Global Information Assurance Certification Paper

Home IT Security:

How to Protect Yourself from the Evil Internet

By

Jay Wilson

June 9, 2003

GIAC Practical Assignment

Version 1.4b

Abstract

This paper is designed to point out the need for home security and what one can do for protection when using the Internet. It explains how the home computer user can implement security tactics for protection against break-ins how to monitor the system successfully. It takes the approach of covering a wide area of issues with even focus on each. The target audience is home computer owners who have some savvy about using computers and are aware of potential security problems and dangers (as well as the annoyances) that go hand in hand with being connected to the Internet full time using DSL or Cable Modem. It is not a technical paper for the IT security professional, but can be used by him/her as guideline if unfamiliar with home security issues.

For my discussion, I take the home computer owner through the setup of a home system from installing the OS through applying security patches to protecting his/her privacy. A lot of papers tell you what to do but not how to do it. I bridge this gap by giving good examples and references (URLs) to more details. Just in case the reader is not fully familiar with hackers, privacy issues, and spam, I touch base on those items before proceeding with the "do's and don'ts". I included a section on both personal and hardware firewalls and compare an easily to install and use personal firewall against a more sophisticated one. Finally I show how the system can be monitored for security and privacy. I also briefly cover wireless and some of the precautions the home user can take to secure that technology. I summed it up with a road map.

Since securing a home system is vastly different than that of an enterprising business system, there will obviously be a lot less technology and services covered in this paper. The information I presented in this paper was based on my many years as an IT professional at home and business, my SANS security training, and lessons learned.

1.0 Introduction

The main things that plague the home computer user are Hackers, Spyware, and Spam. If one is connected to the Internet 24/7 hackers are the main concerns (I'll cover hackers shortly), but what about the other two. Spyware is used to attack your privacy by gaining information about your Internet and computer usage habits and then reporting them to a server or database system to be used to later target you with advertisements. Spam is another annoyance, which at some point may be the same as a denial of service attack if it is severe enough. It sometimes comes as the result of data collected via spyware.

Hackers don't just target national security organizations and big businesses for cyber attacks: "They want your tax returns, network passwords, or bank account numbers" (Hummel, 2000). According to Internet Security Systems, Inc. (ISS), the Internet is a "dangerous place where hackers are constantly looking for ways to steal your passwords, credit card info-even your identity". This is more pronounced in the business environment but is making it's way into the home now days. Hacking has become so popular that there is now a new breed of hackers called *script kiddies*. They aren't very knowledgeable (yet) and use tools and malicious code found on the Internet to break in

Okay, so you don't have personal information on your PC that you care about. According to the CERT, hackers "want to gain control of your computer so they can use it to launch attacks on other computer systems". I think I'd be a little concerned if the FBI came busting in on me one evening because they traced an attack of a government system from my PC. You must also think about the impact of loosing all your personal data and having to recover your system if an attacker decided to obliterate your hard drive. It can take almost a day to install the O/S, applications, and personal data needed to restore your system.

Even through no one can fully protect a computer system from the experienced hacker, any security measure is better than none at all, and the more protection you have the better off you will be. As an analogy to this, some hackers are like simple burglars looking for an easy way to get in. They will go around your home looking for opened windows and doors. Unless you really have something really valuable for them, locked doors and windows will generally keep them out. They can always find an easier target just down the street. A very good reference to home security published by the CERT is at this URL:

http://www.cert.org/tech_tips/home_networks.html.

So now the question now is how can you protect yourself? The answer is by being prudent in deploying various levels of protection, periodically verifying that they are operating correctly, and monitoring your system. According to the SANS, these are layers of protection and you must decide on which ones to employ based upon the risk you may face. Now you don't have to be paranoid and do a complete systems check every time you turn around. Occasionally will suffice or when something just doesn't

seem right. This paper is only a guide and the reader must evaluate what will be the personal lost in terms time, money, and what it would take to recover from a possible identity theft. That is what I plan to discuss in the following sections starting first with a self-check of your system.

2.0 Self Check

Before and after any installs and/or security fixes, it might be nice to see how you are doing. A quick way is by connecting to the Gibson Research Corporation's web page at https://grc.com/x/ne.dll?bh0bkyd2 and let them probe your computer. It is a free test and doesn't harm your machine. Basically it is a port test that lets you know which ports may be vulnerable and how stealthy you are (another words how hackers may see you). Figure 2-1 shows part of the opening screen.

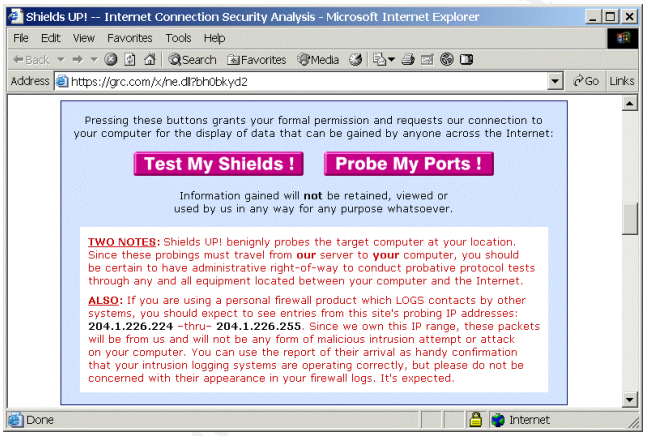

Figure 2-1. Shields Up Test Page

The *Test My Shields!* button is for a quick test and will reveal if your machine is acting as a web server or your NetBIOS ports are exposed (see figure 2-2). These are some entry points that hackers can find their way in to your machine.

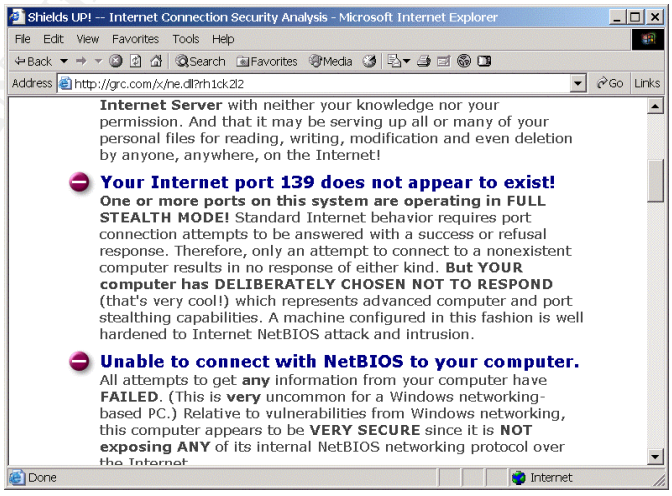

Figure 2-2. Shields Test Results

Clicking the *Probe My Ports!* button will allow some of the more common ports to be probed. Figure 2-3 shows the results when I ran it against my PC. A clear explanation of each test is available by scrolling down the page. The *Shields Up* main page has good internal links that explain it all with background information and insight.

