

Net-Sec newsletter
Issue 34 - 16.10.2000
<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) Security software
- 7) 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

SMALL BUSINESSES, BIG SECURITY RISKS

According to a survey released by analyst GartnerGroup smaller companies particularly lack the security expertise necessary to fend off computer attackers. Its research suggests that, without taking immediate steps to remedy the situation, 50 percent of these businesses will be the victim of a successful hack or a damaging virus outbreak in the next couple of years.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2640674,00.html>

SECURITY BREACH AT BUY.COM

A security hole on buy.com's website exposed the personal information

of customers who returned products to the company. For several hours on Thursday, the buy.com website allowed determined visitors to peruse the names, addresses, and phone numbers of customers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://wired.com/news/technology/0,1282,39438,00.html>

ATTACKING EAGLE NETWORK

A Nederland-based Internet company was back online Wednesday after 11 days during which executives say their service was held hostage by a European hacker making political and monetary demands.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.denverpost.com/business/biz1012d.htm>

ISS UNLEASHES SERVER SECURITY

Security management solutions company, Internet Security Systems has released its RealSecure Server Sensor software, which enables organisations to protect their servers by detecting attacks, and preventing system misuse.

Link: <http://www.netimperative.com/technology/newsarticle.asp?ArticleID=5780>

WATCH OUT FOR MALICIOUS HTML PAGES

Recently discovered security hole in Internet Explorer 5 (allowing for not signed ActiveX components to perform malicious actions on PC) led to invention of new virus called GODMESSAGE. The computer can be infected by simply viewing the web page, containing the Active X applet. Message from the creators : "godmessageIV.html - view, get rooted. It is a modified tHing 1..6 server without ICQ notification, without hide process (so it will run on NT/w2k). A fellow named splyc took out the ICQ notification which I got from blade's forums. I took out the hide process function because it was not allowing the tHing to run on NT or 2k. The tHing listens on port 7777 and the password is pass."

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

BYPASSING EMAIL SERVERS WITH FTPMAIL

FTPMail is a secure communication platform that uses the Point to Point File Transfer Protocol as its exclusive means of information transfer instead of Simple Mail Transport Protocol (SMTP). Some of its features are: Guaranteed Online Privacy, Secure Data Transmissions, Untraceable through SMTP or POP, Does not utilize conventional ports, Password protected interface, Encrypted Message Database...

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

FINAL CIPHER FROM "THE CODE BOOK" CRACKED

A team of researchers in Sweden has cracked the final cipher set by Simon Singh in "The Code Book" and claimed the £10,000 prize. It took a year and month between publication of the challenge and its completion without the use of a super computer.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/13929.html>

HACKERS GOING LEGIT

Hackers from Shanghai Internet Security Base Co. (www.ISBase.com), the largest—hacker organization in China, have begun looking for jobs assisting customers with network security work, reported the Qingnian Bao newspaper last month. It looks like many Chinese hackers are giving up the racket and going legit.

Link: <http://www.insidechina.com/localpress/chonline.php3?id=208769>

FIREWALLS

"Simply put, a Firewall is a system that prevents unauthorized access to or from a private network by examining the incoming packets and/or requests coming from (in this case) the Internet. Here's an analogy, let's say a firewall is like a bouncer at a 21 and over bar called MyNetworkRocks, and the unauthorized InternetGuru is under 21. Well, because InternetGuru is under 21 he's not getting past the firewall (bouncer) into MyNetworkRocks, at least not easily. Firewalls can be setup with software, hardware, or both, depending on how paranoid, I mean secure, you want to be."

Link: <http://www.techextreme.com/display.asp?ID=228&Page=1>

INTERPOL ORDERS IMMEDIATE CYBERCRIME ACTION

The head of Interpol has warned nations, law enforcement groups and companies to act swiftly if they are to stand any chance of beating cybercrime. Speaking at a conference in London Wednesday, Raymond Kendall, secretary general of Interpol said his organisation is concerned that unlawful computer techniques are developing at such a rate that they represent a "new phenomenon" for international law enforcers. Kendall urged international organisations not to wait for conventions to be passed before drawing up guidelines for an allied response to the threat of cybercrime.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/40/ns-18393.html>

