

HNS Newsletter  
Issue 68 - 25.06.2001  
<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>

Current subscriber count to this digest: 2598

Table of contents:

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

=====  
Secure Exchange 2000 against email attacks/viruses!  
=====

LANguard SELM is a network wide event log monitor that retrieves logs from all NT/2000 servers and workstations and immediately alerts the administrator of possible intrusions. Through network wide reporting, you can identify machines being targeted as well as local users trying to hack internal company information. LANguard analyses the system event logs, therefore is not impaired by switches, IP traffic encryption or high-speed data transfer.

Download your evaluation copy from:  
<http://www.net-security.org/cgi-bin/ads/ads.pl?banner=gfitxt>  
=====

General security news  
-----

-----  
**NSA SECURES WIN-2K**

Your tax dollars have been put to good use for a change, as the US NSA has been busy figuring out how to make Windows 2000 more secure, and has released a set of templates and instructions to enable anyone to batten down their '2K hatches. The package had been available briefly at NSA's Web site, but has temporarily been taken down due to overwhelming demand. The files will be available again from NSA within a week's time.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/19761.html>

#### SECURITY TIPS: APPLYING IIS 5 PATCHES

While we try to keep most of the security tips in this column as general as possible, this week's is very specific and addresses a critical vulnerability in Microsoft's Internet Information Server 5 which was recently discovered.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/Features/1123261>

#### CARNIVORE 'NO PROBLEM' FOR NEW E-MAIL ENCRYPTION

If a new software research project proves successful, Web surfers will be able to send secure e-mail and instant messages that are not only automatically encrypted, but are further hidden from prying eyes by a stream of fake data. A research team led by Nikola Bobic, a part-time professor at Ottawa University, aims to create a virtual network on the Internet called "Cryptobox", which would be similar to peer-to-peer systems like Gnutella.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.osopinion.com/perl/story/11281.html>

#### COMPUTER VIRUSES EASIER TO WRITE, HARDER TO FIGHT

As automated programs have made computer hacking and the creation of malicious code easier, more security administrators are scanning for the software tools used to create viruses and attack networks. And while companies and universities are looking to secure their own systems, they are also concerned with the liability that comes with malicious code that was created on their systems being used against other systems.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsfactor.com/perl/story/11333.html>

#### HACKER TOOLS AND THEIR SIGNATURES, PART TWO

This is the second installment in the Hacker Tools and Their Signatures series, a series written to assist system administrators, security administrators, and the security community as a whole to identify and understand the tools that are being used in the hacker community. The first article examined This installment will focus on two tools: Juno and Unisploit. This paper will provide a detailed analysis of these tools, including tcpdump examples and other useful references.

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

#### DDOS ATTACKERS RAISING THE BAR

Distributed denial-of-service attacks - which by some estimates total more than 4,000 a week - are likely to get much worse as the perpetrators hone their skills and new weaknesses in popular platforms are discovered and exploited. As vendors such as Asta Networks Inc. and Mazu Networks Inc. prepare to launch their anti-DDoS solutions in the coming weeks, attackers across the Internet are fine-tuning their tools and creating sophisticated assaults designed to elude even the best defenses.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0%2C11011%2C2775881%2C00.html>

#### LAWYERS RAISE FEARS OVER ALTAVISTA'S SEARCH ENGINE

Lawyers have warned that companies using AltaVista's new search engine

technology are at risk of breaching data protection laws. Launched last week, AltaVista's new software lets people search entire corporate networks allowing employees to access all network folders, personal computers and emails. Lawyers are warning that the search facility could be too intrusive. Unless these are protected in some way, it could allow others to pry into personal records and emails.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/19773.html>

#### BEST PRACTICES AND GOOD ENGINEERING LEADS TO SECURITY

Security has always been a dynamic task, not something you do once and let run forever. The changes in our networked environment, and the increasingly global nature of business and government dictates that you need to be on top of security every second of the day. New vulnerabilities and new attack methodologies are created and distributed as sets of exploit code thru the internet. Underground cells of crackers then take these cookie cutter solutions and use it to further their peer reverence and sometimes to further a political cause.

