

HNS Newsletter
Issue 60 - 23.04.2001
<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: 2258

Table of contents:

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

=====
Advertisement - HAL 2001

=====
Between 10th and 12th August, thousands of hackers will populate the green fields of the campus of the University of Twente, converting it into a large doubleplus-extrawired campsite. When not visiting lectures or workshops, we'll be engaged in technical or political discussions, or maybe just relaxing somewhere in the grass.

If you can truly celebrate the Internet and embrace new technologies, without forgetting your responsibility to tell others that new technologies come with new risks to the individual and to society as a whole, then this is the place to be this summer. To be sure of an entrance ticket, register now! Visit us at <http://www.hal2001.org>

=====
General security news

AVOIDING SECURITY HOLES WHEN DEVELOPING AN APPLICATION

This series of articles tries to put the emphasis on the main security holes that can appear within applications. It shows ways to avoid those holes by changing development habits a little. This article, focuses on memory organization and layout and explains the relationship between a function and memory. The last section shows how to build shellcode.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://mercury.chem.pitt.edu/~tiho/LinuxFocus/English/March2001/article183.shtml>

USING GNUPG WITH PINE FOR SECURE E-MAIL

Many people have no problems sending sensitive data via e-mail. Most of us do not know how easy it is for anybody to read it. Just because somebody holds the title of "Systems Administrator" does not mean they can be trusted. What is stopping them from reading your e-mail? Nothing. This is where PGP comes in; it is easy-to-use encryption meant for the common person.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/feature_stories/feature_story-83.html

EX-SOVIET STATES A HOTBED FOR HACKING

Tonu Samuel says he is part of the solution to the growing threat from computer hackers and cybercriminals. The Estonian Internet company whose system Samuel hacked into says he is part of the problem. Their dispute is a small one in a small nation, but it captures the challenges facing companies and governments in the Internet age.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://chicagotribune.com/news/nationworld/article/0,2669,SAV-0104150339,FF.html>

PREPARING FOR THE SCRIPT-FORM ATTACK

"Today we live in an electronic era, with the use of the Internet growing by leaps and bounds. Along with this growth, we have unfortunately witnessed an increase in the distribution of viruses, DoS attacks, and the break-in and modification of home pages on Web servers operated by government agencies, commercial organizations, and academia. The purpose of this article is to acquaint readers with a relatively new type of network-based attack that can cost your organization money. I will describe what I call a "script-form" attack; I will first examine how this attack can occur, and some prevention methods."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sysadminmag.com/current/0105o/0105o.htm>

FROM TEEN HACKERS TO JOB HUNTERS

At age 3, Patrick Roanhouse got his first computer. At 7, he figured out how to construct a modem out of scrap parts. By 14, he was running around cyberspace under the alias "Anarchist" and working up all sorts of havoc. Then he met the 2600 Club. The group, which publishes a popular hacker magazine, has an almost mythical reputation. It has been investigated by the Secret Service and has inspired monthly gatherings in more than 100 cities around the world. Patrick thought 2600 would teach him how to hack. Instead, it taught him about job hunting, stock options and business plans.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.washtech.com/news/media/9091-1.html>

CHINESE DEFACERS UNDER INVESTIGATION

Chinese defacers, possibly angry about the downing of one of their nation's fighter jets last week, are under investigation by U.S. officials related to the defacement of nine U.S. Web sites.

Link: <http://www.law.com/cgi-bin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=ZZZE6G3MILC&live=true&cst=1&pc=5&pa=0&s=News&Explgnore=true&showsummary=0>

MANTRAP COMING TO INDIA

'Mantrap' will trap the attacker or any malicious intruder by employing 'decoys' at various strategic points of the system and will 'distract' him/her away from the original system. According to Times of India Online, the solution developed by PeakXV Networks, will be soon introduced in India.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.timesofindia.com/today/17info5.htm>

JUMPSTART FOR SOLARIS SYSTEMS PART II

This is the second of two articles examining JumpStart, a tool that enables Solaris system administrators to install and configure systems remotely. In the first article we introduced Sun's JumpStart system as well as the JumpStart Architecture and Security Scripts (JASS) toolkit from Sun. We also showed how the JumpStart system allows a system administrator to automate the installation of Solaris systems, while the JASS toolkit builds on top of JumpStart to allow the automated installation of hardened systems. This article will focus on the use of the JASS toolkit in the installation of a bastion mail host.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/sun/articles/jumpstart2.html>

IP INSECURITY

Stolen credit card numbers, hacked federal computer systems and other high profile online assaults have put many users on their guards and focused the attention of security managers on high-level intrusion-detection systems, chains of firewalls and other high-level defenses. But many forget that, no matter how hard they try to secure a site, vulnerabilities built into the fabric of the Internet still leave them at risk - even though measures to shut down the most glaringly common vulnerabilities are easily available.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59610,00.htm

I

IPTABLES BASICS NHF

"I'm sure many of you have been wondering how to use iptables to set up a basic firewall. I was wondering the same thing for a long time until I recently figured it out. I'll try to explain the basics to at least get you started."

