

HNS Newsletter
Issue 48 - 29.01.2001
<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>

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 : 1855

Table of contents:

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

=====
Help Net Security has organized a contest in which participants have to write an opinion on the "most secure OS". The best five opinions will be published on the site and their authors will get a free copy of "The FreeBSD Corporate Networker's Guide."

For more information use the following URL:
<http://www.net-security.org/various/bookstore/ted/>
=====

General security news

UK GOVERNMENT SITE DOUBLE ATTACKED

Swindon Borough Council's website was defaced twice by two different hacker groups at the weekend. The site, www.swindon.gov.uk, was one of many government and military websites around the world to be defaced on Saturday by a hacking group called Pentaguard, which has been responsible for around 40 hacks over the last year. Other sites attacked were UK government website www.bseinquiry.gov.uk and Australian government website www.brighton.tas.gov.au. Swindon's site was then hacked again on Sunday by a group or individuals known as "Krab".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1116663>

CLINTON APPOINTS 21 TO INFO SECURITY ADVISORY GROUP

On his last full day in office, former President Clinton appointed 21 members to

a newly established council that will advise President George W. Bush on ways to protect the nation's most critical computer systems from cyber attack. The new group to which the appointments were made - the National Infrastructure Assurance Council (NIAC) - was conceived of in 1997 as a group of CEOs from the nation's leading companies in virtually every major infrastructure sector, including energy, telecommunications, transportation, and banking that would advise the president in the event of a cyber attack on one or more of these critical sectors.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/160831.html>

IBM DEVELOPS SECURE MUSIC SOFTWARE

With the music industry seeking safe ways to sell songs online, International Business Machines Corp. said Monday it has developed software that prevents consumers from making unauthorized copies of music downloaded from the Internet. The Electronic Media Management System, which will be made available sometime this quarter, allows music companies to define the terms by which retailers and Internet users can swap songs over so-called peer-to-peer networks, a distribution technology popularized by online music company Napster Inc.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nandotimes.com/technology/story/0,1643,500302547-500483965-503331765-0,00.html>

MACWORLD SF 2001 TREND: PERSONAL FIREWALLS

The rise in permanent Internet connections via cable modems and DSL has raised fears of crackers breaking into individual computers and wreaking havoc. For Windows users, those fears are real, since most of the automated attacks look specifically for security holes in Windows network services. Macs are significantly less vulnerable to such problems, especially if Personal Web Sharing and Personal File Sharing via TCP/IP are turned off or properly secured, but a number of companies are now producing personal firewall products for Mac users who want additional peace of mind or who want to know precisely what's happening. Intego's NetBarrier and Open Door Networks' DoorStop (now the foundation of Norton Personal Firewall) were first on the scene, and they've just been joined by IPNetSentry from Sustainable Softworks, the network wizards who brought us IPNetRouter.

Link: <http://db.tidbits.com/getbits.acgi?tbart=06281>

COMPUTER CRIME INVESTIGATOR'S TOOLKIT: PART IV

Slack space occurs on a hard drive or floppy when a file gets partially overwritten after deletion. The new file does not completely fill in the space created by the old file's data. So, a slack space of residual data remains in the area between the end of file (EOF) boundary of the new file and the end of the cluster. On a given disk, then, large amounts of "hidden data" exist. These fragments may offer considerable evidence about what was deleted from the disk.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/toolkit20010123.html>

PRESIDENT OFFERS JOB TO THE DEFACER OF HIS WEBSITE

A Bulgarian youth has been offered a job by his country's president after criticising the government in a web attack. The attacker - who is known

only by the pseudonym 'Kabaka' - brought down the presidential homepage last week, leaving a message railing against the president for failing Bulgaria's youth. President Petar Stoyanov said that he would employ him without hesitation, because the ingenuity he showed in cracking government security without leaving a trace.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ananova.com/news/story/sm_182455.html

MICROSOFT'S NEW ZEALAND WEBSITE ATTACKED

Microsoft has had another of its international websites broken into and defaced. The Prime Suspectz group broke into Microsoft's New Zealand website overnight, replacing the front page with text like this: "Oh!!! what's hapened!! Another Micro\$oft was hacked? !!Yes!! 'The vulnerability is completely teorical' !! I don't think so !! security wuz broke'n !".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1116687>

