

HNS Newsletter
Issue 88 - 19.11.2001
<http://net-security.org>
<http://security-db.com>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://www.net-security.org>.

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

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

Table of contents:

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

=====
SECURE YOUR SERVERS WITH 128-BIT SSL ENCRYPTION
=====
Guarantee transmitted data integrity, secure all communication sessions and more with SSL encryption from Thawte - a leading global certificate provider.

Learn more in our FREE GUIDE - click here to get it now:
<http://www.gothawte.com/rd126.html>
=====

General security news

MICROSOFT'S RESPONSIBLE VULNERABILITY DISCLOSURE
For almost a decade, a debate over the concept of Full Disclosure has reared its ugly head. Carried out on BBSs, newsgroups, security conferences, mail lists, parties, coffee shops and everywhere else, the Full Disclosure debate can be called "long standing" to say the least. As with everything in the computer industry before, Microsoft is doing nothing new here. Like many times before, Microsoft is re-inventing the wheel and opting for something other than round.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.attribution.org/security/rant/z/ms-disclose.html>

INTERVIEW: NEAL WALFIELD
KernelTrap spoke with Neal Walfield of the GNU/Hurd development team. The Hurd is a radical departure from many UNIX concepts. It is a unique and interesting approach to solving many of the problems found in current

operating systems. While it's not yet production grade, it's evolved enough to be quite usable.

Link: <http://www.kerneltrap.com/article.php?sid=375&mode=thread&order=0>

INTERVIEW: VINNY GULLOTTO

Vinny Gullotto is director of research for the Antivirus Emergency Response Team at McAfee. Gullotto has worked for Avert since 1997 and has been involved in the design and development of the engine and detection technology that forms the basis of its antivirus work. He liases closely with the FBI and other security agencies to tackle emerging virus threats.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.networknews.co.uk/Features/1126731>

BOOK REVIEW: COUNTER HACK

If you have a network connected to the Internet, you will inevitably be hacked. This book shows how to avert such attacks with a counter hack. For a wide-ranging overview of how to secure a system against myriad adversaries, do yourself, your employer, and your networks a favor and read Counter Hack.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/documents/s=1780/urm0111a/0111a.htm>

IMPLEMENTATION OF HONEYNETS

A honeynet is a tool that can be used to learn and force hackers to a controlled environment. Also the methods and tools used by intruders when compromising a system can be documented. Honeynets consist of a network of production systems that will be designed to be compromised.

Link: <http://www.securitytimes.com/article.php?sid=77>

OVERVIEW OF LIDS, PART THREE

This is the third part of a four-part article devoted to the exploration of LIDS, a Linux kernel patch that will allow users to take away the all-powerful nature of root. This installment will discuss granting capabilities, the LIDS-specific capabilities, ACL inheritance and time-based ACLs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1510>

BRUTE-FORCING WEB SESSION IDS

Aron Miller submitted the following - David Endler wrote a paper entitled "Brute Force Exploitation of Web Application Session IDs" where he explains the details and methods for hijacking web sessions using some familiar sites as examples.

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

TWO YEARS FOR GETTING FREE DIRECTV SERVICE

Dandrich Wayne submitted the following - "A California resident nabbed by the FBI for his alleged role involving the reprogramming of access cards for pirating satellite TV signals received a prison term pf 2 years."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.skyreport.com/skyreport/nov2001/111201.htm#two>

PRINTERS COULD BE SECURITY RISK

Security experts are warning that many system and network administrators may have overlooked multiple vulnerabilities in several implementations of line printer systems software. Researchers at CERT said the problems relate to buffer overflow issues that let remote users gain root access to servers.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2099057,00.html)

[bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2099057,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2099057,00.html)

RESEARCHERS PROBE DARK AND MURKY NET

For a variety of reasons ranging from contract disputes among network operators to simple router misconfiguration, over five percent of the Internet's routable address space lacks global connectivity, according to the results of a three-year study by Arbor Networks.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/282)

[bin/news.cgi?url=http://www.securityfocus.com/news/282](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/282)

