A Brief View Into Auditing Windows NT

By George Do

Table of Contents

Overview

The purpose of this paper is to meet the requirements for the SANS GCNT certification as prescribed by the "Securing Windows" curriculum given on October 2000 in Monterey, California. Please note that this paper does not represent a comprehensive audit technique for Windows NT systems and/or domains. Rather it is the personal interpretation of the author on the major steps that can be taken in order to provide assurance that an NT system is adequately secured and protected. The intent was to maximize the usage of vendor-issued tools so as to minimize the reliance on third party tools. This paper assumes that the auditor either has previous experience in NT administration or the assistance of an NT administrator during the review process.

Description

Microsoft's Windows NT systems are insecure out of the box. There are numerous steps that can be taken to secure these systems thereby minimizing the risk of intrusion and/or denial of service attacks. The audit guide contained below will assist an auditor to gage as well as make crucial improvements to the current level of security for an NT system. Before conducting an audit, a comprehensive security policy must be in place in order to assess compliance or non-compliance of targeted systems. This paper assumes that there is such a prerequisite in place and that all modifications to the system are policy-compliant.

Improving security of Windows-based systems requires much more than what is contained in this guide. Systems administrators must continually practice due diligence and be on top of the latest developments via Microsoft security email alerts, newsgroup discussion forums, or sites which post the latest Windows vulnerabilities such as bugtraq or securityfocus.com.

This paper includes many settings that require accessing and/or modifying the NT registry. **A master backup of the entire registry should be made prior to any changes. Modifications to the registry should also be tested first on a non-production environment.** Particular attention should focus on system functionality, availability, and reliability once changes have been made. Note that installing Service Packs will modify registry key settings.

Specifications

Operating System:	Microsoft Windows NT4.0 Server, ServicePack1 Primary Domain Controller (PDC)
File System:	NTFS C:\ - 4Gig Partition D:\ - 13Gig Partition
Network Protocols:	TCP/IP
Microsoft Networking Services:	RPC Configuration NetBIOS Interface Workstation Server IIS – NOT INSTALLED
Additional Applications:	Office2000 Professional SR1 Snag-It 5.0 Microsoft Management Console v1.0 (MMC) Security Configuration Editor (SCE)
Computer Name:	GEORGE
Domain:	GEORGE.NET
Hardware Components:	Intel Pentium III 650MHz 256MB PC100 SDRAM 17Gig E-IDE HD (1) Linksys LNE 100TX FastEthernet NIC

Service Packs

Description

“Service Packs are the means by which Windows NT product updates are distributed. Service Packs keep the product current, and extend and update your computer’s functionality. Service Packs include updates, system administration tools, drivers, and additional components.” (Microsoft Knowledge Base Article ID: Q152734)

Source: “Sherri_Heckendorn.doc”

Risk

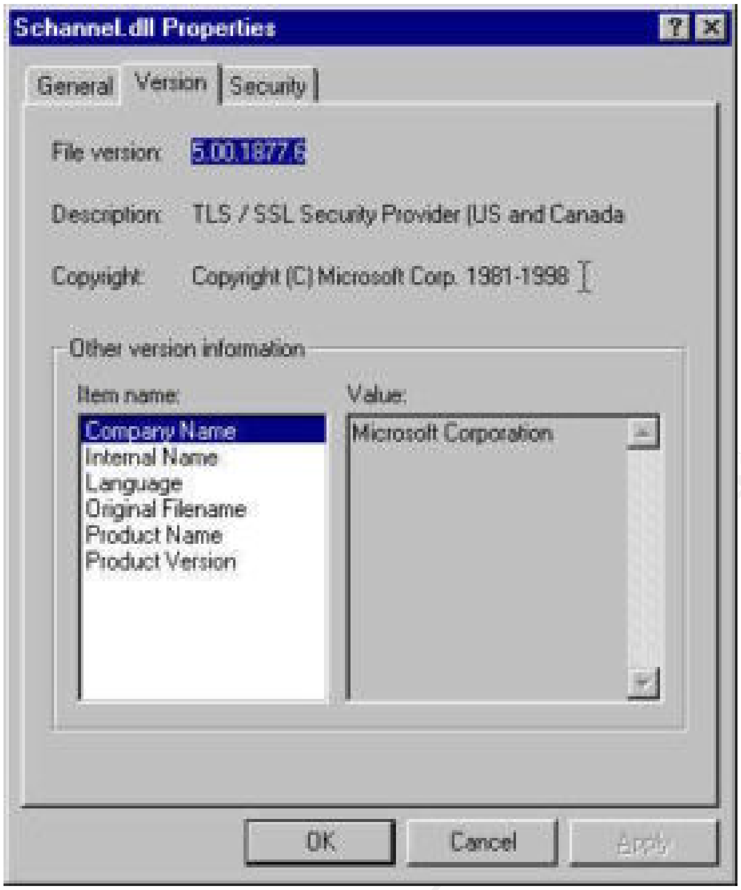
Not having the latest Service Pack installed leaves the system vulnerable to attacks. Attacks may include running unauthorized arbitrary code on the system and/or denial of service attacks.

Audit

Note: **Be sure to test the Service Pack on non-production systems before full deployment. Confirm system functionality, availability, and reliability during test installs.**

Note: Depending on the encryption level of the current NT installation, either a 40bit “Export Version” or a 128bit “US Domestic Version” of the Service Pack may be required**. The 128bit version of the Service Pack will cannot be installed on a lower encryption level system.** To check for the encryption level of the current system:

1. Locate the “schannel.dll” file in the \%systemroot%\system32 directory
2. Right-mouse click on the file and select “Properties”
3. Click on the “Version” tab and look for “US and Canada” for 128bit encryption or “International” for 40bit encryption



File version: 5.00.1877.6

Description: TLS / SSL Security Provider (US and Canada

Copyright: Copyright (C) Microsoft Corp. 1981-1998

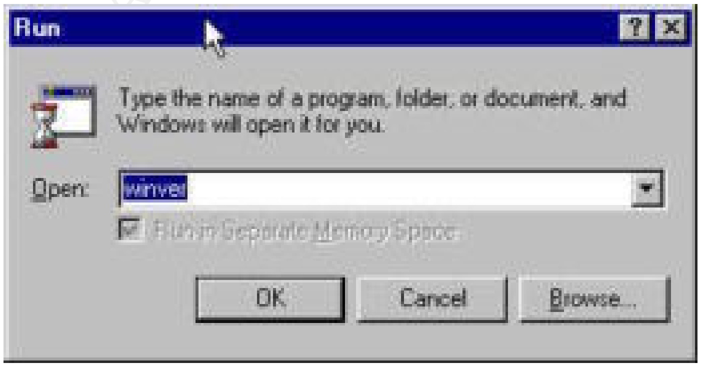
Other version information

Item name:	Value:
Company Name	Microsoft Corporation
Internal Name	
Language	
Original Filename	
Product Name	
Product Version	

Source: "Sherri_Heckendorn.doc"

Check Microsoft's website: http://windowsupdate.microsoft.com for the latest Service Pack information. This site can also be used to look for new hot fixes that are released periodically. As of the writing of this paper, the latest Microsoft Service Pack is SP6a. To check for the currently installed Service Pack:

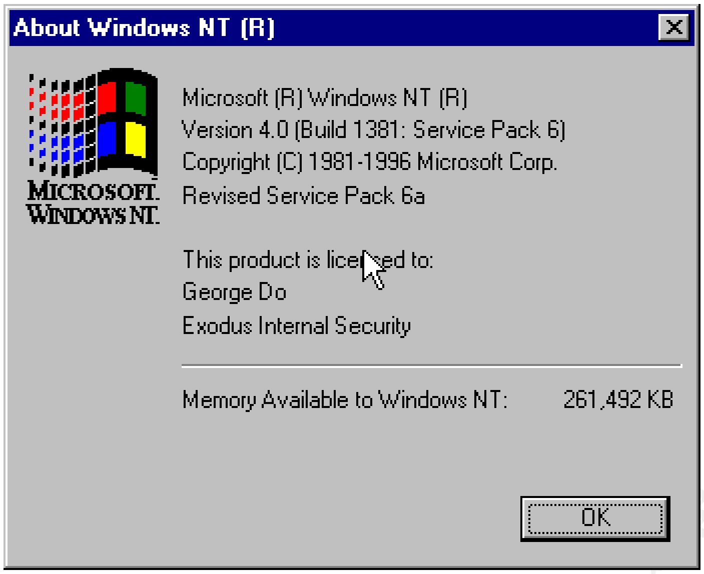
1. Click on the "Start" button
2. Select the "Run…" option
3. Type in "winver" and click on "OK"



Type the name of a program, folder, or document, and Windows will open it for you.

