

Hacking Wireless Networks For Dummies

Right here, we have countless books **Hacking Wireless Networks For Dummies** and collections to check out. We additionally pay for variant types and also type of the books to browse. The agreeable book, fiction, history, novel, scientific research, as without difficulty as various supplementary sorts of books are readily genial here.

As this Hacking Wireless Networks For Dummies , it ends stirring instinctive one of the favored books Hacking Wireless Networks For Dummies collections that we have. This is why you remain in the best website to see the amazing ebook to have.

Hacking Wireless Networks For Dummies - Kevin Beaver 2011-05-09

Become a cyber-hero - know the common wireless weaknesses "Reading a book like this one is a worthy endeavor toward becoming an experienced wireless security professional." --Devin Akin - CTO, The Certified Wireless Network Professional(CWNP) Program Wireless networks are so convenient - not only for you, but also for those nefarious types who'd like to invade them. The only way to know if your system can be penetrated is to simulate an attack. This book shows you how, along with how to strengthen any weakspots you find in your network's armor. Discover how to: Perform ethical hacks without compromising a system Combat denial of service and WEP attacks Understand how invaders think Recognize the effects of different hacks Protect against war drivers and rogue devices

Wireless Hacking - Hugo Hoffman 2020-04-26

Both Wired and Wireless Pen Testing has become a key skill among professional hackers using Kali Linux. If you want to become a Penetration Tester, BUY THIS BOOK NOW AND GET STARTED TODAY! This Book Bundle Includes 3 Books: -Book 1 - Wireless Technology Fundamentals-Book 2 - Learn Fast How To Hack Any Wireless Networks-Book 3 - Learn Fast How To Hack Like A ProBook 1 will cover: -Electromagnetic Spectrum, RF Basics, Antenna Types-2.4 GHz & 5 GHz Band, Modulation Basics, Radio Frequency Encoding-Influencing RF Signals, Path Loss aka Attenuation, Signal to Interference Ratio-Decibels, MIMO Technology, Beamforming, Channel Bonding-Beacons, Active & Passive Scanning, Frame Types-802.11 a/b/g/n/ac /ax/ WiFi 6 / 5G networks and more. Book 2 will cover: -PenTest Tools / Wireless Adapters & Wireless Cards for Penetration Testing-Virtual Box & Kali Linux Installation and Decrypting Traffic with Wireshark-How to implement MITM Attack with Ettercap, How to deploy Rogue Access Point using MITM Attack-How to implement Deauthentication Attack against a Rogue AP-How to deploy Evil Twin Deauthentication Attack with mdk3, How to deploy DoS Attack with MKD3-4-Way Handshake & Fast Roaming Process, Data Protection and Data Tampering and more...Book 3 will cover: -Pen Testing @ Stage 1, Stage 2 and Stage 3, What Penetration Testing Standards exist-Burp Suite Proxy setup and Spidering hosts, How to deploy SQL Injection with SQLmap-How to implement Dictionary Attack with Airodump-ng, How to deploy ARP Poisoning with EtterCAP-How to capture Traffic with Port Mirroring & with Xplico, How to deploy Passive Reconnaissance-How to implement MITM Attack with Ettercap & SSLstrip, How to Manipulate Packets with Scapy-How to deploy Deauthentication Attack, How to capture IPv6 Packets with Parasite6-How to deploy Evil Twin Deauthentication Attack with mdk3, The Metasploit Framework-How to deploy DoS Attack with MKD3, How to implement Brute Force Attack with TCP Hydra-How to deploy Armitage Hail Mary, How to use SET aka Social-Engineering Toolkit and more...BUY THIS BOOK NOW AND GET STARTED TODAY!

Wi-Foo - Andrew A. Vladimirov 2004

The definitive guide to penetrating and defending wireless networks. Straight from the field, this is the definitive guide to hacking wireless networks. Authored by world-renowned wireless security auditors, this hands-on, practical guide covers everything you need to attack -- or protect -- any wireless network. The authors introduce the 'battlefield,' exposing today's 'wide open' 802.11 wireless networks and their attackers. One step at a time, you'll master the attacker's entire arsenal of hardware and software tools: crucial knowledge for crackers and auditors alike. Next, you'll learn systematic countermeasures for building hardened wireless 'citadels' including cryptography-based techniques, authentication, wireless

VPNs, intrusion detection, and more. Coverage includes: Step-by-step walkthroughs and explanations of typical attacks Building wireless hacking/auditing toolkit: detailed recommendations, ranging from discovery tools to chipsets and antennas Wardriving: network mapping and site surveying Potential weaknesses in current and emerging standards, including 802.11i, PPTP, and IPSec Implementing strong, multilayered defenses Wireless IDS: why attackers aren't as untraceable as they think Wireless hacking and the law: what's legal, what isn't If you're a hacker or security auditor, this book will get you in. If you're a netadmin, sysadmin, consultant, or home user, it will keep everyone else out.

