

HNS Newsletter
Issue 426 - 07.07.2008
<http://www.net-security.org>

=====
===
Help Net Security podcasts (no registration needed to listen)
=====
===

- Choosing the Right Security Personnel
- The Rise of User Circumvention and Risky Unauthorized Activities
- Politically motivated Distributed Denial of Service attacks
- Web application security landscape and trends
- Penetration testing considerations

<http://www.net-security.org/articles.php?cat=15>

=====
Table of contents:

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

[Security news]

WHITEPAPER: BACKUP AND RECOVERY - TOP 10 REASONS TO UPGRADE
A new gold standard in continuous data protection and complete system
recovery is here—Symantec Backup Exec 12 and Backup Exec System
Recovery 8.

<http://www.net-security.org/news.php?id=15981>

TOP 10 STRANGEST ANTI-TERRORISM PATENTS

Technology has always played a big role in fighting terrorism.

<http://www.net-security.org/news.php?id=15982>

Q&A: THE THREAT OF MALWARE TO MOBILE PHONES

Richard R. Roscitt is the CEO of SMobile Systems. He keynoted at world-class forums and is regularly featured in leading business and industry trade print and electronic media, having appeared often on CNBC, Bloomberg TV, and CNN/FN. In this interview he discusses the threat of malware to mobile phones.

<http://www.net-security.org/news.php?id=15983>

INSIDE NSA RED TEAM SECRET OPS WITH GOVERNMENT'S TOP HACKERS

What are red teams, you ask? They're sort of like the special forces units of the security industry—highly skilled teams that clients pay to break into the clients' own networks.

<http://www.net-security.org/news.php?id=15984>

REVERSE ENGINEERING: ANTI-CRACKING TECHNIQUES

This paper is a guide into better understanding most of the approaches a reverse engineer can follow in order to achieve his goal. Additionally, it includes a number of advices on how to better protect your software against tracing its sensitive information, like serial key checks and authentication procedures.

<http://www.net-security.org/news.php?id=15985>

WHITEPAPER - BACKUP AND RECOVERY BEST PRACTICES FOR MICROSOFT SQL SERVER 2005

To help you choose from among the available configuration options and backup and recovery procedures, HP has conducted extensive laboratory tests to determine best practices.

<http://www.net-security.org/news.php?id=15986>

WRITING POLICY FOR CONFINED SELINUX USERS

The SELinux management environment (system-config-selinux) has been updated and includes the ability to build customized SELinux policy modules for the confinement of users.

<http://www.net-security.org/news.php?id=15987>

SQL SERVER AND THE WINDOWS SERVER 2008 FIREWALL

For those of you migrating from Windows Server 2003 or earlier to Windows Server 2008, if you have not previously heeded the advice to enable the firewall, you may be surprised by connectivity failures caused by the firewall (for any version of SQL) and you will need to take action to enable the connectivity you want.

<http://www.net-security.org/news.php?id=15988>

AN INTRODUCTION TO THE KISMET PACKET SNIFFER

Kismet is a wireless "detector, sniffer, and intrusion detection system," and one of the growing list of essential open source tools for computer network security professionals.

<http://www.net-security.org/news.php?id=15989>

BOOK REVIEW - GOOGLE APPS HACKS

With all Google's offerings, getting the best out of them and discovering cool features can sometimes be time consuming. Fortunately, there's "Google Apps Hacks", a typical O'Reilly title that cuts to the chase, eliminates the tedious introductions and makes the reader say: "I never thought you could do that!"

<http://www.net-security.org/news.php?id=15990>

[Advisories]

All advisories are located at:

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

Debian Security Advisory - wordpress (DSA-1601-1)

<http://www.net-security.org/advisory.php?id=9032>

Mandriva Linux Security Update Advisory - php4 (MDVSA-2008:130)
<http://www.net-security.org/advisory.php?id=9031>

Mandriva Linux Security Update Advisory - php4 (MDVSA-2008:129)
<http://www.net-security.org/advisory.php?id=9030>

Mandriva Linux Security Update Advisory - php (MDVSA-2008:128)
<http://www.net-security.org/advisory.php?id=9029>

Mandriva Linux Security Update Advisory - php (MDVSA-2008:127)
<http://www.net-security.org/advisory.php?id=9028>

Mandriva Linux Security Update Advisory - php (MDVSA-2008:125)
<http://www.net-security.org/advisory.php?id=9027>

Mandriva Linux Security Update Advisory - php (MDVSA-2008:126)
<http://www.net-security.org/advisory.php?id=9026>

Ubuntu Security Notice - firefox vulnerabilities (USN-619-1)
<http://www.net-security.org/advisory.php?id=9025>

