

July 12, 2006 Newsletter

In this newsletter:

- **Managed Switch Port Mapping Tool 1.42 released.**
- **Version 10 Maintenance Plan Renewals – Online Renewals Now Available**
- **NetScanTools Pro 10.31 is still current – version 10.4 is on the way!**
- **Post NetScanTools Pro 10.31 Database updates**
- **Training Opportunity in Australia from Laura Chappell**

This is our first newsletter since May and we hope you are having a good summer.

Managed Switch Port Mapping Tool 1.42 released May 12, 2006

New in this release

1.42 fixes a longstanding problem with XML exports to Microsoft Excel. If you had too many items attached to a port, then the height of a single row in the grid exceeded a maximum. We now limit the row height to that maximum when exporting – your data is still there, nothing is lost. There were also improvements to the feedback users receive while resolving IP addresses to hostnames including new status bar indications, better monitoring of the Stop button and a DNS lookup watchdog timer. A problem calculating the speed of gigabit and above interfaces was corrected.

About the Managed Switch Port Mapping Tool

This is a tool that can be integrated into NetScanTools Pro or used as a standalone program. It is designed to map managed network switch physical port connections to MAC addresses and with additional queries, the IPv4 addresses of attached network devices. This tool is intended for use by network administrators and other specialists who maintain managed switches. The program uses SNMP v1/v2c to communicate with any SNMP enabled switch and presents the switch mapping results in a spreadsheet-like grid.

Cost is \$99 if you own NetScanTools Pro (any version) or \$199 if you do not own NetScanTools Pro. More information about the Managed Switch Port Mapping tool is here:

<http://www.netscantools.com/spmapmain.html>

How to get the 15 day fully functional trial version:

- From within NetScanTools Pro 10.x or NetScanTools 2004 sp4 (9.4) click on Online/Check for new version. The web page in the right hand window has a direct download link to the Managed Switch Port Mapping tool.
- Or you can visit this URL to request the trial – <http://www.netscantools.com/spmaptrialrequest.html>

V10 Maintenance Plan Renewals – Online Renewals Now Available

Starting with v10, we introduced a one year maintenance plan included with the license. The initial plans began expiring February 18, 2006. Each user has a different expiration date. Your expiration date can be found on the Program Info/About NetScanTools Pro. The software will present you with a renewal reminder window at startup beginning 21 days prior to the expiration

date (assuming you have registered). You can turn off the reminder in Tools/Set Preferences (Enable Reminder Check). The reminder message was improved in 10.31.

The maintenance plan enables you to get upgrades and support. You must login with the use of the access credentials to download the upgrades from our **“Online Left Panel Group/Check for New Version”** page (the access credentials are found below the controls at the top of that window). You must renew the plan to continue to get access after your plan expiration date. **The renewal cost is \$75* per v10 license.** Please contact us by phone (360-683-9888) or email us to get more information about renewing. The contact information is at the bottom of this newsletter. **We now have online ordering for plan renewals linked from this page:**

<http://www.netscantools.com/nstpromaintenance.html>

***cost may be higher if you wait too long to renew, see web page above.**

NetScanTools Pro Version 10.31 was released on March 21, 2006.

This release concentrated on fixes and improvements in the area of registration, maintenance plan reminders, and checking for new versions. There are some user interface responsiveness fixes. The only added features are minor.

You can view the full list of changes from within NetScanTools Pro by selecting Online/NetScanTools Pro News or going to this URL:

<http://www.netscantools.com/nstpronews.html>

Upgrade to v10.31 by running NetScanTools Pro 10 and going to Online group, then selecting Check for New Version. **You must have a valid maintenance plan to upgrade to 10.31.**

Version 10.4 Status Report

One of the things that slowed down the release of 10.4 is the new SNMP Dictionary Attack Tool. It is now 95% complete. This new tool is launched from the SNMP tools window and uses a dictionary to attempt to find the community name (v1 or v2c or both) for an IPv4 device or list of devices. If successful, it shows the community name and SNMP version that was returned with that community name. You can right click for saving to XML, printing and also gathering more system information about the device after the scan is complete. The dictionary is plain text so you can add to it or rearrange it.

