

# **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

### Securing a Windows 2000 Server Connected to the Internet

For SANS New Orleans 2001

By: James Oryszczyn

### Securing Windows 2000 with IIS 5.0 to use on the Internet.

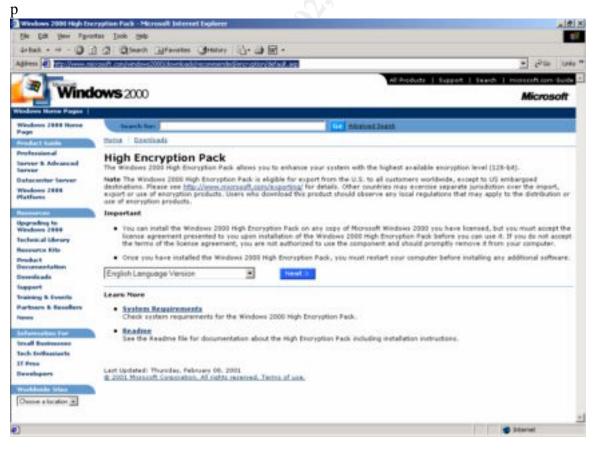
This paper is a guide on how to harden Windows 2000 for use on the Internet. I will also show steps to on how to make IIS 5.0 more secure. Security is ever changing and policies and procedures will change. This document provides no guaranties and should be used only as a guide. This paper was written to fulfill the requirement for SANS GIAC certification.

These procedures were performed on a standalone Windows 2000 server. All of the steps discussed in this document should be tested in a lab situation before implemented on production systems. This will ensure that production systems stay up and running. Always make sure you test changes on non-production machines.

#### **Hot Fixes and Service Packs**

Build you Windows 2000 Web server off of the network and not connected to the Internet. This will ensure that the machine has not been tampered with.

Apply Service Pack 1 for Windows 2000. If you are not running the high encryption pack for Windows 2000 you need to update your system to the 128-bit encryption. Go to http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.as



Use the standard download and download it to your machine



The file you download will be Encpack\_Win2000\_EN. Double click to run it

Microsoft	Microsoft Windows 2000 High Encryption (128-bit) Capability 🔀					
٩	is will need Mercsoft windows 2000 high encryption (128 bit) capability. Do you wish to continue ?					
	Y03 NO					

Click on yes to continue and after the High encryption is installed reboot your computer.

Now you are ready to install Service Pack 1 or greater for Windows 2000(Service Pack 1 was the latest and greatest at the time of this document). You can get this service pack from windowsupdate.microsoft.com. Make sure that you install the lasted and greatest service pack.

You also need to apply some hot fixes to IIS and to Windows 2000. You can automatically check to see what hot fix you need for IIS by downloading the IIS hot fix checking tool <u>http://www.microsoft.com/technet/security/tools.asp</u>.

This tool is a must have for anyone supporting IIS 5.0. It has many useful features like logging missing hot fixes to the event log and you can event customize the script to send you an email on the hot fixes that are missing.

Extract it to a folder of your choice and run it. You may have to run this command cscript.exe //H:Cscript. This will change the default script host to cscript.exe. Go to a command prompt and change to the directory were the hot fix tool was extracted. Run hfcheck.wsf and it will query a Microsoft server and come back with the hot fixes you need for IIS 5.0. Below is an example of the hot fix tool. **Warning!!!! You still need to check for Windows 2000 Hot fixes**.

nun, Sikker (ayakem Jan) muleke	لكلد
HPCHECH Notfix Check Script 1.88 I Thomas Demi (ChanadUnicrosoft.com) :	
otfix Warning for Machine JIDCJ: makta to verify MmLFix install ierosoft Security Bulletin (MSG1-B16) ink: http://www.micrusoft.com/tachmat/security/bullatin/HSG1-G16.asp	
issing Notfix on Machine JIDCJ Detected: icrosoft Xecowity Hulletin (MSM1-M14) alformed URL can Gause Service Failure in HIS 5.0 and Exchange 2000 ink: http://www.microsoft.com/tachmet/security/bulletim/HS01-014.acp	
issing Notfix on Machine JIECJ Detected: icrosoft Scennity Hulletin (MSM1-894) alformed .WIR Request Allows Reading of File Pragments ink: http://www.microsoft.com/tachmat/security/bullatin/NSM1-8941.acp	
issing Hotfix on Machine JTBCJ Datacted: ierosoft Scennity Hulletin (MSHM-188) atch Available for "Malformed Web Forn Submission" Vulnerability ink: http://www.nicrosoft.com/technet/secondity/hulletin/NSHM-1990.asp	
issing Hotfix on Machine JTBCJ Detected: 1erosoft Scourity Hullotin (MSMM-MMS) atch Available for "Web Server File Request Parsing" Vulnerability ink: http://www.nicrosoft.com/technet/secoreity/holletin/NSMM-MS6.asp	
issing Hotfix on Hachine JTECI Detected: lerosoft Scourity Hullotin (MSMM-MNM) atch Available for "Session ID Cookie Marking" Vulnerability ink: http://www.nierosoft.com/tochact/accordity/hotfetim/MSMM-MSH.asp	
issing Hotfix on Hachine JTECI Datasted: lerosoft Scourity Hulletin (MSAN-928) atch Available for "Yeb Server Folder Traversal" Vulnerability ink: http://www.nierosoft.com/technet/scorrity/hotletin/MSAN-MSK-sap	
issing Hotfix on Machine JTECA Detected: ierosoft Security Bulletin (MS08-060) atch Available for "[[S Crocc Site Scripting" Vulnerabilities ink: http://www.nierosoft.com/technet/security/bulletin/MSNN-MAM.asp	
izzing Hutfis un Bachine JTMML Detected: ierozoft Scourity Bulletin (MSCB-D5B) atch Available for "Specialized Header" Volmerability ink: http://www.nierozoft.com/technet/zeeurity/bulletin/DSMM-M58.asp	
izzing Hutfiz un Machine JTMAL Detected: icrosoft Security Dulletin (MSGB 857) atch Available for "File Permission Canonicalization" Volmerability ink: http://www.nierosoft.com/technet/security/bulletin/MSGG-057.asp	
iccing Hutfis on Bachine (TRNA Detected) icrosoft Security Bulletin (HSOB 844)	

Example of the missing hot fix in the event logs. Microsoft has been very helpful by providing the Security Bulletin Number and the URL to the hot fix.

