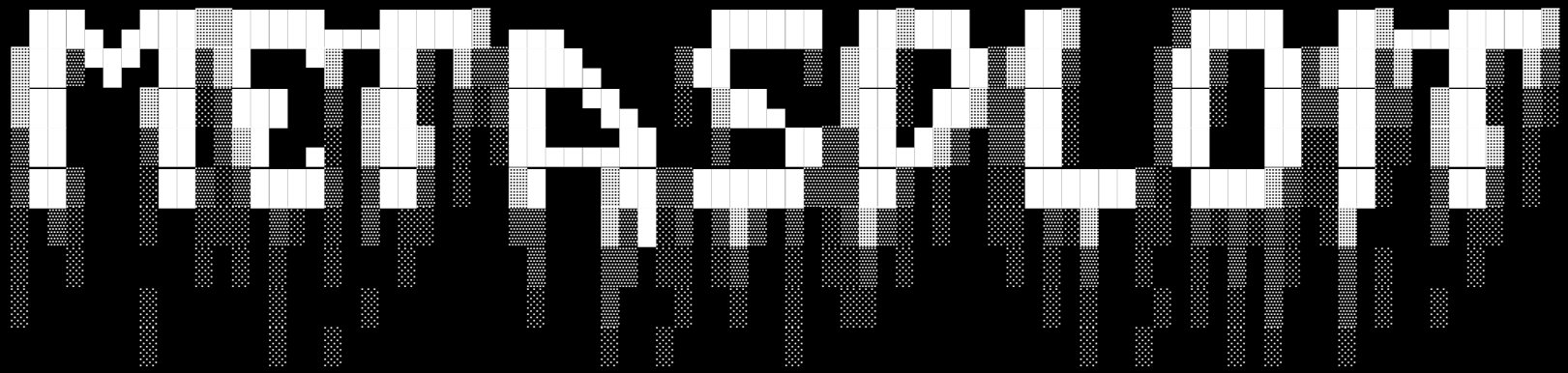
metasploit

Metasploit Framework

- A tool for developing and executing exploit code
- Created by HD Moore in 2003 in Perl
- In 2007 it was rewritten in Ruby
- In 2009 the project was acquired by Rapid7
- Commercial offerings are similar to Immunity's Canvas product and Core Security's Core Impact

Editions

- Metasploit Framework – free command line
- Metasploit Community – free web based
- Metasploit Express – not free (lite edition)
- Metasploit Pro – really expensive
- Armitage – GUI for Metasploit framework
- Cobalt Strike – Armitage + more stuff

Auxiliary Modules

- Modules that do not contain a shell payload for exploitation
- Perform scanning, fuzzing, sniffing, and other probing and information gathering functions
- Admin – allows for connecting and running commands on certain services like DBs
- Scanner – scans for and enumerates various services on the network
- Server – poses as server and captures credentials as users login

Exploitation Modules

- Active Exploits
  - Exploit a specific host, run until completion, and exit
    - Usually server side attacks against services running on a remote host
- Passive Exploits
  - Wait for incoming hosts and exploit them as they connect
    - Usually client side attacks against things like web browsers, file browsers (FTP), etc.
    - Also can encompass executable payloads sent via email, XMPP, etc.

Post Exploitation Modules

- Once a shell/access is obtained
- Privilege escalation
- Dumping hashes
- Clearing logs
- Keylogging, screenshots, searching for files
- Enabling Remote Desktop
- Pivoting to other networks

Meterpreter

- A payload that is somewhere between a shell and malware
- Makes a lot of common tasks easy
  - Dumping hashes
  - Keylogging
  - Screenshots
  - File searching
  - Process injection
- Provides persistence and speed

Payload Generation

- msfpayload can be used to generate payloads
- Hundreds of options
- Can generate in a variety of formats from exe's to Jars to just plain bytecode
- Output can be piped to msfencode to get rid of certain characters like \x00\xd0\x0a

Exploit Development Tools

- Tools commonly used during the exploitation process are available
  - pattern_create.rb
    - Create a pattern to send to a buffer for offset determination
  - pattern_offset.rb
    - Find out where an input overrides a desired value/register
  - nsam
    - A quick way to turn assembly into byte code
  - msfpayload
    - Hundreds of payloads to drop into an exploit
  - msfencode
    - Encoding schemes to obfuscate shellcode and/or remove certain characters

Demo Time

Sources

- http://www.offensive-security.com/metasploit-unleashed/Main_Page
- https://en.wikipedia.org/wiki/Metasploit_Project