GIAC Certified Windows NT Security Analyst

Practical Assignment for

SANS Network Security 2000 at

Monterey, California

submitted by Michael Hom on

November 22, 2000

Introduction

This SANS Practical Assignment is designed to meet the requirements of the SANS Certified GIAN NT/2000 Security Analyst. In this assignment, methods to audit a Windows NT 4.0 Domain Controller are developed. Note that this audit is not comprehensive although some of the more important topics are covered.

The steps outlined were meant to allow a system in production to be audited with minimal intrusion. Third party tools were not used. The GUI interface was used as much as possible thus more steps might be taken to audit a particular item.

Auditor's remarks were italicized and colored blue

Service Pack Version

Background: Security and functional patches are bundled into Service Packs to provide convenient updates to Windows NT 4.0. “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. All are conveniently bundled for easy downloading. Service packs are cumulative -- each new service pack contains all the fixes in previous service packs, as well as any new fixes.” (Microsoft KB Q152734)

Risk: Exposure to widely known security and functional vulnerabilities, such as Denial of Service attacks, are left unfixed, if the current service pack is not installed.

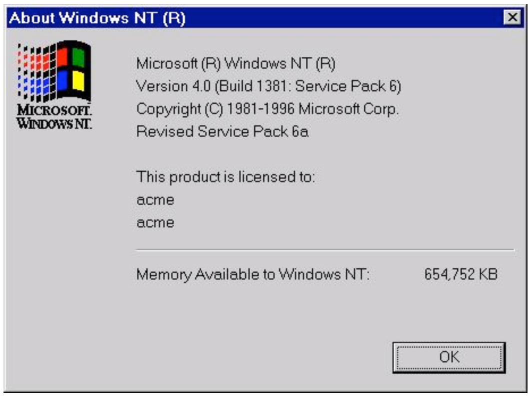
Policy: Once a new service pack is released, test in a non-production environment for a minimum of two months. If the Service Pack is stable and compatible with OS and applications, then deploy. Current policy is to deploy Service Pack 6a with strong (128-bit) encryption. In addition, no post-SP6a hotfixes are mandated.

File (40/56-bit version)	**Directory**	**Description**
Ndiswan.sys	%systemdirectory%\drivers	MS WAN Wrapper Network Driver (Export Version)
Ntlmssps.dll	%systemdirectory%	NtLm Security Support Provider Service DLL (ExportVersion)
(Rsaenh.dll) doesn’t exist		doesn’t exist
Schannel.dll	%systemdirectory%	TLS / SSL Security Provider (Export Version)
Security.dll	%systemdirectory%	NtLm Security Support Provider Client DLL (ExportVersion)
File (128-bit version)	**Directory**	**Description**
Ndiswan.sys	%systemdirectory%\drivers	MS WAN Wrapper Network Driver (Domestic Use Only)
Ntlmssps.dll	%systemdirectory%	NtLm Security Support Provider Service DLL (DomesticUse Only)
Rsaenh.dll	%systemdirectory%	Microsoft Enhanced Cryptographic Provider (US/CanadaOnly, Not for Export)
Schannel.dll	%systemdirectory%	TLS / SSL Security Provider (US and Canada Use Only)
Security.dll	%systemdirectory%	NtLm Security Support Provider Client DLL (DomesticUse Only)

Table 1: File description of 40/56-bit and 128-bit Service Pack files.

Validation:

1. From the Windows NT desktop, click Start, and then click Run.
2. Type "winver" in the Open box and click OK.
3. An About box appears, which lists the service pack version.



About Windows NT (R)

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

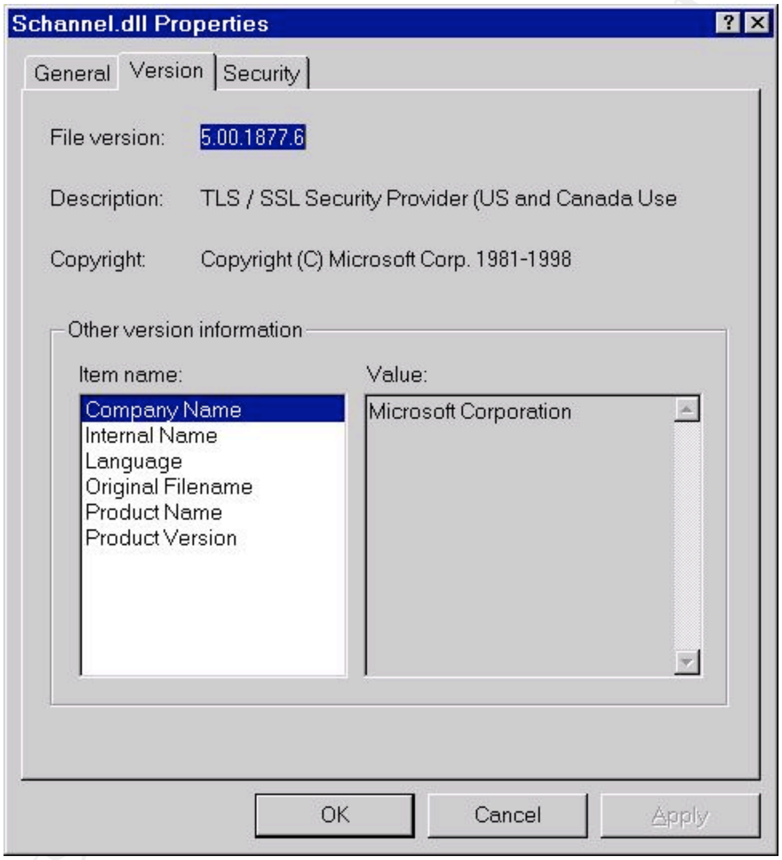
This product is licensed to:
acme
acme

Memory Available to Windows NT: 654,752 KB

Figure 1: About box reveals Service Pack version 6a installed.

Steps to verify the installation of the strong (128-bit) encryption version of the Service Pack:

4. Click Start, point to Find, and then click Files Or Folders.
5. In the Named box, type "schannel.dll", and then click Find Now.
6. In the list of files, right-click the Schannel.dll file, and then click Properties.
7. Click the Version tab. Compare Description to table above.
8. Check with System Administrator if procedures are established to reinstall the Service Pack if system configuration changes.



File version: 5.00.1877.6

Description: TLS / SSL Security Provider (US and Canada Use

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

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

Figure 2: Properties window for Schannel.dll shows description of strong encryption.

Validation	**Policy**	***"ACME"***	***Comment***
Service Pack version	SP 6a	*SP 6a*	*pass*
128-bit version of Service Pack	128-bit	*128-bit version*	*pass*

In additon to the work done by Clyde D'Souza, the 128-bit version of the Service Pack was checked.

System "ACME" has met policy requirements. System Administrator stated that procedures exist to reinstall Service Pack if system configuration changes.

Note: The steps above will also determine if you are running the 128-bit version of Internet Explorer. (Microsoft KB Q164539)

Account Policy

Background: Within User Manager, account requirements can be set and enforced for all accounts within a domain. In addition, password length can be set, but no options within User Manager are available to set password complexity.

Risk: Without a strong account policy implemented in User Manager, vulnerabilities in user accounts as well as administrator accounts can provide opportunity for unauthorized access.

