Global Information Assurance Certification Paper

The Technical Security Assessment Audit

J. Malinda Armstrong
Senior Security Analyst
Student# 941
SANS – New Orleans
Feb. 2001 NT Step by Step

An effective security posture is the key to any organization's ability to perform its critical missions. An effective IT Security Program is a business enabling process, which provides a road map to move an organization from near-term tactical security implementations to long-term strategic planning.

The recommended approach is to first assess the current environment's business vulnerabilities, policies/procedures, real threats, risk assessment and risk-management strategy. The 2nd step is to close exploitable holes, including physical protection, configure systems for protection, implement fixes, vendor updates, develop procedure sand guidelines, training and education, independent assessment and crisis plan. Architect, Design, Develop, and Documentation is the 3rd phase and will provide implementing an Enterprise Security Program with Security policy, strategic plans and a security life cycle. The requirements of this phase include security architecture, technology standards, product standards application development and guidance. The last step will be to strategically deploy technology, which includes strong authentication, authorizations, encryption, data control, auditing Trust domains and relationships, virus detection, firewalls, and security administration tools.

As part of the first step in the development of strong security plan, the identification of the vulnerabilities and basic security weaknesses are established with the Technical Security Assessment. Closing known exploitable holes and implementing an ongoing security-testing program to detect new holes will set a baseline for security. This will provide a sound information assurance program and the momentum and enthusiasm to move to the next steps, beginning with closing the exploitable holes.

Configuring all servers to protect against internal threats requires close reviewing for servers and determining possible scenarios for attacks or hacks that could be implemented from inside the firewall. Upon the identification of these possible vulnerabilities solutions should be developed and implemented to provide a higher degree of security for all systems

If an attacker were to get behind the firewall, if the firewall was compromised, or an insider attack occurs, the network is wide open. Here is a conceptual look at the Defense in depth approach to security.

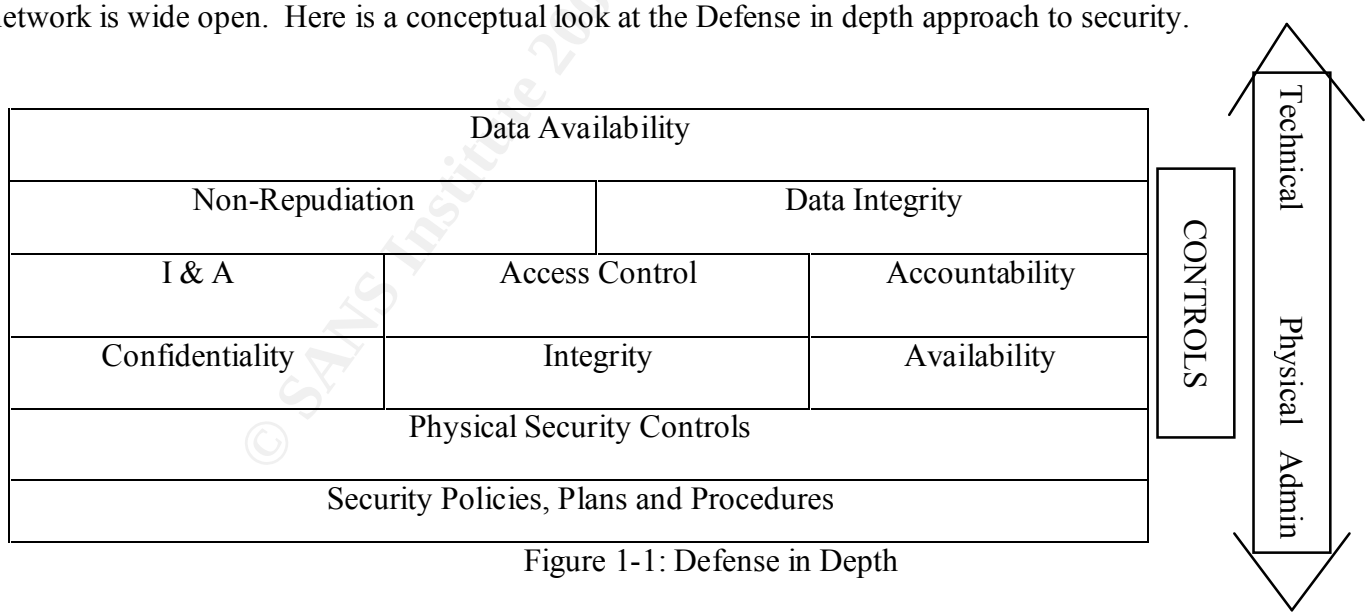


Figure 1-1: Defense in Depth

The basic concept is that if one method fails to stop an attacker, an organization has other methods in place to possibly stop the attack or, at least limit the damage it can cause.

Analysis

The following section list all the vulnerabilities, threats, risks and recommended solutions for all information audited by the security team. Security Requirements are standards by which the security of systems, applications and devices can be assessed. The requirements are based on security policies in place and standard best practices used throughout the industry.

The audit covers the following topics for Windows NT 4.0 security.

1.1 Physical Location

2.1 Server Configuration
- 2.1 Disk Partitions
- 2.2 Protocols
- 2.3 Bindings
- 2.4 Services
- 2.5 Devices
- 2.6 Subsystems
- 2.7 Emergency Repair Disks
- 2.8 Syskey Protection
- 2.9 System Page File
- 2.10 System Usage Polices
- 2.11 Service Packs and Hot Fixes

3.1 Account Management
- 3.1.1 Control access from network
- 3.1.2 Password configurations
- 3.1.3 Administrator account
- 3.1.4 Administrator account password
- 3.1.5 Guest account
- 3.1.6 Anonymous User
- 3.1.7 User name cache

4.1 Null sessions and pipes
- 4.1.1 Restrict null sessions
- 4.1.2 Control null session access to shares
- 4.1.3 Control null session access to named pipes

5.1 File and Registry Access
- 5.1.1 System root lock down
- 5.1.2 Shared level access control
- 5.1.3 Administration shares
- 5.1.4 Restrict network access to registry
- 5.1.5 Authentication
- 5.1.6 SMB Signing

6.1 Auditing
- 7.1.1 Audit Logs
- 7.1.2 Secure access to Event Log File
- 7.1.3 User Manager Audit Policy

8.1 Anti-Viral Software

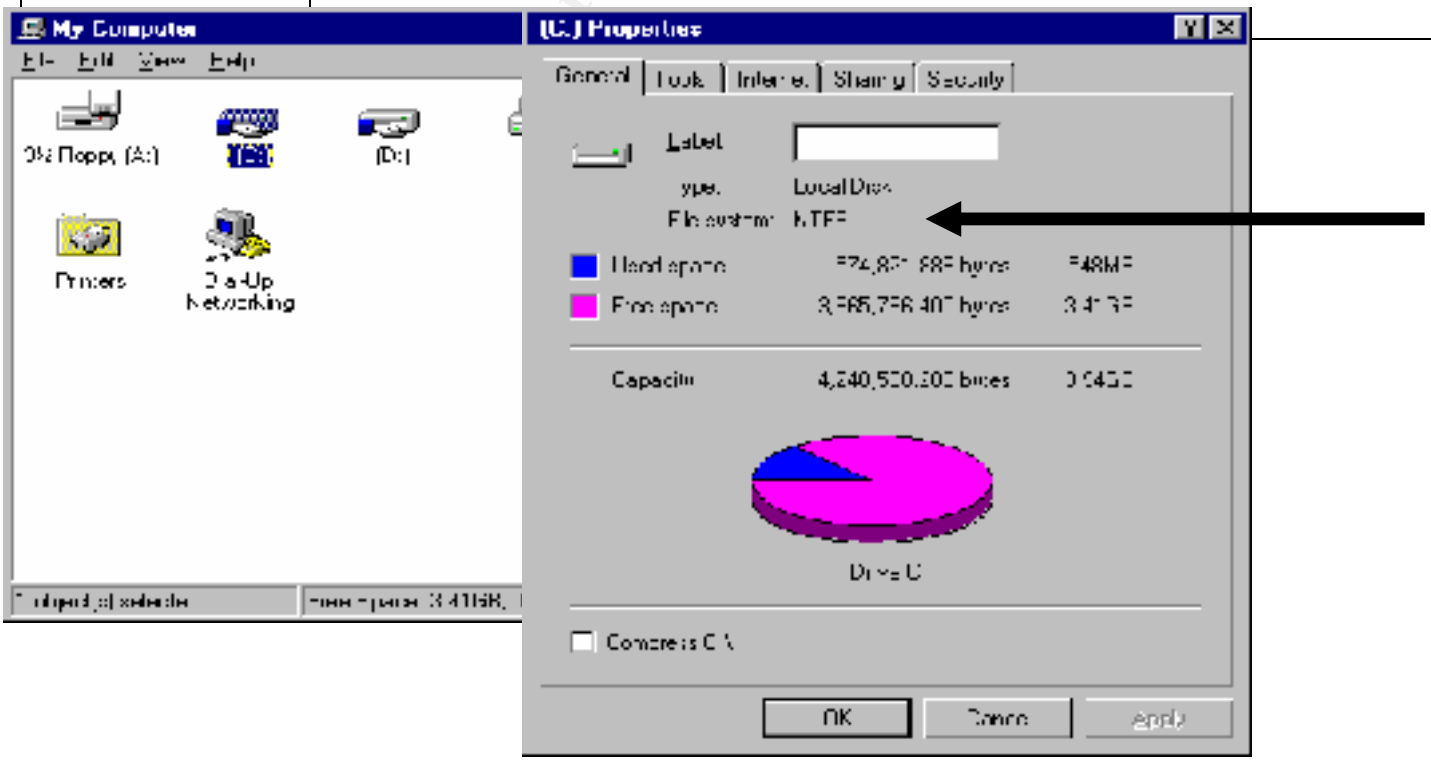
Auditors will use the DumpReg or DumpSec utilities to view Registry Keys. The System Policy Editor will also be used as a tool to view registry lookups. The auditors will note on their findings if the control is enabled or control is not enabled and if compensating controls are evident or not. A date will be set at the time of the audit for a Rescan of the server to verify controls are enabled to meet the company security guidelines. Not all recommendations will be suitable for a particular server in it's own environment and any concerns will be duly noted and documented.

