Windows Insider
35,000 Subscribers Worldwide
May 15, 2002
Issue #92

Feature

Windows 2000 Security Quickstart Read it

Ask Uncle Bill

Q and A's Read it

Security Advisories

Unchecked Buffer in MSN Chat Control Read it

News Headlines & Resources

The Hardware that Connects Us – Part 1 Read it
Upgrade Windows XP/Install XP via RIS Read it
How to Set Up and Configure a Win2K FTP Server Read it
How to Set up and Configure a Win2K Virtual NNTP Server Read it
The License 6.0 Debacle Read it
ISA Server Rules Engine and Web Proxy service Hotfix Read it
Installing Win98/ME AFTER installing Windows XP Read it
Microsoft Considering Desktop and Security Certs Read it
Is your NIC Promiscuous? Read it
Managing an ISA Server Cluster with Application Center Read it

Download of the Week

Mail Enable Read it

Feature

Windows 2000 Security Quickstart

to top

One of the things that keeps Windows 2000 administrators from

optimizing their host and network security infrastructure is the fact that there are about 500 things you have to think about in order to reach "optimal" security. What is optimal security? Optimal Security is the point at which some security wonk tells you that there's nothing left you can do improve on your security scheme, and access to services and resources on the network is impossible because of the security setup. At this point, the security mavens will sigh a breath of relief and you'll head for the funny farm after the 15,000th call to the Help Desk.

While there is no such thing as perfect security on a network that allows you to get work done, there are still some things you can do to shore up a lax security configuration. I've put together a baker's dozen of what I consider some of the most effective and simple security configurations that you can make. These settings will improve your overall security setup without breaking your ISA Server, Exchange Server, SQL Server, Mobile Information Server and Internet Information Server configurations.

1) Rename the Administrator Account

How many times have you heard about this one! Yes, renaming the Administrator account can be a bit of a nightmare if you don't rename it right after you install Windows 2000. Why? Certain services you install on the Windows 2000 Server might depend on the Administrator account for service account credentials. After you rename the Administrator account, the services that depend on the Administrator account will fail. If you have a number of these services, you're guaranteed many hours of fun and games as you try to troubleshoot the problem. If you rename the Administrator account, do it immediately after installing Windows 2000, or research the effect of renaming the Administrator account on network services you have installed on the server.

2) Assign a very complex password to the Administrative Accounts

Most users hate dealing with complex passwords. What's a complex password? A complex password is typically defined as one that has eight or more characters and contains at least one lower case letter, one upper case letter, one number and one symbol. However, this is far too weak! Consider using passwords that have at least 16 characters. Its not that difficult! Use long strings of numbers such as: your telephone number when you were 6 years old, your locker combination when you were in 7th grade, the lifetime earnings of your favorite ball-player or racehorse, somebody else's (not yours!) social security number, your car's VIN, etc.

The key here is to use a string that you know well. Then, use a string of letters such as: the first letter in each word of a poem you have memorized, the name of your favorite ball-player or racehorse, the title of your favorite obscure book, the full first, middle, and last name of your least favorite brother-in- law. Separate each of the meaningful elements with a symbol such as & or %. Such a complex password will keep the click- kiddies at bay for a good long time.

3) Create an alternate Administrator Account

Create an account named "Superuser" or "Allpowerful" or "Root". This account will be one Internet criminals will go after first. Make sure this

account has a complex password and that is doesn't have any rights to do anything useful. Use the Domain Security Policy, Local Security Policy or Domain Controller Security Policy (depending on the machines) consoles to remove the bogus admin's user rights. This should keep script kiddies and junior Internet criminals busy for quite some time as you monitor their progress. Make sure to visit them in the Federal Pen after you successful prosecute your case.

4) Confirm that the Guest Account is Disabled

The Guest account is disabled by default on all Windows 2000 machines. But sometimes the account gets turned on for one reason or another. Double-check all your machines to confirm that the Guest account is disabled.

5) Remove the Everyone Group from all Share Permissions and turn on Auditing

Windows 2000 has the bad habit of allowing full control to Everyone when you create a new share. While NTFS permissions can override share permissions, you're better off if you change the Share permissions to Authenticated Users. After removing the Everyone group and replacing it with the Authenticated Users group in the Share permissions, you can drill down on access controls by setting NTFS permissions on the Files and Folders in the Share. Make sure that you enable auditing of all users on sensitive files and selected users/groups on other frequently accessed files.

6) Create Dummy Folders

This is a great one! Create some dummy folders on the drive and place empty files in those folders. Make sure that you audit Everyone on these files and folders. Give the folders colorful and enticing names such as secret.doc, socialsecuritynumbers.txt, payroll.xls, etc. If you really want to have some fun, create hundreds of these files in the folder and put bogus data in the files. The more time the Internet criminal spends working on these files, the more time you're have to perform your forensic investigations and put the cruising loser in the slammer.

