

Net-Sec newsletter
Issue 36 - 30.10.2000
<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) Featured books
- 6) Security software
- 7) Defaced archives

=====
HELP NET SECURITY ANNIVERSARY

We are proud to announce the second anniversary of HNS. In these 2 years the site has grown and with dedication and enthusiasm it became all we ever wanted it to be. This doesn't mean we are going to stop here, we'll keep on working to bring you even more updates in all the sections, as well as original content. We would like to take this opportunity to thank all the visitors, contributors, affiliates and advertisers who have been with us these past 2 years and that have supported us, giving us the opportunity to make the site better day by day. If you have any ideas, comments or suggestions, please e-mail us, we would like to hear from you.

HNS staff
staff@net-security.org

=====
General security news

VIRUS THREAT'S BAD AND GETTING WORSE - ICSA SURVEY

The number of corporations infected by viruses this year has risen by 20 percent, with the pace of infections accelerating rapidly, according to a report issued Monday by anti-virus consulting firm ICSA.net. Larry Bridwell, content security program manager for ICSA Labs, and a study co-author, said the company's 2000 report indicates the danger for corporate "virus disasters" is worse now than it has ever been in the six years that ISCA has been conducting its annual virus surveys.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/10/24/news7.html>

SECURITY THROUGH OBSCURITY

Is security through obscurity ever a useful way to protect your network, or does it just make things easier for corporate spies and hackers? This week in Unix Security, Carole Fennelly investigates who's benefiting from this security tactic.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunworld.com/sunworldonline/swol-10-2000/swol-1013-unixsecurity.html>

US AND EUROPEAN HACKERS

"U.S. hackers are basically proving things to themselves for ego. European hackers include a significant number of individuals motivated by political, religious, and cultural deeply held beliefs," said Gartner Group computer security analyst William Malik. Bob Sullivan did an article, in which he is talking about difference between European and US hackers (at least his point of view).

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2644086,00.html>

BAD SIGNS

"Digital signatures are not signatures, and they will never fulfill their promise" - Bruce Schneier's opinion on The Standard.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://thestandard.com/article/display/0,1151,19485,00.html>

SDF PREPARES TO COMBAT CYBERTERRORISM

Japan's Defense Agency (SDF) is set to develop computer systems to combat attempts by cyber attackers to disrupt the country's defense operation by breaking into key computer systems, sources said Monday.

Link: <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20001024b5.htm>

DANISH VIGILANTE

CRN has a piece on Danish security company Vigilante and their product - SecureScan - which is an automated Internet security assessment service.

Link: <http://www.crn.com/sections/Upstart/Upstart.asp?RSID=CRN&ArticleID=20749>

FINAL VOTE ON SECRET SEARCHES BILL EXPECTED

Urgent alert from DefendYourPrivacy.com's mailing list - "Two weeks ago we warned you about S. 2516, the Fugitive Apprehension Act of 2000, which would empower federal bureaucrats to subpoena your electronic records without a warrant. This bill has now been attached to another piece of legislation -- The Presidential Threat Protection Act (HR 3048) - and is expected to come up for a final vote on Wednesday or Thursday (October 24 or 25.)"

Link: <http://www.cluebot.com/article.pl?sid=00/10/20/2341243&mode=nested>

PROTECTING FREEDOM OF EXPRESSION

The human rights body of the Organization of American States has approved a declaration that says the "consolidation and development of democracy depends

on the very existence of freedom of expression." The OAS's Inter-American Commission on Human Rights calls the declaration, a "fundamental document for the defense of freedom within the inter-American system."

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://cipherwar.com/news/00/freedom_of_expression.htm

'RUMOR' - SHARING AV UPDATES

Next week, a Network Associates subsidiary, MyCIO.com, will formally roll out Rumor, a Napster-like file-sharing technology for managing antivirus updates.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/42/ns-18647.html>

MICROSOFT NETWORK TROJANED INTO

Guardian Unlimited and some other media outlets reported that Hackers have broken into Microsoft's computer network and may have stolen blueprints to the latest versions of the company's Windows and Office software. And if you read the whole article you will come to the fact that attackers broken into the network by using simple trojan horse program with a bit of social engineering, so they were no hackers in this story.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.guardianunlimited.co.uk/internetnews/story/0,7369,388816,00.html>

