

HNS Newsletter
Issue 77 - 03.09.2001
<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) Featured articles
- 6) 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

TAMING THE WILD NETFILTER

For those of you who have taken the plunge and upgraded from kernel 2.2.X (or even 2.0.X) to 2.4.X, congratulations. If, like a number of folks, you're running some form of firewall using either ipchains or ipfwadm, your scripts may work fine. But sooner or later you're probably going to want to upgrade. Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/lj-issues/issue89/4815.html>

CODE RED IS HERE TO STAY

Code Red will be around 'forever', warns the security expert who has detected a new variation of the Code Red II worm.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com.au/news/breakingnews/story/0,200020826,20257035,00.htm>

IETF LOOKS TO PROMOTE FIREWALL/VPN HARMONY

One of the annoying aspects of implementing VPNs - getting them to work across corporate firewalls - could be resolved soon based on work by the Internet Engineering Task Force. During its recent meeting in London, the standards-setting body reviewed a proposed standard for network address translation (NAT) that would spell out how IP Security VPN tunnels should traverse firewalls and other NAT devices.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/news/2001/0827vpnfirewall.html>

HACKERS' BONFIRE OF THE VANITIES

It's late on a dark, rainy Friday night as a team of some of Europe's best network security experts trawl the woods for a rogue base station. They weave between ghostly birch trees to hunt the hacker who has commandeered part of the wireless local area network (LAN) from inside his tent. Holding out laptops with antennas stuck to the top, the posse tracks base signals. They compare signals until they find one that doesn't match their map - the rogue station. But instead of hauling in the hacker, they politely ask him to turn off the offending station. It's all in a night's work at HAL2001, Europe's largest open-air hacking festival.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://it.mycareer.com.au/news/2001/08/28/FFXB6BYUQQC.html>

MICROSOFT PENETRATED

The security breach, which took place over a six-day period beginning August 12, involved a shopping server that was part of the Microsoft Network in Europe, as well as scores of workstations and servers located overseas. It looks like Microsoft had few servers with open file sharing with no passwords or password phrase being "password".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169408.html>

IF YOU LIKE NSA SELINUX ...

The NSA SELinux web site has been updated. It includes a completely new variant of the SELinux prototype based on the Linux Security Modules (LSM) work. This patches for the LSM-based prototype are based on the Linux 2.4.9 kernel, and the patches for the utilities are known to work with Red Hat Linux 7.1.

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

BRIGHT MARKET FORECAST, A NEW FIREWALL

A rosy forecast for the security-software market, a new firewall product and an industry partnership to combat distributed denial-of-service attacks were among the highlights in security last week.

Link: <http://www.crn.com/Sections/BreakingNews/dailyarchives.asp?ArticleID=29260>

INTRODUCTION TO SECURITY POLICIES, PART ONE

This is the first in a series of four articles devoted to discussing about how information security policies can be used as an active part of an organization's efforts to protect its valuable information assets. In a world that is essentially technology driven; where the latest IIS exploit is countered with a mad rush to install the relevant patch and where the number of different operating systems in a network exceeds the number of hairs on the security administrator's head that haven't turned gray, policies give us an opportunity to change the pace, slow things down and play the game on our own terms.

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

FALLACIES OF A SECURE AND PRIVATE INTERNET

A recent Gartner Group survey found that America Online is the least trusted company on the Web, at least compared to the other businesses on the survey, such as banks, brokerages, credit card companies, retailers like online bookseller Amazon.com and Microsoft. However, no matter what organization you are dealing with online, including the government, consumers cannot and should not realistically expect a 100 percent secure and private experience anywhere.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.osopinion.com/perl/story/13092.html>

CYPHERPUNK SENTENCED TO 10 YEARS

The judge didn't just throw the book at Jim Bell, he threw it twice and made him pay for extra damages. Bell, the Libertarian essayist and contributor to the Cypherpunk mailing list, was sentenced Friday to 10 years in prison for stalking Jeff Gordon, a federal agent who had been investigating his activities.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46341,00.html>

FUTURE IP SECURITY, PART I

This article outlines the future of IP addressing (IPv6) and focuses on the security components of next generation IP services (IPsec). We list major components of IPsec and describe their functionality in terms of the security services they provide. Part II will be devoted to end-user issues with IPsec protocols and their common implementations.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securitywatch.com/RES/August27.html>

US ATTORNEY ON BRIAN WEST NON-CRIME

An article posted on the internet last Friday reported that an internet service provider employee is alleged to have penetrated a hole in the comparative security of a newspaper's website, employed a userid and a password, and downloaded a valuable computer program. The employee reported the penetration to the website owner to include site insecurity, access using user names and passwords, and downloading the program, but claimed his intrusion accidental. The website owner reported the alleged intrusion to law enforcement authorities.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cryptome.org/west-usa.htm>

FOUR OUT OF FIVE PDAS OPEN TO HACKERS: SURVEY

Almost four out of five PDAs have been left unprotected against hacker attacks, a ZDNet reader poll has found. The poll found only 21 percent of respondents had taken measures to protect their handheld devices against unwanted intruders. That left 79 percent of PDAs without any protection.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com.au/news/breakingnews/story/0,2000020826,20257049,00.htm>

SLASHDOT READERS BLAMED FOR SITE DEFACEMENT

Shortly after the site was featured in an article in the New York Times, visitors to the home page of RegisteredToVoteOrNot.com were greeted by messages such as "Hacked by William S," or "Welcome to <http://www.worm.com>"; and "You Lose! Have fun at the EFF." An online version of the Times story, which discussed the problems of making public records available online, was linked to by Slashdot.org. The Slashdot story, "How Public Should Public Records Be?" included the name and birth date of New York Mayor Rudolph Guiliani so that readers could test the system. According to Michael Weiksner, chairman of E The People, the charitable organization that developed the site, vandals from Slashdot appear to have exploited a flaw in the site's comment board section.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169427.html>

