

## Metasploit The Penetration Tester39s Guide Ebook

If you ally obsession such a referred Metasploit The Penetration Tester39s Guide Ebook books that will pay for you worth, get the no question best seller from us currently from several preferred authors. If you desire to humorous books, lots of novels, tale, jokes, and more fictions collections are as well as launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every ebook collections Metasploit The Penetration Tester39s Guide Ebook that we will totally offer. It is not something like the costs. Its practically what you compulsion currently. This Metasploit The Penetration Tester39s Guide Ebook, as one of the most operational sellers here will enormously be in the middle of the best options to review.



### The Ultimate Kali Linux Book Packt Publishing Ltd

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine-based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

### GPEN GIAC Certified Penetration Tester All-in-One Exam Guide Packt Publishing Ltd

An easy to digest practical guide to Metasploit covering all aspects of the framework from installation, configuration, and vulnerability hunting to advanced client side attacks and anti-forensics. About This Book Carry out penetration testing in highly-secured environments with Metasploit Learn to bypass different defenses to gain access into different systems. A step-by-step guide that will quickly enhance your penetration testing skills. 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. What You Will Learn Get to know the absolute basics of the Metasploit framework so you have a strong foundation for advanced attacks Integrate and use various supporting tools to make Metasploit even more powerful and precise Set up the Metasploit environment along with your own virtual testing lab Use Metasploit for information gathering and enumeration before planning the blueprint for the attack on the target system Get your hands dirty by firing up Metasploit in your own virtual lab and hunt down real vulnerabilities Discover the clever features of the Metasploit framework for launching sophisticated and deceptive client-side attacks that bypass the perimeter security Leverage Metasploit capabilities to perform Web application security scanning In Detail This book will begin by introducing you to Metasploit and its functionality. Next, you will learn how to set up and configure Metasploit on various platforms to create a virtual test environment. You will also get your hands on various tools and components used by Metasploit. Further on in the book, you will learn how to find weaknesses in the target system and hunt for vulnerabilities using Metasploit and its supporting tools. Next, you'll get hands-on experience carrying out client-side attacks. Moving on, you'll learn about web application security scanning and bypassing anti-virus and clearing traces on the target system post compromise. This book will also keep you updated with the latest security techniques and methods that can be directly applied to scan, test, hack, and secure networks and systems with Metasploit. By the end of this book, you'll get the hang of bypassing different defenses, after which you'll learn how hackers use the network to gain access into different systems. Style and approach This tutorial is packed with step-by-step instructions that are useful for those getting started with Metasploit. This is an easy-to-read guide to learning Metasploit from scratch that explains simply and clearly all you need to know to use this essential IT power tool.

### Penetration Testing Basics Createspace Independent Publishing Platform

The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you'll learn the Framework's conventions, interfaces, and module system as you launch simulated attacks. You'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to: –Find and exploit unmaintained, misconfigured, and unpatched systems –Perform reconnaissance and find valuable information about your target –Bypass anti-virus technologies and circumvent security controls –Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery –Use the Meterpreter shell to launch further attacks from inside the network –Harness standalone Metasploit utilities, third-party tools, and plug-ins –Learn how to write your own

Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test, Metasploit: The Penetration Tester's Guide will take you there and beyond.

### Coding for Penetration Testers Pearson IT Certification

Build a better defense against motivated, organized, professional attacks Advanced Penetration Testing: Hacking the World's Most Secure Networks takes hacking far beyond Kali linux and Metasploit to provide a more complex attack simulation. Featuring techniques not taught in any certification prep or covered by common defensive scanners, this book integrates social engineering, programming, and vulnerability exploits into a multidisciplinary approach for targeting and compromising high security environments. From discovering and creating attack vectors, and moving unseen through a target enterprise, to establishing command and exfiltrating data—even from organizations without a direct Internet connection—this guide contains the crucial techniques that provide a more accurate picture of your system's defense. Custom coding examples use VBA, Windows Scripting Host, C, Java, JavaScript, Flash, and more, with coverage of standard library applications and the use of scanning tools to bypass common defensive measures. Typical penetration testing consists of low-level hackers attacking a system with a list of known vulnerabilities, and defenders preventing those hacks using an equally well-known list of defensive scans. The professional hackers and nation states on the forefront of today's threats operate at a much more complex level—and this book shows you how to defend your high security network. Use targeted social engineering pretexts to create the initial compromise Leave a command and control structure in place for long-term access Escalate privilege and breach networks, operating systems, and trust structures Infiltrate further using harvested credentials while expanding control Today's threats are organized, professionally-run, and very much for-profit. Financial institutions, health care organizations, law enforcement, government agencies, and other high-value targets need to harden their IT infrastructure and human capital against targeted advanced attacks from motivated professionals. Advanced Penetration Testing goes beyond Kali linux and Metasploit and to provide you advanced pen testing for high security networks.

