Metasploit The Penetration Tester39s Guide

Right here, we have countless book **Metasploit The Penetration Tester39s Guide** and collections to check out. We additionally find the money for variant types and moreover type of the books to browse. The good enough book, fiction, history, novel, scientific research, as skillfully as various supplementary sorts of books are readily easy to use here.

As this Metasploit The Penetration Tester39s Guide, it ends taking place instinctive one of the favored books Metasploit The Penetration Tester39s Guide collections that we have. This is why you remain in the best website to see the amazing ebook to have.

Learn Penetration Testing Packt Publishing Ltd
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

Metasploit, 2nd Edition 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.

Metasploit 5.0 for Beginners Packt Publishing Ltd

Identify, exploit, and test web application security with ease Key FeaturesGet up to speed with Metasploit and discover how to use it for pentestingUnderstand how to exploit and protect your web environment effectivelyLearn how an exploit works and what causes vulnerabilitiesBook 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 learnGet up to speed with setting up and installing the Metasploit frameworkGain first-hand experience of the Metasploit web interfaceUse Metasploit for web-application reconnaissanceUnderstand how to pentest various content management systemsPentest platforms such as JBoss, Tomcat, and JenkinsBecome well-versed with fuzzing web applicationsWrite and automate penetration testing reportsWho 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 BookRix

Get up to speed with various penetration testing techniques and resolve security threats of varying complexity Key FeaturesEnhance your penetration testing skills to tackle security threatsLearn to gather information, find vulnerabilities, and exploit enterprise defensesNavigate secured systems with the most up-to-date version of Kali Linux (2019.1) and Metasploit (5.0.0)Book Description Sending information via the internet is not entirely private, as evidenced by the rise in hacking, malware attacks, and security threats. With the help of this book, you'll learn crucial penetration testing techniques to help you evaluate enterprise defenses. You'll start by understanding each stage of pentesting and deploying target virtual machines, including Linux and Windows. Next, the book will guide you through performing intermediate penetration testing in a controlled environment. With the help of practical use cases, you'll also be able to implement your learning in real-world scenarios. By studying everything from setting up your lab, information gathering and password attacks, through to social engineering and post exploitation,

you'll be able to successfully overcome security threats. The book will even help you leverage the best tools, such as Kali Linux, Metasploit, Burp Suite, and other open source pentesting tools to perform these techniques. Toward the later chapters, you'll focus on best practices to quickly resolve security threats. By the end of this book, you'll be well versed with various penetration testing techniques so as to be able to tackle security threats effectively What you will learnPerform entry-level penetration tests by learning various concepts and techniquesUnderstand both common and not-so-common vulnerabilities from an attacker's perspectiveGet familiar with intermediate attack methods that can be used in real-world scenariosUnderstand how vulnerabilities are created by developers and how to fix some of them at source code levelBecome well versed with basic tools for ethical hacking purposesExploit known vulnerable services with tools such as MetasploitWho this book is for If you're just getting started with penetration testing and want to explore various security domains, this book is for you. Security professionals, network engineers, and amateur ethical hackers will also find this book useful. Prior knowledge of penetration testing and ethical hacking is not necessary.

Metasploit Penetration Testing Cookbook Packt Publishing Ltd

An intensive hands-on guide to perform professional penetration testing for highly-secured environments from start to finish. You will learn to provide penetration testing services to clients with mature security infrastructure. Understand how to perform each stage of the penetration test by gaining hands-on experience in performing attacks that mimic those seen in the wild. In the end, take the challenge and perform a virtual penetration test against a fictional corporation. If you are looking for guidance and detailed instructions on how to perform a penetration test from start to finish, are looking to build out your own penetration testing lab, or are looking to improve on your existing penetration testing skills, this book is for you. Although the books attempts to accommodate those that are still new to the penetration testing field, experienced testers should be able to gain knowledge and hands-on experience as well. The book does assume that you have some experience in web application testing and as such the chapter regarding this subject may require you to understand the basic concepts of web security. The reader should also be familiar with basic IT concepts, and commonly used protocols such as TCP/IP.