Event Prope	rties	-				<u> î ×</u>	
Event							
Tine.	3/ 0/200 0.00 Warning MA JTEC.	Calegoly	N_ri=			+ +	
Peace pro-	m						.5
Microsoft Fatch Av Link: http	lotfix on Moor Sectory Hote allable for 195 2777777 more	tin (M. 1114) tetialized He co <sup>s</sup> t.com/tec	-11) /sder" Valm	ersbilty itte/bulletin/h	45:00-05	8.≣≈p	6
Dista: P*	Bytes 🔿 W	ords				<u>_</u>	
						I	
		I	IK.	Dancel		Apply	

You can modify the script that Microsoft created to allow you to send an email to an admin if a hot fix is missing.

#### Sample:

```
Set objMsg = CreateObject("CDONTS.NewMail")
'Set the properties of the Message
objMsg.From = "HotfixNotification@YourCompany.com"
objMsg.To = "Administrators@YourCompany.com"
objMsg.Subject = "Missing Hotfix Detected!"
objMsg.Body = "Microsoft Security Bulletin
(" + sBulletin + ") " + sTitle + " Link:
    http://www.microsoft.com" + sLink
objMsg.Send
```

You can also schedule the hot fix tool to run with the at schedule command. I recommend scheduling this script to run at least once a week to make sure that all updates have been applied. This tool can also be run remotely. You could run this tool from a management workstation allowing to checking of all the web servers in the enterprise and allowing the tool to log in a central location below is a sample command to schedule the script.

Select LINSANS/System IZ/condiexe
CSN Sal
Status ID Day
Time Connead Line
I Each U
I2:00 AM StreamstooleNhfohsok.wef
CSN

AT.EXE 12:00am /INTERACTIVE /every:Wednesday c:\sanstools\hfcheck.wsf

Below is a URL to the current hot fixes needed to secure IIS 5.0 and Windows 2000. You should apply all of these hot fixes until Windows 2000 SP2 becomes available. Make sure that you install the hot fixes in order. Start with the oldest hot fix and work you way to the latest hot fix.

IIS Link : http://www.microsoft.com/technet/security/current.asp?productID=15

Windows 2000 Link: http://www.microsoft.com/technet/security/current.asp?productID=43

## **OS Hardening**

#### **Disabling Services**

Windows 2000 comes default with a slew of services enabled. Most of these services are unneeded. They either take up server memory or make a web server vulnerable. You need to go to computer management and then services and applications. Expand Services and Applications and click on services.

🖵 Computer Hanagement					
Acaphi Kew 🔶 🔿 🔯	🔄 II; 🔐 🕨 =	11 - 11-			
u <del>na</del>	Kame 🗠	Description	Status	Startup Type	Log 🔺
🔍 (Longues Management (Local)	Sector 👋	Ketfessel	Stated	A romatic	- Latz
🗐 📆 System Tuck	🍇 Application Managara	Provided Service		Manual	L.s.
ភ្មា 🏭 Storaga	Section -	Sipports C		Manual	- Lorz
🗄 💑 Services and Applications	🎭 COM+ Event Evstern	Provides a m	Started	Manual	L.s
🗓 🔂 Iclephony	🎭 Computer Browser	Photoins a	Stated	A romatic	- Lorz
- 🌺 🖓 Unad	Sector Cient	Мана јез на с	Started	Automatic	- Discon
- 🥸 Services	🎭 Detributen Die 15st 👑	Manages In.	"to ted	A romatic	- Invilli
👎 🎇 Cidexing Service	🎭 Dishi Luketi Birk Tra 🗤	Sends rict I	Started	Automatic	- D.all
🗓 🍓 "harend" "hären dan Erry ors	🎭 Distributed Unik i ra	Stores infol .		Manual	- Loce 🔅
	🎭 Dishi Euler, Transaca 👘	Coordinate	Started	Automatic	- D.all
	🎭 D'E Clert	Resolves a	Lts ted	Automatic	- Loce 🔅
	🎭Event Log	Logs event	Started	Automatic	- Lota 🎆
	🎭 to Service	Leips you		Manual	- Loce 🔅
	🎇 Ele Benkritht	Monthins B.,		Manual	— Inv 🚟
	🎭 HF Fublishing Service .	Provides L.	Lts ted	Automatic	- Loce 🔅
	🏀 TS Action Service	Albesteff	Stated	A romatic	- Invilli
	🎭 Inde ang Service	Incepies to		Manual	- Loce 🔅
	🍇 Distance Monitory	Sipportsia	Stated	A romatic	- Invilli
	🎭 Cremet Cornectio	Provided in a		Manual	- L
	🍇 "https://www.com	Albuster		Disabled	larz 💌
	<u> </u>				···· Þ

