

HNS Newsletter
Issue 58 - 09.04.2001
<http://net-security.org>
<http://security-db.com>

This is a newsletter delivered to you by Help Net Security. It covers weekly roundups of security events that were in the news the past week. Visit Help Net Security for the latest security news - <http://www.net-security.org>.

Subscribe to this weekly digest on:
<http://www.net-security.org/text/newsletter>

Archive of the newsletter in TXT and PDF format is available here:
<http://www.net-security.org/news/archive/newsletter>

Current subscriber count to this digest: 2204

Table of contents:

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

=====
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>
=====

General security news

STANFORD LAW SCHOOL DEAN WILL ARGUE 2600 CASE
"In a major boost to our legal battle against the MPAA, Stanford Law School Dean Kathleen Sullivan has joined our team and will be arguing the case in front of the Second Circuit Court of Appeals on May 1. She joins Martin Garbus and the team from the Electronic Frontier Foundation who worked on the initial trial and continue to work diligently on the appeal. Sullivan brings an impressive combination of legal expertise and technical knowledge to this critical point of our case and it demonstrates not only that we intend to win, but that there are many experts in the field who understand the importance of the DeCSS case - and are willing to help."
Link: <http://www.2600.com/news/display.shtml?id=211>

WIN-NT/IIS ADMINS MADE APRIL FOOLS BY HACKERS

Several crews got busy on April Fools Day to make a mockery of Microsoft security by targeting Web sites running MS' IIS server over Windows NT/2K for defacement. Among the higher-profile victims were the Walt Disney Company; the Wall Street Journal's WebWatch; British Telecomms; HSBC; the US Navy's Center for Tactical Systems Interoperability (NCTSI); the US Army Training and Doctrine Command (TRADOC); Ringling Bros and Barnum & Bailey Circus; and the American Society for the Prevention of Cruelty to Animals (ASPCA). None of the sites appeared to have been attacked for any reason other than the fact that they were vulnerable.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/18029.html>

HOW TO AVERT A VIRUS DISASTER

Vinny Gullotto, head of the McAfee Anti-Virus Emergency Response Team (Avert), is a fast-talking techie who the Feds call when they're foxed by the latest virus. "I get a lot of calls from the FBI looking for virus samples," said Gullotto. "They want to know how we rate a particular virus and what threats they should look out for. We can deal with most viruses in somewhere between two and six hours."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/Features/1120000>

THE NT LOCAL ADMINISTRATOR AND SHARED PASSWORDS

There is a Local Administrator account on every NT machine currently deployed. It is extremely common to find many NT machines in an enterprise sharing the same password for this Local Administrator account. This article by SecurityFocus writer Daniel Marvin will establish that this shared password constitutes a security vulnerability. It will subsequently discuss various steps to mitigate the risk arising from the shared password, and make a case for applying unique passwords to every Local Administrator account in your enterprise.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/nt/sharedpass.html>

IT SECURITY PROFESSIONALS MAY BE LICENSED

IT security professionals may require a government licence to work in future, Home Office minister Charles Clarke has warned, leaving the door open for further regulation of the UK IT industry. Clarke has refused to rule out including IT consultants in professions covered by the Private Security Industry (PSI) Bill, which was originally intended to cover bouncers and wheel-clampers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/News/1120010>

HACKER SPEAK

"Hackers and members of the Internet security industry, like workers in other specialty trades, have their own form of shop talk. The following is an abbreviated list of catch phrases and euphemisms used by hackers and security professionals."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/features/article/0,aid,44370,00.asp>

TO TRAP A THIEF

If you want to break into a house, why spend time prying open the front door if the back door is wide open? Same goes when breaking into computer networks. Most networks and servers are set up with configuration errors that are well known to hackers, who can download free tools that will scan many different networks looking for those easy-open entry points. No genius-level code manipulation or high IQ is needed.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59072,00.htm

CHINESE FEDS DEMAND COMPUTER VIRUS SAMPLES

China's Ministry of Public Security has been requiring Western anti-virus vendors to supply samples of malicious code as a condition of doing business with Mainland consumers, the Wall Street Journal reports. The official Chinese explanation would have us believe that the secret police have lately gone into the consumer protection business by claiming that the samples are necessary to enable the Feds to test the effectiveness of the software being sold.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/18057.html>

SECURITY INDUSTRY SLAMS VIRUS REWARD

The antivirus industry lambasted email firewall startup GateKeeper on Monday, after the company announced a reward for any virus writer who can infect a specific computer protected by its product. "It is probably one of the most irresponsible things that someone could do," said Vincent Gullotto, director of the Antivirus Emergency Response Team for security services company Network Associates.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/13/ns-22031.html>

PERSONAL FIREWALL TEST: TERMINET

This article is a part of a series of tests on Personal Firewalls/Intrusion Detection Systems. TermiNET, by DANU Industries, is a relatively simple firewall. It offers access control, stealth mode, web blocking, multiple user profiles, intrusion detection with blocking notification, flexible web browsing control, and restriction by IP address, URL, port and protocol.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/pf_terminet20010403.html

NEW CLOAKED-CODE THREAT TO SECURITY

During a seminar last week at the CanSecWest conference in Vancouver, British Columbia, a hacker named "K2" revealed a program he created that can camouflage the tiny programs that hackers generally use to crack through system security. The cloaking technique is aimed at foiling the pattern-recognition intelligence used by many intrusion detection systems, or IDSeS, known as the burglar alarms of the Internet. "Trust me, this will blow away any pattern matching," said K2, who would not reveal his real name because he also works as a security consultant.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5080532,00.html>

DIRECTORS BLIND TO SECURITY WEAKNESSES

Financial and managing directors are dangerously unaware of the risks surrounding digital business, according to a recent Mori poll. The survey, commissioned by digital risk insurance specialist Safeonline, showed that only 24 per cent of directors at small to medium sized enterprises could identify a security risk without being prompted. Mori found that damage caused by staff, whether by negligence or genuine error, is the most feared risk. When prompted by pollsters, 47 per cent of respondents said that innocent mistakes were the most likely cause of damage.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/News/1120062>

46,000 ADDR.COM STOLEN?

