Metasploit

Julio Valcarcel
julio3@umbc.edu
umbccd-subscribe@lists.umbc.edu
Metasploit

- Exploitation framework
- Managed by Rapid7
  - http://www.rapid7.com/
- Can be found on Github
  - https://github.com/rapid7/metasploit-framework
- Runs on any Linux distribution
  - Pre-packed in pentesting oriented distributions
Metasploit

- Allows an attacker (White/Grey/Black Hat) to semi-automate tedious parts of exploitation
- Provides an intuitive interface to build upon
  - Other tools rely on Metasploit as a backend
    - Armitage
    - Social Engineering Toolkit
    - Beef
Metasploit

- Entire database of pre crafted exploits
  - High profile CVEs
  - [https://www.rapid7.com/db/](https://www.rapid7.com/db/)

- Meterpreter
  - Payload
  - Provides extended functionality to a typical shell
  - Allows to easily gain a stronger foothold
    - Upload custom malware
Metasploit Process

1. Gather Information
   a. Social Engineering
   b. Google

2. Enumerate targets
   a. Services
   b. Versions

3. Choose exploit
   a. Use info from first two steps to pick your attack vector

4. Launch exploit
   a. Exploit vulnerability
   b. Launch a meterpreter shell

5. Gain a foothold
   a. Upload malware (Rootkits/Trojan/etc)
Metasploit Demo
Social Engineering Toolkit (SET)

- Created by David Kennedy of TrustedSec
  - https://www.trustedsec.com
- Again can be found on GitHub
  - https://github.com/trustedsec/social-engineer-toolkit
- Provides an easy way to integrate metasploit and social engineering
- Many different tools and options
  - Mass emailer
  - Spear phishing
  - Web attacks
SET Demo
Questions?