
Download Free Cookbook Testing Penetration Web Python

This is likewise one of the factors by obtaining the soft documents of this **Cookbook Testing Penetration Web Python** by online. You might not require more time to spend to go to the books initiation as capably as search for them. In some cases, you likewise get not discover the proclamation Cookbook Testing Penetration Web Python that you are looking for. It will unconditionally squander the time.

However below, gone you visit this web page, it will be as a result extremely easy to get as without difficulty as download lead Cookbook Testing Penetration Web Python

It will not put up with many period as we run by before. You can get it while appear in something else at home and even in your workplace. fittingly easy! So, are you question? Just exercise just what we come up with the money for under as with ease as review **Cookbook Testing Penetration Web Python** what you considering to read!

KEY=WEB - ALEX RAMOS

PYTHON WEB PENETRATION TESTING COOKBOOK

Packt Publishing Ltd This book gives you an arsenal of Python scripts perfect to use or to customize your needs for each stage of the testing process. Each chapter takes you step by step through the methods of designing and modifying scripts to attack web apps. You will learn how to collect both open and hidden information from websites to further your attacks, identify vulnerabilities, perform SQL Injections, exploit cookies, and enumerate poorly configured systems. You will also discover how to crack encryption, create payloads to mimic malware, and create tools to output your findings into presentable formats for reporting to your employers.

PYTHON PENETRATION TESTING COOKBOOK

PRACTICAL RECIPES ON IMPLEMENTING INFORMATION GATHERING, NETWORK SECURITY, INTRUSION DETECTION, AND POST-EXPLOITATION

Packt Publishing Ltd Over 50+ hands-on recipes to help you pen test networks using Python, discover vulnerabilities, and find a recovery path About This Book Learn to detect and avoid various types of attack that put system privacy at risk Enhance your knowledge of wireless application concepts and information gathering through practical recipes Learn a pragmatic way to penetration-test using Python, build efficient code, and save time Who This Book Is For If you are a developer with prior knowledge of using Python for penetration testing and if you want an overview of scripting tasks to consider while penetration testing, this book will give you a lot of useful code for your toolkit. What You Will Learn Learn to configure Python in different environment setups. Find an IP address from a web page using BeautifulSoup and Scrapy Discover different types of packet sniffing script to sniff network packets Master layer-2 and TCP/ IP attacks Master techniques for exploit development for Windows and Linux Incorporate various network- and packet-sniffing techniques using Raw sockets and Scrapy In Detail Penetration testing is the use of tools and code to attack a system in order to assess its vulnerabilities to external threats. Python allows pen testers to create their own tools. Since Python is a highly valued pen-testing language, there are many native libraries and Python bindings available specifically for pen-testing tasks. Python Penetration Testing Cookbook begins by teaching you how to extract information from web pages. You will learn how to build an intrusion detection system using network sniffing techniques. Next, you will find out how to scan your networks to ensure performance and quality, and how to carry out wireless pen testing on your network to avoid cyber attacks. After that, we'll discuss the different kinds of network attack. Next, you'll get to grips with designing your own torrent detection program. We'll take you through common vulnerability scenarios and then cover buffer overflow exploitation so you can detect insecure coding. Finally, you'll master PE code injection methods to safeguard your network. Style and approach This book takes a recipe-based approach to solving real-world problems in pen testing. It is structured in stages from the initial assessment of a system through exploitation to post-exploitation tests, and provides scripts that can be used or modified for in-depth penetration testing.

PYTHON PENETRATION TESTING COOKBOOK

Over 60 hands-on recipes to pen test networks using Python to discover vulnerabilities and find a recovery path About This Book* Learn to detect and avoid various types of attacks that put the privacy of a system at risk* Enhance your knowledge on the concepts of wireless applications and information gathering through practical recipes.* See a pragmatic way to penetration test using Python to build efficient code and save time Who This Book Is For This book is for developers who have prior knowledge of using Python for pen testing. If you want an overview of scripting tasks to consider while pen testing, this book will give you a lot of useful code or your tool kit. What You Will Learn* Find an IP address from a web page using BeautifulSoup and urllib* Discover different types of sniffers to build an intrusion detection system* Create an efficient and high-performance ping sweep and port scanner* Get to grips with making an SSID and BSSID scanner* Perform network pen-testing by attacking DDoS, DHCP and packet injecting* Fingerprint OS and network applications, and correlate common vulnerabilities* Master techniques to detect vulnerabilities in your environment and secure them* Incorporate various networks and packet sniffing techniques using Raw sockets and Scapy In Detail Penetration testing is the use of tools and code to attack a system in order to assess its vulnerabilities to external threats. Python allows pen testers to create their own tools. Since Python is a highly valued pen-testing language, there are many native libraries and Python bindings available specifically for pen-testing tasks. Python Penetration Testing Cookbook begins by teaching you how to extract information from web pages. You will learn how to build an intrusion detection system using network sniffing techniques. Next, you will find out how to scan your networks to ensure performance and quality, and how to carry out wireless pen testing on your network to avoid cyber attacks. After that, we'll discuss the different kinds of attacks on the network. Next, you'll get to grips with designing your own torrent detection program. We'll take you through common vulnerability scenarios and then cover buffer overflow exploitation so you can detect insecure coding. Finally, you'll discover PE code injection methods to safeguard your network.

VIOLENT PYTHON

A COOKBOOK FOR HACKERS, FORENSIC ANALYSTS, PENETRATION TESTERS AND SECURITY ENGINEERS

Newnes Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker's tools, this book will teach you to forge your own

weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. Demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus

LEARNING PYTHON WEB PENETRATION TESTING

AUTOMATE WEB PENETRATION TESTING ACTIVITIES USING PYTHON

Packt Publishing Ltd Leverage the simplicity of Python and available libraries to build web security testing tools for your application Key Features Understand the web application penetration testing methodology and toolkit using Python Write a web crawler/spider with the Scrapy library Detect and exploit SQL injection vulnerabilities by creating a script all by yourself Book Description Web penetration testing is the use of tools and code to attack a website or web app in order to assess its vulnerability to external threats. While there are an increasing number of sophisticated, ready-made tools to scan systems for vulnerabilities, the use of Python allows you to write system-specific scripts, or alter and extend existing testing tools to find, exploit, and record as many security weaknesses as possible. Learning Python Web Penetration Testing will walk you through the web application penetration testing methodology, showing you how to write your own tools with Python for each activity throughout the process. The book begins by emphasizing the importance of knowing how to write your own tools with Python for web application penetration testing. You will then learn to interact with a web application using Python, understand the anatomy of an HTTP request, URL, headers and message body, and later create a script to perform a request, and interpret the response and its headers. As you make your way through the book, you will write a web crawler using Python and the Scrapy library. The book will also help you to develop a tool to perform brute force attacks in different parts of the web application. You will then discover more on detecting and exploiting SQL injection vulnerabilities. By the end of this book, you will have successfully created an HTTP proxy based on the mitmproxy tool. What you will learn Interact with a web application using the Python and Requests libraries Create a basic web application crawler and make it recursive Develop a brute force tool to discover and enumerate resources such as files and directories Explore different authentication methods

commonly used in web applications Enumerate table names from a database using SQL injection Understand the web application penetration testing methodology and toolkit Who this book is for Learning Python Web Penetration Testing is for web developers who want to step into the world of web application security testing. Basic knowledge of Python is necessary.

