

HNS Newsletter
Issue 33 - 02.10.2000
<http://net-security.org>

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>

Table of contents:

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

=====
Sponsored by Kaspersky Lab - You Personal Anti-Virus Guard
=====
The Breakthrough Technology Protecting Your Computers From Viruses!

Subscribe to Kaspersky Lab's FREE newsletter delivering you the latest and trustworthy information source on computer viruses and their counter measures. You will always be up to date when securing your computer!
Join now! <http://www.kasperskylab.ru/eng/news/maillist.asp>

=====
General security news

BUSH CAMPAIGN MOUNTS EMAIL ASSAULT

"A strangely spamlike viral marketing campaign is being cranked-up in support of George W Bush's campaign for the US presidency. We use the term "spamlike" advisedly; as we all know, spamming is what other people do, we do permissions based email marketing, right?"

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/13824.html>

WHY KIDS SHOULDN'T BE CRIMINAL HACKERS

"Many kids who become criminal hackers think that what they're doing is just good harmless fun - like a neat video game. They are wrong. To understand why using a computer system without permission causes problems, you have to understand the goals of information security: confidentiality, control, integrity, authenticity, availability, and utility."

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/cover/coverstory20001009.html>

A YEAR AGO: SOFTSEEK INFECT USERS WITH NETBUS TROJAN

Internet security Web site, PCHelp, Thursday evening issued a security alert accusing popular download site Softseek.com of infecting the computers of users with Trojan horse program, NetBus, leaving them vulnerable to remote attack. Within the alert, PCHelp alleges that "Windows security program" WinSec, supposed to enable administrators to restrict user access to different Windows features, carries the well-known back door Trojan, Net Bus 170 W95.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/40/ns-18324.html>

OPENBSD PLUGS A RARE SECURITY LEAK

"For most open source projects, news of an overlooked security hole is simply part of the debugging process. But for the developers of OpenBSD, an operating system whose design motto is "secure by default," it's nothing short of an affront."

Link: <http://www.upside.com/texis/mvm/story?id=39dceffe0>

OMTOOL UNVEILS EASY-TO-USE E-MAIL ENCRYPTION TOOL

Client-server software vendor Omtool has launched an encrypted messaging application that it said is simpler to use and deploy than complex PKI-based systems. Although the security level is not as high as with PKI, Omtool's product offers an elevated degree of protection for companies that currently have to send confidential messages via unsecured email.

Link:

http://www.net-security.org/cgi-bin/news.cgi?url=http://www.telekomnet.com/news_security/10-6-00_omtool_encrypttool.asp

SECPROG MAILING LIST

SecurityFocus has opened a new mailing list called SECPROG. It is dedicated to the discussion of secure programming methods and techniques. One of the goals of the mailing list is to work on a comprehensive document that will serve as a secure programming guideline.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/forums/secprog/secure-programming.html>

CYBERCRIME OUTPACING SECURITY SPENDING

Cybercrime is skyrocketing despite increased spending on security measures, according to "The 2000 Information Security Survey," a study released by Information Security magazine. The survey found that more media attention is given to so-called "sexy cyberattacks" - such as denial-of-service (DoS), Web defacements, and buffer overflows - committed by outsiders. However, most cybercrimes are committed by insiders.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ecommercetimes.com/news/articles2000/001006-1.shtml>

EXPERTS APPLAUD MOVE TO CLOSE WAP SECURITY HOLE

European experts welcomed news that US authorities have finally standardised an encryption algorithm, saying that it will help close a security hole in WAP gateways. William Whyte, senior cryptographer at Baltimore Technologies, said: "The point of vulnerability lies at the gateway of a WAP server which potentially could allow anyone to read that message. The universal adoption of AES should make it possible for people to encrypt directly from the wireless device to any web server and it will subsequently remove the point of vulnerability."

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.silicon.com/a40075>

NEW CERT/CC VULNERABILITY DISCLOSURE POLICY

Effective October 9, 2000, the CERT Coordination Center will follow a new policy with respect to the disclosure of vulnerability information. All vulnerabilities reported to the CERT/CC will be disclosed to the public 45 days after the initial report, regardless of the existence or availability of patches or workarounds from affected vendors.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/faq/vuldisclosurepolicy.html>

SECURE SHELL NOW IN NETBSD MAINLINE

An OpenSSH-based Secure Shell is now available in the main NetBSD sources. And it will be pulled into the netbsd-1-5 branch, so it will be available in NetBSD 1.5. (ssh-1.2.27 and OpenSSH were already available in the NetBSD packages collection.) According to an NetBSD announcement, the OpenSSH-based implementation is temporary. They believe it will be replaced within the next couple months with a "completely independent implementation".

