



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

Patch Management in a Windows Environment Revisited

Joe Maloney
February 9, 2003
GSEC v.1.4b

Overview

The outbreak of the SQL Slammer/Sapphire worm brought back the old issue of patch management. As the events unfolded and the worm was unraveled, once again we saw a need to improve security in our community. This event became like déjà vu to many of us. Many people were quick to slam Microsoft once again and jump on the anti-Microsoft bandwagons for their poor security in their products. Internet news articles had flashy headlines about the insecurities of the internet. Then the focus slowly turned to the administrators and the question arose. Why were so many systems vulnerable to an exploit in which a patch had been released for quite some time? This same question was asked when Code Red and other similar malicious codes were released. With this latest example of exploiting systems, my first reaction was history repeats. From the internet community our human nature surfaced as our defense mechanisms took over. Reasons such as patches were complicated to install, there are too many patches to keep up with, limited budgets, and time constraints began to surface.

As I sat down to write this document, I thought about the purpose of the Sans reading room (www.sans.org/rr) which is to help out in the security community. So I decided to share some of my methods of keeping vulnerabilities down to a minimum. This document will discuss some methods of identifying systems that need patches and some methods for implementing patch management. These solutions are all free and some I have provided a couple of scripts that I've developed. Primarily, this document will focus on four tools. They are HFNetChk.exe, Microsoft Security Baseline Analyzer, HFNetChkLT, and Microsoft Software Services. The reason free tools were chosen is because many administrators, myself included, have limited budgets and huge networks. We are always behind it seems by the time we wade through mountains of log files from servers, firewalls, and IDS systems. Without the manpower and the budget, we need to share methods of making our lives easier while helping to do our part in keeping our community secure.

Importance of Patch Management

I'd like to discuss the reason patch management is so important. This section is aimed at the security administrator or system administrator who is new to the field or to those that need convincing. In an online article by Jay Lyman, he suggests that administrators would keep up to date with patches if they would calculate the business impact if the systems were left unpatched (<http://www.ecommercetimes.com/perl/story/19023.html>).^[1] This idea leads to an important discussion. By placing, calculating and assigning risk, you are in effect developing a policy. Lyman goes on to quote Mike Rasmussen, research

director for Giga Information Group (www.gigaweb.com) pointing out the need to make it a policy. "It's just a matter of getting it to be part of [the systems administrators'] function. You should establish a policy and enforce it. This shouldn't be a guideline. This should be policy." ^[1] This is a very good point. After all, isn't the first thing you read about in regards to security is developing security policies and procedures. The policy will describe who is responsible and outline the risk involved for each system. This is necessary to our job function and to ensure we stay on top of patches.

Tim Mullen from Security Focus (<http://online.securityfocus.com>) makes a substantial point as well by saying "if you own the server, you own the responsibility of keeping it patched no matter what OS or applications you choose to run on it." ^[2] It is up to us as a community to help prevent the exploitation of known vulnerabilities. We need to band together and help each other gather ideas and methods for discovering systems that need patches and actually installing those patches. Research from GartnerG2 (www.gartnerg2.com) "projected that through 2005, 90 percent of cyber attacks will exploit known security flaws for which a patch is available or a solution known. In addition, the research firm said, 90 percent of attacks are of the copycat variety." ^[3]

As if this was not enough reason, there have been recent discussions over what has been termed as downstream liability. This basically says that a company could be sued for systems that are unpatched and used in an attack such as a DDOS attack. ^[15] So how do we protect ourselves and the company? How do we accomplish the daunting task of keeping up with updates? The next few sections will deal with some solutions for tackling this task. It is recommended to test all possible solutions and find the best that fits your needs. This list also in no way reflects all solutions out there. Most of these solutions have short comings and if possible, a commercial product should be purchased to help implement a stronger patch management policy. There also may be features within an Active Directory environment that could be taken advantage of. This is aimed at a small network or a large network that is still a NT 4.0 domain.

Identifying and Installing Patches

The next step is to identify the systems in your environment that need patching and how these tools can help you deploy and install patches and service packs. In this section I will discuss four tools. They are HFNetChk.exe, HFNetChkLT, Microsoft Baseline Security Analyzer, and Microsoft Software Update Services. HFNetChk.exe can produce reports for identifying systems that are missing patches however it cannot install the patches. There are some suggestions for using this tool with others to deploy patches. Microsoft Security Baseline Analyzer strictly gives information on what patches are missing on systems. It also gives other valuable security information for locking you're your systems however those are no the topic of this document. HFNetChkLT uses HFNetChk.exe and the qchain utility to identify systems that are missing patches and to install those patches. However, since this is the free version of a commercial product it has some limitations. Microsoft Software Update Services

uses the automatic update service to get updates to systems. However this tool can only update Windows 2000 and higher systems. It has other limitations as well that are discussed. These tools can be obtained from the following sites:

Microsoft Baseline Security Analyzer (MBSA) (version 1.1 current for this document):

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp>

HFNETCHK (version 3.86 current for this document):

<http://www.shavlik.com/pHFNetChkEXE.aspx>

HFNetChkLT (version 3.8.103 current for this document):

<http://www.shavlik.com/pHFNetChkLT.aspx>

NOTE: MBSA provides command line functionality that performs the same procedures as hfnetchk.exe. In this document I will discuss some custom scripts that utilize hfnetchk.exe. The results of the scripts have not been tested using the command line options for MBSA. The scripts are provided as examples of how to use these tools to schedule scans and give administrators ideas on how to use the tools that are provided for administrators and to expand on them if they choose.

Microsoft Software Update Services (SUS) (SP 1 current for this document)

<http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp>

Patch Implementation Issues

Patch implementation is a company policy issue and this is something that needs to be determined before selecting the right tool. In this document, I will discuss using manual methods using hfnetchk reports and MBSA reports, custom scripts, Microsoft's Software Update Services, HFNetChkLT to identify and install patches using these tools.

There are a few different options for installing patches manually:

- Use the text file produced by hfnetchk for each system, go to that system, look up each missing patch and service pack, download and install the patch while rebooting each time if Windows NT 4.0, and run hfnetchk again to ensure all patches were properly installed. Then move to the next computer. Obviously, this method is very tedious.
- Use the report produced from the MBSA tool, go to each system and update the patches one by one listed in this tool. This is the same as above however the reports are in html format.

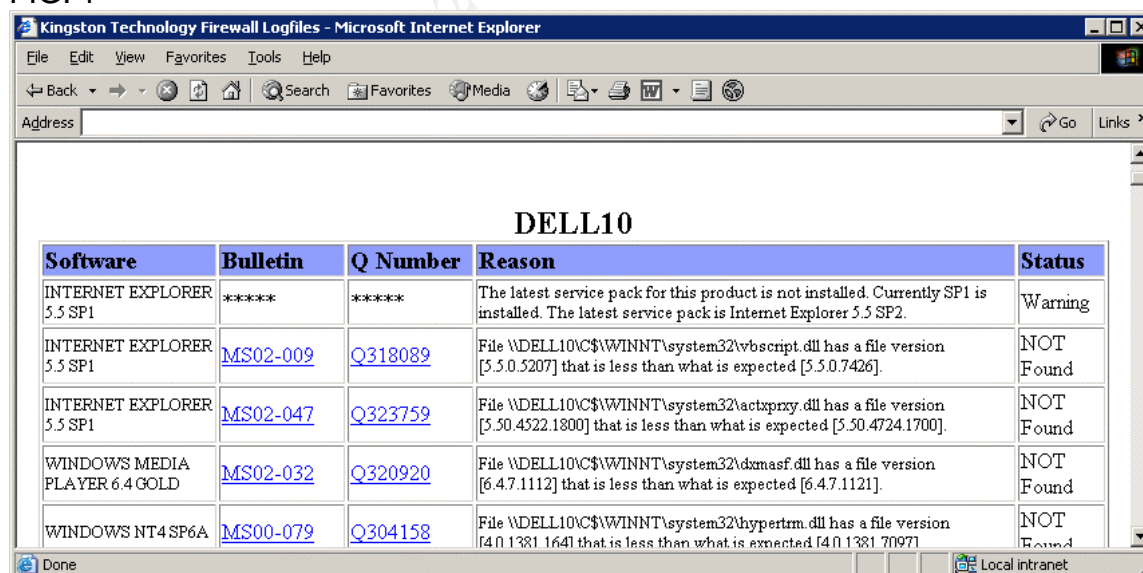
A drawback to both of these methods is that they are time consuming especially if you have a large network.

Another problem with these methods is the reporting. Hfnetchk produces a flat text file that either has to be printed or needs to be placed onto a share that can be accessed from each computer. From the report, you then have to search for each Q article listed to download the missing patch. MBSA stores the reports

in XML files that are stored in the local computer in which it was installed. The default location for the files is <systemdrive>\documents and settings\username\scan reports. The files can only be read from the machine that has MBSA installed. So unless these reports are printed, it is very difficult to view them from the system in which you need to install the patch.

To help with this problem, In Appendix B and Appendix C, I have written DOS scripts that will use hfnetchk, scan servers based on a text file list of servers and produce the results in asp format which can be outputted to a server running IIS or any other web server platform. The setting that uses the text file list of servers can be replaced in the script to an IP range, domain, or any other setting that hfnetchk's command line switches support. Hfnetchk's command line switches are listed in Appendix A. For proper IIS security settings, please refer to <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp> . For other web platforms, please refer to your software manufacturer's recommendations or search for your platform on various security web sites such as <http://www.sans.org>. By placing the results on a website, you can now view the results in a browser when you are at the computer that needs the patches. The script will organize the systems alphabetically on the web page. Because this page contains sensitive information about the security of your servers, I recommend placing access controls such as authentication to the website. This way only those authorized can view this material. Fig. 1 shows an example of what the page looks like. Each missing patch, warning or note produced by hfnetchk has a link to Microsoft's site where the proper information can be found. Now you can just click on each link to install the patches.

FIG. 1



The screenshot shows a web browser window titled "Kingston Technology Firewall Logfiles - Microsoft Internet Explorer". The address bar is empty. The main content area displays a table titled "DELL10". The table has five columns: Software, Bulletin, Q Number, Reason, and Status. The table lists several missing updates for Internet Explorer 5.5 SP1 and Windows Media Player 6.4 Gold.

Software	Bulletin	Q Number	Reason	Status
INTERNET EXPLORER 5.5 SP1	*****	*****	The latest service pack for this product is not installed. Currently SP1 is installed. The latest service pack is Internet Explorer 5.5 SP2.	Warning
INTERNET EXPLORER 5.5 SP1	MS02-009	Q318089	File \\DELL10\C\$\WINNT\system32\vbscript.dll has a file version [5.5.0.5207] that is less than what is expected [5.5.0.7426].	NOT Found
INTERNET EXPLORER 5.5 SP1	MS02-047	Q323759	File \\DELL10\C\$\WINNT\system32\actxprxy.dll has a file version [5.50.4522.1800] that is less than what is expected [5.50.4724.1700].	NOT Found
WINDOWS MEDIA PLAYER 6.4 GOLD	MS02-032	Q320920	File \\DELL10\C\$\WINNT\system32\dxmasf.dll has a file version [6.4.7.1112] that is less than what is expected [6.4.7.1121].	NOT Found
WINDOWS NT4 SP6A	MS00-079	Q304158	File \\DELL10\C\$\WINNT\system32\hypertm.dll has a file version [4.0.1381.164] that is less than what is expected [4.0.1381.7097].	NOT Found

An advantage to this script is that it can be scheduled to run daily, weekly, monthly, etc and allows you to have the results quickly at your finger tips to

implement the patches. The web page it produces can be customized with your company's logo and anything you see fit.

A further improvement to the process would be to download all the patches and hot fixes, then write a script using the Microsoft qchain utility (<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q296861&sd=tech>)^[8] to install multiple hot fixes at once. Appendix E shows some examples of a script from Microsoft's page and the command line switches for qchain. This previous link also describes a limitation of the qchain utility in which it will not work with hot fixes that contain binary files listed in the registry key

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\KnownDLLs.

A reason for installing each patch manually could be that the administrator needs to control patch installment. All patches should be tested on test systems before applying to production systems. There are instances where services may break, patches may cause blue screens, or in-house applications may fail due to the patch installment. Because of these situations, all patches should be tested on test systems that mirror the systems on your network. For example the Windows NT 4.0 Security Roll-up critical update could cause blue screens on Compaq Servers that had old versions of drivers for certain raid controllers. The driver needed to be updated before the patch could be installed (<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B305228>)^[9].

HFNetChk.exe

HFNetChk.exe was developed with Microsoft in its early stages of Trustworthy Computing. Trustworthy Computing was a concept coined by Microsoft to show customers that it cared about the security of their products and that Microsoft was taking steps to secure its applications. This was one of the first tools they released to help administrators identify the absence of security patches.

Pros

From the command line HFNetChk.exe can scan single or multiple computers for patches and service packs for Windows NT 4.0, Windows 2000, and Windows XP. It will also scan for hot fixes and service packs for IIS 4.0 and 5.0, Internet Explorer 5.01 and higher, SQL Server 7.0, SQL Server 2000 (including MSDE), Exchange Server 5.5, Exchange Server 2000, Windows Media Player, Front Page Server Extensions, Microsoft Java Virtual Machine, and MDAC.

Because it is a command line tool, it can be scheduled, it can be scripted, it can be run from almost any system as long as the operating system that it is run on is Windows NT 4.0, Windows 2000, or Windows XP. The output can be saved into various formats to be imported into databases or Excel spread sheets. Results can be placed in plain text files to be read.

Appendix A lists the help file from HFNetChk.exe and shows the flexibility and many options it has in which to run to produce the desired results you need.

Cons

Reports that are in text format would somehow be viewed at each system. Each patch would then have to be looked up on Microsoft's website in order to install it. No easy procedure for going from identifying the systems that need patches to actually applying the updates to the system.

Possible Uses

A possible use for this product is to create batch jobs that scan the network on a scheduled basis. The AT command in Windows NT 4.0 could be used or Windows 2000 task scheduler could be used to schedule the batch job. The reports could be stored on a properly configured share in which only the administrator had access. From there, the report for a particular system could be viewed and the patches downloaded and installed.

This is the same procedure I began to deploy for our servers. Looking up each patch became very time consuming. A better method needed to be created. How could these reports be viewed as a website? I wrote a script that would use the HFNetChk.exe tool and produce output from the results into .asp format. The report would then be saved to a web server. There are numerous documents on the proper procedure for securing a web site and this document's focus is not that. The procedure consists of two scripts. One script executes the HFNetChk.exe command and saves the reports into a file. The second script takes the reports and converts them to .asp. Appendix B has the code for the first script which is called hfreportmkr.bat. Appendix C has the code for the second script called hfnet.bat. These reports were designed to be run on the same web server in which the reports would be viewed. The hfreportmkr.bat uses two text files for the list of servers to be scanned. These are the Netbios names of the servers. I did this because I had servers on my internal network that used different Administrator accounts and passwords than the ones used for my DMZ network. Using the text files allowed me to just update those files and keep the reports moving. Now I could go to a server that needed patches, go to the web site I setup. When hfnet.bat produces the .asp file, it creates links to the Q articles for each patch and the Message article. Now I could go to the server that needed patches, go to this website, and click on the links to get to the patches this server needed. This method for discovering and deploying the patches gives the administrator full control over what patches should be installed. Installing them one by one also reduces the risk of a patch failing during the install as the administrator is watching the progress.

You could take this one step farther and download all patches for each operating system and software such as IE and place them into a shared folder (with proper security permissions set). Then write a batch file that takes the original report and uses Microsoft's qchain.exe (<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q296861&ID=kb;en-us;Q296861>)^[13] to install the patches. Appendix D shows the command line switches for qchain.exe and a sample script which is from Microsoft's web site (<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q296861&ID=kb;en-us;Q296861>)^[13]. I'm sure there are better methods for implementing this. I'm also aware that one could just as easily use Microsoft's update site <http://www.windowsupdate.microsoft.com> to accomplish this same task.

However this is to provide alternatives to methods that some people may not want to use because of policy or other security concerns.

HFNetChkLT

This product is produced by Shavlik who co-created with Microsoft the hfnetch command line utility. This is the free version of the HFNetChkPro software (<http://www.shavlik.com/pHFNetChkPro.aspx>).

