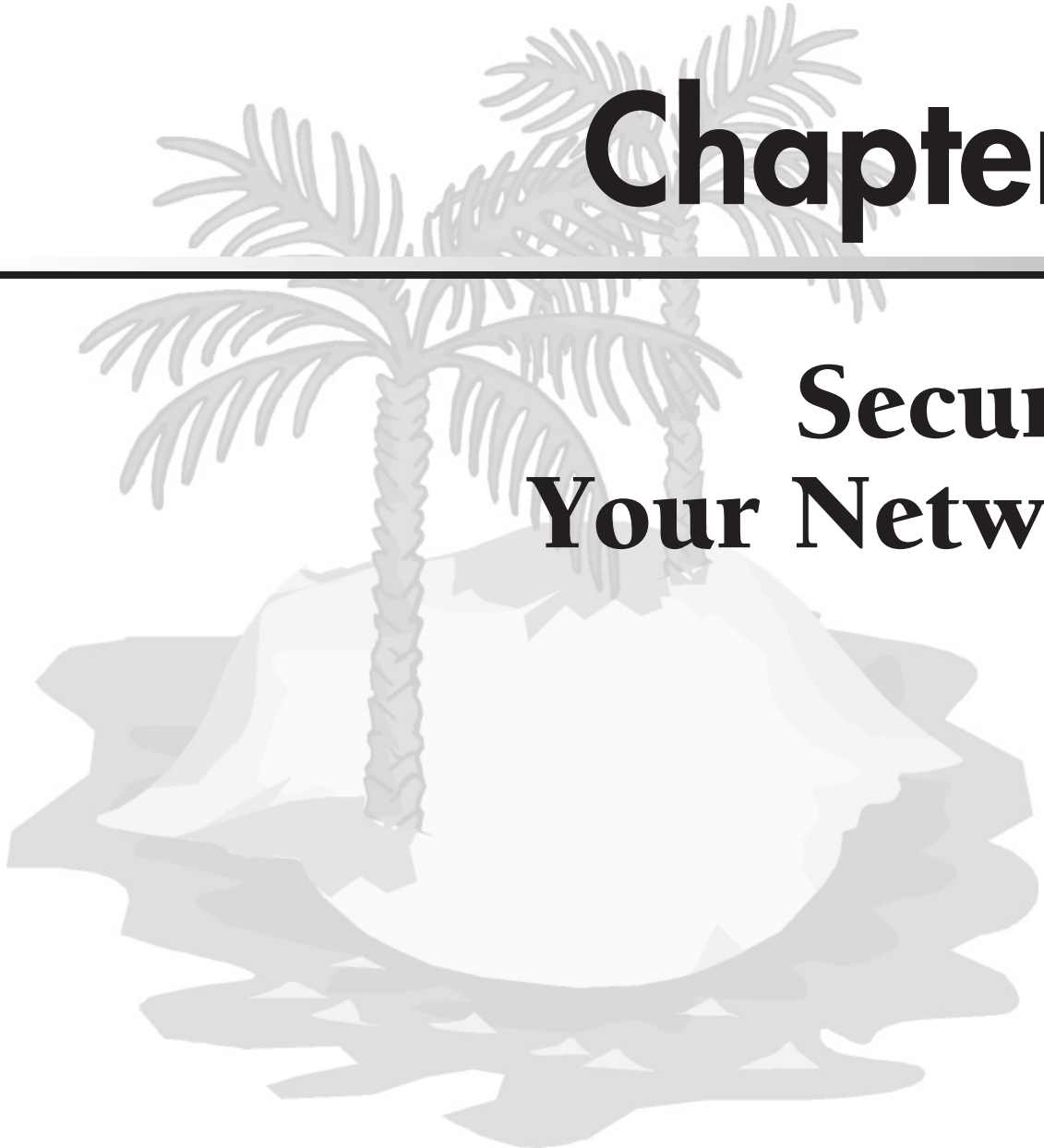


Chapter 6

Securing Your Network

2 Home Networking Survival Guide

So far, our discussions have focused on building your network step by step, from the basic wiring and operating systems support for networking to rudimentary applications. If you have been following along and implementing my suggestions, you have a working network, are doing all sorts of fun things on it, and are enjoying the high-speed connection to the Internet. It is time to get a little more serious and start to tighten things up.

If you have ever had a break-in or been robbed, you know how important it is to protect our homes and families. The sense of personal violation is strong, you feel stupid for it having happened, and you vow to strengthen your protective measures and to improve locking down your doors and other entry points.

While it is relatively easy to protect our homes from physical entry, the same isn't true when it comes to protecting our home networks from potential break-ins. It is harder for us to understand the nature of a break-in, to detect such intrusions, and to prevent further attacks. It isn't as if we were to come home one evening and find the computer missing from the den—computer break-ins are far more subtle and involve more complicated situations than the mere removal of our physical property.

Problems

At the heart of the problem of securing your data is a simple fact: Your computer is now connected to the Internet whenever you turn it on, thanks to all of the hard work you did by following my directions thus far. Your always-on connection gives thieves and mischief-makers an opportunity to commit mayhem with your files. Why? A connected computer is a lot harder to protect.

NOTE

The best way to secure your PC is to keep it off any network, and to not hook it up to the Internet or any other communications network.[1] Once your computers are part of the Internet, they can come into contact with other computers run by people who can try to compromise your programs and data.

Some people spend their lives on the Internet trying to damage others' computers. They develop computer programs that poke and prod until they find someone who has left his or her PC defenseless or weak. They develop new programs that can enter your computer via seemingly innocent e-mail attachments. They use other computers, typically at universities and government research labs that have little or no security measures, to try to attack your computers, making their efforts harder to track down and prevent. Even if you do everything in your power to try to

1 If you want to take things to extremes, the only truly secure computer is one that is powered off.

stop these people and programs from entering into your system, the people you know and work with every day can still harm you. These people can unknowingly attack your system on behalf of the bad guys by forwarding harmful e-mails and other programs.

This is happening every hour of every day, 365 days a year. It is happening while you sleep and while you get up from your machine to get a cup of coffee.

You may think I exaggerate these threats, but consider that scarcely a week goes by without reports of a new virus being discovered by some hapless user, who inadvertently has spread it to hundreds of his or her closest friends. Reports of various Web site break-ins or of graffiti writing over legitimate pages on the site are almost as frequent. Those are the incidents that we hear about—numerous others happen without any fanfare.

Threats from E-Mail Attachments

There are basically three types of threats that you should be aware of. The first and probably biggest threat is receiving a virus or worm or some other program via an e-mail attachment. Since e-mail has become such a universal communications tool, the threat of virus infection is quite real. I don't know anyone who has escaped being infected by a virus. It has happened to me, and I am very careful about the messages that I open and how I go about my day-to-day business.

For our purposes, we don't have to differentiate among these programs—all of them can harm your system and need to be stopped before they enter your network. All of them destroy parts of your system, some more important and harder to recover than others. The differences are in how they enter our network and how they go about their dirty business.[2]

Sometimes these infected e-mail messages arrive with pretty innocent-sounding subject lines, such as "in reference to your e-mail" or "please check out this homepage." Sometimes they have spiced up the subject lines with promises of lurid porn or making money fast or other come-ons that rarely, if ever, deliver. (Indeed, as I was finishing this chapter I got one of those messages, talking about Snow White. Jeez!)

Sometimes the e-mail messages are from your usual correspondents: they have been infected, and the virus rips through their address books, sending out e-mails to everyone in them. If you aren't a suspicious person, or if you are new to e-mail, then I have to warn you that this sort of thing happens every day. It happened to me, and I sent a virus to a neighbor. This virus clogged up their entire corporate e-mail system so badly that the company had to shut it down before they could clean it out. All because of one message that I sent with the virus attached.

2 For a complete discussion about various threats and how to tell their differences, see the Practically Networked page (http://www.practicallynetworked.com/sharing/securitythreats.htm).

The biggest opportunity for virus authors is Microsoft products, which are the products most of us use. The Windows versions of Microsoft Outlook and Outlook Express in particular are extremely easy to use as virus culture media. Think of them as the virtual equivalent of a piece of ripe fruit, attracting all sorts of insect life. These two pieces of software are often the focus of virus authors and can quickly send a copy of some nasty program to friends in your address book. They are also extremely difficult to lock down to prevent virus infections.

Why did I recommend Outlook and Outlook Express in the last chapter? The additional features are worth the risks, but you still need to protect yourself.

Here's why these programs are so risky. Microsoft has designed Outlook/Outlook Express to work effortlessly with a series of programs, in the hopes of making it easier to integrate e-mail with a wide variety of applications. While they have succeeded in this design, they also have succeeded in making it easier for virus authors to integrate their mischief into a wide variety of applications, such as a program automatically e-mailing everyone in my Outlook address book a copy of a virus.

The problems aren't limited to Outlook. Even if you use a Mac or some other e-mail program, you are still at risk. E-mail programs are set up to make it easier for you to use them, and one of the worst things as far as security is concerned is to automatically run programs associated with particular kinds of files.[3]

In the old days, before Windows 95, say, it was harder to use your e-mail system because you had to know the type of program that created a particular file that you received as an e-mail attachment. Now you can click on an attachment, and the operating system will bring up the software it thinks you need to view your file. That is exactly the kind of feature that virus writers play into, and why receiving e-mail attachments is generally not a good idea.

There's no good way to eliminate attachments from our lives. For a few weeks, I set up my copy of Outlook to automatically reject any e-mail messages that contained attachments. That wasn't realistic and vexed some of my correspondents when they received the rejection message. You can set up more complex screening techniques and filters, but many viruses come from people you know and want to communicate with, so these filters don't really help. You can convert all your e-mail over to a host-based system such as Yahoo Mail, which includes virus screening as part of its service, but that isn't practical if you already have another e-mail address that people know you by. Your choice is limited to using an antivirus program that can check your e-mail somewhere in the process and eliminate any problems before they creep into your computer.

