Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Remote Scanning Utilities for Microsoft Hot Fixes and Service Packs

The purpose of this paper is to show how security administration can benefit by the use of six utilities for remote scanning for Microsoft hot fixes and service packs on multiple Windows systems (NT, 2000, XP, IIS 4 and 5, SQL Server 7.0 and 2000, Exchange 5.5 and 2000, Windows Terminal Server, and Windows XP Home Edition). These six utilities are: Baseline Security Analyzer Tool 1.0, HFNetChk (Network Security Hot Fix Checker Tool) Both version 3.32 from Microsoft and version 3.83 from Shavlik Technologies, HFNetChkLT...

Copyright SANS Institute

Author Retains Full Rights

AD

Remote Scanning Utilities for Microsoft Hot Fixes and Service Packs

Larry Nicholl
September 25, 2002

Overview

This paper was written to complete requirements for GIAC GSEC certification.
The purpose of this paper is to show how security administration can benefit by the use of six utilities for remote scanning for Microsoft hot fixes and service packs on multiple Windows systems (NT, 2000, XP, IIS 4 and 5, SQL Server 7.0 and 2000, Exchange 5.5 and 2000, Windows Terminal Server, and Windows XP Home Edition).
These six utilities are:
Free products:

- Baseline Security Analyzer Tool 1.0 from Microsoft
- HFNetChk (Network Security Hot Fix Checker Tool)
  Both version 3.32 from Microsoft
  and version 3.83 from Shavlik Technologies
- HFNetChkLT 3.8.96 from Shavlik Technologies

Commercial products:

- HFNetChkPro 3.8 (Shavlik Network Security Hotfix Checker) from Shavlik Technologies
- UpdateEXPERT 3.2 from St. Bernard Software
- LANguard Network Security Scanner 3.0 from GFI

This paper's discussion will illustrate the advantages and disadvantages of each of the six remote scanning tools by using a comparison of the tools. This discussion will consist of two sections. The first section will focus on the first three free tools as regards remote scanning for Microsoft hotfixes and service packs (SPs), while the second section will focus on the four tools that have two common functions: one – remote scanning for hotfixes and SPs, and two – patch pushing. Although patch pushing or deployment is a very important subject, a discussion of patch pushing in extensive detail is beyond the scope of this paper. The first three tools are free with unlimited use, whereas the three commercial tools are not free. The primary purpose of this paper is to compare and discuss these six tools as regards their primary and common ability: to perform a remote scan to collect information about Microsoft hotfixes and service packs on multiple Windows systems (NT, 2000, XP, IIS 4 and 5, SQL Server 7.0 and 2000, Exchange 5.5 and 2000, Windows Terminal Server, and Windows XP Home Edition).

Introduction

One of the most important tasks in the prevention of intrusions to Windows systems is for a Windows systems security administrator to ensure that each Windows system has the latest Microsoft security patches installed. For administrators of a medium to large number of Windows systems (NT, 2000, XP, IIS 4 and 5, SQL Server 7.0 and 2000, Exchange 5.5 and 2000, Windows Terminal Server, and Windows XP Home Edition), any tool that makes this task easier and faster is likely to be a welcome tool. Additionally, keeping the expense low in both labor and money is a prime motivation for many businesses especially if there are tools

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

that are available for free. Granted, if the tool is free, there usually is more labor involved by the administrator due to the lack of capability of the tool.

The author decided to review tools regardless of their price for one main reason: to report on the main differences and advantages of each product.

The author searched the Internet for utilities that could provide at least a minimum of desirable features in a remote scanning tool. The three free tools found were installed, tested, and reviewed. Of the three commercial (not free) tools found, two of these (UpdateEXPERT 3.2, and LANguard NSS 3.0) were also tested using their evaluation trial versions. The product not tested (using trial software) was HFNetChkPro, which was in effect tested via its free version (LT version: HFNetChkLT 3.8.96). A discussion of these six tool's pros and cons is intended to show how security administration can benefit by the use of these utilities for remote auditing of hot fixes and service packs on multiple Windows systems.

Microsoft methods for patch management

The current methods that Microsoft has provided for security patch management (auditing and deployment) are not as adequate and automated as this huge task could be.
These methods include several steps that should be done in order.
The current Patch Process involves these 4 steps:

1. New Patch Notification
2. Host and Network Assessment
3. Deployment
4. Validation [1]

The New Patch Notification step includes 4 automated methods for notification of administrators and users that new patches are available for download and installation.

- Security Bulletin Notification Service
- Windows Update
- Client Update Notification Applet
- Microsoft Baseline Security Analyzer – via batch script using MBSACLI.exe.
- HFNetChk – via a batch script if scheduled to run as a batch job regularly

The Host and Network Assessment step includes several manual methods for patch assessment or audit. These are:

- Microsoft Baseline Security Analyzer
- HFNetChk
- Windows Update
- Third party tools

The Deployment step includes several methods some of which can be automated and others are best done manually. These are:

- System Management Server (SMS)
- Active Directory / Group Policy such as via Corporate Windows Update or an MSI package

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Third party tools

The Validation step is a post-patch deployment audit to verify that the deployed patches were actually installed, although the Deployment tool may have logged the installs. Several tools for validating patch deployment include:

- Microsoft Baseline Security Analyzer
- HFNetChk
- Third party tools [1]

These 4 steps of the Patch Process include at least two audits of the same systems, in the second step, Host and Network Assessment, and the fourth step, Validation. These two audits are pre and post patch deployment audits. In the first step, New Patch Notification, a baseline audit or a spot check audit could be done periodically to determine a general level of security patch compliance. In the interest of saving time in performing these audits, as well as the patch deployment, any task that can be performed remotely is typically worthwhile. Performing the audits and patch updates locally on the console is a much more laborious and tedious task. Most auditors and patch administrators would prefer to do theses task remotely provided there is adequate planning and implementation to avoid patching servers with an unapproved patch or rebooting servers without approval. Performing the tasks remotely will maximize efficiencies.

A Microsoft overview of security auditing and patching, including details about two of the tools reviewed in this paper, HFNetChkPro and HFNetChk, was presented by Eric Schultze (then of Microsoft; now of Shavlik Technologies) at a Blackhat conference called "How To Keep Up With Security Patches". The presentation is worth viewing and can be found at:
http://www.blackhat.com/presentations/win-usa-02/schultze-winsec02.ppt [1]

What is a vulnerability scan?
A vulnerability scan is most often a *remotely* administered audit of multiple systems, such as an entire IP address range, or an entire domain, or a list of systems with the intent to map or audit vulnerabilities. It could also be referred to as a remote mass audit, an audit scan or simply just a scan. Such a remote scan from one workstation is much more desirable than the opposite, a local audit of each system from each system's console. The scan administrator can reduce labor costs and increase efficiency by performing a scan from one system, typically a workstation if performed manually, or better from a server, if performed via scheduled scans. The audit results can be stored as reports in one secured location in a format that can be more easily reviewed. The audit results can then be used in a planned approach based on certain guidelines that should be followed before applying certain hot fixes and service packs. As this discussion will be focused more on the remote scan task rather than the patch deployment task, these patch deployment guidelines will not be discussed. However, as regards a remote scan (audit for patches), there are many considerations that must be considered in performing a remote scan. Some of the most important are:

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Access:

Can the scan access the remote systems through routers, firewalls, across domains?

File and Share Permission:

Will file and share permissions allow access to a remote scan with sufficient privilege?

Explicit Manager Approval:

Does the scan administrator have explicit manager approval to do a remote scan on the prospective target systems?

Scan Results Secured

Are the scan results secured to prevent unauthorized access?

The scope of this paper, however, does not include an extensive discussion of the necessary precautions and safeguards in the administration of a remote scan. This paper will be focused on a review and comparison of the technology, and not the strategy and policy, of using tools for auditing Microsoft hotfixes and SPs.

Why there is a need for *only* a remote (patch) vulnerability scan or audit?

In many large companies, there is a need to perform ***only*** a remote patch audit that is not also accompanied by a subsequent remote patch deployment ***by the same audit team.*** At least three examples provided describe how only an audit without a patch deployment is sometimes required by company policy.

Audits can be done for at least four different reasons with varied levels of thoroughness, for example:

a) Baseline audit
b) Spot check audit
c) Complete pre-patch deployment audit
d) Complete post-patch deployment audit

A **baseline audit** would be used to measure the absolute minimum level of compliance. A **spot check audit** would be used to quickly demonstrate what the general level of compliance is within a certain department. A **complete pre-patch deployment audit** would be used to determine exactly what patches are missing and need to be applied, and to map vulnerabilities. A final and **complete post-patch deployment audit** is most useful to verify compliance to company security policy. Additionally, repeated audits may be required to maintain consistent level of audit frequency.

Example one: An internal corporate-wide security compliance team is mandated by company security policy to perform information security audits of computer systems. Such audits are used to measure at a minimum, or ensure at a maximum that compliance to information security compliance policies has been met within certain critical departments, such as Finance, or Human Resources, etc or throughout the enterprise.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Example two: An external security audit team may be contracted to provide any level of security audits for a company. This is certainly a team that has no business deploying patches to any internal computers. The only job is to perform an audit.

Example three: An intra-department team, such as an internal Finance team, may be mandated to provide audits of their Finance computers as an extra measure of assurance that the IT department that manages their computers has thoroughly patched the machines.

A remote audit is most certainly an actual need and often a requirement especially in large enterprises.

Why look at free or low-cost audit tools?
Performing the scans with the least amount of resources (labor, time, money) is usually the desired goal. By looking only at free or low-cost tools for audit scans, the attempt at finding a satisfactory tool for the job may be successful. If the use of a free tool can meet or even surpass the requirement for an audit scan tool, then that would be worth the time of reading this paper. Keeping the expense of an audit to a minimum is one of the secondary aims of this paper. Although it is highly likely that the free and low-cost tools will not be satisfactory for many businesses, especially medium and large one, due to their limitations, a review of the free tools is a good starting point. Later discussion of the commercial products will benefit by having first reviewed the free tools.

