Python Web Penetration Testing Cookbook

Kali Linux - An Ethical Hacker's Cookbook
Python Penetration Testing Cookbook
Metasploit Penetration Testing Cookbook
CompTIA Security+ Certification Guide
How to Hack Like a Ghost
Die Kunst des Einbruchs
Bug Bounty Hunting Essentials
Die Kunst des Human Hacking: Social Engineering-Deutsche Ausgabe
IoT Penetration Testing Cookbook
Python: Penetration Testing for Developers
Mastering Machine Learning for Penetration Testing
PHP & MySQL von Kopf bis Fuss
Apache Spark for Data Science Cookbook
Hacking
Mehr Hacking mit Python
Hands-On Red Team Tactics
Kali Linux Network Scanning Cookbook
Learning zANTI2 for Android Pentesting
Kali Linux Web Penetration Testing Cookbook
Python Penetration Testing Essentials
Violent Python
Machine Learning for Cybersecurity Cookbook
Python for Cybersecurity Cookbook
Artificial Intelligence with Python
16th International Conference on Cyber Warfare and Security
Python Penetration Testing Cookbook

Python for Offensive PenTest
Hands-On Cryptography with Python
Modern Python Cookbook
Zed Attack Proxy Cookbook
Bilgisayar Sistemlerinde Güvenlik Ve Gizlilik
Snort Cookbook
Die Kunst der Täuschung
Kuckucksei
Learning Python Web Penetration Testing
Effective Python Penetration Testing
Kali Linux Intrusion and Exploitation Cookbook
Kali Linux Web Penetration Testing Cookbook
Python Web Penetration Testing Cookbook

Python Web Penetration Testing Cookbook
Downloaded from ecobankpayservices.ecobank.com *by guest*

SKYLAR CRUZ

Kali Linux - An Ethical Hacker's Cookbook Packt Publishing Ltd
›Kuckucksei‹ schildert bis ins Detail die hochdramatische Jagd nach deutschen Hackern, die in amerikanische Computernetze eingedrungen waren. Es ist der autobiografische Report eines amerikanischen Computercracks, der leidenschaftlich für die Sicherheit der Datennetze kämpft. (Dieser Text bezieht sich auf eine frühere Ausgabe.)
Python Penetration Testing Cookbook Academic Conferences Limited
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.

Metasploit Penetration Testing Cookbook

Newnes

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

CompTIA Security+ Certification Guide

Packt Publishing Ltd

Over 60 hands-on recipes to pen test networks using Python to discover vulnerabilities and find a recovery pathAbout 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 timeWho This Book Is ForThis 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 ScapyIn DetailPenetration 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.

How to Hack Like a Ghost 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.
Die Kunst des Einbruchs 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 Scrappy 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.
Bug Bounty Hunting Essentials Packt Publishing Ltd
Learn how to use Python for vulnerability scanning, malware analysis, penetration testing, and more KEY FEATURES ● Get familiar with the different aspects of cybersecurity, such as network security, malware analysis, and penetration testing. ● Implement defensive strategies to protect systems, networks, and data from cyber threats. ● Discover advanced offensive techniques for penetration testing, exploiting vulnerabilities, and assessing overall security posture. DESCRIPTION Python is a powerful and versatile programming language that can be used for a wide variety of tasks, including general-purpose applications and specific use cases in cybersecurity. This book is a comprehensive guide to solving simple to moderate complexity problems in cybersecurity using Python. It starts