Below are some of the features in version 3.8.103 ^[14]

- Push Windows XP Service Pack 1 along with many other service packs
- PatchPush^(tm) with 3 mouse clicks!
- Supports Microsoft Windows XP, 2000, NT
- Supports Microsoft Exchange 5.5 & 2000, SQL Server 7 & 2000
- Supports Microsoft Windows Media Player, IIS, IE, Java, FPSE and NT4 Terminal Server
- Supports outbound authenticated proxy
- Fully automated Patch Download Center
- Non-proprietary patch database in XML so you can understand what each patch is doing
- Push both hot fixes and Service Packs
- See what patches have been explicitly installed

The features described were taken from the product guides on their website. (<http://www.shavlik.com/pHFNetChkLT.aspx>) ^[14]. This tool is very useful for pushing Windows Updates and Service Packs to remote systems. It also bridges the gaps between Microsoft's Software Update Services Server by providing patch updating to Windows NT 4.0 systems.

Pros

The software will scan an unlimited amount of servers and will detect missing patches and service packs for Windows 2000, Windows XP, Windows NT 4.0, Exchange 5.5 and 2000, SQL Server 7 and 2000, Windows Media Player, IIS, IE, Java, FPSE, and NT 4.0 Terminal Server.

Based on the patches needed, the Download center will centralize the download of patches to prepare them for installation. This feature allows you to download the patches once instead of multiple times for multiple systems. HFNetChkLT also allows you to specify a proxy server for downloading patches to the Download Center.

HFNetChkLT will produce a report based on machine name of missing patches. Other reports are available in the pay for version HFNetChkPro.

If the system used to scan and deploy is not an administrator of the system that needs the patch, the deployment wizard has an option to specify an administrator account in which to Run As. This is an important feature. It tells you that for one, the system installing patches needs to have administrative privilege to install the patches or you need to specify that when rolling out the deployment.

It gives the administrator deploying the patches control over the installation of the patches such as whether it should be installed quietly (meaning no pop-up messages or prompts), whether the system should be rebooted after the install (recommended), how much bandwidth to use while it copies the patch from the deployment system, and whether it should backup files for uninstall. These are important features to administrators to control depending on the environment or the company's policies and procedures which may dictate these settings for that company's patch deployment. Whatever the reason may be these features are important and key benefits of the software.

Cons

Because this is the free version, it will only allow you to install patches and service packs for Windows 2000, XP and NT 4.0. It will not install updates to Exchange 5.5 and 2000, SQL Server 7 and 2000, Windows Media Player, IIS, IE, Java, FPSE, and NT 4.0 Terminal Server. The PatchPush™ technology for those programs is only supported in the licensed version HFNetchkPro. This is a similar issue with Microsoft Software Update Services. Also, it only allows you to install 2 patches at a time on a particular system. The idea here is that we need to find a way to patch systems not covered by the Microsoft Software Update Services. Microsoft's SUS server will only update Windows 2000 and above. We need this as a possible solution to Windows NT 4.0 systems that might still be hanging around.

I've seen arguments about patch deployment software that state that patches once they are downloaded are not validated before they are installed on the systems. This means that potentially, someone could replace the patches on the deployment system with malicious code and give it the same name as the patch. My argument against this fact, as I have seen this argument with numerous patch deployment products, is that if someone can replace a patch on your patch deployment system, then they have already compromised your network and this may be the least of your worries. As an administrator concerned with security, you should be following correct guidelines to secure the system that will be deploying the patches no matter what deployment software is used. This once again points responsibility back to the administrators in following good practices in securing their environment.

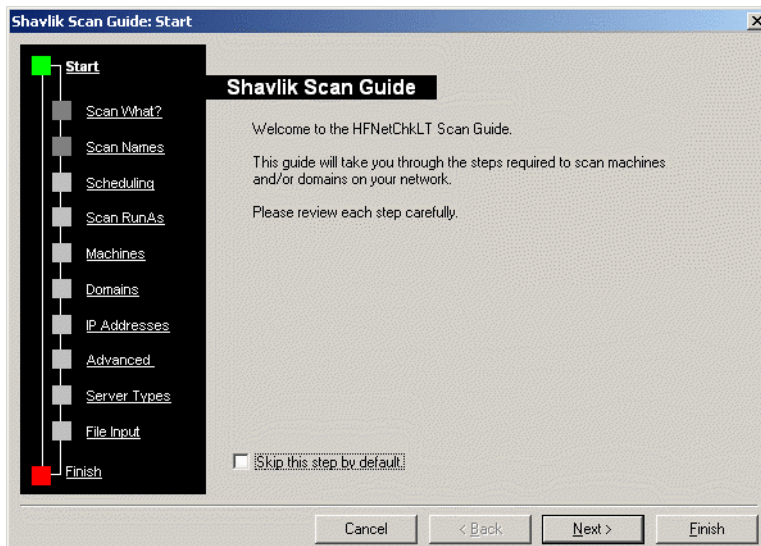
Since this is a free version, once a scan is created it does not save all of the settings for that scan. It will save it as a Favorite, however it will not keep the settings as far as what to scan and when. This means manual intervention is required each time a report is needed. In this situation, the scan should be scheduled to keep up with current patch issues.

Possible Uses

This software can be used as a gui tool to scan your network and identify systems that need patches. It can also deploy patches from a central location. However, because the free version has the limitation of only pushing two patches out at a time, this should only be used on systems in which better methods are not available such as Windows NT 4.0 systems. We will use the rest of this

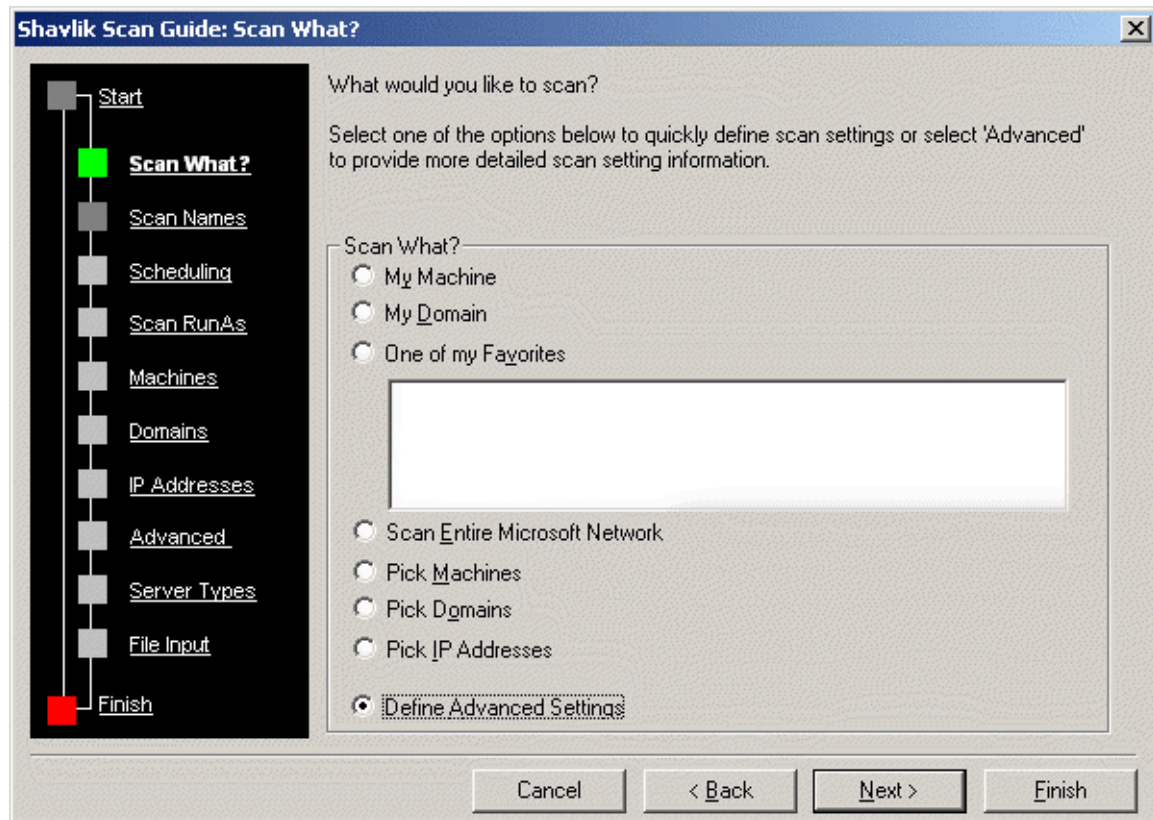
section to explain how to use HFNetChkLT. Once the product has been installed on the system, you can easily select options for scanning systems on your network. Once you open the HFNetChkLT program, you'll be prompted with a wizard asking what to scan. This is referred to as the Shavlik Scan Guide. Fig A shows the beginning of the wizard. From here you would click on the Next button to continue.

FIG. A



The wizard will then ask to define what to scan. The screen shot in Fig. B shows the options available such as my computer, the whole domain, or it gives you the options to select a particular range or single system to scan. For the purpose of this document we will select Define Advanced Settings and then click the Next button.

FIG. B



Next the wizard gives you the option to give your scan settings a name to reference it by in the gui. It can also be set as a favorite so you could load the favorite and scan systems without going through the wizard over again. Once a name has been provided, click the Next button. Refer to Fig. C for details.

FIG. C

Shavlik Scan Guide: Scan Names

The Shavlik Scan Guide allows you to name your scan for easy reference and re-use.

You can supply a user-friendly scan name for easy identification.

Also, if you wish to re-scan the settings you defined during this guide, please provide a 'Favorites' name as well.

Scan Name:

Save in Favorites as:

Favorites Description:

Cancel < Back Next > Finish

The next option is definitely worth investigating. HFNetChkLT will allow you to schedule the scan. You have the option of scheduling it to run once maybe at night to minimize network traffic, or to schedule it to reoccur on a weekly, daily, monthly, or yearly basis. I recommend setting it to weekly to keep an eye on your environment. However for this document we will select the option to run it immediately. Fig. D shows the schedule options.

FIG. D

Shavlik Scan Guide: Scheduling

During this step, you can specify when HFNetChkLT will scan the specified machines. You can also set up the schedule to recur several times so that you do not have to remember to re-scan your critical servers.

Note: If you select a scheduling option other than 'Immediately' you will be required to provide a user name and password.

Scan Time

☒ Immediately

☐ Run once at: 2 /13/2003 12:00:00 AM

☐ Run recurring at: 12:00:00 AM

Recurrence Pattern

☒ Daily

☐ Weekly: Every 1 Day(s)

☐ Monthly

☐ Yearly

☒ Every Weekday

Buttons: Cancel, < Back, Next >, Finish

Part of the security mentioned earlier, HFNetChkLT allows you to specify an administrator account in which to run the scan. Scanning systems with any of the Shavlik tools requires administrative privileges on that system.

FIG. E

Shavlik Scan Guide: Scan RunAs

RunAs is used whenever the user you are logged in as is not an administrator on a target machine. HFNetChkLT uses the RunAs to "login" to the target machine automatically.

Enter: Domain\User - uses the domain account

<Target Machine>\User - uses the target's local account

User - uses the target's local account

☐ RunAs (if you are not an administrator on a target machine)

User name: KTCUS\jmaloney

Password:

Verify Password:

Cancel < Back Next > Finish

For system selection, HFNetChkLT allows three different options for scanning systems. One is to select the computers. This will display each workgroup or domain and allow you to check the systems to be scanned within each. The second option will let you select whole domains to scan. The third option will allow you to select IP addresses to scan. In Fig. F, you can specify a single IP or a range of IP address.

FIG. F

Shavlik Scan Guide: IP Addresses

Please specify which IP Addresses you would like to scan.

You can type the Addresses and hit the 'Right' arrow button to send Addresses to your scan list.

You can specify multiple IP Addresses within this scan.

Single IP Address:

IP Addresses/Ranges To Be Scanned:

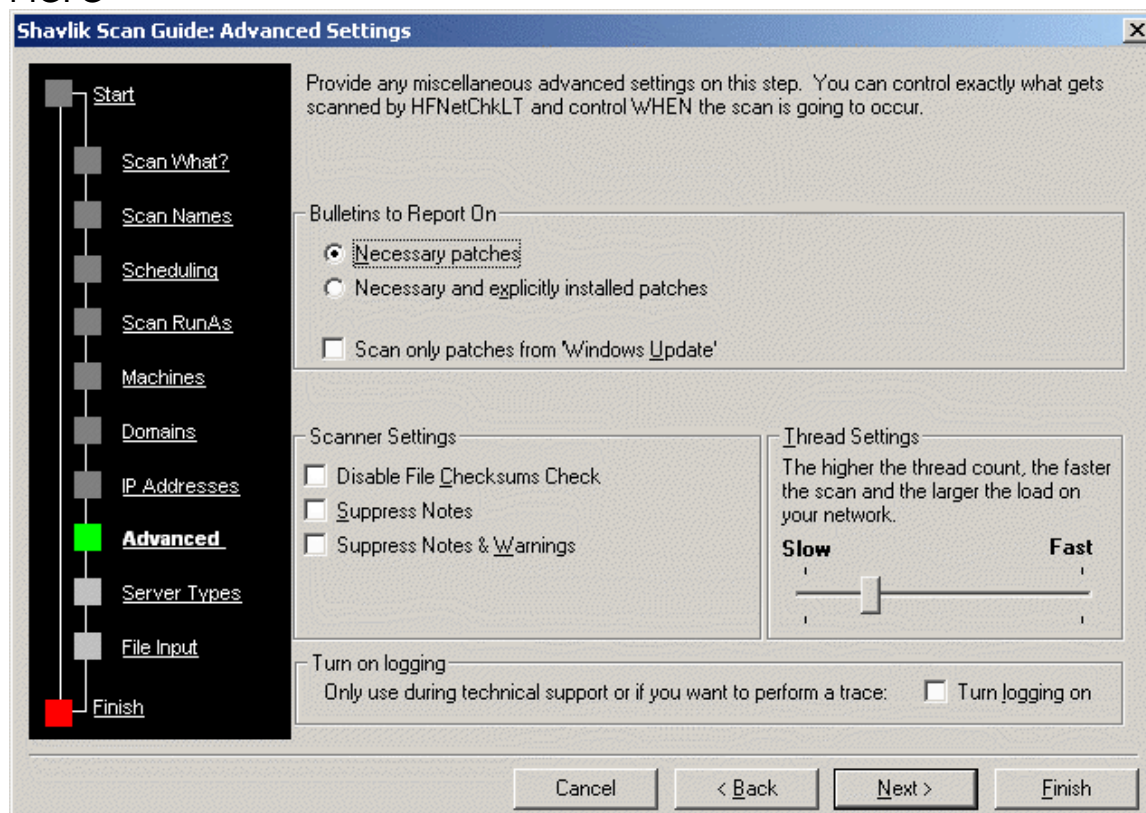
IP Range

Low:

High:

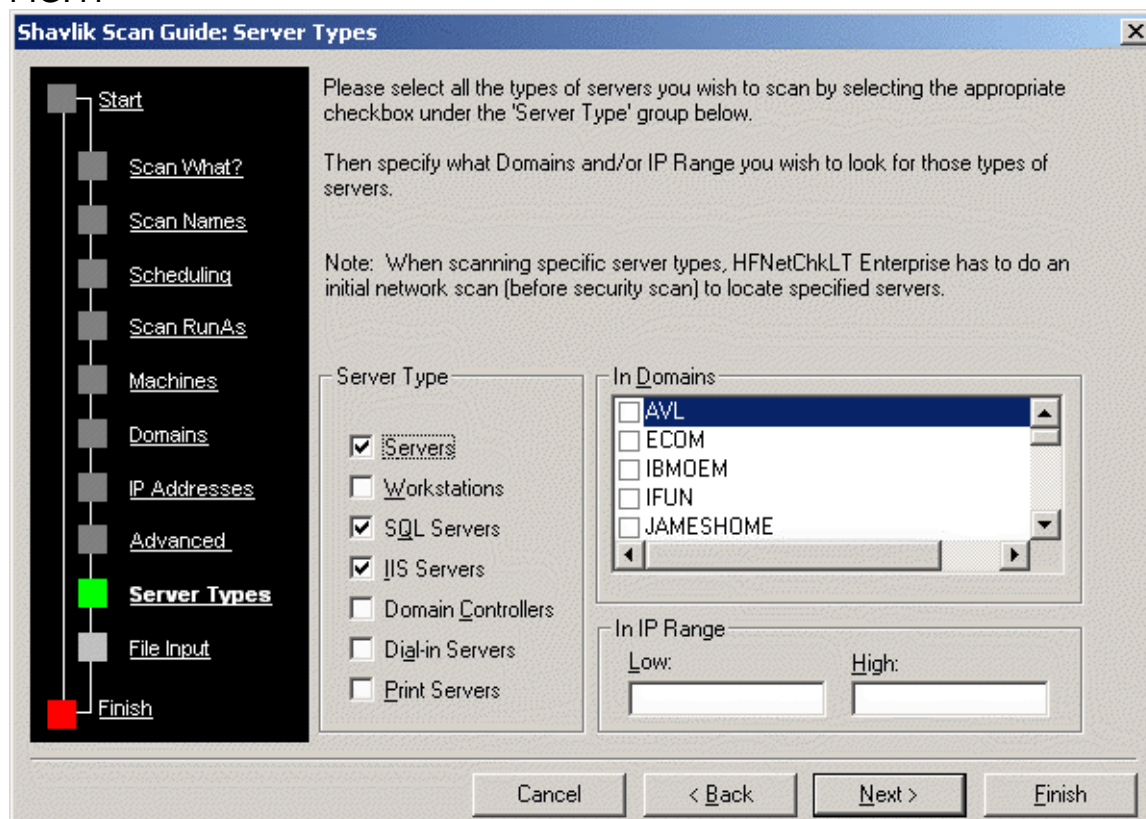
The advanced option shown in Fig. G, show various settings such as suppressing file checksums, amount of bandwidth to use per thread and whether to suppress notes and warnings. There is also an option to turn logging on but it warns that the option should only be used if Technical Support requests it.

