Online Library Owner Xe2 X80 X99s Guide Pdf Free Copy

Web Application Defender's Cookbook Data Wrangling with Python *Programming Python* Data Management in R Professional NoSQL Intelligent Asset Management Cyber Operations *금융 전략을 위한 머신러닝 Women ' s Cinema, World Cinema* Hacking: The Art of Exploitation, 2nd Edition Gray Hat Hacking the Ethical Hacker's The Browser Hacker's Handbook Shellcoder's Programming Uncovered (Uncovered series) The Oracle Hacker's Handbook *Snort 2.1 Intrusion Detection* Hacking- The art Of Exploitation Security Warrior AI and Machine Learning for Coders *Buffer Overflow Attacks* Coding for Penetration Testers Sockets, Shellcode, Porting, and Coding: Reverse Engineering Exploits and Tool Coding for Security Professionals Gray Hat Hacking The Ethical Hacker's Handbook, Fourth Edition *L'arte dell'hacking - Volume 1* Gray Hat Hacking The Ethical Hackers Handbook, 3rd Edition AI and Machine Learning for Coders Underground Front *防駭戰士* Mastering Kali Linux for Advanced Penetration Testing Guia do Hacker Brasileiro セキュリティウォリア Хакинг: искусство эксплойта. 2-е изд. L'arte dell'hacking - Volume 2 Welcome to the Beatles L'arte dell'hacking. Con CD-ROM Wicked Cool Ruby Scripts Advanced Penetration Testing *Hacking y Forensic* Penetration Testing

Защита от взлома: сокеты, shell-код, эксплойты Gray Hat Python

Provides information and tutorials on Python's application domains and its use in databases, networking, scripting layers, and text processing. Defending your web applications against hackers andattackers The top-selling book Web Application Hacker's Handbookshowed how attackers and hackers identify and attack vulnerablelive web applications. This new Web Application Defender'sCookbook is the perfect counterpoint to that book: it shows youhow to defend. Authored by a highly credentialed defensivesecurity expert, this new book details defensive security methodsand can be used as courseware for training network securitypersonnel, web server administrators, and security consultants. Each "recipe" shows you a way to detect and defend againstmalicious behavior and provides working code examples for theModSecurity web application firewall module. Topics includeidentifying vulnerabilities, setting hacker traps, defendingdifferent access points, enforcing application flows, and muchmore. Provides practical tactics for detecting web attacks andmalicious behavior and defending against them Written by a preeminent authority on web application firewalltechnology and web application defense tactics Offers a series of "recipes" that include working code examplesfor the open-source ModSecurity web application firewallmodule Find the tools, techniques, and expert information you need

todetect and respond to web application attacks with WebApplication Defender's Cookbook: Battling Hackers and ProtectingUsers. How hackers, viruses, and worms attack computers from the Internet and exploit security holes in software is explained in this outline of antivirus software, patches, and firewalls that try in vain to withstand the storm of attacks. Some software's effectiveness exists only in the imaginations of its developers because they prove unable to prevent the propagation of worms, but this guide examines where security holes come from, how to discover them, how to protect systems (both Windows and Unix), and how to do away with security holes altogether. Unpublished advanced exploits and techniques in both C and Assembly languages are L'ebook che non si limita a mostrare come funzionano le tecniche di exploit, ma spiega come svilupparle, ritorna in due ebook.Jon Erickson guida il lettore in un percorso di iniziazione alle tecniche hacker. Ancora una volta il presupposto è che conoscere i metodi, le logiche, la teoria e i fondamenti scientifici che stanno alla base dell'hacking stesso, rappresenta l'unica via per costruire sistemi sicuri.Se la prima edizione di questo libro, pubblicata sul finire del 2003 e tradotta in undici lingue, aveva ottenuto vasti consensi confermati da ampie vendite, la seconda, ora disponibile in formato EPUB, porta la conoscenza delle tecniche dell'hacking a un nuovo livello.Volume 1: argomenti in breve- Introduzione all'hacking- Programmazione in C e Assembly- Tecniche di exploit- Vulnerabilità buffer overflow- Exploit da stringa di