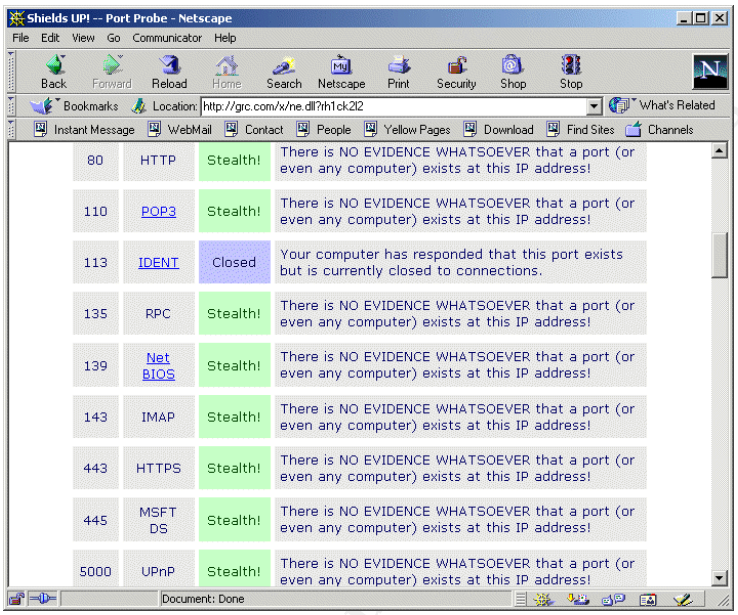

Figure 2-3. Port Probe Results

Another good free utility to use is *Active Ports* and is available from SmartLine at http://www.protect-me.com/freeware.html. It is a far cry better than the Windows *netstat* command line utility, since it monitors ports continuously and shows which application or service is using the port. This is a great real time tool for spotting irregular port usage. Their web site provides information on well know ports with links to the IANA. They have other useful products on their support page as well (see figure 2-4).

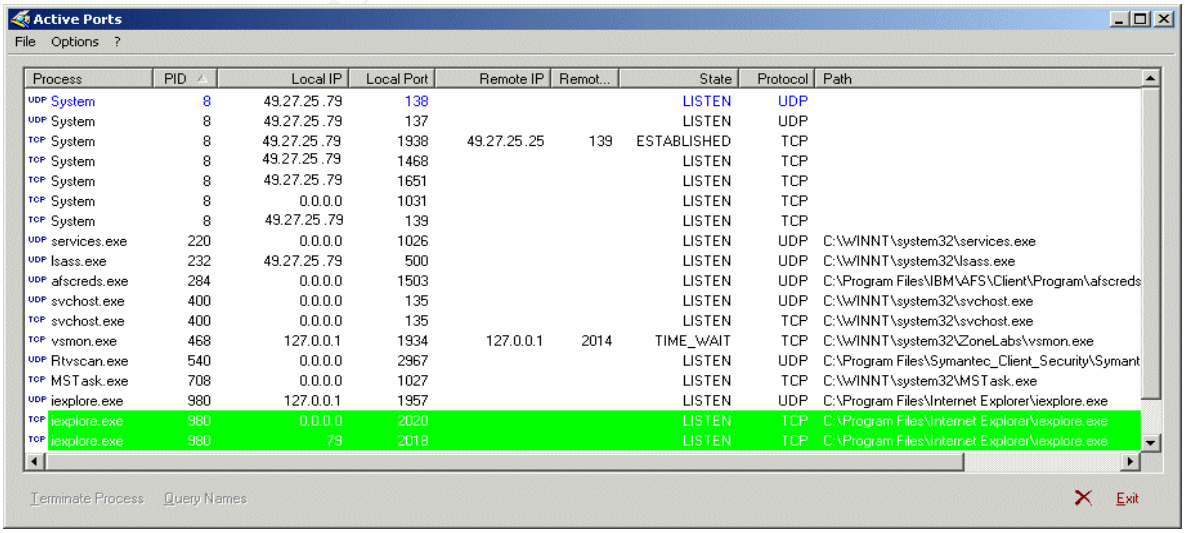

Figure 2-4. Active Ports Example

By reviewing the port information you can see if there is any suspicious port activity or extra ports that shouldn't be there. One thing to look out for is *Trojan Ports*. So how does one know what ports should and should be there? And what is a Trojan Port? Trojan ports are open ports created by hostile software dropped off on your machine so they can easily to get back into your machine at a later date. They can be introduced through downloaded software or opening an email attachment (something you should never do if you don't know the source). If the port shown is suspicious and not in the well know port list, you can check it against any published list on the web. Here are a couple of good links than can explain things:

http://www.simovits.com/sve/nyhetsarkiv/1999/nyheter9902.html

http://www.iss.net/security_center/advice/Exploits/Ports/

In addition, if you don't recognize a service, you can look that up as well.

The explanations at the ISS site are pretty good as you can see in figure 2-5 and also cover the well-known ports. Clicking on the "Back Orifice" link at the bottom, for example, will take you to a page that describes in detail the history of the exploit, how to fix it, and how hackers use it (if you are so inclined).

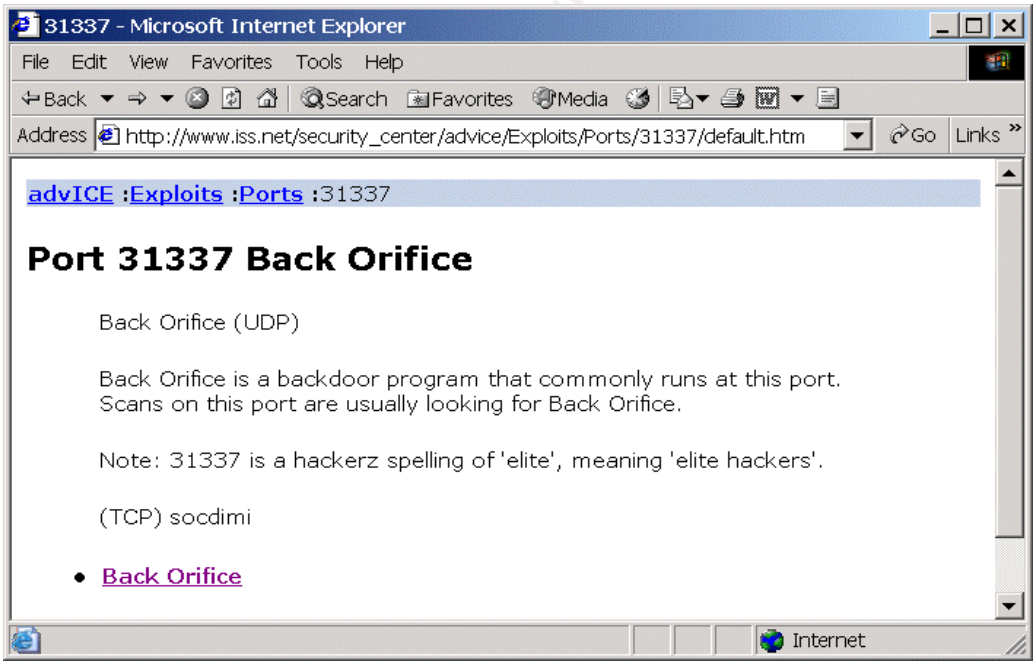

Figure 2-5. Back Orifice Port Defined

Most of the professional anti-virus software will check for Trojans, but recently there may be a trend to get a way from that. There is a web site available that will scan your computer for Trojans at this URL: http://www.trojanscan.com/

Now then, what about privacy? Some of the freeware that you download may contain additional applications bundled with the software's installer file. "Third-party

applications bundled with this download may **record your surfing habits, deliver advertising, collect private information, or modify your system settings"** (download.com, 2003). This is commonly known as *Spyware*. If you must take a chance of downloading certain freeware, then there are a few products that can detect and eradicate it. I found two worth mentioning, Spy Sweeper and Ad-aware. Ad-aware is by Lavasoft, free (although there are advanced versions at a price), and easy to install and can be download from http://www.lavasoft.de/software/adaware. They also provide signature file updates.

