

Net-Sec Newsletter
Issue 40 - 04.12.2000
<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

General security news

HONEYNET TEAM

During just one month of monitoring, the Honeynet team's "honey pot," which poses as a real network to attract attackers, had been scanned by hundreds of unique IP addresses looking for two particular ports: UDP (User Datagram Protocol) port 137, used by the NetBIOS Naming Service, and TCP port 139, the tried-and-true NetBIOS Session Service. This should not surprise loyal Security Watch students, who know that these ports, which are the Achilles' heels of Windows 9x/ME computers, turn users into "easy @Home and DSL victims." Knowing the proliferation of Windows 9x systems on the Internet and admitting more than idle curiosity about attackers targeting Windows systems, the team decided to build a default Windows 98 system with the entire C: drive shared to the world - hoping the "black-hat" bad guys would come. And come they did.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.idg.net/ic_296206_1794_9-10000.html

THE STORY OF JEFF - PART I and II

This story is the ongoing saga of Jeff, a tragic tale full of hardship, heartbreak and triumph over impossible odds. Jeff is your average network administrator, responsible for Acme Inc's Microsoft based corporate network. We start with the basics and steadily spiral into madness and insanity as Jeff's network is repeatedly broken into.

Part I: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/cover/coverstory20001127.html>

Part II: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/jeff20001201.html>

ANY PORT IS A HACKER STORM

"One of the biggest information giveaways for hackers is for you to have machines with ports that aren't in use but respond anyway. Windows, unfortunately, makes it horribly easy to leave your machine open for information to be discovered."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/columnists/2000/1127gearhead.html>

SIGNED CODE: SECURITY OR CENSORSHIP?

Depending on Microsoft's approach, code signing could not only secure the desktop, but the software giant's control over it as well.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.excite.com/news/zd/001127/11/signed-code-security>

SOLARIS BSM AUDITING

When considering the security of a system we need to be concerned not only with which features and tools we use to implement the access restrictions, but also with what logging of access we do. Logging is important for two main reasons: regular analysis of our logs gives us an early warning of suspicious activity and, if stored securely it can provide the evidence required to find out what went wrong when a breach in the security policy occurs. In this article, Darren Moffat, of the Solaris Security Technologies Group at Sun Microsystems, gives us an overview of the Basic Security Module implementation and management aspects, and provides us insight helpful in raising security to another level in "Solaris BSM Auditing."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/sun/articles/bsmaudit1.html>

FORGET PASSWORDS, WHAT ABOUT PICTURES?

We're drowning in passwords, and our brains are rebelling. Most of us have one of two strategies for remembering all these new strings of letters and numbers: use the exact same password across the board, or keep written reminders of the various secret phrases. Either way, the entire purpose of passwords - security - is undermined.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2657540,00.html>

FREEBSD WEB SITE GOT DEFACED

It looks like FreeBSD web site (www.freebsd.org) got defaced. If you surf to the page, you won't see anything strange, but look down and you will see "FreeBSD got a new Security Officer. Nohican and {} would like to wish the new Security Officer (Kris) good luck on his new job. We are sure you will do a great job!". Frank Van Vliet aka {} is well known for his "white hat" hacks of Slashdot and Apache.org

Link: <http://www.net-security.org/misc/sites/www.freebsd.org/>

MICROPROSE WEB SITE DEFACED

Games developer Microprose, famous for such simulation titles as GrandPrix 3, has had its Web site defaced by group known as "Delinquent Hacking Organisation".

Link: <http://www.theregister.co.uk/content/6/15008.html>

'EVIL' UNISYS EMPLOYEES

A former Unisys accounts clerk that went over to the dark side is being sued for deceit and breaches of fiduciary duty for allegedly rerouting more than 828,273 British pounds into an unauthorized bank account.

Link: <http://www.securitywatch.com/scripts/news/list.asp?AID=4856>

CREEPY CRAWLERS

VBS/Jean-A is a Visual Basic Script worm that will send copies of itself to each of the first 50 entries in the Microsoft Outlook addressbook. It targets German Internet users, as the whole message is written in German. Currently Sophos has received just one report of this worm in the wild.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sophos.com/virusinfo/analyses/vbsjeana.html>

PRIVACY, SECURITY TOP CONCERNS FOR ONLINE SHOPPERS

Nearly half of regular Internet users cite privacy and security as their biggest concerns when shopping online, according to a recent survey. Because of those concerns, 31 percent of survey participants said they would not shop on the Web this holiday season, and 38 percent said they will limit the amount they spend online. The survey "proves many consumers will not make purchases on the Web because they are afraid that their personal privacy will be violated or their credit card and identity will be stolen," said Al Decker, Fiderus CEO, in a prepared statement.