TOSHIBA MAKES FINGERPRINT READER FOR NOTEBOOKS

Toshiba America has released the PC Card Fingerprint Reader, a product that provides security for notebook computers. The fingerprint reader attaches to a standard PC card and uses Biometrics technology to provide convenient and reliable security. The device stores the prints of one or more fingers of a user, then allows access to the notebook system when those fingers are scanned into the reader.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.telekomnet.com/writer_telekomnet/1-23-01_toshiba.asp

ANTI-FUR PROTESTERS HACK CHANEL'S SITE

Animal rights activists hacked into French fashion house Chanel's Web site and posted a protest against fur clothes only hours before the label presented its latest haute couture collection Tuesday.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/520407.asp>

REVERSE ENGINEERING

A key ruling last October by the 9th U.S. Circuit Court of Appeals, located in San Mateo, affecting the home video game sector is having a direct impact on the entire software industry. The ruling, which upholds engineers' rights to reverse-engineer other companies' proprietary hardware for purposes of research, flies in the face of federal legislation passed two years ago banning most forms of reverse engineering. The congressional ban - part of the Digital Millennium Copyright Act of 1998 - was intended as a measure to extend existing copyright law into the realm of software. But the Sony vs. Connectix ruling may present the legal loophole that software engineers need to justify other forms of reverse-engineering research, such as dissecting operating systems to enable anti-virus programs to detect irregular behavior by other programs.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.planetit.com/techcenters/docs/security/news/PIT20010123S000>

NFS AND NIS SECURITY

Security problems seem to be inherent in NFS and NIS; however, there are methods and precautions that can be taken to make them more secure than their plain-vanilla implementations. This article by SecurityFocus.com writer Kristy Westphal, will examine some on the ways in which security for NFS and NIS can be enhanced.

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

MORE PROBLEMS FOR NETWORK ASSOCIATES

As is company policy, Internet security firm Network Associates, Inc. declined to comment on any legal matter. However, as many as six separate class action suits have been filed on behalf of shareholders who say Santa Clara based Network Associates filed "positive but false statements about current business and future prospects throughout the second half of 2000."

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://siliconvalley.internet.com/news/article/0,2198,3531_568281,00.html

WHY FIREWALLS?

Firewalls are usually seen as a requirement if you are going to attach your network to other networks, especially the Internet. Unfortunately, some network administrators and managers do not understand the strengths a firewall can offer, resulting in poor product choice, deployment, configuration and management. Like any security technology, firewalls are only effective if the implementation is done properly and there is proper maintenance and response to security events.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20010124.html>

SECOND ATTEMPT

ABC Enterprises, Australia's national broadcaster, was forced to thwart a second attempt to deface its e-commerce website within minutes of an attacker bypassing the server's security yesterday.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theage.com.au/frontpage/2001/01/23/FFXEI9AGAIC.html>

MICROSOFT DEFACEMENT: UPDATE

Microsoft Corp. has played down a defacement of its New Zealand Web site on Tuesday, saying it already knew about the security issue that led to the site's vandalism.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/160947.html>

HP DISTRIBUTES VIRUS INFECTED DRIVERS

Hewlett-Packard has distributed printer drivers corrupted by a computer virus. The infected drivers were inadvertently uploaded onto the hardware giant's Web site, according to a report by Japanese news service Nikkei. The plague drivers, which were distributed between 17 and 19 December 2000, contained the Funlove virus. The issue only came to light after complaints from HP users, and subsequent checks in Japan revealed that 51 program files for printer and BIOS drivers for servers had become infected.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/4/16335.html>

SSL - RUMOURS AND REALITY

You may have connected to a web page every now and then and noticed a small padlock icon at the bottom of your, browser window. What does this padlock signify? It means that the web-site is protected by SSL. SSL stands for 'Secure Sockets Layer' and refers to a protocol (or technique) that ensures a secure connection to a web-site. This article by Charl Van Der Walt will discuss the ways in which SSL provides safe, secure Internet transactions, including: how SSL works, why it is an effective weapon against hackers and how hackers can sometimes use it to their advantage.

