



HNS Newsletter

Issue 195 - 12.01.2004.

<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.

GET THAWTE'S NEW STEP-BY-STEP SSL GUIDE FOR MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates.

Get you copy of this new guide now:

<http://ad.doubleclick.net/clk;6091068;8369143;p>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Reviews
- 6) Software
- 7) Webcasts
- 8) Conferences
- 9) Security world
- 10) Virus news

[**Security news**]

WELCOME TO YET ANOTHER YEAR OF VIRUSES

It's sad, but true. Robert expects we'll see plenty of e-mail viruses in 2004, despite expectations that these pests would disappear in 2003. Here's why viruses won't go away--and how to protect yourself.

<http://www.net-security.org/news.php?id=4352>

NO MORE SEQUELS IN DVD HACKING CASE

Norwegian police said Monday they would not appeal a landmark DVD piracy case for a second time, marking a final victory for a 20-year-old hacker and a defeat for Hollywood.

<http://www.net-security.org/news.php?id=4353>

THE REAL IMPACT OF VIRUSES

It seems that hardly a week goes by when computer viruses aren't making headline news. The release of the SQL Slammer and Sobig worms last January, followed by the MSBlast.exe worm in August, graphically illustrate how the nature of these attacks is ever increasing.

<http://www.net-security.org/news.php?id=4354>

WINDOWS XP SERVICE PACK 2 BETA FIRST LOOK

If there is one thing Microsoft is preoccupied with right now, it would have to be security.

<http://www.net-security.org/news.php?id=4356>

ADRIAN LAMO SAYS HE'LL ACCEPT PLEA BARGAIN

Adrian Lamo, accused of breaking into The New York Times' computer network, is planning to appear in court Thursday to accept a plea bargain.

<http://www.net-security.org/news.php?id=4357>

MANAGING LINUX SECURITY EFFECTIVELY IN 2004

This article examines the process of proper Linux security management in 2004. First, a system should be hardened and patched. Next, a security routine should be established to ensure that all new vulnerabilities are addressed. Linux security should be treated as an evolving process.

<http://www.net-security.org/news.php?id=4358>

INTERNET SECURITY: THE TOP 10 ONLINE BLUNDERS

Here are a few of the most common Internet security blunders.

<http://www.net-security.org/news.php?id=4359>

MICROSOFT PUBLISHES PROGRAM TO BLAST MSBLAST

Microsoft released a removal tool for the MSBlast worm on Monday after Internet service providers complained that home users' PCs infected with the malicious program are still causing network congestion.

<http://www.net-security.org/news.php?id=4360>

COURT PONDERES WEB SITE-BLOCKING LAW

A federal judge in Philadelphia on Tuesday heard a challenge to a controversial state law that has led to more than 1 million innocuous Web sites being accidentally blocked.

<http://www.net-security.org/news.php?id=4361>

FEAR ABOUT REPORTING E-CRIME

Fraud and electronic crime was burgeoning yet was too often swept under the carpet by people and companies who were too ashamed to admit they have been swindled, a report said.

<http://www.net-security.org/news.php?id=4362>

DON'T TAKE PASSWORDS TO THE GRAVE

As an ambulance whisked Jon Hansen to the hospital last year, he held tightly to his wife's hand and told her things she needed to know if he were to die.

<http://www.net-security.org/news.php?id=4363>

MSN WORM DOES ROUNDS

A new worm that targets users of Microsoft's MSN Messenger network is one of several threats in the wild, but a local vendor says the holiday season has been quiet on the infections front.

<http://www.net-security.org/news.php?id=4364>

BASICS ON PROTECTING AN ORGANIZATION AGAINST HACKERS

Includes an explanation of why security problems are escalating, along with 10-point and 90-day plans for improving network security.

<http://www.net-security.org/news.php?id=4365>

WORD'S PASSWORD FEATURE 'NOT A SECURITY TOOL'

Microsoft admits that Word's password-protection feature can be easily bypassed, but argues it was never intended to ensure security.

<http://www.net-security.org/news.php?id=4366>

MISSISSIPPI MAN DENIES BEST BUY BLACKMAIL

A Mississippi man pleaded not guilty on Tuesday to charges that he threatened to reveal security weaknesses in the Web site of electronics seller Best Buy unless the company paid him \$2.5 million.

<http://www.net-security.org/news.php?id=4367>

NETCRAFT CRAFTS ANTI-PHISHING SERVICE

Netcraft has introduced an early warning service to alert banks to phishing scams.

