

Hacking Exposed Malware Rootkits Security Secrets And Solutions Second Edition

Security Secrets And Solutions Second Edition

Thank you definitely much for downloading **hacking exposed malware rootkits security secrets and solutions second edition security secrets and solutions second edition**. Maybe you have knowledge that, people have look numerous time for their favorite books later than this hacking exposed malware rootkits security secrets and solutions second edition security secrets and solutions second edition, but stop in the works in harmful downloads.

Rather than enjoying a good PDF past a cup of coffee in the afternoon, then again they juggled taking into consideration some harmful virus inside their computer. **hacking exposed malware rootkits security secrets and solutions second edition security secrets and solutions second edition** is friendly in our digital library an online admission to it is set as public suitably you can download it instantly. Our digital library saves in combined countries, allowing you to acquire the most less latency epoch to download any of our books behind this one. Merely said, the hacking exposed malware rootkits security secrets and solutions second edition security secrets and solutions second edition is universally compatible similar to any devices to read.

Rootkits and Bootkits Alex Matrosov
2019-05-07

Rootkits and Bootkits will teach you how to understand and counter sophisticated, advanced threats buried deep in a machine's boot process or UEFI firmware. With the aid of numerous case studies and professional research from three of the world's leading security experts, you'll trace malware development over time from rootkits like TDL3 to present-day UEFI implants and examine how they infect a system, persist through reboot, and evade security software. As you inspect and dissect real malware, you'll learn:

- How Windows boots—including 32-bit, 64-bit, and UEFI mode—and where to find vulnerabilities
- The details of boot process security mechanisms like Secure Boot, including an overview of Virtual Secure Mode (VSM) and Device Guard
- Reverse engineering and forensic techniques for analyzing real malware, including bootkits like Rovnix/Carberp, Gapz, TDL4, and the infamous rootkits TDL3 and Festi
- How to perform static and dynamic analysis using emulation and tools like Bochs and IDA Pro
- How to better

understand the delivery stage of threats against BIOS and UEFI firmware in order to create detection capabilities

- How to use virtualization tools like VMware Workstation to reverse engineer bootkits and the Intel Chipsec tool to dig into forensic analysis

Cybercrime syndicates and malicious actors will continue to write ever more persistent and covert attacks, but the game is not lost. Explore the cutting edge of malware analysis with *Rootkits and Bootkits*. Covers boot processes for Windows 32-bit and 64-bit operating systems.

Internet Forensics Robert Jones 2005-10-07
Because it's so large and unregulated, the Internet is a fertile breeding ground for all kinds of scams and schemes. Usually it's your credit card number they're after, and they won't stop there. Not just mere annoyances, these scams are real crimes, with real victims. Now, thanks to *Internet Forensics* from O'Reilly, there's something you can do about it. This practical guide to defending against Internet fraud gives you the skills you need to uncover the origins of the spammers, con artists, and identity thieves that plague the Internet. Targeted primarily at

the developer community, Internet Forensics shows you how to extract the information that lies hidden in every email message, web page, and web server on the Internet. It describes the lengths the bad guys will go to cover their tracks, and offers tricks that you can use to see through their disguises. You'll also gain an understanding for how the Internet functions, and how spammers use these protocols to their devious advantage. The book is organized around the core technologies of the Internet--email, web sites, servers, and browsers. Chapters describe how these are used and abused and show you how information hidden in each of them can be revealed. Short examples illustrate all the major techniques that are discussed. The ethical and legal issues that arise in the uncovering of Internet abuse are also addressed. Not surprisingly, the audience for Internet Forensics is boundless. For developers, it's a serious foray into the world of Internet security; for weekend surfers fed up with spam, it's an entertaining and fun guide that lets them play amateur detective from the safe confines of their home or office.

Malware, Rootkits & Botnets: A Beginner's Guide - Christopher C. Elisan 2012-09-05

Security Smarts for the Self-Guided IT Professional Learn how to improve the security posture of your organization and defend against some of the most pervasive network attacks. Malware, Rootkits & Botnets: A Beginner's Guide explains the nature, sophistication, and danger of these risks and offers best practices for thwarting them. After reviewing the current threat landscape, the book describes the entire threat lifecycle, explaining how cybercriminals create, deploy, and manage the malware, rootkits, and botnets under their control. You'll learn proven techniques for identifying and mitigating these malicious attacks. Templates, checklists, and examples give you the hands-on help you need to get started protecting your network right away. Malware, Rootkits & Botnets: A Beginner's Guide features: Lingo--Common security terms defined so that you're in the know on the job IMHO--Frank and relevant opinions based on the author's years of industry experience Budget Note--Tips for getting security technologies and processes into your organization's budget In Actual Practice--

Exceptions to the rules of security explained in real-world contexts Your Plan--Customizable checklists you can use on the job now Into Action--Tips on how, why, and when to apply new skills and techniques at work *Hacking Exposed Windows 2000*- Joel Scambray 2001

*In the tradition of the wildly successful Hacking Exposed - the 2nd edition of which sold over 75,000 units in just four months.*Unique approach to topic--no other book contains both hacking techniques as well as concrete solutions on how to plug the security holes in a Windows 2000 network.*Authors have winning track record--written by the best-selling authors of Hacking Exposed who are key Windows 2000 security consultants at Microsoft*Includes case studies based on the authors' real experiences and also features the trademark Hacking series elements such as attacks, countermeasures, and risk ratings.

