

HNS Newsletter
Issue 59 - 16.04.2001
<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>

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

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

=====
GFI's Mail essentials for Exchange 2000 is now available!
It can protect Exchange 2000 from all kinds of email-borne threats, like viruses, dangerous attachments, email attacks, spam and offensive content.

Download your evaluation copy from:
<http://www.gfi.com/secdblanmesnl.shtml>

=====

General security news

CISCO SECURE PIX FIREWALL

The Cisco Secure PIX Firewall is the dedicated firewall appliance in Cisco's firewall family and holds the top ranking in both market share and performance. The Cisco Secure PIX Firewall delivers strong security and, with market-leading performance, creates little to no network performance impact. The product line enforces secure access between an internal network and Internet, extranet, or intranet links.

Link: <http://www.security-db.com/product.php?id=680&cid=152>

PORT NUMBERS 7001 THROUGH 65535

A port is a point of connection. In networking, a port acts as the door at each end of a connection through which client/server/peer programs transfer

information during a data exchange. Whenever a network program initiates activity with a remote system, a port is opened up, both locally and remotely, to allow the exchange to take place. Here are links to TCP/IP port lists, which are a valuable resource for anyone involved with firewall configuration or maintenance.

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

HACKERS WORK FROM WITHIN

A study of 1,238 companies, conducted by the KPMG consultancy, found that 90 percent of firms expected their e-commerce systems would be breached by hackers. But KPMG warned that most attacks would be carried out by members of staff. Norman Inkster, president of KPMG Investigation and Security, said studies by KPMG over the last decade had found that 70 percent of fraud was carried out by insiders. "Most security breaches are carried out by individuals who possess intimate knowledge of the systems which they are attacking," he added.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/14/ns-22143.html>

AUSTRALIAN HACKERS FACE JAIL TIME

"People who believe causing damage by hacking or spreading viruses to be trivial or even amusing activities are wrong. These are serious crimes in the 21st century and people can face up to 10 years in jail if convicted," State Attorney General Bob Debus said in a statement. The NSW Government has proposed amendments to the Crimes Act to include provisions covering cyberoffences. "The new offences are based on the latest international moves to fight cybercrime. They will ensure that NSW criminal laws keep pace with international technology and that appropriate penalties are in place," Debus said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2705803,00.html>

CONGRESS ADDRESSES CYBER SECURITY ONCE AGAIN

The security of the U.S. government's information technology (IT) systems is receiving renewed focus in the U.S. Congress. The House Oversight and Investigations Subcommittee April 5 heard testimony on efforts that various government agencies are taking to protect these systems. Subcommittee Chairman Billy Tauzin, a Republican Congressman from Louisiana, opened the session expressing concern about reports of vulnerabilities across the government. Tauzin specifically referred to a newly completed independent auditor's report of the Department of Health and Human Services which showed that electronic data processing systems were weakly controlled, leaving them exposed to a variety of potential problems.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://cipherwar.com/news/01/usgov_comp_sec.htm

SECURITY AUDITING TOOLS FOR THE MACINTOSH

"There really aren't any 'security' tools for the Macintosh to ensure secure passwords. Just lots of text files and reports by hackers on how it's insecure. We will review two programs created by hackers, which can be used for security purposes, and can be used by a hacker. The reason we are reviewing these hackers programs is to bring to light that you need to know the tools

that hackers are using to ensure your own security. Get the programs before the wrong people do and use them on your unsuspecting computers. We will review these programs from a system administrators' point of view."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securemac.com/secauditing.cfm>

CYPHERPUNK'S FREE SPEECH DEFENSE

Jim Bell took the witness stand in federal court on Friday to argue he was attempting to document illegal behavior, not stalk government agents. Bell described his electronic research last year - which the Justice Department says led federal agents to fear for their safety - as entirely lawful and said he never intended to hurt or threaten anyone. The 43-year-old chemist and entrepreneur freely admitted he bought motor vehicle databases and did Internet searches on the names of Treasury Department agents as part of his effort to uncover illegal surveillance by the U.S. government. Bell is charged with five federal counts of interstate stalking.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42909,00.html>

HACKERS TURN RACIST IN ATTACK ON HARDWARE SITE

PC motherboard specialist PC Chips has fallen victim to defacement in an attack that shows that hackers can be unthinking racists. The home page of the site, which runs Apache on a Red Hat Linux server, was replaced by a message from the 1i0n Crew, which contained in its headline the racist remark "Kill all the Japanese!".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/18181.html>

NEW VIRUS WRITTEN IN LOGO LANGUAGE

A virus that announces itself with lyrics from a song performed by a Belgiantechno dance band is written in programming language by Logotron, a educational software publisher, an anti-virus service said today. The proof of concept I-Worm.LogoLogic.A is the first-ever virus written using SuperLogo, said Medina, Ohio-based Central Command Inc. The language is used to train programming students in application development, the company said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/164290.html>

RSA SAYS DEMAND FOR SECURITY SERVICES STILL STRONG

RSA Security Inc. said that demand remains strong for its authentication and encryption services, despite fears over a slowdown in information technology spending that has battered the shares of many Nasdaq-listed security vendors.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.siliconvalley.com/docs/news/tech/037891.htm>

BRUCE SCHNEIER: 'WE ARE LOSING THE BATTLE'

Cryptographer Bruce Schneier reiterated his managed security services gospel in a talk here on the opening day of the RSA Security Conference. But if his message is really being heard, there should be general panic among CIOs in corporate America. "The future of Internet security is not very good," Schneier said. "New methods are being invented, new tricks, and every

year it gets worse. We are not breaking even. We are losing the battle."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2705973,00.html>

PGP WORKING WITH NSA ON SELINUX

A division of PGP Security has entered into a partnership with the National Security Agency and other partners to further develop the NSA's Security Enhanced Linux prototype. Under a \$1.2 million 2-year contract, the NAI Labs division of PGP Security will focus on research and development to improve the security of open-source operating system platforms, particularly Linux, PGP Security said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/01/04/09/010409hnselinux.xml>

