



### **HNS Newsletter**

Issue 159 - 28.04.2003.

<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>.

---

#### **SURFCONTROL E-MAIL FILTER**

---

Spam is a four-letter word - its annoying and can put the brakes on business communications. Combat Spam with the most accurate multi-layered software solution available.

**Download and use SurfControl E-mail Filter free for 30-days.**

<http://www.surfcontrol.com/go/zhnsppl>

---

#### **Table of contents:**

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

[ **Security news** ]

---

#### **UNDERSTANDING SOLARIS 9 DIRECTORY SERVICES**

This article examines the differences between the Solaris 8 Operating Environment (Solaris OE) Lightweight Directory Access Protocol (LDAP) Client and the Solaris 9 OE Secured LDAP Client, and explains how to support them on the same directory server.

>> <http://net-security.org/news.php?id=2438>

#### FILMS ALTERED TO FOIL CAMCORDER PIRATES

Hollywood sends enforcers with night-vision goggles into movie theaters and puts metal detectors outside advance screening rooms, but still the industry can't stop pirates from recording films. So the movie industry is trying to fight back with a high-tech solution of its own.

>> <http://net-security.org/news.php?id=2439>

#### OFFICE WORKERS GIVE AWAY PASSWORDS FOR A CHEAP PEN

Workers are prepared to give away their passwords for a cheap pen, according to a somewhat unscientific - but still illuminating - survey published today.

>> <http://net-security.org/news.php?id=2440>

#### SECURING 802.11 TRANSMISSIONS

The deployment of various wireless LANs and Wi-Fi networks or configurations are under consideration by many organizations, and network security is a major concern.

>> <http://net-security.org/news.php?id=2441>

#### HP CEMENTS THE BASTILLE

Hewlett-Packard has released Version 2.0 of the Bastille security tool and a new Install-Time Security product for its HP-UX operating system.

>> <http://net-security.org/news.php?id=2442>

#### SECURING DIGITAL CONTENT

As Microsoft prepares to release the beta version of its controversial Rights Management Services, a security company has been working on technology that could trump Microsoft's and make it easier for companies to control digital content.

>> <http://net-security.org/news.php?id=2443>

#### CYBERSTALKING IS INCREASING

Cyberstalking is increasing across America according to a study released by Wired Safety, an online safety and help group.

>> <http://net-security.org/news.php?id=2444>

#### ACM WORKSHOP ON WIRELESS SECURITY RFP ANNOUNCED

The objective of this workshop is to bring together researchers from the different research communities in wireless networking, security, and dependability, with the goal of fostering interaction among them.

>> <http://net-security.org/news.php?id=2445>

#### MELDING IT, PHYSICAL SECURITY

Computer Associates, Gemplus and several other companies announced the formation of a group that is working on open specifications and best practices for integrating information security and physical security.

>> <http://net-security.org/news.php?id=2450>

#### TELEPHONE COMPANY TRYING TO COLLECT BILLS FROM THE VICTIMS OF HACKERS

Victims of a telephone hacking swindle are disputing a contention that they are responsible for costly long-distance calls fraudulently made through their voice mail systems.

>> <http://net-security.org/news.php?id=2451>

#### ON CURES THAT ARE WORSE THAN THE DISEASE

Which is worst for the Internet: computer viruses, spam that advertises anti-virus products, or clueless anti-spam solutions?

>> <http://net-security.org/news.php?id=2453>

#### INSIDE CISCO'S EAVESDROPPING APPARATUS

Cisco Systems has created a more efficient and targeted way for police and intelligence agencies to eavesdrop on people whose Internet service provider uses their company's routers.

>> <http://net-security.org/news.php?id=2454>

#### SCHMIDT LEAVES CYBER-SECURITY POST

White House cyber-security adviser Howard Schmidt resigned from his government post Monday, the second high-level official to leave President Bush's Critical Infrastructure Protection Board in as many months.