FORMER BELLCORE CEO SEES LOOMING NETWORK SECURITY ISSUES

"Network security will be a bigger problem than data security," according to former Bellcore CEO George Heilmeier. Heilmeier offered 10 predictions for the IT and telecom industries at a forum this week at Columbia University. Heilmeier explained that third parties who intentionally block access to e-mail pose a greater danger than the risk the information will be read.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.telekomnet.com/writer_telekomnet/10-11-00_sidebar.asp

ANDY MUELLER-MAGUHN ELECTED TO ICANN BOARD

The five new grass-roots members, each representing a major region of the globe, will be a part of a 19-member board elected to run the Internet Corporation for Assigned Names and Numbers, the group charged with overseeing the technical functions of the global Internet. One of the five regional directors is Chaos Club member Andy Mueller-Maguhn.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2639191,00.html>

DEVELOPER TACKLES WAP SECURITY GLITCH

A Swedish company claims that it can solve the security problems related to Wap by doing away with the Wap gateway. Mi4e, developer of mobile internet infrastructure software, has unveiled its ThunderWap software

series, which allows businesses to offer instant Wap capabilities to users without employing a portal.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1112381>

GATES PENETRATING TO NASA

The Orange County Register said its Web site was infiltrated Sept. 29 and an article was changed to say Microsoft Corp. Chairman Bill Gates had been arrested for breaking into NASA computers. Original one for sure...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.denver-rmn.com/business/1011msft8.shtml>

HARDWARE FIREWALL RUNS ON NSA TECHNOLOGY

A relationship with the National Security Agency has netted Marconi Communications the technology to produce a firewall that is said to run at OC-12 speeds (622 Mbits/second) and to be undetectable to potential intruders. The technology, licensed from the NSA and sold back to the agency in product form, is part of a longstanding relationship between government agencies and Fore Systems Inc., which Marconi (Pittsburgh) acquired last year.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.electronicstimes.com/story/OEG20001009S0056>

SECURE VPN

Dynarc is signing a purchase agreement worth \$1.2 million over the next 12 months with Sonet Communications. Dynarc's auto-provisioning routers will contribute to Sonet's initial 10-city network development plan, which will provide business SOHO customers with a high-speed, secure virtual private network (VPN) delivering gigabit data transfer speeds, video and voice over a fiber-optic IP network.

Link: <http://www.fiberopticsonline.com/content/news/article.asp?DocID={C6B5488D-9E9D-11D4-8C6C-009027DE0829}>

LIB DEM EMAILS PENETRATED

A Labour party MP is alleged to have illegally penetrated into a Liberal Democrat's email. Following the allegations, House of Commons officials have been asked to launch an investigation, and a memo has been circulated in the Lib Dem party, warning members to take precautions to protect their emails.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/13864.html>

CYBERWAR

Chinese "hackers" have threatened to destroy rival Taiwan's websites as the island state prepares to celebrate national day on Tuesday, television reports said. The Chinese "hackers" may penetrate major government websites as well as some civil websites close to President Chen Shui-bian, the cable television TVBS said Monday.

Link: <http://www.insidechina.com/news.php3?id=207812>

RED HAT RESPONDS TO QUALITY ALLEGATIONS

This a summary of the events that occurred after the release of Red Hat 7 and it contains a response from the Red Hat people. It also includes some embarrassing comments regarding Slashdot's Red Hat story in which they published that the distribution had over 2,500 bugs.

Link: http://linuxtoday.com/news_story.php3?ltsn=2000-10-09-005-21-NW-CY-RH

FBI PUSHES FOR CYBER ETHICS EDUCATION

FBI agents are spreading a new gospel to parents and teachers, hoping they'll better educate youths that vandalism in cyberspace can be economically costly and just as criminal as mailbox bashing and graffiti spraying. The Justice Department and the Information Technology Association of America, a trade group, has launched the Cybercitizen Partnership to encourage educators and parents to talk to children in ways that equate computer crimes with old-fashioned wrongdoing.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/10/09/ethics.in.cyberspace.ap/index.html>

ENIGMA TO BE RETURNED?

The head of Bletchley Park spy museum is confident that the stolen Enigma code machine will be returned after she spoke directly to one of the mystery men demanding £25,000 for the encrypter.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ananova.com/news/story/sm_79029.html

WEB-BASED E-MAIL ISN'T SAFE FROM CORPORATE EYES

Slashdot has a big discussion related to the October 3rd CNET article - "Unfortunately, security experts say many employees would be surprised to know that Web-based email services also offer little privacy. Messages sent via a Yahoo or Hotmail account, or through instant messaging products, such as ICQ or America Online's Instant Messenger (AIM), are just as accessible to nosy employers."