Beginning Ethical Hacking with Kali Linux Sanjib Sinha 2018-11-29

Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of Beginning Ethical Hacking with Kali Linux. With the theory out of the way, you'll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web server and acquire the skill to be anonymous . When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how SniffJoke prevents poisoning, how to analyze protocols with Wireshark, and using

sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will Learn Master common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as SniffJoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systems Who This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming.

Hacking Exposed - Joel Scambray 2003

Provides coverage of the security features in Windows Server 2003. This book is useful for network professionals working with a Windows Server 2003 and/or Windows XP system.

Practical Malware Analysis - Michael Sikorski 2012-02-01

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: -Set up a safe virtual environment to analyze malware -Quickly extract network signatures and host-based indicators -Use key analysis tools like IDA Pro, OllyDbg, and WinDbg -Overcome

malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques -Use your newfound knowledge of Windows internals for malware analysis -Develop a methodology for unpacking malware and get practical experience with five of the most popular packers -Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions - David Endler 2007

Sidestep VoIP Catastrophe the Foolproof Hacking Exposed Way "This book illuminates how remote users can probe, sniff, and modify your phones, phone switches, and networks that offer VoIP services. Most importantly, the authors offer solutions to mitigate the risk of deploying VoIP technologies." --Ron Gula, CTO of Tenable Network Security Block debilitating VoIP attacks by learning how to look at your network and devices through the eyes of the malicious intruder. Hacking Exposed VoIP shows you, step-by-step, how online criminals perform reconnaissance, gain access, steal data, and penetrate vulnerable systems. All hardware-specific and network-centered security issues are covered alongside detailed countermeasures, in-depth examples, and hands-on implementation techniques. Inside, you'll learn how to defend against the latest DoS, man-in-the-middle, call flooding, eavesdropping, VoIP fuzzing, signaling and audio manipulation, Voice SPAM/SPIT, and voice phishing attacks. Find out how hackers footprint, scan, enumerate, and pilfer VoIP networks and hardware Fortify Cisco, Avaya, and Asterisk systems Prevent DNS poisoning,

DHCP exhaustion, and ARP table manipulation
Thwart number harvesting, call pattern tracking,
and conversation eavesdropping Measure and
maintain VoIP network quality of service and
VoIP conversation quality Stop DoS and packet
flood-based attacks from disrupting SIP proxies
and phones Counter REGISTER hijacking,
INVITE flooding, and BYE call teardown attacks
Avoid insertion/mixing of malicious audio Learn
about voice SPAM/SPIT and how to prevent it
Defend against voice phishing and identity theft
scams

**Hacking Exposed Industrial Control
Systems: ICS and SCADA Security Secrets &
Solutions** - Clint Bodungen 2016-09-22

Learn to defend crucial ICS/SCADA
infrastructure from devastating attacks the
tried-and-true Hacking Exposed way This
practical guide reveals the powerful weapons
and devious methods cyber-terrorists use to
compromise the devices, applications, and
systems vital to oil and gas pipelines, electrical
grids, and nuclear refineries. Written in the
battle-tested Hacking Exposed style, the book
arms you with the skills and tools necessary to
defend against attacks that are debilitating—and
potentially deadly. Hacking Exposed Industrial
Control Systems: ICS and SCADA Security
Secrets & Solutions explains vulnerabilities and
attack vectors specific to ICS/SCADA protocols,
applications, hardware, servers, and
workstations. You will learn how hackers and
malware, such as the infamous Stuxnet worm,
can exploit them and disrupt critical processes,
compromise safety, and bring production to a
halt. The authors fully explain defense strategies
and offer ready-to-deploy countermeasures.
Each chapter features a real-world case study as
well as notes, tips, and cautions. Features
examples, code samples, and screenshots of
ICS/SCADA-specific attacks Offers step-by-step
vulnerability assessment and penetration test
instruction Written by a team of ICS/SCADA
security experts and edited by Hacking Exposed
veteran Joel Scambray

**HACKING EXPOSED MALWARE AND
ROOTKITS** - Michael Davis 2009-09-23

"A harrowing guide to where the bad guys hide,
and how you can find them." --Dan Kaminsky,
Director of Penetration Testing, IOActive "An
amazing resource. It is timely, focused, and what

we need to better understand and defend
against one of the greatest cyber threats we
face." --From the Foreword by Lance Spitzner,
President of the HoneyNet Project Don't let
another machine become a zombie in the
malware army Defend against the ongoing wave
of malware and rootkit assaults the failsafe
Hacking Exposed way. Real-world case studies
and examples reveal how today's hackers use
readily available tools to infiltrate and hijack
systems. Step-by-step countermeasures provide
proven prevention techniques. Find out how to
detect and eliminate malicious embedded code,
block pop-ups and websites, prevent keylogging,
and terminate rootkits. The latest intrusion
detection, firewall, honeynet, antivirus, anti-
rootkit, and anti-spyware technologies are
covered in detail. Understand how malware
infects, survives, and propagates across an
enterprise Learn how hackers use archivers,
encryptors, and packers to obfuscate code
Implement effective intrusion detection and
prevention procedures Defend against
keylogging, redirect, click fraud, and identity
theft threats Detect, kill, and remove virtual,
user-mode, and kernel-mode rootkits Prevent
malicious website, phishing, client-side, and
embedded-code exploits Protect hosts using the
latest antivirus, pop-up blocker, and firewall
software Identify and terminate malicious
processes using HIPS and NIPS

