



Newsletter  
Issue 117 - 01.07.2002  
<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>.

=====

SPI Dynamics ALERT:  
Learn how to outsmart the Top 14 Web Application hacks!

=====

ALERT: Test and assess your Web Applications TODAY! Hackers exploiting Web applications gain entry to backend data via Port 80 and 443! Firewalls and IDS don't stop these attacks because hackers using the Web App Layer are NOT seen as intruders.

Are you vulnerable? 15-Day \*Free\* Trial! Download now!  
<http://www.spidynamics.com/mktg/freewebinspect5>

=====

Table of contents:

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

[ General security news ]

-----

#### INTERVIEW WITH JORDAN HUBBARD

KernelTrap has spoken with guru Jordan Hubbard, one of the creators of FreeBSD and currently a manager of Apple's Darwin project.

>> <http://www.net-security.org/news.php?id=444>

#### MORE "SECURITY" FROM MICROSOFT

A first look at Microsoft's plan to remake the personal computer to ensure security, privacy and intellectual property rights. Will you buy it?

>> <http://www.net-security.org/news.php?id=445>

#### POLICE IN CORPORATE HACKER CRACKDOWN

Police have doubled the size of Greater Manchester force's

computer crime unit in a bid to crack down on hackers whose security breaches have pushed some firms to the brink of closure.  
>> <http://www.net-security.org/news.php?id=446>

**USERS QUESTION JPEG VIRUS, MCAFEE STANDS FIRM**  
Users and antivirus vendors are questioning the seriousness of a virus announced last week by McAfee Security, as well as the manner in which McAfee doled out details about the virus.  
>> <http://www.net-security.org/news.php?id=447>

**HACKERS ATTEMPT TO BREAK INTO RUSSIAN PRESIDENT'S SITE**  
Over the first three hours of operation of the new Presidential site, several dozen attempts were made to break into the Internet-page of the head of state.  
>> <http://www.net-security.org/news.php?id=448>

**USING OPENLDAP FOR AUTHENTICATION**  
This article describes how to use LDAP to authenticate system logins using pam\_ldap and nss\_ldap for a centralized authentication system for a LAN.  
>> <http://www.net-security.org/news.php?id=449>

**DEVELOPERS WORRY WEB TOO CONTROLLED**  
The Internet's potential for promoting expression and empowering citizens is under threat from corporate and government policies that clash with the medium's long-standing culture of openness.  
>> <http://www.net-security.org/news.php?id=450>

**WARNING OVER PASSWORD SECURITY**  
Computer users are being urged to change their passwords regularly to avoid becoming a victim of internet fraud.  
>> <http://www.net-security.org/news.php?id=451>

**MIND GAMES - SOCIAL ENGINEERING**  
This small article is a brief overview on social engineering. It talks a bit about the psychology of social engineering, the security threat it imposes and about the methods used for it.  
>> <http://www.net-security.org/news.php?id=454>

**MITNICK TESTIFIES AGAINST SPRINT IN VICE HACK CASE**  
The ex-hacker details his past control of Las Vegas' telecom network, and raids his old storage locker to produce the evidence.  
>> <http://www.net-security.org/news.php?id=455>

**SPEAK UP FOR SECURITY**  
If plans by Optus and an Irish technology company work out, Australians will soon be able to "sign" their transactions with their voices.  
>> <http://www.net-security.org/news.php?id=456>

**LOTUS TO INCLUDE NEW ANTISPAM TOOLS IN NOTES R6**  
Lotus said the upcoming version of its Notes e-mail software will have server-side antispam tools, which aren't as sophisticated as some sold as add-ons by third-party vendors.  
>> <http://www.net-security.org/news.php?id=457>

**ALL EYES ARE ON YOU**  
Tollbooths, ATMs, doctors' offices, online chat: You leave critical personal data behind wherever you go. Let's follow one American as he scatters his digital DNA.  
>> <http://www.net-security.org/news.php?id=458>

**CD PIRATES IN FROM THE COLD**  
Australia plans to endorse CD-copying kiosks in a controversial world-first plan that legalises music piracy.  
>> <http://www.net-security.org/news.php?id=459>

**FAST MODEMS A HACKER'S HEAVEN**  
Thousands of broadband internet modems are being installed with default passwords, making them vulnerable to hackers who can use them to surf the net at the owners' expense.  
>> <http://www.net-security.org/news.php?id=460>