Metasploit Bootcamp Packt Publishing Ltd

The second edition of the international bestseller Metasploit is written by some of the world ' s best hackers and is the only introduction you ' ll ever need to the legendary Framework. Fully revised to include all new chapters on attacking cloud applications, industrial control systems, and recent vulnerabilities, you ' ll learn Metasploit ' s module system, conventions, and interfaces as you launch simulated attacks. The Metasploit Framework makes discovering, exploiting, and sharing systemic vulnerabilities quick and painless. But, this popular pentesting tool can be hard to grasp for first-time users. Written by some of the world ' s top hackers and security experts, Metasploit fills the gap by teaching you how to best harness the Framework and interact with its vibrant community of Metasploit open-source contributors. This indispensable guide's updated second edition introduces modules and commands recently added to the Metasploit Framework, along with new chapters on the Cloud Lookup (and Bypass) module and attacking IoT or SCADA (industrial) systems using the Mobius client

module. You ' ll learn: Modern pentesting techniques, including network reconnaissance and enumeration The Metasploit Framework's conventions, interfaces, and module system Client-side attacks Wireless exploits Targeted social-engineering attacks In a digital ecosystem increasingly driven by cloud-based and industrial attacks, the modern hacking techniques covered in Metasploit, 2nd Edition are essential for today's penetration testers.

Penetration Testing Packt Publishing Ltd

A comprehensive and detailed, step by step tutorial guide that takes you through important aspects of the Metasploit framework. If you are a penetration tester, security engineer, or someone who is looking to extend their penetration testing skills with Metasploit, then this book is ideal for you. The readers ofthis book must have a basic knowledge of using Metasploit. They are also expected to have knowledge of exploitation and an indepth understanding of object-oriented programming languages.

Metasploit Handbook Createspace Independent Publishing Platform

Master the Metasploit Framework and become an expert in penetration testing. Key FeaturesGain a thorough understanding of the Metasploit FrameworkDevelop the skills to perform penetration testing in complex and highly secure environmentsLearn techniques to integrate Metasploit with the industry ' s leading toolsBook Description Most businesses today are driven by their IT infrastructure, and the tiniest crack in this IT network can bring down the entire business. Metasploit is a pentesting network that can validate your system by performing elaborate penetration tests using the Metasploit Framework to secure your infrastructure. This Learning Path introduces you to the basic functionalities and applications of Metasploit. Throughout this book, you ' ll learn different techniques for programming Metasploit modules to validate services such as databases, fingerprinting, and scanning. You ' ll get to grips with post exploitation and write quick scripts to gather information from exploited systems. As you progress, you ' ll delve into real-world scenarios where performing penetration tests are a challenge. With the help of these case studies, you ' ll explore client-side attacks using Metasploit and a variety of scripts built on the Metasploit Framework. By the end of this Learning Path, you ' ll have the skills required to identify system vulnerabilities by using thorough testing. This Learning Path includes content from the following Packt products: Metasploit for Beginners by Sagar RahalkarMastering Metasploit - Third Edition by Nipun JaswalWhat you will learnDevelop advanced and sophisticated auxiliary modulesPort exploits from Perl, Python, and many other programming languagesBypass modern protections such as antivirus and IDS with MetasploitScript attacks in Armitage using the Cortana scripting languageCustomize Metasploit modules to modify existing exploitsExplore the steps involved in post-exploitation on Android and mobile platformsWho this book is for This Learning Path is ideal for security professionals, web programmers, and pentesters who want to master vulnerability exploitation and get the most of the Metasploit Framework. Basic knowledge of Ruby programming and Cortana scripting language is required.

Mastering Metasploit, Second Edition No Starch Press

This book is a guide for you on how to use Metasploit. The first part of the book is a

guide for you on how to get started with Metasploit. You are guided on how to install Metasploit on Windows and in Linux. You are also guided on how to start Metasploit, both the Graphical User Interface (GUI) and the command line. The book also guides you on how to work with databases and workspaces in Metasploit. The process of backing up data in Metasploit is also discussed. The basic Metasploit commands are examined in detail. You will learn the options which each command takes. Enumeration is also explored in detail. You will learn how to enumerate your target hosts so as to get details about them. The book guides you on how to exploit web applications with Metasploit. Metapsloit can be used to sniff packets which are being sent via a particular interface on a computer. Such packets can then be analyzed with tools such as wireshark. This book guides you on how to sniff packets. You will also learn how to escalate the privileges when logged into a certain computer and be able to perform administrative tasks. Keylogging, which can help you capture keystrokes, is also explored. The following topics are discussed in this book: - Getting started with Metasploit - Basic Metasploit Commands - Enumeration - Exploiting Web Applications - Packet Sniffing - Privilege Escalation - Keylogging

