

# **Global Information Assurance Certification Paper**

## Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## **The Technical Security Assessment Audit**

#### J. Malinda Armstrong

Sharen and a state of the state Senior Security Analyst Student# 941 SANS - New Orleans Feb. 2001 NT Step by Step

© SANS Institute 2000 - 2002

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 2<sup>nd</sup> 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 3<sup>rd</sup> 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.

	Data Availability		ר (	Technical
Non-Repudiation		Data Integrity		ical
I & A	Access Control	Accountability	CONTROLS	
Confidentiality	Integrity	Availability	ROLS	Physical
Phy	ysical Security Controls	]		
Security 1	Policies, Plans and Proced	lures	-	Admin
	Figure 1-1: Defense	e in Depth	- \	$\leftarrow$

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 <u>findings</u> 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	Compan	iy
Audit #	Departm	nent
Date	Server T	Sype
Administrator	IP Addre	ess
	DNS Na	ime

Findings	Control Enabled	Control not Enabled w/compensating controls
	Control not Enabled	×0

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 serve	r area
Findings		
Remediation	Recommendation is electronic surveillance and admitta	ince

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		$\rightarrow$ right click on drives $\rightarrow$ click on Properties $\rightarrow$ Note File		
🛃 My Computer	(C.) Pi	Properties 🛛 🕅 🗙		
El- Enil Vere Enip Dia Roppi, (A:) Dia Roppi, (A:) Dimens Dimens Dia Up Networking		Label     Security       ype.     Local Dick       File ovstrm:     NTFF       Hood space     F24,821 \$85 byres       Fice space     3,41 35		
nd gened joi) weden alter	-ин - расы 3 41168, 1	Capacilii 4,240,500,200 biites 0.0450 Di ve C		

📄 Compretes C 🕾

ПΚ

Canco

epoly

© SANS Institute 2000 \_\_\_\_\_\_GIACNT.doc As part of GIAC practical repository.

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	. G°
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 $\rightarrow$ click on Properties $\rightarrow$ Protocols $\rightarrow$ Note
	Protocols
Findings	
Remediation	Right click on Network Neighborhood $\rightarrow$ Properties $\rightarrow$ Protocols $\rightarrow$ click on
	"protocol" $\rightarrow$ click Remove
	NOTE: Firewalls should only have TCP/IP

í.	work estilization   St	aviers Picturuh Adapters Eindings	
	9 -twork Limbor		
Ē			_
	🍋 10 VE PA	Marcall.	
	<u>4</u> -d		1
	- Decoription:		
		ttio Protocol/Internet Protocol, The default wide	
	Transcort Con ales network	protocal libet provides communication across	
	Transcort Con ales network		
	Transcort Con ales network	protocal libet provides communication across	
	Transcort Con ales network	protocal libet provides communication across	
	Transcort Con ales network	protocal libet provides communication across	
	Transcort Con ales network	protocal libet provides communication across	
	Transcort Con ales network	protocal libet provides communication across	

2.4 Bindings	
<b>Best Practice</b>	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 $\rightarrow$ Properties $\rightarrow$ Bindings $\rightarrow$ Note Bindings
Findings	
Remediation	Right click on Network Neighborhood $\rightarrow$ Properties $\rightarrow$ Bindings $\rightarrow$ "service $\rightarrow$
	Disable NOTE: Firewalls should only have TCP/IP
	Notwork 🛛 🕄
	[centilication   Services   Protocols   Adapters   Dinding :

Network binding: are connections between network cerds, protocols, and services installed on this computer. You can use this page on isable relevants bindings on a large the order in which this computer metsion and method the relevants.	
Lhow Dindings for All services	
Prove Interface Int	
Inable (D)(able )	
14 Second	
	-

2.5 Services	
<b>Best Practice</b>	Install and configure as few services as possible
Risks	Unauthorized access. Destruction or modification of system resources
Test	Inquire Administrator. Start $\rightarrow$ Settings $\rightarrow$ Control Panel $\rightarrow$ Services NOTE the services enabled
Findings	9
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)

