Metasploit Pro Certified Specialist: A New User's Guide to Metasploit Pro

What is it?

You don't need to be an expert pen-tester to identify security risks or confirm vulnerabilities with the aid of Metasploit Pro. This two-day interactive class provides the information necessary for attendees to be able to jumpstart usage of Metasploit Pro.
The ***virtual*** class, which is hosted on a Rapid7 lab and delivered remotely, provides instructor led training and labs on using Metasploit Pro following the logical steps including creating a project, host discovery, service port and operating system identification, various methods of exploitation, evidence collection, and the creation of various reports. The training includes a series of lab exercises where users can apply what they have learned in a fun, yet educational, pentest scenario against a set of target hosts.

Customers who participate in training ***on-site*** will experience hands-on opportunities to apply learned skills in a fun, yet educational, simulation using their own environment.

All participants will have access to **the Metasploit Pro Certified Specialist Exam** as part of their training program. Leverage the knowledge gained as part of the class to become a certified specialist and stand out from the crowd!

Audience and prerequisites

Geared toward security professionals new to Metasploit Pro and penetration testing techniques. This hands-on training session is perfect for individuals within an organization who have been tasked with vulnerability validation or penetration testing using Metasploit Pro as the primary tool.

Ideally, attendees should have experience with the following:

- Experience with Windows® and Linux Operating Systems
- Basic knowledge of network protocols
- Basic vulnerability management system knowledge
- Knowledge of penetration testing concepts

What is the course content?

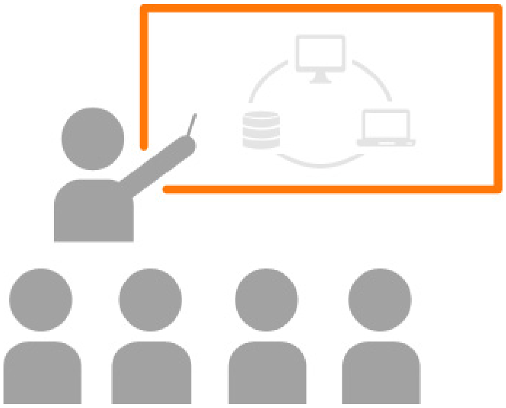
- Metasploit Pro – Product overview and key feature descriptions
- Navigating the GUI – The web interface (GUI) is introduced and demonstrated for administration tasks and working with projects for penetration testing
- Network Scanning – Covers active scanning, network/device enumeration, and importing vulnerability scan data from other products
- Exploitation Techniques - Various techniques for gaining access to hosts using targeted exploits, automated exploitation, and brute-force attacks
- Maintaining Access and Privilege Escalation – Alternative access techniques and privilege escalation methods, including client-side exploits, local system access, and persistence
- Pass The Hash and Pivoting - Take advantage of "pass-the-hash", pivoting, and credential dumping to extend your attack across the network.
- Web Application Testing – Use Metasploit's web application vulnerability scanning and exploitation capabilities.
- Social Engineering – Techniques for utilizing Metasploit Pro to simulate drive-by attacks and spear phishing in order to identify user awareness training gaps.
- Quick Start Wizards and MetaModules – Experience the ease and functionality of the built-in wizards (for quick pentests, web app testing, and campaigns) and the new MetaModules which simplify testing by automating common, complicated security tests
- Reporting – Standard and custom reporting of progress, results, and collected evidence plus data exports for archival or backups

Course Agenda

Day 1

The first day of class provides an introduction to Metasploit Pro and focuses on key foundational knowledge that you will build upon throughout the course. Emphasis will be placed on the Metasploit Pro console, project workflow, understanding of the various modules and payloads, and exploitation techniques. Students will gain practical, hands-on experience in the following areas:

- Metasploit Pro Introduction
- A Discussion of Workflow And Methodology
- Navigating the GUI
- Metasploit Tasks
- Discovering Targets
- Importing Scan Data
- An Overview of Exploits Modules
- Basic Exploitation Techniques
- Password Brute force Exploitation Technique
- Pass-The-Hash Exploitation Technique
- Pivot Attacks
- An Overview of Payload Modules
- An Overview of Command Shell/Meterpreter Payloads



Day 2

The second day of class students build upon the knowledge and skills covered in the first day of class and covers additional exploitation techniques, identification and exploitation of web application vulnerabilities, an overview of conducting a social engineering campaign and generating reports. Students will gain practical, hands-on experience in the following areas:

- Post-Exploitation Techniques
- Maintaining Access and Privilege Escalation
- Web Application Testing/Exploitation
- Demonstration of Metasploit Social Engineering Campaign
- Quick Start Wizards and MetaModules
- Reporting

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