

## Re: How to Maintain an IIS Server?

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.inetserver.iis.security/2002-11/5643.html>

---

**From:** Karl Levinson [x y] mvp ([levinson\\_k@excite.com](mailto:levinson_k@excite.com))

**Date:** 11/06/02

From: "Karl Levinson [x y] mvp" <[levinson\\_k@excite.com](mailto:levinson_k@excite.com)>

Date: Wed, 6 Nov 2002 14:34:40 -0500

You can run HFNETCHK with a switch to run it in verbose mode. This will give you knowledge base article numbers to look up at [www.microsoft.com/support](http://www.microsoft.com/support) to tell you more information. Some of those are known issues and will always alert for you. Other alarms could indicate that a certain .DLL or other file is older or newer than it should be.

For more information, check out those newsgroups mentioned below:

Microsoft.public.security.hfnetchk  
[for Microsoft HFNETCHK tool]

Microsoft.public.security.baseline\_analyzer  
[for MS MBSA Baseline Security Analyzer ]

"Stephen Pak" <[asiats@hotmail.com](mailto:asiats@hotmail.com)> wrote in message  
news:OTBh0kchCHA.1960@tkmsftngp11...

> Thank you to Ken and Karl.

>

> Your infos are very useful!

>

> I have another question regarding MBSA or HFNETCHK.

>

> When I run those two programs, sometimes it reports that I did not apply  
> certain patches (e.g. MS02-008, MS02-022, MS02-053). However, I do  
believe

> I apply the patches. Even if I re-apply those "missing" patches, the I  
run

> the MBSA or NFNETCHK again.....It still says that the patches are  
missing...

>

> Do you happen to know why? If it is not the right newsgroup, could you  
> please tell me where should I post the above question?

>

> Thank you again!

>

> Stephen

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

>  
>  
> "Karl Levinson [x y] mvp" <[levinson\\_k@excite.com](mailto:levinson_k@excite.com)> wrote in message  
> news:OQjZRhUhCHA.1688@tkmsftngp09...  
>>  
>> "Stephen Pak" <[asiats@hotmail.com](mailto:asiats@hotmail.com)> wrote in message  
>> news:eI2#BvThCHA.2700@tkmsftngp09...  
>>> I looked at the Microsoft Security Website.  
>>>  
>>> I understand that there are a lot of information available there.  
>>>  
>>> Actually, I am particular interested in how to prevent worms (e.g.  
>>> Nimda/Code Red/anything else). What anti-virus program is the best  
for  
>> IIS  
>>> server running on a Windows 2000 server.  
>>  
>> Depends. I like Norton. Get a firewall or two as well, and close all  
> ports  
>> incoming and outgoing except for those that are needed.  
>>  
>>> Also, what is the best procedures to restore the IIS server once it is  
>>> hacked by someone. Or, I should ask what is the best way to backup  
the  
>>> server. Any software or product is good for backup/restore  
> (automatically  
>>> backup) the entire site or even the computer.  
>>  
>> You got it... once your web server has been hacked, you should consider  
>> formatting and reinstalling Windows and all programs, then restoring  
data  
>> from backups.  
>>  
>> Since you asked, more info is below:  
>>  
>> =====  
>>  
>> How can I harden my computer or server to secure it from hackers?  
>>  
>> A: [Note that if you have already been hacked, this section will not  
help  
>> you re-secure your computer. In this case, you should first read the  
>> section in this FAQ entitled "How can I re-secure my computer or server  
>> after being hacked?"]  
>>  
>> Here is the short answer:  
>>  
>> 1) Do not put the computer onto the network or the Internet until after  
> the  
>> computer has been hardened using the instructions below [or at least not  
>> before a firewall and antivirus have been installed].

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

> > 2) Use firewall software and hardware and antivirus software that is  
> > configured to download updates every day;  
> > 3) Follow the instructions for hardening Windows and IIS at  
> > [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) ;  
> > 4) Install all service packs and security fixes from Microsoft and  
> > otherwise for all Microsoft software on your computer [Windows, IIS,  
> > Office,  
> > Internet Explorer, Windows Media Player, etc.] from  
> > [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) ;  
> > 5) [Ongoing] Download MBSA from [www.microsoft.com/download](http://www.microsoft.com/download) and run it  
now  
> > and also at regular intervals to look for vulnerabilities in your  
> > settings,  
> > new patches that are missing, etc. Also, check your antivirus to  
confirm  
> > that the last successful update was less than 14 days ago.  
> >  
> > These steps will make your computer fairly secure, but may still leave  
> > some  
> > holes. Keep reading below for additional information you should be  
aware  
> > of:  
> >  
> > A successful hacker, virus or worm intrusion into one of your computers  
> > can  
> > drain your free disk space, slow down your Internet connection,  
compromise  
> > your credit card numbers, damage your personal documents, allow  
intruders  
> > to  
> > access other machines on your network that DO contain important files,  
> > and/or leave you legally liable for other government or business  
computers  
> > on the Internet that are hacked by an intruder using your computer.  
This  
> > is  
> > why you should consider securing ALL the computer systems in your home  
or  
> > network, even if you think there is nothing important on the computer or  
> > it  
> > is "just a test computer."  
> >  
> > All Windows users should seriously consider all of the procedures below  
to  
> > help prevent intrusions on their computers:  
> >  
> > 1) Do not put the computer onto the network or the Internet until after  
> > the  
> > computer has been hardened using the instructions below. [Un-secured  
> > computers can be hacked in just 15 minutes or less after being put onto  
> > the

microsoft.public.inetsrv.iis.security: Re: How to Maintain an IIS Server?

