

# **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

## **Developments in Auditing NT**

Level Two Practical Requirements for Network Security 2000 Monterey, CA October 2000

Tom Robinette

GCNT

Disclaimer: This paper was written to satisfy GIAC 'Certification in NT Security' requirements. This paper is not intended for use as a comprehensive source for Windows NT Server audits. It is merely a guideline for some of the controls suitable to a medium security level network. As with all information related to Information Systems Security, timeliness is very important, and any network administrator should carefully review current information about Windows NT security.

### **Built-In user Accounts**

#### Introduction:

Usernames and passwords are the keys to protection for resources accessed over the network. If an attacker is able to obtain or guess the correct username, then the password is the only thing standing between him or her and the resources in question. Since user names are often based on the users real name and or department, guessing usernames may not be difficult. Tools also exist for discovering usernames on systems even remotely. One can almost define network security in whole as the securing of user accounts and their passwords.

#### **Risks:**

The administrator and guest accounts are often the target of initial attacks, as they exist by default. The Administrator account is an attractive target because it has the most rights on the network, and as an added bonus, this account cannot be locked out by bad login attempts. If the attacker can gain Administrator privileges he or she can accomplish virtually anything on the network. The Guest account by default does not have the same level of rights on the network, but is still targeted because it often has no password, or an easily guessed password. Even this basic account can give an attacker a springboard from which he or she can launch other attacks and or attempt to escalate permissions.

#### **Best Practice:**

Since Windows NT Server 4.0 comes with two default accounts (Administrator and Guest), the Administrator account should be renamed to something less obvious and the Guest account should be disabled unless it will be used. In addition to disabling the Guest account it should be assigned a password.

#### Test work:

- 1. Through inquiry determine the status of the two built-in accounts for the domain. Administrator states that the Administrator account has not been renamed, but that the guest account was renamed, and disabled.
- 2. On a domain controller install Somarsoft's DumpSec tool, available from <u>www.somarsoft.com</u> the tool is free. Open DumpSec and choose Report, then

Dump Users as a Table. From the list of Available fields select UserName, AcctDisabled, and SID as shown in the screen shot next:

Demp Users as Lable			×	
Available lie ds           Strongs           Group Comment           Group Comment           Group Comment           Group Comment           Fullhame           Account Type           Comment           Home Drive           Provile           Locon Verget           Provile Drive           Provile Drive	Arr 3 • Brmws MoveLr MoveQove Dk Cancel	Selected fields (misult unde fi User fikerie Aud Disabled Sid Chow computer accounts miservers)		

After clicking on the OK button (In the lower center of the screen above) a report like the following will be generated:

Senaryoft DampSer	e (formerly DumpAct)	Weatheatcher		- 14
e Thi Seach Ten	nn Meas Isla			
IserNane	OrictD1 sah1 ed	514		
histo	YPS	%-1-5-91-65M928R-1294628888-493919294-1812		
Mainistrator	Hu	S. 1. S. 21. MSR12208. 1294628088. 530219294. S88		
Andre allo utra	Hu	S 1 5 21 MVR12208 1294628088 500219294 1208		
ransku p	Hu	S 1 5 21 MVH1220B 1294M2H0BH 5000219294 1221		
Iberiis	Hu	S 1 5 21 65812208 1294626086 400219294 1194		
ulevų.	Mu	S=1-5-21-65812288-129462888-438219294-1269		
ill	No	5-1-5-21-65812288-129462888348249294-1844		
irapchali	ND	5-1-5-21-65012288-1294628888-488219294-1018		
itrain1	Yes	5-1-5-21-65 <b>0</b> 12288-129 <b>4</b> 628888-488219294-1281		
itiratin?	Yes	5-1-5-21-65M2288-1294628888-488219294-1282		
itrato3	Yes	2-1-5-21-65M2288-12Q4628388-49321Q294-1289		
d rai uh	Ves	S 1 5 21 MSB1220B 1294M280B8 400219294 12B4		
d mai us	Ves	S 1 5 21 MSH1220H 1294M2H0HH 500219295 1295		
I rai ut	Ves	S 1 5 21 MVH12208 1294M28088 500219294 128M		
Lrain/	Yes	S 1 5 21 65812208 1294626086 400219294 1287		
LrainB	Yes	S=1-5-21-65812238-1294628388-433219294-1288		
athyCombs	No	5-1-5-21-65012288-1294628888-488219294-1285		
itraint	Yes	5-1-5-21-65012288-1294628888-488219294-1116		
itrain2	Yes	5-1-5-21-65012288-1294628888-488219294-1117		
1 ay	Nn	5-1-5-21-65M2288-1294628888-488219294-1822		
1	Nn	%-1-5-21-65M2288-12Q4628388-03321Q2Q4-1165		
tao id	Hu	S 1 5 21 ASB1220B 1294A280B8 400219294 1808		
limit is	Hu	S 1 5 21 MS 812208 1294628088 500219294 1807		
han desser	Hu	S 1 5 21 65812208 1296628088 500219296 1259		
LaneCumbs	Hu	S 1 5 21 65812208 1294628088 400219294 1207		
livit	Nu	5-1-5-21-65812238-1294628288-433219294-1258		
xchange	Yes	5-1-5-21-65012288-1294628888-498219294-1198		
100	No	5-1-5-21-65012288-1294628888-488219294-1895		
uestX	Yes	5-1-5-21-65012288-1294628888-488219294-501		
aser	Nn	5-1-5-21-65M2288-1294628888-488219294-1888		
'HSAD NTN	YPS	%-1-5-91-65M9288-1994628888-993919994-1875		
internet	Ves	S 1 5 21 MSR12208 1294M28088 400219294 1808		
112111111111111111111111111111111111111	Hu	S 1 5 21 ASH1220B 1294A2H0BH 500219295 120B		
and Automa				
Start 🔏 Semana	lt DumpSee I 🌇	an an tean	<b>600</b>	100

