Windows Insider

35,000 Subscribers Worldwide

June 19, 2002
Issue #97

CramSession

CramSession StudyGuides InfoCenter Discussions SkillDrill Newsletters

Feature

Quick Start Guide to IIS Security

to top

Have you had a chance to work with Windows 2000's Internet Information Server 5.0? If not, you should take some time to get familiar with it. IIS is a key element in the Windows 2000 MCSE exams. Even if you don't plan to take any exams, you should take some time to learn about IIS so that you can take advantage of the Web services it provides.

Web services allow you to make information available to any user on the Internet. Web services provided by IIS 5.0 include:

- The HTTP (Web) service
- The FTP service
- The SMTP service
- The NNTP service

Each of these services allows you to share information with Internet (and intranet) users in different ways. This week we'll take a look at the IIS Web Service.

Basic Web Site Setup

The IIS Web Service (WWW or W3SVC) is the IIS HTTP server. You can use the IIS WWW service to host Web pages that are accessible via any browser. When IIS is installed on the Windows 2000 machine, two Web sites are created: the Default Web Site and the Administration Web site.

The default Web site is your starting place for creating a new Web. This Web site listens on all interfaces on TCP port 80. All you need to do to get a new Web started is to add your site's files in the Inetpub\wwwroot directory and then change the default document for the site for that directory to point to the home page for your site. The "default" default document for IIS directories is default.htm. If there is no default.htm file in the wwwroot directory, IIS will automatically search for a default.asp file. If there is neither a default.htm or default.asp file, IIS will use the built-in iisstart.asp file as the default document.

Once you place your files, you can access the Web by typing:

http://servername OR http://fully_qualified_domain_name.

You can use the Server name (NetBIOS name) on the intranet, but you'll need to use a FQDN for Internet host access. That means you'll have to setup at the very least, a Host (A) record that maps to an IP address that can be used to access your Web site.

If your Web server is a multihomed computer, and you want the Web site to listen on a single IP address instead of all interfaces, then you'll have to disable socket pooling. **Click here** for more information on how to disable IIS socket pooling.

Web Site Authentication

While setting up a new Web site is sheer simplicity when using IIS 5 (especially compared to Apache), you have to be careful that this simplicity doesn't create a security quagmire. Some things you should consider right out of the box is what type of Web you're going to run.

- Is the Web site publicly available?
- Is the Web site for a limited number of users?
- Do you need to encrypt data between Web client and server?

If your Web site is publicly available, you'll need to allow anonymous access. Anonymous access is secure in the respect that no user name and password information moves over the wire. This prevents malicious persons from using network sniffers to capture credentials that are sent to the Web server. While anonymous access keeps your user credentials secure, its does nothing to limit access to the data on the Web server.

Access control over data stored on the Web server can implemented using a number of different authentication protocols. These include:

- Basic Authentication
- Digest Authentication
- Integrated Windows Authentication
- Client Certificate Mappings

Basic authentication is the most compatible authentication method. All modern browsers support basic authentication. This authentication method passes through proxy servers like a hot knife through butter. The primary limitation of basic authentication is that credentials are passed in clear text. This allows anyone with a packet sniffer to plug into the local network segment and capture user name and password information. This limitation is eliminated by using SSL on all connections to the Web server.

Digest authentication is new with IIS 5. An advantage of this protocol is that it traverses firewalls and proxy servers without burping. However, digest authentication requires that the Web server belong to a Windows 2000 domain and that the Web client application be Internet Explorer 5.0 or above. Another problem with digest authentication is that you must store user passwords using reversible encryption. This is considered by some to be a security issue, so unless you have a compelling reason to use digest authentication, you might want to consider other alternatives.

Integrated authentication was available in IIS 4, but its meaning is expanded with IIS 5. If the clients and servers are members of a Windows 2000 domain, integrated authentication can mean Kerberos authentication. If Kerberos can't be used for some reason, then NTLM (aka NT Challenge/Response) authentication is used. Limitations of integrated authentication are that you must use Internet Explorer 2.0 and above, and that is won't pass through most proxy servers. However, if you use IE 5.5+ and ISA Server, you can pass Integrated authentication through your firewall/proxy.

