Download Free Black Hat Python Python Programming For Hackers And Pentesters modernh.com

Black Hat Python, 2nd EditionPython CrashkursProgrammieren mit PHPGame HackingPraktische Einführung in Hardware HackingPHP & MySQL von Kopf bis FußGray Hat C#Mehr Hacking mit PythonGo – Das PraxisbuchFoundations of Information SecurityGray Hat PythonSerious CryptographyAttacking Network ProtocolsDesigning Secure SoftwareBlack Hat PythonDie Xbox hacken.Hacking mit PythonDie Kunst des EinbruchsMehr Hacking mit PythonMachine Learning KochbuchMehr Hacking mit PythonHackingBlack Hat GoHacken mit Python und Kali-LinuxBlack Hat Python for Pentesters and HackersDie Kunst des Human HackingHacken für DummiesBlack Hat PythonPython-GrundlagenDie Kunst der Anonymität im InternetPython kinderleicht!Black Hat PythonMicroservices mit GoDas Phantom im NetzPython HackingWindows 10 kompakt für DummiesWLAN HackingInformatik für KinderThink Like a Programmer - Deutsche AusgabeViolent Python

Black Hat Python, 2nd Edition

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 this second edition of the bestselling Black Hat Python, you'll explore the darker side of Python's capabilities: everything from writing network sniffers, stealing email credentials, and bruteforcing directories to crafting mutation fuzzers, investigating virtual machines, and creating stealthy trojans. All of the code in this edition has been updated to Python 3.x. You'll also find new coverage of bit shifting, code hygiene, and offensive forensics with the Volatility Framework as well as expanded explanations of the Python libraries ctypes, struct, lxml, and BeautifulSoup, and offensive hacking strategies like splitting bytes, leveraging computer vision libraries, and scraping websites. You'll even learn how to: • Create a trojan command-and-control server using GitHub • Detect sandboxing and automate common malware tasks like keylogging and screenshotting • Extend the Burp Suite web-hacking tool • Escalate Windows privileges with creative process control • Use offensive memory forensics tricks to retrieve password hashes and find vulnerabilities on a virtual machine • Abuse Windows COM automation • Exfiltrate data from a network undetected When it comes to offensive security, you need to be able to create powerful tools on the fly. Learn how with Black Hat Python.

Python Crashkurs

Programmieren mit PHP

Python-Programmierer finden in diesem Kochbuch nahezu 200 wertvolle und jeweils in sich abgeschlossene Anleitungen zu Aufgabenstellungen aus dem Bereich des Machine Learning, wie sie für die tägliche Arbeit typisch sind – von der Vorverarbeitung der Daten bis zum Deep Learning. Entwickler, die mit Python und seinen Bibliotheken einschließlich Pandas und Scikit-Learn vertraut sind, werden spezifische Probleme erfolgreich bewältigen – wie etwa Daten laden, Text und numerische Daten behandeln, Modelle auswählen, Dimensionalität reduzieren und vieles mehr. Jedes Rezept enthält Code, den Sie kopieren, zum Testen in eine kleine Beispieldatenmenge einfügen und dann anpassen können, um Ihre eigenen Anwendungen zu konstruieren. Darüber hinaus werden alle Lösungen diskutiert und wichtige Zusammenhänge hergestellt. Dieses Kochbuch unterstützt Sie dabei, den Schritt von der Theorie und den Konzepten hinein in die Praxis zu machen. Es liefert das praktische Rüstzeug, das Sie benötigen, um funktionierende Machine-Learning-Anwendungen zu entwickeln. In diesem Kochbuch finden Sie Rezepte für: Vektoren, Matrizen und Arrays den Umgang mit numerischen und kategorischen Daten, Texten, Bildern sowie Datum und Uhrzeit das Reduzieren der Dimensionalität durch Merkmalsextraktion oder

Merkmalsauswahl Modellbewertung und -auswahl lineare und logistische Regression, Bäume und Wälder und k-nächste Nachbarn Support Vector Machine (SVM), naive Bayes, Clustering und neuronale Netze das Speichern und Laden von trainierten Modellen

