdc4.inf, and then we will apply the template to configure our security settings. To begin, right click the "hisecdc4" template, and click "Save As." Name the file "Training Lab Security Configuration (based on hisecdc4).inf". Browse the custom template to see the security settings. Although it is possible to customize the template by changing various settings, we will leave them "as is" for the purposes of this document.



Notice from the screenshot above the default password policies for our template. It is possible to change these (or any other settings) simply by double clicking the item to be changed, and modifying it as desired.

Before a template may be applied, an analysis must be performed on the current configuration. Right click the database folder and click "Import Configuration." Double click "Training Lab Security Configuration.inf." Right click the database folder and click "Analyze System Now." Click OK to select the default log file location. The security analysis will be performed (it may take a few minutes). Once it is complete, the log file will be displayed in notepad. To see the results of the security analysis, expand the Database folder, then expand the individual subfolders. For example, an analysis of the password policies displayed the following:



Notice the colored icons displayed to the left of each attribute. These icons indicate conformance with the template that was used for the analysis:

Blue Icon with a Red "X": indicates that current settings do not conform to template
Blue Icon with a Green Checkmark: indicates that current settings conform to template
Blue Icon with No Markings: Setting is not defined in template

The columns to the right of the attributes indicate the Stored Configuration Setting (setting in the template) and the Analyzed System Setting (current configuration setting).

Before applying the template to change the settings on the machine, it is recommended to back up the current configuration settings. Right click the "Database" folder and click "Export Configuration." Type in a filename when prompted (i.e. "Original Security Settings" and click Save. By default, the exported file will be saved in the same location as the other template files (i.e. C:\WINNT\Security\Templates). Right click this folder and click "Refresh" to see the backed up configuration folder.

To apply the "Training Lab Security Configuration" template, right click the Database folder and click "Import Configuration." Double click the "Training Lab Security Configuration" template. Right click on the Database folder and click "Configure System Now." Click OK to accept the default log file location. The selected template will now be applied to the computer, and will modify the security settings accordingly. When the process is complete, you may verify the new settings by right clicking the

Database folder and clicking "Analyze System Now." Once the analysis is done, you may browse the folders located in the database folder to see the new policies.

The Application, System, and Security Log properties may also be set using the SCM. In general, log files should be set with a maximum size of about 100 MB, with the system overwriting events as needed, but only events older than 30 days. Only Administrators should be able to access the log files. In some cases, it may be advantageous to manually rotate logs and halt the machine if the logs become full; this would assure a full audit trail.

Note that there are many other steps available (and often necessary) for securing a Windows NT Server or Workstation. These include but are not limited to:

1. Disable all nonessential services
2. Assure adequate space for temporary and paging files
3. Enable NTLMv2 authentication
4. Employ SYSKEY.EXE to encrypt the SAM database, to prevent password hacking utilities from extracting LanMan and MD4 password hashes
5. Protect against "null sessions" being able to list vital machine information
6. Perform regular system backups
7. Have a detailed "restoration and recovery" plan in place at all times
8. Secure the user account environment (covered in more detail in next section)
9. Implement best practices for groups, user rights, and file permissions
10. Educate the users (security, password protection, "Social Engineering")
11. Update virus scanners regularly
12. Employ host and network-based intrusion detection systems
13. Dedicate the time and resources to ensure that security of systems and resources is a number one priority.

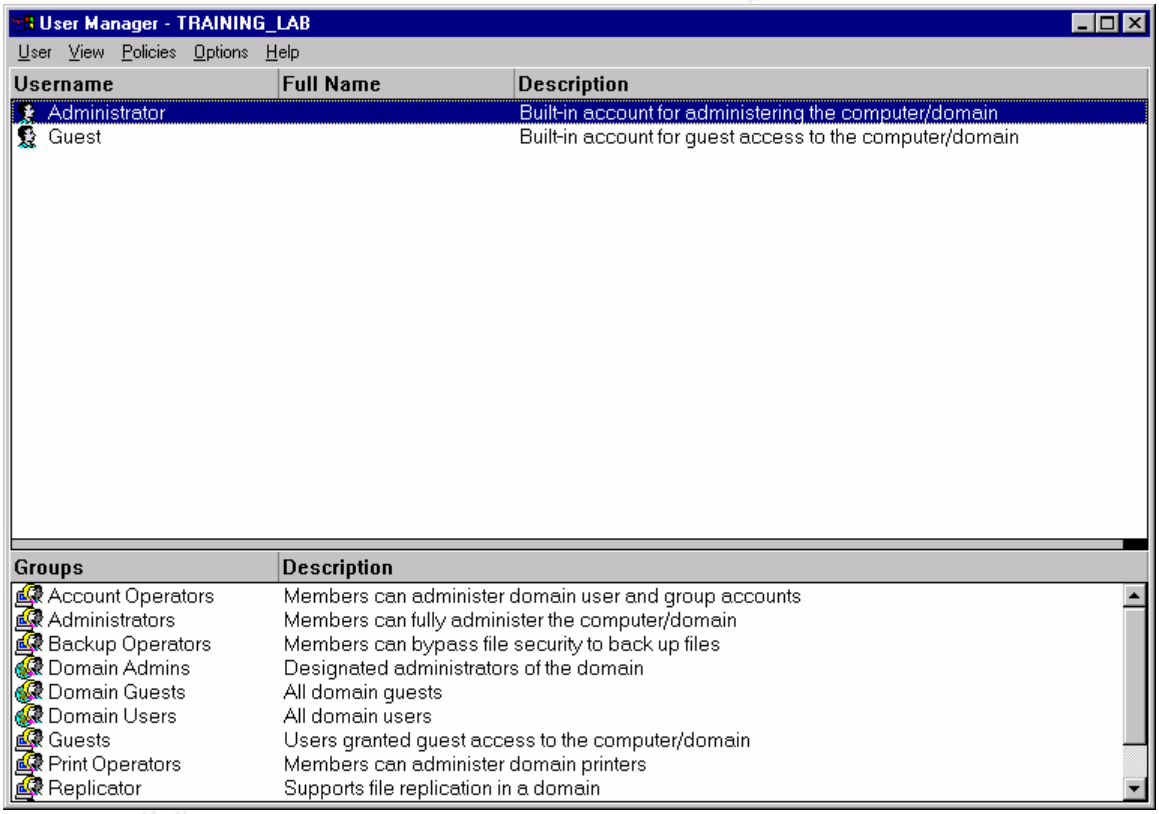
Although these items are extremely important to securing a Windows environment, they are beyond the scope of this project and will not be covered in detail, with the exception of securing the user account environment.

Part Two
Securing the User Account Environment

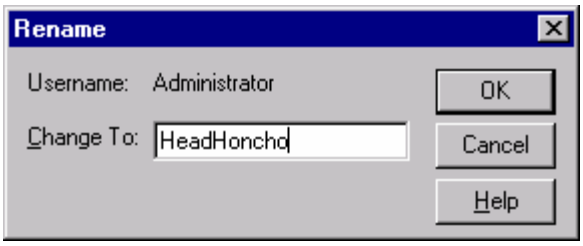
Since our non-trusted TRAINING_LAB domain will primarily be used to authenticate users and control access to the workstations in the training lab, we will pay special attention to the task of securing the account environment.

Rename the Administrator Account. For a potential hacker trying to break into a system, the job is much easier if has knowledge of a valid account on that system (especially an administrative account). Since the default administrative account on all NT Servers and Workstations is "Administrator," the first task after setting up an NT Server (or Workstation) should be to change the name of this account.

Click on Start, Programs, Administrative Tools (Common), User Manager for Domains.



Highlight the "Administrator" account, click on User, Rename. The following dialog box will appear:

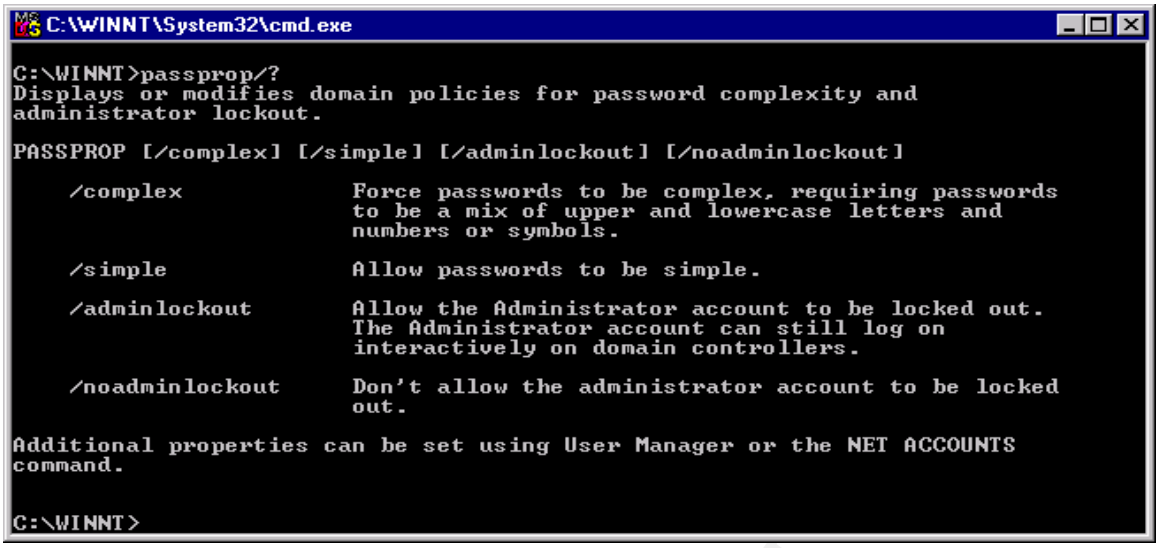


Type in the new name that is desired for the Administrator account and click "OK". The account name will be changed accordingly. Be sure to note what the administrator account name was changed to, especially if the feature "Do Not Display Last Username in Login Screen" is enabled in the registry. Changing the Administrator account name and subsequently forgetting what it was changed to can make the system inaccessible even to administrators!

Enable Administrator account lockout. By default in Windows NT, the Administrator account is never locked out by unsuccessful login attempts, which makes it a prime target for brute-force password cracking attempts. The PASSPROP.EXE utility (available in NT Resource Kit) makes it possible to lock out the Administrator account after reaching the threshold for failed login attempts. Once the account is locked out, it can only be accessed via interactive console login; it is no longer available for login across the network until the account has been unlocked. This is particularly useful to protect against brute force attempts, as well as simple password guessing attempts by users on the network.

Run PASSPROP.EXE interactively from the NT Resource Kit (\i386\netadmin), or copy it to the \winnt folder. It is a command line program; open a command line and navigate to the directory where PASSPROP.EXE resides. The parameters for PASSPROP are as follows:[3]

[3] Microsoft Technet, "Enforce Strong Passwords in NT 4.0," Windows Tips and Secrets, Platinum Technology, Inc., 1998.



To enable Administrator Lockout, type in the following command:

Notice the message stating that the Administrator account may be locked out except for interactive logons on a domain controller. Also notice that PASSPROP provides a means of enforcing strong passwords (discussed below):

Enforce strong passwords. The NT User Manager does not by default require that passwords be complex. Refer back to the PASSPROP.EXE help screen; you will notice that PASSPROP.EXE has the ability to enforce strong passwords, specifically a mixture of upper and lower case letters, symbols, or numbers.

