

HNS Newsletter
Issue 89 - 26.11.2001
<http://net-security.org>
<http://security-db.com>

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://www.net-security.org>.

Subscribe to this weekly digest on:
<http://www.net-security.org/text/newsletter>

Archive of the newsletter in TXT and PDF format is available here:
<http://www.net-security.org/news/archive/newsletter>

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured products
- 5) Security software

=====
FREE SSL GUIDE FROM THAWTE

=====
Are you planning your Web Server Security?

Click here to get a FREE Thawte SSL guide and find the answers to all your SSL security issues.

<http://www.gothawte.com/rd127.html>

=====
General security news

GAPS IN SECURITY PLAN

Microsoft Corp.'s vulnerability-handling plan is a good start but may end up being insufficient as the specter of government regulation of Internet security looms, according to security experts.

Link: <http://www.eweek.com/article/0,3658,s%253D701%2526a%253D18647,00.asp>

AUTOMATIC ALERTS, PATCHES MAKE SECURITY LESS ONEROUS

Configuresoft Inc. says it will make patching easier by automating patch updates for companies running Windows NT and Windows 2000 networks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.informationweek.com/story/IWK20011116S0016>

NETWORK SCANNING

Desktop Unix systems, and now Microsoft systems, come with several services turned on by default. There are utilities that allow to scan a server and discover which ports have daemons listening on them. Many Internet daemons, and especially IIS servers, have security vulnerabilities that can allow hackers to gain control of your computer.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.onlamp.com/pub/a/onlamp/2001/11/15/scanning.htm>

ZEUS THROTTLES APP-LEVEL DOS ATTACKS

Zeus Technology is upgrading its Web server technology to guard against application level DoS attacks. According to Andrew Parker, vice president of corporate strategy at Zeus Technology, organisations can enhance the security of an organisation's web infrastructures by placing Unix boxes running Zeus in front of IIS farms. BT is trialling the technology.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22912.html>

KIDDIENET - A LAST LINE OF DEFENCE?

At Advogato.org MartBrooks writes: "Several months ago I wrote an article to highlight the frustration I feel at Network Administrators who ignore, or are ignorant of, people who are using their network resources to commit what are effectively illegal acts. The article was largely ignored. Even now, I'm still seeing infected Windows boxes probing the outside of my firewall and so I thought I'd re-post the article here for your consideration."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.advogato.org/article/380.html>

ZI HACKADEMY - HACKING SCHOOL

Zi HackAdemY opened its doors near the Bastille on 15 October and has attracted nearly 80 pupils so far. Many teachers and their students are known only by pseudonyms, such as lecturer Clad Strife, a science student who fears his professors might not look kindly upon his teaching the fine art of hacking in his spare time.

Link: <http://www.thescotsman.co.uk/world.cfm?id=123739>

WHEN THE HACKED BECOMES THE HACKER

The latest security software for the Web goes further than ever in identifying the origin of attacks, but experts say computer security is not ready to hack back for fear of harming innocent users and because any hack attack - even a retaliatory one - is illegal.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsfactor.com/perl/story/14874.html>

CAN YOUR BIZ PASS A SECURITY AUDIT?

Are you really sure your network is as secure as it needs to be? Really? When's the last time you actually did a security audit? When's the last time you checked to see that your employees were actually following your security policy? You do have a security policy, don't you?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2825802,00.html>

NEW CYCLONE PROGRAMMING LANGUAGE: BUGS BE GONE!

Cornell University and AT&T Labs are developing Cyclone, a new computer programming language similar to C but much more difficult for programmers to introduce bugs when writing code.

Link: <http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=23262>

THE EVOLUTION OF INTRUSION DETECTION SYSTEMS

This article will endeavour to examine how intrusion detection has evolved to its current state. Starting with a brief overview of different IDS methodologies, the article will then take a brief look at the history of IDS, and will conclude with a look at some of the major players in the IDS field.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1514>

ASIA INCREASES TECH SPENDING ON SECURITY

Asian companies squeezing their information technology budgets because of the global economic slowdown are belatedly realizing they can't cut too many corners in the new security-conscious world.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/11/19/attack.tech.asia.reut/index.html>

SAFEWEB GOES DOWN FOR THE COUNT

Following the regrettable loss of ZeroKnowledge Systems Freedom network, Web proxy SafeWeb has now discontinued its free, anonymous surf portal.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22931.html>

CROSS SITE SCRIPTING HOLES

The following web site lists few of the well known web sites which are vulnerable to cross site scripting. Also with the list, example links are provided just to see how easy is to snatch some kind of information.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.devitry.com/holes.html>

BROADBAND ISPS SHOULDN'T KNOCK DOWN FIREWALLS

Alex Salkever writes: "Get rid of my firewall? Only when you pry my cold dead fingers from the keyboard. So imagine my dismay when an otherwise helpful technical-support person from TimeWarner's RoadRunner cable-broadband unit told me she couldn't assist me until I removed every single trace of the ZoneAlarm firewall from my machine."

