

HNS Newsletter
Issue 98 - 18.02.2002
<http://net-security.org>
<http://security-db.com>

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

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

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

Table of contents:

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

=====
Free Webshield e500 Info Kit
=====
Configure and forget with McAfee Webshield e500
appliance, scan all potential virus-carrying
protocols, even POP3. McAfee's Webshield e500
makes gateway defense instant.
=====
Click for more - <http://www.net-security.org/ad/nai>
=====

General security news

UNPATCHED IE6 SECURITY HOLES

As an interesting reference on security issues with Redmond's favorite browser, Thor Larholm and Tom Gilder compiled a list of unpatched Internet Explorer 6 security holes.

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

MORNINGSTAR CANADA SECURITY ISSUES

Web Security Consultant Noam Eppel posted information about some security problems within MorningStar Canada service. As noted, the company covered it all up, so his advisory ironically starts with - "We recognize that your financial information is very sensitive, and protecting the privacy of this information is a top priority for us." - MorningStar Canada.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.noameppel.com/research/Morningstar.ca.html>

SECURITY ON ALL FRONTS

Much attention in the past few months has focused on how airports and airlines can use IT to improve security in terminals and on planes.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.informationweek.com/story/IWK20020207S0017>

ACCUSED DEA DATA-THIEF ON THE LAM

A former federal drug agent charged last year with peddling data from law enforcement computers has skipped bail, on what would have been the first day of his trial.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/326>

WORRIED ABOUT WIRELESS SECURITY? HERE'S A SOLUTION

Security for most wireless networks is questionable at best. Want to improve the situation? Use a wireless gateway. Lee Schlesinger recommends one that will safeguard your network without sacrificing quality of service.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2846578,00.html>

HOW SECURE IS .NET?

Microsoft's willingness to open up source code to experts in the security field and then get their seal of approval is a good sign that Microsoft is taking .NET security seriously.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/specials/2000/10/enterprise/techrepublic/2002/06/article001.html>

LISTING SECURITY MEASURES IN ANNUAL REPORTS

While no network can ever be completely secure, being secure enough is desirable, if not legally required. The Securities and Exchange Commission now demands that companies list security measures in their annual reports, and a certain amount of due diligence is required. Not for the first time, the actions of the network manager directly influence shareholder value.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/Features/1128996>

MORE LINUX VULNERABILITIES BEING REPORTED

Linux security experts take issue with recent reports from vnunet.com and from WinInformant.com that suggest Windows is more secure than Linux, based on statistics from SecurityFocus. But one Linux security guru says he's seeing more Linux security vulnerabilities reported in the last six months, mostly due to greater awareness on the part of Linux vendors.

Link: <http://www.newsforge.com/article.pl?sid=02/02/11/1340237>

CYBERCRIME BILL

A proposal being debated in Congress would stiffen anti-hacking laws, providing for life imprisonment in some cases.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,50363,00.html>

EMPLOYEE DATA EXPOSED ON WEB

A disgruntled former IT employee at telecommunications firm Global Crossing Holdings Ltd. has been posting the names, Social Security numbers and birth dates of company employees on his Web site.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO68168,00.html)

[bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO68168,00.html](http://www.computerworld.com/storyba/0,4125,NAV47_STO68168,00.html)

RIPTECH BUYING PARA-PROTECT CUSTOMERS

Last summer, Riptech bought the customers of California-based OneSecure Inc. when that company went through a reorganization. In December 2001, Riptech picked up more than 100 customers from Predictive Systems Inc.

In their latest acquisition, they are buying 50 clients from Para-Protect which will be shut down within the next 60 days according to their CFO Joe Ragan.

Link: <http://www.newsbytes.com/news/02/174376.html>

CHARNEY AN OMINOUS MS PICK

What are we to make of Microsoft tapping a former hacker prosecutor and IP lawyer for its top security spot? Nothing good.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/columnists/59)

[bin/news.cgi?url=http://www.securityfocus.com/columnists/59](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/columnists/59)

ICANN APPOINTS SECURITY CHAIRMAN

The Internet Corporation for Assigned Names and Numbers - the nonprofit group that oversees basic technical matters related to the Internet - has appointed a chairman for its newly formed standing committee on security and stability.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/news/2002/0212icann.html)

