Metasploit 5.0 for Beginners

Second Edition

Perform penetration testing to secure your IT environment against threats and vulnerabilities

Sagar Rahalkar

Packt
www.packt.com

Metasploit 5.0 for Beginners
Second Edition

Perform penetration testing to secure your
IT environment against threats and vulnerabilities

Sagar Rahalkar

Packt

BIRMINGHAM—MUMBAI

Metasploit 5.0 for Beginners
Second Edition

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Commissioning Editor: Vijin Boricha
Acquisition Editor: Rohit Rajkumar
Senior Editor: Rahul Dsouza
Content Development Editor: Alokita Amanna
Technical Editor: Sarvesh Jaywant
Copy Editor: Safis Editing
Project Coordinator: Neil Dmello
Proofreader: Safis Editing
Indexer: Pratik Shirodkar
Production Designer: Aparna Bhagat

First published: July 2017
Second edition: April 2020

Production reference: 1080420

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.
ISBN 978-1-83898-266-9

`www.packt.com`

Contributors

About the author

Sagar Rahalkar is a seasoned **InfoSec (IS)** professional, having 13 years of comprehensive experience in various verticals of IS. His domains of expertise are mainly cybercrime investigations, digital forensics, AppSec, VAPT, compliance, and IT GRC. He holds a master's degree in computer science and several industry-recognized certifications, such as Certified Cyber Crime Investigator, CEH, ECSA, ISO 27001 LA, IBM certified Specialist-Rational AppScan, CISM, and PRINCE2. He has been closely associated with Indian law enforcement agencies for more than 3 years, dealing with digital crime investigations and related training, and has received several awards and appreciation from senior officials of the police and defense organizations in India.

About the reviewers

Vaibhav Tole (MCA, CCISO, CRISC, CISA, CEH, Prince2 Foundation) is a multidisciplinary Cyber Security Professional with wide experience in areas including cyber threat intelligence, anti-cybercrime investigations, big data analytics, incident response advisory, vulnerability assessment, application and product security, IS risk, and project management. Apart from being a cybersecurity professional, Vaibhav is an accomplished musician (a pianist with a Grade 8 – Piano Solo from Trinity College London) and a composer and has also founded a band named RURRER. His special interests include conceptualizing and implementing cross-functional interdisciplinary projects in fields such as computational music, healthcare, and IS.

Parag Patil is an IS professional currently associated with Qualys Incorporation as a manager for cloud security and compliance research. For more than 10 years, Parag has extensively worked on digital forensics, IAM, security monitoring/Sec-OPs, security training, security compliance audits, vulnerability management, penetration testing, and IS research. He is the author of CIS benchmarks for AWS, Azure, and GCP.

Thanks to my friends Mahesh Navaghane and Sagar Rahalkar (the author of this book), my sister, Aditi Sahasrabudhe, and my wife, Monika, and daughter, Ira, who have always been there for me through all the ups and downs I have ever experienced in my life.

