NetScanTools® Pro Monthly Newsletter

www.netscantools.com

July 2014

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've got a release of the Switch Port Mapper and NetScanTools Pro coming very soon. I am finishing up the changes soon. I hope you are having a good summer!

-Kirk

Managed Switch Port Mapping Tool 2.34 Released July 9, 2014

This release fixes several problems and adds a color coding key. We addressed problems importing switch lists. It also addressed a fairly rare issue where the VLAN, IP address, hostname columns would be so wide from the data supplied by the switch that they would be unmanageable. We also added a color coding key popup window to explain the colors that appear in some results cells. Access the color coding key through the right click menu. We also fixed a problem

where occasionally the Last Changed Time Column would show negative numbers.

Changes in this release, v2.34 July 9, 2014:

- -Importing a Switch List has been improved. Any problems importing the list are now specifically detailed, ie. SNMP device parameters not present or Switch Group not present. New Save button gives you a way to save the import errors to a text file. Problems with cancelling out of Switch List Import has been fixed. Problem with reimporting a list fixed.
- -Corrected problem where in some cases the VLAN, IP Address, and Hostname columns would be so wide that the column widths could not be reduced. There is a new checkbox in Global Settings that limits these column widths to twice the header text width. The checkbox is enabled by default.
- -Improved message text where Ping Sweep is enabled and no targets are specified.
- -Added new right click option to 'Display Cell Background Color Coding Key'.
- -Web browser switch report now mentions the way to view the color coding key.
- -Last Changed Time column values will no longer occasionally appear negative. They will always be positive or indeterminate.
- -The database 'tempSwitchList.db3' is now deleted on program exit.
- -Updated SQLite to version 3.8.5
- -Updated MAC address/Manufacturer database.

Get the new v2.34 release at SwitchPortMapper.com.

Using the Port Scanner in NetScanTools Pro®

Lately we have had some user questions about using the Port Scanner Tool in NetScanTools Pro. We have heard questions like “it scans some devices fine but other devices show a message about no results and to check WinPcap operation”. But like any tool, before you use it, you need to decide what you are looking for and which part of the tool will get you the answer you are looking for.

There are five (5) modes that the Port Scanner can operate in and there are two different scan patterns plus the ability to scan a list of targets.

The TCP Full Connect mode is not stealthy – as you can see by the name, it makes a full TCP connection to the port and it waits during the ‘Connect Timeout’ period for the connection to be established. If the port has a some program or service listening, the connection will be made then closed after the ‘Wait After Connect’ time period* has expired. This gives us a chance to collect and record any login or other banners that might be sent by the listening service. Note that the WinPcap Interface IP is NOT used in this

mode. **'Wait After Connect' is only used in TCP Full Connect mode, it is not used in the other modes because no connection is made.*

UDP mode is a little more 'stealthy'. Since UDP is a connectionless protocol, but nevertheless, it can be detected by programs looking for scanning. It works by sending a short UDP packet to a port and listening for an ICMP 'port unused' message or no reply at all. No reply can mean one of several things: 1. There is no listening service on the port 2. The message we sent does not conform to the format it expects. 3. No ICMP port unused messages are ever sent back by the target, so little can be learned UNLESS a response comes back. WinPcap Interface IP is used in this mode to listen to replies from the target. We listen for responses for the time period defined by 'Connect Timeout' then it stops listening for response from that port.

TCP Full+UDP Ports is a combination of the previous two modes together.

TCP SYN Half Open mode is more 'stealthy' than TCP Full Connect because only one packet is sent to the port: the SYN flagged TCP packet intended to begin the process of building up a TCP connection. If you are interested in finding out what TCP programs or services are listening to ports, this is probably your best mode to use – however, it uses WinPcap to send and listen for responding packets, so you need to make sure that the WinPcap Interface IP that you have selected is the route packets should take to get to the target. For instance, if you have more than one interface or if you have a virtual machine running on your machine, you need to check the WinPcap Interface IP. Since a TCP connection is not fully established, no banners are collected. You can see that the port is active and also if the port is active and the connection actively refused. We listen for responses for the time period defined by 'Connect Timeout' then it stops listening for response from that port.

TCP Custom Scan is the one that is confusing some users lately. This special mode gives you the ability to independently set each of the six header flags in the TCP packet header. How the target will respond is entirely operating system dependent. Some operating systems will respond to a specific flag combination and others will not. For instance, a Windows 2003 Server being scanning with the FIN flag set will respond with a TCP packet with ACK/RST set for the ports with listening processes. Other ports with no listening processes will not respond at all. If you are looking for a way to find out what is listening to a port on the target, you are better off using one of the other modes. This scan mode is designed for testing how targets respond to malformed TCP packets. Just like the TCP SYN mode, it depends on WinPcap so you need to make sure the right WinPcap interface is selected when scanning a target. We listen for responses for the time period defined by 'Connect Timeout' then it stops listening for response from that port.

About the two scan patterns: the most simple is **Scan Range of Ports**. This pattern scans every port in the range you have specified from the start port through the end port. This applies to any of the scan modes you have selected and if your range is large, it can take a long time. **Scan Common Ports** is designed to give you a way to scan a predetermined set of ports that are non-contiguous. You can edit that list of ports and that list can be

separated into TCP or UDP ports. The default list has ports most commonly used by Windows computers.

To scan a set or list of targets devices (each with different IPs), you need to first create a target list by pressing Edit Target List. After your list of targets is defined, save it and decide which scan mode and pattern you are going to use. Next check the checkbox labeled **Use Target List When Scanning**. Now press Scan Range of Ports or Scan Common Ports.

Port Scanning is a powerful way to see what is running on a target machine, but in order to do it right you need to understand what each scan mode is for and how to use it. Hopefully this article clears up some of that confusion.

As always, please be sure you have the target device owner's permission before scanning the target device.

NetScanTools® Pro Version 11.61 released May 9, 2014

This release fixed an urgent algorithm problem in the Whois tool that was introduced in v11.60. And we added 50 new top level domain Whois servers in addition to the 180+ added in v11.60 – the IANA has been busy. This includes servers for new TLDs like '.wtf' and '.fail'. Another minor change is that the DNS entry boxes labeled 'DNS Server' now all accept up to 48 entries. Some were only accepting 16 before old entries would age out of the list. As usual, the other databases were all updated.

Looking for NetScanTools® Pro Version 11.70 Suggestions

We already have some new tools in work for v11.70, a DNS tool and an IPv6 tool, but we are always looking for suggestions. Tell us what you need and maybe it can become a tool in NetScanTools Pro. There are no guarantees that your suggestion will be implemented, but send an email to support at netscantools dot com if you have a suggestion for a change, improvement or new tool.

You have the NetScanTools® Pro Maintenance Plan, but you are still many versions behind – why?

We see this all the time when people register. We see it when they renew their maintenance plan - we check the logs and see that they have never logged in and downloaded updates. For whatever the reason, the question remains, why are they installing 11.43 (for example) when we are at 11.61?

There are many good reasons to install the latest version: First of all is bug fixes, secondly there are new tools introduced with each .1, .2, .3, .4 etc. edition and thirdly, there are database updates.

OK – A Quick Review on upgrading to a new version. First thing you need is an active NetScanTools Pro maintenance plan. Start NetScanTools Pro

and click on Help/Check for New Version. An embedded browser window opens up on the right side of the program. Click on the download link, a popup window appears. Enter your login credentials (shown to you in the program right above the embedded window) and download the zip file. Exit NetScanTools Pro and run the contents of the zip file which is actually a full install. Restart it and verify the latest version.

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