



Newsletter
Issue 134

Issue 134 - 04.11.2002

<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>.

SECURITY INCIDENT ALERT

Check your Web servers, FTP servers, Mail servers , DNS servers, firewalls, IDS systems, switchers and routers for over 900 up to date vulnerabilities. Secure your critical assets today!

FREE System Security Test and Detailed Report

<http://www.net-security.org/lm/ads/ads.pl?banner=scannerx1>

Table of contents:

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

[General security news]

NEW OUTLOOK TO GIVE SPAMMERS THE BOOT

Microsoft is taking spam fighting more seriously in the next version of its Outlook e-mail and contact-management software.

>> <http://www.net-security.org/news.php?id=1363>

NORTON INTERNET SECURITY 2003 REVIEW

A new Worm Blocking feature checks outbound e-mails so you won't be guilty of passing along the next Sircam...

>> <http://www.net-security.org/news.php?id=1362>

ROOT-SERVER ATTACK TRACED TO SOUTH KOREA, U.S.

Last week's attacks on the Internet's backbone likely emanated from computers in the United States and South Korea, FBI Director Robert Mueller today said.

>> <http://www.net-security.org/news.php?id=1361>

MAC OS AMONG LEAST PRONE TO ATTACK

The Macintosh was among the computer operating systems least prone to attack and damage from malicious hackers, worms and viruses during this year.

>> <http://www.net-security.org/news.php?id=1360>

HACKING VICTIMS TO REMAIN SECRET

The government will increasingly work to keep secret the names of companies that become victims to major hacking crimes, along with any sensitive corporate disclosures that could prove embarrassing.

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

HIRE HACKERS TO FIND LOOPHOLES IN IT SYSTEM, FIRMS ADVISED

As computer system security becomes an increasingly major concern, organisations can look to hiring ethical hackers to uncover their systems' vulnerabilities before the hackers do.

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

DO BUG-HUNTING SECURITY FIRMS PUT USERS AT RISK?

Publicizing software flaws before reporting them to the maker could help hackers attack, some insiders say.

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

SITE SHUTS DOWN CREDIT TRANSACTIONS AFTER SECURITY COMPLAINT

E-commerce site cybergames.co.za was this week forced to stop accepting credit card payments after an anonymous complaint that the site was not secure.

>> <http://www.net-security.org/news.php?id=1352>

RESPONSIBLE BUG DISCLOSURE BY CORPORATE FIAT

The new Organization for Internet Safety aims to make vulnerability disclosure more responsible. It's a good idea, but is the group too corporate to pull it off?

>> <http://www.net-security.org/news.php?id=1351>

STATE OF THE WIRELESS NATION

Computer experts and amateurs are joining forces to map out wireless networks around the world and find out how many are secure.

>> <http://www.net-security.org/news.php?id=1350>

QUESTIONS + ANSWERS: KEVIN MITNICK

Kevin Mitnick talks about the lessons he's learnt over his career and how he's using that knowledge to help business stay secure.

>> <http://www.net-security.org/news.php?id=1349>

WHY CAN'T HACKERS BE STOPPED?

Enterprise networks often use packet firewalls at the network perimeter, but they are of little use against active components because they examine only header information.

>> <http://www.net-security.org/news.php?id=1348>

ARE FIREWALLS AND VIRUS SOFTWARE EFFECTIVE SECURITY MEASURES?

Organisations only making use of traditional security products like firewalls and anti-virus software may not be using the most effective security strategy in the context of a total solution.

>> <http://www.net-security.org/news.php?id=1342>

CIA WARNS OF NET TERROR THREAT

Al-Qaida is not the only terrorist network hoping to wreak havoc on the United States through "cyberwarfare," the CIA says.

>> <http://www.net-security.org/news.php?id=1341>

BOOK REVIEW: NETWORK SECURITY WITH OPENSLL

The latest addition to O'Reilly's "must-have" references is Network Security with OpenSSL. The book covers pretty much all you'd ever need to know about using OpenSSL in your programs.

>> <http://www.net-security.org/news.php?id=1340>

CHINA PREVENTED REPEAT CYBER ATTACK ON US

The Defense Department expected new cyber attacks from China but they never materialized: the Chinese government asked attackers not to repeat the 2001 defacement of U.S. government Web sites.

>> <http://www.net-security.org/news.php?id=1339>

HOW TO PROTECT YOUR PC FROM VIRUSES

Today, a worm or virus can arrive on anyone's machine through e-mail or an infected Web page. Before you lose a day's work to the latest malicious virus, follow these precautions.

>> <http://www.net-security.org/news.php?id=1338>

THE HACKER ATTACKERS GET IN TRAINING

Executrain recently hosted the Middle East's first Symantec Gateway Security training course – the first such programme to be run outside of the USA.

