

Net-Sec Newsletter  
Issue 39 - 26.11.2000  
<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  
-----  
-----

#### NEW ZEALAND ANTI-HACKING BILL FACES SELECT COMMITTEE

A planned amendment to New Zealand's crime bill that would outlaw malicious hacking for the first time - while also controversially allowing security services the freedom to hack into citizens' computers and intercept e-mail and faxes - has passed through to the Government's Law and Order Select Committee. The long-awaited legislation is mainly intended to criminalize computer hacking in New Zealand. The country has so far been without specific laws outlawing malicious hacking.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/11/19/news7.html>

#### TELEWORKING CAUSES SERIOUS SECURITY THREAT

In the wake of the "hack" into Microsoft's network, security administrators have turned their attention to what some believe is the greatest security challenge facing corporations: teleworkers. Network administrator at US firm SR Equipment Craig LaHote is struggling with it now, and just a week ago he had a meeting with executives about it. "We're having a hard time controlling it. It's a real grey area with home computers accessing the network and the Internet," he said. "We really have a hard time enforcing policies there. We have a policy but no real way to audit [users] except basically asking them to comply."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.co.uk/news/2000/46/ns-19163.html>

#### HACKERS AND THE MEDIA

"Have you ever watched the news, read the newspaper, went to your favorite tech site and read the news? Of course you have, and you have probably heard

the term 'Hacker' used before. Well, let me tell you something my feeble-minded friend. You have been subjected to over-hyped crap that is not true."

Link: <http://geeknews.net/article.php?story=20001119193710182>

#### FILESYSTEM SECURITY - EXT2 EXTENDED ATTRIBUTES

If asked to name the top five security features of the Linux kernel, most administrators would probably not mention ext2 filesystem attributes. Although the definitions for most of the useful ext2 filesystem flags appeared in the kernel source at least as early as the 1.1 development series, this humble feature often takes a back seat to more exotic and recently introduced tools for preserving and assuring system integrity such as LIDS, Tripwire, and others.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/linux/articles/ext2attr.html>

#### FIREWALL ACCELERATION OVER ATM

Firewalls are not new; but high-performance firewalls are. Historically, firewalls used software to examine every packet and then make the decision to forward or drop the packet. This made them slow. When administrators placed them in line with low-speed WAN access links, firewalls introduced no bottlenecks. But the trust boundary where a firewall is needed doesn't always lie at a WAN link. A finance department's network needs protection from disruption by other departments in the building.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwfusion.com/news/tech/2000/1120tech.html>

#### THE LATEST SECURITY FAD: PARTNERING

Security vendors, still scrambling for the right combination of software, hardware and services to offer the enterprise, have another new idea: When in doubt, partner. This week, firewall and intrusion detection maker Zone Labs Inc., of San Francisco, and Tokyo-based anti-virus software developer Trend Micro Inc. will announce a close relationship, capping a furious week of partnering and punctuating a year of failed security solutions.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/eweek/stories/general/0,11011,2655640,00.html>

#### INFOSEC, QUALITY ASSURANCE, AND EXTORTION

"...Anyway, in our conversation, the student and I started off discussing the issue of full disclosure of security vulnerabilities, complete with technical details and even exploit code. I argued that there were better ways to contribute to security than to make powerful exploits available even to cyberspace sociopaths and children. But then we shifted the discussion to people who release details of vulnerabilities to pressure software firms for rapid fixes to problems..."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/cover/coverstory20001120.html>

#### BLACKHAT '00 VIDEO INTERVIEW - IAN GOLDBERG

Ian Goldberg, Chief Scientist with Zero-Knowledge System. In this interview, Ian Goldberg, Chief Scientist with Zero-Knowledge System, offers his perspective on privacy and security issues affecting us today.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/media/79>

### RUSSIA'S HACKERS: NOTORIOUS OR DESPERATE?

In a recent poll on a hacker-oriented Web site, 82 percent said Russia had the world's best hackers; only 5 percent said Americans were better. But the bravado is laced with frustration. Hackers are motivated as much by a lack of opportunity in economically struggling Russia as by criminal leanings, people inside and outside the hacker community say. Sergei Pokrovsky, editor of the magazine Khaker, said that hackers in his circle have skills that could bring them rich salaries in the West, but they expect to earn only about \$300 a month working for Russian companies.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/11/20/russia.hackers.ap/index.html>

### 'ANALYZER' DEFENDS ISRAELI SITES

The twenty-one year old Tenenbaum is serving as CTO of the security firm 2XS. Two weeks ago, according to Tenebaum, he heard from a hacker group he founded in 1996, called the "Israeli Internet Underground" (IIU). The group asked Tenebaum if his company would provide security solutions for Israeli companies for free. "They claimed they are going to help all the Israeli sites that are under attack, or sites that there is a good reason to believe will be attacked," says Tenenbaum. "I liked the idea in general."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/news/116>

### IS THERE HOPE?

What is the feasibility of running national federal elections over the Internet? SunWorld guest writer Avi Rubin focuses on the limitations of the currently deployed infrastructure, with an emphasis on concerns over the security of voting hosts and the Internet itself.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sunworld.com/sunworldonline/swol-11-2000/swol-1103-voting.html>