A computer criminal claims to have stolen personal information on 46,000 customers from Web hosting company ADDR.com. The data includes account names and passwords that could be used to alter Web site content, as well as credit card information. ADDR.com has so far not commented on the alleged heist.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/553615.asp>

GOVERNMENT BACKTRACKS ON ENCRYPTION ENQUIRY

The Home Office has backtracked on a promise to commission an independent enquiry into the effects of legislation that will give police and other authorities the power to intercept data transmitted over private networks and demand decryption keys from the place where data is encrypted.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/13/ns-22044.html>

INTERVIEW WITH ELIAS LEVY (BUGTRAQ)

Bugtraq is probably the best security mailing list around. While the quasi founder (I was surprised to find that Aleph1 didn't technically start Bugtraq) is quite prominent online, I wasn't able to find any detailed information about him or Bugtraq (except for one old interview). So, here for you to enjoy is an interview with Aleph1.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010405.html>

ONE IN THREE UK COMPANIES HAVE BEEN HACKED

A survey of IT professionals released today indicates that one in three UK businesses has been the victim of a major security break in. Almost half of those who took part in the poll said that the future of their organisation could be ruined by a serious hacker attack. The survey, commissioned by the Communications Management Association (CMA) questioned 2000 senior IT professionals and guaranteed anonymity to participants.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/13/ns-22045.html>

NEW TECHNOLOGY ENABLES PORTABLE SECURITY

Biocentric Solutions has unveiled its next generation of biometric technology for authentication with portable computing devices. Biocentric also rolled out two products based on its next generation technology, the BioSentry for the Compaq

iPAQ Pocket PC, and BioHub for portable computing devices that run in Windows CE. A portable biometric fingerprint reader designed for the Compaq iPAQ Pocket PC, BioSentry is used in place of the iPAQ expansion pack to prevent unauthorised access to both the hardware and data on the Pocket PC.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/News/1120091>

HAVE MOVIES CREATED THE STEREOTYPE OF THE HACKER?

No doubt you remember Matthew Broderick's portrayal of a hacker in the movie War Games. That film launched hacking as a popular pastime--at least for a specific demographic of teenage males. But it wasn't the first film to feature hacking, or the last. Movie hackers have had many faces: one-dimensional clowns, nefarious villains, mischievous geniuses, anarchic heroes. And as hackers and their motivations in the real world have changed, so have their counterparts in the movies. In more recent films they're more unrealistic, cartoonier, angrier, and able to perform completely impractical or impossible acts.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.pcworld.com/features/article/0,aid,45804,00.asp>

CHASING THE WIND, PART FIVE: THE DEVIL IN THE DETAILS

At long last, SecurityFocus is pleased to present the fifth installment of Robert G. Ferrell's popular series, Chasing the Wind. As we left off last time, Ian, the aspiring hacker, had just successfully defaced Acme Ailerons' web site. Jake, Acme's new SysAdmin, slept peacefully, oblivious to the travails that awaited him. Douglas, a Systems Engineer at Acme Ailerons, was busy trying to decipher some the plans for a mysterious classified project. Meanwhile, Bob, the CIO of the company, had travelled to the high-security C4I center for a very high-level, top-secret meeting...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ih/articles/chasing5.html>

WIRED REPORTER FORCED TO TESTIFY AT CYPHERPUNK TRIAL

Wired chief Washington correspondent Declan McCullagh isn't merely covering the criminal trial of cypherpunk Jim Bell (who's in the dock accused of stalking federal agents); he's also been made a reluctant participant. McCullagh had sought to quash a subpoena requiring him to testify on concerns that he might be forced to disclose information related to Bell's case given to him in confidence, but his motion was denied. The Feds offered assurance that they would question him only on the accuracy of reports he'd already published so that they could be entered into evidence, which would of course be fair; but once a witness is on the stand, there's nothing to prevent a prosecutor asking whatever he or she might please.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/18104.html>

BT HACKED TWICE IN THREE DAYS

BT has had two of its UK websites defaced by hackers over the last three days. On Sunday hackers left a rant about ADSL on the search.bt.com site, and yesterday btworldwide.com was defaced by Prime Suspectz.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1120110>

MORE ON ADORE WORM

The third Linux worm in almost as many months hit the computer systems this week. Known as the Adore worm, the program is designed to create back doors in the security of Linux systems and send information identifying the compromised systems to four different e-mail addresses hosted on servers in China and the United State. If you have been noticing a large number of scans for port 515, it is recommended you take the necessary steps to patch the vulnerabilities noted below.

- Multiple Vendor LPRng User-Supplied Format String Vulnerability
- <http://www.securityfocus.com/bid/1712>
- Wu-Ftpd Remote Format String Stack Overwrite Vulnerability
- <http://www.securityfocus.com/bid/1387>
- ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability
- <http://www.securityfocus.com/bid/2302>
- Multiple Linux Vendor rpc.statd Remote Format String Vulnerability
- <http://www.securityfocus.com/bid/1480>

NEW NSW CYBER CRIME LAWS

SMH reported that New South Wales Government announced new laws dealing with cyber crime. Virus writers could get up to 10 years for their creations and maximum sentence of five years will be the result for online fraudsters.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.smh.com.au/news/0104/05/pageone/pageone4.html>

LION INTERNET WORM ANALYSIS

This paper provides an introduction to the Lion (1i0n) Worm author and a technical analysis of the Lion Internet Worm. Three unique variations of the Lion Worm have been released on the Internet over the past month. All three versions of the Lion Worm are unsophisticated unix shellsript worms. BTW paper gives really comprehensive study on the mentioned worms.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://whitehats.com/library/worms/lion/>

TURBOTAX SOFTWARE HAS PASSWORD GLITCH

A programming glitch in TurboTax software has posed a potential security problem for as many as 150,000 users and may force them to change their passwords, Intuit Inc. said Thursday.

Link: <http://www.nandotimes.com/technology/story/0,1643,500470851-500721068-504029893-0,00.html>

VIRUS PESSIMISM FROM MESSAGELABS?

Virus attacks may treble by the end of the year according to research from UK antivirus firm MessageLabs, which suggests that government departments as well as companies will collapse under the weight of malicious attachments and executables. Sophos' Graham Cluley answered to that: "I don't think there is any scientific evidence that the situation is going to get radically worse than it is now."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/13/ns-22102.html>

CURADOR 'TAKES CARE' OF BILL GATES

The Sun reported that 'Curador' (look a year back for more information), who is awaiting sentence after pleading guilty to stealing credit card details from a number of insecure Web sites, has reportedly claimed he sent a shipment of Viagra to Bill Gates using the Microsoft boss's own credit card.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/18124.html>

GOVERNMENT TARGETS

Unauthorized people gained complete control of at least 155 government computer systems among 32 federal agencies last year, according to a review made public Thursday during a congressional hearing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/04/05/computer.security.ap/index.html>

BIOPASSWORD SECURITY CHECKS USER'S TYPING PATTERN

Call me paranoid, but I'm in good company. Most biometric security programs - which identify a person through their biological traits - store details about a user's unique physical characteristics on a hard drive, and Robert Flores, the CIA's chief technology officer, says it's easy enough for a hacker to get at the data. When I quoted Flores's statement to the five biometric vendors in this review, four of them either changed the subject or essentially said, "Well, nothing is foolproof." The representative of one company, Net Nanny Software Inc., not only agreed with Flores but also said that vulnerability is what makes the company's BioPassword effective.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/164151.html>

IMPROVING APACHE

Unix admins swear by Apache's out-of-the-box robustness, but certain configuration steps are needed to ensure the Web server's security." I'm running Apache, not IIS. Therefore, I'm secure." When it comes to Web server security, many systems admins automatically assume Microsoft's Internet Information Server is the devil, while the open-source Apache is God. Diehard Unix admins swear up and down that they'll never go with IIS because it's a breach waiting to happen and Apache is so secure.