FIG. G



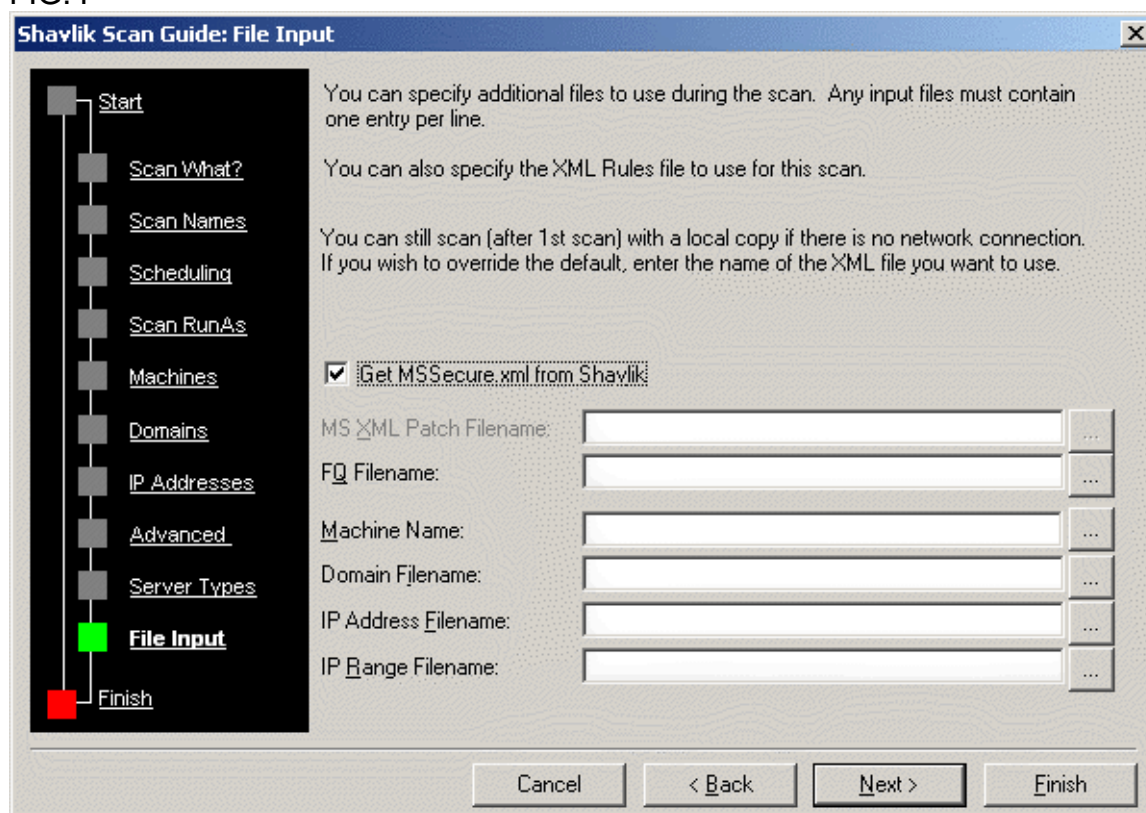
The server type option allows you to specify certain types of systems to scan within a domain or workgroup or within an IP address range. For instance if you wanted to scan all IIS systems within Workgroup, you could check IIS and check Workgroup and it would scan only those systems.

FIG. H



The next option allows you to select where HFNetChkLT should obtain the MSSecure.xml file. This is the file used to identify patches and contains the checksum information for the patches. It is very important to control this so that it does not get replaced with a file that may have locations and checksums for files that may contain malicious code.

FIG. 1

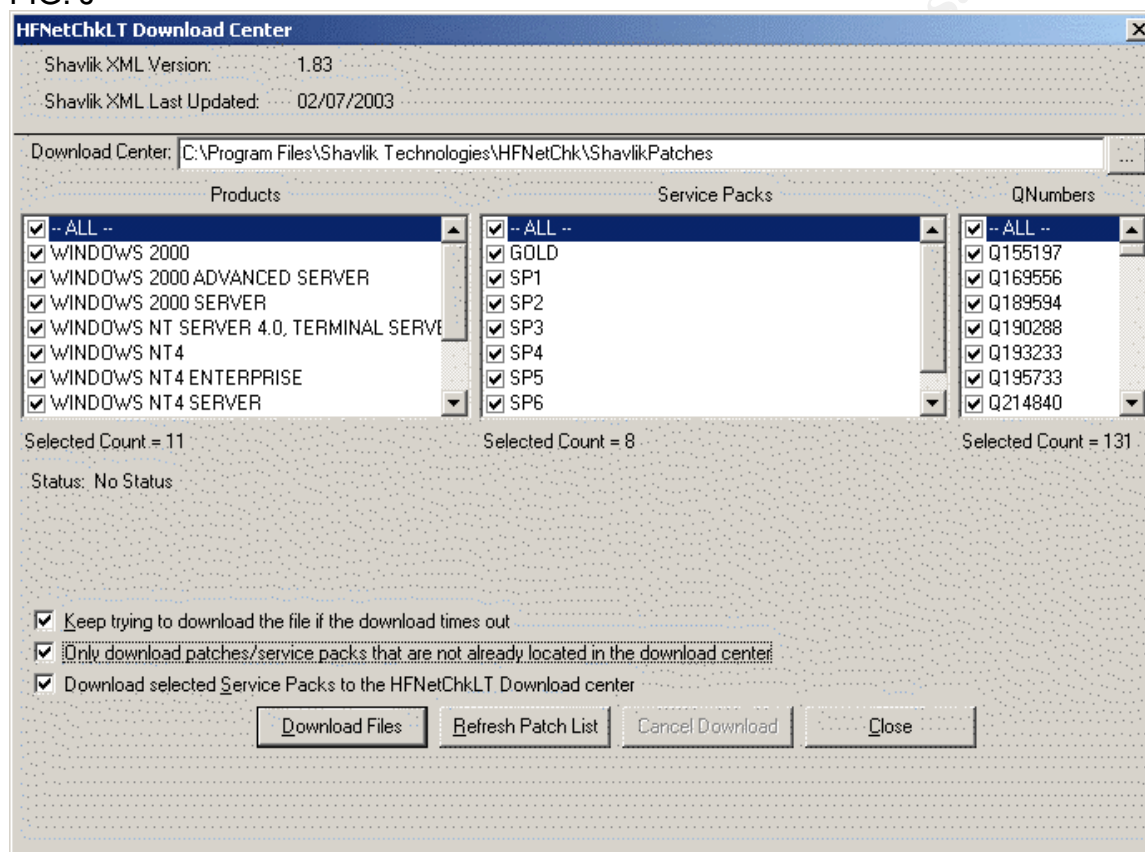


Now the program will scan the systems with the options you specified. Once it completes you will have a drop down list of the patches that are missing. Once again we have identified a way of determining what patches are missing on a system. Now the hard part begins once again of deploying those needed patches to the system.



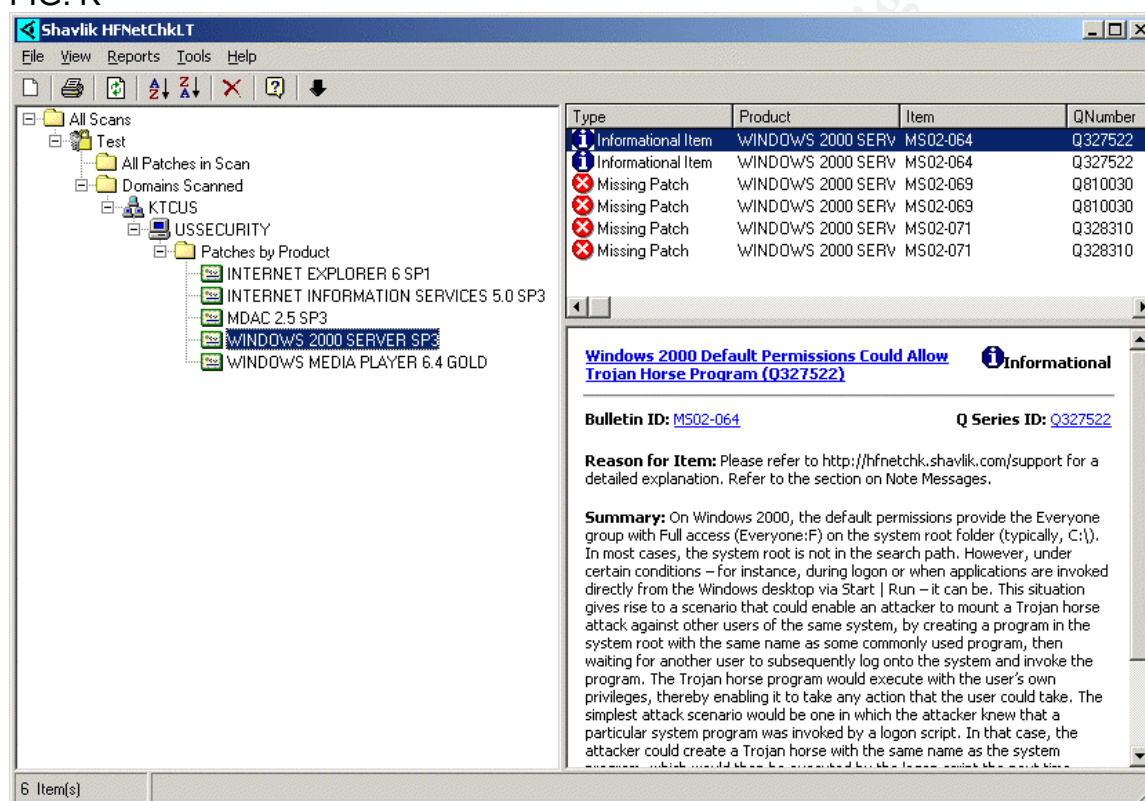
HFNetChkLT has a download center for downloading Microsoft Patches. On the file menu click on Tools and select Download Center. The Download Center will appear. Fig. J shows the interface for the Download Center. To obtain the patches that may be need for a system, select the Service Packs and Hotixes to be downloaded or check the boxes that say All. Then click the download button and the software will download the patches locally to the system, making them available to be pushed out to systems that need them.

FIG. J



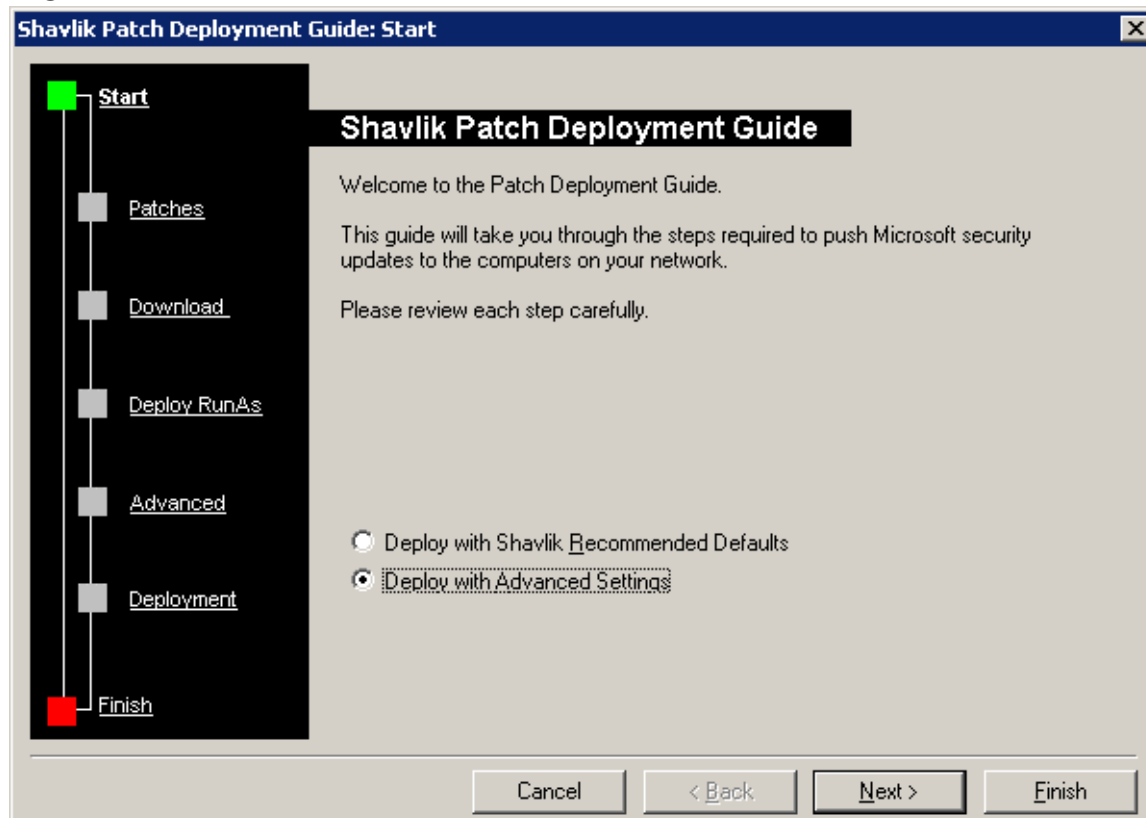
HFNetChkLT has an option for deploying patches. This is done through the deployment wizard. In Fig. K, you can see we have a server called USSECURITY on the left hand side that we have scanned for missing patches. I have chosen to expand the branch that lists the patches by product. Since HFNetChkLT only installs the Windows patches, I selected that on the left so that the missing patches are displayed on the right. Next, while holding down the CTRL-key click on two of the patches on the right so they are highlighted. Right click on them and select Deploy, and then choose Deploy Selected Patches. The deployment wizard will now begin.