formato- Introduzione alle reti: modello OSI e socket- Sniffing di rete How do you take your data analysis skills beyond Excel to the next level? By learning just enough Python to get stuff done. This hands-on guide shows non-programmers like you how to process information that ’ s initially too messy or difficult to access. You don't need to know a thing about the Python programming language to get started. Through various step-by-step exercises, you ’ ll learn how to acquire, clean, analyze, and present data efficiently. You ’ ll also discover how to automate your data process, schedule file- editing and clean-up tasks, process larger datasets, and create compelling stories with data you obtain. Quickly learn basic Python syntax, data types, and language concepts Work with both machine-readable and human-consumable data Scrape websites and APIs to find a bounty of useful information Clean and format data to eliminate duplicates and errors in your datasets Learn when to standardize data and when to test and script data cleanup Explore and analyze your datasets with new Python libraries and techniques Use Python solutions to automate your entire data-wrangling process Contains fifty-eight Ruby scripts to solve a variety of problems for system administration, image manipulation, and management of a Website. THE LATEST STRATEGIES FOR UNCOVERING TODAY'S MOST DEVASTATING ATTACKS Thwart malicious network intrusion by using cutting-edge techniques for finding and fixing security flaws. Fully updated and expanded with nine new chapters, Gray Hat Hacking: The Ethical Hacker's

Handbook, Third Edition details the most recent vulnerabilities and remedies along with legal disclosure methods. Learn from the experts how hackers target systems, defeat production schemes, write malicious code, and exploit flaws in Windows and Linux systems. Malware analysis, penetration testing, SCADA, VoIP, and Web security are also covered in this comprehensive resource. Develop and launch exploits using BackTrack and Metasploit Employ physical, social engineering, and insider attack techniques Build Perl, Python, and Ruby scripts that initiate stack buffer overflows Understand and prevent malicious content in Adobe, Office, and multimedia files Detect and block client-side, Web server, VoIP, and SCADA attacks Reverse engineer, fuzz, and decompile Windows and Linux software Develop SQL injection, cross-site scripting, and forgery exploits Trap malware and rootkits using honeypots and SandBoxes David Litchfield has devoted years to relentlessly searching out the flaws in the Oracle database system and creating defenses against them. Now he offers you his complete arsenal to assess and defend your own Oracle systems. This in-depth guide explores every technique and tool used by black hat hackers to invade and compromise Oracle and then it shows you how to find the weak spots and defend them. Without that knowledge, you have little chance of keeping your databases truly secure. Tools used for penetration testing are often purchased or downloaded from the Internet. Each tool is based on a programming language such as Perl, Python, or Ruby. If a

penetration tester wants to extend, augment, or change the functionality of a tool to perform a test differently than the default configuration, the tester must know the basics of coding for the related programming language. Coding for Penetration Testers provides the reader with an understanding of the scripting languages that are commonly used when developing tools for penetration testing. It also guides the reader through specific examples of custom tool development and the situations where such tools might be used. While developing a better understanding of each language, the reader is guided through real-world scenarios and tool development that can be incorporated into a tester's toolkit. The book is logically divided into 5 main categories with each category representing a major skill set required by most security professionals: 1. Coding – The ability to program and script is quickly becoming a mainstream requirement for just about everyone in the security industry. This section covers the basics in coding complemented with a slue of programming tips and tricks in C/C++, Java, Perl and NASL. 2. Sockets – The technology that allows programs and scripts to communicate over a network is sockets. Even though the theory remains the same – communication over TCP and UDP, sockets are implemented differently in nearly ever language. 3. Shellcode – Shellcode, commonly defined as bytecode converted from Assembly, is utilized to execute commands on remote systems via direct memory access. 4. Porting – Due to the differences between operating

platforms and language implementations on those platforms, it is a common practice to modify an original body of code to work on a different platforms. This technique is known as porting and is incredible useful in the real world environments since it allows you to not " recreate the wheel. 5. Coding Tools – The culmination of the previous four sections, coding tools brings all of the techniques that you have learned to the forefront. With the background technologies and techniques you will now be able to code quick utilities that will not only make you more productive, they will arm you with an extremely valuable skill that will remain with you as long as you make the proper time and effort dedications. *Contains never before seen chapters on writing and automating exploits on windows systems with all-new exploits. *Perform zero-day exploit forensics by reverse engineering malicious code. *Provides working code and scripts in all of the most common programming languages for readers to use TODAY to defend their networks. This book presents a systematic application of recent advances in artificial intelligence (AI) to the problem of asset management. While natural language processing and text mining techniques, such as semantic representation, sentiment analysis, entity extraction, commonsense reasoning, and fact checking have been evolving for decades, finance theories have not yet fully considered and adapted to these ideas. In this unique, readable volume, the authors discuss integrating textual knowledge and market sentiment step-by-step, offering

