Python For Security Professionals Training Class

Leverage Python scripts and libraries to overcome networking and security issues
Automate web penetration testing activities using Python
Learning Data Mining with Python
Python Programming for Hackers and Reverse Engineers
Python for Cybersecurity
A Guided Tour Through the Wilds of Software Security
A practical guide to ethical hacking and penetration testing using Python
Mastering Machine Learning for Penetration Testing
Python for Offensive PenTest
Learn Ethical Hacking from Scratch
Python Programming for Hackers and Pentesters
Learning Python Web Penetration Testing
Analysis, Visualization and Dashboards
Gray Hat Python
Beginning Ethical Hacking with Python

Kali Linux Wireless Penetration Testing: Beginner's Guide
Learn Python 3 the Hard Way
A Bug Hunter's Diary
Artificial Intelligence with Python
Tourism-Oriented Policing and Protective Services
Massive Open Online Courses (MOOCs) For Everyone
A comprehensive guide to getting started in cybersecurity
Automate the Boring Stuff with Python, 2nd Edition
Practical Machine Learning for Data Analysis Using Python
Cyber Security on Azure
Collecting Data from the Modern Web
Data Wrangling with Pandas, NumPy, and IPython
Develop an extensive skill set to break self-learning systems using Python
Your stepping stone to penetration testing
Backtrack 5 Wireless Penetration Testing
Over 80 recipes on how to implement machine learning algorithms for building security systems using Python
Cybersecurity: The Beginner's Guide
Mastering Python for Networking and Security
A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security

Engineers
Black Hat Python, 2nd Edition
Computer Programming and Cyber Security for Beginners
Over 80 Recipes on How to Implement Machine Learning Algorithms for Building Security Systems Using Python
This Book Includes: Python Machine Learning, SQL, Linux, Hacking with Kali Linux, Ethical Hacking. Coding and Cybersecurity Fundamentals.
Safeguard your system by making your machines intelligent using the Python ecosystem
Python for Data Analysis

ROBERTSON OCONNELL

Leverage Python scripts and libraries to overcome networking and security issues "O'Reilly Media, Inc."
Learn web scraping and crawling techniques to access unlimited data from any web source in any format. With this practical guide, you'll learn how to use Python scripts and web APIs to gather and process data from thousands—or even millions—of web pages at once. Ideal for programmers, security professionals, and web administrators familiar with Python, this book not

only teaches basic web scraping mechanics, but also delves into more advanced topics, such as analyzing raw data or using scrapers for frontend website testing. Code samples are available to help you understand the concepts in practice. Learn how to parse complicated HTML pages Traverse multiple pages and sites Get a general overview of APIs and how they work Learn several methods for storing the data you scrape Download, read, and extract data from documents Use tools and techniques to clean badly formatted data Read and write natural languages Crawl through forms and logins Understand how to scrape JavaScript Learn image processing and text recognition

Automate web penetration testing activities using Python

Packt Publishing Ltd

Whether you're searching for new or additional opportunities, information security can be vast and overwhelming. In this practical guide, author Christina Morillo introduces technical knowledge from a diverse range of experts in the infosec field. Through 97 concise and useful tips, you'll learn how to expand your skills and solve common issues by working through everyday security problems. You'll also receive valuable guidance from professionals on how to navigate your career within this industry. How do you get buy-in from the C-suite for your security program? How do you establish an incident and disaster response

plan? This practical book takes you through actionable advice on a wide variety of infosec topics, including thought-provoking questions that drive the direction of the field. Continuously Learn to Protect Tomorrow's Technology--Alyssa Columbus Fight in Cyber Like the Military Fights in the Physical--Andrew Harris Keep People at the Center of Your Work--Camille Stewart Infosec Professionals Need to Know Operational Resilience--Ann Johnson Taking Control of Your Own Journey--Antoine Middleton Security, Privacy, and Messy Data Webs: Taking Back Control in Third-Party Environments--Ben Brook Every Information Security Problem Boils Down to One Thing--Ben Smith Focus on the WHAT and the Why First, Not the Tool--Christina Morillo

Learning Data Mining with Python Packt Publishing Ltd

Python Crash Course is a fast-paced, thorough introduction to Python that will have you writing programs, solving problems, and making things that work in no time. In the first half of the book, you'll learn about basic programming concepts, such as lists, dictionaries, classes, and loops, and practice writing clean and readable code with exercises for each topic. You'll also learn how to make your programs interactive and how to test your code safely before adding it to a project. In the second half of the book, you'll put your new knowledge into practice with three substantial projects: a