<http://www.net-security.org/news.php?id=4368>

INTERVIEW WITH NETSCREEN EXECUTIVE OFFICER DAVID FLYNN

"Historically, the two primary competitors we see are Cisco and Check Point Software, but as this new smarter firewall comes along, we're seeing some of the antivirus [companies], like Symantec and Network Associates, trying to move in this direction," NetScreen's David Flynn told the E-Commerce Times.

<http://www.net-security.org/news.php?id=4369>

SQL SECURITY FLAW PERSISTS IN MANY WEB SITES

Businesses are still failing to make basic security checks on their web sites and are leaving themselves wide open to digital attack, warn experts.

<http://www.net-security.org/news.php?id=4370>

SECURE PASSPORTS TO MEET DEADLINE

The Department of Foreign Affairs and Trade (DFAT) said that new passport security data requirements for entry to the United States would be accepted before the October deadline.

<http://www.net-security.org/news.php?id=4372>

ELECTRONIC FRAUD BURGEONING: REPORT

Fraud and electronic crime was burgeoning, yet was too often swept under the carpet by people and companies who were too ashamed to admit they have been swindled, a report says.

<http://www.net-security.org/news.php?id=4373>

NEW NET BANKING SCAM

Customers of the nation's five leading banks are unwittingly being siphoned of their savings online, after logging on to official internet banking websites.

<http://www.net-security.org/news.php?id=4374>

FEDS SEEK WIRETAP ACCESS VIA VOIP

The FBI and the Justice Department have renewed their efforts to wiretap voice conversations carried across the Internet.

<http://www.net-security.org/news.php?id=4375>

FROM ANTI-SPAM TO ANTI-SPYWARE

EarthLink spokesman Jerry Grasso says consumers want two things from an Internet service provider: secure connections and tools to that cut through the clutter.

<http://www.net-security.org/news.php?id=4376>

CHIPS TO FIGHT VIRUSES

AMD and Intel are developing technology that will prevent processors being hijacked by attackers.

<http://www.net-security.org/news.php?id=4377>

IT SECURITY CRITICAL FOR SMES

Possibly the most critical aspect of any small to medium enterprise's (SME's) information technology infrastructure is the security of that system.

<http://www.net-security.org/news.php?id=4378>

SPAM AND VIRUS TECHNIQUES OVERLAP

A year on from the debut of SoBig.A, the first virus to converge spam and virus writing techniques, its legacy continues, warns a security company.

<http://www.net-security.org/news.php?id=4379>

[Vulnerabilities]

All vulnerabilities are located here:

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

Yahoo Instant Messenger Long Filename Downloading
Buffer Overflow Vulnerability

<http://www.net-security.org/vuln.php?id=3176>

SnapStream PVS LITE Cross Site Scripting Vulnerability

<http://www.net-security.org/vuln.php?id=3175>

ZyXEL10 Router Cross Site Scripting Vulnerability

<http://www.net-security.org/vuln.php?id=3174>

PHPgedview 2.61 Multiple Vulnerabilities

<http://www.net-security.org/vuln.php?id=3173>

FirstClass Client 7.1 Remote Command Execution Vulnerability

<http://www.net-security.org/vuln.php?id=3172>

Phorum 3.4.5 Multiple Vulnerabilities

<http://www.net-security.org/vuln.php?id=3171>

vBulletin Forum 2.3.xx calendar.php SQL Injection

<http://www.net-security.org/vuln.php?id=3170>

HotNews Arbitrary File Inclusion Vulnerability

<http://www.net-security.org/vuln.php?id=3169>

Webcam Watchdog Stack Overflow Vulnerability

<http://www.net-security.org/vuln.php?id=3168>

EasyDynamicPages v.2.0 Arbitrary File Inclusion Vulnerability
<http://www.net-security.org/vuln.php?id=3167>

GoodTech Telnet Server 4.0.103 Denial of Service Vulnerability
<http://www.net-security.org/vuln.php?id=3166>

Switch Off Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3165>

NetObserve Security Bypass Vulnerability
<http://www.net-security.org/vuln.php?id=3164>

Mdaemon Raw Message Handler Remote Buffer
Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3163>

Jordan Telnet Server Buffer Overflow Vulnerability
<http://www.net-security.org/vuln.php?id=3162>

php-ping Remote Command Execution Vulnerability
<http://www.net-security.org/vuln.php?id=3161>

FreznoShop Cross Site Scripting Vulnerability
<http://www.net-security.org/vuln.php?id=3160>

PHPCatalog E-Commerce SQL Injection
<http://www.net-security.org/vuln.php?id=3159>