3 You can break the connection between the type of file and the associated program that will automatically open it, to give you a running start in fighting these types of viruses. However, doing this properly will take lots of work. See Appendix B for more information.

Threats from Microsoft Office Users

E-mail attachments aren't the only security problems. Microsoft Office contains a wide array of small executable programs that go by various names, including macros, templates, and scripts. All of these have been exploited by the bad guys to wreak havoc on unsuspecting users' systems. Also, all of these can easily and sometimes inadvertently be transmitted via e-mail or other Internet communications, including instant messages and Web site visits.

Suppose you are collaborating with someone on a series of presentations, documents, or spreadsheets and are sending them back and forth via e-mail. (Such is the process by which this book was created, for example.) If one of your correspondents has lax security, they could infect your machine with one of these virus files quite easily. Or they could mess up your default settings for your documents to the point where you could spend several hours trying to restore the original settings.

Some nasty people out there create these awful programs. Sometimes people create viruses inadvertently, as a result of a programming project gone wrong that destroys large amounts of data. Either way, you can do nothing about it. We will continue to see their work proliferate on the Internet. As the various means to protect your PCs increase, these people will figure out new ways to circumvent them and new ways to design viruses and worms. That doesn't mean you have to give up hope. You need to get the right set of tools and be better prepared.

The first thing you need to do is obtain an antivirus screening program. Make sure that it is installed and kept up to date on every computer on your home network. I mean each one. You need to do it now. To delay by even a day is to put your household's computers at risk of infection. Some virus screeners are free, while most just cost a few dollars. I'll get into this in the "Solutions" section and give you tips on how to maintain these products, because that is even a bigger commitment than just buying and installing the software.

CAUTION

Virus authors have gotten cleverer as time goes on. In May 2001, I heard about a virus that looks like a message from Symantec. The message tells you about a new virus their research team has discovered. It comes via an e-mail message with the subject line "FW: Symantec Anti-Virus Warning" and claims to contain a description of a nonexistent worm in an attached file named www.symantec.com.vbs. The message, of course, is not from Symantec, and it does contain a virus! As if you didn't have enough to worry about. A list of other hoaxes can be found at Network Associates' Web site: (http://vil.nai.com/VIL/hoaxes.asp).

E-mail-borne viruses are just one means of infection. A second "disease vector" (as epidemiologists would call it) for viruses is via floppy and Zip disks that are moved from

computer to computer. If you bring work home from your office on a disk, and then place the disk into your home computer and copy these files, you are at risk on both machines of transferring a virus between your home and work networks.

I have numerous computers in my office, including many that I use only for testing and run infrequently. Over the years I got lazy and didn't install any virus screening programs on some of the test machines. This was mainly because I didn't use them for extended periods or because I just didn't feel like going through all the motions to get the antivirus stuff set up. This was a mistake. One day I found all my boot floppies that I use to create new operating systems were infected with a virus. The virus wasn't particularly destructive (otherwise I would have found it sooner), but it was annoying to have to go through all my floppy disks and clean them. I also had to install the current version of the antivirus software on all of my machines and make sure that all the virus files were deleted from every machine. Just one floppy, one instance where you drop your guard, can be enough to infect your entire home network and potentially your work network.

This is one reason that many businesses have given up on floppy or Zip or other removable disks, although if you have a CD burner at home, it is also possible to inadvertently place a virus on it and then infect other computers. (Microsoft and several other software vendors have had this happen to some of their beta copies of their production software, much to their collective chagrin.)

Have I convinced you yet to install an antivirus scanner? I hope so. Of course, you still need to set it up properly and make sure floppies and Zip disks are scanned upon insertion, otherwise the best scanner in the world won't help you.

Threats from Visiting Web Sites

The antivirus programs can do only so much, because a third means of infection exists. Being connected to the Internet with your computer is enough to get you into trouble. Even if you turn your computer on and do nothing else—receive no e-mails, go to no Web sites, do absolutely nothing other than supply power to the box and have it running with some kind of Internet connection—your computer is at risk. This is perhaps the scariest part because the dirty business happens completely independently of what you are doing and is hidden to you as an everyday user of your computer.[4]

4 This risk is the same for people who use dial-up connections. I have seen reports that users who spend large blocks of time on dial-up lines can become victims of attacks.

NOTE

You are also at risk whenever you visit a Web site. We can thank Microsoft for this last security wrinkle. As a feature to their Internet Explorer browser, they developed the security cesspools called Active Content and ActiveX. This is content that can add all sorts of excitement to ordinary Web pages, including animation, updates from databases, and other visual tricks. However, it can contain malicious programs that can be automatically run on your computer, without any intervention or action on your part other than visiting the particular Web page where the content is stored. This means that your computer is at risk merely because you view a particular Web page—and you don't have any prior warning when you are going around the Web innocently surfing.

If you took my advice in Chapter 2 and enabled file sharing on one or more of your Windows or Macintosh computers, you might be at risk because this opens up your machine so that others can view your shared files, even others that are out on the Internet and halfway around the world from your humble home. I'll have more to say on how to set this up properly. Chances are good if you are using a frhub that these file sharing network broadcasts are being blocked by your frhub and that no one else outside of your home can see them. Chances are also good that if you aren't using a frhub, you are in deep trouble and need to fix that situation, pronto.

Even if you haven't turned on file sharing on any of your computers, you are still at some level of risk. Security consultants report that their machines are constantly being scanned by potentially malicious programs doing the computer equivalent of rattling their door locks to see if these programs can gain access to the machine's resources. These consultants have tuned their PCs to report on these intrusions and are experts at detecting and repelling these invasions. You are probably not an expert at either and may wonder, why you? What does your modest and unknown home network have to offer these people?

Being scanned is a democratic process. It happens to everyone, whether you are a small two-PC home network or a large corporation with hundreds of Web servers and networked computers. The scanners don't necessarily target their dirty work at anyone in particular. Some people develop programs to exploit particular operating system vulnerabilities. Some are looking for Web servers that have unprotected back doors or other easy entry points. Some just set up their programs to run through a particular range of IP addresses that happen to be located nearby or across the world.

Understanding IP Network Traces

What are these scanning programs actually doing? Recall that in my discussions about IP networks, I mentioned that every computer that is connected to the Internet must have a unique IP address. Each IP address is usually part of a range of addresses that are owned by

your ISP or that bear some relation to your employer's network or some other identifying information. (Or, if you are using a frhub, they are a private range of IP addresses from your DHCP server.) Think of it as a listed phone number, only the way the phone numbers are given out, bears some special meaning. Just as there are reverse phone directories, where you can locate someone's postal address if they have a listed phone number, you can do the same with an IP address and find out what network a person is connected to and who is their ISP.

Let's try it now. If you are running Windows, bring up a command window and type the following command: **`tracert yahoo.com`**. (Note the space and press ENTER after you type in the command.) If you are running a Mac, you should have downloaded WhatRoute from our discussions in Chapter 2.

You are asking your computer to tell you how data gets transmitted from your computer to Yahoo's main servers, and all the places along the way these packets are routed. You'll notice a series of lines that look something like this:

```
Tracing route to yahoo.com [216.115.108.243] over a maximum of 30 hops:
1    80 ms    80 ms    70 ms  pos1-0.core2.mcl.cais.net [63.216.0.14]
2    30 ms    40 ms    30 ms  208.49.231.5
3   100 ms    91 ms   100 ms  pos7-0-2488M.cr2.SNV.gblx.net [208.50.169.86]
4    90 ms   100 ms   101 ms  206.132.254.41
5   101 ms    90 ms    90 ms  bas1r-ge3-0-hr8.snv.yahoo.com [208.178.103.62]
6   100 ms   100 ms    91 ms  img3.yahoo.com [216.115.108.243]
```

Each of these lines shows you the time (in milliseconds) it takes for the packets to get to this point, the name of the router, and its IP address. You can see on line 3 that Yahoo's data at this moment goes through gblx.net. You can also see that the Internet thinks Yahoo.com is located at the IP address of 216.115.108.243.

Once you know the IP address, you are practically inside their computer. Now you need to know what programs they are running and whether they have any open doors that you can enter. Your computer also runs a bunch of programs as part of its operating system. No matter whether you run Windows, MacOS, Linux, or OS/2, your computer uses a series of port numbers to handle its day-to-day business. These port numbers are the way your computer distinguishes various applications and keeps them from getting in each other's way.

Remember how I showed you in Chapter 5 how to turn off AOL's Instant Messaging software by blocking port 5190? A lot more port numbers are out there.

These port numbers are also markers for what is available on your system that can be exploited by hackers. They include numbers for well-known applications, such as Web servers (port 80), e-mail servers (ports 25 and 110), our friendly AOL IM (5190), and other

tasks. They are also for more obscure things, such as the port to run particular network-based games. Napster's port number is 6699. Any malicious programmers know these ports and know how to examine your computer to see whether they can get inside.

CAUTION If someone can figure out your IP address and which ports are open on your machine, they know where you live and what you do and how your computer is vulnerable. They will know what kinds of applications you have running and whether they can access any of them and do some damage.

You don't have to be a server to be vulnerable. For example, if you load Windows Peer Web Services in Windows 98/Me, you may be exposed to attacks coming in over port 80. Even though it goes by some fancy name, this is still a Web server as far as some anonymous hacker is concerned.

Anyone can easily obtain a list of these port numbers. In fact, they are part of the Internet standards process. When someone wants to reserve a port number for their particular application, they have to file a registration document with the appropriate Internet standards-keepers. You can view a complete list of the known ports at the IANA Web site (http://www.iana.org/assignments/port-numbers).