Three Free Auditing Tools
Both Microsoft and Shavlik Technologies have developed three free tools for auditing hotfixes and SPs on Windows systems:

- Baseline Security Analyzer Tool 1.0 (MBSA.exe and MBSACLI.exe) from Microsoft
- HFNetChk (Network Security Hot Fix Checker Tool)
  Both version 3.32 from Microsoft
  and version 3.83 from Shavlik Technologies
- HFNetChkLT 3.8.96 from Shavlik Technologies

The first tool, Baseline Security Analyzer Tool 1.0 (MBSA.exe), is a GUI based tool, however, it also has a command line executable (MBSACLI.exe) that also uses HFNetChk.exe.

The second tool, Network Security HotFix Checker Tool (HFNetChk.exe) has two versions; one from Microsoft, version 3.32 and a newer version 3.83 from Shavlik Technologies. Both versions are command line tools. The later version 3.83 is only available from Shavlik Technologies and has more features and switches than the earlier version 3.32, which is only available from Microsoft. HFNetChk has a long formal name, Network Security HotFix Checker Tool, however, for brevity it is often called HotFix Checker, or HF Net Check, among others. In this paper it will be referred to as Hot Fix Checker or HFNetChk.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The third free tool reviewed is HFNetChkLT 3.8.96 from Shavlik Technologies. This tool is very different from the other two free tools in that it has distinct advantages that put it far above the other two free tools reviewed. This is a 'Lite' version of full version HFNetChkPro.

Comparison of four free auditing tools:
HFNetChkLT, HFNetChk v3.83 and v.3.32, and Baseline Security Analyzer Tool [2]

Features	Free LT version 3.83 Shavlik Tech-nologies HotFix Checker LiteTool (HFNetChkLT)	Free Version 3.83 Shavlik Network Security HotFix Checker Tool (HFNetChk)	Free Version 3.32 Microsoft Network Security HotFix Checker Tool (HFNetChk)	Free Version 1.1 Microsoft Baseline Security Analyzer Tool (MBSA)
Real-time Patch Information	✓	✓	✓	✓
Command Line Interface	✓	ã	ã	ã
GUI Interface	✓	NO	NO	ã
Scan by Hostname	✓	✓	✓	✓
Scan by IP Address	✓	✓	✓	✓
Scan by Range of IP Addresses	✓	✓	✓	✓
Scan by Domain	✓	✓	✓	✓
Scan by Multiple Domains	NO	NO	NO	NO
Scan by Input File	✓ (Up to 256 target systems)	✓ (Up to 256 target systems)	✓ (Up to 256 target systems)	NO
Scan by Patch (MS02-001 Only, etc.)	✓	✓	✓	NO
SCAN by Machine Type (Servers only, Workstations only, etc.)	✓	NO	NO	NO
Terminal Server support	✓	✓	NO	NO
Unlimited Scanning	✓	✓	✓	✓
Detailed support for SQL 7, SQL 2000	✓	✓	✓	✓
Detailed support for Exchange 5.5, Exchange 2000	✓	✓	NO	✓
Detailed Patch installation database	✓ Only operating system patches and SPs	NO	NO	NO

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Patch Pushing and Management	✓ Only operating system patches and SPs	NO	NO	NO
View and Monitor patch deployment history	✓	NO	NO	NO
Full Reporting	✓	✓	✓	✓
Named Scans to Allow for Better Tracking	✓	✓	✓	✓
Sharing of Scans Across Computers to Better Manage Results	✓	NO	NO	NO
Advanced Domain Enumeration to Find All Computers on the Network	✓	NO	NO	NO
Ability to Send Messages to Computers You are Updating to Prepare Users	✓	NO	NO	NO
Cross-Domain Push	✓	NO	NO	NO
Scheduled Scans	✓	NO	NO	NO
Detailed Reporting	✓	✓	✓	NO
Customized Rules	✓	NO	NO	NO
Results Database	✓	NO	NO	✓
Results Comparison	✓	NO	NO	NO
Additional Detailed Info	✓	NO	NO	NO
XML Output	✓	✓	NO	✓
HTML Output	✓	NO	NO	✓
Comma delimited Output	✓	NO	NO	NO
"RunAs" Support to Allow Remote Support on More Computers	✓	✓ by using a switch to enter username and password	✓ by using a switch to enter username and password	✓
One report for all scanned machines	✓	✓	✓	NO
Report output location is user's choice	✓	✓	✓	NO
Option to show the history of all installed and/or not installed hotfixes	✓	✓	✓	NO
Option to suppress Notes and/or	✓	✓	✓	NO

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Warnings				
Option to do a baseline audit	✓	✓	✓	NO
Remote Push operating system patches	✓	NO	NO	NO
Remote Push Microsoft application patches	NO	NO	NO	NO
Browsing MS patch bulletins	✓	NO	NO	✓
Scripting editor	NO	NO	NO	NO
Easy to use	✓	NO	NO	✓

Figure 1.

Comparison of four free auditing tools:
HFNetChkLT, HFNetChk v3.83 and v.3.32, and Baseline Security Analyzer Tool [2]

Following is a review of these three free tools.

HotFix Checker Tool
HFNetChk was developed by Shavlik Technologies and Microsoft. The latest version, 3.83, was recently released (September 18, 2002) and is only available from Shavlik Technologies. Microsoft has not updated their website with the new version. The earlier version, 3.32, can be run from Windows NT 4.0, Windows 2000, or Windows XP systems, and will scan either the local system or remote ones for patches available for the following products: Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server 4.0 and 5.0, SQL Server 7.0 and 2000 (including Microsoft Data Engine), and Internet Explorer 5.01 and later. [3]

The newer version, 3.83, can do all of the above, and additionally can audit systems running Exchange 5.5 and 2000, Windows Terminal Server, and Windows XP Home Edition. It performs significantly faster scanning by host or by IP range. Many bugs were fixed as well. [4]

Microsoft has a Technet Article (Q303215) on Hfnetchk 3.32 called:
Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available (Q303215)
It includes a complete description of HotFix Checker, a download link, and usage syntax for the earlier version, 3.32, which most of the switches still apply in the newer version. [5]

There is a review of HFNetChk in the Windows 2000 & .NET Magazine, InstantDoc #22369, Hfnetchk: The Latest Security Hotfix Audit and Advisor Tool . Although the review is dated September 4, 2001, it is still relevant and informative. The article's author, Paula Sharik, says:

> "… I'm happy to report that despite its ungainly name, this tool is useful in small to midsized network environments. Hfnetchk has three features that you'll appreciate, especially when compared with the old Qfecheck utility.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

> "First, Hfnetchk uses a comprehensive XML-formatted hotfix catalog that Microsoft updates every time the company releases a new security hotfix.
> "Second, because the catalog contains a current list of all security hotfixes for each product, Hfnetchk can advise you of which fixes to apply to bring your system up to date.
> "Third, on the machine where you install Hfnetchk, you can initiate a remote audit of one machine, a group of machines, or all systems in a domain." [6]

Advantages of HotFix Checker Tool

The one main advantage of the HFNetChk command line tool is that it can be used in customized batch scripts to provide added value over the tedious and more time-consuming manual process of running the tool from a command line. Once a batch script is written, it usually only needs modification when a new version of the tool is released. Several or many batch scripts can be created for very specific scanning of remote computers, such as a script for each domain, or each IP range in an enterprise. A batch script can be scheduled to run repeatedly and more reliably than running it manually. So for automated audit scans, a batch script using HFNetChk is much better than a manual process due to less labor and more reliability using repeated and scheduled runs.

Disadvantages of HotFix Checker Tool

The problem with the HFNetChk.exe tool is that there are numerous command line switches. This makes repeated and varied uses of the tool tedious, slow to run various switches, and annoying even for an administrator who is very comfortable at the command line. Just looking at the usage syntax (below) and all the switches possible could be enough to make some administrators avoid using the tool at all.

Version 3.83 switches:

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

HotFix Checker 3.83 is available as a free download from Shavlik Technologies at the HFNetChk webpage:
http://hfnetchk.shavlik.com/

Microsoft has yet to update their website with the newer version, 3.83.
The older version, HotFix Checker 3.32, is still available as a free download from Microsoft at the HFNetChk webpage:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp

Baseline Security Analyzer Tool

Version 1.0 of MBSA includes a graphical and command line interface that can perform local or remote scans of Windows systems. MBSA runs on Windows 2000 and Windows

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

XP systems and will scan for missing hotfixes and vulnerabilities in the following products: Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server (IIS) 4.0 and 5.0, SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000 and 2002. MBSA creates and stores individual XML security reports for each computer scanned and will display the reports in the graphical user interface in HTML. [7]

Advantages of Microsoft Baseline Security Analyzer Tool
This tool can perform not only an audit of hotfixes and SPs, it can also provide other security information via password checks, IIS checks, and SQL checks. The password checks do slow the scan down substantially. If a password audit is not desired, than it is highly recommended to skip the password checking (via the GUI or the command line switch).

Disadvantages of Microsoft Baseline Security Analyzer Tool
The Microsoft Baseline Security Analyzer Tool (MBSA) has 3 major disadvantages when it comes to a remote audit. These disadvantages are so great that it virtually eliminates the MBSA GUI (MBSA.exe) and CLI (MBSACLI.exe) from being used in a remote audit especially of hundreds or thousands of systems.
These disadvantages are:

1. Cannot input a list file of computer systems.
   Comment: Due to this limitation, this tool is severely handicapped as regards a large remote audit. Selective targeting of systems is important for example in doing a spot check, or a re-check of certain systems with the least amount of labor.

2. Reports are created by default in %userprofile%\SecurityScan
   Comment: Due to the reports being created in only one possible location, which also cannot be changed by the user, the storage of audit report files is severely limited. This limitation on storage location also means added labor to make them available to others due to the need to copy/move the files out from the user's profile folder (%userprofile%\SecurityScan) to a shared folder.