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxnewbie.org/nhf/intel/security/iptables_basics.html

FTP ATTACKS

FTP used to be the king of the Internet. If you wanted to download something you went to your favorite ftp server or used Archie to find the file. Even today, the number of ftp servers is staggering, and many ftp sites contain several

hundred gigabytes of online archives (take a look at your local sunsite). FTP was built to be an extremely flexible protocol, and therein lie many of its problems. The FTP protocol not only allows you to transfer files from an ftp server to your machine but from one ftp server to another ftp server directly.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010418.html>

INTRUSION DETECTION

If a firewall is like having a security guard at your office door, checking the credentials of everyone coming and going, then an intrusion-detection system (IDS) is like having a network of sensors that tells you when someone has broken in, where they are and what they're doing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.itworld.com/News/2001/4/CED010416STO59611/>

INFECTABLE OBJECTS, PART FIVE - HTML AND OTHER SCRIPTS

One of the more interesting developments in the virus world has been the extension of viruses from compiled executable files into script files. There is now an expanding range of script file types that can contain malicious code. This article, the fifth and final in a series by SecurityFocus writer Robert Vibert, will offer an overview of script file types that can contain viral code, including batch files, Java, JavaScript and HTML files.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/virus/articles/infobj5.html>

BUG WATCH: IS LINUX SAFE FROM ATTACK?

Fresh concerns have come to light regarding the vulnerabilities of open source operating systems to virus attacks. Last week's Red Worm virus was the latest in a long line to target Linux. There's been a long-standing belief throughout the Linux community that hackers and virus writers had better things to do than target them with malicious attacks - a belief that is beginning to erode.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/News/1120613>

ACCUBYTE LEAVES CUSTOMER CREDIT CARD DETAILS EXPOSED

Customers of computer components supplier Accubyte have been encouraged to check their credit card records for fraudulent misuse after it admitted that its previously lax security left confidential information exposed.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/18328.html>

NEW TOOLS ADDRESS DENIAL-OF-SERVICE THREAT

Concerns about denial-of-service attacks are resulting in a growing number of products and services aimed at helping companies detect, trace and block the threat. But most of the technologies do little to prevent such attacks outright, users said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/04/17/dos.tools.idg/index.html>

'SANDBOXING' TECHNOLOGY CAN STIFLE HACKERS

Forget the popular myth of the teen hacker. An older, more sophisticated hacker is out there, spreading malicious code disguised as files and standard Internet apps into corporate networks. It's this fear of the unknown that's starting to scare some IT managers into adding behavior-blocking, or "sandboxing," technology, as a last line of defense at the desktop. Behavior blocking prevents malicious code from doing something it's not authorized to do. If a downloaded executable program tries to erase the PC's hard drive or copy its address book, for instance, the software stops it cold.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.networkweek.com/wire/story/TWB20010418S0011>

INTERNET BANKS 'IN DENIAL' ON HACKING THEFTS

At least four large internet banks in Britain have been attacked by computer hackers, it emerged yesterday at the launch of a national police unit to tackle cybercrime. It is believed that in each case at least hundreds of thousands of pounds was stolen, but the banks concerned have been reluctant to report the thefts for fear it will damage the credibility of banking online.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.guardianunlimited.co.uk/internetnews/story/0,7369,474815,00.html>

CRACKERS EXPAND PRIVATE WAR

As China and the United States attempt to peacefully end their diplomatic standoff sparked by the mid-air collision between a U.S. spy plane and a Chinese fighter jet, crackers from both countries continue to wage private wars on the Internet. American cracker group PoizonBOx has defaced at least a hundred Chinese websites since April 4. Chinese hackers are now vowing to retaliate with a planned week-long all-out crack attack on American websites and networks which will start on May 1.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,43134,00.html>

SECURITY OF CENSUS DATA 'GUARANTEED'

The public and private agencies involved in the UK Census claim to have taken all precautions to guarantee that the data will be secure. Information held at the main purpose-built processing centre is stored on a closed network of servers with no connection to the outside world, said Census project service director Tom Rowe. "The system is on a local area network, with no network connections. Anything which people could hack wouldn't be allowed," he said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/News/1120701>

IMMUNIX REVIEW

If you get the security mailing list for your Linux distribution or browse CERT's advisories, you've probably noticed that a majority of security advisories are tied to buffer overflows. One aspect of security, then, is to prevent these attacks whenever possible. This is where WireX and their Immunix distribution and StackGuard compiler come in. WireX's StackGuard compiler is based on the egcs compiler, but has been rewritten to remove buffer overflow vulnerabilities. The Immunix distribution is based on Red Hat Linux 7.0, but the majority of the distribution has been compiled with the StackGuard compiler instead of the standard GNU compilers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/reviews/articles/0104/0104e.shtml>