>> <http://net-security.org/news.php?id=2456>

#### ANTI-VIRUS DEFENCE IN DEPTH

This article will discuss defence in depth as it applies to anti-virus protection. While there are many papers written on this topic, most miss out on two crucial components: layered best of breed AV protection and centralized reporting and control.

>> <http://net-security.org/news.php?id=2457>

#### MICROSOFT'S SECURITY STRAW MAN

Is there a "war room" somewhere where scores of Kevin Mitnick wannabes are pounding away at Microsoft products, trying to find weaknesses? If not, too bad.

>> <http://net-security.org/news.php?id=2458>

#### ADRIAN LAMO - A DUTY TO HACK

Adrian Lamo, the 22-year-old "homeless hacker" famous for raiding New York Times computers, pursues his vision of public service by cracking another major corporate network. It's a crime, of course. It's also what he was born to do.

>> <http://net-security.org/news.php?id=2459>

#### AL-JEZEERA, THE FIRST AMENDMENT, AND SECURITY PROFESSIONALS

While attempts to disrupt Web broadcasts of Al-Jazeera may seem like a distant concern, they reflect the problems that should concern security professionals everywhere.

>> <http://net-security.org/news.php?id=2460>

#### IDS: THE INTEGRATED PARTNER FOR YOUR FIREWALL

A firewall shouldn't be your only means of protection. That's

why Intrusion Detection Systems are becoming a necessary complement for existing firewall solutions.

>> <http://net-security.org/news.php?id=2461>

#### WINDOWS 2003 LEAVES SECURITY GAPS

Users will need to take care over deployment options.

>> <http://net-security.org/news.php?id=2462>

#### MOST WOULD REVEAL THEIR COMPUTER PASSWORDS

Computer security remains lax, with a new survey showing that most office workers would give away their computer passwords in exchange for a cheap pen.

>> <http://net-security.org/news.php?id=2463>

#### ATTACKER CAUSES HAVOC FOR WEBSITES

Up to 1,500 websites could have been affected by a recent attack.

>> <http://net-security.org/news.php?id=2464>

#### RUXCON: A SECURITY CONFERENCE WITH A DIFFERENCE

From mysterious men on rooftops with telephoto lenses, to attendees trying to use "household appliances to launch non conventional buffer overflow attacks", the inaugural Ruxcon IT security conference in Sydney had it all.

>> <http://net-security.org/news.php?id=2465>

#### WILL CALIFORNIA LAW SPUR STORAGE CRYPTO?

While the practice of encrypting sensitive data across the Internet has long been established, there is far less consensus on the value of encrypting data "at rest" in a SAN. Now, a new law in California could provide a decisive answer to that question.

>> <http://net-security.org/news.php?id=2466>

#### DEFENSE AGENCY PULLS OPENBSD FUNDING

The unused portion of a grant from the Defense Advanced Research Projects Agency (DARPA) to fund development of the open-source operating system Open Berkeley Software Design (OpenBSD) has been pulled for unspecified reasons.

>> <http://net-security.org/news.php?id=2467>

#### WLAN WARS: WITH N+I COMING, WIRELESS PRODUCTS ABOUND

The battle for the enterprise wireless LAN market continues in the run-up to the Networld+Interop conference, and between now and the start of N+I, seven companies are slated to introduce WLAN systems that put the management of dumb access points at the core of the network.

>> <http://net-security.org/news.php?id=2469>

#### RETAILERS REPORT SALES BOUNCE USING SECURITY CERTIFICATE

Sites showing proof of increased Web security say that up to a third more people went beyond shopping and actually bought, according to an auditing firm.

>> <http://net-security.org/news.php?id=2470>

#### OPEN-SOURCE SECURITY SHINES IN SAMBA CASE

Recently discovered security holes in Samba were serious threats to companies using the popular freeware, which enables end users to access and use files, printers and other commonly shared resources on a company's network or via the Internet.

>> <http://net-security.org/news.php?id=2471>

#### SNORT PROBLEMS

Noel Davis looks at buffer overflows in Snort and SheerDNS, and problems in Xinetd, xie-cron, Oracle E-Business Suite FND, xfsdump, Ximian Evolution, GtkHTML, kdegraphics, and psbanner.