Scan Your Ports

Am I getting through to you yet? Do you think that these are scare tactics, that it can't happen to you? Let's do some analysis of your particular situation with a few simple test tools. I hope to convince you. My aim is to motivate you into acting to protect your network to the strongest extent possible. Part of being security-conscious is understanding the level of the threat against you, and then being able to harden your defenses with the appropriate tools and techniques.

Let's start with a simple port scan of your computer, care of Steve Gibson's Shields UP! service. This simple tool addresses the issue of what parts of your computers are vulnerable to attack. Go now to his Web site, http://grc.com, and click on the graphic for that program. You will see lots of information about what it does and how to proceed through its tests. There are two buttons to click on; choose Probe My Ports, and in a few minutes you will have the results of its analysis.

You'll notice that the first thing Shields UP! tells you is the IP address that your computer is using to connect to the Internet. If you have already installed a frhub as I instructed you to do in Chapter 4, then this IP will actually be the address of the frhub and not your individual machine. More on this in a moment.

Shields UP! examines each of the popular application ports and tries to connect to them, the way a bad guy's program would try to do so over the Internet. When the program tests each port, several possible outcomes can result:

- **Open** This means that the port is wide open and can be exploited by hackers. The trouble is, the more stuff you run on your computer, the more likely you have opened ports available for hackers to exploit.
- **Stealth** This means that Shields UP! didn't detect anything going on with this port. This is the best circumstance you can hope for. You want to hide as much as possible about your computer from outsiders, and the best way to do this is as if the port doesn't exist on your computer.
- **Closed** This means that the port and the application that uses this port have been detected by Shields UP!, but that the program couldn't obtain access to it. This is almost as good as Stealth, and better than having any of your ports wide open.

Ideally, you should run Shields UP! on every computer in your home that is connected to the Internet. More than just telling you if someone has left a back door to your system unlocked, Shields UP! also tells you what to do about it—how you can secure your system and keep your assets protected. Gibson has provided lots of advice on how to correct the problems Shields UP! discovers. This advice is actually more important than doing the tests themselves, because it will get you thinking about how your systems are exposed and how hackers try to force entry into your home network.

If you took my advice and bought and installed a frhub for your home network, the most likely situation to occur is that you have a report full of Stealth results, which is good. You should congratulate yourself on doing what you can to protect your domestic computing environment. You could still be in trouble, however, depending on what else is running on your computer.

Perhaps you were so excited when you got your cable modem that you ignored my advice (or hadn't yet bought this book) and hooked up one of your computers directly to the cable modem without any protection. In the time that it took you to read this paragraph, your computer already could have been compromised, and someone could have installed a piece of software on the machine without your knowledge.

No port scanner in the world is necessarily going to divulge this sort of information, unless it thoroughly scans all 65,000 ports on your computer, and you carefully review its results and understand the implications of the port numbers that it finds open. While this scenario isn't likely, it can happen. Getting rid of these rogue programs isn't easy and is outside the scope of this book. You might have to completely reinstall the operating system from scratch, erasing your entire hard disk.

If you want to learn more, I suggest getting your hands on a more in-depth book on security and following some of its suggestions. There are plenty of network security books, but unfortunately, none is really geared toward beginners. Most are written for administrators of large corporate networks, who often don't know much more than you do, but are willing to spend more time to lock things down since they have more to lose with break-ins than your small home network does. See the section "Recommended Reading" near the end of the chapter for a few books and Web sites to visit.

Solutions

There are several things that you need to do to secure your systems from potential harm. Let's review the items and then cover how you go about installing and maintaining them one by one:

1. Install and configure an antivirus scanner.
2. Protect Windows operating systems, and remove any harmful Windows defaults and Microsoft programs.
3. Ensure that specific firewall options on your frhub have been properly set up.
4. Remember to do ongoing maintenance of your antivirus software and to periodically review your firewall logs.

Antivirus Software

There are numerous antivirus programs on the market. Most cost about $50 and include several months' worth of updates as part of their purchase price. While I have used several of these programs, the one I keep coming back to is Symantec's Norton Anti-Virus (NAV), available for various Windows and Mac operating systems. The program works well, is relatively easy to install and set up, and the company is constantly providing updates to the virus scanning libraries that are used to keep your protection up to date. You can't go wrong with this program, and I'll show you how to set it up properly. If you would rather choose some other antivirus software, go ahead—you are better off getting something rather than nothing—but NAV is the one that I'd use.

In the past several years a number of Internet-based antivirus service providers have sprung up from such well-known vendors as Mcafee/Network Associates. Instead of buying a software package and installing the software from CD, you download a small piece of software from the Internet and use a Web page from the service provider to manage your antivirus situation. The advantage of using these providers is that you minimize the downloaded

software to your machines, and supposedly they are simpler to operate and do just as good a job as the software-based antivirus products. I have tried a few of these providers, but don't yet recommend them even though others have used them with good results. It is still too early to tell in terms of effectiveness, and I would wait until there is more experience with them.

Another twist to the antivirus scene is the inclusion of antivirus screening software on various firewalls and frhub devices. SonicWALL began this trend, and Linksys is also offering this feature. While it sounds like a great idea, since you minimize the amount of software that you install on each machine, I don't recommend the practice. The tools aren't as good as NAV, and getting rid of them once they are installed is painful. If you do want to try this, you'll have to pay an additional subscription fee (beyond the initial purchase price) for this service. See the "Troubleshooting" section later for further comments about this topic.

Many new computers come with preinstalled antivirus software, or you can order the software at the time you place your order for a new computer. If you have some other antivirus software, I recommend replacing it with NAV. This may mean uninstalling the other antivirus software first, and then installing a copy of NAV. This is more work than you bargained for, but trust me, you'll end up doing this later. It isn't any fun to deal with multiple versions of software that do things in slightly different ways.

Choosing your antivirus product has one additional wrinkle. You should purchase and install a separate copy of the program for every machine in your home. This is the method I recommend for most households. Remember that you must install it for every machine: if you leave one unprotected, a virus could enter your home from that machine and infect the rest of your network.

If you are running the original version of Windows 95 and want to install the latest version of NAV on it—you can't. (Note that the current version of NAV supports Windows 95B, also called 95OSR2, which is a more recent version.) At this point, you are faced with a difficult choice: either continue without any virus protection on this machine, upgrade it to a newer version of Windows, or try to find an older copy of NAV that will run on the original Win95. None of these alternatives is great. I'd choose the upgrade path to Windows 98 or 2000 if you were going to upgrade the machine anyway, and if the Win95 version has some problems running something else that you would like to fix. You might be able to find an older version of NAV on the Internet or from a friend.

You can also purchase an enterprise version of the software and set up an antivirus server. The advantage is that you only have to download the virus pattern files once, and then the server will copy these files to all your machines on your network. However, I have found that the server versions are expensive and geared toward networks of several hundred computers, not your average home network situation. I would stick with the separate copy

method. You should purchase a license for each machine you intend to run it on, and the antivirus vendors offer multiple license packs.

Finally, Symantec sells NAV as part of several different packages, depending on if you want other software along with the antivirus checker: SystemWorks (which includes troubleshooting utilities and fax software), Norton Internet Security (which includes a personal software firewall and banner ad blocker), and a bundle of NAV with fax software. I recommend purchasing the basic NAV version; you don't need all these other things. Besides, the additional programs can add up to a lot of dough. The basic NAV program also works on the widest selection of operating systems (but not on NT Server and Windows 2000 Server versions if should you be using either of these versions).

Setting up NAV requires you to set up two separate programs: the actual antivirus software and an additional program called LiveUpdate, which is used to schedule and update the virus definition files. As new viruses are discovered on the Internet, the product team at Symantec makes updates to these definitions, so that their scanners can catch the newest viruses. The trick becomes downloading the updates as soon as they are available and making sure that you stay current with them. Otherwise, you run the risk of being infected.

That doesn't mean that you won't ever get infected with a new virus, because it is possible for something to arrive at your desktop before the good folks at Symantec have had time to process their own update and send it to you. That does happen, and if your company has European offices that are connected via e-mail, you could be the first person in the United States to catch a new virus. This is because Europe is a few hours ahead of us here in the States, and often viruses begin their propagation there as businesses open and as people fire up their e-mail software when they come into work. Sometimes, it pays to go into work late and not be the first one to get your e-mail in your office!

Before you install NAV, make sure that all your computers have your e-mail software installed and set up correctly. While you can do this after you get NAV on your machines, it is best if you have the e-mail software configured properly beforehand, since NAV will discover which e-mail accounts you have set up and will ask you if you want to protect them before finishing up its installation. Of course, if you are reading the chapters in sequence, you've already done that in Chapter 5. If you skipped over that chapter, now might be a good time to go back to it and get your e-mail house in order.

Enough caveats. Put this book down, get a copy (or copies if you want to be legit) of the software, and install it on all your machines. Make sure after you install NAV that you run LiveUpdate immediately and update your virus definition files. You may have to do a few reboots to get everything working, so you might want to pick a time when the rest of the household is out at the mall or sleeping, so you don't interfere with their computing needs.

Once you install the software, you should be careful about several configuration parameters. Let's take a look at some of these screens, which you get to by clicking on the NAV icon in your System Tray (if you are running Windows), or go to the Norton Anti-Virus folder (if you have a Mac).

For Windows, you want to pay attention to three different places on the NAV configuration: the general automatic protection features (see Figure 6-1), the floppy disk scanning features (see Figure 6-2), and the e-mail protection features (see Figure 6-3). Each is important. You need to go through this process for each of your home computers. It sounds like a lot of work, but once you get this set up, you don't have to deal with it again—at least until you get a new computer.

You basically want to set up NAV to work as seamlessly as possible, so you don't have to remember to do anything, yet your computers are still protected. Choose the options that I have selected on the various screen shots for your own computers, and you should be set. The only difference you might see would be if Symantec were to change the program options.

