

HNS Newsletter  
Issue 95 - 14.01.2002  
<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

=====  
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>  
=====

General security news  
-----  
  
-----

#### TURNING SNOOPING INTO ART

In a collaborative art project called "Carnivore," Flash guru Joshua Davis and digital artist Mark Napier, along with other artists, have crafted programs that create audiovisual representations of data traffic that's observed and hijacked from a local area network.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,49439,00.html>

#### GENERIC HOST HARDENING FOR ANY COMPUTER

The ideas of "No one would want to attack my computer, because I have nothing of interest on it," or "There are more valuable sites to attack" are slowly being understood as incorrect. Anyone who has sat on a firewall or looked at its logs can attest to that.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://dcb.sun.com/practices/howtos/generic\\_host.jsp](http://www.net-security.org/cgi-bin/news.cgi?url=http://dcb.sun.com/practices/howtos/generic_host.jsp)

#### LISTEN UP, AOL

By Wednesday morning, Matthew Conover had impatiently waited a week. All he wanted was word one from AOL, acknowledging the two e-mailed warnings he'd sent them. Any indication would do. He just needed to know that the world's largest Internet service provider was working on the security hole he uncovered in its Instant Messenger feature...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.washtech.com/news/netarch/14475-1.html>

#### INCIDENT RESPONSE: BOOK REVIEW

According to the reviewer, this is a good introduction to incident response. Ben Rothke writes: "The authors go into detail about defining what an incident is and analyzing its various components to show how a multi disciplinary approach is required to rectify the situation."

Link: <http://www.unixreview.com/documents/s=1781/uni1009480592688/01121.htm>

#### VIRUS WRITERS HERE TO 'HELP'

Anyone whose computer or network has been disrupted by a piece of nasty code may be surprised to learn that some who create and release worms and viruses look upon their work as performing community service. Many virus writers say their "hobby" is a charitable donation of their time as they provide skills to help others who are less fortunate to learn about computer security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,49483,00.html>

#### SECURITY PROS TAKE CONTROL

Unlike network systems-management software, which can be administered from a central console that lets IT managers track, correlate, and diagnose problems, many security tools require separate management consoles. Now, this situation is changing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.informationweek.com/story/IWK20020103S0010>

#### HOAX E-MAIL WORM SPREADS

Anti-virus software company Ahnlab.com announced a hoax e-mail worm is rapidly spreading on the Internet, advising users that they don't have to delete the hoax worm because it is harmless. "The hoax worm, known as SULFNBK or SULFNBK.EXE, is a normal utility file, not a worm," said Ahnlab spokesman Hwang Mi-kyong.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.korealink.co.kr/kt\\_tech/200201/t2002010817021945110.htm](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.korealink.co.kr/kt_tech/200201/t2002010817021945110.htm)

#### US JUDGE ALLOWS FBI KEYBOARD SNIFFING

A federal judge in New Jersey has ruled that evidence secretly gathered by the FBI to catch an alleged mob loan shark can be used in a trial later this year.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1127991>

#### PLAY WITH THE LOVELY NETCAT

The first but secondary purpose of this article is to introduce you this nifty networking tool: /usr/bin/netcat which is well available from the Debian GNU/Linux under the package name netcat.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxgazette.com/issue74/zhaoway.html>

#### LAWMAKER: LEGALIZE HOME CD BURNING

Rep. Rick Boucher said that he intended to change a controversial copyright law to allow consumers to override technologies that prevent them from making digital copies of music, movies and software.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5101325,00.html>

#### MOBILE VENDORS TOLD TO TIGHTEN SECURITY

The UK government caused controversy among mobile phone vendors and network operators over the weekend following the announcement that it expected to see them toughen up on security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1128063>

#### REPORT: MANY U.S. FIRMS AT RISK FOR CYBERATTACKS

U.S. computer systems are increasingly vulnerable to cyberattacks, partly because companies are not implementing security measures already available, according to a report by the Computer Science and Telecommunications Board, part of the National Research Council.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2002/TECH/industry/01/08/security.reut/index.html>

#### AN INTRODUCTION TO DISTRIBUTED INTRUSION DETECTION SYSTEMS

This article will discuss distributed intrusion detection systems (dIDS), including the general setup of a dIDS and a fictional case study to demonstrate the distributed analysis abilities. It will also try to give the reader some insight into the benefits of running a dIDS system, from both incident analyst and corporate views.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1532>

