



Newsletter
Issue 140



Issue 140 - 16.12.2002

<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>.

Strengthening Network Security: FREE Guide

Network security is a constantly moving target - even proven solutions lose their punch over time.

Find out how to get COMPLETE PROTECTION against ever-growing security threats with our FREE new Guide.

Get your copy today at

https://www.qualys.com/forms/nsguideh_442.php

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]

FEDS LABEL WI-FI A TERRORIST TOOL

Attention, Wi-Fi users: The Department of Homeland Security sees wireless networking technology as a terrorist threat.

>> <http://www.net-security.org/news.php?id=1598>

SETTING UP SOPHOS + AMAVIS FOR POSTFIX

Protecting a system against viruses is an important thing for every system administrator. In this article the author shows us how to install Sophos and Amavis.

>> <http://www.net-security.org/news.php?id=1599>

HACKER FROM THE 'HOOD TELLS ALL

Ejovi Nuwere survived growing up in a tough Brooklyn neighborhood by learning how to hack -- and doing well at it. His message in his new autobiography: "Kids, don't try most of this at home."

>> <http://www.net-security.org/news.php?id=1600>

DROP THAT E-BOOK OR I'LL SHOOT!

With the first ever criminal DMCA trial halfway over, it's already raising novel legal, jurisdictional and ethical challenges.

>> <http://www.net-security.org/news.php?id=1601>

REPORT: SPAM NOT A PROBLEM AT WORK

Contrary to popular belief, the majority of American office workers aren't overwhelmed with spam, and most consider e-mail very valuable in helping them do their jobs, a new study shows.

>> <http://www.net-security.org/news.php?id=1602>

CUSTOMS SEARCHES SOFTWARE FIRM NEAR BOSTON

Customs agents searched a high-tech company looking for evidence that the software provider - which has numerous government agencies as clients - may have ties to al Qaeda.

>> <http://www.net-security.org/news.php?id=1603>

DECSS AUTHOR GOES ON TRIAL

Jon Lech Johansen was only 15 when he wrote DeCSS. The case is seen as an important test of Norway's strict laws against computer piracy and hacking.

>> <http://www.net-security.org/news.php?id=1604>

UK POLICE OFFER CYBER-CRIME VICTIM FIRMS ANONYMITY

Britain's digital crime-fighting force said it will grant businesses victimized by digital attacks full anonymity if they come forward, an effort to jumpstart investigations into the growing wave of cyber crime.

>> <http://www.net-security.org/news.php?id=1608>

NAGIOS - A FEATURE-RICH NETWORK MONITORING PACKAGE

Its displays provide current information about system or resource status across an entire network. It can also send alerts and perform other actions when problems are detected.

>> <http://www.net-security.org/news.php?id=1609>

SECURITY BY NUMBERS?

An Aberdeen Group report claims that open source is less secure than Windows. And how did they come to this profound conclusion?

>> <http://www.net-security.org/news.php?id=1610>

COMPLEX NETWORKS TOO EASY TO HACK

Telecommunications executives advise the FCC on protecting US complex networks from attack by newbie and experienced attackers.

>> <http://www.net-security.org/news.php?id=1611>

GERMANY CAUTIOUS ON MICROSOFT SECURITY

The German government is worried about federal agencies adopting Microsoft's upcoming Palladium security technology, fearing the system could lead to higher costs.

>> <http://www.net-security.org/news.php?id=1612>

IT'S NOT EASY BEING BREACHED

Surviving a security incident is just the beginning. Then you need to figure out what it really cost.

>> <http://www.net-security.org/news.php?id=1613>

THE DANGERS OF DO-IT-YOURSELF SECURITY

Beware the misuse of vulnerability-testing software.

>> <http://www.net-security.org/news.php?id=1614>

STOPPING VIRUSES AT THE GATE

In the past, many companies relied on desktop antivirus software to protect against malicious code, but that approach is no longer sufficient on its own.

>> <http://www.net-security.org/news.php?id=1615>

JON LECH JOHANSEN DENIES DVD PIRATING

Johansen's attorney, Halvor Manshaus, said the teen cannot be convicted of breaking into a DVD that he bought and legally owned.

>> <http://www.net-security.org/news.php?id=1616>

REPORT SUGGESTS ID ALTERNATIVES

National Electronic Commerce Coordinating Council proposes a 'confederated' system.

