Global Information Assurance Certification Paper

Securing Windows NT

by

Andrew Kjell Nielsen

Table of Contents

- PIII/667
- 128MB Ram
- 9GB U2W SCSI Drive
- ATAPI DVD/CD-ROM 16X/40X
- Bay Networks NETGEAR FA310TX F/E Adapter

9GB Disk split in two partitions:

- C: 4001 MB
- D: 4738 MB

Systemroot = C:\winnt

System was installed as a PDC.

Machine Name = DREWPDC
Domain Name = DREWNET

Installed Components

- Accessibility Options (ALL)
- Accessories (ALL)
- Games (ALL)
- Multimedia (ALL)
- Windows Messaging (NOT INSTALLED)

Network Components

- IIS (NOT INSTALLED)
- Bay Networks NETGEAR FA310TX F/E Adapter

Network Protocols

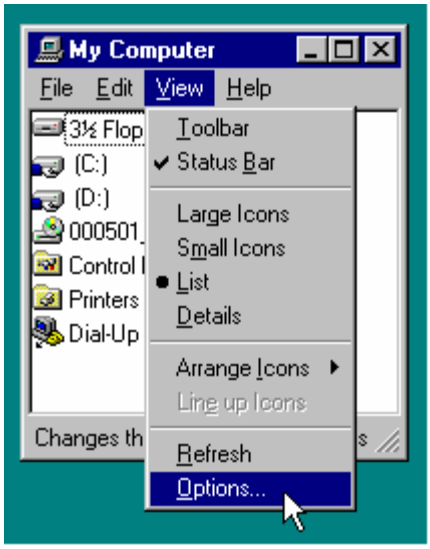
- TCP/IP

Services Installed

- RPC Configuration
- NetBios Interface
- Workstation Service
- Server Service

After NT Server was installed with Service Pack 1
I also installed the following applications:

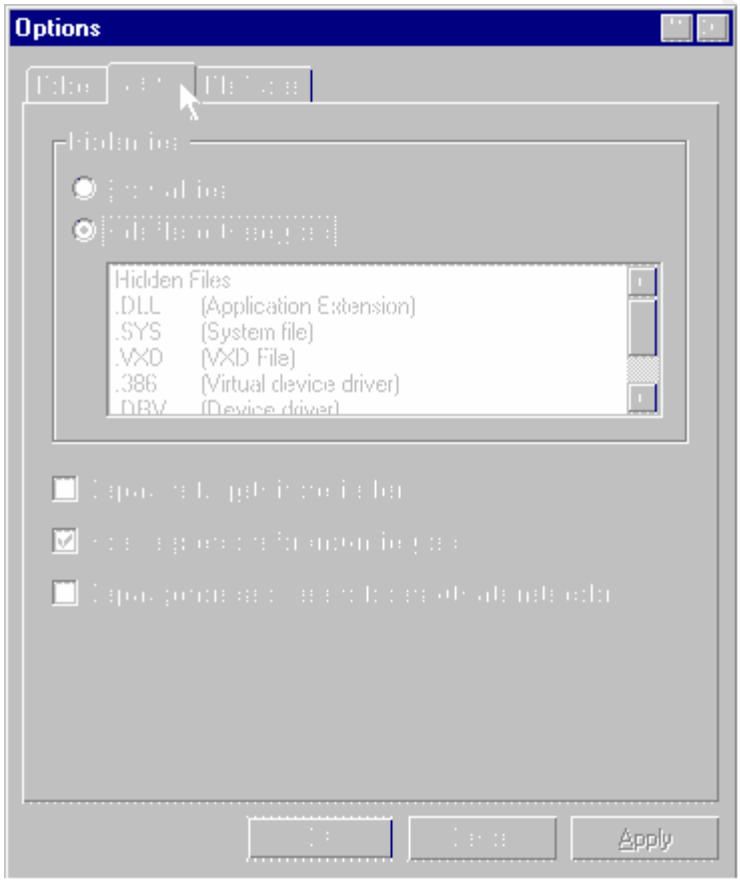
- Winzip 8.0
- Snag-It 5.0
- Windows NT 4.0 Resource Kit Supplement 4



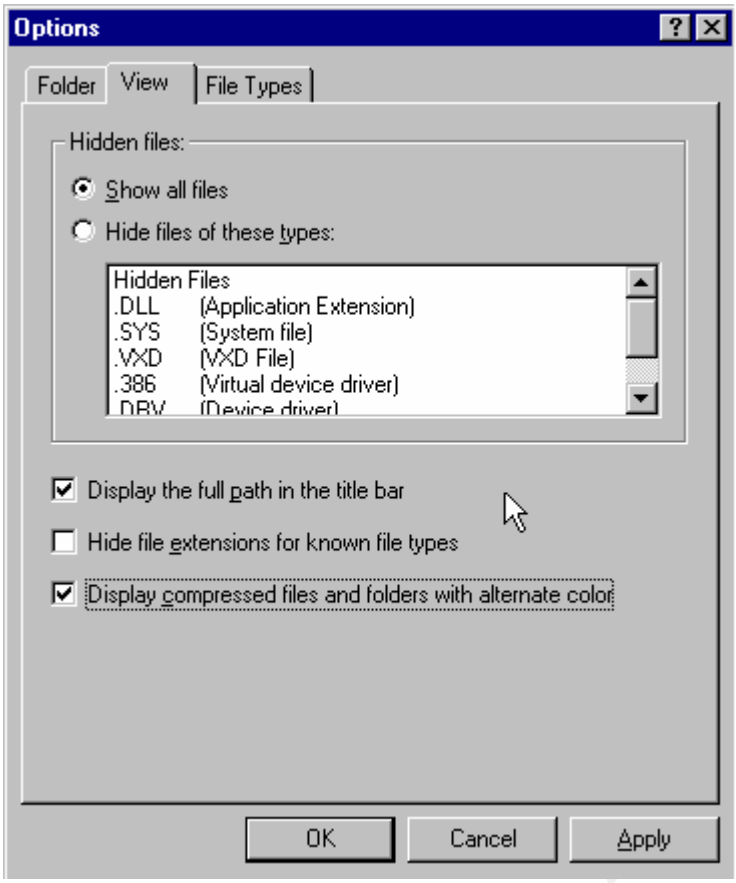
The initial viewing options in NT hides the following files: .dll, .sys, .vxd, .386, .drv, and .pnf files. These initial options also hide extensions for know file types, such as .bat, .txt, .htm, .rtf, .doc, .exe, etc. This represents a security risk since an attacker can hide rogue code under a known file extension.

From the My Computer window choose View → Options.

Once the Options Menu is open select the View Tab.



This is the default configuration for the viewing options after installing NT from the Options → View Tab.



Change the default viewing options to:

1. Show All Files
2. Display Full Path In Title Bar
3. Display Compress Files and Folders with alternate color.

While the first two are mandatory changes, the display of compressed files in a different color is optional. I do it so that I can easily differentiate between compressed and uncompressed files.

A service pack is group of various patches and updates for Microsoft Windows NT. The service pack bundles various hotfixes and updates so that they can be applied all at once to a specific system, rather than one at a time.

Service Packs can be downloaded from http://www.microsoft.com/downloads. When downloading SP6A, which is the latest Service Pack available for Windows NT, you have the option of updating your existing Service Pack or downloading a compressed full version for deployment to multiple systems. I downloaded the full version so that I can script the install.

