Shavlik

# Shavlik NetChk™ Analyzer

## Command Line Reference

# Copyright

# Trademarks

# Document Information and Print History

*Shavlik NetChk™ Analyzer Command Line Reference*

Document number:  N/A

| Date | Version | Description |
|---|---|---|
| May 2006 | 1.0 | Initial release of this guide. |

# CONTENTS

THIS PAGE INTENTIONALLY BLANK

# 1 INTRODUCTION

## About this guide

This guide describes the command line switches that are available for use with Shavlik NetChk™ Analyzer.

## Command requirements

The commands you create must meet the following requirements:

- ❑ Each command must be a complete command
- ❑ Each command must begin with the term “hfcli.exe”

## For further information

If after reading this document you have further questions about the commands available for use with Shavlik NetChk Analyzer, please see visit the Shavlik Support Forum for Shavlik NetChk Analyzer at http://forum.shavlik.com/viewtopic.php?t=3210

# 2 COMMAND SWITCHES

Shavlik NetChk Analyzer supports the following command line switches. Items marked in yellow are new since MBSA 1.2.1.

To view a list of available commandline switches in Shavlik NetChk Analyzer, type hfcli.exe /? at the command line.

## Specifying what machines to scan

The following command switches can be used to specify what machines you want to scan.

| Command Switch | Description |
|---|---|
| [-h hostname] | Specifies the NetBIOS machine name to scan. If you are scanning multiple machines by name, you can separate each hostname with a comma:<br>**Example:** -h pc1,pc2,pc3 (no spaces allowed after the comma)<br>Machine names are converted to IP addresses during the scan process. To ensure accurate results, make sure that DNS, WINS, and DHCP are working correctly.<br>The -h switch can be used in conjunction with any other switch in this category:<br>**Example:** -h pc1,pc2 -d domainname -i 10.1.1.1 |
| [-i ipaddress] | Specifies the IP address of a machine to scan. If you are scanning multiple machines by IPaddress, you can separate each IPaddress with a comma:<br>**Example:** -i 10.1.1.1,10.1.1.2,172.16.1.1 (no spaces allowed)<br>The -i switch can be used in conjunction with any other switch in this category:<br>**Example:** -i 10.1.1.1 -h pc1,pc2 -d domainname |
| [-d domainname] | Specifies the domain name to scan. All machines in the domain will be enumerated and then scanned. To |

| | |
|---|---|
| | scan multiple domains, separate each domain with a comma:<br>**Example:** -d corp,dmz,acme (no spaces allowed after the comma)<br>During domain enumeration, the scan engine will attempt to contact the domain controller(s) for each domain and obtain the machine account list for the domain. Your currently logged on user credentials will be used to authenticate to the domain controller to obtain this information. If you are not logged on to your console with credentials to obtain this information, the network browse list will be used instead.<br>To force the scan engine to use the browse list only, include the -ubo switch below.<br>The -domain switch can be used in conjunction with any other switch in this category:<br>**Example:** -d corp -h pc1,pc2 -i 10.1.1.1 -ubo |
| [-n] | The -n switch will scan all of the Microsoft machines on the local network. The list of machine to scan will approximate the same list of machines that you can see via Network Neighborhood.<br>The -n switch can be used in conjunction with any of the other switches in this category, though it is best used by itself. |
| [-ubo] | Use browse list only. This switch is applicable to the -d switch. This switch forces the scan engine to enumerate the domain membership using the browse list from the master browser of the domain, rather than attempting to gather the list of machine accounts from the domain controllers.<br>In some cases it may be beneficial to use this switch to scan the domain, particularly in cases where the network administrator has not purged stale machine accounts from the domain controller.<br>The -ubo switch is specific to the -d and -n switches. |
| [-r range] | The -r switch specifies a range of IP addresses to scan. This switch is useful when scanning subnets and identifying machines that may not be known, or may not be a member of any domain. (In cases where the scan engine encounters a 'rogue' machine |

