Global Information Assurance Certification Paper

The Holey Internet

Research on Topic in Information Security

GSEC Practical version 1.4b
Option 1
By
John Robert McClure

Abstract

This paper addresses a common issue, which is the majority of people do not fully appreciate or understand the battles that are going on in cyberspace with respect to security. Most users (and some administrators) are simply oblivious to the majority of security issues and the problems that they will face as a result of their non-action or ignorance. The fact that they have an antiviral program on their system and a firewall that is most likely built into a DSL or cable router seems to be enough for the average user. This paper will point out the flaws to that kind of thinking and provide several different methods in which a user can better protect their computer.

People usually only think about security when they have a virus or there is a virus outbreak in the news. While in security circles, many hold the view that even the most basic levels of security are easily implemented, and that there is just no excuse for not securing your system. But what people can easily do and what they actually end up doing are usually two completely different things; they seem to overlook even the easiest of fixes.

IT professionals can help to propagate good security practices to the masses with some good old scare tactics, and step by step instructions for the computer novices. As administrators, it is our job to provide protection even when they don't know they're being protected.

Introduction

As security professionals, we can control (for the most part) what people in our offices do with regards to computer security by enforcing security policies, maintaining firewalls and keeping up to date on patches and upgrades. What we cannot control is what those same employees choose to do with their computers at home. We can include within our company's policy, clauses that require any employee keeping company info on their home machine to follow the same rules as at the office, but we cannot enforce the same without invading their privacy. As notebook computers become more prevalent, the desktop begins to take on less significance in the workplace. Our coworkers and employees take their machines on business trips, home and generally leave the office with them, concerns for securing those systems have more weight.

The average computer users are not very concerned about due diligence when it comes to good computer security. They feel that as long as they have an antivirus program guarding their system, they've done all they can as a security lay person. Sometimes, they will see the security measures laid out in our security policies as too strict or getting in the way of their job.

Showdown at the O.S. Coral

Proponents of Microsoft Windows will tell you that their system is by far the most securable. Furthermore, the reasons for such major security breaches and problems are because of unawareness or just plain lack of concern on the end users part. For this, we are seeing major problems in hacked and compromised systems that are under the control of backdoor Trojans and systems that are disseminating viruses and worms without the users knowledge and control. Is this the signature of a bad system, or the lack of time for users to learn every part of that system? Windows is a deep and convoluted system that unless you are out to get your MCSE, isn't going to be absorbed by most. There has to be a way of helping the security illiterate lock down their computer easily, and without having to know exactly what is happening, because as we all know, if they think they'll have to learn something new. Most people will let it go in one ear and out the other. Of course, every version of Windows right now guides people through the installation without so much as a serious mention of security, passwords or account access capabilities.

Linux backers will tell you that the Linux systems are by far superior in their ability to lock down and secure against becoming unwitting zombies of the black hat hacker, and that viruses and worms practically don't exist for Linux systems, and that those few that do exist have been identified and taken care of. Linux versions Red Hat, Mandrake and SuSE all take the novice through a step-by-step installation, which includes the making of a Root name and password (with password length enforcement) as well as a separate user account. Even though they don't go into a lengthy explanation of why they require this, the safety is there, and the user isn't bothered with the details.

Here are some charts from BugTraq, which show the exploits per OS type.

> Buqtraq vulnerabilities 2001
> Table A shows a cumulative list of vulnerabilities discovered so far in 2001.[1]

Package	Number of vulnerabilities
MandrakeSoft Linux Mandrake 7.2	33
RedHat Linux 7.0	28
MandrakeSoft Linux Mandrake 7.1	27
Debian Linux 2.2	26
Sun Solaris 8.0	24
Sun Solaris 7.0	24
Microsoft Windows 2000	24
MandrakeSoft Linux Mandrake 7.0	22
SCO Open Server 5.0.6	21
RedHat Linux 6.2 i386	20
MandrakeSoft Linux Mandrake 6.1	20
MandrakeSoft Linux Mandrake 6.0	20
Wirex Immunix OS 7.0-Beta	19
Sun Solaris 2.6	19
RedHat Linux 6.2 sparc	18
RedHat Linux 6.2 alpha	18
Debian Linux 2.2 sparc	18
Debian Linux 2.2 arm	18
Debian Linux 2.2 alpha	18
Debian Linux 2.2 68k	18

