

HNS Newsletter
Issue 94 - 07.01.2002
<http://net-security.org>
<http://security-db.com>

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>

Archive of the newsletter in TXT and PDF format is available here:
<http://www.net-security.org/news/archive/newsletter>

Table of contents:

- 1) General security news
- 2) Security issues
- 3) Security world
- 4) Featured products
- 5) Featured article

=====
Sponsored by GFI, the developers of a revolutionary new intrusion detection product - LANguard Security Event Log Monitor.

Download your copy!
<http://www.net-security.org/cgi-bin/ads/ads.pl?banner=gfitxt>
=====

General security news

IPTABLES LINUX FIREWALL WITH PACKET STRING-MATCHING SUPPORT
Linux firewalling code has come a long way since the time ipfwadm was introduced in kernel version 1.2.1 in 1995. Ipfwadm enabled standard TCP/IP packet filtering features such as filtering by source/target addresses and port numbers. Then, in early 1999, when the first stable 2.2.0 kernel was released, firewalling code was replaced with new ipchains-controlled code. New features included support for chains of rules, fragmentation handling, better network address translation (NAT) support and several usability improvements.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1531>

PREDICTABLE PASSWORDS SIMPLIFY A HACKER'S TASK
Computer passwords are supposed to be personal, disposable and discreet. But people become sentimentally attached to them or leave them taped underneath their keyboards or on their monitors, to the dismay of computer security professionals worldwide.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.iht.com/articles/43366.html>

TO CATCH A SPY

Wayne Rash writes: "My friend picked up another corn chip, dipped it in the green salsa, and then started talking again. Somehow, he said, a fellow co worker had talked the IT staff into giving him total access to the organization's network, while still allowing him complete access to the Internet. My friend shook his head in frustration as he continued..."

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/comment/0,5859,2835127,00.html>

'WIN-XP HOLE' MIS-REPRESENTED BY FBI, PRESS, GIBSON

Everyone from the FBI to the LA Times has something scary to say about the new XP vulnerability. Here's why they all have it wrong.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/23517.html>

SECURITY SHOPPING LISTS MADE FOR THE NEW YEAR

Security experts predict that computer security in 2002 will shift away from perimeter defenses in favor of internal access control and authentication management.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.infoworld.com/articles/hn/xml/01/12/31/011231hnsecuritywish.xml>

SWATTING PERSISTENT SECURITY PESTS

DoS attacks, worms, and wireless vulnerabilities constantly hover at the edges of your networks. Squash these bugs before they bite.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.networkmagazine.com/article/NMG20011203S0005>

VIRUSES TO CONTINUE THEIR ASSAULT ON NET

2001 was the worst year yet in the annals of Internet security, and experts say things are only going to get worse in 2002.

Link: <http://www.eweek.com/article/0,3658,s%253D701%2526a%253D20523,00.asp>

UK BANKS BACK SECURE B2B INITIATIVE

Barclays Bank and the Royal Bank of Scotland are to work with some of the world's largest financial institutions to launch a secure online direct business to-business (B2B) payment initiative.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1127903>

AN INSECURE FEELING ABOUT MICROSOFT'S SECURITY

Recent Windows XP security issues casts some doubt on Microsoft's ability to successfully implement its wide-ranging .NET initiative.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.osopinion.com/perl/story/15549.html>

POPULAR FILE-SHARE UTILITIES CONTAIN TROJANS

Popular file-sharing software from Grokster and the Limewire Gnutella Client contain the W32.DIDer Trojan, Symantec revealed last week.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/4/23532.html>

SECURITY, PRIVACY AND RISK MANAGEMENT: 2002 AND BEYOND

Current information security, privacy and risk management problems require new or improved solutions, which can provide new domains for theoretical research or commercial exploitation. In 2002, emerging information security technologies have the potential to resolve these issues; as always, however, the eventual resolution will be more nuanced, subtle and complex than what the press releases often propose.

Link: http://www.gartner.com/DisplayDocument?doc_cd=103566

UNDERSTANDING AND USING IPSEC IN WINDOWS 2000 AND XP

This is the third and final installment in a series devoted to exploring IPsec in Win2K and XP. This article will look at the integration of IPsec policies into Active Directory, attacks on IPsec and other security concerns, as well as a few properties of IPsec.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/infocus/1528>

A ROUGH YEAR FOR SSH

Just as 2000 was a rough year for firewalls, with holes blown in both commercial and open-source products, 2001 was a most uncomfortable year for the secure shell, or ssh. Several groups focused their attentions on this cornerstone of the net, and several problems emerged. ssh has emerged from this scrutiny a stronger product.