As you can see that by default many services are enabled by default. Most of these services are needed when the 2000 Server is part of a domain, but not needed on a web server. When you disable the Server, Workstation and TCP/IP Netbios Helper you can prevent a hacker from pulling information remotely using netbios and null sessions. Below is a list of services and there explanation that can be disabled. I recommended disabling as many services as you can. Warning, Some services like the server service or workstation might need to be enabled if you are using a commercial backup product

Alerter	Used to Send Administrative alerts to a list of Netbios	Disable
	names	
Computer	Builts and maintains a list of computers and domains in	Disable

Browser	Network Neighbor Hood	
Distributed File	Manages logical volumes distributed across a local or	Disable
System	wide area network.	
Distributed Link	Sends notifications of files moving between NTFS	Disable
Tracking Client	volumes in a network domain.	
Distributed Link	Stores information so that files moved between	Disable
Tracking Server	volumes can be tracked for each volume in the domain.	
DNS Client	Resolves and caches Domain Name System (DNS)	*Disable
	names.	
Messenger	Sends and receives messages transmitted by	Disable
	administrators or by the Alerter service.	
Print Spooler	Loads files to memory for later printing.	Disable
Remote Registry	Allows remote registry manipulation.	Disable
Service		
RunAs Service	Enables starting processes under alternate credentials	Disable
Server	Provides RPC support and file, print, and named pipe	Disable
	sharing.	
System Event	Notifies COM+ Event System subscribers of these	Disable
Notification	events.	
TCP/IP Net	Enables support for Net BIOS over TCP/IP (Nest)	Disable
BIOS Helper	service and Net BIOS name resolution.	
Service		
Telephony	Local computer and, through the LAN, on servers that	Disable
	are also running the service.	
Workstation	Provides network connections and communications.	Disable

\*Disable if DNS Name resolution is not needed

#### Netbios/SMB

To disable direct host (445 using SMB) go to Computer Management  $\rightarrow$  System Tools  $\rightarrow$  Device Management  $\rightarrow$  View  $\rightarrow$  Show Hidden Devices  $\rightarrow$  Non Plug and Play Drivers Go to NetBios over TCP/IP right click and disable. This will disable the direct host listener on port 445/tcp. (Windows 2000 uses 445 called direct host to do SMB without having to use netbios. IT uses port 445 instead of port 139 for communication.)

The second state of the	en kanstennigaderej	니하기 [바라 대한 비미 대한 기
A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	2 1 12 1 22	
<pre>versities.com/ v</pre>	<pre>     Provide the set of the</pre>	
📲 के स्वी 🔛 🎥 🕵 📲 👘 के स्वी 🖓	- 1915 💥 spredes - Juones e Ku	See and

To disable Netbios over TCP/IP, right click on my network places and go to properties. Right click properties on local area connection. Uncheck Client for Microsoft Networks and File and Print Sharing for Microsoft Networks as shown in figure and click ok. This will disable Netbios and will disable access to the web server using file sharing.

ton al Area Connection Properties 🔹 👔 🗶				
5 mart				
Connect using:				
🗐 Nord Tarlie Ethenia 100 - Midao 16(E paratiko al				
Cenigure				
Componently checked are used by this connections				
III 🥃 Steer fan Minnen (ESE wit ver III 🚚 Fle wit Fricter Stearing to Minner ('Netvenke Iv 資 Stear et Porto on (TCP/ P)				
nsta L. Uninstal Properties				
Description				
All two years to an index to enclassic reaction sectors of Manus of instructions.				
Show con in faskbar when connected				
CK Cavel				

You can also disable netbios over TCP/IP by going to Local Area Connection Properties and then go to TCP/IP and then advanced. Got to the wins tab and select disable Netbios over TCP/IP as shown in figure

Advanced TCP/IP Settings		11 ×	]
P Soltings DNS WINS Options			
WINS addresses, in order of use:			5,50
		î Ş	
Add . Esit	Femove		
i LMHDETS, optup ivieriauted, ili auplievito all'u TCP/IP is enabled		which	
Enable LMHOSTE Isokus	Import LMH	DSTS.	
<ul> <li>Enable NetFIOS Ever TEPVIP</li> <li>Divable NetBIDE over TCP/ F</li> </ul>			
Use NetBICE setting from the DHCP cerver			
	CK	Cancel	

#### **Event Logs**

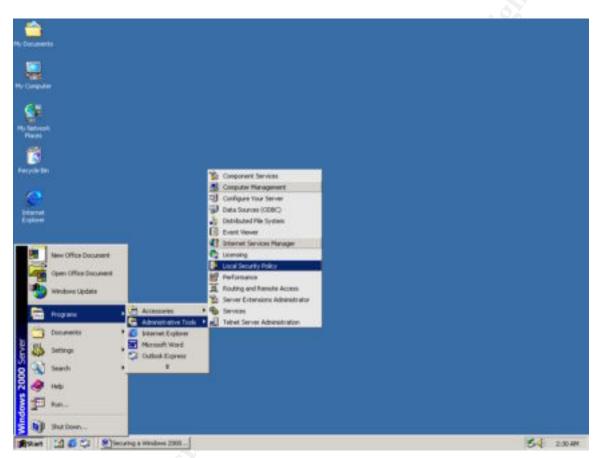
The event logs by default only log 512KB of events before they start to over write. I recommend that you make the event logs size at least 10MBif not 20MB. I would also recommend that you change the overwrite setting to 30 days. This will allow you to look at the logs up to a month back. To change this go to Computer Management, then event viewer. Right Click on each of the logs and set the size. You may also want to secure the event logs by changing permissions on the c:\winnt\system32\config\logname.evt. I recommend setting the access to administrators and local system to Full control and deny everyone else access. You can also change the location of the log files by changing the following registry keys.

