Global Information Assurance Certification Paper

Sharon Waldbillig
GSEC Practical Assignment (v.1.4)
Patch Management: Easier Said Than Done
October 25, 2002

It all started innocently enough. The O.C.C. (Office of the Comptroller of Currency) had completed their yearly examination of our bank, and determined the Information Technology department had some weak spots that needed to be addressed. One of the issues was to identify and correct outstanding potential security issues. As we are not security experts, the bank contracted with a 3rd party vendor to perform an external penetration test, along with internal vulnerability assessments. The external penetration test would identify possible points of attack from an Internet-based hacker while the internal vulnerability test would focus its assessment on the threat from an internal adversary. Our external penetration test proved that we had our act together in preventing outsiders from entering in. However, the internal vulnerability report almost brought us in IT to our knees. The report contained pages and pages of vulnerabilities: workstations and servers were missing all kinds of security patches and incredibly old versions of Internet Explorer existed on some of our PCs. Then the worst, the absolute worst, there it was in black and white, most of our NT workstations had the Guest account enabled with no password. It was a long, long day in our department when that vulnerability report made its way to the executive board.

My job was to clean up this mess, before the next internal vulnerability scan took place. I'm a fairly optimistic person, and thought, "No problem, we are a small bank, we don't have thousands of employees. This assignment can't be that difficult". Now that I write this paper to submit towards my GSEC certification, I laugh to think how incredibly naïve I was. I never bothered to pay much attention to the Microsoft Security Bulletins, because they didn't really affect us. Our network is a private network with private addresses. Employee access to the internet is through a firewall and content filter, and as a member of the IT department, I can guarantee we block almost everything. The mailsweeper application checks e-mail for spam, viruses, profanity, attachments, etc. Remote access is not permitted, consequently not even set up on any of our servers. Lastly, our network is primarily Novell NDS, and not even the hackers have much interest in Novell. Our firewall, content filter, virus protection and mailsweeper applications are all current and up-to-date. We had prepared ourselves for an external attack, but now found ourselves forced to acknowledge the possibility of an internal attack. I fully recognize the danger of a misguided or vengeful employee. I also wish there was a way to say, "STOP"; this is getting out way out of hand. Our bank is a small community bank in a rural area. Myself included, we're not rocket scientists and putting food on the table takes priority over learning the latest Windows hacking techniques. We have a new teller system rolling out next month, retiring DOS workstations and replacing them with Windows 2000 Professional. Training is currently our very top priority, educating our users on basic Windows concepts such as multiple windows, the status bar, minimizing and maximizing screens, and the difference between a right and left mouse click. All this in-house security just does not make

sense in my mind, as there are so many other critical issues to be addressed. However, the O.C.C. does not share my opinion. Regardless of asset size, number of employees, number of branches, etc. all national banks face the same security regulations. The O.C.C. has even gone so far as to ask us (the bank) to provide to them our patch management policy by year-end. Bottom line, I need to pursue these security patch issues, and I need to make it work now.

This paper is about the rocky ride that I took down the patch management yellow brick road. It's one thing to read about security bulletins, it's a whole new world to have to implement them. I thought our workstations were in good shape. Our NT 4.0 workstations had service pack 6a installed, the virus pattern files get updated as soon as a new one is published, and all users had supposedly been updated to Internet Explorer Version 6. Most of our workstations are Windows 98 or Windows NT 4.0, with a few Windows 2000 installations, except for new teller system. As we planned our teller migration from DOS to Windows 2000 Professional, we made sure to include the latest Microsoft W2K Service Pack. Not only that, just two months ago, the Information Security Officer and I visited each workstation, installing the Security Bulletin MS02-015 for Internet Explorer. I truly believed there couldn't be that many security bulletins published that frequently, could there? Dream on! Did you know Microsoft is now releasing a new security bulletin on the average of every 5.5 days? I had a long way to go, before I came to terms with the reality of patch management.

