

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.

Interested in learning more?

Check out the list of upcoming events offering "Securing Windows and PowerShell Automation (Security 505)" at http://www.giac.org/registration/gcwn

Martin A. Golias 246 Airport Road Johnstown, PA 15904

Phone 814-534-8879 Practical T1 Track Parliament Hill, Ottawa

The purpose of this paper is to demonstrate practical methods to secure file servers and company services. It is in not meant to be a complete or final set of rules or procedures in that network security is an ever developing set of techniques of hackers and network administrators.

I plan on using some of the techniques learned at the SANS Parliament Hill classes and additional information acquired from the Internet and in particular Microsoft to demonstrate a working knowledge of steps necessary to implement and research security techniques.

Outline of practical demonstrations

Section 1.

Prepare for Recovery: Emergency repair Disks

Section 2

Limiting information to anonymous users in Exchange

Section 3

Security Event Auditing

Section 4

Service Packs

Section 5

SYN Floods

Section 6

Setting Security Policies

Section 1 Prepare for recovery: Emergency repair disks

The ability to recover from a hacker exploit or other disaster is essential. While tape backups are critical not all of them can save/restore the boot sector and the Master Boot Record. It is essential that a set of Emergency repair disks be prepared, updated frequently and stored in a safe place.

From the Run line execute the following command.

Run	<u>1 ×</u>	
2	Type the name of a program, fuller, document, or Internet recource, and Windows will open it for you	
Open	rdsk./s	
	OK Centel Browse	0

The system will save the current configuration

Next you will be asked if your want to create the Emergency Repair Disk. Click on Yes. The floppy that you are using will be formatted. Click on OK.

You are then instructed to store the ERD in a safe place. Click on OK.

The command above contains the /s switch in order to have a current copy of the SAM database. Without the /s switch only the administrator and guest account OF THE ORIGINAL INSTALLATION are copied to the ERD.

In addition to the ERD disk created for each file server the following disks are also necessary.

An Emergency NT Boot Disk

Three bootable setup disks with a current copy of Setupdd.sys on the second disk if your file server is at Service Pack 6 or later.

Finally you should have a MS-DOS boot disk such as a Windows 98 emergency Boot Disk with utilities such as FDISK, FORMAT, Partition Magic and CD-ROM and tape drivers.

Reference: SANS Parliament Hill 2000 manual page 57.

Section 2

Limiting information accessible to anonymous users in Exchange

Microsoft Exchange, by default, allows anonymous users to search the Exchange Global Address List with an LDAP (The Lightweight Directory Access Protocol) client like Microsoft Outlook Express. Due the incredible amount of data that can be input into the exchange client, information can be acquired and used for social engineering to gain access to unauthorized information.

Steps in limiting the access of information to LDAP users is as follows:

At the Exchange server launch the Microsoft Exchange Administrator.

Highlight Configuration on left panel.

Double Click on DS Site Configuration on the right panel.

🐏 Microvoft Exchange Adhrinive ator		-	E ×
The Tail week Taols "Airces Leas			
	محادة الادائج المراجباتين كاحجا	20 201	
		<u>3. 91</u>	
Server LTEXCHANGE in Site LT - Configurat	in .		X
🍋 DEC Estheringes	Disclar flam, A	Y it st	
29 Richard Sink View	TOL A M 17	6/ 0/00 0 56 AH	-
🕈 🞑 okter:	🖼 Addes to	1/17.00 551 AH	-
🕞 🔁 Globa Armana in	🥥 Connectory	77 7770 5 57 AH	- H
1 0 LT	🖏 Lievog Bulévier	6/ 0/00 0 56 AH	0 H
E 🔕 Completori	🗐 Hontos	1/17/0 551 AH	
10 Bang and	😡 Frank	57 7/10 - 17 CM	- H.
	💼 Sa-az	5/1720 C 65 4H	- H
	[2] D. withologication	71 7 ILES AH	
	💝 ki u - në në 5 e fudiyatir	57 T/T0 5 55 4H	- 10
	🕌 Hita Sto Cong. resor	5/11/10/5/55/4H	- H
	🚮 Sire Adamating	754 - 2500 AM	
	🧏 Site Encline Cantigeration	84 0/00 0 58 AH	- Hill
			- H.
			- 10
			18
			- 10
			18
			2 H I
	han an a		.
L			6
12 Up polity			k.
🍓 Start 📲 🕬 Kar - pa - A 🔯 Necrosoft E	inh 🚉 kasa s Naido no 🛛 🛃 to fa ca	ula 😽 🕹	6-v

After clicking on the DS Site Configuration Properties screen, click on the Attributes Tab.

