hacker ethic, hacker culture, digital freedom, open source philosophy, cyber security values

The Hacker Ethic

#hacker ethic #hacker culture #digital freedom #open source philosophy #cyber security values

Explore the fundamental 'Hacker Ethic,' a set of guiding principles and values that shaped early hacker culture and the digital world. Understand its core tenets, from digital freedom and open access to information, to the collaborative spirit that underpins the open source philosophy and much of modern computing.

The Hacker Ethos

The Hacker Ethos is a condensed, easy-to-read guidebook on the subject of Ethical Hacking and Penetration Testing, the legal procedure for testing computer security by simulating real cyber attacks. Written by an expert in Computer Science and Information Security with ten years of experience in his field at the time of writing, The Hacker Ethos was specifically designed to be put in the hands of the beginner-level hacker, IT professional, and hopeful IT security researcher. This book covers the fundamental concepts of computer science and introduces the core knowledge that is required by all security professionals in the IT industry. The primary goal of the book is to instill what is known as the "Hacker Ethic" into the reader, a philosophy based on the ideal of free information, knowledge, and speech. Its very foundation is the principle of what it means to be a true hacker, an expert in computers at the most primal level, ready to explore new concepts and techniques without ever losing the hunger for knowledge. The reader is encouraged to understand that Hacking is not easy, not is it a singular concept. It encompasses a vast library, covering every field of technology that includes programming, exploitation, web security and design, application security, viruses and malware, networking, wireless technology, telecommunication, phone technology, cellular technology, robotics, and everything that can be classified under the school of computing. Hackers are jacks of all trades, masters of none, but always striving to become so. Contained in this book are the topics of hacker ethics, and details the unwritten law of the Hacker Underground. It casts a bright spotlight on the Hacker Mythos, the subculture of hacking, and dispels the mystique of the Deep Web. It teaches the core techniques of hacking, and what is known as the Hacker Methodology, the list of techniques used my professional security testers and cyber-criminals alike to attack their targets. It teaches critical research techniques, heavily emphasizing self-study, and provides dozens of free resources on the various subjects and schools of hacking, including: programming, web hacking, service and application exploitation, malware development, password cracking, Denial-of-Service, Wireless and physical network penetration, cryptography. Lastly, the book provides a massive toolkit of professional and privately used hacking tools, all completely free, and teaches the reader how to acquire new tools for themselves. This book has been hailed by readers as "the best and easiest beginner's guide to hacking of the millennium," meticulously having collected and organized every necessary tool, technique, and tutorial that beginners of the IT Security field absolutely must know. Its primary lesson is "teach you how to teach yourself," an invaluable skill that drives the field of technology and security more than any other. That a hacker who cannot learn on his own will never last. This book requires strong dedication and an insatiable desire to learn. Make no mistake, its contents will not be simple by any means, as much as it strives to make them easy to understand. There is no "hacking tools that does it all" and there is no magic trick to learning everything. Should you choose to continue, be prepared to adopt the true meaning of The Hacker Ethos, our creed: Information is meant to be free for everyone. Privacy is a right, hard earned; not a commodity, cheaply bought. Censorship is a tyranny delivered by silence. The Internet embodies freedom. Immerse yourself in it. Never stop learning; never stop teaching. Don't learn to hack; hack to learn. "We Are All Alike" Good luck on your Journey, - True Demon

The Hacker Ethic and the Spirit of the Information Age

The Hacker Ethic takes us on a journey through fundamental questions about life in the information age - a trip of constant surprises, after which our time and our lives can be seen from unexpected perspectives.Nearly a century ago, Max Weber's The Protestant Ethic and the Spirit of Capitalism articulated the animating spirit of the industrial age, the Protestant ethic. In the original meaning of the word, hackers are enthusiastic computer programmers who share their work with others; they are not computer criminals. Now Pekka Himanen - together with Linus Torvalds and Manuel Castells - articulates how hackers represent a new opposing ethos for the information age.Underlying hackers' technical creations - such as the Internet and the personal computer, which have become symbols of our time - are the hacker values that produced them. These values promote passionate and freely rhythmed work; the belief that individuals can create great things by joining forces in imaginative ways; and the need to maintain our existing ethical ideals, such as privacy and equality, in our new increasingly technologized society.

The Hacker Ethic

The Hacker Ethic takes us on a journey through fundamental questions about life in the information age - a trip of constant surprises, after which our time and our lives can be seen from unexpected perspectives.Nearly a century ago, Max Weber's The Protestant Ethic and the Spirit of Capitalism articulated the animating spirit of the industrial age, the Protestant ethic. In the original meaning of the word, hackers are enthusiastic computer programmers who share their work with others; they are not computer criminals. Now Pekka Himanen - together with Linus Torvalds and Manuel Castells - articulates how hackers represent a new opposing ethos for the information age.Underlying hackers' technical creations - such as the Internet and the personal computer, which have become symbols of our time - are the hacker values that produced them. These values promote passionate and freely rhythmed work; the belief that individuals can create great things by joining forces in imaginative ways; and the need to maintain our existing ethical ideals, such as privacy and equality, in our new increasingly technologized society.