#### U.S. CONSIDERS ENCODING DATA ON DRIVER'S LICENSES

The government is taking its first steps with the states to develop driver's licenses that can electronically store information - such as fingerprints - for the 184 million Americans who carry the cards. Privacy experts fear the effort may lead to de facto national identification cards that would allow authorities to track citizens electronically, circumventing the intense debate over federal ID cards.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.usatoday.com/life/cyber/tech/2002/01/07/drivers-licenses.htm>

#### HOMELAND SECURITY IT SPENDING LAGS

Most of the federal money made available after the terrorist attacks is not going to information technology projects, but technology will play a larger

role as agencies determine their homeland security needs during the coming months, industry experts said at the Federal Convention on Emerging Technologies in Las Vegas.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.fcw.com/fcw/articles/2002/0107/web-geia-01-08-02.asp)

[bin/news.cgi?url=http://www.fcw.com/fcw/articles/2002/0107/web-geia-01-08-02.asp](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.fcw.com/fcw/articles/2002/0107/web-geia-01-08-02.asp)

#### USER FRIENDLY SECURITY: OXYMORON OR NOT?

Jakub Marcin writes: "Very strong crypto for email, file sharing, discussion boards, etc. (works with Linux) -- 256 bit symmetric AES and 4096 asymmetric crypto among other goodies! Encryption for the nuts and insane or the real world? If you skip the blue and take the red pill, this is for you!!

Link: <http://www.newsforge.com/article.pl?sid=02/01/09/1345223&mode=nocomment>

#### SILICONVALLEY.COM E-MAILS VIRUS TO READERS

According to Cynthia Funnell, director of corporate communications for Knight Ridder Digital, which operates the site, a message containing an attachment infected with a variant of the data-destroying Magistr e-mail worm was sent to subscribers to "Good Morning Silicon Valley," an e-mail version of a daily news roundup.

Link: <http://www.newsbytes.com/news/02/173521.html>

#### VENDORS EYE VOIP SECURITY

According to a recent study by The Yankee Group research firm, network vendors will release a flurry of Voice over IP security products in 2002, sparking IP telephony adoption by easing fears of malicious intrusions or DoS.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/02/01/09/020109hngoipse.x)

[bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/02/01/09/020109hngoipse.xml](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/02/01/09/020109hngoipse.xml)

#### DEBATE CONTINUES OVER SECURITY OF WINDOWS XP

Differences of opinion continue to swirl over a potentially problematic Universal Plug and Play service in Microsoft Corp.'s Windows XP operating system.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2002/TECH/ptech/01/09/xp.security.idg/index.html)

[bin/news.cgi?url=http://www.cnn.com/2002/TECH/ptech/01/09/xp.security.idg/index.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2002/TECH/ptech/01/09/xp.security.idg/index.html)

#### "KONCEPTOR" PLEADS GUILTY

Benjamin Troy Breuninger aka Konceptor pleaded guilty to a single count of unauthorised access and causing damage to a protected computer network at Lawrence Livermore National Laboratory in California, which conducts US nuclear weapons research.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.com.au/technology_story/0,6257,3566338%255E15319,00.htm)

[bin/news.cgi?url=http://news.com.au/technology\\_story/0,6257,3566338%255E15319,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.com.au/technology_story/0,6257,3566338%255E15319,00.html)

#### NAPSTER LAUNCHES A TEST OF NEW SECURE SERVICE

Napster launched a test version of its new service which prevents the unauthorized sharing of copyrighted files - a feature which made the original service popular among users but hated by the recording

industry which sued it for copyright infringement.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.forbes.com/technology/newmedia/newswire/2002/01/10/rtr475847.html>

#### SOCIAL ENGINEERING FUNDAMENTALS, PART II

This is the second part of a two-part series devoted to social engineering. This article will examine some ways that individuals and organizations can protect themselves against potentially costly social engineering attacks. I refer to these practices as combat strategies.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1533>

#### WRITING INFORMATION SECURITY POLICIES

In many ways, an information security policy is like dietary fiber: we all agree that it is necessary and beneficial, but only a handful of people take action to obtain it.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://unixreview.com/documents/uni1010616481936>