COMPUTER FORENSICS

Numerous companies may be battenning down their hatches with this or that security tool, yet more than a few still experience payloads from viruses, breaches from script kiddies and data theft from internal employees. On the face of it, a cybercrime treaty that eases the investigative processes for police agencies around the world may be a move in the right direction, but for countless victims, just understanding what action they can take to determine how an assault on their networks happened at all is of more urgent concern.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.scmagazine.com/scmagazine/2001_04/cover/cover.html

MEET THE 'CYBER AVENGERS'

Kris Haworth pounded away at her keyboard, navigating a labyrinth of computer data in her search for evidence. The board of directors for a \$5 billion company suspected revenues were being inflated. It was up to Haworth to fish out incriminating e-mails thought to have been deleted.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/555451.asp>

DESIGNING SECURE NETWORKS

It has been asserted that advancements in software development have come about mainly as a result of the introduction of the software process model or software lifecycle. SecurityFocus writer Paul Innella argues that, in a similar manner, network security designers can benefit from using the principles of the software process model. In this article, the author outlines eight phases of the software process models as they apply to the design of a secure network.

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

INTRODUCTION TO DIGITAL SIGNATURES IN JAVA

In public key cryptography, there are two keys. One is used by the sender and is usually private. One is used by the receiver and is usually public. The sender uses the private key to encode a message or data, and the receiver uses the public key to decode the message. Digital signatures work just like public key cryptography. The signer encodes data with his own private key, and then anyone with his public key can decode it. This allows any receiver to verify

the source or signer of data as accurate and guarantee its integrity and authenticity.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://softwaredev.earthweb.com/java/sdjjavaee/article/0,,12396_630851,00.html

GERMAN THREAT RAISES INFOWAR FEAR

At least, that's the threat that Interior Minister Otto Schily has made, vowing the German government may resort to denial-of-service attacks as a way to shut down U.S. and other foreign websites that help German neo-Nazis. Condemnation of the plan was immediate. But as of Monday afternoon in Germany, Schily's office had reported no backtracking from his statement, which has been the focus of recent media attention in Germany.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42921,00.html>

ONLINE FRAUD WORRIES EBUSINESSES

Forty-six percent of global companies doing business online believe that online fraud is either a "somewhat" or "very" significant problem, according to a recent survey of 140 members of the Worldwide E-Commerce Fraud Prevention Network. Only 1 percent do not worry about it. The study found that 70 percent believe there are prevention tools that can keep e-fraud to a minimum.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.business2.com/content/research/numbers/2001/04/10/29756>

FREEDOM2SURF OFFERS FREE PRIVACY SUITE

Freedom2Surf, one of the UK's most advanced ISPs, today built on the security and privacy already offered to its users by announcing it is the first company in the UK to offer its subscribers free access to a range of privacy and security features with the Freedom 2.0 Internet Privacy Suite from Zero-Knowledge Systems. Freedom 2.0 will be made available to all new and existing Freedom2Surf subscribers as a free download for a limited time.

Link: <http://www.net-security.org/text/press/986894868,73460,.shtml>

NFR NETWORK INTRUSION DETECTION

NFR Network Intrusion Detection (NFR NID) is an intrusion detection system that unobtrusively monitors networks in real time for activity such as known attacks, abnormal behavior, unauthorized access attempts and policy infringements. Information associated with activity that may be suspicious is recorded and alerts raised as necessary.

Link: <http://www.security-db.com/product.php?id=688&cid=153>

THE SILENCE OF THE HACKED

Almost every day, Internet news sites break stories about newer and ever-more dangerous breaches in computer security. But unless the story involves a virus named after a good-looking tennis star, it probably won't make the national news. This worries Kevin Poulsen, a former hacker who now works as the editorial director of SecurityFocus.com. Poulsen said that because several of the biggest hacking stories don't make the headlines, the public is mostly ignorant about what's been hacked, and what companies are doing to bolster security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,42945,00.html>

SECURITY FLAW FOUND IN ALCATEL DSL MODEMS

The security problems could allow a hacker to bypass users' passwords and alter the devices, making them temporarily or permanently unusable, researchers said. A hacker also could potentially install code to gather unencrypted credit card information or read unencrypted e-mail messages, investigators said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1004-200-5567751.html>

GERMAN POL BACKTRACKS ON HACK

Germany Interior Minister Otto Schily has taken at least a half-step back from a threat to use denial-of-service attacks to shut down neo-Nazi websites in the United States and elsewhere. The statement Tuesday by Schily's spokesman was expected, given the furor in Germany and elsewhere over the idea of a government potentially getting into the hacking business. "It's wrong to talk about hacking," Schily spokesman Dirk Inger said, suggesting that media accounts had misinterpreted Schily's previous remarks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42961,00.html>

RUSSIAN HACKER RECRUITED BY AMERICANS

American diplomats in Moscow recruited a local hacker called 'Vers' to break into computers serving Russia's domestic security agency, the FSB, early this year, it was claimed yesterday.

Link:

<http://www.telegraph.co.uk/et?ac=000579381554028&rtmo=gjngwNku&atmo=99999999&pg=/et/01/4/11/whack11.html>

CRACKS HAPPEN

The various seminars and exhibits at the computer security show here occupy not only an entire wing of the Moscone Convention Center, but also the 15 movie theaters across the street at Sony's Metreon entertainment complex. The RSA Conference is huge; and its size is a testament to the fact that, given the increasing cost of computerized mischief, tech firms are starting to devote serious money to securing their data.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/culture/0,1284,42984,00.html>

A CHINESE CALL TO HACK U.S.

Chinese crackers are being encouraged to "hack the USA" in retaliation for the mid-air collision between a U.S. spy plane and a Chinese fighter jet which claimed the life of a Chinese pilot.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,42982,00.html>

MICROSOFT MAKES 'CLEAN BREAK' ON SECURITY POLICY

During his keynote speech at the RSA Security Conference, David Thompson, vice president for the Windows product server group, stressed that there has been a companywide focus on improving the security of Microsoft's products

over the last year, from the top of the organization down. "We've made a clean break with our past policy on security," said Scott Culp, security program manager at Microsoft. "We recognize that every piece of software has vulnerabilities and bugs. We have to deal with them."

