

HNS Newsletter
Issue 56 - 26.03.2001
<http://net-security.org>
<http://security-db.com>

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

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

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

Current subscriber count to this digest: 2085

Table of contents:

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

General security news

FBI ISSUES WARNING OVER 'STICK'

The Internet crime division of the FBI issued a vaguely-worded warning last week about an alarming new tool soon to be available to computer criminals. The tool--called "Stick" - essentially disarms intrusion detection systems...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2697767,00.html>

PGP DESKTOP SECURITY

PGP Desktop Security 7.0 is the first and only security product to combine personal firewall, intrusion detection, VPN client, and encryption technologies into a single solution that fully protects computers against intruders and theft/loss of data.

Link: <http://www.security-db.com/product.php?id=115&cid=23>

BUILDING A BRIDGING FIREWALL WITH LINUX

"The Linux kernels v2.2 and higher have support for Ethernet bridging. In a bridge, all packets received by one interface are passed to the other, without regard to source or destination IP address, by examining the Ethernet MAC destination address of the packet. AC2I, a French company, distributes a kernel patch that allows the ipchains packet filter to work on the bridged interfaces. This configuration allows you to set up a firewall system that is invisible to the Internet, yet provides a high level of protection and access control for your private network. The remainder of this article explains the

steps necessary to get a bridging firewall up and running."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/articles/misc/0041.html>

REALIZING COMPUTER SECURITY: IF NOT NOW, WHEN?

Security is increasingly recognized as a necessity in today's highly competitive environment. The trouble is that in practice, corporate security policies too often pay only lip service to protecting data assets; in one security analysis in my own practice, a corporate security policy consisted solely of the statement, "The Company recognizes the importance of security in its operations."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/securitynow20010319.html>

PC CARD GIVES NOTEBOOK THIEVES THE FINGER

Toshiba has moved a touch closer to the future as depicted by sci-fi films with the release of a fingerprint reader for notebooks. The imaginatively titled Fingerprint Reader is a PC card and will fit into any Type II slot. A fingerprint reader is nothing new but Toshiba claims this one is the best so far for security as it works at the BIOS level, rather than on top.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17731.html>

LITTLE DAMAGE DONE BY PRO-PALESTINIAN VIRUS

A handful of companies have been hit by a computer virus named Injustice that causes a victim's computer to send pro-Palestinian messages to 25 Israeli organizations and government agencies. The worm is largely benign and does not damage data on the infected PC, but the flurry of e-mails it sends to other computers could swamp a business' network, said Ian Hameroff, business manager for security solutions at antivirus and PC services company Computer Associates.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-5185169.html>

COMPILING THE FREEBSD KERNEL

As with the Linux kernel, compiling the FreeBSD kernel is something of an essential skill. The newly compiled kernel will give you access to your new hardware. It will be your custom configuration. And finally, it will elevate you a couple of points up the Guru scale. Read on for more on how you can achieve all of the above.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/3827/>

REALISTIC EXPECTATIONS FOR INTRUSION DETECTION SYSTEMS

The emergence of IDSs causes some security commentators to see them as a panacea, solving all of the complex and diverse threats to network security. However, as does any weapon in the security arsenal, an IDS has limited capabilities. To expect too much of an IDS places the user's network at risk. This article will discuss reasonable expectations of Intrusion Detection Systems (IDSs). Its purpose is to help users and potential users realize the increasing importance of intrusion detection in all organizations, while also pointing out the realistic outcomes to be expected from current IDS products. It will also discuss those expectations that users may have of intrusion detection systems

that are unrealistic and, as such, may threaten the security of the user's network.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ids/articles/expect.html>

FORENSIC CHALLENGE ENDED

Honeynet Project Forensic Challenge is finished. Organizers received 13 submissions from around the world and one team spent a total of 104 hours on their analysis...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://project.honeynet.org/challenge/results/>

RANDOM PASSWORD GENERATION

If you let users sign up for accounts online, most likely you will be automatically giving them temporary passwords after signup. Sometimes these passwords are given out through email or instantly presented on a web page.