Auditor		Company	
Audit #		Department	
Date		Server Type	
Administrator		IP Address	
		DNS Name	

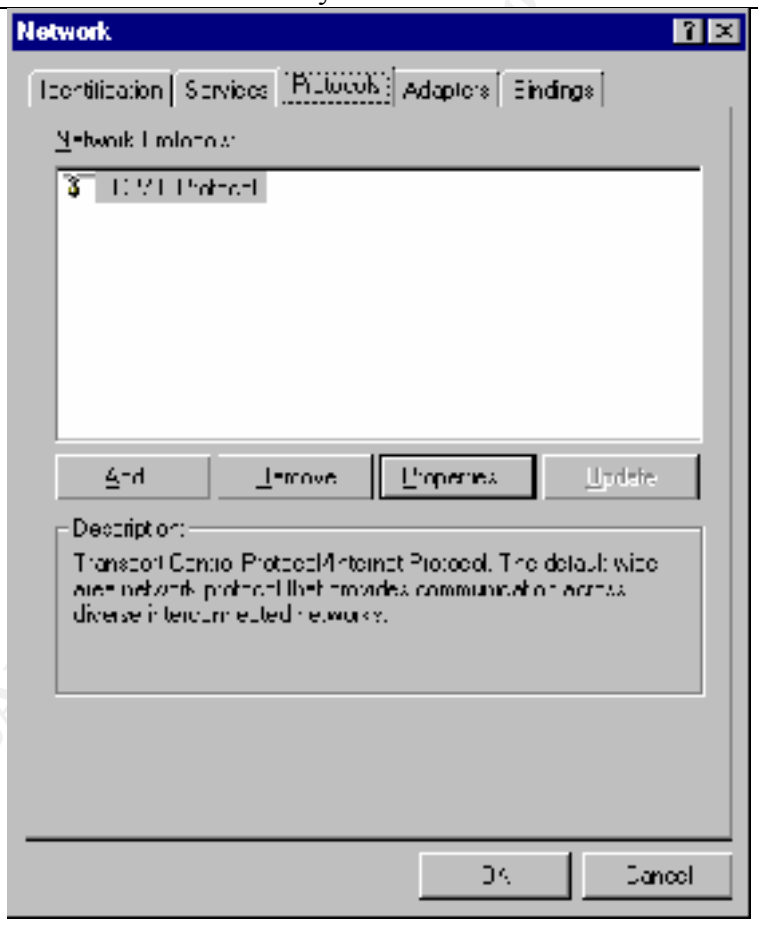
Findings	Control Enabled	Control not Enabled w/compensating controls
	Control not Enabled	

Security Policy 1.1 – Physical Location	
Best Practice	Physical Servers should be behind locked doors. There should be a continuous audit of who enters and leaves the area.
Risks	Access to the firewall, servers or related network cabling provides opportunities for an intruder to bypass the firewall itself
Test	Attempt to use social engineering skills to access server area
Findings	
Remediation	Recommendation is electronic surveillance and admittance

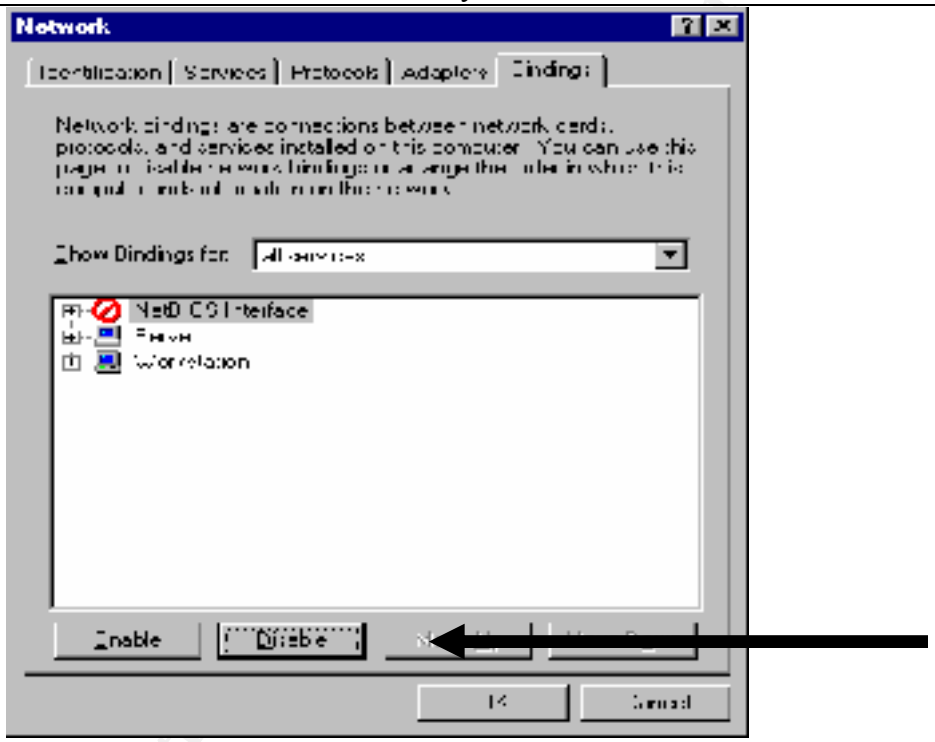
Security Policy 2.1 – Server Configuration	
2.2 Disk Partitions	
Best Practice	Partitions should be NTFS format otherwise auditing features will not be able to be activated.
Risks	Unauthorized access. Destruction or modification of system resources
Test	Open My Computer → right click on drives → click on Properties → Note File System



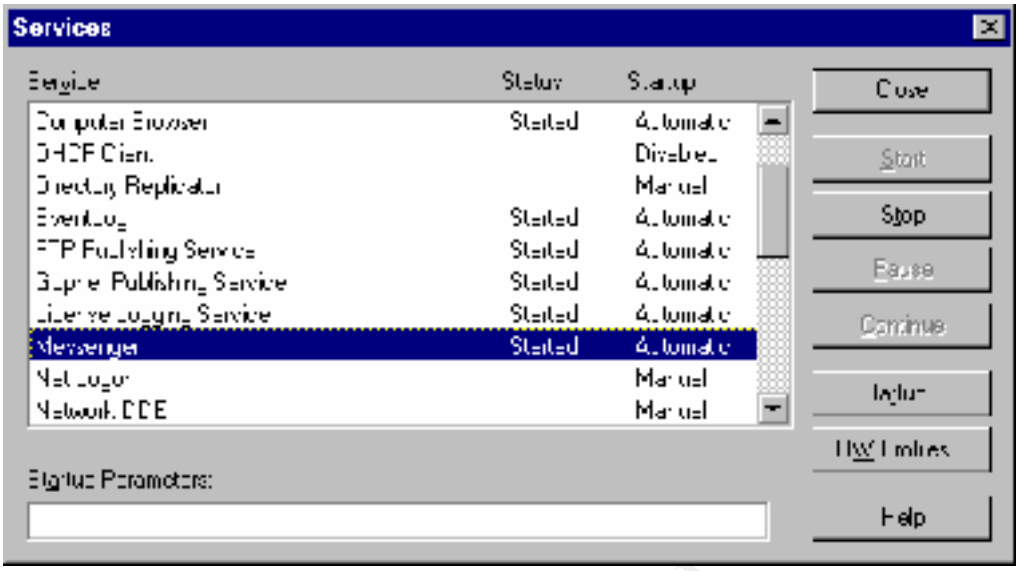
Findings	
Remediation	Use convert utility to convert FAT to NTFS • Use the fixacis.exe utility to reset them from the default access Everyone: Full Control.
2.3 Protocols	
Best Practice	Do not load unnecessary protocols. Protocols allow a hacker to move freely between systems on the network and find weaknesses.
Risks	Denial of Service Attacks
Test	Inquire to Administrator Protocols. Verify protocols loaded. Right click on Network Neighborhood → click on Properties → Protocols → Note Protocols
Findings	
Remediation	Right click on Network Neighborhood → Properties → Protocols → click on "protocol" → click Remove NOTE: Firewalls should only have TCP/IP



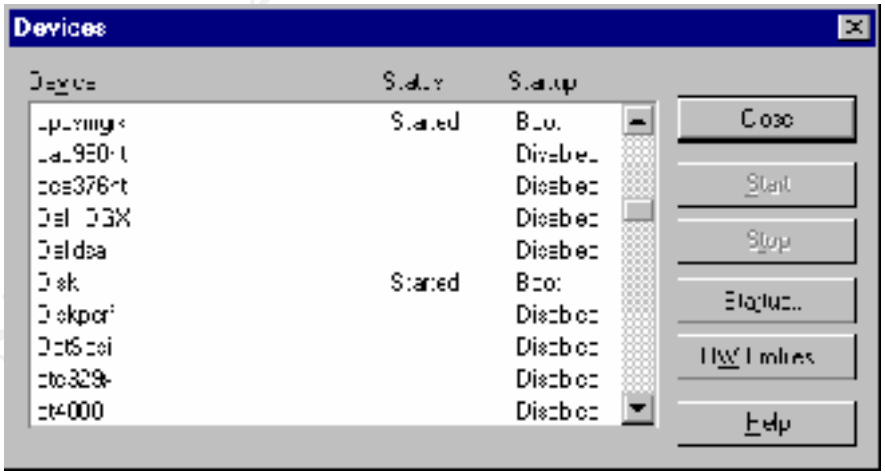
2.4 Bindings	
Best Practice	Remove unnecessary bindings to prevent hacker from moving freely between systems on network and finding weaknesses.
Risks	Denial of Service Attacks
Test	Inquire to Administrator. Verify bindings Right click on Network Neighborhood → Properties → Bindings → Note Bindings
Findings	
Remediation	Right click on Network Neighborhood → Properties →Bindings → "service → Disable NOTE: Firewalls should only have TCP/IP



