Global Information Assurance Certification Paper

GIAC NT

PRACTICAL ASSIGNMENT FOR SANS SECURITY DC 2000

PREPARED BY

DON MICHELLI

TABLE OF CONTENTS

1. INTRODUCTION

This document was written to fulfill requirements for the practical assignment portion of the GIAC-NT certification. It represents only a portion of items to be addressed in terms of threats and vulnerabilities that should be reviewed in a comprehensive audit of a computing environment that utilizes Microsoft's Windows NT. Section 2 reviews eleven best practices for securing such a computing environment. Section 3 covers the installation and use of Pedestal Software's Security Expressions tool to perform an audit of a Windows NT 4.0 Domain Controller. Section 4 of this document provides the results of an audit of a Domain Controller using the Security Expressions tool. References used can be found in Section 5.

1.1 Disclaimers

All efforts have been made to ensure the accuracy and completeness of the information contained in this document. However, discoveries of new vulnerabilities, new software revisions, new or revised fixes, and new or revised vendor documentation may, at any time, make portions of this document invalid in terms of its applicability in a computing environment. This document is meant to serve only as a sample guide and is not a complete list of all best practices that should be followed in attempting to secure a Windows NT environment. A thorough and complete audit and analysis of each computing environment and the processes in place there, is recommended.

All recommendations should be tested throughly before implementing them on production systems.

This document does not address, nor was it intended to address site facility security, network security, or application security.

1.2 Definitions

Confidentiality	Information or data is unable to be understood by parties who do not have a "need to know."
Integrity	Information or data that is valid. The integrity of data can be compromised through human error, hardware failures, natural disasters, software bugs or viruses, or during the transmission of the data from one computer to another.
Availability	Information or data is available to authorized individuals when they need to access it.

2. SECURING WINDOWS NT

This section reviews eleven best practices for securing computers running Windows NT 4.0 Workstation or Server. These eleven best practices are a subset of the best practices identified in Securing Windows NT: Step By Step, published by the System Administration, Networking and Security (SANS) Institute. Implementing these eleven best practices alone will not guarantee the security of a computing environment. They are presented as a guide or sampling of some of the best practices that can be implemented.

A complete review of the entire list of best practices should be performed in order to provide increased levels of confidentiality, integrity and availability of workstations and servers running Microsoft's Windows NT 4.0.

For each of the eleven best practices listed, the following will be identified:

- **Problem** – Defines the security vulnerability and the impact of not implementing the best practice, i.e., to what vulnerability will the workstations or server be left open
- **Best Practice** – presents the recommended approach to mitigating the vulnerability.

2.1 Eleven Best Practices

2.1.1 FILE SYSTEM

2.1.1.1 Store Critical Data in NTFS Partitions

Problem Windows NT manages security only on NTFS file system partitions, and not on FAT (the traditional DOS) file systems. NTFS file system partitions allow access to be controlled to each file and/or folder on a per user basis. This granularity could be used to protect specific files and/or folders from access by unauthorized users.

Best Practice Format all hard drive partitions as NTFS partitions.

2.1.1.2 Set ACLs on O/S files

Problem When a NTFS partition is converted during the setup process the default permissions set give the "Everyone" group full control to all directories and files including critical Operating System folders and files.

Best Practice After the setup completes, the administrator should run the `FIXACLS.EXE` command to limit access to critical Operating System folders and files[1].

2.1.2 REGISTRY

2.1.2.1 Manage Logon Information Display

Problem By default, the Windows NT login screen will display the login of the last user who logged in as a convenience. This login name could be useful to intruders who see it displayed.

Best Practice Disable the display of the last logged on username by setting the following registry value[2] (if it doesn't exist, it must be created):

Hive: `HKEY_LOCAL_MACHINE`

Key: `\Software\Microsoft\Windows NT\CurrentVersion\Winlogin\`

Name: `DontDisplayLastUsername`

Type: REG_SZ

Value: `1`

2.1.2.2 Disable Use of Cached Logons

Problem By default, Windows NT stores the logon credentials for the last 10 users who logged on to the system[3]. This allows servers and workstations, in a domain environment, to be used in the event a domain controller cannot be contacted and to allow remote authentication through network boundaries. In an environment where security is important, it may be desirable to disable this feature.

Best Practice Disable caching of logon information by setting the following registry value (if it doesn't exist, it must be created)

Hive: `HKEY_LOCAL_MACHINE`

Key: `\Software\Microsoft\Windows NT\CurrentVersion\Winlogin\`

Name: `CachedLogonsCount`

Type: REG_SZ

Value: `0`

2.1.2.3 Use of Logon Message as a Warning

Problem Attempts to prosecute intruders have failed in court because the owner of a computer failed to provide sufficient information to warn intruders that they were being monitored.

Best Practice Use the logon message to warn uninvited users that they are not allowed and to warn authorized users that they must use the system only for approved business purposes[4]. Also advise users to not install unapproved software and that use of the computer indicates consent to monitoring by the company including keystroke monitoring.

The registry values (if they don't exist, they must be created)

Hive: HKEY_LOCAL_MACHINE

Key: \Software\Microsoft\Windows NT\CurrentVersion\Winlogin\

Name: LegalNoticeCaption

Type: REG_SZ

Value: NOTICE!! You are being monitored

Name: LegalNoticeText

Type: REG_SZ

Value: To be used only for authorized purposes. No unauthorized software is to be installed on this computer system.

WARNING! By accessing and using this system you are consenting to system and keystroke monitoring for law enforcement and other purposes. Unauthorized use of this computer system may subject you to criminal prosecution and penalties.

2.1.2.4 Enforce Strong Passwords

Problem A malicious user can easily crack weak passwords.