Space Invaders–inspired arcade game, data visualizations with Python’s super-handy libraries, and a simple web app you can deploy online. As you work through Python Crash Course you’ll learn how to: –Use powerful Python libraries and tools, including matplotlib, NumPy, and Pygal –Make 2D games that respond to keypresses and mouse clicks, and that grow more difficult as the game progresses –Work with data to generate interactive visualizations –Create and customize Web apps and deploy them safely online –Deal with mistakes and errors so you can solve your own programming problems If you’ve been thinking seriously about digging into programming, Python Crash Course will get you up to speed and have you writing real programs fast. Why wait any longer? Start your engines and code! Uses Python 2 and 3

Python Programming for Hackers and Reverse Engineers No Starch Press

Leverage the power of Python and statistical modeling techniques for building accurate predictive models Key Features Get introduced to Python's rich suite of libraries for statistical modeling Implement regression, clustering and train neural networks from scratch Includes real-world examples on training end-to-end machine learning systems in Python Book Description Python's ease of use and multi-purpose nature has led it to become the choice of tool

for many data scientists and machine learning developers today. Its rich libraries are widely used for data analysis, and more importantly, for building state-of-the-art predictive models. This book takes you through an exciting journey, of using these libraries to implement effective statistical models for predictive analytics. You'll start by diving into classical statistical analysis, where you will learn to compute descriptive statistics using pandas. You will look at supervised learning, where you will explore the principles of machine learning and train different machine learning models from scratch. You will also work with binary prediction models, such as data classification using k-nearest neighbors, decision trees, and random forests. This book also covers algorithms for regression analysis, such as ridge and lasso regression, and their implementation in Python. You will also learn how neural networks can be trained and deployed for more accurate predictions, and which Python libraries can be used to implement them. By the end of this book, you will have all the knowledge you need to design, build, and deploy enterprise-grade statistical models for machine learning using Python and its rich ecosystem of libraries for predictive analytics. What you will learn Understand the importance of statistical modeling Learn about the various Python packages for statistical analysis Implement

algorithms such as Naive Bayes, random forests, and more Build predictive models from scratch using Python's scikit-learn library Implement regression analysis and clustering Learn how to train a neural network in Python Who this book is for If you are a data scientist, a statistician or a machine learning developer looking to train and deploy effective machine learning models using popular statistical techniques, then this book is for you. Knowledge of Python programming is required to get the most out of this book.

Python for Cybersecurity Newnes

Python for Everybody is designed to introduce students to programming and software development through the lens of exploring data. You can think of the Python programming language as your tool to solve data problems that are beyond the capability of a spreadsheet.Python is an easy to use and easy to learn programming language that is freely available on Macintosh, Windows, or Linux computers. So once you learn Python you can use it for the rest of your career without needing to purchase any software.This book uses the Python 3 language. The earlier Python 2 version of this book is titled "Python for Informatics: Exploring Information".There are free downloadable electronic copies of this book in various formats and supporting materials for the book at www.pythonlearn.com. The course materials are

available to you under a Creative Commons License so you can adapt them to teach your own Python course.

A Guided Tour Through the Wilds of Software Security "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.

A practical guide to ethical hacking and penetration testing using Python Apress

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

Mastering Machine Learning for Penetration Testing

Packt Publishing Ltd

CompTIA Security+ Study Guide (Exam SY0-601)

Python for Offensive

PenTest Packt Publishing Ltd
Learn how to apply modern AI to create powerful cybersecurity solutions for malware, pentesting, social engineering, data privacy, and intrusion detection Key Features Manage data of varying complexity to protect your system using the Python ecosystem Apply ML to pentesting, malware, data privacy, intrusion detection system(IDS) and social engineering Automate your daily workflow by addressing various security challenges using the recipes covered in the book Book Description Organizations today face a major threat in terms of cybersecurity, from malicious URLs to credential reuse, and having robust security systems can make all the difference. With this book, you'll learn how to use Python libraries such as TensorFlow and scikit-learn to implement the latest artificial intelligence (AI) techniques and handle challenges faced by cybersecurity researchers. You'll begin by exploring various machine learning (ML) techniques and tips for setting up a secure lab environment. Next, you'll implement key ML algorithms such as clustering, gradient boosting, random forest, and XGBoost. The book will guide you through constructing classifiers and features for malware, which you'll train and test on real samples. As you progress, you'll build self-learning, reliant systems to handle cybersecurity tasks such as identifying

