# Global Information Assurance Certification Paper

# Quick guide to securing your NT Servers

**Student: Ryan King**

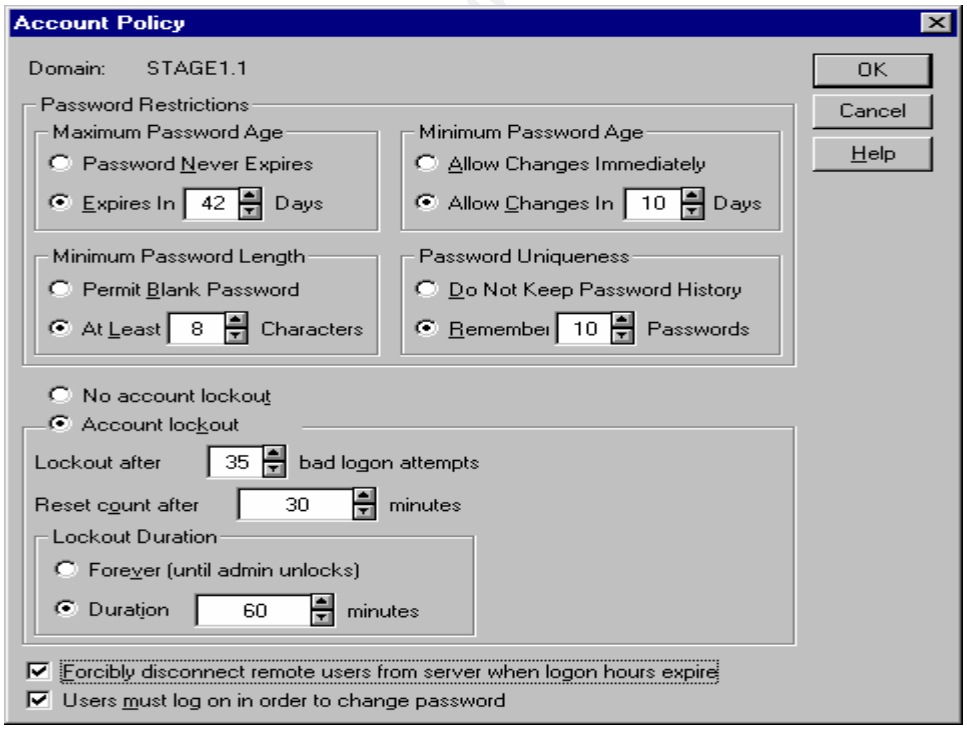
**Date: June 14, 2000**

This guide will show you some easy, but yet crucial changes that can be made to your NT Servers to improve the security.

**What three things do you need to gain access to your network?**

Connection point (be it network or physical)
User name
Password

On that note let's start with some basics like making sure the guest accounts have been disabled on all servers and workstations. Follow this by changing the default local Administrator account user name as the NT default is a prime target for hackers.
configuring your account policies the in User Manager for Domains is crucial to your company data. One recommendation for these settings is as follows:



Another area to think about is your user naming scheme. From my experience, FirstInitial/Lastname is very common in the industry. Depending on how much security you need to have you can determine whether to use some form of the user's name or whether you come up with an assigned random scheme. This would make finding a username more difficult, but could increase the administrative task of creating users. Remember you have to balance security with usability. If you make the user name or even the password policies too difficult, users will tend to post the information so that they can remember it. Some other recommended areas for consideration when tightening down your NT Servers are covered in the rest of this guide.

## User Passwords

In addition to your password policies currently in place, add the Passfilt utility to enforce even stronger passwords. Passfilt filters each password looking for 3 of the 4 following criteria:

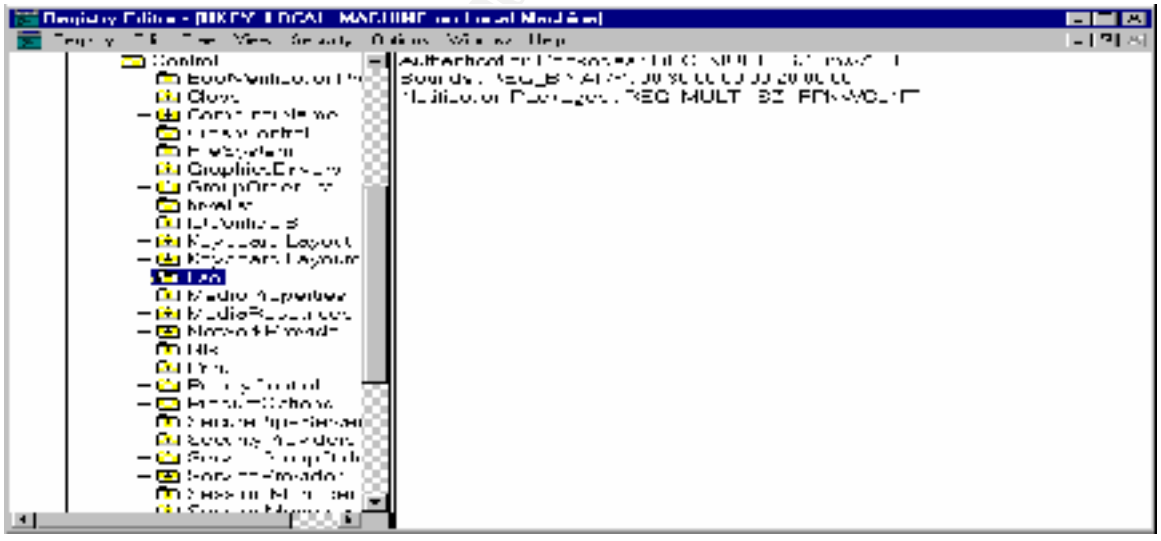
- Uppercase letters
- Lowercase letters
- Numbers
- Non-alphanumeric characters (!,#,/,etc.)

These must be at least 6 characters long. (This setting reflects the configuration in the account policy for minimum length, but defaults to 6).
Implement this filter as follows:

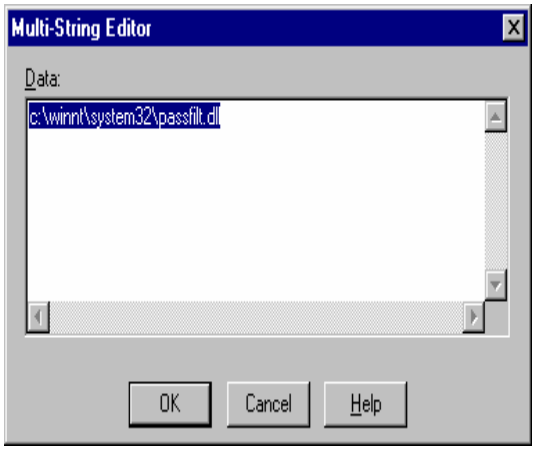
First locate the passfilt.dll on the local system.
Execute regedt32

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

If there is already an entry for “Notification Packages”, open that value and change it to: **%systemdrive%\%systemroot%\system32\passfilt.dll.**



If there is not an entry, then add a new value called “Notification Packages” and choose “REG_MULTI_SZ” for the data type and click OK.
In the text box type: **%systemdrive%\%systemroot%\system32\passfilt.dll.**




Exit and reboot your server

*Note: This will not take effect until the user actually changes his/her password*.



**Protecting your SAM Database**

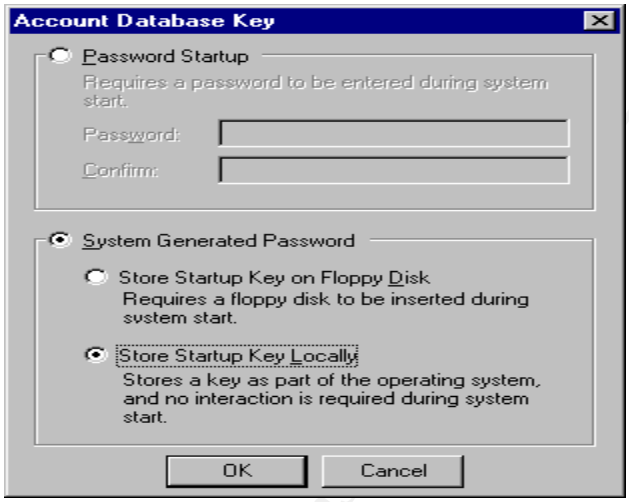
To prevent someone from using a cracking utility such as L0phtcrack to hash out your critical passwords, you should encrypt your SAM database. This adds another level of security to your system should someone gain access to your servers.

To activate Encryption on your SAM database:

Execute Syskey on your Domain Controller


Choose Encryption Enabled.

You will receive a message stating that if you activate encryption you cannot deactivate it. Click OK to confirm.




You will be given three different ways to store your encryption keys.

**Password Startup** will require you to type in the password on startup, but the security is left in the password itself and who has that password.

**Floppy Disk** will require the disk be inserted upon every startup. The security is left to physical access to that disk. Keep in mind that floppy drives can go bad, thus adding additional time to the restart of production servers.

