

The Shellcoders Handbook Discovering And Exploiting Security Holes By Anley Chris Published By Wiley 2nd Second Edition 2007 Paperback

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.

Assessing and Managing Security Risk in IT Systems: A Structured Methodology builds upon the original McCumber Cube model to offer proven processes that do not change, even as technology evolves. This book enables you to assess the security attributes of any information system and implement vastly improved security environments. Part I delivers an overview of information systems security, providing historical perspectives and explaining how to determine the value of information. This section offers the basic underpinnings of information security and concludes with an overview of the risk management process. Part II describes the McCumber Cube, providing the original paper from 1991 and detailing ways to accurately map information flow in computer and telecom systems. It also explains how to apply the methodology to individual system components and subsystems. Part III serves as a resource for analysts and security practitioners who want access to more detailed information on technical vulnerabilities and risk assessment analytics. McCumber details how information extracted from this resource can be applied to his assessment processes. See your app through a hacker's eyes to find the real sources of vulnerability The Mobile Application Hacker's Handbook is a comprehensive guide to securing all mobile applications by approaching the issue from a hacker's point of view. Heavily practical, this book provides expert guidance toward discovering and exploiting flaws in mobile applications by approaching the issue from a hacker's perspective and defending against these attacks for the software developer.

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

Preparing for the Day When Quantum Computing Breaks Today's Cryptography

The Hacker's Handbook

Practical Reverse Engineering

Attacking Network Protocols

A Structured Methodology

Essential COM

Modern cars are more computerized than ever. Infotainment and navigation systems, Wi-Fi, automatic software updates, and other innovations aim to make driving more convenient. But vehicle technologies haven't kept pace with today's more hostile security environment, leaving millions vulnerable to attack. The Car Hacker's Handbook will give you a deeper understanding of the computer systems and embedded software in modern vehicles. It begins by examining vulnerabilities and providing detailed explanations of communications over the CAN bus and betwee devices and systems. Then, once you have an understanding of a vehicle's communication network, you'll learn how to intercept data and perform specific hacks to track vehicles, unlock doors, glitch engines, flood communication, and more. With a focus on low-cost, open source hacking tools such as Metasploit, Wireshark, Kayak, can-utils, and ChipWhisperer, The Car Hacker's Handbook will show you how to -Build an accurate threat model for your vehicle -Reverse engineer the CAN bus to fake engine signals -Exploit vulnerabilities in diagnostic and data-tagging systems -Hack the ECU and other firmware and embedded systems -Seed exploits through infotainment and vehicle-to-vehicle communication systems -Override factory settings and performance-tuning techniques -Build physical and virtual test benches to try out exploits safely If you're curious about automotive security and have the urge to hack a two-ton computer, make The Car Hacker's Handbook your first stop.

WINNER OF THE FT & MCKINSEY BUSINESS BOOK OF THE YEAR AWARD 2021 The Instant New York Times bestseller A Financial Times and The Times Book of the Year 'A terrifying expose' The Times 'Part John le Carré... Spellbinding New Yorker' We plug in anything we can to the Internet. We can control our entire lives, economy and grid via a remote web control. But over the past decade, as this transformation took place, we never paused to think that we were also creating the world's largest attack surface. And that the same nation that maintains the greatest cyber advantage on earth could also be among its most vulnerable. Filled with spies, hackers, arms dealers and a few unsung heroes, This Is How They Tell Me the World Ends is an astonishing and gripping feat of journalism. Drawing on years of reporting and hundreds of interviews, Nicole Perloff litrfs the curtain on a market in shadow, revealing the urgent threat faced by us all if we cannot bring the global cyber arms race to heel.

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

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. The presentation 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 their 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.

Cryptography Apocalypse

Buffer Overflow Attacks

En

The Art of Software Security Assessment

Advanced Penetration Testing

Secrets of Reverse Engineering

The Web Application Hacker's Handbook: Finding And Exploiting Security Flaws, 2nd Ed

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.

Provides information on ways to break into and defend seven database servers, covering such topics as identifying vulnerabilities, how an attack is carried out, and how to stop an attack.

