Global Information Assurance Certification Paper

GIAC NT

Practical Assignment for SANS Parliament Hill 2000

Submitted by Clyde D'Souza

Table of Contents

Overview

Introduction

Systems security audits determine if the systems being audited have reasonable checks to ensure confidentiality, integrity and availability. The goal is to evaluate current security measures and identify vulnerabilities that needed to be addressed.

[i]The steps in the systems audit process are as follows:

1. Gain an understanding
   This step involves collection and analysis of information about the system operational procedures and controls implemented. It also involves learning from management the risks associated with systems being compromised and preparing a statement of sensitivity upon which the audit will be based.
2. Define the scope.
   This step involves reviewing the statement of sensitivity, of the previous step, and deciding what needs to be audited (typically what management has identified as the most critical components)
3. Review the controls.
   This step involves investigating the procedures and controls that have been implemented around these critical components.
4. Report the findings.
   This step involves creating a report that conveys the findings of the audit. The report typically highlights potential vulnerabilities and recommends corrective measures.

Scope of this document

A complete security audit would focus on various aspects of security including but not limited to

- Evaluation of a Disaster Recovery/Business Continuity Plan and Incident Response Plans
- Physical security of servers and workstations
- Server and workstation operating system hardening
- Securing network components like routers
- Use of secure network connections like VPN's
- Deployment of firewalls and intrusion detection systems
- Procedures for backing up and restoring data
- Proper configuration of messaging servers to prevent relaying
- Use of virus scanners
- User education and enforcing usage of strong passwords

This document, written to complete requirements for the GIAC certification is Windows NT, is not intended as a guide to conducting comprehensive audits of network security. It focuses on auditing the security around some important aspects of Windows NT servers. A conscious attempt is made to use tools provided by Microsoft but in some cases third party tools are used.

Assumptions

This document assumes that

- Adequate measures have been taken to ensure the physical security of the systems
- Firewalls have been installed, VPN's are used and network components have been secured.
- Regular backups are being made with adequate measures taken to store backup media securely on and off site
- This is a medium security network
- A single domain is being used

Server Security Review

This section lists the steps taken in auditing different aspects of Windows NT. These steps ensure the most basic level of security, required on every Windows NT server, is implemented.

Service pack version check

Windows NT Service packs, minor releases between major versions, typically contain product updates and fixes for security holes. The practice of keeping operating systems updated with the most current service pack has been proven to increase reliability and availability. For example, frequency of computer restarts was reduced by 50% when Windows NT 4.0, service pack 4 was installed, as compared to Windows NT 4.0, service pack 3.[ii]

To verify the Service Pack level on a server run the command Winver.EXE. (Click on *Start » Run and type in Winver*). You should see a window like the one shown below

Stated policy requires Service Pack 6a.

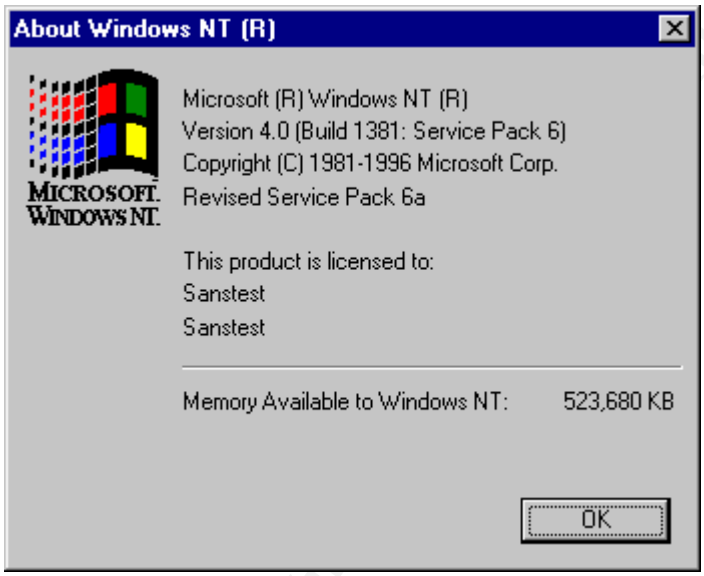

Figure 1: Run Winver.EXE to display the service pack level on the server

Hot fixes are usually minor patches to the operating system and correct specific problems between service packs. These should be applied only if the system experiences the problem corrected by a hot fix.

Stated policy does not require any post-Service Pack 6a hotfixes.

Check file system type

Windows NT 4.0 supports two types of file systems NTFS or FAT. NTFS advantages over FAT include in fault tolerance, transaction logging and recovery techniques, better availability and better performance because the file system is more effectively indexed. Windows NT 4.0 does not support file system security with FAT.

Stated policy requires NTFS.

To verify this run the Disk Administrator *(Start » Programs » Administrative Tools (Common) » Disk Administrator)*

