

HNS Newsletter  
Issue 110 - 13.05.2002  
<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>.

=====  
Sponsored by GFI, the developers of Mail essentials - the market leading email content security & anti-virus software.  
<http://www.net-security.org/lm/ads/ads.pl?banner=gfi1>

Download your free copy of LanGuard Security Event Log Monitor!  
<http://www.net-security.org/lm/ads/ads.pl?banner=gfitxt>

=====

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Security world
- 5) Featured article
- 6) Security software

General security news

-----

-----

REAL TIME VIRUS REPORTS

A new section was added to the viruses zone - RTVR. Provided by BitDefender, now you can see real time statistics about virus infections (past 24 hours, week, month and year).

>> [http://www.net-security.org/v/bd/RTVR/rtvr\\_24hours.php](http://www.net-security.org/v/bd/RTVR/rtvr_24hours.php)

SECURITY TO STEAL SHOW

At the NetWorld+ Interop conference, Cisco, Intruvert Networks, and Recourse Technologies will unveil products armed with improved performance to flag attacks that sift through network defenses.

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

ONLINE BANKING: ANATOMY OF A HACKING

Electronic break-ins can be the work of technological skill, or the result of carelessness with passwords.

>> <http://www.net-security.org/news.php?id=83>

#### BOOK REVIEW: LINUX ADMINISTRATION HANDBOOK

This book is a must-have addition to any system administrator repertoire. Not only is the book aimed at the advanced user but also the intermediate and beginner.

>> <http://www.net-security.org/news.php?id=84>

#### REVERSE CHALLENGE BINARY RELEASED

Honeynet Project is sponsoring the Reverse Challenge. The binary has now been officially released.

>> <http://www.net-security.org/news.php?id=85>

#### PATCH MANAGEMENT DONE RIGHT

How good is Microsoft's might-maligned MBSA security tool? It even tells you about the patches Redmond tries to slip under the radar.

>> <http://www.net-security.org/news.php?id=86>

#### NAME SERVICES: ANOTHER VIEW

McCarty discusses several name server topologies as well as the BIND 9.2.0 new view feature.

>> <http://www.net-security.org/news.php?id=87>

#### WIRELESS INTERNET

This tutorial introduces the reader to the Wireless Internet, WAP, WML, Wireless Protocol Stack and more.

>> <http://www.net-security.org/news.php?id=89>

#### FIRESTARTER: 5 MINUTES TO A LINUX FIREWALL

This article looks at a front-end graphical user interface you can use not only for iptables but for ipchains as well.

>> <http://www.net-security.org/news.php?id=92>

#### IDS EVASION TECHNIQUES AND TACTICS

This article explains basic IDS evasion techniques as well as suggest fixes or what to look for in many of these attacks.

>> <http://www.net-security.org/news.php?id=93>

#### AGING WORMS STILL CRAWL, THREATEN NET

Should unwitting carriers of Nimda, Code Red be penalized for not securing their servers?

>> <http://www.net-security.org/news.php?id=94>

#### CHERNOBYL VIRUS HITCHES A RIDE

The pesky Klez worm is now helping revive the Chernobyl virus, according to a new report from Symantec.

>> <http://www.net-security.org/news.php?id=95>

#### A NEW DEGREE OF SECURITY

The University of Texas at Dallas has joined forces with businesses and law-enforcement officials to create a center for cybercrime education and research.

>> <http://www.net-security.org/news.php?id=96>

#### VERISIGN FOCUSES ON MANAGED SECURITY SERVICES

VeriSign will announce a series of new and enhanced managed services aimed at enterprises that want to outsource the complexity of their security infrastructure.

>> <http://www.net-security.org/news.php?id=97>

#### "DECEPTIVE DUO" CLAIMS ALTRUISTIC MOTIVE

A pair of hackers who have been penetrating U.S. government computer systems say they're trying to call attention to vulnerabilities in national security.

>> <http://www.net-security.org/news.php?id=98>

#### FIRST, DO NO HARM - A HIPPOCRATIC OATH FOR CODERS?

With the increase in spyware, spam, etc, is it time for a Hippocratic Oath for Programmers?

>> <http://www.net-security.org/news.php?id=99>

#### UPCOMING SECURITY CONFERENCES IN 2002

These are some of top security conferences that would be very interesting to visit in the next few months.

>> <http://www.net-security.org/article.php?id=104>

#### CISCO IDS GETS FASTER

Cisco has boosted the speed and added better management capabilities to its line of intrusion detection products.