**Key Locally** does not require any intervention by a user. Then key and the SAM are located on the same system without a password.

Given the pros and cons in conjunction with your security policies, choose the appropriate option. You can change these options later, but you cannot turn them off.

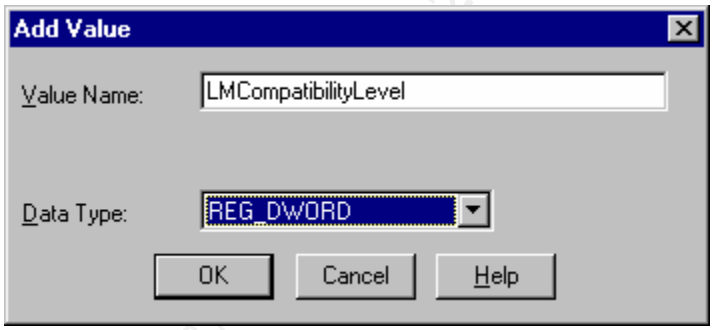
*Note: For auditing purposes, you may not want to enable encryption on one of your BDC servers to allow the system administrator to periodically audit passwords being used.*

## Protecting Against password sniffing

If you operate within a complete Windows NT environment, then you have the ability to require encryption on password passing between server and workstation. To force your systems to use the NTLMv2 protocol you need to make a registry change.

Using regedt32
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

Click on edit, “add Value”

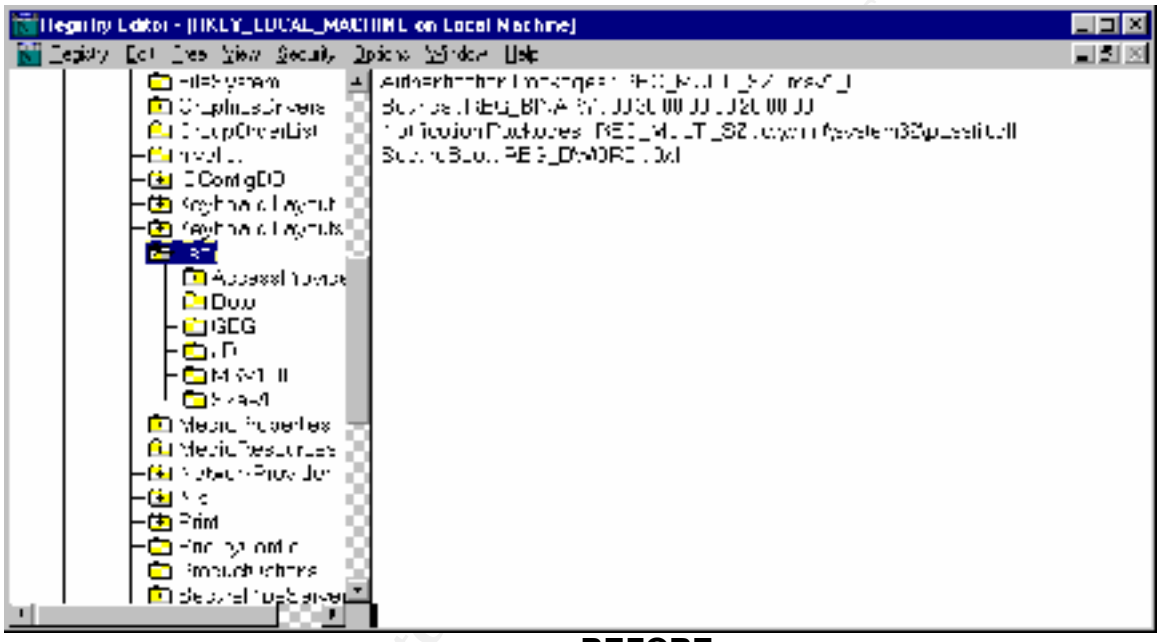



The values name is ‘LMCompatibilityLevel’ using the REG_DWORD value type. At this point you have 5 options to choose from (1-5), (0 is the default if you don’t add this value). 1-3 are for use on client workstations while 4-5 are for domain controllers.