>> <http://www.net-security.org/news.php?id=1337>

WIRELESS LAN SECURITY: TIME TO TAKE ACTION

By using wireless LANs without taking proper security measures, companies leave their networks vulnerable to even relatively unsophisticated attackers.

>> <http://www.net-security.org/news.php?id=1336>

MICROSOFT WIRELESSLY HACKED (NOT BAD MICROSOFT...NOT BAD!)

At Smau, the biggest Italian IT exhibition, Microsoft's wireless system was penetrated halting most of the Wi-Fi network.

>> <http://www.net-security.org/news.php?id=1335>

ATTACK OF THE MOD SQUADS

Game console mod chips can be used for everything from watching movies to installing Linux on your X-Box. But under goofy copyright laws, the piracy app kills all the others.

>> <http://www.net-security.org/news.php?id=1334>

TALKING SECURITY

With vandals trying to disrupt the Internet and probing the weaknesses of America's corporate data networks, White House Cyber Security chief Richard Clarke has his work cut out for him.
>> <http://www.net-security.org/news.php?id=1333>

VIRUS WRITER'S CONVICTION UPHELD

A Dutch appeals court has upheld the conviction of the man who created and unleashed the Anna Kournikova e-mail worm last year.
>> <http://www.net-security.org/news.php?id=1332>

IS THAT A VIRUS, OR A MALFUNCTION?

Virus symptoms are very like those of routine PC malfunctions. If a user thinks the system is infected, how can you be sure?
>> <http://www.net-security.org/news.php?id=1331>

'WE ARE THE WORST SECURITY RISK' - SYS ADMINS CONFESS

More than half of all senior IT managers (58%) think that their own IT departments offer the largest threat to IT security.
>> <http://www.net-security.org/news.php?id=1326>

PAYPAL USERS TARGETED BY E-MAIL SCAM - AGAIN

Users of PayPal have again been targeted by scam artists trying to steal their personal data, including name, address, home and work telephone numbers and credit card information.
>> <http://www.net-security.org/news.php?id=1325>

WE MUST SECURE OURSELVES

The government helped create the Internet and then turned it over to us. Its protection is a matter of national security and economic need.
>> <http://www.net-security.org/news.php?id=1324>

TERRORISTS HIJACKING WEBSITES

The al-Qaeda terror network has begun breaking into websites to create secret pages that send messages to its followers.
>> <http://www.net-security.org/news.php?id=1323>

BLACK LETTER DAY FOR E-CARDS

Software from website friendgreetings.com is currently causing mass spam outbreaks and clogging corporate servers.
>> <http://www.net-security.org/news.php?id=1322>

NETWORK SECURITY: TO BE SECURE OR NOT TO BE?

It is important for both system vendors and network management to understand that hardware-based IPSec and SSL acceleration is the only way to achieve multigigabit performance and throughput.
>> <http://www.net-security.org/news.php?id=1321>

[Vulnerabilities]

All vulnerabilities are located here:
http://www.net-security.org/archive_vuln.php

Linksys BEFSR41 EtherFast Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2188>

Microsoft IIS 5 & 5.1 Denial Of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2187>

Netscreen Denial of Service Caused by CRC32 Exploit
>> <http://www.net-security.org/vuln.php?id=2186>

Buffer Overflow Vulnerability in Abuse
>> <http://www.net-security.org/vuln.php?id=2185>

ION Remote File Retrieving Vulnerability
>> <http://www.net-security.org/vuln.php?id=2184>

perlbot 1.9.2 Remote Command Execution Vulnerability
>> <http://www.net-security.org/vuln.php?id=2183>

Doberman Forum Remote Command Execution Vulnerability
>> <http://www.net-security.org/vuln.php?id=2182>

Apple.LaserWriter 12/640 PS TCP/IP Printer Configuration
Utility Telnet Password Vulnerability
>> <http://www.net-security.org/vuln.php?id=2181>

Mailreader.com POP3 E-Mail Reader Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2180>

Arescom NetDSL-800 MSN Firmware version 5.4.x Username
and Password Sniffing Vulnerability
>> <http://www.net-security.org/vuln.php?id=2179>

Privilege Escalation Vulnerability In phpBB 2.0.0
>> <http://www.net-security.org/vuln.php?id=2178>

Oracle9iAS Web Cache Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2177>

AN HTTPD Cross-site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2176>

BRS WebWeaver Web Server v1.01 Protected File Access Vulnerability
>> <http://www.net-security.org/vuln.php?id=2175>

Liteserve Web Server v2.0 Authorization Bypass Vulnerability
>> <http://www.net-security.org/vuln.php?id=2174>

BadBlue Web Server v1.7 Protected File Access Vulnerability
>> <http://www.net-security.org/vuln.php?id=2173>