>> <http://www.net-security.org/news.php?id=1618>

THREATS MOVE BEYOND LINUX TO WINDOWS

UNIX admins have been dealing with rootkits since the early 1990s. Now, Windows admins must get up to speed, because rootkits are also being used to attack Windows NT and 2000 systems.

>> <http://www.net-security.org/news.php?id=1619>

SECURING OUTLOOK, PART ONE: INITIAL CONFIGURATION

This article is the first of a two-part article that will examine ways that Outlook users can secure their email client.

>> <http://www.net-security.org/news.php?id=1620>

LIVING WITH WORMS, VIRUSES AND DAILY SECURITY

Complicated applications and slipshod development keep security pros one step behind.

>> <http://www.net-security.org/news.php?id=1621>

SECURE PASSWORDLESS LOGINS WITH SSH PART 1

How to create passwordless logins to allow remote administration tasks securely with SSH.

>> <http://www.net-security.org/news.php?id=1628>

ALL BUGS ARE CREATED EQUAL

ISS has promised to handle security vulnerabilities affecting open source and Windows platforms the same way following criticism of its premature disclosure of open source security problems.

>> <http://www.net-security.org/news.php?id=1629>

LAW MAY BE UPDATED TO COVER DOS ATTACKS

Concerns that some types of hacking might not be covered by the UK's Computer Misuse Act could prompt changes to the law, following strong lobbying from industry.

>> <http://www.net-security.org/news.php?id=1630>

DENMARK BILLS USERS FOR DOWNLOADS

A Danish anti-piracy group has begun charging individuals for illegal copies of music, film and software. Could this be the shape of things to come in the United States?

>> <http://www.net-security.org/news.php?id=1631>

ROOTING OUT CORRUPTED CODE

Is there a backdoor on your system? A project from the Shmoo Group could help network administrators spot altered programs.

>> <http://www.net-security.org/news.php?id=1632>

INFOSECURITY: UNISYS MINDING THE SECURITY GAP

With fresh statistics that show gaping holes in the security preparedness of companies, Unisys announced a new initiative that will help companies improve security readiness.

>> <http://www.net-security.org/news.php?id=1633>

TRUSTE TIGHTENS REQUIREMENTS FOR ITS SEAL OF APPROVAL

A leading privacy seal group, Truste, has toughened its privacy seal licensing requirements as well as its ability to monitor the privacy practices of Web sites that display its seal.

>> <http://www.net-security.org/news.php?id=1634>

WARDRIVING FOR WI-FI

Hotspotting for oozing radio waves points to security concerns.

>> <http://www.net-security.org/news.php?id=1638>

ELCOMSOFT CASE IN JURORS' HANDS

Russian software company ElcomSoft, standing trial in U.S. District Court for selling software that cracked copy protection in Adobe e-books, rests its legal fate with the jury.

>> <http://www.net-security.org/news.php?id=1639>

IDC: CYBERTERROR TO HIT IN 2003

A major cyberterrorism event will occur in 2003, a technology research group predicted on Thursday, one that will disrupt the economy and bring the Internet to its knees for at least a day or two.

>> <http://www.net-security.org/news.php?id=1640>

BELGIUM GETS SMART ABOUT IDENTITY

The Belgian government hopes that within five years every citizen will be carrying a new electronic identity card. But will the new 'smart' IDs prove to be the citizen's friend or Big Brother's little helper?

>> <http://www.net-security.org/news.php?id=1641>

SPAM MAY OVERTAKE E-MAIL IN 2003

MessageLabs says e-mail threats, including viruses and spam, are increasing at an "alarming rate."

>> <http://www.net-security.org/news.php?id=1642>

Q&A: SPRINT'S CSO, ROBERT FOX, DEFINES HIS ROLE

Sprint's chief security officer talks about his role overseeing both physical and IT security at the telecommunications provider.

