



HNS Newsletter

Issue 156 - 07.04.2003.

<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>.

ALERT: How a Hacker Launches a SQL Injection Attack - Step-by-Step!

It's as simple as placing additional SQL commands into an input box on a web form giving hackers complete access to all your backend data! Firewalls and IDS will not stop SQL Injection attempts because they are NOT seen as intrusions.

Download this *FREE* white paper from SPI Dynamics for a complete guide to protection!

<http://www.spidynamics.com/mktg/sqlinjection29>

Accurate Anti-Spam Software - Download a Free Trial

>> <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]

BIG BROTHER IS WATCHING YOU SHOP

Commercial databases, such as credit card records, grocery purchases and hotel bills, are the latest pool of information the government says it has a right to collect.

>> <http://www.net-security.org/news.php?id=2276>

CRACKERS STRIKE GEORGIA TECH COMPUTER, GAIN CREDIT CARD DATA

Crackers invaded a computer at Georgia Tech and copied names, addresses and - in some cases - credit card information for 57,000 patrons of the Ferst Center for the Arts.

>> <http://www.net-security.org/news.php?id=2277>

USING POWERDNS

This article covers some of the basics of using PowerDNS and its Web-based front-end PowerAdmin.

>> <http://www.net-security.org/news.php?id=2278>

ENCRYPTION BACKERS BRACE FOR NEW THREATS

Cheating on income taxes or neglecting to pay sales taxes on online shopping could get you 5 extra years in prison if the government succeeds in restricting data-scrambling technology.

>> <http://www.net-security.org/news.php?id=2283>

MICROSOFT BOLSTERS WI-FI SECURITY IN XP

Microsoft Corp will offer users of its Windows XP operating system free upgrades to beef up wireless LAN security.

>> <http://www.net-security.org/news.php?id=2284>

HACKER EYES XBOX REWARD

The \$100,000 reward promised by Lindows founder Michael Robertson could have been won by a hacker who found a buffer overflow flaw in a 007 Xbox game.

>> <http://www.net-security.org/news.php?id=2287>

VULNERABILITIES IN THE MEDIA - WHO TO TRUST?

There are a variety of people and entities that publish information about security problems. Who should you trust?

>> <http://www.net-security.org/news.php?id=2288>

WS-I TO CLEAR PATH FOR WEB SERVICES SECURITY

The Web Services Interoperability Organization (WS-I) has set up a working group to clear a way through overlapping proposals about Web services security.

>> <http://www.net-security.org/news.php?id=2292>

U.S. INFORMATION SECURITY LAW, PART 2

This is the second part of a four-part series looking at U.S.

information security laws and the way those laws affect security professionals.

>> <http://www.net-security.org/news.php?id=2293>

DOMAIN AUTHENTICATION SETS XANDROS DESKTOP APART

The Xandros software development manager talks about domain authentication - one of the essential keys to integrating with, and eventually migrating from, existing Windows networking infrastructures.

>> <http://www.net-security.org/news.php?id=2294>

TRANSACTION SECURITY HARMING WEB SERVICES

Unsecured networks making widespread use of web services impractical, says report.

>> <http://www.net-security.org/news.php?id=2297>

BUGWATCH: NEW ASSUMPTIONS, NEW PROBLEMS

Jude O'Reilly, director of product marketing at Aventail, considers solutions to address the new age of remote access in a world where IT may not control the network, user or desktop.

>> <http://www.net-security.org/news.php?id=2298>

SPYWARE: IT'S LURKING ON YOUR MACHINE

This article looks at common forms of spyware, spyware delivery methods, and a cross-section of tools you can use to start a spy hunt on your machine.

>> <http://www.net-security.org/news.php?id=2299>

DO PRIVACY FEARS ALLOW TERRORISM?

At a gathering of technology and privacy experts, a lawyer for a conservative think tank has one request: Stop the "hysterical cries" over loss of privacy and let the government do what it must to prevent terrorism.

>> <http://www.net-security.org/news.php?id=2304>

SPAM PIPS VIRUSES AS BIGGEST WEB PROBLEM

Spam is overtaking viruses as the biggest pain for businesses using the web.

>> <http://www.net-security.org/news.php?id=2305>

WORMS GROW IN FIRST PART OF 2003

The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months, according to a report by ISS.