Beginning with a basic primer on reverse engineering—including computer internals, operating systems, and assembly language—and then discussing the various applications of reverse engineering, this book provides readers with practical, in-depth techniques for software reverse engineering. The book is broken into two parts, the first deals with security-related reverse engineering and the second explores the more practical aspects of reverse engineering. In addition, the author explains how to reverse engineer a third-party software library to improve interfacing and how to reverse engineer a competitor's software to build a better product. * The first popular book to show how software reverse engineering can help defend against security threats, speed up development, and unlock the secrets of competitive products * Helps developers plug security holes by demonstrating how hackers exploit reverse engineering techniques to crack copy-protection schemes and identify software targets for viruses and other malware * Offers a primer on advanced reverse-engineering, delving into "disassembly"—code-level reverse engineering—and explaining how to decipher assembly language

The first comprehensive guide to discovering and preventingattacks on the Android OS As the Android operating system continues to increase its shareof the smartphone market, smartphone hacking remains a growingthreat. Written by experts who rank among the world's foremostAndroid security researchers, this book presents vulnerabilitydiscovery, analysis, and exploitation tools for the good guys.Following a detailed explanation of how the Android OS works andits overall security architecture, the authors examine howvulnerabilities can be discovered and exploits developedfor various system components, preparing you to defendagainstthem. If you are a mobile device administrator, security researcher,Android app developer, or consultant responsible for evaluatingAndroid security, you will find this guide is essential to yourtoolbox. A crack team of leading Android security researchers explainAndroid security risks, security design and architecture, rooting,fuzz testing, and vulnerability analysis Covers Android application building blocks and security as wellas debugging and auditing Android apps Prepares mobile device administrators, security researchers,Android app developers, and security consultants to defend Androidsystems against attack Android Hacker's Handbook is the first comprehensiveresource for IT professionals charged with smartphonesecurity.

Reversing

Discovering and Exploiting Security Flaws

Detect, Exploit, Prevent

Attacking the Core

Penetration Testing with Shellcode

Identifying and Preventing Software Vulnerabilities

x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

The Metasploit Framework makes discovering, exploiting, and sharing vulnerabilities quick and relatively painless. But while Metasploit is used by security professionals everywhere, the tool can be hard to grasp for first-time users. Metasploit: The Penetration Tester's Guide fills this gap by teaching you how to harness the Framework and interact with the vibrant community of Metasploit contributors. Once you've built your foundation for penetration testing, you'll learn the Framework's conventions, interfaces, and module system as you launch simulated attacks. You'll move on to advanced penetration testing techniques, including network reconnaissance and enumeration, client-side attacks, wireless attacks, and targeted social-engineering attacks. Learn how to -Find and exploit unmaintained, misconfigured, and unpatched systems -Perform reconnaissance and find valuable information about your target -Bypass anti-virus technologies and circumvent security controls -Integrate Nmap, NeXpose, and Nessus with Metasploit to automate discovery -Use the Meterpreter shell to launch further attacks from inside the network -Harness standalone Metasploit utilities, third-party tools, and plug-ins -Learn how to write your own Meterpreter post exploitation modules and scripts You'll even touch on exploit discovery for zero-day research, write a fuzzer, port existing exploits into the Framework, and learn how to cover your tracks. Whether your goal is to secure your own networks or to put someone else's to the test, Metasploit: The Penetration Tester's Guide will take you there and beyond.

Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware is more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

A Guide to Kernel Exploitation: Attacking the Core discusses the theoretical techniques and approaches needed to develop reliable and effective kernel-level exploits, and applies them to different operating systems, namely, UNIX derivatives, Mac OS X, and Windows. Concepts and tactics are presented categorically so that even when a specifically detailed vulnerability has been patched, the foundational information provided will help hackers in writing a newer, better attack; or help pen testers, auditors, and the like develop a more concrete design and defensive structure. The book is organized into four parts. Part I introduces the kernel and sets out the theoretical basis on which to build the rest of the book. Part II focuses on different operating systems and describes exploits for them that target various bug classes. Part III on remote kernel exploitation analyzes the effects of the remote scenario and presents new techniques to target remote issues. It includes a step-by-step analysis of the development of a reliable, one-shot, remote exploit for a real vulnerabilitya bug affecting the SCTP subsystem found in the Linux kernel. Finally, Part IV wraps up the analysis on kernel exploitation and looks at what the future may hold. Covers a range of operating system families – UNIX derivatives, Mac OS X, Windows Details common scenarios such as generic memory corruption (stack overflow, heap overflow, etc.) issues, logical bugs and race conditions Delivers the reader from user-land exploitation to the world of kernel-land (OS) exploits/attacks, with a particular focus on the steps that lead to the creation of successful techniques, in order to give to the reader something more than just a set of tricks

