Metasploit 201: The Journeyman’s Guide to Metasploit

What is it?

Metasploit offers the information security professional a dense collection of attack exploits, payloads, post-exploitation tools and more. Making sense of it all involves first understanding all of the components and how they work together. This two-day interactive class will walk you through some advanced product features and techniques for network penetration testing with the console version of Metasploit Pro. Additionally, concepts related to automation and scripting will be explored to help better incorporate Metasploit into your organization’s risk assessment and vulnerability management programs. This is a highly interactive class and the student will be engaged through a combination of lectures and hands-on lab exercises.

Audience and prerequisites

Geared toward security professionals already comfortable with Metasploit Pro/Express and penetration testing techniques, this hands-on training session is perfect for individuals within an organization who have been tasked with penetration testing, systems security or information security.

Ideally, attendees should have experience with the following:

- Basic knowledge of network protocols
- Comfortable with Linux command shells (bash)
- Vulnerability management system knowledge
- Penetration testing knowledge
- Prior experience using Metasploit

What is the course content?

- Penetration Testing Methodology Refresher – Attendees will get a refresher on penetration testing methodology and process: Discover, Gain Access, Take Control, Collect Evidence
- The “CLI” – MSFConsole, MSFEncode and MSFPayload – Attendees will learn about the command line features of the Metasploit Framework and how it interacts with Metasploit Pro/Express
- Advanced Techniques – In a sprint fashion we will dive into time-boxed activities on the following techniques: Post Exploitation, Macros, Abusing Trusts, Privilege Escalation, Furthering Access, Evasion and Pivoting
- Scenario X – During this portion of the course we will pit your skills against a multitude of common scenarios to test and facilitate the growth of your own pen testing process
Course Agenda

DAY 1
The first day of the class involves deep technical discussion around the command line version of Metasploit Pro. The discussion will focus on core concepts related to the various components and configuration options related to the core console, exploit modules and payload modules. Associated tools, such as msfpayload, msfencode, and msfvenom will be reviewed. Likewise, a variety of active and passive attack types will be discussed.

› The Metasploit Console
› Working With The Backend Database
› The Role Of Metasploit Modules
› A Basic Understanding Of Exploits Modules
› A Basic Understanding Of Payload Modules
› Payload Generation Using msfpayload, msfencode and msfvenom
› A Basic Understanding of Meterpreter
› A Discussion of Workflow And Methodology
› Hands-On Exercises That Explore These Concepts As They’re Presented

DAY 2
The second day of the class involves a series of time-boxed exercises that offer a variety of real-world attack scenarios and their execution. This phase of the class includes step-by-step instructions to accomplish a variety of lab activities. For those looking for a more robust challenge, some alternative goals are outlined. During the second half of this day, the student will be provided access to a live environment that features a variety of technical challenges. This phase is designed to push not only your knowledge and experience with Metasploit but also challenge the student to approach problems creatively and seek out attack vectors that are not immediately obvious.

› Discovering Targets
› Gaining Access
› Taking Control
› Privilege Escalation
› Trust Abuse
› Scripting & Automation
› Putting It All Together – Testing Your Aptitude! During this portion of the course we will pit your skills against a multitude of common scenarios to test and facilitate the growth of your own pen testing process

What is the cost?

› Open-enrollment class - $2,000 per student
› On-site class - $7,000 per course plus travel & expenses, up to 5 attendees
› Applicable CPEs: 16

Want to get started?
Call: 866.7.RAPID7 Email: sales@rapid7.com Schedule: http://www.rapid7.com/services