Game Hacking

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

Praktische Einführung in Hardware Hacking

This practical guide to modern encryption breaks down the fundamental mathematical concepts at the heart of cryptography without shying away from meaty discussions of how they work. You'll learn about authenticated encryption, secure randomness, hash functions, block ciphers, and public-key techniques such as RSA and elliptic curve cryptography. You'll also learn: - Key concepts in cryptography, such as computational security, attacker models, and forward secrecy - The strengths and limitations of the TLS protocol behind HTTPS secure websites - Quantum computation and post-quantum cryptography - About various vulnerabilities by examining numerous code examples and use cases - How to choose the best algorithm or protocol and ask vendors the right questions Each chapter includes a discussion of common implementation mistakes using real-world examples and details what could go wrong and how to avoid these pitfalls. Whether you're a seasoned practitioner or a beginner looking to dive into the field, Serious Cryptography will provide a complete survey of modern encryption and its applications.

PHP & MySQL von Kopf bis Fuß

Gray Hat C#

Python ist eine leicht zu erlernende und dennoch eine sehr vielfältige und mächtige Programmiersprache. Lernen Sie mit der bevorzugten Sprache vieler Hacker, Ihre eigenen Tools zu schreiben und diese unter Kali-Linux einzusetzen, um zu sehen, wie Hacker Systeme angreifen und Schwachstellen ausnutzen. Durch das entwickeln Ihrer eigenen Tools erhalten Sie ein deutlich tiefgreifenderes Verständnis wie und warum Angriffe funktionieren. Nach einer kurzen Einführung in die Programmierung mit Python lernen Sie anhand vieler praktischer Beispiele die unterschiedlichsten Hacking-Tools zu schreiben. Sie werden selbst schnell feststellen, wie erschreckend einfach das ist. Durch Einbindung vorhandener Werkzeuge wie Metasploit und Nmap werden Skripte nochmals effizienter und kürzer. Nutzen Sie das hier erlangte Wissen, um Ihre Systeme auf Lücken zu testen und diese zu schließen bevor andere diese ausnützen können!

Mehr Hacking mit Python

Drahtlose Netzwerke sind heute allgegenwärtig und werden im Zuge von Entwicklungen wie dem "Smart Home" und dem "Internet of Things" in Zukunft eine noch wichtigere Schlüsselrolle bei der Informationsvermittlung spielen. Folglich steht und fällt die Zuverlässigkeit unserer Infrastruktur nicht zuletzt mit der Sicherheit von WLAN-Technologien. Das Buch vermittelt seinen Leserinnen und Lesern das nötige Wissen, um WLAN-Umgebungen wirksam gegen Angriffe abzusichern.

Zahlreiche praxisnahe Beispiele helfen sowohl Anfängern als auch Fortgeschrittenen dabei, verschiedene Angriffsszenarien nachzuvollziehen, um sich effektiv vor Hackern schützen zu können. Vom Auskundschaften einer WLAN-Umgebung bis zur Umgehung von Authentifizierungsverfahren geben die Autoren einen umfassenden Einblick in alle gängigen Angriffswege auf drahtlose Datenübertragungstechnologien. Rechtliche und gesellschaftliche Aspekte wie Störerhaftung und Freifunk runden das Buch ab und machen es zu einem unverzichtbaren Lern- und Nachschlagewerk für alle, denen die Sicherheit ihrer Funknetze am Herzen liegt.