PASSFILT.DLL, which was introduced in Service Pack 2, goes one step further than PASSPROP.EXE. By enabling the PASSFILT.DLL password filter, complexity

requirements will be enforced on passwords whenever they are changed. PASSFILT.DLL enforces very strong passwords by levying the following requirements:[4]

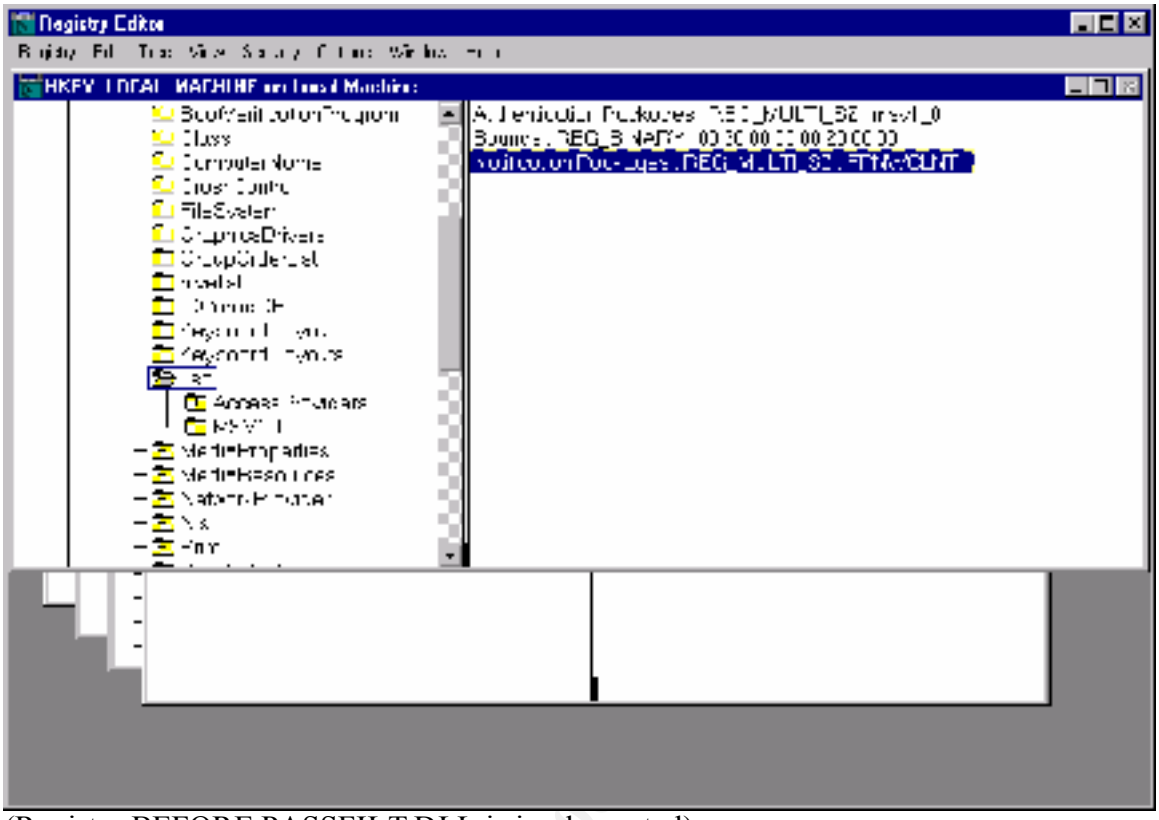
- Passwords must be at least six characters long
- They must contain three out of four of the following: upper case, lower case, numbers, or symbols
- PASSFILT will not accept the user name or any part of the full name as part of the password

After applying an appropriate Service Pack to the system, a registry edit must be made to enable password filtering.

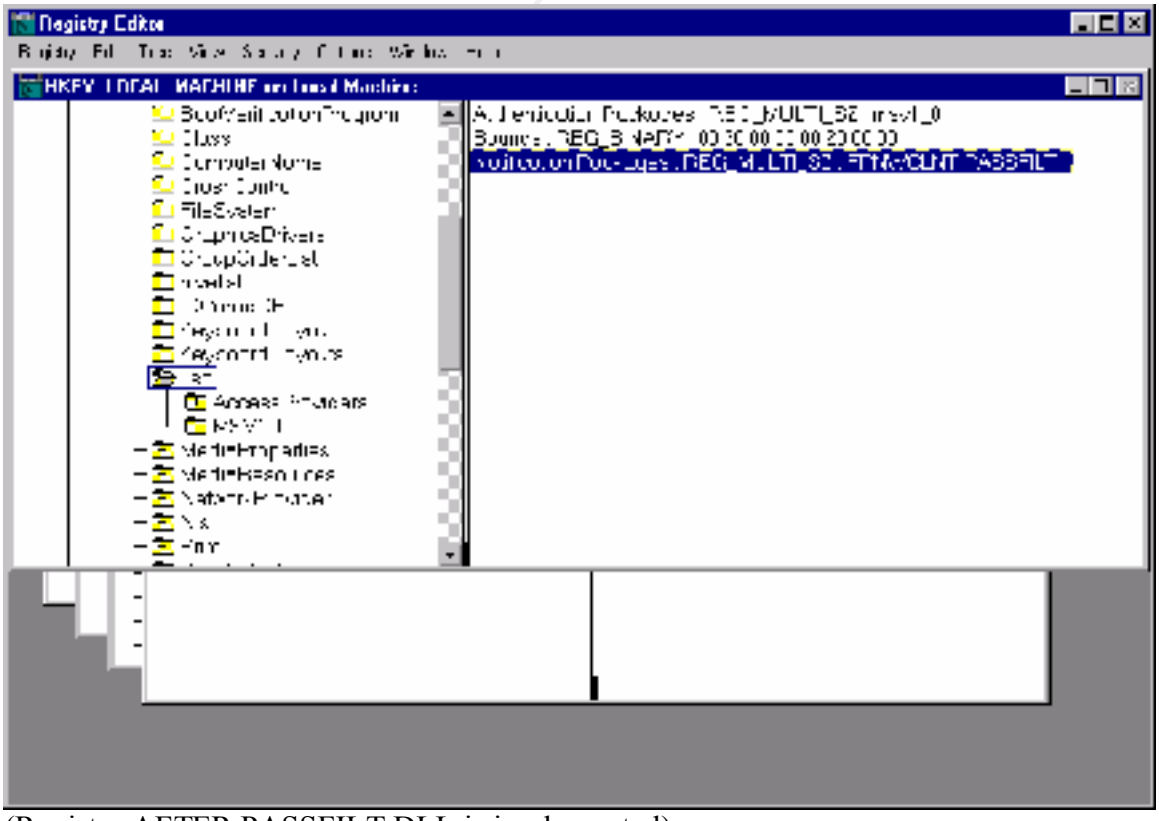
- Copy PASSFILT.DLL from SP2 to \WINNT\SYSTEM32.
- [Start]–Run–Type REGEDT32–[Enter].
- Create (or edit) the following Key: HKLM\SYSTEM\CurrentControlSet\Control\Lsa
- Add a REG_MULTI_SZ value called "Notification Packages" with a value of PASSFILT (If the value FPNWCLNT already exists, then edit the value and add PASSFILT under FPNWCLNT).
- Click OK then exit the Registry Editor [Alt+F4].
- Restart the server.

It should be noted that PASSFILT.DLL will only be enforced on subsequent password changes after it is enabled on the system; current passwords will not be affected. See the following page for registry settings before and after PASSFILT.DLL is implemented.

[4] "How to Enable Strong Password Functionality in Windows NT," Microsoft Knowledge Base Article ID: Q161990.



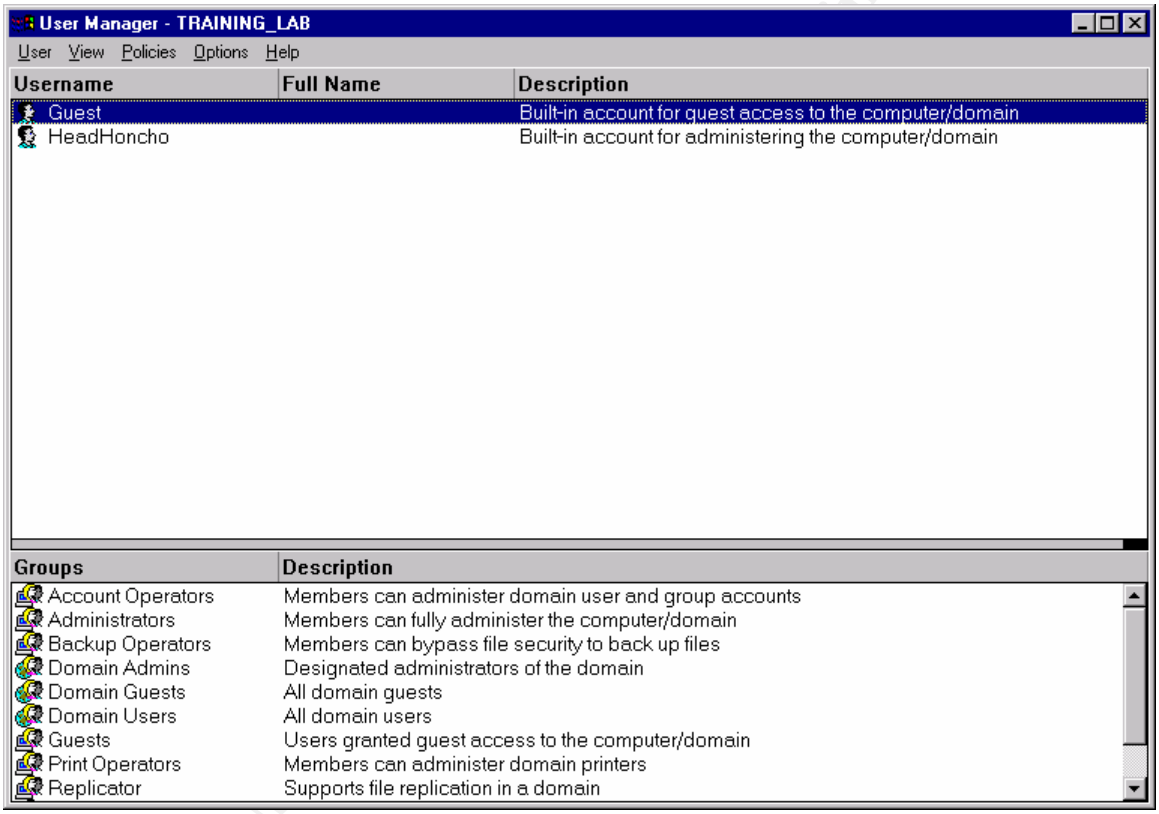
(Registry BEFORE PASSFILT.DLL is implemented)



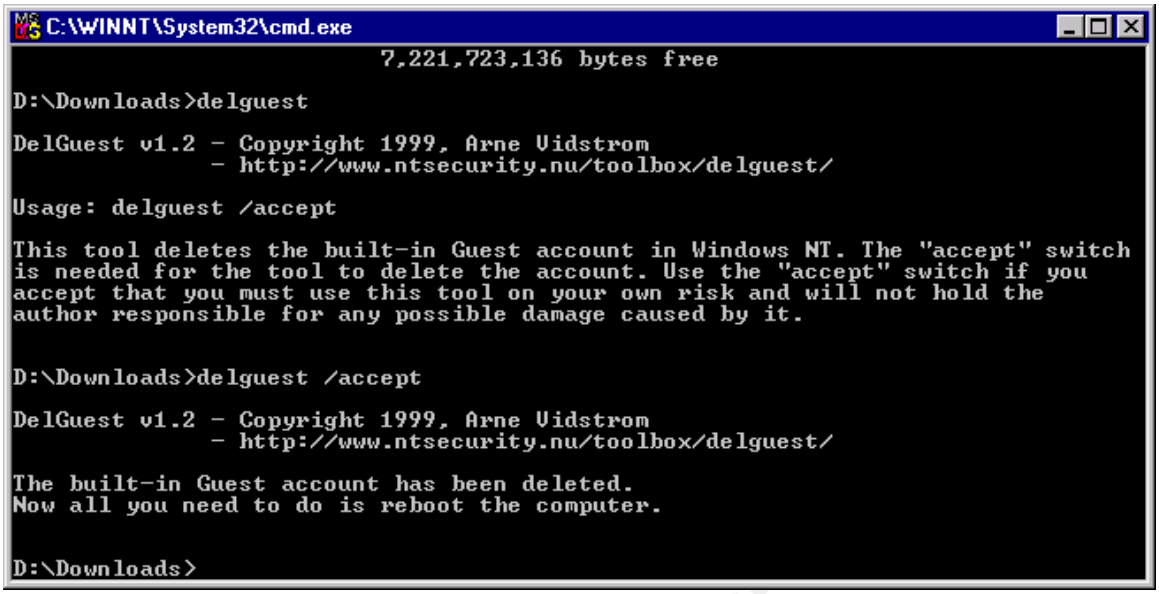
(Registry AFTER PASSFILT.DLL is implemented)

Delete or Disable the Guest account. Although in NT Server it is disabled by default, the risk exists for the account to be inadvertently enabled and made available for use. Microsoft does not provide a means for deleting the Guest account, but a third party utility, "DELGUEST", exists that will remove the account. This tool is available for download at http://ntsecurity.nu. It is advisable to update the Emergency Repair Disk before running this tool, especially since it is unsupported by Microsoft. In fact, it is wise to update the ERD frequently when loading new tools and utilities.