>> <http://www.net-security.org/news.php?id=101>

#### IBM REPORT CITES MOBILE PHONE HACKING RISKS

The majority of GSM phones can be cloned in just a minute or two according to IBM.

>> <http://www.net-security.org/news.php?id=102>

#### WIRELESS LANS - STANDARDS AND SECURITY

This article describes recent standards affecting WLAN technologies, the standard components of a typical WLAN solution and the issue of security on a WLAN.

>> <http://www.net-security.org/news.php?id=103>

#### EDS BANS IM

EDS, the computer arm of the British government, has banned its staff from using Instant Messenger products in the workplace. It cites security concerns, especially over virus transmissions.

>> <http://www.net-security.org/news.php?id=104>

#### RED HAT 7.3 HAS BEEN RELEASED

This version has new productivity tools, personal firewall configuration at installation, video conferencing software and more.

>> <http://www.net-security.org/article.php?id=105>

#### THE POP-UP AD CAMPAIGN FROM HELL

It's the latest in Web marketing innovation: Hijacked Web surfers, exploited Web browser vulnerabilities and malicious spyware all wrapped up together.

>> <http://www.net-security.org/news.php?id=106>

#### PREPARING FOR THE SAIR 202 APACHE EXAM

Dulaney provides a study guide for the Apache/Web servers exam, which is one of two electives leading to Sair Linux and GNU Level II (Engineer) certification.

>> <http://www.net-security.org/news.php?id=107>

#### PREPARING FOR THE SAIR 202 APACHE EXAM

Dulaney provides a study guide for the Apache/Web servers exam, which is one of two electives leading to Sair Linux and GNU Level II (Engineer) certification.

>> <http://www.net-security.org/news.php?id=107>

#### GNUPG 1.0.7 RELEASED

This new release has a lot of features beyond OpenPGP which will be included in a soon to be published RFC2440 successor.

>> <http://www.net-security.org/news.php?id=108>

#### MS: REMEDIES A BONUS FOR CRACKERS

Hackers, crackers and pirates would have a feast if the proposed sanctions against Microsoft go into effect.

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

#### THE DANGERS OF MONOCULTURE

It is common for PC software to be loaded from a standard disk image. This makes support cheaper and easier but leaves the PCs open to the latest virus.

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

#### WHO GOES THERE? EBAY WANTS TO KNOW

eBay is to announce a pact with VeriSign to confirm that sellers are who they say they are. But will it stop online fraud?

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

#### JUDGE: ELCOMSOFT CASE CAN PROCEED

A federal judge says the case against Elcomsoft, the company that employs Dmitri Sklyarov, can continue because a controversial copyright law is constitutional.

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

#### MAPS SUES ITS OWN ANTI-SPAM GURU

What happens if you create software, bring it with you to an organization and then want to take an enhanced version of it when you leave?

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

#### A CANSECWEST 2002 PRESENTATION

Ivan Arce, CTO at CORE SECURITY TECHNOLOGIES, discussed automated penetration testing tools and CORE's new CORE IMPACT product.

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

#### HOUSE PANEL OKS STIFFER CYBERCRIME PENALTIES

Computer criminals would face increased penalties, and Internet users would face greater surveillance by access providers, under a bill approved by a House of Representatives panel.

>> <http://www.net-security.org/news.php?id=115>

#### CABLE MODEM HACKING GOES MAINSTREAM

An ambitious hackware project promises to bring illicit broadband "uncapping" to the masses, and with it the risks that come with high-speed hijinks.

>> <http://www.net-security.org/news.php?id=116>

#### EXPERTS ENVISION GRAPHICS-BASED PASSWORDS

Many people have trouble remembering passwords like XYZ4(NU)T. So they keep passwords down near their computer or replace them with simpler combinations, making their systems vulnerable to attack.

>> <http://www.net-security.org/news.php?id=117>

#### LINUX AND FREE SOFTWARE FESTIVAL - ANKARA 2002

The Linux Users' Association of Turkey is holding the 1st Linux and Free Software Festival between 16-19 May 2002.

>> <http://www.net-security.org/news.php?id=120>

#### IKEY FOR WINDOWS 2000 USB SECURITY TOKEN

Rainbow eSecurity recently developed a new offering in their iKey 2032 USB security token series - iKey for Windows 2000.

