NetScanTools® Pro Monthly Newsletter

www.netscantools.com

July 2018

http://twitter.com/netscantools

http://www.facebook.com/NetScanTools

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

http://netscantools.blogspot.com/

In this newsletter:

News

- **Managed Switch Port Mapping Tool 2.81 Released July 18, 2018**
- **What happened to WHOIS? Hint: GDPR**
- **Network Shares – SMB tool deprecated by Windows changes**
- **SwitchPortMapper.com now HTTPS**
- **NetScanTools Pro 11.85 released April 18, 2018**

News…

From the Editor…

Working on new release of NetScanTools Pro. Still summertime!

-Kirk

Managed Switch Port Mapping Tool 2.81 Released July 18, 2018

This is a major/minor release that could be called the VLAN release – with other things customer requested features added. There are only a few small fixes.

We have added a new "Native VLAN" column and changed the "Assigned VLAN" column to more accurately represent what it actually is: "Egress VLANs" (current egress VLANs or failing that, static egress VLANs). The "VLAN" column itself remains the actual VLAN associated with the each attached MAC address (although because of the way Cisco IOS reports VLAN assignments, this column shows VLANs for ports even though nothing is attached to them).

Another improvement has to do with the reported VLANs for Juniper switches. In the current version an EX2300c will show VLANs with large numbers that make no sense. These large numbers are mapped by the bridge and now we have corrected this so that the VLAN name followed by internal VLAN number and VLAN Tag are shown as they are for the EX2200 series.

Did you know that you can now put your own custom logo/banner on the top of the web page reports instead of our logo? Yes, you can do it – visit Global Settings.

If you are a Switch List user, check out the Switch List Editor. It now shows the switch alias next to the switch IP. That makes it easier to see which switches are in the list. Another addition to the editor is the ability to specify where switch XML files are saved on a per-list basis.

The Database Maintenance window has been simplified to remove direct user access to certain tables that, if they were modified, would cause problems with switch lists.

We added additional methods of populating the Duplex Mode column (now simply called 'mode' column). Unfortunately, we need to make a small change which will result in v2.81.1 during the week of 7/30/18.

Don't forget: Windows XP/2003 support is gone as of version 2.80.3. It will not run on those operating systems. You have had 4 years to move to a newer Windows OS.

Changes in 2.81

- New user defined column headings. Change them from within the Column Order and Visibility Editor.
- Database Maintenance window has been simplified.
- Switch Lists can now have a unique XML file save directory. Use the Switch List Editor to specify. The location entered does not override a file save directory specified from the command line.
- Fixed problem where non-responding switches in Switch List were not noted in the final web browser report. The row was blank.
- Switch List Editor now shows switch alias for each switch in the list.

- Switch List Top Level Editor (where you see all the Switch Lists) now keeps the selected Switch List highlighted after editing the Switch List. You do not have to reselect it in order to map the list manually after editing.

- Added new Native VLAN Column. Note the existing VLAN column shows the VLAN each MAC address is currently using.

- Assigned VLAN column renamed 'Egress VLANs'. Only current egress or static egress VLANs are shown in this column.

- Added new Untagged VLAN column.

- Improved Juniper VLAN reporting for EX2300-c series and related switches.

- Improved duplex mode reporting for Extreme Networks, Netgear and similar switches that do not support dot3StatsDuplexStatus.

- Trunking Status column renamed 'Cisco Trunking Status'. Ports that are not trunking are now labeled 'Access' instead of 'Not Trunking'.

- Voice VLAN column renamed 'Cisco Voice VLAN'.

- Port Security column renamed 'Cisco Port Security'.

- A user defined web page report image (banner/logo) can now be set in Global Settings. GIF image format is currently the only image format supported.

- Minor changes to startup version check to better support https.

- Updated SQLite to version 3.24.0

- Updated MAC address/Manufacturer database.

Click on Help menu/Check for Update to get the latest version. USB version users will be downloading a patch – follow the directions carefully. Installed version users will be installing over the top of their current installed version.

What happened to WHOIS? Hint: GDPR

May 25 changed WHOIS, probably forever. WHOIS is a tool that predates the web. It operates by sending a text string to port 43 on any of 100s of WHOIS servers and retrieving back the response. It was most useful in showing who was responsible for a domain name or an IP address. For those of us working ecommerce to validate buyers, we could see if a domain name matched up to the owner or their business. Law Enforcement also used the IP address mode to find who owned an IP address. In the 1990s and early 2000s you rarely saw any attempts at preserving the privacy of a domain or IP address owner.

