An Introduction to the Metasploit Framework

Mike Tetreault, CISSP
Macrocosmic Technologies

And now, the four disclaimers

- The intention of this presentation is for educational purposes only.
- Should you chose to use the framework, any consequences borne are yours and yours alone.
- Even in “defanged” mode, the Metasploit framework has the ability to affect, impair, and destroy both data and systems.
- Use only with systems for which you have explicit authorization, and can rebuild should the need arise.

What is the Metasploit Framework?

- Penetration tester tool
- Remote vulnerability assessment tool
- Script kiddie dream
- “The Metasploit Framework is a complete environment for writing, testing, and using exploit code. This environment provides a solid platform for penetration testing, shellcode development, and vulnerability research.” –MSF User Crash Course

Terminology used in this presentation

- MSF modules:
  - Exploits
  - Payloads
  - Encoders
  - Nops
- Application memory organization:
  - Code, data, stack, heap
- Application vulnerabilities:
  - Buffer Overflow
  - Heap Overflow

Metasploit Framework features

- Written in PERL – Easy to add code and plug-ins to
- Built-in support for encoding, debugging, logging, and more
- Well-designed API that is flexible, modular, scalable, and easy to use
- Support for differing network technologies allows for developing protocol-dependent code
- Free Open Source Software

Metasploit Framework's competitors

- CORE IMPACT
  - $25k or so per year
  - Supports pivoting
  - Written in Python and C++
- Immunitysec CANVAS
  - More limited syscall proxying
  - Less extensive than CORE IMPACT
  - MUCH less expensive – Roughly $1300
- How is MSF different?

Three primary environments

- msfconsole
- msfcli
- msfweb
- When do you use each?

msfupdate – Windows Update in reverse

- Imagine if you could contact a website to receive the latest and greatest in exploit code and payloads. Now you can!
- Offers updates to exploits, payloads, encoders, nops, and program code

Advanced topics

- Impurity
- Meterpreter
  - aka Meta-Interpreter
- PassiveX payloads
- InlineEgg Python payloads
- Chainable proxies
- VNC server DLL injection

Metasploit Framework 2.5 released Tuesday 10/18

- 32 new exploits
- 105 exploits, 74 payloads total
- Improved proxy support
- Numerous bug fixes
- Smaller Win32 installer
- Dozens of cosmetic changes

What's up for Metasploit 3.0?

- Alpha Due 12/15/2005
- Written in Ruby, not Perl
- Improved automation of exploitation through scripting
- Simplify the process of writing an exploit
- Increase code re-use between exploits
- Improve and generically integrate evasion techniques
- Support automated network discovery and event correlation through *recon* modules
- Continue to provide a friendly outlet to cutting edge exploitation technology

Demo

- Install MSF to your workstation
- Launch the MSF web server
- Run through a couple of demos
- Help with any questions—Time allowing

Resources

- http://www.metasploit.com
  - http://www.metasploit.com/links.html
  - http://metasploit.com:55555/
- framework-subscribe@metasploit.com
- LiveCD's
  - FreeBSD-based freshports
  - Knoppix-based Auditor Linux
- Slides will be posted at http://www.macrocosmictech.com/
- Questions: mikeatmacrocosmictechdotcom