Malware Data Science explains how to identify, analyze, and classify large-scale malware using machine learning and data visualization. Security has become a "big data" problem. The growth rate of malware has accelerated to tens of millions of new files per year while our networks generate an ever-larger flood of security-relevant data each day. In order to defend against these advanced attacks, you'll need to know how to think like a data scientist. In Malware Data Science, security data scientist Joshua Sox introduces machine learning, statistics, social network analysis, and data visualization, and shows you how to apply these methods to malware detection and analysis. You'll learn how to - Analyze malware using static analysis - Observe malware behavior using dynamic analysis - Identify adversary groups through shared code analysis - Catch 0-day vulnerabilities by building your own machine learning detector - Measure malware detector accuracy - Identify malware campaigns, trends, and relationships through data visualization Whether you're a malware analyst looking to add skills to your existing arsenal, or a data scientist interested in attack detection and threat intelligence, Malware Data Science will help you stay ahead of the curve.

The Antivirus Hacker's Handbook

Android Hacker's Handbook

The Art of Memory Forensics

The Mobile Application Hacker's Handbook

Secure Coding in C and C++

Sockets, Shellcode, Porting, and Coding: Reverse Engineering Exploits and Tool Coding for Security Professionals

The Non-coder's Guide to Technology and the Business Strategy Behind it

Discover all the security risks and exploits that can threateniOS-based mobile devices iOS is Apple's mobile operating system for the iPhone and iPad.With the introduction of iOS5, many security issues have come tolight. This book explains and discusses them all. The award-winningauthor, expert in Mac and iOS security, examines thevulnerabilities and the internals of iOS to show how attacks can be mitigated. The book explains how the operating system works, itsoverall security architecture, and the security risks associatedwith it, as well as exploits, rootkits, and other payloadsthat have been developed for it. Covers iOS security architecture, vulnerability hunting,exploit writing, and how iOS jailbreaks work Explores iOS enterprise and encryption, code signing and memoryprotection, sandboxing, iPhone fuzzing, exploitation, ROP payloads, and baseband attacks Also examines kernel debugging and exploitation Companion website includes source code and tools to facilitateyour efforts iOS Hacker's Handbook arms you with the tools needed to identify, understand, and foil iOS attacks.

Master Shellcode to leverage the buffer overflow concept Key Features Understand how systems can be bypassed both at the operating system and network level with shellcode, assembly, and Metasploit Learn to write and modify 64-bit shellcode along with kernel-level shellcode concepts A step-by-step guide that will take you from low-level security skills to covering loops with shellcode Book Description Security has always been a major concern for your application, your system, or your environment. This book's main goal is to build your skills for low-level security exploits, finding vulnerabilities and covering loopholes with shellcode, assembly, and Metasploit. This book will teach you topics ranging from memory management and assembly to compiling and extracting shellcode and using syscalls and dynamically locating functions in memory. This book also covers techniques to compile 64-bit shellcode for Linux and Windows along with Metasploit shellcode tools. Lastly, this book will also show you to how to write your own exploits with intermediate techniques, using real-world scenarios. By the end of this book, you will have become an expert in shellcode and will understand how systems are compromised both at the operating system and network level. What you will learn Extract an isolated lab to test and inject shellcodes (Windows and Linux). Understand both Windows and Linux behavior. Learn the assembly programming language. Create shellcode using assembly and Metasploit. Detect buffer overflows. Debug and reverse-engineer using tools such as GDB, edb, and Immunity (Windows and Linux). Exploit development and shellcodes injections (Windows & Linux). Prevent and protect against buffer overflows and heap corruption. Who this book is for This book is intended to be read by penetration testers, malware analysts, security researchers, forensic practitioners, exploit developers, C language programmers, software testers, and students in the security field. Readers should have a basic understanding of OS internals (Windows and Linux). Some knowledge of the C programming language is essential, and a familiarity with the Python language would be helpful.

The Definitive Insider 's Guide to Auditing Software Security This is one of the most detailed, sophisticated, and useful guides to software security auditing ever written. The authors are leading security consultants and researchers who have personally uncovered vulnerabilities in applications ranging from sendmail to Microsoft Exchange, Check Point VPN to Internet Explorer. Drawing on their extraordinary experience, they introduce a start-to-finish methodology for " ripping apart " applications to reveal even the most subtle and well-hidden security flaws. The Art of Software Security Assessment covers the full spectrum of software vulnerabilities in both UNIX/Linux and Windows environments. It demonstrates how to audit security in applications of all sizes and functions, including network and Web software. Moreover, it teaches using extensive examples of real code drawn from past flaws in many of the industry's highest-profile applications. Coverage includes • Code auditing: theory, practice, proven methodologies, and secrets of the trade • Bridging the gap between secure software design and post-implementation review • Performing architectural assessment: design review, threat modeling, and operational review • Identifying vulnerabilities related to memory management, data types, and malformed data • UNIX/Linux assessment: privileges, files, and processes • Windows-specific issues, including objects and the filesystem • Auditing interprocess communication, synchronization, and state • Evaluating network software: IP stacks, firewalls, and common application protocols • Auditing Web applications and technologies