FIG. K



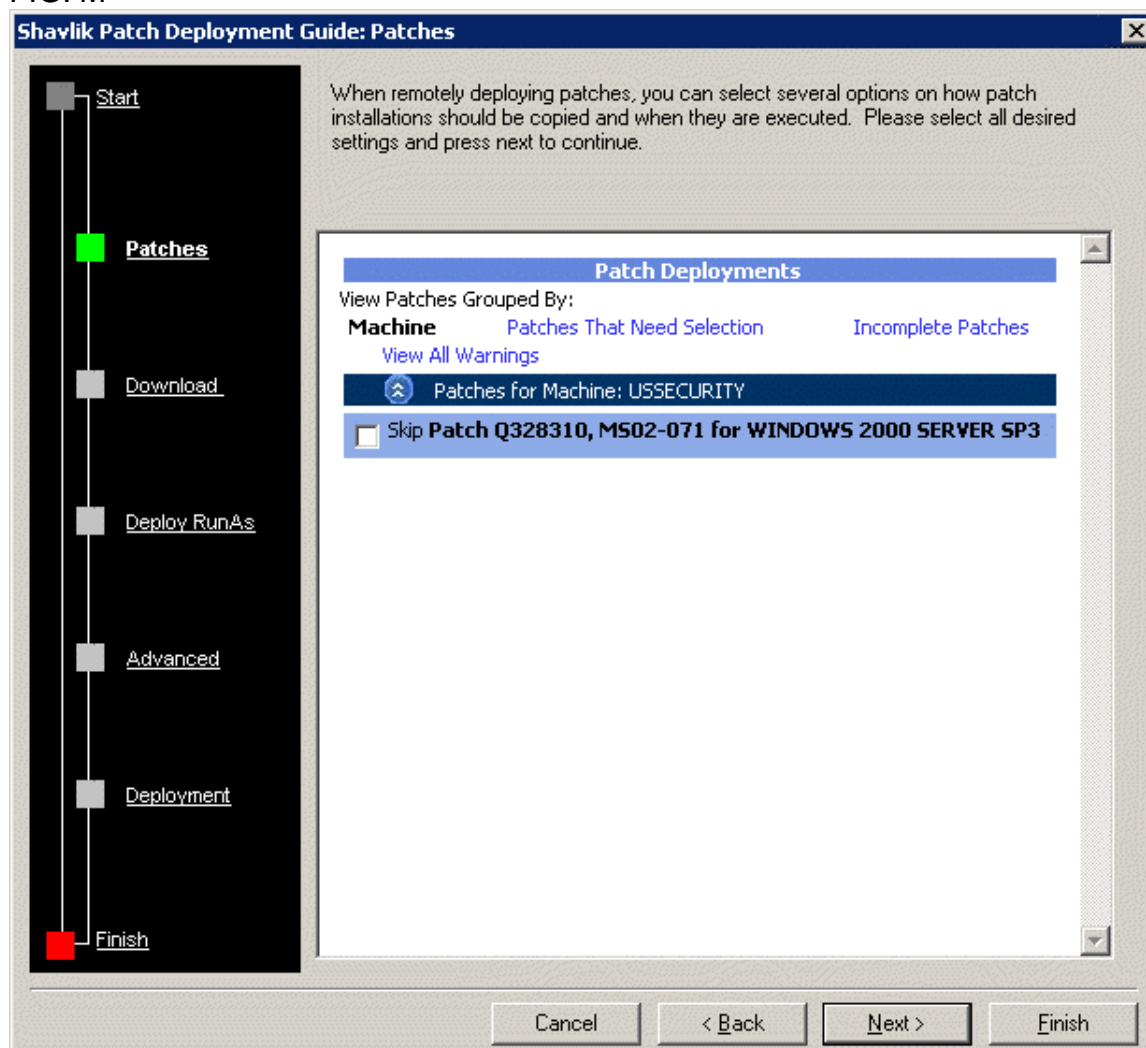
Once the deployment wizard begins, it will want to know if it should use recommended defaults or allow you to specify the settings. I recommend using the advanced settings and specify them yourself.

FIG. L



The next option lets you skip patches if you had the full version and did not want to install certain patches. Since we are limited to two patches with this version, we should have selected only patches we wanted to install. However, if you would like to skip one, just check the box next to the patch.

FIG. M



Now the wizard will give you the opportunity to download the patches to be installed. Click on the Get Patches button. This will check to see if it already exists in the Download Center. If it does not, it will give you the option to download it and add it to the Download Center. Once it has been verified to exist in the Download Center it will let you know as in Fig. O and the you just have to click the Next button.

FIG. N

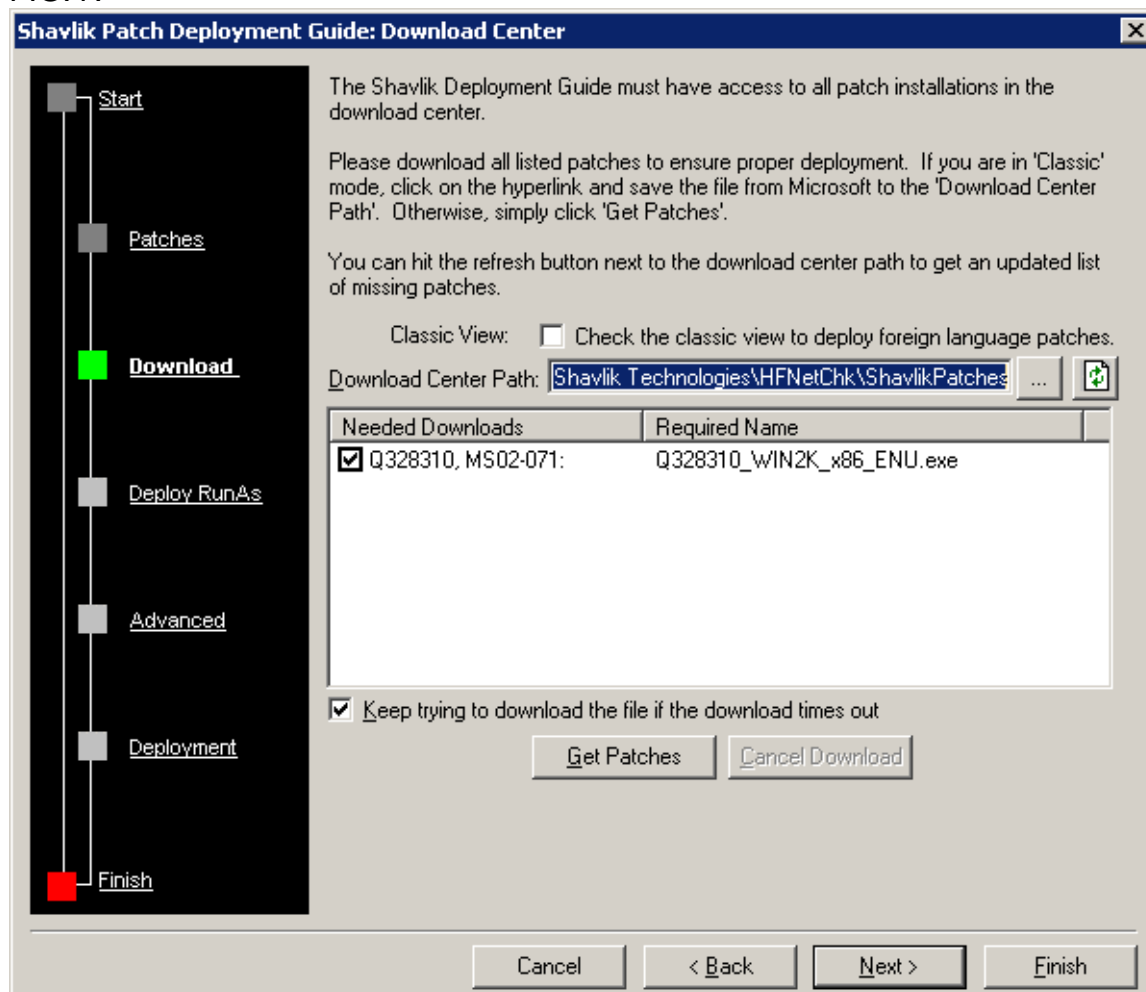
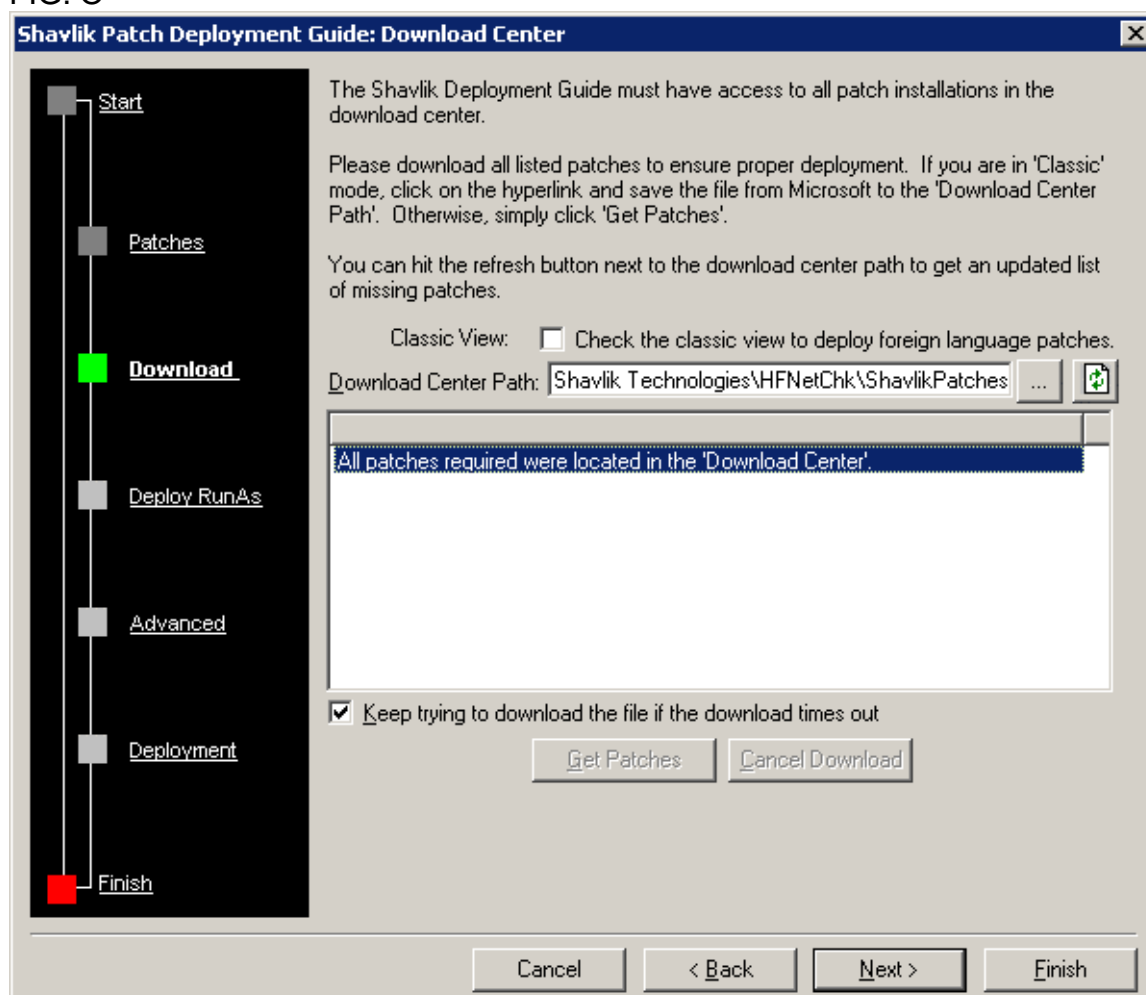


FIG. O



© SANS Institute

Now the wizard will prompt you for an administrator account in which to install the patches. This option is only need if the system in which HFNetChkLT is installed on is not an administrator of the target system.

FIG. P

Shavlik Patch Deployment Guide: Deploy RunAs

RunAs is used whenever the user you are logged in as is not an administrator on a target machine. HFNetChkLT uses the RunAs to "login" to the target machine automatically.

Enter: Domain\User - uses the domain account
<Target Machine>User - uses the target's local account
User - uses the target's local account

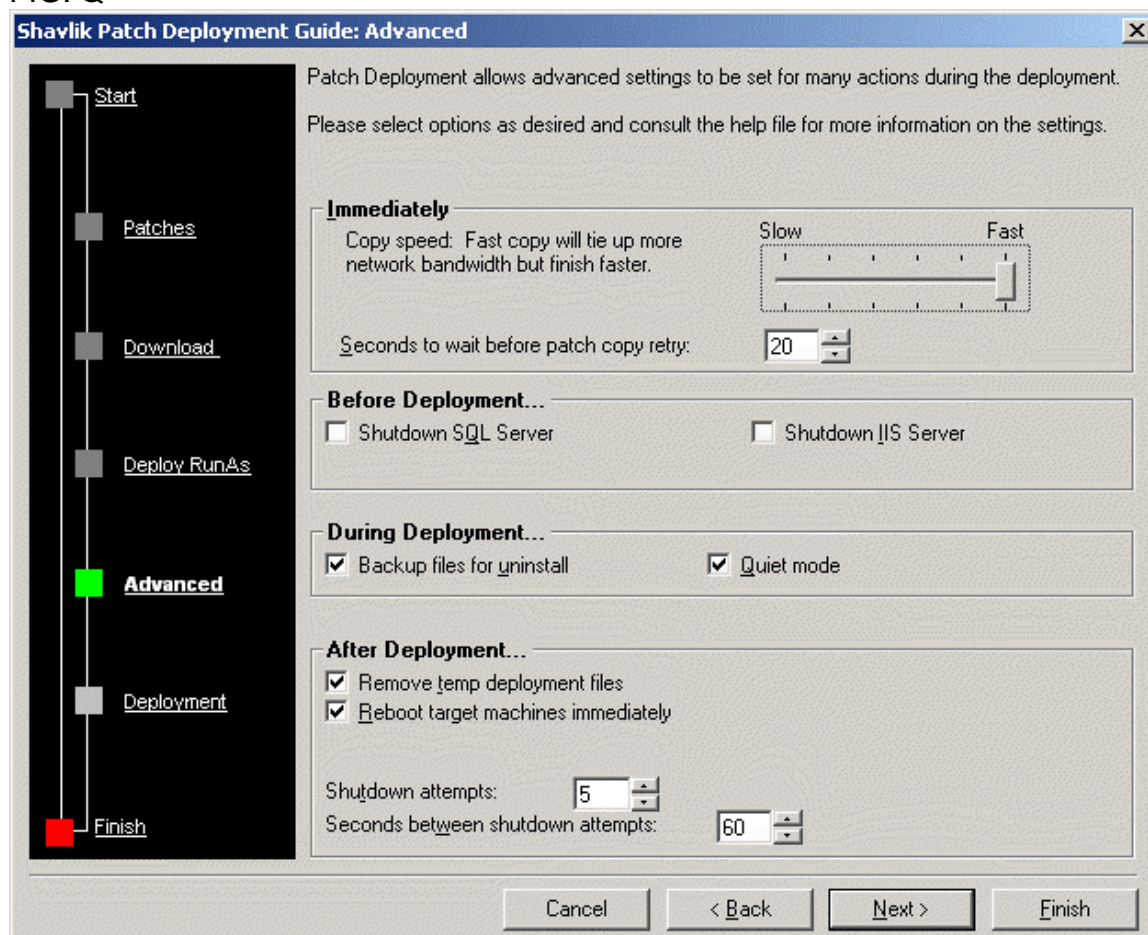
☐ RunAs if you are not an administrator on a target machine

Username:
Password:
Verify Password:

Cancel < Back Next > Finish

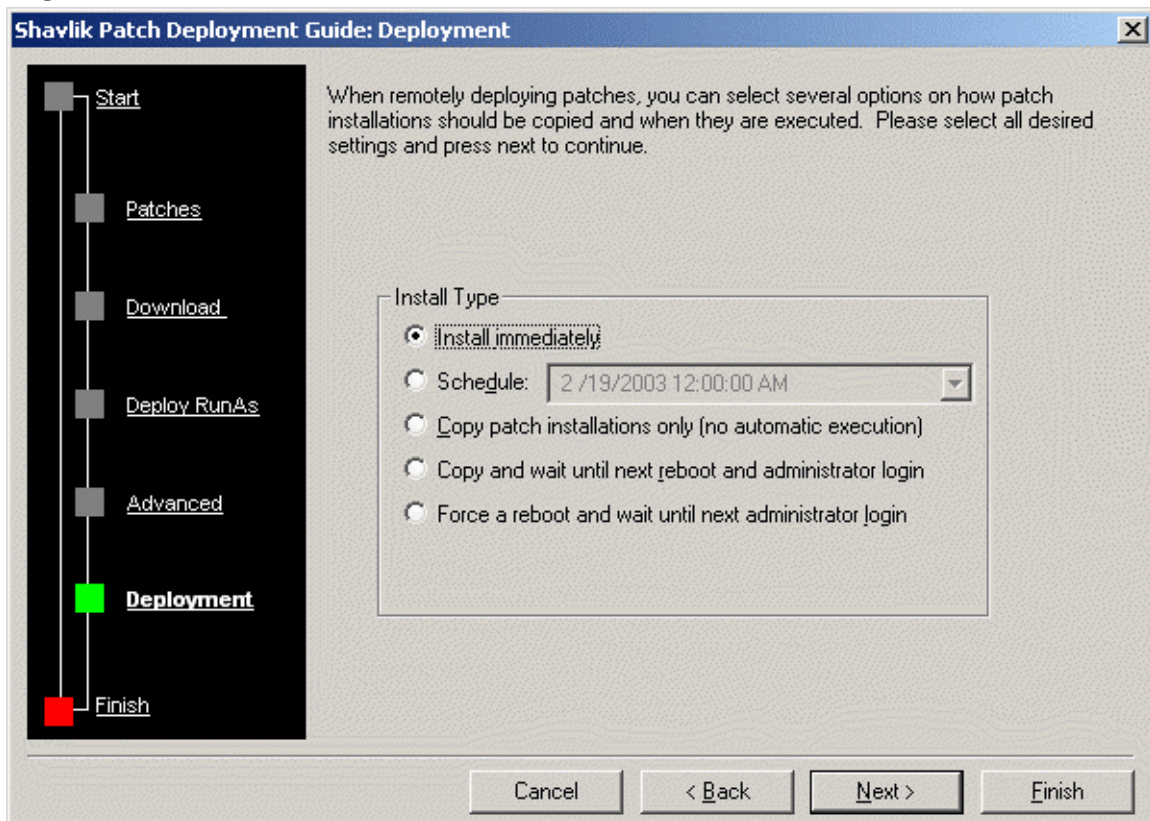
Next it will display the advanced settings. This will allow you to specify such options as bandwidth to use to copy the patches to the target system, shut down services such as SQL or IIS, whether to run in Quiet mode, whether to backup old files for an uninstall of the patches, whether to remove temporary files used by the deployment, and whether to reboot the target system after the install.

