

HNS Newsletter
Issue 80 - 24.09.2001
<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) 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>
=====

General security news

=====
NIMDA WORM SPECIAL COVERAGE

=====
In order to make things easier to find, all the information regarding the worm are in this page. Everything from alerts, news items, solutions, etc.

<http://www.net-security.org/text/articles/coverage/nimda>
=====

GOVERNMENT SMARTCARD PLANS 'OVER-AMBITIOUS'
Government plans to create a single, multipurpose smartcard to work across the public and private sectors may be over-ambitious, according to Arthur Coviello, president and chief executive of RSA Security. He said it would be extremely difficult to develop a multi-functional smartcard in the short term.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2095315,00.html>

SQL SERVER SECURITY BEST PRACTICES

This article discusses the security model of Microsoft SQL Server 7.0 and 2000, along with security best practices to help you secure your data.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sql-server-performance.com/vk_sql_security.asp

NETWORKS BOOST SECURITY AGAINST ATTACKS

An FBI warning has administrators of the nation's corporate networks double checking - and double-locking - their systems in the wake of Tuesday's terrorist attacks. But despite the federal Terrorist Threat Advisory, which calls for IT professionals across the country to "implement appropriate security measures - both physical and cyber," experts say corporate America is a long way from ready, or safe.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2095349,00.html>

GEEKS GATHER TO BACK CRYPTO

Rob Carlson is worried about something that most Americans would consider entirely obscure: the future of encryption technology. Carlson, a 21-year-old programmer, fears that the U.S. Congress, in the wake of last week's bloody attacks, may vote for anti-terrorism legislation that also threatens privacy.

"There's nothing as permanent as a temporary restriction," he says.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46900,00.html>

DESKTOP FIREWALLS

For the most part, you'll spend less money to install and maintain desktop firewalls than you'll spend to recover from an intrusion. This issue's Buyer's Guide provides an overview of available desktop firewall solutions. Many reasonably priced solutions are on the market today.

Link: <http://www.win2000mag.com/articles/index.cfm?articleid=22241>

GERMAN TV HACKERS CRACK BANK SERVER

HypoVereinsbank, one of Germany's largest banks, is considering legal action against a popular consumer high-tech TV show that hired hackers to break into the bank's online banking servers, according to a bank spokeswoman.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/170191.html>

A PERL PACKAGE FOR MONITORING TRAFFIC

The rtr-graph package described in this article is a set of Perl scripts for polling routers (or other SNMP-enabled devices) for information about traffic in and out of specified interfaces. You can set up "rtr-traff" as a cron job to poll the interface at a specified interval, then use a CGI script for a Web front end to the finished graphs.

Link: <http://www.samag.com/documents/s=1146/sam0109k/0109k.htm>

DISPOSABLE PHONES - A SECURITY RISK?

Hop-On Wireless Chief Executive Peter Michaels and the rest of the nascent disposable cell phone industry are scrambling to defend a product that hasn't made it into the United States yet, but is a target of the nation's top crime

fighters as they crack down on terrorism.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5097046,00.html>

DDOS ATTACK KNOCKS OUT ALLDAS.DE - FOR GOOD?

Our friends at Alldas.de are once again looking for a home after a deal to move from its ISP fell through in the wake of a debilitating hack attack. Good luck guys!

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21706.html>

HACKING VIGILANTES DEFACE WTC VICTIM'S SITE

After announcing plans to fight back against terrorism last week, the consortium of hacking groups, which calls itself the Dispatchers, vandalized on Sunday two Web sites operated by the Special Risks Terrorism Team, a unit of Aon Corporation, a Chicago-based risk management and insurance provider.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/170184.html>

INFORMATION SECURITY WILL BE KEY WITH LAWMAKERS

Last week's terrorist attacks are expected to shift government and legislative priorities on a host of technology issues. Internet privacy, for instance, the top technology policy issue barely more than a week ago, will likely be replaced by critical-infrastructure protection as the United States seeks to retaliate against what President Bush has called "an act of war."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/industry/09/17/information.security.idg/index.html>

CAN STRONGER SECURITY ACTUALLY MAKE US MORE VULNERABLE?

