

HNS Newsletter
Issue 108 - 29.04.2002
<http://net-security.org>
<http://security-db.com>

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://www.net-security.org>.

=====
Sponsored by GFI, the developers of a revolutionary new intrusion detection product - LANguard Security Event Log Monitor.

Download your copy!
<http://www.net-security.org/cgi-bin/ads/ads.pl?banner=gfitxt>
=====

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world

General security news

APACHE AND SSL

This article summarizes the basic concepts of how SSL and TLS work and how Apache implements these protocols so that one can transmit information securely over HTTP.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.onlamp.com/pub/a/onlamp/2002/04/18/ssl.html>

INTERVIEW WITH HEIKO ZUERKER, AUTHOR OF DEVIL-LINUX

PortaZero's Gabriele D'Angelo interviewed Heiko Zuerker and asked him some questions regarding the Devil-Linux backstage. Devil-Linux is a Linux distribution used for Firewalls / Routers.

Link:
<http://www.portazero.info/modules.php?name=Sections&sop=viewarticle&artid=25&page=2>

SYMANTEC PREPS LINUX FIREWALL FOR IBM ISERIES

Symantec is working with IBM to deliver a hardened firewall which will run within an iSeries Linux partition and provide protection for the iSeries or other connected servers on corporate networks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/53/24952.html>

INTERPOL WARNS FIRMS OVER SECURITY 'VACUUM'

The chairman of Interpol's European Working Party on IT Crime has warned that a "vacuum of knowledge" surrounding IT security means companies are exposing themselves to unnecessary risk.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computing.vnunet.com/News/1131119>

U.S. ARMY TO CENTRALIZE NETWORK SECURITY SCANNING

The U.S. Army announced a major new initiative designed to help the service get its arms around vulnerability analysis and automated patch management for more than 1.5 million workstations around the world.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO70379,00.html

A BAD YEAR FOR PRIVACY

At the Computers, Freedom and Privacy conference tech activists take on the latest incursions on individual privacy from government and industry.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,51987,00.html>

HOW TEENS STILL HACK MILLION-DOLLAR SECURITY SYSTEMS

More than 26,000 computer intrusion incidents were reported to CERT in the first three months of this year, surpassing the total for all of 2000.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsfactor.com/perl/story/17371.html>

CA, ERNST & YOUNG TEAM ON SECURITY CONSULTING

Hoping to increase its market share among Fortune 1000 companies, Computer Associates International Inc. announced a partnership with Ernst & Young LLP that will see the companies work together on security and risk management issues.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.itworld.com/Man/3886/020422securityconsulting>

CLOSING THE SPYCAM SNIFFER LOOPHOLE

Those cheap wireless video cameras hawked by annoying pop-up ads can be intercepted by anyone with a few hundred dollars and a voyeuristic bent. There's no federal law against it, but there should be.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://online.securityfocus.com/columnists/76>

'MANNHEIM' TO HARDEN ARMY DEFENSE

The Army last week concluded the first exercise of an initiative designed to improve the service's ability to defend its networks against attacks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.fcw.com/fcw/articles/2002/0422/news-mann-04-22-02.asp>

KEEP YOUR FILES SAFE WITH THESE ENCRYPTION TOOLS
Worried someone might read your confidential files? Your data is vulnerable. So what can you do? Use encryption software and digital file shredders.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2862168,00.html>

WIRELESS LAN SECURITY: A SHORT HISTORY
If you're holding back on an 802.11 deployment because of security concerns, you're not alone. Research indicates that the perceived insecurity of wireless networks is a major inhibitor to further market growth.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html>

KEEPING E-MAIL ENCRYPTION ALIVE
"PGP has been around for 10 years and has endured incredible obstacles and hardships," Zimmermann said. "Powerful forces have been arrayed to stop PGP and yet those obstacles were overcome."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2002/TECH/ptech/04/21/encryption.future.ap/index.html>

WHY THE KLEZ WORM JUST WON'T GO AWAY
Every time a virus or worm - like Klez - wreaks havoc across the globe, it's inevitably followed by copycat variants. So how can you protect yourself against these viral descendants?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2862307,00.html>

