Metasploit Tips and Tricks

SecTor 2010
Ryan Linn
Introduction

- Information Security Engineer at SAS Institute
- Columnist for EthicalHacker.net
- Contributor for Metasploit, Browser Exploitation Framework (BeEF), Nikto and others
Agenda

- Discussion of Goals
- Overview of Demonstrations
- Demonstrations
- Questions/Comments
Goals

- Get up to speed with Metasploit
- Learn new techniques
- Ideas for automation
- Awareness of new features
Demo Overview

- Metasploit Basics Overview
- Pivoting Demo
- Payload Creation Demo
- Enumeration Automation Demo
Initial Walkthrough

- What is Metasploit
- Basic Usage
- Basic Exploit
- Payloads
Pivoting Demo

- We have one host in a DMZ with only port 80 exposed
- This website has a vulnerability
- Exploit the host then evaluate VLAN where host is present
- Secondary exploitation of non-exposed systems
Payload Creation Demo

- Payload creation with encoding has never been easier
- Create payload through msfconsole
- Create payload through script
- Use template
Enumeration Demo

- Automating enumeration through scripts
- Start with one token from pass the hash
- How far can that get us?
- Meterpreter scripting + Python = Elevate until Success
Data Sharing Demo

- Use Metasploit for vulnerability storage
- Import Nmap/Nessus/Qualys/etc
- Import Nikto/BeEF etc
- Aggregate Information
- Immediately actionable data
Questions/Comments?

- Contact Info:
  - Email: sussurro@happypacket.net
  - Twitter: @sussurro
  - Websites: http://www.ethicalhacker.net

- Training:
  - SANS 560: Good network pen testing class
  - Offensive Security PWB: Great class for hands on pen testing
Thanks!

- Thanks to SecTor staff
- Thank you for coming
- If you have any questions, feel free to contact me