



HNS Newsletter
Issue 151 - 03.03.2003.
<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>

Table of contents:

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

[**Security news**]

SYSADMIN TALES OF TERROR

The biggest challenge a system administrator ever faces is inheriting a networking mess: taking on a new job, or a new client, with a computing infrastructure that has grown without rhyme or reason.

>> <http://www.net-security.org/news.php?id=2057>

CITIBANK GAGS CRYPTO RESEARCHERS

The High Court in London has imposed an injunction on Cambridge University security experts who claim to have uncovered serious failings in the system banks use to secure ATM PIN codes.

>> <http://www.net-security.org/news.php?id=2058>

SWISS CRACK E-MAIL ENCRYPTION CODE

Researchers at a Swiss university have cracked the technology used to keep people from eavesdropping on e-mail sent over the Web, but U.S. experts said that the impact would likely be minimal.

>> <http://www.net-security.org/news.php?id=2059>

WHITE HAT HACKING SCHOOL

After five days learning how to enter networks illicitly, 12 more white-hat hackers have joined the growing ranks of IT experts who think and act as the bad guys do.

>> <http://www.net-security.org/news.php?id=2060>

WI-FI SECURITY GETS A BOOST

802.11i standard will plug security holes, but products may not be available for almost a year.

>> <http://www.net-security.org/news.php?id=2062>

LOVEGATE WORM'S GOT A HOLD ON PCS

The mass-mailing worm has infected a moderate number of PCs, installing a back-door that leaves them open to control.

>> <http://www.net-security.org/news.php?id=2066>

CIOs DEBATE SECURITY, PRIVACY, LINUX AND OUTSOURCING ISSUES

CIOs from some of the nation's largest companies outlined their fears and hopes about their jobs and about the direction of technology in the year ahead.

>> <http://www.net-security.org/news.php?id=2067>

MEDIA GONE MAD

Why last week's big Windows security hole is nothing more than technology press hot air.

>> <http://www.net-security.org/news.php?id=2068>

VPN EXPERTS DOWNPLAY 'SPLITTING' HEADACHE

Most say split tunneling does not necessarily undermine security.

>> <http://www.net-security.org/news.php?id=2069>

PROGRAM HIDES SECRET MESSAGES IN EXECUTABLES

A new steganography application turns other programs into covert carrier pigeons.

>> <http://www.net-security.org/news.php?id=2071>

THE OPEN ROAD: ALTERNATIVE NAMESERVERS - POWERDNS

PowerDNS is an authoritative-only nameserver, which means that it will answer queries about zones that it is responsible for, but it won't attempt to find information on another zone/domain.

>> <http://www.net-security.org/news.php?id=2076>

CHIPPING AWAY AT WORKERS' PRIVACY

Employers rely more and more on technology - from sensors to cameras to keystroke recorders to GPS - to keep an eye on workers. A new book paints a picture of an increasingly privacy-free workplace.

>> <http://www.net-security.org/news.php?id=2077>

U.S. INFORMATION SECURITY LAW, PART ONE

This article addresses the legal framework for protection of information systems and the role of information security professionals in the creation of trade secret interests, one type of intellectual property.

>> <http://www.net-security.org/news.php?id=2078>

MUCH ADO ABOUT KEVIN MITNICK

Until Mitnick does something noteworthy with his non-criminal career, let the guy be. He's served his time and has earned the right to be known as something other than a former computer criminal.

>> <http://www.net-security.org/news.php?id=2079>

'SMART CARDS' IN DEMAND AS CONCERNS ABOUT SECURITY RISE

With security tighter than ever, "smart card" IDs are becoming a first line of defense against attackers seeking to penetrate computer networks and office buildings.

>> <http://www.net-security.org/news.php?id=2082>

SECURE APPS TO STOP NETWORK ATTACKS

When securing your network, don't neglect the applications running on it. These tips will help you secure your network against attacks that exploit application vulnerabilities.

>> <http://www.net-security.org/news.php?id=2083>

ACLU ADMITS ANOTHER PRIVACY GAFFE

Protecting personal information on the digital frontier remains a tough task, even for the most ardent privacy activists.

>> <http://www.net-security.org/news.php?id=2084>

SSL 'INVENTOR' SUES VERISIGN AND RSA

A retired engineer has claimed he owns the patent for SSL, an authentication standard used by millions of Web sites.

