

HNS Newsletter
Issue 54 - 12.03.2001
<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: 2014

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Security software
- 5) Defaced archives

General security news

DEMONIZING CRYPTOGRAPHY

Judging from recent headlines, one would think cryptography is responsible for all current evils, from child pornography to global terrorism. But is it really something to fear?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixinsider.com/unixinsideronline/swol-02-2001/swol-0223-unixsecurity.html>

HACKING EXPOSED REVIEW

If you spend enough time with Hacking Exposed, you could probably learn enough to start hacking networks yourself, although anyone else who has the book could probably learn enough to stop you. The fact is, if you really want to protect your network, you'll need more information than any one book can hold. But if you want a head start on keeping your network safe, make sure Hacking Exposed is on your bookshelf.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/books/casad/0102Hackex.shtml>

BUSH FORWARDS CLINTON INFRASTRUCTURE SECURITY REPORT

The Bush administration has forwarded to Congress a report on the Clinton administration's efforts to protect the nation's most critical computer systems from cyber-attack. The 200-page study was completed more than a week before Bill Clinton left office, but never was signed by Clinton or forwarded

to Congress, as required by law.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/01/03/05/news11.html>

SHOCKS WITH PHONE BILLS

Annette Leech received quite an unpleasant surprise when she was informed that \$700 of calls had been rung up on her phone in a single afternoon. Watch out what are you downloading, because there are lot of programs that dial sex lines through your computer.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.smh.com.au/news/0103/05/national/national2.html>

VIERIKA WORM

F-Secure has issued a level two alert to users of its Radar virus alerting service this morning. The firm has warned about a visual basic worm called Vierika, which is known to be circulating "in the wild." As usual with VBS viruses, F-Secure said that this worm spreads like LoveLetter. The firm said it consists of two different script parts: one that arrives in an MS-Outlook message as an attachment and another that is available on a Web site.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/162695.html>

SURVEY: BREACHES DRIVE SECURITY UPGRADES

A major security breach within a company is the single greatest catalyst for effecting increased security measures across that organization, according to the results of a recently released survey from IDC. Other big drivers of increased security measures include the growth in Internet usage and the trend toward mobile computing, according to IDC. A majority of the 1,000 companies that responded to the survey identified viruses as the most common security problem, with 90% saying they had been hit by a virus. The other most common security problem was unauthorized use of system resources and data.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/stories/0,1199,NAV47-68-84-88_STO58255,00.html

CHECK POINT FIREWALL-1 ON LINUX, PART TWO

This article is the second in a series of three by SecurityFocus writer David "Del" Elson that looks at Check Point Firewall-1 for Linux. The first article consisted of a brief introductory overview of Firewall-1, and a discussion of installation, post-installation tasks, as well as single and multi-system installations. This installment will cover Firewall-1 concepts such as network objects, firewall rules, address translation rules, and NAT, as well as features and limitations of Firewall-1. The final article will then discuss aspects of Firewall-1 such as file and directory layout, rulesets, migrating existing Firewall-1 installation to Linux, and back-up and standby configurations.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/checkpoint2.html>

SQL 7.0 SECURITY MODES COVERED

In this article, Alexander Chigrik talks about two security modes (authentication modes) in SQL Server 7.0.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.swynk.com/friends/achigrik/SQL70SecurityModes.asp>

FBI ROOTS OWN SYSTEMS TO FIND SPY'S BACKDOOR

The FBI is systematically searching for evidence that suspected double agent Robert Hanssen, who has computer programming skills, compromised systems at the Bureau and/or the State Department with some manner of malicious backdoor. "The jury is still out as to what he was able to do," the official is quoted as saying. But "because of the possibilities, we've got to take a look." Hanssen had the highest security clearance, which gave him access to extremely sensitive data. The FBI fears that he might have enabled Russian spies to access secure systems used by the FBI, State and other agencies.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17359.html>

CREDIT CARD INFO STOLEN FROM BIBLIOFIND?

After Bibliofind web site got defaced past month, internal investigation showed that attacker(s) had access to Bibliofind server from October 2000 and February 2001. Company's representative said all 98,000 customers will be notified of the incident via e-mail.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/03/05/bibliofind/index.html>

A TOOL FOR COLD MIRRORING OF SOLARIS SYSTEM DISKS

Minimum downtime and prevention of data loss is important for most system administrators. The traditional solution is to use backups or RAID to cover for disk failures. We describe an alternative for "cold mirroring" of system disks - it mounts a spare disk, copies files to the spare, installs a boot block and copies over a new vfstab. This creates a fully updated bootable spare disk. The administrator is notified of success/failure by syslog or email. This tool, called mirror_boot.sh, has been tested on several Solaris versions.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/coldmirroring20010306.html>

TOP 50 THINGS TO KNOW TO PASS SAIR EXAM 101

As I mentioned last month, you must pass four Sair exams to become a Linux Certified Administrator (LCA). One of the four exams is the Installation and Configuration 101 exam; passing this exam will earn you the designation of Linux Certified Professional (LCP). All of the Sair exams are available through Prometric testing centers. The following is a list of 50 key points to know for Exam 101. There is some overlap between the topics listed here and those I mentioned for the LPI 101 and 102 exams, due to the fact that they are competing certifications on the same topics.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.unixreview.com/columns/dulaney/0103sair.shtml>

SECURITY CONSULTANTS TO BE LICENSED

IT security consultants could soon join wheel-clampers and bouncers in having to apply for licences. The UK government's Private Security Industry

Bill proposes the creation of an authority to set standards of conduct and training for consultants, and to carry out inspections. The Security Industry Authority would check a consultant's background for any criminal record before issuing a licence. It would also keep a public register, and establish a voluntary body of approved contractors.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1118593>

NEW ZEALAND PHREAKING CASE

Borislav Mistic arrived in New Zealand in April 1998 from Yugoslavia and a year later was granted refugee status. He was convicted on two counts of fraud and one count of forgery involving the use of a piece of "blue boxing" software to make 80,000 minutes of international calls using Telecom's Home Country Direct service. There are debates over there regarding whether he did anything wrong according to the New Zealand law.