Open: winver

☑ Run in Separate Memory Space



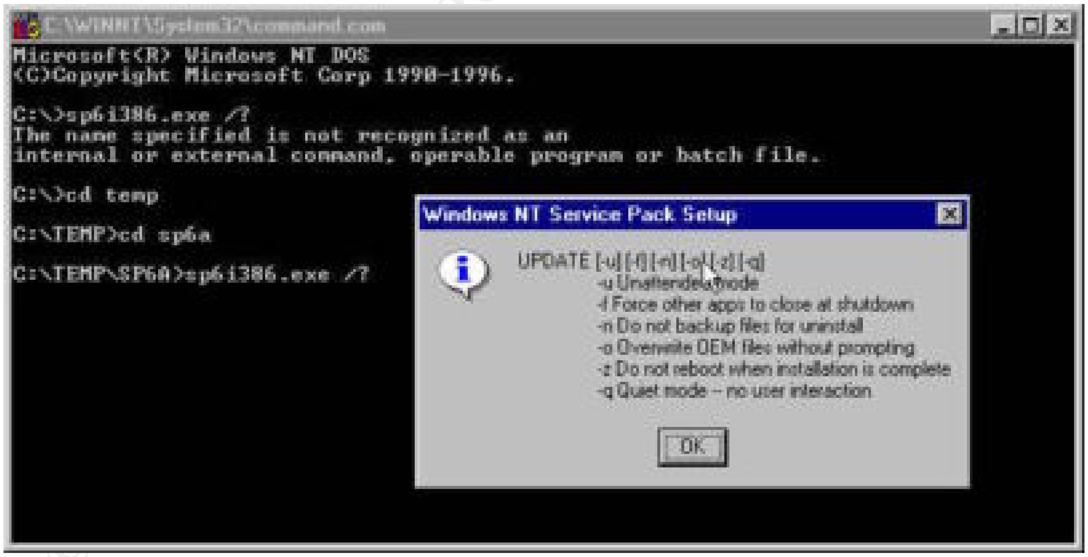
Microsoft (R) Windows NT (R)
Version 4.0 (Build 1381: Service Pack 6)
Copyright (C) 1981-1996 Microsoft Corp.
Revised Service Pack 6a

This product is licensed to:
George Do
Exodus Internal Security

Memory Available to Windows NT: 261,492 KB

To install the latest Service Pack, download the appropriate version from Microsoft's website: http://windowsupdate.microsoft.com

1. Open a DOS Prompt
2. Traverse to the directory where the Service Pack was downloaded
3. Type "<ServicePackName> /?" to see all options available for install



```
Microsoft(R) Windows NT DOS
(C)Copyright Microsoft Corp 1990-1996.

C:\>sp6i386.exe /?
The name specified is not recognized as an
internal or external command, operable program or batch file.

C:\>cd temp

C:\TEMP>cd sp6a

C:\TEMP\SP6A>sp6i386.exe /?
```

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

Service Packs can also be installed by simply double-clicking on the service pack file itself. The primary advantage of installing via the command line is installation can be accomplished via batch jobs without user interaction. Command line installations are also better suited for networks with many domain controllers.

Password Policies

Description

Usernames and passwords are the method by which a user authenticates him/herself to the system. When authenticated, a set of permissions to applications, services, and files are assigned to the user. This unique identification can also be used to audit user activities such as file and application access.

Risk

Since passwords are the keys to access the system, many attacks focus on extracting passwords by cracking password hashes or social-engineering a password from a user. This risk is compounded if the user uses weak passwords. These passwords can be compromised even with a simple brute-force attack.

Source: Hacking Exposed, Network Security Secrets & Solutions

Audit

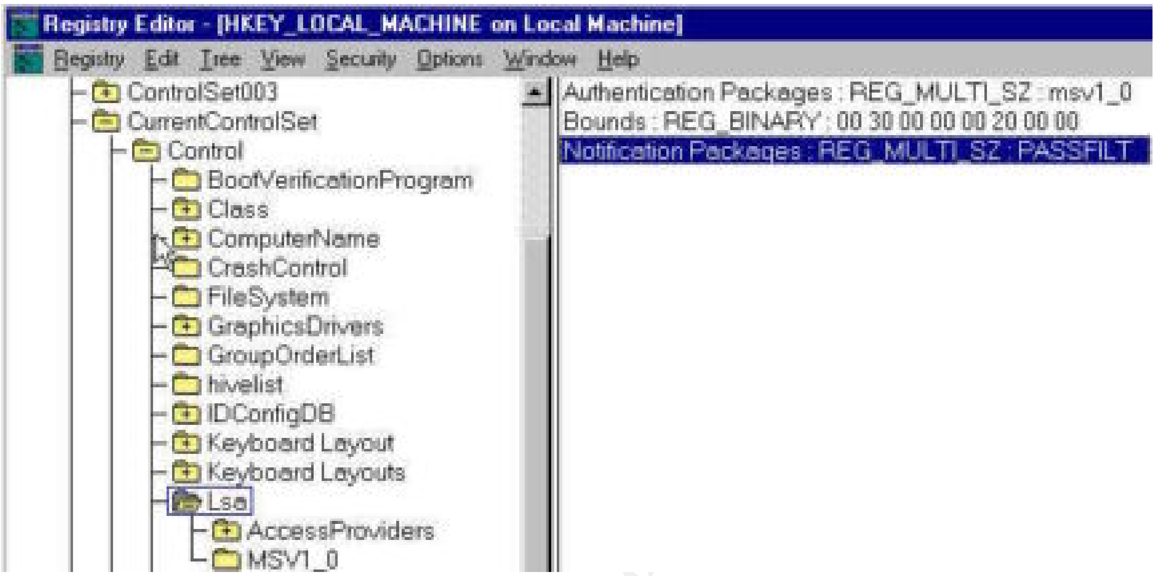
"With Service Pack 2 and later, a service that can enforce complex passwords is available. This service will ensure that passwords are (1) at least 6 characters long, (2) contain characters from at least three of the following four groups: lower case letters, upper case letters, numbers, non-alphanumeric characters, and (3) passwords do not contain your user name or any part of your full name. These requirements are enforced the next time a user changes his or her password."

Source: "SANS Windows NT Security Step By Step, Version 2.15, July 30, 1999"

To enforce a strong password policy:

1. Make sure the latest Service Pack has been installed
2. Confirm that the "passfilt.dll" file is present in the \%systemroot%\system32 directory
3. Confirm the following Registry Key Setting

Hive:	HKEY_LOCAL_MACHINE
Key:	\SYSTEM\CurrentControlSet\Control\LSA
Name:	Notification Packages
Type:	REG_MULTI_SZ
Value:	PASSFILT



```
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
Notification Packages : REG_MULTI_SZ : PASSFILT
```

Note: **The password policy will not take effect until the next time users go to change their passwords. You must also activate the "Minimum Password Length" in order for the password filter to take effect.** Go to User Manager -> Policies -> Account… and enable the Minimum Password Length. Settings for Minimum/Maximum Password Age and Password Uniqueness are also available for enforcement from this menu.

Source: "Securing Windows NT" by Andrew Kjell Nielsen

Logon Policies

Description

Logging onto Windows NT is the common process shared by all users to gain access to the system. There should be logon policies relating to how users should be able to attempt authentication with the system. Attackers focus on this simple process, looking for vulnerabilities for exploitation.