>> <http://www.net-security.org/news.php?id=2306>

NO CODE IS UNBREAKABLE - SO WHAT'S GOOD ENOUGH?

When shopping for a new security solution, you should look for a company that backs up its hype with detailed information on how its product works, what algorithms are used and how the product has been tested.

>> <http://www.net-security.org/news.php?id=2307>

IN SEARCH OF NETWORK SECURITY

The challenges of managing a user's network identity and multiple, disconnected identities scattered across isolated Internet sites took center stage during Wednesday's keynote at the InfoWorld CTO Forum.

>> <http://www.net-security.org/news.php?id=2308>

FREE LINUX SOFTWARE WILL HELP DETECT CYBER ATTACKS

FloodGuard Alert software can detect a variety of attacks, including distributed denial of service, distributed reflective denial of service, Worm propagation, and other flooding attacks.

>> <http://www.net-security.org/news.php?id=2309>

Stop Spam Now - Free SurfControl E-mail Filter Trial

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

[Vulnerabilities]

All vulnerabilities are located here:

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

Interbase ISC_LOCK_ENV Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2588>

Netgear FM114P ProSafe Wireless Router WAN Username and Password Retrieval Vulnerability

>> <http://www.net-security.org/vuln.php?id=2587>

Progress PROSTARTUP Root Owned File Reading Vulnerability

>> <http://www.net-security.org/vuln.php?id=2586>

Buffalo AirStation G54 Denial of Service Vulnerability

>> <http://www.net-security.org/vuln.php?id=2585>

AOLServer Proxy Daemon API unformatted syslog() call

>> <http://www.net-security.org/vuln.php?id=2584>

IkonBoard Arbitrary Command Execution Vulnerability

>> <http://www.net-security.org/vuln.php?id=2583>

Microsoft Terminal Services Man in The Middle Attacks

>> <http://www.net-security.org/vuln.php?id=2582>

BEA WebLogic Internal Hostname Disclosure Vulnerability

>> <http://www.net-security.org/vuln.php?id=2581>

Phorum 3.4 Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=2580>

Python Documentation Server Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=2579>

Xoops glossary 1.3.x Module Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=2578>

Progress Database DLC Local Root Exploit Vulnerability

>> <http://www.net-security.org/vuln.php?id=2577>

D-Link DSL-300G/DSL-300G+ Broadband Router Multiple Security Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2576>

BRS WebWeaver Multiple Security Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2575>

Sambar Server SysUser Login System Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2574>

TYPSoft FTP Server Directory Traversal Vulnerability

>> <http://www.net-security.org/vuln.php?id=2573>

Windows QuickTime Player Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2572>

Solaris dtsession Heap Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2571>

Solaris lpq Stack Buffer Overflow Vulnerability

>> <http://www.net-security.org/vuln.php?id=2570>

Kerio WinRoute Firewall Denial of Service Vulnerability

>> <http://www.net-security.org/vuln.php?id=2569>

SAP DB World Writable Server Binaries

>> <http://www.net-security.org/vuln.php?id=2568>

HP Instant TopTools Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2567>

Personal FTP Server Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=2566>

Mod_Survey ENV Tag Vulnerability
>> <http://www.net-security.org/vuln.php?id=2565>

CCLOG USER-AGENT and REFERER Script Injection Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2564>

CCGuestBook Script Injection Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2563>

Michal Zalewski on Sendmail Vulnerability
>> <http://www.net-security.org/vuln.php?id=2562>

SurfControl E-mail Filter Stops Spam - Free 30-Day Trial
>> <http://www.surfcontrol.com/go/zhnspl>

[Advisories]

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

Conectiva Linux Security Announcement - file
>> <http://www.net-security.org/advisory.php?id=1862>

Conectiva Linux Security Announcement - dhcp
>> <http://www.net-security.org/advisory.php?id=1861>

Conectiva Linux Security Announcement - sendmail
>> <http://www.net-security.org/advisory.php?id=1860>

Conectiva Linux Security Announcement - samba
>> <http://www.net-security.org/advisory.php?id=1859>

Conectiva Linux Security Announcement - snort
>> <http://www.net-security.org/advisory.php?id=1858>

Debian Security Advisory - New sendmail packages fix denial of service
>> <http://www.net-security.org/advisory.php?id=1857>

SuSE Security Announcement - openssl
>> <http://www.net-security.org/advisory.php?id=1856>

