



METASPLOIT 3.3 NOW AVAILABLE

Largest Framework for Publicly Available Exploits Expands Coverage, Payload Sophistication, Performance and Platform Support

AUSTIN, Texas – November 17, 2009 – The Metasploit Project announced the immediate availability of version 3.3 of the Metasploit Framework, the world's most popular open source exploit development and [penetration testing](#) platform. Incorporating community contributions from 12 months of development effort, Metasploit 3.3 has updated its framework with a particular focus on expanding its exploit coverage, payload sophistication, stability, performance, third-party integration capabilities and platform support.

“The Metasploit community has worked hard over the last 12 months to build a penetration testing platform with unique features and unmatched flexibility,” said HD Moore, chief architect of Metasploit and chief security officer at Rapid7, which manages the Metasploit Project. “I’m confident that Metasploit users will immediately benefit from the new capabilities of the framework and I look forward to raising the bar even further in the coming months.”

Key enhancements include:

Expanded Exploit Coverage

This release features significant advances in exploit coverage across a wide range of targets, now including more than 440 exploits, 215 auxiliary modules and hundreds of payloads, including an in-memory VNC service and the Meterpreter. Covering over 400 unique CVEs, Metasploit continues to provide the world's largest database of publicly available exploits.

Additional Platform Support

The latest version of the Metasploit Framework is supported on all modern operating systems, including 32-bit and 64-bit versions of Windows®, Linux and Mac OS® X. The framework also runs on a wide variety of devices, from the Apple® iPhone™ to IBM mainframes. This release is the first version to support Ruby 1.9.1, Windows 7 and a native console interface on the Windows platform. AIX support as a target platform has been improved, with a number of additional payloads, which support versions 5.3.7 through 6.1.4 of the AIX platform. Oracle databases are now first-class targets to Metasploit with the addition of pre-authentication, post-authentication and SQL injection modules.

Payload Sophistication

Metasploit 3.3 provides additional support for advanced payloads, including support for JSP payloads, IPv6, NX and DEP. In addition, Metasploit now supports advanced payload masking to aid penetration testers using social engineering techniques. The Meterpreter payload now supports screen shots, packet sniffing and key stroke logging. With these advances, Metasploit continues to improve the state of the art in superior penetration testing tools.

Vastly Improved Performance and Manageability

Metasploit 3.3 loads faster than previous versions due to performance improvements made to the core libraries and module loader. Windows users will see a significant improvement in both the usability and responsiveness of the Metasploit console on that platform.

Metasploit 3.3 also improves manageability, with simplified installation on Windows and Linux, an improved user interface and notification of last update times. Performance and stability have also been a focus of this release.

Enhanced Integration with The Open Source Vulnerability Database (OSVDB)

This release features enhanced integration with the OSVDB, with all relevant exploits having associated OSVDB ID references and two-way links between the osvdb.org entry and the metasploit.com module browser. CVE references have been modified across the entire module tree.

Community-Driven

With a community-based development team, this release of the Metasploit Framework was driven by numerous key contributors, including James Lee, Yoann Guillot, Steve Tornio, MC, Chris Gates, Alexander Kornbrust, Ramon Carvalle, Stephen Fewer, Ryan Linn, Lurene Grenier, Mike Kershaw, Patrick Webster, Max Moser, Efrain Torres, Alexander Sotirov, Ty Bodell, Joshua Drake, JR, Carlos Perez, Kris Katterjohn and many others.

For a detailed listing of these and other enhancements, please see the [Metasploit's 3.3 Release Notes](#).

About Metasploit

Metasploit runs on all modern operating systems, including Linux, Windows®, Mac OS® X and most flavors of Berkeley Software Distribution (BSD). Metasploit has been used on a wide range of hardware platforms, from massive Unix mainframes to the Apple® iPhone™. Installers are available for the Windows and Linux platforms, bundling all dependencies into a single package for ease of installation. The latest version of the Metasploit Framework, as well as images, video demonstrations, documentation and installation instructions for many platforms can be found online at <http://www.metasploit.com/framework/>.

The Metasploit Project is managed by Rapid7, the leading provider of unified [vulnerability management](#), compliance and penetration testing solutions that deliver actionable intelligence about an organization's entire IT environment. For more information, visit www.rapid7.com.

###