### The Complete Metasploit Guide Packt Publishing Ltd

Evade antiviruses and bypass firewalls with the most widely used penetration testing frameworks Key FeaturesGain insights into the latest antivirus evasion techniquesSet up a complete pentesting environment using Metasploit and virtual machinesDiscover a variety of tools and techniques that can be used with Kali LinuxBook Description Penetration testing or ethical hacking is a legal and foolproof way to identify vulnerabilities in your system. With thorough penetration testing, you can secure your system against the majority of threats. This Learning Path starts with an in-depth explanation of what hacking and penetration testing is. You ' ll gain a deep understanding of classical SQL and command injection flaws, and discover ways to exploit these flaws to secure your system. You'll also learn how to create and customize payloads to evade antivirus software and bypass an organization's defenses. Whether it ' s exploiting server vulnerabilities and attacking client systems, or compromising mobile phones and installing backdoors, this Learning Path will guide you through all this and more to improve your defense against online attacks. By the end of this Learning Path, you'll have the knowledge and skills you need to invade a system and identify all its vulnerabilities. This Learning Path includes content from the following Packt products: Web Penetration Testing with Kali Linux - Third Edition by Juned Ahmed Ansari and Gilberto Najera-GutierrezMetasploit Penetration Testing Cookbook - Third Edition by Abhinav Singh , Monika Agarwal, et alWhat you will learnBuild and analyze Metasploit modules in RubyIntegrate Metasploit with other penetration testing toolsUse server-side attacks to detect vulnerabilities in web servers and their applicationsExplore automated attacks such as fuzzing web applicationsIdentify the difference between hacking a web application and network hackingDeploy Metasploit with the Penetration Testing Execution Standard (PTES)Use MSFvenom to generate payloads and backdoor files, and create shellcodeWho this book is for This Learning Path is designed for security professionals, web programmers, and pentesters who want to learn vulnerability exploitation and make the most of the Metasploit framework. Some understanding of penetration testing and Metasploit is required, but basic system administration skills and the ability to read code are a must.

### Penetration Testing: A Survival Guide Packt Publishing Ltd

Learn how to break systems, networks, and software in order to determine where the bad guys might get in. Once the holes have been determined, this short book discusses how they can be fixed. Until they have been located, they are exposures to your organization. By reading Penetration Testing Basics, you'll gain the foundations of a simple methodology used to perform penetration testing on systems and networks for which you are responsible. What You Will Learn Identify security vulnerabilities Use some of the top security tools to identify holes Read reports from testing tools Spot and negate common attacks Identify common Web-based attacks and exposures as well as recommendations for closing those holes Who This Book Is For Anyone who has some familiarity with computers and an interest in information security and penetration testing.

### Hacking with Kali Syngress

Get to grips with security assessment, vulnerability exploitation, workload security, and encryption with this guide to ethical hacking and learn to secure your AWS environment Key FeaturesPerform cybersecurity events such as red or blue team activities and functional testingGain an overview and understanding of AWS penetration testing and securityMake the most of your AWS cloud infrastructure by learning about AWS fundamentals and exploring pentesting best practicesBook Description Cloud security has always been treated as the highest priority by AWS while designing a robust cloud infrastructure. AWS has now extended its support to allow users and security experts to perform penetration tests on its environment. This has not only revealed a number of loopholes and brought vulnerable points in their existing system to the fore, but has also opened up opportunities for organizations to build a secure cloud environment. This book teaches you how to perform penetration tests in a controlled AWS environment. You'll begin by performing security assessments of major AWS resources such as Amazon EC2 instances, Amazon S3, Amazon API Gateway, and AWS Lambda. Throughout the course of this book, you'll also learn about specific tests such as exploiting applications, testing permissions flaws, and discovering weak policies. Moving on, you'll discover how to establish private-cloud access through backdoor Lambda functions. As you advance, you'll explore the no-go areas where users can't make changes due to vendor restrictions and find out how you can avoid being flagged to AWS in these cases. Finally, this book will take you through tips and tricks for securing your cloud

environment in a professional way. By the end of this penetration testing book, you'll have become well-versed in a variety of ethical hacking techniques for securing your AWS environment against modern cyber threats. What you will learn