Hacking - James Squires 2016-11-15

Want to See How Easy It Is To Hack Your Wireless Network? Methods and Guide Here Show You How - Easy as 1 2 3

Computer Networking Hacking - Ramon Base 2019-07-26

Buy the Paperback version of this book, and get the Kindle eBook version included for FREE Do you want to make a career in an exciting and rewarding field like computer management? Are you interested in training for a job that helps in manipulating the normal behaviour of the network connections, in order to provide help for a noble cause? The truth is: Computer networking is a field which is always evolving. It requires the help of a well-researched study of the operating systems and network configurations to excel in them. True hacking once referred to activities which were meant for good intentions. Malicious things done to impose an attack on the computer networks were officially known as cracking. Protecting a network and the various devices or computers attached to it from phishing, Trojans, unauthorized access and malware is a very important job and requires much practice and knowledge. DOWNLOAD: Computer Networking Hacking, Ultimate Guide to Ethical Hacking, Wireless Network, Cyber security with Practical Penetration Test on Kali Linux and System Security Practices. Programming skills are something which every hacker should have. Other than the programming skills, a good hacker should also know networking skills to become an effective hacker. He should know how to employ the internet and the search engines to his best use. The goal of the book is simple: The eBook is the ultimate guide to ethical hacking. It provides a complete knowledge about hacking, its types, getting started with ethical hacking, wireless network hacking, installing and using kali Linux, virtualizing machines and description of the main programs which are used in the world. The book also stresses on Ultimate Guide to Ethical Hacking, Wireless Network, and Cyber security with Practical Penetration Test on Kali Linux and System Security Practices. You will also learn: History of hacking What is hacking and the differences between hacking and cracking Types of hacking to combat brute force, ransomware, network attacks, dos, ddos, phishing, tabnapping, web attack and social engineering. How to start with ethical hacking? Wireless network hacking and testing the system. Also understanding the various threats in the wireless networks. encryption and password security, wep, wpa, wpa2, wpa3, all type off attack on those password practical example to make keylogger, gain access on remote machine, client/server hack Best practices to make a system secure practical example to configure a real network and make secure(switch, router, firewall etc Scripting Backup and restore a network Sandbox attack prevention methods Best practises to stay safe online Would you like to know more? Download the eBook, Computer Networking Hacking, immediately to know more about ethical hacking. Scroll to the top of the page and select the buy now button.

Network Security For Dummies - Chey Cobb 2011-05-09

CNN is reporting that a vicious new virus is wreaking havoc on the world's computer networks. Somebody's hacked one of your favorite Web sites and stolen thousands of credit card numbers. The FBI just released a new report on computer crime that's got you shaking in your boots. The experts will tell you that keeping your network safe from the cyber-wolves howling after your assets is complicated, expensive, and best left to them. But the truth is, anybody with a working knowledge of networks and computers can do just about everything necessary to defend their network against most security threats. Network Security For Dummies arms you with quick, easy, low-cost solutions to all your network security concerns. Whether your network consists of one computer with a high-speed Internet connection or hundreds of workstations distributed across dozens of locations, you'll find what you need to confidently: Identify your network's security weaknesses Install an intrusion detection system Use simple, economical techniques to secure your data Defend against viruses Keep hackers at bay Plug security holes in individual applications Build a secure network from scratch Leading national expert Chey Cobb fills you in on the basics of data security, and he explains more complex options you can use to keep your network safe as you grow your business. Among other things, you'll explore: Developing risk assessments and security plans Choosing controls without breaking the bank Anti-virus software, firewalls, intrusion detection systems and access controls Addressing Unix, Windows and Mac security issues Patching holes in email, databases, Windows Media Player, NetMeeting, AOL Instant Messenger, and other individual applications Securing a wireless network E-Commerce security Incident response and disaster recovery Whether you run a storefront tax preparing business or you're the network administrator at a multinational accounting giant, your computer assets are your business. Let Network Security For Dummies provide you with proven strategies and techniques for keeping your precious assets safe.

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

Wireless Network Hacks and Mods For Dummies - Danny Briere 2005-09-19

Fun projects and valuable content join forces to enable readers to turn their wireless home network into a high-performance wireless infrastructure capable of entertainment networking and even home automation Step-by-step instructions help readers find, buy, and install the latest and greatest wireless equipment The authors are home tech gurus and offer detailed discussion on the next-generation wireless gear that will move the wireless LAN beyond computers and into telephony, entertainment, home automation/control, and even automotive networking The number of wireless LAN users in North America is expected to grow from 4.2 million current users to more than 31 million by 2007

Understanding Network Hacks - Bastian Ballmann 2015-01-19

This book explains how to see one's own network through the eyes of an attacker, to understand their techniques and effectively protect against them. Through Python code samples the reader learns to code tools on subjects such as password sniffing, ARP poisoning, DNS spoofing, SQL injection, Google harvesting and Wifi hacking. Furthermore the reader will be introduced to defense methods such as intrusion detection and prevention systems and log file analysis by diving into code.