ZOMBIES INVADING HOMES OVER CABLE

Speaking at the Securing the Financial Services World briefing in Sydney last week, Top Layer Networks Australian manager David Britt said a DoS attack could be generated using a small amount of bandwidth. As home users put their machines on broadband connections such as cable modems and DSL, which allowed them to leave their machines connected all the time, hackers were scenting rich pickings, Mr Britt said. "The connection-based DoS attacks we have seen recently are much more concerted and malicious than the old-style flooding attacks," he said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://australianit.news.com.au/common/storyPage/0,3811,2699850%25E442,00.html>

CHINESE MINISTRY REPORTS SITUATION OF CODE RED II

China's Ministry of Public Security (MPS) issued a report on the situation of the Code Red II computer virus in China, which has infected a large number of Chinese computer operating systems.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://english.peopledaily.com.cn/200108/28/eng20010828_78547.html

THE NEW BUSINESS FORTRESS: INTERNET MESSAGING SECURITY

As the Internet and email communications have become the lifeblood of many organisations in recent years, security risks have developed into a vulnerable front in the battlefield of business.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com.au/biztech/ebusiness/story/0,2000010339,20257051,00.htm>

NOKIA ADDS SMART CARDS TO SECURITY PORTFOLIO

Nokia Internet Communications announced it is adding a range of features to its line of virtual private network software, designed to make integration with public key infrastructure systems easier. The VPN offerings will also support smart card-based public key infrastructure for the first time.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2093915,00.html>

CLEAR AND PRESENT DANGER?

That's what a House subcommittee is investigating at hearings today, as it scrutinizes the government's current level of security in the wake of a series of recent computer attacks.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://abcnews.go.com/sections/scitech/DailyNews/govt_security010829.html

GET A FIREWALL

Home PC users are starting to catch on that surfing the Net requires a certain level of protection, security software makers say. "Folks are starting to see that firewalls are as important as antivirus," said Tom Powledge, group product manager for Symantec. "I think there is, for many, a sense of urgency."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdn/stories/news/0,4586,5096302,00.html>

CERT SUMMARY

Each quarter, the CERT Coordination Center issues the CERT Summary to draw attention to the types of attacks reported to our incident response team, as well as other noteworthy incident and vulnerability information. The summary includes pointers to sources of information for dealing with the problems.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/summaries/CS-2001-03.html>

HACKS A MILLION

Cybercrime is on the rise in the UK and, for the first time, businesses that are hit by hacks are more likely to be attacked by hackers from outside of the company instead of inside, according to a study published by the Confederation of British Industry. Of the 148 companies surveyed for the study Cybercrime Survey 2001, two thirds have been the victim of a 'serious' cybercrime in the past year, said CBI spokesman Roger Davidson.

Link: http://www.pcadvisor.co.uk/news/print_news.cfm?NewsID=1471

PARENTS DEFEND HACKER AT SENTENCING

Mafiaboy, who paralyzed several major Web sites, including CNN and Yahoo, needs structure, but should be spared further detention, his parents said at a sentencing hearing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-7004125.html>

DON'T GET MAD AT SIRCAM, GET EVEN

A new tool offers relief for computer users still plagued by e-mails infected with the file-stealing SirCam worm – or who have voyeuristic tendencies. ClipSirc is

a tiny DOS utility that automatically dissects the data files that come attached to messages generated by SirCam. Developed by Israeli anti-virus vendor Invircible, the free tool strips the worm's installation code from the legitimate document it uses as a Trojan horse.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169522.html>

GALLERY OF CSS DESCRAMBLERS

If code that can be directly compiled and executed may be suppressed under the DMCA, as Judge Kaplan asserts in his preliminary ruling, but a textual description of the same algorithm may not be suppressed, then where exactly should the line be drawn? This web site was created to explore this issue, and point out the absurdity of Judge Kaplan's position that source code can be legally differentiated from other forms of written expression.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cs.cmu.edu/~dst/DeCSS/Gallery/>

MANAGERS 'SLACK ON SECURITY'

Despite a succession of incidents involving viruses, worms, hackers and security "holes" in widely used software, real concern about computer security is still at a surprisingly low ebb, says Kentucky-based networking specialist Gary Porter. Porter, who holds Novell's Master CNE qualification, was a keynote speaker at Novell's "one Net summit" in Wellington last week. He was appointed to Novell's major accounts advisory board in 1996.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idgnet.co.nz/webhome.nsf/UNID/5584F084B7A09991CC256AB6000CA268!opendocument>

AN AUDIT OF ACTIVE DIRECTORY SECURITY

In the last article, there was a brief introduction to Active Directory as it relates to LDAP, NT 4 directory services, and a few other things. Understanding the structural and syntactical layout of an LDAP/AD database was also covered in brief. Lastly, some general thoughts were given out about the implications of making a computer network as integrated, reliant, and controlled by a massive directory service like AD. In this article, we'll begin to approach AD security implications in a more technical manner.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/aads2.html>

SYSADMIN SPY LEFT DIGITAL TRAIL

The FBI investigation that led to last week's arrest of a former Air Force sergeant on espionage charges had more in common with a modern Internet hacker hunt than a John le Carre novel, court records show.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21327.html>

TWO ARRESTED FOR TRYING TO SELL ENCRYPTION TO CHINA

U.S. Customs Service agents have arrested two men for allegedly attempting to export military-grade encryption technology to China. Authorities arrested Eugene You Tsai Hsu, of Blue Springs, Mo., and David Tzu Wvi Yang, of Temple City, Calif., accusing the two of plotting to export an encryption technology designed for use exclusively by the U.S. government.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169546.html>

SECURE THE WIRELESS NETWORK FIRMWARE

Security issues surrounding wireless networking can be addressed without upgrading hardware, Intel said today. The future ubiquity of wireless networking has been a key theme of the Intel Developer Forum this week, with much talk of a mobile computing future where laptop computers automatically select the best connection via either a wireless LAN or high-speed mobile network.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21343.html>

VISA PASSWORD? THAT WILL DO NICELY!