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2706838,00.html)

[bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2706838,00.html](http://www.zdnet.com/eweek/stories/general/0,11011,2706838,00.html)

CARE AND FEEDING OF RPM

RPM is a very complex and powerful tool for building software packages. Blindly downloading and installing RPM's is of course very dangerous (this goes for installing software on any operating system). If you choose to build foreign RPM's on your machine then you should inspect the SPEC file for malicious commands and also verify the source code used and any patches. The good news is that verifying the origin of RPM's is relatively easy, and as the majority of your RPM's will likely come from trusted sources, you should not have too many problems. Lastly, with the use of scripts and triggers you can easily build RPM's that will notify you when installed (e.g. implement a command to send mail out so you know when someone has upgraded a machine), or properly clean up after themselves. Used properly, RPM is a very powerful tool.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010411.html)

[bin/news.cgi?url=http://securityportal.com/closet/closet20010411.html](http://securityportal.com/closet/closet20010411.html)

HACKER TOOLS AND THEIR SIGNATURES, PART ONE: BIND8X.C

This article is the first in a series of papers detailing hacker exploits/tools and their signatures. This installment will examine the Berkley Internet Name Domain exploit bind8x.c. The discussion will cover the details of bind8x.c and provide signatures that will assist an IDS analyst in detecting it. This paper assumes that the reader has some basic knowledge of TCP/IP and understands the tcpdump format.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ids/articles/bind8.html)

[bin/news.cgi?url=http://www.securityfocus.com/focus/ids/articles/bind8.html](http://www.securityfocus.com/focus/ids/articles/bind8.html)

ANTI-VIRUS WITH SENDMAIL AND FBSD

This is a very nice add on for ISPs or someone that wants to safeguard all email coming into their system from viruses. The following article will walk you through installing and setting up several programs, to get this project done.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.defcon1.org/html/Linux_mode/install-swap/anti-virus-sendmail.html)

[bin/news.cgi?url=http://www.defcon1.org/html/Linux_mode/install-swap/anti-virus-sendmail.html](http://www.defcon1.org/html/Linux_mode/install-swap/anti-virus-sendmail.html)

ALCATEL WORKING WITH CERT

In response to security issues raised by the San Diego Supercomputer Center Monday regarding certain Alcatel ADSL modems, the French communications equipment maker said that it is aware of vulnerabilities and is working with the CERT Coordination Center to resolve the problems. Alcatel also said that it is not aware of any instance where a Speed Touch Home ADSL modem user's device has been compromised due to the reported vulnerabilities.

Link: [http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/prod-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.internetnews.com/prod-news/article/0,,9_741871,00.html)
[news/article/0,,9_741871,00.html](http://www.internetnews.com/prod-news/article/0,,9_741871,00.html)

SECURITY FOR WEB DATABASE APPLICATIONS

If you're using a development tool like ColdFusion, ASP, or PHP, your application developers have probably unknowingly opened holes directly into your database that could wreak havoc on your system. Not obscure, difficult-to-exploit holes, but real big delete-everything-from-the-database kind of holes. Today, we're going to discuss how those security holes arise and more importantly, how to plug them.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://webreview.com/2001/04_13/developers/index02.shtml

MAKE SSH DO MORE

Presumably you have already installed SSH and are using it to securely log in to remote systems. However, most people simply connect via SSH, enter their passwords, and type away. They don't realize that SSH has advanced key management features that allow them to avoid having to retype their passwords; that its port-forwarding options can secure other, normally insecure, packages; and that they can employ little tricks in SSH that would make their lives easier.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.itworld.com/Comp/2384/LWD010410sshhttps/>

LINUX SECURITY MODULE INTERFACE

"One of the byproducts of the Linux 2.5 Kernel Summit was the notion of an enhancement of the loadable kernel module interface to facilitate security oriented kernel modules. The purpose is to ease the tension between folks (such as Immunix and SELinux) who want to add substantial security capabilities to the kernel, and other folks who want to minimize kernel bloat & have no use for such security extensions. We have started a new mailing list called linux-security-module. The charter is to design, implement, and maintain suitable enhancements to the LKM to support a reasonable set of security enhancement packages. The prototypical module to be produced would be to port the POSIX Privs code out of the kernel and make it a module. An essential part of this project will be that the resulting work is acceptable for the mainline Linux kernel."

Link: http://linuxtoday.com/news_story.php?itsn=2001-04-12-021-20-SC-KN

WAR DRIVING BY THE BAY

In a parking garage across from Moscone Center, the site of this year's RSA Conference, Peter Shipley reaches up though the sunroof of his car and slaps a dorsal-shaped Lucent antenna to the roof. "The important part of getting this to work is having the external antenna. It makes all the difference" says Shipley, snaking a cable into the car and plugging it into the wireless network card slotted into his laptop. The computer is already connected to a GPS receiver. He starts some custom software on the laptop, starts the car and rolls out. Shipley, a computer security researcher and consultant, is demonstrating what many at the security super-conference are quietly describing as the next big thing in hacking. It doesn't take long to produce results. The moment he pulls out of the parking garage, the laptop displays the name of a wireless network operating within one of the anonymous downtown office buildings: "SOMA AirNet."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/192>

EX-CYBERCOP: HACKERS NOT THE ONLY PROBLEM

Malicious intruders, corporate espionage and uneducated employees all contribute to make "network security" almost an oxymoron in today's wired world, four security experts agreed at the RSA Data Security Conference.

"It's not just the hackers who are the threats but all of us who are part of the problem as well," said Vatis, former executive director of the federal government's National Infrastructure Protection Center.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-5586254.html>

CAN MCVEIGH KILLING BE HACKED?

