

HNS Newsletter  
Issue 72 - 23.07.2001  
<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: 2649

Table of contents:

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

=====  
LANguard Security Event Log Monitor

=====  
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  
-----

-----

#### CODE RED WORM SPECIAL COVERAGE

In order to make things easier to find, all the information regarding the worm are in this page. Everything from alerts, news items, solutions, etc.  
<http://www.net-security.org/text/articles/coverage/code-red>

#### U.S. GOVERNMENT WANTS A FEW GOOD HACKERS

That was the message that from a seven-member "Meet the Fed" panel, where government officials answered the questions of a roomful of hackers at the Def

Con conference here Saturday. Including members of law enforcement, a congressman and security experts, the panel illuminated the problems the government has in securing systems and appealed to hackers not to make it any harder--both to help the government and to help themselves.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-6571082.html>

#### PORTSENTRY AND SNORT COMPARED

Snort is a fine piece of software, there is certainly no comparison with Port Sentry, it does so much more, and where they do the same thing, Snort does it much better. Without a bit of configuring (especially WRT ignoring DNS server traffic) you might get more information than you want, but the configuration files are organised in such a way that you can comment out an include line to ignore a certain class of exploits.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linux.ie/articles/portsentryandsnortcompared.php>

#### DO YOU NEED A SECURITY ASSESSMENT?

Every day the number of people using the Internet increases, not just in the United States, but all over the world. With so many people online, security risks increase, as does the need for an effective security strategy. There is an increasing amount of activity by people sneaking and peeking, testing to see if they can gain access to your network or systems for various reasons, some just to see how far they can go, others may have malicious intent. Are you willing to take the chance?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sans.org/infosecFAQ/securitybasics/assess.htm>

#### DEF CON KEEPS HACKERS HOOKED

Conference organizers call it the "annual computer underground party for hackers," and Defcon is known as much for its technical content as its beer tinged hijinks. Pranks like smoke bombs in hotel pools, portions of telephone trucks mysteriously appearing in the convention hall, and concrete dumped in toilets have earned Defcon a reputation as a kind of annual hacker bacchanalia. This weekend wasn't that different: an ambulance hauled off one conference-goer who allegedly overdosed on a cocktail of drugs, and witnesses said one hapless attendee had his laptop smashed after displaying an unflattering PhotoShop-edited photo of another hacker who happened to be nearby.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,45248,00.html>

#### INFOSEC IN THE REAL WORLD

At last, Information Security policy, ("InfoSec") is getting more attention and more companies are beginning to take seriously the threat that security breaches may have a serious impact on the well-being - or, indeed, the very existence - of their business. This awareness brings with it increasing pressure on InfoSec professionals - many of whom may have reached their position as "the company security expert" by default or without the benefit of specialised technical knowledge or traditional management training.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/infosec\\_realworld20010716.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/infosec_realworld20010716.html)

### HACKING FOR HUMAN RIGHTS

Human rights activists put out a call to hackers here to help get the word out about their cause--not by having them deface sites, but by creating applications that can help the organizations manage data.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-6575468.html>

### WHICH IS MORE SECURE? - OPEN SOURCE VS. PROPRIETARY

Is open source software more secure than proprietary software? in a word, "yes." However, will using open source software solve your security needs? The answer is a resounding "no." Many people believe security is a functionality of software. But network security is a process, not a checklist on the side of a software box.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/intweek/stories/news/0,4164,2784795-2,00.html>

### BASIC SECURITY MECHANISMS FOR WIRELESS NETWORKS

As wireless applications become more common, security becomes a more important issue. Unfortunately, due to the ease of wireless deployment, and the freshness of the technology, many people do not realize the risks associated with operating wireless technologies. This article will offer a brief overview of the security concerns involved with wireless networks, including: how and why they are vulnerable to compromise, how they can be protected, and some expected future developments.

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

### FLAWS IN WIRELESS SECURITY DETAILED

A cryptologist who discovered several gaping holes in the international standard governing the design of wireless network devices and the encryption algorithm meant to protect those networks last week detailed vulnerabilities that could be leaving corporate systems open to hackers.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0%2C4125%2CNAV47\\_STO62220%2C00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0%2C4125%2CNAV47_STO62220%2C00.html)

### PROFESSIONAL PARANOIA: SECRETS OF SECURITY EXPERTS

First of all, you probably don't want to become a security professional. Sure, it sounds glamorous: You strut in, violate a network a dozen different ways, and show that you know a lot about security. That really isn't a big deal; you can do the same sort of thing just by demonstrating that you're good in any field. All you have to add is the strut.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.onlamp.com/pub/a/onlamp/2001/07/12/prof\\_paranoia.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.onlamp.com/pub/a/onlamp/2001/07/12/prof_paranoia.html)

### HARDENING BSD

sil writes: "Hardening BSD is definitely trickier than hardening a Linux based workstation being that the top 3 distributions of BSD, Net, Open, Free, have done an excellent job of strengthening the systems on their own. Using FreeBSD at home while I write this, I'll try to focus in on it, but in general (and I may get flamed from the OpenBSD advocates or even NetBSD advocates) you could follow suit between the three. (Dare I say it)".

