

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

Secure Windows XP from hackers/unwanted intruders.

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2003-08/1062.html

From: kathryn resop (katresop_at_hotmail.com)

Date: 08/06/03

Date: Tue, 5 Aug 2003 15:26:13 -0700

>-----Original Message-----

>

>

>This 17 step guide will help you secure Microsoft Windows XP, especially

>if you plan on using IIS to host simple webservers in XP, or just want

>to keep hackers/intruders out of your system.

>

>All the info is free, all it takes is some time to do and a willingness

>to harden your system.

>

>

>

>The full guide with screenshots and working links is here

>

>

>

>Europe:

>

><http://anyweb.kicks-ass.net/SecureXP/>

>

>USA:

>

><http://www.lokbox.net/SecureXP/>

>

>cheers

>

>anyweb.

>

>

>Checklist for Securing a Windows XP IIS 5.1 Webserver

>by Greg Thatcher, MCSE, CCNA and Niall Brady, CNA.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

>

>

>*This document was inspired by the need for Windows XP Professional IIS*

>*5.1 administrators to have a checklist available for them which clearly*

>*explains how to secure their Web Server from the many Worms and script*

>*kiddies who will inevitably target them. Windows XP Professional*

>*includes IIS 5.1, it is not installed by default, you have to physically*

>*install it as an optional extra. By default, XP will install several*

>*folders, help files, ASP files, remote web support and more. If you are*

>*reading this document and already have a running XP Pro IIS Webserver*

>*then you should consider backing it up first. XP includes a backup*

>*feature for IIS and it is explained below. If however, you are just*

>*installing IIS for the first time, read this first, then go ahead and*

>*install everything (we're going to remove or disable most of it anyway).*

>

>*Before implementing any of these changes on your XP machine, it is*

>*strongly recommended that you backup your system (including the "System*

>*State") and also backup IIS. Click here for examples of how to do this.*

>

> * 1.) *Verify that Automatic Updates are set to install*

>*automatically. This utility is built into Windows XP and keeps you*

>*notified of Critical Updates and Service Packs. Most hacker attacks*

>*target machines that DO NOT have the latest Service Packs and Hotfixes*

>*installed on them. To see how to set this up click here. Alternatively*

>*you can manually update your system by going to Microsoft at*

>*<http://windowsupdate.microsoft.com>*

>

> * 2.) *Disable and Audit the following files:*

ftp.exe, tftp.exe,

command.com, cmd.exe, telnet.exe, wscript.exe, and

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

cscript.exe.

