

Rapid7 presents penetration testing to the enterprise with Metasploit Pro release

Analyst: Andrew Hay

Following on the heels of its Metasploit Express release in May, **Rapid7** has launched the latest product in its penetration-testing portfolio – Metasploit Pro. Aimed at professional penetration-testing teams, auditors and consulting organizations, Metasploit Pro looks to further enhance the polish and commercial appeal of **Metasploit**, which Rapid7 acquired in October 2009.

The 451 take

We consider this release the next evolution in Rapid7's commercial Metasploit product roadmap. Metasploit Express gave the company's customers a glance at how they could either interweave penetration-testing methodology and tools into their existing vulnerability management process or even bring penetration-testing exercises back in-house. We like the teaming features of Metasploit Pro and suspect that the ability to collaboratively work on testing projects will likely be an attractive enticement for large organizations with disparate follow-the-sun testing teams.

Being open to running in parallel with other products in adjacent or sometimes-similar sectors has certainly helped Rapid7's proliferation. Qualys already integrates with Metasploit, so it's not inconceivable that other vulnerability management vendors will seek out Rapid7 to add penetration-testing functionality to their own wares in the near future. Should this happen, vendors like Core and Immunity might see the penetration-testing space become very crowded, very quickly.

Designed with professional penetration testers and security auditors in mind, Metasploit Pro expands upon the automated penetration-testing engine capabilities that the company included in the Metasploit Express release. The Pro version of the software boasts several new features, including a new multiuser 'team testing' capability, social engineering component, VPN pivoting, antivirus evasion and Web vulnerability support in addition to a new customized reporting engine.

The collaborative team testing is an interesting feature, especially for large organizations with disparate teams or team members dedicated to specific tasks – for example, the separation of discovery, vulnerability identification and exploitation duties. Metasploit Pro also includes the ability to craft targeted phishing emails for social-engineering portions of the penetration exercise. Client-side exploits can be attached to emails, as can custom binary payloads. Leveraging Metasploit Pro's VPN pivoting functionality, testers can pivot through an

exploited host using a virtual network kernel driver (TUN/TAP) hooked into the targeted host, acting as a sniffer. To evade antivirus scanners, Metasploit Pro first signs the executable templates with a self-signed certificate. Next, the payload is placed inside the actual signature section of the binary. By using this trick, Rapid7 claims that the payload is not detected, and that code-signing and application-whitelisting characteristics remain intact.

Web application scanning, auditing and exploitation capabilities have also been added to Metasploit Pro to allow users to search for Web forms and active content for vulnerabilities and exploit those detected. Leveraging the Anemone open source project, Metasploit Pro can search for, and exploit, cross-site scripting vulnerabilities in addition to remote and local file-inclusion vulnerabilities. Reporting has also been enhanced with customizable report templates and the ability to upload custom JasperReports JRXML-formatted templates.

From a corporate strategy angle, Rapid7 has continued its promiscuous integration stance with Metasploit Pro and continues to expose the ability for third-party tools to absorb derived data in the form of the product's XML-formatted results. The company admits that many of its customers run a combination of vendor products to meet organizational vulnerability and penetration-testing objectives. For example, some of its customers use both Rapid7's NeXpose vulnerability management product in tandem with **Core Security Technologies'** CORE IMPACT, while others use NeXpose internally and **Qualys** for external vulnerability scans.

Metasploit Pro is priced on a per-user basis and comes in at \$15,000 per user. Metasploit Express has a price tag of \$3,000 and is tailored to independent penetration testers just starting their practice or organizations with limited funding. Metasploit Pro, however, is aimed at established penetration-testing or security audit organizations. Although Rapid7 is very promiscuous in its integration strategy, there are obvious benefits to combining both Metasploit Pro and the company's flagship NeXpose vulnerability management product – something we suspect Rapid7 is counting on for upsell and cross-sell opportunities.

Competition

In the commercial penetration-testing space, Rapid7 will continue to face pressure from traditional competitors Core Security Technologies' CORE IMPACT and **Immunity Inc's** CANVAS. In addition to its head-to-head rivals, Rapid7 will also feel crowded by the likes of **Mu Dynamics**, **SAINT Corporation** and **BreakingPoint Systems** in addition to vulnerability management vendors like **Lumension Security**, **Critical Watch**, **nCircle**, **Qualys**, **McAfee (Foundstone)**, **StillSecure**, **Tenable Network Security**, **Trustwave**, **Shavlik Technologies**, **Cenzic**, **eEye**, **GFI Software** and Sweden's **Outpost24**. Specific to Web application penetration testing and vulnerability discovery, Rapid7 will likely encounter **IBM (Ounce Labs and Watchfire)**, **Hewlett-Packard (SPI Dynamics and Fortify Software)**, **Protegrity (Kavado)**, **Acunetix**, **Armorize Technologies**, **WhiteHat Security** and **Cenzic**, among others. Competition also comes from companies like **Gleg** and **Argeniss** that offer commercially available exploits.

Professional penetration testers, many of whom work as independents or as members of an organization's internal testing team, may be reluctant to switch to a 'professional' edition of the open source Metasploit framework. Similarly, those who wield individual tools such as Nmap, Netcat, dsniff, sqlmap, fasttrack, enum, LdapMiner, Ncrack, Maltego, hping2 and Cain in addition to bootable CD distributions like Samurai WTF or BackTrack, are not Metasploit Pro's target audience. That being said, these free tools will continue to provide competition to Rapid7 and its rivals, especially within cash-strapped organizations.

Reproduced by permission of The 451 Group; copyright 2009-10. This report was originally published within The 451 Group's Market Insight Service.

For additional information on The 451 Group or to apply for trial access, go to:
www.the451group.com