

HNS Newsletter
Issue 79 - 17.08.2001
<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

=====
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>

The site has been updated in various areas: a new database, a new layout and we removed the advertisement banners making the site faster to load.

=====

General security news

HACKING, YOUTH MARK INTERNET

Half of China's Internet users claim they've been hacked in the past year, a startling new study on domestic Internet trends indicated. The data points to an alarming level of carelessness and ignorance about security among online users, a population that tends to be younger and less affluent than the general public.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www1.chinadaily.com.cn/itchina/2001-09-10/32042.html>

GPG: THE BEST FREE CRYPTO YOU AREN'T USING, PART I

Ten years after Phil Zimmermann released PGP v.1.0 (Pretty Good Privacy), PGP has evolved from an underground tool for paranoiacs to the gold standard,

even an internet standard, for e-mail encryption. GnuPG, the GNU Privacy Guard, is a 100% free alternative to commercial PGP and is included in most Linux distributions. And yet, not nearly as many people who need it (and already have it) use it.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/lj-issues/issue89/4828.html>

VIRUS THREATS IGNORED BY EMPLOYEES

IT managers are coming under renewed pressure to draw up clear email security policies that are readily understood by users. The advice follows evidence that despite recent high-profile virus attacks, individual users are still not changing their online security practices.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094855,00.html>

PUBLIC KEY INFRASTRUCTURE OVERVIEW

Today's Internet clientele demand stringent security protocols to protect their interests, privacy, communication, value exchange, and information assets. This article demonstrates how public key cryptography supports risk management requirements and solves e-commerce security problems in heterogeneous network environments.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sun.com/blueprints/0801/publickey.html>

INFORMATION WARFARE: HOW TO SURVIVE CYBER ATTACKS - REVIEW

Every chapter is concluded by a high-level agenda for action, mostly targeted to government and big business. The book suggests that the best way to prevent future "ruinous" cyberattacks is to establish a "super cyber patrol" for the Internet. Another suggestion is that computer users maintain constant battle readiness, a scenario analogous to the Cold War, in order to thwart potential attacks.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securitywatch.com/lit/network_security/infowar.html

DUBLIN TEAM CRACKS CHILD PORN CODE

Two Dublin biologists developed the tracking device, which can detect pornographic images hidden behind computer code or in otherwise inaccessible files. The technology was first created to identify breast cancer in tissue images.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunday-times.co.uk/news/pages/sti/2001/09/09/stiireire01015.html>

VIRUS-MANIA: HOW MICROSOFT GETS OFF LIGHTLY

During the recent state of heightened awareness induced by the Code Red virus, one central fact was overlooked in virtually reports - you could only be affected if you were running Windows. And as Robert Cringely writes in his latest column, the forthcoming Windows XP is very likely to increase the frequency virus and worm attacks. So why is it that no-one is laying the blame for this at Microsoft's doors.

Link:

<http://www.macuser.co.uk/SpyDa/php3/openframe.php3?page=/newnews/newsarticle.php3?id=1266>

CODE BLUE COULD BE MISGUIDED BUT GOOD WORM

"It is possible that Code Blue was created to cause chaos and to change configuration of the Internet Information Server so that Code Red can no longer spread," says Allan Dyer, chief consultant at Yui Kee Computing, an antivirus and network security firm in Hong Kong.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,61424,00.asp>

SPAM PUTS PAYHOUND IN THE PRIVACY DOGHOUSE

Web payment firm PayHound sent out a promotional email Sept 7 that revealed the addresses of thousands of recipients to its mailing list. The message does not specifically infringe any of the terms of the UK start-up's privacy policy, but it flies in the face of accepted Internet standards - particularly for a firm whose business is to act as an online cash wallet, keeping users' details private and secure.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21584.html>

COMPUTER VIRUSES: CAN WE EVER OUTSMART THEM?

Anticipating a new breed of computer viruses capable of self-spreading and cross-infecting with cutting-edge effectiveness, antivirus experts are refining the "behavioral" approach to malicious code to create software that can out-think a virus.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsfactor.com/perl/story/13450.html>

VIRTUAL PRIVATE NETWORKS: A BROKEN DREAM?