Link:

<http://www.nzherald.co.nz/storydisplay.cfm?storyID=175646&thesection=technology&thesubsection=general>

GERMANY SKEPTICAL ON US PLANS

German industry and the German government responded with skepticism to the news of US plans to build a national defense shield, or firewall, against attacks on data networks.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.handelsblatt.com/hbiwwangebott/fn/reihbi/sfn/buildhbee/cn/bp_artikel_e/strucid/PAGE_201098/pageid/PAGE_201098/docid/391343/SH/0/depot/0/index.html)

[bin/news.cgi?url=http://www.handelsblatt.com/hbiwwangebott/fn/reihbi/sfn/buildhbee/cn/bp_artikel_e/strucid/PAGE_201098/pageid/PAGE_201098/docid/391343/SH/0/depot/0/index.html](http://www.handelsblatt.com/hbiwwangebott/fn/reihbi/sfn/buildhbee/cn/bp_artikel_e/strucid/PAGE_201098/pageid/PAGE_201098/docid/391343/SH/0/depot/0/index.html)

EMAIL SNOOPING CODE OF PRACTICE DELAYED

The Data Protection Registrar's code of practice for surveillance in the workplace has been delayed due to the large number of responses from a public consultation. The code of practice is vital for clarifying what employees and employers are entitled to do in the workplace following several pieces of new legislation. The controversial and flawed RIP Act opens up the possibility of widespread email and phone surveillance. But this has also to tie in with the Human Rights Act, which enshrines the right to reasonable privacy, and the Data Protection Act, which insists that data is recovered "in a fair and proportionate manner".

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17365.html)

[bin/news.cgi?url=http://www.theregister.co.uk/content/8/17365.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17365.html)

TCP WRAPPERS: PART 2

In the second part of our series on TCP Wrappers, we look at its various features, implementation and configuration.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/3768/>

CARNIVORE, CYBERCRIME TAKE PRIME TIME

Carnivore, cryptography and cybercrime are just a few of the topics on tap this week at the Computers Freedom and Privacy Conference 2001 concerning recent developments in Internet policy and civil liberties. The conference will feature a forum for privacy watchdogs, free-speech activists and human-rights specialists to discuss how the Internet is changing society.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2692921,00.html>

NAKEDWIFE VIRUS HITS U.S. MILITARY, COMPANIES

A virus advertising itself as an e-mailed photo of someone's wife has started infecting computers in Europe and the United States and may have started spreading from the U.S. military. Four different antivirus software companies have reported that at least 68 organizations have computers infected by the virus.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-201-5041693-0.html>

WHY HOTMAIL USERS GET SO MUCH SPAM

Hotmail has come under criticism for placing its subscribers' email addresses on a public Internet directory site when they sign up for the service, making them easy prey for spammers, something that has got under the skin of privacy activists. Unless users opt-out by checking a box on Hotmail's registration form, their addresses can rapidly enter spammers' databases, as Infospace's privacy protection methods can be bypassed using a number of methods.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17379.html>

POWER GRIDS COULD BE VULNERABLE TO "HACKERS"

Nationwide rolling blackouts could have a devastating impact on the economy, but experts also fear that the stress being placed on the nation's power grid could make it more susceptible to disruptions from hackers. In California's Silicon Valley, large Internet data centers have been blamed for stressing the region's power grid beyond what its Korean War-era design can handle. Now, other states, including Oregon, Utah and Washington, are preparing for possible rolling blackouts.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/03/06/power.hackers.idg/index.html>

THE GREAT SECURITY DEBATE: LINUX VS. WINDOWS

Microsoft operating systems have often been attacked for their vulnerability, but the perception that the software titan's systems are insecure is changing as the company shores up its servers and applications. Meanwhile, supposedly stronger Unix and Linux systems have suffered security breaches of their own.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsfactor.com/perl/story/7907.html>

HACKER GROUP FINDS FAULTS IN CRACK CHALLENGE

Hacker advocacy group 2600 Australia has called on a Perth company to honor its promise to donate \$US1 million to charity after its network security device remained uncracked after a 30-day public trial. 2600 Australia yesterday

criticised the company's decision to move the cracking challenge into a second phase, which was to have launched on the company's website.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.it.fairfax.com.au/breaking/20010307/A27390-2001Mar7.html)

[bin/news.cgi?url=http://www.it.fairfax.com.au/breaking/20010307/A27390-2001Mar7.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.it.fairfax.com.au/breaking/20010307/A27390-2001Mar7.html)

SECUREWAVE - STUFF MS SHOULD HAVE DONE

"Like many people, I use Microsoft products on a regular basis, but having spent as much or more (probably more) time in Unix, I find certain things frustrating. In the Unix world, I take for granted the ability to set permissions on files and devices. While NT and 2000 have file permissions, you cannot easily restrict users' access to communications ports and removable media, for example. I also want to be able to restrict what users can and cannot run. There are a number of ways to do this in Unix, with varying degrees of difficulty to implement and of effectiveness."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010307.html)

[bin/news.cgi?url=http://securityportal.com/closet/closet20010307.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010307.html)

ANTI-VIRUS COMPANY BLASTS MEDIA FOR SCARE TACTICS

Susan Orbuch, spokesperson for Trend Micro, told Newsbytes misinformation about viruses is more dangerous than the bugs themselves. "There is a vast body of knowledge and folklore out there, much of which is incorrect," said Orbuch. "The end user is constantly exposed to misinformation and myths by the media and by popular fiction such as movies, TV and novels."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/162786.html)

[bin/news.cgi?url=http://www.newsbytes.com/news/01/162786.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/162786.html)

RUNNING SNORT ON IIS WEB SERVERS PART 2

Snort is a rule-based intrusion detection system that monitors network traffic by applying rules based on known attack signatures. However, in addition to guarding against known attacks, it is vital that an IDS be able to detect new or lesser-known exploits. In this article, SecurityFocus writer Mark Burnett introduces three strategies that will enable administrators to set up Snort to detect new or obscure exploits. These strategies include: monitoring outgoing traffic, establishing command-based rules and watching for traffic from online scanning sites.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/iis/mssnort2.html)

[bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/iis/mssnort2.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/iis/mssnort2.html)

ESCAN CONTENT CHECKING

eScan is a comprehensive Content Security and Traffic Scanning software package that checks the content in the e-mails, the attachment files and all the web pages. The checks are made for viruses, restricted words & phrases and embedded objects such as Java applets etc. before these reach the recipient.