Go – Das Praxisbuch

Schwachstellen von IoT- und Smart-Home-Geräten aufdecken Hardware, Firmware und Apps analysieren und praktische Tests durchführen Zahlreiche Praxisbeispiele wie Analyse und Hacking elektronischer Türschlösser, smarter LED-Lampen u.v.m. Smarte Geräte sind allgegenwärtig und sie sind leicht zu hacken – umso mehr sind Reverse Engineers und Penetration Tester gefragt, um Schwachstellen aufzudecken und so Hacking-Angriffen und Manipulation vorzubeugen. In diesem Buch lernen Sie alle Grundlagen des Penetration Testings für IoT-Geräte. Die Autoren zeigen Schritt für Schritt, wie ein Penetrationstest durchgeführt wird: von der Einrichtung des Testlabors über die OSINT-Analyse eines Produkts bis hin zum Prüfen von Hard- und Software auf Sicherheitslücken – u.a. anhand des OWASP-Standards. Sie erfahren darüber hinaus, wie Sie die Firmware eines IoT-Geräts extrahieren, entpacken und dynamisch oder statisch analysieren. Auch die Analyse von Apps, Webapplikationen und Cloudfunktionen wird behandelt. Außerdem finden Sie eine Übersicht der wichtigsten IoT-Protokolle und ihrer Schwachstellen. Es werden nur grundlegende IT-Security-Kenntnisse (insbesondere in den Bereichen Netzwerk- und Applikationssicherheit) und ein sicherer Umgang mit Linux vorausgesetzt. Die notwendigen Elektronik- und Hardwaredesign-Grundlagen geben Ihnen die Autoren mit an die Hand. Aus dem Inhalt: Testumgebung einrichten Vorbereitende OSINT-Analyse Elektronik-Grundlagen Einführung in das Hardware-Design von IoT-Geräten: 8-/32-Bit-Controller Android Embedded Devices All-in-One SoC Hardware-Analyse und Extraktion von Firmware Dateisysteme von IoT-Geräten Statische und dynamische Firmware-Analyse IoT-Protokolle und ihre Schwachstellen: Bluetooth LE ZigBee MQTT App-Analyse anhand des OWASP-Standards Testen von Backend-Systemen, Webapplikationen und Cloud-Umgebungen

Foundations of Information Security

High-level overview of the information security field. Covers key concepts like confidentiality, integrity, and availability, then dives into practical applications of these ideas in the areas of operational, physical, network, application, and operating system security. In this high-level survey of the information security field, best-selling author Jason Andress covers the basics of a wide variety of topics, from authentication and authorization to maintaining confidentiality and performing penetration testing. Using real-world security breaches as examples, Foundations of Information Security explores common applications of these concepts, such as operations security, network design, hardening and patching operating systems, securing mobile devices, as well as tools for assessing the security of hosts and applications. You'll also learn the basics of topics like: • Multifactor authentication and how biometrics and hardware tokens can be used to harden the authentication process • The principles behind modern cryptography, including symmetric and asymmetric algorithms, hashes, and certificates • The laws and regulations that protect systems and data • Anti-malware tools, firewalls, and intrusion detection systems • Vulnerabilities such as buffer overflows and race conditions A valuable resource for beginning security professionals, network systems administrators, or anyone new to the field, Foundations of Information Security is a great place to start your journey into the dynamic and rewarding field of information security.

Gray Hat Python

Ihr Einstieg in Go Sie haben schon Erfahrung mit objektorientierten Programmiersprachen und wollen sich jetzt Googles Programmiersprache Go genauer ansehen? Dann ist dieses Buch genau das Richtige für Sie! Denn Sie steigen direkt in die Besonderheiten von Go ein und lernen das

Ökosystem rund um Tools und Testing kennen. Dabei liegt stets ein Fokus auf der Codequalität, damit Ihr Code von Anfang an den gängigen Code-Konventionen der Go-Community entspricht. Das alles lernen sie nicht nur mit grauer Theorie, sondern direkt an der Tatstatur mit Übungsaufgaben und Beispielprojekten.

Serious Cryptography

Attacking Network Protocols

Designing Secure Software

Black Hat Python

Python wird mehr und mehr zur bevorzugten Programmiersprache von Hackern, Reverse Engineers und Softwaretestern, weil sie es einfach macht, schnell zu entwickeln. Gleichzeitig bietet Python die Low-Level-Unterstützung und die Bibliotheken, die Hacker glücklich machen. Hacking mit Python bietet eine umfassende Anleitung, wie man diese Sprache für eine Vielzahl von Hacking-Aufgaben nutzen kann. Das Buch erläutert die Konzepte hinter Hacking-Tools und -Techniken wie Debugger, Trojaner, Fuzzer und Emulatoren. Doch der Autor Justin Seitz geht über die Theorie hinaus und zeigt, wie man existierende Python-basierte Sicherheits-Tools nutzt - und wie man eigene entwickelt, wenn die vorhandenen nicht ausreichen. Sie lernen, wie man: - lästige Reverse Engineering- und Sicherheits-Aufgaben automatisiert - einen eigenen Debugger entwirft und programmiert - Windows-Treiber "fuzzed" und mächtige Fuzzer von Grund auf entwickelt - Code- und Library-Injection, Soft- und Hard-Hooks und andere Software-Tricks vornimmt - gesicherten Traffic aus einer verschlüsselten Webbrowser-Session erschnüffelt - PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU und andere Software nutzt Die weltbesten Hacker nutzen Python für ihre Arbeit. Warum nicht auch Sie?