Macintosh users of NAV don't have as many options to set up. You should check the boxes labeled "Scan floppies" and "Treat all removable disks as floppies," and that should do it for you.

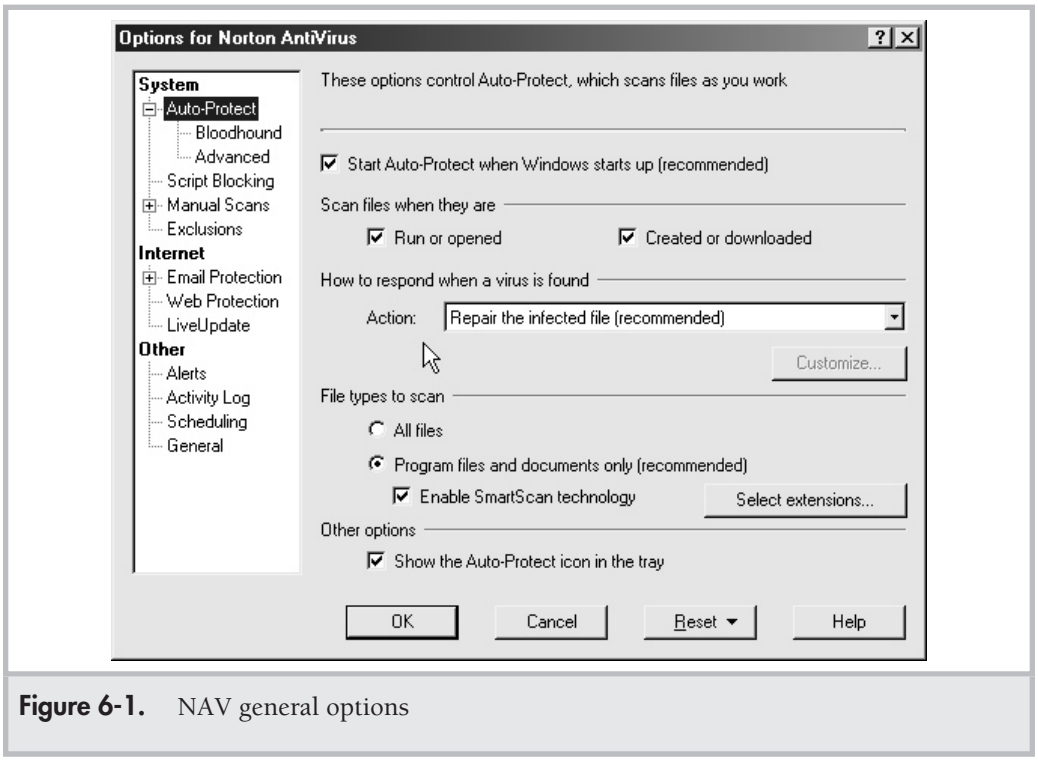


Figure 6-1. NAV general options

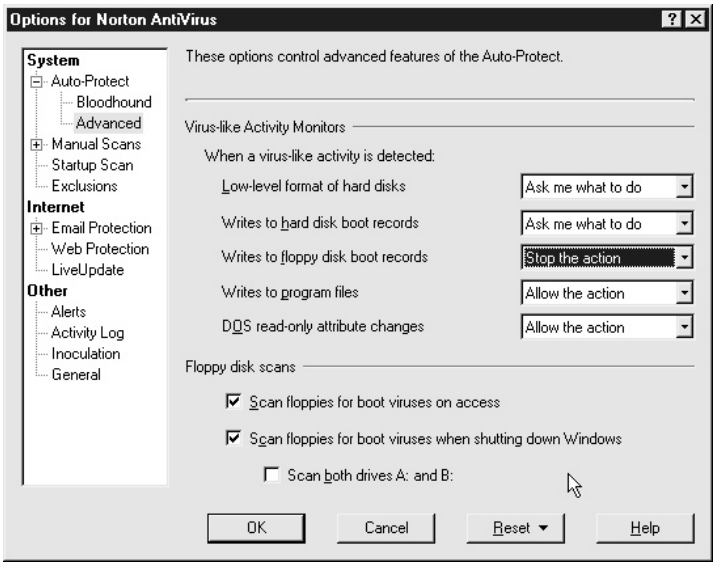


Figure 6-2. NAV floppy scan options

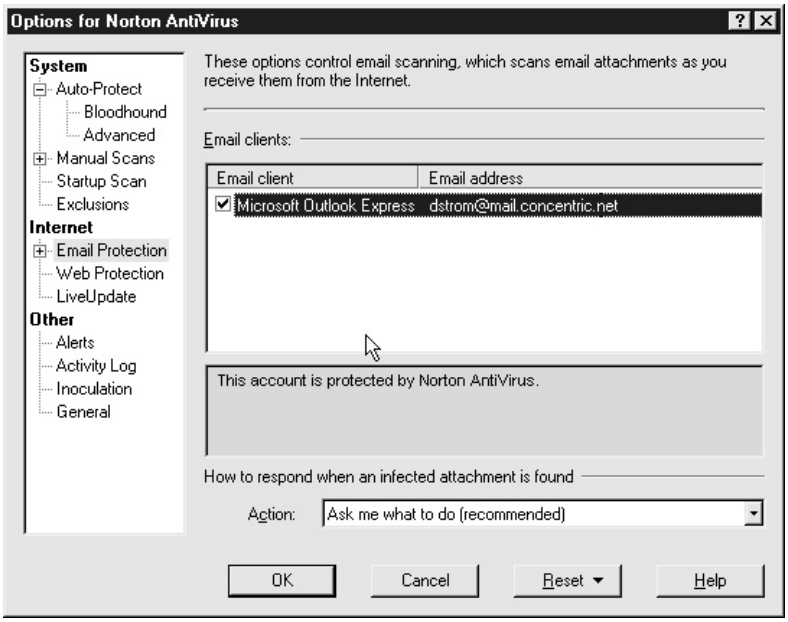
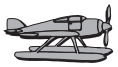


Figure 6-3. NAV e-mail options



SURVIVAL TIP

I'd like you to do take an additional step with NAV: Do a full system scan on each of your machines and create a series of emergency disks for at least one of the machines. If you have more than one version of Windows, create the emergency disks for the more recent operating system version, at the very least. If your PC comes with an internal Zip drive, you can speed things up by creating an emergency boot disk on a Zip disk instead of on a series of floppies. You'll see the appropriate menu choice for creating a boot Zip disk in this situation.

You'll need emergency disks if one of your machines gets so toasted by a virus that this is the only way you can easily recover all the files and bring the machine back to working order. You can boot from the original NAV CD-ROM if your PC supports a bootable CD drive. It is far better to set up the emergency disks and keep these disks someplace that you'll remember in the moment of panic when your PC is rendered a useless hunk of metal and plastic by some nasty virus.

If you've gotten this far and wonder where I talk about how to fix your PC when it receives a virus, turn to the "Troubleshooting" section. Let's move on to other changes you'll need to make to secure your PCs.

Windows Changes

If you own one or more Macs, you can skip this next section and feel somewhat superior to your friends who have invested in the Microsoft Windows monopoly. MacOS is an inherently more secure operating system, mainly because Microsoft mucked up Windows with so many designed-in security problems. You should still use antivirus software, and you should still put a firewall on your home network. At least you don't have to baby-sit the numerous operating system leaks and problems that I'll describe here.

If you want to further explore various security issues on your Macs, I suggest trying out or purchasing software from these vendors: Open Door Networks (http://www.opendoor.com), Sustainable Softworks' IPNetSentry (http://www.sustworks.com), and MultiRouter Traffic Grapher http://people.ee.ethz.ch/~oetiker/Webtools/mrtg).

Maybe one day we will see a version of Windows that will equal the Mac in terms of security strengths, but it isn't likely. XP adds some new back doors that will require your attention, and if you are running XP or planning on buying a new computer that comes with XP, then you should read that section and set things up accordingly.

There are five things you need to do on just about every version of Windows:

1. **For all Windows versions, lock down your network configuration.** If you have enabled file sharing, make sure that all of your shared folders require a password as I instructed you to do in Chapter 2. If you are *not* using a frhub and have your computers connected directly to the Internet, you need to unbind the TCP/IP protocols from Windows Networking services. (See http://grc.com/su-explain.htm for more information on how to do this.)

2. **For Windows 95/98, disable Windows Scripting Host (WSH).** This is one way Bubbleboy and other scripting-style viruses get into your life. Go to Control Panel | Add/Remove Programs | Windows Setup | Accessories | Details and clear WSH. Then click Apply. Unless you are running Visual Basic scripts, you won't miss this piece of software, and you are better off without it.
3. **For all Windows versions, if you are running Internet Explorer version 5, download the "eyedog" scripting patch.** This plugs another hole in the scripting side of things. Get the patch from Microsoft (http://www.microsoft.com/TechNet/IE/tools/scrpteye.asp).
4. **For all Windows versions, you should change your browser's Internet security options** to prevent scripts and ActiveX controls from automatically running. This will take some fooling around with the options, depending on which browser version you are running and whether you are totally paranoid and want to turn off cookies and scripts entirely.
5. **For all Windows versions, remove automatic VBS execution ability.** Thanks to *PCWorld,* this is how to set this up: In Windows 95/98 Explorer, open Folder Options under the View menu (or Tools in Windows Me/2000). Select the File Types tab, and scroll to VBScript Script File. Click on the Edit button (the Advanced button in Windows Me/2000). Another window will open showing the possible file actions, with the default action indicated in boldface type. The default action is likely Open. Highlight instead the word "Edit," and click the Set Default button. "Edit" should now appear in boldface.