Link: <http://www.security-db.com/product.php?id=630&cid=141>

DESCRAMBLE THAT DVD IN 7 LINES

Descrambling DVDs just got even easier, thanks to a pair of MIT programmers. Using only seven lines of Perl code, Keith Winstein and Marc Horowitz have created the shortest-yet method to remove the thin layer of encryption that is designed to prevent people - including Linux users - from watching DVDs without proper authorization.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,42259,00.html>

CARNEGIE MELLON AND EIA JOIN FORCES

The Electronic Industries Alliance (EIA) has formed a new alliance with the nation's top federally funded computer security group in an effort to help companies evade computer security threats online. The new partnership, dubbed the Internet Security Alliance, will draw upon the collaborative efforts of EIA member companies and computer security experts at Carnegie Mellon's Software Engineering Institute in Pittsburgh, the same unit that hosts the university's CERT Centers, a research and development organization sponsored by the Department of Defense.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/162845.html>

MITNICK: IDENTITY THEFT EASY AS PIE

Thanks to lame online security measures, stealing an individual's identity is like taking candy from a baby, said Kevin Mitnick. Passwords, user names and other data used by financial institutions and utility companies to verify identity, such as an account holder's Social Security number, driver's license information and mother's maiden name, are readily accessible in myriad databases on the Web, according to Mitnick.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/01/03/07/news6.html>

URL, URL, LITTLE DO WE KNOW THEE

Today we will look closer at URLs and the associated security implications. "Interesting" ways of using them have been known by spammers for a while, but now the KB spoof and the February issue of Crypto-Gram have made the Internet community more aware of what URLs can do.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/urlurl20010307.html>

ZEN AND THE ART OF BREAKING SECURITY - PART II

There are cases in which "gentle" techniques like timing or power analyses are not enough to fulfill the attacker's goal. Or the goal itself is not to break the protection scheme but to break through it, to the end target the mechanism is protecting, in a modern reenactment of Alexander the Great's "solution" to the Gordian knot. Enter failure-inducing attacks, in which the technique is to induce a failure in the very protection mechanism itself.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/zenandsecurity20010308.html>

NSA AND FBI BIG WINNERS AT BIG BROTHER AWARDS

The great and the good, when it comes to privacy invasion, have been "honoured" for their efforts to mess up life for the rest on us online. Privacy

International last night handed out "Big Brother" awards to government agencies, companies and initiatives which have done most to invade personal privacy. The National Security Agency, the US government's signals intelligence arm, took a lifetime menace award for "clipper, Echelon and 50 years of spying". In a separate category, the FBI's Carnivore email surveillance system was judged the most invasive proposal of the year.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17428.html>

FEDS ESCALATE WARNING ABOUT E-COMMERCE HACKS

The federal government's central computer-crime bureau reported that there is an ongoing and organized series of hacker attacks against e-commerce Web sites that has resulted in the theft of more than 1 million individual credit-card numbers. The National Infrastructure Protection Center said it has been working with the Federal Bureau of Investigation and the United States Secret Service for several months on the investigation and has identified more than 40 victim sites in 20 states.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2694098,00.html>

LEVY RECOUNTS THE HISTORY OF PUBLIC KEY CRYPTOGRAPHY

What are the roots of cryptography, and how has it evolved over the last 30 years? In this month's Bill's Bookshelf, Bill Rosenblatt reviews Steven Levy's new book on the history of public key cryptography, and finds it to be a balanced and engaging work.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunworld.com/unixinsideronline/swol-03-2001/swol-0302-bookshelf.html>

DIFFERENT APPROACH TO INTRUSION DETECTION

A security firm has put together two intrusion detection products to create technology it says takes a different approach to defending against hack attacks. CentraxICE, from security integrator Articon-Integralis, is positioned as a product which provides "defence in depth" from hack attacks beyond that offered by firewalls. It is designed to defend against packet floods - attempts to break into systems by bombarding an organisation's Web server with traffic and thereby overwhelming an organisation's defences.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17451.html>

UNCOVERING THE SECRETS OF SE LINUX: PART 1

In an uncharacteristic move, the U.S. National Security Agency recently released a security-enhanced version of Linux - code and all - to the open source community. This dW-exclusive article takes a first look at this unexpected development - what it means and what's to come - and delves into the architecture of SE Linux.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www-106.ibm.com/developerworks/library/s-selinux/>

MICROSOFT CO-OPTS OPEN SOURCE APPROACH

In a major extension of corporate policy, Microsoft has quietly started a program to provide selected large enterprise customers with copies of the source code for Windows 2000 (Professional, Server, Advanced Server and Data Center), Windows XP (released betas) and all related service packs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-201-5067896-0.html>

LAWYERS WITH HACKING SKILLS

With online and other various computer attacks against companies becoming increasingly common, corporate lawyers are arming themselves with new technical skills. "Ultimate Hacking: Hands On," a new crash course offered by the security-consulting firm Foundstone, will teach lawyers about common cybercrimes by re-enacting them in the classroom. Lawyers will come out of the course a bit more dangerous than when they walked in. Among the new skills they'll acquire is the ability to create a backdoor into a company's system using a remote-access Trojan, an application that allows crackers to gain access to restricted networks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,42278,00.html>

CRYPTOGRAPHY TOOLS: ARE THEY REALLY ONLY FOR CROOKS?