Buqtraq vulnerabilities 2000
Table B shows the 2000 vulnerabilities listed by the same source.[1]

Package	Number of vulnerabilities
Microsoft Windows NT 4.0	71
RedHat Linux 6.2 i386	65
RedHat Linux 6.2 sparc	53
RedHat Linux 6.2 alpha	53
Microsoft Windows 2000	52
Debian Linux 2.2	48
RedHat Linux 6.1 i386	47
Microsoft Windows 98	40
RedHat Linux 6.1 sparc	39
RedHat Linux 6.1 alpha	39
MandrakeSoft Linux Mandrake 7.0	37
Microsoft Windows 95	35
RedHat Linux 6.0 i386	33
Microsoft IIS 4.0	29
Microsoft BackOffice 4.5	29
Microsoft BackOffice 4.0	29
RedHat Linux 7.0	28
MandrakeSoft Linux Mandrake 7.1	26
RedHat Linux 6.0 alpha	25
Conectiva Linux 5.1	25

[1]McCormick, 2001 TechRepublic

As evidenced in the above charts, you can see that the Windows is at a similar level of exploits as with the many Linux operating systems. So why are the Linux flavors deemed more secure? For that matter, why are they out of the box a more secure system?

For all of the Linux flavors ease of initial secure installation, their ease of use after leaves much to be desired and are not the point and click operating systems the average user has come to expect.

Both sides in this debate enthusiastically champion that their systems are far better than the others, and that security issues would be better addressed if everyone would adopt or correctly use their supported system. Both systems have their good sides and both have their downsides.

Linux and some of it's vulnerabilities

One thing I have noticed as I climbed up the steep slope that is the Linux shell command learning curve is the heavy use of commands in their how-to books

rather than the pretty pictures and easy to follow point and click administration techniques of Microsoft Windows. As a long time Windows user, it has been quite a challenge for me to become familiar with the inner workings of Linux. To me, a graphical user interface (GUI) and UNIX (which is how I though of Linux when first learning) did not go together. I was always greatly intimidated by the user-unfriendly UNIX operating system; a command-line only operating system for computer-literate users who could remember hundreds of special commands. But luckily for me, the new flavors of Linux are slowly starting to dispel that bias. The real power of Linux is the choice of several different GUIs like KDE, GNOME and X Windows. But despite the growth towards a user-friendlier GUI environment, Linux still requires some getting used to. Sure the desktop environments like KDE, GNOME and X Windows are able to hide the complex command-line environment with pretty-looking front-end programs that drive the underlying, text-mode utilities. The problem is that more than a few of the front-end programs utilize only a fraction of the various different command-line capabilities. And it is in many of those capabilities that you can identify some of Linux's top vulnerabilities. I will discuss a few that I have become aware of here.

Remote procedure calls (RPC) allow programs on one computer to execute programs on a second computer. They are used to access network services like shared files in NFS. Numerous vulnerabilities caused by flaws in RPC, are being actively exploited. The main problem with RPC is the fact that the initial distribution was created by SUN Microsystems and are now being used by the majority of all other systems. This in effect means that all systems are using the same protocol making RPC a logical single point of failure for all Nix-flavored systems. Over the years, Sun has released patches for the many problems that have cropped up. In order to ensure that your print servers, file servers and other machines are all up to date, it is advisable to download the necessary patches.

Another vulnerability in Linux systems are the R-Services commands. These are the commands that have been used in a combined DoS and DNS spoofing attack not unlike what Kevin Mitnik did in his famous attack against security guru, Tsutomu Shimomura's system. All it takes is a single system on a network to become compromised at the root level for the entire network to then be compromised. Rsh, rcp, rlogin, rdist and rexec all allow external access to a system and make it easy to administer multiple systems without having to log in each time. But R-Services are at the same time, quite dangerous because they are not encrypted and use poor host authentication. Although most UNIX and Linux systems now all have R-Services installed but disabled by default, it is most likely that on older machines, this issue may not be addressed yet. If you remote administer your machines, one way to make sure you're safe is by using SSH to allow you to login to remote systems and have a encrypted connection. If you don't need to remote connect to your machine, you really want to disable the rsh/rlogin/rcp utilities, including login (used by rlogin), shell (used by rcp), and exec (used by rsh) from being started in /etc/inetd.conf. These protocols are extremely insecure and have been the cause of exploits in the past.

