



HNS Newsletter

Issue 174 - 11.08.2003.

<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) Review
- 6) Security world
- 7) Software
- 8) Virus news

[Security news]

DOS & DON'TS: CONFIGURING LINUX ROUTERS

Even the most experienced network administrator can get stumped when configuring Linux routers, says Tony Mancill, author of *Linux Routers: A Primer for Network Administrators*, 2nd Ed. <http://www.net-security.org/news.php?id=3247>

WIRELESS SECURITY: HARDER THAN YOU THINK

Adding encryption to wireless networking isn't always simple. <http://www.net-security.org/news.php?id=3248>

BLOCKING MALICIOUS URLS

Many exploits on many Web servers - most often Microsoft IIS - have been based on URLs that were technically legal but employed buffer overflows or similar techniques.

<http://www.net-security.org/news.php?id=3249>

WHEN EMPLOYEES ARE THE ENEMY - SECURITY FROM THE INSIDE

Beyond the network level, firewalls also can be erected at the application and desktop levels to give employees only the access they need according to Check Point project marketing manager Sweta Duseja.

<http://www.net-security.org/news.php?id=3250>

MICROSOFT WARNS BROWSER USERS ABOUT 'WORM' VIRUS

Microsoft is warning its customers about a computer worm that exploits a flaw in its Internet Explorer browser.

<http://www.net-security.org/news.php?id=3251>

MICROSOFT'S WEB SITE BROUGHT DOWN BY ATTACK

Denial of service is blamed for outage that lasted more than an hour.

<http://www.net-security.org/news.php?id=3252>

PATCH YOUR SOFTWARE - IT'LL HELP SECURE THE NET

When a security researcher or vendor first releases information about a software vulnerability, the clock starts ticking. How long will it be until a malicious user takes advantage of it?

<http://www.net-security.org/news.php?id=3254>

SECURESUITE XS DISPOSES OF PASSWORDS

I/O software's SecureSuite XS Workstation 4.2 reduces help desk costs associated with forgotten user passwords by eliminating passwords altogether.

<http://www.net-security.org/news.php?id=3255>

VIRUS POSES AS ADMIN E-MAIL

People are being warned to be on the lookout for a Windows e-mail virus which pretends to be a message from computer support staff.

<http://www.net-security.org/news.php?id=3256>

IBM GIVES NOD TO WAVE SECURITY TOOLS

Wave Systems' push to pull in corporate customers for its security software got a lift from IBM, which has given the thumbs-up to two of the company's new products.

<http://www.net-security.org/news.php?id=3257>

NZ CCIP CHIEF TALKS SECURITY

Monitoring security issues and making sure all the latest patches are installed on your system could be almost a full-time job for one staff member in a moderate-sized IT department, says Jay Garden, head of the New Zealand government's Centre for Critical Infrastructure Protection.

<http://www.net-security.org/news.php?id=3258>

HACK ATTACKS AT RECORD LEVELS

Attacks on Australian computer systems are at record levels. More than 1000 incidents a week are being reported, internal figures from the security organisation, AusCERT, reveal.

<http://www.net-security.org/news.php?id=3259>

DEMONSTRATING ROI FOR PENETRATION TESTING (PART TWO)

The second article in this series will introduce Risk Management concepts as they relate to Information Asset valuation.

<http://www.net-security.org/news.php?id=3260>

BERKELEY BRACES FOR HACKER ATTACK

University to shut down outside access to part of its network this morning.

<http://www.net-security.org/news.php?id=3262>

ROBOT 'GUARD DOG' SNIFFS OUT WIFI HOLES

DefCon: A group of security experts have created a two-wheeled robot that detects security problems in Wi-Fi networks.

<http://www.net-security.org/news.php?id=3263>

'ETHICAL HACKERS' TEST FOR WEAKNESS

In a 17th-floor corner office in north Toronto, a group of computer nerds is feverishly attacking Corporate Canada -- and getting paid for its efforts.

<http://www.net-security.org/news.php?id=3264>

COUNTRY-CODED COMPUTER WORMS MAY BE AHEAD

Future computer worms could be programmed to attack only within a particular country, according to a leading computer security expert.

