

SECURITY DATABASE

KEEP A VIGILANT EYE ON YOUR DEFENSES

Best IT Security Tools & Software

REWIND 
TO THE PAST 2009

Nabil OUCHN
CEO & Founder

Maximiliano SOLER
ToolsWatch Process Leader

<http://www.security-database.com>

The year 2009 was very intense of emotions, sadness, sorrows, and conflicts. The world as we knew or at least our parents did is changing so fast and unfortunately not in the right way.

The very bad economic situation, the stinky religions conflicts, the riots and wars, the increase of radical extremists and the policy of fear that the governments feed us are urging this earth to an excruciating end.

But instead of talking about politicians and their immature and childish job they are doing as spreading fear, making the wrong choices (as usual), wasting taxpayers money and time, dumping people into poverty, we'd prefer focusing into enumerating the great software and tools we've seen this year.

So, we are happy that 2009 is finally over and we expect the best for 2010.

Scoring criteria

We've conducted this new survey on the basis on some criteria (as we did two years before).

Since the last survey (2007), we decided to add these new criteria:

- Community support
- Documentation
- Popularity (Twitter followers)

Criteria	Comment
Audience	Each tool has its target audience.
Community Support	Tool has a community version with support and the appropriate documentation.
Documentation	All documentation are easy to read and to understand and at least written in English. Wiki, blogs and other collaborative support are a must.
Features	Built-in, plug-in, functionalities, capabilities, use of APIs, interoperability with other systems...
Maintenance	Frequency of bugs fixing, generating new releases, nightly builds, beta testing.
Popularity	The popularity of the tool among the community. Twitter followers. Average of visits and download based on our statistics for the year 2009.
Reporting	Support of charts, dashboard, exporting to multiple formats (HTML, XML, PDF).
Standards, Metrics & Open Standards	The ability of the tool to map findings with Compliance, standards and open standards or to score vulnerability / risks with metrics. Standard and metrics could be: CVE, CVSS, CWE, CPE, CCE, OVAL, SCAP, CAPEC, ISO 2700x, NIST, PCI DSS...
Updates	Frequency of updates: adding new features, new plug-in, updating vulnerability database, updating techniques...

Open Source & Free Utilities

Penetration Tests and Ethical Hacking

	Winner	Excellent	Recommended (Promising)
Information Gathering	Maltego	Binging	
Network Scanners and Discovery	Nmap v5	Ex æquo: Netifera AutoScan	Angry IP Scanner
Vulnerability Scanners	Ex æquo: Nessus NeXpose	OpenVAS	
Application Scanners	W3AF	Samurai WTF	Nikto
Exploitation Frameworks	Metasploit v3	DB Exploit Website	
Wireless Hacking	OSWA	AirCrack suite	AiroScript-NG
Live CDs	BackTrack 4	Katana	Matriux

Security Assessment

	Winner	Excellent	Recommended (Promising)
Windows Auditing	OVAL interpreter	Nessus Local Plug-ins	Sysinternals tools
Unix Auditing	Lynis	CIS Scoring	OpenSCAP
Firewall & Filtering Devices	None	None	None
Application Assessment	BurpSuite	WebSecurify	CAT The manual web application

	Winner	Excellent	Recommended (Promising)
Wireless Auditing	OSWA	Ex æquo: Kismet Kismac	Inssider
Forensics	CAINE	Ex æquo: Mobius / Process Hacker	Netwitness Free Edition
Datamining / Logs Management	Splunk community release	Dradis	
IT Management	SpiceWorks	Paglo IT	
Code Analysis	Rats	Graudit	MS CAT.net
Password Analysis	Ex æquo: Cain & Abel OphCrack	John The Ripper	
Database Auditing	Db Audit Free edition	Ex æquo: Pangolin SQL Map	Wapiti
VoIP / Telephony Auditing	VAST Viper	WarVox	

Commercial software

	Winner	Excellent	Recommended (Promising)
Vulnerability Management	Ex æquo: Tenable Nessus ProFeed	Ex æquo: WebSaint / NeXpose Enterprise	
Application Security Assessment	Ex æquo: Acunetix / N-stalker	IBM AppSCAN	Netsparker
Patch Management	GFI Languard NSS	Lumension EndPoint	
Penetration Testing and Exploitation	CoreImpact	SaintExploit	