		Statup	Cose
fur pater Browser	Startad	Automatic 💻	ī ———
HCF Cien.		Divebel 💮	Start
hectory Replicator		Manuel	
ventro_	Stated	Actomatic	Stop
TP Fullyling Service	Stated	Altomatic 🛄	
iupre Publishing Service	Stated	- Altomatic 🎆	Eause
iler ve bolg nij Service	Stated	- Altomatic 🏢	Cominue
lewenge	Startad	4. tomatic	
l=t_u_u.		Mar usi 🔛	
Istoonii, DDE		Mar uel 📃 📼	laglur -
			H <u>W</u> Embres

2.6 Devices		
<b>Best Practice</b>	Install and configure as few devices as possible	
Risks	Unauthorized access. Destruction or modification of system resources	
Test	Inquire Administrator. Start $\rightarrow$ Settings $\rightarrow$ Control Panel $\rightarrow$ Devices NOTE the	
	devices enabled	
Findings		
Remediation	Start $\rightarrow$ Settings $\rightarrow$ Control Panel $\rightarrow$ 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	

Degree	Statur	Statup	
-plying <	Statled	BLU. 💻	Cose
La1950-1		Divablet 🔛	
cc∋376rt		Dicabled 🧾	Start
Del DGX		Dicabled 💻	
Delidea		Dicabled 🎆	Stop
Disk	Started	Boo:	
Diokpor <sup>i</sup>		Discbicc 🧾	Elaglus.
DetSeci		Discbicc 🧾	H <u>W</u> Embres
ctc329+		Discbicc 🧾	
ct4000		Diseb ee 💌	<u>E</u> elp

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 $\rightarrow$ Report $\rightarrow$ Dump Registry $\rightarrow$ HKEY_LOCAL_MACHINE $\rightarrow$ CTL-F $\rightarrow$ 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
Benistru	

Registry Editor	_ I I Ă
Recistry Edit Tree View Security Options w/incow Held	
Rev_LOCAL_MACHINE on Local Machine	_ 🗆 🖂
<ul> <li>DOB Devices ▲ Debug : DED_EXDAND_S2:</li> <li>Environment</li> <li>Everutive</li> <li>EleDenomeO:</li> <li>EleDenomeO:</li> <li>CrowrDLLs</li> <li>Memory Manov</li> <li>Vernory Manov</li> <li>Required : REG_EXDAND_S2: %System</li> <li>Setup</li> <li>System Resources</li> <li>TimeZoneintomat</li> <li>Virtua DeviceDrive ↓</li> </ul>	nsix nFront%\system37\ds? emRoot%\system02\ba q t/vindows
	Þ

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		
Remediation	<ul> <li>Execute the RDISK /s utility in the \%SystemRoot%\System32 subfolder.</li> </ul>		
	<ul> <li>When prompted insert disk when files are ready to be copied.</li> </ul>		
	<ul> <li>Use the /s switch to copy the current SAM to the ERD</li> </ul>		
	19		
	Create Emergency NT Boot Disk Contains NTL DP. POOT INL and NTDETECT COM		
	<ul> <li>Contains NTLDR, BOOT.INI and NTDETECT.COM</li> <li>if commuter has a SCSI hast drive which does not have BIOS enabled, the dial</li> </ul>		
	<ul> <li>if computer has a SCSI boot drive which does not have BIOS enabled, the dis will also contain NTBOOTDD.SYS</li> </ul>		
	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.		
	<ul> <li>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.</li> </ul>		
	• 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		
	· Сору		
	· Format		
	· Fdisk		
	· Mem		
	· Sys.com		
	· a text editor		
	· DiskSave		
	PLACE DISKS IN A SECURED AREA.		
2.9 Syskey Protection	on S		
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 $\rightarrow$ Tools $\rightarrow$ Options		
	$\rightarrow$ Unclick Enabled under Brute Force Attack $\rightarrow$ File $\rightarrow$ Import SAM file		
	(C:\winnt\repair) $\rightarrow$ SAM_ $\rightarrow$ View accounts & passwords		
Findings			
Remediation	NOTE: Update ERD before running syskey and make a 2 <sup>nd</sup> ERD after installing		
	syskey		
	• At the Run Command type syskey and press enter $\rightarrow$ Encryption Enabled $\rightarrow$		
	$OK \rightarrow Store Startup Key Locally \rightarrow OK \rightarrow Reboot$		