### SIX MONTHS DOWNTIME

A former computer science student has been sentenced in the US to six months house arrest, two years probation and been banned from using computers for recreational purposes after he attacked Nasa computers last year. 29-year-old Ikenna Iffih, from Boston, Massachusetts, pleaded guilty to charges of defacing a commercial website and wilful malicious interference of communications in June.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1114257>

### A STAR WARS DEFENSE

Basing their strategy on a grad student's work, a new Internet security company has begun beta-testing its solution to Denial-of-Service attacks on the high-speed experimental Internet2 backbone. Asta Networks was formed earlier this year to develop and market the security system by Asta chief scientist Stefan Savage, a doctoral candidate at the University of Washington, and members of the school's Computer Science and Engineering faculty. Their approach to the Denial-of-Service problem is based on his doctoral thesis.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/technology/0,1282,40297,00.html>

#### INTRODUCTION TO FIREWALLS

"In this article I cover some of the design decisions that have to be made before creating a firewall, from architecture to various decisions that should be made."

Link: <http://www.linux.com/sysadmin/newsitem.phtml?sid=1&aid=11296>

#### WINDOWS WHISTLER ADVANCED SECURITY FEATURES

Jim Ewel, Vice President of IT infrastructure and hosting for Microsoft, told reporters in London that the next build of Windows codenamed Whistler, will feature several new security options. One such feature, set to prevent the onslaught of viruses and other scripting problems, prevents Windows from executing any single application lacking a digital signature.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/sp/stories/news/0,4538,2655786,00.html>

#### SECURING ROAMING ACCESS PORTS ON YOUR NETWORK

In this day of the mobile office, a system administrator may have to not only worry about all of the boxes that "live" permanently on the network, but must also now manage hundreds, possibly even thousands, of machines that plug in and out of the network randomly. The people using these roaming machines expect that they will have similar access on their laptops as they do on their desktops, an expectation that can prove to be quite problematic. Each user can theoretically have their own configurations of hardware and software, none of it necessarily having any strong links to the machines that are currently on your network. How then can we still keep a secure network amongst all of this diversity?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://securityportal.com/articles/roaming20001121.html>

#### OPENSHELL INSTALLATION AND CONFIGURATION

The Internet is built with communication in mind. You will routinely move around the Web from one site to the other or telnet to another machine to check your mail or to administer that machine. The trouble with most of these protocols is that they are not encrypted. Over a telnet connection, your passwords are sent as plain-text, which can be read by anyone. Using packet sniffers, even an amateur hacker can spy on your connection and grab your data. Secure Shell was built to address these faults and provide a more secure environment to work in. SSH encrypts all your traffic including your passwords when you connect to another machine over the net. SSH also replaces telnet, ftp, rsh, rlogin and rexec.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.freeos.com/articles/2745/2/13/>

#### ENCRYPTION, FREE SPEECH AND GOVERNMENT REGULATION

Encryption software has sparked regulation by the U.S. government and at least two important lawsuits involving the First Amendment. Exporting encryption products requires a thorough understanding of what's legal and what's not. This article explains the issues.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.gigalaw.com/articles/grossman-2000-05a-p1.html>

#### FREEBSD 4.2-RELEASE IS NOW AVAILABLE

Following the release of FreeBSD 4.1.1 in September, 2000, many bugs were fixed, important security issues dealt with, and a conservative number of new features added. 4.2-RELEASE is now available for i386 and alpha in "FTP installable" form and can be installed directly over the net using the boot floppies or copied to a local NFS/ftp server.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.bsdtoday.com/2000/November/News338.html>

#### MOROCCO GOVT INTERNET SITE ATTACKED

A attacker broke into Morocco's Finance Ministry's Web site for the first time at the weekend but caused no damage, an official said on Monday. Web surfers or potential investors visiting the site at [www.mfie.gov.ma](http://www.mfie.gov.ma) found a message in bad French saying the cover page had been hacked by "NetOperat." The tainted page maintained a link with the ministry's original Internet site stressing the server was not corrupted and invited authorities to protect their system better.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.timesofindia.com/today/22info23.htm>

#### DIMITRI VISITS MICROSOFT IN THE NEDERLANDS

"We saw each other last week and had a useful conversation," Michiel Gosens, a spokesperson for Microsoft in the Netherlands said, after 19-year-old IT student with handle 'Dimitri', visited Microsoft's Dutch office. If you don't remember, Dimitri penetrated and defaced one of the Microsoft's servers for two times in past few weeks.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/00/11/21/001121hnsecret.xml>

#### WORM BLOCKS ANTI-VIRUS SITES

The software virus known as W95/MTX now can block users from going to certain anti-virus software vendor Web sites, thus preventing access to updates. Command Software Systems, a security provider, said the virus was spreading quickly. W95/MTX is a virus, worm, backdoor access Trojan that arrives through e-mail as an attachment, and has a variety of decoy file names. Once launched, it can wipe out files and be difficult to remove.