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2000/October/News299.html>

BINDV9 AND INTERNET SECURITY RELATED INTERVIEW

In this interview, Paul Vixie and David Conrad talk about the Internet Software Consortium, the changes in the latest major version of bind, the security features designed into it, and the future of Internet security.

Link:

http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/feature_stories/conrad_vixie-1.html

SECURITY BREACH CONCERNS ARE UP

Audits conducted last year by the General Accounting Office and agency inspectors general show that 22 of the largest federal agencies have significant computer security weaknesses. Among the common problems cited were poor controls over system access, data access and software development.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.latimes.com/business/cutting/20001003/t000093746.html>

BOSSSES GAIN EMAIL SNOOPING RIGHTS

The Government has abandoned "impractical" plans to force companies to seek permission from their staff to monitor email and phone usage at work. From October 24th, companies will be permitted "routine access" to any business emails and phone calls to see if they are business-related.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/13722.html>

WARNER MUSIC PLAYS WITH DIGITAL SECURITY

In an effort to develop new digital products and thwart Internet piracy, Warner Music Group is expanding its partnerships with secure online distributors and preparing to unveil a new, high-quality DVD-audio format with anti-copying features.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-2925971.html>

INTERVIEW WITH MARK ABENE A.K.A. PHIBER OPTIK

Mark Abene, former member of MOD and founder of Crossbar Security talks candidly about his early hacking and the supposed "war" with LOD as well as offering his thoughts on the "Golden Age" of hacking.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/media/65>

AOL, HP EXECS CALL FOR NET PRIVACY LAWS

America Online and Hewlett Packard executives told U.S. lawmakers that industry efforts alone are insufficient to protect consumer privacy online and legislation is needed to guard personal data.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.usatoday.com/life/cyber/tech/cti608.htm>

FIRSTGOV.GOV FLUNKS SECURITY TEST

A one-stop gateway to all 27 million U.S. government Web pages set up last month is inadequately protected from attackers.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2635962,00.html>

VIRUS NAMING CHAOS CAUSES CONFUSION

A need to standardise the naming of viruses has become apparent after the same virus was given at least four different names by antivirus vendors. Trend Micro this week issued an alert for a virus it calls VBS_Columbia, a Love Bug variant, which spreads itself by email. Rival vendor Symantec said the virus was actually discovered several weeks ago and is called VBS.Plan.A. Sophos calls it Loveletter.AS and Network Associates calls it Loveletter.AV.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1112012>

LINUX VIRUS SCANNERS: COMMON PROBLEMS

"So, we've covered Virus scanning for Linux in general, as well as where to place the scanning software. Even if you do all that perfectly, though, you can still run into problems."

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/linuxscan20001003-1.html>

FBI RELEASES FIRST BATCH OF CARNIVORE DOCUMENTS

The Electronic Privacy Information Center, which sued the FBI for the information through the Freedom of Information Act, is reviewing the documents and will soon release its analysis based on the data. The FBI is required to release additional files at regular intervals, until all 3,000 pages have been delivered to EPIC.

Link:

<http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-2917414.html>

Security issues

All vulnerabilities are located at:

<http://net-security.org/text/bugs>

VULNERABILITY IN MOREOVER.COM'S CACHED_FEED.CGI

Yet another CGI that lacks sufficient (or in this case -any-) input validation, leading to the exposure of readable files on the system.

Link: <http://www.net-security.org/text/bugs/970533061,34083,.shtml>

GNORPM LOCAL /TMP VULNERABILITY

While fixing other problems with the gnorpm package a locally exploitable security hole was found where a normal user could trick root running GnoRPM into writing to arbitrary files due to a bug in the gnorpm tmp file handling. A new release of GnoRPM (0.95.1) is now available. This fixes significant numbers of gnorpm bugs including the security hole. Administrators who use this program on multi-user machines may well want to update it, and anyone who uses it regularly will probably appreciate the fact it now works rather better than before.