>> <http://www.net-security.org/news.php?id=2085>

SPY AGENCIES TIGHT-FISTED ON DATA

While the U.S. government fine-tunes its computer networks to better fight terrorism, federal intelligence agencies can't agree on the best way to share crucial information with each other.

>> <http://www.net-security.org/news.php?id=2086>

SINGAPORE NETS RECORD PIRACY HAUL

The police in Singapore uncovered the city-state's biggest-ever cache of pirated goods, which included software, CDs and games.

>> <http://www.net-security.org/news.php?id=2087>

IS VIGILANTE HACKING LEGAL?

A legal expert is arguing that those under attack from 'zombie servers' and other Internet nuisances may be able to legally strike back - as long as they are careful.

>> <http://www.net-security.org/news.php?id=2089>

IDENTITY THEFT PROBLEMS IN AUSTRALIA

Within five years automatic teller machines will be scanning eyes before handing out the cash. It is just one of the measures to thwart identity theft, the fastest growing crime in Australia.

>> <http://www.net-security.org/news.php?id=2090>

NO NEED TO FEEL INSECURE ABOUT ZEROCONF / RENDEZVOUS SECURITY

Jim Banahan describes how he set up a multi-platform networking environment for a local business.

>> <http://www.net-security.org/news.php?id=2091>

ROOT 101

For many who are accustomed to single-user operating systems the concept of root is an unfamiliar one. This article is

intended to help explain what root access is, whether you need it, what you can do with it.

>> <http://www.net-security.org/news.php?id=2092>

UK E-COMMERCE SITES: TOP 10 FLAWS

UK customer credit card details and sensitive data is at risk because of simple e-commerce flaws, according to a study.

>> <http://www.net-security.org/news.php?id=2093>

HOLLYWOOD, SOFTWARE FIRE SUITS AT PIRATES

Two major trade groups filed on Thursday a slew of civil lawsuits against people they claim were selling pirated copies of films and software via online auction sites.

>> <http://www.net-security.org/news.php?id=2094>

MCAFEE PREPS 'WORM-KILLER' VIRUSSCAN

McAfee next week will unveil VirusScan Enterprise 7.0, its first major update to VirusScan in years.

>> <http://www.net-security.org/news.php?id=2095>

[Vulnerabilities]

All vulnerabilities are located here:

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

NetPBM Multiple Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2486>

Axis 2400 Webcams Multiple Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2485>

TCPDUMP Denial of Service Vulnerability in ISAKMP Packet Parsing

>> <http://www.net-security.org/vuln.php?id=2484>

ISMAIL Remote Buffer Overrun Vulnerability

>> <http://www.net-security.org/vuln.php?id=2483>

MS-Windows ME IE/Outlook/HelpCenter Critical Vulnerability

>> <http://www.net-security.org/vuln.php?id=2482>

Opera Browser Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2481>

nCipher nShield Unexpected Duplicates of Imported
Software Based Keys
>> <http://www.net-security.org/vuln.php?id=2480>

Nokia 6210 SMS Denial of Service
>> <http://www.net-security.org/vuln.php?id=2479>

Self-Executing HTML: Internet Explorer 5.5 and 6.0 Part II
>> <http://www.net-security.org/vuln.php?id=2478>

CuteNews PHP Source Code Injection Vulnerability
>> <http://www.net-security.org/vuln.php?id=2477>

QuickTime/Darwin Streaming Administration Server
Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2476>

GOnicus System Administrator PHP Injection Vulnerability
>> <http://www.net-security.org/vuln.php?id=2475>

Multiple Terminal Emulators Security Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2474>

Mambo SiteServer Privilege Elevation Vulnerability
>> <http://www.net-security.org/vuln.php?id=2473>

Webmin/Usermin Session ID Spoofing Vulnerability #2
>> <http://www.net-security.org/vuln.php?id=2472>

PlatinumFTPserver V1.0.11 Directory Traversal Vulnerability
>> <http://www.net-security.org/vuln.php?id=2471>

WWWBoard Cross Site Scripting Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2470>

Nuked-Klan Cross Site Scripting and Function
Execution Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2469>

zlib 1.1.4 Buffer Overrun Vulnerability
>> <http://www.net-security.org/vuln.php?id=2468>