Link: [http://www.telekomnet.com/xml\\_news/story.asp?id=xml\\_news\\_data/11-22-00\\_worm\\_antivirussites.xml](http://www.telekomnet.com/xml_news/story.asp?id=xml_news_data/11-22-00_worm_antivirussites.xml)

#### WORKERS OPEN BACK DOORS FOR ATTACKERS

Employees are the biggest threat to network security - and they don't even know it. Unauthorised equipment attached to a company network can, according to Robin Dahlberg, UK MD of Internet Security Systems, compromise the best efforts of a network manager to secure the system by creating a "backdoor" into the network.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/1/14910.html>

#### CONTROLLING AND MONITORING COMMUNICATIONS

Aaron Sullivan's popular series "The Crux of NT Security" continues with a look at secure network design and implementation - Where should the Exchange server go? The database server? The firewall?? What protocols should be permitted, and where?

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/microsoft/nt/crux3.html>

#### BIG BUSINESSES STILL IGNORE VIRUS ALERTS

British businesses are still failing to grasp the importance of internet security and network availability according to research released this morning. Despite a raft of scare stories in recent months, more than 70 per cent of respondents believe employees aren't aware of security threats and 40 per cent felt end users remain the most dangerous part of the network.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.silicon.com/a41036>

#### SHROPSHIRE RALLIES AGAINST ATTACKER

The Virtual Shropshire website is tightening security after it was invaded by the attacker who rubbished the county online, describing it as a "series of decaying and festering market towns". The website's description of the county as a rural idyll that welcomed visitors from all over the world was changed by the attacker to a "land of boringly verdant landscapes which have inspired unsuccessful writers and artists for centuries".

Link:

[http://www.thisislondon.com/dynamic/news/story.html?in\\_review\\_id=337726&in\\_review\\_text\\_id=280865](http://www.thisislondon.com/dynamic/news/story.html?in_review_id=337726&in_review_text_id=280865)

#### MORE ON CARNIVORE

House Republican leader Dick Armey added his voice Wednesday to those accusing an outside review panel of whitewashing a controversial FBI cyber surveillance tool. "The Department of Justice stacked the deck for this report," said Armey, a Texas Republican known as a champion of smaller, less intrusive government. "It selected reviewers and set the rules in order to ensure they would get the best possible review."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,40342,00.html>

#### YAHOO! VOWS TO STOP PEDOPHILES

In an exclusive interview with ZDNet News U.K., Martina King, U.K. managing director of Yahoo!, confirmed that the company is about to employ a Yahoo! "inspector" charged with ensuring that Yahoo!'s Messenger system is not polluted with pedophile content.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.msnbc.com/news/493473.asp>

#### U.S. ARMY KICK-STARTS CYBERWAR MACHINE

The U.S. military has a new mission: Be ready to launch a cyberattack against potential adversaries, some of whom are stockpiling cyberweapons. Such an attack would likely involve launching massive distributed denial-of-service assaults, unleashing crippling computer viruses or Trojans, and jamming the enemy's computer systems through electronic radio-frequency interference. An order from the National Command Authority - backed by President Clinton and Secretary of Defense William Cohen - recently instructed the military to

gear up to wage cyberwar. The ability of the U.S. to conduct such warfare "doesn't exist today," according to a top Army official speaking at a conference in Arlington, Va., last week.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2000/TECH/computing/11/22/cyberwar.machine.idg/index.html>

#### TOP 50 SECURITY TOOLS

"I was so impressed by the list they created that I am putting the top 50 up here where everyone can benefit from them. I think anyone in the security field would be well advised to go over the list and investigate any tools they are unfamiliar with. I also plan to point newbies to this page whenever they write me saying "I do not know where to start". Respondants were allowed to list open source or commercial tools on any platform. Commercial tools are noted as such in the list below."

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

#### SNAPSHIELD INTRODUCES ENCRYPTED PHONE CALL SERVICE

Snapshield, formerly known as Microlink, an Israeli company, has developed a phone encryption technology that it says is almost unbreakable. The firm has teamed with Bezeq, the Israeli telecommunications carrier, to offer the service to end users. Bezeq is running its system on a Snapshield secure network access platform, an IT security system that encrypts voice and fax communications.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/11/23/news6.html>

#### BAWP WEB SITE DEFACED

The Register reports that The British Association of Web Professionals Web site ([www.bawp.co.uk](http://www.bawp.co.uk)) has been defaced by a character known as Evil Angelica.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/6/14983.html>

#### THREE ARRESTED IN JAPAN

A team of investigators from five prefectural police forces in Japan arrested three people Thursday on suspicion of illegally accessing computer networks (using others' passwords).

Link: <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20001124a9.htm>

#### MORE REGARDING THE MIDDLE EAST CONFLICT

As tensions in the Middle East continue to simmer, more than a hundred Web sites have been defaced or shut down by pro-Palestinian and pro-Israeli attackers, often with the assistance of activists from several countries not actively involved in the conflict, according to security experts. Ben Venzke, director of intelligence production at iDefense, a Web security firm that has been monitoring the Middle East conflict as it plays out online, said attackers from as far away as South America to the U.S. are expanding the conflict by contributing their skills to whichever side has their sympathies.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computeruser.com/news/00/11/25/news1.html>

-----

## Security issues

---

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

---

### RED HAT - NEW NETSCAPE PACKAGES

A buffer overflow exists in Netscape's HTML parsing code. By using specially designed code, a remote website could cause arbitrary code to be run on the local machine.