Best Practice Enforce the use of strong passwords by implementing a password filter such as "passfilt.dll" which Microsoft delivered with Service Pack 2 and later for Windows NT 4.0. The password policy enforced by passfilt.dll requires passwords to be at least six characters in length and use characters from three of four character "classes"—Uppercase, lowercase, numeric or punctuation characters.[5]

To implement, the passfilt.dll file is placed in %systemroot%\system32 and an edit to the registry is required.

The registry values (if it doesn't exist, it must be created)

Hive: HKEY_LOCAL_MACHINE

Key: \SYSTEM\CurrentControlSet\Control\LSA\

Name: Notification Packages

Type: REG_MULTI_SZ

Value: **PASSFILT**

2.1.2.5 Control Remote Access to the Registry

Problem The Windows NT registry on remote computers can be accessed over a network by registry tools delivered with Windows NT and the NT Resource Kit. A malicious user could utilize these tools to remotely make changes to the registry of a computer running Windows NT 4.0.

Best Practice The ACL set on the registry key

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg` determines which users or groups can access the registry remotely across the network[6]. If the key does not exist, remote access is not restricted. The ACL should be set to give only Administrators full control.

2.1.3 Password Controls and Account Policies

2.1.3.1 Limit Failed Logon Attempts

Problem By default, Windows NT allows a user to attempt to logon repeatedly to an account, neither logging the failed attempts nor disabling the user account after a predetermined number of failed attempts.

Best Practice Lock user account after five failed login attempts[7].

2.1.3.2 Disable the Guest Account

Problem The Guest account is well known and a likely target for malicious users attempting to gain access to a computer running Windows NT. This account is enabled by default on Windows NT 4.0 Workstation and disabled by default on Windows NT 4.0 Server.

Best Practice Make sure that on both Windows NT 4.0 Workstation and Server the Guest account is disabled and has a non-trivial password assigned to it[8].

2.1.3.3 Secure and Manage Event Logs

Problem The Application and System logs for Windows NT can, by default, be accessed by ordinary users.

Best Practice Set NTFS permissions on the event log files (located in `%systemroot%\system32\config\*.evt`) to allow access by Administrators and System accounts. Do not give any regular user the *Manage Security and Audit Log* right.

2.1.4 Other Actions

2.1.4.1 Install the Latest Service Pack for Windows NT

Problem Microsoft uses Service packs to distribute product updates, bug fixes and security updates to fix recently discovered vulnerabilities. Failure to install a service pack can leave your computer vulnerable.

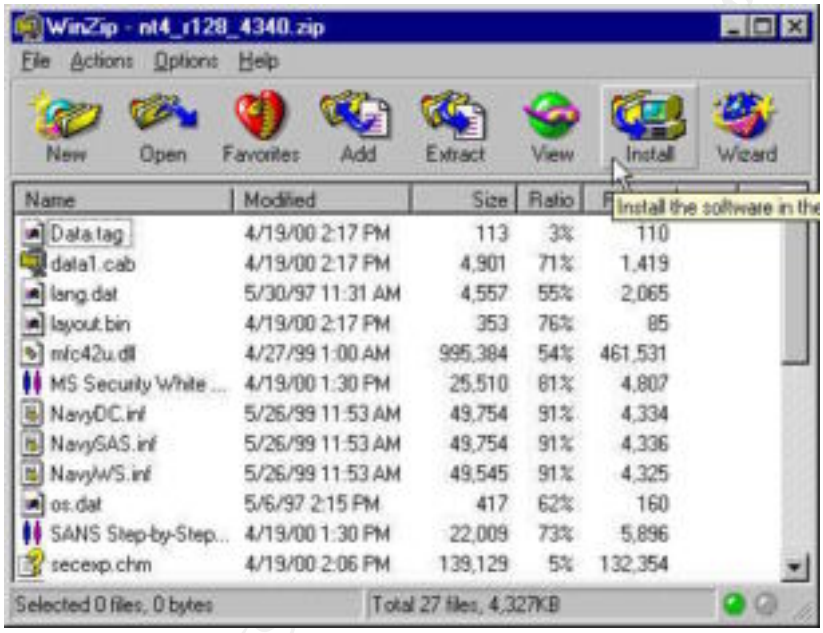
Best Practice Ensure that the latest service pack for Windows NT 4.0 (Service Pack 6) is installed[9]. This can be verified by making sure the value of `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\CSDVersion` is set to "`Service Pack 6`"

3. SECURITY EXPRESSIONS BY PEDESTAL SOFTWARE LLC

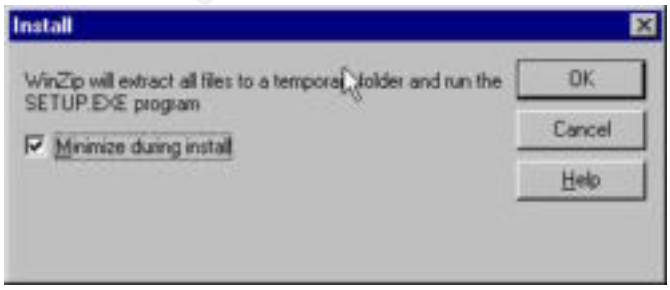
According to Pedestal Software, their Security Expressions tool allows administrators to lock down computers running Windows NT based on policy guidelines like those developed by the National Security Agency, SANS, and others. Security Expressions allows an administrator to load a policy template and then audit local and remote computers for their adherence to the loaded policy template. An administrator can easily customize templates for use with the Security Expressions tool.