IE-6 PRIVACY SOLUTION BACKFIRES
It may seem ironic, but privacy functionality in IE6 makes it possible to launch several attacks against the browser, and against Outlook and Outlook Express, security researcher Thor Larholm has discovered.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/24997.html>

USING GNUPG
GnuPG is the open source equivalent to PGP. Using GPG is very easy and straightforward. It is a text-based command line tool, but there are frontends to GPG that make it even easier to use.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.mandrakesecure.net/en/docs/gpg.php>

RSA SECURITY SAYS IT WILL CUT 200 JOBS

Computer security provider RSA Security Inc. on Wednesday said it will cut about 200 jobs in order to reduce operating expenses.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnet.com/investor/news/newsitem/0-9900-1028-9775517-0.html>

SECURITY EXHIBITORS SET UP INSECURE WLANS

Wireless networking insecurity was a key theme of this week's InfoSecurity show with a number of suppliers coming out with surveys on just how vulnerable world+dog is to drive by hackers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/25000.html>

CHECK POINT BOOSTS FIREWALL PERFORMANCE

Check Point Software Technologies Inc. detailed a new firewall performance enhancement module for use with its firewall and virtual private network products.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetweek.com/breakingNews/INW20020424S0005>

AN IPSEC TUNNEL IMPLEMENTATION FOR LINUX

I started this project because I was using a number of IPsec tunnels to connect a number of private networks over the Internet, and I needed encryption for a few reasons.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://ringstrom.mine.nu/ipsec_tunnel/

UPGRADING TO SOLARIS 8

Solaris 8 is inarguably the best Solaris release generally available, but it may not be right for everyone. Galvin explores reasons to stay put and reasons to upgrade, and provides detailed how-to upgrade instructions.

Link: <http://www.unixreview.com/documents/s=2426/uni1019674877319/0204m.htm>

SETTING UP A FREEBSD FIREWALL WITH AN IPSEC UPLINK

This article shares steps for setting up an IPsec tunnel for securing a 802.11b wireless uplink. The article also covers basic NAT and IPFW for use with this setup.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2002/April/Features671.html>

TEACHING THE RULES OF THE ROAD

Bad system administrators affect more than their own computers - they make the entire Internet a little less safe.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://online.securityfocus.com/columnists/77>

KLEZ WORM COULD COMPROMISE SENSITIVE DATA

The initially innocuous Klez worm is turning nasty as vandals tweak both the mode of attack and the payload.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://techupdate.zdnet.co.uk/story/0,,t481-s2108922,00.html)

[bin/news.cgi?url=http://techupdate.zdnet.co.uk/story/0,,t481-s2108922,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://techupdate.zdnet.co.uk/story/0,,t481-s2108922,00.html)

FAA HACKED BY PATRIOTS

Hackers were able to penetrate a Federal Aviation Administration system earlier this week and download unpublished information on airport passenger screening activities.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/25029.html)

[bin/news.cgi?url=http://www.theregister.co.uk/content/55/25029.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/25029.html)

SET UP A LINUX FIREWALL WITH EASE USING FIRESTARTER

Firestarter provides a clean, powerful interface for quickly creating a firewall and getting it started.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://techupdate.zdnet.co.uk/story/0,,t481-s2109197,00.html)

[bin/news.cgi?url=http://techupdate.zdnet.co.uk/story/0,,t481-s2109197,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://techupdate.zdnet.co.uk/story/0,,t481-s2109197,00.html)

RIAA WANTS TAX DOLLARS TO COMBAT PIRACY

The Recording Industry Association of America is calling for additional federal funding to combat the ongoing wave of piracy, saying that the number of arrests and convictions or copyright crimes has skyrocketed over the course of a year.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://zdnet.com.com/2100-1105-891781.html>

BUILDING A SECURE KIOSK WITH EMBEDDED LINUX

Patrick Glennon relates his experiences in creating a small Linux based system for a client that required robust, easy-to-use, low-cost kiosks for conducting surveys at hotels.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxdevices.com/articles/AT2869412121.html)