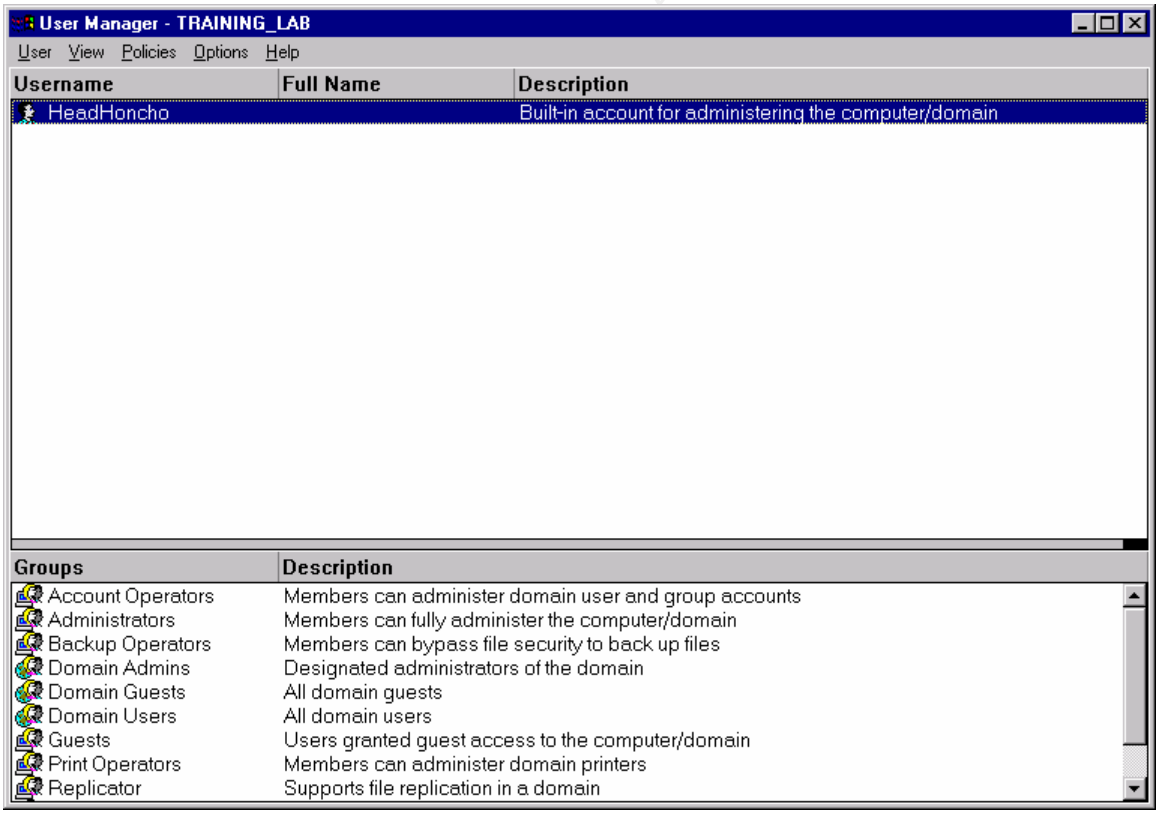
Download the Delguest utility to an appropriate directory on the system. Notice from the screenshot below that the Guest account still exists on the system.



Delguest must be executed from the command line. See below for the syntax and details of the execution. Note that the "/accept" switch must be included with the command in order for it to execute properly; by using the "/accept" switch, the user is acknowledging that the tool is to be utilized at the user's own risk. Again, it is very important to update the ERD immediately before running this utility.



Once delguest has been run, reboot the computer. Open "User Manager for Domains" again and notice that the Guest account no longer exists.



Many administrators will likely choose not to utilize the "Delguest" utility, since it is an unsupported tool and could be considered risky. In this case, disable the Guest account and remove any rights it has to the system. Also assure it has a non-blank password.

Establish and Enforce Policies to Control Access to the Workstations and the Domain. Listed below are the policies we will enforce to control access to the training lab workstations and the TRAINING_LAB domain. These policies are designed to provide a comprehensive and methodical way of administering the training lab. Special considerations are required because of the high "turnover" of users in and out of the training lab and the potential security vulnerabilities that are possible as a result.

1. Users will be required to read, fill out and sign a computer access request form. This form will detail the policies and rules for computer use and the consequences if they are not followed. The form will be available at the beginning of class, and will be required for each student to gain access to the computer. In addition, the form will specify access to a certain workstation (i.e. LAB6), and the student will be required to use the same workstation for the duration of the course. The training coordinator will perform the distribution and collection of the forms.

2. Users who have current accounts on the domain will still be required to fill out the forms mentioned in #1 above and use special training accounts, since the training lab domain will be non-trusted by the primary account domain. In addition, it will be necessary to be a member of the "Training Users" group or other special groups (discussed in detail later) in order to gain access to the appropriate training resources.

3. Since the training lab is located on a military installation, each workstation is required to display the standard government warning message (covered in detail later), which must be displayed and acknowledged by all users upon logging on to the computer.

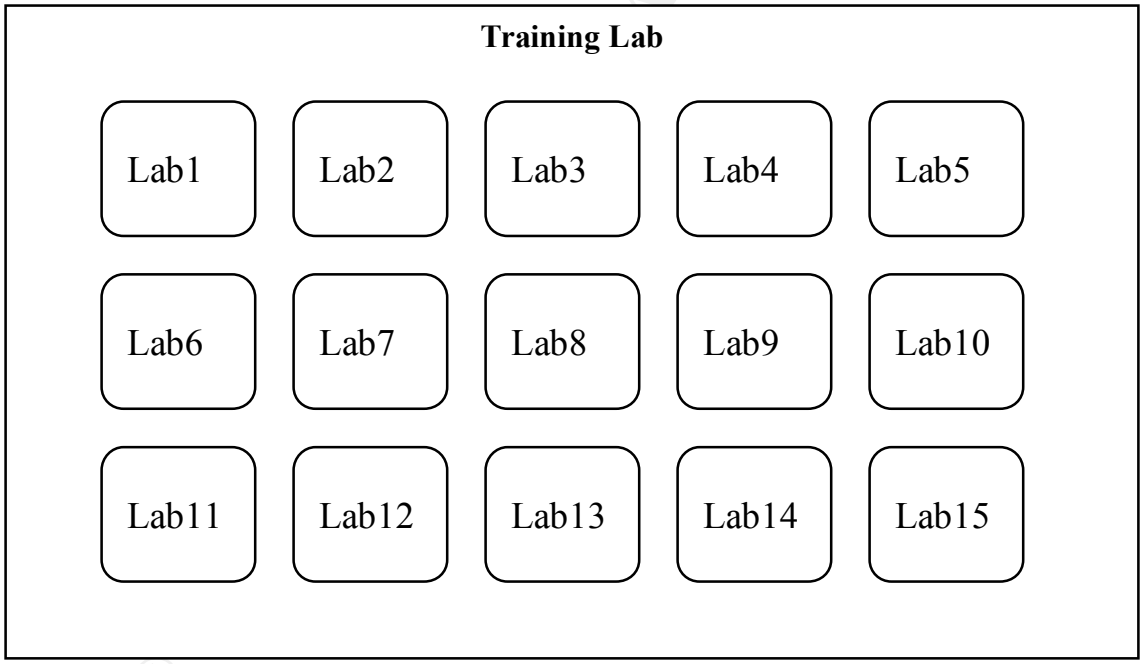
4. The domain account for use on the workstation will have the same or a similar name as the workstation itself (i.e. user account for workstation LAB3 will be "lab3". Time controls will be enforced (i.e. 8:00 to 5:00 only). In addition, each user account will only be allowed to log in at the specified workstation (i.e. account LAB1 may only log in to workstation LAB1).

5. By default, the computer accounts will always be disabled. When a class is scheduled, it is the responsibility of the training coordinator to notify the administrator of the dates and times of the class, and how many workstations will be required. The administrator will enable the appropriate number of training accounts immediately before commencement of the training session. In addition, he will set the passwords to some default password, and check the box "User required to change password at next logon" in the User Manager. He will notify the training coordinator of the default password for the workstations. When users begin their training, they will initially log on with the predefined default password, and will be required to change it at that time (keep in

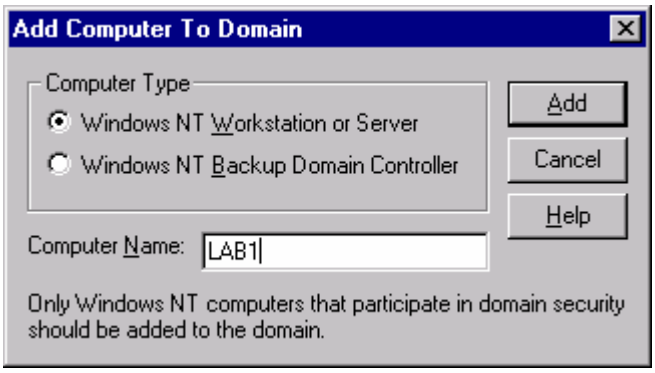
mind that we have enabled PASSFILT.DLL to require very complex passwords). At the end of the scheduled training session, the accounts will again be disabled. Note that a training session is considered the entire duration of the training, not each day of training.

6. For college courses that are held in the evening, a separate set of accounts will be set up. These will be established on a per course basis, and will be deleted at the end of the class. This is necessary and prudent because college courses generally last for three to four months, and are scheduled on particular nights of the week. Accounts will be set to expire at the end of the course. Again, these accounts will have names similar to those of the corresponding workstations and logon limitations will be enforced as in #4 above.

Connect the NT Workstations in the training lab to the non-trusted TRAINING_LAB domain. We will assume that we have already configured the 15 NT Workstations and loaded the latest Service Pack on them. The layout of the lab and machine names is as follows:

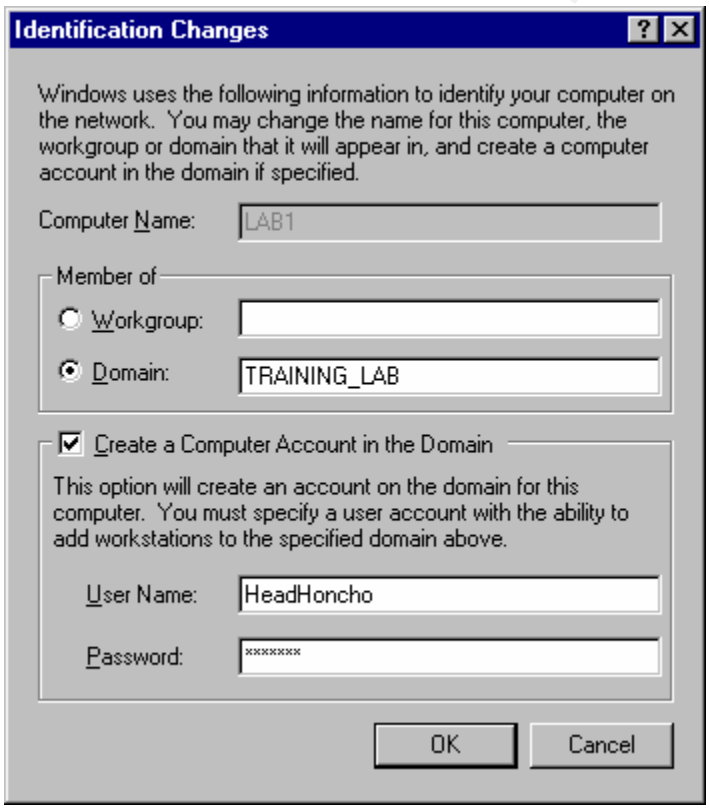


There are two ways of adding workstations to a domain. The first is by utilizing "Server Manager", and allows the addition of remote machines. Click Start, Programs, Administrative Tools (Common), Server Manager. From the Server Manager main window, click Computer, Add to Domain. The following window will be displayed:



Accept default of "Windows NT Workstation or Server", type in the name of the computer at the prompt for "Computer Name", and click Add. The workstation will be added to the domain. Perform this procedure for each of the 15 workstations in the training lab. This method is convenient in cases where the administrator is sitting in front of the server console with a list of machines to be added to the domain.

Assume that the administrator is in the training lab setting up the machines, and the domain server is located in a separate building. In this case, it is possible to add each workstation to the domain interactively from that workstation. Click Start, Control Panel, and double-click Network (or right-click Network Neighborhood, Properties). From the identification tab, click Change. The following screen will appear:



If the settings are still at their default, "Workgroup" will be selected with a workgroup called "WORKGROUP". Select "Domain" and type in the name of the domain to join (TRAINING_LAB). Check the box "Create a Computer Account in the Domain," which will create an account for this workstation on the domain. Enter a user name and password that has the right to add workstations to the specified domain. In this case we used "HeadHoncho," which is the administrative account for the domain. Click OK. In a few seconds a window will be displayed that says "Welcome to the TRAINING_LAB Domain." Perform this action for each of the fifteen workstations to make them members of the training lab domain.