**Hacking Exposed Malware & Rootkits:
Security Secrets and Solutions, Second
Edition** - Christopher C. Elisan 2016-12-16

Arm yourself for the escalating war against
malware and rootkits Thwart debilitating cyber-
attacks and dramatically improve your
organization's security posture using the proven
defense strategies in this thoroughly updated
guide. Hacking Exposed™ Malware and
Rootkits: Security Secrets & Solutions, Second
Edition fully explains the hacker's latest
methods alongside ready-to-deploy
countermeasures. Discover how to block pop-up
and phishing exploits, terminate embedded
code, and identify and eliminate rootkits. You
will get up-to-date coverage of intrusion
detection, firewall, honeynet, antivirus, and anti-
rootkit technology. • Learn how malware infects,
survives, and propagates across an enterprise •
See how hackers develop malicious code and

target vulnerable systems • Detect, neutralize, and remove user-mode and kernel-mode rootkits • Use hypervisors and honeypots to uncover and kill virtual rootkits • Defend against keylogging, redirect, click fraud, and identity theft • Block spear phishing, client-side, and embedded-code exploits • Effectively deploy the latest antivirus, pop-up blocker, and firewall software • Identify and stop malicious processes using IPS solutions
Hacking Exposed Web Applications - Joel Scambray 2006

Hacking Exposed 5th Edition - Stuart McClure 2005-04-19

Analyzes attacks on computer networks, discusses security, auditing, and intrusion detection procedures, and covers hacking on the Internet, attacks against Windows, e-commerce hacking methodologies, and new discovery tools.

Hacking Exposed 5th Edition - Stuart McClure 2005-05-10

"The seminal book on white-hat hacking and countermeasures... Should be required reading for anyone with a server or a network to secure." --Bill Machrone, PC Magazine "The definitive compendium of intruder practices and tools." -- Steve Steinke, Network Magazine "For almost any computer book, you can find a clone. But not this one... A one-of-a-kind study of the art of breaking in." --UNIX Review Here is the latest edition of international best-seller, Hacking Exposed. Using real-world case studies, renowned security experts Stuart McClure, Joel Scambray, and George Kurtz show IT professionals how to protect computers and networks against the most recent security vulnerabilities. You'll find detailed examples of the latest devious break-ins and will learn how to think like a hacker in order to thwart attacks. Coverage includes: Code hacking methods and countermeasures New exploits for Windows 2003 Server, UNIX/Linux, Cisco, Apache, and Web and wireless applications Latest DDoS techniques--zombies, Blaster, MyDoom All new class of vulnerabilities--HTTP Response Splitting and much more

Designing BSD Rootkits - Joseph Kong 2007 "Designing BSD Rootkits" introduces the fundamentals of programming and developing rootkits under the FreeBSD operating system. Written in a friendly, accessible style and

sprinkled with geek humor and pop culture references, the author favors a "learn by example" approach that assumes no prior kernel hacking experience.

Rootkit Arsenal - Bill Blunden 2013

While forensic analysis has proven to be a valuable investigative tool in the field of computer security, utilizing anti-forensic technology makes it possible to maintain a covert operational foothold for extended periods, even in a high-security environment. Adopting an approach that favors full disclosure, the updated Second Edition of The Rootkit Arsenal presents the most accessible, timely, and complete coverage of forensic countermeasures. This book covers more topics, in greater depth, than any other currently available. In doing so the author forges through the murky back alleys of the Internet, shedding light on material that has traditionally been poorly documented, partially documented, or intentionally undocumented. The range of topics presented includes how to: -Evade post-mortem analysis - Frustrate attempts to reverse engineer your command & control modules -Defeat live incident response -Undermine the process of memory analysis -Modify subsystem internals to feed misinformation to the outside -Entrench your code in fortified regions of execution - Design and implement covert channels -Unearth new avenues of attack

Mobile Malware Attacks and Defense - Ken Dunham 2008-11-12

Malware has gone mobile, and the security landscape is changing quickly with emerging attacks on cell phones, PDAs, and other mobile devices. This first book on the growing threat covers a wide range of malware targeting operating systems like Symbian and new devices like the iPhone. Examining code in past, current, and future risks, protect your banking, auctioning, and other activities performed on mobile devices. * Visual Payloads View attacks as visible to the end user, including notation of variants. * Timeline of Mobile Hoaxes and Threats Understand the history of major attacks and horizon for emerging threats. * Overview of Mobile Malware Families Identify and understand groups of mobile malicious code and their variations. * Taxonomy of Mobile Malware Bring order to known samples based on

infection, distribution, and payload strategies. * Phishing, SMishing, and Vishing Attacks Detect and mitigate phone-based phishing (vishing) and SMS phishing (SMishing) techniques. *

Operating System and Device Vulnerabilities Analyze unique OS security issues and examine offensive mobile device threats. * Analyze Mobile Malware Design a sandbox for dynamic software analysis and use MobileSandbox to analyze mobile malware. * Forensic Analysis of Mobile Malware Conduct forensic analysis of mobile devices and learn key differences in mobile forensics. * Debugging and Disassembling Mobile Malware Use IDA and other tools to reverse-engineer samples of malicious code for analysis. * Mobile Malware Mitigation Measures Qualify risk, understand threats to mobile assets, defend against attacks, and remediate incidents. * Understand the History and Threat Landscape of Rapidly Emerging Mobile Attacks * Analyze Mobile Device/Platform Vulnerabilities and Exploits * Mitigate Current and Future Mobile Malware Threats

Penetration Testing Georgia Weidman
2014-06-14

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.