Risk

By default configuration, NT allows simple brute-force logon attempts to user accounts with no lockout protection. Blank passwords are permitted and there are no password histories kept to prevent the recycling of passwords. These settings are insecure and provide a simple yet effective way for attackers to exploit the system.

Audit

Modify the default settings within User Manager to the recommended settings. Note however "longer lockouts enable a different kind of denial-of-service attack in which attackers can force users to be locked out of their workstation."

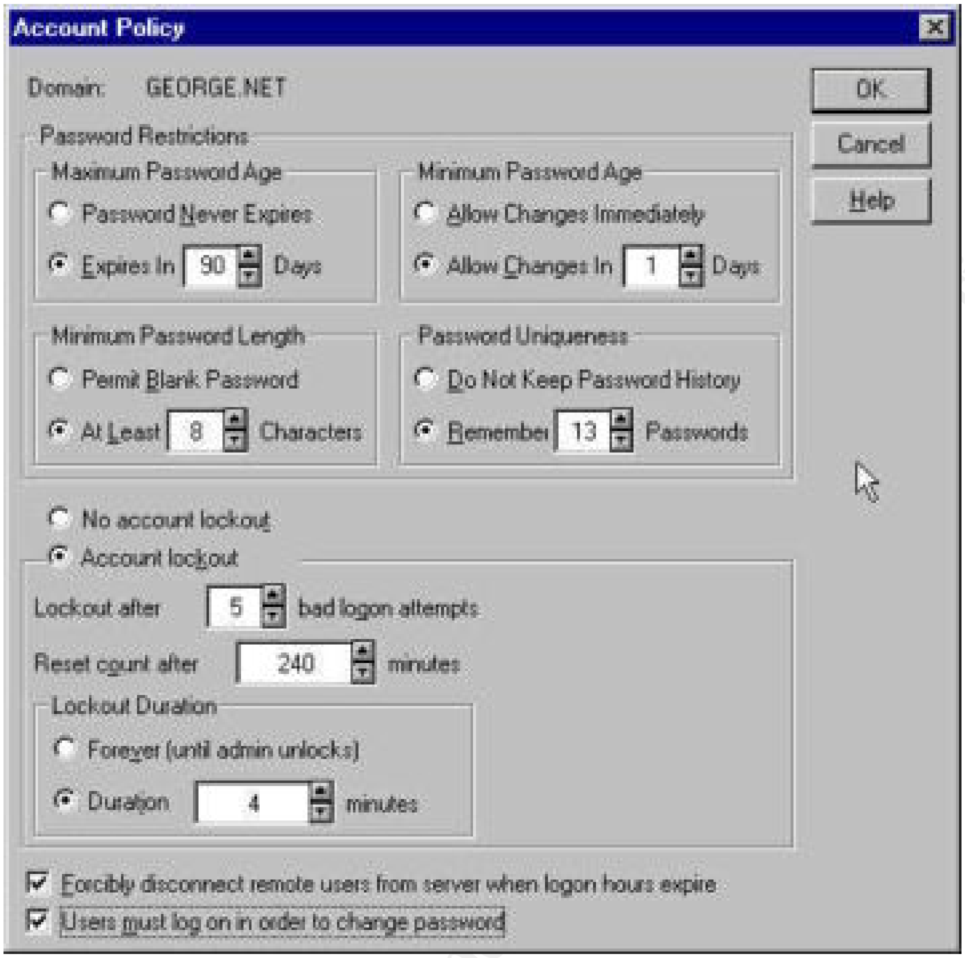
Source: "SANS Windows NT Security Step By Step, Version 2.15, July 30, 1999"

To change default settings:

1. Go to User Manager -> Policies -> Account
2. These are recommended settings as specified by the SANS Securing Windows NT Step By Step Guide

   Maximum Password Age = 45-90 Days
   Minimum Password Age = 1-5 Days
   Minimum Password Length = 8 Characters
   Password Uniqueness = 8-13 passwords
   Account Lock = Lockout after 5 Hours, Reset Count after 4 Hours
   Lock Duration = 4 Hours (or require Administrator intervention)
   Users Must Logon to Change Passwords = Yes

Note: **These settings are highly dependent on the size and complexity of the network. Settings should be made in small increments to find an acceptable balance between security and user requirements.**



Account Policy

Domain: GEORGE.NET

Password Restrictions

Maximum Password Age
○ Password Never Expires
● Expires In 90 Days

Minimum Password Age
○ Allow Changes Immediately
● Allow Changes In 1 Days

Minimum Password Length
○ Permit Blank Password
● At Least 8 Characters

Password Uniqueness
○ Do Not Keep Password History
● Remember 13 Passwords

○ No account lockout
● Account lockout

Lockout after 5 bad logon attempts

Reset count after 240 minutes

Lockout Duration
○ Forever (until admin unlocks)
● Duration 4 minutes

☑ Forcibly disconnect remote users from server when logon hours expire
☑ Users must log on in order to change password

Restrict Null Sessions / Access

Description

Null User Sessions are defined as "an over-the-network logon where the username and password are both the null character." These types of connections are used for administrative purposes when a conventional account is not available or cannot be used due to the level of rights and permissions. For example, "the local System account, under which many network services run, can only connect to remote machines with null user sessions."

Source: Securing Windows NT Step-By-Step, Parts 1-3, by Jason Fossen and Jennifer Kolde

Risk

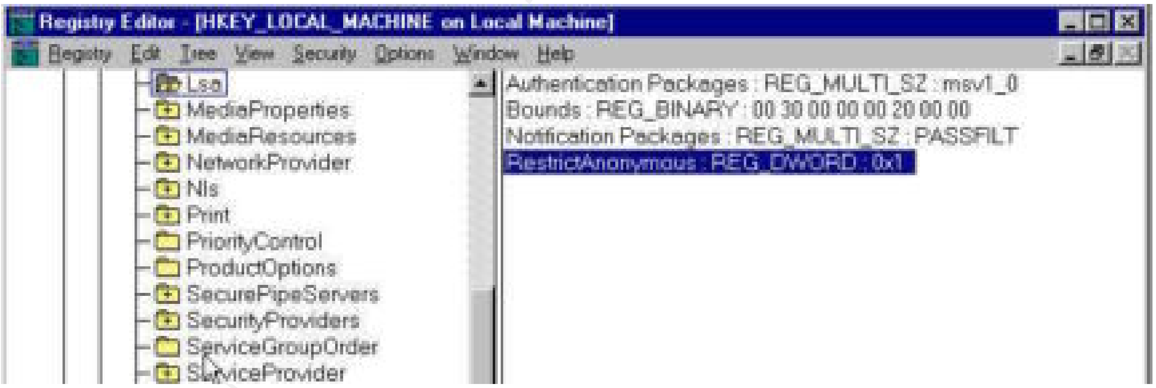
Null users are considered to be members of the Everyone group without providing any credentials. Null sessions can be used to extract a list of usernames and groups from a remote domain controller. This provides "valuable recognizant information for attackers that can be used for immediately for brute-force attacks". Null Sessions can also be used to gain access to folders and files that have poor NTFS permissions.

Source: Hacking Exposed, Network Security Secrets & Solutions

Audit

The NT registry can be modified so as to prevent null sessions from listing users and groups from one's domain. This change must be made on all primary domain controllers.