7) Create a Bogus password file

I like this one because it's the ultimate in misdirection. Create a file called something like passwords.txt or passwords.doc. Enter about a 100 user names that are NOT in use on your network. For each of these accounts, come up with a 30+ character password that is impossible to remember or break. Just go to town on the keyboard or if you want to make it even more fun, use a random password generator. Make sure that auditing is enabled on this file and that you log failed log on attempts. Once you detect someone has accessed the file, turn on that packet sniffer and nail the bastard!

8) Disable or remove dead accounts

Unused accounts can be a security issue because many of them are for former employees. Those former employees can create problems for you if they can still access the network. Make sure to disable or remove

those unused accounts.

9) Use "What I am, What I have, What I know" security

A key feature in secure environments is that you must combine What you are with What you have with What you know. What you are would be a biometric measure, such as a fingerprint or iris scan. What you have would be a token or Smart Card, and what you know would be password. While it's possible that one of these things could be stolen or forged, its very unlikely that all three of them could be. Most implementations allow for the What I am and What I know. Superior solutions require all three in order to authenticate with a Windows 2000 Domain.

10) Use NTFS on All Partitions

This is a given. You all know there is no security in FAT. Convert any FAT partitions to NTFS. Otherwise, you won't be able to use NTFS access controls!

11) Antivirus Software on all Workstations and Servers

Antivirus software is not a luxury, it's a requirement. Virus writers are getting more and more sophisticated, so you have to stay on top of the virus threat. Of course, AV programs aren't much good unless you update the virus definitions on a regular basis. Most corporate versions of popular antivirus programs allow you to download the latest updates to a central server from where the workstations should get the latest update. Don't allow the workstations to update themselves from the vendor's web site.

12) Centralized Email Virus and Spam Removal

While antivirus solutions on the workstations can whack viruses that arrive to the users' workstations, a better solution is to implement a centralized solution to the email virus problem. Use a server-based application such as Mail Essentials or Mail Security (www.gfi.com). These server-based virus killers can also whack spam. Spam often contains dangerous links that could get users into trouble. Spam itself is a major problem that can easily cause a network DoS, and should be handled centrally.

13) Install the Latest Hotfixes

This goes without saying! You must stay on top of the latest security updates and hotfixes on the Microsoft site. Make it a habit of visiting www.microsoft.com/security every day and subscribe to the Microsoft security alerts mailing list. Use the HFNetChk utility to scan your servers and workstations to see what fixes are required. You can find the utility here.

Summary

Security is job 1.5, right next to getting the work done that allows your company to make money! If you set your security too high or too restrictive, you'll have the safest network in bankruptcy court since your users won't be able to get any work done. Follow these easy security

steps and you've got a good start on securing your Windows 2000 network.

This week's feature article by
Thomas W. Shinder,
M.D., MCSE

Ask Uncle Bill

Q and A's

to top

Question:

Hi, Uncle Bill.
Is there anyway to get the User Manager for Domains from NT 4.0 into an MMC? Our domain is still an NT 4 domain (until later this summer) and we are running 2000 and XP for clients as Admins, we cannot figure out how to add the User Manager into a snap-in. I have seen that MMC 1.0 has User Manager and Server Manager as shortcut buttons on the toolbar, but I can't figure out how to do that with the MMC that ships with 2000 or XP. Any suggestions?
-–Beatphreek.

Uncle Bill says:

Yo Beatphreak! You can't add the old NT "managers" to the MMC because they don't know anything about the MMC. Snap-ins have to be designed to use the MMC. However, all is not lost! You can just copy your NT "managers" executable files to your Windows 2000/XP hard disk and they'll work! While you're at it, you can copy the old winfile.exe and really have some fun.

Question:

Hi, Uncle Bill
I am facing a strange problem these days. My Active Directory Users & Computers tool in Administrative Tools does not open. I also tried to open it using the MMC console and still it didn`t work. I am not able to manage the user accounts and this thing is getting very annoying now. I would be really glad if you could suggest a solution to this problem.
–-Mangesh.

Uncle Bill says:

Hiya Mangesh! Strange problem, that's for sure. Have you made any changes to the configuration recently? Have you applied a security template or made some manual changes to the domain or local security policy? If your DNS configured properly? Does your account have permissions? It could be a dreaded DCOM problem. You might check out Q299943 and see if that helps.

Don't Be Shy!

Got a question about MCSE certification or an event log error that just won't go away? Send it in! We'll be answering a question or two every week. Send your submissions to Uncle Bill **here**.

