**NorthWest Performance Software, Inc.**

# May 2008 Newsletter

**In this newsletter:**

- **NetScanTools Pro 10.60 Released**
- **Maintenance Plan – NetScanTools Pro**
- **NetScanTools Pro USB Version**
- **Power User Tip for NetScanTools Pro – Using SNMP Dictionary Attack**
- **How to Upgrade NetScanTools Pro**
- **Current Release - Managed Switch Port Mapping Tool 1.92, March 14, 2008**
- **Status of NetScanTools Pro Self-Paced Training**
- **Contact Information**

**This is our monthly newsletter.**

## NetScanTools Pro 10.60 Released

We released version 10.60 on May 14. All parts of NetScanTools Pro have now been converted from the Visual C++ 6 compiler to Visual C++ 8 (2005). This involved over a thousand internal changes and in the process we made a number of internal improvements to remove things like duplicated code.

A few of the major changes are below:

- Email Validate: many internal changes to speed it up plus the addition of bulk validate of a list of email addresses. Also added test type selection, HELO/EHLO hostname and Verbose or Short results formatting.
- Connection Detection and Ident Server: Added warning message that the port cannot be used if the port is already in use by another program.
- Launcher now shows the current handling executable for each protocol: http, ftp etc.
- Preferences/Set Web Browser now shows the default handling program for the file extension .html. Added button to reset this value to the default. This only affects viewing results in the web browser. It is independent of the Launcher HTTP setting.
- Name Server Lookup: added server response time reporting to Test Default Servers. The test default server button now grays out properly.
- Port Scanner: fixed problem where if ARP did not return the MAC address of the target or the gateway, it would keep doing ARP packet sends/waits for every port. Now it tries ARP twice, then uses the broadcast MAC on failure. Applies to all WinPcap modes on your local subnet.
- NetBIOS Info now shows Windows Vista/Server 2008 computers and MAC address is now upper case. Additional attribute decoding.
- TTCP: fixed multiple internal issues. It now works properly.
- Improved WinPcap interface selection dialog that is used when we cannot identify the interface as selected by the user under WinPcap Interface IP.
- A number of changes were made to work towards better Section 508 compliance.
- All the databases were updated and the SQLite and SNMP libraries were also updated.

You can view the full list of changes by release from within NetScanTools Pro by selecting Online/NetScanTools Pro News or going to this URL: http://www.netscantools.com/nstpronews.html

**Upgrading:** If you need help upgrading to 10.60, please see the section later in this newsletter.

## Maintenance Plan - NetScanTools Pro

**Having an active maintenance plan is important if you want to obtain the latest release.** A FULL Install of the "installed version 10.60" (not a patch) is available on our secure site for download. Those who have the USB version are supplied with a patch for download from the secure site. You must have an active maintenance plan in order to login to the secure site. See the section **How to Upgrade NetScanTools Pro** below for help downloading the current release.

One year of maintenance (beginning at date of purchase) is included with a new or upgrade license. A core benefit of the plan is the ability to download updates. In calendar year 2007 we released 6 updates mostly targeted towards Windows Vista compatibility and 5 updates in calendar year 2006. We have released two updates in 2008 and anticipate another minor release of 10.x before June is over.

**If you let your maintenance plan expire**, the cost to renew the plan increases the longer you wait. We do give a 30 day grace period after your expiration date during which the renewal cost is $75 per license. If you are unsure when your plan expires, please feel free to contact us by email or phone before renewing (see end of newsletter for contact information). You can always continue using the program even after the maintenance plan expires, but you will not get any changes or updated databases.

## NetScanTools Pro USB Version

The USB version operates the same as the installed version except you do not install it on the computer you are using it on. You run the NetScanTools Pro executable (as administrator) and everything is saved on the USB drive.

This method of using the program is invaluable to people who move from computer to computer during the course of their work. On site support technicians will find it very useful because the tools they use all the time can be used on the computer they are troubleshooting.