As I first started to address all the unapplied security patches, it was easy. I had a copy of the internal vulnerability report, which included every single missing patch by workstation. Also included in the report, were recommendations to modify the workstation's registry to prevent remote registry access. I am not a fan of Regedit or Regedt32. Call me old fashioned or overly conservative, but having been burned in a previous life from registry modifications, my philosophy has been to stay out of these utilities! I don't care how easy the Microsoft Knowledge Base Articles make it sound, something always go wrong and the backup diskettes are missing or were never created in the first place. Yet here these much more knowledgeable security consultants were instructing me, and who am I to question them? What do I know? If they say to modify the registry, then that is what we'll do. These same experts also recommended disabling the Microsoft File and Printer Sharing capability as well as the Server Service. After all, the bank is a Novell network, not a Microsoft network. I didn't know at the time, but eventually this would come back to haunt me. As documentation is my specialty, I knew we would have to track these updates on the workstations. Using Visio, I developed these beautiful forms for documentation: a Workstation Security Update form and the Workstation Registry Modification form. As we updated a workstation we would fill out these forms, saving them for future reference. I originally assumed I would not be the one visiting all these desktops again; after all I design and plan the process. That dream died a long and painful death, no one in their right mind wanted anything to do with security patches. Meanwhile, I dutifully created a CD with all the required patches for Windows NT. First, I practiced on a few workstations, enhancing my forms, downloading patches, adding notes on what could and did go wrong with the patch installation. When my perfect package was complete, I selected

an older workstation, to run through this update process from start to finish, just to get a general time frame. This turned out to be the first of many eyebrow-raising experiences. I noticed right away, the Novell Client on the workstation was not the current version, somehow that update had been overlooked. Still confident, I upgraded the Client software and started my security patch updates. Two and ½ hours later, during which the workstation ran out of space on the local C: drive and I don't remember how many reboots, my task was completed. I was a little frustrated, but I had my first set of completed Security Update forms, and they looked good! I still had in the back of my mind I would impress the auditors and the O.C.C. with my organizational skills and system documentation. The very next morning, Microsoft released another critical security bulletin, one that needed to be applied to all our workstations. I could see what my perfect Security Update form was really worth, I threw it out…

It was pretty obvious multiple reboots, one after each hotfix was installed, was not a practical idea at all, unless I truly wanted to spend day and night at work. I started researching at the Microsoft web site concerning security bulletins and came up with Microsoft's QChain[1] utility which allows you to install multiple patches with only one final reboot. The instructions were simple enough: download each hotfix to its own directory on the local workstation, run each hotfix from the command line adding the –z switch. This switch prevents the hotfix from automatically rebooting the workstation. After all the hotfix patches have been applied, run the QChain utility, which will force a reboot of the machine. This utility also resolved the issue of applying hotfix patches out of order if you had managed to maneuver around rebooting after each installation. Under this scenario it is possible for an older version of an updated system file to be running. QChain runs on Windows NT 4.0 Workstation, Server, Server Enterprise Edition and Terminal Edition, but must be downloaded from Microsoft. Windows 2000 Professional and Windows 2000 Server post-Service Pack 3 (SP3) already include Qchain, eliminating the download requirements. I used this utility at an NT 4.0 workstation were I installed 5 security bulletins in random order. Preparing for the worst, I was thrilled when the updates and QChain utility ran without a hitch. Perhaps there was hope?

My next stop while wandering through Microsoft's Website was Windows Update[2], an online utility to apply recommended security patches. My god, it was all here! Microsoft provided me with the tool to resolve my security issues and I wasn't even aware of it. All I had to do at this website, was let Microsoft scan my workstation for recommended security updates. Within a minute, there it was, the list of suggested patches to apply. I printed the recommendations as documentation for the auditors and updated my machine. Only one reboot, it was so easy. I don't know why people make such a big deal of these issues, when there is such a simple solution. Triumphantly, I went to another Windows NT 4.0 workstation to test this uncomplicated solution. I selected the option to scan the system, and promptly got this error: "to display this page correctly, you need to download and install Visual Basic Scripting Support". No problem, there was a download box to click on, so I did. Nothing downloaded, instead it asked me for the Windows NT CD. I ran upstairs, grabbed the CD, ran back downstairs, loaded the CD, only to be told, "Install on Demand could not connect to the required network, etc". I tried various other solutions, but nothing would work. This workstation had been