PostNuke 0.726 Phoenix Multiple Vulnerabilities
<http://www.net-security.org/vuln.php?id=3158>

[Advisories]

All advisories are located at:

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

Debian Security Advisory - New Linux 2.4.18 packages fix local root exploit (alpha) (DSA 417-2)
<http://www.net-security.org/advisory.php?id=2867>

Debian Security Advisory - New phpgroupware packages fix unintended PHP execution and SQL injection (DSA-419-1)
<http://www.net-security.org/advisory.php?id=2866>

Slackware Security Advisory - Slackware 8.1 kernel security update (SSA:2004-008-01)
<http://www.net-security.org/advisory.php?id=2865>

Gentoo Linux Security Advisory - Linux kernel do_mremap() privilege escalation vulnerability (GLSA 200401-01)
<http://www.net-security.org/advisory.php?id=2864>

Cisco Security Advisory - Cisco Personal Assistant User Password Bypass (47765)
<http://www.net-security.org/advisory.php?id=2863>

Mandrake Linux Security Update Advisory - Updated kernel packages fix local root vulnerability (MDKSA-2004:001)
<http://www.net-security.org/advisory.php?id=2862>

OpenPKG Security Advisory - inn (OpenPKG-SA-2004.001)
<http://www.net-security.org/advisory.php?id=2861>

Debian Security Advisory - New vbox3 packages fix privilege leak (DSA-418-1)
<http://www.net-security.org/advisory.php?id=2860>

SGI Security Advisory - SGI Advanced Linux Environment security update #8 (20040101-01-U)
<http://www.net-security.org/advisory.php?id=2859>

Red Hat Security Advisory - Updated Ethereal packages fix security issues (RHSA-2004:001-01)
<http://www.net-security.org/advisory.php?id=2858>

Debian Security Advisory - New Linux 2.4.18 packages fix local root exploit (powerpc+alpha) (DSA 417-1)
<http://www.net-security.org/advisory.php?id=2857>

Slackware Security Advisory - Kernel security update (SSA:2004-006-01)
<http://www.net-security.org/advisory.php?id=2856>

Debian Security Advisory - New fsp packages fix buffer overflow, directory traversal (DSA 416-1)
<http://www.net-security.org/advisory.php?id=2855>

Debian Security Advisory - New zebra packages fix denial of service (DSA 415-1)
<http://www.net-security.org/advisory.php?id=2854>

Debian Security Advisory - New jabber packages fix denial of service (DSA 414-1)
<http://www.net-security.org/advisory.php?id=2853>

Debian Security Advisory - New Linux 2.4.18 packages fix locate root exploit (DSA 413-1)
<http://www.net-security.org/advisory.php?id=2852>

Conectiva Linux Security Announcement - lftp (CLA-2004:800)
<http://www.net-security.org/advisory.php?id=2851>

Debian Security Advisory - New nd packages fix buffer overflows (DSA 412-1)
<http://www.net-security.org/advisory.php?id=2850>

Turbolinux Security Announcement - kernel mremap vulnerability (06/Jan/2004)
<http://www.net-security.org/advisory.php?id=2849>

Debian Security Advisory - New mpg321 packages fix format string vulnerability (DSA 411-1)
<http://www.net-security.org/advisory.php?id=2848>

Debian Security Advisory - New libnids packages fix buffer overflow (DSA 410-1)
<http://www.net-security.org/advisory.php?id=2847>

Debian Security Advisory - New bind packages fix denial of service (DSA 409-1)
<http://www.net-security.org/advisory.php?id=2846>

Immunix Secured OS Security Advisory - kernel (IMNX-2004-73-001-01)
<http://www.net-security.org/advisory.php?id=2845>

SUSE Security Announcement - Linux Kernel (SuSE-SA:2004:001)
<http://www.net-security.org/advisory.php?id=2844>

Trustix Secure Linux Security Advisory - kernel (2004-0001)
<http://www.net-security.org/advisory.php?id=2843>

Cisco Security Advisory Update - Transparent Cache Engine and Content Engine TCP Relay Vulnerability
<http://www.net-security.org/advisory.php?id=2842>

Conectiva Linux Security Announcement - Conectiva Linux Security Announcement (CLA-2004:799)
<http://www.net-security.org/advisory.php?id=2841>

Debian Security Advisory - New screen packages fix group utmp exploit (DSA 408-1)
<http://www.net-security.org/advisory.php?id=2840>

Guardian Digital Security Advisory - kernel bug and security fixes (ESA-20040105-001)
<http://www.net-security.org/advisory.php?id=2839>

