

Hacken Lernen Buch

Yeah, reviewing a books **Hacken Lernen Buch** could accumulate your near contacts listings. This is just one of the solutions for you to be successful. As understood, exploit does not suggest that you have fantastic points.

Comprehending as with ease as promise even more than supplementary will come up with the money for each success. next-door to, the message as without difficulty as perception of this Hacken Lernen Buch can be taken as well as picked to act.

Buch der Muetter oder Anleitung fuer Muetter, ihre Kinder bemerken und reden zu lehren - Pestalozzi 1803

Les bases du hacking - Patrick Engebretson 2013-08-23
Créez votre propre laboratoire de hacking ! Vous souhaitez, comme les hackers, apprendre à pénétrer les réseaux et les systèmes informatiques ? Les bases du hacking est une introduction aux techniques de hacking et aux tests d'intrusion. Grâce à des explications claires et à une approche originale, apprenez à utiliser tous les outils des professionnels de la sécurité et des hackers éthiques. Maîtrisez les quatre phases du test d'intrusion et du hacking : reconnaissance, scan, exploitation, post-exploitation. Informez-vous sur votre cible, trouvez ses vulnérabilités, exploitez-les pour attaquer, puis maintenez les accès ! Vous n'aurez besoin d'aucune expérience préalable pour comprendre et suivre les différentes étapes présentées dans cet ouvrage. En menant de véritables attaques et tests d'intrusion contre des machines virtuelles, vous saurez repérer les faiblesses des systèmes, et apprendrez toutes les techniques de la sécurité offensive. Pas-à-pas, grâce des exercices pratiques et simples, l'auteur vous enseignera les principes et les techniques de hacking, depuis l'ingénierie sociale jusqu'aux rootkits, en passant par l'utilisation de tous les outils modernes (Kali, BackTrack Linux, MetaGooFil, Nmap, Nessus, Metasploit, w3af, Netcat et bien d'autres !).
The Web Application Hacker's Handbook: Finding And Exploiting Security Flaws, 2nd Ed - Dafydd Stuttard

Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition - Daniel Regalado 2018-04-05
Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 13 new chapters, Gray Hat Hacking, The Ethical Hacker's Handbook, Fifth Edition explains the enemy's current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-try testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. And the new topic of exploiting the Internet of things is introduced in this edition. •Build and launch spoofing exploits with Ettercap •Induce error conditions and crash software using fuzzers •Use advanced reverse engineering to exploit Windows and Linux software •Bypass Windows Access Control and memory protection schemes •Exploit web applications with Padding Oracle Attacks •Learn the use-after-free technique used in recent zero days •Hijack web browsers with advanced XSS attacks •Understand ransomware and how it takes control of your desktop •Dissect Android malware with JEB and DAD decompilers •Find one-day vulnerabilities with binary diffing •Exploit wireless systems with Software Defined Radios (SDR) •Exploit Internet of things devices •Dissect and exploit embedded devices •Understand bug bounty programs •Deploy next-generation honeypots •Dissect ATM malware and analyze common ATM attacks •Learn the business side of ethical hacking
Raspberry Pi - dein Einstieg - Matt Richardson 2022-12-20

Ihre Lösung für Office - Multimedia - Entertainment - Smarthome Eine Einführung für vielfältige Anwendungsmöglichkeiten Programmierung mit Python Einsatz mit Linux und anderen Betriebssystemen Der Raspberry Pi ist ein kreditkartengroßer, kostengünstiger Computer, der an Ihren Fernseher und eine Tastatur angeschlossen wird. Er ist ein leistungsfähiger kleiner Computer, der für Elektronikprojekte und für viele Dinge verwendet werden kann, die auch Ihr Desktop-PC erledigt,

wie Tabellenkalkulationen, Textverarbeitung, Surfen im Internet und Spiele. Nutzen Sie Ihren Raspi als auf ihre Bedürfnisse abgestimmte Smarthome-Zentrale oder als Mediaplayer - der Computer spielt auch hochauflösende Videos ab. Das Autorenteam stellt die verschiedenen Modelle des Raspberry Pi vor und erläutert ihre jeweiligen Einsatzgebiete. Es geht auf den Betrieb mit Linux und anderen Betriebssystemen ein und begleitet Sie bei den ersten Schritten in der Programmiersprache Python.