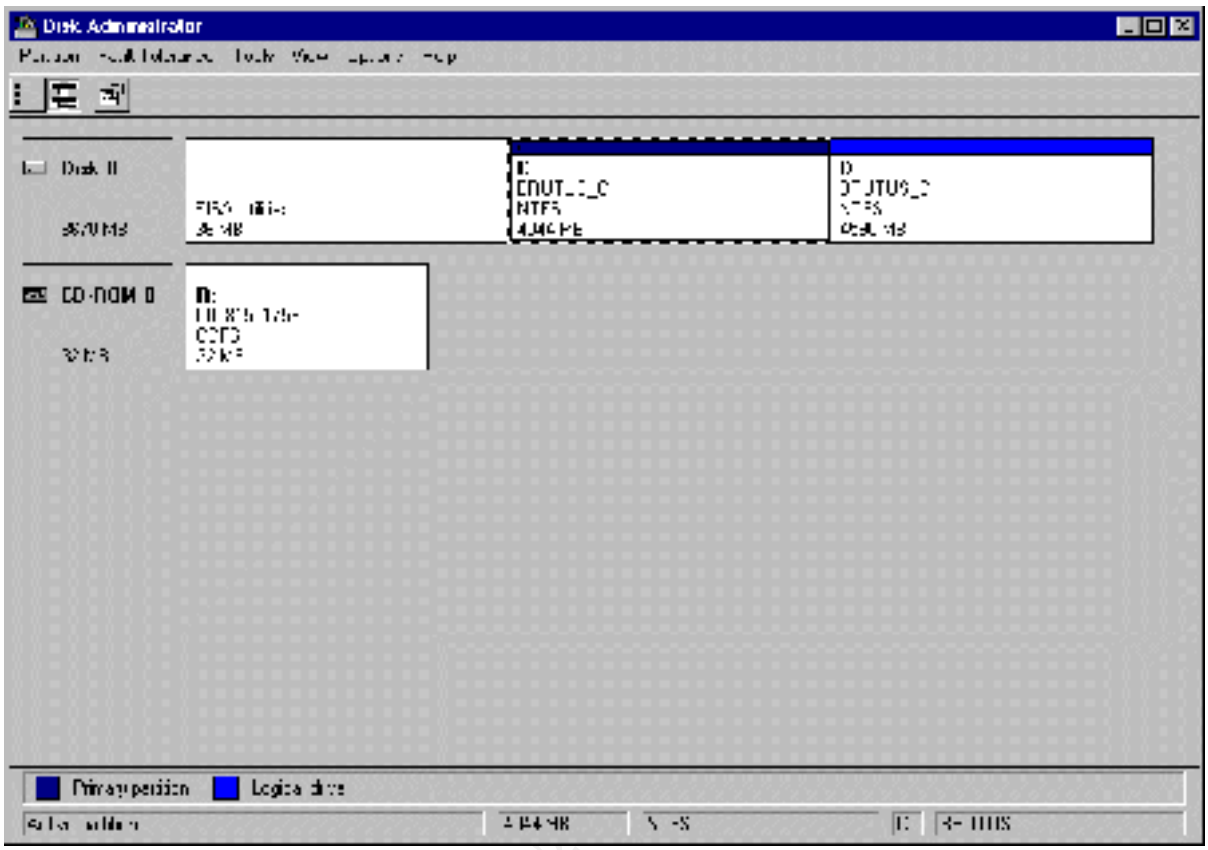

Figure 2: Disk Administrator can be used to determine the file system type on each of the server disks

Audit policy

Windows NT supports auditing of user and system activities. A default installation of Windows NT does not have auditing enabled. Enabling audit policies enables tracking of user and system activities. Ensure that this feature is enabled and also ensure that certain events are audited as per stated policy.

The stated policy is

Audit Item		Policy
Logon and Logoff	Success	Enabled
Logon and Logoff	Failure	Enabled
File and Object Access	Success	Disabled
File and Object Access	Failure	Enabled
Use of User Rights	Success	Disabled
Use of User Rights	Failure	Enabled
User and Group Management	Success	Enabled
User and Group Management	Failure	Enabled
Security Policy Changes	Success	Enabled
Security Policy Changes	Failure	Enabled
Restart, Shutdown and System	Success	Enabled
Restart, Shutdown and System	Failure	Enabled
Process Tracking	Success	Disabled
Process Tracking	Failure	Disabled

Verifying the audit policy is done using User Manager *(Start » Programs » Administrative Tools (Common) » User Manager for Domains)*

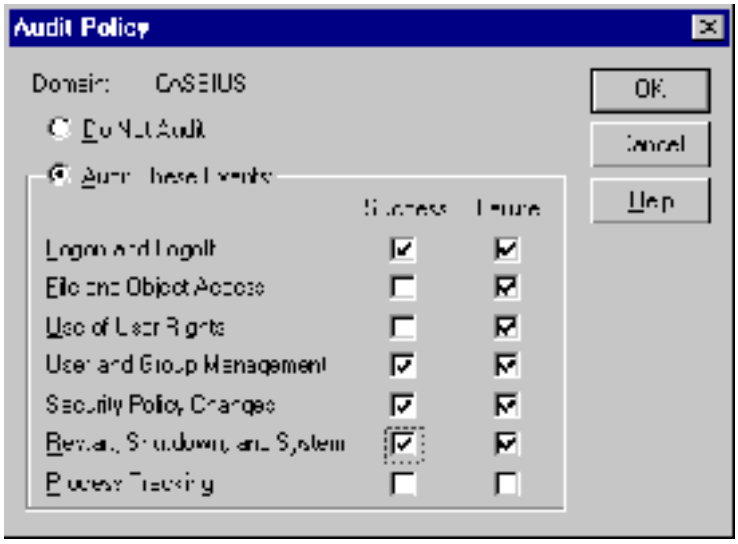

Figure 3: User Manager for Domains can be used to set audit policies.

Password policy

Security on most systems is compromised by the lack of enforcement of a strong password policy. Obvious passwords can be guessed easily. [iii]Windows NT 4.0 Service Pack 2 and later includes a password filter DLL file (Passfilt.dll) that allows enforcement of strong user passwords. Passfilt.dll provides enhanced security against "password guessing" or "dictionary attacks" by outside intruders. If the implementation of the password policy in PASSFILT.DLL does not meet the security requirements of an organization it is possible to write a DLL and implement it the same as the Microsoft version.

To use Passfilt.Dll, the administrator must configure the password filter DLL in the system registry on all domain controllers. This can be done as follows:

Setup the following registry key value:

Hive: HKEY_LOCAL_MACHINE\SYSTEM
Key: System\CurrentControlSet\Control\LSA
Name: Notification Packages
Type: REG_MULTI_SZ
Value: Add string “PASSFILT” (do not remove existing ones).

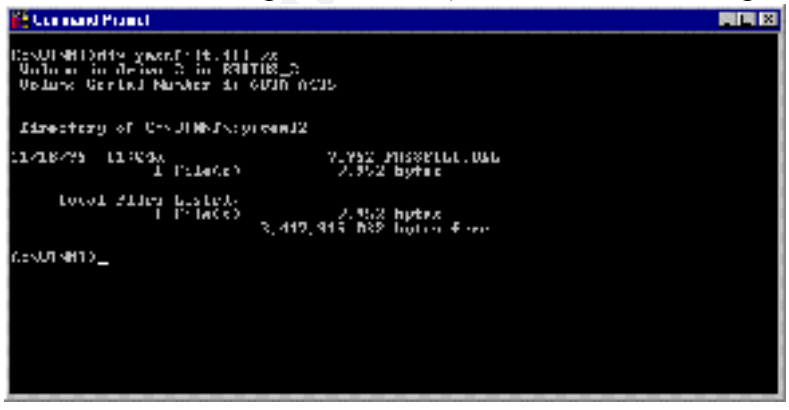

Figure 4: Verifying the existence of the PASSFILT.DLL file.

