

Net-Sec Newsletter
Issue 38 - 19.11.2000
<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

General security news

FOILING DNS ATTACKS

Most of us take DNS servers for granted. Here, in a continuing series on attacking and defending your own machines, I discuss how people attack DNS servers and what you can do to better your security. I answer these questions: How do crackers exploit your DNS servers? How can you harden your DNS servers via configuration? How can you really make it a pain to hack your DNS servers?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/cover/coverstory20001113.html>

WHERE THE LOG FILES LIVE

You know there are logs on your FreeBSD system somewhere; you've probably also heard that it is a good thing to read these logs on a regular basis. You may have even heard horror stories about logs filling up a user's hard drive. So how do we go about finding these mysterious logs?

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.oreillynet.com/pub/a/bsd/2000/11/08/FreeBSD_Basics.html

BLACKHAT '00 VIDEO INTERVIEW - JOHN FLOWERS

A feature video interview with John Flowers, CEO of Hiverworld. In this interview, John discusses recent advances in IDS technology and the IDS industry as a whole.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/media/76>

CYBERTERROR SHOULD BE INTERNATIONAL CRIME

As pro-Israeli and pro-Palestinian attackers continue to attack Middle Eastern Web sites, Israel's former science minister has called for an international convention that would make sabotage over the Internet an international crime, "just like any other terrorism."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/11/13/news13.html>

ENCRYPTION SYSTEM FOR GOVT BOSSES

Top bureaucrats will be able to swap classified material on the Net with the launch this week of a "Secure Electronic Environment" linking Treasury, the State Services Commission and the Department of Prime Minister and Cabinet. The system should reduce the need to courier sensitive information between departments and make it easier for policy-makers to share information and work jointly on projects from their desktop computers. But the system will not offer quite the level of security originally envisaged, as "compromises" have been made to ensure it is usable. Instead of secure individual-to-individual e-mail, it will only offer security between departments. The Secure Electronic Environment (SEE) lets about 500 policy-makers and managers exchange encoded e-mail, electronically "signed" by digital certificates.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.stuff.co.nz/inl/index/0,1008,484516a28,FF.html>

SECURITY MEASURES MAY BE VIRUS CARRIERS

Leading European security experts have warned that viruses may be spread through the use of public keys. Digital signatures, as a part of the public key infrastructure, can create a false sense of security between the sender and receiver as the signature makes the message appear secure. However, specialists have warned that encrypted viruses will be on the increase as soon as encrypted communication becomes more commonplace.

Link: <http://www.silicon.com/public/door?REQUNIQ=974125583&6004REQEVENT=&REQINT1>

MYCIO.COM PLANS

"Security has gotten much more serious as we've moved from trying to figure out how we secure our data to trying to figure out how we selectively expose that data to partners and customers. And companies are looking at every way possible to make the data secure." - said myCIO.com's CEO Zach Nelson.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2653766,00.html>

BSA HITS SOFTWARE PIRATES

It looks like the Business Software Alliance filed lawsuits in the United States and United Kingdom and has brought enforcement actions in Germany, charging dozens of individuals with selling pirated and counterfeit software over auction sites like eBay and QXL.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsa.org/usa/press/newsreleases//2000-11-14.350.phtml>

MOBILE HANDSET SECURITY

CellF-Shield technology, which the Israeli company White Cell plans to licence to the wireless communications hardware industry, can protect a handset as effectively as an anti-virus program protects a PC, its creators say.

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

ISRAELIS HACKERS VOW TO DEFEND

A group of self-described ethical hackers are taking the reins of the Israelis' Web networks into their own hands in the Middle East's cyberwar. Known as the Israeli Internet Underground, the coalition of anonymous online activists from various Israeli technology companies has set up a website to disseminate information concerning the ongoing battle in cyberspace.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,40187,00.html>

LOW-LEVEL E-SECURITY DESPITE HIGH PROFILE ATTACKS

Despite high profile attacks, companies are still not taking e-security seriously, according to research group Datamonitor. E-security breaches cause over \$15bn damage worldwide each year, yet the total spend on security and services is only just over half that at \$8.7bn.