Hacking & Security - Michael Kofler 2022-11-10

Gray Hat Hacking: The Ethical Hacker's Handbook, Sixth Edition - Allen Harper 2022-03-11

Up-to-date strategies for thwarting the latest, most insidious network attacks This fully updated, industry-standard security resource shows, step by step, how to fortify computer networks by learning and applying effective ethical hacking techniques. Based on curricula developed by the authors at major security conferences and colleges, the book features actionable planning and analysis methods as well as practical steps for identifying and combating both targeted and opportunistic attacks. Gray Hat Hacking: The Ethical Hacker's Handbook, Sixth Edition clearly explains the enemy's devious weapons, skills, and tactics and offers field-tested remedies, case studies, and testing labs. You will get complete coverage of Internet of Things, mobile, and Cloud security along with penetration testing, malware analysis, and reverse engineering techniques. State-of-the-art malware, ransomware, and system exploits are thoroughly explained. Fully revised content includes 7 new chapters covering the latest threats Includes proof-of-concept code stored on the GitHub repository Authors train attendees at major security conferences, including RSA, Black Hat, Defcon, and Besides

Einführung in Data Science - Joel Grus 2019-11-20
Neuaufgabe des Standardwerks, jetzt zu Python 3.6 Der idealer Einstieg in Data Science - didaktisch klug angelegt und gut nachvollziehbar Bietet mathematisches Hintergrundwissen und einen Crashkurs für Python Enthält neues Material zu Deep Learning, Statistik und Natural Language Processing Dieses Buch führt Sie in Data Science ein, indem es grundlegende Prinzipien der Datenanalyse erläutert und Ihnen geeignete Techniken und Werkzeuge vorstellt. Sie lernen nicht nur, wie Sie Bibliotheken, Frameworks, Module und Toolkits konkret einsetzen, sondern implementieren sie auch selbst. Dadurch entwickeln Sie ein tieferes Verständnis für die Zusammenhänge und erfahren, wie essenzielle Tools und Algorithmen der Datenanalyse im Kern funktionieren. Falls Sie Programmierkenntnisse und eine gewisse Sympathie für Mathematik mitbringen, unterstützt Joel Grus Sie dabei, mit den mathematischen und statistischen Grundlagen der Data Science vertraut zu werden und sich Programmierfähigkeiten anzueignen, die Sie für die Praxis benötigen. Dabei verwendet er Python: Die weit verbreitete Sprache ist leicht zu erlernen und bringt zahlreiche Bibliotheken für Data Science mit.

Black Hat Python - Justin Seitz 2014-12-21
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

Gray Hat Hacking The Ethical Hacker's Handbook, Fourth Edition - Daniel Regalado 2015-01-09

Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 12 new chapters, Gray Hat Hacking: The Ethical Hacker's Handbook, Fourth Edition explains the enemy's current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-deploy testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. Build and launch spoofing exploits with Ettercap and Evilgrade Induce error conditions and crash software using fuzzers Hack Cisco routers, switches, and network hardware Use advanced reverse engineering to exploit Windows and Linux software Bypass Windows Access Control and memory protection schemes Scan for flaws in Web applications using Fiddler and the x5 plugin Learn the use-after-free technique used in recent zero days Bypass Web authentication via MySQL type conversion and MD5 injection attacks Inject your shellcode into a browser's memory using the latest Heap Spray techniques Hijack Web browsers with Metasploit and the BeEF Injection Framework Neutralize ransomware before it takes control of your desktop Dissect Android malware with JEB and DAD decompilers Find one-day vulnerabilities with binary diffing