LEARNING PENETRATION TESTING WITH PYTHON

Packt Publishing Ltd Utilize Python scripting to execute effective and efficient penetration tests About This Book Understand how and where Python scripts meet the need for penetration testing Familiarise yourself with the process of highlighting a specific methodology to exploit an environment to fetch critical data Develop your Python and penetration testing skills with real-world examples Who This Book Is For If you are a security professional or researcher, with knowledge of different operating systems and a conceptual idea of penetration testing, and you would like to grow your knowledge in Python, then this book is ideal for you. What You Will Learn Familiarise yourself with the generation of Metasploit resource files Use the Metasploit Remote Procedure Call (MSFRPC) to automate exploit generation and execution Use Python's Scapy, network, socket, office, Nmap libraries, and custom modules Parse Microsoft Office spreadsheets and eXtensible Markup Language (XML) data files Write buffer overflows and reverse Metasploit modules to expand capabilities Exploit Remote File Inclusion (RFI) to gain administrative access to systems with Python and other scripting languages Crack an organization's Internet perimeter Chain exploits to gain deeper access to an organization's resources Interact with web services with Python In Detail Python is a powerful new-age scripting platform that allows you to build exploits, evaluate services, automate, and link solutions with ease. Python is a multi-paradigm programming language well suited to both object-oriented application development as well as functional design patterns. Because of the power and flexibility offered by it, Python has become one of the most popular languages used for penetration testing. This book highlights how you can evaluate an organization methodically and realistically. Specific tradecraft and techniques are covered that show you exactly when and where industry tools can and should be used and when Python fits a need that proprietary and open source solutions do not. Initial methodology, and Python fundamentals are established and then built on. Specific examples are created with vulnerable system images, which are available to the community to test scripts, techniques, and exploits. This book walks you through real-world penetration testing challenges and how Python can help. From start to finish, the book takes you through how to create Python scripts that meet relative needs that can be adapted to particular situations. As chapters progress, the script examples explain new concepts to enhance your foundational knowledge, culminating

with you being able to build multi-threaded security tools, link security tools together, automate reports, create custom exploits, and expand Metasploit modules. **Style and approach** This book is a practical guide that will help you become better penetration testers and/or Python security tool developers. Each chapter builds on concepts and tradecraft using detailed examples in test environments that you can simulate.

PYTHON PENETRATION TESTING ESSENTIALS

TECHNIQUES FOR ETHICAL HACKING WITH PYTHON, 2ND EDITION

Packt Publishing Ltd This book gives you the skills you need to use Python for penetration testing, with the help of detailed code examples. This book has been updated for Python 3.6.3 and Kali Linux 2018.1. **Key Features** Detect and avoid various attack types that put the privacy of a system at risk Leverage Python to build efficient code and eventually build a robust environment Learn about securing wireless applications and information gathering on a web server **Book Description** This book gives you the skills you need to use Python for penetration testing (pentesting), with the help of detailed code examples. We start by exploring the basics of networking with Python and then proceed to network hacking. Then, you will delve into exploring Python libraries to perform various types of pentesting and ethical hacking techniques. Next, we delve into hacking the application layer, where we start by gathering information from a website. We then move on to concepts related to website hacking—such as parameter tampering, DDoS, XSS, and SQL injection. By reading this book, you will learn different techniques and methodologies that will familiarize you with Python pentesting techniques, how to protect yourself, and how to create automated programs to find the admin console, SQL injection, and XSS attacks. **What you will learn** The basics of network pentesting including network scanning and sniffing Wireless, wired attacks, and building traps for attack and torrent detection Web server footprinting and web application attacks, including the XSS and SQL injection attack Wireless frames and how to obtain information such as SSID, BSSID, and the channel number from a wireless frame using a Python script The importance of web server signatures, email gathering, and why knowing the server signature is the first step in hacking **Who this book is for** If you are a Python programmer, a security researcher, or an ethical hacker and are interested in penetration testing with the help of Python, then this book is for you. Even if you are new to the field of ethical hacking, this book can help you find the vulnerabilities in your system so that you are ready to tackle any kind of attack or intrusion.

PYTHON: PENETRATION TESTING FOR DEVELOPERS

Packt Publishing Ltd Unleash the power of Python scripting to execute effective and efficient penetration tests About This Book Sharpen your pentesting skills with Python Develop your fluency with Python to write sharper scripts for rigorous security testing Get stuck into some of the most powerful tools in the security world Who This Book Is For If you are a Python programmer or a security researcher who has basic knowledge of Python programming and wants to learn about penetration testing with the help of Python, this course is ideal for you. Even if you are new to the field of ethical hacking, this course can help you find the vulnerabilities in your system so that you are ready to tackle any kind of attack or intrusion. What You Will Learn Familiarize yourself with the generation of Metasploit resource files and use the Metasploit Remote Procedure Call to automate exploit generation and execution Exploit the Remote File Inclusion to gain administrative access to systems with Python and other scripting languages Crack an organization's Internet perimeter and chain exploits to gain deeper access to an organization's resources Explore wireless traffic with the help of various programs and perform wireless attacks with Python programs Gather passive information from a website using automated scripts and perform XSS, SQL injection, and parameter tampering attacks Develop complicated header-based attacks through Python In Detail Cybercriminals are always one step ahead, when it comes to tools and techniques. This means you need to use the same tools and adopt the same mindset to properly secure your software. This course shows you how to do just that, demonstrating how effective Python can be for powerful pentesting that keeps your software safe. Comprising of three key modules, follow each one to push your Python and security skills to the next level. In the first module, we'll show you how to get to grips with the fundamentals. This means you'll quickly find out how to tackle some of the common challenges facing pentesters using custom Python tools designed specifically for your needs. You'll also learn what tools to use and when, giving you complete confidence when deploying your pentester tools to combat any potential threat. In the next module you'll begin hacking into the application layer. Covering everything from parameter tampering, DDoS, XSS and SQL injection, it will build on the knowledge and skills you learned in the first module to make you an even more fluent security expert. Finally in the third module, you'll find more than 60 Python pentesting recipes. We think this will soon become your trusted resource for any pentesting situation. This Learning Path combines some of the best that Packt has to offer in one complete, curated package. It includes content from the following Packt products: Learning Penetration Testing with Python by Christopher Duffy Python Penetration Testing Essentials by Mohit Python Web Penetration Testing Cookbook by Cameron Buchanan, Terry Ip, Andrew Mabbitt, Benjamin May and Dave Mound Style and approach This course provides

a quick access to powerful, modern tools, and customizable scripts to kick-start the creation of your own Python web penetration testing toolbox.