Die Xbox hacken.

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

Hacking mit Python

Eine Warnung vorab: Dieses Buch ist nichts für schwache Nerven. Es bringt Sie in jene dunklen Ecken der Gesellschaft, wo die Black Hats (bösartige Hacker) das Sagen haben. Hier werden die Techniken des Social Engineerings, die Spione und Trickbetrüger einsetzen, aufgedeckt und eingehend erforscht. Außerdem wird anhand ganz normaler Alltagssituationen gezeigt, inwiefern es sich auch dabei oft um komplexe Szenarien des Social Engineerings handelt. Am Ende deckt das Buch die Tipps und Tricks der Insider, der professionellen Social Engineers und auch der kriminellen Profis auf. Dieses Buch ist mehr als eine Sammlung cooler Storys, toller Hacks oder abgefahrener Ideen. Wissenschaftlich fundiert (dabei höchst unterhaltsam), stellt es das

weltweit erste Framework für Social Engineering vor, auf dessen Grundlage der Autor genau analysiert, geradezu seziert, was einen guten Social Engineer ausmacht. Mit praktischen Ratschlägen wird der Leser befähigt, Skills zu entwickeln, die es ihm ermöglichen, die nachweislich größte Schwachstelle in IT-Sicherheitssystemen auf die Probe zu stellen: den Menschen.

Die Kunst des Einbruchs

Black Hat Python explores the darker side of Python's capabilities, helping you test your systems and improve your security posture.

Mehr Hacking mit Python

Attacking Network Protocols is a deep dive into network protocol security from James Forshaw, one of the world’s leading bug hunters. This comprehensive guide looks at networking from an attacker’s perspective to help you discover, exploit, and ultimately protect vulnerabilities. You’ll start with a rundown of networking basics and protocol traffic capture before moving on to static and dynamic protocol analysis, common protocol structures, cryptography, and protocol security. Then you’ll turn your focus to finding and exploiting vulnerabilities, with an overview of common bug classes, fuzzing, debugging, and exhaustion attacks. Learn how to: - Capture, manipulate, and replay packets - Develop tools to dissect traffic and reverse engineer code to understand the inner workings of a network protocol - Discover and exploit vulnerabilities such as memory corruptions, authentication bypasses, and denials of service - Use capture and analysis tools like Wireshark and develop your own custom network proxies to manipulate network traffic Attacking Network Protocols is a must-have for any penetration tester, bug hunter, or developer looking to understand and discover network vulnerabilities.

Machine Learning Kochbuch

Learn to use C#'s powerful set of core libraries to automate tedious yet important tasks like performing vulnerability scans, malware analysis, and incident response. With some help from Mono, you can write your own practical security tools that will run on Mac, Linux, and even mobile devices. Following a crash course in C# and some of its advanced features, you’ll learn how to: –Write fuzzers that use the HTTP and XML libraries to scan for SQL and XSS injection –Generate shellcode in Metasploit to create cross-platform and cross-architecture payloads –Automate Nessus, OpenVAS, and sqlmap to scan for vulnerabilities and exploit SQL injections –Write a .NET decompiler for Mac and Linux –Parse and read offline registry hives to dump system information –Automate the security tools Arachni and Metasploit using their MSGPACK RPCs Streamline and simplify your work day with Gray Hat C# and C#’s extensive repertoire of powerful tools and libraries.