The Web Application Hacker's Handbook - Dafydd Stuttard 2011-08-31

The highly successful security book returns with a new edition, completely updated Web applications are the front door to most organizations, exposing them to attacks that may disclose personal information, execute fraudulent transactions, or compromise ordinary users. This practical book has been completely updated and revised to discuss the latest step-by-step techniques for attacking and defending the range of ever-evolving web applications. You'll explore the various new technologies employed in web applications that have appeared since the first edition and review the new attack techniques that have been developed, particularly in relation to the client side. Reveals how to overcome the new technologies and techniques aimed at defending web applications against attacks that have appeared since the previous edition Discusses new remoting frameworks, HTML5, cross-domain integration techniques, UI redress, framebusting, HTTP parameter pollution, hybrid file attacks, and more Features a companion web site hosted by the authors that allows readers to try out the attacks described, gives answers to the questions that are posed at the end of each chapter, and provides a summarized methodology and checklist of tasks Focusing on the areas of web application security where things have changed in recent years, this book is the most current resource on the critical topic of discovering, exploiting, and preventing web application security flaws. Also available as a set with, CEHv8: Certified Hacker Version 8 Study Guide, Ethical Hacking and Web Hacking Set, 9781119072171.

The Shellcoder's Handbook - Chris Anley 2011-02-16

This much-anticipated revision, written by the ultimate group of top security experts in the world, features 40 percent new content on how to find security holes in any operating system or application New material addresses the many new exploitation techniques that have been discovered since the first edition, including attacking "unbreakable" software packages such as McAfee's Enterscept, Mac OS X, XP, Office 2003, and Vista Also features the first-ever published information on exploiting Cisco's IOS, with content that has never before been explored The companion Web site features downloadable code files

Hacking Exposed - Stuart McClure 2002

Gray Hat Hacking, Second Edition - Shon Harris

2008-01-10

"A fantastic book for anyone looking to learn the tools and techniques needed to break in and stay in." --Bruce Potter, Founder, The Shmoo Group "Very highly recommended whether you are a seasoned professional or just starting out in the security business." --Simple Nomad, Hacker

The Web Application Hacker's Handbook - Dafydd Stuttard 2011-03-16

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

Pädagogische Blätter - 1896

CEH v10 Certified Ethical Hacker Study Guide - Ric Messier 2019-05-31

As protecting information becomes a rapidly growing concern for today's businesses, certifications in IT security have become highly desirable, even as the number of certifications has grown. Now you can set yourself apart with the Certified Ethical Hacker (CEH v10) certification. The CEH v10 Certified Ethical Hacker Study Guide offers a comprehensive overview of the CEH certification requirements using concise and easy-to-follow instruction. Chapters are organized by exam objective, with a handy section that maps each objective to its corresponding chapter, so you can keep track of your progress. The text provides thorough coverage of all topics, along with challenging chapter review questions and Exam Essentials, a key feature that identifies critical study areas. Subjects include intrusion detection, DDoS attacks, buffer overflows, virus creation, and more. This study guide goes beyond test prep, providing practical hands-on exercises to reinforce vital skills and real-world scenarios that put what you've learned into the context of actual job roles. Gain a unique certification that allows you to understand the mind of a hacker Expand your career opportunities with an IT certificate that satisfies the Department of Defense's 8570 Directive for Information Assurance positions Fully updated for the 2018 CEH v10 exam, including the latest developments in IT security Access the Sybex online learning center, with chapter review questions, full-length practice exams, hundreds of electronic flashcards, and a glossary of key terms Thanks to its clear organization, all-inclusive coverage, and practical instruction, the CEH v10 Certified Ethical Hacker Study Guide is an excellent resource for anyone who needs to understand the hacking process or anyone who wants to demonstrate their skills as a Certified Ethical Hacker.