3. Report output is one report per computer
   Comment: Using a browser to view one report per computer at a time can be very tedious and time-consuming. Whereas by comparison, the HotFix Checker Tool (HFNetChk.exe) report files can contain all the computers scanned. This one report (tab delimited) can be imported into a spreadsheet or a database for review, which is by far easier and faster for reviewing when dealing with an audit of hundreds or thousands of systems.

For a review of Microsoft Baseline Security Analyzer, you can visit www.w2knews.com and read the Issue 347, Feb 25, 2002 . The author states that MBSA "is a very low-end, pretty much end-user oriented tool." [8]

To view a screen shot of the MBSA scanning options, go to Appendix C.

To view a screen shot of the MBSA scan results of one machine, go to Appendix D.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Microsoft Baseline Security Analyzer Tool (MBSA) is available as a free download from Microsoft at the MBSA webpage:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsahome.asp

Batch scripting HFNetChk or MBSACLI
Both HFNetChk and MBSACLI can be run from the command line, and can be run from a batch script. To make the hotfix audit task easier and quicker, a security administrator can create a simple batch script to run either utility.

- HotFix Checker (HFNetChk.exe)
- Microsoft Baseline Security Analyzer Tool (MBSA) using the command line executable, MBSACLI.exe

The ease of use and the speed gained by using a batch script makes it much more likely that an administrator will run hotfix audits.

A batch script that runs either executable can be run periodically and scheduled using Task Scheduler thus reducing the labor involved for a security administrator to manually perform the audit task.

Examples of batch scripts
Several examples of very simple batch scripts follow to show how simple it is to run these executables.

HotFix Checker Tool (HFNetChk.exe) Script Examples
Example 1 – Audit a domain
hfnetchk -d *domainname* -o tab -f *domainname*_scan_%date%.txt

The above example will scan the entire domain provided, and output the results to a text file in a tab-delimited format. The file name will include the current date.

Example 2 – Audit an IP range
hfnetchk –r 192.168.1.1-192.168.1.254 -o tab -f 192.168.1.1-254_scan.txt

The above example will scan the range of IP addresses shown, and output the results to a text file in a tab-delimited format.

Baseline Security Analyzer Tool (MBSACLI.exe) Script Examples
Example 1 – Audit a domain for only hotfixes and operating system checks
mbsacli /d *domainnameI* /n password /n sql /n iis /o *domainname*_scan_%date%

The above MBSACLI example will scan the entire domain provided, and output the results to an XML format file. The file name will include the current date. The 3 checks: password, SQL, and IIS will be skipped. Only operating system and hotfix checks will be performed.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Example 1 – Audit an IP range for all checks
mbsacli /r 192.168.1.1-192.168.1.254 /o 192.168.1.1-254_scan_%date%

The above MBSACLI example will scan the IP range provided, and output the results to an XML format file. The file name will include the current date. The 5 checks: password, SQL, IIS, operating system and hotfix checks will be performed (default).

HFNetChkLT - Free GUI based HFNetChk tool
Shavlik Technologies has created a GUI based utility for auditing hotfixes and service packs. Not only can it perform relatively easy audit scans of remote computers, it can only push operating system patches. [1] This is the only free utility that the author found that has the four very important features in a free auditing tool.

1. Easy to use due to GUI interface
2. Results database to track scans
3. Scheduling of HFNetChkLT runs to automate secure scanning
4. Patch pushing (only operating system and hotfix patches)

HFNetChkLT, the LT version of HFNetChKPro (the full non-free professional version), has so many features and strong advantages over the other two free tools that discussing each of them would be more than most readers could bare. The four key advantages of this tool put it way above the first two free tools. Without going into a long discourse about the many other features that this tool has that the other two free tools do not, a short discussion of the four advantages noted will suffice.

First, a tool that is GUI based is almost always much easier to use for the greatest number of users. The Baseline Security Analyzer, although a GUI and therefore easy to use, does not have nearly the number of options available. For example, the Advanced Settings screen has many options that are much harder to use with the command line tools.

To view the **HFNetChkLT Advanced Settings** screen, go to Appendix E.

Second, an audit tool that can keep the scan results in a database is a highly desirable feature. When a large number of computers are being audited, having a database for storage of results is almost a necessity. The results database is possibly the best feature of HFNetChkLT. The database scan results allow the user to view the scan results by product as well as in total. By selecting the 'All Patches in Scan' folder, one can view all the missing patches. To view the screen **All Patches in Scan** results of one machine, go to Appendix F. Note the total of 5 patches and 2 SPs that were detected as missing.

In the example scan results, 3 products were detected as missing patches: Internet Explorer 6 Gold, Windows Media Player, and Windows XP Gold.
By selecting one product in the 'Patches by Product' folder, one can view only those patches missing for that product. To view the screen **Patches by Product** scan results of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

one machine, go to Appendix G. Note the 4 missing patches and 1 SP are ordered by product, in this case Windows XP Gold.

Also note that a patch is selected in the top right pane and that patch's bulletin is displayed in the lower right pane. This is very helpful in quickly determining if such a patch should be deployed if a quick determination is required. In most cases, however, a planned approach to deploying patches is warranted to avoid patching pre-maturely without careful consideration to the impact first. Nonetheless, being able to view the patch bulletin is a welcome feature.

Third, scheduling of HFNetChkLT running to automate secure scanning makes this tool a valuable time-saving tool. Scheduling of any task makes the task automated, and saves on labor and improves frequency, reliability and consistency of data. This scheduling option within the tool can make auditing an automated task. Scheduling using this tool is so easy when compared to scheduling a batch script using Task Scheduler.

To view the **HFNetChkLT Scheduling** screen, go to Appendix H.

Fourth, and finally, patch pushing of operating system and hotfix patches is something extra for free, and although it is not necessary for remote audits, it is an extremely nice feature to have. Sure, patch pushing can be done with another free command line tool, Qchain.exe from Microsoft. However, to have this capability in a free GUI should not be minimized, although only operating system and hotfix patches can be pushed using this LT version of HFNetChk. A detailed patch pushing or deployment discussion is not in the scope of this paper. However, patch pushing is such a convenient feature that after having used it in testing, I am spoiled. It sure makes the task easy. An added benefit is a deployment history is generated as well for easy reference after many scans.

To view the **HFNetChkLT Deployment Guide: Advanced** screen, go to Appendix I.

The download of HFNetChkLT is available from the following locations:
http://hfnetchk.shavlik.com/special/hfnetchkltsetup.exe
ftp://hfnetchk.shavlik.com/pub/hfnetchkltsetup.exe

More information on HFNetChkLT is available here:
http://www.shavlik.com/security/prod_hf_compare.asp

Summary Comparison of the three free tools
HotFix Checker, Baseline Security Analyzer, HFNetChkLT
HFNetChkLT has enough advantages to warrant it the best choice in free utilities for performing remote audits.

For a remote audit especially of hundreds of systems for hotfixes and service packs, the Hot Fix Checker Tool is a better choice than the Baseline Security Analyzer. For an audit of just one to say 50 systems, the Baseline Security Analyzer (MBSA) is sufficient, or for a larger number of systems, the command line executable (MBSACLI.exe) can be used. Either the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

GUI or the command line executable can provide other security information that has nothing to do with hotfixes and service packs. A discussion of the other auditable security information is not within the scope of this paper. Due to the previously outlined disadvantages of the HFNetChk and the Baseline Security Analyzer, neither is a good choice for an audit of a large enterprise. HFNetChkLT is the better tool for large audits due to its database, results comparison, and deployment history.

Comparison of HFNetChkLT, HFNetChkPro, UpdateEXPERT and LANguard NSS 3.0 [1]

Features	Free LT version Shavlik Technologies HotFix Checker LiteTool 3.8.96	Commercial version Shavlik Technologies HotFix Checker Pro 3.8.96	Commercial version St. Bernard Software UpdateEXPERT 3.2	Commercial version GFI LANguard Network Security Scanner 3.0
Real-time Patch Information	✓	✓	✓	✓
Command Line Interface	✓	ã	ã	ã
GUI Interface	✓	ã	ã	ã
Scan by Hostname	✓	✓	✓	✓
Scan by IP Address	✓	✓	✓	✓
Scan by Range of IP Addresses	✓	✓	✓	✓
Scan by Domain	✓	✓	✓	✓
Scan by Multiple Domains	✓	✓	NO	NO
Scan by Input File	✓	✓	✓	✓
Scan by Patch (MS02-001 Only, etc.)	✓	✓	✓	✓
SCAN by Machine Type (Servers only, Workstations only, etc.)	✓	✓	✓	✓
Terminal Server support	✓	✓	✓	NO
Unlimited Scanning	✓	✓	✓	✓
Detailed support for SQL 7, SQL 2000	✓	✓	✓	✓
Detailed support for Exchange 5.5, Exchange 2000	✓	✓	✓	✓
Detailed Patch installation database	✓	✓	✓	✓

© SANS Institute 2002, Author retains full rights.