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

#### ATTACKERS STEAL VITAL DATA FROM FORMULA ONE TEAM

Officials at the Benetton Formula One team admitted that its computer systems have been broken into and that valuable data was stolen. Jean-Jacques His, technical director of Renault, claimed that someone penetrated the Benetton systems last year when the team were developing this season's car. This forced the team to discard some of their work, in case a rival team had seen the data that had been removed.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2091380,00.html>

#### MALICIOUS WEB ATTACKS MAY BE NEW IIS WORM

A new Internet worm may be on the loose and could have already infected thousands of sites running Web server software from Microsoft. Since late last week, a malicious program has been scanning the Internet and compromising Microsoft systems running unpatched versions of the IIS. Experts who have reviewed the signature of the code left behind in Web server logs said it appears to exploit a buffer overflow flaw in IIS that was discovered by eEye Digital Security and published last month. In a bulletin released June 18, Microsoft said the flaw could enable an attacker to take complete control of vulnerable IIS systems. The company has released a patch to correct the vulnerability.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168003.html>

#### HACKERS SECURE A DOWNGRADED STORM

Hackers have liberated one of the Internet's most popular security websites from its corporate owners. This time, however, it's perfectly legal. A ragtag group of programmers, system administrators and newly unemployed security consultants said last weekend at the Defcon convention that they purchased the rights to Packet Storm from Securify for just \$1.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/privacy/0,1848,45275,00.html>

#### RUSSIAN MAFIA THREATENS NET

Attackers have launched computer viruses and DoS attacks, but the biggest danger comes from attackers with ties to organized crime breaking into computers, FBI officials said. Spearheading the organized hacking rings is the Russian Mafia, security experts say. The Russian Mafia has infiltrated many businesses in the former Soviet Union, and is becoming increasingly sophisticated in computer crimes. These groups are penetrating computers in the U.S. and other Western countries to obtain illegal profits, said John Collingwood, FBI assistant director for public affairs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2784950,00.html>

#### HALF OF U.S. BROADBAND USERS UNPROTECTED

Why? Because subscribers to "always on" Net connections aren't using any protection - like a firewall or antivirus software - to keep the black hats from gaining access to their PCs. "I think a lot of it is they don't realize there is a

problem, especially more of the novice users," says Jaclynn Bumback, research analyst for In-Stat's enterprise and residential communications group. "They don't realize that even when their browser is not open, they are vulnerable to attacks. Since they don't realize they are vulnerable, they don't pay the money for the software and hardware that can protect them."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/news/article/0,aid,55154,00.asp>

#### EBOOK HACKER ARRESTED BY FBI

Dmitry Sklyarov, a programmer at Russian software company Elcomsoft, who was arrested after giving a talk at Def Con 9 in Las Vegas titled "eBook Security: Theory and Practice." Elcomsoft publishes a program to remove restrictions from encrypted PDF files, which has severely annoyed Adobe Corporation. Adobe was apparently responsible for the arrest, charging that Elcomsoft is violating the Digital Millennium Copyright Act by publishing the software and giving the presentation at Def Con. Just to add the Elcomsoft has about 25 products in their "advanced recovery" series and lot of them are available for downloading trough ZDNet's Download.com.

Link: <http://slashdot.org/article.pl?sid=01/07/17/130226&mode=thread>

#### PROBLEMS WITH SOME IMPLEMENTATIONS OF THE LDAP

Several implementations of the Lightweight Directory Access Protocol (LDAP) protocol contain vulnerabilities that may allow denial-of-service attacks, unauthorized privileged access, or both.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/advisories/CA-2001-18.html>

#### FBI'S GOOFS WITH COMPUTERS

BBC News report that a total of 184 computers are missing from FBI, including 13 that are believed to have been stolen. Three of the missing machines may contain classified information, said officials.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://news.bbc.co.uk/hi/english/world/americas/newsid\\_1444000/1444482.stm](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.bbc.co.uk/hi/english/world/americas/newsid_1444000/1444482.stm)

#### PHONE HACKING: THE NEXT GENERATION

The phone network and the Internet are converging. That's good news for smart telephones, new telephony services, and customer convenience, and bad news for security. If you think that phone hacking is bad now, take a gander at what's coming.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.counterpane.com/criptogram-0107.html#1>

#### NEW CIO STARTING AT NSA

Richard Turner, former chief information officer of the Federal Trade Commission, will report for duty today as the National Security Agency's CIO. Turner has about three decades of experience in information systems and information resources management. In addition to the FTC, Turner also has worked at NASA and for the Army.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.fcw.com/fcw/articles/2001/0716/web-nsa-07-17-01.asp>

### INBOUND SERVICE PROXIES

Outbound service proxies are all the rage. Instead of providing direct access to the Internet most companies, academic and governmental networks utilize proxy servers to mediate that access, cache data and generally make life easier for the users and administrators. Almost all sites use email proxies, the email generated on your workstation is then delivered to a local mail server which in turn handles the sending of it. However on the flip side of the coin very few people use inbound service proxies, instead simply placing the server directly online and letting people access it.

Link: <http://securityportal.com/php/t.php?l=131&s=28>

### PEOPLE AND PASSWORDS

The use of passwords and pin numbers is the most common security "tool" in use today. Other new technologies are being developed, including a host of biometric solutions, smart cards etc., but for the immediate future the humble password will still be the key component in most systems.

Link: <http://www.it-director.com/article.asp?id=2002>

### VENDOR RESPONSE TO NEW VIRUS REPORTS

You've just come across a suspicious file that seems to be causing problems on a machine in your organization. You think it may be a virus, but all of the antivirus programs you use to scan it say the file is clean. What's your logical next step? For many people, the best thing to do is to send the suspicious file to one or more antivirus software developers for analysis. Just what do you think the response from these specialists should be?