CODED WARNING

Hacking attacks are on the increase in the UK and concerns are mounting that the country's leading organisations are not fully prepared to cope with the problem. A report published last week claimed that a third of the UK's major companies and public sector organisations had been hacked into by cyber-terrorists. Speaking in the Commons, the foreign secretary, Robin Cook, said: "Computers now manage most of our critical national infrastructure but with these new opportunities there also comes the risk of new threats. A computer-based attack could cripple the nation more quickly than a military strike."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.guardian.co.uk/online/story/0,3605,474650,00.html>

THE UNWIELDY E-COMMERCE SECURITY QUESTION

Government agencies and non-governmental nonprofit organizations have been very busy announcing massive Internet fraud cases. Furthermore, the news announcing cybercrimes has yet to ebb. One search engine lists more than 180,000 pages discussing the problem of credit card fraud.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.osopinion.com/perl/story/8993.html>

NETWORK ENCRYPTION KEYS

[Q] My new 3Com wireless network has only one problem - each PC uses a different grid to enter the encryption key.

[A] Those are just different ways to present the same number. An encryption key - used to secure transmissions from one PC to another in your home network - of 1122334455 will be displayed as 11.22.33.44.55 in the software on one computer and as 11223 34455 on another. As long as both include the same sequence of numbers, things will work.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.washtech.com/news/software/9146-1.html>

EUDORA ADDS NEW SECURITY IN VERSION 5.1

Eudora, a standalone e-mail program, is noteworthy for its support of the Macintosh operating system. The Eudora version that can be used under the Mac OS X is currently in beta. Version 5.1 enables more secure connections for sending and receiving e-mail and conducting online transactions over the Internet by employing the Secure Socket Layer Internet security standard.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1006-200-5671480.html>

PONYING UP FOR REAL-TIME SECURITY ALERTS

CERT Coordination Center, formerly known as the Computer Emergency Response Team at Carnegie Mellon University, and the Electronic Industries Alliance (EIA), an electronics industry trade organization, on Thursday launched the Internet Security Alliance (ISA). The new organization will deliver up-to-the-minute warnings on viruses and security attacks to companies willing to pay anywhere from \$2,500 to \$70,000 annually for its service. Members will receive warnings roughly 45 days before the information is available to the public.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-5665677.html>

FIREWALL DESIGN WHITE PAPER

"First of all let's define what a firewall is but a bit differently. Here I will digress a bit from the commonly accepted wisdom, and will define a firewall as an access nexus in the digital communication infrastructure of any organization. That is you build a firewall not only to protect your internal data but to also be able to overall enhance your communication abilities. This paper here is not a set of instructions of how to built an access nexus it is more like a white paper of things you should expect from such a device and be able to ask for them from you vendor. Please do tell them that they are currently available on Open Source Servers."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unix.gr/fwdesign.html>

\$50,000 PRIZE TO HACK U.K. WEB SERVER

Computer hackers from around the world are being invited to break into a locked-down Web server in a competition launched for to publicise Britain's largest security conference, Infosec. US-based security firm Argus Systems Group will offer the prize money to any hacker that can penetrate its PitBull security software, which is used commercially to secure Web sites from intruders.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/15/ns-22334.html>

CIH STILL A SERIOUS THREAT THREE YEARS LATER

"Thursday, April 26, 2001 is the date that Win95.CIH is scheduled to once again drop its vicious payload. Chen Ing-Hau wrote Chernobyl, a variant of the CIH family, in May or June of 1998 while a student at the Tatung Institute of Technology. Some say that CIH may just be the most prolific virus in circulation, as well as having one of the most destructive payloads around. Chernobyl attempts to continuously overwrite the hard disk, which crashes the system, and overwrites the BIOS, which may render the computer unbootable. We at SecurityPortal want to remind our readers to install and use updated antivirus software NOW, to avoid Malware such as CIH before they strike. Malware in

the CIH family continue to be major players in our Top 20 Virus/Malware list each week."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/cih20010420.html>

NETBSD SECURITY PROCESSES AND SERVICES

"This document covers secure processes and services for NetBSD Operating Systems and Networks. Most of the information in this document can easily be translated to other BSD systems, however. The NetBSD Operating System comes with a full host of built in and (as of release 1.5) kernel level enabled by default security tools for the Systems and Networks Administrator. As of the 1.5 release, the default installation is bulletproof in regards to remote attacks, this makes it even more appealing."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.diverge.org/doc/nsps/>

Security issues

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

QPC POPD BUFFER OVERFLOW VULNERABILITY

The pop daemon that ships with the QVT/NET software suite contains an unchecked buffer in the logon function. When a username or password of 584 bytes or more gets fed to the server the buffer will overflow and will trigger an access violation, after which the server dies.