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

CAR MAKERS WEB SITES DEFACED

The UK web sites of car makers Mitsubishi and Fiat are the latest to fall victim to a vandal who exploits vulnerabilities with Microsoft's Internet Information Server. Like Microsoft's New Zealand site, which fell victim to defacement yesterday, the car sites were defaced by Prime Suspectz with a message mocking the security of Microsoft's software.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/16345.html>

OPENING OF INDUSTRY LINUX LAB

The industry's first independent, non-profit lab designed for developers who are adding new business-oriented capabilities to Linux and Linux-based software opened today with the support of 19 sponsor companies and more than \$24 million in funding.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.intel.com/pressroom/archive/releases/20010124comp.htm>

VATICAN RADIO SITE ATTACKED

Italian daily newspaper "Il Messaggero", reported that the web site of Vatican Radio, the official radio broadcaster of the Vatican, has been attacked by "hackers". The article is mentioning DDoS attacks, but it looks like it was defaced. InfoGuerra's Editor contributed that Alldas.de has the mirror.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/161109.html>
Link: <http://defaced.alldas.de/mirror/2001/01/24/www.radiovaticano.com>

MICROSOFT CONTACTS FBI

Ananova reports that Microsoft contacted the FBI after a DDoS attack, intermittently keeping Web surfers shut out from Microsoft Internet properties such as Microsoft.com and MSN.com.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ananova.com/news/story/sm_186169.html

DECSS ALLIES GANGING UP

A federal court decision that restricted a DVD-descrambling program ignores free speech rights and should be overturned, eight different coalitions claim.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wirednews.com/news/politics/0,1283,41441,00.html>

REAL USER LAUNCHING 'REAL' SECURITY MONDAY

On Monday, Real User Corp. will publicly launch itself and its face-based Internet authentication technology. The group hopes to some day overcome cookies and passcodes as the methods of choice for surfers and e-commerce companies to verify identity and information. "What we're trying to do is provide an integral part of the security structure of the Internet that doesn't already exist," Real User Chief Executive Officer Paul Barrett said in an interview today. "That is, tackling usability and security at the same time."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/161145.html>

LINUX SECURITY BASICS

How to achieve the goal of every system admin: boring, predictable computers. Here is a defensive driving course for the information superhighway. Learn to develop a threat model, to implement security measures, and to find out what the newest threats may be.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/linuxworld/lw-2001-01/lw-01-security.html>

SMC BARRICADE 4-PORT ROUTER AND PRINT SERVER

SMC has been around for the better of 25 years providing high-quality hubs, switches, adapters, USB hardware - heck, anything that has to do with networking, SMC has covered or had it covered at some point in the last 25 years. The SMC Barricade is an interesting product that fills the aforementioned void quite well, while also adding in some extras like full print serving capabilities and great user control of port availability.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.awaremag.com/hardware/SMC/barricade/barricade_1.html

EPSON WEB SITE ATTACKED

"Some files were overwritten through the breach in Microsoft IIS, the software we're running. We host quite a large number of corporate websites but this is the first time we've had a breach like this," - Karim Hussona, chief executive officer at Compass Communications, the company that hosts the Epson website.

Link:
<http://www.nzherald.co.nz/storydisplay.cfm?storyID=169810&thesection=technology&thesubsection=general>

HECKENKAMP PLEADS INNOCENT TO HACKING

Jerome Heckenkamp, who began working at Los Alamos last June, has said an unknown person broke into the companies' computers by working through his computer while he was a student at the University of Wisconsin. If you are interested in this story, please check the FREESK8.org web site. Read the excerpt from the mentioned site: "This web page is dedicated to public awareness concerning the case of Jerome Heckenkamp, a 21 year old Los Alamos National Laboratory employee who was arrested for allegedly committing several computer crimes under the alias of MagicFX. Hopefully as you browse through the resources below, you will come to the natural conclusion that this fine young individual has merely become the scapegoat

of a restless and unrelenting Federal Bureau of Investigation, caught in the middle of a 21st century spin-off of McCarthyism."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/computing/01/26/hacking.arrest.ap/index.html>

TOP TEN SECURE SHELL FAQs

SSH, the Secure Shell, is a set of protocols and software that provide secure, remote terminal sessions between networked computers. In addition to a simple remote command prompt, most SSH implementations also provide secure forwarding of X Window traffic as well as forwarding of connections to arbitrary TCP ports. These features can protect otherwise insecure protocols such as POP, IMAP, SMTP, and so on. An SSH session applies cryptographically assured privacy and integrity protection as well as mutual authentication to the data passing through it. Used properly, SSH is an extremely valuable tool that helps users more safely navigate today's Internet and helps system administrators secure their networks or perform remote administration.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://sysadmin.oreilly.com/news/sshtips_0101.html