Link: <http://slashdot.org/article.pl?sid=00/10/08/2048204>

CYBERCRIME TREATY

The new, improved draft of the international Cybercrime treaty is out, and David Banisar says it's bigger and badder than ever.

Link: <http://www.securityfocus.com/commentary/98>

Security issues

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

MASTER INDEX TRAVERSE ADVISORY

Synnergy Labs has found a flaw within Master Index that allows a user to successfully traverse the filesystem on a remote host, allowing arbitrary files/folders to be read.

Link: <http://www.net-security.org/text/bugs/971179170,91401,.shtml>

DEBIAN LINUX - NEW VERSIONS OF BOA PACKAGES

In versions of boa before 0.94.8.3, it is possible to access files outside of the server's document root by the use of properly constructed URL requests. This problem is fixed in version 0.94.8.3-1, uploaded to Debian's unstable distribution on October 3, 2000. Fixed packages are also available in proposed updates and will be included in the next revision of Debian/2.2 (potato).

Link: <http://www.net-security.org/text/bugs/971179295,4133,.shtml>

DEBIAN LINUX - ESOUND PACKAGE IS NOT AFFECTED

Linux-Mandrake has recently released a Security Advisory covering a race condition in the esound.

Link: <http://www.net-security.org/text/bugs/971179403,38597,.shtml>

CONNECTIVA LINUX - TMPWATCH LOCAL DOS

Versions of the tmpwatch package as shipped with Conectiva Linux contain a vulnerability which could lead to a local DoS. These versions, though, are not vulnerable to the local root exploit published earlier because they do not have the fuser option, which appeared only in later versions.

Link: <http://www.net-security.org/text/bugs/971179510,7441,.shtml>

SUSE LINUX - NOT AFFECTED TO TMPWATCH PROBLEM

"The tmpwatch packages as shipped with SuSE distributions are not vulnerable to the attacks as discussed on security forums, initiated and discovered by zenith parsec. The version of tmpwatch that we ship is a bit older than the bleeding edge, but it has proven to do what it says, which is just as important. We did not (silently) fix the problems in the package - the version that we use does not have the features that cause the security problems."

Link: <http://www.net-security.org/text/bugs/971179586,22555,.shtml>

TRUSTIX SECURE LINUX - TMPWATCH PROBLEMS

All versions of Trustix Secure Linux have hitherto been shipped with a version of tmpwatch that can be tricked into excessive fork()ing filling up the process table, requiring the box to be rebooted. The version of tmpwatch can also, in certain cases, be tricked into giving local users a root shell.

Link: <http://www.net-security.org/text/bugs/971179653,98073,.shtml>

EXTROPIA WEBSTORE DIR TRAVERSAL VULNERABILITY

The Web Store is a shopping cart product by eXtropa. This script merges Selena Sol's Electronic Outlet HTML and Database shopping cart apps and adds all new routines for error handling, order processing, encrypted mailing, frames, Javascript and VBscript.

Link: <http://www.net-security.org/text/bugs/971179782,82714,.shtml>

INTERACTIVE'S WEB SHOPPER DIR TRAVERSAL VULNERABILITY

shopper.cgi allows users to switch between product pages using the \$VALUES{'newpage'} variable. This would make <http://example.com/cgi-bin/shopper.cgi?newpage=product1.htm> display product1.htm. Although this script has regex statements that single out the double dot (..), it does not perform these checks by default.
Link: <http://www.net-security.org/text/bugs/971179934,13930,.shtml>

MICROSOFT SECURITY - "SHARE LEVEL PASSWORD" PATCH

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Windows 95, 98, 98SE, and Windows Me. The vulnerability could allow a malicious user to programmatically access a Windows 9x/ME file share without knowing the entire password assigned to that share.
Link: <http://www.net-security.org/text/bugs/971265164,93554,.shtml>

MANDRAKE LINUX - OPENSSSH UPDATE

A problem exists with openssh's scp program. If a user uses scp to move files from a server that has been compromised, the operation can be used to replace arbitrary files on the user's system. The problem is made more serious by setuid versions of ssh which allow overwriting any file on the local user's system.
Link: <http://www.net-security.org/text/bugs/971265294,96285,.shtml>