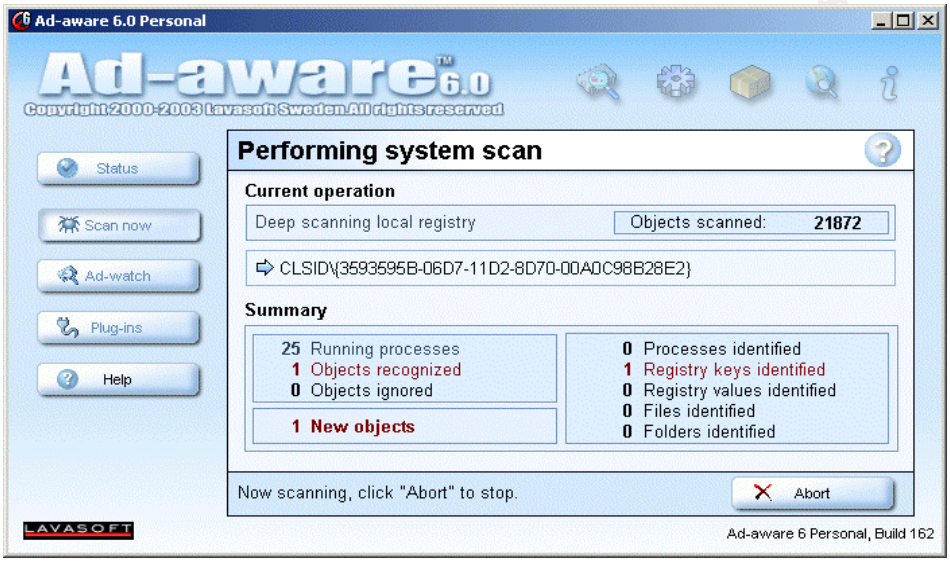

Figure 2-6. Ad-aware During a Scan

Figures 2-6 and 2-7 show Ad-aware finding something suspicious during a scan. At home, I find that there are a lot of tracking cookies that show up in my wife's cookies each time she browses the web. She is mostly looking for vacation spots and camping locations. Most of them are innocuous, but one can still be tracked this way as well by seeing just where you have been. Sometimes is a way that they get you on a mailing list (depending on who your browser is configured).

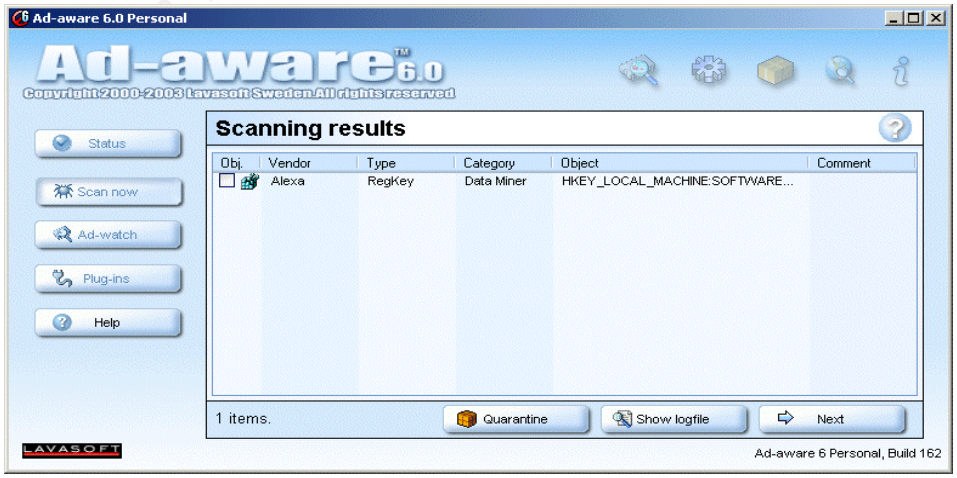

Figure 2-7. Ad-aware Finding Spyware Reference in Registry

While there are many other tools out there, these are the ones I find quick, easy, and safe to use. They can be executed whenever you feel a need as a basic security check or to baseline your system. There are also more advanced tools for the security professional sold at a premium, but some are not worth the investment for home use. Later on I will cover some vulnerability assessment tools than can be used. Some are available with the Windows OS while others can be downloaded from the Microsoft Security web page and other places.

3.0 Basic Defenses

As previously mentioned, a good defense is for you to know what your system does normally. This is called base lining your system. Before you do that, you might want to tweak your system a bit towards a more secure environment by:

- Turning off unused services
- Enabling event logging
- Setting a better local security policy

Turning **off** services that you don't use not only improves your security defenses, but also improves system performance. To turn off unused services you first go to Start >> Settings >> Control Panel and double click on *Administrative Tools*. From there, launch *Services*. Run down the list and find things you don't and turn them off (it is easier if you sort by Status to see what has started). Computer browser is not needed if you are the only computer on you network, DHCP Client if you have a static IP address, and so forth. To stop a service, right click on the item for the menu and select stop. To disable it all together go to properties and select disable for *Startup Type*. You can also come here to check if you expect a system compromise. Telnet being turned on may indicate a break in for example. Here is a list of other services to consider disabling. If you are not sure, leave them on or check the web for there usage:

- Remote Registry Service (for sure)
- Telephony
- Fax Service
- NetLogin

Turning **on** event logging is a must if you want to ever determine what went wrong or if a hacker has paid a visit. While there are lots of recommendations out there, there are only a few you really need for the home system. To start configuring, launch the *Local Security Settings* program from the Administrator Tools, and then click on *Local Policies*. To enable event logging, click on the *Audit Policy* section (see figure 3-1). You should at least elect to audit login and management events both for success and failure. In addition, consider privilege use.