Patch Pushing and Management	✓	✓	✓	✓
View and Monitor patch deployment history	✓	✓	✓	✓
Full Reporting	✓	✓	✓	✓
Named Scans to Allow for Better Tracking	✓	✓	✓	✓
Sharing of Scans Across Computers to Better Manage Results	✓	✓	✓	✓
Advanced Domain Enumeration to Find All Computers on the Network	✓	✓	✓	✓
Ability to Send Messages to Computers You are Updating to Prepare Users	✓	✓	✓	NO
Cross-Domain Push	✓	✓	✓	✓
Scheduled Scans	✓	✓	✓	✓
Detailed Reporting	✓	✓	✓	✓
Customized Rules	✓	✓	✓	✓
Results Database	✓	✓	✓	✓
Results Comparison	✓	✓	✓	✓
Additional Detailed Info	✓	✓	✓	✓
XML Output	✓	✓	✓	✓
HTML Output	✓	✓	✓	✓
Comma delimited Output	✓	✓	✓	NO
"RunAs" Support to Allow Remote Support on More Computers	✓	✓	✓	✓
One report for all scanned machines	✓	✓	✓	✓
Report output location is user's choice	✓	✓	✓	✓
Option to show the history of all installed and/or not installed hotfixes	✓	✓	✓	✓
Option to suppress Notes and/or Warnings	✓	✓	✓	✓
Option to do a	✓	✓	✓	✓

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

baseline audit				
Push operating system patches	✓	✓	✓	✓
Push Microsoft application patches	NO	✓	✓	✓
Browsing MS patch bulletins	✓	✓	✓	✓
Scripting editor	NO	NO	NO	✓
Easy to use	✓	✓	✓	✓

Figure 2

Comparison of HFNetChkLT, HFNetChkPro, UpdateEXPERT and LANguard NSS 3.0 [1]

HFNetChkLT - Free GUI based HFNetChk tool
This product was previously reviewed and charted in the first section on the free tools. However, for a side-by-side comparison with the three commercial tools, this product was also included in the above comparison chart. Note the many similar capabilities that this free product has with the other commercial products.

To view the previous review, go to HFNetChkLT.

HFNetChkPro
Shavlik Technologies (www.shavlik.com) has produced a full version of HFNetChk called Shavlik Network Security HotFix Checker or simply HFNetChkPro for short. It is a very capable GUI-based tool for auditing and pushing both patches for operating systems, hotfixes and SPs, as well as Microsoft application patches. [7] It has more features than LANguard NSS 3.0, as regards auditing and pushing patches. However, the additional features (listed in the table above) are not outstanding enough to discuss and are not significant enough to consider as large advantages when comparing HFNetChkPro to the other two products reviewed next, UpdateEXPERT 3.2, and LANguard NSS 3.0.
A complete description of HFNetChkPro is available at:
www.shavlik.com/security/prod_hf.asp [7]

UpdateEXPERT 3.2
St. Bernard Sofware (www.stbernard.com) has produced UpdateEXPERT 3.2; a GUI-based tool for auditing and pushing patches for operating systems, hotfixes, SPs, as well as Microsoft application patches. [10] Much like HFNetChkPro, it has more features than LANguard NSS 3.0, as regards auditing and pushing patches. However, the additional features are not outstanding enough to discuss and are not significant enough to consider as large advantages when comparing UpdateEXPERT 3.2 to the other two products reviewed, HFNetChkPro, and LANguard NSS 3.0.
A complete description of UpdateEXPERT 3.2 is available at:
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp [10]

To view the **UpdateEXPERT scan results of one machine**, go to Appendix J.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

LANguard Network Security Scanner 3.0
LANguard NSS 3.0 from GFI (www.gfi.com) is a product that is almost as capable as its rivals, HFNetChkPro and UpdateEXPERT, in the same capacities of remote auditing and patching of Windows systems. Although LANguard has fewer features than both for this purpose, it is only LANguard, however, that has many other security checks unrelated to remote auditing and patching of Windows systems. This product is actually a vulnerability scanner that includes auditing and patching of Microsoft hotfixes and SPs. [11] A detailed discussion of these other security checks and the other features of LANguard are unrelated to the scope of this paper. However, it is important to note (see below) many of these features to show the value and capability of this product above and beyond remote audit scans and patching. LANguard scan options can be set so that only missing patches and SPs are checked, as is also true of any of the many other security checks possible. By only checking for missing patches, the scan will run much faster.

There are a number of other features in LANguard that make it a very well rounded and fully capable vulnerability scanner for any size network of Windows systems.
More complete and detailed information about LANguard NSS 3.0 can be found at:
http://www.gfi.com/lannetscan/index.htm [11]

To view the **LANguard NSS 3.0 scan results of one machine – Missing Patches viewed from LANguard**, go to Appendix K.

To view the **LANguard NSS 3.0 scan results of one machine – Missing Patches viewed from HTML Report**, go to Appendix L.

Similarities of HFNetChkLT, HFNetChkPro, UpdateEXPERT, and LANguard NSS 3.0
There are so many similarities of HFNetChkLT, HFNetChkPro , UpdateEXPERT, and LANguard that it is too redundant to list all of them, so only the important similarities are listed.
The most important similarities of these four tools are:

- Audit hotfixes and service packs
- Push patches (except HFNetChkLT pushes only operating system patches)
- Scan by hostname
- Scan by IP address
- Scan a range of IP addresses
- Scan a domain
- "RunAs" Support to Allow Remote Support on More Computers
- GUI interface
- Browse MS Bulletins
- Results database
- Results comparison
- Full reporting
- Use Microsoft XML file (mssecure.xml) containing all latest patch data

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Differences between HFNetChkLT, HFNetChkPro, UpdateEXPERT, and LANguard
There are several distinguishing differences between HFNetChkLT, HFNetChkPro, UpdateEXPERT, and LANguard that are worth noting. The most important differences are listed below:

HFNetChkLT :
- Free download
- Only pushes operating system patches and hotfixes

HFNetChkPro and UpdateEXPERT have:
- A much higher cost
  - (see Pricing of HFNetChkPro) (see Pricing of UpdateEXPERT)

LANguard has:
- A much lower cost (see Pricing of LANguard NSS 3.0)
- Scripting editor (LANS) – more customization possible
- Many more security checks than only auditing hotfixes and SP's

LANguard NSS 3.0 differences in detail

A much lower cost
LANguard NSS 3.0 is much less costly and yet is very comparable to the Shavlik Technologies HFNetChkPro and UpdateExpert in remote auditing and patching. Pricing tables are shown below to illustrate the large differences in cost. The pricing for each product was found at each product's website.

Pricing of HFNetChkPro

Number of IP addresses	HFNetChkPro – Desktop	HFNetChkPro – SQL
Up to 50	$1123.75	$2122.75
Up to 100	$2185.25	$3185.25
Up to 250	$3748.75	$4747.75
Above 250	Contact Shavlik Technologies	Contact Shavlik Technologies

Figure 3

Pricing of UpdateEXPERT

Number of IP addresses	UpdateEXPERT
Up to 50	$795
Up to 100	$1400
Up to 250	$3460
Up to 500	$5070

Figure 4

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Pricing of LANguard NSS 3.0

Number of IP addresses	LANguard NSS 3.0
Up to 50	$249
Up to 100	$349
Up to 250	$450
Unlimited	$695

Figure 5

Many more security checks than only auditing hotfixes and SP's

Below are many of the other features and security checks of LANguard NSS 3.0.

- Fast TCP & UDP port scanning & identification
- "Alerts" pinpoint security issues & recommend action
- Finds all shares on your network
- Finds unused local users & groups
- Audits UNIX issues and CGI vulnerabilities.
- A script creator for writing complex security checks
- Identifies all installed NT/2000/XP services
- Checks if auditing is enabled & enable network wide
- Checks password policy
- Checks for programs that run automatically
- Tests password strength on Windows 9x/NT/2000 systems using a dictionary of commonly used passwords
- Support for sending spoofed messages (social engineering) [12]

Scripting editor (LANS) – more customization possible

LANguard has a scripting editor, and a scripting language called LANS that is used for writing your own customized security checks to be used in the Alerts module. The scripting editor has two welcome features: syntax highlighting and debugging. Having written many batch scripts, I particularly appreciate this feature to customize LANguard. There are a number of sample LANS scripts that come with LANguard to help the initial scripting process. Although the LANS scripting feature is not necessary for running the audit scans for hotfixes and SPs, it is an extra feature that could be used for customized alerting as regards hotfixes or SPs, though this would not be a typical use of the scripting function. [11]

Important Guidelines

- Ideally run remote audits from on only the most secured and hardened Windows workstations (NT, 2000, XP) that are solely used by the auditor(s).
- Auditing tools, such as executables, scripts, and the reports generated by such tools should be treated as highly confidential.
- Change management control of some degree should be implemented on all auditing tools including audit scripts.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

The security administrator has at least three choices of free utilities for auditing hot fixes and security patches on Windows systems. A free utility however may not be the best choice due to their inherent limitations. Certainly a free utility has an obvious advantage over purchased utilities, however, both the first two free tools reviewed were severely limited for any audits greater than a small number of systems.

Through the comparison of the three free tools,

Microsoft Network Security HotFix Checker Tool (HFNetChk.exe),
Microsoft Baseline Security Analyzer (MBSA.exe, MBSACLE.exe), and
HFNetChkLT, the Lite version of HFNetChkPro,

and the comparison of the three commercial tools,

HFNetChkPro
UpdateEXPERT 3.2
LANguard NSS 3.0

you have hopefully gained more understanding of these tools for auditing Windows hotfixes and service packs. Depending on the size of the enterprise and the advantages of a certain tool, a better choice of tool can be made using the review and discussion in this paper.

The GUI based tool, HFNetChkLT, has the most important features for auditing purposes:

- Free
- Easy to use
- Patch articles viewable in the GUI
- Results database to track scans
- Scheduling and saving scans easily.

As a freebie, it is also capable of pushing operating system and hotfix patches.

The HotFix Checker Tool, (command line HFNetChk), could conceivably be used for a remote mass audit of hundreds or thousands of systems. However, due to the lack of a built-in database, extra labor would be involved in tracking the scan results and importing them into a database or spreadsheet for review. Such a task could be a daunting and tedious one. This is tool is more suited for a scan of a small number of systems, such as 256 which is the maximum number of machines that an input file can process.

The Baseline Security Analyzer is only sufficient for a very small number of systems, for example 50 or less. Its only advantage over the other two free tools is that it can provide additional security information unrelated to hotfixes and service packs, such as password audit information.

The three scanning products that are not free, HFNetChkPro, UpdateEXPERT, and LANguard NSS 3.0, are all very capable and very similar for the purpose of auditing and pushing hotfixes and SPs. However, only LANguard stands out as the superior product

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

for two reasons. It has a much lower cost when compared to the other two products, and it has more features due to its many other security checks although these checks are unrelated to auditing and patching Microsoft hotfixes and SPs.