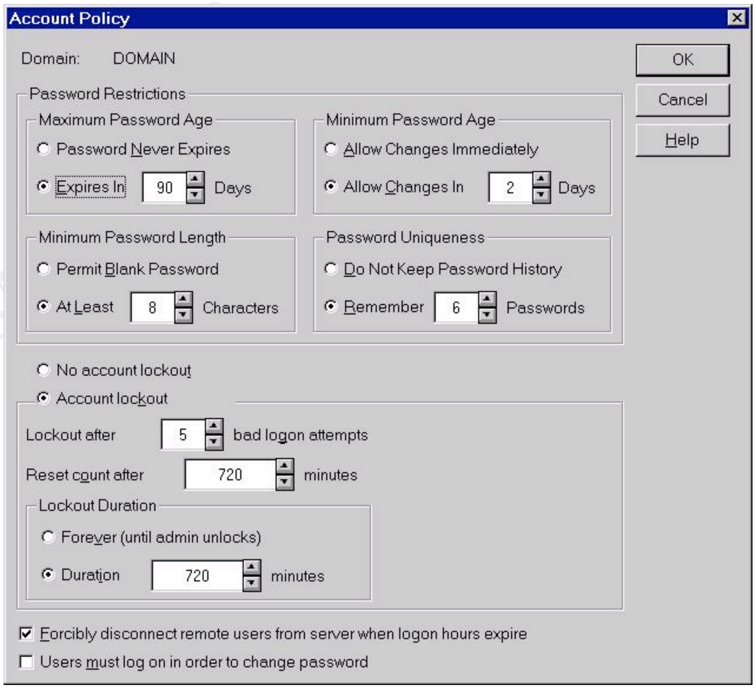
Policy: Account Policy is stated below.

Account Parameters	**Policy**
Maximum Password Age	90 days
Minimum Password Age	1 day
Minimum Password Length	8 characters
Password Uniqueness History	8 passwords
Account Lockout Count	5
Lockout Duration	240 minutes
Reset Account Lockout Count After	15 minutes
Forcibly Disconnect Remote User from Server when Logon Hours Expire	enable
Users Must Logon to Change Password	disable

Table 2: Account Policy

Validation:

1. Go to Start -> Programs -> Administrative Tools -> User Manager.
2. Within User Manager, go to Policies -> Account.
3. Compare the Account Policy settings with the stated policy.



Domain: DOMAIN

Password Restrictions

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

Minimum Password Age
○ Allow Changes Immediately
● Allow Changes In 2 Days

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

Password Uniqueness
○ Do Not Keep Password History
● Remember 6 Passwords

○ No account lockout
● Account lockout

Lockout after 5 bad logon attempts
Reset count after 720 minutes

Lockout Duration
○ Forever (until admin unlocks)
● Duration 720 minutes

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

Figure 3: Account Policy for a domain.

Account Parameters	**Policy**	***ACME***	***Comment***
Maximum Password Age	90 days	*90 days*	*pass*
Minimum Password Age	1 day	*2 days*	*exceeded*
Minimum Password Length	8 characters	*8 characters*	*pass*
Password Uniqueness History	8 passwords	*6 passwords*	*didn't pass*
Account Lockout Count	5	*5*	*pass*
Lockout Duration	240 minutes	*720 minutes*	*exceeded*
Reset Account Lockout Count After	15 minutes	*720 minutes*	*exceeded*
Forcibly Disconnect Remote User when Expired	enable	*enabled*	*pass*
Users Must Logon to Change Password	disable	*disabled*	*pass*

Acme server exceeded policy requirements in Minimum Password Age, Lockout Duration, and Reset Account Lockout Count After. Acme did not pass on the parameter Password Uniqueness History. Noted to the System Administrator to change the setting for Password Uniqueness History from 6 to 8.

Password Policy

Background: Account Policy within User Manager can enforce minimum password length but not password complexity. PASSFILT can enforce increased password complexity by requiring categories of characters, such as uppercase, lowercase, number, or non-alphanumeric, as part of the password policy.

Risk: User password policy must be strong to protect against "password guessing" and "dictionary attacks". Otherwise, user accounts as well as administrator accounts are vulnerable to password cracking tools.

Policy: Use the PASSFILT functionality. The passwords must be at least six (6) characters long and must contain characters from at least three (3) of the following four (4) classes:

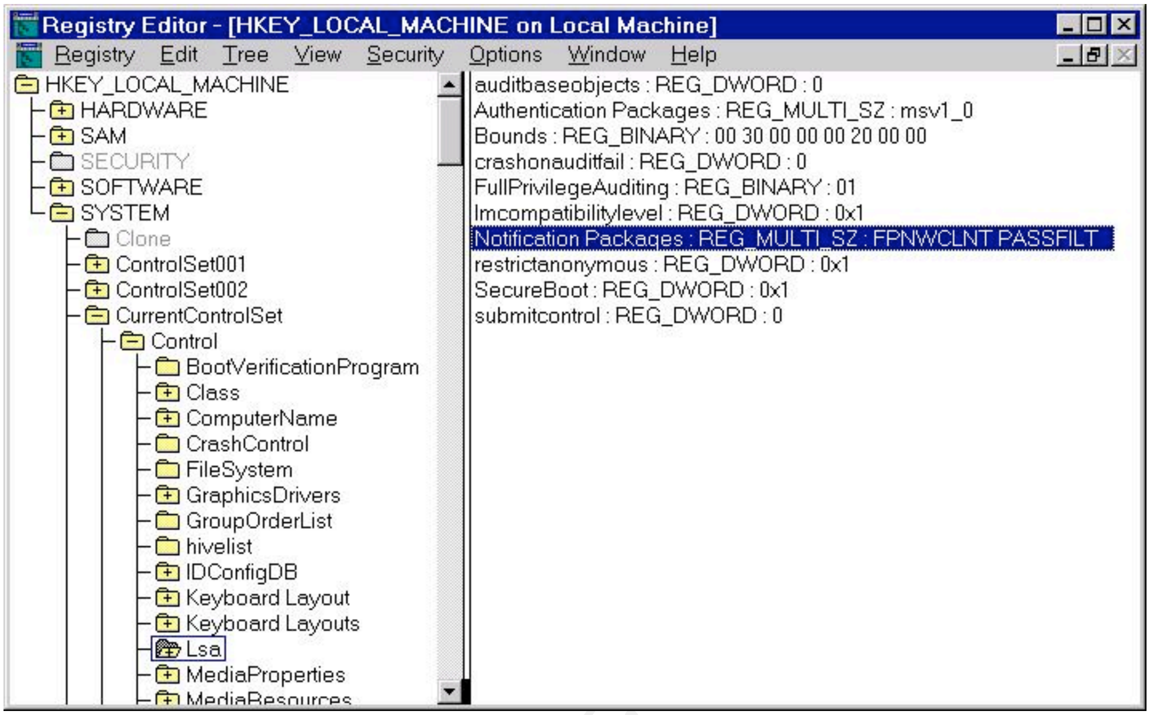
Description	**Examples**
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized Arabic numerals	0, 1, 2, ... 9
Non-alphanumeric ("special characters")	such as punctuation symbols

Table 3: PASSFILT Password Policy.

In addition, passwords may not contain your user name or any part of your full name.

Validation:

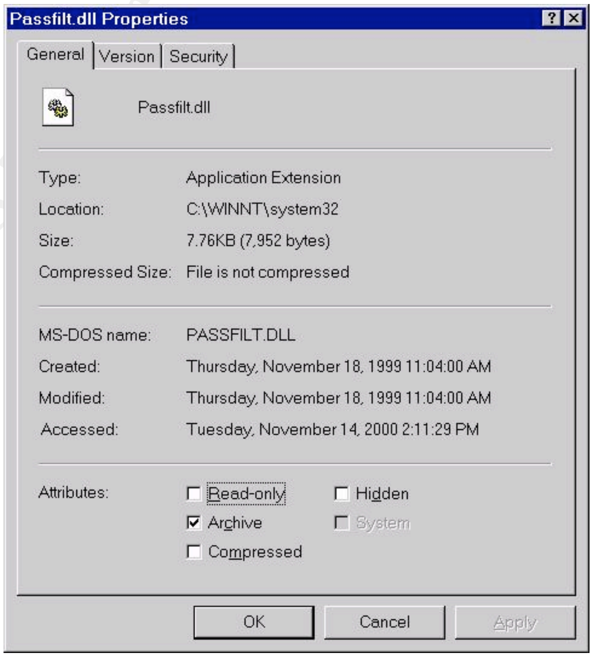
1. Click Start, click Run.
2. Start Registry, by typing "regedt32" and pressing enter.
3. Locate and click the following key in the Registry:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa.
4. Click on key "Notification Packages" and note value that includes "PASSFILT".



```
auditbaseobjects : REG_DWORD : 0
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
crashonauditfail : REG_DWORD : 0
FullPrivilegeAuditing : REG_BINARY : 01
lmcompatibilitylevel : REG_DWORD : 0x1
Notification Packages : REG_MULTI_SZ : FPNWCLNT PASSFILT
restrictanonymous : REG_DWORD : 0x1
SecureBoot : REG_DWORD : 0x1
submitcontrol : REG_DWORD : 0
```

Figure 4: Confirming PASSFILT Policy Filter within the Registry.