> *Regardless of the mechanism a hacker uses to break into your machine,*

> *the goal is the same: to execute the hacker's code on your machine. The*

> *above mentioned programs can be used by hackers to install hacker*

> *software, and also run code of the hackers choice.*

>

> *By disabling and auditing a file, you prevent the hacker from*

> *doing damage, and also audit the hacker's activities in Event Viewer so*

> *that you can detect the attacks.*

>

> *It is not recommended that you Delete or Rename any of these*

> *files. Windows XP includes a feature called "Windows File Protection"*

> *which will automatically replace some of these files (e.g. cmd.exe) if*

> *they are deleted or renamed.*

>

> *If you need access to one of these programs, it is recommended*

> *that you make a copy of the program with a different name (e.g.*

> *"cmdsafe.exe" or "ftp99.exe") -- don't forget to update any shortcuts to*

> *these files. This way, the hacker will not likely be able to find it*

> *(only you will know the name).*

>

> *o Click here to learn how to disable a file.*

> *o Click here to learn how to audit a file.*

>

>

> ** 3.) Rename the Administrator account and disable the Guest account.*

> *By default, winXP creates two accounts that many hackers look for*

> *on your machine, "Guest" and "Administrator". If your machine is a*

> *member of a domain, you will need to do this twice: Once on your*

> *machine, and once in Active Directory (Active Directory is beyond the*

> *scope of this article).*

>

> *Click here to see an example of disabling the*

> *Guest account, and*

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

>renaming the Administrator account.
>
> * 4.) Use strong Account Policies:
>
> The easiest way for a hacker to break into your network is via
>weak passwords and account policies. Using "Local Security Settings" (or
>Group Policy if you are using Active Directory), you should set the
>following:
>
> o Password Policy (these make it hard for hackers to guess
>passwords)
> + Enforce password history: 24 passwords remembered
> + Maximum password age: 42 days
> + Minimum password age: 2 days
> + Minimum password length: 8 characters
> + Passwords must meet complexity requirements: Enabled
> + Store passwords using reversible encryption: Disabled
>(this may create problems for Macintosh or RAS users in your network)
>
> o Account policies (these make it hard to run dictionary
>attacks against your machine)
> + Account lockout duration: 60 minutes
> + Account lockout threshold: 3 invalid logon attempts
> + Reset account lockout counter after: 60 minutes
>
>
> Note that these account lockout policies do not apply to the
>Administrator account. It is very important to rename the Administrator
>account, as hackers will often run dictionary attacks against the
>Administrator account.
>
> Click here to see an example of setting account policies.
>
>
> * 5.) Auditing Windows XP Pro allows you to audit your machine

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

>through several mechanisms:

>

> o IIS Logs: You should enable IIS Logging on all websites

>your machine hosts. You should periodically review these log files for

>hacker attempts. Specifically, search these files for failed (e.g. 404)

>requests, and also for the following words: echo, copy, rename, dir,

>del, format, cmd.exe, command.com, tftp.exe, ftp.exe, and in general,

>any .exe, .com, .bat or other file extension which your web users should

>not be using. The IIS Log files will also include the IP address of the

>attacker. You can use the Whois Tool included with InternetPeriscope to

>find out information about the hacker and his ISP from this IP address.

>

> Click here to see how to setup IIS logging.

>

> o Event Viewer -- Security Log: Windows XP

Pro comes with a

>tool called Event Viewer (available under the Programs--Administrative

>Tools menu.) This tool logs Application, System, and Security Events.

>Unfortunately, the default installation of winXP does not enable any

>Security logging; you must turn on Security Auditing manually.

>

> It is recommended that you configure the following using

>"Local Security Policy" or Active Directory Group policy (if your

>machine is a member of a domain.)

>

> + Audit account logon events: Failure

> + Audit account management: Success/Failure

> + Audit logon events: Failure

> + Audit object Access: Failure

> (Note: This allows you to audit failed access to

>files. In addition to enabling this policy, you must also explicitly

>configure the file or directory for auditing. Click here to see an

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

- >example of this.)
- > + *Audit policy change: Success/Failure*
- > + *Audit privilege use: Failure*
- > + *Audit system events: Success/Failure*
- >
- >
- > *Of course, it is very important to periodically review the Event*
- >*Viewer Security log. It is strongly recommended that you backup ALL log*
- >*files and set Event logs to "Do not overwrite events (clear log manually)".*
- >
- > *Click here to see an example of setting up Audit Policy.*
- >
- > * 6.) *Disable unnecessary services/drivers*
- >
- > *o Disable Ftp Service: Ftp sends passwords in cleartext. This*
- >*makes it easy for a hacker to "snoop" on traffic to your machine, and*
- >*obtain your passwords. If you must run an ftp service on your webserver,*
- >*it is strongly recommended that you disable "Write" access (Click here*
- >*for info on how to do this.) If you must enable ftp write access, it is*
- >*strongly recommended that you use IPSec to encrypt ftp traffic between*
- >*your ftp server and clients. IPSec is beyond the scope of this article.*
- > *o Disable SNMP: Recently, many flaws have been found in the*
- >*implementation and specification of SNMP. In addition, the default*
- >*installation of SNMP allows hackers to obtain information on your server*
- >*via the "Public" Community string.*
- >
- > *Click here to learn how to determine if your machine is*
- >*running an SNMP agent, and how to remove it.*
- > *o Disable Indexing Service: This indexing service allows you*
- >*(and hackers) to quickly search for files on your system. Unless your*
- >*webserver is using the Indexing Service to create a "Site Search" of*
- >*your website, it is strongly recommended that your remove this service*

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

>(More on this later.)

>

> Click here to learn how to remove the Indexing Service.