CYBERCRIME DRAFT

European Committee On Crime Problems and Committee Of Experts On Crime In Cyber-Space in april released a paper for "Draft Convention On Cyber-Crime"

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://conventions.coe.int/treaty/en/projets/cybercrime.htm>

MICROSOFT HACKED... NOT

The Register - "MS hacked again - 'illuminati terrorists,' this time",
IT-Analysis.com - "Microsoft domain falls foul to hacker terrorists" (I presume the first article on this story, as I bookmarked it yesterday, and today lot of online news sites have information on this "issue". So is Microsoft hacked? Not of course... Some reader sent a mail to IT-Analysis.com staff saying that he checked DNS record for Microsoft.com and that they were corrupted. By searching microsoft.com in whois lookup, you come to:

MICROSOFT.COM.IS.SECRETLY.RUN.BY.ILLUMINATI.TERRORISTS.NET
MICROSOFT.COM

So as you could see there was no hacking activity in this case, but just some tactics of creating subdomains similar to the Microsoft's domain, so it could come out as part of search results. Do whois on Microsoft.com (just whois not a search like these 'journalists' did), and you will see that everything is fine with DNS records.

ISLAMIC ATTACKERS CRASH ISRAELI WEB SITES

Several Israeli Web sites containing the government's perspective on the Mideast conflict crashed after Islamic groups abroad jammed them with fake traffic. The cyberattack was the most intense since Israel's government launched its Internet sites several years ago, and opens a new front in Israel's confrontation with the Arab world.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.salon.com/tech/wire/2000/10/26/cyberwar/index.html>

BLACKHAT '00 SINGAPORE - GREG HOGLUND

Conference video from Blackhat '00 Singapore - Advanced Buffer Overflow Techniques. This is a technical talk aimed at people who have already been exposed to buffer overflows and want to learn more. The talk assumes the audience has at least some knowledge of CPU's and Processes.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/media/71>

LINUX FIREWALL SURVEY PART 3

In the final entry of a three-part series of firewall product reviews, Pawel Leszek looks at dedicated appliance firewalls based on Linux. "Fire and forget" is the main idea behind hardware firewall appliances like WatchGuard's Firebox II, the Raptor Firewall from Cobalt and Axent, the Phoenix Adaptive Firewall from Progressive Systems, and the T.Rex firewall appliance from Freemont Avenue Software.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxworld.com/linuxworld/lw-2000-10/lw-10-fwproducts3.html>

OBLIVION

Issue 8 of Oblivion, a monthly eZine dedicated to security, technology and internet issues, is out. Oblivion is released every month and is read by thousands around the world. So grab a copy today and get reading.

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

GLOBAL HACKER AGREEMENT COULD AFFECT BUG HUNTERS

The Council of Europe's Draft Convention on Cybercrime aims to foster a common international criminal policy that addresses offenses directed against computer systems, data or networks. The treaty is intended to encourage legislation around the world. More than 40 countries, including the United States, are participating in the treaty, which is set to be signed by December and adopted by the council's Committee of Ministers in early autumn 2001. The treaty could go too far by prohibiting tools commonly used by legitimate computer researchers to discover and fix software vulnerabilities, computer security experts say.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1005-200-3314003.html>

YANKEES WEB SITE ATTACKED

The team's official site, www.yankees.com, was temporarily closed early Friday. "There was a hacking incident. The Web site was temporarily shut down because of it," Yankees spokesman Rick Cerrone said. "We have turned it over to the FBI and intend to prosecute to the fullest extent of the law."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.salon.com/tech/wire/2000/10/27/hacker/index.html>

WAY BACK - WAZZU

Surfing through PSS, I found an article in Cheyenne security newswire from October 1996 which pointed out that the September edition of Microsoft's Solution Provider

CD contained a document infected with the WM.Wazzu virus. Old news, but it is interesting how Microsoft employees like viruses/trojans ;) Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://packetstorm.securify.com/advisories/cheyenne/cheyenne.003>

DO YOU KNOW IF YOUR DATA IS SAFE?

Brian Robison explains what companies need to do above and beyond the firewall level to ensure the protection and integrity of their information assets. This is an excellent non-technical article for the CTO or CIO trying to determine what kinds of safeguards need to be in place at their organization.