> > *Internet.] Depending on your environment, it may be acceptable to put  
> your  
> > computer on the Internet after installing a firewall and antivirus  
> software  
> > with the latest updates.  
> >  
> > 2) Seriously consider enabling or installing firewall software and/or  
> > firewall hardware. There are a number of free firewalls available,  
> > including the ICF feature that comes with Windows XP [unless XP is  
joined  
> to  
> > a Windows domain], and/or other third-party firewalls available on the  
> > Internet.  
> >  
> > For more information on how and where to locate free and not-free  
firewall  
> > software and hardware, see the section in this FAQ entitled "Which  
> > firewall  
> > should I choose? Which firewall is the best?"  
> >  
> > 3) Seriously consider installing an antivirus program and configure it  
to  
> > automatically download updates daily.  
> >  
> > For more information on where and how to locate and use free and  
not-free  
> > antivirus software, see the section in this FAQ entitled "Which  
antivirus  
> > should I choose? Which antivirus is the best?"  
> >  
> > 4) Follow the instructions for hardening Windows 2000 and also IIS [if  
> > IIS  
> > is installed] at [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security)  
> >  
> > [Note that for Windows 2000 / NT, hardening IIS should include  
installing  
> > IISlockdown including URLScan. For computers with FTP service  
installed,  
> > it  
> > should include removing the Posix subsystem and removing write  
permission  
> > from the anonymous user account, among other things. Information on  
> > removing the Posix subsystem is available at:  
> > [www.microsoft.com/technet/security/tools/chklist/CheckList.htm#4](http://www.microsoft.com/technet/security/tools/chklist/CheckList.htm#4)  
> > [www.labmice.net/articles/securingwin2000.htm](http://www.labmice.net/articles/securingwin2000.htm)  
> >  
> > 5) Download and install all the service packs and security patches from  
> > [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) for all the Microsoft and  
non-Microsoft  
> > software installed on your computer, especially Microsoft Windows,  
Office,*

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

> > *Internet Explorer, Outlook Express, Windows Media Player and IIS [if IIS  
> is  
> installed].*  
> >  
> > *Note that Windows 2000, XP, .NET and NT users should also download  
patches  
> > for Indexing Services a.k.a. Index Server. Do not assume that Index  
> Server  
> > patches are included with any IIS comprehensive service pack rollup you  
> may  
> > already have installed, because they are not.*  
> >  
> > *[If you want a shortcut to do this faster, you could try this:  
> > \* Download and install the latest Windows service pack from  
> > [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security);  
> > \* Reboot and visit <http://windowsupdate.microsoft.com> to receive  
> additional  
> > patches;  
> > \* Reboot, download and run MBSA [Microsoft Baseline Security Analyzer]  
or  
> > HFNETCHK from [www.microsoft.com/download](http://www.microsoft.com/download) to discover other missing  
> patches;  
> > \* Manually download from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) and install  
> any  
> > patches that were found to be missing, as well as patches for any server  
> > products that may not be included in Windows Update and MBSA/HFNETCHK,  
> such  
> > as possibly SQL Server, ISA Server, etc.  
> > \* NOTE however that Windows Update, MBSA and HFNETCHK do NOT necessarily  
> > list all Microsoft patches or search all Microsoft products, so you  
could  
> > be  
> > missing some patches if you rely just on these tools.]*  
> >  
> > 6) [ONGOING] Re-run the MBSA tool from [www.microsoft.com/download](http://www.microsoft.com/download) every  
> > 60  
> > days or sooner to look for missing patches, and confirm that your  
> > antivirus  
> > program received an update in the past 10 days or less.  
> >  
> >  
> > *If you want or need even more security [or are particularly paranoid or  
at  
> > risk], you can consider some of the additional steps below. Some of the  
> > tools below may be more security than you need, unless you are running a  
> > server such as IIS web or FTP services.*  
> >  
> > \* Download and install MyNetWatchman or Dshield. These are free  
programs  
> > that work with your firewall software or hardware to automatically  
report

