Global Information Assurance Certification Paper

Microsoft Windows Security Patches

Dan B Rolsma
SANS Security Essentials
GSEC Practical Assignment
Version 1.2e

This paper is for those who have a Microsoft Windows computer attached to the Internet, and haven't installed the latest Microsoft security patches. The first section is where to get these patches and how to install them. The second is why. Many people don't think it is important enough to keep current on the latest security patches released by Microsoft, at least not important enough to actually do it. Those are two main reasons I have come across for people to not keep current on the latest MS Security patches. The first being how, and the second being expressed by "Do I really care?" A prudent person would also have a firewall (or two) between their MS Windows computer and the Internet as well, so hopefully I can convince the reader to do this as well.

In a perfect world, all software would work as intended. I am a computer system administrator working across a few government projects. My main focus is keeping servers up and running and users connected to these systems from their workstations. Some are on the local network and some are connected in from the Internet. I have shown people how to check for the latest security updates, and install them, just by clicking a few buttons. Yet a few months later the user's system gets broken into because they haven't installed the latest patch released for a known vulnerability. The latest lamest reason I was given is that installing them requires a reboot. And rebooting their system, you know, well that's just not going to happen if they can help it! A little convincing is needed to get people to keep their systems current.

If you are in that group of people wondering why you should bother, skip on down to the section "Is This Really All That Important?" You can always return here later. If you aren't in that group, you may think about joining it once you start the process of keeping up to date. Microsoft has some tools to help you out you may not be aware of to make this task less tedious.

Checking That Software Security Updates Are Current

These tools from Microsoft will search your system and tell you what you are missing. If you have ever looked at the long laundry list of patches for Microsoft products listed on their website, around 200 and growing the last I looked, it can be overwhelming. These three tools can help.

1) The Windows Update Tool

The website for this tool is http://windowsupdate.microsoft.com. In IE 5 or later, you can get to it by selecting Windows Update from the Tools menu. On the Windows Update web page, there is a link for Product Updates. Clicking it will run the Microsoft product updates program. It will display "Please Wait … Windows Update is customizing the product updates catalog for your computer. This is done without sending any information to Microsoft" as it is running.

After the program completes, you'll be looking at another web page displaying a list of updates your system could use. You are concerned with the ones under the heading Critical Updates. These are the security patches. To install them, follow the directions on the screen.

One non-critical update I recommend from this page is the Windows Critical Updates Notification. It notifies you when your Windows operating system needs a critical update. It does this by checking the update web site for you on a regular basis (3).

2) Microsoft Office Product Updates

Most likely, if you have Microsoft Windows, you also have Microsoft Office. This has some security patches as well. From the Microsoft Windows Update page, there is a link on the left for Microsoft Office Update. It brings you to http://office.microsoft.com/productupdates/. The pop up window, when it is examining your system, looks a little different, but it says pretty much the same "Please Wait … The Product Updates site is determining which updates your computer needs. This is done without sending any information to Microsoft."

After the program completes, updates are listed. There isn't a Critical Updates section as with the Windows Update Tool. It lists all updates. If the update description says "security update" or has the word "vulnerability" in its description, then you want to install it.

3) Internet Information Services (IIS) updates

There is yet another tool for updating IIS, if you are running Windows 2000 Server. The URL for it is http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168. At least, that was the URL last I looked. You know, I'll have found something at the Microsoft web site, and when I go back a second time I have a hard time finding it again. I'm not too sure why that is. If the above link doesn't work, the Microsoft Security Homepage is http://www.microsoft.com/security/default.asp. You will see a link to the left for "Tools and Checklists." From there you want to scroll down for the Hotfix Checking Tool for IIS 5.0.

If you have NT 4.0, or more precisely, IIS 4.0 (which only runs on NT 4.0) Microsoft doesn't have a tool. The same goes for Windows 2000 Professional. You'll have to go to the Microsoft Security Home Page, do some reading, and install the patches you need manually. I cover how in step 4 below.