Link:

http://www.securityfocus.com/frames/?content=/templates/forum_message.html%3fforum=2%26head=3649%26id=3649

Security issues

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

PHP INFO WWW SEARCH AND SERVER INFO GATHERING

The `phpinfo()` function available from PHP versions gives out a `_LOT_` of server information, directories things are installed in, versions etc.

Link: <http://www.net-security.org/text/bugs/972433288,21401,.shtml>

POSSIBLE SECURITY ISSUE IN NAV2001 ON WIN2K

If you place a virus or other known malware in the `c:_RESTORE` folder Norton Antivirus will not scan that folder in a "full-system" scan. This seems to be Symantec's poor choice not to scan such files? However if you manually scan `C:_RESTORE NAV` will find the infected file but won't be able to delete, repair nor quarantine the file? This could lead a malicious user to drop files into the restore folder - there're a few obvious ways to exploit this.

Link: <http://www.net-security.org/text/bugs/972433331,66345,.shtml>

ALLAIRE'S JRUN PROBLEMS WITH WEB-INF DIRECTORY

A severe security flaw exists with Allaire's JRun 3.0 allowing an attacker to access `WEB-INF` directories on the JRun 3.0 server. The `WEB-INF` directory tree contains web application classes, pre-compiled JSP files, server side libraries, session information and files such as `web.xml` and `webapp.properties`.

Link: <http://www.net-security.org/text/bugs/972433386,31966,.shtml>

ALLAIRE JRUN 2.3 ARBITRARY FILE RETRIEVAL

Multiple show code vulnerabilities exist in Allaire's JRun Server 2.3 allowing an attacker to view the source code of any file within the web document root of the web server. Using the same vulnerability, it is also possible to retrieve arbitrary files that lie outside the web document root on the host operating

system's file system.

Link: <http://www.net-security.org/text/bugs/972433407,34255,.shtml>

ALLAIRE JRUN 2.3 REMOTE COMMAND EXECUTION

It is possible to compile and execute any arbitrary file within the web document root directory of the JRUN's web server as if it were a JSP file, even if the file type is not .jsp. If applications running on the JRUN 2.3 server write to files within the web document root directory, it is possible to insert executable code in the form of JSP tags and have the code compiled and executed using JRUN's handlers. This can potentially cause an attacker to gain administrative control of the underlying operating systems.

Link: <http://www.net-security.org/text/bugs/972433423,22015,.shtml>

MS - "SESSION ID COOKIE MARKING" BUG PATCHED

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Internet Information Server. The vulnerability could allow a malicious user to "hijack" another user's secure web session, under a very restricted set of circumstances.

Link: <http://www.net-security.org/text/bugs/972435493,54113,.shtml>

IIS UNICODE - '>' REDIRECT

"I was having problems executing a command that contains a redirect (>) using any of the IIS Unicode exploits. In order to get some interesting tools on the victim, you would probably want to have the victim to FTP to the attacker. Problem without redirect is that you cannot build the FTP command file, and you are a bit stuck."

Link: <http://www.net-security.org/text/bugs/972524142,79006,.shtml>

"VM FILE READING" VULNERABILITY PATCHED

Microsoft has released a patch that eliminates a security vulnerability in the Microsoft virtual machine, that originally was discussed in Microsoft Security Bulletin MS00-011. Like the original vulnerability, the new variant could enable a malicious web site operator to read files from the computer of a person who visited his site or read web content from inside an intranet if the malicious site was visited by a computer from within that intranet.

Link: <http://www.net-security.org/text/bugs/972524163,7,.shtml>

SUN SECURITY BULLETIN - BROWSER CERTIFICATES

Sun advises of a potential compromise of 2 specific security certificates which had limited distribution. Sun recommends that you follow the directions found at http://sunsolve5.sun.com/secbull/certificate_howto.html to determine if your web browser has accepted any of the potentially compromised certificates.

Link: <http://www.net-security.org/text/bugs/972524178,81366,.shtml>

HOTJAVA BROWSER 3.0 JAVASCRIPT BUG

There is a security vulnerability in HotJava Browser 3.0 which allows accessing the DOM of arbitrary URLs after viewing a web page. This allows stealing of cookies. The problem is opening an javascript: URL in a named window, which allows accessing the DOM of the document in the named window.