>> <http://www.net-security.org/news.php?id=1643>

[Vulnerabilities]

All vulnerabilities are located here:

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

Multiple MySQL Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2300>

Portable Network Graphics (PNG) Deflate Heap Corruption Vulnerability

>> <http://www.net-security.org/vuln.php?id=2299>

Mambo Site Server Multiple Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=2298>

Visnetic WebSite HTTP Referer Header Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=2297>

Adelphia Powerlink Man in the Middle Attacks by Cable Modem Users

>> <http://www.net-security.org/vuln.php?id=2296>

Directory Traversal Vulnerabilities in FTP Clients

>> <http://www.net-security.org/vuln.php?id=2295>

MTPSR1-120 Firewall Proxy Configuration Software Passwordless Telnet Access

>> <http://www.net-security.org/vuln.php?id=2294>

myServer Webserver Directory Traversal Vulnerability

>> <http://www.net-security.org/vuln.php?id=2293>

VisNetic WebSite Denial of Service
>> <http://www.net-security.org/vuln.php?id=2292>

Kunani FTP-Server v.1.0.10 Directory Traversal Vulnerability
>> <http://www.net-security.org/vuln.php?id=2291>

TFTP32 Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=2290>

apt-www-proxy Multiple Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2289>

PC-cillin pop3trap.exe Unchecked Buffer
>> <http://www.net-security.org/vuln.php?id=2288>

Enceladus Server Suite v3.9 Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=2287>

Cyrus SASL Library Buffer Overflows
>> <http://www.net-security.org/vuln.php?id=2286>

Ikonboard 3.1.1 Cross Site Scripting Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2285>

WebReflex Directory Traversal Vulnerability
>> <http://www.net-security.org/vuln.php?id=2284>

Ultimate PHP Board Cross Site Scripting and Path Disclosure Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=2283>

APBoard Allows Subscribing to Internetal Threads
>> <http://www.net-security.org/vuln.php?id=2282>

[Advisories]

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

Debian Security Advisory - lynx CRLF injection
>> <http://www.net-security.org/advisory.php?id=1392>

Debian Security Advisory - two wget problems
>> <http://www.net-security.org/advisory.php?id=1391>

Mandrake Linux Security Advisory - wget
>> <http://www.net-security.org/advisory.php?id=1390>

Red Hat Security Advisory - Updated apache, httpd, and mod_ssl packages available
>> <http://www.net-security.org/advisory.php?id=1389>

Debian Security Advisory - New Perl packages correct Safe handling
>> <http://www.net-security.org/advisory.php?id=1388>

Microsoft Security Bulletin MS02-071 - Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation
>> <http://www.net-security.org/advisory.php?id=1387>

Microsoft Security Bulletin MS02-070 - Flaw in SMB Signing Could Enable Group Policy to be Modified
>> <http://www.net-security.org/advisory.php?id=1386>

Microsoft Security Bulletin MS02-069 - Flaw in Microsoft VM Could Enable System Compromise
>> <http://www.net-security.org/advisory.php?id=1385>

CERT Advisory CA-2002-35 - Vulnerability in RaQ 4 Servers
>> <http://www.net-security.org/advisory.php?id=1384>

SCO Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0: uuencode performs inadequate checks on user-specified output files
>> <http://www.net-security.org/advisory.php?id=1383>

Debian Security Advisory - New tetex-lib packages fix arbitrary command execution
>> <http://www.net-security.org/advisory.php?id=1382>

Cisco Security Advisory - OSM Line Card Header Corruption Vulnerability
>> <http://www.net-security.org/advisory.php?id=1381>

SCO Security Advisory - Linux: buffer overflow in nss_ldap DNS SRV
>> <http://www.net-security.org/advisory.php?id=1380>

Debian Security Advisory - tcpdump BGP decoding error
>> <http://www.net-security.org/advisory.php?id=1379>

Debian Security Advisory - gtetrinet buffer overflows
>> <http://www.net-security.org/advisory.php?id=1378>

Mandrake Linux Security Advisory - python (update)
>> <http://www.net-security.org/advisory.php?id=1377>

Red Hat Security Advisory - Updated Canna packages
fix vulnerabilities
>> <http://www.net-security.org/advisory.php?id=1376>

Red Hat Security Advisory - Updated wget packages fix
directory traversal bug
>> <http://www.net-security.org/advisory.php?id=1375>

SCO Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0:
closed file descriptor race vulnerability
>> <http://www.net-security.org/advisory.php?id=1374>

Microsoft Security Bulletin MS02-068 - Cumulative Patch
for Internet Explorer (Revised)
>> <http://www.net-security.org/advisory.php?id=1373>