malicious URLs, spam email detection, intrusion detection, network protection, and tracking user and process behavior. Later, you'll apply generative adversarial networks (GANs) and autoencoders to advanced security tasks. Finally, you'll delve into secure and private AI to protect the privacy rights of consumers using your ML models. By the end of this book, you'll have the skills you need to tackle real-world problems faced in the cybersecurity domain using a recipe-based approach. What you will learn Learn how to build malware classifiers to detect suspicious activities Apply ML to generate custom malware to pentest your security Use ML algorithms with complex datasets to implement cybersecurity concepts Create neural networks to identify fake videos and images Secure your organization from one of the most popular threats - insider threats Defend against zero-day threats by constructing an anomaly detection system Detect web vulnerabilities effectively by combining Metasploit and ML Understand how to train a model without exposing the training data Who this book is for This book is for cybersecurity professionals and security researchers who are looking to implement the latest machine learning techniques to boost computer security, and gain insights into securing an organization using red and blue team ML. This recipe-based book will also be useful for data scientists and machine

learning developers who want to experiment with smart techniques in the cybersecurity domain. Working knowledge of Python programming and familiarity with cybersecurity fundamentals will help you get the most out of this book.

Learn Ethical Hacking from Scratch "O'Reilly Media, Inc."

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

Python Programming for Hackers and Pentesters
World Scientific
If you are a security professional, pentester, or anyone interested in getting to grips with wireless penetration testing, this is the book for you. Some familiarity with Kali Linux and wireless concepts is beneficial.

Learning Python Web Penetration Testing IGI Global

Practical Machine Learning for Data Analysis Using Python is a problem solver's guide for creating real-world intelligent systems. It provides a comprehensive approach with concepts, practices, hands-on examples, and sample code. The book teaches readers the vital skills required to understand and solve different problems with machine learning. It teaches machine learning techniques necessary to become a successful practitioner, through the presentation of real-world case studies in Python machine learning ecosystems. The book also focuses on building a foundation of machine learning knowledge to solve different real-world case studies across various fields, including biomedical signal analysis, healthcare, security, economics, and finance. Moreover, it covers a wide range of machine learning models, including regression, classification, and forecasting. The goal of

the book is to help a broad range of readers, including IT professionals, analysts, developers, data scientists, engineers, and graduate students, to solve their own real-world problems. Offers a comprehensive overview of the application of machine learning tools in data analysis across a wide range of subject areas Teaches readers how to apply machine learning techniques to biomedical signals, financial data, and healthcare data Explores important classification and regression algorithms as well as other machine learning techniques Explains how to use Python to handle data extraction, manipulation, and exploration techniques, as well as how to visualize data spread across multiple dimensions and extract useful features

Analysis, Visualization and Dashboards No Starch Press

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

Gray Hat Python No Starch Press

Uncover hidden patterns of data and respond withcountermeasures Security professionals need all the tools at their disposal toincrease their visibility in order to prevent security breaches andattacks. This careful guide explores two of the most powerful data analysis and visualization. You'll soon understand how toharness and wield data, from collection and storage to managementand analysis as well as visualization and presentation. Using ahands-on approach with

real-world examples, this book shows you howto gather feedback, measure the effectiveness of your securitymethods, and make better decisions. Everything in this book will have practical application forinformation security professionals. Helps IT and security professionals understand and use data, sothey can thwart attacks and understand and visualizevulnerabilities in their networks Includes more than a dozen real-world examples and hands-onexercises that

demonstrate how to analyze security data andintelligence and translate that information into visualizationsthat make plain how to prevent attacks Covers topics such as how to acquire and prepare security data,use simple statistical methods to detect malware, predict roguebehavior, correlate security events, and more Written by a team of well-known experts in the field ofsecurity and data analysis Lock down your networks, prevent hacks, and thwart malware byimproving visibility into the environment, all through the power ofdata and Security Using Data Analysis, Visualization, andDashboards.

Beginning Ethical Hacking with Python CRC Press Learn the basics of ethical hacking and gain insights into the logic, algorithms, and syntax of Python. This book will set you up with a foundation that will help you understand the advanced concepts of hacking in the future. Learn Ethical Hacking with Python 3 touches the core issues of cyber security: in the modern world of interconnected computers and the Internet, security is increasingly becoming one of the most important features of programming. Ethical hacking is closely related to Python. For this reason this book is organized in three parts. The first part deals with the basics of ethical hacking; the second part deals with Python 3; and the third part deals with more advanced features of ethical hacking. What You Will Learn Discover the legal constraints of ethical hacking Work with

