Windows Insider

35,000 Subscribers Worldwide

May 22, 2002
Issue #93

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters

CramSession

Feature

Windows 2000 Security Tools

to top

Anyone who's been paying attention knows that security is the new "cash cow" in the IT industry. In the glory days of yesteryear, the MCSE was the cash cow. Well, that cow is now hamburger and the security cow has taken its place in the somewhat denuded field of IT spending. The fact is that if you want to get a job that pays more than what you can make at McDonald's, you're going to need to be a security expert.

The current focus on security is making for interesting times. You know that anytime a new hot field enters the scene that there is going to be a ton of people flooding into the arena. We saw that with the MCSE. Like the MCSE, the overwhelming percentage of people will have no business entering the field. I think this will be even more problematic with computer security.

Why? You cannot make someone into a security person. Security people are more likely born, and not made. Sure, some traumatic incident may take a Peter Pan network admin and turn him into a hardcore security freak, but it's more often the case that the Peter Pan admin will get shaken up for a short time, and then fly away and completely forget that there are criminals out there who want to take, break, and ruin his stuff.

What's really interesting is that there doesn't seem to be much of a relationship between law enforcement and security mindedness. How many cops do you know who blithely park straight behind the car they stop? How many swagger to the driver's side, lean over on your window and ask for your to present your ID? If they were security minded, they would require you to get out of the car with your hands on the roof of the car. These same law enforcement types will use simple, easily guessable user names and crackable passwords on user accounts. They never update their software, and the Security Event Log is the police blotter section of the newspaper.

What makes you a candidate for a security analyst? First, you need to feel in the core of your soul that there are bad guys out there who want to do you harm. That's a tough one for most people, because our mothers told us that most people are good inside. Also, its not politically correct to admit that some people are downright rotten and that there's nothing you can do about it.

Second, you have to be fairly paranoid. You can't just realize there are bad guys out there, you must worry about it every day and be constantly thinking about ways to thwart them. Finally, you have to be very detail oriented. Only the dumbest of criminals leave obvious signs of their criminal behavior. You have to cross every t and dot every i if you expect to make it as a security pro.

Now with that said, suppose you are aware that there are criminals out there, you worry about it, and your're detail oriented. You've got the right stuff to be a security analyst, or at least you're someone who can be trusted with shoring up your network to rebuff Internet criminals. Note that I use the term Internet criminal, and not hacker. There's been too much of a glorification of the term "hacker", so that when a hacker does something it doesn't seem quite as destructive to society then if a criminal had done something. Forget about that! They are just as much criminals as the punk who steals your car, the psycho who kills your kids or the wacko who lights your house on fire. Get used to it and start calling them what they are: criminal scum. Note that there are White Hat hackers who are not criminals. You do a real disservice to these good guys when you call Internet criminals hackers.

So what tools does Windows 2000 bring to the plate to help you on your quest to secure your network? Let's take a quick look at some of these tools.

Group Policy

Have you delved into your Group Policy templates yet? If you use Active Directory, you can apply a security group policy to all of the computers in your domain, and even configure custom security policies for machines and users contained within organization units. You can even use Group Policy security templates on stand-alone computers that do not belong to a dreaded Active Directory domain.

Check it out! On a domain controller, open the Active Directory Users and Computers console. Right click your domain name and click Properties. Click on the Group Policy tab. Pick the appropriate policy and click Edit.

Expand the Computer Configuration node, and then expand the Windows Settings node. Next, expand the Security Settings node. Bingo! Now expand all those nodes under security settings. There is a wealth of security settings that you can set for all the computers in the domain. Make it a point to study each one of these and look up the ones you don't understand. Then consider if your network might be able to take advantage of a particular setting. If so, implement it. If not, don't use it.

Do the same for the User Configuration node. There aren't so many options here, but if you have added the Windows XP template, you'll be able to do some cool stuff with software restriction!

Security Templates and Security Configuration and Analysis

Windows 2000 comes with a number of pre-built security templates you can use to quickly secure workstations, servers, and domain controllers on your network. These pre-built templates have all of the settings already configured for you. All you need to do is apply the template, and you're good as gold.