Although SSH is by far more secure than Telnet, FTP, and R-commands that it replaces, it has in the past, and will in the future develop vulnerabilities. Therefore, it's always good practice to keep all your software updated with the latest patches. The current Openssh implementation is based on a early version of the datafellows ssh (www.datafellows.com) and has been totally reworked to not include any patented or proprietary pieces. It can be found at: http://www.openssh.com.

Apache Internet Web servers are inherently at risk for various reasons. One reason that an Apache web server is more vulnerable than your normal network machine is because it's always on the net exposed the world. As we all know, firewalls and web servers don't mix. If you want to host a web server, you must either open the ports through your firewall so that traffic won't be blocked, or do it in a DMZ. Apache out of the box is initially much more secure than IIS, however that doesn't mean it's totally safe, and the assumption that it is safe may lead some to be less than diligent when taking security precautions for their web server. When you first install Linux for use as a web server, Apache will most likely be enabled. It is probably a good idea to find out how to quickly enable and disable Apache to protect your server while you prepare it for use. You should apply Apache patches before you do anything else because it's always good practice to keep your software up to date. Compile only the functions you really need. For a complete list of safe steps you can take to help secure Apache see the SANS/FBI report at http://www.sans.org/top20/#U2.

Windows and some of it's vulnerabilities

Now that I've covered the Linux operating system and two of it's better known vulnerabilities, it's time to dive into the OS I am most familiar with. Microsoft Windows is touted as a user-friendly operating system that is strong, flexible and easy to maintain and how true it is, why even my own computer illiterate mother can install Windows without too many questions. Following the install for Windows is fairly simple with only a few parts that can confuse a novice, like the networking section for example. Once the user has installed the OS, they're taken on a tour, which tends to gloss over many security features. One of the inherent problems with the Windows OS is that upon installation, it essentially leaves everything open or on. Much of the security settings are by default, open season for hackers and their nefarious tools.

First, I would like to point out that there is a pension to install Windows and not check for patches or fixes that could prevent future problems. Windows doesn't stress the importance of this enough to the end user. This is one of the reasons that the Code Red Worm infection rate spread as fast as it did. But relying on the users alone to be the responsible parties to patch their machines is bad design. There are alerts, which pop up on the taskbar, but they usually go unheeded by

users. And, as has been the case many a time, patches have been known to cause as many vulnerabilities as they fix.

Now I will draw attention to a vulnerability that really irks me to no end – Windows Default Security Policies. Let's face it, you really have to delve into Microsoft Windows quite some way before you start grasping what security templates, audit policies and password policies are. It is in these areas of the Windows operating system that I find to be cryptic and convoluted to the average user, and a definite point of weakness in the armor. The initial template applied to a Windows 2000 computer is called the Local Computer Policy. The default of this policy is quite open and has little to no protections implemented initially. If a person has some familiarity with Windows, they can implement some basic lock down procedures using a MMC snap-in to build or import the security policy they need. But the problem is, most people I talk to have no clue what I'm talking about when I mention the Windows security policy templates. So, it's not that Windows is inherently unsafe, or vulnerable, instead, it's because of its deeper user unfriendliness that it is a vulnerable system.

These two Windows vulnerabilities rest squarely on the shoulders Microsoft's lack of a secure installation for the OS, and Windows too great a reliance on the actions of the user to secure their computer. And as Uncle Ben told a young Peter Parker, "with great power there must also come... great responsibility!"[2]

[2]Lee, Stan. "Amazing Fantasy - #15"
August, 1962

However, the greatest downfall of Microsoft Windows is it's vast and complex code base, which comprises the bulk of the monolithic operating system. Due to the complexities of the programs in Windows, and the fact that the source code isn't widely shared, Windows leaves quite a large window (pardon the pun) open for hackers to climb in through and a difficult perimeter to protect for those writing anti-virus or other protection software. You can't fix it if you don't know it's broken!

