Site To Download Counter Hack A Step By Step Guide To Computer Attacks And Effective Defenses The Radia Perlman Series In Computer Networking And Security

Thank you very much for downloading **Counter Hack A Step By Step Guide To Computer Attacks And Effective Defenses The Radia Perlman Series In Computer Networking And Security**.Most likely you have knowledge that, people have see numerous time for their favorite books similar to this Counter Hack A Step By Step Guide To Computer Attacks And Effective Defenses The Radia Perlman Series In Computer Networking And Security, but stop occurring in harmful downloads.

Rather than enjoying a fine book in the manner of a cup of coffee in the afternoon, instead they juggled subsequent to some harmful virus inside their computer. **Counter Hack A Step By Step Guide To Computer Attacks And Effective Defenses The Radia Perlman Series In Computer Networking And Security** is within reach in our digital library an online access to it is set as public therefore you can download it instantly. Our digital library saves in combination countries, allowing you to get the most less latency era to download any of our books in the same way as this one. Merely said, the Counter Hack A Step By Step Guide To Computer Attacks And Effective Defenses The Radia Perlman Series In Computer Networking And Security is universally compatible considering any devices to read.

7D2 - ELLISON KRAMER

Practically every crime now involves some aspect of digital evidence. This is the most recent volume in the Advances in Digital Forensics series. It describes original research results and innovative applications in the emerging discipline of digital forensics. In addition, it highlights some of the major technical and legal issues related to digital evidence and electronic crime investigations.

Never HIGHLIGHT a Book Again! Virtually all of the testable terms, concepts, persons, places, and events from the textbook are included. Cram101 Just the FACTS101 studyguides give all of the outlines, highlights, notes, and quizzes for your textbook with optional online comprehensive practice tests. Only Cram101 is Textbook Specific. Accompanys: 9780131481046 .

Introductory textbook in the important area of network security for undergraduate and graduate students * Comprehensively covers fundamental concepts with newer topics such as electronic cash,

bit-coin, P2P, SHA-3, E-voting, and Zigbee security * Fully updated to reflect new developments in network security * Introduces a chapter on Cloud security, a very popular and essential topic * Uses everyday examples that most computer users experience to illustrate important principles and mechanisms * Features a companion website with Powerpoint slides for lectures and solution manuals to selected exercise problems, available at http://www.cs.uml.edu/~wang/NetSec

There are many books that detail tools and techniques of penetration testing, but none of these effectively communicate how the information gathered from tests should be analyzed and implemented. Until recently, there was very little strategic information available to explain the value of ethical hacking and how tests should be performed in order to provide a company with insight beyond a mere listing of security vulnerabilities. Now there is a resource that illustrates how an organization can gain as much value from an ethical hack as possible. The Ethical Hack: A Framework for Business Value Penetration Testing explains the methodologies, framework, and "unwritten conventions" that ethical hacks should employ to provide the maximum value to organizations that want to harden their security. This book is unique in that it goes beyond the technical aspects of penetration testing to address the processes and rules of engagement required for successful tests. It examines testing from a strategic perspective, shedding light on how testing ramifications affect an entire organization. Security practitioners can use this resource to reduce their exposure and deliver a focused, valuable service to customers. Organizations will learn how to align the information about tools, techniques, and vulnerabilities that they gathered from testing with their overall business objectives.

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.

This video training course will empower network and system administrators to defend their information from hackers. Leading network security expert Ed Skoudis presents the insiders explanation of today's most destructive hacker tools and provides proven counter measures to keep your information safe.