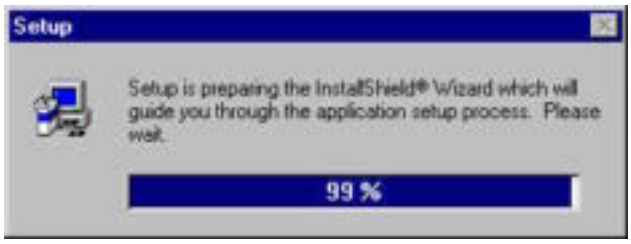
3.1 Installing Security Expressions

1. Upon purchasing Security Expressions from Pedestal Software you will receive an e-mail providing you with your license key and a URL for downloading the current version of Security Expressions. After saving the downloaded file (in our case nt4_r128_4340.zip) Security Expressions can be installed opening the zip file with WinZip and clicking on the [**Install**] button, which will execute the setup.exe found in the zip file.



2. Clicking on [**OK**] will start the InstallShield® Wizard.

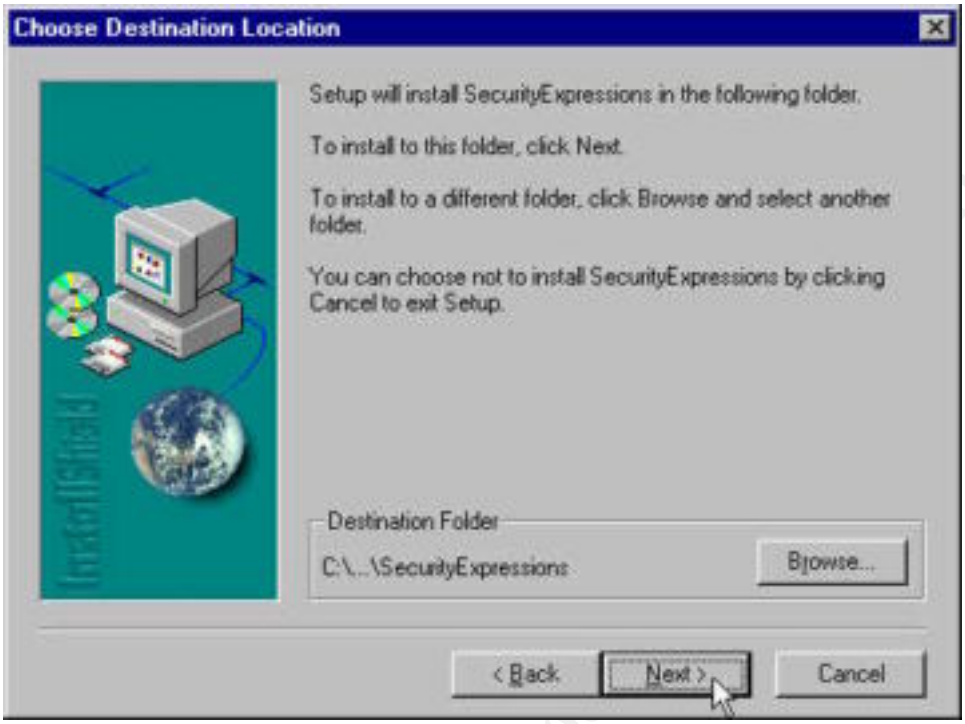




3. On the Welcome screen, click on [**Next**] to continue.

4. Read the Software License Agreement and if you agree to its Terms & Conditions, click on [**Yes**] to continue.

5. Click on [**Next**] to install Security Expressions in its default location of `C:\program files\Pedestal Software\SecurityExpressions`



6. Click on [**Next**] to place the shortcuts in their default Program Folder

7. After the installation has completed, click on [**Finish**] to complete the Setup

4.2 Using Security Expressions

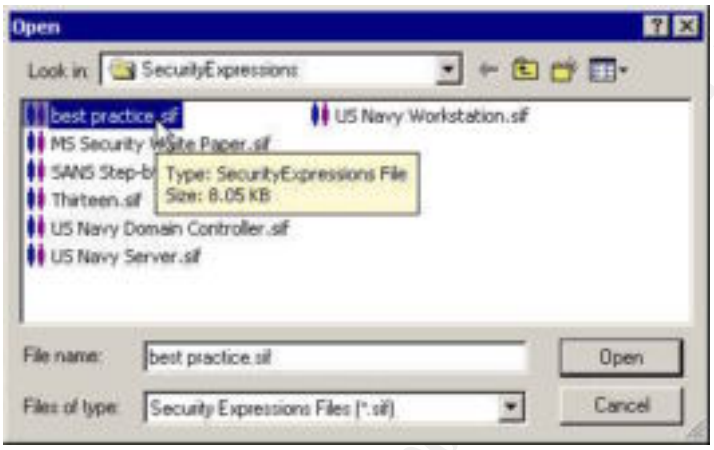
1. Start Security Expressions by clicking on [**START**], **Programs**, **SecurityExpressions**, **SecurityExpressions**

2. If this is the first time you have used Security Expressions since you purchased it you can enter your license key on the following screen and click on [**Register**], or you may click on [**Cancel**].

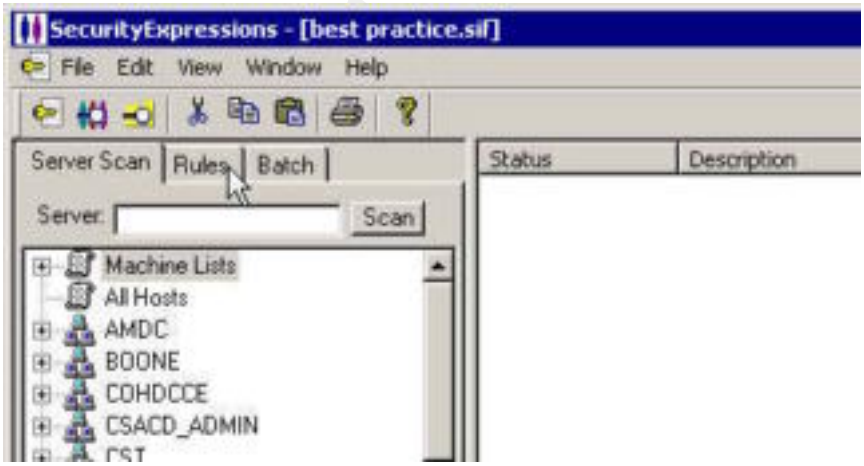
Note: The key entered in the above screen capture is not a valid license key and is for illustrative purposes only.

