

HNS Newsletter
Issue 274 - 18.07.2005.
<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.

InfoSec Research Library - <http://net-security.bitpipe.com>

In association with BitPipe, Help Net Security is giving you a possibility to freely read the latest white papers, case studies, webcasts and product information related to information security.

Some of the topics covered include: Authentication, Email Security, Identity Management, Network Security, Security Policies. VPN and Wireless Security.

Point your browsers to: <http://net-security.bitpipe.com>

Table of contents:

- 1) Security news
- 2) Vulnerabilities
- 3) Advisories
- 4) Articles
- 5) Software
- 6) Webcasts
- 7) Conferences
- 8) Security World
- 9) Virus News

[Security news]

TROJAN EXPLOITS LONDON BOMBINGS
Promised eyewitness video's carries a payload of its own
<http://www.net-security.org/news.php?id=8244>

APACHE FACES WEB SERVICES SECURITY SPEC ROADBLOCK

Open source organization to meet with Microsoft, IBM.

<http://www.net-security.org/news.php?id=8245>

PUNISHMENT INCONSISTENT FOR CONVICTED HACKERS

These cases involving hackers and purveyors of viruses are scaring off individuals from using the Internet.

<http://www.net-security.org/news.php?id=8246>

MICROSOFT TO REWARD INFORMANTS AFTER SASSER CONVICTION

Microsoft plans to split the \$250,000 reward for the information leading to the Sasser author between two tipsters.

<http://www.net-security.org/news.php?id=8247>

VENDORS TOUT WLAN SECURITY ADVANCES

Two wireless LAN security vendors last week separately announced streamlined versions of their software.

<http://www.net-security.org/news.php?id=8248>

WRITING LINUX FIREWALL RULES WITH IPTABLES

This guide will give you some background on IPTables and how to use it to secure your network.

<http://www.net-security.org/news.php?id=8249>

WHO OWNS THE INFORMATION?

From the music you purchase and download to your personal details stored online, it's all just bits of information.

<http://www.net-security.org/news.php?id=8250>

SARBANES-OXLEY LEGISLATION CRITICISED

Influential US judge and one of the legislation's architects, Michael Oxley, highlight its faults.

<http://www.net-security.org/news.php?id=8251>

TO CATCH AN ID THIEF

Bank-sponsored Identity Theft Assistance Center will share information with the FTC to help catch identity thieves.

<http://www.net-security.org/news.php?id=8252>

PENETRATION TESTING: TAKING THE GUESSWORK OUT OF VULNERABILITY MANAGEMENT

Despite the ongoing investment in information security, sensitive customer information and intellectual property continue to be compromised, this paper focuses on the best practices that will enable organizations to secure this information.

<http://www.net-security.org/news.php?id=8253>

FEDS FEAR AIR BROADBAND TERROR

Law enforcement officials want to eavesdrop on air passengers' internet use with a court order. The federal agencies are concerned that terror attacks could be coordinated using new in-flight broadband connections.

<http://www.net-security.org/news.php?id=8254>

RISKS AND THREATS TO STORAGE AREA NETWORKS

The foundation of enterprise risk analysis is the threat model which defines the points of attack and the methods of attack at each point. This paper investigates risk and common security threats against storage area networks (SANs) and the countermeasures that can be taken to mitigate the vulnerability of the enterprise SAN.

<http://www.net-security.org/news.php?id=8255>

SECURITY: KNOW YOUR RISKS

Speed is vital to assess and manage swiftly changing risks and meet regulatory demands. A matrix-based approach can offer a faster route than traditional, bottom-up methods.

<http://www.net-security.org/news.php?id=8256>

AIRMAGNET BINDS CISCO KIT INTO WI-FI SECURITY

Wi-Fi security vendor AirMagnet has increased the support for Cisco access points in AirMagnet Enterprise 6, as well as adding multi-tasking sensors, making set-up easier and adding intelligence to spot new attacks.

<http://www.net-security.org/news.php?id=8257>

IDS PAYS OFF, EVEN IF THERE'S NO HACKING

When I came into work after the weekend, a very interesting e-mail

message was waiting for me. The message, with the subject line "Account Alert," appeared to be from our help desk. It requested that I read an attached document pertaining to my user account.
<http://www.net-security.org/news.php?id=8258>

HAS MICROSOFT MADE SECURITY STRIDES?

Two years after Microsoft CEO Steve Ballmer announced a corporate-wide focus on security, Microsoft claimed that the company is fulfilling its promise.
<http://www.net-security.org/news.php?id=8259>

INTRODUCTION TO IPAUDIT

IPAudit is a handy tool that will allow you to analyze all packets entering and leaving your network.
<http://www.net-security.org/news.php?id=8260>

LONGHORN FOLLOWING UNIX ON SECURITY?