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

### THE DEADLY AOL.EXE VIRUS

US comedian Ray Owens has demanded compensation from anti-virus vendor Symantec for publishing his work without copyright. Owens wrote a fake virus warning which advises people to delete the "insidious aol.exe virus" - the executable which boots up the AOL application. The joke, known as AOL.exe hoax, was reported on many anti-virus vendors' sites, many of them included Owens' entire copyrighted material in their descriptions.

Link: <http://www.vmyths.com/rant.cfm?id=347&page=4>

### RSA SECURITY PONDERES SECURITIES SALE

RSA Security, maker of e-business authentication and encryption software, has filed a shelf registration - a pre-application to sell securities - with the Securities and Exchange Commission.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://boston.internet.com/briefs/article/0,1928,2371\\_803061,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://boston.internet.com/briefs/article/0,1928,2371_803061,00.html)

### CRYPTO: A HARD SELL

The recent news of significant layoffs at PKI-vendor Entrust is further evidence of something I once learned the hard way: A viable market for user-level encryption software simply doesn't exist.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/july01/columns\\_curmudgeon.shtm](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/july01/columns_curmudgeon.shtm)

1

#### CODE RED WORM CAN BE KILLED BY REBOOT

A new Internet worm may have already infected more than 20,000 computers running IIS. But security experts have determined a simple way of snuffing out the malicious program: reboot the computer. Since it was first reported Friday, the Code Red Worm has compromised more than 22,000 systems running IIS, according to intrusion statistics compiled by the SANS Institute.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168089.html>

#### WILL CDC PRIVACY APP PEEKABOOTY PUT USERS AT RISK?

"Based on that and several other conversations with networking specialists, we developed the impression that Peekabooty could be a fairly self-destructive tool in the hands of non-technical computer users in repressive countries, which might, ironically, give the very people it's designed to help a dangerously false sense of security."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/20472.html>

#### 'HACK IN A BOX' TOOL EMERGES AT DEF CON

Argentinian security firm Core-SDI created a storm of controversy when it unveiled an 'intelligent' hacking tool which automates system penetration. The as yet unnamed tool, showcased at the Def Con and Black Hat conference in Las Vegas, is capable of scanning the target, mapping networks, finding vulnerabilities and scripting and compiling customised code to exploit those flaws before systematically trying to gain higher levels of access.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1124018>

#### SYMMETRIC CRYPTOGRAPHY IN PERL

Modern ciphers, usually publicly known and widely studied, rely on the secrecy of a key instead. They encrypt the same plaintext differently for each key; to decrypt a ciphertext, you must know the key used to produce it. New keys are easy to generate, so the compromise of a single key is a smaller problem. Although messages encrypted with the stolen key are rendered readable, the algorithm itself can be reused. Algorithms that use the same key for both encryption and decryption are called symmetric ciphers. To use such an algorithm, Alice and Bob must agree on a key to use before they can exchange messages. Since decryption depends only on the knowledge of this key, they must ensure that they share the key by a secure channel that Eve cannot access (Alice could whisper the key into Bob's ear over dinner, for example).

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.perl.com/pub/a/2001/07/10/crypto.html>

#### HACKER ARREST STIRS PROTEST

When the FBI arrested a Russian programmer this week on charges of criminal copyright violations, the government unwittingly ignited a powder keg of outrage. Web pages immediately sprouted to demand the release of Dmitry Sklyarov, who was visiting the United States to describe his work at the Defcon hacker convention in Las Vegas. Newly minted activists set up a mailing list, launched a defense fund, and trashed Adobe Systems for urging the U.S. government to arrest Sklyarov on charges of circumventing its copy protection methods.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,45342,00.html>

#### NEW ZEALAND HACKER CONVICTED IN LANDMARK CASE

A landmark court case in New Zealand has resulted in the conviction of a hacker who in 1998 deleted almost 4,500 Web sites from a server based in the U.S. Andrew Garrett was convicted in the Manukau District Court this week in the first case of its kind in New Zealand.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168118.html>

#### CONTROVERSIAL RESEARCH AT USENIX SECURITY CONFERENCE

The USENIX Association confirmed the inclusion of a controversial research paper to its Security Symposium. The paper reveals inherent security risks with the recording industry's digital music access-control technologies. Dr. Edward Felten, the Princeton University scientist who was a key member of the research team, will also participate in a panel discussion about the paper's recent legal wrangles.

Link: <http://www.newsforge.com/article.pl?sid=01/07/19/1854215&mode=thread>

#### IDS TERMINOLOGY, PART TWO: H - Z

Intrusion Detection Systems are still very much in their infancy, but in terms of development they are growing at an extraordinary rate. The terminology associated with IDS is also growing at rapidly. This is the second article of a two-part series, is intended to introduce readers to some IDS terminology, some of it basic and relatively common, some of it somewhat more obscure.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ids/articles/idsterms2.html>

#### MAJOR ALERT ON CODE RED WORM

Gary Warner contributed: "eEye provided the security community with a very thorough analysis of the Code Red worm. Here is how one security group used this analysis to see what was going on in their customer's networks. We saw enormous activity yesterday EVERY IP on our monitored networks was hit AT LEAST six times, followed by NOTHING in the late night hours. And, oh yes, the White House is aware and safe."