Metasploit for Beginners Pearson IT Certification

Introducing the "Metasploit Masterclass for Ethical Hackers" Book Bundle – Your Path to Becoming a Cybersecurity Expert! Are you fascinated by the world of ethical hacking and cybersecurity? Do you want to master the art of securing networks, web applications, wireless devices, and IoT technology? Are you ready to embark on a journey that will turn you into a cybersecurity pro? Look no further! This exclusive book bundle brings together four comprehensive volumes designed to make you a cybersecurity expert. Say hello to the "Metasploit Masterclass for Ethical Hackers" – your ultimate guide to becoming a highly skilled ethical hacker and a defender of the digital world. Book 1: Network Reconnaissance and Vulnerability Scanning Learn the fundamentals of ethical hacking, network reconnaissance, and vulnerability scanning. Gather critical information about target networks, identify potential vulnerabilities, and become a pro at scanning for weaknesses. Book 2: Web Application Penetration Testing Dive deep into the realm of web application security. Discover how to assess, exploit, and secure vulnerabilities in web applications. Your expertise in web application security will be in high demand. Book 3: Wireless and IoT Hacking With the rise of wireless networks and IoT devices, new threats emerge. Uncover the secrets of wireless and IoT hacking – from exploiting vulnerabilities to securing these technologies effectively. Book 4: Advanced Threat Detection and Defense Stay on the cutting edge of cybersecurity. Explore advanced threat detection methods, proactive threat hunting, and the use of Metasploit for defensive purposes. Protect against even the most sophisticated cyber threats. This book bundle is your gateway to a world of cybersecurity excellence. Whether you're starting your cybersecurity journey or seeking to enhance your skills, these books offer a holistic and hands-on approach to mastering the art and science of ethical

hacking. Why Choose the "Metasploit Masterclass for Ethical Hackers" Bundle? · Expert Guidance: Learn from experienced cybersecurity professionals. · Hands-On Learning: Gain practical skills through real-world examples and exercises. · Comprehensive Coverage: Master various aspects of ethical hacking and cybersecurity. · Career Advancement: Boost your career prospects in the high-demand field of cybersecurity. Secure your digital future and become a guardian of cyberspace with the "Metasploit Masterclass for Ethical Hackers" book bundle. Get started on your path to becoming a cybersecurity expert today! Don't miss this opportunity to invest in your cybersecurity knowledge. Click the link to grab your bundle and start your journey towards becoming a cybersecurity pro!

Metasploit Penetration Testing Cookbook No Starch Press

Over 100 recipes for penetration testing using Metasploit and virtual machines About This Book Special focus on the latest operating systems, exploits, and penetration testing techniques Learn new anti-virus evasion techniques and use Metasploit to evade countermeasures Automate post exploitation with AutoRunScript Exploit Android devices, record audio and video, send and read SMS, read call logs, and much more Build and analyze Metasploit modules in Ruby Integrate Metasploit with other penetration testing tools Who This Book Is For If you are a Security professional or pentester and want to get into vulnerability exploitation and make the most of the Metasploit framework, then this book is for you. Some prior understanding of penetration testing and Metasploit is required. What You Will Learn Set up a complete penetration testing environment using Metasploit and virtual machines Master the world's leading penetration testing tool and use it in professional penetration testing Make the most of Metasploit with PostgreSQL, importing scan results, using workspaces, hosts, loot, notes, services, vulnerabilities, and exploit results Use Metasploit with the Penetration Testing Execution Standard methodology Use MSFvenom efficiently to generate payloads and backdoor files, and create shellcode Leverage Metasploit's advanced options, upgrade sessions, use proxies, use Meterpreter sleep control, and change timeouts to be stealthy In Detail Metasploit is the world's leading penetration testing tool and helps security and IT professionals find, exploit, and validate vulnerabilities. Metasploit allows penetration testing automation, password auditing, web application scanning, social engineering, post exploitation, evidence collection, and reporting. Metasploit's integration with InsightVM (or Nexpose), Nessus, OpenVas, and other vulnerability scanners provides a validation solution that simplifies vulnerability prioritization and remediation reporting. Teams can collaborate in Metasploit and present their findings in consolidated reports. In this book, you will go through great recipes that will allow you to start using Metasploit effectively. With an ever increasing level of complexity, and covering everything from the fundamentals to more advanced features in Metasploit, this book is not just for beginners but also for professionals keen to master this awesome tool. You will begin by building your lab environment, setting up Metasploit, and learning ho ...