Link: <http://www.net-security.org/text/bugs/974730975,56143,.shtml>

### REMOTE DOS IN SMARTSERVER 3

There are remote DoS vulnerabilities in both the SMTP and POP components of the SmartServer3 email server. By passing large arguments to commands in both components, the services can be caused to fail.

Link: <http://www.net-security.org/text/bugs/974730989,79739,.shtml>

### DECRYPTING PASSWORDS FOR SMARTSERVER 3

SmartServer3 (SS3) is a small business email server from NetCPlus. It installs by default in C:\Program Files\smartserver3\ . In this folder it stores a configuration file called 'dialsrv.ini' . This file is accessible to all authenticated users (authenticated to Windows) and contains entries for every user which include their weakly encrypted password.

Link: <http://www.net-security.org/text/bugs/974731010,81908,.shtml>

### WINVNC 3.3.X VULNERABILITY

During the InstallShield setup utility, it creates the registry key:

HKEY\_LOCAL\_MACHINE\Software\ORL\WinVNC3\

which is used to store all of WinVNC's default settings. By default, Administrator and SYSTEM have full control, and Everybody has Special Access (read and modify). The connection password, ip and query restrictions and other settings are all stored here, all editable by anybody.

Link: <http://www.net-security.org/text/bugs/974731046,16257,.shtml>

### ANOTHER IE 5.X/OUTLOOK VULNERABILITY

There is a security vulnerability in IE 5.5/Outlook/Outlook Express which allows executing arbitrary programs using .chm files and revealing the location of temporary internet files folder. This may lead to taking full control over user's computer.

Link: <http://www.net-security.org/text/bugs/974764463,85116,.shtml>

### CGIFORUM 1.0 VULNERABILITY

CGIForum is a free forum. We can set 'thesession' parameter to view files on the vulnerable system with privileges of the user "nobody". This is caused from

OutputHTMLFile function in cgiforum.pl script where \$section (= \$thesection ) isn't checked (never besides in this script).

Link: <http://www.net-security.org/text/bugs/974764481,65837,.shtml>

#### "SESSION ID COOKIE MARKING" VULNERABILITY

On October 23, 2000, Microsoft released the original version of this bulletin, to discuss the availability of a patch that eliminates a security vulnerability in Microsoft Internet Information Server. The vulnerability could allow a malicious user to "hijack" another user's secure web session, under a very restricted set of circumstances. On November 20, 2000, we re-released the bulletin to advise customers using IIS 4.0 on Alpha platforms, or IIS 5.0 on x86 platforms, that new versions of these patch are available, to correct an error in the original version of the patch. The x86 IIS 4.0 patch was not affected by the error, and customers using these systems do not need to take any action.

Link: <http://www.net-security.org/text/bugs/974813634,97052,.shtml>

#### SECURITY PROBLEM IN ADCYCLE INSTALLATION

Adcycle is a banner management system which is written in Perl and uses MySQL for data storage. Installation is done by editing AdConfig.pm, creating a Mysql user/password/database and then running the build.cgi script. That script checks if the database connection is working (showing the username/password it reads from AdConfig.pm) and creating the tables within the database. The 'exploit' is quite simple: when the build.cgi remains executable for your httpd process after the installation, every internet user can view the output of it, including your manager password and database password. Attackers can delete, change and add banner campaigns. Another big problem is when build.cgi is called from a webbrowser, the AdCycle tables are dropped so all banner campaigns are lost.

Link: <http://www.net-security.org/text/bugs/974813650,52259,.shtml>

#### DISCLOSURE OF JSP SOURCE CODE

Under a particular configuration, ServletExec AS v3.0C will disclose the source code of JSP pages when some special characters are appended to HTTP requests.

Link: <http://www.net-security.org/text/bugs/974858485,9354,.shtml>

#### LINUX MANDRAKE - PINE UPDATE

By adding specific headers to messages, the pine mail reader could be made to exit with an error message when users attempted to manipulate mail folders containing those messages.

Link: <http://www.net-security.org/text/bugs/974858502,41213,.shtml>

#### QUICKSTORE SHOPPING CART VULNERABILITY

In a few versions of QuikStore's Shopping Cart it is possible to read any world readable file on the server. One such example is that someone could easily get your password file if it is unshadowed. Also, it's possible, after the passwords have been cracked, to steal credit card information(Yes it does use pgp but some admins may keep the key on the same system. Yes its very likely it could happen.) ,or client personal information.

Link: <http://www.net-security.org/text/bugs/974858522,49182,.shtml>

#### LINUX MANDRAKE - JOE UPDATE

When exiting joe in a non-standard way (such as a system crash, closing an xterm, or a network connection going down), joe will unconditionally append its open buffers to the file DEADJOE. This can be exploited by the creation of DEADJOE symlinks in directories where root would normally use joe. In this way, joe could be used to append garbage to potentially sensitive files, resulting in a denial of service or other problems.