What 'they' don't know can and will hurt you,

Virtually everything the common user knows about computer security, they learn from the news, TV and the movies. We security professionals know that hackers usually aren't good-looking kids in high school trying to work out some teenage ridden angst, or impress some foxy girl and breaking into big bad evil corporations to expose some evil plot…. or at least I hope we all know that. But the visions that the average user has of a hacker are quite close to what they see in the movies. We know that just because you have the newest version of Dr. Quagmire's Virus Software and it's fully updated doesn't mean that you are safe from all viruses, worms and trojans. But unfortunately, most computer users out there think that if their antivirus software is new, and fully updated, they are

totally safe from viruses…and most don't know that there is a difference between a virus a worm and a trojan. What's worse is that with this false sense of security, the user tends to forget that their system is vulnerable to a multitude of other attacks including cyber theft.

There is an inherent danger in ignorance, and that is, if you don't know your enemy, you can't defend yourself against them. The biggest problem facing the security world today isn't only poorly protected commercial and corporate networks, it also includes millions of unprotected, unsecured home networks and computers that add to and exacerbate the threat. I look to two separate instances where two different security certification bodies point out the flaws in today's current security practices. First there is a study conducted by the Computing Technology Industry Association in which they state;

> The survey found that in more than 63 percent of IT security breaches that human error played a role. The survey also found that of those questioned only 8 percent said that security problems were the result of technological failures.[3]
>
> [3] Berniker, Internetnews.com, Developer

Although in this article, the writer also asserts that because the CTIA has IT security training courses, they could have an ulterior motive for making claims about the lack of security training in the IT community. If left to only CTIA, I might believe that ulterior motive claim to be a valid one, save for the article almost two years ago by our beloved SANS making similar claims about IT professionals lacking proper security training in a CertCities article in 2001.

> "One of the saddest dimensions of information security is that hundreds of thousands of people earned MCSE certifications without being required to demonstrate any competence in security."[4]
>
> [4] CertCities

What these two excerpts provide us with is a glimpse into the IT worlds looming need for better and more thorough training. Now if the IT professionals are lacking in some security fundamentals, how much worse are the home based computers?

We lock our homes and offices against theft, but not our computers,

This is a very interesting attitude to me. Just because you can't see someone entering your home, and you can't quantify what's being taken, does not mean that it's not a problem. In the US, if a person owns a gun, they're required to be responsible for that because as we all know, a gun is a weapon. If that gun is stolen and someone uses it in a crime, you may very well get in trouble.

Computers more and more are becoming quite the useful weapon. As more and more of the worlds infrastructure becomes dependant on computer technology, it also becomes more vulnerable to cyber attacks. A hacker can easily cause millions of dollars in damage with just one computer and in a very short period of time. What's worse is that the damage that a hacker can cause may now be more than just monetary loss; it could result in a loss of life. Lets say for example, if a hacker was able to cut power from an entire electricity grid or cause power stations to randomly shut down and overload in winter, elderly people and those who are relying on that power could very well die. An example from real life just happened the other day when the slammer worm took down a 911 system in Washington State. Here is an excerpt from an article from Security Focus Online;

> "General Internet congestion is always expected for a worm like this, but the peripheral effects of Slammer caught many by surprise. They caught me by surprise. Financial institutions and government bodies were affected by this worm. I was skeptical of mainstream media reports of Slammer's infestation of a 911 emergency response system, so I contacted the reportedly hard-hit Bellevue, WA center directly. The conversation was sobering. According to an operator in the dispatch center, the worm forced them to switch to manual systems. If a non-trivial emergency event had occurred during this period -- a car pileup or a major fire or explosion -- there would have been a "most definite" risk to human life due to process delays and system unavailability. According to this official, someone could have died. Like many others, I had taken the threat of "cyber-terrorism" with a large grain of salt. But where the interdependencies of multiple systems connected to the Internet make it possible for a worm to shut down normal operations of an emergency dispatch center by accident, it does make me wonder what could happen if someone launched a coordinated attack on purpose. So, what needs to change?"[5]
>
> [5]Mullen, Security Focus Online, Feb 3, 2003

And all of the problems that transpired around the world for days, if not weeks were all from a three hundred and seventy six byte worm. The simple fact is, anyone with a rudimentary skill in programming can re-write any virus, worm or Trojan, changing it just enough to evade detection of the antivirus software and the game starts all over again. The pen may be mightier than the sword, but the keyboard certainly has become more deadly.