SUSE Security Announcement - kernel-source-2.6.8 (2.6.8-17sarge1)
(SUSE-SA:2008:031)
<http://www.net-security.org/advisory.php?id=9024>

Debian Security Advisory - sympa (DSA-1600-1)
<http://www.net-security.org/advisory.php?id=9023>

Slackware Security Advisory - xorg-server, libxfont, xfree86
(SSA:2008-183-01)
<http://www.net-security.org/advisory.php?id=9022>

Gentoo Linux Security Advisory - Motion: Execution of arbitrary code

(GLSA 200807-02)

<http://www.net-security.org/advisory.php?id=9021>

Gentoo Linux Security Advisory - Python: Multiple integer overflows

(GLSA 200807-01)

<http://www.net-security.org/advisory.php?id=9020>

Apple Security Update - Safari 3.1.2 for Mac OS X v10.4.11

(APPLE-SA-2008-06-30)

<http://www.net-security.org/advisory.php?id=9019>

Apple Security Update - Security Update 2008-004 and Mac OS X v10.5.4

(APPLE-SA-2008-06-30)

<http://www.net-security.org/advisory.php?id=9018>

Ubuntu Security Notice - samba regression (USN-617-2)

<http://www.net-security.org/advisory.php?id=9017>

Slackware Security Advisory - gnutls (SSA:2008-180-01)

<http://www.net-security.org/advisory.php?id=9016>

Slackware Security Advisory - ruby (SSA:2008-179-01)

<http://www.net-security.org/advisory.php?id=9015>

[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

ACTIVE DIRECTORY CHANGE REPORTER (Windows)

Active Directory change auditing is an important procedure for limiting unauthorized changes and errors to AD and Group Policy configurations.

<http://www.net-security.org/software.php?id=722>

BOTAN 1.7.7 (Linux)

Botan aims to be a portable, easy to use, and efficient C++ crypto library.

<http://www.net-security.org/software.php?id=94>

CAIN & ABEL 4.9.16 (Windows)

Cain & Abel is a password recovery tool for Microsoft operating systems.

<http://www.net-security.org/software.php?id=110>

CLEAN DISK SECURITY 7.77 (Windows)

This program gives you secure file deletion, making sure that deleted files cannot be undeleted again.

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

CRYPTOEXPERT 2008 PROFESSIONAL 7.6.2 (Windows)

CryptoExpert creates encrypted virtual disks and these disks are visible as usual disks with drive letters.

<http://www.net-security.org/software.php?id=305>

CUTE PASSWORD MANAGER 2008.1.3.6 (Windows)

Cute Password Manager is a free form filling software that auto fill userID and password.

<http://www.net-security.org/software.php?id=721>

MINORFS 0.3.2 (Linux)

MinorFS combines a small set of cooperating userspace filesystems for Linux that provide private storage to pseudo persistent processes.

<http://www.net-security.org/software.php?id=701>

OUTPOST FIREWALL PRO 6.5.2355.316.0597 (Windows)

This is a comprehensive solution for online protection.

<http://www.net-security.org/software.php?id=276>

OUTPOST SECURITY SUITE PRO 2008 6.5.2355.316.0597 (Windows)

A combination of antivirus, antispymware, firewall and antispam.

<http://www.net-security.org/software.php?id=278>

PASSWORD MANAGER XP 2.3.437 (Windows)

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

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

PRELUDE MANAGER 0.9.13 (Linux)

Prelude Manager is the main program of the Prelude Hybrid IDS suite.

<http://www.net-security.org/software.php?id=264>

SECTOOL 0.8.0 (Linux)

sectool is a security tool for RPM based distributions. It can be used for security auditing and intrusion detection.

<http://www.net-security.org/software.php?id=700>

SEGATEX 6.50 (Linux)

segatex is a tool to configure SELinux policy with the help of a GUI

<http://www.net-security.org/software.php?id=697>

SHOREWALL 4.0.12 (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>

[Conferences]

All conferences are located at:

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

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>

Black Hat USA 2008 Briefings & Training

Organized by Black Hat - 2 August-7 August 2008

<http://www.net-security.org/conference.php?id=262>

Breakaway 2008

Organized by CompTIA - 5 August-7 August 2008

<http://www.net-security.org/conference.php?id=261>

NETWAYS Nagios Conference 2008

Organized by Netways - 11 September-12 September 2008

<http://www.net-security.org/conference.php?id=263>

IT Security World 2008 Conference & Expo

Organized by MIS Training Institute - 13 September-18 September 2008

<http://www.net-security.org/conference.php?id=258>

VB2008

Organized by Virus Bulletin - 1 October-3 October 2008

<http://www.net-security.org/conference.php?id=256>

I Digital Security Forum

Organized by FSD - 7 November-8 November 2008

<http://www.net-security.org/conference.php?id=255>

The Fourth International Conference on Availability, Reliability and Security (ARES 2009)

Organized by Vienna University of Technology / Secure Business Austria - 16 March-19 March 2009

<http://www.net-security.org/conference.php?id=260>

[Articles]

All articles are located at:

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

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

REVERSE ENGINEERING: ANTI-CRACKING TECHNIQUES

This paper is a guide into better understanding most of the approaches a reverse engineer can follow in order to achieve his goal. Additionally, it includes a number of advices on how to better protect your software against tracing its sensitive information, like serial key checks and authentication procedures.