The secondary effects of last week's horrific terrorist attacks are becoming visible. The tertiary ones probably haven't even begun manifesting themselves. What is immediately apparent, however, is that the U.S. government considers this a good time to reiterate its long-standing desire to make computer security - and most especially, strong cryptography - something that ordinary people aren't supposed to have.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2812913,00.html>

ANALYSTS: TERRORISTS WILL USE THE WEB

Expect terrorists to find ways to use the Web as a weapon. Although there have been no reported cases of cyberterrorism or hacks of corporate or U.S. government sites, companies must remain vigilant in the coming days, say analysts from the research firm Gartner.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,62284,00.asp>

STATICALLY DETECTING LIKELY BUFFER OVERFLOWS

Buffer overflow attacks may be today's single most important security threat. This paper presents a new approach to mitigating buffer overflow vulnerabilities

by detecting likely vulnerabilities through an analysis of the program source code.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://lclint.cs.virginia.edu/usenix01.html>

ISLAMIST MAILING LIST CRACKED

An attacker has cracked a German-based Islamist Web site, publishing on the Web hundreds of e-mail addresses of subscribers to its mailing list, including one of a suspect in last week's terrorist attack.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_695961_1794_9-10000.html

ERA OF PICKING YOUR OWN PDA DRAWS TO A CLOSE

Firms may soon mandate the use of particular handheld devices and mobile phones in order to establish some kind of control over security risks. That's the view Symantec's director of wireless strategy, Jason Conyard, who is encouraging firms to develop security policies to combat mobile security threats such as hacking into wireless networks and next-generation malicious code.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21732.html>

YAHOO! NEWS HACKED

In a development that exposes grave risks of news manipulation in a time of crisis, a hacker demonstrated Tuesday that he could rewrite the text of Yahoo! News articles at will, apparently using nothing more than a web browser and an easily-obtained Internet address.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/254>

RSA TO BUILD CHINESE INTERNET SECURITY SYSTEM

RSA Security said it would develop a Chinese software system that will provide online Chinese companies with defenses against hackers. To build the system, a Chinese-language version of its RSA SecurID package, RSA Security said it would team up with a Chinese company, Sichuan Anmeng E-security Co. Ltd on the project.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/170256.html>

PRO-BIN LADEN PAKISTANI DEFACE WORLD TRADE SITE

In a move that could ignite hacker tensions, the founder of a group called the Pakistan Hackerz Club defaced the Web site of World Trade Services, a California-based firm that facilitates international e-commerce. In a message left at the defaced site, an individual calling himself "Doctor Nuker" suggested the U.S. government may have orchestrated the terrorist attacks on America to justify widening its manhunt for Osama bin Laden.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/170267.html>

A 'TARPIT' THAT TRAPS WORMS

"LaBrea" is a free, open-source tool that deters worms and other hack attacks by transforming unused network resources into decoy-computers that appear and act just like normal machines on a network. But when malicious hackers or mindless worms such as Nimda or Code Red attempt to connect with a LaBrea-equipped system, they get sucked into a virtual tarpit that grabs their computer's connection - and doesn't release it.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,46964,00.html>

AN INTRODUCTION TO OPENSLL, PART THREE

This is the third article in a series on OpenSSL, a library written in the C programming language that provides routines for cryptographic primitives utilized in implementing the SSL protocol. This article will introduce Public Key Infrastructure and show the commands that OpenSSL provides for managing PKI.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/sun/articles/openssl3.html>

UK CRIME UNIT ASKS ISPS TO KEEP DATA

The UK government has asked ISPs and telecommunication companies to retain traffic data for the next month in light of the recent terrorist events. The National High-Tech Crime Unit (NHTCU) sent out a request to freeze all traffic logs in case the data is needed by the FBI as part of their investigations.

Link:

<http://www.silicon.com/public/door?6004REQEVENT=&REQINT1=47562&REQSTR1=silicon.com>

CRUNCHBOX FIREWALL BY CAPTAIN CRUNCH

John Draper - The CrunchBox itself is a very proactive device and can be programmed to satisfy any company's security policy. It can also be programmed to do some pretty nasty things, should you want it to.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.guardian.co.uk/online/story/0,3605,554523,00.html>

TWELVE TIPS TO IMPROVE YOUR COMPANY'S SECURITY

Telenisus, a managed services provider specializing in Internet security, is providing tips on what to do now to tighten business security at your company.

Link: <http://www.varbusiness.com/sections/news/dailyarchives.asp?ArticleID=29969>

IT SECURITY BUDGETS SOAR

IT security sales will triple in value to \$21 billion by the end of 2005, compared with the \$6.7bn recorded in 2000. This represents a compound annual growth rate of 25.5%, according to IDC which makes the forecasts.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21781.html>

MICROSOFT CLAIMS WORM DIDN'T MAKE FRONTPAGE

Microsoft refuted claims Wednesday that the main Web site for its

FrontPage software had been infected by the Nimda virus, despite the antivirus software alarms set off by viewing the site.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5097206,00.html>

ANONYMIZING WITH SQUID PROXY

The debate over the ethics of using an employer's system to surf the Net is ongoing. Employee privacy rights and whether or not the company owns the contents of employees' machines are just two facets of it. The opportunity for system administrators to view personal information disclosed through Web surfing may also pose serious security concerns.