The Enemy at the Gates,

The Internet is many things to many people and it's growing in complexity every year. One of the great things about the Internet is its vast amount of information, the ability of people to disseminate that information as well as its reach into much

of the world. Unfortunately, the Internet's greatest strengths are it's greatest downfalls as well.

Much is happening in the way of Internet attacks and abuses that make use of unsecured computers. Here are some of the more notorious and public security problems today with real world examples included.

DDoS or distributed denial of service attacks are automated attacks that run simultaneously from multiple computers designed to lock out legitimate users from web sites or networks. Hackers will unleash autonomous programs onto the Internet that will go around seeking out vulnerabilities on multiple remote computers and then report back to a central computer for compiled list of all the computers, which can later be compromised at will. Some of these Bots can even plant a Trojan horse program on the victim's computer. These trojans will usually 'phone home' and announce itself to the hacker's main computer when the victims computer is on the net. This will allow the hacker to plant whatever automated attack program (known as a script) he wants, on the victim's computer. The Trojan horse programs on the computers of unsuspecting accomplices throughout the network or Internet at a given hour will coordinate requests for information from the overloaded victim computer. Due to the numbers involved, such an attack can be very difficult to stop. The most prolific example to date happened as recently as October 21, 2002.

> "Around 5:00 p.m. EDT on Monday, a "distributed denial of service" (DDOS) attack struck the 13 "root servers" that provide the primary roadmap for almost all Internet communications. Despite the scale of the attack, which lasted about an hour, Internet users worldwide were largely unaffected, experts said."[6]
>
> [6]McGuire and Krebs, WashingtonPost.com

Next I'll talk about spoofing. Spoofing means pretending to be someone you are not. Out on the Internet it means pretending to be a different address or site other than the one you really have in order to gain something.

The simplest spoof is to catch the people who mistype the web URL they are looking for, or put the wrong locator at the end of the domain name. Let's take a look at a few examples of what I mean. (Please note that there is no suggestion that these are hacker sites, but the redirection stated here was verified on March 21, 2003)

www.mictosoft.com = This site's potential traffic could be quite large seeing how close the 't' and 'r' are on the keyboard.
www.whitehouse.net = Obviously a fake Whitehouse site, however, when first arriving, the initial glance might fool the unaware.
http://www.whitehouse.org = A parody site.

www.whitehouse.com = A pornographic website.
www.whutehouse.com = Potential haven for viruses and trojans to be downloaded by accident. I encountered java pop-ups and a pornographic script trying to download itself to my computer.
www.yshoo.com = takes you to the site www.freemoney.com
www.goggle.com = brings you to a site where multiple software packages ask for your trust including one from Gator.com.

What the above sites prove is that there are people out there just waiting for you to mistype a URL or just type an extension wrong out of ignorance. Although most people probably know that the real Whitehouse site has the extension .gov(dot gov), there is the off chance that someone doesn't know and these sites are well laid traps for just such people.

DNS Spoofing is a different sort of attack that is kind of like the hacker's version of smoke and mirrors or slight of hand. These can be sophisticated attempts to steer web surfers to an illegitimate site. To understand just how this happens, I'll have to explain a little about DNS and then some ways of subverting or hijacking DNS queries.

When you navigate your browser to a site on the net, your computer will look up that entry in an immense directory called the Domain Name Service (DNS) database, and then send you to the appropriate site. The DNS database matches every name to a numerical address. Servers throughout the Internet maintain a constantly updating database of these DNS entries.

The DNS research, software and consultancy, Men & Mice states,

> "A third of all DNS servers on the Internet are vulnerable to spoofing.[7]"

[7]Men & Mice, Domain Health Survey for .COM - November 2002

A DNS spoof takes place when a hacker alters a DNS entry on a server to redirect the browser to an alternate site. If a consumer wanting to visit Yahoo gets sent instead to Yoo-hoo, then business can be stolen. A hacker can also create a fake site that pretends to be Yahoo. In this way the hacker might steal passwords, personal data or even credit cards from the consumer. The example below illustrates how DNS spoofing can also be used to download malicious software via an OS's auto update function, bypassing the user all together.