**SECURITY MESSAGES POSTED ON THE NET**  
Secret radio conversations between security guards minding royals and government ministers are being intercepted and posted on the internet by an amateur enthusiast, the BBC claimed today.  
>> <http://www.net-security.org/news.php?id=461>

**MANAGED SERVICES UNDERMINE SECURITY THREAT**  
The need for holistic security management is crucial - the scale of compromised systems around the world has reached unprecedented heights.  
>> <http://www.net-security.org/news.php?id=462>

**SOFTWARE LETS USERS MANAGE OWN PASSWORDS**  
Avatier Corp. is shipping a password reset application - Password Station.NET 2.0 - built on Microsoft's .NET technology.  
>> <http://www.net-security.org/news.php?id=463>

**DOD WILL TEST BIOMETRICS TO SECURE ITS SMART CARDS**  
The Defense Department's Biometrics Fusion Center will begin testing software on four types of biometric devices for use on its Common Access smart cards.  
>> <http://www.net-security.org/news.php?id=464>

**STAY SECURE ON THE ROAD**  
A secure method to retrieve and send email is essential and mail2web.com offers some convenient security features not typically available.  
>> <http://www.net-security.org/news.php?id=465>

#### A FLAWED RANDOM-NUMBER THEORY

There's a privacy-protection scheme that aims to eliminate the need for aliases. But it's not as comprehensive as it appears.

>> <http://www.net-security.org/news.php?id=466>

#### WIRELESS SECURITY IN THIS MODERN WORLD

This article discusses the technological advances since WEP, the brief steps you can take in either wireless or wired and why security is such a big deal.

>> <http://www.net-security.org/news.php?id=467>

#### BUGGY SOFTWARE COSTS USERS, VENDORS NEARLY \$60B ANNUALLY

The federal study also found that better testing could reduce the cost by \$22.5 billion, though it wouldn't eliminate all software errors.

>> <http://www.net-security.org/news.php?id=468>

#### RUSSIAN MOB INFILTRATES UNIVERSITY COMPUTERS

The government has issued an alert about identity and credit card theft on U.S. campuses, saying individuals linked to the Russian mob tried to tap into at least five college computer systems.

>> <http://www.net-security.org/news.php?id=469>

#### EUROPEAN WEBSITES FACE HIJACK RISK

A "worrying" number of European websites could be at risk from hijack due to inherent security glitches in the Ripe internet address databasing system.

>> <http://www.net-security.org/news.php?id=470>

#### SECURITY OVERVIEW? READ INTERNET LOCKDOWN

Internet Lockdown may be too general for some, but it is a valuable and clear overview of the topic of security administration. Its user friendly, nonbureaucratic language is one of the book's strengths.

>> <http://www.net-security.org/news.php?id=471>

#### CRITICS TAKE AIM AT NEW FILTERING SERVICE

New filtering software has found favor with some of the Internet's most popular portals, but developers of commercial filtering products question the value of the system's voluntary approach.

>> <http://www.net-security.org/news.php?id=473>

#### "MOD CHIP" FOR HACKING XBOX DISCONTINUED

One of the companies making Xbox "mod chips" has gone out of business, possibly because of legal pressure from Microsoft.

>> <http://www.net-security.org/news.php?id=474>

#### INTERNAL IT STAFF POSE SECURITY RISK

Internal IT staff should not be involved in the development of anti-fraud systems, consultants Detica has warned.

>> <http://www.net-security.org/news.php?id=475>

#### U.S. FEARS AL QAEDA CYBER ATTACKS

Ron Ross, who heads an "information assurance" partnership between the NSA and the NIST said: "It's not science fiction. A cyberattack can be launched with fairly limited resources."  
>> <http://www.net-security.org/news.php?id=476>

#### LINUX: FEELIN' SECURE

IT pros navigating a minefield of insecure software and systems are finding safe ground in Linux. That's because Linux has become a model of security.  
>> <http://www.net-security.org/news.php?id=477>

#### LAWMAKER TRIES TO FOIL ILLEGAL FILE-SHARING

Copyright holders would receive carte blanche to use aggressive tactics to stop the illegal distribution of their works on online services under legislation outlined by Rep. Howard Berman.  
>> <http://www.net-security.org/news.php?id=478>

#### WEB SITE EXPOSES CREDIT CARD FRAUD

An anti-fraud education group called CardCops has opened a Web site that will let Americans check to see if their card numbers are in the hands of thieves.  
>> <http://www.net-security.org/news.php?id=479>