Securing the Windows NT Account Database	🔀 Account Database Key
This too will allow you to contigure the Acco. Database to enable and honal encryption, but protecting the database from non-promise. Once enabled, the encryption cannot be	
disatled O Enclyption Discbloc O Discyption Litented	System Benerated Personal
OK Carcel Lpdats	Store Statup Key Locally     Store Starup Key Locally     Store Starup Key Locally     Store Starup Key Locally     Stores a key as part of the operating system     and to interaction is required during system     V.et.     OK Cancel

2.10 System Page	eFile	
<b>Best Practice</b>	Wipe Page file at system shutdown	
Risks	Unsecured data	
Findings		
Test	Use DumpReg utility $\rightarrow$ Report $\rightarrow$ Dump Registry $\rightarrow$ HKEY_LOCAL_MACHINE $\rightarrow$ CTL-F $\rightarrow$ 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 → CurrentContro         Control → SessionManager → Memory Management → ClearPageFile       → Edit → DWORD → type in 1 for Data → click OK → Reboot for		

2.11 System Usag	ye 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

	🙆 Local Computer Properties	×
	P Inces P Inces Local Computer P Astwork P System P	
Q	<ul> <li>Window: NT Shell</li> <li>Windows NT System</li> <li>I-I U Logun</li> <li>I-I U Logun</li> <li>I-I Enche sturdown nom Authenteolich dialog bos</li> <li>I-I Do no: diepla, last looged on uzer nome</li> <li>I-I Dur legen scripts synchronous y.</li> </ul>	
	Sellings to 1, grothermer Caption [Warring ] Text [7] answer is locally in the tomas on to mp.]	
© SANSTINStrung2000 alinda_C		ancel

2.12 Service Pack			
<b>Best Practice</b>	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 $\rightarrow$ Open My Computer $\rightarrow$ c:\WINNT\System32		
	Right click on Schannel.dll $\rightarrow$ click on Properties $\rightarrow$ 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. <u>http://www.microsoft.com/security</u>		
	Y'		

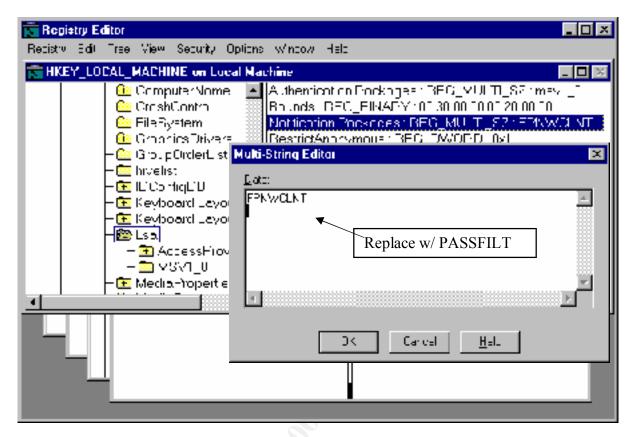
About Windows NT (R)		Test 1
MICROSOFT	Microvoft (R) (windowy KT (R) Version 4.0 (Build 1981, Bervice Fack 5) Copyright (C) 1981-1996 Microsoft Cord. Reviced Service Pack 6s	Test I
	Tiris croduct is licenced to MDACC MDACC	
	Memory, Available to Windows N (* 1918), 1918	
C	()X()	

Ide Ide Vest Isp         Ide Ide Vest Isp	Scharmeloff Properties       Scharmeloff Properties       General Venior Score ()       A version of 1117/1       Description (015/2011) estantly row dec() Score ()       Description (015/2011) estantly row dec() ()	Test 2	
	OK Cancel	≙xobr    ₫	
Cestaples ≪ toreatti			
📲 Start 🕼 Winnsoll Wood 📃 🔍	ع⊠ ( مدير ياعوا	AMININT 🔰 🛄 CANADIN TANAN A	32 👘 K 57 PM