previously upgraded to Internet Explorer version 6. Who knows why I thought of it, but I finally reinstalled IE6. Voila, this time Windows Update worked great, displaying the recommended security patches to install. I updated, reboot and things were looking up. Surely, my struggles with this older machine and the Windows Update process were a one-time fluke. Internet Explorer 6 had not been installed properly, but once that was corrected all problems were resolved. Joyfully, I went directly to my manager, announced our security patch problems were over, and I'd be happy to demonstrate using his computer. Just go to the Microsoft website, and ask it to evaluate your workstation. After we printed the list of recommended patches to apply, I confidently said, "Go ahead, and update". Obviously I was still out of touch with reality. The update abruptly stopped, no reason, just that the update could not be completed. A dump was provided that I could e-mail to Microsoft, but I chose not to at the time. After humbly returning to my cubicle to think this situation over, I realized it had to be the computer. It had been reassigned to multiple users over the course of the past two years. Who knows who, what, and when had played with that workstation? For all I knew someone had been in the registry making modifications. My solution was to attempt this update process on a workstation I personally upgraded to Windows 2000 Professional. I knew this workstation was squeaky clean. If you haven't guessed by now, the Windows Update also failed on this machine, same unable to complete error message as at my manager's computer. This time, I chose the option to send dump to Microsoft, fully explaining the entire situation, confident they would provide me with a simple solution. That was two months ago, and I'm still waiting.

Of course, my next step was to experiment with Hfnetchk[3], Microsoft's Network Security Hotfix Checker. Hfnetchk is a free, downloadable utility that will examine workstations and servers to determine what security bulletins or hotfixes need to be applied to secure the machine. Shavlik Technologies LLC developed this patch utility for Microsoft. An XML database, MSSECURE.XML contains all the available hotfixes for each Microsoft product currently supported. Information about each patch is stored in this database such as the associated security bulletin, all affected files with their new file version, each files' checksum, the registry keys modified by the patch, and the corresponding knowledge base article number. To run Hfnetchk requires an XML-parser, but a parser is included with Internet Explorer 5 and greater. A downloadable parser is available at the Microsoft web site, but please don't tell me anyone is using a version older than 5? When Hfnetchk is executed using the default options, MSSECURE.CAB[4] is downloaded from the Microsoft website and decompressed to the MSSECURE.XML database. Once running, Hfnetchk analyzes the workstation to verify the operating system, what service packs and software are installed to determine which security patches are applicable to your system. Hfnetchk employs 3 different criteria in determining if a patch has been applied. First the registry is examined, looking for the registry key with the corresponding patch number. Once the registry key is located, the modified file(s) version number and checksum are verified with the XML database. If all three factors check out to be true, then the patch is identified as "Found". Otherwise the security patch is labeled as "Not Found", with an accompanying error message describing where the check failed. Hfnetchk has many different run options. A few of the available options include skipping any of the patch determination checks, creating a wrapped or

tabbed output file of the scan results, and whether to use a previously downloaded local/network shared MSSECURE.XML database or download the most current one from the Microsoft web site. Best of all, it can scan remote workstations by either IP number or Netbios Name. Too bad, I didn't read the fine print, that the server service and remote registry access are required. But at the time, the thought of not running across the street, up and down the stairs between departments was appealing.

I have 2 workstations, one with NT 4.0 and the other with Windows 2000 Professional. Experimenting with Hfnetchk on my machines, I became familiar with many of its options, creating tabbed output files and importing them into Excel, producing these great spreadsheets that eventually meant nothing. Actually, I was pretty impressed with the results. I ran a scan utilizing the history option to see what that looked like. This was my first introduction to the "Note" status. For example, the status for MS-022 was "Note", not "Found" or "Not Found". It turns out that Hfnetchk is unable to determine the installation status of a number of hotfixes, and those are flagged with a "Note" status. If you refer to Microsoft Knowledge Base Article Q306460, each undeterminable patch is explained in detail as to why it fit in this category. MS02-053 also had a status of "Note", but that was not referenced in the Knowledge Base Article. I guess sometimes it's up to the patch manager to keep track of what was installed, and that thought does not thrill me. I also learned that the history option is not just plain old history, but a history of whether patches were explicitly installed or not. Hfnetchk can only tell if a patch was specifically applied. For example, the Windows NT 4.0 post-SP6a Security Rollup Package is MS01-041, which encompasses approximately 20 earlier security fixes. MS01-031 is one of the included patches. If you were to install the SRP MS01-041 and did not previously specifically install MS01-031, then the history option would not show MS01-031 as found. As long as you know it, then there shouldn't be any surprises.