Set up your AWS account and get well-versed in various pentesting services

Delve into a variety of cloud pentesting tools and methodologies

Discover how to exploit vulnerabilities in both AWS and applications

Understand the legality of pentesting and learn how to stay in scope

Explore cloud pentesting best practices, tips, and tricks

Become competent at using tools such as Kali Linux, Metasploit, and Nmap

Get to grips with post-exploitation procedures and find out how to write pentesting reports

Who this book is for

If you are a network engineer, system administrator, or system operator looking to secure your AWS environment against external cyberattacks, then this book is for you. Ethical hackers, penetration testers, and security consultants who want to enhance their cloud security skills will also find this book useful. No prior experience in penetration testing is required; however, some understanding of cloud computing or AWS cloud is recommended.

[Mastering Kali Linux for Advanced Penetration Testing](#) Packt Publishing Ltd

Hacking with Kali introduces you the most current distribution of the de facto standard tool for Linux pen testing. Starting with use of the Kali live CD and progressing through installation on hard drives, thumb drives and SD cards, author James Broad walks you through creating a custom version of the Kali live distribution. You'll learn how to configure networking components, storage devices and system services such as DHCP and web services. Once you're familiar with the basic components of the software, you'll learn how to use Kali through the phases of the penetration testing lifecycle; one major tool from each phase is explained. The book culminates with a chapter on reporting that will provide examples of documents used prior to, during and after the pen test. This guide will benefit information security professionals of all levels, hackers, systems administrators, network administrators, and beginning and intermediate professional pen testers, as well as students majoring in information security. Provides detailed explanations of the complete penetration testing lifecycle

Complete linkage of the Kali information, resources and distribution downloads

Hands-on exercises reinforce topics

[Metasploit for Beginners](#) John Wiley & Sons

Identify, exploit, and test web application security with ease

Key Features

Get up to speed with Metasploit and discover how to use it for pentesting

Understand how to exploit and protect your web environment effectively

Learn how an exploit works and what causes vulnerabilities

Book Description

Metasploit has been a crucial security tool for many years. However, there are only a few modules that Metasploit has made available to the public for pentesting web applications. In this book, you'll explore another aspect of the framework – web applications – which is not commonly used. You'll also discover how Metasploit, when used with its inbuilt GUI, simplifies web application penetration testing. The book starts by focusing on the Metasploit setup, along with covering the life cycle of the penetration testing process. Then, you will explore Metasploit terminology and the web GUI, which is available in the Metasploit Community Edition. Next, the book will take you through pentesting popular content management systems such as Drupal, WordPress, and Joomla, which will also include studying the latest CVEs and understanding the root cause of vulnerability in detail. Later, you'll gain insights into the vulnerability assessment and exploitation of technological platforms such as JBoss, Jenkins, and Tomcat. Finally, you'll learn how to fuzz web applications to find logical security vulnerabilities using third-party tools. By the end of this book, you'll have a solid understanding of how to exploit and validate vulnerabilities by working with various tools and techniques. What you will learn

Get up to speed with setting up and installing the Metasploit framework

Gain first-hand experience of the Metasploit web interface

Use Metasploit for web-application reconnaissance

Understand how to pentest various content management systems

Pentest platforms such as JBoss, Tomcat, and Jenkins

Become well-versed with fuzzing web applications

Write and automate penetration testing reports

Who this book is for

This book is for web security analysts, bug bounty hunters, security professionals, or any stakeholder in the security sector who wants to delve into web application security testing. Professionals who are not experts with command line tools or Kali Linux and prefer Metasploit's graphical user interface (GUI) will also find this book useful. No experience with Metasploit is required, but basic knowledge of Linux and web application pentesting will be helpful.