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

#### JUSTICE DEPT. CREATES ANTI-'HACKING' UNITS

U.S. Attorney General John Ashcroft announced the creation of 10 "specialized prosecutorial units" designed help the federal government further crack down on Internet crime. Located in nine U.S. Cities (with two in New York) the Computer Hacking and Intellectual Property (CHIP) units will consist of special teams of attorneys trained to prosecute people on charges of computer intrusion, electronic copyright violations, fraud and "other Internet crimes," Ashcroft said in prepared remarks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/168195.html>

### SIRCAM' WORM GETTING HOTTER

Some e-mail in-boxes continue fill up with an odd assortment of other people's personal documents and images sent without their owner's permission, compliments of the worm-virus dubbed "SirCam." Discovered in the wild on Wednesday, security experts had assumed the virus would quickly be contained. But now it appears that the worst is yet to come: SirCam is spreading fast and is expected to hit many more computers over the weekend.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,45427,00.html>

### SUPPORTERS RALLY BEHIND ARRESTED RUSSIAN HACKER

The arrest this week of a 26-year-old Russian software programmer accused of violating U.S. copyright law has sparked protests and pledges of support from a wide range of free speech advocates, defense lawyers and consumer groups. "Free Dmitry" rallies are scheduled for Monday in San Jose, Boston, Denver, Chicago, Seattle, Portland, Reno and Moscow, according to the Electronic Frontier Foundation.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/investor/news/newsitem/0-9900-1028-6628223-0.html>

### SAVE YOUR WIRELESS NETWORKS FROM HACKERS

Security managers need to be aware of the inherent weaknesses in wireless technology, which although similar to those in wired networking, add a few more headaches. According to security professionals, the IEEE wireless protocol 802.11 not only shares unlicensed frequencies with other devices, including consumer-based Bluetooth devices, cordless phones, and baby monitors - which can, and do, interfere with each other - it also has weaknesses in its encryption structure.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/Analysis/1124135>

-----

### Security issues

-----

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

-----

### SEARCH ENGINE VULNERABILITY (I.E LYCOS)

It seems that the engine does not correctly handle html code written as html encoded text on the indexed page.

example:

page: <input>

engine: < input >

the encoded string will be returned to the user with > instead of \$gt; and the users browser will create a input field (it handels it as correct html code).

A malicious user may create a interface embended into the engines pages or start a redirect attack.

Link: <http://www.net-security.org/text/bugs/995381087,11371,..shtml>

#### ARGOSOFT FTP SERVER WEAK PASSWORD ENCRYPTION

ArGoSoft FTP Server 1.2.2.2 for win32 is vulnerable to decryption of the password file. As a matter of fact the programmers are aware of this since they have implemented decryption algorithms within the FTP Server program itself, as we can find the decrypted passwords when watching the program's memory dumps, or using system debuggers or special tools to peek at the password (User Properties) which is hidden with \*\*\*\* (normally one would expect this to contain something like "-=encrypted=-" so that it can only be changed, but in this case it contains the plaintext password)-

Link: <http://www.net-security.org/text/bugs/995381139,92852,..shtml>

#### RED HAT SECURITY ADVISORY: ELM

Elm had a buffer overflow when handling very long message-ids. This overwrote other header fields, and could potentially cause more damage. Note that Red Hat Linux 7.1/Alpha shipped with this newer version.

Link: <http://www.net-security.org/text/bugs/995381210,28028,..shtml>

#### CARD SERVICE INTL. / LINKPOINT API SECURITY CONCERNS

When you are approved for a CSI merchant account (or even when you are approved for a test account), CSI sends you two emails. One of the emails has the subject "Welcome to LinkPoint API" (the other is unimportant). This email contains two pieces of information:

The gateway server's hostname

Your "Store Name" (the six digit number)

They attach your certificate AND \_private key\_ to the bottom of the message. The idea is that you copy and paste the cert + private key into a file for the client API to use when it connects.

Link: <http://www.net-security.org/text/bugs/995381345,62812,..shtml>

#### RED HAT SECURITY ADVISORY: NEW UTIL-LINUX PACKAGES

vipw, from the util-linux package in Red Hat Linux 7.1, included a new option that allowed editing of the /etc/shadow file as well as /etc/passwd. However, this option did not take measures to ensure that the file remained only readable by root.

Link: <http://www.net-security.org/text/bugs/995381395,7691,..shtml>

#### SPECIAL DEVICES ACCESS IN MULTIPLE ARCHIVERS

Archive extraction is usually treated by users as safe operation. There are a lot of problem with files extraction though.

Link: <http://www.net-security.org/text/bugs/995381475,78014,..shtml>

#### ADCYCLE SQL COMMAND INSERTION VULNERABILITY

AdCycle does not propely validate the user input. This input is used to form SQL commands, which are passed to a mySQL database. By submitting cleverly crafted input, an attacker can bypass the administrator password check.

Link: <http://www.net-security.org/text/bugs/995381520,8208,..shtml>

#### INTERACTIVE STORY FILE DISCLOSURE VULNERABILITY

Interactive Story does not properly validate the contents of a hidden field entitled "next". By setting that field to the name of a file, and using double dots and poison nulls, an attacker can cause Interactive Story to display the contents of any file.

Link: <http://www.net-security.org/text/bugs/995381686,39134,.shtml>

#### CALDERA - DOCVIEW LOCAL HTTPD EXPLOIT

Docview is a set of CGI scripts providing documentation over http. A argument validation problem in one of the CGI scripts made it possible for a local attacker to gain access to the 'httpd' account.

