



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 of Microsoft Products Using HFNetChkPro by Shavlik Technologies

Kris Poznanski
December 25, 2002 (retake)
Version 1.4

Table of content:

1.	ABSTRACT.....	3
2.	INTRODUCTION.....	4
3.	MICROSOFT PRODUCTS SUPPORTED BY HFNETCHKPRO.....	5
4.	FEATURES OF HFNETCHKPRO	6
5.	HFNETCHKPRO SCAN ENGINE.....	7
6.	SCANNING PRE-REQUISITES	8
7.	PERFORMING SCANS USING HFNETCHKPRO	9
8.	SAMPLE SCAN RESULT BY HFNETCHKPRO	21
9.	DOWNLOAD CENTER	23
10.	PATCH DEPLOYMENT OVERVIEW	25
11.	PATCH DEPLOYMENT TESTING.....	26
12.	PATCH DEPLOYMENT USING HFNETCHKPRO	29
13.	PATCH DEPLOYMENT VERIFICATION USING HFNETCHKPRO.....	38
14.	REPORTING	41
15.	SUMMARY.....	45
16.	REFERENCES	46

© SANS Institute 2003, Author retains full rights.

1. Abstract

On many occasions security breaches could have been prevented if software patches and updates were applied when they were first available. In fact, figures from the SANS Institute and FBI show that the majority of commonly exploited vulnerabilities are due to the failure to apply fixes that were available from vendors for several weeks or even a month. For those who work with Microsoft products, it's a known fact, that keeping them secured, presents a great deal of challenge to any security or network administrator, especially when critical updates are being issued by Microsoft almost on a weekly basis. In response to such a challenge Microsoft together with Shavlik Technologies has developed a Network Security Hotfix Checker the HFNetChk tool (Hfnetchk.exe), which is a command-line tool that administrators can use to centrally assess a computer or group of computers for the absence of security patches. Unfortunately, the Microsoft version can only be used as a command-line tool and it's limited only for reporting of missing security patches. The burden of patch deployment is still placed on the shoulders of network and security administrators.

© SANS Institute 2003, Author retains full rights.

2. Introduction

Shavlik Technologies Network Security Hotfix Checker Professional HFNetChkPro is the commercial, more full-featured version of the HFNetChk product distributed by Microsoft that allows administrators to centrally inspect Windows based computer systems or group of systems on their networks to ensure that they have the most up-to-date security patches. HFNetChkPro provides both identification of missing patches and detailed information on the reason a security patch is required. New or needed patches can then be downloaded to a central repository and pushed out to the machines that need them, or scheduled for later downloading and patching. By using HFNetChkPro multiple patches can be applied to the same system with only one reboot. The new version of HFNetChkPro, version 3.8, allows also monitoring the installation of pushed patches and service packs. The new version also comes equipped with a patch installation database that includes information on and descriptions of patches from Microsoft, as well as verification that the patches being downloaded are actually coming from Microsoft.

© SANS Institute 2003, Author retains full rights.

3. Microsoft Products Supported by HFNetChkPro

The HFNetChkPro can be used to scan and patch systems running the following Microsoft products:

- Windows NT 4.0
- Windows NT 4.0 Enterprise Edition
- Windows NT 4.0 Server Terminal Server Edition
- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows XP
- Windows XP Tablet PC
- SQL Server 7.0 and 2000
- Exchange Server 5.5 and 2000
- Internet Information Services 4 and 5
- Internet Explorer 5.0 and up
- MDAC 2.5, 2.6 and 2.7
- Windows Media Player 6.4, 7.0, 7.1
- Windows Media Player for Windows XP

© SANS Institute 2003, Author retains full rights.

4. Features of HFNetChkPro

The following are the key features of Shavlik HFNetChkPro tool:

- Real-time Patch Information
- Both Command Line and GUI Interface
- Scan by IP Address, by Hostname and by Domain
- Patch Pushing and Management
 - o Full Event Log Writing and Viewing to Track Install Success and Failures
 - o Push Patches One by One or by Group
 - o Push Patches to One Computer or to Many at One Time
 - o Microsoft Patch Files are Signed and Validated to Assure They are From Microsoft
 - o Push Patches by Schedule, Immediately, or Just Copy Patches
 - o Robust Scheduling of Patch Installation to Allow for Off-Hours Installations
 - o Remote Reboot Support
- View and Monitor Patch Push History
- SQL Server and Microsoft Access Data Storage Database Support for Storing Patch Push Results and History
- Full Reporting
 - o XML, HTML and comma-delimited output
- Turn off SQL Server and IIS Remotely to Help with Installation and to Disable Rogue Servers
- Named Scans to Allow for Better Tracking
- Advanced Domain Enumeration to Find All Computers on the Network
- Ability to Send Messages to Computers You are Updating to Prepare Users
- Remote Patch Deployment
- Cross-Domain Patch Deployment
- Pre-install Validation Engine
- Scheduled Scans
- Scan by Product (IIS only, SQL Only etc.)
- Scan by Patch (MS02-001 Only, etc.)
- Scan by Machine Type (Servers only, Workstations only, etc.)

5. HFNetChkPro Scan Engine

In order to determine which patches need to be applied to a scanned system, the HFNetChkPro scan engine uses XML (eXtended Markup Language) technology. HFNetChkPro stores information about all hotfixes inside the MSSecure.XML file which is updated by Microsoft every time a new security bulletin is released. The following information about a particular hotfix is stored in the MSSecure.XML file:

- Which operating system it's for
- Which version it's applicable to
- What service pack it's applicable to

The file has all of the details that come with the hotfix: the file version, the file checksum, the file location, registry keys which tell whether or not this patch has been applied or not and the supersedence information.

© SANS Institute 2003, Author retains full rights.

6. Scanning Pre-Requisites

Before scanning computer system using HFNetChkPro occurs, the following criteria must be met to ensure a successful scan:

When scanning your local machine:

- You must have administrative access to your local machine.
- The machine must be capable of obtaining the patch database XML file, either from a location on the Internet, or from another specified location (either on the local machine, or from a specified network location.)
- The local machine's Workstation service must be started.
(NOTE: The Server service is not required to be started on the local machine.)

When scanning a remote machine you must meet all the requirements for the local scan above, plus:

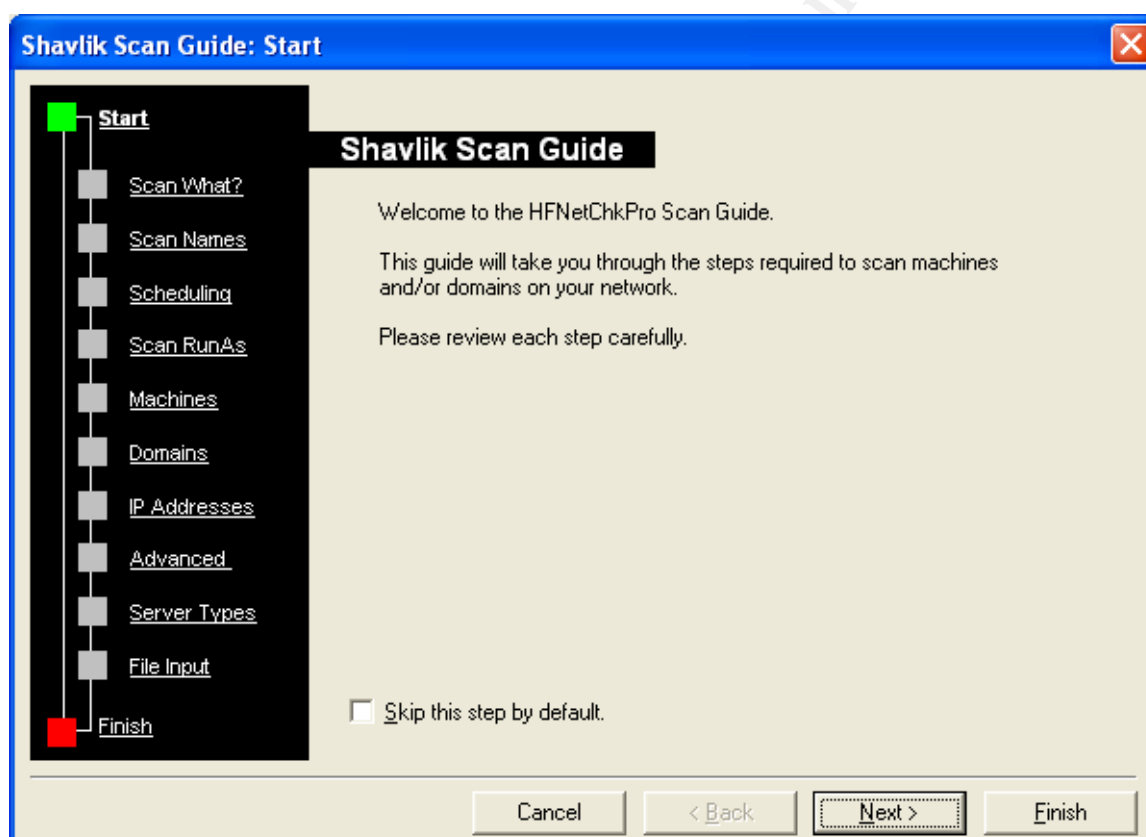
- You must have administrative rights on the remote machine and be able to logon to this machine from the workstation performing the scan.
- The NetBIOS (tcp139) or Direct Host (tcp445) ports must be accessible on the remote machine.
- The remote machine must be running the Server service.
(NOTE: the Workstation service is not required to be started on the remote machine.)
- The remote machine must be running the Remote Registry service.
- The %systemroot% share (usually C\$ or similar) must be accessible on the remote machine

© SANS Institute 2003. Author retains full rights.

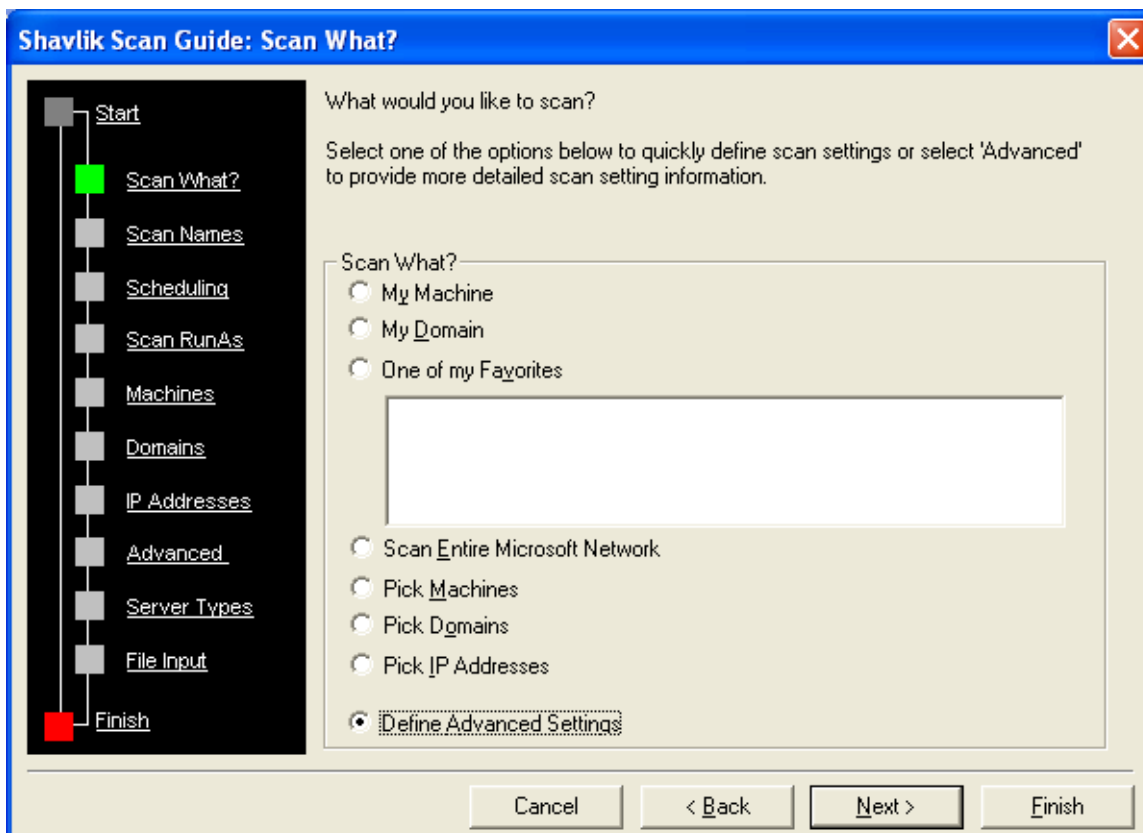
7. Performing Scans Using HFNetChkPro

The Shavlik HFNetChkPro interface provides a method for the user to quickly set up a powerful set of scan rules/settings to use when performing a network security scan. The screens below illustrate each step included in configuring Scan Settings.

In order to perform a scan start HFNetChkPro and click File-New Scan on the main toolbar. You will be presented with a Shavlik Scan Guide that will walk you through the steps of setting scanning parameters and performing scans on your network.

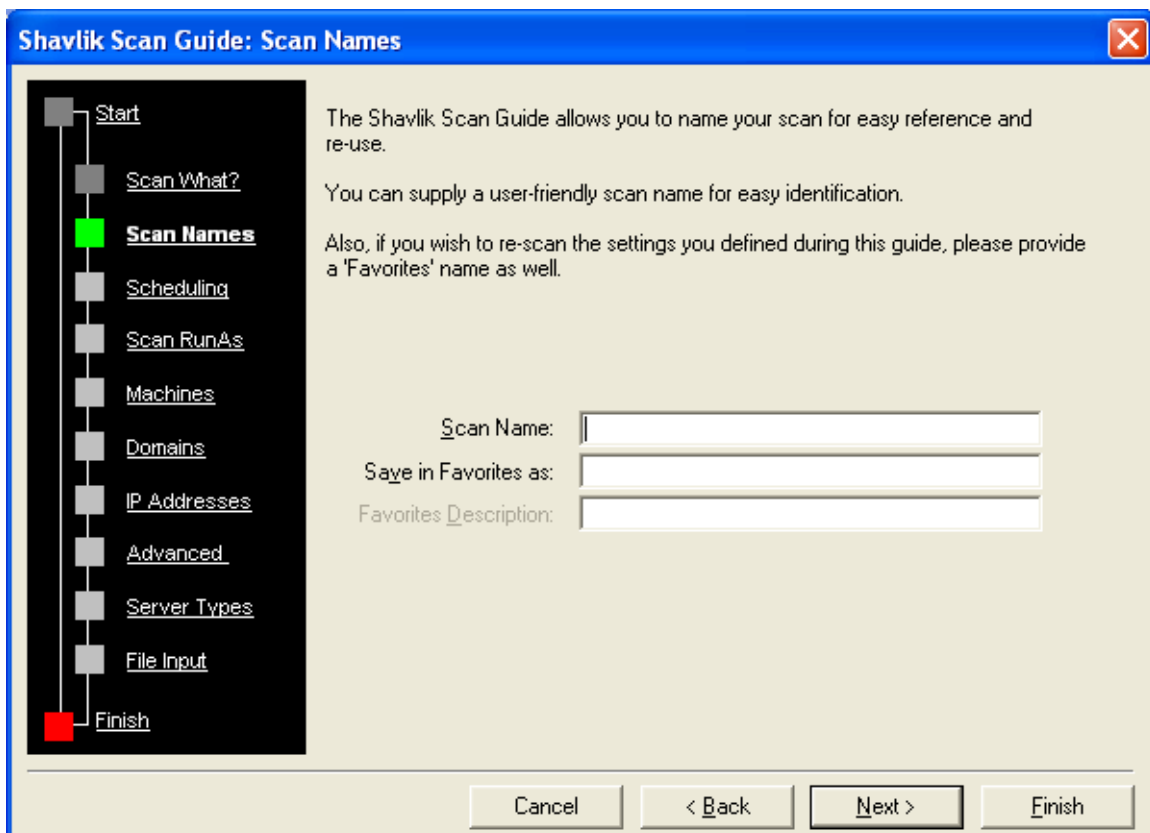


Start Screen: This first screen displays a set of basic steps that need to be performed when setting up a network scan.