5. Go to Start -> Find -> Files or Folders.
6. Type "passfilt.dll" and press "Find Now".
7. Right click on "passfilt.dll" and select Properties.
8. Note that "passfilt.dll" is in the %systemdirectory% folder.



Passfilt.dll

Type: Application Extension
Location: C:\WINNT\system32
Size: 7.76KB (7,952 bytes)
Compressed Size: File is not compressed

MS-DOS name: PASSFILT.DLL
Created: Thursday, November 18, 1999 11:04:00 AM
Modified: Thursday, November 18, 1999 11:04:00 AM
Accessed: Tuesday, November 14, 2000 2:11:29 PM

Attributes: □ Read-only □ Hidden ☑ Archive □ System □ Compressed

Figure 5: Properties of Passfilt.dll that show its location at c:\winnt\system32.

First, the value "PASSFILT" was present in the key HKEY_LOCAL_MACHINE\System\ CurrentControlSet\Control\Lsa\Notification Packages. And, the file passfilt.dll resides in c:\winnt\system32. The PASSFILT configuration on "ACME" meets policy requirements.

Audit Policy

Background: Windows NT 4.0 includes built-in auditing for system and user security events. Auditing enables administrators to track security events such as resource access, logon attempts, policy changes and shutdowns or restarts of a system.

Risk: With auditing, security events can be logged for security analysis. Auditing logs provides administrators the capability to routinely analyze unauthorized activity on Windows NT 4.0.

Policy: The auditing policy is stated below.

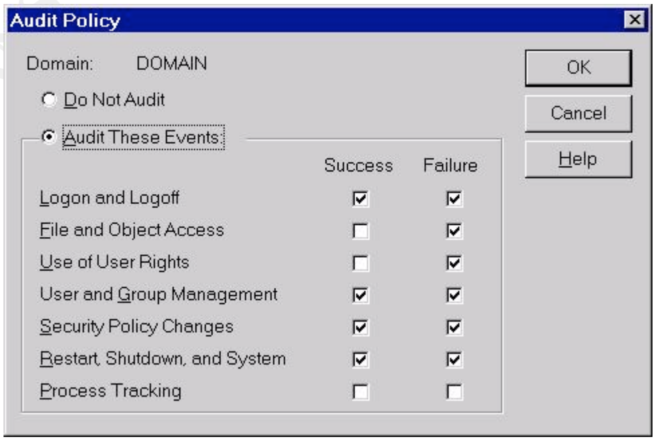
Security Events	**Policy**
Logon and Logoff	Success and Failure
File and Object Access	Failure
Use of User Rights	Failure
User and Group Management	Not Configured
Security Policy Changes	Success and failure
Restart, Shutdown, and System	Success and failure
Process Tracking	Not Configured

Table 4: Audit Policy

In addition, within the registry, setup auditing for backup and restore privileges.

Validation:

1. Go to Start -> Programs -> Administrative Tools -> User Manager.
2. On User Manager's Policies Menu, click Audit.
3. Note Audit Policy for Domain.



Domain: DOMAIN

○ Do Not Audit

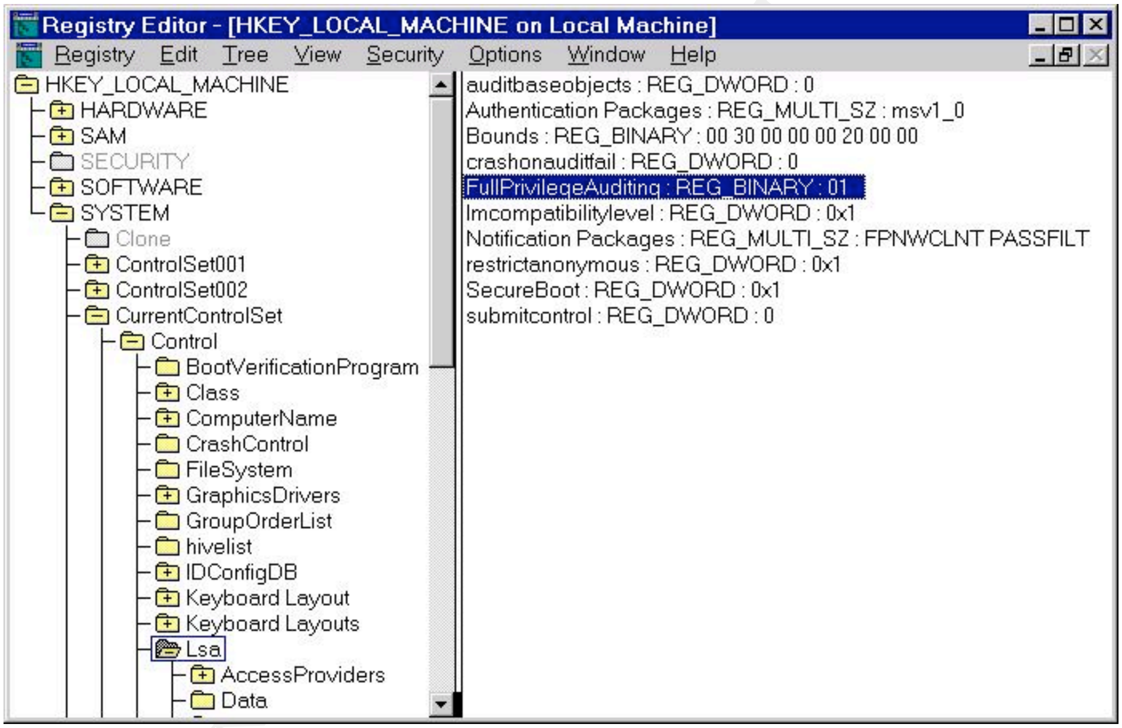
● Audit These Events:

	Success	Failure
Logon and Logoff	☑	☑
File and Object Access	□	☑
Use of User Rights	□	☑
User and Group Management	☑	☑
Security Policy Changes	☑	☑
Restart, Shutdown, and System	☑	☑
Process Tracking	□	□

Figure 6: Audit Policy on ACME.

Security Events	**Policy**	***Validation***	***Comment***
Logon and Logoff	Success and Failure	*Success and Failure*	*pass*
File and Object Access	Failure	*Failure*	*pass*
Use of User Rights	Failure	*Failure*	*pass*
User and Group Management	Not Configured	*Success and Failure*	*exceeded policy*
Security Policy Changes	Success and failure	*Success and Failure*	*pass*
Restart, Shutdown, and System	Success and failure	*Success and Failure*	*pass*
Process Tracking	Not Configured	*Not Configured*	*pass*

4. Check key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FullPrivilegeAuditing for a value of 0x01. This enables auditing of backup and restore privileges.



```
auditbaseobjects : REG_DWORD : 0
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
crashonauditfail : REG_DWORD : 0
FullPrivilegeAuditing : REG_BINARY : 01
Imcompatibilitylevel : REG_DWORD : 0x1
Notification Packages : REG_MULTI_SZ : FPNWCLNT PASSFILT
restrictanonymous : REG_DWORD : 0x1
SecureBoot : REG_DWORD : 0x1
submitcontrol : REG_DWORD : 0
```

Figure 7: Registry setting to allow auditing of backup and restore privileges.

In addition to the work done by Clyde D'Souza, auditing of backup & restore privileges were enabled.

Auditing requirements in User Manager is either meet or exceeded. In addition, backup and restore privileges are also audited.