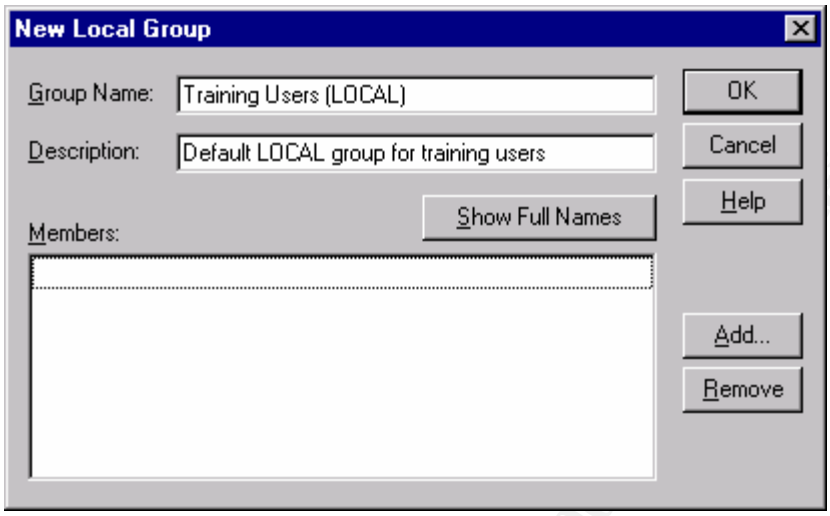
Create Global and Local Groups for Training Users. Creating groups before creating users is not necessary, but proves to be convenient when creating users and user templates, since group membership for that particular type of user may be predefined, instead of being performed as a separate step. Global groups categorize users based upon their particular job functions and access needs within the organization. Global groups are then "dropped into" local groups, which contain the appropriate rights and permissions for access to resources. Global groups may be dropped into local groups on other trusted domains (hence the term "global) as well as the local domain. Rights and permissions should never be assigned to global groups, and accounts should never be assigned to local groups. Depending upon the type of training being held, different types of local groups may need to be created to facilitate access to the appropriate machine resources. However, for the purposes of this document, one global group and one generic local group will be created to illustrate the process.

To create global and local groups, click Start, Programs, Administrative Tools (Common), User Manager for Domains. Once the User Manager window is opened, click User, New Global Group. The following window will be displayed:

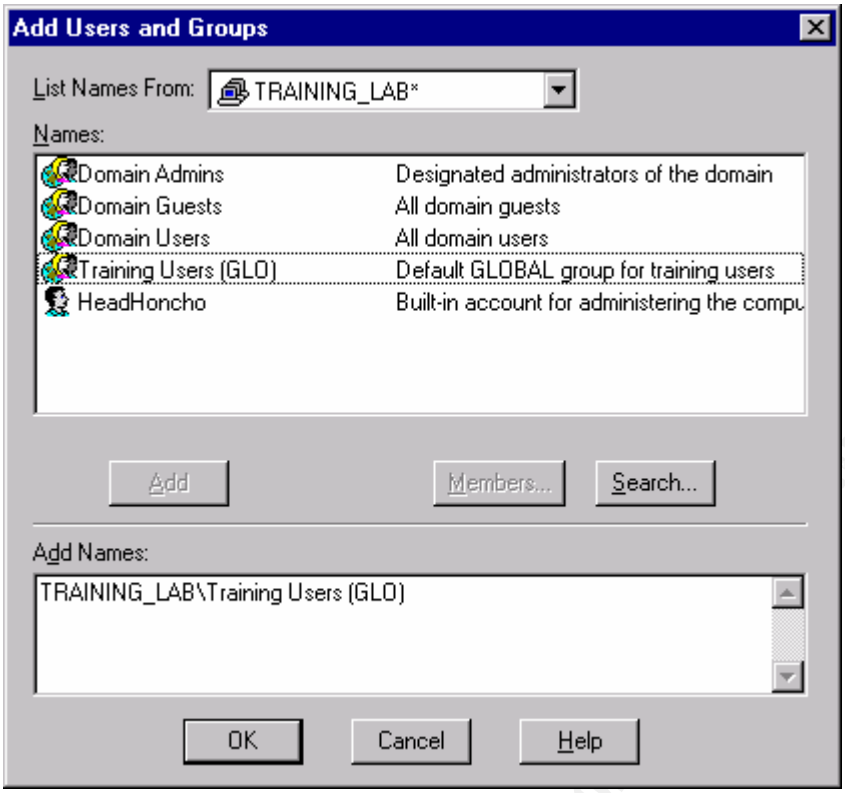
Type in the global group name and a description of the group. Be sure to include the words "global group" either in the group name itself, or in the description. This makes it

much easier to distinguish global groups from local groups in User Manager later. Keep in mind that the global group name field is limited to 20 characters, so it may be necessary to distinguish global groups from local groups in the description field. Remove "HeadHoncho" (administrator) from the group and click OK.

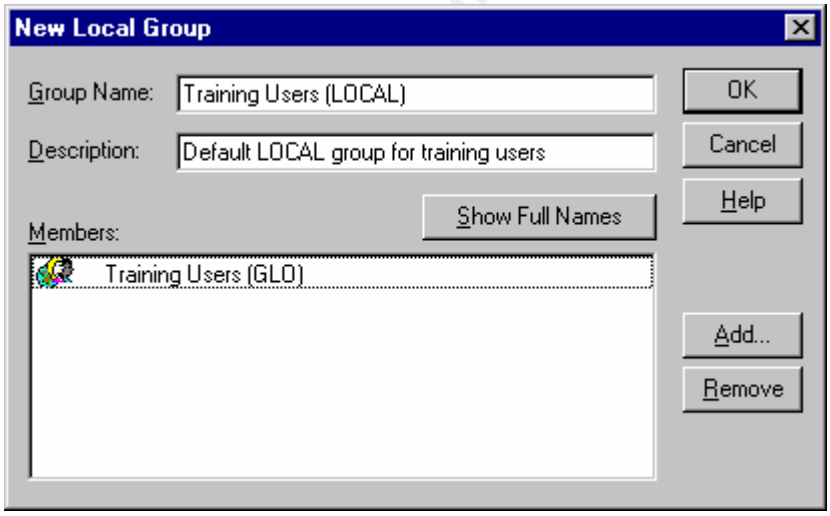
To create a local group, click User, New Local Group. The following window will be displayed:



Type in the local group name and a description of the group. Again, make sure to include the word "local" either in the group name or description to make it easier to distinguish. Click Add to drop the appropriate global group into the local group. The following window will be displayed:



Highlight "Training Users (GLO)" and click Add. The Training Users Global Group will be dropped into the Training Users Local Group. Click OK.

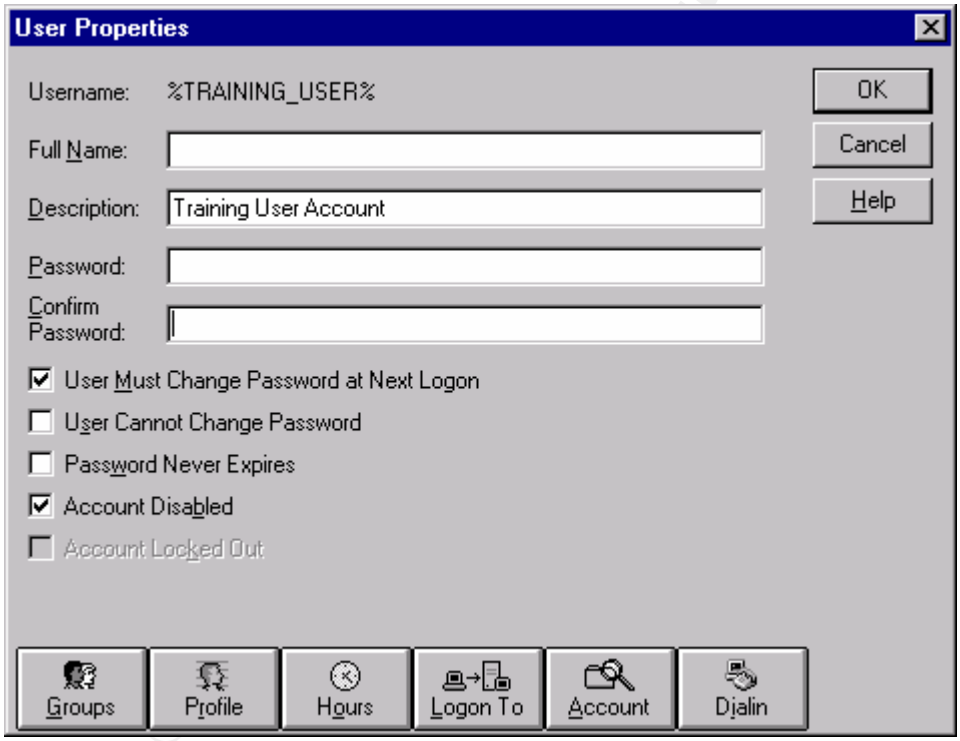


The Training Users Global Group will be displayed as a member of the Training Users Local Group. Click OK. Now it is possible to assign the proper rights and permissions to files and directories using the Training Users Local Group; the rights will then automatically be granted to the members of the Training Users Global Group.

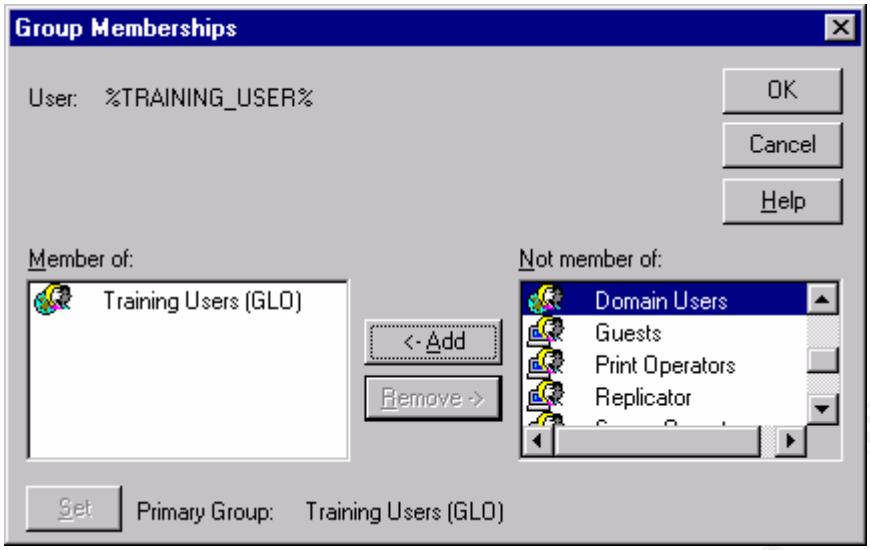
Assure local groups only have access to the minimum resources needed for training. As mentioned in the introduction, various types of training will be administered in the lab (i.e. software packages, internet access, corporate systems, various college courses). Different local groups may be necessary to control access based upon the type of training that is being given.

Create User Account Templates. The use of account templates eases the task of administration and decreases the probability of errors while creating the account by enabling the administrator to set defaults for various aspects of the account (i.e. Group Membership, time constraints, account expiration dates, etc.).