Link: <http://www.net-security.org/text/bugs/970533126,51743,.shtml>

VULNERABILITY IN CYBEROFFICE SHOPPING CART

It is possible with default installations (according to vendor instructions) of CyberOffice to gain access to the database which holds information on customer orders, details and credit card information. This data is held in an unprotected and un-encrypted Microsoft Access Database.

Link: <http://www.net-security.org/text/bugs/970533370,54017,.shtml>

WINGATE 4.0.1 DENIAL-OF-SERVICE

The Wingate engine can be disabled by sending an abnormal string to the Winsock Redirecter Service. The attack is not logged. Vulnerable: Wingate Home/Standard/Pro 4.0.1, possible prior versions (untested).

Link: <http://www.net-security.org/text/bugs/970533572,73497,.shtml>

LOCAL VULNERABILITY IN XFCE 3.5.1

XFCE 3.5.1 ships with the following entry in /etc/X11/xfce/xinitrc:

xhost +\$HOSTNAME If a person is using this on a multiuser system, all local users may connect to their X session and capture keystrokes, etc.

Link: <http://www.net-security.org/text/bugs/970575943,34613,.shtml>

PROBLEMS WITH THTTPD 2.19 SSI

The included cgi-bin program "ssi" (combined with a lesser bug in the thttpd server) allows the viewing of arbitrary files on the remote server. This includes files outside of the web root and files in cgi-bin directories (that would normally only be executed). However, only files readable by the user that the server is running under (usually user 'nobody') can be viewed. This typically limits the exposure to world-readable files only.

Link: <http://www.net-security.org/text/bugs/970576048,12856,.shtml>

RESOURCES NOT FOR ALL

This patch gives limited access for non-root to process table ,only root see all process and have access to their entries in proc filesystem. Permission to directories in proc filesystem is changed to 550 (dr-xr-x---). Non-root users can only see own proceses.

Link: <http://www.net-security.org/text/bugs/970576193,14761,.shtml>

PEGASUS MAIL FILE READING VULNERABILITY

The default setup of Pegasus Mail contains a remotely exploitable security hole that allows a remote website to gain copies of files on the users hard drive.

Link: <http://www.net-security.org/text/bugs/970621168,87016,.shtml>

CALDERA LINUX - GNORPM PACKAGE

Gnorpm versions prior to 0.95 use files in the /tmp dir in an insecure manner. If gnorpm is run as root, this vulnerability could lead to any file on the system being overwritten by gnorpm.

Link: <http://www.net-security.org/text/bugs/970621281,58939,.shtml>

PROBLEM WITH GNU GROFF UTILITIES

The vulnerability is particularly dangerous in Linux distributions that have the "lesspipe" feature. By default, a "LESSOPEN" environment variable is set which points to a wrapper script for the "less" pager program named "/usr/bin/lesspipe.sh". If less is passed a filename with any of the extensions ".1" through ".9", ".n", or ".man", it automatically calls groff to handle the file.

Link: <http://www.net-security.org/text/bugs/970702976,58239,.shtml>

UNAUTHORIZED "DIRECTORY LISTINGS" UNDER IIS 5.0

It is possible to gain a directory listing of the root directory and every

sub directory. The impact of this is such that attackers may be able to discover "hidden" files or enumerate .inc files used in ASP applications and then directly download them. .inc files can contain sensitive information such as database login names and passwords.

Link: <http://www.net-security.org/text/bugs/970703043,90499,.shtml>

IMMUNIX OS SECURITY UPDATE FOR LPR

RedHat has put out an update to the lpr package due to a potential format string security bug.

Link: <http://www.net-security.org/text/bugs/970703094,39891,.shtml>

AOL INSTANT MESSENGER DOS

AOL Instant Messenger version 4.1.2010 (others?) appears to be vulnerable to a DoS attack when handling file transfers with filenames containing %s. This DoS is apparently related to a problem with format strings.

Link: <http://www.net-security.org/text/bugs/970703303,25609,.shtml>

"WORD MAIL MERGE" VULNERABILITY PATCHED

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Word 2000 and 97. The vulnerability could allow a malicious user to run arbitrary code on a victim's computer without their approval.

Link: <http://www.net-security.org/text/bugs/970836665,24380,.shtml>

ANOTHER IE 5.5/OUTLOOK SECURITY VULNERABILITY

Internet Explorer 5.5/Outlook allow executing arbitrary programs after viewing web page or email message. This may lead to taking full control over user's computer.