This book presents a comprehensive study of different tools and techniques available to perform network forensics. Also, various aspects of network forensics are reviewed as well as related technologies and their limitations. This helps security practitioners and researchers in better understanding of the problem, current solution space, and future research scope to detect and investigate various network intrusions against such attacks efficiently. Forensic computing is rapidly gaining importance since the amount of crime involving digital systems is steadily increasing. Furthermore, the area is still underdeveloped and poses many technical and legal challenges. The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of online attacks. There are many reasons which are motivating the attackers to be fearless in carrying out the attacks. For example, the speed with which an at-

tack can be carried out, the anonymity provided by the medium, nature of medium where digital information is stolen without actually removing it, increased availability of potential victims and the global impact of the attacks are some of the aspects. Forensic analysis is performed at two different levels: Computer Forensics and Network Forensics. Computer forensics deals with the collection and analysis of data from computer systems, networks, communication streams and storage media in a manner admissible in a court of law. Network forensics deals with the capture, recording or analysis of network events in order to discover evidential information about the source of security attacks in a court of law. Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. Network forensics generally refers to the collection and analysis of network data such as network traffic, firewall logs, IDS logs, etc. Technically, it is a member of the already-existing and expanding the field of digital forensics. Analogously, network forensics is defined as "The use of scientifically proved techniques to collect, fuses, identifies, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities." Network forensics plays a significant role in the security of today's organizations. On the one hand, it helps to learn the details of external attacks ensuring similar future attacks are thwarted. Additionally, network forensics is essential for investigating insiders' abuses that constitute the second costliest type of attack within organizations. Finally, law enforcement requires network forensics for crimes in which a computer or digital system is either being the target of a crime or being used as a tool in carrying a crime. Network security protects the system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. However, network forensics involves post mortem investigation of the attack and is initiated after crime notification. There are many tools which assist in capturing data transferred over the networks so that an attack or the malicious intent of the intrusions may be investigated. Similarly, various network forensic frameworks are proposed in the literature.

Terrorism, sadly, seems here to stay and to stay with a vengeance. It turns out that the United States was not prepared for it and now must play catch-up. In doing so, even agreement on how to define terrorism is in doubt and what to do about it seems beyond comprehension at the moment. This volume presents a broad cross section of analyses of weaknesses and actions in the ongoing battle including cyberterrorism, international terrorism, and societal implications of terrorism.

Presents information on getting the most out of a PC's hardware and software, covering such topics as upgrading the BIOS, configuring the hard drive, installing more RAM, improving CPU performance, and adding COM ports.

This handbook reveals those aspects of hacking least understood by network administrators. It analyzes subjects through a hacking/security dichotomy that details hacking maneuvers and defenses in the same context. Chapters are organized around specific components and tasks, providing theoretical background that prepares network defenders for the always-changing tools and techniques of intruders. Part I introduces programming, protocol, and attack concepts. Part II addresses subject areas (protocols, services, technologies, etc.) that may be vulnerable. Part III details consolidation activities that hackers may use following penetration.

Communications represent a strategic sector for privacy protection and for personal, company, national and international security. The interception, damage or lost of information during communication can generate material and non material economic damages from both a personal and collective point of view. The purpose of this book is to give the reader information relating to all aspects of communications security, beginning at the base ideas and building to reach the most advanced and updated concepts. The book will be of interest to integrated system designers, telecommunication designers, system engineers, system analysts, security managers, technicians, intelligence personnel, security personnel, police, army, private investigators, scientists, graduate and postgraduate students and anyone that needs to communicate in a secure way.

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

Are You Looking To Learn About Hacking & Information Security? Have You Ever Wanted To Be a Hacker? Are You Tired Of The Overly Complicated Hacking Books? Yes, you can learn everything you need to know to dominate and ensure the skills needed to hack! Even if you've never hacked, coded, or operated a computer before! "Hacking: The Hacking For Beginners Guide To Computer Hacking, How To Hack And Basic Security" itself contains actual step-by-step techniques and guides to simplify the programming process. In order to prevent your system from being compromised, you need to stay a step ahead of any criminal hacker. You can do that by learning how to hack and how to do a counter-hack. This book contains proven steps and strategies on how to hack and make sure that you maintain a high level of security. Here Is What You'll Learn About... Basics of Hacking For the Good Hackers Programming Language Types of Hacking Putting Hacking into Action Hacking on Your Own (Includes Wireless Hacking) You will know exactly what it is hackers do when you reach the end of this book, as well as how you, too, can get started on the right track to become a hacker yourself! What makes this hacking book different