The Birth Of The Hacker Ethic

If you work within the field of computing and have an interest in how and why things have developed the way they have, then this book is one that you really should get. In this context, "Hacker" is not a pejorative term; it does not refer to the people that set out to maliciously damage systems, but rather to those that tried to understand how and why things work the way they do, by deconstructing them and then trying to make them work more efficiently. The author provides details of how many of the pioneers of modern computing honed their skills; the relationships between the various people and also try to give an insight into their thinking. It's clear that in many cases, no one was particularly driven to go down a particular route, they were just trying to see what they could do. It's equally clear that some of the development was the result of external forces from people that probably knew little if anything about the potential of the coming computer revolution. This book provides the origins and history of electronic intruders that includes the first written "code of ethics" of the computer underground.

The Timeline Of Computer Hackers And The Hacker Ethic

If you work within the field of computing and have an interest in how and why things have developed the way they have, then this book is one that you really should get. In this context, "Hacker" is not a pejorative term; it does not refer to the people that set out to maliciously damage systems, but rather to those that tried to understand how and why things work the way they do, by deconstructing them and then trying to make them work more efficiently. The author provides details of how many of the pioneers of modern computing honed their skills; the relationships between the various people and also try to give an insight into their thinking. It's clear that in many cases, no one was particularly driven to go down a particular route, they were just trying to see what they could do. It's equally clear that some of the development was the result of external forces from people that probably knew little if anything about the potential of the coming computer revolution. This book provides the origins and history of electronic intruders that includes the first written "code of ethics" of the computer underground.

Hackers

This 25th anniversary edition of Steven Levy's classic book traces the exploits of the computer revolution's original hackers -- those brilliant and eccentric nerds from the late 1950s through the early '80s who took risks, bent the rules, and pushed the world in a radical new direction. With updated material from noteworthy hackers such as Bill Gates, Mark Zuckerberg, Richard Stallman, and Steve Wozniak, Hackers is a fascinating story that begins in early computer research labs and leads to the first home computers. Levy profiles the imaginative brainiacs who found clever and unorthodox solutions to computer engineering problems. They had a shared sense of values, known as "the hacker ethic," that still thrives today. Hackers captures a seminal period in recent history when underground activities blazed a trail for today's digital world, from MIT students finagling access to clunky computer-card machines to the DIY culture that spawned the Altair and the Apple II.

Coding Freedom

Who are computer hackers? What is free software? And what does the emergence of a community dedicated to the production of free and open source software--and to hacking as a technical, aesthetic, and moral project--reveal about the values of contemporary liberalism? Exploring the rise and political significance of the free and open source software (F/OSS) movement in the United States and Europe, Coding Freedom details the ethics behind hackers' devotion to F/OSS, the social codes that guide its production, and the political struggles through which hackers question the scope and direction of copyright and patent law. In telling the story of the F/OSS movement, the book unfolds a broader narrative involving computing, the politics of access, and intellectual property. E. Gabriella Coleman tracks the ways in which hackers collaborate and examines passionate manifestos, hacker humor, free software project governance, and festive hacker conferences. Looking at the ways that hackers sustain their productive freedom, Coleman shows that these activists, driven by a commitment to their work, reformulate key ideals including free speech, transparency, and meritocracy, and refuse restrictive intellectual protections. Coleman demonstrates how hacking, so often marginalized or misunderstood, sheds light on the continuing relevance of liberalism in online collaboration.

Hacking the Hacker

Meet the world's top ethical hackers and explore the tools of the trade Hacking the Hacker takes you inside the world of cybersecurity to show you what goes on behind the scenes, and introduces you to the men and women on the front lines of this technological arms race. Twenty-six of the world's top white hat hackers, security researchers, writers, and leaders, describe what they do and why, with each profile preceded by a no-experience-necessary explanation of the relevant technology. Dorothy Denning discusses advanced persistent threats, Martin Hellman describes how he helped invent public key encryption, Bill Cheswick talks about firewalls, Dr. Charlie Miller talks about hacking cars, and other cybersecurity experts from around the world detail the threats, their defenses, and the tools and techniques they use to thwart the most advanced criminals history has ever seen. Light on jargon and heavy on intrigue, this book is designed to be an introduction to the field; final chapters include a guide for parents of young hackers, as well as the Code of Ethical Hacking to help you start your own journey to the top. Cybersecurity is becoming increasingly critical at all levels, from retail businesses all the way up to national security. This book drives to the heart of the field, introducing the people and practices that help keep our world secure. Go deep into the world of white hat hacking to grasp just how critical cybersecurity is Read the stories of some of the world's most renowned computer security experts Learn how hackers do what they do—no technical expertise necessary Delve into social engineering, cryptography, penetration testing, network attacks, and more As a field, cybersecurity is large and multi-faceted—yet not historically diverse. With a massive demand for qualified professional that is only going to grow, opportunities are endless. Hacking the Hacker shows you why you should give the field a closer look.