readers new insights into the most popular portfolio optimization theories: the Markowitz model and the Black-Litterman model. The authors also provide valuable visions of how AI technology-based infrastructures could cut the cost of and automate wealth management procedures. This inspiring book is a must-read for researchers and bankers interested in cutting-edge AI applications in finance. In Women ' s Cinema, World Cinema, Patricia White explores the dynamic intersection of feminism and film in the twenty-first century by highlighting the work of a new generation of women directors from around the world: Samira and Hana Makhmalbaf, Nadine Labaki, Zero Chou, Jasmila Zbanic, and Claudia Llosa, among others. The emergence of a globalized network of film festivals has enabled these young directors to make and circulate films that are changing the aesthetics and politics of art house cinema and challenging feminist genealogies. Extending formal analysis to the production and reception contexts of a variety of feature films, White explores how women filmmakers are both implicated in and critique gendered concepts of authorship, taste, genre, national identity, and human rights. Women ' s Cinema, World Cinema revitalizes feminist film studies as it argues for an alternative vision of global media culture. Cyber Operations walks you through all the processes to set up, defend, and attack computer networks. This book focuses on networks and real attacks, offers extensive coverage of offensive and defensive techniques, and is supported by a

rich collection of exercises and resources. You'll learn how to configure your network from the ground up, starting by setting up your virtual test environment with basics like DNS and active directory, through common network services, and ending with complex web applications involving web servers and backend databases. Key defensive techniques are integrated throughout the exposition. You will develop situational awareness of your network and will build a complete defensive infrastructure—including log servers, network firewalls, web application firewalls, and intrusion detection systems. Of course, you cannot truly understand how to defend a network if you do not know how to attack it, so you will attack your test systems in a variety of ways beginning with elementary attacks against browsers and culminating with a case study of the compromise of a defended e-commerce site. The author, who has coached his university ' s cyber defense team three times to the finals of the National Collegiate Cyber Defense Competition, provides a practical, hands-on approach to cyber security.
В своей новой книге Джеймс Фостер, автор ряда бестселлеров, впервые описывает методы, которыми пользуются хакеры для атак на операционные системы и прикладные программы. Он приводит примеры работающего кода на языках C/C++, Java, Perl и NASL, в

которых иллюстрируются методы обнаружения и защиты от наиболее опасных атак. В книге подробно изложены вопросы, разбираться в которых насущно необходимо любому программисту, работающему в сфере информационной безопасности: программирование сокетов, shell-коды, переносимые приложения и принципы написания эксплойтов. 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 Underground Front is a pioneering examination of the role that the Chinese Communist Party has played in Hong Kong since the creation of the party in 1921, through to the present day. The second edition goes into greater depth on the party ’ s view on “ one country, two systems ”, “ patriotism ”, and “ elections ”. The introduction has been extensively revised and the concluding chapter has been completely rewritten in order to give a thorough account of the post-1997 governance and political system in Hong Kong, and where challenges lie. Christine Loh endeavours to keep the data and the materials up to date and to include the discussion of some recent events in Hong Kong. The appendices on the key targets of the party ’ s united front activities also make the book an especially useful read for all who are interested in Hong Kong history and politics, and the history of modern China. ‘ Although the author calls herself an “ outsider ”,

this book provides such a distinctly incisive analysis that even an “ insider ” will pale by comparison. Christine Loh ’ s exposition of the Communist Party ’ s co-optation and persuasion is particularly revealing for anyone not versed in communist-speak. A must-read for anyone who cares for Hong Kong—simply because the Communist Party in Hong Kong is a heavyweight player in shaping our future. ’ —Ching Cheong ‘ Authoritative, thoroughly researched and lucidly written, Christine Loh ’ s work must be read by everyone who wants to make sense of the Chinese Communist Party ’ s agenda in Hong Kong. This book is remarkable for its fair-mindedness in evaluating the party ’ s record. She provides an absorbing account of its leaders ’ hard-headed pragmatism in tolerating this outpost of colonial and capitalism during the Cold War and the Cultural Revolution. Her analysis of the party ’ s involvement in contemporary Hong Kong is an impressive contribution to our understanding of Beijing ’ s expanding involvement in Hong Kong affairs. The author has achieved a notable breakthrough with this fascinating study of a political organisation whose role and influence in Hong Kong have hitherto been shrouded in secrecy. ’ —Leo Goodstadt Why study programming? Ethical gray hat hackers should study programming and learn as much about the subject as possible in order to find vulnerabilities in programs and get them fixed before unethical hackers take advantage of them. It is very much a foot race: if the vulnerability exists, who will find it first? The purpose of this chapter is to give you the survival skills