May 25, 2018 was the date of full implementation of the General Data Protection Regulation (GDPR) in the EU. As a response it appears that for domain searches, full privacy is now the rule rather than the exception – even for non-EU domain holders.

IP addresses are usually not private in that they show the ISP or the business they are assigned to. The domain name privacy is so pervasive now that only one of my searches in the last month has come up with anything other than full privacy.

This query for a German domain is typical with only the very basics – the Name Servers and the status. Note that it does not even tell you when the domain expires – I cannot believe they consider that fact private information. They direct you to their web base whois lookup for more information. But even that is limited. They will not give you much more only after making a request. Thanks GDPR.

```
Domain: ???????.de
Nserver: b1.wpns.hosteurope.de
Nserver: b1.wsns.hosteurope.de
Status: connect
Changed: 2008-01-10T02:41:54+01:00
```

At least Godaddy tells you more about the new policy:

```
IMPORTANT: Port43 will provide the ICANN-required minimum data set per
ICANN Temporary Specification, adopted 17 May 2018.
Visit https://whois.godaddy.com to look up contact data for domains
not covered by GDPR policy.
```

Network Shares – SMB tool deprecated by Windows changes

It was bound to happen someday. This old tool depends on some older operating system functions that allowed you to 'crawl' the Microsoft Windows Network domain and obtain a list of workstations/servers. Then it contacted each one found and asked for the shares both visible and hidden. **It still works if your computer is the 'master browser'** (Open an administrator command prompt window and enter the command net view. If it is the master, a list of computers will quickly appear – otherwise it slowly reports only the single host or errors out.). This tool depended on the Computer Browser service operating and as I understand it the Computer Browser only talks SMB1. So after Wannacry hit, SMB1 has been quietly removed from Windows (except for XP). Now you are lucky to get a few rows "Microsoft Terminal Services", "Microsoft Windows Network", the domain along with the shares of the computer running NetScanTools Pro. It clearly no longer gives a long list of computers and their shares. Workaround? -none that I know of.

Microsoft explains their SMB1 position here:
https://support.microsoft.com/en-us/help/4034314/smbv1-is-not-installed-by-default-in-windows

The new SMB (version) Scanner works fine because it communicates directly with the SMB port and asks for the list of supported SMB versions.

SwitchPortMapper.com is now HTTPS

Chrome among others now calls plain old http port 80 websites insecure. As a result of this push by Google we have converted SwitchPortMapper.com to https and put a lot of work into speeding it up.

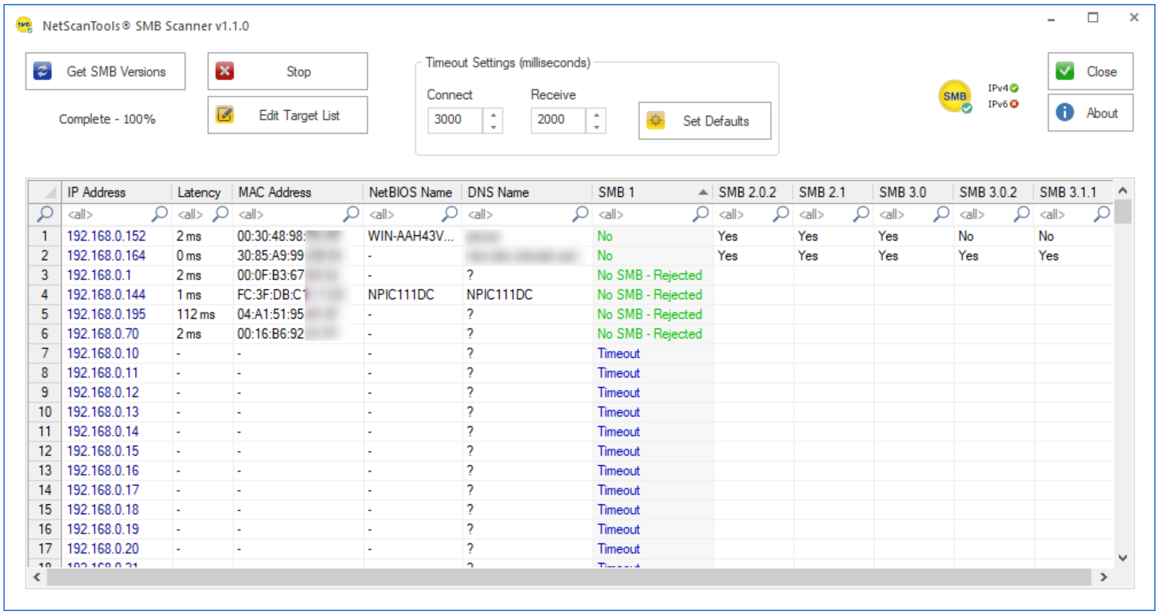
NetScanTools Pro 11.85 released April 18, 2018

This release enhances both the new SMB Scanner and the SSL Certificate Scanner.