#### TECH ATTACKS ARE BIG CHALLENGE TO SMALL FIRMS

Companies of all sizes must guard against data thieves and vandals. But the job is tougher for small ventures because most cannot afford full time tech wizards.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.usatoday.com/life/cyber/tech/2002/01/09/tech-attacks-challenge.htm>

#### VIRUS WRITERS TAKE AIM AT .NET

Virus writers have apparently made the early developer list for Microsoft's .Net initiative. Known as W32.Donut, the virus does little but infect other .Net files, but it shows that the programmers who create such code are looking ahead, said Motoaki Yamamura, a virus researcher with Symantec.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5101515,00.html>

#### KNOW YOUR ENEMY

What's the first thing most companies do when they get hacked? Probably nothing, because most of them won't realise it's happened. The serious attacks to which we refer are those insidious intrusions that reach deep into your system, bypassing your expensive firewalls and stealing or damaging your data slowly, over long periods of time.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.transceiver.co.uk/txt/kye.html>

#### HACKING ACTIVITY PLUMMETS

Security breaches and hacking attacks have diminished in numbers since the September 11 terrorist attacks, according to data from the Federal Computer Incident Response Center.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/23628.html>

#### NORWAY CRACKS DOWN ON DVD HACKER

Jon Johansen, 18, has been indicted for allegedly bypassing DVD anti-copying technology.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,49638,00.html>

#### FIREWALL SPEEDS J.CREW E-TRANSACTIONS

A great transaction performance achieved by the J.Crew was partly thanks to a new firewall system deployed prior to the start of the holiday rush. Based on J.Crew's experience, Digex announced that it will make the firewall system (which is built around technology from Nokia and Check Point Software) available as a service to other corporate users.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2002/TECH/industry/01/10/web.transaction.speed.idg/index.html>

#### NETWORK SECURITY THE NUMBER ONE CONCERN

Network security, Windows 2000 migration and disaster recovery are the top concerns for 2002, according to over 5,000 IT administrators that responded to the survey carried out by Sunbelt Software.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computing.vnunet.com/News/1128189>

#### 'TROJAN' COMPANY CHANGES HORSES

Antivirus companies say software from Internet lottery maker NetupProfits wasn't really a Trojan after all. But hacker attacks prompt the company to stop tracking user movements online.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,49561,00.html>

#### AIT TAKES SECURITY TO EXTREMES

Web-hosting company Advanced Internet Technologies has razor wire fences, painted black windows in some areas, and even a munitions closet with 12-gauge shotguns and 9-millimeter Beretta pistols. Its data centers are protected by 8-inch reinforced concrete and 24 hour guards. And those precautions were taken before the Sept. 11 terrorist attacks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-8436310.html>

#### SOFTWARE FIREWALL VENDORS UNDER SALES PRESSURE

The European firewall market is expanding strongly but in transition as sales of appliances eclipse those of software for the first time. That's the finding of market analyst firm Frost & Sullivan which estimates that software will, by 2005, account for 38.3 per cent of the total European firewall market of \$1.25 billion.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/23645.html>

VBS/RTF-SENECS INFO

VBS/RTF-Senecs arrives in an email message with the message subject "Scene from last weekend" The message body contains the text "Please do not forward". Just to note that the attachment filename is scenes.zip. Link: <http://www.net-security.org/text/viruses/1010761349,63900,medium.shtml>

MICROSOFT FAILING SECURITY TEST?

Microsoft's security initiatives and the release of the company's "most secure operating system yet" haven't quashed myriad holes that security experts say put customers in harm's way. Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5101593,00.html>

SECURITY AUDITING INDUSTRY SET TO GROW

The network security insurance auditing industry is set for major growth as companies are asked to prove that they are secure against hackers and viruses. Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1128237>

-----  
=====  
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>

-----  
TRUSTIX SECURE LINUX SECURITY ADVISORY - MUTT UPDATE  
Mutt in version 1.2.5i has a buffer overflow which can be remotely exploited. Link: <http://www.net-security.org/text/bugs/1010499861,66251,.shtml>

SGI ADVISORY - NQE CONTAINS VULNERABILITIES  
CRAY's NQS Network Queuing System contains multiple format string vulnerabilities. In the past, SGI has sold a version of NQS called "NQE - Network Queuing Environment", and through investigations has determined that NQE has vulnerabilities. Link: <http://www.net-security.org/text/bugs/1010500049,3608,.shtml>

#### RED HAT LINUX - MUTT UPDATE

An overflow exists in mutt's RFC822 address parser. A remote attacker could send a carefully crafted email message which when read by mutt would be able to overwrite arbitrary bytes in memory. The updated mutt-1.2.5.1 release fixes the problem. Thanks go to Joost Pol for discovering the bug and the Mutt team for the fixed release.