3. After Security Expressions opens, select **File**, **Open**.

4. In the following dialog box select the policy template file you will be using and click [**Open**]. For this document we will use a file named `best practice.sif`[1].

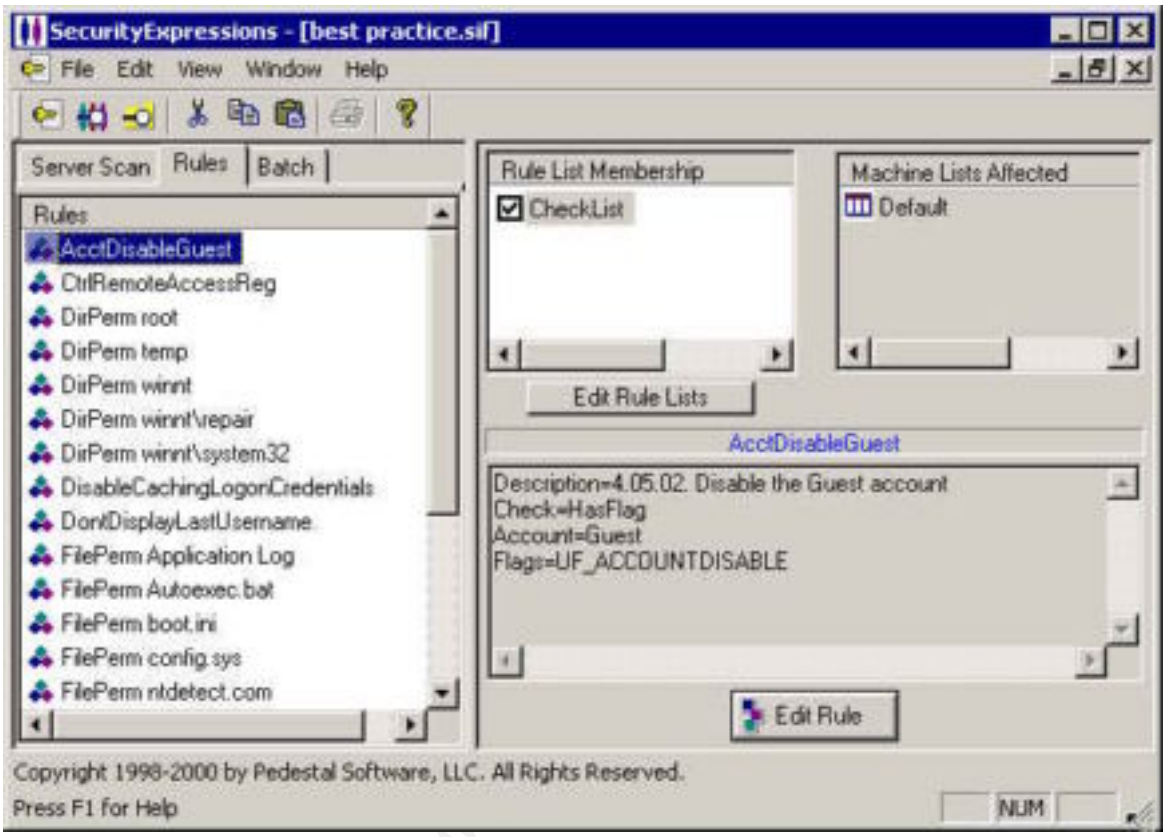


5. Click the **Rules** tab to see a list of the vulnerabilities checked for in the `best practice.sif` file.

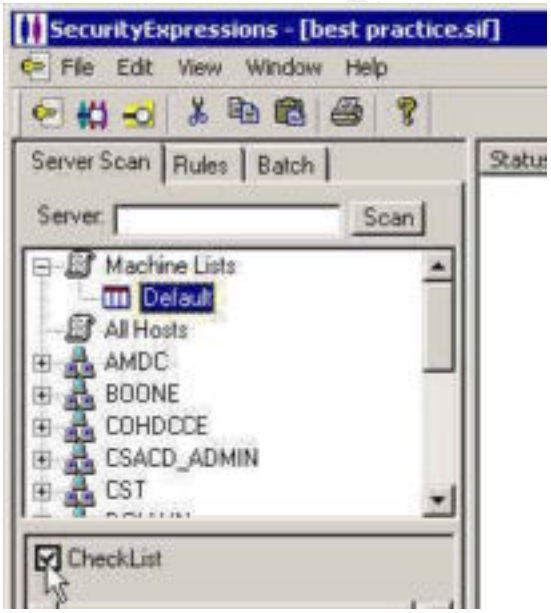


[1] I created the file "`best practice.sif`" specifically for those best practices reviewed in section two of this document. The file is not delivered as a part of the Security Expressions product.

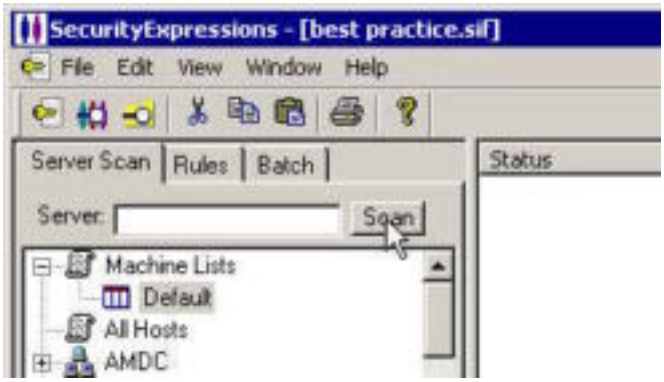
6. The vulnerabilities that are checked for appear listed as rules on the left-hand side of the displayed screen.