Links and References

	Editor
Maltego	http://www.paterva.com/web4/index.php/maltego
Binging	http://www.blueinfo.com
Nmap	http://www.nmap.org
Netifera	http://netifera.com
AutoScan	http://autoscan-network.com
Angry IP Scanner	http://www.angryip.org
Nessus	http://www.nessus.org
NeXpose	http://community.rapid7.com
OpenVAS	http://www.openvas.org
W3AF	http://w3af.sourceforge.net
Metasploit	http://www.metasploit.org
Samurai WTF	http://samurai.inguardians.com
Nikto	http://cirt.net/nikto2
Exploit DB	http://www.exploit-db.com
OSWA	http://securitystartshere.org/page-training-oswa.htm
AirCrack-NG Suite	http://www.aircrack-ng.org
AiroScript-NG	http://airoscrip.aircrack-ng.org
BackTrack 4	http://www.remote-exploit.org
Katana	http://www.hackfromacave.com/katana.html
Matriux	http://www.matriux.com
Oval Interpreter	http://oval.mitre.org
Sysinternals suite	http://technet.microsoft.com/sysinternals
Lynis	http://www.rootkit.nl

	Editor
CIS Scoring tools	http://www.cisecurity.org
OpenSCAP	http://www.open-scap.org
BurpSuite	http://portswigger.net
Websecurify	http://www.websecurify.com
CAT The Manual Web Application Audit	http://cat.contextis.co.uk
Kismet	http://www.kismetwireless.net
Kismac	http://kismac-ng.org
Inssider	http://www.metageek.net/products/inssider
CAINE	http://www.caine-live.net
Mobius Forensics Toolkit	http://freshmeat.net/projects/mobiusft
Process Hacker	http://processhacker.sourceforge.net
Netwitness Free Edition	http://www.netwitness.com
Splunk Community	http://www.splunk.com
Dradis	http://dradisframework.org
Spiceworks Community	http://www.spiceworks.com
Paglo IT	http://paglo.com
RATS	http://www.fortify.com
Graudit	http://www.justanotherhacker.com
OWASP Code Crawler	http://www.owasp.org
Cain & Abel	http://www.oxid.it
OphCrack	http://ophcrack.sourceforge.net
John the Ripper	http://www.openwall.com/john
DB Audit Free Edition	http://www.softretech.com
Pangolin	http://www.nosec.org

	Editor
SQL Map	http://sqlmap.sourceforge.net
Wapiti	http://wapiti.sourceforge.net
VAST Viper	http://vipervast.sourceforge.net
WarVox	http://warvox.org
	Commercial software
Tenable Nessus Profeed	http://nessus.org/products/professional-feed/
WebSaint	http://www.saintcorporation.com
NeXpose Enterprise	http://www.rapid7.com/
Acunetix	www.acunetix.com/
N-Stalker	http://www.nstalker.com/
IBM AppSCAN	http://www-01.ibm.com/software/awdtools/appscan/
NetSparker	http://www.mavitunasecurity.com/
GFI Languard	http://www.gfi.com/languard/
Lumension EndPoint	http://www.lumension.com
Core Impact	http://www.coresecurity.com/
SaintExploit	http://www.saintcorporation.com



Security news in brief

What's happened

	Link
Returns of The L0pht Industry	▪ http://www.security-database.com/toolswatch/The-famous-l0pht-com-is-up-and.html ▪ http://www.security-database.com/toolswatch/L0phtCrack-is-back-with-a-new.html
VoIPScanner the first VoIP scanner As A Service	▪ http://www.security-database.com/toolswatch/VoIPScanner-com-the-First-VoIP.html
Rapid7 acquires Metasploit	▪ http://www.rapid7.com/metasploit-announcement.jsp
Nmap v5.0 released	▪ http://nmap.org/5/
Metasploit 3.x the best exploitation framework	▪ http://blog.metasploit.com/2009/11/metasploit-framework-33-released.html
The attack of conficker	▪ http://www.security-database.com/toolswatch/Scanners-and-utilities-to-detect.html ▪ http://www.security-database.com/detail.php?alert=CVE-2008-4250
Sara project retired	▪ http://www.security-database.com/toolswatch/SARA-project-retired-Last-release.html
Nessus turns to web with version 4.2	▪ http://blog.tenablesecurity.com/2009/11/nessus-42-released.html
OWASP Guide v3.0 released	▪ http://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents
CWE/SANS top dangerous programming errors	▪ http://www.security-database.com/toolswatch/CWE-SANS-Top-25-Most-Dangerous.html

The idiot move

Nipper the dog is retired from Sourceforge.

<http://sourceforge.net/projects/nipper/>

The smart move

Keeping Metasploit open source and even adding support of Nexpose from Rapid7.

<http://blog.metasploit.com/2009/12/metasploit-331-nexpose-community.html>

Security Hoax

The death of Str0ke from milw0rm

- <http://www.security-database.com/toolswatch/+RIP-str0ke-milw0rm+.html>
- <http://twitter.com/str0ke>

The worst and shameless Internet innovation

And the winner is France for HADOPI LAW.

- http://en.wikipedia.org/wiki/HADOPI_law
- <http://www.laquadrature.net/>
- <http://www.korben.info/ipredator-la-solution-100-anti-hadopi.html>
- <http://www.partipirate.org/blog/index.php>

Big brother project of the year

And the winner is France for HADOPI LAW.