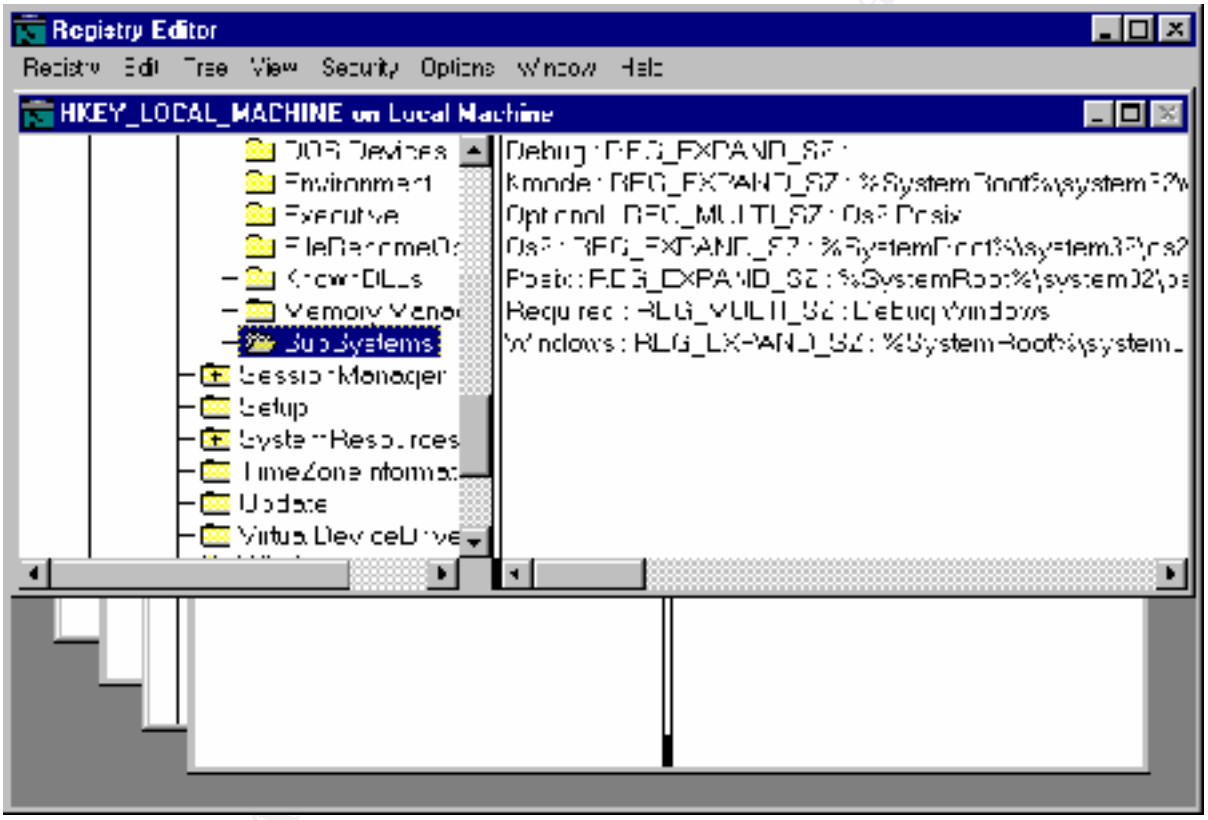
2.5 Services	
Best Practice	Install and configure as few services as possible
Risks	Unauthorized access. Destruction or modification of system resources
Test	Inquire Administrator. Start → Settings → Control Panel → Services NOTE the services enabled
Findings	
Remediation	Start → Settings → Control Panel → Services NOTE: # of services is unique to the server NOTE: Firewalls should not have RPC, Net Bios, Workstation, Server or ComputerBrowser enabled Recommended services to discontinue on a member server are Messenger, FTP, RAS, IP forwarding and GOPHER (IP forwarding is left on for firewalls)



2.6 Devices	
Best Practice	Install and configure as few devices as possible
Risks	Unauthorized access. Destruction or modification of system resources
Test	Inquire Administrator. Start → Settings → Control Panel → Devices NOTE the devices enabled
Findings	
Remediation	Start → Settings → Control Panel → Devices NOTE: # of devices is unique to the server Recommend devices to disable if not being used are modem, usb, remote access, serial Ps/2 and Alerter

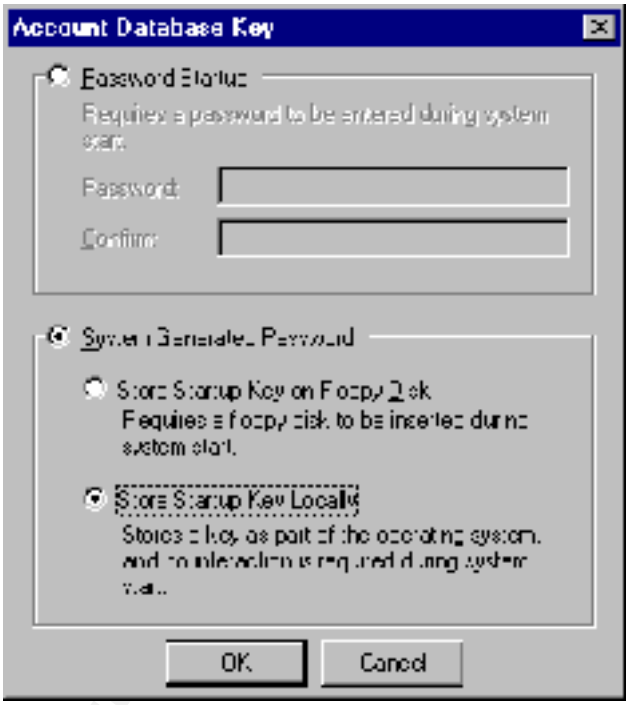


2.7 Subsystems.	
Best Practice	Domain controllers should not have more than one OS installation. Subsystems can degrade existing NT security and introduce new vulnerabilities
Risks	Denial of Service Attacks
Test	Use DumpReg utility → Report → Dump Registry → HKEY_LOCAL_MACHINE → CTL-F → Os2LibPath NOTE: if in registry
Findings	
Remediation	Make back up of registry. Remove these subsystems by performing the following registry actions. HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → Session Manager → SubSystems → key "Os2/Posix" → Edit → Delete Reboot to make changes in effect

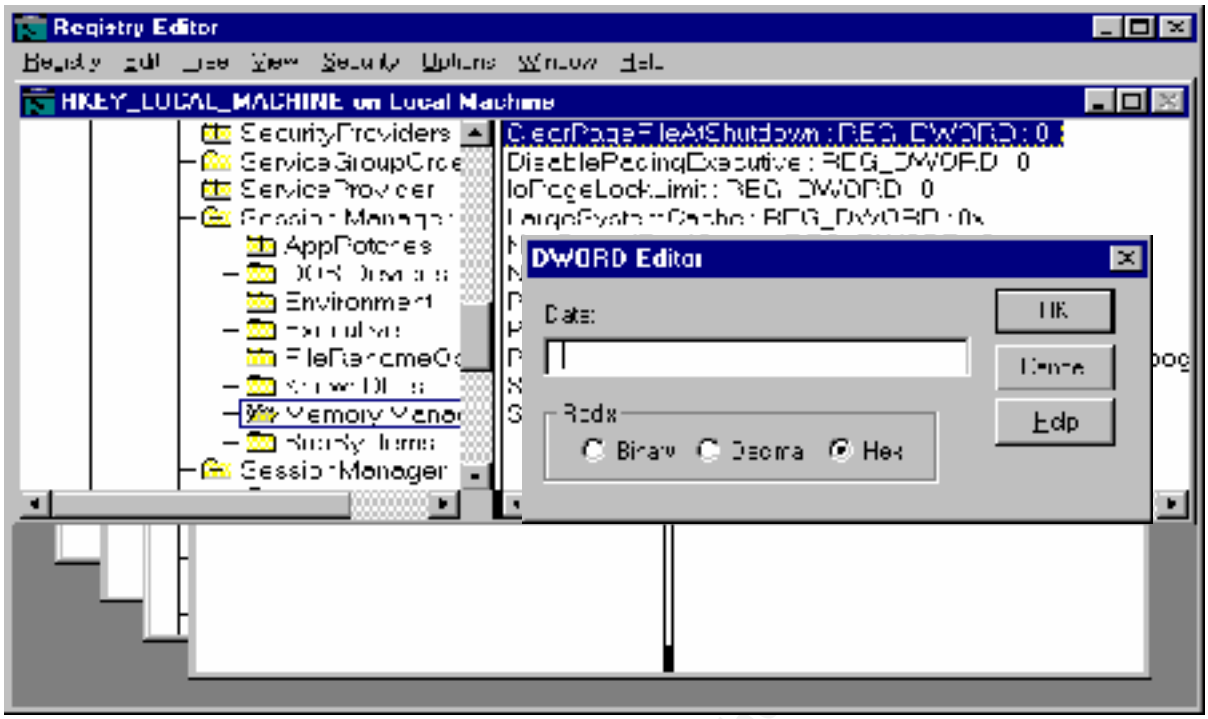


2.8 Emergency Repair Disk	
Best Practice	Recent Emergency Repair Disk should be maintained along with Emergency NT Boot Disk, Setup Disks and MS-DOS Boot Disk
Risks	Data loss, productivity, and time loss. Bottom line is money
Test	Ask Administrator to review disks. Check dates and files on disks. Make sure they are stored in a secured area.
Findings	