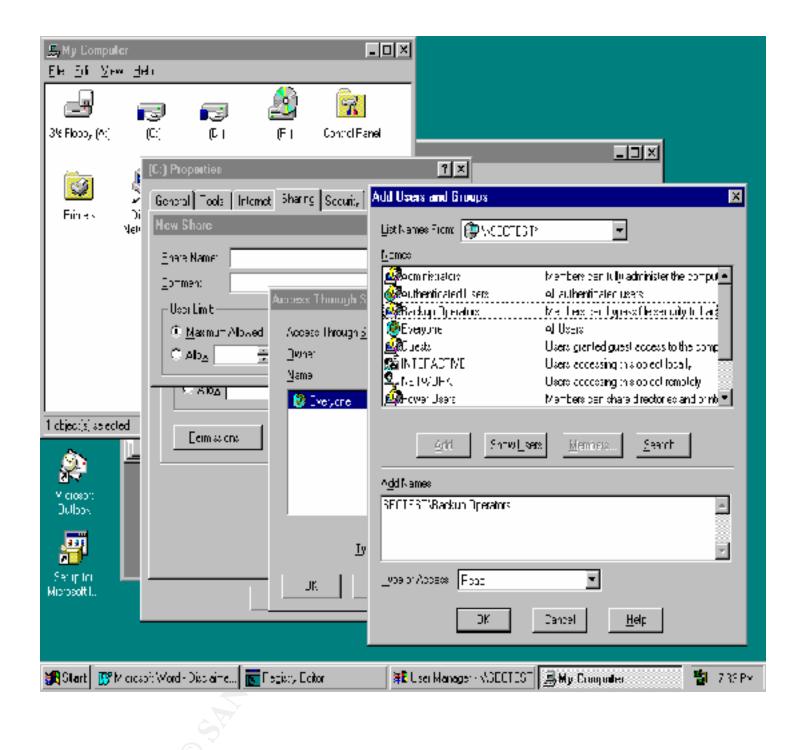
3.2 System Accou	nts
3.2.1 Password Co	onfiguration
Best Practice	Strengthen password policies and Disable Blank passwords
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	Use DumpSec utilities. DumpSec → Report → Dump Policies NOTE: password polices
Remediation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

Additional Information:	1) Strong passwords may be implemented using the <u>passfilt.dll</u> 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 $1^{st}$ ) Backup registry $\rightarrow$ type at run command regedt32 $\rightarrow$ HKEY_LOCAL_MACHINE $\rightarrow$ SYSTEM $\rightarrow$ CurrentControlSet $\rightarrow$ Control $\rightarrow$ LSA $\rightarrow$ Notification Packages - $\rightarrow$ ReG_MULTI_SZ $\rightarrow$ replace FPNWCLNT with PASSFILT $\rightarrow$ Reboot
	The NT Resource Kit includes a tool, <u>passprop.exe</u> -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

Account Policy		×
Computer, SECTEST - Possword Festitioners - Maximum Hassivo d'Age - C. Forsword <u>M</u> over Estitics	Minnium Hassivo di Aqe Ri Allow Changes Introdictoly	OK Croce Eelp
© Explice n 42 ∰ Daye	C Allow Qhanges In Days	
C At Less I There is a characters	Do Not Keep Lassword 1:100	
<ul> <li>Kontetour litekout</li> <li>Account litegout</li> </ul>		]
Loskiu. Du ator	allemply nin.tos	
O Fore <u>v</u> er (undi somin unlocks) O Durațon minu	4=×	
Eardialy disconnect renate users in Use a great og on morale for ang		