from other hacking books you might ask? Most of the hacking books provide a holistic view of everything that is entailed in hacking, explaining both the negative side of hacking and the positive side. The details that are discussed in this book include how to acquire the right ethical hacking skills, and how to then develop these skills over a period of time. It doesn't matter what you have heard, or what you think you know. If you have been searching for reliable, legal and ethical information on how to become a hacker, then you are at the right place. Purchase "Hacking: The Hacking For Beginners Guide To Computer Hacking, How To Hack And Basic Security" right away and open yourself up to a whole new world of possibilities!

Coding for Penetration Testers: Building Better Tools, Second Edition provides readers with an understanding of the scripting languages that are commonly used when developing tools for penetration testing, also guiding users 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 book presents real--world scenarios and tool development that can be incorporated into a tester's toolkit. This completely updated edition focuses on an expanded discussion on the use of Powershell, and includes practical updates to all tools and coverage. Discusses the use of various scripting languages in penetration testing Presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages Provides a primer on scripting, including, but not limited to, web scripting, scanner scripting, and exploitation scripting Includes all-new coverage of Powershell

This book describes open source tools commonly used in network administration. Open source tools are a popular choice for network administration because they are a good fit for many organizations. This volume brings together a collection of these tools in a single reference for the networkadministrator.

Bill Gates recently told Wired that if he were a teenager today, he would be hacking biology. "If you want to change the world in some big way," he says, "that's where you should start-biological molecules." The most disruptive force on the planet resides in DNA. Biotech companies and academic researchers are just beginning to unlock the potential of piecing together life from scratch. Champions of synthetic biology believe that turning genetic code into Lego-like blocks to build never-before-seen organisms could solve the thorniest challenges in medicine, energy, and environmental protection. But as the hackers who cracked open the potential of the personal computer and the Internet proved, the most revolutionary discoveries often emerge from out--of-the-way places, forged by brilliant outsiders with few resources besides boundless energy and great ideas. In Biopunk, Marcus Wohlsen chronicles a growing community of DIY scientists working outside the walls of corporations and universities who are committed to democratizing DNA the way the Internet did information. The "biohacking" movement, now in its early, heady days, aims to unleash an outbreak of genetically modified innovation by making the tools and techniques of biotechnology accessible to everyone. Borrowing their ideal-

ism from the worlds of open-source software, artisinal food, Internet startups, and the Peace Corps, biopunks are devoted advocates for open--sourcing the basic code of life. They believe in the power of individuals with access to DNA to solve the world's biggest problems. You'll meet a new breed of hackers who aren't afraid to get their hands wet, from entrepreneurs who aim to bring DNA-based medical tools to the poorest of the poor to a curious tinkerer who believes a tub of yogurt and a jellyfish gene could protect the world's food supply. These biohackers include: -A duo who started a cancer drug company in their kitchen -A team who built an open--source DNA copy machine -A woman who developed a genetic test in her apartment for a deadly disease that had stricken her family Along with the potential of citizen science to bring about disruptive change, Wohlsen explores the risks of DIY bioterrorism, the possibility of genetic engineering experiments gone awry, and whether the ability to design life from scratch on a laptop might come sooner than we think.

This book will teach you how you can protect yourself from most common hacking attacks - by knowing how hacking actually works! After all, in order to prevent your system from being compromised, you need to stay a step ahead of any criminal hacker. You can do that by learning how to hack and how to do a counter-hack. In this hacking for beginners book, you will discover: - Active Attacks - Masquerade Attacks - Replay Attacks - Modification of Messages - Denial of Service or DoS - Spoofing Techniques - Mobile Hacking And so much more! Get this book NOW. Hacking is real, and many people know how to do it. You can protect yourself from cyber attacks by being informed and learning how to secure your computer and other devices.