Gray Hat Hacking - Harris 2005-02-01

Hacking - Eric Amberg / Daniel Schmid 2021-12-07

• Methoden und Tools der Hacker, Cyberkriminellen und Penetration Tester • Mit zahlreichen Schritt-für-Schritt-Anleitungen und Praxis-Workshops • Inklusive Vorbereitung auf den Certified Ethical Hacker (CEHv11) mit Beispielfragen zum Lernen Dies ist ein praxisorientierter Leitfaden für angehende Hacker, Penetration Tester, IT-Systembeauftragte, Sicherheitsspezialisten und interessierte Poweruser. Mithilfe vieler Workshops, Schritt-für-Schritt-Anleitungen sowie Tipps und Tricks lernen Sie unter

anderem die Werkzeuge und Mittel der Hacker und Penetration Tester sowie die Vorgehensweise eines professionellen Hacking-Angriffs kennen. Der Fokus liegt auf der Perspektive des Angreifers und auf den Angriffstechniken, die jeder Penetration Tester kennen muss. Dabei erläutern die Autoren für alle Angriffe auch effektive Gegenmaßnahmen. So gibt dieses Buch Ihnen zugleich auch schrittweise alle Mittel und Informationen an die Hand, um Ihre Systeme auf Herz und Nieren zu prüfen, Schwachstellen zu erkennen und sich vor Angriffen effektiv zu schützen. Das Buch umfasst nahezu alle relevanten Hacking-Themen und besteht aus sechs Teilen zu den Themen: Arbeitsumgebung, Informationsbeschaffung, Systeme angreifen, Netzwerk- und sonstige Angriffe, Web Hacking sowie Angriffe auf WLAN und Next-Gen-Technologien. Jedes Thema wird systematisch erläutert. Dabei werden sowohl die Hintergründe und die zugrundeliegenden Technologien als auch praktische Beispiele in konkreten Szenarien besprochen. So haben Sie die Möglichkeit, die Angriffstechniken selbst zu erleben und zu üben. Das Buch ist als Lehrbuch konzipiert, eignet sich aber auch als Nachschlagewerk. Sowohl der Inhalt als auch die Methodik orientieren sich an der Zertifizierung zum Certified Ethical Hacker (CEHv11) des EC-Council. Testfragen am Ende jedes Kapitels helfen dabei, das eigene Wissen zu überprüfen und für die CEH-Prüfung zu trainieren. Damit eignet sich das Buch hervorragend als ergänzendes Material zur Prüfungsvorbereitung. Aus dem Inhalt:

- Aufbau einer Hacking-Laborumgebung
- Einführung in Kali Linux als Hacking-Plattform
- Sicher und anonym im Internet kommunizieren
- Reconnaissance (Informationsbeschaffung)
- Vulnerability-Scanning
- Password Hacking
- Bind und Reverse Shells
- Mit Mailware das System übernehmen
- Spuren verwischen
- Lauschangriffe und Man-in-the-Middle
- Social Engineering
- Web- und WLAN-Hacking
- Angriffe auf IoT-Systeme
- Cloud-Hacking und -Security
- Durchführen von Penetrationstests

Advanced Penetration Testing - Wil Allsopp 2017

Featuring techniques not taught in any certification prep or covered by common defensive scanners, this book integrates social engineering, programming, and vulnerability exploits into a multidisciplinary approach for targeting and compromising high security environments. --

Hands on Ethical Hacking and Network Defense - Michael T. Simpson 2006

With cyber-terrorism and corporate espionage threatening the fiber of our world, the need for trained network security professionals continues to grow. This book describes the tools and penetration testing methodologies used by ethical hackers to better understand how to protect computer networks.