Hacking

Be a Hacker with Ethics

Ethical Hacking

A hands-on guide to hacking computer systems from the ground up, from capturing traffic to crafting sneaky, successful trojans. A crash course in modern hacking techniques, Ethical Hacking is already being used to prepare the next generation of offensive security experts. In its many hands-on labs, you'll explore crucial skills for any aspiring penetration tester, security researcher, or malware analyst. You'll begin with the basics: capturing a victim's network traffic with an ARP spoofing attack and then viewing it in Wireshark. From there, you'll deploy reverse shells that let you remotely run commands on a victim's computer, encrypt files by writing your own ransomware in Python, and fake emails like the ones used in phishing attacks. In advanced chapters, you'll learn how to fuzz for new vulnerabilities, craft trojans and rootkits, exploit websites with SQL injection, and escalate your privileges to extract credentials, which you'll use to traverse a private network. You'll work with a wide range of professional penetration testing tools—and learn to write your own tools in Python—as you practice tasks like: Deploying the Metasploit framework's reverse shells and embedding them in innocent-seeming files Capturing passwords in a corporate Windows network using Mimikatz Scanning (almost) every device on the internet to find potential victims Installing Linux rootkits that modify a victim's operating system Performing advanced Cross-Site Scripting (XSS) attacks that execute sophisticated JavaScript payloads Along the way, you'll gain a foundation in the relevant computing technologies. Discover how advanced fuzzers work behind the scenes, learn how internet traffic gets encrypted, explore the inner mechanisms of nation-state malware like Drovorub, and much more. Developed with feedback from cybersecurity students, Ethical Hacking addresses contemporary issues in the field not often covered in other books and will prepare you for a career in penetration testing. Most importantly, you'll be able to think like an ethical hacker`: someone who can carefully analyze systems and creatively gain access to them.

Ethical Hacking

This book is written for those people who want to hack systems to test identify the security holes and vulnerabilities of thosesystems. This book outlines different tricks and techniques that an ethical hacker can use to assess the security of the systems, identify vulnerabilities and fix those vulnerabilities. This is done to prevent any malicious attacks against the system.The hacking we talk about in this book is professional, above board and is a legal type of testing. It is for this reason that it is called ethical hacking. Network and computer security is a complex subject, which constantly changes. You have to stay on top of it to ensure that the information you own is secure from the crackers or criminal hackers.Ethical hacking, also called white-hat hacking or penetration testing, is a tool that will help you ensure that the information system you use is truly secure. Over the course of this book, you will gather information on the different tools and software you can use to run an ethical hacking program. There are some programs in this book that you can use to start off the ethical hacking process.In this book you will learn: What exactly is Ethical HackingThe dangers that your system can face through attacksThe Ethical Hacking Process and what it meansUnderstanding a hackers mindsetAn introduction to PythonAnd much much more!

A Tour Of Ethical Hacking

If you are a beginner and want to become a Hacker then this book can help you a lot to understand the hacking. This book contains several techniques of hacking with their complete step by step demonstration which will be better to understand and it can also help you to prevent yourself from hacking or cyber crime also.

The New Hacker's Dictionary, third edition

This new edition of the hacker's own phenomenally successful lexicon includes more than 100 new entries and updates or revises 200 more. This new edition of the hacker's own phenomenally successful lexicon includes more than 100 new entries and updates or revises 200 more. Historically and etymologically richer than its predecessor, it supplies additional background on existing entries and clarifies the murky origins of several important jargon terms (overturning a few long-standing folk etymologies) while still retaining its high giggle value. Sample definition hacker n. [originally, someone who makes furniture with an axe] 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating {hack value}. 4. A person who is good at programming quickly. 5. An expert at a particular program, or one who frequently does work using it or on it; as in `a UNIX hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) 6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example. 7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. 8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term is {cracker}. The term 'hacker' also tends to connote membership in the global community defined by the net (see {network, the} and {Internet address}). It also implies that the person described is seen to subscribe to some version of the hacker ethic (see {hacker ethic, the}). It is better to be described as a hacker by others than to describe oneself that way. Hackers consider themselves something of an elite (a meritocracy based on ability), though one to which new members are gladly welcome. There is thus a certain ego satisfaction to be had in identifying yourself as a hacker (but if you claim to be one and are not, you'll quickly be labeled {bogus}). See also {wannabee}.