DDOS HOSTS AND SSH PROBLEMS

Threads on security newsgroups have suggested that hackers may be breaking into Linux boxes running the SSH1 protocol, using a known vulnerability in the SSH cyclic redundancy checksum that was published late last month. Writing on BugTraq William Salusky, of security firm DMZS, said: "It appears that someone may be building up a network of [potential] DDos hosts."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1126812)

[bin/news.cgi?url=http://www.vnunet.com/News/1126812](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1126812)

SIFTING THROUGH DATA TO DETECT NEW ATTACKS

In the wake of Sept. 11, security experts working to prevent future attacks are taking a closer look at computer software that helps retailers mail catalogs and credit companies combat fraud.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.boardwatch.com/reuters/111301_gt7.htm)

[bin/news.cgi?url=http://www.boardwatch.com/reuters/111301_gt7.htm](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.boardwatch.com/reuters/111301_gt7.htm)

ORACLE EXTREMELY SECURE?

Larry Ellison told computer hackers that his software is so secure they would never be able to break into Oracle's Web site, a boast that may be taken by many as a challenge. "This is a very dangerous thing to say - I'm not inviting a bunch of hackers to bring down the Oracle Web site, but so far, with more than 1000 attacks a day, we've had no downtime, no interruption of service."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,70663,00.asp)

[bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,70663,00.asp](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,70663,00.asp)

BUG SECRECY VS. FULL DISCLOSURE

Bruce Schneier writes: "Scott Culp, manager of the security response center at Microsoft, published an essay describing the current practice of publishing security vulnerabilities to be "information anarchy." He claimed that we'd all be a lot safer if researchers would keep details about vulnerabilities to themselves, and stop arming hackers with offensive tools. Last week, at Microsoft's Trusted Computing Forum, Culp announced a new coalition to put these ideas into practice."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2824251,00.html)

[bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2824251,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2824251,00.html)

HOW COMPUTER WORMS WORK - AND WHY THEY NEVER DIE

Although their names are not necessarily in the latest headlines, security bulletins or virus alerts, old computer worms such as Magistr, Sircam and, more recently, Nimda, continue to stay atop the threat lists of many anti virus firms. Why can't we squash them?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.osopinion.com/perl/story/14733.html>

CYBERCRIME TREATY GETS GREEN LIGHT

A controversial treaty that tries to tackle cybercrime has been adopted by the 43-nation Council of Europe. The treaty outlaws some online activities such as fraud and child pornography, clarifies some jurisdictional issues and outlines what police forces can do when pursuing computer criminals.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://news.bbc.co.uk/hi/english/sci/tech/newsid_1651000/1651381.stm

PREVENTING VIRUS INFECTIONS

Merely owning antivirus software is not enough to protect your PC from infection. The software requires a certain amount of care and feeding beyond the initial purchase. Fortunately, a few minutes of prevention can prevent hours of frustration during a real attack.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2824299,00.html>

FIREWALL POLICY

Firewall Definition: For purposes of this policy, firewalls are defined as security systems that control and restrict both Internet connectivity and Internet services. Firewalls establish a perimeter where access controls are enforced. Connectivity reflects which systems can exchange information.

Link: <http://www.securitytimes.com/article.php?sid=82>

DO-IT-YOURSELF INTERNET ANONYMITY

How do you make a truly anonymous post to a newsgroup or a BBS? How do you keep the Web sites you visit a secret? How do you send e-mail and ensure that its contents can't be read by someone who intercepts it? How do you chat anonymously?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22831.html>

WIRELESS SECURITY IS CONCERN, SAYS HANDSPRING

However, one of the not-so-obvious aspects of the increasing widespread "mobile Internet" is security, said Chief Product Officer Jeff Hawkins. Handheld communication devices are on all the time, he said, "and we've never tested the security of the cell networks." Being constantly connected to a carrier that is then connected to the Internet is a recipe for trouble, he said. "The opportunities for creating havoc here are very large."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,70864,00.asp>

FINDING SECURITY IN A CAVE

Looking for a safe place to put your primary or backup data center or

co-location services? Try a 100-year-old former gypsum mine.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.informationweek.com/story/IWK20011114S0009>

ZIMMERMANN: MORE PIE PLEASE

Phil Zimmermann, inventor of PGP and chairman of the OpenPGP Alliance, doesn't play the banjo, as mainstream media has reported. He showed up at the Annual Linux showcase keysigning Birds of a Feather (BoF) to set the record straight about the banjo thing and, more importantly, to talk about keysigning, among other things.