As more and more vulnerabilities are found in the Mac OS X (Leopard) operating system, security researchers are realizing the importance of developing proof-of-concept exploits for those vulnerabilities. This unique tome is the first book to uncover the flaws in the Mac OS X operating system—and how to deal with them. Written by two white hat hackers, this book is aimed at making vital information known so that you can find ways to secure your Mac OS X systems, and examines the sorts of attacks that are prevented by Leopard ' s security defenses, what attacks aren ' t, and how to best handle those weaknesses.

A Hands-On Introduction to Hacking

The Database Hacker's Handbook

The Car Hacker's Handbook

A Guide for the Penetration Tester

Creating and Automating Security Tools

Exploiting Software: How To Break Code

The Windows 2000 Device Driver Book

Analyzing how hacks are done, so as to stop them in thefuture Reverse engineering is the process of analyzing hardware orsoftware and understanding it, without having access to the sourcecode or design documents. Hackers are able to reverse engineer'systems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. PracticalReverse Engineering goes under the hood of reverse engineeringfor security analysts, security engineers, and system programmers,so they can learn how to use these same processes to stop hackersin their tracks. The book covers x86, x64, and ARM (the first book to cover allthree); Windows kernel-mode code rootkits and drivers; virtualmachine protection techniques; and much more. Best of all, itoffers a systematic approach to the material, with plenty ofhands-on exercises and real-world examples. Offers a systematic approach to understanding reverseengineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architecturesas well as defobfuscation and virtual machine protectiontechniques Provides special coverage of Windows kernel-mode code(rootkits/drivers), a topic not often covered elsewhere, andexplains how to analyze drivers step by step Demystifies topics that have a steep learning curve Includes a bonus chapter on reverse engineering tools Practical Reverse Engineering: Using x86, x64, ARM, WindowsKernel, and Reversing Tools provides crucial, up-to-dateguidance for a broad range of IT professionals.

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. An authoritative guide to Windows NT driver development, now completely revised and updated. The CD-ROM includes all source code, plus Microsoft hardware standards documents, demo software, and more.

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 Enterecept, 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

The Shellcoder's Handbook

Hacking: The art Of Exploitation

Winner of the FT & McKinsey Business Book of the Year Award 2021

The Browser Hacker's Handbook

Attack Detection and Attribution

Hacking the World's Most Secure Networks

A Guide for Programmers

"The security of information systems has not improved at a rate consistent with the growth and sophistication of the attacks being made against them. To address this problem, we must improve the underlying strategies and techniques used to create our systems. Specifically, we must build security in from the start, rather than append it as an afterthought. That's the point of Secure Coding in C and C++. In careful detail, this book shows software developers how to build high-quality systems that are less vulnerable to costly and even catastrophic attack. It's a book that every developer should read before the start of any serious project." –Frank Abagnale, author, lecturer, and leading consultant on fraud prevention and secure documents Learn the Root Causes of Software Vulnerabilities and How to Avoid Them Commonly exploited software vulnerabilities are usually caused by avoidable software defects. Having analyzed nearly 18,000 vulnerability reports over the past ten years, the CERT/Coordination Center (CERT/CC) has determined that a relatively small number of root causes account for most of them. This book identifies and explains these causes and shows the steps that can be taken to prevent exploitation. Moreover, this book encourages programmers to adopt security best practices and develop a security mindset that can help protect software from tomorrow's attacks, not just today's. Drawing on the CERT/CC's reports and conclusions, Robert Seacord systematically identifies the program errors most likely to lead to security breaches, shows how they can be exploited, reviews the potential consequences, and presents secure alternatives. Coverage includes technical detail on how to improve the overall security of any C/C++ application Thwart buffer overflows and stack-smashing attacks that exploit insecure string manipulation logic Avoid vulnerabilities and security flaws resulting from the incorrect use of dynamic memory management functions Eliminate integer-related problems: integer overflows, sign errors, and truncation errors Correctly use formatted output functions without introducing format-string vulnerabilities Avoid I/O vulnerabilities, including race conditions Secure Coding in C and C++ presents hundreds of examples of secure code, insecure code, and exploits, implemented for Windows and Linux. If you're responsible for creating secure C or C++ software—or for keeping it safe—no other book offers you this much detailed, expert assistance.