#### OPENSSSL: THE CRYPTOGRAPHY LEGO SET

Anne Carasik uses a Lego analogy to discuss cryptography tools and digital certificates.  
>> <http://www.net-security.org/news.php?id=480>

#### SECURITY AND OPEN SOURCE

Security problems in software are an extremely bad thing, regardless of the business model under which the software was written.  
>> <http://www.net-security.org/article.php?id=139>

#### SUN SIGNS UP TO RIVALS' SECURITY STANDARDS

A security specification for Web services submitted by Microsoft, IBM and VeriSign has won the backing of rival Sun.  
>> <http://www.net-security.org/news.php?id=484>

#### NETWORK AMERICA: WIRELESS SECURITY? READ IT AND WEP

Some guys think it's cool to drive around the San Francisco financial district with computers in the back seat, sucking down emails and web pages that fly over poorly-secured wireless networks.  
>> <http://www.net-security.org/news.php?id=485>

#### POLAND HUNTS HACKER WHO PENETRATED NASA

Polish prosecutors are searching for a computer hacker believed by the US to have penetrated the NASA space agency, causing damage reportedly estimated at \$1 million.  
>> <http://www.net-security.org/news.php?id=486>

**BUG WATCH: DEVELOPERS AT FAULT**

Gunter Ollmann, manager of X-Force Security Assessment Services at Internet Security Systems, looks at the security issues faced by web application developers.

>> <http://www.net-security.org/news.php?id=487>

**IRRESPONSIBLE DISCLOSURE**

Internet Security Systems violated community standards and common sense with its surprise Apache bug announcement.

>> <http://www.net-security.org/news.php?id=488>

**SEARCHES BY POLICE, FBI TARGET BANDITS OF BANDWIDTH**

Authorities investigating the theft of high-speed Internet cable service yesterday seized modems and other computer equipment from homes in Toledo and surrounding suburbs.

>> <http://www.net-security.org/news.php?id=489>

**MICROSOFT SECURITY: WILL IT BE DIFFERENT THIS TIME?**

Microsoft wants to redesign the computer so it will have built-in security and privacy functions, including some etched onto special chips.

>> <http://www.net-security.org/news.php?id=490>

**CHANGE MY PASSWORD AGAIN?**

Sex, Drugs, Money...How many of these words are common passwords on your network? The answer is probably too many.

>> <http://www.net-security.org/news.php?id=491>

**ANALYZING SELECTED NETWORK ATTACKS**

Michael Pichler analyzes some interesting network attacks, explains how they work, and shows how some features included in your own software can actually be turned against you.

>> <http://www.net-security.org/news.php?id=492>

-----  
=====  
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)

---

Format String Vulnerability in decfingerd 0.7  
>> <http://www.net-security.org/vuln.php?id=1819>

Remote Buffer Overflow in Resolver Code of libc  
>> <http://www.net-security.org/vuln.php?id=1818>

OpenSSH Remote Challenge Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1817>

PHPsquidpass Unauthorized User Deleting  
>> <http://www.net-security.org/vuln.php?id=1816>

Netware FTP Server Denial of Service Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1815>

Caucho Resin Path Disclosure Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1814>

AdvServer Denial of Service Vulnerability  
>> <http://www.net-security.org/vuln.php?id=1813>

Pirch 98 Link Handling Buffer Overflow  
>> <http://www.net-security.org/vuln.php?id=1812>

Commentary: ISS Apache Advisory Response  
>> <http://www.net-security.org/vuln.php?id=1811>

---

[ Advisories ]

All advisories are located at:

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

---

Microsoft Security Bulletin MS02-033 - Unchecked Buffer in Profile Service Could Allow Code Execution in Commerce Server

>> <http://www.net-security.org/advisory.php?id=810>

Microsoft Security Bulletin MS02-032 - Cumulative Patch for Windows Media Player

>> <http://www.net-security.org/advisory.php?id=809>

Mandrake Linux Security Advisory - openssh

>> <http://www.net-security.org/advisory.php?id=808>

Debian Security Advisory - ssh (update 2)

>> <http://www.net-security.org/advisory.php?id=807>

Debian Security Advisory - ssh (update 1)