Link: <http://www.net-security.org/text/bugs/974858537,65453,.shtml>

#### INPERSON VULNERABILITIES

InPerson is a multimedia desktop conferencing tool for IRIX workstations. There have been several reports of vulnerabilities in InPerson which allow users with local accounts on IRIX workstations to obtain root access. SGI has investigated the issue and recommends the following steps for neutralizing the exposure. It is HIGHLY RECOMMENDED that these measures be implemented on ALL vulnerable SGI systems.

Link: <http://www.net-security.org/text/bugs/974858551,11592,.shtml>

#### BROKER FTP VULNERABILITY

Broker FTP is vulnerable to two very dangerous attack. First one allows attacker to browse servers whole disk while second one allows attacker to fetch passwords and account information easily.

Link: <http://www.net-security.org/text/bugs/975035606,70513,.shtml>

#### UPDATED OPENSSSH FOR RED HAT LINUX 7.0

An OpenSSH client will do agent or X11 forwarding at the request of a server, even if the user has not requested that it be done. A malicious server can exploit this vulnerability to gain access to the user's display.

Link: <http://www.net-security.org/text/bugs/975035631,86990,.shtml>

#### DEBIAN LINUX - NEW VERSION OF JOE RELEASED

When joe (Joe's Own Editor) dies due to a signal instead of a normal exit it saves a list of the files it is editing to a file called `DEADJOE' in its current directory. Unfortunately this wasn't done safely which made joe vulnerable to a symlink attack. This has been fixed in version 2.8-15.1

Link: <http://www.net-security.org/text/bugs/975035645,47327,.shtml>

#### UPDATE: MICROSOFT SECURITY BULLETIN #86

On November 06, 2000, Microsoft released the original version of this bulletin, announcing the availability of a patch that eliminates a security vulnerability in Microsoft IIS 5.0. On November 10, 2000, we updated the bulletin to clarify the scope of the issue. On November 21, 2000, we updated it again, to discuss two newly-discovered variants of the original vulnerability. The new variants don't change the effect of exploiting the vulnerability. However, they do affect a larger number of products. The original variant affected IIS 5.0 in all cases, but only affected IIS 4.0 when a service pack prior to Windows NT 4.0 Service Pack 6a was in use. The new variants affect both IIS 4.0 and IIS 5.0 regardless of the service pack is in use. Microsoft recommends that all affected customers apply the new versions of the patches.

Link: <http://www.net-security.org/text/bugs/975035667,76284,.shtml>

#### "DOMAIN ACCOUNT LOCKOUT" VULNERABILITY

Microsoft has released a patch that eliminates a security vulnerability in Microsoft Windows 2000. The vulnerability could allow a malicious user to use repeated attempts to guess an account password even if the domain administrator had set an account lockout policy.

Link: <http://www.net-security.org/text/bugs/975035697,89168,.shtml>

#### DOS POSSIBILITY IN SYSLOG-NG

When syslog-ng parses log messages a variable named "left" is used to store the remaining length of the log message. The priority part in the message should look like this:

< 6>

When the line ends without the closing '>' this "left" variable becomes -1 due a to a bug. The remaining part of the message parsing routine checks if there's any characters left using the condition: left != 0, since -1 is not 0, this condition evaluates to true.

Link: <http://www.net-security.org/text/bugs/975035728,81790,.shtml>

#### 602PRO LAN SUITE WEB ADMIN OVERFLOW

The remote administration component (webprox.dll) of this application is subject to a buffer overflow attack through a lengthy GET command. If this request contains 1059 bytes or more it will overflow a buffer and allow the execution of arbitrary code.

Link: <http://www.net-security.org/text/bugs/975035749,3698,.shtml>

#### PHORUM PHP MESSAGE BOARD VULNERABILITY

Any user can parse a choosed php script file using the Phorum suestem. It is also possible, under certain circumstances, to execute arbitrary commands on the server as the httpd user. This is fixed in version 3.2.7 that was released on 2000-11-22.

Link: <http://www.net-security.org/text/bugs/975035768,82550,.shtml>

-----  
Security world  
-----

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

-----  

#### SMARTCARD SECURITY FOR E-BUSINESS - [20.11.2000]

Cylink Corporation announced that it will offer Veridicom's fingerprint-based smartcard reader with Cylink's PrivateCard under a reseller's agreement that will allow the e-business security pioneer to deliver a new class of secure martcards protected with fingerprint authentication for secure desktop and laptop e-business transactions.

Press release:

< <http://www.net-security.org/text/press/974731559,96730,.shtml> >

---

SECURE BLUETOOTH-BASED FINANCIAL SERVICES - [21.11.2000]

Rainbow Technologies, Inc., a leading provider of high-performance security solutions for the Internet and eCommerce, today announced an agreement to partner with Consumer Direct Link, Inc. (CDL) and Acer, Inc., to jointly develop secure Bluetooth-based solutions for the financial services and retail markets. Under terms of the agreement, the companies will develop BluePoint and BlueZone Access Controllers with Rainbow's Virtual Private Network (VPN) encryption technology.