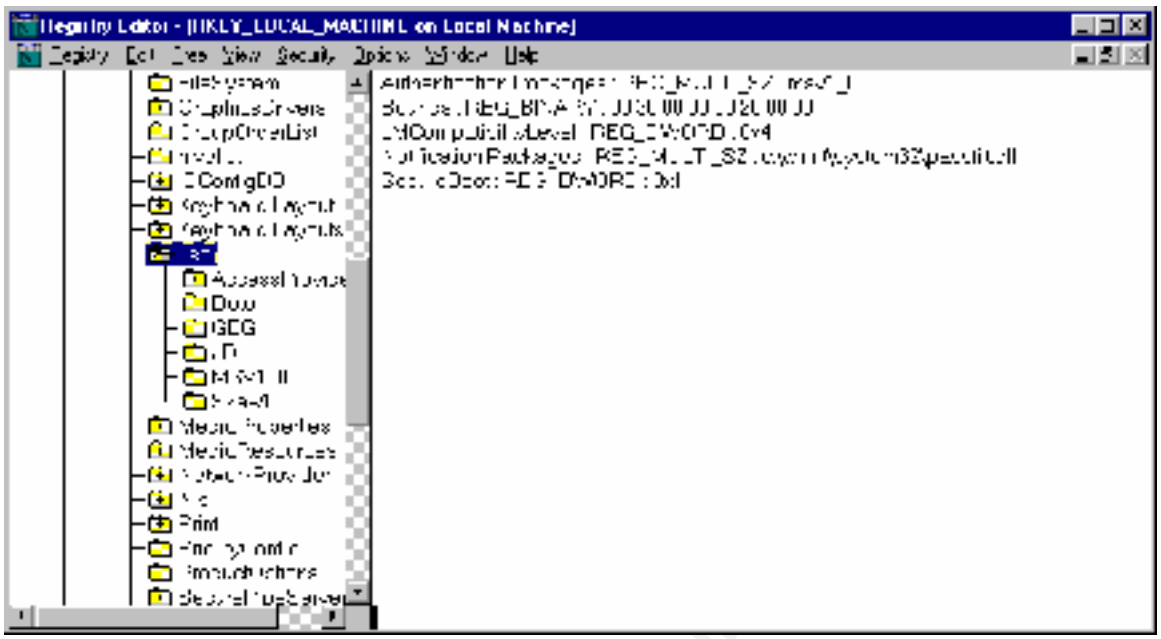
0- Send both LM and NT (MD4) authentication across the wire.
1- Clients will negotiate the best protocol to use starting with NTLMv2.
2- Clients will only use NT (MD4) authentication.
3- Clients will only use NTLMv2 authentication.
4- Domain controllers will only accept NT (MD4) or NTLMv2 authentication.

5- Domain controllers will only accept NTLMv2 authentication.

If you still have Windows 9x clients, then adding this value and using the “1” value will at least protect the NT systems to reduce your potential weak points. If your environment is all NT then you can set the clients at “3” and the Domain Controller(s) at “5” for ideal protection. This can also help ward off unauthorized machines for connecting to your network.