Link: <http://www.linuxjournal.com/article.php?sid=5605>

LINUX SECURITY QUICK-START GUIDES

After many months of work, Hal Burgiss has finished the first version of his very thorough Linux Security Quick-Start Guides.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/feature_stories/feature_story-93.html

UNDERSTANDING & INSTALLING SELINUX

Security Enhanced Linux is a NSA sponsored Linux project to develop a more secure Linux. SELinux is a set of Linux kernel patches and utilities designed around a usable but mandatory access control system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/site-stories/2001/1113.selinux.html>

CISCO - MULTIPLE VULNERABILITIES IN ACL

Six vulnerabilities involving Access Control List (ACL) have been discovered in multiple releases of Cisco IOS Software Release for Cisco 12000 Series Internet Routers. Not all vulnerabilities are present in all IOS releases and only line cards based on the Engine 2 are affected by them.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cisco.com/warp/public/707/GSR-ACL-pub.shtml>

AUTHENTICATION AS THE FOUNDATION FOR EBUSINESS

This article outlines the reasons why authentication is critical for a successful business, along with a discussion of the two main security methods it can be applied to. Additionally, this article will discuss authentication methods that are currently available, along with some factors that businesses must take into account to ensure they choose an authentication system that makes the most sense for them.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1513>

CISCO HIGH-END ROUTERS IN DOS PERIL

Cisco has issued a fix for a flaw which potentially makes its high-end routers susceptible to denial of service attacks. The performance of Cisco 12000 series routers can be degraded when they have to send a large number of Internet Control Message Protocol unreachable packets, something that usually happens as a result of heavy network scanning.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22869.html>

SECURITY REVOLUTION IN TOP GEAR

The security revolution is in top gear this week at the Comdex trade show, as new and improved products resourcefully related to security were showcased.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computing.vnunet.com/News/1126909>

WIRELESS NETWORKS VULNERABLE IN SYDNEY

A recent analysis conducted by the X-Force team in Australia tested the security of wireless networks operating within Pitt St, Sydney - a major retail and business centre. The team discovered 12 wireless networks that were easily accessible and vulnerable.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2099348,00.html>

AMERICAN MUSLIM COUNCIL SECURITY PROBLEMS

Vnunet reported that the American Muslim Council is furious after its website was hacked a few days before the start of its holy month of Ramadan. When you read the article you see that they weren't hacked, but it looks like the attacker got access to their mailing list.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1126902>

JAPAN TO SIGN CONVENTION ON CYBERCRIME

Yoshi contributed the following - "Japanese government plans to sign the Convention on Cybercrime, designed to deal with international crimes connected to the Internet. Actions that will be regarded as crimes include infringing on copyrights, interrupting and intercepting the sending and receiving of data, producing, acquiring, possessing and distributing child pornography and producing, possessing and distributing computer viruses".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.yomiuri.co.jp/newse/20011116wo02.htm>

CONFIDENTIALITY CLAWS

Researchers at Imperial College London are developing mathematical and programming techniques to better assess the extent that systems prevent the leakage of confidential information.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/22886.html>

FINGERPRINTING PORT 80 ATTACKS

CGIsecurity.com released a paper that describes the most common attack signatures in both web server and web application security. 11 pages long document was also a base point for a set of Snort rules connected with attacks on port 80.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cgisecurity.com/papers/fingerprint-port80.txt>

=====

HNS Security Database

=====

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

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

=====

Security issues

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

VULNERABILITY IN CDE SUBPROCESS CONTROL SERVICE

Internet Security Systems X-Force has discovered a buffer overflow in the Subprocess Control Server (dtspcd) in all Unix variants running CDE (Common Desktop Environment) system. The vulnerability in the dtspcd daemon may allow remote attackers to execute arbitrary commands on a target system with super user privilege.