[bin/news.cgi?url=http://www.nwfusion.com/news/2002/0212icann.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/news/2002/0212icann.html)

CRYPTOLOGIC TAKES \$1.3M CHARGE FOR SECURITY BREACH

Upon breaking into the gambling software firm's servers, attackers reprogrammed slot machines and a craps table at two Web-based casinos which use the firm's software so that illicit players won every time they played. The net impact of the breach, which took place in August, on CryptoLogic was originally expected to be \$600,000, after an expected insurance claim of \$1.3 million.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/24032.html)

[bin/news.cgi?url=http://www.theregister.co.uk/content/55/24032.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/24032.html)

WIRELESS LANS RAISE SECURITY WORRIES

Sandia National Laboratories has begun testing wireless local area networks to determine whether they can meet the kind of rigorous security required for any Department of Energy facility.

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,83844,00.asp)

[bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,83844,00.asp](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,83844,00.asp)

SNMP SECURITY FLAW THREATENS NETWORK INFRASTRUCTURE

CERT said the problem might allow malicious hackers to snarl equipment ranging from routers and switches at the heart of the Internet to the high-speed modems that deliver Net access to cable and DSL customers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityfocus.com/news/328>

FREE, DEPENDABLE IDS

Any enterprise in search for a host-based IDS to protect its Linux environment has found itself stymied by a lack of available solutions. The host-based approach offers advantages such as the capability to detect attacks that network-based solutions sometimes miss and greater flexibility for fine-tuning which activities should be monitored.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/tc/xml/02/01/28/020128tcsnare.xml>

CRACKDOWN ON SPAM

Federal regulators kicked off a crackdown on junk e-mail with an announcement that they had settled charges against seven people accused of running an e-mail pyramid scheme.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2002/TECH/internet/02/12/tech.spam.reut/index.html>

PORN HUNTERS UNWELCOME IN CANADA?

Proposed legislation would make it a crime to do so much as alert the authorities that a website is peddling kiddie porn.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,50325,00.html>

THE SNMP FIASCO: STEPS YOU NEED TO TAKE

Thomas C Greene writes: "We received a bulletin from Counterpane saying that the vulnerability does not appear to have been exploited yet. So basically, you're playing 'beat the clock' with the blackhat community. Second, this is a developing story to which we haven't got any final answers and for which our recommendations are both preliminary and incomplete, being cobbled together from numerous bulletins and a bit of homebrew tinkering."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/24042.html>

DSHIELD - PRELIMINARY SNMP DATA

On February 12th DShield.org updated the following - "At this point, we do not see a significant increase in SNMP scanning traffic. None of the SNMP sources reported lately scanned more than one target, which usually indicates either a mistake (someone entered the wrong IP into their network admin tool) or a false positive (someone is rejecting legitimate SNMP traffic). We will continue to monitor and update this page as new data is added to our database".

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

VALENTINE'S DAY - BEWARE OF VIRUSES

With Valentine's Day almost upon us, computer users are being warned about the dangers of recurring socially engineered viruses. Some of the most successful viruses over the last couple of years have used the promise of love to get users to set off the damaging electronic payload.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computing.vnunet.com/News/1129212>

CISCO BOOSTS ITS SECURITY OFFERINGS

Moving to help its customers manage their security architectures and help those systems keep up with traffic, Cisco Systems announced new software for its Pix Firewall platform and the availability of new hardware models to join that line.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/02/02/13/020213hnciscosecure.xml>

NAI SELLS FIREWALL BUSINESS

Secure Computing has acquired the Gauntlet firewall and VPN business from Network Associates for an undisclosed amount.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/24050.html>

MSN MESSENGER WORM ENTICES THE UNWARY

The 'Cool Worm' relies on malicious Web sites and exclamation points to spread its message.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/331>

SEVEN HACKERS JAILED IN TWO YEARS IN THE UK

Industry experts are calling for a revamp of the Computer Misuse Act after the government revealed that only seven hackers have been imprisoned in the past two years. At the same time an influential lobby group has warned that improvements in tackling e-crime are needed before its growth overwhelms the UK's ability to fight back.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1129242>

HOUSE CYBERTERRORISM BILL WOULD PROTECT ISPS

Another cybersecurity proposal is wending its way through the U.S. Congress, this one designed to relax the liability of Internet service providers when reporting a potential threat.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/02/02/13/020213hncyberbill.xml>

PREVENTING AND DETECTING INSIDER ATTACKS

Insider attacks are particularly insidious and difficult to protect against. This article will offer a brief overview of some strategies to prevent inside attacks and to detect such attacks when they occur.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1546>

ADMINISTERING LINUX IPSEC VIRTUAL PRIVATE NETWORKS

This article will discuss some of the more advanced features of FreeS/WAN that you can leverage to implement flexible and reliable IPSec VPNs.