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011120_6165.htm

PLAYBOY SAYS ATTACKER STOLE CUSTOMER INFO

Playboy.com has alerted customers that an intruder broke into its Web site and obtained some customer information, including credit card numbers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1007-200-7932825.html>

CONSUMER WATCH: NATIONAL SECURITY VS. ONLINE PRIVACY

You've probably heard a lot of debate over the USA Patriot Act, the federal legislation passed in October to give investigators more tools for apprehending terrorists. Proponents of the law say we need it to protect ourselves. Opponents say it threatens our constitutional rights. But whatever position you take on these issues, it's important to know how the new law will affect your life online.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/features/article/0,aid,68769,00.asp>

SUN DENIES UNIX FLAW

Six vendors, including IBM, Hewlett-Packard and Sun, have been alerted to a vulnerability that ships with several Unix systems, which could allow a malicious attacker to take control of an affected system. Sun Microsystems is refusing to acknowledge that any problem exists.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1126973>

BUILDING AN E-MAIL VIRUS DETECTION SYSTEM FOR YOUR NETWORK

The usual first approach that administrators take in virus prevention is to install a desktop virus protection program. That is wise, but it seems to me the most fail-safe way to protect a corporate network from viruses is to prevent their entrance into the system in the first place.

Link: <http://noframes.linuxjournal.com/article.php?sid=4882>

MS VICTIM OF HUMOROUS DNS NON-HACK

It appears that someone has again associated at least fifty (probably more) domain names with microsoft.com, and given them humorous titles tending to disparage the mighty Redmond Leviathan.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22957.html>

CERT SUMMARY CS-2001-04

CERT - "Since the last regularly scheduled CERT summary, issued in August 2001 (CS-2001-03), we have seen a new worm known as "Nimda," as well as active exploitation of a vulnerability in Microsoft DNS servers. In addition, we have published a paper on denial of service trends, issued a new PGP key, and updated the UNIX Security Checklist."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/summaries/CS-2001-04.html>

PROJECT ECHELON: ORBITING BIG BROTHER?

Earth-orbiting listening posts are on active duty in the United States-led war on terrorism. Signal-seeking spacecraft not only play a critical role in eavesdropping on nations from on high, but also within the borders of the U.S. itself.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.space.com/business/technology/echelon_011121-1.html

FBI.GOV VX "SCENE"

SV has an article entitled "FBI borrows from hackers in reported virus project". According to MSNBC, the FBI wants to be able to send sleuthing software, called "Magic Lantern," to computers through an e-mail message in the same way that most malicious computer viruses are distributed.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.siliconvalley.com/docs/news/tech/040656.htm>

POWER TO THE GOVERNMENT

AP's Technology Writer bases a story on the fact that Justice Department, using the recently approved antiterrorism law, can now prosecute foreign hackers when they attack computers in their own or other countries outside the United States. Article offers few critics on this law summed up with the following sentence by former Justice Department computer crimes prosecutor Mark Rasch - "It's a massive expansion of U.S. sovereignty".

Link: <http://sns.chicagotribune.com/technology/sns-ap-policing-the-internet1121nov21.story?coll=sns%2Dtechnology%2Dheadlines>

HELP SYMANTEC DISCOVER VIRUSES

Symantec recently increased the price of its necessary subscription renewal program from \$3.95 to \$9.95 a year. Symantec executives said that price increase helps defray the company's costs of discovering new viruses and updating the software.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_733144_5055_1-2793.html

CENSORSHIP BONANZA IN CHINA

The Register reports that the Chinese Government has shut down 17,488 Internet cafes. The official reason for the closures is their failure to block sites considered subversive or pornographic.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/22968.html>

REDSIREN ACQUIRES ATOMIC TANGERINE ASSETS

RedSiren Technologies, Inc., announced it has completed its previously announced acquisition of the assets of AtomicTangerine. Terms of the agreement were not disclosed. As it can be seen from the press release, RedSiren has added a significant number of AtomicTangerine staffers as part of the acquisition, saying, "We consider them to be an enormous part of the value that AtomicTangerine offered. They elevate our thinking, they increase our abilities, and they will be a major factor in our growth and success in the marketplace." SecurityPortal.com's future wasn't discussed.

