www.internetnews.com/dev-news/article.php/3776831

Back to Article

Metasploit 3.2 Offers More 'Evil Deeds'

By Sean Michael Kerner
October 8, 2008

TORONTO -- Hacking into systems (albeit for testing purposes) is apparently getting easier with the upcoming open source Metasploit 3.2 framework, according to its creator.

During a packed presentation at that SecTor conference here yesterday, Metasploit creator H. D. Moore detailed some of the new features in the upcoming Metasploit 3.2 release. They include names such as Browser AutoPwn, Metasploit in the Middle and the Evil Wireless Access Point.

"For http we do a whole bunch of evil things to a browser," Moore said, addressing an audience of security and networking professionals from sectors such as government and leading corporations. Many attend the conference in order to stay up to date on vulnerability assessments and how hackers exploit networks.

Metasploit is an open source attack framework first developed by Moore in 2003. With the Metasploit 3.0 release, the project has moved to an all Ruby programming base, which Moore credits with quickening development and exploits.

Take the context map payload feature, which encodes attack shellcode. Moore claimed that the new feature will make it even more difficult to detect attack code.

Getting attack code onto a target machine will also be easier on Metasploit 3.2 with improvements to the Raw Packet Tools function. A new library call PacketFu is expected by Moore to achieve packet injection for both wired and wireless end points.

It also provides improved support for exploiting multi-core CPU machines, which had been more difficult to attack with previous versions of Metasploit.

Metasploit is also able to take exploit code and weaponize it in an .EXE (executable file) that can be deployed by an attacker. Moore said the EXE template that created EXE attacks has been improved in Metasploit 3.2 in order to defeat AntiVirus vendor signature detection.

Moore boasted that he is using the same resources that the anti-virus vendors are using to identify virus signatures to ensure that the Metasploit EXE template is not identified.

If that wasn't enough, Metasploit 3.2 will include a new super weapon that will make exploiting browsers a trivial matter. The new Browser Autopwn feature is a client side auto attack system that will fire up exploits automatically against a user's browser with the goal of providing a shell into the browser.

Man in the middle attacks are also addressed in the package features. Moore explained that Metasploit in the Middle Feature puts the attack framework in between the users and their intended location. The man in the middle approach could be used to spoof DNS or to create a fake access point.

"It will abuse the HTTP security model, stealing cookies and saved form data," Moore said.

And if that's not enough to give security researchers a taste of the latest developments in security vulnerabilities, there is the Evil Wireless Access Point feature. Moore said it

can create an access point that consumes all other access points around it. Adding insult to evil, it has the ability to spoof any access point that is already on a user's preferred access point list. Browsers beware.

Last but certainly not least in this testing culture, Moore announced that Metasploit 3.2 now has full IPv6 support.

"The US Government has a mandate for IPv6 support, so there is at least one target there for you," Moore said.

Let the testing begin.