| | |
|---|---|
| | and does not have the credentials to logon to this machine, the scan results will identify each machine that it attempted to scan and failed, so you can later research the 'rogue' system.)<br><br>If you are scanning multiple IP ranges, you can separate each IP range with a comma:<br>**Example:**<br>-r 10.1.1.1-10.1.1.255,172.16.1.1-172.16.1.127<br><br>The -i switch can be used in conjunction with any other switch in this category:<br>**Example:**<br>-r 172.16.1.1-172.16.1.255 -i 10.1.1.1 -h pc1,pc2 |
| [-ou ou_name] | Specifies the organizational unit (OU) to scan. All machines in the OU will be scanned.<br><br>In order to enumerate the OU membership, your currently logged on username will be used to authenticate to the domain controller. If you do not have admin access to the domain associated with this OU, then the enumeration may fail.<br><br>If you would like to include child OUs when scanning the specified OU, use the -ouc switch below.<br><br>The -ou switch can be used in conjunction with any other switch in this category:<br>**Example:**<br>-ou ou=development,DC=shavlik,dc=com -h pc1,pc2 |
| [-ouc ou_name] | Specifies that children OUs of the specified OU should be included in the scan.<br><br>The -ouc switch can be used in conjunction with any other switch in this category:<br>**Example:**<br>-ouc cn=computers,DC=shavlik,dc=com -h pc1,pc2 |
| [-fh hostfile] | Specifies a text file that contains a list of NetBIOS machine names to scan. Each machine name should be entered on its own line:<br>PC1<br>PC2<br>PC3<br><br>The text file will be read at scan time and any machine names listed in this file will be scanned. |

| | |
|---|---|
| | This switch may be useful if you are using a separate utility to create a list of machines to scan. For example, you may wish to schedule hfcli.exe to scan every hour, where it will scan the contents of the specified text file. The text file is the result of a script that enumerates the domain and outputs the results to a text file.<br>The -fh switch can point to a file of hosts in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -fh \\server1\data\machines.txt<br>The -fh switch can be used in conjunction with any of the other switches in this category:<br>**Example:**<br>-fh s:\data\machines.txt -h pc1,pc2 -i 10.1.1.1 |
| [-fip ipfile] | Specifies a text file that contains a list of IP addresses to scan. Each IP address should be entered on its own line:<br>10.1.1.1<br>10.1.1.2<br>10.1.1.3<br>The text file will be read at scan time and any IP addresses listed in this file will be scanned.<br>This switch may be useful if you are using a separate utility to create a list of IP addresses to scan. For example, you may wish to schedule hfcli.exe to scan every hour, where it will scan the contents of the specified text file. The text file is the result of a port scanner tool that outputs IP addresses that it finds.<br>The -fip switch can point to a file of IPs in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -fip \\server1\data\ipaddrs.txt<br>The -fip switch can be used in conjunction with any of the other switches in this category:<br>**Example:**<br>-fip s:\data\ipaddrs.txt -h pc1,pc2 -i 10.1.1.1 |
| [-fd domainfile] | Specifies a text file that contains a list of domain names to scan. Each domain name should be entered on its own line:<br>corp |

| | |
|---|---|
| | dmz<br>development<br><br>The text file will be read at scan time and any domains listed in this file will be enumerated and scanned.<br><br>The -fd switch can point to a file of domains in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -fd \\server1\data\domains.txt<br><br>The -fip switch can be used in conjunction with any of the other switches in this category:<br>**Example:**<br>-fd s:\data\domains.txt -ubo -fh \\server1\hosts.txt |
| [-fipr rangefile] | Specifies a text file that contains a list of IP address ranges to scan. Each IP range should be entered on its own line:<br>10.1.1.1-10.1.1.255<br>172.16.1.1-172.17.255.255<br>192.168.0.1-192.168.2.255<br><br>The text file will be read at scan time and any IP ranges in this file will be scanned.<br><br>The -fipr switch can point to a file of domains in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -fipr \\server2\data\ipranges.txt<br><br>The -fip switch can be used in conjunction with any of the other switches in this category:<br>**Example:** -fipr s:\data\ranges.txt -h pc1,pc2 -d corp |
| [-mf machinefilter] | The -mf switch instructs the scan engine to filter the machines to scan for based on their machine type.<br><br>(1) Scan servers only<br>(2) Scan workstations only<br>(3) Scan both servers and workstations.<br><br>Scanning both workstations and servers is the default.<br><br>If you do NOT use this switch, the scan engine will scan both workstations and servers. It is not necessary to use this switch unless you'd like to scan for only workstations and not servers, or vice versa. |

| | |
|---|---|
| | This switch may be used in conjunction with any other switch in this category:<br>**Example:** -mf 1 -d corp |