By now, you would think I would be happy with my Hfnetchk results; a concise list of recommended patches to apply, a checklist created from the output scan file. But NO!!!!! I had to run Windows Update. After all, they are both Microsoft products, I should get the same results, right? You would think by now I would know better, but apparently I didn't. I know now that the two products utilize two different databases and were written by different developers, but I somehow I thought they should still be similar. Using my primary Windows 2000 workstation, I ran the two utilities. At least both searches indicated that this workstation needed Internet Explorer 6 Service Pack 1 installed along with MS02-055. Windows Update also recommended installing MS02-051, MS02-052 and MS02-058 while Hfnetchk indicated nothing. I have since learned that Hfnetchk does not cover Outlook Express which explains why MS02-058 was not on Hfnetchk's list. I'm sure if I pursue these other two patches I will come up with a valid explanation, but why bother. I can see what I am up against. You can't win either way.

Stil, I needed to continue on with my testing, and decided to test the remote option on a Windows NT 4.0 workstation. My first attempt immediately failed, with an "Authentication Error, WnetAddConnection2 returned 67" (the network name could not

be found). It didn't take too long to figure out this problem. Remember our security experts recommended that we turn off the File and Printer Sharing capability, as it was a potential vulnerability? This turned out only to be the first reason why the remote scan did not work. With a little more research at the Microsoft web site, I came to learn that in Windows NT 4.0, disabling the File and Printer Sharing capability is essentially also disabling the server service. This rang a bell in my memory concerning our new W2K teller workstations. Sure enough, the workstations had this service removed from the Local Area Connection along with the Server service disabled. I was not done being punished by the patch demons because Hfnetchk still would not run on that workstation. It turned out to be because I had removed remote registry access through registry modifications to eliminate that vulnerability too. I couldn't wait to explain this to management, why we need to have known vulnerabilities on all our workstations in our non-Microsoft network in order to use Microsoft's security utility tool. About the same time, I took my completed Registry Modify Forms I created earlier, and threw them in the trash.

I decided my next logical step in this patch process; I should at least look into Microsoft's Baseline Security Analyzer. Again, until I got involved in this process, I was not aware of its existence. Before attempting to use this utility, I read MBSA's white paper[5]. Basically it is a GUI version of Hfnetchk with additional enhancements. MBSA uses the same XML security database as Hfnetchk, and the same three factors to determine if a patch was applied. Some of MBSA's enhanced capabilities include a reporting feature locally storing the scan report, a check to see if Guest was enabled, simple examination of passwords looking for blanks, matching user name, etc. and look for unnecessary services running on a workstation. MBSA can also scan all the machines in a specified domain, determine if a workstation's hard drive system is formatted with NTFS, check if the machine is a domain controller, and check basic system configurations on an Internet Information Server (IIS) and SQL Server. It amused that this white paper pointed out that depending on which Hfnetchk options were selected to run, the scanned results could be different than the MBSA results. What a surprise! Since I had familiarized myself with Hfnetchk, was painfully aware of our Guest account situation, and we do not participate in a domain environment, I opted not to bother experimenting with the Security Base Analyzer.

By now, I am reading everything I can get my hands on concerning the subject of patch management. I came across an article entitled "Patch Management Done Right[6]". Tim Mullen, the author, stated right up front, he was a "card-carrying Microsoft supporter", but as the CIO at AnchorIS.com he recognizes how critical maintaining current security patch levels can be. His article briefly described both Hfnetchk and Microsoft Security Baseline Analyzer function. It was the usual upbeat introduction to two free tools, supplied by a concerned Microsoft. His enthusiasm for MBSA was so great that he even stated "The tool rocks. Microsoft's Laura Sosnosky, who 'owns' MBSA, deserves kudos". Wow, I must be doing something wrong to not fully appreciate the value of these indispensable tools. Then I began reading the reader feedback and cracked up. To this author's credit there were a few positive comments on Microsoft and their direction toward security management. The rest were all negative, some very negative.