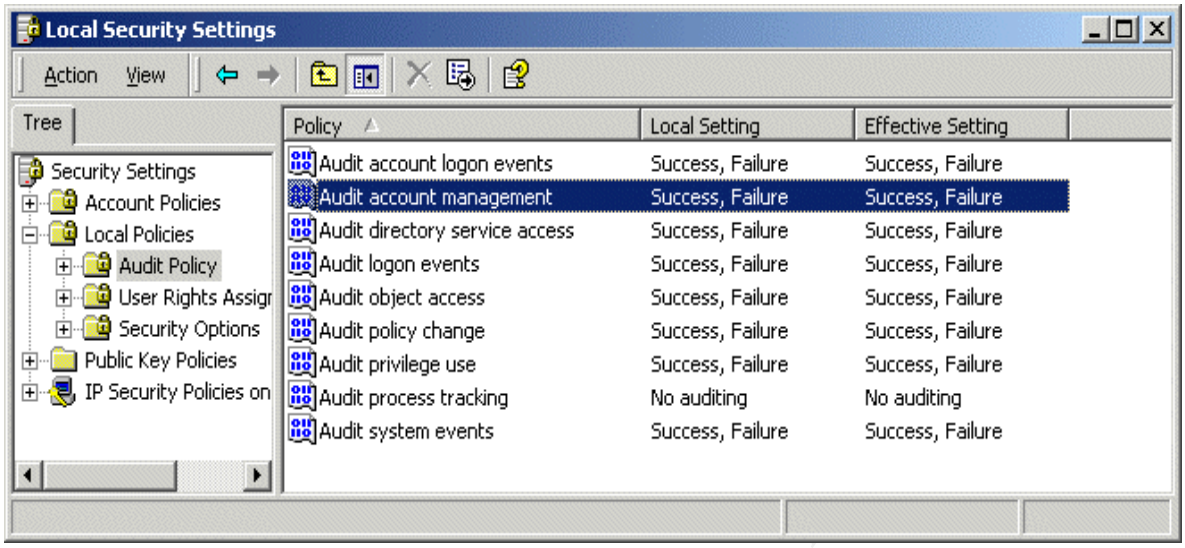

Figure 3-1. Audit Policy Settings

The local security policies that you get out-of–the-box from Microsoft are limited and you should improve them. Some of these are a must and shouldn't be ignored. As an example, If you intend on enabling NetBIOS and shares for other computers in your home network, under the *User Rights Assignments* to allow only specific users to access the machine. Under *Security Options*, make sure that the *Additional restrictions for anonymous users* is not set to "None, relay on default permissions".

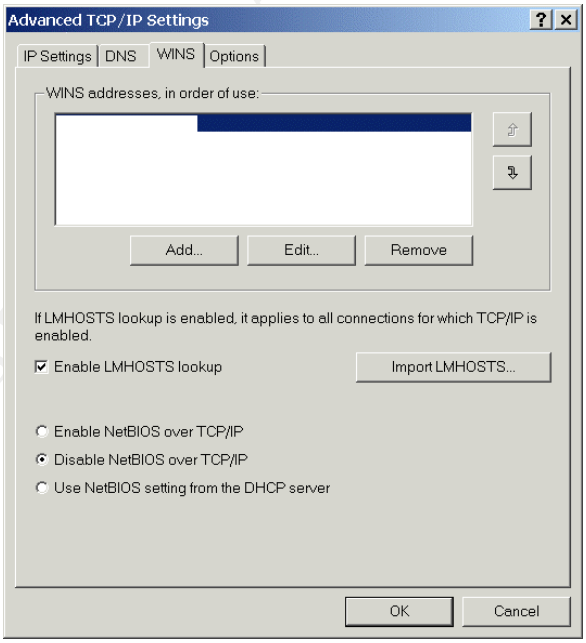

Figure 3-2. Temporarily Disabling NetBIOS

To check what network components are installed on your machine, open up the Local Area Connection Properties window by holding down the <Alt> Key and double clicking on *My Network Places*. Then view the properties by right clicking. If you won't

be sharing Printers and Folders, uncheck “File and Printer Sharing for Microsoft Networks”. If you want to share, you can quickly disable NetBIOS when you’re done by opening up the TCP/IP Properties window and going to Advanced >> WINS and clicking the disable button as shown in figure 3-2.

Microsoft has their Baseline Security Analyzer (MSBA) that you can you download and use to check your OS as well as Microsoft Office products. This may help with the decisions you can make about setting your local security policies. MBSA scans your machine and not only reports vulnerabilities but gives you good marks if you have there suggestions implemented already. Microsoft states that it “provides a streamlined method of identifying common security misconfigurations”, but beware: it may not be in sync with the windows update website (MSCE world.info, 2003). Nonetheless, it is a good tool and can be downloaded at this URL:

www.microsoft.com/downloads/results.aspx?productID=&freetext=MBSA&DisplayLang=en

Figure 3-3. Clip of MSBA Scan Results

The following URL points to a great resource that will provides tips on what you can do to lock down your computer: http://www.sanx.org/tips.asp?action=security. Consider it an augment to the MSBA. For the hardcore or those who want a challenge, there are professional assessment tools out there at a premium. One such tool is the ISS Internet Scanner. You can go to this URL to download a trail version if you are so inclined:

http://www.iss.net/products_services/enterprise_protection/vulnerability_assessment/scanner_internet.php

Now you can by baseline your system so you have a reference point that you can occasionally check back to when you feel the need (you’ve done something stupid like

installed Morpheus to download MP3s) or your system seems unusually slow. The tools discussed in the Self Check section can be used now and then again later on to see if something has changed. This means write is down and/or take snapshots.

It probably goes without saying that you should have anti-virus software installed and keep it updated weekly. Some of the better ones are from McAfee and Norton who provide automatic updates. Whenever you down load software, the first thing you should so is scan it. If it is a zipped file, make sure your virus scanner is set up to look inside.

Finally, don't stay connected to the Internet when access is not required. Unplugging the cable from your NIC is the quickest method, but sometimes this causes problems. If you have a personal firewall, then using it to lock out the Internet is a better solution. If you are going away on vacation, just power the computer off.

4.0 Installing the OS

For this part I am assuming that Microsoft Windows 2000 Professional is the target OS. Windows XP may be similar, but according to the SANS Security Essentials course, Windows XP is just not stable enough to trust since it is new. In addition, the home version is awful so if you must, make sure you have the professional version. Windows 2000 has been out awhile and I feel that keeping up with all the security patches is good enough for the home. However, one must still be cautious about the Internet Explorer, since it comes bundled with the OS.

If you really want to make sure your system is secure, you should wipe the drive before installing the OS. This includes the boot record. Then install everything from scratch (it is never recommended to install over older or existing operating systems). Before you start, you first must collect everything you need in advance. I'll assume that you have a good working copy of the OS install disk with license key. But before proceeding to install, go to the Microsoft web site and download the latest service packs for the OS and IE. Don't even think about putting your newly configured PC on the Internet until you have it patched. Always get the full downloads (not the install links) and save them on CD-ROM. As an example you would first go to their web page where the download appears, right click on *Download Windows 2000 SP3* and then *Save Target As*. After that, make sure you get the Cumulative Patch for Internet Explorer and/or Version 6.0. To quote Microsoft directly from their TechNet page: "During the installation process, a system will be vulnerable to exploits of known vulnerabilities until the installation has completed and all applicable service packs and hot fixes have been applied". The best starting point is more information is here:

http://www.microsoft.com/windows2000/security/default.asp

Now you can start the install. I recommend that you partition the drive in to C: and D: drives and install the OS and applications all on the C: drive. Keep the D: drive for your data (documents, spread sheets, and project files). This segregation makes it easier to restore incase of a disaster and it simplifies backups. You'll have to determine

the size of the partitions based on what you have, leaving room for growth. (If you blow it and have to change later on, third party tools such as *Partition Magic* are available for a low price.) If you have any additional drivers for your devices like the video adapter or NIC, now is a good time to install these as well.