Link: <http://www.alphaque.com/article.php?sid=21>

#### SOCIAL WORKER ADVISES DETENTION FOR MAFIABOY

Hanny Chung, a court-appointed social worker, told a sentencing hearing that his lack of remorse meant a "moderate risk" existed he would do it again. "Not only is he not taking full responsibility for what he did, he's still trying to justify that what he did was right," Chung told Judge Gilles Ouellet. Mafiaboy, who can't be identified under Canadian law because of his age, pleaded guilty in January to 58 charges related to the attacks and security breaches of sites in Canada, the United States, Denmark and South Korea.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.salon.com/tech/wire/2001/06/19/hacker/index.html>

#### (UN)AUTHORIZED ACCESS

"Continuing with our theme of legality online this week, I'll be going over (un)authorized access. Specifically, I will be looking at the issue of accessing online resources, attempted access, and what people providing restricted services should be aware of."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010620.html>

#### KEEPING SECRETS

This is an interview with Michael Jacobs, information assurance director at the NSA. "The security side of the development cycle was risk-averse. Now, we've got a risk-complex environment [because] we don't have the luxury of time. For example, firewalls upgrade every 18 months. So we have to be more agile in our approach to dealing with security problems. This has shifted the burden of security from the developer - us - to the customer."

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/story/0,1199,NAV47\\_STO61396,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/story/0,1199,NAV47_STO61396,00.html)

#### ULTIMATE IN INTERNET SECURITY OR ANTI-HACKER HYPE?

A security firm headed by a former KGB agent has come under fire for claims

its forthcoming products provide the ultimate solution to computer security problems. Invicta Networks, is developing security products that attempt to foil cracking attacks by using constantly changing IP addresses, which it claims "has the ability to cloak entire computer networks with a shield that makes them invisible and impossible to hack". According to Invicta, this means its hardware system protects against both external and internal hackers as well as denial of service attacks and computer viruses.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/19814.html>

#### ONLINE SHOPS EXPOSE CUSTOMER ORDER DATA

Several small online shops are exposing their customer order data, including credit card numbers, because of improperly installed online shopping cart software. Hundreds of unencrypted customer records were viewable Tuesday by anyone with a Web browser at a candle-making supply store, a computer seller, a music shop and a photographer's gallery, Newsbytes has confirmed. The exposed sites are all running a free online shopping cart program called DCShop, from Boston-based DC Business Solutions.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167000.html>

#### KNOW THY ENEMY

Open ports and any unsolicited attempts by your computer to contact the Net should always be a cause for concern. Unfortunately, most of us never really know what our computers are doing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/anchordesk/stories/story/0,10738,2777057,00.html>

#### SECURE ONLINE BEHAVIOR, PART TWO

This is the second article in a series devoted to introducing readers to secure online behaviors. In the first article, we saw how users have come to rely on the Internet for exchanging business and personal information, and looked at some of the security risks that this might pose. This article will discuss secure e-mail behavior by looking at the various threats posed by using e-mail, as well as some secure habits that users should take to minimize those risks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/basics/articles/sechabits2.html>

#### NETWORK NEGLIGENCE CREATES SECURITY RISK

Rob Enderle, research fellow at Giga Information Group, said that maintenance on user accounts has become an important networking issue. He warned that negligence in closing accounts after a user left the company could subject corporate networks to the mercy of disgruntled ex-employees, temps or contractors. He argued that organisations usually deploy multiple software applications, with separate accounts to set-up. After creation, each login needs maintenance and closure when users leave the company. But the complexity of account maintenance process was prone to create 'orphan accounts', which remained open even though users had left.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1123341>

#### PERFORMANCE CO-PILOT FIXED PACKAGES

Performance Co-Pilot (version 2.2.1-3) is now available. This version contains fixes for the recent security issues uncovered against the earlier 2.2.0-18 release. New source and binary RPMs are available from SGI.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://oss.sgi.com/projects/pcp/download>

#### ECHELON PANEL CALLS IT A DAY

The defining accomplishment of the European Parliament's temporary committee on Echelon may be that it is due to close up shop right on schedule, less than a year after it began its work. Many will remember the committee for backing off from accusing the United States of using the alleged satellite-based surveillance system for industrial espionage, as many of the committee's 36 members clearly believe it did.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,44721,00.html>

#### PHREAKERS HIT GEORGIA COMPANY

They used a Covington company's toll-free line to run up \$89,911.80 in overseas calls. Now, it's a question of who pays the bill. Officials of the Covington company, Gerri Murphy Realty, say they bear no blame for the calls to Pakistan, India, Bangladesh and other spots outside metro Atlanta. Finding that the phone line was misused was unpleasant. Finding that the company is supposed to pay sent the trio who owns and runs Murphy Realty scrambling for lawyer Robert Stansfield.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.thedigest.com/more/129/129-135.html>