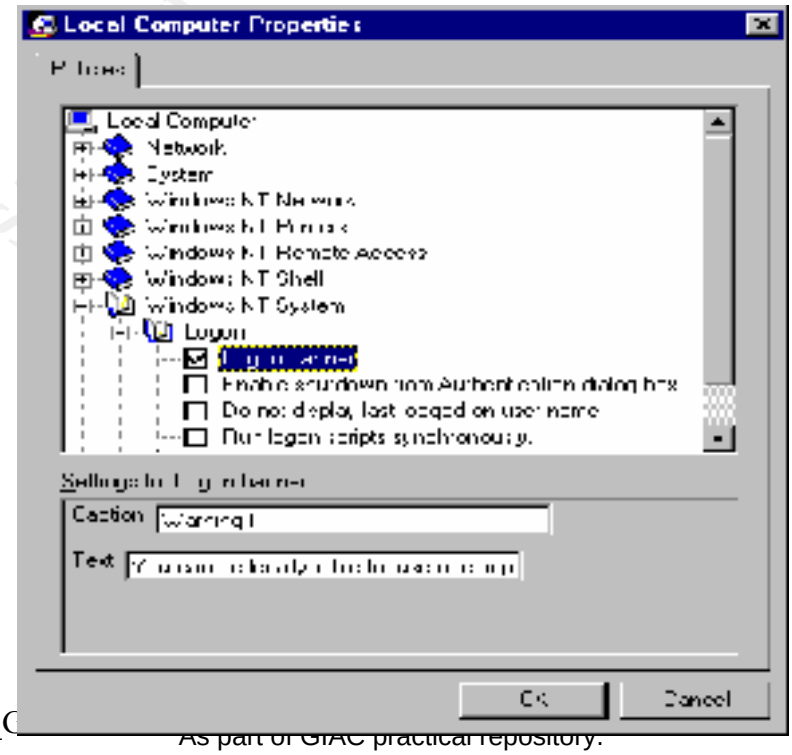
Remediation	Create ERD • Execute the RDISK /s utility in the \%SystemRoot%\System32 subfolder. • When prompted insert disk when files are ready to be copied. • Use the /s switch to copy the current SAM to the ERD Create Emergency NT Boot Disk • Contains NTLDR, BOOT.INI and NTDETECT.COM • if computer has a SCSI boot drive which does not have BIOS enabled, the disk will also contain NTBOOTDD.SYS Create Setup Disks • Execute WINNT /ox command in the Run line (creates 3 bootable disks) Create MS-DOS Boot Disks • Start MS-DOS. Put a blank floppy disk in drive A. • Type format a: /s and press ENTER. • You must specify the /s switch to make the floppy disk bootable. This switch causes the format program to copy the file Command.com to the floppy disk. • Copy other MS-DOS-based utilities that you might want to use to the floppy disk. At a minimum, you should copy these files: · Attrib · Copy · Format · Fdisk · Mem · Sys.com · a text editor · DiskSave PLACE DISKS IN A SECURED AREA.
2.9 Syskey Protection	
Best Practice	System key provides the capability to use strong 128-bit encryption on the SAM database.
Risks	Unauthorized access. Destruction or modification of system resources
Test	Run password-cracking program L0phtcrack to determine whether passwords are encrypted (do not run the brute force option) L0phtcrack.exe → Tools → Options → Unclick Enabled under Brute Force Attack → File → Import SAM file (C:\winnt\repair) → SAM_ → View accounts & passwords
Findings	
Remediation	NOTE: Update ERD before running syskey and make a 2nd ERD after installing syskey • At the Run Command type syskey and press enter → Encryption Enabled → OK → Store Startup Key Locally → OK → Reboot



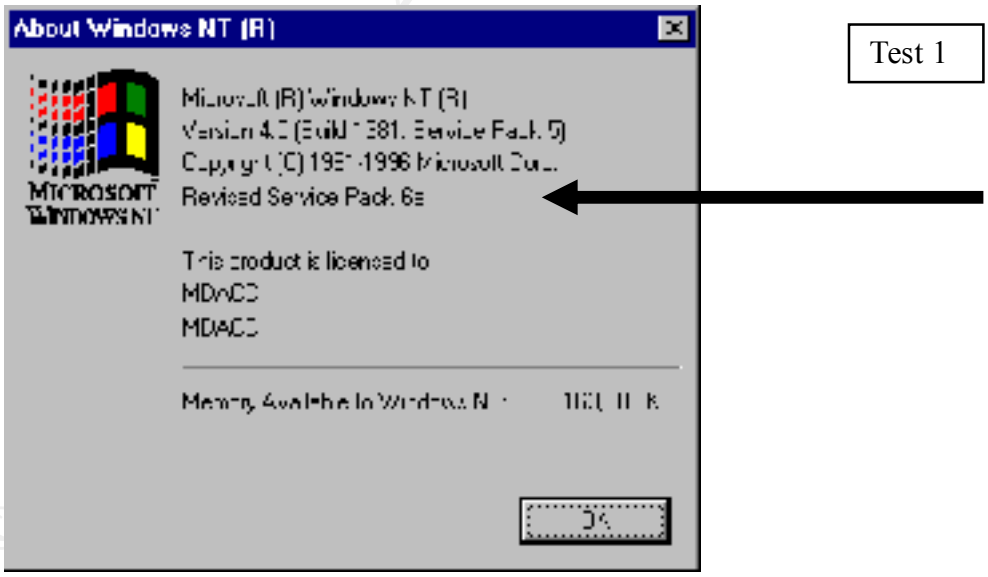
2.10 System PageFile	
Best Practice	Wipe Page file at system shutdown
Risks	Unsecured data
Findings	
Test	Use DumpReg utility → Report → Dump Registry → HKEY_LOCAL_MACHINE → CTL-F → ClearPageFileAtShutDown NOTE: value in registry
Remediation	Back up registry. Change key value At Run Command type regedt32 and press enter Click on HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → SessionManager → Memory Management → ClearPageFileAtShutDown → Edit → DWORD → type in 1 for Data → click OK → Reboot for changes to take effect

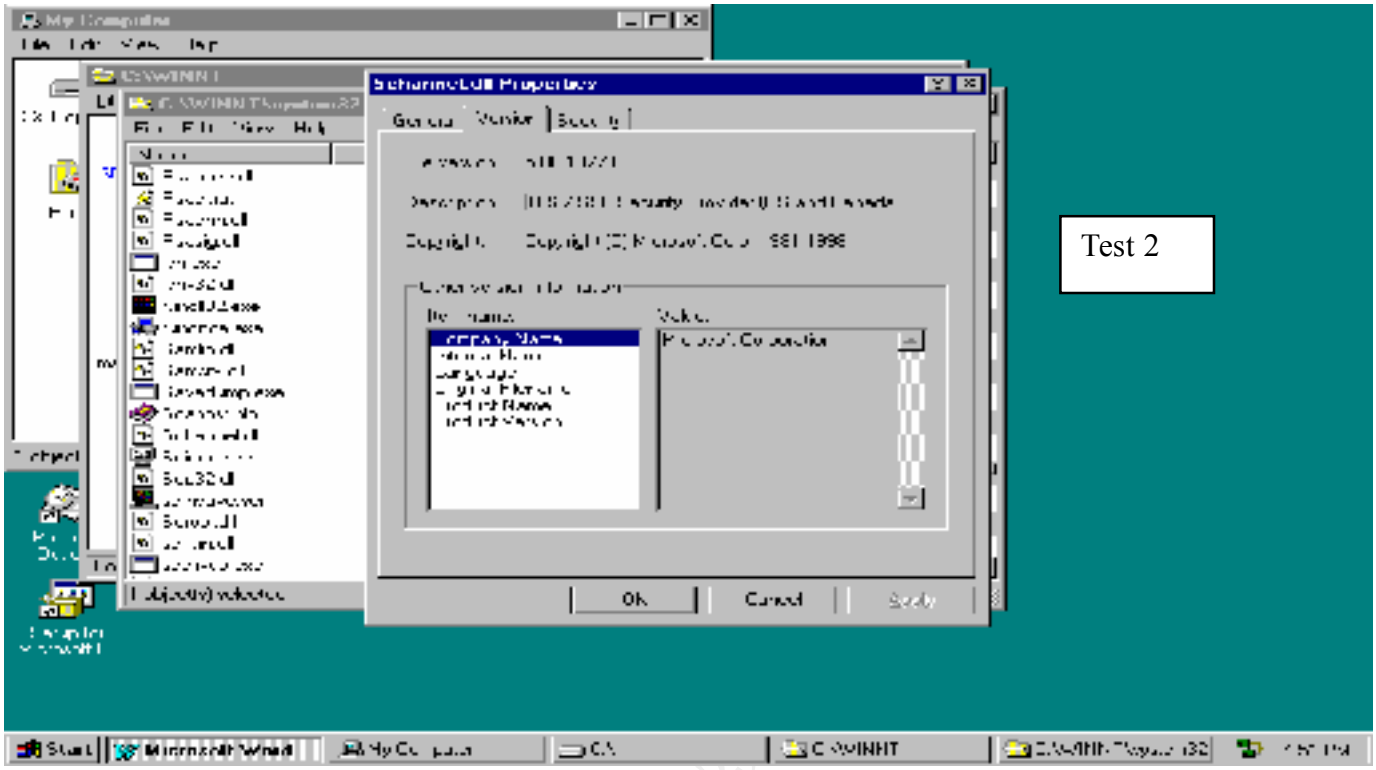


2.11 System Usage Policy	
Best Practice	Display warning message that notifies potential users that they can be legally liable if they attempt to use the computer without have been properly authorized to do so.
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	
Remediation	Start → Programs → Administrative Tools → System Policy Editor → File → Open Registry → Edit → Properties → Windows NT System → Logon → Logon Banner → Caption type WARNING! → Text → type "legally liable . . . " → OK