But what is IIS, you ask? How do you know you have it? This isn't always a case of "if you don't know what it is, then you probably haven't installed it." If you share this computer, someone else may have installed it. If someone else setup this system for you, then you **really** want to check. They may have installed everything off the Windows 2000 CD for you, or in the case of NT 4.0, they installed the Windows NT 4.0 Option Pack. Other family members at home, or coworkers for systems at work, may have installed it as well.

To find if you have it, you can go to Add/Remove Programs (Start Button -> Settings -> Control Panel -> Add/Remove Programs) and you are looking for Microsoft Internet Information Server (NT 4.0) or Internet Information Services (Windows 2000).

IIS lets you serve out web pages from your PC as well as run an FTP service. Most people don't use it. I mention it, because it comes on the Windows 2000 CD, Professional and Server, so it gets installed sometimes when it shouldn't be. It is supposed to be the latest cool thing you can do to join the Internet revolution. It is also one of the fastest ways to let a hacker into your system if you don't update it. Web servers don't have a good history of being secure, which you may want to keep in mind (3). Just as a caveat, many people don't think it wise to put personal financial information on the same system that is serving out web pages.

4) The Microsoft Security Home Page

(http://www.microsoft.com/security/default.asp)

This page has a link to Bulletins, which brings you to the Microsoft Security Bulletin Search page. This is the manual method of installing patches, such as for IIS that is running on Windows 2000 Professional. There is a drop down list of Microsoft products. Take a look at the list for other Microsoft products you may have. From the vast array of patches Microsoft has released, this narrows down the search.

It may encourage you that the MS01-026 patch originally released May 14, 2001 is a cumulative patch. It covers vulnerabilities in IIS available since the release of NT 4.0 SP5. This is explained in the Technical Details section of the bulletin for this patch. June 18, 2001 there was another patch for IIS. It isn't accumulative, but that just leaves you with two patches to install, MS01-026 and MS01-033 as of this writing (July 1, 2001). And that is the key, as of this writing! Do you notice the two dates above? May 14 and June 18 aren't very far apart, so how is anyone supposed to keep up?

5) Join the e-mail notification list.

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/notify.asp

The above URL describes using the Microsoft e-mail notification list in detail. In summary, send e-mail to microsoft_security-subscribe-request@announce.microsoft.com from the e-mail address that you want to receive notices at. The subject and body do not matter. You should get an e-mail back in return confirming you want to be added to the list.

So are your eyes glazing over yet? Are you wondering how you can get out of updating your system?

Is This Really All That Important?!

It may take only one look at the long list of Microsoft security patches for someone to ask himself or herself if they really need them. Clicking on the link for one and reading the bulletin may only

reinforce this. Life would be easier if no one needed to.

The speed at which vulnerabilities are found, and exploited, happens in "Internet time." For instance, on May 1, 2001, Microsoft made available a patch for a recently discovered vulnerability in IIS, as described in http://www.microsoft.com/technet/security/bulletin/MS01-026.asp. By May 4th programs were available for download on the Internet, which would let a novice computer user break into Microsoft systems that had not been patched. On May 9, the SANS Institute (homepage http://www.sans.org) reported that it had received reliable confirmation to prove that hackers exploiting this vulnerability had defaced well over 9,000 websites running Microsoft IIS. It is assumed that personal information from customers, along with their credit card numbers, have been downloaded from these sites as well (2).

People have had personal information stolen from their PCs (4). Identity theft can occur from your home PC directly connected to the Internet. This is one of the fastest growing crimes in the United States (5). People that have their identity stolen spend untold hours over a period of months to years undoing the damage that takes place (6). Keeping your system updated with the latest security patches goes a long way towards stopping intruders (7).

But stop and think a moment about the process of patch production for these known vulnerabilities. There is a time lag between when the vulnerability exists, when it becomes discovered, and when a patch is produced. Looking at all of the patches that have been created for all of the vulnerabilities is a little disconcerting. Steve Ballmer, Microsoft's CEO, has been quoted to have said (disgustedly), "You would think we could figure out how to fix buffer overflows by now." This quote was concerning the IIS vulnerability I mentioned earlier (2). It affected IIS 4.0 as well as 5.0. IIS 4.0 has been out for ***YEARS!*** Referring again to the list of patches available that just seems to continue to grow and grow, the Windows operating system along with the software that is bundled with it, is like Swiss cheese! Of course, this latest patch refers to people using IIS, not just Windows, but it isn't this latest patch alone that is the source of frustration. It is the accumulation of them, for Windows and IIS, that Steve Ballmer is frustrated over and which I am talking about as well.