> The exploit takes advantage of SoftwareUpdate, Apple's software updating mechanism in OS X, which checks weekly for new updates from the company. According to Harding, who claims to have discovered the exploit, the feature downloads updates over the Web with no

> authentication and installs them on a system. So far, there are no patches available for this problem.[8]
>
> [8]Loney, c|net

Although this problem was downplayed in comparison to Microsoft level threats by security professionals like SecurityFocus' senior threat analyst Ryan Russell;

> Still, Russell said there is no indication that the exploit is being used. "If it was [used] in any kind of massive way, it would be noticed quickly," Russell noted. He added, "it could be used in a smaller, targeted way in terms of not being detected."[9]
>
> [9] Lyman, NewsFactorNetwork

Packet Sniffing - Like many hacker tools, packet sniffers were initially designed as a tool for system administrators to help debug networking problems. For all intents and purposes, they are computer programs, which allow the user to intercept and interpret "packets" of information traversing a network. Any information shared among a network of computers--username/password pairs, email, and files being transferred--gets translated into "packets," which are sent out across the network. Every piece of data you send over the Internet contains an Ethernet header, a sort of numerical address, to make sure that the right machine gets the right information. Each machine is supposed to pay attention only to packets with its own Ethernet address in the destination field. However, an Ethernet packet sniffer is software, which allows a hacker, or network administrator, to "eavesdrop" by recording information on packets not addressed to his or her computer. This is something that most average users I know are not aware of at all.

> We have received reports of intruders using distributed network sniffers to capture usernames and passwords. The distributed sniffer consists of a client and a server portion. The sniffer clients have been found exclusively on compromised Linux hosts.[10]
>
> [10]CERT, Incident Note IN-99-06

Social engineering is a hacker term for deceiving or manipulating people into giving out information about a network or how to access it. A hacker may pose as an employee who forgot his or her password, or a software vendor asking for information about a network in order to determine what the company's software needs are. The hacker could invariably pose as a law enforcement official or computer security specialist and play on your coworker and employee's fears. Kevin Mitnick is probably the most talked about hacker out there who used social engineering to obtain the information he needed to hack the system.

> The CERT/CC has received reports of social engineering attacks on users of Internet Relay Chat (IRC) and Instant Messaging (IM) services. Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks. The reports to the CERT/CC indicate that tens of thousands of systems have recently been compromised in this manner.[11]
>
> [11]CERT, Incident Note IN-2002-03

Worms and viruses are surreptitiously "self-replicating" programs that can spread exponentially throughout a network. The first worm released on the Internet, the Morris Worm, was an experiment by a university graduate student. However, it replicated itself so efficiently and took up so much memory and computing resources on the Internet that many computers crashed, and system administrators across the country were forced to take their machines off the Internet. Modern-day virus writers often have malicious intent, however, and they use viruses and worms to spread destructive programs among unwitting hosts. A virus spreads by infecting another object on the computer system--a program file, a document, or the boot sector of a floppy disk. A worm can copy itself from computer to computer on a network without needing a file or other object. We are now all too fully aware of the power of a well-written worm as we learned the hard way with the recently released 'Slammer'. And delivery of these worms is coming in more varied ways like being disguised as MP3s.

> The Windows XP vulnerability, which Microsoft calls "Unchecked Buffer in Windows Shell Could Enable System Compromise," can be exploited through an MP3 or WMA audio file.
>
> The malicious audio file can be placed on a website, sent in an e-mail or stored on a shared network drive.
>
> Users do not need to click on, load or play the audio file to compromise their computers. If a user simply holds the mouse pointer over the icon for the malicious file, or opens the folder where the file is stored, the vulnerable code is activated, Kurtz said.
>
> Once the malicious file's code has been activated, an attacker can gain complete remote control over the affected system, including creating, modifying or deleting data, reconfiguring the system, reformatting the hard drive or running programs of the attacker's choice. [12]
>
> [12] Delio, Wired News

Be sure to show your coworkers and employees this information. Post it near the water cooler and coffee machine to make sure they're made aware of it's seriousness and so that they never let their guard down. The sheer fact that there are all of these new vulnerabilities out there requires security professionals to be aggressively proactive towards the issue.