LEARN PENETRATION TESTING WITH PYTHON 3.X

PERFORM OFFENSIVE PENTESTING AND PREPARE RED TEAMING TO PREVENT NETWORK ATTACKS AND WEB VULNERABILITIES (ENGLISH EDITION)

BPB Publications Identify vulnerabilities across applications, network and systems using simplified cybersecurity scripting

KEY FEATURES

- Exciting coverage on red teaming methodologies and penetration testing techniques.
- Explore the exploitation development environment and process of creating exploit scripts.
- Includes powerful Python libraries to analyze the web and helps identifying critical vulnerabilities.
- Conduct wireless attacks and identify potential threats using Python.

DESCRIPTION This book starts with an understanding of penetration testing and red teaming methodologies and teaches Python 3.x from scratch for those who are not familiar with programming. The book gives the skills of how to create scripts for cracking, and brute force attacks. The second part of this book focuses on the network and wireless level. The book teaches you the skills of how to create an offensive tool using Python 3.x to identify different services and ports using different Python network modules and conducting network attacks. In the network monitoring section, you will be able to monitor layers 3 and 4. And finally, you will be able to conduct different attacks on wireless. The last part of this book focuses on web applications and exploitation developments. It focuses on how to create scripts to extract web information such as links, images, documents, etc. It also focuses on how to create scripts to identify and exploit web vulnerabilities and how to bypass WAF. The last chapter of this book focuses on exploitation development starting with how to play with the stack and then moving on to how to use Python in fuzzing and creating exploitation scripts.

WHAT YOU WILL LEARN

- Learn to code Python scripts from scratch to identify web vulnerabilities.
- Conduct network attacks, create offensive tools, and identify vulnerable services and ports.
- Perform deep monitoring of network up to layers 3 and 4.
- Execute web scraping scripts to extract images, documents, and links.

WHO THIS BOOK IS FOR This book is for Penetration Testers, Security Researchers, Red Teams, Security Auditors and IT Administrators who want to start with an action plan in protecting their IT systems. All you need is some basic understanding of programming concepts and working of IT systems. Hands-on experience with python will be more beneficial but not required.

TABLE OF CONTENTS

1. Start with Penetration Testing and Basic Python
2. Cracking with Python
3. Service and Applications Brute Forcing with Python
- 4.

Python Services Identifications - Ports and Banner 5. Python Network Modules and Nmap 6. Network Monitoring with Python 7. Attacking Wireless with Python 8. Analyze Web Applications with Python 9. Attack Web Application with Python 10. Exploitation Development with Python

PYTHON FOR OFFENSIVE PENTEST

A PRACTICAL GUIDE TO ETHICAL HACKING AND PENETRATION TESTING USING PYTHON

Packt Publishing Ltd Your one-stop guide to using Python, creating your own hacking tools, and making the most out of resources available for this programming language Key Features Comprehensive information on building a web application penetration testing framework using Python Master web application penetration testing using the multi-paradigm programming language Python Detect vulnerabilities in a system or application by writing your own Python scripts Book Description Python is an easy-to-learn and cross-platform programming language that has unlimited third-party libraries. Plenty of open source hacking tools are written in Python, which can be easily integrated within your script. This book is packed with step-by-step instructions and working examples to make you a skilled penetration tester. It is divided into clear bite-sized chunks, so you can learn at your own pace and focus on the areas of most interest to you. This book will teach you how to code a reverse shell and build an anonymous shell. You will also learn how to hack passwords and perform a privilege escalation on Windows with practical examples. You will set up your own virtual hacking environment in VirtualBox, which will help you run multiple operating systems for your testing environment. By the end of this book, you will have learned how to code your own scripts and mastered ethical hacking from scratch. What you will learn Code your own reverse shell (TCP and HTTP) Create your own anonymous shell by interacting with Twitter, Google Forms, and SourceForge Replicate Metasploit features and build an advanced shell Hack passwords using multiple techniques (API hooking, keyloggers, and clipboard hijacking) Exfiltrate data from your target Add encryption (AES, RSA, and XOR) to your shell to learn how cryptography is being abused by malware Discover privilege escalation on Windows with practical examples Countermeasures against most attacks Who this book is for This book is for ethical hackers; penetration testers; students preparing for OSCP, OSCE, GPEN, GXPN, and CEH; information security professionals; cybersecurity consultants; system and network security administrators; and programmers who are keen on learning all about penetration testing.

PRACTICAL WEB PENETRATION TESTING

SECURE WEB APPLICATIONS USING BURP SUITE, NMAP, METASPLOIT, AND MORE

Packt Publishing Ltd Learn how to execute web application penetration testing end-to-end Key Features Build an end-to-end threat model landscape for web application security Learn both web application vulnerabilities and web intrusion testing Associate network vulnerabilities with a web application infrastructure Book Description Companies all over the world want to hire professionals dedicated to application security. Practical Web Penetration Testing focuses on this very trend, teaching you how to conduct application security testing using real-life scenarios. To start with, you'll set up an environment to perform web application penetration testing. You will then explore different penetration testing concepts such as threat modeling, intrusion test, infrastructure security threat, and more, in combination with advanced concepts such as Python scripting for automation. Once you are done learning the basics, you will discover end-to-end implementation of tools such as Metasploit, Burp Suite, and Kali Linux. Many companies deliver projects into production by using either Agile or Waterfall methodology. This book shows you how to assist any company with their SDLC approach and helps you on your journey to becoming an application security specialist. By the end of this book, you will have hands-on knowledge of using different tools for penetration testing. What you will learn Learn how to use Burp Suite effectively Use Nmap, Metasploit, and more tools for network infrastructure tests Practice using all web application hacking tools for intrusion tests using Kali Linux Learn how to analyze a web application using application threat modeling Know how to conduct web intrusion tests Understand how to execute network infrastructure tests Master automation of penetration testing functions for maximum efficiency using Python Who this book is for Practical Web Penetration Testing is for you if you are a security professional, penetration tester, or stakeholder who wants to execute penetration testing using the latest and most popular tools. Basic knowledge of ethical hacking would be an added advantage.