Security experts said it would be difficult, but not impossible, to intercept and decode the closed-circuit video of Timothy McVeigh's execution. The Justice Department won't say much about the measures it is taking to ensure that the pictures of the May 16 execution are not made public. Attorney General John Ashcroft kept his description of the transmission methods vague when speaking to reporters. "The broadcast will use the latest encryption technology integrated with state-of-the-art video-conferencing over high-speed digital telephone lines," Ashcroft said. "Federal regulations prohibit any recording of the execution. Therefore, any closed-circuit transmission will be instantaneous and contemporaneous." Security experts say Ashcroft was describing ISDN, short for Integrated Services Digital Network. ISDN lines can transmit data at least twice as fast as normal telephone lines, although the data travels through public phone networks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,43040,00.html>

CLOSED SOURCE IS MORE SECURE - MS

The head of Microsoft's security response team argued that closed source software is more secure than open source projects, in part because nobody's reviewing open source code for security flaws. "Review is boring and time consuming, and it's hard," said Steve Lipner, manager of Microsoft's security response center. "Simply putting the source code out there and telling folks 'here it is' doesn't provide any assurance or degree of likelihood that the review will occur."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/18286.html>

BADTRANS VIRUS FAILS TO SPREAD

A virus that monitors a PC's network connections and sends itself in response to any incoming e-mail has apparently failed to spread, despite, or because of, warnings issued by several major antivirus software makers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5081157,00.html>

EICAR TEST FILE

In 1996, the European Institute for Computer Antivirus Research (EICAR) developed the EICAR test file. The EICAR test file tests the functionality of antivirus software, by giving the antivirus software a chance to detect the EICAR file during antivirus scans. The test file may render a variety of results within various antivirus programs but is NOT a virus. All major antivirus software developers support the EICAR test file. If your antivirus software detects the EICAR test file it does NOT guarantee that it will

catch all malware. In fact, no single antivirus solution is able to block all malware. Thus, the EICAR test file, safe computing practices, and updated antivirus software are just a few of the tools that users will want to employ to lower the risk of malware infections.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/eicar20010413.html>

Security issues

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

RED HAT LINUX - NTPD REMOTE ROOT EXPLOIT

The Network Time Daemon (ntpd) supplied with all releases of Red Hat Linux is vulnerable to a buffer overflow, allowing a remote attacker to potentially gain root level access to a machine. All users of ntpd are strongly encouraged to upgrade.

Link: <http://www.net-security.org/text/bugs/986822554,64400,.shtml>

CALDERA - REMOTE ROOT EXPLOIT IN NTPD

Link: <http://www.net-security.org/text/bugs/986822600,4830,.shtml>

TALKBACK.CGI SECURITY VULNERABILITY

Talkback.cgi may allow remote users (website visitors) to view any file on a webserver (depending on the user the webserver is running on). Regard this URL:
<http://www.VULNERABLE-HOST.com/cgi-bin/talkback.cgi?article=../../../../../../../../etc/passwd%00&action=view&matchview=1>

This will display the /etc/passwd (if the webserver user has access to this file).

Link: <http://www.net-security.org/text/bugs/986899132,17397,.shtml>

DEBIAN LINUX - NTP UPDATE

Przemyslaw Frasunek reported that ntp daemons such as that released with Debian GNU/Linux are vulnerable to a buffer overflow that can lead to a remote root exploit. A previous advisory (DSA-045-1) partially addressed this issue, but introduced a potential denial of service attack. This has been corrected for Debian 2.2 (potato) in ntp version 4.0.99g-2potato2. We recommend you upgrade your ntp package immediately.

Link: <http://www.net-security.org/text/bugs/986899319,43520,.shtml>

SUSE LINUX - UPDATED XNTP PACKAGES

Link: <http://www.net-security.org/text/bugs/986899379,2605,.shtml>

PROGENY - MAILX BUFFER OVERFLOW

Mailx is a simple program to read and send e-mail. Mailx is installed setgid mail on Progeny and Debian systems. A buffer overflow in mailx allows for a local user to gain access to the mail group, which would allow that user to read and write to other mail spools. Debian resolved this problem by no longer shipping mailx setgid mail. Progeny has decided to use Debian's fix. This means that on mail systems that do not have world writable mail spools one will not be able to properly lock one's mailbox.

Link: <http://www.net-security.org/text/bugs/986899525,60483,.shtml>

VULNERABILITIES IN MULTIPLE FTP DAEMONS

Multiple FTP server implementations contain buffer overflows that allow local and remote attackers to gain root privileges on affected servers. These vulnerabilities are contingent upon the remote user having the ability to create directories on the server hosting the FTP daemon, with the exception of a few cases noted below. The vulnerabilities presented are all related to the use of the glob() function, and can be divided into the following two categories:

- glob() expansion vulnerabilities

User input that has been expanded by glob() can exceed expected lengths and trigger otherwise benign buffer mismanagement problems present in certain FTP daemons.

- glob() implementation vulnerabilities

Certain implementations of the glob() function contain buffer overflows. These vulnerabilities are exploitable through FTP daemons that utilize these problematic implementations.

CVE Candidate numbers for these issues have been assigned and are listed in the Vulnerable Systems section.

Link: <http://www.net-security.org/text/bugs/986909866,42751,.shtml>

SOLARIS KCMS_CONFIGURE VULNERABILITY

The problem exists in the parsing of command line options. By exploiting this vulnerability an attacker can achieve local root privileges. The Kodak Color Management System (KCMS) packages have contained many vulnerabilities in the past, we recommend disabling them if you are not currently using them.

Link: <http://www.net-security.org/text/bugs/986909911,14102,.shtml>

SUSE - MIDNIGHT COMMANDER VULNERABILITY

The Midnight Commander, mc(1), is a ncurses-based file manager. A local attacker could trick mc(1) into executing commands with the privileges of the user running mc(1) by creating malicious directory names. This attack leads to local privilege escalation.

Link: <http://www.net-security.org/text/bugs/986980267,29692,.shtml>

ORACLE APPLICATION SERVER VULNERABILITY

An exploitable buffer overflow has been identified in a shared library which is being shipped with Oracle Application Server 4.0.8.2, and used by iPlanet Web Server if it is configured as external web-listener.