Well, guess again.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/april01/features1_web_server_sec.shtml

BETA RELEASE OF TRUSTIX SECURE LINUX 1.4.80

"This is to announce the BETA release for the upcoming Trustix Secure Linux 1.5 release. It has version 1.4.80, and is nicknamed "Ooops". It is in several ways INCOMPATIBLE with 1.2, and you do not want to just continue without knowing a little more of what is ahead. If it breaks your system, let us know so we can prevent it from happening to others. But don't say you didn't know it would :-)"

Link: http://linuxtoday.com/news_story.php3?ltsn=2001-04-05-020-20-SC

HACKER TOOL THREATENS .NET

Microsoft's .Net platform has been dealt a security blow before it has even been released. The discovery of what is thought to be the first C# decompiler for the software giant's much heralded next-generation operating system will undermine confidence in the platform. John Safa, a former cracker and CTO of security vendor BitArts, said: "The cracking community now has a C# decompiler, which unravels application code. If you got on the inside of a network using this tool, you could do anything."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/News/1120202>

E-MAIL WIRETAPPING

Corporate spies are using covert JavaScript code within email to track the contents of sensitive financial communications. That's the warning from managed service provider Activis which said that it is seeing increasing use of malicious JavaScript coding to create Web bug that spy on Internet traffic. These Web bugs can be embedded into HTML based emails before they are sent. The code then acts to covertly copy the original sender each time this email is forwarded on within the recipient's system.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/18147.html>

DISTANT EARLY WARNING

Keeping a pulse on national and international developments that impact computer security is like trying to catch a subway train just leaving the station. You do a lot of running, and maybe, you still miss the train. If your company does business across multiple political borders, strange questions may arise.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/earlywarning20010406.html>

MACINTOSH OS X SECURITY

Security to the general Macintosh user has never been much of an issue. Turn it on, use it, turn it off when you're done. And even if you've got a DSL or other dedicated line, warnings related to hack attempts on open and dedicated networks lines never seemed to instill fear in a Mac user. Sure there are products like Norton Personal Firewall or NetBarrier 2.0, but these are for professionals right?

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

INTERVIEW WITH LANCE SPITZNER

Introduction by Max Vision: "Lance is an absolutely essential leader in the whitehat community. He infects everyone with his passion and enthusiasm for network security. But more importantly, he organizes a fairly disparate group of security experts into a productive, cooperative team. This is no easy feat in an industry that increasingly favors non-disclosure. Lance is an exemplar of a true whitehat: curious, intelligent, and honest. He is simply good."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.safemode.org/LanceSpitzner.html>

PASSWORD RECOVERY SOFTWARE

Elcom is a private russian company established in 1990. They develop password recovery software: for archives (ZIP, RAR, ARJ, ACE), Adobe Acrobat PDF, Microsoft Office (Word, Excel, Access, Outlook, Visio, PowerPoint, VBA), MS Project, MS Backup, MS Mail, MS Schedule+, Symantec ACT!, Intuit Quicken & QuickBooks, Borland/Corel Paradox and Lotus WordPro, 1-2-3.

Link: <http://www.security-db.com/info.php?id=150>

CAN YOU BREAK WINDOWS XP SECURITY?

Microsoft quietly put a new test site online last Saturday to let hackers attempt to breach Windows XP's security. Microsoft placed a version of Windows XP Home Edition online in a configuration that resembles a typical user's home setup. The Web site will help Microsoft determine configuration settings that it can recommend to potential users of the new OS.

Link: <http://www.ntsecurity.net/Articles/Index.cfm?ArticleID=20596>

WOH 'S INTERVIEW

Alldas.de has an interview with RuBiX, a member of WoH (World Of Hell) - a defacing group that attacks web sites of rich and famous companies.

Link: <http://security.alldas.de/interviews/?id=2>

ATTACKERS HIT CRICKET, BOLLYWOOD SITES

Attackers have defaced two Indian internet sites catering to movie fans and cricket lovers, the chief of the company which runs the sites said on Saturday. One of the sites showed pasted statements criticising India's role in Kashmir. The other had a dark green colour resembling the Pakistani flag.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.economictimes.com/today/08tech05.htm>

Security issues

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

TOMCAT MAY REVEAL SCRIPT SOURCE CODE

Tomcat (<http://jakarta.apache.org/tomcat/>), the Reference Implementation for the Java Servlet 2.2 and JavaServer Pages 1.1 Technologies, may be tricked into revealing the source code of JSP scripts by using simple URL encoding.

Link: <http://www.net-security.org/text/bugs/986039232,20871,..shtml>

BEA WEBLOGIC MAY REVEAL SCRIPT SOURCE CODE

BEA WebLogic may be tricked into revealing the source code of JSP scripts by using simple URL encoding of characters in the filename extension.

Link: <http://www.net-security.org/text/bugs/986039343,69657,..shtml>

SILENT RUNNER COLLECTOR BUFFER OVERFLOW

Silent Runner Collector (SRC) has a buffer overflow condition in the routines that parse SMTP traffic. SRC is the "sniffer" component of the Silent Runner network traffic analysis suite. The overflow was noticed in SRC v1.6.1 but is likely present in other versions as well. The actual buffer in question holds the SMTP HELO line. The overflow occurs when a HELO command in excess of 4096 bytes transits a network segment that the collector is monitoring. This vulnerability can be exploited by an intruder to crash the collector and thus stop the monitoring of transiting network traffic.

Link: <http://www.net-security.org/text/bugs/986039956,52213,.shtml>

VIRUS BUSTER 2001 BUFFER OVERFLOW

The buffer overflow occurs when MUA received email with the header defined in RFC 822 including unusually long strings. As a result, the user of this software is not able to receive any e-mail(s) more. An attacker could use this vulnerability to execute arbitrary commands. A restart of the computer is required in order to gain normal functionality.