>> <http://net-security.org/news.php?id=2472>

#### APACHE WEB SERVING WITH JAGUAR, PART THREE

In the first part of this series, Kevin showed you how to easily start serving web pages from your Mac OS X computer. In the second article, he explored the world of CGI access. Today, he looks at PHP and simple access controls.

>> <http://net-security.org/news.php?id=2473>

#### SCHOOLS TEST "EYE SCANNER" SECURITY

Plumsted district's three schools became the test site for a cutting-edge eye-recognition security system designed to keep out strangers.

>> <http://net-security.org/news.php?id=2474>

#### SQL SERVER STRING, CURSOR, SECURITY AND ROWSET FUNCTIONS

Baya Pavliashvili continues his series on system-supplied functions by discussing the string, security, cursor, and rowset functions. Also discover some extra features, which are not mentioned in the SQL Server online documentation.

>> <http://net-security.org/news.php?id=2475>

#### CYBER WAR GAME TESTS FUTURE TROOPS

In a basement lab littered with computers, monitors and chalkboard diagrams, 14 Naval Academy midshipmen are buzzing about the latest hacker assault on the computer network they created.

>> <http://net-security.org/news.php?id=2476>

#### THEO DE RAADT: HACKATHON WILL GO ON

Theo de Raadt intends to host a gathering of coders in Canada next month, despite a decision by a U.S. military research agency to withdraw funding for the event.

>> <http://net-security.org/news.php?id=2479>

#### EX-CON MAN ADVISES ON IDENTITY THEFT

Digital thieves are becoming more professional and hard to fight, he warns.

>> <http://net-security.org/news.php?id=2481>

#### MICROSOFT SNAGS CD COPY-BLOCK DEAL

Microsoft dug its roots a little deeper into the music business Wednesday, as copy-protection company Macrovision agreed to license its Windows digital rights management technology for CDs.  
>> <http://net-security.org/news.php?id=2482>

#### SOFTWARE DEVELOPER FEARS LEGAL TAR PIT

An independent coder says a new copyright law could make one of his apps illegal.  
>> <http://net-security.org/news.php?id=2483>

#### RUNNING LINUX AND NETFILTER ON NOKIA IP SERIES HARDWARE

A tutorial for setting up some open-source software on market leading, proprietary firewall hardware.  
>> <http://net-security.org/news.php?id=2484>

#### WEB USERS WARY ON PRIVACY, NOT SECURITY

Web users are overcoming fears of sending credit card details over the internet, but are increasingly worried about the privacy of personal information, according to research.  
>> <http://net-security.org/news.php?id=2485>

#### WHAT HACKERS CAN TEACH YOU ABOUT SECURITY

Robert Vamosi: We should listen when Kevin Mitnick says that traditional network security tools aren't enough to keep our information safe.  
>> <http://net-security.org/news.php?id=2486>

#### AUDITING WEB SITE AUTHENTICATION

This is the first part of a two-part article discussing a standard audit procedure consisting of a list of questions to test Web site authentication schemes.  
>> <http://net-security.org/news.php?id=2487>

#### THE PARANOIA THAT PAID OFF

Fears of cyberterrorism during the war on Iraq proved unfounded, says Peter Rojas, but increased online security will benefit us all.  
>> <http://net-security.org/news.php?id=2488>

---

## [ Vulnerabilities ]

All vulnerabilities are located here:

[http://www.net-security.org/archive\\_vuln.php](http://www.net-security.org/archive_vuln.php)

-----  
Cisco Secure ACS Web Management Interface Remote  
Buffer Overflow Vulnerability