Link: <http://www.linuxjournal.com//article.php?sid=5672>

ANTI.SECURITY.IS DEFACED

As posted to the defaced-commentary mailing list on Attrition.org: "anti.security.is has been an outspoken site arguing against the full disclosure concept related to vulnerability disclosure. On January 1, a group known as 'Gobbles' defaced their site with an interesting message. It is unknown if this was really the work of 'Gobbles', a group focusing on full disclosure and releasing many advisories and vulnerability warnings in the past month."

Link: <http://defaced.alldas.de/mirror/2002/01/01/anti.security.is>

ZACKER WORM ATTACKS SAFEGUARDS

A destructive new worm that destroys antivirus software on infected computers was slowly spreading Wednesday.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,5101163,00.html>

NON-STOP AUTHENTICATION WITH LINUX CLUSTERS

As an organization adds applications and services, centralizing authentication and password services can increase security and decrease administrative and developer headaches. This paper describes how we create a reliable, highly

available authentication server using open source software.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www-1.ibm.com/servers/esdd/articles/linux_clust/index.html

WIKIPEDIA: DRINKORDIE

DrinkOrDie (DoD) was a Web-based software cracking and trading (warez) network during the 1990s, shut down in a major raid in 2001. DrinkOrDie was founded in 1993 in Moscow by a Russian with the handle "deviator". By 1995, the group was global. One of its earliest major accomplishments was the Internet release of Windows 95 two weeks before Microsoft released the official version.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wikipedia.com/wiki/DrinkOrDie>

CHROOTING ALL SERVICES IN LINUX

Chrooted system services improve security by limiting damage that someone who broke into the system can possibly do.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxfocus.org/English/January2002/article225.shtml>

PORN TROJAN EXPLOITS OLD MICROSOFT HOLE

The malicious JS/Seeker-E script installed on some Web pages is exploiting a hole in Internet Explorer to redirect users to porn sites.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2102008,00.html>

BUG WATCH: NO SUCH THING AS SECURE IT

Stuart McMillan, European vice president of digital insurance provider Safeonline, argues that there's a big hole in the debate about data security. Businesses must wake up to the fact that you can never create a totally secure IT environment.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1127975>

IT PROS: UNCLE SAM WANTS YOU

The war on terrorism continues to affect the lives of IT professionals. IT pros are answering President Bush's call for greater vigilance, strengthening sensitive internal networks, and coordinating with federal law enforcement agencies to defend against terrorist attacks.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.techweb.com/tech/security/20020104_security

RARE LINUX VIRUS ON THE LOOSE

Linux users are advised not to run exploits from unknown sources. Once RST.b has gained a foothold into the system, it installs a back door and attempts to escalate its permissions to root privileges.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1127965>

BUILDING A LINUX FIREWALL

The 2.4 Kernel of Linux has a great tool called netfilter, which is a framework for creating firewalls. Many new Linux distributions such as RedHat 7.1 come with basic firewall rulesets that allow you to automatically create low, medium, or high security firewalls during installation. Of course, basic rulesets won't usually fit your needs, so you'll need to understand how to create custom rulesets...

Link: <http://www.sys-con.com/linux/articleprint.cfm?id=35>

NVIDIA SETTLES DUTCH HACKING LAWSUIT

Nvidia has settled a lawsuit brought against two computer enthusiasts who published confidential information after allegedly hacking into the graphic chip firm's Web site. Terms are undisclosed.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/23551.html>

FBI REVERSES ADVICE OVER WINDOWS XP VULNERABILITY

The FBI has reversed its advice for computer users trying to protect themselves against serious flaws in the latest version of Windows:

Applying the free fix from Microsoft is adequate, after all.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2002/TECH/industry/01/03/hackers.ap/index.html>

SNORT-SETUP FOR STATISTICS HOWTO

This HOWTO describes how to configure Snort version 1.8.3 to be used in conjunction with the statistical tools ACID (Analysis Console for Intrusion Databases) and SnortSnarf. It also intends to get some internal statistics out of snort, e.g. if there are packets dropped.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.linuxsecurity.com/docs/HOWTO/Snort-Statistics-HOWTO/index.html>