Red Hat Security Advisory - Updated kernel resolves security vulnerability (RHSA-2003:417-01)
<http://www.net-security.org/advisory.php?id=2838>

Debian Security Advisory - New ethereal packages fix several vulnerabilities (DSA 407-1)
<http://www.net-security.org/advisory.php?id=2837>

Debian Security Advisory - New lftp packages fix arbitrary code execution (DSA 406-1)
<http://www.net-security.org/advisory.php?id=2836>

Mandrake Linux Security Update Advisory - Updated proftpd packages fix remote root vulnerability (MDKSA-2003:095-1)
<http://www.net-security.org/advisory.php?id=2835>

Debian Security Advisory - New xsok packages fix local group games exploit (DSA 405-1)
<http://www.net-security.org/advisory.php?id=2834>

[Articles]

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

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

VIDEO: SECURITY PREDICTIONS FOR 2004

While attending the RSA Conference 2003 in Amsterdam, we met up with some key people in the security industry and asked them to share their thoughts on the future of computer security. In this video you can see what experts believe we're facing in 2004 as they discuss online security, wireless security, SSL VPNs, and other information security topics.

<http://www.net-security.org/article.php?id=625>

IMPROVING PASSIVE PACKET CAPTURE: BEYOND DEVICE POLLING

This paper proposes a new approach to passive packet capture that combined with device polling further improves it and allows, on fast machines, packets to be captured at (almost) wire speed.

<http://www.net-security.org/article.php?id=626>

[Reviews]

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

THE EFFECTIVE INCIDENT RESPONSE TEAM

How do incident response teams function? Who are the people in the team? What steps do they take in order to increase the security of your network? The answer to these and numerous other questions lie within the pages of this book.

<http://www.net-security.org/review.php?id=119>

ESSENTIAL SYSTEM ADMINISTRATION POCKET REFERENCE

The information contained in this pocket reference will be of interest to administrators of any Linux, FreeBSD, Solaris, HP-UX or AIX machine. The whole idea behind this title is the ultra portability that should convince all of you paper-hating people to carry it around. Is it that good? Read on to find out.
<http://www.net-security.org/review.php?id=118>

[**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

TRUSTSIGHT SECURITY SCANNER 6.4

TrustSight Security Scanner helps maintain the security of web sites or the implementation of security documents, such as the SANS/FBI Top 20 List.
<http://www.net-security.org/software.php?id=535>

[**Webcasts**]

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

Tripwire for Network Devices: Overview and Product Demo
Organized by Tripwire on 13 January 2004, 9:00 AM PDT
<http://www.net-security.org/webcast.php?id=174>

Using the Microsoft Security Tools
Organized by Microsoft on 13 January 2004, 9:30 AM PT
<http://www.net-security.org/webcast.php?id=163>

Information About Microsoft's January Security Bulletins
Organized by Microsoft on 13 January 2004, 10:00 AM PT
<http://www.net-security.org/webcast.php?id=165>

Architecting Your 802.1x-Based WLAN Deployment
Organized by Funk Software on 13 January 2004, 1:00 PM EST
<http://www.net-security.org/webcast.php?id=157>

Keeping Secrets in .NET Applications
Organized by Microsoft on 13 January 2004, 1:00 PM PT
<http://www.net-security.org/webcast.php?id=164>

Best Practices for Wireless LAN Security
Organized by Forrester Research on 13 January 2004, 2:00 PM ET
<http://www.net-security.org/webcast.php?id=155>

Not All Anti-Virus Software is Created Equal
Organized by Sophos on 14 January 2004, 12:00 PM PST
<http://www.net-security.org/webcast.php?id=183>

Vulnerability Expert Forum
Organized by eEye on 14 January 2004, 1:00 PM EST
<http://www.net-security.org/webcast.php?id=158>

Tripwire for Servers: Overview and Product Demo
Organized by Tripwire on 15 January 2004, 11:00 AM PDT
<http://www.net-security.org/webcast.php?id=177>

Defending Your Organization with Intrusion Protection Solutions
Organized by Symantec on 15 January 2004, 12:00 PM EST
<http://www.net-security.org/webcast.php?id=181>

Network Forensics Made Easy
Organized by eEye on 15 January 2004, 2:00 PM EST
<http://www.net-security.org/webcast.php?id=159>

Microsoft Executive Circle: Implementing more security products
won't make you more secure, better management will
Organized by Microsoft on 19 January 2004, 9:00 AM PT
<http://www.net-security.org/webcast.php?id=152>

Implementing More Security Products Won't Make You More
Secure, Better Management Will
Organized by Microsoft on 19 January 2004, 9:00 AM PT
<http://www.net-security.org/webcast.php?id=166>