CEH v11 Certified Ethical Hacker Study Guide - Ric Messier 2021-07-16

As protecting information continues to be a growing concern for today's businesses, certifications in IT security have become highly desirable, even as the number of certifications has grown. Now you can set yourself apart with the Certified Ethical Hacker (CEH v11) certification. The CEH v11 Certified Ethical Hacker Study Guide offers a comprehensive overview of the CEH certification requirements using concise and easy-to-follow instructions. Chapters are organized by exam objective, with a handy section that maps each objective to its corresponding chapter, so you can keep track of your progress. The text provides thorough coverage of all topics, along with challenging chapter review questions and Exam Essentials, a key feature that identifies critical study areas. Subjects include common attack practices like reconnaissance and scanning. Also covered are topics like intrusion detection, DoS attacks, buffer overflows, wireless attacks, mobile attacks, Internet of Things (IoT) and more. This study guide goes beyond test prep, providing practical hands-on exercises to reinforce vital skills and real-world scenarios that put what you've learned into the context of actual job roles. Gain a unique certification that allows you to function like an attacker, allowing you to identify vulnerabilities so they can be remediated. Expand your career opportunities with an IT certificate that satisfies the Department of Defense's 8570 Directive for Information Assurance positions Fully updated for the 2020 CEH v11 exam, including the latest developments in IT security Access the Sybex online learning center, with chapter review questions, full-

length practice exams, hundreds of electronic flashcards, and a glossary of key terms Thanks to its clear organization, all-inclusive coverage, and practical instruction, the CEH v11 Certified Ethical Hacker Study Guide is an excellent resource for anyone who needs to understand the hacking process or anyone who wants to demonstrate their skills as a Certified Ethical Hacker.

Hacken für Dummies - Kevin Beaver 2016-11-10

Fürchten Sie um Ihre Unternehmensdaten? Machen Sie sich Sorgen um Ihre IT-Systeme, wenn Sie wieder einmal lesen, dass unbekannte Hacker ein Unternehmen für Wochen lahmgelegt haben? Warten Sie nicht ab, bis es auch in Ihren Systemen passiert, sondern tun Sie etwas! Dabei hilft Ihnen dieses Buch. Versetzen Sie sich als erstes in die Rolle des Schurken und lernen Sie zu denken wie ein Krimineller! Wo sind die Hürden am niedrigsten? Welche grundlegenden Hackertechniken gibt es? Kevin Beaver zeigt Ihnen, wo Ihre Systeme verwundbar sein könnten, sodass Sie im Rennen um die IT-Sicherheit die Nase vorn behalten.

Hacking & IT-Security für Einsteiger - Max Engelhardt 2020-07

Gray Hat Hacking - Shon Harris 2008

Hacking Questions - Connie Hamilton 2019-04-09

"Look out, Socrates! Here comes Connie Hamilton, the newest innovator of questionology! -- Marcia Gutiérrez, High School Educator A fresh perspective on the art of questioning Questions are the driving force of learning in classrooms. Hacking Questions digs into framing, delivering, and maximizing questions in the classroom to keep students engaged in learning. Known in education circles as the "Questioning Guru," Connie Hamilton shows teachers of all subjects and grades how to: Hear the music: listen for correct answers Scaffold to trigger student thinking without doing it for them Kick the IDK bucket to avoid "I don't know" as the final answer Punctuate your learning time to end with reflection questions Spin the throttle to fuel students to ask the questions Fill your back pocket with engagement questions Make yourself invisible by establishing student-centered protocols Be a Pinball Wizard and turn students into facilitators Praise for Connie Hamilton and Hacking Questions "Connie Hamilton is known by teachers and leaders as the Questioning Guru. She offers minor tweaks and major perspective shifts. You will be a better questioner tomorrow." -Dr. Dorothy VanderJagt, Professional Learning Coordinator "Connie Hamilton is a world-class presenter with expertise in the art of questioning. She provides a fresh perspective and practical tips on integrating research-based strategies." -Melisa Mulder, Intervention Teacher "Connie is an incredible driver of change in our focus on classroom questioning as a best practice instructional strategy." -Troy VanderLaan, Middle School Administrator Answers to your questions about questions Hacking Questions provides practical solutions to the universal questioning problems that teachers face daily. Find your answers now.

Hacken für Dummies - Kevin Beaver 2019-01-14

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!