Myguestbook Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2467>

login_Idap Anonymous Authorization Vulnerability
>> <http://www.net-security.org/vuln.php?id=2466>

phpBB Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2465>

HNS Book Giveaway: <http://net-security.org/news.php?id=2104>
> Cisco Secure Virtual Private Networks
> Cisco Secure Intrusion Detection System

[Advisories]

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

Debian Security Advisory - New mhc-utils packages fix
predictable temporary file
>> <http://www.net-security.org/advisory.php?id=1652>

SuSE Security Announcement - hypermail
>> <http://www.net-security.org/advisory.php?id=1651>

Debian Security Advisory - New tcpdump packages fix
denial of service vulnerability
>> <http://www.net-security.org/advisory.php?id=1650>

Debian Security Advisory - New NANOG traceroute packages
fix buffer overflow
>> <http://www.net-security.org/advisory.php?id=1649>

Mandrake Linux Security Advisory - shadow-utils
>> <http://www.net-security.org/advisory.php?id=1648>

Mandrake Linux Security Advisory - webmin
>> <http://www.net-security.org/advisory.php?id=1647>

Microsoft Security Bulletin MS03-006 - Flaw in Windows
Me Help and Support Center Could Enable Code Execution
>> <http://www.net-security.org/advisory.php?id=1646>

SGI Security Advisory - Buffer Overrun Vulnerability
in /sbin/ps
>> <http://www.net-security.org/advisory.php?id=1645>

SuSE Security Announcement - openssl
>> <http://www.net-security.org/advisory.php?id=1644>

Mandrake Linux Security Advisory - MNF8.2
>> <http://www.net-security.org/advisory.php?id=1643>

SuSE Security Announcement - libmccrypt
>> <http://www.net-security.org/advisory.php?id=1642>

FreeBSD Security Advisory - OpenSSL timing-based
SSL/TLS attack (revised)
>> <http://www.net-security.org/advisory.php?id=1641>

Mandrake Linux Security Advisory - lynx
>> <http://www.net-security.org/advisory.php?id=1640>

Mandrake Linux Security Advisory - vnc
>> <http://www.net-security.org/advisory.php?id=1639>

Gentoo Linux Security Announcement - vnc
>> <http://www.net-security.org/advisory.php?id=1638>

Gentoo Linux Security Announcement - tightvnc
>> <http://www.net-security.org/advisory.php?id=1637>

EnGarde Secure Linux Advisory - WebTool session ID
spoofing vulnerability
>> <http://www.net-security.org/advisory.php?id=1636>

Conectiva Linux Security Announcement - openssl
>> <http://www.net-security.org/advisory.php?id=1635>

Red Hat Security Advisory - Updated VNC packages fix
replay and cookie vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1634>

FreeBSD Security Advisory - Brute force attack on SYN cookies
>> <http://www.net-security.org/advisory.php?id=1633>

FreeBSD Security Advisory - OpenSSL timing-based SSL/TLS attack
>> <http://www.net-security.org/advisory.php?id=1632>

Debian Security Advisory - New OpenSSL packages fix
timing-based attack vulnerability
>> <http://www.net-security.org/advisory.php?id=1631>

Gentoo Linux Security Announcement - usermin
>> <http://www.net-security.org/advisory.php?id=1630>

Gentoo Linux Security Announcement - apcupsd
>> <http://www.net-security.org/advisory.php?id=1629>

[**Featured articles**]

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

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

INTERVIEW WITH CYRUS PEIKARI
The CEO of AirScanner Mobile Security and co-author of
"Maximum Wireless Security" talks about wireless security.
>> <http://www.net-security.org/article.php?id=396>

INTERVIEW WITH AVIEL RUBIN
The Computer Science Professor at Johns Hopkins University and
Technical Director of the JHU Information Security Institute
talks about firewalls and computer security in general.
>> <http://www.net-security.org/article.php?id=399>

INTERVIEW WITH ERIC GREENBERG
The author of "Mission-Critical Security Planner: When

Hackers Won't Take No for an Answer" speaks about his book and general security issues.

>> <http://www.net-security.org/article.php?id=400>

CORPORATE SECURITY

Most businesses use digital technologies to run more efficiently. Unfortunately, these also pose a threat to system integrity with security breaches being reported regularly.