>> <http://net-security.org/vuln.php?id=2638>

Internet Explorer ActiveX Control Heap Overflow Vulnerability

>> <http://net-security.org/vuln.php?id=2637>

VisNetic ActiveDefense Denial of Service Vulnerability

>> <http://net-security.org/vuln.php?id=2636>

Options Parsing Tool Library Multiple Buffer  
Overflow Vulnerabilities

>> <http://net-security.org/vuln.php?id=2635>

PHP-Nuke 6.5 FINAL Cross Site Scripting Vulnerability

>> <http://net-security.org/vuln.php?id=2634>

XMB SQL Injection Vulnerability

>> <http://net-security.org/vuln.php?id=2633>

YABB SE Remote Command Execution Vulnerability

>> <http://net-security.org/vuln.php?id=2632>

AN HTTPd Sample Script File Truncation Vulnerability

>> <http://net-security.org/vuln.php?id=2631>

Windows XP Service Control Manager Service Shutdown  
Mechanism Race Condition Vulnerability

>> <http://net-security.org/vuln.php?id=2630>

Monkey HTTP Daemon Remote Buffer Overflow Vulnerability

>> <http://net-security.org/vuln.php?id=2629>

PTNews v1.7.7 Administrative Functions Unprivileged  
Access Vulnerability

>> <http://net-security.org/vuln.php?id=2628>

mod\_ntlm Multiple Remote Vulnerabilities

>> <http://net-security.org/vuln.php?id=2627>

BadBlue Arbitrary Administrative Actions Vulnerability  
>> <http://net-security.org/vuln.php?id=2626>

-----

[ **Advisories** ]

All advisories are located at:  
[http://www.net-security.org/archive\\_adv.php](http://www.net-security.org/archive_adv.php)

-----

SGI Security Advisory - Multiple Vulnerabilities  
in BSD LPR Subsystem  
>> <http://net-security.org/advisory.php?id=1961>

SGI Security Advisory - Vulnerability in nsd LDAP  
Implementation  
>> <http://net-security.org/advisory.php?id=1960>

Red Hat Security Advisory - Updated m1CQ packages  
fix vulnerability  
>> <http://net-security.org/advisory.php?id=1959>

Mandrake Linux Security Update Advisory - ethereal  
>> <http://net-security.org/advisory.php?id=1958>

Red Hat Security Advisory - Updated LPRng packages  
fix psbanner vulnerability  
>> <http://net-security.org/advisory.php?id=1957>

Red Hat Security Advisory - Updated squirrelmail  
packages fix cross-site scripting  
>> <http://net-security.org/advisory.php?id=1956>

Mandrake Linux Security Update Advisory - kde3  
>> <http://net-security.org/advisory.php?id=1955>

Cisco Security Advisory - Cisco Catalyst Enable  
Password Bypass Vulnerability  
>> <http://net-security.org/advisory.php?id=1954>

Microsoft Security Bulletin MS03-014 - Cumulative  
Patch for Outlook Express  
>> <http://net-security.org/advisory.php?id=1953>

SuSE Security Announcement - KDE  
>> <http://net-security.org/advisory.php?id=1952>

Microsoft Security Bulletin MS03-015 - Cumulative  
Patch for Internet Explorer  
>> <http://net-security.org/advisory.php?id=1951>

Microsoft Security Bulletin MS03-007 - Unchecked Buffer  
In Windows Component Could Cause Server Compromise (revised)  
>> <http://net-security.org/advisory.php?id=1950>

Debian Security Advisory - New gkrellm-newsticker  
packages fix DoS and arbitrary command execution  
>> <http://net-security.org/advisory.php?id=1949>

Cisco Security Advisory -Cisco Secure Access Control  
Server for Windows Admin Buffer Overflow Vulnerability  
>> <http://net-security.org/advisory.php?id=1948>

SOT Linux Security Advisory - Updated samba package  
for SOT Linux 2002  
>> <http://net-security.org/advisory.php?id=1947>

SOT Linux Security Advisory - Updated kernel package  
for SOT Linux 2002  
>> <http://net-security.org/advisory.php?id=1946>

Debian Security Advisory - New mime-support packages  
fix temporary file race conditions  
>> <http://net-security.org/advisory.php?id=1945>

Red Hat Security Advisory - Updated tcpdump packages  
fix various vulnerabilities  
>> <http://net-security.org/advisory.php?id=1944>