In some older systems the Edit function may not appear. In such instances, click the New button and enter **Edit** in the action field and **Notepad.exe** in the application field. Once Edit appears, make it the default action, as just described. While in the file-type screen, also make sure the boxes for Always Show Extension and Enable Quick View are also selected. Click OK to close the open windows.

You can also follow the instructions in Appendix B to eliminate other more troublesome file extensions.

If you would rather download a utility program called VBS Defender that makes some of these changes for you, go to *PC World*'s Web site: http://www.pcworld.com/downloads/file_description/0,fid,8106,00.asp.

I realize that all of these suggestions are a lot of work, particularly since you have to do them on *all* of your Windows computers that you have at home. You'll thank me later, when you hear from one of your neighbors that they are infected or under attack.

Firewall Issues

One of the biggest differences between cable and DSL connections is the potential security options that are part of the device used to connect you to the outside world. The cable modem

has none, while the DSL router/modem comes with some significant security features. The trick is in setting them up or knowing how to get them set up for you.

This means that if you do your homework and get your DSL router configured properly, it can serve as a firewall and block potential attacks before a single data packet makes it further into your home. With a cable modem, you don't have the possibility of this protection, which is why I strongly recommended the frhubs in the last chapter.

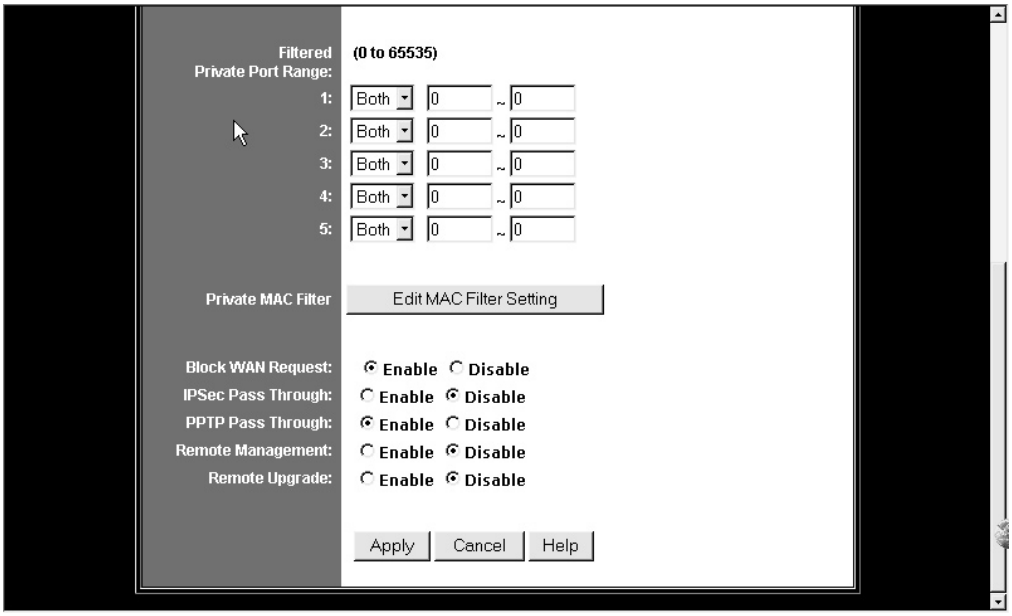
Let's talk about how you set up your frhub for specific security issues and then return to how you can harden your DSL router if you went that route.

With some of the frhubs, there is little you can do to increase their default security options. I'll mention a couple of things to check and then cover how to set up real firewall rules on the SonicWALL, which has a fully featured, rules-based, inspection-type of firewall that you can use to lock down just about everything on your network.

The first thing that you want to turn off is the ability for Windows networking broadcasts to leave your home. This is one way that intruders find out what you have on your PCs, and also a way for them to attach to your computer and start examining your files. All of the firewalls turn this off by default, but it is a good idea to check it nonetheless if you can. The Netgear frhubs don't have any mechanism for changing this, so you don't have anything to do.

On the Linksys frhubs, go to the Advanced | Filters page, select Enable for Block WAN Request, and select Disable for both Remote Management and Remote Upgrade. This will make your network go to Stealth mode and make sure that no one else from the outside can mess with your configuration. (See the illustration.)

Ill 6-1

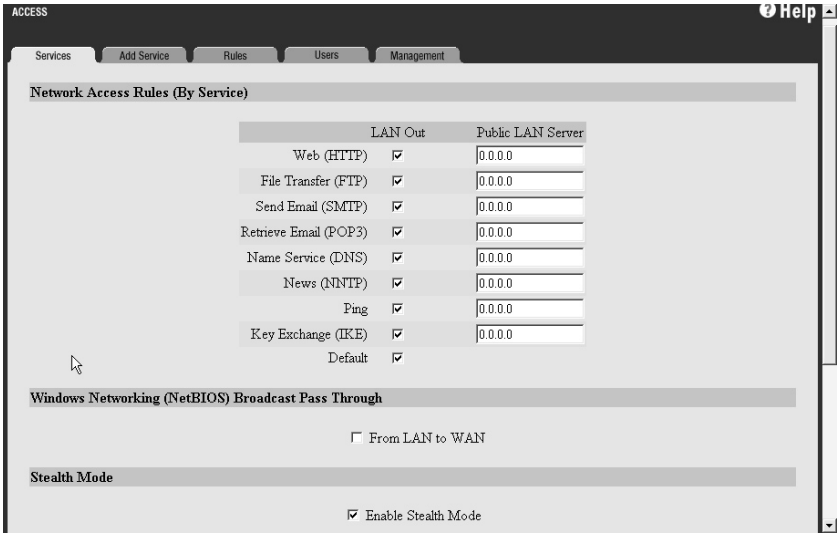


On the MaxGate frhubs, you want to go to the Device Admin. page and choose Disable for External Admin., Yes for Block WAN Probing, and Yes for Block WAN ICMP. (Why all the vendors can't use Yes and No universally is beyond me, but let's not get into that rant right now.) Your settings screen should look like this:

Ill 6-2

On the SonicWALL, go to Access | Services and make sure that the check box is clear for Windows Networking Broadcast Pass Through. This will keep your networking commands strictly in-house. It is also a good idea to select Enable Stealth Mode. This will ensure that the SonicWALL won't respond to any requests from the Internet, making it as invisible as possible to potential hackers. (See the illustration.)

Ill 6-3

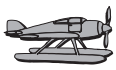


If you want to be even more thorough, you can specifically block certain ports, just as we did in the previous chapter when it came time to turn off AOL IM. I don't recommend you fool around too much here, but know that you have at your disposal a way to isolate your network, should the need arise.

Enterprise-class firewalls come with the ability to set up a series of rules to prevent all sorts of mischief from creeping into their networks. The SonicWALL is the most capable unit of the frhubs I recommend here, and it can be set up in a similar fashion. Why would you want to use these rules? It could be that the firewall is doing too good a job at blocking your applications from actually working, so you might need to relax their prohibitions (what computer geeks call "poking a hole in the firewall") so that these applications can work unimpeded. The kinds of applications that are usually in the most trouble are various network-based games. This is outside the scope of this book, but you can find some good information on how to set up the firewalls to let the games continue if you go to PractiallyNetworked site (http://www.practicallynetworked.com).

Ongoing Maintenance

Our discussion of firewalls and antivirus software is really just the beginning. Keeping your network secure doesn't have to be a full-time job, unless you work as a security consultant for a large corporation.



SURVIVAL TIP

You do have to spend some time each week routinely maintaining your computers if you want to take true protective measures. Think of it as being the security guard who makes his or her rounds and rattles the doors in a building, to ensure that they are still locked and no one has broken in.

You should do three things regularly:

1. Periodically scan each computer's hard disk for viruses and irregularities.
2. Periodically update your virus scanning software with the latest virus pattern files.
3. Periodically review the access log of your frhub to make sure that everything is hunky-dory and that there aren't any break-ins to your network.

Each of these measures doesn't take more than a few minutes to do, and with the right kinds of software, you can have certain things happen automatically (so you don't have to remember to do them explicitly). Let me explain.

If you are using NAV, the first two steps can be automated completely, provided you have set up both NAV and LiveUpdate properly. I recommend having NAV perform an automatic scan of your entire hard disk once every month and having LiveUpdate check every day for new virus patterns.

To set up these parameters, you'll first need to bring up the Configure Anti-Virus screens by right-clicking on the icon in your Windows task bar and then choosing the LiveUpdate menu, as shown in Figure 6-4. Make sure the Enable Automatic LiveUpdate check box is selected, and make sure that the button Apply Updates Without Interrupting Me is also selected. This way, your computer can grab those updates without you having to worry about them.

Next, bring up the NAV program itself, click on the Scheduling button, and then click Add Event. A wizard will walk you through the process. Add two events: one that does the daily LiveUpdate request and one that does the monthly hard disk scan. You can set up both

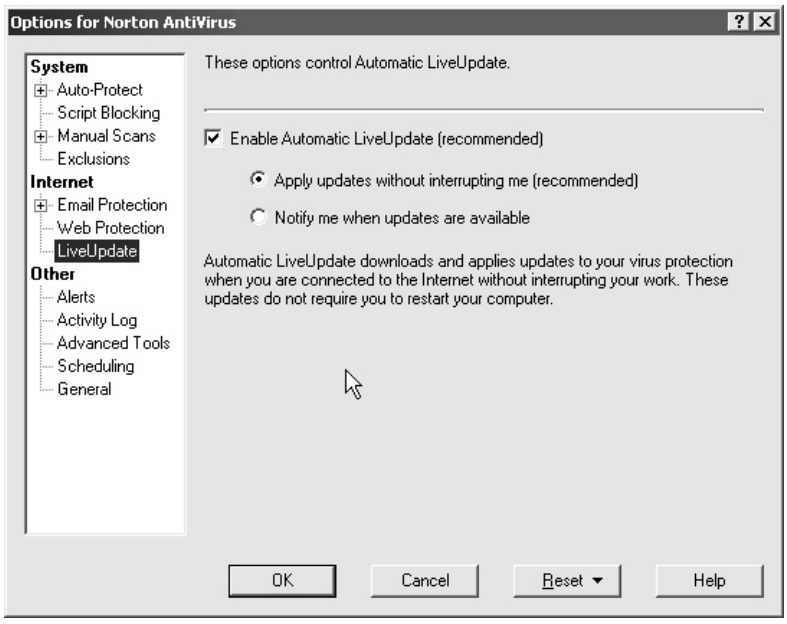


Figure 6-4. LiveUpdate options for NAV

activities to run in the middle of the night, when you aren't usually using your computers, as long as you leave them turned on all the time. If you tend to turn off your computers at night, then schedule these events for times when you won't be using them or when you can afford to have them go do their thing without interrupting some important work. When you are finished, your Scheduling screen should resemble Figure 6-5.