STUDENT DEFENDS HANDLING OF AOL SECURITY FLAW

A 19-year-old Utah college student says he revealed a security flaw in AOL's instant messaging service because when he tried to tell the media giant privately, he was ignored.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.ciol.com/content/news/repts/102010505.asp>

HOME IS WHERE THE HACKERS ARE

As if you didn't have enough to worry about, that computer on your desk at home could be yet another way to threaten your security.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2002/TECH/ptech/01/04/hacking.home.computers.ap/index.html>

=====

HNS Security Database

=====

HNS Security Database consists of a large database of security related companies, their products, professional services and solutions. HNS Security Database will provide a valuable asset to anyone interested in implementing security measures and systems to their companies' networks.

Visit us at <http://www.security-db.com>

=====

Security issues

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

HP SECURE OS SOFTWARE FOR LINUX - APACHE UPDATE

HP Secure OS software for Linux Release 1.0 was released with the 1.3.19 version of Apache. Since then, Apache 1.3.22 has been released to correct a number of security related problems.

Link: <http://www.net-security.org/text/bugs/1010408839,58214,.shtml>

LINKSYS DSL ROUTERS INFORMATION LEAKAGE

LinkSys DSL 'routers' have some serious information leakage, and potent DDoS usage. The following models have been confirmed as having this problem: BEFN2PS4 (EtherFast Cable/DSL Router & Voice with 4-Port Switch) BEFSR81 (EtherFast Cable/DSL Router with 8-Port Switch).

Link: <http://www.net-security.org/text/bugs/1010409052,39498,.shtml>

IE JAVASCRIPT MODELESS POPUP LOCAL DOS

There is a bug in Internet Explorer 6 (probably lower versions down to 5.0 as well) that allows for a javascript to call an infinite amount of modeless dialogs containing the page it was opened in, thus creating an endless loop and rendering the internet explorer useless, this also managed to stay open after killing the iexplore process and continued to loop until cpu usage was maxed at 100%. Due to the nature of the showModelessDialog() function, the dialog fails to give up focus and the machine may even become unable to function requiring a reboot of the machine to regain control of the user interface.

Link: <http://www.net-security.org/text/bugs/1010409190,37058,.shtml>

AOLSERVER 3.4.2 FILE DISCLOSURE VULNERABILITY

Due to a flaw in AOLserver 3.4.2 for Windows, it is possible for a user to gain read access of known password protected files residing on a AOLserver host.

Link: <http://www.net-security.org/text/bugs/1010409253,84126,.shtml>

VULNERABILITY IN NEW USER CREATION IN GEEKLOG 1.3

When the first, new user is created during a fresh installation of Geeklog, that regular user is assigned to the GroupAdmin Group, and subsequently, is a member of the UserAdmin Group. This is a major issue, because if the website is rolled out to the public, in theory, the first new user registered would have Admin rights, which would allow the new user to have control over Geeklog, and subsequently, the entire website.

Link: <http://www.net-security.org/text/bugs/1010409341,92484,.shtml>

MICROSOFT IE LOCAL FILES READING

There is a security vulnerability in IE 5.5 and 6 (probably other versions as well) which allows reading and sending of local files. The problem lies in the fact that you are able to access a local file's dom by calling the execScript function on a newly created window. The sample exploit provided can only read browser readable files however it is highly likely that reading binary files is possible as well (By attaching an event to the dom that calls the xmlhttpcomponent, witch itself at the point of writing is still vulnerable as well) In order for this exploit to work the file name must be known.

Link: <http://www.net-security.org/text/bugs/1010409464,88665,.shtml>

VULNERABILITY IN USER POSTING IN NICK.COM FORUMS

When you create a user and log in to their message board system (powered by PeopleLink), a JavaScript window pops up with the forum selection and main content inside. This doesn't work too well with window resizing/scrolling in Mac OS X (my OS of choice) so I chose to open the JavaScript's html contents in a new window. This helped the problem, but reviled a major flaw in their user identification system.

Link: <http://www.net-security.org/text/bugs/1010409497,33309,.shtml>

HOSTING CONTROLLER - MULTIPLE SECURITY VULNERABILITIES

Hosting Controller has a security flaw which allows outside attackers to browse any file and any directory on that server without any authentication. You're not allowed to read files. However, I believe the second vulnerability (explained below) will allow you to take control of the server.