HANDS-ON PENETRATION TESTING WITH PYTHON

ENHANCE YOUR ETHICAL HACKING SKILLS TO BUILD AUTOMATED AND INTELLIGENT SYSTEMS

Packt Publishing Implement defensive techniques in your ecosystem successfully with Python Key Features Identify and expose vulnerabilities in your infrastructure with Python Learn custom exploit development . Make robust and

powerful cybersecurity tools with Python Book Description With the current technological and infrastructural shift, penetration testing is no longer a process-oriented activity. Modern-day penetration testing demands lots of automation and innovation; the only language that dominates all its peers is Python. Given the huge number of tools written in Python, and its popularity in the penetration testing space, this language has always been the first choice for penetration testers. Hands-On Penetration Testing with Python walks you through advanced Python programming constructs. Once you are familiar with the core concepts, you'll explore the advanced uses of Python in the domain of penetration testing and optimization. You'll then move on to understanding how Python, data science, and the cybersecurity ecosystem communicate with one another. In the concluding chapters, you'll study exploit development, reverse engineering, and cybersecurity use cases that can be automated with Python. By the end of this book, you'll have acquired adequate skills to leverage Python as a helpful tool to pentest and secure infrastructure, while also creating your own custom exploits. What you will learn Get to grips with Custom vulnerability scanner development Familiarize yourself with web application scanning automation and exploit development Walk through day-to-day cybersecurity scenarios that can be automated with Python Discover enterprise-or organization-specific use cases and threat-hunting automation Understand reverse engineering, fuzzing, buffer overflows , key-logger development, and exploit development for buffer overflows. Understand web scraping in Python and use it for processing web responses Explore Security Operations Centre (SOC) use cases Get to understand Data Science, Python, and cybersecurity all under one hood Who this book is for If you are a security consultant , developer or a cyber security enthusiast with little or no knowledge of Python and want in-depth insight into how the pen-testing ecosystem and python combine to create offensive tools , exploits , automate cyber security use-cases and much more then this book is for you. Hands-On Penetration Testing with Python guides you through the advanced uses of Python for cybersecurity and pen-testing, helping you to better understand security loopholes within your infrastructure .

METASPLOIT PENETRATION TESTING COOKBOOK

Packt Publishing Ltd Over 80 recipes to master the most widely used penetration testing framework.

CODING FOR PENETRATION TESTERS

BUILDING BETTER TOOLS

Elsevier Coding for Penetration Testers discusses the use of various scripting languages in penetration testing. The

book presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages. It also provides a primer on scripting including, but not limited to, Web scripting, scanner scripting, and exploitation scripting. It guides the student through specific examples of custom tool development that can be incorporated into a tester's toolkit as well as real-world scenarios where such tools might be used. This book is divided into 10 chapters that explores topics such as command shell scripting; Python, Perl, and Ruby; Web scripting with PHP; manipulating Windows with PowerShell; scanner scripting; information gathering; exploitation scripting; and post-exploitation scripting. This book will appeal to penetration testers, information security practitioners, and network and system administrators. 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

HANDS-ON PENETRATION TESTING WITH PYTHON

ENHANCE YOUR ETHICAL HACKING SKILLS TO BUILD AUTOMATED AND INTELLIGENT SYSTEMS

Packt Publishing Ltd Implement defensive techniques in your ecosystem successfully with Python Key FeaturesIdentify and expose vulnerabilities in your infrastructure with PythonLearn custom exploit development .Make robust and powerful cybersecurity tools with PythonBook Description With the current technological and infrastructural shift, penetration testing is no longer a process-oriented activity. Modern-day penetration testing demands lots of automation and innovation; the only language that dominates all its peers is Python. Given the huge number of tools written in Python, and its popularity in the penetration testing space, this language has always been the first choice for penetration testers. Hands-On Penetration Testing with Python walks you through advanced Python programming constructs. Once you are familiar with the core concepts, you'll explore the advanced uses of Python in the domain of penetration testing and optimization. You'll then move on to understanding how Python, data science, and the cybersecurity ecosystem communicate with one another. In the concluding chapters, you'll study exploit development, reverse engineering, and cybersecurity use cases that can be automated with Python. By the end of this book, you'll have acquired adequate skills to leverage Python as a helpful tool to pentest and secure infrastructure, while also creating your own custom exploits. What you will learnGet to grips with Custom vulnerability scanner developmentFamiliarize yourself with web application scanning automation and exploit developmentWalk through day-

to-day cybersecurity scenarios that can be automated with Python Discover enterprise-or organization-specific use cases and threat-hunting automation Understand reverse engineering, fuzzing, buffer overflows , key-logger development, and exploit development for buffer overflows. Understand web scraping in Python and use it for processing web responses Explore Security Operations Centre (SOC) use cases Get to understand Data Science, Python, and cybersecurity all under one hood Who this book is for If you are a security consultant , developer or a cyber security enthusiast with little or no knowledge of Python and want in-depth insight into how the pen-testing ecosystem and python combine to create offensive tools , exploits , automate cyber security use-cases and much more then this book is for you. Hands-On Penetration Testing with Python guides you through the advanced uses of Python for cybersecurity and pen-testing, helping you to better understand security loopholes within your infrastructure .

EFFECTIVE PYTHON PENETRATION TESTING

Packt Publishing Ltd Pen test your system like a pro and overcome vulnerabilities by leveraging Python scripts, libraries, and tools About This Book Learn to utilize your Python scripting skills to pentest a computer system, network, and web-application Get proficient at the art of assessing vulnerabilities by conducting effective penetration testing This is the ultimate guide that teaches you how to use Python to protect your systems against sophisticated cyber attacks Who This Book Is For This book is ideal for those who are comfortable with Python or a similar language and need no help with basic programming concepts, but want to understand the basics of penetration testing and the problems pentesters face. What You Will Learn Write Scapy scripts to investigate network traffic Get to know application fingerprinting techniques with Python Understand the attack scripting techniques Write fuzzing tools with pentesting requirements Learn basic attack scripting methods Utilize cryptographic toolkits in Python Automate pentesting with Python tools and libraries In Detail Penetration testing is a practice of testing a computer system, network, or web application to find weaknesses in security that an attacker can exploit. Effective Python Penetration Testing will help you utilize your Python scripting skills to safeguard your networks from cyberattacks. We will begin by providing you with an overview of Python scripting and penetration testing. You will learn to analyze network traffic by writing Scapy scripts and will see how to fingerprint web applications with Python libraries such as ProxMon and Spynner. Moving on, you will find out how to write basic attack scripts, and will develop debugging and reverse engineering skills with Python libraries. Toward the end of the book, you will discover how to utilize cryptography toolkits in Python and how to automate Python tools and libraries. Style and approach This is an expert's guide to Python with a practical based approach, where each chapter will help you improve your penetration testing skills using

Python to become a master pen tester.

WEB SECURITY TESTING COOKBOOK

"O'Reilly Media, Inc." Offering developers an inexpensive way to include testing as part of the development cycle, this cookbook features scores of recipes for testing Web applications, from relatively simple solutions to complex ones that combine several solutions.

KALI LINUX PENETRATION TESTING BIBLE

John Wiley & Sons Your ultimate guide to pentesting with Kali Linux Kali is a popular and powerful Linux distribution used by cybersecurity professionals around the world. Penetration testers must master Kali's varied library of tools to be effective at their work. The Kali Linux Penetration Testing Bible is the hands-on and methodology guide for pentesting with Kali. You'll discover everything you need to know about the tools and techniques hackers use to gain access to systems like yours so you can erect reliable defenses for your virtual assets. Whether you're new to the field or an established pentester, you'll find what you need in this comprehensive guide. Build a modern dockerized environment Discover the fundamentals of the bash language in Linux Use a variety of effective techniques to find vulnerabilities (OSINT, Network Scan, and more) Analyze your findings and identify false positives and uncover advanced subjects, like buffer overflow, lateral movement, and privilege escalation Apply practical and efficient pentesting workflows Learn about Modern Web Application Security Secure SDLC Automate your penetration testing with Python

PENETRATION TESTING

A HANDS-ON INTRODUCTION TO HACKING

No Starch Press 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.