Link:

<http://www.silicon.com/public/door?REQUNIQ=974292920&6004REQEVENT=&REQINT1=40841>

SECURE XML STANDARD DEFINED FOR E-COMMERCE

Netegrity announced plans on Wednesday to develop an XML-based standard to secure e-commerce transactions. Called Security Services Markup Language (S2ML), the standard seeks to build a common vocabulary for sharing user information and transactions -- and encourage single-sign-on -- across multiple platform business-to-business portal and business-to-consumer environments, Bill Bartow, vice-president of marketing at Netegrity, said.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/00/11/15/001115hnnnetegrity.xml>

WASTING AN ATTACKER'S TIME

Attackers regularly waste the time and resources of system and network administrators. Constant port scans result in reams of firewall logs, masking real attacks and requiring significant resources to process. The majority of attackers have plenty of time to devote to probing and attacking networks, while the majority of network admins are quite busy and stretched for time. One attacker can easily probe thousands of machines overnight in an automated fashion, then cull that data to collect more detailed information, and finally check things out manually later on. So why not implement mechanisms to slow attackers down, and ultimately force them to waste time going after imaginary targets?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/closet/closet20001115.html>

FIGHTING THE RISING TIDE

Today, the Internet is more like the everyday world, with all of its promises and problems, than a reflection of academia or an island village. While it's become a tremendous tool for commerce and information, the 'Net has also become a home to thieves, terrorists and vandals. Unlike the real world, where you can usually tell when you're entering a bad neighborhood or confronted by a thug, the Net provides concealment for malicious users.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infosecuritymag.com/nov2000/uwash.htm>

POLICY.COM DEFACED

According to the Newsbytes article, politics web site Policy.com, was defaced by a group called "Anti-Security Hackers". Article covers the story about the defacement, then from the perspective Attrition.org team and then finishes with saying that Mafiaboy is a 'notorious hacker'...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/00/158206.html>

COMPUTER SECURITY 2000 MEXICO

The Computer Security Department of the University of Mexico (UNAM), invites everyone to the Computer Security 2000 Mexico congress which will be held from November 25 to November 30th.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.seguridad2000.unam.mx>

CAN LINUX BE PIRATED?

Linux luminaries including Linus Torvalds and Jon 'maddog' Hall attempted to answer this question during a low-key panel session in the darkest depths of Comdex this week. In a debate about the internationalisation of Linux, the panel was asked whether Linux would suffer the same problems with software piracy that Microsoft and others have in areas such as Asia and Eastern Europe. The 200 or so delegates heard several opinions, but none that nailed down the awkward question.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1114020>

PYTHON: SECURITY ASPECTS

The great flexibility of Python rests in its ability to accept HTTP requests and to be embedded in HTML pages. It is a powerful scripting language, like a Unix shell script with overdrive capabilities. Being able to handle more complex data structures such as associative arrays, the language fills a wide range of roles, including searching databases or acting as a CGI script...

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/python20001116.html>

NEW CRYPTO-GRAM NEWSLETTER

New issue of Bruce Schneier's CRYPTO-GRAM is released. Topic include - Why Digital Signatures Are Not Signatures, Crypto-Gram Reprints, Counterpane Internet Security News. _Secrets and Lies_ News, SDMI Hacking Challenge and Microsoft Hack (the Company, not a Product).

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.counterpane.com/crypto-gram-0011.html>

"BE SECURE OR BE SUED" BUSINESSES WARNED

Businesses around the world are sitting on a legal powder keg by failing to adequately protect their servers from intrusions. Nick Lockett, ecommerce lawyer at Sidley & Austin, said that sites which were used by attackers to launch DoS attacks could be liable for large compensation claims. Lockett said: "There is a distinct probability that if your site has been hijacked for

a denial of service attack, then you could be liable for damages. I would definitely advise clients they have grounds to sue."

