



HNS Newsletter
Issue 168 - 30.06.2003.
<http://net-security.org>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://net-security.org>.

GRAB A COUPLE OF SECURITY WHITEPAPERS FROM THAWTE!

- * Securing your Apache Server for Business
- * The value of authentication
- * The Starter PKI Program

<http://www.net-security.org/v/thawte/>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Reviews
- 6) Security world
- 7) Software
- 8) Virus news

[Security news]

PROXY TERMINOLOGY 101

If you've ever accessed the Internet from an office environment, chances are your communications passed through a proxy.
<http://www.net-security.org/news.php?id=2941>

MICROSOFT HALTS GECAD LINUX/NOVELL ANTIVIRUS

Software giant's latest acquisition to drop development of non-Windows antivirus software.
<http://www.net-security.org/news.php?id=2942>

THE FEDS LOVE LINUX

Three weeks ago, John P. Stenbit, chief information officer of the U.S. Department of Defense, issued an agencywide memo that has Linux lovers rejoicing. The brief outlined the DOD's policy on acquiring, using and developing open-source software, including the Linux operating system.

<http://www.net-security.org/news.php?id=2943>

USENIX THE PERFECT CONFERENCE FOR UBER GEEKS

USENIX is that it is not a trade show. At USENIX you see a lot of programmers dressed in casual geek chic: shorts or jeans, lots of sandals (with or without socks), and t-shirts. Especially black t-shirts.

<http://www.net-security.org/news.php?id=2944>

FROM THE BOOBY HATCH

Senator Orrin Hatch says he wants to destroy music swappers' computers, but what he really means is that kids today have no respect for their elders.

<http://www.net-security.org/news.php?id=2945>

BIOMETRICS MEETS E-COMMERCE

Personal traits such as vocal or typing patterns could soon serve as powerful fraud-prevention tools for online shoppers.

<http://www.net-security.org/news.php?id=2946>

UNIVERSITY SYSTEMS HACKED TO DERAIL STUDENT ELECTIONS

A 21-year-old student was arrested for allegedly hacking into a university computer system during student elections to cast hundreds of votes for a made-up candidate he named American Ninja.

<http://www.net-security.org/news.php?id=2947>

HAS INTERNET MYSTERY CODE BEEN TRACKED?

Worm? Trojan? Attack tool? Network administrators and security experts continue to search for the cause of an increasing amount of odd data that has been detected on the Internet.

<http://www.net-security.org/news.php?id=2950>

SECURING PHP STEP-BY-STEP

This article shows the basic steps in securing PHP, one of the most popular scripting languages used to create dynamic web pages on the Internet.

<http://www.net-security.org/news.php?id=2951>

SECURITY FIRM DEVELOPS NEW PDA PROTECTION

Network Associates releases antivirus application for wireless handhelds.

<http://www.net-security.org/news.php?id=2953>

WI-FI - NEW BUNDLES IMPROVE MANAGEMENT AND SECURITY OPTIONS

Wi-Fi networks have, up until this point, been a bit like the Wild West: exciting, but difficult to control and keep safe.

<http://www.net-security.org/news.php?id=2954>

BEST BUY WARNS OF E-MAIL SCAM

Some consumers were tricked into sharing personal info.

<http://www.net-security.org/news.php?id=2955>

DVD-PIRACY PARANOIA PROVES COUNTERPRODUCTIVE

A little program called DeCSS caused a lot of commotion when it surfaced on the Internet four years ago.

<http://www.net-security.org/news.php?id=2956>

CREDIT CARDS CANCELLED OVER FRAUD FEARS

Banks have been forced to recall thousands of Irish credit cards amid fears they may have been used by fraudsters in the US.

<http://www.net-security.org/news.php?id=2957>

EU BACKS BIOMETRIC PASSPORTS

European Union governments last week agreed to embed computer chips containing biometric data in passports.