## Specifying what machines not to scan

The following command switches can be used to specify what machines you don't want to scan.

| Command Switch | Description |
|---|---|
| [-ih hostname] | The -ih switch specifies a NetBIOS machine name that should not be scanned. You may ignore multiple machine names by placing commas in between the machine names:<br>**Example:** -ih pc9,pc8<br>This switch may be useful when scanning a domain where you wish to exclude certain machines:<br>**Example:** -d corp -ih payroll,ceo<br>The -ih switch should be used in conjunction with domain (-d), network (-n), and OU (-ou and -ouc) scans. Do not use this switch when scanning by IP address or IP range.<br>This switch may be combined with other switches in this category:<br>**Example:** -d corp -ih payroll -i 10.1.1.1 -mf 1 |
| [-iip ipaddress] | The -iip switch specifies an IP address that should not be scanned. You may ignore multiple IP addresses by placing commas in between the addresses:<br>**Example:** -iip 192.168.1.10,192.168.1.11<br>This switch may be useful when scanning an IP range where you wish to exclude certain addresses from being scanned:<br>**Example:**<br>-r 192.168.1.1-192.168.2.255 -iip 192.168.2.1<br>The -iip switch should be used in conjunction with IP range (-r)scans. Do not use this switch when scanning by machine name, domain name, network, or OU. |

| | |
|---|---|
| | This switch may be combined with other switches in this category:<br>**Example:** -r 10.1.1.1-10.1.1.155 -iip 10.1.1.10 -mf 1 |
| [-id domainname] | The -id switch specifies a domain name that should not be scanned.  You may ignore multiple domain names by placing commas in between the names:<br>**Example:** -id dev,qa<br>This switch may be useful when scanning the entire network where you wish to exclude certain domains from being scanned<br>**Example:** -n -id dmz,finance<br>The -id switch should be used in conjunction with network (-n) scans.  Do not use this switch when scanning by machine name, domain name, OU, IP address or IP range.<br>This switch may be combined with other switches in this category:<br>**Example:** -n -id corp -mf 1 |
| [-ir range] | The -ir switch specifies an IP range that should not be scanned.  You may ignore multiple IP ranges by placing commas in between the entries:<br>**Example:** -ir 10.1.1.20-10.1.1.25,10.1.1.90-10.1.1.95<br>This switch may be useful when scanning large IP address ranges, but you wish to ignore specified ranges from being scanned.  As an example, you may wish to scan your corporate IP range but ignore the IP addresses assigned to a remote access dial-in pool.<br>**Example:**<br>-r 10.1.1.1-10.1.17.255 -ir 10.1.9.1-10.1.9.255<br>The -ir switch should be used in conjunction with IP range (-r) scans.  Do not use this switch when scanning by machine name, domain name, OU, or IP address scans.<br>This switch may be combined with other switches in |

| | |
|---|---|
| | this category:<br>**Example:**<br>-r 10.1.1.1-10.1.17.255 -ir 10.1.9.1-10.1.9.255 -mf 1 |
| [-ifh hostfile] | The -ifh switch is similar to the -ih switch (to ignore specified machine names), however it uses a text file to list the machine names to ignore.<br>Create a text file and list each machine name to ignore, placing each machine name on its own line:<br>payroll<br>ceo<br>sql<br>pc1<br>The text file will be read at scan time and any machine names listed in this file will be ignored.<br>The -ifh switch should be used in conjunction with domain (-d), network (-n), and OU (-ou and -ouc) scans.  Do not use this switch when scanning by IP address or IP range.<br>The -fh switch can point to a file of hosts in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -ifh \\server1\data\badmachines.txt<br>The -ifh switch can be used in conjunction with any of the other switches in this category or the prior category:<br>**Example:**<br>-ifh s:\data\badmachines.txt -d corp -i 10.1.1.1 |
| [-ifip ipfile] | The -ifip switch is similar to the -iip switch (to ignore specified IP addresses), however it uses a text file to list the IP addresses to ignore.<br>Create a text file and list each IP address to ignore, placing each address on its own line:<br>10.1.1.10<br>172.16.1.9<br>192.168.1.1<br>The text file will be read at scan time and any IP addresses listed in this file will be ignored.<br>The -ifip switch should be used in conjunction with IP |