with fundamental issues in reconnaissance and then moves on to the depths of the topics such as forensic analysis, malware and phishing analysis, and working with wireless devices. Furthermore, it also covers defensive and offensive security topics, such as system hardening, discovery and implementation, defensive security techniques, offensive security techniques, and penetration testing. By the end of this book, you will have a strong understanding of how to use Python for cybersecurity and be able to solve problems and create solutions independently. WHAT YOU WILL LEARN ● Learn how to use Python for cyber forensic analysis. ● Explore ways to analyze malware and phishing-based compromises. ● Use network utilities to gather information, monitor network activity, and troubleshoot issues. ● Learn how to extract and analyze hidden information in digital files. ● Examine source code for vulnerabilities and reverse engineering to understand software behavior. WHO THIS BOOK IS FOR The book is for a wide range of people interested in cybersecurity, including professionals, researchers, educators, students, and those considering a career in the field. TABLE OF CONTENTS 1. Getting Started 2. Passive Reconnaissance 3. Active Reconnaissance 4. Development Environment for Advanced Techniques 5. Forensic Analysis 6. Metadata Extraction and Parsing 7. Malware and Phishing Analysis 8. Working with Wireless Devices 9. Working with Network Utilities 10. Source Code Review and Reverse Engineering 11. System Hardening, Discovery, and Implementation 12. Defensive Security Techniques 13. Offensive Security Techniques and Pen Testing

Die Kunst des Human Hacking: Social Engineering-Deutsche Ausgabe 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.

IoT Penetration Testing Cookbook Packt Publishing Ltd

Wenn es um die Entwicklung leistungsfähiger und effizienter Hacking-Tools geht, ist Python für die meisten Sicherheitsanalytiker die Sprache der Wahl. Doch wie genau funktioniert das? In dem neuesten Buch von Justin Seitz - dem Autor des Bestsellers "Hacking mit Python" - entdecken Sie Pythons dunkle Seite. Sie entwickeln Netzwerk-Sniffer, manipulieren Pakete, infizieren virtuelle Maschinen, schaffen unsichtbare Trojaner und vieles mehr. Sie lernen praktisch, wie man • einen "Command-and-Control"-Trojaner mittels GitHub schafft • Sandboxing erkennt und gängige Malware-Aufgaben wie Keylogging und Screenshotting automatisiert • Windows-Rechte mittels kreativer Prozesskontrolle ausweitet • offensive Speicherforensik-Tricks nutzt, um Passwort-Hashes abzugreifen und Shellcode in virtuelle Maschinen einzuspeisen • das beliebte Web-Hacking-Tool Burp erweitert • die Windows COM-Automatisierung nutzt, um einen Man-in-the-Middle-Angriff durchzuführen • möglichst unbemerkt Daten aus einem Netzwerk abgreift Eine Reihe von Insider-Techniken und kreativen Aufgaben zeigen Ihnen, wie Sie die Hacks erweitern und eigene Exploits entwickeln können.

Python: Penetration Testing for Developers Packt Publishing Ltd

Mitnick führt den Leser in die Denk- und Handlungsweise des Social Engineering ein, beschreibt konkrete Betrugsszenarien und zeigt eindrucksvoll die dramatischen Konsequenzen, die sich daraus ergeben. Dabei nimmt Mitnick sowohl die Perspektive des Angreifers als auch des Opfers ein und erklärt damit sehr eindrucksvoll, wieso die Täuschung so erfolgreich war - und wie man sich effektiv dagegen schützen kann.

Mastering Machine Learning for Penetration Testing Packt Publishing Ltd

Discover the most common web vulnerabilities and prevent them from becoming a threat to your site's security Key Features Familiarize yourself with the most common web vulnerabilities Conduct a preliminary assessment of attack surfaces and run exploits in your lab Explore new tools in the Kali Linux ecosystem for web penetration testing Book Description 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 that provides a broad array of testing tools, many of which can be used to execute web penetration testing. Kali