<http://www.net-security.org/news.php?id=2958>

A DICTIONARY FOR VULNERABILITIES

CVE gives users, vendors, and toolmakers a common vocabulary for vulnerabilities. Unfortunately, the bad guys move quite a bit faster.

<http://www.net-security.org/news.php?id=2959>

TOOL ANALYZES PATCHES

The new Radia Patch Manager applies a policy-based model to the process of updating security patches across servers, workstations and mobile devices. It will initially support Windows servers but will quickly follow up with support for a variety of Unix platforms, officials said.

<http://www.net-security.org/news.php?id=2960>

VENDORS FACE HOSTILITY OVER SECURITY REPORTING

Industry plans to change the way third parties report security vulnerabilities in software systems will probably be ignored say experts.

<http://www.net-security.org/news.php?id=2962>

MS WORKER 'RAN' \$17M SOFTWARE RACKET

A Microsoft worker has been charged with stealing \$17 million of software from Microsoft's internal store in the second case of its type in recent months.

<http://www.net-security.org/news.php?id=2963>

JOE PUBLIC BLAMES BANKS FOR CREDIT CARD FRAUD

Over half of all consumers (54%) feel that banks and building societies aren't doing enough to protect them from credit and debit card fraud, according to the results of a survey published today.

<http://www.net-security.org/news.php?id=2964>

TOWARD A SPAM-FREE FUTURE

Unsolicited commercial email is a spreading plague that feeds off the unique power of the Internet to connect hundreds of millions of computer users around the world, at virtually no cost.

<http://www.net-security.org/news.php?id=2965>

DDOS ATTACK HITS CLICKBANK AND SPAMCOP.NET

The attack, which began sometime on Saturday June 21, has flooded both companies' servers with bogus traffic, having the effect of blocking access to legitimate users' service requests.

<http://www.net-security.org/news.php?id=2966>

A NEW BREED OF "HACKTIVISTS" TAKES ON INTERNET CENSORSHIP

The free exchange of information over the Internet has proven to be a threat to the social and political control that repressive governments covet.

<http://www.net-security.org/news.php?id=2967>

HACKER TARGETS NASA VIA UNIVERSITY

A hacker has broken into a server at Kobe University and installed a program attempting to gain illegal access to the National Aeronautics and Space Administration's servers in the United States.

<http://www.net-security.org/news.php?id=2968>

HACKERS MOVE ON TO HIJACKING

Some call it "cyberjacking." Others call it corporate identity theft. It's the latest twist among computer hackers who have figured out new ways to hijack Web sites and use them to launch all kinds of unauthorized activity.

<http://www.net-security.org/news.php?id=2969>

TRUSTING ID MANAGEMENT TECHNOLOGY

The escalating need for identity management systems is driving privacy concerns to the forefront.

<http://www.net-security.org/news.php?id=2970>

IDS CRITICISMS KINDLE DEBATE

Intrusion detection is more trouble than it's worth, Gartner says.

<http://www.net-security.org/news.php?id=2971>

TCP/IP CONNECTION CUTTING ON LINUX FIREWALLS AND ROUTERS

This article describes how a Linux IPTables based firewall/router can be used to send the right combination of TCP/IP packets to both ends of a connection to cause them to abort the conversation.
<http://www.net-security.org/news.php?id=2972>

DOING IT ALL WITH OPENSSSH, PART 2

Welcome back to the Sysadmin's Corner and the continuing saga of secure communications, SSH-style.
<http://www.net-security.org/news.php?id=2973>

GATES: SECURITY ISN'T ALL BIG BROTHER

On the 100th anniversary of George Orwell's birth, Microsoft Chairman Bill Gates said the author of 1984 was only partially correct and predicted that technology will help preserve privacy rights.
<http://www.net-security.org/news.php?id=2974>

FEDERAL GOVERNMENT HAS A WAYS TO GO TO SECURE SYSTEMS

Federal officials and the GAO tell House subcommittee that agencies must continue to improve IT security.
<http://www.net-security.org/news.php?id=2975>