| | |
|---|---|
| | range (-r)scans.  Do not use this switch when scanning by machine name, domain name, network, or OU.<br>This switch may be combined with other switches in this category:<br>**Example:**<br>-r 10.1.1.1-10.1.1.155 -ifip ignoreIPs.txt -mf 1<br>The -ifip switch can point to a file of IP addresses in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -ifip \\server1\data\badIPs.txt<br>The -ifip switch can be used in conjunction with any of the other switches in this category or the prior category:<br>**Example:** -ifip s:\badIPs.txt -r 10.1.1.1-10.1.1.255 |
| [-ifd domainfile] | The -ifd switch is similar to the -id switch (to ignore specified domains), however it uses a text file to list the domains addresses to ignore.<br>Create a text file and list each domain name to ignore, placing each domain name on its own line:<br>dmz<br>dev<br>test<br>The text file will be read at scan time and any domain names listed in this file will be ignored.<br>This switch may be useful when scanning the entire network where you wish to exclude certain domains from being scanned<br>**Example:** -n -ifd c:\data\ignoredomains.txt<br>The -ifd switch should be used in conjunction with network (-n) scans.  Do not use this switch when scanning by machine name, domain name, OU, IP address or IP range.<br>This switch may be combined with other switches in this category: |

| | |
|---|---|
| | **Example:** -n -ifd \\server3\ignoredomains.txt -mf 2 |
| [-ifipr rangefile] | The -ifipr switch is similar to the -ir switch (to ignore ranges of IP adddresses), however it uses a text file to list the IP address ranges to ignore.<br>Create a text file and list each IP address range to ignore, placing each range on its own line:<br>10.1.1.10-10.1.1.15<br>172.16.1.1-172.16.1.25<br>192.168.1.1-192.168.1.99<br>The text file will be read at scan time and any IP ranges listed in this file will be ignored.<br>The -ifipr switch should be used in conjunction with IP range (-r)scans. Do not use this switch when scanning by machine name, domain name, network, or OU.<br>This switch may be combined with other switches in this category:<br>**Example:**<br>-r 10.1.1.1-10.1.1.155 -ifipr ignoreIPranges.txt<br>The -ifipr switch can point to a file of IP ranges in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -ifipr \\server1\data\badIPranges.txt |

## Specifying what patches to scan or not scan

The following command switches can be used to specify what patches you want to scan for or not scan for.

| Command Switch | Description |
|---|---|
| [-q q_number] | The -q switch specifies a patch to scan for. You may specify multiple patches to scan for by separating the list of qnumbers with a comma:<br>**Example:** -q q123456,q654321,q223344<br>The 'QNumber' corresponds to the KB article number usually assigned by the vendor. Shavlik modifies this number so it always begins with the letter Q, and is usually followed by 6 numbers. (The easiest way to determine the assigned qnumber for a given patch is to scan a machine where this patch is currently |

| | |
|---|---|
| | missing or installed)<br>When scanning for a specific qnumber, supersedence logic is disabled.  For example, patch Q112233 is rolled up and included in patch Q223344 and would normally not be scanned for in a default 'missing' scan.  However, by including this qnumber in an explicit request to scan for this patch, the supersedence logic is disabled and the explicit state of Q112233 will be assessed.  Only those patches specifically referenced by this switch will be scanned. (Service Pack status, however, is always returned.)<br>This switch may be used in conjunction with any other set of switches:<br>**Example:** -d corp -q Q112233,Q123456 |
| [-fq file_of_q_numbers] | The -fq switch is similar to the -q switch, however it uses a text file to list the patches to scan. Each number should be listed on its own line:<br>Q123456<br>Q654321<br>Q112233<br>The text file will be read at scan time and any patches listed in this file will be explicitly scanned.<br>The -fq switch can point to a file of qnumbers in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -fq \\server1\data\qnumbers.txt<br>The -fq switch can be used in conjunction with any other set of switches:<br>**Example:** -fq qnumbers.txt -d corp |
| [-iq q_number] | The -iq switch specifies a list of qnumbers to ignore. You may specify multiple qnumbers by placing a comma in between each qnumber:<br>**Example:** -iq Q333333,Q444444<br>Ignoring a QNumber makes the scan engine behave as if this patch does not exist in the patch data XML file.<br>This switch may be useful if you'd like to ignore the latest patch released for Internet Explorer and instead |