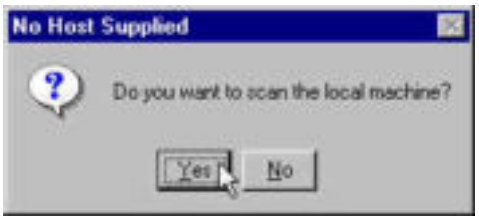
7. Click the **Server Scan** tab, double-click on **Machine Lists**, highlight **Default**, and place a checkmark in the **checklists** box to use those rules contained in the `best practice.sif` file.



8. Click on the [**Scan**] button to begin to scan the local workstation.

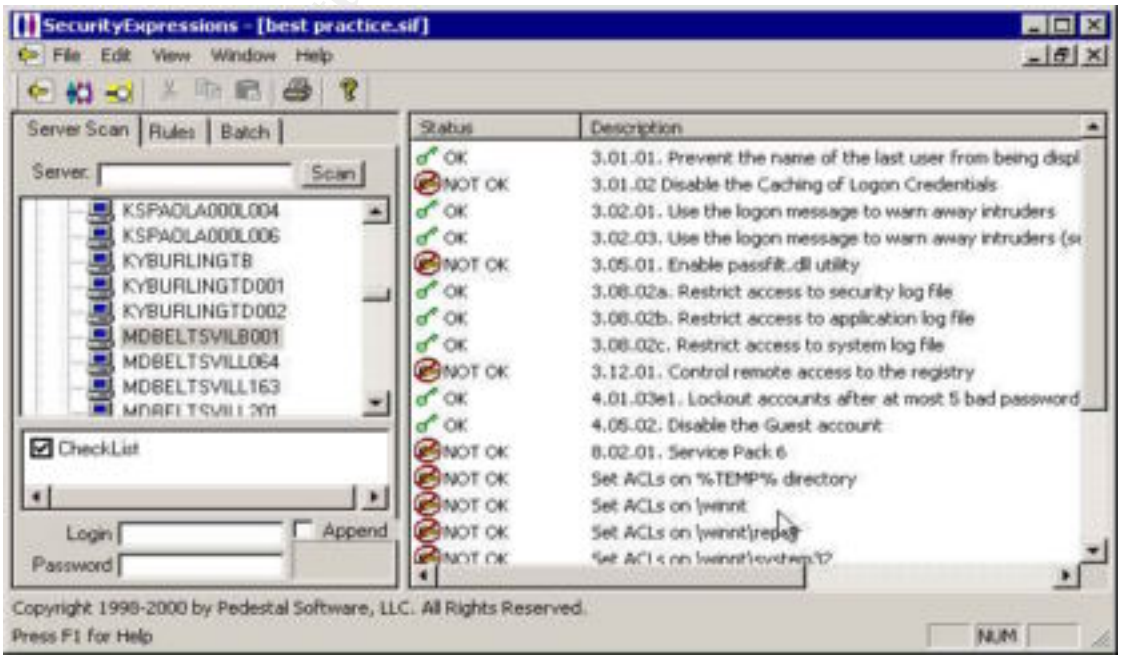


9. Click on [**Yes**] in the following dialog box:

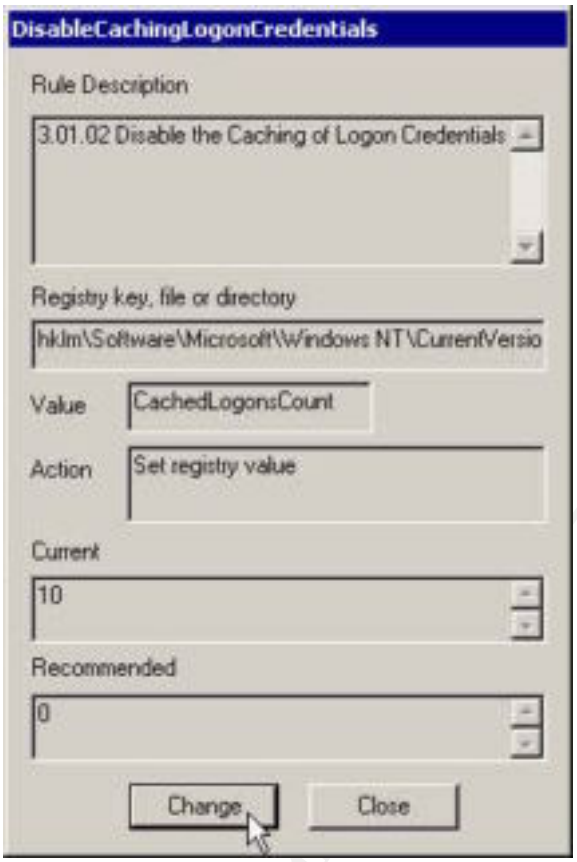


10. Click on [**Yes**] in the following dialog box:

11. The results of the scan of the eleven best practices presented in section two of this document is presented on the right hand side of the screen.



12. Items marked, as NOT OK may be double-clicked on to view further information about the vulnerability. Clicking the [**Change**] button in the dialog box that appears will implement the recommended best practice. In the dialog box shown below, clicking [**Change**] will modify the value of `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\CachedLogonsCount` to zero `(0)` to disable the caching of logon credentials.