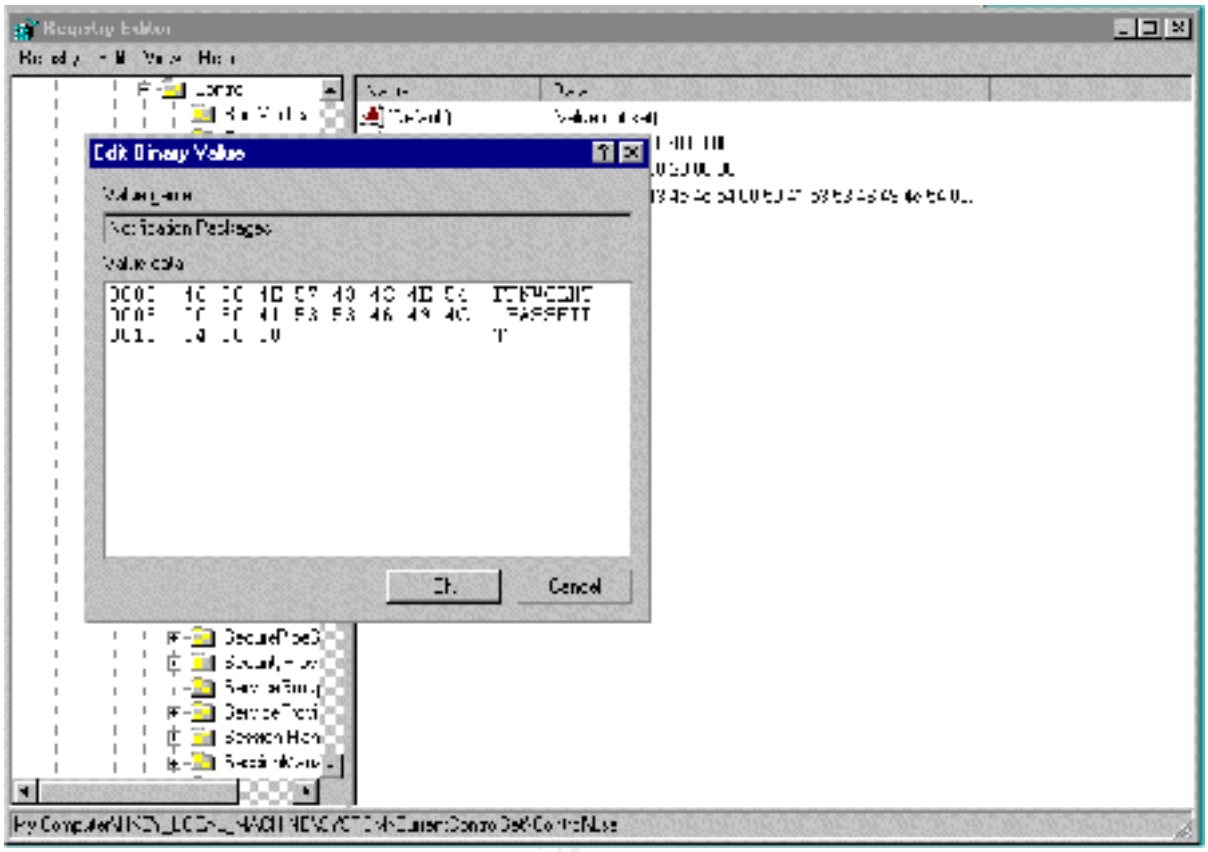

Figure 5: Verifying the implementation of PASSFILT.DLL using Registry Editor (Regedit.EXE)

Account Policy

The Account policy controls how passwords must be used by all user accounts for a computer or domain and also determines the account lockout policy. Examine the account policy for all accounts by running User Manager *(Start » Programs » Administrative Tools » User Manager for Domains » Policies Account.)*

Stated account policy settings are:

Maximum Password Age (days)	90
Minimum Password Age (days)	3
Minimum Password Length (characters)	8
Password Uniqueness (passwords)	4
Account Lockout	Yes
Account Lockout (bad attempts)	3
Account Lockout (reset count in minutes))	120
Lockout Duration (minutes)	1440 (1 day)
Forcibly disconnect remote users from server when logon hours expire	Yes
Users log on to change password	Yes