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

> > *hacking attempts to the hacker's ISP. You get to see information about*  
> > *whether that IP address has been used to scan or hack other computers,*  
or  
> > *whether it might be targeting just your computer. You also get to see*  
> > *whether the ISP has responded or taken action against the offending*  
user.  
> > *This is highly recommended. You can get this software at one of the*  
links  
> > *below:*  
> >  
> > *www.mynetwatchman.com*  
> > *www.dshield.org*  
> >  
> > *\* Sign up for the Microsoft security mailing list at*  
> > *www.microsoft.com/technet/security to receive emails with a link to new*  
> > *critical security patches as they are released, and install them ASAP.*  
> >  
> > *\* Use Vision [or Fport] from www.foundstone.com/knowledge or Active*  
Ports  
> > *from www.webattack.com/get/activeports.shtml or pslist / pstoools from*  
> > *www.sysinternals.com to look at the open ports on your computer and the*  
> > *program or executable using that port. Some firewall software such as*  
> > *www.sygate.com will also tell you this information.*  
> >  
> > *You can also use the NETSTAT -A command that comes with Windows to look*  
> > *at*  
> > *open ports; however, this will not identify which program is using the*  
> > *port.*  
> >  
> > *[You may want to run a command such as FPORT >> C:\OPENPORTS.TXT or*  
> > *PSLIST >> C:\OPENPORTS.TXT or NETSTAT -A >> C:\OPENPORTS.TXT*  
> > *This command will create a "baseline" text file named c:\openports.txt*  
> > *that*  
> > *can be compared later with the results of the command to tell you*  
whether  
> > *additional ports are now open, a possible sign of intrusion.]*  
> >  
> > *\* Consider running one or more vulnerability scanners to look for*  
security  
> > *flaws and configuration errors on your computers. Vulnerability*  
scanners  
> > *should be run after you have installed and hardened a new computer or*  
> > *server, and also run at regular intervals to confirm that your computers*  
> > *are*  
> > *still secure. You might also run a port scanner against your computers*  
as  
> > *well to look for open ports.*  
> >  
> > *See the section in this FAQ entitled "How can I scan my computer or*  
> > *firewall*  
> > *to look for open ports or confirm that my machine is secure?" for more*

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

- > > *information.*
- > >
- > > \* *Consider searching for and following additional checklists for hardening*
- > > *Windows 2000 by searching an Internet search engine such as [www.google.com](http://www.google.com)*
- > > *for words such as "harden OR hardening windows-2000" [e.g. [www.google.com/search?q=harden+OR+hardening+windows-2000](http://www.google.com/search?q=harden+OR+hardening+windows-2000) ]. Several such*
- > > *checklists are available at:*
- > >
- > > *<http://nsa1.www.conxion.com/win2k/download.htm> a.k.a. <http://www.nsa.gov>*
- > > *[www.labmice.net/articles/securingwin2000.htm](http://www.labmice.net/articles/securingwin2000.htm)*
- > > *[www.labmice.net/security](http://www.labmice.net/security)*
- > > *[http://csrc.nist.gov/itsec/guidance\\_W2Kpro.html](http://csrc.nist.gov/itsec/guidance_W2Kpro.html)*
- > > *<http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf>*
- > > *<http://rr.sans.org>*
- > >
- > > \* *Uninstall any unnecessary Windows components [e.g. click on Start, Settings, Control Panel, Add/Remove Programs, Add/Remove Windows Components]. Pay particular attention to Indexing Service, Internet Information Services (IIS), Management and Monitoring Tools, Message Queuing*
- > > *Services, Networking Services, Other Networking File and Print Services, Outlook Express, and Windows Media Player. If you are not sure whether something is unnecessary, try searching [www.google.com](http://www.google.com) or posting a question*
- > > *to the appropriate Microsoft security newsgroup.*
- > >
- > > \* *Disable any unnecessary Windows services [e.g. click on Start, Settings, Control Panel, Administrative Tools, Services]. If you are not sure whether something is unnecessary, try searching [www.google.com](http://www.google.com) or posting a question*
- > > *to the appropriate Microsoft security newsgroup.*
- > >
- > > \* *Consider using a Trojan scanner. Antivirus programs generally detect some*
- > > *but not all of the most common Trojans and hacker tools. Some people choose*
- > > *to use a Trojan scanner in addition to antivirus.*
- > >
- > > *For more information on where and how to locate and use free and not-free*
- > > *Trojan scanner software, see the section in this FAQ entitled "Which antivirus should I choose? Which antivirus is the best?"*
- > >
- > > \* *Enable logging. Most logging is disabled by default, and usually this is*