>> <http://www.net-security.org/article.php?id=107>

#### TEAM TACKLES WINDOWS SECURITY

Government, industry and academia have teamed up to secure

the most popular system being deployed on servers in the public and private sectors: Windows 2000.

>> <http://www.net-security.org/news.php?id=123>

#### THE BOY WHO CRIED WORM

Hoaxes can be just as damaging to resources and reputations as real viruses. Natasha Staley, anti-virus consultant at Sophos speaks.

>> <http://www.net-security.org/news.php?id=124>

#### "CUTE" TROJAN HORSE SPREADING BY E-MAIL

The worm has been rated low risk, but it could damage firewall and security programs on infected PCs.

>> <http://www.net-security.org/news.php?id=125>

#### UNDERSTANDING SECURITY THREATS: YOU ARE A TARGET!

Just as armies have developed standard ways of discussing and thinking about war, IT professionals should develop common ways of thinking about information threats.

>> <http://www.net-security.org/news.php?id=126>

#### SHARING SEEN AS CRITICAL FOR SECURITY

Industry must collaborate with the government to protect the nation's critical infrastructure, experts say.

>> <http://www.net-security.org/news.php?id=127>

#### 'OPERATION WEB SWEEP' TARGETS PORN

Federal and state officials said that they were targeting up to 200 suspects in what they called the first undercover computer sting operation to combat child pornography.

>> <http://www.net-security.org/news.php?id=128>

#### ASTARO SECURITY LINUX 3.0 ANNOUNCED

At the Networld + Interop Conference, Astaro Corporation announced version 3 of Astaro Security Linux.

>> <http://www.net-security.org/article.php?id=108>

#### CUTTING SPAM AT A COST

Spam is not only an annoyance, it also drains productivity and leaves companies open to threats, such as well-disguised denial-of-service attacks.

>> <http://www.net-security.org/news.php?id=130>

#### TRACKING FOREIGN STUDENTS

Attorney General John Ashcroft said that a new Internet-based system will start to better track the 1 million foreign students in USA.

>> <http://www.net-security.org/news.php?id=131>

## XBOX EMULATOR IS A TROJAN

An "Xbox emulator" currently being offered for free on the Web is actually a Trojan horse designed to covertly rack up money for its authors.

>> <http://www.net-security.org/news.php?id=134>

---

---

Computer Security Institute Survey: 90% Say Systems Hacked.

How Secure Is Your Network? Get a FREE Assessment!

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

---

[ Vulnerabilities ]

All vulnerabilities are located here:

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

---

MnoGoSearch 3.1.19 Vulnerability

>> <http://www.net-security.org/vuln.php?id=1678>

inJoin V4.0 Directory Server Directory Traversal

>> <http://www.net-security.org/vuln.php?id=1677>

inJoin V4.0 Directory Server Cross Site Scripting

>> <http://www.net-security.org/vuln.php?id=1676>

Wu-imap Buffer Overflow Condition

>> <http://www.net-security.org/vuln.php?id=1675>

SafeWeb Vulnerability - Fingerprinting Websites Using Traffic Analysis

>> <http://www.net-security.org/vuln.php?id=1674>

Linux kernel 2.4 "weak end host" issue

>> <http://www.net-security.org/vuln.php?id=1673>

Cisco ATA-186 Admin Password Circumvention

>> <http://www.net-security.org/vuln.php?id=1672>

OpenBSD local Denial of Service and root exploit

>> <http://www.net-security.org/vuln.php?id=1671>

Multiple Vulnerabilities in Novell Border Manager 3.6  
>> <http://www.net-security.org/vuln.php?id=1670>

Novell Netware Client Multiple Buffer Overflows  
>> <http://www.net-security.org/vuln.php?id=1669>

Netware FTP server Denial of Service Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1668>

ISC DHCPDv3 Remote Root Compromise  
>> <http://www.net-security.org/vuln.php?id=1667>

Webmin/Usermin Session ID Spoofing Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1666>

Webmin/Usermin Cross-site Scripting Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1665>

MSN Messenger OCX Buffer Overflow  
>> <http://www.net-security.org/vuln.php?id=1664>

NTFS and PGP interact to expose EFS encrypted data  
>> <http://www.net-security.org/vuln.php?id=1663>

DNS2Go Client 2.6.00 Stores Password in Plain Text  
>> <http://www.net-security.org/vuln.php?id=1662>

Lysias Lidik Webserver Directory Traversal Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1661>