Link: <http://www.net-security.org/text/bugs/995469351,75256,.shtml>

#### PHP MAIL FUNCTION VULNERABILITY

php mail() function does not do check for escape shell commandes, even if php is running in safe\_mode. It may be possible to bypass the safe\_mode restriction and gain shell access.

Link: <http://www.net-security.org/text/bugs/995534103,28541,.shtml>

#### PHP LOCAL DENIAL OF SERVICE

PHP scripting allows "opening" files through HTTP:

```
$file=fopen("http://host/page.html","r");
```

If script opening itself through HTTP, it will result in DoS attack:

as much as possible HTTP connections and great number of executing PHP scripts. Timeout settings are useless.

Link: <http://www.net-security.org/text/bugs/995534301,88119,.shtml>

#### MULTIPLE VENDOR TELNET DAEMON VULNERABILITY

Within most of the current telnet daemons in use today there exist a buffer overflow in the telnet option handling. Under certain circumstances it may be possible to exploit it to gain root priviledges remotely.

Link: <http://www.net-security.org/text/bugs/995534424,30993,.shtml>

#### SQUID HTTPD ACCELERATION ACL BUG

Squid has a known bug in 2.3STABLE4 which ignores acl's in httpd\_accel mode. Note this is only if in httpd\_accel\_host is set and httpd\_accel\_with\_proxy off is set. This is not the default configuration so it is not vulnerable without making these configuration changes. This enables portscanning via squid running in this mode potentially allowing remote attackers to compromise machines through a squid set up this way.

Link: <http://www.net-security.org/text/bugs/995534512,94121,.shtml>

#### HTTPROTECT VULNERABILITY

Even if attackers have the root privilege, protected files cannot be changed, but they can change protected files under these conditions:

- 1.Attackers can make symlink in a writable directory(ex. /tmp)
- 2.They are the owner of the target file or they have root privilege.

example: (A protected file is /opt/www/html/index.html)

```
$ ln -s /opt/www/html/index.html /tmp/foo
```

```
$ vi /tmp/foo (cat /tmp/hack.html > /tmp/foo)
```

Link: <http://www.net-security.org/text/bugs/995534597,5990,.shtml>

#### TRUSTIX SECURE LINUX SECURITY ADVISORY - SQUID

Versions 2.3.STABLE2 through 2.3.STABLE4 have a serious security bug when Squid is used in the 'httpd\_accel' mode. If you configured httpd\_accel\_with\_proxy off then any request to Squid is allowed. Malicious users may use your proxy to port-scan remote systems, forge email, and do other nasty things.

Link: <http://www.net-security.org/text/bugs/995627697,78708,.shtml>

#### BUFFER OVERFLOW VULNERABILITY IN LIBI18N LIBRARY

AIX ships with the library "libi18n" located in the "/usr/ccs/lib" directory. This library contains a function that is vulnerable to a buffer overflow through the LANG environment variable.

Link: <http://www.net-security.org/text/bugs/995627904,92485,.shtml>

#### RED HAT LINUX - UPDATED SQUID PACKAGES

New squid packages are available for Red Hat Linux 7.0 that fix a possible security problem with Squid's HTTP accelerator feature. If Squid was configured in accelerator-only mode, it was possible for remote users to portscan machines through the Squid proxy, potentially allowing for access to machines not otherwise available.

Link: <http://www.net-security.org/text/bugs/995628872,15795,.shtml>

#### TESTING FOR IDQ.DLL VULNERABILITY

I had to come up with a way to test a server remotely for this vulnerability without actually killing it and running the plethora of exploit code that is out.

Link: <http://www.net-security.org/text/bugs/995634801,15771,.shtml>

#### CISCO - "CODE RED" WORM CUSTOMER IMPACT

A malicious self replicating program known as the "Code Red" worm is targeted at systems running the Microsoft Internet Information Server (IIS). Several Cisco products are installed or provided on targeted systems. Additionally, the behavior of the worm can cause problems for other network devices.

Link: <http://www.net-security.org/text/bugs/995708464,23707,.shtml>

#### REMOTE ROOT EXPLOIT IN SSH SECURE SHELL 3.0.0

A potential remote root exploit has been discovered in SSH Secure Shell 3.0.0, for Unix only, concerning accounts with password fields consisting of two or fewer characters. Unauthorized users could potentially log in to these accounts using any password, including an empty password. This affects SSH Secure Shell 3.0.0 for Unix only.

Link: <http://www.net-security.org/text/bugs/995731141,44241,.shtml>

#### ORACLE VULNERABILITY DISCOVERED IN OID

There's a new vulnerability discovered in the Oracle Internet Directory (Oracle's LDAP server). It has been in the database since 7/16, but I haven't seen it mentioned here yet.

Link: <http://www.net-security.org/text/bugs/995731212,25914,.shtml>

#### NETWIN AUTHENTICATION MODULE 3.0B PROBLEMS

The 'NetWin Authentication module' which is used by SurgeFTP, DMail and other programs uses a quite 'unusual' hashing algorithm to store the password

hashes. Because of the complexity of the hashing algorithm, the users of NWAAuth may not be aware of it, but the algorithm is flawed in (at least) two ways:

- 1) the password hashes can be decrypted
- 2) one hash can match more than one password

Link: <http://www.net-security.org/text/bugs/995731406,27182,.shtml>

#### IBM TFTP SERVER FOR JAVA VULNERABILITY

The IBM alphaWorks TFTP Server for Java available at <http://www.ibm.com> is vulnerable to a standard directory traversal attack.