Linux Web Penetration Testing Cookbook gives you the skills you need to cover every stage of a penetration test – from gathering information about the system and application, to identifying vulnerabilities through manual testing. You will also cover the use of vulnerability scanners and look at basic and advanced exploitation techniques that may lead to a full system compromise. You will start by setting up a testing laboratory, exploring the latest features of tools included in Kali Linux and performing a wide range of tasks with OWASP ZAP, Burp Suite and other web proxies and security testing tools. As you make your way through the book, you will learn how to use automated scanners to find security flaws in web applications and understand how to bypass basic security controls. In the concluding chapters, you will look at what you have learned in the context of the Open Web Application Security Project (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 this book, you will have acquired the skills you need to identify, exploit, and prevent web application vulnerabilities. What you will learn Set up a secure penetration testing laboratory Use proxies, crawlers, and spiders to investigate an entire website Identify cross-site scripting and client-side vulnerabilities Exploit vulnerabilities that allow the insertion of code into web applications Exploit vulnerabilities that require complex setups Improve testing efficiency using automated vulnerability scanners Learn how to circumvent security controls put in place to prevent attacks Who this book is for Kali Linux Web Penetration Testing Cookbook 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. The basics of operating a Linux environment and prior exposure to security technologies and tools are necessary.

PHP & MySQL von Kopf bis Fuss Packt Publishing Ltd

These proceedings represent the work of contributors to the 16th International Conference on Cyber Warfare and Security (ICCWS 2021), hosted by joint collaboration of Tennessee Tech Cybersecurity Education, Research and Outreach Center (CEROC), Computer Science department and the Oak Ridge National Laboratory, Tennessee on 25-26 February 2021. The Conference Co-Chairs are Dr. Juan Lopez Jr, Oak Ridge National Laboratory, Tennessee, and Dr. Ambareen Siraj, Tennessee Tech's Cybersecurity Education, Research and Outreach Center (CEROC), and the Program Chair is Dr. Kalyan Perumalla, from Oak Ridge National Laboratory, Tennessee.

Apache Spark for Data Science Cookbook BPB Publications

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.

Hacking 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.

Mehr Hacking mit Python Packt Publishing Ltd

Dive into security testing and web app scanning with ZAP, a powerful OWASP security tool Purchase of the print or Kindle book includes a free PDF eBook Key FeaturesMaster ZAP to protect your systems from different cyber attacksLearn cybersecurity best practices using this step-by-step guide packed with practical examplesImplement advanced testing techniques, such as XXE attacks and Java deserialization, on web applicationsBook Description Maintaining your cybersecurity posture in the ever-changing, fast-paced security landscape requires constant attention and advancements. This book will help you safeguard your organization using the free and open source OWASP Zed Attack Proxy (ZAP) tool, which allows you to test for vulnerabilities and exploits with the same functionality as a licensed tool. Zed Attack Proxy Cookbook contains a vast array of practical recipes to help you set up, configure, and use ZAP to protect your vital systems from various adversaries. If you're interested in cybersecurity or working as a cybersecurity professional, this book will help you master ZAP. You'll start with an overview of ZAP and understand how to set up a basic lab environment for hands-

on activities over the course of the book. As you progress, you'll go through a myriad of step-by-step recipes detailing various types of exploits and vulnerabilities in web applications, along with advanced techniques such as Java deserialization. By the end of this ZAP book, you'll be able to install and deploy ZAP, conduct basic to advanced web application penetration attacks, use the tool for API testing, deploy an integrated BOAST server, and build ZAP into a continuous integration and continuous delivery (CI/CD) pipeline. What you will learnInstall ZAP on different operating systems or environmentsExplore how to crawl, passively scan, and actively scan web appsDiscover authentication and authorization exploitsConduct client-side testing by examining business logic flawsUse the BOAST server to conduct out-of-band attacksUnderstand the integration of ZAP into the final stages of a CI/CD pipelineWho this book is for This book is for cybersecurity professionals, ethical hackers, application security engineers, DevSecOps engineers, students interested in web security, cybersecurity enthusiasts, and anyone from the open source cybersecurity community looking to gain expertise in ZAP. Familiarity with basic cybersecurity concepts will be helpful to get the most out of this book.

Hands-On Red Team Tactics 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.