#### FULL DISCLOSURE STUDY RESULTS

The goal of this distinction project was to determine the attitudes about disclosure practices in the computer security community regarding issues surrounding full disclosure. Two hypotheses were tested. First, a majority of those in the computer security field support the full disclosure model of disseminating vulnerability information and second, attitudes on the full disclosure debate will vary across participation in different computer security circles. In order to test these hypotheses, opinions from users of full disclosure information and computer security practitioners were solicited using an on-line survey.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://fisher.osu.edu/people/goens\\_1/results.htm](http://www.net-security.org/cgi-bin/news.cgi?url=http://fisher.osu.edu/people/goens_1/results.htm)

#### CALIFORNIA INDICTMENT IN RUSSIAN HACKS

A Russian computer programmer imprisoned in the U.S. on charges that he perpetrated a cyber crime spree of extortion and credit card fraud was indicted in California - adding the Golden State to a growing list of destinations on the accused hacker's whirlwind tour of U.S. detention centers. Alexey V. Ivanov, 20, was slammed with fifteen counts of computer fraud and extortion for the Southern California portion of a string of financially-motivated attacks on e-commerce companies and small financial institutions, aimed at stealing credit card numbers and consumer information, and strong-arming companies into paying protection money.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/219>

### CIA CAN'T COMPETE WITH HACKERS

The CIA cannot predict computer attacks on U.S. systems before they happen, as the agency is expected to do with political and military events, a top CIA official told Congress on Thursday. Despite a major increase in intelligence efforts dedicated to computer security, attackers still develop new tools and techniques faster than the CIA can keep up, Lawrence K. Gershwin said. Often, "we end up detecting it after it's happened," said Gershwin, the CIA's top adviser on science and technology issues. "I don't feel very good about our ability to anticipate."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://cbsnews.com/now/story/0,1597,297811-412,00.shtml>

### INTRODUCTION TO IPv6

This article discusses features of IPv6: bigger address space, support for mobile devices, and built-in security. It also shows some of the changes from IPv4 to IPv6.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.onlamp.com/pub/a/onlamp/2001/05/24/ipv6\\_tutorial.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.onlamp.com/pub/a/onlamp/2001/05/24/ipv6_tutorial.html)

### GIBSON POSTS LIST OF ATTACK SITES

After weathering seven denial of service attacks in a little over one month, Steve Gibson has decided to name names. He has successfully logged the addresses of 195 machines that were used by the attackers to flood GRC.com with data. In a move designed both to prod the operators into patching their systems, and to cut the legs out from under his attackers, Gibson has posted a list of the machines at his site.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/167145.html>

### WEB SECURITY LAPSE PUTS WHICH? IN DOCK

Naming and shaming is all in a day's work for the Consumers' Association, but Friday it had to name and shame itself. It had to warn more than 2,700 people who had bought Which? TaxCalc software from its website that their financial details had been available on the internet and could have fallen in to the wrong hands. The program helps with self-assessment tax forms. The association has advised the customers to cancel the cards used, to head off fraud.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.guardianunlimited.co.uk/internetnews/story/0,7369,511452,00.html>

### E-COMMERCE FEARS? GOOD REASONS

The little lock icon that appears in your Web browser's window is supposed to prove you are engaging in a safe transaction. But it may be nothing more than a visual placebo. The icon is intended to indicate that information is being encrypted as it moves from your computer to the e-commerce site's computer. But complete and uncrackable encryption of outgoing and incoming information may not always take place every time the lock appears on your computer's screen. And safe arrival at the site's servers doesn't guarantee your information is safe forever. Experts say that once the data arrives at the e-commerce site, it's often stored decrypted on the site's servers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/ebiz/0,1272,44690,00.html>

#### STARTUPS AIM TO PREVENT DoS ATTACKS

With more than \$100m in venture funding, four startups aim to combat DoS network attacks, which by some estimates total more than 4000 a week. Arbor Networks, Asta Networks, Lancop Technologies and Mazu Networks are attempting to automate the response to DoS attacks which still require the co-operation of the major internet service providers as most DoS attacks cannot be traced.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://webserv.vnunet.com/News/1123388>

---

#### Security issues

---

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

---

#### REMOTE BUFFER OVERFLOW IN MICROSOFT IIS

There exists a remote buffer overflow vulnerability in all versions of Microsoft Internet Information Services (IIS) Web server software. The vulnerability lies within the code that allows a Web server to interact with Microsoft Indexing Service functionality. The vulnerable Indexing Service ISAPI filter is installed by default on all versions of IIS. The problem lies in the fact that the .ida (Indexing Service) ISAPI filter does not perform proper "bounds checking" on user inputted buffers and therefore is susceptible to a buffer overflow attack.