Link: <http://www.net-security.org/text/bugs/995732281,29605,.shtml>

#### IMP 2.2.6 RELEASED - FIXES SECURITY HOLES

The Horde team announces the availability of IMP 2.2.6, which fixes three potential security issues. We strongly recommend that all sites running IMP 2.2.x upgrade to this version.

Link: <http://www.net-security.org/text/bugs/995817276,88786,.shtml>

---

#### Security world

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

---

#### OBLIX: FIRST XML-BASED WEB SECURITY SOLUTION - [16.07.2001]

Oblix Inc., a leading developer of e-business infrastructure software, announced that its newly released Oblix NetPoint 5.0 is the first XML-based web access management solution that addresses demand for openness and interoperability through a Web services architecture built for the enterprise. Oblix NetPoint 5.0 features AccessXML, IdentityXML, and PresentationXML that lower the cost of administration by automating business processes and easing the integration of Web access management systems with an existing e-business infrastructure.

Press release:

< <http://www.net-security.org/text/press/995301147,82072,.shtml> >

---

#### SYBARI SHIPS ANTIGEN 6.0 FOR DOMINO SERVERS - [16.07.2001]

Sybari Software, Inc., the premier developers of Antigen, a comprehensive anti-virus, content-management, and e-mail security solution for Lotus Domino/Notes environments, ships Antigen 6.0 for Domino servers. Antigen 6.0 for Domino was designed specifically to meet the highly-specialized antivirus and security needs required by Domino/Notes administrators to maintain virus free groupware environments.

Press release:

< <http://www.net-security.org/text/press/995301200,46630,.shtml> >

---

#### BINDVIEW ANNOUNCES SEVEN REGIONAL PARTNERS - [16.07.2001]

BindView Corporation, a leading provider of IT administration and security management solutions, announced at Microsoft Fusion its alliance with seven regional partners: FrontWay, GMSI, Intrinsic, Para-Protect, RK Dixon, TEKsystems and Xerox Connect - Houston. These partners are utilizing BindView's market-leading technology to develop robust, flexible and customized solutions and services offerings for their customers. The strategic alliances enable BindView and its partners to offer a wide range of comprehensive services, including security consulting and vulnerability assessment, Microsoft Windows 2000 and Active Directory platform migration and compliance with federal privacy and security regulations such as the Health Information Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act.

Press release:

< <http://www.net-security.org/text/press/995301319,27710,.shtml> >

---

#### VULNWATCH SECURITY MAILING LIST LAUNCHES - [17.07.2001]

VulnWatch.org, today at the Black Hat computer security conference in Las Vegas, announced a new non-profit, independent security vulnerability disclosure mailing list to serve the vulnerability information needs of IT professionals, software and hardware vendors, and security researchers.

Press release:

< <http://www.net-security.org/text/press/995376126,27804,.shtml> >

---

#### NIST GIVES AWAY VULNERABILITY DATABASE - [17.07.2001]

The NIST Computer Security Division's ICAT project team is now giving away copies of the ICAT vulnerability database for public use (<http://icat.nist.gov>). The database currently contains 2628 vulnerabilities. This means that ICAT can now be used as a royalty free vulnerability database for commercial and free products. In addition, the ICAT data file contains a GUI interface allowing people to use ICAT as an off-line application. The ICAT team supports the public sharing of vulnerability information that can help secure systems and we are excited about releasing control of our data.

Press release:

< <http://www.net-security.org/text/press/995381571,93687,.shtml> >

---

#### F-SECURE AND EDS PARTNER - [17.07.2001]

F-Secure Corporation, a leading developer of centrally managed security solutions for the mobile enterprise, and EDS, announced they have formed an

agreement in which EDS will re-sell F-Secure products and provide integration, security management and support services to F-Secure customers worldwide. Additionally, F-Secure is providing security content for EDS' Cyber Security Institute, a computer security curriculum to arm IT professionals and consumers with skills to battle hackers, security breaches and viruses.

Press release:

< <http://www.net-security.org/text/press/995386779,37165,.shtml> >

---

#### LATEST KASPERSKY ANTI-VIRUS FOR UNIX/LINUX OUT - [17.07.2001]

Kaspersky Labs, an international data-security software-development company, announces the release of the latest version of the popular Kaspersky Anti-Virus for Unix/Linux operating systems. The latest version of Kaspersky Anti-Virus affords customers the opportunity of additionally installing a centralized anti-virus defense for file servers and application servers operating on OpenBSD 2.8 and Solaris 8 (for Intel processors) systems, and also for exim e-mail gateways (one of the five most popular e-mail gateways for Unix/Linux).

Press release:

< <http://www.net-security.org/text/press/995386846,48998,.shtml> >

---

#### JAM ECHELON DAY ON OCTOBER 21ST 2001 - [17.07.2001]

A large group of individuals in the Global Internet Community have set out to bring attention to the communications monitoring system known as ECHELON. Two years ago, when this idea was launched, the existence of ECHELON was denied by all of the participating agencies. Now with the recent issuing of the report by the "Temporary Committee on the ECHELON Interception System" its existence and invasive practices are no longer in doubt.

Press release:

< <http://www.net-security.org/text/press/995403788,97012,.shtml> >

---

#### INFORMATICA AND RSA SECURITY PARTNER - [18.07.2001]

RSA Security Inc., the most trusted name in e-security, and Informatica Corporation, the leading provider of business analytic solutions, announced that Informatica has incorporated RSA BSAFE Crypto-J encryption software into its new PowerChannel offering to help secure sensitive data that is transferred via the Internet.