FIG. Q



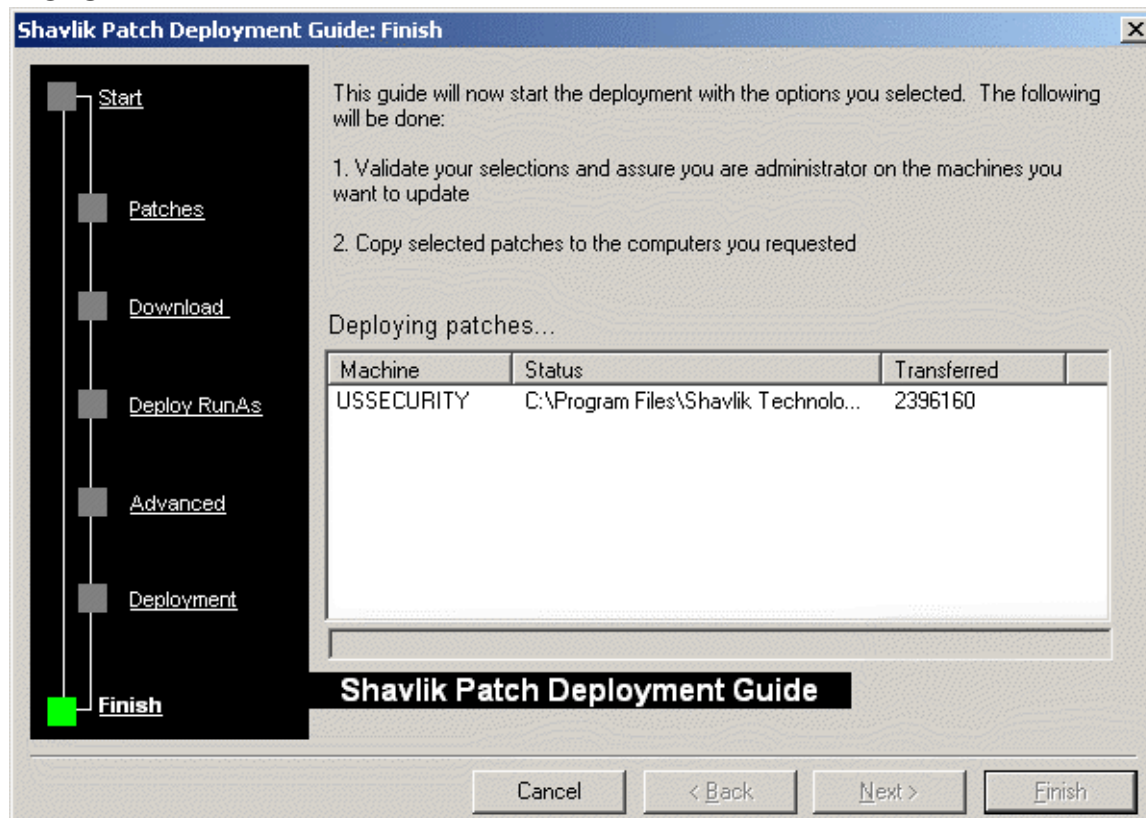
KFNetChkLT gives you the options to install the patches immediately or to schedule the install of the patch.

FIG. R



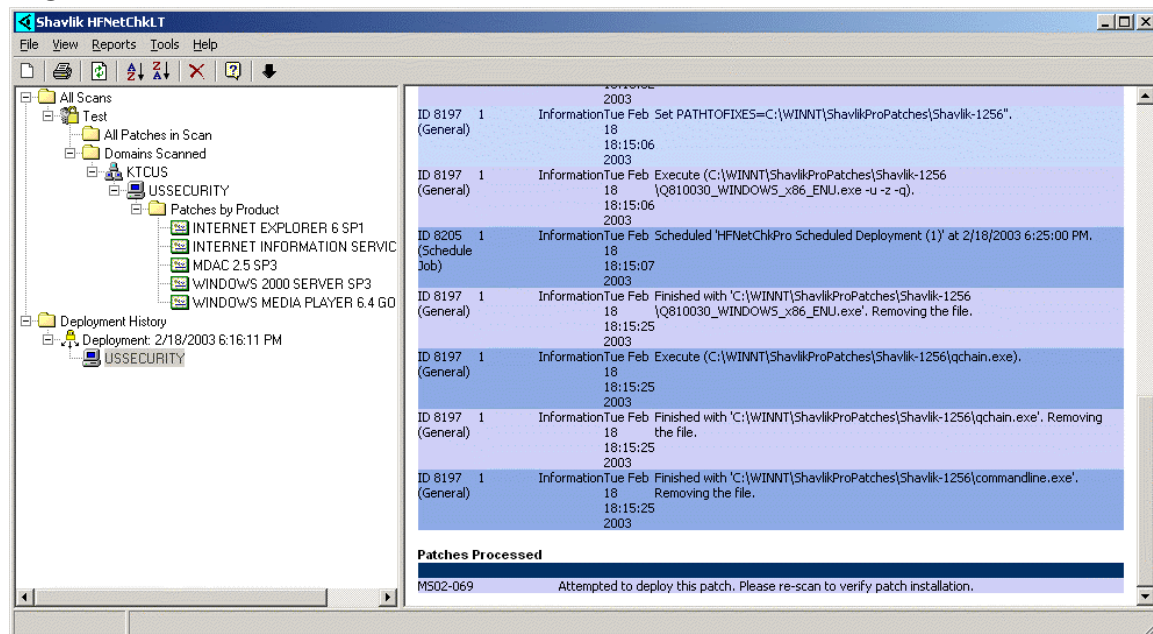
Once this is complete, click on the finish button and the install will begin.

FIG. S



Once the install of the patch is complete, HFNetChkLT gives a complete history of the patch deployment. This will show step by step exactly what the program did. From this you can see that it actually uses the qchain.exe utility to install the patches.

FIG. T



This has demonstrated the use of the HFNetChkLT utility to identify patches needed on a system and how to deploy some of the patches.

Microsoft Baseline Security Analyzer

Some of this information was obtained from Element K Journals, Inside Microsoft Windows 2002 ^[5]. Microsoft Baseline Security Analyzer is a GUI based security assessment tool. The utility will scan Windows NT 4.0, Windows 2000, and Windows XP system and produce a report of potential vulnerabilities. It also scans for IIS, SQL Server 7.0 and SQL Server 2000.

MBSA can only be installed on a Windows 2000 or XP computer preferably with Internet Explorer 5.01 or higher. If the version of Internet Explorer is a version prior to 5.01, an XML parser is needed. MSXML 3.0 SP2 is the latest version as of this document. More information and links to download it are located here at the following location.

<http://msdn.microsoft.com/downloads/default.asp?url=/downloads/sample.asp?url=/MSDN-FILES/027/001/772/msdncompositedoc.xml&frame=true>

Pros

In order to scan a system you need to have either domain administrative or local administrative privileges. This is a plus if you are a security minded individual to know that these tools cannot be used to scan your servers for known vulnerabilities using these particular free tools. Also, the Server service and the Remote Registry service need to be running. It gives detailed reports on missing patches that are XML based. Its main focus is to provide a baseline of security for your servers. So not only does it provide missing patch information is also provides numerous other security settings and warnings as well. Below is a

description of the sections that appear based on the MBSA checks in the order that they appear in the report.

Security Update Scan Results

It will determine missing hot fixes and service packs for:

- Windows NT 4.0 Service Pack 4 or higher
- Windows 2000
- Windows XP
- Internet Explorer 5.01 and higher
- IIS 4.0
- IIS 5.0
- SQL Server 7.0
- SQL Server 2000
- Windows Media Player
- Exchange Server

Windows Scan Results

- It checks Passwords for blank or easily guessable passwords.
- Each drive is checked to see if their file systems are NTFS.
- It checks the Guest account to make sure it is disabled. Windows XP systems that have simple file sharing enabled are not checked because all remote users authenticate as Guest.
- It checks to see if RestrictAnonymous is set to one in the registry setting HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA.
- If there are more than two members in the local Administrator group, it will alert you to the fact and it will list all of the usernames that are contained in the group.
- It checks to see if the autologon feature has been enabled. This option is skipped on XP systems not part of a domain.
- It also verifies if the password have an expiration policy set. This option is skipped on XP systems not part of a domain.

Additional System Information

- MBSA checks to see if auditing is turned on for various security events. This option is skipped on XP systems not part of a domain.
- It lists unnecessary services that are running. This feature is well suited for administrators because it adds configurability to the software. Besides the default services that are verified to be running, the administrator can add services to a text file located in the MBSA program folder to add more security to the system.
- It identifies the shares that exist on the system and the NTFS and share level permissions of the folder.
- The Windows version is determined as well.

Internet Information Services (IIS) Scan Results

- It checks to see if parent paths are enabled in IIS on all websites configured in IIS.
- MBSA verifies that the IIS lockdown tool was installed.
- Also it checks to see if the IIS sample applications have been installed.
- It looks for the IIS Admin virtual directory and makes sure that the IISADMPWD virtual directory does not exist.
- Furthermore it makes sure the MDAC and Scripts virtual directories do not exist.

Additional System Information

- MBSA checks to see if IIS logging is enabled and if the correct options are selected for logging.

SQL Server Scan Results

- If SQL Server 7.0 or SQL 2000 is installed, MBSA will check to see which accounts have administrative privileges.
- It checks to see if the sa password is stored in plain text.
- The Guest account is then checked to see if it has access to SQL.
- It reports if an accounts have simple or blank passwords.
- It also checks to see if SQL is installed on a domain controller.

Desktop Application Scan Results

- MBSA checks the Internet Explorer security settings for each user profile on a system for secure settings.
- It then checks Outlook's security zone settings.
- Finally it displays any warnings about Macro security settings for Office 2000 and Office XP.

Cons

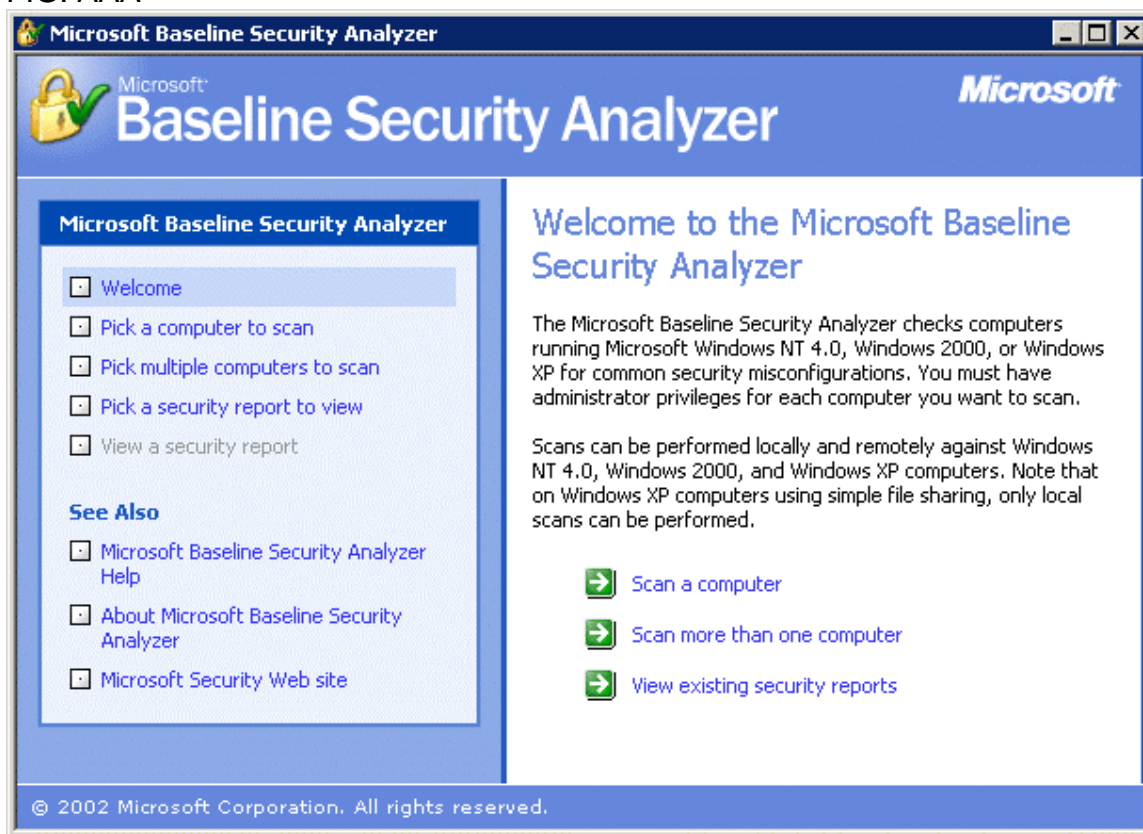
Reports can only be viewed from the system in which Microsoft Security Baseline Analyzer is installed. It also has no means in which to deploy the patches to the system.

Possible Uses

The main use for this product is to identify the systems that are missing patches. The reports can be printed and used as a reference on the system that needs the patches.

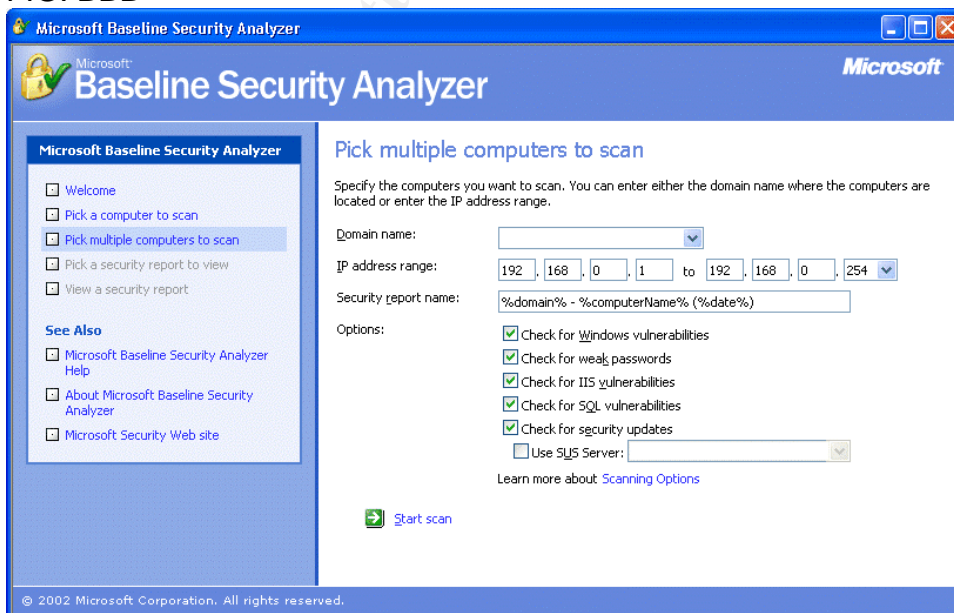
Once you have MBSA installed you can run the program either from the desktop icon (if you chose to install the desktop icon from the custom install) or by clicking on Start, Programs, and selecting Microsoft Baseline Security Analyzer. Once it loads it will ask if you would like to scan a single host or a range of computers. This feature makes it very convenient for administrators to view many systems at once to determine the state of the network's security. The main page also allows you to view previous reports that may have been produced. Fig. AAA shows the main screen.

FIG. AAA



In this example I chose to scan multiple computers. You can either enter the domain name to be scanned or the IP address range of the systems to be scanned. Fig. BBB shows the multiple computer scan option.