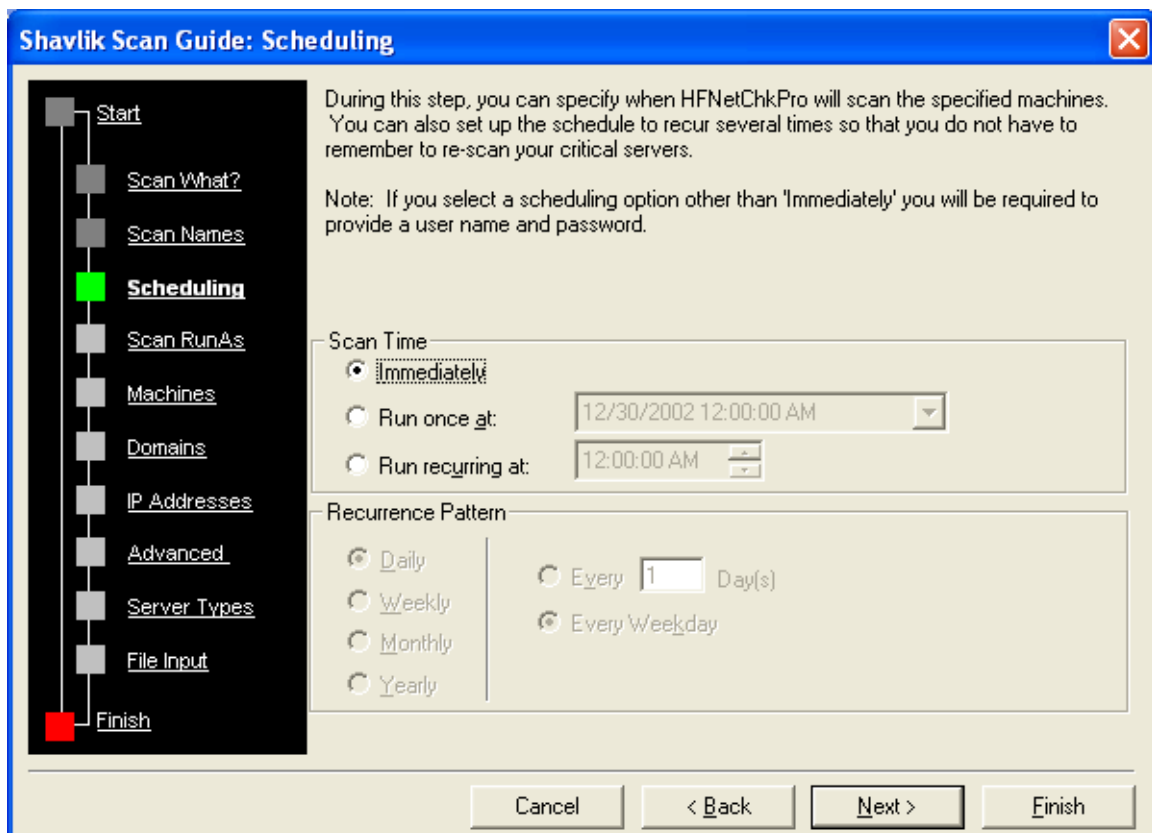
Scan What? Screen: This step allows to quickly defining what needs to be scanned. Each available option is explained below:

1. My Machine - Allows perform a scan of your machine only.
2. My Domain - Allows perform a scan of your current domain.
3. One of my Favorites – Allows re-running of one of the previous scans saved in your Favorites
4. Scan Entire Microsoft Network – Allows scanning of your entire Microsoft Network
5. Pick Machines - This option will enable the 'Machines' step in the wizard allowing you to scan one or many machines based on the names you provide.
6. Pick Domains - This option will enable the 'Domains' step in the wizard allowing you to scan one or many domains based on the names you provide.
7. Pick IP Addresses - This option will enable the 'IP Addresses' step in the wizard allowing you to scan one or many IP Addresses/Ranges based on the information you provide.
8. Define Advanced Settings - This option will enable ALL steps in the wizard allowing the network administrator full control over all scan settings.



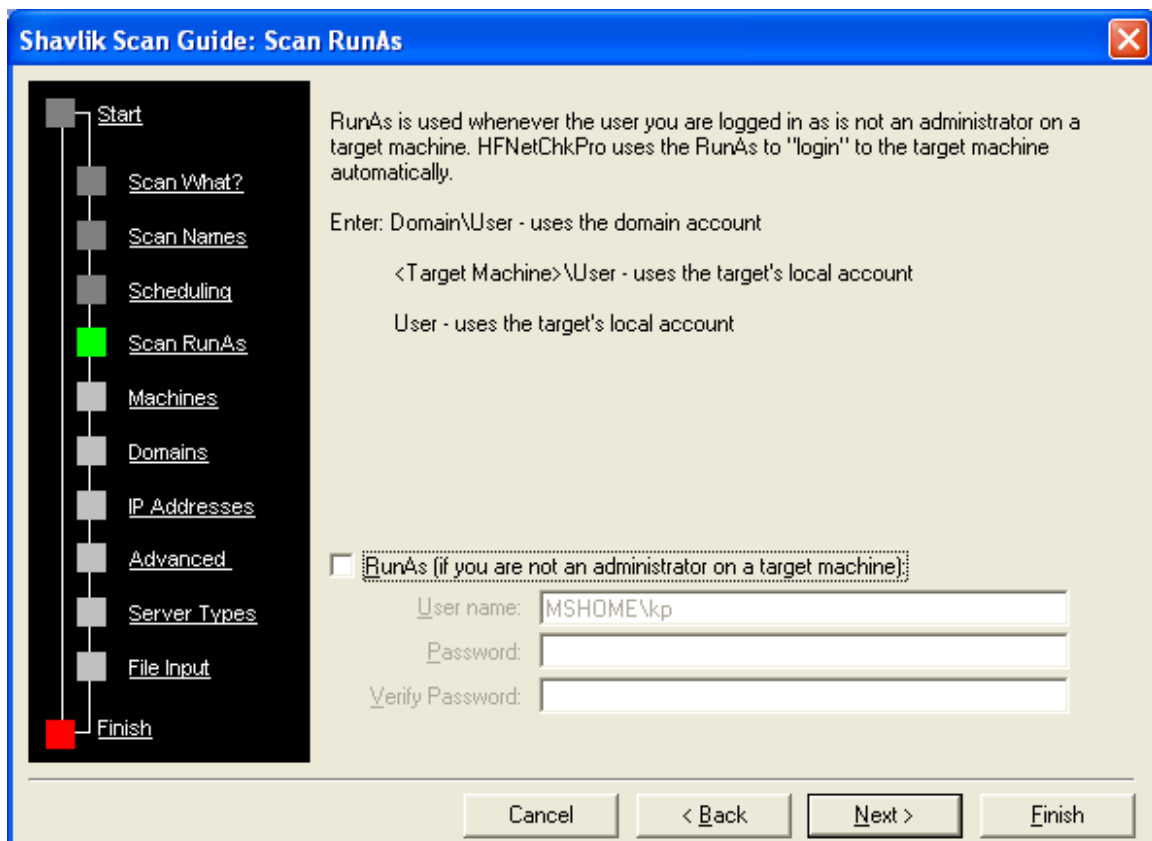
Scan Names Screen: This option allows defining names for the scan for future and easier identification.

1. Scan Name – It provides you an option to name your scan, so you can easily reference to it in the future. For example, the scan name can contain a date of the scan and the name of the computer system to be scanned. When performing more complex scans of your network, for example by machine type, it is a good idea to incorporate the scanned machine type in the scan name for future reference (ex. 'All SQL Servers on December 29, 2002'). Another words, the scan name needs to effectively describe the rule set that is defined for a particular scan.
2. Save in Favorite as - This option allows you to save all the settings provided during the Scan Guide for later re-use. For example, when defining complex scans with multiple IP ranges, this option will save you time re-entering all IP addresses every time a scan needs to be performed. Using this option, you can save all your preferences to the database so you can simply right click on a favorite and select 'Re-Scan'.



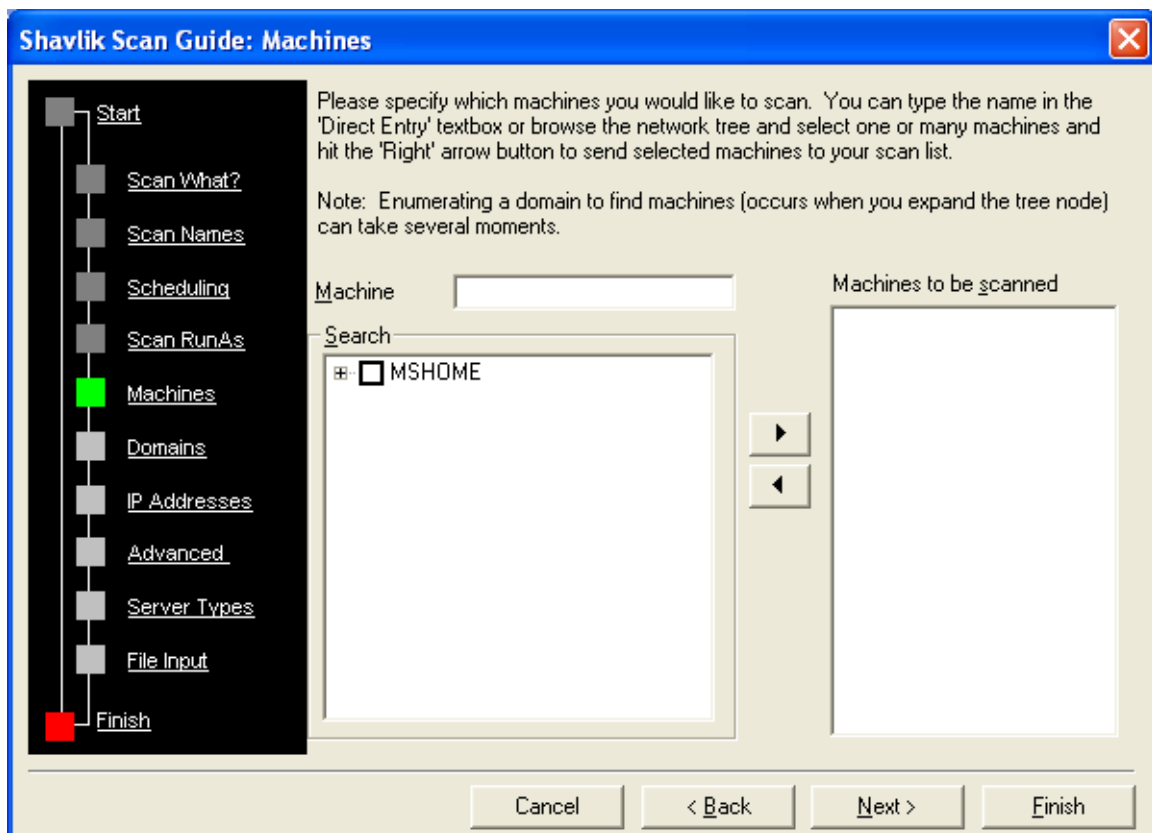
Scheduling Screen: This option allows network administrators to schedule when a particular scan will be executed. By default all scans will run immediately unless specified differently. Since making your network secured is an ongoing effort and new vulnerabilities are being discovered frequently, you can configure your scans to re-occur automatically by utilizing the Run recurring at option and setting the Recurrence Pattern. Shavlik Scan Scheduling is enabled by placing a job in the Windows Task Scheduler to execute a batch file created automatically by the application.

© SANS Institute



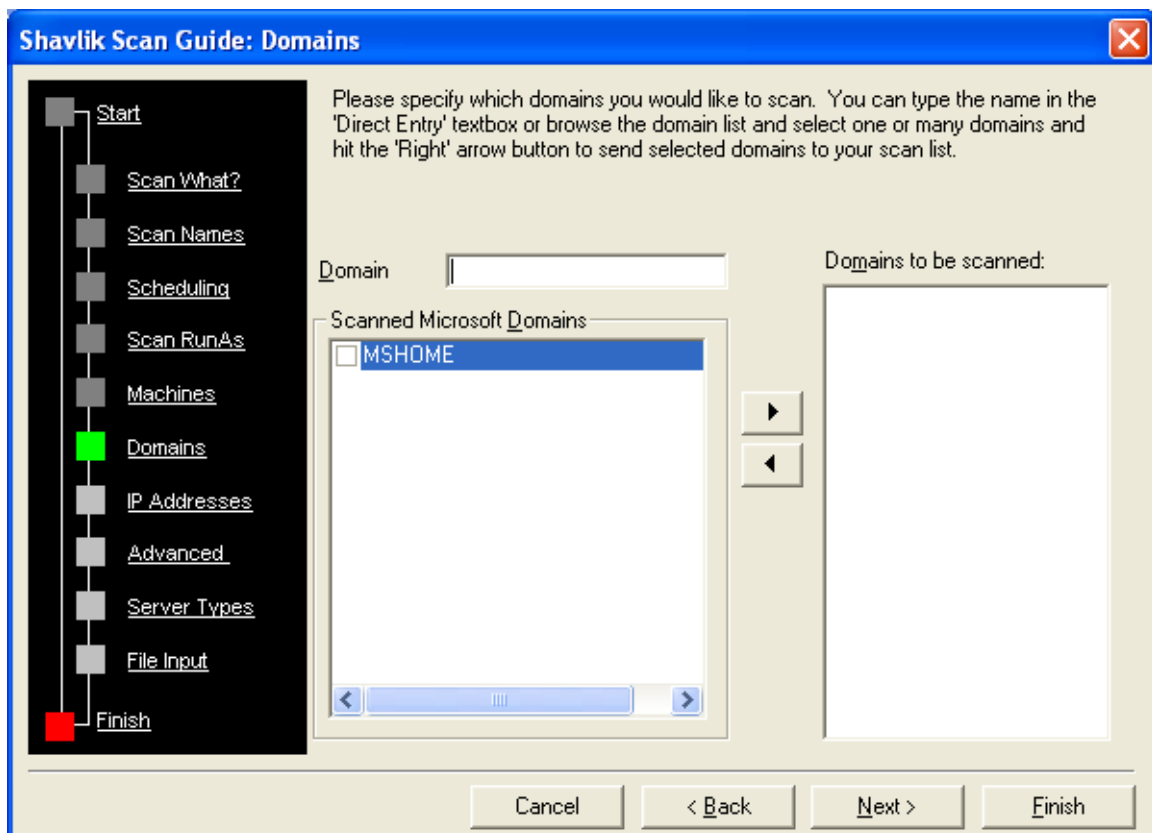
Scan RunAs Screen: The Shavlik HFNetChkPro requires administrative credentials if the scan settings contain machines and/or domains that the current user login does not have rights to. This option allows you to specify a user name and the password that has administrative privileges to a scanned computer system.

© SANS Institute



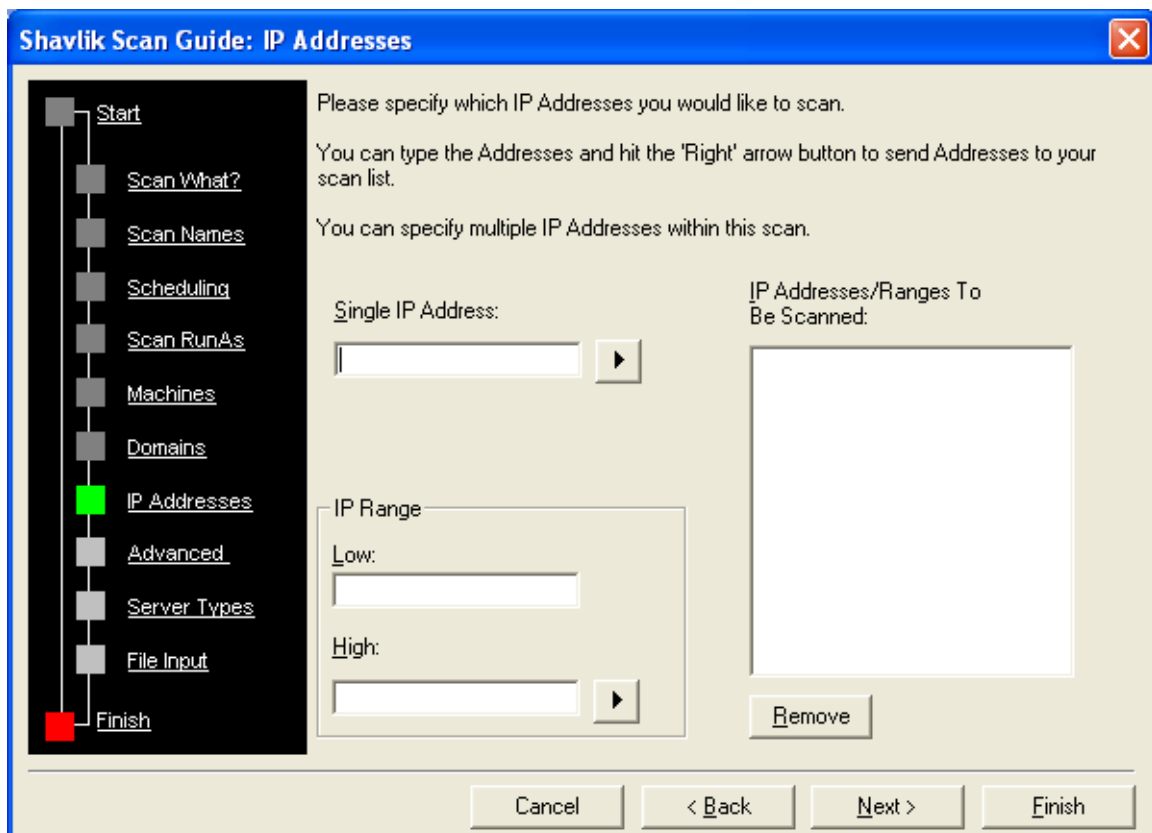
Machines Screen: This step allows you to enter a single or multiple machine names to be scanned. A single or multiple machines can be entered in the Machine field. You must click on the right-arrow button '>' for the machine to appear on the Machines to be scanned list. Multiple machine names can be also selected by browsing the Search tree.

