

Net-Sec newsletter
Issue 37 - 06.11.2000
<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

=====
We are glad to announce that, in association with Zero Knowledge Systems, you can win several copies of their cutting-edge Internet Privacy software - Freedom. For your chance to win, please submit your opinion on the following topic:

What are the current Internet privacy threats?

Opinion submit form is located on:
<http://www.net-security.org/your-opinion/zks/>

=====
General security news

IT SECURITY SPENDING MISSING MARK

Despite an expected 300 percent spending increase on information technology security over the next four years, bad decision-making will leave U.S. companies almost as vulnerable to security breaches as they are today, according to a new report issued by Forrester Research.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ecommercetimes.com/news/articles2000/001030-3.shtml>

CANADA'S HOLES A THREAT TO U.S.?

"James Adams, who has worked with the NSA and the CIA, told the National Post Canada's vulnerability is a concern to security circles in Washington. That's because so many major U.S. corporations have offices in Canada". Hmm who

would tell them that system administrators and their security expertise is crucial for the state of computer security in those "U.S. corporations", and not to generalize the security situation to the whole Canada...

Link: <http://www.nationalpost.com/home/story.html?f=/stories/20001030/445647.html>

DOWNPLAYING THE SITUATION

On Friday, Microsoft said the attackers had roamed its systems for five weeks. Now, Microsoft insists that they had high-level access for just 12 days, were monitored during this time, and that no damage was done.

Link: http://news.bbc.co.uk/hi/english/business/newsid_998000/998449.stm

'INFECTING' THE BACKBONE

"The president of Israel's leading Internet-service provider, Gilad Rabinovich, tells Newsweek that hackers have tried 'to infect the Internet backbone' of the country". Strange but as article speaks about Denial of Service attacks and mass spamming, where should we put the verb infecting?

Link: <http://www.hoovershbn.hoovers.com/bin/story?StoryId=CoFU84bWbsfntvtaWnMe>

GATEWAY SECURITY "NOT TOTALLY WORKED OUT"

The official charged with ensuring Britain's public bodies can interoperate electronically has shed more light on the confusion surrounding the Government Gateway project. Anwar Choudhury, deputy director in the Office of the e-Envoy at the Cabinet Office, said on 31 October 2000 that the security infrastructure of e-government "has not been totally worked out yet".

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.kablenet.com/kable.nsf/Frontpage/B59CDF190B182238802569890057D826>

MIDDLE EAST CYBER TENSION COULD ESCALATE

Some(?) security experts are warning that the electronic skirmish in the Middle East could escalate and spill over to the United States. Tensions in the Middle East have spread to the online arena, with an increased level of activity against Web sites related to Israel and pro-Palestinian organizations, according to the FBI's National Infrastructure Protection Center (NIPC). However, Yoran's firm services clients in the Middle East, and they have not been threatened.

Link: <http://www.crn.com/Sections/BreakingNews/dailyarchives.asp?ArticleID=21152>

DECREASE YOUR STRESS

Much of a systems administrator's stress comes from unexpected downtime and dissatisfied users. This month in Pete's Super Systems, Pete introduces two free tools that will help reduce the chances of both.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunworld.com/sunworldonline/swol-10-2000/swol-1027-supersys.html>

VNUNET WRITES ABOUT ANTI-ONLINE DEFACEMENT

Vnunet picked up a story about AntiOnline defacement. While writing this item the web site was currently not available, but I read earlier that they published information about the break in. I remember that it started with something like 'between millions of hack attempts, we had a successful break in'.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1113199>

IT TASK FORCE DISCUSSES SECURITY

The Indo-Singapore task force on IT, communication and systems has held its first meeting in New Delhi and discussed various issues related to e-commerce laws, content, online security and ways to establish joint research and development efforts

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://asia.internet.com/2000/11/1101-india.html>

DOES IT MEETS MINIMUM SECURITY STANDARDS?

Benchmarks for measuring security got a boost this week when the Center for Internet Security released a first draft of consensus security actions for Solaris systems.