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

> > *not discovered until after an intrusion, when the logs are needed.*  
> >  
> > *Enable logging of your IIS web server, FTP server, etc. For sites with  
a  
> > small number of hits, consider changing logs to rotate monthly instead  
of  
> > daily to allow easier searching of logs.*  
> >  
> > *Enable logging on your Internet router, switch or firewall. [Because  
> these  
> > devices usually do not have much storage space for saving logs, doing  
this  
> > may involve installing free syslog software onto your computer to be  
able  
> to  
> > capture the logs.]*  
> >  
> > *Enable auditing of security events on your Windows system, including  
logon  
> > successes and/or failures and NTFS auditing of files and registry keys.  
> For  
> > more information, see the section in this FAQ entitled "How can I enable  
> > auditing / logging on my computer / server?"*  
> >  
> > *Change the Windows event log settings to be appropriate for your  
> > environment. Consider increasing the maximum log size to retain more  
> > information. Be careful not to log too much, or you might find that  
your  
> > logs contain only a few minutes or hours worth of data.*  
> >  
> > *Check the logs to be sure logs are really being captured.*  
> >  
> > *\* Consider using a file change checker, such as the unsupported free  
tool  
> > Languard File Integrity Checker at [www.gfi.com/languard/lantools-fic.htm](http://www.gfi.com/languard/lantools-fic.htm)  
> > Files changing on your system can sometimes indicate a hacker intrusion.*  
> >  
> > *\* Consider using a Windows event log monitor. Some types of intrusions  
> > leave entries in one of the logs on your computer. [On an especially  
> > vulnerable or secure system, you should be sure that you've configured  
> > logging to detect events such as intrusions.] Some network monitors  
such  
> as  
> > [www.ipsentry.com](http://www.ipsentry.com) can send a message to your email/screen/pager if a  
server  
> > or service stops responding, an event or error appears in a Windows log,  
> > etc. Windows log monitors can be found by searching an Internet search  
> > engine or your favorite software web site, or by using the links below:  
> >  
> > [www.ipsentry.com](http://www.ipsentry.com) [around \$100 US]  
> > [www.sunbelt-software.com](http://www.sunbelt-software.com)*

Re: How to Maintain an IIS Server?

> > [www.webattack.com](http://www.webattack.com)  
> > [www.wilders.org](http://www.wilders.org)  
> > [www.download.com](http://www.download.com)  
> > [www.tucows.com](http://www.tucows.com)  
> > [www.google.com/search?q=windows+event+log+monitor](http://www.google.com/search?q=windows+event+log+monitor)  
> >  
> > \* Consider using EFS file encryption [under Windows 2000 / XP / .NET] or  
> > third-party utilities to encrypt the files on your computer may be  
> something  
> > to consider. Some of these utilities can encrypt your entire hard drive  
> > including Windows, whereas other tools just encrypt some of your data  
> files  
> > and are not suitable for encrypting or preventing access to Windows.  
> >  
> > Note that using any form of encryption can slow down your computer's  
> > performance. Also, you must be extremely careful to back up and protect  
> > your encryption key and any passwords. If the encryption keys are not  
> > backed up, users can lose their encrypted files forever when Windows is  
> > reinstalled, Windows encounters a problem so that Windows no longer  
starts  
> > up, etc.  
> >  
> > For more information on EFS file encryption on Windows 2000 / XP / .NET,  
> see  
> > the section in this FAQ entitled "I used Windows 2000 / XP EFS file  
> > encryption to encrypt some files. Now, I can't read the files. How can  
I  
> > unencrypt them or recover the key?"  
> >  
> > Third party encryption software can be found at the following locations:  
> >  
> > [www.pgp.com](http://www.pgp.com)  
> > [www.scramdisk.clara.net](http://www.scramdisk.clara.net)  
> > [www.e4m.net](http://www.e4m.net)  
> > [www.jetico.com](http://www.jetico.com) ["BestCrypt"]  
> > [www.download.com](http://www.download.com)  
> > [www.tucows.com](http://www.tucows.com)  
> > [www.google.com](http://www.google.com)  
> >  
> >  
> > \_\_\_\_\_  
> >  
> > Which firewall should I choose? Which firewall is the best?  
> >  
> > (6.2) What are some ways for me to enable Intrusion Detection or IDS?  
> >  
> > (6.3) How can I enable or configure the Windows XP ICF Internet  
> Connection  
> Firewall?  
> >  
> > (6.4) How can I enable or configure TCP/IP Filters or IPsec policies to

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

- > > *protect my computer, filter, block, encrypt or tunnel traffic?*
- > >
- > > *A: The answer to this question varies depending on your computer systems,*
- > > *your security requirements and your personal preferences. Below are some*
- > > *firewalls and other forms of firewall-like packet filtering:*
- > >
- > > ***NO MATTER WHICH FIREWALL YOU CHOOSE...***
- > > *No matter which firewall you choose, you should seriously consider*
- > > *downloading and installing MyNetWatchman or Dshield. These are free*
- > > *programs that work with your firewall software or hardware to*
- > > *automatically*
- > > *report hacking attempts to the hacker's ISP. You get to see information*
- > > *about whether that IP address has been used to scan or hack other*
- > > *computers,*
- > > *or whether it might be targeting just your computer. You also get to see*
- > > *whether the ISP has responded or taken action against the offending user.*
- > > *You can get this software at one of the links below:*
- > >
- > > *www.mynetwatchman.com*
- > > *www.dshield.org*
- > >
- > > *Also, no matter which firewall you choose, the lists below of port numbers*
- > > *for common software services may be helpful when configuring your firewall*
- > > *or when trying to monitor the firewall logs for signs of intrusion:*
- > >
- > > *<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q289241> [common*
- > > *ports on Windows 2000]*
- > > *<http://www.iana.org/assignments/port-numbers>*
- > > *<http://www.iisfaq.com/default.asp?View=P106>*
- > >
- > >
- > > ***FIREWALL SOFTWARE:***
- > > *www.sygate.com [free for non-commercial use, also works like a*
- > > *sniffer]*
- > > *www.kerio.com [free for non-commercial use]*
- > > *www.agnitum.com [free for non-commercial use]*
- > > *www.zonealarm.com [free for non-commercial use, also blocks pop-ups]*
- > > *www.iss.net [Black Ice]*
- > > *www.symantec.com [Norton]*
- > > *www.webattack.com*
- > > *www.download.com*
- > > *www.tucows.com*
- > > *[Windows XP users can also consider using the ICF firewall that comes with*
- > > *XP, more info below]*