© SANS Institute



Domains Screen: This step allows you to enter a single or multiple domain names to be scanned. A single or multiple domains can be typed in the Domain field. You must click on the right-arrow button '>' for the domain to appear on the Domains to be scanned list. Multiple domain names can be also selected by browsing the Scanned Microsoft Domains tree.

© SANS Institute



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 Range

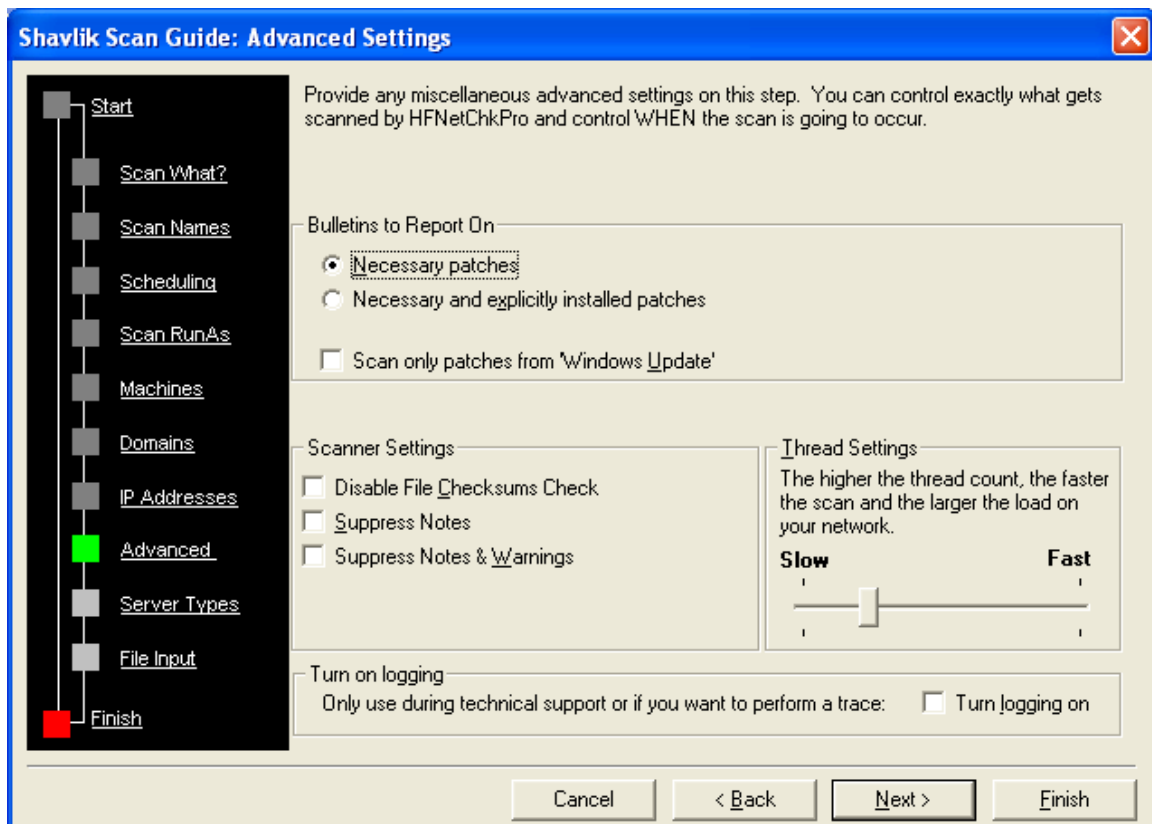
Low:

High:

IP Addresses/Ranges To Be Scanned:

IP Addresses Screen: This step allows network administrators to add a custom list of IP Addresses and/or IP Ranges. Users can input a single IP address to be scanned by entering a valid IP address into the Single IP Address field and hitting Enter or clicking on the right-arrow button '>'. You can also specify a range or multiple ranges of IP addresses to be scanned by entering the beginning address of the IP range in the Low field and the end address of the IP range in the High field. All IP addresses and IP ranges will appear on the IP Addresses/Ranges To Be Scanned list.

© SANS Institute

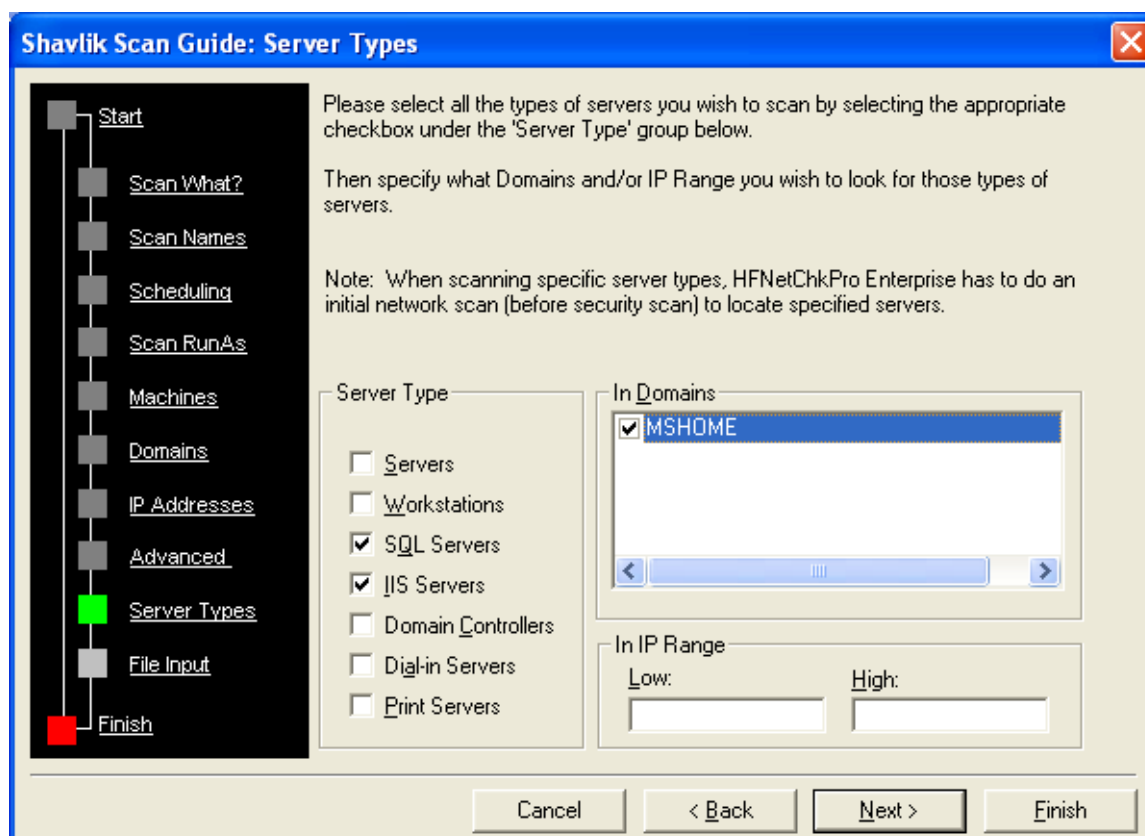


Advanced Screen: This step allows users to set some advanced scan rules to be applied to the scanner while performing the scan. Below are the explanations of each advanced settings:

1. Bulletins to Report On - The user can determine which type of bulletins to report on.
2. Scanner Settings - The user can configure what type of checks the scanner will perform. Currently there is only one type of scan checks a) File Checksums. Additionally the user can configure the scanner to ignore Notes and Warning bulletins.
3. Thread Settings - The user can control the thread count of the scanner. The higher the thread count, the faster the scan will perform however there will be a larger load on the network as a result.
4. Turn on logging – This option can be used to troubleshoot the scan when working with Shavlik's Technical Support staff.

Note: Shavlik recommends leaving 'Disable File Checksums Check' **unchecked**. This allows the scanner to execute an "Anti-spoof Scan" which is a detailed binary analysis of each file for each patch to assure that no one has tried to "fake" a file on your network. You should run this level on scan on your key computers on a regular basis. However, the scan does take more time and network bandwidth. Do not check this box when doing large scale scans from one server point. It is strongly recommended that Anti-Spoof

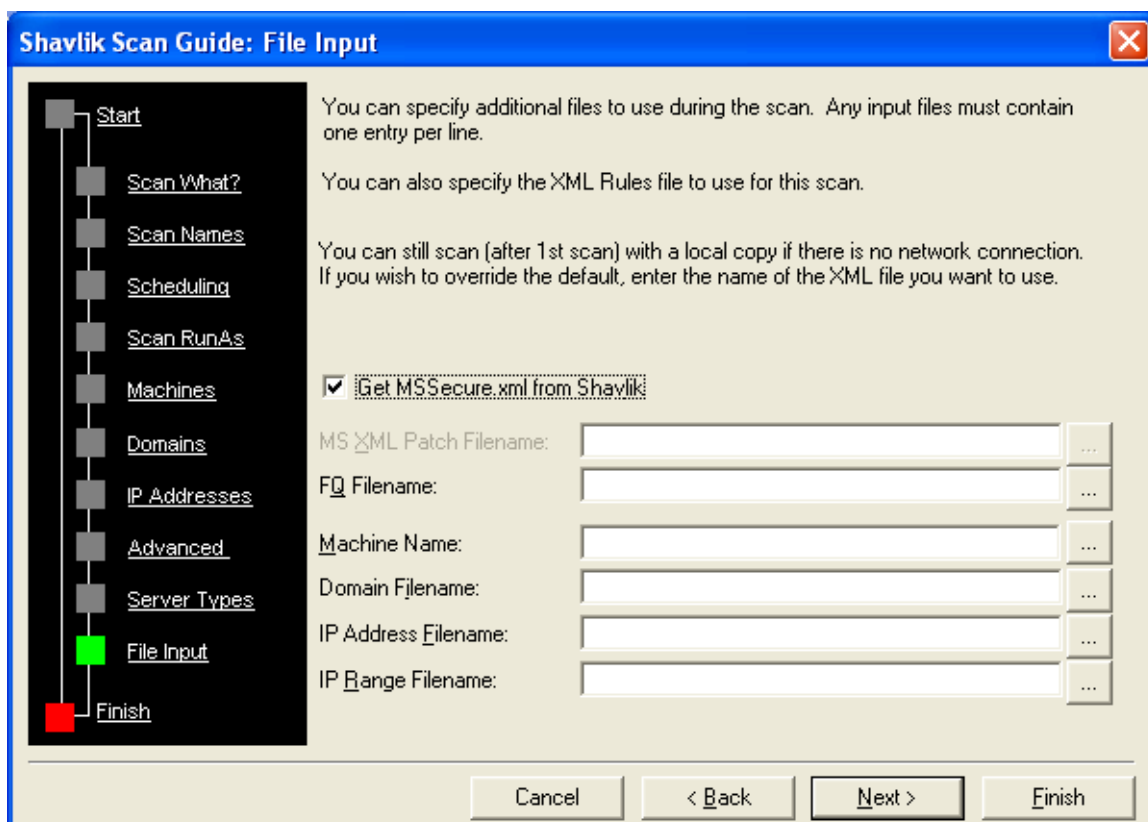
scans be done on a regular basis on all computers. Scans that do not use Anti-Spoofing still get full file version checking.



Server Types Screen: This step allows network administrators to build custom files containing a list of machine types. This tab provides users with the power of building scans only against machines that perform a specific function (e.g. SQL Servers only) and are located in a specific domain and/or IP Range.

1. Server Type - Use the list of Server Type options to build your custom machine list file. These options are *not* exclusive (e.g. if SQL Servers and IIS Servers are checked and the domain is MSHOME as displayed, the build list process will enumerate every machine on the MSHOME domain to determine if SQL Server or IIS server is installed. If SQL Server or IIS server is installed, then the machine name will be placed in the custom machine file.
2. In Domains - The user can look for any type of server in any domain. For all domains checked, the build list process will enumerate each machine in that domain and check it to see if *any* of the server type options apply. If any server type option applies, the machine name will be added to the file.
3. In IP Range - The user can look for any type of server in any IP Range. For all IP Ranges supplied, the build list process will enumerate each machine in that domain and check it to see if *any* of the server type options apply. If any server type option applies, the machine name will be added to the file.

Note: The IP Range and the In Domain selections are *not* exclusive. The build list process will first walk all Domains in the In Domain regardless of any IP Ranges provided. When the domains are complete, the process will then walk all IP Ranges provided regardless of any domains checked.

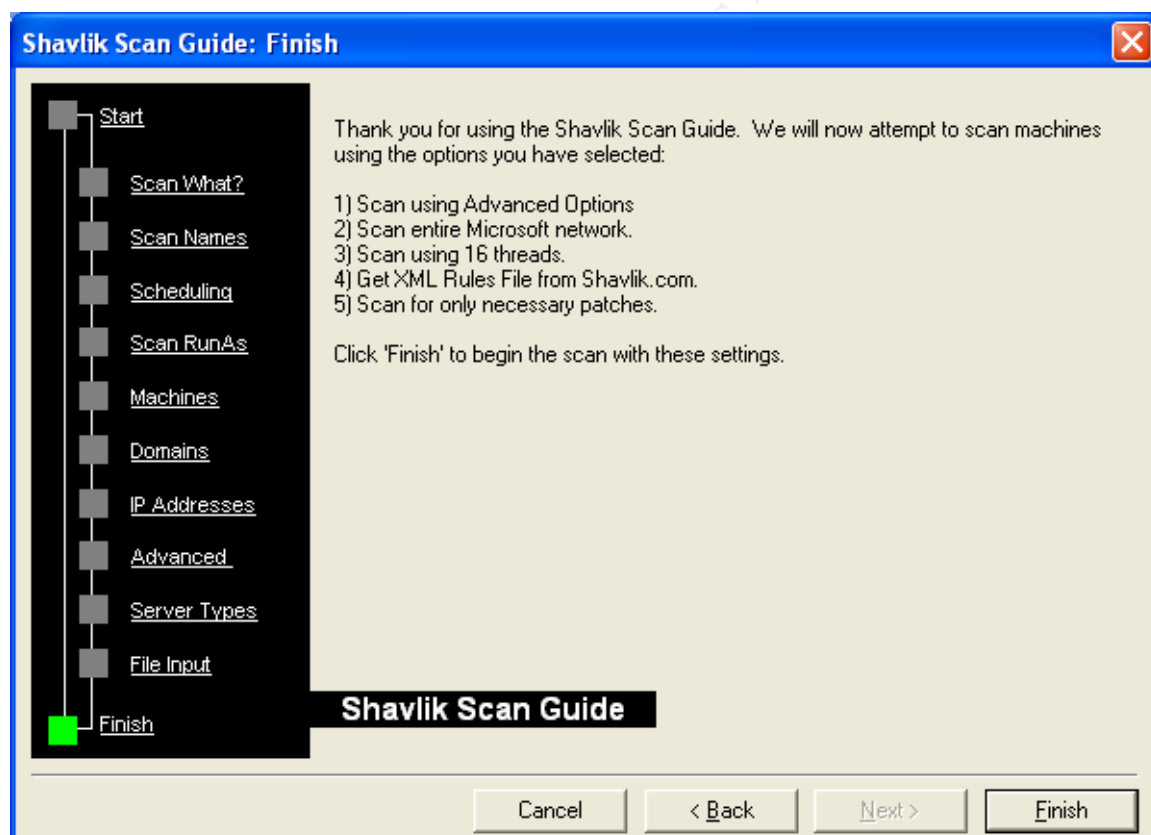


The image shows a Windows-style dialog box titled "Shavlik Scan Guide: File Input". On the left is a vertical navigation pane with a tree view containing the following items: Start, Scan What?, Scan Names, Scheduling, Scan RunAs, Machines, Domains, IP Addresses, Advanced, Server Types, File Input (highlighted with a green square), and Finish (highlighted with a red square). The main area of the dialog contains instructions and input fields. The instructions are: "You can specify additional files to use during the scan. Any input files must contain one entry per line.", "You can also specify the XML Rules file to use for this scan.", and "You can still scan (after 1st scan) with a local copy if there is no network connection. If you wish to override the default, enter the name of the XML file you want to use." Below these instructions is a checkbox labeled "Get MSSecure.xml from Shavlik:" which is checked. Below the checkbox are six text input fields, each followed by a browse button (three dots): "MS XML Patch Filename:", "FQ Filename:", "Machine Name:", "Domain Filename:", "IP Address Filename:", and "IP Range Filename:". At the bottom of the dialog are four buttons: "Cancel", "< Back", "Next >", and "Finish".

File Input Screen: This step allows network administrators to define the file input rules (e.g. the XML Patch file, a user created Domain List file, a user created IP Address file, and/or a user create IP Range file).