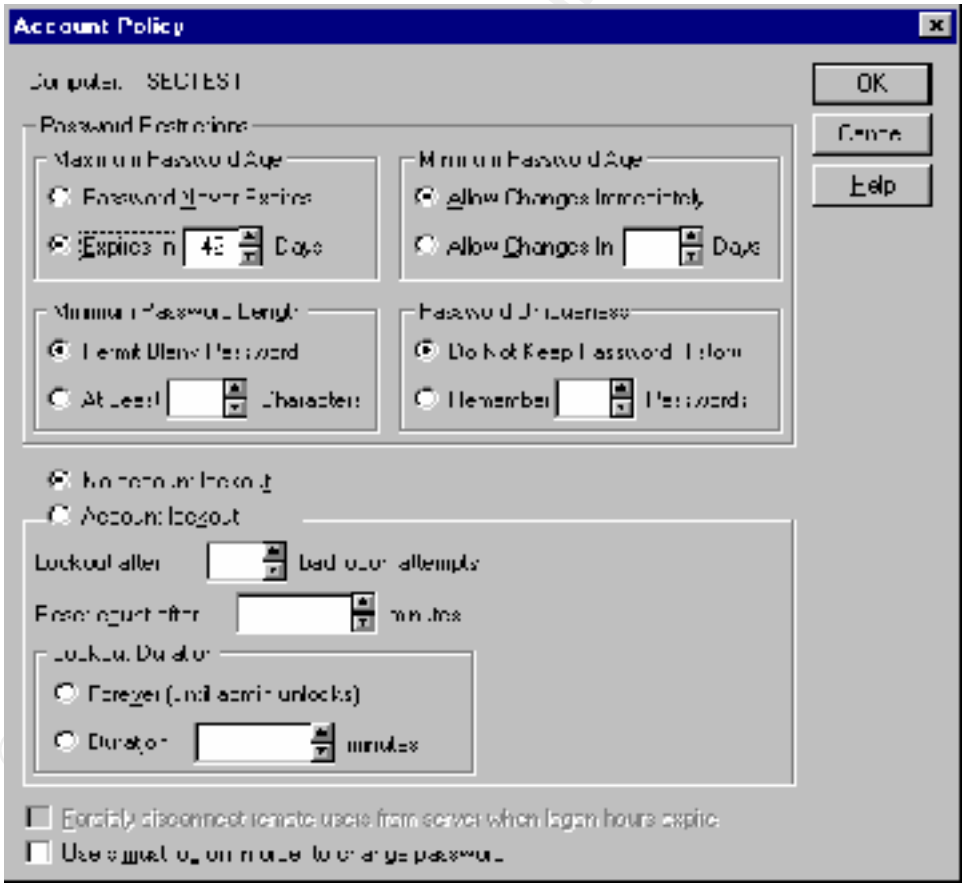
2.12 Service Packs and Hot Fixes	
Best Practice	Service Packs include all security fixes from previous service packs. Microsoft recommends you keep up to date on service pack releases and hotfixes. Service Packs must be reapplied whenever configuration of server changes.
Risks	Denial of Service Attacks
Test	1. At the Run Command type "Winver" and press enter. Note the service pack installed 2. Check encryption level → Open My Computer → c:\WINNT\System32 Right click on Schannel.dll → click on Properties → click version tab and view description NOTE: Export version is 40-bit/U.S. domestic version is 128-bit
Findings	
Remediation	Download and install service packs. http://www.microsoft.com/ntserver/nts/downloads Microsoft issues security bulletins through its Security Notification Service. Upon receiving bulletin notice of security hotfix, you should immediately download and install the hotfix on your servers. These are available at the Microsoft download center. http://www.microsoft.com/security

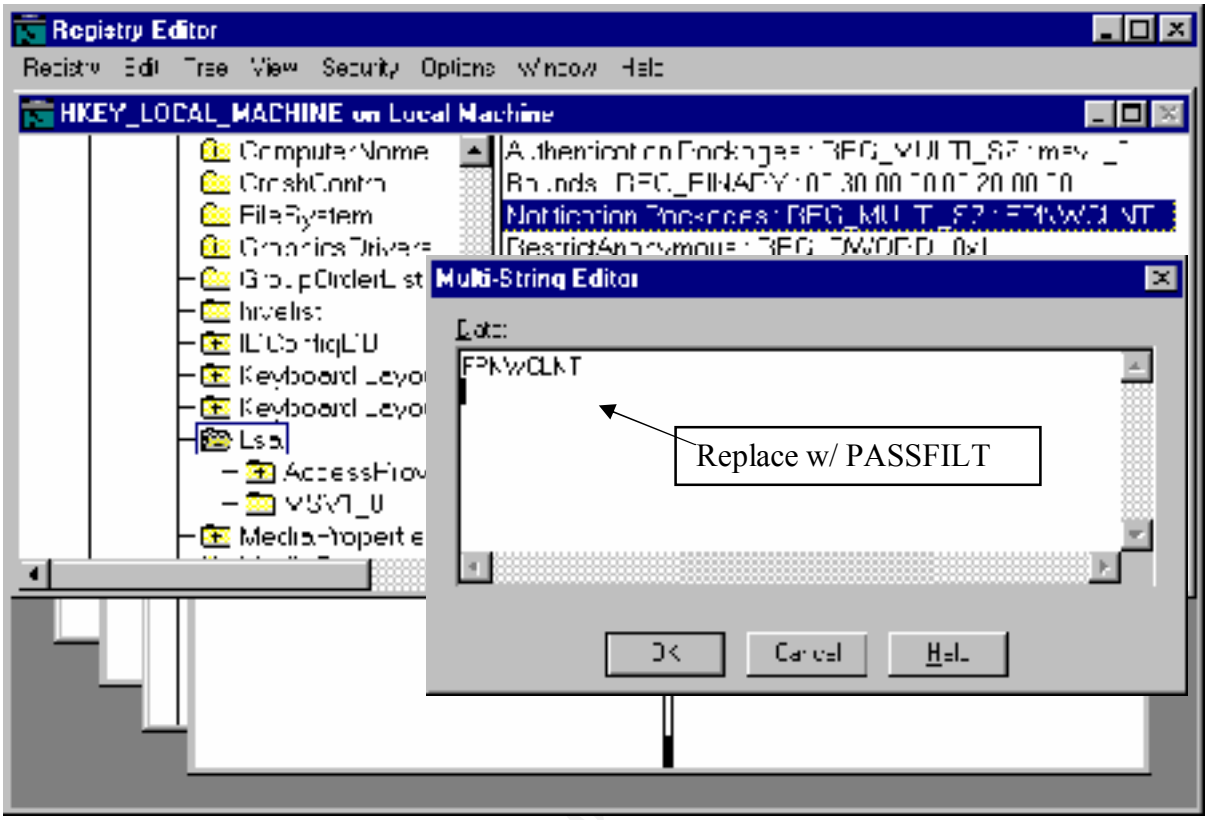




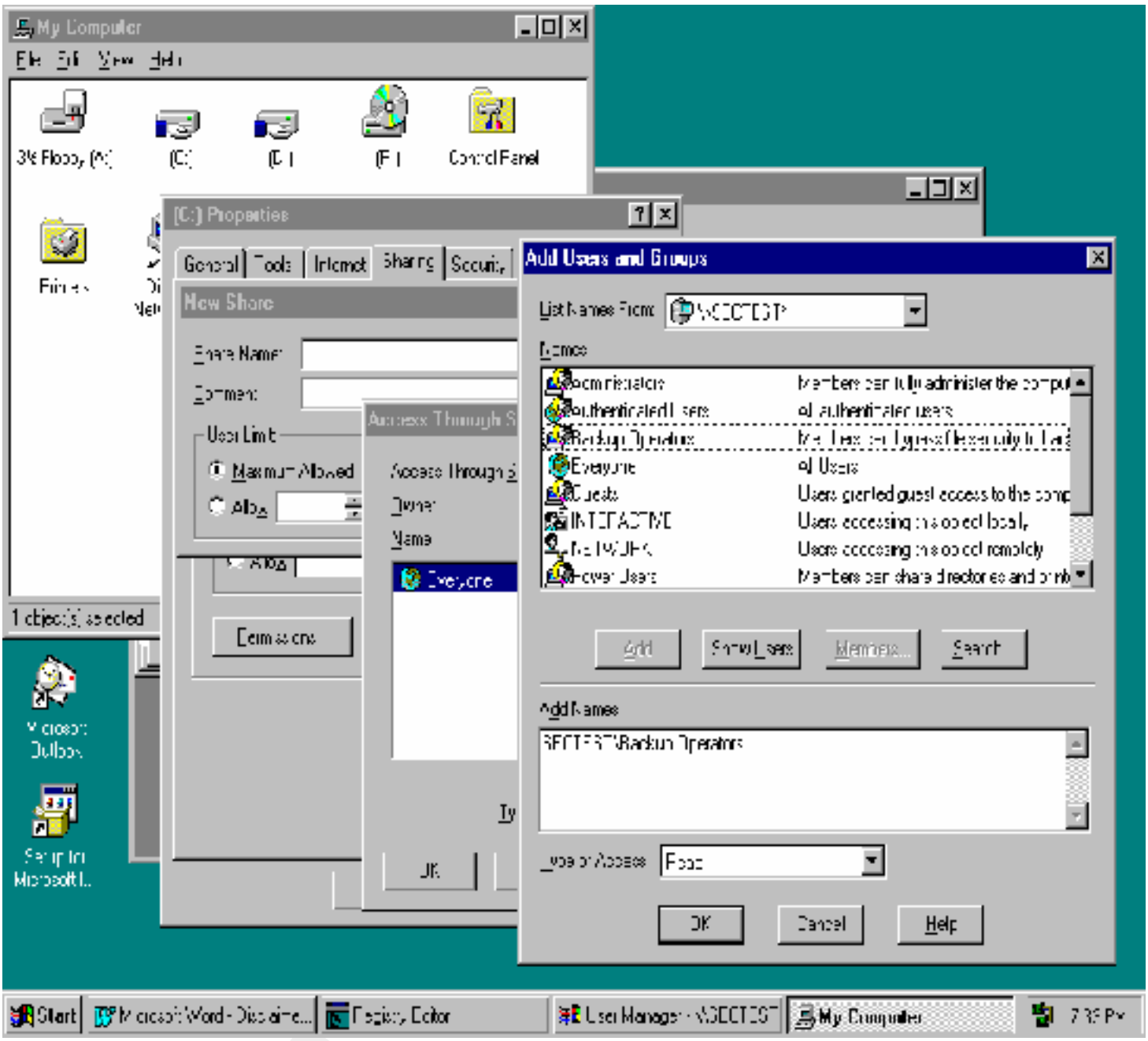
Security Policy 3.1 – Account Management	
3.2 System Accounts	
3.2.1 Password Configuration	
Best Practice	Strengthen password policies and Disable Blank passwords
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	Use DumpSec utilities. DumpSec → Report → Dump Policies NOTE: password polices
Remediation	Click on Start → Programs → Administrative Tools → User Manger for Domains → Policies → Account Recommend Policy : • Maximum password 30-60 days, • Minimum password 7 days, • Minimum password length 8 characters, • Password Uniqueness 10 password, • Account lockout, • Account lockout lockout after 3 tries, • Lockout Duration Forever,Forcibly disconnect remote users • Users must log on in order to change password