Link: <http://www.net-security.org/text/bugs/972524196,6460,.shtml>

WINDOWS (ME) PRINTER SHARING VULNERABILITY

"One of the new "features" of Windows ME that immediately caught my eye was that as soon as I got networking up and running it had gone ahead and created shortcuts to all visible network shares and installed all networked printers without even hassling me with one "are you sure" dialog. At first glance it appeared to be nothing more than an annoyance. Later I came to thinking that naturally host machines must keep a list of files needed to install their printer. What if we were to replace one of these files with a trojan? Or perhaps add a trojan onto this list of files?"

Link: <http://www.net-security.org/text/bugs/972650098,62744,.shtml>

RED HAT - UPDATED SECURE WEB SERVER PACKAGES

Security bugs in versions of Apache prior to 1.3.14 also affect Secure Web Server. A new release which incorporates 1.3.14 is now available.

Link: <http://www.net-security.org/text/bugs/972694410,70614,.shtml>

SUSE LINUX - LOCAL ROOT COMPROMISE

The ncurses library is used by many text/console based applications such as mail user agents, ftp clients and other command line utilities. A vulnerability has been found by Jouko Pynnönen in the screen handling functions: Insufficient boundary checking leads to a buffer overflow if a user supplies a specially drafted terminfo database file. If an ncurses-linked binary is installed setuid root, it is possible for a local attacker to exploit this hole and gain elevated privileges.

Link: <http://www.net-security.org/text/bugs/972694424,49042,.shtml>

NETBSD - REMOTE EXECUTION OF SHELL COMMANDS

When using the CGI interface of the Global v3.55 package, it's possible to execute random commands. The exploit of this is possible due to insufficient handling of quoted or escaped characters in this version, and command line arguments that are then handed off to shell commands.

Link: <http://www.net-security.org/text/bugs/972694452,89982,.shtml>

NETBSD - POSSIBLE REMOTE ROOT COMPROMISE

The cfd daemon in GNU CFEngine contains several format string vulnerabilities in syslog() calls. This could permit remote hosts to inject the network daemon with a message causing a segmentation fault. As cfd is almost always run as root due to its nature (centralized configuration management), this could lead to a root compromise.

Link: <http://www.net-security.org/text/bugs/972694471,61555,.shtml>

PROBLEMS WITH CISCO VCO/4000 SNMP

If an attacker knows the read-only community string of a VCO/4K, then they can obtain a list of users and their obfuscated passwords. The obfuscation can be easily reversed, allowing an attacker to obtain additional privileges on the VCO/4K.

Link: <http://www.net-security.org/text/bugs/972694517,63881,.shtml>

REMOTE AND LOCAL VULNERABILITIES IN PAM_MYSQL

pam_mysql is a pluggable authentication module to allow user authentication

against mysql databases. The module constructs SQL statements using user input (username and password) without escaping it. This leads to trivial attacks that can result in the exposure of plaintext passwords/ hashes to remote unauthorized login.

Link: <http://www.net-security.org/text/bugs/972694530,83265,.shtml>

CISCO CATALYST REMOTE COMMAND EXECUTION

Cisco Catalyst 3500 XL series switches have a webserver configuration interface. This interface lets any anonymous web user execute any command without supplying any authentication credentials by simply requesting the /exec location from the webserver.

Link: <http://www.net-security.org/text/bugs/972694543,5289,.shtml>

Security world

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

BETRUSTED CHOSEN BY NCIPHER TO GUARD ITS EMAIL - [25.10.2000]

beTRUSTed(sm), the PricewaterhouseCoopers unit that offers trust services for Internet transactions, has been chosen by leading Internet security company nCipher to help provide its employees with secure email and authenticated network access. nCipher will use beTRUSTed digital certificates to ensure the security of its electronic transactions - nCipher is itself a leading developer of high performance hardware security products for e-commerce and public key infrastructure (PKI) applications.

Press release:

< <http://www.net-security.org/text/press/972432017,44785,.shtml> >

SECOND G-8 CONFERENCE ON INTERNATIONAL SECURITY - [26.10.2000]

Symantec Corp., a world leader in Internet security technology, today announced it has again been invited to join the U.S. delegation at the G-8 Government/Industry Workshop on Safety and Confidence in Cyberspace, to be held Oct. 24 through 26 in Berlin. Ron Moritz, senior vice president and chief technical officer at Symantec, will serve as one of only seven U.S. industry delegates to the conference. The G-8 conference offers a unique opportunity for international government and private sector representatives to meet to discuss ways to combat computer crime.