From User Manager, click User, New User. Create a "Training User" template that will be used for the typical users that will be in training during the regular workday. Assign a name to the template by enclosing it with "%" signs. Fill in all infomation that will be common to all accounts of this type. Disable the account. The "User Must Change Password at Next Logon" will be checked by default and should remain checked. The template will be similar to the following:

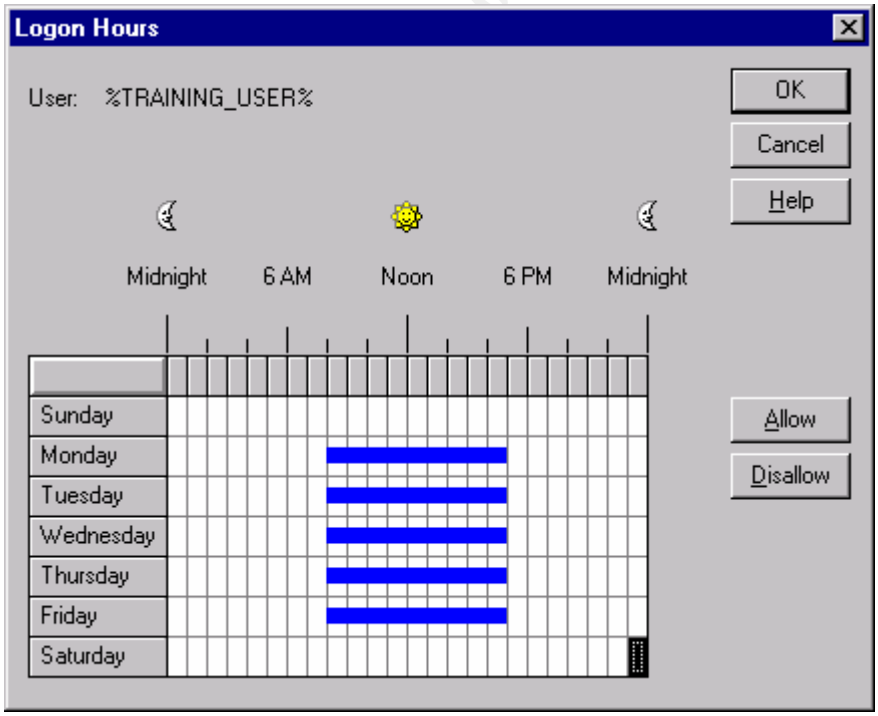


Click on the "Groups" tab. The following window will be displayed:

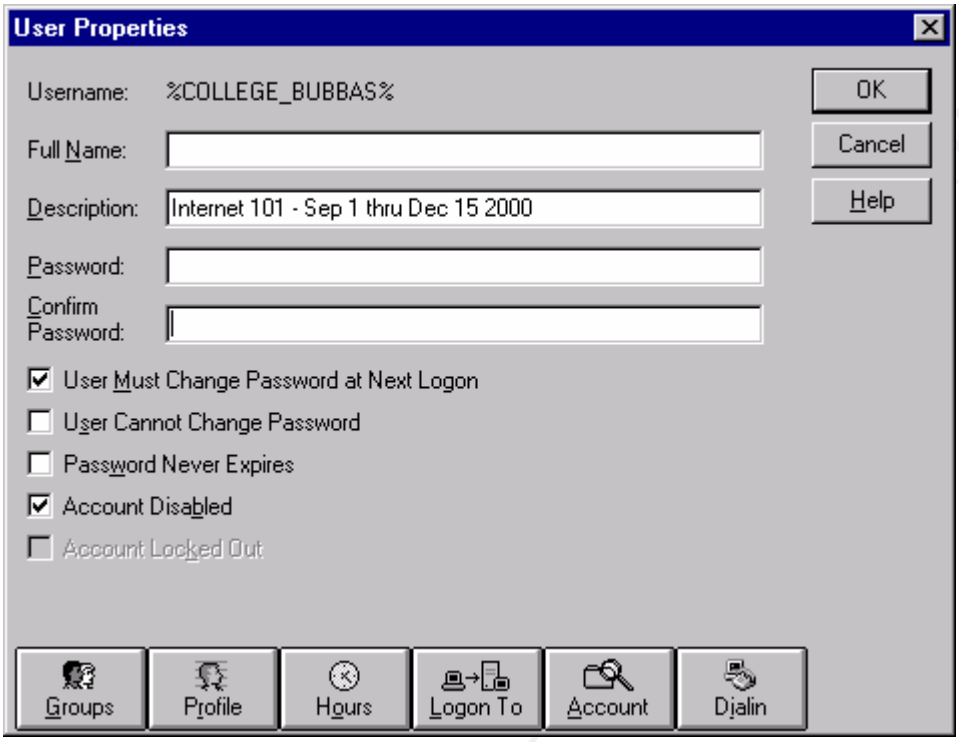


Remove the group "Domain Users", and add the Training Users Global Group. This assures that the accounts created using this template only have access to resources specifically intended for training users. Click OK.

Click the hours tab. By default, 24/7 access is allowed. Using the mouse, highlight all days and times when users are not allowed access to the domain. In our example, access is allowed Monday-Friday from 8:00 AM – 5:00 PM. Highlight all other times that do not fall into this window and click Disallow. Or, highlight the entire span of time when users are allowed access to the domain, and click Allow.

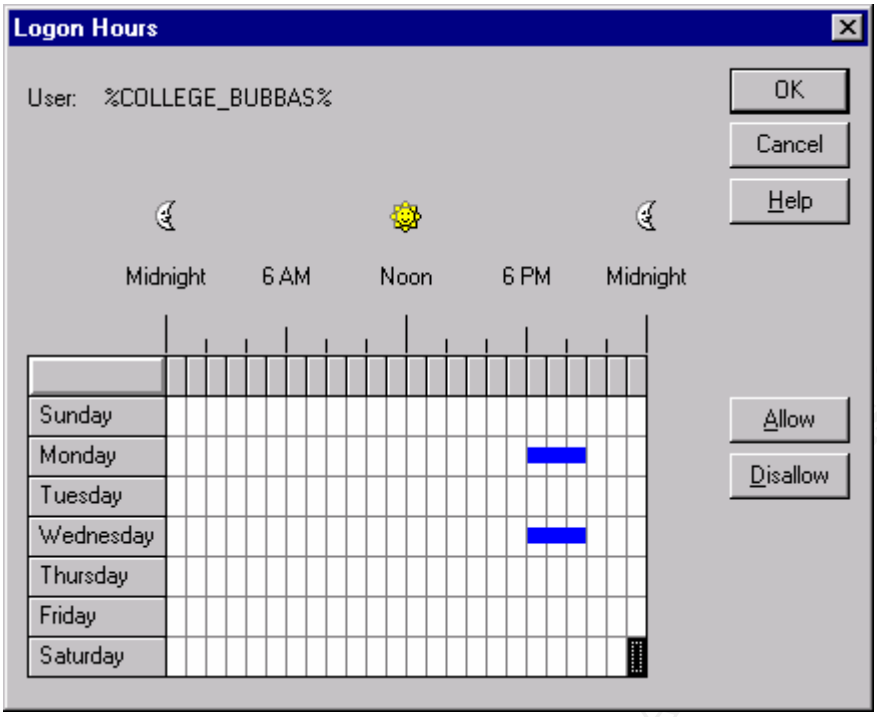


Create another template for the accounts that will be needed for an evening college course. Template creation will be essentially the same, with a couple of notable exceptions:

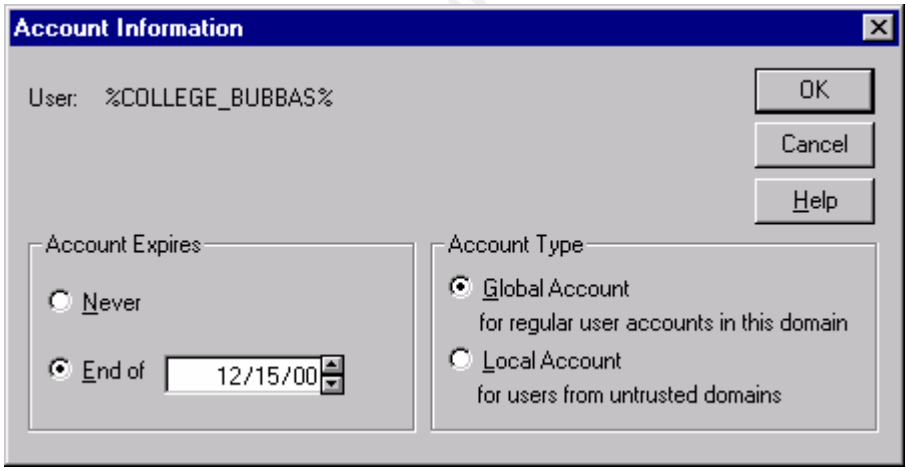


Create the user template using the same method as before. In the description field, type in specific information about the course and when it begins and ends. This will aid in administration duties later. Consider creating separate global and local groups for college student accounts, naming them something such as "College Hackers" ☺ and assuring that their access is kept to a bare minimum. Follow the same procedures as previously discussed for creating global and local groups.

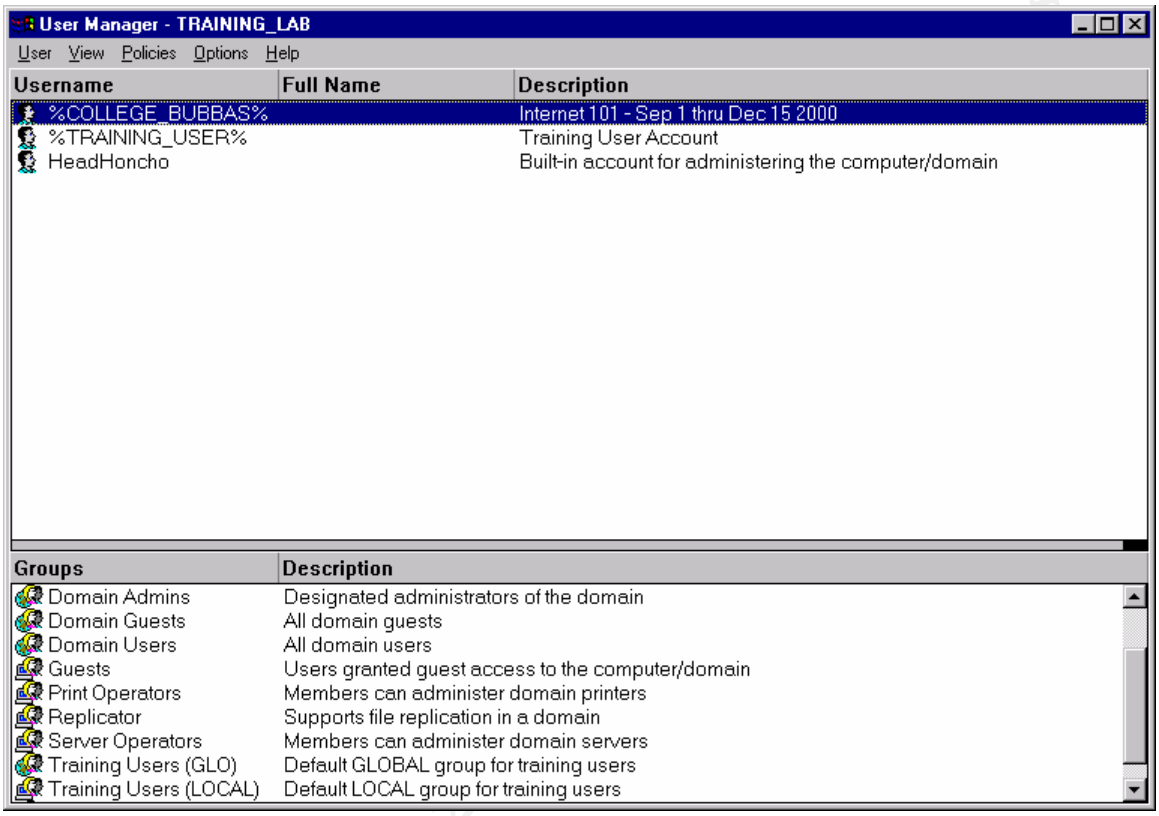
Click on the "Hours" tab. Since we know the days and times that this course will be taught, restrict the hours of access to only those hours when class is in session (for example, Monday and Wednesday from 6-9 PM):



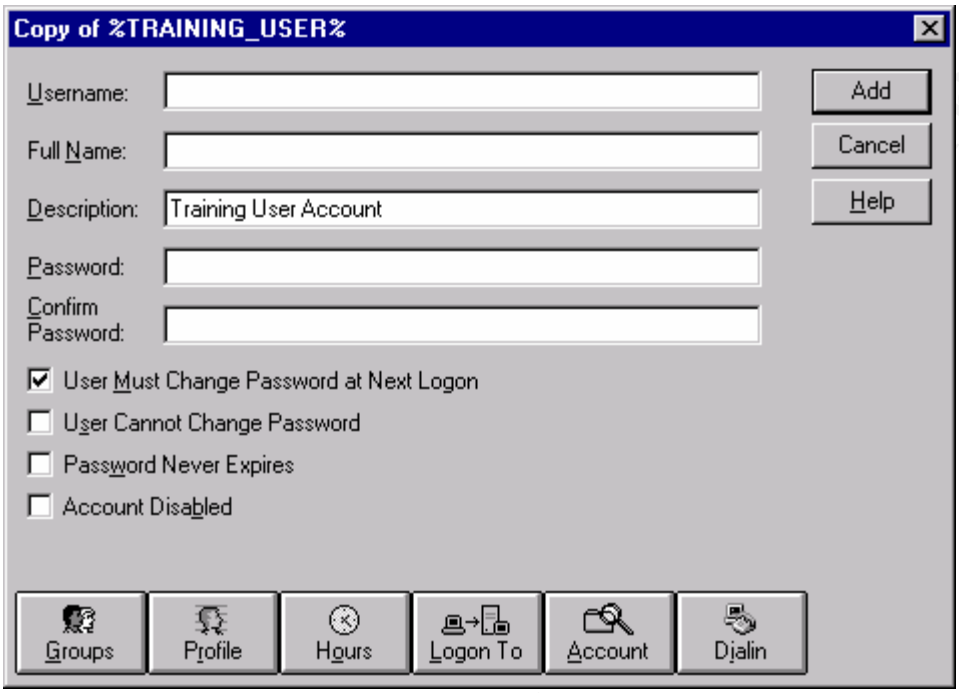
Since college accounts are set up on a per course basis and we know the date when the class will end, click on the "Account" tab and set the account to expire at the end of the course (in this case 12/15/00). Once the course is over, the accounts will be deleted; however, setting the accounts to automatically expire simply adds an extra measure of security until the administrator has the opportunity to delete them.