Link: <http://www.net-security.org/text/bugs/986980304,50130,.shtml>

PGP 7.0 SPLIT KEY/CACHED PASSPHRASE VULNERABILITY

Wkit Security AB has found that if any caching option in PGP Desktop Security 7.0 is activated there is a vulnerability that allows a malicious user to encrypt/

decrypt or sign any file or e-mail with a split key that has been previously authenticated by an appropriate number of split-key shareholders.

Link: <http://www.net-security.org/text/bugs/986980500,97972,.shtml>

RED HAT - NEW NETSCAPE PACKAGES

New netscape packages are available to fix a problem with the handling of JavaScript in certain situations. By exploiting this flaw, a remote site could gain access to the browser history, and possibly other data.

Link: <http://www.net-security.org/text/bugs/986999609,13050,.shtml>

GHOST MULTIPLE DENIAL OF SERVICE

The first flaw involves the database engine, which isn't a Symantec product, but it is shipped with Symantec Ghost 6.5 (and possibly older versions as well).

The database engine is the run-time engine by Sybase. Connecting to the database engine on tcp port 2638 and sending a string of approx. 45Kb will cause a buffer overflow that results in registers being overwritten. The database engine needs to be restarted in order to regain functionality.

"State Dump for Thread Id 0x5c8

eax=0063f0e4 ebx=0063f204 ecx=41414141 edx=41414141 esi=00630020

edi=00630000 eip=65719224 esp=08fbfbf0 ebp=00000000

iopl=0 nv up ei pl nz na po nc

cs=001b ss=0023 ds=0023 es=0023 fs=003b gs=0000 efl=00010206"

The Ghost Configuration Server is running on TCP port 1347. It is periodically vulnerable to crash triggered the same way as the database engine overflow.

This is not a buffer overflow, and can only be used as a DoS attack.

Link: <http://www.net-security.org/text/bugs/987079641,96179,.shtml>

PROGENY - EXECVE()/PTRACE() EXPLOIT

This vulnerability exploits a race condition in the 2.2.x Linux kernel within the execve() system call. By predicting the child-process sleep() within execve(), an attacker can use ptrace() or similar mechanisms to subvert control of the child process. If the child process is setuid, the attacker can cause the child process to execute arbitrary code at an elevated privilege.

Link: <http://www.net-security.org/text/bugs/987079790,60855,.shtml>

LOTUS DOMINO MULTIPLE DOS

The Lotus Domino Web Server contains multiple flaws that could allow an attacker to cause a Denial of Service situation.

Link: <http://www.net-security.org/text/bugs/987079825,54870,.shtml>

CFINGERD REMOTE VULNERABILITY

There is a critical bug in cfingerd daemon <= 1.4.3, (a classic format bug) that makes possible to acquire full control over the remote machine if it runs the cfingerd program, the configurable and secure finger daemon.

Link: <http://www.net-security.org/text/bugs/987151748,43182,.shtml>

IBM WEBSPPHERE/NETCOMMERCE3 DOS

Exploit:

<http://host/cgi-bin/ncommerce3/ExecMacro/macro.d2w/NOEXISTINGHTMLBLOCK>

Result:

DTWP029E: Net.Data is unable to locate the HTML block NOEXISTINGHTMLBLOCK in file /usr/NetCommerce3/macros/en_US/macro.d2w
+DoS with Long URL

Link: <http://www.net-security.org/text/bugs/987151822,94005,.shtml>

CALDERA - VIM EMBEDDED MODLINE EXPLOITS

There exists a possibility for an attacker to embed special modelines into a text file which when opened with vim could compromise the account of the user. Also editing files in world writeable directories like /tmp could lead to a local attacker gaining access to the editing users account due to possible symlink attacks on editor backup and swap files.

Link: <http://www.net-security.org/text/bugs/987171863,30479,.shtml>

OPENSSSH SUBJECT TO TRAFFIC ANALYSIS

Solar Designer has conducted a very thorough analysis of several weaknesses in implementations of the SSH protocol. These weaknesses allow for an attacker to significantly speed up brute force attacks on passwords. Solar Designer's complete analysis can be found at the following page:

<http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt>

In February of 2001, Core SDI released a security announcement which described ways in which would allow an attacker to compromise the session of an SSH protocol 1.5 session. The detailed report is at the following URL:

http://www.core-sdi.com/advisories/ssh1_sessionkey_recovery.htm

Link: <http://www.net-security.org/text/bugs/987171905,95561,.shtml>

Security world

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

SYMANTEC'S SECUREXCHANGE 2001 CONFERENCE - [09.04.2001]

Symantec Corporation opened electronic registration for the company's Worldwide Users' Conference, SecureXchange 2001, formerly AXENT Technologies, Inc.'s Users' Conference. The conference focuses on solutions to organizations' security issues with over 30 classes on product integration, expert case studies, technical tips, and e-security strategies and management.

Press release:

< <http://www.net-security.org/text/press/986818398,42999,.shtml> >

SSH SECURE SHELL 3.0 ANNOUNCED - [09.04.2001]

SSH Communications Security, a world-leading developer of Internet security technologies, announced SSH Secure Shell 3.0, the next-generation of its leading encryption software product designed to protect end-users, businesses and developers from the most common break-in method used by hackers - stealing passwords from the Internet. SSH Secure Shell 3.0's new functionality includes support for PKI (Public Key Infrastructure), smart cards and the Rijndael (proposed AES - Advanced Encryption Standard) algorithm. The SSH Secure Shell 3.0 product provides transparent, strong security over any IP-based connection for both client and server applications by authenticating and encrypting terminal connections and file transfers over the Internet.

Press release:

< <http://www.net-security.org/text/press/986818611,16882,.shtml> >

VIGILANTE AND ISS PARTNER - [09.04.2001]

VIGILANTE, a leading provider of automated security assessment services, and Internet Security Systems, the world's leading provider of security management solutions for the Internet, today announced a strategic partnership. The agreement allows VIGILANTE to integrate Internet Security Systems' market-leading network security assessment software, Internet Scanner, into their award-winning security assessment service, SecureScan. SecureScan is an automated service, delivered via the Internet, which conducts intelligent assessments of Internet security perimeters. The SecureScan service is updated weekly and available on demand - providing security assurance when and where it is needed.