Press release:

< <http://www.net-security.org/text/press/995453888,56914,.shtml> >

---

#### RAPIDSTREAM AWARDED ICASA LABS IPSEC CERTIFICATION - [18.07.2001]

RapidStream, Inc., the developer of scalable, integrated high-performance firewall and virtual private networking (VPN) appliances, announced that its

security products have earned IPSec certification from ICSA Labs, a division of TruSecure Corporation. The RapidStream 2000, RapidStream 4000, RapidStream 6000 and the RapidStream 8000, which all previously received ICSA Labs' Firewall certification, were also awarded IPSec certification in this latest round of testing.

Press release:

< <http://www.net-security.org/text/press/995453962,40776,.shtml> >

-----

#### IDC REPORTS MCAFEE AS AV MARKET SHARE LEADER - [18.07.2001]

For the fourth consecutive year, IDC (International Data Corp.) reports McAfee, a division of Network Associates, Inc., as the number one market share leader of anti-virus software worldwide. In the recently published "Worldwide Antivirus Software Market Forecast and Analysis, 2001-2005" report, IDC cites McAfee as the overall leader in anti-virus software with 29% market share.

Press release:

< <http://www.net-security.org/text/press/995454046,47485,.shtml> >

-----

#### EU DIGITAL SIGNATURE DIRECTIVE DEADLINE - [18.07.2001]

Almost all member states of the European Union have met the target of implementing the EU Digital Signature Directive by the July 19, 2001 deadline. The EU Directive 99/93 on electronic signatures specifies minimal requirements for certificates, certification service providers and signature creation and verification devices. The cornerstone of the law is the advanced electronic signature, which requires the use of "qualified certificates" to have the same legal effect as a handwritten signature. GlobalSign, a leading Trust Service Provider for Internet-based and mobile transactions, is today ready to deliver qualified certificates that meet the requirements of the EU Directive on Electronic Signatures.

Press release:

< <http://www.net-security.org/text/press/995466912,92362,.shtml> >

-----

#### GFI LAUNCHES SECURITY EVENT LOG MONITOR - [19.07.2001]

GFI has launched LANguard Security Event Log Monitor (S.E.L.M.), a revolutionary host-based intrusion detection tool. This new network security product is a centralized event log security analyzer that retrieves all security event logs from servers and workstations and alerts administrators about breaches for immediate intrusion detection.

Press release:

< <http://www.net-security.org/text/press/995535077,59099,.shtml> >

-----

HUSH COMMUNICATIONS LAUNCH HUSHMAIL VERSION 2.0 - [19.07.2001]

Hush Communications ([www.hush.com](http://www.hush.com)), a leading global provider of managed security solutions and encryption key-serving technology, has launched HushMail Version 2.0, the latest version of its world premier secure Web-based email service. The upgrade now supports the OpenPGP standard, offers improved functionality, and exciting new features. Version 2's support for OpenPGP marks a major breakthrough in widening the appeal and usability of HushMail, as Version 2.0 is a major move toward achieving interoperability with the other member companies. Very soon Hush users will be able to communicate securely with PGP and other member company applications, creating a universal interoperable platform for secure digital technologies. PGP is the most widely used email security protocol and this new version opens up HushMail users to an estimated 8 million PGP users worldwide.

Press release:

< <http://www.net-security.org/text/press/995535225,4567,.shtml> >

-----

SOPHOS SIX-MONTH SUMMARY OF VIRUS ACTIVITY - [19.07.2001]

Sophos, a world leader in corporate anti-virus protection, has announced that it has detected and protected against 6,127 new viruses in the first six months of 2001. In the same period, calls to Sophos's customer helpdesk suggested that those viruses which demanded the most media attention were not necessarily those causing the biggest problem. Sophos's research highlights the importance of safe computing practices and the need to keep anti-virus (AV) software up to date.

Press release:

< <http://www.net-security.org/text/press/995535309,62699,.shtml> >

-----

KASPERSKY ANTI-VIRUS FOR PALM OS RELEASED - [20.07.2001]

Kaspersky Lab, an international data-security software-development company, announces that the latest version of its world-famous, award-winning Kaspersky Anti-Virus for the Palm operating system is now available for online purchase in Kaspersky Lab's Online Store.

Press release:

< <http://www.net-security.org/text/press/995627130,48698,.shtml> >

-----

TRUSTED SECURITY FOR REMOTE AND ROAMING USERS - [20.07.2001]

TrustWorks Systems, an innovator in network security solutions, announced that "Trusted Security for Remote and Roaming Users" is now shipping as an integral part of the company's latest VPN security platform. Trusted Security delivers powerful remote and roaming user security enforcement and management benefits that make deploying and managing roaming users dramatically easier and less costly than other solutions. TrustWorks' new Trusted Security solution is connection independent, providing a secure connection wherever a user is located. Each individual client is both a

distributed firewall and an IPsec VPN agent that supports strong user authentication, access control and data communication protection for information that resides on corporate networks.