DS Site Configuration Properties	×	
Offine Address Book Custom Attributes General Felmissions Office Address Book	Attributes Echedule	
DS Site Configuration		
Display name. Diff. #= Conngurshop		
Directory name: Site-DSA-Contic		
Garbage collection interval (houro): 2 Anunyi lous access Anunyi lous access	-	
Baseword:		
_ionim Password		
Created Home ote: LT 6/10/00 5:58 AM 6/	Lac: motified 2700-5:55 4 4	
CK Careal Apply	Нор	

In the example that I am using, authenticated requests to the Exchange directory have the ability to view all of the attributes.

DS Site Configuration Properties	×
General Fermissions Office Addisory Book IDS Site Confid	Office Address Book Behedule
Configure: Anonymitus requests Colliner restation	Show altributes for: All nather opients Actent messages from Address
Check the attributes which will be available to authenticated LOAF directory requests	Admoster Line Admoster Admoster Admoster Allow out of other messages Allow out of other Allow out of other Admoster Adm
<u>ск</u>	

Then, with Anonymous requests highlighted, check or uncheck the information attributes that you want the anonymous user to be able to access.

DS Site Contiguration Properties	×			
General Fermissions Offine Address Book	Offine Address Book Echedule Curto n Att Buter Attributes			
05 Site Conti	guration			
Loni guro: Anonympus requests Authenticated requests Intersite regination	Show all butes for:			
	Address Inne			
Check the attributed which will be available to anonymous LDAP directory requests.				
	Avvivlar Cohune nur ber Businevs chune nur ber 2 Carl send on behelf of Cign			
СК	Careol Apoly Hop			

In my example, I removed the ability of the LDAP users to view the users home phone number, address, first name, department, the persons manager, mobile phone number and any notes about the mail recipient and any other information that could allow an individual to be compromised by social engineering.

What is left would be the maximum I would want anonymous users to be able to view.

This same technique could be used to limit information for authenticated and to limit or augment Inter-site replication.

Reference: SANS Parliament Hill 2000 manual page 31.

Section 3 Security Event Auditing

NT Server maintains three event logs to which entries are added – the System log the Applications log and the Security log. You can set up security auditing of numerous events to assist in tracking users access to various parts of the system.

Proper setting and monitoring the Audit Logs created by the Audit Policy administrators can keep watch on unauthorized access to files.

Steps in accomplishing this are as follows. Click on User Manager for Domains Highlight Policies Click on Audit

NOTE: The default setting for auditing is Do Not Audit.

Audit Policy			×
Domein: LAUREL1 Cl <u>D</u> o Nut Audit Cl <u>D</u> orn These Lixents;	Success	Leure	OK. Cancel Llep
Logon and Logolf Elicitht Object Access Use of User Rights User and Group Management Security Policy Changed <u>Revials</u> Stoudowry and System <u>P</u> rocess Tracking		<u>रारायाय</u> रा	

Once the events that you want to audit have been selected you can open the Event Viewer by going to:

Start

Programs

Administrative Tool (common)

Then scroll to the event that you want to investigate and double click.

In my example I wanted to verify that the Policy Change that I had chosen was logged and that the system was auditing for login failures.