4. RESULTS OF AUDITING A DOMAIN CONTROLLER

4.1 Before Implementing Best Practices

The following output was obtained by using Security Expressions with the `best practice.sif` file to audit a Windows NT Domain Controller (MDTEST0000P002), running Windows NT Server 4.0 with Service Pack 6, prior to implementing the best practices covered in section two of this document:

Status	Description	Host*	Priority	Rule
OK	3.01.01. Prevent the name of the last user from being displayed on the login screen .		Normal	DontDisplayLastUsername
NOT OK	3.01.02 Disable the Caching of Logon Credentials Current: 10 Desired: 0		Normal	DisableCachingLogonCredentials
OK	3.02.01. Use the logon message to warn away intruders		Normal	LogonMessage
OK	3.02.03. Use the logon message to warn away intruders (set a caption)		Normal	LogonMessageCaption
NOT OK	3.05.01. Enable passfilt.dll utility Current: FPNWCLNT C:\WINNT\System32\pwdriver.dll Desired: PASSFILT		Normal	PasswordStrength
NOT OK	3.08.02a. Restrict access to security log file Current: ACL: Administrators, (All), Server Operators, (RWXD), SYSTEM, (All) Desired: ACL: Administrators, (All), SYSTEM, (All)		Normal	FilePerm Security Log
NOT OK	3.08.02b. Restrict access to application log file Current: ACL: Administrators, (All), Server Operators, (RWXD), SYSTEM, (All) Desired: ACL: Administrators, (All), SYSTEM, (All)		Normal	FilePerm application Log
NOT	3.08.02c. Restrict access to system		Normal	FilePerm System Log

OK	log file Current: ACL: Administrators, (All), Server Operators, (RWXD), SYSTEM, (All) Desired: ACL: Administrators, (All), SYSTEM, (All)			
NOT OK	3.12.01. Control remote access to the registry Current: ACL: Administrators, (Full)*1, Backup Operators, (QWCENR)*1 Desired: ACL: Administrators, (Full)*1, SYSTEM, (Full)*1		Normal	CtrlRemoteAccessReg
OK	4.01.03e1. Lockout accounts after at most 5 bad passwords		Normal	PolicyLockout
OK	4.05.02. Disable the Guest account		Normal	AcctDisableGuest
OK	8.02.01. Service Pack 6		Normal	SP6
NOT OK	Set ACLs on %TEMP% directory Current: ACL: Administrators, (All)(All)*, CREATOR OWNER, (All)(All)*, Everyone, (RWXD)(RWXD)*, SYSTEM, (All)(All)* Desired: ACL: Administrators, (All)(All)*, Authenticated Users, (RWX)(RWX)*, SYSTEM, (All)(All)*		Normal	DirPerm temp
NOT OK	Set ACLs on \winnt Current: ACL: Administrators, (All)(All)*, CREATOR OWNER, (All)(All)*, Everyone, (RWXD)(RWXD)*, SYSTEM, (All)(All)* Desired: ACL: Administrators, (All)(All)*, Authenticated Users, (RX)(RX)*, CREATOR OWNER, (All)(All)*, SYSTEM, (All)(All)*		Normal	DirPerm winnt
OK	Set ACLs on \winnt\repair		Normal	DirPerm winnt\repair
NOT OK	Set ACLs on \winnt\system32 Current: ACL: Administrators, (All)(All)*, CREATOR OWNER, ()(All)*2, Everyone, (RWXD)(RWXD)*, SYSTEM, (All)(All)* Desired: ACL: Administrators, (All)(All)*, Authenticated Users, (RX)(RX)*,		Normal	DirPerm winnt\system32

	CREATOR OWNER, (All)(All)*, SYSTEM, (All)(All)*			
NOT OK	Set ACLs on autoexec.bat Current: ACL: Administrators, (All), Everyone, (RX), Server Operators, (RWXD), SYSTEM, (All) Desired: ACL: Administrators, (All), Authenticated Users, (RX), SYSTEM, (All)		Normal	FilePerm autoexec.bat
NOT OK	Set ACLs on boot.ini Current: ACL: Administrators, (All), Server Operators, (RWXD), SYSTEM, (All) Desired: ACL: Administrators, (All), SYSTEM, (All)		Normal	FilePerm boot.ini
NOT OK	Set ACLs on config.sys Current: ACL: Administrators, (All), Everyone, (RX), Server Operators, (RWXD), SYSTEM, (All) Desired: ACL: Administrators, (All), Authenticated Users, (RX), SYSTEM, (All)		Normal	FilePerm config.sys
NOT OK	Set ACLs on ntdetect.com Current: ACL: Administrators, (All), Server Operators, (RWXD), SYSTEM, (All) Desired: ACL: Administrators, (All), SYSTEM, (All)		Normal	FilePerm ntdetect.com
NOT OK	Set ACLs on ntldr Current: ACL: Administrators, (All), Server Operators, (RWXD), SYSTEM, (All) Desired: ACL: Administrators, (All), SYSTEM, (All)		Normal	FilePerm ntldr
NOT OK	Set ACLs on root of %SystemDrive% Current: ACL: Administrators, (All)(All)*, Authenticated Users, (RX)(RX)*, CREATOR OWNER, (All)(All)*, Server Operators, (W)(), SYSTEM, (All)(All)* Desired: ACL: Administrators, (All)(All)*, Authenticated Users, (RX)(RX)*, SYSTEM, (All)(All)*		Normal	DirPerm root