- Applicaton Log HKEY LOCAL MACHINE \SYSTEM\CurrentControlSet\Services\Eventlog\Application
- System Log HKEY LOCAL MACHINE \SYSTEM\CurrentControlSet\Services\Eventlog\System

• Security log HKEY LOCAL MACHINE \SYSTEM\CurrentControlSet\Services\Eventlog\Security

### Audit and Policy Settings

Go to start  $\rightarrow$  program files  $\rightarrow$  Administrative tools  $\rightarrow$  Local security policy



Go to password policy and set the following to your desired setting. I recommend enabling Passwords must meet complexity requirements. Below are the default setting and what I recommend.

Policy	Default Setting	Recommended setting
Enforce password history	0 passwords remembered	6 passwords remembered
Maximum password age	42 days	30 or 42 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	10 or more characters
Passwords must meet	Disabled	Enabled
complexity requirements		
Store passwords using	Disable	Disabled
reversible encryption for all		
users in the domain		

■Examily Settings 						
The     Total       Sociality Sectings     Chick to pessivore fibro y       Construction     Chick to pessive to perform	Louis Solving Cloass-Acids remember of Minkey Cloavs Line Lan Chapter Reciec	E coll-c Sulla y O pecsivo iki erreni Collega O ceva O deva O deva Disali ec Disali ec				

Then go to account lockout policy. By default accounts will not lock out after bad logon attempts. This is a dangerous setting as hackers could keep banging away with cracking utilities until they crack the accounts. The lock out setting can help prevent that and make them work harder.

Policy	Default Setting	Recommended Setting
Account Lockout Duration	Not defined	30 minutes
Account Lockout Threshold	Account will not lock out	5 invalid logon attempts
Reset account lockout	Not defined	30 minutes
counter after		

🛃 Local Security Settings			
lenar gea i de ⇒	S 🖬 🖳 🐔		
Tree Security Sectings Control Folder Control Folder Contr	Totuy - 4 Count indecut du at on Service at la total est Service at la total est Second account indicut countres arts	Doninutes Cominutes - ray allo any troppo Cominutes	El coll-le Sultà y No: cettrec Harva franca ro No: cettrec
💁 🛛 🖉 Sour ya Masaz	2000. 🛛 🕄 Local Security Settings 🖉 – 6. 🔊	No.sp.d	

Then go to local policies  $\rightarrow$  Audit policy. I recommend auditing on everything except Audit systems events and audit process tracking. If you audit these events you security log can fill with events that are non-important. Auditing these events will give you enough information of people trying to break in. You can now track when security policies are changed and when people log on and off. This will leave you a very good audit trail latter on.

Policy	Default Setting	Recommended Setting
--------	-----------------	---------------------

Audit account logon events	No auditing	Audit Success and Failure
Audit account management	No auditing	Audit Success and Failure
Audit directory service	No auditing	Audit Success and Failure
access		
Audit logon events	No auditing	Audit Success and Failure
Audit object access	No auditing	Audit Failure
Audit policy change	No auditing	Audit Success and Failure
Audit privilege use	No auditing	Audit Success and Failure
Audit process tracking	No auditing	No auditing
Audit system events	No auditing	No auditing

nan Ana 🗍 💠 🕂	🔽 🔟 📉 🛃 💆			
	Way A	Loca SAU iy	Ellipsie Edung	
Scountly Sectings	🖁 Audit account logon events	Success, Fallure	No suo drig	
	🖞 Addit aboard in Lincopenier (t	Success, Fullery	No coolaite	
	🖁 Audit oli ector viser-ke access	Success, Fallure	No suo drig	
- 🔁 Koowink Lockal : 🛛 🛃	🖞 Adulk Kupo I wa Ka	Success, Fuiltre	No coolaite	
🙆 Local Policies 🛛 🔋 🚦	Audit cojectecces	Felu e	No suo drig	
透 Audit Policy 🔰 🚶	🖁 4a kiy kiwala ng	No. 1996 March 10	N 10 0	
E 🏩 ka Pijhts Arny 🛢	S Audit pi vi ege use	Success, Fall, w	No euclarg	
🛓 - 🔝 – Anne itali Cherra 🛛 🚺	A Marines a larg	these Many	N 10 0	
📄 Austin Gey Antimes 👔 🛃 19 Met inty Austin Strategy	Audit system evenus	No autiting	No suo drig	

#### Users Rights Assignments

Then go to Users Rights Assignment as show in figure 2-B. I have listed below what rights to change. By default everyone can log on locally. This is dangerous as anyone could log on. Even Guest if it got enabled accidentally. I recommend that all users get removed except Webmasters and Administrative Users that need console access. The Access this computer from the network also has the everyone group in it by default. I recommend removing all user accounts except the anonymous user. If you have IIS control the anonymous users password, than you need to allow Access this Computer from the Network. If you don't allow IIS to control the password than you need to allow the anonymous user to log on Locally. I recommend having IIS control the password.