Link:

<http://www.silicon.com/public/door?REQUNIQ=974418189&6004REQEVENT=&REQINT1=40900>

INFECTABLE OBJECTS

What parts of my Windows system can be infected by a virus? In the third articles in this series on infectable objects, Robert Vibert examines what's vulnerable and what's not in the face of the new macro viruses.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/virus/articles/infobj3.html)

[bin/news.cgi?url=http://www.securityfocus.com/focus/virus/articles/infobj3.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/virus/articles/infobj3.html)

BIOMETRICS LET YOU FORGET YOUR PASSWORD

At Comdex earlier this week, a host of companies making everything from fingerprint scanners to voice and face recognition systems showed off their products - many of which are in the \$100-per-user range. "It's out there. It's not a concept anymore," said Identix president Jim Scullion, as workers at his booth held up black signs reading "Kill the passwords" and "Practice safe computing" on the Comdex floor.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/11/16/comdex.biometrics.idg/index.html)

[bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/11/16/comdex.biometrics.idg/index.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/11/16/comdex.biometrics.idg/index.html)

WILL THE FUTURE BE ANONYMOUS?

The work of David Chaum and Stefan Brands on protocols, such as blind signatures, that provide anonymity has attracted a great deal of interest among people interested in cryptography.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/anonymous20001117.html)

[bin/news.cgi?url=http://securityportal.com/articles/anonymous20001117.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/anonymous20001117.html)

CREATE FIREWALL-FRIENDLY DISTRIBUTED APPS

The Simple Object Access Protocol (SOAP) promises nothing less than to change how you architect, implement, and deploy VB applications today. At the same time, SOAP, as it stands now, has some significant limitations, not the least of which is performance. Understanding what SOAP is and what it can do for you, as well as what it can't, is the key to using it effectively.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.xmlmag.com/upload/free/features/xml/2000/05win00/ys0005/ys0005.asp)

[bin/news.cgi?url=http://www.xmlmag.com/upload/free/features/xml/2000/05win00/ys0005/ys0005.asp](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.xmlmag.com/upload/free/features/xml/2000/05win00/ys0005/ys0005.asp)

BELGIAN DE MORGEN WEB SITE DEFACED

SecurityWatch reports about the defacement of Belgian daily newspaper De Morgen. Rant mode ON - "So let's analyze the newsworthiness of the story. These observations will ring true for the majority of defacements we've seen this year". Ranting keeps on till the end of the article...

Link: <http://www.securitywatch.com/scripts/news/list.asp?AID=4725>

EDS DEVISES PACKAGE TO PRE-EMPT ATTACKERS

Services giant EDS last week said it knew about recent denial-of-service attacks two months before they happened, and had even identified the tools

the crackers were planning to use. Speaking in Las Vegas before the launch of new EDS Internet security services, vice-president for global information assurance Shakil Kidwai said the company was now offering its anti-attacker intelligence as part of a package of security measures.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/45/ns-19144.html>

ID FRAUD BOOK GOES TOO FAR - MITNICK

Kevin Mitnick, said that a new book that documents how people can uncover ID fraud, as well as conceal their own identities, has gone too far. In his review of "Who Are You? The Encyclopedia of Personal Identification," Mitnick said that the book is "dangerous to the general public and should never have been published."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/00/158317.html>

XINETD

xinetd - extended Internet services daemon - provides a good security against intrusion and reduces the risks of Deny of Services (DoS) attacks. Like the well known couple (inetd+tcpd), it allows to fix the access rights for a given machine, but it can do much more. In this article we will discover its many features.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://mercury.chem.pitt.edu/~tiho/LinuxFocus/English/November2000/article175.shtml>

Security issues

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

GAIM REMOTE VULNERABILITY

There is a buffer overflow in Gaim's parsing of HTML tags when using the OSCAR protocol which allows shell code to be executed when receiving a message with a large HTML tag (i.e. < AAAA...AAA >). The size of the static buffer which is overflowed is about 4100.