I AM THE LAW

Taking steps to secure your computer should be something that is easy to do for even the most green of users. Unfortunately nothing about computer operating systems is simple aside from the surface interface. Windows security is nothing less than cryptic and the glut of information out there about which tools are good for making the home PC secure is so vast, that it literally drains all the will to live from someone if they stare at it long enough! Ok, maybe it's not quite that bad, but really, there is way too much information for a person who's not really interested in 'Computer Security' as a job description.

This is not to say that there isn't a need for computer security. This is just facing the fact that with an ever-increasing amount of people using computers on the Internet and with the computers becoming ever more complex, the security issue must become a no-brainer for the vast amount of cyber neophytes we're giving free reign on the Net. We must appeal to the most prevalent operating system designers to incorporate secure setup routines into the initial installation or usage of the computer. Of course, requiring the Software industry to do this will probably take quite some time, so it's up to the security professionals to help secure the world.

A good start

One simple fix and a good starting point that I have found are the Center for Internet Security (CIS) free downloadable Benchmark scoring tools for both Windows and Linux OSs. With the downloadable benchmark scoring tools comes a whole selection of templates and a how-to instruction guide of just how to go about applying those templates to your system. With this, even non-professionals can apply the templates on their home computers and help us to make the Internet a far less dangerous place. You can find the tools at www.cisecurity.org .

Another fairly simple fix is to download ZoneAlarm personal firewall. The free version is easy to set up and automatically blocks dangerous Internet threats - known and unknown - guarding your PC from hackers and data thieves. ZoneAlarm provides the basic protection individuals need to secure their PC and keep their valuable information private. You can download this free product from www.zonealarm.com .

Become proactive

Vulnerabilities are a liability sometimes long before they come out in the news and alerts. As system administrators, the buck will stop at you if anything goes wrong. So it's up to you to do everything you can to ensure that it doesn't, and if it does, you'll be able to show the effort you personally made to prevent it.

How to find vulnerabilities:

- Maintain more than one subscription to a security bulletin mailing list.
- Try and crack your own system.
- Pay Ethical Hackers to break into your systems.
- Break into a friends system (with their permission of course)
- Have your friend to try and break into yours.
- Ask non-tech people how they access and use the data network.

Remind your employer through memos about the dangers of the Internet jungle. Scare him about the possibility of having a competitor hack the system and steal all your customer data, or anything that might give your competitor the edge. Tell him of the failings of "Security through obscurity" and about the failure of the DVD Copy Control Association and their DVD encryption that they shared with no one during development, only to have a some hackers make short work of it right after it's release and disseminate 'DeCSS' encryption utility all over the globe.

Updates, patches and fixes oh my…

Maintaining systems with up-to-date security patches under harsh real-world conditions and the off chance that a patch or update could take down a vital part of the network is one of the main reasons administrators tend to hesitate on updating their systems. Mission-critical systems require that all changes be tested before going into production require a lot of an administrators time and effort. Time and effort he may not necessarily be able to give either due to a lack of staff, or a lack of knowledge. These systems need a patch stream that will have minimal impact on the functionality of working systems, allowing patches to be put into production quickly and safely. If there are too many unrelated changes in a service pack release, then it may not be deployed in a timely manner, or at all.

Unsophisticated administrators tend to let the machines run on and on as long as they don't cause too many problems. Their approach to administration is the Dutch boy at the dike syndrome, they spend most of their time fixing leaks, and

not enough if any time addressing the real issues at hand. But what's worse, they often don't know what is running on their machines, quite possibly because their systems were set up by a consultant who is currently not responsible for maintaining the system.

My suggestion is to have a machine that is similar to your mission critical machine to test the updates and fixes on before you install them on your production machine.

What's this button do?