Defense in Depth

There is a concept of having defense in depth (1). Windows has had vulnerabilities in the past, and it is a likely bet that there are vulnerabilities yet to be discovered. This is one reason to install a firewall on your personal computer. There are quite a few to choose from. Some you must buy and some you can use for free, if used for personal use. Otherwise the cost is nominal.

There are two that I have used, and that are free for personal use. One is ZoneAlarm that can be downloaded from www.zonealarm.com. The other is Personal Firewall from Tiny Software available from http://www.tinysoftware.com. They are software products that run on your computer. One nice security feature is that they can control what programs are allowed to access the Internet from your PC. You can lock the settings with a password. If someone else installs some software when you aren't looking (for example IIS) they would also need to know the password to get it to access the Internet. ZoneAlarm and Personal Firewall stop any new programs from being able to access the

Internet, until you give permission along with the password. Both will also stop someone who tries to rename a program to take the place of a program you have already allowed. More details are at the respective Internet web sites for these two products along with, of course, how to use them.

Now what if a hacker discovers some vulnerability in your firewall software installed on your PC? A PC where you work is probably behind a commercial firewall. Most commercial firewalls are certainly sophisticated, but they still get penetrated. Defense in depth would mean that there is the main commercial firewall, your software firewall, and you have all the latest security patches installed on your PC. There may be more than one firewall that your Internet-bound traffic goes through before getting to and from the Internet, which just means there is more depth to the defense of your work PC. A hacker needs to get past all of these security layers before getting to what is stored on your PC. Unfortunately, a commercial firewall may stop you from being able to run the Windows Update program, which makes maintaining patches for your PC more difficult. Your employer may have a procedure for updating your PC with security patches, so it may not be an issue. You'll need to follow the policy where you work on whether you can install a software firewall on your PC. I could imagine some not allowing it.

Where I work, the resident computer security specialists encourage the use of ZoneAlarm or the Personal Firewall from Tiny Software. They also want people to configure them to allow the corporate scanning software to check for security patches their PC may be missing. Otherwise, they will eventually disallow your IP address from accessing the Internet. What I am saying is, the only way to know what the policy is on these host-based software firewalls where you work is to ask. They may be helpful. They may also look at you like you have holes in your head. You may even get a very helpful person, and the not-so-helpful person at the same company. Computer technology, and especially computer security technology, seems to go a little faster than most people are able to keep up with.

The ZoneAlarm firewall and the Tiny Software Personal Firewall will by default stop NT Domain traffic. If you need to participate with an NT Domain, you will need to configure to allow IP traffic from the domain controllers. I haven't seen this documented anywhere. The way I dealt with it was that the firewall by default pops up a window when an "intrusion" occurs. That is to say, outside network traffic tried to access my system, and by default the firewall stops any incoming traffic and calls it an intrusion. As a user you need to tell it which systems are allowed to access your system. It was quicker to set this in the Tiny Software firewall.

The Tiny Software firewall displayed the name of the computer in a pop up window, and the port it tried to use. I was able to recognize the function of most systems by the name in the window. The pop up window also asks what to do about the attempted access. The choices are permit or deny along with a check box whether to remember the setting. It was a little tedious at first, but after a while things were running smoothly and it stopped asking me since it eventually had rules recorded for which computers were to be allowed access.

ZoneAlarm displayed a pop up window, but it didn't give the computer name. It just gave an IP number and a port. I had to look up what these systems were named, which was a but of a pain. I also could not record what to do on the fly as with the Tiny Software firewall. Instead ZoneAlarm

divides the world into two zones, a local zone and the Internet zone. Nothing is in the local zone unless you go into the customize area and add computers, by their IP numbers, into the local zone. Once recorded in the local zone, they will be allowed access. ZoneAlarm is less flexible, but I would say it is the easier of the two for a beginner. If you are installing a firewall as a home user, you probably don't need to put anything into the local zone in ZoneAlarm for it to work just fine. It will prompt you for programs that want to access the Internet, and you can set them for Yes or No on-the-fly. It is the traffic coming in that isn't as convenient as with the Tiny Software firewall. If you are dealing with a PC at work, you most likely need to let traffic in, such as NT domain traffic. I also had to add the server that backs up my system at night into the local zone. My PC didn't get backed up for a few nights until I realized that. With a home PC, there is most likely nothing you need to add to the local zone if you just want to surf the web and get your e-mail.