I especially liked the reader whose comment started out, "You must have gotten the working version then." Obviously, I was not alone in patch management hell. Many of the readers had experienced much worse problems than I had even imagined. I couldn't wait to go out and scan more workstations!

Automated patch management started to sound like a pretty good idea to me. I came across an article "PatchLink Helps Keep Windows Closed"[7] published in Network Computing Magazine comparing automated patch management products. Their test environment included 20 servers, 1,000 workstations, utilizing Microsoft Windows 2000 Professional, Windows NT 4.0 Workstation, Windows 98, W2K Server with IIS and SQL, and finally Windows NT 4.0 Server with IIS. Each patch management application would be tested for their ease in installation, the patch update process, and the managing capability of the patch levels. The total cost of the software and licensing could not exceed $50,000. Five products were chosen to evaluate:

1) BigFix: BigFix Enterprise Suite
2) Gravity Storm Software: Service Pack Manager 2000
3) PatchLink Corporation: PatchLink Update
4) Shavlik Technologies: HfnetchkPRO Enterprise
5) St.Bernard Software: UpdateExpert

Basically, these five packages operate in one of two methods. The first and probably easiest just scans the hosts from a workstation, checking for applied patches. This normally requires the Server Service enabled, Remote Registry access permitted, and local Administrator rights to each host scanned. The second method used is agent based, where the client agent software is installed on each host, and runs in the background. The client agent periodically polls an in-house "patch server", inquiring if new patches need to be applied. Non-agent based products work well in a static network environment, where roaming users and remote site WAN connections do not exist. The software is installed only on the workstation that will be scanning. On the other hand, agent-based products require additional time to setup a patch server, along with visiting each host to install and configure the agent. Network Computing selected PatchLink as the overall winner. Based on this article, I chose which patch management packages I would test. I eliminated BigFix Enterprise Suite immediately due to its cost at around $30,000 while the others all came in between $11,000 and $12,000. Even if BigFix had been chosen as the superior patch management tool, that price range was beyond our budget capabilities. I also eliminated Gravity Storm Software, as it came in last due to its lack of reporting features. Shavlik and St. Bernard products seemed pretty much the same. I ended up choosing Shavlik, as they were Hfnetchk's developer and because of their Gold Certified Partner relationship with Microsoft.

At Shavlik's web site, I downloaded HfnetchkLT[8], which is a demo or light version of HfnetchkPRO. HfnetchkLT will scan all your workstations and provide you with the hotfix status, but it will only let you apply two patches at a time per deployment. Installing the application on my W2K workstation went smoothly, as did scanning most of the workstations in my immediate area. I was able to quickly determine what and how to scan, different options to select a scan, and deploy security hotfixes. Once I

selected a workstation to update, HfnetchkLT Patch Deployment Guide walked me through the process, which included a stop at the Download Center. The Download Center is a database of all accumulated patches, hotfixes and service packs for the Windows O/S systems. At that point you can select to download only the patches you are going to install. Of course, at any time you can also download as many patches as you want, or everything available for a specific operating system. When I was ready to test the patch update process, I selected a Windows NT 4.0 workstation, and chose to deploy all patches. HfnetchkLT reminded me of my two-patch limit, and selected the first two patches to update. The process was smooth enough, but the output log file surprised me. The status messages stated that 'MS01-022, MS02-006 - Attempted to deploy this patch. Please re-scan to verify patch installation". Wasn't HfnetchkLT sure? I hadn't planned on rescanning a workstation every time I deployed a patch. I re-scanned the computer and yes; MS02-006 security bulletin had been applied. MS01-022 looked the same as it did before; it had an Informational Message attached to it. I knew immediately this was one of those patches that Hfnetchk cannot determine if the patch was applied. Since the workstation I was experimenting with needed additional patches installed, I selected deploy all patches again. After the two patch limit reminder, HfnetchkLT went ahead and re-applied MS01-022 along with MS02-050. Same log messages: re-scan to verify patches were installed. MS01-022 had the same Note indication. I was disappointed in that it appeared any patch that belonged to the undeterminable group, would be applied every time deploy all patches was selected. That leaves me to manually check and uncheck any patch with a Note status, another manual process. Also, I quickly got tired of entering the Administrator user id and password every time I wanted to scan or deploy a patch. I realize it is because Hfnetchk needs authorization for access, but I just get tired of re-keying the same information over and over again. I was a little frustrated with HfnetchkLT, in that I expected the software to tell me if the patch installation was successful or not, not rely on me to rescan the workstation. All in all, even though I wasn't raving about Hfnetchk, I would still consider purchasing HfnetchkPRO because it beat my sneaker netting.