Link: <http://www.samag.com/documents/s=4072/sam0203c/sam0203c.htm>

SNORT SNIFFS OUT A COMMERCIAL FUTURE

The creator of the popular open source intrusion detection system gets \$2 million in venture capital for a Snort start-up. He's moving the company out of his suburban Maryland living room into an 8,000 square foot furnished office.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/332>

SAFEWEB PROMISES SECURITY FIX

The CIA-funded firm that promises users anonymous Web browsing says it will issue a patch to repair well-documented bugs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/ebiz/0,1272,50424,00.html>

ISP ATTACKERS MAKING A CLEAN GETAWAY?

The attackers that brought down UK Internet Service Provider Cloud Nine look almost certain to avoid prosecution.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://zdnet.com.com/2100-1105-837412.html>

WAS DIGITAL SECURITY WARNING TOO HASTY?

Security experts gave mixed reviews to the way in which a software-reliability company disclosed a bug in Microsoft's newest tools for building applications for its .Net framework and Windows OS. "There is no way that Microsoft could fix this in a day," said Al Huger, vice president of SecurityFocus. "Full disclosure has to be coupled with responsible disclosure."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.com.com/2100-1001-838096.html>

NSDAP SOLARIS ROOTKIT TRIPWIRE REPORT

If you are interested in what NSDAP rootkit does, Shawn posted a tripwire report which shows what files are added/deleted/changed on the compromised box.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://codepiranha.org/~pakkit/rootkits/tripwire_report.txt

HACKING AND SPYING RIVALS IN JAPAN

An aerospace company employee hacked into the computer network of Japan's space agency in order to spy on a rival firm, an official said yesterday. The worker for NEC Toshiba Space System Co. illegally accessed Mitsubishi Electric Corp.'s antenna designs for a high-speed Internet satellite 2 months ago.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.canoe.ca/CNEWSspace0202/14_space-ap.html

SCANNING FOR SNMP VULNERABILITIES

SANS has released a scanning tool called SNMPing which will find SNMP daemons running on a TCP/IP network. It defaults to port 161, but you

can enter the port of your choice.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/24083.html>

GOVERNMENT, NEW PRODUCTS GET TOP BILLING AT RSA

Cybersecurity and the protection of critical computer infrastructure have become a hot topic at trade shows, and the RSA Security Conference 2002 doesn't figure to be any different.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_811343_5055_1-2793.html

=====
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 issues

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

ISS ON PROTOS REMOTE SNMP ATTACK TOOL

Speaking of SNMP security issues, ISS notes that the following vendors may or may not be vulnerable to the PROTOS SNMP tool: 3Com, Alcatel, Amber Networks, Arbor, Banyan Networks, Canon, Cisco, Compaq, Computer Associates, D-Link, Dell, Digi, Ericsson, Extreme networks, F5, Foundry, Fujitsu Siemens, HP, Hitachi, IBM, ICL, Intel, Juniper Networks, Lantronix, Laurel, Lotus Lucent, Marconi-Fore, Microsoft, Multitech, NET-SNMP, NetGear, Nokia, Nortel, Novell, SMC, Shiva, Siemens, Sumimoto, Sun Microsystems, Telebit, Teledat, Windriver, Xerox, Xylan, Zyxel.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.iss.net/security_center/alerts/advise110.php

CERT ADVISORY CA-2002-03 - SNMP PROBLEMS

CERT/CC published a thorough advisory entitled Multiple Vulnerabilities in many Implementations of the Simple Network Management Protocol, which gives a lot of information regarding these problems and the solutions for them.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/advisories/CA-2002-03.html>

CERT'S SNMP VULNERABILITIES FAQ

As an interesting and usefull abstract to the CERT advisory linked below, CERT published Simple Network Management Protocol (SNMP) Vulnerabilities Frequently Asked Questions (FAQ).