Unlike a PC at most work places, your PC at home isn't behind another firewall unless you go get one. By all means install one of the free host-based software firewalls. You can and should also install another firewall, one that is separate from your PC. You can buy a firewall for home use relatively inexpensively, in the $100 to $200 range. Three I know of are from Linksys, D-Link, and Netgear. To be specific, there is the Linksys Instant High-Speed Internet Sharing EtherFast Cable/DSL Router. There is a 1 port model, a 4 port model, or an 8 port. This would correspond to whether you have 1 PC, 4 PCs, or up to 8 PCs at home you connect to the Internet. Product information on these routers and others is available from the Linksys website http://www.linksys.com/products/group.asp?grid=5. Some of the other Linksys routers support wireless home networks as well. NetGear is another vendor of residential firewalls. Netgear can firewall a DSL or Cable connection, the same as with the Linksys Internet sharing router. Netgear also has a model that will firewall a dial-up connection. More information on models is available at their website http://www.netgear.com/routers_main.asp. The D-Link web link for their residential firewalls is http://www.dlink.com/products/DigitalHome/CableDsl/. Netgear also has two they advertise as a small office firewall. They include Stateful Packet Inspection to prevent DoS attacks and malicious packets, VPN pass-through, and logging and reporting capabilities. The small office firewalls also cost more, are probably more than what most people would use, but are still very affordable at around $200. It may be what you want if you have a VPN connection with the network where you work that you want to use. Netgear has some less expensive ones that rival Linksys and D-Link low-end firewalls in price and performance.

What all these low-end firewalls do is they use NAT, which is the acronym for Network Address Translation. It works really cool, so I'm going to explain it. Basically the way NAT works is you assign to the firewall the IP address that your Internet Service Provider (ISP) has given you for your PC. To the rest of the world, your firewall is what they now see on the Internet. Your firewall then, is a Dynamic Host Configuration Protocol (DHCP) server and it assigns an IP address to your PC (or PCs if you have more than one you are hooking to the Internet). It is a different IP than the one your ISP gave you to use. When your PC accesses the Internet, it communicates with the firewall using this different IP address. The firewall translates your PC's IP communication, and uses the IP address that your ISP gave you. The firewall records that your PC sent out a communication. When a response comes back, it is checked to see if it is a response for what was sent out from your PC. If it matches, the firewall forwards it to your PC. Your PC can contact web sites out on the Internet and

get information back and not be directly connected to the Internet. If someone from the Internet comes along looking for your PC, they can't find it. The firewall won't forward any traffic that your PC didn't specifically ask for. This makes it very tough for a hacker to get into your system (8).

This relates to Microsoft security patches by stopping a potential intruder from getting any meaningful access to your PC. You may have a vulnerability that is exploitable, but if a hacker can't get to your PC he can't exploit it. Now you may be thinking that this is the panacea for not having to keep Microsoft patches current. Many people with PCs behind company firewalls at work like to think so. It is a whole lot better, but if your NAT firewall is penetrated from the Internet, because it is found at some future date to have a vulnerability (nothing is perfect), your one wall of defense is gone and your hacked. Being prudent you have applied all of the latest Windows patches so the hacker still can't find a way in. If you have also installed a host-based software firewall on your PC, such as ZoneAlarm, there is yet another layer they need to get through. They would need to know how to get through the NAT firewall, through your software firewall, and then take advantage of some Windows vulnerability. That is what defense in depth is about. Per chance they break through one, well they have more to go through.