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

PRIVACY SERIES - OVERVIEW

There has been a lot of news and noise about privacy online lately. Some people seem to be getting very concerned that their online activities might be monitored. As with many public issues, the focus is on the simple and mostly harmless aspects of the problem. The really nasty issues are quietly being largely ignored; in fact, most people are blissfully unaware of them. This is unfortunate because as privacy erodes, people will become used to the process, thus allowing it to erode further. This is the first article in a series that I plan to work on over the next few weeks or months.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010321.html>

BOB TOXEN'S LINUX SECURITY TIPS

Bob Toxen, the author of Real World Linux Security: Intrusion Prevention, Detection, and Recovery, boasts an impressive résumé as a writer, developer, creator, and software architect. Cameron Laird conducted a lively discussion with Toxen on security, Linux hacking, open source development, and more.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/linuxworld/lw-2001-03/lw-03-toxen.html>

ASSOCIATED PRESS SITE ATTACKED

The Associated Press (AP) overnight joined the lengthening list of sites struck by a Brazilian group of defacers... The news organization said its AP.org site was attacked about 2:19 AM ET. The site carries information about the AP's products and services.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-5202358.html>

PGP INVENTOR SAYS ENCRYPTION FLAW MINOR

A flaw found by two Czech researchers in the popular OpenPGP digital signature standard is real but relatively minor according to Phil Zimmermann, chairman of the open-source group.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-5208418.html>

INFORMATION DISCOVERY - SEARCHING AND PROCESSING

This is the eighth and final article in SecurityFocus.com writer Timothy Wright's Field Guide for Investigating Computer Crime. The last installment introduced the basics for the information discovery process. It then discussed three basic rules of thumb that should act as guides for any information discovery, mentioning along the way how each rule has a parallel in the world of physical search and seizure. This installment will bring the series to a close by examining the final two stages - searching for and processing data evidence.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/ih/articles/crimeguide8.html>

HOW TO HACK

"The first class of attackers probably forms more than 95% of the population, and are often referred to as "script-kiddies". Beyond being able to use a computer and having a very basic knowledge of networks and operating systems, script-kiddies do not have much skill. They typically download packaged software (and in some cases, precompiled software) that they then use to attack other computers. Often, they do not even know how the software works, other than it will allow them to gain access to other computers, or deny use of remote services (by crashing the machine or simply flooding the link it is on)."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.samag.com/articles/2000/0011/0011e/0011e.htm>

INTERNET SECURITY FIRMS HANGING TOUGH

Internet security companies, which specialize in deterring hackers, setting up firewalls and delivering virtual private networks to corporations, are allegedly recession resistant. The consensus view is that security is needed to keep e-business moving. It's a necessity. But shares in companies such as Check Point Software, Internet Security Systems and Netegrity have taken their lumps of late as Wall Street frets about possible profit warnings.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-5207856.html>

FBI'S CYBERDEFENSE UNIT GETS NEW LEADER

The FBI appointed one of its veteran investigators to head the bureau's cyberdefense unit, as security experts and lawmakers on Capitol Hill continue to debate how best to organize federal efforts to protect the nation's critical infrastructure from a devastating cyberattack. FBI Director Louis Freeh announced the appointment of Ronald Dick as the new head of the National Infrastructure Protection Center (NIPC).

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://computerworld.com/cwi/story/0,1199,NAV47_STO58837,00.html

DEFACED: UK GOVT, EBAY, COMPAQ

The Register reports that several United Kingdom Government sites got defaced. Govtalk.gov.uk was the hackers' main target as in particularly embarrassing because that it is the site used by e-envoy Andrew Pinder to discuss within government how to bring about the e-revolution. Also Alldas.de mirror list shows that a subdomain on eBay.com was attacked today. Apocalypse Dow contributed that Alldas.de, today mirrored two Compaq defacements...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17778.html>

GERMANS LAUNCH \$5,000 CEBIT HACKER CHALLENGE

A German computer security firm is inviting hackers to break into its products live at this year's CeBIT computer fair. Wibu will place its reputation on the line by asking a group of "ethical" hackers to crack a file scrambled with its encryption technology. Although the event has been decried as little more than a publicity stunt by one UK computer security expert, it is sure to draw a crowd at this year's show: the company is offering a prize of \$5,000 to any hacker that can break its copy protection system and decrypt a hidden message.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2001/11/ns-21758.html>

DEVELOPERS CALL FOR WEB SECURITY STANDARD

A group of security developers has called for an industry standard for internet security testing. The group, called Ideahamster, which includes a mixture of security experts and developers, has suggested that the introduction of such a standard would make it easier for users to judge security products. Security firms currently use a number of different methodologies for testing their products.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thebusiness.vnunet.com/News/1119548>

EUROPEAN PARLIAMENT CONTINUES ECHELON INVESTIGATION

The European Parliament will continue its investigation into the Echelon spying system today in Brussels. A temporary committee was set up half way through last year when reports of the US, UK, Australia and New Zealand-sponsored spying system entered wide circulation. The European Parliament will decide what it should do regarding Echelon in a series of meetings, the second set of which started today. The French are particularly upset about the spying system - mostly because they're not part of it - and have started up their own rival system. They also ran their own investigation into whether Echelon has been used to spy on and influence important international business decisions. The report decided they did and asked for greater encryption in Europe.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/8/17800.html>

