Net Admin Weekly
55,000 Subscribers Worldwide
October 16, 2002
Issue #13

Feature

Q & A

Security Advisories

News Headlines & Resources

Download of the Week

Feature

Implementing Broadband Security

to top

Broadband – everybody wants it, and more and more homes and businesses are finally getting it. Broadband Internet access is all the rage, and with good reason. It has two very appealing qualities: it's fast and it's cheap. Once upon a time, if you wanted high speed 'Net connectivity, you had to shell out thousands of dollars per month for a T-1 line. Today, in many areas, you can get cable modem access through your CATV company or DSL from the phone company that gives you at least the equivalent speed of T-1 (1.44Mbps) at a fraction of the cost.

Of course, T-1 still has some advantages, such as a Service Level Agreement that guarantees uptime and bandwidth, and T-1 itself costs far less than it did just a few years ago. Now full T-1 lines, including local loop and ISP service, can be had for under $400 per month. That still seems pretty expensive when compared to all those cable and DSL users who pay $35 to $80 per month for their service. And speed isn't the only great feature that consumer broadband shares with T-carrier service. The "always on" characteristic is another reason computer users are switching from analog dialup.

Unfortunately, there is a down side to all of this. Broadband technologies have opened up new possibilities for Internet users, such as video conferencing, audio streaming, and other high bandwidth applications. But these features have also opened up their systems to increased vulnerability to hack attacks. In this article, we'll explore why that is, and what you can do about it.

The Trouble with Broadband

What makes a broadband connection less secure than a regular modem connection? There are several security issues involved with high speed, low cost, always-on connections. The first problem is the 24/7 nature of the connection. Back when users had to manually initiate a connection in order to surf the Web or download their email, their systems were offline a good deal of the time. After you hang up the phone, you're no longer on the network, and thus no longer vulnerable to attack.

Crackers often need time to get into your computer, especially if they're relying on brute force or dictionary attacks to guess your password. Removing the computers from the Internet when not in use helped to prevent this.

A second aspect of this always-connected issue is the IP address assigned to a system. With dial-up modem connectivity, a PC is usually configured to use DHCP to obtain its IP address, and is assigned a different address each time the connection is established. Thus, a modem-connected PC that has one address today will usually have a different address tomorrow, and the address it used yesterday will be assigned to a different system today. This makes tracking individual systems difficult. However, with broadband connectivity, systems are often assigned a dedicated IP address, or are able to continually renew their DHCP-assigned IP addresses so their online identifiers remain consistent over a long period of time (if not indefinitely). This makes

tracking (and hacking) a specific system extremely easy.

The longer a system remains online, especially when it retains the same IP address, the more vulnerable that system is to repeated brute force and port scanning attacks. Given enough time, every system can be breached, even if security-conscious administrators have taken standard precautions such as deploying a firewall, installing patches, and assigning strong passwords. Remember, security is a deterrent—it is not an impenetrable barrier. Given enough time and determination, any security measure can be breached.

How to Implement Broadband Security

Simply powering down the computers when not in use isn't enough to protect against these threats. Through the power of automation, crackers can continuously scan an IP address to determine when the computer is on or off. Yes, it is possible to prevent the attack from progressing while the PC is powered down, but the attack can resume right where it left off once the system boots back up. Instead of relying on "security through obscurity" (attempting to hide the existence of a system or data from an attacker), there are numerous proactive steps you can take to reduce your vulnerability to broadband-specific attacks.

1) Deploy anti-virus software of your choice to protect your system from malicious code that can be sent to you via email or downloaded without your knowledge from a website running scripts or Active-X controls.

2) Define strong user passwords to protect from crackers. Passwords should consist of alphabetic, numeric, and symbol characters; should not be words that are in the dictionary; and should be of sufficient length (at least 8 characters) to make guessing difficult.

3) Use an operating system that allows you to set access permissions on files, folders and other objects. Windows NT/2000/XP are far preferable to Windows 9x because the former allow you to use file-level permissions on NTFS-formatted partitions.

4) Disable file and printer sharing (Server service on NT machines) if your broadband-connected computer doesn't need it for sharing files on a LAN. If it is needed for that purpose, unbind the service from the broadband connection network adapter and bind it only to the NIC that connects to your internal local network.