Wireless Hacking: Projects for Wi-Fi Enthusiasts - Lee Barken 2004-10-29

Sales of wireless LANs to home users and small businesses will soar this year, with products using IEEE 802.11 (Wi-Fi) technology leading the way, according to a report by Cahners research. Worldwide, consumers will buy 7.3 million wireless LAN nodes--which include client and network hub devices--up from about 4 million last year. This third book in the "HACKING" series from Syngress is written by the SoCalFreeNet Wireless Users Group and will cover 802.11a/b/g ("Wi-Fi") projects teaching these millions of Wi-Fi users how to "mod" and "hack" Wi-Fi access points, network cards, and antennas to run various Linux distributions and create robust Wi-Fi networks. Cahners predicts that wireless LANs next year will gain on Ethernet as the most popular home network technology. Consumers will hook up 10.9 million Ethernet nodes and 7.3 million wireless out of a total of 14.4 million home LAN nodes shipped. This book will show Wi-Fi enthusiasts and consumers of Wi-Fi LANs who want to modify their Wi-Fi hardware how to build and deploy "homebrew Wi-Fi networks, both large and small. Wireless LANs next year will gain on Ethernet as the most popular home network technology. Consumers will hook up 10.9 million Ethernet nodes and 7.3 million wireless clients out of a total of 14.4 million home LAN nodes shipped. This book will use a series of detailed, inter-related projects to teach readers how to modify their Wi-Fi hardware to increase power and performance to match that of far more expensive enterprise networking products. Also features hacks to allow mobile laptop users to actively seek wireless connections everywhere they go! The authors are all members of the San Diego Wireless Users Group, which is famous for building some of the most innovative and powerful "home brew" Wi-Fi networks in the world.

Cybersecurity For Dummies - Joseph Steinberg 2019-10-15

Protect your business and family against cyber attacks Cybersecurity is the protection against the unauthorized or criminal use of electronic data and the practice of ensuring the integrity, confidentiality, and availability of information. Being "cyber-secure" means that a person or organization has both protected itself against attacks by cyber criminals and other online scoundrels, and ensured that it has the ability to recover if it is attacked. If keeping your business or your family safe from cybersecurity threats is on your to-do list, Cybersecurity For Dummies will introduce you to the basics of becoming cyber-secure! You'll learn what threats exist, and how to identify, protect against, detect, and respond to these threats, as well as how to recover if you have been breached! The who and why of cybersecurity threats Basic cybersecurity concepts What to do to be cyber-secure Cybersecurity careers What to think about to stay cybersecure in the future Now is the time to identify vulnerabilities that may make you a victim of cyber-crime — and to defend yourself before it is too late.

Hacking - John Smith 2016-09-04

Use These Techniques to Immediately Hack a Wi-Fi Today Ever wondered how easy it could be to hack your way into someone's computer? Ever wanted to learn how to hack into someone's password-protected WiFi? Written with the beginner in mind, this new book looks at something which is a mystery to many. Set out in an easy-to-follow and simple format, this book will teach you the step by step techniques needed and covers everything you need to know in just 5 concise and well laid out chapters; Wi-Fi 101 Ethical Hacking Hacking It Like A Villain - WEP-Protected Networks Hacking It Like A Villain - WPA-Protected Networks Basic Hacking-ology Terms But this isn't just a guide to hacking. With a lot of focus on hackers continuously working to find backdoors into systems, and preventing them from becoming hacked in the first place, this book isn't just about ways to break into someone's WiFi, but gives practical advice too. And with a detailed section at the end of book, packed with the most common terminologies in the hacking community, everything is explained with the novice in mind. Happy hacking! John.

Wireless Network Security A Beginner's Guide - Tyler Wrightson 2012-05-06

Security Smarts for the Self-Guided IT Professional Protect wireless networks against all real-world hacks by learning how hackers operate. Wireless Network Security: A Beginner's Guide discusses the many attack vectors that target wireless networks and clients--and explains how to identify and prevent them. Actual cases of attacks against WEP, WPA, and wireless clients and their defenses are included. This practical resource reveals how intruders exploit vulnerabilities and gain access to wireless networks. You'll learn how to securely deploy WPA2 wireless networks, including WPA2-Enterprise using digital certificates for authentication. The book provides techniques for dealing with wireless guest access and rogue access points. Next-generation wireless networking technologies, such as lightweight access points and cloud-

based wireless solutions, are also discussed. Templates, checklists, and examples give you the hands-on help you need to get started right away. *Wireless Network Security: 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 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 This is an excellent introduction to wireless security and their security implications. The technologies and tools are clearly presented with copious illustrations and the level of presentation will accommodate the wireless security neophyte while not boring a mid-level expert to tears. If the reader invests the time and resources in building a lab to follow along with the text, s/he will develop a solid, basic understanding of what "wireless security" is and how it can be implemented in practice. This is definitely a recommended read for its intended audience. - Richard Austin, IEEE CIPHER, IEEE Computer Society's TC on Security and Privacy (E109, July 23, 2012)