Debian Security Advisory - New kdelibs packages fix  
arbitrary command execution  
>> <http://net-security.org/advisory.php?id=1943>

Conectiva Linux Security Announcement - tcpdump  
>> <http://net-security.org/advisory.php?id=1942>

Mandrake Linux Security Update Advisory - apache2  
>> <http://net-security.org/advisory.php?id=1941>

Debian Security Advisory - New mime-support packages  
fix temporary file race conditions  
>> <http://net-security.org/advisory.php?id=1940>

HP Security Bulletin - HP Tru64 UNIX/TruCluster Server -  
Cluster Alias/NFS Potential Security Vulnerability  
>> <http://net-security.org/advisory.php?id=1939>

HP Security Bulletin - HP Tru64 UNIX screend  
Potential Security Vulnerability  
>> <http://net-security.org/advisory.php?id=1938>

Conectiva Linux Security Announcement - balsa  
>> <http://net-security.org/advisory.php?id=1937>

Gentoo Linux Security Announcement - snort  
>> <http://net-security.org/advisory.php?id=1936>

Debian Security Advisory - New ircII packages fix  
DoS and arbitrary code execution  
>> <http://net-security.org/advisory.php?id=1935>

---

### [ Featured articles ]

All articles are located at:  
[http://www.net-security.org/articles\\_main.php](http://www.net-security.org/articles_main.php)

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

---

#### INTERVIEW WITH ANDREW G. MASON

The author of "Cisco Secure Virtual Private Networks" and "Cisco Secure Internet Security Solutions" talks about his writing and general security issues.

>> <http://www.net-security.org/article.php?id=467>

#### TRUSTED DEBIAN V1.0 OFFICIALLY RELEASED

The Trusted Debian project aims to create a highly secure but usable Linux platform. To accomplish this, the project will use currently available security solutions for Linux and knit these together to a highly secure Linux platform.

>> <http://www.net-security.org/article.php?id=469>

#### INTERVIEW WITH BILLY BARRON

The co-author of "Maximum Security 4/e" and an architect and developer at Avatier Corporation for cross-platform products, discusses his writing and other computer security topics.

>> <http://www.net-security.org/article.php?id=470>

#### HOW TO USE PASSWORDS SECURELY

Every day, more and more services and applications require password authentication. For this reason, we will be looking at the risks of using the same password for various services, and we'll go over some tips for making them more secure.

>> <http://www.net-security.org/article.php?id=471>

#### INTERVIEW WITH GREG VAUGHN

The enterprise application programmer and co-author of "Maximum Security 4/e" talks about the book and general security issues.

>> <http://www.net-security.org/article.php?id=472>

#### ACCESS CARDS: SECURING CORPORATE NETWORKS

The technology for strong user authentication, whether based on two or three factors, is already available to establish trusted digital ID credentials for secure access to multiple applications.

>> <http://net-security.org/article.php?id=473>

#### NETWORKS RISK GROUNDING WITHOUT AIRPORT-LEVEL SECURITY

Nigel Nigel Hawthorn, Marketing Director of Blue Coat Systems, compares security issues facing IT departments to the issues facing airports.

>> <http://net-security.org/article.php?id=474>

---

#### [ Reviews ]

All reviews are located at:

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

---

#### THE HACK-COUNTER HACK TRAINING COURSE: A NETWORK SECURITY SEMINAR FROM ED SKOUDIS

Some people prefer books that deliver a wealth of theoretical knowledge they can build on, while other always go for the hands-on experience. This course is all hands-on experience and lots of it.