We can tell by looking at this report that the Administrator account (Note that the SID ends with 500) has not been renamed, and has not been disabled. On the other hand if we look lower down to find the built-in Guest account, we see that it has been renamed to GuestX and that it has in fact been disabled. We are able to know which account is the built-in Guest account because its SID ends with 501, as shown in the screenshot below:

🚑 Sonaroft Dang See	(formerly DompArt)	Walketcher	_ 8 ×
The Tril Seach Terr	n Mexic Jeb		
liserNane	OrictD1 sah1 ed	51d	
Admin .	YPS	2-1-5-91-65M9288-1994628388-083919994-1812	
Administrator	Hu	S 1 5 21 ASB1220B 1294A280B8 500219295 588	
Routee allowing	Hu	S 1 5 21 AV 812208 1294628088 500219294 1208	
hackop	Hu	S 1 5 21 MSH1220B 129462H08H 500219294 1221	
Uberuis	Hu	S 1 5 21 65812208 1294628088 430219294 1194	
blevy	Mu	S-1-5-21-65812288-129462888-488219294-1269	
Bill	No	5-1-5-21-65012288-1294628888-488219294-1044	
brapchali	No	5-1-5-21-65012288-1294628888-488219294-1018	
btrain1	Yes	5-1-5-21-65012288-1294628888-488219294-1281	
htrai n8	YPS .	S-1-5-21-65M2288-1294628888-488219294-1282	
htrain9	YPS	2-1-5-21-65M2238-12Q4628388-48321Q2Q4-1288	
htrainh	Ves	S 1 5 21 ASB1220B 1294A280B8 430219294 1284	
hteri oʻs	Ves	S 1 5 21 65812208 1296628088 600219296 1285	
htrain <b>h</b>	Ves	S 1 5 21 65812208 1296628088 600219296 1286	
btrain/	Ves	S 1 5 21 65812208 1294628088 430219294 1287	
ULTJINU	Yes	S-1-5-21-65012288-129462888-488219294-1288	
CathyConbs	ND	5-1-5-21-65012288-1294628888-488219294-1285	
citraint	Yes	5-1-5-21-65012288-1294628888-488219294-1116	C
citrain2	Yes	5-1-5-21-65012288-1294628888-488219294-1117	
61 ay	Nn	S-1-5-21-65M2288-1294628888-488219294-1822	
c1 conhs	Nn	\$-1-5-21-65M9238-12Q4628388-49321Q294-1165	
David	Hu	S 1 5 21 ASB1220B 1294A280B8 400219294 1808	
dimit is	Hu	S 1 5 21 MSH12208 1294M2H08H 600219294 1807	C
diam desser	Hu	S 1 5 21 MSH1220H 1294M2H0HH 600219294 1269	
DianeCumbs	Hu	S 1 5 21 65812208 1294628088 430219294 1207	
drivirt	Mu	S-1-5-21-65012288-1294628288-488219294-1258	
Exchange	Yes	5-1-5-21-65012288-1294628888-488219294-1148	
Clen	No	5-1-5-21-65012288-1294628888-488219294-1005	C
Guest&	Yes	5-1-5-21-65012288-1294628888-488219294-501	
Hourr	Nn	S-1-5-21-65M2288-1294628888-488219294-1888	
THAADNTN	YPS	2-1-5-21-65M223R-1204628388-493210204-1875	
Tuleruel	Ves	S 1 5 21 ASB1220B 1296A280B8 400219294 180B	
10020_010000112	Hu	х т. у рт. мунтррон. труммуновн. косортуруул. трон.	
-bund 70,000%			0.13
🈹 Start 🔏 Semanal	t DumpSee J 🚿	Tan Juer 2 - Kin asati Wand	😸 🔕 😸 – Acto – V –

Built-In Account	Renamed (Yes or No)	Disabled (Yes or No)	Meets Best Practice Standards (Yes or
	)		No)
Administrator	No	No	No
Guest	Yes	Yes	Yes

#### **Conclusion:**

Administrator reports that the Administrator password is changed on a regular basis, and that many tools exist to determine the username for the Administrator account even when it has been renamed. While this is true we still recommend renaming the Administrator account. We also verified through the use of L0phtCrack (Discussed in the next section) that the Guest account has a password in addition to being disabled.