Hands-On Ethical Hacking and Network Defense - Michael T. Simpson 2016-10-10

Cyber-terrorism and corporate espionage are increasingly common and devastating threats, making trained network security professionals more important than ever. This timely text helps you gain the knowledge and skills to protect networks using the tools and techniques of an ethical hacker. The authors begin by exploring the concept of ethical hacking and its practitioners, explaining their importance in protecting corporate and government data from cyber attacks. The text then provides an in-depth guide to performing security testing against computer networks, covering current tools and penetration testing methodologies. Updated for today's cyber security environment, the Third Edition of this trusted text features new computer security resources, coverage of emerging vulnerabilities and innovative methods to protect networks, a new discussion of mobile security, and information on current federal and state computer crime laws, including penalties for illegal computer hacking. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

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.

Wireless Hacking 101 - Karina Astudillo 2017-10-10

Wireless Hacking 101 - How to hack wireless networks easily! This book is perfect for computer enthusiasts that want to gain expertise in the interesting world of ethical hacking and that wish to start conducting wireless pentesting. Inside you will find step-by-step instructions about how to exploit WiFi networks using the tools within the known Kali Linux distro as the famous aircrack-ng suite. Topics covered: •Introduction to WiFi Hacking •What is Wardriving •WiFi Hacking Methodology •WiFi Mapping •Attacks to WiFi clients and networks •Defeating MAC control •Attacks to WEP, WPA, and WPA2 •Attacks to WPS •Creating Rogue AP's •MITM attacks to WiFi clients and data capture •Defeating WiFi clients and evading SSL encryption •Kidnapping sessions from WiFi clients •Defensive mechanisms

Hacking Wireless Access Points - Jennifer Kurtz 2016-12-08

Hacking Wireless Access Points: Cracking, Tracking, and Signal Jacking provides readers with a deeper understanding of the hacking threats that exist with mobile phones, laptops, routers, and navigation systems. In addition, applications for Bluetooth and near field communication (NFC) technology continue to multiply, with athletic shoes, heart rate monitors, fitness sensors, cameras, printers, headsets, fitness trackers, household appliances, and the number and types of wireless devices all continuing to increase dramatically. The book demonstrates a variety of ways that these vulnerabilities can be—and have

been—exploited, and how the unfortunate consequences of such exploitations can be mitigated through the responsible use of technology. Explains how the wireless access points in common, everyday devices can expose us to hacks and threats Teaches how wireless access points can be hacked, also providing the techniques necessary to protect and defend data Presents concrete examples and real-world guidance on how to protect against wireless access point attacks

WiFi Hacking for Beginners - James Wells 2017-07-03

In this book you will start as a beginner with no previous knowledge about penetration testing. The book is structured in a way that will take you through the basics of networking and how clients communicate with each other, then we will start talking about how we can exploit this method of communication to carry out a number of powerful attacks. At the end of the book you will learn how to configure wireless networks to protect it from these attacks. This course focuses on the practical side of wireless penetration testing without neglecting the theory behind each attack, the attacks explained in this book are launched against real devices in my lab.

Hacking: A Beginners Guide to Your First Computer Hack; Learn to Crack a Wireless Network, Basic Security Penetration Made Easy - Kevin White 2018-02-22

Hacking will demand your full dedication and interest and also a desire and a craving for knowledge and constant advancement. If your goal is to be a hacker, this is the book to start with!. Today only, get this bestseller for a special price. This book contains proven steps and strategies on how to hack a Wireless Network, carry out a penetration test and so much more. It gives an insight to the most used hacking techniques and how to develop your basic skills Here Is A Preview Of What You'll Learn... What is Hacking? How to Crack Wireless Networks Kali Linux Linux Hacking Tools Penetration Test Your First Hack: WEP Network And basically everything you need to help you to start your Hacking career Get your copy today! Take action today and buy this book now at a special price!

WarDriving and Wireless Penetration Testing - Chris Hurley 2007

Provides information on analyzing wireless networks through wardriving and penetration testing.

Maximum Wireless Security - Cyrus Peikari 2003

0672324881.ld A detailed guide to wireless vulnerabilities, written by authors who have first-hand experience with wireless crackers and their techniques. Wireless technology and Internet security are the two fastest growing technology sectors. Includes a bonus CD packed with powerful free and demo tools to audit wireless networks. Reviewed and endorsed by the author of WEPCrack, a well-known tool for breaking 802.11 WEP encryption keys. *Maximum Wireless Security* is a practical handbook that reveals the techniques and tools crackers use to break into wireless networks, and that details the steps network administrators need to take to secure their systems. The authors provide information to satisfy the experts hunger for in-depth information with actual source code, real-world case studies, and step-by-step configuration recipes. The book includes detailed, hands-on information that is currently unavailable in any printed text -- information that has been gleaned from the authors work with real wireless hackers ("war drivers"), wireless security developers, and leading security experts. Cyrus Peikari is the chief technical officer for VirusMD Corporation and has several patents pending in the anti-virus field. He has published several consumer security software programs, including an encrypted instant messenger, a personal firewall, a content filter and a suite of network connectivity tools. He is a repeat speaker at Defcon. Seth Fogie, MCSE, is a former United State Navy nuclear engineer. After retiring, he has worked as a technical support specialist for a major Internet service provider. He is currently the director of engineering at VirusMD Corporation, where he works on next-generation wireless security software. He has been invited to speak at Defcon in 2003.