Link: <http://www.net-security.org/text/bugs/1005617438,27923,.shtml>

RUNAS SENSITIVE DATA EXPOSURE

The command line utility "RunAs" leverages the RunAs service in an effort of launching an application in a distinct security context. However, the utility suffers from the fact that the buffer is never erased after the application terminates execution.

Link: <http://www.net-security.org/text/bugs/1005617535,10676,.shtml>

THTTPD AND MINI_HTTP PERMISSION BYPASS VULNERABILITY

The problem lies in the way the httpd daemon handles file requests. If a file is marked 403(not world readable), or is in a directory that is password protected, then it is possible to remotely view these files. The thttpd webserver is only effected when the chroot option is used(Kinda ironic), and all versions of mini_httpd webserver appear to be affected.

Link: <http://www.net-security.org/text/bugs/1005702073,1677,.shtml>

WIN2K/XP TERMINAL SERVICES IP SPOOFING

Terminal services has a bug that allows an attacker to cause both the Terminal Services Manager and the Event Log to record a spoofed IP address for Terminal Services connections. Although the operating system itself is not fooled, if an administrator is not aware of the issue he would not have reason to distrust the IP address reported by Terminal Services. The vulnerability is exploited by sending traffic through a router that uses Network Address Translation (NAT). Note that although we have used the term "spoofing", this is not related to other well-known TCP-IP spoofing techniques.

Link: <http://www.net-security.org/text/bugs/1005843327,60790,.shtml>

STEALING COOKIES FROM ULTIMATE BULLETIN BOARD

Posting something like this UBB tag:

[IMG][http://about: test\"onerror= \"top.location.href='http://punk.tomsk.ru';](http://about: test\) [/IMG]
to Infopop Ultimate Bulletin

Board, we are able to redirect users browser to <http://punk.tomsk.ru>

Link: <http://www.net-security.org/text/bugs/1005872033,66809,.shtml>

ACTIVEPERL PERLIS.DLL BUFFER OVERFLOW VULNERABILITY

NSFOCUS Security Team has found a exploited buffer overflow vulnerability in a dynamic link library (perlIS.dll) of ActivePerl when handling overlong filename. Exploit of it, an attacker could remotely execute arbitrary code.

Link: <http://www.net-security.org/text/bugs/1005872395,50017,.shtml>

AT&T/@HOME CABLE MODEM ENUMERATION

AT&T/@Home has standardized on using DHCP for end-user workstation configuration. This configuration is done via the standard DHCP implementation, but also is configured to send a string to the DHCP server with the "hostname" of the client.

Link: <http://www.net-security.org/text/bugs/1005921249,71418,.shtml>

BUFFER OVERFLOW IN SOLARIS 'FORMAT' COMMAND

The 'format' utility provided with the Solaris 2.6 and 2.8(and probably others as well) does not handle command line arguments correctly. Any argument that is passed on the command line that is not a switch is treated as a path to a disk device. Each of these arguments is then strcpy()'d into a buffer of length MAXPATHLEN which is set to 1024 at compile time. This is done without any bounds checking leaving the possibility of an overflow.

Link: <http://www.net-security.org/text/bugs/1005939098,1386,.shtml>

NETWORK TOOL 0.2 ADDON FOR PHPNUKE VULNERABILITY

Network Tool 0.2 does not check for special meta-characters like &;`\"|*?~<>^()[]{\$ comming from the \$hostinput variable.

Asking the Php script for Pinging, Nmap, or traceroute this kind of adresse <www.somehost.com;ls -al> will allow any user to run " ls -al " command as whatever user runs the web server.