Link: <http://www.net-security.org/text/bugs/992957789,83405,.shtml>

#### MULTIPLE VULNERABILITIES IN AMLSERVER

AMLServer's "Webpaging" http interface is susceptible to a directory traversal attack. Adding the string "../" to a URL allows an attacker access to files outside of the webserver's publishing directory. This allows read access to any file on the server. A second problem is found in the file pUser.Dat. All username/password combinations applicable to the various services provided by AMLServer are stored in this file in plaintext. The mentioned userfile is stored in the server's main directory. The exact location can be obtained exploiting another problem in the web interface, a path disclosure bug. The http-header field 'Location' contains the full path to servermaindir/Messages.

Link: <http://www.net-security.org/text/bugs/992958480,13379,.shtml>

#### SECURITY VULNERABILITY IN CISCO TFTP SERVER 1.1

TFTP is vulnerable to some kind of primitive directory transversal attack which allows a remote user to obtain any file from the target system.

Link: <http://www.net-security.org/text/bugs/992958565,61005,.shtml>

#### DCSHOP SECURITY VULNERABILITY

The issue does not show up on properly configured servers, i.e. where the "Everyone"-group has "Full Access" to the CGI-BIN or sub-folders.

Link: <http://www.net-security.org/text/bugs/992958636,8903,.shtml>

#### CONECTIVA LINUX SECURITY ANNOUNCEMENT - FETCHMAIL

Fetchmail would segfault when receiving emails with large "To:" headers. This was due to a buffer overflow in the header parser and it could be exploited remotely.

Link: <http://www.net-security.org/text/bugs/993038284,68116,.shtml>

#### SURGEFTP VULNERABILITIES

- 1.) A simple directory transversal bug allows listing of normally unaccessible files
- 2.) FTP allows anybody to DOS the machine with a well known con/con attack.

Link: <http://www.net-security.org/text/bugs/993038307,52537,.shtml>

#### MANDRAKE LINUX SECURITY - KDELIBS UPDATE

A problem exists with the kdesu component of kdelibs. It created a world readable temporary file to exchange authentication information and delete it shortly after. This can be abused by a local user to gain access to the X server and could result in a compromise of the account that kdesu would access.

Link: <http://www.net-security.org/text/bugs/993038396,68436,.shtml>

#### RED HAT LINUX LOCALLY EXPLOITABLE FORMAT STRING

A format string vulnerability exists in the batch SMTP processing code, which is triggered by any SMTP response that includes a part of its SMTP command.

Link: <http://www.net-security.org/text/bugs/993125773,14203,.shtml>

#### W3M MALFORMED MIME HEADER BUFFER OVERFLOW

w3m, a text file/Web browser which is similar to lynx, has a buffer overflow vulnerability in a routine to parse MIME header. If a user retrieves/downloads a malformed Web page with w3m, a malicious Web server administrator may gain an escalated privilege from the w3m user, which is run by w3m remotely.

Link: <http://www.net-security.org/text/bugs/993125802,52251,.shtml>

#### CONECTIVA - TWO SECURITY FIXES FOR XINETD

"xinetd" is an alternative to the inetd superserver. zen-parse reported on Bugtraq a remote buffer overflow vulnerability in xinetd that could be used by a remote attacker to execute arbitrary commands on the server with root privileges. Another vulnerability that has been corrected with this release is the umask setting, which previous versions were configuring to zero. With the umask set to zero, applications started by xinetd could inadvertently create world writable files if they did not check this setting before.

Link: <http://www.net-security.org/text/bugs/993125833,6282,.shtml>

#### MULTIPLE VENDOR 802.11B ACCESS POINT SNMP FLAW

ISS X-Force has discovered a serious flaw in the authentication mechanism of the Atmel VNET-B Simple Network Management Protocol (SNMP) implementation. Atmel devices are provided via Original Equipment Manufacturer (OEM) agreements

to Netgear and Linksys. These devices do not implement any SNMP security measures, which may allow an attacker to gain access to or control a wireless LAN (WLAN).