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/tech_tips/snmp_faq.html

HP J3210A ADVANCESTACK AUTHENTICATION BYPASS

A problem with the HP switch allows some users to change configuration of the switch. A bug introduced in the HP AdvanceStack J3210A that could allow users full access on the switch. Upon taking advantage of this vulnerability, the user could change the configuration of the switch and could change admin password.

Link: <http://www.net-security.org/text/bugs/1013423129,83653,.shtml>

ISS BLACKICE KERNEL OVERFLOW EXPLOITABLE

Matt Taylor posted to several security mailing lists stating that BlackICE was vulnerable to a Denial of Service attack that could result in the BlackICE service crashing and or blue screens of the remote system. There was various talk on mailing lists about the "Denial of Service" attack and what other versions it affected. The day after Matt posted his DoS attack against BlackICE to various mailing lists, ISS (Makers of BlackICE) then posted their security advisory to notify clients of the new vulnerability and a work around until a patch is released. ISS's advisory also described the vulnerability as a denial of service attack. As of yet we've not seen anyone produce accurate technical information about the "Denial of Service" vulnerability. Ryan Permech and Riley Hassell however conducted research recently that shows the BlackICE "Denial of Service" vulnerability is in fact an exploitable buffer overflow. Therefore allowing anyone to remotely compromise users of BlackICE and potentially RealSecure Server Sensor.

Link: <http://www.net-security.org/text/bugs/1013423685,31598,.shtml>

ARESCOM NETDSL-1000 TELNETD DOS

The router leaves a telnet-port open for the ISP to reconfigure the router if the need arises. The software serving this telnet port is not aware of actual sessions: The telnet connection gets wired in software directly to something behaving more like a serial console. When you connect to it, it asks for a configuration password. If you pass it a long string (say the good old 'a'x256) the login system will break this request in a couple of shorter chunks and interpret each of these chunks as a separate attempt to log in. After three or so failures, the telnet connection is closed off.

Link: <http://www.net-security.org/text/bugs/1013423733,8131,.shtml>

ACCOUNT THEFT IN MAKEBID AUCTION DELUXE 3.30

MakeBid Auction Deluxe is a commercial PERL CGI which allows web users to add items to an online auction. The following fields are not properly sanitized when placing a new item on auction:

- + City/State/Zip of new auction registrant
- + Title Descripton of new auction item
- + Item Description for new auction item

This allows an attacker to place an item on auction with potentially malicious code in the description fields. Thus, being executed by simply viewing the item.

Link: <http://www.net-security.org/text/bugs/1013423882,40589,.shtml>

SECURITY ISSUE IN ICEWARP

When you create a new user , icewarp gives him a static number. If this user does not logout after checking his inbox you can access his inbox.

Link: <http://www.net-security.org/text/bugs/1013423939,82941,.shtml>

MSN MESSENGER HIJACKING

There has recently been reported some privacy problems in MSN Messenger. However, these problems pale in comparison to what can be done if you use MSN Messenger through unpatched IE vulnerabilities. Using these, a malicious programmer can easily hijack the MSN Messenger client from a user, allowing him/her (among others) to silently and automatically read their contact list (harvesting email addresses) and impersonate the user by sending arbitrary messages, email or local files to anyone.

Link: <http://www.net-security.org/text/bugs/1013424008,89936,.shtml>

INSTANTSERVICES MINIportal MULTIPLE VULNERABILITIES

The FTP server coming with MiniPortal contains multiple vulnerabilities which could be exploited by an attacker to obtain user account information, read access to any file on the local HD and which could lead to arbitrary code execution.

Link: <http://www.net-security.org/text/bugs/1013424110,37572,.shtml>

SYBEX E-TRAINER DIRECTORY TRAVERSAL VULNERABILITY

The vulnerability that takes place is the infamous ".." directory traversal. With a specially crafted request to the web server you can view any file on the target's computer under the logged in users permissions.

Link: <http://www.net-security.org/text/bugs/1013520990,88200,.shtml>

IE AND ACCESS - MACROS ARE EXECUTED AUTOMATICALLY

GFI has recently discovered a security flaw within Internet Explorer which allows a malicious user to run arbitrary code on a target machine as it attempts to view a website or an HTML email. The problem is exploited by embedding a VBA code within a Access database file (.mdb) within an Outlook Express email file or Multipart HTML (mht) file.