[Metasploit Bootcamp](#) Packt Publishing Ltd

Coding for Penetration Testers: Building Better Tools, Second Edition provides readers with an understanding of the scripting languages that are commonly used when developing tools for penetration testing, also guiding users through specific examples of custom tool development and the situations where such tools might be used. While developing a better understanding of each language, the book presents real-world scenarios and tool development that can be incorporated into a tester's toolkit. This completely updated edition focuses on an expanded discussion on the use of Powershell, and includes practical updates to all tools and coverage. Discusses the use of various scripting languages in penetration testing

Presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages

Provides a primer on scripting, including, but not limited to, web scripting, scanner scripting, and exploitation scripting

Includes all-new coverage of Powershell

[Practical Lock Picking](#) Packt Publishing Ltd

Exploit the secrets of Metasploit to master the art of penetration testing. About This Book

Discover techniques to integrate Metasploit with the industry's leading tools

Carry out penetration testing in highly-secured environments with Metasploit and acquire skills to build your defense against organized and complex attacks

Using the Metasploit framework, develop exploits and generate modules for a variety of real-world scenarios

Who This Book Is For

This course is for penetration testers, ethical hackers, and security professionals who'd like to master the Metasploit framework and explore approaches to carrying out advanced penetration testing to build highly secure networks. Some familiarity with networking and security concepts is expected, although no familiarity of Metasploit is required. What You Will Learn

Get to know the absolute basics of the Metasploit framework so you have a strong foundation for advanced attacks

Integrate and use various supporting tools to make Metasploit even more powerful and precise

Test services such as databases, SCADA, and many more

Attack the client side with highly advanced techniques

Test mobile and tablet devices with Metasploit

Understand how to Customize Metasploit modules and modify existing exploits

Write simple yet powerful Metasploit automation scripts

Explore steps involved in post-exploitation on Android and mobile platforms

In Detail

Metasploit is a popular penetration testing framework that has one of the largest exploit databases around. This book will show you exactly how to prepare yourself against the attacks you will face every day by simulating real-world possibilities. This learning path will begin by introducing you to Metasploit and its functionalities. You will learn how to set up and configure Metasploit on various platforms to create a virtual test environment. You will also get your hands on various tools and components and get hands-on experience with carrying out client-side attacks. In the next part of this learning path, you'll develop the ability to perform testing on various services such as SCADA, databases, IoT, mobile, tablets, and many more services. After this training, we jump into real-world sophisticated scenarios where performing penetration tests are a challenge. With real-life case studies, we take you on a journey through client-side attacks using Metasploit and various scripts built on the Metasploit framework. The final instalment of your learning journey will be covered through a bootcamp approach. You will be able to bring together the learning together and speed up and integrate Metasploit with leading industry tools for penetration testing. You'll finish by working on challenges based on user's preparation and work towards solving the challenge. The course provides you with highly practical content explaining Metasploit from the following Packt books: [Metasploit for Beginners](#) [Mastering Metasploit, Second Edition](#) [Metasploit Bootcamp](#)

Style and approach

This pragmatic learning path is packed with start-to-end instructions from getting started with Metasploit to effectively building new things and solving real-world examples. All the key concepts are explained with the help of examples and demonstrations that will help you understand everything to use this essential IT power tool.

[Wireshark for Security Professionals](#) Packt Publishing Ltd

This innovative new resource provides both professionals and aspiring professionals with clear guidance on how to identify and exploit common web application vulnerabilities. The book focuses on offensive security and how to attack web applications. It describes each of the Open Web Application Security Project (OWASP) top ten vulnerabilities, including broken authentication, cross-site scripting and insecure deserialization, and details how to identify and exploit each weakness. Readers learn to bridge the gap between high-risk vulnerabilities and exploiting flaws to get shell access. The book demonstrates how to work in a professional services space to produce quality and thorough testing results by detailing the requirements of providing a best-of-class penetration testing service. It offers insight into the problem of not knowing how to approach a web app pen test and the challenge of integrating a mature pen testing program into an organization. Based on the author's many years of first-hand experience, this book provides examples of how to break into user accounts, how to breach systems, and how to configure and wield penetration testing tools.