Press release:

< <http://www.net-security.org/text/press/974763478,86814,.shtml> >

---

MCAFFEE PLAYS WITH HOLIDAY HYPE - [21.11.2000]

McAfee Consumer Products Division, a business unit of Network Associates, will again provide consumers with extensive online protection this holiday season with the strong privacy and security technology found in Internet Guard Dog and Internet Guard Dog Pro software. These comprehensive suites offer strong, customizable, privacy controls and security features such as personal firewall technology and encryption, to safeguard consumers' sensitive information while they shop online for holiday gifts. A recent survey by Jupiter Media Metrix reports 35 million people in the United States will purchase gifts online this holiday season, compared with 20 million who shopped online last year.

Press release:

< <http://www.net-security.org/text/press/974814019,13449,.shtml> >

---

SECURE STUDENT-TO-GOVERNMENT TRANSACTIONS - [21.11.2000]

VeriSign, Inc., the leading provider of Internet trust services, announced that it will provide Public Key Infrastructure (PKI) consulting and application integration support for a number of Federal Agencies to enable students to use digital certificates to secure online transactions with the Agencies. These Federal Agencies, including the Department of Education, Department of Labor, Department of Veterans Affairs and the United States Postal Service are collaborating to offer students a single online interface to a multitude of Federal programs, such as student financial aid applications.

Press release:

< <http://www.net-security.org/text/press/974814103,24903,.shtml> >

---

DYNAMIC INTERNET SECURITY MARKETPLACE - [22.11.2000]

In an effort to maximize shareholder value and capitalize on the growth and profit potential of the Internet security software business, Inforum Communications, Inc. announces a shift in business strategy that will allow the Company to focus solely on the continued development of its Internet

security software subsidiary, 2Cactus Development, Inc.

Press release:

< <http://www.net-security.org/text/press/974858708,65409,.shtml> >

---

#### ENTRUST ESTABLISHES PRESENCE IN SINGAPORE - [22.11.2000]

Entrust Technologies Inc., a global leader in solutions that bring trust to e-business, announced plans to establish a local presence in Singapore to better serve and support customers in the South East Asian markets. Recognizing the importance of the region as a hub of e-commerce growth, Entrust plans to directly invest in Singapore to create an infrastructure to expand business throughout South East Asia.

Press release:

< <http://www.net-security.org/text/press/974858767,8054,.shtml> >

---

#### ALADDIN RELEASES HASP CD9 WITH LINUX SUPPORT - [22.11.2000]

Aladdin Knowledge Systems, a global leader in the field of Internet content and software security, announced the release of HASP CD9, the latest software for the HASP4 hardware-based software protection system that offers high-level security for Linux developers, as well as new ease-of-use features.

Press release:

< <http://www.net-security.org/text/press/974858982,86834,.shtml> >

---

#### PARTNERSHIP TO SECURE BUSINESS WEBS - [22.11.2000]

Bowstreet, a leading provider of business web automation solutions for plug-and-play e-commerce, and Netegrity Inc., the leading provider of e-commerce infrastructure solutions for secure portal management, joined forces to bring enhanced security to "business webs." Business webs are emerging e-business networks that connect partner companies to lower transaction costs, generate new revenue, enable collaboration on new products and services, and deliver new value to customers.

Press release:

< <http://www.net-security.org/text/press/974859095,77195,.shtml> >

---

#### ZONE LABS AND TREND MICRO PARTNER - [24.11.2000]

Zone Labs Inc., developers of the award-winning security products ZoneAlarm and ZoneAlarm Pro, and Trend Micro, a leading provider of enterprise antivirus and content security products, announced a far-reaching strategic partnership that allows Trend Micro to incorporate Zone Labs' patented technology in the next generation of Trend Micro's best-of-breed antivirus products. In addition, the agreement opens new co-marketing and distribution channels for each company.

Press release:

< <http://www.net-security.org/text/press/975083837,5240,.shtml> >

---

#### WEBTRENDS SECURITY ANALYZER AWARDED - [24.11.2000]

WebTrends Corporation, the leading provider of Enterprise Solutions for eBusiness Intelligence and Visitor Relationship Management, announced that WebTrends Security Analyzer was awarded Editors' Choice in PC Magazine's November 16 roundup of security scanners.

Press release:

< <http://www.net-security.org/text/press/975083917,88772,.shtml> >

---

#### SONICWALL APPLIANCE AWARDED - [24.11.2000]

SonicWALL, Inc., the market leader in Internet security solutions announced that its ipXpress load-balancing appliance has received the "Best of The Tests" award for Web Acceleration Tools from Network World magazine. The ipXpress was originally a product of Phobos Corporation, a manufacturer of secure transaction processing and load balancing products, which was recently acquired by SonicWALL.

Press release:

< <http://www.net-security.org/text/press/975083972,90488,.shtml> >

---

#### Featured articles

---

All articles are located at:

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

Articles can be contributed to [staff@net-security.org](mailto:staff@net-security.org)

Below is the list of the recently added articles.