| | |
|---|---|
| | scan for the prior cumulative IE update.<br>Patches that have not yet been approved for your organization (but have already been included in the patch data XML file from Shavlik) can be ignored by specifying these qnumbers in with the -iq switch.<br>The -iq switch can be used in conjunction with any other set of switches:<br>**Example:** -iq Q123456 -d corp |
| [-ifq file_of_q_numbers] | The -ifq switch specifies a file of qnumbers to ignore. Each qnumber should be listed on its own line in the file:<br>Q777777<br>Q888888<br>The text file will be read at scan time and any Numbers listed in this file will be ignored.<br>The -ifq switch can point to a file of qnumbers in any directory on the local machine, a network drive, or a UNC share:<br>**Example:** -ifq \\server1\data\badnumbers.txt<br>The -fq switch can be used in conjunction with any other set of switches:<br>**Example:** -ifq badqnumbers.txt -d corp |
| [-pt patchtype] | The -pt switch instructs the scan engine to scan for a particular type of patches.<br>The base set of patch types include:<br>(1) Security patches (default)<br>(4) Security tools<br>(8) Non-Security patches<br>*NOTE: Shavlik NetChk Analyzer for Microsoft will only scan for patchtype 1. SNA for Microsoft does not support scanning for non-security patches or tools.*<br>If you do not specify any patch type, only security patches will be scanned. |

| | |
|---|---|
| | To scan for security tools only (such as the Microsoft Malware Removal Tool), use -pt 4.<br>To scan for non security updates, such as the non-security critical updates that you find on WindowsUpdate, use -pt 8.<br>To scan for any combination of the above, add their patchtype numbers together to generate a new patchtype number. For example:<br>• To scan for security (1) and non security (8) patches use -pt 9 (this is the combination of pt's 1+8)<br>• To scan for tools and non security patches only, use -pt 12 (4+8)<br>• To scan for all three, use -pt 13 (1+4+8) |

## Specifying additional scan parameters

The following command switches can be used to specify additional scan parameters.

| Command Switch | Description |
|---|---|
| [-st scantype] | The -st switch instructs the scan engine to perform a particular type of scan. The two options are:<br>(0) Patch scan (default)<br>(2) Product list only. No patch scan<br>Scan type '0' is a normal patch scan.<br>Scan type '2' will not perform a patch scan, but will instead, provide a listing of the products and service packs installed on each system. (This is specific to the products that the Shavlik engine can scan for.)<br>If you do not specify any scan type, the default 'patch scan' will be performed. |
| [-pf product_filter] | The -pf switch specifies the list of products that the scan engine will assess for patch status. You may specify multiple products, each separated by a comma:<br>**Example:** -pf 1,2,3,4,5,6,7,17,18<br>Please see Shavlik Knowledge Base Article SKB3214 for a complete list of the product filter codes: |