### Passwords

#### Introduction:

Assuming that the NetBIOS Session service, has not been disabled, then the single most effective method of attacking Windows NT Server is plain old remote password guessing. In other words, connecting to an enumerated share and trying a username/password combination, until one is found that grants access (Source: Hacking Exposed, Second Edition, Network Security Secrets and Solutions)

#### **Risks:**

Unauthorized access to system resources and data, including tampering with or destroying the information on your network.

#### **Best Practice:**

A password policy should be developed implemented and verified. This policy should include rules for minimum password length, password complexity and maximum password age. Windows NT 4.0 SP3 and later includes an optional password filter which can require complex passwords, and other third party tools are also available.

#### Test work:

1. Through inquiry determine if a password policy exists and what the details are of this policy with respect to password length, complexity, and age.

Administrator states that there is no maximum password age, that each password is required to be at least 5 characters in length and that he uses L0phtCrack to periodically test for password complexity.

2. On a Domain Controller open User Manager for Domains and click on Policies. Screenshot next:

Account Policy		×
Elomana Bostriotions Password Bostriotions Maximum Password A_e ● Hassword Nerre Express ● Expressin 📑 Days	Monnum Passivo CAge © Alox Changeo Innedialely © Alox Ebanges In Edialely Days	UK Cancel Heb
Minimum Pessword lengt: Ol Fernik Dienk, Pastword @ Al Least U 🔮 Unarade s	Peasword Ling Jeness C. Do Not Keep Fassword History C. Bemember G. A. Passwords	

3. On a Domain Controller install the L0phtCrack NT password Cracker available from <u>www.l0pht.com</u>. This tool allows an administrator to evaluate the strength of passwords on the Domain. While logged on as the Domain Administrator or equivalent you can dump the password Hashes directly from the registry and then begin cracking them. It should be noted that there are other ways to obtain the password hashes, and this tool could be used by malicious individuals to obtain passwords for accounts they are not authorized to use. The L0phtCrack tool takes advantage of weaknesses in the older LANMAN hashes. First it splits each password into two 7 character passwords and attacks each one individually. Also the LANMAN hash does not allow for lowercase characters and this reduces the number of combinations that must be attempted during a brute force attack. Screenshot of L0phtCrack below:

C.VProgo	C.VProgram Filer/L.Oph/Erack 2.9/pwd36.kr - LOph/Erack 2.5					
ile gat Taola Ministration						
For Your Stonger Let prove 2 - 0 - 10 - 7000 - other set						
	Inclusive	8	21 Passing	usedan wash	KT cash	-
SIDES-				34 345030 (0200399) 01 884504335335	E02250381E6221849452122A0015310	E 📄
· HOLD SYP				VICTOR FREE SCREEDED AND ARREST	WARE ACTO REPARTS ADDRESS AND	- T
20.00				27 YOM CLEARANNA-228-628 (19-08-6	EXAMPLE 2018 NUMBER OF A DESCRIPTION OF	
_#A3 8				08401801172810795158312708407303	492119755766338923977518801EA2+	- Ll
Sieary	EXHL:	~	1000	238mb7042088cm78mm78842sB5140466	EXCEPTINGENCE (BDM/DANESYN/NUBBN	e -
Chescy	202803	×	700014	0000100120057801888 3040305140488	CCCCC+94272007+918274280826272	s 🖬
Copay	EXACTOR	×	Talayon	SATE STERAL DESCENARE ADD STREAM AND	A077474E0044247Ab8007820752b017	2 7
Caristell	22045	×	12045	ALEO AD DE DACTE CADALE XDAE XDAE XDAE AD SUADAEB	7421700F00007500418+70400F140D5	e 🔲
Generativ	100000000000000000000000000000000000000			P7540200100010P00102X00018020081	2/1840/022/022114/001113/04/201	4 L.
Slenzy	CATACO		non-the	R077827174 (R5214 \$\$128432851404 \$\$	2411476517863#A6350141560738-25	e -
8				288455105476470480440881028514014F	771550A114825583150275128851824	2 di
CP.0				AND REPORTED AND A CONTRACT OF A CONTRACT.	VARANTE AND DESCRIPTION AND TWE	• 7
Longe				205 ACC 2045 DATES CARS AND FE	HE READ AND A VIEW OF MANY AND ADDRESS.	
Cosd.	17813	.1	19502	eesibtVoodesiPhKaaDSSRooB514016B	V055570118085177859286949198871	신물
Cosde		~		90455284m981cm78mm17854558514046m	CoE4FTX (#Se05loBJ550%mlo%Si5525	a -
Course	TOSLOC	×	yellow	CIAPOLACCODOCCOOLAR XD4CADS140488	4120026140205720000000000000000000	e 👘
Courde	G2.3.5 B	×	10.000	1052 SECTOR STRANGE SHOWER	CORCHODAD CLASSEWEREDOND 71100100	2 T
Courds	CHERRY	×	Chevry	GEODESCOT FOTOECOMMENDADESDADSLAGANE	0102#3.60#760070047000070770073A	a 🗐
For:11	CATECON	~	tion of the h	32000078500+1830840.0040305140+88	CONTRACT/2007/004280-1487580001	- 2
Fox93	STOZEK		-1 I'M	30345221212040275502843285140188	POTRESCREASS FLORENCESS PETRECORE	e
Fu - 45	0.33550		There's	2717874874271874462819285140188	202220050C8B4100328254549855932	2 🖬
1 44	80033-0			A S CHEMY - 24 THE S CHECK DOWN MILLER	S MALEA MR (S VAR 100 DO LARROV CONA-	• T
1.0.4.1	100.000.000.000			VAREFAR OF THE SEARCH HERE HERE IN THE DECK	VARANTE NEWLY AREA AND DEPART.	
Local	EVILOPAL <sup>2</sup>		Evilouid	3805568-AV7552871A5811878PA60350	collings:ASPloPeCUTIVES.e21:	2
Cosdia	Casta	~	11951	22090764/2274807mm7845885140465	AIZIIOBSIIVASIBSERISBS (DSSESBIE	
Cordic	2112221		-	907/3070070341001400205310000422	D118700044417007410007070780008	-
Cordia	LCSCCADE:		scritable	D0212+D0500D00XII37D+87100416820	7075&1705A7A2761076D7001D8001D1	•
Cordic		×		STERZON NOTENDAR (D40705140483	3100100000012516400010000014160	:
For 11 C	E THE EV	~	"doers	0003030201-050028403040305140488	20521000326081608161081608160-8	1 🗖
٩						ЪĒ
haering, p2p	an Shound July				ПЛН	
🗰 Start 🖗	The over 3 bies	usadi 9.5	والمرجد التراس	non Meall In	<b>(49)</b>	1
			Carl and the second	and the state of t		16 T