The author's recommendation is to try free 30-day evaluation copy of LANguard and the free HFNetChkLT (no time limit), and the 15-day evaluation copy of UpdateEXPERT. The evaluation copy of LANguard will not let you do patch pushing nor scheduled scans, however, If you like it for auditing hotfixes and SPs, you could buy the full-featured purchased version of LANguard for $349 for up to 50 IP addresses. You can always upgrade to more IP addresses later if you need to.

As for the other two commercial products, HFNetChkPro, and UpdateEXPERT, there are two reasons that could warrant either product's purchase instead of LANguard.
These two reasons are:

- If your audit and patch deployment team members are to be restricted from having access to any data of a confidential nature that the LANguard product is capable of collecting that is unrelated to the Microsoft patches and SPs. This is by far the most important reason to consider HFNetChkPro or UpdateEXPERT over LANguard.

- If HFNetChkPro or UpdateEXPERT outweighs LANguard in their very similar patch auditing and pushing features, as well as outweighs LANguard's unique although unrelated functions of other security checks.

If you feel that one or both of the above are true in your business, then you could try the lowest cost HFNetChkPro –the Desktop version for up to 50 IP addresses, or the lowest cost UpdateEXPERT for up to 50 IP addresses. And if you like either product, and need more IP addresses scanned than 50, then upgrade after testing the lowest cost version.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendices

Appendix A – HotFix Checker Tool scan results of one machine - Word wrapped

Appendix B –HotFix Checker Tool scan results of one machine - Tab delimited

Appendix C – MBSA scanning options

Appendix D – MBSA scan results of one machine

Appendix E – HFNetChkLT Advanced Settings

Appendix F – HFNetChkLT scan results of one machine – All patches in Scan

Appendix G – HFNetChkLT scan results of one machine – Patches by Product

Appendix H – HFNetChkLT Scheduling options

Appendix I – HFNetChkLT Patch Deployment Guide: Advanced

Appendix J – UpdateEXPERT scan results of one machine

Appendix K – LANguard NSS 3.0 scan results of one machine – Missing Patches viewed from LANguard

Appendix L – LANguard NSS 3.0 scan results of one machine – Missing Patches viewed from HTML report

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix A

HotFix Checker Tool scan results of one machine - Word wrapped

```
----------------------------
166-XP1 (192.168.1.104)
----------------------------

    * WINDOWS XP GOLD

    Patch NOT Found MS01-054      Q309521
    Patch NOT Found MS01-059      Q315000
    Patch NOT Found MS02-006      Q314147
    Patch NOT Found MS02-008      Q318202
    Patch NOT Found MS02-008      Q318203
    Patch NOT Found MS02-017      Q311967
    Patch NOT Found MS02-029      Q318138

    * INTERNET EXPLORER 6 GOLD

    Patch NOT Found MS02-009      Q318089
    Patch NOT Found MS02-023      Q321232
    Note          MS02-027      Q323889


Microsoft Network Security Hotfix Checker, 3.32
Copyright (C) Shavlik Technologies, 2001-2002
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)

Please use the -v switch to view details for
Patch NOT Found, Warning and Note messages
Attempting to download the CAB from:
http://download.microsoft.com/download/xml/security/1.0/NT5/EN-US/mssecure.cab

File was successfully downloaded.

Attempting to load C:\Batch\HFCJU\mssecure.xml.
Using XML data version = 1.0.1.309  Last modified on 7/2/2002.

Scanning 166-XP1
.............
Done scanning 166-XP1
```

© SANS Institute 2002, Author retains full rights.

Appendix B

HotFix Checker Tool scan results of one machine - Tab delimited

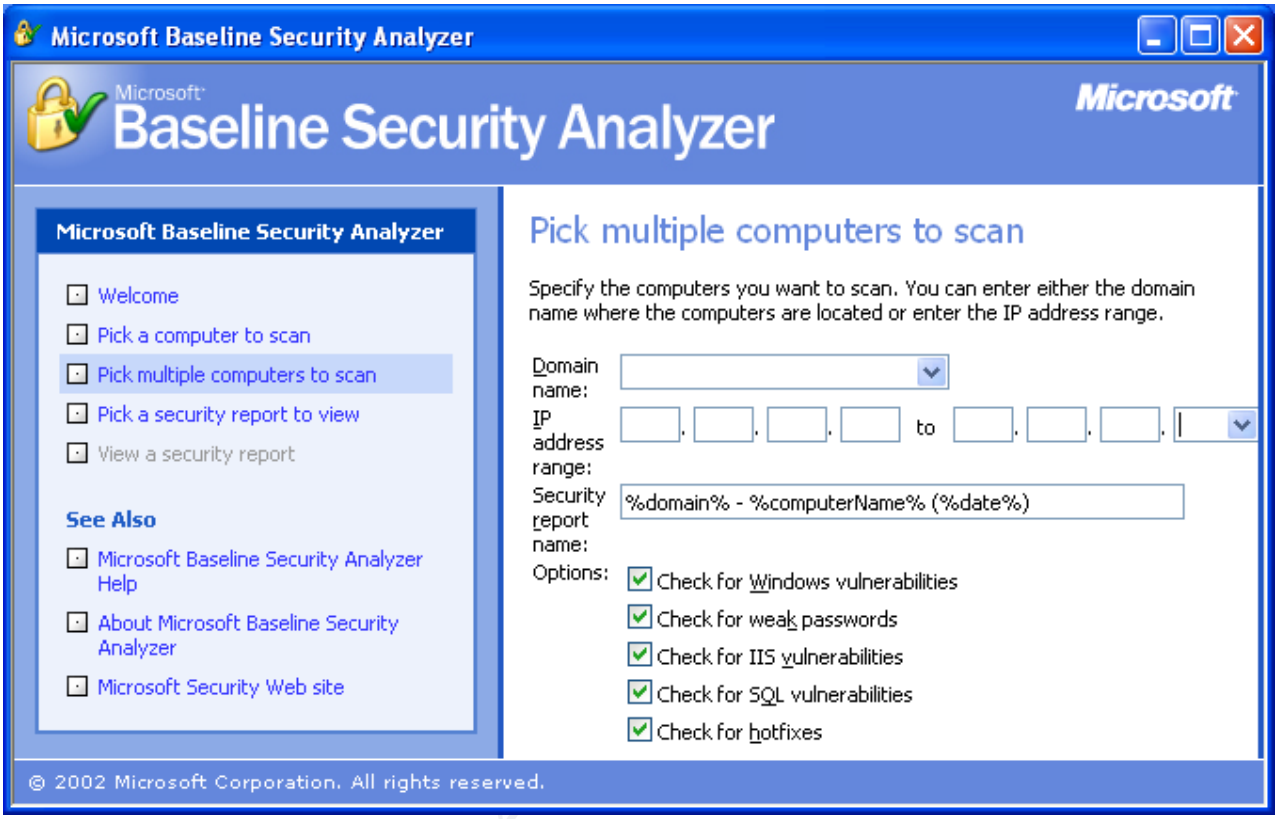
Machine Name	Product	Bulletin	Q Number
166-XP1 (192.168.1.104)	WINDOWS XP GOLD	MS01-054	Q309521
166-XP1 (192.168.1.104)	WINDOWS XP GOLD	MS01-059	Q315000
166-XP1 (192.168.1.104)	WINDOWS XP GOLD	MS02-006	Q314147
166-XP1 (192.168.1.104)	WINDOWS XP GOLD	MS02-008	Q318202
166-XP1 (192.168.1.104)	WINDOWS XP GOLD	MS02-008	Q318203
166-XP1 (192.168.1.104)	WINDOWS XP GOLD	MS02-017	Q311967
166-XP1 (192.168.1.104)	WINDOWS XP GOLD	MS02-029	Q318138
166-XP1 (192.168.1.104)	INTERNET EXPLORER 6 GOLD	MS02-009	Q318089
166-XP1 (192.168.1.104)	INTERNET EXPLORER 6 GOLD	MS02-023	Q321232
166-XP1 (192.168.1.104)	INTERNET EXPLORER 6 GOLD	MS02-027	Q323889

© SANS Institute 2002, Author r

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix C

MBSA scanning options



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix D

MBSA scan results of one machine

Microsoft Baseline Security Analyzer - Microsoft Internet Explorer

Microsoft Baseline Security Analyzer

6 missing hotfixes were found.