Additional Information:	1) Strong passwords may be implemented using the passfilt.dll program available with Service Pack 3. 2)Allows you to enforce strong password rules for password changes. 3)At least 6 character long, 4) May not contain user account name, or any portion of the user's full name, 5)Must contain characters from 3 of the following: uppercase, lowercase, numeric, and non-alphabetic punctuation characters To install, make the following Registry change (always backup registry 1st) Backup registry → type at run command regedt32 → HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → LSA → Notification Packages - → ReG_MULTI_SZ → replace FPNWCLNT with PASSFILT → Reboot The NT Resource Kit includes a tool, passprop.exe -Allows you to turn on complex password check and to lock out the administrator account, /complex switch turns on a requirement that all passwords must have at least one uppercase letter, one number, or one ASCII symbol, /adminlockout switch allows the administrator account to be locked out

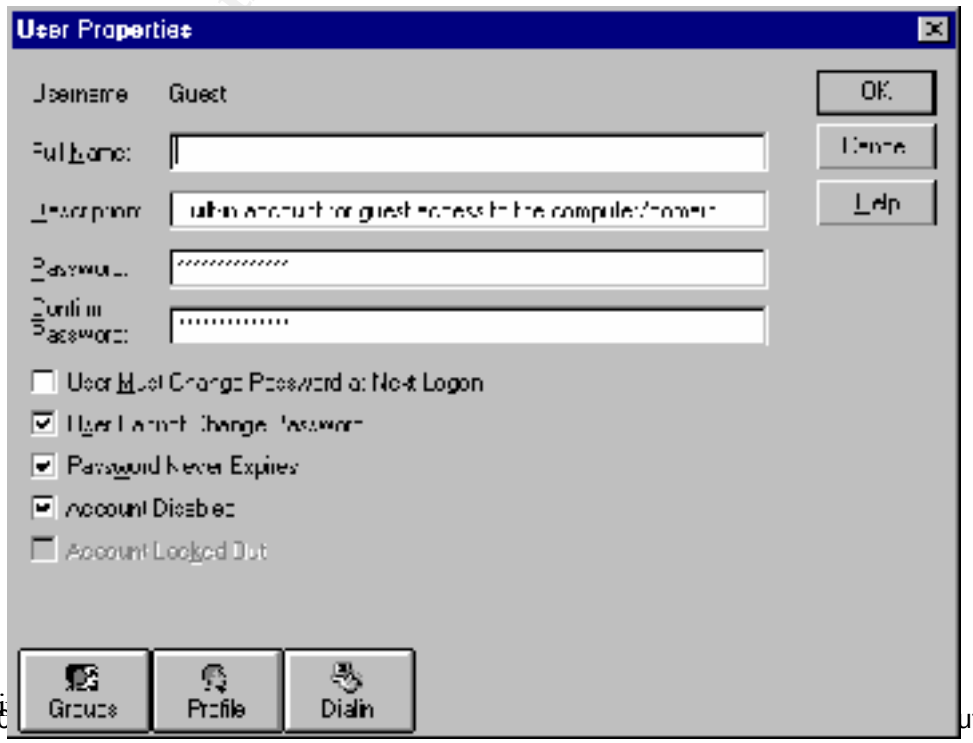




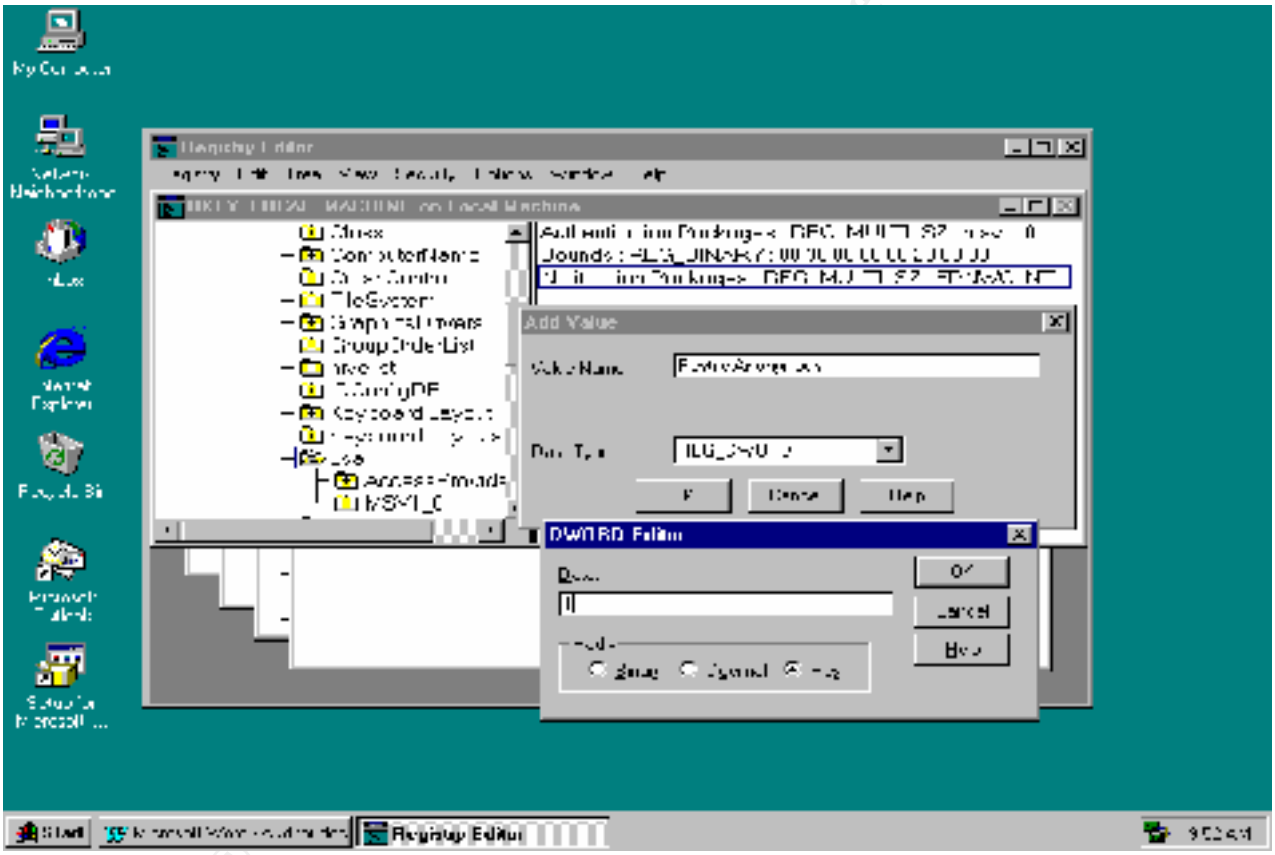
3.2.2 Access computer from network	
Best Practice	Replace Everyone Group with Authenticated Users Group
Risks	Unauthorized access. Destruction or modification of system resources
Test	Login with user account → type at run command \\computername\share
Findings	
Remediation	Right click on drives, file folders devices → Sharing → New Share → type Share Name → Permissions → Add → Group → Add – Type of Access → OK → Everyone Group → Remove → OK → Add → Authenticated Users → Add → Type of Access → OK →OK



3.2.3 Administrator account	
Best Practice	Assign administrators two accounts – one for e-mail and general work and a second for performing administrative tasks
Risks	Unauthorized access. Destruction or modification of system resources
Test	Try logging on as Administrator with no password (default)
Findings	
Remediation	• Rename account and establish a decoy account named Administrator with no privileges. • Enable account lockout on the real Administrator account with passprop utility. • Disable the local machine Administrator account
3.2.4 Administrator account – password	
Best Practice	Administrator account must have a strong password
Risks	Unauthorized access. Destruction or modification of system resources
Test	Run L0phtcrack utility (take off brute force attack)
Findings	
Remediation	Ask Administrator to change password. Recommended is minimum of 8 characters and numbers, Lower and Upper case and symbol.
3.2.5 Guest account	
Best Practice	Disable "known" Microsoft accounts Service Pack3 and forward disable the account
Risks	Unauthorized access. Destruction or modification of system resources
Test	Start → Programs → Administrative Tools → User Manager for Domains NOTE if account is enabled.
Findings	
Remediation	Start → Programs → Administrative Tools → User Manager for Domains → Guest (double click) → check Disable Account. Recommendation: Create a unique user id for guest with an expiration date