Red Hat Security Advisory - Updated balsa and mutt packages fix vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1855>

NetBSD Security Advisory - sendmail buffer overrun in prescan() address parser
>> <http://www.net-security.org/advisory.php?id=1854>

NetBSD Security Advisory - Cryptographic weaknesses in Kerberos v4 protocol
>> <http://www.net-security.org/advisory.php?id=1853>

Debian Security Advisory - New Linux kernel packages (s390) fix local root exploit
>> <http://www.net-security.org/advisory.php?id=1852>

SCO Security Advisory - OpenLinux: sendmail sign extension buffer overflow
>> <http://www.net-security.org/advisory.php?id=1851>

Debian Security Advisory - New apcupsd packages fix remote root exploit
>> <http://www.net-security.org/advisory.php?id=1850>

SGI Security Advisory - Sendmail parseaddr security vulnerability
>> <http://www.net-security.org/advisory.php?id=1849>

Red Hat Security Advisory - Updated NetPBM packages fix multiple vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1848>

Red Hat Security Advisory - Updated Eye of GNOME packages fix vulnerability
>> <http://www.net-security.org/advisory.php?id=1847>

Debian Security Advisory - New lpr-ppd packages fix local root exploit
>> <http://www.net-security.org/advisory.php?id=1846>

SuSE Security Announcement - sendmail, sendmail-tls

>> <http://www.net-security.org/advisory.php?id=1845>

Red Hat Security Advisory - Updated kerberos packages
fix various vulnerabilities

>> <http://www.net-security.org/advisory.php?id=1844>

Red Hat Security Advisory - Updated vsftpd packages
re-enable tcp_wrappers support

>> <http://www.net-security.org/advisory.php?id=1843>

Red Hat Security Advisory - New samba packages fix
security vulnerabilities

>> <http://www.net-security.org/advisory.php?id=1842>

Red Hat Security Advisory - Updated OpenSSL packages
fix vulnerabilities

>> <http://www.net-security.org/advisory.php?id=1841>

Mandrake Linux Security Update Advisory - krb5

>> <http://www.net-security.org/advisory.php?id=1840>

Mandrake Linux Security Update Advisory - sendmail

>> <http://www.net-security.org/advisory.php?id=1839>

Mandrake Linux Security Update Advisory - mutt

>> <http://www.net-security.org/advisory.php?id=1838>

Mandrake Linux Security Update Advisory - Eterm

>> <http://www.net-security.org/advisory.php?id=1837>

HP Security Bulletin - HP Tru64 UNIX - Potential Buffer
Overflows and Potential Denial of Service

>> <http://www.net-security.org/advisory.php?id=1836>

HP Security Bulletin - HP Tru64 UNIX, HP -UX, Potential
libc Security Vulnerabilities

>> <http://www.net-security.org/advisory.php?id=1835>

Immunix Secured OS Security Advisory - samba

>> <http://www.net-security.org/advisory.php?id=1834>

Immunix Secured OS Security Advisory - sendmail

>> <http://www.net-security.org/advisory.php?id=1833>

Immunix Secured OS Security Advisory - openssl,
openssh, mod_ssl

>> <http://www.net-security.org/advisory.php?id=1832>

Red Hat Security Advisory - Updated dhcp packages fix possible packet storm
>> <http://www.net-security.org/advisory.php?id=1831>

Apple Security Advisory - QuickTime Player for Windows
>> <http://www.net-security.org/advisory.php?id=1830>

OpenBSD Announcement - new sendmail buffer overflow
>> <http://www.net-security.org/advisory.php?id=1829>

Red Hat Security Advisory - Updated sendmail packages fix vulnerability
>> <http://www.net-security.org/advisory.php?id=1828>

Red Hat Security Advisory - Updated Evolution packages fix multiple vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1827>

Gentoo Linux Security Announcement - krb5 and mit-krb5
>> <http://www.net-security.org/advisory.php?id=1826>

Gentoo Linux Security Announcement - dietlibc
>> <http://www.net-security.org/advisory.php?id=1825>

Gentoo Linux Security Announcement - sendmail
>> <http://www.net-security.org/advisory.php?id=1824>

FreeBSD Security Advisory - second sendmail header parsing buffer overflow
>> <http://www.net-security.org/advisory.php?id=1823>

SurfControl E-mail Filter - Try the Enterprise Spam Solution
>> <http://www.surfcontrol.com/go/zhnsppl>

[Featured articles]

All articles are located at:

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

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

HOW TO SECURE YOUR TELEWORKERS WITH A VPN

Many in the industry fear that the move towards teleworking and the corresponding change of the enterprise network from a closed, protected architecture to an open, Internet-based system leaves a lot of questions unanswered.