<http://www.net-security.org/news.php?id=3265>

THOUGHT FOR THE DAY: STOP CRYING VIRUS WOLF

The security industry has a duty to be more realistic, says security expert Jan Hruska.

<http://www.net-security.org/news.php?id=3266>

E-MAIL FRAUD TAKES A NEW TWIST

There's a new Internet fraud scheme you can add to

your list: phishing.

<http://www.net-security.org/news.php?id=3268>

HOST-BASED INTRUSION DETECTION WITH SAMHAIN

Samhain is a wonderful GPL host-based intrusion detection system.

<http://www.net-security.org/news.php?id=3269>

HACKER HIT PARADE GOES LIVE

Security firm Qualys has begun producing a real-time index of the vulnerabilities that are the current favourites of the net's community of malicious hackers.

<http://www.net-security.org/news.php?id=3270>

WARDRIVERS MAP VAST AREAS OF WIRELESS HOTSPOTS

Wardrivers Matthew Hyson, left, and J.P. Tanguay, CEO of Wireless Friendly, know where unprotected wireless networks are in Toronto and they say the number is worrisome.

<http://www.net-security.org/news.php?id=3271>

BRITAIN: A NATION OF CYBER SNOOPERS

Britain is fast becoming a nation of cyber snoopers, according to a study.

<http://www.net-security.org/news.php?id=3272>

DEFCON 2003 - MYTH, REALITY AND PICTURES

Attendees at this year's DEFCON hacker convention in Las Vegas were more annoyed at the long lines for speaker sessions than any appearance by "The Man" (i.e. the Feds).

<http://www.net-security.org/news.php?id=3273>

ATTACK OF THE MUTANT INTERNET WORMS

Internet worms that spread themselves through corporate networks or e-mail programs, wreaking havoc on thousands of computers, are growing faster, smaller and more virulent, a security expert has said.

<http://www.net-security.org/news.php?id=3274>

LINUX APPROVED FOR USE ON SENSITIVE COMPUTERS IN THE US

Linux software has been approved for use on the most sensitive computers in US corporations and the US federal government, including those inside banks and the Pentagon, an important step for software widely considered the top rival to Microsoft.

<http://www.net-security.org/news.php?id=3275>

REDUCING "HUMAN FACTOR" MISTAKES

This paper will try to summarize various mistakes done by System Administrators, Company Executives and of course the end users, and will also provide you with useful strategies that will definitely help you reduce or completely eliminate the mistakes.

<http://www.net-security.org/news.php?id=3276>

MEMORY STICKS ARE THE LATEST SECURITY RISK

Memory sticks have been branded as the latest security risk by security firm SecureWave, whose intrusion prevention technology can be used to control the use of the popular devices in corporate environments.

<http://www.net-security.org/news.php?id=3278>

WIRELESS LAN SECURITY FALLS SHORT

Wireless LAN vendors have failed to deliver interoperable, highly secure wireless LANs, according to META Group.

<http://www.net-security.org/news.php?id=3280>

THE INTERNET SECURITY DEMON THAT WON'T DIE

"A traditional regulatory model applied to the Internet is doomed to failure. By the time it was regulated, you'd be dealing with an Internet that was two years older," says Larry Clinton, chief operating officer at the Internet Security Alliance.

<http://www.net-security.org/news.php?id=3281>

HACKERS AND VENDORS BRAWL OVER NOTHING

The issue of security vulnerability disclosure has been a hot topic for a long time now, however recent efforts to bring in new disclosure guidelines are unlikely to change anything.

<http://www.net-security.org/news.php?id=3282>

SECURITY GUARD

Once burned, lesson learned, the adage goes. So why do IT departments keep getting burned by the same security issues?

<http://www.net-security.org/news.php?id=3283>

THE COSTLY PASSWORD PROBLEM

Do you have a card in your wallet or a list on your PDA consisting of user names and passwords you use? If so, you're not the only person who can't remember them all, and there may be security risks and costs associated with the way you manage the data.