Replacement - Michael T. Simpson 2005-11

Gray Hat Hacking The Ethical Hacker's Handbook, Fourth Edition - Daniel Regalado 2015

Offering field-tested remedies; case studies; and ready-to-deploy testing labs; this cutting-edge book presents techniques for finding and fixing critical security flaws and explains how hackers gain access; overtake network devices; script and inject malicious code; and plunder Web applications and browsers. --

Black Hat Python - Justin Seitz 2014-12-21

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

Hacking For Dummies - Kevin Beaver 2022-04-26

Learn to think like a hacker to secure your own systems and data Your smartphone, laptop, and desktop computer are more important to your life and business than ever before. On top of making your life easier and more productive, they hold sensitive information that should remain private. Luckily for all of us, anyone can learn powerful data privacy and security techniques to keep the bad guys on the outside where they belong. Hacking For Dummies takes you on an easy-to-follow cybersecurity voyage that will teach you the essentials of vulnerability and penetration testing so that you can find the holes in your network before the bad guys exploit them. You will learn to secure your Wi-Fi networks, lock down your latest Windows 11 installation, understand the security implications of remote work, and much more. You'll find out how to: Stay on top of the latest security weaknesses that could affect your business's security setup Use freely available testing tools to "penetration test" your network's security Use ongoing security checkups to continually ensure that your data is safe from hackers Perfect for small business owners, IT and security professionals, and employees who work remotely, Hacking For Dummies is a must-have resource for anyone who wants to keep their data safe.

Hacken mit Kali-Linux - Mark B. 2020-07-07

Bei meiner Arbeit stoße ich immer wieder auf Netzwerke und Webseiten mit erheblichen Sicherheitsproblemen. In diesem Buch versuche ich dem Leser zu vermitteln, wie leicht es mittlerweile ist, Sicherheitslücken mit diversen Tools auszunutzen. Daher sollte meiner Meinung nach jeder, der ein Netzwerk oder eine Webseite betreibt, ansatzweise wissen, wie diverse Hackertools arbeiten, um zu verstehen, wie man sich dagegen schützen kann. Selbst vor kleinen Heimnetzwerken machen viele Hacker nicht halt. Wenngleich das Thema ein sehr technisches ist, werde ich dennoch versuchen, die Konzepte so allgemein verständlich wie möglich erklären. Ein Informatikstudium ist also keinesfalls notwendig, um diesem Buch zu folgen. Dennoch will ich nicht nur die Bedienung diverser Tools erklären, sondern auch deren Funktionsweise so weit erklären, dass Ihnen klar wird, wie das Tool arbeitet und warum ein bestimmter Angriff funktioniert.

Geistiges Hacken - Mentale Manipulation und Dunkle

Psychologie - KEVIN J. ALLEN

Möchten Sie etwas über die Dunkle Psychologie und ihre Grundlagen erfahren? Möchten Sie Manipulationstechniken beherrschen, um Menschen zu beeinflussen? Hast du das Gefühl, dass dich jemand manipuliert und du dich verteidigen willst? Wenn Sie die menschliche Psyche in der Tiefe kennenlernen möchten, lernen, sich zu meistern, zu erkennen und sich gegen mentale Manipulation zu verteidigen, lesen Sie weiter, um die Bedeutung der Dinge zu sehen, die Sie mit diesem Buch lernen werden. Unter Dark Psychology verstehen wir die Techniken, die verwendet werden, um Menschen zu manipulieren und zu überzeugen. Diese Techniken können sowohl negativ gegen uns als auch positiv in unserem täglichen Leben eingesetzt werden, um Akzeptanz zu erlangen und sozial oder bei der Arbeit einflussreicher zu sein. Daher ist es notwendig, diese Techniken zu verstehen, um zu vermeiden, Opfer derer zu werden, die sie anwenden, und um unseren Zustand der menschlichen Beziehungen zu verbessern. IN DIESEM BUCH ERFAHREN SIE : - DIE GRUNDLAGEN DER DUNKLEN PSYCHOLOGIE UND IHRE