Policy	Default Setting	Recommend Setting
Access this Computer from the	Everyone and all the	Remove all users accounts
network	default install Groups	and groups except the
Q		anonymous IIS user
Bypass transverse Checking	Everyone	Remove all user accounts
Log on locally	Everyone	Remove all accounts except
		User accounts that need to
		log on to the web server.
Shut down the system	Power Users, Backup	Remove all groups except
	Operators,	administrators.
	Administrators	

Figure	2-B
1 15410	

	A		The second
	Recent contractor in the second se	0:003.00	
	Star - House to your	-	
	Mar a blank and		
A meniny	Second Subtracts	Sector Concernance Statutes	Section Council Section 2.1
	Dependent in the large		Skolycholia od Nekor Cabili
	E Charge the current one	<ul> <li>Security and the second se second second sec</li></ul>	Reportion substances
	The man appropriate	stor trev c	stor treat 4
	Shumbert a w		
	Mar da a constante de las		
	Maria a general de la companya de la	Selve and the	Selve an area
	🔟 te velasi büslar tela i vedir ete a		
	🚊 juarty bijos er svervos		
	Real and the second sec		
	Sharring trade is a scalated fr	1.	
	🔊 - an shi ana bar an a sheet	Advantation of the second s	Selve an ex-
	💹 Our en al d'Antonie de La California de California		
	📇 Dro esse euxeau	Advin (atox a	Advir (atox a
	🚊 Dro Helskovské naj se prov	Novin care of a	Novin care of a
	🕞 ne izadu birac navos citars	stor track	stor track
	All the process of the second		
	20 million and a second sec	TREADED FOR THE REPORT OF	161 (164) 1 ··· 1 ··
	🔊 e e e service		
	🖄 kala kal-	Additional Activity	OR COTA ALL ALL
	🚊 ji arogo skili vy oraciosu istiog	Advir (atox a	Advir (atox a
	🚍 je s for even av soner ar ac	when carecold	when care a
	No di sen de la sec	A methodologic contra	A matter shall be
	🗶 daram mir me	Man and a	Man and a
	Managaran ang sa	and the first photoe in the	· • • • • • • • • • • • • • •
	💭 varan fina ang ili pate ka	top up Copress suAching pote a	Des Las Coerces (
	Eps sor in other	Netwin company	Street Los albectas
	Eterritorize cremo grande has		
	Shelman and public to an algorithm.	She was	Selection of the select

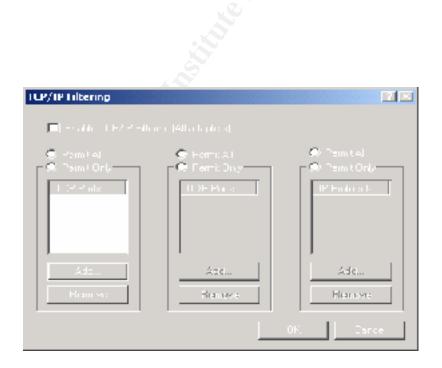
Security Options Go to start  $\rightarrow$  program files  $\rightarrow$  Administrative tools  $\rightarrow$  Local security policy. Then go to Security options. Below I have listed the default setting and what the setting should be set to.

Policy	Default Setting	Recommended Setting
Additional restrictions for	None. Rely on Default	Do not allow enumeration
anonymous connections	permissions	of SAM accounts and
		shares
Do not display last user name	Disabled	Enabled
in logon screen		
LAN Manager Authentication	Send LM & NTLM	Send NTLMv2 response
Level	responses	only/refuse LM & NTLM
Message text for users	None	You choice EX (This
attempting to log on		system is subject to usage
		logging and monitoring.
		Authorized Access only)
Message tile for users	None	Warning!!!!!
attempting to log on		
Prevent System maintence of	Disabled	Enabled

computer account password		
Recovery Console: Allows automatic Administrative logon	Disabled	Enabled
Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled
Restrict Floppy Access to locally logged-on user only	Disabled	Enabled

#### **Packet Filtering**

In Windows 2000 there are ways to control which ports users can access. You can right click on My Network Places  $\rightarrow$  Go to Properties  $\rightarrow$ Right click on Local Area Connection  $\rightarrow$ Go to Properties  $\rightarrow$  Highlight TCP/IP Protocol and chick on properties  $\rightarrow$  Go to advanced settings and double click on TCP/IP Filtering. This will block all ports except what you have defined in the Permit only List. I recommend only Allowing Port 80 (HTTP), and if need 443 (SSL) and FTP (21). This will stop people from probing other ports.



#### **Routing and Remote Access**

You can also use the routing and remote access service to control packet filtering. I don't like to use this and I don't recommend it. You need to have the workstation service enabled to use it. It is also a service so if someone was able to crash the service or stop the service the benefits of Using Routing and Remote Access are defeated. I recommend using IPSEC policies instead. It is also another service that would need to be running.

#### **IPSEC Polices**

IPSEC is the framework and a standard for IP Security. IPSEC provides an authenticated, secure channel with the following protocols and standards.

- Authentication using the Internet Key Exchange Protocol (IKE, RFC 2409)
- Integrity Protection using the Authentication Header (AH, RFC 2402)
- Encryption Using the Encapsulating Security Payload (ESP, RFC 2406)

Before two hosts can establish a secure connection they must authenticate one another. They negotiate a set of encryption parameters called a security association (SA). Windows 2000 uses IKE (Internet Key Exchange) to establish these parameters. IPSEC is a good way to secure the server, as the packet will be dropped even before it makes it up the OSI model, which makes it very secure. To set up an IPSEC policy you need to follow the steps below

- 1. Go to Start → Program Files → Administrative Tools → Local Security Policy.
- 2. Click on the IP Security Section on Local machine

🐺 Local Security Settings				
(m = 200   da →   🔟 🕅 🚮	喝 👩 🖆 📩			
Trav	N 11 - 4	Company	Buyers	
Sciency systems	👫 Dent Clescord On 🗤	Communicate normally (unsul-	to .	
🔄 🍱 Alixan Fukuta	🎽 anna a sa (Sagi what i u		to .	
🔄 📫	🖬 Server (Request Seconds)	For all D Gall and easy rect	E.	
💷 🤰 Malk Ary Diana				
🛃 D'Strady Viets in Lood Paciely				
koorne e - franz 2001 👔 Enrol Serunty S	setting.			84