Security Advisories

Unchecked Buffer in MSN Chat Control Can Lead to Code Execution

to top

An unchecked buffer exists in one of the functions that handles input parameters in the MSN Chat control. A security vulnerability results because it is possible for a malicious user to levy a buffer overrun attack and attempt to exploit this flaw. A successful attack could allow code to run in the user's context.

Read more...

News Headlines and Resources

The Hardware that Connects Us – Part 1

to top

Years ago, the home or SOHO user had one choice to connect to the Internet: an analog modem. Now, average folks have a full plate of Internet connection options. Deb Shinder surveys the iNet connection landscape in Part 1 of this three-part article on connectivity.

Read more...

Upgrade Windows XP / Install XP via RIS

to top

Thinking about upgrading to Windows XP soon? How about using RIS to install Windows XP? If so, you should check out this article. Jason Zandri goes through the steps to get you where you want to go in no time.

Read more...

How to Set Up and Configure an FTP Server in Windows 2000

to top

Why expose yourself to the security risks inherent in Instant Messenger programs? Just set up an FTP server and share your files via FTP! This Microsoft KB article takes you through the steps and shows you a couple of cool tricks too.

Read more...

How to Set up and Configure a Win2K Virtual NNTP Server

to top

Where to you go to find the answer to an impossible-to-solve problem? Newsgroups! Newsgroups provide you with threaded discussions that make it easy to share important information with anyone. Newsgroups are faster and easier to search than Web boards! Check out this article on how to create your own newsgroups.

Read more...

The License 6.0 Debacle

to top

License 6.0 is rearing its ugly head and promises to significantly increase the cost of doing business for many who do not read the fine print. Why buy bloatware when you can rent it? Does the light at the end of the tunnel include self-destructing rentware?

Read more...

Read more...

ISA Server Rules Engine and Web Proxy service Hotfix

to top

There's a slight glitch in the ISA Server rules engine that could allow particularly clever users to get around your outbound access policies. Not good! This fix will prevent them from getting to sites that you've explicitly blocked. There's also a fix for the Web Proxy service too.

Read more...

Installing Win98/ME AFTER installing Windows XP

to top

Have you tried to install a Win9x operating system after Windows XP has been installed on your box? It's not too easy! Check out this page which gives you the steps on how to get your gaming OS onto a Windows XP box.

Read more...

Microsoft Considering Desktop and Security Certs

to top

If you're a hiring manager, you'll love to hear about this. Microsoft is considering adding two more certs to the certification mix. One is a security-oriented cert and the other is a desktop operating system cert. Want/need more letters after your name?

Read more...

Is your NIC Promiscuous?

to top

Is your NIC promiscuous? No, I'm not wondering if your NIC is inserting itself in a number of different computers. A promiscuous NIC could indicate someone has inserted a sniffer on your box! Check out this free download that will check if your NIC has been placed in Promiscuous mode.

Read more...

Managing an MS ISA Server Cluster with Application Center

to top

Microsoft Application Center 2000 provides a server management solution for ISA Server customers who are not using Active Directory, but need a tool for managing and synchronizing ISA Server configuration settings. By using these products in combination, you can achieve a high degree of security, reliability, scalability, and manageability.

Read more...

Download of the Week

Mail Enable

to top

Mail Enable Standard is an extremely cool freeware mail server. This cool piece of freeware includes: an SMTP server, POP3 server, list server, and an MMC administrative interface. I found Mail Enable incredibly easy to set up and the list server is a great piece to include with Freeware!

Download it today if you need a swanky mail server for FREE.

Read more...

Mark Minasi's Windows 2000 Resource Kit: A $124.96 value is yours for just $9.99. Here you'll learn how to solve Registry problems in an instant, master Active Directory quickly, configure Windows 2000 networks perfectly and supercharge the Windows 2000 desktop.

Click here for details.

Free Cramsession IT Newsletters - Choose Your Topics!

H = HTML Format **T** = Text Format

H	T		H	T		H	T	
☐	☐	A+ HardCore News	☐	☐	Engineers Weekly	☐	•	Must Know News
☐	•	ByteBack!	•	☐	Exam Tips 'N Tricks	☐	•	.NET Insider
☐	☐	Cisco Insider	☐	•	IIT Pro News	•	☐	Script Shots
☐	•	CIW Insider	☐	☐	IT Career Tips	☐	☐	Security Insider
☐	☐	Developers Digest	•	☐	Linux News	•	☐	Trainers News

Enter your Email

Subscribe Now!

CramSession
Prepare for Success!

Your subscribed e-mail address is:steven.thode@toadworld.net
To unsubscribe, simply **click here** and hit "send" in your e-mail reader,
or visit the **CramSession Unsubscribe Page** .