After the basic OS install, apply the service packs and the IE upgrade before you put your apps on. Go back to Microsoft and check for updates. The easiest way is to open the IE up and pull down the *Tools* menu to *Windows Update* and let Microsoft scan for updates. At this time, you should only be concerned with "Critical Updates and Service Packs". For the other suggestions you will have to know your system or perhaps come back here later.

If you have any Microsoft Office products to install, they should be installed before the rest of your applications. I have found that in the past it is best to get this squared up first. After they are installed, you can go back to Microsoft to and check for updates and security patches this URL: http://office.microsoft.com/productupdates

It is now time to set the security policies, as I described in the Basic Defenses section. This is also a good time to secure up your web browsers and turn off services you know that you won't need.

At this point you are pretty well set up and you may want to make a disaster recovery backup and label it "Virgin OS Install". I usually like to go a step further and install some other common or basic third part items like Abode Acrobat Reader, the latest version of Real Player, Anti-virus software, and so forth, before I do the back up. The reason for this is that it is sure a lot easier than going through this rigmarole again! After the backup, I recommend installing all of your stable applications, utilities and tools, and anything else that you need for your home system (including your personal firewall if you will be using one one), then do another disaster recovery backup and call it "Full Install" or "Baseline Install". Now you two points of reference to fall back upon if your system ever became clobbered.

To wrap things up, I recommend installing a raw version of Windows on C:\WINNT2 without networking and editing c:\boot.ini to indicate the ER boot choice on the system startup screen. Example:

```
[boot loader]
timeout=10
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Win2K Professional -Norm boot" /fastdetect
multi(0)disk(0)rdisk(0)partition(1)\WINNT2="Microsoft Win2K Professional -ER boot" /fastdetect
```

It is very useful to have a second boot in the case of emergencies. If fact, I used it this weekend when and it was a lifesaver. A driver (mxlw2k.sys) installed by Music Match Juke Box V7.5 got corrupted. Since their install had hooked into the CD ROM driver, I was dead in the water with the *blue screen of death*. It was simple matter to reboot with the 2nd OS install and correct the problem.

5.0 Personal Firewalls

So what is a personal firewall? It is a software-based tool that resides on a personal computer to help avert attacks from hackers or intruders from accessing your personal data. There are many types of industrial strength firewalls available, which do everything from full *stateful packet filtering* to VPN and proxy server. For the home, the personal firewall is a scaled down version of this technology. Some don't even have any stateful packet filtering or if they do, it is a limited version. But, as a plus, they include privacy controls, block popup ads, and may provide for DMZ configuration. Several have been in the market for a while; Zone Labs' Zone Alarm/Pro, Tiny Software's Tiny Firewall, Network Ice's BlackICE Defender (recently acquired by ISS), and Deerfield's VisNetic Firewall. BlackICE is a good firewall to use in the business, since a server version is available. VisNetic and Tiny firewall do stateful packet filtering, as does Zone Alarm to some extent. VisNetic and Tiny have more granular setup and control. Symantec and McAfee are also joining the market with theirs. To be competitive most home versions list from $34 to $69 and have on-line support.

Since I have mentioned stateful packet filtering a few times I'd better explain it. In basic (or static) packet filtering, firewall compares each IP packet header to against a list (called an ACL or rule set) to determine whether to pass it (permit) on or drop it (deny). Your standard router is capable of this as well as the rudimentary TCP/IP filtering available in Windows 2000 Professional and Servers. Stateful packet filtering is sometimes called *dynamic packet filtering*. This is where the software examines the packet and only allows it in if you (on the inside of the firewall) make initiate the connection. Think of it as a temporary rule or ACL being opened up for you session that goes away when you're finished. Tiny Personal Firewall 4.5 includes a standard bi-directional stateful packet inspection firewall (Tiny Software Inc, 2001). The ultimate is a proxy firewall whereas it completely takes over by managing the connection on both ends (host and client). It insures that the packets are well behaved and don't pose a problem to the client on the inside. The trade off here is lower performance or throughput to the internal network. Personal firewalls for the home don't usually contain this feature.

Tiny Firewall	BlackICE	ZoneAlarm
Excellent product for setting up a DMZ and providing detailed filtering rules. Any form of traffic can be filtered, logged and monitored. The remote administration capability makes it very easy for IT admins to support telecommuters. The typical user will have difficulty maintaining and understanding the complex filtering rules, but with an additional product for alerting (like BID), WinRoute can be used to set up a detailed DMZ and provide full control over the remote user environment.	BID's alerting capabilities are first rate. DNS lookups can easily resolve names and point to the advice database of attack signatures. The software is very easy for a typical user to configure and maintain. Combined with a product such as WinRoute, BID is a robust security solution.	ZoneAlarm provides very good security for a remote system. It's easy to install and configure. For end users who don't need onstant support or remote administration of their system, ZoneAlarm provides comprehensive security that can keep the host system safe from known and unknown attacks.

Figure 5-1. http://www.infosecuritymag.com/articles/july01/charts/cover_story_chart.pdf

Information Security Magazine did a comparison of BlackICE, Zone Alarm, and Tiny Firewall in 2001. Since then there have been many improvements on these products (see the whole story at their website). See figure 5-1 for their results.

Since this research was over two years ago, I decided to do some of my own comparisons. I have talked to co-workers and other IT professionals and have discovered that the two mostly used personal firewalls are Zone Alarm any Tiny Firewall. I personally like Zone Alarm better because it's easy to configure, it learns and it is free. The Pro version ($39) comes with one-year support, has privacy features, and a popup ad blocker. A nice thing about Zone Alarm is when you get an alert you can easily click on "More Information" and get a detailed report about the alarm and where (and sometimes who) it came from. In the latest version they call it "Hacker ID" (see Figure 5-2). If you want to have more control or granularity over what is going on then Tiny Firewall is the best bet. In addition, application authentication can be done through MD5 hash for greater security against applications that have been altered to contain malicious code. The down side is that is manually intensive and in comes out of the box with everything protected so you have to configure it to get anywhere. Tiny Firewall comes with a 30-day "demo" version that must be registered ($39) to continue to operate past that time.