Press release:

< <http://www.net-security.org/text/press/986818730,92501,.shtml> >

ALADDIN ANNOUNCES ETOKEN ENTERPRISE 2.0 - [09.04.2001]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, today announced the release of eToken Enterprise 2.0, the latest set of "out of the box" plug and play 2-factor security solutions that provides quick implementation for a variety of network security and e-Business solutions. Using Aladdin's USB-based eToken security key, eToken Enterprise 2.0 allows organizations to implement the use of eTokens with a minimal amount of effort. eToken Enterprise 2.0 consists of several pre-packaged security clients that erase the need for organizations to modify their existing software, create custom applications or write additional code.

Press release:

< <http://www.net-security.org/text/press/986818832,29750,.shtml> >

FREEDOM2SURF OFFERS FREE PRIVACY SUITE - [10.04.2001]

Freedom2Surf, one of the UK's most advanced ISPs, today built on the security and privacy already offered to its users by announcing it is the

first company in the UK to offer its subscribers free access to a range of privacy and security features with the Freedom 2.0 Internet Privacy Suite from Zero-Knowledge Systems. Freedom 2.0 will be made available to all new and existing Freedom2Surf subscribers as a free download for a limited time. The suite was developed by Zero-Knowledge Systems, the leading provider of privacy technologies and services for consumers and business, and is the only solution that protects and secures the privacy and personal information of Internet users without requiring users to trust their data to a third party.

Press release:

< <http://www.net-security.org/text/press/986894868,73460,.shtml> >

RAINBOW SHIPS NEW SENTINEL 7.1.1 - [10.04.2001]

The Digital Rights Management (DRM) group of Rainbow Technologies, Inc. a leading provider of high-performance security solutions for the Internet, eCommerce and software protection, is now shipping the newest version of the industry's leading solution for secure electronic management, licensing, and distribution. The new SentinelLM 7.1.1's leading-edge software licensing and management tools are designed to secure applications from unauthorized execution and software piracy. The newest version includes new usability features and stronger security to combat online software piracy.

Press release:

< <http://www.net-security.org/text/press/986900556,82853,.shtml> >

F-SECURE INTEGRATES PRODUCTS WITH HP - [10.04.2001]

F-Secure Corp., a leading provider of centrally managed security solutions for the mobile, distributed enterprise, today announced integration of its F-Secure products with the HP OpenView VantagePoint enterprise management system [EMS] from Hewlett-Packard. By integrating F-Secure applications into HP OpenView VantagePoint, companies can now control most aspects of the applications through the familiar HP OpenView console, thus protecting their existing investment. F-Secure is believed to be the only security vendor offering true security suite integration for HP's EMS platform.

Press release:

< <http://www.net-security.org/text/press/986900647,92025,.shtml> >

PGP SECURITY'S PARTNERS WITH NSA - [10.04.2001]

NAI Labs, a division of PGP Security, a Network Associates, Inc. company, announced they are joining with the National Security Agency (NSA) and its other partners to further develop the NSA's Security-Enhanced Linux (SELinux) prototype. The \$1.2 million will be paid over the life of the two-year contract, and the work will focus on research and development to improve the security of open-source operating system platforms, the core of Internet infrastructures that have become business critical in today's economy.

Press release:

< <http://www.net-security.org/text/press/986910796,64451,.shtml> >

VIGILANTE AND NETWORKS VIGILANCE MERGER - [11.04.2001]

VIGILANTE and Networks Vigilance, a subsidiary of Cyrano, have announced plans to combine their businesses, with the new company retaining the name VIGILANTE. The companies signed an agreement on March 31st and intend to merge no later than April 13th. The deal will create a global company with an array of security assessment solutions. The combination of VIGILANTE and Networks Vigilance technology, products, services, and global partners will allow VIGILANTE to extend security assurance to the widest possible range of customers in North America, Europe and Asia. VIGILANTE will immediately combine the companies' award-winning assessment methodologies to extend its services beyond the Internet to the IT infrastructure. Customers will benefit from automated real-time security risk analysis of both their internal and external networks.

Press release:

< <http://www.net-security.org/text/press/986979179,92457,.shtml> >

RAINBOW'S IKEY 2000 IS ENTRUST-READY - [11.04.2001]

The Digital Rights Management group of Rainbow Technologies, Inc., a leading provider of high-performance security solutions for the Internet and eCommerce, announced that the company's iKey 2000 series workstation security solution has been awarded the Entrust-Ready, the leading global provider of Trust Relationship Management(software and managed services. The Entrust-Ready designation means that the iKey 2000 PE for Entrust has been tested for compatibility and interoperability with Entrust's market-leading PKI software.

Press release:

< <http://www.net-security.org/text/press/986981381,14396,.shtml> >

RAINBOW'S SMART TOKENS REACH CRITICAL MASS - [11.04.2001]

The Digital Rights Management group of Rainbow Technologies, Inc. a leading provider of high-performance security solutions for the Internet, eCommerce and software protection, today claimed leadership of the worldwide smart-token security market by announcing that Rainbow has sold 26 million software security keys, high-security authentication tokens, and workstation security solutions. Rainbow made the announcement at today's 2001 RSA Data Security Conference and Software Development West trade shows.

Press release:

< <http://www.net-security.org/text/press/986981568,39553,.shtml> >

PGP SECURITY AND RAINBOW TECHNOLOGIES PARTNER - [13.04.2001]

PGP Security, a Network Associates Company, announced a partnership with Rainbow Technologies, a leading provider of Internet and eCommerce security solutions, to improve security for electronic transactions and communications. PGP Security's private key technology will be incorporated into Rainbow's iKey authentication-token family, which enables users to store their private keys securely on the token rather than on a PC where it is vulnerable to unauthorized access and privacy.

