--
+

NetScanTools® Pro Monthly Newsletter

www.netscantools.com

October 2016

http://twitter.com/netscantools

http://www.facebook.com/NetScanTools

http://www.youtube.com/user/netscantools

http://netscantools.blogspot.com/

In this newsletter:

News...

From the Editor...

I spent my whole October working on a fairly major release of ipPulse. The first new test I've added is a good one – checking web server operation by retrieving a webpage. The second topic is very important if you are NetScanTools Pro user on Windows 10. Please review it.

-Kirk

ipPulse 1.90 Released October 26, 2016

This release has the first major change in a long time – it can now retrieve a page from a web server, check the server status code and optionally look for the presence of static visible or hidden text. This new 'secondary' test is important because it can allow you to monitor the health of a web server and it can also help check for web page defacement. It supports both unencrypted http:// connections and secure https:// connections in addition to allowing you to connect to

non-standard ports using this notation –
http://www.example.com:8080/somepage.html

Server Status Codes are normally '200 OK', but you can set it to trigger an error on codes like 404 Not Found or 500 Server Error. You can optionally put in a string of text to check for in the web page. If the text is not found, it will trigger an error. The text must always be in the page either visible or hidden – we search the whole page.

Visit http://www.ippulse.com/ to download.

ipPulse 1.90 Release Notes

- Added new secondary test: web page retrieval supporting both http and https. Unexpected server response code or the lack of a specific string (visible or hidden) in the retrieved web page can trigger an error. Server status codes generating errors are user controllable.
- New columns for webpage retrieval test: in Settings/Program Control tab/Column Visibility - URL to test, Server Response Status Code after URL retrieval is attempted and a column showing any text expected to appear in the web page retrieved.
- Target List Editor supports adding/editing new web page retrieval secondary test parameters.
- Added new defaults buttons to Primary and Secondary Test settings and to Program Control/Edit Column Visibility.
- Reformatted all settings tabs for less clutter.
- Default TCP test ports changed from 7 to 80.
- Settings icon now changed to universally accepted gear.
- Compiled and tested on Windows 10 Anniversary Edition.
- Updated documentation.
- Code signing now uses both SHA256 and SHA1 for maximum operating system portability.

Windows 10 affects NetScanTools Pro Upgrade Links

A week after we released NetScanTools Pro 11.80 users began to report problems with downloading the NetScanTools Pro installation file. It seems that the problem only affects users who had installed the new Windows 10 Anniversary edition.

Here is what happens: when you click on Help/Check for New Version the embedded web page loads as usual. If you click on any of the download links, a popup appears from the operating system asking you to 'switch to another app'. No matter what you select the only way out of it is to kill NetScanTools Pro in task manager.

The workaround do Help/Check For New Version, view the embedded webpage, then right click on one of the download link and select *Copy shortcut*. Next open a standalone web browser – Edge, IE, Chrome, Firefox - and paste the link in then start the download. The username/password box appears normally and after entering those things your download will proceed normally.

Managed Switch Port Mapping Tool v2.70 Released September 6, 2016

This release had many changes including an important simplification of SNMPv3 and improvements to stack switch reporting. Additional changes were made to gather HP specific Physical Port Type and HP transceiver information. An often requested change was made that allows you to 'multi-select' switch group items to add to a switch list. LAG/trunk interface speeds are now calculated and shown correctly. Several fixes were also completed.

About the changes to SNMPv3. In June we submitted documents required to obtain an Encryption Registration Number. That number, along with ECCN 5D992.c will allow us to distribute the SNMPv1/2/3 DLL and the OpenSSL encryption DLL that we need to support all modes of SNMPv3.

It will not make your life easier as far as all the SNMPv3 mode selection and passwords you have to enter, but you will no longer have to chase down the correct encryption DLL and you will no longer have to use the SNMP Library Manager.

Download the 'installed' version 2.70 from here SwitchPortMapper.com and install it over the top of your current installed version.
http://www.switchportmapper.com/

USB version users need to use the Help Menu/Check for Update selection to obtain the upgrade patch.

2.70 September 6, 2016 release notes:

- SNMPv2 is now the default.
- Changes to SNMPv3 to allow you to set it up without having to download and install libeay32.dll. Simplified SNMPv3 settings window.
- Switch List Editor now allows multi-selection of 'switch group (switch+server/router 1+server/router 2)' items to add into switch list.
- HP Transceiver information is now retrieved and displayed in the web page report for the switch. It is also saved to the history database.
- HP Physical Port Type enhanced descriptions for Type column are now shown in addition to generic port types like Ethernet(6).
- Entity Mib stack and chassis data now retrieved and saved in history database.
- Improvements to the switch stack reporting method. Additional switch brands beyond HP and Cisco will now report. Simplified methods of obtaining model/serial/revisions etc. are a byproduct. Generic switch stack report added to web page report.
- Asset number and service tag number added to web page report.
- Tech Support SNMP Walk tool: fixed occasional crash problem cause by data and the target field now grays out when in use.
- Improved DNS resolver 'save to database' speed.
- Prohibited sorting columns or activating right click popup menu items while switch is being mapped.
- Speeds of LAG/Trunk interfaces are now calculated since most switches do not report the true speed.