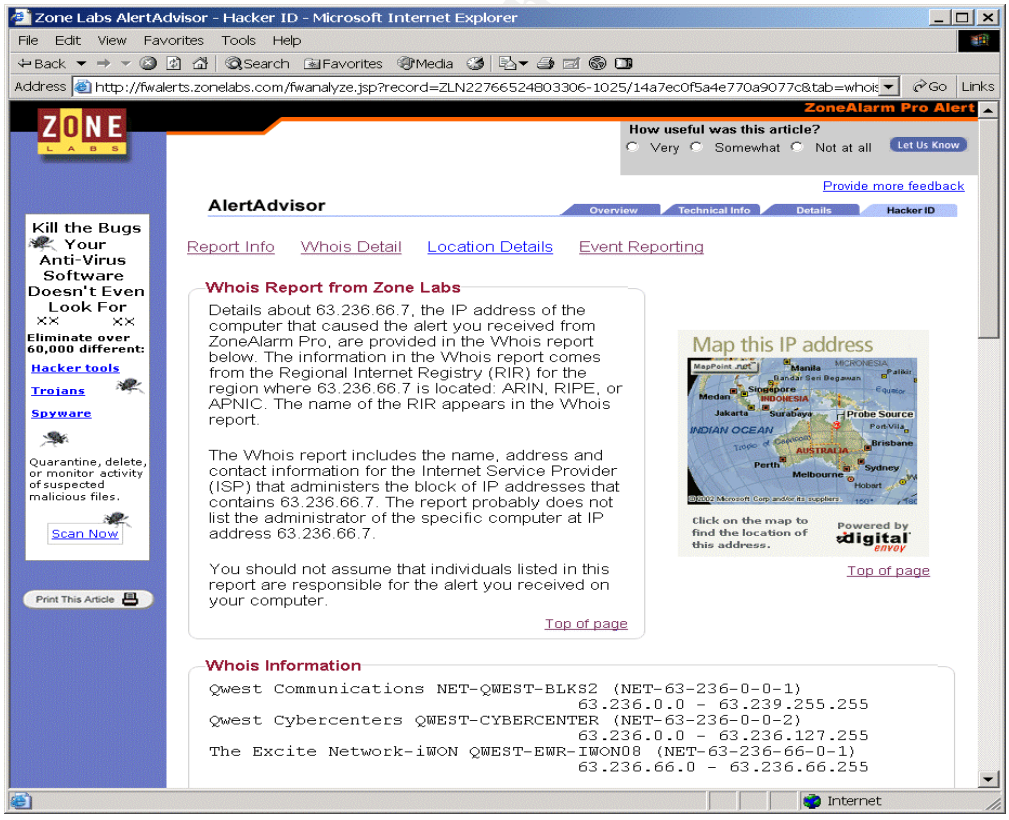

Figure 5-2. Zone Alarm's Hacker ID

I didn't analyze BlackICE since is does not provide outbound filtering. I find that a must in a firewall. If you want to make sure your firewall has outbound filtering, download and run LeakTest from Gibson Research at http://grc.com/lt/howtouse.htm.

Zone Alarm detects your network and it starts blocking immediately and is ready to learn. This is great for the neophyte. Its single page pop-up with tabs allows easy access to the log, firewall zones, configuration, and program control status. With Tiny Firewall you need an understanding of rules and rule sets, along with TCP and UDP services, and is probably best left for the experience or security professional to use. It's interface is a "Admin Tool" which allows configuration of application security (Windows Security), Intrusion Detection System (IDS) and the Firewall it self. It has 2 modes of configuration: Easy and Advanced. It also has an activity monitor window which you can view all open connections (ports) and their controlling process. When you move to another network you have to reconfigure Tiny Firewall but Zone Alarm seems to catch on right away. A nice thing about Tiny Firewall that Zone Alarm doesn't have is that it has an alert when you download and/or execute new software that allows you a chance to add it to the trusted application group or not. Zone alarm only checks software that accesses the network.

To verify the effectiveness of the personal firewall there are vulnerability assessment tools available. nmap is a tool to scan your PC or your network and is free from insecure.org. And, as I covered in the Self Check section, Gibson Research (grc.com) has LeakTest and in addition, *Shields Up* in which they will scan your system and report back their findings in about 30 seconds or less.

6.0 Hardware Firewalls

One may ask "Why do I need another firewall when I already have a personal firewall on my PC?" To quote Steve Gibson: "there is no better and more secure solution than running a single, external, Linksys NAT router - providing redundant external intrusion protection - coupled with copies of the FREE ZoneAlarm firewall - providing the PC industry's most comprehensive internal extrusion management." PC Magazine answers this question with: "Hardware firewalls provide an additional outer layer of defense that can more effectively hide one or more connected PCs". They inherently protect you against ping discovery. If the hacker attacks you he is attacking the firewall box (which can't do much) and not your computer. Now bear in mind that they are not as robust as the professional security appliances for the workplace that provide things like *Statefull Packet Inspection*, for example.

For the home, these hardware devices can be purchased for about $70-$100 and will extend protection to the whole home network. They have various names based upon the manufacturers preference for sales and marketing purposes (Firewall/Switch, Cable/DSL Router, etc.), but nonetheless they afford basic protection. Some even have wireless access points incorporated and/or VPN. They all provide Network Address Translation (NAT) and address management (DHCP), allow many computers with only one ISP provided IP address, have a web interface for configuration and status, and

work nicely out-of-the-box with little or no setup. Most all seem to have 4-ports (or segments) that are separately configurable and you can put hub on each port to fan out about 250 IP addresses. The great thing about this is that you can block everything except http/https (port 80 and 443), as an example, on one segment while allowing other ports on the others.

Some of the popular brands are Linksys, Netgear, D-Link, and Asanti. Visit http://www.firewallguide.com/hardware.htm for further information and comparisons.

7.0 Monitoring Your System

One surefire way to see what is coming into and going out of your computer is to employ a packet monitor. WinDump and Ethereal are the tools that come to mind. WinDump is a command line utility while Ethereal is a GUI tool. To use ether one, you need to download and install WinPcap. They are available at:

Ethereal - http://www.ethereal.com/

WinPcap & WinDump - http://winpcap.polito.it/

Many times I have found Ethereal a lifesaver. I have discovered spyware and other mysterious things going on with these tools. You can also use Active Ports as described in the Self Check section. In addition, look at your personal firewall logs to see if someone was trying to get in. If you see a lot of attempts by the same source IP address on different ports with in a short time period, it would indicate a scan. Check you event logs at the times corresponding to the scan.

You can use the build in Windows tools like *nslookup* to resolve an IP address or *tracert* to find out where the probe may of came from. There more advanced tools that are commercially available at a small price. I recommend either NeoTrace Pro from McAfee ($39) or VisualRoute from Visualware ($49). Incidentally, you can use the VisulaRoute server for free at:

http://www.visualware.com/visualroute/livedemo.html

But you must use Netscape for it doesn't work with IE. Hit the snap button to get a plain text copy for printing. Bear in mind that this is a trace from their server and not your machine. The purchased versions use lookup techniques to find out which ISP or institution owns the address and/or subnet and reports it back. One thing to beware of is that this won't help much if the source IP address is spoofed.

8.0 Wireless

Wireless in the home is not as big of concern as it is for businesses that have a lot of proprietary information, but nevertheless you should be careful. Just remember one thing: **It is <u>not</u> secure.** If you don't believe this just visit this URL:

http://www.iss.net/wireless/WLAN_FAQ.php

If you want to take a chance and have the convenience of wireless then you should do these basic things:

- Locate the access point in the center of your house
- Put it in the DMZ (if applicable)
- Turn on WLAN security features
    - Change SSID (Key ID)
    - Force MAC Addresses
    - Set and Require passwords
- Monitor packet inputs
- Turn it off when not in use

Locating the access point in the center of the house sounds logical because that would be a good way to get the most coverage, but it helps with security as well. If you place it near a window street you may be asking for trouble. Do you know your neighbors? If you can, put it in the DMZ area using your DSL Router/Firewall do it (most of these appliances that incorporate wireless have that option).

Turn **on** the encryption (or WEP). It may not keep out the veteran hacker but it will keep out the casual surfer. Still WEP key ID and MAC control are not enough. Sessions can be hijacked so disable wireless access when not in use. You can also monitor packet data on you LAN with WinDump or Ethereal for additional security. I just don't use it.