Link: <http://www.net-security.org/text/bugs/986040790,23239,.shtml>

PROBLEMS WITH INCORRECT MIME HEADER

Microsoft has released a security bulletin

<http://www.microsoft.com/technet/security/bulletin/ms01-020.asp> entitled "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment". EML files are MIME multipart files that IE 5 will parse. There is a vulnerability allowing arbitrary code execution using this kind of files. This vulnerability could allow an hostile page or e-mail to perform any action on your computer. The vulnerability affects IE 5, IE 5.5 over all windows platforms.

Link: <http://www.net-security.org/text/bugs/986042902,80256,.shtml>

TREND MICRO'S SCANMAIL FOR EXCHANGE BUG

Several registry values are created during installation and during use of the product's Management Console to store the credentials of the last user to log on. These credentials are valid at least on the server, and possibly valid on the entire domain depending on the last user to log in. Additionally, these keys are created with Everyone set to Special Access, which includes the ability to read the values. The usernames and passwords are rolled right a number of characters and then XOR'ed with a constant key (0xB15A0E707EEDEB80F70FB78F1399).

Link: <http://www.net-security.org/text/bugs/986122048,75503,.shtml>

SECURITY BUG IN INTERNET EXPLORER

By visiting a web page with IE it is possible to read arbitrary local files (in very rare cases small amount of the file's content is lost) if the file name is known and send them to an arbitrary server. It is also possible to read arbitrary web pages to which the victim has access. Probably this bug may be more serious, have not investigated further - an interesting scenario seems to be playing with C:\Documents and Settings\USERNAME\Local Settings\Temporary Internet Files\Content.IE5\index.dat. which probably may lead to executing arbitrary programs.

Link: <http://www.net-security.org/text/bugs/986122152,59013,.shtml>

TOMCAT 3.2.1 FOR WIN2000 DIR. TRAVERSAL

A security vulnerability has been found in Windows NT/2000 systems that have Tomcat 3.2.1 installed. The vulnerability allows remote attackers to access files outside the document root directory scope.

Link: <http://www.net-security.org/text/bugs/986122415,77089,.shtml>

WINAMP 2.63 FULL DISCLOSURE EXPLOIT

I have written a full disclosure buffer overflow exploit for the winamp 2.63 buffer overflow found in the M3U file parser. Attached is a file called DROPPER.M3U, if you execute the following commands in dos :
COPY /B DROPPER.M3U+C:\WINDOWS\CDPLAYER.EXE HACKME.M3U when you click HACKME.M3U, the file will drop and execute the appended exe file, CDPLAYER.EXE in this case...

Link: <http://www.net-security.org/text/bugs/986145682,48652,.shtml>

INTERNET & ACCELERATION SERVER EVENT DOS

If an alert action has been chosen in the ISA server console, a malicious attacker can cause a Denial of Service situation on the ISA server.

Link: <http://www.net-security.org/text/bugs/986229749,12002,.shtml>

MALWARE.COM ADVISORY: THE BAT!

We are able to blind the The BAT! with trivial file extension modifications and carefully calculated file name lengths:

Content-Type: image/gif;

Content-Transfer-Encoding: base64

Content-Disposition: inline;

filename=" what's this?"

v .gif.exe"

vWill create an inline attachment, which, while not important will not be indicted in the in-box. What is important is that the attachment viewed once the mail message has been opened will be with the icon of something else. On two win98 machines, we achieved the icon of a folder: vv (screen shot:

<http://www.malware.com/guano.jpg> 32KB)

and the icon of the local machine hard drive. BAT! worse, when clicking the icon, the *.exe is executed without warning. The comprehensive warning for *.exe attachments is bypassed. As far as the client is concerned there is no attachment and their is no file extension, other than what we decide to give it.

Link: <http://www.net-security.org/text/bugs/986301594,30398,.shtml>

RED HAT - UPDATED OPENSSSH PACKAGES

Updated openssh packages are now available for Red Hat Linux 7. These packages fix an error in the supplied init script and PAM configuration file.

Link: <http://www.net-security.org/text/bugs/986379615,60428,.shtml>

RED HAT - UPDATED KERBEROS 5 PACKAGES

Updated Kerberos 5 packages are now available for Red Hat Linux 7. These updates resolve a linkage problem introduced in RHSA-2001:025.

Link: <http://www.net-security.org/text/bugs/986379723,44012,.shtml>

ANOTHER PHP-NUKE VULNERABILITY

There is a bug in the banner section of PHP-Nuke (<http://www.phpnuke.org>). In order to change the URL of the first banner you should enter in your browser the following

<http://target/banners.php?op=Change&bid=bannerid&url=http://where.to>

If we want to change the banner number 1 to redir to www.you_are_redir we write

<http://www.foo.com/banners.php?op=Change&bid=1&url=http://you.are.redir>
where www.foo.com is the server running PHP-Nuke

Link: <http://www.net-security.org/text/bugs/986379826,58027,.shtml>

ORINOCO RG-1000 WEP KEY EXPOSURE

An attacker can determine the network name (SSID), and current WEP encryption key - allowing unrestricted access to the LAN.

Link: <http://www.net-security.org/text/bugs/986379950,66980,.shtml>

NAVISION FINANCIALS SERVER DOS

Sending a null character followed by approx. 30k of A's to TCP port 2407 causes a buffer overflow and terminates the process (SERVER.EXE). The overflow does not appear to be exploitable. A smaller amount can also be used, and will silently kill the process. This requires approx. 10 connections starting with a null character, followed by 100+ characters.

Link: <http://www.net-security.org/text/bugs/986380075,16618,.shtml>

MS PATCH Q292108 OPENS A VULNERABILITY

Last MS patch Q290108 released with the bulletin MS01-020 opens a new vulnerability. A tricked EML file can confuse the user displaying him a fake downloaded file name. Executable files can be disguised as other supposedly innocent files (text, sound or images).

Link: <http://www.net-security.org/text/bugs/986470161,75358,.shtml>

BINTEC X4000 ACCESS ROUTER DOS

A simple nmap SYN scan (`nmap -sS`) will cause the machine to lock up completely. It can neither be accessed through LAN nor through a serial connection or the built in, LCD-display-based MMI (man-machine-interface). The only way of getting it back to life is to pull the plug and put it back in.