As with any new update for Windows NT, Service Packs should be tested on an independent system away from your production environment. This way if there are any issue with the SP they will be discovered in testing rather than running the risk of adversely affecting your test environment.

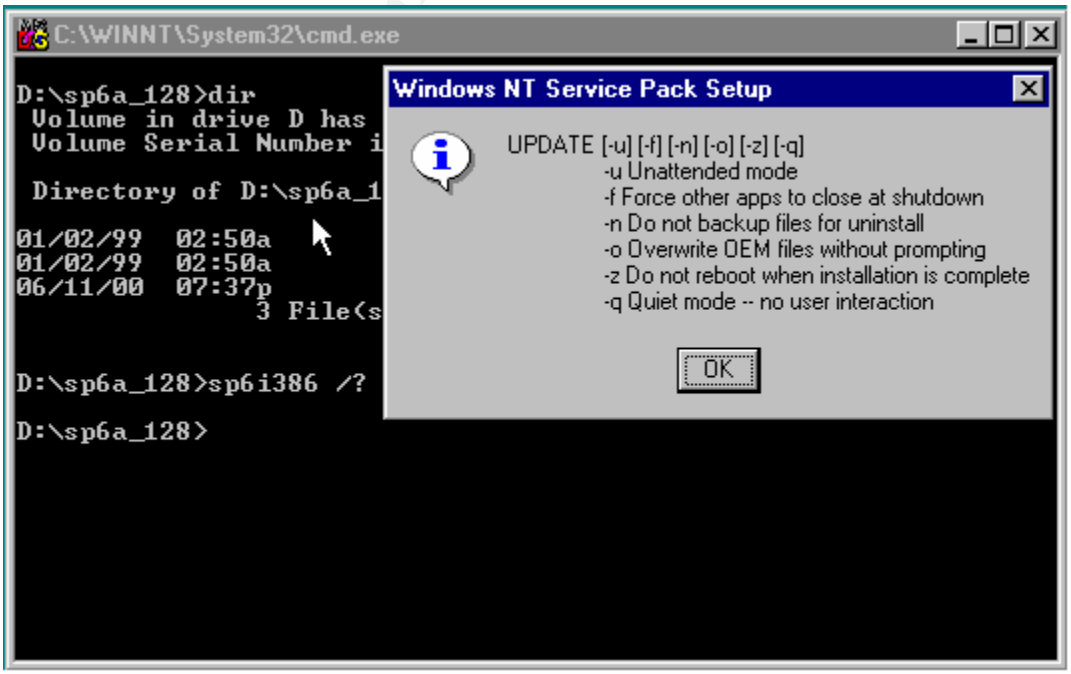
Installing the Service Pack

For this installation of Service Pack 6a I copied the SP (about 35 MB) to a directory on my D: drive called sp6a_128. From this directory I can write a script to install SP6a in various modes. You can launch the executable and do a standard install where you can choose to back up your old files (in case you need to roll back).

To view the modes for installing the Service Pack follow the steps listed below:

1. Open a command prompt from the RUN menu
2. Move to the directory where the service pack executable is located.
3. Once in that directory type the following:
   - (executable name) /?

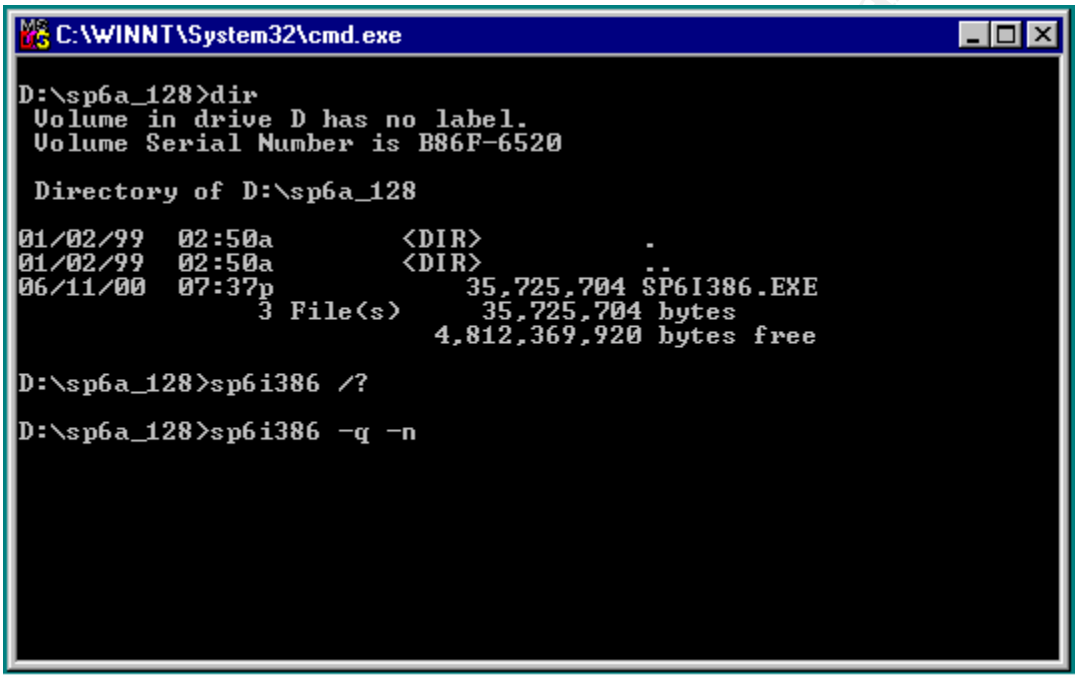
The service pack will expand in a temp directory and you will see the following:



After running the executable with the **"/?"** switch you have the following options of installing the service pack.

- -u Unattended mode
- -f Force other apps to close at shutdown
- -n Do backup files for uninstall
- -o Overwrite OEM files without prompting
- -z Do not reboot when installation is complete
- -q Quiet Mode – no user interaction

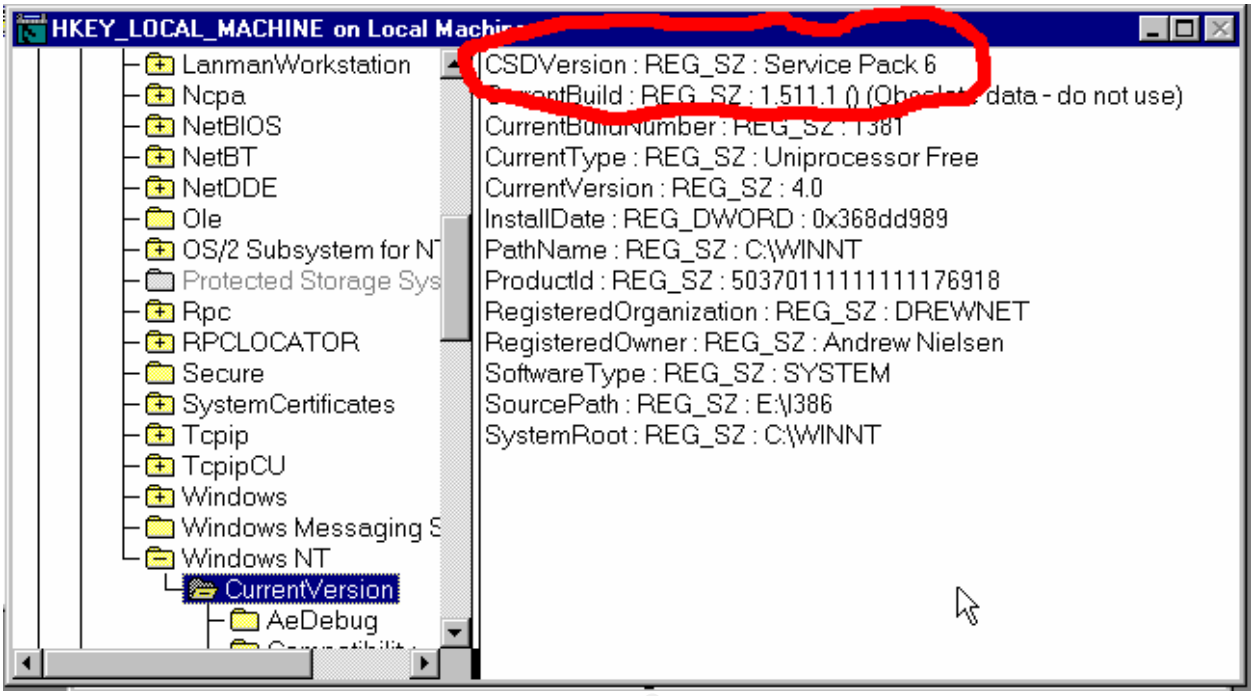
Using these various switches from the command prompt I will install the Service Pack in Quiet Mode (-q), without backing up the files for uninstall (-n).