Link: <http://www.net-security.org/text/bugs/1013598808,69363,.shtml>

TEMPORARY FILE HANDLING IN GNAT

The run-time library of the GNU Ada compiler (GNAT) handles temporary files in an unsafe manner. The impact depends on the application creating the temporary file. It ranges from temporary to permanent denial of service, from data eavesdropping to system compromise.

Link: <http://www.net-security.org/text/bugs/1013598893,79519,.shtml>

POWERFTP PERSONAL FTP SERVER VULNERABILITIES

The PowerFTP server contains multiple vulnerabilities which could provide an attacker with the capability to enumerate a system's structure, obtain read access to any file on the system and carry out a denial of service attack against it.

Link: <http://www.net-security.org/text/bugs/1013689972,6884,.shtml>

FALCON WEB SERVER AUTHENTICATION VULNERABILITY

Falcon Web Server supports virtual directory mapping and allows the server administrator to use a user-authentication scheme to protect the content of these directories. Due to a problem in the parsing of requests made to said directories however, it is possible to circumvent this authentication scheme and access any file in a protected directory without supplying the proper credentials.

Link: <http://www.net-security.org/text/bugs/1013690086,83027,.shtml>

BUFFER OVERFLOW IN MSHTML.DLL

mshtml.dll contains buffer overflow while parsing HTML with embedded ActiveX components. Stack overrun occurs during concatenation of two Unicode strings. It's possible to exploit this vulnerability to execute any code of attacker's choice (we do have proof-of-concept code, it will be published later with details of vulnerability). This overflow can only be exploited if "Run ActiveX Controls and Plugins" security option is enabled. *This option is disabled by default for Restricted Sites Zone Outlook 2000, Outlook Express 6.0 and prior with security update installed open all mail, but enabled by default in all different cases. This bug doesn't depend on Windows version.

Link: <http://www.net-security.org/text/bugs/1013690219,31764,.shtml>

NETWIN CWMAIL.EXE BUFFER OVERFLOW

CWMail is a fully featured Corporate Web Mail System for institutions or ISP's using the web as their primary means of access to email. CWMail is available for a wide variety of platforms and allows all email processing to be handled via a client web browser rather than from an email client package.

Link: <http://www.net-security.org/text/bugs/1013690277,79131,.shtml>

ETTERCAP - REMOTE ROOT COMPROMISE

Due to improper use of the memcpy() function, anyone can crash ettercap and execute code as root user.

Link: <http://www.net-security.org/text/bugs/1013772441,90571,.shtml>

=====
HNS Security Database

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

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

=====

Security world

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

NETOCTAVE CLOSES SECOND-ROUND FUNDING

NetOctave, Inc., a developer of security processors and security accelerator boards for the SSL (Secure Sockets Layer), IPsec (Internet Protocol Security), and IP Storage markets, announced that it has secured a second round of equity funding of \$7.8 Million. The round was led by Intersouth Partners and includes investments by Intel Communications Fund, Kitty Hawk Capital, MCNC, North Carolina Enterprise Fund, L.P and Wakefield Group.

Press release:

< <http://www.net-security.org/text/press/1013446766,33774,.shtml> >

GFI FINDS SECURITY FLAW IN IE AND MS ACCESS 2000

GFI, leading developer of email content checking and network security software, has discovered a security flaw in Internet Explorer and Microsoft Access 2000 that allows macros to be executed automatically on a victim's machine. GFI has notified Microsoft Corp., which issued an advisory (Microsoft Security Bulletin number MS02-005).

Press release:

< <http://www.net-security.org/text/press/1013522453,43462,.shtml> >

2002 INFORMATION SECURITY EXCELLENCE FINALISTS!

Information Security?magazine today announced the finalists for its 2002 Information Security Excellence Awards. The annual award program recognizes the IT/security industry's leading products as determined by the magazine's subscribers.

Press release:

< <http://www.net-security.org/text/press/1013527498,3181,.shtml> >

MCAFEE VISUAL TRACE EMPOWERS LAW ENFORCEMENT

McAfee.com, a leading provider of Web security services, announced that the company's advanced graphical trace utility, demonstrated last week on "The Oprah Show," is proving to be a valuable tool in deterring and apprehending online criminals.