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker's tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus No source code? No problem. With IDA Pro, the interactive disassembler, you live in a source code-optimal world. IDA can automatically analyze the millions of opcodes that make up an executable and present you with a disassembler. But at that point, your work is just beginning. With The IDA Pro Book, you'll learn how to turn that mountain of mnemonics into something you can actually use. Hailed by the creator of IDA Pro as "profound, comprehensive, and accurate," the second edition of The IDA Pro Book covers everything from the very first steps to advanced automation techniques. You'll find complete coverage of IDA's new QT-based user interface, as well as increased coverage of the IDA debugger, the Bochs debugger, and IDA scripting (especially using IDAPython). But because humans are still smarter than computers, you'll even learn how to use IDA's latest interactive and scriptable interfaces to your advantage. Save time and effort as you learn to :INavigate, comment, and modify disassembly IIdentify known library routines, so you can focus your analysis on other areas of the code iUse code graphing to quickly make sense of cross references and function calls iExtend IDA to support new processors and filetypes using the SDK iExplore popular plug-ins that make writing IDA scripts easier, allow collaborative reverse engineering, and much more iUse IDA's built-in debugger to tackle hostile and obfuscated code Whether you're analyzing malware, conducting vulnerability research, or reverse engineering software, a mastery of IDA is crucial to your success. Take your skills to the next level with this 2nd edition of The IDA Pro Book.

WANT A NON-CODING JOB AT A TECH COMPANY? Interested in product management, marketing, strategy, or business development? The tech industry is the place to be: nontechnical employees at tech companies outnumber their engineering counterparts almost 3 to 1 (Forbes, 2017). You might be worried that your lack of coding skills or tech industry knowledge will hold you back. But here's the secret: you don't need to learn how to code to break into the tech industry. Written by three former Microsoft PMs, Swipe to Unlock gives you a breakdown of the concepts you need to know to crush your interviews, like software development, big data, and internet security. We'll explain how Google's ad targeting algorithm works, but Google probably won't ask you how to code to increase ad revenue from a particular market segment. And if you know how Google's ad platform works, you'll be in a far stronger position to come up with good growth strategies. We'll show you how Robinhood, an app that lets you trade stocks without commission, makes money by earning interest on the user's keep in their accounts. No one will ask you to explain this. But if someone asks you to come up with a new monetization strategy for Venmo (which lets you send and receive money without fees), you could pull out the Robinhood anecdote to propose that Venmo earn interest off the money sitting in users' accounts. We'll talk about some business cases like why Microsoft acquired LinkedIn. Microsoft interviewers probably won't ask you about the motive for the purchase, but they might ask you for ideas to improve Microsoft Outlook. From our case study, you'll learn how the Microsoft and LinkedIn ecosystems could work together, which can help you craft creative, impactful answers. You could propose that Outlook use LinkedIn's social graph to give salespeople insights about clients before meeting them. Or you could suggest linking Outlook's organizational tree to LinkedIn to let HR managers analyze their company's hierarchy and figure out what kind of talent they need to add. (We'll further explore both ideas in the book.) Either way, you're sure to impress. Learn the most know concepts of tech from authors who have received job offers for Facebook's Rotational Product Manager, Google's Associate Product Marketing Manager, and Microsoft's Program Manager to get a competitive edge at your interviews!

This Is How They Tell Me the World Ends

The Mac Hacker's Handbook

Shellcoder's Programming Uncovered (Uncovered series)

Defending Database Servers

The IDA Pro Book, 2nd Edition

A Hacker's Guide to Capture, Analysis, and Exploitation

Violent Python

Shows developers how COM operates and how to use it to create efficient and stable programs consistent with the COM philosophy, allowing disparate applications and components to work together across a variety of languages, platforms, and host machines. Original. (Advanced.)

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 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 wide 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 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.