necessary to understand upcoming chapters and later find the holes in software before the black hats do. In this chapter, we cover the following topics: • C programming language • Computer memory • Intel processors • Assembly language basics • Debugging with gdb • Python survival skills К а ж д ы й п р о г р а м м и с т п о с у т и с в о е й — х а к е р . В е д ь п е р в о н а ч а л ь н о х а к и н г о м н а з ы в а л и п о и с к и с к у с н о г о и н е о ч е в и д н о г о р е ш е н и я . П о н и м а н и е п р и н ц и п о в п р о г р а м м и р о в а н и я п о м о г а е т н а х о д и т ь у я з в и м о с т и , а н а в ы к и о б н а р у ж е н и я у я з в и м о с т е й п о м о г а ю т с о з д а в а т ь п р о г р а м м ы , п о э т о м у м н о г и е х а к е р ы з а н и м а ю т с я т е м и д р у г и м о д н о в р е м е н н о . И н т е р е с н ы е н е с т а н д а р т н ы е х о д ы е с т ь к а к в т е х н и к а х н а п и с а н и я э л е г а н т н ы х п р о г р а м м , т а к и в т е х н и к а х п о и с к а с л а б ы х м е с т . С ч е г о н а ч а т ь ? Ч т о б ы п е р е з а п и с ы в а т ь п а м я т ь с п о м о щ ь ю п е р е п о л н е н и я б у ф е р а , п о л у ч а т ь д о с т у п к у д а л е н н о м у с е р в е р у и п е р е х в а т ы в а т ь с о е д и н е н и я в а м п р е д с т о и т

программировать на Си и ассемблере, использовать шелл-код и регистры процессора, познакомиться с сетевыми взаимодействиями и шифрованием и многое другое. Как бы мы ни хотели верить в чудо, программное обеспечение и компьютерные сети, от которых зависит наша повседневная жизнь, обладают уязвимостями. Мир без хакеров — это мир без любопытства и новаторских решений. Джон Эриксон Discusses the intrusion detection system and explains how to install, configure, and troubleshoot it. If you're looking to make a career move from programmer to AI specialist, this is the ideal place to start. Based on Laurence Moroney's extremely successful AI courses, this introductory book provides a hands-on, code-first approach to help you build confidence while you learn key topics. You'll understand how to implement the most common scenarios in machine learning, such as computer vision, natural language processing (NLP), and sequence modeling for web, mobile, cloud, and embedded runtimes. Most books on machine learning begin with a daunting amount of advanced math. This guide is built on practical lessons that let you work directly with the code. You'll learn: How to build models with TensorFlow using

skills that employers desire The basics of machine learning by working with code samples How to implement computer vision, including feature detection in images How to use NLP to tokenize and sequence words and sentences Methods for embedding models in Android and iOS How to serve models over the web and in the cloud with TensorFlow Serving Hackers exploit browser vulnerabilities to attack deep withinnetworks The Browser Hacker's Handbook gives a practicalunderstanding of hacking the everyday web browser and using it as abeachhead to launch further attacks deep into corporate networks.Written by a team of highly experienced computer security experts,the handbook provides hands-on tutorials exploring a range ofcurrent attack methods. The web browser has become the most popular and widely usedcomputer "program" in the world. As the gateway to the Internet, itis part of the storefront to any business that operates online, butit is also one of the most vulnerable entry points of any system.With attacks on the rise, companies are increasingly employingbrowser-hardening techniques to protect the unique vulnerabilitiesinherent in all currently used browsers. The Browser Hacker'sHandbook thoroughly covers complex security issues and exploresrelevant topics such as: Bypassing the Same Origin Policy ARP spoofing, social engineering, and phishing to accessbrowsers DNS tunneling, attacking web applications, andproxying—all from the browser Exploiting the browser and its ecosystem (plugins andextensions) Cross-origin attacks,

including Inter-protocol Communicationand Exploitation The Browser Hacker's Handbook is written with aprofessional security engagement in mind. Leveraging browsers aspivot points into a target's network should form an integralcomponent into any social engineering or red-team securityassessment. This handbook provides a complete methodology tounderstand and structure your next browser penetration test. A practical guide to testing your infrastructure security with Kali Linux, the preferred choice of pentesters and hackers Key FeaturesEmploy advanced pentesting techniques with Kali Linux to build highly secured systemsDiscover various stealth techniques to remain undetected and defeat modern infrastructuresExplore red teaming techniques to exploit secured environmentBook Description This book takes you, as a tester or security practitioner, through the reconnaissance, vulnerability assessment, exploitation, privilege escalation, and post-exploitation activities used by pentesters. To start with, you'll use a laboratory environment to validate tools and techniques, along with an application that supports a collaborative approach for pentesting. You'll then progress to passive reconnaissance with open source intelligence and active reconnaissance of the external and internal infrastructure. You'll also focus on how to select, use, customize, and interpret the results from different vulnerability scanners, followed by examining specific routes to the target, which include bypassing physical security and the exfiltration of data using a variety of techniques. You'll discover concepts