Ever since Internet shopping began there has been a constant stream of security issues that have affected the public's confidence in the safety of shopping online. The stories that have made the news are too numerous to mention but on several occasions a common theme stood out. Credit card details that shoppers had used to buy goods and services over the web were left unsecured on poorly protected servers and consequently the Internet hacking community picked up this information. Unsurprisingly, the stolen data was then often used in Web transactions to obtain goods fraudulently.

Link: <http://www.it-director.com/article.php?id=2126>

SECURITY MARKET: A DOUBLE EDGED SWORD

The security industry is clearly in a state of a flux. Whilst companies like Baltimore and iDefense are suffering self-evident problems, the rest of the market appears to be buoyant. IDC reported last week that the security industry looks set for a bumper few years and with the UK's Confederation of British Industry stating that two thirds of companies fell victim to cyber crime last year, it seems that security companies could be set to boom.

Link: <http://www.it-analysis.com/article.php?id=1586>

EXPERT HACKS HOTMAIL IN 1 LINE OF CODE

Twice this month, Internet security consultant Jeremiah Grossman, 24, poked gaping security holes in Hotmail and Passport, Microsoft's free Web-based e-mail and identity-authentication services. It took just three lines of code for Grossman to breach Hotmail filters and access Passport ID and credit card data. The second time it took just one line. And the former Yahoo security auditor says he could do it again given 8 hours.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.usatoday.com/life/cyber/tech/2001-08-31-hotmail-security.htm>

"REAL WORLD LINUX SECURITY" BOOK REVIEW

Toxen is one of the original developers of Berkeley Unix, and his book is full of interesting historical tidbits from the computer science halls of UC Berkeley in the early 1970s. When it comes to Unix security, Toxen's mantra is certainly "been there, done that." Toxen is one of a very few writers who can write in the first person about developing operating systems while dropping names such as Bill Joy and Ken Thompson.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/articles/2001/0108/0108I/0108I.htm>

AIR FORCE TO TEST BIOMETRIC SECURITY

The Air Force will soon begin testing three types of biometric applications for greater security in daily operations, with partial funding from the Defense Department.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.gcn.com/vol1_no1/daily-updates/16966-1.html

PROGRAMMER CLAIMS TO CRACK MS READER

In another potential blow to online publishing, a U.S. programmer says he has developed software that defeats the most advanced encryption features of Microsoft's Reader, a software program for distributing electronic books.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2809412,00.html>

NEW VIRUS TARGETS AND ENCRYPTS .EXE FILES

Antivirus vendor Central Command Inc. has detected a new worm that, disguised as a warning from Microsoft Corp., mass mails itself to users and once launched from an attachment, encrypts executable files, rendering them unusable.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/story/0,1199,NAV47_STO63419,00.html

INDIA'S CYBER CRIME POLICE STATION

India's first cyber crime police station was inaugurated at the CoD headquarters in Bangalore yesterday. Speaking to reporters, Home Minister Mallikarjun M. Kharge said the station will register cyber crime cases under the Information Technology Act, 2000, with jurisdiction all over the state.

Link: http://timesofindia.indiatimes.com/articleshow.asp?art_id=69539761

E-ENVOY BACKS SMARTCARD USE

The UK government is to set up bodies to encourage the use of versatile smartcards and digital signatures in both the public and private sectors.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094275,00.html>

SECURITY SOFTWARE: BLIND LEAD BLIND

It's incredible that in this day and age some of the most popular security products, products that are marketed as protecting you from the evils of computers, are so badly designed. Case in point: The many antivirus products that failed to detect and stop the highly effective SirCam worm, even when updated with the latest signatures and when configured correctly.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/21384.html>

THINKING ABOUT SECURITY

Joe "Zonker" Brockmeier writes: "This month, I thought I'd take a slight detour to talk about security. The Code Red worm and its sequels have been in the news a great deal, and admins running *Nix servers and Apache might be getting a little complacent in the security department, figuring that all is

well as long as they're not running IIS."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/articles/2001/0108/0108m/0108m.htm>

DESIGN FLAW STOPS INVALIDSSL WORM

A potentially dangerous new Internet worm has been rendered sterile, thanks to a weakness in the program's code, anti-virus experts said. The data destroying worm, which has been dubbed InvalidSSL and other aliases, travels as a Trojan horse program attached to an e-mail message masquerading as a Microsoft security bulletin.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169608.html>

LINUX RUNNING ON SECURE CRYPTOGRAPHIC COPROCESSOR

IBM Research has demonstrated Linux running on the IBM 4758 secure cryptographic coprocessor, a hardware security module. This is the first general purpose OS running on a secure coprocessor. The IBM 4758 cryptographic coprocessor is an advanced, tamper-sensing and responding, programmable PCI card. Its specialized cryptographic electronics, along with a microprocessor, memory and random number generator are housed within a tamper-responding environment to provide a highly secure subsystem in which data processing and cryptography can be performed.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://researchweb.watson.ibm.com/resources/news/20010828_mycroft.shtml

OLD WORM STRIKES SECURITY CONTRACTOR - REPORT

A Web server operated by Veridian Corporation has been infected with the Sadmind Worm, according to a report by a French hacking information site. In an online article published Monday, Kitetoea.com claimed that it had discovered evidence that Veridian's site was compromised by Sadmind, a self-propagating worm that replaces the homepage on infected sites with a profane, anti-American message in red letters on a black background.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169660.html>

NASA USES OPENBSD; OVERCOMES 802.11B SECURITY FLAWS

The network security group in the NASA Advanced Supercomputing (NAS) Division at Ames Research Center, in California's Silicon Valley uses OpenBSD and other open source software for its wireless firewall gateway implementation. They successfully installed a secure interoperable wireless network addressing the well-known problems of the 802.11b standard wireless systems.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2001/August/News546.html>

CELLPHONE WITH MILITARY SECURITY

Thanks to a German company called Rohde And Schwarz, and cellphone giant Siemens, the new TopSec cellphone is being marketed to politicians and corporate honchos who want to make sure that nobody but the other party (or parties) is listening in.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.popularmechanics.com/technology/telecom/2001/6/topsec_cellphone/

CODE RED WORM REPORTEDLY CAME FROM CHINA

The "Code Red" computer worm, which caused \$2.4 billion in estimated cleanup costs on Internet-linked computers last month, seems to have been born at a university in China's southern Guangdong province, according to the nonpartisan investigative arm of the U.S. Congress.