1. Get MSSecure.XML from Shavlik - The user can set which XML file the scanner will use to locate information about security bulletins. It is suggested that you leave this blank and use the default XML file from Shavlik that will be downloaded at the time of the scan. However, if you are scanning without a connection to the Internet, you can specify a local file name (e.g. the MSSecure.XML file downloaded during a previous scan) to override the default.
2. FQ Filename - The user can specify a file name containing a list of favorite scans. The file should be in the format of Favorites separated by line feeds. The scanner will then parse this file and attempt to enumerate each Favorite scan supplied.
3. Machines - The user can specify a file name containing a list of machines. The file should be in the format of Machines separated by line

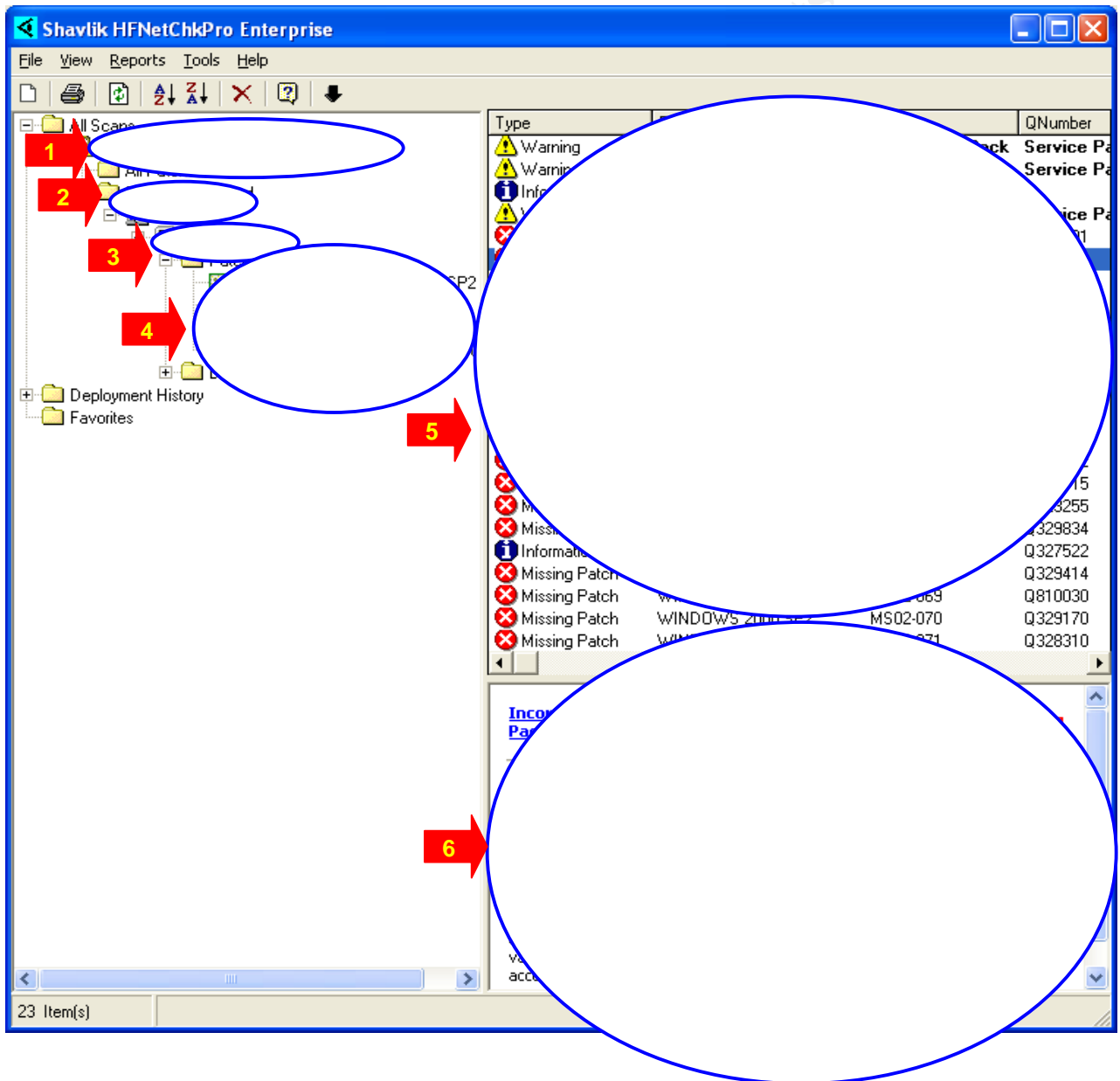
- feeds. The scanner will then parse this file and attempt to enumerate each Machine supplied.
4. Domain Filename - The user can specify a file name containing a list of domains. The file should be in the format of Domain Name separated by line feeds. The scanner will then parse this file and attempt to enumerate each domain supplied.
 5. IP Address Filename - The user can specify a file name containing a list of IP Addresses. The file should be in the format of IP Address separated by line feeds. The scanner will then parse this file and attempt to scan each IP Address supplied.
 6. IP Range Filename - The user can specify a file name containing a list of IP Ranges. The file should be in the format of [IP Low Address]-[IP High Address] (e.g. 1.1.1.1-1.2.2.2) separated by line feeds. The scanner will then parse this file and attempt to scan each IP Address within the range supplied.



Finish Screen: This step allows network administrators to review all the options they have selected before continuing on. If all the options listed look correct, simply click 'Finish' and the HFNetChkPro will performed the desired scan.

8. Sample Scan Result by HFNetChkPro

In order to illustrate Shavlik HFNetChkPro scan results, I have performed a sample scan on a computer configured with Windows 2000 Professional. The scan results are shown on the screen shot below. As you can see, valuable information is being provided about this scan.



1 → This field represents the name of the scan which tells us what kind of machine (Win2kPro) has been scanned, on what date (12/29/2002) and time 10:48 PM).

2 → This field represents the domain name (MSHOME) that Win2kPro workstation is a member of.

3 → This field represents the name (WIN2KPRO) of the machine that has been scanned.

4 → This section allows to displaying the patch information categorized by product. It allows security or network administration to drill down and find any security information related to a specific product in a matter of a few mouse clicks.

5 → This section called list navigation pane displays the list of missing security patches including effected products, Microsoft Security Bulletin numbers, Q articles numbers and short descriptions. In addition, it also displays warnings about not installed service packs.

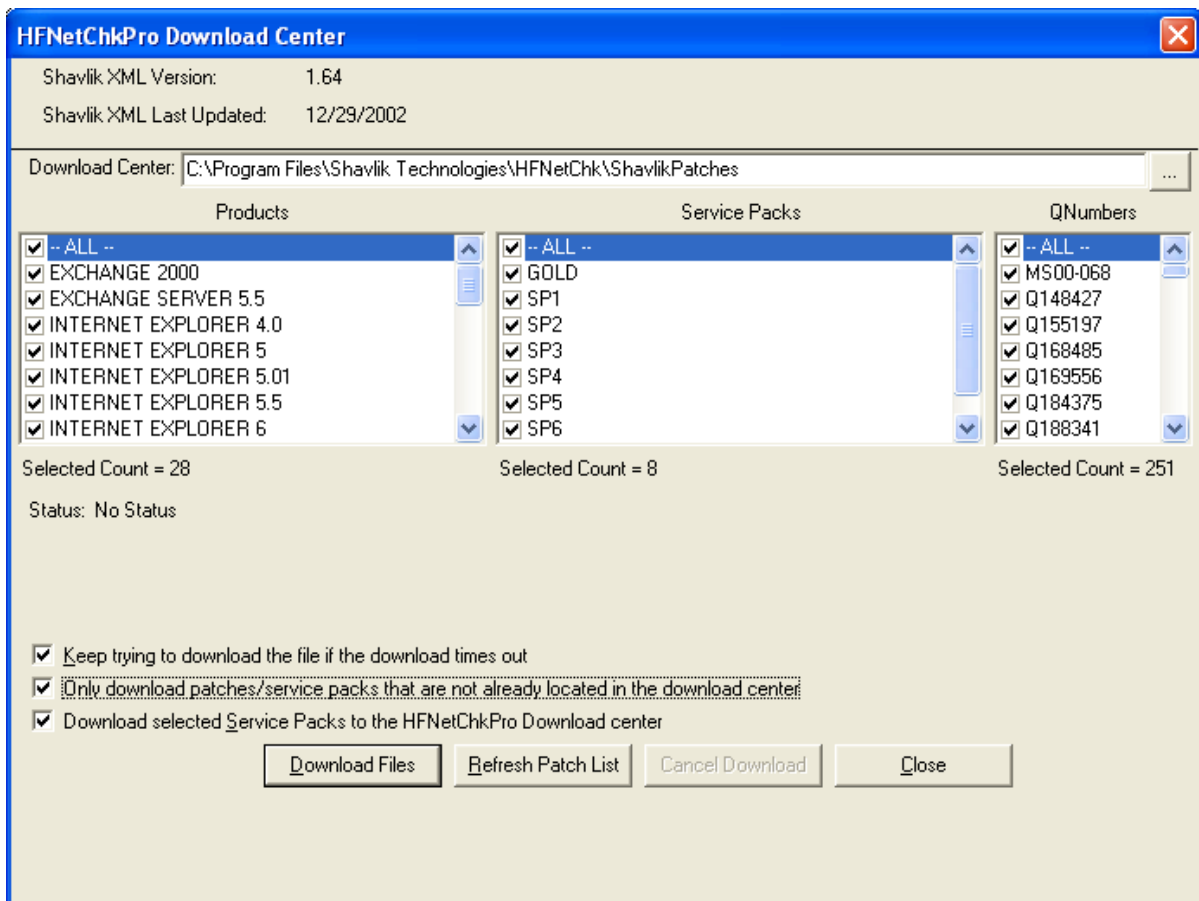
6 → This section of the screen is called a preview pane. Every time the user clicks on an item in the list navigation pane, a detailed report will appear in the preview pane. In the example above, the user has clicked on a Missing Patch and the preview pane has displayed all important information for that patch and provided direct links to Microsoft Security Bulletins and Q articles to download and install the patch.

© SANS Institute 2003, All rights reserved. Author retains full rights.

9. Download Center

The Shavlik Technologies Network Security Hot fix Checker Pro provides an option to automatically download any or all Microsoft service pack and patch files by using the Download Center. The Download Center management option can be found under the Tools on the main menu bar by selecting the "Download Center". It is recommended that you first establish your download location which is where all your service pack and patch files will be downloaded, stored, and used by the deployment wizard. Since the Download Center is a directory created during installation, it is strongly advised that the download center path is properly secured to ensure that no malicious users can place 'spoofed' files in the directory. The Download Center can be placed anywhere that the HFNetChkPro application has access to. In case when several administrators or one administrator manage the network from several machines, the Download Center can be placed on a shared drive on the network so that all required users/machines have access to it. Downloading service packs and hotfixes to the Download Center first, makes patch deployment a lot faster. To avoid downloading the same patches or service packs over and over, simply check the "Only download patches/service packs that are not already located in the download center" option. Also, to ensure that all patches and service packs will be stored in the Download Center, make sure that the "Download selected Service Packs to the HFNetChkPro Download center" option is checked. If the check box "Keep trying to download the file if the download times out" is checked, HFNetChkPro will attempt to download any files that time out until they have been successfully downloaded. From time to time, Microsoft's host site gets busy and you are not able to download certain files. To correctly use HFNetChkPro, you need an available Internet connection to download PatchDetails2.cab which contains PatchDetails.XML and Commandline.cab which contains CommandLine.EXE. Both files can be downloaded by clicking on the "Refresh Patch List" button located on bottom of the Download Center management screen. If these files DO NOT exist, HFNetChkPro will not function properly. The picture on the following page shows the main screen of the HFNetChkPro Download Center management tool.

© SANS INSTITUTE



© SANS Institute 2003

10. Patch Deployment Overview

The Shavlik HFNetChkPro allows local and remote patch deployment in a very simple manner. The current solution for many network administrators is to use HFNetChk command line version or a similar tool, diagnose the security state of each machine and then go around to every machine downloading the patches and applying them. This can be a tremendous time burden. Remote deployment feature greatly simplifies this and allows the network administrator to manage a vast majority of the tasks of network security directly from one user interface console.

Before discussing the patch deployment, it should be noted that before each patch installation is copied from the Download Center to the remote target machine, the Microsoft Signature is verified to eliminate malicious/spoofed application installations. Also, HFNetChkPro uses Microsoft's Qchain.exe during remote deployment to allow applying several hotfixes without a reboot.

When using HFNetChkPro, network administrators have several options for deploying security patches and service packs. They can select one, several or all patches for one machine or for a group of machines.

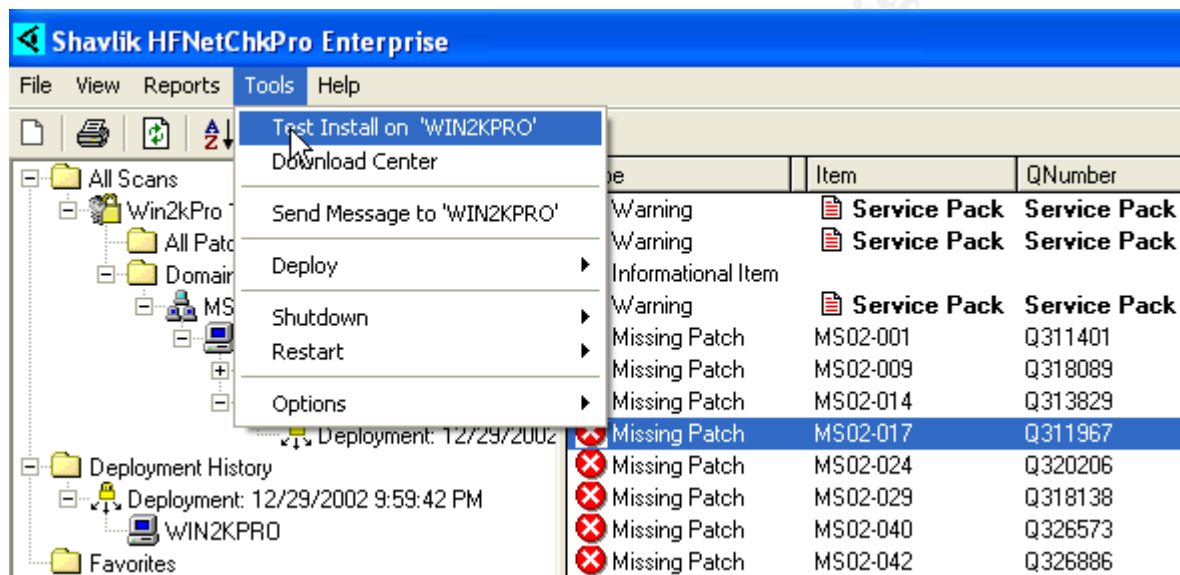
Another feature that HFNetChkPro incorporated to allow more security control of a network is the ability to shut down machines remotely and even shut down the IIS Service or SQL Service on remote machines. This can be beneficial if a new patch is released by Microsoft and the criticality of the patch is so severe that a network administrator may want to immediately shut down a specified service until the patches are deployed.