Client certificate mappings are perhaps the most secure, but the more obscure method of securing Web site resources. Although its been a couple of years since Windows 2000 hits the streets, many Windows 2000 administrators still shy away from certificates and certificates services. Yes, the Windows 2000 Resource Kit documentation on certificate services reads like the Federal Register. But you don't have to set up a PKI to support the entire Solar System just to get a good basic certificate service infrastructure set up for your organization.

Client certificate mappings allow Web clients to present a client certificate as credentials to access a secure Web site. This obviates the need for user names and passwords moving over the wire. It can also prevent "reuse" of credentials by persons who shouldn't have access to said credentials.

Web Site Authorization

Access to resource requires more than just authentication. Authorization takes place after a user authenticates. IIS uses two methods for resource authorization:

1. IIS specific access controls
2. NTFS-based access controls

The IIS specific access controls are accessed through the IIS Management console. These IIS specific options control:

- Script source access
- Read access
- Write access
- Directory browsing

You can also limit access to Web site files using NTFS file system permissions. Note that the IIS specific controls will be evaluated before the NTFS permissions. For example, you might set NTFS permissions to allow Write access to a particular folder on the site, but if the IIS specific controls prohibit Write access, then write access will be ignored. However, if IIS is configured to allow Write access, but NTFS permission allow only Read access, then only read access will be allowed. NTFS permissions allow more granular, user/group based access controls.

Summary

In this quick-start guide on IIS security, we covered basic Web site setup, IIS authentication, and authorization. With these basics, you can start your jump into IIS and start your IIS test lab and really dive into the application.

Securing IIS can be thought of as a "weird science". The reason for this is that you never know what security configuration is going to break your Web sites. The biggest problem is that documentation is either lacking or vague about how you should secure the files located on your Web servers so that Internet criminals can't destroy what you've taken so long to create. The only solution is to test each security configuration in a lab setup *before* you actually roll it out on a production network.

A great place to start learning about IIS security is to use the IIS Lockdown tool and URLScan. You get both of these applications when you install and run the IIS Lockdown tool on your IIS 5 machine. **Click here to check them out.**

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.
I have a very weird problem. For about 1 year now I have used Win2K Advanced Server as my "workstation" OS, with which I am very happy. The problem is that I now need RRAS to work for me. Every time I try to open the RRAS MMC I see the server with a green arrow (yep, the service is running hapilly) but when I double click on it, it pops a message saying that I don't have the appropriate permissions to view the properties (also the server from green arrow gets a red X . I double checked NTFS permissions, svc dependencies, everything. The message still keeps popping up. I really need RRAS without reinstalling the OS.
Thank you in advance...
--DisMan

Uncle Bill says:

Yo DisMan. Looks like you're the victim of a security expert. Did anyone suggest to you that you should disable the Remote Registry Service? If so, check out whether this service is running. If not, enable it. You won't be able to run the RRAS console properly unless the Remote Registry Service is running.

Question:

Hi, Uncle Bill
We have a standalone Win2K server in our workgroup environment. Can one "upgrade" it to become a DC for a new domain, even if there isn't any existing domain structure? If so, how? If not, grrrrr....
--Poseidon33

Uncle Bill says:

Hey Poseidon! You bet! Just open the Run command and type dcpromo in the Open text box. Click OK and away you go! I've got one suggestion for you, though. Make sure you create your DNS zone *before* you run dcpromo. That was you avoid the dreaded Active Directory Wizard's DNS server configuration routine. Good luck!

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 Gopher Protocol Handler Can Run Code of Attacker's Choice

to top

There is an unchecked buffer in a piece of code which handles the response from Gopher servers. This code is used independently in IE, ISA, and Proxy Server. A security vulnerability results because it is possible for an attacker to attempt to exploit this flaw by mounting a buffer overrun attack through a specially crafted server response. If you use Internet Explorer, Proxy Server 2.0 or ISA Server, you need this fix. SEVERITY: Critical

Read more...

Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise

▲ to top

This one involves a buffer overrun in the Chunked Encoding data transfer mechanism in IIS 4.0 and 5.0, and could be used to overrun heap memory on the system, with the result of either causing the IIS service to fail or allowing code to be run on the server. SEVERITY: Moderate

Read more...

Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution

▲ to top

A flaw exists in the RAS phonebook implementation: a phonebook value is not properly checked, and is susceptible to a buffer overrun. The overrun could be exploited for either of two purposes: causing a system failure, or running code on the system with Local System privileges. A successful attack will allow the malicious user system privileges. SEVERITY: Critical

Read more...

Unchecked Buffer in SQLXML Could Lead to Code Execution

▲ to top

Two vulnerabilities exist in SQLXML: An unchecked buffer vulnerability in an ISAPI extension that could, in the worst case, allow an attacker to run code of their choice on the Microsoft Internet Information Services (IIS) Server; and a vulnerability in a function specifying an XML tag that could allow an attacker to run script on the user's computer with higher privilege. For example, a script might be able to be run in the Intranet Zone instead of the Internet Zone. SEVERITY: Moderate

Read more...

News Headlines and Resources

How Video Cards Take Data From Processor To Screen

▲ to top

Ever wonder how your computer is able to take zeros and ones and turn them into the miracle of the graphical interface? If so, you might want to take a look at this article by Deb Shinder. She covers the basics of how your video card does its tricks.

Read more...

You Cannot Access Protected Data After You Change Your Password

▲ to top

Looks like there's a flaw in how the EFS file encryption system works. The Q article has a rather bizarre explanation as to what the cause of the problem is. However, it looks bad enough that you probably should get a fix, especially if you're using EFS in your organization.

Read more...

RASPPPOE Available for Windows 2000

▲ to top

If you have a dreaded DSL PPPoE connection, you're probably using the sludgeware provided by your ISP. Why not try a true Windows 2000 PPPoE implementation that was designed for Windows 2000? Best of all, its freeware. This is the best PPPoE implementation you can get!

Read more...

Updated Exam Guides for MCSA Exams

▲ to top

Microsoft has published a couple of new exam guides for the 70-210 and 70-215 (Win2K Professional and Server) exams. Don't get your hopes up. The exam objectives don't match the actual exams any more than they did before. But, they do a nice sales job for Microsoft training and instructional materials.

Read more...

Windows 2000 Troubleshooting Best Practices

▲ to top

The network admin's bread and butter is solving problems. No problems, no job. To fix problems you need excellent troubleshooting skills! Check out this article on 9 Windows 2000 troubleshooting best practices to keep those skills sharp.

Read more...

Online Event: Publishing Servers with ISA Server

▲ to top

Are you wrestling with ISA Server Web and Server Publishing Rules? Need to learn the tricks and traps of ISA Server publishing? Then come listen to me talk about how to get ahead of ISA Server when it comes to ISA Server publishing. Pencil me in on your calendar for June 27th.

Read more...

Support WebCast - Microsoft Windows Messenger for Windows XP: New Features, Common Issues, and Troubleshooting

▲ to top

In this session, you will learn about common issues that users may face and how to troubleshoot and resolve these issues. You will hear about the new features of Windows Messenger that help make the user experience more enjoyable.

Read more...

Download of the Week

FreeRAM XP Pro 1.1

▲ to top

Do you find your workstation gets sluggish by the end of the day? Need more pep for your RAM hungry games? Then what you need is a RAM optimization tool. Try out FreeRAM XP Pro 1.1. This product does the job and you can't beat the prices: FREE. But send the developer 5 bucks just to say thanks for a well-done program.

Read more...

Get the skills, knowledge and credentials you need to excel in your career by attending University of Phoenix Online. Our curriculum is one of the most up-to-date and relevant available anywhere – including degree programs in accounting, marketing, nursing, education, information technology, business, management, and more. The curriculum is continually updated to provide the skills and expertise in high demand.

Click here to learn more!

Free Cramsession IT Newsletters - Choose Your Topics!

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

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

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.