Mac users of NAV go through a similar sequence of steps to accomplish the same thing.

Finally, you need to examine your frhub's access logs and set its particular features. I'll show you what to do with the Netgear RP114 and the SonicWALL, both of which have this feature. (Some of the other Netgear frhubs may or may not include this feature.) Either product can send you e-mail notifications when someone tries to break into your network as well as send you periodic information when other events occur.

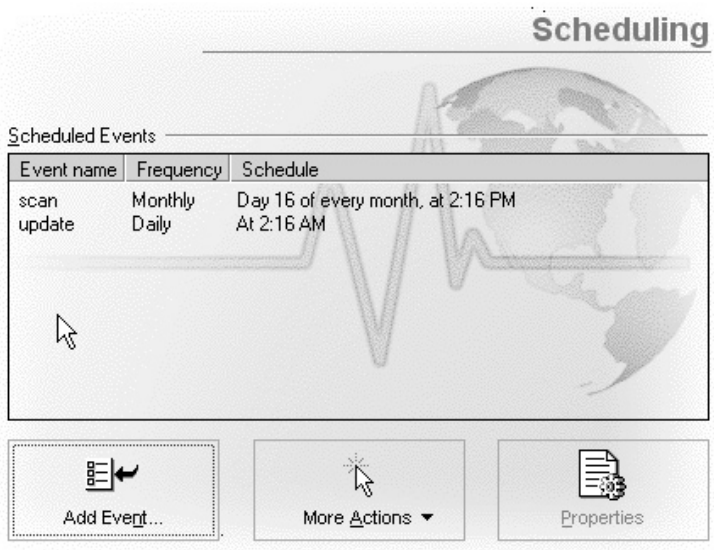
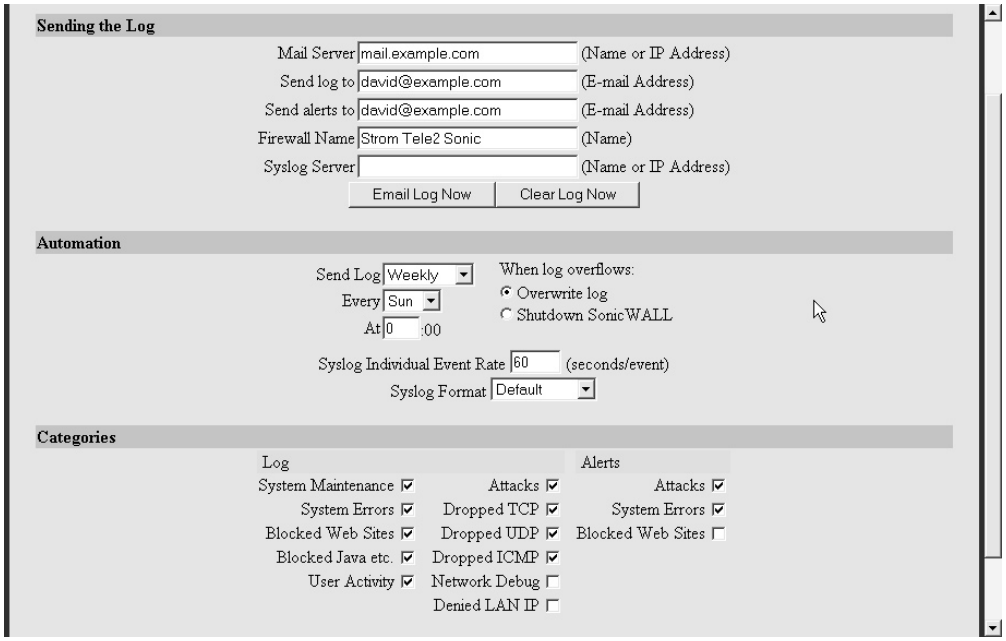


Figure 6-5. NAV Scheduling options

For the SonicWALL, bring up your browser, and enter the IP address of your SonicWALL firewall. Then log in with the correct user name and password, and go to the Log button and Log Settings tab.

You'll notice in the following illustration that I have put in my e-mail address and mail server information, along with instructions to e-mail me the log every Sunday. I have also selected the various categories of events that I want to be notified about, including system errors, attacks, and dropped packets.

Ill 6-4

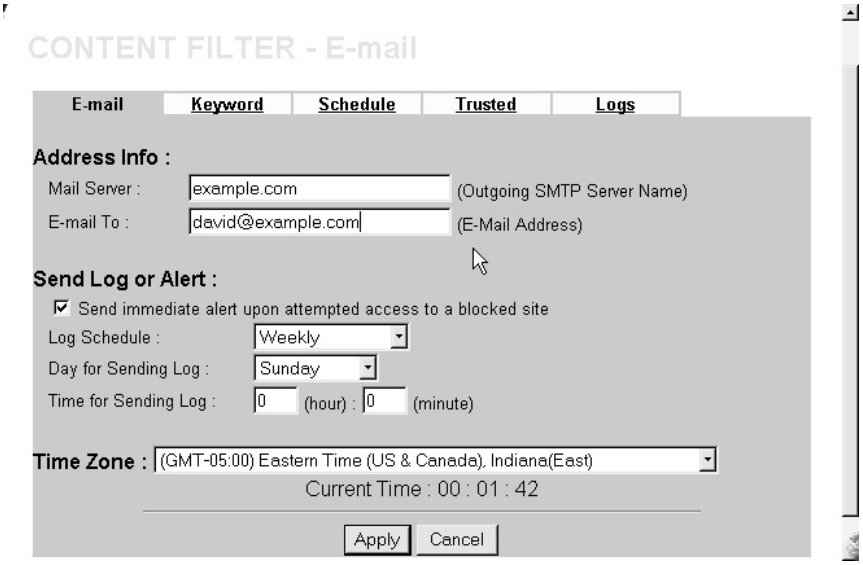


You might want to choose these parameters or to experiment with others once you are more comfortable with seeing the reports that are generated. To test to make sure that you have set up everything properly, you can click on the button E-mail Log Now, and the SonicWALL should send a copy of the log to your e-mail address within a few minutes.

Now you are set. You will get notifications from your SonicWALL when your network is under attack and also have your computers updated with the latest Norton software when they are available.

For the Netgear RP114, bring up your browser and type in the IP address of the frhub, and then enter your user name and password to log in. Next go to Advanced | Content Filter | E-mail. Fill out the screen as shown in the following illustration, again with your e-mail server and e-mail address, and selecting the appropriate boxes to send you the log every Sunday.

Ill 6-5



Changes to Windows XP

Windows XP has introduced the concept of its own built-in firewall as part of the expanded range of services for the operating system. While no software-based firewall can match the abilities of the SonicWALL and other hardware firewalls, it is probably worth a closer look to see if this can help protect at least those machines on your network that are running XP. I don't recommend that you upgrade your older Windows operating systems to XP just for the firewall feature—you probably can't since XP needs lots of memory and processing power found on newer computers. If you have to buy a new computer, and that new computer comes with XP preinstalled, then it is worth turning on the firewall feature, if only to serve as additional protection for that PC.

To get started, go to Control Panel | Network Connections | LAN Connections and right-click on Properties. Then go to Advanced | Internet Connection Firewall | Settings, and you'll see a series of screens, as shown in the upcoming figures. While some of this isn't absolutely necessary since you should be protected by your frhub, it doesn't hurt to also protect your XP machine with these measures, too.

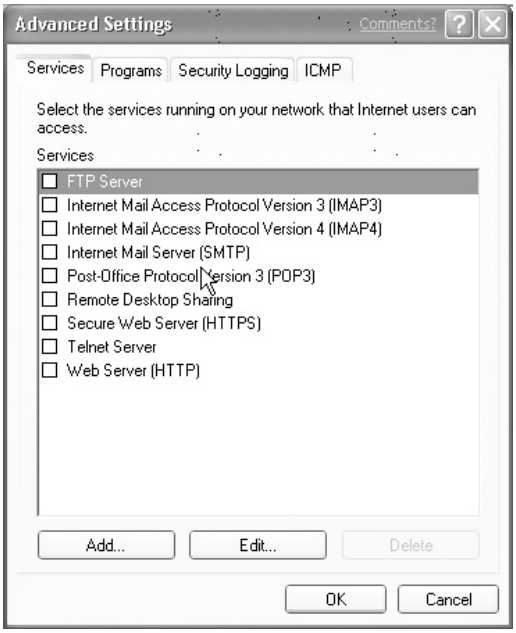


Figure 6-6. Advanced firewall settings on XP firewall

Ensure that no one can access the services you have running on your XP machine, that your machine appears in Stealth mode whenever possible, and that you log any possible break-in attempts on your machine. (See Figure 6-6.)