Link: <http://www.japantoday.com/e/?content=news&cat=7&id=65098>

SKLYAROV BOSS EXHIBITS COJONES

ElcomSoft President Alexander Katalov - voluntarily, proudly, manfully - stood beside Sklyarov and answered charges on behalf of his company. The symbolism was rare and delightful. Sklyarov is not going to face prosecution by an alien state, for performing a perfectly legal service in his home country, alone and unaided. We'd like to see an American or European corporate president exhibit a fraction of Katalov's cojones in the face of whingeing shareholders and scolding underwriters.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21397.html>

JAILED TEEN HACKER GETS FRESH START

Moran, who went by the online name "Coolio," runs a computer services company that a mentor helped him set up while in jail. He is chauffeured to jobs on work-release during the day and returned to jail each night.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://europe.cnn.com/2001/TECH/internet/08/31/hackers.fresh.start.ap/index.html>

Security issues

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

QUICK TEMPORARY FIX FOR OWA DOS

Configure IIS to Challenge-Response the access on the login page, that way, non legitimated users that tries to cause the DOS in your OWA won't have access to the component that cause that problem.

Link: <http://www.net-security.org/text/bugs/998911357,34419,.shtml>

SECURITY VULNERABILITY IN PHPROJEKT

By modifying the ID number in links an user can view, moduify or delete data of other users randomly.

Link: <http://www.net-security.org/text/bugs/998911431,43328,.shtml>

EUDORA MUA: RISKY PRACTICE

Attachments received with messages are stored in a directory, where they are left although the user erases the message. "Automatic attachment deletion" seems to be an optional feature, while it should be the default behavior.

Link: <http://www.net-security.org/text/bugs/999001131,94813,.shtml>

REMOTE BUFFER OVERFLOW VULNERABILITY IN HP-UX

Internet Security Systems (ISS) X-Force has discovered a buffer overflow in the HP-UX line printer daemon (rpldaemon). The rpldaemon service contains a buffer overflow that may allow a remote or local attacker to execute arbitrary code with superuser privilege.

Link: <http://www.net-security.org/text/bugs/999001383,29683,.shtml>

OPENSERVR: BIND BUFFER OVERFLOWS

The BIND subsystem contains several buffer overflows, detailed in CERT advisory CA-2001-02. This advisory announces the availability of a preliminary version of BIND 8.2.5. Since there is no packaged installation of this preliminary offering, it should only be installed by experienced system administrators. A formal installable fix containing this version of BIND is forthcoming.

Link: <http://www.net-security.org/text/bugs/999001501,36544,.shtml>

OPEN UNIX, UNIXWARE: UIDADMIN BUFFER OVERFLOW

A very long argument to the uidadmin "-S" (scheme) argument causes uidadmin to core dump. This might be exploited by an unauthorized user to gain privilege.

Link: <http://www.net-security.org/text/bugs/999001564,6097,.shtml>

CONNECTIVA LINUX - VULNERABILITY IN XLOADIMAGE

This program contains a buffer overflow in the code handling FACE type images. In conjunction with plugger and netscape, this could be used by remote attackers to execute arbitrary code on the user's machine when this user visited a site containing a specially crafted image.

Link: <http://www.net-security.org/text/bugs/999086089,35970,.shtml>

LINUX MANDRAKE - KERNEL 2.4 UPDATE

A security hole was found in the earlier Linux 2.4 kernels dealing with iptables RELATED connection tracking. The iptables ip_conntrack_ftp module, which is used for stateful inspection of FTP traffic, does not validate parameters passed to it in an FTP PORT command. Due to this flaw, carefully constructed PORT commands could open arbitrary holes in the firewall. This hole has been fixed, as well as a number of other bugs for the 2.4 kernel shipped with Mandrake Linux 8.0.

Link: <http://www.net-security.org/text/bugs/999086195,48364,.shtml>

OPEN UNIX: LPSYSTEM BUFFER OVERFLOW

A long argument to /usr/sbin/lpsystem can cause lpsystem to have a segmentation violation. This might be used by an unauthorized user to gain privilege.

Link: <http://www.net-security.org/text/bugs/999086268,20690,.shtml>

VULNERABILITIES IN APACHE AUTHENTICATION MODULES

RUS-CERT has discovered that several Apache authentication modules which use SQL databases to store authentication information are vulnerable to a remote SQL code injection attack.

Link: <http://www.net-security.org/text/bugs/999189217,41850,.shtml>

BSD LINE PRINTER DAEMON REMOTE BUFFER OVERFLOW

Internet Security Systems (ISS) X-Force has discovered a vulnerability in several BSD implementations. A buffer overflow vulnerability exists in the BSD Unix line printer daemon ("in.lpd" or "lpd"). Remote or local attackers may use this vulnerability to execute arbitrary code with superuser privilege on a vulnerable target.