PYTHON PENETRATION TESTING ESSENTIALS

Packt Pub Limited If you are a Python programmer or a security researcher who has basic knowledge of Python programming and want to learn about penetration testing with the help of Python, this book is ideal for you. Even if you are new to the field of ethical hacking, this book can help you find the vulnerabilities in your system so that you are ready to tackle any kind of attack or intrusion.

MASTERING MODERN WEB PENETRATION TESTING

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 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.

KALI LINUX WEB PENETRATION TESTING COOKBOOK

Packt Publishing Ltd Over 80 recipes on how to identify, exploit, and test web application security with Kali Linux 2
About This Book Familiarize yourself with the most common web vulnerabilities a web application faces, and understand how attackers take advantage of them Set up a penetration testing lab to conduct a preliminary assessment of attack surfaces and run exploits Learn how to prevent vulnerabilities in web applications before an attacker can make the most of it **Who This Book Is For** This book is for IT professionals, web developers, security enthusiasts, and security professionals who want an accessible reference on how to find, exploit, and prevent security vulnerabilities in web applications. You should know the basics of operating a Linux environment and have some exposure to security technologies and tools. **What You Will Learn** Set up a penetration testing laboratory in a secure way Find out what information is useful to gather when performing penetration tests and where to look for it Use crawlers and spiders to investigate an entire website in minutes Discover security vulnerabilities in web applications in the web browser and using command-line tools Improve your testing efficiency with the use of automated vulnerability scanners Exploit vulnerabilities that require a complex setup, run custom-made exploits, and prepare for extraordinary scenarios Set up Man in the Middle attacks and use them to identify and exploit security flaws within the communication between users and the web server Create a malicious site that will find and exploit vulnerabilities in

the user's web browser Repair the most common web vulnerabilities and understand how to prevent them becoming a threat to a site's security In Detail Web applications are a huge point of attack for malicious hackers and a critical area for security professionals and penetration testers to lock down and secure. Kali Linux is a Linux-based penetration testing platform and operating system that provides a huge array of testing tools, many of which can be used specifically to execute web penetration testing. This book will teach you, in the form step-by-step recipes, how to detect a wide array of vulnerabilities, exploit them to analyze their consequences, and ultimately buffer attackable surfaces so applications are more secure, for you and your users. Starting from the setup of a testing laboratory, this book will give you the skills you need to cover every stage of a penetration test: from gathering information about the system and the application to identifying vulnerabilities through manual testing and the use of vulnerability scanners to both basic and advanced exploitation techniques that may lead to a full system compromise. Finally, we will put this into the context of OWASP and the top 10 web application vulnerabilities you are most likely to encounter, equipping you with the ability to combat them effectively. By the end of the book, you will have the required skills to identify, exploit, and prevent web application vulnerabilities. Style and approach Taking a recipe-based approach to web security, this book has been designed to cover each stage of a penetration test, with descriptions on how tools work and why certain programming or configuration practices can become security vulnerabilities that may put a whole system, or network, at risk. Each topic is presented as a sequence of tasks and contains a proper explanation of why each task is performed and what it accomplishes.

THE BASICS OF HACKING AND PENETRATION TESTING

ETHICAL HACKING AND PENETRATION TESTING MADE EASY

Elsevier The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn,

Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test.

MASTERING MACHINE LEARNING FOR PENETRATION TESTING

DEVELOP AN EXTENSIVE SKILL SET TO BREAK SELF-LEARNING SYSTEMS USING PYTHON

Packt Publishing Ltd Become a master at penetration testing using machine learning with Python Key Features Identify ambiguities and breach intelligent security systems Perform unique cyber attacks to breach robust systems Learn to leverage machine learning algorithms Book Description Cyber security is crucial for both businesses and individuals. As systems are getting smarter, we now see machine learning interrupting computer security. With the adoption of machine learning in upcoming security products, it's important for pentesters and security researchers to understand how these systems work, and to breach them for testing purposes. This book begins with the basics of machine learning and the algorithms used to build robust systems. Once you've gained a fair understanding of how security products leverage machine learning, you'll dive into the core concepts of breaching such systems. Through practical use cases, you'll see how to find loopholes and surpass a self-learning security system. As you make your way through the chapters, you'll focus on topics such as network intrusion detection and AV and IDS evasion. We'll also cover the best practices when identifying ambiguities, and extensive techniques to breach an intelligent system. By the end of this book, you will be well-versed with identifying loopholes in a self-learning security system and will be able to efficiently breach a machine learning system. What you will learn Take an in-depth look at machine learning Get to know natural language processing (NLP) Understand malware feature engineering Build generative adversarial networks using Python libraries Work on threat hunting with machine learning and the ELK stack Explore the best practices for machine learning Who this book is for This book is for pen testers and security professionals who are interested in learning techniques to break an intelligent security system. Basic knowledge of Python is needed, but no prior knowledge of machine learning is necessary.

BLACK HAT PYTHON

PYTHON PROGRAMMING FOR HACKERS AND PENTESTERS

No Starch Press When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. But just how does the magic happen? In **Black Hat Python**, the latest from Justin Seitz (author of the best-selling **Gray Hat Python**), you'll explore the darker side of Python's capabilities—writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy trojans, and more. You'll learn how to: -Create a trojan command-and-control using GitHub -Detect sandboxing and automate common malware tasks, like keylogging and screenshotting -Escalate Windows privileges with creative process control -Use offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machine -Extend the popular Burp Suite web-hacking tool -Abuse Windows COM automation to perform a man-in-the-browser attack -Exfiltrate data from a network most sneakily Insider techniques and creative challenges throughout show you how to extend the hacks and how to write your own exploits. When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how in **Black Hat Python**. Uses Python 2

BEYOND THE BASIC STUFF WITH PYTHON

BEST PRACTICES FOR WRITING CLEAN CODE

No Starch Press **BRIDGE THE GAP BETWEEN NOVICE AND PROFESSIONAL** You've completed a basic Python programming tutorial or finished Al Sweigart's bestseller, **Automate the Boring Stuff with Python**. What's the next step toward becoming a capable, confident software developer? Welcome to **Beyond the Basic Stuff with Python**. More than a mere collection of advanced syntax and masterful tips for writing clean code, you'll learn how to advance your Python programming skills by using the command line and other professional tools like code formatters, type checkers, linters, and version control. Sweigart takes you through best practices for setting up your development environment, naming variables, and improving readability, then tackles documentation, organization and performance measurement, as well as object-oriented design and the Big-O algorithm analysis commonly used in coding interviews. The skills you learn will boost your ability to program--not just in Python but in any language. You'll learn: • Coding style, and how to use Python's Black auto-formatting tool for cleaner code • Common sources of bugs, and how to

detect them with static analyzers • How to structure the files in your code projects with the Cookiecutter template tool • Functional programming techniques like lambda and higher-order functions • How to profile the speed of your code with Python's built-in timeit and cProfile modules • The computer science behind Big-O algorithm analysis • How to make your comments and docstrings informative, and how often to write them • How to create classes in object-oriented programming, and why they're used to organize code Toward the end of the book you'll read a detailed source-code breakdown of two classic command-line games, the Tower of Hanoi (a logic puzzle) and Four-in-a-Row (a two-player tile-dropping game), and a breakdown of how their code follows the book's best practices. You'll test your skills by implementing the program yourself. Of course, no single book can make you a professional software developer. But **Beyond the Basic Stuff with Python** will get you further down that path and make you a better programmer, as you learn to write readable code that's easy to debug and perfectly Pythonic Requirements: Covers Python 3.6 and higher