Link: <http://www.net-security.org/text/bugs/987418109,21193,.shtml>

QPC FTPD DIRECTORY TRAVERSAL VULNERABILITY

The ftpd daemon that ships with above mentioned packages is vulnerable to a directory traversal problem. Adding '../' ('s excluded) to a listing request ('ls') any user can gain read access to other directories than his/her own.

Link: <http://www.net-security.org/text/bugs/987418481,53996,.shtml>

DEBIAN LINUX - MULTIPLE KERNEL PROBLEMS

The kernels used in Debian GNU/Linux 2.2 have been found to have multiple security problems.

Link: <http://www.net-security.org/text/bugs/987418235,95064,.shtml>

DEBIAN LINUX - EXUBERANT-CTAGS PROBLEMS

Colin Phipps discovered that the exuberant-ctags packages as distributed with Debian GNU/Linux 2.2 creates temporary files insecurely. This has been fixed in version 1:3.2.4-0.1 of the Debian package, and upstream version 3.5.

Link: <http://www.net-security.org/text/bugs/987418545,9980,.shtml>

RED HAT LINUX - UPDATED PINE PACKAGES

Previous versions of the pine email client, and the pico editor have had various temporary file creation issues that allow any user with local system access, to cause files owned by anyone including root to potentially be overwritten if the right set of conditions are met.

Link: <http://www.net-security.org/text/bugs/987418417,29761,.shtml>

TREND MICRO INTERSCAN VIRUSWALL 3.01 VULNERABILITY

A combination of bugs found in the ISADMIN service that would allow an attacker to remotely compromise a system running Trend Micro Interscan Viruswall 3.01. Notice, file paths may change between various distributions so they may not be totally accurate.

Link: <http://www.net-security.org/text/bugs/987418647,24350,.shtml>

SOLARIS IPCS VULNERABILITY

Eeye: We have discovered a buffer overflow in the /usr/bin/i86/ipcs utility provided with Solaris 7. The problem exists in the parsing of the TZ (TIMEZONE) environment variable. By exploiting this vulnerability an attacker can achieve local sys group privileges. IPCS is used for gathering information on active inter-process communication facilities. Exploitation of this vulnerability would be very difficult, but not impossible.

Link: <http://www.net-security.org/text/bugs/987418882,57858,.shtml>

DCFORUM ALLOWS REMOTE READ/WRITE/EXECUTE

In line 121 of file dcboard.cgi, there is a line "require < prefix>< az hidden form field>< suffix>;". (The exact line was not quoted do to copyright limitations.)

The perl statement "require EXPR" will open the file EXPR, parse it, and execute it, as regular perl, as if the entire contents of that file appeared at that point.

Therefore, an attacker who writes a file containing perl commands to the server will be able to execute them by setting the az field to the name of his file on the server. To make matters worse, no input checking is done on the az field, so as long the file is located anywhere on the server, an attacker can reference it, using double dots to undo the prefix and a %00 to truncate off the suffix.

Getting the file onto the server is no problem either. DCForum, by default, allows any user to upload any file, by setting az=upload_file. However, there are other ways of getting files onto the server, so even servers that disable uploading are vulnerable.

Link: <http://www.net-security.org/text/bugs/987517406,83674,.shtml>

BUBBLEMON 1.31 VULNERABILITY

Users can execute programs/shellsript by clicking on the bubblemon app. bubblemon is installed sgid kmem on FreeBSD and does not drop its egid before executing programs.

Link: <http://www.net-security.org/text/bugs/987517561,18230,.shtml>

ACTIVESYNC CAN ACCESS LOCKED WORKSTATION

MS ActiveSync can access files (Outlook appts, contacts, synced files, etc) from a Win2K workstation even though the workstation has been locked. By simply dropping the HP into the dock, or hooking it up to the COM port (depending on which sync method is configured), it will sync and download data from a "locked" workstation.

Link: <http://www.net-security.org/text/bugs/987517714,84422,.shtml>

MICROSOFT ISA SERVER DENIAL OF SERVICE

Microsoft ISA Server 1.0 on Windows 2000 Server SP1 is vulnerable to a simple network-based attack which stops all incoming and outgoing web traffic from passing through the firewall until the firewall is rebooted or the affected service is restarted. If the firewall is configured to use the "Web Publishing" feature (inbound HTTP proxy to a web server), this attack can be performed remotely.

Link: <http://www.net-security.org/text/bugs/987517821,75691,.shtml>

GUNINSKI - DANGERS OF DOUBLECLICKING

By double clicking from Window Explorer or Internet Explorer on filenames with innocent extensions the user may be tricked to execute arbitrary programs.