MICROSOFT WARNS OF HIJACKED CERTIFICATES

Two digital certificates have been mistakenly issued in Microsoft's name that could be used by virus writers to fool people into running harmful programs. In this case, a person using the VeriSign-issued certificates could post a virus on the Web that would appear to be from Microsoft but could actually be used to wipe out a person's hard drive, for example.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-5222484.html>

AN INTRODUCTION TO WEBLOGIC SERVER 6.0 FOR LINUX

If you develop Java on Linux, there is a good chance that you use WebLogic. Discover the new features in version 6.0 and find tips on installing, configuring and deploying that widely used server.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/linuxworld/lw-2001-03/lw-03-weblogic.html>

GETTING STARTED WITH TRIPWIRE

In this feature story, F. William Lynch outlines how to install and configure Tripwire, Open Source Linux Edition. Tripwire is a very effective host intrusion detection system. A crude yet effective intrusion detection system such as Tripwire can alert systems administrators to possible intrusion attempts by periodically verifying the integrity of a server's file systems. Systems intruders will often use trojan binaries for login, su, ps, and ls, etc. to cover their tracks and keep a low profile on the system. Under normal circumstances even astute systems administrators may not observe the intrusion because the trojan binaries mimic the system binaries so well.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/feature_stories/feature_story-81.html

APACHE INSECURITY REVEALS DIRECTORY CONTENTS

This weeks Security Alerts is out. "In this column, we look at buffer overflows in icecast, Half-Life Dedicated Server, Solaris SNMP, ipop2d, ipop3d, and imapd; format string vulnerabilities in icecast, mutt, Half-Life Dedicated Server, and cfengine; temporary-file problems in the SGML-Tools package and Mesa; and problems with Apache, several FTP daemons, a Solaris SNMP agent, vBulletin, FTPFS, and Ikonboard."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.oreillynet.com/pub/a/linux/2001/03/20/insecurities.html>

NSA'S RICE CALLS FOR JOINT WEB SECURITY EFFORT

The protection of the American infrastructure is an important part of the agenda of the National Security Council, according to President Bush's National Security Advisor, Condoleezza Rice. Speaking to industry and government leaders at the Partnership for Critical Infrastructure of the US Chamber of Commerce annual meeting in Washington, Rice said, "Today, the cyber economy is the economy. And I don't mean the dot-coms. I mean virtually every vital service - water supply, transportation, energy, banking and finance, telecommunications, public health. All of these rely upon computers and the fiber-optic lines, switchers and routers that connect them."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/163535.html>

CEBIT - LET'S GO WIRELESS - WITH SECURITY, TOO

Cellular or wireless communications is seen as a hostile environment for security, mainly because it's a radio-based platform. Most mobile phones use firmware-based software, and it's difficult to authenticate a mobile user reliably without less than seamless technology. Now, Baltimore Technologies is teaming with Gemplus, the smart card vendor, and AU Systems, the firm behind Ericsson's WAP technology, to offer what it says is the world's first digital signature system that works over high-speed wireless networks such as GPRS.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/163542.html>

MS PLANS A "SECURE PC" FOR AUDIO FILES

Microsoft's research division is busily inventing a mysterious beast called the Secure PC, which is designed to win hearts, minds and wallets in the recording industry by blocking unlicensed copying of digital music. We know that the Secure PC exists at least as a concept, because it's listed as a project of Microsoft research's cryptography group.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/4/17851.html>

"LION" WORM COULD CAUSE SERIOUS DAMAGE

Lion is similar to the Ramen worm. However, this worm is significantly more dangerous and should be taken very seriously. It infects Linux machines running the BIND DNS server. It is known to infect bind version(s) 8.2, 8.2-P1, 8.2.1, 8.2.2-Px, and all 8.2.3-betas. The specific vulnerability used by the worm to exploit machines is the TSIG vulnerability that was reported on January 29, 2001. The Lion worm spreads via an application called "randb". Randb scans random class B networks probing TCP port 53. Once it hits a system, it checks to see if it is vulnerable. If so, Lion exploits the system using an exploit called "name". It then installs the t0rn rootkit which enables the attacker to wreak havoc on the compromised machine.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sans.org/y2k/lion.htm>

SECURITY ALERT SHAKES UP VERISIGN

The security alert raised on Thursday by Verisign, after an individual posing as a Microsoft employee managed to obtain two digital certificates, or online signatures, has served only to compound existing fears.

