



Newsletter
Issue 116 - 24.06.2002
<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>.

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>

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]

TIME TO SMARTEN UP ABOUT SECURITY

You'd think we would have learned some important lessons about security when WEP was broken last year by products like AirSnort. Unfortunately, we did not.
>> <http://www.net-security.org/news.php?id=393>

IBM SOFTWARE AIMS TO SHUT DOWN "DRIVE-BY HACKING"

IBM announced a technology designed to close some of the holes in corporate wireless networks and prevent outsiders from stealing data through drive-by hacking.
>> <http://www.net-security.org/news.php?id=394>

FORUM SYSTEMS AIMS AT XML SECURITY SPACE

Forum Systems Inc. becomes one of the first entrants into the emerging XML security space with its Forum Sentry appliance.
>> <http://www.net-security.org/news.php?id=395>

DON'T FIGHT SECURITY CANCERS WITH ASPIRIN

When it comes to security, we have met the enemy and it is

most definitely us.

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

FOXNEWS.COM, OTHER SITES ATTACKED

Foxnews.com and a number of other web sites came under an apparent DoS attack, which disrupted service to hundreds of thousands of Internet users.

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

SAMPLE FIREWALL GENERATOR

Citadec Solutions Ky has a sample firewall generator at their website, give it a try.

>> <http://www.citadec.com/FirewallGenerator.html>

INTERNET LAW & POLICY FORUM CONFERENCE 2002

This year, the ILPF Conference will focus on the timely subjects of security and privacy, exploring the different legal and regulatory regimes adopted around the world.

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

HOTTEST HARDWARE FOR WI-FI SECURITY

"If you're an enterprise, you're going to be locked into the wireless cards and the access points of one vendor," Gartner analyst Bill Clark told Wireless NewsFactor.

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

IM'ERS GET A SECURE CHAT ROOM

Instant messaging is about as private as two people talking on the train; you never know who's listening. Encryption could change that. Of course, that might not be good news to those fighting the evildoers.

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

IT INTEGRATION KEY TO U.S. SECURITY

The success of the proposed Department of Homeland Security hinges on IT systems integration, security experts said last week.

>> <http://www.net-security.org/news.php?id=403>

CISCO AUGMENTS WIRELESS LAN SECURITY

Cisco Systems Inc. addressed the security of wireless LANs with a new add-on product to complement its offerings in this area.

>> <http://www.net-security.org/news.php?id=404>

SECURITY WARNING TOO QUICK FOR COMFORT?

Internet Security Systems faced criticism after it released critical security information without giving the open-source community adequate time to respond.

>> <http://www.net-security.org/news.php?id=405>

EARTHLINK'S PASSWORDS ARE NAKED

EarthLink's practice of allowing service reps to see customers'

passwords could be exposing subscribers to a range of security threats.

>> <http://www.net-security.org/news.php?id=406>

HACKERS DO NOT BREAK, THEY BUILD

In the pursuit of advanced systems knowledge, hackers might indeed penetrate systems, but they're not interested primarily in breaking into a system for its own sake.

>> <http://www.net-security.org/news.php?id=407>

2600 IRC SERVER OFFLINE INDEFINITELY

As a result of a massive Denial of Service attack of biblical proportions, irc.2600.net does not have a home anymore.

>> <http://www.net-security.org/news.php?id=408>

BOY OF 17 HACKS INTO MISSILE SECRETS

The Pentagon has had its second major intelligence embarrassment in a week after a teenager in Austria hacked into secret plans, including the location of US nuclear missiles.

>> <http://www.net-security.org/news.php?id=409>

FILTERING E-MAIL WITH POSTFIX AND PROCMail, PART ONE

This series will examine the use of Postfix and Procmail to eliminate spam before it hits the client.

>> <http://www.net-security.org/news.php?id=410>

APACHE CHUNK HANDLING ROUNDUP

There are various problems regarding Apache in the news today. Here is a roundup of all the reported problems with the, so far, available solutions and patches.