- Fixed problem displaying cell colors for duplex column when previous mapping is reloaded from history database.
- Minor internal speed enhancements when in SNMPv2 and SNMPv3 bulk walk modes.
- Web page report now correctly shows 'down' interface count.
- Fixed obscure problem with VLAN indexed community names for Cisco mappings.
- Updated SQLite to version 3.14.1
- Updated MAC address/Manufacturer database.
- Code signing now uses both SHA256 and SHA1 for maximum operating system portability.

NetScanTools Pro 11.80 released August 4, 2016

This version has a new tool, a revised tool and a change to the way WinPcap compatible interfaces are selected. It is also the first release to include the ability to use the authPriv encrypted level of SNMPv3.

The new tool is an IPv6 routing table tool. It shows the IPv6 routes for operating systems that allow us to access that information. *That does not include Windows XP – by the way, NetScanTools Pro still runs on XP, but not for much longer. It's been over two years since XP was deprecated by Microsoft, so do not count on any of our newer software releases working on XP unless specifically addressed in the release notes.*

The tool with major revisions is the Real Time Blacklist Check tool. Instead of a text oriented output, it now uses a grid and it is now multi-threaded which means it gathers results much faster and also queries more RBL servers simultaneously.

WinPcap interface selection has always been a problem and the old method relied on you choosing the IPv4 address in the dropdown list. Now we show the actual interface name and show the IPv4 address in parenthesis. We no longer try to match the IPv4 address from the list with the available interfaces, we use the interface name instead. This is more reliable than the old method.

There are a number of other smaller changes and fixes.

Please update soon. You will need an active maintenance plan to do so. Click on Help/Check for New Version for the download links to the full installer. USB users are downloading an upgrade patch.

Speaking of the full installer – save it in a safe place and replace any old versions. We constantly run across users who have reinstalled or moved their software to a new computer and they do so by using an old installer. Sometimes the installer is many, many versions older - so SAVE the latest one and discard the old ones!

11.80 Release Notes

- Compiled on Windows 10.
- New Tool: IPv6 Routing Table.

- Significant change to the way WinPcap compatible interfaces are listed and chosen. Layout of some tools had to change to support longer selection box. Opening and using a WinPcap network interface no longer depends on matching the IPv4 address.
- We now test to verify that the official WinPcap service or the alternative npcap or Win10Pcap services are running.
- Realtime Black List Check tool completely rewritten with new user interface and it is now multithreaded for increased speed.
- SNMP Core and Advanced tools now have simplified SNMPv3 options. SNMP DLL now has libeay32.dll added and SNMP Library Manager was removed. ECCN 5D992.c
- SNMP Scanner, SNMP Dictionary Attack and Protected Storage Viewer have updated grid controls and are now prevented from sorting by clicking on the column header while the tool is working. Exporting with Microsoft Excel schema has been updated - simply 'open' the XML file from Excel (do not import it). SNMP v1+v2c setting is now properly saved.
- ARP based tools now confirm that the target IPv4 addresses are within the same subnet as the chosen WinPcap interface.
- ARP Scan now automatically sorts by the IP address column when complete.
- Whois changed so that if whois server does not respond, it times out and automatically stops.
- Assigned IPv6 Teredo server is shown in IPv6 Compatible Interfaces.
- Corrected privilege problems with writing to certain parts of the registry during registration process.
- Updated SQLite to version 3.13.0
- Updated MAC address/Manufacturer database.
- Updated IP to Country database.
- Code signing now uses both SHA256 and SHA1 for maximum operating system portability.

NetScanTools Products and Windows 10

All of our products have been tested on Windows 10 in it's various iterations both 32 and 64 bit. That includes the new Windows 10 Anniversary edition. Most software is now being built on Windows 10.

NetScanTools Pro, NetScanTools LE, NetScanTools Basic, ipPulse and the Managed Switch Port Mapping Tool have all been recently compiled on Windows 10. All development is now done on Windows 10.

Contact Information

If you have any questions or suggestions, please feel free to email.

Northwest Performance Software, Inc.
PO Box 1375
Sequim WA 98382
(360) 683-9888
www.netscantools.com

sales [at] netscantools [dot] com