After the machine reboots you can verify the Service Pack in the registry by using Regedt32 and going to the following registry value

HIVE	HKEY_LOCAL_MACHINE
KEY	\Software\Microsoft\Windows NT\CurrentVersion
Value Name	CSDVersion
Value Type	REG_SZ
Value Data	Service Pack X (X being the service pack version installed)

A view of the Registry for this value should look similar to the following graphic:



In this case you can see that Service Pack 6 has installed correctly. Remember that when you change the configuration of your server (the server configuration changes when a service pack or hotfix is applied), such as installing services from the original NT 4 CD, you will have to reapply the service pack and all subsequent hotfixes.

After installing the Service Pack successfully I like to install **IE 5.01**. I use the version from the March 2000 MSDN CD (Disc 20) which contains **IE 5.01** and two patches. The patches are the **schannel.dll** and **Server-Side Page Reference Redirect Vulnerability**. Since we already installed **Service Pack 6a** the **schannel.dll** has already been updated, but you will still have to install the **Server-Side Page Reference Redirect Vulnerability**. We can install that when we script and install numerous hot fixes later in the paper.

To date I have not been able to find the entire **IE 5.01 75MB executable** anywhere on Microsoft's website. When installing **NT Server** I keep **IE 5.01** on a cd. If you do not have access to **MSDN** you can install **IE 4.01** which can be found on the **Service Pack 4** distribution, or on **NT 4.0 Option Pack**. Once you have installed **IE 4.01** you can download a host of fixes as well as **IE 5.01** from Microsoft at http://windowsupdate.microsoft.com, http://www.microsoft.com/NTServer/all/downloads.asp, or http://www.microsoft.com/ie.

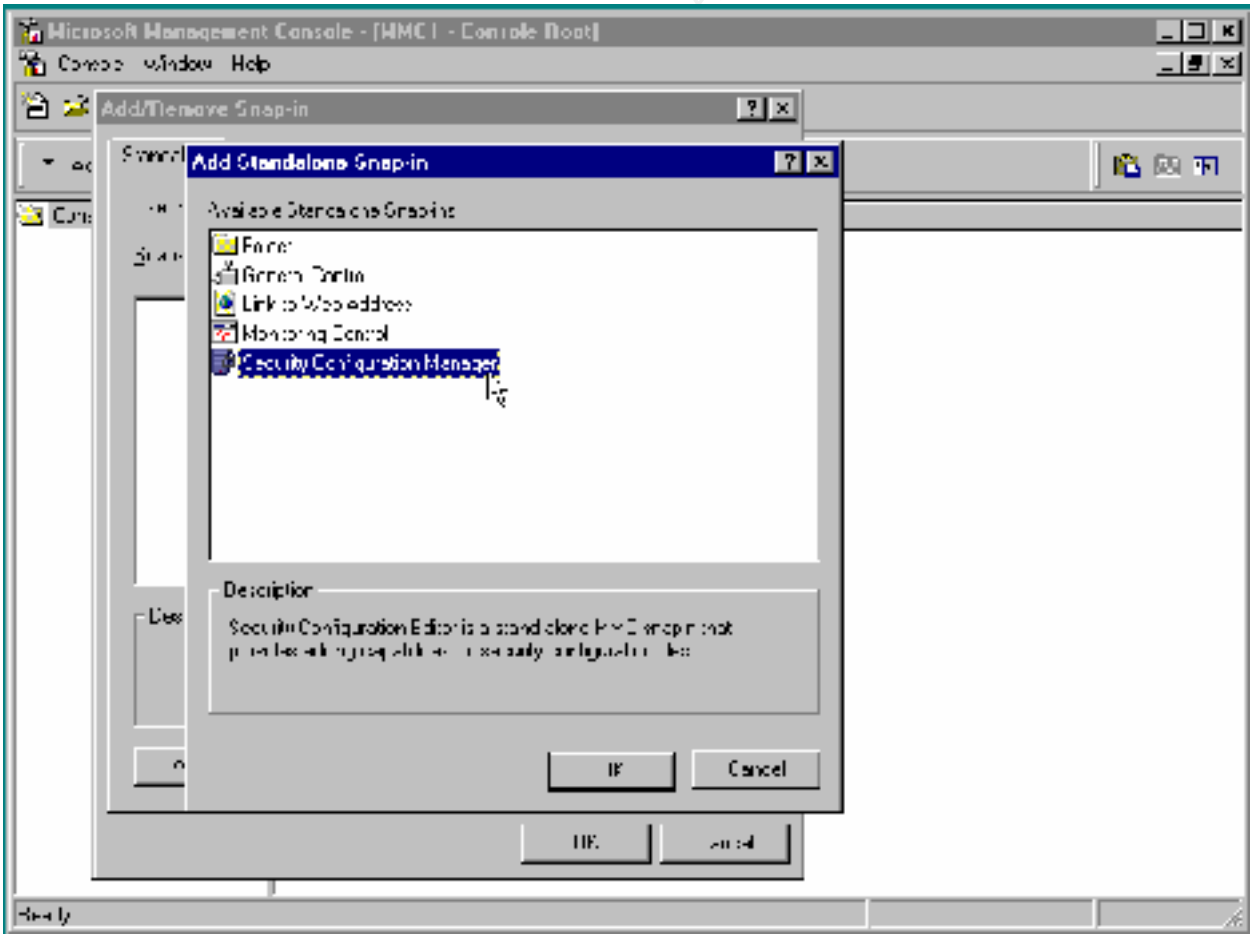
While this site lets you download the 56 bit encryption version, after you install the **IE 5.01** then go to http://www.microsoft.com/windows/ie/download/128bit/intro.htm to download the 128 bit **High Encryption Pack for IE 5.01**. Install the update and your done with **IE 5.01** for now.

The Microsoft Security Configuration Editor is a great tool from Microsoft to define security templates, compare current machine security settings against pre-canned or custom define templates, and configure current machine setting to match those templates. The MS SCE can be obtained from Service Pack 4.0 or from http://www.microsoft.com/download. Since this tool is originally designed as a Windows 2000 utility, it is a good idea to get some experience with it on **NT 4** so your transition to Windows 2000 Security Configurations will be that much easier.