"Are there crypto success stories out there? I suspect that the kinds of shops using crypto are also the kinds of shops that don't talk about their work, but I hope some of you will write and tell me that crypto is working for your company, and how so. Until I'm convinced otherwise, I have to stick with the position that crypto is just more trouble than it's worth, and that it's likely to lull you into a false sense of security."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/op/xml/01/03/12/010312opswatch.xml>

EU ENCRYPTION SYSTEM NOT BROKEN

Paranoia is alive and well at the European Union Commission, which has been forced to officially deny its encryption system has been compromised by the NSA. Fears of eavesdropping by the ultra-secretive US spy agency grew out of comments by a Commission employee, Briton Desmond Perkins, who told a EU Parliamentary committee of regular but unsuccessful attempts by the NSA to crack the Commission's encryption system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17492.html>

Security issues

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

TROJANED REALITY FUSION APPLICATION

The executable rfupd.exe included in the Reality Fusion products bundled with many popular cameras sends data to 204.176.10.168 port 80 every time you use the app, reboot your computer or change configuration.

Link: <http://www.net-security.org/text/bugs/983755970,25167,.shtml>

SLIMSERVE HTTPD DIRECTORY TRAVERSAL

it is possible to view dir. and (download) files outside of the wwwroot directory.

Link: <http://www.net-security.org/text/bugs/983755986,60952,.shtml>

BROKER FTP SERVER 5.0 VULNERABILITY

Users can break out of their root directory and list directories. Depending on the priv. you have other commands like delete maybe executed outside of the home. directory.

Link: <http://www.net-security.org/text/bugs/983756002,47106,.shtml>

REMOTE BUFFER OVERFLOW IN POST-QUERY

The overflow condition is *very* easily exploitable, since the code actually supplies the pointer to the exploit code itself, odd as it may seem. The pointer thusly does not need to be second-guessed at all, making life much easier for crackers.

Link: <http://www.net-security.org/text/bugs/983838961,73107,.shtml>

VULNERABILITIES IN CURRENT IRCD'S TKSERV

There are 3 major bugs in the current IRCd distribution (as used on the IRCnet for example). The included service daemon 'tkserv' (tkserv.c v1.3.0 and all previous versions) suffers from:

- a) remote exploitable buffer overflow while querying tklines
- b) memory leak due to strdup'ing a string and not freeing the mem
- c) format string bug while reading the ircd's config file

Link: <http://www.net-security.org/text/bugs/983839093,38311,.shtml>

SUSE LINUX - CUPS UPDATE

A SuSE-internal security audit conducted by Sebastian Krahmer and Thomas Biege revealed several overflows as well as insecure file handling. These bugs have been fixed by adding length-checks and securing the file-access.

Link: <http://www.net-security.org/text/bugs/983840455,45873,.shtml>

DEBIAN LINUX - SUDO BUFFER OVERFLOW

Todd Miller announced a new version of sudo which corrects a buffer overflow that could potentially be used to gain root privileges on the local system. This bugfix has been backported to the version which was used in Debian GNU/Linux

2.2. The most recent advisory covering sudo missed one architecture that was released with 2.2. Therefore this advisory is only an addition to DSA 031-1 and only adds the relevant package for the powerpc architecture.

Link: <http://www.net-security.org/text/bugs/983880197,9394,.shtml>

DEBIAN LINUX - REMOTE DOS IN PROFTPD

In Debian Security Advisory DSA 029-1 we have reported several vulnerabilities in proftpd that have been fixed.

Link: <http://www.net-security.org/text/bugs/983880227,72205,.shtml>

DEBIAN LINUX - MGETTY UPDATE

In Debian Security Advisory DSA 011-1 we have reported insecure creation of temporary files in the mgetty package that have been fixed.

Link: <http://www.net-security.org/text/bugs/983880279,18936,.shtml>

DEBIAN LINUX - PROFTPD UPDATE

The following problems have been reported for the version of proftpd in Debian 2.2 (potato):

1. There is a configuration error in the postinst script, when the user enters 'yes', when asked if anonymous access should be enabled. The postinst script wrongly leaves the 'run as uid/gid root' configuration option in /etc/proftpd.conf, and adds a 'run as uid/gid nobody' option that has no effect.
2. There is a bug that comes up when /var is a symlink, and proftpd is restarted. When stopping proftpd, the /var symlink is removed; when it's started again a file named /var is created.

Link: <http://www.net-security.org/text/bugs/983965297,39939,.shtml>

LINUX MANDRAKE - JOE UPDATE

The joe text editor looks for configuration files in the current working directory, the user's home directory, and finally in /etc/joe. A malicious user could create their own .joerc configuration file and attempt to get other users to use it. If this were to happen, the user could potentially execute malicious commands with their own user ID and privileges. This update removes joe's ability to use a .joerc configuration file in the current working directory.

Link: <http://www.net-security.org/text/bugs/983965343,54664,.shtml>

DEBIAN LINUX - SGLM-TOOLS PROBLEM

Former versions of sgml-tools created temporary files directly in /tmp in an insecure fashion. Version 1.0.9-15 and higher create a subdirectory first and open temporary files within that directory.

We recommend you upgrade your sgml-tools package.

Link: <http://www.net-security.org/text/bugs/984081490,22578,.shtml>

DEBIAN LINUX - ATHENA WIDGET REPLACEMENTS

It has been reported that the AsciiSrc and MultiSrc widget in the Athena widget library handle temporary files insecurely. Joey Hess has ported the bugfix from XFree86 to these Xaw replacements libraries. We recommend you upgrade your nextaw, xaw3d and xaw95 packages.

Link: <http://www.net-security.org/text/bugs/984081556,93503,.shtml>

DEBIAN LINUX - MIDNIGHT COMMANDER UPDATE

It has been reported that a local user could tweak Midnight Commander of another user into executing a random program under the user id of the person running Midnight Commander. This behaviour has been fixed by Andrew V. Samoilov. We recommend you upgrade your mc package.