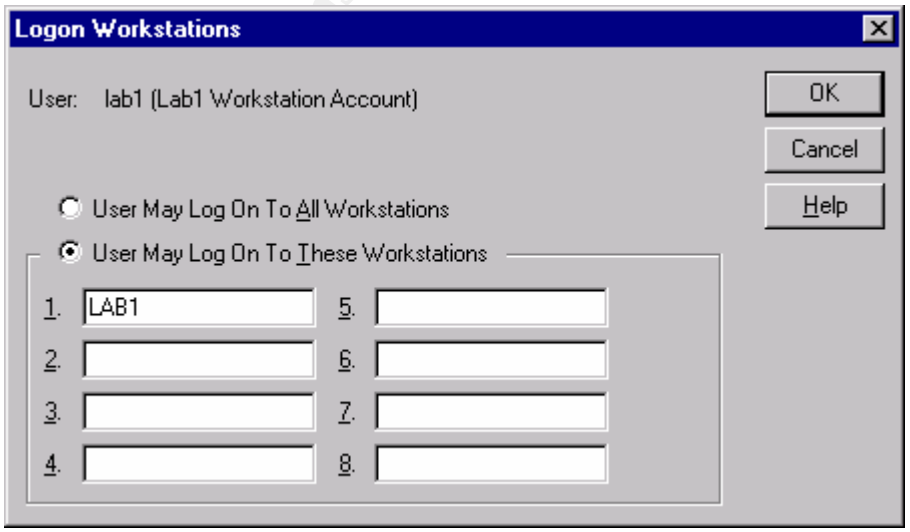
Now that the basic templates have been created, we are ready to create the individual user accounts. Notice from the screen shot below that account templates are displayed at the top of the User Manager window, making it easy to locate them for use in actual account creation.



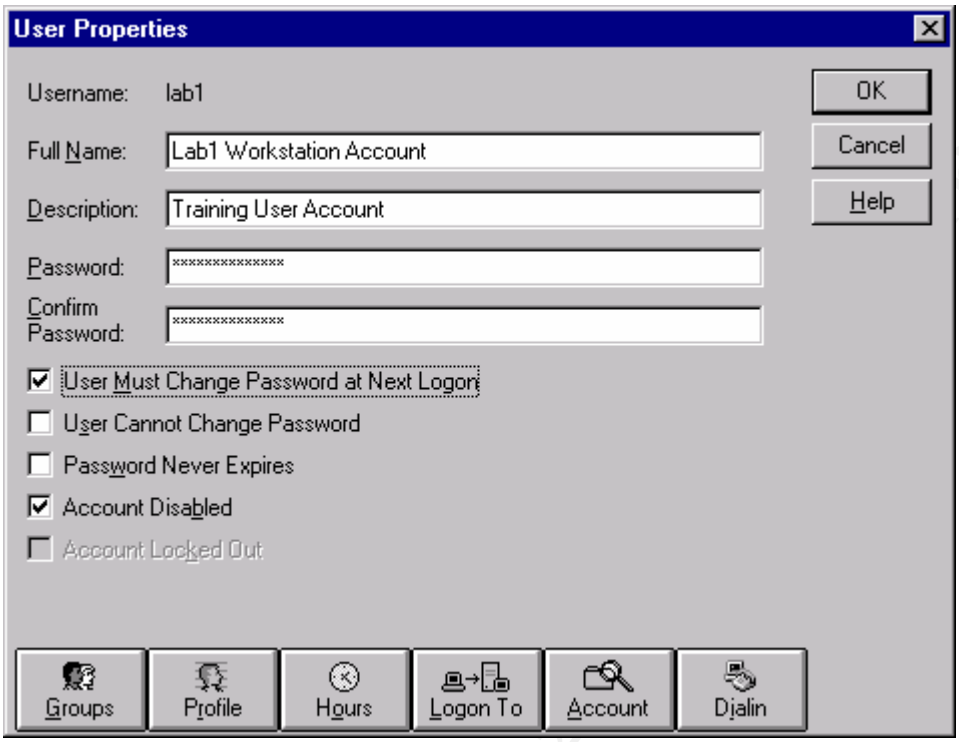
Create User Accounts. From User Manager, highlight the appropriate template account (i.e. %TRAINING_USER%), click User, Copy. A copy of the template account will be made and displayed, ready for input.



Notice that the "Description" field is filled in, and "User Must Change Password at Next Logon" is checked. Upon clicking the "Groups" and "Hours" tabs, you will notice that the parameters set up in the template are already in place. Type in a username, a descriptive full name, and a default password. Disable the account. Click the "Logon To" tab to restrict account logon to the workstation which shares the same name as the user account:



This assures that the lab1 account is only able to logon to the LAB1 workstation in the lab, and no place else. Click OK.



The first account is now created. Follow this procedure for the other 14 user accounts to be created for the lab. Follow the same procedure for college courses that need to be created, assigning account names that may be associated with the workstation names (i.e. CollegeBubba1 account for LAB1 workstation, CollegeBubba2 for LAB2, etc.). In the college student accounts, the student's name may be entered into the description field, once students have been assigned accounts and workstations.

It is also a good idea to create separate accounts for course instructors and for the training coordinator. These accounts should be included in the "Training Users" group; therefore, the appropriate template may be used to create them. The only difference between these and the regular training accounts will be that these two accounts will be allowed to log on to any workstation in the training lab. In addition, you may find in time that the training coordinator is trustworthy and capable of assisting in account management duties, such as enabling/disabling accounts, setting up new accounts for college courses, changing passwords, etc. If that is the case, you may put him in the built-in "Account Operators" group so that he may perform some of these duties. Although you still must monitor his activity closely, this will relieve you of some of the day-to-day "busy work" associated with account management.

Part Three
Securing the Workstation Environment

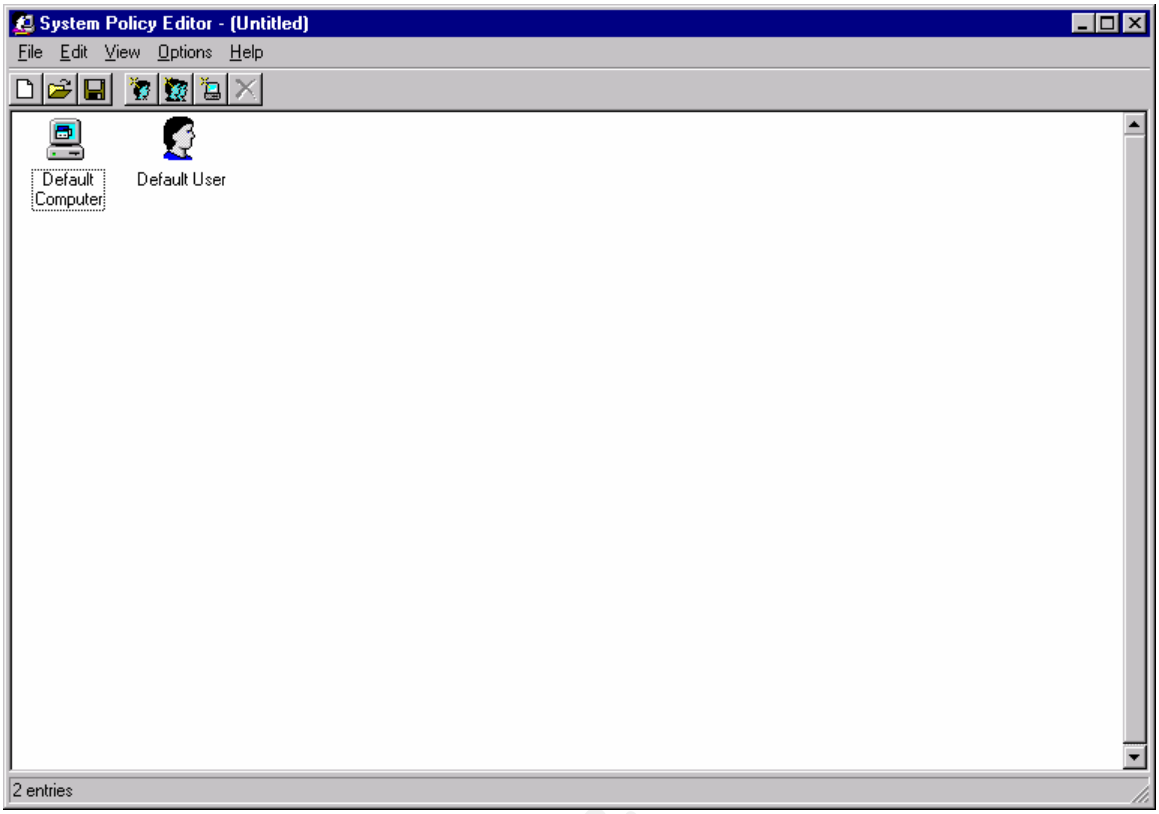
One of the biggest challenges faced by administrators, PC technicians, and training coordinators in a training environment is that of securing the workstations in the lab and preventing potentially harmful changes to them. Users cannot resist changing wallpaper, modifying system settings, and even loading their own personal software onto the machine during class. This can cause an administrative and technical nightmare if no method is adopted of guaranteeing that the system configuration remains stable from one training session to the next. Fortunately Microsoft provided the System Policy Editor, which allows administrators to control the configuration of the machine so that the users are not allowed to make any undesired changes. It also allows for policies to be set that will assist in various security matters and provide the administrator with a means of displaying required logon banners. Policies may be created for computers and users to control just what the user will be allowed to do at the workstation.

Computer policies apply to every computer they are applied to, no matter who logs on to that computer; they are applied at system startup (assuming the computer is connected to a network). Conversely, user and group policies apply to every user or group they are applied to, no matter where they log on in the domain; they are applied at domain logon. Computers on a domain will automatically look for an NTCONFIG.POL (NT Systems) or a CONFIG.POL (W9x Systems) in the NETLOGON share of the authenticating domain controller (these .POL files are automatically replicated to the NETLOGON shares of backup domain controllers as well). The NETLOGON share is located in the \%SystemRoot%\System32\Repl\Import\Scripts folder.[5]

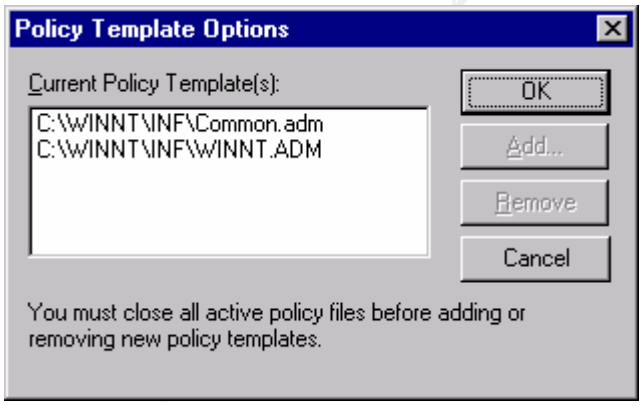
It is important to note that policies enforced across the domain are only enforced when the computer or user is actually logged into that domain. Unplugging the computer from the network prevents the policy file from being applied to the computer. For this reason, you should consider installing the System Policy Editor locally and enforcing the most important system policies directly on the workstations. However, for the controlled environment of the computer training lab, we will set up and enforce all policies from the domain controller.

To use the System Policy Editor, Click Start, Programs, Administrative Tools (Common), System Policy Editor. Once the window is displayed, click File, New Policy. A default computer and default user policy will be displayed, which may be modified and saved to implement whatever controls are desired.

[5] The SANS Institute, p. 208.