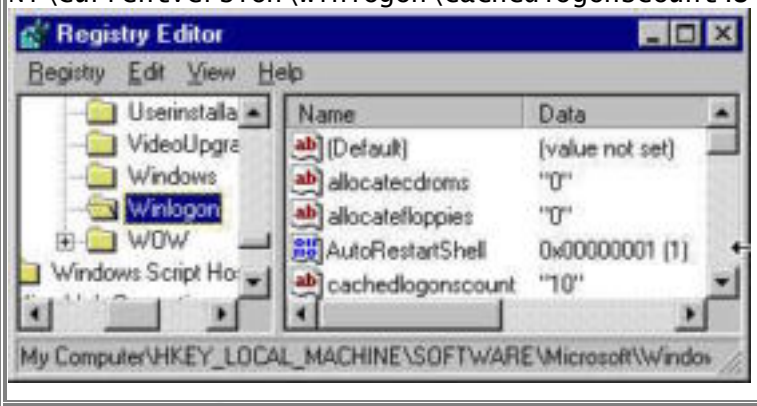
* Host name deleted to improve readability

4.2 After Implementing Best Practices

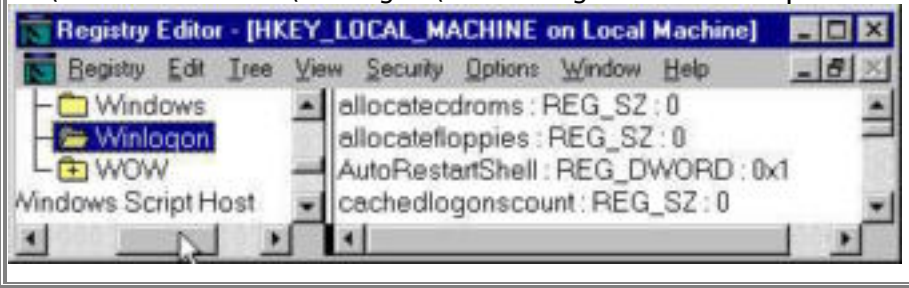
The following output was obtained by using Security Expressions with the `best practice.sif` file to audit a Windows NT Domain Controller (MDTEST0000P002), running Windows NT Server 4.0 with Service Pack 6, after implementing the best practices covered in section two of this document. Those best practices which involve changing a registry key and marked with a NOT OK in the previous report above, have a screen capture of the registry before and after the change below:

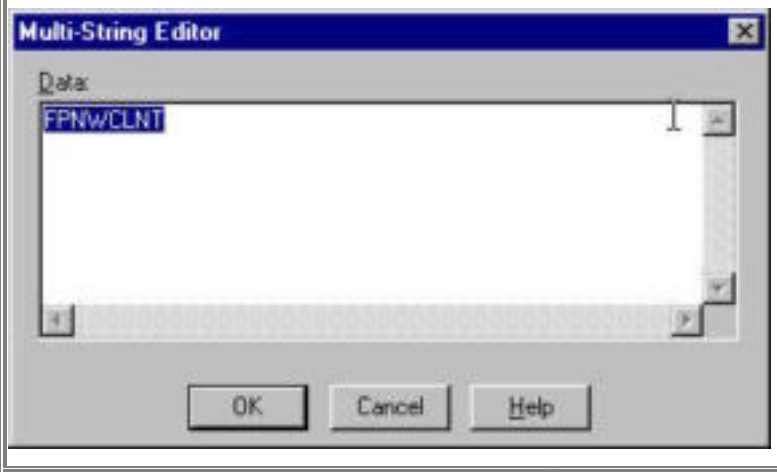
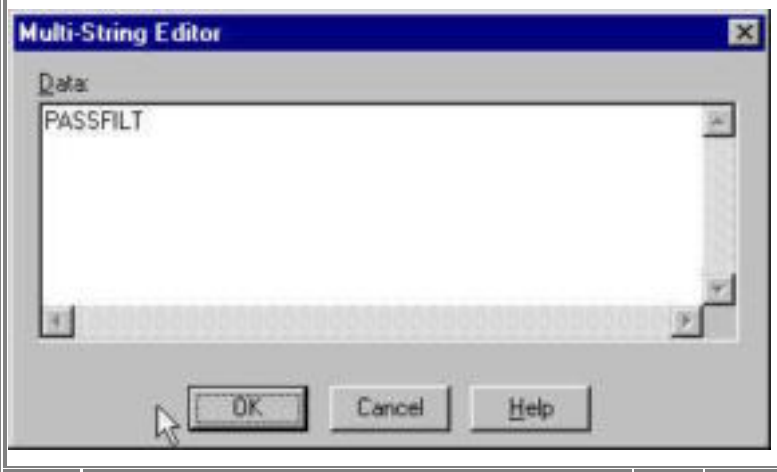
Status	Description	Host*	Priority	Rule
OK	3.01.01. Prevent the name of the last user from being displayed on the login screen .		Normal	DontDisplayLastUsername
OK	3.01.02 Disable the Caching of Logon Credentials		Normal	DisableCachingLogonCredentials

Prior to implementing the best practice, the value of `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\cachedlogonscount` is equal to 10



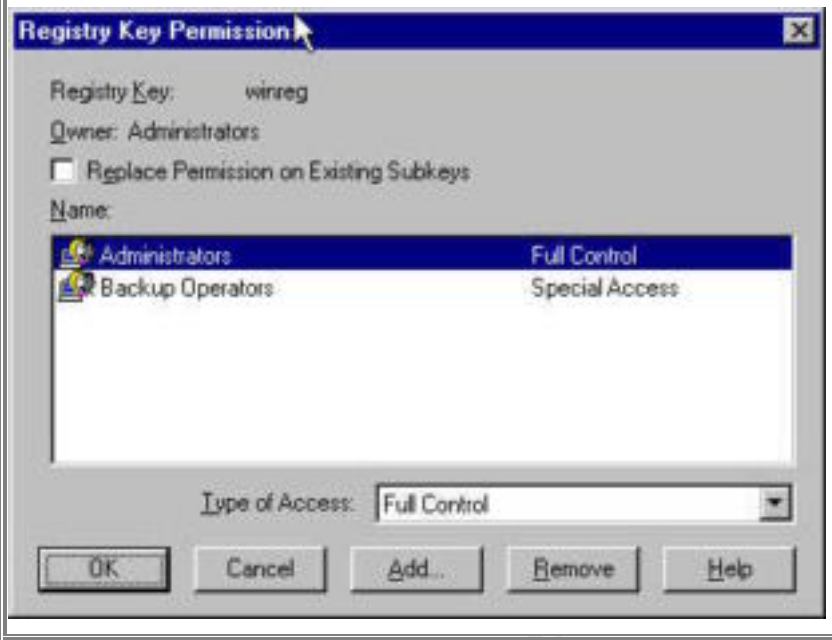
After implementing the best practice, the value of `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\cachedlogonscount` is equal to 0