such as social engineering, attacking wireless networks, web services, and embedded devices. Once you are confident with these topics, you'll learn the practical aspects of attacking user client systems by backdooring with fileless techniques, followed by focusing on the most vulnerable part of the network – directly attacking the end user. By the end of this book, you'll have explored approaches for carrying out advanced pentesting in tightly secured environments, understood pentesting and hacking techniques employed on embedded peripheral devices. What you will learnConfigure the most effective Kali Linux tools to test infrastructure securityEmploy stealth to avoid detection in the infrastructure being testedRecognize when stealth attacks are being used against your infrastructureExploit networks and data systems using wired and wireless networks as well as web servicesIdentify and download valuable data from target systemsMaintain access to compromised systemsUse social engineering to compromise the weakest part of the network - the end usersWho this book is for This third edition of Mastering Kali Linux for Advanced Penetration Testing is for you if you are a security analyst, pentester, ethical hacker, IT professional, or security consultant wanting to maximize the success of your infrastructure testing using some of the advanced features of Kali Linux. Prior exposure of penetration testing and ethical hacking basics will be helpful in making the most out of this book. Este libro se dirige a toda persona que desee aprender Python para el Hacking y el análisis forense y formarse en

el diseño de herramientas en Python, así como a los profesionales de la seguridad informática y del Análisis Forense. Tiene como objetivo llevar al lector a una comprensión de las librerías específicas de Python para poder luego diseñar sus herramientas personalizadas, adaptadas a situaciones particulares en Hacking y Forensic. Para sacar el máximo provecho posible, es necesario contar con nociones de seguridad informática. El libro consta de 8 capítulos, cada uno ilustrado por muchos ejemplos y ejercicios con sus correcciones al final del capítulo, para proporcionar al lector una forma de auto-evaluación. El capítulo 1 permitirá aprender los conceptos del lenguaje Python, y las bases del lenguaje. El capítulo 2 está dedicado a la programación en red. Abordaremos la programación de sockets y luego los diferentes servicios tales como HTTP, FTP, POP, SSL, al igual que las expresiones regulares y el acceso a bases de datos. El capítulo 3 está dedicado a la librería scapy, muy útil en hacking y Forensic; el autor detalla el tratamiento de las tramas, el tunneling, los diferentes tipos de escaneo de red y también aborda el protocolo IPv6. Para el capítulo 4, son indispensables conocimientos básicos de la arquitectura PC y ensamblador, así como el uso de depuradores, para la correcta comprensión de la librería PyDbg empleada. El capítulo 5 está dedicado al Fuzzing ; en la primera parte el autor utiliza librerías ya vistas en capítulos anteriores para luego, en una segunda parte, estudiar una librería específica, llamada Sulley, especializada en el fuzzing. El capítulo 6 examina la

librería PIL que va a permitir la gestión de imágenes, su edición, y captura de imágenes desde una webcam para extraer los datos; el autor examinará también un elemento particular de la seguridad en la web, los captcha. El capítulo 7 desarrolla los conceptos vistos en el capítulo 2, a fin de construir en Python herramientas de análisis de seguridad para sitios web. Por último, el capítulo final estádedicado íntegramente al análisis forense (Forensic); el autor efectúa una revisión, no exhaustiva, de las diferentes técnicas, recorriendo la esteganografía, la criptografía, y elacoso por e-mail. El autor ha querido hacer de este libro un compendio no exhaustivo de las librerías más útiles, explicándolas e ilustrándolas con ejemplos concretos para que el lector pueda dominar su funcionamiento. Los scripts de cada capítulo pueden descargarse desde el sitio www.ediciones-eni.com. Los capítulos del libro: Prólogo – Python: los fundamentos – La red – Red: la librería Scapy – Depuración en Windows – El fuzzing – Tratamiento de imágenes – Un poco más sobre la Web – Análisis forense Hacking is the art of creative problem solving, whether that means finding an unconventional solution to a difficult problem or exploiting holes in sloppy programming. Many people call themselves hackers, but few have the strong technical foundation needed to really push the envelope. Rather than merely showing how to run existing exploits, author Jon Erickson explains how arcane hacking techniques actually work. To share the art and science of hacking in a way that is accessible to everyone, Hacking: The Art of