[Quick Start Guide to Penetration Testing](#) Packt Publishing Ltd

Master the art of penetration testing with Metasploit Framework in 7 days

About This Book

A fast-paced guide that will quickly enhance your penetration testing skills in just 7 days

Carry out penetration testing in complex and highly-secured environments. Learn techniques to Integrate Metasploit with industry's leading tools

Who This Book Is For

If you are a penetration tester, ethical hacker, or security consultant who quickly wants to master the Metasploit framework and carry out advanced penetration testing in highly secured environments then, this book is for you. What You Will Learn

Get hands-on knowledge of Metasploit

Perform penetration testing on services like Databases, VOIP and much more

Understand how to Customize Metasploit modules and modify existing exploits

Write simple yet powerful Metasploit automation scripts

Explore steps involved in post-exploitation on Android and mobile platforms. In Detail

The book starts with a hands-on Day 1 chapter, covering the basics of the Metasploit framework and preparing the readers for a self-completion exercise at the end of every chapter. The Day 2 chapter dives deep into the use of scanning and fingerprinting services with Metasploit while helping the readers to modify existing modules according to their needs. Following on from the previous chapter, Day 3 will focus on exploiting various types of service and client-side exploitation while Day 4 will focus on post-exploitation, and writing quick scripts that helps with gathering the required information from the exploited systems. The Day 5 chapter presents the reader with the techniques involved in scanning and exploiting various services, such as databases, mobile devices, and VOIP. The Day 6 chapter prepares the reader to speed up and integrate Metasploit with leading industry tools for penetration testing. Finally, Day 7 brings in sophisticated attack vectors and challenges based on the user's preparation over the past six days and ends with a Metasploit challenge to solve. Style and approach

This book is all about fast and intensive learning. That means we don't waste time in helping readers get started. The new content is basically about filling in with highly-effective examples to build new things, show solving problems in newer and unseen ways, and solve real-world examples.

[Penetration Testing Fundamentals](#) Packt Publishing Ltd

Web Applications are the core of any business today, and the need for specialized Application Security experts is increasing these days. Using this book, you will be able to learn Application Security testing and understand how to analyze a web application, conduct a web intrusion test, and a network infrastructure test.

[Learn Penetration Testing](#) BPB Publications

The perfect introduction to pen testing for all IT professionals and students

- Clearly explains key concepts, terminology, challenges, tools, and skills
- Covers the latest penetration testing standards from NSA, PCI, and NIST
- Welcome to today's most useful and practical introduction to penetration testing. Chuck Easttom brings together up-to-the-minute coverage of all the concepts, terminology, challenges, and skills you'll need to be effective. Drawing on decades of experience in cybersecurity and related IT fields, Easttom integrates theory and practice, covering the entire penetration testing life cycle from planning to reporting. You'll gain practical experience through a start-to-finish sample project relying on free open source tools. Throughout, quizzes, projects, and review sections deepen your understanding and help you apply what you've learned. Including essential pen testing standards from NSA, PCI, and NIST, [Penetration Testing Fundamentals](#) will help you protect your assets – and expand your career options.
- LEARN HOW TO
  - Understand what pen testing is and how it's used
  - Meet modern standards for comprehensive and effective testing
  - Review cryptography essentials every pen tester must know
  - Perform reconnaissance with Nmap, Google searches, and ShodanHq
  - Use malware as part of your pen testing toolkit
  - Test for vulnerabilities in Windows shares, scripts, WMI, and the Registry
  - Pen test websites and web communication
  - Recognize SQL injection and cross-site scripting attacks
  - Scan for vulnerabilities with OWASP ZAP, Vega, Nessus, and MBSA
  - Identify Linux vulnerabilities and password cracks
  - Use Kali Linux for advanced pen testing
  - Apply general hacking technique ssuch as fake Wi-Fi hotspots and social engineering
  - Systematically test your environment with Metasploit
  - Write or customize sophisticated Metasploit exploits