Virtual Private Networks allow organizations to establish secure links with business partners and extend communications to regional and isolated offices. In doing so, they significantly diminish the cost of communications for an increasingly mobile workforce. While VPNs are gaining widespread acceptance as security solutions, they are not a panacea. This article will serve as a brief introduction to VPN technology. It will also illustrate some vulnerabilities that have been discovered in VPNs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/basics/articles/vpn.html>

CYBERCRIME TREATY MAY NOT CUT IT

The first international treaty to combat cybercrime, including malicious hacking, financial fraud, and child pornography over the Internet, is headed for ratification by the Council of Europe this November. Given the global nature of Internet crime, the treaty is an essential first step. But critics say it doesn't go far enough to protect privacy and individual rights.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://msnbc.com/news/626859.asp>

WORLD'S FIRST DECSS EXECUTABLE PRIME NUMBER

Mathematician Phil Carmody, who in March of this year managed to encode the DeCSS source in a prime number, has upped the ante by producing a prime number which represents an executable version of the banned CSS descrambler.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21591.html>

HACKERS CLEAN UP IN ONLINE CASINOS

Call it the gambling industry's dirty little secret. Hackers are sabotaging online casinos with greater regularity, security and gambling experts say, in some cases scamming large sums of money from the gaming firms.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094955,00.html>

SECURITY STILL THE BIG ISSUE

Survey results released last week by Computing Economics, Market Resources and Computing/PwC all show security at the top of the IT agenda still. And, given the cost figures produced by the first of these, it's hardly surprising.

Link: <http://www.it-director.com/article.php?id=2160>

PUNTERS CHANGE PRICES ON VIRGIN INTERACTIVE SITE

Virgin Interactive has said it will not honour orders made on its Web site if consumers have altered the price of games software. The statement comes after a reader discovered that a simple bit of cutting and pasting could allow punters to change the price of the console games on offer. And he was right. We gave it a go. And it was easy. We could have ordered scores of Playstation and Dreamcast titles for next to nothing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21595.html>

FBI OPERATION PENETRATES HACKER UNDERGROUND

The FBI has gained a foothold in the hacker underground thanks to an 18 month undercover operation launched during the height of the U.S. military's 1999 bombing campaign in Kosovo. What started out as a Defense Department operation designed to ferret out pro-Serbian hackers responsible for the April 1999 denial-of-service attacks against U.S. government and NATO Web sites soon led to the first coordinated undercover operation targeting U.S.-based hackers.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO63711,00.html

REDUCE FALSE POSITIVES AND FALSE NEGATIVES IN NIDS

By providing an additional layer of protection above and beyond access control devices such as a firewall, network-based intrusion detection systems (NIDS) can be a valuable addition to the security arsenal. However, NIDS has been criticized for its propensity to generate a perceived large amount of false positives and false negatives. This article is the first of a two-part series that will offer an overview of network-based intrusion detection and false reports. This installment will offer a brief overview of NIDS devices and will examine how and why false reports take place.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityfocus.com/focus/ids/articles/falsealarm1.html>

AKAMAI CTO KILLED IN ASSAULT

Daniel C. Lewin of Akamai Technologies was killed in an American Airlines plane crash at the World Trade Center. He was the co-founder, chief technology officer and board member of Akamai. Lewin, 31, and is survived by his wife and two sons.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,46710,00.html>

US TERRORIST ATTACKS KNOCK NEWS SITES OFF INTERNET

The incredible spate of terrorist attacks has knocked most the world's news sites off the Internet as people tried to find out the latest news. CNN has been offline ever since the news that a second plane had crashed into the World trade Center. MSNBC was available for a short while but seems to have disappeared as well following the posting of a video of the second plane crashing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/21606.html>

ANTI-ATTACK FEDS PUSH CARNIVORE

Federal police are reportedly increasing Internet surveillance after Tuesday's deadly attacks on the World Trade Center and the Pentagon. Just hours after three airplanes smashed into the buildings in what some U.S. legislators have dubbed a second Pearl Harbor, FBI agents began to visit Web-based, e-mail firms and network providers, according to engineers at those companies who spoke on condition of anonymity. An administrator at one major network service provider said that FBI agents showed up at his workplace on Tuesday "with a couple of Carnivores, requesting permission to place them in our core, along with offers to actually pay for circuits and costs."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46747,00.html>

IN WAKE OF ATTACKS, FEDS REVIEW CYBER-SECURITY

One day after terrorist attacks shook the nation's capital and the heart of the country's financial world, the U.S. federal government is taking another look at weaknesses that invite attacks on federal computer systems. And so far, it doesn't look good, according to the federal government's chief auditing agency.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/170024.html>

PRIVACY VS. SECURITY?

Wharton professor says open access to the Internet also creates a vulnerability and society must decide if it is prepared to give up some privacy to gain security. But director of technology institute sees no need for restrictions.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.informationweek.com/story/IWK20010912S0009>

DID ENCRYPTION EMPOWER THESE TERRORISTS?