3. Remove the three default IP Security Polices.

🐺 Local Security Settings				
l Anna - Anna 🛛 🔶 🕂 🔽 🔟	[명] 🛃 🖱 🔠 👘			
Troe	Name A	Diseriji, o	Du sy ésá, na	
🔁 Security Security				
국-@ Account Policies 국-@ Local Policies				
The second rectors       The second rectors       The second rectors	-			
uria - «ñ Joas 2001 - 🔂 Local Secu				54

4. Right Click on IP Security Policies on the Local machine and select manage IP filter lists and filter actions.

Manage IP filter lists and Manage IP Filer Lyly Mo		
This cicleg allows you to make maintain the IP Filter Lists that tescribe your belowsk the available IP Litter Lists are shared by eLIP Siecurity Publics.		
F Filler Lole:	·	
Nome	Description	
ALLIZE Fahrs	Matches al II MP taskels betw	
All F Traffic	t⁄atohas al IP papkeis from trip	
Ad- I -	n Lemove	
	Linxe Cancel Aprily	

5. Create an IP Security Policy called allowed web server traffic and uncheck use add wizard.

28 IP Filter Li	st			? x
Ar Ar Ar	r IP filter livt iv compov diesses and protocols	ed of multicle filters. In . : can be combined into	hiv wayn olt pre sobri one Fifter	ets, IP
Name:				
4 lowe Web	Ecryc: Traific			
Description:				4cd
Traffic that i	is allowed to the web :	carve.	<u>م</u>	Edit . Fenove
L hers				os Apd Wizard
Minored	lever prior	L miono	Source Lod	Designation
٩				▶ Cared
				111.

6. Click on add and select source address any IP address, destination IP address my IP address.

er Propertie				17
Ary P Au		on		
	1 =::-			
Describer	and max			
🔲 Mingredji	Also match packe	is with the exac	t opposite sicur	:earc
zeo:inalio	r addreskek			

 Go to protocol and Select TCP as the protocol type. Select from any IP port to local port 80. Repeat Steps 6 and 7 for FTP (TCP 21) and HTTPS (443).

Filter Properties		
Activeshing Potocol Description		
E clest a protocol groe		
- Set the IP publico polit		Y
🗭 Linn ary prit		
C Fun tris put.		
C To any tor		
C To the post		
LIR. Dancel Ap	r ly	

8. It should look like the example below. Click on close

lame:				
Alowo Web Server	Tiailio			
)escription				Add
Taficih≘t salo∾e	d to the web server		<u></u>	E ::
			<u>_</u>	Beinzve
les.				🔲 Uee Add Wisaid
Devination Port	Source DKS Name	Source Address	Source Mark	Destination DNE
80	<any address="" ip=""></any>	(Any IP Address)	0.0.2.0	(My IP Address)
21	<ul> <li>kány IP Adulevsty</li> </ul>	<ul> <li>kány IP Aduevso</li> </ul>	0.0.2.0	<pre>kMyIP.Adurevs)</pre>
24(1	kàn, L'Admeso	≺Anyi 'Adhess)		< My II "Address"

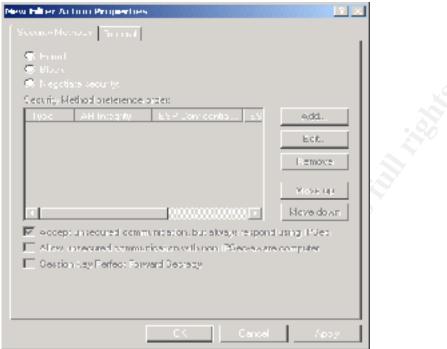
9. Click on add and Give this filter a name of block all other traffic

98 II' Hiter List			? ×
An IP liter Ist is compored addresses and protocol	vad of molfiele filters. In . a can be combined info	liv way nut pe subre one iFitter	la, IP
Name:			
Block all other traific			
Description:		_	Acd
		<u> </u>	Edt
		<u> </u>	Fenove
L hers		E Los	e Apd Wizard
Minored Resorption	l mioto	Source Lod	Desmator
	<b>1</b>		
•			
		DA	Carool

10. Go to manage filter actions, uncheck use add wizard and click on add.

Manage IP filter lists and filter	r actions		
Manago IP Filter Liele Marraya I	File Actions		
This cicleg allows you to make maintain the filter posions that tesserible the vecurity of your network the available filter posions are shared by all if it security.			
policies.	· ·		
Filter Actions			
Morrie	Description	T I I	
Demo	Permit unsecured III, packets to		
Recuest Security (Optional) Henure Security	Accepts Unsequed Communicati . Accepts Unsequed Communicati		
nt I the	Lienove 📃 ise Adr Wizard		
	Hear Dancel Apply		

11. You need to create a block security policy. On the general tab give this filter name block. Then go to the security methods and select block. Then select ok. A permit policy is already defined.



- 12. Right click on IP Security Policies on local machine and select create IP Security Policy.
- 13. A policy Wizard will come up. Select Next.
- 14. For an IP Security Policy Name Give It Secure Web Server. Select Next
- 15. Uncheck the Activate the default response rule and click next than finish.
- 16. A properties screen will come up. Uncheck add wizard and click on add

Sections Web Server Pro-	perfiles		
L des   General	curso c	Rectifices computer IN	ulicyy
L i schut, Da ev	e lot communicating same d	her computers	_
PF ka Lat	File Actor	Authorn cation To	
🗖 :Eynamet	Detail, Revier ve	Ambeloz Ho	
-			
	. I		
E	di Benzee	📄 🗖 Use Acd Wizs L	
	U	and Apple	

17. Go to the IP Filter list and Select Allows Web Server Traffic, then go to filter action and select permit. Then click on add. Click on add again and select block all other traffic. Then go to filter action and select block. Then select OK.