<http://www.net-security.org/news.php?id=3284>

SWOLLEN ORDERS SHOW SPAM'S ALLURE

A New Hampshire company appears to be grossing close to half a million dollars each month by spamming people with sales pitches for an herbal "male enhancement" product. The discovery may explain the intractability of junk e-mailers on the Internet.

<http://www.net-security.org/news.php?id=3285>

BLOGS: ANOTHER TOOL IN THE SECURITY PRO'S TOOLKIT (PART TWO)

Part two on blogs covers RSS feeds that are highly relevant to

the security community.

<http://www.net-security.org/news.php?id=3286>

WIN32 DEVICE DRIVERS COMMUNICATION VULNERABILITIES - TUTORIAL

The following a complete tutorial on how to exploit Norton Antivirus's device driver to gain elevated privileges. The tutorial is comprehensive, and detailed enough to be used to learn on the issue, and how to find these types of vulnerabilities in other products.

<http://www.net-security.org/news.php?id=3287>

NIAP CERTIFICATION BECOMING A PRIORITY

The government's plan to pressure software vendors to build more secure products seems to be gathering a bit of momentum.

<http://www.net-security.org/news.php?id=3288>

SCO BATTLE ROOTED IN UNIX'S FRAGMENTED HISTORY

The SCO Group's attempts to squeeze a revenue stream out of Linux is rooted in the long and tangled history of computer operating systems.

<http://www.net-security.org/news.php?id=3291>

TIME RUNNING OUT TO MANAGE SECURITY

Hundreds of point security solutions and a poor industry record in security management have led to a level of complexity today that can still be resolved.

<http://www.net-security.org/news.php?id=3292>

HACKER GETS ACXION CUSTOMER INFORMATION

A computer hacker gained access to private files at Acxiom Corp., one of the world's largest consumer database companies, and was able to download sensitive information about some customers of the company's clients.

<http://www.net-security.org/news.php?id=3293>

KNOW YOUR SECURITY ONIONS

Steve Brown, managing director of Novell UK, recommends the multiple, overlapping layers of the 'onion' approach to cybersecurity.

<http://www.net-security.org/news.php?id=3294>

HACKER ATTACK DAMAGES 2,000 COMPUTERS AT STANFORD

Officials at Stanford University are scrambling to repair the damage from a hacking attack that has infected thousands of campus computers.

<http://www.net-security.org/news.php?id=3295>

NEW SECURITY WOES FOR E-VOTE FIRM

A January source code leak revealed the innards of Diebold Election Systems' proprietary voting software. A new breach threatens to expose the company's business practices -- including its security methods.

<http://www.net-security.org/news.php?id=3296>

LINUXWORLD: 2.6 KERNEL CURES SOME SECURITY SHORTCOMINGS

Concerns about security may keep some IT shops from choosing Linux. Those concerns aren't justified, says Dan Frye, director of IBM Corp.'s Linux Technology Center. In this interview, Frye discusses Linux's few security shortcomings and the security advances coming in the 2.6 kernel.

<http://www.net-security.org/news.php?id=3297>

NEW WLAN ATTACKS IDENTIFIED

AirDefense says that during monitoring at the DefCon hacker convention in Las Vegas last weekend the company identified new security issues specifically effecting wireless LANs.

<http://www.net-security.org/news.php?id=3298>

NEW ID SYSTEM SPARKS PRIVACY DEBATE

Fingerprints, DNA and behavioural characteristics are unique and difficult to forge, but using them to identify an individual in the modern world is legally problematic.

<http://www.net-security.org/news.php?id=3299>

SA BANKS, RETAILERS PREPARE FOR GLOBAL SECURITY STANDARDS

SA banks and retailers have stepped up their efforts to meet the mandated Visa and MasterCard deadline for the security of their PIN-handling systems to comply with the global Triple DES (T-DES) algorithm standard.