Link: <http://www.net-security.org/text/bugs/984081612,94030,.shtml>

DEBIAN LINUX - MAN2HTML REMOTE DOS

It has been reported that one can tweak man2html remotely into consuming all available memory. This has been fixed by Nicolás Lichtmaier with help of Stephan Kulow. We recommend you upgrade your man2html package immediately.

Link: <http://www.net-security.org/text/bugs/984081653,45766,.shtml>

DEBIAN LINUX - EPERL BUFFER OVERFLOW

Fumitoshi Ukai and Denis Barbier have found several potential buffer overflow bugs in our version of ePerl as distributed in all of our distributions. When eperl is installed setuid root, it can switch to the UID/GID of the scripts owner. Although Debian doesn't ship the program setuid root, this is a useful feature which people may have activated locally. When the program is used as /usr/lib/cgi-bin/nph-eperl the bugs could lead into a remote vulnerability as well.

Link: <http://www.net-security.org/text/bugs/984081700,15344,.shtml>

PROBLEMS WITH CISCO AIRONET 340 SERIES

It is possible to view and modify the bridge's configuration via Web interface even when Web access is disabled in the configuration. This defect is documented as Cisco bug ID CSCdt52783. This defect is present in the following hardware models:

- * Aironet AP4500,
- * Aironet AP4800,
- * Aironet BR100,
- * Aironet BR500,
- * Cisco Aironet AIR-BR340

Link: <http://www.net-security.org/text/bugs/984081837,49416,.shtml>

INDEXU AUTHENTICATION BYPASS

INDEXU uses a web frontend to manage every database it uses. The admin section is located in /admin. When you login there it asks for a user name and password (defaults to admin/admin). Once you log in it sets a cookie with the following format:
host.where.indexu.is.installed TRUE / FALSE 1388494785 cooki e_admin_authenticated 1
This cookie will (or should be) deleted when the current session finishes, and is used to determine whether you are an admin or not.

Link: <http://www.net-security.org/text/bugs/984081986,83035,.shtml>

WEBSWEEPER INFINITE HTTP REQUEST DOS

The Websweeper application from Baltimore Technologies is vulnerable to a Denial of Service attack. Malicious usage can lead to the application crashing.

Link: <http://www.net-security.org/text/bugs/984082157,92183,.shtml>

VULNERABILITY IN NOVELL NETWORK

Novell Netware allows a user to log into a Novell Network by using a Printer Server as the username. By default, Novell Print Servers have blank passwords. In addition, Novell Print Servers do not have intruder detection capability as a user account would, so they are vulnerable to a brute force attack without risk of account lockout. When a Print Server is logged into as a User, the account will have the same rights as are assigned to the container that it resides in.

Link: <http://www.net-security.org/text/bugs/984150567,84290,.shtml>

LINUX MANDRAKE - SLRN UPDATE

A buffer overflow exists in versions of the slrn news reader prior to 0.9.6.3pl4 as reported by Bill Nottingham. This problem exists in the wrapping/unwrapping functions and a long header in a message might overflow a buffer which could result in execution of arbitrary code encoded in the message.

Link: <http://www.net-security.org/text/bugs/984331181,9246,.shtml>

DEBIAN LINUX - ZOPE UPDATE

This advisory covers several vulnerabilities in Zope that have been addressed.

Link: <http://www.net-security.org/text/bugs/984331233,25603,.shtml>

ZOPE SECURITY ALERT AND ZOPE HOTFIX

An issue has come to our attention (thanks to Randy Kern) that necessitates a Zope hotfix. Hotfix products can be installed to incorporate modifications to Zope at runtime without requiring an immediate installation upgrade. Hotfix products are installed just as you would install any other Zope product.

Link: <http://www.net-security.org/text/bugs/984331340,63840,.shtml>

Security world

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

CYLINK: AVAILABILITY OF ISDN ENCRYPTORS - [05.03.2001]

Cylink, a leading provider of e-business security solutions, announced the general availability in Japan and Europe of ISDN Basic Rate Interface and Primary Rate Interface (PRI) encryptors for applications including remote computing, video-conferencing, and LAN-to-LAN communications.

"These solutions mark an important step as we expand our presence in Japan and begin to penetrate the enormous market for ISDN encryption products in Europe," said William P. Crowell, President and CEO of Cylink.

"These two cost-effective solutions are powerful additions to our WAN family of encryptors.

Press release:

< <http://www.net-security.org/text/press/983755586,20362,.shtml> >

CYBERELAN NOW EVINCIBLE - [05.03.2001]

CyberElan, a leading developer of business-to-business (B2B) security solutions is now Evincible. The company's focus is unchanged, continuing to deliver scalable and comprehensive policy- centric security solutions that provide authorization, authentication, confidentiality, integrity, and non-repudiation capabilities to both Internet and wireless e-business applications. "The name 'Evincible,' which means 'demonstrable,' more closely reflects our mission and defines our purpose: enabling strong, clear and trustworthy e- business," said Vijay Takanti, Evincible Chief Executive Officer. "We've made great strides in identifying market needs, delivering our core products and developing and patenting new concepts in the last year. 'Evincible' further establishes a more immediate synergy with our current product direction and identity."

Press release:

< <http://www.net-security.org/text/press/983796069,12247,.shtml> >

BioNetrix and Netmarks Partner - [05.03.2001]

BioNetrix Systems Corporation, provider of the only authentication management platform that secures data, applications and transactions across the Internet and the enterprise, announced it has partnered with Tokyo-based integrator Netmarks, Inc. to launch the internationalized version of BioNetrix's industry-leading security platform for the Japanese market in the second quarter of 2001. The three-year deal marks BioNetrix's entry into the Japanese market, a key international target for the company. Netmarks will directly sell and market BioNetrix's Authentication Suite and engage other value-added resellers for reselling. In addition, Netmarks will provide support to localize the product for Kanji and professional services to integrate Japanese customer applications into the product.