Event Log

Background: The system, security, and application events are stored in logs that are available for analysis. Event logs contains the audit entries that may record unauthorized activity on a system.

Risk: Erasure of the event logs is a risk since intruders may attempt to delete any recorded unauthorized activities.

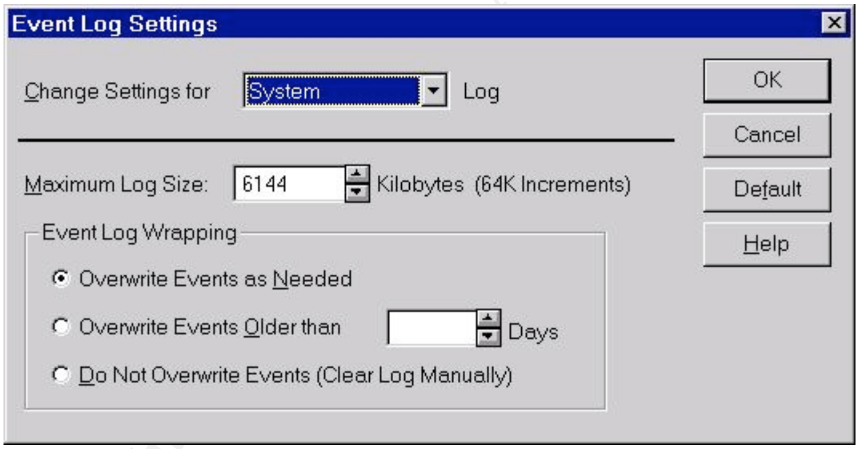
Policy:

Settings for Event Logs	**System, Security, Application Logs**
maximum log size for all logs	6144KB
event log wrapping for all logs	retain all logs for 15 days
Registry Setting	
restrict guest access to all logs (RestrictGuestAccess)	enabled (value 1)
ACL	
permissions on EVT files in %systemdirectory% folder	administrators & system have full control

Table 5: Event Log Policy

Validation:

1. Go to Start -> Programs -> Administrative Tools -> Event Viewer.
2. Click on the Log menu and select Log Settings.
3. Note settings for System, Security, and Application Logs.



Change Settings for: System Log

Maximum Log Size: 6144 Kilobytes (64K Increments)

Event Log Wrapping

● Overwrite Events as Needed

○ Overwrite Events Older than Days

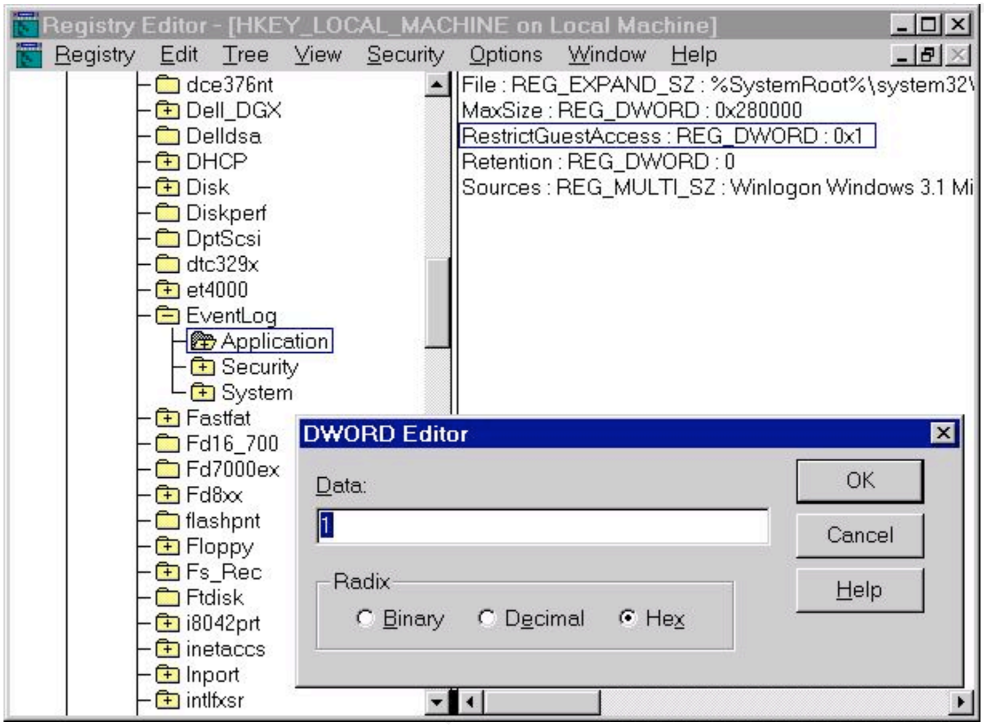
○ Do Not Overwrite Events (Clear Log Manually)

Figure 8: System Event Log Policy for ACME

Settings for Event Logs	Policy	*System*	*Security*	*Application*	*Comments*
maximum log size	6144KB	*6144KB*	*6144KB*	*6144KB*	*pass*
event log wrapping	retain all logs for 15 days	*overwrite as needed*	*overwrite as needed*	*overwrite as needed*	*didn't pass*

4. Click Start, click Run.
5. Start Registry, by typing “regedt32” and pressing enter.
6. Locate and click the following key in the Registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\EventLog\[LogName].
7. Click on key “RestrictGuestAccess” and note the value. A value of 1 will restrict guest access to the logs.
8. Go to Start -> Find -> Files or Folders.
9. Type “*.evt” and press “Find Now”. These file should be in %systemdirectory%\config.

10. Right click on appevent.evt, secevent.evt, & sysevent.evt, and select Properties for each.
11. Click the security tab and note what the file permissions are for each log file. Only administrators and system should have full access.

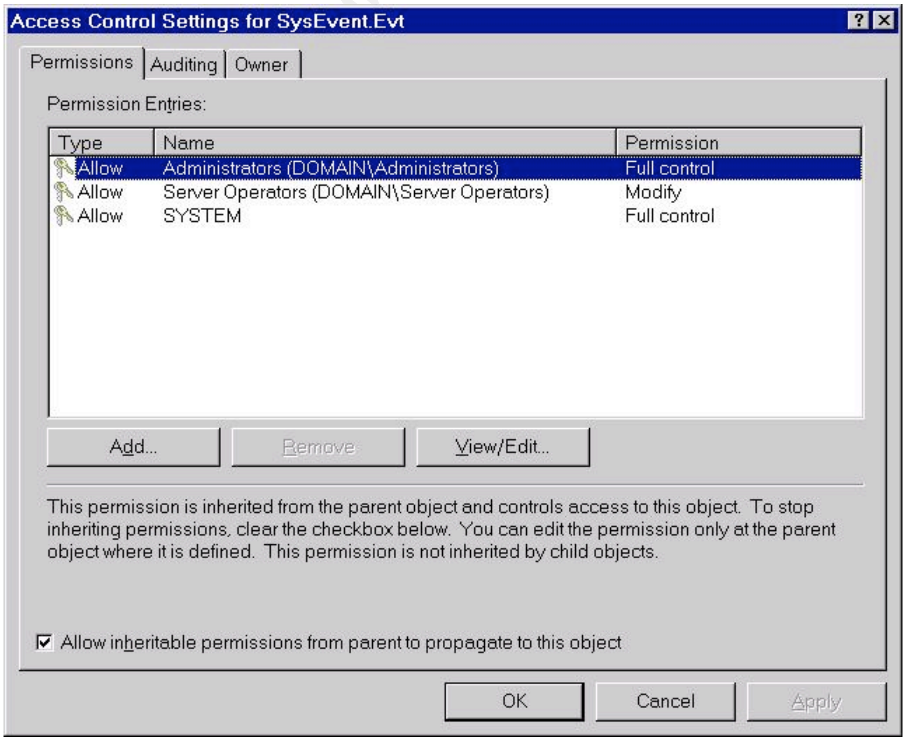


```
File : REG_EXPAND_SZ : %SystemRoot%\system32\
MaxSize : REG_DWORD : 0x280000
RestrictGuestAccess : REG_DWORD : 0x1
Retention : REG_DWORD : 0
Sources : REG_MULTI_SZ : Winlogon Windows 3.1 Mi
```

Data: 1

Radix: ○ Binary ○ Decimal ● Hex

Figure 9: On ACME, RestrictGuestAccess value is 1.