Wireless Home Networking For Dummies - Danny Briere 2011-02-08

Wireless home networks are better than ever! The emergence of new industry standards has made them easier, more convenient, less expensive to own and operate. Still, you need to know what to look for (and look out for), and the expert guidance you'll find in *Wireless Home Networks For Dummies*, 3rd Edition helps you ensure that your wire-free life is also a hassle-free life! This user-friendly, plain-English guide delivers all of the tips, tricks, and knowledge you need to plan your wireless home network, evaluate and select the equipment that will work best for you, install and configure your wireless network, and much

more. You'll find out how to share your Internet connection over your network, as well as files, printers, and other peripherals. And, you'll learn how to avoid the "gotchas" that can creep in when you least expect them. Discover how to: Choose the right networking equipment Install and configure your wireless network Integrate Bluetooth into your network Work with servers, gateways, routers, and switches Connect audiovisual equipment to your wireless network Play wireless, multiuser computer games Establish and maintain your network's security Troubleshoot networking problems Improve network performance Understand 802.11n Whether you're working with Windows PCs, Mac OS X machines, or both Wireless Home Networking For Dummies, 3rd Edition, makes it fast and easy to get your wireless network up and running—and keep it that way!

Wireless Hacking with Kali Linux - Hugo Hoffman 2020-04-04

Wireless penetration testing has become a key skill in the range of the professional penetration testers. This book will teach you how to Hack any Wireless Networks! If you are interested in Wireless Penetration testing using Kali Linux, this book is for you! This book will cover: -What Wireless PenTest Tools you must have-What Wireless Adapters & Wireless Cards are best for Penetration Testing-How to Install Virtual Box & Kali Linux-Wireless Password Attacks-WPA/WPA2 Dictionary Attack-Countermeasures to Dictionary Attacks-Deploying Passive Reconnaissance with Kali Linux-Countermeasures Against Passive Reconnaissance -How to Decrypt Traffic with Wireshark-How to implement MITM Attack with Ettercap-Countermeasures to Protect Wireless Traffic-How to Secure Ad Hoc Networks-How to Physically Secure your Network -How to deploy Rogue Access Point using MITM Attack-How to use Wi-Spy DGx & Chanalyzer-How to implement Deauthentication Attack against a Rogue AP-How to deploy Evil Twin Deauthentication Attack with mdk3-How to deploy DoS Attack with MKD3-Encryption Terminology & Wireless Encryption Options-WEP Vulnerabilities & TKIP Basics-Defining CCMP & AES-Wireless Authentication Methods & Processes-4-Way Handshake & Fast Roaming Process-Message Integrity, Data Protection and Data Tampering-MIC Code Packet Spoofing Countermeasures and more...BUY THIS BOOK NOW AND GET STARTED TODAY!

Hands on Hacking - Matthew Hickey 2020-09-16

A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker's perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you'll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. An introduction to the same hacking techniques that malicious hackers will use against an organization Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws Based on the tried and tested material used to train hackers all over the world in the art of breaching networks Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.

Backtrack 5 Wireless Penetration Testing - Vivek Ramachandran 2011-09-09

Wireless has become ubiquitous in today's world. The mobility and flexibility provided by it makes our lives more comfortable and productive. But this comes at a cost - Wireless technologies are inherently insecure and can be easily broken. BackTrack is a penetration testing and security auditing distribution that comes with a myriad of wireless networking tools used to simulate network attacks and detect security loopholes.

Backtrack 5 Wireless Penetration Testing Beginner's Guide will take you through the journey of becoming a Wireless hacker. You will learn various wireless testing methodologies taught using live examples, which you will implement throughout this book. The engaging practical sessions very gradually grow in complexity giving you enough time to ramp up before you get to advanced wireless attacks. This book will take you through the basic concepts in Wireless and creating a lab environment for your experiments to the business of different lab sessions in wireless security basics, slowly turn on the heat and move to more complicated scenarios, and finally end your journey by conducting bleeding edge wireless attacks in your lab. There are many interesting and new things that you will learn in this book - War Driving, WLAN packet sniffing, Network Scanning, Circumventing hidden SSIDs and MAC filters, bypassing Shared Authentication, Cracking WEP and WPA/WPA2 encryption, Access Point MAC spoofing, Rogue Devices, Evil Twins, Denial of Service attacks, Viral SSIDs, HoneyPot and Hotspot attacks, Caffe Latte WEP Attack, Man-in-the-Middle attacks, Evading Wireless Intrusion Prevention systems and a bunch of other cutting edge wireless attacks. If you were ever curious about what wireless security and hacking was all about, then this book will get you started by providing you with the knowledge and practical know-how to become a wireless hacker. Hands-on practical guide with a step-by-step approach to help you get started immediately with Wireless Penetration Testing