Exploitation, 2nd Edition introduces the fundamentals of C programming from a hacker's perspective. The included LiveCD provides a complete Linux programming and debugging environment—all without modifying your current operating system. Use it to follow along with the book's examples as you fill gaps in your knowledge and explore hacking techniques on your own. Get your hands dirty debugging code, overflowing buffers, hijacking network communications, bypassing protections, exploiting cryptographic weaknesses, and perhaps even inventing new exploits. This book will teach you how to: – Program computers using C, assembly language, and shell scripts – Corrupt system memory to run arbitrary code using buffer overflows and format strings – Inspect processor registers and system memory with a debugger to gain a real understanding of what is happening – Outsmart common security measures like nonexecutable stacks and intrusion detection systems – Gain access to a remote server using port-binding or connect-back shellcode, and alter a server's logging behavior to hide your presence – Redirect network traffic, conceal open ports, and hijack TCP connections – Crack encrypted wireless traffic using the FMS attack, and speed up brute-force attacks using a password probability matrix Hackers are always pushing the boundaries, investigating the unknown, and evolving their art. Even if you don't already know how to program, Hacking: The Art of Exploitation, 2nd Edition will give you a complete picture of programming, machine architecture, network

communications, and existing hacking techniques. Combine this knowledge with the included Linux environment, and all you need is your own creativity. 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? 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. If you're looking to make a career move from programmer to AI specialist, this is the ideal place to start. Based on Laurence Moroney's extremely successful AI courses, this introductory book provides a hands-on, code-first approach to help you build confidence while you learn key topics. You'll understand how to implement the most common scenarios in machine learning, such as computer vision, natural language processing (NLP), and sequence modeling for web, mobile, cloud, and embedded runtimes. Most books on machine learning begin with a daunting amount of advanced math. This guide is built on practical lessons that let you work directly with the code. You'll learn: How to build models with TensorFlow using skills that employers desire The basics of machine learning by working with code samples How to implement computer vision, including feature detection in images How to use NLP to tokenize and sequence words and sentences Methods for embedding models in Android and iOS How to serve models over the web and in the cloud with TensorFlow Serving When it comes to network security, many users and administrators are running scared, and justifiably so. The sophistication of attacks against computer systems increases with each new Internet worm.What's the worst an attacker can do to you? You'd better find out, right? That's what Security Warrior teaches you. Based on the principle that the only way to defend yourself is to understand your attacker in depth, Security Warrior reveals how your systems can be

attacked. Covering everything from reverse engineering to SQL attacks, and including topics like social engineering, antiforensics, and common attacks against UNIX and Windows systems, this book teaches you to know your enemy and how to be prepared to do battle.Security Warrior places particular emphasis on reverse engineering. RE is a fundamental skill for the administrator, who must be aware of all kinds of malware that can be installed on his machines -- trojaned binaries, "spyware" that looks innocuous but that sends private data back to its creator, and more. This is the only book to discuss reverse engineering for Linux or Windows CE. It's also the only book that shows you how SQL injection works, enabling you to inspect your database and web applications for vulnerability.Security Warrior is the most comprehensive and up-to-date book covering the art of computer war: attacks against computer systems and their defenses. It's often scary, and never comforting. If you're on the front lines, defending your site against attackers, you need this book. On your shelf--and in your hands. L'ebook che non si limita a mostrare come funzionano le tecniche di exploit, ma spiega come svilupparle, ritorna in due ebook.Jon Erickson guida il lettore in un percorso di iniziazione alle tecniche hacker. Ancora una volta il presupposto è che conoscere i metodi, le logiche, la teoria e i fondamenti scientifici che stanno alla base dell'hacking stesso, rappresenta l'unica via per costruire sistemi sicuri.Se la prima edizione di questo libro, pubblicata sul finire del 2003 e tradotta in undici lingue, aveva ottenuto

vasti consensi confermati da ampie vendite, la seconda, ora disponibile in formato EPUB, porta la conoscenza delle tecniche dell'hacking a un nuovo livello.Volume 2: argomenti in breve- Attacchi DoS (Denial of Service)- Dirottamento TCP/IP- Scansione di porte- Programmi shellcode- Crittografia e crittoanalisi- Violazione di sistemi cifrati- Cracking di password- Attacchi e contromisure Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you ’ ll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you ’ ll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You ’ ll even explore

