NetScanTools® Pro Monthly Newsletter

www.netscantools.com

January 2018

http://twitter.com/netscantools

http://www.facebook.com/NetScanTools

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

http://netscantools.blogspot.com/

In this newsletter:

News

News...

From the Editor...

I finally finished the new NetScanTools Pro 11.84 release. Check out the new SMB Scanner tool described below – it is what took so long to complete the release – well, that and the holiday season.

Also, remember that due to changes in the Windows operating system you must install WinPcap or Npcap on the host computer prior to using NetScanTools Pro USB. See the related topic below.

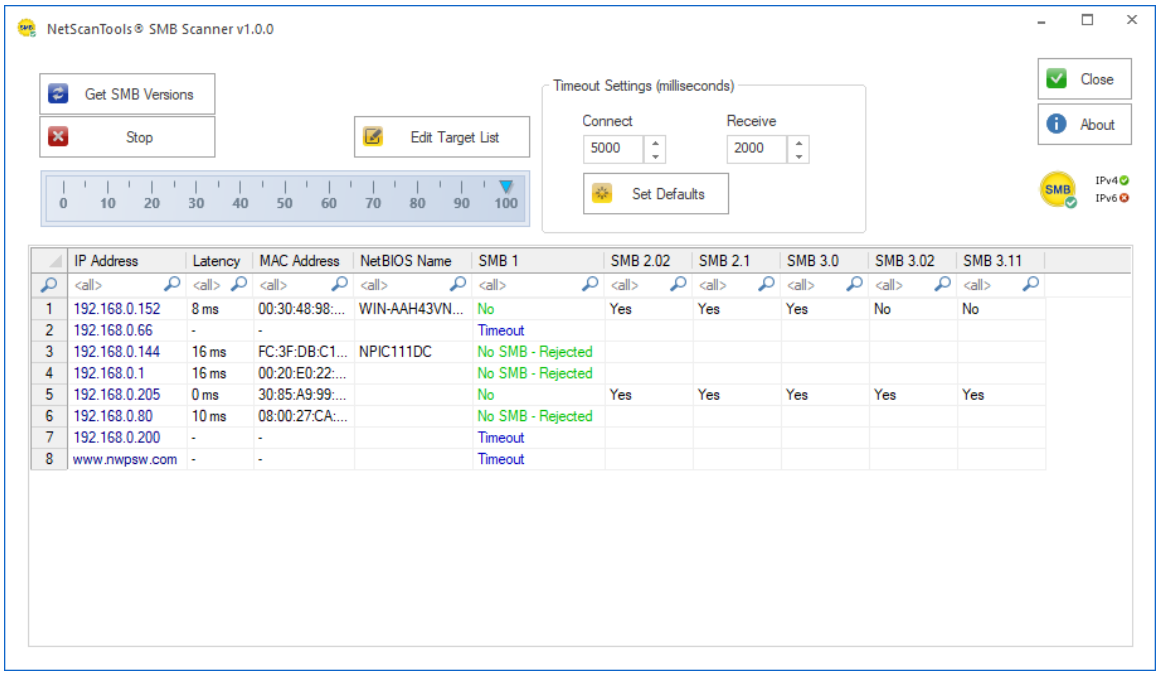
-Kirk

NetScanTools Pro 11.84 released January 25, 2018

This release adds a new tool and enhances another.

The new tool is an SMB Scanner. What does it do? It tries to connect to the SMB port on the target. If it connects, it asks the target which versions of SMB are supported. IPv4 targets and hostnames are currently supported. IPv6 will be added later.

Back when Wannacry came around we had many requests for this type of tool. And this is what it looks like:



What else does it do? It shows connection latency and the MAC address and NetBIOS machine name if the target also supports NetBT. Of course you have a right click menu for exporting, printing and copying results.

The Network Neighbors tool was enhanced. We have observed that the local neighbors (remember this is IPv6 only) were not completely populated with known neighbors. The solution is to introduce a method of getting those neighbors to talk with us. There is a new button to 'mPing' (multicast ping) the link local network and get them talking. Select the network interface of interest and press the button. After the ping is sent it waits 10 seconds for things to stabilize to update the display.

There were many other changes and fixes listed below. If you have an active maintenance plan you can download 11.84 through the Help menu/Check for New Version.

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!