Link: <http://www.crn.com/Sections/BreakingNews/dailyarchives.asp?ArticleID=21928>

CYBER-TERRORISM

A focus is beginning to emerge about the topic of cyber-terrorism. For some time, everything bad, or perceived as bad, on the Internet fell into the black hole known as cyber-terrorism. Events as varied as hacking, political protests, actions by international terrorists, wartime attacks on computers, denial of service attacks, and trashing Websites came under cyber-terrorism.

Fortunately, a more mature perspective continues to emerge.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/cyberterrorism20001128.html>

SMART CARDS POISED TO CHANGE THE FACE OF PAYMENT

The ability to manufacture forged smart chip processors will likely be beyond the means of all but the most organized criminal operations. Because of this, Visa International believes that a move to smart card technology could reduce payment card fraud by as much as 90 percent. That's because defrauding a smart card system isn't a matter of copying down numbers and expiration dates, or forging government notes. Those types of crimes involve fooling a person. But smart card purchases don't go through until the card itself says they're OK.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sfgate.com/technology/expound/>

MTX VIRUS WON'T LET YOU GET HELP

A computer virus that's smart enough to block its victims from getting help is steadily spreading around the Internet. The bug, called MTX, was discovered in August and initially labeled a low risk. But in recent weeks, infections have

been growing and last week it was the most prevalent virus in the world, according to one antivirus firm. The bug has one very sinister feature: once it infects a user, it's programmed to stop the victim from visiting antivirus Web sites and sending "mayday" emails to antivirus companies.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/47/ns-19366.html>

ISC DHCPD

It's interesting to see the number of articles written on ISC's DNS server BIND, compared with the total lack of coverage of one of their other products that is just as important - DHCP. DHCP stands for Dynamic Host Control Protocol and does exactly what it claims. There is practically no information available online regarding DHCP security. This is odd, considering the ubiquity of DHCP servers on most networks. Unlike BIND, the ISC DHCP server does not have command line options to chroot the server or run it as a non-root user. This means that most DHCP servers are running non-chrooted and as root, increasing the chances that any security flaws found will be quite serious.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20001129.html>

SDMI AWARDS HACKERS IN CONTEST

A music and technology forum that ran a \$10,000 contest back in September challenging people to hack into copyright protection technologies said it was paying prize money to two hackers. The Secure Digital Music Initiative (SDMI) said it was contacting two successful challengers, who will receive \$5,000 each, for participation in the HackSDMI public invitation. The two challengers emerged from a field of 447 submissions as the only ones able to remove the protection systems and successfully disable one of five technologies currently under consideration for SDMI screening technology, the group said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/47/ns-19363.html>

YAHOO!: ENCRYPTION FOR THE MASSES

Yahoo! is the first Web portal to introduce an email encryption service. The company is clear that the service is not end-to-end, but offers a "certain level of security" to the person receiving the email. While some people question the value of mass market encryption products, Topsoft, a UK encryption specialist, positively encourages it. "Encryption suffers from something of an image problem," says Topsoft's non-executive director, Tom Parker. "We need to get it into use in the general population. People are beginning to see the value of the security it offers, but are intimidated by the techie image it has."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/15100.html>

ADVANCED BIOMETRICS GIVES SECURITY A HAND

Advanced Biometrics is developing biometric track ball and mouse technology to be used in identification and authentication. The track ball or mouse, provisionally named Live Grip, maps the substructure of the human hand by measuring veins, deep creases, scars and fatty tissue density through infrared light. With alpha testing scheduled for the first quarter of next year and with e-commerce beta testers signed on, the company is targeting the technology for business-to-business Web sites, credit card issuers and financial institutions.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2658995,00.html>

SECURITY REVIEW: VELOCIRAPTOR FIREWALL KICKS!