U.S. HOUSE APPROVES \$30 BILLION SECURITY BLANKET

The U.S House of Representatives has cast its vote in favor of sending \$29.4 billion to the Homeland Security Department, and some Democrats don't think this is enough.
<http://www.net-security.org/news.php?id=2976>

SECURITY SURVEY SAYS LIFE'S A BREACH

More than two-thirds of financial institutions globally have reported their information security procedures were "compromised" in the past year.
<http://www.net-security.org/news.php?id=2977>

WEB PRIVACY POLICIES CONFUSE NET SURFERS

Privacy policies that explain a company's Web surveillance habits have done little to dispel confusion among Internet users about how they are tracked online, according to a report released Wednesday.
<http://www.net-security.org/news.php?id=2978>

TIPS ON SETTING UP A WIRELESS LAN

When setting up a wireless LAN for your company, there are a couple of things you should keep in mind, according to Craig Mathias, a mobile and wireless analyst and founder of Ashland, Mass.-based Farpoint Group.
<http://www.net-security.org/news.php?id=2979>

STUMBLER MAPPING NETWORKS FOR FUTURE ATTACKS

The recently discovered Stumbler network-mapping tool represents a variety of malware that leaves enterprises with little in the way of defense, other than to lock down networks and employ intrusion detection, experts said.

<http://www.net-security.org/news.php?id=2980>

ONLINE PIRACY SPURS HIGH-TECH ARMS RACE

Sharing illegal copies of songs and movies on the Internet is a common practice, with the risks of getting caught slim.

<http://www.net-security.org/news.php?id=2981>

MICROSOFT READIES WINDOWS SERVER 2003 SP1 - FOR DECEMBER

Microsoft will roll out the final release of the first service pack for Windows Server 2003 in December and include a new security wizard that lets administrators lock down unnecessary processes and ports.

<http://www.net-security.org/news.php?id=2982>

TECHNO COPS NEEDED TO CATCH CYBER CRIMINALS - BLUNKETT

Police must embrace cutting edge technology to stay ahead of criminals in the fight against crime, the Home Secretary will tell an audience of senior policemen tonight.

<http://www.net-security.org/news.php?id=2983>

RFID CHIPS ARE HERE

RFID chips are being embedded in everything from jeans to paper money, and your privacy is at stake.

<http://www.net-security.org/news.php?id=2986>

HOW TO HIRE A SECURITY GURU

"There are personality traits that are important, like the ability to work extremely independently and to navigate competing technologies," Yankee Group senior analyst Eric Ogren told the E-Commerce Times.

<http://www.net-security.org/news.php?id=2987>

ACTIVCARD GETS PHYSICAL (SECURITY) WITH LINUX

There is a tale that gets told around the offices of LinuxPlanet that never fails to bring a chuckle when it's shared. I will share it, but names have been hidden to protect the innocent and the pompous.

<http://www.net-security.org/news.php?id=2988>

HACKER HOW-TO GOOD SUMMER READING

Stealing the Network is an entertaining hacking manual that purports to get inside the minds of hackers, explaining how they think. It's a good read, but it may infuriate some security types.

<http://www.net-security.org/news.php?id=2989>

NETWORK PROGRAMMING WITH THE TWISTED FRAMEWORK, PART 1

Twisted is an increasingly popular pure-Python framework for programming network services and applications.

<http://www.net-security.org/news.php?id=2990>

IS YOUR FINANCIAL DATA REALLY SAFE?

The threat is remote but real. With a world of hackers, hijackers and spoofers out there waiting to steal your stuff, a little caution is in order - online and off.

<http://www.net-security.org/news.php?id=2991>

REPORTER EXPLOITS WEAK WIFI NETWORK; ACCESSES STUDENT INFO

When the Palo Alto Unified School District decided to go high-tech and install wireless computer connections throughout its offices and on some campuses, it obviously hadn't gambled on security becoming an issue.