SolarWinds TFTP Server Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2172>

Mojo Mail Sign-Up Form Cross Site Scripting Vulnerability
>> <http://www.net-security.org/vuln.php?id=2171>

[**Advisories**]

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

Debian Security Advisory - New log2mail packages fix several vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1221>

Gentoo Linux Security Announcement - pam_ldap
>> <http://www.net-security.org/advisory.php?id=1220>

Gentoo Linux Security Announcement - sharutils
>> <http://www.net-security.org/advisory.php?id=1219>

Microsoft Security Bulletin MS02-064 - Windows 2000 Default Permissions Could Allow Trojan Horse Program
>> <http://www.net-security.org/advisory.php?id=1218>

Microsoft Security Bulletin MS02-063 - Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks
>> <http://www.net-security.org/advisory.php?id=1217>

Microsoft Security Bulletin MS02-062 - Cumulative Patch
for Internet Information Service
>> <http://www.net-security.org/advisory.php?id=1216>

SuSE Security Announcement - lprng, html2ps
>> <http://www.net-security.org/advisory.php?id=1215>

SuSE Security Announcement - syslog-ng
>> <http://www.net-security.org/advisory.php?id=1214>

Debian Security Advisory - New krb5 packages fix buffer overflow
>> <http://www.net-security.org/advisory.php?id=1213>

SCO Security Advisory - Linux: inn format string and insecure
open vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1212>

SCO Security Advisory - Linux: chfn (util-linux) temp file
race vulnerability
>> <http://www.net-security.org/advisory.php?id=1211>

Conectiva Linux Security Announcement - libpng
>> <http://www.net-security.org/advisory.php?id=1210>

SCO Security Advisory - Linux: bzip2 file creation and
symbolic link vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1209>

Mandrake Linux Security Advisory - krb5
>> <http://www.net-security.org/advisory.php?id=1208>

Gentoo Linux Security Announcement - mod_ssl
>> <http://www.net-security.org/advisory.php?id=1207>

Gentoo Linux Security Announcement - krb5
>> <http://www.net-security.org/advisory.php?id=1206>

Gentoo Linux Security Announcement - ypserv
>> <http://www.net-security.org/advisory.php?id=1205>

EnGarde Secure Linux Advisory - syslog-ng buffer overflow
in macro handling code (update)
>> <http://www.net-security.org/advisory.php?id=1204>

EnGarde Secure Linux Advisory - mod_ssl cross-site
scripting vulnerability
>> <http://www.net-security.org/advisory.php?id=1203>

SCO Security Advisory - Linux: pam_ldap format string vulnerability
>> <http://www.net-security.org/advisory.php?id=1202>

SCO Security Advisory - Linux: udecode performs inadequate checks on user-specified output files
>> <http://www.net-security.org/advisory.php?id=1201>

CERT Advisory CA-2002-29 Buffer Overflow in Kerberos (CORRECTION)
>> <http://www.net-security.org/advisory.php?id=1200>

Debian Security Advisory - New kghostview packages fix buffer overflow
>> <http://www.net-security.org/advisory.php?id=1199>

CERT Advisory CA-2002-29 - Buffer Overflow in Kerberos Administration Daemon
>> <http://www.net-security.org/advisory.php?id=1198>

Gentoo Linux Security Announcement - kth-krb & heimdal
>> <http://www.net-security.org/advisory.php?id=1197>

MIT krb5 Security Advisory - Buffer overflow in kadmind4
>> <http://www.net-security.org/advisory.php?id=1196>

MIT krb5 Security Advisory - Remote root vulnerability in MIT krb5 admin system
>> <http://www.net-security.org/advisory.php?id=1195>

[**Featured articles**]

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

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

Snort Enterprise Implementation
>> <http://www.net-security.org/article.php?id=232>

Microsoft releases IIS, Windows XP and Windows 2000 security patches
>> <http://www.net-security.org/article.php?id=231>

ActivCard Launches ActivCard Gold 2.2
>> <http://www.net-security.org/article.php?id=230>

Implementing secure web portals with RSA ClearTrust webinar
>> <http://www.net-security.org/article.php?id=229>

Network Associates Fights Spam
>> <http://www.net-security.org/article.php?id=228>

The IP Smart Spoofing
>> <http://www.net-security.org/article.php?id=227>

Check Point VPN-1/FireWall-1 added to Computer History Museum
>> <http://www.net-security.org/article.php?id=226>

No more security patches for SuSE Linux 7.0
>> <http://www.net-security.org/article.php?id=225>

DallasCon Wireless Security Conference for your wireless needs
>> <http://www.net-security.org/article.php?id=224>

[Security world]

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

Datakey Smart Card Technology Integrated with Pointsec for PC
>> <http://www.net-security.org/press.php?id=1088>

Diversinet's Advanced Security Now Available on Symbian
OS Mobile Phones
>> <http://www.net-security.org/press.php?id=1087>