As you can tell from the screenshot, a tool like L0phtCrack can make very quick work of simple passwords. After running for only a few seconds it has found nearly half the passwords in the domain and will have finished a brute force attack in less than 3 hours.

Domain Name	Minimum	Minimum	Maximum	Compensating
	Password	Password	Password Age	Controls
	Length	Complexity		present
SDGI	5 Characters	Stated Policy does not meet Best Practice	None	L0phtCrack is used to test Password complexity on an approximately monthly basis

#### **Conclusion:**

While L0phtCrack is a very useful tool for testing the strength of NT passwords, a tool such as PASSFILT.DLL available on Windows NT SP 3 and higher gives a network administrator the ability to manage password policies in a much more structured manner. This is especially important on larger networks. In order to install PASSFILT.DLL you should open REGEDT32 on the Domain Controller and browse to the Notification Packages shown below: Add the Value PASSFILT, close REGEDT32 and reboot.



Further recommendations include: Increasing the password length to 8 characters and setting passwords to expire in 45 days. These setting can be changed on a Domain Controller by opening User Manager for Domains and then clicking on Policies, and then clicking on Account. It should be noted that simply installing PASSFILT.DLL does not affect the passwords already in existence on the Domain, and unless those passwords are set to expire they will not be affected by the installation of PASSFILT.DLL until the next time the passwords are changed (Source: Heckendorn, Sherri, SANS GCNT Certification Practical).

### **Service Packs**

#### Introduction:

"Service packs are the means by which Windows NT product updates are distributed. Service packs keep the product current, and extend and update your computer's functionality. Service packs include updates, system administration tools, drivers, and additional components. ... Service packs are cumulative – each new service pack contains all the fixes in previous service packs, as well as any new fixes. You do not need to install a previous service pack before you install the latest one." (Source: How to Obtain the Latest Windows NT 4.0 Service Pack, Microsoft Knowledge Base Article ID Q152734)

#### Risks:

Microsoft publishes fixes to security holes, and Denial of Service attacks, and then bundles them together into Service packs along with other components. Because of Windows NT's complexity these ongoing updates; which occur as the OS is exposed to attack over a period of time, are perhaps the second best way (after installing a perimeter Firewall) to protect your system from Known Security Vulnerabilities and Denial of Service attacks.

#### **Best Practices:**

Your NT servers should all be brought up to the most recently available Service Pack level as soon as possible, but it is very important that these new Service Pack's be tested in a Non-Production environment first, to ensure that they will not cause unforeseen problems on the network.

#### Test work:

1. For the Domain Controllers on the network run the Winver.exe program located in the <u>\\systemroot\system32</u> subdirectory. Click on Start, then run, then type winver.exe and press enter. A screen similar to the one shown below should appear. Note that the Service Pack level along with the version number of the Operating System and the Memory available to the Operating System are all shown on this screen. Screenshot next:

About Window	vs NT (R) 💌	
MICROSOFT MICROSOFT	Microvelt (R) Windowy NT (R) Version 4.0 (Build 1981, Bervice Fack 6) Copyr grit (C) 1981-1996 Microsoft Dore, Revised Service Pack 6a	
	Tiris product is licensed to USB Systems Elesign Group	
	Memory Available to Windows N (* 1111) 404 K	
	[	400

At the time of this writing, Service pack 6a was the most up to date Service Pack available for Windows NT 4.0 Server.