Press release:

< <http://www.net-security.org/text/press/987151028,7348,.shtml> >

PITBULL LX TECHNOLOGY ON SOLARIS 8 RELEASED - [13.04.2001]

Argus Systems Group, Inc., the global leader in Internet security and intrusion prevention systems, announces the availability of its award-winning PitBull LX security technology on the Solaris 8 platform. PitBull LX on Solaris delivers the strength and power of market-leading PitBull security in a simple to install, intuitive and non-intrusive implementation. The availability of PitBull LX on Solaris 8 marks the latest in a series of security developments by Argus this year, following the release of PitBull LX for Linux and a Trusted Web Server Appliance software suite.

Press release:

< <http://www.net-security.org/text/press/987151117,12009,.shtml> >

TOP SECURITY FIRMS JOIN MSSPP - [13.04.2001]

Microsoft Corp. announced at RSA Conference 2001 that three of the top names in computer security - Computer Sciences Corp. (CSC), Foundstone Inc. and Guardent Inc. - will join with Microsoft to provide security consulting services as part of the Microsoft Security Services Partner Program. Designed to provide customers with an online directory of consulting companies with security expertise, the Microsoft Security Services Partner Program supports a community of technical professionals - over 50 partners in 16 countries - that specialize in securing Microsoft environments. Participants have ongoing access to quality security information and training from Microsoft as well as support for managed security services that assist customers in securing their individual environments.

Press release:

< <http://www.net-security.org/text/press/987151241,64199,.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

GUARDIAN FIREWALL-5

Guardian Firewall-5 is a low cost security solution for the small office/home office (SOHO) market. NetGuard is currently offering Guardian Firewall-5 to the North and South American market in a concerted effort to ensure that all companies are secured against malicious attacks. Guardian Firewall-5 allows small networks to achieve the utmost in security while maintaining the ease of installation that smaller companies require. Guardian Firewall-5 is based on MAC-Layer Stateful Inspection technology to ensure superior protection and performance.

Read more:

< <http://www.security-db.com/product.php?id=135> >

This is a product of NetGuard, for more information:

< <http://www.security-db.com/info.php?id=24> >

HP IPSEC/9000

HP IPsec/9000 provides secure, private communication over the Internet and within the enterprise without having to modify a single application. Along with authentication, data integrity, and confidentiality, IPsec/9000 offers protection against replays, packet tampering, and spoofing—and it keeps others from intercepting critical data such as passwords and credit card numbers sent over the Internet. Whether or not a public key infrastructure (PKI) has been implemented, HP IPsec/9000 easily integrates into the existing enterprise infrastructure. It has the flexibility to create an authenticated tunnel, using either digital certificates from Entrust and Verisign or self-generated pre-shared keys.

Read more:

< <http://www.security-db.com/product.php?id=707> >

This is a product of HP Internet Security, for more information:

< <http://www.security-db.com/go.php?id=156> >

NETRECON

NetRecon is a network vulnerability assessment tool that discovers, analyzes and reports holes in network security. NetRecon achieves this by conducting an external assessment of network security by scanning and probing systems on the network. NetRecon reenacts common intrusion or attack scenarios to

identify and report network vulnerabilities, while suggesting corrective actions.

Read more:

< <http://www.security-db.com/product.php?id=303> >

This is a product of AXENT, for more information:

< <http://www.security-db.com/info.php?id=60> >

SDK SOFTWARE DEVELOPMENT KIT

Veridicom's software creates and identifies a unique representation of an individual's fingerprint-enabling reliable, convenient personal authentication solutions. Veridicom's proprietary software is available in modules that perform image capture, quality control, processing, and one-to-one or one-to-few verification matching. The Imaging Suite software modules and Verification Suite modules are based on open architecture standards. They can be used with either Veridicom 5thSense personal authentication peripherals or your own hardware based on Veridicom's solid-state fingerprint sensors.

Read more:

< <http://www.security-db.com/product.php?id=299> >

This is a product of Veridicom, for more information:

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

DISKGUARD

If you are the only person working on your Macintosh, you can protect your computer by typing in one password. That's all there is to it. If your computer is shared with other people, give them a second password which limits their access, according to your own requirements, to certain days of the week or to specific hours during the day. At start-up, DiskGuard requests a password. No one will be able to start the Macintosh without supplying the proper password, even if he tries to boot with a System disk or holds down the Shift key to bypass extensions. DiskGuard also keeps a close watch on your computer while you are at work. When you take a moment's leave, DiskGuard automatically hides your screen from prying eyes. As soon as someone tries to access the computer, DiskGuard will prompt for the proper password. DiskGuard also keeps track of valid and invalid access attempts to your hard disk so you can see at any time if somebody tried accessing your computer during your absence.

Read more:

< <http://www.security-db.com/product.php?id=605> >

This is a product of Highware, for more information:

< <http://www.security-db.com/info.php?id=131> >

Featured article

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

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

"LOGIC" WORM - PROOF-OF-CONCEPT MALICIOUS CODE

Recently, some anti-virus vendors have been touting the discovery of a new Internet-worm "Logic" - the first malicious code written in the Logo programming language used in a limited number of schools for educational purposes only. Kaspersky Labs firmly states that this Internet-worm still has not yet been found "in-the-wild," and poses absolutely no threat to the majority of computer users, simply because, in order to be activated, "Logic" requires the Logo interpreter to be installed on the target systems (for example, SuperLogo for Windows).

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

Security Software

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

SMARTBLOCK 1.50

SmartBlock offers the ability to filter indecent Web sites in real time, thus protecting your children from objectionable Internet material. SmartBlock intercepts all words in real time, restricts your children's access to games, and protects files and folders from being deleted or renamed. It can also capture screenshots and save them to the hard disk to help you monitor computer usage.

Info/Download:
< <http://www.net-security.org/various/software/987348093,23594,windows.shtml> >

IPNETSENTRY

IPNetSentry is a simple and intelligent security application which protects your Macintosh from outside Internet intruders. This is particularly important for Macintosh users who have cable modem, DSL, or another high-speed Internet

service where connections can be maintained and left unattended for hours (or days) at a time. Unlike most other Internet security products, IPNetSentry does not erect barriers for the safe use of your Internet connection. There is no need to "punch holes" in a firewall for specific applications you may wish to run. Instead, IPNetSentry silently and intelligently watches for suspicious behavior, and when triggered, invokes a solid filter which completely bans the potential intruder from your Macintosh.