SHRED 1.0 BUG REPORT

Ran a test with Shred v1.0 and found some unexpected results. This utility is supposed to overwrite a file with several passes of different bit patterns followed by one random pattern. The file is then unlinked. This is supposed to make the file unrecoverable with utilities which read raw disk blocks. Using the icat utility from Dan Farmer and Wietze Venema's TCT Toolkit it appears that the data is not overwritten. This test was done on two different RedHat 6.0 systems.
Link: <http://www.net-security.org/text/bugs/971265364,54158,.shtml>

HP JETDIRECT MULTIPLE DOS

The firmware in the HP JetDirect card contain multiple vulnerabilities that can have effects ranging from the service crashing to the printer initiating a firmware upgrade based on random garbage in the memory, and in the last case powercycling won't fix the crash. It requires a new firmware burn by eg. HP to restore the Jetdirect card.
Link: <http://www.net-security.org/text/bugs/971265417,19017,.shtml>

MS - WEBTV FOR WINDOWS DENIAL OF SERVICE

There is a denial of service vulnerability in WebTV for Windows that may allow a malicious user to remotely crash either the WebTV for Windows application and/or the computer system running WebTV for Windows. Restarting the application and/or system will return the system to its normal state. Microsoft has released a patch that eliminates this security vulnerability.
Link: <http://www.net-security.org/text/bugs/971375310,5567,.shtml>

MANDRAKE LINUX - APACHE UPDATE

The Apache web server comes with a module called mod_rewrite which is used to rewrite URLs presented by the client prior to further processing. There is a flaw in the mod_rewrite logic that allows an attacker to view arbitrary files on

the server system if they contain regular expression references.

Link: <http://www.net-security.org/text/bugs/971375814,81283,.shtml>

PHP REMOTE FORMAT STRING VULNERABILITIES

Format string vulnerabilities exist in the error logging routines of PHP versions 3 and 4, allowing remote users to execute arbitrary code under the web server's user id. A web server having PHP installed and one or more PHP scripts is vulnerable to the problem if error logging is enabled in php.ini. Also any PHP script using the "syslog" command of PHP may be vulnerable, regardless of error logging.

Link: <http://www.net-security.org/text/bugs/971375894,65809,.shtml>

PROBLEM WITH NETSCAPE MESSAGING SERVER 4.15

The problem is that the POP3 server displays a different message for an authentication error due to an invalid password then for one due to an invalid username. This could be used to "harvest" email addresses for spam lists.

Link: <http://www.net-security.org/text/bugs/971439529,51461,.shtml>

APACHE 1.3.14 RELEASED

The Apache Software Foundation and The Apache Server Project are pleased to announce the release of version 1.3.14 of the Apache HTTP server. Version 1.3.13 was never released. This version of Apache is primarily a security fix and bug fix release, but there are a few new features and improvements.

Link: <http://www.net-security.org/text/bugs/971484402,83017,.shtml>

DEBIAN LINUX - CURL AND CURL-SSL UPDATE

The version of curl as distributed with Debian GNU/Linux 2.2 had a bug in the error logging code: when it created an error message it failed to check the size of the buffer allocated for storing the message. This could be exploited by the remote machine by returning an invalid response to a request from curl which overflows the error buffer and trick curl into executing arbitrary code.

Link: <http://www.net-security.org/text/bugs/971559341,76634,.shtml>

REMOTE RETRIEVAL OF AUTHENTICATION DATA FROM IE

"We will show that it could be possible to retrieve the cached authentication data from your user's web browser with little or no user's cooperation, even when due care was taken to protect the communication between browser and server with SSL."

Link: <http://www.net-security.org/text/bugs/971559586,2881,.shtml>

MS - "CACHED WEB CREDENTIALS" VULNERABILITY

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Internet Explorer. Under a daunting set of conditions, the vulnerability could enable a malicious user to obtain another user's userid and password to a web site.

Link: <http://www.net-security.org/text/bugs/971559684,92219,.shtml>

MANDRAKE LINUX - MOD_PHP3 UPDATE

PHP version 3 which ships with Linux-Mandrake are vulnerable to format string attacks due to logging functions that make improper use of the syslog() and

vsprintf() functions. This renders PHP3-enabled servers vulnerable to compromise by remote attackers. This attack is only effective on PHP installations that log errors and warnings while those servers that do not are not affected. By default, Linux-Mandrake systems do not have logging enabled.