Link: <http://www.net-security.org/text/bugs/999189297,17625,.shtml>

SECURITY ADVISORY FOR BUGZILLA V2.13 AND OLDER

There are many patches that need to be applied to properly close these holes, so they are not included here. If you will not be upgrading your system to 2.14 and instead wish to apply these patches to your existing system, please consult the bug reports on bugzilla.mozilla.org for the bug numbers listed below, where you can obtain the patches attached to those bugs.

Link: <http://www.net-security.org/text/bugs/999189357,73947,.shtml>

PHPMYEXPLORER VULNERABLE TO DIRECTORY TRAVERSAL

eRiskSecurity has discovered a fatal flaw in PhpMyExplorer, a popular (and very good looking) PHP based file manager. It is vulnerable to directory traversal. If the web server doesn't have appropriate limits set, like most out-of-the-box Linux distributions, the intruder can browse the entire drive, even reading sensitive files such as /etc/passwd.

Link: <http://www.net-security.org/text/bugs/999189435,59127,.shtml>

GNUT GNUTELLA CLIENT HTML INJECTION

I recently discovered a bug in gnut, a console/www Gnutella client for Linux and Windows, that allows the injection of html code in the Search Result Page of the Webfrontend.

Link: <http://www.net-security.org/text/bugs/999254301,92914,.shtml>

VULNERABILITY IN CREDIT UNION'S E-STATEMENT FEATURE

Sioux Falls Federal Credit Union gives its clients the ability to be alerted via e-mail when their monthly statement is available. There is a rather severe flaw in this feature, however. By following the link you can see an example of the e-mail which a client using the online statement notification would receive.

Link: <http://www.net-security.org/text/bugs/999364987,47903,.shtml>

MANDRAKE LINUX - FETCHMAIL UPDATE

A vulnerability was found by Salvatore Sanfilippo in both the IMAP and POP3 code of fetchmail where the input is not verified and no bounds checking is done. This can be exploited by a remote attacker to write arbitrary data into memory. The attacker must have control of the mail server the client is connecting to via fetchmail in order to exploit this vulnerability.

Link: <http://www.net-security.org/text/bugs/999436487,3601,.shtml>

MANDRAKE LINUX - XINETD UPDATE

An audit has been performed on the xinetd 2.3.0 source code by Solar Designer for many different possible vulnerabilities. The 2.3.1 release incorporated his patches into the xinetd source tree. The audit was very thorough and found and fixed many problems. This xinetd update includes his audit patch.

Link: <http://www.net-security.org/text/bugs/999436735,84125,.shtml>

Security world

All press releases are located at:
<http://net-security.org/text/press>

IDS USERS GRAPPLE WITH MANAGEMENT ISSUES - [27.08.2001]

Despite increasing speed and complexity of networks that have made IDS solutions difficult to deploy and manage, the technology is accepted and improving Intrusion detection systems are here to stay as an integral part of the network security infrastructure. But security solutions vendors must work to overcome user skepticism and frustration about intrusion detection stemming from poorly performing early deployments, lack of scalability, and difficulties in management and data gathering and analysis.

Press release:

< <http://www.net-security.org/text/press/998911583,25027,.shtml> >

ANTI-VIRUS FILTRATION FOR SMTP? NOW THERE IS! - [27.08.2001]

Kaspersky Labs, an international data-security software developer, announces the beta release of the popular Kaspersky Anti-Virus for SMTP gateways. The new program offers customers the opportunity of embedding a centralized anti-virus scanning for e-mail independent of the type of server being used.

Press release:

< <http://www.net-security.org/text/press/998911839,27184,.shtml> >

'PUPPY' FINGERPRINT IDENTIFICATION UNIT AVAILABLE - [27.08.2001]

Sony's sleek, award-winning FIU-710 fingerprint identification device - otherwise known as the Puppy unit -- is currently available for purchase at <http://www.SonyStyle.com>. Consumers can now "adopt" their Puppy unit for just \$299 and have it house-trained within the next few days!

Press release:

< <http://www.net-security.org/text/press/998911968,7671,.shtml> >

QUALYS TEAMS WITH ESPIRIA - [28.08.2001]

Qualys, Inc., a leading provider of enterprise network vulnerability assessment and monitoring solutions, and Espiria, a leading developer of comprehensive security programs, announced a strategic partnership to provide Espiria customers with Qualys' online network vulnerability auditing services. The agreement enhances Espiria's current security program by offering Qualys' Web-based scanning capabilities as another component of defense in securing their electronic environment.

Press release:

< <http://www.net-security.org/text/press/999001754,726,.shtml> >

ROXIO AND SYMANTEC JOIN FORCES - [28.08.2001]

Roxio, Inc., The Digital Media Company, today announced the inclusion of GoBack 3 Personal Edition in Symantec's Norton SystemWorks 2002. GoBack 3 Personal Edition delivers quick and easy system recovery capabilities to users, providing them with the power to undo system crashes, virus damage, failed software installations and user error. Norton SystemWorks 2002 offers a comprehensive, integrated security solution set to help keep PCs running at optimal performance levels.

Press release:

< <http://www.net-security.org/text/press/999001810,51855,.shtml> >

SERVICE PACK MANAGER 2000 SECURITY PRODUCT OUT - [28.08.2001]

Gravity Storm Software today announced the release of Service Pack Manager 2000 v6.0. This software utility enables system administrators to fix security vulnerabilities and stability problems in Windows NT/2000 and additional Microsoft products. The increasing number of viruses such as Code Red worm and continuous discoveries of security flaws in Microsoft products mandate cost effective security measures, provided by Service Pack Manager 2000, to protect both servers and workstations on the enterprise networks.