WEB PENETRATION TESTING WITH KALI LINUX

EXPLORE THE METHODS AND TOOLS OF ETHICAL HACKING WITH KALI LINUX, 3RD EDITION

Packt Publishing Ltd Build your defense against web attacks with Kali Linux, including command injection flaws, crypto implementation layers, and web application security holes Key Features Know how to set up your lab with Kali Linux Discover the core concepts of web penetration testing Get the tools and techniques you need with Kali Linux Book Description Web Penetration Testing with Kali Linux - Third Edition shows you how to set up a lab, helps you understand the nature and mechanics of attacking websites, and explains classical attacks in great depth. This edition is heavily updated for the latest Kali Linux changes and the most recent attacks. Kali Linux shines when it comes to client-side attacks and fuzzing in particular. From the start of the book, you'll be given a thorough grounding in the concepts of hacking and penetration testing, and you'll see the tools used in Kali Linux that relate to web application hacking. You'll gain a deep understanding of classicalSQL, command-injection flaws, and the many ways to exploit these flaws. Web penetration testing also needs a general overview of client-side attacks, which is rounded out by a long discussion of scripting and input validation flaws. There is also an important chapter on cryptographic implementation flaws, where we discuss the most recent problems with cryptographic layers in the networking stack. The importance of these attacks cannot be overstated, and defending against them is relevant to most internet users and, of course, penetration testers. At the end of the book, you'll use an automated technique called fuzzing to identify

flaws in a web application. Finally, you'll gain an understanding of web application vulnerabilities and the ways they can be exploited using the tools in Kali Linux. What you will learn Learn how to set up your lab with Kali Linux Understand the core concepts of web penetration testing Get to know the tools and techniques you need to use with Kali Linux Identify the difference between hacking a web application and network hacking Expose vulnerabilities present in web servers and their applications using server-side attacks Understand the different techniques used to identify the flavor of web applications See standard attacks such as exploiting cross-site request forgery and cross-site scripting flaws Get an overview of the art of client-side attacks Explore automated attacks such as fuzzing web applications Who this book is for Since this book sets out to cover a large number of tools and security fields, it can work as an introduction to practical security skills for beginners in security. In addition, web programmers and also system administrators would benefit from this rigorous introduction to web penetration testing. Basic system administration skills are necessary, and the ability to read code is a must.

THE WEB APPLICATION HACKER'S HANDBOOK

DISCOVERING AND EXPLOITING SECURITY FLAWS

John Wiley & Sons This book is a practical guide to discovering and exploiting security flaws in web applications. The authors explain each category of vulnerability using real-world examples, screen shots and code extracts. The book is extremely practical in focus, and describes in detail the steps involved in detecting and exploiting each kind of security weakness found within a variety of applications such as online banking, e-commerce and other web applications. The topics covered include bypassing login mechanisms, injecting code, exploiting logic flaws and compromising other users. Because every web application is different, attacking them entails bringing to bear various general principles, techniques and experience in an imaginative way. The most successful hackers go beyond this, and find ways to automate their bespoke attacks. This handbook describes a proven methodology that combines the virtues of human intelligence and computerized brute force, often with devastating results. The authors are professional penetration testers who have been involved in web application security for nearly a decade. They have presented training courses at the Black Hat security conferences throughout the world. Under the alias "PortSwigger", Dafydd developed the popular Burp Suite of web application hack tools.

HACKING AND PENETRATION TESTING WITH LOW POWER DEVICES

Syngress Hacking and Penetration Testing with Low Power Devices shows you how to perform penetration tests using small, low-powered devices that are easily hidden and may be battery-powered. It shows how to use an army of devices, costing less than you might spend on a laptop, from distances of a mile or more. Hacking and Penetration Testing with Low Power Devices shows how to use devices running a version of The Deck, a full-featured penetration testing and forensics Linux distribution, and can run for days or weeks on batteries due to their low power consumption. Author Philip Polstra shows how to use various configurations, including a device the size of a deck of cards that can easily be attached to the back of a computer. While each device running The Deck is a full-featured pen-testing platform, connecting systems together via 802.15.3 networking gives you even more power and flexibility. This reference teaches you how to construct and power these devices, install operating systems, and fill out your toolbox of small low-power devices with hundreds of tools and scripts from the book's companion website. Hacking and Pen Testing with Low Power Devices puts all these tools into your hands and will help keep you at the top of your game performing cutting-edge pen tests from anywhere in the world! Understand how to plan and execute an effective penetration test using an army of low-power devices Learn how to configure and use open-source tools and easy-to-construct low-power devices Leverage IEEE 802.15.4 networking to perform penetration tests from up to a mile away, or use 802.15.4 gateways to perform pen tests from anywhere in the world Access penetration testing operating systems with hundreds of tools and scripts on the book's companion web site

MODERN PYTHON COOKBOOK

Packt Publishing Ltd The latest in modern Python recipes for the busy modern programmer About This Book Develop succinct, expressive programs in Python Learn the best practices and common idioms through carefully explained and structured recipes Discover new ways to apply Python for the new age of development Who This Book Is For The book is for web developers, programmers, enterprise programmers, engineers, big data scientist, and so on. If you are a beginner, Python Cookbook will get you started. If you are experienced, it will expand your knowledge base. A basic knowledge of programming would help. What You Will Learn See the intricate details of the Python syntax and how to use it to your advantage Improve your code readability through functions in Python Manipulate data effectively using built-in data structures Get acquainted with advanced programming techniques in Python Equip yourself with functional and statistical programming features Write proper tests to be sure a program works as advertised Integrate

application software using Python In Detail Python is the preferred choice of developers, engineers, data scientists, and hobbyists everywhere. It is a great scripting language that can power your applications and provide great speed, safety, and scalability. By exposing Python as a series of simple recipes, you can gain insight into specific language features in a particular context. Having a tangible context helps make the language or standard library feature easier to understand. This book comes with over 100 recipes on the latest version of Python. The recipes will benefit everyone ranging from beginner to an expert. The book is broken down into 13 chapters that build from simple language concepts to more complex applications of the language. The recipes will touch upon all the necessary Python concepts related to data structures, OOP, functional programming, as well as statistical programming. You will get acquainted with the nuances of Python syntax and how to effectively use the advantages that it offers. You will end the book equipped with the knowledge of testing, web services, and configuration and application integration tips and tricks. The recipes take a problem-solution approach to resolve issues commonly faced by Python programmers across the globe. You will be armed with the knowledge of creating applications with flexible logging, powerful configuration, and command-line options, automated unit tests, and good documentation. Style and approach This book takes a recipe-based approach, where each recipe addresses specific problems and issues. The recipes provide discussions and insights and an explanation of the problems.