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

SEACH, SPAM, ETC.

If you often use search engines, next Wired story will look strange, because it talks of some current issues surrounding search inquiries. At least it looked strange to me ;) Slashdot also picked it of course...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,39896,00.html>

UBER ATTACKERS

NewsMax.com has a FUD article saying that targets by 'Russian hackers' are "America's power plants, telecommunications systems, bridges, dams, sewage treatment plants, water stations and other key installations."

Link: <http://www.newsmax.com/showinsidecover.shtml?a=2000/11/1/24737>

HUSHMAIL BACKS UK ANTI-SNOOPING EFFORT

UK Internet civil liberties group Cyber Rights & Cyber Liberties has teamed up with US email encryption company Hush Communications to overcome the RIP Act, which was recently made law. Through a joint project 'Cyber-Rights.Net', the pair will provide a route to bypass snooping regulations in the UK and at the same time draw attention to what they view as international moves to synchronise Internet surveillance.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/43/ns-18819.html>

HITACHI UNVEILS SECURE NOTEBOOK RANGE

Electronics giant Hitachi has launched a range of secure notebook PCs specifically aimed at companies and users looking to safeguard their data and equipment from malicious attacks. The HN7200, 7300 and 8300 notebooks, which go on sale next month, come equipped with remote networking facilities, a configurable firewall and email filtering tools aimed at defending workers based outside the corporate firewall from attempted hacks and malicious code appended to emails.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1113381>

MCAFEE VIRUS DEFINITION CRASHES WINDOWS

Keeping virus scanning software files current is usually a good idea... except for today. Network Associates has confirmed a bug in the latest McAfee VirusScan's virus definition file that could cause many Windows systems to freeze during start up. The problem is an incompatibility between a recent virus remedy file and the scan engine software in VirusScan. For those bitten by this bug, the only solution is to boot Windows in Safe Mode and disable VirusScan's system scanning at start up. Then, when an upgraded version of the scan engine is applied to the system, the user can go back and re-enable startup scans.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/43/ns-18853.html>

NEW SAFE HARBOR DATA PRIVACY WEBSITE LAUNCHES

Commerce Department Under Secretary Robert LaRussa announced the opening of a new website that enables U.S. companies to sign up online to participate in the U.S.-European Union "safe harbor" data privacy framework and thus comply with EU privacy rules.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://cipherwar.com/news/00/safe_harbor_2.htm

CRACKERS ATTACK PRO-ISRAELI SITE

Pakistani-based attackers attacked a U.S. website belonging to a pro-Israel lobby, stealing credit card numbers and member records in the latest volley in what has become an online war. The attack, against the American-Israel Public Affairs Committee, consisted of the attackers defacing its website with pro-Palestinian slogans and e-mails downloaded from the website databases.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,39950,00.html>

NET DAD VINT CERF SLAMS RIP

Vinton Cerf, one of the founding fathers of the Internet, has attacked the RIP bill as a dangerous new piece of legislation. Speaking at the Compsec conference in London yesterday he commented: "Oh my god. A lot of us in the US are very worried about the RIP Bill, it has raised some of the same concerns as Carnivore."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/14451.html>

MICROSOFT'S SLOPPY ADMINS

The Dutch hacker Dimitri, said to IT World that Microsoft failed to install a patch for a known bug, which let him enter one of Microsoft's servers. A Microsoft spokesman confirmed that the hacker reached at least one server, but said that Microsoft security personnel were rechecking their servers for holes to patch. Funny (or tragic) thing is that Microsoft doesn't secure their servers with their own patches...

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www2.itworld.com/cma/ett_article_frame/0,,1_3315,00.html

Security issues

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

IIS 5.0 CROSS SITE SCRIPTING VULNERABILITY

Using specially designed URLs, IIS 5.0 may return user specified content to the browser. This poses great security risk, especially if the browser is JavaScript enabled and the problem is greater in IE. By clicking on links, just visiting hostile web pages or opening HTML email the target IIS sever may return user defined malicious active content. This is a bug in IIS 5.0, but it affects end users and is exploited with a browser. A typical exploit scenario is stealing cookies which may contain sensitive information.