Monthly Update from Microsoft's VP for Security
Organized by Microsoft on 20 January 2004, 8:30 AM PT

Monthly Update from Microsoft's VP for Security
Organized by Microsoft on 20 January 2004, 8:30 AM PT
<http://www.net-security.org/webcast.php?id=151>

[Conferences]

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

Access Denied 2004
Organized by New Leaf Productions - 11 January -
13 January 2004
<http://www.net-security.org/conference.php?id=75>

Spam Conference 2004
Organized by Gilberte Houbart - 16 January-16 January 2004
<http://www.net-security.org/conference.php?id=80>

Security Venture Fair
Organized by Infocast - 21 January-23 January 2004
<http://www.net-security.org/conference.php?id=78>

IT-Defense 2004
Organized by cirosec GmbH/dpunkt.Verlag - 28 January -
30 January 2004
<http://www.net-security.org/conference.php?id=56>

FAA IT/ISS Partnership Conference
Organized by FBC - 10 February-11 February 2004
<http://www.net-security.org/conference.php?id=84>

Infosecurity Italia 2004
Organized by Fiera Milano International - 13 February -
14 February 2004
<http://www.net-security.org/conference.php?id=34>

RSA Conference 2004 USA

Organized by RSA Security - 23 February-27 February 2004

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

Southeast Cybercrime Summit 2004

Organized by ATLCCS - 2 March-5 March 2004

<http://www.net-security.org/conference.php?id=77>

InfoSec World Conference and Expo 2004

Organized by MIS Training Institute - 22 March-24 March 2004

<http://www.net-security.org/conference.php?id=68>

Infosecurity Europe 2004

Organized by Reed Exhibitions - 27 April-29 April 2004

<http://www.net-security.org/conference.php?id=27>

Dallascon Security Conference 2004

Organized by DallasCon - 1 May-2 May 2004

<http://www.net-security.org/conference.php?id=73>

RSA Conference 2004 Japan

Organized by RSA Conference 2004 Japan Executive Committee -

31 May-1 June 2004

<http://www.net-security.org/conference.php?id=82>

BCS Birmingham IT Security Conference 2004

Organized by British Computer Society - 8 June-8 June 2004

<http://www.net-security.org/conference.php?id=81>

16th Annual FIRST Conference

Organized by FIRST - 13 June-18 June 2004

<http://www.net-security.org/conference.php?id=22>

NetSec 2004

Organized by Computer Security Institute - 14 June-16 June 2004

<http://www.net-security.org/conference.php?id=20>

[**Security world**]

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

Send your press releases to press@net-security.org

MSN and Network Associates Deliver Comprehensive
Safety and Security Features to Broadband Users
<http://www.net-security.org/press.php?id=1912>

Kavado Interdo 3.0 Named Technology Of The Year By Infoworld
<http://www.net-security.org/press.php?id=1911>

Paraglyph Press Announces New Edition of Bestselling Guide
on Scripting for Windows Administrators
<http://www.net-security.org/press.php?id=1910>

Utimaco Delivers Notebook Security Solutions to AGA Gas
<http://www.net-security.org/press.php?id=1909>

F-Secure Expands Business in Slovenian Data Security Market
<http://www.net-security.org/press.php?id=1908>

Astaro to Bundle its Security Software with Toshiba
Magnia SG25, SG30 and Z310 Servers
<http://www.net-security.org/press.php?id=1907>

TrustSight Security Scanner Declared CVE-Compatible
<http://www.net-security.org/press.php?id=1906>

Commhub Teams With Trapeze Networks To Offer Multi-Tenant
Wired and Wireless Access In Commercial Office Buildings
<http://www.net-security.org/press.php?id=1905>

Pointsec Signs Agreement with Volvo IT
<http://www.net-security.org/press.php?id=1904>

GFI releases freeware version of GFI Network Server Monitor
<http://www.net-security.org/press.php?id=1903>

[**Virus News**]

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

Weekly Virus Report - Mimail N, Dluca.D and Xcmd.A Trojans
http://www.net-security.org/virus_news.php?id=341

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

Unsubscribe from this weekly digest on:
<http://www.net-security.org/subscribe.php>

The archive of the newsletter in TXT and PDF format is available
http://www.net-security.org/newsletter_archive.php

GET THAWTE'S NEW STEP-BY-STEP SSL GUIDE FOR MSIS

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you MSIS web server. Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates.

Get you copy of this new guide now:
<http://ad.doubleclick.net/clk;6091068;8369143;p>