After installing the MS SCE from Service Pack 4 you have to add the Security Configuration Editor as a snap-in to the Microsoft Management Console.

From the a command prompt launch the MMC:

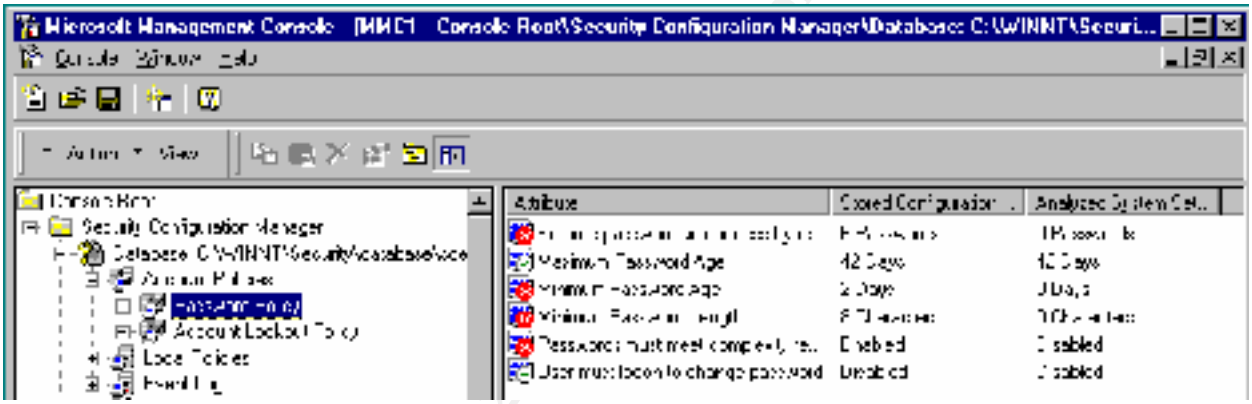
1. Start → Run → mmc
2. From the Console Menu select Add/Remove Snap-In
3. From the Add/Remove Snap-In click Add to open the Add Standalone Snap-in
4. Select Security Configuration Manager then click OK
5. Click OK again



After installing this Snap-In you will be able to configure the following:

- Password Policy
- Account Lockout Policy
- Audit Policy
- User Rights Assignment
- Event Logs Settings
- Group Membership
- System Services Options
- Registry Values
- Registry Permissions and Auditing
- NTFS Folder/File Permissions and Auditing

If you want to compare your current system configuration to a pre-defined security configuration you may do so in the following graphic:



Which security configuration is right for you? This would depend on the type of environment in which you are operating. If you are in a highly secure facility **hisecdc4** might be the best. If you work in a low security environment **basicdc4** might be acceptable. Create a security configuration that works the best for you and then test it on a system away from your production environment.

When you get a configuration that is acceptable and you would like to deploy it to multiple systems, you can use the command line utility **SECEDIT** to map a drive and apply the policy via batch files, System Policy, etc.

Making changes to you security configuration has the possibility of adversely affecting your production environment so **test, test, test!**

As with Service Packs in Windows NT, so are the regularly and irregularly released patches and updates for various Microsoft products such as the OS, Internet Explorer, and various Security Patches.

BEFORE INSTALLING ANY HOTFIX OR UPDATE ON A PRODUCTION SYSTEM MAKE SURE THAT IT HAS BEEN THOROUGHLY TESTED ON A NON-PRODUCTION SYSTEM.

One of the most annoying things about tracking down patches from Microsoft is a lack of a central distribution points from which to obtain these patches.

I usually use the following URL's to obtain patches:

http://windowsupdate.microsoft.com
http://www.microsoft.com/NTServer/all/downloads.asp
http://www.microsoft.com/downloads

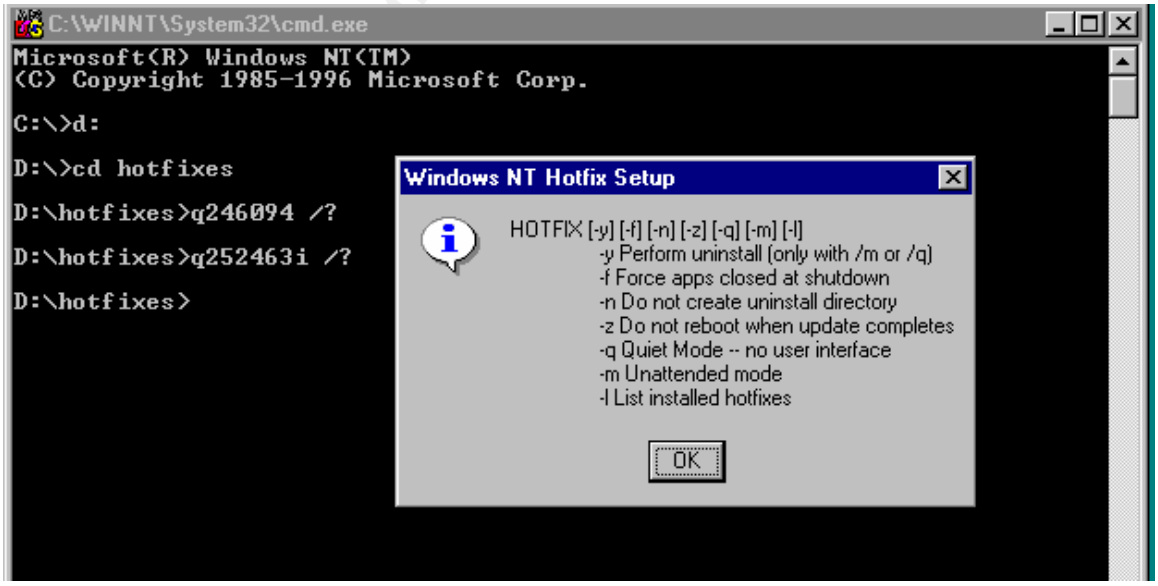
One of the best single sources of Hot Fixes and Services Packs that Microsoft has available is at:

http://www.microsoft.com/technet/support/sp.asp

One thing that I absolute recommend if you want to stay on top of the latest security patches is subscribing to Microsoft's Security Bulletin Service at:

http://www.microsoft.com/technet/security/notify.asp

The rule of thumb with hot fixes and updates is that you should only install them if you are having the problem the hot fix fixes. Once you have downloaded the go to the location and type the name of the executable followed by "/?". This will give you a list of switches as seen below.



These switches, which are similar to the switches that we saw in the Service Pack section of this document, can be useful for scripting numerous hotfixes at one time in a batch file. However, there are a couple of things that you should be aware before installing a hotfix.

- You should always test any hotfix before installing it on a production system.
- Different patches and hotfixes have different switches. Make sure you are aware of all the switches for a particular hotfix before installing or scripting an install of the patch.

When I want to install a group of hotfixes I script them. The following is an example of script that will install a group of hotfixes from a folder called "hotfixes" on the D drive.