Link: <http://www.net-security.org/text/bugs/987594992,20897,.shtml>

IPLANET WEB SERVER 4.X PRODUCT ALERT

iPlanet has identified a security vulnerability in the iPlanet Web Server Enterprise Edition 4.x products. This problem does not affect any releases of the product prior to the 4.x versions; however it does affect all iPlanet applications operating on the iPlanet Web Server platform. A patch and implementation instructions to address it are now available.

Link: <http://www.net-security.org/text/bugs/987595169,63098,.shtml>

LOTUS DOMINO WEBSERVER PATH REVEALING

Lotus Domino is a webserver. It has a simple physical path revealing problem.

Link: <http://www.net-security.org/text/bugs/987595856,48919,.shtml>

SAMBA 2.0.8 SECURITY FIX

This release fixes a significant security vulnerability that allows local users to corrupt local devices (such as raw disks). For most users the Samba Team recommends Samba 2.2.0 which has just been released. Version 2.2.0 has all the security fixes plus many new features and other bug fixes. Version 2.0.8 is meant for very conservative sites that want a absolutely minimal security fix rather than a large update.

Link: <http://www.net-security.org/text/bugs/987595922,56064,.shtml>

EUDORA FILE LEAKAGE PROBLEM

An attacker may be able to get any file from a users hard drive if he can make the receiving party to forward a mail containing a false attachment reference to this local file.

Link: <http://www.net-security.org/text/bugs/987596714,99006,.shtml>

DEBIAN LINUX - SAMBA SYMLINK ATTACK

Marcus Meissner discovered that samba was not creating temporary files safely in two places: When a remote user queried a printer queue samba would create a temporary file in which the queue data would be written. This was done using a predictable filename and insecurely, allowing a local attacker to trick samba into overwriting arbitrary files. smbclient "more" and "mput" commands also create temporary files in /tmp insecurely. Both problems have been fixed in version 2.0.7-3.2. and we recommend that you upgrade your samba package immediately.

Link: <http://www.net-security.org/text/bugs/987596849,60354,.shtml>

NETSCAPE REMOTE JAVASCRIPT VULNERABILITY

There is a vulnerability related to javascript in versions below 4.77 of Netscape that allow a remote webserver (which the user is accessing at a particular time) to, for example, obtain information about the client using the "about:" protocol, such as browser history (about:global) or even browser configuration (about:config).

Link: <http://www.net-security.org/text/bugs/987596977,37269,.shtml>

PROBLEM WITH IPLANET CALENDAR SERVER 5.0P2

the standard install of iPlanet Calendar server stores the NAS LDAP admin username and password in plaintext in the world readable file:

```
-rw-r--r-- 1 icsuser icsgroup 37882 Feb 20 10:18
```

```
/opt/SUNWics5/cal/bin/config/ics.conf
```

in the fields

local.authldapbinddn (username)

and

local.authldapbindcred (password)

this potentially gives all local users full read/write access to the underlying NAS LDAP database (which is normally used for admin facilities such as storing user / group profiles, passwords, ACLs, SSL certificates and/or other sensitive company information), and full administrative control of the local NAS server. this access could in turn lead to compromise of other facilities such as web/e-commerce sites, directories etc.

Link: <http://www.net-security.org/text/bugs/987674342,69070,.shtml>

LINUX-MANDRAKE - KERNEL UPDATE

A number of security problems have been found in the Linux kernels prior to the latest 2.2.19 kernel.

Link: <http://www.net-security.org/text/bugs/987680482,55033,.shtml>

DEBIAN - SAMBA FOR SPARC WAS INCORRECTLY BUILT

The updated samba packages that were mentioned in DSA-048-1 were unfortunately compiled incorrectly: the stable chroot we used turned out to be running unstable instead. A new package with version 2.0.7-3.2.1 have been made that are correctly compiled.

Link: <http://www.net-security.org/text/bugs/987680525,81086,.shtml>

VMWARE SYMLINK PROBLEMS

While mounting virtual disk drives using the vmware-mount.pl script, a temporary file named vmware-mount.pl.PID where PID is the current pid of the command will be created in an insecure manner. This allows an

attacker to overwrite any local file, if root mounts a VMware's virtual partition (mounting is usually done as root).
Link: <http://www.net-security.org/text/bugs/987747822,9604,.shtml>