SOME THOUGHTS ON THE NSA LINUX RELEASE

"There are two things I am sure of after all these years: there is a growing societal need for high assurance software, and market forces are never going to provide it. Superficially, I'm going to offer a few comments on the technology underlying the NSA release. My real intent is to induce the Open Source community into building on this release - so when society wakes up to the fact that this stuff is really, truly needed, something is actually there. You won't get rich working on high assurance technology, but you may end up feeling pretty good about how you spent your career."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.linuxjournal.com/articles/buzz/0043.html>

WORLD BANK DEFACED

One of the servers of the World Bank got penetrated into and defaced. Message left on the site was - "I want to thank the WorldBank for its kind attitude to our country. We would have been long lost away even from Romania. This should be taken as a request for future help to Bulgaria. Dear Gentlemen as you can see, our country shows greater and positive economic condition. The crazies caused by the Communist party (a.k.a Socialistic party) seem to be through. I'd like to congratulate the government and the president of Bulgaria."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://net-security.org/misc/sites/sima-ext.worldbank.org/>

TOP MALWARE OF 2000

The negative impacts of malware have escalated over the past few years as independent and corporate users have become more dependent upon networked computing solutions. The complexity and sheer bulk of code in software that accompanies such development has opened up a host of new vulnerabilities. The continued growth of Microsoft products across a large audience has also created an environment where one exploit within a Microsoft product may impact a large number of users worldwide.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/malware20010129.html>

A HACKER'S NEED FOR QUBE3

I often hear fellow hackers say, that everything a Linux appliance does can be done with a 200\$ PC and the right software. That is certainly right. Why should a hacker like me go out and buy a US\$ 1,995 to store files and use it as a web server, ftp server, and mail server? This review recounts my experience as a Linux kernel hacker and driver developer, using the Linux-powered Qube3 in trying to make all above-mentioned functionality of a server appliance in my lab. My lab consists of about 25 Linux servers and assorted other Unix servers. The lab connects to the Internet by means of a DSL line.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.moelabs.com/reviews1.html>

Security issues

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

MULTIPLE VULNERABILITIES IN FASTREAM FTP++

FaSTream's embedded ftp-server can be flooded into unresponsiveness by sending a request of 2048 bytes or greater size to it.

Link: <http://www.net-security.org/text/bugs/980261700,9485,.shtml>

LOCALWEB2000 DIRECTORY TRAVERSAL VULNERABILITY

Adding the string "../" to an URL allows an attacker access to files outside of the webserver's publishing directory. This allows read access to any file on the server.

Link: <http://www.net-security.org/text/bugs/980261718,95799,.shtml>

WATCHGUARD FIREWALL VULNERABILITY

I have found that the embedded Linux-based Watchguard Firebox II Firewall product range is vulnerable to read-write access using only a read-only passphrase. This gives a read-only user the ability to make changes to the firewall remotely without either authorization or a read-write passphrase. The risk is remote firewall compromise.

Link: <http://www.net-security.org/text/bugs/980261732,73378,.shtml>

PROBLEMS WITH ORACLE JSP/SQLJSP HANDLERS

It is possible to view files outside the web root. Also possible is execution of .JSP files outside the web root in the same partition as the web server's root.

Link: <http://www.net-security.org/text/bugs/980261749,15101,.shtml>

BUFFER OVERFLOW IN LOTUS DOMINO SMTP SERVER

Lotus Domino/Notes server has a 'policy' feature, which is used to define relaying rules. However, improper bounds checking allow remote user to

overflow the buffer and execute arbitrary code. If policy is enabled to check for domain name it is possible to trigger the overflow.

Link: <http://www.net-security.org/text/bugs/980304915,69914,.shtml>

PATCH FOR ORACLE XSQL SERVLET VULNERABILITY

Oracle has corrected this vulnerability in the new release of XSQL Servlet as well as provided more secure behavior by default. The new release of XSQL Servlet, Release 1.0.4.0, can be obtained from Oracle Technology Network, OTN, http://otn.oracle.com/tech/xml/xsql_servlet. A patch will also be available in the upcoming Oracle8i, Release 8.1.7.1, patch set and available for use with iAS Release 1.0.2.1.