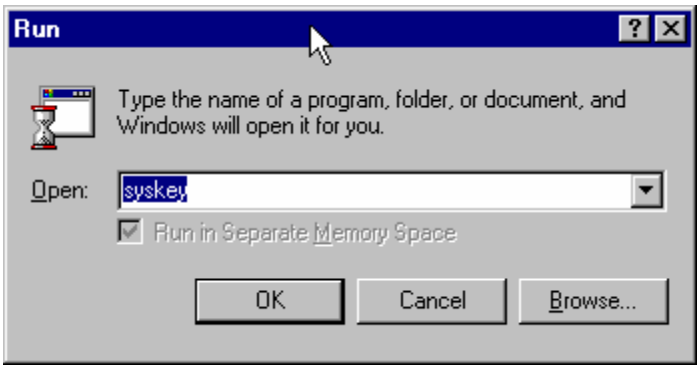
```
cd

d:

cd hotfixes

Q249863i.exe /q /n /z
Q249973i.exe /q /n /z
Q252463i.exe /q /n /z
Q257870i.exe /q /n
```

When this script runs it will run all fixes in quiet mode. It will not back up old files and will not reboot the system until after it finishes Q257870i.exe.

I usually run this script with a Service Pack ahead of all the scripts. Take some time to play with Hotfix and Service Pack scripting and find out what works for you.

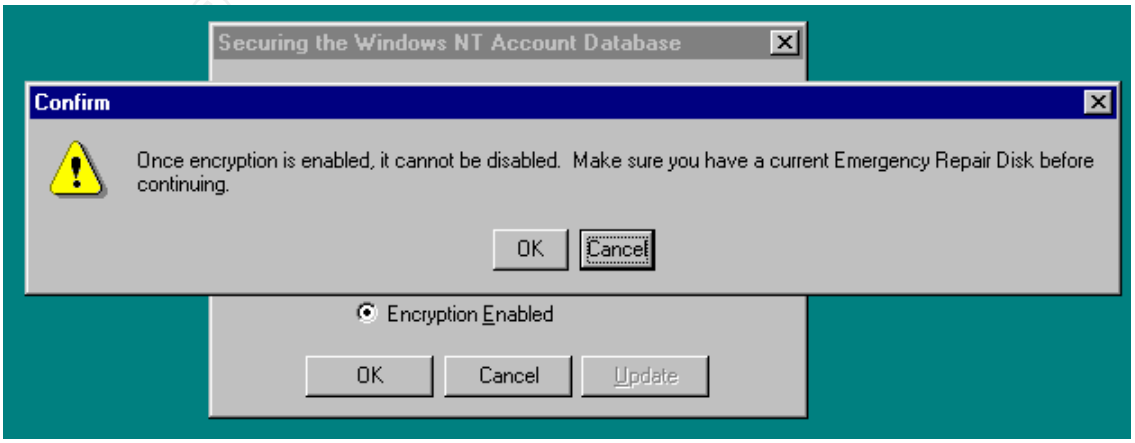
Due to the increase of utilities that can access the password hashes of the SAM database, you can put a second layer of encryption for the LanManager and MD4 hashes of the SAM. If you have installed Service Pack 3 or later, you can run Syskey which will provide this second layer of encryption.

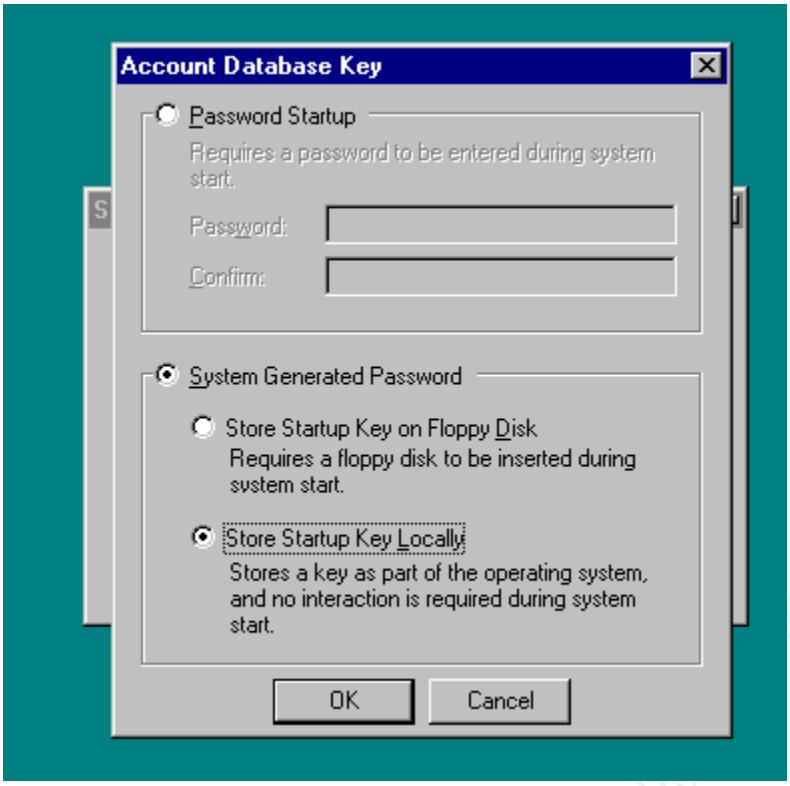
From the run command type: syskey.



By default Encryption disabled is the default.

When you check Encryption Enabled you get a warning message telling you that once you enable the Syskey encryption, it cannot be disabled. Before you go on, you should have a current RDISK available. If you don't, cancel out of this operation and update your RDISK set.



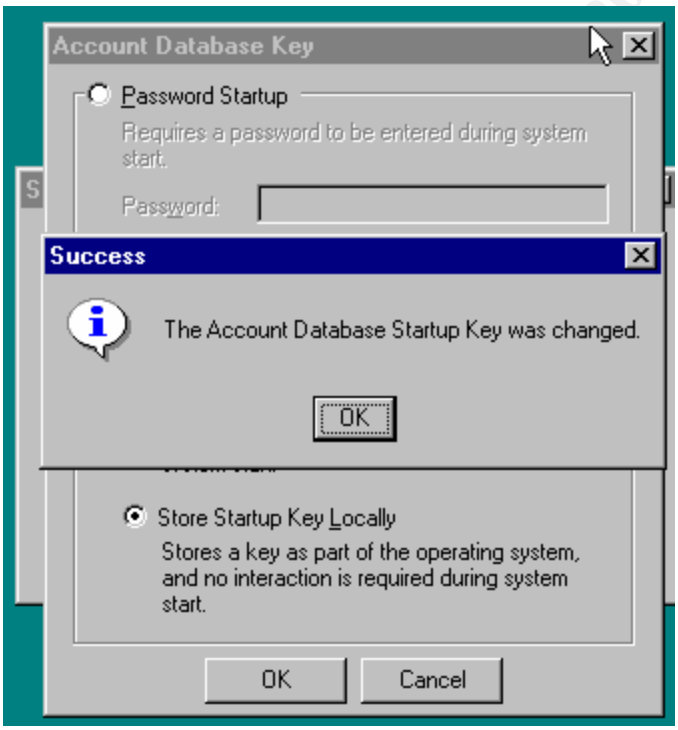


Once you have verified or created a good RDISK, then you need to make a decision where to store the encryption key for the SYSKEY operation.

If you store the StartUp key on a floppy and the server goes down or needs to be restarted you must have the floppy with the key available. If you choose this option you need to make sure that you properly archive this disk. If the disk becomes corrupt, you will not be able to boot the system.

If you store the key locally, then there is no interaction, such as a floppy, to start the computer.

Click OK to SYSKEY the SAM.



Once the process has completed, as seen in the graphic to the left, click OK.