[bin/news.cgi?url=http://www.linuxdevices.com/articles/AT2869412121.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxdevices.com/articles/AT2869412121.html)

DR. DAMN CLEANS HOUSE FOR FILE-SWAPPERS

The record companies had their Napster, and the stream of file swapping companies that followed. The file-swapping companies now have their "Dr. Damn."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://zdnet.com.com/2100-1105-891761.html>

OVERVIEW OF ATTACK TRENDS

This paper in PDF format, gives a brief overview of recent trends that affect the ability of organizations and individuals to use the Internet safely.

Link: http://www.cert.org/archive/pdf/attack_trends.pdf

Security issues

All vulnerabilities are located at:
<http://net-security.org/text/bugs>

MULTIPLE VULNERABILITIES IN PVOTE 1.5

A lot of the scripts in the PVote package do not properly check who the user are and therefore lets anyone add or delete polls at any time. Also, there exist a vulnerability that lets anyone change the Admin password or set it to null.

Link: <http://www.net-security.org/text/bugs/1019476993,38850,.shtml>

COLDFUSION PATH DISCLOSURE

Requests for certain DOS-devices are parsed by the isapi filter that handles .cfm and .dbm and result in error messages containing the physical path to the web root.

Link: <http://www.net-security.org/text/bugs/1019477014,79839,.shtml>

FOUNDSTONE FSCAN FORMAT STRING BUG

A flaw in Foundstone Fscan could result in a malicious service banner overwriting the stack and the EIP on the PC performing the scanning.

Link: <http://www.net-security.org/text/bugs/1019477031,84756,.shtml>

MICROSOFT DISTRIBUTED TRANSACTION COORDINATOR DOS

A flaw in the way MSDTC handles malformed packets could allow an attacker to hang the service and exhaust resources on the Server.

Link: <http://www.net-security.org/text/bugs/1019477052,69639,.shtml>

DENIAL OF SERVICE IN MULTIPLE IE VERSIONS

OBJECT elements are used for embedded OLE in HTML documents.

A flaw in the way Microsoft Internet Explorer processes this directive allows a page that causes a loop in object dependency, or loads itself in a certain manner in an OBJECT, to completely crash Internet Explorer.

Link: <http://www.net-security.org/text/bugs/1019477085,70900,.shtml>

POSTCALENDAR VULNERABILITY

A user can add an event with unchecked HTML tags in. This includes the <script> tag which allows an attacker to steal cookies, redirect the site and much more.

Link: <http://www.net-security.org/text/bugs/1019477102,43921,.shtml>

SNITZ FORUMS 2000 SQL QUERY VULNERABILITY

Snitz Forums 2000 is open source ASP-based web forum software. It runs on Microsoft Windows operating systems. A vulnerability

exists in Snitz Forums 2000 which makes it possible for a malicious user to remotely manipulate the logic of SQL queries. As a result, it may be possible for attackers to view all data in the forum's database. This vulnerability can be exploited with a web browser.
Link: <http://www.net-security.org/text/bugs/1019477123,12504,.shtml>

INTELLISOL XPEDE MULTIPLE VULNERABILITIES

There are several serious vulnerabilities both in the product design and its implementation.

Link: <http://www.net-security.org/text/bugs/1019477140,62569,.shtml>

CGISCRIP.TNET - CSMAILTO.CGI - REMOTE COMMAND EXECUTION

The script stores all its configuration data in hidden form fields, relying on the user to accurately (and honestly) echo that information back with each form submission. The only thing allowing a user from having complete control over the script is a referer check which is easily bypassed.

Link: <http://www.net-security.org/text/bugs/1019726143,95500,.shtml>

DENIAL OF SERVICE IN MOSIX 1.5.X

Mosix and probably open-Mosix are vulnerable to an Denial of Service attack, the problem lies in the mosix-protocol-stack, mosix are not able to handle garbage-packets correctly.