Hacking Exposed Wireless Johnny Cache
2007-04-10

Secure Your Wireless Networks the Hacking Exposed Way Defend against the latest pervasive and devastating wireless attacks using the tactical security information contained in this comprehensive volume. *Hacking Exposed Wireless* reveals how hackers zero in on susceptible networks and peripherals, gain access, and execute debilitating attacks. Find out how to plug security holes in Wi-Fi/802.11 and Bluetooth systems and devices. You'll also learn how to launch wireless exploits from Metasploit, employ bulletproof authentication and encryption, and sidestep insecure wireless hotspots. The book includes vital details on new, previously unpublished attacks alongside real-world countermeasures. Understand the concepts behind RF electronics, Wi-Fi/802.11, and Bluetooth Find out how hackers use NetStumbler, WiSPY, Kismet, KisMAC, and AiroPeek to target vulnerable wireless networks Defend against WEP key brute-force, aircrack, and traffic injection hacks Crack WEP at new speeds using Field Programmable Gate Arrays or your spare PS3 CPU cycles Prevent rogue AP and certificate authentication attacks Perform packet injection from Linux Launch DoS attacks using device driver-independent tools Exploit wireless device drivers using the Metasploit 3.0 Framework Identify and avoid malicious hotspots Deploy WPA/802.11i authentication and encryption using PEAP, FreeRADIUS, and WPA pre-shared keys

Analyzing Computer Security Charles P. Pfleeger 2012

In this book, the authors of the 20-year best-selling classic *Security in Computing* take a fresh, contemporary, and powerfully relevant new approach to introducing computer security. Organised around attacks and mitigations, the Pfleegers' new *Analyzing Computer Security* will attract students' attention by building on the

high-profile security failures they may have already encountered in the popular media. Each section starts with an attack description. Next, the authors explain the vulnerabilities that have allowed this attack to occur. With this foundation in place, they systematically present today's most effective countermeasures for blocking or weakening the attack. One step at a time, students progress from attack/problem/harm to solution/protection/mitigation, building the powerful real-world problem solving skills they need to succeed as information security professionals. Analyzing Computer Security addresses crucial contemporary computer security themes throughout, including effective security management and risk analysis; economics and quantitative study; privacy, ethics, and laws; and the use of overlapping controls. The authors also present significant new material on computer forensics, insiders, human factors, and trust.

Reverse Deception: Organized Cyber Threat Counter-Exploitation - Sean M. Bodmer
2012-07-06

In-depth counterintelligence tactics to fight cyber-espionage "A comprehensive and unparalleled overview of the topic by experts in the field."--Slashdot Expose, pursue, and prosecute the perpetrators of advanced persistent threats (APTs) using the tested security techniques and real-world case studies featured in this one-of-a-kind guide. Reverse Deception: Organized Cyber Threat Counter-Exploitation shows how to assess your network's vulnerabilities, zero in on targets, and effectively block intruders. Discover how to set up digital traps, misdirect and divert attackers, configure honeypots, mitigate encrypted crimeware, and identify malicious software groups. The expert authors provide full coverage of legal and ethical issues, operational vetting, and security team management. Establish the goals and scope of your reverse deception campaign Identify, analyze, and block APTs Engage and catch nefarious individuals and their organizations Assemble cyber-profiles, incident analyses, and intelligence reports Uncover, eliminate, and autopsy crimeware, trojans, and botnets Work with intrusion detection, anti-virus, and digital forensics tools Employ stealth honeynet,

honeypot, and sandbox technologies Communicate and collaborate with legal teams and law enforcement

The Mac Hacker's Handbook- Charlie Miller
2011-03-21

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.

Android Hacker's Handbook - Joshua J. Drake
2014-03-26

The first comprehensive guide to discovering and preventing attacks on the Android OS As the Android operating system continues to increase its share of the smartphone market, smartphone hacking remains a growing threat. Written by experts who rank among the world's foremost Android security researchers, this book presents vulnerability discovery, analysis, and exploitation tools for the good guys. Following a detailed explanation of how the Android OS works and its overall security architecture, the authors examine how vulnerabilities can be discovered and exploits developed for various system components, preparing you to defend against them. If you are a mobile device administrator, security researcher, Android app developer, or consultant responsible for evaluating Android security, you will find this guide is essential to your toolbox. A crack team of leading Android security researchers explain Android security risks, security design and architecture, rooting, fuzz testing, and vulnerability analysis Covers Android application building blocks and security as well as debugging and auditing Android apps Prepares mobile device administrators, security researchers, Android app developers, and security consultants to defend Android systems against attack Android Hacker's Handbook is the first comprehensive resource for IT professionals

charged with smartphone security.