If you are still contemplating to solely rely on the NAT firewall, or your company firewall anyway, there are known Internet Explorer (IE) vulnerabilities which need security patches applied to fix them. A NAT firewall won't stop traffic from malicious web sites that you may visit. Remember how NAT works? If you ask for a connection to a web site, the NAT firewall will let the traffic back through. So the Microsoft security patches are still important for this reason even if you have a NAT firewall. A malicious web site operator could try to send stuff back to you that will zing your computer with an exploit, and you won't see it coming. So install those security patches!

A good explanation of how NAT works in detail from a security standpoint is at http://www.linux.org/docs/ldp/howto/IP-Masquerade-HOWTO.html. It also details how to set up a NAT based firewall using Linux. If you have an older PC that will run Linux, you can use it to build a NAT based firewall. I would consider it a higher end firewall than the previously mentioned NAT firewalls. The technical knowledge needed to set it up is considerably more, but it is a very good option for a NAT firewall as well (8).

You should also, of course, use Anti Virus software. Anti Virus software has been around for a while and most people understand how to use it, and what it is for, so it probably doesn't need explaining here. Although this paper is on Microsoft Security patches, there are many programs written by malicious hackers that Microsoft Security patches will not stop. Internet firewalls will not stop them as well. The software firewalls, such as ZoneAlarm, will stop and detect some of them if they try to access the Internet or come through your e-mail. But they won't scan your disk drives for them and remove them from your system. NAT firewalls can also keep worms from coming into your system from the Internet. If you use a PC at work, hopefully there is antivirus software on it. You may be able to install it on your home PC as part of the software license that your employer has purchased. Ask, since if so, it will be no additional money out of your pocket for this software. Whatever source you get it from, whether work or buying it yourself, you should use it.

Hopefully I have pointed you in the right direction for making your Internet-connected PC more

secure. If nothing else, you are aware that if you install any of the Microsoft Windows operating systems on your PC and just hook it up to the Internet, that it is extremely vulnerable to compromise. You need to go through the extra steps to keep your system updated with the latest security patches. Also you should install a software firewall, particularly if there is no other firewall between you and the Internet. Don't laugh, my Windows work PC has no firewall between it and the Internet world. If you can, get another firewall separate from your Windows PC. Any NAT based firewall will work. Install and use antivirus software.

You could, of course, disconnect your PC from the Internet entirely, not do any online shopping or banking, and never let a floppy disk that was inserted in someone else's PC be put into your PC. But consider that we all take risks no matter what we do. Shopping in person has risks, such as getting your purse stolen or loosing your wallet. A bus can hit you. There is a lot of good freeware out there that you could download or get from friends you'll be missing out on. So get your PC updated with the latest Microsoft security patches, use antiviral software, and put one or two firewalls in place. Remember to watch for buses, and have a great time traveling whether on foot or in Cyberspace.

List of References

(1) Northcutt, Stephen. "Information Assurance Foundations." SANS GIAC Level One. V 1.41 January 13, 2001: Page 21

(2) SANS News Bites Vol. 3 Num. 19, May 9, 2001

(3) The SANS Institute, "Networking and Internet Security Settings", Windows NT Security Step by Step Version 3.03, February 2001: page 38

(4) Hoar, Sean B., Assistant United States Attorney, District of Oregon. "Identity Theft: The Crime of the New Millennium." U.S. Department of Justice Executive Office for United States Attorneys, USA Bulletin March 2001 Vol. 49, No.2
URL: http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm July 1, 2001

(5) Ricciardi, Sal. **"**In Pursuit Of Internet Intruders." Smart Business
URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2398494,00.html July 1, 2001

(6) Alvis, Sierra. "Credit Fraud Horror." MyPrimeTime, Inc.
URL: http://www.myprimetime.com/money/priorities/content/personal_firewall/index2.shtml July 1, 2001

(7) Noack, David. "The Back Door Into Cyber-Terrorism." June 2, 2000 URL: http://www.apbnews.com/newscenter/internetcrime/2000/06/02/computerholes0602_01.html July 1, 2001

(8) Ranch, David. "Linux IP Masquerade HOWTO." Linux Documentation Project. V 1.95,

November 14, 2000. URL: http://www.linux.org/docs/ldp/howto/IP-Masquerade-HOWTO.html. July 2, 2001.

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 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
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 Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event