Link: <http://www.atomictangerine.com/pdf/RSATClosing.pdf>

SECURE DISK PROTECTION NI-3100 SERIES

Seiko Instruments Inc. developed a new hard disk drive protection system, the "Secure Disk Protection Ni-3100 Series." This gadget is supposed to be a physical security layer against attacks on the web server. According to the article, HDD has a mode switch option which can be triggered to allow or disallow access to write on the system.

Link: <http://www.nikkeibp.asiabiztech.com/wcs/leaf?CID=onair/asabt/news/156233>

3A SECURITY SOFTWARE TO BOOM

The European market for administration, authorisation and authentication (3A) security software will grow from \$742 million in 2000 to \$2.4 billion in 2005, an annual increase of 27 per cent.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22987.html>

AXELERO ADMITS INTRUSION

Hungarian Internet service provider Axelero yesterday advised its customers to change their password at the company's website or on a toll-free number because of a break in that finished up with intruders being able to access confidential data.

Link: <http://www.bbj.hu/user/article.asp?ArticleID=135265>

SECURITY: THE ENEMY WITHIN

KPMG surveyed more than 1,200 IT directors and senior managers from some of the world's largest organisations, and found that 79% believed that a security breach to one of their e-commerce systems would be the result of an external force. Of course, they think wrong.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22974.html>

SOPHOS MAILMONITOR NEWS

Sophos MailMonitor for SMTP has been released on the Linux platform. Shortly Sophos will open a beta trial for Sophos MailMonitor for SMTP on Unix (Solaris SPARC), broadening the MailMonitor product portfolio even further.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sophos.com/companyinfo/news/smtpunix.html>

ELCOMSOFT BACKS FROM BLACK HAT EUROPE

ElcomSoft, the Russian employer of Dimitri Sklyarov, has cancelled its planned participation in the Black Hat Europe hacking conference, on legal advice.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22985.html>

MUDGE: FROM THE LOPHT TO THE WEST WING

It was supposed to be the year Peiter Zatko aka Mudge could finally step out from behind the digital curtain. Invited to a February 2000 photo op with President Bill Clinton in the White House Cabinet Room, he felt that he'd finally be able to reveal himself and receive the public recognition for security work he had done for the government.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/november01/people_mudge.shtml

=====

HNS Security Database

=====

HNS Security Database consists of a large database of security related companies, their products, professional services and solutions. HNS Security Database will provide a valuable asset to anyone interested in implementing security measures and systems to their companies' networks.

Visit us at <http://www.security-db.com>

=====

Security issues

All vulnerabilities are located at:
<http://net-security.org/text/bugs>

CONECTIVA LINUX - IMP UPDATE

Joao Pedro Goncalves reported a vulnerability in the Imp webmail system which could be used by a remote attacker to access a victim's email. It is possible to include a script in an URL via html tags. Since these tags are not treated appropriately in previous versions ($\leq 2.2.6$) of Imp, such scripts can be executed by an unsuspecting user if clicked on when viewing an email. By emailing such a crafted URL to an user and having this user click on it, the attacker is able to retrieve the authentication cookies used in the webmail session, thus gaining access to the user's webmail account.

Link: <http://www.net-security.org/text/bugs/1006174298,59613,.shtml>

USING GOOGLE FOR GETTING INTERESTING INFORMATION

I heard recently about the capacity of google to deal with documents from Word, Excel or Powerpoint. Intested in that fact, I decided to experiment some words and expression (with ") to look for (sorry if my english is not perfect..) and I found some combos that give enormous results. In google, if you type things like :

- 1)"Index of /admin"
- 2)"Index of /password"
- 3)"Index of /mail"
- 4)"Index of /" +banques +filetype:xls (for france...)
- 5)"Index of /" +passwd
- 6)"Index of /" password.txt

And you can continue as long as your imaginatio is active. For example of my results, I saw great informations from the central banks of Luxemboug and Switzerland, could admin a SQL server, ...

Link: <http://www.net-security.org/text/bugs/1006191723,14192,.shtml>

HYPERMAIL SSI VULNERABILITY

Hypermail can be used to create arbitrary files, with arbitrary extensions, on the server, which may then possibly be used to execute SSI commands.