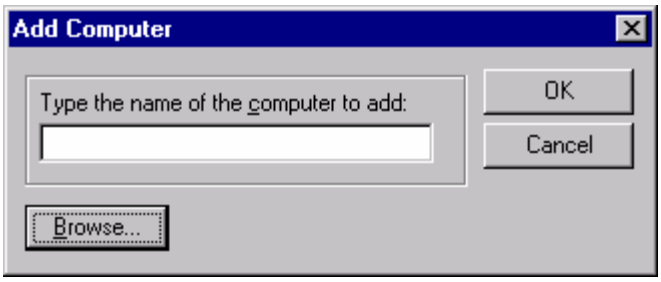
To use a particular template, click Options, Policy Template and choose the one (or ones) desired. The default templates in use are Common.adm and Winnt.adm. More than one template may be used at a time. In addition, templates may be edited using a standard editor, such as notepad, to add new registry values. More information on this process may be obtained from Microsoft.



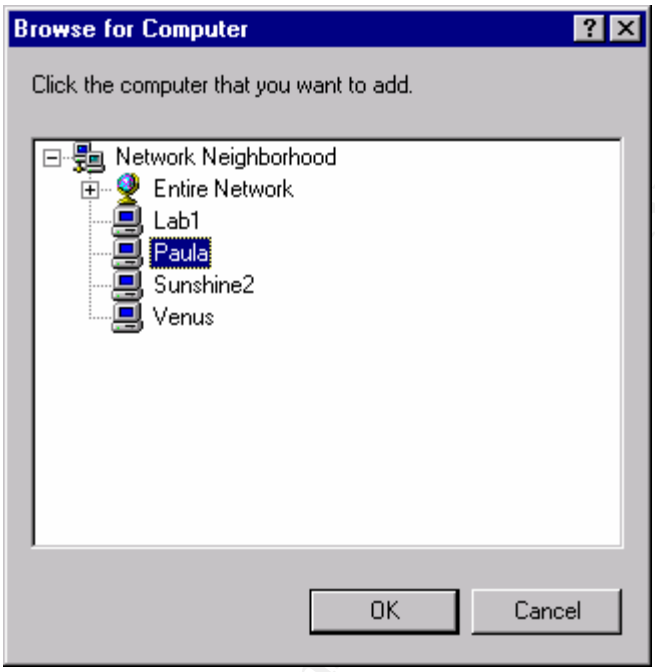
Many other templates are available from Microsoft, which are specifically tailored to various operating systems and applications. These are generally available on the Operating System CD-ROMS, Resource Kits, or are downloadable from Microsoft.

Before making any changes to the "Default Computer" and "Default User" policies, create a new computer policy for the NT Server/domain controller (and any other

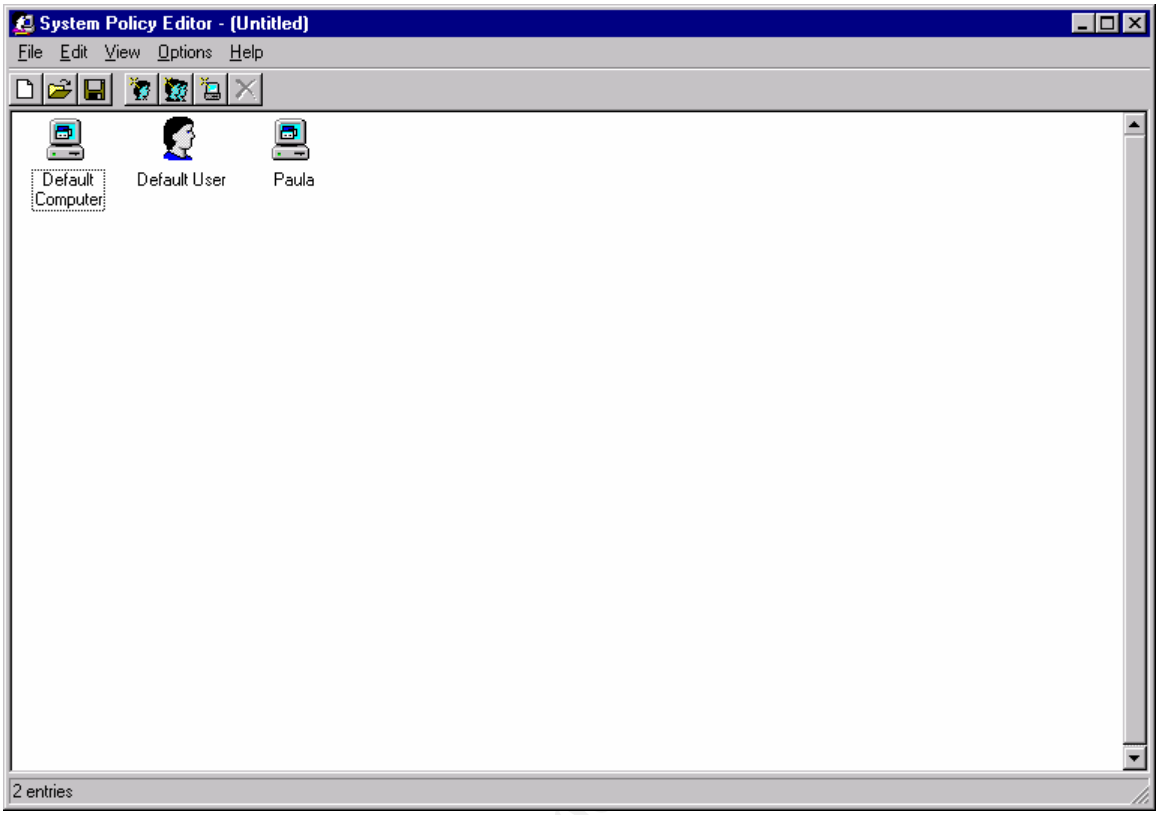
machines you may wish to exclude from the default policy). Click Edit, Add Computer (or click on the "Add Computer" icon on the toolbar):



Type in the name of the computer you wish to add, or click Browse:



Select the appropriate computer and click OK. The computer will now be displayed in the System Policy Editor window. The computer you just added will be controlled by its own individual policy and therefore exempt from any policy changes that are made to the "Default Computer" policy. The same may be done for users you wish to exempt from the "Default User" policy.



Double click the "Default Computer" icon. The configurable policies will be displayed. There are many different policy options that may be configured; however, we will configure a few that would be relevant to protecting machines in a training lab.

Upon opening the "Default User" and "Default Computer" policies, notice that each property has three settings:

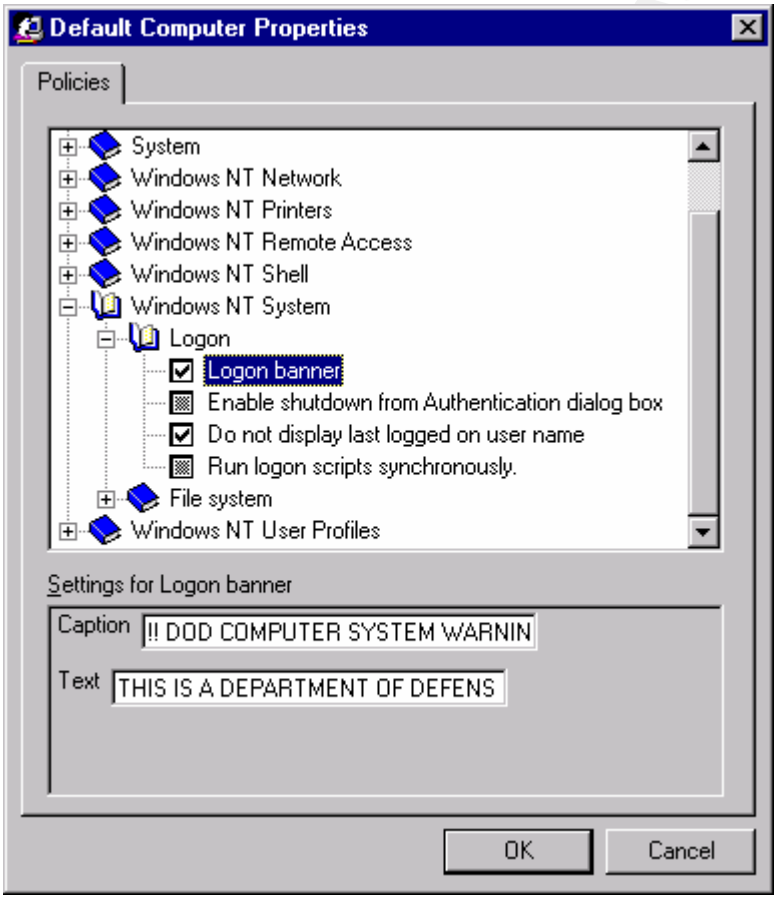
1. Grayed out: will default to whatever property setting is on the workstation
2. White: will clear whichever property setting is on the workstation. Even if the workstation has a restriction set as a default, this choice will clear it (remove the restriction).
3. Check marked: will set the property active regardless of how it is set on the workstation (add the restriction).[6]

The first policy we will set will be that of a logon banner. As mentioned earlier, these fifteen workstations reside on a military base and are connected to a military network. Any computer that is owned by the Department of Defense and/or resides on a DoD network requires that a standard warning be displayed and acknowledged each time that computer is logged on. The warning is as follows:

[6] Redick, Stacey, "System Policy Editor Tutorial," http://www.elkantler.net/security, April 1998.

"This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including internet access), are provided only for authorized U. S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or other adverse action. Use of this system constitutes consent to monitoring for these purposes. Unauthorized use could result in criminal prosecution."[7]

Double click the "Default Computer" icon in the policy editor. Navigate to "Windows NT System," "Logon" and click the plus sign. The following options will be displayed:



[7] Courtesy of an actual government computer logon banner.

The screenshot above displays the "Logon" options that may be set for the set of computers desired. Check "Do Not Display Last Logged On User Name" to force the username field to be blank at logon. To institute the DoD Warning Banner, check the "logon banner" box. Notice the "Caption" and "Text" fields that are available to be filled in at the bottom of the window. Type the appropriate text into the caption and text fields, and click OK. Until recently the System Policy Editor did not allow a Logon Banner text field of greater than 1024 characters; the DoD Warning Banner is slightly longer. Service Pack 6a allows the administrator to create a logon banner of up to 2048 characters.[8] However, a change to the winnt.adm file is required. Use a text editor to make the following change:

From:

```
CATEGORY !!Login_Policies
  POLICY !!LogonBanner
  KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Winlogon"

    PART !!LogonBanner_Text          EDITTEXT
    VALUENAME "LegalNoticeText"
    MAXLEN 1024
    DEFAULT !!LogonBanner_DefText
    END PART
```

To:

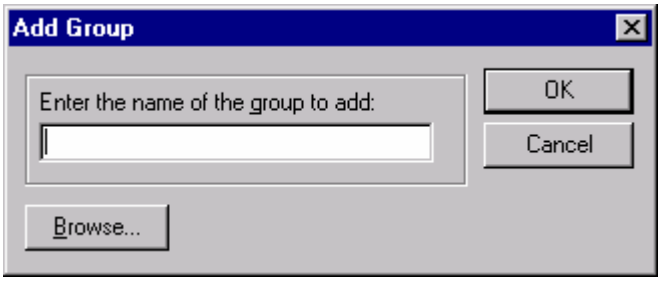
```
CATEGORY !!Login_Policies
  POLICY !!LogonBanner
  KEYNAME "Software\Microsoft\Windows NT\CurrentVersion\Winlogon"

    PART !!LogonBanner_Text          EDITTEXT
    VALUENAME "LegalNoticeText"
    MAXLEN 2048
    DEFAULT !!LogonBanner_DefText
    END PART
```

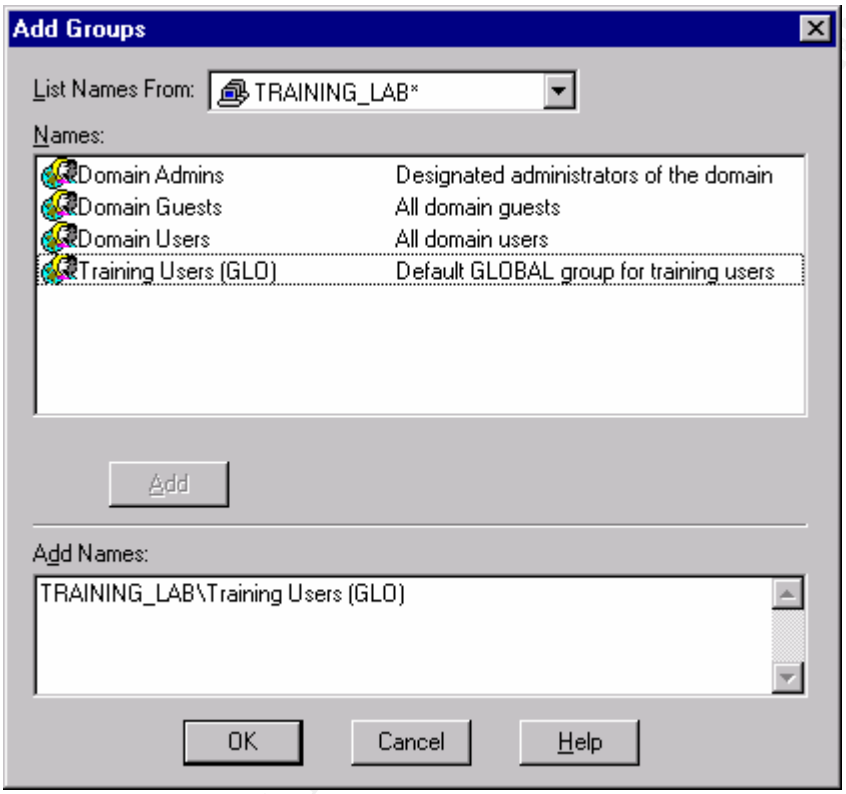
Once this change is made to the winnt.adm file, the logon banner may be up to 2048 characters long.