Link: <http://www.net-security.org/text/bugs/980304938,81797,.shtml>

DEBIAN - NEW VERSION OF MYSQL RELEASED

Nicolas Gregoire has reported a buffer overflow in the mysql server that leads to a remote exploit. An attacker could gain mysqld privileges (and thus gaining access to all the databases). Upgrade immediately.

Link: <http://www.net-security.org/text/bugs/980304969,2953,.shtml>

DEBIAN - NEW VERSION OF MICQ RELEASED

PkC has reported that there is a buffer overflow in sprintf() in micq versions 0.4.6, that allows to a remote attacker able to sniff packets to the ICQ server to execute arbitrary code on the victim system. We recommend you upgrade your micq package immediately.

Link: <http://www.net-security.org/text/bugs/980304996,80556,.shtml>

MAKE THE NETOPIA R9100 ROUTER TO CRASH

If you have the password of the router and if you are logged to it you will not be able to delete all the traces. The router logs the connection and the disconnection of telnet sessions. If you want to delete the connection from the logs you just have to delete them. But if you want to delete the disconnection log you can't. The only way to do that is to make it crash. Just use the telnet program which is inside the router. Try to make a connection from the IP of the router to the IP of the router. It will crash it, as a consequence, you will NOT be logged !

Link: <http://www.net-security.org/text/bugs/980359282,81709,.shtml>

BORDERWARE V6.1.2 PING DOS VULNERABILITY

Sending a ping to the broadcast on the network causes Borderware's ping server to continuously send echo request to the entire network. It is possible that a Denial-of-Service attack (smurf attack) can be executed on the network using freely available exploit code. This can occur externally if broadcast packets aren't dropped at the router or on the local network if other machines aren't configured to deny directed broadcasts. Borderware has confirmed this problem. They upgraded the problem below to a bug and informed me that the pings can be stopped on-site by resetting the interfaces, which can be done from the Borderware client. Provided the exploit doesn't attempt to re-establish a connection when the network interface comes back up, this is a temporary fix.

Link: <http://www.net-security.org/text/bugs/980613054,97813,.shtml>

IBM WEBSHERE SHOWCODE VULNERABILITY

When IBM WebSphere application server shares the same document root as Netscape Enterprise server it is possible for a malicious user to view the source of any JSP file in the document root.

Link: <http://www.net-security.org/text/bugs/980613070,85509,.shtml>

JRUN MALFORMED URI WEB-INF DIRECTORY

It is possible to get a directory listing of the WEB-INF directory when requesting pages from a JRun Web Server. It is also possible to display the contents of the web.xml file in WEB-INF.

Link: <http://www.net-security.org/text/bugs/980613087,77841,.shtml>

Security world

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

PKI SOLUTION WITH ENHANCED PERFORMANCE - [23.01.2001]

Business security provider Cylink Corporation announced the general availability of NetAuthority 3.1, a next-generation public key infrastructure solution that provides advanced performance, functionality and ease of use. The PKI also is interoperable with solutions from a growing list of Cylink partners to enable an expanded set of applications.

Press release:

< <http://www.net-security.org/text/press/980261192,95348,.shtml> >

SECURE COMPUTING ANNOUNCES SMARTFILTER 3.0 - [23.01.2001]

Secure Computing announced SmartFilter 3.0, the latest release of the industry's first Internet access management application. SmartFilter 3.0 provides unprecedented flexibility for managing employee productivity and reducing liability associated with the misuse of company-provided Internet resources. Now organizations can choose the simplest way to manage employee Internet access by selecting from a broad range of URL filtering options and categories, using a new policy-based management console. More importantly, simple, sophisticated management reporting makes it easy to understand and control Internet access.

Press release:

< <http://www.net-security.org/text/press/980261322,64982,.shtml> >

ANTI-VIRUS BETA-VERSION FOR NOVELL NETWARE - [24.01.2001]

Kaspersky Lab, an international data-security software-development company, announces the release of the KasperskyT Anti-Virus beta-version for Novell NetWare powered by a new Java-based management system. The program also contains a set of unique features that significantly extend a user's ability for the centralized management of a network's anti-virus defense, thus decreasing attending expenses and making the product the world's most technically improved anti-virus system.