9.0 Spam

Spam is defined to be "unsolicited e-mail usually sent to a large number of people that usually tries to sell something or get people involved in some sort of scam" as per Ernst Orlando Lawrence Berkley National Laboratory. Simply put, it is an overload of unwanted junk email messages and is a growing concern in both the business world as well as the home as it continues to grow. Marketers use this to target email users to buy their products. According to McAfee worldwide studies have shown that these "junk messages are being estimated between 25-50% of all email". Other sources suggest that it is even worse for the home user since they are doing more on-line shopping and browsing the Internet, as compared to the workplace, and hence; more susceptible to this. Spam in the workplace may mean lost productivity (i.e., the bottom line suffers), but at home it is a nuisance that can be compared to a Distributed Denial of Service (DDoS) attack if it gets bad enough. Why? Well, considering that most home user's mailboxes are very limited in capacity, they fill up with junk mail rather quickly causing important messages to be missed. I actually had a real life problem while attending the University of Phoenix. We had a team project due and were collaborating on-line as we neared the completion date. There was one student being flooded with so much junk mail, it impacted our assignment. He was the prime contact for inputs for the paper and wasn't receiving them from the team members. Needless to say it was a stressful situation as the dead line approached.

So how can the home computer family cope with this? The best place to stop it is at the mail server, but the home user can't really do this. He/she can change to a better provider that offers some protection. The free ones just don't provide good service and they sometimes spam you themselves. Remember the old adage "you get what you pay for". The two major competitors, AOL and MSN both claim they can reduce if not eliminate spam, but don't believe them entirely. I find that Verizon.Net mail that comes with my DSL is a good choice. In any case, you still must watch out. With those computer generated email addresses, it is really hard for any provider to really control it. There is still some manual work involved on your part in any case (you may still have to move messages to the junk mail bin).

According to the Berkley Labs you should never respond to spam mail, especially to the instructions to remove you from the list. This just confirms that you have a legitimate email address. The home user could have different email accounts: A primary one strictly for business, school, and close family while having another (less important one) for everything else. This primary address should not be casually given out. When the less important one becomes too inundated to use with spam, dump it and get another. Another thing one can do is to give a phony email address to those sites where it is required prior to obtaining information or downloading free software. (Remember: Don't forget to check for spyware after the install, since that is also a way to get on junk mail lists as well!)

There are some services available to those who have web mail that can help. Mailshell.com is one of those. They act as a buffer between the user's real email address and a list of aliases the user and his family can generate. Mailshell is a web interface between your real address and the rest of the world. There service boasts having "disposable addresses" which can be set to expire in so many days, or you can just remove an alias at any time and make a new one. Of course there is a price to pay: "The company supports itself by selling three lines of advertising that appear at the end of incoming messages" (News.Com). Zone Labs has just released a product called Mailwasher Pro.

For more tips from Microsoft (including setting up Microsoft Outlook, see the Crabby Office Lady's tips at:

http://office.microsoft.com/assistance/2002/articles/colNoSpam.aspx

10.0 Privacy

Protecting your privacy is pretty important in this day and age of electronic communications. It is some times hard because of the accessibility of public records on the Internet for a small fee, or even sometimes for free. As an experiment, I tried to find out information on my deceased stepfather without paying for it. I went to google.com and started searching for outfits that offered services. Right away I found his Social Security Number along with his last known address and other information. The government revealed this in some posted documents, since he was a veteran and interned at the Riverside National Cemetery. One of the ways to help is to have an

unlisted phone number, although it only foils the free searches sometimes. If you sign up for services or information, make up a phony email address. You can also limit your on-line purchases. You can also take steps to see if your identity has been stolen by enrolling in on-line credit watch programs. Equifax and TRW each have one. The American's Most Wanted web site offers a service for only $5.00 a month. Microsoft also has some suggestions at:

http://www.microsoft.com/security/articles/saferbrowsing_personalinfo.asp

Here is a quick list of what you can do to protect your personal information:

- Encrypt sensitive documents
- Use wipe utility to delete
- Degauss discarded hard drives
- Delete Cookies and clear cache
- Tighten browser security level
- Clear pagefile

You should encrypt all sensitive documents and email correspondences that contain personal information using a tool such as PGP by Network Associates. Make sure you use a secure or privacy delete tool when you delete unencrypted files. The PGP tool kit has a utility to wipe free space on you hard drive. When you upgrade your computer with a new hard drive, degauss or do a security wipe of your entire hard drive you are discarding. Formatting is not enough.

As another precaution, you should always delete your cookies, and clear the disk cache after doing financial business on the Internet. In the IE, you would pull down the *Tools* menu and select the *General* tab of Internet Options. If you use the Netscape 7.0 browser, pull down the *Edit* menu, go to *Advanced/Cache* to clear the cache and *Privacy & Security/Cookies* and click on *Manage Stored Cookies* to clear the cookies. I recommend clearing the history also

Another important thing to do for protection is to disable SSL version 2 in your browsers. This is the older less secure encryption method and some online banking and consumer sites may still support this. SSL version 3 is more secure. For IE, go to the Advanced Internet Options tab and uncheck "Use SSL 2.0". If you use the Netscape 7.0 browser, pull down the Edit menu, go to Preferences/SSL and uncheck "Enable SSL version 2.

If you have a Personal Firewall, use it to turn off tracking cookies or restrict them in your web browser security settings. If the site doesn't load because of your restriction then maybe you should go elsewhere.

Finally, open up the Local Security Policy manager and set the security option to *Clear virtual memory pagefile when system shuts down*. The ultimate solution would be to have one computer for browsing the Internet and another for your projects and

personal data, which would never be connected. This is not usually possible and would be a great inconvenience to many.

11.0 Physical Security

Physical security is not as strong an issue as it would be in the work place where you have a lot of traffic. But in some cases, you may want to apply some controls. As an example, my son has LAN parties where 3 or 4 friends come over and game. Since I am not always home when this occurs, I elected to do three things:

- Password protect the BIOS setup
- Disable booting from Floppy or CD-ROM
- Disabled Autorun

Now these guys seem okay, but you never know, so why take a chance. If you have Windows 2000 you can disable *autorun* by modifying the registry. Microsoft presents a convoluted solution at their MSDN web site. An easier method is to run *regedit*, to set the following key to 0, and reboot the machine:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CDRom

If the value is not there, you can create it. The data type is DWORD and Value name is Autorun.

If your system is a laptop and you travel, keep an eye on it at all times. Recent new articles indicate that laptop thefts are on the rise for steeling both corporate and private individual data. For added security, consider using an encryption device (one that plugs into the USB port) or disk encryption software. A good URL to visit for more information is:

http://www.securityworld.com/library/workplacetech/laptopsecurity.html

12.0 Good Practices and Common Sense

Even if you have your network secure, there is nothing better than practicing *Safe Interneting*. Some of the more important things to remember are password security, being careful from where you browse and download software, and being smart about email attachments.

Everyone knows that to protect your information you need a strong password (a mixture of 7 or more alphanumeric and special characters). But what many people don't realize is that you shouldn't use the same password that you use for on-line banking for other things like email. For one thing, public email services don't generally use a secure site (https) so they aren't encrypted. For another, if someone gets a hold of your password at one place he/she could get access to all of your accounts. One more thing about passwords -- don't use variations of the same password like adding different numbers at the end. That is lame!