Describes various types of malware, including viruses, worms, user-level RootKits, and kernel-level manipulation, their haracteristics and attack method, and how to defend against an attack.

Presents information on how to analyze risks to your networks and the steps needed to select and deploy the appropriate countermeasures to reduce your exposure to physical and network threats. Also imparts the skills and knowledge needed to identify and counter some fundamental security risks and requirements, including Internet security threats and measures (audit trails IP sniffing/spoofing etc.) and how to implement security policies and procedures. In addition, this book covers security and network design with respect to particular vulnerabilities and threats. It also covers risk assessment and mitigation and auditing and testing of security systems as well as application standards and technologies required to build secure VPNs, configure client software and server operating systems, IPsec-enabled routers, firewalls and SSL clients. This comprehensive book will provide essential knowledge and skills needed to select, design and deploy a public key infrastructure (PKI) to secure existing and future applications. * Chapters contributed by leaders in the field cover theory and practice of computer security technology, allowing the reader to develop a new level of technical expertise * Comprehensive and up-to-date coverage of security issues facilitates learning and allows the reader to remain current and fully informed from multiple

viewpoints * Presents methods of analysis and problem-solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions
Denial-of-service attacks are one of the most severe challenges confronting the online world. This ground-breaking volume discusses a new method of countering denial-of-service attacks called hop integrity. It details a suite of protocols for providing hop integrity. In particular, each protocol in this suite is specified and verified using an abstract and formal notation, called the Secure Protocol Notation. In addition, the book presents an alternative way to achieve strong hop integrity with hard sequence numbers.

Presents a collection of tips and techniques for getting the most out of eBay.
This book helps people find sensitive information on the Web. Google is one of the 5 most popular sites on the internet with more than 380 million unique users per month (Nielsen/NetRatings 8/05). But, Google's search capabilities are so powerful, they sometimes discover content that no one ever intended to be publicly available on the Web including: social security numbers, credit card numbers, trade secrets, and federally classified documents. Google Hacking for Penetration Testers Volume 2 shows the art of manipulating Google used by security professionals and system administrators to find this sensitive information and "self-police their own organizations. Readers will learn how Google Maps and Google Earth provide pinpoint military accuracy, see how bad guys can manipulate Google to create super worms, and see how they can "mash up" Google with MySpace, LinkedIn, and more for passive reconaissance. • Learn Google Searching Basics Explore Google's Web-based Interface, build Google queries, and work with Google URLs. • Use Advanced Operators to Perform Advanced Queries Combine advanced operators and learn about colliding operators and bad search-fu. • Learn the Ways of the Google Hacker See how to use caches for anonymity and review directory listings and traversal techniques. • Review Document Grinding and Database Digging See the ways to use Google to locate documents and then search within the documents to locate information. • Understand Google's Part in an Information Collection Framework Learn the principles of automating searches and the applications of data mining. • Locate Exploits and Finding Targets Locate exploit code and then vulnerable targets. • See Ten Simple Security Searches Learn a few searches that give good results just about every time and are good for a security assessment. • Track Down Web Servers Locate and profile web servers, login portals, network hardware and utilities. • See How Bad Guys Troll for Data Find ways to search for usernames, passwords, credit card numbers, social security numbers, and other juicy information. • Hack Google Services Learn more about the AJAX Search API, Calendar, Blogger, Blog Search, and more.
This volume constitutes the proceedings of the Third European Symposium on Research in Computer Security, held in Brighton, UK in November 1994. The 26 papers presented in the book in revised versions were carefully selected from a total of 79 submissions; they cover many current aspects of computer securi-

ty research and advanced applications. The papers are grouped in sections on high security assurance software, key management, authentication, digital payment, distributed systems, access control, databases, and measures.