11.84 Release Notes

- New SMB Scanner Tool: a launched App that accepts a set of IPv4 addresses or hostnames and rapidly scans them for SMB (server message block) support and then identifies which versions of SMB are supported beginning with insecure version 1.
- Network Neighbors: Added Discover Neighbors and Refresh button which sends an IPv6 multicast Ping through the selected interface to rapidly find all link local IPv6 devices. The results get updated with the responders and show Entry Type 'Reachable'.
- DNS Tools - Advanced: fixed gray out of IPv6 Address Validation button.
- Firewall Rules: Parsing of UDP protocol corrected.
- File menu/Accessibility: corrected operation of left control panel operation when a tool is selected. Added missing tools and added SMB Scanner.
- RFC Reference: several RFCs added.
- Whois: Remove Legal Notices and Advertising checkbox state is now retained. Results text 'jumping' issue has now been fixed - if you did a Whois, then scrolled to the bottom and tried to select text, it would jump back to the top without selecting the text - but only the first time you tried to do it.
- Changed methods of determining which operating system is hosting the software.
- USB Version only: improvements for software launch process.
- Updated SQLite to version 3.22.0
- Updated MAC address/Manufacturer database.
- Updated IP to Country database.
- Updated dates in all programs to 2018.

Managed Switch Port Mapping Tool v2.79.1 released December 11, 2017

Managed Switch Port Mapping Tool v2.79.1 is a minor update that had a fix to the new dot1x column data display algorithm. It also updated the MAC Address/Manufacturer database.

Download the 'installed' version 2.79.1 from 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. Please see important USB version topic in this newsletter.

Managed Switch Port Mapping Tool v2.79 released December 4, 2017

Managed Switch Port Mapping Tool v2.79 adds a new IEEE 802.1x column (dot1x), improves HP trunk/LAG reporting and an algorithm change to compensate for a switch data reporting problem.

New dot1x column – this shows information about the dot1x configuration on a per port basis. Keep in mind that implementations do vary slightly between manufacturers and we are only reporting the values we find at the moment. Add the column by clicking on Settings and Tools menu/Column Order and Visibility Editor.

HP trunk/LAG reporting – we now display manually created trunks that do not use LACP. These trunks are shown with the prefix Trunk -> in the interface type column.

Cisco Small Business series switches of the SG220 family were not showing MAC addresses or the columns depending on the MAC addresses. This is due to a problem with the data they report which is inconsistent with other SB series switches, so we now compensate for this issue.

Here are the changes in this release.

- Added new dot1x column to display IEEE 802.1x information. See menu item Settings and Tools/Column Order and Visibility Editor.
- Improved HP trunk/LAG reporting by now reporting manual trunks that do not use LACP. These types of trunks are prefixed by Trunk -> in the type column.
- Certain models of Cisco Small Business switches like SG220 series do not correctly report the status of a learned device mac address. Algorithm changes were made to allow for this issue.
- All columns required by 10SCAPE export are now included in the default column set.
- Algorithm change to Export to 10SCAPE.
- Last switch results after mapping a switch list now have column widths automatically size.
- SNMP Walk Tool now has dot1x preset.
- Fixed problem graying out Export to XML button in Review History.
- Updated MAC address/Manufacturer database.

Windows XP Support Ending

It has been nearly 4 years since Microsoft stopped supporting Windows XP and we have now run into issues that mean we have to stop supporting it – at least for the USB versions. When we release the next NetScanTools Pro and Managed Switch Port Mapping Tool versions, we will no longer test on XP and the USB versions will require Windows Vista or newer for operation.

NetScanTools Pro USB Version requires WinPcap or Npcap installed on the host

I guess it was inevitable. Since before 2010 we have included special version (last updated in 2010) of WinPcap on the NetScanTools Pro USB version distribution. This WinPcap self-installs a driver at run time, hence our longstanding requirement for using 'Run as administrator'. Apparently it is no more. At least on Windows 10 and probably other versions of Windows that are being updated. Some recent change in Windows prevents this self-install and driver run from happening.

Since WinPcap is no longer being updated, you have two options. If you have a USB version older than 11.82 you will need to install regular WinPcap from winpcap.org on the host if NetScanTools Pro gives error messages. If you have 11.83 (or newer) you can also install Npcap in WinPcap compatibility mode as an alternative to WinPcap. Npcap is under active development.

We cannot distribute Npcap due to licensing. You must download it and install it yourself.

Bottom line: the host must have WinPcap (winpcap.org) or Npcap (nmap.org/npcap) installed for NetScanTools Pro USB version to work.

Using npcap instead of WinPcap for NetScanTools Pro/LE (revised)