writing your own exploits. Then it ’ s on to mobile hacking—Weidman ’ s particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs. 적용 사례 연구 및 코드 예제를 함께 제공하는 금융 분야의 ML 및 AI를 다루는 ‘ 완전한 ’ 책 앞으로 금융 산업은 머신러닝과 데이터 과학으로 인해 변화될 것이다. 이 책은 금융업계에서 종사하는 분석가, 거래자, 연구원, 개발자, 데이터 엔지니어에게 유익한 머신러닝 알고리즘 구축법을 다룬다. 자연어 처리와 함께 지도 학습, 비지도 학습, 강화 학습에 필요한 머신러닝 개념과 19가지 사례 연구를 살펴본다. 또한 헤지 펀드, 투자 은행, 핀테크 회사 등 투자 전문가로 성장하기에 필요한 딥러닝 기반의 가이드를 제공한다. 포트폴리오 관리, 알고리즘 거래, 파생 상품 가격 책정, 이상 거래 탐지, 자산 가격 예측, 감정 분석, 챗봇 개발에 대해 자세히 설명한다. 실무자가 직면한 실제 문제를 코드와 예제를 활용해 해결할 수 있도록 과학적 솔루션을 제공한다. 복잡한 금융 데이터를 제대로 다루고 싶다면 꼭 읽어야 할 필독서! 금융 서비스 분야는 방대한 데이터를 실시간으로 생성하며, 데이터 해석에 따른 올바르고 신속한 판단과 결정이 필요합니다. 금융 사기 탐지, 신용 대출 심사, 주가 변화 추이 예측, 포트폴리오 구성 및 재조정 등 다양한 금융 서비스에 머신러닝을 활용할 수 있습니다. 이 책의 실전 문제에서 다양한 활용법을 소개 및 구현하고 시연합니다. 더 나아가 각 장 마무리에 연습 문제를 제시하여 어떻게 응용, 발전시킬지 구체적 방향을 제시합니다. 머신러닝을 이해하고 금융 서비스에 활용하는 시대, 나아가 금융 자산을 보호하고, 자산 가치를 극대화하는

시대가 현실화되고 있습니다. 이 책을 재밌게 읽고 책에서 소개한 내용을 실제로 활용 및 응용할 수 있기를 바랍니다. 대상 독자 금융 데이터를 제대로 다루고 싶은 학생, 관련 직업 종사자 파이썬을 활용하여 자신의 기존 전략을 정량화하고 자동화하고 싶은 독자 주요 내용 거래 전략, 파생 상품 가격 책정, 포트폴리오 관리 — 회귀 기반 지도 학습 모델 신용 부도 위험 예측, 이상 거래 탐지와 거래 전략 — 분류 기반 지도 학습 모델 포트폴리오 관리, 거래 전략과 수익률 곡선 구성에 대한 사례 연구 — 차원 축소 기법 거래 전략과 포트폴리오 관리에 대한 사례 연구와 함께 유사한 개체 찾기 — 알고리즘과 클러스터링 기술 거래 전략 구축, 파생 상품 헤징과 포트폴리오 관리 — 강화 학습 모델과 기법 텍스트 분석, 텍스트 마이닝, 전산 언어학, 콘텐츠 분석 — NLP 기술 A hands-on guide to leveraging NoSQL databases NoSQL databases are an efficient and powerful tool for storing and manipulating vast quantities of data. Most NoSQL databases scale well as data grows. In addition, they are often malleable and flexible enough to accommodate semi-structured and sparse data sets. This comprehensive hands-on guide presents fundamental concepts and practical solutions for getting you ready to use NoSQL databases. Expert author Shashank Tiwari begins with a helpful introduction on the subject of NoSQL, explains its characteristics and typical uses, and looks at where it fits in the application stack. Unique insights help you choose which NoSQL solutions are best for solving your specific data storage needs. Professional NoSQL: Demystifies the concepts that relate to NoSQL databases, including column-family oriented stores, key/value databases, and

document databases. Delves into installing and configuring a number of NoSQL products and the Hadoop family of products. Explains ways of storing, accessing, and querying data in NoSQL databases through examples that use MongoDB, HBase, Cassandra, Redis, CouchDB, Google App Engine Datastore and more. Looks at architecture and internals. Provides guidelines for optimal usage, performance tuning, and scalable configurations. Presents a number of tools and utilities relating to NoSQL, distributed platforms, and scalable processing, including Hive, Pig, RRDtool, Nagios, and more. The SANS Institute maintains a list of the "Top 10 Software Vulnerabilities." At the current time, over half of these vulnerabilities are exploitable by Buffer Overflow attacks, making this class of attack one of the most common and most dangerous weapon used by malicious attackers. This is the first book specifically aimed at detecting, exploiting, and preventing the most common and dangerous attacks. Buffer overflows make up one of the largest collections of vulnerabilities in existence; And a large percentage of possible remote exploits are of the overflow variety. Almost all of the most devastating computer attacks to hit the Internet in recent years including SQL Slammer, Blaster, and I Love You attacks. If executed properly, an overflow vulnerability will allow an attacker to run arbitrary code on the victim ' s machine with the equivalent rights of whichever process was overflowed. This is often used to provide a remote shell onto the victim machine, which can be used for further exploitation. A