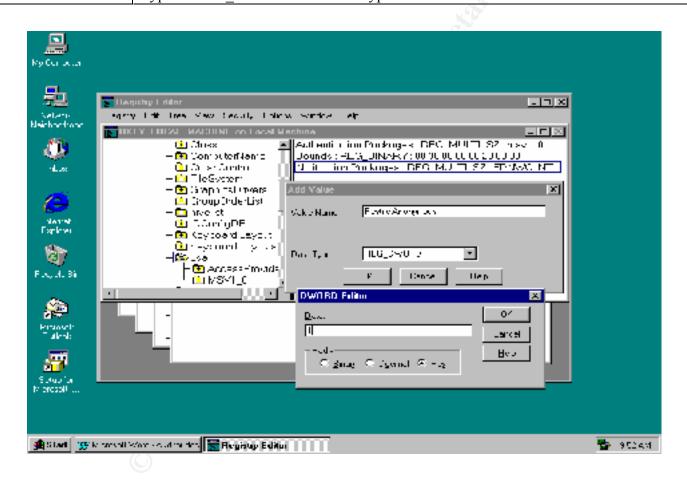
3.2.2 Access compu	ater from network
<b>Best Practice</b>	Replace Everyone Group with Authenticated Users Group
Risks	Unauthorized access. Destruction or modification of system resources
Test	Login with user account $\rightarrow$ type at run command <u>\\computername\share</u>
Findings	
Remediation	Right click on drives, file folders devices $\rightarrow$ Sharing $\rightarrow$ New Share $\rightarrow$ type Share Name $\rightarrow$ Permissions $\rightarrow$ Add $\rightarrow$ Group $\rightarrow$ Add $-$ Type of Access $\rightarrow$ OK $\rightarrow$ Everyone Group $\rightarrow$ Remove $\rightarrow$ OK $\rightarrow$ Add $\rightarrow$ Authenticated Users $\rightarrow$ Add $\rightarrow$ Type of Access $\rightarrow$ OK $\rightarrow$ 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	
r munigs	
Remediation	• Rename account and establish a decoy account named Administrator with no privileges.
	• Enable account lockout on the real Administrator account with passprop utility.
2.2.4.4.1	Disable the local machine Administrator account
3.2.4 Administrator	
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	Ś.
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 $\rightarrow$ Programs $\rightarrow$ Administrative Tools $\rightarrow$ User Manager for Domains
	NOTE if account is enabled.
Findings	
Remediation	Start $\rightarrow$ Programs $\rightarrow$ Administrative Tools $\rightarrow$ User Manager for Domains $\rightarrow$ Guest (double click) $\rightarrow$ check Disable Account. Recommendation: Create a unique user id for guest with an expiration date

	U¢er Praperti	ie¢					×		
	Jæinerre	Guect				[	OK.		
	Ful <u>N</u> ame:	<b>I</b>					Dente		
	Teverbiou	ubn ato:	turt or great	ectess to the	computer/cometa		Leip		
	2657900								
	Bontini Bass∾orc:								
	⊡ Ucer <u>M</u> uol	Change Peo	sword a: Ne-#	Logon					
	🖂 H <u>a</u> er Latr	of Change 1	asser						
	Paysword	Never Expire	5						
	💌 Account D	vic≘biec							
	🔲 Account L	.co <u>k</u> ed Dut							
© SANSTMSHIDLE2000 21	n Circucs	¶§ Profile	- 🎭 Dialin					uthor retains ful	rights.

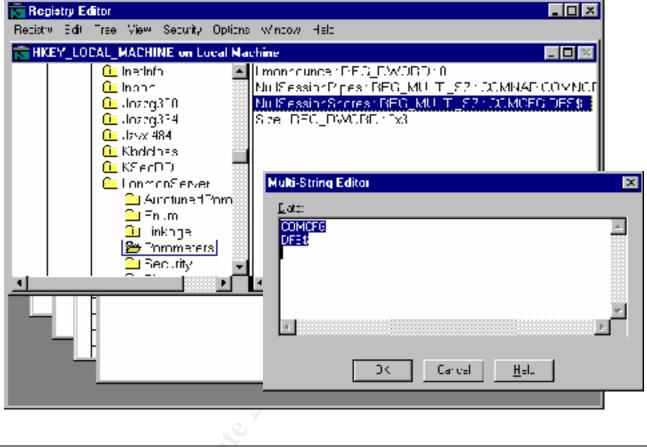
3.2.6 Anonymous U	Jser
<b>Best Practice</b>	Disable "known" Microsoft
Risks	Unauthorized access. Destruction or modification of system resources
Test	Use DumpReg utility $\rightarrow$ Report $\rightarrow$ Dump Registry $\rightarrow$ HKEY_LOCAL_MACHINE
	$\rightarrow$ CTL-F $\rightarrow$ RestrictAnonymous 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 $\rightarrow$ CurrentControlSet $\rightarrow$ LSA Edit $\rightarrow$ Add Value $\rightarrow$ type RestrictAnonymous for Value name $\rightarrow$ change Data Type to REG_DWORD $\rightarrow$ OK $\rightarrow$ type 1 in Data box $\rightarrow$ click OK $\rightarrow$ Reboot



