NetScanTools® Pro
Monthly Newsletter
www.netscantools.com

August 2018

http://twitter.com/netscantools

http://www.facebook.com/NetScanTools

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

http://netscantools.blogspot.com/

In this newsletter:

News

- **NetScanTools LE 1.61 Released August 8, 2018**
- **Managed Switch Port Mapping Tool 2.81.2 Released August 8, 2018**
- **NetScanTools Basic 2.51 Released August 1, 2018**
- **What happened to WHOIS? Hint: GDPR**
- **SwitchPortMapper.com now HTTPS**
- **NetScanTools Pro 11.85 is the current release. 11.86 in work.**

News...

From the Editor...

Three releases at the beginning of the month. Working on release 11.86 of NetScanTools Pro. I've been on a semi-vacation for a good part of August after those releases in the first two weeks of the month.

-Kirk

NetScanTools® LE 1.61 Released August 8, 2018

This is a minor release that addresses a couple issues. They are small fixes – but they are important. The changes are quite similar to the changes in NetScanTools Basic 2.51.

The most important were changes to some target input fields to eliminate the possibility of crashing due to invalid input.

Ping was not displaying any message if it could not find an IPv4 address for a given hostname. That has been corrected.

SQLite was updated to the latest version as were the databases.

Changes in 1.61

- Changes to prevent crashing due to invalid input.

- Ping now properly displays message showing inability to find IP for a hostname.

- Updated SQLite to v3.24.0.0

- Updated database files.

Click on Help menu/Check for New Version to get the latest version. Install over the top of the current installed version.

Managed Switch Port Mapping Tool 2.81.2 Released August 8, 2018

This is a minor release that follows the August 3 release of 2.81.1. There are only a few small fixes – but they are important.

The fix in **2.80.1** corrected a minor algorithm problem with the Mode column (formerly Duplex Mode) where certain switches would provide an incomplete MAU table – the only things in it were the active ports.

2.81.2 addressed a problem with the Add New Group button in the Switch List Editor. It was not showing all the columns correctly. This was introduced when we added the alias column for the switch.

Another issue we fixed was in Review History/Show Mapping Differences. If you right clicked in the results and selected Export as CSV, it was using a semicolon as the column delimiter. It now uses a comma. Unless someone thinks there should be a choice between a semicolon and a comma, it will stay as a comma.

Both releases updated the MAC address to manufacturer database.

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

Changes in 2.81.2

- Add New Group in Switch List Editor now works correctly.

- Export to CSV from Review History/Show Mapping Differences now exports with comma separator instead of semicolon.

- Updated MAC address/Manufacturer database.

Changes in 2.81.1

- Minor change to duplex mode column algorithm.

- 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.

NetScanTools® Basic 2.51 Released August 1, 2018

This is a minor release that addresses a couple issues. They are small fixes – but they are important.

The most important were changes to some target input fields to eliminate the possibility of crashing due to invalid input.

Ping was not displaying any message if it could not find an IPv4 address for a given hostname. That has been corrected.

The clear history button on Graphical Ping did not work – it does now.

SQLite was updated to the latest version as were the databases.

Changes in 2.51

- Changes to prevent crashing due to invalid input.

- Ping now properly displays message showing inability to find IP for a hostname.

- Graphical Ping clear history list button now works.

- Updated SQLite to v3.24.0.0

Click on Help menu/Check for New Version to get the latest version. Install over the top of the 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.
```

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.
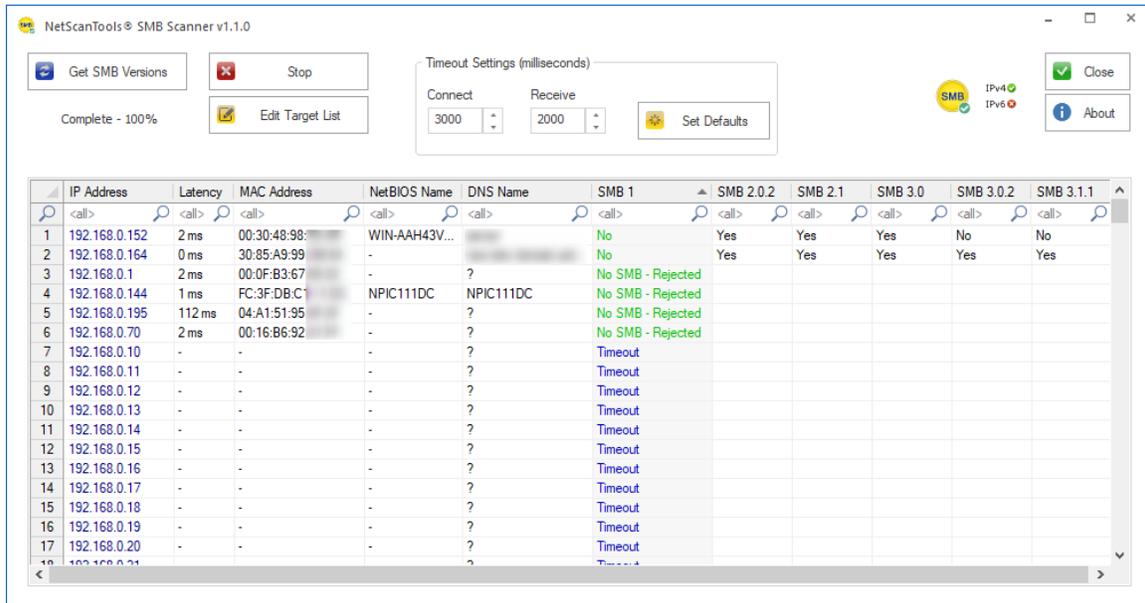
NetScanTools® Pro 11.85 released April 18, 2018

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:

NetScanTools® SMB Scanner v1.1.0

Get SMB Versions | Stop | Timeout Settings (milliseconds) | IPv4 ✓ IPv6 ✗ | Close
Complete - 100% | Edit Target List | Connect 3000 Receive 2000 | Set Defaults | About

	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:	WIN-AAH43V...		No	Yes	Yes	Yes	No	No
2	192.168.0.164	0 ms	30:85:A9:99:	-		No	Yes	Yes	Yes	Yes	Yes
3	192.168.0.1	2 ms	00:0F:B3:67:	-	?	No SMB - Rejected					
4	192.168.0.144	1 ms	FC:3F:DB:C1	NPIC111DC	NPIC111DC	No SMB - Rejected					
5	192.168.0.195	112 ms	04:A1:51:95:	-	?	No SMB - Rejected					
6	192.168.0.70	2 ms	00:16:B6:92:	-	?	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					

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 <u>old</u> versions. We constantly run across users who have reinstalled or moved their software to a new computer and they do so by using an <u>old</u> installer. Sometimes the installer is many, many versions older - so SAVE the latest one and <u>discard the old ones</u>!

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