Link: <http://www.net-security.org/text/bugs/993126131,21102,.shtml>

#### EPERL ALLOWS THE USER TO EMBED PERL CODE

ePerl allows the user to embed perl code (specified inside ePerl delimiters) in HTML. ePerl has the ability to "safely" include untrusted files using the #sinclude directive. The untrusted file is not supposed to be able to specify any perl code to run, but this safe mode can easily be circumvented. The #sinclude directive operates by replacing the ePerl delimiters on the untrusted file so that they are ignored during parsing. The problem is that it still follows the preprocessing directives, so the untrusted file can then include another file while not in safe mode.

Link: <http://www.net-security.org/text/bugs/993221840,96404,.shtml>

#### KAV (AVP) FOR SENDMAIL FORMAT STRING BUG

While testing this software by permission of Kaspersky Lab, format string bug was found in syslog() call in avpkeeper /usr/local/share/AVP/avpkeeper/avpkeeper utility, which is launched from sendmail to scan and disinfect messages.

Link: <http://www.net-security.org/text/bugs/993222097,77121,.shtml>

#### CERBERUS FTP SERVER 1.X REMOTE DOS ATTACK

Cartel security team has found a buffer overflow in the Cerberus FTP server, which means that an attacker can execute a denial of service attack against it. This attack will crash the server, without any error. FTP service is then unavailable.

Link: <http://www.net-security.org/text/bugs/993222237,68606,.shtml>

#### A-FTP ANONYMOUS FTP SERVER REMOTE DOS ATTACK VULNERABILITY

Cartel security team has found a buffer overflow in the A-FTP anonymous FTP server, which means that an attacker can execute a denial of service attack against it. Once the big buffer has been sent, the server is vulnerable. Only one more connection is needed to make the FTP service unavailable.

Link: <http://www.net-security.org/text/bugs/993222306,99442,.shtml>

-----

Security world  
-----

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

-----  
BASTILLE LINUX RELEASES VERSION 1.2 - [18.06.2001]

The Bastille Linux development team today announced the release of Bastille Linux 1.2, a hardening script for multiple Linux distributions. With this release, Bastille Linux delivers on the full promise of simplified, automated security administration for Linux systems.

Press release:

< <http://www.net-security.org/text/press/992862006,86386,.shtml> >

-----  
MANAGED SECURITY SERVICES PORTAL BY LURHQ - [18.06.2001]

LURHQ Corporation announced the release of the Managed Security Services Portal, a technology that allows the customer to co-manage and monitor their information security infrastructure. The Managed Security Services Portal provides a consolidated interface to LURHQ's Managed Firewall, Intrusion Detection, Anti-virus, and SherlockESM (enterprise security monitoring) customers.

Press release:

< <http://www.net-security.org/text/press/992862138,82967,.shtml> >

-----  
NAI EXPANDS GAUNTLET FIREWALL 6.0 - [18.06.2001]

PGP Security, a division of Network Associates, announced that it has expanded Gauntlet Firewall 6.0 and virtual private networking (VPN) software support to include the 64-bit Solaris 8 Operating Environment (Solaris OE) from Sun Microsystems. This makes PGP Security, with its Gauntlet 6.0 product, one of the first major firewall application providers to fully support the Solaris OE on all of Sun's hardware platforms, including the recently introduced Netra T1 and X1 thin servers and the UltraSPARC(TM) III based servers.

Press release:

< <http://www.net-security.org/text/press/992862401,65792,.shtml> >

-----

SECUREINFO CORP. EXPANDS SECURETRAINING INSTITUTE - [18.06.2001]

SecureInfo Corporation has expanded its business operations to include the newly formed SecureTraining Institute which has added an additional 3000 feet of classroom space and new offices to SecureInfo Corp.'s current location in the Koger Center.

Press release:

< <http://www.net-security.org/text/press/992862692,65353,.shtml> >

-----

WATCHGUARD ANNOUNCED LIVESECURITY SERVICE GOLD - [18.06.2001]

WatchGuard Technologies, Inc., a leader in Internet security solutions, announced LiveSecurity Service Gold, a premium support package that helps administrators quickly and easily deploy large scale, multi-site Virtual Private Networks. LiveSecurity reduces the complexity of managing Internet security by integrating customer support with value-added customer care services that help administrators safeguard their network against evolving threats.