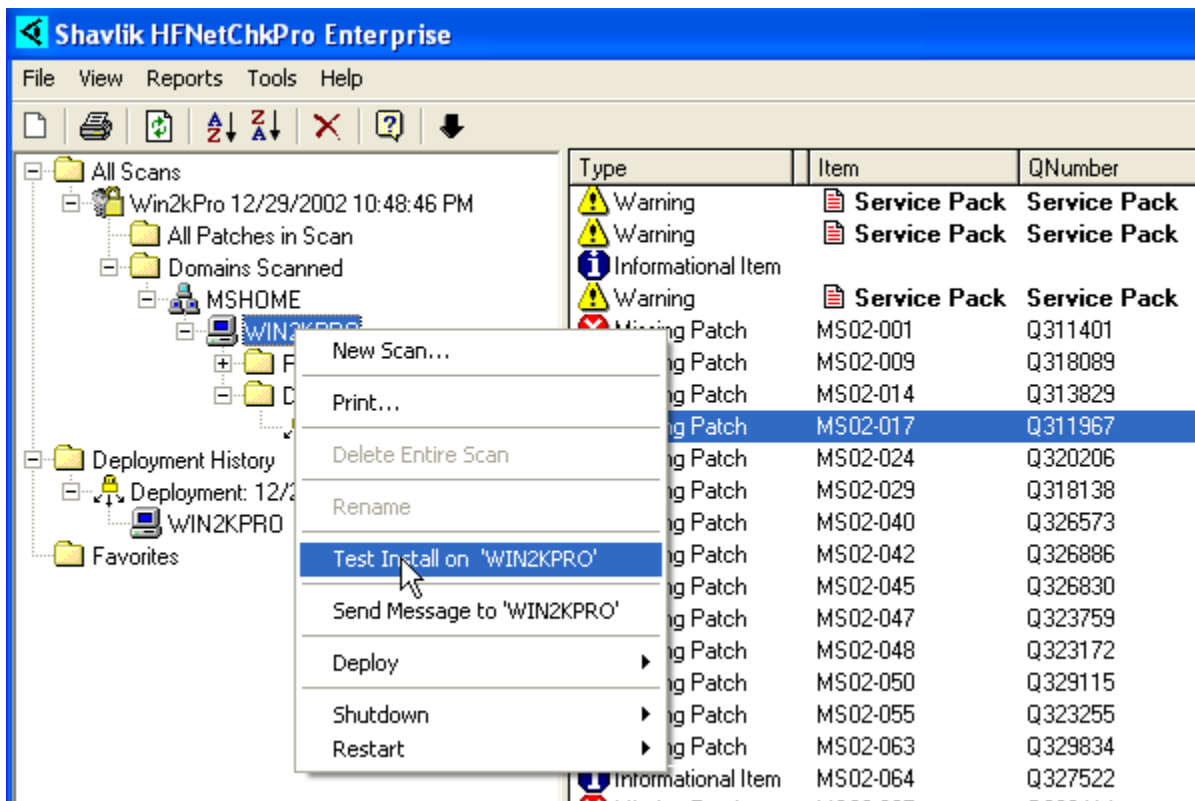
© SANS Institute 2003

11. Patch Deployment Testing

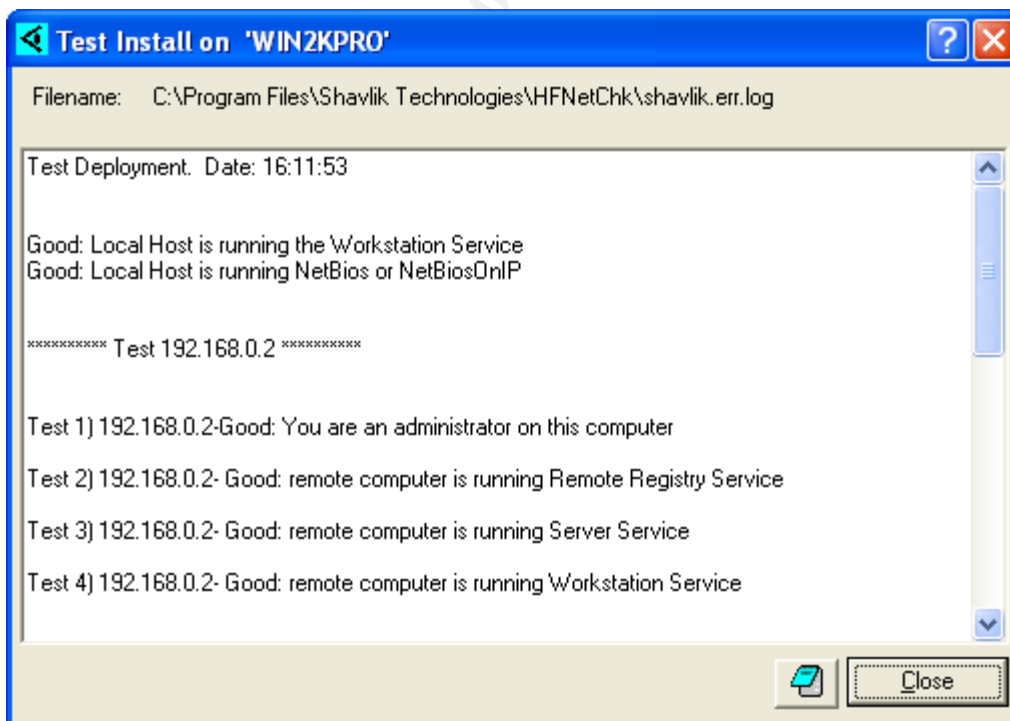
HFNetChkPro also offers Patch Deployment Testing that makes sure that the proper services are running, you have the proper security, and you are able to schedule a task on the target machine(s).

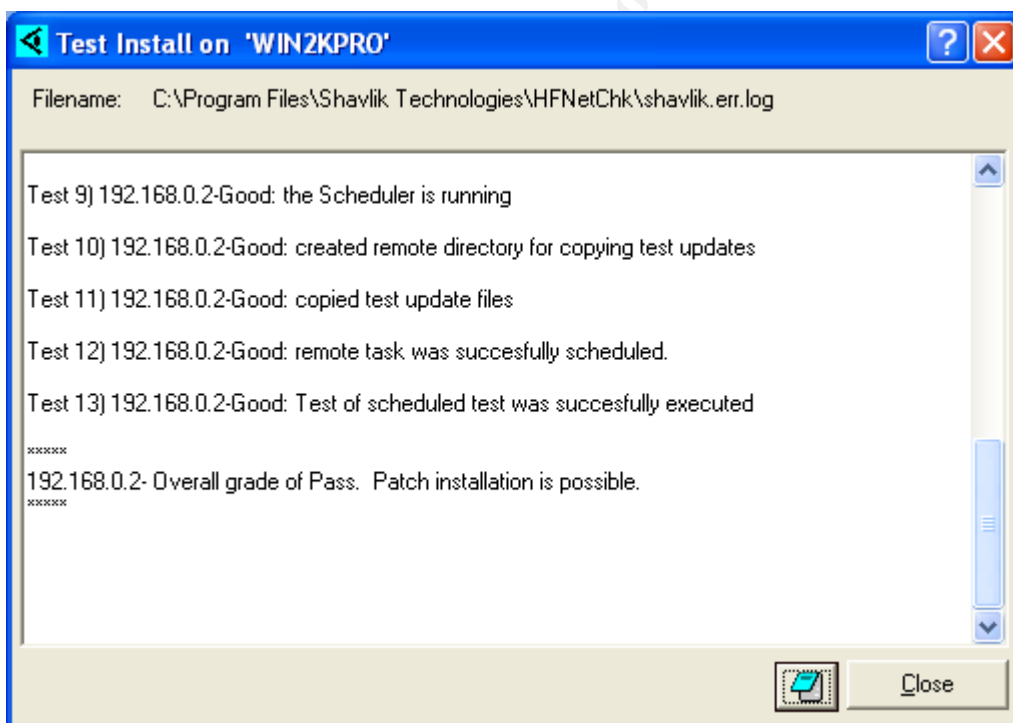
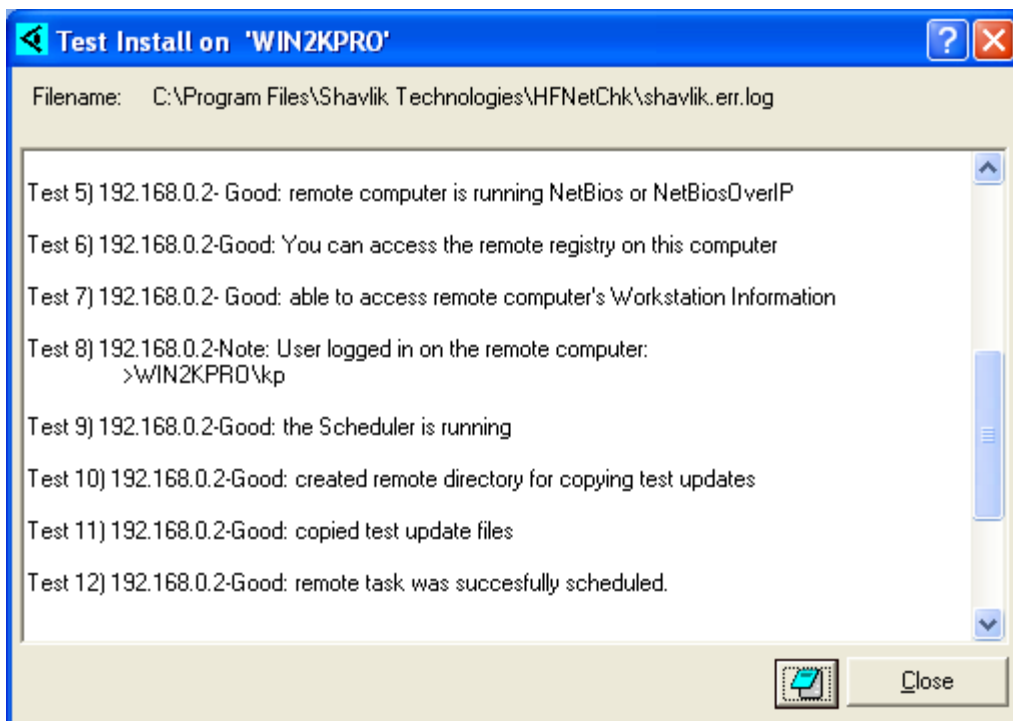
The “Test Install...” option can be found on the Tools menu or by simply performing a right-click on the target machine. The pictures below and on the following page are illustrating both methods of accessing this option:





If all requirements for the remote patch deployment are met, HFNetChkPro will display the following results:

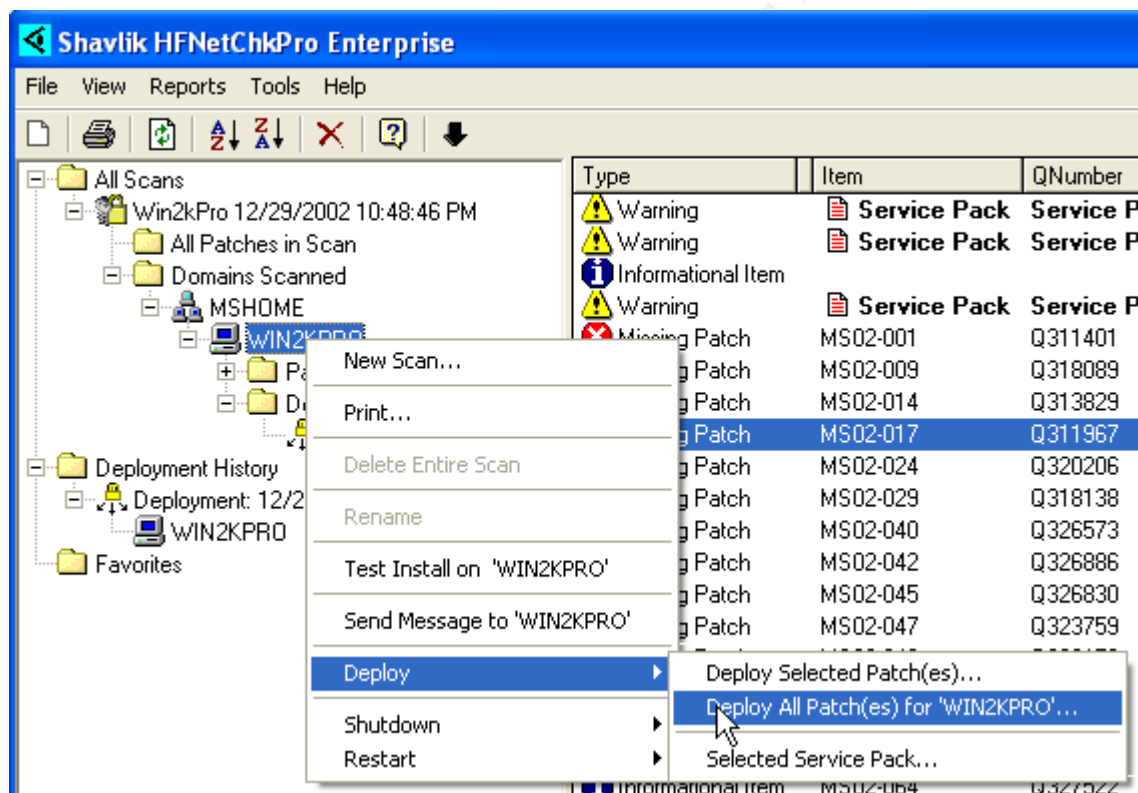




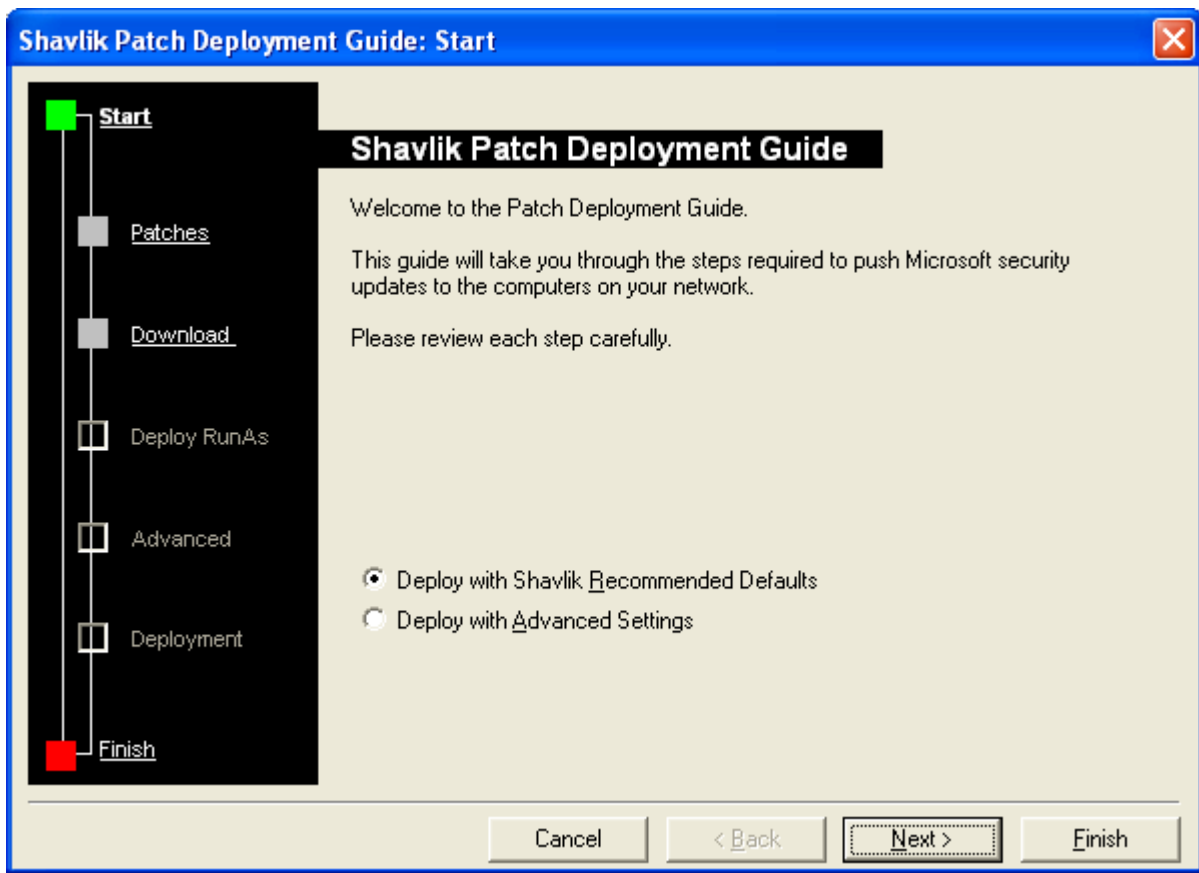
If any of the steps have failed, take necessary steps to fix them and then run the test again. Once all the steps have a status of Good, you can deploy your patches.

12. Patch Deployment Using HFNetChkPro

Using Shavlik HFNetChkPro tool for remotely deploying patches is a very simple task and it can be done just with few mouse clicks. All necessary steps are described below. In order to deploy patches remotely to a selected machine right click on the machine name (in this case WIN2KPRO) and select Deploy option. Next, you will be presented with another menu that will offer you to deploy Selected Patch(es), Deploy All Patch(es) for the selected machine or Deploy Selected Service Pack. In this example we will remotely deploy all patches to the WIN2KPRO computer which is shown on the screenshot below.

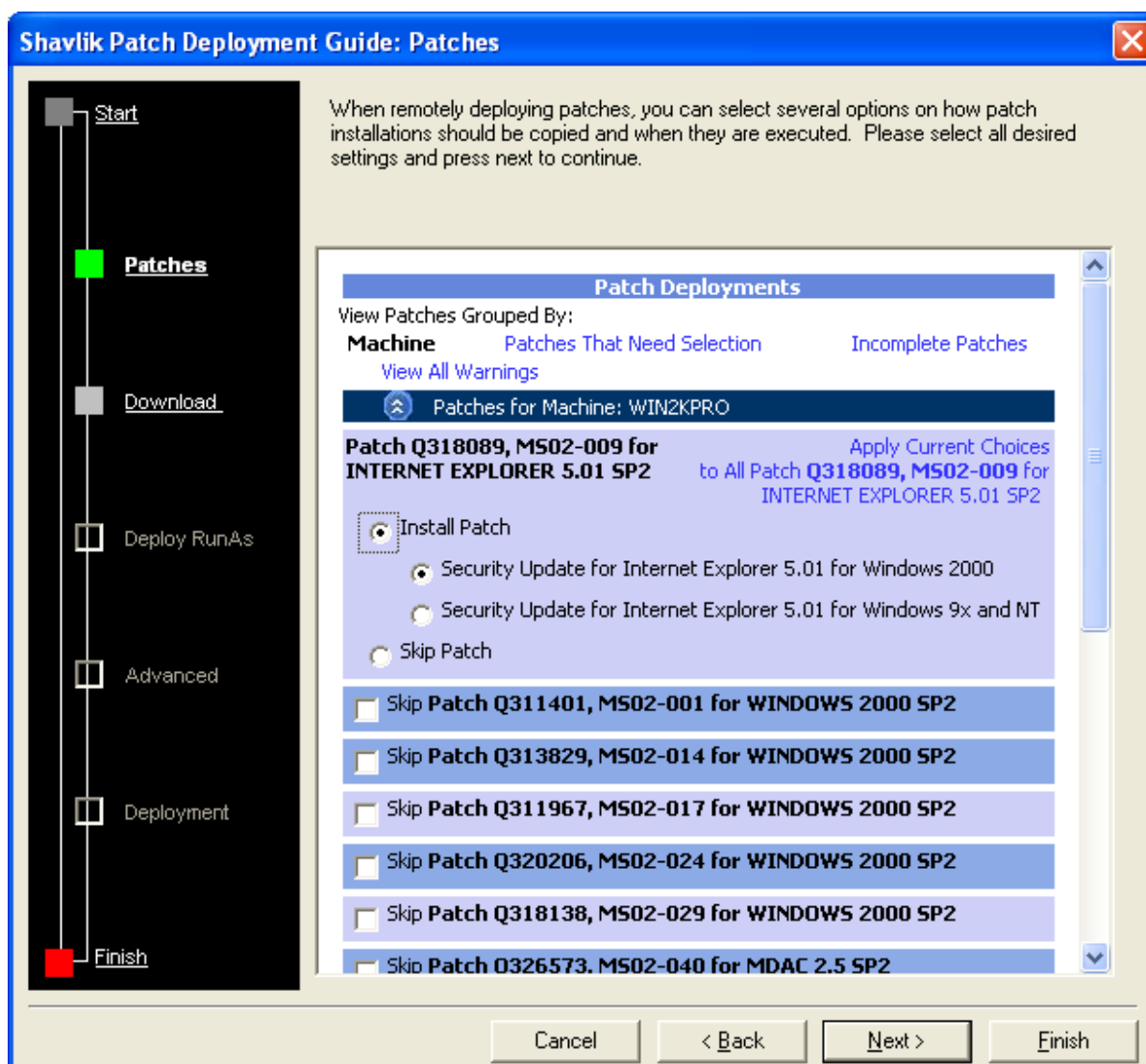


After selecting “Deploy All Patch (es) fro ‘WIN2KPRO’...” HFNetChkPro will automatically start the Shavlik Patch Deployment Guide which will guide you through the basic steps in remote patch deployment.