Other changes completed in 10.4 include a new SNMP engine for all the SNMP tools and a long list of improvements to Packet Viewer. Packet Viewer now displays ARP packets and now will save the whole packet including Ethernet headers to the database.

There have been many minor fixes too. More work will be done on the Packet Generator and much will be done to reduce the need for administrator privileges. Our goal is to have it run without admin privileges as much as possible. It will still need admin privileges to install. Our list is long, but we are targeting the end of July to complete the work.

Post NetScanTools Pro 10.31 Database Updates

We are going to be putting out database updates in between releases. I would like to do one a month if possible. The database updates include changes to the IP to Country Mapping database, the whois server database and the network interface card mac address database. There is one available now that was done in early June. Get it by going to the Online group, then click on the Check for New Version icon. Login to the secure site and download the database update patch. Exit NetScanTools Pro and run the patch. ****You must have a valid maintenance plan to get these database updates.**

Training Opportunity in Australia from Laura Chappell

Laura Chappell is a well known security trainer and business associate of ours. Her website is www.packet-level.net. This is an advertisement for a class she is conducting in Australia.

As a network and security specialist, you have conquered firewall settings, access control list settings, automated patch/update processes and system lock-down. What happens then, when someone gets through all your carefully conceived and implemented protections to plan a Trojan on the CEO's laptop? (Most likely she/he downloaded some ugly code when plugging into the Internet from home.sigh). Now you need to move into the reactive world to perform a forensic examination on the laptop, watch the traffic flowing to/from that system, and find the host that appears to have remote access to the machine. This is where the skills of reconnaissance/traceback and forensics come into play.

Everyone responsible for their organisation's network should have at least a cursory ability to trace back to a target and perform general forensic investigation procedures.

Join Laura Chappell, IT Security guru (US) as she shows you many of the skills she has taught Australian and US Law Enforcement as well as major corporations worldwide.

For training on these skills go to <http://www.frontend.com.au/net> for more information and registration details.

NETSCANTOOLS PRO ARE OFFERING A SPECIAL PRICE FOR THESE WORKSHOPS.
ENTER THE CODE NET26 TO RECEIVE BETWEEN \$350 - \$800 DISCOUNTS.

NETWORK FORENSICS

Network forensics is the process of listening in on the traffic to and from a victim system and to identify the communications to and from the victim.

You will learn to identify OS fingerprinting processes, network flooding signatures, UDP/TCP/ICMP scans, vulnerability scans, etc. Recognizing the traffic patterns of these functions and their unique signatures enables you to block these communications inside and at the border of your network.

HOST FORENSICS

So you have that compromised system on your desk - now what? Host forensics is the process of imaging the drive for off-line investigation of the drive contents. Where is the malware planted? Are any other files 'of concern' located on the victim's drive? Host forensic tools enable us to remove the 'known to be good' files from the view so we can concentrate on the questionable files. You will perform host forensic analysis on the image of a victim's drive.

RECONNAISSANCE AND TRACEBACK

Reconnaissance and traceback is used to identify the source of an attack, infection, or even spam. For example, if you find someone sending spam out pretending to be your company offering some false or offensive products, you can perform a forensic examination on the contents of the email header.

In the Recon/Traceback course, attendees perform reconnaissance on a series of email headers, identify the owner of a domain (and relationships to other domain names), determine available services on a host, identify the host's location, find out the host's ISP and more!

ABOUT LAURA CHAPPELL

Laura has been trusted by organisations that include the FBI, the US Navy, IBM, HP, Cisco Systems and Microsoft. She is an active member of HTCIA (High Technology Crime Investigation Association) and an IEEE Associate since 1990.

These 'next generation' skills will enhance your security knowledge by adding investigative capabilities to your already-impressive list of capabilities. If you are serious about protecting your network and corporate assets, then these labs are for you!

Registration details are online at www.frontend.com.au/net

NETSCANTOOLS PRO ARE OFFERING A SPECIAL PRICE FOR THESE WORKSHOPS. ENTER THE CODE NET26 TO RECEIVE SUBSTANTIAL DISCOUNTS

Other things...

Spam Filtering Issues

We are having **significant ongoing problems** with our email not getting through to our customers. Please whitelist or permit email from sales at netscantools dot com and support at netscantools dot com.

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