Press release:

< <http://www.net-security.org/text/press/992862901,82296,.shtml> >

-----

SURFCONTROL'S SUPERSCOUT GETS 5 STAR FROM SC MAG - [19.06.2001]

SurfControl, The Internet Filtering Company, announced today that SC Magazine has awarded its SuperScout Web Filter an overall rating of five stars in its June Market Survey of various security related hardware and software products. SuperScout Web Filter, a software solution that enhances employee productivity, optimizes bandwidth and reduces legal liability, earned the highest five star ranking for its features, performance and ease of use among others.

Press release:

< <http://www.net-security.org/text/press/992958804,3720,.shtml> >

-----

ICSA LABS ANNOUNCES NIDS CERTIFICATION - [19.06.2001]

TruSecure Corporation, the leader in information security assurance, announced that its ICSA Labs division will offer the industry's first and only continuously deployed testing and certification program for Network Intrusion Detection Systems (NIDS) to test the functionality and compliance of intrusion detection products. The NIDS Certification Program offers an independent and comprehensive process that vigorously tests, assesses and validates the security of intrusion detection systems relied upon by corporations and public entities.

Press release:

< <http://www.net-security.org/text/press/992959084,73052,.shtml> >

---

SECURITY BIOMETRICS ACQUIRES NETFACE LLC - [20.06.2001]

Security Biometrics Inc. announced today that the Company has signed an agreement to acquire 100% of NetFace LLC for 20 million Security Biometrics Inc.'s common shares. NetFace holds the exclusive option to license DSI Datotech, Inc.'s Gesture Recognition Technology specific for video gaming and Internet/Interactive TV markets. Through its exercise of this license, NetFace has the first "right of refusal" on the development of other GRT horizontal markets.

Press release:

< <http://www.net-security.org/text/press/993038646,41062,.shtml> >

---

#### SYGATE SECURE ENTERPRISE 2.0 RELEASED - [20.06.2001]

Sygate Technologies, the leader in securing the remote enterprise, unveiled a new version of its flagship product suite, enabling IT professionals to successfully defend their organizations from a new generation of stealthy viruses. These emerging corporate security threats have the power to fool traditional defenses by changing the way they look several times a day, or masquerading as known computer programs. They prey on the unprotected machines of remote workers and mobile professionals to gain access to corporate data centers via existing VPN and wireless communications, giving hackers unrestricted access to valuable databases and files.

Press release:

< <http://www.net-security.org/text/press/993038820,2135,.shtml> >

---

#### MAX. 6 MONTH TO AUTHOR OF KOURNIKOVA WORM - [21.06.2001]

The suspected author of the infamous Anna Kournikova worm is to face prosecution in the Netherlands. Jan de Wit is suspected of being "OnTheFly", the author of the Kournikova worm. It is alleged that he identified himself as the worm's creator after it infected thousands of computers across the globe in February. De Wit is due to appear in court on September 12th charged with spreading information via a computer network with the intention of causing damage. According to Dutch authorities the maximum sentence he could receive is either 6 months imprisonment or a fine of 100,000 guilders, equivalent to over £27,000.

Press release:

< <http://www.net-security.org/text/press/993122455,25589,.shtml> >

---

#### 11TH ANNUAL VIRUS BULLETIN CONFERENCE IN PRAGUE - [21.06.2001]

Virus Bulletin today announces that the 11th annual Virus Bulletin international conference and exhibition will be held at the Hilton, Prague on Thursday 27th and Friday 28th September 2001. VB2001 is the only event to focus exclusively on the threat of viruses and includes an exhibition and conference programme.

Press release:

< <http://www.net-security.org/text/press/993126494,65876,.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](mailto:staff@net-security.org)

---

### NET-COMMANDO 2000 LITE

Net-Commando 2000 Lite is a High-grade Hacker Protection/Prevention, Trojan Horse virus Detection/Prevention/Removal, it is a cut-down version of its bigger brother - Net-Commando 2000. It provides uses technology from Net-Commando 2000 to rank itself a Quality Hacker Protection and Trojan Horse virus Detection Systems.

Read more:

< <http://www.security-db.com/product.php?id=599> >

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

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

---

### DIRECTORYSMART

DirectorySmart, is a proven platform for securing Web applications and defining, enforcing and delegating e-business security policies across complex business relationships. By integrating role-based policy management, Web access control and delegated authority into one comprehensive and easy-to-deploy product, DirectorySmart enables companies to bring their e-business initiatives to market quickly and scale to millions of users without incremental costs.