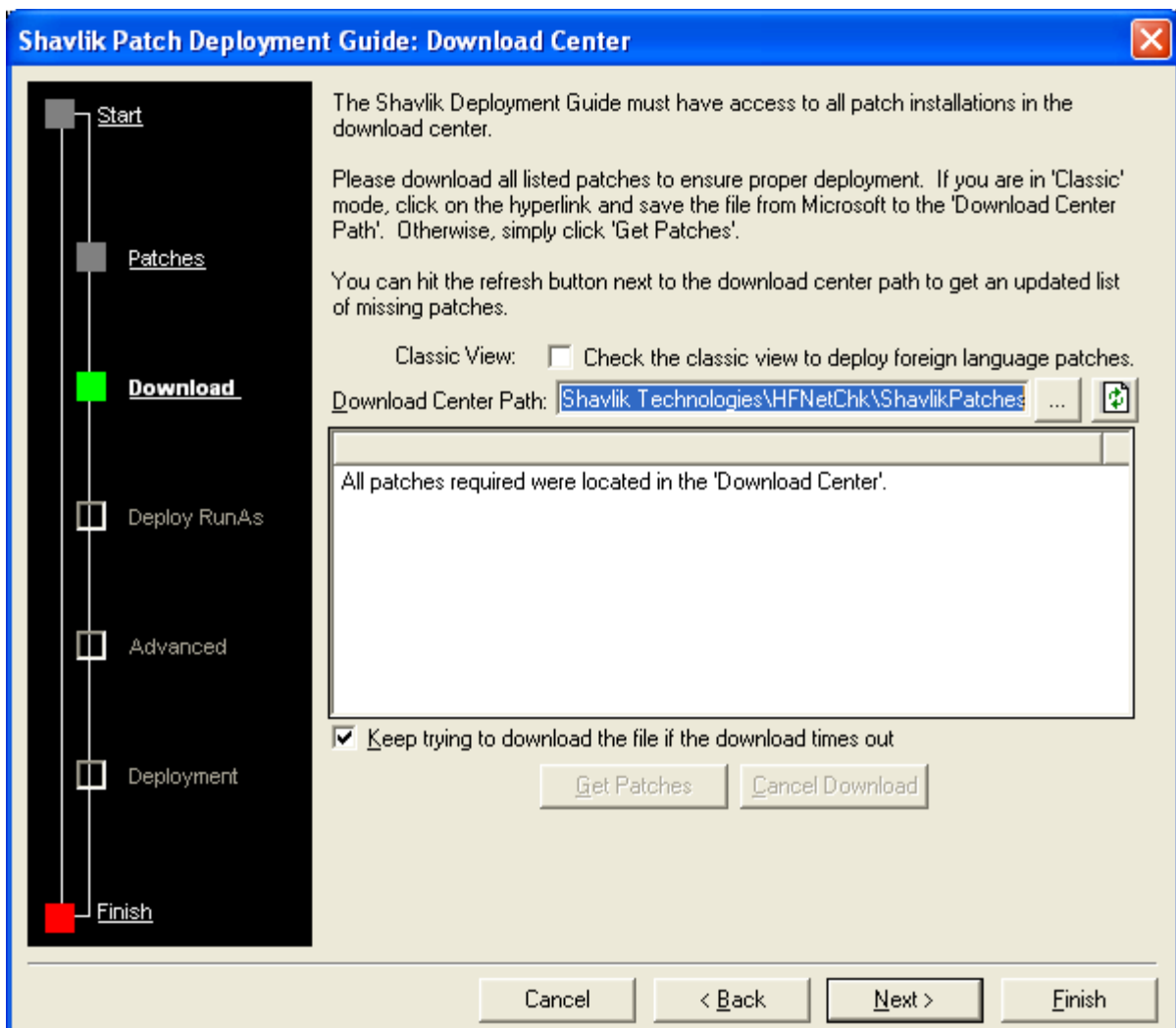


Start Screen: The Start screen offers the following two options for the patch deployment:

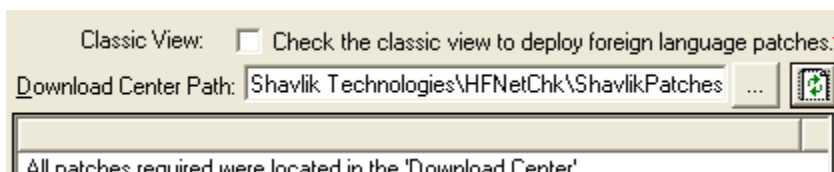
1. Deploy with Shavlik Recommended Defaults - If you pick this option, the deployment guide will automatically make some choices for you based on Shavlik recommendations. These recommendations are as follows:
 - a. Install all patches immediately
 - b. Reboot after deployment
 - c. Overwrite existing files
 - d. Do not shutdown SQL or IIS service before applying patches
 - e. Remove temporary files after deployment
 - f. Do not make backup files for uninstall
 - g. Run patch installations in quiet mode
2. Deploy with Advanced Settings - Allows network administrators to manually define all properties listed above.



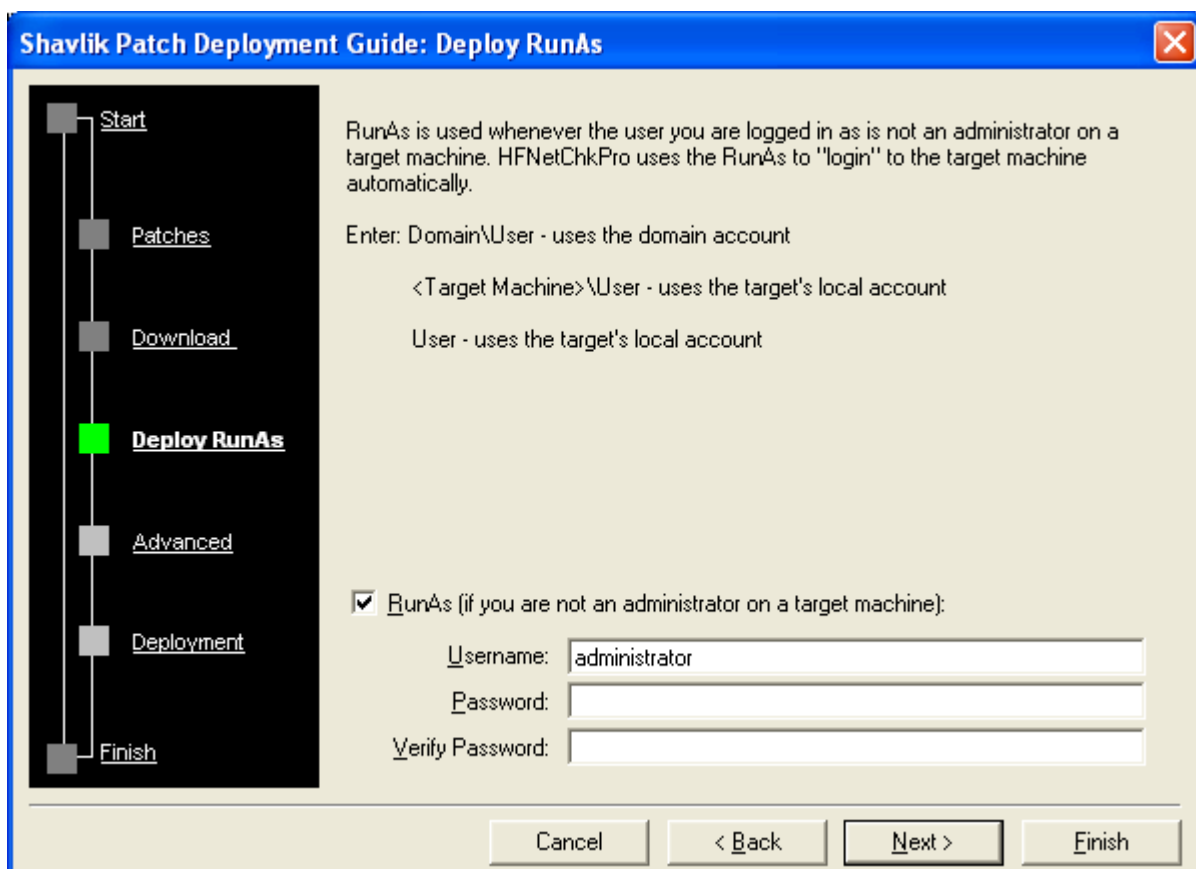
Patches Screen: During this step users will confirm/complete any choices required for patches. For the majority of cases, you will be able to ignore this step. However, for Service Packs and/or Patches that have component choices (such as the Q318089 patch listed above) you will need to make a selection before continuing. For any patch that does not have any sub components to choose from, the 'Skip' checkbox is left unchecked and by default this patch will be included in the deployment. For any patch that **does** have sub components to choose from, by default the 'Install Patch' option and the 'Skip Patch' option are both left blank so that user interaction is required.



Download Center Screen: During this step HFNetChkPro will compare the list patches to be deployed with the list of patches available via Download Center. If all necessary patches are already in Download Center the “All patches required were located in the Download Center” message will be displayed. If any of the required patches are missing in the Download Center, HFNetChkPro will list them and offer a user to download them by clicking on “Get Patches” button. After an attempt of downloading missing patches, you can confirm if they have been successfully place into the Download Center by clicking on the Refresh button shown on the picture below:



After confirming that all required patches have been successfully placed into the Download Center you can proceed with the next step by clicking on the "Next" button.



The image shows a Windows-style dialog box titled "Shavlik Patch Deployment Guide: Deploy RunAs". On the left is a vertical navigation pane with a black background and white text, listing steps: Start, Patches, Download, **Deploy RunAs** (highlighted with a green square), Advanced, Deployment, and Finish. The main area has a light beige background. It contains explanatory text about RunAs, three examples of how to enter the RunAs string, a checked checkbox for using RunAs, and three input fields for Username, Password, and Verify Password. At the bottom are four buttons: Cancel, < Back, Next >, and Finish.

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. HFNetChkPro 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: administrator

Password:

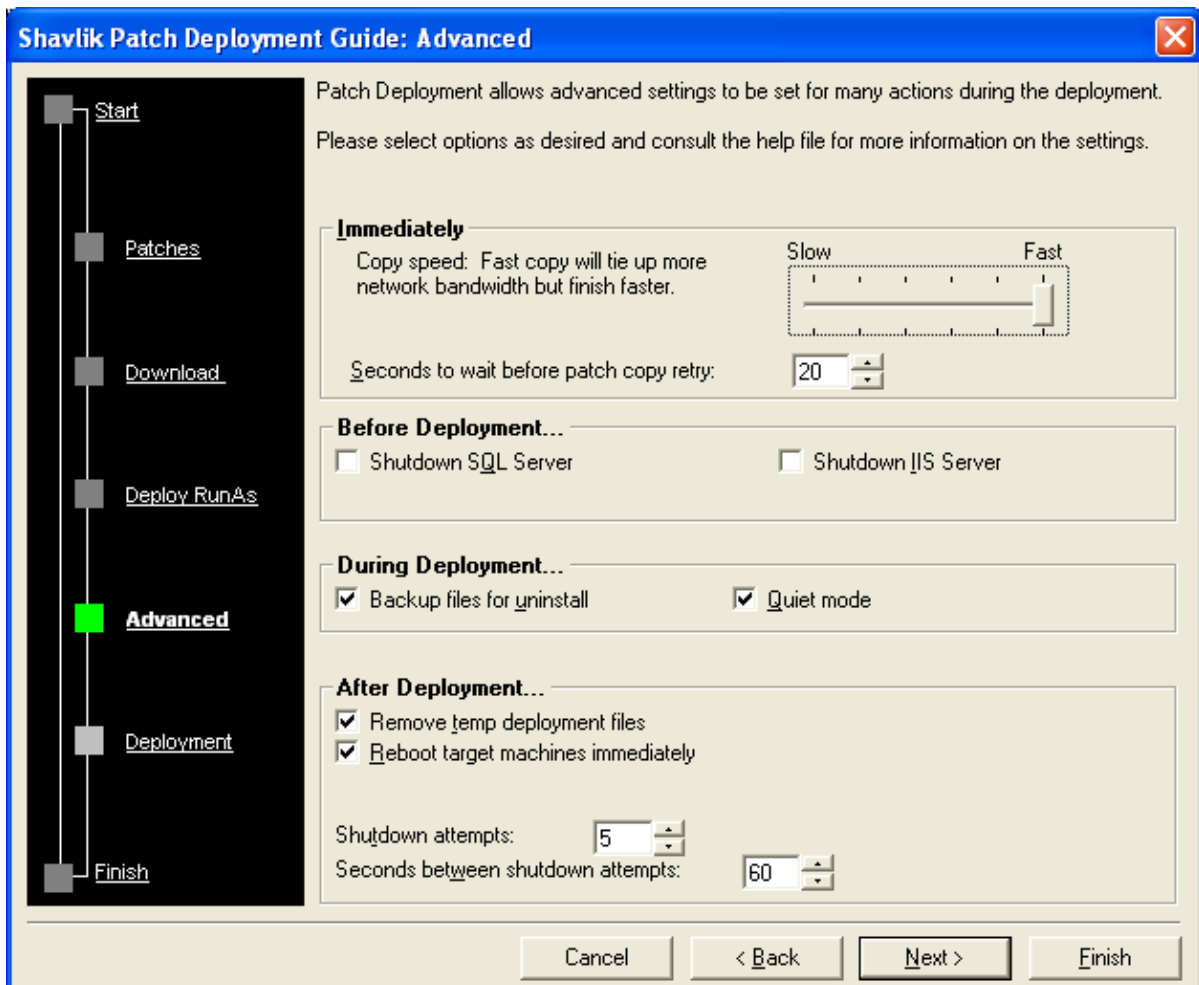
Verify Password:

Cancel < Back Next > Finish

Deploy RunAs Screen: The Shavlik HFNetChkPro uses your current logged on credentials to automatically "login" to the target machine(s) and copy and schedule the patch deployment. If the current logged in credentials do not have administrative rights on all of the target machines, you need to enter a RunAs. HFNetChkPro will use the RunAs credentials to automatically "login" into the target machines.

If you enter Domain\User, HFNetChkPro will use the domain account rights.

If you enter <Target Machine>\User or just user, HFNetChkPro will use the target's local account rights.



Advanced Screen: The next step in the guide allows the user to change options that specify to how the patch deployment should execute.