Date: 9/20/2000 E vent ID: 612 Time: 7:45:57 Source: Security <u>User:</u> Administrator Type: Success Audit Computer: LTSERVER1 Category: Policy Change Description: Audit Policy Change: New Policy: Success Failurel + + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management Data: Bytes Words Close Previous Next Help	Date: 9/20/2000 Event ID: 612 Time: 7:45:57 Source: Security User: Administrator Type: Success Audit Computer: LTSERVER1 Category: Policy Change Description: Audit Policy Change: New Policy: Success Failure! + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Account Management Date: © Bytes © Words Close Previous Next Help	Ate: 9/20/2000 Event ID: 612 ime: 7:45:57 Source: Security Iser: Administrator Type: Success Audit computer: LTSERVER1 Category: Policy Change escription: Audit Policy Change: New Policy: Success Failure + + Logon/Logoff - + Dbject Access - + Privilege Use - + Detailed Tracking + + Account Management Igte: Bytes C Words		Ľ
Time: 7:45:57 Source: Security User: Administrator Type: Success Audit Computer: LTSERVER1 Category: Policy Change Description:	Time: 7:45:57 Source: Security User: Administrator Type: Success Audit Computer: LTSERVER1 Category: Policy Change Description: Audit Policy Change: New Policy: Success Failure + + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management Detailed Tracking Close Previous Next Help	ime: 7:45:57 Source: Security [ser: Administrator Type: Success Audit Category: Policy Change Pescription: Audit Policy Change: New Policy: Success Failure + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Account Management rate: ⓒ Bytes ⓒ Words I Close Previous Next Help	Date: 9/20/2000 Event ID: 612	
User: Administrator Type: Success Audit Computer: LTSERVER1 Category: Policy Change Description:	User: Administrator Type: Success Audit Computer: LTSERVER1 Category: Policy Change Description: Audit Policy Change: New Policy: Success Failure + + Logon/Logoff - + Dbject Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management ✓ Dgtar ⓒ Bytes ⓒ Words Close Previous Next Help	Iser: Administrator Type: Success Audit Category: Policy Change Audit Policy Change: Audit Policy Change: Success Failurel + + Logon/Logoff + Diject Access + + Doing/Logoff + + Doing/Logoff + + Doing/Logoff + + Policy Change + + Account Management * *	Time: 7:45:57 Source: Security	
Computer: LTSERVER1 Category: Policy Change Description: Audit Policy Change: New Policy: Success Failure + + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management Data: Data: Close Previous Next Help	Computer: LTSERVER1 Category: Policy Change Description: Audit Policy Change: New Policy: Success Failure + + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Account Management Data: Bytes C Words Close Previous Next Help	Computer: LTSERVER1 Category: Policy Change Pescription: Audit Policy Change: New Policy: Success Failurel + + Logon/Logoff + Detailed Tracking + + Policy Change + + Detailed Tracking + + Policy Change + + Account Management * * * * * * * * * * * * * * * * *	User: Administrator Type: Success Audit	
Description: Audit Policy Change: New Policy: Success Failure + + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management ✓ Data: Bytes Words Close Previous Next Help	Description: Audit Policy Change: New Policy: Success Failure + + Logon/Logoff - + Dbject Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management ✓ Dgta: Bytes Words	Audit Policy Change: New Policy: Success Failure + + System + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Account Management Interest Interest	Computer: LTSERVER1 Category: Policy Change	
Audit Policy Change: ▲ New Policy: Success Failure + + System + + Logon/Logoff - + Object Access - + Privilege Use - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management ✓ Data: Close Previous Next Help	Audit Policy Change: New Policy: Success Failure + System + Logon/Logoff - H Dbject Access - H Privilege Use - H Detailed Tracking + Policy Change + Account Management	Audit Policy Change: New Policy: Success Failure + + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management	Description:	
Success Failurel + + + + Logon/Logoff - + - - - - - - - - - - - - - - - - - - - - - - - - - - -	Success Failure + + + + Logon/Logoff - + Dietaled Tracking + + Detailed Tracking + + Policy Change + + + + Policy Change + + Account Management ▼	Success Failure + + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management ▼ I I I Close Previous Next Help	Audit Policy Change:	_
+ + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Policy Change + + Account Management ✓ Data: Bytes Words Close Previous Next Help 	+ + System + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Account Management ▼ Deta: ● Bytes ● Words ▼ Close Previous Next Help	+ + System + + Logon/Logoff - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management ▼ Pata: ● Bytes ● Words Close Previous Next Help	Success Failure	
+ + Logon/Logott - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management	+ + Logon/Logoft - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management	+ + Logon/Logot - + Object Access - + Privilege Use - + Detailed Tracking + + Policy Change + + Account Management Pate: Bytes Words Close Previous Next Help	+ + System	
		 + Object Access + Privilege Use + Detailed Tracking + + Policy Change + + Account Management 	+ + Logon/Logoff	
		 + Detailed Tracking + Policy Change + Account Management 	- + Privilege Use	
+ + Policy Change + + Account Management ✓ Data: ● Bytes ● Words Close Previous Next Help	+ + Policy Change + Account Management Date: Bytes Words Close Previous Next Help	+ + Policy Change + + Account Management gata: Bytes Words Close Previous Next Help Out	- + Detailed Tracking	
+ + Account Management D_ata: ● Bytes ● Words	+ + Account Management Data: Bytes Previous Next Help	+ + Account Management Pata: Bytes Words Close Previous Next Help	+ + Policy Change	
Data: © Bytes C Words Close Previous Next Help	Data: Bytes Vords	Data: Bytes	+ + Account Management	•
Close Previous Next Help	Close Previous Next Help	Close Previous Next Help	D _{ætar} ♥ <u>B</u> ytes . ♥ <u>₩</u> ords	
Close Previous Next Help	Close Previous Next Help	Close Previous Next Help		A
Close Previous Next Help	Close Previous Next Help	Close Previous Next Help		
Close Previous Next Help	Close Previous Next Help	Close Previous Next Help		
Close Previous Next Help	Close Previous Next Help	Close Previous Next Help		-
Close <u>Previous</u> <u>Next</u> <u>H</u> elp	Close Previous Next Help	Close Previous Next Help	् र	
Close <u>Previous Next</u> <u>H</u> elp	Close <u>Previous Next</u> <u>H</u> elp	Close <u>Previous Next</u> <u>H</u> elp		
AND	Shar hashing	Shi Shirt	Close <u>P</u> revious <u>N</u> ext <u>H</u> elp	