Link: <http://www.marketsandexchanges.com/index.asp?news=13490>

ATTACKS ON GOVERNMENT SITES

Silicon reports that Government websites receive around 100,000 hits from various cyber attackers every day. The source in this story, a former government intelligence expert, said that around 30 per cent of these are classified as "serious".

Link:

<http://www.silicon.com/public/door?REQUNIQ=985389196&6004REQEVENT=&REQINT1=43446&REQSTR1>

OPEN SOURCE SECURITY

Network security appliances generally offer firewalling and/or virtual private networking, and perhaps other services such as single sign-on (SSO) or content filtering. Any or all of these functions are easily provided with almost any open-source BSD-based OS or Linux. For example, Cobalt Networks uses Red Hat Linux as its base OS. WireX Communications adapts and hardens Red Hat Linux and then packages it into a software network appliance that can be licensed for resale.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/march01/features1_open_source_sec.shtml

FAQ: MICROSOFT'S SECURITY BREACH

After two digital certificates were mistakenly issued in Microsoft's name, consumers may wonder if they are now vulnerable to downloading software

from less-than-safe sources. Here are some frequently asked questions about how digital signatures work, and the risks of downloading software from the Internet.

Link: http://www.zdii.com/industry_list.asp?mode=news&doc_id=ZD5080023

P3P PRIVACY SUPPORT TO APPEAR IN EXPLORER

Microsoft has again committed itself to releasing a version of IE that includes support for open standards that can make such software respond automatically to a Web site's privacy policies. The Platform for Privacy Preferences Project (P3P) has long been touted as offering Web surfers an opportunity to take control of their personal information online, arming browser software with the ability to scope out a site's approach to privacy before loading a single page. However, the effort, led by the World Wide Web Consortium (W3C), has languished while supporters waited for Web sites and browser makers to implement the P3P protocols.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/01/03/23/news3.html>

A BRIEF COMPARISON OF EMAIL ENCRYPTION PROTOCOLS

"This document briefly reviews and compares five major email encryption protocols under consideration: MOSS, MSP, PGP, PGP/MIME, and S/MIME. Each is capable of adequate security, but also suffers from the lack of good implementation, in the context of transparent email encryption. I will try to address issues of underlying cryptographic soundness, ease of integration with email, implementation issues, support for multimedia and Web datatypes, and backwards compatibility."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.arraydev.com/commerce/JIBC/9603-2.htm>

ACQUIRING PKI

Discussions on public key infrastructure (PKI) usually focus on the complexities of its underlying technology or the difficulties of implementing it in a live setting. Given the current state of PKI, it's no wonder these areas have consumed so much of our attention. While PKI in theory provides an effective, robust means of securing electronic communications and transactions, deploying and managing the technology remains a daunting challenge to many organizations.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/articles/march01/features3_pki.shtml

THE COMPLETE LINUX SHELL PROGRAMMING TRAINING COURSE

The book is intended primarily as an entry-level teaching text, but because topics are from the outset presented in extreme detail, it is probably not appropriate to the total neophyte. According to the welcome movie in the courseware, the authors assume only that you have a working knowledge of some Unix text editor. In fact, you should probably be familiar with either vi or emacs. If your only previous experience has been with a visual editor such as gedit, you may find some of the jargon in the first few chapters unfamiliar. Even though there are some reference materials in the appendices, (specifically, command references for several utilities and a concise comparison of several shells), the book is clearly a teaching text and not a reference work.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://unixreview.com/reviews/articles/software/0103linuxshell.shtml>

Security issues

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

TRUSTIX SECURE LINUX - MUTT UPDATE

This release fixes at least one grave IMAP error which may lead to confusing display and other strangeness, and our instances of the "wuftpd format bug", which had (mostly) the effect that your IMAP server's operator could break into your computer with some work.

Link: <http://www.net-security.org/text/bugs/985136109,86701,.shtml>

CONNECTIVA - REMOTE BUFFER OVERFLOW IN IMAP

"imap" is a package which contains POP3 and IMAP mail servers. Several buffer overflow vulnerabilities have been found in this package by their authors and by independent groups.

Link: <http://www.net-security.org/text/bugs/985136159,13868,.shtml>

REMOTE BUFFER OVERFLOW IN ICECAST

Our latest update to this software changes the package to use an unprivileged user ("icecast") for the daemon, so the impact of this vulnerability is not as high. Recent distributions (CL >= 5.1) have this package compiled with StackGuard to make it more difficult to exploit buffer overflows. All icecast users are urged to upgrade.