Beware of some institutions that don't encrypt you password when it is stored (https is not enough). I was once horrified when I called tech support with a logon problem and they read back my password to me. I tend to keep away from those sites and those that don't let me enter a strong type password if they deal with my personal information. Here is one thing that really scares me: Some banks, like the bank I was with, will automatically enable your on-line account access with your SSAN as the account name and last 4 of your SSAN as your password. These accounts are dangerous if you never use them or know such a service exists.

Always check out the site that offers software download. As I mentioned before, scan it for virus before using it and for spyware after installing it. Some software is hard to uninstall or won't uninstall completely. You can purchase a tool that snap shots you're registry before and after the install. If something doesn't work out right it can help you surgically remove it. It is called Active Registry Monitor (ARM), sells for $40, and is found at: http://www.protect-me.com/arm/. SmartLine Software also claims it helps detect Trojans. After you install, check the processes and services running so you are aware of what was done.

The CERT recommends that you disable Java Script and ActiveX in your browsers for any site you are "not familiar with or do not trust." I have taken it one step further and have created a user account on my home computer with no privileges except to the user area for the browser. I use Netscape 4.77, since it is a lot easier confining that user account's permissions to the one directory (i.e., C:\Program Files\Netscape\users\surfer). I use that account when I go to those kind of places on the Internet.

Email attachments are how a lot of viruses spread these days. Attachments can also contain malicious code that is not recognized as a virus yet. They are commonly contain in Microsoft document macros and files with hidden extensions. For an example, the message might say "Hey! Check out this great picture of Anna Nicole in the nude." The attachment would be something like anna_nude.jpg.exe and you would never be the wiser (boys will be boys). The default for Windows OS is to hide extensions for known file types. You might consider disabling this option, but never the less you should never open an email attachment if you don't know where it came from.

13.0 Conclusion

So here is a quick road map to a safe secure home system:

- Start clean with a new OS Install
  - Wipe the Drive
  - Install all security patches
  - Turn off unused services
  - Improve the security policies
    - OS
    - Browser(s)

- Add a Personal Firewall and Virus protection
- Base line the system and correct problems
    - Active Ports
    - Packet Tracer
    - Ad-Aware
    - Built in OS tools
    - Record results
- Back it up for disaster Recovery
- Check logs and monitor output from time to time
    - Active Ports
    - Ethereal
    - Compare to baseline
- Consider
    - Adding a hardware firewall
    - Physical security
    - Data encryption

I want to leave with this important note. A single layer of protection, like a personal firewall in itself, is not complete for good home network or system protection and sometimes leads to a false sense of security. One must be prudent in all areas, like keeping the OS updated with the latest security patches and applying a good local security policy. Microsoft's Baseline Security Analyzer tool can be used check for potential vulnerability problems and there are many tools and references available on the Internet. Anti-Virus software and security patches must be kept up to date. Those connected full time to the Internet through DSL or Cable-Modem should be cautious and disconnect while away. One should practice good password security and encrypt sensitive data (items containing bank account numbers, SSANs, tax records, and legal documents). A DSL/Cable-Modem Firewall to provide network address translation should be used to protect the internal network. Since these are appliance devices and are sort of a proxy, you are less likely to be vulnerable to an attack. Finally, one must use self-restraint in what they do when they are on the Internet and not let their guard down. Investigate anything that looks suspicious. Oh, and don't forget backups! The bottom line here is to use all the security options and protections you can.

References

Bahadur, Gary. “Personal Firewalls Under Fire.” Information Security Magazine. July 2001. URL: http://msdn.microsoft.com/netframework (May 2003)

CERT Coordination Center. “Home Network Security.” 5 Dec 2001. URL: http://www.cert.org/tech_tips/home_networks.html (May 2003)

Cisco Systems, Inc. “Cisco SAFE: Wireless LAN Security in Depth.” 23 Apr 2003 URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm (June 2003)

CNET Networks, Inc. “Morpheus 3.1 *popular new*." download.com. 2003 URL: http://download.com.com/3000-2166_4-10205715.html?tag=just_in (May 2003)

Cole, E., Newfield, M., Millican, J. GSEC Security Essentials Toolkit (2002). Indianapolis: Sans Press

Berkeley Lab. “Preventing Spam (Unsolicited E-mail).” 8 May 2003 URL: http://www.lbl.gov/ITSD/CIS/CITG/email/spam-blocking.html (May 2003)

Curtin, C Matthew. “Firewalls FAQ.” 2 Jul 2001. Ohio State University Dept. of Computer and Info. Science. URL: http://www.faqs.org/faqs/firewalls-faq/ (June 2003)

Daniel Petri Ltd (1998). “Windows Update Problems.” MSCE world.info. 1998. URL: http://www.petri.co.il/wu_problems.htm (May 2003)

Gibson, Steve. “Hardware Firewalls/NAT Routers." 3 Nov 2001. Gibson Research Corporation. URL: http://grc.com/lt/hardware.htm (June 2003)

Hummel, Robert. “How It Works: Personal Firewalls.” 5 June 2000. PC World Magazine. URL: http://www.pcworld.com/howto/article/0,aid,17012,00.asp (June 2003)

Internet Security Systems. “BlackICE Overview.” URL: http://blackice.iss.net/index.php (June 2003)

Network Associates. “Anti-Spam Protection.” McAfee Security. 2003 URL: http://www.mcafeeb2b.com/products/anti-spam-protection.asp (June 2003)

Markus, Henry. “Home PC Firewall Guide.” 5 Jun 2003. URL: http://www.firewallguide.com/ (June 2003)

Microsoft. “Browsing Safety: Help Control Your Personal Information Online.” 21 Apr 2003.

URL: http://www.microsoft.com/security/articles/saferbrowsing_personalinfo.asp (May 2003)

Microsoft. “Crabby's Top 10 Spam-Fighting Tips.” Office Assistance Center. 2003 URL: http://office.microsoft.com/assistance/2002/articles/colNoSpam.aspx (June 2003)

Microsoft. “Microsoft Security Tool Kit: Installing and Securing a New Windows 2000 System.” TechNet. 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/w2knew.asp (May 2003)

Livingston, Brian. “Blocking Spam Before it Slams You.” News.Com 6 Jul 2001. URL: http://www.mailshell.com/corporate/news/aboutcompany_newscnet070601.html (June 2003)

Ziff Davis Media. “Hardware Firewalls: D-Link DI-604, Linksys Firewall.” PC Magazine. 23 Oct 2002. URL: http://www.pcmag.com/article2/0,4149,646316,00.asp (May 2003)

SANX Software Services. “Windows 2000 and Windows XP Tweaks and Tips.” 2003. URL: http://www.sanx.org/tips.asp (May 2003)

Tiny Software, Inc. “TPF 4.5 Overview: Firewall Security.” 200. URL: www.tinysoftware.com/home/tiny2?s=1252655227594282221A1&la=EN&va=&pg=tpf4_overview

Zone Labs, Inc. “Zone Alarm Pro.” [Computer Software] 2003. URL: http://www.zonelabs.com/store/content/catalog/products/zap/zap_details.jsp (May 2003)