> >  
> > *FIREWALL DEVICES [HOME / SOHO]:*  
> > *www.linksys.com [starts around \$70 US]*  
> > *www.netgear.com [starts around \$70 US]*  
> > *<http://search.ebay.com/search/search.dll?query=firewall> [prices on new  
> > and  
> > used firewalls]*  
> >  
> > *FIREWALL DEVICES [PROFESSIONAL / ENTERPRISE]:*  
> > *www.netscreen.com*  
> > *www.netgear.com*  
> > *www.intrusion.com*  
> > *www.cisco.com*  
> > *www.nortelnetworks.com/products/family/contivity.html*  
> > *www.nokia.com/securitysolutions*  
> > *www.microsoft.com/isa*  
> > *<http://search.ebay.com/search/search.dll?query=firewall> [prices on new  
> > and  
> > used firewalls]*  
> >  
> > *LINUX / BSD FIREWALLS:*  
> > *<http://www.ipcop.org> [install to hard drive, friendly GUI]*  
> > *<http://www.smoothwall.org> [install to hard drive, friendly GUI]*  
> > *<http://www.devil-linux.org> [boot CD firewall]*  
> > *<http://gibraltar.at> [boot CD firewall]*  
> > *<http://www.sentryfirewall.com> [boot CD firewall]*  
> > *<http://www.thinman.com/eLSD> [boot CD firewall]*  
> > *<http://www.closedbsd.org> [boot floppy firewall]*  
> > *<http://thewall.sf.net> [boot floppy firewall]*  
> >  
> > *INTRUSION DETECTION:*  
> > *<http://www.snort.org> [free, has a version for Windows]*  
> > *<http://www.trinux.org> [free, runs from a boot floppy disk or  
> > CD]*  
> > *<http://www.iss.net>*  
> >  
> > *Linux / BSD firewalls can be run on an old spare 486 PC to protect your  
> > network, and the software is often free of charge. Some of the  
firewalls*  
> > *above are supposedly intended to be easy enough for small offices and  
home*  
> > *users with no previous Linux experience to use. Linux firewalls are one  
> > inexpensive way to be able to add advanced firewall features that may be  
> > very expensive to add to commercial firewalls. [Features such as  
> > bandwidth*  
> > *usage reporting, QoS bandwidth limiting, intrusion detection, alerts in  
> > real-time to your email or pager, a third network interface to create a  
> > DMZ,*  
> > *identical spare backup firewalls for fault tolerance and scalability,  
etc.*  
> > *are generally free.] Unlike some commercial firewalls, 24x7 on-site*

> > *technical support for Linux / BSD firewalls can be purchased from a number*  
> > *of companies in most cities.*  
> >  
> > *Intrusion detection is software or hardware that generally monitors the*  
> *data*  
> > *transmissions on your network in order to add better alerting, analysis*  
> *and*  
> > *detection of intrusions [without necessarily blocking those intrusions].*  
> > *Note that with most IDS systems, you must tune the default rules and*  
> > *settings, or else you will receive too many false alarms.*  
> >  
> > *Linux firewalls and intrusion detection are not likely to be the best*  
> *way*  
> *to*  
> > *protect just one home computer or laptop [unless you are an expert*  
> *computer*  
> > *user or computer hobbyist]. These tools are probably more useful to*  
> *network*  
> > *administrators.*  
> >  
> >  
> > *ICF – WINDOWS XP INTERNET CONNECTION FIREWALL –*  
> > *If you are using a Windows XP computer at home and do not log into a*  
> *Windows*  
> > *domain, you can enable the free ICF – Internet Connection Firewall –*  
> *that*  
> > *comes with Windows XP. The ICF firewall is generally well respected and*  
> > *secure for home users.*  
> >  
> > *You can enable or configure ICF either by clicking on Start, Settings,*  
> > *Control Panel, double-click Networking and Internet Connections, click*  
> > *Network Connections, right-click the connection on which you would like*  
> *to*  
> > *enable ICF, and then click Properties, Advanced and select "Protect my*  
> > *computer or network."*  
> >  
> > *See the articles below for more information:*  
> >  
> > *How to enable or disable ICF –*  
> > <http://support.microsoft.com/default.aspx?scid=kb;en-us:Q283673>  
> > *More information on ICF and how to configure ICF –*  
> > <http://support.microsoft.com/default.aspx?scid=kb;en-us:Q320855>  
> > <http://support.microsoft.com/default.aspx?scid=kb;en-us:Q298804>  
> > <http://support.microsoft.com/default.aspx?scid=kb;en-us:Q308127>  
> >  
> >  
> > =====  
> >  
> > *How can I tell if I've been hacked?*  
> >