Result Details

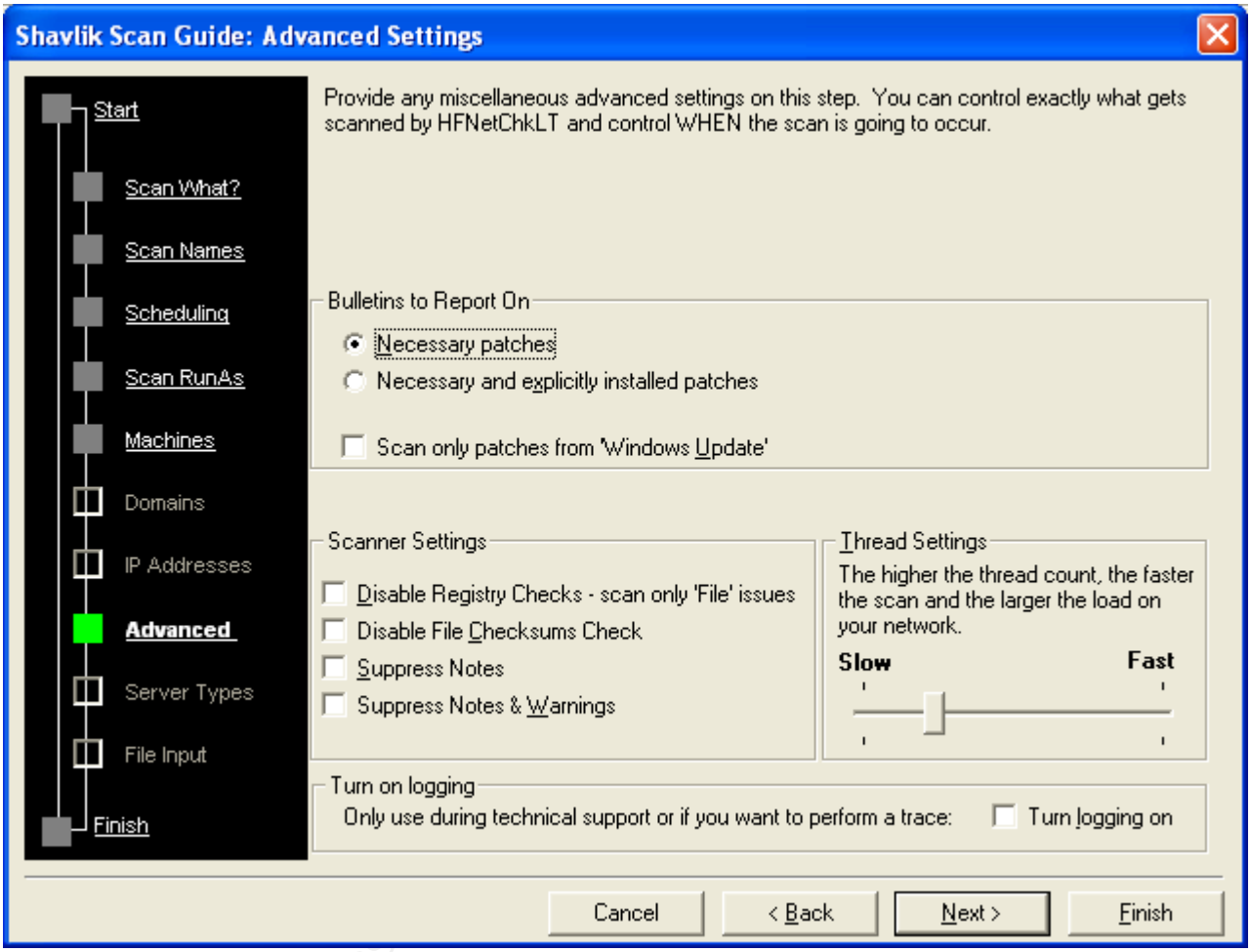
Hotfixes confirmed as missing on the scanned computer are marked with a red X. Hotfixes that the tool cannot confirm as installed on the scanned computer are marked with a yellow X.

Score	Hotfix	Description
✗		The latest service pack for this product is not installed.
✗	MS02-008	XMLHTTP Control Can Allow Access to Local Files
✗	MS02-045	Unchecked Buffer in Network Share Provider can lead to Denial of Service (Q326830)
✗	MS02-047	Cumulative Patch for Internet Explorer (Q323759)
✗	MS02-048	Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172)
✗	MS02-051	Cryptographic Flaw in RDP Protocol can Lead to Information Disclosure (Q324380)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix E