Secure Web Server Pro	operties es fui comunicating wit	· other computers	<u>1×</u>
F Security Roles. F Fille Lyt ☑ Illock et other hal ☑ Allowy Web Serve	Filte Aution	Authant cation. Keiberos Keiberos Keiberos	. T. Nr Nu Nc
		-	
-h4	Ldt Lenove	👘 🔲 Ise Ada V	X zer
	11-2-	Cancel	Apyly

18. Then select close. Then Right Click on the Secure Web Server policy and Click Assign.

versilee (	New York Street	제 # # B - 2 길	<u> </u>		<u>1×</u> _
	60 60	Here 2	- 444	Eller Coarte I	T
	491.4.4 🔯 Securationes	A states		16	
	1980 SAME 🖓 A LA CALA		a <u>r</u> )		
	<ul> <li>A state of the sta</li></ul>	- 14 - 14 - 14 - 14 - 14 - 14 - 14 - 14	who is		
	🗣 4 👼 I Den 1- 'n ooren 100 'k	crire De	141F		
	16 s i	-	eren in the second s		
	1994 T	74	neemer		
	\$40.00 B				
	ិទ្ធិវិទាទ កិត្តកំពោះ		F		
	Second				
	4				
	492.5				
	(in the second s				
	lingstare Agenca				
	See.				
	<b>6</b>				
	1999 a.				
	1987.x1				
	Salars Salar				
	Sec.				
	2011 - C				
	Ware as a support of the state of	N1			
	STRATICK AND LEAST AND		ana 1969-194		
	Sufficiency and Antonia Successive Company		r.a .xx2:xx		
	🖓 Vinco-s Inde a 👘 Sintain, apaile and		ec 2499		
	Repairing the second		TA WARNER		
		•			
	Mark and a second				
	A∰arta sa ta anan Agartata ha barta sa ta				

You now have a secure web server. Remember if you want to browse the web, ftp or do DNS lookups from the web server you need to make sure that you create a policy to allow that traffic out. By using an IP Sec Policy you also prevent some one from putting a listener on the web server and binding to a high port. You will still be vulnerable if the hacker binds it to port 80.

#### **User Accounts**

You should always rename the Administrator account. All hackers know that Administrator is the default admin account. I recommend renaming this account. Then create another account called administrator with no rights. This account is called the honey-pot or jail admin account. I also recommend creating user accounts for all administrative users and give them only the rights that they need. You could then come up with a very complex administrative password and lock it away until you need it. This will also let you create an audit trail of the administrative users. I also recommend that you create a new IIS anonymous user account. Again, all hackers know that the IIS anonymous account is IUSR\_machine name. Leave the old anonymous account on the server but disable it. This will create a jail anonymous account. This is good practice and will go a long way in securing your web server.

#### **Moving Dangerous File**

Windows 2000 has some potentially dangerous files that are located in the system path. Examples of these files are tftp.exe, cmd.exe, etc. These files should be moved to a different folder with auditing enabled on the folder and with permissions for only administrators. I recommend creating a secure folder.

Here is a partial list of the dangerous files.

- At.exe
- Calcs.exe
- Cmd.exe
- Csript.exe
- ftp.exe
- tftp.exe
- regedit.exe
- regedit32.exe
- runas.exe
- nbtstat.exe
- telnet.exe
- net.exe

#### Securing IIS

The steps below will go threw the steps needed to secure IIS. A create document that will list some to most of these steps is at

http://www.microsoft.com/technet/security/iis5chk.asp. This is a very good security checklist from Microsoft's web site.

#### Installation

The default install off IIS installs a bunch of services and samples applications. I recommend running IIS setup again and removing what you do not need. Go to start  $\rightarrow$  setting  $\rightarrow$  control panel  $\rightarrow$  add/remove programs. Double click on add remove programs and go to add /remove windows components. Select Internet Information Services and click on details. I recommend removing the following,

- Documentation
- Internet Server Manager HTML (Could allow a hacker easy access to hack the web site)
- FrontPage server ext.
- SMTP service.

Internet Information Services (IIS)	×
Fo add or remove a component, dick the check box. A chaded box of the component will be installed. To see what sine upped in a comp	
Subcomponents of Internet Information Stervices (19)	
🗹 🎲 Common Files	10 MB 💻
🗔 🙈 The mentalism	0.5 MI
🗹 💭 Fie Transfei Protocol (FTP) Server	01 MB
🗹 🔶 i mit fage zit it Server Extensions	4 2 MB
🗹 📸 Internet Information Services Snap-In	1 3 MB
🗹 🚳 ntemet Services Menager (, 11 M. )	0.7 MB
🖂 💻 NNTE Service	4 5 MB 💌
Description: Publiching, site content, and wisb and PTP cervariad notuding ABF documentation and samples.	mnølfalion lodice,
Tota disk space repured: D.9 MB	E.ctzie
Space everalle on Lisk. 3545.0 MB	6- 9-30 / V 13
СК	Cared

#### File security

Below is a table that outlines the file security needed on the web pages and scripts. Remember that some asp pages might need read and write.

File Type	Access Control Lists
CGI (exe dll cmd pl)	Administrators and System (Full Control)
	System (Full Control)
	Everyone (Read)
Script files (asp)	Administrators and System (Full Control)
	System (Full Control)
	Everyone (Read)
Static files (html, htm, gif, jpeg)	Administrators and System (Full Control)
	System (Full Control)
	Everyone (Read)

A better option would be to creating directories for the different files types and but the ACLs on the directory. EX (d:\inetpub\wwwroot\script, d:\inetpub\wwwroot\static)

#### Log Files

Log files are written to %systemroot%system32Logfiles. I like to move these files to a different drive. This keeps them off the operating system drive and prevents the hacker from easily removing or modifying the log files. Do change the directory open the Internet Information Services and got to the name of your web server and click on properties.