Press release:

< <http://www.net-security.org/text/press/999001889,14697,.shtml> >

NAI GETS PATENT FOR UPDATING AV OVER THE INTERNET - [28.08.2001]

Network Associates, Inc. announced that the United States Patent and Trademark Office has granted the company United States Patent number 6,269,456 for its technology invention in the field of updating anti-virus software over the Internet. The anti-virus updating technology described in United States Patent 6,296,456, entitled "Method and System for Providing

Automated Updating and Upgrading of Antivirus Applications Using a Computer Network," further distinguishes the company's McAfee brand anti-virus solutions from other anti-virus products and vendors. According to a particular example of the newly patented technology, updated anti-virus files are automatically pushed over the Internet from McAfee, or another source, to a local distribution server within a customer's network. Files are then pushed from the distribution server to additional servers and desktops within the customer network.

Press release:

< <http://www.net-security.org/text/press/999001982,95663,.shtml> >

GARRISON TECHNOLOGIES PARTNERS WITH QUALYS - [28.08.2001]

Qualys, Inc., a leading provider of enterprise network vulnerability assessment and monitoring solutions, today announced that Garrison Technologies, a leading network security consultancy, is now providing Qualys-powered online network vulnerability scanning to its premiere eNSPECTOR Security Assessment Services (SAS) clients. As an added feature of Garrison's comprehensive eNSPECTOR security assessment services, the Qualys service enables companies to identify and assess their network and host security exposures in real time over the Internet.

Press release:

< <http://www.net-security.org/text/press/999004027,13275,.shtml> >

USB-BASED SENTINEL SYSTEM DRIVERS GOT MS CERT. - [28.08.2001]

The eSecurity group of Rainbow Technologies, Inc. a leading provider of high performance security solutions for the Internet, eCommerce and software protection, today announced that its USB-based Sentinel System Drivers for SuperPro and SuperProNet software security tokens have gained Windows Hardware Quality Labs certification from Microsoft. The certification means the drivers and USB Sentinel hardware keys have met rigorous standards for operation with the Windows 2000 operating system.

Press release:

< <http://www.net-security.org/text/press/999031690,11353,.shtml> >

EURO909.COM EXPANDS ITS SECURITY PRODUCT LINE - [29.08.2001]

euro909.com A/S announced it has acquired 85 percent of the Danish security firm WISEhouse Denmark A/S, a remote data backup and storage service provider, for 25 million DKK (U.S. \$3.0 million) -- 10 million DKK in cash (U.S. \$1.2 million) to the previous shareholders and an additional 15 million DKK (U.S. \$1.8 million) towards WISEhouse's working capital.

Press release:

< <http://www.net-security.org/text/press/999087552,2917,.shtml> >

INET INTRODUCES SMARTALERTS APPLICATION - [29.08.2001]

Inet Technologies, Inc., a leading global provider of communications software solutions for next-generation networks, announced the introduction of SmartAlerts, a new advanced application of the company's GeoProbe and GeoProbe Mobile solutions.

Press release:

< <http://www.net-security.org/text/press/999087616,52322,.shtml> >

DEVELOPING LINUX PORT FOR SECURE HARDWARE - [29.08.2001]

Cryptographic Appliances first demonstrated Linux running on the IBM 4758 secure cryptographic coprocessor in April at the RSA Conference 2001. "Reaction to the 4758 was astounding," said Chris Zimman, CTO of Cryptographic Appliances. The 4758, a FIPS 140 level 4 device, utilizes a host side driver developed with Cryptographic Appliances.

Press release:

< <http://www.net-security.org/text/press/999087699,34729,.shtml> >

PKI NOT INCLUDED IN CURRENT FTSE500 SECURITY POLICIES - [29.08.2001]

Research from the UK's largest on-line security consultancy Detica, shows that only three per cent of FTSE 500 firms are currently deploying public key infrastructure products. PKI is the technology and process behind securing on-line transactions with the use of digital signatures and certificates.

Press release:

< <http://www.net-security.org/text/press/999089765,48419,.shtml> >

GRAND JURY CHARGES ELCOMSOFT AND SKYLAROV - [29.08.2001]

A United States grand jury this afternoon indicted Russian company Elcomsoft along with previously jailed programmer Dmitry Sklyarov on charges of trafficking and conspiracy to traffic in a copyright circumvention device. Since the grand jury handed down a five-count indictment, Sklyarov -- who is out of custody on \$50,000 bail -- could face a prison term of up to twenty-five years and a US \$2,250,000 fine. As a corporation, Elcomsoft faces a potential US \$2,500,000 fine.

Press release:

< <http://www.net-security.org/text/press/999090336,60617,.shtml> >

ASTARO SECURITY LINUX VERSION 2.0 RELEASED - [29.08.2001]

The new version 2.0. significantly enhances the easy-to-manage software with added functionality such as VPN for IPsec and PPTP for secure road warrior communications and SCSI-Support for high availability security

solutions.

Press release:

< <http://www.net-security.org/text/press/999093415,54923,.shtml> >

CIPHERTRUST LAUNCHES E-MAIL SECURITY APPLIANCE - [29.08.2001]

Addressing the increasing need for next generation application security, CipherTrust, a leader in e-mail security, today announced the availability of IronMail. IronMail is an application- specific security appliance for e-mail, which integrates hardware and pre- configured software. It sits between network firewalls such as Check Point Firewall-1 and Cisco PIX and corporate e-mail servers such as Microsoft Exchange and Lotus Notes. IronMail is a category defining product, providing comprehensive security for e-mail servers and e-mail messages.

Press release:

< <http://www.net-security.org/text/press/999094235,36984,.shtml> >

CHECK POINT NEXT GENERATION TRAINING - [30.08.2001]

Check Point Software Technologies Ltd., the worldwide leader in securing the Internet, announced the availability of training on Check Point Next Generation, Check Point's powerful new product suite, at the 225-plus Check Point Authorized Training Centers (ATCs) worldwide. These courses give customers the knowledge they need to most effectively utilize Check Point's new comprehensive product suite for Internet security, Check Point Next Generation, and maximize their return on investment. For specific course starting dates and ATC contact information please visit <http://www.checkpoint.com/atc>.