Multiple Vulnerabilities in MDaemon + WorldClient  
>> <http://www.net-security.org/vuln.php?id=1660>

Pointsec for PalmOS PIN disclosure  
>> <http://www.net-security.org/vuln.php?id=1659>

AOL Instant Messenger remote overflow #2  
>> <http://www.net-security.org/vuln.php?id=1658>

Malformatted Message Header Causes MSN  
Messenger Crash  
>> <http://www.net-security.org/vuln.php?id=1657>

B2 PHP Remote Command Execution

>> <http://www.net-security.org/vuln.php?id=1656>

Digitally Signing Buggy Components

>> <http://www.net-security.org/vuln.php?id=1655>

Solaris cachefs remote buffer overflow vulnerability

>> <http://www.net-security.org/vuln.php?id=1654>

4D WebServer Buffer Overflow

>> <http://www.net-security.org/vuln.php?id=1653>

Snapgear Lite+ Firewall Denial of Service

>> <http://www.net-security.org/vuln.php?id=1652>

Macromedia Flash Activex Buffer overflow

>> <http://www.net-security.org/vuln.php?id=1651>

Logitech Keyboard Denial of Service

>> <http://www.net-security.org/vuln.php?id=1650>

-----  
[ Advisories ]

All advisories are located at:

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

-----  
Mandrake Linux Security Advisory - iptables/kernel

>> <http://www.net-security.org/advisory.php?id=686>

CERT Advisory CA-2002-13 - Buffer Overflow in Microsoft's  
MSN Chat ActiveX Control

>> <http://www.net-security.org/advisory.php?id=685>

Red Hat Security Advisory - perl-Digest-MD5 UTF8 bug

>> <http://www.net-security.org/advisory.php?id=684>

Conectiva Linux Security Announcement - dhcp

>> <http://www.net-security.org/advisory.php?id=683>

Red Hat Security Advisory - Netfilter information leak  
>> <http://www.net-security.org/advisory.php?id=682>

CERT Advisory CA-2002-12 - Format String Vulnerability  
in ISC DHCPD  
>> <http://www.net-security.org/advisory.php?id=681>

SGI Security Advisory - fsr\_xfs vulnerability  
>> <http://www.net-security.org/advisory.php?id=680>

Red Hat Security Advisory - Updated mod\_python packages  
available (revised)  
>> <http://www.net-security.org/advisory.php?id=679>

Cisco Security Advisory - NTP Vulnerability  
>> <http://www.net-security.org/advisory.php?id=678>

Microsoft Security Bulletin MS02-022 - Unchecked Buffer  
in MSN Chat Control Can Lead to Code Execution  
>> <http://www.net-security.org/advisory.php?id=677>

Caldera Security Advisory - Open UNIX 8.0.0 UnixWare 7.1.1:  
CDE /var/dt and subdirectories are writable by world  
>> <http://www.net-security.org/advisory.php?id=676>

Conectiva Linux Security Announcement - imlib  
>> <http://www.net-security.org/advisory.php?id=675>

Conectiva Linux Security Announcement - imp (updated)  
>> <http://www.net-security.org/advisory.php?id=674>

SuSE Security Announcement - sysconfig  
>> <http://www.net-security.org/advisory.php?id=673>

Conectiva Linux Security Announcement - tcpdump  
>> <http://www.net-security.org/advisory.php?id=672>

Conectiva Linux Security Announcement - gmp  
>> <http://www.net-security.org/advisory.php?id=671>

Conectiva Linux Security Announcement - mailman  
>> <http://www.net-security.org/advisory.php?id=670>

SGI Security Advisory - netstat vulnerability  
>> <http://www.net-security.org/advisory.php?id=669>

SuSE Security Announcement - imlib  
>> <http://www.net-security.org/advisory.php?id=668>

CERT Advisory CA-2002-11 - Heap Overflow in Cachefs  
Daemon (cachefsd)  
>> <http://www.net-security.org/advisory.php?id=667>

---

[ Security world ]

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

---

Sophos Protects Ann Summers Against Virus Threat  
>> <http://www.net-security.org/press.php?id=773>

SOFTWIN Releases BitDefender Free Edition v.7  
>> <http://www.net-security.org/press.php?id=772>

Trend Micro Unveils InterScan VirusWall 3.6 CSP with Support  
for NetScreen-100 and NetScreen-500  
>> <http://www.net-security.org/press.php?id=771>