5) Use Network Address Translation (NAT) to share a broadband connection between multiple computers on a home LAN, rather than having each one assigned a public IP address and going through a router. This hides the internal addresses from the Internet.

6) Use a firewall to protect the broadband-connected computer and any other systems on the LAN from unauthorized access from the Internet. Available firewalls range from free or shareware downloads, to inexpensive consumer-oriented products, to expensive software firewalls such as Microsoft's ISA Server, to hardware firewalls such as Cisco's PIX.

Windows XP even comes with a built-in (albeit rudimentary) firewall.

7) Disable unneeded services, protocols, and applications through which your system may be exposed to hackers.

8) Configure system auditing so that if security is breached (or if an unsuccessful attempt is made), you'll be aware of it and can take added precautions.

9) Install operating system and application patches and security updates to ensure that security "holes" left in these programs by developers will be plugged, and can't be exploited to give hackers access to your system. Be sure your email client and web browser software are configured for best security.

Summary

The growing availability of broadband technologies is great for consumers—but carries with it some hidden dangers. Broadband connectivity makes your system and LAN more vulnerable to hackers, crackers, and network attackers than when you were poking along in the slow lane, using your 56Kbps modem. However, there are steps you can take to make your broadband-connected systems more secure. If you have a cable or DSL connection, take a moment to go through our checklist and ensure that you're doing all you can to protect your system from those who might want to snoop or have a little "fun" at your expense.

This week's feature article by
Deb Shinder, MCSE, etc.
Net Admin Weekly Editor
deb@shinder.net

Q & A

Mystery of the Missing Web Page

to top

Question:

Hi Dr. Tom,

In IIS Manager 5.0, I created a new Web site, made sure that the service was started for it, configured the port on my router, and created a simple web page "Hi can you see this web page" for example. The thing is I can't get to this page through my intranet (192.168.1.20 is the server's IP). Am I missing something? Where should I put the file so that 192.168.1.20 shows my simple web page? -–Mike

Answer:

Hey Mike! I'm going to assume that IIS is installed and the WWW service and the Web site are started. The most likely reason for this is that you don't have your new page set up as the "default document". For

example, suppose you created a new page and named it "newpage.htm". If you placed that page in the default Web root \Inetpub\wwwroot and typed in the http://servername/ the page would not automatically show up. Why? Because the path is incomplete. You didn't type in the name of the file, so the Web server serves up the default document. IIS includes three default document entries – iisstart.asp, default.asp and default.htm. You can find these entries on the "Documents" tab in the Web site's Properties dialog box. The solution is to either add your new page to the default documents list, or rename the page to one of the default document names already listed. Or, you could type in the full path to the page: http://servername/newpage.htm.

Secure FTP Site Access

to top

Question:

Dear Dr. Tom,

We run an FTP site on our network that we use to allow traveling employees access to confidential data. The employees have no problem accessing the FTP site, but someone recently brought up the concern that the data moving from the FTP site to the client computer over the Internet is "in the clear". If someone was to put a sniffer on the network or at the perimeter, they would be able to access the data with very little trouble. We're using IIS 5.0 for the FTP site. We've locked down access using NTFS permissions, but that doesn't do anything for us once the data is "lifted" off the disk and onto the wire. Do you have any suggestions? –-Insecure FTP Admin

Answer:

Hey Insecure, you do have some problems. FTP is one of the most unsecure network applications around. Getting FTP to work in a secure fashion through a firewall is an even bigger nightmare! Vendors like **GlubTech** and **IPSwitch** provide secure FTP servers and clients. The problem with these solutions is they are a bear to work with through firewalls, and they require alterations in the client and server environment.

My favorite secure FTP fix is ISA Server and Web Publishing Rules. ISA Server allows you to publish FTP Servers on the internal network so that external users can use HTTP requests to get the data. The HTTP request is forwarded as an FTP request from the ISA Server to the internal network FTP server. The FTP server sends the data to the ISA Server, and the ISA Server forwards it back to the HTTP client (Web browser). The cool thing is that you can force the client to use HTTPS (SSL) connections to connect to the ISA Server and get the FTP data! The information is protected in an SSL tunnel between the client and the ISA Server.