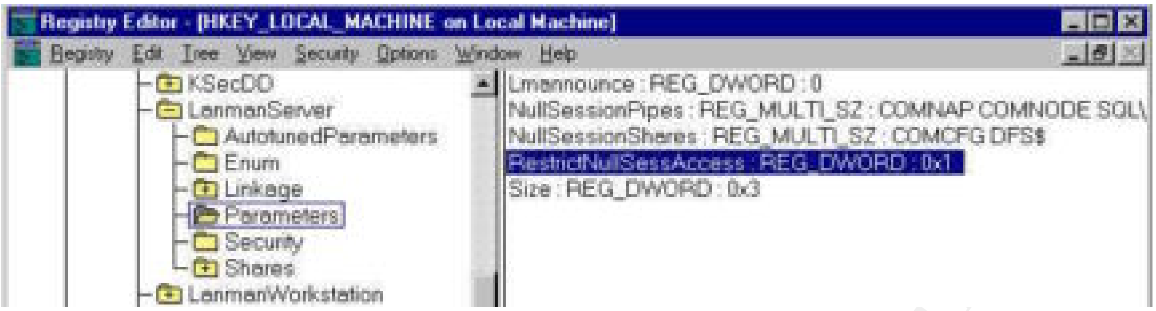
Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Control\LSA
Value Name: RestrictAnonymous
Value Type: REG_DWORD
Value Date: 1



```
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
Notification Packages : REG_MULTI_SZ : PASSFILT
RestrictAnonymous : REG_DWORD : 0x1
```

The NT registry also has 2 registry keys that govern Null Session share access. To restrict ALL Null Session access to all shares, make sure the following Registry Key is present:

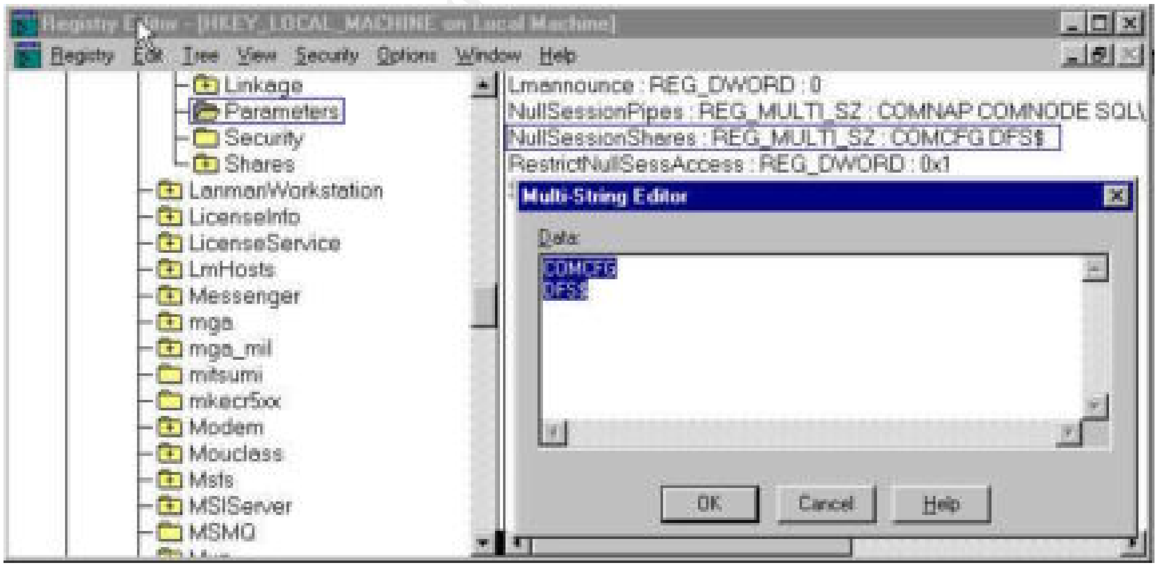
Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name: RestrictNullSessAccess
Value Type: REG_DWORD
Value Date: 1



```
Lmannounce : REG_DWORD : 0
NullSessionPipes : REG_MULTI_SZ : COMNAP COMNODE SQL\
NullSessionShares : REG_MULTI_SZ : COMCFG DFS$
RestrictNullSessAccess : REG_DWORD : 0x1
Size : REG_DWORD : 0x3
```

Setting the Value to 1 to will restrict all Null Session access to share. **Note however that certain applications may need to use null sessions to access shares such as commercial backup software packages. Setting this key alone may break these applications.** Careful examination of the implications of turning off null sessions should be considered before implementation. As with any registry modification, these changes should be first tested on a non-production environment. In a case where known applications require null sessions to access shares, use the second registry key to make exceptions to this deny-all rule:

Hive: HKEY_LOCAL_MACHINE
Key: \System\CurrentControlSet\Services\LanmanServer\Parameters
Value Name: NullSessionShares
Value Type: REG_MULTI_SZ
Value Date: <Share Names>



```
Lmannounce : REG_DWORD : 0
NullSessionPipes : REG_MULTI_SZ : COMNAP COMNODE SQL\
NullSessionShares : REG_MULTI_SZ : COMCFG DFS$
RestrictNullSessAccess : REG_DWORD : 0x1
```

```
COMCFG
DFS$
```

Please note that <Share Names> should not be the explicit UNC path to the share but rather just the name of the share. Setting these 2 keys will restrict Null Sessions to all shares, effectively denying all null connections to all shares, while allowing null session access to only those shares that require the null session to function.

Registry & SAM Database Backup

Description

The NT registry holds crucial information regarding systems and security settings. In the event of a system crash, it is imperative that backups of the registry and SAM database are available for recovery. However backing up the registry is often taken for granted by many system administrators.

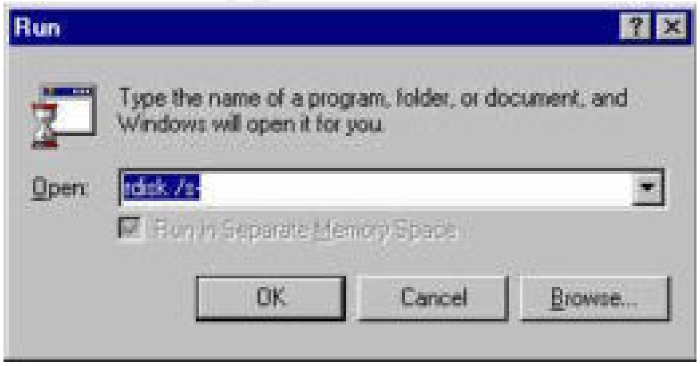
Risk

Without current and viable backups of the registry and SAM database, recovery in the event of a disaster is impossible.

Audit

A full backup of the system registry and SAM DB should be made. **This is especially important when using the SYSKEY utility to encrypt the SAM DB (See Below).** The archiving media (floppy, zip disk, etc.) should be physically protected as it contains the original entire SAM DB. To produce a complete backup of the entire registry and SAM database:

1. Go to Start -> Run…
2. Type in "rdisk /s-"

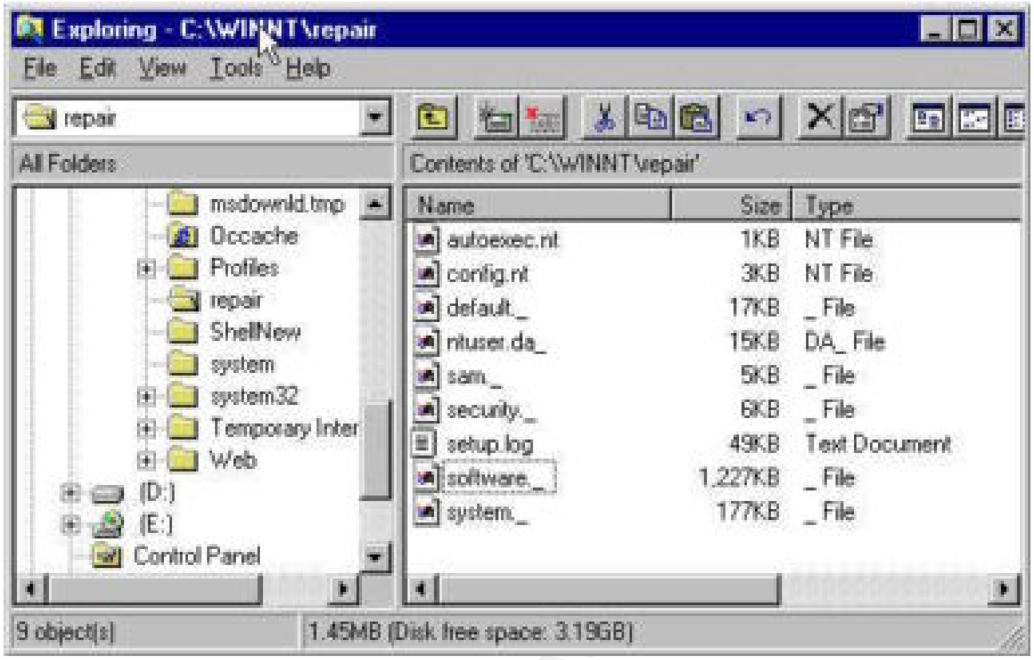


Type the name of a program, folder, or document, and Windows will open it for you.