Press release:

< <http://www.net-security.org/text/press/972432224,44203,.shtml> >

POINT-AND-CLICK PKI-BASED DIGITAL SIGNATURES - [26.10.2000]

E-business security leader Cylink Corporation today announced plans to bundle E-Lock Technologies' digital signature solution with Cylink's public key infrastructure (PKI) to provide a seamless point-and-click solution for securing electronic documents. Together, the solutions will enable healthcare providers, financial institutions and other organizations that handle sensitive electronic documents such as patient records and loan applications to maintain the highest levels of data confidentiality and dramatically streamline document processing

Press release:

< <http://www.net-security.org/text/press/972515023,50852,.shtml> >

SMART WATCH TOP RATED IN SC MAGAZINE - [26.10.2000]

WetStone Technologies is pleased to announce that SMART Watch, the company's premier product offering, earned a perfect 5 star rating from SC Magazine's product review team this October. SMART Watch is a Preemptive Hacker Defense Tool and host based intrusion detection system that detects when key "Watched" Files or Directories have been maliciously or accidentally altered.

Press release:

< <http://www.net-security.org/text/press/972523152,24040,.shtml> >

NORTON ANTIVIRUS FOR MACINTOSH RELEASED - [26.10.2000]

Symantec Corporation, today announced the latest versions of Norton Utilities for Macintosh and Norton AntiVirus for Macintosh. Norton Utilities for Macintosh 6.0 helps customers optimize performance and easily solve problems, such as disk errors, lost or accidentally erased data, or fragmented files. Norton AntiVirus for Macintosh 7.0 detects and repairs infected files to keep personal data safe and secure.

Press release:

< <http://www.net-security.org/text/press/972523671,14261,.shtml> >

PRIVACY CONFERENCE ANNOUNCED BY ZKS - [27.10.2000]

Zero-Knowledge Systems, the leading developer of privacy solutions for consumers and companies, today announced the first annual "Privacy by Design: The Future of Privacy Compliance and Business" conference, sponsored by Royal Bank Financial Group, IBM, Merrill Lynch, and PricewaterhouseCoopers. Bringing world-class privacy experts together with companies implementing privacy practices and solutions, the conference will be held at Le Chateau Montebello, Quebec from November 19 to 21, 2000.

Press release:

< <http://www.net-security.org/text/press/972648319,95401,.shtml> >

VPN SECURITY FOR FEDERAL LAW ENFORCEMENT - [27.10.2000]

V-ONE Corporation (Nasdaq:VONE), a leading provider of Virtual Private Networks (VPN), today announced it has been selected by Louisiana State University (LSU) and their subcontractor, Science Applications International Corporation (SAIC) to provide security for Law Enforcement Online (LEO), the Federal Bureau of Investigation (FBI) project which established the nation's first-ever communications mechanism to link all levels of law enforcement across the country

Press release:

< <http://www.net-security.org/text/press/972648475,5255,.shtml> >

SPHINX FIREWALL SOLUTION FROM BIODATA - [31.10.2000]

Biodata Information Technology, global leader in network and communications security, is recommending that home PC users as well as large corporations take further steps to protect their internal network or personal PC's connected to the Internet through `always on' cable, T1 or DSL connections. The announcement comes as attackers based in St. Petersburg, Russia, successfully employed an attack on Microsoft's network - stealing source code to the company's Windows operating system and Office software suite.

Press release:

< <http://www.net-security.org/text/press/972960020,30864,.shtml> >

PANEL DISCUSSION ON CYBERCRIME - [31.10.2000]

Symantec Corp., a world leader in Internet security, today announced Ron Moritz, senior vice president and chief technical officer at Symantec, has been invited to participate as a panel speaker at the Software Development Conference & Expo (SD 2000), to be held Oct. 29 - Nov. 2, at the Washington Convention Center in Washington D.C

Press release:

< <http://www.net-security.org/text/press/972960112,41653,.shtml> >

E-SECURITY EXECUTIVE BREAKFAST SERIES - [31.10.2000]

AXENT Technologies, Inc., one of the world's leading Internet security solutions providers for e-business, which recently entered into a definitive

merger agreement with Symantec Corporation, today announced their sponsorship of AXENT's Executive Breakfast Series for CXOs, senior level VPs, and senior management of Fortune 1000 companies. The series will feature Scott Charney, former Department of Justice chief of computer crime division, who will engage attendees by discussing his cyber-crime experiences and will offer a vision for executives on how to effectively minimize their e-business security risks.