Network and System Security provides focused coverage of network and system security technologies. It explores practical solutions to a wide range of network and systems security issues. Chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Coverage includes building a secure organization, cryptography, system intrusion, UNIX and Linux security, Internet security, intranet security, LAN security; wireless network security, cellular network security, RFID security, and more. Chapters contributed by leaders in the field covering foundational and practical aspects of system and network security, providing a new level of technical expertise not found elsewhere Comprehensive and updated coverage of the subject area allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

Presents theories and models associated with information privacy and safeguard practices to help anchor and guide the development of technologies, standards, and best practices. Provides recent, comprehensive coverage of all issues related to information security and ethics, as well as the opportunities, future challenges, and emerging trends related to this subject.

"Digital forensics is the science of collecting the evidence that can be used in a court of law to prosecute the individuals who engage in electronic crime"--Provided by publisher.

Computer security touches every part of our daily lives from our computers and connected devices to the wireless signals around us. Breaches have real and immediate financial, privacy, and safety consequences. This handbook has compiled advice from top professionals working in the real world about how to minimize the possibility of computer security breaches in your systems. Written for professionals and college students, it provides comprehensive best guidance about how to minimize hacking, fraud, human error, the effects of natural disasters, and more. This essential and highly-regarded reference maintains timeless lessons and is fully revised and updated with current information on security issues for social networks, cloud computing, virtualization, and more.

Empowers network and system administrators to defend their information and computing assets. This guide presents explanations of destructive hacker tools and tactics - and specific counter measures for both UNIX and Windows environments. It provides information about how hackers build elegant attacks from simple building blocks, and more.

With more than a million dedicated programmers, Perl has proven to be the best computing language for the latest trends in computing and business. While other languages have stagnated, Perl remains fresh, thanks to its community-based development model, which encourages the sharing of information among users. This tradition of knowl-

edge-sharing allows developers to find answers to almost any Perl question they can dream up. And you can find many of those answers right here in Perl Hacks. Like all books in O'Reilly's Hacks Series, Perl Hacks appeals to a variety of programmers, whether you're an experienced developer or a dabbler who simply enjoys exploring technology. Each hack is a short lesson--some are practical exercises that teach you essential skills, while others merely illustrate some of the fun things that Perl can do. Most hacks have two parts: a direct answer to the immediate problem you need to solve right now and a deeper, subtler technique that you can adapt to other situations. Learn how to add CPAN shortcuts to the Firefox web browser, read files backwards, write graphical games in Perl, and much more. For your convenience, Perl Hacks is divided by topic--not according toany sense of relative difficulty--so you can skip around and stop at any hack you like. Chapters include: Productivity Hacks User Interaction Data Munging Working with Modules Object Hacks Debugging Whether you're a newcomer or an expert, you'll find great value in Perl Hacks, the only Perl guide that offers somethinguseful and fun for everyone.

This guide empowers network and system administrators to defend their information and computing assets--whether or not they have security experience. Skoudis presents comprehensive, insider's explanations of today's most destructive hacker tools and tactics, and specific, proven countermeasures for both UNIX and Windows environments.

This book provides an in-depth exploration of the phenomenon of hacking from a multidisciplinary perspective that addresses the social and technological aspects of this unique activity as well as its impact. • Documents how computer hacking fits into various forms of cybercrime • Describes the subculture of computer hackers and explains how this social world plays an integral role in the business of hacking • Clarifies the subtle differences between ethical and malicious hacks • Focuses on the non-technical aspects of computer hacking to enable the reader to better understand the actors and their motives