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

10 MINUTES TO AN IPTABLES-BASED LINUX FIREWALL

Worrying about the latest worm? Or the next? Spend a few minutes with iptables to fortify your Linux boxes from obvious attacks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/site-stories/2001/0920.ipchains.html>

AMERICANS WANT UNCRYPTION

Three in four Americans favour tough anti-encryption laws, in the wake of last week's terrorist atrocities, a survey finds. Seventy-two per cent believe anti-encryption laws will be "somewhat" or "very" helpful in combating terrorism, according to the survey, conducted by Princeton Survey Research Associates.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21791.html>

HACKERS START CYBER SKIRMISH

Earlier this week, a group of rogue online vigilantes, who dub themselves the Dispatchers, decided to destroy data and Internet connections within Afghanistan and Palestine. The group claims to have already disabled several Palestinian Internet service providers, and warns that ISPs and Web servers based in Afghanistan will be next "with the intent to destroy them and disable any use," said one warning on a Web site defaced by the Dispatchers.

Link: <http://www.cmpnetasia.com/ViewArt.cfm?Artid=12013&Catid=5&subcat=50>

COMMENTARY ON PATRIOTIC HACKING

Attrition staff have been getting several mails warning of impending "patriotic hacking" in retaliation for the terrorist attacks on September 11. Some are from the usual opportunists, exploiting world-wide attention on the recent terrorist attacks to further their own agenda. Others are from people who just want to do -something- to feel like they are striking back at those responsible, even if it's the wrong thing...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.attrition.org/security/commentary/patriotic.html>

AUSTRALIA WON'T DISCLOSE STANCE ON ENCRYPTION

Despite calls for a ban on 'uncrackable' encryption products in the US, the

Australian government isn't saying whether it will support the Americans.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2095772,00.html>

MOBILE AND WIRELESS SECURITY

Mobile, Internet-connected devices are the new personal computing revolution. Enterprises must develop support plans to minimize security risks.

Link: http://www3.gartner.com/DisplayDocument?doc_cd=101044

HOW TO INSTALL GNUPG

Adding public-key encryption to Linux e-mail clients is easier than you may think, thanks to GnuPG and gpgme.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/site-stories/2001/0919.gnupg.html>

'HAPPY HACKER' DROPS A BOMB ON SECURITY EXPERTS

On Wednesday, the 14,300-strong subscribers to a popular security list known as Vuln-Dev received what may have appeared a rare treat: a message to the list containing source code to a program that gave the user full control of a remote Unix system. List member Jason Parker he glanced over the code before compiling it, decided it looked legitimate, and ran it on the test account of a system. "I lost everything in the home directory, including information I would rather not have lost, but that's the price you pay for trusting," said Parker.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/170392.html>

CYBER SECURITY ALARM IN CANBERRA

Insecure and vulnerable government websites have been fortified against cyber attacks after an Auditor-General's security review. But the security levels were still insufficient in the majority of cases, acting Auditor-General Ian McPhee reported. In the midst of the crippling Nimda computer virus attacks, Mr McPhee said audited federal government agencies had not properly secured their internet services and had been forced to fix a number of vulnerabilities during the process of the audit.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://australianit.news.com.au/common/storyPage/0,3811,2904111%255E442,00.html>

SECURITY TAKES CENTRE STAGE AT CONFERENCE

The Information Security Solutions Europe (ISSE) 2001 conference in London next week will attract many companies eager to improve computer security. Speakers will include UK e-commerce minister Douglas Alexander, e-envoy Andrew Pinder, and executive director of the International Centre for Security Analysis, Dr Andrew Rathmell.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2095840,00.html>

Security issues

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

(E)SHOP ONLINE-SHOP SYSTEM VULNERABILITY

Script doesn't check for symbol ";". any user can execute any *nix commands on webserver.

Link: <http://www.net-security.org/text/bugs/1000834458,71994,.shtml>

ARCSERVE 6.61 SHARE ACCESS VULNERABILITY

The default install of ARCServe for NT creates a hidden share on Windows NT machines when it is installed. The name of this share is ARCSERVE\$. The permissions of the share allow all users in a domain to map this share. However, this is not the worst part. Within the share is a file named aremote.dmp. The full path is ARCSERVE\$\DR\aremote.dmp. In the aremote.dmp file, the account name that runs the backup is in cleartext within this file. Also, a little further within the file, the password for the account is in cleartext. Seeing as how the account that performs backups can access system files, this is very dangerous. Some places run their backups as the NT domain administrator account.