Event Detail for a successful Policy Change.

Event Detail for an unsuccessful login

Event Deta	il				×	
Date: Time: <u>U</u> ser: Co <u>m</u> puter:	9/20/2000 7:06:36 NT AUTHORITY\S LTSERVER1	SYSTE	Event ID: Source: Type: Category:	529 Security Failure Audit Logon/Logoff		11
Descriptior [.ogon Fai	n: Reason: User Name: Domain: Logon Type: Logon Process: Authentication Pac OFT_AUTHENTICA Workstation Name:	Unkno CGLES KSecD kage: TION_F \\LTM	wn user na SSNER DD PACKAGE_Y SU4	me or bad passwo	rd V	
	ose <u>P</u> revio	us	Next	<u>H</u> elp	* * *	

Notes:

Because of the amount of logging required for my location I have increased the log file size from the default size of 512 KB for the Security log, System log and the Application log. Also, there is a small performance overhead factor for each audit check the system performs.

For auditing to be effective regular inspection of the logs is necessary.

Reference: Microsoft Windows NT Server Networking Guide.

Section 4 Verify latest service pack from Microsoft

Microsoft Service packs are a collection of upgrades and patches for Microsoft servers. Many of the upgrades or patches are developed to fix security holes in the Microsoft NOS.

- 1. For each domain controller:
 - 1. Click Start, click Run.
 - 2. Type "Winver" and press enter.
 - 3. Note the Service Pack installed: <u>Revised Service Pack 6a</u>.

About Window	vs NT (R)
MICROSOFT. WINDOWS NI	Microsoft (R) Windows NT (R) Version 4.0 (Build 1381: Service Pack 6) Copyright (C) 1981-1996 Microsoft Corp. Revised Service Pack 6a
	This product is licensed to: MIS DRS Laurel Technologies
	Memory Available to Windows NT: 261,480 KB
	OK]

- 4. Click Start, point to Programs, and then click Windows NT Explorer.
- 5. Click the Winnt folder and then click the System 32 folder.
- 6. Right click on Schannel.dll, click Properties, click version tab and then view description.

Schannel.dll Properties
General Version Security File version: 5.00.1877.1 Description: TLS / SSL Security Provider (US and Canada Convright: Convright (C) Microsoft Corp. 1981-1998
Other version information Item name: Value: Company Name Internal Name Language Original Filename Product Name Product Version
OK Cancel Apply

If these service packs were not up to the current version, access the Microsoft site and either download the entire service pack to keep on CD or do a live update. If you believe that there is a possibility of a root kit or other hacker materials it would be best to download the service pack in it's entirety and proceed with the service pack installation.

Finally, point the source path of the service pack updates to the update folder on the file server. This is to eliminate the re-application of the service pack each time that changes are made to the file server. Hive:HKEY_LOCAL_MACHINEKey:\Software\Microsoft\Windows NT\CurrentVersionValue Name:SourcePathValue Type:REG_SZValue Data:<path to the distribution NT files.</td>



NOTE: The current service pack is NOT always recommended for a application specific server. The application ISS RealSecure is currently only tested and approved at Service Pack 5.