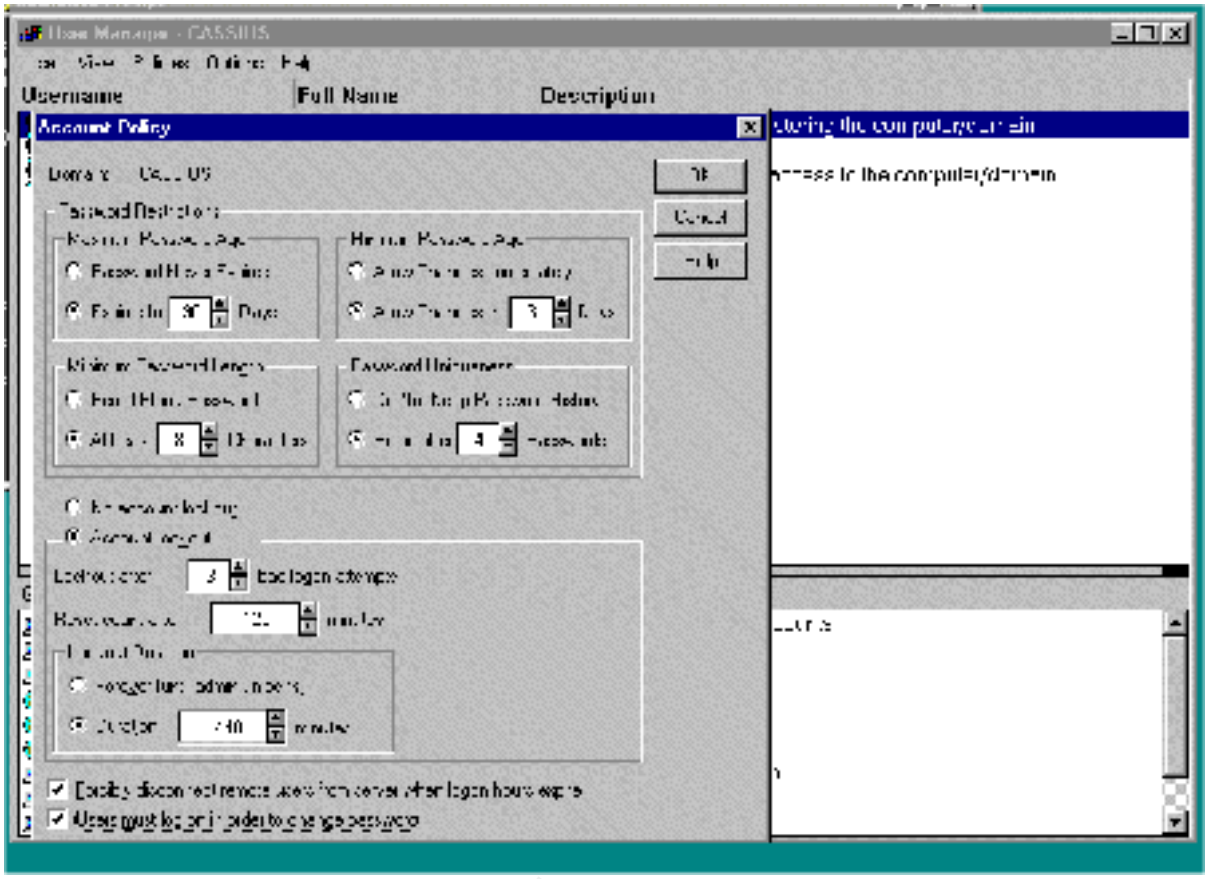

Figure 6: User Manager for Domains is used to set and verify the Account Policies.

Event Log Settings

Windows NT Server records events in three kinds of logs:

- The system log contains events logged by the Windows NT Server system components. Windows NT Server predetermines the event types logged by system components. Examples include driver or component failure.
- The security log can contain security-related events like valid and invalid logon attempts, successful and failed attempts at resource usage.
- The application log contains events logged by applications. Application developers decide which events to monitor.

All users can view system and application logs; security logs are accessible only to system administrators. Logging starts automatically when you start the computer. Logging stops when an event log becomes full and cannot overwrite itself — either because you've set it for manual clearing or because the first event in the log is not old enough. To configure the Event Log Settings run Event Viewer *(Start » Programs » Administrative Tools (Common) » Event Viewer)* and Click on "Log Settings"

Log file size

It is good practice to keep the size of the log files large enough so that logging does not stop at any point. The initial maximum size of log files is 512 K.

Stated policy for log file size is 8192 K

To verify that the max. log file size has been set run Event Viewer and click on "Log Settings" and verify the "Maximum Log Size" for the System, Security and Application logs.

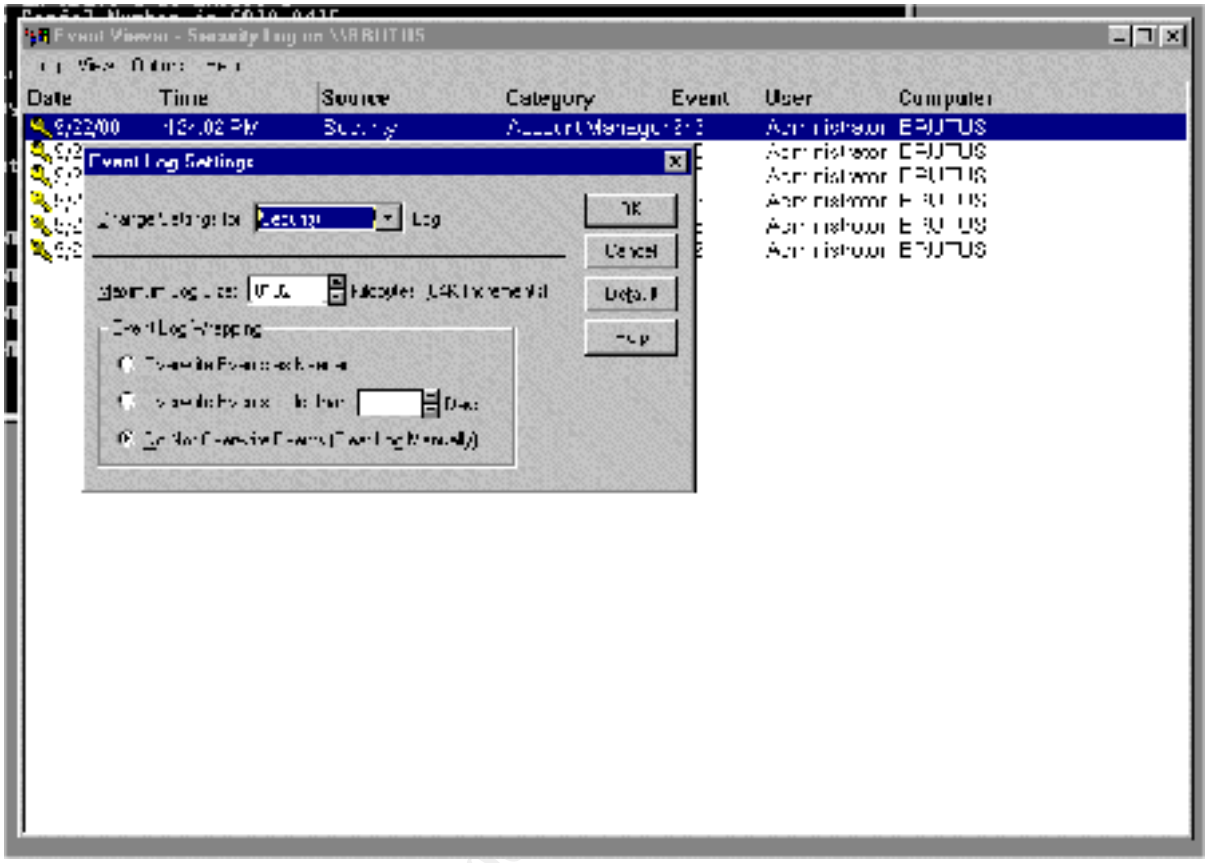

Figure 7: Event Viewer is used to determine the maximum size of the event logs

The size of the event log files can also be determined by examining the registry keys
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\EventLog\Application\"MaxSize".
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\EventLog\System\"MaxSize".
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\EventLog\Security\"MaxSize".
The value corresponding to 8192 K is 800000

Event Log Wrapping

Policies dictate that security logs cannot be overwritten and have to be cleared manually. The application and systems logs have to be set to overwrite events older than 7 days. Associated with this policy is the practice of dumping and clearing security logs manually every day. The other logs are dumped every week.