Firewalls For Dummies - Brian Komar 2003-09-24

What an amazing world we live in! Almost anything you can imagine can be researched, compared, admired, studied, and in many cases, bought, with the click of a mouse. The Internet has changed our lives, putting a world of opportunity before us. Unfortunately, it has also put a world of opportunity into the hands of those whose motives are less than honorable. A firewall, a piece of software or hardware that erects a barrier between your computer and those who might like to invade it, is one solution. If you've been using the Internet for any length of time, you've probably received some unsavory and unsolicited e-mail. If you run a business, you may be worried about the security of your data and your customers' privacy. At home, you want to protect your personal information from identity thieves and other shady characters. Firewalls For Dummies® will give you the lowdown on firewalls, then guide you through choosing, installing, and configuring one for your personal or business network. Firewalls For Dummies® helps you understand what firewalls are, how they operate on different types of networks, what they can and can't do, and how to pick a good one (it's easier than identifying that perfect melon in the supermarket.) You'll find out about Developing security policies Establishing rules for simple protocols Detecting and responding to system intrusions Setting up firewalls for SOHO or personal use Creating demilitarized zones Using Windows or Linux as a firewall Configuring ZoneAlarm, BlackICE, and Norton personal firewalls Installing and using ISA server and FireWall-1 With the handy tips and hints this book provides, you'll find that firewalls are nothing to fear - that is, unless you're a cyber-crook! You'll soon be able to keep your data safer, protect your family's privacy, and probably sleep better, too.

Hacking For Dummies® - Kevin Beaver 2009-12-18

A new edition of the bestselling guide—now updated to cover the latest hacks and how to prevent them! It's bad enough when a hack occurs—stealing identities, bank accounts, and personal information. But when the hack could have been prevented by taking basic security measures—like the ones described in this book—somehow that makes a bad situation even worse. This beginner guide to hacking examines some of the best security measures that exist and has been updated to cover the latest hacks for Windows 7 and the newest version of Linux. Offering increased coverage of Web application hacks, database hacks, VoIP hacks, and mobile computing hacks, this guide addresses a wide range of vulnerabilities and how to identify and prevent them. Plus, you'll examine why ethical hacking is oftentimes the only way to find security flaws, which can then prevent any future malicious attacks. Explores the malicious hacker's mindset so that you can counteract or avoid attacks completely Covers developing strategies for reporting vulnerabilities, managing security changes, and putting anti-hacking policies and procedures in place Completely updated to examine the latest hacks to Windows 7 and the newest version of Linux Explains ethical hacking and why it is essential Hacking For Dummies, 3rd Edition shows you how to put all the necessary security measures in place so that you avoid becoming a victim of malicious hacking.

Hacking For Dummies - Kevin Beaver 2018-06-27

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.

802.11 Wireless Networks: The Definitive Guide - Matthew S. Gast 2005-04-25

As we all know by now, wireless networks offer many advantages over fixed (or wired) networks. Foremost on that list is mobility, since going wireless frees you from the tether of an Ethernet cable at a desk. But that's just the tip of the cable-free iceberg. Wireless networks are also more flexible, faster and easier for you to use, and more affordable to deploy and maintain. The de facto standard for wireless networking is the 802.11 protocol, which includes Wi-Fi (the wireless standard known as 802.11b) and its faster cousin, 802.11g. With easy-to-install 802.11 network hardware available everywhere you turn, the choice seems simple, and many people dive into wireless computing with less thought and planning than they'd give to a wired network. But it's wise to be familiar with both the capabilities and risks associated with the 802.11 protocols. And *802.11 Wireless Networks: The Definitive Guide, 2nd Edition* is the perfect place to start. This updated edition covers everything you'll ever need to know about wireless technology. Designed with the system administrator or serious home user in mind, it's a no-nonsense guide for setting up 802.11 on Windows and Linux. Among the wide range of topics covered are discussions on: deployment considerations network monitoring and performance tuning wireless security issues how to use and select access points network monitoring essentials wireless card configuration security issues unique to wireless networks With wireless technology, the advantages to its users are indeed plentiful. Companies no longer have to deal with the hassle and expense of wiring buildings, and households with several computers can avoid fights over who's online. And now, with *802.11 Wireless Networks: The Definitive Guide, 2nd Edition*, you can integrate wireless technology into your current infrastructure with the utmost confidence.