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

> > *A: This can be a complicated procedure and usually requires both prior  
> > experience with forensic investigations and knowledge of what the  
computer*

> > *looked like [which files existed, which ports were open, etc.] or what a  
> > similar computer looks like before being compromised.*

> >

> > *Also, the procedures you follow may vary depending on your security  
needs.*

> > *For example, performing some of the procedures below may modify the  
files*

> > *on*

> > *your computer so that it is not admissible as evidence in court. Other*

> > *procedures below could alert a hacker to the fact that you are looking  
for*

> > *her, causing her to delete evidence or retaliate against you in some  
way.*

> >

> > *If this is a business computer, your company should seriously consider*

> > *hiring a security consultant or contacting the appropriate local law*

> > *enforcement agency, both for the initial forensic response and also to*

> > *improve your security to avoid future intrusions.*

> >

> > *Keep in mind during the investigation that this might NOT be a hacker*

> > *intrusion and might instead be regular network activity or a worm.*

**Books**

> > *such as Incident Response, Hacker's Challenge and/or Hacking Exposed 3rd*

> > *Edition may offer you more information on how to investigate intrusions.*

> >

> > *You may consider performing the actions below:*

> >

> > *1) Unplugging the network cable is one possible way to try to prevent*

> > *further damage.*

> >

> > *2) Use Vision [or Fport] from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge) or Active*

> *Ports*

> > *from [www.webattack.com/get/activeports.shtml](http://www.webattack.com/get/activeports.shtml) or `pstools` from*

> > *[www.sysinternals.com](http://www.sysinternals.com) to look at the open ports on your computer and the*

> > *program or executable using that port. Some firewall software such as*

> > *[www.sygate.com](http://www.sygate.com) will also tell you this information.*

> >

> > *You can also use the NETSTAT –A command that comes with Windows to look  
at*

> > *open ports; however, this will not identify which program is using the*

> *port.*

> >

> > *If you're unsure about the purpose of a particular port or program, try*

> > *searching an Internet search engine such as [www.google.com](http://www.google.com) for the name*

> *of*

> > *the port or program, or try right-clicking on the file in question to*

> *see*

> > *the properties. Or, you could even try to telnet to that port e.g. by*

## microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

- > > *typing TELNET LOCALHOST PORTNUMBER or TELNET COMPUTERNAME PORTNUMBER*
- > > *[example, TELNET LOCALHOST 82 ] and press the Enter key a few times to*
- > *see*
- > > *if any informative messages appear.*
- > >
- > > *3) Consider using a file change checker, such as the unsupported free*
- > *tool*
- > > *Languard File Integrity Checker at*
- www.gfi.com/languard/lantools-fic.htm.*
- > > *Recently changed files on your system can sometimes indicate an*
- intrusion.*
- > > *You could also find and list the files on your hard drives that have*
- been*
- > > *modified in the past 3 days by clicking on Start, Search [or Find],*
- Files*
- > *or*
- > > *Folders, and setting the appropriate date [though note that this may*
- > *change*
- > > *the "Last Accessed" date stamp on some of these files]. "The Forensic*
- > > *Toolkit" from www.foundstone.com/knowledge includes command-line tools*
- to*
- > > *list files without modifying the date.*
- > >
- > > *4) Inspect the programs that launch when Windows starts on your*
- computer,*
- > > *by using MSCONFIG or Startup Cop. Suspicious programs starting when*
- > *Windows*
- > > *starts can indicate a successful intrusion. [These can also indicate*
- less*
- > > *serious events such as a virus or worm infection or even the*
- installation*
- > *of*
- > > *a freeware or ad-ware program such as an MP3 music file-sharing*
- program.]*
- > > *See the section in this FAQ entitled "I think there may be a suspicious*
- > > *program, Trojan, ad-ware, "porn dialer," etc. starting up on my computer*
- > > *when Windows starts" for more information on how to do this.*
- > >
- > > *5) Check the logs on your computer, especially your Internet router or*
- > > *firewall logs, the IIS web and ftp server logs and Windows security*
- event*
- > > *log. [This is probably the first thing to do if IIS web services are*
- > > *running on the computer.] Some of these logs may not exist if you have*
- not*
- > > *already enabled them.*
- > >
- > > *Many common hacks are first seen in the IIS web server logs. Any line*
- in*
- > > *your web server log that contains % or .EXE and which also contains a*
- 200*
- > > *or 502 error code is cause for further investigation. If you are*