Link: <http://www.net-security.org/text/bugs/970837661,95810,.shtml>

RED HAT LINUX - TRACEROUTE SETUID ROOT EXPLOIT

A root exploit due to a segfault when using multiple -g options is fixed for Red Hat Linux 6.x and Red Hat Linux 5.x. A potential denial-of-service attack is alleviated by enforcing a maximum buffer size of 64Kb. On Red Hat Linux 6.x, loose source routing (LSRR) now works correctly.

Link: <http://www.net-security.org/text/bugs/970919340,13901,.shtml>

RED HAT LINUX - ESOUND CONTAINS A RACE CONDITION

Esound, the Gnome sound server, contains a race condition that a malicious user could exploit to change permissions of any file owned by the esound user.

Link: <http://www.net-security.org/text/bugs/970919495,33832,.shtml>

INSECURE CALL OF EXTERNAL PROGRAMS IN RH LINUX TMPWATCH

The tmpwatch utility is used in Red Hat Linux to remove temporary files. This utility has an option to call the "fuser" program, which verifies if a file is currently opened by a process. The fuser program is invoked within tmpwatch by calling the system() library subroutine. Insecure handling of the arguments to this subroutine could potentially allow an attacker to execute arbitrary commands.

Link: <http://www.net-security.org/text/bugs/971105993,28410,.shtml>

IMMUNIX OS SECURITY UPDATE FOR TMPWATCH

RedHat has put out an update to the tmpwatch package due to a local denial of service problem and a potential root exploit

Link: <http://www.net-security.org/text/bugs/971106040,86351,.shtml>

PHPIX 1.0.X DIRECTORY TRAVERSAL VULNERABILITY

Synnergy has discovered a flaw within PHPix that allow a remote user to traverse a directory as a request to the script using the \$mode=album&album=_some_dir_variable.

It is then possible to read any file or folder's contents with priviledges as the httpd.

Link: <http://www.net-security.org/text/bugs/971106264,49747,.shtml>

Security world

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

ADVANCED ENCRYPTION STANDARD FROM BALTIMORE TECH. - [03.10.2000]

Baltimore Technologies, a global leader in e-security, announced that it will fully support the new AES algorithm, Rijndael, across its full product range, including both its hardware and software products. The AES algorithm, chosen today by the United States National Institute of Standards and Technology (NIST), will be incorporated in all Baltimore products including Baltimore KeyTools, a radical new suite of developer products and Baltimore SureWare, a range of next generation e-security hardware products. The AES algorithm will be available within the KeyTools family beginning Wednesday, October 11th.

Press release:

< <http://www.net-security.org/text/press/970533748,63057,.shtml> >

NOKIA AND MCAFEE TEAM UP - [03.10.2000]

Nokia, a proven leader in network security infrastructure and McAfee, a Network Associates, Inc. business unit and the recognized leader in virus protection, announced the WebShield for Nokia Appliance, a joint offering designed to leverage the growing trend toward network appliance implementations and managed services.

Press release:

< <http://www.net-security.org/text/press/970575888,50055,.shtml> >

ADDITIONS TO BALTIMORE'S SOLUTIONSPPLUS - [03.10.2000]

Baltimore Technologies, a global leader in e-security solutions, announced the addition of its Signature Validation Platform as part of SolutionsPlus for the Identrus system. Baltimore's SolutionsPlus for the Identrus system is designed to provide leading financial institutions worldwide with all the tools they need to quickly implement Identrus systems that enable secure business-to-business e-commerce transactions in a private, confidential, non-reputable manner.

Press release:

< <http://www.net-security.org/text/press/970591283,10421,.shtml> >

MVPN SELECTS BALTIMORE'S SECURE VPN SOLUTION - [03.10.2000]

Baltimore Technologies, a global leader in e-security solutions, announced that mVPN has deployed Baltimore's Secure VPN solution, part of the Baltimore SolutionsPlus line of e-business solutions. The Secure VPN solution is a combination of best-of-breed partners and leading PKI technology for the implementation of Virtual Private Networks (VPNs). Secure VPN ensures highly scalable, cost-effective and easy-to-deploy, yet secure, access to protected corporate data using public networks such as the Internet.