Press release:

< <http://www.net-security.org/text/press/972960272,57108,.shtml> >

TRIPWIRE LINUX EDITION NOW AVAILABLE - [31.10.2000]

Tripwire, Inc., the leading provider of data and network integrity solutions, today announced the availability of its Open Source product for the Linux operating system. Delivering on the commitment made earlier this year, Tripwire Open Source, Linux Edition is hosted on VA Linux Systems' SourceForge, the world's largest Open Source development center. The software is also included on the recently announced Red Hat Linux 7 Open Source Operating System. Tripwire Open Source, Linux Edition will continue to be integrated into other Linux solutions.

Press release:

< <http://www.net-security.org/text/press/972960761,34362,.shtml> >

Featured articles

All articles are located at:

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

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

Below is the list of the recently added articles.

BEWARE THE PIF! - A DANGEROUS MONSTER CAN HIDE BENEATH HARMLESS FILES

Kaspersky Lab, an international anti-virus software development company, considers it necessary to draw users' attention to a threat that programs with PIF extension can pose to the normal operating of personal computers and corporate networks. Because of the lack of awareness of this problem Kaspersky Lab has begun to receive numerous reports of virus infections caused by this type of malicious program.

Read more:

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

VIRUSES: THEN AND NOW by Randy M. Nash

Computer viruses and the people who engineer them have grown smarter and more devious as technology has grown. Early computer viruses would attach themselves to executable files (either .COM or .EXE), or would infect diskettes and hard drives. They were silent, irritating, and sometimes devastating. They were commonly passed via floppy diskette when sharing files between one computer and another. They had such names as Stoned and Anti.Exe. That was then.

Read more:

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

THE HISTORY OF ZERO KNOWLEDGE SYSTEMS by Jordan Socran

Austin & Hamnett Hill - the brothers behind Zero-Knowledge Systems, were involved with the Internet at a very young age. At 21 Austin founded the ISP Infobahn Online Services with money from his father and a small group of investors. They soon called upon Hamnett, a 23 year-old reformed Deadhead studying accounting in Montana, to be CFO...

Read more:

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

PASSWORDS - THE WEAK LINK by Randy M. Nash

A chain is only as strong as its weakest link. In the security world, that weak link is the human element, and it manifests in the poor management of user passwords. As our society becomes increasingly wired we need to remember an increasingly large number of accounts, PINs, and passwords.

Read more:

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

ONLINE SECURITY: WHAT'S YOUR APPROACH? by Randy M. Nash

In the rush to get online, many companies consider security as an afterthought. The hurry to develop an online presence causes them to overlook the obvious... they could be compromised. Many companies are willing to accept this. They consider themselves too "low profile" to be at risk. The reality is, you don't have to be an e-Bay, Yahoo, or e-Trade to get attacked. Systems are compromised for several reasons.

Read more:

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

LINUX KERNEL INTERNALS

This book is written for anybody who wants to learn more about Linux. It explains the inner mechanisms of Linux from process scheduling to memory management and file systems, and will tell you all you need to know about the structure of the kernel, the heart of the Linux operating system. CD-ROM included.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201331438/netsecurity> >

EXAM CRAM CCNP ROUTING (EXAM CRAM)

The book sports some of the snappiest writing ever to grace an Exam Cram book which is good, because routing concepts are tricky little devils that you just can't memorize. You need to internalize how each of the various protocols works, and not just snarf down some list of functions. The explanations for the reason that each protocol (RIP, OSPF, EIGRP, BGP) was developed and how it's implemented are well written and concise. The occasional spot illustration helps flesh out your knowledge of how routers share information under each protocol. If you've been a trifle unclear on what the precise differences are between the various routing approaches, this is where all will be revealed. Later sections of the book deal with traffic management and routing updates, and do it well, mixing a bit of real-world experience with lectures to give a well-rounded approach. Sadly, information on actual router configuration is fairly spotty, so probably you'll want to write down some additional cheat sheets for the actual configuration commands.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1576106330/netsecurity> >