Link: <http://www.net-security.org/text/bugs/1005939215,20823,.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>

BALTIMORE TECHNOLOGIES ANNOUNCE WEBSWEEPER 4.1

Baltimore Technologies, a global leader in e-security, announced that the latest version of its Web content security solution, WEBSweeper 4.1, offers optional restriction of more than 689 million web pages in 40 categories with provision for 14 languages. WEBSweeper 4.1 also offers support for Microsoft Windows 2000 as well as performance gains of up to 50 percent when using Windows 2000 multiprocessor support.

Press release:
< <http://www.net-security.org/text/press/1005616929,75642,.shtml> >

AUTHENTOR RELEASES SMARTPATH 2.2

Authentor Systems Inc. released version 2.2 of its SmartPath Web access management and authentication system. SmartPath 2.2, which consists of hardware and software components as well as a proprietary behavior-profiling engine, provides businesses with advanced levels of network security and simplified user management. The release features new behavior-profiling options, including access frequency and access location, to enhance traditional authentication methods and ensure that users are who they claim to be. Out-of-the-box application integration and automation of security-policy configurations will help companies deploy their e-business initiatives quickly and reduce administrative costs. In addition, the new release provides extended logging and reporting capabilities that support compliance with a variety of federally mandated security and privacy regulations.

Press release:
< <http://www.net-security.org/text/press/1005616969,48786,.shtml> >

ICSA LABS ANNOUNCES 3RD QUARTER PRODUCT

TruSecure Corporation, a leading security services provider, announced that its ICSA Labs division has certified twenty-three Internet Protocol Security (IPSec) and firewall products in Q3 2001 that meet the industry's most stringent testing criteria. The ICSA Labs' Certification Program provides assurance to the user community that Certified products meet industry-accepted product standards worldwide.

Press release:
< <http://www.net-security.org/text/press/1005650818,65105,.shtml> >

NEXT GENERATION MCAFEE.COM PERSONAL FIREWALL

McAfee.com, a leading provider of Web security services, announced the next-generation of the McAfee.com Personal Firewall (MPF), which will incorporate advanced intrusion detection, a graphical trace utility and will be compatible with the new Windows XP operating system. This newly redesigned service will give consumers and businesses robust, state-of-the-art and up-to-date protection for their Internet connections from hackers, intruders and other unwanted network traffic.

Press release:

< <http://www.net-security.org/text/press/1005654540,30698,.shtml> >

MERILUS LAUNCHES PREFERRED RESELLER PROGRAM

Merilus, Inc. announced that it has now launched its Preferred Reseller Program, wherein value added resellers (VARs) and system integrating resellers of Merilus' suite of computer security products may be eligible to receive a variety of valuable benefits for reaching sales targets.

Press release:

< <http://www.net-security.org/text/press/1005871848,7165,.shtml> >

ANTI-NETWORK TERRORISM TECHNOLOGY UNVEILED

As companies and the United States Government's Internet sites and networks are under increased terrorist attacks from so-called Distributed Denial of Service attacks, Cyber Operations announced the availability of real-time prevention against Distributed Denial of Service attacks via their Anti-Network Terrorism (A.N.T.) technology.

Press release:

< <http://www.net-security.org/text/press/1005872593,11604,.shtml> >

CYLINK LINK ENCRYPTOR T3 (CLE T3) RELEASED

Cylink Corporation introduced the Cylink Link Encryptor T3 (CLE T3) for securing high-speed data communications. The CLE T3 is the latest addition to Cylink's comprehensive set of leased-line security solutions. Designed to meet the market's requirements for speed and reliability, the CLE T3 supports Triple-DES and provides secure data communications at the full T3/DS3 data rate of 45 Mbps.

Press release:

< <http://www.net-security.org/text/press/1005872636,58366,.shtml> >

ZONE LABS SUES SYGATE FOR PATENT INFRINGEMENT

Zone Labs Inc., a leading creator of Internet security solutions, announced

that it has filed a patent infringement complaint against Sygate in the federal district court for the Northern District of California. In its filing, the San Francisco company alleges that Sygate Technologies, Inc. is infringing upon U.S. Patent No. 5,987,611 and seeks an injunction to prevent Sygate from continuing the infringement as well as monetary damages.