Link: <http://www.net-security.org/text/bugs/986470239,57678,.shtml>

CISCO CONTENT SERVICES SWITCH VULNERABILITY

The Cisco Content Services (CSS) switch product, also known as Arrowpoint, has a security vulnerability in a previous release that allows non-privileged users to escalate their privilege level, permitting them configuration ability on affected units. This vulnerability can only be exercised from a valid user account. To remove the vulnerability, Cisco is offering free software upgrades to revision 4.01B19s for all affected platforms. This defect is documented as Cisco bug ID CSCdt32570.

Link: <http://www.net-security.org/text/bugs/986470409,87666,.shtml>

DEBIAN FIXES REMOTE ROOT EXPLOIT IN NTP

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. This has been corrected for Debian 2.2 (potato) in ntp version 4.0.99g-2potato1. We recommend you upgrade your ntp package immediately.
Link: <http://www.net-security.org/text/bugs/986506509,167,.shtml>

602PRO LAN SUITE DENIAL OF SERVICE

Connect to lan suite on port 80 with telnet or something and send the following request.

```
GET / HTTP/1.1
```

```
Proxy-Authorization: AAAAAAAAAAAAAA.....
```

Where A x 1033 or more characters, as long as its over 1032, it will work. Lan suite terminates, that means ALL services go with it. And YES you have to restart the program to get everything working. ALL services going again require restart of Lansuite.exe because its dead after it recieves the BAD header
Link: <http://www.net-security.org/text/bugs/986551102,54597,.shtml>

TRUSTIX - LOCAL ROOT EXPLOIT IN KERNEL

Some time ago, a vulnerability was discovered that allowed for root access through ptrace call in the linux kernel. This was originally considered fixed in a previous patch, but as it turns out, it wasn't. This is fixed in kernel version 2.2.19.

Link: <http://www.net-security.org/text/bugs/986551308,48499,.shtml>

WATCHGUARD FIREBOX II KERNEL DOS

This vulnerability makes it possible to force the Firebox into a condition where it stops responding to packets of a certain protocol after it has been sent large bursts of packets for that protocol.

Link: <http://www.net-security.org/text/bugs/986551556,48015,.shtml>

IMMUNIX OS - NTP AND XNTP3 UPDATE

Przemyslaw Frasunek has found a buffer overflow in the ntpd package. The StackGuard protection in Immunix is effective at stopping this attack. If the published exploit is run against the Immunix version, it will cause ntpd to exit with a StackGuard detection message but no penetration vulnerability is possible. WireX is releasing updated packages to prevent the residual DoS attack.

Link: <http://www.net-security.org/text/bugs/986646295,76110,.shtml>

LINUX MANDRAKE - NTP/XNTP3 UPDATE

Link: <http://www.net-security.org/text/bugs/986646364,83413,.shtml>

Security world

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

SYBARI AWARDED "FIVE-STAR" RATING - [02.04.2001]

Sybari Software, Inc., the premier anti-virus and security specialist for groupware solutions, announced its anti-virus solution, Antigen, has earned a five-star rating from SC Magazine. Five is the highest possible rating and indicates the importance of Sybari's anti-virus technology in delivering reliable e-mail security solutions for messaging infrastructures. SC Magazine's product reviews through its West Coast Labs are recognized globally as a prime source in providing functional measures on product effectiveness and performance.

Press release:

< <http://www.net-security.org/text/press/986229209,98816,.shtml> >

THE INTERNET SECURITY CONFERENCE IN JUNE - [02.04.2001]

To be held June 4-8, 2001 at the Century Plaza Hotel in Los Angeles, The Internet Security Conference (TISC) offers a growing cast of the leading experts in the Internet security field. "Say TISC, and security professionals, CTOs and CIOs think quality, uncompromising education," says David Piscitello, TISC conference founder and program chairman. "We came strong out of the gate with some of the most respected security experts in the world - Radia Perlman, Stephen Kent, Tina Darmohray, and Charlie Kaufmann. As the word spreads, TISC is attracting new and rising stars of the Internet Security field to complement our already knowledgeable faculty."

Press release:

< <http://www.net-security.org/text/press/986229300,66109,.shtml> >

LOCKHEED MARTIN AND RIPTECH PARTNER - [02.04.2001]

Lockheed Martin, a proven leader in information technology for both commercial and government clients, today announced a strategic alliance with Riptech Inc., the only provider of real-time managed security services. Through this arrangement, both commercial and government customers will benefit from a seamless offering that combines Riptech's around-the-clock managed security services with Lockheed Martin's broad engineering and consulting expertise.

Press release:

< <http://www.net-security.org/text/press/986229334,85578,.shtml> >

SOPHOS: TOP TN VIRUSES IN MARCH 2001 - [02.04.2001]

This is the latest in a series of monthly charts counting down the ten most frequently occurring viruses as compiled by Sophos, a world leader in corporate anti-virus protection.

Press release:

< <http://www.net-security.org/text/press/986229465,39850,.shtml> >

SECURIFY SECURVANTAGE SERVICES ANNOUNCED - [02.04.2001]

As part of its new strategic direction, Securify, Inc., a leading provider of security technologies and services for connected businesses, today introduced Securify SecurVantage Services, a managed security offering that connected organizations can use to control the quality of security as they extend their network infrastructures and applications to e-partners. By first setting baseline security metrics for "correct" network behavior and then continuously monitoring traffic, Securify SecurVantage Services offer businesses a unique way to verify the ongoing safety of their trust relationships with partners, suppliers and customers - as well as the safety of their Intranet - as they communicate and share critical business information.

Press release:

< <http://www.net-security.org/text/press/986229615,14193,.shtml> >

RSA HELPING GOVERNMENT CUSTOMERS - [03.04.2001]

RSA Security Inc. announced that WareOnEarth Communications, Inc., a leading provider of network security and "Trusted Information Exchange" solutions, has licensed RSA BSAFE Cert-C and RSA BSAFE Cert-J security software. The company has incorporated this software into its Hypership peer-to-peer transport technology, which helps enable trusted information exchange over the Internet. Hypership relies on RSA Security software to help provide a complete public key infrastructure (PKI) solution - including authentication of senders and receivers, data security in transit and at rest, and binding non-repudiation. As a result, WareOnEarth is able to offer its government customers the security they require to leverage the speed and cost advantages of electronic delivery.

Press release:

< <http://www.net-security.org/text/press/986299842,19253,.shtml> >

AUTHENTIFY PROTECTS AGAINST INTERNET FRAUD - [0.04.2001]

Authentify, Inc., an emerging provider of Internet identity solutions, introduced a first-of-its-kind product, Authentify|Register. The company also announced that leading middleware provider mVPN, LLC has integrated Authentify|Register into its mPKI Platform. The integration enables mVPN to provide a crucial layer of security for its e-business customers by providing them an enhanced process for the secure deployment of digital certificates.