Kali Linux Network Scanning Cookbook MITP-Verlags GmbH & Co. KG

Kevin Mitnick, einst der meistgesuchte Verbrecher der USA, saß fünf Jahre im Gefängnis, weil er in zahlreiche Netzwerke großer Firmen eingebrochen war. Heute ist er rehabilitiert, gilt aber nach wie vor weltweit als Prototyp des Hackers. Seit längerer Zeit hat Mitnick in der Hackerszene nach authentischen und spannenden Geschichten gesucht, die auch für Sicherheitsverantwortliche in Firmen hoch-interessante Erkenntnisse abwerfen. Die hier vorliegende Sammlung von Geschichten ist das Ergebnis dieser Suche. „Tauchen Sie aus der Sicherheit und Geborgenheit Ihres Lesesessels ein in die feindselige Welt der Computerkriminalität. Mitnick präsentiert zehn packende Kapitel, jedes das Ergebnis eines Interviews mit einem echten Hacker, der von einem echten Angriff erzählt. Pflichtlektüre für jeden, der sich für Computersicherheit interessiert.“ Tom Parker, Computer-Sicherheitsanalytiker und Gründer der Global InterSec LLC

Learning zANTI2 for Android Pentesting dpunkt.verlag

Kali Linux Network Scanning Cookbook is intended for information security professionals and casual security enthusiasts alike. It will provide the foundational principles for the novice reader but will also introduce scripting techniques and in-depth analysis for the more advanced audience. Whether you

are brand new to Kali Linux or a seasoned veteran, this book will aid in both understanding and ultimately mastering many of the most powerful and useful scanning techniques in the industry. It is assumed that the reader has some basic security testing experience.

Kali Linux Web Penetration Testing Cookbook MITP-Verlags GmbH & Co. KG

Your one-stop guide to learning and implementing Red Team tactics effectively Key FeaturesTarget a complex enterprise environment in a Red Team activityDetect threats and respond to them with a real-world cyber-attack simulationExplore advanced penetration testing tools and techniquesBook Description Red Teaming is used to enhance security by performing simulated attacks on an organization in order to detect network and system vulnerabilities. Hands-On Red Team Tactics starts with an overview of pentesting and Red Teaming, before giving you an introduction to few of the latest pentesting tools. We will then move on to exploring Metasploit and getting to grips with Armitage. Once you have studied the fundamentals, you will learn how to use Cobalt Strike and how to set up its team server. The book introduces some common lesser known techniques for pivoting and how to pivot over SSH, before using Cobalt Strike to pivot. This comprehensive guide demonstrates advanced methods of post-exploitation using Cobalt Strike and introduces you to Command and Control (C2) servers and redirectors. All this will help you achieve persistence using beacons and data exfiltration, and will also give you the chance to run through the methodology to use Red Team activity tools such as Empire during a Red Team activity on Active Directory and Domain Controller. In addition to this, you will explore maintaining persistent access, staying untraceable, and getting reverse connections over different C2 covert channels. By the end of this book, you will have learned about advanced penetration testing tools, techniques to get reverse shells over encrypted channels, and processes for post-exploitation. What you will learnGet started with red team engagements using lesser-known methodsExplore intermediate and advanced levels of post-exploitation techniquesGet acquainted with all the tools and frameworks included in the Metasploit frameworkDiscover the art of getting stealthy access to systems via Red TeamingUnderstand the concept of redirectors to add further anonymity to your C2Get to grips with different uncommon techniques for data exfiltrationWho this book is for Hands-On Red Team Tactics is for you if you are an IT professional, pentester, security consultant, or ethical hacker interested in the IT security domain and wants to go beyond Penetration Testing. Prior knowledge of penetration testing is beneficial.

Python Penetration Testing Essentials "O'Reilly Media, Inc."

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.

Related with Python Web Penetration Testing Cookbook:
© Python Web Penetration Testing Cookbook The Cask Of Amontillado Digital Escape Room Answer Key Pdf
© Python Web Penetration Testing Cookbook The Biggest Winner Math Challenge
© Python Web Penetration Testing Cookbook The Biology Of Trauma