MICROSOFT WINDOWS ME SECRETS

For nearly a decade, Brian Livingston and Davis Straub have been tracking down the shortcuts, fixes, and workarounds that let you get more done - and have more fun - with Microsoft Windows. From streamlining Internet access to tweaking the Registry, their latest guide delivers hundreds of Windows Me secrets that will take your productivity to a new level.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0764534939/netsecurity> >

THE NEW HACKER'S DICTIONARY

This third edition of the tremendously popular Hacker's Dictionary adds 100 new entries and updates 200 entries. In case you aren't familiar with it, this is no snoozer dictionary of technical terms, although you'll certainly find accurate definitions for most techie jargon. It's the slang and secret language among computer jocks that offers the most fun. Don't know what the Infinite-Monkey Theorem is? Or the meaning of "rat dance?" It's all here. Most people don't sit down to read dictionaries for entertainment, but this is surely an exception.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0262680920/netsecurity> >

Security Software

All programs are located at:

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

FWLOGWATCH 0.0.22

fwlogwatch 0.0.22 is a RUS-CERT (Universitat Stuttgart Computer Emergency Response Team) project to build an ipchains packet filter log analyzer with text and html summary output, interactive incident report generator, and realtime anomaly response capability

Link:

< <http://net-security.org/various/software/972384323,89827,.shtml> >

ETHERREAL 0.8.13

Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session

Link:

< <http://net-security.org/various/software/972687117,59532,.shtml> >

MIMEDEFANG V.0.5

With the proliferation of e-mail trojans and viruses, e-mail is becoming a preferred mechanism for attacking PC's. The best way to avoid these trojans and viruses is

not to use any insecure client software on your PC (especially software from Microsoft, which is notorious for security problems.) Use Linux as your operating system and one of many excellent e-mail packages as your mail client

Link:

< <http://net-security.org/various/software/972729772,36460,.shtml> >

TRIPWIRE 2.3.47

Tripwire is a very popular file integrity checker which saves checksums of selected files in a database. Any changes to these files are flagged and logged, including those that were added or deleted, with optional email / pager reporting. Databases and reports are cryptographically signed.

Link:

< <http://net-security.org/various/software/972961108,21294,.shtml> >

Defaced archives

[23.10.2000] - North Eastern Wisconsin Linux Users Group

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/23/www.newlug.org/>

[24.10.2000] - Easy (YU)

Original: <http://www.easy.co.yu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/24/www.easy.co.yu/>

[24.10.2000] - Philippine Air Force

Original: <http://paf.mil.ph/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/24/paf.mil.ph/>

[25.10.2000] - FSCIT Mil (SE)

Original: <http://www.fscit.mil.se/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/25/www.fscit.mil.se/>

[25.10.2000] - FHS Mil (SE)

Original: <http://www.fhs.mil.se/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/25/www.fhs.mil.se/>

[25.10.2000] - Honda Motor Company Singapore

Original: <http://www.honda.com.sg/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/25/www.honda.com.sg/>

[25.10.2000] - Letterkenny Institute of Technology

Original: <http://dns2.lyit.ie/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/10/25/dns2.lyit.ie/>

[26.10.2000] - Mercedes Benz

Original: <http://www.mercedes-benz.ca/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/10/26/www.mercedes-benz.ca/>

[26.10.2000] - World Brokers

Original: <http://www.world-brokers.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/10/26/www.world-brokers.com/>

[26.10.2000] - Leonardo DiCaprio

Original: <http://www.leonardodicaprio.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/10/26/www.leonardodicaprio.com/>

[27.10.2000] - Atlas Security

Original: <http://www.atlassecurity.co.za/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/10/27/www.atlassecurity.co.za/>

[27.10.2000] - Ford Motors, Brasil

Original: <http://www.ford.com.br/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/10/27/www.ford.com.br/>

[27.10.2000] - Windows Guru

Original: <http://www.windowguru.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/10/27/www.windowguru.com/>

[28.10.2000] - Governo Do Estado De Sao Paulo

Original: <http://www.araraquara.sp.gov.br/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/10/28/www.araraquara.sp.gov.br/>

[28.10.2000] - AntiOnline

Original: <http://www.antionline.com/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/10/28/www.antionline.com/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org
<http://net-security.org>