Protocol Analysis Institute Newsletter (by Laura Chappell)
July 2006

In this newsletter: Disney Film Announcement, Calendar (Australia one week away + HP Conference added), Article: Tools on a Stick - Reviewing The Network Toolkit by CACE Technologies, Ethereal becomes WireShark (Reminder: The Reconnaissance/Traceback self-study course is now shipping - www.podbooks.com)

ARTICLE
- Tools on a Stick - Reviewing The Network Toolkit by CACE Technologies

SELF-STUDY COURSES AVAILABLE (www.podbooks.com)
- Performing Network and Security Analysis with Ethereal (DVD)
- Reconnaissance and Traceback (Technologies and Tools) - new release

CALENDAR - 3-MONTH VIEW
(One week away!) Australia (Melbourne) – July 17-18 - Network Analysis/Host Forensics
(One week away!) Australia (Sydney) - July 19-21 - Network Analysis/Host Forensics + Reconnaissance
GET DETAILS and REGISTER NOW at www.frontend.com.au

NAST NYC - July 31-Aug 2 (www.hotlabs.org/toolkit) - space limited
NAST Seattle - Aug 7-9 (www.hotlabs.org/toolkit) - space limited
NAST Chicago - Aug 14-16 (www.hotlabs.org/toolkit) - space limited
NAST Minneapolis - Aug 28-30 (www.hotlabs.org/toolkit) - space limited

NAST Boston - Sept 11-13 (www.hotlabs.org/toolkit) - space limited
HP Tech Forum - Sept 17-21 (www.hptechnologyforum.com - registration open now)
Pre-Conference seminar and 8 conference sessions (1744, 1766-1771, 1866 and 1868)

------Details/Discount on NAST Course
The first NAST (Network Analysis and Security Toolkit) courses are completed - topics/tools covered include network forensics, traceback and reconnaissance, honeypot/IDS configurations, application sniffing, signature identification, penetration testing, network flooding, interception/redirection, password recovery, host forensics, steganography, encryption techniques, deep registry viewing, application locking, NAST system backup/maintenance.

------Ethereal Becomes WIRESHARK (www.wireshark.org)
Gerald Coombs (the creator of Ethereal) has signed on with CACE Technologies (www.cacetech.com) - Ethereal has now become Wireshark (www.wireshark.org) which is available on its own just as Ethereal was and is also included in CACE Technologies' The Network Toolkit. Ethereal was renamed because of copyright issues - all the Ethereal developers are over at Wireshark now. You can read the official press release at http://www.prweb.com/releases/2006/6/prweb396098.htm.

------Hot Tools on a Stick - Reviewing The Network Toolkit by CACE Technologies
Many of you have seen me demonstrate the cool USB earrings that contain a variety of tools for reconnaissance, analysis, forensics, etc. The USB content was defined and developed by Keith Parsons of the Institute for Network Professsionals (INP) who are my road-show partners for NAST. Hopefully Keith and his team will continue developing their Ultimate Toolkit (I will keep you informed of their developments).

In the meantime, check out The Network Toolkit by CACE Technologies. The Network Toolkit is available for US $39.95 (single download) or US $89.95 (12-month update version). I recently ordered, downloaded and played with the toolset and am impressed with the tools included, the simple GUI and the ability to run the tools from USB stick.

Note: During the installation of The Network Toolkit, McAfee had a fit with a few PUPs (Potentially Unwanted Programs) during the installation, which is to be expected.

Tools in The Network Toolkit include:

AdapterWatch (v. 1.0.1) : tool for retrieving statistics about a network adapter.
AirSnare (v. 1.2.11) : network monitor useful for tracking hosts that communicate on your network.
Analyzer (v. 3.0 alpha) : network analysis and monitoring software.
Angry IP scanner (v. 2.21) : a simple-to-use GUI-based network scanner.
ArpCacheWatch (v. 1.3) : ARP cache monitor.
Asterisk Logger (v. 1.02) : reveals passwords behind asterisks.
AsterWin IE (v. 1.03) : discovers passwords used in Internet Explorer.
Blat (v. 2.5.0) : Win32 command line utility that sends e-mail using the SMTP or NNTP protocols.
Cain & Abel (v. 2.8.9) : password recovery tool.
cdpr (v. 2.2.0) : decoder for the Cisco Discovery Protocol.
CurrPorts (v. 1.08) : displays opened TCP/IP ports and connections.
D-ITG (v. 2.4) : advanced traffic generator able to generate TCP, UDP, ICMP, DNS, Telnet and VoIP traffic.
Dialupass (v. 2.43) : discovers passwords used in Dial-Up authentications.
Dice (v. 2.9.9) : decodes network trace files and emits statistics.
DnsEye (v. 1.2) : monitors DNS requests.
DOS Command Prompt : runs a DOS Command Prompt in the command line tools directory.
DriverView (v. 1.10) : utility to view details about installed drivers.
Wireshark (v. 0.99.1) : powerful network analyzer with support for more than 700 protocols.
FreeSnmp (v. 1.2) : simple tool to perform SNMP queries.
Hydra (v. 5.2) : simple password revealer.
John the Ripper (v. 1.7.0.1) : utility to discover weak passwords.
NBTscan (v. 1.5) : command line NETBIOS name scanner.
netcat (v. 1.11) : reads and writes data across network connections, using TCP or UDP protocol.
NetMeter (v. 0.9.9.9 beta2) : bandwith monitor.
NetSNMP (v. 5.3.0.1) : a suite of SNMP manager tools.
ngrep (v. 1.44) : grep-like utility to search inside network packets.
Nmap (v. 4.01) : utility for network exploration and security auditing.
Protected Storage PassView (v. 1.62) : reveals IE, Outlook Express and MSN Explorer passwords.
PuTTY (v. 0.58) : Telnet and SSH terminal.
RegScanner (v. 1.20) : utility to search inside the registry.
Sam Spade (v. 1.14) : a freeware network query tool.
Snort (v. 2.4.3) : a lightweight network intrusion detection system.
StartupRun (v. 1.22) : shows applications that are scheduled to start during the startup of the OS.
THC-Amap (v. 5.2) : a scanning tool based on a database of triggers and responses.
ttcp : simple TCP and UDP Test utility, designed to test the performance of a network link.
UMIT (v. 0.0.0-soc-270) : a graphical user interface for Nmap.
Unix network clients : various standard network tools.
Unix Shell (v. 2006-04-11) : Windows version of the Bash shell.
wget (v. 1.10.1) : utility to perform non-interactive downloads of files via HTTP, HTTPS, FTP.
Win32Whois (v. 0.9.11) : simple Whois client.
WinDump (v. 3.9.3) : command line network analyzer, the Windows version of the well known tcpdump.
WinPcap (v. 3.1) : installer-version of WinPcap. Can be used with tools not present in this collection.
WinSCP (v. 3.7.6) : SFTP client using SSH.
WinUpdatesList (v. 1.12) : displays the operating systems updates, including the involved files.

Sure, you can go round up all these utilities separately, but The Network Toolkit contains all the utilities under a simple menu-driven interface with parameters and help information linked directly into the interface.

One of my favorite applications included in The Network Toolkit (other than Wireshark, of course) is D-ITG (Distributed Internet Traffic Generator) that is available to run in a Unix shell, at the DOS prompt or through a Windows GUI. This tool enables you to generate a variety of packets to a target to test one-way or round-trip latency or even just test blocking devices along a path. D-ITG comes with 13 pre-defined templates that include Telnet, DNS, Voice and customized packet flows using small and huge packets. Getting the most of this tool requires a bit of practice.

Another hot tool is Dice - Dice is used to analyze trace files. You know those charts and graphs you have been missing in Ethereal/Wireshark? Well check out Dice. Simply launch the Dice application, open a trace file and click the Graphs button. There are six different charts to choose from: packet size distribution, frame destination type, protocol distribution, most traffic (sender), most traffic (receiver) and packet throughput. I hope Dice continues to evolve to give us more graphical output for our trace files.

There is a long list of additional applications I would like to see CACE include with The Network Toolkit.

Since the CACE Technologies group includes the developers of WinPcap, these folks could put together a comprehensive toolset for Windows that actually works!

For more information on The Network Toolkit, visit www.cacetech.com.

------Disney Feature Film Announcement
If you happened to pick up the June 20th copy of the Hollywood Reporter you may have seen an article entitled Dis Picks Up Mother of All Spy Pics announcing that Walt Disney Pictures picked up a film entitled Mother of Invention. This films is about a Mom who performs some interesting cybercrime jobs while traveling and raising two kids... sound familiar? You are right. Although they do not mention my name in the article, the film is loosely based on my crazy world of balancing family and work. I am the Technical Consultant on the picture as well. No release dates yet. No cast information yet. Just another interesting project in the works.

\\\070706.end