Similar to the Nokia IP650 firewall appliance, VelociRaptor runs on an Intel compatible AMD-K6 platform. Its Remote Management Console (RMC) for Windows NT and Windows 2000 makes it ideal for organizations that need to manage firewall services remotely at customer sites or field offices. All communication between the RMC console and the VelociRaptor is encrypted for secure management over a public network. Included with all VelociRaptor units is a proxy-secured gateway-to-gateway Virtual Private Network (VPN) tunneling capabilities. The VPN capabilities are based on the standard IPSec protocol.

Link: http://alllinuxdevices.com/news_story.php3?ltsn=2000-11-29-006-03-SC-SA

INTRODUCTION TO INCIDENT HANDLING

Incident handling is a generalized term that refers to the response by a person or organization to an computer security incident or attack. An organized and careful reaction to an incident could mean the difference between complete recovery and total disaster. This paper by Chad Cook provides a logical, sequential approach to managing two of the most common forms of attack - viruses and system compromise. The method this article describes is a useful step-by-step approach for safe recovery and response without the need for highly technical knowledge.

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

PHP.PIRUS

This virus is written in PHP and is contained in a file that is 718 bytes long. When executed, the virus searches the current directory for files with .php or .htm extensions. If one of these files is writable, the virus opens the file to determine if the file is already infected. If the file is not infected, the virus inserts a line to execute the original viral file rather than appending itself to the infected file.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sarc.com/avcenter/venc/data/php.pirus.html>

SECURITY COMPANY'S WEB SITE ATTACKED

Computer security firm Network Associates was left embarrassed after two of its corporate Web site were defaced Wednesday although it claims it is not its fault. A group calling itself Insanity Zine defaced the Brazilian homepages of two Network Associates sites: www.nai.com.br and www.mcafee.com.br. The defacement represents as a major embarrassment for a company that produces software designed to protect computer systems from security threats.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/47/ns-19398.html>

SECURITY-SERVICES MARKET

Demand for information-security services will skyrocket in the next three years, according to market-research and advisory firm IDC. The U.S. market for security consulting, implementation, management and training services will leap to \$8.2 billion in 2004 from \$2.8 billion this year, IDC says. The worldwide market will

increase at a compound annual growth rate of 26 percent, to \$17.2 billion in 2004 from \$5.5 billion in 1999.

Link: <http://www.crn.com/Sections/BreakingNews/dailyarchives.asp?ArticleID=22034>

FINGERPRINTS AND SMARTCARDS

Fighting off hooligans and providing disco dollars to regulars, a new "cyber bouncer" is making waves in European nightclubs. It cuts through the fake IDs, credit cards and drivers licenses to allow club owners to easily assess who causes trouble and who doesn't. The new system, developed by a U.S. company, has been implemented with a piece of technology the size of a credit card. These "smart cards" have a computer strip that stores a swathe of information. It can record biometric data including a person's fingerprints.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://abcnews.go.com/sections/world/DailyNews/britain_cyberbouncers001130.html

BENCHMARKING SOLARIS

A new collaborative security organization is preparing to release the first in a wave of security benchmarks for commercial products widely used in government, industry and academia.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.fcw.com/fcw/articles/2000/1127/web-cis-11-29-00.asp>

JUDICIARY WEIGHS PRIVACY, ACCESS

The federal judiciary is asking for the public's help in hashing out the privacy issues attendant with allowing web access to court case files, which can sometimes include such sensitive information as medical histories, personnel files, tax returns and social security numbers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/120>

WEBCASTERS, MEDIA GROUPS SPAR OVER COPYRIGHT PROPOSAL

Digital media companies and leaders in the entertainment industry faced off in a hearing that could lead Congress to propose changes to online intellectual-property laws. The first, and most contentious proposal would have amended Section 109 of the act to make the "first sale" privilege - the provision that permits the resale of used books, for example - apply expressly to digital transmissions of copyrighted works.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/12/01/news1.html>

Security issues

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

IIS 5.0 WITH PATCH Q277873 IS BAD FOR YOU

Microsoft issued: "Microsoft Security Bulletin (MS00-086). Patch Available for "Web Server File Request Parsing" Vulnerability. Originally posted: November 06, 2000. Updated: November 21, 2000" which installs patch Q277873.

Unfortunately patch Q277873 opens another vulnerability which allows executing arbitrary programs on the web server.

Link: <http://www.net-security.org/text/bugs/975377848,40922,.shtml>

SECURITY PROBLEMS WITH TWIG WEBMAIL SYSTEM

Twig is designed to allow the use of virtual hosting, unfortunately the script that checks this fails to check for user supplied input, thus allowing anyone to submit malicious values as the configuration directory.