Press release:

< <http://www.net-security.org/text/press/980305376,54403,.shtml> >

DEVICELOCK MILLENNIUM EDITION RELEASED - [24.01.2001]

SmartLine, Inc. announced the new release of DeviceLock Millennium Edition, a Windows service for restricting access to local devices running Windows 95/98/Me. Preventing the introduction of inappropriate software and data is important when trying to protect and administer a company's computer network. The traditional solution has been a physical lock on the floppy drive. DeviceLock Me eliminates the need for physical locks and has a number of advantages. It is easy to install and administrators can have instant access from the remote computers when necessary.

Press release:

< <http://www.net-security.org/text/press/980305435,13048,.shtml> >

SECURE COMPUTING RECEIVES OPSEC CERTIFICATION - [25.01.2001]

Secure Computing announced that its SafeWord authentication and authorization system has received OPSEC (Open Platform for Security) certification from Check Point Software Technologies Ltd. for Check Point VPN-1/FireWall-1. OPSEC certification confirms that SafeWord is fully compatible with Check Point's authentication standards. Through this certification, end-users can select the security solutions that best meet their requirements and be assured that interoperability and central policy definitions are guaranteed.

Press release:

< <http://www.net-security.org/text/press/980387499,3755,.shtml> >

AMERICAN BANK'S NEW SECURITY FEATURES - [25.01.2001]

American Bank, a leading provider of Internet banking and financial services (www.pcbanker.com), announced the implementation of several new security features for online customers. These new features reinforce American Bank's commitment to maintaining the safety and security of their customers' financial information.

Press release:

< <http://www.net-security.org/text/press/980387696,23828,.shtml> >

DEPLOYING INTRUSION DETECTION SYSTEMS - [25.01.2001]

Learning Tree International, Inc. is announcing the release of a new Hands-On IT course, Deploying Intrusion Detection Systems, where participants learn to design, configure and deploy an Intrusion Detection System for their network.

Press release:

< <http://www.net-security.org/text/press/980387775,96667,.shtml> >

VIGILANTE AND MYCIO PARTNER - [27.01.2001]

VIGILANTE, the premier provider of automated security assessment services over the Internet, today announced a strategic technology alliance with myCIO, a leading provider of Internet security management solutions and a wholly owned subsidiary of Network Associates. SecureScan, VIGILANTE's flagship security service, integrates myCIO's CyberCop ASaP with open source, and other third-party proprietary scanners, as well as its own suite of software. This key industry alliance provides the SecureScan customer base with unmatched capabilities for identifying and addressing Internet perimeter vulnerabilities.

Press release:

< <http://www.net-security.org/text/press/980616100,62526,.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

FREEBSD CORPORATE NETWORKER'S GUIDE (WITH CD-ROM)

This book is written for the beginning FreeBSD administrator who wants to take advantage of the power and cost savings afforded by use of this operating system on their organization's production network. FreeBSD is a UNIX-like operating system that takes its name from the Berkeley Software Distribution group. "FreeBSD has been the secret weapon of serious network administrators for many years now and this book should provide a welcome introduction to those who have yet to discover it for themselves." - Jordan Hubbard, Co-founder, The FreeBSD Project.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201704811/netsecurity> >

INSIDE LINUX

The author acknowledges that adequately teaching how to use Linux involves more than communicating a series of recipes. For that reason, he goes to considerable effort to explain what's going on when the user executes various commands. He uses procedures to expose facts about Linux's innards, rather than as mere strategies for achieving desired effects. Therefore, his prose - particularly his extended coverage of the bash shell - reads like a scientist's journal: If we do this, here's what happens (and by the way, here's why). The approach is more leisurely than that of many introductory Linux books, and it leads to a deeper understanding of what's going on under the shell. The author shows how to configure and use XFree86, the K Desktop Environment (KDE), and GNOME. These are handy skills to have, even if most distributions will more or less automate those processes and some readers may wish instead for information on more obscure aspects of the operating system. Coverage of network configuration, where an intimate knowledge of the command line and configuration files is critical, suits this book's experiment-and-observe format very well. The reader gets to see lots of important pieces of software in action.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0735709408/netsecurity> >

PROFESSIONAL LINUX PROGRAMMING: DATABASES, POSTGRESQL, MYSQL, LDAP, SECURITY, DEVICE DRIVERS, GTK+, GNOME, GLADE, GUI, KDE, QT, PYTHON, PHP, RPC, DISKLESS SYSTEMS, MULTIMEDIA, INTERNATIONALIZATION, CORBA, PAM, RPM, CVS, FLEX, BISON, BEOWULF, CLUSTERING, ORBIT, MPI, PVM, AND XML