HFNetChkLT Advanced Settings

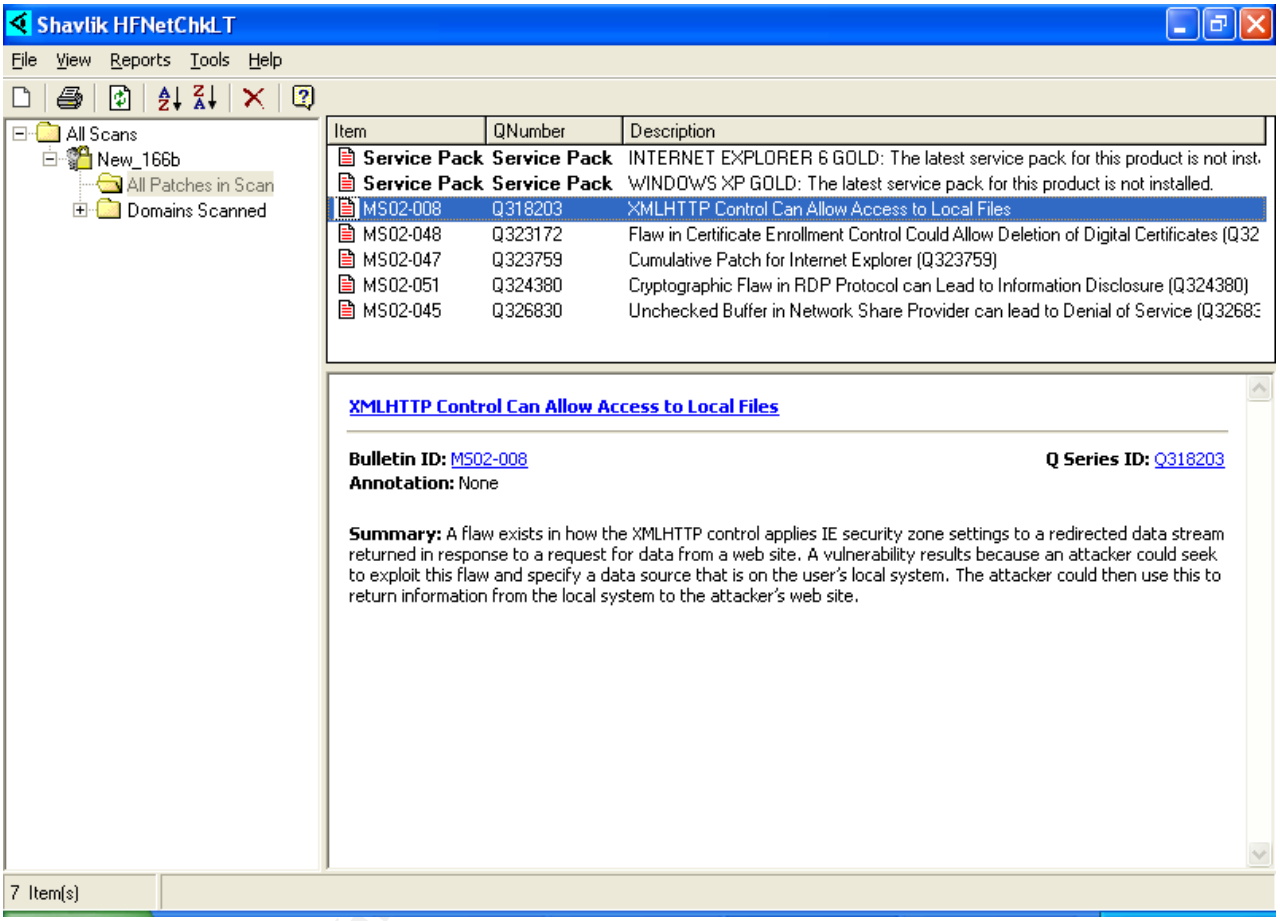


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix F

HFNetChkLT scan results of one machine

All Patches in Scan

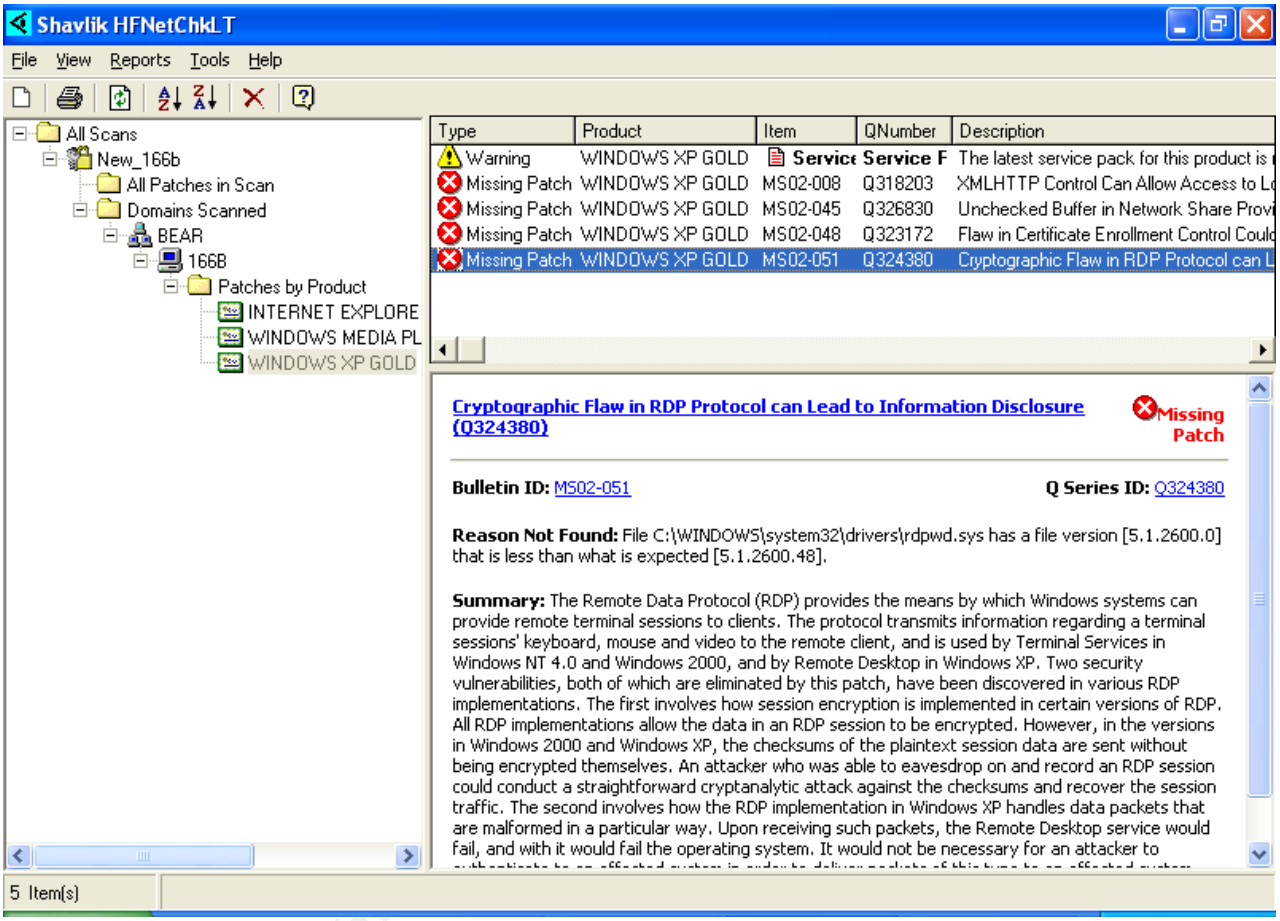


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix G

HFNetChkLT scan results of one machine

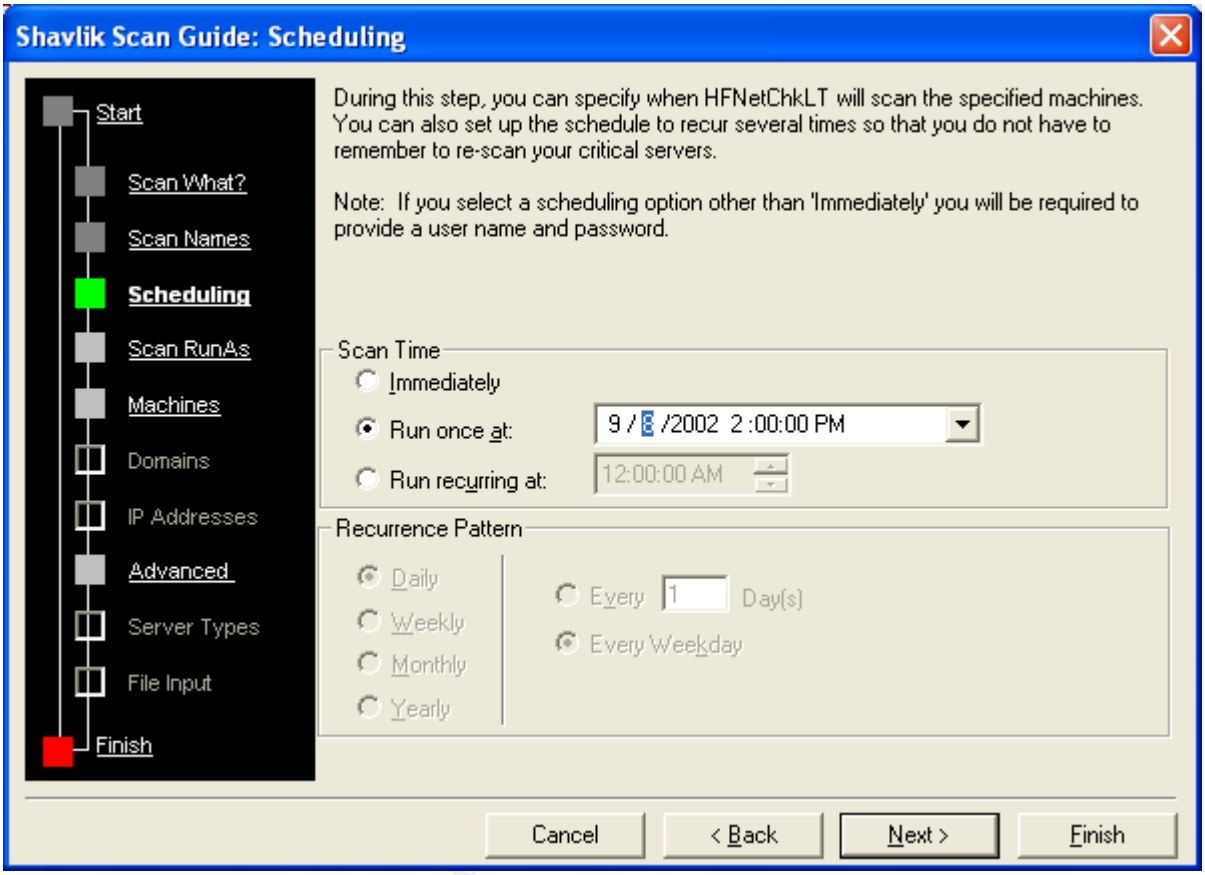
Patches by Product



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix H

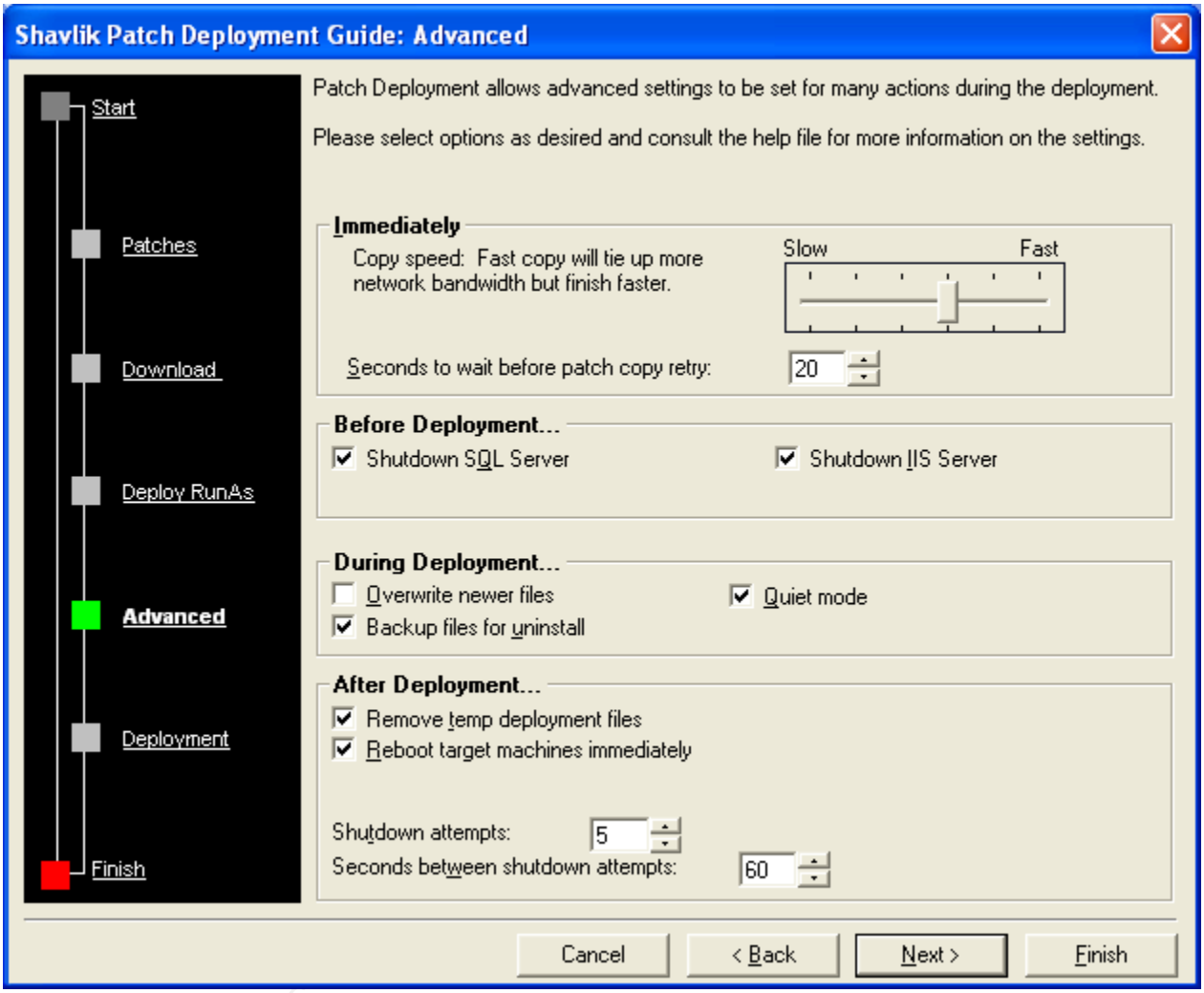
HFNetChkLT Scheduling options



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix I

HFNetChkLT Patch Deployment Guide: Advanced

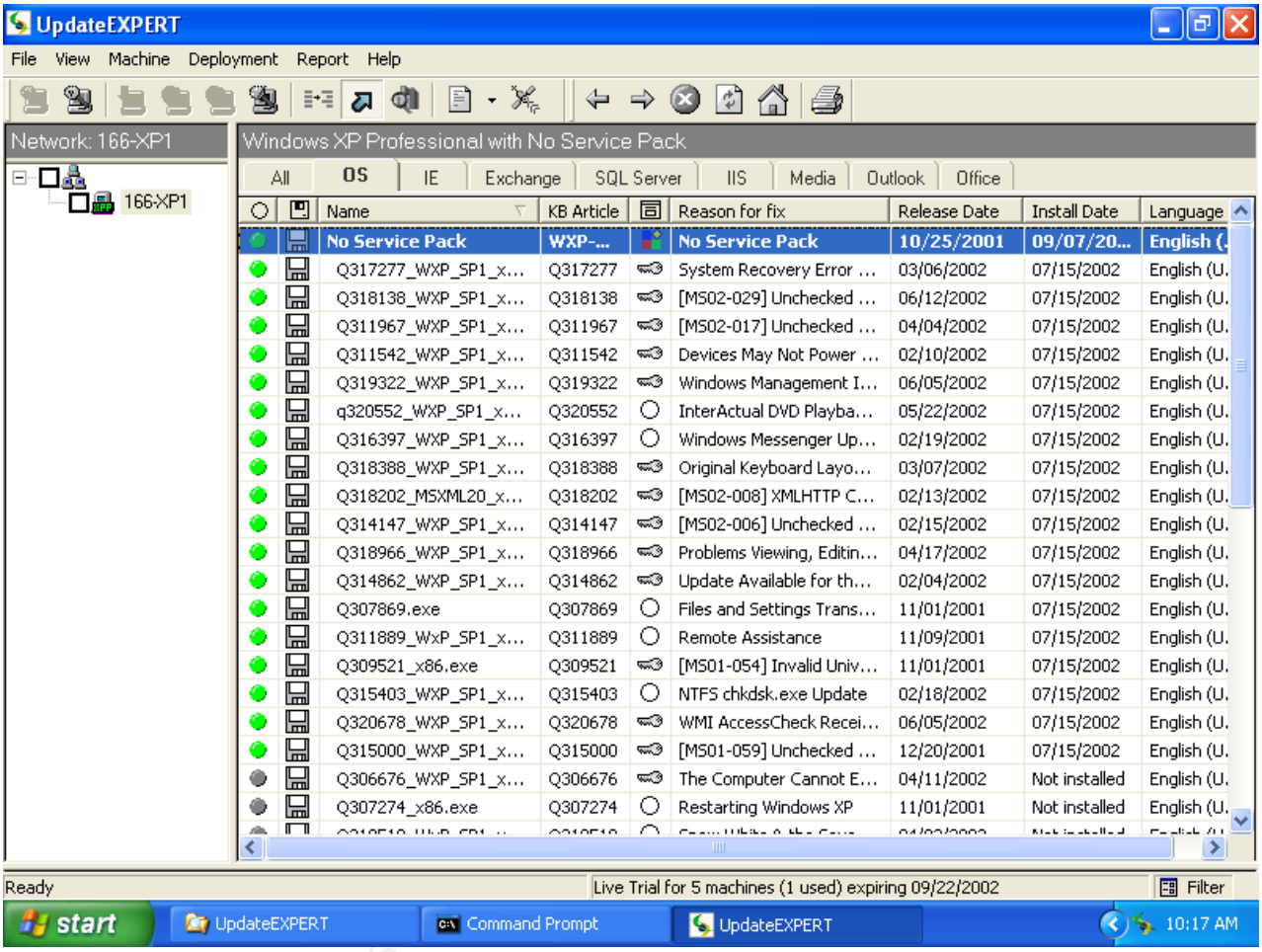


© SANS

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix J

UpdateEXPERT scan results of one machine

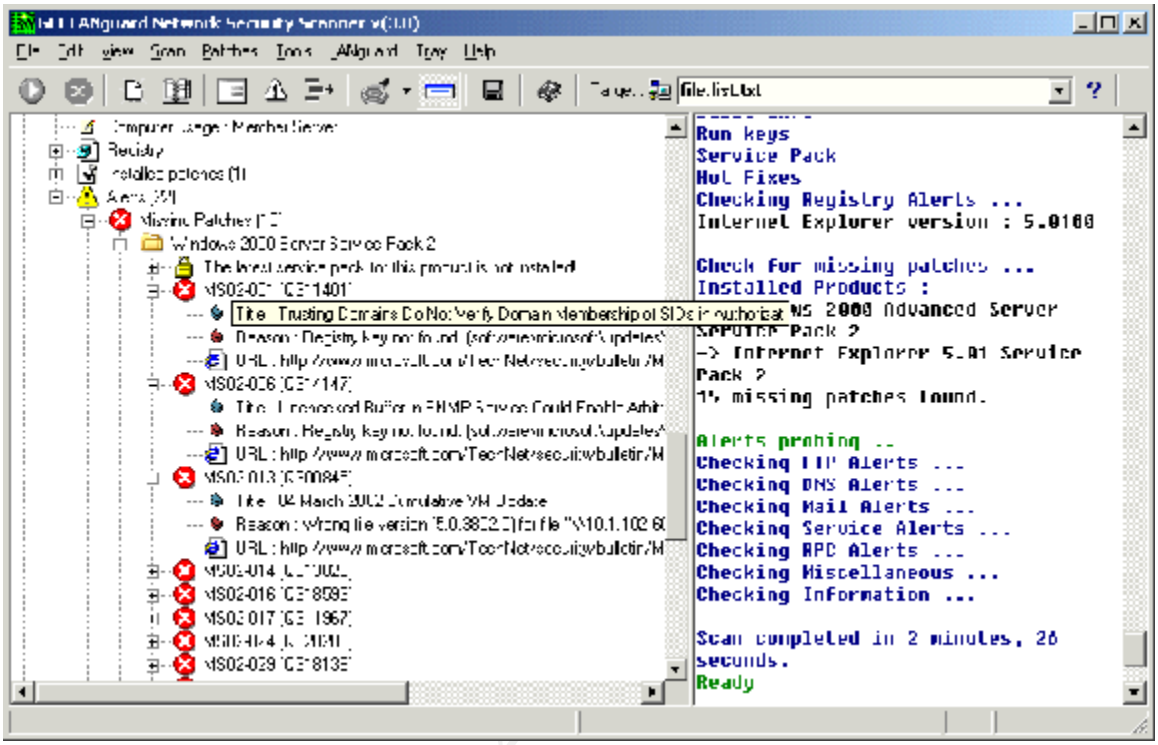


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix K

LANguard NSS 3.0 scan results of one machine

Missing Patches viewed from LANguard



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Appendix L

LANguard NSS 3.0 scan results of one machine

Missing Patches viewed from HTML Report

P:\MyDocs\GSEC\LANguard\results - 21 September - missing patches.html - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address P:\MyDocs\GSEC\LANguard\results - 21 September - missing patches.html Go Links

10.1.102.1 [ ]

IP Address : **10.1.102.1**
Operating System :
Time to live : **128**

Alerts

Missing patches

Windows 2000 Server Service Pack 2

The latest service pack for this product is not installed !
Latest SP available : Service Pack 3
http://www.microsoft.com/technet/security/news/w2ksp3.asp

MS02-001 - Q311401
Trusting Domains Do Not Verify Domain Membership of SIDs in Authorization Data
Registry key not found. (software\microsoft\updates\windows 2000\sp3\sp2srp1)
http://www.microsoft.com/TechNet/security/bulletin/MS02-001.asp

MS02-006 - Q314147
Unchecked Buffer in SNMP Service Could Enable Arbitrary Code to be Run
Registry key not found. (software\microsoft\updates\windows 2000\sp3\q314147)
http://www.microsoft.com/TechNet/security/bulletin/MS02-006.asp

MS02-008 - Q318203
XMLHTTP Control Can Allow Access to Local Files
Wrong file version (8.0.7820.0) for file _\\10.1.102.9\C$\WINNT\system32\msxml3.dll_, should be (8.20.9415.0)
http://www.microsoft.com/TechNet/security/bulletin/MS02-008.asp

MS02-013 - Q300845
04 March 2002 Cumulative VM Update
Wrong file version (5.0.3802.0) for file _\\10.1.102.9\C$\WINNT\system32\msawt.dll_, should be (5.0.3805.0)
http://www.microsoft.com/TechNet/security/bulletin/MS02-013.asp

MS02-014 - Q313829
Unchecked Buffer in Windows Shell Could Lead to Code Execution
Wrong file version (5.0.3315.2902) for file _\\10.1.102.9\C$\WINNT\system32\shell32.dll_, should be (5.0.3502.4718)