Batch jobs should be scheduled to run Somarsoft's DUMPEVT.EXE and dump and then clear the event log files.

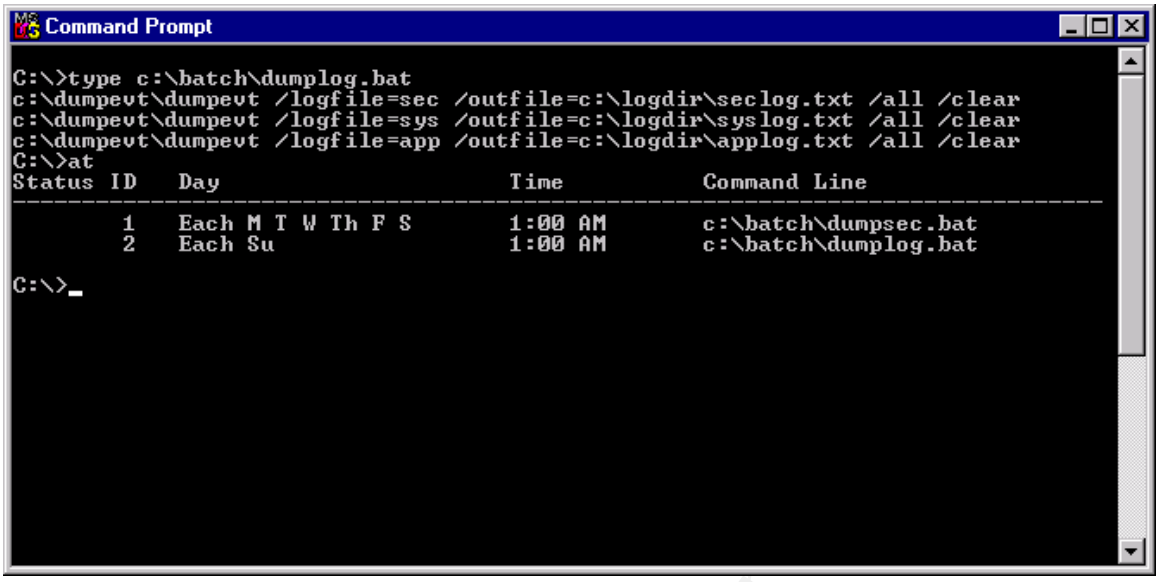

Figure 8: Somarsoft DumpEvent utility can dump event logs and clear them as well.

Secure Event Log Viewing

A default installation of Windows NT allows Guest accounts and null logons access to event logs. To secure this make the following changes to the default registry configuration to restrict Guest account[iii]

Hive	HKEY_LOCAL_MACHINE
Key	\System\CurrentControlSet\Services\EventLog\Application
Key	\System\CurrentControlSet\Services\EventLog\Security
Key	\System\CurrentControlSet\Services\EventLog\System
Value Name	RestrictGuestAccess
Type	REG_DWORD
Value	1

Secure access to the Event Log files

[iv]Each of the event logs is stored as an individual file in the \%Systemroot%\System32\Config folder. The file names are SysEvent.evt, SecEvent.evt, AppEvent.evt.

NTFS permissions on these files should be set so as to restrict access to only members of the Administrators group and the System account. These files should also be audited. The Administrators group should be audited for successful and failed access attempts and the Everyone group should be audited for failed attempts only.