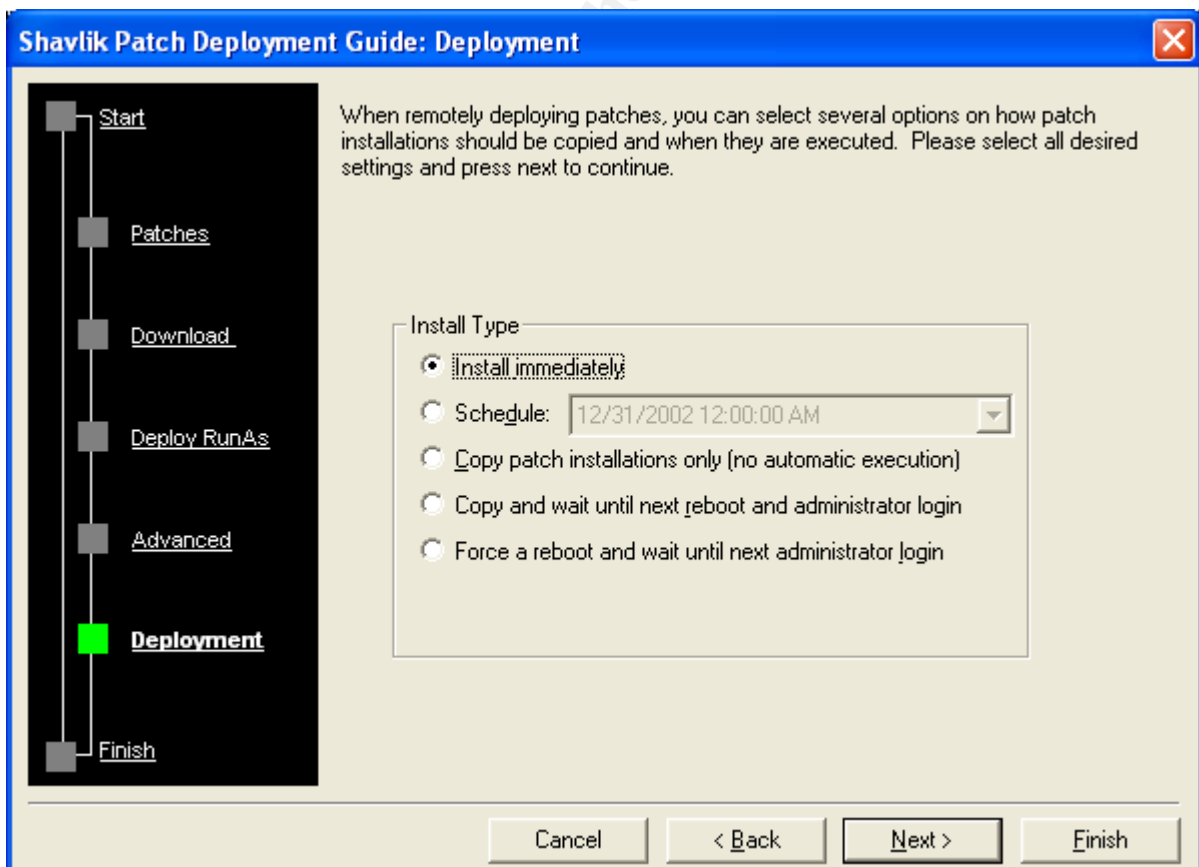
1. Copy speed - This option allows you to control the copy speed during the 'pushing' process of patches.
2. Shutdown SQL Server - If you are deploying SQL Server patches, you can specify to shutdown the SQL Server Service before deploying patches.
3. Shutdown IIS Server - If you are deploying IIS patches, you can specify to shutdown the IIS Service before deploying patches.
4. Backup files for uninstall - This option informs each Hotfix to backup files appropriately if the installation package is capable of doing such a task. If a particular hotfix is capable of backing up files for uninstall, selecting this feature will offer you an option for uninstalling it after the deployment. This is a very good feature especially when some hotfixes may cause other unforeseeable results causing a computer system to malfunction.
5. Quiet Mode - If this option is checked, all Microsoft Hotfix installations are run in unattended mode during remote deployment so that no user interaction is required on remote machines. If the Quiet mode is turned off, the installation

can display progress messages and other non-interactive messages during the install.

6. Remove temp deployment files - If this option is selected, every file used during this deployment will be removed with the exception of CommandLine.exe and Qchain.exe since they could be used in other deployments, if more than one was scheduled or executing them at the same time.
7. Reboot target machines deployment - All reboots on Microsoft Hotfixes are suppressed so that several Hotfixes can be applied at once. This option instructs the remote deployment of whether or not it should reboot the computer when finished.

Note: It is strongly recommends rebooting the computer after a remote deployment to ensure that all patches are successfully applied.

8. Number of shutdown attempts - If a shutdown fails for any reason, this will instruct the program to retry the specified number of times.
9. Number of seconds to wait between shutdown attempts - If multiple shutdown attempts are required, this value specifies how long to wait between each attempt.

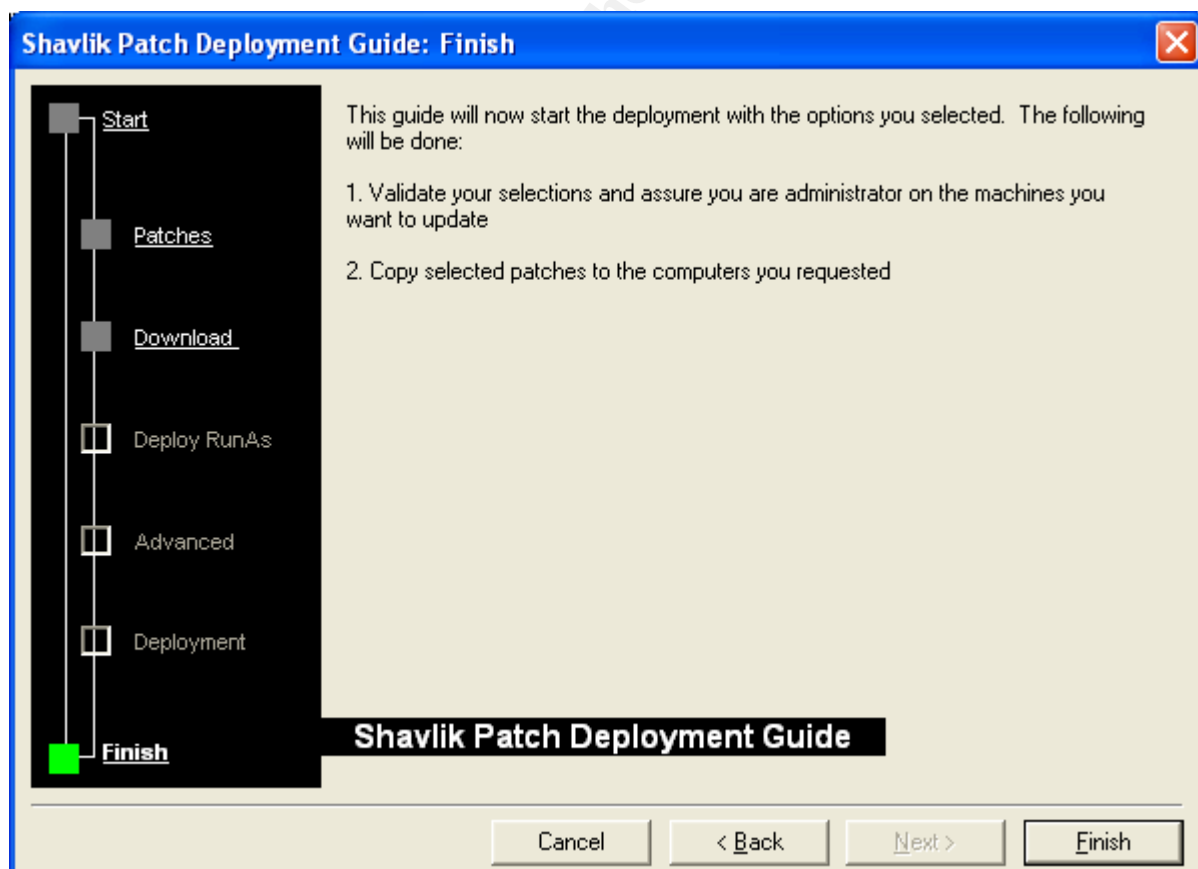


Deployment Screen: The next step in the Patch Deployment is the Install Type. HFNetChkPro offers several options for installing patches. Selected patches can be installed immediately or be scheduled for a specific day and time. The scheduling option is especially valuable when it comes to computer systems that cannot be disrupted during the business hours.

The “Copy patch installations only (no automatic execution)” option provides network administrators with ability to transfer all patches, QChain.exe and the batch file created by the Deployment Guide (Wizard) to a target machine with no execution. The installation can be then performed manually at any convenient time.

The “Copy and wait until next reboot and administrator login” option is very similar to the previous option except the patch deployment execution will be performed after someone reboots the machine first and logs into it with administrative privileges.

The “Force a reboot and wait until next administrator login” option copies over all patches and dependent files and forces the machine to reboot (there will be a 60 second warning for any user sitting at the machine). After the reboot occurs, the deployment will begin as soon as an administrator logs into the system.



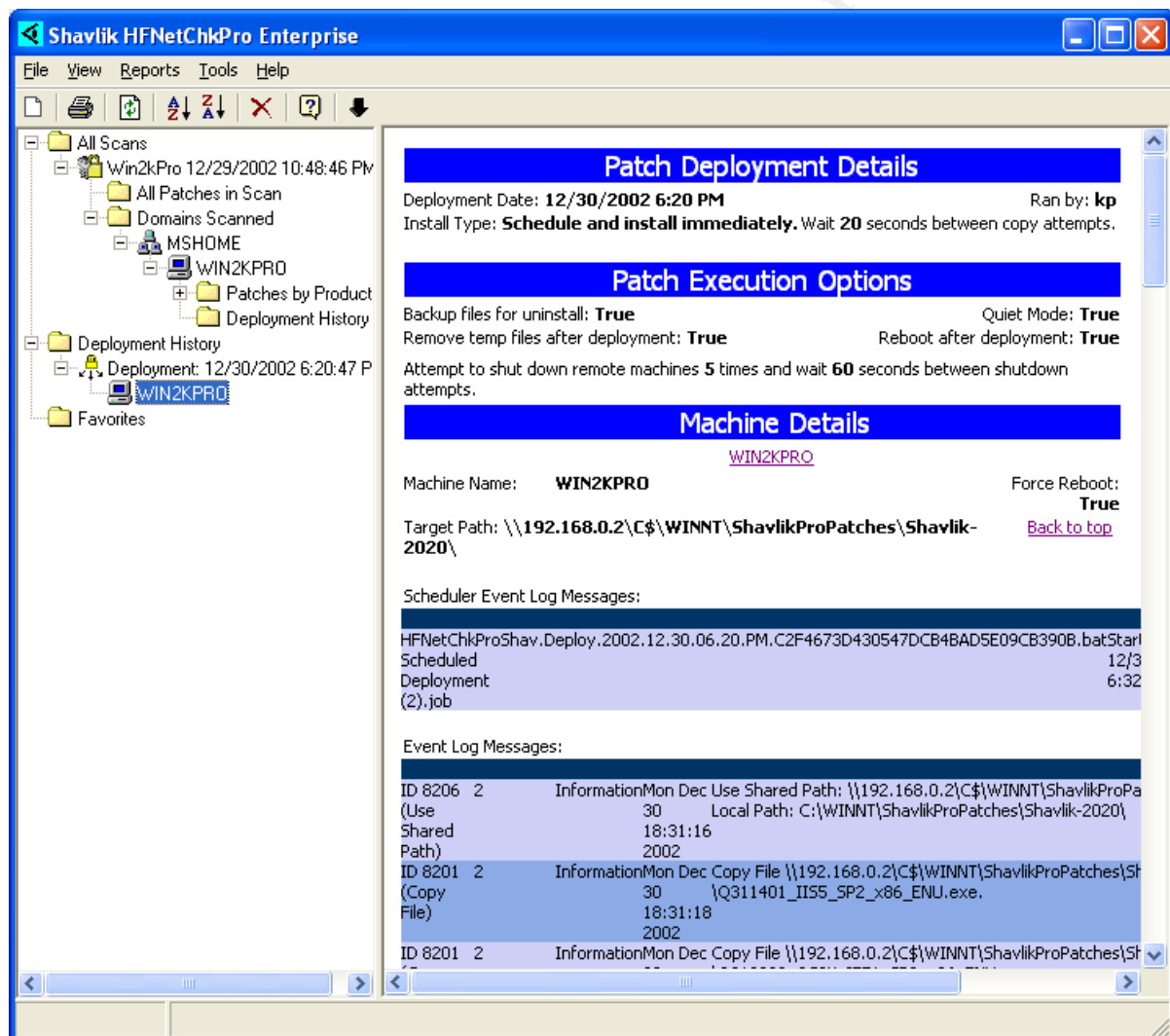
Finish Screen: This is your last chance to review the patch installation options. If any of the settings still need to be changed, it can be done by navigating to an appropriate screen by pressing the “Back” or “Next” buttons. If everything seems to be configured correctly, press the “Finish” button to execute the patch deployment.

HFNetChkPro will copy all files over to target machines and run the created batch files based on the installation type option selected. During the copy process, several events are logged to the application log on the target machine. This information can be viewed in the patch Deployment History (shown below in the next section), however the application log should be configured to allow older log entries to be automatically purged so that no errors occur if the event log should become full.

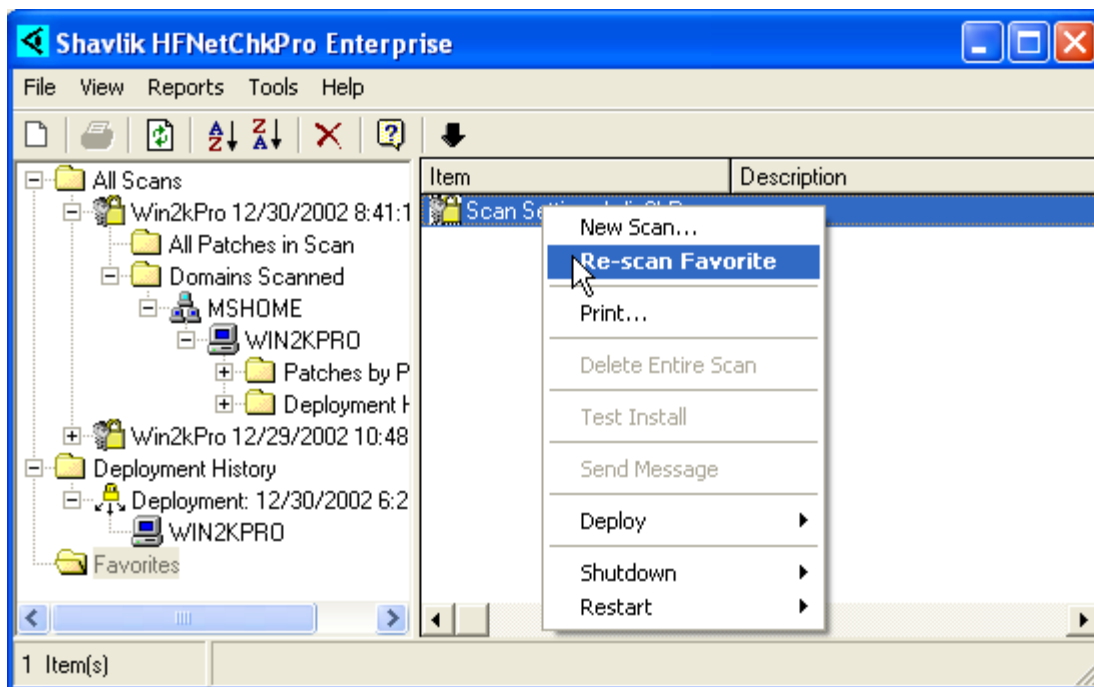
© SANS Institute 2003, Author retains full rights

13. Patch Deployment Verification Using HFNetChkPro

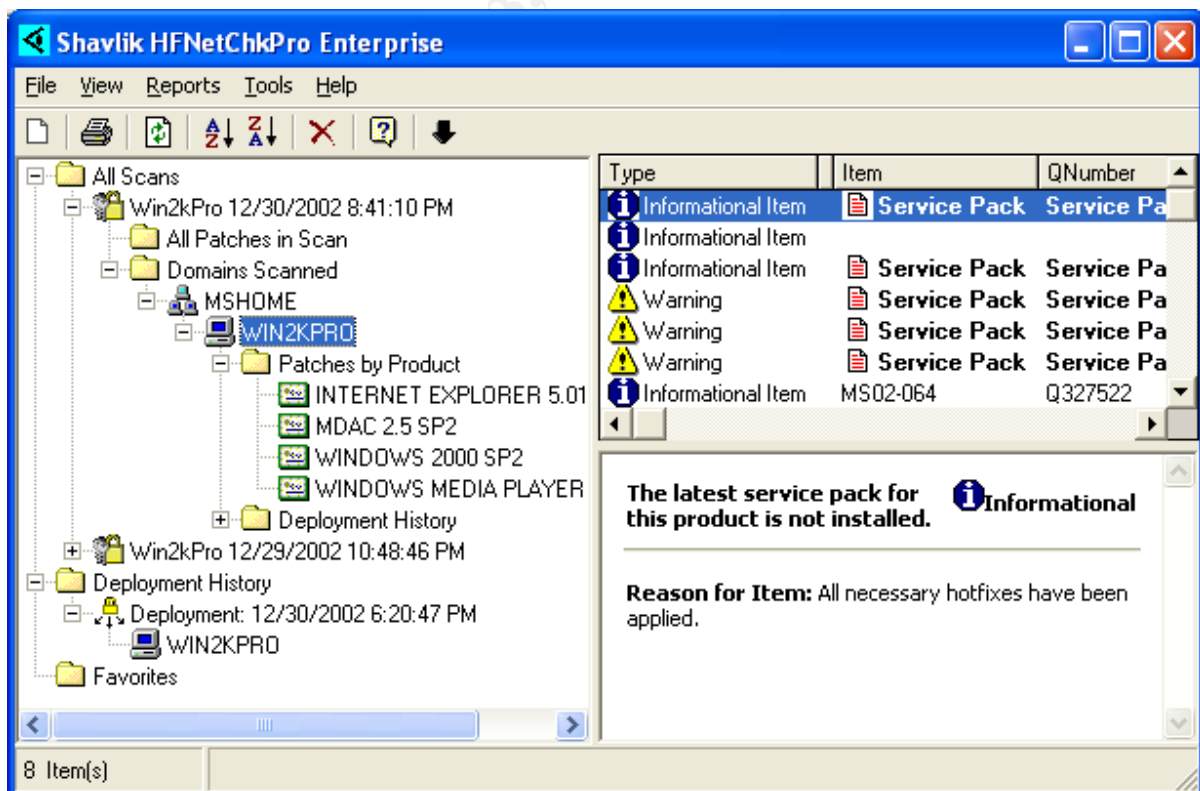
It's a good practice to verify that all planned to deploy patches have been actually successfully installed on a target machines or a group of machines. HFNetChkPro provides an excellent facility to accomplish this task. Simply, expand the Deployment History tree and double-click on the target machine. All the information about a particular deployment including Patch Deployment Details, Execution Options, Machine Details, Scheduler Event Log Messages and Event Log Messages will be displayed in the right pane.