"Well, I guess this is the end now..." So wrote the first Netizen to address the tragedy on the popular discussion group, sci.crypt. The posting was referring what seems like an inevitable reaction to the horrific terrorist act: an attempt to roll back recent relaxations on encryption tools, on the theory that cryptography helped cloak preparations for the deadly events.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/627390.asp>

HACKERS DISCUSS RETALIATORY CYBERSTRIKES

Although the U.S. government has yet to publicly identify suspects in Tuesday's terrorist attacks on America, some hackers are already plotting counterstrikes against Islamic Web sites, according to postings in Internet newsgroups. So far, the impact of the planned retaliatory hacking has been limited.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/170025.html>

INSECURE ABOUT MICROSOFT SECURITY

Windows aims to ease the struggle of computing for users not able to fathom the task. It is interactive, sometimes to an annoying degree, and it aims to prevent users from making accidental mistakes, which could harm the overall integrity of the operating system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.osopinion.com/perl/story/13482.html>

AIRPORT SECURITY TECHNOLOGY UNDER SCRUTINY

Tuesday's terrorist attacks have some leading aviation experts calling for improved technology and beefed-up surveillance at the nation's airports - regardless of privacy advocates' concerns. Security experts are particularly bullish on face-recognition technology and other so-called biometric security devices.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-7141717.html>

MAFIABOY GETS EIGHT MONTHS

Mafiaboy has been sentenced to eight months in a youth detention centre, a move welcomed by prosecutors as a strong message against the world's hacking community.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2095156,00.html>

AUTOMATIC PATCHING: ARE WE GOING TO BE SAFE FROM WORMS?

Worms and viruses often target specific vulnerabilities in common software. But what if the terms were reversed? Rather than attacking the vulnerability of software for malicious purposes, what if the worm or virus actually attempted to secure the software by applying a patch? Like it or not, it is already happening.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2811976,00.html>

AN AUDIT OF ACTIVE DIRECTORY SECURITY, PART THREE

This article is the third in a series devoted to discussing security issues surrounding Active Directory, also known as AD. The first article offered a brief overview of Active Directory. The second article offered an overview of the security implications of AD's default settings. This article will offer an overview of the relationship between LDAP, SASL and Kerberos, and examine what they have to do with Active Directory Security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/2k/adaudit3.html>

MIDDLE EAST ATTACKS

As posted on Incidents mailing list by John - "An associate of mine who monitors certain IRC channels has let me know that a group of individuals are discussing plans to attack domains located in the middle east. I don't have all of details at this point, but it seems a few of them have private codes they might use. I don't know what the private codes affect or if they even have them, but that's what I have been told. I would just like to let all the admins on this list know before these ignorant individuals start these attacks. I'm not aware of any denial of service attacks or distributed denial of service attacks as of yet."

ANOTHER POST FROM INCIDENTS LIST

As posted on Incidents mailing list by Ben Venzke - "A number of 'hackers' have begun calling for and attacking both Arab nation state networks and terrorist related sites. If they begin to meet with some success we can expect a significant response along the lines of the attacks by pro-Palestinian actors during the Israeli-Palestinian Cyber Conflict almost a year ago."

TERRORIST SEARCH LEADS TO ISPS

Both America Online and EarthLink acknowledged that they are working with the FBI to turn over specific information that may be relevant to the case. "We are cooperating with them in this ongoing investigation," said Nicholas Graham, spokesman for AOL. Although Graham wouldn't provide details, he denied reports that the company had agreed to install a Carnivore surveillance system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-7141812.html>

SPOOK, ENCRYPTION TOOL FOR DATA SECURITY

BlackHole Corp. has launched Spook, an integrated software based data security solution. Concealment is a special feature of Spook that allows encrypted data to be stored either to an existing non-overlaid DOS executable file or floppy disk.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ciol.com/content/news/repts/101091303.asp>

SECURITY BUGWARE CLOSED

Well known security vulnerability archive "Security Bugware" which operated since 1996, stopped working a few days ago. Hrvoje Crvelin, its sole administrator, decided to stop updating the site due to lack of time.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://oliver.efri.hr/~crv/security/bugs/>

ANNA VIRUS WRITER GOES ON TRIAL

Jan de Wit, the 20-year-old who wrote the Anna Kournikova virus, went to trial, but the prosecutor asked for a relatively light sentence with no jail term - 240 hours of community service.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2095252,00.html>

INTERVIEW WITH ELIAS LEVY

Elias Levy, or Aleph1 is the bugtraq moderator one of the most important security mailing list of the world.