Packt is searching for authors like you

Table of Contents

Preface

Section 1: Introduction and Environment Setup

1 Introduction to Metasploit and Supporting Tools

2 Setting Up Your Environment

3

Metasploit Components and Environment Configuration

Section 2: Practical Metasploit

4

Information Gathering with Metasploit

5
Vulnerability Hunting with Metasploit

6
Client-Side Attacks with Metasploit

7
Web Application Scanning with Metasploit

8

Antivirus Evasion and Anti-Forensics

9

Cyber Attack Management with Armitage

10

Extending Metasploit and Exploit Development

11

Case Studies

Other Books You May Enjoy

Preface

For more than a decade or so, the use of technology has been rising exponentially. Almost all businesses are partially or completely dependent on the use of technology. From Bitcoin to the cloud to the Internet of Things (IoT), new technologies are popping up each day. While these technologies completely change the way we do things, they also bring threats along with them. Attackers discover new and innovative ways to manipulate these technologies for fun and profit! This is a matter of concern to thousands of organizations and businesses around the world. Organizations worldwide are deeply concerned about keeping their data safe. Protecting data is certainly important; however, testing whether adequate protection mechanisms have been put in place is equally important. Protection mechanisms can fail, hence testing them before someone exploits them for real is a challenging task. Having said that, vulnerability assessment and penetration testing have gained great importance and are now trivially included in all compliance programs. With vulnerability assessment and penetration testing done in the right way, organizations can ensure that they have put in the right security controls and they are functioning as expected! For many, the process of vulnerability assessment and penetration testing may look easy just by running an automated scanner and generating a long report with false positives. However, in reality, this process is not just about running tools but a complete life cycle. Fortunately, the Metasploit Framework can be plugged into almost every phase of the penetration testing life cycle, making complex tasks easier. This book will take you through some of the absolute basics of Metasploit Framework 5.x to the advanced and sophisticated features that the framework has to offer!

Who this book is for

If you are a penetration tester, ethical hacker, or security consultant who wants to quickly learn the Metasploit Framework to carry out elementary penetration testing in highly secured environments, then this book is for you. This book also targets users who have a keen interest in computer security, especially in the area of vulnerability assessment and penetration testing, and who want to develop practical skills in using the Metasploit Framework.

What this book covers

Chapter 1, *Introduction to Metasploit and Supporting Tools*, introduces the reader to concepts such as vulnerability assessment and penetration testing. Then, it explains the need for a penetration testing framework along with a brief introduction to the Metasploit Framework. Moving ahead, the chapter explains how the Metasploit Framework can be effectively used across all stages of the penetration testing life cycle, along with some supporting tools that extend the Metasploit Framework's capabilities. This chapter also introduces some of the new features of Metasploit 5.x.

Chapter 2, *Setting up Your Environment*, guides you through setting up the environment for the Metasploit Framework. This includes setting up the Kali Linux virtual machine, independently installing the Metasploit Framework on various platforms (such as Windows and Linux), and setting up exploitable or vulnerable targets in the virtual environment, along with Metasploit Vulnerable Services Emulator.

Chapter 3, *Metasploit Components and Environment Configuration*, covers the structure and anatomy of the Metasploit Framework, followed by an introduction to various Metasploit components. This chapter also covers the local and global variable configuration, along with how to keep the Metasploit Framework updated.

Chapter 4, *Information Gathering with Metasploit*, lays the foundation for information gathering and enumeration with the Metasploit Framework. It covers information gathering and enumeration for various protocols, such as TCP, UDP, FTP, SMB, HTTP, SSH, DNS, and RDP. It also covers extended usage of the Metasploit Framework for password sniffing, along with advanced search for vulnerable systems using Shodan integration.

Chapter 5, *Vulnerability Hunting with Metasploit*, starts with instructions on setting up the Metasploit database. Then, it provides insights on vulnerability scanning and exploiting using NMAP, Nessus, and the Metasploit Framework, concluding with the post-exploitation capabilities of the Metasploit Framework. It also provides a brief introduction to MSF utilities.

Chapter 6, *Client-Side Attacks with Metasploit*, introduces the key terminology related to client-side attacks. It then covers the usage of the msfvenom payload creator to generate custom payloads, along with the Social-Engineer Toolkit. The chapter concludes with advanced browser-based attacks using the `browser_autopwn` auxiliary module.

Chapter 7, *Web Application Scanning with Metasploit*, covers the procedure of setting up a vulnerable web application such as Hackazon and OWASP Juice Shop. It then covers the wmap module within the Metasploit Framework for web application vulnerability scanning, and concludes with some additional Metasploit auxiliary modules that can be useful in web application security assessment.

Chapter 8, *Antivirus Evasion and Anti-Forensics*, covers the various ways to prevent your payload from getting detected by various antivirus programs. These techniques include the use of encoders, binary packages, and encryptors, along with the latest evasion modules. The chapter also introduces various concepts for testing payloads and concludes with various anti-forensic features of the Metasploit Framework.