Link: <http://www.net-security.org/text/bugs/975377903,16734,.shtml>

IBM NET.DATA LOCAL PATH DISCLOSURE

IBM's Net.Data package (often used in conjunction with NetCommerce3 and db2www) will disclose the local path of server files if fed improper requests.

This software is in use on a variety of sites, including several online-shopping locales.

Link: <http://www.net-security.org/text/bugs/975462531,47164,.shtml>

SUSE LINUX 6.X 7.0 IDENT BUFFER OVERFLOW

This advisory details a buffer overflow vulnerability under SuSE Linux that can enable a malicious user to cause Identification Protocol (Ident) handling to crash. Due to the overflow, the system will no longer be able to establish certain connections which use Ident, for example IRC (Internet Relay Chat) connections. If the Ident daemon is not running, users wishing to connect to IRC will not be allowed to make a connection. In the this case the vulnerability could be used in a denial of service attack to keep a person of irc. It's not clear at this present time whether this vulnerability could be exploited in such a way that arbitrary code is executed. If so, this will happen with the privileges of the user "nobody" in a default installation.

Link: <http://www.net-security.org/text/bugs/975462563,49538,.shtml>

24LINK WEBSERVER VULNERABILITY

A vulnerability was found in 24Link 1.06 Web Server for Windows 95/98/2000/NT machines. The vulnerability allows you to view any password protected files on the Web Server, provided that the Authorization - Check User Name and Password- On all Requests option wasn't chosen, which asks for user name/password for every request sent to the server.

Link: <http://www.net-security.org/text/bugs/975462579,88789,.shtml>

REMOTE FILE ATTACHMENT THEFT

WebMail (possibly WhoWhere.com software) as installed on comm.lycos.com, angelfire.com, eudoramail.com and others allows an attacker to hijack other people's attachments by modifying the hidden form fields on the compose message form.

Link: <http://www.net-security.org/text/bugs/975547058,21897,.shtml>

MANDRAKE LINUX - BASH1 UPDATE

The bash1 shell program has the same << vulnerability that tcsh has and incorrectly creates temporary files without the O_EXCL flag. This vulnerability does not exist in bash2 which uses the O_EXCL flag when creating temporary files.
Link: <http://www.net-security.org/text/bugs/975547095,61321,.shtml>

CISCO 675 DENIAL OF SERVICE ATTACK

The Cisco 675 DSL routers with the Web Administration Interface enabled can be crashed (hard) using a simple GET request. CBOS versions 2.0.x through 2.2.x have been found to be vulnerable. The new CBOS 2.3.x has not been tested, but there are no notes in the 2.3.x changelogs to indicate that they've fixed this problem. Effectuated 675s were configured in PPP mode. The 'Web Administration Interface' is enabled by default in CBOS revisions 2.0.x and 2.2.x.
Link: <http://www.net-security.org/text/bugs/975547115,60889,.shtml>

DOS IN SONICWALL SOHO FIREWALL

I was just playing a bit with a Sonicwall SOHO firewall, to verify performances and security of the product. I've noticed that using a very long string (some hundreds of chars) as the User Name in the auth page of the Sonicwall web server, the firewall reacts strangely: it begins to refuse connections to the 80/tcp port and it stops routing packets from the internal LAN. After about 30 seconds it apparently returns normal.
Link: <http://www.net-security.org/text/bugs/975547130,93049,.shtml>

SUSE SECURITY ANNOUNCEMENT: NETSCAPE

Michal Zalewski <lcamtuf@DIONE.IDS.PL> has found a buffer overflow in the html parser code of the Netscape Navigator in all versions before and including 4.75. html code of the form

```
< form action=foo method=bar>  
< input type=password value=long string here>  
more form tags  
< /form>
```

can crash the browser. It may be possible for an attacker to supply a webpage that executes arbitrary code as the user running netscape. As of today, no exploit code is known to exist in the wild.

Link: <http://www.net-security.org/text/bugs/975637488,44617,.shtml>

DEBIAN LINUX - FSH SYMLINK ATTACK

Colin Phipps found an interesting symlink attack problem in fsh (a tool to quickly run remote commands over rsh/ssh/lsh). When fshd starts it creates a directory in /tmp to hold its sockets. It tries to do that securely by checking if it can chown that directory if it already exists to check if it is owner by the user invoking it. However an attacker can circumvent this check by inserting a symlink to a file that is owner by the user who runs fhsd and replacing that with a directory just before fshd creates the socket.