Link: <http://www.net-security.org/text/bugs/971559791,26568,.shtml>

ANACONDA FOUNDATION DIRECTORY VULNERABILITY

Synnergy Labs has found a flaw within Anaconda Foundation Directory that allows a user to successfully traverse the filesystem on a remote host, allowing arbitrary files/folders to be read

Link: <http://www.net-security.org/text/bugs/971559891,18741,.shtml>

CALDERA SECURITY UPDATE: FORMAT BUG IN PHP

There's a format bug in the logging code of the mod_php3 module. It uses apache's aplog_error function, passing user-specified input as the format string. This can be exploited by a remote attacker to execute arbitrary shell commands under the HTTP server account (user httpd). In order for this bug to be exploitable, the PHP error logging must be enabled. By default, error logging is off.

Link: <http://www.net-security.org/text/bugs/971690142,53185,.shtml>

WINU 1.0-5.1 BACKDOOR PASSWORDS

"After downloading WinU 5.1 I noticed the built-in "emergency password" capability, mentioned in the help file. I decided to take a look around.

AND WOW! GOT 'EM ALL!"

Link: <http://www.net-security.org/text/bugs/971690328,13624,.shtml>

DEBIAN LINUX - LOCAL EXPLOIT IN NIS PACKAGE

The version of nis as distributed in Debian GNU/Linux 2.1 and 2.2 contains an ypbind package with a security problem. ypbind is used to request information from a nis server which is then used by the local machine. The logging code in ypbind was vulnerable to a printf formatting attack which can be exploited by passing ypbind a carefully crafted request. This way ypbind can be made to run arbitrary code as root.

Link: <http://www.net-security.org/text/bugs/971690367,54647,.shtml>

MS - "NETMEETING DESKTOP SHARING" VULNERABILITY

Microsoft has released a patch that eliminates a security vulnerability in NetMeeting, an application that ships with Microsoft Windows 2000 and is also available as a separate download for Windows NT 4.0. The vulnerability could allow a malicious user to temporarily prevent an affected machine from providing any NetMeeting services and possibly consume 100% CPU utilization during an attack.

Link: <http://www.net-security.org/text/bugs/971690405,3329,.shtml>

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

SITEARMOR SUITE OF ADVANCED SECURITY OPTIONS - [10.10.2000]

To protect e-businesses from hacker intrusion and denial of service attacks, Space4rent.com announced the launch of its SiteArmor suite of security services, a comprehensive compilation offering customers complete, scalable security services designed to protect Internet-based applications, data and e-commerce activities.

Press release:

< <http://www.net-security.org/text/press/971180165,61814,.shtml> >

INVENTORS OF PKI CRYPTOGRAPHY AWARDED BY MARCONI - [11.10.2000]

Two innovators whose mathematical formulations developed nearly 25 years ago unleashed the key to private communications and secure transactions on the Internet will receive the 26th annual Marconi International Fellowship award October 10 for their breakthrough invention and activism in the cause of privacy rights. Whitfield Diffie and Martin Hellman will share the \$100,000 fellowship prize honoring advances in telecommunications for humanitarian benefit, to be presented at Columbia University in New York City, the academic home of the Marconi International Fellowship Foundation.

Press release:

< <http://www.net-security.org/text/press/971265008,5331,.shtml> >

COM21 LICENSES SONICWALL TECHNOLOGY - [13.10.2000]

SonicWALL, Inc., a leading provider of Internet security solutions, announced a license agreement with Com21 to embed its high performance Internet security technology into Com21's Internet access products. Under the terms of the agreement, SonicWALL will embed its security technology into consumer cable modems manufactured by Com21, enabling service providers to deliver secure access and other value added services to their broadband subscribers.

Press release:

< <http://www.net-security.org/text/press/971439887,80256,.shtml> >

ALADDIN SECURES HONG KONG'S ESDLIFE PORTAL - [14.10.2000]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, announced that Hong Kong's high-profile Electronic Service Delivery (ESD) Scheme uses Aladdin's eSafe for proactive and comprehensive Internet security.

Press release:

< <http://www.net-security.org/text/press/971528523,49326,.shtml> >

CO-OPERATION ON SMART CARD PKI - [16.10.2000]

Fingerprint Cards AB and Litronic Inc. have signed a Memorandum of Understanding that they will co-operate on the development of a new, strong authentication solution combining fingerprint biometrics and smart card based digital signatures on the Microsoft Windows Powered Smart Card platform.