buffer overflow is an unexpected behavior that exists in certain programming languages. This book provides specific, real code examples on exploiting buffer overflow attacks from a hacker's perspective and defending against these attacks for the software developer. Over half of the "SANS TOP 10 Software Vulnerabilities" are related to buffer overflows. None of the current-best selling software security books focus exclusively on buffer overflows. This book provides specific, real code examples on exploiting buffer overflow attacks from a hacker's perspective and defending against these attacks for the software developer. Um clássico da literatura sobre Hackers. Lançado em 2002, foi o primeiro livro de Marcos Flávio Araújo Assunção, que se tornou depois referência internacional na área publicando outros livros como: Desafio Linux Hacker, Segredos do Hacker Ético, Honeypots e Honeynets e Wireless Hacking: Ataques e Segurança de Redes sem fio Wi-Fi. 犯罪者から身を守るためには何が必要か?ただ闇雲に塀を高くしたり、よく切れるナイフを懐に入れておくだけでは十分とは言えない。防御をより完璧に近づけるためには、犯罪者の手口を知り、詳しく分析して対策を練る必要がある。同時に自分の弱点を知ることも重要。本書は攻撃者の手口の詳細はもちろん、心理や目的にまで踏み込んでさまざまな観点から多角的に検討。その上で効果的な対策方法を示している。日夜クラッカーと戦うシステム管理者だけでなく、すべてのPCユーザに贈る最強のセキュリティ本。UNIX、Linux、Windows、WindowsCE対応。 An invaluable, step-by-step guide to data management in R for social science researchers. This

book will show you how to recode data, combine data from different sources, document data, and import data from statistical packages other than R. It explores both qualitative and quantitative data and is packed with a range of supportive learning features such as code examples, overview boxes, images, tables, and diagrams. Build a better defense against motivated, organized, professional attacks Advanced Penetration Testing: Hacking the World's Most Secure Networks takes hacking far beyond Kali linux and Metasploit to provide a more complex attack simulation. 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. From discovering and creating attack vectors, and moving unseen through a target enterprise, to establishing command and exfiltrating data—even from organizations without a direct Internet connection—this guide contains the crucial techniques that provide a more accurate picture of your system's defense. Custom coding examples use VBA, Windows Scripting Host, C, Java, JavaScript, Flash, and more, with coverage of standard library applications and the use of scanning tools to bypass common defensive measures. Typical penetration testing consists of low-level hackers attacking a system with a list of known vulnerabilities, and defenders preventing those hacks using an equally well-known list of defensive scans.

The professional hackers and nation states on the forefront of today's threats operate at a much more complex level—and this book shows you how to defend your high security network. Use targeted social engineering pretexts to create the initial compromise Leave a command and control structure in place for long-term access Escalate privilege and breach networks, operating systems, and trust structures Infiltrate further using harvested credentials while expanding control Today's threats are organized, professionally-run, and very much for-profit. Financial institutions, health care organizations, law enforcement, government agencies, and other high-value targets need to harden their IT infrastructure and human capital against targeted advanced attacks from motivated professionals. Advanced Penetration Testing goes beyond Kali linux and Metasploit and to provide you advanced pen testing for high security networks.

- Intelligent Asset Management
- Cyber Operations
-
- Womens Cinema World Cinema
- Hacking The Art Of Exploitation 2nd Edition
- Gray Hat Hacking The Ethical Hackers
- The Browser Hackers Handbook
- Shellcoders Programming Uncovered Uncovered Series
- The Oracle Hackers Handbook
- Snort 21 Intrusion Detection
- Hacking The Art Of Exploitation
- Security Warrior
- AI And Machine Learning For Coders
- Buffer Overflow Attacks
- Coding For Penetration Testers
- Sockets Shellcode Porting And Coding Reverse Engineering Exploits And Tool Coding For Security Professionals
- Gray Hat Hacking The Ethical Hackers Handbook Fourth Edition
- Larte Dellhacking Volume 1
- Gray Hat Hacking The Ethical Hackers Handbook 3rd Edition
- AI And Machine Learning For Coders
- Underground Front

- Mastering Kali Linux For Advanced Penetration Testing

- Guia Do Hacker Brasileiro

- 2
- Larte Dellhacking Volume
- Welcome To The Beatles
- Larte Dellhacking Con CD ROM
- Wicked Cool Ruby Scripts
- Advanced Penetration Testing
- Hacking Y Forensic
- Penetration Testing
- Shell
- Gray Hat Python