



Metasploit Pro 4.0 Helps Defenders Prevent Data Breaches Through Greater Enterprise Integration, Cloud Deployment and Automation

Penetration Testing Platform Introduces Interface for SIEM Integration, Public and Private Cloud Deployments and Post-Exploitation Macros

BOSTON, MA - July 26, 2011 - [Rapid7](#), the leading provider of security risk intelligence solutions, today announced the launch of Metasploit® Pro 4.0: a [penetration testing](#) solution that enables defenders to respond to the changing threat landscape by identifying and understanding security holes in their enterprise infrastructure. This new version is designed to better meet enterprise needs by offering integrations with other elements of security risk intelligence ecosystems, a range of deployment models and a number of features for automated penetration testing. By reducing the cost and complexity of security testing, Metasploit Pro 4.0 enables enterprises to conduct broader and more frequent security audits to prevent data breaches.

"Organizations looking to reduce data breach risks need smarter and more efficient security risk intelligence. One way to get this is through frequent, broad-scale penetration testing," said HD Moore, Rapid7's chief security officer and Metasploit chief architect. "The new features of Metasploit Pro 4.0 make this a practical reality for defenders by automating penetration testing workflow steps, better integrating with vulnerability management solutions and introducing new interfaces for SIEM systems."

Metasploit Pro 4.0 provides security professionals with a better view of their threat landscape by integrating with more than a dozen [vulnerability management](#) and Web application scanners, and by providing data to security information and event management (SIEM) systems through a documented interface. This enables defenders to identify vulnerabilities that could lead to a data breach and prioritize their remediation more effectively. Security teams increase their productivity by spending less time fixing unimportant vulnerabilities and have an effective way to verify that remediation was successful. Rapid7's own vulnerability management solution, Nexpose® uniquely offers even greater integration with Metasploit Pro through documented, supported APIs that enable Metasploit Pro users to schedule new vulnerability scans and leverage data from decentralized locations running Nexpose scans.

"Metasploit Pro is the tool of choice for our penetration testing team and something that has helped mature our information security program. We leverage Metasploit Pro heavily in order to be precise and strategic in what we go after, which has given us invaluable visibility into our tangible risk exposures," said Dave Kennedy, chief information security officer of Diebold, a Rapid7 Metasploit Pro and Nexpose customer. "There are so many aspects that we love about Metasploit Pro, from the knowledge-sharing collaboration capabilities to the ability to reproduce vulnerabilities and exposures. We're really looking forward to seeing even greater collaboration and automation features in the new version, as well as the increased capabilities and performance of Meterpreter."

The new version also offers support for both public and private cloud deployments. Defenders leveraging the public cloud can now easily conduct external penetration tests from Metasploit Pro in the Amazon Elastic Compute Cloud (Amazon EC2). Metasploit Pro is available as an Amazon Machine Image (AMI) making external penetration tests from the cloud quick, easy and inexpensive. Organizations using virtualization technologies such as VMware vSphere to underpin a private cloud deployment can now easily penetration test remote sites.

The new capabilities in Metasploit Pro 4.0 now enable defenders to:

Integrate security risk intelligence

- Integrate Metasploit Pro with your security information and event management (SIEM) system to improve your dashboard information
- Import scan results from more than a dozen third-party Web application scanners and vulnerability assessment tools to prioritize vulnerabilities and eliminate false positives
- Increase productivity in your security team by integrating Metasploit Pro with Nexpose vulnerability management solutions to directly access vulnerabilities that need to be verified



- Automate verification of vulnerabilities and reporting through new programming interface and XML results
- Easily document compliance with FISMA reports that map findings to controls and requirements

Deploy in a way that works for you

- Install on Windows, Ubuntu, or Red Hat Enterprise Linux
- Provision a VMware image to your data centers with VMware vSphere
- Host an Amazon Machine Image (AMI) in Amazon Elastic Compute Cloud (Amazon EC2)

Automate penetration testing steps

- Automatically gather evidence with customizable post-exploitation
- Re-establish dropped shells with persistent sessions and listeners
- Replay previously successful attacks to verify remediation
- Easily crack encrypted passwords offline
- Remotely control Metasploit Pro through a programming Interface (RPC API)
- Pull penetration testing reports from Metasploit Pro in an XML format

Metasploit Pro 4.0 is based on the [Metasploit Framework](#), the most widely used and mature penetration testing solution in the market with more than one million unique downloads and the world's largest, public collection of quality-assured exploits. The Metasploit Framework is continuously updated and version 4.0 marks the inclusion of 36 new exploits, 27 new post-exploitation modules and 12 auxiliary modules, all added since the release of version 3.7.1 in May 2011. These additions include nine new SCADA exploits, improved 64-bit Linux payloads, exploits for Firefox and Internet Explorer, full-HTTPS and HTTP Meterpreter stagers, and post-exploitation modules for dumping passwords from Outlook, WSFTP, CoreFTP, SmartFTP, TotalCommander, BitCoin and many other applications. For more information on the ongoing development of the Metasploit Framework, please visit the [Metasploit blog](#).

In addition to Metasploit Pro, Rapid7 also offers [Metasploit Express](#) as an entry-level option for vulnerability verification and penetration testing. With a reduced feature set from Metasploit Pro, Metasploit Express is optimized for security professionals who need an accessible and affordable penetration testing solution to verify the findings of their vulnerability scanners without extensive training.

For more information about learning to use Metasploit Pro to help prevent data breaches, please attend Rapid7's Webinar, "[HD Moore Offers Personal Sneak Preview of New Metasploit Version](#)" at 2:00 p.m. - 3:00 p.m. EST on Thursday, July 28th 2011.

Pricing and Availability

Metasploit Pro 4.0 is available from August 2011. For information on pricing please contact info@rapid7.com. To learn more, visit <http://www.rapid7.com/products/metasploit-pro.jsp>.

About Rapid7

Rapid7 is a leading provider of IT security risk management software. Its integrated [vulnerability management](#) and [penetration testing](#) products, Nexpose and Metasploit, and [mobile risk management](#) solution, Mobilisafe, enable defenders to gain contextual visibility and manage the risk associated with the IT environment, users and threats relevant to their organization. Rapid7's simple and innovative solutions are used by more than 2,000 enterprises and government agencies in more than 65



countries, while the Company's free products are downloaded more than one million times per year and enhanced by more than 175,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by *Inc. Magazine* and as a "Top Place to Work" by the *Boston Globe*. Its products are top rated by Gartner®, Forrester® and *SC Magazine*. The Company is backed by Bain Capital and Technology Crossover Ventures. For more information about Rapid7, please visit <http://www.rapid7.com>.