Link: <http://www.net-security.org/text/bugs/1000834493,19433,.shtml>

ORACLE 9I APPLICATION SERVER PATH DISCLOSURE

The Oracle 9i Application Server uses the Apache web server for HTTP service. However, if a request is made for a non-existent .jsp file, the complete path is shown.

Link: <http://www.net-security.org/text/bugs/1000834649,46301,.shtml>

AMERICAN AIRLINES NOT ENCRYPTING DATA

Looks like aa.com (American Airlines) is NOT encrypting customer data for purchasing e-tickets. Hopefully this isn't still the case by the time this posts. This holds true for both Advantage login and non-members as well. At no time did I get a redirect to an SSL server for my session.

Link: <http://www.net-security.org/text/bugs/1000834720,25195,.shtml>

PROBLEMS IN FORTE DEVELOPER 6 DBX AND INSTALL DOCS

Sun's compilers for sparc come with a very nice feature: the debugger can instrument an a.out and check for some classes of errors at runtime. There's also a very nice batch interface to this: "bcheck -all a.out". Unfortunately this mechanism doesn't work properly in any version of Forte Developer 6 to date: it fails to detect many obvious buffer out of bounds array references. This is Sun bugID 4460648, which I'm told is marked as "Completed Closed" and "Not Fixed".

Link: <http://www.net-security.org/text/bugs/1000834816,79873,.shtml>

LOTUS NOTES: ISSUE WITH FILE ATTACHMENTS

The short version is that file attachments and other objects may be

extracted from Notes databases regardless of any author or reader fields on the documents the objects are attached to.
Link: <http://www.net-security.org/text/bugs/1000834915,66956,.shtml>

OPENSSSH: SFTP & BYPASSING KEYPAIR AUTH RESTRICTIONS

If you 1) are using keypairs and ~/.ssh/authorized_keys2 to enable remote execution of commands via OpenSSH's sshd and 2) have sshd configured to provide sftp service via the sftp-server subsystem, then clients who have access with "restricted" keypairs can gain additional access on the server side. In most cases, sftp can be used to evade the authorized_keys2 command= and other restrictions (i.e., obtaining the regular shell access that the server was configured to deny them). It appears that both OpenSSH 2.9 (the official OpenBSD code) and OpenSSH 2.9p2 (the official "portable" code for other systems) by default *do* have the sftp subsystem enabled, and their users would be vulnerable if they set up restricted keypairs.

Link: <http://www.net-security.org/text/bugs/1000902454,343,.shtml>

ICQ PORTAL CROSS SITE SCRIPTING VULNERABILITY

The icq portal suffer from multiple Cross Site Scripting Vulnerability.

Link: <http://www.net-security.org/text/bugs/1001073872,31326,.shtml>

HALF-LIFE REMOTE BUFFER OVERFLOW VULNERABILITY

There is a buffer overflow in the console command "connect" on Windows Half-Life clients. The "connect" command is a command available in the client console which is used to connect to game servers when given a specific IP address and port.

Link: <http://www.net-security.org/text/bugs/1001074613,67495,.shtml>

FIREWALL-1 GUI LOG VIEWER VULNERABILITY RESPONSE

An issue exists in VPN-1/FireWall-1 Management Servers running on Windows NT or Windows 2000. A malicious administrator can exploit a buffer overflow condition in the GUI authentication code to potentially impair management station functionality or to execute code. Any attack must come from an IP address explicitly defined as an authorized GUI client. Only management stations running Windows NT or Windows 2000 are affected.

Link: <http://www.net-security.org/text/bugs/1001074687,93740,.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>

=====
NIMDA WORM SPECIAL COVERAGE
=====

In order to make things easier to find, all the information regarding the worm are in this page. Everything from alerts, news items, solutions, etc.

<http://www.net-security.org/text/articles/coverage/nimda>
=====

FIRST SECURE CONTENT NETWORKING PLATFORM

Ingrian Networks, the leader in secure content networking, announced a strategic partnership with Netegrity, the leading provider of software solutions for securely managing e-business. Under the terms of the agreement, Netegrity's SiteMinder web authentication and access control agent will be tightly integrated into Ingrian Network's Secure Content Networking platforms, delivering top solutions for access management and end-to-end content security in one platform.