<http://www.net-security.org/news.php?id=2992>

CLOSING GAPS IN CORPORATE PRIVACY PROGRAMS

Are you vulnerable to a privacy breach? Mind the gaps.

<http://www.net-security.org/news.php?id=2993>

LEGENDARY CON ARTIST WARNS: HACKERS PLAY MIND GAMES

The biggest danger of hackers comes not from massive coding assaults but smiles and conversations.

<http://www.net-security.org/news.php?id=2994>

SECURING VOIP ON THE INTERNET

Two start-ups take aim at securing IP voice outside the corporate firewall.

<http://www.net-security.org/news.php?id=2995>

[Vulnerabilities]

All vulnerabilities are located here:

http://www.net-security.org/archive_vuln.php

Microsoft Windows Media Services Remote Command Execution Vulnerability

<http://www.net-security.org/vuln.php?id=2787>

Moregroupware Multiple Vulnerabilities

<http://www.net-security.org/vuln.php?id=2786>

iWeb Server 2 Directory Traversal Vulnerability

<http://www.net-security.org/vuln.php?id=2785>

WebAdmin.exe Remote Buffer Overrun Vulnerability

<http://www.net-security.org/vuln.php?id=2784>

Symantec Security Check ActiveX Buffer Overflow

<http://www.net-security.org/vuln.php?id=2783>

NetScreen ScreenOS Authentication Vulnerability

<http://www.net-security.org/vuln.php?id=2782>

GuestBookHost Cross Site Scripting Vulnerability

<http://www.net-security.org/vuln.php?id=2781>

OptiSwitch Remote Root Compromise Vulnerability

<http://www.net-security.org/vuln.php?id=2780>

Tutos Multiple Vulnerabilities

<http://www.net-security.org/vuln.php?id=2779>

XMB Forum Multiple Cross Scripting Vulnerabilities

<http://www.net-security.org/vuln.php?id=2778>

QNX Internet Appliance Toolkit http-daemon

Arbitrary File Reading Vulnerability

<http://www.net-security.org/vuln.php?id=2777>

Internet Explorer 5.0 and higher Buffer Overflow
Vulnerability
<http://www.net-security.org/vuln.php?id=2776>

MyServer 0.4.1 Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=2775>

phpBB viewtopic.php Cross Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=2774>

PerlEdit Remote Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=2773>

[**Advisories**]

All advisories are located at:
http://www.net-security.org/archive_advi.php

Gentoo Linux Security Announcement - gnotcan
<http://www.net-security.org/advisory.php?id=2177>

Gentoo Linux Security Announcement - noweb
<http://www.net-security.org/advisory.php?id=2176>

Gentoo Linux Security Announcement - phpbb
<http://www.net-security.org/advisory.php?id=2175>

Conectiva Linux Security Announcement - kopete
<http://www.net-security.org/advisory.php?id=2174>

Mandrake Linux Security Update Advisory - ypserv
<http://www.net-security.org/advisory.php?id=2173>

Mandrake Linux Security Update Advisory - xpdf
<http://www.net-security.org/advisory.php?id=2172>

Conectiva Linux Security Announcement - radiusd-cistron
<http://www.net-security.org/advisory.php?id=2171>

Turbolinux Security Advisory - gzip Symlink attack
<http://www.net-security.org/advisory.php?id=2170>

Turbolinux Security Advisory - Vulnerabilities in mget ty
<http://www.net-security.org/advisory.php?id=2169>

Microsoft Security Bulletin MS03-022 - Flaw in ISAPI
Extension for Windows Media Services Could Cause
Code Execution
<http://www.net-security.org/advisory.php?id=2162>

Microsoft Security Bulletin MS03-021 - Flaw In Windows
Media Player May Allow Media Library Access
<http://www.net-security.org/advisory.php?id=2161>

Red Hat Security Advisory - Updated XFree86 4.1.0
packages are available
<http://www.net-security.org/advisory.php?id=2160>