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

NIGERIA HOAX SPAWNS COPYCATS

The Nigerian bank account scam, one of the best-known e-mail frauds, is taking on new forms. Recent versions involve a U.S. commando and a World Trade Center survivor, among others.

>> <http://www.net-security.org/news.php?id=412>

'MOD' SQUAD HACKS AWAY AT XBOX

Soldered into an Xbox, another 'mod chip' lets owners hack into their console to play pirated games and run PC software.

Microsoft is now considering a crackdown.

>> <http://www.net-security.org/news.php?id=413>

SECURE CONTENT SOFTWARE MARKET GROWS AT A LICK

Market forecast data compiled by International Data Corp Inc indicates that the worldwide secure content management market will reach a level of \$4.2bn by 2005, growing at an annual clip of 20%.

>> <http://www.net-security.org/news.php?id=414>

SLACKWARE 8.1 IS RELEASED

Highlights of this release include KDE 3.0.1, GNOME 1.4.1, Mozilla 1.0, support for many new filesystems like ext3, ReiserFS, JFS, and XFS, and support for several new SCSI and ATA RAID controllers.

>> <http://www.net-security.org/news.php?id=415>

ARMY WEBSITES EXPOSE SECURITY DATA

US Army websites have been criticised for publishing potentially sensitive information that could be of use to terrorists.

>> <http://www.net-security.org/news.php?id=416>

PEACEFIRE GETS UNDER SKIN OF ANTI-PORN FILTERERS

Internet activist Bennett Haselton has made a name for himself by helping minors disable filtering programs designed to block Web sites that their parents deem offensive or pornographic.

>> <http://www.net-security.org/news.php?id=417>

REPORT: VIRUSES SPREADING ON THE DOUBLE

The first half of 2002 has seen worms infect PCs at twice the rate they did last year, says security company MessageLabs. And they're more malicious too.

>> <http://www.net-security.org/news.php?id=418>

HACKING'S NOT JUST FOR GEEKS

Blended security threats are increasing, meaning that chief information officers have more to worry about than just hackers.

>> <http://www.net-security.org/news.php?id=419>

PRO-ISLAMIC HACKERS JOIN FORCES

There is mounting evidence that individual hacker groups connected by a pro-Islamic agenda are working together to carry out hack attacks, say experts.

>> <http://www.net-security.org/news.php?id=420>

CENSOR SECRECY OKAY: TRIBUNAL

Electronic Frontiers Australia had requested access under the Freedom of Information Act to a number of Australian Broadcasting Authority documents relating to censored websites.

>> <http://www.net-security.org/news.php?id=422>

UPDATE ON APACHE CHUNK HANDLING VULNERABILITY

A few security advisories (SGI, EnGarde Secure Linux and Debian Linux related) were released regarding the problems with Apache chunk handling.

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

SECURITY TOOLS TAKE AIM AT NETWORK THREATS

Tools designed to prevent and combat damaging attacks on enterprise networks took the spotlight here at the NetSec 2002 Computer Security Conference.

>> <http://www.net-security.org/news.php?id=424>

EXPERTS WARN OF CYBER SECURITY HOLES

At a town hall meeting on cyber security, experts warned that the risks of going online have become especially prevalent as hackers find new ways to poke holes in Internet security systems.

>> <http://www.net-security.org/news.php?id=425>

THE INTERNET GETS SERIOUS

Today, the Internet is messy, dangerous ground. Viruses and system break-ins are on the rise, while vested interests battle over what isn't allowed.

>> <http://www.net-security.org/news.php?id=426>

BOOK REVIEW: ESSENTIAL CHECKPOINT FIREWALL-1

Ben Rothke checks out the latest book by Dameon Welch-Abernathy, who's known as the man for Firewall-1.

>> <http://www.net-security.org/news.php?id=427>

SECURITY MERGER GETS REDSIREN NOTICED

A black horse in the nascent managed-security business caught up with the rest of the herd, when relative unknown RedSiren announced its merger with Veridian's security subsidiary, Veritect.

>> <http://www.net-security.org/news.php?id=428>

WHITEHAT ARSENAL 2.0

This is a collection of basic tools that help security professionals test Web applications for common security vulnerabilities in the midrange of competitive pricing.

>> <http://www.net-security.org/news.php?id=429>

HOW TO PRACTICE SAFE B2B

Before swapping information with multiple e-commerce partners, it really pays to protect yourself by pushing partners to adopt better security practices.

>> <http://www.net-security.org/news.php?id=430>

GAME CONSOLES - THE NEXT HACKER TARGET?

Xbox and Playstation 2 decks are coming to the Internet in droves this fall. How will they stand up against the legions of hackers waiting for them there?

>> <http://www.net-security.org/news.php?id=431>

HACKERS AND PORN AND PIRATES, OH MY

The Business Software Alliance asked Finnish Internet service provider Jippii Group last November to remove a customer's Web site that allegedly helped others to scam bootlegged software.

>> <http://www.net-security.org/news.php?id=432>

STAFF TRAINING IS VITAL FOR SECURITY

IT departments must keep other employees aware of security, warns a leading CIO, as laziness can put businesses at risk.

>> <http://www.net-security.org/news.php?id=433>

WATCHING THE GATEKEEPERS

Industry observers are seeing pressure on systems administrators from two areas: increasing network capacities and more complex threats, both of which strain traditional security components.

>> <http://www.net-security.org/news.php?id=434>

ETHICAL HACKERS EXPOSE LEGAL FLAWS

After a training course, journalist Roger Howorth casts his eye over the world of ethical hacking.

>> <http://www.net-security.org/news.php?id=435>

STUDY: OPEN, CLOSED SOURCE EQUALLY SECURE

A scientific paper finds that, theoretically, neither closed-source nor open-source approaches improve software security.

>> <http://www.net-security.org/news.php?id=436>

U.S. ASKS ALLIES TO HELP CYBER SECURITY EFFORTS

U.S. officials seeking to tighten the security of U.S. data and financial networks are working with allies with close ties to the U.S. electronics industry to secure the networks against cyberattacks.

>> <http://www.net-security.org/news.php?id=437>

BUILDING SECURE SYSTEMS

This article provides a brief overview of some of the key issues of secure coding.

>> <http://www.net-security.org/news.php?id=438>

SECURITY FLAWS CONTINUE TO BE ISSUE FOR MICROSOFT

Critics say piggybacking new features on a CD of security patches shows Microsoft is not ready to abandon its feature-driven heritage.

>> <http://www.net-security.org/news.php?id=439>

WESTCOAST PRESENTS CUSTOMERS WITH A VIRUS

The Inquirer has received complaints that UK distributor Westcoast is bombarding its customers, friends and enemies alike with virus carrying emails.

>> <http://www.net-security.org/news.php?id=440>

SCHOOL HACKERS MAY FACE SECRET SERVICE

Students at universities in four states may have been monitored by "spyware" placed on computers by online criminals to capture passwords and credit card numbers.

>> <http://www.net-security.org/news.php?id=441>

REUTERS OFFERS MONITORED IM

Reuters Group has developed an instant messaging application for the financial services industry and will incorporate monitoring technology into the software.

>> <http://www.net-security.org/news.php?id=442>

[Vulnerabilities]

All vulnerabilities are located here:

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

IRIX rpc.xfsmd Multiple Remote Root Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=1810>

Half-life Multiplayer Management Problem

>> <http://www.net-security.org/vuln.php?id=1809>

Insecure Temporary Files in Acrobat Reader 4.05

>> <http://www.net-security.org/vuln.php?id=1808>

Xitami Web Server 2.5b4 Plaintext Administrator Password Storage

>> <http://www.net-security.org/vuln.php?id=1807>

PHP source Injection in PHPAddress

>> <http://www.net-security.org/vuln.php?id=1806>

Cisco VPN Client Local Root Vulnerability

>> <http://www.net-security.org/vuln.php?id=1805>

Apache Tomcat Path Disclosure Vulnerability

>> <http://www.net-security.org/vuln.php?id=1804>

Irssi Denial of Service Vulnerability

>> <http://www.net-security.org/vuln.php?id=1803>

Multiple Vulnerabilities in BasiliX

>> <http://www.net-security.org/vuln.php?id=1802>

Macromedia ColdFusion MX Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=1801>

4D 6.7 Web Server Buffer Overflow Vulnerability
>> <http://www.net-security.org/vuln.php?id=1800>

Metacart Readable Database Vulnerability
>> <http://www.net-security.org/vuln.php?id=1799>

WebBBS Remote Command Execution
>> <http://www.net-security.org/vuln.php?id=1798>

Commentary: Feedback on Malicious PHP Source Injection in phpBB
>> <http://www.net-security.org/vuln.php?id=1797>

Commentary: Cisco's Response to Catalyst 4000 Unicast Packets Problem
>> <http://www.net-security.org/vuln.php?id=1796>

DeepMetrix LiveStats Javascript Injection
>> <http://www.net-security.org/vuln.php?id=1795>

Mandrake 8.2 msec Security Issue
>> <http://www.net-security.org/vuln.php?id=1794>

Apache httpd: Vulnerability With Chunked Encoding
>> <http://www.net-security.org/vuln.php?id=1793>

Directory Traversal in Wolfram Research's webMathematica
>> <http://www.net-security.org/vuln.php?id=1792>

Remote Compromise Vulnerability in Apache HTTP Server
>> <http://www.net-security.org/vuln.php?id=1791>

Console Java Applications Can Leak Passphrases on Windows
>> <http://www.net-security.org/vuln.php?id=1790>

Resin Large Parameter Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=1789>

Resin view_source.jsp Arbitrary File Reading Vulnerability
>> <http://www.net-security.org/vuln.php?id=1788>

PHP Source Injection in osCommerce
>> <http://www.net-security.org/vuln.php?id=1787>

Malicious PHP Source Injection in phpBB
>> <http://www.net-security.org/vuln.php?id=1786>

Microsoft SQL Server 2000 pwdencrypt() Buffer Overflow
>> <http://www.net-security.org/vuln.php?id=1785>

Buffer Overflow in Microsoft Rasapi32.dll
>> <http://www.net-security.org/vuln.php?id=1784>

Fore/Marconi ATM Switch 'land' Vulnerability
>> <http://www.net-security.org/vuln.php?id=1783>

Zeroboard SQL Injection Vulnerability
>> <http://www.net-security.org/vuln.php?id=1782>

Cross Site Scripting in CiscoSecure ACS v3.0
>> <http://www.net-security.org/vuln.php?id=1781>

IGMP Denial of Service Vulnerability
>> <http://www.net-security.org/vuln.php?id=1780>

Cgiemail Open Relaying Vulnerability
>> <http://www.net-security.org/vuln.php?id=1779>

Lumigent Log Explorer 3.xx Buffer Overflow
>> <http://www.net-security.org/vuln.php?id=1778>

[Advisories]

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

SGI Security Advisory - xfsmd vulnerability
>> <http://www.net-security.org/advisory.php?id=789>

Trustix Security Advisory - apache
>> <http://www.net-security.org/advisory.php?id=788>

Microsoft Security Bulletin MS02-031 - Cumulative Patches
for Excel and Word for Windows
>> <http://www.net-security.org/advisory.php?id=787>

Cisco Security Advisory - Cisco ONS15454 IP TOS Bit Vulnerability
>> <http://www.net-security.org/advisory.php?id=786>

Cisco Security Advisory - Buffer Overflow in UNIX VPN Client
>> <http://www.net-security.org/advisory.php?id=785>

Debian Security Advisory - apache-ssl
>> <http://www.net-security.org/advisory.php?id=784>