Link: <http://www.net-security.org/text/bugs/985136439,63985,.shtml>

MICROSOFT PWS UNICODE VULNERABILITY

"Just wanted to point out that while testing my Default installation of Windows 98 running Microsoft Personal Web Server that came with the Windows98 SE CD I discovered that the famous IIS 4/5 Unicode Directory Traversal Vulnerability applies also to this Server just as bad as in IIS."

Link: <http://www.net-security.org/text/bugs/985136954,14208,.shtml>

PROBLEMS WITH EUDORA 5.02

Silent delivery and installation of an executable on a target computer. No client input other than opening an email using Eudora 5.02 - Sponsored Mode provided 'use Microsoft viewer' and 'allow executables in HTML content' are enabled.

Link: <http://www.net-security.org/text/bugs/985136999,53955,.shtml>

WEBSERVER PRO VULNERABILITY

Website Pro, all versions, reveals the web directory with a simple character similar to the past vulnerability but all have been fixed except this one.

Link: <http://www.net-security.org/text/bugs/985137021,24388,.shtml>

RPM-4.0.2 FOR ALL RED HAT PLATFORMS

A common version of rpm for all Red Hat distributions is being released. This version of rpm understands legacy version 3 packaging used in Red Hat 6.x/5.x distributions as well as version 4 packaging used in Red Hat 7.x. In addition, rpm-4.0.2 has support for both the legacy db1 format used in Red Hat 6.x/5.x databases as well as support for the db3 format database used in Red Hat 7.x
Link: <http://www.net-security.org/text/bugs/985258597,16357,.shtml>

LINUX MANDRAKE - LICQ PROBLEMS

Versions of Licq prior to 1.0.3 have a vulnerability involving the way Licq parses received URLs. The received URLs are passed to the web browser without any sanity checking by using the system() function. Because of the lack of checks on the URL, remote attackers can pipe other commands with the sent URLs causing the client to unwillingly execute arbitrary commands. The URL parsing code has been fixed in the most recent 1.0.3 version.

Link: <http://www.net-security.org/text/bugs/985258666,52078,.shtml>

RED HAT LINUX - UPDATED LICQ PACKAGES

Link: <http://www.net-security.org/text/bugs/985355306,89514,.shtml>

SURFCONTROL BYPASS VULNERABILITY

It appears that there is yet another way to bypass the site blocking feature of SurfControl for MS Proxy.

Link: <http://www.net-security.org/text/bugs/985259149,80992,.shtml>

REDI STORES PASSWORDS IN CLEAR TEXT

User name and password are stored in a clear text file on the users computer every time the user logs in. The file, defaulting to E:\Program Files\SLK\REDI\Logon\StartLog.txt contains information about the programs startup useful for troubleshooting.

Link: <http://www.net-security.org/text/bugs/985259229,51161,.shtml>

SUSE LINUX - POP UPDATE

The eMail access daemons imapd(8), ipop2d(8) and ipop3d(8) of SuSE 6.1 are vulnerable to several buffer overflows. Due to a misconfiguration these vulnerabilities could be triggered remotely after a user had been authenticated.

Link: <http://www.net-security.org/text/bugs/985355413,14944,.shtml>

SUSE LINUX - NKITB/NKITSERV UPDATE

Two parts of the nkitb/nkitserv package are vulnerable to security related bugs. in.ftpd(8): A one-byte bufferoverflow was discovered in the OpenBSD port of the FTP daemon in.ftpd(8) several weeks ago. This bug could just be triggered by authenticated users, which have write access. This bug is believed to not be exploitable under Linux. However, we prefer to provide a fixed update package to make sure that the daemon is on the safe side.

in.ftpd(8) will be invoked by inetd(8) and is activated by default.

timed(8): The time server daemon timed(8), which is started at boot time, tries to synchronize the local host time with the time of other machines on the local area network.

A bug in timed(8) was reported by the FreeBSD Security Officer, that could be triggered remotely to crash the time server daemon.

Link: <http://www.net-security.org/text/bugs/985355486,67630,.shtml>

COMPAQ INSIGHT MANAGER PROXY VULNERABILITY

Compaq Insight Manager has a serious configuration issue which allows the use of the software as a proxy server. No logging is performed on either the OS or app., making this a perfect anonymous proxy.