Permission Entries:

Type	Name	Permission
Allow	Administrators (DOMAIN\Administrators)	Full control
Allow	Server Operators (DOMAIN\Server Operators)	Modify
Allow	SYSTEM	Full control

This permission is inherited from the parent object and controls access to this object. To stop inheriting permissions, clear the checkbox below. You can edit the permission only at the parent object where it is defined. This permission is not inherited by child objects.

☑ Allow inheritable permissions from parent to propagate to this object

Figure 10: On ACME, File Permissions on the System Event Log.

The registry key RestrictGuestAccess is set to 1. This is disables guest access to log files. In addition, the file permissions on the event log files do not meet the policy requirements. The system administrator will have to disable inheritance and only allow administrators & system full control to sysevent.evt, secevent.evt, and appevent.evt. The settings for "event log wrapping" will also need to change to "overwrite events older than 15 days".

In addition to work done by George Stanton, additional permission restrictions were placed on the event log files.

System Key

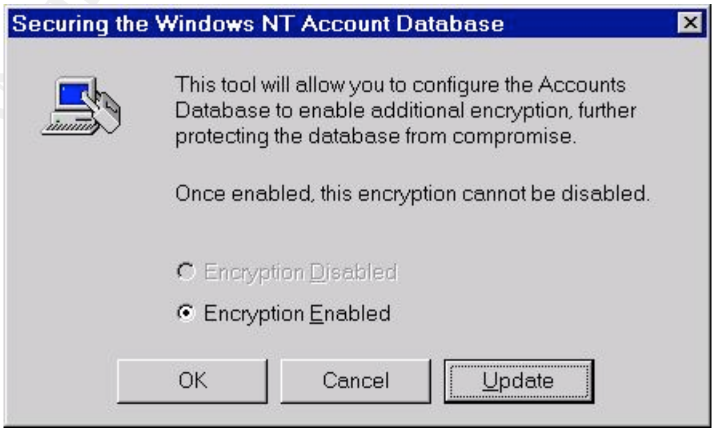
Background: Windows NT 4.0 user account and password information are contained in the Security Account Manager (SAM) database, in addition to the Emergency Repair Disk and backup tapes of the SAM. Tools, such as L0phtCrack and PWDUMP2, can extract usernames and password hashes for the purpose of password cracking. An additional layer of protection can be used by using a 128-bit cryptographic random key to encrypt the password information contained within the SAM. This feature has been incorporated into Service Pack 3 or later.

Risk: Known hacker tools can extract password information within the SAM for password cracking.

Policy: Enable SYSKEY encryption and store the Startup Key locally on each Domain Controller. The main goal to is prevent unauthorized users from extracting password information, yet not restricting unattended reboots. In addition install SYSKEY update from Microsoft's KB Q248183

Validation:

1. Click Start, click Run.
2. Type "syskey" and press enter.
3. If the System Key is enabled, then the option "Encryption Disable" is grayed out and the option "Encryption Enabled" is permanently selected.



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.

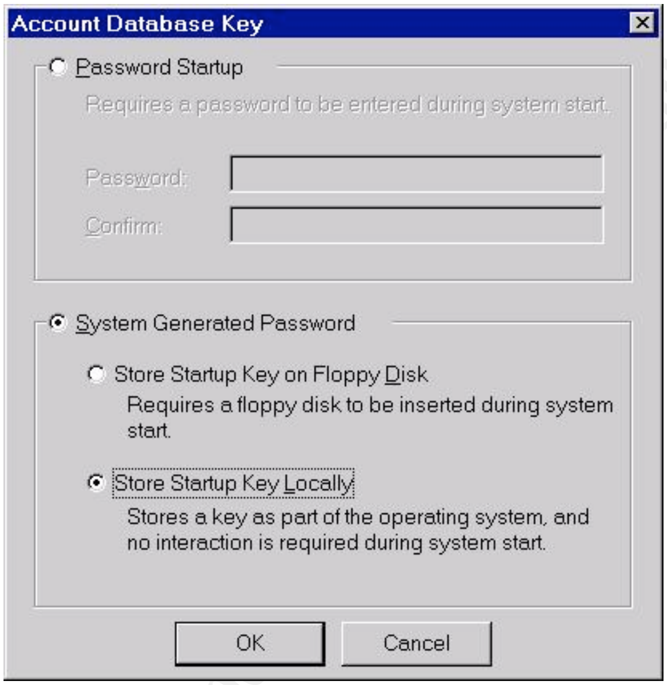
Once enabled, this encryption cannot be disabled.

○ Encryption Disabled

● Encryption Enabled

Figure11: System key is enabled on ACME.

4. To determine where the Startup Key is stored, continue on by pressing “Update” and view which option is selected.
5. The options “System Generated Password” and “Store Startup Key Locally” should be selected.
6. Advanced Options other than “Store Startup Key Locally” exceeds stated policy.



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.

Figure 11: SYSKEY is shown to be stored locally on ACME.

All policy requirements for SYSKEY have been met. The SYSKEY update was validated.

Update: From Microsoft’s KB Q248183 - Syskey Tool Reuses Keystream

“A cryptographic error in the Syskey tool makes offline password attacks easier than previously believed. Syskey reuses keystream when encrypting certain elements in the Security Accounts Manager (SAM) database, making the tool vulnerable to an attack using a known cryptanalytic method. This vulnerability could allow offline password attacks to be mounted against a Syskey-protected SAM database.”

Microsoft KB article Q248183, Syskey Utility Reuses Keystream is located at:
http://support.microsoft.com/support/kb/articles/q248/1/83.asp

The Microsoft Security Bulletin MS99-056 is located at:
http://www.microsoft.com/technet/security/bulletin/ms99-056.asp

The Patch for MS99-056 is located at:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=16798

Check the following:

Date	**Time**	**Size**	**File name**	**Platform**	***Comment***
12/06/1999	06:52p	155,408	Lsasrv.dll	x86	*pass*
12/06/1999	06:53p	174,352	Samsrv.dll	x86	*pass*

Table 6: Updated SYSKEY file from Microsoft KB Q248183

In additon to the work done by George Stanton, the SYSKEY Q248183 was checked.

NTLMv2 Authentication

Background: Starting with Service Pack 4 or later, the NTLMv2 feature was to improve authentication and session security mechanisms. “Recent improvements in computer hardware and software algorithms have made these protocols vulnerable to widely published attacks for obtaining user passwords. In its ongoing efforts to deliver more secure products to its customers, Microsoft has developed an enhancement, called NTLM version 2, that significantly improves both the authentication and session security mechanisms. NTLM 2 has been available for Windows NT 4.0 since Service Pack 4 (SP4) was released, and it is supported natively in Windows 2000. You can add NTLM 2 support to Windows 95 and Windows 98 by installing the Directory Services Client from the Windows 2000 CD-ROM.” (Microsoft KB Q239869)

Risk: With tools like L0phtCrack, authentication sessions sending across password hashes could be sniffed off the network. Microsoft provided NTLMv2 to fix this security vulnerability.

Policy: A phased approach to NTLMv2 is currently taken. Use level 1 for year 2000/1 for backwards compatibility with existing Windows 95/98 workstations that do not have Directory Services Client installed. In addition, any new Windows 95/98 workstations will be configured with the Directory Services Client which will be compatible with NTLMv2.