Link: <http://www.underlinux.com.br/sections.php?op=viewarticle&artid=92>

FLUFFI BUNNI GOES JIHAD

An undisclosed number of Web sites have had their front page redirected by "Fluffi Bunni" in response to the events that have shaken the world. They all appear to be victims of a hacking of the DNS of NetNames, a domain name registrar. Entitled "Fluffi Bunni goes Jihad", those behind the hack say: "If you want to see the internet again, give us Mr Bin Laden and \$5 million in a brown paper bag. Love Fluffi B."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/57/21668.html>

CONGRESS MULLS STIFF CRYPTO LAWS

The encryption wars have begun. For nearly a decade, privacy mavens have been worrying that a terrorist attack could prompt Congress to ban communications-scrambling products that frustrate both police wiretaps and U.S. intelligence agencies. Tuesday's catastrophe, which shed more blood on American soil than any event since the Civil War, appears to have started that process.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46816,00.html>

DON'T OVERLOOK STAFF IN DISASTER RECOVERY

For a group of IT professionals, now bound not only by the industry but also by the horrific events of Sept. 11, disaster planning and recovery has taken on a whole new meaning. For them, more important than data recovery is ensuring you have the people to implement the plan in the first place.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2812179,00.html>

EX-HACKER OFFERS \$10 MILLION REWARD

Germany's most flamboyant Internet multi-millionaire Kim Schmitz offered up to \$10 million on Thursday for information leading to the arrest of Osama bin Laden in the wake of terror attacks against the United States.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/newsbursts/0,7407,2812189,00.html>

GOOD VIRUSES HAVE A FUTURE

The concept of a self-replicating program was born in 1949, when computer pioneer John von Neumann presented a paper on the Theory and Organization of Complicated Automata. Many of us have come to call such programs computer viruses, and we rarely do so with fondness. The popular belief is that viruses are bad. But two newly-released programs have challenged that belief, and renewed an old debate: should we create and launch so-called 'good' computer viruses to combat the bad ones?

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.businessweek.com/technology/content/sep2001/tc20010913_1182.htm

CHINA NABS FIRST HACKER

Police have arrested a computer student suspected of littering government-run Web sites with pornography in China's first seizure of a hacker. Police in the central province of Hubei detained 19-year-old Wang Qun last month on suspicion of posting erotica on the homepage of a well-known science Web site, the news agency said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/newsbursts/0,7407,2812412,00.html>

GNU-DARWIN AUTHENTICATION AND ENCRYPTION POSITION PAPER

Dr. Michael L. Love writes: "Personal encryption tools, such as GnuPG, are vital to our strength as a nation, and such tools should be promoted in order to enhance the security of our individual citizens and of our vital institutions as well."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://gnu-darwin.sourceforge.net/war.html>

SECURITY AUDITS PAY DIVIDENDS

The widespread perception that security does not offer a return on investment is wrong, according to IBM Global Services. Speaking at a recent briefing, IBM security specialist James Luke commented, "[Installing security products] is not a zero-return investment. Firms need to look at the broader benefits."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2095311,00.html>

HACKERS DIVIDED OVER RESPONSE TO TERRORISM

Groups of online vandals and hackers are split over how to respond to this week's terrorist attacks on the WTC and the Pentagon, with some Internet vigilantes calling for an assault on perceived terrorist sites and others pleading for calm.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-7166935.html>

CCC HACKERS URGE RESTRAINT

Members of Germany's famed Chaos Computer Club gathered expecting to celebrate the group's 20th anniversary by talking up the joys of hacking. Instead, they have been spending their time urging their fellow hackers around the world not to hack.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,46868,00.html>

MAC SECURITY SITES WILL RETURN

Mantra contributed - "SecureMac.com and the other Macintosh Security sites which have been down over the past 2 weeks will resume its traffic once the server is returned. The scsi controller went out on the IBM Netfinity 4000r a few weeks back and the team has just been awaiting the return of the server."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.macsecurity.org/>

NEW ISSUE OF CRYPTO-GRAM IS HERE

Crypto-Gram is a free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography. This

month's Crypto-Gram discusses NSA's Dual Counter Mode, the new Microsoft Root Certificate Program, and more.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.counterpane.com/crypto-gram-0109.html>

Security issues

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

RLMADMIN V3.8M VIEW FILE SYMLINK VULNERABILITY

rlmadmin is a user management utility for RADIUS which comes with the Merit AAA Server package. Using this program and a simple symlink, you can view any file on the system as root.

Link: <http://www.net-security.org/text/bugs/1000121344,64585,.shtml>

VULNERABILITIES IN PAM AND NSS MODULES

During investigating the problem described in RUS-CERT Advisory 2001-08:01, it became evident that a few PAM and NSS modules which use PostgreSQL as database backend are vulnerable to SQL code injections attacks, too.