Link: <http://www.net-security.org/text/bugs/1019726369,69164,.shtml>

KERBEROS4 FTP CLIENT HEAP OVERFLOW

A bug in the code may cause a heap overflow which leads to remote code execution. The overflow occurs when the server responds to client's request for passive mode. If the server responds with a long reply in the place of IP and port, pasv buffer will overflow.

Link: <http://www.net-security.org/text/bugs/1019726489,87199,.shtml>

PHPROJEKT MULTIPLE VULNERABILITIES

There are many security holes in this program divided into five categories.

Link: <http://www.net-security.org/text/bugs/1019726552,4777,.shtml>

LABVIEW WEB SERVER DOS VULNERABILITY

When the malformed HTTP request is received by the LabVIEW Web Server, the entire LabVIEW application crashes, including the Web Server, and any other LabVIEW programs.

Link: <http://www.net-security.org/text/bugs/1019726687,76035,.shtml>

LIL' HTTP SERVER DIRECTORY TRAVERSAL VULNERABILITY

Lil' HTTP Server is a Windows HTTP server that supports several features in a relatively compact application. It is vulnerable to a classic (stupid) attack:

[http://\[target\]/../../../../windows/win.ini](http://[target]/../../../../windows/win.ini)

Link: <http://www.net-security.org/text/bugs/1019726959,52817,.shtml>

SUDO PASSWORD PROMPT VULNERABILITY

Sudo - A popular utility for allowing users to execute commands as other users contains a vulnerability which may be exploited to execute arbitrary commands.

Link: <http://www.net-security.org/text/bugs/1019823011,90906,.shtml>

Security world

All press releases are located at:
<http://net-security.org/text/press>

SOPHOS AWARDED TWO QUEEN'S AWARDS FOR ENTERPRISE

Sophos, a world leader in corporate anti-virus protection, has been awarded two prestigious Queen's Awards for Enterprise, the UK's top awards for business performance. The Oxfordshire-based company has been rewarded for both its technical excellence and business acumen by receiving awards in two separate categories - 'Innovation' and 'International Trade'.

Press release:

< <http://www.net-security.org/text/press/1019466655,69989,.shtml> >

TRUSECURE ANNOUNCES NEXT GENERATION SERVICE FOR CENTRAL MANAGEMENT OF COMPREHENSIVE SECURITY ASSURANCE

TruSecure Corporation, a leading managed security services provider, announced TruSecure 5.0, the next evolutionary step for companies wanting to centralize the comprehensive management of their enterprise security efforts. In a related announcement, TruSecure also announced TruSecure Lifecycle Risk Management (LRM), the only enterprise security services strategy that continuously measures, manages and monitors information security risks.

Press release:

< <http://www.net-security.org/text/press/1019523913,31189,.shtml> >

TRUSECURE INTRODUCES LIFECYCLE RISK MANAGEMENT STRATEGY

TruSecure Corporation, a leading managed security services provider, unveiled its comprehensive business strategy that enables organizations to adopt a more holistic approach to information security. Called Lifecycle Risk Management (LRM), the strategy

brings together technologies, expert support and real-time intelligence that address all the essential phases and processes of information risk management. TruSecure now offers the only integrated, enterprise-scale programs that allow organizations to build and assure a continuously effective security posture.

Press release:

< <http://www.net-security.org/text/press/1019523943,80679,.shtml> >

AUTHENEX AND FUNK SOFTWARE PROVIDE INTEGRATED TWO-FACTOR SECURITY SOLUTION

Authenex, a leading developer of strong authentication and encryption applications, today announced an alliance with Funk Software, the developer of the market-leading Steel-Belted Radius family of RADIUS/AAA servers for remote and wireless LAN user authentication, authorization and accounting. Together the companies will provide a seamless security solution that leverages Authenex's two-factor strong encryption A-Key system.

Press release:

< <http://www.net-security.org/text/press/1019523965,38037,.shtml> >

NETWORK-1 EXPANDS MANAGEMENT TEAM WITH FORMER COMPUTER ASSOCIATES/CHEYENNE SOFTWARE EXECUTIVES

Network-1 Security Solutions, Inc., a technology leader in intrusion prevention software, announced today the addition of two key executives to the Company's management team as part of its continuing efforts to position Network-1 for long-term success in the security software market. Jonathan Greene will oversee the Company's product marketing strategy and business development activities. Jonna Stopnik will lead Network-1's partnership and distribution channel development initiatives.