Mehr Hacking mit Python

Python ist eine weltweit akzeptierte, gut interpretierte und hochrangige Allzweck-Programmiersprache, die 1991 von Guido van Rossum entworfen und erstellt wurde. Das objektorientierte Ziel der Sprache und ihrer Sprachkonstrukte hilft den Programmierern zusammen einen logischen und klaren Code für große und kleine Projekte zu generieren. Die Verwendung der Programmiersprache Python wurde sowohl in kleinen Branchen wie der Entwicklung mobiler Apps, der Entwicklung von Websites, zur Durchführung mathematischer Berechnungen usw. als auch in großen Branchen wie maschinellem Lernen und künstlicher Intelligenz gefunden. Die Verwendung von Python-Programmiersprachen wird aus verschiedenen Gründen gegenüber anderen Programmiersprachen wie C und C ++ bevorzugt, beispielsweise aufgrund der in der Python-Programmiersprache verwendeten Syntax, die der englischen Sprache am ähnlichsten ist. Es kann auf einer Vielzahl verschiedener Plattformen wie Linux, Mac, Pi, Windows, Raspberry usw. verwendet werden. Die Funktionsweise der Programmiersprache Python basiert auf dem Interpretersystem und schließlich, weil es auf funktionale Weise verwendet werden kann oder objektorientiert. Der Datentyp ist die

kategorisierte und klassifizierte Information, die der Variablen zugewiesen wird. Es gibt zwei Arten von Datentypen in den Python-Mutable-Datentypen und den unveränderlichen Datentypen. Anzahl, Zeichenfolgen und Tupel sind unveränderliche Datentypen. Listen, Wörterbuch und Sätze sind veränderbare Datentypen. Die Operatoren in dieser Sprache sind als Symbole definiert, die eine wichtige Rolle bei der Ausführung einer bestimmten Operation zwischen zwei Operanden spielen. Diese werden als Säulen der Python-Programmiersprache angesehen, auf der die Logik des gesamten Programms basiert.

Hacking

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

Black Hat Go

Hacken mit Python und Kali-Linux

Typische Programmieraufgaben kreativ lösen am Beispiel von C++ Von der Aufgabe zur Lösung – so gehen Sie vor Probleme analysieren und schrittweise bearbeiten Systematisches Vorgehen lernen und anwenden Aus dem Inhalt: Strategien zur Problemlösung Eingabeverarbeitung Statusverfolgung Arrays Zeiger und dynamische Speicherverwaltung Klassen Rekursion Wiederverwendung von Code Rekursive und iterative Programmierung Denken wie ein Programmierer Die Herausforderung beim Programmieren besteht nicht im Erlernen der Syntax einer bestimmten Sprache, sondern in der Fähigkeit, auf kreative Art Probleme zu lösen. In diesem einzigartigen Buch widmet sich der Autor V. Anton Spraul genau jenen Fähigkeiten, die in normalen Lehrbüchern eher nicht behandelt werden: die Fähigkeit, wie ein Programmierer zu denken und Aufgaben zu lösen. In den einzelnen Kapiteln behandelt er jeweils verschiedene Programmierkonzepte wie beispielsweise Klassen, Zeiger und Rekursion, und fordert den Leser mit erweiterbaren Übungen zur praktischen Anwendung des Gelernten auf. Sie lernen unter anderem: Probleme in diskrete Einzelteile zerlegen, die sich leichter lösen lassen Funktionen, Klassen und Bibliotheken möglichst effizient nutzen und wiederholt verwenden die perfekte Datenstruktur für eine Aufgabenstellung auswählen anspruchsvollere Programmiertechniken wie Rekursion und dynamischen Speicher einsetzen Ihre Gendanken ordnen und Strategien entwickeln, um bestimmte Problemkategorien in Angriff zu nehmen Die Beispiele im Buch werden mit C++ gelöst, die dargestellten kreativen Problemlösungskonzepte gehen aber weit über die einzelnen Programmiersprachen und oft sogar über den Bereich der Informatik hinaus. Denn wie die fähigsten Programmierer wissen, handelt es sich beim Schreiben herausragender Quelltexte um kreative Kunst und der erste Schritt auf dem Weg zum eigenen Meisterwerk besteht darin, wie ein Programmierer zu denken. Über den Autor: V. Anton Spraul hat über 15 Jahre lang Vorlesungen über die Grundlagen der Programmierung und Informatik gehalten. In diesem Buch fasst er die von ihm dabei perfektionierten Verfahren zusammen. Er ist auch Autor von »Computer Science Made Simple«.