Info/Download:

< <http://www.net-security.org/various/software/987349021,10394,mac.shtml> >

WEBROOT WINGUARDIAN 2.6

Parents, schools, libraries, churches, and anyone else wishing to control access to the Internet can use WinGuardian to monitor which Web sites users visit, what they type (via keystroke logging), which programs they access, and the time they spend using the programs. WinGuardian can also secure Windows so that users cannot run unauthorized programs or modify Windows configurations such as wallpaper and network settings. It also features network support and the ability to display an acceptable-use policy. Features include screen-shot capturing, enhanced keystroke capturing (captures lowercase and special characters), America Online support, Opera support, and the ability to email log files to a specific email address.

Info/Download:

< <http://www.net-security.org/various/software/987348286,54994,windows.shtml> >

BRICKHOUSE

BrickHouse was developed by Brian Hill to ease the process of configuring MacOS X's built-in Firewall. His hard work has paid off; hundreds of OS X owners use his program. Changing Firewall settings manually without a GUI can be tedious and confusing for unexperienced users; this program removes those barriers. By using BrickHouse to configure your computer's firewall, you can more effectively keep unauthorized users from gaining access to your computer via your internet connection. BrickHouse makes it easy to use your firewall to guard against denial of service or resource-based internet attacks. Network attacks will bounce off the firewall, preventing your computer from slowing down or crashing. BrickHouse provides a simple and easy interface to activate and configure your firewall's filters. It also includes a firewall monitor window that allows you to see how frequently each filter is used. Filter settings can be saved and toggled quickly, and can be imported and exported to and from disk. Settings can be created by knowledgeable users and admins, who can distribute them to others, quickly disabling specific or recently discovered attack techniques.

Info/Download:

< <http://www.net-security.org/various/software/987349194,20968,mac.shtml> >

ETHERREAL-0.8.17-A

Ethereal is a GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames. The goal of the project is to create a commercial-quality analyzer for Unix and to give Ethernet features that are missing from closed-source sniffer. Changes: New dissectors include CUPS browsing protocol, Cisco HDLC, DCE RPC support, LMI for frame relay, Wellfleet compression, BACNET, and RWALL. Many other dissectors were updated and bug-fixed. New 3D logo. The Windows version can now dynamically load the wpcap.dll at run-time. And a Windows installer has been added. Add -D flag to tethereal to show list of all network. Added support for packet data decompression and decoding.

Info/Download:

< <http://www.net-security.org/various/software/987348497,42703,linux.shtml> >

Defaced archives

[09.04.2001]

Original: <http://www.sony-center.ch/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/09/www.sony-center.ch/>

OS: Windows

Original: <http://pbrown.ios.doi.gov/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/09/pbrown.ios.doi.gov/>

OS: Windows

Original: <http://www.aiwa.com.pa/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/09/www.aiwa.com.pa/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/04/09/www.crackattack.com/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/04/09/dataframe.net/>

OS: Windows

[10.04.2001]

Original: <http://www.ericsson.ly/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/10/www.ericsson.ly/>

OS: Windows

Original: <http://www.ericsson.cbc.dk/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/10/www.ericsson.cbc.dk/>

OS: Windows

Original: <http://www.apache.or.kr/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/10/www.apache.or.kr/>
OS: Linux

Original: <http://www.pepsi-music.co.uk/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/10/www.pepsi-music.co.uk/>
OS: Windows

Original: <http://www.netnanny.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/10/www.netnanny.com/>
OS: Windows

Original: <http://www.honda.ca/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/10/www.honda.ca/>
OS: Windows

[11.04.2001]

Original: <http://www.sony-training.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/11/www.sony-training.com/>
OS: Windows

Original: <http://www.yourcriminalattorney.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/11/www.yourcriminalattorney.com/>
OS: Windows

Original: <http://www.golfhackers.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/11/www.golfhackers.com/>
OS: Windows

Original: <http://www.nortel.it/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/11/www.nortel.it/>
OS: Windows

Original: <http://www.gatorade.com.ar/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/11/www.gatorade.com.ar/>
OS: Windows

[12.04.2001]

Original: <http://www.dortp.gov.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/12/www.dortp.gov.tw/>
OS: Windows

Original: <http://www.vipfe.gov.bo/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/12/www.vipfe.gov.bo/>
OS: Windows

Original: <http://www.sony-training.de/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/12/www.sony-training.de/>
OS: Windows

Original: <http://www.crack3r.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/12/www.crack3r.com/>
OS: Windows

[13.04.2001]

Original: <http://www.sonymonitor.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/13/www.sonymonitor.com/>
OS: Windows

Original: <http://www.tech-help.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/13/www.tech-help.com/>
OS: Unknown

Original: <http://www.drinkpepsi.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/13/www.drinkpepsi.com/>
OS: Windows

Original: <http://www.fazenda.pbh.gov.br/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/13/www.fazenda.pbh.gov.br/>
OS: Windows

[14.04.2001]

Original: <http://www.coca-colaecuador.org/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/14/www.coca-colaecuador.org/>
OS: Windows

Original: <http://www.profuturo.com.pe/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/14/www.profuturo.com.pe/>
OS: Windows

Original: <http://www.britishembassy.ee/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/14/www.BritishEmbassy.ee/>
OS: Windows

Original: <http://www.pepsi-music.co.uk/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/14/www.pepsi-music.co.uk/>
OS: Windows

Original: <http://www.linuxtampico.org.mx/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/14/www.linuxtampico.org.mx/>
OS: Linux

[15.04.2001]

Original: <http://www.musicworld4u.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/15/www.musicworld4u.com/>
OS: Windows

Original: <http://www.spytoy.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/15/www.spytoy.com/>
OS: Linux

Original: <http://www.creative-computer.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/15/www.creative-computer.com/>
OS: Windows

Original: <http://www.networksensors.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/15/www.networksensors.com/>
OS: BSDI

Original: <http://www.antiviral.uab.edu/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/15/www.antiviral.uab.edu/>
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>