>> <http://www.net-security.org/article.php?id=397>

THE NEW FIREWALLANALYZER 3.0 SUPPORTS LEADING FIREWALLS

eIQnetworks released version 3.0 of their FirewallAnalyzer.

This tool is the industry's first browser-based, cross-platform Firewall/VPN analysis and reporting solution with support for all leading firewalls.

>> <http://www.net-security.org/article.php?id=398>

HNS Book Giveaway: <http://net-security.org/news.php?id=2104>

> Cisco Secure Virtual Private Networks

> Cisco Secure Intrusion Detection System

[Review]

All reviews are located at:

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

CISCO SECURE INTRUSION DETECTION SYSTEM

The book offers a comprehensive guide through all the perspectives of planning, deploying and maintaining Cisco Secure IDS. While the book format cannot compete with the actual hands-on courses at Cisco, it provides a valuable component in meeting the ever growing demand for Cisco Certifications.

>> <http://www.net-security.org/review.php?id=35>

[**Security world**]

All press releases are located at:

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

F-Secure Takes Linux Security to a New Level

>> <http://www.net-security.org/press.php?id=1267>

Disclaimer Software for Exchange Server Provided Free by GFI

>> <http://www.net-security.org/press.php?id=1266>

Datakey Inc. Announces 2002 Year-end and Fourth Quarter Results

>> <http://www.net-security.org/press.php?id=1265>

Sophos Partners With Barbedwire Technologies To Provide
Enterprise Security Appliance

>> <http://www.net-security.org/press.php?id=1264>

Central Command: Lakes Regional General Healthcare Selects
Vexira Antivirus To Protect Its 1200 Computers From Viruses

>> <http://www.net-security.org/press.php?id=1263>

Global Interest in Ubizen Professional Services Shifts
from Reactive to Proactive Security Measures

>> <http://www.net-security.org/press.php?id=1262>

Trusecure Expands Executive Sales Team In Response To
Increased Demand For Security Services

>> <http://www.net-security.org/press.php?id=1261>

TruSecure Names Michael Rothman As Vice President Of Marketing

>> <http://www.net-security.org/press.php?id=1260>

Intrusion Advances Internet Security Appliance Management
with PDS Pilot 2.7 Management System

>> <http://www.net-security.org/press.php?id=1259>

[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

PIXILATE 0.3 (Linux)

Pixilate is a commandline packet generation utility that reads Cisco PIX 6.2x or Cisco IOS ACLs as input and generates the appropriate packets.

>> <http://www.net-security.org/software.php?id=457>

MY-SWATCH 0.3 (Linux)

my-swatch pretends to be an implementation of msyslog and swatch together. What it pretends to accomplish is put all together, to log events to a remote database (like msyslog), and to awake triggers (like swatch).

>> <http://www.net-security.org/software.php?id=458>

BITDEFENDER ANTILOVGATE (Windows)

This tool removes the LovGate virus. The worm comes by e-mail, without exploiting the famous I-Frame vulnerability, but bringing to table a series of well-defined, social engineering structures.

>> <http://www.net-security.org/software.php?id=459>

WEBJOB 1.2.3 (Windows)

WebJob downloads a program over HTTP/HTTPS and executes it in one unified operation. Output may be directed to stdout/stderr or a Web resource.

>> <http://www.net-security.org/software.php?id=460>

TCP/IP LIBRARY 4.0 (Windows)

Komodora's TCP/IP library V4.0 (free, open source) is a unique combination of a security oriented library that allows the user to create arbitrary TCP/UDP/IP packets, and a complete communication library solution (for TCP/UDP/ICMP).

>> <http://www.net-security.org/software.php?id=461>

[**Virus News**]

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

Weekly Virus Report - Lovgate and Gibe Worms, CrazyBull
Trojan and Ekiam Macro Virus
>> http://www.net-security.org/virus_news.php?id=193

Trojans Used to Spread Massive Infections on the Increase
>> http://www.net-security.org/virus_news.php?id=192

42% of SMEs Only Update their Anti-Virus Software Once a Week
>> http://www.net-security.org/virus_news.php?id=191

Panda Software Reports the Appearance of Three New Worms
>> http://www.net-security.org/virus_news.php?id=190

Worm Becomes Part Of The Windows OS
>> http://www.net-security.org/virus_news.php?id=189

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>