Black Hat Python for Pentesters and Hackers

Die Kunst des Human Hacking

Hacken für Dummies

"Python Crashkurs" ist eine kompakte und gründliche Einführung, die es Ihnen nach kurzer Zeit ermöglicht, Python-Programme zu schreiben, die für Sie Probleme lösen oder Ihnen erlauben, Aufgaben mit dem Computer zu erledigen. In der ersten Hälfte des Buches werden Sie mit grundlegenden Programmierkonzepten wie Listen, Wörterbücher, Klassen und Schleifen vertraut gemacht. Sie erlernen das Schreiben von sauberem und lesbarem Code mit Übungen zu jedem Thema. Sie erfahren auch, wie Sie Ihre Programme interaktiv machen und Ihren Code testen, bevor Sie ihn einem Projekt hinzufügen. Danach werden Sie Ihr neues Wissen in drei komplexen Projekten in die Praxis umsetzen: ein durch "Space Invaders" inspiriertes Arcade-Spiel, eine Datenvisualisierung mit Pythons superpraktischen Bibliotheken und eine einfache Web-App, die Sie online bereitstellen können. Während der Arbeit mit dem "Python Crashkurs" lernen Sie, wie Sie: - leistungsstarke Python-Bibliotheken und Tools richtig einsetzen – einschließlich matplotlib, NumPy und Pygal - 2D-Spiele programmieren, die auf Tastendrücke und Mausklicks reagieren, und die schwieriger werden, je weiter das Spiel fortschreitet - mit Daten arbeiten, um interaktive Visualisierungen zu generieren - Web-Apps erstellen und anpassen können, um diese sicher online zu deployen - mit Fehlern umgehen, die häufig beim Programmieren auftreten Dieses Buch wird Ihnen effektiv helfen, Python zu erlernen und eigene Programme damit zu entwickeln. Warum länger warten? Fangen Sie an!

Black Hat Python

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-Grundlagen

"When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. 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. In this course, you'll explore the darker side of Python's capabilities--writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy trojans, and more. This course starts from scratch and provides the latest tools and techniques available for Pentesting using Python scripts. We'll show you the concepts and how to implement hacking tools and techniques such as debuggers, fuzzers, and emulators. You'll detect sandboxing and automate com-mon malware tasks, such as keylogging and screenshotting. You'll be able to escalate Windows privileges with creative process control, use offensive memory forensics tricks to retrieve password hashes, and inject shellcode into a virtual machine. Later, you'll learn to extend the popular Burp Suite web-hacking tool, abuse Windows COM automation to perform a man-in-the browser attack, and exfiltrate data from a network most sneakily."--Resource description page.

Die Kunst der Anonymität im Internet

Ob Sie wollen oder nicht – jede Ihrer Online-Aktivitäten wird beobachtet und analysiert Sie haben keine Privatsphäre. Im Internet ist jeder Ihrer Klicks für Unternehmen, Regierungen und kriminelle Hacker uneingeschränkt sichtbar. Ihr Computer, Ihr Smartphone, Ihr Auto, Ihre Alarmanlage, ja sogar Ihr Kühlschrank bieten potenzielle Angriffspunkte für den Zugriff auf Ihre Daten. Niemand kennt sich besser aus mit dem Missbrauch persönlicher Daten als Kevin Mitnick. Als von der US-Regierung ehemals meistgesuchter Computer-Hacker kennt er alle Schwachstellen und Sicherheitslücken des digitalen Zeitalters. Seine Fallbeispiele sind spannend und erschreckend: Sie werden Ihre Aktivitäten im Internet neu überdenken. Mitnick weiß aber auch, wie Sie Ihre Daten bestmöglich schützen. Er zeigt Ihnen anhand zahlreicher praktischer Tipps und Schritt-für-Schritt-Anleitungen, was Sie tun können, um online und offline anonym zu sein. Bestimmen Sie selbst über Ihre Daten. Lernen Sie, Ihre Privatsphäre im Internet zu schützen. Kevin Mitnick zeigt Ihnen, wie es geht. Hinterlassen Sie keine Spuren ? Sichere Passwörter festlegen und verwalten ? Mit dem Tor-Browser im Internet surfen, ohne Spuren zu hinterlassen ? E-Mails und Dateien verschlüsseln und vor fremden Zugriffen schützen ? Öffentliches WLAN, WhatsApp, Facebook & Co. sicher nutzen ? Sicherheitsrisiken vermeiden bei GPS, Smart-TV, Internet of Things und Heimautomation ? Eine zweite Identität anlegen und unsichtbar werden

Python kinderleicht!