Press release:

< <http://www.net-security.org/text/press/983806061,99115,.shtml> >

NORMAN RECEIVES CHECKMARK CERTIFICATION - [05.03.2001]

Norman Data Defense Systems announced that its award-winning anti-virus product, Norman Virus Control, has once again earned the Checkmark Certification from West Coast Labs, a globally recognized, independent research and test center. Norman Virus Control for Windows 98, Lotus Notes, NetWare, Windows 2000 Professional, and OS/2 have all attained Anti-Virus Checkmark Level One, making them among the highest quality and most reliable security products on the market capable of detecting all viruses in the wild.

Press release:

< <http://www.net-security.org/text/press/983806127,22863,.shtml> >

ANNOUNCING RSA SECURID CARD STUDIO - [05.03.2001]

RSA Security Inc., the most trusted name in e-security, announced RSA SecurID Card Studio, a cryptographic smart card personalization system that enables a single card to be programmed for network access, digital credentials, physical building access and corporate identification. RSA SecurID Card Studio is designed to enable organizations to deploy smart cards quickly and effectively throughout the enterprise by allowing them to securely personalize and manage the deployment of their smart cards.

Press release:

< <http://www.net-security.org/text/press/983806181,82825,.shtml> >

IPASS'S AND CERTICOM'S STRATEGIC ALLIANCE - [05.03.2001]

iPass Inc., a premier provider of global remote Internet access services, and Certicom, a leading provider of mobile e-business security, announced an alliance that will enable mobile professionals to easily and securely access corporate databases and applications from a handheld device anywhere in the world. The alliance includes joint sales and marketing initiatives, interoperability and compatibility testing, development roadmap coordination and the exchange of support, tools and training.

Press release:

< <http://www.net-security.org/text/press/983808678,6218,.shtml> >

ANTI-VIRUS VIDEO GAME FROM MCAFEE - [05.03.2001]

McAfee, a Network Associates business, debuted an Internet-based anti-virus video game that engages Value Added Resellers in an online competition against one another with the chance to win a \$500,000 grand prize. Developing the innovative game entitled "Virus Attack," McAfee has integrated the qualities of the Internet with interactive marketing and training to capture mind-share amongst the challenging reseller market. "McAfee is pleased to embark on this new online adventure with our resellers, building greater awareness of McAfee's industry-leading solutions," said Diane Seghposs, vice president of channel marketing for Network Associates. "This creative offering provides our VAR partners a wealth of knowledge to help enhance our competitiveness and customer loyalty within the channel."

Press release:

< <http://www.net-security.org/text/press/983808731,59333,.shtml> >

SAFEWEB CHOOSES IVEA'S CRYPTOSWIFT - [06.03.2001]

iVEA Technologies, a Rainbow Technologies company and a leading provider of high-performance security solutions for the Internet and eCommerce, announced that SafeWeb, a leading developer of online privacy and security solutions based in Oakland, has selected iVEA's CryptoSwift eCommerce accelerator to power secure transactions of secure Web content as well as optimize Web-server performance. SafeWeb's privacy technology allows Internet users to surf the

Web anonymously and protect themselves against intrusions into their online activities. By acting as an intermediary, SafeWeb encrypts all data transmitted between a user and a Web site. CryptoSwift accelerates the encryption process so SafeWeb users obtain fast and secure transactions for their online communications.

Press release:

< <http://www.net-security.org/text/press/983839393,91021,.shtml> >

INTERACTIVE WEEK ON E-SHOPLIFTERS - [06.03.2001]

As if business already isn't difficult, online retailers now are being ripped off by electronic price tag alteration, according to an article in the March 5 issue of Interactive Week. An estimated one-third of all shopping cart applications at Internet retailing sites have software holes that make them vulnerable to the price switching scam, Peggy Weigle, CEO of security software company Sanctum told the Internet's newspaper. For example, a major PC manufacturer sells a sleek new laptop for \$1,600, but the company's shopping cart software code can be manipulated to change the price to \$1.60. "Thieves are coming in the front door," Weigle said.

Press release:

< <http://www.net-security.org/text/press/983839480,50791,.shtml> >

EMED TECHNOLOGIES CHOOSES GUARDENT - [06.03.2001]

eMed Technologies, a leading provider of image management and web solutions for radiologists, has chosen Guardent, a premier provider of end-to-end digital security/privacy services, as eMed's trusted security and privacy advisor. eMed has contracted with Guardent to audit eMed's products and services for continuing compliance with the privacy and security standards put forth in the Health Insurance Portability and Accountability Act. "Our relationship with Guardent is just one of the many measures we have taken to ensure not only eMed's HIPAA compliance, but also the compliance of our customers who rely on our technology, Internet, and networking expertise," explains eMed Chief Executive Officer, Caren Mason. "This was no small investment for eMed, but it is a big demonstration of our commitment to patient confidentiality and the secure transmission of sensitive healthcare information."

Press release:

< <http://www.net-security.org/text/press/983839526,56929,.shtml> >

NEW SNIFFER CERTIFIED PROFESSIONAL PROGRAM - [06.03.2001]

Sniffer Technologies, a business unit of Network Associates, is setting a worldwide standard by introducing its IT certification program for network management called the Sniffer Certified Professional Program (SCPP). While meeting the industry's demand for network professionals with vendor-specific certification, the SCPP will identify IT professionals with first-class Sniffer-specific troubleshooting and protocol analysis skills to protect and optimize networks across the enterprise.

Press release:

< <http://www.net-security.org/text/press/983839594,24397,.shtml> >

SOPHOS: INFORMATION ON NAKED WIFE WORM - [07.03.2001]

Sophos, a world leader in corporate anti-virus protection, has reminded companies of the importance of safe computing practice in the wake of the latest virus to become widespread via email. The W32/Naked worm arrives as an attached executable file to an email entitled "Fw: Naked Wife" containing the text "My wife never look like that! ;-)". The virus is the latest in a long line to use social engineering in an attempt to lure users into activating it. Earlier viruses have pretended to be loveletters, pictures of Russian tennis players, and even the Pikachu Pokemon character.

