

HNS Newsletter
Issue 109 - 06.05.2002
<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>.

<<-- HNS has a completely new look, check it out -->>

=====
Sponsored by GFI, the developers of Mail essentials - the market leading email content security & anti-virus software.

For more information click here:
<http://www.net-security.org/lm/ads/ads.pl?banner=gfi1>

=====
Table of contents:

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

[General security news]

FUTURE TECH: HACK-PROOF CHATTING

Discover magazine outlines the first successful laser photon communication utilizing Quantum Cryptography.
>> <http://www.net-security.org/news.php?id=47>

CRACKERS FAVOUR WAR DIALLING AND WEAK PASSWORDS

During a debate at InfoSecurity Europe, hacker KP said that when he broke into a network he did so 90% of the time through an unprotected modem, often through war dialling.
>> <http://www.net-security.org/news.php?id=48>

EMPLOYEES SEEN AS COMPUTER SABOTEURS

Digital cameras, MP3 players and handheld computers could be the tools that disgruntled employees use to sabotage computer systems or steal vital data, warn security experts.
>> <http://www.net-security.org/news.php?id=49>

EU TO HARMONISE CYBERCRIME LAWS

The Commission of the EU has adopted a proposal for a Council framework decision that seeks to harmonize the EU's legal response to so-called cybercrimes.

>> <http://www.net-security.org/news.php?id=50>

WLANS TO GET MORE SECURE

ReefEdge is readying a wireless solution for carriers that want to offer WLAN services and IT managers who want assurances data is secure.

>> <http://www.net-security.org/news.php?id=51>

'BLENDED' ATTACKS POSE SERIOUS SECURITY THREAT

Attacks that target different areas of your network are a major danger, and a strong defence is essential.

>> <http://www.net-security.org/news.php?id=52>

BETTER SECURITY NEEDS SCARE TACTICS

IT managers need to scare senior executives into adopting information security awareness programmes, but initiate a range of innovative marketing campaigns to sell it to the end user.

>> <http://www.net-security.org/news.php?id=53>

XP UPDATES START TO P.O. USERS

Windows XP's pop-up patches allow users to play games and access file-trading systems. But experts are worried the bulky updates may compromise security patches.

>> <http://www.net-security.org/news.php?id=54>

MS SECURITY COP PATROLS A TOUGH BEAT

Microsoft's chief security strategist aims to keep security at the forefront of the software giant's agenda, but observers want action not words.

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

WORMS: WHO'S THE DEADLIEST OF THEM ALL?

The latest fast-spreading versions of the Klez worm have so far infected 7.2 percent of PCs worldwide.

>> <http://www.net-security.org/news.php?id=56>

NETWORK FORENSICS: TAPPING THE INTERNET

Simson Garfinkel examines the current crop of network monitoring tools and the ethical issues involved in scanning network traffic.

>> <http://www.net-security.org/news.php?id=57>

HACK YOURSELF FOR TOP SECURITY

Learn how to become the best protector of your own security with ExtremeTech/syscheck.

>> <http://www.net-security.org/news.php?id=58>

ASTARO: A "SWISS-ARMY KNIFE" OF SECURITY SOFTWARE

ASL brings together Astaro's proprietary middleware, user interface, and Web-based administration tools with a hardened Linux kernel and several open source security components.

>> <http://www.net-security.org/news.php?id=60>

KLEZ: DON'T BELIEVE 'FROM' LINE

Why are Catholic priests sending porn spam? Why is a Grammy Award-winning band's e-mail list automatically subscribing unwitting users? These are just some of the victims of the raging Klez virus.

>> <http://www.net-security.org/news.php?id=61>

ONLINE BANKS: PRIME TARGETS FOR ATTACKS

Instead of a note and a gun, high-tech bank robbers use a program and an e-mail. Security firms are working overtime to ward off the mounting number of hack attacks.

>> <http://www.net-security.org/news.php?id=62>

AUTHENTICATION OF USER ACCOUNTS ON OPENBSD

This article shows the steps for configuring OpenBSD to authenticate user accounts against an LDAP directory via the RADIUS protocol.

>> <http://www.net-security.org/news.php?id=63>

WHERE'S SDMI? CODE TO BATTLE PIRACY IS MIA

Four years ago the record industry and some technology companies banded together to match wits in a combined effort to stamp out Internet music piracy...

>> <http://www.net-security.org/news.php?id=64>

SECURITY THREATS CHANGING

The Department of Trade and Industry released the findings of a survey of one thousand people responsible for IT Security in UK business during the recent InfoSec show. The results are not encouraging.