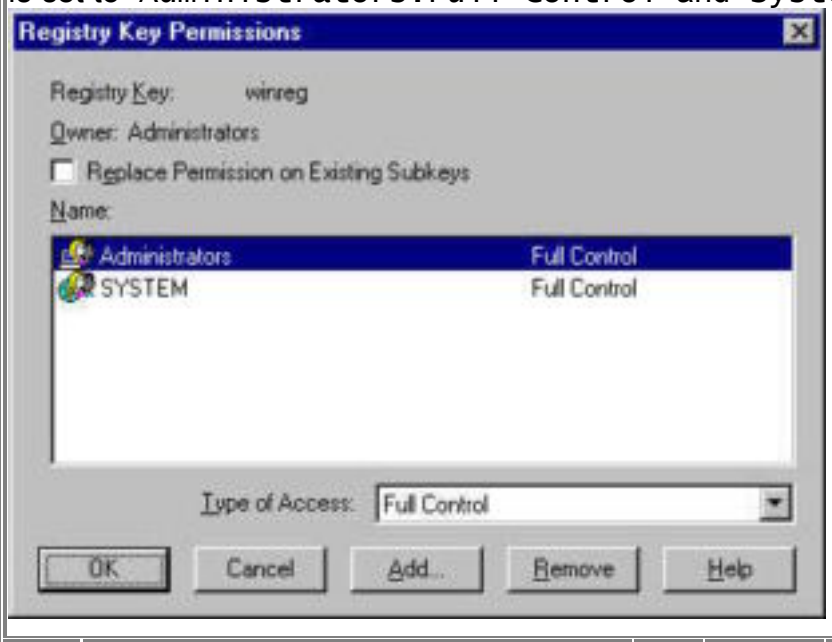
OK	3.02.01. Use the logon message to warn away intruders		Normal	LogonMessage
OK	3.02.03. Use the logon message to warn away intruders (set a caption)		Normal	LogonMessageCaption
OK	3.05.01. Enable passfilt.dll utility		Normal	PasswordStrength
Prior to implementing the best practice, the value of `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\Notification packages` is equal to the string "`FPNWCLNT`" 				
After implementing the best practice, the value of `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\Notification packages` is equal to the string "`PASSFILT`" 				
OK	3.08.02a. Restrict access to security log file		Normal	FilePerm Security Log
OK	3.08.02b. Restrict access to application log file		Normal	FilePerm application Log
OK	3.08.02c. Restrict access to system		Normal	FilePerm System Log

	log file			
OK	3.12.01. Control remote access to the registry		Normal	CtrlRemoteAccessReg

Prior to implementing the best practice, the Registry Key Permissions for `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg` is set to `Administrators:Full Control and Backup Operators:Special Access`



After implementing the best practice, the Registry Key Permissions for `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg` is set to `Administrators:Full Control and System:Full Control`



OK	4.01.03e1. Lockout accounts after at		Normal	PolicyLockout

	most 5 bad passwords			
OK	4.05.02. Disable the Guest account		Normal	AcctDisableGuest
OK	8.02.01. Service Pack 6		Normal	SP6
OK	Set ACLs on %TEMP% directory		Normal	DirPerm temp
OK	Set ACLs on \winnt		Normal	DirPerm winnt
OK	Set ACLs on \winnt\repair		Normal	DirPerm winnt\repair
OK	Set ACLs on \winnt\system32		Normal	DirPerm winnt\system32
OK	Set ACLs on autoexec.bat		Normal	FilePerm autoexec.bat
OK	Set ACLs on boot.ini		Normal	FilePerm boot.ini
OK	Set ACLs on config.sys		Normal	FilePerm config.sys
OK	Set ACLs on ntdetect.com		Normal	FilePerm ntdetect.com
OK	Set ACLs on ntldr		Normal	FilePerm ntldr
OK	Set ACLs on root of %SystemDrive%		Normal	DirPerm root

* Host name deleted to improve readability

5. REFERENCES

[1] "Setacl.exe Not Available in Windows NT 4.0", Microsoft Knowledge Base Article Q157963

[2] Ivens, Kathy. *Managing Windows NT Logons*. O'Reilly & Associates, Inc.

[3] Robichaux, Paul. *Managing the Windows NT Registry.* O'Reilly & Associates, Inc.

[4] "Windows Logon Welcome, Displaying Warning Message", Microsoft Knowledge Base Article Q101063

[5] "How to Enable Strong Password Functionality in Windows NT", Microsoft Knowledge Base Article Q161990

[6] "Regulate Network Access to the Windows NT Registry", Microsoft Knowledge Base Article Q155363

[7] SANS Institute (et. al.). *Windows Security Step By Step.* The SANS Institute, 1999

[8] Fossen, Jason and Jesper Johansson. *Windows NT Security: Step by Step.* The SANS Institute GIAC Training, 2000

[9] "How to Obtain the Latest Windows NT 4.0 Service Pack", Microsoft Knowledge Base Article Q152734