The book is framed as a case study for building a custom database program in Linux for a video rental store. After a tour of the requirements and a brief look at project management for creating this software, the various Linux packages that are needed to implement this system are described, along with sample code, most of which is written in C. Some packages, such as the CVS version control package, come with most distributions of Linux; others will require downloading additional software over the Internet. In every case, you're provided with the actual command-line arguments that are needed to install, configure, and run each package. Besides a great exploration of CVS for version control, this title offers excellent coverage of the free PostgreSQL and MySQL databases, which are two very popular choices for Linux databases. The book also does a good job of explaining UI design under both the GTK+ GNOME and KDE (two popular Linux desktops), and how to extend the reach of the sample database application by using Remote Procedure Calls (RPCs) and CORBA. Of course, the finished application doesn't use every Linux API that's covered here, but the book does cast a wide net, and introduces features and tools that are available.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1861003013/netsecurity> >

AD HOC NETWORKING

"Ad hoc" networks are wireless, mobile networks that can be set up anywhere and anytime - outside the Internet or another preexisting network infrastructure - whose time has come. The field has tremendous commercial and military potential, supporting applications, such as mobile conferencing outside the office, battlefield communications, and embedded sensor devices that automate household functions, among others. Ad Hoc Networking is a collection of algorithms, protocols, and innovative ideas from the leading practitioners and researchers that will propel the technology toward mainstream deployment. It discusses numerous potential applications, reviews relevant networking concepts, and examines the various approaches that define emerging ad hoc networking technologies.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201309769/netsecurity> >

HIGH AVAILABILITY NETWORKING WITH CISCO

This book explores and discusses a wide range of potential approaches to improving network availability, allowing you to choose those most appropriate for your organization and its unique needs and constraints. The goal is to show how to achieve higher network availability both in theory and in practice. In economic terms, this means pushing the design to the point where the cost of eliminating further unavailability exceeds the cost to the organization of the losses due to downtime. While the theoretical aspects apply to networks of all sizes and technologies, the example solutions provided focus on the needs of moderate sized extended corporate networks using IP version 4 and stable, moderate performance technologies such as frame relay, ISDN, and Ethernet - not because these technologies are fundamentally more or less reliable than others, but because these tend to be the networks which have grown to the point of being critical to the day-to-day operations of the organization without a staff of dedicated network designers and architects to provide optimization and support.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201704552/netsecurity> >

Security Software

All programs are located at:

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

SECURITY SETUP II LIGHT

Security SetUp II Light is an easy-to-use security application which allows you to protect your Windows configuration. The program lets you maintain your

current Windows setup and protect your desktop, network, printer, modem, screen saver, and Internet settings from being modified. It enables you to limit other users' access by setting up control levels, hide selected drives, add password protection, disable access to the Control Panel, and more.

Info/Download:

< <http://www.net-security.org/various/software/979836656,78721,windows.shtml> >

SECURITY DEPARTMENT 1.3.3.1

Security Department is a resident file system protector which can provide several levels of protection for different folders and files. You can prevent various actions for folders and files, including copying, moving, deleting, and renaming, and make selected folders and files read-only, fully-protected, or protected according to a custom protection level. Security Department also supports different access setups to various folders and files for each user group on a single computer, and includes administrator password-protection capability.

Info/Download:

< <http://www.net-security.org/various/software/979836840,54669,windows.shtml> >

ADVANCED NT SECURITY EXPLORER

Advanced NT Security Explorer helps NT system administrators find system security holes. It analyzes user password hashes, and tries to recover plain-text passwords. If it's possible to recover the password in a reasonable time, the password should be considered to be insecure, and so it's time to change it. Some users like simple and easy to remember passwords, unfortunately. This program is very applicable for NT workstations, where users can access a hard drive from another computer in the network and copy a SAM registry key, where password hashes are stored. Also, users can sniff a network and recover password hash from sniffer results. Advanced NT Security Explorer (ANTExp) will help you in your way to complete system security. In addition, ANTExp could be used for recovering lost passwords of particular users.