Link:

WINDOWS 2000 TELNET SERVICE DOS

The Telnet Service in question is vulnerable to a simple Denial of Service attack. The problem apparently lies within the login routine of the daemon. The problem can be demonstrated by telnetting to a machine running the specified version of the Telnet Service and waiting at the login/password prompt until a session

timeout takes place. However, after it does time out the connection is not reset by the daemon until the user presses a key. In Windows 2000 Professional, due to the fact, it allows only one telnet connection per host, this will effectively disable access for the authorized user.

Link: <http://www.net-security.org/text/bugs/975637518,37939,.shtml>

Security world

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

SECURE COMPUTING PARTNER WITH EDS - [28.11.2000]

Secure Computing, announced the formation of an alliance agreement with EDS, the leading pure-play global services company that offers corporations and government clients a scalable safe, secure extranet for their growing e-business strategies.

Press release:

< <http://www.net-security.org/text/press/975376733,13922,.shtml> >

PRIVILEGE - FINALIST FOR SIIA 2001 CODIE AWARD - [28.11.2000]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, today announced the Software & Information Industry Association named Aladdin's Privilege software licensing and distribution solution a finalist for SIIA's coveted 2001 Codie Award in the Best Application Service Solution category.

Press release:

< <http://www.net-security.org/text/press/975376826,41652,.shtml> >

US AF AWARDS TINY SOFTWARE WITH CONTRACT - [28.11.2000]

Tiny Software Inc., a leader in router and firewall software solutions for small to medium size networks, today announced that it has been awarded a contract by the Air Force Information Warfare Center to develop a centrally managed desktop security (CMDS) system. When complete, the CMDS will provide the Air Force the capability to manage its network security enterprise environment in a truly hierarchical method. The CMDS will manage the network security environment through policy enforcement. The system is designed to report suspicious events through the network-established hierarchy and will log network connections to the desktop.

Press release:

< <http://www.net-security.org/text/press/975376889,25418,.shtml> >

TINY PERSONAL FIREWALL V.2 FREE FOR DOWNLOAD - [28.11.2000]

Tiny Software Inc., a leader in router and firewall software solutions for small to medium size networks, today released version two of its popular Tiny Personal Firewall. Free for personal use, Tiny Personal Firewall v.2 is an easy-to-use software firewall that prevents unauthorized access, offers high security for computers and is based on the award winning, ICSA-certified WinRoute Pro security technology.

Press release:

< <http://www.net-security.org/text/press/975376937,92063,.shtml> >

FORMER CTO OF XEROX.COM JOINS VYNAMIC - [29.11.2000]

Vynamic™, the Portsmouth, NH based e-Learning security firm, announced the appointment of Fred Damiano as Chief Technology Officer. Mr. Damiano joins Vynamic from his former position as CTO for Xerox Corporation's Internet Business Group/ www.xerox.com. Mr. Damiano will be responsible for leading all aspects of Vynamic's technology development, including the launch of the company's technology center - a 25-person engineering team that will be located in Rochester, NY.

Press release:

< <http://www.net-security.org/text/press/975463471,52026,.shtml> >

SOPHOS GETS CERTIFICATION FOR 100% DETECTION - [29.11.2000]

Sophos Anti-Virus, the world's leading developer of corporate anti-virus protection, announced today that the three versions of its product recently submitted for Checkmark certification have passed the test effortlessly. Sophos Anti-Virus for Windows 95/98, Windows NT and NetWare have all attained Anti-Virus Checkmark level 1, providing further proof that the products are capable of detecting all known 'in-the-wild' viruses.

Press release:

< <http://www.net-security.org/text/press/975463562,39020,.shtml> >

MCP MAG'S 'COMPREHENSIVE FIREWALL PROTECTION' - [01.12.2000]

Network-1 Security Solutions, Inc., a leader in distributed intrusion prevention solutions for e-Business networks, announced that it was favorably reviewed and recommended by Microsoft Certified Professional Magazine, considered by many to be the most prestigious of the Microsoft-dedicated publications.