Rootkits - Greg Hoglund 2006

A guide to rootkits describes what they are, how they work, how to build them, and how to detect them.

Hacking Exposed Mobile - Neil Bergman
2013-08-05

Proven security tactics for today's mobile apps, devices, and networks "A great overview of the new threats created by mobile devices. ...The authors have heaps of experience in the topics and bring that to every chapter." -- Slashdot
Hacking Exposed Mobile continues in the great tradition of the Hacking Exposed series, arming business leaders and technology practitioners with an in-depth understanding of the latest attacks and countermeasures--so they can leverage the power of mobile platforms while ensuring that security risks are contained." -- Jamil Farshchi, Senior Business Leader of Strategic Planning and Initiatives, VISA Identify and evade key threats across the expanding mobile risk landscape. Hacking Exposed Mobile: Security Secrets & Solutions covers the wide range of attacks to your mobile deployment alongside ready-to-use countermeasures. Find out how attackers compromise networks and devices, attack mobile services, and subvert mobile apps. Learn how to encrypt mobile data, fortify mobile platforms, and eradicate malware. This cutting-edge guide reveals secure mobile development guidelines, how to leverage mobile OS features and MDM to isolate apps and data, and the techniques the pros use to secure mobile payment systems. Tour the mobile risk ecosystem with expert guides to both attack and defense Learn how cellular network attacks compromise devices over-the-air See the latest Android and iOS attacks in action, and learn how to stop them Delve into mobile malware at the code level to understand how to write resilient apps Defend against server-side mobile attacks, including SQL and XML injection Discover mobile web attacks, including abuse of custom URI schemes and JavaScript bridges Develop stronger mobile authentication routines using OAuth and SAML Get comprehensive mobile app development security guidance covering everything from threat modeling to iOS- and Android-specific tips Get started quickly using our mobile pen testing and consumer security

checklists

The Basics of Hacking and Penetration

Testing - Patrick Engebretson 2013-06-24

The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test.

Virtual Honeypots - Niels Provos 2007-07-16

Honeypots have demonstrated immense value in Internet security, but physical honeypot deployment can be prohibitively complex, time-consuming, and expensive. Now, there's a breakthrough solution. Virtual honeypots share many attributes of traditional honeypots, but you can run thousands of them on a single system--making them easier and cheaper to build, deploy, and maintain. In this hands-on, highly accessible book, two leading honeypot pioneers systematically introduce virtual honeypot technology. One step at a time, you'll learn

exactly how to implement, configure, use, and maintain virtual honeypots in your own environment, even if you've never deployed a honeypot before. You'll learn through examples, including Honeyd, the acclaimed virtual honeypot created by coauthor Niels Provos. The authors also present multiple real-world applications for virtual honeypots, including network decoy, worm detection, spam prevention, and network simulation. After reading this book, you will be able to Compare high-interaction honeypots that provide real systems and services and the low-interaction honeypots that emulate them Install and configure Honeyd to simulate multiple operating systems, services, and network environments Use virtual honeypots to capture worms, bots, and other malware Create high-performance "hybrid" honeypots that draw on technologies from both low- and high-interaction honeypots Implement client honeypots that actively seek out dangerous Internet locations Understand how attackers identify and circumvent honeypots Analyze the botnets your honeypot identifies, and the malware it captures Preview the future evolution of both virtual and physical honeypots

CEH Certified Ethical Hacker Study Guide - Kimberly Graves 2010-06-03

Full Coverage of All Exam Objectives for the CEH Exams 312-50 and EC0-350 Thoroughly prepare for the challenging CEH Certified Ethical Hackers exam with this comprehensive study guide. The book provides full coverage of exam topics, real-world examples, and includes a CD with chapter review questions, two full-length practice exams, electronic flashcards, a glossary of key terms, and the entire book in a searchable pdf e-book. What's Inside: Covers ethics and legal issues, footprinting, scanning, enumeration, system hacking, trojans and backdoors, sniffers, denial of service, social engineering, session hijacking, hacking Web servers, Web application vulnerabilities, and more Walks you through exam topics and includes plenty of real-world scenarios to help reinforce concepts Includes a CD with an assessment test, review questions, practice exams, electronic flashcards, and the entire book in a searchable pdf