We supply the software on a Lexar Lighting 1GB drive. This is one of the fastest drives on the market and this was verified by our tests. It is not a U3 drive, but you can still run software from it. If you have other USB drive portable software such as WireShark, you can easily install it on the drive. We do not fill up the drive, but just in case you experience any problems, we ask that you make a full permanent backup of the drive after you register it. That way we can help you restore it very quickly if necessary.

**Learn more about the NetScanTools Pro USB version here including "sidegrade" and "upgrade" pricing for current NetScanTools Pro licensees:**
http://www.netscantools.com/nstprousb.html

# Power User Tip for NetScanTools Pro – Using SNMP Dictionary Attack.

This topic in our newsletter highlights a part of the program you may not be aware of. All tips refer to the latest version, currently 10.60.

**Did you know that you have a tool for finding the community name (password) for accessing an SNMP v1/v2c device?** This tool is called the SNMP Dictionary Attack Tool. It works by rapidly sending community names from a dictionary of common community names to the devices in a list. You can test multiple devices at the same time. Once the community name is found for a device, it is displayed and the other devices continue to be tested. Remember that anytime you do this sort of a brute force attack, you are leaving tracks in whatever intrusion detection system may be in use on the targets – **we always advise that you have permission to do a scan like this.**

**How to use the SNMP Dictionary Attack Tool**. Select the SNMP tool from the NetScanTools Pro Tools group. You will find a dropdown list below the Perform Action button. Select Dictionary Attack from the list and press Perform Action. The tool will launch but before you get started you need to define a target list. Press Target List Editor. Create a list of IPv4 addresses using the editor and press OK to save them. Now press Setup and choose the SNMP version that you will be testing against the targets. Select the WinPcap interface from the Available Interfaces list and select the attack speed. Now you can press Attack! As each community name is found, that target will have the status, community name and other parameters shown in the grid.

## How to upgrade NetScanTools Pro

We have heard from some customers that they do not know how to upgrade to the latest version or they paid for their maintenance plan and never received any upgrades. The ability to upgrade your software has *always* been right there within the software.

**How to upgrade:**
1. Prerequisites:
   - You must have the NetScanTools Pro v10.x installed.
   - You must have a **valid active maintenance plan**.
   - The software must be registered AND you must have applied the "NST Pro 10 Registration Code" email message we sent back to you – if it is not registered, our secure site will not have any login credentials ready for you.
2. Start NetScanTools Pro and click on the Online group in the left panel. Then click on the Check for New Version icon. Once the web page appears in the right pane, you will see the Login link text. (**NEW Alternative:** Version 10.54 added a Check for New Version link to the Help menu)
3. After clicking on the Login text, you will see a popup asking for a username and password. Those are found in the Login Access Credentials area as shown in the image on the next page. **The username and password ARE CASE SENSITIVE.** We recommend using copy and paste.

If your access credentials do not work please check for typos in your username or password (we recommend copy and paste). Your username is your email address that you gave when you registered and the password is the registration number.

It is also possible that your maintenance plan expired. Please contact us with the username and password you are using and we can check your status. **You must have a valid maintenance plan to download an upgrade.**

Once you have logged in to the secure server, the **full download** is ready for installation by those of you with installed versions. You will need your CDKEY/serial number to run the installer – see the About NetScanTools Pro window to get it. Please install over the top of your current installation.

USB Version users can download an upgrade patch from the secure server. The latest version of the Managed Switch Port Mapping Tool is also available for download from this window and it is publically available elsewhere on our main site.