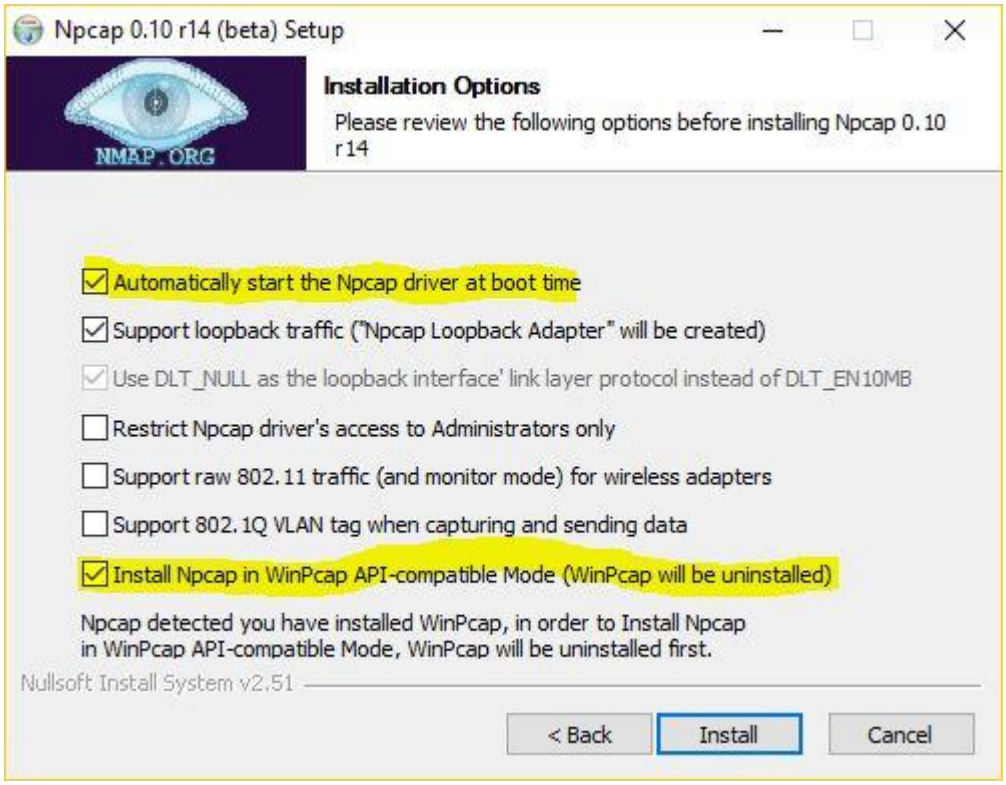
WinPcap has not been significantly worked on by its maintainers for several years now and is getting stale. While it still does work on Windows 10, I would not expect that work forever. Case in point: during the Windows 10 betas the NDIS 5 portion of the network software was deprecated for a version or two. This broke WinPcap 4.1.3. But some changes were made in Windows and WinPcap has worked again for a number of major Windows 10 revisions including the latest Creators Update. But that could easily change.

Npcap is the solution.

Npcap is a WinPcap fork created and supported by the nmap people. It is based on the newer and faster NDIS 6 and has had many releases even this year. We cannot distribute it with our software, but you can download it as an end user.

How to use install npcap instead of WinPcap:

1. Do not uninstall WinPcap!
2. Download the latest npcap installer from nmap.org/npcap
3. Install npcap and be sure to use the settings highlighted in yellow (if you are using NetScanTools Pro in a Virtual Machine, like VMware we recommend clearing (uncheck) the 'Support loopback traffic' option. Use 'bridge' mode with VMs.



What to do if there are problems installing npcap. If there is a problem it is because WinPcap could not be totally removed. This is what to do:

Try this manual removal of WinPcap – especially if WinPcap has been 'uninstalled':

1. Open an Administrator command prompt (or PowerShell) and type> net stop npf followed by enter - you may see a message about it successfully stopped or not found - either is good. Close the command prompt.

2. Remove the directory c:\program files (x86)\WinPcap if it exists (64 bit OS) or c:\program files\WinPcap (32 bit OS).

3. Search for and delete all instances of packet.dll and wpcap.dll in c:\windows. You may find them in c:\windows\system32 and in c:\windows\SysWOW64. Also delete c:\windows\system32\drivers\npf.sys (do not delete npfs.sys - be careful!)

4. open regedit. Remove HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\WinPcap (64 bit OS) or Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WinPcap (32 bit OS)

5. Remove HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst (64 bit OS) or Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst (32 bit OS)

6. Remove HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\npf and close regedit.

7. Reinstall winpcap downloaded from www.winpcap.org. Reboot and try NetScanTools Pro and Wireshark.

8. Once they have been verified to work, try installing npcap again using the earlier steps.

Tip: What to do when switches partially map ie. show few MAC Addresses

Sometimes you may run into a switch that is configured the same as other switches that map fine, yet when you map it you see everything but the MAC address column and columns that depend on the MAC addresses like IP address and hostname.

The problem may be that the switch is too busy. The default setting for Bulk Reps is 8 which means that we make one request and the switch can reply with up to 8 responses combined in one packet. Try reducing that value (see switch settings) to 2 or even 1.

A customer ran into this issue recently with very busy stacked Cisco 3850 running IOS-XE Software, Version 03.06.06E RELEASE SOFTWARE (fc1) and solved it by reducing that value to 2.

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