Link: <http://www.net-security.org/text/bugs/972959321,32876,.shtml>

MICROSOFT TO GEORGI GUNINSKI

Microsoft takes reports of all security vulnerabilities seriously. That being said, we'd like to share the events surrounding the receipt and impending resolution of this issue. The Microsoft Security Response Center received a report of this vulnerability on October 24th, as Georgi states below. Within 24 hours of receiving Georgi's notification, we had a draft patch designed to correct this problem. What's more at issue here is the manner in which Georgi has decided to release this security advisory. We informed Georgi that we were working to address the issue and would probably have a patch available in short order (within eight days of the time he reported it to us). We asked that he give us time to finish the patch so we could do a joint release, thus protecting our mutual customers and reporting the issue in a responsible manner.

Link: <http://www.net-security.org/text/bugs/972959339,58883,.shtml>

GEORGI GUNINSKI REPLIES TO MICROSOFT

I did not reply to secure@microsoft.com's emails because they were just informative emails without any questions. Here are some quick checkable facts regarding Microsoft's time to release a patch: Since Microsoft claims "Microsoft takes reports of all security vulnerabilities seriously" I'd like to point out that Microsoft has not fixed several vulnerabilities for very long time. One of them is file reading bug in IE 5.5 and has not been fixed for 3 1/2 months. Has they taken them seriously? The least they could do would be to inform their customers about a workaround.

Link: <http://www.net-security.org/text/bugs/972959359,54942,.shtml>

REMOTE COMMAND EXECUTION VIA KW WHOIS 1.0

There is a vulnerability in Kootenay Web Inc's KW Whois v1.0 which allows malicious users to execute commands as the uid/gid of the webserver. The hole lies in unchecked user input via an input form box. The form element `<input type=text name="whois">` is not checked by the script for unsafe characters.

Link: <http://www.net-security.org/text/bugs/972959380,40592,.shtml>

MINOR BUG IN PAGELOG.CGI

Any file on the system with a '.log' extension readable by the uid/gid of the webserver can be viewed. In addition, two files with extensions of '.txt' and '.log' can be created in any directory on the system that is writable by the web server. This bug lies in the failure of the script to check for directory traversal.

Link: <http://www.net-security.org/text/bugs/972959395,24878,.shtml>

ADDITIONAL THEORY ON PAGEDLOG.CGI SECURITY ISSUE

At this time this is just a theory, since i can't seem to find any sites running pagelog.cgi to test it, or a copy of the code anywhere to take a look at it. But, in theory, if you were to append a %20 to the address you should be able to open any file it is capable of displaying.

Link: <http://www.net-security.org/text/bugs/972959438,13878,.shtml>

SAMBA 2.0.7 SWAT VULNERABILITIES

The program swat included in the samba distribution allows username and password bruteforcing. An attacker can easily generate userlists and then bruteforce their passwords. Comments in the source code show that somebody tried to prevent this from happening.

Link: <http://www.net-security.org/text/bugs/972959456,32735,.shtml>

UNIFY EWAVE SERVLETEXEC DOS

Unify's eWave ServletExec is a JSP and a Java Servlet engine which is to be used as a plug-in to popular web servers like Apache, IIS, Netscape, etc. It is possible to send a URL request which causes the ServletExec servlet engine to terminate abruptly. The web server, however, is not affected.

Link: <http://www.net-security.org/text/bugs/972959470,90979,.shtml>

PEGASUS MAIL FILE READING VULNERABILITY

David Harris, the author of Pegasus Mail, has released a utility called WSendTo that protects against the file reading vulnerability discussed on BugTraq a few weeks ago.

Link: <http://www.net-security.org/text/bugs/973042673,34444,.shtml>

"MALFORMED MIME HEADER" VULNERABILITY PATCHED

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Exchange Server 5.5. The vulnerability could enable a malicious user to cause an Exchange server to fail.