Link: <http://www.net-security.org/text/bugs/1010500191,86663,.shtml>

#### RED HAT LINUX - STUNNEL UPDATE

Updated stunnel packages are now available for Red Hat Linux 7.2. These updates close a format-string vulnerability which is present in some earlier versions of stunnel.

Link: <http://www.net-security.org/text/bugs/1010500273,23971,.shtml>

#### ICQ REMOTE BUFFER OVERFLOW VULNERABILITY

This is very similar to the AIM overflow recently discovered. ICQ protocol uses the same TLV (2711) packet and there is a similar weakness in the parsing of the packet.

Link: <http://www.net-security.org/text/bugs/1010500333,45987,.shtml>

#### VULNERABILITIES IN ORACLE9IAS WEB CACHE

This advisory describes multiple vulnerabilities in Oracle9iAS Web Cache that allow an attacker with local access to overwrite any files accessible to "oracle" user, gain "oracle" user privileges and capture the password of the Web Cache admin account.

Link: <http://www.net-security.org/text/bugs/1010500382,94354,.shtml>

#### AFTPD CORE DUMP VULNERABILITY

The vulnerability is the following: when any user (including an anonymous one) executes the following command on the ftp server: cd ~ (yes it's that simple) aftpdump dumps core in the current directory. The aftpdump.core file can be downloaded but wouldn't contain a lot of valuable information. But, if a user would try to login first with another username and the wrong password, the daemon reads the entire passwordfile into it's memory. When a user afterwards logs in with anonymous the cd ~ trick can be used to dump the core with the encrypted passwords in it. These can be cracked with your favourite password cracker.

Link: <http://www.net-security.org/text/bugs/1010500513,70443,.shtml>

#### FAQMANAGER.CGI FILE READ VULNERABILITY

: Faqmanager can be used to read files on the server the httpd has access to. Example: faqmanager.cgi?toc=/etc/passwd%00 will show the system's /etc/passwd file. Exploitation with Windows systems wasn't tested.

Link: <http://www.net-security.org/text/bugs/1010500652,89702,.shtml>

#### CITIBANK'S C2IT.COM CROSS SITE SCRIPTING BUGS

CitiBank's online cash site, C2IT.com, has substantial vulnerabilities to Cross Site Scripting. The site is similar to PayPal in that it lets users attach Bank and Credit Card account to this online system. Users can then "send" cash to any user via their email address.

Link: <http://www.net-security.org/text/bugs/1010500748,86089,.shtml>

#### RED HAT LINUX - UPDATED EXIM PACKAGES

Updated exim packages are available, which fix a problem when handling certain types of addresses with some configurations. The default configuration does not exhibit this problem.

Link: <http://www.net-security.org/text/bugs/1010599179,84107,.shtml>

#### BEA WEBLOGIC DOS-DEVICE DENIAL OF SERVICE

A flaw in the way the Bea Weblogic server handles specific requests containing DOS-devices can cause a Denial of Service situation, where web requests are no longer being serviced.

Link: <http://www.net-security.org/text/bugs/1010599490,13222,.shtml>

#### MULTIPLE VULNERABILITIES IN CISCO SN 5420 ROUTERS

Three vulnerabilities have been discovered in Cisco SN 5420 Storage Router software releases up to and including 1.1(5). Two of the vulnerabilities can cause a Denial-of-Service attack. The other allows an access to the SN 5420 configuration if it has been previously saved on the router.