NETOPIA MAC OS X TIMBUKTU VULNERABILITY

At the login screen of the freshly updated Mac OS X with preview version of Timbuktu for Mac OS X we have found a Timbuktu icon in the upper left hand portion of the screen. The menu contains all of the goodies (open timbuktu, turn tcp on/off, about, etc) Timbuktu users have known and loved from the classic OS. The menu About Timbuktu when clicked on gives you full control to the apple menu and system preferences without even being logged into OS X. Having access to the System Preferences without being logged in can allow access to the users panel where someone could change passwords or any system setting. Essentially, you've got admin access to the entire system prefs window and the users panel even shows the hidden admin/root user.
Link: <http://www.net-security.org/text/bugs/987748824,30773,.shtml>

Security world

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

SG2000 CARRIER-CLASS NET SECURITY GATEWAY - [16.04.2001]

ServGate Technologies, Inc., a pioneer in next generation network processor based security gateways, today unveiled a network security gateway designed to meet the rigorous demands of service providers and large enterprises, the ServGate SG2000. The ServGate SG2000 is an all-in-one security device that supports gigabit wire-speed stateful inspection firewall and 3DES IPSec VPN performance. Based on next-generation network processor technology, the SG2000 meets the rigorous performance, availability, and scalability demands of today's rapidly changing network security environment.

Press release:

< <http://www.net-security.org/text/press/987433347,44793,.shtml> >

RED HAT ANNOUNCES RED HAT LINUX 7.1 - [16.04.2001]

Red Hat, Inc., the leader in developing, deploying and managing open source solutions, announced today the availability of Red Hat Linux 7.1, the latest version of the world's most popular open source server operating environment. Red Hat Linux 7.1 includes the new 2.4 kernel with improved SMP support for superior performance on Intel multi-processor platforms. Red Hat Linux 7.1 also delivers new configuration tools that enable users to effortlessly set up and administer DNS, Web and print servers. This release features Red Hat Network

connectivity, including software manager.

Press release:

< <http://www.net-security.org/text/press/987433963,40528,.shtml> >

SERVERPROTECT CERT. FOR CITRIX METAFRAME SERVERS - [16.04.2001]

Awarded Citrix MetaFrame 1.8 Certification by Independent Testing Lab; Advances to Premier Level of Citrix Business Alliance Trend Micro Inc., a worldwide leader in network antivirus and Internet content security solutions, announced that its file server antivirus solution, ServerProtect 5, has earned certification for Citrix MetaFrame 1.8 software. WTS-Center, a German independent testing laboratory, certified that ServerProtect successfully met rigorous functionality and performance criteria.

Press release:

< <http://www.net-security.org/text/press/987439949,90898,.shtml> >

SECURITY INTELLIGENCE PRODUCT LAUNCHED - [17.04.2001]

SecureInfo Corporation delivers a web-based security intelligence service, focusing on Information Systems Security and the protection of critical corporate data. Powered by over 300 years of combined security industry experience, TESS stands alone in the groundbreaking Security Intelligence for Business Continuity (SI4BC) category of security products. To further strengthen its leadership position in the SI4BC category and remain true to its industry trademark "The One Stop Security Shop", SecureInfo Corporation has created a suite of applications that empower Information Technology Professionals to proactively create and take charge of their organization's network security policy and certification process.

Press release:

< <http://www.net-security.org/text/press/987516593,52439,.shtml> >

SANDSTORM ANNOUNCES PHONESWEEP 3.0 - [17.04.2001]

Sandstorm Enterprises announces the new release of its popular PhoneSweep telephone scanner, used by security professionals to audit telephone systems for vulnerabilities. Now used in more than 30 countries, PhoneSweep discovers undocumented or misconfigured modems that are exploitable by criminals, hackers and "crackers." PhoneSweep is similar to an attacker's "war dialer," in that it will dial a large block or set of telephone numbers and report its findings. But PhoneSweep 3.0's capabilities extend beyond mere hacker freeware. PhoneSweep includes a recognition engine that can identify hundreds of different remote access systems. The program can dynamically control many modems simultaneously, slashing scanning time. And PhoneSweep can repeatedly call a set of known "good" numbers to confirm the availability and proper operation of modems required for emergency remote access.

Press release:

< <http://www.net-security.org/text/press/987516790,14570,.shtml> >

INTRUSION.COM'S CHANNELPLUS PROGRAM - [17.04.2001]

Intrusion.com, Inc., a leading provider of enterprise security solutions for the information-driven economy, today strengthened its commitment to helping companies meet the growing demand for security solutions through the launch of its ChannelPlus program. The new program provides channel partners with a deeper level of product and customer knowledge to meet the needs of customers seeking market-leading security solutions.

Press release:

< <http://www.net-security.org/text/press/987516844,27925,.shtml> >

CYBERGUARD SPONSORS SC MAGAZINE AWARDS - [17.04.2001]

As information security breaches continue to dominate headlines around the world and hackers and cyberthieves grow bolder, the spotlight on companies who provide world-leading security solutions shines brighter. For the fifth year, SC Magazine, a division of WestCoast Publishing, will hold a major awards event in London in conjunction with an important information security conference. At the banquet, to be held on April 24 at the Royal Lancaster Hotel in Hyde Park, London, winners in a number of general and specific security categories will be announced.