Server Name	Service Pack Installed	Control in Place to Monitor
		new Service Pack Releases?
SURFWATCHER	Revised Service Pack 6a	Administrator receives
		TechNet Subscription from
		Microsoft Corporation,
		which includes new Service
	JC 1	Packs upon release.

#### **Conclusion:**

A policy of testing the Service packs on non-production machines was not well defined, and the Administrator knew of times when installing the latest available service pack had cause unforeseen problems. With this knowledge we recommend that all new Service Packs be tested on non-production machines before being placed into production environments.

### Modems

#### Introduction:

When users connect modems to their workstations, they have created another avenue into the network, which may completely bypass all the other security controls in place on a network.

#### Risks:

Attackers can use wardialers to search for and identify modems attacked to computers. Once these modem numbers are identified the attacker will have another way to attack the system.

#### **Best Practices:**

Define a company wide policy on the use of Modems on individual workstations, and whenever possible do not allow individual modems on the network. In the cases where a demonstrable need exists, do not use phone numbers within the same block as published phone numbers for the company and leave the modems turned off or unplugged unless they are actually in use, or need to be in use.

#### Test work:

- 1. Determine through inquire which workstations need modems. Administrator states, that the only modems on network client machines are on laptop computers and than none of them should be connected to an analog phone line at any time. Administrator further states that he controls access to the only analog phone lines in the company and only connects them when a specific need arises. He is aware of cellular technology which would allow users to connect to the Internet without the use of an analog line but this risk is deemed miniscule.
- 2. Visually inspect workstations to determine which if any have modems and whether they are attached to phone lines.

Domain username	Machine Serial	Is Modem Present	Is Modem attached
for Primary User	Number	(Yes/No)	to functioning
			phone line (Yes/No)
Papa	6822BW27L333	No	No
Smurfette	6822BW27L346	No	No
Brainy	6822BW27L291	No	No
Grouchy	6822BW27J462	Yes	No

Gargamel	6822BW27L398	No	No
Нарру	6822BW27L316	Yes	No
Azrial	6822BW27J461	No	No

#### **Conclusion:**

While controls are not in place to ensure that the stated policy remains in effect, the stated policy does conform to best practices, and no further action is necessary other than periodically verifying that users with modems do not have easy access to phone lines that the Administrator is unaware of.

## **Audit Logs**

#### Introduction:

One of the most important steps in detecting intruders or other unauthorized activity is to enable audit logs within NT 4.0. Auditing is not enabled by default in NT server and must be enabled. Of course merely turning auditing on is not sufficient; there must also be a mechanism in place for reviewing the logs.

#### Risks:

First you have to decide which events to audit and then whether to audit success or failure or both for each event. If you choose too many events, you may lose valuable information under a sea of unnecessary events. If on the other hand you do not audit enough events, then the useful information may never be recorded in the first place. Another risk lies in how well you can protect the logs after they have been generated. An attacker may attempt to fill the log files up in order to cause your system to hang or stop responding, or if the attacker gains sufficient rights on your network, he or she may attempt to change or delete individual entries or the entire log file.

#### **Best Practices:**

See table below (In Test work Section) for best practices for Medium Security Network. (Source: Windows Security Step-by-Step. The SANS Institute)

#### Test work:

On a domain controller (Logged in as Administrator or equivalent) open User Manager for Domains, click on Polices, and then Audit. The next Screenshot shows the result:

Audit Policy			×	
Domein: SDGI			OK.	
C <u>D</u> o Mut Andik			Cancel	
	Success	Leure	Цер	:00
Logon and Logolt				
Elic and Object Access	R.	R		c
<u>U</u> se of User Rights	R	R		
User and Group Menagement		Π		
Security Policy Changed	5	M		
Bevlar, Shudown, and System		Γ		r
Process Tracking	<b>V</b>	9		

Event to be Audited	Stated Policy from Inquiry to Network Administrator	Best Practice from SANS Windows NT Security Step- by-Step	Value discovered in Testing	Comments
Logon and Logoff Success	Disabled	Enabled	Disabled	Complies with stated policy but the stated policy does not meet Best Practice.
Logon and Logoff Failure	Disabled	Enabled	Disabled	Complies with stated policy but the stated policy does not meet Best Practice.
File and Object Access Success	Enabled	Disabled	Enabled	Complies with stated policy but the stated policy does not meet Best Practice.
File and Object Access Failure	Enabled	Enabled	Enabled	
Use of User Rights Success	Enabled	Disabled	Enabled	Exceeds Best Practice
Use of User Rights Failure	Enabled	Enabled	Enabled	
User and Group Management Success	Disabled	Disabled	Disabled	
User and Group Management Failure	Disabled	Disabled	Disabled	
Security Policy	Enabled	Enabled	Enabled	