Hacking Exposed 7 : Network Security

Secrets & Solutions, Seventh Edition - Stuart McClure 2012-07-11

The latest tactics for thwarting digital attacks "Our new reality is zero-day, APT, and state-sponsored attacks. Today, more than ever, security professionals need to get into the hacker's mind, methods, and toolbox to successfully deter such relentless assaults. This edition brings readers abreast with the latest attack vectors and arms them for these continually evolving threats." --Brett Wahlin, CSO, Sony Network Entertainment "Stop taking punches--let's change the game; it's time for a paradigm shift in the way we secure our networks, and Hacking Exposed 7 is the playbook for bringing pain to our adversaries." --Shawn Henry, former Executive Assistant Director, FBI Bolster your system's security and defeat the tools and tactics of cyber-criminals with expert advice and defense strategies from the world-renowned Hacking Exposed team. Case studies expose the hacker's latest devious methods and illustrate field-tested remedies. Find out how to block infrastructure hacks, minimize advanced persistent threats, neutralize malicious code, secure web and database applications, and fortify UNIX networks. Hacking Exposed 7: Network Security Secrets & Solutions contains all-new visual maps and a comprehensive "countermeasures cookbook." Obstruct APTs and web-based meta-exploits Defend against UNIX-based root access and buffer overflow hacks Block SQL injection, spear phishing, and embedded-code attacks Detect and terminate rootkits, Trojans, bots, worms, and malware Lock down remote access using smartcards and hardware tokens Protect 802.11 WLANs with multilayered encryption and gateways Plug holes in VoIP, social networking, cloud, and Web 2.0 services Learn about the latest iPhone and Android attacks and how to protect yourself

The Antivirus Hacker's Handbook - Joxean Koret 2015-08-19

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 software program and work your way back through its development using the functions and other key elements of the software. Next, you leverage your new knowledge about software development to evade, attack, and exploit antivirus software—all of which can help you strengthen your network and protect your data. While not all viruses are damaging, understanding how to better protect your computer against them can help you maintain the integrity of your network. Discover how to reverse engineer your antivirus software Explore methods of antivirus software evasion Consider different ways to attack and exploit antivirus software Understand the current state of the antivirus software market, and get recommendations for users and vendors who are leveraging this software The Antivirus Hacker's Handbook is the essential reference for software reverse engineers, penetration testers, security researchers, exploit writers, antivirus vendors, and software engineers who want to understand how to leverage current antivirus software to improve future applications.

Hacker, Hoaxer, Whistleblower, Spy Gabriella Coleman 2014-11-04

Here is the ultimate book on the worldwide movement of hackers, pranksters, and activists that operates under the non-name Anonymous, by the writer the Huffington Post says “knows all of Anonymous’ deepest, darkest secrets.” Half a dozen years ago, anthropologist Gabriella Coleman set out to study the rise of this global phenomenon just as some of its members were turning to political protest and dangerous disruption (before Anonymous shot to fame as a key player in the battles over WikiLeaks, the Arab Spring, and Occupy Wall Street). She ended up becoming so closely connected to Anonymous that the tricky story of her inside-outside status as Anon confidante, interpreter, and erstwhile mouthpiece forms one of the themes of this witty and entirely engrossing book. The narrative brims with details unearthed from within a notoriously mysterious subculture, whose semi-legendary tricksters—such as Topiary, tflow, Anachaos, and

Sabu—emerge as complex, diverse, politically and culturally sophisticated people. Propelled by years of chats and encounters with a multitude of hackers, including imprisoned activist Jeremy Hammond and the double agent who helped put him away, Hector Monsegur, Hacker, Hoaxer, Whistleblower, Spy is filled with insights into the meaning of digital activism and little understood facets of culture in the Internet age, including the history of “trolling,” the ethics and metaphysics of hacking, and the origins and manifold meanings of “the lulz.”

Ethical Hacking - Alana Maurushat 2019-04-09

How will governments and courts protect civil liberties in this new era of hacktivism? Ethical Hacking discusses the attendant moral and legal issues. The first part of the 21st century will likely go down in history as the era when ethical hackers opened governments and the line of transparency moved by force. One need only read the motto “we open governments” on the Twitter page for Wikileaks to gain a sense of the sea change that has occurred. Ethical hacking is the non-violent use of a technology in pursuit of a cause—political or otherwise—which is often legally and morally ambiguous. Hacktivists believe in two general but spirited principles: respect for human rights and fundamental freedoms, including freedom of expression and personal privacy; and the responsibility of government to be open, transparent and fully accountable to the public. How courts and governments will deal with hacking attempts which operate in a grey zone of the law and where different ethical views collide remains to be seen. What is undisputed is that Ethical Hacking presents a fundamental discussion of key societal questions. A fundamental discussion of key societal questions. This book is published in English. - La première moitié du XXIe siècle sera sans doute reconnue comme l'époque où le piratage éthique a ouvert de force les gouvernements, déplaçant les limites de la transparence. La page twitter de Wikileaks enchâsse cet ethos à même sa devise, « we open governments », et sa volonté d'être omniprésent. En parallèle, les grandes sociétés de technologie comme Apple se font compétition pour produire des produits de plus en plus sécuritaires et à protéger les données de leurs clients, alors même que les gouvernements tentent de limiter