Press release:

< <http://www.net-security.org/text/press/986299926,82090,.shtml> >

INTERNET GUARD DOG CAPTURES HIGHEST MARKS - [03.04.2001]

McAfee Consumer Products Division, a business unit of Network Associates, Inc. announced that its Internet Guard Dog software was named Best Filtering Software by Family PC Magazine. Awarded the only "A" grade in a competitive roundup that included CyberPatrol, CyberSitter, NetNanny and SOS Kid Proof, Internet Guard Dog software was deemed "your child's best online friend," earning the highest marks for its easy installation and set-up.

Press release:

< <http://www.net-security.org/text/press/986300214,22309,.shtml> >

F-SECURE AND TELIA ANTIVIRUS DEPLOYMENT - [03.04.2001]

F-Secure Corporation and the Swedish Telia e-bolaget AB in Sweden have signed a cooperation contract. The collaboration will offer a managed anti virus solution to consumers and the small-to-medium businesses. F-Secure Anti-Virus is a component in Telia's service Telia Antivirus. F-Secure Anti Virus provides simple and reliable protection against viruses, e-mail worms and malicious code. F-Secure Anti-Virus with service specifications by Telia, is targeted for Telia's Internet and broadband customers. The service has been available since March 19.

Press release:

< <http://www.net-security.org/text/press/986301407,76377,.shtml> >

CRYPTOSWIFT 400 ECOMMERCE ACCELERATOR OUT - [04.04.2001]

IVEA Technologies, a Rainbow Technologies company and a leading provider of Internet and eCommerce security solutions, debuted the CryptoSwift 400, a new 400 transaction-per-second (TPS) PCI-based eCommerce accelerator that sets a new standard for entry-level cryptographic acceleration for fast, secure online transactions and Web-server performance enhancement. The CryptoSwift 400 optimizes Web-server performance without sacrificing the rapid acceleration of complex and robust encryption processes for today's high-capacity eCommerce Web servers. The new entry-level CryptoSwift 400 allows eCommerce Web sites to handle substantially more traffic, securely, with virtually no end-user waiting.

Press release:

< <http://www.net-security.org/text/press/986381125,42907,.shtml> >

CRYPTOSWIFT EN-2000 ECOMMERCE ACCELERATOR OUT - [04.04.2001]

iVEA Technologies, a Rainbow Technologies company and a leading provider of Internet and eCommerce security solutions, today introduced the CryptoSwift EN-2000, the industry's fastest stand-alone SSL acceleration appliance designed for large business-to-business Web-server farms or high-end data centers when SSL acceleration is shared across multiple servers. The EN-2000 provides up to 2,000 transactions per second (TPS) performance, making it the fastest available SSL acceleration appliance on the market today. The CryptoSwift EN-2000's 100BaseT Ethernet rack-mountable appliance form factor permits high performance security acceleration to scale to a network of servers without consuming additional PCI slots. The EN-2000 offers twice the processing power of the first-generation EN-1000 accelerator and can easily be integrated into all popular server platforms including iPlanet Web Server, Apache, and Microsoft IIS. The large capacity provided by this processing power allows the EN-2000 to scale with the needs of today's ever-growing IT infrastructures. Like other members of iVEA's CryptoSwift family, the EN-2000 works with existing secure Web-server resources and makes an organization's Web server infrastructure investment last longer.

Press release:

< <http://www.net-security.org/text/press/986381216,40945,.shtml> >

DETECT COMPUTER ABUSE WITH BOSS EVERYWARE - [04.04.2001]

Alexander Jmerik has released Boss Everyware v. 2.2, a powerful Windows security program that secretly records data about how your computer is being used. Boss Everyware keeps a log of which programs each user has run, and how much time they've spent on them. In addition, it records all of the users' keystrokes, allowing the computer owner or network administrator to answer questions about what correspondence is being created. Boss Everyware makes it easy to answer questions about what new software has been installed, and what specific web sites are being visited.

Press release:

< <http://www.net-security.org/text/press/986381324,34086,.shtml> >

FORENSICS EXPLORERS INTRODUCES NETWITNESS - [04.04.2001]

Forensics Explorers introduces NetWitness, a suite of products that go far beyond other network security systems and solves problems most network security software cannot even detect. In addition, NetWitness is the only network security system that can guard against the most dangerous and difficult to detect threats: threats from an organization's trusted employees, clients and strategic partners, the people who operate behind the firewall.

Press release:

< <http://www.net-security.org/text/press/986400826,81864,.shtml> >

LOCKHEED MARTIN SPONSORS BIOMETRIC TESTING - [05.04.2001]

Lockheed Martin announced that it is an official sponsor of International Biometric Group's Comparative Biometric Testing. IBG's Comparative Biometric Testing is the de facto industry standard for evaluating the accuracy of leading biometric technologies. Round Three of Testing, to commence later this month, will address the following technical and marketing questions regarding biometrics: How do finger-scan, iris-scan, facial-scan and voice scan technologies compare in terms of accuracy? Within a given technology field, which vendors have the most effective technology? What are the exact accuracy rates that can be expected when applications are rolled out in the field? How easy are biometrics to use?

Press release:

< <http://www.net-security.org/text/press/986483731,80761,.shtml> >

NEW SSL AND PKI ENABLED SECURITY PRODUCTS - [05.04.2001]

Andes Networks, a leading provider of next generation SSL acceleration systems and Chrysalis-ITS, the worldwide leader in the field of high security key protection in PKI, today announced the introduction of a new class of security products for both SSL and PKI enabled security on the Internet. Through the combination of Andes Networks Packetized SSL acceleration technology and FIPS 140-1 validated Ultimate Trust(TM) secure key management technology from Chrysalis-ITS, the companies plan to unveil joint product offerings that will dramatically increase the level of security and scalability associated with delivery of information over the Internet.

Press release:

< <http://www.net-security.org/text/press/986483838,66032,.shtml> >

EDS LAUNCHES CYBER SECURITY INSTITUTE - [05.04.2001]

Continuing its fight against the rising tide of cyber crime, EDS launched its Cyber Security Institute (CSI) - a computer security curriculum to arm IT professionals and consumers with skills to battle hackers, security breaches and viruses. EDS launched the CSI for internal use at COMDEX Fall 2000 in November 2000. As of today, companies and consumers can access the CSI's interactive, on-demand, globally-available courseware. It offers a cost-effective method for training in critical security topics such as secure system administration, firewalls, network security, risk assessment, incident handling and response, threats, vulnerabilities and countermeasures.