Link: <http://www.net-security.org/text/bugs/974250880,29780,.shtml>

DOS VULNERABILITY IN SUN ANSWERBOOK2

Sun's Answerbook fails under certain conditions to delete temporary files that are built by its print function, filling /tmp, and causing the system to fail because processes cannot fork. Briefly, the dwhttp print function builds Postscript files in /tmp and downloads them to the user's browser. It deletes Postscript files after they are successfully sent to the browser. It fails to delete postscript files if the requesting TCP connection is broken before files are completely built and sent to the browser. Undeleted files can be large, and they are more likely to be large than small. First, some printed documents are in excess of 50mb. Second, users

often abort print requests for large documents because the requests require a long time to fulfill and users believe that their requests have failed. Users often try again. Relatively few large requests are necessary to fill a reasonably sized /tmp directory. When /tmp fills Solaris fails because /tmp is used for swap. If/when /tmp fills, swap space eventually also fills preventing additional processes from being swapped. Eventually system memory will fill causing a failure of process spawning altogether.

Link: <http://www.net-security.org/text/bugs/974250893,61218,.shtml>

MORE PROBLEMS FOR PHP-NUKE

Recently the "fixed" version of the user.php script was released. The vulnerability was reported in the article which can be read in <http://www.phpnuke.org/article.php?sid=251>.

This new version though still allows any registered user to alter the password and other personal details of other registered users.

Link: <http://www.net-security.org/text/bugs/974250908,80619,.shtml>

VULNERABILITY IN DCFORUM CGI SCRIPT

Any file can be read with the permissions of user nobody (or webserver) Possible root compromise in /dcforum/dcboard.cgi script. Command execution is not allowed. (Read Only) This has only been tested on unix and linux versions and is unknown if windows versions are effected.

Link: <http://www.net-security.org/text/bugs/974338238,4697,.shtml>

TRUSTIX - BIND AND OPENSSH UPDATES

Trustix has created updated packages for Trustix Secure Linux 1.0x and 1.1 that fixes one security problem and one DOS attack: openssh, openssh-clients, openssh-server: The openssh client does not enforce the "ForwardX11 no", and "ForwardAgent no" configuration options, so that a malicious server could force a client to forward these even if they are turned off.

Link: <http://www.net-security.org/text/bugs/974338263,38259,.shtml>

NETOPIA ISDN ROUTER 650-ST ISSUE

The logs of the router can be viewed from the telnet login screen by pressing a certain key combination. To access the WAN event log type Ctrl-F at the login screen. To access the device event log type Ctrl-E at the login screen Access to these logs may allow access to sensitive information such as usernames or passwords to an arbitrary internet user.

Link: <http://www.net-security.org/text/bugs/974465255,239,.shtml>

NETSNAP WEBCAM SOFTWARE REMOTE OVERFLOW

There's a problem in the handling of GET requests by named server. An unchecked buffer here can be overflowed by a string of approximately 342 bytes, effectively crashing the server and allowing the execution of arbitrary code.

Link: <http://www.net-security.org/text/bugs/974465278,55718,.shtml>

JOE'S OWN EDITOR FILE LINK VULNERABILITY

If a joe session with an unsaved file terminates abnormally, joe creates a rescue copy of the file being edited called DEADJOE. The creation of this rescue copy is made without checking if the file is a link. If it is a link, joe will append the

information in the unsaved file to the file that is being linked to DEADJOE, resulting in a corrupted file.

Link: <http://www.net-security.org/text/bugs/974465302,15109,.shtml>

RED HAT - FIXIED LOCAL ROOT EXPLOIT BUG

modutils, a package that helps the kernel automatically load kernel modules (device drivers etc.) when they're needed, could be abused to execute code as root. modutils versions between 2.3.0 and 2.3.20 are affected.

Link: <http://www.net-security.org/text/bugs/974465337,62610,.shtml>

STILL A CGI-SECURITY HOLE IN DNSTOOLS

"following the notice about Version 1.08 of Dnstoools I looked into the new version (1.10) that is currently downloadable on dnstoools.com. It still contains a sedurity bug by not parsing input-values."