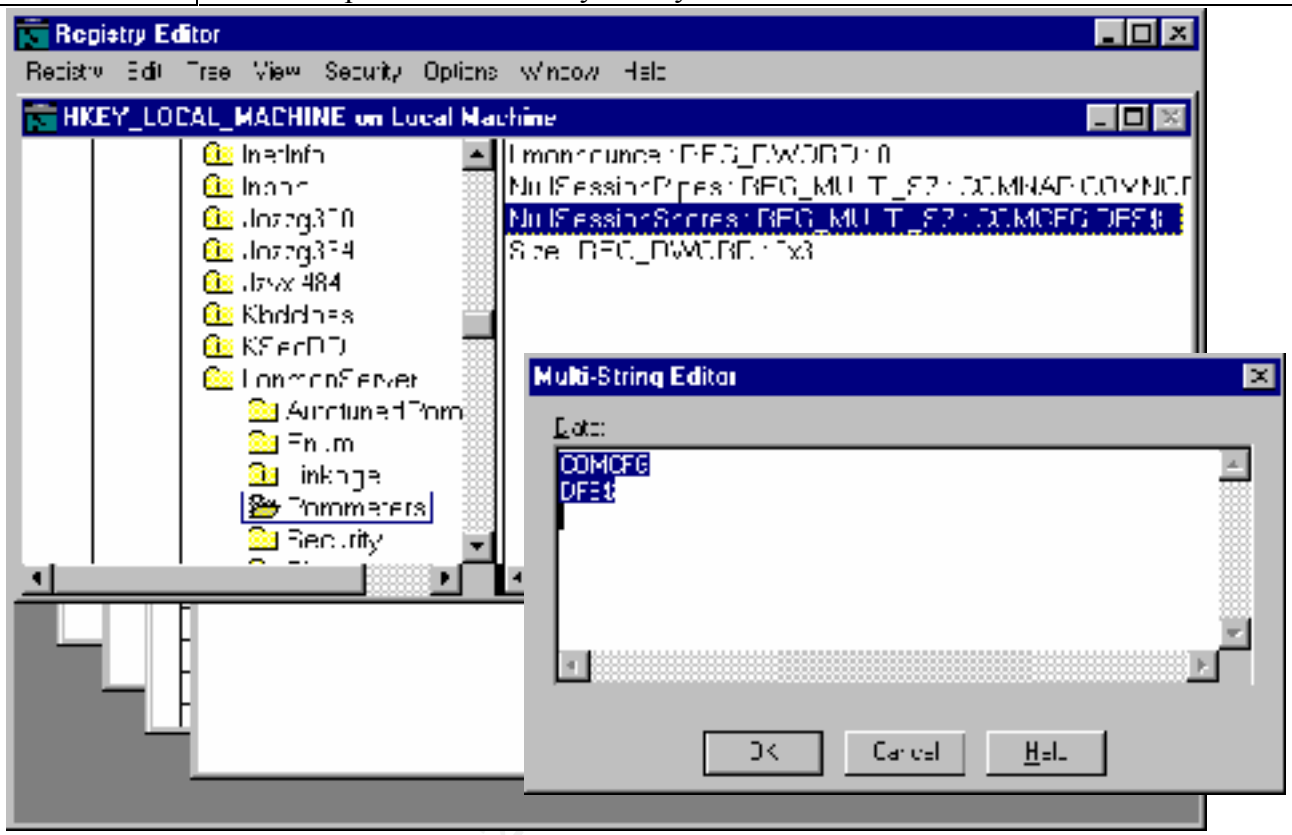
3.2.6 Anonymous User	
Best Practice	Disable “known” Microsoft
Risks	Unauthorized access. Destruction or modification of system resources
Test	Use DumpReg utility → Report → Dump Registry → HKEY_LOCAL_MACHINE → CTL-F → RestrictAnonymous NOTE: value in registry
Findings	
Remediation	Set registry value to 1 for RestrictAnonymous Make backup copy of Registry At Run command type regedt32 and hit enter HKEY_LOCAL_MACHINE → CurrentControlSet →LSA Edit → Add Value → type RestrictAnonymous for Value name → change Data Type to REG_DWORD → OK → type 1 in Data box → click OK → Reboot



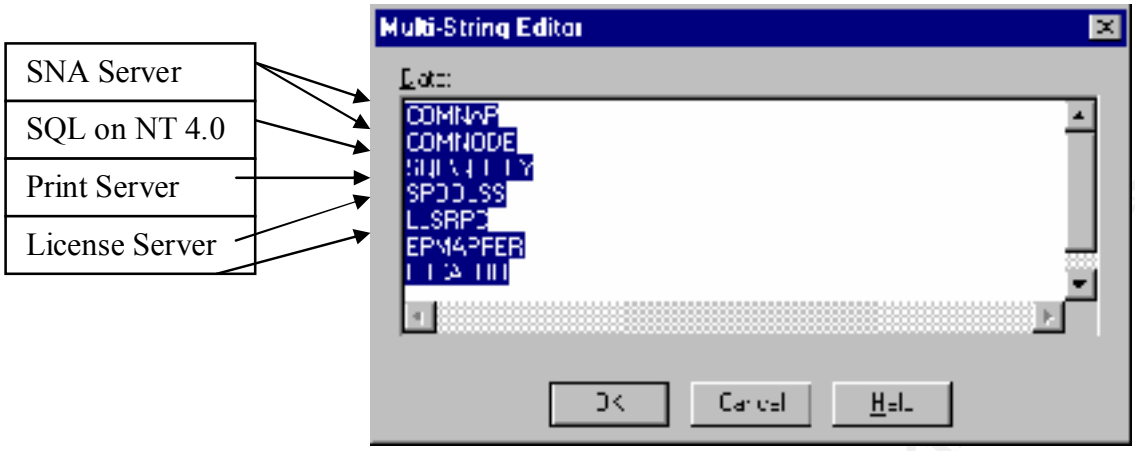
3.2.7 User Name Cache	
Best Practice	Removing the display of cached user names keeps a potential attacker from assessing accounts
Risks	Unauthorized access. Destruction or modification of system resources
Test	Use DumpReg utility → Report → Dump Registry → HKEY_LOCAL_MACHINE → CTL-F → DontDisplayLastUsername NOTE: value in registry → CTL-F → DefaultPassword → Note if present in registry
Findings	
Remediation	Set registry value to 1 for DontDisplayLastUsername Make backup copy of Registry At Run command type regedt32 and hit enter HKEY_LOCAL_MACHINE → SOFTWARE → Microsoft → Windows NT → Current Version → Winlogon → Edit → String → 1 → Also delete DefaultPassword if present → Reboot

4.1 Null Sessions and Pipes	
4.1.1 Restrict null sessions	
Best Practice	Null Sessions can be required by third-party Applications to run. Care should be taken before proceeding with remediation.
Risks	Unauthorized access. Destruction or modification of system resources
Test	At the Run command type net use *IP_ADDRESS*\ipc$ "" /user:""
Findings	
Remediation	Back up registry before proceeding Create registry entry At Run command type regedt32 and hit enter Click on HKEY_LOCAL_MACHINE → CurrentControlSet →Services → LanmanServer → Parameters →Edit → Add Value → type RestricNullSessAccess for Value name → change Data Type to REG_DWORD → OK → type 1 in Data box → click OK → Reboot
4.1.2 Control null session access to shares	
Best Practice	Some applications can only connect to a share via a null connection. This is Microsoft way to allow shares to be accessed will null connections, while blocking access to all the other shares on the system. The way this is done is by placing only the shares that require a null session into NullSessionShares Key. See Knowledge base Q174296 and Q11850
Risks	Unauthorized access. Destruction or modification of system resources
Test	Use DumpSec utilities. DumpSec → Report → Dump →HKEY _LOCAL_MACHINE → CTL-F → NullSessionShares Note if key is there
Findings	

Remediation	Back up registry before proceeding Create registry entry At Run command type regedt32 and hit enter Click on HKEY_LOCAL_MACHINE → CurrentControlSet →Services → LanmanServer → Parameters → Double click on NullSessionShares → Highlight items and press the delete key on keyboard → Reboot



4.13 Control null session access to named pipes	
Best Practice	Some named pipes can only work via a null connection. Microsoft provided a way to allow some named pipes to be accessed in this fashion while blocking this access to all the other shares on the system. The way this is done is by placing only the shares that require a null session into NullSessionPipes Key.
Risks	Unauthorized access. Destruction or modification of system resources
Test	Use DumpSec utilities. DumpSec → Report → Dump →HKEY _LOCAL_MACHINE → CTL-F → NullSessionPipes Note if key is there
Findings	
Remediation	Back up registry before proceeding Create registry entry At Run command type regedt32 and hit enter Click on HKEY_LOCAL_MACHINE → CurrentControlSet →Services → LanmanServer → Parameters → Double click on NullSessionPipes → Highlight items and press the delete key on keyboard →Reboot



Security Policy 5.1 – File & Registry Access	
5.1.1 System Root Lockdown	
Best Practice	Lock down the system root to prevent tampering
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	Not applicable - this is only a recommendation and does not have to be implemented
Remediation	See following chart:[1]

Directory	*Group Level Access Control*
root of NTFS volume	**Administrators, System Full Control** **Server Operators Change** **Everyone Change** **CREATOR OWNER Full Control**
\%SystemRoot%	**Administrators, System Full Control**
All \%SystemRoot%Sub-Directories	**Server Operators Change** **Everyone Read** **CREATOR OWNER Full Control**
\Boot.ini	**Administrators Full Control** **SYSTEM Full Control**
\Ntdetect.com	**Administrators Full Control** **SYSTEM Full Control**
\Ntldr	**Administrators Full Control** **SYSTEM Full Control**
\Autoexec.bat	**Administrators Full Control** **SYSTEM Full Control** **Everyone Read**
\Config.sys	**Administrators Full Control**

	SYSTEM Full Control **Everyone Read**
\TEMP	**Administrators Full Control** **SYSTEM Full Control** **CREATOR OWNER Full Control** **Everyone Special Directory Access - Read, Write and Execute, Special File Access - None**
\Program Files	**Administrators Full Control** **SYSTEM Full Control**
All \Program Files Sub-Directories	**Server Operators Change** **Everyone Read** **CREATOR OWNER Full Control**