Link: <http://www.net-security.org/text/bugs/973042712,32774,.shtml>

ALLAIRE'S JRUN DoS

A denial of service vulnerability exists within the Allaire JRun 3.0 web application server which allows an attacker to bring down the JRun application server engine.

Link: <http://www.net-security.org/text/bugs/973132487,53954,.shtml>

HOTMAIL CAN ACT AS EMAIL AMPLIFIER

Hotmail can act as email size amplifier with a factor of at least 1000, allowing flooding and mail-bombing a victim while using a negligible amount of your own bandwidth.

Link: <http://www.net-security.org/text/bugs/973132501,46670,.shtml>

UNIFY EWAVE SERVLETEXEC UPLOAD

Unify's eWave ServletExec is a JSP and a Java Servlet engine which is used as a plug-in to popular web servers like Apache, IIS, Netscape, etc. ServletExec has a servlet called "UploadServlet" in its server side classes. UploadServlet, when invocable, allows an attacker to upload any file to any directory on the server. The uploaded file may have code that can later be executed on the server, leading to remote command execution.

Link: <http://www.net-security.org/text/bugs/973132522,4578,.shtml>

NETSCAPE SERVERS HEAP BUFFER OVERFLOW

An exploitable heap buffer overflow vulnerability was discovered in the Netscape Directory Server product. The Netscape Certificate Management System also has several server components that share the problem. Vulnerable systems allow the execution of arbitrary code as the user running the services.

Link: <http://www.net-security.org/text/bugs/973132538,13785,.shtml>

NETSCAPE SERVERS DENIAL OF SERVICE

A bug in several components of the Netscape Servers suite of products allows an attacker to successfully conduct a denial of service attack against the vulnerable systems. The Netscape Certificate Management System has also several server components that share the problem.

Link: <http://www.net-security.org/text/bugs/973132561,625,.shtml>

"NETMON PROTOCOL PARSING" BUG PATCHED

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Windows NT and Windows 2000 server products and Systems Management Server. The vulnerability could allow a malicious user to gain control of an affected server.

Link: <http://www.net-security.org/text/bugs/973135591,74009,.shtml>

"INDEXING SERVICES CROSS SITE SCRIPTING" PATCH

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Indexing Services for Windows 2000. This vulnerability could allow a malicious web site operator to misuse another web site as a means of attacking users.

Link: <http://www.net-security.org/text/bugs/973261837,75960,.shtml>

MULTIPLE NETWORK MONITOR OVERFLOWS

The Windows Network Monitor tool allows an administrator to capture network traffic destined to the local host or all traffic on a local network. Network Monitor is designed to capture network traffic before the information can be viewed in the graphical interface. Individual packets received from the network are parsed to provide a readable representation in the user interface. Each application level protocol is parsed by a separate dynamic linked library within Network Monitor. One of the vulnerable libraries, 'browser.dll', is documented in the samples section of the Visual C++ documentation in the MSDN library. Multiple stack overflows in various function calls within Network Monitor's parsing libraries may allow remote attackers to gain control of the Network Monitor application and execute arbitrary code.

Link: <http://www.net-security.org/text/bugs/973261858,1489,.shtml>

NAI'S DISTRIBUTED SNIFFER AGENT PROBLEMS

NAI's Distributed Sniffer Agent can be overflowed remotely to grant SYSTEM privilege. Additional vulnerabilities exist in the management protocol to allow an attacker to recover logins passwords, take control of the agent, and delete logs.
Link: <http://www.net-security.org/text/bugs/973261889,85022,.shtml>

"ACTIVEX PARAMETER VALIDATION" PATCH

An ActiveX control that ships as part of Windows 2000 contains an unchecked buffer. If the control was called from a web page or HTML mail using a specially malformed parameter, it would be possible to cause code to execute on the machine via a buffer overrun. This could potentially enable a malicious user to take any desire action on the user's machine, limited only by the permissions of the user. Microsoft has released a patch that eliminates this vulnerability.
Link: <http://www.net-security.org/text/bugs/973261905,68040,.shtml>