HANDS-ON WEB PENETRATION TESTING WITH METASPLOIT

THE SUBTLE ART OF USING METASPLOIT 5.0 FOR WEB APPLICATION EXPLOITATION

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 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 PENETRATION TESTING COOKBOOK

SECOND EDITION

Packt Publishing Ltd 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.

LEARN PYTHON 3 THE HARD WAY

A VERY SIMPLE INTRODUCTION TO THE TERRIFYINGLY BEAUTIFUL WORLD OF COMPUTERS AND CODE

Addison-Wesley Professional You Will Learn Python 3! Zed Shaw has perfected the world's best system for learning Python 3. Follow it and you will succeed—just like the millions of beginners Zed has taught to date! You bring the discipline, commitment, and persistence; the author supplies everything else. In Learn Python 3 the Hard Way, you'll learn Python by working through 52 brilliantly crafted exercises. Read them. Type their code precisely. (No copying

and pasting!) Fix your mistakes. Watch the programs run. As you do, you'll learn how a computer works; what good programs look like; and how to read, write, and think about code. Zed then teaches you even more in 5+ hours of video where he shows you how to break, fix, and debug your code—live, as he's doing the exercises. Install a complete Python environment Organize and write code Fix and break code Basic mathematics Variables Strings and text Interact with users Work with files Looping and logic Data structures using lists and dictionaries Program design Object-oriented programming Inheritance and composition Modules, classes, and objects Python packaging Automated testing Basic game development Basic web development It'll be hard at first. But soon, you'll just get it—and that will feel great! This course will reward you for every minute you put into it. Soon, you'll know one of the world's most powerful, popular programming languages. You'll be a Python programmer. This Book Is Perfect For Total beginners with zero programming experience Junior developers who know one or two languages Returning professionals who haven't written code in years Seasoned professionals looking for a fast, simple, crash course in Python 3

BLACK HAT PYTHON, 2ND EDITION

PYTHON PROGRAMMING FOR HACKERS AND PENTESTERS

No Starch Press Fully-updated for Python 3, the second edition of this worldwide bestseller (over 100,000 copies sold) explores the stealthier side of programming and brings you all new strategies for your hacking projects. When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. In Black Hat Python, 2nd Edition, you'll explore the darker side of Python's capabilities—writing network sniffers, stealing email credentials, brute forcing directories, crafting mutation fuzzers, infecting virtual machines, creating stealthy trojans, and more. The second edition of this bestselling hacking book contains code updated for the latest version of Python 3, as well as new techniques that reflect current industry best practices. You'll also find expanded explanations of Python libraries such as ctypes, struct, lxml, and BeautifulSoup, and dig deeper into strategies, from splitting bytes to leveraging computer-vision libraries, that you can apply to future hacking projects. You'll learn how to:

- Create a trojan command-and-control using GitHub
- Detect sandboxing and automate common malware tasks, like keylogging and screenshotting
- Escalate Windows privileges with creative process control
- Use offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machine
- Extend the popular Burp Suite web-hacking tool
- Abuse Windows COM automation to perform a man-in-the-browser attack
- Exfiltrate data from a network most sneakily

When it comes to offensive security, your ability to create powerful tools on the fly is

indispensable. Learn how with the second edition of **Black Hat Python**. New to this edition: All Python code has been updated to cover Python 3 and includes updated libraries used in current Python applications. Additionally, there are more in-depth explanations of the code and the programming techniques have been updated to current, common tactics. Examples of new material that you'll learn include how to sniff network traffic, evade anti-virus software, brute-force web applications, and set up a command-and-control (C2) system using GitHub.

BEGINNING PROGRAMMING WITH PYTHON FOR DUMMIES

John Wiley & Sons The easy way to learn programming fundamentals with Python Python is a remarkably powerful and dynamic programming language that's used in a wide variety of application domains. Some of its key distinguishing features include a very clear, readable syntax, strong introspection capabilities, intuitive object orientation, and natural expression of procedural code. Plus, Python features full modularity, supporting hierarchical packages, exception-based error handling, and modules easily written in C, C++, Java, R, or .NET languages, such as C#. In addition, Python supports a number of coding styles that include: functional, imperative, object-oriented, and procedural. Due to its ease of use and flexibility, Python is constantly growing in popularity—and now you can wear your programming hat with pride and join the ranks of the pros with the help of this guide. Inside, expert author John Paul Mueller gives a complete step-by-step overview of all there is to know about Python. From performing common and advanced tasks, to collecting data, to interacting with package—this book covers it all! Use Python to create and run your first application Find out how to troubleshoot and fix errors Learn to work with Anaconda and use Magic Functions Benefit from completely updated and revised information since the last edition If you've never used Python or are new to programming in general, **Beginning Programming with Python For Dummies** is a helpful resource that will set you up for success.

BEGINNING ETHICAL HACKING WITH KALI LINUX

COMPUTATIONAL TECHNIQUES FOR RESOLVING SECURITY ISSUES

Apress Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of **Beginning Ethical Hacking with Kali Linux**. With the theory out of the way, you'll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web

server and acquire the skill to be anonymous . When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how Sniffjoke prevents poisoning, how to analyze protocols with Wireshark, and using sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will Learn Master common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as Sniffjoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systems Who This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming.

THE ULTIMATE KALI LINUX BOOK

PERFORM ADVANCED PENETRATION TESTING USING NMAP, METASPLOIT, AIRCRACK-NG, AND EMPIRE

Packt Publishing Ltd Explore the latest ethical hacking tools and techniques to perform penetration testing from scratch Key Features Learn to compromise enterprise networks with Kali Linux Gain comprehensive insights into security concepts using advanced real-life hacker techniques Use Kali Linux in the same way ethical hackers and penetration testers do to gain control of your environment Book Description Kali Linux is the most popular and advanced penetration testing Linux distribution within the cybersecurity industry. Using Kali Linux, a cybersecurity professional will be able to discover and exploit various vulnerabilities and perform advanced penetration testing on

both enterprise wired and wireless networks. This book is a comprehensive guide for those who are new to Kali Linux and penetration testing that will have you up to speed in no time. Using real-world scenarios, you'll understand how to set up a lab and explore core penetration testing concepts. Throughout this book, you'll focus on information gathering and even discover different vulnerability assessment tools bundled in Kali Linux. You'll learn to discover target systems on a network, identify security flaws on devices, exploit security weaknesses and gain access to networks, set up Command and Control (C2) operations, and perform web application penetration testing. In this updated second edition, you'll be able to compromise Active Directory and exploit enterprise networks. Finally, this book covers best practices for performing complex web penetration testing techniques in a highly secured environment. By the end of this Kali Linux book, you'll have gained the skills to perform advanced penetration testing on enterprise networks using Kali Linux. What you will learn

- Explore the fundamentals of ethical hacking
- Understand how to install and configure Kali Linux
- Perform asset and network discovery techniques
- Focus on how to perform vulnerability assessments
- Exploit the trust in Active Directory domain services
- Perform advanced exploitation with Command and Control (C2) techniques
- Implement advanced wireless hacking techniques
- Become well-versed with exploiting vulnerable web applications

Who this book is for This pentesting book is for students, trainers, cybersecurity professionals, cyber enthusiasts, network security professionals, ethical hackers, penetration testers, and security engineers. If you do not have any prior knowledge and are looking to become an expert in penetration testing using the Kali Linux operating system (OS), then this book is for you.