<http://www.net-security.org/news.php?id=3300>

[**Vulnerabilities**]

All vulnerabilities are located here:

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

Cisco CSS 11000 Series Denial of Service Vulnerability

<http://www.net-security.org/vuln.php?id=2870>

Sustworks Unauthorized Network Monitoring and
tcpflow Format String Vulnerabilities
<http://www.net-security.org/vuln.php?id=2869>

VMware Workstation 4.0.1 Symbolic Links Vulnerability
<http://www.net-security.org/vuln.php?id=2868>

Crob FTP Server 2.60.1 Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=2867>

Password Safe Information Leak Vulnerability
<http://www.net-security.org/vuln.php?id=2866>

Zone Alarm Device Driver Vulnerability
<http://www.net-security.org/vuln.php?id=2865>

Invision Board Input Filtering Vulnerability
<http://www.net-security.org/vuln.php?id=2864>

IBM DB2 7.1 db2job Permission Checking Error Vulnerability
<http://www.net-security.org/vuln.php?id=2863>

Postfix Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=2862>

[Advisories]

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

Red Hat Security Advisory - up2date improperly checks
GPG signature of packages
<http://www.net-security.org/advisory.php?id=2345>

Debian Security Advisory - New xpcd packages fix buffer overflow
<http://www.net-security.org/advisory.php?id=2344>

Debian Security Advisory - New xtokkaetama packages
fix buffer overflow
<http://www.net-security.org/advisory.php?id=2343>

Debian Security Advisory - New man-db packages
fix problem with DSA-364-1
<http://www.net-security.org/advisory.php?id=2342>

Trustix Secure Linux Security Advisory - stunnel
<http://www.net-security.org/advisory.php?id=2341>

Trustix Secure Linux Security Advisory - postfix
<http://www.net-security.org/advisory.php?id=2340>

Immunix Secured OS Security Advisory - wu-ftpd
<http://www.net-security.org/advisory.php?id=2339>

OpenPKG Security Advisory - perl-www
<http://www.net-security.org/advisory.php?id=2338>

OpenPKG Security Advisory - openssh
<http://www.net-security.org/advisory.php?id=2337>

Guardian Digital Security Advisory - 'stunnel' signal
handler race denial-of-service
<http://www.net-security.org/advisory.php?id=2336>

Debian Security Advisory - New eroaster packages
fix insecure temporary file creation
<http://www.net-security.org/advisory.php?id=2335>

Debian Security Advisory - New phpgroupware package
fix several vulnerabilities
<http://www.net-security.org/advisory.php?id=2334>

Debian Security Advisory - New kernel packages fix
potential "oops" (update)
<http://www.net-security.org/advisory.php?id=2333>

FreeBSD Security Advisory - Single byte buffer overflow
in realpath(3) (update)
<http://www.net-security.org/advisory.php?id=2332>

Debian Security Advisory - New kernel packages fix potential "oops"
<http://www.net-security.org/advisory.php?id=2331>

Debian Security Advisory - New man-db packages fix buffer overflows, arbitrary command execution
<http://www.net-security.org/advisory.php?id=2330>

Conectiva Linux Security Announcement - postfix
<http://www.net-security.org/advisory.php?id=2329>

Conectiva Linux Security Announcement - wget
<http://www.net-security.org/advisory.php?id=2328>

Guardian Digital Security Advisory - 'postfix' Remote denial-of-service
<http://www.net-security.org/advisory.php?id=2327>

NetBSD Security Advisory - off-by-one error in realpath(3)
<http://www.net-security.org/advisory.php?id=2326>

NetBSD Security Advisory - remote panic in OSI networking code
<http://www.net-security.org/advisory.php?id=2325>

Red Hat Security Advisory - New postfix packages fix security issues
<http://www.net-security.org/advisory.php?id=2324>

Turbolinux Security Announcement - Wu-ftpd fb_realpath() off-by-one bug
<http://www.net-security.org/advisory.php?id=2323>

SuSE Security Announcement - postfix
<http://www.net-security.org/advisory.php?id=2322>

FreeBSD Security Advisory - Single byte buffer overflow in realpath(3)
<http://www.net-security.org/advisory.php?id=2321>

[Featured articles]

All articles are located at:

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

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

CHIEF SECURITY OFFICER'S POINT OF VIEW

CSO magazine recently did a poll, where 480 chief security officers and senior security executives discussed security issues and industry regulations.