Press release:

< <http://www.net-security.org/text/press/1019523991,73422,.shtml> >

GUARDEDNET'S NEUSECURE NAMED A 2002 FINALIST BY NETWORK COMPUTING FOR WELL-CONNECTED AWARD

GuardedNet announces that its neuSECURE enterprise security management software was selected by CMP Media's Network Computing magazine, as a 2002 Well-Connected Award finalist in the category of Security Information Management (SIM). The product was chosen because of its combination of real-time correlation and threat analysis, trouble-ticket tracking and report generation that makes it the most flexible, cost effective solution in the security information management (SIM) marketplace.

Press release:

< <http://www.net-security.org/text/press/1019524015,43869,.shtml> >

F-SECURE ANTI-VIRUS FOR LINUX AS A SERVICE FOR CAPNOVA CUSTOMERS

F-Secure Corporation and Capnova Oy of Finland announced that they have signed an agreement to use F-Secure Anti-Virus for Linux to check the e-mail inboxes of Capnova's webhotel customers for viruses.

Press release:

< <http://www.net-security.org/text/press/1019643931,23217,.shtml> >

SYBARI PARTNERS WITH KASPERSKY LABS TO DELIVER A POWERFUL DEFENSE AGAINST VIRUSES

Sybari Software, Inc., the premier developers of Antigen, a comprehensive antivirus, content-management, and e-mail security solution for Microsoft Exchange and Lotus Domino environments, announced that the company has forged a partnership with Kaspersky Labs, an international data security company focused on the development, marketing, and distribution of leading information security technologies and software.

Press release:

< <http://www.net-security.org/text/press/1019645302,56474,.shtml> >

F-SECURE ANTI-VIRUS FOR LINUX AS A SERVICE FOR CAPNOVA CUSTOMERS

F-Secure Corporation is still monitoring the Klez.H virus, which has been spreading around the world for a week. Klez.H is a mass mailing Windows worm, which can generate massive amounts of e-mail traffic.

Press release:

< <http://www.net-security.org/text/press/1019645338,15427,.shtml> >

GFI MAILSECURITY EARNS CHECKMARK CERTIFICATION FOR ANTI-VIRUS PROTECTION

GFI announced that MailSecurity, its new email security package for Exchange and SMTP servers, has been awarded Anti-Virus Checkmark Level 1 certification from West Coast Labs. The certification ensures that GFI MailSecurity meets the Checkmark program's rigorous standards for detecting in-the-wild viruses.

Press release:

< <http://www.net-security.org/text/press/1019645882,47403,.shtml> >

IDEFENSE TO DELIVER ALERT CYBER-THREAT INTELLIGENCE TO
THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

The U.S. Department of Health and Human Services (HHS) selected iDEFENSE Inc. to provide cyber-threat intelligence across its entire information technology enterprise. iDEFENSE, a global security intelligence company, generates thousands of Intelligence Reports on a variety of cyber threats.

Press release:

< <http://www.net-security.org/text/press/1019675323,76485,.shtml> >

F-SECURE GROUP'S FINANCIAL RESULTS JANUARY 1 - MARCH 31, 2002

For the 1st quarter of 2002, F-Secure reported revenues of 10.0 million euros. This represents no change from the first quarter of 2001 and a decrease of 10% from the previous quarter. The decline was due to normal seasonal variation and a continuing slowdown in corporate spending.

Press release:

< <http://www.net-security.org/text/press/1019725089,81570,.shtml> >

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org
<http://net-security.org>
<http://security-db.com>

Unsubscribe by sending your e-mail address to:
info@net-security.org with UNSUBSCRIBE in the
message body.

The archive of the newsletter in TXT and PDF format is available
here: <http://www.net-security.org/news/archive/newsletter>