Coding for Penetration Testers Syngress

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.

Advanced Penetration Testing for Highly-Secured Environments Elsevier

The Metasploit framework has been around for a number of years and is one of the most widely used tools for carrying out penetration testing on various services. This book is a hands-on guide to penetration testing using Metasploit and covers its complete development. It will help you clearly understand the creation process of various exploits and modules and develop approaches to writing custom functionalities into the Metasploit framework. This book covers a number of techniques and methodologies that will help you learn and master the Metasploit framework. You will also explore approaches to carrying out advanced penetration testing in highly secured environments, and the book's hands-on approach will help you understand everything you need to know about Metasploit.

The The Complete Metasploit Guide Rob Botwright

This book follows a Cookbook style with recipes explaining the steps for penetration testing with WLAN, VOIP, and even cloud computing. There is plenty of code and commands used to make your learning curve easy and quick.This book targets both professional penetration testers as well as new users of Metasploit, who wish to gain expertise over the framework and learn an additional skill of penetration testing, not limited to a particular OS. The book requires basic knowledge of scanning, exploitation, and the Ruby language.

Improving your Penetration Testing Skills Packt Publishing Ltd

Understand and Conduct Ethical Hacking and Security Assessments KEY FEATURES ● Practical guidance on discovering, assessing, and mitigating web, network, mobile, and wireless vulnerabilities. ● Experimentation with Kali Linux, Burp Suite, MobSF, Metasploit and Aircrack-suite. ● In-depth explanation of topics focusing on how to crack ethical hacking interviews. DESCRIPTION

Penetration Testing for Job Seekers is an attempt to discover the way to a spectacular career in cyber security, specifically penetration testing. This book offers a practical approach by discussing several computer and network fundamentals before delving into various penetration testing approaches, tools, and techniques. Written by a veteran security professional, this book provides a detailed look at the dynamics that form a person's career as a penetration tester. This book is divided into ten chapters and covers numerous facets of penetration testing, including web application, network, Android application, wireless penetration testing, and creating excellent penetration test reports. This book also shows how to set up an in-house hacking lab from scratch to improve your skills. A penetration tester's professional path, possibilities, average day, and day-to-day obstacles are all outlined to help readers better grasp what they may anticipate from a cybersecurity career. Using this book, readers will be able to boost their employability and job market relevance, allowing them to sprint towards a lucrative career as a penetration tester. WHAT YOU WILL LEARN ●Perform penetration testing on web apps, networks, android apps, and wireless networks. ●Access to the most widely used penetration testing methodologies and standards in the industry. ●Use an artistic approach to find security holes in source code. ●Learn how to put together a high-quality penetration test report. ● Popular technical interview questions on ethical hacker and pen tester job roles. ● Exploration of different career options, paths, and possibilities in cyber security. WHO THIS BOOK IS FOR This book is for aspiring security analysts, pen testers, ethical hackers, anyone who wants to learn how to become a successful pen tester. A fundamental understanding of network principles and workings is helpful but not required. TABLE OF CONTENTS 1. Cybersecurity, Career Path, and Prospects 2. Introduction to Penetration Testing 3. Setting Up Your Lab for Penetration Testing 4. Web Application and API Penetration Testing 5. The Art of Secure Source Code Review 6. Penetration Testing Android Mobile Applications 7. Network Penetration Testing 8. Wireless Penetration Testing 9. Report Preparation and Documentation 10. A Day in the Life of a Pen Tester