>> <http://www.net-security.org/news.php?id=65>

SECURITY CERTIFICATES OFFER LITTLE GUARANTEE

As the IT training market becomes flooded with security courses and certifications, experts have warned that qualifications may be leading companies into a false sense of security.

>> <http://www.net-security.org/news.php?id=66>

MELISSA VIRUS CREATOR JAILED

The creator of a computer virus which caused millions of dollars of damage by disrupting networks all over the world has been jailed for 20 months by a United States court.

>> <http://www.net-security.org/news.php?id=67>

DEF CON 10 CALL FOR PAPERS ANNOUNCEMENT

Papers and presentations are now being accepted for DEF CON TEN, the largest "hacking" convention on the planet.

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

MUSIC PLAYER BUG COULD LET IN MP3 VIRUSES

The code inside Winamp contains a bug that could allow computer viruses to be concealed within MP3 files.

>> <http://www.net-security.org/news.php?id=69>

SURVEILLANCE CAMERAS TO PREDICT BEHAVIOUR

CCTV cameras that can predict behaviour could play a vital role in the fight against crime.

>> <http://www.net-security.org/news.php?id=70>

SOLARIS 9 TO BEEF UP OS, APPLICATION SECURITY

With Sun getting ready to launch Solaris 9, sometime between now and the end of June, everyone is scrambling to try to figure out what will make Solaris 9 different from the existing Solaris 8.

>> <http://www.net-security.org/news.php?id=71>

INTERIOR SECURITY FLAGGED AGAIN

A month after getting permission to reconnect some of its sites to the Internet, the Interior Department's Minerals Management Service is back in the hot seat.

>> <http://www.net-security.org/news.php?id=72>

BIOMETRIC SECURITY NOT QUITE READY TO REPLACE PASSWORDS

Biometrics vendors are doing their best to supplant passwords as the chief form of computer security, but Government Computer News Lab tests indicate that many of their products are not quite ready.

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

HOW TO STAY ONE STEP AHEAD OF HACKERS

Malicious code can take many forms and attack your enterprise in many ways. Though such "blended" threats are nothing new, the code within them is learning new tricks.

>> <http://www.net-security.org/news.php?id=74>

NO CRISIS OVER 1,024-BIT ENCRYPTION

Security firm RSA has hit back at cryptography experts' claims that 1,024-bit encryption is no longer secure.

>> <http://www.net-security.org/news.php?id=75>

HONEYNET PROJECT: THE REVERSE CHALLENGE

The goal of this challenge is to develop reverse engineering skills amongst the security community.

>> <http://www.net-security.org/news.php?id=76>

FAULT FOUND IN .NET SECURITY

Microsoft needs to iron some problems out of the .Net Web services infrastructure, suggests H.D. Moore, a hacker and senior security analyst for Digital Defense.

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

IT SECURITY EFFORTS 'POOR'

According to Gartner, the real lack of security stems from bad habits that include poor password management, unintentional data exposure and careless software installations.

>> <http://www.net-security.org/news.php?id=78>

HOW TO INSTALL PURESECURE, THE PAINLESS IDS

PureSecure is much more polished, more complete, and more fully featured than its free software counterpart ACID. It's not free for commercial use, however.

>> <http://www.net-security.org/news.php?id=79>

WIRELESS (IN)SECURITY

Dubrawsky discusses weaknesses in the Wired Equivalent Privacy protocol and notes security factors to keep in mind when deploying a wireless LAN.

>> <http://www.net-security.org/news.php?id=80>

HACKING IN THE SHADOW OF 9/11

David Dittrich, senior security engineer for the University of Washington, discusses the newest tools of the trade with K2.

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

[Vulnerabilities]

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

Levcgi.com MyGuestbook JavaScript Injection Vulnerability
>> <http://www.net-security.org/vuln.php?id=1649>

Remote Denial of Service in RealSecure Network Sensor
>> <http://www.net-security.org/vuln.php?id=1648>

Bea Weblogic incorrect URL parsing issues
>> <http://www.net-security.org/vuln.php?id=1647>

Reading local files in Netscape 6 and Mozilla
>> <http://www.net-security.org/vuln.php?id=1646>

Blahz-DNS Authentication bypass vulnerability
>> <http://www.net-security.org/vuln.php?id=1645>

Sun Solaris cachefsd mount file buffer overflow vulnerability
>> <http://www.net-security.org/vuln.php?id=1644>

Sun Solaris cachefsd denial of service vulnerability
>> <http://www.net-security.org/vuln.php?id=1643>