HISTORISCHEN UND WISSENSCHAFTLICHEN GRUNDLAGEN. - MENTALE MANIPULATIONSTECHNIKEN - ERKENNE UND VERTEIDIGE DICH VOR MANIPULATOREN, DIE DEIN LEBEN NEGATIV BEEINFLUSSEN - MENTALE MANIPULATION AKTIV NUTZEN, UM IHR SOZIAL- UND ARBEITSLEBEN ZU VERBESSERN - AKTIVE UND PASSIVE MANIPULATIONSTECHNIKEN Psychologie und Manipulation, zusammen mit den einfachen und praktischen Techniken, die Sie in dem Buch finden, werden Ihnen helfen, Ihre Lebensbedingungen zu verbessern und sich besser mit allen zu identifizieren. WENN DU MEHR WISSEN WILLST UND DIE KONTROLLE ÜBER DICH UND DEIN LEBEN WIEDERERLANGEN WILLST, WARTE NICHT... GEHEN SIE ZURÜCK ZUM SEITENANFANG UND KLICKEN SIE AUF JETZT KAUFEN! Mehr Hacking mit Python - Justin Seitz 2015-10-09 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.

Hacken - Joseph Connor 2016-11-02

Meistern Sie das 21. Jahrhundert Diese Buch bring Ihnen alles bei, was Sie wissen müssen!! Wenn Sie vor haben eines Tages zu einem Hacker zu werden, dann sind Sie hier genau richtig! Dieses Buch ist für den Anwender mit guten Absichten geeignet. Es deckt sowohl die Vor- als auch die Nachteile des Hackens ab. Werden Sie ein richtiger Hacker - Computerviren, Cracking, Malware, IT-Sicherheit ist nun in der 2. Auflage erschienen! Dieses Buch dient als perfektes Werkzeug für jeden, der sich gerne mit dieser Materie beschäftigen möchte und so viel wie möglich darüber erfahren will. Besonders ist, dass dieses Buch beide Seiten der Medaille aufgreift und Ihnen somit einen Weg aufzeigt, um zum Besten "weißen" Hacker (Hacker mit guten Absichten) empor zu steigen. Hier finden Sie eine Übersicht der Themen in diesem Buch:- Cracking - ein anderer Vorgang als Hacken- Malware: Der Scherge des Hackens- Computer Virus: Die häufigste Malware- IT-Sicherheit Warum sollten Sie dieses Buch erhalten?- Es enthält wichtige Informationen.- Es erläutert Ihnen den ethischen Hackansatz.- Lernen Sie verschieden Arten von Viren kennen und wie Sie diese gewissenhaft einsetzen können.- Einfach zu lesen und einfach zu verstehen. Also auf was warten Sie noch? Schnappen Sie sich Ihre Kopie von Werden Sie ein richtiger Hacker - Computerviren, Cracking, Malware, IT-Sicherheit - 2. Auflage noch HEUTE und werden Sie ein Hacker! Viel Spaß!

Black Hat Go - Tom Steele 2020-01-24

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 products Build an RC2 symmetric-key bruteforcer Implant data within a Portable Network Graphics (PNG) image. Are you ready to add to your arsenal of security tools? Then let's Go!

Hacking - Jon Erickson 2011

The Basics of Hacking and Penetration Testing - Patrick Engebretson 2013-06-24

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

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

Hacking - John Slavio 2017-01-26

All you wanted to know about Hacking and Computer Security 50% off for a limited time... This book will teach you everything you need to know about hacking, the history of hacking, the types of hacking and security measures that you should undertake. This book will teach you about the techniques you can use to prank your friends or spy on your significant other (maybe). It can also get you started on your journey towards being an ethical hacker, which is a fast-growing, in-demand field. What's Included in This Book History of Hacking Various Types of Hackers Types of Hacking Attacks Basic Hacking Tools and Softwares Common Attacks and Threats Hiding IP Address Mobile Hacking Hacking an Email Address Penetration Testing Spoofing Attacks Scroll up and download now

Hacking- The art Of Exploitation - J. Erickson

2018-03-06

This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.