Info/Download:

< <http://www.net-security.org/various/software/979837872,60459,windows.shtml> >

MACLOCKSMITH 2.4.0

The MacLocksmith is an useful application to save your files from indiscreet eyes. It protects your files/folders quickly by using a very strong encryption method and a password. The MacLocksmith supplies also a second, soft and fast, protection system, you may use it in situations of already high security level. The MacLocksmith allows you to create Cryptet. Cryptets are stand alone autodecrypting applications containing one encrypted or protected file. A Cryptet may decrypt the contained file or simply save it on HD. Distribution of encrypted files is no longer a problem, now. You may create FAT, PPC or 68k applications and choose a text file that will be used, by created Cryptet, as custom About box.

Info/Download:

< <http://www.net-security.org/various/software/979838190,4213,mac.shtml> >

POWERCRIPT

PowerCrypt implements the major cryptographic methods, standards and hash algorithms: DES, IDEA, RSA, DSA, PKCS, MD2, MD5. As well, PowerCrypt implements the major secure e-mail protocols: PEM, S/MIME. PowerCrypt handles standard X 400 certificates: It stores received new certificates both as a local password protected copy and a public copy in a central Certificate Directory accessible to other users. It creates new keys and prototype certificates for certificate requests.

Info/Download:

< <http://www.net-security.org/various/software/979840697,21005,mac.shtml> >

ENSCRIPT 2.0

EnScript is an encryption tool for Macintosh based scripting environments. It gives Macintosh cryptographers and developers what they need to build digital signatures, secure passwords, and other security.

Info/Download:

< <http://www.net-security.org/various/software/979841473,82473,mac.shtml> >

SECUREPASS 2.01

This is a secure Macintosh archiving utility for passwords and other security keys. Designed for the user who accesses secure network services or who deals with multiple passkeys that are difficult to secure, memorize, use, change, or keep track of.

Info/Download:

< <http://www.net-security.org/various/software/979841570,22014,mac.shtml> >

PALMPASSWORD

PalmPassword is a dual application with a PC and Palm Connected Organizer module, which working together do exactly that - create the perfect way to keep your personal account and password information both secure and mobile.

Info/Download:

< <http://www.net-security.org/various/software/979841841,68017,palm.shtml> >

Defaced archives

[22.01.2001] - Guardian Security Company

Original: <http://www.guardian-security.net/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/22/www.guardian-security.net/>

[22.01.2001] - Canon (Greece)

Original: <http://www.canon.gr/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/22/www.canon.gr/>

[22.01.2001] - ByteCom (Morocco)

Original: <http://www.bytecom.net.ma/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/22/www.bytecom.net.ma/>

[22.01.2001] - #2 U.S. Navy Electronic Commerce Homepage

Original: <http://www.ec.navsup.navy.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/22/www.ec.navsup.navy.mil/>

[22.01.2001] - Chanel

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/22/www.chanel.com/>

[22.01.2001] - Ford Motor Company

Original: <http://media.ford.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/22/media.ford.com/>

[22.01.2001] - Microsoft Corporation (NZ)

Original: <http://www.microsoft.co.nz/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/23/www.microsoft.co.nz/>

[23.01.2001] - Ford Motors (Korea, south)

Original: <http://www.ford.co.kr/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/23/www.ford.co.kr/>

[23.01.2001] - EPSON New Zealand

Original: <http://www.epson.co.nz/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/23/www.epson.co.nz/>

[23.01.2001] - Fiat Auto (U.K.)

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/23/www.fiat.co.uk/>

[23.01.2001] - Mitsubishi

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/23/www.mitsubishi.co.uk/>

[23.01.2001] - Toyota (CN)

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/24/www.toyota.com.cn/>

[24.01.2001] - Compaq Computer Corporation

Original: <http://www.millicent.digital.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/24/www.millicent.digital.com/>

[24.01.2001] - Iranian Television

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/24/www.irtv.com/>

[24.01.2001] - Acer Computers (CN)

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/24/www.acer.com.cn/>

[24.01.2001] - EXCALIBUR Group, A Time Warner Company

Original: <http://www.neo.rr.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/24/www.neo.rr.com/>

[25.01.2001] - Coca-Cola (DK)

Original: <http://www.coca-cola.dk/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/25/www.coca-cola.dk/>

[25.01.2001] - Inprise Korea

Original: <http://www.borland.co.kr/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/25/www.borland.co.kr/>

[25.01.2001] - U.S. Navy

Original: <http://nif.navy.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/25/nif.navy.mil/>

[26.01.2001] - Homepage Central

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

Defaced: <http://www.attrition.org/mirror/attrition/2001/01/26/www.internationalhosting.com/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>