http://www.microsoft.com/TechNet/security/bulletin/MS02-014.asp

MS02-016 - Q318593
Opening Group Policy Files for Exclusive Read Blocks Policy Application (Q318593)
Wrong file version (5.0.2195.2862) for file _\\10.1.102.9\C$\WINNT\system32\w32tm.exe_, should be (5.0.2195.4600)
http://www.microsoft.com/TechNet/security/bulletin/MS02-016.asp

MS02-017 - Q311967
Unchecked Buffer in the Multiple UNC Provider Could Enable Code Execution (Q311967)
Wrong file version (5.0.2195.2104) for file _\\10.1.102.9\C$\WINNT\system32\drivers\mup.sys_, should be (5.0.2195.5080)
http://www.microsoft.com/TechNet/security/bulletin/MS02-017.asp

http://www.microsoft.com/TechNet/security/bulletin/MS02-006.asp Local intranet

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References

(1) Microsoft overview by Eric Schultze of HFNetChk at Blackhat called "How To Keep Up With Security Patches", URL: http://www.blackhat.com/presentations/win-usa-02/schultze-winsec02.ppt (September 25, 2002)

(2) Shavlik Technologies, Comparison of HFNetChk, HFNetChkLT, and HFNetChkPro, URL: http://www.shavlik.com/security/prod_hf_compare.asp (September 25, 2002)

(3) Microsoft Corp., "HFNetChk ", TechNet, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp (September 25, 2002)

(4) Shavlik Technologies, What's New in HFNetChk version 3.83, URL: http://hfnetchk.shavlik.com/support/hfreadme.htm (September 25, 2002)

(5) Microsoft Corp., "Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available (Q303215)", Knowledge Base, March 11, 2002 http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303215 (September 25, 2002)

(6) Sharick, Paula "Hfnetchk: The Latest Security Hotfix Audit and Advisor Tool", Windows 2000 & .NET Magazine, InstantDoc #22369, September 4, 2001, URL: http://www.win2000mag.com/Articles/Index.cfm?ArticleID=22369 (September 24, 2002)

(7) Microsoft Corp., "Microsoft Baseline Security Analyzer", TechNet, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsahome.asp (September 25, 2002)

(8) W2knews.com issue, "New Microsoft Security Freeware Scans For Windows Holes" about Microsoft Baseline Security Analyzer, Issue 347, Feb 25, 2002 (September 24, 2002)

(9) Shavlik Technologies, Overview of HFNetChkPro, URL: http://www.shavlik.com/security/prod_hf.asp (September 25, 2002)

(10) St. Bernard Software, Overview of UpdateEXPERT 3.2, URL: http://www.stbernard.com/products/updateexpert/products_updateexpert.asp (September 24, 2002)

(11) GFI, Overview of LANguard Network Security Scanner 3.0, URL: http://www.gfi.com/lannetscan/index.htm (September 25, 2002)

(12) GFI, LANguard Network Security Scanner Features, URL: http://www.gfi.com/lannetscan/lanscanfeatures.htm (September 25, 2002)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**