BUFFER OVERFLOW IN NETWORK MONITOR

Internet Security Systems (ISS) X-Force has discovered a buffer overflow vulnerability in Microsoft's Network Monitor utility. The vulnerability allows code to be executed on the remote computer with the privilege levels of the current user. Administrative privileges are required to run Network Monitor.
Link: <http://www.net-security.org/text/bugs/973261921,19800,.shtml>

Security world

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

ZKS INTRODUCES MANAGED PRIVACY SERVICES - [31.10.2000]

Zero-Knowledge Systems, the leading developer of privacy solutions, introduced its new Managed Privacy Services offering to solve the privacy challenges of businesses and enable enterprise to thrive in a privacy-conscious climate. Delivering a unique combination of technology, policy and strategy expertise, Zero-Knowledge Managed Privacy Services (MPS) enables clients to turn privacy into a competitive advantage by leveraging rich data resources while building stronger and more profitable relationships with customers, employees and partners. MPS is based on responsible and ethical information management in accordance with relevant legislation and industry standards.

Press release:

< <http://www.net-security.org/text/press/973006780,81960,.shtml> >

INFOEXPRESS STRENGTHENS PRESENCE IN CANADA - [31.10.2000]

Responding to exponential growth in demand for effective remote access security for enterprises, InfoExpress announced the opening of a new office in Ottawa, Canada, the fast growing high-tech capital city. The new office will focus on marketing InfoExpress' award-winning CyberArmor Enterprise Personal Firewall Suite(TM) and FireWalker VPN Suite(TM) to companies in Ottawa, Toronto, Montreal, and the northeastern United States. In addition to sales activity, engineering support will also be available from the Ottawa office.

Press release:

< <http://www.net-security.org/text/press/973006842,37204,.shtml> >

ERAP VIRUS SUSPECT ARRESTED IN PHILIPPINES - [31.10.2000]

Reports from the Philippines indicate that a 19 year old male youth has been questioned by the authorities about the so-called "Erap Estrada" worm. The youth, who has not been named, was arrested on October 22 by agents of the National Bureau of Investigation (NBI) at his house in Laguna. Floppy disks and other computer equipment were seized by the Anti-Fraud and Computer Crimes division of the NBI. The man was later released pending further investigation.

Press release:

< <http://www.net-security.org/text/press/973009201,9686,.shtml> >

TOP TEN VIRUSES REPORTED TO SOPHOS IN OCTOBER - [01.11.2000]

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/973009653,81553,.shtml> >

VENTUREWORX ANNOUNCES STAKE IN SECURITY FIRM - [01.11.2000]

VentureWorx announced an equity stake in Vynamic™ an Internet infrastructure company providing security solutions expressly designed to support the needs of the e-Learning marketplace. Vynamic utilizes a proprietary, secure student ID technology, which insures that students are authenticated and all online learning transactions are encrypted and protected. In addition, Vynamic's secure student ID enables both corporate training and academic e-Learning platforms the ability to protect their intellectual property by "locking in" their course content.

Press release:

< <http://www.net-security.org/text/press/973041155,37624,.shtml> >

ALADDIN AND DST PARTNER - [01.11.2000]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, and Digital Signature Trust, an affiliate of Zions Bancorporation and an issuer of trusted digital identity certificates, announced a partnership that combines Aladdin's eToken and DST's TrustID certificates to provide highly secure digital certificate storage and authentication.

Press release:

< <http://www.net-security.org/text/press/973041378,67098,.shtml> >

NEW ENCRYPTION TECHNOLOGY PREMIERED - [01.11.2000]

CNET's Download.com launched the world's first encrypted Instant Messaging utility. The Encrypted Messenger program is unique in that it protects user's online chat and instant messaging by encrypting the text in real-time. The program will help quell the fear of consumers who are wary of potential online privacy invasions both from hackers and from accidental eavesdropping by programs such as Carnivore and Echelon.