>> <http://www.net-security.org/advisory.php?id=806>

Debian Security Advisory - ssh

>> <http://www.net-security.org/advisory.php?id=805>

Conectiva Linux Security Advisory - openssh

>> <http://www.net-security.org/advisory.php?id=804>

SuSE Security Announcement - openssh

>> <http://www.net-security.org/advisory.php?id=803>

EnGarde Secure Linux Advisory - openssh introduce privilege separation into sshd

>> <http://www.net-security.org/advisory.php?id=802>

Caldera Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0: dtprintinfo buffer overflow with Help search

>> <http://www.net-security.org/advisory.php?id=801>

Caldera Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0: in.rarpd format string vulnerability in error() and syserr()

>> <http://www.net-security.org/advisory.php?id=800>

SGI Security Advisory - pmpost vulnerability

>> <http://www.net-security.org/advisory.php?id=799>

SGI Security Advisory - neventd vulnerability (update)  
>> <http://www.net-security.org/advisory.php?id=798>

SGI Security Advisory - neventd vulnerability  
>> <http://www.net-security.org/advisory.php?id=797>

Debian Security Advisory - apache-perl  
>> <http://www.net-security.org/advisory.php?id=796>

Conectiva Linux Security Advisory - ImageMagick  
>> <http://www.net-security.org/advisory.php?id=795>

Caldera Security Advisory - Linux: Apache Web Server Chunk Handling Vulnerability  
>> <http://www.net-security.org/advisory.php?id=794>

Red Hat Security Advisory - Updated Apache packages fix chunked encoding issue  
>> <http://www.net-security.org/advisory.php?id=793>

Mandrake Linux Security Advisory - apache (revised #2)  
>> <http://www.net-security.org/advisory.php?id=792>

Mandrake Linux Security Advisory - apache (revised)  
>> <http://www.net-security.org/advisory.php?id=791>

Mandrake Linux Security Advisory - apache  
>> <http://www.net-security.org/advisory.php?id=790>

---

[ Virus News ]

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

---

GameSpy Arcade Linked on Download.com Infected With Nimda  
>> [http://www.net-security.org/virus\\_news.php?id=38](http://www.net-security.org/virus_news.php?id=38)

The Internet, Application Vulnerabilities and Viruses:  
A Deadly Combination  
>> [http://www.net-security.org/virus\\_news.php?id=37](http://www.net-security.org/virus_news.php?id=37)

Yaha-E Worm Spreading in the Wild  
>> [http://www.net-security.org/virus\\_news.php?id=36](http://www.net-security.org/virus_news.php?id=36)

[ Security world ]

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

---

NBG Selects neuSECURE, Security Event Management Software For  
Resale To The Fortune 2000

>> <http://www.net-security.org/press.php?id=870>

RSA Security Announces Web Access Management Support for  
BEA WebLogic Platform 7.0

>> <http://www.net-security.org/press.php?id=869>

ADC Shuts Down Viruses From the Desktop to the Gateway With  
Trend Micro OfficeScan and ScanMail

>> <http://www.net-security.org/press.php?id=868>

GFI Combines McAfee Anti-Virus Technology from Network Associates  
with GFI MailSecurity

>> <http://www.net-security.org/press.php?id=867>

McAfee.com to Announce Second Quarter 2002 Operating Results

>> <http://www.net-security.org/press.php?id=866>

EMS Global Ltd teams up with iPass to deploy Secure Global Internet  
Connectivity for UK and Irish Corporations

>> <http://www.net-security.org/press.php?id=865>

Utimaco Safeware and Datakey Partner to Integrate High-Profile  
Smart Card Solutions and PKI

>> <http://www.net-security.org/press.php?id=864>

RSA ClearTrust Web Access Management Supports Leading Data  
Stores to Allow for Better Data Utilization, Efficiency

>> <http://www.net-security.org/press.php?id=863>

Entercept Introduces Elite Security Squad - The Ricochet Team

>> <http://www.net-security.org/press.php?id=862>

French Overseas Public Radio-And-TV Network Taps CA's Unicenter  
And eTrust To Ensure Non-Stop Operations

>> <http://www.net-security.org/press.php?id=861>

Check Point CEO Gil Shwed Receives Prestigious Academy of  
Achievement Award

>> <http://www.net-security.org/press.php?id=860>

V-ONE Announces High Performance VPN Solution for VSAT & Satellite Data Networks

>> <http://www.net-security.org/press.php?id=859>

Trusecure Security Assurance Services Address Information Risk Management For The Utility And Energy Industries

>> <http://www.net-security.org/press.php?id=858>

---

[ Featured articles ]

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)

---

#### VIOLATING DATABASE - ENFORCED SECURITY MECHANISMS

This paper discusses the feasibility of violating the access control, authentication and audit mechanisms of a running process in the Windows server operating systems.