familiar

> > *with DOS commands, you may be able to see exactly what commands the  
> intruder  
> > tried to execute. Keep in mind that every web server on the Internet  
will  
> > have suspicious looking entries from worms like Nimda, though these are  
> not  
> > necessarily signs of a successful intrusion.  
> >  
> > For more information on deciphering web server logs, see the section in  
> this  
> > FAQ entitled "I keep seeing strange things in my IIS web server logs,  
like  
> > 'NNNNNNNNN' or 'GET /scripts/root.exe' Have I been hacked?"  
> >  
> > 6) Consider using a Trojan scanner. Antivirus programs generally  
detect  
> > some but not all of the most common Trojans and hacker tools. Some  
people  
> > choose to use a Trojan scanner in addition to antivirus.  
> >  
> > For more information on where and how to locate and use free and  
not-free  
> > Trojan scanner software, see the section in this FAQ entitled "Which  
> > antivirus should I choose? Which antivirus is the best?"  
> >  
> > 7) Consider installing an antivirus program that is configured to  
> > automatically download updates daily.  
> >  
> > For more information on where and how to locate and use free and  
not-free  
> > antivirus software, see the section in this FAQ entitled "Which  
antivirus  
> > should I choose? Which antivirus is the best?"  
> >  
> > 8) Consider running a port scanner [and/or a vulnerability scanner] to  
> look  
> > for security flaws and configuration errors on your computers. For  
> example,  
> > you might also run a port scanner against your computers to look for  
open  
> > ports. A particular open port might indicate the way a hack occurred  
> and/or  
> > might give you a way to identify other infected computers. Begin with  
> > Vision, Fport and/or SuperScan from [www.foundstone.com/knowledge](http://www.foundstone.com/knowledge), MBSA  
> from  
> > [www.microsoft.com/download](http://www.microsoft.com/download) and/or Languard Network Scanner from  
> [www.gfi.com](http://www.gfi.com)  
> >  
> > See the section in this FAQ entitled "How can I scan my computer or  
> firewall*

microsoft.public.inetsrvr.iis.security: Re: How to Maintain an IIS Server?

- > > *to look for open ports or confirm that my machine is secure?" for more*
- > > *information.*
- > >
- > > *9) Consider enabling or installing a firewall and/or a sniffer [either*
- > > *software or hardware based] to monitor and look for unusual network*
- > > *traffic.*
- > > *There are a number of free firewalls available on the Internet which can*
- > > *show network transmissions to and from your computer, such as*
- > > *www.sygate.com, or you could use the Network Monitor which comes with*
- > > *Windows 2000 / XP / NT / .NET, or Ethereal at www.ethereal.com, or*
- > > *Windump*
- > > *at <http://windump.polito.it>*
- > >
- > > *For more information on how and where to locate free and not-free*
- > > *firewall*
- > > *software and hardware, see the section in this FAQ entitled "Which*
- > > *firewall*
- > > *should I choose? Which firewall is the best?"*
- > >
- > > *10) The third party web sites and tools below may also be helpful:*
- > >
- > > *www.sysinternals.com*
- > >
- > > *For example, some of the helpful free tools on this site include*
- > > *Filemon,*
- > > *Regmon and Process Explorer which all display activity on your computer*
- > > *you*
- > > *might not otherwise be able to see. These tools show which files,*
- > > *registry*
- > > *keys, .DLLs and other objects are currently being accessed and by which*
- > > *process.*
- > >
- > > *Pstools is a group of tools including pslist, which lists detailed*
- > > *information about processes, and psloggedon, which displays who is*
- > > *logged*
- > > *onto your computer currently.*
- > >
- > > *www.foundstone.com/knowledge*
- > >
- > > *In addition to the Vision / Fport tools, one of the free tools on this*
- > > *site*
- > > *is NTLlast, a security event log analysis tool that helps identify who*
- > > *has*
- > > *gained access to the system, using the NT security event logs [assuming*
- > > *auditing has previously been turned on].*
- > >
- > > *Also, the Forensic Toolkit is a collection of tools including:*
- > > *\* Afind, which lists recently accessed files without changing the date*
- > > *stamp*
- > > *on the file;*
- > > *\* Hfind, which scans the disk for hidden files;*

microsoft.public.inetserver.iis.security: Re: How to Maintain an IIS Server?