Link: <http://www.net-security.org/text/bugs/974465354,28429,.shtml>

"EXCHANGE USER ACCOUNT" VULNERABILITY

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Exchange 2000 Server and Exchange 2000 Enterprise Server. This vulnerability could potentially allow an unauthorized user to remotely login to an Exchange 2000 server and possibly other servers on the affected computer's network.

Link: <http://www.net-security.org/text/bugs/974465386,87359,.shtml>

REALSERVER MEMORY CONTENTS DISCLOSURE

A memory contents disclosure vulnerability was found on RealNetworks RealServer which will give out information about the server configuration, runtime memory data and tokens and authentication credentials. This information allows an external attacker to possibly obtain administrative access to the server or to data belonging to other user sessions.

Link: <http://www.net-security.org/text/bugs/974465400,56046,.shtml>

ANALOGX PROXY SERVER VULNERABILITY

The Problem lies when FTP Service is ON and Logging is enabled or disabled, or SMTP Service is ON and Logging is enabled or disabled, POP3 Service is ON and logging is enabled. When the Attacker Sends a Multiple Abnormal Strings to a certain affected service it causes the whole Proxy to ShutdOwn. the proxy needs to re-start again to perform normal operation.

Link: <http://www.net-security.org/text/bugs/974465418,74337,.shtml>

Security world

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

SYBARI - NEW WORM VIRUS NAVIDAD.EXE - [12.11.2000]

"The viral part of the e-mail is an attachment called: NAVIDAD.EXE. If executed, it displays a dialog box containing the text "UI" It will then try to use senders' addresses from new emails to email itself to others. The worm copies itself into the Windows and Windows system directories with the filenames WINSVRC.VXD and WINSVRC.EXE and makes changes to the registry so that it executes on boot."

Press release:

< <http://www.net-security.org/text/press/974035838,46210,.shtml> >

DEVATES ON IP PROTECTION AT WEBNOIZE 2000 - [12.11.2000]

Can any digital media truly be secured against piracy? No. It quite simply can't be done. Yet developers of digital rights management systems say that their solutions aren't designed to eliminate piracy, only to keep already honest consumers honest. Still, debates exist relevant even to that seemingly modest proposal.

Press release:

< <http://www.net-security.org/text/press/974035896,68022,.shtml> >

INSIDER ABUSE OF INFORMATION - BIGGEST SECURITY THREAT - [12.11.2000]

Company insiders intentionally or accidentally misusing information pose the biggest information security threat to today's Internet-centric businesses, said Jack Strauss, president and CEO of SafeCorp, a professional information security consultancy headquartered in Dayton, Ohio.

Press release:

< <http://www.net-security.org/text/press/974036126,43054,.shtml> >

VYNAMIC CLOSES \$ 1.2 M FINANCING - [15.11.2000]

Vynamic, the Portsmouth, NH based e-Learning security firm, announced the close of a \$ 1.2 M seed round of financing from individual investors. Vynamic is 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 ensures that students are authenticated and all online learning transactions are encrypted and protected.

Press release:

< <http://www.net-security.org/text/press/974249672,45444,.shtml> >

INFOEXPRESS UNVEILS CYBERGATEKEEPER - [15.11.2000]

In response to increasing security threats resulting from explosive growth in the number of remote users of corporate networks via the Internet, InfoExpress, Inc.

has unveiled "CyberGatekeeper", a remote access firewall solution that dynamically enforces the security policies of a corporate network.

Press release:

< <http://www.net-security.org/text/press/974249896,20488,.shtml> >

STRONGEST ROOT-KEY PROTECTION AVAILABLE - [15.11.2000]

E-business security pioneer Cylink Corporation announced the integration of Chrysalis-ITS' Luna CA, the most widely deployed root-key management device in the public key infrastructure market, with Cylink's NetAuthority PKI software to provide the strongest root-key protection available.