Press release:

< <http://www.net-security.org/text/press/983964479,1538,.shtml> >

FIRST ANTI VIRUS FOR POSTFIX GATEWAYS - [07.03.2001]

Kaspersky Labs, an international data-security software-development company, introduces the beta-version of the world's first virus protection software for Postfix e-mail gateways. Since 1998, Postfix has been known as an alternative to the widely used Sendmail program. Postfix provides users with nearly the same capabilities, but it is more effective when processing e-mail, is easier to use and provides better security and management. These features have allowed Postfix to enter the top three of the most popular e-mail gateways for Unix -platforms in only two years.

Press release:

< <http://www.net-security.org/text/press/983964626,14579,.shtml> >

F-SECURE ANTI-VIRUS FOR FIREWALLS ON LINUX - [07.03.2001]

F-Secure Corporation, a leading developer of centrally managed security solutions for the mobile, distributed enterprise, today brought its acclaimed anti-virus firewall solution to the open source world. F-Secure Anti-Virus for Firewalls on Linux provides unsurpassed detection and disinfection of Internet borne viruses and malicious code passing through OPSEC CVP firewalls. As with other products in the F-Secure Policy Manager family, the anti-virus firewall solution operates under a company's established security policies, transparently to end-users. This means that policies can be enforced, administered, and monitored remotely without disrupting, or even being noticed by, a user.

Press release:

< <http://www.net-security.org/text/press/983964710,32251,.shtml> >

F-SECURE: ANTI-VIRUS PROTECTION FOR PALMS - [07.03.2001]

F-Secure, a leading provider of security for mobile, distributed enterprises, announced the release of its second generation anti-virus product and service for the Palm OS. F-Secure Anti-Virus for Palm OS provides protection against any known malware (viruses, trojans, etc.) on the Palm platform. The product offers on-device protection with continuous, automatic update service and technical support. It supports all Palm OS devices with OS 2.0 or later. "PDAs are no longer immune to security threats," said Chris Vargas, President of F-Secure Corporation. "There's no way to predict when the next virus will occur, but when it does, F-Secure users receive the antidote automatically and get the fastest possible protection for their devices."

Press release:

< <http://www.net-security.org/text/press/983964876,85849,.shtml> >

HACKERS AT LARGE 2001 CONFERENCE - [07.03.2001]

From August 9th until August 12th, the campus of the University of Twente will feature a congress that is unique in its kind: Hackers at Large, or HAL 2001. The congress expects to receive thousands of guests from all over the world and from many different disciplines to debate issues ranging from advanced technical issues regarding some obscure aspect of the Internet to easy-to-understand lectures on some of the dangers of the information society, as well as many, many other topics. But more than debate, the guests at HAL2001 take ample time to get on-line, relax, build and discuss cool stuff, and engage in good old analog interfacing.

Press release:

< <http://www.net-security.org/text/press/983965181,1660,.shtml> >

RAINBOW'S IKEY EARNS OPSEC CERTIFICATION - [08.03.2001]

The Digital Rights Management group of Rainbow Technologies, a leading provider of security solutions for the Internet and eCommerce, announced that its iKey 1000 workstation and network security authentication token has been certified by Check Point Software Technologies Open Platform for Security Alliance. OPSEC certification proves that Rainbow's iKey VPN Solution Series is interoperable with Check Point's industry-leading VPN-1 solution, an integral part of its Secure Virtual Network architecture. With OPSEC certification, Rainbow has integrated the iKey 1000 VPN Solution Series into the Check Point VPN-1 software to provide an easy-to-use, two-factor logon authentication when connecting from a remote location.

Press release:

< <http://www.net-security.org/text/press/984080768,72511,.shtml> >

IDC NAMES ISS WORLDWIDE LEADER IN IDS - [08.03.2001]

Internet Security Systems (ISS) was officially recognized by International Data Corporation (IDC) as the worldwide leader in the Intrusion Detection and Vulnerability Assessment (IDnA) market according to a recent market-share report (Gaining control over the infrastructure: Intrusion Detection and Vulnerability Assessment). IDC reports that ISS' security software solutions have continued to gain momentum in the areas of host- and network-based vulnerability assessment and intrusion detection, capturing 30 percent of the worldwide IDnA market, the number one ranking for 1999. This number increases to 34 percent worldwide when hardware revenues associated with Intrusion Detection purchases are excluded.

Press release:

< <http://www.net-security.org/text/press/984080961,95550,.shtml> >

DEUTSCHE BUNDESBANK USES RSA SECURID - [08.03.2001]

RSA Security Inc., the most trusted name in e-security, announced that the Deutsche Bundesbank will use its RSA SecurID authentication solutions to enable secure communication with the information and control module of the bank's new large-value euro payment system RTGS(plus) (Real Time Gross Settlement System). The Deutsche Bundesbank chose RSA Security for this new application based on the bank's experience as an existing RSA Security customer and because RSA Security solutions are already successfully implemented in numerous credit institutions throughout Germany and Europe. Additional factors in the decision-making process were the ease of use and scalability RSA Security's products are designed to deliver.

Press release:

< <http://www.net-security.org/text/press/984081064,87805,.shtml> >

BIOCONX DELIVERS ADVANCED SECURITY SOFTWARE - [0.03.2001]

BioconX, Inc., a developer of network security software that applies biometrics to safeguard network and application access, announces the release of version 3.0 of its software. "With 3.0, BioconX is even more adaptable and convenient for IT professionals seeking to fortify security and control their networks and applications," says Thor Christensen, chief executive officer of BioconX, Inc.