Osis' AccessNow Express Wins Best Of Interop Awards  
At N+I 2002 Las Vegas  
>> <http://www.net-security.org/press.php?id=770>

Osis Introduces SiteStripper  
>> <http://www.net-security.org/press.php?id=769>

Sophos launches OEM team to span the globe  
>> <http://www.net-security.org/press.php?id=768>

Rainbow and ERUCES Team Up on High-Assurance Data Security  
>> <http://www.net-security.org/press.php?id=767>

One of the Industry's Fastest Biometric Identification Solutions,  
Matches 10,000 Fingerprints Per Second

>> <http://www.net-security.org/press.php?id=766>

Rainbow Debuts NetSwift iGate Web Access Appliance  
at Networld+Interop

>> <http://www.net-security.org/press.php?id=765>

Activis Named Winner of Two Major Industry Awards

>> <http://www.net-security.org/press.php?id=764>

FalconStor Partners With Network-1

>> <http://www.net-security.org/press.php?id=763>

McAfee.com Unveils 'SpamKiller' for Consumers and Businesses

>> <http://www.net-security.org/press.php?id=762>

Tiny Software's Trojan Trap Stops Cyber-Threats Undetectable  
by Antivirus Software

>> <http://www.net-security.org/press.php?id=761>

SAFLINK Corporation To Present At Wall Street Analyst Forum

>> <http://www.net-security.org/press.php?id=760>

SC Magazine Presents Rainbow's iKey with "Editor's Special"  
Award at 2002 SC Awards

>> <http://www.net-security.org/press.php?id=759>

Datastrip Offers Advanced 2D Bar Code System Helps Reduce ID Fraud

>> <http://www.net-security.org/press.php?id=758>

McAfee.com CEO to Speak at the 30th Annual JP Morgan H&Q  
Technology Conference

>> <http://www.net-security.org/press.php?id=757>

InfoExpress Unveils CyberGatekeeper Appliance

>> <http://www.net-security.org/press.php?id=756>

Authenex ASAS To Support Microsoft ISA Server

>> <http://www.net-security.org/press.php?id=755>

OSITIS' AccessNowEXPRESS Named Finalist In The Best Of  
Interop Awards For NW+I 2002

>> <http://www.net-security.org/press.php?id=754>

Kaspersky Labs The Virus Top Twenty for April 2002  
>> <http://www.net-security.org/press.php?id=753>

---

[ Featured article ]

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)

---

**SIMPLICITY AND AWARENESS – KEYS TO NETWORK SECURITY**  
The modern networking environment is destroying both simplicity and awareness. The purpose of this article is to explain how security professionals can deal with this hostile situation.  
>> <http://www.net-security.org/article.php?id=106>

---

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

---

**BACKSTEALTH 1.1**  
BackStealth is an innovative Security Utility which allows to bypass the outbound protection of a Personal Firewall in order to establish a remote connection.  
>> <http://www.net-security.org/software.php?id=101>

**RATS 1.4**  
RATS, the Rough Auditing Tool for Security, is a security auditing utility for C, C++, Python, Perl and PHP code. RATS scans source code, finding potentially dangerous function calls. The goal of this project is not to definitively find bugs. The current goal is to provide a reasonable starting point for performing manual security audits.  
>> <http://www.net-security.org/software.php?id=102>

#### WINFINGERPRINT 0.4.4

Winfingerprint is a Win32 based security tool that is able to Determine OS, enumerate users, groups, shares, transports, sessions, services, service pack and hotfix level, date and time, disks, and open tcp ports.

>> <http://www.net-security.org/software.php?id=103>

#### IPFC 1.0.4

IPFC is a software and framework to manage and monitor multiple types of security modules across a global network. Security modules can be as diverse as packet filters (like netfilter, pf, ipfw, IP Filter, checkpoint FW1...), NIDS (Snort, arpswatch...), web servers and other general devices (from servers to embedded devices).

>> <http://www.net-security.org/software.php?id=104>

-----  
Questions, contributions, comments or ideas go to:

Help Net Security staff  
[staff@net-security.org](mailto:staff@net-security.org)  
<http://net-security.org>

-----  
Subscribe to this weekly digest on:  
<http://www.net-security.org/text/newsletter>

Unsubscribe by sending your e-mail address to:  
[info@net-security.org](mailto:info@net-security.org) with UNSUBSCRIBE in the message body.

The archive of the newsletter in TXT and PDF format is available here: <http://www.net-security.org/news/archive/newsletter>