Python ist eine leistungsfähige, moderne Programmiersprache. Sie ist einfach zu erlernen und macht Spaß in der Anwendung – mit diesem Buch umso mehr! "Python kinderleicht" macht die Sprache lebendig und zeigt Dir (und Deinen Eltern) die Welt der Programmierung. Jason R. Briggs führt Dich Schritt für Schritt durch die Grundlagen von Python. Du experimentierst mit einzigartigen (und oft urkomischen) Beispielprogrammen, bei denen es um gefräßige Monster, Geheimagenten oder diebische Raben geht. Neue Begriffe werden erklärt, der Programmcode ist farbig dargestellt, strukturiert und mit Erklärungen versehen. Witzige Abbildungen erhöhen den Lernspaß. Jedes Kapitel endet mit Programmier-Rätseln, an denen Du das Gelernte üben und Dein Verständnis vertiefen kannst. Am Ende des Buches wirst Du zwei komplette Spiele programmiert haben: einen Klon des berühmten "Pong" und "Herr Strichmann rennt zum Ausgang" – ein Plattformspiel mit Sprüngen, Animation und vielem mehr. Indem Du Seite für Seite neue Programmierabenteuer bestehst, wirst Du immer mehr zum erfahrenen Python-Programmierer. - Du lernst grundlegende Datenstrukturen wie Listen, Tupel und Maps kennen. - Du erfährst, wie man mit Funktionen und Modulen den Programmcode organisieren und wiederverwenden kann. - Du wirst mit Kontrollstrukturen wie Schleifen und bedingten Anweisungen vertraut und lernst, mit Objekten und Methoden umzugehen. - Du zeichnest Formen mit dem Python-Modul Turtle und erstellst Spiele, Animationen und andere grafische Wunder mit tkinter. Und: "Python kinderleicht" macht auch für Erwachsene das Programmierenlernen zum Kinderspiel! Alle Programme findest Du auch zum Herunterladen auf der Website!

Black Hat Python

What every software professional should know about security. Designing Secure Software consolidates Loren Kohnfelder’s more than twenty years of experience into a concise, elegant guide to improving the security of technology products. Written for a wide range of software professionals, it emphasizes building security into software design early and involving the entire team in the process. The book begins with a discussion of core concepts like trust, threats, mitigation, secure design patterns, and cryptography. The second part, perhaps this book’s most unique and important contribution to the field, covers the process of designing and reviewing a software design with security considerations in mind. The final section details the most common coding flaws that create vulnerabilities, making copious use of code snippets written in C and Python to illustrate implementation vulnerabilities. You’ll learn how to: • Identify important assets, the attack surface, and the trust boundaries in a system • Evaluate the effectiveness of various threat mitigation candidates • Work with well-known secure coding patterns and libraries • Understand and prevent vulnerabilities like XSS and CSRF, memory flaws,

and more • Use security testing to proactively identify vulnerabilities introduced into code • Review a software design for security flaws effectively and without judgment Kohnfelder's career, spanning decades at Microsoft and Google, introduced numerous software security initiatives, including the co-creation of the STRIDE threat modeling framework used widely today. This book is a modern, pragmatic consolidation of his best practices, insights, and ideas about the future of software.

Microservices mit Go

Andy Rathbone zeigt Ihnen schnell und dennoch verständlich alles Wichtige, was Sie über Windows 10 und dessen Updates wissen müssen: Erfahren Sie, was neu ist, wie Sie die neuen Funktionen nutzen und wie Sie altbekannte wiederfinden. Der Autor unterstützt Sie dabei, Ihre Daten von einem alten Computer auf einen neuen Windows-10-PC zu übertragen und Windows 10 an Ihre Bedürfnisse anzupassen. So kommen Sie mit Ihrem neuen Betriebssystem im Handumdrehen zurecht und fühlen sich schnell wieder zuhause.