>> <http://net-security.org/review.php?id=55>

#### HACK ATTACKS REVEALED: A COMPLETE REFERENCE FOR UNIX, WINDOWS, AND LINUX WITH CUSTOM SECURITY TOOLKIT 2/E

Every day we are introduced to new security vulnerabilities, successful hacking stories and predictions that things will go from bad to worse. The continuing growth of the Internet, as seen from ever growing number of new Internet users and companies doing their business online, is creating a new line

of possible victims susceptible to Internet attacks. As the author notes, the primary objective of this book is to lay a solid foundation from which to explore the world of security.  
>> <http://net-security.org/review.php?id=56>

#### THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY

Kevin Mitnick is one of the best-known figures in the world of computer security. There's a lot of controversy surrounding Mitnick - some regard him as a hacker, others as a cracker. The legendary Steve Wozniak wrote in the preface of the book: "Kevin Mitnick is one of the finest people I know." As the book came out, it's been frequently noted that this is like a method of redemption for Mitnick. I want you to read this review not thinking about anything you know about Kevin Mitnick and just concentrate on the knowledge packed into the book.  
>> <http://net-security.org/review.php?id=57>

---

#### [ Security world ]

All press releases are located at:  
[http://www.net-security.org/press\\_main.php](http://www.net-security.org/press_main.php)

---

Trend Micro Announces First Quarter Consolidated Results  
>> <http://net-security.org/press.php?id=1365>

Epson Chooses Trend Micro Enterprise Protection Strategy  
>> <http://net-security.org/press.php?id=1364>

Datakey Announces 2003 First Quarter Results  
>> <http://net-security.org/press.php?id=1363>

NetScreen Technologies, Inc. Reports Record Second Quarter Results  
>> <http://net-security.org/press.php?id=1362>

PureEdge E-forms Solutions Receive DoD Public Key Infrastructure Interoperability Certification  
>> <http://net-security.org/press.php?id=1361>

RAV AntiVirus Provides Security Support for SCOoffice Mail Server  
>> <http://net-security.org/press.php?id=1360>

Websense Enterprise for Small and Medium Businesses Offers Easy, Stand-Alone Deployment

>> <http://net-security.org/press.php?id=1359>

Latest Cyberstalking Statistics Released

>> <http://net-security.org/press.php?id=1358>

Ubizen and Saudi Telecom Open Doors to New Security Operations Center

>> <http://net-security.org/press.php?id=1357>

nCipher Delivers Enhanced Security to Web Applications

>> <http://net-security.org/press.php?id=1356>

Zix Corporation Provides National Imaging Associates Inc. with Comprehensive e-Messaging Protection

>> <http://net-security.org/press.php?id=1355>

ZixCorp is Selected By University of Utah Health Sciences Center to Provide Enterprise-wide Email Security in Compliance with HIPAA

>> <http://net-security.org/press.php?id=1354>

IT Decision-Makers Identify Most Pressing Security Topics In Latest Sage Technology Roundtable

>> <http://net-security.org/press.php?id=1353>

---

## [ Security Software ]

Windows software is located at:

[http://net-security.org/software\\_main.php?cat=1](http://net-security.org/software_main.php?cat=1)

Linux software is located at:

[http://net-security.org/software\\_main.php?cat=2](http://net-security.org/software_main.php?cat=2)

---

### AMRITA VPN 0.91

Amrita VPN is an easy-to-use open source VPN solution that runs on the GNU/Linux platform. The implementation is fully in userspace and requires no kernel patches or enhancements. It uses SSL for strong encryption and authentication.

>> <http://www.net-security.org/software.php?id=484>

### SCAPY 0.9.12BETA

Scapy is a powerful interactive packet manipulation tool, packet generator, network scanner, network discovery tool, and packet sniffer.

>> <http://www.net-security.org/software.php?id=485>

[ **Virus News** ]

All virus news are located at:

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

-----  
New Coronex Worm Exploits SARS Worries  
>> [http://net-security.org/virus\\_news.php?id=220](http://net-security.org/virus_news.php?id=220)  
-----

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 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  
[http://www.net-security.org/newsletter\\_archive.php](http://www.net-security.org/newsletter_archive.php)

-----  
**SURFCONTROL E-MAIL FILTER**  
-----

Spam is a four-letter word - its annoying and can put the brakes on business communications. Combat Spam with the most accurate multi-layered software solution available.

**Download and use SurfControl E-mail Filter free for 30-days.**

-----  
<http://www.surfcontrol.com/go/zhnsppl>  
-----