Link: <http://www.net-security.org/text/bugs/1010674617,39040,.shtml>

#### LINUX INTRUSION DETECTION SYSTEM VULNERABILITY

The use of LD\_PRELOAD can make a program with privileges given by LIDS execute attackers code. This mean that a root intruder can get every capability or fs access you configured LIDS to grant. Moreover, if you granted CAP\_SYS\_RAWIO or CAP\_SYS\_MODULE to a program, an attacker could deactivate LIDS and thus, access any file. In some configurations, this also lead to users being able to become root. (there must be a program granted CAP\_SETUID which is not setuid)

Link: <http://www.net-security.org/text/bugs/1010674784,32458,.shtml>

#### ALLAIRE FORUMS VULNERABILITY

There is a vulnerability in Allaire Forums, a popular web-board service. Through this vulnerability, it is possible to impersonate other users.

Link: <http://www.net-security.org/text/bugs/1010674937,29898,.shtml>

#### MIRAMAIL 1.04 CAN GIVE POP ACCOUNT ACCESS

The problem in MiraMail lies in the way it stores its variables: Everything is stored in an ".ini" file in plain text. This includes POP account usernames and passwords. This is not limited to the POP accounts either. The user accounts and groups are also stored in the same file, all in plain text. Any user with access to the directory in which MiraMail is installed can potentially "snoop" the file for accounts and passwords, or could add additional users or groups with ease.

Link: <http://www.net-security.org/text/bugs/1010675101,260,.shtml>

#### ESERV 2.97 PROTECTED FILE READ ACCESS VULNERABILITY

The vulnerability allows you to view any password protected files and folders on the webserver.

Link: <http://www.net-security.org/text/bugs/1010675249,65682,.shtml>

-----

Security world  
-----

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

-----  
SNIFF'EM CAPTURES AND MONITORS NETWORK TRAFFIC

After 15 months of development, Y.A.S.C (Yet Another Software Company) has released the gold master CD of Sniff'em. Sniff'em is a competitively priced, high performance Windows packet sniffer that monitors and analyzes network traffic, allows network managers to detect and eliminate bottlenecks and other network related problems, and performs application debugging, fault analysis, network protocol analysis, data stream filtering, network intrusion detection, and usage monitoring. Sniff'em makes it easy to discover why computers on the network can't communicate with each other, or why traffic is backing up on a particular device. Network intrusion can be detected, and logs can be created and saved to preserve an audit trail of all data that moves through the network.

Press release:

< <http://www.net-security.org/text/press/1010499542,63139,.shtml> >

-----  
SURVEY: CONCERNS ABOUT WIRELESS SECURITY

A recent survey of more than 1,200 IT and security professionals found that concerns about wireless security are paralleling the rapid build-out of wireless infrastructure in corporate settings, but the skills set for securing those networks aren't keeping pace. The survey, published in the January 2002 issue of Information Security magazine, an independent media division of TruSecure Corp., is part of a cover story feature on wireless security.

Press release:

< <http://www.net-security.org/text/press/1010499687,7192,.shtml> >

-----  
QUALYS JOINS NEW OPSEC SECURITY ASSESSMENT INITIATIVE

Qualys, Inc., the pioneer of Automated Vulnerability Assessment, announced participation in the Check Point Software Technologies Ltd. OPSEC (Open Platform for Security) Security Assessment Initiative. The newly announced initiative provides a method for certification of tools and services that help validate network security through vulnerability assessment and corrective action.

Press release:

< <http://www.net-security.org/text/press/1010499761,38818,.shtml> >

-----

SOPHOS DISCOVERS FIRST SHOCKWAVE VIRUS

The SWF/LFM-926 virus targets webmasters who use Shockwave to make their websites more attractive with animation and special effects. End users who browse an affected website may become infected if they download and open the Flash file on their computer.

Press release:

< <http://www.net-security.org/text/press/1010516941,53674,.shtml> >

NETWORK-1 CERTIFIED AS NETIQ WEBTRENDS PARTNER

Network-1 Security Solutions, Inc., announced that its CyberwallPLUS family of products completed and passed certification for interoperability with NetIQ's WebTrends Firewall Reporting Solutions. Network-1 is one of the first intrusion prevention solutions for desktops, laptops and servers to be certified under the program. This certification assures users of the compatibility of CyberwallPLUS with the security management tools in WebTrends Firewall Reporting Solutions.