Press release:

< <http://www.net-security.org/text/press/974291057,32468,.shtml> >

SOPHOS DOWNGRADES NAVIDAD AND HYBRIS - [16.11.2000]

Sophos Anti-Virus, one of the world's leading developers of anti-virus solutions, called for calm regarding two new viruses, Navidad and Hybris and urged computer users to follow safe computing guidelines. The move followed media interest and a decision by the US Army to rate Hybris as 'high risk'.

Press release:

< <http://www.net-security.org/text/press/974337447,59776,.shtml> >

NETWORK-1 NAMES MARK TO BOARD OF DIRECTORS - [16.11.2000]

Network-1 Security Solutions, Inc., a leader in distributed intrusion prevention solutions for e-Business networks, today announced that Jonathan I. Mark has been named to its Board of Directors.

Press release:

< <http://www.net-security.org/text/press/974337609,20138,.shtml> >

ZKS'S DR. STEFAN BRANDS RELEASES A BOOK - [16.11.2000]

Dr. Stefan Brands, a renowned senior cryptographer at leading privacy company Zero-Knowledge Systems and adjunct professor at McGill University's School of Computer Science, unveils new privacy-enhancing techniques in his book "Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy," published by MIT Press.

Press release:

< <http://www.net-security.org/text/press/974337742,17621,.shtml> >

NETSTORE SELECTS TREND MICRO FOR AV PROTECTION - [16.11.2000]

Trend Micro Inc., a leading provider of enterprise antivirus and content security, announced that it has entered into an agreement with NetStore, Europe's leading ASP, to provide its customers with protection from email-borne viruses using ScanMail for Microsoft Exchange 2000 v5.0, a solution specially designed for the Microsoft Exchange 2000 platform.

Press release:

< <http://www.net-security.org/text/press/974384956,21064,.shtml> >

SONICWALL ACQUIRES PHOBOS CORP. - [16.11.2000]

SonicWALL, the leading supplier of Internet access security and security services to small and medium business, today announced that it has completed its acquisition of Phobos Corporation, a manufacturer of Internet transaction security technology.

Press release:

< <http://www.net-security.org/text/press/974385053,64093,.shtml> >

ENETSECURE SELECTS BLUE WAVE SYSTEMS - [16.11.2000]

Blue Wave Systems Inc. has announced that eNetSecure Inc., a leading provider of scalable network security solutions and a subsidiary of Applied Signal Technology, Inc., is using its ComStruct building blocks for communications processing in its new telecommunications security system.

Press release:

< <http://www.net-security.org/text/press/974385135,11778,.shtml> >

PROVIDING SECURE DIGITAL IDENTITIES - [16.11.2000]

Equifax Inc., a worldwide leader in information management and e-commerce solutions, and Arcot Systems, Inc., the leading provider of secure digital identities, announced that they have established a strategic partnership to provide end-to-end digital authentication for validation and protection of all e-business transactions. With combined capabilities, Equifax and Arcot will address new customer needs and application requirements.

Press release:

< <http://www.net-security.org/text/press/974385239,37512,.shtml> >

OPERATOR SECURITY SYSTEM FOR LABVIEW - [15.11.2000]

Engineers and scientists who develop mission-critical LabVIEW applications can now take advantage of the Operator Security System (OSS) released by e-NoteBooks. The LabVIEW OSS is a fully integrated user password/security management system. Its main features include programmable operator security levels; an encrypted user/passwords database; a security time-out function

that reverts the system back to a "safe" (low security clearance) state after a preprogrammed time interval; a configuration set-up wizard to step end-users through security system configuration; complete online configuration and updating; automatic operator log file generation; networking capabilities for distributed HMI configurations, and more.

Press release:

< <http://www.net-security.org/text/press/974464286,89716,.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.

A GUIDE TO SYSTEM V INIT by Aleksandar Stancin aka D'Pressed

After you have exorcised all of the daemons that were haunting your system, you might be interested in all of the boring processes that occur when booting your linux. It might seem a bit mystical right now, but it's all quite simple.