<http://net-security.org/article.php?id=539>

ENTRUST RELEASES NEW SECURE WEB PORTAL SOLUTION

Entrust released its latest Secure Web Portal Solution based on Entrust TruePass Version 7.0, the first Web security solution in the market today to deliver bi-directional, end-to-end security for online information regardless of an organization's Web infrastructure.

<http://www.net-security.org/article.php?id=538>

VULNERABILITY ASSESSMENT

This document serves as an introduction to the subject of security vulnerability assessments. It focuses primarily on vulnerability assessments performed from an external/remote location (like that of an actual hacking attack).

<http://www.net-security.org/article.php?id=537>

LACK OF SECURITY AT WIRELESS CONFERENCES

During the 802.11 Planet Expo in Boston, wireless security company AirDefense monitored WLAN activity and reported a number of security issues.

<http://www.net-security.org/article.php?id=536>

NOVELL EDIRECTORY HAS ADDITIONAL LINUX SUPPORT AND ENHANCED SECURITY

Novell eDirectory will ship with built-in support for advanced authentication methods, such as biometrics, smart cards and tokens.

<http://www.net-security.org/article.php?id=535>

LDAP INJECTION: ARE YOUR WEB APPLICATIONS VULNERABLE?

The objective of this paper is to inform developers, system administrators and security professionals about various techniques that can be used to attack their applications. It also describes preventive measures for protecting applications from these intrusions.

<http://www.net-security.org/article.php?id=534>

[**Review**]

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

WEB SERVICES SECURITY

Web Services are appearing and dominate as new application solutions. At the same time they present great challenges for security. This book describes a union of Web Services and information security. Several technologies are presented (i.e. XML Signature, XML Encryption, SAML...), and then related to Web Services so that the reader can get the whole picture.
<http://www.net-security.org/review.php?id=89>

[**Security world**]

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

AirDefense Identifies New WLAN Denial-of-Service Attack,
Investigating Potential Threats
<http://www.net-security.org/press.php?id=1576>

Revenues from Global Enterprise Investment in Security
Products Predicted to Hit \$13.5bn by 2006
<http://www.net-security.org/press.php?id=1575>

Entrust Secure Web Portal Solution First to Deliver
Bi-directional, End-to-End Online Information Security
<http://www.net-security.org/press.php?id=1574>

Microexpert Limited Launches Remote Network Access System
<http://www.net-security.org/press.php?id=1573>

Snapgear and TZO Partnership Brings Secure Internet
Connections To Small- And Medium-Sized Enterprises
<http://www.net-security.org/press.php?id=1572>

New Snapgear Security Appliances Deliver Secure,
High Availability Internet Connections to SMEs
<http://www.net-security.org/press.php?id=1571>

Snapgear Announces New Embedded Linux Platforms
For Intel Network Processors
<http://www.net-security.org/press.php?id=1570>

WildPackets Announces GigaPeek NX Full-Duplex Analysis Solution
<http://www.net-security.org/press.php?id=1569>

SSH Communications Security Teams With RSA Security To
Provide a Trusted Identity And Access Management Solution
<http://www.net-security.org/press.php?id=1568>

Uncertainty Surrounding Growth Opportunities Prevails
In IP VPN Services Industry
<http://www.net-security.org/press.php?id=1567>

UK Firms Waking Up To Micemail Attack
<http://www.net-security.org/press.php?id=1566>

Neoteris Expands SSL-Based Access Options To Deliver
Unprecedented Range Of Application Support
<http://www.net-security.org/press.php?id=1565>

[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

SENSORTRENDS 0.4
sensorTrends is a GPL web-based application that displays a
high-level view of the ports that are being scanned over the
course of time.
<http://www.net-security.org/software.php?id=507>

RESET 0.1.0

Reset is a floppy-based system for erasing data from a harddrive in a secure manner.

<http://www.net-security.org/software.php?id=508>

[**Virus News**]

All virus news are located at:

<http://www.net-security.org/viruses.php>

Weekly Virus Report - Autorroter Trojan, Panol and Mimail Worms

http://www.net-security.org/virus_news.php?id=283

Autorroter Worm - One More Reason To Patch Your Computer

http://www.net-security.org/virus_news.php?id=282

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/>