Microsoft's delayed Longhorn operating system appears to be taking a page from the Unix management book by curbing user's administration rights.
<http://www.net-security.org/news.php?id=8261>

SECURITY BREACH - THE PRICE IS RIGHT

How much does a security breach actually "cost," and who pays for it?
<http://www.net-security.org/news.php?id=8262>

WHEN MANAGEMENT SETS THE WRONG SECURITY CULTURE

During a recent tele-banking transaction, I was instructed to enter my bank account and Social Security numbers.
<http://www.net-security.org/news.php?id=8263>

DOM BASED CROSS SITE SCRIPTING OR XSS OF THE THIRD KIND

Application developers and owners need to understand DOM Based XSS, as it represents a threat to the web application, which has different preconditions than standard XSS.
<http://www.net-security.org/news.php?id=8264>

USERS ACT TO ENCRYPT MOBILE DATA

Concerns linger about untested handheld tools.

<http://www.net-security.org/news.php?id=8265>

SECURITY PRODUCT LETS ONLY GOOD CODE RUN

Why try and prevent every potential security threat when you can just direct the network to run nothing but authorized code?

<http://www.net-security.org/news.php?id=8266>

SPAMMERS MOST LIKELY USERS OF E-MAIL AUTHENTICATION

Spammers are continuing to adopt Sender ID and Sender Policy Framework, two of the prominent e-mail authentication schemes that are actually intended to stop spam.

<http://www.net-security.org/news.php?id=8267>

FIRMS IGNORANT OF HACKER RISK

Most IT managers admit they have no way of measuring risk.

<http://www.net-security.org/news.php?id=8268>

SARBOX CHALLENGE DRAINS SECURITY BUDGETS

International corporate spending on compliance with the Sarbanes-Oxley data security legislation has come at the expense of dealing with other security threats, according to the Information Security Forum (ISF).

<http://www.net-security.org/news.php?id=8269>

GIVING NEW MEANING TO 'SPYWARE'

Supreme Court Justice Potter Stewart famously said that he couldn't define obscenity, but that he knew it when he saw it.

<http://www.net-security.org/news.php?id=8270>

HOT SKILLS: NETWORK SECURITY

Security systems are becoming easier to set up, but they need skilled staff to configure and maintain them.

<http://www.net-security.org/news.php?id=8271>

SOPHOS GLITCH LEAVES PCS HANGING

A recent security update from Microsoft is tripping up users of Sophos's flagship anti-virus scanning software.

<http://www.net-security.org/news.php?id=8272>

HACKERS GROW ARMIES OF ZOMBIE PCS

Number of systems infected with malicious software has jumped more than 300 percent, McAfee says.

<http://www.net-security.org/news.php?id=8273>

ONLY 10 PER CENT OF EMAILS ARE GENUINE

Just 10 per cent of all email is a genuine message, with the volume of spam email, phishing attacks, trojans and virus-infected email messages rising 600 per cent in the past year.

<http://www.net-security.org/news.php?id=8274>

HOW DO COMPLIANCE ISSUES AFFECT YOUR NETWORK?

This article looks at how regulations affecting specific industries impact the computer networks of companies in those industries, as well as some of the common myths and misconceptions about various compliance requirements.

<http://www.net-security.org/news.php?id=8275>

UK EU PRESIDENCY AIMS FOR EUROPE-WIDE BIOMETRIC ID CARD

The UK is using its Presidency of the Council of the European Union to push for the adoption of biometric ID cards and associated standards across the whole of the EU.

<http://www.net-security.org/news.php?id=8276>

HACKERS ALREADY EXPLOITING XP FLAWS

Latest patches more critical than ever, warns Microsoft.

<http://www.net-security.org/news.php?id=8277>

PRIVACY GROUP: ONLINE INVESTIGATORS DIG UP TOO MANY SECRETS

The Electronic Privacy Information Center says online private eyes dig up unlisted phone numbers, addresses, detailed phone records, employment history, and motor vehicle data on private individuals, often using deceptive practices.

<http://www.net-security.org/news.php?id=8278>

PENALTY PLEA ON CYBER CRIMINALS

Tougher sentences are needed to make sure computer crime is treated seriously by courts and prosecutors, said an MP as he proposed new laws.

<http://www.net-security.org/news.php?id=8279>

DATA BREACHES: TURN BACK THE TIDE

The complexity of today's business-technology systems, the sorry state of software application security, the general lack of employee IT-security awareness, and the growing "connectedness" of partners and customers all work against the task of security managers to protect critical business information.

<http://www.net-security.org/news.php?id=8280>

WORD BUG SHOWS TREND IN FILE FORMAT HACKS

The vulnerability in Microsoft Word is only the latest in a spreading trend that's seeing hackers probe for foibles and failings in file formats, a security firm says.

<http://www.net-security.org/news.php?id=8281>

APPLE PEELS WRAPS OFF OSX SECURITY PATCHES

Denial of service attack hole and file overwrite bug fixed.

<http://www.net-security.org/news.php?id=8282>

WHAT IS ENDPOINT SECURITY?