**The image below shows where in the program you need to go to login to our secure site.**
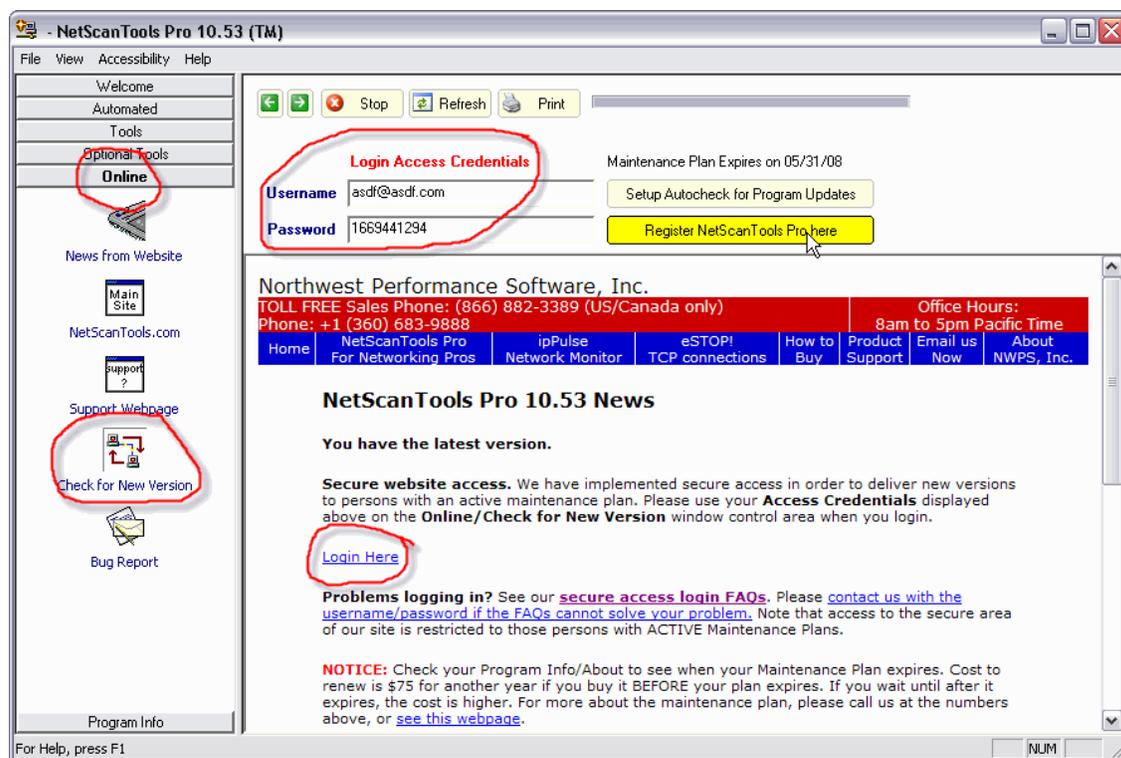


## Current Release - Managed Switch Port Mapping Tool 1.92, March 14, 2008

Releases 1.90 through 1.92 brought some fairly major internal changes to the program:

- **A redesigned Ping Sweep utility** which allows you to ping more than one range of IP addresses. You can build a whole list of IPs to be pinged, either in ranges or a single IP. We added this in response to a customer request.
- **A new Column Order and Visibility editor**. This allows you to rearrange (reorder) columns and hide columns you do not need. This was requested by a number of

customers and it was needed to add additional columns. We are making the four byte count columns and the last change column default to hidden to make room for new Spanning Tree Protocol columns (not yet added).

- **Added support for displaying Spanning Tree Protocol State.** Other parameters such as the root device MAC address and IP address are also shown on the port communicating with the root device.
- **Added more toolbar menu selections** to correspond to right click popup menu selections in a effort to become more compliant with Section 508 rules.
- **Updated HTML report to show Spanning Tree Protocol information** if available.
- **Improved accuracy of identifying connected switches** using historical data.
- **And more...**

We are working towards making this tool the leader in manufacturer independent switch mapping tools. We are well on the way towards this goal with many new additional features planned for release in 2008.

More information about the Managed Switch Port Mapping tool:
http://www.netscantools.com/spmapmain.html
You can visit this URL to immediately download the trial:
http://www.netscantools.com/switchportmapperdownload.html

## Status of NetScanTools Pro Self-Paced Training

We are partnering with the Protocol Analysis Institute to develop quality in-depth self-paced training on reconnaissance, traceback, troubleshooting and network discovery techniques using NetScanTools Pro. The course will be defined as a new "Laura Chappell presents(TM)" course to be available through NetScanTools.com, Wireshark University and Protocol Analysis Institute web sites. **Video courses are currently being recorded by Laura Chappell and should be available soon.**

## Contact Information

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

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