> o *Disable Simple TCP/IP Services: These services are not*

>*installed by default, but many Sys Admins install them because they*

>*include such fun services as "Quote of the Day" and "Daytime". These*

>*services have been favorite targets of attackers for many years.*

>

> Click here to learn how to determine if your machine is

>*running these services.*

> o *Disable Network Monitor Driver. This driver is used by*

>*"Network Monitor" and/or SMS to analyze traffic on your machine.*

>

> * 7.) *Default winXP Installation Directories.*

>

> *Many hacker scripts depend on the default installation of Windows*

>*to work. For example, a hacker may, through a variety of mechanisms,*

>*attempt to run the following command from inside your Web directory:*

>*...\. \windows\system32\cmd.exe /C del c:*.**

>

> *This command would successfully delete the files on your C drive*

>*provided that:*

> o A.) *Your website was installed in the*

c:\inetpub\wwwroot

>*directory.*

> o B.) *Windows is installed in the c:\windows directory.*

>

>

> *When installing ANY software on your machine, it is very*

>*important that you not choose the default installation directory. When*

>*installing Windows XP, don't install it in the default c:\windows (or*

>*c:\winnt) directory. Instead, install it in the*

j:\winXP10 directory (or

>*something else that's hard to figure out). When creating a website,*

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

> *don't install it in c:\inetpub\wwwroot, instead, install it in*
> *m:\internet\websites\public directory.*
>
> *Most hackers are running scripts that were written by someone*
> *else. These scripts often make default assumptions about how your server*
> *was installed. By not using the default partitions (or volumes) and*
> *directories, you can "fool" their scripts.*
>
> ** 8.) IIS Server Configuration*
>
> *o a.) Remove FrontPage Extensions. There are a number of*
> *exploits against FrontPage. It is strongly recommended that you remove*
> *this. Click here to learn how.*
> *o b.) Remove Remote Desktop Web Connection (TSWEB). By*
> *default, IIS includes a website that enables you to administer the*
> *computer hosting IIS via a website. Typically that would show up as a*
> *url such as <http://www.yoursitename.com/tsweb>. Click here to learn how*
> *to remove this.*
> *o c.) Remove unused App Mappings from Web Server. IF YOU DO*
> *NOTHING ELSE, AT LEAST DO THIS!*
>
> *IIS includes a number of "Application Mappings" that invoke*
> *various programs when a web page with a certain file extension (e.g.*
> *..asp or .pl) is called. Even if you don't have a file in your website*
> *with one of these extensions, your server may still be vulnerable to an*
> *exploit against one of these file types -- and there are MANY exploits*
> *against various Application Mappings.*
>
> *It is strongly recommended that you remove all unused*
> *Application mappings. "IIS Security Audit" can help you determine which*
> *Application Mappings you need to remove.*
>
> *Specifically, you should remove the*