Link: <http://www.net-security.org/text/bugs/1006277411,81476,.shtml>

MS INTERNET EXPLORER PASSWORD INPUTS

If you enter a password that contains a mix of non-alphabetic and alphabetic characters to an MS IE password input and then use the keyboard to select it while holding down tab the cursor / selected region jumps between the non-alphabetic characters in exactly the same manner as it does when you apply the same technique in word, Interdev, vb etc.

Link: <http://www.net-security.org/text/bugs/1006354548,26198,.shtml>

LINUX MANDRAKE - GNUPG FORMAT STRING VULNERABILITY

A format string vulnerability exists in gnupg 1.0.5 and previous versions which is fixed in 1.0.6. This vulnerability can be used to invoke shell commands with privileges of the currently logged-in user.

Link: <http://www.net-security.org/text/bugs/1006354634,83282,.shtml>

REMOTE VULNERABILITY IN HP-UX LINE PRINTER DAEMON

Internet Security Systems (ISS) X-Force has discovered a vulnerability in the HP-UX line printer daemon (rlpdaemon). This vulnerability may allow a remote or local attacker to execute arbitrary code with superuser privilege.

Link: <http://www.net-security.org/text/bugs/1006354728,4526,.shtml>

=====

Sponsored by GFI, the developers of a revolutionary new intrusion detection product - LANguard Security Event Log Monitor.

Download your copy!

<http://www.net-security.org/cgi-bin/ads/ads.pl?banner=gfitxt>

=====

Security world

All press releases are located at:

<http://net-security.org/text/press>

GUARDEDNET OPENS NEW YORK OFFICE

GuardedNet, developer of the most advanced threat management and information security operations software, announces the opening of an office in New York, New York, serving large, global organizations, especially the financial services industry.

Press release:

< <http://www.net-security.org/text/press/1006191995,5947,.shtml> >

IBM ANNOUNCES GLOBAL SECURITY INITIATIVE

IBM Global Services Expands Security Practice; adds Kroll's Physical Security Protection to e-business security portfolio. The initiative, built on a two-pronged approach, aligns IBM's extensive safety and security offerings within an expanded IBM Global Services Practice and creates a new corporate-level Global Solutions Office to address broader and emerging safety and security issues in industry, global commerce and society.

Press release:

< <http://www.net-security.org/text/press/1006192027,45640,.shtml> >

SSH SECURE SHELL FOR HANDHELDS AVAILABLE

SSH Communications Security, a world-leading developer of Internet security solutions, announced the immediate availability of SSH Secure Shell for Handhelds, the industry's first Secure Shell application for wireless platforms which was announced earlier this year. This Secure Shell product, based on the widely accepted SymbianOS operating system for wireless communications, is the first security application to protect IP-based communication over wireless devices, such as e-mail and terminal emulation.

Press release:

< <http://www.net-security.org/text/press/1006192062,3789,.shtml> >

GFI LAUNCHES EMAIL SECURITY TESTING ZONE

GFI has launched an Email Security Testing Zone to enable organizations to check whether their email systems are vulnerable to email viruses and attacks. The zone, <http://www.gfi.com/emailsecuritytest/>, allows visitors to discover instantly if their system is secure against current and future email threats, such as emails containing infected attachments, emails with malformed MIME headers, and HTML mails with embedded scripts.

Press release:

< <http://www.net-security.org/text/press/1006276809,44656,.shtml> >

GLOBALSIGN LAUNCHES ABOUTDIGITALSIGNATURES.NET

GlobalSign, one of the leading European providers of PKI solutions and services, has launched a pan-European web site. GlobalSign took the initiative in order to stress the importance of the use of digital certificates while doing transactions over the Internet and to raise awareness amongst the web users with regard to this issue.

Press release:

< <http://www.net-security.org/text/press/1006276907,37573,.shtml> >

INTERSCAN MESSAGING SECURITY SUITE FOR SMTP 5.0 OUT

Trend Micro Inc., a worldwide leader in network antivirus and Internet content security solutions, announced the availability of Trend Micro InterScan Messaging Security Suite for SMTP Version 5.0. InterScan Messaging Security Suite stops and contains email-borne viruses using its advanced content-filtering technology and the antivirus expertise of TrendLabs, Trend Micro's worldwide research and support organization.

Press release:

< <http://www.net-security.org/text/press/1006276986,38784,.shtml> >

SECURITYFOCUS IDENTIFIES NEW DDOS THREAT

SecurityFocus, the leading provider of security intelligence products and services for business, has identified a new hybrid tool that combines distributed denial of service (DDoS) tools, with the automated propagation techniques previously seen only in worms.