3.2.7 User Name C	Cache	
<b>Best Practice</b>	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 $\rightarrow$ Report $\rightarrow$ Dump Registry $\rightarrow$ HKEY_LOCAL_MACHINE	
	$\rightarrow$ CTL-F $\rightarrow$ DontDisplayLastUsername NOTE: value in registry $\rightarrow$ CTL-F $\rightarrow$	
	DefaultPassword $\rightarrow$ 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 $\rightarrow$ SOFTWARE $\rightarrow$ Microsoft $\rightarrow$ Windows NT $\rightarrow$	
	Current Version $\rightarrow$ Winlogon $\rightarrow$ Edit $\rightarrow$ String $\rightarrow 1 \rightarrow$ Also delete	
	DefaultPassword if present $\rightarrow$ Reboot	

4.1 Null Sessions a	d Pipes			
4.1.1 Restrict null	essions			
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 <u>\/IP_ADDRESS\ipc\$</u> "" /user:""			
Findings				
Remediation	Back up registry before proceeding			
	Create registry entry			
	At Run command type regedt32 and hit enter			
	Click on HKEY_LOCAL_MACHINE $\rightarrow$ CurrentControlSet $\rightarrow$ Services $\rightarrow$			
	LanmanServer $\rightarrow$ Parameters $\rightarrow$ Edit $\rightarrow$ Add Value $\rightarrow$ type RestricNullSessAccess			
	for Value name $\rightarrow$ change Data Type to REG_DWORD $\rightarrow$ OK $\rightarrow$ type 1 in Data			
	box $\rightarrow$ click OK $\rightarrow$ Reboot			
4.1.2 Control null s	ession access to shares			
<b>Best Practice</b>	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 $\rightarrow$ Report $\rightarrow$ Dump $\rightarrow$ HKEY			
	$\_LOCAL\_MACHINE \rightarrow CTL-F \rightarrow NullSessionShares$ 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 $\rightarrow$ CurrentControlSet $\rightarrow$ Services $\rightarrow$
	LanmanServer $\rightarrow$ Parameters $\rightarrow$ Double click on NullSessionShares $\rightarrow$ Highlight
	items and press the delete key on keyboard $\rightarrow$ Reboot



4.13 Control null s	ession 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 $\rightarrow$ Report $\rightarrow$ Dump $\rightarrow$ HKEY LOCAL MACHINE $\rightarrow$ CTL-F $\rightarrow$ NullSessionPipes Note if key is there
Findings	Ő –
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

	Multi-String Editor 🔀
SNA Server	<u>L</u> ate:
SQL on NT 4.0	
Print Server	SULVEL M SPOOLSS
License Server	EPM4PER
	DK Carcel <u>H</u> el

Security Polic	Security Policy 5.1 – File & Registry Access		
5.1.1 System	Root I	Lockdown	
<b>Best Practice</b>	st Practice Lock down the system roo		prevent tampering
Risks		Unauthorized access. Destruct	ion 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: <sup>1</sup>	
	Directory		Group Level Access Control
	root c	of NTFS volume	Administrators, System Full Control Server Operators Change Everyone Change CREATOR OWNER Full Control
	\%Sys	stemRoot%	Administrators, System Full Control
	<b>AII</b> \%	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
	\Auto	exec.bat	Administrators Full Control SYSTEM Full Control Everyone Read