Press release:

< <http://www.net-security.org/text/press/1010598893,56987,.shtml> >

QUALYS ANALYSIS ON REMOTE SHELL TROJAN

Qualys, Inc., a leader in Managed Vulnerability Assessment, announces the detection and analysis of a new and potentially dangerous Remote Shell Trojan, referenced as RST.b, with backdoor and self-replicating functionality. Machines can become infected through binary email attachment or downloaded files. RST.b then installs a backdoor that listens for network traffic coming through any UDP port, making this trojan different and significantly more dangerous than the Remote Shell Trojan identified earlier by Qualys in September 2001. RST.b detection and cleansing tools are available at <https://www.qualys.com/forms/remoteshellb.html>.

Press release:

< <http://www.net-security.org/text/press/1010674253,65243,.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](mailto:staff@net-security.org)

---

## OPSEC SOLUTIONS

In addition to the billable services described in the Enforcement Point section, Check Point's SVN for Managed Service Providers is also integrates at the Application Program Interface (API) level, solutions from over 200 partners. These partners provide solutions for Content Security, Authentication and Authorization, Intrusion Detection, Event Analysis and Reporting, High Availability, Secured Operation Systems, Directory Services, and PKI Products and Services. Click here for an overview.

Read more:

< <http://www.security-db.com/product.php?id=428> >

This is a product of Check Point, for more information:

< <http://www.security-db.com/company.php?id=93> >

---

## E:)SCAN

e:)scan works by filtering e-mail on the Internet before it arrives at companies networks. So, companies do not have to invest in hardware and software which requires constant maintenance and upgrading, or invest in security expertise. Instead we do that for you e:)scan services are located on the backbone of the Internet at key points around the world, both in Europe and North America.

Read more:

< <http://www.security-db.com/product.php?id=1180> >

This is a product of Activis, for more information:

< <http://www.security-db.com/company.php?id=279> >

---

## XM1200

The XM1200 is a standard PCI card equipped with dual cryptographic processors, each containing ARM7TDMI processors. Not simply fixed function processors, they contain general purpose CPUs capable of running programs. This allows OEM customers to tailor the XM1200 to their needs. The appliance can be reprogrammed to accelerate a virtual private networking (VPN) infrastructure, public key infrastructure, CPU intensive tasks such as volume transaction processing and a wide range of other application opportunities.

Read more:

< <http://www.security-db.com/product.php?id=885> >

This is a product of Cryptographic Appliances, for more information:

< <http://www.security-db.com/company.php?id=216> >

---

## Security Software

---

All programs are located at:

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

---

### DELTACRYPT 1.12R

Deltacrypt (DTI) offers easy to use public key encryption for data and puts the power of 6144-bit encryption in the hand of the everyday person. Powerful? Yes. Heavy? No: About 400KB total.

Info/Download:

< <http://www.net-security.org/various/software/1010589320,64073,windows.shtml> >

---

### FOLDER LOCK 4.0

Folder Lock is a fast file security software which can password protect your personal files and folders within 2 seconds even if GBs of data is in the Locker. It is very useful to keep your sensitive files away from peeping eyes. It is unlike other encrypting tools that take a lot of time to super encrypt a file. It is fast, provides easy accessibility, one click locking convenience and is very easy to use. It does not load any file at startup like other encrypting tools making it, one of its kind.

Info/Download:

< <http://www.net-security.org/various/software/1010669529,64896,windows.shtml> >

---

### NET-ALYZER 3.0

Net-alyzer is a sophisticated management tool that analyzes and integrates information on both Email and Internet activity. net-alyzer provides the information with which organizations can decide what is excessive or inappropriate Internet use, giving them an opportunity to establish acceptable boundaries of Internet activity. It is not a restricting tool that blocks web sites indiscriminately. It is a tool that encourages productive use of Email and the Internet. With net-alyzer in place, a company and its employees can safely benefit from the huge business advantages that the Internet offers.

Info/Download:

< <http://www.net-security.org/various/software/1010588966,92787,windows.shtml> >

---

### ET 3.3

ET is the phone home device which will, in the event of your computer being stolen, phone your telephone number every time your computer is switched on and at a preset time every day. When you take the call you simply dial 1471 (in the UK - Check with your local telecom company) and be told the number from which your computer phoned you. This will lead the police straight to your computer, meaning the recovery of your equipment. ET does not require a subscription to any monitoring service.

Info/Download:

< <http://www.net-security.org/various/software/1010588872,2928,windows.shtml> >

---

Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)

<http://net-security.org>

<http://security-db.com>