Link: <http://www.net-security.org/text/bugs/1000205174,68436,.shtml>

OPENLINUX - UUCP ARGUMENT HANDLING PROBLEMS

There is a argument handling problem which allows a local attacker to gain access to the uucp group. Using this access the attacker could use badly written scripts to gain access to the root account.

Link: <http://www.net-security.org/text/bugs/1000205544,97679,.shtml>

NEW BUGZILLA PACKAGES FOR REDHAT LINUX

The updated bugzilla package fixes numerous security issues which were present in previous releases of bugzilla.

Link: <http://www.net-security.org/text/bugs/1000205603,69143,.shtml>

SUSE LINUX APACHE-CONTRIB PROBLEMS

The Apache module mod_auth_mysql 1.4, which is shipped since SuSE Linux 7.1, was found vulnerable to possible bypass authentication by MySQL command injection. An adversary could insert MySQL commands along with a password and these commands will be interpreted by MySQL while mod_auth_mysql is doing the password lookup in the database. A positive authentication could be returned.

Link: <http://www.net-security.org/text/bugs/1000205772,10543,.shtml>

SECURITY PROBLEMS IN APACHE ON MAC OS X

We've already seen the security problems (or potential problems) in Apache on MacOSX associated to the case-insensitivity of HFS+. By exploiting the case insensitivity of HFS+, an attacker can evade Apache's access controls.

Link: <http://www.net-security.org/text/bugs/1000205966,4603,.shtml>

IBM AIX: BUFFER OVERFLOW VULNERABILITIES IN LPD

The Line Printer daemon, lpd, shipped with AIX contains several buffer overflow vulnerabilities that potentially allow a malicious remote user to gain root privileges. Two of the three vulnerabilities found require the attacker's system be listed in /etc/hosts.lpd or /etc/hosts.equiv. The third requires that the malicious user have control over the victim's domain name server (DNS).

Link: <http://www.net-security.org/text/bugs/1000289758,59583,.shtml>

NETOP SCHOOL ADMIN FOR WINDOWS 2000 VULNERABILITY

The problem arises in the way that netOP handles no authorised users. When netop school is installed on a local area network, Full control of the network and all work stations can be taken.

Link: <http://www.net-security.org/text/bugs/1000289924,52129,.shtml>

SPEECHIO.ORG SPEECHD VULNERABILITY

there is a vulnerability in speechd that allows you to run arbitrary code as the root user or whoever is running speechd (hopefully not root!).

Link: <http://www.net-security.org/text/bugs/1000290049,90772,.shtml>

MANDRAKE LINUX - XLI/XLOADIMAGE UPDATE

A buffer overflow exists in xli due to missing boundary checks. This could be triggered by an external attacker to execute commands on the victim's machine. An exploit is publically available. xli is an image viewer that is used by Netscape's plugger to display TIFF, PNG, and Sun-Raster images.

Link: <http://www.net-security.org/text/bugs/1000379368,57356,.shtml>

PROBLEMS WITH TREND MICRO INTERSCAN EMANAGER

Trend Micro InterScan eManager for NT contains buffer overflow vulnerability. It may allow an attacker to execute arbitrary codes remotely with Local System context.

Link: <http://www.net-security.org/text/bugs/1000380157,97666,.shtml>

VULNERABLE SSL IMPLEMENTATION IN ICDN

A security vulnerability has been discovered in version 3.x of the RSA BSAFE SSL-J Software Developer Kit made by RSA Security. This vulnerability enables an attacker to establish a Secure Socket Layer (SSL) session with the server, bypassing the client authentication and using a bogus client certificate.

Link: <http://www.net-security.org/text/bugs/1000380628,25889,.shtml>

MYOWNEMAIL.COM VULNERABLE TO SCRIPT ATTACK

Whenever you login to a Myownemail account the inbox is opened. If you send a email with a specially formed "from" field, which usually contains a name, you can execute javascript, vbscript, etc. on the computer of the

person who logged in.

Link: <http://www.net-security.org/text/bugs/1000380721,43134,.shtml>

HUSHMAIL.COM VULNERABLE TO SCRIPT ATTACK

Whenever you login to a Hushmail account the inbox is opened. If you send a email with a specially formed "from" field, which usually contains a name, you can execute javascript, vbscript, etc. on the computer of the person who logged in. This also works for the "topic" field.

Link: <http://www.net-security.org/text/bugs/1000380786,77175,.shtml>

YAHOO FRANCE SITE VULNERABLE TO CROSS SITE SCRIPTING

French Yahoo's web site may inadvertently include malicious HTML tags or script in a dynamically generated page based on unvalidated input from user.

