LOUISVILLE METASPLOIT CLASS

David "ReL1K" Kennedy
Martin "PureHate" Bos
Elliott "Nullthreat" Cutright
pwrcycle
Adrian “Irongeek” Crenshaw

http://Irongeek.com

Thanks to

The ISSA Officers for getting this organized
http://www.issa-kentuckiana.org/

The Speakers:
David "ReL1K" Kennedy, Martin "PureHate" Bos, Elliott "Nullthreat" Cutright, pwrcycle

TippingPoint for Lunch
http://www.tippingpoint.com/

HD Moore and crew for the tools
http://www.metasploit.com/

Metasploit Unleashed/Offensive Security team for the docs
http://www.offensive-security.com/metasploit-unleashed/

Johnny Long for the charity work
http://www.hackersforcharity.org/

Bunch of others who I'm forgetting, but who also helped…

INTRO TO METASPLOIT

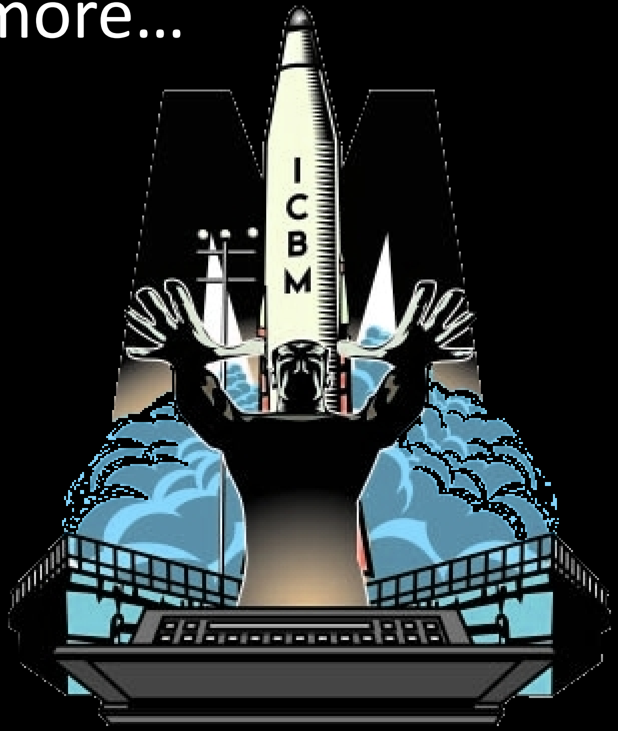
Adrian Crenshaw

About Adrian

- I run Irongeek.com
- I have an interest in InfoSec education
- I don't know everything - I'm just a geek with time on my hands

What is Metasploit?

- An exploitation framework
- Written in Ruby
- Includes: Exploits, Payloads, Auxiliaries, Automation Tools, Lots more…



Some Terminology

- Exploit
  The vector for getting into the system, whether it be because of a vulnerability or a bad config
- Payload
  What you want the exploit to do.
- Encoders
  Ways to mangle the code so anti-malware apps won’t detect the payload
- Auxillary
  Just another fun little app that comes with Metasploit

A bit about payload types

- Inline
  All the shellcode to be executed goes with the payload. More stable, but may be too big.
- Staged
  The payload is just a small stub that grabs the rest of the shell code after the exploit works. Smaller, and less for AV to grab a hold of.
- Reverse
  Instead of having to establish a connection in after an exploit works, the payload connects back you. This has a better chance of getting around firewalls with weak egress filtering.
- NoNX
  These payloads try to work around things like DEP (Data Execution Prevention)

The simple side

- My part is just an intro, Metasploit is much more that just:

1. Set Exploit
2. Set Payload
3. Set Target
4. “Pop a box” TM

- But it is also that. ☺

Ways to interface with the MSF

- Msfconsole

  +Most well suported of the interfaces
  +Pretty much all options are avaliable
  -Not as point and click as msggui/msfweb

- Msfcli

  +Easy to add Metasploit goodness to your scripts

  -Not as well supported as msfconsole

  -Harder to use

- Msfweb

  +Pretty interface

  +Easy to read descriptions

  +Good for showing management the easy of exploitation

  -Not as well supported as msfconsole

  -Slower

- Msfgui

  + Pretty interface

  -No longer being maintained

Basic MSFConsole Commands

- Anything you can run from the command line
- help
- search
- set
- setg
- show (options/advanced/etc)
- exploit/run
- sessions –l
- sessions -i 1

Demo Fun!!!