Press release:

< <http://www.net-security.org/text/press/986484228,80978,.shtml> >

SOPHOS SHOWS MINISTER ABOUT VIRUS RISKS - [05.04.2001]

Paddy Tipping, Parliamentary Secretary to the Privy Council Office, visited the Abingdon HQ of Sophos Anti-Virus, a world leader in corporate anti-virus protection. The minister used the visit to discuss the needs of fast-growing, hi-tech businesses such as Sophos and to benefit from advice on how organisations can protect against computer viruses. In his role in the Government's Business Coordination Unit, Mr Tipping regularly visits both small and large businesses to discuss their needs and what they feel is required from the Government. As part of the Government's initiative for all UK businesses to be online by 2005, Mr Tipping is keen to listen to the viewpoints of organisations such as Sophos.

Press release:

< <http://www.net-security.org/text/press/986505498,96592,.shtml> >

BIOMETRIC SINGLE SIGN-ON DEMONSTRATION - [06.04.2001]

SAFLINK Corporation, a leading provider of biometric software solutions, and a Computer Associates (CA) Development Partner and Novell Industry Partner, will be attending the upcoming RSA Security Conference to support its partners' presentations of biometric solutions for the enterprise market. The Conference will be held April 8-12 at San Francisco's Moscone Center.

Press release:

< <http://www.net-security.org/text/press/986509672,97322,.shtml> >

VERISIGN CEO TO SPEAK AT RSA 2001 CONFERENCE - [06.04.2001]

Stratton Sclavos will offer a visionary perspective on digital identity and the Internet's central role as an easily accessed, universal locator and repository of personal information. Attendees will walk away with a better understanding on the latest technologies available to deliver robust methods of seamless authentication and trusted transactions on the Internet.

Press release:

< <http://www.net-security.org/text/press/986509820,60827,.shtml> >

AUTHENTIFY TEAMS WITH RSA SECURITY - [06.04.2001]

Authentify, Inc., an emerging provider of Internet identity solutions, announced it has joined the RSA Secured(TM) Partner Program to support interoperability between Authentify|Register service and RSA Keon PKI software.

Authentify|Register delivers real-time authentication of a user's identity during the online registration process. By synchronizing an Internet session with an automated telephone call to the end user, Authentify|Register provides an added level of security to the RSA Keon OneStep(TM) registration process by utilizing the world's most widely deployed infrastructure, the telephone network. The Authentify|Register process is highly scalable and provides an enhanced audit trail for increased security. The automation provided by Authentify|Register reduces costs and eliminates the risk of human error or omission. Authentify's

customizable application provides two-factor authentication and, integrated with RSA Keon OneStep, it allows an organization to quickly, securely and cost-effectively deploy digital certificates.

Press release:

< <http://www.net-security.org/text/press/986509886,31224,.shtml> >

TREND MICRO'S OFFERS OUTLOOK ON VIRUS INDUSTRY - [06.04.2001]

David Perry, global director of education for Trend Micro, Inc., a worldwide leader in network antivirus and Internet content security solutions, will be a featured speaker at the RSA Conference held at San Francisco's Moscone Center. This e-Security Expo will be held April 8-12 and will address the latest issues surrounding current implementations of enterprise security and secure electronic commerce. Perry will be speaking on April 12, at 11 a.m. Given the recent onslaught of viruses, Perry will provide attendees with an analysis of significant malicious code exploits seen thus far in 2001. In addition, Perry will touch on the newest challenges to the security industry, viruses for broadband and wireless, as well as a discussion of the specific solutions that are currently in place to combat these threats. Perry will round out the presentation with suggestions for how to best combat the myths, hypes, hoaxes, and common misperceptions surrounding viruses.

Press release:

< <http://www.net-security.org/text/press/986562195,19617,.shtml> >

NETWORK ICE DE-ROBES LATEST CLOAKING HACK - [06.04.2001]

Network ICE, a leading provider of consumer and corporate intrusion detection systems, has warned users to be wary of a cloaking technique, known as polymorphic coding, designed to disguise buffer overflow code. The camouflage code was revealed at the recent CanSecWest conference in Vancouver, British Columbia by a hacker going by the alias 'K2'. This cloaking technique allows intruders to evade network-based intrusion detection system (IDS's). This is an important development because it means while IDSs may detect the common 'script kiddies', they are useless against the serious, expert hacker.

Press release:

< <http://www.net-security.org/text/press/986562666,36028,.shtml> >

SECUNET SECURITY NETWORKS OPENS SECULAB - [06.04.2001]

Germany's secunet Security Networks AG, one of Europe's leading IT security service companies, announced its entry into the U.S. market with the opening of Seculab, Inc., headquartered in Austin, Texas. Seculab is one of only five Common Criteria testing labs in the United States accredited by the National Security Agency (NSA) and National Institute for Standards and Technology (NIST). Seculab is the world's only Common Criteria lab accredited in both the United States and Europe. In addition to Common Criteria testing, Seculab provides IT security consulting services and has access to secunet's global

network of security experts. Seculab offers client companies services that include security audits, vulnerability assessments and PKI consulting and implementation.

Press release:

< <http://www.net-security.org/text/press/986570488,96969,.shtml> >

MASTERING THE ART OF NETWORKED SECURITY SEMINARS - [06.04.2001]

Rainfinity, the provider of continuous availability software for business transactions over the Internet, in conjunction with Check Point Software, Compaq Computer Corporation, NetIQ and Trend Micro Inc., launched a seminar series entitled 'Mastering the Art of Networked Security.' The focus of the seminar series is to help IT managers learn how to create a more secure enterprise by integrating high availability and security best practices within their server and network infrastructures. The first seminar will take place on April 17, 2001, in Washington, D.C. at the American Institute of Architects. Other seminars will follow throughout April and May 2001 at museums and cultural venues in locations across North America.

Press release:

< <http://www.net-security.org/text/press/986570605,2425,.shtml> >

Featured article

All articles are located at:

<http://www.net-security.org/text/articles>

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

ISSUES: "SAVE A BUG, SAFE A LIFE?" by Thejian

Above exchange, from the novel "Hogfather" by Terry Pratchett, holds quite an accurate description of what hacking is, or at least of the ideal of what hacking should be. That is, to me personally, because one of the things coherent with the scene where this practice thrives is the many different clashing opinions and ideas. You may "smash the stack" for fun, for profit, or maybe just because you're a vicious lil' bugger with too much time on his hands, but the ideal most people have concerning what a hacker is, is someone who opens stuff up to find out the why and the how.

