Metasploit

Metasploit

- An open-source framework for developing, testing, and using exploit code.
- A tool that lets users customize known vulnerabilities with varying payloads and encoders into specific exploits.
- A set of of tools to help generate new exploits that can be added to the Metasploit framework.

Metasploit Console

- Comes with 158 exploits & 76 payloads ‘out-of-the-box’.

- Users can mix and match exploits, targets, payloads, and encoders to create a unique exploit for any occasion.

- Demo

Metasploit Advanced

- The Meterpreter - A special payload to allow in-process command injection.
- PassiveX Payloads – Arbitrary ActiveX execution on remote machines
- Impurity ELF Injection – Allows arbitrarily complex C programs to be exectued in memory on remote machines.
- Win32 DLL Injection Payloads – Remotely injects a user created DLL into the target process.
- VNC Server DLL Injection – On exploit, will launch a VNC server and take control of the current desktop session

Writing Exploits

- Metasploit comes with many helpful tools and libraries to write exploits.
- Pex::Text::PatternCreate() - a way to find buffer overflow offsets
- Opcode DB – finding instructions to execute
- Msfpayload – taking advantage of the entire set of Metasploit payloads

Adding to the Metasploit Framework

- Metasploit 2.7 allows you to write a PERL module to take your custom exploit and include it in the console listing.

- Users define the basic fields seen on the ‘info exploit_name’ screen in the console.

- Example

The End

- In summary, Metasploit is cool.

- Questions?

www.metasploit.com
www.acm.uiuc.edu/sigmil/