Hacking for Beginners - Julian James McKinnon 2021-03-29

-- 55% OFF for Bookstores! -- Hacking is a term most of us shudder away from; we assume that it is only for those who have lots of programming skills and loose morals and that it is too hard for us to learn how to use it. But what if you could work with hacking like a good thing, as a way to protect your own personal information and even the information of many customers for a large business? This guidebook is going to spend some time taking a look at the world of hacking and some of the great techniques that come with this type of process as well. Whether you are an unethical or ethical hacker, you will use a lot of the same techniques, and this guidebook is going to explore them in more detail along the way, turning you from a novice to a professional in no time. Some of the different topics we will look at concerning hacking in this guidebook includes: The basics of hacking and some of the benefits of learning how to use this programming technique. The different types of hackers, why each one is important, and how they are different from one another. How to work with your own penetration test. The importance of strong passwords and how a professional hacker will attempt to break through these passwords. A look at how to hack through a website of any company that doesn't add in the right kind of security to the mix. A look at how to hack through the different wireless networks that are out there to start a man-in-the-middle attack or another attack. Some of the other common attacks that we need to work with including man-in-the-middle, denial-of-service attack malware, phishing, and so much more. Some of the steps that you can take in order to ensure that your network will stay safe and secure, despite all of the threats out there. Hacking is a term that most of us do not know that much about. We assume that only a select few can use hacking to gain their own personal advantage and that it is too immoral or too hard for most of us to learn. But learning a bit about hacking can actually be the best way to keep your own network safe. Are you ready to learn more about hacking and what it can do to the safety and security of your personal or business

network?

Hacking - Alex Wagner 2017-06-15

The Ultimate Guide to the 17 Most Dangerous Hacking Attacks ## ## ## Do you want to learn about today's most sophisticated Hacking attacks? Do you want to know more about Cyber criminals and their operations? Do you want to learn about Robot Networks, Trojans & Ransomware? In this book you will learn about: ADVWARE | SPYWARE | MALWARE | MAN IN THE MIDDLE | LOCKYTRAFFIC REDIRECTION | PAYLOAD INJECTION | ARP POISONING WORMS ROGUE WIRELESS ACCESS POINTS | MISS-ASSOCIATION ATTACKS DE-AUTHENTICATION ATTACKS | COLLISION ATTACKS | REPLAY ATTACKS PHISHING | VISHING | WHALING | SMISHING | SPEAR PHISHING DUMPSTER DIVING | SHOULDER SURFING | BRUTE FORCE ATTACK DICTIONARY ATTACKS | RAINBOW TABLES | KEYSTROKE LOGGINGS SPOOFING | SOCIAL ENGINEERING | SPAMMING | SQL INJECTIONS DDOS ATTACKS | TCP SYN FLOOD ATTACK | PING OF DEATH | VIRUSES ROOTKITS | LOGIC BOMBS | TROJAN HORSES WANNAYCRY RANSOMWARE BOTNETS

Wireless Hacking - Evan Lane 2017-03

How to Hack Wireless Networks - for Beginner's Hacking is the method used to get into a system without the administrator ever knowing. This is usually done to gain access to information that may be located on the server. This can either be done maliciously or for educational purposes. Wireless hacking is going to be the act of getting into someone's wireless network so that you can get onto their computer and find out various pieces of information. Wireless hacking is just another method that hackers use on a long list of hacking methods. With wireless hacking, you are going to be using various methods and programs to achieve a goal. You need to keep in mind that when you are hacking a wireless network, you must be quick and you have to be stealthy or else you are going to get caught and when you get caught. In this book, you are going to learn things such as: Getting information on a target Scanning ports Common programs used for hacking Vulnerabilities And more The purpose of this book is to give you the knowledge on wireless hacking that you are seeking and for you to use it in an educational manner, not a malicious one.

Kali Linux Wireless Penetration Testing: Beginner's Guide - Vivek Ramachandran 2015-03-30

If you are a security professional, pentester, or anyone interested in getting to grips with wireless penetration testing, this is the book for you. Some familiarity with Kali Linux and wireless concepts is beneficial.

Kismet Hacking - Frank Thornton 2008-08-08

Kismet is the industry standard for examining wireless network traffic, and is used by over 250,000 security professionals, wireless networking enthusiasts, and WarDriving hobbyists. Unlike other wireless networking books that have been published in recent years that geared towards Windows users, Kismet Hacking is geared to those individuals that use the Linux operating system. People who use Linux and want to use wireless tools need to use Kismet. Now with the introduction of Kismet NewCore, they have a book that will answer all their questions about using this great tool. This book continues in the successful vein of books for wireless users such as WarDriving: Drive, Detect Defend. *Wardrive Running Kismet from the BackTrack Live CD *Build and Integrate Drones with your Kismet Server *Map Your Data with GPSMap, KisMap, WiGLE and GpsDrive