Open: rdisk /s-

☑ Run in Separate Memory Space

This command will archive the complete SAM DB into the \%systemroot%\repair directory. Simply copy the contents of this directory into removable media or a secure location.



Contents of 'C:\WINNT\repair'

Name	Size	Type
autoexec.nt	1KB	NT File
config.nt	3KB	NT File
default._	17KB	_ File
ntuser.da_	15KB	DA_ File
sam._	5KB	_ File
security._	6KB	_ File
setup.log	49KB	Text Document
software._	1,227KB	_ File
system._	177KB	_ File

9 object(s) 1.45MB (Disk free space: 3.19GB)

SYSKEY – SAM Database Encryption

Description

By default, all user MD4 password hashes are stored in the SAM database. Though passwords are not stored in clear text, the password hashes are easily extracted for cracking via password cracking utilities such as l0phtcrack. Microsoft provides a mechanism called SYSKEY for encrypting the password hashes to prevent utilities such as l0phtcrack from extracting them from the SAM database. **Note that this does NOT protect password hashes that are stored in cache memory or in transit over the network.** L0phtcrack is also capable of extracting the hashes from cache memory to proceed with its password cracking.

Risk

The NT MD4 hash is weak. Utilities such as l0phcrack uses a dictionary method of attack where it compares the user password hashes to the hashes computed from given strings (a dictionary file, randomly computed characters, etc.) to see if they match. If a match is made, then the user password is simply the given string.

Audit

With Service Pack 3 and later, NT password hashes can be encrypted with use of a system key, SYSKEY.EXE. Note that only password hashes are encrypted and that the rest of the SAM database is not. SYSKEY "will generate a 128bit random key with which to encrypt the password hashes in the SAM DB. This random key is then encrypted with a second key called the System Key." **The System Key is crucial in that it holds the key to unlock the SAM DB and as such, it should be protected accordingly.**

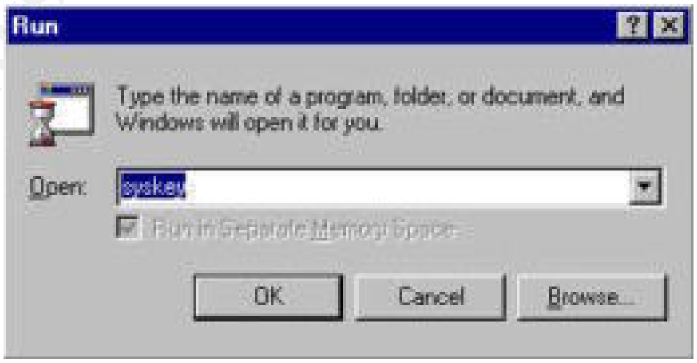
Source: Securing Windows NT Step-By-Step, Parts 1-3, by Jason Fossen and Jennifer Kolde

Note: **Encrypting the SAM DB is irreversible. Please see the above procedure for backing up the registry and SAM DB in the event that the System Key is not available.** The System Key is required for the system to boot up. There are 3 options to backup the System Key:

1. Hidden on the computer itself with a "complex obscuring function" to conceal it (**Advantages:** unattended reboots, **Disadvantages:** system key is stored locally and may be compromised in the future)
2. Stored on a floppy, floppy must be available for all reboots (**Advantages:** system key is not stored locally, **Disadvantages:** floppy is needed every time the system reboots)
3. System Key can be generated (MD5) from a password up to 128 characters long. (**Advantages:** key is generated every time the system reboots, no need for backup, **Disadvantages:** individual(s) must be entrusted with this password)

To use the SYSKEY utility:

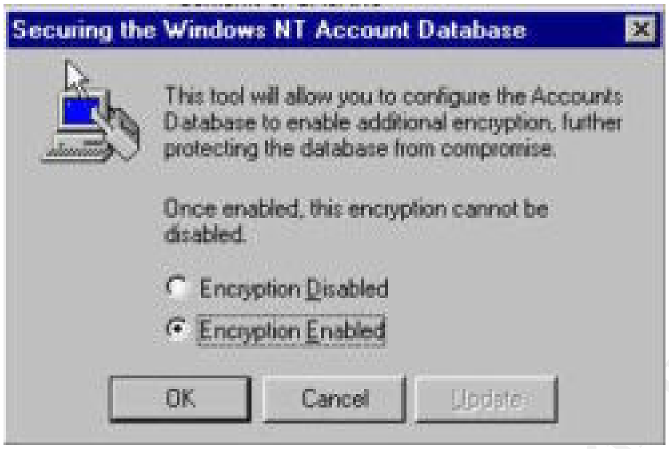
1. Go to Start -> Run…
2. Type in "syskey" at the prompt and Click OK


Type the name of a program, folder, or document, and Windows will open it for you.

Open: syskey

☑ Run in Separate Memory Space

3. Select "Encryption Enabled" and Click OK



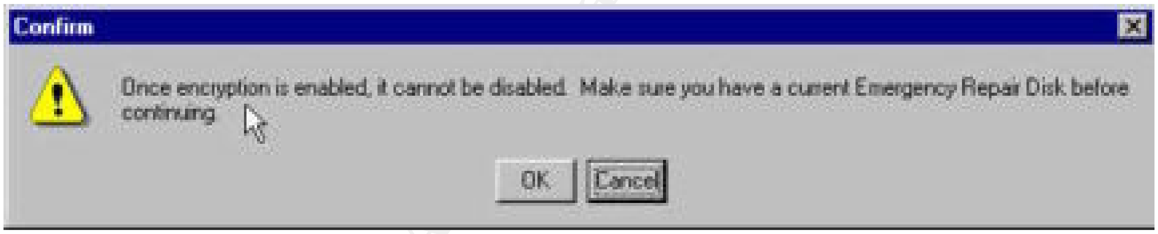
Securing the Windows NT Account Database

This tool will allow you to configure the Accounts Database to enable additional encryption, further protecting the database from compromise.

Once enabled, this encryption cannot be disabled.

○ Encryption Disabled

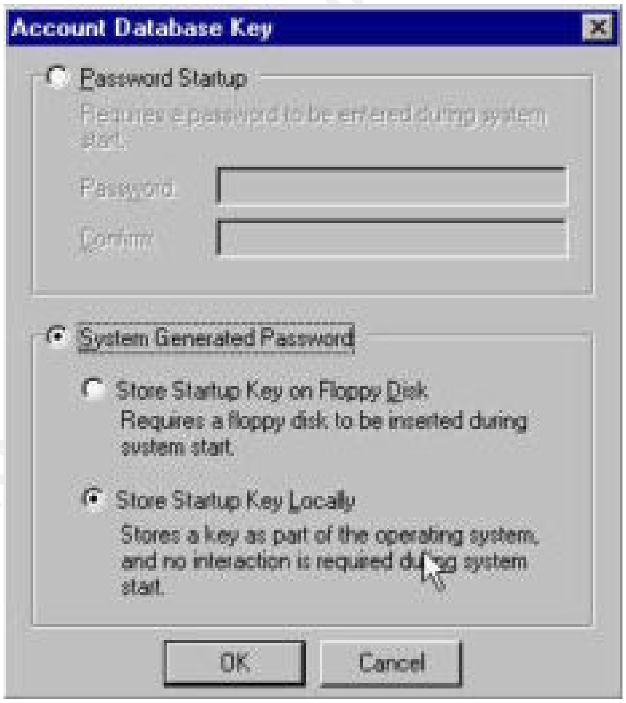
● Encryption Enabled



Confirm

Once encryption is enabled, it cannot be disabled. Make sure you have a current Emergency Repair Disk before continuing

4. Select 1 out of the 3 options for backing up the System Key



Account Database Key

○ Password Startup

Requires a password to be entered during system start.