Press release:

< <http://www.net-security.org/text/press/971690462,22362,.shtml> >

NETWORK-1 SECURITY SOLUTIONS AND RIPPLE PARTNER - [16.10.2000]

Network-1 Security Solutions, Inc., a leader in distributed intrusion prevention solutions for e-Business networks, announced a strategic technology alliance with Ripple Technologies, Inc., a leading developer of enterprise-wide, management system solutions. Network-1 has entered into an agreement to include RippleTech LogCaster, a Windows NT and Windows 2000 systems and applications management software, in its CyberwallPLUS family of distributed firewalls.

Press release:

< <http://www.net-security.org/text/press/971708821,6720,.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.

UNVERIFIED FIELDS - A PROBLEM WITH FIREWALLS & FIREWALL TECHNOLOGY TODAY by Ofir Arkin

The following problem (as discussed in this paper) has not yet been identified. Certain firewalls today, will not authenticate the validity of certain protocol fields, within the packet they are processing. The risk is exposure of information. What kind of information can be exposed? Mainly it will be unique patterns of behavior produced by the probed machines answering our crafted queries (or other kind of network traffic initiated in order to elicit a reply). Those patterns will help a

malicious computer attacker to identify the operating systems in use.

Paper:

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

SUID PROGRAMS, GETTING TO THE ROOT OF THE PROBLEM
by Aleksandar Stancin aka D'Pressed

Here we go again. There are still some little touches left to make your linux even a bit more secure, involving suid, nouser, sudo and etc. Now, this article is also newbie friendly, but also it requires some small amount of knowledge.

Article:

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

TESTING TIMES FOR TROJANS by Ian Whalley

In the field of computing, Trojan horses have been around for even longer than computer viruses – but traditionally have been less of a cause for concern amongst the community of PC users. In recent years, however, they have been the focus of increased attention from anti-virus companies and heightened levels of user concern. This paper aims to investigate the Trojan phenomenon; particular attention will be paid to the claims made in the field of NVM detection and those made by those who aim to test the vendors' claims.

Paper:

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

A STUDY-GUIDE ON HOW TO DETECT A VIRUS HOAX YOURSELF by Kaspersky Lab

It is difficult to imagine anybody today who does not treat computer viruses as a real threat to a regularly functioning computer system. However, contiguously with the virus spreading has occurred another syndrome, which is not any less dangerous – virus hoaxes.

Article:

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

THINK UNIX

The many variants of the Unix operating system require use of a mode of thought that's significantly different from the one that's required by simpler operating systems. Think Unix introduces readers to important fundamental and intermediate Unix commands and, in the process, inculcates them in the Unix way of thinking. It's a worthy goal in a world with more Linux users than ever, and author Jon Lasser accomplishes it. He's both a capable writer and a knowledgeable user of Unix shell commands. Lasser uses bash under Red Hat Linux in most examples, which usually apply equally well to other Unix variants, and makes asides about other shells and environments, as needed.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/078972376X/netsecurity> >

SOLARIS 8: THE COMPLETE REFERENCE

This book shows you what you need to understand if you want to make a living as administrator of a modern Sun workstation. Of course, this book is not absolutely complete - no technical book about a subject as large as Solaris 8 could hope to be - but it should be more than adequate for most readers' purposes. Whether you have experience with another enterprise operating system and have recently been charged with figuring out Solaris, or you're a long-time Solaris jock and need a handy reference to guide you through procedures that you don't follow every day, this book has your number.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0072121432/netsecurity> >

STEAL THIS COMPUTER BOOK: WHAT THEY WON'T TELL YOU ABOUT THE INTERNET

Viruses, e-mail bombings, ANSI bombings, keystroke monitors, scams - just what are these phenomena? Steal This Computer Book answers this question and discusses the ethical issues surrounding hacking. This thoroughly updated new edition incorporates the latest on: Trojan Horse programs how they work, where to find them, and what kind of damage they can cause; the illegal copying of MP3 music files and DVD-encrypted movie disks; computer forensics used for recovering deleted data; security issues accompanying broadband Internet technologies; and more. A gallery of hacker's tools and a CD-ROM with various antihacker and security tools are included.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1886411425/netsecurity> >