Press release:

< <http://www.net-security.org/text/press/970591356,78974,.shtml> >

E-SECURITY EXPO AND CONFERENCE INFORMATION - [04.10.2000]

The e-Security Expo and Conference, to be held November 7-8 at the San Francisco Hilton & Towers will provide executives and technology professionals the information they need to protect their customer data, business intelligence, and minimize disruptions to their businesses. The conference also focuses on new opportunities that can be advantageous for their company's e-business provided the right e-security measures are taken.

Press release:

< <http://www.net-security.org/text/press/970621097,14964,.shtml> >

ALADDIN RELEASES ETOKEN ENTERPRISE 1.1 - [0.10.2000]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, released the beta version of eToken Enterprise 1.1. Providing simple implementation of two-factor authentication, secure login, secure messaging, digital signatures and GINA replacement, eToken Enterprise is truly an out-of-the-box solution for securing corporate networks, e-commerce, e-banking and Virtual Private Networks (VPNs).

Press release:

< <http://www.net-security.org/text/press/970700204,76777,.shtml> >

SECURE COMPUTING ANNOUNCES Q3 RESULTS - [05.10.2000]

Secure Computing Corporation, will announce third quarter results on Thursday, October 19, after market close. A one-hour conference call has been scheduled at 2:00 p.m. PDT (5:00 p.m. EDT). John McNulty, chairman and CEO, Tim McGurran, SVP of operations and CFO, and Carr Biggerstaff, SVP product planning, marketing & business development, will discuss the results followed by a question-and-answer session.

Press release:

< <http://www.net-security.org/text/press/970702188,50462,.shtml> >

E-MAIL ENCRYPTION FOR WEB BASED EMAIL PROVIDERS - [06.10.2000]

Sigaba Corporation, a secure Internet communications company, announced Sigaba's Software Developer's Kit that lets web-based email companies offer their users a one click security solution to encrypt their mail. "Email users today are more savvy than ever and they are very aware of the online threats to their privacy," said Gary B. Friedman, Sigaba Chairman/co-founder.

Press release:

< <http://www.net-security.org/text/press/970835866,84227,.shtml> >

BALTIMORE TECH. ANNOUNCES NEW DEPUTY CHAIRMAN - [06.10.2000]

Baltimore Technologies, a global leader in e-security, announced that Mr. Fran Rooney, Chief Executive Officer of the Company, has also been appointed to the position of Deputy Chairman on the Board of Directors, with immediate effect.

Press release:

< <http://www.net-security.org/text/press/970836014,73596,.shtml> >

ALADDIN'S ESAFE PROTECTS AGAINST NEW IE EXPLOIT - [06.10.2000]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, today announced its eSafe content security solutions protect against a new security hole discovered in Internet Explorer. Though the exploit itself is not a vandal, it allows hackers to infect user's PCs with dangerous trojans, vandals and other malicious code.

Press release:

< <http://www.net-security.org/text/press/970843885,74986,.shtml> >

LATEST NEWS FROM BINDVIEW CORPORATION - [09.10.2000]

BindView Corporation, a leading provider of IT administration and security management solutions, today announced that it identified and Microsoft eliminated recent vulnerabilities in the Microsoft operating system. These latest vulnerabilities could allow a range of effects, including possible

Denial of Service Attacks and privilege elevation. The two companies have created a well-defined process for efficiently working together to identify and close these type of vulnerabilities.

Press release:

< <http://www.net-security.org/text/press/971105242,81029,.shtml> >

CISCO IP VPN SOLUTION FOR SERVICE PROVIDERS - [09.10.2000]

Cisco Systems, Inc., the worldwide leader in networking for the Internet, announced a complete network-based IPsec VPN solution. Based on the new Cisco VPN 5000 concentrator and client, and available today, the new Virtual Private Network (VPN) platform securely connects remote users and branches to their corporate networks and business partners across the Internet. Cisco's new VPN 5000 solution brings service providers a new revenue generating opportunity by allowing them to offer their customers a single, secure solution for both remote access and Intranet and Extranet VPNs from a variety of client platforms.

Press release:

< <http://www.net-security.org/text/press/971105289,22829,.shtml> >

SIGABA ANNOUNCES EMAIL ENCRYPTION FOR USE WITH MS IE 5.5 - [09.10.2000]

Sigaba Corporation, a secure Internet communications company, announced that SigabaSecure(TM), an email encryption client, is now available for use with Microsoft Internet Explorer 5.5 to encrypt Hotmail and Yahoo! Mail. SigabaSecure for IE 5.5 is a plug-in which allows users to send encrypted mail, shred mail so it cannot be re-opened, and confirm that mail has been read from their Yahoo! Mail and Hotmail accounts.