Press release:
< <http://www.net-security.org/text/press/1000837195,88348,.shtml> >

SAFENET AND RSA SECURITY FORM STRATEGIC PARTNERSHIP

Internet security leaders SafeNet, Inc. and RSA Security Inc. announced that the companies have signed a strategic partnership agreement to create wireless VPN clients for the mobile marketplace based on RSA Security technology. The companies will contribute components of their field-proven technologies to provide end-to-end security for a variety of wireless Internet devices including personal digital assistants, mobile phones, and pagers.

Press release:
< <http://www.net-security.org/text/press/1000837254,86958,.shtml> >

EVIDIAN AND SSH PARTNER ON VPN SECURITY

SSH Communications Security, a leading developer of Internet security technologies, and Evidian, a global supplier of secure e-business and telecommunications management software today announced a technology partnership in the area of VPN security.

Press release:
< <http://www.net-security.org/text/press/1000837306,36247,.shtml> >

IPIN SELECTS NCIPHER TO ENRICH E-PAYMENT SECURITY MODEL

nCipher, a leading developer of Internet security products for e-commerce and PKI applications, announced that iPIN, the leading provider of e-Payment technology, has selected nCipher to further manage security risks at all levels of the e-Payment value chain, including secure communications over the Internet and the encryption of critical, private information stored in secure databases. iPIN provides financial institutions, telecomm service providers, automotive OEMs, ISPs, and e-commerce merchants with modular payment software that gives customers a wide range of payment options and transaction choices over any Internet-enabled device.

Press release:

< <http://www.net-security.org/text/press/1001079338,41289,.shtml> >

ENTRUST CEO CALLS FOR COOPERATION

Unprecedented cooperation is needed among government, business and American citizens to protect the nation's critical infrastructure against cyber attack, one of the nation's leading experts on Internet security told members of Congress and their staffs. At a briefing on Capitol Hill, Bill Conner, president and chief executive officer of Dallas-based Entrust, Inc., said businesses, government and the public must fully cooperate to deploy enhanced Internet security measures to protect the nation's communications infrastructure, commerce, government, utilities and other essential services.

Press release:

< <http://www.net-security.org/text/press/1001279878,7346,.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

NET-WORMER

We have designed and developed a Win32 based program that can be installed on any platform of Microsoft Windows; it offers full protection to VBS, VBE, JS, JSE, WSF, and WSH script worms. This protection includes full Programmatic Script Analysis based using the Virus-IDENT engine. Net-Wormer also provides easy functionality for the beginner user, with a Danger Rating. After analysis you can choose an action

to take on the script - Delete, Ignore or Run Script.

Read more:

< <http://www.security-db.com/product.php?id=598> >

This is a product of Delta Design UK, for more information:

< <http://www.security-db.com/company.php?id=130> >

HUSH KEY SERVER NETWORK

The Hush Key Server Network hosts and manages PKI Key pairs. This means that Hush facilitates the distribution of the electronic Keys used for encrypting and decrypting data and for signing and verifying signatures. The Hush Key Server Network is unique in its secure hosting of both the Public and Private Key. This repository of Public and Private Key pairs can be easily applied to a wide variety of applications. We can review your applications and determine how we can apply our technology to secure your communications.

Read more:

< <http://www.security-db.com/product.php?id=872> >

This is a product of Hush Communications, for more information:

< <http://www.security-db.com/company.php?id=62> >

SAFEWORD PLUS

SafeWord Plus is Secure Computing's new system of software authentication services using Public Key Infrastructure (PKI) technology to provide role-based privilege management of computer and network resources.

Read more:

< <http://www.security-db.com/product.php?id=48> >

This is a product of Secure Computing, for more information:

< <http://www.security-db.com/company.php?id=11> >

Security Software

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

LABREA

LaBrea is a program that creates a tarpit or, as some have called it, a "sticky honeypot". LaBrea takes over unused IP addresses on a network and creates "virtual machines" that answer to connection attempts. LaBrea answers those connection attempts in a way that causes the machine at the other end to get "stuck", sometimes for a very long time.

Info/Download:
< <http://www.net-security.org/various/software/1000976129,95030,linux.shtml> >

URLSCAN SECURITY TOOL

Microsoft has developed a tool that lets web server administrators ensure the security of their servers. The tool, URLScan, screens all incoming requests to the server, and filters them based on rules set by the administrator. This significantly improves the security of the server by helping ensure that it only responds to valid requests.

Info/Download:
< <http://www.net-security.org/various/software/1000903205,44343,windows.shtml> >

PACKET2SQL 2.1.0

Packet2sql will convert any text file/log file which contains ipchains packet logs into a stream of SQL inserts which can be used as the base for a firewall-analyzing database application.

Info/Download:
< <http://www.net-security.org/various/software/999956350,76824,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