But I warn you – be VERY careful about applying security templates willy-nilly. Applying a security template without understanding the settings in the template is a good, quick way to break many of your networking services. If you don't understand the settings in the template, you'll have no idea which setting broke your service and how to fix it. Sometimes you can fix the problem, but more often the hapless network admin must reformat and restore from backup.

If you do choose to apply a built-in template, I highly advise you to recreate your server environment in a test lab and apply the template to the test server first. Then run client simulations against the new server. If everything works the way you want it to, great! If something gets broke, figure out why it broke and fix the setting in the security template.

You can edit and create security templates using the Security Templates MMC snap-in. If you want to check the computer's current security settings against one of your template, you need to use the Security

Configuration and Analysis (SCA) snap-in. SCA allows you to test your new template against a current security configuration, and reports the results in either the GUI interface or to a text file.

You can also use the SCA snap-in to apply a new security template to a computer, organizational unit, or domain. You can also save your security templates and settings, so that they'll be available if you need to reapply them in the future. SCA is a powerful tool that you should become familiar with.

Event Logs

You computer's Event Logs are a gold mine of security information! How often do you check your Event logs? Every hour? Every day? Once a week? Once a month!?! Once you enable security auditing, your event logs will tell you who's trying to do what, when, and to whom. Valuable information is reported by network services to the Event Log. The Event Log is your one-stop shop for valuable security info.

Tracking the Event Logs can be a frustrating and complicated procedure. If you have your auditing adequately configured, you can easily build up tens or hundreds of MBs of Event Log entries in virtually no time. Even tracking a couple of servers is a real adventure. The only way you can really stay on top of your Event Logs in a larger environment is to use an automated Event Log analyst. There are a number of these on the market. Microsoft has recently released its own analyst, called the Microsoft Operations Manager. You will have to use some automated approach, because you'll miss something if you don't!

IPSec, Network Monitor and EFS

You can use many other tools. The Encrypting File System (EFS) allows you to secure files on disk. If the user can't present the correct credentials to access an encrypted file on the hard disk, too bad! The user won't be able to access the file. Period.

The problem with EFS is that it only encrypts the files on disk. Once the file leaves the disk, it's fair game. If you send the file over the network, it's sent as clear text. You'll need to use IPSec to protect that file as it moves over the network.

You can use the Windows 2000 IPSec feature to encrypt files as they move over the network. IPSec is highly configurable and you can apply IPSec Policies to individual computers, organizational units, or to an entire domain.

No network security scheme should go without periodic monitoring of all network traffic. That's where your Network Monitor comes in. Set the buffer on your Network Monitor to something like 1 GB, and let 'er rip. Of course, if you're working on a switched network (and who isn't?) you're limited to the traffic going to and from the computer you're running the monitoring tool on. Of course, you have this limitation anyhow with the built-in Network Monitor tool. You can get the SMS version of NetMon and put it in promiscuous mode, or use a 3rd-party network analyzer.

Conclusion

For the most part, security people are born and not made. If you don't have the character to be a good security admin, then don't even try and let someone else deal with that aspect of networking. There's still a lot of other work to be done! If you have the right stuff to take care of network security, start working with the built-in tools provided with Windows 2000. After you master those, start looking at 3rd-party offerings and continue to expand your knowledge base. Remember, there are plenty of evil doers out there who would be very happy to make your life unhappy and miserable. Take the offensive and start working on protecting yourself and putting Internet criminals in jail. Most of them are lonely anyhow, so they'll benefit from their new "relationship" with their cellmates.

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 any way to broadcast a message to all currently logged in users in Windows 2000 (for shut down warning etc.)?
-- Sham.

Uncle Bill says:

Yo, Sham! You bet. This is the oldest trick in the book. Just open a command prompt and type net send * WARNING WILL ROBINSON and everyone will get the message. Make sure you're not connected when you do the test :)

Question:

Hi, Uncle Bill
I'm trying to disable the right click on Outlook XP, so users won't be able to change anything in Outlook. I used GPO with the outlook10.adm file to give Outlook properties to GPO & I used the ops file to customize a special toolbar. I have a problem that I can't disable the right click mouse, and thus users can change the fields properties and other display properties. Do you know a way to disable the right click mouse in Outlook ? I didn't find it in the Office profile wizard nor in the Outlook10.adm file.
-- Ofer Nissim

Uncle Bill says:

Heya Ofer! What kind of users to do you have? Can they be trusted with computers? Computers are now thought of as security devices, so I would suggest you require users have MOUS certification and pass a criminal background check before you let them near Outlook. One wrong right click and POWEE! Maybe you could remove the right mouse button from the mouse itself, or buy them all single-button mice.