Press release:

< <http://www.net-security.org/text/press/995640671,76080,.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)

-----  
KSignWPKI

KSignWPKI Products Features:

- Adoption of De-facto international standard WAP solution
- General WPKI solution to be accepted by ME (Mobile Explorer)
- Interoperability of domestic Public Certificate Authorities
- Developed by making the most use of KSignPKI development know-how at home and abroad
- Applied short-lived certificate mechanism to reduce the Revocation list check overhead
- Guarantee User Authentication, Non-Repudiation, Data Integration, E2E Confidentiality on WPKI Platform
- Supporting E2E (End to End) mobile Internet security solution
- Supporting Optimized terminal (MS) Crypto module

Read more:

< <http://www.security-db.com/product.php?id=588> >

This is a product of KSign, for more information:

< <http://www.security-db.com/info.php?id=126> >

-----  
AIR SMARTGATE

V-ONE has extended its award winning SmartGate Internet VPN technology into the wireless network environment by introducing Air SmartGate to its product portfolio. Air SmartGate is an advanced messaging security solution that uses a innovative system for pager-to-server communications (patent pending) that supports a sophisticated authentication method and data encryption scheme that provides a high level of data security prior to transmission over the air. Air SmartGate uses a special pager proxy that manages information flow between a carrier's message switch and the

Air SmartGate server.

Read more:

< <http://www.security-db.com/product.php?id=208> >

This is a product of V-ONE, for more information:

< <http://www.security-db.com/info.php?id=35> >

---

#### 5THSENSE COMBO PERSONAL AUTHENTICATION PERIPHERAL

Built on the silicon FPS110 Silicon Fingerprint Sensor, the 5thSense Combo family is a revolutionary new line of personal authentication peripherals for computer and network security. The 5thSense Combo peripheral brings the security and convenience of fingerprint-based personal authentication to a broad range of IT and e-commerce applications. Veridicom's high performance imaging and verification software suites complement the 5thSense Combo peripheral.

Read more:

< <http://www.security-db.com/product.php?id=298> >

This is a product of Veridicom, for more information:

< <http://www.security-db.com/info.php?id=59> >

---

## Featured articles

---

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)

---

## "CODE RED" WORM RELATED ARTICLES

All the articles can be found in our special coverage related to the worm.

Read more:  
< <http://www.net-security.org/text/articles/coverage/code-red> >

---

## AUTOMATING PENETRATION TESTS: A NEW CHALLENGE FOR THE IS INDUSTRY?

This is the presentation from the BlackHat Briefings by Iván Arce and Máximiliano Cáceres.

Read more:  
< <http://www.net-security.org/text/articles/index-download.shtml#BlackHat> >

---

## FINDING USER-WRITTEN CGI SKRIPTS BY ANALYZING HTML OBJECTS

incubus writes: "So, why this? Well.. because there are far too many chkcgi.c's on the internet, even if it's wrapped in some nice anti-IDS package, and even if it finds a way through zillions of proxy servers.. People still check for the same bugs over and over again.. php.cgi, phf, unicode, msadc,... you name it, those tools test it. So, we can find a lot more information on a website instead of trying to access some cgi scripts. Just by looking and analyzing the results we get from the website."

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

---

## Security Software

---

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

---

### ADVANCED NT SECURITY EXPLORER 2.0

Advanced NT Security Explorer (ANTExp) is an application for Microsoft Windows NT, Windows 2000 and Windows XP system administrators for finding holes in system security. It analyses user password hashes, and tries to recover plain-text passwords. If it's possible to recover the password in a reasonable time, the password should be considered to be insecure. Some users like simple and easy to remember passwords, unfortunately.

Info/Download:  
< <http://www.net-security.org/various/software/994768117,83599,windows.shtml> >

---

### SYGATE PERSONAL FIREWALL 4.1 (BETA PREVIEW)

New features:

- Customizable Advanced Firewall Rules
- Ability to Configure Global Settings such as trusted IP addresses
- User-friendly Rule Viewer & Rule Editor
- Message Console to display security alerts and system information
- Unique Dynamic Help System assists users with rule creation
- Enhanced ability to capture and log packets per rule
- Ability to control incoming and outgoing ICMP packets by type

Info/Download:  
< <http://www.net-security.org/various/software/994939723,24937,windows.shtml> >

---

### MYNETWATCHMAN 1.13

Centralized firewall log analyzer that works with BlackICE and ZoneAlarm. Decodes, analyzes, backtraces, and filters your firewall event log. Automatically escalates appropriate incidents to the responsible site owner/ISP and provides your full feedback. Say goodbye to spending hours doing traceroutes and whois lookups, myNetWatchman does it all for you.

Info/Download:  
< <http://www.net-security.org/various/software/995020375,95627,windows.shtml> >

---

PASSWORD-CREATOR 2.0

This program creates passwords by choosing eight characters randomly (from numerals and uppercase and lowercase letters) and copying them to your Clipboard.

Info/Download:

< <http://www.net-security.org/various/software/995272293,47867,windows.shtml> >

KEYSPY 6.5

KeySpy can capture (log) what someone has typed on a PC keyboard and send the recorded keys in an encrypted, compressed format to your e-mail, or save them in a hidden disk file. By pasting the encrypted keys in the decryptor window, you can see what has been typed. The task manager lets you easily download and execute any program on the monitored computer, as well as copy, delete, and move any file.

Info/Download:

< <http://www.net-security.org/various/software/995279663,44008,windows.shtml> >

=====  
Help Net Security T-Shirt available  
=====

Thanks to our affiliate Jinx Hackwear we are offering you the opportunity to wear a nifty HNS shirt :) The image speaks for itself so follow the link and get yourself one.

Get one here: <http://207.21.213.175:8000/ss?click&jinx&3af04db0>  
=====

Questions, contributions, comments or ideas go to:

Help Net Security staff

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

<http://net-security.org>

<http://security-db.com>