Press release:

< <http://www.net-security.org/text/press/1013527711,21730,.shtml> >

FOUNDSTONE OFFERS SNSCAN

Foundstone Inc., the premier provider of security assessments and vulnerability protection, today announced SNScan, a freeware tool to quickly and accurately detect SNMP (Simple Network Management Protocol) enabled devices on a network.

Press release:

< <http://www.net-security.org/text/press/1013700994,88757,.shtml> >

SAFEWEB ADDRESSES VULNERABILITY IN PRIVACY TECHNOLOGY

SafeWeb, a leading provider of Web-based security and privacy technologies, announced that it will address JavaScript security vulnerabilities in its licensed consumer privacy technology that were highlighted in a recent a study. The company closed down the free privacy service in November 2001 for financial reasons.

Press release:

< <http://www.net-security.org/text/press/1013772264,56085,.shtml> >

COOL WORM CHILLS USERS' ONLINE CHATS

Sophos, a world leader in corporate anti-virus protection, is warning users to be cautious when using instant messaging platforms after a new worm was discovered. JS/Coolnow-A (aka Cool worm) targets MSN Messenger by exploiting a vulnerability in Microsoft Internet Explorer.

Press release:

< <http://www.net-security.org/text/press/1013773327,51929,.shtml> >

SECURITY TESTING MANUAL 2.0 SET FOR RELEASE

The Open Source Security Testing Methodology Manual (OSSTMM) is unique in that it is the first and most widely available standard in development for the comprehensive security testing of Internet systems and networks. Created by the Ideahamster organisation, the OSSTMM is a continuously evolving document with over 150 collaborators – ensuring that as IT focus changes and new developments in Internet security occur, the OSSTMM remains current and up to date.

Press release:

< <http://www.net-security.org/text/press/1013775748,35430,.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>
=====

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

GTA CONSULTING

GTA Consulting, is a security auditing service offering expert consultancy on your IT security policy, Internet security policy and acceptable use policy. 1 in 3 security breaches occur after a firewall has been installed. This is almost always down to mis-configuration during the installation process. It is advisable to have the security measures tested and audited. GTA offer a range of services to suit different customer needs, from penetration testing, to configuration verification. A firewall is there to enforce a security policy and we can ensure that it does!

Read more:
< <http://www.security-db.com/product.php?id=500> >

This is a product of Global Technology Associates Limited, for more information:
< <http://www.security-db.com/company.php?id=109> >

INCIDENT HANDLING

Incident handling is required when the security of a system or network has been compromised. Analysing and fixing a compromised network or server requires very high-end security skills. The exercise determines the extent of attack, identifies the possible source and takes corrective measures.

Read more:
< <http://www.security-db.com/product.php?id=1109> >

This is a product of Paladion Networks, for more information:
< <http://www.security-db.com/company.php?id=251> >

TINY PERSONAL FIREWALL

Tiny Personal Firewall represents smart, easy-to-use personal security technology that fully protects personal computers against hackers. Built on ICSA-certified security technology, it is also an integral part of The Tiny Software Centrally Managed Desktop Security (CMDS) system selected by the US Air Force for its approximately 500,000 desktop computers.

Read more:

< <http://www.security-db.com/product.php?id=490> >

This is a product of Tiny Software, for more information:

< <http://www.security-db.com/company.php?id=106> >

Security Software

All programs are located at:

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

DEEPCYPHER 3.0

Custom, high encryption application for mission critical message security. Runs on any web server, IIS, PWS, Apache and others, on any platform, Windows, Unix type, Mac and others, on a local intranet or the World Wide Web. Complete control over key length, cypher depth, and frequency of key generation. Key generation and encryption can be done in Streaming mode for 'no files/no trace' operation, or Static mode for 'no screen data' operation. Easy to use interface.

Info/Download:

< <http://www.net-security.org/various/software/1013774125,29466,linux.shtml> >

XMAIL 1.4

XMail is a fast, compact, and fully featured SMTP, POP3, POP3-SYNC, and Finger server. It supports multiple domains, authentication, spam protection, and many other powerful features.

Info/Download:

< <http://www.net-security.org/various/software/1013773684,93667,linux.shtml> >

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>