SCO Security Advisory - Linux: groff pic buffer overflow
>> <http://www.net-security.org/advisory.php?id=1372>

Debian Security Advisory - New IM packages correct
hidden architecture dependency
>> <http://www.net-security.org/advisory.php?id=1371>

Debian Security Advisory - New html2ps packages correct
fix against arbitrary code execution
>> <http://www.net-security.org/advisory.php?id=1370>

[Featured articles]

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

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

NAI SECURES HIGH-SPEED WIRELESS NETWORKS WITH SNIFFER WIRELESS
Network Associates announced new security and management for high-speed wireless networks through its Sniffer Wireless solution.
>> <http://www.net-security.org/article.php?id=296>

WORLDCOM ANNOUNCES THEIR ANTI-SPAM SOLUTION
The WorldCom Internet Managed Scanning Service is an anti-spam service that enables customers to effectively counteract the costs and lost productivity incurred by unsolicited emails.
>> <http://www.net-security.org/article.php?id=297>

EEYE DIGITAL SECURITY RAISES ADDITIONAL \$9 MILLION
eEye Digital Security announced that they have raised \$9 million in the Series C financing round.
>> <http://www.net-security.org/article.php?id=298>

NCIPHER SECURES WEB SERVICES
nCipher announced a strategy that aligns its hardware-based encryption products as a basis for securing XML-based applications and Web Services.
>> <http://www.net-security.org/article.php?id=299>

NEW GENERATION OF SME VPN FIREWALL PRODUCTS
SnapGear Inc. has augmented their VPN Firewall gateway lineup with new security products developed expressly for the small medium enterprise marketplace.
>> <http://www.net-security.org/article.php?id=300>

RSA CONFERENCE 2003 DETAILS
Organizers of the RSA Conference, the world's leading e-security event, unveiled the educational program for RSA Conference 2003, which will be held April 13-17 at San Francisco's Moscone Center.
>> <http://www.net-security.org/article.php?id=301>

NEW VERSION OF WEBWASHER CLASSIC RELEASED
Following the success of WebWasher Enterprise Edition and Protected Gateway editions, Germany based webwasher.com AG, announced the new version of WebWasher Classic.
>> <http://www.net-security.org/article.php?id=302>

TRANSPARENT DOCUMENT SECURITY FOR MICROSOFT OFFICE LAUNCHED
Adhaero Technologies, released Adhaero Doc - a comprehensive

solution that encrypts and controls the use of Microsoft Office documents and emails.

>> <http://www.net-security.org/article.php?id=303>

SECURIFY ANNOUNCES SECVANTAGE ENTERPRISE REPORTING

Securify, Inc., developers of SecurVantage automated security system, announced the addition of rich reporting functionality into their flagship product.

>> <http://www.net-security.org/article.php?id=304>

NOVELL RELEASES A NEW UDDI SERVER

Novell announced the availability of a new Universal Description, Discovery and Integration server that adds secure identity management to the UDDI standard.

>> <http://www.net-security.org/article.php?id=305>

MICROSOFT RELEASES THREE MORE SECURITY BULLETINS

In yet another combo pack, Microsoft released 3 security bulletins. The bulletins which are labeled from moderate to critical, deal with Microsoft VM, Windows 2000, XP and NT 4 security problems.

>> <http://www.net-security.org/article.php?id=306>

PROTECT YOUR MACINTOSH WITH MACSCAN

SecureMac.com announced the release of their first security application to protect the Macintosh from spyware and applications that could offer remote access when improperly configured.

>> <http://www.net-security.org/article.php?id=307>

ARRAY NETWORKS DELIVERS NETWORK TRAFFIC ANALYSIS

Array Networks announced the new Array SR Series, the first wire-speed network traffic analyzer designed to detect potential security breaches and network abuse across TCP/IP-based protocols.