>> <http://www.net-security.org/article.php?id=140>

#### SECURITY AND OPEN SOURCE

Security problems in software are of course an extremely bad thing, regardless of the business model under which the software was written. I want to consider why anybody thinks that the business model matters, and whether there is evidence that it does. I shall also look somewhat to the future.

>> <http://www.net-security.org/article.php?id=139>

#### OPENSSSH REMOTE VULNERABILITY ROUNDUP

Stuff updated in the roundup includes: Debian, Conectiva, Red Hat, NetBSD, Trustix, Cisco, Caldera and CERT security advisories, SUN commentary and OpenBSD 3.1 sshd remote root exploit.

>> <http://www.net-security.org/article.php?id=138>

#### SECURITY: SOURCE ACCESS AND THE SOFTWARE ECOSYSTEM

The goal of this paper is to explore the relationship between the security of software and the model under which that software was produced and distributed.

>> <http://www.net-security.org/article.php?id=137>

---

## [ 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=2](http://net-security.org/software_main.php?cat=2)

---

### APPCAP

Appcap is a tricky application for x86 Linux which allows an user with enough power (usually the superuser) on a machine to attach and redirect standard input and output of any application to his actual tty.

>> <http://www.net-security.org/software.php?id=166>

### PANDORA 1.8.0.306

Pandora Automatic Scanner is fully automatic multi-thread netbios scanner. It can scan "B" class networks (more than 65000 hosts) for shared resources. It can automatically download files from each shared disk, brute force passwords for closed shares, send logs, downloaded files to e-mail, and more.

>> <http://www.net-security.org/software.php?id=167>

### SUNGAZER PACKETFILTER 0.2.2

The SunGazer Packetfilter is a small and simple tool to set up firewall rules. It works with iptables and is easy to use and configure.

>> <http://www.net-security.org/software.php?id=168>

### ANGRY IP SCANNER 2.06

Angry IP scanner is a very fast IP scanner for Windows. It can scan IPs in any range, even 1.1.1.1 to 255.255.255.255. Its binary file size is very small compared to other IP scanners.

>> <http://www.net-security.org/software.php?id=169>

### PACE CHECK 1.0

Pace Check is a utility that searches through system logs and finds cases where someone has tried to gain access to your server (non-legit), then it saves them to a log, mails them to you, or sends them to stdout. It supports HTTP, FTP, and others.

>> <http://www.net-security.org/software.php?id=170>

### VLAD THE SCANNER 0.9.2

VLAD the Scanner is an open-source security scanner that checks for the SANS Top Ten security vulnerabilities commonly found to be the source of a system compromise. It has been tested on Linux, OpenBSD, and FreeBSD. It requires several Perl modules to run.

>> <http://www.net-security.org/software.php?id=171>

### PASSWORD SAFE 1.9.0

Password Safe is a password database utility. Users can keep their

passwords securely encrypted on their computers. A single Safe Combination unlocks them all.

>> <http://www.net-security.org/software.php?id=172>

#### BESTCRYPT 7.07

BestCrypt data encryption systems bring military strength encryption to the ordinary computer user without the complexities normally associated with strong data encryption.

>> <http://www.net-security.org/software.php?id=173>

#### W32.NIMDA.E@MM REMOVAL TOOL

This tool is designed to remove infections of W32.Nimda.E@mm.

>> <http://www.net-security.org/software.php?id=174>

#### W32.NIMDA.A@MM REMOVAL TOOL

This is a fixtool to remove infections of W32.Nimda.A@mm.

<http://www.net-security.org/software.php?id=175>

#### ANTINIMDA

This is a removal tool for the Nimda virus.

<http://www.net-security.org/software.php?id=176>

#### QUICKWIPER 7.4.1

QuickWiper is a file wipe utility with system cleaner. Windows deletion is not secure enough. When you delete files in Windows by moving them into the Recycle Bin all the data remain on your hard disk.

>> <http://www.net-security.org/software.php?id=177>

#### SMOKEPING 1.12

With SmokePing you can measure latency, latency distribution and packet loss in your network. SmokePing uses RRDtool to maintain a longterm datastore and to draw pretty graphs giving up to the minute information on the state of each network connection.

>> <http://www.net-security.org/software.php?id=178>

-----  
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](http://www.net-security.org/newsletter_archive.php)