Penetration Testing with the Metasploit Framework No Starch Press

A complete pentesting guide facilitating smooth backtracking for working hackers About This Book Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux Gain a deep understanding of the flaws in web applications and exploit them in a practical manner Pentest Android apps and perform various attacks in the real world using real case studies Who This Book Is For This course is for anyone who wants to learn about security. Basic knowledge of Android programming would be a plus. What You Will Learn Exploit several common Windows network vulnerabilities Recover lost files, investigate successful hacks, and discover hidden data in innocent-looking files Expose vulnerabilities present in web servers and their applications using server-side attacks Use SQL and cross-site scripting (XSS) attacks Check for XSS flaws using the burp suite proxy Acquaint yourself with the fundamental building blocks of Android Apps in the right way

Take a look at how your personal data can be stolen by malicious attackers See how developers make mistakes that allow attackers to steal data from phones In Detail The need for penetration testers has grown well over what the IT industry ever anticipated. Running just a vulnerability scanner is no longer an effective method to determine whether a business is truly secure. This learning path will help you develop the most effective penetration testing skills to protect your Windows, web applications, and Android devices. The first module focuses on the Windows platform, which is one of the most common OSes, and managing its security spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Employs the most advanced tools and techniques to reproduce the methods used by sophisticated hackers. In this module first,you'll be introduced to Kali's top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities so you can exploit a system remotely. You'll not only learn to penetrate in the machine, but will also learn to work with Windows privilege escalations. The second module will help you get to grips with the tools used in Kali Linux 2.0 that relate to web application hacking. You will get to know about scripting and input validation flaws, AJAX, and security issues related to AJAX. You will also use an automated technique called fuzzing so you can identify flaws in a web application. Finally, you'll understand the web application vulnerabilities and the ways they can be exploited. In the last module, you'll get started with Android security. Android, being the platform with the largest consumer base, is the obvious primary target for attackers. You'll begin this journey with the absolute basics and will then slowly gear up to the concepts of Android rooting, application security assessments, malware, infecting APK files, and fuzzing. You'll gain the skills necessary to perform Android application vulnerability assessments and to create an Android pentesting lab. This Learning Path is a blend of content from the following Packt products: Kali Linux 2: Windows Penetration Testing by Wolf Halton and Bo Weaver Web Penetration Testing with Kali Linux, Second Edition by Juned Ahmed Ansari Hacking Android by Srinivasa Rao Kotipalli and Mohammed A. Imran Style and approach This course uses easy-to-understand yet professional language for explaining concepts to test your network's security.

AWS Penetration Testing Packt Publishing Ltd

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 learnSet up your AWS account and get well-versed in various pentesting servicesDelve into a variety of cloud pentesting tools and methodologiesDiscover how to exploit vulnerabilities in both AWS and applicationsUnderstand the legality of pentesting and learn how to stay in scopeExplore cloud pentesting best practices, tips, and tricksBecome competent at using tools such as Kali Linux, Metasploit, and NmapGet to grips with post-exploitation procedures and find out how to write pentesting reportsWho 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.

Penetration Testing: A Survival Guide 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

The Penetration Tester's Guide to Web Applications Elsevier

Discover the next level of network defense and penetration testing with the Metasploit 5.0 framework Key FeaturesMake your network robust and resilient with this updated edition covering the latest pentesting techniquesExplore a variety of entry points to compromise a system while remaining undetectedEnhance your ethical hacking skills by performing penetration tests in highly secure environmentsBook Description Updated for the latest version of Metasploit, this book will prepare you to face everyday cyberattacks by simulating real-world scenarios. Complete with step-by-step explanations of essential concepts and practical examples, Mastering Metasploit will help you gain insights into programming Metasploit modules and carrying out exploitation, as well as building and porting various kinds of exploits in Metasploit. Giving you the ability to perform tests on different services, including databases, IoT, and mobile, this Metasploit book will help you get to grips with real-world, sophisticated scenarios where performing penetration tests is a challenge. You'll then