For the first series of settings, select any of the services you have running on your machine that you wish others to have access to. Ideally, none of these should be selected, so that no one can see your machine. However, if you want to run a Web or e-mail server on your XP machine, and you can set up your frhub to allow outsiders access to these services, then select these boxes. Of course, you also have to ensure that your Web and e-mail and whatever server is set up properly. If you now click on the Security Logging tab, make sure to select Log Unsuccessful Inbound Connection Attempts, as shown here.

Ill 6-6

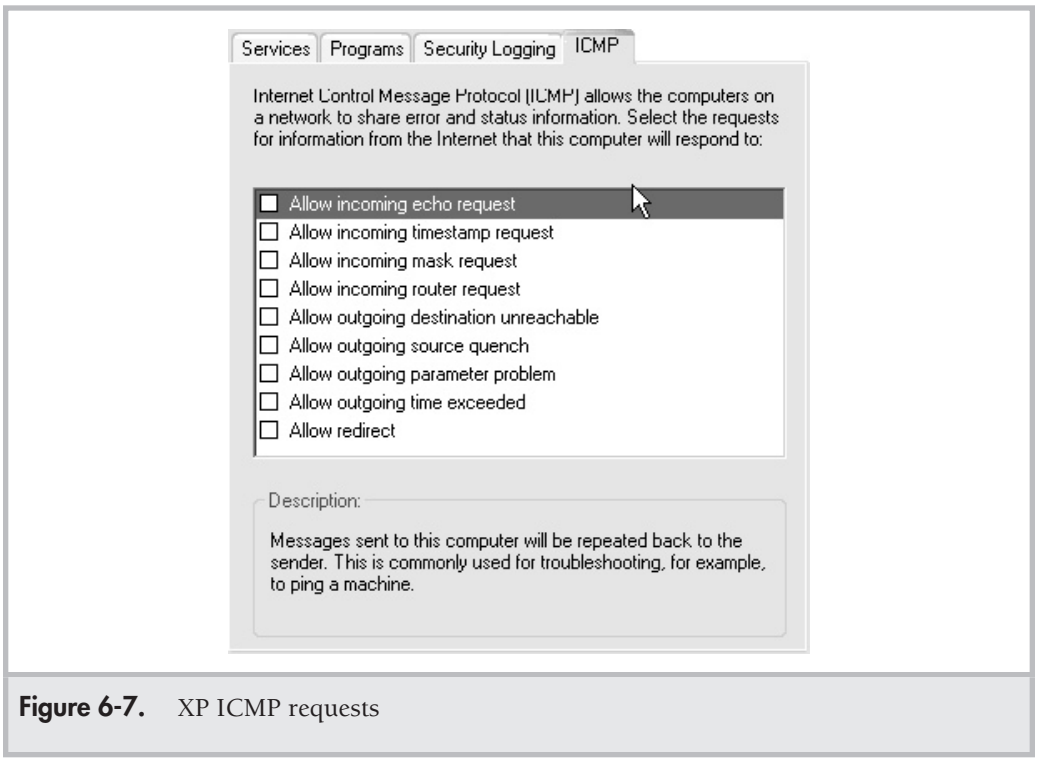


Figure 6-7. XP ICMP requests

Finally, go to the ICMP tab. ICMP is the protocol that computers use to communicate with each other, mainly used by routers, but it can be used by hackers to penetrate your systems. Again, to be as stealthy as possible, all of these boxes should remain unchecked. You might have to check one or more of them to enable certain games or applications to run on your XP machine. (See Figure 6-7.)

Troubleshooting

Our coverage of security issues wouldn't be complete without touching on ways that you can troubleshoot various problems. Let's review some of the ways you can remove a virus once you are infected, see how to track down the origins of a virus, and examine alternatives to NAV. As promised, I go into setting up a virtual private network and give you plenty of additional reading if you want to learn more.

Is It Really a Virus?

Sometimes, the e-mail warnings that you get from your well-intentioned correspondents about viruses turn out to be wrongheaded. Let's take a look at one message that a friend of mine received:

L 6-1 It was brought to my attention yesterday that a virus is in circulation via e-mail. I looked for it and to my surprise I found it on my computer. Please follow the directions and remove it from yours. TODAY!!!!!!! I do not know how long it has been on my computer, but no virus software can detect it. It will become active on June 1, 2001. It might be too late by then. It wipes out all files and folders on the hard drive. This virus travels thru E-mail and migrates to the 'C:\windows\command' folder.

To find it and get rid of it off of your computer, do the following : Go to the "START" button. Go to "FIND" or "SEARCH" Go to "FILES & FOLDERS" Make sure the find box is searching the "C:" drive. Type in; SULFNBK.EXE. If it finds it, highlight it. Go to 'File' and delete it. Close the find Dialog box Open the Recycle Bin Find the file and delete it from the Recycle bin and you should be safe.

The bad part is: You need to contact everyone you have sent ANY e-mail to in the past few months. Many major companies have found this virus on their computers. Please help your friends !!!!!!!! DO NOT RELY ON YOUR ANTI-VIRUS SOFTWARE. McAFEE and NORTON CANNOT DETECT IT BECAUSE IT DOES NOT BECOME A VIRUS UNTIL JUNE 1ST. WHATEVER YOU DO, DO NOT OPEN THE FILE!!!

Before you do anything like delete the file indicated in the message, you should first check and make sure that you are at risk. Let's go to Symantec's Anti-Virus Research Center Web site and track this down. Go to http://www.symantec.com/avcenter, click on the Virus Encyclopedia, enter in the search box **SULFNBK.EXE**, and see what turns up. As luck would have it, this is a hoax, not a virus, and the message is asking you to delete a legitimate Windows executable file, so you should ignore the message.

When Not to Give Someone Your Credit Card Number

While we are on the subject of e-mail hoaxes, I should mention one other situation that comes up with disturbing frequency: the scam of trying to get you to divulge your credit

card number to someone who may not be whom you think they are. Let's take a look at a typical e-mail request:

L 6-2

```
Subj: AOL Billing Center

From: BillingRep46@aol.com

Below is the result of your feedback form.  It was submitted by

(BillingRep46@aol.com) on Sunday, May 27, 2001 at 07:43:44

---------------------------------------------------------------------

Hello from America Online,

We apologize for the inconvenience, but the credit card information for your
account has expired.

In order to enjoy your America Online experience and keep your account
active, you must enter new, *valid* credit card information within 24 hours
of receiving this e-mail. To enter new credit card information and keep your
account active, please click here.

Our Regards,

Matt Glazer

America Online Billing Department and Staff
```

What is wrong with this message? First off, AOL never asks people to send their credit card numbers in this way. Second, your AOL is active forever; those who have tried to discontinue service can attest to the zeal with which AOL will attempt to keep you subscribed. Finally, the e-mail address is suspicious: "billingrep46@aol.com" doesn't sound like a legit AOL employee, now does it?

Beware of these and other kinds of scams, particularly if someone you don't know is asking you for your personal information. If you get something like this, report it to abuse@aol.com (or whatever domain it purportedly came from).

Removing a Virus from Your PC

No antivirus program is perfect, and a time will come when your computer gets infected. The trick is to limit your exposure and get rid of the virus without mangling your PC.

If you realize that the e-mail attachment (or floppy disk file) that you just opened contains a virus, don't start cursing. Immediately, and I mean immediately, reach over behind the computer, grab the Ethernet cable, and disconnect it from your computer. You should take care not to rip the cable off from the RJ45 plastic connector if at all possible. Why the Ethernet cable? That's the fastest method of isolating your machine from the rest of your home network and the Internet at large. If you can't reach over to the cable fast enough, or don't have the presence of mind to do this, then press the power switch to turn the computer off.

Either way, you have to bring up NAV (or whatever antivirus program you're using) and try to eliminate the virus. If you turned off your PC, boot from those emergency repair disks that you created earlier in the chapter. Oops, decided to skip that step, did you? Don't despair. You might be able to boot directly from the original NAV CD-ROM, if you can find it and if your computer is set up to boot from CD drives. (If you are running Windows, you should be able to press DEL or F1 and see some setup options that you can fool around with to select the boot device order.)

If it is a virus that NAV doesn't recognize, which is likely because it should have stopped it before you opened your attachment, then you will have to figure out a way for it to clean the darn thing off your machine. If you have a working machine elsewhere at home, try going to Symantec's antivirus Web site (http://www.symantec.com/avcenter). See if you can track down some specific advice on how to remove the virus. Depending on what you have caught, you may be in for a rather long period to disinfect your PC.

You should also review your configuration settings; make sure that the automatic protection features have been set properly and that you have the latest pattern file to recognize what that you just caught.

Tracking Virus Origins

If you have isolated the virus on your computer and want to spend some time tracking down where it came from, more power to you. Once I find the darn things, the last thing I want to do is spend any more time with them, but I am not the type of person who slows down when he sees a wreck on the side of the freeway. You might be more of a gawker than I, in which case, this section is for you.

I did spend some time tracking down why I got a copy of the "Snow White" virus. It is one of the Hybris class, which are a series of well-known viruses to security experts. Like

many people, the first thing I did was look at where the virus was coming from in the e-mail message header. The e-mail message I received said it was from hahaha@sexyfun.net.

Naturally, I thought it was just another porn site, but I was surprised when I did a whois lookup on this domain. (If you go to the Web site http://easywhois.com, you can enter the domain name, in this case, sexyfun.net.) I found an interesting result: it was almost as if some Good Samaritan was trying to provide antivirus information in the actual whois record, anticipating that I (and others like me) would try to track this stuff down. The record looks like this:

L 6-3
```
BLACKBURN, CASEY (CXB1127)

Research.the.Hybris.virus.The.e-mail.is.not.from.us@sexyfun.net

For Virus/Spam Help or Questions Go To

WWW.SEXYFUN.NET. NC 27609 US 919-875-4974

The From Field Is Faked
```

If this information was to be believed, it meant that the sexyfun.net domain wasn't actually where the virus originated. This sort of thing is very typical with many viruses, which can rewrite e-mail header information to some made-up address. What was curious was how Blackburn had manipulated the whois record for his domain. To get more information, I spoke to Gary Moe, who hosts the sexyfun.net Web site.