Press release:

< <http://www.net-security.org/text/press/971105808,83402,.shtml> >

SECURE COMPUTING SUPPORTS CISCO'S SAFE E-BUSINESS - [09.10.2000]

Secure Computing Corporation, a leading provider of safe, secure extranets for e-Business, today announced that Secure's SafeWord and SafeWord Plus AAA servers provide managed, secure access for the new SAFE security blueprint from Cisco Systems, Inc. SAFE is a flexible, comprehensive security blueprint that is designed to help organizations securely, reliably and cost-effectively engage in e-business.

Press release:

< <http://www.net-security.org/text/press/971105865,58560,.shtml> >

TELERELAY TEAMS WITH TREND MICRO - [09.10.2000]

Trend Micro Inc., a leading provider of enterprise antivirus and content

security solutions, and messaging outsourcing specialist TeleRelay today announced that they are working together to provide a safer electronic messaging environment by delivering reliable, managed virus protection to the business community.

Press release:

< <http://www.net-security.org/text/press/971105924,88098,.shtml> >

Featured articles

All articles are located at:

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

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

Listed below are some of the recently added articles.

ISSUES: THE MEDIA'S GUIDE TO TALKING TO HACKERS by Thejian

Two years ago, the then just started HNN, published an article in their Buffer Overflow section called "A hacker's guide to talking to the media". It was received with different opinions around the scene (I remember it referred to as "a hackers guide to talking to your local newspaper") but what people failed to grasp at that point was the importance of the attempt to educate the hax0rs on relations with the media. Wether you like it or not, especially in this scene, what one person says WILL affect us all.

Article:

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

USING CONSERVATION OF FLOW AS A SECURITY MECHANISM IN NETWORK PROTOCOLS by Tuomas Aura, Matt Bishop and John Hughes

The law of Conservation of Flow, which states that an input must either be absorbed or sent on as an output (possibly with modification), is an attractive tool with which to analyze network protocols for security properties. One of its uses is to detect disruptive network elements that launch Denial of Service attacks by absorbing or discarding packets. Its use requires several assumptions about the protocols being analyzed. In this paper, the authors examine the WATCHERS algorithm to detect misbehaving routers. They show that it uses Conservation of Flow without sufficient verification of its assumptions, and can consequently be defeated. They suggest improvements to make the use of Conservation of Flow valid.

Article:

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

SECURING A DEFAULT LINUX INSTALLATION by Aleksandar Stancin aka D'Pressed

This article is written for a linux newbie or anybody who cares, at least a bit about the data stored on his hard drive. You'll notice that it's aimed mainly for home-users, not for large network administrators or similar. All procedures have been done and checked on an installed SuSE 6.4 linux distribution.

Article:

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

KASPERSKY LAB LAUNCHES A NEW VERSION OF ANTIVIRAL TOOLKIT PRO

Kaspersky Lab announces the launch of a new version, 3.5, of its world famous, award-winning virus hunter, AntiViral Toolkit Pro (AVP). It is powered by numerous unique anti-virus technologies and features a new design of the main user interface.

Article:

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

Featured books

The HNS bookstore is located at:

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

Suggestions for books to be included into our bookstore can be sent to staff@net-security.org

UPGRADING AND TROUBLESHOOTING NETWORKS: THE COMPLETE REFERENCE

Read this one if you're new to data communications, seeking any of several professional certifications that have to do with computer connectivity, or even if you've established yourself as a networking pro and want a solid reference on hand. This book generally deals with network equipment and protocols in a platform-independent way, although it dips into the specifics of Novell NetWare and Microsoft Windows networking after the foundation is laid. Topics covered: Local and wide area networking for personal computers, both generically and as implemented under Windows NT, Windows 2000, and Novell NetWare. Hardware and architecture coverage is followed by a detailed discussion of protocols, naming schemes and name-allocation services, directory services (notably Novell Directory Services and Active Directory), and Internet services.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0072122560/netsecurity> >