Link: <http://www.net-security.org/text/bugs/1000472878,10897,.shtml>

PASSWORD SAFE LEAK OF INFORMATION

Password Safe has an option (I think is default) to "lock password database on minimize and prompt on restore" and is doing a good job, at least this is what I can tell, without source. And looks like is cleaning the memory so there are no username/passwords exposed (this is what you expect from a good designed password utility). However, in some cases the last entered username remains in memory exposed in cleartext. This is happening for example if the user had on the screen the window with "Would you like to set "example_user" as your default username?" This could be also a windows memory management problem, and there is probably a workaround.

Link: <http://www.net-security.org/text/bugs/1000473122,66156,.shtml>

BANK OF AMERICA ONLINE BANKING SECURITY

Users of the Bank of America Online Banking website are vulnerable to a basic web security hole.

Link: <http://www.net-security.org/text/bugs/1000567966,9480,.shtml>

MICROSOFT INDEX SERVER 2.0 PATH REVEALING

The Index Server Sample file SQLQHit.asp shipped with Microsoft Index Server 2.0 and Option pack 4.0 , is installed under the directory "/inetpub/iissamples/ISSamples/" by default. SQLQHit.asp file is used for SQL based Search, can be used by a malicious user to gather information about files in virtual folders under certain conditions.

Link: <http://www.net-security.org/text/bugs/1000568665,7826,.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>

PROCHECKUP LAUNCH NEW SERVICE FOR WEB SERVERS - [10.09.2001]

London based Internet Security company ProCheckUp Ltd are set to launch an additional service based on their successful Artificial Intelligence technology - ProCheckNet. ProCheckWeb is a fully automated sub-set of ProCheckNet, and is used specifically for finding security vulnerabilities on public web servers.

Press release:

< <http://www.net-security.org/text/press/1000121543,89329,.shtml> >

TECHTRACKER DESKTOP 2.0 CHECKS YOUR SOFTWARE - [10.09.2001]

TechTracker, Inc., a provider of computer stability solutions, announced the availability of TechTracker Desktop 2.0. TechTracker Desktop is a software utility designed to simplify the time-consuming task of software version management and extend the life of software through proactive alerts of available updates, patches and upgrades for the software on a user's computer.

Press release:

< <http://www.net-security.org/text/press/1000122177,5851,.shtml> >

ZONE LABS ZONEALARM SOFTWARE STOPS MAGISTR.B - [10.09.2001]

Recent reports indicate that a new strain of the Magistr virus (Magistr.B) can disable ZoneAlarm and ZoneAlarm Pro. According to our tests, these reports are false. ZoneAlarm 2.6 and ZoneAlarm Pro 2.6 continue to protect PCs, even if Magistr.B is present and will deny the virus access to the Internet.

Press release:

< <http://www.net-security.org/text/press/1000122247,16588,.shtml> >

Magistr.B information:

< <http://www.net-security.org/text/viruses/999613294,89500,low.shtml> >

OKENA ANNOUNCES STORMWATCH 2.0 - [10.09.2001]

OKENA, Inc., the leading developer of proactive security software, announced the general availability of StormWatch 2.0 on Windows 2000 and NT. This new release of OKENA's flagship product provides out-of-the-box, enterprise-level protection against intrusions with increased scalability and easier installation,

management and usability. StormWatch 2.0 brings uncompromising intrusion prevention security to the enterprise by deploying intelligent agents on desktops and servers that defend against the proliferation of attacks across networks.

Press release:

< <http://www.net-security.org/text/press/1000137728,4115,.shtml> >

MCAFEE.COM LAUNCHES MCAFEE VISUAL TRACE - [11.09.2001]

McAfee.com, a leading provider of Web security services, announced the launch of McAfee Visual Trace (MVT), a graphical trace-route utility that gives users the ability to trace the network path from their computer or host to a target system anywhere on the Internet. This new service combined with McAfee.com's Personal Firewall service, gives PC users the ability to protect themselves against hackers and other online threats and trace these threats to the source.

Press release:

< <http://www.net-security.org/text/press/1000205041,12444,.shtml> >

ORACLE SECURITY HANDBOOK RELEASED - [11.09.2001]

According to a recent Computer Security Institute & FBI poll, companies reported annual increases of more than 35% per year in data in network sabotage incidents from 1997 to 2000. Before the Internet revolution, databases and their products and services were so well hidden in the darkest depths of customers' data centers that they simply didn't register on the radar of hackers, crackers and other attackers. The Internet has opened up the availability of companies' vital information, and with that it has become increasingly important for companies to be well prepared for the onslaught of malicious internal and external security attackers.