[The Hacker Playbook](#) Packt Publishing Ltd

Master Wireshark to solve real-world security problems

If you don't already use Wireshark for a wide range of information security tasks, you will after this book. Mature and powerful, Wireshark is commonly used to find root cause of challenging network issues. This book extends that power to information security professionals, complete with a downloadable, virtual lab environment. [Wireshark for Security Professionals](#) covers both offensive and defensive concepts that can be applied to essentially any InfoSec role. Whether into network security, malware analysis, intrusion detection, or penetration testing, this book demonstrates Wireshark through relevant and useful examples. Master Wireshark through both lab scenarios and exercises. Early in the book, a virtual lab environment is provided for the purpose of getting hands-on experience with Wireshark. Wireshark is combined with two popular platforms: Kali, the security-focused Linux distribution, and the Metasploit Framework, the open-source framework for security testing. Lab-based virtual systems generate network traffic for analysis, investigation and demonstration. In addition to following along with the labs you will be challenged with end-of-chapter exercises to expand on covered material. Lastly, this book explores Wireshark with Lua, the light-weight programming language. Lua allows you to extend and customize Wireshark's features for your needs as a security professional. Lua source code is available both in the book and online. Lua code and lab source code are available online through GitHub, which the book also introduces. The book's final two chapters greatly draw on Lua and TShark, the command-line interface of Wireshark. By the end of the book you will gain the following: Master the basics of Wireshark

Explore the virtual w4sp-lab environment that mimics a real-world network

Gain experience using the Debian-based Kali OS among other systems

Understand the technical details behind network attacks

Execute exploitation and grasp offensive and defensive activities, exploring them through Wireshark

Employ Lua to extend Wireshark features and create useful scripts

To sum up, the book content, labs and online material, coupled with many referenced sources of PCAP traces, together present a dynamic and robust manual for information security professionals seeking to leverage Wireshark.

[Advanced Penetration Testing](#) Apress

Get started with NMAP, OpenVAS, and Metasploit in this short book and understand how NMAP, OpenVAS, and Metasploit can be integrated with each other for greater flexibility and efficiency. You will begin by working with NMAP and ZENMAP and learning the basic scanning and enumeration process. After getting to know the differences between TCP and UDP scans, you will learn to fine tune your scans and efficiently use NMAP scripts. This will be followed by an introduction to OpenVAS vulnerability management system. You will then learn to configure OpenVAS and scan for and report vulnerabilities. The next chapter takes you on a detailed tour of Metasploit and its basic commands and

---

configuration. You will then invoke NMAP and OpenVAS scans from Metasploit. Lastly, you will take a look at scanning services with Metasploit and get to know more about Meterpreter, an advanced, dynamically extensible payload that is extended over the network at runtime. The final part of the book concludes by pentesting a system in a real-world scenario, where you will apply the skills you have learnt. What You Will Learn Carry out basic scanning with NMAP Invoke NMAP from Python Use vulnerability scanning and reporting with OpenVAS Master common commands in Metasploit Who This Book Is For Readers new to penetration testing who would like to get a quick start on it.

Metasploit Revealed: Secrets of the Expert Pentester Apress

A practical guide to testing your network's security with Kali Linux, the preferred choice of penetration testers and hackers. About This Book Employ advanced pentesting techniques with Kali Linux to build highly-secured systems Get to grips with various stealth techniques to remain undetected and defeat the latest defenses and follow proven approaches Select and configure the most effective tools from Kali Linux to test network security and prepare your business against malicious threats and save costs Who This Book Is For Penetration Testers, IT professional or a security consultant who wants to maximize the success of your network testing using some of the advanced features of Kali Linux, then this book is for you. Some prior exposure to basics of penetration testing/ethical hacking would be helpful in making the most out of this title. What You Will Learn Select and configure the most effective tools from Kali Linux to test network security Employ stealth to avoid detection in the network being tested Recognize when stealth attacks are being used against your network Exploit networks and data systems using wired and wireless networks as well as web services Identify and download valuable data from target systems Maintain access to compromised systems Use social engineering to compromise the weakest part of the network—the end users In Detail This book will take you, as a tester or security practitioner through the journey of reconnaissance, vulnerability assessment, exploitation, and post-exploitation activities used by penetration testers and hackers. We will start off by using a laboratory environment to validate tools and techniques, and using an application that supports a collaborative approach to penetration testing. Further we will get acquainted with passive reconnaissance with open source intelligence and active reconnaissance of the external and internal networks. We will also focus on how to select, use, customize, and interpret the results from a variety of different vulnerability scanners. Specific routes to the target will also be examined, including bypassing physical security and exfiltration of data using different techniques. You will also get to grips with concepts such as social engineering, attacking wireless networks, exploitation of web applications and remote access connections. Later you will learn the practical aspects of attacking user client systems by backdooring executable files. You will focus on the most vulnerable part of the network—directly and bypassing the controls, attacking the end user and maintaining persistence access through social media. You will also explore approaches to carrying out advanced penetration testing in tightly secured environments, and the book's hands-on approach will help you understand everything you need to know during a Red teaming exercise or penetration testing Style and approach An advanced level tutorial that follows a practical approach and proven methods to maintain top notch security of your networks.