| | |
|---|---|
| | http://forum.shavlik.com/viewtopic.php?t=3214 |
| [-ds] | The -ds switch will disable the supersedence logic in the scan engine. This switch is not necessary for normal operation.<br>By default, the scan engine will use patch supersedence criteria when performing a scan for missing patches. For example: MS02-001 is a cumulative rollup for Windows 2000 SP2 systems.<br>Installing this patch supersedes the need to install 40 earlier hotfixes. When scanning a Win2K SP2 system with NO patches installed, the scan engine will NOT display the 40 earlier patches as missing, but will instead list the superseding rollup patch, MS02-001, as being missing. Installing this patch effectively installs the 40 earlier patches.<br>Similarly, each Internet Explorer patch 'usually' supersedes the prior released IE security patch. Since the new patch supersedes all prior IE patches, the scan engine will 'skip' the earlier patch and will display the latest IE patch as the only patch that is required to be installed. (Since the earlier IE patches are contained inside the newest IE patch, there is no value to also showing the earlier IE patches as missing, nor to install these earlier patches as installation of the latest patch will bring the machine into a fully patched state.<br>The -ds switch will disable the above scan logic and will instead display patch state for each of the missing patches, whether they are superseded or not.<br>This switch is included only for use when performing specific audit functions where you would like to display each of the prior superseded patches as missing.<br>**Note**: The supersedence logic above only applies to the 'Patch NOT Found' scan. Superseded patches that have been installed will always appear as 'PATCH FOUND' in the scan results. |
| [-history <level>] | The -history switch instructs the scan engine to perform different types of patch scans. Specifically,<br>• -history: Missing & Explicitly installed |

- -history 1: Explicitly installed only
- -history 2: Missing with -ds
- -history 3: Missing and Explicitly installed with -ds
- -history 4: Effectively installed and Explicitly installed
- -history 5: Missing, Effectively installed and Explicitly installed

The default patch scan (without the -history flag) displays patches that are missing and are necessary to be installed to bring the machine into a full patched state.

The -history flag can be used to provide display additional patch status, such as 'which patches have been explicitly installed?' and 'which patches have been effectively installed through the installation of cumulative patches?'

Using the '-history' switch with no parameters will display the patches that are missing and are necessary to be installed, as well as the patches that have been explicitly installed on the computer. (This is the recommended usage for normal operation.)

The '-history 1' switch is included for compatibility with MBSACLI.exe /HF scripts and will display patches that have been explicitly installed.

The '-history 2' switch will display all the patches that are missing from a machine that have not been installed. -history 2 disables supersedence – similar to the -ds switch.

The '-history 3' switch will display the explicitly installed patches as well as the missing patches (with supersedence disabled). This is effectively a combination of results from scans done with -history 1 and -history 2.

The '-history 4' switch will display patch status for those patches that have been either explicitly installed or effectively installed. It does not report on missing patches.

The '-history 5' switch displays everything from -history 4 plus the missing (non superseded) patches on each system being scanned.

| | |
|---|---|
| | For additional information on the -history switch, plus definitions of effectively installed and explicitly installed, please see Shavlik Knowledge Base Article SKB 3213:<br>http://forum.shavlik.com/viewtopic.php?t=3213 |
| [-v] | The -v switch displays additional information about why the scan engine believes a patch to be missing.<br>If the scan engine displays a particular patch as 'Patch NOT Found', and you believe the patch has been properly installed, run the scan engine again with the '-v' switch and it will display the reason why the patch failed the scan test.<br>-v data is automatically included in all output types other than wrap (see below) |
| [-o outputformat] | The -o switch controls the output format of the scan engine. Output can be generated in several different formats, including:<br>• (wrap): Outputs data to the screen (default).<br>• (tab): Outputs in tab delimited format.<br>• (comma): Outputs in comma delimited format.<br>• (xml4): Outputs in xml format.<br>*NOTE: Shavlik NetChk Analyzer for Microsoft will only output in wrap and tab format.*<br>The default (no use of -o switch) will display in a basic wrapped text output.<br>By specifying '-o tab' the output will be formatted in a tab separated value (tsv) format.<br>By specifying '-o comma' the output will be formatted in a comma separated value (csv) format.<br>When combined with the -f outfile command below, the tab and comma formatted outputs may be useful for importing to a spreadsheet for further analysis.<br>The '-o xml4' output will save each machine's results to an individual XML file. If you are scanning ten systems, ten individual XML files will be created. |