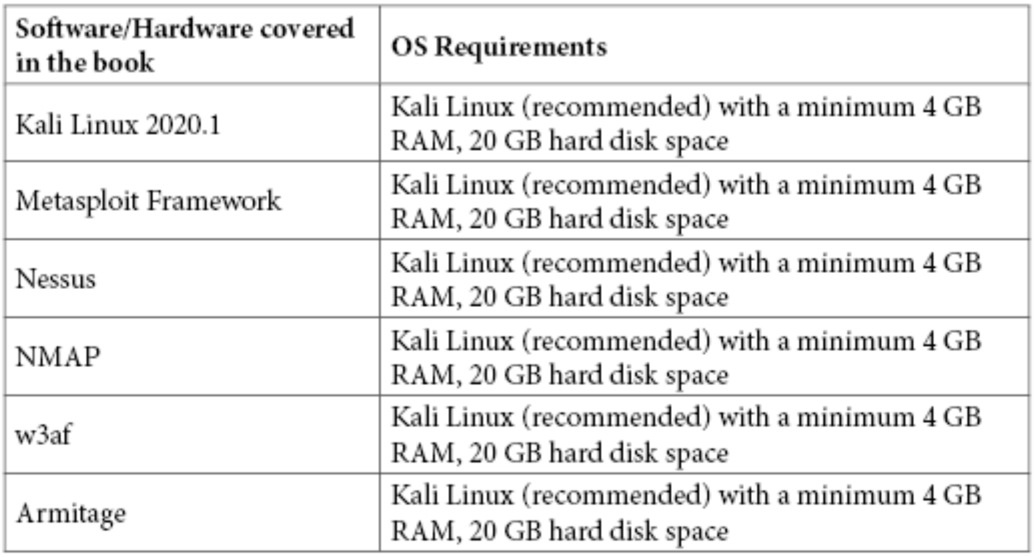
Chapter 9, *Cyber Attack Management with Armitage*, introduces a cyber attack management tool called Armitage, which can be used effectively along with the Metasploit Framework for complex penetration testing tasks. This chapter covers the various aspects of Armitage, including opening the console, performing scanning and enumeration, finding suitable attacks, and exploiting the target.

Chapter 10, *Extending Metasploit and Exploit Development*, introduces the various exploit development concepts, followed by how the Metasploit Framework can be extended by adding external exploits. The chapter concludes with an explanation of the Metasploit exploit templates and mixins that can be readily utilized for custom exploit development.

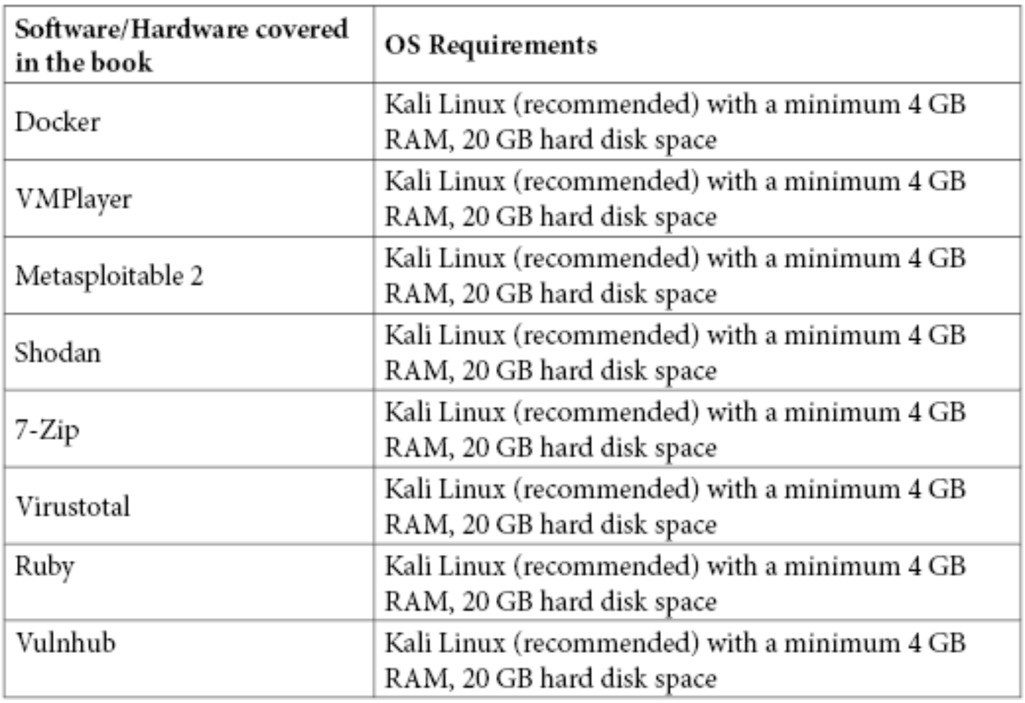
Chapter 11, *Real-World Case Study*, helps the reader to put all the knowledge they have learned throughout the book together to hack into targets in real-world scenarios. This will immensely help the reader to understand the practical importance of all the modules and plugins they've learned about throughout the book.