Read more:

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

PARANOIA VS. TRANSPARENCY AND THEIR EFFECTS ON INTERNET SECURITY by Mixer

Lately, reactions to non-intrusive probes and network activity that is merely unexpected are becoming increasingly hostile; a result from increasing amounts of incidents and security threats. From my perspective of security, overreactions to activities not crossing authorization and legal boundaries, are leading to a scenario where anyone acquiring basic information about a system needs to be afraid about potential consequences. Seen under a wide scope, this leads to network security no longer being transparent.

Read more:

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

ONLINE BANK SECURITY: COVER YOUR ASSETS! by Randy M. Nash

Why are there so many concerns about online banking? Where is the breakdown in security? Even brick and mortar banks have internal networks that must be secured. It's my understanding that these are very well secured indeed. What

happens when these security-conscious organizations move their presence to the Internet?

Read more:

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

HYBRIS: THE STORY CONTINUES

Kaspersky Lab, warns users of the discovery of Hybris, a new Internet-worm. Kaspersky Lab has been receiving reports of the discovery of this virus "in the wild" worldwide, being particularly active in Latin America although infections by this virus have also been found in Europe.

Read more:

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

EXTRAORDINARY SIMULTANEOUS ACTIVITY OF SEVERAL DANGEROUS INTERNET-WORMS HAS BEEN DETECTED

Kaspersky Lab, an international data-security software-development company, warns users of the notable activity of several dangerous Internet-worms occurring at this time.

Read more:

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

IN THE TRENCHES: INSTALLING AND ADMINISTERING LINUX

Installing and Administering Linux helps network professionals bridge the gap between their prior experience on Windows NT-, NetWare-, and UNIX-based networks and Linux. In a fast-paced, reference style, the authors focus on topics, concepts, and commands for readers with a working knowledge of networking. The Publisher's Edition of Red Hat Linux 6.2 is included on a CD-ROM. Additional technical information and value-added resources are available to readers at the publisher's Web site.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1930713002/netsecurity> >

THE ESSENTIAL GUIDE TO NETWORKING

>From the back cover: Your complete, no-nonsense guide to networking: the fundamentals, without the hype! The Essential Guide to Networking is the complete briefing on networking and the Internet for every non-technical professional! In one easy-to-understand book, James Keogh explains all of today's hottest networking technologies - and helps you make sense of the fast-changing networking industry. The Essential Guide to Networking is a breath of fresh air: an intelligent, thorough, friendly, and up-to-date guide to networking for non-engineers!

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130305480/netsecurity> >

DEBUGGING WINDOWS PROGRAMS: STRATEGIES, TOOLS, AND TECHNIQUES FOR VISUAL C++ PROGRAMMERS

The focus is on providing practical tips for more successful debugging, but many of the suggestions are for tweaking the way in which you write C++ code. Early sections examine how to take full advantage of assert statements (whether in C, MFC, or custom functions), which can be used to write safer code; trace statements, which are used to log debug messages, are covered, too. (Chances are that you haven't seen all of the APIs; luckily, they're rounded up for you here.) There are also numerous tips about C++ style, like how to choose readable variable names, along with the debugging dos and don'ts of working with errors, exceptions, COM objects, and threads.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/020170238X/netsecurity> >

CORE C++: A SOFTWARE ENGINEERING APPROACH

Aimed at the Visual C++ newcomer, Core C++: A Software Engineering Approach provides a rich and sometimes densely packed tour of the language, with plenty of advice on the best ways to use this powerful programming language effectively. It's full to the brim with useful advice for creating and using classes effectively, and gaining an expert's understanding of the language. The writing style and presentation of C++ in this book are outstanding. The explanations of key C++ concepts, from basic language features to class design to advanced C++ whistles and bells, are by turns colloquial, garrulous, and almost always enjoyable and understandable. While it's not uncommon for today's computer book to weigh in at over 1,000 pages, the raw word count here is quite exceptional. You're challenged repeatedly to think for yourself, and the intricacies of C++ are exposed thoroughly, from language features that are indispensable to what to avoid in your code.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130857297/netsecurity> >