learn a variety of methods and techniques to evade security controls deployed at a target's endpoint. As you advance, you ' ll script automated attacks using CORTANA and Armitage to aid penetration testing by developing virtual bots and discover how you can add custom functionalities in Armitage. Following real-world case studies, this book will take you on a journey through client-side attacks using Metasploit and various scripts built on the Metasploit 5.0 framework. By the end of the book, you ' ll have developed the skills you need to work confidently with efficient exploitation techniques What you will learnDevelop advanced and sophisticated auxiliary, exploitation, and post-exploitation modulesLearn to script automated attacks using CORTANATest services such as databases, SCADA, VoIP, and mobile devicesAttack the client side with highly advanced pentesting techniquesBypass modern protection mechanisms, such as antivirus, IDS, and firewallsImport public exploits to the Metasploit FrameworkLeverage C and Python programming to effectively evade endpoint protectionWho this book is for If you are a professional penetration tester, security engineer, or law enforcement analyst with basic knowledge of Metasploit, this book will help you to master the Metasploit framework and guide you in developing your exploit and module development skills. Researchers looking to add their custom functionalities to Metasploit will find this book useful. As Mastering Metasploit covers Ruby programming and attack scripting using Cortana, practical knowledge of Ruby and Cortana is required.

Mastering Metasploit Packt Publishing Ltd

In the fast-paced and ever-evolving landscape of cybersecurity, the need for robust penetration testing techniques is paramount. "Mastering Metasploit: A Comprehensive Guide to Cybersecurity Penetration Testing" by Zusman Aronowitz stands as an authoritative resource, providing a deep dive into the world of Metasploit - a powerful framework widely used for penetration testing, ethical hacking, and security assessments. Unlocking the Power of Metasploit: Metasploit has established itself as a cornerstone in the toolkit of cybersecurity professionals, and this book serves as an indispensable guide for both beginners and seasoned practitioners. Zusman Aronowitz, a respected authority in the field, distills years of hands-on experience into a comprehensive exploration of Metasploit's capabilities, equipping readers with the knowledge and skills needed to navigate the complex realm of penetration testing. Key Features of the Book: Comprehensive Coverage: The book spans a wide array of topics, ensuring a holistic understanding of Metasploit's functionalities. From the fundamentals to advanced techniques, readers are guided through every facet of this powerful framework. Hands-On Examples: Learning by doing is central to the book's approach. Practical, real-world examples and walkthroughs accompany each concept, allowing readers to apply their newfound knowledge in simulated environments. Step-by-Step Tutorials: Detailed step-by-step tutorials take readers through the execution of various penetration testing scenarios. Whether you're a novice or an experienced professional, these tutorials provide actionable insights for honing your skills. Strategic Insight: Zusman Aronowitz goes beyond the technicalities, providing strategic insight into the application of Metasploit in different cybersecurity contexts. This includes guidance on creating

effective penetration testing strategies and adapting to diverse environments. Real-world Case Studies: The inclusion of real-world case studies adds a practical dimension to the book. Readers gain valuable insights into how Metasploit has been used to uncover vulnerabilities and strengthen the security postures of actual organizations. In "Mastering Metasploit: A Comprehensive Guide to Cybersecurity Penetration Testing," Zusman Aronowitz not only demystifies the complexities of Metasploit but also empowers readers to become proficient ethical hackers. This SEO-friendly book provides a wealth of knowledge that transcends traditional cybersecurity literature. In an era where cyber threats are increasingly sophisticated, the book serves as a beacon for those looking to fortify digital defenses. From learning the basics to mastering advanced penetration testing techniques, Zusman Aronowitz's expertise shines through, making this book an invaluable asset for cybersecurity enthusiasts, IT professionals, and anyone seeking to enhance their skills in ethical hacking. Readers will appreciate the clear and concise writing style, coupled with engaging examples that bridge the gap between theory and practical application. The strategic insights provided ensure that the book is not just a technical manual but a guide for developing a proactive and adaptive cybersecurity mindset. Whether you're a cybersecurity professional aiming to stay ahead of the curve or an aspiring ethical hacker looking to enter this dynamic field, "Mastering Metasploit" is your gateway to a comprehensive understanding of one of the industry's most powerful tools. In conclusion, Zusman Aronowitz's "Mastering Metasploit" is more than a guide; it's a roadmap to cybersecurity proficiency. Dive into the world of penetration testing with confidence, armed with the knowledge and skills needed to navigate the ever-changing landscape of cybersecurity.