Gentoo Linux Security Announcement - ethereal
<http://www.net-security.org/advisory.php?id=2159>

Gentoo Linux Security Announcement - acroread
<http://www.net-security.org/advisory.php?id=2158>

Gentoo Linux Security Announcement - xpdf
<http://www.net-security.org/advisory.php?id=2157>

Gentoo Linux Security Announcement - proftpd
<http://www.net-security.org/advisory.php?id=2156>

Conectiva Linux Security Announcement - ethereal
<http://www.net-security.org/advisory.php?id=2155>

Turbolinux Security Advisory - Vulnerability in Xpdf
<http://www.net-security.org/advisory.php?id=2154>

Red Hat Security Advisory - Updated XFree86 packages
provide security and bug fixes
<http://www.net-security.org/advisory.php?id=2153>

Red Hat Security Advisory - Updated ypserv packages
fix a denial of service vulnerability
<http://www.net-security.org/advisory.php?id=2152>

SGI Security Advisory - Multiple IPv6-Induced Bugs
& Vulnerabilities
<http://www.net-security.org/advisory.php?id=2151>

Mandrake Linux Security Update Advisory - ethereal
<http://www.net-security.org/advisory.php?id=2150>

Debian Security Advisory - New tcptraceroute packages
fix failure to drop root privileges
<http://www.net-security.org/advisory.php?id=2149>

[Featured articles]

All articles are located at:
http://www.net-security.org/articles_main.php

Articles can be contributed to staff@net-security.org

INTERVIEW WITH KEVIN DAY

The author of "Inside the Security Mind: Making the Tough Decisions" and one of the founders of Relational Security Corporation, an organization that focuses on new tools and methodologies for Information Security Assessment and Risk Management discusses his book and general security issues.

<http://www.net-security.org/article.php?id=513>

OUTSOURCING – POTENTIAL SECURITY NIGHTMARE?

This article examines the major reason why so many corporations, who have recognised the compelling arguments for outsourcing, go right to the brink of making a decision and then pull back.

<http://www.net-security.org/article.php?id=514>

ALADDIN KNOWLEDGE SYSTEMS LAUNCHES NEW ADVANCED ANTI-SPAM SERVICE

Aladdin Knowledge Systems announced its collaboration with Cobion, technology leader in content security software, and the launching of a new Advanced Anti-spam Service designed to equip eSafe 4 customers with state-of-the-art spam control.

<http://www.net-security.org/article.php?id=515>

CONFERENCE ON MOBILE AND WIRELESS SECURITY ANNOUNCED
MIS Training Institute announced that The Conference on Mobile

and Wireless Security will be held in Chicago, IL, September 23-25, 2003, with optional workshops on September 22, 25, and 26.
<http://www.net-security.org/article.php?id=516>

[**Reviews**]

All reviews are located at:
<http://www.net-security.org/reviews.php>

TCP/IP UNLEASHED

With over 1000 pages, this book is a big and heavy volume. "TCP/IP Unleashed (third edition)" is an attempt to collect all information about the TCP/IP protocol suite and its implementation in today's operating systems. Is the book right for you? Read on to find out.

<http://www.net-security.org/review.php?id=81>

[**Security world**]

All press releases are located at:
http://www.net-security.org/press_main.php

Secure your eSecrets' - A New and Simplified Approach to Electronic Document Security
<http://www.net-security.org/press.php?id=1499>

Zix Corporation Selected by Blue Cross and Blue Shield of Nebraska to Provide e-Messaging Safeguards for HIPAA Compliance
<http://www.net-security.org/press.php?id=1498>

Diversinet And Hongkong Post Sign Agreement To Develop And Deploy A Secure Wireless E-Mail Service For Hong Kong
<http://www.net-security.org/press.php?id=1497>

Scalable Networks Partners with Netilla
<http://www.net-security.org/press.php?id=1496>