Read more:

< <http://www.security-db.com/product.php?id=765> >

This is a product of OpenNetwork Technologies, for more information:

< <http://www.security-db.com/info.php?id=176> >

---

### BV-CONTROL FOR UNIX

As BindView's premier security solution, bv-Control for UNIX ensures the safety and reliability of UNIX systems. From comprehensive security assessments to routine disk space analysis, bv-Control for UNIX delivers the information necessary to efficiently secure and maintain optimal network service levels. bv-Control's superior reporting capabilities are flexible and easy-to-use, allowing security administrators to quickly pinpoint and close security risks - improving enterprise security and productivity.

Read more:

< <http://www.security-db.com/product.php?id=577> >

This is a product of BindView, for more information:  
< <http://www.security-db.com/info.php?id=29> >

---

Featured article  
-----

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

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

---

ANONYMIZED? SAFE WEB? NOT YET. by Alexander K. Yezhov

Just a couple of words about the JavaScript filtering problems I've discovered recently. You could see my posts to bugraq or some reprinted versions somewhere. I bet almost everyone knows the Anonymizer service. It's a good tool that lets you stay anonymous surfing the web. Moreover, it blocks the JavaScript code placed on the web pages. The problem is that it just comments scripts instead of cutting them out. On the one hand it's good since you can look at the original JavaScript code if you want. On the other hand this commenting has some disadvantages.

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

---

Defaced archives  
-----

[18.06.2001]

Original: <http://www.kenwood.cd/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/18/www.kenwood.cd/>  
OS: Windows

Original: <http://www.hackerwatch.org/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/18/www.hackerwatch.org/>  
OS: Windows

Original: <http://www.parliament.ru/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/18/www.parliament.ru/>  
OS: Windows

[19.06.2001]

Original: <http://www.interface.microsoft.co.za/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/19/www.interface.microsoft.co.za/>

OS: Windows

Original: <http://www.bentleyslondon.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/19/www.bentleyslondon.com/>

OS: Windows

Original: <http://www.governor.state.tx.us/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/19/www.governor.state.tx.us/>

OS: Windows

[20.06.2001]

Original: <http://www.artmuseum.net/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/20/www.artmuseum.net/>

OS: Windows

Original: <http://www2.saude.sp.gov.br/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/20/www2.saude.sp.gov.br/>

OS: Windows

[21.06.2001]

Original: <http://arulk.rte.microsoft.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/21/arulk.rte.microsoft.com/>

OS: Windows

Original: <http://feeds.mobile.msn.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/21/feeds.mobile.msn.com/>

OS: Windows

Original: <http://redsand.rte.microsoft.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/21/redsand.rte.microsoft.com/>

OS: Windows

[22.06.2001]

Original: <http://atwnt368.external.hp.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/22/atwnt368.external.hp.com/>

OS: Windows

Original: <http://service-asc.sel.sony.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/22/service-asc.sel.sony.com/>

OS: Windows

Original: <http://webcfeedback.msn.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/06/22/webcfeedback.msn.com/>

OS: Windows

[23.06.2001]

Original: <http://booksrv2.raleigh.ibm.com/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/23/booksrv2.raleigh.ibm.com/>  
OS: Windows

Original: <http://www.x.org/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/23/www.X.Org/>  
OS: Windows

Original: <http://www.ericsson.co.ma/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/23/www.ericsson.co.ma/>  
OS: Windows

Original: <http://ecs08.external.hp.com/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/23/ecs08.external.hp.com/>  
OS: Windows

Original: <http://www.netbsd.hu/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/23/www.netbsd.hu/>  
OS: Windows

[24.06.2001]

Original: <http://www.fiat.ch/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/24/www.fiat.ch/>  
OS: Windows

Original: <http://www.lancia.ch/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/24/www.lancia.ch/>  
OS: Windows

Original: <http://www.schmidt.de/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/24/www.schmidt.de/>  
OS: Windows

Original: <http://www.police.york.on.ca/>  
Defaced: <http://defaced.alldas.de/mirror/2001/06/24/www.police.york.on.ca/>  
OS: Windows

-----  
=====  
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, summer is just around the corner.  
Get one here: <http://207.21.213.175:8000/ss?click&jinx&3af04db0>  
=====

Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)  
<http://net-security.org>  
<http://security-db.com>