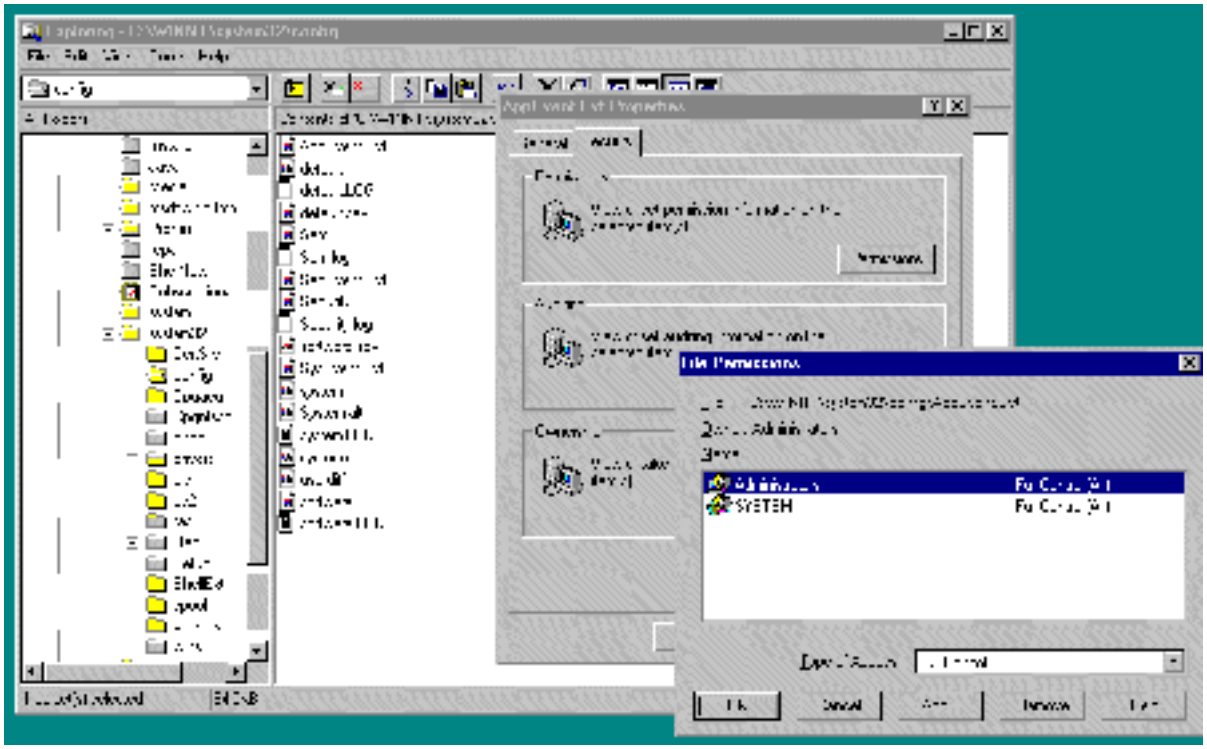

Figure 9: Windows Explorer is used to set permissions on the Event log files

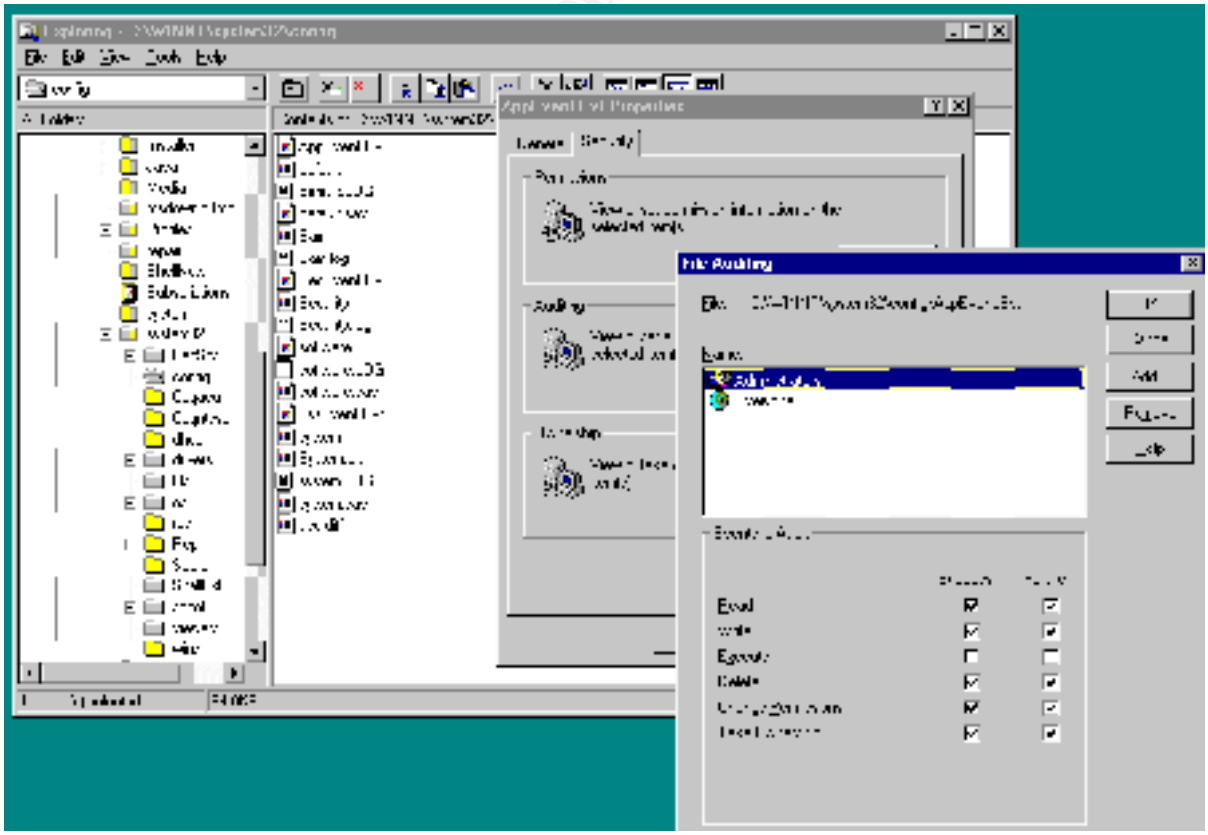

Figure 10: Windows Explorer is used to set up auditing on event log files.

Clear paging file at system shutdown

The paging file contains code and data from applications that require more memory than physically available. This data remains on disk even when the system is shutdown. There is a possibility of this data being compromised.[v]

Clearing the paging file eliminates this possibility of compromise. To force Windows NT to clear the page file at shutdown edit the following registry value

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Control\Session Manager\Memory Management
Value Name	ClearPageFileAtShutdown
Type	REG_DWORD
Value	1

Disable caching of logon information

Windows NT 4.0 has the capability to cache logon information in short-term memory. If the domain controller cannot be found during logon and the user has logged on to the system in the past, it can use those credentials to log on. If the Administrator disables a user's domain account, the user could still use the cache to log on by disconnecting the net cable. Disabling the cache results in a somewhat longer logon time, but prevents hackers from tapping logon information from short-term memory. [iii]The registry value that disables caching of logon information is

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows NT\CurrentVersion\Winlogon
Value Name	CachedLogonsCount
Type	REG_SZ
Value	0

Mitigating SYN floods

SYN floods are a common method of Denial of Service attack. They work as described below:

- Many TCP connection requests (SYN) are sent to the target computer with the source IP address in the packet "spoofed".
- Upon receiving the connection request, the target computer allocates resources to handle and track the new connection, then responds with a "SYN-ACK" to the "spoofed" IP address.
- Normally no response is received to the SYN-ACK. A default-configured Windows NT computer will retransmit the SYN-ACK 5 times, doubling the time-out value after each retransmission. The initial time-out value is three seconds, so retries are attempted at 3, 6, 12, 24, and 48 seconds. After the last retransmission, 96 seconds are allowed to pass before the computer gives up on receiving a response, and de-allocates the resources that were set aside earlier for the connection. The total elapsed time that resources are in use is 189 seconds.

A registry value setting reduces the number of SYN-ACK retries. [iv] This setting cannot totally eliminate the damage caused by SYN floods but can mitigate it to an extent.

Hive	HKEY_LOCAL_MACHINE\SYSTEM

Key	CurrentControlSet\Services\Tcipip\Parameters
Value Name	SynAttackProtect
Type	REG_DWORD
Value	2