THE HUNDREDTH WINDOW: PROTECTING YOUR PRIVACY AND SECURITY IN THE AGE OF THE INTERNET

The proverbial hundredth window represents the most vulnerable link in a system. It derives from an allegory relating castle windows to potential security holes. If even one out of a hundred windows is left open, security becomes compromised. Since the Internet maximizes information sharing (admittedly a largely beneficial enterprise) would-be big-time marketers and shady characters can - without trying all that hard--spy on your Web clicking habits, read your e-mail, and even see files on your hard disk drive. This means you may receive spam from marketers who think they know what kind of stuff you like to buy--e-mail that can be helpful to some and aggravating to others. Sharing your name and other identifying personal information can cause you more serious problems: someone else could use that information to commit fraud or other crimes--and you would be responsible.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/068483944X/netsecurity> >

WINDOWS: SYSTEM POLICY EDITOR

Considering that most administrators could figure out the System Policy Editor through experimentation and some study of its documentation - this book includes lots of advice on proper use of the utility. Case studies are most helpful; a typical one explains how to set up system policies for a machine that will live in a university computer lab that's accessible to the public. Topics covered: How and why to use the Windows System Policy Editor to set user, group, and computer access privileges on computers that run Windows 9x and Windows NT. The user interface is fully documented, as are the structure and syntax of policy files and templates.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1565926498/netsecurity> >

Security Software

All programs are located at:

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

ADVANCED PASSWORD GENERATOR 2.7

Advanced Password Generator is a application designed to generate passwords of any length and character content. Advanced Password Generator allow users to do choice random number generator, which built into this application. This feature is used to generate an extremely random seed value.

Link:

< <http://net-security.org/various/software/971265936,63201,.shtml> >

SYBERGEN SECURE DESKTOP 2.1

Sybergen Secure Desktop is a personal firewall software that protects a single computer from malicious intruders and Trojan horse applications. Unlike standard network firewalls, Secure Desktop guards against these attempts while users are not connected to a corporate network.

Link:

< <http://net-security.org/various/software/971265985,41824,.shtml> >

WEB CONFIDENTIAL 2.1 (SYSTEM 7)

Web Confidential is a security program that manages passwords with an intuitive card-file metaphor. The program is fully configurable and integrates easily into Netscape Navigator, Internet Explorer, and other similar applications. Web Confidential also lets you encrypt your password files with a key of up to 448 bits in length.

Link:

< <http://net-security.org/various/software/971266080,20694,.shtml> >

POLAR CRYPTO COMPONENT 1.0

This ActiveX component allows you to easily include powerful encryption and decryption features in your applications. It uses the strong SHS hash algorithm and the formidable Twofish encrypting algorithm with a 128-, 192-, and 256-bit key, thus ensuring maximum level security for the encrypted data.

Link:

< <http://net-security.org/various/software/971266181,17759,.shtml> >

Defaced archives

[08.10.2000] - Ohio State Government

Original: <http://www.oy2k.state.oh.us/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/08/www.oy2k.state.oh.us/>

[08.10.2000] - Southern New England Telecommunications

Original: <http://www.tsac.snet.net/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/08/www.tsac.snet.net/>

[08.10.2000] - The Centre for Electronics Design and Technology

Original: <http://www.cedt.iisc.ernet.in/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/08/www.cedt.iisc.ernet.in/>

[08.10.2000] - Naperville File Exchange

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/08/www.nfe.com/>

[09.10.2000] - Scania Slovenija, d.o.o.

Original: <http://www.scania.si/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/09/www.scania.si/>

[09.10.2000] - Arpao Servicos de Informatica Ltda

Original: <http://www.arpao.com.br/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/09/www.arpao.com.br/>

[10.10.2000] - Dalian Software Park Development

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/10/www.dlsoftwarepark.com/>

[10.10.2000] - LARC NASA

Original: <http://se-pc7.larc.nasa.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/10/se-pc7.larc.nasa.gov/>

[10.10.2000] - Net Deamon

Original: <http://www.netdaemon.org/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/10/www.netdaemon.org/>

[12.10.2000] - Mississippi State Board of Contractors

Original: <http://www.msdoc.state.ms.us/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/12/www.msdoc.state.ms.us/>

[12.10.2000] - Portland Communications Ltd

Original: <http://ksusha.port5.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/12/ksusha.port5.com/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>