Another recommended method of verifying that a patch deployment has been successfully completed is to re-run the scan. In order to use this option the scan needs to be first saved in the Favorites. This can be accomplished when defining scan settings using HFNetChkPro Scanning Guide (Wizard). The following screen illustrates how to re-scan a machine:



The results of the new scan will be stored under All Scans tree located in the left pane of the HFNetChkPro main screen. The following screenshot represents the results of the another re-scan performed on WIN2KPRO computer system after deploying all missing patches identified during the initial scan.

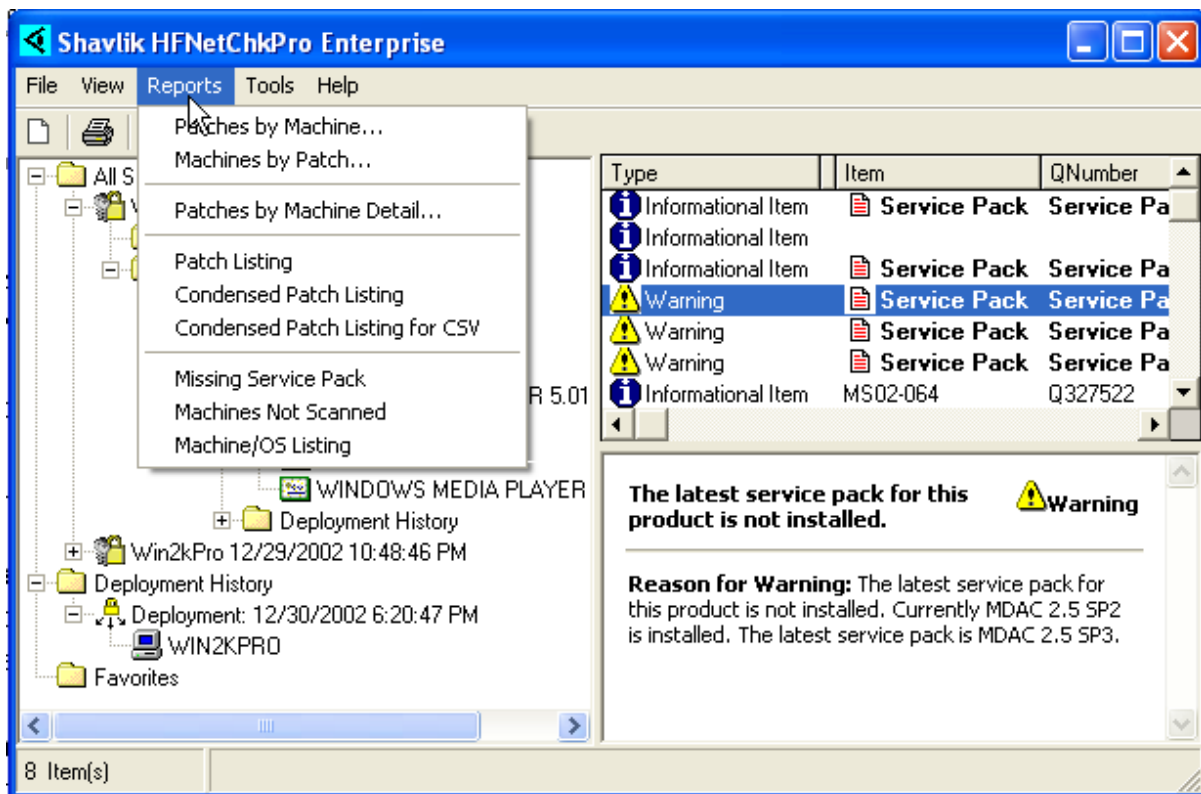


As you can see, all the critical items about the missing patches identified after the initial scan have disappeared and the only items that are left are the informational and warning messages about the latest service packs that have not been installed yet for different products.

© SANS Institute 2003, Author retains full rights.

14. Reporting

One of the strengths of HFNetChkPro is its reporting capabilities. Several reports can be accessed via Reports menu located on the main menu bar. The screenshot below shows variety of reports available within the software:



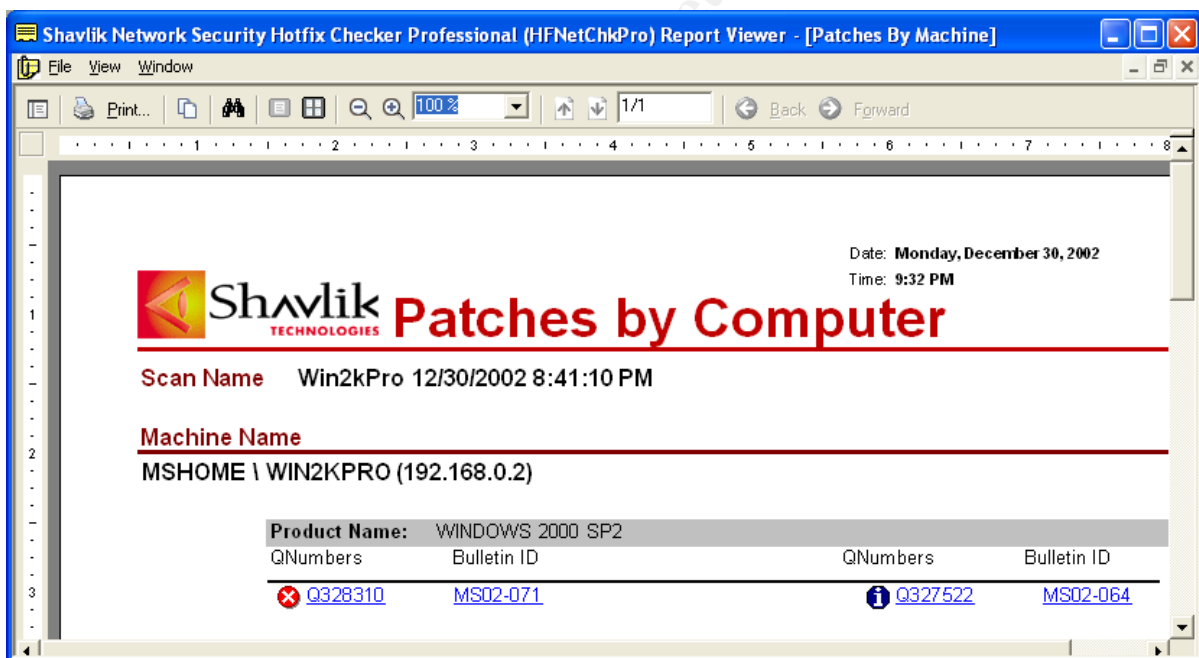
Currently, HFNetChkPro has the following reports:

- **Patches by Machine** - Listing report that displays all patch information grouped by Machine Name.
- **Machines by Patch** - Listing report that displays all patch information grouped by Patch BulletinID and QNumber.
- **Patches by Machine Detail** - A detailed listing of every patch found grouped by Machine Name. For each patch, the entire summary and reason is listed in the report. Note that this report can take very long if ran against 1000's of computers.
- **Patch Listing** - A concise listing (one line per patch processed) of all patches for all scanned machines sorted by 'Missing', 'Found', and 'Informational' and 'Warning' first, then sorted by user preferences.
- **Condensed Patch Listing** - This report is designed to fit as much data on the page as possible. The report is grouped by machine and if many

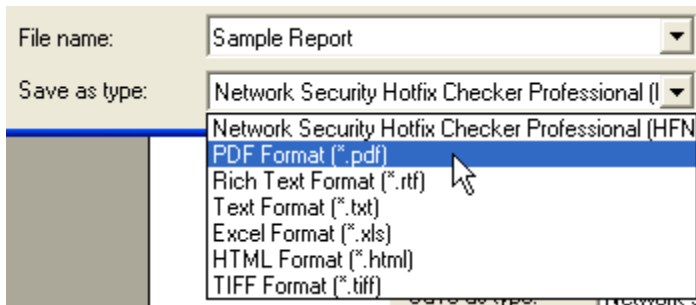
machines are processed and you want a listing of every patch for each machine, this report will contain minimal amount of pages.

- **Condensed Patch Listing for CSV** - This report is designed to output data in optimum format if the user wants to do a CSV export. The output is a simple text listing where each patch is on a single line. Instead of showing icons stating the status of the patch, the initials M, F, I, and W are used meaning Missing, Found, Information, and Warning respectively.
- **Missing Service Packs** - This report is a quick overview of all machines that are missing service packs for supported products. This report skips the simple criteria filter and displays the advanced criteria filter immediately. These filtering options will be explained below.
- **Machines Not Scanned** - This report lists out all machines not scanned and the reason they were not scanned
- **Machine/OS Listing** - This report lists out all operating systems for the machine(s) scanned.

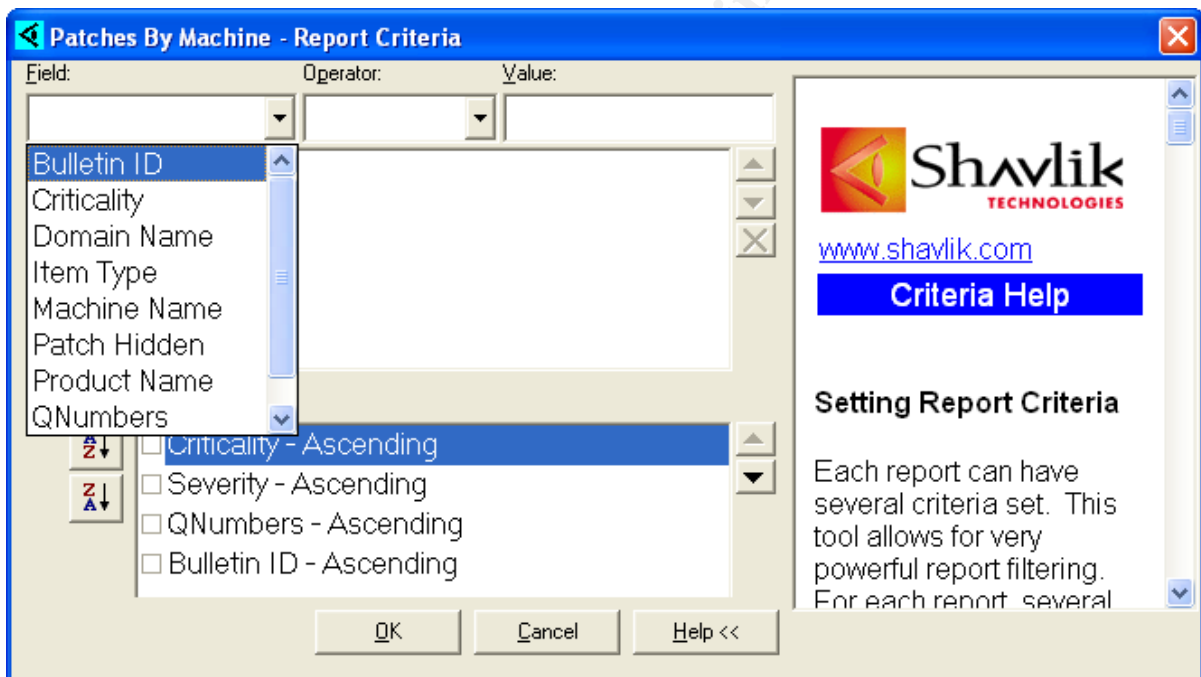
A sample report of Patches by Machine (Computer) is shown below:



For a future reference all reports can be saved as a file using the following available file formats:



The Shavlik Technologies Network Security Hotfix Checker reporting interface was designed to provide the user with wide range of filtering possibilities. The reporting features make the Shavlik tool very powerful, however, in addition to the standard report criteria, the tool provides offers options for advanced filtering, allowing users to create any reports they desire. Some advanced filtering options are shown on the screen below:



Below is the list of operators that HFNetChkPro supports under the advanced filtering options:

1. (=) Means that the field must exactly match the text in 'Value'.
2. (<>) Means that the field must NOT equal the text in 'Value'.
3. (IN) Means that the user will provide a ',' delimited list of values and the field must exactly match one of the text elements in 'Value'.
4. (NOT IN) Means that the user will provide a ',' delimited list of values and the field must NOT equal one of the text elements in 'Value'.
5. (NULL) Means that the field must be NULL in the database.
6. (NOT NULL) Means that the field must *not* be NULL in the database.

7. (>), (<), (<=), (>=) Means 'Greater Than', 'Less Than', 'Less Than or Equal To', and 'Greater Than or Equal To' respectively. A numeric comparison (value based) or alpha comparison (alphabetically) will be performed to filter out values.
8. (LIKE) Means that the field must match the wildcard specifications provided. % means match anything and any length and '_' means match anything but only the length specified by the number of '_' characters. For more information, see SQL Server Books Online and review 'LIKE' in 'SELECT' statements.
9. (IS BLANK), (IS NOT BLANK) Means that a text field either contains an empty string value or does not contain an empty string.

© SANS Institute 2003, Author retains full rights.

15. Summary

HFNetChkPro is a great tool to help you manage the patch status and security of the systems in your enterprise. HFNetChkPro provides several advantages over the freely distributed Microsoft command-line version HFNetChk. Its graphical user interface is very intuitive, self explanatory, and easy to navigate. HFNetChkPro allows administrators not only to scan systems or groups of systems to check for up-to-date and improperly configured security patches and service packs but also provides an extensive list of options for pushing them out to the machines that need them, or scheduling them for later downloading and patching. Using HFNetChkPro multiple patches can be applied to the same system with only one reboot. The tool provides excellent facilities for downloading new or needed patches into a central and hopefully well secured repository on the enterprise network. Once downloaded, patches and service packs are stored in the HFNetChkPro download center, there is no need for repeating this usually time consuming step over and over again. The new version of HFNetChkPro provides network and security administrators the ability to check the readiness of computer systems for remote patch installation. That gives an opportunity to correct any already existing issues prior to applying actual patches or service packs and ensures future successful deployment. HFNetChkPro also delivers options for patch deployment verification as well as extensive reporting features that are especially valuable when dealing with large enterprise class networks. The new version also comes equipped with a patch installation database that includes information on and descriptions of patches from Microsoft, as well as verification that the patches being downloaded are actually coming from Microsoft. In addition, it allows the scanner to execute an "Anti-spoof Scan" which is a detailed binary analysis of each file for each patch to assure that no one has tried to "fake" a file on your network.

You can try a free version of this tool HFNetChkLT which can be downloaded from Shavlik Technologies corporate web site by going to the following link <http://www.shavlik.com/pHFNetChkLT.aspx>. HFNetChkLT is the fully functional version of HFNetChkPro. HFNetChkLT offers unlimited scanning, a complete GUI, and Shavlik's exclusive PatchPush™ capabilities. No keys and no timeouts required so you can use this useful tool all you like.

16. References

The Twenty Most Critical Internet Security Vulnerabilities (Updated)

<http://www.sans.org/top20/>

Shavlik Technologies

<http://shavlik.com/>

Shavlik Technologies HFNetChkLT

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

Best Practices for Applying Service Packs, Hotfixes and Security Patches

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpsp.asp>

Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available

Microsoft Knowledge Base Article - 303215

<http://support.microsoft.com/default.aspx?scid=KB;en-us;q303215>

Shavlik eases Microsoft patch management

By Sam Costello

<http://www.nwfusion.com/news/2002/0724shavlik.html>

Shavlik eases Microsoft patch management

By Sam Costello

http://www.idg.net/ic_897716_5055_1-2793.html

Patch Management Done Right by *Tim Mullen* May 06, 2002

<http://online.securityfocus.com/columnists/79>

Microsoft Users Tired of Patch Management Headaches by John Fontana

http://www.nwfusion.com/news/2002/131957_04-22-2002.html

Perfect Patch Management Requires a Patchwork of Vendors

<http://www.computerworld.com/securitytopics/security/story/0%2C10801%2C72632%2C00.html>

Microsoft Users Tired of Patch Management Headaches by John Fontana

http://www.nwfusion.com/news/2002/131957_04-22-2002.html

Microsoft Security and Privacy

<http://www.microsoft.com/security/>

Microsoft HotFix & Security Bulletin Service

<http://www.microsoft.com/technet/security/current.asp>

Computing Safely, Securing Your Systems From The Inside Out

Using Shavlik Technologies solutions created for Microsoft and Microsoft customers Version 2.0