Never thought of removing right-click functionality from a single application. What you can do is use the Office Profile Wizard to save the approved profile. When they mess it up in their attempts to subvert your security infrastructure, punish them to the full extent of the law. Use the Wizard to restore their approved profile. **You can get more info on the Wizard here.**

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

Cumulative Patch for Internet Explorer

to top

Time to patch your Internet Explorer again! There has been a bit of controversy over this patch, but you should install it nonetheless. **Click here** and **here** to get the patch and find out what the buzz is all about.

News Headlines and Resources

Circuit Switching v. Packet Switching

to top

What's the difference between a circuit-switched and a packet- switched network? Sure, you were *supposed* to learn the difference in your network essentials class, but did your instructor really know? Check out this article and get a high-level view of these network switching methodologies.

Read more...

Compare IIS 5.0 with IIS 5.1S

to top

Windows XP Pro and .NET will include a new and improved version of IIS. Should you upgrade just to get the new IIS? Check out this article by IIS guru Brett Hill to learn all you need to know about the IIS 5.1 improvements.

Read more...

What's the Remote Storage Service All About?

to top

OK, show of hands... What Windows 2000 feature has the most worthless documentation? If you said the Remote Storage service, you win the prize! Check out this article to learn the stuff that Windows 2000 Help and Resource Kit didn't want to tell you.

Read more...

Use RIS to Roll Out Secure Servers

to top

How about installing your Windows 2000 Servers using RIS? Sure, you can do it! Now, how about installing your new Windows 2000 Server with all the service packs and hotfixes already installed? Cool! Check out this article by Windows 2000 pro Mark Minasi and find out how.

Read more...

Overview of .NET Server with Screen Shots!

to top

Don't have a copy of .NET Server beta? Not a problem! Check out this article and see some cool screen shots and learn a bit about the new OS. One thing though – is this compliant with the NDA? :-)

Read more...

Support for Mode 5 (ATA-100) Disks in Windows 2000

to top

That speedy ATA-100 IDE disk doesn't seem any faster than your old ATA-33 spinner? Could be that you need a patch! In fact, you must have the patch to get full ATA-100 support in Windows 2000. What's really cool is you don't have to call Microsoft PSS to get it.

Just download here.

Windows Update Corporate Site

to top

Want some control over what updates you download? Want to make the updates available on a central server so that you don't crush your Internet connection? Check it out!

Read more...

Watch for the Upcoming Release of "Scene of the Cybercrime"

to top

Tired of reading hacker books and just learning how to be a bad guy? Want to be a good guy? The goal of SCENE OF THE CYBERCRIME is to bring the worlds of law enforcement and IT professionals together, to show how together they can — and must — unite against, detect, and prosecute those who use technology to harm individuals, companies, and society.

Written by a police officer and networking security consultant, the book helps IT pros and law enforcement personnel understand each other's roles, and why an organized, cooperative effort is necessary to win the fight against Internet criminals.

Read more...

ISA Server Presentations and White Papers

to top

Getting ready to dump that black box for a new ISA Server? Here's a great site where you can access a bunch of videos, presentations and white papers on ISA Server. Lots of good stuff, so come back again and again.

Read more...

Support WebCast: Microsoft Win2K Print Servers and Drivers

to top

"In this session, we will discuss some of the common issues surrounding deploying Windows 2000 print servers. We will evaluate how to choose the correct printer drivers, we will discuss how to back up and migrate print servers, we will discuss point and print, and we will examine some interoperability issues."

Read more...

Download of the Week

WebCam2000

to top

OK, so you lost your job, your wife left you, and then your girlfriend left you. You post phony information about your income on the personals sites, and you spend every weekend with a DVD player watching "The Net" and thinking how great life used to be. What's the last step to prove you're a complete loser without a life? Get a WebCam and post pictures of yourself on a Web site automatically! I used to do this while between wives, and it's a great technique for getting people to feel sorry for you and offer to help you "get a life". If you're going to get a WebCam, make sure you use WebCam2000. Its FREE and it does the job.

Read more...

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 .