Sophos Anti-Virus Enters Chinese Market
<http://www.net-security.org/press.php?id=1495>

Integralis Calls On Businesses To Undergo "Wireless Mobs"
<http://www.net-security.org/press.php?id=1494>

Anti-spam Groups to Benefit from Sales of SpamSquelcher,
the First Product to Stop Spam at the Source
<http://www.net-security.org/press.php?id=1493>

Trapeze Networks, Makes a Big Splash in The United Kingdom
Winning Best Product Of Networks For Business 2003
<http://www.net-security.org/press.php?id=1492>

ActiveState and Osis Partner on All-in-One Security Appliance
<http://www.net-security.org/press.php?id=1491>

Snapgear and Zone Labs Team to Offer Internet Security
Solution for Home and Office Networks
<http://www.net-security.org/press.php?id=1490>

Panda Antivirus for Exchange Server 2003 Harnesses the Most
Innovative Technology for Combating Malicious Code
<http://www.net-security.org/press.php?id=1489>

Cisco Press Announces New Suite of Products for CCNA
640-801, 811 and 821 Exams
<http://www.net-security.org/press.php?id=1488>

EMF Chooses F-Secure Anti-Virus for its Managed
Email Filtering Services
<http://www.net-security.org/press.php?id=1487>

NetFrameworks announces BlastDoor Secure File Exchange
Corporate Server and Online Service
<http://www.net-security.org/press.php?id=1486>

Cable and Wireless and Attix5 Join Forces to Deliver
Comprehensive Data Backup Solution
<http://www.net-security.org/press.php?id=1485>

Tumbleweed Communications Corp. Announces
Completion of Merger with Valicert, Inc.
<http://www.net-security.org/press.php?id=1484>

Nemx Anti-Spam Software Provides Cost-Effective Solution
<http://www.net-security.org/press.php?id=1483>

Clientless VPNs Give Channel An Insatiable Appetite For More
<http://www.net-security.org/press.php?id=1482>

Veterans Affairs Recognizes Cyber Security Experts
<http://www.net-security.org/press.php?id=1481>

GFI Releases MailSecurity 8 - Introduces Trojan
and Executable Analyzer
<http://www.net-security.org/press.php?id=1480>

[**Security Software**]

Windows software is located at:
http://net-security.org/software_main.php?cat=1

Linux software is located at:
http://net-security.org/software_main.php?cat=2

ADMSMB 0.3

ADMsmB is a security scanner for Samba based on the source of smbclient. It will get the netbios name, share list, workgroup, domain, and OS. It will then try to access any exported shares, perform a session brute force, and perform brute force on a directory specified.

<http://www.net-security.org/software.php?id=499>

[**Virus News**]

All virus news are located at:
<http://www.net-security.org/viruses.php>

Weekly Virus Report - Linux Typot Trojan, Sobi, Sluter,
Fortnight, Trile and Auric Worms
http://www.net-security.org/virus_news.php?id=263

Unzip at Your Peril - It May be Sobig Worm
http://www.net-security.org/virus_news.php?id=262

Panda Software Reports the Appearance of Sobig.E
http://www.net-security.org/virus_news.php?id=261

"Punk" Worm Pays Tribute To The Offspring
http://www.net-security.org/virus_news.php?id=260

Eset Releases Version 2.0 of their NOD32 Anti Virus Product
http://www.net-security.org/virus_news.php?id=259

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

Subscribe to this weekly digest on:
<http://www.net-security.org/subscribe.php>
Unsubscribe by sending the e-mail address you are subscribed
with to: info@net-security.org with UNSUBSCRIBE in the message body.

The archive of the newsletter in TXT and PDF format is available
http://www.net-security.org/newsletter_archive.php

GRAB A COUPLE OF SECURITY WHITEPAPERS FROM THAWTE!

- * Securing your Apache Server for Business
- * The value of authentication
- * The Starter PKI Program

<http://www.net-security.org/v/thawte/>