Exceptions to the Table above

Directory	***Group Level Access Control***
\%SystemRoot%\REPAIR	**Administrators Full Control**
\%SystemRoot%\COOKIES **\%SystemRoot%\FORMS** **\%SystemRoot%\HISTORY** **\%SystemRoot%\OCCACHE** **\%SystemRoot%\PROFILES** **\%SystemRoot%\SENDTO** **\%SystemRoot%\Temporary Internet Files** **\%SystemRoot%\Cursors** **\%SystemRoot%\Fonts** **\%SystemRoot%\PRINTERS** **\%SystemRoot%\TMP**	**Administrators Full Control** **CREATOR OWNER Full Control** **Everyone Special Directory Access - Read, Write and Execute, Special File Access - None** **System Full Control**
\%SystemRoot%\SYSTEM32\CONFIG	**Administrators Full Control** **CREATOR OWNER Full Control** **Everyone List** **System Full Control**
\%SystemRoot%\SYSTEM32\system32	**Administrators, System Full Control** **CREATOR OWNER Full Control** **Everyone Change** **Server Operators Change**
\%SystemRoot%\SYSTEM32\drivers	**Administrators, System Full Control** **CREATOR OWNER Full Control** **Everyone Read** **Server Operators Full Control**
\%SystemRoot%\SYSTEM32\repl	**Administrators, System Full Control** **CREATOR OWNER Full Control** **Everyone Read**

	Server Operators Change
\%SystemRoot%\SYSTEM32\spool	Administrators, System Full Control CREATOR OWNER Full Control Everyone Read Print, Server Operators Full Control Power Users Change
\%SystemRoot%\SYSTEM32\repl\import	Administrators, System Full Control CREATOR OWNER Full Control Everyone Read Server Operators Change Replicator Change Network No Access
\%SystemRoot%\SYSTEM32\repl\export	Administrators, System Full Control CREATOR OWNER Full Control Server Operators Change Replicator Read

[1]

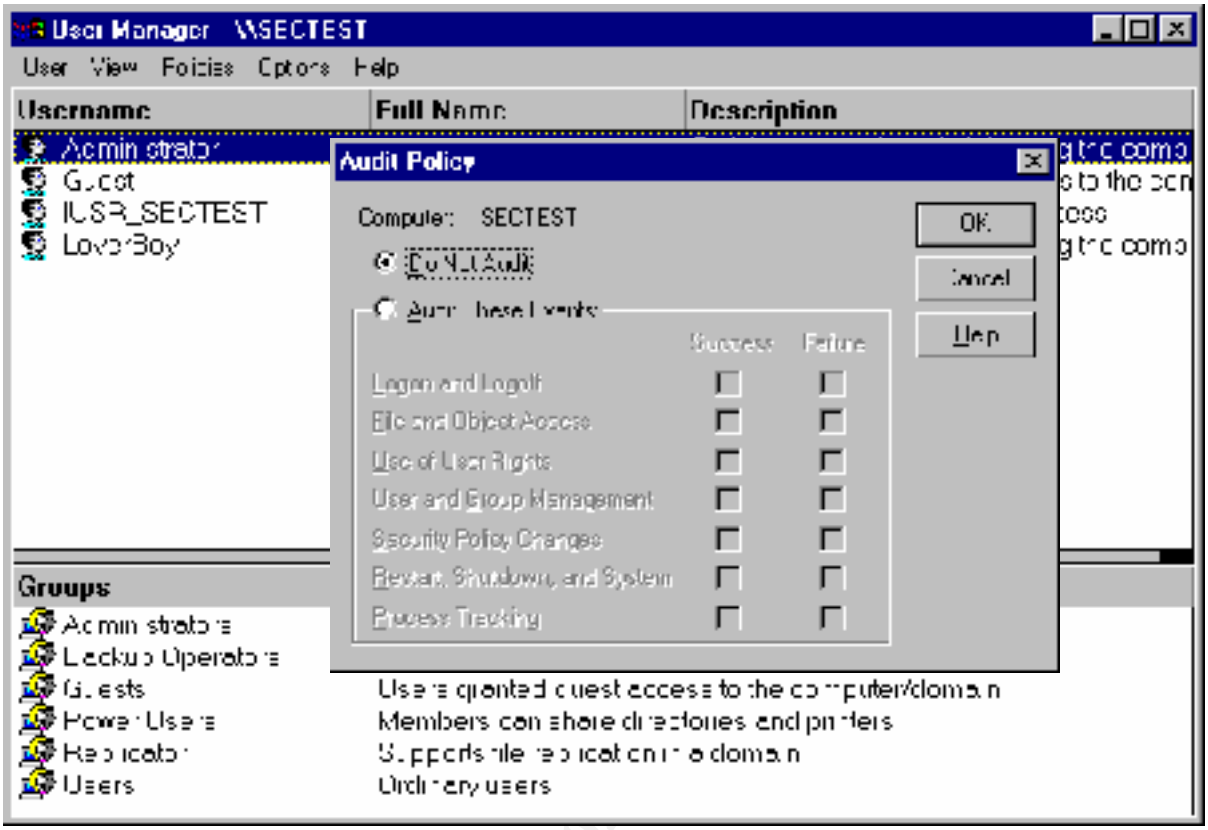
5.1.2 Share Level Access Control	
Best Practice	Restrict permissions to share directories on servers
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	Use DumpSec utilities. DumpSec → Report → Dump Permission to File System → C:\ → Note permissions for everyone group
Remediation	Back up the registry. Type at the run command regedt32 → HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → Services → LanmanServer → Shares → Security → restrict write access to shares key and all subkeys to those groups or users who should be provided access. Set all other users (Everyone group) to a maximum "Read" permission [1]
5.1.3 Restrict network access to registry	
Best Practice	Control access to registry
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	Use DumpReg utilities. DumpReg → Report → Dump Registry → Edit → Filter → SecurePipeServers → check value
Remediation	Back up registry Change key value At Run Command type regedt32 and press enter Click on HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → SecurePipeServers → Winnreg → set to 1

[1] "Windows NT 4.0 Security Graded Security Configuration, Leigh Purdie and George Cora V1.4, 1/2001 htttp://www.intersectalliance.com/project/WinNTConfig.html#4.2

5.1.4 Authentication	
Best Practice	For a higher level of security Network Authentication levels must be changed
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	Inquire Administrator
Remediation	NT supports the following challenge-response authentication: • LanManager (LM – NT default) • NT Lan Manager (NTLM) – uses 56 bit encryption and not immune to attacks • NT Lan Manager version 2 (NTLMv2) – uses 128 bit encryption and adds a session level security for the challenge-response, immune to brute force attacks • Registry keys to modify are HKEY_LOCAL_MACHINE → SYSTEM → CurrentConrolSet → Control → LSA → LMCompatibilityLevel → change value to 2 (above LM) NOTE: there are 5 levels to choose from , See Knowledge Base Q147706
5.1.5 SMB Signing	
Best Practice	Promote a higher level of security Network Authentication
Risks	SMB sessions are susceptible to man-in-the-middle, packet-replay and other attacks[2]
Findings	
Test	Inquire Administrator
Remediation	Make the following registry changes to enforce SMB signing on NT: HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Services → LanManServer → Parameters → EnableSecuritySignature → REG_DWORD → 1 HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Services → LanManServer → Parameters → RequireSecuritySignature → REG_DWORD → 1

6.1 Auditing			
6.1.1 Audit Logs			
Best Practice	Run audit logs if risk assessment is high		
Risks	Volume of information produced may be significant		
Findings			
Test	Check audit policy Start → Programs → Administrative Tools → User Manager for Domains → Policies → Audit (note was is being audited)		
Remediation	Recommended :	Success	Failure
	Logon & Logoff levels	ON	ON
	Startup,Shutdown & System	ON	ON
	Security Policy Change	ON	ON
	User & Group Management	ON	ON
	Use of User Rights	OFF	ON
	File & Object Access	OFF	OFF
	Process Tracking	OFF	OFF[2]
	Auditing is up to the administrator		

[2] "Securing Windows NT Step-by-Step, Jason Fossen, Jan. 28, 2001, pg 164



6.1.2 Secure Access to Event Log	
Best Practice	Access logs contain confidential information and should be protected
Risks	Data and audit trail loss
Findings	
Test	Check NTFS permission on SysEvent.evt, SecEvent.evt and AppEvent.evt files in the \%SystemRoot%\System32\Config folder
Remediation	Assign the system account and the local Administrators group Full Control of event log files.
6.1.3 Manage Audit and Security Log	
Best Practice	Configuring SACLs on folders, files, registry keys and printers and viewing and clearing the security log are Administrator privileges
Risks	Confidential information could be loss
Findings	
Test	Start → Programs → Administrative tools → User Manager for Domains → Policies → User Rights → Right → Manage Auditing and Security Log → Note Group granted rights

Remediation	Start → Programs → Administrative tools → User Manager for Domains → Policies → User Rights → Right → Manage Auditing and Security Log → Grant to Administrators group only → OK

7.1 Anti-Viral Software	
Best Practice	Prevention from Infected files from unknown sources
Risks	Data loss and down time. Bottom line is money
Findings	
Test	Check to see if Anti-virus program is installed
Remediation	Purchase software and download from the internet.

References

Securing Windows NT, Step-by-Step, Jason Fossen Document Version 3.7, 07/24/00

www.microsoft.com/technet/security/dccklst.asp

Hardening Windows NT Against Attack, Paul E. Proctor, January 1999

Windows NT 4.0 Security Graded Security Configuration Document, Leigh Purdie and George Cora, Vs. 1.4, 1/16/01

Analysis of the Security of Windows NT, Hans Hedbom, Stefan Lindskog

Limiting Anonymous Logon/Network Access to Named Pipes and Shares, John W. Albright 6/28/2000

Using the NT Resource Kit C2 Configuration Manager for Microsoft Windows NT 4.0, Manuel A. H. Offenberg

Securing/Configuring Windows NT Server, Jeffrey Fieldman, 5/27/99

GIAC Securing NT Practical Assignment, Robert Hayden, Version1, June 2000

(http://www.sans.org/y2k/practical/Sherri_Heckendorn.doc)