To get the most out of this book

You require the following:



Software/Hardware covered in the book	**OS Requirements**
Kali Linux 2020.1	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
Metasploit Framework	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
Nessus	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
NMAP	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
w3af	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
Armitage	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space



Software/Hardware covered in the book	OS Requirements
Docker	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
VMPlayer	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
Metasploitable 2	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
Shodan	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
7-Zip	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
Virustotal	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
Ruby	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space
Vulnhub	Kali Linux (recommended) with a minimum 4 GB RAM, 20 GB hard disk space

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `http://www.packtpub.com/sites/default/files/downloads/9781838982669_ColorImages.pdf`.

Conventions used

There are a number of text conventions used throughout this book.

`Code in text`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: "Download and install the `msi` file."

A block of code is set as follows:

```
#include <stdio.h>
void AdminFunction()
{
printf("Welcome!\n");
printf("You are now in the Admin function!\n");
}
void echo()
{
char buffer[25];
printf("Enter any text:\n");
scanf("%s", buffer);
printf("You entered: %s\n", buffer);
}
int main()
{
echo();
return 0;
}
```

Any command-line input or output is written as follows:

```
root@kali:~#apt-get  install  nmap
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "Click on the **Hosts** menu."

> **Tips or important notes**
>
> Appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packtpub.com/support/errata`, selecting your book, clicking on the Errata Submission Form link, and entering the details.

Piracy: If you come across any illegal copies of our works in any form on the Internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions, we at Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit `packt.com`.

Section 1: Introduction and Environment Setup

You will learn to setup the Metasploit environment efficiently before getting into the details of the framework.

This section comprises the following chapters:

Chapter 1, Introduction to Metasploit & Supporting Tools

Chapter 2, Setting Up your Environment

Chapter 3, Metasploit Components and Environment Configuration

1
Introduction to Metasploit and Supporting Tools

Before we take a deep dive into various aspects of the Metasploit Framework, let's first lay a solid foundation of some of the absolute basics. In this chapter, we'll conceptually understand what penetration testing is all about and where the Metasploit Framework fits in exactly. We'll also browse through some of the additional tools that enhance the Metasploit Framework's capabilities.

In this chapter, we will cover the following topics:

- The importance of penetration testing
- Understanding the difference between vulnerability assessments and penetration testing
- The need for a penetration testing framework
- Introduction to Metasploit
- Introduction to new features in Metasploit 5.0
- When to use Metasploit
- Making Metasploit effective and powerful using supplementary tools

Technical requirements

The following software is required:

- Kali Linux
- The Metasploit Framework
- Nessus
- NMAP
- w3af
- Armitage

The importance of penetration testing

For over a decade or so, the use of technology has been rising exponentially. Almost all businesses are partially or completely dependent on the use of technology. From Bitcoins to the cloud to the **Internet of Things** (**IoT**), new technologies are popping up each day. While these technologies completely change the way we do things, they also bring along threats with them. Attackers discover new and innovative ways to manipulate these technologies for fun and profit! This is a matter of concern for thousands of organizations and businesses around the world.

Organizations worldwide are deeply concerned about keeping their data safe. Protecting data is certainly important. However, testing whether adequate protection mechanisms have been put to work is also equally important. Protection mechanisms can fail, hence, testing them before someone exploits them for real is a challenging task. Having said this, vulnerability assessments and penetration testing have gained high importance and are now trivially included in all compliance programs. If the vulnerability assessment and penetration testing is done correctly, it significantly helps organizations gain confidence in the security controls that they have put in place and that they are functioning as expected!

We will now move on to understanding the difference between vulnerability assessments and penetration testing.

Understanding the difference between vulnerability assessments and penetration testing