Press release:

< <http://www.net-security.org/text/press/975638135,29699,.shtml> >

TOP TEN VIRUSES IN NOVEMBER 2000 - [01.12.2000]

This is the latest in a series of monthly charts counting down the ten most frequently occurring viruses as compiled by Sophos, the world leaders in corporate anti-virus protection.

Press release:

< <http://www.net-security.org/text/press/975638244,77952,.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.

HYPE AND THE SECURITY SCENE: TAKING THE "REP" by Thejian

Ever since there has been a "hackerscene" there has been a constant struggle between its "inhabitants" and mainstream media over words. That's all it is you know, "what's in a name" to put it really (really :) trite. Wether it was hacker, cracker or script kiddie, wether it was Kevin Mitnick or Mafiaboy (or neither) who represents the word "hacker", there was and will always be disagreements and misconceptions in and about this scene when it comes to words.

Read more:

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

THE ATTRITION.ORG STAFF ON CYBERWAR AND THE MEDIA

"CyberWar Rages in the Middle East!!! YOUR Servers could be next!!!" - is is the kind of crap coming out of so-called security companies and news media lately. The real irony is that they are using data from the Attrition web defacement mirror to support their hyped conclusions. Let's take a little reality break, folks - the sky isn't falling.

Read more:

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

RHCE: RED HAT CERTIFIED ENGINEER STUDY GUIDE

Passing the RHCE Certification Exam (RH302) isn't easy, students must master intense lab-based components. The hands-on exam requires success in installing and configuring Red Hat, setting up common network (IP) services, and performing essential administration, diagnostic tests and troubleshooting, among other internetworking and systems administration tasks. The RHCE Study Guide is THE answer for anyone who wants to take and pass the RHCE Certification Exam (RH302) in order to become certified in setting up and administering a Red Hat Linux server for critical network services and security. Coverage includes important background information, hands-on exercises for lab-based topics, real-world troubleshooting exercises for a variety of scenarios, challenging review questions for each exercise, strategies, tips and tricks for passing the exam.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0782127932/netsecurity> >

WINDOWS NT/2000 NETWORK SECURITY

This book is intended primarily for LAN administrators, system programmers, information security staff, and advanced users. Although the main focus of the book will be technical, many facets of Windows NT security involve practicing sound control procedures. As such, much of the book's discussion will be pertinent to all three groups. Topics covered: How to keep Microsoft Windows NT 4.0 and Windows 2000 secure in networked environments. Specific areas of coverage include a primer on the various modes of attack, security-minded everyday system administration, security of specific services, protection against viruses, and maintenance of security in a virtual private network.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1578702534/netsecurity> >

SAIR LINUX AND GNU CERTIFICATION LEVEL 1, SYSTEM ADMINISTRATION

Topics covered: The concepts, facts, and procedures you need to understand to pass the installation and configuration exam (3X0-103) en route to Sair Linux & GNU Certified Professional (LCP) certification. Most coverage goes to the Linux 2.2.x kernel itself, but the author walks you through installation and configuration of Red Hat Linux 6, SuSE Linux 6.1, Caldera OpenLinux 2.2, and Slackware 4. He

also highlights some differences that show up in a few other distributions. Other coverage goes to hardware compatibility, preinstallation planning, the bash shell and its important commands, and top utilities.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0471369764/netsecurity> >

SSL AND TLS: DESIGNING AND BUILDING SECURE SYSTEMS

>From the Back Cover "This is the best book on SSL/TLS. Rescorla knows SSL/TLS as well as anyone and presents it both clearly and completely.... At times, I felt like he's been looking over my shoulder when I designed SSL v3. If network security matters to you, buy this book." Paul Kocher, Cryptography Research, Inc. Co-Designer of SSL v3 "Having the right crypto is necessary but not sufficient to having secure communications."

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0201615983/netsecurity> >

PROFESSIONAL WINDOWS DNA: BUILDING DISTRIBUTED WEB APPLICATIONS WITH VB, COM+, MSMQ, SOAP, AND ASP

This book is for anyone involved with building distributed web applications that want to see the bigger picture. As such the book assumes a working knowledge of VB and ASP in places, but the emphasis is not so much on the code as on where each of the pieces fit into the puzzle. It's designed to give you an idea of how each area or technology affects you, enabling you to make informed decisions about whether to pursue a subject further, or confidently assert that you can do without it. This book takes an in-depth look at the DNA architecture, focusing on fitting the pieces of the puzzle together. Each of the logical tiers is examined, with particular emphasis placed on the features COM+ contains to make component building simpler and more powerful.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1861004451/netsecurity> >

Security Software

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

EMAILPATROL 1.0

EmailPatrol is an online email previewer. EmailPatrol will download the headers and a user defined number of lines for a fast preview of the mailbox contents.