et de décrypter ces nouvelles technologies d'encryption. Entre-temps, le marché des vulnérabilités en matière de sécurité augmente à mesure que les experts en sécurité informatique vendent des vulnérabilités de logiciels des grandes technologies, dont Apple et Google, contre des sommes allant de 10 000 à 1,5 million de dollars. L'activisme en sécurité est à la hausse. Le piratage éthique est l'utilisation non-violence d'une technologie quelconque en soutien d'une cause politique ou autre qui est souvent ambiguë d'un point de vue juridique et moral. Le hacking éthique peut désigner les actes de vérification de pénétration professionnelle ou d'experts en sécurité informatique, de même que d'autres formes d'actions émergentes, comme l'hacktivisme et la désobéissance civile en ligne. L'hacktivisme est une forme de piratage éthique, mais également une forme de militantisme des droits civils à l'ère numérique. En principe, les adeptes du hacktivisme croient en deux grands principes : le respect des droits de la personne et les libertés fondamentales, y compris la liberté d'expression et à la vie privée, et la responsabilité des gouvernements d'être ouverts, transparents et pleinement redevables au public. En pratique, toutefois, les antécédents comme les agendas des hacktivistes sont fort diversifiés. Il n'est pas clair de quelle façon les tribunaux et les gouvernements traiteront des tentatives de piratage eu égard aux zones grises juridiques, aux approches éthiques conflictuelles, et compte tenu du fait qu'il n'existe actuellement, dans le monde, presque aucune exception aux provisions, en matière de cybercrime et de crime informatique, liées à la recherche sur la sécurité ou l'intérêt public. Il sera également difficile de déterminer le lien entre hacktivisme et droits civils. Ce livre est publié en anglais.

Hacking For Dummies - Kevin Beaver
2018-07-11

Stop hackers before they hack you! In order to outsmart a would-be hacker, you need to get into the hacker's mindset. And with this book, thinking like a bad guy has never been easier. In *Hacking For Dummies*, expert author Kevin Beaver shares his knowledge on penetration testing, vulnerability assessments, security best practices, and every aspect of ethical hacking that is essential in order to stop a hacker in their

tracks. Whether you're worried about your laptop, smartphone, or desktop computer being compromised, this no-nonsense book helps you learn how to recognize the vulnerabilities in your systems so you can safeguard them more diligently—with confidence and ease. Get up to speed on Windows 10 hacks Learn about the latest mobile computing hacks Get free testing tools Find out about new system updates and improvements There's no such thing as being too safe—and this resourceful guide helps ensure you're protected.

[Cybersecurity Blue Team Toolkit](#) - Nadean H. Tanner 2019-04-04

A practical handbook to cybersecurity for both tech and non-tech professionals As reports of major data breaches fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity. Most books on the subject, however, are either too specialized for the non-technical professional or too general for positions in the IT trenches. Thanks to author Nadean Tanner's wide array of experience from teaching at a University to working for the Department of Defense, the *Cybersecurity Blue Team Toolkit* strikes the perfect balance of substantive and accessible, making it equally useful to those in IT or management positions across a variety of industries. This handy guide takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals, whether they be new to the field or looking to expand their expertise. Tanner gives comprehensive coverage to such crucial topics as security assessment and configuration, strategies for protection and defense, offensive measures, and remediation while aligning the concept with the right tool using the CIS Controls version 7 as a guide. Readers will learn why and how to use fundamental open source and free tools such as ping, tracer, PuTTY, pathping, sysinternals, NMAP, OpenVAS, Nexpose Community, OSSEC, Hamachi, InSSIDer, Nexpose Community, Wireshark, Solarwinds Kiwi Syslog Server, Metasploit, Burp, Clonezilla and many more. Up-to-date and practical cybersecurity instruction, applicable to both management and technical positions • Straightforward explanations of the theory behind cybersecurity best practices •

Designed to be an easily navigated tool for daily use • Includes training appendix on Linux, how to build a virtual lab and glossary of key terms
The Cybersecurity Blue Team Toolkit is an excellent resource for anyone working in digital policy as well as IT security professionals, technical analysts, program managers, and Chief Information and Technology Officers. This is one handbook that won't gather dust on the shelf, but remain a valuable reference at any career level, from student to executive.

Hackers Beware - Eric Cole 2002

Explains how and why hackers break into computers, steal information, and deny services to machines' legitimate users, and discusses strategies and tools used by hackers and how to defend against them.

Computer Security Threats - Ciza Thomas
2020-09-09

This book on computer security threats explores the computer security threats and includes a broad set of solutions to defend the computer systems from these threats. The book is triggered by the understanding that digitalization and growing dependence on the Internet poses an increased risk of computer security threats in the modern world. The chapters discuss different research frontiers in computer security with algorithms and implementation details for use in the real world. Researchers and practitioners in areas such as statistics, pattern recognition, machine learning, artificial intelligence, deep learning, data mining, data analytics and visualization are contributing to the field of computer security. The intended audience of this book will mainly consist of researchers, research students, practitioners, data analysts, and business professionals who seek information on computer security threats and its defensive measures.

[Hacking Exposed Windows: Microsoft Windows Security Secrets and Solutions, Third Edition](#) - Joel Scambray 2007-12-04