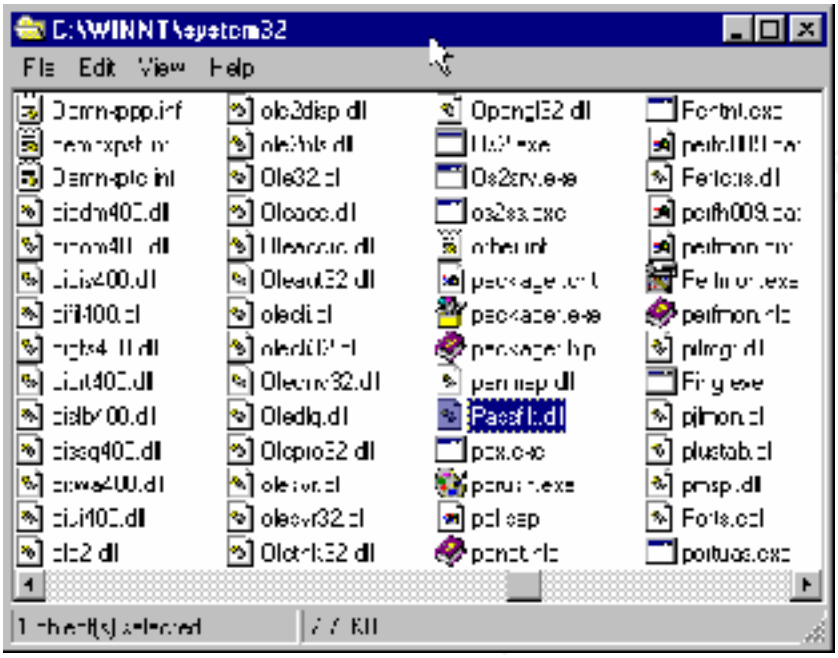
Once you click OK, restart the system.

Once the system has been restarted and you have logged on, go to the Run command and type SYSKEY. The Securing the Windows NT Account Database Windows appears and the Encryption Enabled radio button is filled, while the Encryption Disabled radio Button and text is grayed out.

SYSKEY is now enabled.

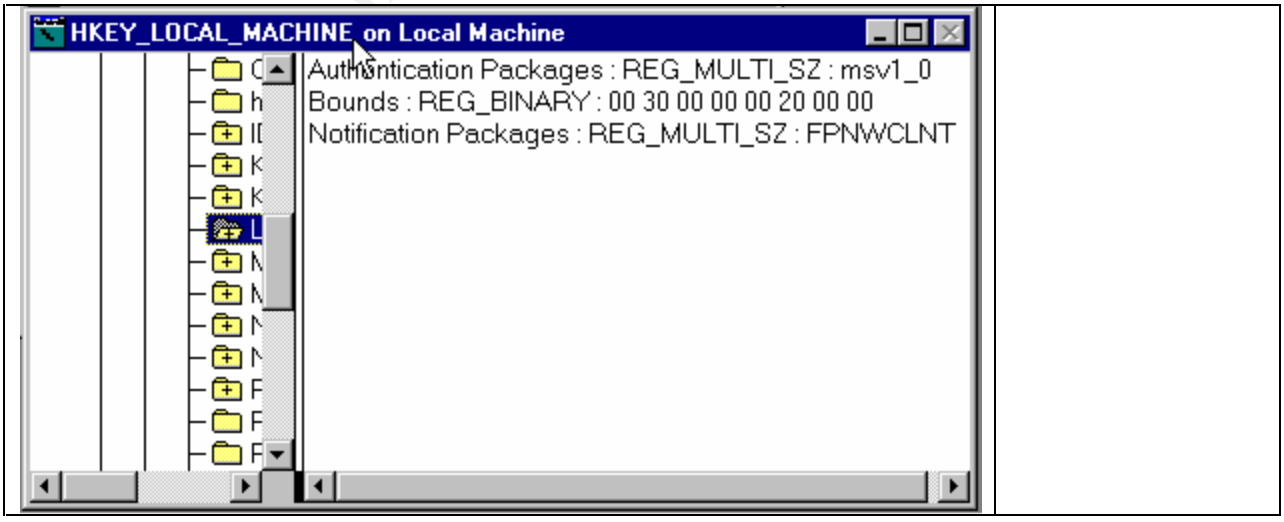
In order to strengthen passwords, Microsoft provides **Passfilt.dll. Passfilt** enforces a minimum of six character passwords, does not contain any part of the users full name, and contains at least three out of the four of the following characters:

- Numbers
- Non-alphanumeric symbols
- Uppercase Letters
- Lowercase Letters

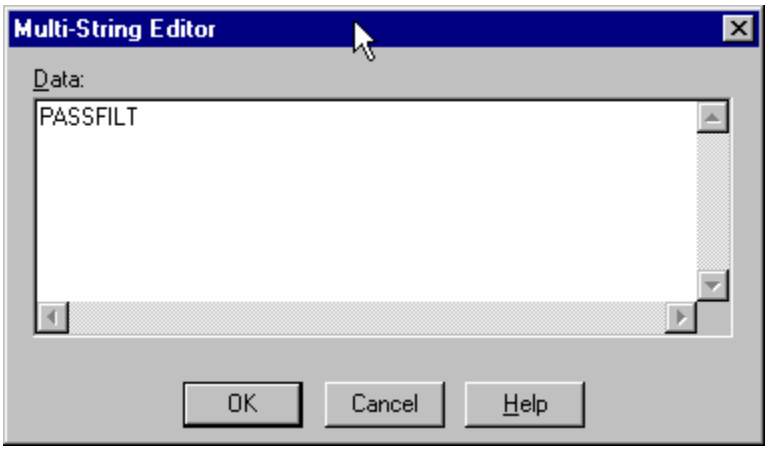


Passfilt.dll can be found in the %systemroot%\system32 directory.

Once you verify that **Passfilt.dll** is in your **%systemroot%\system32**, open **regedt32** from the Run menu and go to **HKLM\CurrentControlSet\Control\LSA.** In the right window you will see the following value for Notification Packages.



Double Click the Notification Packages Value and change the data to the following:

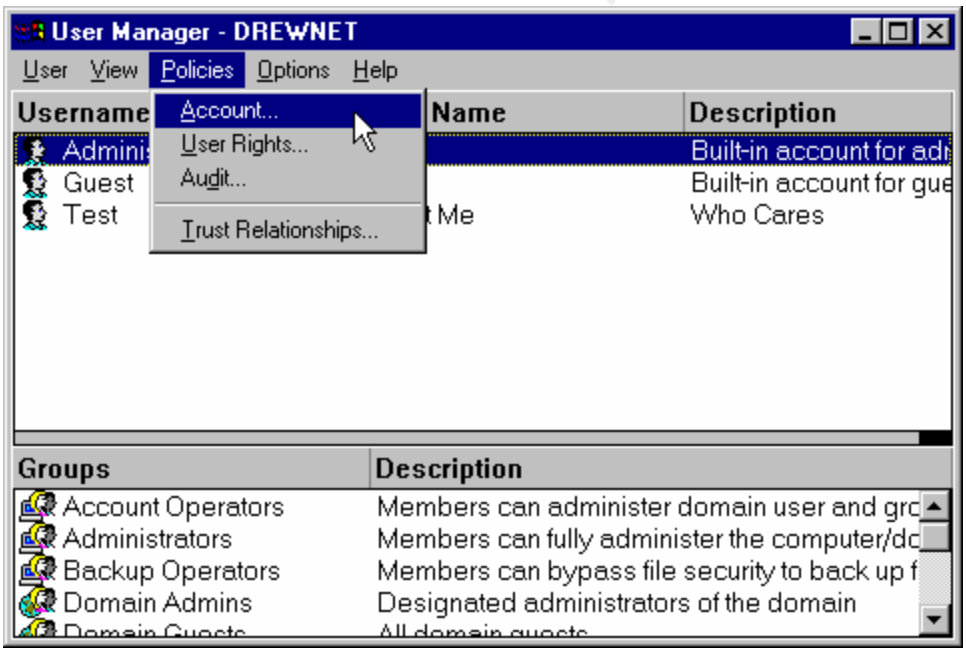


After verifying that the data value has changed close **regedt32** and reboot your system.