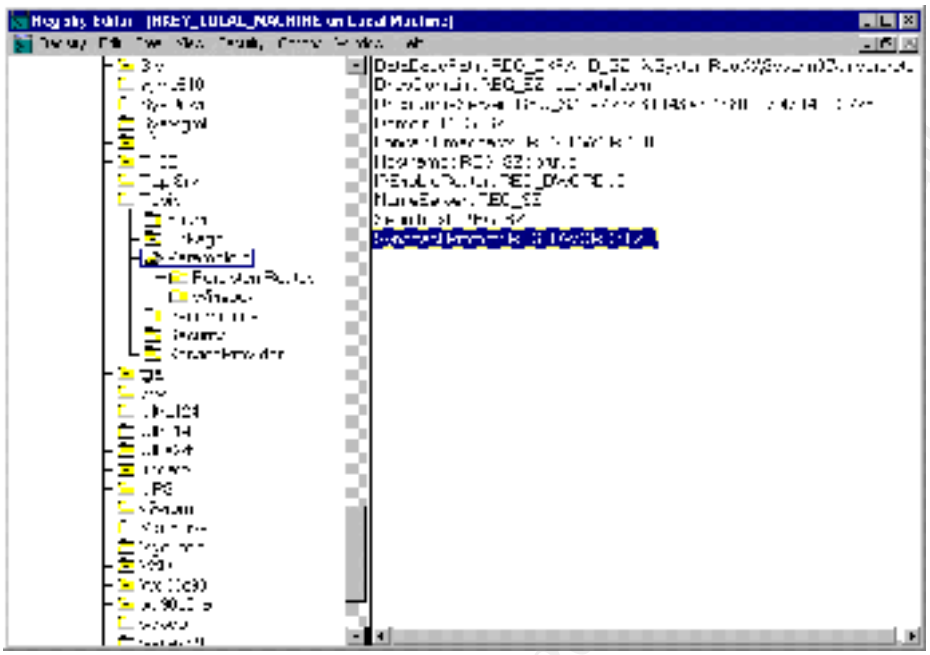

Figure 11: Registry Editor (REGEDT32.EXE) is used to create and verify the registry value to protect against SYN floods.

Restrict untrusted users' ability to plant Trojan horse programs

Trojan horses can take advantage of the Run utility if it is unguarded. There are some Trojan horses that are written to execute during an Uninstall operation. To restrict the ability of users to plant Trojan horse programs[vi]:

Use the Registry Editor (REGEDT32) to find the following keys:

Hive	HKEY_LOCAL_MACHINE\SOFTWARE
Key	Microsoft\Windows\CurrentVersion

Values Run, RunOnce, Uninstall (if present), AEDebug and all their subkeys

Select each subkey, click the Security menu, and then click Permissions

For each subkey set the permissions for Everyone and all untrusted users to a maximum of Read, and then click OK.

Securing the NETLOGON channel

The Netlogon channel is a two-way named pipe through which changes to the directory database stored on the PDC are synchronized with all BDC's. It is also used for Pass-through authentication. Every Windows NT computer, including BDC's and domain controllers in trusting domains, in a domain establishes a communications channel with the PDC at boot-up. By default communication on this channel is not encrypted and it is not checked for integrity (e.g. Digital signatures), thus exposing it to packet sniffing and man-in-the-middle attacks.[iv]

Hive	HKEY_LOCAL_MACHINE\SYSTEM

Key	CurrentControlSet\Services\Netlogon\Parameters
Value Name	RequireSignOrSeal
Type	REG_DWORD
Value	1

This causes all outgoing Netlogon channel traffic to be at least digitally signed and, depending on negotiation with a remote system, even encrypted.

Allow only Administrators to create new shares

This allows the administrator to control who can access a computer from its network interface and what information is shared over the network interface. To prevent non-administrators from creating shares, do the following:[vii]

Use the Registry Editor to find the following registry subkey:

Key	HKEY_LOCAL_MACHINE\SYSTEM
Subkey	CurrentControlSet\Services\LanmanServer\Shares

Select Shares and all its subkeys, click the Security menu, and then click Permissions. For Shares and each of its subkey, set the permissions for Everyone and all untrusted users to a maximum of Read, and then click OK.

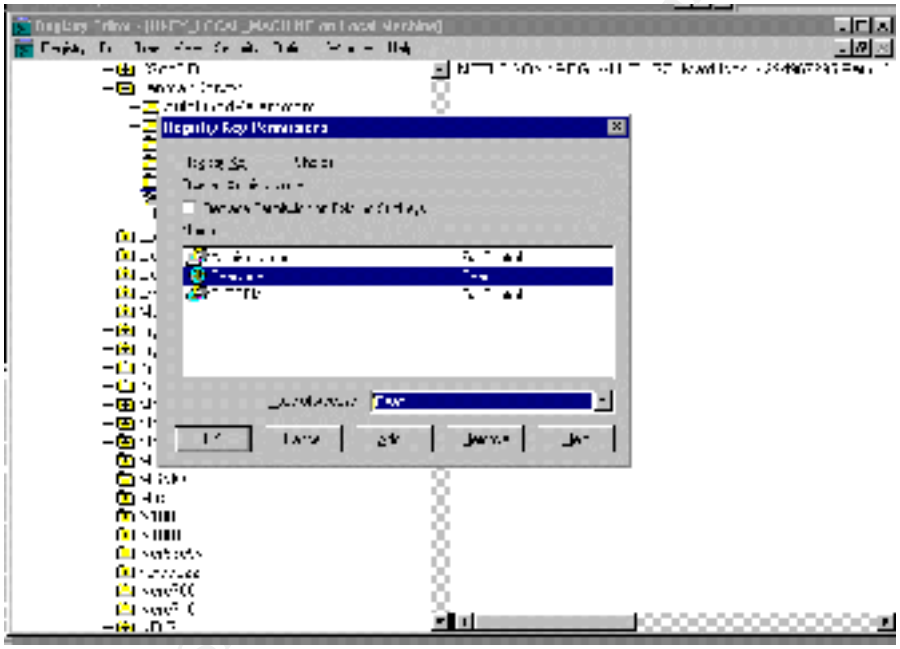

Figure 12: Use Registry Editor (REGEDT32.EXE) to restrict ability to create shares

Enabling NTLMv2 Authentication

Windows NT supports multiple authentication methods, i.e. LAN Manager (LM), Windows NT Challenge Response (NTLM v1) and NTLMv2.

Both the LM and NTLMv1 methods are inherently insecure because of the method in which they compute and transmit password hashes. Attackers using a readily available packet sniffer can easily grab data sent across the network and guess at the real password.

NTLMv2 overcomes some of the limitations of LM and NTLMv1

To set NTLMv2 as the default authentication method on all clients add the following registry key

Hive	HKEY_LOCAL_MACHINE\SYSTEM
Key	CurrentControlSet\Control\Lsa
Value Name	LMCompatibilityLevel
Type	REG_DWORD
Value	5

Notes

Some very common techniques of securing Windows NT have been left out of this document. Their exclusion from this document does not undermine their importance. Some are excluded because of the assumptions made at the beginning of this document. In a physically secure environment the following would not be emphasized

- Restricting access to server floppy and CD ROM drives only to interactive users
- Not displaying last logged on user name.