Press release:

< <http://www.net-security.org/text/press/973086289,42744,.shtml> >

SC MAGAZINE AWARDS LATEST CYBERWALLPLUS - [01.11.2000]

Security Solutions, Inc., a leader in distributed intrusion prevention solutions for e-Business networks, announced that SC Magazine has performed a technical product review of its CyberwallPLUS family of firewall products and awarded them its highest overall rating of 5 stars. The review is published in the October issue of SC Magazine.

Press release:

< <http://www.net-security.org/text/press/973087847,13789,.shtml> >

SECUREPRINT BIOMETRIC SOLUTION UNVEILED - [02.11.2000]

Intermate and LCI SMARTpen Inc. introduce SECUREprint, an elegant solution that enables the secure printing of confidential or sensitive data to any standard laser printer through biometric authentication. The concept consists of two parts, the LCI SMARTpen, a biometric authentication system based on the users unique signature, and LCI Intermate's SECUREprint card for standard laser printers.

Press release:

< <http://www.net-security.org/text/press/973135001,25125,.shtml> >

INTEL SELECTS SAFENET'S ENCRYPTION BOARD - [02.11.2000]

SafeNet, Inc., formerly IRE, the foundation of Internet security and de facto leader of VPN technology, announced that Intel has licensed its SafeNet PCI

board to accelerate encryption functionality of the Intel NetStructure 3130 VPN Gateway. The integration of SafeNet PCI into Intel's NetStructure product offers the highest performing VPN gateway available for fast and secure Internet communications for mobile users, between offices and partners, and over corporate networks.

Press release:

< <http://www.net-security.org/text/press/973135554,92946,.shtml> >

CONTROL RISKS GROUP RELEASES RISKMAP 2001 - [03.11.2000]

The business risk consultancy, Control Risks Group, launches its annual survey, RiskMap 2001 detailing the political, security and reputational risks that will define the international environment in the year ahead.

Press release:

< <http://www.net-security.org/text/press/973262892,95889,.shtml> >

BINDVIEW'S FREE TROJAN SCOUT FINDS QAZ TROJAN - [03.11.2000]

Following recent hacks exposing Microsoft product code, BindView Corporation, a leading provider of IT administration and security management solutions, announced Trojan Scout, software that not only identifies the security vulnerability created by the QAZ Trojan, but also offers instruction for closing the "backdoor" created as a result of the intrusion.

Press release:

< <http://www.net-security.org/text/press/973264008,56796,.shtml> >

ANOTHER TREND MICRO PARTNERSHIP DEAL - [03.11.2000]

Trend Micro Inc. has joined forces with Taiwan Telecommunications Network Services Co., Ltd., Taiwan's largest value-added network service provider and third-largest ISP, to protect TTN customers from the threat of Internet-borne viruses. Through this strategic alliance, TTN will offer its dial-up, broadband and lease-line Internet subscribers an optional virus scanning and cleaning service for their email messages and user mailboxes, using Trend Micro's award-winning antivirus technology

Press release:

< <http://www.net-security.org/text/press/973264084,15124,.shtml> >

BRILAW INTERNATIONAL WINS GOLD AGAIN - [04.11.2000]

Stockport based Brilaw International has been re-accredited as a " Gold CSN Partner". This is an accreditation that relates to the reselling and adding value to Citrix. Citrix is the ultimate solution for organisations wishing to speed up applications, reduce their IT overhead and improve security. Brilaw International has renewed its commitment to the Citrix brand by complying with the new

demands Citrix has placed on its premier resellers.

Press release:

< <http://www.net-security.org/text/press/973337772,2484,.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.

SONIC: SELF-UPDATING INTERNET WORM DISCOVERED "IN THE WILD"

Kaspersky Lab, an international anti-virus software development company, is warning users of the discovery of a new internet-worm, Sonic. This worm was discovered in France and Germany on the morning of 30th October 2000. The distinctive feature of this malicious program is its ability to update itself (ie: to automatically download additional component functionality) via the Internet.