Press release:

< <http://www.net-security.org/text/press/1000206151,98107,.shtml> >

@STAKE EXPERTS TO KEYNOTE RSA SECURITY SEMINAR - [11.09.2001]

@stake Inc., the world's leading digital security consulting firm, announced that several of its executives including Dr. Daniel Geer, chief technology officer, and Chris Wysopal, director of Research & Development, will serve as the keynote speakers for RSA Security's seminar series on "Web Security Issues and Technologies." These free, half-day seminars will be held over the next three months in 16 cities across the United States. They are geared toward developers and business executives who are serious about their company's security initiatives. The @stake keynote will discuss new approaches to security and examples of how leading companies are addressing security.

Press release:

< <http://www.net-security.org/text/press/1000207615,56208,.shtml> >

REAL NETWORK SECURITY RISKS REMAIN UNDERESTIMATED - [11.09.2001]

An Inside Out Look at Enterprise Security" - a white paper by Cryptek Secure Communications is now available. Despite attention to hackers, viruses and sensational Web site attacks, the most serious security threats still go unaddressed. Learn about enterprise security oversights and the next generation solutions for protecting trade secrets, patents, business plans, databases and other invaluable corporate information assets in today's networked economy.

Press release:

< <http://www.net-security.org/text/press/1000207813,55473,.shtml> >

HACKERS EERILY QUIET ON TERRORIST ATTACK DAY - [13.09.2001]

Hacking activity on September 11, 2001 was "eerily quiet" according to Skoudis. While observing the activities of computer hackers on three probes monitoring Internet traffic located at the World Trade Center, he was surprised to see the lack of activity. When the hijacked planes hit the structures, the probes continued to function. The probes "flat-lined" as the buildings collapsed.

Press release:

< <http://www.net-security.org/text/press/1000381557,80791,.shtml> >

IDC DECLARES TREND MICRO SERVER-BASED AV LEADER - [14.09.2001]

According to a recently published report from International Data Corporation (IDC), Trend Micro Inc. dominates the antivirus market as the worldwide leader in server-based antivirus software sales, including Internet gateway (Web server) and Groupware virus protection. The study by IDC titled, "Antivirus Software: A Segmentation of the Market," follows an earlier July 2001, IDC report titled, "Worldwide Anti-virus Software Market Forecast and Analysis, 2000-2001," which found Trend Micro to be the fastest growing antivirus vendor with an annual growth rate of 51% in the year 2000.

Press release:

< <http://www.net-security.org/text/press/1000474375,76621,.shtml> >

SUSPECTED KOURNIKOVA VIRUS AUTHOR IN DOCK - [15.09.2001]

Sophos Anti-Virus is calling for businesses to report virus infections to the authorities, in order to provide evidence of the amount of damage viruses can cause. Evidence submitted by the FBI at the trial in the Netherlands of the suspected author of the Kournikova worm shows US investigators were only able to list 55 incidents of infection, causing just \$166,827 worth of damage. Jan de Wit, aka OnTheFly, is alleged to have unleashed

the Anna Kournikova worm in February of this year, and computer virus experts estimate millions of computer users around the world were affected.

Press release:

< <http://www.net-security.org/text/press/1000568868,90499,.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

BIOMOUSE

The Ankari BioMouse desktop fingerprint scanner replaces traditional passwords with a simple fingerprint scan. BioMouse marries high security with convenience by providing a method of positive identification that cannot be lost, stolen, shared or forgotten. Password proliferation is a critical security issue in most large enterprises. BioMouse, combined with corporate Public Key Infrastructure (PKI) or controlled usage of custom applications, removes this issue and increases the security of your network.

Read more:

< <http://www.security-db.com/product.php?id=1120> >

This is a product of Ankari, for more information:

< <http://www.security-db.com/company.php?id=257> >

CYBERTRACE

The CyberTrace client is the world's first Network Security Management System. Any systems administrator knows that it is difficult, if not impossible, to tell what is going on on the network. When they use tcpdump, or the Lanalyzer they have to be an expert to wade through the data. Even if your company has an expert, better use can be made of that expertise than doing the drudge work of data reduction. What you need is a tool that not only collects the network traffic but makes a judgment as to what looks suspicious. Because CyberTrace flags connections high priority with numbers, 0-10 an administrator can review the highlights and even replay those sessions and ignore connections with low priorities numbers, 30-100.