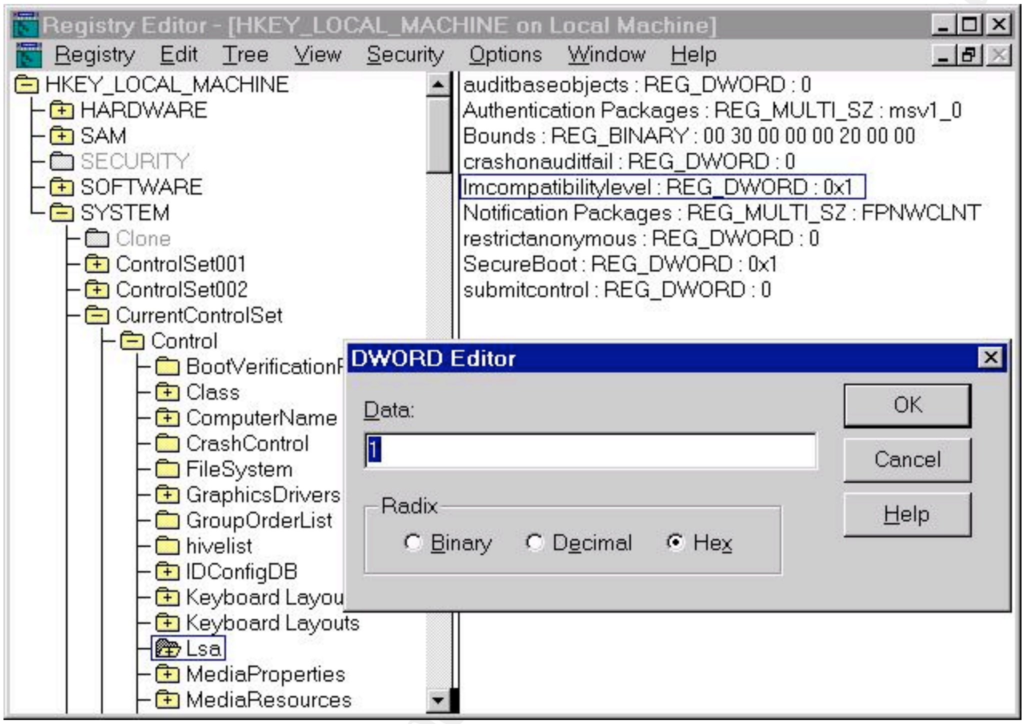
LMCompatibilityLevel values	**Description of LMCompatibilityLevel value**
Level 0	Send LM and NTLM response; never use NTLM 2 session security. Clients use LM and NTLM authentication, and never use NTLM 2 session security; domain controllers accept LM, NTLM, and NTLM 2 authentication.
Level 1	Use NTLM 2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.
Level 2	Send NTLM response only. Clients use only NTLM authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.
Level 3	Send NTLM 2 response only. Clients use NTLM 2 authentication, and use NTLM 2 session security if the server supports it; domain controllers accept LM, NTLM, and NTLM 2 authentication.
Level 4	Domain controllers refuse LM responses. Clients use NTLM 2 authentication, and use NTLM 2 session security if the server supports it; domain controllers refuse LM authentication (that is, they accept NTLM and NTLM 2).
Level 5	Domain controllers refuse LM and NTLM responses (accept only NTLM 2). Clients use NTLM 2 authentication, use NTLM 2 session security if the server supports it; domain controllers refuse NTLM and LM authentication (they accept only NTLM 2).

Table 7: Registry Key LMCompatibility values and description from Microsoft KB Q239869

Validation:

1. Click Start, click Run.

2. Start Registry, by typing “regedt32” and pressing enter.
3. Locate and click the following key in the Registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa.
4. Click on key “lmcompatibilitylevel and note value.



```
auditbaseobjects : REG_DWORD : 0
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
crashonauditfail : REG_DWORD : 0
lmcompatibilitylevel : REG_DWORD : 0x1
Notification Packages : REG_MULTI_SZ : FPNWCLNT
restrictanonymous : REG_DWORD : 0
SecureBoot : REG_DWORD : 0x1
submitcontrol : REG_DWORD : 0
```

Data: 1

Radix ○ Binary ○ Decimal ● Hex

Figure 12: Registry Key LMCompatibility shown to have a value of 1.

NTLMv2 configuration meets policy as shown by the key LMCompatibility’s value of 1.

FYI: “The Directory Services Client is included on the Windows 2000 CD-ROM as Clients\Win9x\Dsclient.exe. When you run Dsclient.exe is run on a Windows 95/98 computer, the system files that provide NTLM 2 support are automatically installed as well. These files are Secur32.dll, Msnp32.dll, Vredir.vxd, and Vnetsup.vxd. If you uninstall Dsclient, the NTLM 2 system files are not removed because they provide both enhanced security functionality and security-related fixes. (Microsoft KB Q239869)

NetLogon Channel

Background: NetLogon allows communication, like pass-through authentication and synchronization of user accounts, to occur within an Windows NT domain. Although information passed, such as computer account password, is encrypted, other data sent over the NetLogon channel lacks integrity checking. With Windows NT 4.0 Service Pack 4 or later, the NetLogon channel can be configured for encryption and digitally signature.

Risk: Unsecured NetLogon communication is vulnerable to packet sniffing and man-in-the-middle attacks.

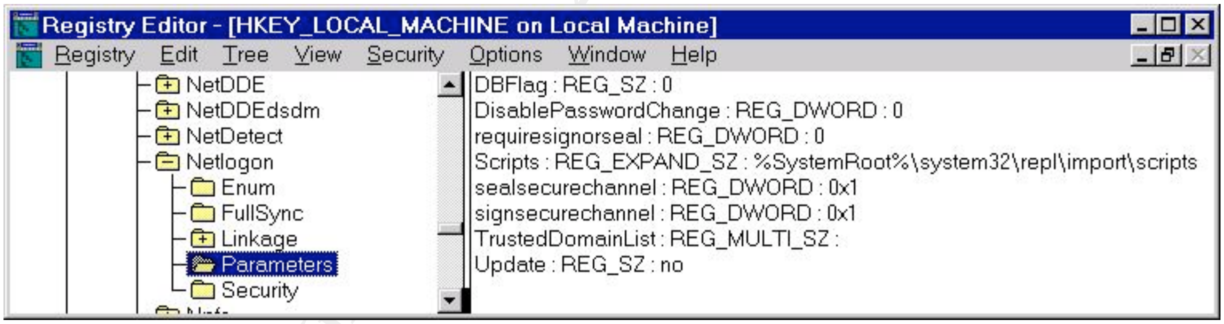
Policy: Policy set for a secure NetLogon Channel is…

Key	Valid Range	Description
SignSecureChannel	0 (FALSE) or 1 (TRUE) Default: TRUE **Policy: TRUE**	This parameter specifies that all outgoing secure channel traffic should be signed. If SealSecureChannel is also TRUE, it will override any setting for this parameter and force it to TRUE.
SealSecureChannel	0 (FALSE) or 1 (TRUE) Default: TRUE **Policy: TRUE**	This parameter specifies that all outgoing secure channel traffic should be encrypted.
RequireSignOrSeal	0 (FALSE) or 1 (TRUE) Default: FALSE **Policy: FALSE**	This parameter specifies that all outgoing secure channel traffic must be either signed or sealed. Without this parameter, this is negotiated with the Domain Controller. This flag should only be set if ALL of the domain controllers in ALL the trusted domains support signing and sealing. If this parameter is TRUE, SignSecureChannel is implied to be TRUE.

Table 8: Description of Secure NetLogon Channel Configuration.

Validation:

1. Click Start, click Run.
2. Start Registry, by typing "regedt32" and pressing enter.
3. Locate and click the following key in the Registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetLogon\Parameters.
4. Note values for keys SignSecureChannel, SealSecureChannel, and RequireSignOrSeal.



```
DBFlag : REG_SZ : 0
DisablePasswordChange : REG_DWORD : 0
requiresignorseal : REG_DWORD : 0
Scripts : REG_EXPAND_SZ : %SystemRoot%\system32\repl\import\scripts
sealsecurechannel : REG_DWORD : 0x1
signsecurechannel : REG_DWORD : 0x1
TrustedDomainList : REG_MULTI_SZ :
Update : REG_SZ : no
```

Figure 13: Secure NetLogon Configuration on ACME.