Das Phantom im Netz

Like the best-selling Black Hat Python, Black Hat Go explores the darker side of the popular Go programming language. This collection of short scripts will help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset. Black Hat Go explores the darker side of Go, the popular programming language revered by hackers for its simplicity, efficiency, and reliability. It provides an arsenal of practical tactics from the perspective of security practitioners and hackers to help you test your systems, build and automate tools to fit your needs, and improve your offensive security skillset, all using the power of Go. You'll begin your journey with a basic overview of Go's syntax and philosophy and then start to explore examples that you can leverage for tool development, including common network protocols like HTTP, DNS, and SMB. You'll then dig into various tactics and problems that penetration testers encounter, addressing things like data pilfering, packet sniffing, and exploit development. You'll create dynamic, pluggable tools before diving into cryptography, attacking Microsoft Windows, and implementing steganography. You'll learn how to: • Make performant tools that can be used for your own security projects • Create usable tools that interact with remote APIs • Scrape arbitrary HTML data • Use Go's standard package, net/http, for building HTTP servers • Write your own DNS server and proxy • Use DNS tunneling to establish a C2 channel out of a restrictive network • Create a vulnerability fuzzer to discover an application's security weaknesses • Use plug-ins and extensions to future-proof productsBuild an RC2 symmetric-key brute-forcer • Implant data within a Portable Network Graphics (PNG) image. Are you ready to add to your arsenal of security tools? Then let's Go!

Python Hacking

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.

Windows 10 kompakt für Dummies

Um einen Hacker zu überlisten, müssen Sie sich in die Denkweise des Hackers hineinversetzen. Deshalb lernen Sie mit diesem Buch, wie ein Bösewicht zu denken. Der Fachmann für IT-Sicherheit Kevin Beaver teilt mit Ihnen sein Wissen über Penetrationstests und typische Schwachstellen in IT-Systemen. Er zeigt Ihnen, wo Ihre Systeme verwundbar sein könnten, sodass Sie im Rennen um die IT-Sicherheit die Nase vorn behalten. Denn wenn Sie die Schwachstellen in Ihren Systemen kennen, können Sie sie besser schützen und die Hacker kommen bei Ihnen nicht zum Zug!

WLAN Hacking

You don’t need to be a wizard to transform a game you like into a game you love. Imagine if you could give your favorite PC game a more informative heads-up display or instantly collect all that loot from your latest epic battle. Bring your knowledge of Windows-based development and memory management, and Game Hacking will teach you what you need to become a true game hacker. Learn the basics, like reverse engineering, assembly code analysis, programmatic memory manipulation, and code injection, and hone your new skills with hands-on example code and practice binaries. Level up as you learn how to: –Scan and modify memory with Cheat Engine –Explore program structure and execution flow with OllyDbg –Log processes and pinpoint useful data files with Process Monitor –Manipulate control flow through NOPing, hooking, and more –Locate and dissect common game memory structures You’ll even discover the secrets behind common game bots, including: –Extrasensory perception hacks, such as wallhacks and heads-up displays –Responsive hacks, such as autohealers and combo bots –Bots with artificial intelligence, such as cave walkers and automatic looters Game hacking might seem like black magic, but it doesn’t have to be. Once you understand how bots are made, you’ll be better positioned to defend against them in your own games. Journey through the inner workings of PC games with Game Hacking, and leave with a deeper understanding of both game design and computer security.

Informatik für Kinder

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.

Think Like a Programmer - Deutsche Ausgabe

Unser Alltag wird in rasantem Tempo von Informationstechnik durchdrungen und es ist höchste Zeit, auch den jungen Mitgliedern unserer Gesellschaft Informatikbildung anzubieten. Während in osteuropäischen Ländern und England in frühen Schuljahren eine Informatische Bildung integriert wurde, beschränken sich deutsche Schulen eher auf eine Medienbildung. Konzepte aus der Informatik werden zwar schon länger diskutiert, aber erst in letzter Zeit haben bildungspolitische Entscheidungen die hiesigen Aktivitäten für die Klassen 1 bis 7 intensiviert. Seit 2006 werden auf dem Münsteraner Workshop Beiträge zu unterschiedlichen Themen aus dem Gebiet der Schulinformatik diskutiert. Ziel der Veranstaltung ist insbesondere die Förderung des Austauschs zwischen den Schulen und der Hochschule. Der Workshop richtet sich an Informatiklehrerinnen und -lehrer, an Referendarinnen und Referendare, an Fachdidaktiker(innen) und an alle, die sich zur Informatik in der Schule engagieren.

Violent Python

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?