| | |
|---|---|
| | The XML files are saved in the format:<br>YYYYMMDDHHMM-IPAddress.xml<br>The -o xml4 switch will bypass any settings specified by the -f outfile switch, but will respect settings indicated by the -op switch. |
| [-x datasource] | The -x switch specifies the XML data source location for the patch assessment data.<br>By default, the scan engine will download hfnetchk6.xml (via hfnetchk6.cab) from the Shavlik website.<br>If you would like to specify an alternate location for this data file, use the -x switch and point to a local directory, network share or UNC path:<br>**Example:** -x c:\data\hfnetchk6.xml<br>This switch may be useful when executing a scan on a network that is not connected to the Internet, or when there are multiple scan engines on the network and each is configured to pull the XML file from a central location.<br>If there is no access to the Internet, and no alternate location is specified, the scan engine will look in the local directory (where the scan engine is located) for a copy of hfnetchk6.xml. |
| [-t threads] | The -t switch specifies the number of threads to use when scanning remote systems.  The default is 64. The maximum is 256.<br>*Note: Shavlik NetChk Analyzer for Microsoft has a maximum of 64 threads.*<br>Each remote system is scanned inside of an individual 'worker thread'.  The scan engine will launch one worker thread per machine it is scanning. The scan engine is capable of launching 256 worker threads simultaneously.  As soon as one worker thread has completed scanning a machine, the thread is discarded and a new one started to scan a new |

| | |
|---|---|
| | machine, thus allowing the scan engine to scan up to 50,000 machines using 256 threads simultaneously.<br>Each additional simultaneous thread that is launched consumes resources both on the scanning console and on the local network. In some cases, 256 simultaneous threads may overwhelm an older computer processor, or can flood a slow network with a lot of packets.<br>To scan WAN links, it is more efficient to reduce the number of simultaneous threads. Eight threads at a time may be an ideal number for scanning machines on a WAN, whereas 256 threads may be ideal for scanning machines on a local area network. |
| [-u username] | The -u switch specifies a username that will be presented to remote systems being scanned. This switch should be used in conjunction with the -p password switch below.<br>The username can be presented in a variety of formats, specifically:<br>• domainname\username (to use a domain account)<br>• machinename\username (to use a local machine account)<br>• ipaddress\username (to use a local machine account)<br>• workgroupname\username (to use a local machine account)<br>• .\username (this will prepend the scanned machine name to the username)<br>If each of the machines being scanned has a local acct called 'fred', and the password for fred is the same on each machine, then it is recommended to use the .\fred format for the username. (Note that although this is a prevalent configuration, it is not a recommended security practice to have each machine's local account use the same password as every other machine's local account.)<br>If the username and password credentials supplied via the -u and -p switches fail, the scan engine will attempt one additional connection to the remote system using your currently logged on user credentials. (IOW, it will use the username and |

| | |
|---|---|
| | password with which you logged on to the console machine and under which context you are running the scan engine.) |
| [-p password] | The -p switch specifies the password to be used for the -u username specified above.<br>The password is not sent across the network in clear-text. Instead, the scanning console will use the machine's existing security framework to authenticate to remote systems using these credentials over LanMAN, NTLM, NTLMv2, or Kerberos protocols, depending upon whatever protocols are configured on the scanning machine and are accepted by the target system.<br>**Note:** It is NOT a recommended practice to store passwords in script files.<br>**Examples:**<br>-u domainname\domainadmin -p Password123<br>-u .\administrator -p Password456 |
| [-pd connect_delay] | The -pd switch specifies the length of time that the scan engine will wait for a response when it tries to connect to remote machines over tcp 139 and tcp 445.<br>**Note:** ICMP is NOT used to determine machine existence.<br>The scan engine's default TCP connection timeout is 5 seconds and is suitable for normal LAN connections and most WAN connections. If your network experiences a high degree of latency, you may wish to increase this timeout value. |
| [-f outfile] | The -f switch specifies the name and location where the scan engine should output the scan result files.<br>The -f switch may be used to reference a location on the local system, a network share, or a UNC path:<br>**Examples:**<br>-f \\server1\data\scanresults.txt<br>-f s:\scanresults\domainscan.csv<br>Wrap, comma, and tab formatted output can be sent |

| | |
|---|---|
| | to a location and filename specified by the -f switch.<br>XML4 output does not respect this switch.  Instead, use the -op switch below. |
| [-op output_path] | The -op switch specifies the directory location for XML4 formatted output.  This may be a local directory, a network share, or a UNC path:<br>\\server2\results<br>s:\data\results<br>Ensure that the specified directory exists before executing a scan with this directory name. |
| [-about] | The -about switch displays the product banner. |
| [-trace] | The -trace switch enables the scan engine log file. The log file is saved to the local directory as hfcli.log. This log file is overwritten each time a scan is performed.<br>The -trace switch is enabled by default and does not need to be specified at the command line. |