Press release:

< <http://www.net-security.org/text/press/999188537,43469,.shtml> >

WATCHGUARD CONTINUES VPN MARKET LEADERSHIP - [30.08.2001]

WatchGuard Technologies, Inc. a leader in Internet security solutions, announced that it was once again named revenue market share leader in the mid-range VPN hardware market.

Press release:

< <http://www.net-security.org/text/press/999188655,49697,.shtml> >

PC MAGAZINE REWARDS NOKIA VPN - [30.08.2001]

Nokia announced that the CC500 and CC2500 Nokia VPN gateways have received PC Magazine's celebrated Editors' Choice Awards in recent VPN tests due to appear in the September 25, 2001 issue. According to PC Magazine, the Nokia CC500 and CC2500 VPN gateways were selected as Editors' top pick due to their ease of installation and deployment,

centralized management, solid operational ability, very high throughput, well structured management, and overall most attractive and affordable offering in its class.

Press release:

< <http://www.net-security.org/text/press/999188728,7063,.shtml> >

BALTIMORE'S SELECTACCESS FOR BEA WEBLOGIC - [30.08.2001]

Baltimore Technologies, a global leader in e-security, announced that its access and authorization management product, SelectAccess, now provides seamless integration with BEA WebLogic from BEA Systems, Inc., one of the world's leading e-business infrastructure software companies. Customers deploying BEA WebLogic can now use SelectAccess to smoothly manage all access privileges of users into their critical e-business systems such as intranets, extranets and portals in a highly secure, scalable and precise manner.

Press release:

< <http://www.net-security.org/text/press/999188855,88049,.shtml> >

NASA DEPLOYS SECURELOGIX TELEWALL FIREWALL - [30.08.2001]

SecureLogix Corporation, a leader in secure network convergence, announces the purchase of their award-winning TeleWall Telecom Firewall by NASA Ames Research Center. The vulnerability that unauthorized modems introduce into data networks is widely recognized. The TeleWall Telecom Firewall eliminates this threat and completes the security of the network perimeter.

Read more:

< <http://www.net-security.org/text/press/999188946,86696,.shtml> >

SECURE VIRTUAL PRIVATE NETWORKS TUTORIAL BY QUALYS - [30.08.2001]

Qualys, Inc., a leading provider of enterprise network vulnerability assessment and monitoring solutions, today announced that it is co-sponsoring an eight-city seminar tour across North America this Fall focusing on the implementation of secure Virtual Private Networks (VPNs). Produced by Network World and entitled "VPNs ... Guiding Your Way Toward Network Security," the seminars will include a tutorial from Qualys on how online network vulnerability scanning provides VPNs of all sizes with a proactive and perpetually up-to-date defense against would-be intruders.

Read more:

< <http://www.net-security.org/text/press/999189091,59989,.shtml> >

RSA SECURITY PROVIDES SECURE E-SIGNATURES FOR EORIGINAL - [31.08.2001]

RSA Security Inc., the most trusted name in e-security, announced that eOriginal Inc. has selected RSA Keon Certificate Authority (CA) PKI software to support its virtual and secure system to conduct business transactions over the Internet. eOriginal, a leading provider of advanced e-commerce business solutions, will use RSA Keon CA software to issue its Public Key Infrastructure (PKI) certificates that support creation and verification of digital signatures.

Read more:

< <http://www.net-security.org/text/press/999254628,10505,.shtml> >

VPN DYNAMICS OFFERS CHECK POINT TRAINING - [31.08.2001]

VPN Dynamics Inc., leading security services and training firm providing flexible network security and VPN solutions, announced that it is one of the first Check Point Software Technologies Ltd. Authorized Training Centers (ATC) in Northern California to offer comprehensive certification training for the Check Point Next Generation Internet security product suite.

Read more:

< <http://www.net-security.org/text/press/999254726,62149,.shtml> >

SOPHOS: TOP TEN VIRUSES IN AUGUST 2001 - [01.09.2001]

This is the latest in a series of monthly charts counting down the ten most frequently occurring viruses as compiled by Sophos, a world leader in corporate anti-virus protection.

Read more:

< <http://www.net-security.org/text/press/999365130,43356,.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

MOVIANVPN

Certicom has developed the first IPSec VPN client designed for handheld devices that is interoperable with popular VPN gateways from Check Point, Cisco, and

Nortel. The VPN client allows companies to extend their VPN infrastructure to include wireless and mobile devices, providing secure access to corporate email and applications behind the corporate gateway. Using Certicom's patented ECC technology, the client provides a security solution to meet the bandwidth and footprint constraints of today's handheld devices. The client runs on the Palm operating system v3.5, Microsoft Windows CE 3.0 and will be available on EPOC and other platforms soon.

Read more:

< <http://www.security-db.com/product.php?id=365> >

This is a product of Certicom, for more information:

< <http://www.security-db.com/company.php?id=78> >

PARA-APPROVED

As communication and commerce grow rapidly on the Internet, corporate futures will depend on established measurable levels of trust between business, clients, and partners. One way of building the trust is to identify secure Internet environments through examination and certification.

Para-Approved is the seal that, when viewed on a website, provides an immediate reliable, trusted notice that the website meets a structured set of best security practices.

Para-Protect's State-of-the-HackSM competency ensures that websites displaying the Para-Approved seal have met the most current standards against threats and vulnerabilities. Only websites that meet Para-Protect's State-of-the-HackSM and conduct best practice standards are eligible to display the Para-Approved seal.

Read more:

< <http://www.security-db.com/product.php?id=553> >

This is a product of Para-Protect Services, for more information:

< <http://www.security-db.com/company.php?id=121> >

TRUSECURE SOLUTIONS

Through its TruSecure Solutions, the company provides certification of organizations that have addressed all the rigorous requirements for achieving and maintaining a sound information security posture. These Certified customers have undergone a series of evaluations and recommendations on overall network architecture, connectivity, physical security, redundancy and disaster recovery capabilities, environmental controls, system configurations, and operational policy compliance. Once the site is officially certified, TruSecure Corporation security analysts work with the organization to continually monitor adherence to evolving essential practices.

