

Introduction to Pentesting with Metasploit

Objective

Pentesting is hard. It's even harder to figure out how to get started on this journey. This bootcamp is aimed at absolute beginners and to give them an easy to understand learning path. Metasploit is one of the most popular tools around and we will use it to help teach the basics of pentesting.

The focus of this bootcamp is to familiarize you with how to use Metasploit and perform pentesting on Linux and Windows machines. The bootcamp will cover various phases of pentesting with Metasploit, we will also take a look at how to write custom metasploit modules to automate attacks.

Completing the bootcamp will equip you to pentest Windows and Linux machines with Metasploit in real-world engagements.

Prerequisites

- A basic knowledge of computers and networking
- Familiarity with any Linux and Windows OS

Course Content

Module I: Metasploit Fundamentals

- Framework Organization
- Exploits
- Payloads
- Encoders
- Databases
- Meterpreter

Module II: Reconnaissance

- Network Scanning
- Port Scanning
- Service Enumeration

Module III: Identifying Vulnerabilities and Exploitation

- Web Applications
- Web Servers
- Database Servers
- RMI Servers
- WMI
- WinRM

Module IV: Post Exploitation

- File and Keylogging
- Screen Capture
- Mimikatz
- Enabling Remote Desktop
- Enabling WinRM
- Pass the hash (PsExec)
- Token Stealing and Incognito
- Stdapi and Priv Extensions
- Kiwi and Extapi Extensions
- Espia and Sniffer Extensions

Module V: Privilege Escalation

- Basic Misconfigurations
- Vulnerable services
- UAC Bypass
- DLL Hijacking
- Kiwi and Extapi Extensions
- Espia and Sniffer Extensions

Module VI: Pivoting

- Port Forwarding
- Socks Proxy

Module VII: Maintaining Access

- Tampering Registry
- Scheduled Tasks
- Leveraging WMI
- Service Backdoors

Module VIII: Custom Modules and Scripts

- Meterpreter Scripting
 - Meterpreter API Basics
 - Writing Meterpreter Scripts
- Writing Metasploit Modules

For Learnworlds:

Pentesting with Metasploit

Familiarize yourself with how to use Metasploit to its full extent while performing pentesting on Windows and Linux machines.

What's included?

Bootcamp Completion Certificate

Get a course completion certificate on attending all 5 live sessions.

5 live sessions, 2.5 hour each session, over 50 lab exercises

What will you learn?

[Use the entire objective paragraphs above]

Weekly 2.5h sessions start at 12:00pm ET and end at 2:30pm ET.

Live Session Schedule

Week 1	Metasploit Fundamentals and Reconnaissance
Week 2	Exploitation
Week 3	Post Exploitation Part I

Week 4	Post Exploitation Part II
Week 5	Metasploit Modules and Scripting

Social media copies