

Free Armitage and Metasploit Video Training Course

By Raphael Mudge, Armitage Creator

Armitage is a front-end for Metasploit that allows team collaboration and exposes the advanced features of the framework. Raphael Mudge has made a six-part training series on Armitage and Metasploit for the ethicalhacker.net community. These demonstration-heavy lectures introduce the penetration testing process and walk you through each step. You'll learn how to break into hosts, carry out post-exploitation activities, develop more access from your initial foothold, and you'll do this in a team environment.

These lectures were initially created for the Austin, TX ISSA and OWASP half-day Metasploit training event in June. Elated after several tex-mex meals, Raphael recorded these lectures for us. If you're new to penetration testing and want to understand Metasploit and Armitage, these lectures are for you. Also, be sure to read *Hacking Linux with Armitage* from February 2011. Enjoy the training!

del.icio.us

[Discuss in Forums {mos_smf_discuss:Special Events}](#)

1. Introduction

This lecture introduces penetration testing, this course, and the overall network penetration testing process.

2. Metasploit

This lecture introduces the Metasploit Framework and Armitage. By the end of this lecture, you will understand Metasploit, the vocabulary around it, and how to work in the Metasploit console.

3. Access

This lecture teaches you how to use Metasploit to break into hosts. You'll learn how to hack without exploits, use client-side attacks, and launch the right remote exploit when applicable.

4. Post-Exploitation

This lecture teaches what to do after you break into a host. You'll learn how to interact with a host, browse files, steal keystrokes, kill programs, and use Metasploit's powerful post-exploitation modules. Armitage's logging features are covered as well.

5. Maneuver

The last step is to take your access and turn it into more access. This lecture shows how to use Metasploit's pivoting to get at otherwise unreachable hosts, scan through a pivot, dump hashes, and abuse a Windows Active Directory domain.

6. Team Tactics

Now you know the whole network attack process, but you'll rarely work alone. This lecture shows you how to use the teaming features of Armitage to accomplish everything from the previous lectures. You'll learn how to use Armitage for real-time communication, data sharing, and session sharing. Finally, you'll also learn how to use external tools with Metasploit's pivoting ability.

Lab

The Austin, TX version of this training also included a hands-on lab and exercises. You just need VMWare Player, Metasploit, and the Metasploitable virtual machine to play along.

The instructions call for a Mint-9 Virtual Machine as well. This virtual machine is a standard Mint Linux distribution that Raphael installed Java and the Java plugin onto. Replace references to this VM with any VM capable of running Java applets in a browser.

If you'd like to try this lab out, the materials are available at:

<http://codebazaar.blogspot.com/2011/06/introduction-to-metasploit-and-armitage.html>

Further Resources

The following resources were mentioned throughout these lectures:

- Metasploit Unleashed Course
- Metasploit: The Penetration Tester's Guide
- Metasploit Homepage
- Armitage Documentation and Resources
- BackTrack Linux
- Penetration Testing and Vulnerability Analysis Class at NYU:Poly

About the Author

Raphael Mudge is a Washington, DC based security engineer. He's created several projects including jIRCii, Sleep, and After the Deadline. He's now working on Armitage, a cyber attack management tool for Metasploit. You can contact him at <http://www.hick.org/~raffi/>.