virtual machines and virtualization Develop skills in Python 3 See the importance of networking in ethical hacking Gain knowledge of the dark web, hidden Wikipedia, proxy chains, virtual private networks, MAC addresses, and more Who This Book Is For Beginners wanting to learn ethical hacking alongside a modular object oriented programming language. Kali Linux Wireless Penetration Testing: Beginner's Guide Python for CybersecurityUsing Python for Cyber Offense and Defense
Many countries around the world rely on the tourism industry to support their economies, making the safety and protection of travelers and workers in the industry of paramount importance. However, few police departments around the world have special divisions dedicated to the protection of tourism, tourists, and tourist centers. Tourism-Oriented Policing and Protective Services is a collection of innovative research on new methods and strategies for ensuring the security and safety of tourists, while also allowing law enforcement to take an active role in aiding the economic development of their city. While highlighting topics including visitor protection, cultural tourism, and security services, this book is ideally designed for government officials, policymakers, law enforcement, professionals within the tourism industry, academicians,

researchers, and students.

Learn Python 3 the Hard Way Pethuraja.S

Nowadays, configuring a network and automating security protocols are quite difficult to implement. However, using Python makes it easy to automate this whole process. This book explains the process of using Python for building networks, detecting network errors, and performing different security protocols using Python Scripting.

A Bug Hunter's Diary Packt Publishing Ltd

The second edition of this best-selling Python book (over 500,000 copies sold!) uses Python 3 to teach even the technically uninclined how to write programs that do in minutes what would take hours to do by hand. There is no prior programming experience required and the book is loved by liberal arts majors and geeks alike. If you've ever spent hours renaming files or updating hundreds of spreadsheet cells, you know how tedious tasks like these can be. But what if you could have your computer do them for you? In this fully revised second edition of the best-selling classic Automate the Boring Stuff with Python, you'll learn how to use Python to write programs that do in minutes what would take you hours to do by hand--no prior programming experience required. You'll learn the basics of Python and explore Python's rich library of modules for performing specific tasks, like scraping data off websites, reading PDF and

Word documents, and automating clicking and typing tasks. The second edition of this international fan favorite includes a brand-new chapter on input validation, as well as tutorials on automating Gmail and Google Sheets, plus tips on automatically updating CSV files. You'll learn how to create programs that effortlessly perform useful feats of automation to: • Search for text in a file or across multiple files • Create, update, move, and rename files and folders • Search the Web and download online content • Update and format data in Excel spreadsheets of any size • Split, merge, watermark, and encrypt PDFs • Send email responses and text notifications • Fill out online forms Step-by-step instructions walk you through each program, and updated practice projects at the end of each chapter challenge you to improve those programs and use your newfound skills to automate similar tasks. Don't spend your time doing work a well-trained monkey could do. Even if you've never written a line of code, you can make your computer do the grunt work. Learn how in Automate the Boring Stuff with Python, 2nd Edition.

Artificial Intelligence with Python Packt Publishing Ltd

Get a comprehensive, in-depth introduction to the core Python language with this hands-on book. Based on author Mark Lutz’s popular training course, this updated fifth edition will help you

quickly write efficient, high-quality code with Python. It's an ideal way to begin, whether you're new to programming or a professional developer versed in other languages. Complete with quizzes, exercises, and helpful illustrations, this easy-to-follow, self-paced tutorial gets you started with both Python 2.7 and 3.3— the latest releases in the 3.X and 2.X lines—plus all other releases in common use today. You'll also learn some advanced language features that recently have become more common in Python code. Explore Python's major built-in object types such as numbers, lists, and dictionaries Create and process objects with Python statements, and learn Python's general syntax model Use functions to avoid code redundancy and package code for reuse Organize statements, functions, and other tools into larger components with modules Dive into classes: Python's object-oriented programming tool for structuring code Write large programs with Python's exception-handling model and development tools Learn advanced Python tools, including decorators, descriptors, metaclasses, and Unicode processing

Tourism-Oriented Policing and Protective Services

John Wiley & Sons

Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make

hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: –Automate tedious reversing and security tasks –Design and program your own debugger –Learn how to fuzz Windows drivers and create powerful fuzzers from scratch –Have fun with code and library injection, soft and hard hooking techniques, and other software trickery –Sniff secure traffic out of an encrypted web browser session –Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you?

Fat, Boost Energy, And Balance Hormones By Dr. Mindy Pelz
• The Body Keeps The Score: Brain, Mind, And Body In The Healing Of Trauma
• The Housemaid's Secret: A Totally Gripping Psychological Thriller With A Shocking Twist
• Saved: A War Reporter's Mission To Make It Home By Benjamin Hall
• If Animals Kissed Good Night
• To Kill A Mockingbird
• The Five-star Weekend By Elin Hilderbrand
• It's Not Summer Without You By Jenny Han