As a side, while learning the ins and outs of HfnetchkLT, I came across two great support sites that answered so many of my questions. The first was at Microsoft's TechNet site, where there are public newsgroups for all kinds of Microsoft products. There is a newsgroup for Hfnetchk[9] under Security and just reading through the previous discussion questions opened doors for me. The discussions also recommended Shavlik's newsgroup that had included specific forums for Hfnetchk, HfnetchkLT, and HfnetchkPRO[10]. This site was too much! First I learned that the Hfnetchk I downloaded from Microsoft was an old version (version 3.3.2) released in February. If you download Hfnetchk from Shavlik, you get version 3.83 with has some nice enhancements. But the big shocker was discovering that there are two different versions of MSSECURE.XML. Microsoft has theirs, but Shavlik also has their own, an enhanced version of Microsoft's. One example is Shavlik's version of MSSECURE.XML handles the Note issues with MS01-022. I reran Hfnetchk using Shavlik's XML file and the scan reported different results than the original scan. I could not really describe what I felt, between anger, frustration and no hope for this patch management project.

Does the average IT person know all this already and I'm just an idiot? I cannot believe the incredible amount of time I have spent doing research and testing.

Still feeling pretty discouraged, I began reading the white paper for PatchLink Update[11]. I started to perk up when I read all the features this package had. First of all, PatchLink can update Windows 98 machines. HfnetchkPRO and any other non-agent patch management software require remote registry access for patch installation, which is not available on Windows 95 and Windows 98. Many of our workstations are still Windows 98. We plan to upgrade them next year, but there are no guarantees and this feature could easily improve the quality of my life short-term. Another feature of PatchLink is its ability to update virus pattern files, a process that is almost becoming a daily procedure. We do use the automated update feature with our current anti-virus vendor, but have experienced problems with Administrator sign-on, server and workstation services, etc. PatchLink will also distribute software to workstations, which could really decrease our sneaker-net time when departments purchase new software packages. Other features include workstation inventory, software and hardware inventory change control; notifying the administrator if a user modifies, adds or removes software or hardware at their workstation, downloads taking place in the background, automatic download resuming if the download was disconnected for whatever reason, and it can update multiple vendors' software and operating systems, not just Microsoft. Communication between the patch server and PatchLink's Update Master Archive utilizes a 128-bit SSL connection when downloading security patches. The information itself is encrypted, compressed, CRC checked and digitally signed. Obviously security is a priority.

No need to say anymore, PatchLink Update sounded fantastic. The only drawback for me was that it requires a Windows 2000 server with Internet Information Services loaded. We don't have a spare server, which immediately becomes a budgetary concern. Desperately searching for equipment, I found a very OLD NT 4.0 server, that I could upgrade to W2K. It wouldn't be fast or elegant, but at least we could see PatchLink Update 4.0 in action. I downloaded the evaluation version of Update 4.0[12], which includes 10 client licenses with a 14 day evaluation period. Update's deployment guide walked me through the installation on my new patch server, as well as installing the client software on my two workstations. The patch server quickly identified what patches my workstations needed and I sat back ready for PatchLink to began downloading patches from the PatchLink Archive Master. It seemed like the download process was taking an extremely long time. Well the download wasn't taking a long time, because the download wasn't happening. An experienced PatchLink user would have picked this up immediately, but I was pretty much in the dark. I called my PatchLink Account Executive, who immediately got technical support involved. These guys know their product and had my problem corrected in a very short time. Somehow I had managed to mangle the client agent on the Patch Server, so the software was trying to download the patches, just not having any success. Anyways, I was very impressed with the support group's efficiency and attitude. Within a couple hours, my patches were downloaded. I selected a patch to be applied to my workstations and poof it happened! The patch installation took place! It was so cool; I had to try it again. It worked again! I had a week left on our evaluation copy and seven additional licenses