GFI Beefs up Anti-Spam Features in GFI MailEssentials
>> <http://www.net-security.org/press.php?id=1086>

Partner Advanced Internet Security Inc. Earns Symantec Certification
>> <http://www.net-security.org/press.php?id=1085>

Akonix and ZANTAZ Announce Integrated IM Security & Archiving Solution

>> <http://www.net-security.org/press.php?id=1084>

NetScreen Technologies Reports Record Fiscal Fourth Quarter and 2002 Financial Results

>> <http://www.net-security.org/press.php?id=1083>

F-Secure Group's Financial Results January 1 - September 30, 2002

>> <http://www.net-security.org/press.php?id=1082>

SSH and Symark Announce Integration of SSH Secure Shell With Symark Powerpassword and Distribution of SSH Secure Shell Software

>> <http://www.net-security.org/press.php?id=1081>

Intentia's Internal Investigation Regarding Information Leaks Shows that the Reuters News Agency Broke into Intentia's IT Systems

>> <http://www.net-security.org/press.php?id=1080>

Trusecure Launches Authorized Training Partner Program, Licenses It Training Centers To Provide TICSA Certification

>> <http://www.net-security.org/press.php?id=1079>

SSH Signs Red Bull Technologies as Internet Security Reseller

>> <http://www.net-security.org/press.php?id=1078>

[Review]

All reviews are located at:

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

INCIDENT RESPONSE - INVESTIGATING COMPUTER CRIME

This book is packed with wagons of useful information, and most importantly, the authors have a great penchant for details. If you want detailed insider talk on this matter, well, you'll jump several feet in the air out of pure happiness when you read this book.

>> <http://www.net-security.org/review.php?id=15>

[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

IPARMOR 5.39

IParmor will detect and kill both known and unknown trojans. This useful system-tray utility packs a lot of punch and the known virus database can be updated daily.

>> <http://www.net-security.org/software.php?id=335>

HIDE IN PICTURE 2.1

Hide In Picture (HIP) is a steganography program. It is a program that allows you to "hide" any kind of file inside standard bitmap pictures. The pictures look like normal images, so people will not suspect they contain hidden data.

>> <http://www.net-security.org/software.php?id=336>

SCPONLY 3.1

"scponly" is an alternative 'shell' (of sorts) for system administrators who would like to provide access to remote users to both read and write local files without providing any remote execution privileges.

>> <http://www.net-security.org/software.php?id=337>

NGSECUREWEB 2.00

NGSecureWeb is the result of the fusion of two security technologies: Firewalls and IDSs, (Intrusion Detection Systems).

>> <http://www.net-security.org/software.php?id=338>

PORTLISTENER 1.0

This program is running in systray and it monitors if someone is trying to connect to a specific port on your computer.

>> <http://www.net-security.org/software.php?id=339>

HACKBOT 2.14

Hackbot is a vulnerability scanner. Hackbot scans over 300 CGI's, scans for banners of several services, does unicode checks, checks for open relays, outsmarts Cisco PIX MailGuard, can do ripe checkup, spamcop db checkup, X connect test and lots more.

>> <http://www.net-security.org/software.php?id=340>

SNORTCON 0.01

SnortCon is a web-based utility that provides a high-level overview of the threats that a network is facing. SnortCon requires that Snort is logging to a MySQL database.

>> <http://www.net-security.org/software.php?id=341>

QUARANTINE FIREWALL 0.2.1

Quarantine firewall has masquerade, type-of-service, and traffic shaping features. It has a lot of options, but is quite easy to configure.

>> <http://www.net-security.org/software.php?id=342>

RAZORBACK 1.0.3

RazorBack is a log analysis program that interfaces with the Snort open source Intrusion Detection System to provide real time visual notification when an intrusion signature has been detected on the network.

>> <http://www.net-security.org/software.php?id=343>

ANGST 0.4B

Angst is an active sniffer, based on libpcap and libnet. Angst provides methods for aggressive sniffing on switched local area network environments.

>> <http://www.net-security.org/software.php?id=344>

[Virus News]

All virus news are located at:

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

Sophos: Top 10 Viruses and Hoaxes in October 2002

>> http://www.net-security.org/virus_news.php?id=114

Virus Hunting in Saudi Arabia

>> http://www.net-security.org/virus_news.php?id=113

BitDefender Professional 6.5 Released

>> http://www.net-security.org/virus_news.php?id=112

Panda ActiveScan 4.0 Includes Specific Trojan Detection

>> http://www.net-security.org/virus_news.php?id=111

The Virus Underground Webinar

>> http://www.net-security.org/virus_news.php?id=110

Weekly Virus Report - Opaserv Worm Variants

>> http://www.net-security.org/virus_news.php?id=109

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