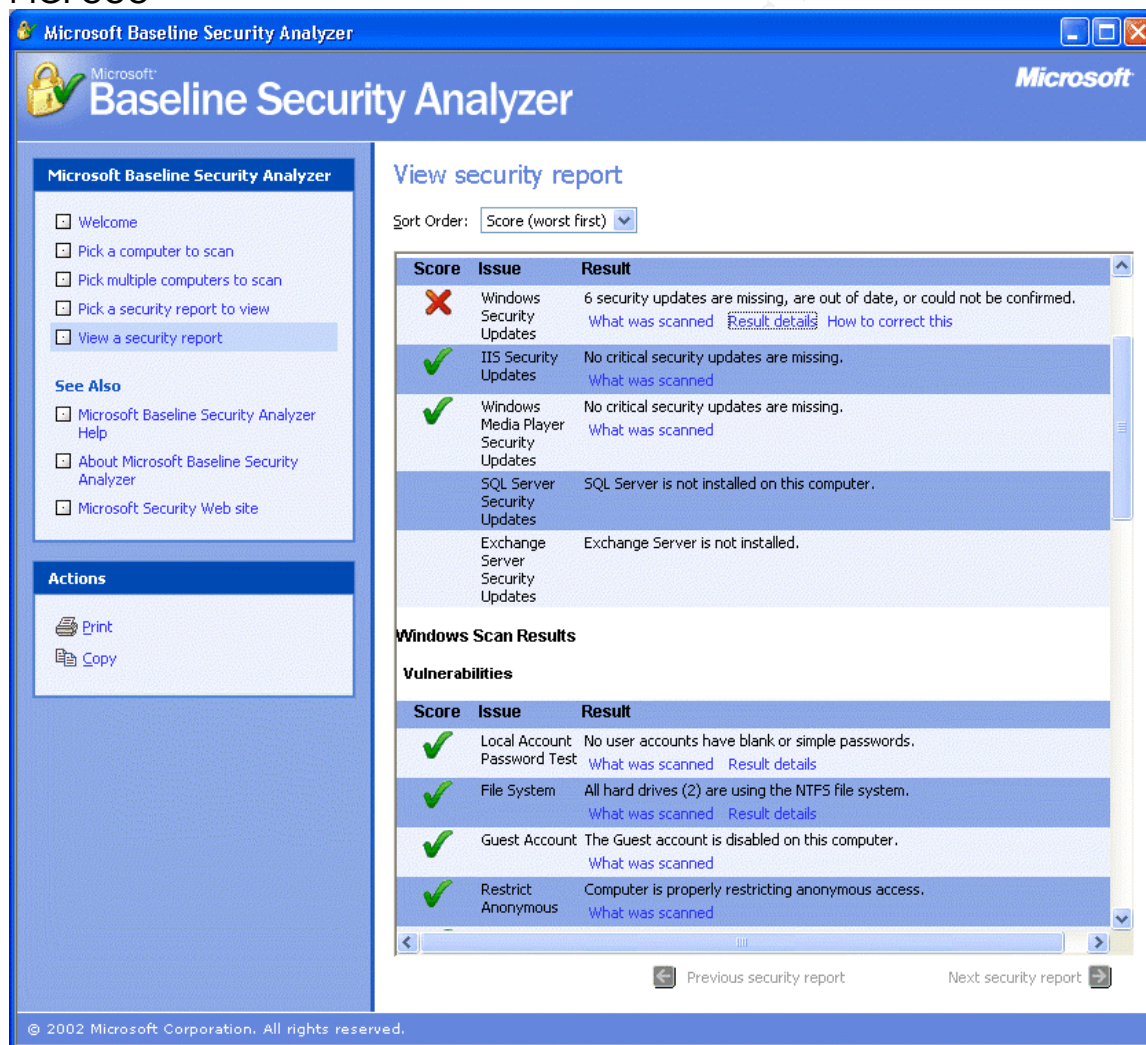
FIG. BBB



Once it finishes a scan you are presented with the report. The report is divided into different sections. Some sections are displayed only if the product exists. A green check is placed next to items that have passed the test, red X's appear for items that are missing or pose a high security risk, yellow checks are for settings that are medium risk, and blue asterisks indicate notes or information.

The area of the report that we will focus on is the first section labeled Security Update Scan Results. This is the section that explains what patches need to be installed on this particular system. In Fig. CCC there is a red X next to Windows Security Updates. This indicates that there are missing Windows patches. The green check marks next to IIS Security Updates and Windows Media Player Updates indicate that all current patches for these products have been installed. Nothing next to SQL Server Updates and Exchange Server Updates indicate that those products are not installed on the system that was scanned.

FIG. CCC

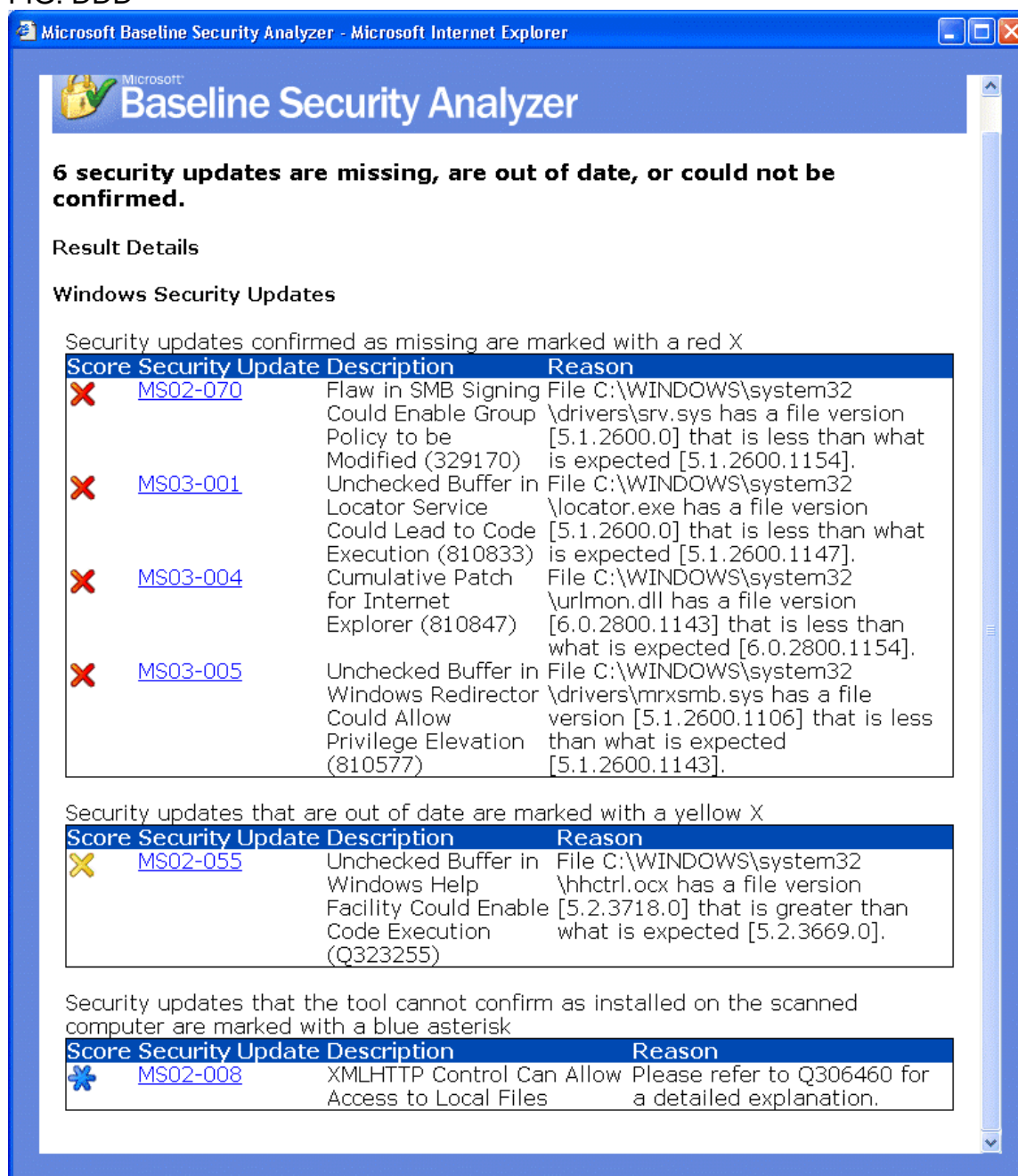


In Fig. CCC under the results column there are three links labeled What was scanned, Result details, and How to correct this. Click on the link labeled Result details. The page that is displayed shows what updates are missing for this computer system. They are listed by priority from highest to lowest. Red X's mean the patch is missing. Yellow X's indicate out of date patches (patch may have been updated by Microsoft meaning it was pulled and then reposted. This is sometimes referred to as a silent update by Microsoft). Blue asterisks mark things that cannot be determined to be either set correctly or if the patch is installed. Since MBSA uses hfnetchk technology, some issues are notes for settings to be implemented or updates that need to be installed and are not considered a hot fix or security update. Fig. DDD shows that for the missing patches, there is a link for the Message article on Microsoft's site that describes the patch and the message article will provide the download link for the update. From this report you now have a list of patches that are needed for this computer system.

This product's other features are really what makes the tool useful to security professionals. This simply provides a way to determine missing patches on systems and provide you with reports. It can also be used to double check other patch management software to ensure it is properly installing patches and keeping the systems up to date.

© SANS Institute 2003, Author retains full rights.

FIG. DDD



Microsoft Software Update Services

Another method for deploying patches is Microsoft's Software Update Services

(<http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp>) [12].

This will be referred to SUS from time to time through out this document. Some information about SUS functionality was obtained from the SUS deployment guide which can be found at the following location

http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc [11].

SUS is Microsoft's first initiative in helping the administrator install patches where SMS is too costly to deploy. This tool utilizes their Automatic Windows Update technology that Microsoft first introduced in Windows XP. It is made up of two pieces, the SUS server and the Automatic Updates client. The server software is installed on Windows 2000 server or higher running IIS 5.0 or higher. The client can be installed on any Windows 2000 or XP system. The client is included with Windows 2000 SP3, Windows XP SP1 and Windows 2003.

Pros

Microsoft has implemented some security features into the product. The SUS server can download updates either from Microsoft's website or from another SUS server. All downloads are checked to see if they are properly signed by Microsoft. The Automatic Updates Client can download patches either from Microsoft's site or from the SUS server. Before the patch is installed by the client, the SUS server verifies that the patch is signed by Microsoft. Then the Automatic Updates client checks the CRC of the patch to ensure no tampering of the file took place. These features were not present in earlier versions and have been added in response to the security of this process. It also allows you to approve what patches your clients will be able to download and install from the SUS server. This will allow you to test patches before they are approved to be installed on the clients. Also, during the installation of the SUS server, it installs the IIS Lockdown tool to better protect the IIS server from vulnerabilities. The benefit to the SUS architecture is that it is easy to deploy and it uses Microsoft's Background Intelligent Transfer Service (BITS) to control the amount of bandwidth it uses to download patches.

Cons

Based on the description there are a few limitations to SUS. The biggest is that it only supports Windows 2000 or higher. Another limitation is that it only updates hot fixes and critical updates. It does not update Service Packs. OK, this is not a perfect world, but this can save you a lot of time with those intermediate updates for your Windows 2000 and higher systems.

Possible Uses

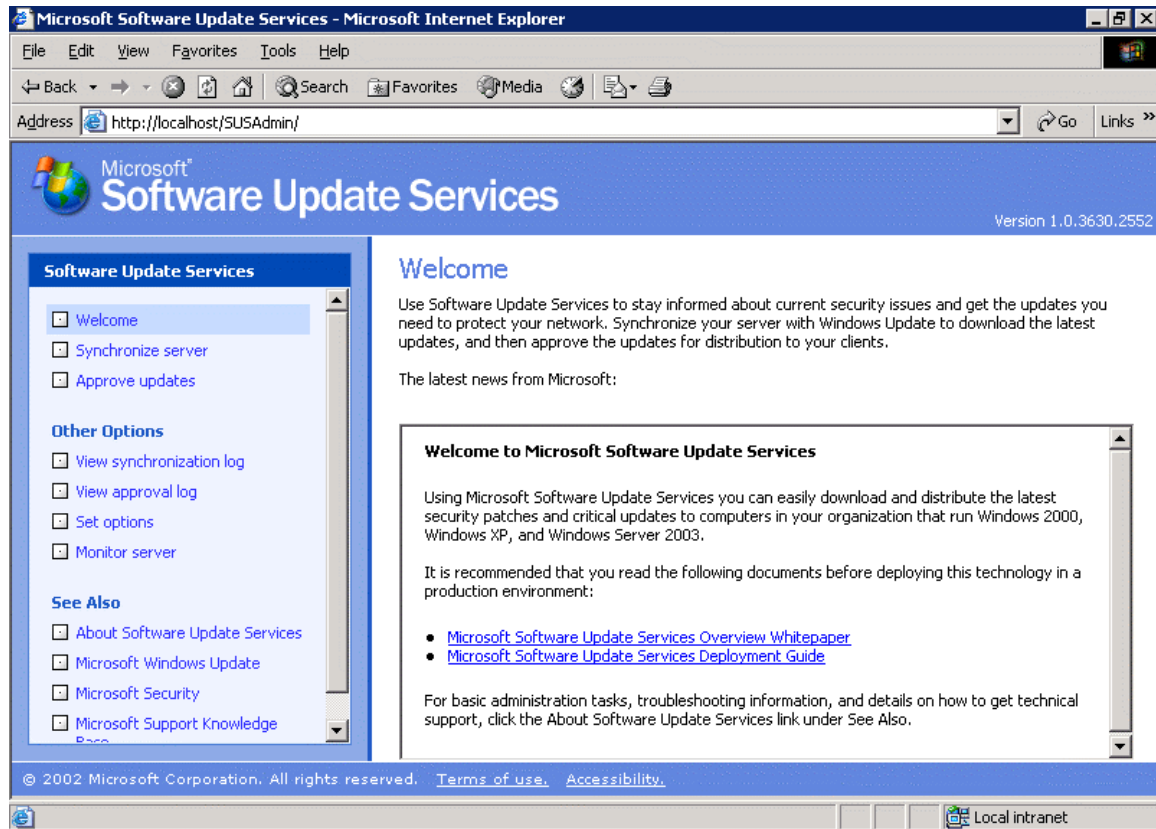
The SUS process consists of two components; the server and the client. The server is recommended to be installed on a dedicated IIS box. Once the SUS server has been installed there are only a few settings that need to be saved.

After installation of the server, you can access the administration page for the SUS server by going to <http://<yourservename>/SUSAdmin>.

© SANS Institute 2003, Author retains full rights.

When you first navigate to the admin page you are presented with the Welcome screen. This provides the navigation bar on the left hand side to configure more options on the SUS server and also has links to the SUS overview white paper and the SUS deployment guide white paper on Microsoft's site. The welcome screen can be viewed in Fig. AA.

FIG. AA



Now on the left hand side on the navigation bar, click on the option that says Synchronize server. Under here you can manual synchronize the updates from Microsoft's site, or you can schedule the updates to reoccur daily or weekly. There are two buttons, one that says synchronize now and one that says synchronization schedule. If you click synchronize now, the SUS server will immediately begin to synchronize with Microsoft's site. You can specify another SUS server to synchronize with but we will get to that setting later. If you click on synchronization schedule, you will get the options screen for automatic synchronizations. Fig. BB shows the options screen. Once you have selected your particular settings, click the OK button to save them.