Security Software

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

SAINT JUDE LKM

Saint Jude LKM is a Linux Kernel Module for 2.2.11 and greater kernels. This module implements the Saint Jude model for improper privilege transitions. This will permit the discovery of local, and ultimately, remote root exploits during the exploit itself. Once discovered, Saint Jude will terminate the execution, preventing the root exploit from occurring. This is done without checking for attack signatures of known exploits, and thus should work for both known and unknown exploits.

Info/Download:
< <http://net-security.org/various/software/973306563,75975,.shtml> >

SACKURITY 2.0

SACKurity was made for all those people who want to leave their computer and know no one is messing around with it while you are gone. When the password is stored on the computer, it is encrypted, so it is not easily cracked. Ctr. + Alt. + Delete, taskbar, and other functions are disabled, so you cannot leave the SACKurity screen without entering the correct password.

Info/Download:
< <http://net-security.org/various/software/974252964,23274,.shtml> >

SUPER SECURE 2000 V.1.0

Super Secure 2000 is a easy program that can lock anything from the control panel to applications. Super secure is a windows based program that's easy, and fast to use. Ideal for home / office / schools. Protect your settings with a CSuper Secure is not like most security programs, most security programs run a program in the back ground that protects the computer, however, if the file is not loaded it will not protect. Super secure doesn't load a program in the background, it makes the changes to windows that you specify, then by loading a simple EXE, it unlocks it. Super Secure 2000 is fast, reliable, and easy.

Info/Download:
< <http://net-security.org/various/software/974253942,10521,.shtml> >

DREAMENCRYPT V.1.0

DreamEncrypt is an advanced text encryption system which uses a random algorithm based code to ensure your data stays secure. It is ideal for transferring confidential information across the internet or by e-mail. It encrypts your information using the random-seed generator inside your computer, making codes almost impossible to decypher and keeping your data safe.

Info/Download:

< <http://net-security.org/various/software/974254357,89487,.shtml> >

TCPSPY V.1.1

tcpspy is a linux administrator's tool that logs information about incoming and outgoing TCP/IP connections: local address, remote address and, probably the most useful feature, the user name. The current version allows you to include and exclude certain users from logging - this may be useful if you suspect one of the users on your system is up to no good but do not want to violate the privacy of the other users.

Info/Download:

< <http://net-security.org/various/software/974254437,44635,.shtml> >

Defaced archives

[13.11.2000] - Harvard University

Original: <http://www.hbsp.harvard.edu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/13/www.hbsp.harvard.edu/>

[13.11.2000] - Presidenza Del Consiglio Dei Ministri

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/13/www.protezionecivile.it/>

[14.11.2000] - Georgia Department of Education - Office of Technology

Original: <http://techservices.doe.k12.ga.us/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/14/techservices.doe.k12.ga.us/>

[15.11.2000] - #2 National Highway Traffic Safety Administration

Original: <http://www.nhtsa.dot.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/15/www.nhtsa.dot.gov/>

[15.11.2000] - University of Missouri - Law Department

Original: <http://www.law.umkc.edu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/15/www.law.umkc.edu/>

[16.11.2000] - Eastern Energy Resources Team

Original: <http://energy.er.usgs.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/16/energy.er.usgs.gov/>

[16.11.2000] - Ministerio De Desarrollo Economico

Original: <http://www.mindesa.gov.co/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/16/www.mindesa.gov.co/>

[17.11.2000] - Governo do Estado de Sao Paulo

Original: <http://pfeinfo.fazenda.sp.gov.br/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/17/pfeinfo.fazenda.sp.gov.br/>

[17.11.2000] - Ministere de l'Economie et des Finances

Original: <http://www.mfie.gov.ma/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/17/www.mfie.gov.ma/>

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>