Debian Security Advisory - apache (revised)
>> <http://www.net-security.org/advisory.php?id=783>

Caldera Security Advisory - Linux: dhcpd dynamic DNS
format string vulnerability
>> <http://www.net-security.org/advisory.php?id=782>

Conectiva Linux Security Advisory - apache
>> <http://www.net-security.org/advisory.php?id=781>

SuSE Security Announcement - apache
>> <http://www.net-security.org/advisory.php?id=780>

EnGarde Secure Linux Advisory - Apache chunk handling
overflow vulnerability
>> <http://www.net-security.org/advisory.php?id=779>

Debian Security Advisory - apache
>> <http://www.net-security.org/advisory.php?id=778>

Caldera Security Advisory - UnixWare 7.1.1 Open UNIX 8.0.0:
ppptalk root privilege vulnerability
>> <http://www.net-security.org/advisory.php?id=777>

SGI Security Advisory - Apache Web Server Chunk Handling
Vulnerability
>> <http://www.net-security.org/advisory.php?id=776>

CERT Advisory CA-2002-17 - Apache Web Server Chunk
Handling Vulnerability
>> <http://www.net-security.org/advisory.php?id=775>

Caldera Security Advisory - Linux: fetchmail imap message
count vulnerability
>> <http://www.net-security.org/advisory.php?id=774>

Conectiva Linux Security Advisory - openldap
>> <http://www.net-security.org/advisory.php?id=773>

Cisco Security Advisory - Cable Modem Termination System
Authentication

>> <http://www.net-security.org/advisory.php?id=772>

Microsoft Security Bulletin MS02-027 - Unchecked Buffer in Gopher Protocol Handler Can Run Code of Attacker's Choice (Version 2.0)

>> <http://www.net-security.org/advisory.php?id=771>

Compaq Security Bulletin - Compaq Insight Manager & Potential SQL Server and MSDE Security Vulnerability

>> <http://www.net-security.org/advisory.php?id=770>

Caldera Security Advisory - OpenServer 5.0.6a: squid compressed DNS answer message boundary failure

>> <http://www.net-security.org/advisory.php?id=769>

[Virus News]

All virus news are located at:

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

Computer Viruses Don't Take A Vacation

>> http://www.net-security.org/virus_news.php?id=35

Filipino Claims to be JPEG Virus Author

>> http://www.net-security.org/virus_news.php?id=34

[Security world]

All press releases are located at:

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

eEye Digital Security Offers Free Vulnerability Scanning Utility to Combat Bug in Apache Web Servers

>> <http://www.net-security.org/press.php?id=857>

Veridicom Announces Standalone Fingerprint Authentication Module

>> <http://www.net-security.org/press.php?id=856>

Data on 7000 Syngenta Notebooks Protected by Utimaco
Safeware's SafeGuard Easy
>> <http://www.net-security.org/press.php?id=855>

RSA Security Announces RSA Keon Web Server SSL Solution
to Help Protect the Privacy of Transmitted Data
>> <http://www.net-security.org/press.php?id=854>

Voice Authentication Launched to Safeguard Australian
Finance Community
>> <http://www.net-security.org/press.php?id=853>

Kyberpass Teams with IBM to Deliver Trusted e-Payments
Solution to Banks Around the World
>> <http://www.net-security.org/press.php?id=852>

BitDefender Announces Free Online Security Kit's Success
>> <http://www.net-security.org/press.php?id=851>

StarForce Announces M3/Replitech 2002
>> <http://www.net-security.org/press.php?id=850>

Leading Cable Device Providers Choose RSA Security to
Help Secure Broadband Connections
>> <http://www.net-security.org/press.php?id=849>

Utimaco Safeware and Ernst & Young IT-Security
GmbH form strategic cooperation
>> <http://www.net-security.org/press.php?id=848>

PivX Provides Free Fix For The Microsoft Internet
Explorer Gopher Hole
>> <http://www.net-security.org/press.php?id=847>