FIG. BB

Schedule Synchronization -- Web Page Dialog

☐ Do not synchronize on a schedule

☒ Synchronize using this schedule:

At this time: 03:00

On the following day(s):

☒ Daily

☐ Weekly

☒ Sunday ☐ Monday ☐ Tuesday

☐ Wednesday ☐ Thursday ☐ Friday

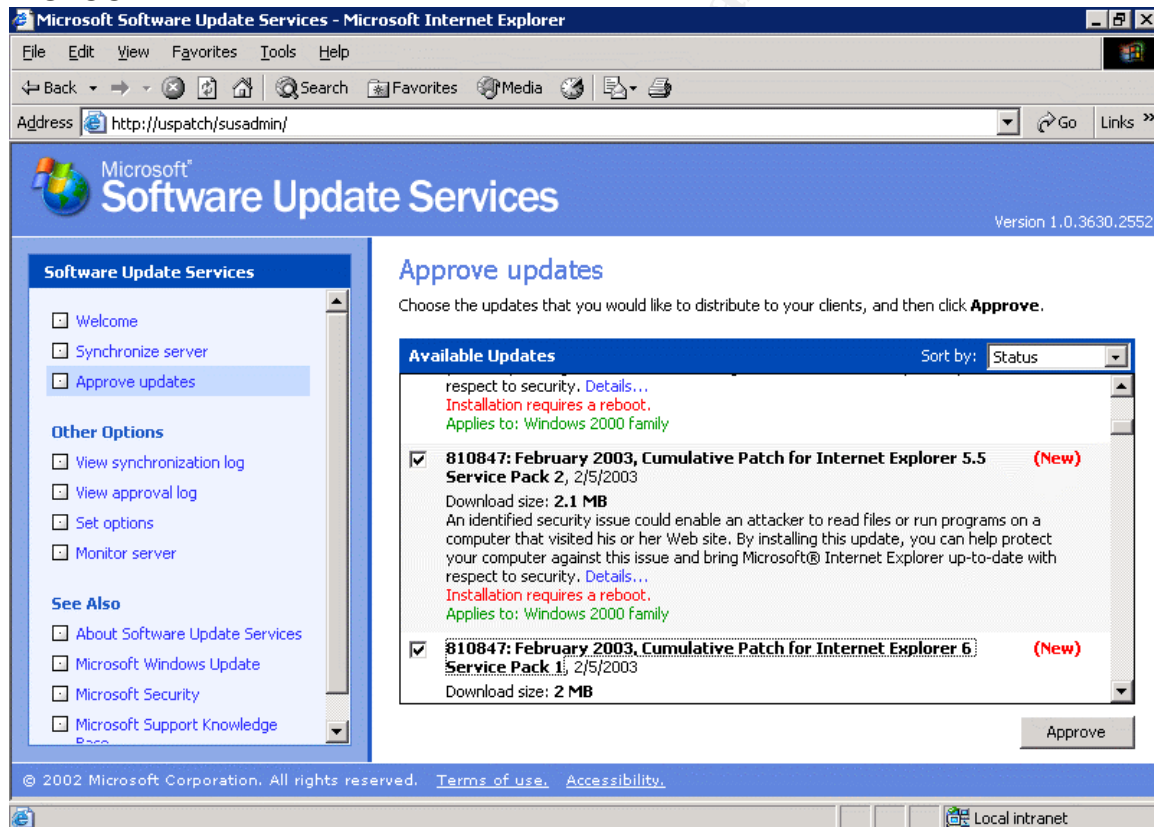
☐ Saturday

Number of synchronization retries to attempt on a scheduled synchronized failure: 3

OK Cancel

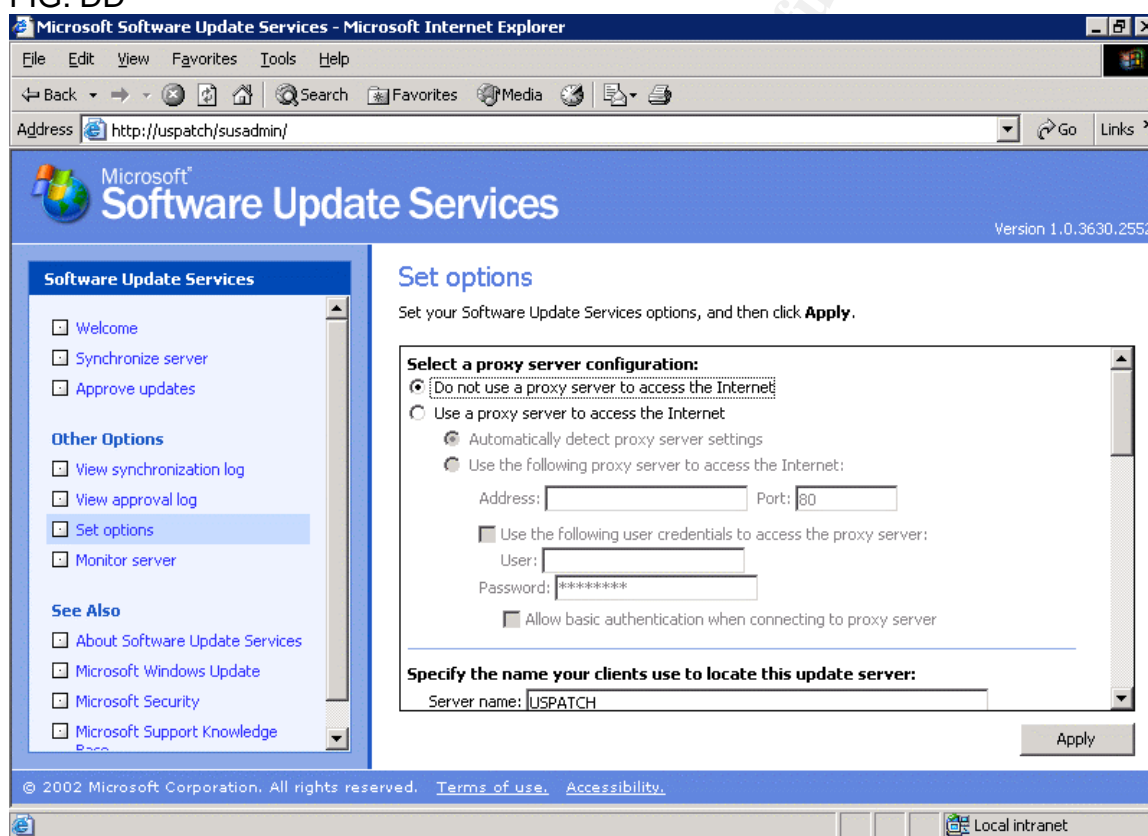
Next on the navigation bar is the option to approve updates. This is a very important feature in the SUS architecture. Clients cannot download updates from the SUS server unless the updates are approved. This option allows you to test updates before you approve them for your clients to download and install. There are a number of reasons why testing should be done. Some updates may cause issues with other applications your company may run. Also, Microsoft from time to time has released updates that have caused issues within Windows, pulled the updates and replaced them with fixed versions of the updates. These kind of update issues from Microsoft are sometimes referred to as silent updates by Microsoft. Once you navigate to the approve updates screen, SUS server will sort the updates listing the new updates that need approval first. By checking or un-checking the box next to an update, you can click the approve button and approve or disapprove updates. If the box is checked, the update will be approved. If it is unchecked, the update will no longer be available for download. FIG. CC shows the approval screen.

FIG. CC



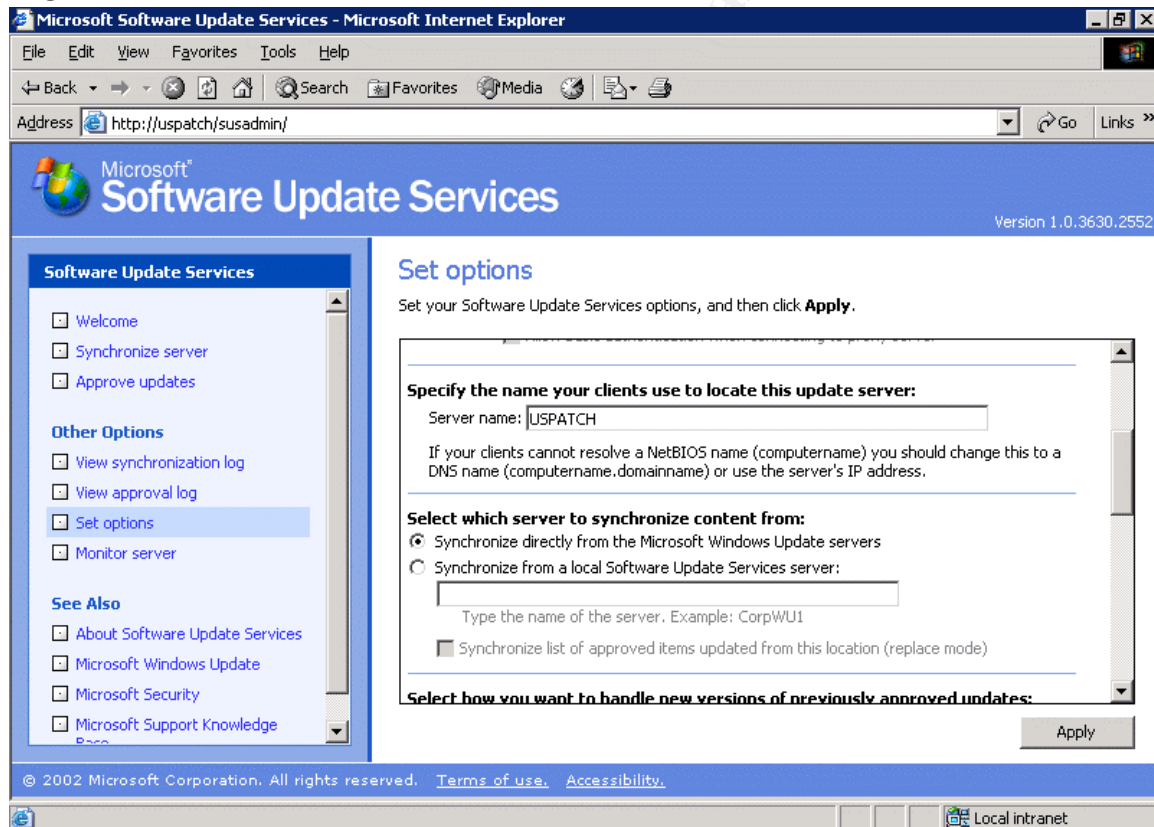
The next important setting on the navigation bar on the left is the Set Options setting. This has various settings for the SUS server. The first part allows you to specify a proxy server to use to download updates from the internet. If your network uses a proxy server for internet access, this setting allows you to configure the SUS server to use that connection. I recommend this especially if your proxy server scans downloaded files for viruses. This can help prevent redirection of the Microsoft site and having a patch replaced by malicious code. Even though SUS uses CRC's and the checksums when downloading the file, company's have been know to release patches with viruses accidentally. Microsoft has taken many measures on their servers to prevent this but I fell more comfortable scanning them myself as well. Fig. DD shows the settings for this.

FIG. DD



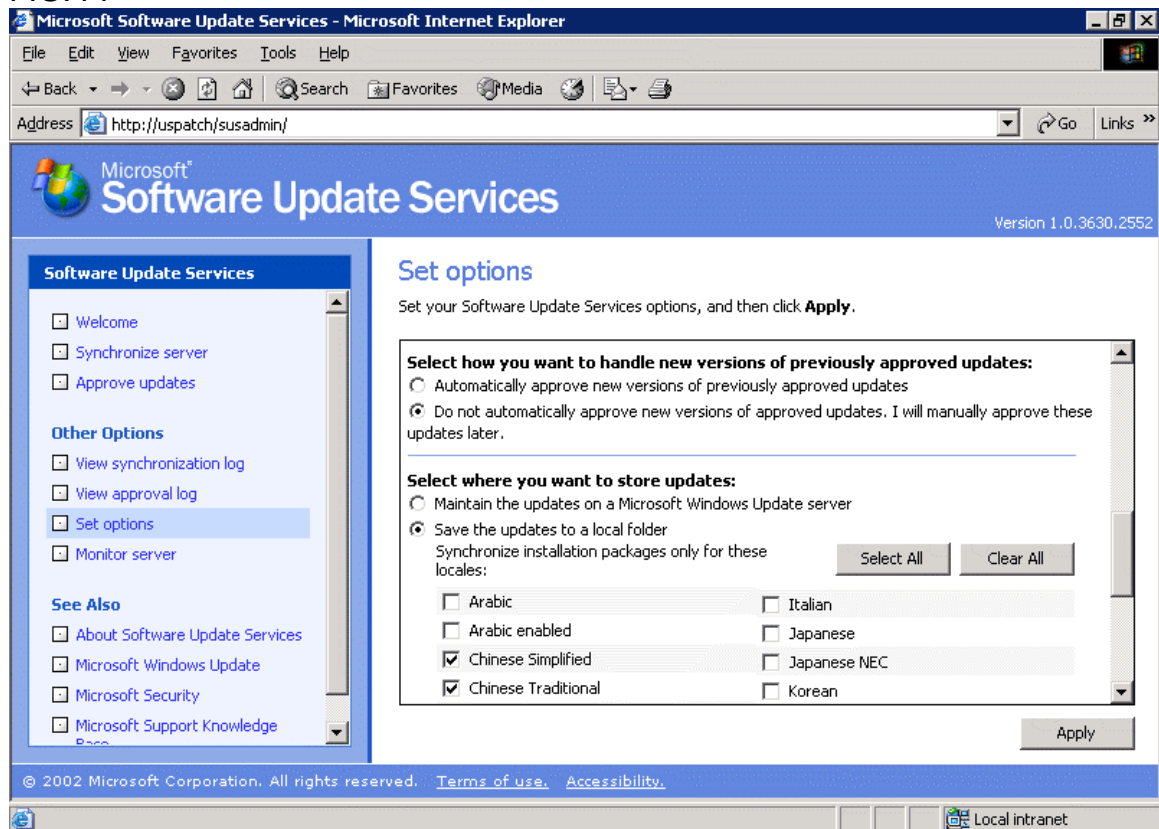
The next option provided in the set options section is to specify the name of your server in which the client will access the server. In this example, the clients will access the server name uspatch via <http://uspatch>. So this in this setting I placed the name of the server uspatch. The option after that allows you to control where the SUS server downloads the patches from. It can download them either directly from Microsoft's site or from another SUS server. It also has an option to synchronize the list of approved items from the other SUS server. Let's say this is a remote SUS server or a secondary SUS server. You may need a second SUS server depending on the number of clients in your network. You should review the deployment guide to determine how many SUS servers you may need. You can have one central SUS server that downloads from Microsoft's site, and then the secondary ones download from that server. You can then approve updates on the primary or central SUS server and have the secondary servers synchronize their approval list with that server. This way you do not have to approve updates on each server. Fig. EE shows these settings.

FIG. EE



The next options allow you to either automatically approve updates once they are downloaded or tell the server not to automatically approve them. The recommended setting is to manually approve the updates. We have discussed the numerous reasons for testing patches before they are approved. The SUS server then gives you the options of what languages to download for updates. Fig. FF shows these settings.

FIG. FF



The other links on the left navigation bar are for the synchronization log, the approval log, and the monitor server option. The synchronization log shows when the updates were last synchronized and whether they were done manually or scheduled. The log will give a detail of what was downloaded and any errors encountered. The approval log will display a list of dates and what was approved and who approved the updates. This is a good feature for identifying admins that may be approving updates before they are tested. It also should be viewed to make sure someone is not approving updates when they are not authorized to do so. The monitor server will list the categories of updates for Windows 2000, Windows XP and the Internet Explorer updates. This will show you how many updates have been downloaded for each. It also will display each of the patches in detail under each category. Samples of all the logs can be seen in the Deployment Guide.

Now the SUS server has been configured and our updates approved. It is now time to configure the clients. The first issue is to deploy the clients. This can be done by install Windows 2000 SP3 or Windows XP SP1. The automatic update clients are installed by default with those service packs. The client also be downloaded from Microsoft's website <http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp> . Either way, you will have to decide based on your company's policy, how to deploy the automatic update client. Once the client is installed, the settings to download from the SUS server and the frequency in which to download update needs to be configured on each system. This can be done through Group Policies either locally or in AD. They also can be done through registry entries. The Deployment Guide gives many examples of scenarios for configuring the clients. I have chosen one that should suite everyone needs for end users. Appendix E give the reg file for setting the client. The reg file can be rolled out into a login script to modify the end users systems. This setting may be ideal for servers as well. Basically these settings do the following:

- Schedule the automatic update service on the client to install and reboot the system at 3 a.m. every day (if there is an approved update available).
- The RescheduleWaitTime option basically says that if the system is shut down at 3 a.m., then the install will be rescheduled. You can set this value from 1 to 60 minutes. Basically it means that after the system is started up, as soon as the automatic update service starts, it will wait that amount of time in minutes configured in the RescheduleWaitTime option. In this case it is set to one minute. So when the system boots up, it will schedule the install one minute after the automatic update service starts.
- The NoAutoRebootWithLoggedOnUsers option tells the automatic update service to not reboot the system if a user is logged on to the system. If the system is locked or a user is logged in and working at 3 a.m. the automatic update service will download and install the updates, however it will not reboot. It will prompt the user that new updates have been installed and that a reboot is required. If the user is an administrator of the system, there will be a yes button to reboot and a no button to cancel the

reboot. If the user is not an administrator, the dialog box will have the yes button however the no button will be grayed out and cannot be selected. This gives the user time to save and close any applications that may be opened. If the system were locked, the same things apply however the dialog box will sit there and wait for the logged on user to unlock the system and make a decision on whether to reboot.

- The combination of the NoAutoRebootWithLoggedOnUsers and the RescheduleWaitTime will have another affect as well. If a system misses the 3 a.m. install time because it was shut down, the automatic update service will schedule the install one minute after the automatic update service starts during the reboot. If the user does not log on after the system boots and the one minute reschedule time goes by, automatic update service will install the updates and reboot the machine. If the user logs in the system before the one minute reschedule time has passed, the prompt to reboot with the yes button will appear.