We will now create a group policy to control the users in the "Training Users" global group. Click Edit, Add Group (or click the "Add Group" icon on the toolbar). The following screen will be displayed:

[8] "System Policy Editor Will Not Allow More Than 255 Characters," Microsoft Knowledge Base Article ID: Q173385.

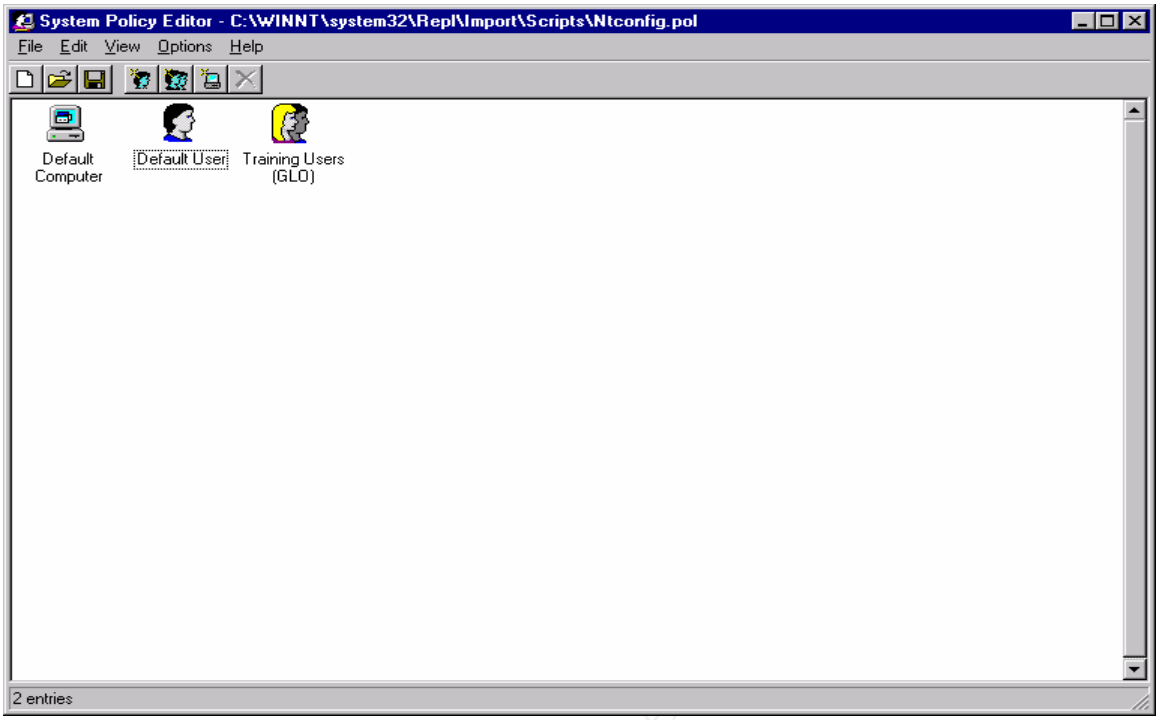


Click Browse. Click "Training Users (GLO)" and click ADD.

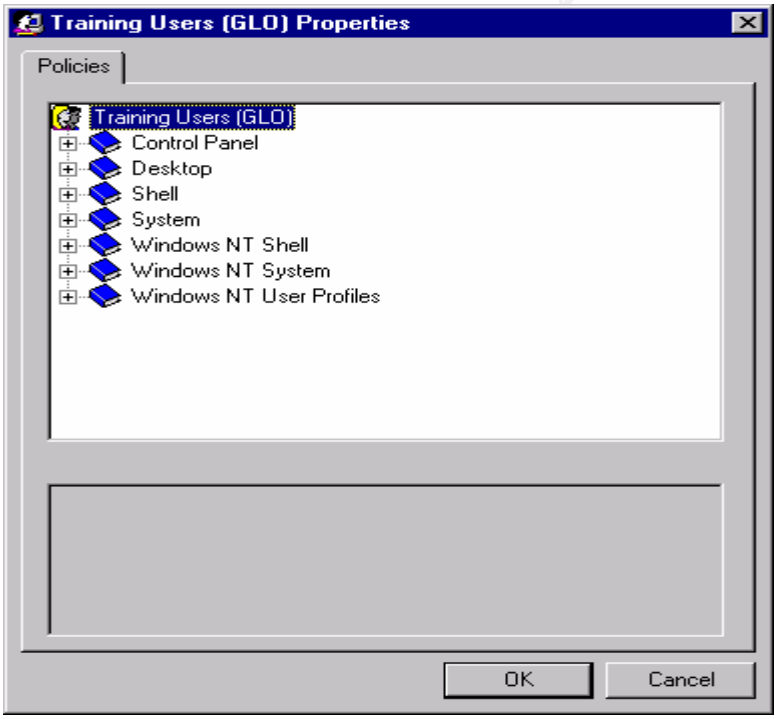


Click OK. The policy editor screen will now display a new group called "Training Users (GLO)". Note that in order to make the best use of the System Policy Editor, it is a good idea to create groups for the different types of users, depending upon the restrictions you wish to set. For example, you may also create an "Administrators" group for use by administrators, with no policy restrictions.

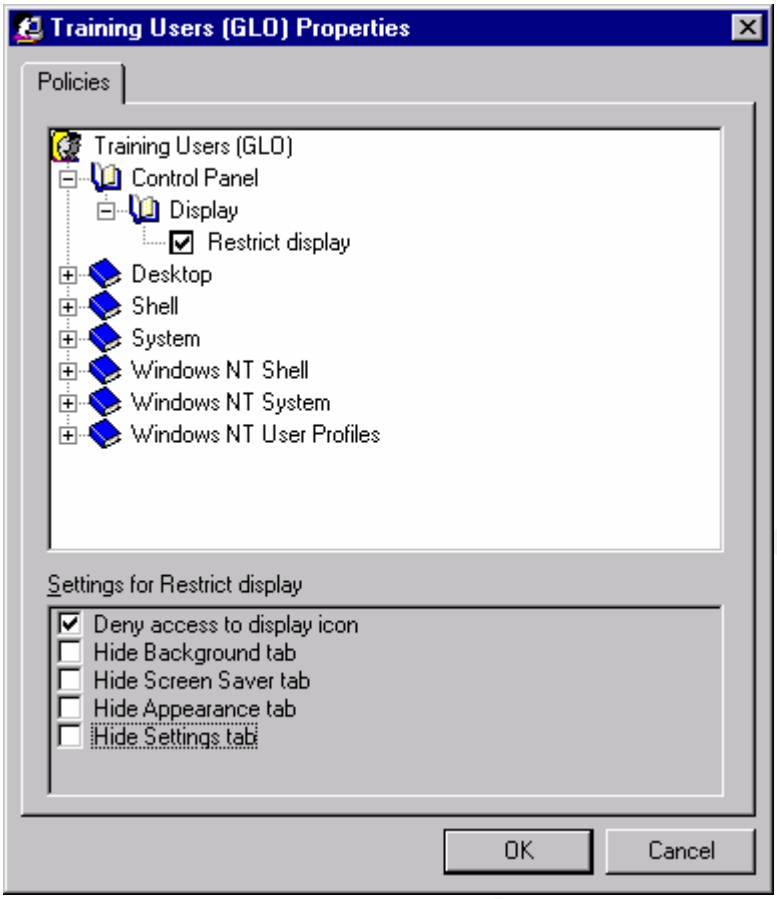
There is also a feature in the System Policy Editor for enforcing the priority of policy application to the users. This is necessary when the user belongs to more than one group and different groups contain conflicting policies. These priorities may be set by clicking on Options, Priorities and setting the priorities in the order desired.



Double click the "Training Users (GLO)" icon to begin modifying the training users group. The following screen will be displayed:



Let us assume we want to restrict the Control Panel display in the user policy. Click Control Panel, Display, Restrict Display. The following screen will be displayed:



Check the "Restrict Display" box and notice that there are several options for restricting various control panel displays. If "Deny Access to Display Icon" is checked, the user will not be able to access the display icon at all. If you desire to restrict certain portions of the display in the control panel, check the ones you wish to turn off. In this case, the control panel display will still be available, but the tabs you have hidden will not be displayed.

There are many attributes that may be set using the common.adm and winnt.adm templates. In the case of the training lab, some settings are related to security and others are related to maintaining the state of the workstation. Recommended security settings include:

- Hide Network Neighborhood
- No Entire Network in Network Neighborhood
- Remove the "Map Network Drive" and "Disconnect Network Drive" options
- Remove Find Command from Start Menu
- Disable Registry Editing Tools
- Run Only Allowed Windows Applications. Make sure that if this policy is put into place, the appropriate list of allowed applications is added.

Other settings that aid in security as well as maintaining the state of the machine include:

- Remove Run Command from Start Menu
- Restrict Display (Control Panel)
- Don't Save Settings at Exit

To save the System Policy File, click File, Save. As discussed before, the policy must be saved as NTCONFIG.POL (for NT systems) or CONFIG.POL (for W9x systems), and it must be placed in the \%SystemRoot%\System32\Repl\Import|\Scripts folder. Whenever a computer on the domain starts, or a user logs on to the domain, the user's computer will search the NETLOGON share of the user's authenticating domain controller for the current policy, and will put that policy into effect for that user or computer.

There are many other restrictions that may be set using different templates or by editing the templates to add other registry settings to control. Keep in mind, however, that policies set forth for a group of users may have to be adjusted, depending on the changing needs of that group. In some cases, new groups may need to be established. For example, let's assume that a course in Windows NT is being offered. In this case, many of the restrictions put on regular training users are too prohibitive for users who are learning how to use Windows NT, because so many of the features have been taken away. In this case, it would be prudent to create a new group policy ("NT Training Users") with the appropriate restrictions. This policy would have to be applied to the group of users it is intended to control.

Although there are many restrictions that may be put into place using the System Policy Editor, there is no guarantee that nothing will go wrong with the workstation. In a dynamic heterogeneous environment such as a training lab, it is a good idea to use an enterprise PC management tool, such as Symantec Ghost, to create backup image files of the workstations. Systems can quickly be recovered, restored, or rebuilt using a product such as Ghost. In addition, systems may be "cloned" so that they are all identical.

Conclusion: When planning and implementing a training lab, there are a huge number of unique issues that must be considered in order to assure an effective but secure training environment. This document has attempted to address several of the key issues in establishing this type of environment; however, it is impossible to fully explore each one without creating a much more detailed and comprehensive document than was presented here. Hopefully this document can be viewed as a general "road map" for starting to explore all of the necessary details in setting up an environment for "special users."

References:

Hadfield, Lee; Hatter, Dave; Bixler, Dave. Windows NT Server 4 Security Handbook. Indianapolis, IN: The Que Corporation, 1997.

"How to Enable Strong Password Functionality in Windows NT." Microsoft Knowledge Base Article ID: Q161990.

Kapp, Justin. "Securing Windows NT." PC Network Advisor, Issue 115 (February 2000), pp 11-18.

Microsoft Technet. "Enforce Strong Passwords in NT 4.0." Windows Tips and Secrets. Platinum Technology, Inc., 1998.

Miller, Stuart S. Windows NT Security Guide. Wodburn, MA: Butterworth-Heinemen, 1998.

Redick, Stacey. "System Policy Editor Tutorial." http://www.elkantler.net/security. April 1998.

The SANS Institute. Windows NT Security Step-by-Step. SANS Network Security 2000.

"System Policy Editor Will Not Allow More Than 255 Characters." Microsoft Knowledge Base Article ID: Q173385.

Last Updated: October 23rd, 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**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
Southern California- Anaheim 2018 - SEC505: Securing Windows and PowerShell Automation	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**vLive**
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**