Once the system has restarted and you have logged on go to:

Start→Programs→Administrative Tools→User Manager for Domains.

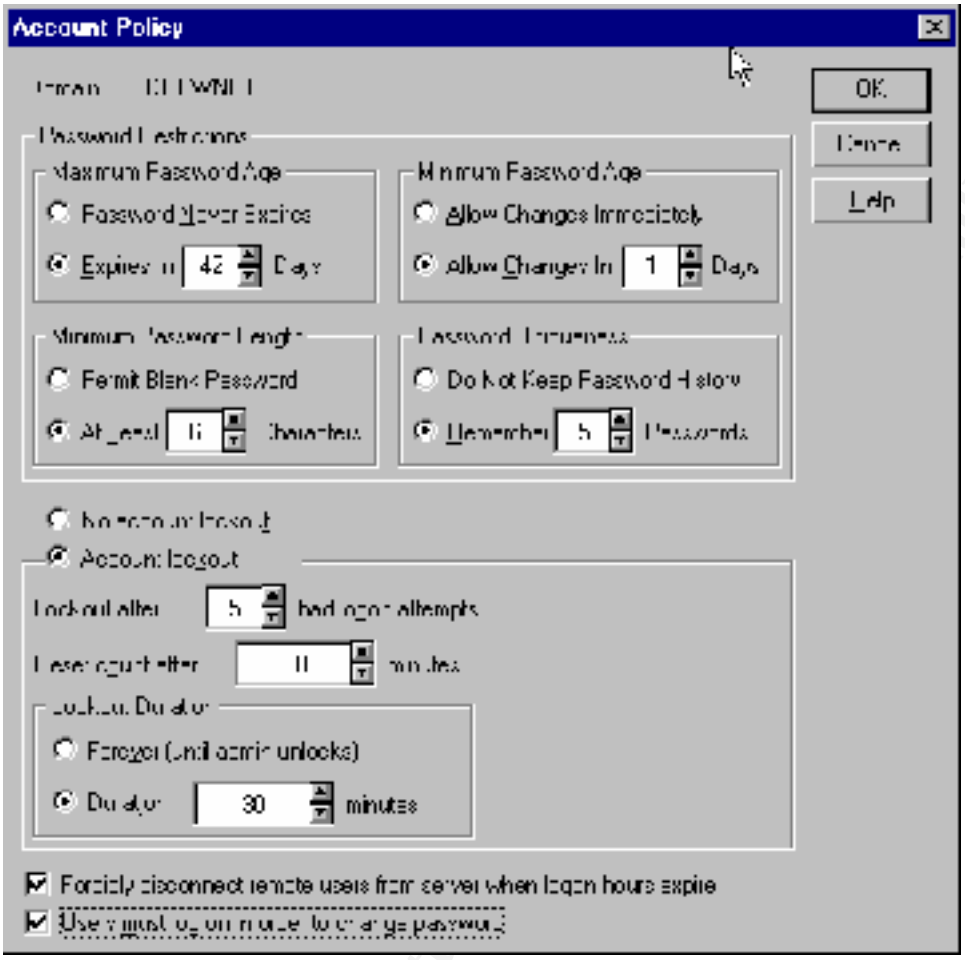
Once User Manager is open go to the Account Policy menu.



Here is the interesting thing about **Passfilt**. It does not turn on its password strengthening until you activate Minimum Password Length. From this Account Policy menu you can also edit the following settings:

Maximum Password Age
Minimum Password Age
Minimum Password Length

Password Uniqueness
Account Lockout Policy
Account Lockout Duration



These settings and others can be configured with the Microsoft Security Configuration Editor.

Once the you have activated the aforementioned settings create a user account and set the password to "**sans**" with no quotes. If **Passfil**t is working you will get the following message:

Protecting the Administrator Account

- Enable Administrator Account Lockout with the **Passprop** utility from the **ResKit**
- Use strong passwords with extended **ASCII** characters
- Remove "Log On Over Network Right" from the admin user rights
- Rename to the administrator to something non-descript
- Create a "honeypot" administrator account that has no rights, but is extensively logged

Disable The Guest

- Make sure that the Guest account is disabled
- Rename the Guest Account
- Create a "honeypot" administrator account that has no rights, but is extensively logged

NTLM v2 Authentication

NTLM is a challenge/response protocol used by Windows NT to that passwords are not sent over the wire. The encryption algorithms used in v1 were the same MD-4 and LanManager of the SAM. This made it easy to crack the password on the wire with such tools as L0pht Crack. With Service Pack 4 NTLM v2 updated NTLM v1. NTLM v2 uses MD-5 and 128 Bit password keys.

In order to enable NTLM v2 go the following registry hive

HIVE	HKEY_LOCAL_MACHINE
KEY	\System\CurrentControl Set\Control\Lsa
Value Name	Lmcompatibilitylevel
Value Type	REG_DWORD
Value Data	0 to 5 (Level 0-3 for Clients) (Level 4-5 for DC's)

Level 0	This is the default behavior. NTLM v2 is not enabled.
Level 1	The user's computer will attempt to negotiate NTLM v2 with the domain controller. If the attempt is unsuccessful the negotiation will revert to Level 0 Authentication.
Level 2	The user's computer will only NT authentication (MD4). All DC's must be upgraded to SP4.
Level 3	The user's computer will only authenticate with NTLM v2. Server running Win9x, Win for Workgroups, and WinNT SP3 can still be accessed as long as DC's are running SP4 or higher.
Level 4	Set this on a DC when you only want to use MD4 and NTLM v2 clients. I.E. the clients must be Windows NT.
Level 5	Set this on a DC when you only want to use NTLM v2. All clients must be WinNT with SP4 or later installed.

Preventing Null Sessions from Listing Usernames

A hacker can use null sessions that can be used to get a list of user accounts from the registry. Since **NT** uses null sessions in place of username and passwords when accessing resources, etc. they are a source of security holes.

Since restricting null sessions has the possibility of breaking certain network services, it is important to test this registry edit on a non-production system.

In order to stop Null Sessions from listing these usernames make the following registry edit.

HIVE	HKEY_LOCAL_MACHINE
KEY	\System\CurrentControlSet\Control\Lsa
Value Name	RestrictAnonymous
Value Type	REG_DWORD
Value Data	1

There are also other registry hacks where you can **Restrict Null Session**, **Share Access** and **Named Pipes**. The registry hacks are as follows for **Shares** and **Named Pipes** respectively:

There are two hacks for Null Session Share Access: **RestrictNullSessionAccess** and **NullSessionAccess.** The **RestrictNullSessionAccess** value restricts access to all shares.