Some techniques may not be appropriate to all environments. These include

- Restricting null sessions from listing user ID's, from accessing shares, and accessing named pipes
- Disabling administrative shares

Other important security measures not listed here are

- Creating a "Honey pot" Administrator account after renaming the original account.
- Ensuring that the Guest account is disabled with a non-blank password.
- Securing the data through NTFS and share permissions other than the default.
- Controlling Network Access to the Registry
- Crash on Audit Failure

Reports

This section documents the findings of the investigations conducted in the previous section.
Server Name: BRUTUS
Date: Friday, September 22, 2000

Audit Item	Policy	Best Practice	Observation	Notes
SERVICE PACK INSTALLATION				
	SP6a	SP6a	Installed	Meets policy
FILE SYSTEM				
	NTFS	NTFS	NTFS	Meets policy
AUDIT POLICY				
Auditing enabled	Yes	Yes	Yes	Meets policy
Logon and Logoff-Success	Enabled	Enabled	Disabled	Does not meet policy
Logon and Logoff-Failure	Enabled	Enabled	Enabled	Meets policy
File and Object Access-Success	Disabled	Disabled	Disabled	Meets policy
File and Object Access-Failure	Enabled	Enabled	Enabled	Meets policy
Use of User Rights-Success	Disabled	Disabled	Disabled	Meets policy
Use of User Rights-Failure	Enabled	Enabled	Enabled	Meets policy
User and Group Management-Success	Enabled	Enabled	Enabled	Meets policy
User and Group Management-Failure	Enabled	Enabled	Enabled	Meets policy
Security Policy Changes-Success	Enabled	Enabled	Enabled	Meets policy
Security Policy Changes-Failure	Enabled	Enabled	Enabled	Meets policy
Restart, Shutdown and System-Success	Enabled	Enabled	Enabled	Meets policy
Restart, Shutdown and System-Failure	Enabled	Enabled	Enabled	Meets policy
Process Tracking-Success	Disabled	Disabled	Disabled	Meets policy
Process Tracking-Failure	Disabled	Disabled	Disabled	Meets policy
PASSWORD POLICY				
PASSFILT.DLL present in Systemroot\System32	Yes	Yes	Yes	Meets policy
Registry entry made				
HKLM\System\CurrentControlSet\Control\LSA\Notification Packages	Should have PASSFILT		Present	Meets policy
ACCOUNT POLICY				
Maximum Password Age (days)	90	90	90	Meets policy.

Audit Item	Policy	Best Practice	Observation	Notes
Minimum Password Age (days)	3	3	3	Meets policy.
Minimum Password Length (characters)	8	8	8	Meets policy.
Password Uniqueness (passwords)	4	10	4	Meets policy. Policy does not meet best practice
Account Lockout	Yes	Yes	Yes	Meets policy.
Account Lockout (bad attempts)	3	3	3	Meets policy.
Account Lockout (reset count in minutes))	120	20	120	Meets policy. Policy exceeds best practice
Lockout Duration (minutes)	1440 (1 day)	240	1440	Meets policy. Policy exceeds best practice
Forcibly disconnect remote users from server when logon hours expire	Yes	Yes	Yes	Meets policy.
Users log on to change password	Yes	Yes	Yes	Meets policy.
EVENT LOG				
Security Log size	8192 K		8192 K	Meets policy.
System Log size	8192 K		8192 K	Meets policy.
Application Log size	8192 K		8192 K	Meets policy.
Security Log wrapping	Never		Never	Meets policy.
System Log wrapping	7 days		7 days	Meets policy.
Application Log wrapping	7 days		7 days	Meets policy.
Frequency of dumping event log (sec/ app, sys)	1 day / 7 days		1 day / 7 days	Meets policy.
Frequency of clearing event logs (sec/ app, sys)	1 day /7 days		1 day / 7 days	Meets policy.
REGISTRY ENTRY FOR SECURE ACCESS TO EVENT LOG FILES				
HKLM\System\CurrentControlSet\Services\EventLog\Application\Restrict GuestAccess	1		1	Meets policy.
HKLM\System\CurrentControlSet\Services\EventLog\Security\ RestrictGuestAccess	1		1	Meets policy.
HKLM\System\CurrentControlSet\Services\EventLog\System\	1		1	Meets policy.

Audit Item	Policy	Best Practice	Observation	Notes
RestrictGuestAccess				
FILE PERMISSIONS APPLIED TO EVENT LOG FILES				
Restricted to group Administrators and account System	Restrict		Done	Meets policy.
CLEAR PAGING FILE AT SYSTEM SHUTDOWN				
HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management\ClearPageFileAtShutdown	1		1	Meets policy.
DISABLE CACHING OF LOGON INFORMATION				
HKLM\Software\Microsoft\Windows NT\Current Version\Winlogon\CachedLogonsCount	0		0	Meets policy.
MITIGATING SYN FLOODS				
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	2		2	Meets policy.
RESTRICT PLANTING OF TROJAN HORSES				
Permissions on HKLM\Software\Microsoft\Windows NT\Current Version\ Run RunOnce Uninstall AEDebug	Everyone set to Read only		Set as per policy	Meets policy.
SECURE NETLOGON CHANNEL				
HKLM\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal	1		1	Meets policy.
RESTRICT CREATION OF NEW SHARES TO ONLY ADMINISTRATORS				
Permissions on HKLM\System\CurrentControlSet\Services\LanmanServer\Shares	Everyone set to Read only		Set as per policy	Meets policy.

Audit Item	Policy	Best Practice	Observation	Notes
ENABLE NTLMV2 AUTHENTICATION				
HKLM\System\CurrentControlSet\Control\Lsa\LMcompatibilityLevel	5		5	

References

[i] Technical Reference Microsoft Windows NT 4.0 Security, Audit and Control By James G. Jumes, Neil F. Cooper, Paula Chamoun, and Todd M. Feinman - Chapter 13 Auditing Windows NT Security Features and Controls

[ii] Microsoft Windows High Availability Deployment Guide - Chapter 1 Introduction - Microsoft Corporation

[iii] Securing Windows NT 4.0 Installation. - Microsoft Corp.

[iv] Windows NT Security - Step by Step - Jason Fossen et al. SANS Institute

[v] Microsoft Knowledge Base Article Q182086 How to Clear the Windows NT Paging File at Shutdown

[vi] C2 Administrator's and User's Security Guide - Microsoft Corp.

[vii] Windows NT C2 Configuration Checklist - Microsoft Corp.