Unnecessary services should not be running. Unnecessary services expose the user to attacks on services that they are not even aware they are running. Machines should be secure out of the box. The administrator needs to specifically select which services they want to run and be prepared to deal with any problems. Unfortunately, the average user does not know what they need. With modern Linux distributions, potentially thousands of programs may be installed. The beginning user simply installs everything, not knowing what will be needed later. The solution to this problem is to have things disabled by default. A user-friendly administration console allows the user to make informed decisions about what should be enabled, giving help about what functions the program performs and any security impact (e.g., enabling a mail server to be used for relaying spam).

Perimeter defense includes the inside as well

Firewalling should by default prevent all connections. The user should need to manually enable services to be run. Again, this requires a user-friendly interface for enabling and disabling services, which describes the function of the service and its security impact. Broad categories are necessary for ease of use, e.g. "client only", "share files and printers". Server and network administrators rather than desktop machines primarily address this issue. It serves as a second line of defense to protect the network from attacks. Egress filtering allows only known data to be passed outside the machine or network. This prevents problems like the "Slammer" worm from propagating.

Conclusion

How many of us have seen our cyber neophyte parent, sibling, spouse, friend or co-worker stare at the computer for hours on end surfing the Net. How many times have we told them to keep it secure, only to come back and see that the security settings in Internet Explorer are all on low and they are accepting cookies from all sites. What are they doing? Why is it that our efforts went unheeded?

Well I think one way we can help them is to supply them with the tools to secure their system for free, like the free security benchmark utility created by the Center for Internet Security and the firewall product from Zone Labs. Had all of the security professionals just taken the time to disseminate this utility to all of their friends and family, a disaster may have been averted, or at least it's bite would have been lessened.

> Not only could companies have easily slammed the door on the Slammer worm if they had installed the patch released by Microsoft Corp. six months ago, but they could also have uncovered the vulnerability exploited by the worm using a free benchmark developed jointly by the government and private sector.[13]
>
> [13]Verton, Computerworld

It is our job to keep our companies secure, but that means we've got to think outside the box. People's home computers are fast becoming the unwitting tools of the malicious hacker and are usually the source for many of the virus and worm outbreaks. Let's do ourselves a favor and start trying to secure their systems so we can narrow down the possible attack machines on the Internet. This is going to have to be a group effort on the part of all security professionals around the world. Remember, it's our job to be proactive and to patch all the holes, because no one else will.

References

McCormick, John. "By the numbers: Windows vs Linux security",
02 October 2001
http://www.zdnet.com.au/newstech/os/story/0,2000024997,20260847,00.htm

CertCities. "SANS Blames MCSE Training for Spread of Code Red"
August 15, 2001
http://certcities.com/certs/microsoft/news/story.asp?EditorialsID=160

Berniker, Mike. "Study: Human Error Causes Most Security Breaches"
internetnews.com, Developer
March 20, 2003
http://www.internetnews.com/dev-news/article.php/2120051

Mullen, Tim. "Something Needs to Change", Security Focus Online,
Feb 03, 2003
http://online.securityfocus.com/columnists/139

McGuire, David and Krebs, Brian. "Attack On Internet Called Largest Ever"
Tuesday, October 22, 2002; 5:40 PM
http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A828-2002Oct22&notFound=true

Men & Mice, Domain Health Survey for .COM - November 2002
http://www.menandmice.com/6000/61_recent_survey.html

Loney, Matt. "Hacker to Apple: Watch those downloads"
July 8, 2002, 4:10 PM PT
http://news.com.com/2100-1001-942265.html

Lyman, Jay. “Apple Warned of Update Exploit” NewsFactor Network
July 9, 2002
http://www.newsfactor.com/perl/story/18527.html

CERT, Incident Note IN-99-06 ‘Distributed Network Sniffer’
Monday, October 25, 1999
http://www.cert.org/incident_notes/IN-99-06.html

CERT, Incident Note IN-2002-03 'Social Engineering Attacks via IRC and Instant Messaging'
Release Date: March 19, 2002
http://www.cert.org/incident_notes/IN-2002-03.html

Delio, Michelle. "Beware the Latest MP3 Worms"
Dec. 18, 2002
http://www.wired.com/news/infostructure/0,1377,56924,00.html

Verton, Dan. "Free benchmark could have found Slammer vulnerability"
JANUARY 31, 2003
http://www.computerworld.com/securitytopics/security/holes/story/0,10801,78063,00.html?nas=PM-78063

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor