

HNS Newsletter  
Issue 404 - 04.02.2008  
<http://www.net-security.org>

=====  
Free Whitepaper: Winning the PCI Compliance Battle  
A Guide for Merchants and Member Service Providers  
=====

This white paper reviews the basics of PCI, including who must comply, compliance requirements, validation requirements and penalties. It also examines key things to look for when selecting a PCI network testing service and introduces QualysGuard PCI.

To download this guide, please complete this form:  
<http://www.qualys.com/forms/wp/pci/?lsid=6880>

=====  
Table of contents:

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

[ Security news ]

-----  
**CELEBRITY ADVICE ON KEEPING YOUR LINUX DESKTOP SECURE**

One of the main reasons people move from Windows to Linux is the promise of greater security from malware on the Internet. Everyone knows you need to add extra security to try to keep a Windows desktop safe, but what do you have to do to accomplish the same thing on Linux?

<http://www.net-security.org/news.php?id=15723>

### TROUBLESHOOTING RPC ACROSS FIREWALLS

Applications that want to talk to other servers will often use the Remote Procedure Call (RPC) infrastructure to communicate instead of inventing their own protocol.

<http://www.net-security.org/news.php?id=15724>

### BUSH ORDER EXPANDS NETWORK MONITORING

President Bush signed a directive this month that expands the intelligence community's role in monitoring Internet traffic to protect against a rising number of attacks on federal agencies' computer systems.

<http://www.net-security.org/news.php?id=15725>

### SECURITY POLICY IN THE AGE OF COMPLIANCE

A properly drafted and implemented security policy serves to protect information, systems and even people; it sets guidelines for expected employee behavior, and authorizes security personnel to monitor, probe, investigate, define, and determine the consequences of violating the policy.

<http://www.net-security.org/news.php?id=15726>

### SPIES IN THE PHISHING UNDERGROUND

Well-known security researchers that have recently managed to infiltrate the phishing underground. In this interview, they expose the tactics and tools that phishers use, illustrate what happens when your confidential information gets stolen, discuss how phishers communicate and even how they phish each other.

<http://www.net-security.org/news.php?id=15727>

### WHITEPAPER - NAC: MANAGING UNAUTHORIZED COMPUTERS

Learn how your enterprise can combat today's threats and still remain nimble enough for tomorrow's potential threats.

<http://www.net-security.org/news.php?id=15728>

### SOFTWARE REVIEW - LAVASOFT DIGITAL LOCK

Lavasoft is a company well known for their flagship product Ad-Aware, one of the early software programs that dealt with spyware and adware threats. In 2007 they switched focus from solely developing the anti malware product, into more mainstream tools such as a personal

firewall, file shredder and an encryption utility. The fine folks from the company recently shipped us a couple of registration keys for their products, so here is a review of their crypto part of the portfolio - Lavasoft Digital Lock.

<http://www.net-security.org/news.php?id=15729>

**ANONYMOUS HACKERS FIND AND PUNISH THE WRONG GUY**  
Anti-Scientology agitators have repeatedly harassed and threatened violence against a 59-year-old PG&E worker and his wife, who were mistakenly flagged as pro-Scientology hackers.

<http://www.net-security.org/news.php?id=15730>

**TERROR SUSPECTS HONE ANTI-DETECTION SKILLS**

Simple codes, remote sites, Internet phone calls among means used to foil high-tech surveillance.

<http://www.net-security.org/news.php?id=15731>

**WHERE'S MY IPHONE? A LESSON IN INCIDENT RESPONSE**

What follows is the incident response procedure that I followed once I found out my iPhone had been stolen. It's not a comfortable feeling to know that someone else has control over a device containing your information. However, you must remain calm and follow some sort of incident response procedure. Sometimes this is not as easy as it sounds, as you will see in this article. Once the incident is over the most important thing you must do is learn from it. Hopefully you can learn from my experience.

<http://www.net-security.org/news.php?id=15732>

**THREATS FROM EVERYWHERE IN 'CYBER STORM'**

In the middle of the biggest-ever "Cyber Storm" war game to test the nation's hacker defenses, someone quietly targeted the very computers used to conduct the exercise.

<http://www.net-security.org/news.php?id=15733>

**NEW NX APIS ADDED TO VISTA SP1, XP SP3 AND WINDOWS SERVER 2008**

In the interests of helping secure the platform, we want more people to opt-in to using Data Execution Prevention (aka DEP aka NX), and we have lowered the barrier to entry for application developers in Windows Vista SP1, Windows XP SP3 and Windows Server 2008.

<http://www.net-security.org/news.php?id=15734>

#### EFFICIENT RSYNCRYPTO HIDES REMOTE SYNC DATA

The rsync utility is smart enough to send only enough bytes of a changed file to a remote system to enable the remote file to become identical to the local file.

<http://www.net-security.org/news.php?id=15735>

#### WHITEPAPER: GOOD ARCHITECTURE AND SECURITY

The Good System puts security completely in the hands of IT managers and does not require users to set security parameters or make any security decisions.

<http://www.net-security.org/news.php?id=15736>

#### RESEARCH DEBUNKS COMMON MYTHS ASSOCIATED WITH IT RISKS

Despite traditional perceptions associating IT risk primarily with security risks, survey results indicate the emergence of a broader view among IT professionals. Of the survey respondents, 78 percent gave “critical” or “serious” ratings to availability risk as opposed to security, performance and compliance risks, with 70, 68 and 63 percent respectively.

<http://www.net-security.org/news.php?id=15737>

-----

=====  
Free Whitepaper: Winning the PCI Compliance Battle  
A Guide for Merchants and Member Service Providers  
=====

This white paper reviews the basics of PCI, including who must comply, compliance requirements, validation requirements and penalties. It also examines key things to look for when selecting a PCI network testing service and introduces QualysGuard PCI.

To download this guide, please complete this form:  
<http://www.qualys.com/forms/wp/pci/?lsid=6880>

=====

[ Advisories ]

All advisories are located at:

[http://www.net-security.org/archive\\_adv.php](http://www.net-security.org/archive_adv.php)

-----

Mandriva Linux Security Update Advisory - xdg-utils (MDVSA-2008:031)

<http://www.net-security.org/advisory.php?id=8458>

Mandriva Linux Security Update Advisory - pcre3 vulnerabilities  
(MDVSA-2008:030)

<http://www.net-security.org/advisory.php?id=8457>

Ubuntu Security Notice - pulseaudio vulnerability (USN-573-1 )

<http://www.net-security.org/advisory.php?id=8456>

Mandriva Linux Security Update Advisory - ruby (MDVSA-2008:029)

<http://www.net-security.org/advisory.php?id=8455>

Gentoo Linux Security Advisory - PeerCast: Buffer overflow (GLSA  
200801-22:02)

<http://www.net-security.org/advisory.php?id=8454>

Gentoo Linux Security Advisory - Xdg-Utils: Arbitrary command  
execution (GLSA 200801-21)

<http://www.net-security.org/advisory.php?id=8453>

Gentoo Linux Security Advisory - libxml2: Denial of Service (GLSA  
200801-20)

<http://www.net-security.org/advisory.php?id=8452>

Gentoo Linux Security Advisory - GOffice: Multiple vulnerabilities  
(GLSA 200801-19)

<http://www.net-security.org/advisory.php?id=8451>

Gentoo Linux Security Advisory - Kazehakase: Multiple vulnerabilities (GLSA 200801-18)  
<http://www.net-security.org/advisory.php?id=8450>

Cisco Security Advisory - Cisco Wireless Control System Tomcat mod\_jk.so Vulnerability (cisco-sa-20080130-wcs)  
<http://www.net-security.org/advisory.php?id=8449>

Mandriva Linux Security Update Advisory - mysql (MDVSA-2008:028)  
<http://www.net-security.org/advisory.php?id=8448>

Mandriva Linux Security Update Advisory - sphinx (MDVA-2008:019)  
<http://www.net-security.org/advisory.php?id=8447>

Mandriva Linux Security Update Advisory - icu (MDVSA-2008:026)  
<http://www.net-security.org/advisory.php?id=8446>

Gentoo Linux Security Advisory - Netkit FTP Server: Denial of Service (GLSA 200801-17)  
<http://www.net-security.org/advisory.php?id=8445>

Gentoo Linux Security Advisory - MaraDNS: CNAME Denial of Service (GLSA 200801-16)  
<http://www.net-security.org/advisory.php?id=8444>

Debian Security Advisory - linux-2.6 (DSA-1479)  
<http://www.net-security.org/advisory.php?id=8443>

SUSE Security Announcement - php4, php5 (SUSE-SA:2008:004)  
<http://www.net-security.org/advisory.php?id=8442>

Gentoo Linux Security Advisory - PostgreSQL: Multiple vulnerabilities (GLSA 200801-15)

<http://www.net-security.org/advisory.php?id=8441>

Debian Security Advisory - mysql-dfsg-5.0 vulnerabilities (DSA-1478-1)

<http://www.net-security.org/advisory.php?id=8440>

Mandriva Linux Security Update Advisory - pulseaudio (MDVSA-2008:027)

<http://www.net-security.org/advisory.php?id=8439>

Debian Security Advisory - gforge (DSA-1475-1)

<http://www.net-security.org/advisory.php?id=8438>

Gentoo Linux Security Advisory - CherryPy: Directory traversal vulnerability (GLSA 200801-11)

<http://www.net-security.org/advisory.php?id=8437>

Gentoo Linux Security Advisory - xine-lib: User-assisted execution of arbitrary code (GLSA 200801-12)

<http://www.net-security.org/advisory.php?id=8436>

Gentoo Linux Security Advisory - nglRCd: Denial of Service (GLSA 200801-13:02)

<http://www.net-security.org/advisory.php?id=8435>

Gentoo Linux Security Advisory - Blam: User-assisted execution of arbitrary code (GLSA 200801-14)

<http://www.net-security.org/advisory.php?id=8434>

Debian Security Advisory - pulseaudio (DSA-1476-1)

<http://www.net-security.org/advisory.php?id=8433>

Debian Security Advisory - yarssr (DSA-1477-1)

<http://www.net-security.org/advisory.php?id=8432>

Turbolinux Security Announcement - httpd, postgresql  
<http://www.net-security.org/advisory.php?id=8431>

---

[ Articles ]

All articles are located at:  
[http://www.net-security.org/articles\\_main.php](http://www.net-security.org/articles_main.php)

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

---

#### WHERE'S MY IPHONE? A LESSON IN INCIDENT RESPONSE

What follows is the incident response procedure that I followed once I found out my iPhone had been stolen. It's not a comfortable feeling to know that someone else has control over a device containing your information. However, you must remain calm and follow some sort of incident response procedure. Sometimes this is not as easy as it sounds, as you will see in this article. Once the incident is over the most important thing you must do is learn from it. Hopefully you can learn from my experience.

<http://www.net-security.org/article.php?id=1111>

#### INTERVIEW WITH NITESH DHANJANI AND BILLY RIOS, SPIES IN THE PHISHING UNDERGROUND

Both Nitesh and Billy are well-known security researchers that have recently managed to infiltrate the phishing underground. In this interview, they expose the tactics and tools that phishers use, illustrate what happens when your confidential information gets stolen, discuss how phishers communicate and even how they phish each other.

<http://www.net-security.org/article.php?id=1110>

---

[ Reviews ]

All reviews are located at:

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

---

LAVASOFT DIGITAL LOCK

<http://www.net-security.org/review.php?id=177>

---

[ Software ]

Windows software is located at:

[http://net-security.org/software\\_main.php?cat=1](http://net-security.org/software_main.php?cat=1)

Linux software is located at:

[http://net-security.org/software\\_main.php?cat=2](http://net-security.org/software_main.php?cat=2)

Pocket PC software is located at:

[http://net-security.org/software\\_main.php?cat=3](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](http://net-security.org/software_main.php?cat=5)

---

ACUNETIX WEB VULNERABILITY SCANNER 5 (Windows)

This tool can automatically audit the security of your website and web applications.

<http://www.net-security.org/software.php?id=633>

BESTCRYPT 8.03.1 (Windows)

BestCrypt data encryption systems bring military strength encryption to the ordinary computer user without the complexities normally associated with strong data encryption.

<http://www.net-security.org/software.php?id=173>

BIG CROCODILE 3.12 (Windows)

Big Crocodile is a powerful, secure password manager.

<http://www.net-security.org/software.php?id=198>

DEKART PRIVATE DISK 2.10 (Windows)

Powerful, reliable and flexible disk encryption program that lets you create encrypted disk partitions (drive letters) to protect your confidential information.

<http://www.net-security.org/software.php?id=562>

GPGE 1.31 (Windows)

GPGe is a shell extension for Windows explorer that acts as an assistant for using GNU Privacy Guard (GnuPG/GPG).

<http://www.net-security.org/software.php?id=642>

KASPERSKY ANTI-VIRUS 7 (Windows)

Kaspersky Anti-Virus 6.0 combines traditional antivirus defense methods with the latest proactive technologies.

<http://www.net-security.org/software.php?id=652>

KMYFIREWALL 1.1.1 (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>

LOCKNOTE 1.0.4 (Windows)

LockNote will change the way you work with confidential notes.

Application and document in one: the mechanism to encrypt and decrypt a note is part of it. Secure, simple, independent. No installation required.

<http://www.net-security.org/software.php?id=649>

#### NAGIOS 3.0 RC2 (Linux)

Nagios is a host and service monitor designed to inform you of network problems before your clients, end-users or managers do.

<http://www.net-security.org/software.php?id=279>

#### PRIVATE SHELL 3.0 beta (Windows)

SSH client for Windows with SSH1 and SSH2 protocols support, includes Secure FTP client and command line tools.

<http://www.net-security.org/software.php?id=517>

#### SAMHAIN 2.4.3 (Linux)

Samhain is an open source file integrity and host-based intrusion detection system.

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

#### SCPONLY 4.8 (Linux)

"scponly" is an alternative 'shell' (of sorts) for system administrators who would like to provide access to remote users to both read and write local files without providing any remote execution priviledges.

<http://www.net-security.org/software.php?id=337>

#### SECURE HIVE 1.3 (Windows)

Secure Hive encryption software protects files, emails, graphics and text.

<http://www.net-security.org/software.php?id=240>

#### THE SLEUTH KIT 2.50 (Linux)

The Sleuth Kit is a collection of UNIX-based command line file system forensic tools.

<http://www.net-security.org/software.php?id=215>

#### TUNNELIER 4.25 (Windows)

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

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

WINSSHD 4.23 (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>

---

[ Conferences ]

All conferences are located at:

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

---

Black Hat DC 2008

Organized by Black Hat - 18 February-21 February 2008

<http://www.net-security.org/conference.php?id=239>

ARES 2008

Organized by DEXA Society - 4 March-7 March 2008

<http://www.net-security.org/conference.php?id=236>

InfoSec World Conference & Expo 2008

Organized by MISTI - 10 March-12 March 2008

<http://www.net-security.org/conference.php?id=247>

Black Hat Europe 2008

Organized by Black Hat - 25 March-28 March 2008

<http://www.net-security.org/conference.php?id=240>

RSA Conference 2008

Organized by RSA Security - 7 April-11 April 2008

<http://www.net-security.org/conference.php?id=243>

HITBSecConf2008

Organized by Hack in the Box - 14 April-17 April 2008

<http://www.net-security.org/conference.php?id=246>

Infosecurity 2008

Organized by Reed Exhibitions - 22 April-24 April 2008

<http://www.net-security.org/conference.php?id=245>

Hacker Halted USA 2008

Organized by EC-Council - 28 May-4 June 2008

<http://www.net-security.org/conference.php?id=244>

Second International Symposium on Human Aspects of Information Security & Assurance

Organized by Information Security & Network Research Group,  
University of Plymouth - 8 July-10 July 2008

<http://www.net-security.org/conference.php?id=238>

-----

[ Security World ]

All security world articles are located at:

[http://www.net-security.org/secworld\\_main.php](http://www.net-security.org/secworld_main.php)

Send your press releases to [press@net-security.org](mailto:press@net-security.org)

-----

Research debunks common myths associated with IT risks

<http://www.net-security.org/secworld.php?id=5791>

State of email authentication and the Internet trust ecosystem

<http://www.net-security.org/secworld.php?id=5792>

Distributed Ethereal sniffer as a managed service  
<http://www.net-security.org/secworld.php?id=5790>

New Cisco book: "Router Security Strategies: Securing IP Network Traffic Planes"  
<http://www.net-security.org/secworld.php?id=5787>

Million dollar email scammers plead guilty  
<http://www.net-security.org/secworld.php?id=5786>

Free books from Open Web Application Security Project  
<http://www.net-security.org/secworld.php?id=5785>

New high performance security risk management appliance  
<http://www.net-security.org/secworld.php?id=5784>

Yahoo! CAPTCHA broken? Recognition engine available for download  
<http://www.net-security.org/secworld.php?id=5783>

Mortgage spam jumps in response to Fed rate cut  
<http://www.net-security.org/secworld.php?id=5782>

New book: "Mainframe Basics for Security Professionals"  
<http://www.net-security.org/secworld.php?id=5781>

New U.S. patent for network security testing  
<http://www.net-security.org/secworld.php?id=5780>

Virtual infrastructure security for Citrix XenServer  
<http://www.net-security.org/secworld.php?id=5779>

Barracuda defends free and open source software from patent threat  
<http://www.net-security.org/secworld.php?id=5771>

Online self-assessment tool for information security professionals  
<http://www.net-security.org/secworld.php?id=5770>

WatchGuard upgrades software on its appliances  
<http://www.net-security.org/secworld.php?id=5769>

New release: The Book of Wireless  
<http://www.net-security.org/secworld.php?id=5768>

HITBSecConf2008: IT professionals come to Dubai  
<http://www.net-security.org/secworld.php?id=5767>

-----

=====  
Free Whitepaper: Winning the PCI Compliance Battle  
A Guide for Merchants and Member Service Providers  
=====

This white paper reviews the basics of PCI, including who must comply, compliance requirements, validation requirements and penalties. It also examines key things to look for when selecting a PCI network testing service and introduces QualysGuard PCI.

To download this guide, please complete this form:  
<http://www.qualys.com/forms/wp/pci/?lsid=6880>

=====

[ Virus News ]

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

-----

WoW password stealing worm and YouTube video playing trojan  
[http://www.net-security.org/virus\\_news.php?id=916](http://www.net-security.org/virus_news.php?id=916)

University course on malware analysis  
[http://www.net-security.org/virus\\_news.php?id=915](http://www.net-security.org/virus_news.php?id=915)

-----

Questions, contributions, comments or ideas go to:

Help Net Security staff  
[staff@net-security.org](mailto: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](http://www.net-security.org/newsletter_archive.php)