UNDERSTANDING MICROSOFT WINDOWS 2000 DISTRIBUTED SERVICES

This book explains the big picture in its latest Windows DNA and Windows 2000 incarnations. This isn't strictly a programmer's text (it doesn't give recipes for building distributed applications), but neither is it just an administrator's guide (instructions for configuring Active Directory appear in other books). Instead, it's a thorough and carefully written explanation of how Windows 2000 and its applications run in a distributed environment, and how Windows supports distributed software and data in a secure way. Topics covered: Windows 2000 and the Windows DNA distributed computing technologies, including Active Directory, the Component Object Model (COM), COM+, ActiveX Data Objects, Distributed Transaction Services, and Microsoft Message Queuing Services. Also, there's in-depth discussion of how they all fit together.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/157231687X/netsecurity> >

UNDERSTANDING SQL AND JAVA TOGETHER : A GUIDE TO SQLJ, JDBC, AND RELATED TECHNOLOGIES

Many books on Java cover JDBC in detail, but this title goes much further by surveying a handful of other database standards from a variety of vendors, including Oracle and Sybase. (Don't worry: there's full coverage of JDBC for versions 1.0 and 2.0.) The real focus of this book is on SQLJ, which really comprises three standards. SQLJ Part 0 is the easiest to understand, as it supports embedded SQL calls within Java code. Next comes SQLJ Part 1, by which a database product (like Oracle) can use Java to define stored procedures. Here, the authors take care to show off how to deploy JAR files into a database. (Their sample movie database, used throughout this book, is both comprehensible and a little more entertaining than most sample database schemas.) Next, the authors look at SQL user-defined types (UDTs) and SQLJ Part 2, which allows Java code to make use of these UDTs directly, as well as store Java objects in a database. The last stop on the tour is a "true" object/relational mapping, Sun's Java Blend standard, which allows Java objects to be saved and restored from a database transparently.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1558605622/netsecurity> >

WEB SECURITY

Tiwana, who writes a monthly column for Information Technology, offers a guide for systems administrators, security consultants, and others concerned about the security of web sites. He explains how to create and execute a comprehensive strategy, identify and eliminate potential vulnerabilities, frame a security policy, and test existing security measures. The CD-ROM contains security and weakness scanners, log analysis tools, firewalls, and other software.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1555582109/netsecurity> >

BEGINNING VISUAL BASIC 6 APPLICATION DEVELOPMENT

This book puts enterprise-level programming into the hands of intermediate VB users with a capable tour of every facet of multitiered development. This book is all you need to start using server-side objects and Web-based interfaces with VB. What's best here is the comprehensive yet approachable guide to all of the Microsoft tools, APIs, and standards that are needed for using VB to create large enterprise-level applications. This means looking at the three tiers for application partitioning--user, business, and data services--along the lines of Microsoft's recommended practice. The authors cover all of the steps needed to design and code applications in today's corporate environments, along with a solid introduction to UML diagrams. Wherever possible, they make use of tools (like the VB Class Builder) to speed up development; also, the title is chock full of actual screenshots to help you along.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1861001096/netsecurity> >

Defaced archives

[01.10.2000] - Stanford University

Original: <http://almond.stanford.edu/>

Defaced:

<http://www.attrition.org/mirror/attrition/2000/10/01/almond.stanford.edu/>

[02.10.2000] - Ministerio de Economia, El Salvador

Original: <http://www.minec.gob.sv/>

Defaced:

<http://www.attrition.org/mirror/attrition/2000/10/02/www.minec.gob.sv/>

[03.10.2000] - NTAS Gov (TW)

Original: <http://www.ntas.gov.tw/>

Defaced:

<http://www.attrition.org/mirror/attrition/2000/10/03/www.ntas.gov.tw/>

[03.10.2000] - State of Washington

Original: <http://dor.wa.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/03/dor.wa.gov/>

[03.10.2000] - US DOI, Bureau of Land Management

Original: <http://adoptahorse.blm.gov/>

Defaced:

<http://www.attrition.org/mirror/attrition/2000/10/03/adoptahorse.blm.gov/>

[04.10.2000] - Society for Electronics Test Engineering, India

Original: <http://www.sete.gov.in/>

Defaced:

<http://www.attrition.org/mirror/attrition/2000/10/04/www.sete.gov.in/>

[04.10.2000] - IntiGov (AR)

Original: <http://ayelen.inti.gov.ar/>

Defaced:

<http://www.attrition.org/mirror/attrition/2000/10/04/ayelen.inti.gov.ar/>

[07.10.2000] - Moscow Institute of Physics and Technology

Original: <http://games.mipt.ru/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/07/games.mipt.ru/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>