Hack your antivirus software to stamp out future vulnerabilities The Antivirus Hacker's Handbook guides you through the process of reverse engineering antivirus software. You explore how to detect and exploit vulnerabilities that can be leveraged to improve future software design, protect your network, and anticipate attacks that may sneak through your antivirus' line of defense. You'll begin building your knowledge by diving into the reverse engineering process, which details how to start from a finished antivirus and then key elements of the concepts you need to know to crush your interviews, like software development, big data, and internet security. We'll explain how Google's ad targeting algorithm works, but Google probably won't ask you how to code to increase ad revenue from a particular market segment. And if you know how Google's ad platform works, you'll be in a far stronger position to come up with good growth strategies. We'll show you how Robinhood, an app that lets you trade stocks without commission, makes money by earning interest on the user's keep in their accounts. No one will ask you to explain this. But if someone asks you to come up with a new monetization strategy for Venmo (which lets you send and receive money without fees), you could pull out the Robinhood anecdote to propose that Venmo earn interest off the money sitting in users' accounts. We'll talk about some business cases like why Microsoft acquired LinkedIn. Microsoft interviewers probably won't ask you about the motive for the purchase, but they might ask you for ideas to improve Microsoft Outlook. From our case study, you'll learn how the Microsoft and LinkedIn ecosystems could work together, which can help you craft creative, impactful answers. You could propose that Outlook use LinkedIn's social graph to give salespeople insights about clients before meeting them. Or you could suggest linking Outlook's organizational tree to LinkedIn to let HR managers analyze their company's hierarchy and figure out what kind of talent they need to add. (We'll further explore both ideas in the book.) Either way, you're sure to impress. Learn the most know concepts of tech from authors who have received job offers for Facebook's Rotational Product Manager, Google's Associate Product Marketing Manager, and Microsoft's Program Manager to get a competitive edge at your interviews!

Assembly languages are

Malware Data Science
Discovering and Exploiting Security Holes
Penetration Testing
A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
Gray Hat C#

The Web Application Hacker's Handbook

A Guide to Kernel Exploitation

Hackers exploit browser vulnerabilities to attack deep within networks. The Browser Hacker's Handbook gives a practical understanding of hacking the everyday web browser and using it as a beachhead 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 of current attack methods. The web browser has become the most popular and widely used computer "program" in the world. As the gateway to the Internet, it is part of the storefront to any business that operates online, but it is also one of the most vulnerable entry points of any system. With attacks on the rise, companies are increasingly employing browser-hardening techniques to protect the unique vulnerabilities inherent in all currently used browsers. The Browser Hacker's Handbook thoroughly covers complex security issues and explores relevant topics such as: Bypassing the Same Origin Policy, ARP spoofing, social engineering, and phishing to access browsers; DNS tunneling, attacking web applications, and proxying—all from the browser; Exploiting the browser and its ecosystem (plugins and extensions); Cross-origin attacks, including Inter-protocol Communication and Exploitation. The Browser Hacker's Handbook is written with a professional security engagement in mind. Leveraging browsers as pivot points into a target's network should form an integral component into any social engineering or red-team security assessment. This handbook provides a complete methodology to understand and structure your next browser penetration test.

*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 every 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 platform. This technique is known as porting and is incredibly 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.*

Will your organization be protected the day a quantum computer breaks encryption on the internet? Computer encryption is vital for protecting users, data, and infrastructure in the digital age. Using traditional computing, even common desktop encryption could take decades for specialized 'crackers' to break and government and infrastructure-grade encryption would take billions of times longer. In light of these facts, it may seem that today's computer cryptography is a rock-solid way to safeguard everything from online passwords to the backbone of the entire internet. Unfortunately, many current cryptographic methods will soon be obsolete. In 2016, the National Institute of Standards and Technology (NIST) predicted that quantum computers will soon be able to break the most popular forms of public key cryptography. The encryption technologies we rely on every day—HTTPS, TLS, WiFi protection, VPNs, cryptocurrencies, PKI, digital certificates, smartcards, and most two-factor authentication—will be virtually useless. . . unless you prepare. Cryptography Apocalypse is a crucial resource for every IT and InfoSec professional for preparing for the coming quantum-computing revolution. Post-quantum crypto algorithms are already a reality, but implementation will take significant time and computing power. This practical guide helps IT leaders and implementers make the appropriate decisions today to meet the challenges of tomorrow. This important book: Gives a simple quantum mechanics primer Explains how quantum computing will break current cryptography Offers practical advice for preparing for a post-quantum world Presents the latest information on new cryptographic methods Describes the appropriate steps leaders must take to implement existing solutions to guard against quantum-computer security threats Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto is a must-have guide for anyone in the InfoSec world who needs to know if their security is ready for the day crypto break and how to fix it.

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.

Swipe to Unlock

The Penetration Tester's Guide

Assessing and Managing Security Risk in IT Systems

The Strategy Behind Breaking into and Defending Networks

iOS Hacker's Handbook

Metasploit