The latest Windows security attack and defense strategies "Securing Windows begins with reading this book." --James Costello (CISSP) IT Security Specialist, Honeywell Meet the challenges of Windows security with the exclusive Hacking Exposed "attack-countermeasure" approach. Learn how real-world malicious hackers conduct reconnaissance

of targets and then exploit common misconfigurations and software flaws on both clients and servers. See leading-edge exploitation techniques demonstrated, and learn how the latest countermeasures in Windows XP, Vista, and Server 2003/2008 can mitigate these attacks. Get practical advice based on the authors' and contributors' many years as security professionals hired to break into the world's largest IT infrastructures. Dramatically improve the security of Microsoft technology deployments of all sizes when you learn to:
Establish business relevance and context for security by highlighting real-world risks
Take a tour of the Windows security architecture from the hacker's perspective, exposing old and new vulnerabilities that can easily be avoided
Understand how hackers use reconnaissance techniques such as footprinting, scanning, banner grabbing, DNS queries, and Google searches to locate vulnerable Windows systems
Learn how information is extracted anonymously from Windows using simple NetBIOS, SMB, MSRPC, SNMP, and Active Directory enumeration techniques
Prevent the latest remote network exploits such as password grinding via WMI and Terminal Server, passive Kerberos logon sniffing, rogue server/man-in-the-middle attacks, and cracking vulnerable services
See up close how professional hackers reverse engineer and develop new Windows exploits
Identify and eliminate rootkits, malware, and stealth software
Fortify SQL Server against external and insider attacks
Harden your clients and users against the latest e-mail phishing, spyware, adware, and Internet Explorer threats
Deploy and configure the latest Windows security countermeasures, including BitLocker, Integrity Levels, User Account Control, the updated Windows Firewall, Group Policy, Vista Service Refactoring/Hardening, SafeSEH, GS, DEP, Patchguard, and Address Space Layout Randomization

Hacking Exposed Malware & Rootkits: Security Secrets and Solutions, Second Edition - Aaron LeMasters 2016-06-22

The latest exclusive Hacking Exposed strategies for defending against the world's number one attack type: malware Fully updated to cover the most current tools, techniques, and exploits, Hacking Exposed Malware & Rootkits, Second

Edition walks you through the process of defending against the consistent onslaught of malware and rootkit assaults using failsafe methods. The second edition includes all-new real-world case studies and cutting-edge examples to reveal how hackers use readily available tools to infiltrate and hijack networks. The book takes a step-by-step approach to explaining countermeasures to provide the best training in the detection and elimination of malicious, embedded code. The latest intrusion detection, baits, antivirus, anti-rootkit, and anti-spyware technologies are all covered in detail. Counter today's most virulent network attack types Find out how malware infects, survives, and propagates across an enterprise Detect, kill, and remove virtual, user-mode, and kernel-mode rootkits Learn how hackers use archivers, encryptors, and packers to obfuscate code Defend against keylogging, redirect, click fraud, and identity theft threats

Hacking Exposed - Joel Scambray 2002

Get in-depth coverage of Web application platforms and their vulnerabilities, presented the same popular format as the international bestseller, *Hacking Exposed*. Covering hacking scenarios across different programming languages and depicting various types of attacks and countermeasures, this book offers you up-to-date and highly valuable insight into Web application security. "Required reading for Web architects and operators." -- Erik Olson, Microsoft Program Manager, Security, ASP.NET "Just as the original *Hacking Exposed* revealed the techniques the bad guys were hiding behind, *Hacking Exposed Web Applications* will do the same for this critical technology. Its methodical approach and appropriate detail will enlighten, educate, and go a long way toward making the Web a safer place in which to do business." -- from the Foreword by Mark Curphey, Chair of the Open Web Application Security Project "This is a serious technical guide that is also great reading -- scary enough to motivate folks to take Web security seriously but approachable enough to be an effective learning tool. Required reading for Web architects and operators." -- Erik Olson, Program Manager, Security, ASP.NET "What better way to defend against hackers than to understand the tools and techniques that are used to penetrate your site?

Hacking Exposed Web Applications offers a detailed look at common vulnerabilities within your applications and explains how to protect yourself from them." -- Mike Mullins, Ecommerce Security Engineer for a leading specialty apparel retailer "At last, your personal guide to preventing the next generation of security threats. This book explains in intricate detail how you can do everything right when it comes to network security and still be owned at the Web application layer." -- Chip Andrews, www.sqlsecurity.com "If you're involved in writing Web-based applications using ASP/ASP.NET, Java, JSP, PHP, or other languages, the *Hacking Exposed* series is something you DEFINITELY need to read. Before writing one line of code, this book will spark ideas about how to design and secure your Web applications. There are techniques potential hackers could use that I've never even thought of! Great resource!" -- Steve Schofield, Creator and Managing Editor, ASPFree.com

Hacking: The Next Generation Nitesh Dhanjani 2009-08-29

With the advent of rich Internet applications, the explosion of social media, and the increased use of powerful cloud computing infrastructures, a new generation of attackers has added cunning new techniques to its arsenal. For anyone involved in defending an application or a network of systems, *Hacking: The Next Generation* is one of the few books to identify a variety of emerging attack vectors. You'll not only find valuable information on new hacks that attempt to exploit technical flaws, you'll also learn how attackers take advantage of individuals via social networking sites, and abuse vulnerabilities in wireless technologies and cloud infrastructures. Written by seasoned Internet security professionals, this book helps you understand the motives and psychology of hackers behind these attacks, enabling you to better prepare and defend against them. Learn how "inside out" techniques can poke holes into protected networks Understand the new wave of "blended threats" that take advantage of multiple application vulnerabilities to steal corporate data Recognize weaknesses in today's powerful cloud infrastructures and how they can be exploited Prevent attacks against the mobile workforce and their devices containing valuable

data Be aware of attacks via social networking sites to obtain confidential information from executives and their assistants Get case studies

that show how several layers of vulnerabilities can be used to compromise multinational corporations