



Newsletter
Issue 114 - 10.06.2002
<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>.

=====

LANguard Security Event Log Monitor

=====

LANguard SELM is a network wide event log monitor that retrieves logs from all NT/2000 servers and workstations and immediately alerts the administrator of possible intrusions. Through network wide reporting, you can identify machines being targeted as well as local users trying to hack internal company information. LANguard analyses the system event logs, therefore is not impaired by switches, IP traffic encryption or high-speed data transfer.

Download your evaluation copy from:
<http://www.net-security.org/lm/ads/ads.pl?banner=gfitxt>

=====

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]

STARTUP TAKES ON WLAN SECURITY

AirDefense Inc. is taking a new approach to the problem of WLAN security by applying the concepts of intrusion detection and constant monitoring to Wi-Fi deployments.

>> <http://www.net-security.org/news.php?id=291>

EUROPE BANS SPAM

The European Parliament has voted to ban the sending of unsolicited commercial email.

>> <http://www.net-security.org/news.php?id=292>

COMING CLEAN ON PATCHES

A high-stakes battle is brewing between software developers and security researchers over when to release discovered vulnerability data and patches.

>> <http://www.net-security.org/news.php?id=293>

VIRUS AFFECTS BOTH WINDOWS AND LINUX

Symantec has published details of the first known polymorphic metamorphic virus to infect under both Windows and Linux.

>> <http://www.net-security.org/news.php?id=295>

SURE, SECURITY IS HARD, BUT...

The New York Times recently switched from one paid membership management system to another. Marc Hedlund notes how insecure they sent new login details to the members.

>> <http://www.net-security.org/news.php?id=296>

SENTENCE IN LIBRARY HACKING CASE

A Philadelphia man who hacked into a western New York library Web site was sentenced to one to three years in prison.

>> <http://www.net-security.org/news.php?id=297>

SUN HEATS UP SOLARIS

Sun Microsystems last week unveiled the latest release of its Solaris operating system. This is a list of some security features it includes.

>> <http://www.net-security.org/news.php?id=298>

VERISIGN TO HELP TELECOMS WITH WIRETAP ORDERS

Security and Web address provider VeriSign Inc. unveiled a new service to help U.S. telecommunications carriers comply with wiretapping regulations.

>> <http://www.net-security.org/news.php?id=299>

WANTED: GREAT SECURITY FOR WIRED CARS

Easy, reliable authentication is crucial as mobile devices - including autos - go online, execs say.

>> <http://www.net-security.org/news.php?id=301>

SECURITY UNDER THE GUN

Everyone predicted that IT security jobs would be hot after the Sept. 11 terrorist attacks, but the reality is quite the opposite.

>> <http://www.net-security.org/news.php?id=302>

RANDOMIZATION - IBM'S ANSWER TO WEB PRIVACY

IBM Corp's new Privacy Institute has decided that randomization may be the key to protecting consumer privacy on the web while also providing e-businesses with informative metrics on their customers.

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

SCAN OF THE MONTH CHALLENGE #21

Three different members of the HoneyNet Research Alliance received a flurry of strange UDP packets. This month's Scan of the Month challenge is to understand the purpose of these packets.

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

IT SECURITY BREACHES HIT 80% OF FIRMS IN IRELAND

KPMG published new research showing that 80% of companies have suffered a security incident or breach, such as a virus or hacker attack, in the past year.

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

NET FRAUD IS TANGLED WEB FOR VICTIMS, POLICE

Even when the SEC does find fraud, it has no criminal authority. As the Furr case shows, the SEC can win a multimillion-dollar civil judgment but may never collect the money.

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

NSA LAUNCHES AD CAMPAIGN URGING SECRECY

The NSA has launched a flock of ads urging military personnel to protect national secrets during this time of terrorist crisis.

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

SOLVING KID PORN'S 'REAL' PROBLEM

A company says it can create a database that differentiates actual child porn from the computer-generated kind. In the wake of a U.S. Supreme Court ruling, that might be a great tool for law enforcement.

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

US COPS TARGET HACKERS

The US Secret Service will launch task forces in eight cities to prevent and prosecute cybercrime, identity and data theft and hacking of corporate databases.

>> <http://www.net-security.org/news.php?id=310>

VIRUS NAMING PRACTICES

This article will offer a brief overview of naming conventions that are used to develop names for viruses and other malware.

>> <http://www.net-security.org/news.php?id=311>

SMARTS MOVES ON ATM, FRAME AND SECURITY

Smarts will launch a module for managing frame relay and ATM, to follow up its security and application services management software.

>> <http://www.net-security.org/news.php?id=312>

FEDS SEEK BETTER MICROSOFT SECURITY

Government technology officials, tired of security holes in Microsoft's products, are discussing whether to use their collective purchasing power to force changes in the way the software giant does business.

>> <http://www.net-security.org/news.php?id=313>

LACK OF TRUST HOLDS BACK SECURITY

If you believe the hype, companies terrified by the prospect of electronic attack will turn to third parties to defend their businesses.

>> <http://www.net-security.org/news.php?id=314>

BROADBAND IN EVERY HOME? NOT UNTIL IT'S MORE SECURE

Senator Joseph Lieberman wants everyone to have super-fast Net access. But Robert says the plan poses some pretty serious security risks.

>> <http://www.net-security.org/news.php?id=315>

ULTIMATE COMPUTER SECURITY DEVICES

Yankee Group senior analyst Anil Phull told NewsFactor that the best practice for companies using biometric devices is to deploy them with other identification tools.

>> <http://www.net-security.org/news.php?id=316>

SECURING NIS

The following is a compendium of what the people at Auburn University College of Engineering use to secure their NIS networks.

>> <http://www.net-security.org/news.php?id=317>

ILPF CONFERENCE 2002: SECURITY V. PRIVACY

The Annual Internet Law & Policy Forum Conference will take place on September 18-19, 2002 at the Bell Harbor International Conference Center, Seattle, WA.

>> <http://www.net-security.org/news.php?id=318>

MSNBC REPORTER SUBPOENAED IN HACKING CASE

U.S. prosecutors sent a subpoena to MSNBC demanding a reporter's notes, e-mails and other information as part of an investigation into the NYT hack earlier this year.

>> <http://www.net-security.org/news.php?id=319>

DEAD MEN TELL NO PASSWORDS

The man in charge of electronic copies of Norway's most important historical documents is dead and so is access to those archives. Hackers help is sought to crack the center's password-protected database.

>> <http://www.net-security.org/news.php?id=321>

PRIVACY VS. SECURITY: A BOGUS DEBATE?

Author of The Transparent Society, David Brin says what's needed are rules and tools to let citizens "watch the watchers".

>> <http://www.net-security.org/news.php?id=322>

COMPUTER FRAUD HITS COMPANIES

A new computer fraud costing thousands of euro has hit at least 10 Irish companies.

>> <http://www.net-security.org/news.php?id=323>

OUR MAN ORDERED WAFFLES, BUT PAID FOR TOOLS OF WAR

All I wanted was a warm, crispy waffle. But I ended up sending a night-vision rifle scope to some criminal in Saudi Arabia. Such are the realities of credit card fraud and identity theft in the Internet age.

>> <http://www.net-security.org/news.php?id=324>

MICROSOFT PLANS NEW WEB SERVICES PUSH

Microsoft is developing new security software it hopes will make its entire product lineup more appealing to big companies.

>> <http://www.net-security.org/news.php?id=325>

SECURITY THROUGH OBSOLESCENCE

Here's an interesting way to secure an Internet-connected computer against intruders: Make sure the operating system and software it runs are so old that current hacking tools won't work on it.

>> <http://www.net-security.org/news.php?id=326>

CLARKE WARNS EDUCATORS ABOUT NEED FOR BETTER SECURITY

President Bush's cybersecurity czar called on colleges and universities to beef up their own IT security and broaden the kinds of security courses offered to students.

>> <http://www.net-security.org/news.php?id=327>

XP PROFESSIONAL SECURITY FEATURES: AN INTRODUCTION

This article will offer an overview of the security features that are available in Microsoft XP Professional.

>> <http://www.net-security.org/news.php?id=328>

MANAGING INFORMATION SECURITY

Last year, U.S. businesses reported 53,000 system break-ins. The true number is probably higher because concerns about negative publicity mean that almost two-thirds of all incidents actually go unreported.

>> <http://www.net-security.org/news.php?id=329>

SECURITY ADVISORIES WEEK: 30 MAY - 6 JUNE 2002

This is an overview of security advisories that were released in the past 7 days by several Linux vendors, SUN Microsystems, Microsoft and CERT.

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

REVIEW: ENGARDE SECURE LINUX PROFESSIONAL 1.1

Guardian Digital's Engarde Secure Linux Professional offers a lightweight, robust, and secure Linux Distribution for small and large networks.

>> <http://www.net-security.org/news.php?id=331>

OPTIMIZING NIDS PERFORMANCE

To help network intrusion detection systems keep up with the demands of today's networks there are a number of things

that the NIDS administrator can do to improve the performance of their NIDS.

>> <http://www.net-security.org/news.php?id=332>

BAD GUY WISDOM

Who's more open and honest, hackers or corporate America? Communicate. Organize yourselves. Talk honestly about security failures, what you've learned and how you're adapting.

>> <http://www.net-security.org/news.php?id=333>

AN IDEA TO CAN THE SPAM

The problem is that filters do not always prevent mail from bad sources, and the whole "opt-in" farce has resulted in spammers sending whatever messages they want.

>> <http://www.net-security.org/news.php?id=334>

TEDDY BEAR VIRUS HOAX CAUSES ALARM

Internet users have been warned to ignore a hoax virus alert that experts say has become a major problem.

>> <http://www.net-security.org/news.php?id=335>

WORLD CUP EMAIL LEADS TO VIRUS PENALTY

Fans looking for World Cup results could get more than they bargained for with an email-based virus.

>> <http://www.net-security.org/news.php?id=336>

HIGH SCHOOL HACKERS MAKE THE GRADE

Two high school hackers have been caught running a racket where they charged \$5 to change fellow pupils' exam grades.

>> <http://www.net-security.org/news.php?id=337>

ANTI-VIRUS/ANTI-SPAM MAIL SERVER SETUP USING MAILSCANNER

Wouldn't it be great to have the ability to stop email-borne virus traffic, arguably the most ubiquitous kind, at the server level where you control the action?

>> <http://www.net-security.org/news.php?id=338>

SCAN YOUR COMPUTER FOR VIRUSES

If you don't have an anti virus product installed on your computer, you should check the Online scan from HNS web site. Unfortunately, it just works with Internet Explorer, but it is a great and fast scanner.

>> <http://www.net-security.org/v/bd/scan/>

KAZAA INSECURE, USERS OBLIVIOUS

File-swapping service Kazaa is rife with security holes and may pose a risk to its users, according to research conducted by HP Labs.

>> <http://www.net-security.org/news.php?id=341>

SECURITY VULNERABILITIES IN BUGZILLA

Various security issues of varying importance have been fixed in

Bugzilla 2.14.2. Most of these were fixed already in 2.16rc1, a few were not.

>> <http://www.net-security.org/news.php?id=342>

HISTORICAL DATABASE PASSWORD RETRIEVED

As we mentioned earlier, Norwegian educational center for cultural preservation lost the password to a vast database and asked hackers to help. Password was quickly retrieved.

>> <http://www.net-security.org/news.php?id=343>

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

CBMS Cross Site Scripting and SQL Injection Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=1758>

Multiple Vulnerabilities in SeaNox DevWex

>> <http://www.net-security.org/vuln.php?id=1757>

Security Vulnerabilities in LokwaBB and W-Agora

>> <http://www.net-security.org/vuln.php?id=1756>

Multiple Red-M 1050 Blue Tooth Access Point Vulnerabilities

>> <http://www.net-security.org/vuln.php?id=1755>

Format String Vulnerability in TrACERoute 6.0 Gold

>> <http://www.net-security.org/vuln.php?id=1754>

Splatt Forum Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=1753>

PHP(Reactor) Cross Site Scripting Vulnerability

>> <http://www.net-security.org/vuln.php?id=1752>

eDonkey 2000 ed2k URL Buffer Overflow

>> <http://www.net-security.org/vuln.php?id=1751>

BlackICE Agent not Firewalling After Standby
>> <http://www.net-security.org/vuln.php?id=1750>

Vulnerabilities in the Telindus 11xx Router Series
>> <http://www.net-security.org/vuln.php?id=1749>

SCO OpenServer Crontab Format String Vulnerability
>> <http://www.net-security.org/vuln.php?id=1748>

SHOUTcast 1.8.9 Buffer Overflow
>> <http://www.net-security.org/vuln.php?id=1747>

Slurp News Retriever Remote Format String Vulnerability
>> <http://www.net-security.org/vuln.php?id=1746>

Solaris snmpdx Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1745>

SQL Injection in LogiSense Software
>> <http://www.net-security.org/vuln.php?id=1744>

Buffer Overflow in Internet Explorer Gopher Code
>> <http://www.net-security.org/vuln.php?id=1743>

Remotely Exploitable fmt String Vulnerability In Squid
>> <http://www.net-security.org/vuln.php?id=1742>

MIME::Tools Problems
>> <http://www.net-security.org/vuln.php?id=1741>

Self-Executing HTML in Internet Explorer 5.5 and 6.0
>> <http://www.net-security.org/vuln.php?id=1740>

Multiple Vulnerabilities in csPassword.cgi
>> <http://www.net-security.org/vuln.php?id=1739>

BadBlue Web Server v1.7.0 Directory Contents Disclosure
>> <http://www.net-security.org/vuln.php?id=1738>

Courier CPU exhaustion + bonus on imap-uw
>> <http://www.net-security.org/vuln.php?id=1737>

AIM+ is a Spyware Program
>> <http://www.net-security.org/vuln.php?id=1736>

Mnews Local and Remote Overflow Vulnerabilities
>> <http://www.net-security.org/vuln.php?id=1735>

Shambala Server 4.5 Directory Traversal and DoS
>> <http://www.net-security.org/vuln.php?id=1734>

[Advisories]

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

EnGarde Secure Linux Advisory - Remote buffer overflow in imap daemon
>> <http://www.net-security.org/advisory.php?id=753>

Trustix Security Advisory - tcpdump
>> <http://www.net-security.org/advisory.php?id=752>

Conectiva Linux Security Announcement - bind
>> <http://www.net-security.org/advisory.php?id=751>

SGI Security Advisory - MediaMail vulnerability
>> <http://www.net-security.org/advisory.php?id=750>

SuSE Security Announcement - bind9, bind9-beta
>> <http://www.net-security.org/advisory.php?id=749>

Conectiva Linux Security Announcement - kernel
>> <http://www.net-security.org/advisory.php?id=748>

Caldera International Security Advisory - Linux: tcpdump
AFS RPC and NFS packet
>> <http://www.net-security.org/advisory.php?id=747>

Conectiva Linux Security Announcement - tcpdump
>> <http://www.net-security.org/advisory.php?id=746>

CERT Advisory CA-2002-16 - Multiple Vulnerabilities in
Yahoo! Messenger
>> <http://www.net-security.org/advisory.php?id=745>

Sun Microsystems Security Bulletin - SEA SNMP
>> <http://www.net-security.org/advisory.php?id=744>

Red Hat Security Advisory - Ghostscript command execution vulnerability
>> <http://www.net-security.org/advisory.php?id=743>

Red Hat Security Advisory - Updated bind packages fix denial of service attack
>> <http://www.net-security.org/advisory.php?id=742>

Red Hat Security Advisory - Updated xchat packages fix /dns vulnerability
>> <http://www.net-security.org/advisory.php?id=741>

CERT Advisory CA-2002-15 - Denial-of-Service Vulnerability in ISC BIND 9
>> <http://www.net-security.org/advisory.php?id=740>

SGI Security Advisory - rpc.passwd vulnerability
>> <http://www.net-security.org/advisory.php?id=739>

Microsoft Security Bulletin MS02-025 - Malformed Mail Attribute can Cause Exchange 2000 to Exhaust CPU Resources
>> <http://www.net-security.org/advisory.php?id=738>

Caldera Security Advisory - Volution Manager: Directory Administrator password in cleartext
>> <http://www.net-security.org/advisory.php?id=737>

Debian Security Advisory - memory allocation error in ethereal
>> <http://www.net-security.org/advisory.php?id=736>

Debian Security Advisory - in.uucpd string truncation problem
>> <http://www.net-security.org/advisory.php?id=735>

[Virus News]

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

Beware of Virus Authors Exploiting World Cup Themes
>> http://www.net-security.org/virus_news.php?id=28

Trojan Hunts Down Graduating Students
>> http://www.net-security.org/virus_news.php?id=27

Case Study: Kaspersky Labs Implementation for Golden Telecom
>> http://www.net-security.org/virus_news.php?id=26

Kaspersky Labs The Virus Top Twenty for May 2002
>> http://www.net-security.org/virus_news.php?id=25

Win an MP3 Player by Taking Sophos Customer Survey
>> http://www.net-security.org/virus_news.php?id=24

[Security world]

All press releases are located at:
http://www.net-security.org/press_main.php

World Cup Virus Aims To Foul Football Fans
>> <http://www.net-security.org/press.php?id=817>

Shakira Worms Her Way Back For An Encore
>> <http://www.net-security.org/press.php?id=816>

Sophos and Sandvine Partner to Deliver Network-Based Anti-Virus Solution
>> <http://www.net-security.org/press.php?id=815>

GFI Launches GFI LANguard Security Event Log Monitor (S.E.L.M.) 3.0
>> <http://www.net-security.org/press.php?id=814>

Sophos Anti-Virus for Windows XP Receives Virus Bulletin 100% Award
>> <http://www.net-security.org/press.php?id=813>

Trend Micro Defends 22,000 Fairfax County Public School Staff and 400 Servers from Viruses and Malicious Code

>> <http://www.net-security.org/press.php?id=812>

TruSecure And Pantellos Team To Provide Security Services To The Pantellos Trading Community

>> <http://www.net-security.org/press.php?id=811>

Kaspersky Labs The Virus Top Twenty for May 2002

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

[Featured articles]

All articles are located at:

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

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

BACKDOORED DSNIFF, FRAGRROUTE AND FRAGRROUTER

In a recent hack of irssi server, attacker modified the configure script which gave him shell access to any system that installed the backdoored irssi program. The same thing happened to Dug Song's Monkey.org - dsniiff-2.3, fragroute-1.2, and fragrouter-1.6 were modified.

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

REVIEW: WINTASKS 4 PROFESSIONAL

For IT professionals and software developers WinTasks 4 Professional makes resource management easier than ever before.

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

AN INTRODUCTION TO SNORT

This is a presentation at the Houston ISSA Meeting in April by Ricard Bejtlich, a senior forensic consultant for Foundstone.

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

[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

MAILSECURITY FOR EXCHANGE/SMTP

GFI MailSecurity acts as an Email Firewall and protects you from email viruses, exploits and threats, as well as email attacks targeted at your organization. GFI MailSecurity is available for VS API or as an SMTP gateway version. The VS API version integrates seamlessly with Exchange Server 2000 and scans the Exchange 2000 information stores.

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

AD-AWARE 5.82

Ad-aware is a free multi spyware removal utility that scans your memory, registry and hard drives for known spyware and scumware components and lets you remove them safely.

>> <http://www.net-security.org/software.php?id=135>

DOWNLOADSECURITY FOR ISA SERVER

Download content checking & anti-virus for Microsoft ISA Server. Install this version on the ISA server machine.

>> <http://www.net-security.org/software.php?id=136>

KMYFIREWALL 0.4.4

KMyFirewall is a Kde/Qt Programm that tries to provide an easy to use and comfortable GUI for the Linux 2.4 "iptables" command. As a difference to other projects KMyFirewall will be able to import/export its ruleset for easy setup of big networks.

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

DEAD MAN'S SWITCH

This is basically a system that, if not reset by a given time, will automatically carry out a series of tasks, such as posting messages to websites, sending e-mails to loved ones (or hated ones), and encrypting or destroying sensitive files.

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

SECURE RM 1.2.5

srm is a secure replacement for rm(1). Unlike the standard rm, it overwrites the data in the target files before unlinking them. This prevents command-line recovery of the data by examining the raw block device. It may also help frustrate physical examination of the disk, although it's unlikely that it can completely prevent that type of recovery. It is, essentially, a paper shredder for sensitive files.

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

DNS HIJACKER 1.2

DNS Hijacker is a libnet/libpcap based DNS sniffer/spoofers. A versatile tool, it supports tcpdump-style filters that allow you to specifically target victims. DNS answers are forged based on entries in a "fabrication table" or by simply forging one answer to all requests. A print-only mode is also supported, allowing one to simply monitor DNS traffic. DNS Hijacker is an excellent tool for blocking and removing advertisements at the network level.

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

SSMART 0.3.1

ssmart is a little Perl script to store a secure shell identity/cfs passwords blowfish-encrypted to a smartcard. There will be no local copy of your identity on your harddrive, or even worse on an NFS share. It also allows you to quick mount all stored cfs directories, and it has a GNOME GUI (useful if you want it to use it with your .xinitrc). It uses the smartcard program to interact with the chipdrive.

>> <http://www.net-security.org/software.php?id=141>

PRISMSTUMBLER 0.5.0

PrismStumbler is a wireless LAN (WLAN) which scans for beaconframes from accesspoints. Prismstumbler operates by constantly switching channels and monitors any frames recived on the currently selected channel.

>> <http://www.net-security.org/software.php?id=142>

ZEBEDEE 2.4.1

Zebedee is a simple program to establish an encrypted, compressed "tunnel" for TCP/IP or UDP data transfer between two systems. This allows traffic such as telnet, ftp and X to be protected from snooping as well as potentially gaining performance over low bandwidth networks from compression.

>> <http://www.net-security.org/software.php?id=143>

MAILSCANNER 3.15-3

MailScanner is a virus scanner for e-mail designed for use on e-mail gateways. It can also detect a large proportion of unsolicited commercial e-mail (spam) passing through it.

>> <http://www.net-security.org/software.php?id=144>

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