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

following: .cer .cdx

>..asa .htr .idc .shtm .shtml .stm .printer plx

>

> *In addition, if you are not using .asp or Perl files, you*

>*should remove the following application*

mappings: .asp, .pl

>

> *Click here to learn how to remove Application Mappings.*

>

> *Click here to learn more about vulnerabilities against*

>*various App Mappings.*

>

> * 9.) *Website Configuration*

>

> *o a.) Disable the "Default Web Site" and delete all of its*

>*files. Hackers look for this configuration -- get rid of it. Create your*

>*own website, and don't put it in the c:\inetpub\wwwroot directory.*

>

> *o b.) Turn off "Index this resource" on ALL websites. If you*

>*want to create a "Site Search" for your website, use a 3rd party tool*

>*that does not index the SOURCE CODE of your server-side scripts.*

>

> *o c.) Turn off "Directory browsing" on ALL websites and*

>*virtual directories. Don't allow hackers to "browse" through your files.*

>

> *o d.) Delete the "AdminScripts", "IISamples" and "Scripts"*

>*directories. Hackers know of these default directories, and know of many*

>*exploits against the files that are installed in these directories in a*

>*default installation of IIS. Get rid of these directories, and never*

>*name your directories with these names.*

>

> *o e.) Remove any residual FrontPage directories. Frontpage*

>*installs a bunch of directories that begin with the "_" character.*

>*Delete all of these directories and files, and get rid*

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

of any files or

> *directories that your website is not using.*

>

> *o f.) Make sure that none of your websites have the "Write"*

> *Permission turned on.*

>

> *To learn how to configure an IIS website, click here.*

>

> ** 10.) Enable auditing on Web and Ftp directories for Write,*

> *Delete, and Change Permissions.*

>

> *Remember that to enable auditing, you must perform two steps:*

> *o A.) Turn on "Audit object access" in "Local Security*

> *Settings" or "Group Policy".*

> *o B.) Enable auditing for individual files and directories.*

>

>

> *You should only enable auditing on files and directories that do*

> *not change often. Do not enable auditing on your mail directories (e.g.*

> *mailroot), or web directories that are generated periodically by log*

> *analysis programs (like Analog).*

>

> *Be sure to check the Event Viewer – Security log periodically for*

> *hacker attempts.*

>

> ** 11.) Check all open TCP/IP ports.*

>

> *First, check to see which ports your machine has open, and figure*

> *out which services the ports map to. For the former, you can use*

> *"netstat –an" from a DOS prompt. Many users may find the Port Scan*

> *feature of InternetPeriscope easier to use, as it tells you which*

> *services are commonly used by which ports. Install and run*

> *InternetPeriscope ON your server for this first test.*

>

> *Next, perform a Port Scan on your server from a machine that is*

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

> *OUTSIDE of your firewall. Again, InternetPeriscope can help you to do*
> *this. This will give you an idea of what ports the hacker's see when*
> *they scan your system.*
>
> *If you see any services on your machine that you do not need, you*
> *should remove them to further "harden" your server's security.*
>
> ** 12.) Miscellaneous Tasks*
>
> *o A.) winXP Servers include a "Security Configuration and*
> *Analysis Tool". Unfortunately, this tool is well hidden in a default*
> *installation. Click here to learn how to use this tool.*
>
> *o B.) Disable "Enumeration of SAM accounts and Shares (by*
> *anonymous users)". Depending on your configuration, Hackers can*
> *sometimes get a list of the usernames and share names on your machine*
> *using a "Null Session Vulnerability". This information can help the*
> *hacker to more easily crack passwords or take advantage of an unsecured*
> *share.*
>
> *Click here to learn how to turn off "Enumeration of SAM*
> *accounts and Shares (by anonymous users)".*
>
> ** 13.) Disable Remote Data Services (RDS)*
> *RDS is known to be vulnerable to hacker attacks that enable a*
> *hacker to run files on your machine. Most websites do not use RDS, so*
> *RDS can be safely disabled. "IIS Security Audit" can help you determine*
> *if your machine is vulnerable to an RDS attack.*
>
> *Click here to learn more about the RDS vulnerability.*
>
> ** 14.) Disable ODBC Shell Access Vulnerability*
> *IIS is vulnerable to an attack via the Jet Database Engine that*
> *can enable a malicious user to execute programs on an*

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

IIS Server. "IIS

>*Security Audit" can help you determine if your machine is vulnerable to*

>*an ODBC Shell Access attack.*

>

> *Click here to learn more about the ODBC vulnerability.*

>

> * 15.) *Check Startup Files for Hacker Software*

> *Windows has a number of methods for automatically launching*

>*software when a machine first boots or when a user first logs in. If*

>*your machine is attacked by hackers or infected by a Trojan, it is very*

>*likely that malicious software will be installed that uses one of these*

>*"auto-starting" mechanisms.*

>

> *It is recommended that you periodically check and document which*

>*software is configured to "auto-start" on your server.*

If you believe

>*your machine has been compromised, it is important that you check for*

>*"auto-starting" software before you reboot your machine.*

>

> *"InternetPeriscope" can help you check for "auto-starting"*

>*software on your machine.*

>

> *Click here to learn more about the "auto-starting" methods used*

>*by hackers.*

>

> * 16.) *Use NTFS permissions to block Write Access*

> *For many companies, the most horrifying danger posed by hackers*

>*is the modification of their web or ftp site.*

Specifically, they don't

>*want hackers to deface their web pages or install trojan software on*

>*their ftp site. Fortunately, this is easy to prevent using NTFS.*

>

> *NTFS allows you to specify which users can read or write specific*

>*directories and files. Unfortunately, the*

group "Everyone" is given the

>*"Full Control" permission by default. This means that anyone who gains*

Secure Windows XP from hackers/unwanted intruders.

microsoft.public.windowsxp.security_admin: Secure Windows XP from hackers/unwanted intruders.

> access to your web directory can write to it through a variety of hacks.

>

> *It is strongly recommended that you either "Deny" or remove the*

> *"Write" permission from the "Everyone" Group on your web and ftp*

> *directories. This way even if a hacker gains access to your system, it*

> *very unlikely that he will be able to modify your web or ftp files,*

> *causing your company great embarrassment.*

>

> *Click here to learn how to change NTFS permissions.*

>

> ** 17.) Remove Remote Access capability to your Windows XP computer.*

>

> *Click here to learn how to change your Remote Access capability*

> *via Microsoft Terminal Services.*

>

>

>

>

>

>