

HNS Newsletter
Issue 78 - 10.09.2001
<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
- 6) Security software

=====
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

COMPUTER VIRUS COSTS REACH \$10.7B THIS YEAR
The cost of virus attacks on information systems around the world reached an estimated \$10.7 billion so far this year, according to Computer Economics of Carlsbad, California. That compares with \$17.1 billion for all of 2000 and \$12.1 billion in 1999, Computer Economics said.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.washtech.com/news/netarch/12267-1.html>

BOARDS FAIL THE SECURITY TEST
Company boards should do more to improve e-business security, as digital crime is deterring many firms from selling goods and services over the Internet, according to a recent report.
Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094338,00.html>

BIOMETRICS: JUST IN A JAMES BOND FLICK? NOT ANYMORE!

We all know that Linux is growing in popularity with embedded device makers of all kinds. Due to a variety of compelling factors Linux may well be the operating system behind all kinds of items of technology you use every day, without even knowing it. Security systems will be one of those. This article provides a brief overview of the new science of biometrics and how it is shaping up in the security technology sector.

Link: <http://www.linux.com/enhance/newsitem.phtml?sid=1&aid=12511>

ICAC TO INVESTIGATE HACKING AT NSW PARLIAMENT

The anti-corruption watchdog has been asked to investigate allegations of computer hacking at New South Wales Parliament. The allegations arose after files belonging to the Opposition found their way on the computer belonging to Labor MP Tony Kelly. An investigation by police has cleared Mr Kelly of allegations that he hacked into the Coalition's computers.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.abc.net.au/news/politics/2001/09/item20010902114054_1.htm)

[bin/news.cgi?url=http://www.abc.net.au/news/politics/2001/09/item20010902114054_1.htm](http://www.abc.net.au/news/politics/2001/09/item20010902114054_1.htm)

RUSSIAN COMPUTER EXPERTS WARNED

Russia warned its computer experts on Friday of the dangers of visiting the United States after a Russian software designer was arrested there for violating a controversial new law.

Link: http://finance.individual.com/display_news.asp?doc_id=RTH31a8161rittz&page=news

INFORMATION SECURITY CERTIFICATION: A RULE OF THUMB

There were heady times - 1994, 1995 - when IT security skills were considered a nice-to-have, an extra string in the IT professional's bow. The industry has since matured. Businesses are now recognizing the primacy of information security as a business enabler. And spiraling demand for security skills - not to mention the intellectual challenges and camaraderie of the field - has meant that IT professionals are flocking to board the security train. The question is, "How do you go about it?"

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securitywatch.com/TRE/062001.html)

[bin/news.cgi?url=http://www.securitywatch.com/TRE/062001.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securitywatch.com/TRE/062001.html)

FBI WARNS AS UNIX WEB SERVER FLAW GETS AUTOMATED

A worm called x.c, which takes advantage of a buffer overflow vulnerability in the telnet daemon program commonly used on Unix boxes, has been discovered, and security experts fear it is a harbinger of worse to come.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21438.html)

[bin/news.cgi?url=http://www.theregister.co.uk/content/55/21438.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21438.html)

DUBAI 'HACKER' APPEALS CASE JUDGEMENT

The British computer consultant last month found guilty of hacking into Etisalat, the United Arab Emirates' only ISP, has appealed against the outcome. Twenty-two-year-old Lee Ashurst, currently detained in Dubai, is appealing the fine on the grounds that there are no laws against computer hacking in the UAE.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computing.vnunet.com/News/1125113)

[bin/news.cgi?url=http://www.computing.vnunet.com/News/1125113](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computing.vnunet.com/News/1125113)

APOST WORM SPREADING

Apost is an email-aware worm which makes use of the Microsoft Outlook mail client. The worm arrives in an email with the following characteristics: "Subject line: 'As per your request!'" and Message body: 'Please find attached file for your review. I look forward to hear from you again very soon.

Link: <http://www.net-security.org/text/viruses/999557280,99395,medium.shtml>

CACHE CORRUPTION ON MICROSOFT DNS SERVERS

The CERT/CC has received reports from sites experiencing cache corruption on systems running Microsoft DNS Server. The default configuration of this software allows data from malicious or incorrectly configured servers to be cached in the DNS server. This corruption can result in erroneous DNS information later being returned to any clients which use this server.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cert.org/incident_notes/IN-2001-11.html

KELLY DEMANDS APOLOGY OVER HACKING CLAIMS

A NSW Labor MP cleared of allegations he hacked into confidential Liberal Party computer files wants an apology from Opposition Leader Kerry Chikarovski. An internal report concluded that confidential files of shadow cabinet secretary Charlie Lynn were accidentally loaded onto the parliamentary computer of Tony Kelly by IT staff.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://news.ninemsn.com.au/national/story_17955.asp

WHAT IS ECHELON?

The following information consists entirely of excerpts from the European Parliament's "Temporary Committee on the ECHELON Interception System" report. After reading the entire lengthy, and often technical, report I decided to sift through and find the information that most people would find informative and applicable to their own lives and use of the Internet and electronic communications in general.

Link: http://www.net-security.org/cgi-bin/news.cgi?url=http://cipherwar.com/news/01/echelon_ep.htm

NEW MAGISTR WORM VARIANT

In Magistr.b, a substantially reworked encoding algorithm of the virus code is utilized. Because of this, none of the known anti-virus scanners are able to recognize this new virus variant even with the heuristic code analyzer switched on, commented Eugene Kaspersky, Head of Anti-Virus Research at Kaspersky Labs.

Link: <http://www.net-security.org/text/viruses/999613294,89500,low.shtml>

HONEYNET PROJECT UPDATE

Scan 15 challenge was to recover a deleted rootkit from a compromised Linux partition. This month's scan it to decode and analyze the Snort binary capture of that same attack. All submissions are due no later than 17:00 CST, Friday, 21 September. Results will be released Monday, 24 September.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://project.honeynet.org/scans/scan18/>

DUG SONG CITES DMCA

Jon O. on DMCA_discuss list - "Dug Song is a highly respected OpenBSD, OpenSSH programmer, the author of Dsniff and numerous security papers including a common vulnerability in many firewall applications and servers. He has censored his own website, citing the DMCA:

<http://www.monkey.org/~dugsong/>

At this time it is not clear whether the site was taken down under pressure from corporations or simply attempting to express feelings about the DMCA and possibly start a trend whereby security researchers withhold their own research because they are at risk under the DMCA."

VIRUS THREATS UPDATE

"We've had several reports of Apost over the last few days, but to be honest it's a lot smaller than Magistr or SirCam," said Graham Cluely, senior technology consultant at anti-virus company Sophos. "After six months we are still getting reports of Magistr, and SirCam is even bigger although it has not been around for as long," he added.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094583,00.html)

[bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094583,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094583,00.html)

TREND GETS SECURITY PATENT FOR JAVA CODE DEFENCE

Trend Micro has secured the patent for a technique to detect malicious code in Java applets. According to Reuters, Trend believes the patent will help put it ahead of its competitors in protecting mobile devices and phones for the next wave of computer viruses. The agency reports it is in talks with an unspecified number of telcos about licensing agreements concerning its technology.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21477.html)

[bin/news.cgi?url=http://www.theregister.co.uk/content/55/21477.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21477.html)

SINGAPORE, BELGIUM TIE UP FOR VIRUS ALERTS

Using a videoconferencing link, ministers from Singapore and Belgium signed an agreement setting out cooperation on national virus early warning systems. Each country's relevant agencies will work together designing effective national virus alert systems.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169746.html)

[bin/news.cgi?url=http://www.newsbytes.com/news/01/169746.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169746.html)

BRITISH NAVY EMBRACES WEB FOR WAR GAMES

The British Navy is taking the Internet to its heart in its new three-month military manoeuvres in the Gulf starting next month. The commanders of the biggest deployment of ships since the Falklands war will use a secure Net chatroom to discuss tactics and problems.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21483.html)

[bin/news.cgi?url=http://www.theregister.co.uk/content/55/21483.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21483.html)

XP CRACKS APPEAR BEFORE PRODUCT

In Microsoft's battle against software piracy, the first round goes to pirates, even though the starting bell hasn't even rung yet. Microsoft's new operating system, Windows XP, won't be in stores for another seven weeks, but pirated copies are already floating around on the Internet. There are also a number of hacks and patches designed to circumvent the operating system's

controversial Activation process, a new antipiracy measure.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://wired.com/news/business/0,1367,46531,00.html)

[bin/news.cgi?url=http://wired.com/news/business/0,1367,46531,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://wired.com/news/business/0,1367,46531,00.html)

IN PKI WE TRUST?

When PKIs hit the streets a few years ago, a media frenzy ensued - remember 1999, the year of the public-key infrastructure? Now it's the morning after, and we've gotten a dose of reality when it comes to the cost and complexity of rolling out a PKI. But one thing remains constant: Positive authentication is vital for doing business regardless of whether you're express-mailing paper contracts and purchase orders or sending those documents electronically.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwc.com/1218/1218f3.html)

[bin/news.cgi?url=http://www.nwc.com/1218/1218f3.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.nwc.com/1218/1218f3.html)

STUDY: WHO NEEDS PRIVACY LAWS?

In a bid to thwart federal regulations on how companies collect information, a California nonprofit group is saying that technology will protect Americans' privacy better than new laws can. During an event at the National Press Club, Pacific Research Institute staff members handed out copies of their new privacy study, which advises legislators to act cautiously when imposing rules on U.S. businesses and consider the potential negative consequences of regulations.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/privacy/0,1848,46558,00.html)

[bin/news.cgi?url=http://www.wired.com/news/privacy/0,1848,46558,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/privacy/0,1848,46558,00.html)

HACKER FORCES SOME BANKS TO CANCEL VISA DEBIT CARDS

Several banks in the Washington area have been forced to cancel and reissue thousands of Visa debit cards after a hacker allegedly intercepted a file containing purchase data from a local online merchant. First Virginia Banks Inc. this week began notifying 500 of its customers that their card numbers and expiration dates, telephone numbers and addresses had been compromised. Likewise, Atlanta-based SunTrust Banks Inc. also began monitoring several customer accounts that may have been compromised.

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO63555,00.html)

[bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO63555,00.html](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.computerworld.com/storyba/0,4125,NAV47_STO63555,00.html)

LARA CROFT VIRUS BUSTS IRC

Security experts have warned internet surfers to be on the look out for a 'Lara Croft' virus that emerged into the wild. The worm is the first malicious virus hosted and spread by Windows Desktop Theme files. The threat is not deemed serious as the LaraCroft.theme host file can only be spread via IRC.

Link: <http://www.net-security.org/text/viruses/999730541,68104,low.shtml>

Link: [http://www.net-security.org/cgi-](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1125181)

[bin/news.cgi?url=http://www.vnunet.com/News/1125181](http://www.net-security.org/cgi-bin/news.cgi?url=http://www.vnunet.com/News/1125181)

SECURITY EXECES SEE HP-COMPAQ MERGER AS POSITIVE

Art Coviello, CEO and president of RSA Security, said the merger would be good for the industry. "The PC market looks like it needs consolidation, and I think there are great cultures of innovation at both companies," he said.

"Provided they can execute on the always difficult task of bringing two companies together, I think it can be wonderful for shareholders, customers and the industry."

Link: <http://www.crn.com/Sections/BreakingNews/dailyarchives.asp?ArticleID=29554>

PRIVACY FLAW FIXED AT VERIZON WIRELESS SITE

Verizon Wireless has plugged a hole that was leaking private information about cell phone customers who used one of its Web sites, Newsbytes reports.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169781.html>

AN INTRODUCTION TO OPENSLL, PART TWO

This is the second article in a series on OpenSSL, a library written in the C programming language that provides routines for cryptographic primitives utilized in implementing the SSL protocol. In the first article in the series, we discussed some of the basics of cryptography. This article will cover acquiring and compiling OpenSSL and explore some commands that facilitate encryption and decryption.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securityfocus.com/focus/sun/articles/openssl2.html>

JAIL INTERNALS

On most UNIX systems, root has omnipotent power. This promotes insecurity. If an attacker were to gain root on a system, he would have every function at his fingertips. This article focuses on the internals (source code) of Jail and Jail NG. Jail is becoming the new security model. People are running potentially vulnerable servers such as Apache, BIND and Sendmail within jails, so that if an attacker gains root within the jail, it is only an annoyance, and not a devastation.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.daemonnews.org/200109/jailint.html>

LINUX ADMINISTRATOR'S SECURITY GUIDE UPDATED

Kurt Seifried writes: "After many months (ok, years) of inactivity I have started to update the Linux Administrator's Security Guide (LASG)."

Link: http://linuxtoday.com/news_story.php3?ltsn=2001-09-05-023-20-SC-HL

FRENCH JUDGE CONSIDERS MORE NET NAZI BANS

A French judge launched hearings on Tuesday into whether Internet service providers should censor portals accessible on their networks to stop French citizens viewing links to neo-Nazi Web sites.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.cnn.com/2001/TECH/internet/09/05/france.internet.nazi.reut/index.html>

MAILMONITOR FOR SMTP PUBLIC BETA

A public beta of MailMonitor for SMTP, Sophos's anti-virus solution for mail gateways, is now available for download from the beta area of the Sophos website. The current release works on the Windows NT/2000 operating systems, a beta for the Linux operating system will be available shortly.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.sophos.com/downloads/beta/>

SECURITY EXPERTS SLAM DOJ DECISION

Security experts slammed the U.S. Department of Justice's decision not to pursue a breakup of Microsoft. Bruce Schneier, chief technology officer at Counterpane Internet Security, agreed. "Currently we don't see a lot of software quality from Microsoft in terms of security and reliability," he said. "There's no competitive reason for Microsoft to produce secure software. When you control so much of the market, you don't have to."

Link: <http://www.crn.com/Sections/BreakingNews/dailyarchives.asp?ArticleID=29603>

SECURITY FIRM RAPS FBI'S CODE RED RESPONSE

The security company that discovered the software hole exploited by the Code Red worm has launched an attack on the FBI for its reluctance to publicize the flaw.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-7078908.html>

WHO'S READING YOUR RESUME?

People who post their resumes on Monster.com, the world's largest job-seeking site, "face considerable threats to their privacy," according to a watchdog group. In a 24-page report, The Privacy Foundation accused Monster of attempting to sell users' private data to marketers, failing to completely remove resumes after job-seekers deleted them, and sending user information to America Online to satisfy the terms of a business agreement.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/business/0,1367,46559,00.html>

ENEMIES ARE EVERYWHERE

Seizing upon the timely topic of Internet security risks, IBM this week has launched a global advertising and public relations initiative to plug its e-business security software and consulting expertise. Business managers, concerned at the threat of attack, are fortifying their internal computer systems. Last week, a Corporation for British Industry survey revealed that two-thirds of U.K. businesses have been the victim of a serious computer-related incident, whether it be hacking, a virus attack or some form of cyber fraud.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.zdnet.com/zdnn/stories/news/0,4586,2810785,00.html>

OPENSSE KEY MANAGEMENT, PART 2

Many developers use the excellent OpenSSH as a secure, encrypted replacement for the venerable telnet and rsh commands. One of OpenSSH's more intriguing features is its ability to authenticate users using the RSA and DSA authentication protocols, which are based upon a pair of complementary numerical "keys". One of the main appeals of RSA and DSA authentication is the promise of being able to establish connections to remote systems without supplying a password. In this second article, Daniel introduces ssh-agent (a private key cache) and keychain, a special bash script designed to make key-based authentication incredibly convenient and flexible.

Link: <http://www-106.ibm.com/developerworks/linux/library/l-keyc2/?open&l=252,t=grl,p=ossh2>

THE U.S. RECRUITS NEW HACKERS

The government desperately needs experts to fight hackers. So they've recruited a 63-year-old retired aerospace engineer, a midwestern mother of three, and a long-haired former teen golfing champ to do the job.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/politics/0,1283,46567,00.html>

'CODE BLUE' WORM EMERGES ON THE NET

New menace emerges in the form of a worm that exploits a different weakness in Microsoft's Internet Information Server.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094796,00.html>

QUANTUM CRYPTO TO THE RESCUE

This week has been big for cryptography. It's seen both technical and theoretical advances in next-generation quantum crypto systems and technology. It's seen a prototype enter its testing phase that could send secret crypto keys through open air to a satellite or across town. And it's seen the announcement of a new breed of laser that could someday form the backbone of secure, long-distance quantum cryptographic communications over fiber-optic lines.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.wired.com/news/infostructure/0,1377,46610,00.html>

PGP OPENS UP COMPLETE ENCRYPTION SOURCE CODE

PGP Security - a division of Network Associates that has been criticised in the past for being too proprietary - has made available the electronic distribution of its complete source code for the PGP SDK, its cryptographic toolkit.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094808,00.html>

INTERNET SECURITY HELPED BY CODE RED

Security researchers are now finding that the creatures' digital namesakes might be good for security. In its monthly report released earlier this week, Internet survey firm Netcraft found that Web servers running Microsoft's software have become much more secure in the wake of the Code Red worm attack.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.cnet.com/news/0-1003-200-7083150.html>

BACKDOOR G2 TROJAN

This is the server side of a hacking tool and enables a remote user running the client side of the tool to access an infected computer. The Trojan copies itself to the infected system and modifies the registry so that it is executed at every boot up.

Link: <http://www.net-security.org/text/viruses/999864805,39347,low.shtml>

CODE BLUE CONFIRMED BUT CONTAINED

Virus experts confirmed the existence of Code Blue, the latest Internet worm to target unpatched Microsoft Webservers. The new worm, which does not

appear to be spreading rapidly, exploits a nearly year-old flaw in Microsoft's IIS software known as the Web Server Folder Traversal vulnerability, according to an analysis of the code published today by major US-based virus researchers.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169891.html>

TOOL COPIES HACKERS TO DETECT FLAWS

UK firm ProCheckUp has developed an online tool to expose network security flaws by using artificial intelligence to mimic the actions of a hacker. However, experts question how successful the software will be at detecting security holes.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://news.zdnet.co.uk/story/0,,t269-s2094843,00.html>

POLISH WORM PROVIDES JOLT TO UNIX OPERATORS

A new Internet worm that prompted an FBI warning last month has been confirmed dead. But security experts cautioned that X.C. could be the first in a series of self-propagating worms designed to target a common flaw in Unix systems.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.newsbytes.com/news/01/169859.html>

THE CISCO INTRUSION UNDETECTION SYSTEM

Cisco has issued an alert for its Intrusion Detection System, one day after launching an enhanced security portfolio. IDS inspects network traffic and raises alerts for suspect traffic and it can be fooled by hackers who encode packets using "%u", a non-standard form for coding similar to Unicode. Suspect packets made using this method of coding would be flagged straight through by Cisco's IDS.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.theregister.co.uk/content/55/21547.html>

PRIORITIZING PATCHES: A PRECIPITOUS PANDEMONIUM

Is the patching of mission critical systems and related software a priority for your business? May I suggest that patching such software become an imperative task incorporated into an IT position ASAP. Recent virus outbreaks and increases in overall attacks have resulted in a precipitous pandemonium for IT administrators and managers who failed to make patching and security a high priority.

Link: <http://www.net-security.org/cgi-bin/news.cgi?url=http://www.securitywatch.com/RES/September3.html>

Security issues

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

VERIZON WIRELESS WEBSITE GAPING PRIVACY HOLES

Cell phone bills are often very interesting things, since they contain names, addresses, and a complete record of calls placed and received, along with the approximate location the user was when the call was made. I'm sure I'm not alone in expecting my provider to provide a reasonable level of privacy for this data. A typical URL used by this "my account" service is:
https://www.app.airtouch.com/jstage/plsql/ec_navigation_wrapper.nav_frame_display?p_session_id=3346178&p_host=ACTION
Note the p_session_id parameter. This is the only session identifier used. They are assigned sequentially to each user as they login, and are valid until the user logs out or the session times out. Obviously, this makes it trivial to access the sessions of other users by guessing the session ID. Automated tools to grab this information in bulk as users login over time are also trivial.
Link: <http://www.net-security.org/text/bugs/999527596,2374,.shtml>

POP3LITE 0.2.3B MINOR VULNERABILITIES

POP3Lite is a modular POP3 daemon developed to be fast, flexible and easy to use. It runs on Linux and *BSD. POP3Lite fails to escape dots in messages it transfers to clients. Clients popping their mail from a vulnerable POP3Lite can be sent arbitrary server responses embedded in carefully crafted emails, possibly leading to arbitrary message injection, lost messages, or otherwise annoying client misbehaviour.
Link: <http://www.net-security.org/text/bugs/999527726,9730,.shtml>

IPLANET MESSAGING SERVER 5.1 BUFFER OVERFLOW

Netscape Administration Server, provided by iPlanet Messaging Server 5.0 as a console program for administration, has a buffer overflow vulnerability. It allows remote users to execute arbitrary commands with SYSTEM privilege.
Link: <http://www.net-security.org/text/bugs/999527877,67378,.shtml>

SE SECURITY - NKITB/NKITSERV/TELNETD

The telnet server which is shipped with SuSE distributions contains a remotely exploitable buffer-overflow within its telnet option negotiation code. This bug is wide-spread on UN*X systems and affects almost all implementations of telnet daemons available. SuSE 7.2 distribution ships the telnet-server package which contains the vulnerable telnet daemon. This package has been fixed.
Link: <http://www.net-security.org/text/bugs/999553288,42184,.shtml>

GAUNTLET FIREWALL VULNERABILITY

There is to be a buffer overflow vulnerability in SMTP proxy in Gauntlet firewalls 5.x and 6.0 under Solaris and HP-UX. Also in the PGP e-ppliance 300 series version 1.0, 1.5, and 2.0; PGP e-ppliance 1000 series versions 1.5 and 2.0; McAfee e-ppliance 100 and 120 series; and McAfee WebShield for Solaris v4.1.
Link: <http://www.net-security.org/text/bugs/999700233,8118,.shtml>

INTER7 VPOPMAIL DB PW PROBLEM

The passwords to the MySQL server get compiled into libvpopmail.a which is where they belong for various reasons, which basically means that one can get them out of there rather easily (a short description for FreeBSD 4.3/gcc 2.95.2 is below). Now since all the command line utilities link against libvpopmail.a, they all contain the passwords too. This means that there's absolutely no need to write some code that will segfault as all binaries are chmod 755 which means that every user can read their contents, including the passwords.

Link: <http://www.net-security.org/text/bugs/999700598,71907,.shtml>

DOS VULNERABILITY IN MARCONI ATM SWITCH SOFTWARE

Marconi ATM switches can be configured with IP addresses for remote administration via telnet and web interfaces. There is a bug that can be used to deny telnet access to the switch, the web interface does not appear vulnerable and console management is unaffected.

Link: <http://www.net-security.org/text/bugs/999700653,12510,.shtml>

PGPSDK KEY VALIDITY VULNERABILITY

A vulnerability in PGP's display of key validity has been discovered that could allow an attacker to fool users into thinking that a valid signature was created by what is actually an invalid user ID. If the attacker can obtain a signature on their key from a trusted third party, they can then add a second user ID to their key which is unsigned. The attacker must then switch the unsigned false user ID to primary and convince the victim to place the key on their keyring. In such a case, some of the displays in PGP do not properly identify the false user ID as invalid because the second user ID is fully valid. Whenever PGP displays validity information on a per-user ID basis, the display is correct. Thus, attentive users who examine the user IDs of all public keys which they import to their keyrings will immediately notice this problem before it could have any impact.

Link: <http://www.net-security.org/text/bugs/999700718,79605,.shtml>

BALTIMORE WEBSWEEPER URL FILTERING PROBLEMS

WEBSweeper is Baltimore Technologies' Web Content Security solution. It enables customers to implement Content Security policies on Web, HTTP and passive FTP transfers.

Link: <http://www.net-security.org/text/bugs/999802392,96044,.shtml>

SHOPPLUS CART VULNERABILITY

Script doesn't check symbols. any user can execute commands on webserver.

Link: <http://www.net-security.org/text/bugs/999802456,39913,.shtml>

PAM LIMITS DROPS PRIVILEGES

If there are any limits set for a group of users then those users, logging in by any method using /bin/login (console login, telnet, etc) can get privileges of the last user last logged in via ssh (we're using openssh).

Link: <http://www.net-security.org/text/bugs/999802514,44684,.shtml>

CISCO SECURE IDS SIGNATURE OBFUSCATION VULNERABILITY

Intrusion Detection Systems inspect network traffic for suspect or malicious packet formats, data payloads and traffic patterns. Intrusion detection systems typically implement obfuscation defense - ensuring that suspect

packets cannot easily be disguised with UTF and/or hex encoding and bypass the Intrusion Detection systems. Recently, the CodeRed worm has targeted an unpatched vulnerability with many MicroSoft IIS systems and also highlighted a different encoding technique supported by MicroSoft IIS systems.

Link: <http://www.net-security.org/text/bugs/999802650,45838,.shtml>

CONNECTIVA LINUX - REMOTE VULNERABILITY IN FETCHMAIL

Fetchmail is a program used to retrieve email from POP and IMAP servers. Salvatore Sanfilippo did an audit and found a remote vulnerability in fetchmail that allows a remote attacker to write arbitrary data into memory. To take advantage of this problem, an attacker has to have control over the mail server being queried by the fetchmail process.

Link: <http://www.net-security.org/text/bugs/999802831,84903,.shtml>

GNUTELLA BUILT-IN DENIAL OF SERVICE

Once on the network, the Gnutella client connects to other hosts running Gnutella and starts exchanging lists of "up" hosts and search queries. This (at least on my machine) creates about 5-45k worth of background noise while the client is running. Additional bandwidth gets consumed when the user downloads files from someone else or vice versa.

Link: <http://www.net-security.org/text/bugs/999803569,38869,.shtml>

CONNECTIVA LINUX - MAILMAN SECURITY PROBLEMS

This update fixes two security problems and some other issues not related to security.

Link: <http://www.net-security.org/text/bugs/999802925,50506,.shtml>

CERT - BUFFER OVERFLOW IN GAUNTLET FIREWALL

The buffer overflow occurs in the smap/smmapd and CSMAP daemons. According to PGP Security, these daemons are responsible for handling email transactions for both inbound and outbound email.

Link: <http://www.net-security.org/text/bugs/999866049,6168,.shtml>

OUTLOOK WEB ACCESS INFORMATION DISCLOSURE

Among the functions Outlook Web Access (OWA) in Exchange 5.5 offers is the ability to search the global address list (GAL). By design, this is an authenticated function, implemented as a two-tier architecture - a front tier that provides a user interface and a back-end tier that actually performs the search. However, only the front tier actually checks authentication. An attacker who sent a properly formatted request to the back-end function that actually performs the search could enumerate the GAL without authenticating.

Link: <http://www.net-security.org/text/bugs/999866147,65491,.shtml>

NETBSD SENDMAIL(8) LOCAL ROOT COMPROMISE

Certain variables were treated as signed values, but should have been unsigned. Bounds checking was not done when incrementing an index. Combined with supplied command-line arguments, a local user could exploit the setuid-root sendmail binary and the lack of bounds checking to perform a root compromise.

Link: <http://www.net-security.org/text/bugs/999866995,77974,.shtml>

SHOPPING CART VERSION 1.23 VULNERABILITY

User can execute command, but can't use "../"

Link: <http://www.net-security.org/text/bugs/999961805,34399,.shtml>

BUG IN OLDER CHECKPOINT FIREWALLS

When a Firewall Policy is compiled, Firewall compilation creates a temporary file in /tmp with the policy name and ".cpp" appended to it. The access mode of the file is rw-rw-rw- (666). A user can elevate their access levels by exploiting this knowledge.

Link: <http://www.net-security.org/text/bugs/999962058,74409,.shtml>

=====

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>

The site has been updated in various areas: a new database, a new layout and we removed the advertisement banners making the site faster to load.

=====

Security world

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

CITADEL PROVIDES DEFENSE AGAINST INVALIDSSL WORM - [03.09.2001]

CT Holdings, Inc., which develops and markets the Citadel Technology line of network security and privacy software, provides the first line of defense against Win32.Invalid.A@mm, a new virus identified and reported in InfoWorld.com. The virus, circulating in disguise as a warning from Microsoft, encrypts executable files, rendering them unusable. Citadel Technology's SecurePC software includes features that enable security administrators to harden system files to prevent changes by anyone - or any program - without authorization.

Press release:

< <http://www.net-security.org/text/press/999528704,52054,.shtml> >

PIRT SECURITY SUITE TO BE EXHIBITED - [03.09.2001]

The Cyber Group Network, Inc. announced that CenDyne, Inc. has made them their exhibiting partner for Retail Vision. This premier invitation-only event, gives

The Cyber Group the opportunity to show their new PIRT Security Suite to more than 200 OEM and Retail decision makers. Last week, the companies formed an exclusive worldwide alliance to have CenDyne, Inc. market the new PIRT Security Suite software.

Press release:

< <http://www.net-security.org/text/press/999552760,98597,.shtml> >

BIOMETRICS SOLUTIONS FOR HIPAA SECURITY - [04.09.2001]

Keyware and HosplTech Solutions announced Tuesday that they have formed a strategic alliance to assist healthcare organizations comply with security standards mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), through the use of biometric technologies.

Press release:

< <http://www.net-security.org/text/press/999611523,72744,.shtml> >

CUBIC'S EMBEDDED NETWORK ENCRYPTION TECHNOLOGY - [04.09.2001]

Cubic Solutions, Samsung's System LSI business division, announces the availability of SafeNet, Inc.'s SecureIP embedded network encryption technology on SOC, ASIC and in Samsung-branded Application Specific Standard Products. The SecureIP encryption engine, licensed from SafeNet, Inc., provides hardware-based cryptographic acceleration for Virtual Private Networks, major network infrastructure, broadband security, and network security for the next generation of wireless devices including personal digital assistants, phones and pagers.

Press release:

< <http://www.net-security.org/text/press/999611613,33959,.shtml> >

CISCO EXTENDS AND ENHANCES SAFE SECURITY BLUEPRINT - [04.09.2001]

Continuing to expand its technical and market leadership by delivering practical security and VPN innovations for real-world business demands, Cisco Systems, Inc. today announced a series of rich solutions to enhance and extend its SAFE security blueprint. These include the introduction of the Cisco PIX 501 Firewall for small office/home office environments, and the Cisco IDS Host Sensor, a new host-based intrusion detection solution protecting critical server resources.

Press release:

< <http://www.net-security.org/text/press/999611701,49750,.shtml> >

NORTON ANTIVIRUS 2002 DESIGNED FOR WINDOWS XP - [04.09.2001]

Symantec Corp., a world leader in Internet security, announced that Norton AntiVirus 2002 is the world's first anti-virus solution to earn the Designed for

Windows XP logo from Microsoft. The Designed for Windows XP logo assures consumers that Norton AntiVirus has passed a rigorous set of certification requirements and has proven to provide an optimal experience for users of Microsoft's newest operating system.

Press release:

< <http://www.net-security.org/text/press/999611750,88691,.shtml> >

CISCO ANNOUNCES PIX 501 FIREWALL FOR SOHO - [04.09.2001]

Cisco Systems, Inc., the worldwide leader in networking for the Internet, announced that it is extending its market-leading enterprise-class Cisco PIX Firewall technology to small office and telecommuter network environments.

Press release:

< <http://www.net-security.org/text/press/999611790,11202,.shtml> >

CISCO IDS HOST SENSOR ANNOUNCED - [04.09.2001]

Cisco Systems, Inc., the worldwide leader in networking for the Internet, announced it is expanding its already rich portfolio of intrusion protection offerings with the introduction of the Cisco IDS Host Sensor, a host-based solution for enterprise-wide intrusion protection, and enhancements to its market-leading network-based IDS software.

Press release:

< <http://www.net-security.org/text/press/999611845,88528,.shtml> >

MAGISTR WORMV MAKES GRAND RETURN - [04.09.2001]

Kaspersky Labs warns users about the detection of the new variant of the dangerous "Magistr" virus. Kaspersky Labs has already received several reports regarding infection in Spain by this malicious program. "In 'Magistr.b,' a substantially reworked encoding algorithm of the virus' code is utilized. Because of this, none of the known anti-virus scanners are able to recognize this new virus variant even with the heuristic code analyzer switched on," commented Eugene Kaspersky, Head of Anti-Virus Research at Kaspersky Labs.

Press release:

< <http://www.net-security.org/text/press/999613132,62790,.shtml> >

EVIDIAN ANNOUNCES SUPPORT FOR NOVELL'S EDIRECTORY - [04.09.2001]

Evidian, the leading supplier of secure e-infrastructure management software; and Novell, the leading provider of Net services software; announced that interoperability has been achieved among Novell's eDirectory and Evidian's security products, PortalXpert™ and AccessMaster™. Through this agreement, which broadens the companies' existing partnership, Evidian

joins Novell's growing list of security partners and Novell becomes an Associate Partner of Evidian.

Press release:

< <http://www.net-security.org/text/press/999617985,4549,.shtml> >

QUALYS PROTECTS AGAINST NEW LINUX BACKDOOR TROJAN - [05.09.2001]

Qualys, Inc., a leading provider of enterprise network vulnerability assessment and monitoring solutions, announced that its QualysGuard online vulnerability scanning service is the first scanning solution capable of detecting the presence of a potentially dangerous new Linux backdoor Trojan identified as the Remote Shell Trojan. This Trojan consists of two primary components - a virus-like self replication capability, and the ability to install a backdoor process to enable remote attacks on the infected system. Qualys is making available a free downloadable tool to probe for the trojan's presence on a Linux machine along with a free downloadable fix to cleanse infected files.

Press release:

< <http://www.net-security.org/text/press/999700049,72695,.shtml> >

LARA WORM SPREADING IN DESKTOP THEMES FILES - [05.09.2001]

Kaspersky Labs, an international data-security software developer, announces the detection of the Internet worm "Lara": the first malicious program that spreads in Desktop Themes files. At the moment, Kaspersky Labs has received two reports of infections by this worm.

Press release:

< <http://www.net-security.org/text/press/999700148,85565,.shtml> >

WATCHGUARD APPOINTS NEW VP OF EMEA SALES - [05.09.2001]

WatchGuard Technologies, Inc., a leader in Internet security solutions, announced the appointment of Jeremy Butt to WatchGuard's management team as Vice President of EMEA (Europe, Middle East and Africa) Sales. "Jeremy brings a deep understanding of EMEA markets to WatchGuard, and we look forward to him complimenting our strong sales teams in those markets," said Jim Cady, President and COO of WatchGuard. "His strong IT experience and demonstrated management skills are an excellent fit for the requirements of this growing market."

Press release:

< <http://www.net-security.org/text/press/999702593,95315,.shtml> >

RAINBOW DEBUTS CRYPTOSWIFT HSM 200 - [05.09.2001]

Rainbow eSecurity, a Rainbow Technologies company and a leading provider of high-performance network security solutions for the Internet and eCommerce, announced the availability of the new CryptoSwift HSM 200 eCommerce

accelerator. The CryptoSwift HSM 200 was developed for high-assurance business, banking and financial services environments that require the highest levels of security and Web server performance. The CryptoSwift HSM (Hardware Security Module) has been certified for the National Institute of Standards and Technology (NIST) for the Federal Information Processing Standard (FIPS 140-1 Level 3). The iKey 2032 obtained FIPS 140-1 Level 2 certification in August, giving Rainbow a powerful client/server high-assurance security solution.

Press release:

< <http://www.net-security.org/text/press/999702655,47415,.shtml> >

TREND MICRO - PATENT FOR ACTIVE CONTENT SECURITY TECH - [06.09.2001]

Trend Micro Inc., a leader in antivirus and Internet content security solutions, announced that the U.S. Patent and Trademark Office has awarded it Patent No. 6,272,641 for technology which manages the security risks of "applications" received through the Web, including Java applets and Active X controls. The multi-tiered process involves server-based scanning and malicious code filtering at the Internet gateway, followed when necessary by real-time behaviour analysis at the client browser. In that final step, a suspect application is wrapped in security monitoring code, which causes it to terminate immediately upon any forbidden behaviour.

Press release:

< <http://www.net-security.org/text/press/999802226,67215,.shtml> >

QWEST OFFERS "LONG-TERM" FIX TO CODE RED - [06.09.2001]

DSL subscribers whose service was knocked out by the Code Red family of worms now have access to software designed to protect Cisco routers from the pesky invaders. But users won't be credited for lost service because a "criminal act" caused a non-Qwest product to go haywire, the company said. "Cisco has made a long-term solution available for affected customers who use either the Cisco 675 or 678 modem," Qwest Communications said in an e-mail to its DSL (digital subscriber line) customers.

Press release:

< <http://www.net-security.org/text/press/999805007,93617,.shtml> >

BRYAN CAVE LLP TO PROVIDE ZIXMAIL SECURE SERVICES - [06.09.2001]

ZixIt Corp., a leading provider of products and services that bring privacy, security, and convenience to Internet communications, announced that it is implementing its ZixMail secure email service at Bryan Cave LLP, a leader among corporate, transactional, and litigation law firms with a diversified national and international practice.

Press release:

< <http://www.net-security.org/text/press/999805072,93556,.shtml> >

IBM SAYS SOME OF YOUR CO-WORKERS COULD BE HACKERS - [06.09.2001]

Computer hackers come in many shades - extortion artists, corporate saboteurs, determined teenagers and legitimate IT professionals. But according to security experts at International Business Machines Corp , they have one thing in common: every office has at least one. Seizing upon the timely topic of Internet security risks, IBM this week has launched a global advertising and public relations initiative to plug its e-business security software and consulting expertise.

Press release:

< <http://www.net-security.org/text/press/999805112,81878,.shtml> >

LOKBOX SOFTWARE RELEASES INTERNETPERISCOPE - [06.09.2001]

LokBox Software of San Francisco announced the release of InternetPeriscope, its multi-purpose internet server monitoring and auditing software. Internet Periscope includes a wide array of features and tools that will be most useful to System Administrators of small and large networks of internet servers. Along with its many useful monitoring tools the product also includes several intrusion detection devices that will greatly assist the administrator in managing intrusion prevention and tracking as well as hacker detection and identification.

Press release:

< <http://www.net-security.org/text/press/999805171,32896,.shtml> >

SECURITYEXPRESSIONS 2.0 FOR UNIX AND SOLARIS - [06.09.2001]

SecurityExpressions, which one reviewer called a "powerful, user friendly tool for closing security loopholes", has helped organizations with large-scale systems lockdown and reduced systems administration costs by automating the process of deploying, assessing, and maintaining consistent security policies for Windows NT and 2000 systems. Now, 2.0 will support UNIX and Solaris operating systems as well.

Press release:

< <http://www.net-security.org/text/press/999805261,58568,.shtml> >

MCAFFEE.COM WARNS OF W32/MAGISTR.B@MM VIRUS - [07.09.2001]

McAfee.com announced that it has received a serious number of reports from both South America and Europe of a virus that's been infecting users over the last 48 hours. This virus, named "W32/Magistr.b@mm," is a variant of "Magistr.a" and has been rated "medium risk" for corporate and home users due to the number of reports coming from the two continents. So far, the company has received relatively few reports coming from within the United States. McAfee.com has posted removal instructions for this virus on its Web site, available at www.mcafee.com. The company's virus detection and deletion services, Clinic and VirusScan Online, have also been updated to protect current subscribers to these services. Over 30% of McAfee.com's subscribers are outside the US.

Press release:

< <http://www.net-security.org/text/press/999864302,87858,.shtml> >

WATCHGUARD ANNOUNCES ITS WORMBUSTER SOLUTION - [07.09.2001]

WatchGuard Technologies, Inc., a leader in Internet security, announced new defense-in-depth solutions designed to protect enterprise networks and servers against damage from Internet worms, such as Code Red and its derivatives. The new Wormbuster solutions are designed for companies with Web sites running Microsoft IIS on Windows NT and Windows 2000 servers, and enable these customers to rapidly deploy comprehensive protection for their systems from a range of security threats at both the network perimeter and server level.

Press release:

< <http://www.net-security.org/text/press/999865439,82713,.shtml> >

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

NTSEC SECURITY TOOLS

Manipulate and view file and directory access control lists, registry security, and network printer and disk shares. These programs provide a method for scripting and nondestructively changing permissions and auditing settings, as well as users, group, rights and policies.

Read more:

< <http://www.security-db.com/product.php?id=930> >

This is a product of Pedestal Software, for more information:

< <http://www.security-db.com/company.php?id=224> >

PROCHECKNET

The ProCheckNet security network is unique, as it intelligently looks for security flaws. ProCheckNet uses Artificial Intelligence (AI) and a unique proprietary language to gather as much information as is possible about your systems, and then uses attacks specific to the information found to determine if any vulnerabilities exist. These vulnerabilities are further exploited, using the attack

strategies stored on its knowledgebase to discover more vulnerabilities. The knowledgebase is updated daily with the latest exploits discovered by our research team, currently we hold over 1,000 exploits on our knowledgebase.

Read more:

< <http://www.security-db.com/product.php?id=932> >

This is a product of ProCheckUp, for more information:

< <http://www.security-db.com/company.php?id=226> >

BIOWEB

BioWeb secures websites through the use of biometric technology! You can easily implement this with just a few minutes work.

Where can I use it?

BioWeb is best suited for web environments where you can determine the hardware configuration at each client's machine. This is because a biometric scanning device is required on the client side.

Read more:

< <http://www.security-db.com/product.php?id=964> >

This is a product of Biometrics.co.za, for more information:

< <http://www.security-db.com/company.php?id=230> >

Featured article

All articles are located at:

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

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

THE FIRST STEP OF EXPLORING A SYSTEM

The first step to exploring a system is not just another point and click. It is the part that suprisingly, no one really talks about; gathering information on the subject. In order to successfully get in a system, one must know enough about the entity to gain access to it. This can be acomplished by choosing a subject (network/computer) and learning all there is to know about how it ticks. This information can be found a number of ways; the main ones being searching the Internet, discovering the networks behind the domains, finding locations and phone numbers, and finding a path in.

Read more:

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

Security Software

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

GHOST PORT SCAN 0.7.0

The aim of Ghost Port Scan is to provide administrators and pen-testers with a tool that allow them to easily test firewalls and get information from a remote host. GPS is a port scanner and a firewall rules disclosure (FWRD) tool, which uses IP spoofing, ARP poisoning and some other stratagems in order to perform a stealth and untrackable information collect.

Info/Download:

< <http://www.net-security.org/various/software/999557263,80083,linux.shtml> >

BLAIM 0.2.975

Blaim is a plugin for GAIM, a 448-bit blowfish encryption package highlighted by a nice Diffie-Hellman key exchange protocol.

Info/Download:

< <http://www.net-security.org/various/software/999557866,55540,linux.shtml> >

DEVIL-LINUX V0.44

Devil-Linux is a special Linux distribution, which is used for Firewalls / Routers. The goal of Devil-Linux is to have a small, customizable and secure (what is secure in the internet?) Linux.

Benefits:

- Boots from CD
- Configuration is saved on a floppy disk
- No need for a harddisk
- Support for Intel 486 and higher
- Runs with 32MB RAM
- uses Standard Kernel 2.4.x
- Glibc 2.2.x
- IPTables Support

Info/Download:

< <http://www.net-security.org/various/software/999567299,58004,linux.shtml> >

BABELWEB 1.0

Babelweb is a program which allows to automate tests on a HTTP server. It is able to follow the links and the HTTP redirect but it is programmed to remain on the original server. The main goal of babelweb is to obtain informations

about a remote web server and to sort these informations. It is thus possible to draw up the list of the accessible pages, the cgi scripts met, the various files found like .zip, .pdf...

Info/Download:

< <http://www.net-security.org/various/software/999567602,47899,linux.shtml> >

LINK LOGGER 1.2

Link Logger is the premier Windows logging tool for the Linksys BEF family of Routers. Link Logger allows you to know what is happening at your Linksys for both incoming and outgoing traffic. Link Logger features alerts for suspicious traffic both coming into your network and leaving. You can even custom configure alarms to let you know the instant that traffic occurs involving an IP address or Port number.

Info/Download:

< <http://www.net-security.org/various/software/999568338,87738,windows.shtml> >

IDSCENTER 1.08D

IDScenter is a GUI for Snort IDS on Win32 systems.

Features of IDScenter are:

Snort 1.7 and Snort 1.6 support, integration in taskbar (tray-icon), immediate autorestart of Snort if it was killed (TaskManager, Ctrl-Break... or unusual exits...), IP/Interface detection, audio alert (WAV) / beep alerts, execution of other programs on alerts (e.x. net send...), integrated log viewer (arachNIDS/Aris query, seach function, cursor position at end of log), "Test configuration" button, e-mail alert, download link for new rulesets, support for external viewers/editors (ACID/SnortSnarf/WinSnort2HTML and others), process priority option...

Info/Download:

< <http://www.net-security.org/various/software/999568595,68622,windows.shtml> >

IPTRAF 2.5.0

IPTraf is a console-based network statistics utility for Linux. It gathers a variety of figures such as TCP connection packet and byte counts, interface statistics and activity indicators, TCP/UDP traffic breakdowns, and LAN station packet and byte counts.

Info/Download:

< <http://www.net-security.org/various/software/999569128,13775,linux.shtml> >

MEDUSA DS9 V.0.8.1

Medusa is a package that improves the overall security of the Linux OS by extending the standard Linux (Unix) security architecture while preserving backward compatibility. Briefly, it supports, at the kernel level, a user-space authorization server (and is thus fully transparent to any user space applications). Before the execution of certain operations, the kernel asks the authorization server for confirmation. The authorization server then permits or forbids the operation. The authorization server can also affect the way an operation is executed in some cases, which are described later. This method allows the use of almost any security architecture. When the authorization server is properly configured, it can determine access rights within the system to a very fine level and do very good auditing.

Info/Download:

< <http://www.net-security.org/various/software/999569499,38706,linux.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>
=====

Questions, contributions, comments or ideas go to:

Help Net Security staff

staff@net-security.org
<http://net-security.org>
<http://security-db.com>