Press release:

< <http://www.net-security.org/text/press/1005872771,73712,.shtml> >

NSTL EVALUATES PESTPATROL SOFTWARE

When exterminating computer pests is the goal, IT personnel have a new resource to help achieve it. National Software Testing Labs (NSTL), an independent testing service, announces the availability of a test report that ranks the leading pest-detection software programs according to their detection success rates.

Press release:

< <http://www.net-security.org/text/press/1005874209,7543,.shtml> >

THE SOUTHWEST CYBERTERRORISM SUMMIT ANNOUNCED

DallasCon.com announced a bold move in the war against cyber-terrorism. The Southwest CyberTerrorism Summit to be held May 4, 2002 in Dallas, TX will feature cutting-edge presentations from both underground hackers and from industry security experts. Topics include Wireless Hacking, Cyber-attacks, Information Warfare, Privacy, Computer Viruses, Industrial Espionage and Identity Theft.

Press release:

< <http://www.net-security.org/text/press/1005939480,63779,.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

XACTA TRAINING

Xacta Web C&A has been developed to help our customers conduct a complete and meaningful security certification and accreditation program. This requires that users develop not only an understanding of how to

operate the software itself, but also gain an appreciation of why and how compliance with government/industry C&A processes is beneficial to an organization in the short- and long-term.

A typical training course provides an overview of the DITSCAP/NIACAP process as well as extensive hands-on instruction and practice with the application. The course also includes detailed tutorials on the use of the Xacta Web C&A product to generate a DITSCAP/NIACAP-compliant SSAA document.

Read more:

< <http://www.security-db.com/product.php?id=754> >

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

< <http://www.security-db.com/company.php?id=172> >

INTERNET SECURITY SERVICES

Corporates and Business Organizations cannot survive in the e-commerce world without knowing the intricacies of the internet. The company needs to share and receive information essentially through the Net; this being the fastest known method to date. Well, there's where the security check comes under focus. Your company's private network has to be prevented from being penetrated and tampered by some unwanted elements or hackers.

Read more:

< <http://www.security-db.com/product.php?id=1197> >

This is a product of Highband Communications Pvt. Ltd., for more information:

< <http://www.security-db.com/company.php?id=283> >

ENGARDE LINUX

EnGarde is a secure distribution of Linux engineered from the ground-up to provide organizations with the level of security required to create a corporate Web presence or even conduct e-business on the Web. It can be used as a Web, DNS, e-mail, database, e-commerce, and general Internet server where security is a primary concern.

Read more:

< <http://www.security-db.com/product.php?id=889> >

This is a product of Guardian Digital, Inc., for more information:

< <http://www.security-db.com/company.php?id=217> >

=====
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>
=====

Featured article

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

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

AN ANALYSIS OF THE RADIUS AUTHENTICATION PROTOCOL

RADIUS is a widely used protocol in network environments. It is commonly used for embedded network devices such as routers, modem servers, switches, etc. This analysis deals with some of the characteristics of the base RADIUS protocol and of the User-Password attribute.

Read more:
< <http://www.net-security.org/text/articles/dl/An%20Analysis%20of%20the%20RADIUS%20Authentication%20Protocol.htm> >

Security Software

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

SKIN 0.1.1

Skin is a TCP/UDP port scanner that allows the user to guess what services are run on the ports scanned. It uses a plugable architecture, with one module for each security test, and with a special network library for plugins so adding one is very easy.

Info/Download:
< <http://www.net-security.org/various/software/1006171420,82621,linux.shtml> >

ONLINE KEYS 1.0

Online Keys is a small utility to safely and confidentially store all your passwords on an encrypted file. Add all the services you have an account with. Use different usernames and passwords for each if you want. Online Keys will remember them all along with the web addresses for each service.

Info/Download:

< <http://www.net-security.org/various/software/1006171652,36951,windows.shtml> >

Questions, contributions, comments or ideas go to:

Help Net Security staff

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