# 3 EXAMPLES

This chapter provides some real-life examples of how you may use the various command switches.

| |
|---|
| **Command:** hfcli.exe |
| **Description:** Running the executable without any parameters will scan your local system for missing security hotfixes. |
| **Command:** hfcli.exe -v |
| **Description:** The -v switch will display verbose output which includes specifics about why a patch was considered not found. |
| **Command:** hfcli.exe –history |
| **Description:** The –history switch will show both missing and explicitly installed security hotfixes for the local computer. |
| **Command:** hfcli.exe -h hostname |
| **Description:** The –h switch will display a list of missing security patches for the specified machine. |
| **Command:** hfcli.exe -h h1,h2,h3 -st 2 |
| **Description:** Will display a list of installed products and service packs on the three machines named h1, h2, and h3. |
| **Command:** hfcli.exe -h host_name -history -f out.txt |
| **Description:** Will scan the specified machine name for missing and explicitly installed security hotfixes and will save the results to a file in the local directory called 'out.txt'. |
| **Command:** hfcli.exe -d domain_name -u domain\username -p password -t 256 |
| **Description:** Will scan the specified domain for missing and explicitly installed hotfixes using the username and password included at the command line. The scan engine will use 256 threads to scan 256 machines simultaneously. |

| |
|---|
| **Command:** hfcli.exe -i 192.168.1.1 -history -pt 9 -x \\server1\hfnetchk6.xml |
| **Description:** Will scan the specified IP address for missing and explicitly installed security and non security hotfixes using the hfnetchk6.xml file from server1. |
| **Command:** hfcli.exe -i 192.16.1.1,192.16.1.8 -h host_name -x hfnetchk6.xml |
| **Description:** Will scan the two specified IP addresses and the one specified machine name for missing security hotfixes using the hfnetchk6.xml file from the local directory. |
| **Command:**<br>hfcli.exe -d domain_name -ubo -o tab -f results.csv -x c:\temp\hfnetchk6.xml |
| **Description:** Will scan the machines in the specified domain for missing security hotfixes. Machines from the domain will be enumerated from the browse list only (and not the machine list on the DC). Results will be saved to a comma separated value text file in the local directory called 'results.csv', and the scan engine will use the hfnetchk6.xml file from the c:\temp directory. |
| **Command:** hfcli.exe -r 192.168.1.1-192.168.1.254 -history 5 |
| **Description:** Will scan the specified IP range for missing, explicitly installed, and effectively installed security hotfixes. Results will be returned to the screen. |
| **Command:** hfcli.exe   -x "c:\Space In Path\hfnetchk6.xml" |
| **Description:** Will scan the machine machine for missing security hotfixes using the hfnetchk6.xml file in the specified directory. Note that when referencing directories with spaces in the name, the entire path and filename must be enclosed in quotes. |
| **Command:** hfcli.exe   -fip c:\MyIPFile.txt -pd 7 -t 16 |
| **Description:** Will scan the list of IP addresses specified in the c:\MyIPFile.txt for missing security hotfixes. Only 16 threads will be used, and the connection delay is increased to 7 seconds. |
| **Command:** hfcli.exe   -fh c:\MyHostFile.txt -op c:\scan -o xml4 |
| **Description:** Will scan the list of machines from the text file 'MyHostFile.txt' for missing security hotfixes. Results will be output to individual XML files in the c:\scan directory. |
| **Command:**<br>hfcli.exe   -d domain_name -t 256 -q q123456,q654321 -o comma -f c:\out.csv |
| **Description:** Will scan the machines in the specified domain (using a machine list from the DC) for two specific patches. Machines missing these patches will be identified in a comma separated value file called out.csv. 256 threads will be used to perform the scan. |

# INDEX