>> <http://www.net-security.org/article.php?id=434>

INTERVIEW WITH LISA YEO

The author of "Personal Firewalls for Administrators and Remote Users" talks about her book and firewalls in general.

>> <http://www.net-security.org/article.php?id=435>

THE CASE FOR SECURE EMAIL

This non-technical article is designed to educate you about how email really works, what the real security issues are, what the solutions are, and how you can mitigate your exposure to these security risks.

>> <http://www.net-security.org/article.php?id=436>

RED HAT LINUX 9 HAS BEEN RELEASED

Red Hat, Inc. announced the availability of Red Hat Linux 9. Drawing from the work of the open source community, Red Hat Linux 9 allows users to take advantage of the newest open source technology first.

>> <http://www.net-security.org/article.php?id=437>

INTERVIEW WITH SUNIL JAMES

The Manager of iDEFENSE's Vulnerability Contributor Program talks about his company and computer security in general.

<http://www.net-security.org/article.php?id=438>

CYBER TERRORISM - IS IT A SERIOUS THREAT TO COMMERCIAL ORGANIZATIONS?

Cyber Terrorism is a hot topic in the popular press and on general Computer industry web sites. Unfortunately, the 'hype' surrounding the topic is actually doing a disservice to the application of sensible security defences in the commercial and industrial sectors.

>> <http://www.net-security.org/article.php?id=439>

FIREWALL + FIREWALL POLICY = IMPROVED SECURITY

The best way to achieve security effectiveness is to design a security policy. This will ensure the integrity of any mission

critical device - especially firewalls. Here is a guide on how to create a firewall policy.

>> <http://www.net-security.org/article.php?id=440>

LT AUDITOR+ SECURITY SOFTWARE BUNDLED WITH NOVELL NETWORKWARE

Blue Lance announced that a new version of LT Auditor+ has been developed exclusively for Novell and packaged with "Nakoma," the next official release of NetWare.

>> <http://www.net-security.org/article.php?id=441>

INTERVIEW WITH MARK G. SOBELL

The author of "A Practical Guide to Red Hat Linux 8" talks about his book and Linux in general.

>> <http://www.net-security.org/article.php?id=442>

NEW APACHE 2.0.45 FIXES DENIAL OF SERVICE VULNERABILITY

Newly released Apache HTTP Server 2.0.45, fixes yet unspecified Denial of Service vulnerability. The vulnerability information will be disclosed by iDefense on 8 April 2003. Here you can find a partial reprint of the Apache announcement.

>> <http://www.net-security.org/article.php?id=443>

WARCALKING AND OTHER WIRELESS WORRIES

Wireless technologies promise increase flexibility but are the security risks worth the benefits?

>> <http://www.net-security.org/article.php?id=444>

INTERVIEW WITH JOHN CHIRILLO

author of "Hack Attacks Testing: How to Conduct Your Own Security Audit" talks about his book, online security problems, enterprise security and the disclosure of vulnerabilities.

>> <http://www.net-security.org/article.php?id=445>

AS PREDICTED THE SPAM PROBLEM RAGES

As the experts have been predicting, the spam problem is growing at alarming rates and poses much more than an annoyance to businesses as it clogs networks and drags down productivity.

>> <http://www.net-security.org/article.php?id=446>

Stop Spam & Controls E-mail Risks - Download Free Trial

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

[Reviews]

All reviews are located at:

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

HACK ATTACKS TESTING: HOW TO CONDUCT YOUR OWN SECURITY AUDIT

As you can see from the title, the author bases this publication on the information containing resources and methodologies needed to start your own security audits. Don't expect that after reading this book you will become a skilled penetration tester, but if you are interested in security audits it will provide an introduction to some of the best security tools around.

>> <http://www.net-security.org/review.php?id=46>

ESSENTIAL APACHE FOR WEB PROFESSIONALS

If you ever worked with Apache, you probably know that this little package offers great functions and features, and this book will provide you an insight on the Apache stages, from installation to the advanced usage.