APACHE SPARK FOR DATA SCIENCE COOKBOOK

Packt Publishing Ltd Over insightful 90 recipes to get lightning-fast analytics with Apache Spark About This Book Use Apache Spark for data processing with these hands-on recipes Implement end-to-end, large-scale data analysis better than ever before Work with powerful libraries such as MLLib, SciPy, NumPy, and Pandas to gain insights from your data Who This Book Is For This book is for novice and intermediate level data science professionals and data analysts who want to solve data science problems with a distributed computing framework. Basic experience with data science implementation tasks is expected. Data science professionals looking to skill up and gain an edge in the field will find this book helpful. What You Will Learn Explore the topics of data mining, text mining, Natural Language Processing, information retrieval, and machine learning. Solve real-world analytical problems with large data sets. Address data science challenges with analytical tools on a distributed system like Spark (apt for iterative algorithms), which offers in-memory processing and more flexibility for data analysis at scale. Get hands-on experience with algorithms like

Classification, regression, and recommendation on real datasets using Spark MLlib package. Learn about numerical and scientific computing using NumPy and SciPy on Spark. Use Predictive Model Markup Language (PMML) in Spark for statistical data mining models. In Detail Spark has emerged as the most promising big data analytics engine for data science professionals. The true power and value of Apache Spark lies in its ability to execute data science tasks with speed and accuracy. Spark's selling point is that it combines ETL, batch analytics, real-time stream analysis, machine learning, graph processing, and visualizations. It lets you tackle the complexities that come with raw unstructured data sets with ease. This guide will get you comfortable and confident performing data science tasks with Spark. You will learn about implementations including distributed deep learning, numerical computing, and scalable machine learning. You will be shown effective solutions to problematic concepts in data science using Spark's data science libraries such as MLlib, Pandas, NumPy, SciPy, and more. These simple and efficient recipes will show you how to implement algorithms and optimize your work. Style and approach This book contains a comprehensive range of recipes designed to help you learn the fundamentals and tackle the difficulties of data science. This book outlines practical steps to produce powerful insights into Big Data through a recipe-based approach.

KALI LINUX INTRUSION AND EXPLOITATION COOKBOOK

Packt Publishing Ltd Over 70 recipes for system administrators or DevOps to master Kali Linux 2 and perform effective security assessments About This Book Set up a penetration testing lab to conduct a preliminary assessment of attack surfaces and run exploits Improve your testing efficiency with the use of automated vulnerability scanners Work through step-by-step recipes to detect a wide array of vulnerabilities, exploit them to analyze their consequences, and identify security anomalies Who This Book Is For This book is intended for those who want to know more about information security. In particular, it's ideal for system administrators and system architects who want to ensure that the infrastructure and systems they are creating and managing are secure. This book helps both beginners and intermediates by allowing them to use it as a reference book and to gain in-depth knowledge. What You Will Learn Understand the importance of security assessments over merely setting up and managing systems/processes Familiarize yourself with tools such as OPENVAS to locate system and network vulnerabilities Discover multiple solutions to escalate privileges on a compromised machine Identify security anomalies in order to make your infrastructure secure and further strengthen it Acquire the skills to prevent infrastructure and application vulnerabilities Exploit vulnerabilities that require a complex setup with the help of Metasploit In Detail With the increasing threats of breaches and attacks on critical infrastructure, system administrators and architects can use Kali

Linux 2.0 to ensure their infrastructure is secure by finding out known vulnerabilities and safeguarding their infrastructure against unknown vulnerabilities. This practical cookbook-style guide contains chapters carefully structured in three phases - information gathering, vulnerability assessment, and penetration testing for the web, and wired and wireless networks. It's an ideal reference guide if you're looking for a solution to a specific problem or learning how to use a tool. We provide hands-on examples of powerful tools/scripts designed for exploitation. In the final section, we cover various tools you can use during testing, and we help you create in-depth reports to impress management. We provide system engineers with steps to reproduce issues and fix them. Style and approach This practical book is full of easy-to-follow recipes with based on real-world problems faced by the authors. Each recipe is divided into three sections, clearly defining what the recipe does, what you need, and how to do it. The carefully structured recipes allow you to go directly to your topic of interest.

IOT PENETRATION TESTING COOKBOOK

IDENTIFY VULNERABILITIES AND SECURE YOUR SMART DEVICES

Packt Publishing Ltd Over 80 recipes to master IoT security techniques. About This Book Identify vulnerabilities in IoT device architectures and firmware using software and hardware pentesting techniques Understand radio communication analysis with concepts such as sniffing the air and capturing radio signals A recipe based guide that will teach you to pentest new and unique set of IoT devices. Who This Book Is For This book targets IoT developers, IoT enthusiasts, pentesters, and security professionals who are interested in learning about IoT security. Prior knowledge of basic pentesting would be beneficial. What You Will Learn Set up an IoT pentesting lab Explore various threat modeling concepts Exhibit the ability to analyze and exploit firmware vulnerabilities Demonstrate the automation of application binary analysis for iOS and Android using MobSF Set up a Burp Suite and use it for web app testing Identify UART and JTAG pinouts, solder headers, and hardware debugging Get solutions to common wireless protocols Explore the mobile security and firmware best practices Master various advanced IoT exploitation techniques and security automation In Detail IoT is an upcoming trend in the IT industry today; there are a lot of IoT devices on the market, but there is a minimal understanding of how to safeguard them. If you are a security enthusiast or pentester, this book will help you understand how to exploit and secure IoT devices. This book follows a recipe-based approach, giving you practical experience in securing upcoming smart devices. It starts with practical recipes on how to analyze IoT device architectures and identify vulnerabilities. Then, it focuses on enhancing your pentesting skill set, teaching you how to

exploit a vulnerable IoT device, along with identifying vulnerabilities in IoT device firmware. Next, this book teaches you how to secure embedded devices and exploit smart devices with hardware techniques. Moving forward, this book reveals advanced hardware pentesting techniques, along with software-defined, radio-based IoT pentesting with Zigbee and Z-Wave. Finally, this book also covers how to use new and unique pentesting techniques for different IoT devices, along with smart devices connected to the cloud. By the end of this book, you will have a fair understanding of how to use different pentesting techniques to exploit and secure various IoT devices. Style and approach This recipe-based book will teach you how to use advanced IoT exploitation and security automation.