Both Moe and Blackburn are network system administrators with good hearts. Moe's company provides the Web hosting resources for the domain, while Blackburn did most of the work creating the content. Moe told me, "Our main goal was to help people who were running into this problem, and raise public awareness. We aren't into this for making money. Indeed, we have turned down several offers to post banner ads pushing particular products on our site."

A nice sentiment, indeed. If you go to Blackburn's Web site, you'll be impressed, too. It was filled with helpful information on how to eradicate this virus, along with lots of tips on how to set up mail filters to prevent future attacks. Blackburn and Moe also provide links to the major antivirus software vendors, so you can research the virus yourself if you don't believe them. Moe told me that they have received plenty of angry e-mails from people who think they created this virus. (The latest information is that a Brazilian group is the author.)

I did learn a few things in the process. First, I came across a helpful newsgroup called alt.comp.virus that discusses things you can do to keep your system virus-free. (Remember

newsgroups from the last chapter?) While there were several thousand messages when I checked this morning, I could easily sort through them to find out more about Snow White and Hybris.

When I followed a link on Blackburn's site, I found a discussion about one "feature" of Windows Me that isn't widely known, the ability to automatically restore a system to a previous state. I remember when I first came across this feature, I thought, what a great idea. However, as you see from a bulletin from Microsoft—http://support.microsoft.com/support/kb/articles/Q263/4/55.asp—you'll find out that the restore function can keep virus scanners from completely removing infected system files. You might have to turn off the automatic restores before you can get rid of the infection completely.

I mention this not to knock Windows Me but to point out that things have gotten complicated. Even the most experienced computer user will have to keep up to date on the developments to stay ahead of the twisted people who create these viruses.

Let's praise people like Blackburn and Moe. They are a reminder of the culture that was common on the Internet ten or so years ago. Blackburn and Moe didn't have to go through all this trouble to buy the domain name and host a site and prepare all these pages. Instead, they are helping others who possess less knowledge than they do, by providing tools and helpful advice. Of course, you have to know where to look for this advice, and sometimes tracking it down isn't easy. Their site offers a great starting place. More people should emulate them.

Using Alternative Antivirus Programs

While I am partial to Norton's Anti-Virus products, if you want to use some other virus scanner besides Norton, here's what you do. Read *PC Magazine*'s review about other products on ZDnet (http://www.zdnet.com/products/stories/reviews/0,4161,397221,00.html).

They still rate Norton the highest of those tested, but you might be attracted to another product. Maybe you have some other product that you are familiar with because you use it at work or because it came preinstalled on your new computer, and you don't want to go looking for something else. It really doesn't matter: While there are subtle differences among the various products, the important thing is to install one, get it working, update its virus pattern files regularly, and scan your complete hard disk once a quarter. Just make sure that with any product, you cover the basic operations: automatically scan all floppies, screen e-mail attachments, periodically update patterns, and regularly scan your entire hard disk.

Setting Up Antivirus on the SonicWALL

Another alternative to individual virus-scanning programs on each desktop is to stop the infections where they first penetrate your home network, at the firewall. SonicWALL was the first to include this on their frhubs, and other vendors have announced similar products. For an additional yearly subscription fee, you can purchase virus scanning

protection and install a small piece of software on each of your desktops, as long as they happen to be Windows machines. You can buy an annual ten-user license for about $300. Macs are not yet supported. More details can be found at the company's Web site (http://www.sonicsys.com/anti-virus).

Going this route has advantages. You have to do absolutely nothing once you get everything set up. The Sonic AV takes care of scanning, updating, configuring, blocking and tackling, and keeping your network safe and secure. You don't have to worry about e-mail attachments because they never even enter your PC: They are stopped by the SonicWALL, which isn't even running Windows, so you don't have to worry about the viruses messing it up either.

While this sounds attractive (and perhaps expensive, since you can't just buy a couple of licenses, but have to pony up for that ten-license minimum nut), I don't recommend this solution. My impression (and this is more anecdotal than based on lots of testing) is that the Sonic AV software is not as robust or as fastidious as the NAV that I know and love so well.

If you do want to set it up, you'll have to purchase the upgrade and install the software by activating it. (Bring up your browser, go to the IP address of your SonicWALL, go to the Anti-Virus page, and click on the Activation button.) Then register your SonicWALL on the company's Web site. It sounds more complex than it is. You'll then have to download software to each of your Windows desktops and probably have to reboot them before your protection kicks in. If you have Macs on your home network, you are out of luck since Sonic doesn't have software for them yet.

Setting Up a VPN on the SonicWALL

I mentioned virtual private networks (VPNs) a few times before and suggested that if you need to be extremely careful about the kind of data that you are sending and receiving over your home network, you might want to consider them. As you should know by now, just about every e-mail message that you send or receive is sent in clear text that anyone could read, should they be inclined to monitor your conversations. A VPN prevents this sort of eavesdropping by encrypting your traffic using one of a variety of encoding mechanisms.

Any VPN comes with two components: a client piece and a server piece. You locate the client on your home desktop, and the server piece is located someplace on the target network that you wish to communicate with securely. You can have a VPN client running on your remote firewall, or either inside or outside the firewall's boundaries. There are advantages and disadvantages to each method, and most likely you'll have little say in where the VPN server is running and what software it is using. You can also have VPNs running on two firewalls and two separate networks so that all network communications between the two are encrypted.

To set up a VPN—no matter what the configuration—is beyond the scope of this book. The instructions for the SonicWALL are obtuse and obscure, and will confound most of you and take some careful study plus probably a few calls to their technical support phone lines to clarify some things. It took me several hours to get my own VPN working, and that was after lots of personal coaching from the SonicWALL engineers.

If you are interested in learning more about VPNs, you should take some time to read the chapter on IPsec protocols (the underlying protocol that all VPNs are built on top of) in the Norberg book cited in the next section. Windows 2000 and XP come with support for IPsec built into the operating system in both client and server versions. This is probably as good a place as any to get started understanding the issues involved with setting up a VPN. Plenty of documentation is available on the ICSAlabs.com Web site, an organization that tests IPsec implementations and interoperability issues.

Recommended Reading

The point of this chapter was to introduce you to the bigger security issues and give you some solid foundations to start protecting your home network. Obviously, you can and should do much more to protect your computing resources. If you are interested, I recommend the following books that will guide you through the next steps.

A good book for beginners is *The Happy Hacker* by Carolyn Meinel (American Eagle Publications, 1999) which is available from her Web site at http://www.happyhacker.org. It contains plenty of illustrations of how hackers work and is written for non–computer experts.

If you want to learn more about what hackers can do to gain access to your systems, a very readable book is *Inside Internet Security—What Hackers Don't Want You to Know* by Jeff Crume (Addison Wesley, 2000). Crume gives you a detailed explanation of the methods that hackers use and practical advice on securing your network.

If you are planning on running NT or Windows 2000 servers on your home network, say a Web or e-mail server, then you need to harden those systems accordingly. The best book for this is *Securing Windows NT/2000 Servers for the Internet* by Stefan Norberg and deborah Russell (O'Reilly, 2000). It details on what you have to do for both operating systems to eliminate their security vulnerabilities.

The most technical and detailed of these books is *Hacking Exposed* by Scambray, McClure, and Kurtz (Osborne/McGraw-Hill, 2000). It covers both Windows and UNIX systems in detail and gives lots of tool recommendations and examples on how to understand the weaknesses in your systems and how to lock them down.

Another resource worth taking some time with is Project Honeynet, at http://project .honeynet.org. An informal group of Internet security consultants put together monthly

challenge puzzles that use real-world situations and problems. Solutions are posted the following month. You can learn a great deal from the information posted on this site. With one puzzle, I learned that the hard part isn't understanding how your network has been compromised, it is figuring out how to fix it and return it to a state where it won't be threatened again.

The average time spent to investigate the attack used in this one puzzle by the people who turned in their answers turned out to be about 34 hours per person. That is a staggering amount of person-hours, and these are the supposed experts with years of security training. Yet the attack, which happened to a university Linux computer last fall, took all of about a minute for someone to break into the system and install some automated attack tools. I particularly liked (in the white papers section) the conversation recorded between D1ck and J4n3 (Dick and Jane), two bad guys talking about various exploits, over an IRC channel, giving plenty of insight into some of their motives.

You should also periodically go back to the Web site of your antivirus software vendor, and check to see what is going on in the ever-changing world of viruses and their prevention. Most of the major vendors maintain quite good sites, where you can search for information about specific viruses and updates to their software, along with other security-related matters.

Futures

Network security is getting more potent and easier to use, and is slowly finding its way to home networks. As more people get continuous Internet connections, the growing need for easy to use and easy to set up devices motivates the major vendors to pack more security features in a wider selection of their product lines, at increasingly attractive prices. Having purchased a frhub, you have gone a major step toward improving your chances of practicing "safe hex," as one Web site calls it. Don't congratulate yourself too long, because being secure means continuously maintaining vigil over your network and desktop computing resources, and making sure that new and nastier ways haven't been found to penetrate your virtual home in cyberspace.

All of these measures and countermeasures are aimed at people from the outside trying to break in. An entire other set of circumstances covers what happens when people from the inside try to break out. In our next chapter, I'll go into details about another potential threat to your family's peace of mind—what can happen when your children are viewing potentially harmful and inappropriate materials on the Internet, and ways you can at least keep track of their surfing habits.