Key	Policy	*ACME*	*Comment*
SignSecureChannel	1 (TRUE)	*1 (TRUE)*	*Pass*
SealSecureChannel	1 (TRUE)	*1 (TRUE)*	*Pass*
RequireSignOrSeal	0 (FALSE)	*0 (FALSE)*	*Pass*

NetLogon configuration meets policy requirements.

Logon Banner & Don't Display Last User

Background: A Logon Banner can be displayed prior to logging on. This can provide the opportunity to warn users against unauthorized activity.

In addition, Windows NT 4.0 displays the last user logged on. This can be changed where no username is display, thus requiring a user to manually enter a username and password for each logon.

Risk: Legal action may not be successful against unauthorized access if a logon banner is not displayed to warn any user.

Policy: The policy is to display a logon banner and require a user to manually enter a username and password for authentication. The logon banner will state…

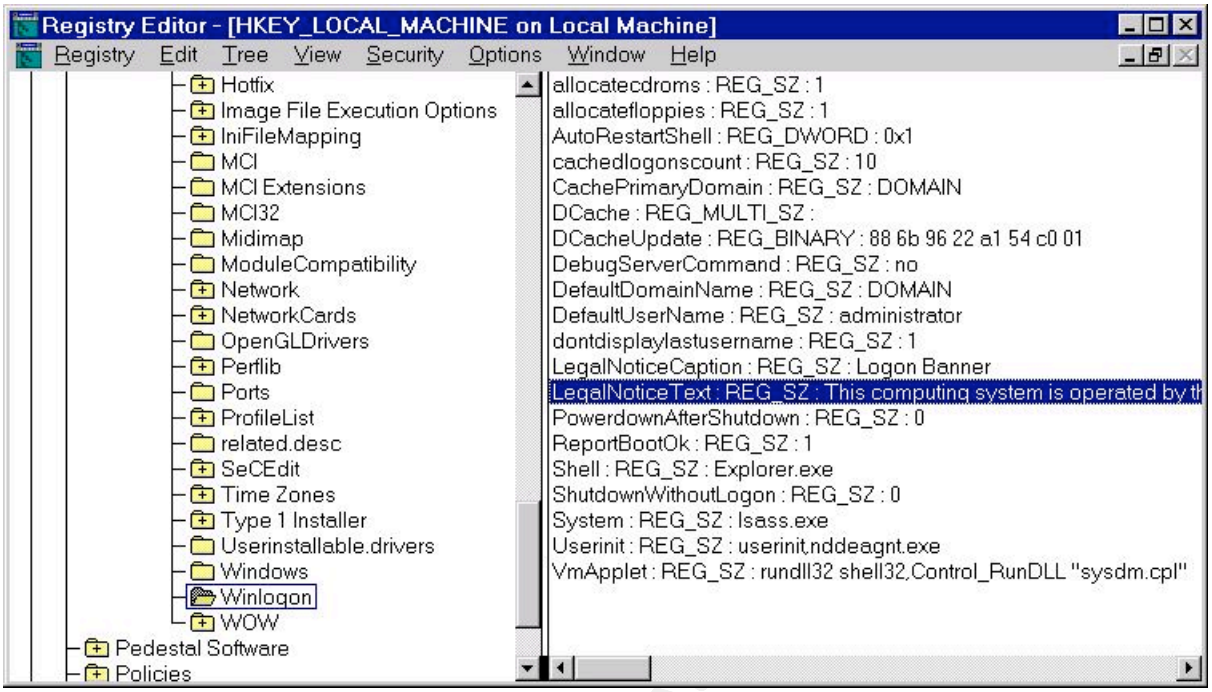
"This computing system is operated by this Company and is for official use only. Unauthorized access, unauthorized attempted access, or unauthorized use of this computing system is a violation of State Penal Code and/or applicable Federal Law, and may be subject to prosecution. Individuals using this computing system without authority, or in excess of their authority, are subject to having their activities on this system monitored and recorded by system personnel. In the course of such monitoring, or in the course of system maintenance or trouble shooting, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, further legal action may be taken."

The default setting displays the last logged user on Windows NT 4.0. This setting is to be changed so that the last user is not displayed. When a user logs in, the user will have to manually enter both the username and password.

Validation:

1. Start Regedt32.exe and locate the following registry key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
2. Note values for LegalNoticeText and DontDisplayLastUserName.

Registry Key	Policy	*ACME*	*Comment*
DontDisplayLastUserName	1	*1*	*pass*
LegalNoticeCaption	text entered	*text entered*	*pass*
LegalNoticeText	stated above	*same as text above*	*pass*



```
allocatecdroms : REG_SZ : 1
allocatefloppies : REG_SZ : 1
AutoRestartShell : REG_DWORD : 0x1
cachedlogonscount : REG_SZ : 10
CachePrimaryDomain : REG_SZ : DOMAIN
DCache : REG_MULTI_SZ :
DCacheUpdate : REG_BINARY : 88 6b 96 22 a1 54 c0 01
DebugServerCommand : REG_SZ : no
DefaultDomainName : REG_SZ : DOMAIN
DefaultUserName : REG_SZ : administrator
dontdisplaylastusername : REG_SZ : 1
LegalNoticeCaption : REG_SZ : Logon Banner
LegalNoticeText : REG_SZ : This computing system is operated by th
PowerdownAfterShutdown : REG_SZ : 0
ReportBootOk : REG_SZ : 1
Shell : REG_SZ : Explorer.exe
ShutdownWithoutLogon : REG_SZ : 0
System : REG_SZ : lsass.exe
Userinit : REG_SZ : userinit,nddeagnt.exe
VmApplet : REG_SZ : rundll32 shell32,Control_RunDLL "sysdm.cpl"
```

Figure 14: ACME Registry settings on Legal Notice and Displaying Last Username.

System ACME passed policy requirements. Also checked banner and logon window by actually logging onto ACME.

Restrict Remote Access to NT Registry

Background: Remote Registry access is controlled by the permissions on HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg.

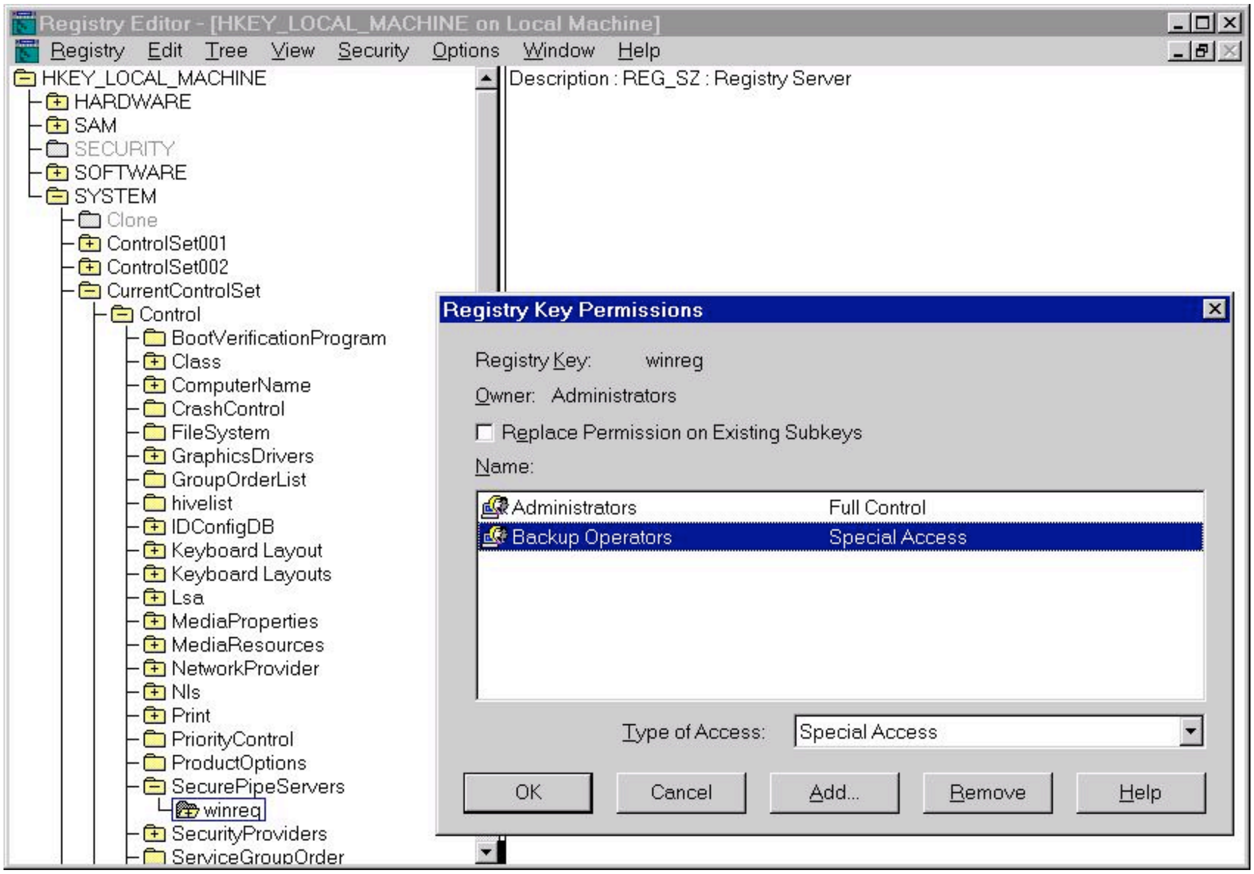
Risk: Permissions on "winreg" needed to be carefully configured since access to the Registry from a remote location can be a vulnerability.