Password:

Confirm:

● System Generated Password

○ Store Startup Key on Floppy Disk

Requires a floppy disk to be inserted during system start.

● Store Startup Key Locally

Stores a key as part of the operating system, and no interaction is required during system start.

NTLMv2 Authentication

Description

"Authentication is the process of proving one's identity to another party. Users authenticate themselves to domain controllers and servers by providing a set of credentials: username and password." Clear text passwords are not transmitted in clear text over the network. NT uses a challenge/response authentication method, whereby the password is used as an encryption key for encrypting a random challenge sent to the client from the server. If the server can decrypt the client's response, it proves that the user knows the password.

Risk

NT's default authentication method is called LanManager (LM) and NTLM. When the challenge/response authentication packets are transmitted over the network, they can be sniffed with use of a protocol analyzer or utilities such as l0phtcrack. From the sniffed packets, attackers can extract the LM and NTLM password hashes and proceed with password cracking activities just as though the hashes had been read out of the SAM DB.

Audit

NT supports multiple authentication methods, the default being LM and NTLMv1 which are weak and can be easily compromised with a utility such as l0phcrack. Starting with Service Pack 4, a new authentication method called NTLMv2 can be used to thwart network-based types of attacks. Some key features of NTLMv2 include:

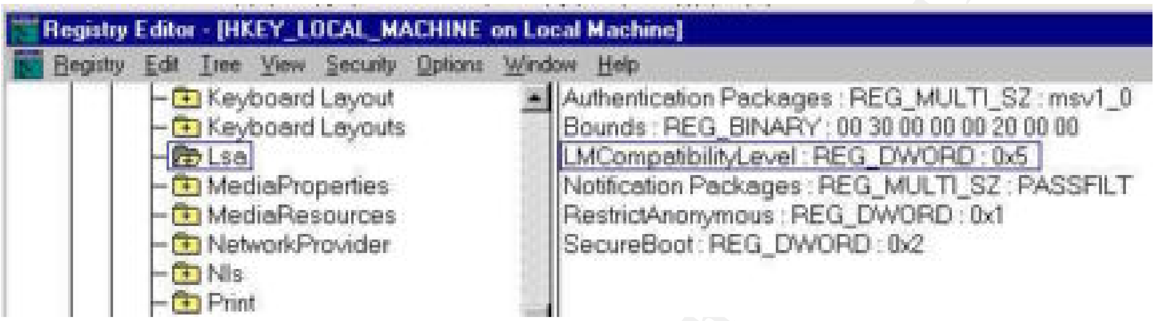
1. Mutual authentication between client and server
2. Use of timestamps
3. 128bit password hashes

NTLMv2 will prevent:

1. "Man-in-middle" attacks
2. Replay attacks
3. l0phcrack packet sniffing attacks

NTLMv2 is configured via a registry key

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Control\LSA
Value Name:	LMCompatibilityLevel
Value Type:	REG_DWORD
Value Data:	<Level Number (0 to 5)>



```
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
LMCompatibilityLevel : REG_DWORD : 0x5
Notification Packages : REG_MULTI_SZ : PASSFILT
RestrictAnonymous : REG_DWORD : 0x1
SecureBoot : REG_DWORD : 0x2
```

Level Number	LMCompatibilityLevel Authentication Types
0	Default behavior if key does not exist. Client will authenticate exactly as it did before and not use NTLMv2. Domain controllers will accept NTLMv2 if a client requests it.
1	Clients will attempt to negotiate NTLMv2, but will fall back to LM and NTLMv1 authentication when necessary. Domain controllers will accept NTLMv2 if client requests it.
2	Clients will use NTLMv1 authentication only. Clients will not use LM or NTLMv2 responses. Domain controllers will accept NTLMv2 if client requests it.
3	Clients will use NTLMv2 authentication only. Domain controllers will accept NTLMv2 authentication if client requests it.
4	Clients will use NTLMv2 authentication only. Domain controllers will refuse LM authentication and accept NTLMv1 or NTLMv2 authentication if client requests it.
5	Clients will use NTLMv2 authentication only. Domain controllers will refuse LM/NTLMv1 authentication and accept only NTLMV2.

Source: Securing Windows NT Step-By-Step, Parts 1-3, by Jason Fossen and Jennifer Kolde

Ideally, Level 5 should be used for maximum security, however "consider that all **clients must be able to authenticate using NTLMv2**." Windows 95/98 clients by default do not use NTLMv2 but can be configured to do so. Select a level that best fits your environment as well as meets an acceptable level of security.

Source: Essential Windows NT System Administration, by AEleen Frisch, O'Reilly and Associates, January 1998

NetLogon Channels

Description

"NetLogon channels are used for pass-through authentication and synchronization of the user accounts database." (i.e. A user is able to log on at one computer even though their account is located on another computer) Communications between BDC's and PDC's also utilize the NetLogon Channel. NetLogon channels are a requirement for large NT networks.

Risk

Although the NetLogon channel can be considered as a "secure" channel between NT systems, only the computer account password information is encrypted. A major weakness of the NetLogon channel is the lack of integrity-checking, which leaves the channel vulnerable to sniffing and man-in-the-middle attacks.

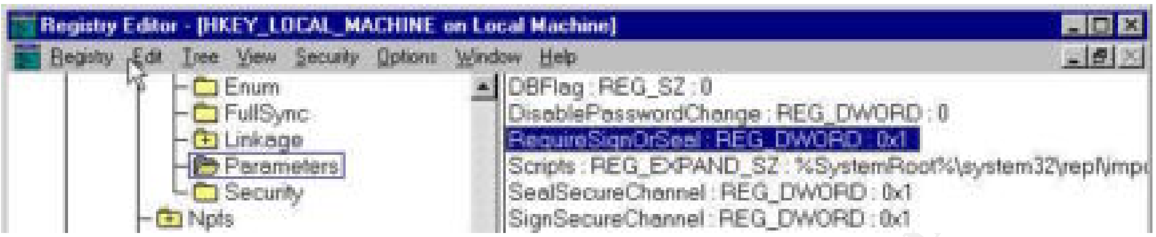
Audit

With at least Service Pack 4 installed, the NetLogon channel can be encrypted and digitally signed for integrity. Modification of the following registry key can be used to secure NetLogon channels.

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\Netlogon\Parameters

Value Name	Value Type	Effects
SignSecureChannel	REG_DWORD	When set to 1, all outgoing NetLogon channel packets will be digitally signed for integrity-checking
SealSecureChannel	REG_DWORD	When set to 1, all outgoing NetLogon channel traffic will be encrypted. This option also forces digital signing.
RequireSignOrSeal	REG_DWORD	When set to 1, all outgoing NetLogon channel traffic must at least be digitally signed, but may also be encrypted. These options will be negotiated.

Source: Securing Windows NT Step-By-Step, Parts 1-3, by Jason Fossen and Jennifer Kolde


Registry Editor - [HKEY_LOCAL_MACHINE on Local Machine]
Registry Edit Tree View Security Options Window Help

```
Enum
FullSync
Linkage
Parameters
Security
Npfs
```

```
DBFlag : REG_SZ : 0
DisablePasswordChange : REG_DWORD : 0
RequireSignOrSeal : REG_DWORD : 0x1
Scripts : REG_EXPAND_SZ : %SystemRoot%\system32\repl\imp
SealSecureChannel : REG_DWORD : 0x1
SignSecureChannel : REG_DWORD : 0x1
```

Ideally all 3 values should have a value of 1 to insure integrity. As stated earlier, changes to the registry should be tested thoroughly on a non-production environment before actual implementation.

Microsoft Security Configuration Editor (SCE)

Description

Microsoft provides a crucial security tool for NT systems called the Security Configuration Editor (SCE), available in Service Pack 4 or downloadable at ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/ SCE is a "snap-in" to the Microsoft Management Console (MMC) and is used to configure comprehensive sets of security settings that can be saved as templates and applied to individual systems.