Press release:

< <http://www.net-security.org/text/press/984081193,52482,.shtml> >

MCAFEE RECEIVES ICSA ANTI-VIRUS CERT. - [08.03.2001]

McAfee, a Network Associates, Inc. business, announced that its Internet gateway anti-virus solution, WebShield SMTP, has received certification from ICSA Labs, a worldwide leader in security standards-setting for Internet connected companies. "Internet gateway virus protection is increasingly critical in maximizing virus protection in the corporate environment, and we are pleased to certify McAfee's WebShield SMTP gateway product,"

said Larry Bridwell, Content Security Programs Manager for ICSA Labs. "McAfee offers a high level of protection at the network perimeter with the WebShield product, fighting off the latest computer viruses, worms and malicious code."

Press release:

< <http://www.net-security.org/text/press/984081235,3518,.shtml> >

Security Software

All programs are located at:

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

CGIPROXY

CGIProxy is a Perl CGI script that acts as an Internet proxy. Through it, you can retrieve resources that may be inaccessible from your own machine. No user info is transmitted, so it can be used as an anonymous proxy. HTTP and FTP are supported. Options include text-only browsing (to save bandwidth), selective cookie and script removal, simple ad filtering, encoded target URLs, configuration by end user, and more.

Info/Download:

< <http://www.net-security.org/various/software/984396829,33976,linux.shtml> >

BLOWCRYPT

Blowcrypt is a file encryption software suite based around the blowfish algorithm. Blowfish comes with a graphical user interface (Tk front-end), but can also be used from the command line. The key length is currently set to 448 bits. It contains two perl scripts and two modules. Encrypt and decrypt are the perl scripts that manipulate the base programs. Next, are the base modules blowfish and RSA's md5 that do the actual encryption. Finally, there is a tk program, called tkblow. This GUI front-end to the perl scripts enables multiple selections of files for encryption and decryption.

Info/Download:

< <http://www.net-security.org/various/software/984397215,23610,linux.shtml> >

RASLOCK ME V1.0

RASLock Me allows you to set user-level security for Internet dial-up (RAS) connections. Using RASLock Me you can limit incoming and outgoing traffic, limit time online, and set allowed and denied time periods for any user. The program enhances the standard Windows security by allowing you to control

Internet access via modems. RASLock Me runs transparently in the background and is invisible to users. It automatically disconnects users that exceed allowed time or traffic.

Info/Download:

< <http://www.net-security.org/various/software/984397628,63510,windows.shtml> >

LOCKTIGHT V2.0

LockTight Security System lets you encrypt files by simply dragging and dropping them into the LockTight interface. You can mix encryption engines, keys, and passwords to protect your data.

Info/Download:

< <http://www.net-security.org/various/software/984398117,44778,windows.shtml> >

Defaced archives

[05.03.2001]

Original: <http://www.ncx.gov.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/05/www.ncx.gov.cn/>

OS: Solaris

Original: <http://directnews.net/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/05/directnews.net/>

OS: Linux

Original: <http://www.fujitsu.com.hk/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/05/www.fujitsu.com.hk/>

OS: Windows

Original: <http://tjfolio.tj.sc.gov.br/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/05/tjfolio.tj.sc.gov.br/>

OS: Windows

Original: <http://www.fiat.co.uk/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/05/www.fiat.co.uk/>

OS: Windows

Original: <http://www.chenzhou.gov.cn/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/05/www.chenzhou.gov.cn/>

OS: Solaris

Original: <http://www.sony.com.my/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/05/www.sony.com.my/>

OS: Windows

[06.03.2001]

Original: <http://www.quicktime.com.tw/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/06/www.quicktime.com.tw/>

OS: Linux

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

Defaced: <http://defaced.alldas.de/mirror/2001/03/06/www.crimebusters.org/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/03/06/www.audiofind.com/>

OS: Linux

Original: <http://www.linux.org.in/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/06/www.linux.org.in/>

OS: Linux

Original: <http://www.capnhq.gov/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/06/www.capnhq.gov/>

OS: Windows

Original: <http://www.linux.com.hk/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/06/www.linux.com.hk/>

OS: Linux

[07.03.2001]

Original: <http://kungfulinux.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/07/kungfulinux.com/>

OS: Linux

Original: <http://www.honda.com.mx/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/07/www.honda.com.mx/>

OS: Linux

Original: <http://www.hp.com.tw/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/07/www.hp.com.tw/>

OS: Windows

Original: <http://arts.endow.gov/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/07/arts.endow.gov/>

OS: Windows

Original: <http://goes2.gsfc.nasa.gov/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/07/goes2.gsfc.nasa.gov/>

OS: Windows

[08.03.2001]

Original: <http://epg.er.usgs.gov/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/08/epg.er.usgs.gov/>

OS: Windows

Original: <http://www.globalnews.it/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/08/www.globalnews.it/>
OS: Windows

Original: <http://www.linuxbsa.org/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/08/www.linuxbsa.org/>
OS: Linux

Original: <http://www.appeal.tcg.gov.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/08/www.appeal.tcg.gov.tw/>
OS: Unknown

Original: <http://www.fbi.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/08/www.fbi.com/>
OS: Windows

[09.03.2001]

Original: <http://www.ecorecycle.vic.gov.au/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/09/www.ecorecycle.vic.gov.au/>
OS: Windows

Original: <http://www.chcc.nsw.gov.au/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/09/www.chcc.nsw.gov.au/>
OS: Windows

Original: <http://www.bromley.gov.uk/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/09/www.bromley.gov.uk/>
OS: Windows

Original: <http://www.linuxkorea.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/09/www.linuxkorea.com/>
OS: Linux

Original: <http://www.chifeng.gov.cn/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/09/www.chifeng.gov.cn/>
OS: Windows

[10.03.2001]

Original: <http://www.mcdonalds.com.co/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/10/www.mcdonalds.com.co/>
OS: Windows

Original: <http://see.msfc.nasa.gov/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/10/see.msfc.nasa.gov/>
OS: Windows

Original: <http://www.scs.df.gov.br/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/10/www.scs.df.gov.br/>
OS: Windows

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>

<http://security-db.com>