This book provides a concise yet comprehensive overview of computer and Internet security, suitable for a one-term introductory course for junior/senior undergrad or first-year graduate students. It is also suitable for self-study by anyone seeking a solid footing in security – including software developers and computing professionals, technical managers and government staff. An overriding focus is on brevity, without sacrificing breadth of core topics or technical detail within them. The aim is to enable a broad understanding in roughly 350 pages. Further prioritization is supported by designating as optional selected content within this. Fundamental academic concepts are reinforced by specifics and examples, and related to applied problems and real-world incidents. The first chapter provides a gentle overview and 20 design principles for security. The ten chapters that follow provide a framework for understanding computer and Internet security. They regularly refer back to the principles, with supporting examples. These principles are the conceptual counterparts of security-related error patterns that have been recurring in software and system designs for over 50 years. The book is “elementary”

in that it assumes no background in security, but unlike “soft” high-level texts it does not avoid low-level details, instead it selectively dives into fine points for exemplary topics to concretely illustrate concepts and principles. The book is rigorous in the sense of being technically sound, but avoids both mathematical proofs and lengthy source-code examples that typically make books inaccessible to general audiences. Knowledge of elementary operating system and networking concepts is helpful, but review sections summarize the essential background. For graduate students, inline exercises and supplemental references provided in per-chapter endnotes provide a bridge to further topics and a springboard to the research literature; for those in industry and government, pointers are provided to helpful surveys and relevant standards, e.g., documents from the Internet Engineering Task Force (IETF), and the U.S. National Institute of Standards and Technology.

Research on Internet security over the past few decades has focused mainly on information assurance, issues of data confidentiality and integrity as explored through cryptograph algorithms, digital signature, authentication code, etc. Unlike other books on network information security, Network Infrastructure Security addresses the emerging concern with better detecting and preventing routers and other network devices from being attacked or compromised. Network Infrastructure Security bridges the gap between the study of the traffic flow of networks and the study of the actual network configuration. This book makes effective use of examples and figures to illustrate network infrastructure attacks from a theoretical point of view. The book includes conceptual examples that show how network attacks can be run, along with appropriate countermeasures and solutions.

Presents a collection of tips and techniques for getting the most out of Amazon.com, covering such topics as browsing and searching, community features, selling through Amazon, and Amazon Web services.

"I finally get it! I used to hear words like rootkit, buffer overflow, and idle scanning, and they just didn't make any sense. I asked other people and they didn't seem to know how these things work, or at least they couldn't explain them in a way that I could understand. Counter Hack Reloaded is the clearest explanation of these tools I have ever seen. Thank you!"--Stephen Northcutt, CEO, SANS Institute "Ed Skoudis does it again! With this new edition, Ed takes a phenomenal work to the next level! This book is a 'must-have' and a 'must-read' for anyone remotely associated with computers and computer security." -Harlan Carvey, CISSP, author of Windows Forensics and Incident Recovery "Ed Skoudis is a rare individual. He knows the innards of all the various systems, knows all the latest exploits and defenses, and yet is able to explain everything at just the right level. The first edition of Counter Hack was a fascinating read. It's technically intriguing and very clear. ... A book on vulnerabilities, though, will get out of date, and so we definitely needed this updated and significantly rewritten second edition. This book is a wonderful overview of the field." -From the Foreword by Radia Perlman, series editor, The Radia Perlman Series in Computer Networking and Security; author of Interconnections ;

and coauthor of Network Security: Private Communications in a Public World "What a great partnership! Ed Skoudis and Tom Liston share an uncanny talent for explaining even the most challenging security concepts in a clear and enjoyable manner. Counter Hack Reloaded is an indispensable resource for those who want to improve their defenses and understand the mechanics of computer attacks." -Lenny Zeltser, coauthor of Malware: Fighting Malicious Code "Ed Skoudis does it again! With this new edition, Ed takes a phenomenal work to the next level! This book is a 'must-have' and a 'must-read' for anyone remotely associated with computers and computer security." -Harlan Carvey, CISSP, author of Windows Forensics and Incident Recovery "In addition to having breadth of knowledge about and probing insights into network security, Ed Skoudis's real strength is in his ability to show complex topics in an understandable form. By the time he's done, what started off as a hopeless conglomeration of acronyms starts to sound comfortable and familiar. This book is your best source for understanding attack strategies, attack tools, and the defenses against bot ...

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.