> > \* *Sfind*, which scans the disk for files hidden in data streams.  
> >  
> > [www.incident-response.org/IRCR.htm](http://www.incident-response.org/IRCR.htm)  
> >  
> > *Incident Response Collection Report (IRCR)* is a collection of forensic  
> > tools  
> > that automates many of the tasks a forensics expert might perform.  
> >  
> > If you have trouble understanding the results of any of these tools, you  
> > can  
> > post your results along with your question to an appropriate Usenet  
> > newsgroup. Note that the Microsoft newsgroups may not be the place to  
> > get  
> > the best answers to your questions, though you can try and see what  
> > happens.  
> >  
> > [Thanks to Susan Bradley, Rob Lee and others]  
> >  
> >  
> > \_\_\_\_\_  
> >  
> > (7.2) How can I re-secure my computer or server after being hacked?  
> >  
> > A: If your computer or server has been compromised, it is highly  
> > recommended that you follow this procedure to secure your computer:  
> >  
> > 1) Hire someone with security experience to investigate your computer  
> > and  
> > confirm that it has been hacked, learn how it was hacked, collect  
> > evidence,  
> > confirm that your other computers have not been hacked, etc.;  
> > 2) Back up your data files;  
> > 3) Format the hard drives;  
> > 4) Reinstall Windows and all other software onto the computer;  
> > 5) Do not put the computer back on the network or the Internet until  
> > the  
> > previous steps are completed [since un-secured computers on the Internet  
> > can  
> > be hacked within 15 minutes].  
> > 6) Follow the further instructions for securing your computer by  
> > reading  
> > the section in this FAQ entitled "How can I harden my computer or server  
> > to  
> > secure it from hackers?"  
> >  
> > This procedure [formatting and reinstalling] is recommended because it  
> > is  
> > difficult to be certain that you have found and removed all changes the  
> > intruder made to your computer. If the hacker added a login ID, changed  
> > a  
> > password, installed remote control software, etc. onto your computer,

the

> > *hacker or other hackers could easily get back into your computer.*

> >

> > *If you wish, you can take the chance and just try your best to remove*

> > *everything you can find, but then you may still be at risk.*

Instructions

> > *for how to manually re-secure your system without formatting and*

> > *reinstalling everything can be complex and are beyond the scope of this*

> *FAQ.*

> > *However, some general tips are given in the section in this FAQ entitled*

> > *"How can I tell if I've been hacked?"*

> >

> > *BEFORE you format and reinstall Windows, it may be a good idea to have*

> > *someone investigate the computer to look for clues as to how the*

computer

> > *was compromised and by whom. This information can help you to:*

> >

> > *1) Confirm that you really were hacked, possibly saving you from*

> *needlessly*

> > *formatting and reinstalling Windows on your computer;*

> > *2) Find other machines on your network that were also hacked;*

> > *3) Learn what mistakes were made that allowed the computer to be*

> > *compromised and avoid making those mistakes in the future.*

> >

> > *Instructions for how to determine whether or not you've been hacked are*

> > *complex and are beyond the scope of this FAQ. However, some general*

tips

> > *are given in the section in this FAQ entitled "How can I tell if I've*

been

> > *hacked?"*

> >

> > *Note that unless you are already experienced in forensics, any actions*

you

> > *take on your computer will probably reduce your ability to use your*

> *computer*

> > *as evidence in a court of law, and could provoke the hacker into*

> *retaliating*

> > *against you in some way. [On the other hand, your chances of being able*

> *to*

> > *find and prosecute the hacker are slim, unless you are a business, or a*

> > *government entity, or can prove substantial financial loss as a result*

of

> > *the hacking. If you fall into one of these categories, you should*

contact

> *a*

> > *local law enforcement agency, such as the local FBI office in your city*

if

> > *you are in the U.S.]*

> >

> >

> >

>>  
>> *Which port scanner or vulnerability should I use? Which scanner is the  
>> best?*  
>>  
>> *(8.3) How can I scan my computer or firewall to look for 'open ports'  
or  
>> confirm that my machine is secure?"*  
>>  
>> *A: Computers on the Internet use IP addresses and port numbers while  
>> exchanging communications to make sure the communications get to the  
right  
>> software program on the right computer. Just as a single cable carries  
>> multiple distinct cable TV channels using different channel numbers  
> [channel  
>> 2, channel 3, etc.] to your TV at the same time, the Internet carries  
>> multiple different messages to and from your computer using different  
port  
>  
>> numbers [TCP port 80, UDP port 53, etc] to distinguish one message from  
>> another and also to distinguish which software on your computer should  
>> receive the message.  
>>  
>> *An "open port" on your computer generally means that a piece of software  
> on  
>> your computer is "listening" and accepting messages from other  
computers.  
>> If that software on your computer has a vulnerability or is missing a  
>> security patch, someone could use that open port and the vulnerability  
>> within it to control of your computer.  
>>  
>> There are a number of web sites that help you do a port scan to look for  
>> some common open ports on your computer. Some of these sites include:  
>>  
>> <http://scan.sygatetech.com> – longer, more thorough  
>> <https://grc.com/x/ne.dll?bh0bkyd2> – brief, scans just key ports  
>> <http://www.blackcode.com/scan>  
>> <http://security2.norton.com>  
>> <http://www.auditmypc.com>  
>> <http://www.sdesign.com/securitytest>  
>> <http://www.doshelp.com/dostest.htm>  
>>  
>> *Note that few or none of the scans above scan every single possible port  
> on  
>> your machine. There are 65,535 possible TCP ports and 65,535 possible  
UDP  
>> ports on your machine. FYI, most of the scans above do simple port  
scans  
>> looking for open ports on your computer, which is probably good enough  
for  
>> security purposes, but is not exactly the same type of scan a hacker may  
>> use.***