Read more:

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

RISK E-BUSINESS by Randy M. Nash

Well, it's finally happened. I had my first close encounter with real life crackers! A good friend of mine recently went to work for a small Internet startup company (I generally refer to them as "3 Men and a Web Server"). I sent him an email Tuesday morning after the long President's Day weekend. His response came as a complete surprise, "Hey, I was just thinking about calling you. We've been hacked! Can you help us out?"

Read more:

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

We have a new section opened in cooperation with Newtork World Fusion, listed below are the seven articles added to that section.

WATCH OUT FOR FAX VOTE SCAM by M. E. Kabay

< <http://www.net-security.org/text/articles/nwf/fax-vote.shtml> >

BANKS AND BIOMETRICS by M. E. Kabay

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

FORGED HEADERS AND THE LAW by M. E. Kabay

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

HOW TO RESPOND TO A HOAX by M. E. Kabay

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

PEER-TO-PEER SOFTWARE AND SECURITY by M. E. Kabay

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

UNAUTHORIZED VULNERABILITY SCANS by M. E. Kabay

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

SNIFFING E-MAIL by M. E. Kabay

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

CISCO ROUTERS FOR IP NETWORKING BLACK BOOK: A PRACTICAL IN DEPTH GUIDE FOR CONFIGURING CISCO ROUTERS FOR INTERNETWORKING IP-BASED NETWORKS

Explores complex topics in-depth, in the popular Black Book format, using a complete systematic approach to Cisco IP networking along with examples and diagrams. Covers the most important routing concepts by introducing the subject and then going through relevant practical examples. The configurations in this book were implemented in a lab with real Cisco routers. Especially written as a comprehensive guide for intermediate and advanced network professionals, or network specialists studying for the CCIE certification, to help answer all major router configuring and troubleshooting issues.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1576106101/netsecurity> >

WINDOWS 2000 REGISTRY (NETWORKING SERIES)

This book targets professional users, system administrators, and support specialists. It enables the reader to master Registry concepts, properly use all of its features, plan and implement the most appropriate Registry backup strategy, and solve the most common problems using the Registry. This book contains in-depth information, and offers tips, tricks, and useful techniques for

editing, customizing, and securing the Registry.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1584500816/netsecurity> >

UNIX NETWORK PROGRAMMING, VOLUME 1: NETWORKING APIS - SOCKETS AND XTI

The classic programming text Unix Network Programming has been updated by author W. Richard Stevens to encompass three new volumes. There have been a few changes in the computing world since 1990 (the year the original was published), and Stevens has taken the opportunity to create a complete set of reference manuals for programmers of all skill levels. The first volume, Networking APIs: Sockets and XTI, covers everything you need to know to make your programs communicate over networks. Stevens covers everything from writing your programs to be compatible with both Internet Protocol version 4 (IPv4) and IPv6, to raw sockets, routing sockets, User Datagram Protocol (UDP), broadcasting/multicasting, routing sockets, server internals, and more, plus a section covering Posix threads. Stevens also notes compatibility issues with different operating systems so that readers can create code that is more portable, and he offers plenty of advice on how to make code more robust.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/013490012X/netsecurity> >

DNS AND BIND

This book's early chapters give a view of DNS from high altitude, explaining basic concepts such as domains, name servers, and name resolution. From there, the authors proceed on a more practical tack, presenting specific instructions for setting up your own domain and DNS server using BIND. The authors then tell you what to do as your domain grows and you need to add more machines, subdomains, and greater throughput capacity. They also talk a lot about nslookup and C programming with the various DNS and BIND libraries. Administrators will find the chapter on BIND debugging output particularly helpful. Here, the authors translate BIND's mysterious error messages and offer specific strategies for fixing and optimizing the program. This edition covers BIND 8.1.2, but pays lots of attention to older versions that are still in wide use (4.8.3 and 4.9). The authors are careful to note differences among the versions.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1565925122/netsecurity> >

Security Software

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

SAINT VERSION 3.1

SAINT (Security Administrator's Integrated Network Tool) is a security assessment tool based on SATAN. Features include scanning through a firewall, updated security checks from CERT & CIAC bulletins, 4 levels of severity (red, yellow, brown, & green) and a feature rich HTML interface. Changes: Check for folder traversal vulnerability in IIS 4.0 and 5.0, JRun server vulnerabilities, iPlanet Directory Server and Certificate Management System, hex-encoded dot-dot-slash vulnerability in web servers, dot-dot-slash vulnerability in Web+, and HTTP PUT vulnerabilities. This version has a new custom scan level, giving you more control over which probes SAINT will run.