Press release:

< <http://www.net-security.org/text/press/1006396544,11690,.shtml> >

ALLOT'S NETENFORCER BLOCKS DENIAL OF SERVICE ATTACKS

Allot Communications, the premier provider of policy-based networking solutions, announced the successful implementation of Allot's NetEnforcer to enhance network security and block Denial of Service (DoS) attacks as well as enhance protection of system resources from computer-worms like the Nimda and Code Red.

Press release:

< <http://www.net-security.org/text/press/1006396865,52102,.shtml> >

Featured products

The HNS Security Database is located at:
<http://www.security-db.com>

Submissions for the database can be sent to: staff@net-security.org

ADVANCED FORENSICS TRAINING

An in-depth look at computer crimes and how to deal with them, one of the most important areas in information technology today...

This three-day course describes the methods used in the investigation of computer crimes. It deals with the need for proper investigation and illustrates the process of locating, handling and processing computer evidence. We also discuss when and why you might want to notify law enforcement and how to foster effective working relationships with them.

Read more:

< <http://www.security-db.com/product.php?id=916> >

This is a product of Security University, for more information:

< <http://www.security-db.com/company.php?id=222> >

VULNERABILITY ANALYSIS

Determines the current level of vulnerabilities of external and/or internal networks or computer systems. The analysis will list potential security weaknesses at a given point in time.

Read more:

< <http://www.security-db.com/product.php?id=813> >

This is a product of Breakwater, for more information:

< <http://www.security-db.com/company.php?id=191> >

OPSEC SOLUTIONS

In addition to the billable services described in the Enforcement Point section, Check Point's SVN for Managed Service Providers is also integrates at the Application Program Interface (API) level, solutions from over 200 partners. These partners provide solutions for Content Security, Authentication and Authorization, Intrusion Detection, Event Analysis and Reporting, High Availability, Secured Operation Systems, Directory Services, and PKI Products and Services. [Click here for an overview.](#)

Read more:

< <http://www.security-db.com/product.php?id=428> >

This is a product of Check Point, for more information:
< <http://www.security-db.com/company.php?id=93> >

=====
Help Net Security T-Shirt available
=====

Thanks to our affiliate Jinx Hackwear we are offering you the opportunity to wear a nifty HNS shirt :) The image speaks for itself so follow the link and get yourself one.

Get one here: <http://207.21.213.175:8000/ss?click&jinx&3af04db0>

=====
Security Software

All programs are located at:
<http://net-security.org/various/software>

PHOTOLACER 1.1

Photolacer's purpose is to allow the user to control his or her privacy. The program allows the user to create secret documents, protect them, communicate them to others, and destroy them. Photolacer allows you to encrypt data (files from your disk or a message you create from within Photolacer), save the encrypted data, and optionally send it to an e-mail recipient. The program also allows you to hide the encrypted data within a set of JPEG images.

Info/Download:

< <http://www.net-security.org/various/software/1006790616,38625,windows.shtml> >

CSSS 2.2

CSSS program provides effective premises guarding by means of a microphone or several microphones, which act as sensors and a modem, which acts as a signaling (informing) device. The CSSS principle of action consists in microphone (microphones) survey on the scale of real time and highly intellectual analysis of coming signals on the basis of special algorithms based on the methods of speech recognition. Due to the flexible system of tooling the user is able to adjust the action of the program himself in accordance with the specific requirements of the premises. The system can be adjusted for different frequency ranges and different levels of average total sound signals amount received from the microphone or all microphones in the system. So, it's possible to adjust the system e.g. for human steps only (low frequency sound signals) i.e. the level will start rising considerably after the appearance of low frequency sound signals. There is a function of scaring away, with the help of sound files playback (siren), and also recording of a sound on the disk. In case of voice modem usage, there is a possibility of listening of a guarded room by telephone.

Info/Download:

< <http://www.net-security.org/various/software/1006790806,87113,windows.shtml> >

DIABLO KEYS 2.2

Diablo Keys is a freeware advanced windows32 keylogger. A keylogger is a small program that logs all activity on a system, including keystrokes, windows captions, day and time, saving all to a file in the HD, and then you can see things like.. chats, passwords, documents... Diablo Keys is a trojan/tool that you can use to spy anyone and even you are the administrator of your system you can warn users that are being spy.

Info/Download:

< <http://www.net-security.org/various/software/1006791482,47466,windows.shtml> >

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>

<http://security-db.com>