Changes Success				
Security Policy	Enabled	Enabled	Enabled	
Changes Failure				
Restart, Shutdown,	Disabled	Enabled	Disabled	Complies with
and System				stated policy but
Success				the stated policy
				does not meet Best
				Practice.
Restart, Shutdown,	Disabled	Enabled	Disabled	Complies with
and System Failure				stated policy but
				the stated policy
			c.S	does not meet Best
				Practice.
Process Tracking	Enabled	Disabled	Enabled	Exceeds Best
Success				Practice
Process Tracking	Enabled	Disabled	Enabled	Exceeds Best
Failure				Practice

#### **Conclusion:**

The Audit events which are not being monitored to the level suggested as Best Practice for a medium security network should be escalated to that minimum level. Policies should also be in place for how large these logs are allowed to grow, and what happens when the log reaches its maximum size. If the log overwrites older data you may lose log entries before they can be reviewed, but if you don't allow the log entries to wrap, then an attacker may use this as a denial of service attack. The recommendation is to have sufficient space for log entries to give you time to move them to a more permanent storage device. In order to set the configuration options for the size and wrapping of the logs open the event viewer from the Administrative Tools folder. Click on Log, and then click on Log Settings. Screenshot below:

Event Log Settings	×
Change Settings for System 💌 Log	OK.
	Dancel
Moximum Log Size: 1101034 🖹 Kilobytooi (644 Incremento)	Default
vent Log Wiasping	Нер
C Elverynte Events as <u>N</u> eenen	
🐑 Hverzht- Events Elter than 🛛 🚍 Days	
O Do No: Overwrite Evento (Clear Log f/ anually)	

## Hotfixes

#### Introduction:

While the subject of Hotfixes is undeniably related to Service packs discussed above, there are key differences which warrant individual attention. Hotfixes, are released by Microsoft in order to fix bugs, or close security holes which cannot wait for the next Service pack release. Typically many of these Hotfixes are bundled together to form a service pack.

#### Risks:

Hotfixes are not nearly as thoroughly tested as Service packs, and even Service packs sometimes have unexpected results. Consider the following statement from a Microsoft Hotfix: (This is typically found on virtually all Hotfixes, especially when they first come out) 'Emphasis added'

A supported fix that corrects this problem is now available from Microsoft, but <u>it has not been fully regression tested</u> and should be applied only to computers that are experiencing this specific problem. <u>If you are not severely affected</u> by this specific problem, Microsoft recommends that you <u>wait for the next Windows NT 4.0 service pack</u> that contains this fix.

As you can tell from the statement, you should be very cautious about applying Hotfixes, and only apply them after they have been tested on non-production machines. The network administrator must then make a decision about whether to apply Hotfixes based on the perceived threat the Hotfix is patching.

#### **Best Practices:**

Many Hotfixes fix security vulnerabilities that should be addressed as quickly as possible, so it may not be possible to wait for the Service pack release to apply the patch to your system. Therefore the best practice is to review all the Hotfixes available for the current Service pack release you have in Production and decide which if any of them should be applied immediately. Third party tools are available to help Administrators track, research and apply Hotfixes to NT servers. One such tool is called SPQuery, and is available from St. Bernard Software (http://www.stbernard.com). This tool allows administrators to remotely check which hotfixes are applied on servers, research hotfixes on Microsoft's website, and even download and apply the hotfixes to remote servers. After installing the product on the management workstation, you merely select the domain and then the specific machine or group of machines you are interested in then click the Query Machine button. The output which is generated (shown below) lists all the available Hotfixes for the service pack level running on the machine, and whether or not that particular Hotfix has been applied. In the example below only the first Hotfix has been applied. Highlighting any of the Hotfixes and clicking the Hotfix Info button opens a window to Microsoft's technical support database which contains the most current information about the hotfix