WWW Service Master Properties for (tec)	
Locuments         Directory Ecourity         HTTP Headers         Dustom Errors         Service           Wob Bits         Operatory         Perfuminance         IEAPI Filtery         Home Directory	
Wet Site Identified or Description: IP Address: (All Uncesigned) Advenced	100
Contactors Contactors Culture Contactors Culture Cultu	
Entreshon imenut seconds E I I I' Keepsèlixes i nehlet Enable Lug_r g	
Active log forma:	
OK. Conto Apply Holp	

Go to the active log format and click on properties.

Extended Logging Properties	
General Properties Elstonoco Proportios	
New Log Time Period I Hourly Daly Woodly Normality Uninted fills size When the vice reaches.	
Use opa time for lie naming and rollover op He directory: Browver,	
og tils namer – WOB24D2Asxyummdic log	
DA Dance Appy Help	

Change the log file directory. You can enable additional logging by going to the extended properties tab. I recommend turning on bytes send and received.

Extended Logging Pro			×
r strenderd opging	-		
	Danco	4сру	Holp

#### Sample Applications

IIS comes default with some sample applications and documentation installed. These sample applications and documentation have been known to have bugs and reveal information. I recommend removing the sample applications. Below are the paths to the sample applications. I suggest deleting these directories.

- IIS Samples- C:\inetpub\iissamples
- IIS documentation- c:\winnt\help\iishelp
- Data Access c:\program files\common files\system\msadc
- Admin Scripts c:\inetpub\admin scripts.

#### **Default Web Site**

I recommend removing the default web site and creating a new web site. The default web site has been known to have a bunch off vulnerabilities in it. It is better to create a new web site.

#### **Remove the IISADMPWD Virtual Directory**

The IISADMPWD allows users to change passwords. This is dangerous as it could allow someone to try and change your admin password. I recommend removing this virtual directory.

#### Script mappings

IIS by default has a bunch of script mappings enable. I recommend removing the script mapping you do not need. To remove these script mappings

- 1. Right-Click the the root of the web site and choose properties
- 2. Click the home directory tab
- 3. Click Configuration
- 4. Remove the mappings that you do not want.

Bellow is a list of the script mappings.

If you don not need this	Then remove this
Web password reset	.htr
Internet Database connector	.idc
Internet printing	.printer
Index Server	.ida .idq .htw
Server Side Includes	.stm, .shtm, shtml
Certificate Request	.cer
Active Server Pages	.asp .asa

#### **Parent Paths**

The Parent Paths option allows you to use ".." in calls to functions such as *MapPath*. By default, this option is enabled, and you should disable it. Follow this procedure to disable the option:

1. Right-click the root of the web site, and choose properties

- 2. Click the Home Directory tab.
- 3. Click Configuration.
- 4. Click the App Options tab.
- 5. Uncheck the Enable Parent Paths check box.

#### Web Server Root Directory

By default the web server's root directory is c:\inetpub\wwwroot. I recommend that you move this path to a different volume. This would prevent someone from jumping off this directory to get to the root of the OS.

#### **FTP Service**

If you use the FTP service to update your website you might want to use IP address restrictions on the ftp site. To get to IP address restrictions go to the FTP site and right click and go to properties. Then go to directory security. Put only the addresses needed to update the web site.

#### **Maintaining Security**

To maintain security on the web site you need to setup good policies and procedures. Some examples of policies and procedures are backup polices, polices when the web site gets hacked. If you put polices in place early, you can avoid disaster latter.

#### **Security Scan**

Run a third party tool like IIS Internet Scanner to get a look at the security from the Internet. This would allow you to test your web server for over 800 vulnerabilities and to fix any holes that are left open. This scan should be run yearly if not quarterly to check against any new security developments.

#### **Intrusion Detection**

Consider getting an intrusion detection system. This system could provide you with an early warning alarm of someone trying to hack you. You can get two types of IDS systems, host based and network based. You might want to consider both for extra protection. Some IDS systems even work with firewalls changing firewall rules to block access.

#### **Security Mailing Lists**

Consider subscribing to security related mailing lists to keep on top of the latest developments. Here is are some links to mailing lists

- <u>www.ntbugtraq.com</u>
- <u>www.securityfocus.com</u>
- <u>www.microsoft.com/security</u>
- <u>http://www.securityfocus.com</u>

#### Web Server Placement

If you are running a public web site you should consider putting it in a DMZ. A DMZ is a packet screened and filtered subnet. When you put your web server on the DMZ you can

limit the services coming in to the DMZ to what is needed to access the web site. You can also limit what goes out from the DMZ. This will prevent a hacker from using the web server to jump into the production network. It will also limit were a hacker can go and prevent him from using you server to hack other Internet web servers.

#### **References:**

- 1. Securing Windows NT/2000 Servers for the Internet by Stefan Norberg, O'Reilly ISBN 1-56592-768-0
- 2. Microsoft TechNet Security Web Site, http://www.microsoft.com/technet/security/default.asp
- Hacking Exposed 2<sup>nd</sup> Edition by Joel Scambray, Stuart McClure, George Kurtz, Osborne ISBN 0-07-212748-1
- 4. Securing Internet Information Server 5.0 by Jason Fossen, SANS Institute

Securing Windows 2000 © SANS Institute 2000 - 2002