Metasploit Packt Publishing Ltd

Master the art of conducting modern pen testing attacks and techniques on your web application before the hacker does! About This Book This book covers the latest technologies such as Advance XSS, XSRF, SQL Injection, Web API testing, XML attack vectors, OAuth 2.0 Security, and more involved in today's web applications Penetrate and secure your web application using various techniques Get this comprehensive reference guide that provides advanced tricks and tools of the trade for seasoned penetration testers Who This Book Is For This book is for security professionals and penetration testers who want to speed up their modern web application penetrating testing. It will also benefit those at an intermediate level and web developers who need to be aware of the latest application hacking techniques. What You Will Learn Get to know the new and less-publicized techniques such as PHP Object Injection and XML-based vectors Work with different security tools to automate most of the redundant tasks See different kinds of newly-designed security headers and how they help to provide security Exploit and detect different kinds of XSS vulnerabilities Protect your web application using filtering mechanisms Understand old school and classic web hacking in depth using SQL Injection, XSS, and CSRF Grasp XML-related vulnerabilities and attack vectors such as XXE and DoS techniques Get to know how to test REST APIs to discover security issues in them In Detail Web penetration testing is a growing, fast-moving, and absolutely critical field in information security. This book executes modern web application attacks and utilises cutting-edge hacking techniques with an enhanced knowledge of web application security. We will cover web hacking techniques so you can explore the attack vectors during penetration tests. The book encompasses the latest technologies such as OAuth 2.0, Web API testing methodologies and XML vectors used by hackers. Some lesser discussed attack vectors such as RPO (relative path overwrite), DOM clobbering, PHP Object Injection and etc. has been covered in this book. We'll explain various old school techniques in depth such as XSS, CSRF, SQL Injection through the ever-dependable SQLMap and reconnaissance. Websites nowadays provide APIs to allow integration with third party applications, thereby exposing a lot of attack surface, we cover testing of these APIs using real-life examples. This pragmatic guide will be a great benefit and will help you prepare fully secure applications. Style and approach This master-level guide covers various techniques serially. It is power-packed with real-world examples that focus more on the practical aspects of implementing the techniques rather going into detailed theory.

AWS Penetration Testing McGraw Hill Professional

Take your penetration testing and IT security skills to a whole new level with the secrets of Metasploit About This Book Gain the skills to carry out penetration testing in complex and highly-secured environments Become a master using the Metasploit framework, develop exploits, and generate modules for a variety of real-world scenarios Get this completely updated edition with new useful methods and techniques to make your network robust and resilient Who This Book Is For This book is a hands-on guide to penetration testing using Metasploit and covers its complete development. It shows a number of techniques and methodologies that will help you master the Metasploit framework and explore approaches to carrying out advanced penetration testing in highly secured environments. What You Will Learn Develop advanced and sophisticated auxiliary modules Port exploits from PERL, Python, and many more programming languages Test services such as databases, SCADA, and many more Attack the client side with highly advanced techniques Test mobile and tablet devices with Metasploit Perform social engineering with Metasploit Simulate attacks on web servers and systems with Armitage GUI Script attacks in Armitage using CORTANA scripting In Detail Metasploit is a popular penetration testing framework that has one of the largest exploit databases around. This book will show you exactly how to prepare yourself against the attacks you will face every day by simulating real-world possibilities. We start by reminding you about the basic functionalities of Metasploit and its use in the most traditional ways. You'll get to know about the basics of programming Metasploit modules as a refresher, and then dive into carrying out exploitation as well building and porting exploits of various kinds in Metasploit. In the next section, you'll develop the ability to perform testing on various services such as SCADA, databases, IoT, mobile, tablets, and many more services. After this training, we jump into real-world sophisticated scenarios where performing penetration tests are a challenge. With real-life case studies, we take you on a journey through client-side attacks using Metasploit and various scripts built on the Metasploit framework. By the end of the book, you will be trained specifically on time-saving techniques using Metasploit. Style and approach This is a step-by-step guide that provides great Metasploit framework methodologies. All the key concepts are explained details with the help of examples and demonstrations that will help you understand everything you need to know about Metasploit.