Metasploit 3.0

Metasploit 3.0: The Middle of the End of the End of the Middle?

by

Aaron Grothe, CISSP, NSA IAM/IEM, Security+

September 19, 2007

My Background

- Currently “doing time” as an Oracle DBA
- Am currently looking into web-enabling an Oracle Database, bringing up a lot of concerns
- Member of NEbraskaCERT for 5+ years now
- In no way is this talk supported/endorsed by my current employer

3 Years Ago

- I did a talk on a then new tool called Metasploit
- I believed at the time it would change the way we do exploit testing
- I was arguably right :-)

Intro Quote Credit

“Now this is not the end. It is not even the beginning of the end. But it is perhaps, the end of the beginning.” - Winston Churchill

From my talk 3 years ago

Disclaimer

“In some cases ... the knife can turn savagely upon the person wielding it ... You use the knife carefully, because you know it doesn't care who it cuts.” -- Steven King

Three Things you'll hopefully walk away from this talk with

- Metasploit is arguably the standard for exploit testing
- Standardized testing is the next logical step in vulnerability assessments
- I should try Metasploit, if I haven't already

Problems Metasploit Solves

- How can I verify that the patch or workaround I applied worked?
- How can I trust exploit code that I found on the net?
- How can I demonstrate an exploit to the non-technical?
- I'm a script kiddie without the skillz/time to do any work and want to pwn some systems

Typical Usage of Metasploit in 5 easy steps

I. Pick an Exploit
II. Check whether victim is susceptible
III. Chose payload
IV. Chose Encoding Technique
V. Execute Exploit

Pick an Exploit

- About 200 exploits are part of Metasploit 3.0
- Some CVEs are including Metasploit exploit samples in them
- CVE-2007-1465 a potential CVE has exploit code as part of the description

Payloads

- Command execution
- File access
- VNC access
- Remote Shells

Encoding Techniques

- Attempts to bypass IPS and IDS systems
- Can also use SSL for access if supported

How is 3.0 different than 2.0?

- Written in Ruby
- Wifi Tools
- Fuzzing Tools
- New license
- Offset Database

Ruby?

- Ruby is another programming language
- Many consider it to be a more readable perl
- Old Metasploit was a hodge podge of Perl/C/Assembler and python
- Ruby on Rails is currently the most high profile Ruby Project -

Ruby? (Cont)

- Metasploit is one of the largest Ruby projects in terms of code size ~100k lines
- One of the reasons the project was rewritten in Ruby was to make it work better on Microsoft Windows

New License

- Metasploit 2.0 was licensed under the GPL V2 and Artistic Licenses
- Metasplit 3.0 is licensed under the Metasploit Framework License
- Neither Metasploit 3.0 or any of its modules can be sold for more than distribution costs
- License reviewed by the Hacker Foundation
- Commercial Modules can be created -

New License (Cont)

- Not aware of any attempt to fork the 2.x version under the old license
- This has happened with the following projects
- ssh -> openssh
- x11 -> X.org
- nessus -> gnessus, openvas -

Why no Fork?

- The four main developers contributed most of the code
- They have a smaller number of users compared to the other projects
- Created a pretty acceptable license
- Have not done an obvious “land grab”

New License (cont)

- Attempt to lay the ground work for a revenue stream
- Sourcefire – snort – 30 day wait for new rules
- Tenable – Nessus – 7 wait for new vulns. Closed source.
- Heimdall Linux – Versions with Common Criteria Certification

WiFi Tools

- Includes a wrapped version of the LoRCon tools
- Just another set of exploits
- Opens up new devices to exploits
- Can't wait to see the first Linksys exploits

Fuzzing aka Fuzz Testing

- Provide Random or Semi-Random data to a program seeing what happens
- If the program crashes or does something weird it is worth investigating
- Might be the beginnings of a buffer overflow attack

Offset Database

- Windows 3.1 -> Windows 3.11. What was its purpose? Break OS/2 Windows for Warp?
- Techniques such as PIE/NX are making it harder to execute some exploits
- A lot of windows patches shove addresses around making it harder to execute an exploit
- The offset database gives clues on offsets to try

Semi Demo

- Going to show a flash video of using the VNC injection payload to break into a locked Windows desktop and monitor the user

Tips for Metasploit

- Metasploit requires a decent machine to run
- Metasploit can be run on a Nokia N770, but is supposed to be horrible
- If you run with a headless server, metasploit by default only listens on localhost:5555, change this to the IP address if you want to run it remotely

Metasploit Competitors

- Core Security's Impact
- Immunity's Canvas
- Saint Corporation's SaintExploit

- Core Security's Impact Single user License costs about $25k

Size of the Metasploit Community

- It has passed 250k downloads for all versions
- about 100k people have registered for updates
- Windows outnumbers Linux/Mac OS X downloads by 10 to 1

How to get 3.0

- Source Package is available
http://www.metasploit.org

- Live CDs
- Backtrack has Metasploit 3.0 on it
http://remote-exploit.org/backtrack.html
- Fedora Custom spin for Security
currently has metasploit on its wishlist
http://fedoraproject.org/wiki/CustomSpins

How to get 3.0

- Microsoft Windows has a typical installer for it

- Mac OS X
- requires using Fink or Darwin Ports or possibly Gentoo for Mac OS X for Ruby
- After getting ruby. Install the Unix version from source

How to get 3.0

- Gentoo Linux has an ebuild for 3.0
- Metasploit.org has documentation for installing on Fedora/Debian/Ubuntu

How much do I use Metasploit?

- Not that much lately.
- Being able to demonstrate exploits is useful, but even then it requires people to understand that they have been exploited
- With 3.0's wifi tools and fuzzing tools. I'm planning on getting back into it again

Other Stuff at Metasploit

- They have started doing some very cool stuff with anti-forensics and the wifi/fuzzing stuff is just beginning
- Checkout their website at http://www.metasploit.org

References

- Metasploit 3.0 Licensing Change – Article on techtarget
- http://tinyurl.com/34f73u
- Metasploit 3.0 book at Wikibooks
- http://en.wikibooks.org/wiki/Metasploit/Cor

Contact Info

- You can get in touch with me at ajgrothe@gmail.com