HIVE	HKEY_LOCAL_MACHINE
KEY	\System\CurrentControlSet\Control\Services\LanmanServer\Parameters
Value Name	RestrictNullSessAccess
Value Type	REG_DWORD
Value Data	1

When **RestrictNullSessionAccess** is equal to 1, **Null Session** users cannot access any share, even those shared to the Everyone Group. If there are shares that you would like to allow **Null Session** users to access to then use the following hack:

HIVE	HKEY_LOCAL_MACHINE
KEY	\System\CurrentControlSet\Control\Services\LanmanServer\Parameters
Value Name	NullSessionAccess
Value Type	REG_DWORD
Value Data	<sharenames – do not use UNC or full drive path>

If you would like to control **Null Session** access to named pipes use the following registry hack. This hack works in conjunction with the **RestrictNullSessionAccess** registry key.

HIVE	HKEY_LOCAL_MACHINE
KEY	\System\CurrentControlSet\Control\Services\LanmanServer\Parameters
Value Name	NullSessionPipes
Value Type	REG_DWORD
Value Data	<list of one or more named pipes>

Securing the Net Logon Channel

With Service Pack 4 the NetLogon Channel data can be encrypted and digitally signed for integrity.

Use **regedt** to go to the following registry entry

HIVE	HKEY_LOCAL_MACHINE
KEY	\System\CurrentControlSet\Services\Netlogon\Parameters
Value Name	SignSecureChannel, SealSecureChannel, or RequireSignoOrSeal
Value Type	REG_DWORD
Value Data	1

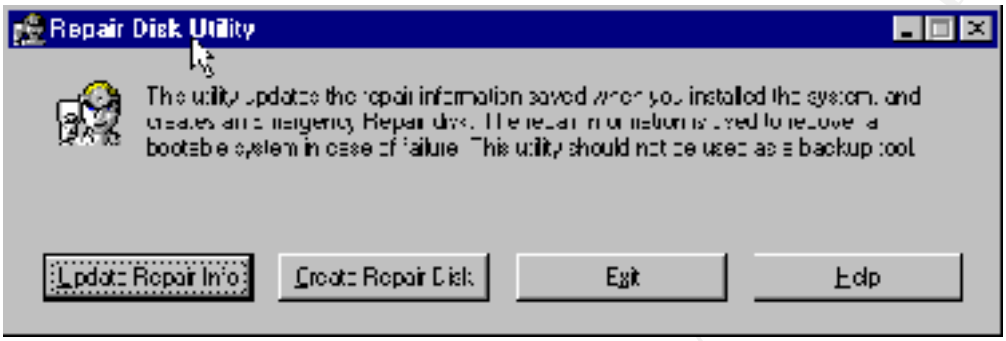
You have three options for value names**: SignSecureChannel, SealSecureChannel**, or **RequireSignoOrSeal.**

SignSecureChannel	When the value for SignSecureChannel is set to 1, all outgoing NetLogon Channel packet are signed for integrity checking.
SealSecureChannel	When the value for SealSecureChannel is set to 1, all outgoing NetLogon Channel packets will be encrypted, as well as digitally signed.
RequireSignoOrSeal	When the value for RequireSignOrSeal is set to 1, all outgoing NetLogon Channel traffic must be digitally signed, but has the option of being encrypted. These options of digital signature and encryption are negotiated between systems. If one of the two systems does not support either option the connection will fail. Only do this if all DC's have been upgraded to SP4 or later. This also included DC's in trusted domains.

Once you have completed the previous step in this paper it is time to preserve what has been done.

One of the things that has been taken for granted is the creation of the **Emergency Repair Disk** and the backing up of the **SAM Database**. I know a lot of System Administrators who either get too busy or simply forget to create **ERD Disks**. When systems go down this can equate to disaster.

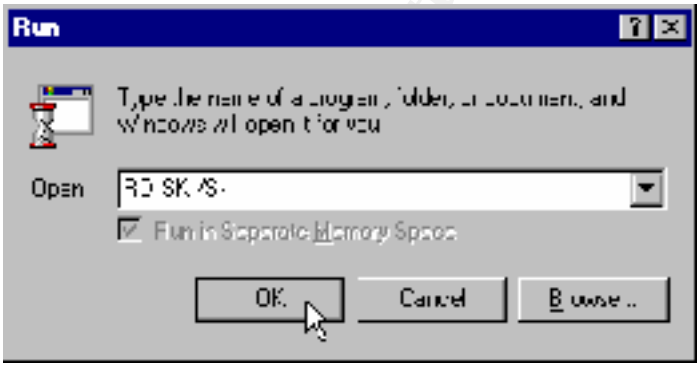
To create an **ERD** disk go the Run menu and type**: rdisk**. You will get the following menu.



From this menu you can create a new Emergency Repair Disk, as well as update an existing one. However, running the standard **RDISK** does not give you a copy of the **SAM** on a floppy disk. It only gives you two accounts in the **SAM**, the original Administrator account and password from the original install of **NT**, which may have been changed.

If you want a copy of the you can **RDISK /S** switch which will copy the **SAM** to the **ERD**.

Another option that might work better is using **RDISK** with the following switches:



Using the "Rdisk /S-" runs Rdisk in quiet mode with no dialogue boxes and does not copy the SAM to a floppy. However it will copy the SAM to: %systemroot%\winnt\repair.

Since it is important to keep a recent copy of the SAM and important system files, I have written the following batch file which will run Rdisk /S- and then copy them to a folder with all their existing attributes in a folder on a separate partition:

The batch file is as follows:

```
rdisk /s-
cd\%systemroot%
xcopy repair D:\rdiskbak /D /A /H /K
```

Once these files are copied to the new directory they can be backed up on tape or other device in preparation for a recovery.

Some other notes for Emergency Repair Disks:

- If you are using Service Pack 6, you will have to copy the Setupdd.sys from the Service Pack to disk 2 of the WINNT setup disks
- ERD Disks should be archived just as back up tapes are archived on a regular basis
- ERD Disks should be protect with measure in effect to control physical access to the disk, as well as the appropriate NTFS permissions be applied to the %systemroot%\repair folder.

The material in this paper was compiled from Windows NT Security: Step-by-Step written by Jason Fossen and Jesper Johansson. The curriculum in this text was delivered from Thrusday May 11th – 13th at the Double Tree Hotel in San Jose, CA.

Microsoft Security Bulletin Service can be obtained at:

http://www.microsoft.com/technet/security/notify.asp

Microsoft Service Packs and Hotfixes can be obtained at:

http://www.microsoft.com/technet/support/sp.asp

L0pht is a trademark of L0pht Heavy Industries

Microsoft Windows, Windows NT, SCE, and all other references to Microsoft are a trademark of the Microsoft Corporation.

All other manufacturers referenced in this document reserve their own copyrights and trademarks respectively.

All screen captures in this document were made with Snag-It 32 v 5.01 which can be obtained at:

http://www.techsmith.com/products/snagit/default.asp

Last Updated: July 24th, 2017

Upcoming Training

SANS Virginia Beach 2017	**Virginia Beach, VA**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS vLive - SEC505: Securing Windows and PowerShell Automation	**SEC505 - 201709,**	**Sep 18, 2017 - Nov 13, 2017**	**vLive**
Secure DevOps Summit & Training	**Denver, CO**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
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**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**