Read more:

< <http://www.net-security.org/text/articles/thejian/bug.shtml> >

Security Software

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

INTRUDER PROTECTION 1.0

Intruder Protection is a program to keep anyone you dont want on your computer off. Whenever the computer is started it will ask for a password before windows starts. If you do not know the password you can not get into the computer. The default password is 0000 you will need to change this to something that you want.

Info/Download:
< <http://www.net-security.org/various/software/986746031,94910,windows.shtml> >

SYGATE PERSONAL FIREWALL 4.0

Sygate Personal Firewall is a bi-directional intrusion defense system for your personal computer. It ensures that your computer is protected from hackers and other intruders while preventing unauthorized programs on your computer from accessing the network. Sygate Personal Firewall makes machines invisible to the outside world. It works on computers connected to a private network or the Internet. This program assures that your business, personal, financial and other data is safe and secure. This version includes advanced active-scan vulnerability assessment to pinpoint your every weakness and fine-tune your security policy.

Info/Download:
< <http://www.net-security.org/various/software/986746226,47831,windows.shtml> >

FREEVSD 1.4.7

FreeVSD facilitates true Linux Virtual Servers within a 'chroot' environment, allowing Web servers and other applications to be deployed and administered discretely, without compromise to security. Each Virtual Server has its own IP address(es), Apache webserver, and view of the process table. FreeVSD expands the Linux system by creating a pseudo-'super user' (admin) for each Virtual Server. The admin user has the ability to create extra POP3/FTP and Telnet users and also administrate vital services such as the webserver.

Info/Download:
< <http://www.net-security.org/various/software/986746661,92183,linux.shtml> >

PROCWATCH

Procwatch is a perl script which watches a /proc filesystem for new processes. When a process is created, procwatch reports the time, the username, the PID, and the binary that was run. Its output is suitable for logging to log files and is geared for system administrators who are testing a new but as yet untrusted UNIX system. Although it cannot detect, and is not proof against, hacked loadable kernel modules that have modified /proc, it is useful in watching for possible rogue binaries.

Info/Download:

< <http://www.net-security.org/various/software/986302285,89785,linux.shtml> >

REMOTE NMAP 0.5.2 BETA

Remote Nmap is a python client/server package which allows many authorized clients to connect to a centralized nmap server to do their port scanning. This could be useful for security companies who want to have all their scans come from a dedicated machine.

Info/Download:

< <http://www.net-security.org/various/software/986746439,36162,linux.shtml> >

Defaced archives

[02.04.2001]

Original: <http://www.efdpac.navfac.navy.mil/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.efdpac.navfac.navy.mil/>

OS: Windows

Original: <http://www.toshiba.cz/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.toshiba.cz/>

OS: IRIX

Original: <http://www.volvo.fr/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.volvo.fr/>

OS: Unknown

Original: <http://www.martini.nl/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.martini.nl/>

OS: Unknown

Original: <http://route.opel.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/02/route.opel.com/>

OS: Windows

Original: <http://www.opelhaendler.de/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.opelhaendler.de/>
OS: Windows

Original: <http://www.canon.co.nz/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.canon.co.nz/>
OS: Windows

Original: <http://www.macromedia.cl/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.macromedia.cl/>
OS: Unknown

Original: <http://www.goodyearmotors.net/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.goodyearmotors.net/>
OS: Windows

Original: <http://www.goodyear.se/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.goodyear.se/>
OS: Windows

Original: <http://webwatch.wsj.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/02/webwatch.wsj.com/>
OS: Windows

Original: <http://www2.disney.go.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www2.disney.go.com/>
OS: Windows

Original: <http://www.toyota-esbjerg.dk/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/02/www.toyota-esbjerg.dk/>
OS: Windows

[03.04.2001]

Original: <http://www.hyundai.co.za/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/03/www.hyundai.co.za/>
OS: Windows

Original: <http://www.btworldwide.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/03/www.btworldwide.com/>
OS: Windows

Original: <http://www.toyota-ghana.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/03/www.toyota-ghana.com/>
OS: Windows

Original: <http://www.toyota-ep.co.jp/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/03/www.toyota-ep.co.jp/>
OS: Unknown

Original: <http://thestore.sonymusic.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/03/thestore.sonymusic.com/>
OS: Unknown

Original: <http://www.ace.bridgestone.co.jp/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/03/www.ace.bridgestone.co.jp/>
OS: Windows

Original: <http://cfdev.wwf.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/03/cfdev.wwf.com/>
OS: Windows

[04.04.2001]

Original: <http://www.mitsubishi-engine.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/04/www.mitsubishi-engine.com/>
OS: Windows

Original: <http://www.mitsubishi-electric.it/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/04/www.mitsubishi-electric.it/>
OS: Windows

Original: <http://3mdweb.3com.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/04/3mdweb.3com.com/>
OS: Windows

Original: <http://www.delphi.fi/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/04/www.delphi.fi/>
OS: Windows

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

[05.04.2001]

Original: <http://restaurantrow.lycos.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/05/restaurantrow.lycos.com/>
OS: Windows

Original: <http://www.activebuyersguide.looksmart.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/05/www.activebuyersguide.looksmart.com/>
OS: Windows

Original: <http://www.compaq-novell.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/05/www.compaq-novell.com/>
OS: Windows

Original: <http://www.compaq-ontraq.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/05/www.compaq-ontraq.com/>
OS: Windows

Original: <http://www.polizei.co.at/>
Defaced: <http://defaced.alldas.de/mirror/2001/04/05/www.polizei.co.at/>
OS: Unknown

[06.04.2001]

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

Defaced: <http://defaced.alldas.de/mirror/2001/04/06/www.packardbell.com.my/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/04/06/www.xerox.com.cn/>

OS: Windows

Original: <http://www.compaq-signup.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/06/www.compaq-signup.com/>

OS: Windows

Original: <http://www.compaq-pshk.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/06/www.compaq-pshk.com/>

OS: Windows

[07.04.2001]

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

Defaced: <http://defaced.alldas.de/mirror/2001/04/07/www.sony-center.ch/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/04/07/www.quiksilver.com/>

OS: Windows

Original: <http://www.bc.gov.cu/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/07/www.bc.gov.cu/>

OS: Unknown

[08.04.2001]

Original: <http://www.casio.co.id/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/08/www.casio.co.id/>

OS: Windows

Original: <http://3comleads.3com.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/08/3comleads.3com.com/>

OS: Windows

Original: <http://www.shell.se/>

Defaced: <http://defaced.alldas.de/mirror/2001/04/08/www.shell.se/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/04/08/www.sony-center.ch/>

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>