Read more:

< <http://www.security-db.com/product.php?id=539> >

This is a product of TruSecure Corporation, for more information:

< <http://www.security-db.com/company.php?id=119> >

Featured articles

All articles are located at:
<http://www.net-security.org/text/articles>

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

NEEDFUL THINGS: NESSUS

Another day, another week, and /etc and what a better start of another in the must-have series of articles in which I deal with needful things for an average linux user or admin? This time, I'll focus on Nessus, a free and indeed powerful (as they say it on its homepage) scanner. But, lets not get too hasty, and start from the beginning...

Read more:
< <http://www.net-security.org/text/articles/nessus.shtml> >

WHICH HAT ARE YOU?

It was inevitable that the hacking scene be split into new sub categories with new terminology to represent the mentality of the world's brightest hackers. A decade ago it was a lot easier to understand what a hacker was and could do. Now we have millions of people using computers each day for email, e-commerce, banking, business, socialising, etc. It's clear cyberspace has become a mirror of reality with more and more people getting online every day. The internet follows the same patterns as the universal guiding pattern of birth, a system rises, transforms itself and the world. Birth, change, death, rebirth, but on the net it's beta, version 1, obsolete, prototype.

Read more:
< <http://www.net-security.org/text/articles/hat.shtml> >

IS THERE REALLY A NEED FOR PC SECURITY?

Many people seem to be clueless about PC Security. Some apparently do not even care. But facts are simple in this regard. It can be virus, hacker, and other intrusion. The method of intrusion matters little. What matters most is the price tag subsequent to the intrusion.

Read more:
< <http://www.net-security.org/text/articles/pcsecurity.shtml> >

A COMMENT ON BUGTRACKING

The point is that I really appreciate the work of bughunters. Of course I would like to know as soon as possible whether the programs I use have security flaws. I'm honestly thankful for every bug that someone finds in my programs. I also understand the greed for being the first to report a bug.

Read more:

< <http://www.net-security.org/text/articles/comment.shtml> >

TRADITIONAL ID MODEL OUTDATED AND DISTRACTING

The Internet and interoperable intranets are a vast and complex dimension of both enabling and inhibiting data flows. Current generation intrusion detection (ID) systems are not technologically advanced enough to create the situational knowledge required to manage these networks. Next generation ID system will fuse data, combining both short-term sensor data with long-term knowledge databases, to create cyberspace situational awareness.

Read more:

< <http://www.net-security.org/text/articles/traditional.shtml> >

Security Software

All programs are located at:

<http://net-security.org/various/software>

EVIDENCE ERASER 1.0

Evidence Eraser exceeds Department of Defense specifications for PC data destruction. It has proven to defeat even "forensic analysis" software used by many private investigators and law enforcement agencies. In addition, you will reclaim disk space and increase your PC's performance by permanently destroying cookies, cache files, temp files, browser history, temporary Internet files, and many more types of secret hidden data.

Info/Download:

< <http://www.net-security.org/various/software/999009610,4785,windows.shtml> >

WINSIGMA 1.0

WinSigma is a shareware encryption program for Windows (95,98, and probably

others). It employs the Sigma A and Sigma B encryption algorithms for low to medium level security.

Info/Download:

< <http://www.net-security.org/various/software/999009992,64834,windows.shtml> >

ACID 0.9.6b12

The Analysis Console for Intrusion Databases (ACID) is a PHP-based analysis engine to search and process a database of incidents generated by security related software such as IDSeS and firewalls (e.g., Snort or ipchains). It provides a search interface for finding alerts matching practically any criteria. This includes arrival time, signature time, source/dest address/port, flags, payload, etc. ACID also provides the ability to annotate and logically group related events, delete false positives, or archive alerts among databases. Finally, a variety of statistics and graphs can be generated based on time, IP address, ports, alert classification, and sensor.

Info/Download:

< <http://www.net-security.org/various/software/999010236,37538,linux.shtml> >

BLINDFOLD

Blindfold is a utility which is intended to find some combination of IP packets which will make the Linux TCP/IP stack crash. It uses a blind brute-force method for doing this search. The goal of the project is to discover possibly hidden bugs in the implementation of Linux's TCP/IP stack.

Info/Download:

< <http://www.net-security.org/various/software/999010648,61081,linux.shtml> >

CHAPASSWD

chapasswd is a set of tools to manipulate the chap-secrets files, which are utilized by PPP for CHAP-based authentication. It aims to be similar to passwd and related tools. At the moment, it can change the passwords for a given user.

Info/Download:

< <http://www.net-security.org/various/software/999010759,83995,linux.shtml> >

CORKSCREW 2.0

corkscrew is a small program for tunneling SSH through HTTP proxies. It features easy configuration and support for several Unix variants.

Info/Download:

< <http://www.net-security.org/various/software/999011001,89210,linux.shtml> >

ELIOTT 1.0

Eliott is a tool to help system administrators and programmers discover insecure temporary file creation, even in closed-source applications. It watches a directory for file creation/deletion/writes using the dnotify facility of Linux 2.4.x . Every change is logged, even temporary files with a very short lifetime. In addition to logging, Eliott can simulate hard-link exploits in order to find and report vulnerable applications.

Info/Download:

< <http://www.net-security.org/various/software/999011213,78045,linux.shtml> >

FIRE-WALLER 1.2.1

Fire-Waller reads your syslog against packet filter rows and creates HTML output of the found rows. All addresses in logfiles are checked against a nameserver and protocols/services are converted from numeric values to text.

Info/Download:

< <http://www.net-security.org/various/software/999011295,65458,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>