---

#### GUIDE TO KERNEL COMPILATION WITH SHORT REFERENCE TO THE NEW 'IPTABLES' FIREWALLING by Aleksandar Stancin aka D'Pressed

In the following article I'll discuss, in brief, compiling of a new kernel, or an old one, which ever pleases you most, on a example of the upcoming kernel 2.4.0, by using the 2.4.0-test9 version, and some references on new and improved firewalling implemented in it, called iptable.

Read more:

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

---

## ENABLING A NEW PGP KEY by M. E. Kabay

You will recall that PGP generates two keys at a time (a keypair) that are complementary: what one key encrypts, the other decrypts - and vice versa. One of the keys is made public; the other is kept secret by its user. This asymmetric encryption algorithm makes possible the public-key crypto-system, and that is very useful indeed.

Read more:

< <http://www.net-security.org/text/articles/nwf/pgp.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](mailto:staff@net-security.org)

---

## SUSE LINUX AND NETFINITY SERVER INTEGRATION GUIDE (REDBOOKS)

>From the Back Cover: Here's all the information you need to maximize SuSE Linux performance and reliability on IBM's state-of-the-art Netfinity server platforms. In this book, a team of IBM's top Linux experts presents start-to-finish, Netfinity server-specific coverage of SuSE Linux 6.2/6.3 deployment and system administration throughout the entire system lifecycle! You'll get running fast with IBM's expert step-by-step preparation and installation techniques: review updating your BIOS and firmware; making the CD-ROM bootable, preparing SCSI devices, partitioning, configuration, XWindows setup, deploying IBM ServeRAID in SuSE Linux environments, and much more. Next, you'll master all the key techniques of day-to-day SuSE Linux system administration, including backup and recovery, Internet and email connectivity, DNS/DHCP name services, and using SuSE Linux with Samba as a world-class file/print server for Windows workstations. IBM-tested, proven, and crystal clear, this is the one essential book for everyone running SuSE Linux on Netfinity servers.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0130286753/netsecurity> >

---

## VISUAL BASIC SHELL PROGRAMMING

Windows users take advantage of shell extensions on the desktop every single day, but understanding what they are and how to program with them can be tricky and, until now anyway, usually required the use of Visual C++. Filled with

expert knowledge of the underlying Windows shell COM objects, Visual Basic Shell Programming is all that you need to write shell-enabled applications that look more professional, as well as rival the functionality of programs that are written in C++. First and foremost, this efficiently packaged text is a reference to all of the COM objects and APIs that are needed to program with the Windows shell successfully. Each section is organized by topic, with an explanation of what kind of functionality you can add, and then all of the COM objects, methods, and constants that you'll need to use in VB, along with sample code. For many of the examples, a custom file extension (.rad) illustrates how to integrate this file into the desktop, and extend what it can do within the Windows desktop.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/1565926706/netsecurity> >

---

### Managing IMAP

Topics covered: The Internet Mail Access Protocol and its implementation, especially in the University of Washington's IMAP server and the Cyrus IMAP server. After presenting the case for IMAP and comparing it to Post Office Protocol (POP), the book shows how to set up and administer both major IMAP servers. It also compares IMAP clients. Other topics that are covered include security, user management, and scalability. A directory of IMAP administration interfaces and an IMAP command reference round out the volume.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/059600012X/netsecurity> >

---

### THE UNIVERSAL HISTORY OF COMPUTING: FROM THE ABACUS TO THE QUANTUM COMPUTER

>From the I Ching to AI, tremendous human brainpower has been devoted to devising easier means of counting and thinking. Former math teacher Georges Ifrah has devoted his life to tracking down traces of our early calculating tools and reporting on them with charm and verve. This book gives a grand title to a grand subject, and Ifrah makes good on his promise of universality by leaping far back in time and spanning all of the inhabited continents. If his scope is vast, his stories and details are still engrossing. Readers will hang on to the stories of 19th-century inventors who converged on multiplication machines and other, more general "engines," and better understand the roots of biological and quantum computation. Ifrah has great respect for our ancestors and their work, and he transmits this feeling to his readers with humor and humility.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0471396710/netsecurity> >

---

### JAVA EXAMPLES IN A NUTSHELL

Aimed at those who have some previous Java experience, Java Examples in a Nutshell, 2nd Edition provides an outstanding collection of code samples that

are designed to help you improve your programming skills--by studying code that works. With over 150 expert examples that illustrate a wide range of Java APIs, this volume definitely can bring your knowledge of Java to the next level. Many programming titles rely on code excerpts to illustrate key programming concepts. This book reverses that approach by emphasizing the code itself, enhancing it with introductory material and explanations. While some short examples illustrate simple algorithms (such as random-number generation and sorting), many of the examples are substantial: for example, how to create a multithreaded Web server, a proxy server, and even a simple Web browser (by using built-in Swing classes for a user interface). These longer examples occupy several pages; generally, they're well-commented models of coding clarity.