**BEFORE**



**AFTER**

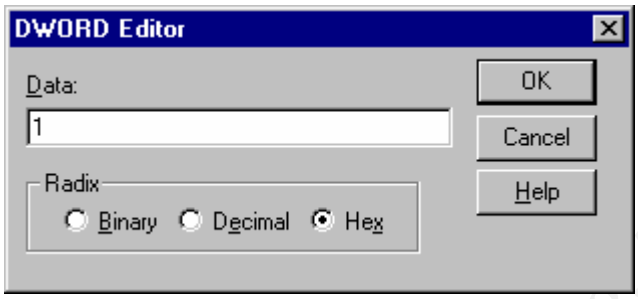
# Protecting against unwanted guests

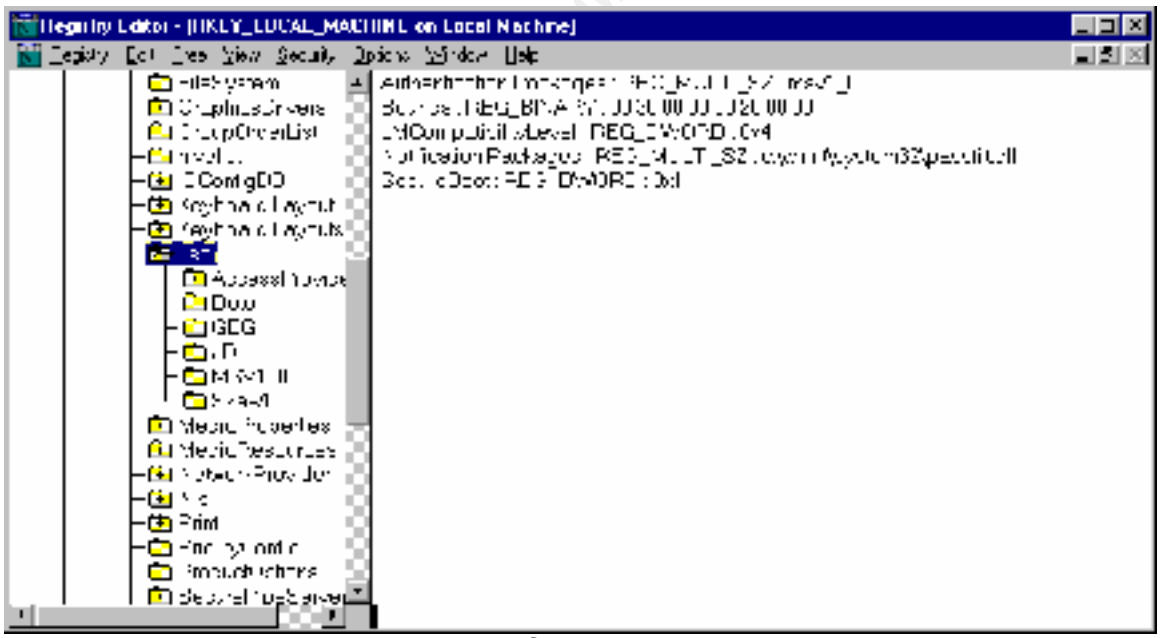
How to close off null users. A null user session is the ability to make a connection to a resource without a validated username and password. A null user session uses a Microsoft created hole to access the system when an authenticated username and password is not available. A null session consists of no username nor password, making connection easy, but security extremely difficult. There are a couple of areas that can be locked down for null sessions.

Shut down share names, user name and group listings
Restrict allowed null sessions.

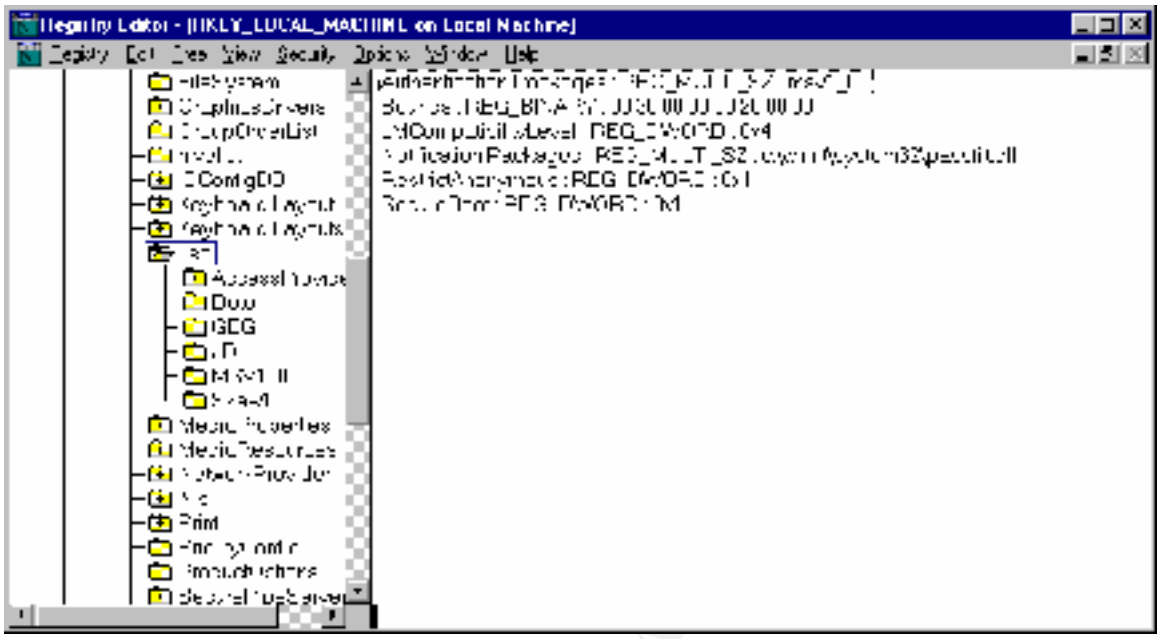
To shutdown share name listing
Use the RestrictAnonymous setting in your registry
Using regedt32
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA

Add the value RestrictAnonymous with the value type “REG_DWORD” and the Data Value set to 1.

**Before**



**After**

Other topics not covered in this guide are Securing external access to your network systems. Preparing your users for "Social Engineering" attacks. These can all be researched at:

www.sans.org
www.win2000.com
www.microsoft.com