Policy: Permissions on "winreg" are to be Administrator (full control) and Backup Operator (read + set value + create subkey).

Validation:

1. Start Registry Editor (Regedt32.exe) and go to the following key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers.
2. Click on key "winreg".
3. Select the Security menu and choose Permissions.
4. Note Permissions for key "winreg".

Permissions on key "winreg" meet state policy requirements.



Description : REG_SZ : Registry Server

Registry Key: winreg

Owner: Administrators

□ Replace Permission on Existing Subkeys

Name:

Administrators	Full Control
Backup Operators	Special Access

Type of Access: Special Access

Figure 15: ACME's Permission Settings for Key "winreg".

Null Sessions

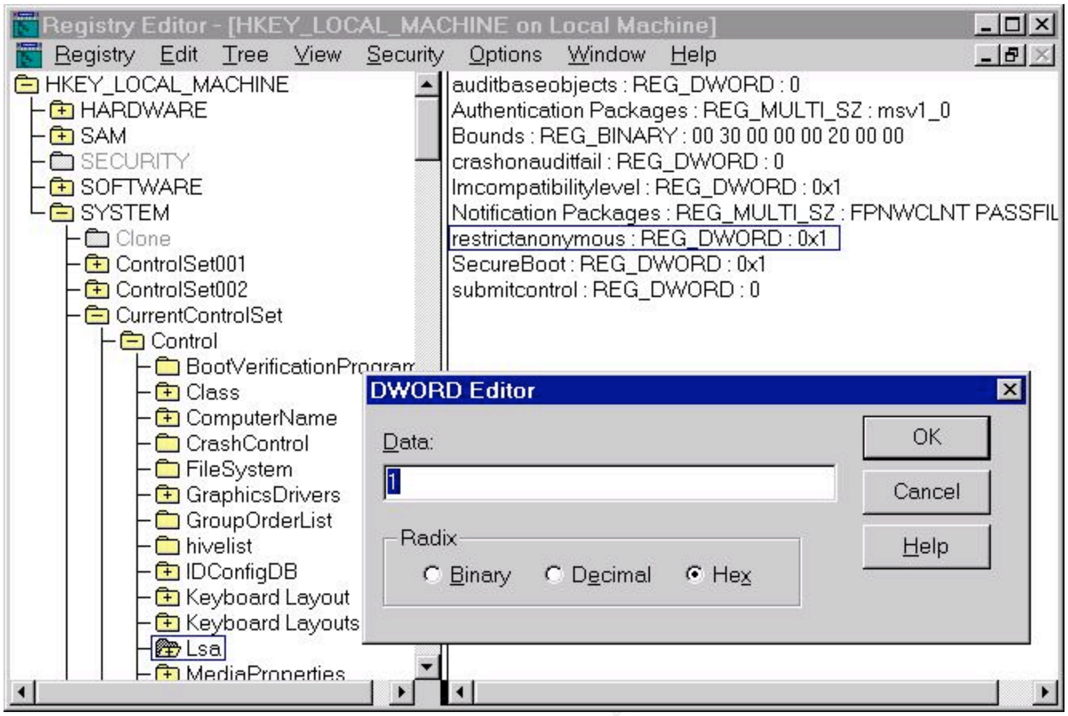
Background: Null sessions allow someone to access information of remote Windows NT computer without using a username and password for authentication. One would use a null character ("") for both the username and password.

Risk: Access to usernames, group names and shares can be obtained by anyone that is able to create null sessions. This may provide enough information for reconnaissance that may lead to greater risks.

Policy: Restrict null session access so that usernames and share names are not listed.

Validation:

1. Start Registry Editor (Regedt32.exe) and go to the following key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
2. Note the value of "RestrictAnonymous". The value should be 1.



```
auditbaseobjects : REG_DWORD : 0
Authentication Packages : REG_MULTI_SZ : msv1_0
Bounds : REG_BINARY : 00 30 00 00 00 20 00 00
crashonauditfail : REG_DWORD : 0
lmcompatibilitylevel : REG_DWORD : 0x1
Notification Packages : REG_MULTI_SZ : FPNWCLNT PASSFIL
restrictanonymous : REG_DWORD : 0x1
SecureBoot : REG_DWORD : 0x1
submitcontrol : REG_DWORD : 0
```

Data: 1

Radix: ○ Binary ○ Decimal ● Hex

Figure 15: RestrictAnonymous value set to 1.

Policy to restrict null session access ACME is meet.

Reference Materials

Microsoft Knowledge Base Article Q101063 – Windows Logon Welcome, Displaying Warning Message.

Microsoft Knowledge Base Article Q114463 – Hiding the Last Logged On Username in the Logon Dialog.

Microsoft Knowledge Base Article Q132475 – Determining If a Service Pack Has Been Installed.

Microsoft Knowledge Base Article Q143474 – Restricting Information Available to Anonymous Logon Users.

Microsoft Knowledge Base Article Q143475 – Windows NT System Key Permits Strong Encryption of the SAM.

Microsoft Knowledge Base Article Q147706 – How to Disable LM Authentication on Windows NT.

Microsoft Knowledge Base Article Q153183 – How to Restrict Access to NT Registry from a Remote Computer.

Microsoft Knowledge Base Article Q157238 – How to Activate Security Event Logging in Windows NT 4.0.

Microsoft Knowledge Base Article Q161990 – How to Enable Strong Password Functionality in Windows NT.

Microsoft Knowledge Base Article Q176820 – Differences Between 128-bit and 40-bit versions of SP3 & SP4.

Microsoft Knowledge Base Article Q183859 – Integrity Checking on Secure Channels with Domain Controllers.

Microsoft Knowledge Base Article Q239869 – How to Enable NTLM 2 Authentication for Windows 95/98/2000/NT.

Microsoft Knowledge Base Article Q245128 – Restrict Remote Access to Event Viewer on Windows NT Server.

Microsoft Knowledge Base Article Q248183 – Syskey Tool Reuses Keystream.

Microsoft Windows NT 4.0 Security, Audit and Control by James G. Jumes, Neil F. Cooper, Paula Chamoun, and Todd M. Feinman, Microsoft Technical.

Securing Windows NT, Step-by-Step by Jason Fossen & Jennifer Kolde, SAN NS2000 (Monterey, CA).

Securing Windows NT 4.0 Installation, NT Server Technical Notes – Planning, Microsoft TechNet.

Windows NT Security Step by Step version 1.4, by the SANS Institute.