Read more:

< <http://www.security-db.com/product.php?id=1151> >

This is a product of Ryan Net Works, for more information:
< <http://www.security-db.com/company.php?id=268> >

VERIVOICE SL

The VeriVoice Security Lock is a patented voice verification technology that provides a fast, highly accurate, and customizable solution for identification of enrolled users. There are two implementations of the SL. One for recording and verification over a microphone and one for recording and verification over a telephone.

Read more:
< <http://www.security-db.com/product.php?id=1147> >

This is a product of VeriVoice, for more information:
< <http://www.security-db.com/company.php?id=264> >

Security Software

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

TCPTRACEROUTE 1.2

tcptraceroute is a traceroute implementation using TCP packets. The more traditional traceroute(8) sends out either UDP or ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets are taking to reach the destination. The problem is that with the widespread use of firewalls on the modern Internet, many of the packets that traceroute(8) sends out end up being filtered, making it impossible to completely trace the path to the destination. However, in many cases, these firewalls will permit inbound TCP packets to specific ports that hosts sitting behind the firewall are listening for connections on. By sending out TCP SYN packets instead of UDP or ICMP ECHO packets, tcptraceroute is able to bypass the most common firewall filters.

Info/Download:
< <http://www.net-security.org/various/software/999570140,6382,linux.shtml> >

REMOTE PASSWORD ASSASSIN

Remote Password Assassin (RPA) is a powerful security tool to test passwords across networks. In a simple way, RPA is a Network Password Cracker using

Brute Force Attack and able to attack very common ports on servers. When RPA is finish it will generate a HTML report, easy to follow and detailing the session.

Info/Download:

< <http://www.net-security.org/various/software/999570268,83530,linux.shtml> >

WORKSTATION LOCK 3.2

WorkStation Lock provides a simple and effective way to password-protect your system without involving a screensaver. The program is easy to configure and requires no modifications to your current system configuration. Features include scheduled locking activation, remote update capability, online help, and easy access via the system tray. There is a command-line option, so only the administrator can terminate the program. Version 3.2 adds improved security for Windows 98/Me and Windows 2000.

Info/Download:

< <http://www.net-security.org/various/software/999774672,57872,windows.shtml> >

TK8 SAFE 1.4

TK8 Safe is useful when you have passwords to use and to remember. In addition to manage passwords, TK8 Safe will help you to keep also other sensitive information like serial numbers, bank properties etc. The program has many powerful features like send (click a mouse and you are logged in), run, customizable folder tree with unlimited folders, password generator, password bar, quick find etc. TK8 Safe files are protected with Blowfish encryption algorithm and are secure.

Info/Download:

< <http://www.net-security.org/various/software/999775291,42992,windows.shtml> >

TYPHON

Typhon, an updated version of Cerberus Internet Scanner, is a vulnerability assessment tool. It will scan a given host for known security holes and vulnerabilities. It does this by looking at the services offered by a host and each of these are examined for holes. For example, Typhon will check for over 180 known vulnerabilities in the web service or daemon offered by a server. Once a scan has been completed a report in HTML is produced detailing what security holes were found, the impact of those holes and how to fix them. Once these holes have been removed then the host will be more secure against attacks. As new vulnerabilities are discovered almost on a daily basis it is necessary to ensure that the Typhon is kept upto date and hosts are scanned on a regular basis.

Info/Download:

< <http://www.net-security.org/various/software/999866655,6627,windows.shtml> >

SMS SPOOF

SMS spoof is an application that allows you to send spoofed SMS messages with a palm pilot. It uses a dialup connection to an EMI/UCP-compatible SMSC. It works with a modem connected to the Palm, such as an IR link to a GSM phone with a built-in modem.

Info/Download:

< <http://www.net-security.org/various/software/999869858,13391,palm.shtml> >

NETBRUTE SCANNER SUITE 1.0.0.7

NetBrute (formerly NetView) is a suite of three security applications that allows to audit a site for security vulnerabilities. NetBrute scans a range of IP addresses for shared resources that have been shared via Microsoft File and Printer Sharing to see what types of resources are shared on a network and to warn the computer users if any unsecured resources are displayed.

Info/Download:

< <http://www.net-security.org/various/software/999870076,74458,windows.shtml> >

ADEOS 1.0

Adeos is an automated filesystem security scanner. It recursively walks all mounted filesystems on the local system, and attempts to identify common security concerns, such as SUID, and world-writeable files. The output is available as text or HTML, with either output type formatted in either report or list style. Text is written to stdout and may be redirected to a file, while HTML is written to a file named results.html in the local directory.

Info/Download:

< <http://www.net-security.org/various/software/999870516,57982,linux.shtml> >

=====
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>
=====

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org
<http://net-security.org>
<http://security-db.com>