Endpoint security is something that many IT professionals think they have, though few can agree on what it is.

<http://www.net-security.org/news.php?id=8283>

HACKER TELLS OF BUNGLER THAT MAY HAVE COST \$1 MILLION

"You end up lusting after more and more complex security measures," the unemployed systems administrator said. "It was like a game. It was addictive. Hugely addictive."

<http://www.net-security.org/news.php?id=8284>

USERS FLOCK TO SPAM MESSAGES

11 per cent admits to buying Viagra and other goods advertised in spam.

<http://www.net-security.org/news.php?id=8285>

COULD BLOGGING SPREAD COMPUTER WORMS?

Could RSS feeds become a conduit for the transmission of computer worms? Security experts are at odds over the possibility.

<http://www.net-security.org/news.php?id=8286>

ZOMBIEALERT SCOURS NETWORKS FOR SPAM-SPEWING PCS

Sophos is touting a new service that scours corporate networks for zombies -- PCs that have been hijacked without the owner's knowledge and turned into spam-spewing engines.

<http://www.net-security.org/news.php?id=8287>

BANK OF AMERICA ADDS NEW ONLINE SECURITY

Stung by recent high-profile security breaches, Bank of America Corp. is rolling out a new online banking security system aimed at making it harder for cyberthieves to crack customer accounts.

<http://www.net-security.org/news.php?id=8288>

SIX RULES FOR ENCRYPTING YOUR ENTERPRISE DATA

Regulatory compliance requirements for protecting sensitive data have led many companies to consider encryption. This document provides six fundamental rules that should be considered prior to data encryption deployment.

<http://www.net-security.org/news.php?id=8289>

SUN TO EXPAND OPEN SOURCE MOVES INTO SECURE ID ARENA

Java developers are encouraged to write apps featuring identity management.

<http://www.net-security.org/news.php?id=8290>

ORACLE INTEGRATES WEB SERVICES, SECURITY PRODUCTS

Oracle plans to combine two of its Web services products to make it easier for developers to set security policies for applications built using its Oracle BPEL Process Manager software, a company executive said Tuesday.

<http://www.net-security.org/news.php?id=8291>

PERSONAL DATA QUIZ THROWS WRENCH INTO ID THEFT

Identity thieves and impersonators thrive on publicly available personal information and data pilfering.

<http://www.net-security.org/news.php?id=8292>

OPEN SOURCE VS. WINDOWS: SECURITY DEBATE RAGES ON

Open source is foremost an "ethos" that "is precisely the best social environment for the best development of anything," said Tim Clarke, I.T. director at Manifest, a maker of electronic voting and research tools.

<http://www.net-security.org/news.php?id=8293>

VERISIGN ACQUIRES SECURITY FIRM IDEFENSE FOR US\$40M

VeriSign announced Wednesday that it had purchased security intelligence firm iDefense for approximately US\$40m in cash.

<http://www.net-security.org/news.php?id=8294>

TROJANS TAKING OVER FROM WORMS

Worm activity fell last month by over 80 per cent.

<http://www.net-security.org/news.php?id=8295>

FIREFOX UPDATE FOCUSES ON SECURITY AND STABILITY

"Software sometimes can be the victim of its own success," said Cluley. Certainly, that is the case with Microsoft's Internet Explorer, which is the leader in the Web browser realm and thus sustains proportionately more malicious attacks.

<http://www.net-security.org/news.php?id=8296>

TREND MICRO BUG PROVES COSTLY

Faulty software update released earlier this year cost the company \$8 million.

<http://www.net-security.org/news.php?id=8297>

SPYWARE, A THORN IN MY SIDE

The scenario: You are doing research on the Web - which, by the way, is what a vast majority (more than 80%) of so-called surfers do " and you find a link that looks right on target.

<http://www.net-security.org/news.php?id=8298>

AN OPEN SOURCE APPROACH TO SECURITY

The perception that a Linux environment and open source software statistically has more vulnerabilities in comparison with other operating systems is only half true.

<http://www.net-security.org/news.php?id=8299>

CYBERCRIME RATES, LOSSES FALL, SURVEY SAYS

The downturn in losses is because of both better management of security tools and sheer luck in the form of a 12-month run without fast-spreading, big-dollar-amount attacks. But the survey also detailed some gloomier news: Losses to identity and information theft are up--way up.

<http://www.net-security.org/news.php?id=8300>

JUNIPER'S INFRANET INITIATIVE GETS BACKING OF CISCO

Juniper's Infranet initiative, designed to help service providers deliver security and quality-of-service guarantees across their boundaries, welcomed Cisco Systems to the group.

<http://www.net-security.org/news.php?id=8301>

[Vulnerabilities]

All vulnerabilities are located here:

<http://www.net-security.org/vulnerabilities.php>

Microsoft Windows Network Connections Service netman.dll Remote DoS

<http://www.net-security.org/vulnerability.php?id=17885>

SquirrelMail options_identities.php Variable Overwrite Privilege Escalation

<http://www.net-security.org/vulnerability.php?id=17874>

SunOS buglib.so sync Account Local Privilege Escalation

<http://www.net-security.org/vulnerability.php?id=17840>

SunOS Unpassworded sync Account Multiple Issues

<http://www.net-security.org/vulnerability.php?id=17839>

Affix btftp Client OBEX File Share Filename Overflow
<http://www.net-security.org/vulnerability.php?id=17852>

Affix btsrv Crafted Filename Arbitrary Shell Command Injection
<http://www.net-security.org/vulnerability.php?id=17853>

MailEnable IMAP STATUS Command Remote Overflow
<http://www.net-security.org/vulnerability.php?id=17844>

Microsoft Office .doc Font Parsing Overflow
<http://www.net-security.org/vulnerability.php?id=17829>

Microsoft Windows Color Management Module ICC Profile Format Tag
Remote Overflow
<http://www.net-security.org/vulnerability.php?id=17830>

Blog Torrent newusers User Credential Disclosure
<http://www.net-security.org/vulnerability.php?id=17832>

Squito Gallery photolist.inc.php photoroot Variable Remote File
Inclusion
<http://www.net-security.org/vulnerability.php?id=17835>

PPA functions.inc.php config[ppa_root_path] Variable Remote File
Inclusion
<http://www.net-security.org/vulnerability.php?id=17836>

PHP shtool Symlink Arbitrary File Overwrite
<http://www.net-security.org/vulnerability.php?id=17808>

OpenLDAP shtool Symlink Arbitrary File Overwrite
<http://www.net-security.org/vulnerability.php?id=17804>

OpenPKG shtool Symlink Arbitrary File Overwrite
<http://www.net-security.org/vulnerability.php?id=17802>

Id Board sql.cls.php tbl_suff Variable SQL Injection
<http://www.net-security.org/vulnerability.php?id=17811>

DownloadProtect download.php file Variable Traversal Arbitrary File
Access
<http://www.net-security.org/vulnerability.php?id=17806>

[Advisories]

All advisories are located at:
http://www.net-security.org/archive_advi.php

Fedora Legacy Update Advisory - Updated PostgreSQL packages fix
security issues (FLSA:152844)
<http://www.net-security.org/advisory.php?id=5039>

Fedora Legacy Update Advisory - Updated squirrelmail package fixes
security issue (FLSA:152900)
<http://www.net-security.org/advisory.php?id=5038>

Fedora Legacy Update Advisory - Updated kdelibs/kdebase packages fix
security issues (FLSA:152769)
<http://www.net-security.org/advisory.php?id=5037>

Fedora Legacy Update Advisory - Updated gd packages fix security
issues (FLSA:152838)
<http://www.net-security.org/advisory.php?id=5036>

Fedora Legacy Update Advisory - Updated openssl packages fix security
issues (FLSA:152841)
<http://www.net-security.org/advisory.php?id=5035>

Fedora Legacy Update Advisory - Updated samba packages fix security issues (FLSA:152874)
<http://www.net-security.org/advisory.php?id=5034>

Fedora Legacy Update Advisory - Updated cpio package fixes security issue (FLSA:152891)
<http://www.net-security.org/advisory.php?id=5033>

Fedora Legacy Update Advisory - Updated curl packages fix a security issue (FLSA:152917)
<http://www.net-security.org/advisory.php?id=5032>

Fedora Legacy Update Advisory - Updated mysql packages fix security issues (FLSA:152925)
<http://www.net-security.org/advisory.php?id=5031>

Fedora Legacy Update Advisory - Updated gdk-pixbuf packages fix a security issue (FLSA:154272)
<http://www.net-security.org/advisory.php?id=5030>

Fedora Legacy Update Advisory - Updated mozilla packages fix security issues (FLSA:158149)
<http://www.net-security.org/advisory.php?id=5029>

SUSE Security Announcement - SUSE-SA:2005:042 (acoread 5)
<http://www.net-security.org/advisory.php?id=5028>

Slackware Security Advisory - XV (SSA:2005-195-02)
<http://www.net-security.org/advisory.php?id=5027>

Slackware Security Advisory - tcpdump DoS (SSA:2005-195-10)
<http://www.net-security.org/advisory.php?id=5026>

Conectiva Linux Security Announcement - php4 (CLA-2005:980)
<http://www.net-security.org/advisory.php?id=5025>

Trustix Secure Linux Security Advisory - kerberos5, kernel, php4
(2005-0036)
<http://www.net-security.org/advisory.php?id=5024>

Mandriva Linux Security Update Advisory - mozilla-firefox
(MDKSA-2005:120v)
<http://www.net-security.org/advisory.php?id=5023>

Mandriva Linux Security Update Advisory - krb5 (MDKSA-2005:119)
<http://www.net-security.org/advisory.php?id=5022>

Debian Security Advisory - phpgroupware (DSA 746-1)
<http://www.net-security.org/advisory.php?id=5021>

US-CERT Technical Cyber Security Alert - Oracle Products Contain
Multiple Vulnerabilities (TA05-194A)
<http://www.net-security.org/advisory.php?id=5020>

Debian Security Advisory - squirrelmail (DSA 756-1)
<http://www.net-security.org/advisory.php?id=5019>

Cisco Security Advisory - Cisco Security Agent Vulnerable to Crafted
IP Attack
<http://www.net-security.org/advisory.php?id=5018>

Cisco Security Advisory - Cisco ONS 15216 OADM Telnet
Denial-of-Service
<http://www.net-security.org/advisory.php?id=5017>

Debian Security Advisory - tiff (DSA 755-1)
<http://www.net-security.org/advisory.php?id=5016>

Debian Security Advisory - centericq (754-1)
<http://www.net-security.org/advisory.php?id=5015>

SUSE Security Announcement - SUSE Security Summary Report
(SUSE-SR:2005:017)
<http://www.net-security.org/advisory.php?id=5014>

Turbolinux Security Announcement - Multiple vulnerabilities exist in
krb5 (13/Jul/2005)
<http://www.net-security.org/advisory.php?id=5013>

Microsoft Security Bulletin - Microsoft Security Bulletin Summary for
July 2005 (1.0)
<http://www.net-security.org/advisory.php?id=5012>

Mandriva Linux Security Update Advisory - ruby (MDKSA-2005:118)
<http://www.net-security.org/advisory.php?id=5011>

Mandriva Linux Security Update Advisory - dhcpcd (MDKSA-2005:117)
<http://www.net-security.org/advisory.php?id=5010>

US-CERT Technical Cyber Security Alert - Microsoft Windows, Internet
Explorer, and Word Vulnerabilities (TA05-193A)
<http://www.net-security.org/advisory.php?id=5009>

Fedora Legacy Update Advisory - Updated ImageMagick packages fix
security issues (FLSA:152777)
<http://www.net-security.org/advisory.php?id=5008>

MIT krb5 Security Advisory - double-free in krb5_recvauth
(2005-07-12)
<http://www.net-security.org/advisory.php?id=5007>

Cisco Security Advisory - buffer overflow, heap corruption in KDC (
2005-002)
<http://www.net-security.org/advisory.php?id=5006>

Cisco Security Advisory - Cisco CallManager Memory Handling
Vulnerabilities (1.0)

<http://www.net-security.org/advisory.php?id=5005>

Mandriva Linux Security Update Advisory - gedit (DSA 753-1)
<http://www.net-security.org/advisory.php?id=5004>

Mandriva Linux Security Update Advisory - cpio (MDKSA-2005:116)
<http://www.net-security.org/advisory.php?id=5003>

Slackware Security Advisory - PHP packages updated again for 8.1, 9.0, 9.1 (SSA:2005-192-02))
<http://www.net-security.org/advisory.php?id=5002>

Mandriva Linux Security Update Advisory - clamav (MDKSA-2005:113)
<http://www.net-security.org/advisory.php?id=5001>

Mandriva Linux Security Update Advisory - leafnode (MDKSA-2005:114)
<http://www.net-security.org/advisory.php?id=5000>

Mandriva Linux Security Update Advisory - mplayer (MDKSA-2005:115)
<http://www.net-security.org/advisory.php?id=4999>

Slackware Security Advisory - PHP (SSA:2005-192-01)
<http://www.net-security.org/advisory.php?id=4998>

Fedora Update Notification - Updated openssh packages fix a security issue (2005-07-11)
<http://www.net-security.org/advisory.php?id=4997>

Fedora Legacy Update Advisory - Updated telnet packages fix security issues (FLSA:152583)
<http://www.net-security.org/advisory.php?id=4996>

NetBSD Security Advisory - A zlib buffer overflow has been announced (20050708-1)
<http://www.net-security.org/advisory.php?id=4995>

Debian Security Advisory - gzip (DSA 752-1)
<http://www.net-security.org/advisory.php?id=4994>

Debian Security Advisory - squid (DSA 751-1)
<http://www.net-security.org/advisory.php?id=4993>

Debian Security Advisory - ruby1.8 (DSA 748-1)
<http://www.net-security.org/advisory.php?id=4992>

Debian Security Advisory - dhcpd (DSA 750-1)
<http://www.net-security.org/advisory.php?id=4991>

Turbolinux Security Announcement - zlib (11/Jul/2005)
<http://www.net-security.org/advisory.php?id=4990>

Fedora Legacy Update Advisory - Updated dhcp package fixes security issue (FLSA:152835)
<http://www.net-security.org/advisory.php?id=4989>

Fedora Legacy Update Advisory - Updated mailman package fixes security issue (FLSA:152895)
<http://www.net-security.org/advisory.php?id=4988>

Fedora Legacy Update Advisory - Updated gftp package fixes security issue (FLSA:152908)
<http://www.net-security.org/advisory.php?id=4987>

Fedora Legacy Update Advisory - Updated sharutils package fixes security issue (FLSA:154991)
<http://www.net-security.org/advisory.php?id=4986>

Fedora Legacy Update Advisory - Updated php packages fix security issues (FLSA:155505)
<http://www.net-security.org/advisory.php?id=4985>

Debian Security Advisory - ettercap (DSA 749-1)
<http://www.net-security.org/advisory.php?id=4984>

Debian Security Advisory - egroupware (DSA 747-1)
<http://www.net-security.org/advisory.php?id=4983>

[Articles]

All articles are located at:
http://www.net-security.org/articles_main.php

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

DATA BREACHES: TURN BACK THE TIDE

The complexity of today's business-technology systems, the sorry state of software application security, the general lack of employee IT-security awareness, and the growing "connectedness" of partners and customers all work against the task of security managers to protect critical business information.

<http://www.net-security.org/article.php?id=804>

RISKS AND THREATS TO STORAGE AREA NETWORKS

The foundation of enterprise risk analysis is the threat model which defines the points of attack and the methods of attack at each point. This paper investigates risk and common security threats against storage area networks (SANs) and the countermeasures that can be taken to mitigate the vulnerability of the enterprise SAN.

<http://www.net-security.org/article.php?id=803>

[Software]

Windows software is located at:
http://net-security.org/software_main.php?cat=1

Linux software is located at:
http://net-security.org/software_main.php?cat=2

Pocket PC software is located at:
http://net-security.org/software_main.php?cat=3

Mac OS X software is located at:
http://net-security.org/software_main.php?cat=5

ARPALERT 0.4.7 (Linux)

This software listens on a network interface (without using 'promiscuous' mode) and catches all conversations of MAC address to IP request.

<http://www.net-security.org/software.php?id=335>

CRYPTOCRAT 2005 4.60 (Windows)

This is a program for encrypting files with using strong Blowfish algorithm.

<http://www.net-security.org/software.php?id=28>

DANTE 1.1.17 (Linux)

Dante is a circuit-level firewall/proxy that can be used to provide convenient and secure network connectivity to a wide range of hosts.

<http://www.net-security.org/software.php?id=43>

IDS POLICY MANAGER 1.7.0 (Windows)

IDS Policy Manager is a Visual Basic application that was written to easily manage policies for multiple Snort sensors.

<http://www.net-security.org/software.php?id=5>

IP SENTINEL 0.12 (Linux)

This program tries to prevent unauthorized usage of IPs within the local ethernet broadcastdomain by giving an answer to ARP-requests.

<http://www.net-security.org/software.php?id=376>

JSCH 0.1.21 (Windows)

JSch is a pure Java implementation of SSH2.

<http://www.net-security.org/software.php?id=417>

KILLDISK 3.1 (Windows)

KillDisk is powerful and compact DOS software that allows you to destroy all data on hard and floppy drives completely, excluding any possibility of future recovery of deleted files and folders.

<http://www.net-security.org/software.php?id=371>

KMYFIREWALL 1.0 Beta 1 (Linux)

KMyFirewall is a Kde/Qt Programm that tries to provide an easy to use and comfortable GUI for the Linux 2.4 "iptables" command.

<http://www.net-security.org/software.php?id=137>

KNETFILTER 3.4.0 (Linux)

Knetfilter is a KDE application designed to manage the netfilter functionalities that come with kernel 2.4.x.

<http://www.net-security.org/software.php?id=130>

LINKSYSMON 1.1.4 (Linux)

linksysmon is a tool for monitoring Linksys BEFSR41 and BEFSR11 firewalls.

<http://www.net-security.org/software.php?id=194>

LINUX TRUSTEES 3.03 pre3 (Linux)

The main goal of the Linux Trustees project is to create an advanced permission management system for Linux.

<http://www.net-security.org/software.php?id=179>

LISTMODULES 1.2 (Windows)

ListModules lists the modules (EXE's and DLL's) that are loaded into a process.

<http://www.net-security.org/software.php?id=76>

NETCAT 0.7.1 (Linux)

Netcat is a featured networking utility which reads and writes data

across network connections, using the TCP/IP protocol.
<http://www.net-security.org/software.php?id=365>

NETSPOC 2.6 (Linux)

NetSPoC is a tool for security management of large computer networks with different security domains.

<http://www.net-security.org/software.php?id=86>

NUFW 1.0.10 (Linux)

NuFW is an "authenticating gateway". This means it requires authentication for any connections to be forwarded through the gateway.

<http://www.net-security.org/software.php?id=526>

PADS 1.2 (Linux)

Pads (Passive Asset Detection System) is a signature-based detection engine used to passively detect network assets.

<http://www.net-security.org/software.php?id=60>

PAM_USB 0.3.2 (Linux)

pam_usb is a PAM module that allows you to log in to your Linux box using a mobile USB storage device such as an USB pen.

<http://www.net-security.org/software.php?id=35>

PASSWORD MANAGER XP 2.1 (Windows)

Password Manager XP is a program that will help you systematize secret information.

<http://www.net-security.org/software.php?id=70>

PERISCOPE 1.2 (Windows)

PERiscope is a PE file inspection tool.

<http://www.net-security.org/software.php?id=77>

PHP ANTI-VIRUS 1.0.3 (Linux)

Scans your web server's file system for dangerous and malicious code.

<http://www.net-security.org/software.php?id=265>

PHPSECUREPAGES 0.29b (Linux)

phpSecurePages is a PHP module to secures pages with a login name and password.

<http://www.net-security.org/software.php?id=213>

PROSHIELD 3.7.21 (Linux)

ProShield is a security program for Debian Linux.

<http://www.net-security.org/software.php?id=282>

PROXYTOOLS 2004.12.2 (Windows)

ProxyTools is a package of Perl network utilities designed to assist those whose Internet access is censored, unreliable, or otherwise damaged.

<http://www.net-security.org/software.php?id=116>

SARA 6.0.4 (Linux)

The Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool.

<http://www.net-security.org/software.php?id=21>

SECPANEL 0.5.1 (Linux)

SecPanel serves as a graphical user interface for managing and running SSH (Secure Shell) and SCP (Secure Copy) connections.

<http://www.net-security.org/software.php?id=31>

SECURE PASSWORD STORE 2.52.1.2 (Windows)

Secure Password Store is a secure Password database program that stores all your passwords in a secure database.

<http://www.net-security.org/software.php?id=89>

SECURE RM 1.2.8 (Linux)

srm is a secure replacement for rm(1).

<http://www.net-security.org/software.php?id=139>

SHOREWALL 2.4.1 (Linux)

Shorewall is an iptables based firewall that can be used on a dedicated firewall system, a multi-function masquerade gateway/server or on a standalone Linux system.

<http://www.net-security.org/software.php?id=40>

SNORT SMS 0.16.9 (Linux)

A Web-based remote sensor management and monitoring system.

<http://www.net-security.org/software.php?id=342>

SPAMEATER PRO 4.0.5 build 151 (Windows)

SpamEater Pro is an anti-spam application that will seek out and delete Spam from your mailbox before you download it to your mail client.

<http://www.net-security.org/software.php?id=368>

SUPHP 0.6.0 (Linux)

suPHP is a combination of an Apache module (mod_suphp) and an executable which provides a wrapper for PHP.

<http://www.net-security.org/software.php?id=161>

SYMBION SSL PROXY 1.0.3 (Linux)

The Symbion SSL Proxy listens on a TCP port, accepts SSL connections, and forwards them to an other (local or remote) TCP port, or UNIX domain socket.

<http://www.net-security.org/software.php?id=186>

TCPDUMP 3.9.1 (Linux)

TCPDUMP prints out the headers of packets on a network interface that match the boolean expression.

<http://www.net-security.org/software.php?id=13>

TIGHTVNC 1.3dev7 (Windows)

TightVNC is a VNC distribution with many new features, improvements, and bugfixes over VNC.

<http://www.net-security.org/software.php?id=188>

TUNNELIER 4.02 (Windows)

Tunnelier is a powerful SSH2 port forwarding client with many features.

<http://www.net-security.org/software.php?id=181>

WINSOCP 3.7.5 Beta (Windows)

WinSCP is an open source SSH file transfer protocol and secure copy

client for Windows using SSH.
<http://www.net-security.org/software.php?id=6>

WINSSHD 4.02 (Windows)
WinSSHD is an SSH Secure Shell 2 server for Windows NT4, Windows 2000 and Windows XP.
<http://www.net-security.org/software.php?id=180>

XML SECURITY LIBRARY 1.2.9 (Linux)
XML Security Library is a C library based on LibXML2 and OpenSSL.
<http://www.net-security.org/software.php?id=197>

YAFIC 1.2 (Linux)
Yafic is Yet Another File Integrity Checker.
<http://www.net-security.org/software.php?id=403>

ZOC 5.04 (Windows)
This powerful terminal emulator and telnet/Secure Shell client is well known for it's outstanding user interface.
<http://www.net-security.org/software.php?id=369>

ZORP GPL 3.0.5 (Linux)
Zorp is a new generation proxy firewall suite.
<http://www.net-security.org/software.php?id=66>

[Webcasts]

All webcasts are located at:
<http://net-security.org/webcasts.php>

Spam Protection for Small Businesses
Organized by Symantec on 19 July 2005, 9:00 AM

<http://www.net-security.org/webcast.php?id=387>

Simplify Your Life - Eliminate Passwords

Organized by PowerTech Group on 19 July 2005, 2:00 PM

<http://www.net-security.org/webcast.php?id=385>

Trends in Enterprise Wireless Technology

Organized by Good Technology, Inc. on 20 July 2005, 2:00 PM

<http://www.net-security.org/webcast.php?id=386>

Automate and Streamline with Symantec LiveState Patch Manager

Organized by Symantec on 28 July 2005, 9:00 AM

<http://www.net-security.org/webcast.php?id=384>

[Conferences]

All conferences are located at:

<http://net-security.org/conferences.php>

Black Hat Briefings & Training USA 2005

Organized by Black Hat - 23 July-28 July 2005

<http://www.net-security.org/conference.php?id=138>

14th USENIX Security Symposium

Organized by USENIX - 31 July-5 August 2005

<http://www.net-security.org/conference.php?id=136>

3rd Annual Midwest Network Security Forum

Organized by The Institute for Applied Network Security - 3 August-4 August 2005

<http://www.net-security.org/conference.php?id=139>

Crypto 2005

Organized by International Association for Cryptologic Research - 14 August-18 August 2005

<http://www.net-security.org/conference.php?id=122>

8th Information Security Conference(ISC'05)

Organized by Institute for Infocomm Research - 21 September-23 September 2005

<http://www.net-security.org/conference.php?id=123>

The 4th International Workshop for Applied PKI (IWAP'05)

Organized by Institute for Infocomm Research - 21 September-23 September 2005

<http://www.net-security.org/conference.php?id=124>

RSA Conference Europe 2005

Organized by RSA Conference - 17 October-19 October 2005

<http://www.net-security.org/conference.php?id=133>

CNIS 2005: IASTED International Conference on Communication, Network and Information Security

Organized by IASTED - 14 November-16 November 2005

<http://www.net-security.org/conference.php?id=137>

Asiacrypt 2005

Organized by International Association for Cryptologic Research - 1 December-4 December 2005

<http://www.net-security.org/conference.php?id=125>

[Security World]

All press releases are located at:

http://www.net-security.org/press_main.php

Send your press releases to press@net-security.org

SpamStopsHere Announces HIPAA Compliant Anti-Spam for Medical Professionals

<http://www.net-security.org/press.php?id=3311>

Sourcefire launches worldwide training and certification programme

<http://www.net-security.org/press.php?id=3310>

CipherTrust reveals success of email authentication at Microsoft implementation summit

<http://www.net-security.org/press.php?id=3309>

Syhunt Security Announces Sandcat 1.6 with Expanded Testing for Web Applications

<http://www.net-security.org/press.php?id=3308>

LURHQ Leverages Purpose-Built Technology and Expertise to Provide Security Information and Event Management (SIEM) Managed Service

<http://www.net-security.org/press.php?id=3307>

Fewer than 25 percent of organizations regularly review external risks, IT Governance Institute study reveals in part one of research series

<http://www.net-security.org/press.php?id=3306>

Janus Associates In Stamford Receives Connecticut Quality Improvement Award For Its BIO*GATE Product

<http://www.net-security.org/press.php?id=3305>

Intellitactics Positioned in Leader Quadrant in Security Information Management Research Report

<http://www.net-security.org/press.php?id=3304>

Yankee Group Confirms Need For Security Risk Management Measuring and

Monitoring Solutions

<http://www.net-security.org/press.php?id=3303>

Thor Technologies Launches Identity Management 8.5 Version

<http://www.net-security.org/press.php?id=3302>

FrontBridge Reports Dramatic Drop in Virus Infected Email and Rise in Spam and Scams

<http://www.net-security.org/press.php?id=3301>

QuickArrow Secures its Professional Services Automation Solution with

<http://www.net-security.org/press.php?id=3300>

GFI MailEssentials earns Windows Server 2003 certification through VeriTest

<http://www.net-security.org/press.php?id=3299>

Irish Department of Defence Selects nCipher Security Solution to Protect Sensitive Data

<http://www.net-security.org/press.php?id=3298>

Vircom launches first Windows- based email security appliance at the Microsoft Worldwide Partner Conference

<http://www.net-security.org/press.php?id=3297>

Information Security Forum Warns That The Cost Of Sarbanes-Oxley Compliance Is At The Expense Of Other Security Spending

<http://www.net-security.org/press.php?id=3296>

O'Reilly Releases "Learning Unix for Mac OS X Tiger"

<http://www.net-security.org/press.php?id=3295>

[Virus News]

All virus news are located at:
<http://www.net-security.org/viruses.php>

Weekly Report on Viruses and Intruders - Mytob worm Variants, Bobin.A
Trojan and Application/SpyPc
http://www.net-security.org/virus_news.php?id=565

Questions, contributions, comments or ideas go to:

Help Net Security staff
staff@net-security.org
<http://net-security.org>

Unsubscribe from this weekly digest on:
<http://www.net-security.org/subscribe.php>

The archive of the newsletter in TXT and PDF format is available
http://www.net-security.org/newsletter_archive.php