<http://www.net-security.org/article.php?id=1152>

Q&A: THE THREAT OF MALWARE TO MOBILE PHONES

Richard R. Roscitt is the CEO of SMobile Systems. He keynoted at world-class forums and is regularly featured in leading business and industry trade print and electronic media, having appeared often on CNBC, Bloomberg TV, and CNN/FN. In this interview he discusses the

threat of malware to mobile phones.

<http://www.net-security.org/article.php?id=1151>

[Reviews]

All reviews are located at:

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

GOOGLE APPS HACKS

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

[Conferences]

All conferences are located at:

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

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>

Black Hat USA 2008 Briefings & Training

Organized by Black Hat - 2 August-7 August 2008

<http://www.net-security.org/conference.php?id=262>

Breakaway 2008

Organized by CompTIA - 5 August-7 August 2008

<http://www.net-security.org/conference.php?id=261>

NETWAYS Nagios Conference 2008

Organized by Netways - 11 September-12 September 2008

<http://www.net-security.org/conference.php?id=263>

IT Security World 2008 Conference & Expo

Organized by MIS Training Institute - 13 September-18 September 2008

<http://www.net-security.org/conference.php?id=258>

VB2008

Organized by Virus Bulletin - 1 October-3 October 2008

<http://www.net-security.org/conference.php?id=256>

I Digital Security Forum

Organized by FSD - 7 November-8 November 2008

<http://www.net-security.org/conference.php?id=255>

The Fourth International Conference on Availability, Reliability and Security (ARES 2009)

Organized by Vienna University of Technology / Secure Business Austria - 16 March-19 March 2009

<http://www.net-security.org/conference.php?id=260>

[Security World]

All security world articles are located at:

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

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

Rise in SQL injection attacks exploiting unverified user data input
<http://www.net-security.org/secworld.php?id=6288>

Recent potential email and Web threats
<http://www.net-security.org/secworld.php?id=6287>

Understanding the Web browser threat
<http://www.net-security.org/secworld.php?id=6286>

250GB fire-safe/waterproof hard drive
<http://www.net-security.org/secworld.php?id=6285>

E-mail spam morphs in first half of 2008
<http://www.net-security.org/secworld.php?id=6284>

Experiment reveals the growing psychological nature of spam
<http://www.net-security.org/secworld.php?id=6283>

Virtual Private Racks with Gigabit speed and VPN services
<http://www.net-security.org/secworld.php?id=6282>

Free forensic tool suite
<http://www.net-security.org/secworld.php?id=6281>

Embedded systems device authentication
<http://www.net-security.org/secworld.php?id=6280>

ContentWatch expands its web security appliances line
<http://www.net-security.org/secworld.php?id=6279>

Free e-book: "Security Manager's Guide to Video Surveillance"

<http://www.net-security.org/secworld.php?id=6278>

Additional payment devices to strengthen cardholder data security

<http://www.net-security.org/secworld.php?id=6277>

Next generation of Extensible Threat Management solutions

<http://www.net-security.org/secworld.php?id=6276>

Realtime troubleshooting functionality added to the AirDefense Wireless IPS

<http://www.net-security.org/secworld.php?id=6275>

Tool encourages schools to rate their security

<http://www.net-security.org/secworld.php?id=6274>

Fraud prevention tips

<http://www.net-security.org/secworld.php?id=6273>

Majority of security software is acquired online

<http://www.net-security.org/secworld.php?id=6272>

New online training in enterprise and forensic investigations

<http://www.net-security.org/secworld.php?id=6271>

Image Risk scanner for enterprise email

<http://www.net-security.org/secworld.php?id=6270>

Endpoint productivity advances with Anti-Executable 3.0

<http://www.net-security.org/secworld.php?id=6269>

[Virus News]

All virus news are located at:

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

Independence Day brings down attack on computer users

http://www.net-security.org/virus_news.php?id=955

Visitors to Sony Playstation website at risk of malware infections

http://www.net-security.org/virus_news.php?id=954

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