Press release:

< <http://www.net-security.org/text/press/987516933,50154,.shtml> >

MERILUS COLLABORATES WITH RSA SECURITY - [17.04.2001]

Merilus, Inc., a leader in digital security innovation, announced that it has joined the RSA Security's RSA Secured Partner Program to support interoperability between Merilus GateKeeper products and RSA SecurID authentication and RSA BSAFE encryption technology. As part of the program, the Merilus GateKeeper product has been awarded both the "RSA Secured RSA SecurID Ready" certification and "RSA Secured RSA BSAFE enabled" certification signaling its compatibility with RSA Security's authentication and encryption software. The RSA Secured certification ensures that Merilus GateKeeper products are compatible with RSA Security's market-leading security products and technologies.

Press release:

< <http://www.net-security.org/text/press/987517015,43546,.shtml> >

SECUREINFO CORPORATION HIPAA SOLUTION - [18.04.2001]

Don Richey, Administrator of Guadalupe Valley Hospital and Keith Frederick, President and CEO of SecureInfo Corporation, will meet in Seguin, Texas to sign a Consulting Services Agreement; to help fulfill part of their mission statement "To serve, our community, patients...with the best possible healthcare...delivered efficiently..." Guadalupe Valley Hospital is dedicated to ensuring that the appropriate information privacy and information security measures are implemented to protect their patient's records. With the Information Security Expertise of SecureInfo Corporation, applying the privacy and security standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), they will take the steps necessary to keep their neighbor's medical records confidential and secure.

Press release:

< <http://www.net-security.org/text/press/987599218,10869,.shtml> >

INTRUSION PREVENTION FOR ITANIUM PROCESSOR - [19.04.2001]

Argus Systems Group, Inc., an international vendor of Internet security and intrusion prevention systems, today announced its pending support of Intel Itanium-based enterprise servers with its PitBull LX intrusion prevention systems. PitBull LX for the Itanium-based platform is to run on the Linux 2.4.x operating system kernel and is estimated to be available in Q3 2001.

Press release:

< <http://www.net-security.org/text/press/987599807,825,.shtml> >

'TOTAL ENTERPRISE SECURITY SERVICE' PRESENTED - [19.04.2001]

SecureInfo Corporation delivers a web-based security intelligence service, focusing on Information Systems Security and the protection of critical corporate data. Powered by over 300 years of combined security industry experience, TESS stands alone in the groundbreaking Security Intelligence for Business Continuity (SI4BC) category of security products.

Press release:

< <http://www.net-security.org/text/press/987679170,57137,.shtml> >

MAC CLIENT SUPPORT FOR INTEL VPN PRODUCTS - [20.04.2001]

PGP Security, a Network Associates company, today introduced Virtual Private Networking client software that will enable Intel VPN Gateways to support the Mac Operating System. PGP Security's award winning VPN client technology paired with Intel VPN Gateways provides Mac OS users with a secure encrypted tunnel to transfer information among partners, employees and customers across organizations and locations.

Press release:

< <http://www.net-security.org/text/press/987747653,17172,.shtml> >

GUARDENT JOINS INTERNET SECURITY ALLIANCE - [20.04.2001]

Guardent, Inc., the leading provider of security and privacy programs for Global 2000 organizations, today announced its full support of the Internet Security Alliance (ISA). Formally launched today, ISA assembles a roster of global leaders from multiple industry segments to create the most comprehensive, business-led network for up-to-the-minute threat reports, best practice standards, risk management strategies, certification and more.

Press release:

< <http://www.net-security.org/text/press/987747705,78850,.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

LT AUDITOR+

Blue Lance's LT Auditor+ is a Windows-based intrusion detection/audit trail security software solution. LT Auditor+ is designed to protect organizational assets accessible through NT and/or Novell networks. LT Auditor+ provides around-the-clock monitoring of network activity across the enterprise. LT Auditor+ is used to secure corporate assets against unauthorized access, fraud and theft.

Read more:

< <http://www.security-db.com/product.php?id=436> >

This is a product of Blue Lance, for more information:

< <http://www.security-db.com/info.php?id=97> >

GENUITY SITE SCAN

Genuity Site Scan Service can help a business strengthen its network perimeter security by periodically looking for potential weaknesses and generating recommendations about how to fix them. With Genuity Site Scan, organizations can reduce their susceptibility to Internet attacks.