These settings should prevent any loss of data due to a logged on user while still providing a message that updates have been installed and the system needs to be rebooted. This setting is ideal for servers as well. If you have servers that are data servers, many times these servers do not have anyone logged into the system. This will allow the system to reboot at 3 a.m. which may be off-hours for most companies. Once the system reboots, the shares and data are available to the users. This can also be ideal for a web server as well. In the case where an application may be running that requires a logged in user, the system will display the dialog box and wait for an administrator to reboot the server. This way they can log the server in and start the application that needs to be running. It will also prevent the automatic update service from rebooting while a application is running and possibly losing data. You can change the NoAutoRebootWithLoggedOnUsers setting for Data Server or Web server in which no users or application runs so that it reboots no matter what. In this case, if a user is logged in a dialog box will appear and a timer will countdown to the reboot.

You can alter the reg file settings in any way to produce the desired results for your company's policy for installing automatic updates. The Deployment Guide provides detailed information on what each setting does and what combinations can produce what results.

Conclusion

These tools have been provided by Microsoft and Shavlik Technologies to help administrators detect and protect their systems. It is our responsibility as administrators to find ways of implementing these tools to secure computer systems on the internet. It is also our responsibility to help each other to implement methods of patching and securing our computer systems. I hope to see more papers that help our community to implement strategies more efficiently and to improve on past processes. Patch management is only one step in securing our systems, but it seems like it is the most over looked and

most underestimated step in system security. We need to place a higher value on it and prevent the glorification of attacks like Code Red, Nimda, and SQL Slammer/Sapphire worms.

© SANS Institute 2003, Author retains full rights.

Appendix A

HFNETCHK Help File

hfnetchk.exe [-trace] [-h hostname] [-i ipaddress] [-d domainname]
[-n][-r range] [-history] [-t threads] [-b] [-ver]
[-o output] [-x datasource] [-v] [vv] [-s suppression]
[-nosum] [-sum] [-u username] [-p password] [-f outfile]
[-proxy] [-pxip] [-pxpt] [-pxp] [-pxu] [-pxd] [-pxs] [-ms]
[-fh hostfile] [-fip ipfile] [-about] [-fq ignorefile]

Description:

The HFNetChk tool assesses a machine or group of machines for security hotfixes that have either been installed and/or need to be installed.

For more information on this tool, please refer to:

<http://hfnetchk.shavlik.com/support>

Parameter List:

-about		About HFNetChk.
-h	hostname	Specifies the NetBIOS machine name to scan. Default is the localhost.
-fh	hostfile	Specifies the name of a file containing NetBIOS machine names to scan. One machine name per line, 256 max per file.
-i	ipaddress	Specifies the IP address of a machine to scan.
-fip	ipfile	Specifies the name of a file containing addresses to scan. One IP address per line, 256 max per file.
-fq	ignorefile	Specifies the name of a file containing Q numbers to ignore. One Q number per line.
-r	range	Specifies the IP address range to be scanned, starting with ipaddress1 and ending with ipaddress2 inclusive. <ipaddress1-ipaddress2>
-d	domain_name	Specifies the domain_name to scan. All machines in the domain will be scanned.

-n	network	All systems on the local network will be scanned. (i.e., all hosts in Network Neighborhood)
-history		Displays hotfixes that are explicitly installed and non-superseded hotfixes that are missing. This switch is not necessary for normal operation. Do not use this switch unless you've read -history usage at http://hfnetchk.shavlik.com/support/history .
-t	threads	Number of threads used for executing scan. Possible values are from 1 to 128. Default is 64
-o	output	Specifies the desired output format. (tab) outputs in tab delimited format. (wrap) outputs in a word wrapped format. (xml) outputs in simple xml format. (xml2) outputs in detailed xml format. Default is wrap.
-x	datasource	Specifies the xml datasource containing the hotfix information. Location may be an xml filename, compressed xml cab file, or URL. Default is mssecure.cab from the Shavlik website.
-s	suppress	Suppresses NOTE and WARNING messages 1 = Suppress NOTE messages only 2 = Suppress both NOTE and WARNING messages Default is to show all messages.
-nosum	checksum	Do not evaluate file checksum. The checksum test calculates the checksum of files. This can use up large amounts of bandwidth. Using this option will speed up a scan and use less bandwidth. File version checks will be still done.
-b	baseline	Display the status of hotfixes required to meet minimum baseline security standards.

-v	verbose	Displays the details for Patch NOT Found, WARNING and NOTE messages. Enabled by default in tab mode.
-vv	very verbose	Displays detailed information including bulletin summary, bulletin title and bulletin URL. Enabled by default in XML output.
-f	outfile	Specifies name of the file to save the results. Default is to display to screen.
-u	username	Specifies optional user name for login to remote computer.
-p	password	Specifies password to be used with user name.
-sum		Perform file checksum tests. Force checksum tests to be run on non-English language systems. Use only if you have a custom XML file with language-specific checksums.
-proxy		Use a proxy server.
-pxip	IP	IP address of the proxy server.
-pxpt	port	Port used for the proxy server.
-pxd	domain	Domain of the user for the proxy.
-pxu	user	Username to use for proxy server.
-pxp	password	Password to use for proxy server.
-pxs		Save the credentials used for the proxy.
-ver		Perform a version test of HFNetChk.
-ms		Download the mssecure.cab from Microsoft. The default uses the version hosted by Shavlik.
-trace		Enable debug logging. This must be the 1st parameter on the command line. The log file is written to hf.log. This command is not necessary for normal operation and should only be used when

troubleshooting an issue with Shavlik Support.

-? help Displays this menu.

Examples:

HFNETCHK
HFNETCHK -v -b
HFNETCHK -h hostname
HFNETCHK -h hostname -f out.txt
HFNETCHK -d domainname -u domainname\username -p password
HFNETCHK -d domainname -u username -p password
HFNETCHK -h h1,h2,h3
HFNETCHK -i 192.168.1.1 -s 2 -t 10 -v
HFNETCHK -i 192.168.1.1,192.168.1.8 -h hostname -x mssecure.xml
HFNETCHK -d domain_name -s 1 -o tab -x c:\temp\mssecure.xml
HFNETCHK -r 192.168.1.1-192.168.1.254 -history -t 20
HFNETCHK -x http://www.xyz.abc/mssecure.xml
HFNETCHK -x "c:\Space In Path\mssecure.xml"
HFNETCHK -fh d:\MyHostFile.txt
HFNETCHK -fip d:\MyIPFile.txt
HFNETCHK -o xml2
HFNETCHK -history
HFNETCHK -ver
HFNETCHK -proxy
HFNETCHK -pxu user -pxp password -pxd domain -pxip 192.168.1.29
-pxpt 8080 -pxs -proxy
HFNETCHK -trace -v -b
HFNETCHK -about

Appendix B

NOTE: This script is offered as is. Any modifications to the script that cause system issues or damage are solely the responsibility of the person making the modifications. Although the current script has been tested many, many times, the author is in no way responsible for problems caused by this script.

Hfreport.bat

*****cut*****

@ECHO OFF

```
REM *****
REM *The program only accepts the same parameters that HFNetChk.exe *
REM *can accept. Any parameters specified will be passed to the *
REM * HFNetChk.exe command line below. Sample usage might be: *
REM *C:\hfreportmkr.bat -vv *
REM * *
REM *****
```

REM Check to make sure HFNetChk.exe exists in the folder specified. If it does
REM not or it is located somewhere else, please modify this portion to point to
REM HFNetChk.exe on your system.

IF NOT EXIST c:\hfnetchk\HfNetChk.EXE GOTO FileMissing

REM You can modify its parameters but be
REM sure to keep the "-o tab" parameter and the redirection
REM of the output.
HfNetChk -fh serversdomain1.txt -u domain1\adminaccount -p adminpassword -o
tab %1 %2 %3 %4 %5 %6 %7 %8 %9 > list.txt
HfNetChk -fh serversdomain2.txt -u domain2\adminaccount -p adminpassword -o
tab %1 %2 %3 %4 %5 %6 %7 %8 %9 >> list.txt

REM Sort the output
%SystemRoot%\system32\sort < list.txt > report.txt

REM Output the results to HTML format. This is done by calling the hfnet.bat file.
Call hfnet.bat

REM Skip over error handlers
GOTO Done

:FileMissing
ECHO Error!
IF NOT EXIST HfNetChk.EXE ECHO HfNetChk.EXE is missing
ECHO Please make sure the Microsoft HfNetChk tool is installed
ECHO Pressing any key will exit

PAUSE
GOTO Done

:Done
REM End.

*****cut*****

© SANS Institute 2003, Author retains full rights.

Appendix C

NOTE: This script is offered as is. Any modifications to the script that cause system issues or damage are solely the responsibility of the person making the modifications. Although the current script has been tested many, many times, the author is in no way responsible for problems caused by this script.

Hfnet.bat

```
*****cut*****
```

Echo Off

```
Set CountryID=
Set Country=
Set Temp1=
Set Temp2=
Set Temp3=
Set ServerNameIP=
Set ServerName=
Set Software=
Set Bulletin=
Set QNumber=
Set Reason=
Set Status=
Set z=0
```

```
Set CountryID=US
Set Country=United States
goto Begin
```

```
:Next1
Set CountryID=UK
Set Country=United Kingdom
goto Begin
```

```
:Next2
Set CountryID=IE
Set Country=Ireland
goto Begin
```

```
:Next3
Set CountryID=MY
Set Country=Malaysia
goto Begin
```

```
:Next4
Set CountryID=FE
Set Country=Taiwan
goto Begin
```

```
:Begin
> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<!Website Info Comment Here^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<html^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<head^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<title^>Web Page Title Here^</title^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^</head^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<body^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>^<br^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<CENTER^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<font size="+3"
color="#008080" ^>^<div align="center" ^>^<strong^>%COUNTRY% Servers^</div^>^</strong^>^</font^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<br^>^<br^>^<br^>
```

```

For /F "tokens=1,2,3,4,5,6 delims=      " %%i in (c:\hfnetchk\report.txt) Do CALL :Process "%%i" "%%j" "%%k" "%%l"
"%%m" "%%n"
Set /A z=%z%+1
If [%z%]==[5] goto End
goto Next%z%

```

```

:Process
Set Temp1=%1
IF [%Temp1]==[] goto End
Set ServerNameIP=%Temp1:~1,-1%
Echo %ServerNameIP% > c:\hfnetchk\temp.txt
For /F %%i in (c:\hfnetchk\temp.txt) Do SET ServerNameIP=%%i
Echo %ServerNameIP%
Set ServerName=%ServerNameIP:~0,3%
IF [%ServerName%]==[Mac] goto Next

```

```

Set Temp1=%2
Set Software=%Temp1:~1,-1%
Set Temp1=%3
Set Bulletin=%Temp1:~1,-1%
Set Temp1=%4
Set QNumber=%Temp1:~1,-1%
Set q1=%QNumber:~0,4%
Set q2=%QNumber:~4,1%
Set q3=%QNumber:~5,2%
Set Temp1=%5
Set Reason=%Temp1:~1,-1%
Set Temp1=%6
Set Status=%Temp1:~1,-1%

```

```

IF [%Temp2%]==[%ServerNameIP%] goto Continue
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
width="800">
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
bgcolor="#8F9DFC">
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
size=+1^>^<Strong^>Software^</Strong^>^</Font^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
bgcolor="#8F9DFC">
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
size=+1^>^<Strong^>Bulletin^</Strong^>^</Font^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
bgcolor="#8F9DFC">
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
Number^</Strong^>^</Font^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
bgcolor="#8F9DFC">
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
size=+1^>^<Strong^>Reason^</Strong^>^</Font^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
bgcolor="#8F9DFC">
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
size=+1^>^<Strong^>Status^</Strong^>^</Font^>
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
Set Temp2=%ServerNameIP%

```

```

^</table^>
^<br^>^<br^>^<br^>
^<Center^>
^<font size=+2^>
^<Strong^>
%ServerNameIP%
^</Strong^>
^</font^>
^</Center^>
^<table border=1
^<tr^>
^<td
^<Font
^</td^>
^<td
^<Font
^</td^>
^<td
^<Font size=+1^>^<Strong^>Q
^</td^>
^<td
^<Font
^</td^>
^<td
^<Font
^</td^>
^<td
^<Font
^</td^>
^<tr^>

```

goto Continue

:Warning

```
Set Status=%QNumber%
Set QNumber=*****
Set Reason=%Bulletin%
Set Bulletin=*****
Goto Continue
```

:Info

```
Set Status=%QNumber%
Set QNumber=*****
Set Reason=%Software%
Set Bulletin=*****
Goto Continue
```

:Error

```
Set Status=%Bulletin%
Set QNumber=*****
Set Reason=%Software%
Set Bulletin=*****
Set Software=Error
Goto Continue
```

:Continue

```
Set Temp3=%Bulletin:-0,3%
IF [%Temp3%]==[Inf] goto Error
IF [%QNumber%]==[Warning] goto Warning
IF [%QNumber%]==[Information] goto Info
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
IF [%Bulletin%]==[*****] goto Blank1
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<a
href='http://www.microsoft.com/technet/security/bulletin/%Bulletin%.asp' target='_blank'^>
:Blank1
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
IF [%Bulletin%]==[*****] goto Blank2
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
:Blank2
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
IF [%QNumber%]==[*****] goto Blank3
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO ^<a
href='http://support.microsoft.com/support/kb/articles/%q1%/%q2%/%q3%.asp' target='_blank'^>
:Blank3
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
IF [%QNumber%]==[*****] goto Blank4
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
:Blank4
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
>> c:\inetpub\wwwroot\HFNetchk\%CountryID%\%CountryID%.asp ECHO
:Next
:END
```

*****cut*****

```
^<tr^>
^<td^>
^<font size=-1^>
%Software%
^</font^>
^</td^>
^<td width=90^>

%Bulletin%

^</a^>

^</td^>
^<td Width=90^>

%QNumber%

^</a^>

^</td^>
^<td^>
^<font size=-1^>
%Reason%
^</font^>
^</td^>
^<td^>
%Status%
^</td^>
^</tr^>
```

Appendix D

Switch	Description

/F	Forces other applications to close at shutdown.
/N	Does not back up files for removing hotfixes.
/Z	Does not restart the computer after the installation is completed.
/Q	Uses quiet mode; no user interaction is required.
/M	Uses unattended Setup mode (Windows 2000).
/U	Uses unattended Setup mode (Windows XP).
/L	Lists installed hotfixes.

The following code sample is a batch file that installs hotfixes and makes sure that the correct files are replaced after the computer is restarted.

```
@echo off

setlocal

set PATHTOFIXES=E:\hotfix

%PATHTOFIXES%\Q123456_w2k_sp4_x86.exe /Z /M

%PATHTOFIXES%\Q123321_w2k_sp4_x86.exe /Z /M

%PATHTOFIXES%\Q123789_w2k_sp4_x86.exe /Z /M
```


Appendix E

*****cut*****

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUp
date]

"WUServer"="http://<yourservername>"

"WUStatusServer"="http://<yourservername>"

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUp
date\AU]

"NoAutoUpdate"=dword:00000000

"AUOptions"=dword:00000004

"ScheduledInstallDay"=dword:00000000

"ScheduledInstallTime"=dword:00000003

"UseWUServer"=dword:00000001

"NoAutoRebootWithLoggedOnUsers"=dword:00000001

"RescheduleWaitTime"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Win
dowsUpdate\Critical Update]

"SelfUpdServer"="http://<yourservername>/SelfUpdate/CUN5_4"

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Win
dowsUpdate\Critical Update\Critical Update SelfUpdate]

"SelfUpdServer"=http://<yourservername>/SelfUpdate/CUN5_4

*****cut*****

References:

1. Lyman, Jay. "The Trouble with Software Patches." 16 April 2002.
URL: <http://www.ecommercetimes.com/perl/story/19023.html>
2. Mullen, Tim. "Patch Management Done Right." 06 May 2002.
URL: <http://online.securityfocus.com/columnists/79>.
4. Lyman, Jay. "Gartner: IT Security Efforts 'Poor'." 02 May 2002.
URL: <http://www.newsfactor.com/perl/story/17572.html>.
5. LaPage, Andrew. "Accessing Security Risks with the Microsoft Baseline Analyzer." *Inside Microsoft Windows 2000*. Vol. 2. December 2002: 1 – 5.
6. www.sans.org/rr
7. www.microsoft.com/security
8. <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q296861&sd=tech>
9. <http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B305228>
10. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp>
11. http://www.microsoft.com/windows2000/docs/SUS_Deployguide_sp1.doc
12. <http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp>
13. <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q296861&ID=kb;en-us;Q296861>
14. <http://www.shavlik.com/pHFNetChkLT.aspx>
15. Mimoso, Micahel. "Patching negligence can get you sued." 12 Feb. 2003.
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci880118,00.html