

# Metasploit

- What is it?
- How does it work?
- Features

# Metasploit - what is it?

- Framework for developing and executing exploit code.
- Cross Platform (runs on Linux, Windows, OSX)
- Many interfaces (web, console, GUI, CLI)
- Open Source
- Great tool for automated pentesting
- Completely rewritten in Ruby (v.3.0+ )

# Metasploit – how does it work?

- Two main modules:
  - Exploits (breaking in)
  - Payloads (mischief tools)
- Workflow:
  1. Select appropriate exploit to get your foot in
  2. Select a payload to deliver
  3. Configure the payload
  4. Execute the new dynamically created exploit
  5. PWN

# Metasploit - features

- Over 262 ready exploits and 177 payloads
- IDS/IPS evasion options
- Scriptable (for automation)
- Create packaged executable payloads
- Reporting tools
- Concurrent exploits and sessions
- Pivoting (used compromised hosts to launch new attacks)

# Metasploit – building an exploit

- Target program: FileCOPA 1.01 (osvdb 27389)
- Vulnerable to Buffer Overflow
- Improper bounds-checking in the LIST function allows specially crafted requests to overwrite the stack.
- Tools needed:
  - Metasploit 3.1 +
  - OllyDBG
  - Windows

# Script Kiddie Cheat Sheet

- 1. show exploits
- 2. use <exploit name>
- 3. show payloads
- 4. set PAYLOAD <payload name>
- 5. info
- 6. set <CONFIG NAME> <setting>
- 7. exploit
- 8. PWN!