ISA 564
SECURITY LAB

Metasploit Framework
The Metasploit Framework

- **What is it?**
  - An extensible platform for developing and using exploits
  - A collection of standardized exploits and payloads

- **Why does it matter?**
  - No comparable open source solution
  - Useful as a learning and test tool
  - The “standard” in non-commercial exploits
Ethics

- **Should security tools be restricted?**
  - Registered, license requirement, etc
  - Would raise the entry level for attackers
    - But are those type really a threat, and would advanced attackers be impacted?
    - Criminal by definition break laws
      - Would policy do more than provide a good feeling?
      - What could policy put into law enforcement’s toolbox?
  - But make it harder for white hats
    - To pentest your own network or to train new people

- **Straw-man comparisons to kinetic weapons**
  - They are just tools, like a hammer, that only inherit intent from user
  - You could use a hammer to break a window or build a swing
What we will cover

- The framework in general
- Directory structure
- Modules
- Exploits
- Payloads
Metasploit v3.2 -- Architecture

- **custom plugins**
  - msfconsole
  - msfcli
  - msfweb
  - msfwx
  - msfapi

- **libraries**
  - rex
  - framework-core
  - framework-base

- **protocols**
  - protocol tools

- **interfaces**
  - interfaces

- **security tools**
  - security tools

- **web services**
  - web services

- **integration**
  - integration

- **modules**
  - exploits
  - payloads
  - encoders
  - nops
  - auxiliary
Pre-installed on Kali

- From terminal run
  - msfconsole or msfvenom

- Source located at
  - /usr/share/metasploit-framework

- Ignore the hostname and paths visible in the following two slides
  - They reference an older isa564 lab VM
  - Use the path above on Kali
Example payload: `shell_bind_tcp.rb`
Documentation

- Documentation & Support:
  http://www.metasploit.com/framework/support/
  - Installation
  - Metasploit Framework User Guide
  - Metasploit Framework Developer Guide
  - Meterpreter Guide
The following slides are taken from

http://opensecuritytraining.info/HTID.html

I recommend scanning the various slides from that course if you want to learn more details