The only drawback to this method is that the data is not secured by SSL when moving between the internal interface of the ISA Server and the FTP server. If you need this kind of end-to-end security, you can use one of the 3rd-party solutions, or allow users to download via HTTP instead

of FTP. You can configure the ISA Server to create a second SSL tunnel between the ISA Server's internal interface and the Web server on the internal network. This allows end-to-end security for your data. For details on these configurations, check out "**ISA Server and Beyond**".

Security Advisories

Flaw Discovered in Outlook Express Patch

to top

Last week Microsoft released a patch to fix a security flaw in Outlook Express. The fix was included in the IE 6.0 SP1 update and also in Windows XP Service Pack 1, but you also had the option of installing the standalone patch. The problem is that the patch gives a false error message when you try to install it! Check out the article for details.

Read more...

Spammer Gets Beat Down in Court

to top

A spammer recently sued the owner of the SPEWS.org RBL. While I'm definitely no friend of RBLs, it sounds like these guys are pretty nasty spammers. They claimed that the blacklisting cost them over $40K US, including $14K US to change IP addresses! Amazing they weren't held in contempt for lying about the cost of IP addresses <g>

Read more...

OpenOffice Installation Vulnerability

to top

It was just a matter of time. With OpenOffice becoming more and more popular, there just had to be something found wrong with it. Turns out there's a security problem related to how temporary files are created during OpenOffice installation. There aren't any vendor-based fixes, but there is a workaround.

Read more...

News Headlines and Resources

Stegano--what?

to top

Have you heard about hiding information inside graphics files? The method used to hide info in a graphics file is called Steganography. Your internal network users could be hiding trade secrets in graphics files and sending them to competitors! Check out this article by Joern Wettern and learn how bad guys can use Steganography to get around your network security policy.

Read more...

Microsoft Events and Errors Message Center

to top

You know what its like; everything seems to be working fine and then POW! The application stops working. The good news is an error was reported to the Event Log. The bad news is you can't find any

information on that error! Microsoft has heard your cries. Check out their Events and Errors Message Center. It's free and it works.

Read more...

IPSec NAT Traversal Overview

to top

OK, you know its nuts from a security point of view to allow someone to VPN into an untrusted network from your network, but the boss says to allow the contractor access to his home network. Your job is more important than company network security. The problem is the contractor needs to use L2TP/IPSec and you have a NAT device between your network and the Internet. IPSec NAT Traversal can fix this problem. If you don't know about NAT traversal, then you need to check out this article.

Read more...

Maxtor Personal Storage 5000XT

to top

I know a lot of you use VMware to run your network labs. VMware allows you to create an entire lab on one machine, but disk space is always an issue. If those VMs are taking up all your space, then check out this hard drive MONSTER! The 5000XT gives you 250 GB of Firewire or USB 2.0 storage. 7200 RPM, 9ms seek time, and a 2 MB buffer all in the box. This drive will allow you to store more VMs than ever!

Read more...

IIS Lockdown Tool Update – Version 2.1 Now Available

to top

If you run IIS Web services for public or private access, you know that the IIS Lockdown Tool is your best friend. This key security tool has been upgraded to version 2.1, and includes new server roles that support almost all of Microsoft's server products. IIS Lockdown also includes URLScan; when you run a template, URLScan will be automatically configured!

Read more...

Inside the Windows 2003 Encrypting File System

to top

If you use Windows 2000, you probably have worked with the Encrypting File System (EFS). Chances are the when you move up to Windows 2003 that you'll want to continue to use it. Be aware that EFS doesn't work exactly the same in Windows XP and Windows 2003! Check out this article for all the details.

Read more...

Support WebCast - Windows .NET Server 2003: Upgrading, Migrating, and Restructuring Windows Domains

to top

Thinking about upgrading your aging Windows NT 4.0 Domain to Windows 2003 Active Directory? Then this Webcast is for you! In the talk they'll describe methods for migration and restructuring so that your Windows 2003 Active Directory upgrade goes as smoothly as possible.

Read more...

Download of the Week

TDIMon

to top

Here's a very cool tool that let's you know what services are using what ports to connect to network resources. The TDIMon appl allows you to check up on all TCP and UDP activity on your system. If you've ever run netstat –na from the command prompt, you might have wondered what local services are connecting to other hosts on the network. Never wonder again! TDIMon will tell you exactly what service is doing what to whom. Best of all, this powerful utility is FREE! A definite "must-have" for any network admin.

Read more...

Free Cramsession IT Newsletters - Choose Your Topics!

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

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