STOL 199					비미 저	
For the Nation Technic Is But	4					
Pathapati Hali	COL Protection (1)	e dest	Stationard Handle Latter Station			
1 CAMP	Notice SETEXABLE METALE DETENDED TO THE REPORT OF THE TWO AND AND AN ADDRESS TO A DETENDED AND					
프 [] (je tali sa angela)	Co Fame	<ul> <li>FL Arche</li> </ul>	IN COMPANY AND A DESCRIPTION OF A DESCRI	213	29.0 •	
† <b>D</b> ≦ :-u	<ul> <li>Comparison</li> </ul>	3.65723	Window Style (1997) and a provide Hall thread DEC Control Worth Alter	202031	versor with	
1 : 1 <b>모광</b> : 10 1	🔶 CT 162 1-5	1.0485	We hould be also be. Been also is it you work the instance of the	Ne in de	a tina inte	
1 T 🗖 🛃 T (107)	I A AK F - 1	N 1 7 28	An harden of the sub-sub-the beaution in the second data and	16 A 16	ST DO AN	
· · · · · · · · · · · · · · · · · · ·	🔶 CARROES	\$ 7757510	Walkerin, #UWA 17D #1Strategic Advanced a Differential	"K.sk.	A Distance of the second se	
	⊕ C0.0001-C	11276	Vardes N 400 Scouty Sick Held to Like Shoth with y	'k: <b>r</b> :xka	ve sværeke	
	6 C/3091C	3.0.57.29	Window Killin George Bion Neo, e En Unide Vitalience p	'komules	<ul> <li>discurption</li> </ul>	
	e compre	1.013.2	Window Mit 4 Stends Texts 100 Text Charles & Anneship	An Broken	COMPANY MAL	
1 1 <b>1 2</b>	• convict	1.07.25	We know it for all generations that the available of the state	A A A	. I that whe	
i i 🗖 🕽 end end lingt	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	·	ta kunk in se skinde Kon bases bulanti. Anna a a ba		1 1 1 1 1 1 1	
1 10 - 5 11 11	Costants E S	s rours	Valuety 40 a distribution where the structure and at the	"K.sk.	CO DATA MALE	
i i 🗆 🗛 🖓 VALLE	1 @ Ca.2012	31.8.2.9	Mulders M. A. Sondi, Roth Repair (Reaction of Repairs According 4) and	'k: <b>r</b> :xk:	NO DOWN HORKS	
i 🛛 🗗 Hasan Hah	10 CL751C	7 1 3 7 5	Window F. 10 Group, Web IV Spield Virie L. 1915 Straight Fee	ACTIONS	1 9 00/2 Sideo	
	D COMPTO	1.0511	A DESAULT THE SECOND CONTRACT OF SOME TWO AND A		11112 010-	
+ Da - Frank	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	11. 416	Caller, the should be a source to the state			
I Hat	The Local Action	C 1. 041-8				
· □3 === a	W CRESSER	5 1.22.2.5	AND AND A DATE OF THE AND THE AND THE AND	R.8R.	CO DAY AND	
		111122	Kundelwighten in Einschnermatigen verschieft von Versicherung was eine anderenden um Werden eine die Neuerale under die eine die in die einstellte.	K:F:XK:	NO 2007 X 200	
		2 A 20 Car	- An active in the backgroup of the methods of the second state of the second secon	ACTION 2	· 5 50/2 51345	
	- C2 5214	1.07TZ	All the second secon	al book	1.0.0	
	the second second		te base of the second second of the second second			
		61.000.00	the shear has been been a shear and below the second s			
	a second	1 1 4 2 1	<ul> <li>Constitute Description and a constant of the second se second second sec</li></ul>	'been obe	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
	a possile	1.000	Service of the servic	K.S.XKS		
1	<u> </u>				n non all	

After gathering the information on the Hotfix, you can elect to download it into the SPQuery database, at which time it will be available to install on any of the remote machines. SPQuery is also updated automatically so its list of available hotfixes remains current.

In order to install a hotfix on a remote machine you must first download the hotfix in question. This is accomplished by right clicking on the Hotfix and choosing download. SPQuery automatically downloads the hotfix from the Microsoft FTP site, and places it in its download database. It then shows that the Hotfix is downloaded:

19 1 H M.			
The view in case. Device Toxic	Set is		
H. 7 Martin - Bal		utres as	
50746 x	Mathers well, Ref. and Representations are seen to be a state of the second	al Carlon, 1794, 1914, 1944	
H Die Karlowerten H Die Herten Hart Herten Hier Herten	<ul> <li>Test for a</li> <li>Winstein R. Standy P. B. Berner, M. B. Berner, M. B. Berner, M. B. Berner, P. B. Berner, P. B. Standy, P. Berner, B. Berner, B. Berner, B. Berner, B. Berner, B. B. Berner, M. Berner, B. Berner,</li></ul>	New 112 + 11 123 + 11 124 + 14 124 + 14 124 + 14 125 + 16 125 + 17 125 + 17 1	Claim House consul House consul
	<ul> <li>Constant A. D. Samponi, C. Maria (Ref. p. 1988) in proceeds. Neurosci 1999; S. S. Samponi, S. Samponi</li></ul>	4 medite 4 medi	Historysond Historysond Historysond Historysond Historysond Historysond Historysond Historysond Historysond Historysond Historysond Historysond Historysond

When you are ready to apply the hotfix to a remote machine simply click on the machine in the left pane, and then right click on the hotfix in the right pane, and then choose "Install to..[machine\_name]" as shown in the screenshot below:

Marra			<b>A</b> N
and the build of the second of the second	H4		
100 <b>2</b> 000 Si Lao	- 38년 1월 🖬 👘 🎲	0	
vertexnet indentation in A	entreed Average will been write free care tool	·	
1 a Asm	For a MINARCE ARE One and December of the second system of the second sy	The second second second second	
E - TRACKARTAN	hile	[.es	Charles
医 新聞	STSERTATES and the analysis and shows any	12.22 YY	Hab.s.b
3 2E011S	IN A Second se	N I wild a	
<b>14</b> 7-520 V	(10) AUXOR (Private Private Reasonably and ).	NU WALK	DOMESTIC:
-12-1-14	<ul> <li>Bill AUG-bill MetzAlever Antonio Reprod Accus, Edit Protomos, CARP, M. Jop 1.</li> </ul>	Not related	He karaska
15 ACC ELU	(A) "UNacceptions and a show Shall at "Chandels"	F di stalac	Holdstein auto:
	<ul> <li>HT- Cetary Data Clengte TV DestroySuperiting</li> </ul>	the only	Here's week
· · · · ·	<ul> <li>HT DOES - Does IN Set Set and Million Re-</li> </ul>	Li Caleba	Hake ek
그 김 가슴을 걸었다.	10.19. In the other production is the standard sector.	N Emilia -	Haberth
	1042 with the second	N L while a	
	CHI 401 Adductions (19 dy LLPA), page 1 A sets on the direct Million	Not véalor	He kar ock:
	INTA Vectory Lass 2 Tec. U.2.1 and Devel Possick Decking Values aligned	to states	Heldsternade:
HA LOOM	<ul> <li>HT - Oderany Two or Shipped TD and IPC Power drawning:</li> </ul>	the velocity	Hark a wis
1. 10.	<ul> <li>HT - Official in Terror Material Pair (particular and end Ball)</li> </ul>	Li Caleba	Hake ek
⊨ - <b>Isa</b> Nation	III - OS and - Rook Malician Frank, "Frank and Prank Works in gPFR and	K the faile	Hakes ik
E- 📷 A	III Albert a second prophysics (Karl Press alg	N L while a	
F 🕂 🖬 \$\$72	<ul> <li>III 4 Public Hall of Around Collector Could a for the Around a State</li> </ul>	NJ WALK	BARALE.
	:1001Acrolingue ar Loke/All of Local (Reds) is predictor as a set 1	No water	Holds.et adds
	(All SUSACONST as a style OF Low Walk );	F 3 (Jalac	Holdstein auto:
	<ul> <li>HT 100 eta ny Taona diafantan'i Pantana al-Asarik -Panashiy,</li> </ul>	th all the second se	How to an order
	<ul> <li>HT_00005020 av 16 wiep005 17</li> </ul>	L L Mala	Hake ek
	(B) S100 (a) the K[S46]Second state of the boot Hadren parameter in the fill.	N Frank (	Haberth
	provide the Collinson of the Colling and the Collinson of the Collinson of the Collinson of the Collinson of the	N L HER L	the data of the
	As Occur costs as a list. Longology and a list of the second seco	No waloo	Heidelwer socke
	(Hit repeat for angiather realing) when a state of the second s	F 3 states	<ul> <li>Holdstart adds;</li> </ul>
	(HT) Cenary Even elsement Extend Parslags)	the value	Horizon with
	CONTRACTOR -		
	Concentration and Concentration		
	rg now		
	2F		
	14		

#### Test work:

Generate Report from SPQuery and compare it to the list the Administrator keeps of Hotfixes which should be applied to the NT servers. The Administrator generates his list of Hotfixes to apply based on researching the available hotfixes listed in SPQuery and reading his subscription to the Microsoft Security Bulletin. You can subscribe to this service by following these steps: (The following taken from the Microsoft Website, http://www.microsoft.com/technet/security/notify.asp)

- 1. Compose an e-mail to <u>microsoft security-subscribe-request@announce.microsoft.com</u>. The subject line and the message body are not used to process the subscription request, and can be anything you like.
- 2. Send the e-mail.
- 3. You'll receive a response, asking you to verify that you really want to subscribe. Compose a reply, and put "OK" in the message body. (Without the quotes). Send the reply
- 4. You'll receive two e-mails, one telling you that you've been added to the subscriber list, and the other with more information on the notification the

## service and its purpose. You'll receive security notifications whenever we send them.

#### **Conclusion:**

Once a hotfix is identified as one that should be applied to a server, it is then tested on a Non-Production machine, and only then placed on the list to be applied to the Production machines, using SPQuery. The Microsoft Security Bulletin is an excellent way to keep up to date with the Hotfixes available for a particular Service Pack. The stated policy for this section is above and beyond the best practice recommendation and is working as intended.

© SANS Institute 2000 - 2002

#### References

- Fossen, Jason; Kolde, Jennifer. Securing Windows NT, Step-by-Step, Parts 1-3. The SANS Institute GIAC Training 2000.
- Heckendorn, Sherri, SANS GCNT Practical. The SANS Institute. Available Online at <u>http://www.sans.org/y2k/practical/Sherri\_Heckendorn.doc</u>
- "How to Obtain the Latest Windows NT 4.0 Service pack." Microsoft Knowledge Base Article ID: Q152734. Available Online at <u>http://support.microsoft.com</u>
- McDowall, Tracey. Developments in Auditing NT. SANS GCNT Practical. The SANS Institute. Available Online at http://www.sans.org/y2k/practical/Tracey\_McDowall.doc
- Scambray, Joel; McClure, Stuart; Kurtz, George. Hacking Exposed, Second Edition, Network Security Secrets & Solutions. Osborne/McGraw-Hill, 2001.
- Schultz, E. Eugene. Windows NT/2000 Network Security. Macmillan Technical Publishing. 2000.
- Windows Security Step-by-Step. The SANS Institute, 1999. Available online at <u>http://www.sans.org</u>