Hacking Wireless Networks - Andreas Kolokithas 2015-03-05

Are you tired of buying security books and at the end discover that they contain only theory and no practical examples at all? Do you want to setup your own hacking lab and learn through practice? If yes, then this is the book for you! *Hacking Wireless Networks - The ultimate hands-on guide*, is a book written for people who seek to practice the techniques of assessing the security of wireless infrastructures. Through 30 real life scenarios and more than 300 figures the book examines in details the following areas: - Discovery and Profiling of wireless networks - Denial of Service attacks - Attacks against WEP secured wireless networks - Attacks against WPA/WPA2 secured wireless networks - Bypass techniques for popular Authentication mechanisms - Encryption keys cracking using special techniques - Attacks against the Access Point's management interface - Attacks against special security features like WPS - Stealthy techniques to avoid getting caught by wireless IDS Now that the world agrees that wireless security is central to computer security, it is time to put theory into practice.

Hacking] - Julian James McKinnon 2021-03-08

-- 55% OFF for Bookstores -- Hacking: three books in one Would you like to learn more about the world of hacking and Linux? Yes? Then you are in the right place.... Included in this book collection are: Hacking for Beginners: A Step by Step Guide to Learn How to Hack Websites, Smartphones, Wireless Networks, Work with Social Engineering, Complete a Penetration Test, and Keep Your Computer Safe Linux for Beginners: A Step-by-Step Guide to Learn Architecture, Installation, Configuration, Basic Functions, Command Line and All the Essentials of Linux, Including Manipulating and Editing Files Hacking with Kali Linux: A Step by Step Guide with Tips and Tricks to Help You Become an Expert Hacker, to Create Your Key Logger, to Create a Man in the Middle Attack and Map Out Your Own Attacks Hacking is a term most of us shudder away from. We assume that it is only for those who have lots of programming skills and loose morals and that it is too hard for us to learn how to use it. But what if you could work with hacking like a good thing, as a way to protect your own personal information and even the information of many customers for a large business? This guidebook is going to spend some time taking a look at the world of hacking, and some of the great techniques that come with this type of process as well. Whether you are an unethical or ethical hacker, you will use a lot of the same techniques, and this guidebook is going to explore them in more detail along the way, turning you from a novice to a professional in no time. Are you ready to learn more about hacking and what you are able to do with this tool?

Networking For Dummies - Doug Lowe 2020-07-14

Set up a secure network at home or the office Fully revised to cover Windows 10 and Windows Server 2019, this new edition of the trusted *Networking For Dummies* helps both beginning network administrators and home users to set up and maintain a network. Updated coverage of broadband and wireless technologies, as well as storage and back-up procedures, ensures that you'll learn how to build a wired or wireless network, secure and optimize it, troubleshoot problems, and much more. From connecting to the Internet and setting up a wireless network to solving networking problems and backing up your data—this #1 bestselling guide covers it all. Build a wired or wireless network Secure and optimize your network Set up a server and manage Windows user accounts Use the cloud—safely Written by a seasoned technology author—and jam-packed with tons of helpful step-by-step instructions—this is the book network administrators and everyday computer users will turn to again and again.

Learn Ethical Hacking from Scratch - Zaid Sabih 2018-07-31

Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the

different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

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

Wireless Networks For Dummies - Barry D. Lewis 2004-10-27

You've probably heard the expression, "It's timeto cut the cord." Well, it may be time to "cut thecables" at your office and free yourself from your desk andcomputer. Wireless networks are the waves of thefuture—literally. *Wireless Networks For Dummies* guidesyou from design through implementation to ongoing protection ofyour system and your information so you can: Remain connected to the office in airports and hotels Access the Internet and other network resources in thelunchroom, conference room, or anywhere there's an accesspoint Use your PDA or laptop to query your database from thewarehouse or the boardroom Check e-mail wirelessly when you're on the road Get rid of the cable clutter in your office *Wireless Networks For Dummies* was coauthored by Barry D.Lewis, CISSP, and Peter T. Davis, who also coauthored *ComputerSecurity For Dummies*. Barry Lewis is president of aninformation security consulting firm and an internationally knownleader of security seminars. Peter Davis is founder of a firmspecializing in the security, audit, and control of information.Together, they cut through the cables, clutter, and confusion andhelp you: Get off to a quick start and get mobile with IrDA (InfraredData Association) and Bluetooth Perform a site survey and select the right standard, mode,access point, channel and antenna Check online to verify degree of interoperability of devicesfrom various vendors Install clients and set up roaming Combat security threats such as war driving, jamming,hijacking, and man-in-the-middle attacks Implement security and controls such as MAC (Media AccessControl) and protocol filtering, WEP (Wireless Equivalent Privacy),WPA, (Wi-Fi Protected Access), EAP (Extensible AuthenticationProtocol), and VPN (Virtual Private Network) Set up multiple access points to form a larger wirelessnetwork Complete with suggestions of places to get connected, Web siteswhere you can get more information, tools you can use to monitorand improve security, and more, *Wireless Networks ForDummies* helps you pull the plug and go wireless!