>> <http://www.net-security.org/article.php?id=308>

[Security world]

All press releases are located at:

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

Infonetics VPN/Firewall Market Report: NetScreen Leads in Revenue Growth for Q3 2002

>> <http://www.net-security.org/press.php?id=1164>

GFI Launches LANguard S.I.M. - New Freeware Entry Level IDS

>> <http://www.net-security.org/press.php?id=1163>

Serco Justice New Authorized Reseller Of Locksteps Leading
Web Site Protection Solutions
>> <http://www.net-security.org/press.php?id=1162>

nCipher First Hardware Security Vendor to Deliver Enhanced
Security and Performance to Secure Web Services
>> <http://www.net-security.org/press.php?id=1161>

Sophos Secures Anti-Virus Protection for Aviva
>> <http://www.net-security.org/press.php?id=1160>

Skanska Orders Comprehensive Security Solution for 8,500
Workplaces from Utimaco Safeware
>> <http://www.net-security.org/press.php?id=1159>

Kaspersky Anti-Hacker - Optimal Protection For Your Home PC
>> <http://www.net-security.org/press.php?id=1158>

Chrysalis-ITS Awarded World's First Common Criteria
Certification For A Hardware Security Module
>> <http://www.net-security.org/press.php?id=1157>

Sophos And CipherTrust Secure Specsavers' Email Systems
>> <http://www.net-security.org/press.php?id=1156>

PureEdge Solutions Appoints Software Industry Veteran as New CEO
>> <http://www.net-security.org/press.php?id=1155>

[**Featured Review**]

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

PANDA ANTIVIRUS TITANIUM
This is an anti virus product meant for home users. Lately, it has
been recognized in several computer magazines as being one of
the be best AV solutions out there. Read more to see it in action.
>> <http://www.net-security.org/review.php?id=19>

[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

HORATIO 1.0 (Linux)

The Horatio system is a firewall authentication tool.

>> <http://www.net-security.org/software.php?id=395>

SPYWAREBLASTER 1.1 (Windows)

SpywareBlaster doesn't scan and clean for spyware - it prevents it from ever being installed.

>> <http://www.net-security.org/software.php?id=396>

LockIt 1.0 (Windows)

This program locks a Windows 2000, XP based workstation.

LockIt is written in MASM and does nothing but call the LockWorkStation API call.

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

SNMP NETWORK AUDITOR 0.1 (Linux)

SNMP Network Auditor is a small collection of Perl scripts that can be used to scan an arbitrary set of networks, defined in a configuration file, and identify any nodes which are running an SNMP service on a user-specified UDP port (default 161) with a user-specified community string (default public).

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

PERL ADVANCED TCP HIJACKING 0.5 (Linux)

Perl Advanced TCP Hijacking is a collection of tools for inspecting and hijacking TCP connections written in Perl.

>> <http://www.net-security.org/software.php?id=399>

FILEGUARDIAN 1.0.1 (Windows)

FileGuardian is an safe and easy to use file encryption utility.

Simply drag and drop files to quickly protect your sensitive files from unwanted viewing.

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

WIREKISMET 1.0.1 (Linux)

WireKisnet is a small GTK frontend for Kismet that was written for the iPaq.

>> <http://www.net-security.org/software.php?id=401>

SNIFFDET 0.7 (Linux)

Sniffdet is an OpenSource implementation of a set of tests

for remote sniffers detection in TCP/IP network environments.
>> <http://www.net-security.org/software.php?id=402>

YAFIC 1.1 (Linux)

Yafic is Yet Another File Integrity Checker. It saves information about the state of a filesystem to a database, which later can be used to compare against the current state of the filesystem, letting you know of any changed, added, or removed files.
>> <http://www.net-security.org/software.php?id=403>

CRAMPASS 1.0.1 (Linux)

Crampass is a CRAM MD5 password file update tool which is useful with the WU IMAP and POP3 daemons. It allows users to update the stored password without root intervention.
>> <http://www.net-security.org/software.php?id=404>

[Virus News]

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

Weekly Virus Report - Pursue and CrackBox Trojans, Prestige Worm
>> http://www.net-security.org/virus_news.php?id=143

New "Prestige" Worm Uses Social Engineering
>> http://www.net-security.org/virus_news.php?id=142

Holiday Offer from BitDefender
>> http://www.net-security.org/virus_news.php?id=141

Sophos Anti-Virus Receives West Coast Checkmark
>> http://www.net-security.org/virus_news.php?id=140

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

Strengthening Network Security: FREE Guide

Network security is a constantly moving target - even proven
solutions lose their punch over time.

Find out how to get COMPLETE PROTECTION against ever-growing
security threats with our FREE new Guide.

Get your copy today at
https://www.qualys.com/forms/nsguideh_442.php