Vulnerability assessments and penetration testing are two of the most common phrases that are often used interchangeably. However, it is important to understand the difference between the two. To understand the exact difference, let's consider a real-world scenario.

A thief intends to rob a house. To proceed with his robbery plan, he decides to recon his robbery target. He visits the house (that he intends to rob) casually and tries to gauge what security measures are in place. He notices that there is a window at the back of the house that is often open and so it's easy to break in. In our terms, the thief just performed a vulnerability assessment. Now, after a few days, the thief actually goes to the house again and enters through the back window that he had discovered earlier during his recon phase. In this case, the thief performed an actual penetration into his target house with the intent of robbery.

This is exactly what we can relate to in the case of computing systems and networks. You can first perform a vulnerability assessment of the target in order to assess the overall weaknesses in the system and then later perform a planned penetration test to practically check whether the target is vulnerable or not. Without performing a vulnerability assessment, it would be difficult to plan and execute the actual penetration.

While most vulnerability assessments are non-invasive by nature, the penetration test could cause damage to the target if not done in a controlled manner. Depending on the specific compliance needs, some organizations choose to perform only a vulnerability assessment, while others go ahead and perform a penetration test as well.

Now that we have understood the difference between vulnerability assessments and penetration testing, let's move on to understand the need for a penetration testing framework.

The need for a penetration testing framework

Penetration testing is not just about running a set of a few automated tools against your target. It's a complete process that involves multiple stages and each stage is equally important for the success of the project. Now, for performing all the tasks throughout every stage of penetration testing, we would need to use various tools and might need to perform some tasks manually. Then, at the end, we would need to combine the results from all the different tools together to produce a single meaningful report. This is certainly a daunting task. It would be really easy and timesaving if one single tool could help us perform all the required tasks for penetration testing. This exact need is satisfied by a framework such as Metasploit.

Now let's move on to learning more about the Metasploit Framework.

Introduction to Metasploit

The birth of Metasploit dates back to 16 years ago, when H. D. Moore, in 2003, wrote a portable network tool using Perl. By 2007, it was rewritten in Ruby. The Metasploit project received a major commercial boost when Rapid7 acquired the project in 2009. Metasploit is essentially a robust and versatile penetration testing framework. It can literally perform all the tasks that are involved in a penetration testing life cycle. With the use of Metasploit, you don't really need to reinvent the wheel! You just need to focus on the core objectives, the supporting actions will all be performed through various components and modules of the framework. Also, since it's a complete framework and not just an application, it can be customized and extended as per our requirements.

Metasploit is, no doubt, a very powerful tool for penetration testing. However, it's certainly not a magic wand that can help you hack into any given target system. It's important to understand the capabilities of Metasploit so that it can be leveraged optimally during penetration testing.

> **IMPORTANT NOTE:**
>
> Did you know? The Metasploit Framework has more than 3,000 different modules available for exploiting various applications, products, and platforms, and this number is growing on a regular basis.

While the initial Metasploit project was open source, after the acquisition by Rapid7, commercial-grade versions of Metasploit also came into existence. For the scope of this book, we'll be using the Metasploit Framework edition.

Introduction to new features in Metasploit 5.0

Ever since the Metasploit Framework was born 16 years ago, it has been through significant changes and improvements. In early 2019, Metasploit 5.0 was released, which is considered its first major release since 2011. While the Metasploit is commercially supported and developed by Rapid7, it also has rich community support, which enables its growth.

The latest Metasploit 5.0 version brings in a lot more features and improvements:

- **Database and automation API's**: The latest Metasploit 5.0 now allow users to run the database as a RESTful service. It also introduces the new JSON-RPC API, which would be of significant help to users who wish to integrate Metasploit with other tools. The API interface can be extremely handy in several automation and orchestration scenarios. It thus makes the framework even more agile and powerful.