Link:

< <http://net-security.org/various/software/973132818,56196,.shtml> >

POWER CRYPTO 1.0

PowerCrypto lets you type in, or paste in, messages for instant encryption. The encrypted nonsense text can then be copied into e-mails, as ordinary text. The receiver then copies this nonsense text into PowerCrypto and decrypts your secret message, IF and ONLY IF, he has your secret key. The program also handles all types of files; documents, programs, pictures, and music files, for example.

Link:

< <http://net-security.org/various/software/973043805,81111,.shtml> >

COMPUTER SOUND SECURITY SYSTEM 1.04

CSSS programme provides effective premises guarding by means of a microphone or several microphones, which act as sensors and a modem, which acts as a signaling (informing) device. The CSSS principle of action consists in microphone (microphones) survey on the scale of real time and highly intellectual analysis of coming signals on the basis of special algorithms based on the methods of speech cognition. Due to the flexible system of tooling the user is able to adjust the action of the programme himself in accordance with the specific requirements of the premises. The system can be adjusted for different frequency ranges and different levels of average total sound signals amount received from the microphone or all microphones in the system. So, it's possible to adjust the system e.g. for human steps only (low frequency sound signals) i.e. the level will start rising considerably after the appearance of low frequency sound signals.

Link:

< <http://net-security.org/various/software/973043978,70494,.shtml> >

OKIDOKI GUARD 1.1.2 (MACOS)

Okidoki Guard is a simple program designed to password-protect your computer. After you put in your name and password, an icon will be placed in the startup folder. After you reboot your Mac, a password prompt screen will come up, asking for your password.

Link:

< <http://net-security.org/various/software/973044264,7082,.shtml> >

STEALTH SIGNAL 3.8

Stealth Signal is a laptop security system that specializes in providing peace of mind to you, the laptop owner. Stealth Signal equips your computer with an undetectable software-based transmitter that sends homing signals to our monitoring network. These signals are transmitted at random times over any Internet connection or phone line.

Link:

< <http://net-security.org/various/software/973044421,5870,.shtml> >

Defaced archives

[01.11.2000] - Silverton Chamber of Commerce

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/01/www.silverton.org/>

[01.11.2000] - Royal Jordainian Web Site

Original: <http://www.rja.com.jo/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/01/www.rja.com.jo/>

[02.11.2000] - Governo do Estado da Paraiba

Original: <http://ntiserv1.saude.pb.gov.br/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/02/ntiserv1.saude.pb.gov.br/>

[02.11.2000] - Cybernet

Original: <http://www.cybernetinc.net/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/02/www.cybernetinc.net/>

[02.11.2000] - The American Israel Public Affairs Committee

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/02/www.aipac.org/>

[02.11.2000] - SCM Labs, Inc.

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/02/www.scmlabs.com/>

[02.11.2000] - SimTel Computers DBA

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/02/www.simtelcomputers.com/>

[03.11.2000] - Jewish Bible Association

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/03/www.jewishbible.org/>

[03.11.2000] - Yizrael Valley College (Mihlelet Emek Yizrael)

Original: <http://www.yvc.ac.il/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/03/www.yvc.ac.il/>

[03.11.2000] - Quantum Computer Services

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/03/www.myownemail.com/>

[03.11.2000] - the hehe.com e-mail service

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/03/www.hehe.com/>

[03.11.2000] - Visiting Israel Students Association

Original: <http://www.visa.org.il/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/03/www.visa.org.il/>

[03.11.2000] - Health Infosystems Association, Israel

Original: <http://www.healthinfonet.co.il/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/03/www.healthinfonet.co.il/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>