Link: <http://www.net-security.org/text/bugs/1010409624,77228,.shtml>

SAVANT WEBSERVER BUFFER OVERFLOW VULNERABILITY

The server crashes after sending very long parameter a few times.

Link: <http://www.net-security.org/text/bugs/1010409856,82934,.shtml>

SECURITY ADVISORY FOR BUGZILLA V2.15 AND OLDER

All users of Bugzilla, the bug-tracking system from mozilla.org, who are using a version of Bugzilla installed from a downloaded tarball or package file are strongly recommended to update to version 2.14.1.

Link: <http://www.net-security.org/text/bugs/1010409902,54657,.shtml>

Security world

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

NEW SECURITY HARDENED PROTOCOL REPLACES SMTP

SETAP (Secure Email Transport Authentication Protocol) is a network Email Server protocol that incorporates 2048-bit 4AES Encryption for secure data transmission; a virtually infallible method of client authentication without the use of certificates that may be intercepted and forged; and utilizes Random Data Ports over a 2048-bit 4AES Encrypted Channel using a Unique Session Key for each transaction.

Press release:
< <http://www.net-security.org/text/press/1010077783,54619,.shtml> >

NEWS FROM GFI'S EMAIL SECURITY TESTING ZONE

GFI's Email Security Testing Zone, <http://www.gfi.com/emailsecuritytest/>, has launched two email tests targeted at Outlook XP administrators. Despite Outlook XP's default security settings that do not allow users to run any executable attachments, certain email threats can circumvent Outlook XP's standard protection measures. The two new tests enable Outlook XP users to check whether their system is vulnerable to such threats.

Press release:
< <http://www.net-security.org/text/press/1010162231,35796,.shtml> >

SOPHOS: TOP TEN VIRUSES IN DECEMBER 2001

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

Press release:
< <http://www.net-security.org/text/press/1010162427,30687,.shtml> >

=====
Help Net Security T-Shirt available

=====
Thanks to our affiliate Jinx Hackwear we are offering you the opportunity to wear a nifty HNS shirt :) The image speaks for itself so follow the link and get yourself one.

Get one here: <http://207.21.213.175:8000/ss?click&jinx&3af04db0>

=====

Featured products

The HNS Security Database is located at:
<http://www.security-db.com>

Submissions for the database can be sent to: staff@net-security.org

KEYTRONIC SECURE SCANNER KEYBOARD

Key Tronic Corporation has long been a leading innovator in state-of-the-art computer input devices. The company has been on the forefront of nearly every keyboard innovation, including fingerprint recognition, smart-card reader capability, infrared wireless and Universal Serial Bus (USB) technology. Key Tronic's Secure line of products has been designed to increase both network and desktop security. Gone is the hassle of remembering and administering scores of passwords. Now, users rely on personal identification that cannot be duplicated, forgotten, or cracked by hackers. The 104-key Secure Scanner Keyboard is easy to use and cost efficient, making network security more manageable and affordable than ever. Identix's BioLogon software is packaged with each unit.

Read more:

< <http://www.security-db.com/product.php?id=262> >

This is a product of Identix Incorporated, for more information:

< <http://www.security-db.com/company.php?id=50> >

NORMAN PRIVACY

Using Norman Privacy you can encrypt and decrypt:

- Removable disks
- Directories
- Files
- Text
- Encrypt e-mails, including attachments if required
- Create self-decrypting files, directories and disks
- Compress encrypted data
- Set expiry dates for encrypted data
- Choose from three algorithms
- Securely handle original files

Read more:

< <http://www.security-db.com/product.php?id=1065> >

This is a product of Norman, for more information:

< <http://www.security-db.com/company.php?id=234> >

VTCP REMOTE ACCESS VPN

VTCP is a remote access VPN that securely extends the corporate network to remote users over the Internet. The software creates a tunnel between the remote user's PC that protects data through encryption, authentication, and authorization.

Read more:

< <http://www.security-db.com/product.php?id=1040> >

This is a product of InfoExpress, Inc., for more information:

< <http://www.security-db.com/company.php?id=7> >

Featured article

All articles are located at:

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

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

AUTHENTICATION: BOOK REVIEW

Recommended reading material to get yourself acquainted with Authentication, passwords and public keys, and an easy one to follow.

Read more:

< <http://www.net-security.org/various/bookstore/smith/> >

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org

<http://net-security.org>

<http://security-db.com>