GFI Launches GFI Mail essentials for Exchange 7
>> <http://www.net-security.org/press.php?id=846>

France Telecom's SNPI Division Calls On Ca's Unicenter
To Slash Operating Costs And Improve Quality Of Service
>> <http://www.net-security.org/press.php?id=845>

Citrix MetaFrame XP Ranks Among Education's Most
Valued Technology Products
>> <http://www.net-security.org/press.php?id=844>

Psionic Technologies Introduces 'ClearResponse' to Automate
Enterprise Intrusion Response
>> <http://www.net-security.org/press.php?id=843>

Intrusion SecureNet 2245 Prices Leading Network
Intrusion Detection for Remote and Branch Offices
>> <http://www.net-security.org/press.php?id=842>

McAfee.com SpamKiller Receives PC World 'Best Buy' Award
>> <http://www.net-security.org/press.php?id=841>

F-Secure Provides Data Security to Telenordia's Customers
>> <http://www.net-security.org/press.php?id=840>

Microsoft and Trusecure Partner To Address Security
Needs For Financial Service Firms
>> <http://www.net-security.org/press.php?id=839>

[Featured articles]

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

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

TrueSign: Under the Hood
>> <http://www.net-security.org/article.php?id=136>

Achilles' Shield: A New Internet Security System for Protecting
Networks and Computer Systems Against Viruses and Malicious Code
>> <http://www.net-security.org/article.php?id=135>

Apache Chunk Handling Roundup
>> <http://www.net-security.org/article.php?id=134>

Roundup on BIND Denial of Service
>> <http://www.net-security.org/article.php?id=133>

[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

GOPHER SMOKER 0.06

This is a free fix for the MSIE Gopher Root Vulnerability. This hole in Microsoft's Internet Explorer (all versions) leaves most windows computers wide open.

>> <http://www.net-security.org/software.php?id=156>

SLIDENTD 0.0.19

Slidentd is a minimal ident (RFC1413) daemon which runs from inetd, xinetd, or tcpserver. It is similar in purpose to pidentd, which is installed with most Linux systems.

>> <http://www.net-security.org/software.php?id=157>

SMTP MAP 0.7

SMTP map uses a fingerprinting technology to scan for the version of whatever SMTP server software which is running on a machine. IPv6 is fully supported.

>> <http://www.net-security.org/software.php?id=158>

ANGEL NETWORK MONITOR 0.7

Angel is a simple yet useful tool to monitor the services on your network.

>> <http://www.net-security.org/software.php?id=159>

SPY GUARD

Spy Guard will scan your entire system, and will notify you if any spy related programs are running on your pc. It will look for any type of keystroke logging software, web browser loggers, password capturing programs, chat and email programs, and any other type of monitoring software installed on your pc.

>> <http://www.net-security.org/software.php?id=160>

SUPHP 0.1

suPHP is a combination of an Apache module (mod_suphp) and an executable which provides a wrapper for PHP. With both together, it is possible to execute PHP scripts with the permissions of their owner without having to place a PHP binary in each user's cgi-bin directory.

>> <http://www.net-security.org/software.php?id=161>

RUBY/PASSWORD 0.1.0

Ruby/Password is a set of useful methods for creating, verifying, and manipulating passwords.

>> <http://www.net-security.org/software.php?id=162>

PLUSHS 1.1

PluSHS allows you to resolve the names of a direction or a rank of direction's IP, allowing you to maintain a "map" of the names that it has assigned to each host that comprises a certain network.

>> <http://www.net-security.org/software.php?id=163>

EVENTWATCHNT 2.31

EventwatchNT is a WinNT/Win2000 service that monitors the eventlog (configurable) and sends you critical eventlog entries in realtime by SMTP email.

>> <http://www.net-security.org/software.php?id=164>

TURTLE FIREWALL 1.0

Turtle Firewall allows you to make a Linux firewall fast, it's based on Kernel 2.4.x and IPTables.

>> <http://www.net-security.org/software.php?id=165>

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