Administrators Full Control

\Config.sys

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

1

5.1.2 Share Level	Access Control
<b>Best Practice</b>	Restrict permissions to share directories on servers
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	Use DumpSec utilities. DumpSec $\rightarrow$ Report $\rightarrow$ Dump Permission to File System $\rightarrow$ C:\ $\rightarrow$ 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 <sup>1</sup>
5.1.3 Restrict net	work access to registry
<b>Best Practice</b>	Control access to registry
Risks	Unauthorized access. Destruction or modification of system resources
Findings	
Test	Use DumpReg utilities. DumpReg $\rightarrow$ Report $\rightarrow$ Dump Registry $\rightarrow$ Edit $\rightarrow$ Filter $\rightarrow$ SecurePipeServers $\rightarrow$ 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

<sup>&</sup>lt;sup>1</sup> "Windows NT 4.0 Security Graded Security Configuration, Leigh Purdie and George Cora V1.4, 1/2001 http://www.intersectalliance.com/project/WinNTConfig.html#4.2

5.1.4 Authentication	n
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 $\rightarrow$ SYSTEM $\rightarrow$ CurrentConrolSet $\rightarrow$ Control $\rightarrow$ LSA $\rightarrow$ LMCompatibilityLevel $\rightarrow$ 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 <sup>2</sup>
Findings	
Test	Inquire Administrator
Remediation	Make the following registry changes to enforce SMB signing on NT:
	HKEY_LOCAL_MACHINE $\rightarrow$ SYSTEM $\rightarrow$ CurrentControlSet $\rightarrow$ Services $\rightarrow$
	LanManServer $\rightarrow$ Parameters $\rightarrow$ EnableSecuritySignature $\rightarrow$ REG_DWORD $\rightarrow$ 1
	HKEY_LOCAL_MACHINE $\rightarrow$ SYSTEM $\rightarrow$ CurrentControlSet $\rightarrow$ Services $\rightarrow$
	LanManServer $\rightarrow$ Parameters $\rightarrow$ RequireSecuritySignature $\rightarrow$ REG_DWORD $\rightarrow$ 1
6.1 Auditing	

6.1 Auditing	0				
6.1.1 Audit Logs					
<b>Best Practice</b>	Run audit logs if risk assessme	nt is high			
Risks	Volume of information product	Volume of information produced may be significant			
Findings					
Test	Check audit policy Start $\rightarrow$ Programs $\rightarrow$ Administrative Tools $\rightarrow$ User Manager for				
	Domains $\rightarrow$ Policies $\rightarrow$ Audit (	note was is being audite	d)		
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 <sup>2</sup>		
	Auditing is up to the administra	Auditing is up to the administrator			

<sup>&</sup>lt;sup>2</sup> "Securing Windows NT Step-by-Step, Jason Fossen, Jan. 28, 2001, pg 164

semane	Full Name	Descrip	ntion		
Administrator	Audit Policy			×	atre co
S Guad USR_SECTEST	Compute:: SECTEST				s to the tess
LovarBoy	•			OK.	gtrc co
	🖲 (Do AltAudi)			Cancel	Ĩ.
	C Autor based vents			Hep	
		Success	-	Tich	
	Logon and Logolf	<u> </u>	<u> </u>		
	Elle and Object Access	<u> </u>			
	Lise of Liser Rights	<u> </u>			
	User and Group Management	<u> </u>			
	Security Policy Changes				
gunde	Bestart, Shutdown, and System				
🚱 Administratore	Process Tracking	Г	Г		
🖉 Liackup Operatore –				w/slaws a	
🖉 (J. ests 🖉 Power Usera	Users granted quest acce Members can share dried				
Repicator	Supportante replication in			, ,	
🕼 Users	Ordinary users				

6.1.2 Secure Access	to Event Log
<b>Best Practice</b>	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
<b>Best Practice</b>	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 $\rightarrow$ Programs $\rightarrow$ Administrative tools $\rightarrow$ User Manager for Domains $\rightarrow$ Policies
	$\rightarrow$ User Rights $\rightarrow$ Right $\rightarrow$ Manage Auditing and Security Log $\rightarrow$ Grant to
	Administrators group only $\rightarrow$ OK

. Sco.

7.1 Anti-Viral So	Prevention from Infected files from unknown sources
Best Practice	
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)