Link: <http://www.net-security.org/text/bugs/985355516,2948,.shtml>

WINDOWS SHARING ALLOWS TRACKING

As long as you can monitor others, there are others that will be able to monitor you. Here's a possible scenario: You were given access to an NT Server via shares just to do some tweaks or whatever. You leave in peace and go back to the rest of your work. What you just did was leave traces of online receipts, cookies, etc., without even knowing it. Part of the problem is that, to my knowledge, there is no option from stopping this from happening, so the cleansing of the transferred cache must be done manually. One minor setting that can contribute to defending from this problem is to enable the "Temporary Internet Files clean on closing" option in Internet Explorer 5x.

Link: <http://www.net-security.org/text/bugs/985355546,32327,.shtml>

Security world

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

FIRST ENTERPRISE LEVEL PDA SECURITY PRODUCT - [19.03.2001]

Trust Digital LLC, a recently formed subsidiary of Applied Technologies, Inc., announced that it would formally release the first enterprise capable data security product for PDA handheld devices at the FOSE trade show in Washington, DC. The new product, PDASecure, secures handheld devices that use the Palm Operating System (OS). The product uses the newly established Advanced Encryption Standard (AES) based on the Rijndael or "Rain Doll" algorithm, selected in a competition by the National Institute of Standards and Technology (NIST).

Press release:

< <http://www.net-security.org/text/press/984972585,90929,.shtml> >

SOPHOS: NO FEAR FROM INJUSTICE WORM - [21.03.2001]

Sophos, a world leader in corporate anti-virus protection, has advised computer users that there is no need to panic following reports of the latest email-aware computer worm. So far Sophos has received just a single report of the worm in the wild, but - as it is self replicating and has the potential to spread quickly -

users are advised to be cautious of suspicious looking emails and to ensure they have up to date anti-virus protection.

Press release:

< <http://www.net-security.org/text/press/985137079,33528,.shtml> >

NO.1 MID-RANGE VPN HARDWARE SOLUTION - [21.03.2001]

WatchGuard Technologies, Inc., a leader in Internet security solutions, announced that Infonetics Research has named WatchGuard the revenue market share leader in mid-range VPN hardware. According to the February 2001 Infonetics report, "VPN Hardware and Software," WatchGuard owned 20% of the market in 2000, earning the top spot as the No. 1 revenue generating mid-range VPN hardware. WatchGuard prevailed as the leader, consistently generating more revenue quarter-over-quarter than Intel, Lucent, Netscreen, Nortel, Red Creek, SafeNet and SonicWall.

Press release:

< <http://www.net-security.org/text/press/985137545,21129,.shtml> >

INFO ON MOBILE COMMUNICATIONS SECURITY - [22.03.2001]

F-Secure Corporation and Sonera Zed Ltd. announced a strategic agreement to cooperate in the development, production and licensing of security solutions for value added mobile communication services. Under the arrangement, Sonera Zed will offer F-Secure products to existing and prospective zed for business customers as well as test and evaluate F-Secure products and platforms. The companies will initially focus on content security solutions for wireless infrastructure, starting with the integration of F-Secure Anti-Virus for WAP Gateways into zed's mobile business services offering.

Press release:

< <http://www.net-security.org/text/press/985258482,43891,.shtml> >

BALTIMORE LAUNCHES SUREWARE RUNNER - [23.03.2001]

Baltimore Technologies, a global leader in e-security, announced availability of Baltimore SureWare Runner, the latest product in its next generation hardware security range. SureWare Runner provides enhanced security and performance for Web Servers utilising the Secure Sockets Layer (SSL) protocol, accelerating the speed of connection and accessibility for customers using online services.

Press release:

< <http://www.net-security.org/text/press/985354578,93110,.shtml> >

STONESOFT ANNOUNCES STONEGATE FIREWALL - [23.03.2001]

Stonesoft Corporation, a leading provider of enterprise-level security and high availability software solutions, today announced StoneGate, its fully scalable

Firewall and VPN solution for large-scale enterprises, service providers and carriers. The StoneGate Firewall and VPN provides maximum network and VPN security as it includes all the latest secure firewall features and adds Stonesoft's proven high availability, high throughput and advanced, enterprise wide management. StoneGate, with its revolutionary Multi-Link technology, is the industry's first firewall to enable end-to-end high availability and security from the corporate intranet out to multiple ISP connections. With the StoneGate Firewall and VPN, Stonesoft delivers upon its vision for the Secure, Highly Available Enterprise.