This feature is specially designed to avoid potential security risks regarding the spread of macro viruses by email attachments. EmailPatrol has a browser-like interface, and provides basic information about all the messages in the user's mailbox. The user can then choose to delete the message, drag and drop the whole message contents into the desktop or forward the message to another address.

Info/Download:

< <http://net-security.org/various/software/975087472,3606,.shtml> >

PASSWORD STORE 1.81 (PALMOS 2.0)

Password Store is a program that stores a list of all of your passwords. It makes it easy to keep track of passwords and PINs for credit cards, email accounts, phone cards, and more. Password Store can also be protected with its own password to keep your information safe.

Info/Download:

< <http://net-security.org/various/software/975087617,111,.shtml> >

FLOWPROTECTOR GLOBAL INTERNET SECURITY

FlowProtector Global Internet Security provides computer protection for Internet users. It includes a secure Web browser that neutralizes spy software, cleans up cookies and cache, adds a proxy for parental control, and includes a micro firewall that detects online activity.

Info/Download:

< <http://net-security.org/various/software/975087760,99482,.shtml> >

Defaced archives

[26.11.2000] - Borland (mail server)

Original: <http://mail.borland.pl/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/26/mail.borland.pl/>

[26.11.2000] - Israel Lands Authority

Original: <http://mmichavah.mmi.gov.il/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/26/mmichavah.mmi.gov.il/>

[26.11.2000] - Wuqing China Gov

Original: <http://www.tjwq.gov.cn/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/26/www.tjwq.gov.cn/>

[26.11.2000] - AT&T Global Network Services Italia

Original: <http://www.att.it/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/26/www.att.it/>

[26.11.2000] - State of California
Original: <http://svhqwebstat1.dot.ca.gov/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/26/svhqwebstat1.dot.ca.gov/>

[27.11.2000] - National Institutes of Health
Original: <http://nlmplan.nlm.nih.gov/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/27/nlmplan.nlm.nih.gov/>

[27.11.2000] - Banco Central do Brasil
Original: <http://www.bcb.gov.br/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/27/www.bcb.gov.br/>

[27.11.2000] - Taipei Hospital, Department of Health
Original: <http://www.ptph.gov.tw/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/27/www.ptph.gov.tw/>

[28.11.2000] - Ministry of Endowments and Islamic Affairs
Original: <http://www.islamweb.net/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/28/www.islamweb.net/>

[28.11.2000] - Posta Crne Gore d.o.o. Podgorica
Original: <http://www.posta.cg.yu/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/28/www.posta.cg.yu/>

[28.11.2000] - Department of Materials Science and Engineering, U of Arizona
Original: <http://oxygen.mse.arizona.edu/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/28/oxygen.mse.arizona.edu/>

[29.11.2000] - Samsung [South Africa]
Original: <http://www.samsung.co.za/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/29/www.samsung.co.za/>

[29.11.2000] - Sony Schweiz SA
Original: <http://www.sony.ch/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/29/www.sony.ch/>

[29.11.2000] - McAfee - Network Associates do Brasil
Original: <http://www.mcafee.com.br/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/29/www.mcafee.com.br/>

[29.11.2000] - Network Associates do Brasil
Original: <http://www.nai.com.br/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/29/www.nai.com.br/>

[29.11.2000] - Istra Informaticki Inzenjering
Original: <http://www.iii.hr/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/29/www.iii.hr/>

[29.11.2000] - SRH - Secretaria dos Recursos Hídricos do Estado do Ceará
Original: <http://www.ra.gov.ee/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/29/www.ra.gov.ee/>

[29.11.2000] - Ministerio de la Presidencia de la república de Venezuela
Original: <http://www.venezuela.gov.ve/>
Defaced: <http://www.attrition.org/mirror/attrition/2000/11/29/www.venezuela.gov.ve/>

[29.11.2000] - Federal Aviation Administration - ABA Home Page

Original: <http://abaweb.faa.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/29/abaweb.faa.gov/>

[30.11.2000] - Dell Computadores

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/30/www.dell.com.br/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>