Book:

< <http://www.amazon.com/exec/obidos/ASIN/0596000391/netsecurity> >

---

## Security Software

---

All programs are located at:

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

---

## NCPQUERY V.1.2

NCPQuery is an open source tool that allows probing of a Novell Network 5.0/5.1 server running IP. It uses TCP port 524 to enumerate objects with public read access, disclosing such information as account names, server services, and other various objects. A remote attacker can gather the equivalent information provided by the console command "display servers" and the DOS client command "cx /t /a /r" without authentication.

Info/Download:

< <http://net-security.org/various/software/974254520,53276,.shtml> >

---

## LINUX INTRUSION DETECTION SYSTEM [UPDATE]

The Linux Intrusion Detection System is a patch which enhances the kernel's security. When it's in effect, many system administration operations can be made impossible even for root. You can turn the security protection on or off on the fly and you can hide sensitive processes and prevent anyone from using ptrace or any other capability on your system. LIDS can also provide raw device and I/O access protection. Changes: Fixed umount filesystem bug, fixed NFSd and FTPd capability usages, and sys\_sysctl() bugfixed.

Info/Download:

< <http://net-security.org/various/software/974467282,92979,.shtml> >

---

### COOKIE PAL 1.6 BETA 3

Cookie Pal is a complete Internet cookie management system for Windows 95 and NT 4.0. It lets you automatically accept or reject Internet cookies from all sites or just from sites you specify, without having to click on the Web browser's annoying "Cookie Alert" messages all the time. Cookie Pal also allows you to view and delete existing cookies on your system.

Info/Download:

< <http://net-security.org/various/software/975086967,64299,.shtml> >

---

### EWALLET (PALM OS) 2.0

With eWallet you can store, protect, and back up your important information, and find it as soon as you need it. Have your most important personal information backed up for safekeeping, encrypted and password-protected for security on your Palm Powered handheld and desktop PC.

Info/Download:

< <http://net-security.org/various/software/975087040,99608,.shtml> >

---

### CHAOS 2.04

The CHAOS data encryption system provides comprehensive and secure data storage and access control facilities. CHAOS data encryption offers protection against unauthorized data access. CHAOS is totally transparent for application programs.

Info/Download:

< <http://net-security.org/various/software/975087395,68704,.shtml> >

---

### Defaced archives

---

[21.11.2000] - Goodyear Indonesia

Original: <http://www.goodyear-indonesia.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/21/www.goodyear-indonesia.com/>

[21.11.2000] - Alcatel Alcanet International Italia

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/21/www.alcatel.it/>

[22.11.2000] - Harley-Davidson Mexico

Original: <http://www.harley-davidson.com.mx/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/22/www.harley-davidson.com.mx/>

[22.11.2000] - AIWA (UK) Ltd

Original: <http://www.aiwa.co.uk/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/22/www.aiwa.co.uk/>

[22.11.2000] - Government of Guam

Original: <http://govt.gov.gu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/22/govt.gov.gu/>

[23.11.2000] - NEC Brasil

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www.nec.com.br/>

[23.11.2000] - ADC Networks ISP Guadalajara, Mexico

Original: <http://www.adc.net.mx/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www.adc.net.mx/>

[23.11.2000] - Numazu Internetwork Council

Original: <http://www2.numazu-net.or.jp/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www2.numazu-net.or.jp/>

[23.11.2000] - Bulgarian Academy of Science

Original: <http://www.imbm.bas.bg/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www.imbm.bas.bg/>

[23.11.2000] - British Association of Web Professionals

Original: <http://www.bawp.co.uk/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www.bawp.co.uk/>

[23.11.2000] - National Aeronautics and Space Administration Langley Research Center

Original: <http://vabpcnt2.larc.nasa.gov/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/vabpcnt2.larc.nasa.gov/>

[23.11.2000] - Nintendo Spain

Original: <http://www.nintendo.es/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www.nintendo.es/>

[23.11.2000] - NEC Colombia

Original: <http://www.nec.com.co/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www.nec.com.co/>

[23.11.2000] - Stanford University

Original: <http://daily.stanford.edu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/daily.stanford.edu/>

[23.11.2000] - UIS KG (YU)

Original: <http://www.uis.kg.ac.yu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www.uis.kg.ac.yu/>

[23.11.2000] - TMF BG (YU)

Original: <http://www.tmf.bg.ac.yu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/23/www.tmf.bg.ac.yu/>

[24.11.2000] - Naval School of Health Science, San Diego

Original: <http://nshssd.med.navy.mil/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/24/nshssd.med.navy.mil/>

[24.11.2000] - Information on Social Security

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/24/www.socialsecurity.com/>

[24.11.2000] - MicroProse, Inc.

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/24/www.microprose.com/>

[25.11.2000] - Hyundai Motor Company

Original: <http://www.hyundai-motor.com/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/25/www.hyundai-motor.com/>

[25.11.2000] - Massachusetts Institute of Technology

Original: <http://ac.mit.edu/>

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/25/ac.mit.edu/>

[25.11.2000] - California Department of Transportation

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

Defaced: <http://www.attrition.org/mirror/attrition/2000/11/25/www.dot.ca.gov/>

-----  
Questions, contributions, comments or ideas go to:

Help Net Security staff

[staff@net-security.org](mailto:staff@net-security.org)

<http://net-security.org>