Changes in 11.85: The SMB Scanner has a new 'DNS Name' column added and the progress control was changed – the underlying method of target list storage was changed from a simple text file to an SQLite database table.

What does the SMB Scanner tool do? It attempts 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:



Complete - 100%

Timeout Settings (milliseconds)

Connect 3000

Receive 2000

	IP Address	Latency	MAC Address	NetBIOS Name	DNS Name	SMB 1	SMB 2.0.2	SMB 2.1	SMB 3.0	SMB 3.0.2	SMB 3.1.1
	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>	<all>
1	192.168.0.152	2 ms	00:30:48:98:[redacted]	WIN-AAH43V...	[redacted]	No	Yes	Yes	Yes	No	No
2	192.168.0.164	0 ms	30:85:A9:99[redacted]	-	[redacted]	No	Yes	Yes	Yes	Yes	Yes
3	192.168.0.1	2 ms	00:0F:B3:67[redacted]	-	?	No SMB - Rejected					
4	192.168.0.144	1 ms	FC:3F:DB:C[redacted]	NPIC111DC	NPIC111DC	No SMB - Rejected					
5	192.168.0.195	112 ms	04:A1:51:95[redacted]	-	?	No SMB - Rejected					
6	192.168.0.70	2 ms	00:16:B6:92[redacted]	-	?	No SMB - Rejected					
7	192.168.0.10	-	-	-	?	Timeout					
8	192.168.0.11	-	-	-	?	Timeout					
9	192.168.0.12	-	-	-	?	Timeout					
10	192.168.0.13	-	-	-	?	Timeout					
11	192.168.0.14	-	-	-	?	Timeout					
12	192.168.0.15	-	-	-	?	Timeout					
13	192.168.0.16	-	-	-	?	Timeout					
14	192.168.0.17	-	-	-	?	Timeout					
15	192.168.0.18	-	-	-	?	Timeout					
16	192.168.0.19	-	-	-	?	Timeout					
17	192.168.0.20	-	-	-	?	Timeout					
18	192.168.0.21				?	Timeout					

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 SSL Certificate Scanner tool was enhanced both visibly and internally. Visible changes include replacement of the progress control with the new circular progress control. There was also a problem maximizing then restoring the window to previous size – that was fixed. Another visible change is the export to text (CSV or tabbed) now includes the header.

The final most important change is both visible and internal: you can now specify the target port, so if your webservers are not using port 443, no problem. In order to do this we had to change the target list storage from a simple text file to a database table.

About the ARP Scanner changes. We (and some customers) have noticed that the ARP Scanner does not always get responses from the targets even though they are active, so we worked on some changes that will hopefully elicit responses and show them.

Packet Generator and other tools have changes where a TCP packet is being defined and sent using WinPcap driver. While we were unable to reproduce this issue here because it may be somewhat hardware dependent, a user pointed out that the sequence and acknowledgement packet header values were not always what was entered. We isolated the problem and corrected it in the Packet Generator and other tools that use the WinPcap driver to send a TCP packet.

There are other changes and fixes listed below. If you have an active maintenance plan you can download 11.85 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!

11.85 Release Notes

- All tools that 'import lists from a text file' now have a check for non-ANSI text files. We can only accept ANSI (plain ASCII) text files. UNICODE format is not allowed.
- ARP Scanner now has improvements for gathering ARP reply packets.
- Corrected problem defining TCP header components Sequence and Acknowledgement in Packet Generator, Ping Enhanced, Port Scanner and Traceroute.
- Traceroute Settings Ack Number edit box now grays out as required.
- SMB Scanner: Activity indicator pointer graph was changed to a circular progress indicator.
- SMB Scanner: changed target list to a database table and now includes a new DNS hostname column. Speed improvements.
- SMB Scanner: Right click Export to Tabbed or CSV now includes the column header in the export file.
- SSL Certificate Scanner: Activity indicator pointer graph was changed to a circular progress indicator.
- SSL Certificate Scanner: Fixed problem where a maximized window did not return to original size.
- SSL Certificate Scanner: Now allows specifying a target SSL port other than 443.
- SSL Certificate Scanner: Skip on timeout checkbox now correctly grays out during scanning.
- SSL Certificate Scanner: Right click Export to Tabbed or CSV now includes the column header in the export file.
- Updated SQLite to version 3.23.1
- Updated MAC address/Manufacturer database.
- Updated IP to Country database.

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