to experiment with. I can't begin to tell you how much I liked this software package. I was sure it would prove to be a valuable asset for our department. With PatchLink's Update patch management software, just maybe, I could return to my real job of network support.

As my story comes to its end, I wish I could tell you "and the IT department lived happily ever after….". It doesn't because this is the real world; and in the real world there are budget constraints. Next year's budget will include the purchase of a Windows 2000 Server and patch management software. My choice is absolutely PatchLink Update, and I look forward to the day it is up and running. In the meantime, I will apply hotfixes, service packs and support rollup packages the old fashioned way. I'll use HfnetchkLT to assist me in remotely scanning all our workstations, and from that I'll build some sort of inventory tracking spreadsheet. If I feel like tormenting myself, I'll probably play with the Windows Update again and maybe even experiment with Microsoft's Security Base Analyzer. I desperately need to sit down and address the nine new Microsoft Security Bulletins that have been published since I started this paper. The Information Security Officer and I have designed a form to use when I review the bulletins. It includes a brief description (in layman terms) what issue the patch resolves, how critical it is, what workstations are affected, and if and when I installed the hotfix. These forms along with my patch inventory will be available for the O.C.C. to examine at year-end satisfying their requirement. It's the best we can do given our situation. If there's one security measure I have been effective at, our users are employing their screen saver when they leave their desk. They have learned, if their computer is not locked and I am lurking about, chances are their machine is going to get updated. Meanwhile, my life has been changed forever with respect to Security Bulletins and hotfixes. I just treated myself to a brand new pair of sneakers, while I enjoy my new career as Patch Manager Extraordinaire!!!!

---

[1] Use QChain.exe to Install Multiple Hotfixes With Only One Reboot;
Microsoft Knowledge Base Article Q296861;
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q296861

[2] Microsoft Windows Update
Windows NT 4.0: http://windowsupdate.microsoft.com
Windows 2000: http://v4.windowsupdate.Microsoft.com/en/default.asp

[3] Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available
Microsoft Knowledge Base Article Q303215
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q303215&sd=tech

Frequently Asked Questions about the Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool; Microsoft Knowledge Base Article Q305385
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q305385

Hfnetchk.exe Returns NOTE Messages for Installed Patches;

Microsoft Knowledge Base Article Q306460
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q306460

[4] MSSECURE.CAB download
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab

[5] Microsoft Security Base Analyzer White Paper
http://www.microsoft.com/technet/security/tools/tools/mbsawp.asp

[6] "Patch Management Done Right", Tim Mullen, May 6, 2002
http://online.securityfocus.com/columnists/79

[7] "PatchLink Helps Keep Windows Closed", CMP Network Computing;
Tim Mullen, September 2, 2002
http://www.nwc.com/1318/1318f3.html

[8] HfnetchkLT: Shavlik Technologies LLC, St. Paul, MN
http://www.shavlik.com/security/prod_hf.asp

[9] Microsoft Newsgroup Hfnetchk
http://www.microsoft.com/technet/newsgroups/?url=/technet/newsgroups/NodePages/security.asp

[10] Shavlik Newsgroup Hfnetchk, HfnetchkLT, HfnetchkPRO
http://news.shavlik.com

[11] PatchLink Update 4.0 White Paper; PatchLink Corporation; Scottsdale, AZ
http://www.patchlink.com/support/documents/PUW4.html

[12] PatchLink Update 4.0 Download; PatchLink Corporation; Scottsdale, AZ
http://www.patchlink.com/forms/evaldisplay1.asp

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event