SCE can be used to:

1. "Define a template of security configuration settings"
2. "Compare the local machine's settings against a template"
3. "Configure the local machine's settings to match a template"

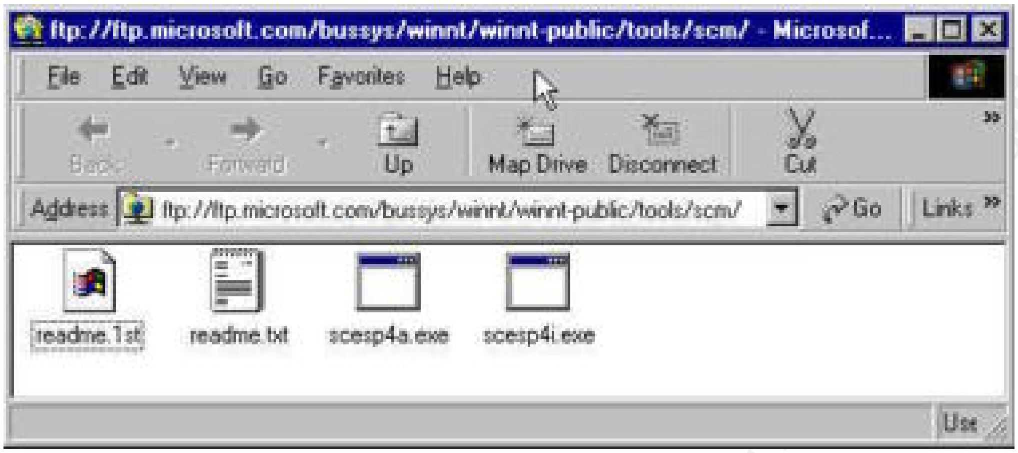
Source: Securing Windows NT Step-By-Step, Parts 1-3, by Jason Fossen and Jennifer Kolde

Risk

Using the **SCE will reduce the security risk to NT systems**. SCE also provides a simple yet effective method of managing security settings for large and complex NT networks.

Audit

If not already installed, download and install the SCE from Microsoft's website - ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/ This will install both the Microsoft Management Console (MMC) and the Security Configuration Editor (SCE).

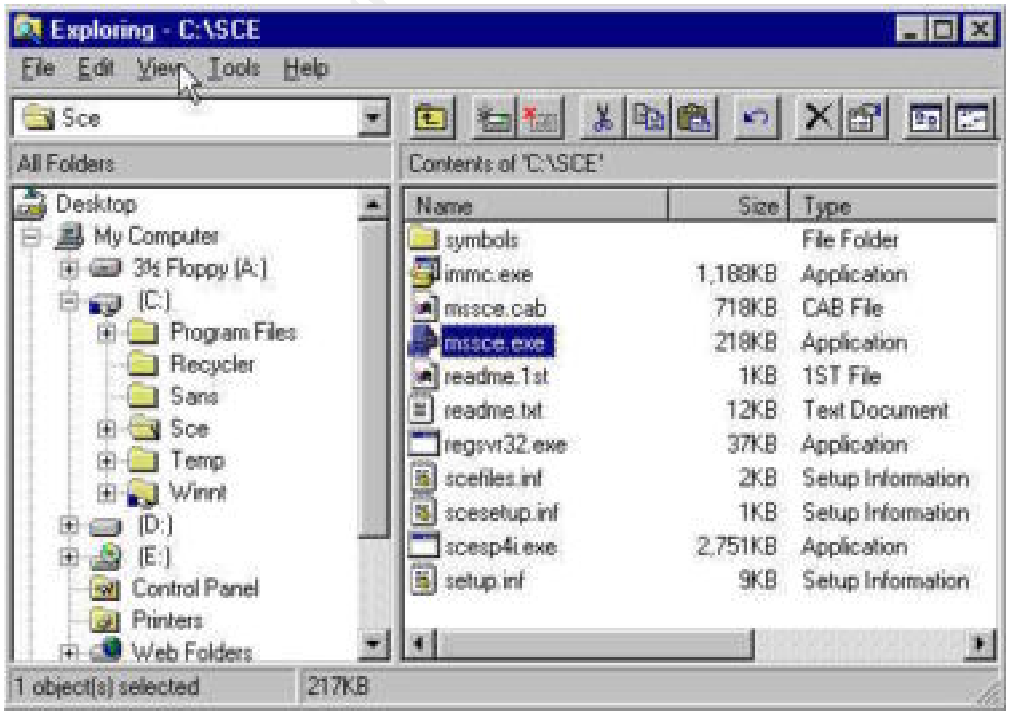

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/ - Microsof...

Address: ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/

readme.1st   readme.txt   scesp4a.exe   scesp4i.exe

To install MMC and SCE:

1. Download the "readme.txt" and "scesp4i.exe" files from the ftp site listed above. "scesp4a" is for Alpha-based systems and "scesp4i" is for i386-based systems.
2. Assuming an i386-based system, double-click on the "scesp4i.exe" file after downloading. This will extract install files into the current directory.


Exploring - C:\SCE

All Folders: Desktop, My Computer, 3½ Floppy (A:), (C:), Program Files, Recycler, Sans, Sce, Temp, Winnt, (D:), (E:), Control Panel, Printers, Web Folders

Contents of 'C:\SCE'

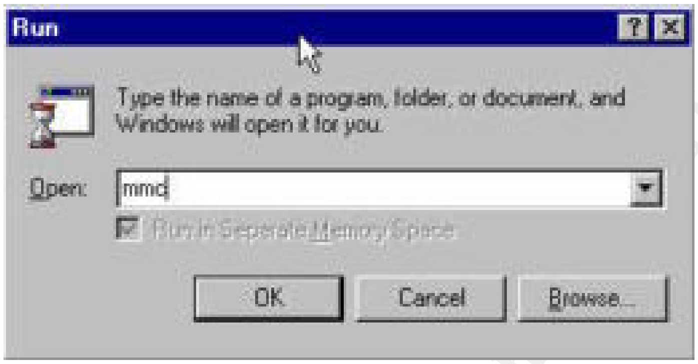
Name	Size	Type
symbols		File Folder
immc.exe	1,188KB	Application
mssce.cab	718KB	CAB File
mssce.exe	218KB	Application
readme.1st	1KB	1ST File
readme.txt	12KB	Text Document
regsvr32.exe	37KB	Application
scefiles.inf	2KB	Setup Information
scesetup.inf	1KB	Setup Information
scesp4i.exe	2,751KB	Application
setup.inf	9KB	Setup Information

1 object(s) selected   217KB

3. Double-click on the “mssce.exe” file and follow directions to complete the install process.

To start MMC:

1. Go to Start -> Run…
2. Type in “mmc” to invoke the Microsoft Management Console

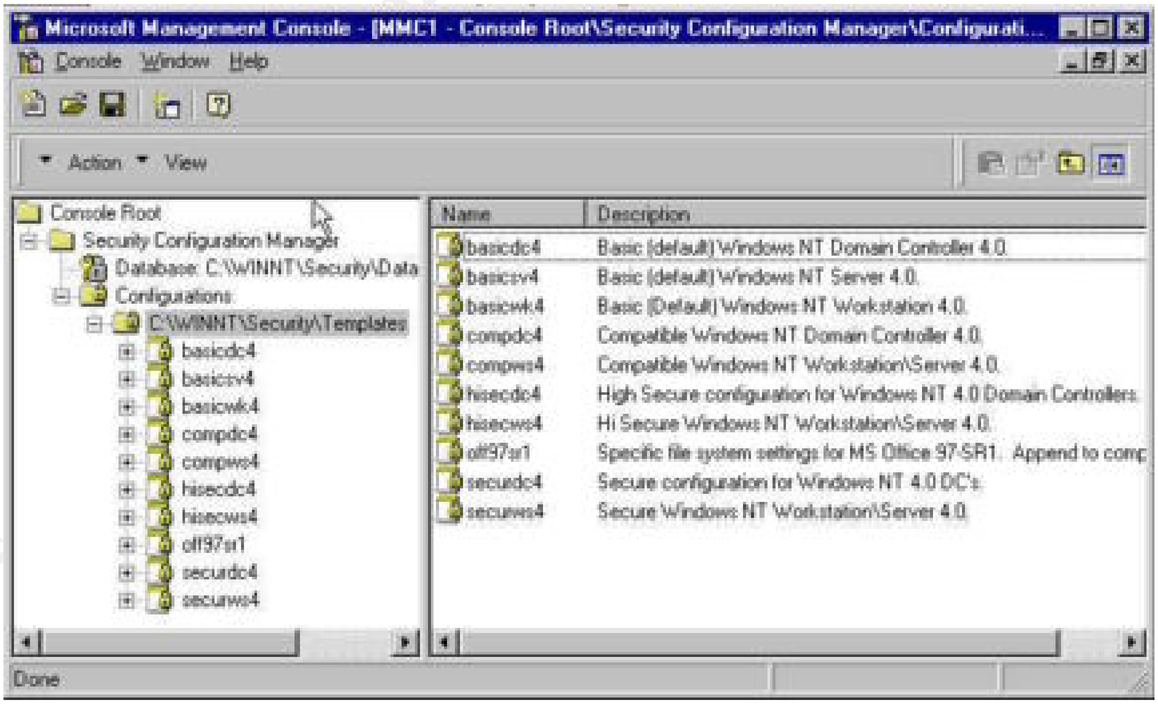


Type the name of a program, folder, or document, and Windows will open it for you.

Open: mmc

☑ Run in Seperate Memory Space

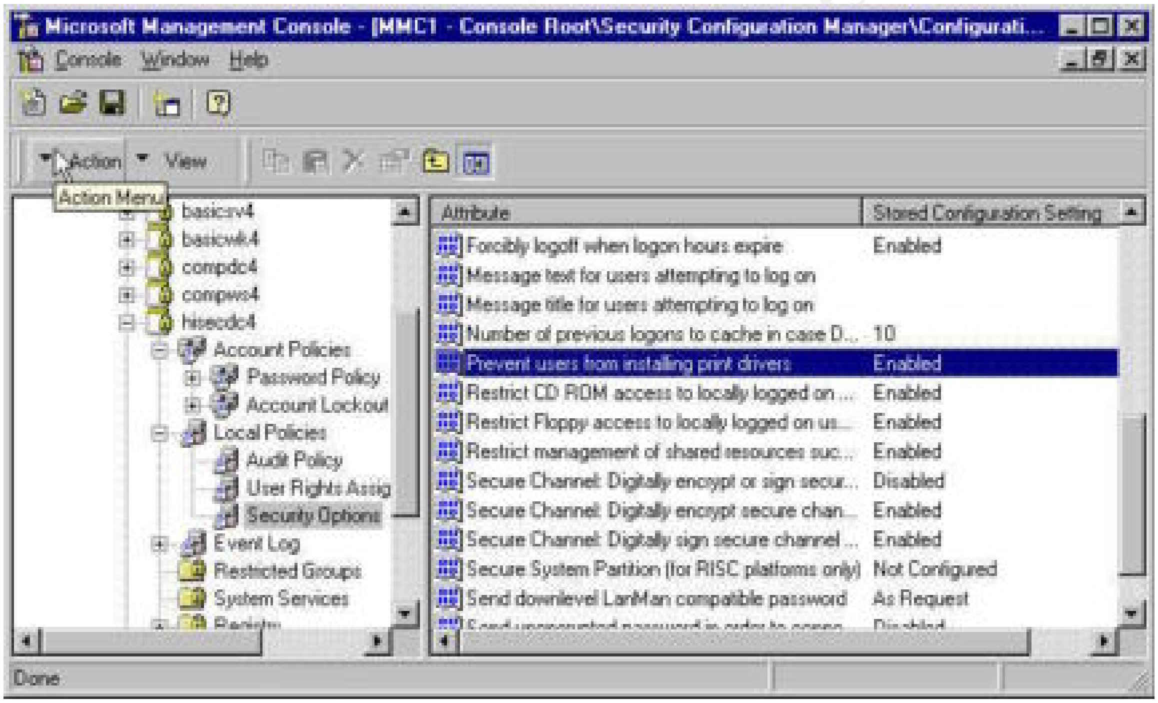
3. Within the MMC window, select Console -> Add/Remove Snap-In -> Add… -> Security Configuration Manager -> OK


Microsoft Management Console - [MMC1 - Console Root\Security Configuration Manager\Configurati...
Console
Window
Help
Action
View
Done

```
Console Root
⊟ Security Configuration Manager
    Database: C:\WINNT\Security\Data
  ⊟ Configurations
    ⊟ C:\WINNT\Security\Templates
      ⊞ basicdc4
      ⊞ basicsv4
      ⊞ basicwk4
      ⊞ compdc4
      ⊞ compws4
      ⊞ hisecdc4
      ⊞ hisecws4
      ⊞ off97sr1
      ⊞ securdc4
      ⊞ securws4
```

Name	Description
basicdc4	Basic (default) Windows NT Domain Controller 4.0.
basicsv4	Basic (default) Windows NT Server 4.0.
basicwk4	Basic (Default) Windows NT Workstation 4.0.
compdc4	Compatible Windows NT Domain Controller 4.0.
compws4	Compatible Windows NT Workstation\Server 4.0.
hisecdc4	High Secure configuration for Windows NT 4.0 Domain Controllers
hisecws4	Hi Secure Windows NT Workstation\Server 4.0.
off97sr1	Specific file system settings for MS Office 97-SR1. Append to comp
securdc4	Secure configuration for Windows NT 4.0 DC's.
securws4	Secure Windows NT Workstation\Server 4.0.

From this menu, you can choose a basic security template for which to model for your specific configuration. Templates can be created, modified, and implemented all within this menu. Comparisons between the current system settings and a template can also be achieved. The Security Configuration Editor also has a command-line interface to facilitate batch jobs for large NT networks. SCE provides a comprehensive set of security settings that can be centrally produced and distributed accordingly. Here is a small snap-shot on the types of settings that can be modified:



Attribute	Stored Configuration Setting
Forcibly logoff when logon hours expire	Enabled
Message text for users attempting to log on	
Message title for users attempting to log on	
Number of previous logons to cache in case D...	10
Prevent users from installing print drivers	Enabled
Restrict CD ROM access to locally logged on ...	Enabled
Restrict Floppy access to locally logged on us...	Enabled
Restrict management of shared resources suc...	Enabled
Secure Channel: Digitally encrypt or sign secur...	Disabled
Secure Channel: Digitally encrypt secure chan...	Enabled
Secure Channel: Digitally sign secure channel ...	Enabled
Secure System Partition (for RISC platforms only)	Not Configured
Send downlevel LanMan compatible password	As Request
Send unencrypted password in order to conne...	Disabled

Note: **A comprehensive security policy must be in place prior to implementing any of the SCE templates as configurations within these templates directly relate to security policies. Templates should also be thoroughly tested on non-production environments prior to implementation.**

Works Cited

Fossen, Jason and Jennifer Kolde. Securing Windows NT Step-By-Step, Parts 1-3. The SANS Institute – Network Security 2000, Monterey, CA

Frisch, Aeleen, et. al. Essential Windows NT System Administration. Sebastopol: O'Reilly & Associates, 1998.

Heckendorn, Sherri. GCNT Certification Submission, **http://www.sans.org/giactc/gcnt.htm** Analyst Number 0016 Sherri_Heckdorn.doc

McClure, Stuart; Scambray, Joel; Kurtz, George. Hacking Exposed, Network Security Secrets and Solutions. Berkeley: Osborne/McGraw-Hill, 1999.

Nielsen, Andrew Kjell. GCNT Certification Submission, **http://www.sans.org/giactc/gcnt.htm** Analyst Number 0013 andrewnielsen.doc

SANS Institute. Windows Security Step by Step, Version 2.15, July 30, 1999. The SANS Institute, 1999.

"How to Obtain the Latest Windows NT 4.0 Service Pack.", Microsoft Knowledge Base Article ID: Q152734