Read more:

< <http://www.security-db.com/product.php?id=147> >

This is a product of Genuity, for more information:

< <http://www.security-db.com/info.php?id=27> >

QUADRASOLVE SECURE SERVER APPLIANCE

The QuadraSolve Secure Server Appliance ships with the easy to use, browser based remote administration tool -RSAM, making configuration and management simple. Setting up the QuadraSolve for Web hosting can be done in minutes. These servers are razor-thin when it comes to form-factor...if you're an ISP, you can squeeze 41 of these into a single data center cabinet, providing long term cost savings on that real estate.

Read more:

< <http://www.security-db.com/product.php?id=253> >

This is a product of LinuxSolve, for more information:

< <http://www.security-db.com/info.php?id=47> >

Featured article

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

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

STARTING POINTS OF A SECURE LINUX SYSTEM by Aleksandar Stancin

Here we go again. After some time has passed, I decided to write another article concerning some overall security aspects of installing and running linux, and as you can see it's connected to the very first one 'Securing a default linux installation' and makes a good reading companion to it. To keep it short and simple, here are some good pointers to enhancing your system's security. But remember, there's no absolute security, so keep your eyes open, subscribe yourself to good sec-related mailing lists, and keep your software up-to-date.

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

Security Software

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

ELDOS KEEPER 2.5.4

EldoS Keeper is designed to keep all your passwords and account-related information in secure, encrypted files so that you don't need to remember or write down the information. The only thing you need to remember is the password to the file where all the information is stored. EldoS Keeper keeps all records in a hierarchical form, allowing you to organize the data as you like. Version 2.54 adds password expiration tracking.

Info/Download:
< <http://www.net-security.org/various/software/988018687,61436,windows.shtml> >

SUBSEVEN: FIREWALL 1.0

From the developer: "This is a remarkable trojan blocker, and fake server. If you are being hacked using Subseven then go for this program. It has many features. Including chatting to the client. This is a must download for internet security. You can even sometimes preprogram the ports to stop other trojans

like T3000 etc."

Info/Download:

< <http://www.net-security.org/various/software/988018773,18730,windows.shtml> >

Defaced archives

[16.04.2001]

Original: <http://www.xerox.com.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/16/www.xerox.com.cn/>

OS: Windows

Original: <http://wwwgps.incra.gov.br/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/16/wwwgps.incra.gov.br/>

OS: Windows

Original: <http://www.systematics.co.il/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/16/www.systematics.co.il/>

OS: Windows

Original: <http://office.lefcobank.ru/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/16/office.lefcobank.ru/>

OS: Linux

Original: <http://www.governmentclub.org/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/16/www.governmentclub.org/>

OS: Windows

[17.04.2001]

Original: <http://www.carlsberg-beer.co.kr/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/17/www.carlsberg-beer.co.kr/>

OS: Windows

Original: <http://esenler-bld.gov.tr/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/17/esenler-bld.gov.tr/>

OS: SCO

[18.04.2001]

Original: <http://audiology.meei.harvard.edu/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/18/audiology.meei.harvard.edu/>

OS: Windows

Original: <http://crnet.mgh.harvard.edu/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/18/crnet.mgh.harvard.edu/>

OS: Windows

Original: <http://www.puma.co.jp/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/18/www.puma.co.jp/>
OS: Windows

Original: <http://www.nato.lv/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/18/www.nato.lv/>
OS: Windows

[19.04.2001]

Original: <http://www.microsoft.be/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/19/www.microsoft.be/>
OS: Windows

Original: <http://www.ericsson.com.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/19/www.ericsson.com.tw/>
OS: Windows

Original: <http://www.cybernanny.net/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/19/www.cybernanny.net/>
OS: FreeBSD

Original: <http://www.jenniferaniston.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/19/www.jenniferaniston.com/>
OS: Windows

Original: <http://www.melgibson.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/19/www.melgibson.com/>
OS: Windows

[20.04.2001]

Original: <http://www.emicrosoft.org/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/20/www.emicrosoft.org/>
OS: Windows

Original: <http://www.poderjudicial.gov.bo/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/20/www.poderjudicial.gov.bo/>
OS: Linux

Original: <http://www.chinaconsulatechicago.org/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/20/www.chinaconsulatechicago.org/>
OS: Windows

Original: <http://www.microsoft.com.gr/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/20/www.microsoft.com.gr/>
OS: SCO

Original: <http://www.hackers.com.mx/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/20/www.hackers.com.mx/>
OS: Linux

[21.04.2001]

Original: <http://molbio.princeton.edu/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/21/molbio.princeton.edu/>
OS: Windows

Original: <http://www.fellows.lanl.gov/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/21/www.fellows.lanl.gov/>
OS: Windows

Original: <http://www.quantum.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/21/www.quantum.com/>
OS: Windows

Original: <http://www.e-net.com.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/21/www.e-net.com.tw/>
OS: Windows

=====
Advertisement - 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>
=====

Questions, contributions, comments or ideas go to:

Help Net Security staff

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