Reference: SANS Parliament Hill 2000 page 41.

Section 5 Tuning TCP Parameter for SYN floods

A common DOS attach is a SYN flood. The following is a brief description of what a SYN flood is a Denial of Service attack.

Technical Description: A standard TCP connection is established by sending a SYN packet to the destination host. If the destination is waiting for a connection on the specified port, it will respond with a SYN/ACK packet. The initial sender then replies to the SYN/ACK with an ACK packet, and the connection is established. When the SYN/ACK is sent back to the source, a block of memory is allocated to hold information about the state of the connection that is currently being established. Until the final ACK is received or a timeout is reached, this block of memory sits unused, waiting for more information to be received from the source host. By sending numerous SYN packets to a host, the destination will exhaust the portion of memory it has on-hand to deal with opening connections. Legitimate connections will no longer be able to connect to the host. The flood of SYN packets can detect this situation without accompanying responses. It can be corrected by sending the destination RST packets that correspond to the initial SYNs. This results in the destination host freeing up that block of memory and making room for a new legitimate connection.

Why this is important: Most systems have a pre-defined limit of active TCP connections. Once this limit is reached, additional connections are ignored. A SYN Flood attack attempts to use up these connections and then leave them idle so that the victim station cannot accept any additional connections.

How to remove this vulnerability: You should consider upgrading your operating system version or applying a service patch. Many operating systems now have heuristics for terminating idle connections that prevent SYN Floods from locking out valid connections. You can also increase the default limit of connection buffers.

Available in Service Pack 5 and later is a registry value that can reduce the number of SYN-ACK retries.

From the Run command line type REGEDIT and click on OK.

When editing the Registry it is always advisable to export a copy of the Registry before making any changes. This will enable you to restore the Registry if there are any problems with the additional or changed Registry value.

Make a backup of you current Registry.

Export Regist	ry File		1 ×	1	
Savejn. 🗍	📸 (=xkt-p	- 24	🗃 🛅 🗉		
📕 My Lompul	e.				
Network Na	sighuo hood				
📸 My Breicad	2				
File n≘rre	iecback		<u>S</u> ave	\$	
Save as piper	Bag shafian Filey	•	Cancel	7	
Lisport lange					
© AI					
© Sected transh					
			Y		

Open REGEDT32 and make the following change to your registry.

Add Value		×
<u>V</u> alue Name:	SynAttackProtect	
<u>D</u> ata Type:	REG_DWORD	▼ <u>H</u> elp
DWORD Editor		×
<u>D</u> ata:		OK
2		Cancel
Radix C <u>B</u> inary (D D <u>e</u> cimal ⊙ He <u>x</u>	

🔚 l leg	istry L	ditor						
Faqistiy	Edi.	T ≞e	View	Seculty	Options	Windler	Нөр	
THE	Y_I n	CAL_	малн	NE on L	ncal Mar	hine		
			stisos Symt Ti 28 Ti 28	i4 F1f .vent .vont num rkage rometei 2 Pers at	× 	Detellia Domain LinebleS Forward Hosthen IPEheblir NemeS: Scarcht SynAta:	eFat RFG Broat Broat Broat ROUT Broat Strict Strict	ERECI EXPANELISZ: SyStem Tradition SZ: Machine nem gillifers : REGI DYORD I U Joacts I REGI DYORD I U LGI SZ : Itservert Ior : REGI DYORD I (: REGI SZ: 14/160/211 tt 14/160/125 1014 EG_SZ: Infloch com : sot : REGI DYORD I 0/2
		-	م ا <mark>ص</mark> -	⊇Wirse Erumen I				
1			- (#1) Si - (22) - - (22) - Vi	i Cîvero Vi00 DE Catilo Fr	Ficgrøi Progrøi	n Groups ent		

Hive:	HKEY_LOCAL_MACHINE
Key:	\System\CurrentControlSet\Services\Tcpip\Parameters
Value Name:	SynAttackProtect
Value Type:	REG DWORD
Value Data:	2

The Value Data of 2 reduces the AYN-ACK retries and also the full three-way handshake must complete before the afd.sys driver commits additional resources.

Reference: SANS Parliament Hill 2000 page 54. RealSecure on-line documentation.