Press release:

< <http://www.net-security.org/text/press/985355137,16829,.shtml> >

RSA SECURITY SELECTED BY ESPEED - [23.03.2001]

Continuing its momentum in the B2B marketplace, RSA Security Inc. announced that eSpeed, Inc., a leading interactive electronic marketplace engine for business-to-business (B2B) e-commerce, has licensed RSA BSAFE SSL-C software for incorporation into its eSpeedsm platform. RSA BSAFE SSL-C software will further enhance eSpeed's ability to provide its customers the comprehensive security solution they require to operate highly secure marketplaces and trading communities. "We recognize RSA Security as a leader in its market, and are proud to incorporate RSA BSAFE SSL-C software into our eSpeedsm platform," said Joe Noviello, chief technology officer of eSpeed.

Press release:

< <http://www.net-security.org/text/press/985355200,42067,.shtml> >

GLOBALSIGN PARTNERS WITH E-TELBank - [23.03.2001]

GlobalSign, a leading Trust Services Provider for Internet-based transactions, is signing a partnership with E-Telbank, a new company owned for 100% by BPT Telbank, number one data network operator in Poland, providing telecommunication services for the Polish banking and financial sector. This new partnership enables E-Telbank to issue different types of certificates to all Telbank customers setting through GlobalSign MyVirtualCA solution. My VirtualCA is a customised Public Key Infrastructure (PKI) solution that delivers Certification Authority capabilities to the customer, tailored to address Telbank's unique PKI-requirements. This solution will be implemented as a first stage of the Strategic Licensing ProgramTM. With this partnership, GlobalSign realises its first steps on the Polish market and acquires hence an important opening to Central and East-European market. Moreover, the partnership confirms the success of outsourced PKI solutions to the financial sector. This major contract represents a starting value of 200.000 Euro and is set to grow significantly as the amount of delivered certificates will increase rapidly.

Press release:

< <http://www.net-security.org/text/press/985358579,42653,.shtml> >

Featured articles

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

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

Below is the list of the recently added articles.

ANALYSIS OF VENDOR ACKNOWLEDGEMENT OF VULNERABILITIES

"Many disclosure debates focus on researchers who discover vulnerabilities. Little attention is given to the impact on busy security analysts who must determine which vulnerabilities exist, and if they can be patched. There is little or no emphasis on the role of vendors of the vulnerable software. Given continued discussions of vulnerability disclosure practices, most recently regarding vendor contacts on the PEN-TEST list, we decided to offer some results of an informal analysis we performed in October 2000. We also make some recommendations for improvements."

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

ATTACK ON PRIVATE SIGNATURE KEYS OF THE OPENPGP FORMAT, PGP PROGRAMS AND OTHER APPLICATIONS COMPATIBLE WITH OPENPGP

The article describes an attack on OpenPGP format, which leads to disclosure of the private signature keys of the DSA and RSA algorithms. The OpenPGP format is used in a number of applications including PGP, GNU Privacy Guard and other programs specified on the list of products compatible with OpenPGP. Therefore all these applications must undergo the same revision as the actual program PGP. The success of the attack was practically verified and demonstrated on the PGP program, version 7.0.3 with a combination of AES and DH/DSS algorithms. As the private signature key is the basic information of the whole system which is kept secret, it is encrypted using the strong cipher. However, it shows that this protection is illusory, as the attacker has neither to attack this cipher nor user's secret passphrase.

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

Security Software

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

SECURETROY 2.14

From the developer: "SecureTroy is the ultimate internet security suite. It offers extremely high protection against hackers and is able to detect attempts by hackers to break into your system. It also includes many useful utilities that give you more control over your system.

Info/Download:

< <http://www.net-security.org/various/software/985563243,24735,windows.shtml> >

SIMPROBE CODER V4 4.05

From the developer: "with coder v4 you can encrypt and decrypt files with your own passwords. It supports any files that are on your computer. It has compression support and plenty more features including Auto-Update. Coder v4 is totally free!

Info/Download:

< <http://www.net-security.org/various/software/985563353,4688,windows.shtml> >

COLD FUSION ENCRYPTOR 1.51

Tired for typing DOS command and finding the correct path to encrypt your Cold Fusion application? This is a program that give you the ability to encrypt all your scripts that you have wrote just in one click. It's work as an assitance tool with cfencode.exe which provided by Allaire to perform the task. With backup feature and 2000/NT bug fixed.

Info/Download:

< <http://www.net-security.org/various/software/985563468,6455,windows.shtml> >

ZORP 0.8.0

Zorp is a new-generation modular proxy firewall suite to fine tune proxy decisions with its built in script language, fully analyze complex protocols (like SSH with several forwarded TCP connections), and utilize out of band authentication techniques (unlike common practices where proxy authentication had to be hacked into the protocol).