>> <http://www.net-security.org/review.php?id=47>

HACKING EXPOSED: NETWORK SECURITY SECRETS & SOLUTIONS 4/E

With every edition this books keeps getting better and better. I can recommend it to anyone interested in computer security, as it will certainly give you a real-world course on the subject.

>> <http://www.net-security.org/review.php?id=48>

Try the Most Accurate Anti-Spam Solution for the Enterprise

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

[Security world]

All press releases are located at:

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

E92Plus and Cobion Team to Offer Anti-Spam and Content Filtering Solutions

>> <http://www.net-security.org/press.php?id=1326>

Datakey and Precise Biometrics Sign License Agreement

>> <http://www.net-security.org/press.php?id=1325>

Virus-infected emails drop by over two-thirds in March,
reveals VIA NET.WORKS UK
>> <http://www.net-security.org/press.php?id=1324>

Hong Kong Institute Of Vocational Education To Offer Diversinet's
Wireless Security Software For Student Project
>> <http://www.net-security.org/press.php?id=1323>

ActivatorDesk Introduced as the First Dot-Kids Safe
Internet Desktop Browser for Children
>> <http://www.net-security.org/press.php?id=1322>

Independent Study Finds NetScreen Security Solutions Outperform
Legacy, Software-Based Products in Cost of Ownership
>> <http://www.net-security.org/press.php?id=1321>

Bitdefender Wins Testing For Home Antivirus Protection
>> <http://www.net-security.org/press.php?id=1320>

Intrusion Releases Next Generation Upgrades for SecureNet
Network IDS System
>> <http://www.net-security.org/press.php?id=1319>

Trend Micro Enterprise Protection Strategy Selected for Superior
End-to-End Protection From Viruses and Malicious Content
>> <http://www.net-security.org/press.php?id=1318>

ActiveState Anti-Spam Task Force Established Experts
Vow to "Out-Innovate" Spammers
>> <http://www.net-security.org/press.php?id=1317>

nCipher announces its Membership in the Microsoft
Gold Certified Partner Program
>> <http://www.net-security.org/press.php?id=1316>

Cinea Selects SafeNet's SafeXcel 241-PCI Card to
Secure High Value Digital Video Content
>> <http://www.net-security.org/press.php?id=1315>

Accurate Anti-Spam Software - Download a Free Trial
>> <http://www.surfcontrol.com/go/zhnspl>

[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

NETWORK AUDITOR 3.0.11.5

Network Auditor lets you take control of your network audit, by letting you scan your network to see what machines you have then hone in and discover exactly what hardware and software is installed on each of them.

>> <http://www.net-security.org/software.php?id=477>

VPNDIALER 3.7

The main goal of VPNDialer is giving the normal end-user the ability to connect to a site via IPSec using the native IPSec-stack of Windows 2000 and XP.

>> <http://www.net-security.org/software.php?id=478>

ACTIVATORDESK ENTERPRISE DESKTOPS CONTROLLER 6.0.0.16

Enterprise Controller offers centralized automatic remote control of many Windows desktops running ActivatorDesk Enterprise Client desktop browser programs.

>> <http://www.net-security.org/software.php?id=479>

SurfControl Email Filter Stops Spam - Free 30-Day Trial

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

[Virus News]

All virus news are located at:

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

Weekly Virus Report - Trj/Kamouflao3 Trojan, Grimgram and Cult.B Worms

>> http://www.net-security.org/virus_news.php?id=215

Panda Antivirus Appliance FAQ

>> http://www.net-security.org/virus_news.php?id=214

Worms/Trojans: The Latest Virus Threat

>> http://www.net-security.org/virus_news.php?id=213

Sophos: Top 10 Viruses and Hoaxes in March 2003

>> http://www.net-security.org/virus_news.php?id=212

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

ALERT: How a Hacker Launches a SQL Injection Attack - Step-by-Step!

It's as simple as placing additional SQL commands into an input box on a web form giving hackers complete access to all your backend data! Firewalls and IDS will not stop SQL Injection attempts because they are NOT seen as intrusions.

Download this *FREE* white paper from SPI Dynamics for a complete guide to protection!

<http://www.spidynamics.com/mktg/sqlinjection29>