Section 6 Setting Security Policies

User access to network resources – files, folders and devices – in NT Server is controlled in two ways: by assigning rights to a user that grant or deny access to certain objects and by assigning permissions to objects that specify who is allowed to use objects and under what conditions.

Rights generally authorize a user to perform certain system tasks such as logging on to a server, back up and restore data or modify printer options on a shared printer.

Proper setting of the User Rights Policy found in the User Manager for Domains is essential.

Properly setting the User Rights Policy can help in securing your network. If an intruder or a displaced network administrator can set up what is being audited and what user rights can be controlled the security of your network can be compromised.

Steps in accomplishing this are as follows.

Click on User Manager for Domains Highlight Policies Click on User Rights Check the box for Show Advanced User Rights.

U≠er Rights Palicy	×
Doman LAUREL	OK.
Bight Access this computer from nervors	lancel
<u>B</u> ant T.,	Нер
Doman Admins	
Doman Leors	
Evelyone	Eqs.
	Bemove
ShowAdvanced Use Rights	

After you have accessed the above screen click on the **Right:** drop box and choose the rights that you want to modify.

For this example, use the drop down box to choose **Back up files and directories.**

User Rights Palicy	×	
Opman LAUREL	OK.	22
Bight lines and directions	lancel	.00
<u>B</u> and TL.	<u>Н</u> ер	
Administrators Backup Decrators		8-17-
Ecryc: Operators	≧dt	
	Bemove	S.
<u>Show</u> Advanced Use Bi ₂ h.v		

The rights that are granted to an individual or a group to back up files is very important because the backup operator must have access to all files in order to back them up.

As shown in the table below, from Microsoft, you only want **trusted** individuals or groups to be able to do this. Trusted groups for Domain: Lauel1 are Administrators, Backup Operators and Server Operators. If you want to Add or Remove users or groups double click on the appropriate box and choose the user/group that you want to add or remove.

User Right	Domain Controllers	Member Servers	Workstations
Access this computer from network	(anyone)	(anyone)	(anyone)
Act as part of the operating system	(no one)Do not assign to any user.	(no one)Do not assign to any user.	(no one)Do not assign to any user.
Add workstations to domain	(no one)	(no one)	(no one)
Back up files and directories	trusted users	trusted users	trusted users
Bypass traverse checking	(anyone)	(anyone)	(anyone)

Change the system time	trusted users	trusted users	trusted users
Create a pagefile	trusted users	trusted users	trusted users
Create a token object	(no one)Do not assign to any user.	(no one)Do not assign to any user.	(no one)Do not assign to any user.
Create permanent shared objects	(no one)	(no one)	(no one)
Debug programs	(no one)This right is not auditable and should not be assigned to any user, including system administrators.	(no one)This right is not auditable and should not be assigned to any user, including system administrators.	(no one)This right is not auditable and should not be assigned to any user, including system administrators.
Force shutdown from a remote system	trusted users	trusted users	trusted users
Generate security audits	(no one)Do not assign to any user.	(no one)Do not assign to any user.	(no one)Do not assign to any user.
Increase quotas	trusted users	trusted users	trusted users
Increase scheduling priority	trusted users	trusted users	trusted users
Load and unload device drivers	trusted users	trusted users	trusted users
Lock pages in memory	(no one)	(no one)	(no one)
Log on as a batch job	trusted users(as needed)	trusted users(as needed)	trusted users(as needed)
Log on as a	trusted users(as	trusted users(as	trusted users(as

needed)	needed)	needed)
trusted users	(anyone)	(anyone)
trusted users	trusted users	trusted users
trusted users	trusted users	trusted users
trusted users	trusted users	trusted users
trusted users	trusted users	trusted users
(no one)Do not assign to any user.	(no one)Do not assign to any user.	(no one)Do not assign to any user.
trusted users	trusted users	trusted users
trusted users	(anyone)	(anyone)
trusted users	trusted users	trusted users
	needed) trusted users trusted users trusted users trusted users trusted users (no one)Do not assign to any user. trusted users trusted users	needed)needed)trusted users(anyone)trusted userstrusted userstrusted userstrusted userstrusted userstrusted userstrusted userstrusted userstrusted userstrusted users(no one)Do not assign to any user.(no one)Do not assign to any user.trusted userstrusted users

Reference: Microsoft/technet/security/c2config **Reference:** Mastering Windows NT Server 4 5th edition