Sun Solaris admintool media installation path buffer overflow vulnerability
>> <http://www.net-security.org/vuln.php?id=1642>

Sun Solaris lbxproxy display name buffer overflow vulnerability
>> <http://www.net-security.org/vuln.php?id=1641>

CIDER SHADOW CGI arbitrary command execution
>> <http://www.net-security.org/vuln.php?id=1640>

CDE dtprintinfo Help search buffer overflow vulnerability
>> <http://www.net-security.org/vuln.php?id=1639>

Sun Solaris admintool -d and PROVERS buffer overflow vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1638>

Bypassing of ATGuard Firewall possible
>> <http://www.net-security.org/vuln.php?id=1637>

[Advisories]

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

Red Hat Security Advisory - Updated Nautilus for symlink
vulnerability writing metadata files

>> <http://www.net-security.org/advisory.php?id=666>

Red Hat Security Advisory - Updated mod_python packages available

>> <http://www.net-security.org/advisory.php?id=665>

Conectiva Linux Security Announcement - mod_python

>> <http://www.net-security.org/advisory.php?id=664>

CERT Advisory CA-2002-10 - Format String Vulnerability in rpc.rwalld

>> <http://www.net-security.org/advisory.php?id=663>

Red Hat Security Advisory - Insecure DocBook stylesheet option

>> <http://www.net-security.org/advisory.php?id=654>

Caldera Security Advisory - OpenServer 5.0.5 : sar -o buffer overflow

>> <http://www.net-security.org/advisory.php?id=653>

Caldera Security Advisory - Linux: imlib processes untrusted images

>> <http://www.net-security.org/advisory.php?id=652>

SGI Security Advisory - Xlib vulnerability

>> <http://www.net-security.org/advisory.php?id=651>

SGI Security Advisory - pmcd Denial of Service vulnerability

>> <http://www.net-security.org/advisory.php?id=650>

SGI Security Advisory - IRIX nsd symlink vulnerability

>> <http://www.net-security.org/advisory.php?id=649>

SGI Security Advisory - /dev/ipfilter Denial of Service vulnerability

>> <http://www.net-security.org/advisory.php?id=648>

SGI Security Advisory - IRIX cpr vulnerability

>> <http://www.net-security.org/advisory.php?id=647>

SuSE Security Announcement - sudo

>> <http://www.net-security.org/advisory.php?id=646>

Caldera Security Advisory - Linux: Race condition in fileutils

>> <http://www.net-security.org/advisory.php?id=645>

[Security world]

All press releases are located at:

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

Secos Introduces Intrusion Detection System SecoShield 3.0

>> <http://www.net-security.org/press.php?id=752>

Top Ten Viruses And Hoaxes Reported To Sophos In April 2002

>> <http://www.net-security.org/press.php?id=751>

Melissa Worm Author Convicted - Sophos Welcomes Decision But
Calls For Swifter Sentencing

>> <http://www.net-security.org/press.php?id=750>

NetOctave To Demonstrate NSP2000B-SSL Security Accelerator Board
Performing Greater Than 1,700 SSL Transactions Per Second at
Networld+Interop Las Vegas 2002

>> <http://www.net-security.org/press.php?id=749>

Rainbow to Host a TechTarget Webinar on Windows Security

>> <http://www.net-security.org/press.php?id=748>

[Featured article]

All articles are located at:

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

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

REMOTE TIMING TECHNIQUES

This paper describes remote timing techniques based on TCP/IP intrinsic operation and options.

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

[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=1

MONITOR 4.0BETA

A lightweight (distributed?) network security monitor for TCP/IP+Ethernet LANs. It will capture certain network events and record them in a relational database. The recorded data will be available for analysis through a CGI based interface.

>> <http://www.net-security.org/software.php?id=100>

ETHERREAL 0.9.1

Ethereal is a free network protocol analyzer. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet.

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

KERBEROS 5 RELEASE 1.2.3

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

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

FIREWALL 2.6

If you don't block it you could be victim of hackers who could invade your equipment while you are connected on the Internet. The permanent connections such as xDSL or long term connections on the net make you more vulnerable. Protect your business or home valuable information. Block any entrance through Backdoors from theft, avoid failures, trojans or any unwanted intruder in your Network.

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

IRCCRYPT 1.0

IRCCrypt is a local IRC Proxy-style utility that provide application layer encryption for public channels. It is a perfect solution when you need to hold private chats in public areas.

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

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/text/newsletter>

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 here: <http://www.net-security.org/news/archive/newsletter>