

# [Full-disclosure] Metasploit Framework v3.1 Released

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2008-01/msg00530.html>

---

- *From:* H D Moore <[fdlist@xxxxxxxxxxxxxxxxxxxxxx](mailto:fdlist@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 27 Jan 2008 23:32:06 -0600
- 

## METASPLOIT UNLEASHES VERSION 3.1 OF THE METASPLOIT FRAMEWORK New Version of Attack Framework Ready to Pwn

Austin, Texas, January 28th, 2008 — The Metasploit Project announced today the free, world-wide availability of version 3.1 of their exploit development and attack framework. The latest version features a graphical user interface, full support for the Windows platform, and over 450 modules, including 265 remote exploits.

"Metasploit 3.1 consolidates a year of research and development, integrating ideas and code from some of the sharpest and most innovative folks in the security research community" said H D Moore, project manager. Moore is referring the numerous research projects that have lent code to the framework.

These projects include the METASM pure-ruby assembler developed by Yoann Guillot and Julien Tinnes, the "Hacking the iPhone" effort outlined in the Metasploit Blog, the Windows kernel-land payload staging system developed by Matt Miller, the heapLib browser exploitation library written by Alexander Sotirov, the Lorcon 802.11 raw transmit library created by Joshua Wright and Mike Kershaw, Scruby, the Ruby port of Philippe Biondi's Scapy project, developed by Sylvain Sarmejeanne, and a contextual encoding system for Metasploit payloads. "Contextual encoding breaks most forms of shellcode analysis by encoding a payload with a target-specific key" said Iruoid, author of the Uninformed Journal (volume 9) article and developer of the contextual encoding system included with Metasploit 3.1.

The graphical user interface is a major step forward for Metasploit users on the Windows platform. Development of this interface was driven by Fabrice Mourron and provides a wizard-based exploitation system, a graphical file and process browser for the Meterpreter payloads, and a multi-tab console interface. "The Metasploit GUI puts Windows users on the same footing as those running Unix by giving them access to a console interface to the framework" said H D Moore, who worked with Fabrice on the GUI project.

The latest incarnation of the framework includes a bristling

## [Full-disclosure] Metasploit Framework v3.1 Released

arsenal of exploit modules that are sure to put a smile on the face of every information warrior. Notable exploits in the 3.1 release include a remote, unpatched kernel-land exploit for Novell Netware, written by toto, a series of 802.11 fuzzing modules that can spray the local airspace with malformed frames, taking out a wide swath of wireless-enabled devices, and a battery of exploits targeted at Borland's InterBase product line. "I found so many holes that I just gave up releasing all of them", said Ramon de Carvalho, founder of RISE Security, and Metasploit contributor.

"Metasploit continues to be an indispensable and reliable penetration testing framework for our modern era", says C. Wilson, a security engineer who uses Metasploit in his daily work. Metasploit is used by network security professionals to perform penetration tests, system administrators to verify patch installations, product vendors to perform regression testing, and security researchers world-wide. The framework is written in the Ruby programming language and includes components written in C and assembler.

Metasploit runs on all modern operating systems, including Linux, Windows, Mac OS X, and most flavors of BSD. Metasploit has been used on a wide range of hardware platforms, from massive Unix mainframes to the tiny Nokia n800 handheld. Users can access Metasploit using the tab-completing console interface, the Gtk GUI, the command line scripting interface, or the AJAX-enabled web interface. The Windows version of Metasploit includes all software dependencies and a selection of useful networking tools.

The latest version of the Metasploit Framework, as well as screen shots, video demonstrations, documentation and installation instructions for many platforms, can be found online at

<http://metasploit3.com/>

###

If you'd like more information about this topic, or to schedule an interview with the developers, please email [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>