Info/Download:

< <http://www.net-security.org/various/software/985563626,80206,linux.shtml> >

Defaced archives

[19.03.2001]

Original: <http://www.selcuklu-bld.gov.tr/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/19/www.selcuklu-bld.gov.tr/>

OS: Windows

Original: <http://www.izmirpolis.gov.tr/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/19/www.izmirpolis.gov.tr/>

OS: Windows

Original: <http://www.airtc.defence.gov.au/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/19/www.airtc.defence.gov.au/>

OS: Windows

Original: <http://www.saude.ce.gov.br/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/19/www.saude.ce.gov.br/>

OS: Windows

Original: <http://www.energy.gov.tt/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/19/www.energy.gov.tt/>

OS: Unknown

[20.03.2001]

Original: <http://www.alcatel.altech.co.za/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/20/www.alcatel.altech.co.za/>

OS: Windows

Original: <http://www.manuscripts.idsc.gov.eg/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/20/www.manuscripts.idsc.gov.eg/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/03/20/www.threestooges.com/>

OS: Windows

Original: <http://www.citroen.co.th/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/20/www.citroen.co.th/>

OS: Windows

[21.03.2001]

Original: <http://booksrv2.raleigh.ibm.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/21/booksrv2.raleigh.ibm.com/>

OS: Windows

Original: <http://www.parkinsons-foundation.org/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/21/www.parkinsons-foundation.org/>

OS: Windows

Original: <http://www.nas.gov.uk/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/21/www.nas.gov.uk/>

OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/03/21/www.linuxerfer.com/>

OS: Linux

Original: <http://www.ml-mpsj.gov.my/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/21/www.ml-mpsj.gov.my/>

OS: Windows

Original: <http://www.hp.co.za/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/21/www.hp.co.za/>

OS: Windows

Original: <http://www.linux.hu/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/21/www.linux.hu/>

OS: Linux

[22.03.2001]

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

Defaced: <http://defaced.alldas.de/mirror/2001/03/22/www.ericsson.ly/>

OS: Unknown

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

Defaced: <http://defaced.alldas.de/mirror/2001/03/22/www.suzukicars.co.uk/>

OS: Windows

Original: <http://www.qa.ebay.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/22/www.qa.ebay.com/>

OS: Unknown

Original: <http://www.ols2.software-acq.compaq.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/22/www.ols2.software-acq.compaq.com/>

OS: Windows

Original: <http://lotus.carepaq.emea.compaq.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/22/lotus.carepaq.emea.compaq.com/>

OS: Windows

Original: <http://server2.acu4.spear.navy.mil/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/22/server2.acu4.spear.navy.mil/>

OS: Windows

[23.03.2001]

Original: <http://www.epson.com.ve/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/23/www.epson.com.ve/>

OS: Windows

Original: <http://www.public-data.ford.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/23/www.public-data.ford.com/>

OS: Windows

Original: <http://wwwdeviii.lason.ford.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/23/wwwdeviii.lason.ford.com/>
OS: Windows

Original: <http://www.mcdonalds.si/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/23/www.mcdonalds.si/>
OS: Windows

Original: <http://www.lawsearch.gov.au/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/23/www.lawsearch.gov.au/>
OS: Windows

[24.03.2001]

Original: <http://www.nissan.com.ar/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/24/www.nissan.com.ar/>
OS: Windows

Original: <http://www.nissan.com.sg/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/24/www.nissan.com.sg/>
OS: Windows

Original: <http://www.mpl.gov.my/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/24/www.mpl.gov.my/>
OS: Windows

Original: <http://www.marine.toyota.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/24/www.marine.toyota.com/>
OS: Windows

Original: <http://www.audi.co.yu/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/24/www.audi.co.yu/>
OS: Windows

[25.03.2001]

Original: <http://www.verbatim.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/25/www.verbatim.com/>
OS: Windows

Original: <http://www.aiwa.com.pa/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/25/www.aiwa.com.pa/>
OS: Windows

Original: <http://www.cfs.canon.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/25/www.cfs.canon.com/>
OS: Windows

Original: <http://www.martini.com/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/25/www.martini.com/>
OS: Windows

Original: <http://www.pizzahut.com.tw/>
Defaced: <http://defaced.alldas.de/mirror/2001/03/25/www.pizzahut.com.tw/>
OS: Windows

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

Defaced: <http://defaced.alldas.de/mirror/2001/03/25/www.sanyo.com.mx/>

OS: Windows

Original: <http://support.canon.de/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/25/support.canon.de/>

OS: Unknown

Original: <http://www.patents.att.com/>

Defaced: <http://defaced.alldas.de/mirror/2001/03/25/www.patents.att.com/>

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>