The Ethical Hack

There are many books that detail tools and techniques of penetration testing, but none of these effectively communicate how the information gathered from tests should be analyzed and implemented. Until recently, there was very little strategic information available to explain the value of ethical hacking and how tests should be performed in order t

The Ethics of Cybersecurity

This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.

The Ethics of Hacking

Political hackers, like the Anonymous collective, have demonstrated their willingness to use political violence to further their agendas. However, many of their causes are intuitively good things to fight for. This book argues that when the state fails to protect people, hackers can intervene. It highlights the space for hackers to operate as legitimate actors; details what actions are justified towards what end; outlines mechanisms to aid ethically justified decisions; and directs the political community on how to react. Applying this framework to hacking operations including the Arab Spring, police brutality in the USA, and Nigerian and Ugandan homophobic legislation, it offers a unique contribution to hacking as a contemporary political activity.

Ethical Hacking for Begginers

Do you know if you were hacked? Do you know if some personal information was stolen from your system or account? Have you always wanted to learn how to protect your system from such attacks? If you answered yes to all these questions, you've come to the right place.Unlike malicious hacking, ethical hacking is a legal way to test the vulnerabilities of a system. Many organizations are still wary of ethical hackers, and they have every right to be since some hackers lie for their own benefit. That being said, many organizations are now searching for ethical hackers because they want to identify a way to protect themselves and their customers and employees.Over the course of the book, you will learn more about what ethical hacking is and will begin to comprehend the different types of attacks that an ethical hacker can perform on a system. This book will talk about: What ethical hacking is and how it is different from malicious hackingWhy it's important to hack a systemWhat the different phases of ethical hacking areThe steps that an ethical hacker must take to protect himselfThe different skills an ethical hacker must haveThe different tools that a hacker can utilize to test a systemDifferent types of attacks that can be performed on a systemHow the hacker should protect a system from such attacksThis book provides numerous examples of different attacks and also includes some exercises that you can follow when you're performing these attacks for the first time. It is important to remember that ethical hacking is becoming one of the most sought-after professions because every organization is looking for a way to protect their data

Ethical Hacking

Ethical hacking is a profession that has gained popularity in the last few years. Network security and cybersecurity have become important aspects of every business. Hackers have always hacked the network or server of an organization to obtain personal information that can derail the company. It is for this reason that organizations have begun to hire the professionals to help them maintain this security. These professionals are ethical hackers. An ethical hacker will run numerous tests and hacks that another cracker may use to obtain sensitive information about the system. As an ethical hacker, you'll learn how to beat the black hat hacker at his own game! Learn to recognize and counter social engineering attacks, trojan horses, malware and more.In this book you'll discover many unexpected computer vulnerabilities as we categorize the systems in terms of vulnerability. You may be surprised to learn that simple gaps under an office door can put your organization at risk for being hacked! In additional, you will learn in step by step detail how you can hack into a Windows operating system. The pre-attack stage involves footprinting, enumerations, and scanning, while the attack stage covers password cracking, keyloggers and spyware, threats and vulnerability scanning, and steganography. Penetration testing is a vital aspect of ethical hacking. During testing, the ethical hacker simulates the ways intruders gain access to a company's system. The book explains the different ways in which it is used and the countermeasures an ethical hacker can use to foil the work of the hacker. If you're interested in being an ethical hacker, or are just curious about the field of hacking, then this book is for you! Click the Buy Now button to get started.Grab this 3 in 1 bundle today and secure your Cyber networks!

The Ethics of Hacking

Political hackers, like the infamous Anonymous collective, have demonstrated their willingness to use political violence to further their agendas. However, many of their causes – targeting terrorist groups, fighting for LGBTQ+ rights, and protecting people’s freedom of expression, autonomy and privacy – are intuitively good things to fight for. This book will create a new framework that argues that when the state fails to protect people, hackers can intervene and evaluates the hacking based on the political or social circumstances. It highlights the space for hackers to operate as legitimate actors; guides hacker activity by detailing what actions are justified toward what end; outlines mechanisms to aid hackers in reaching ethically justified decisions; and directs the political community on how to react to these political hackers. Applying this framework to the most pivotal hacking operations within the last two decades, including the Arab Spring, police brutality in the USA and the Nigerian and Ugandan governments’ announcements of homophobic legislation, it offers a unique contribution to conceptualising hacking as a contemporary political activity.

ETHICAL HACKING FOR BEGINNERS

Would you like to learn to be an ethical hacker? Would you like to acquire computer skills for a useful purpose? Ethical hackers, called "white hat" or "ethical hackers". Their main activity consists in simulating malicious hacker attacks to find vulnerabilities in the systems before real attacks, trying to solve the problems encountered. Computer skills in this field are in high demand in the world of work, many big companies worried about their IT vulnerability, they always look for heavier "hackers" hired to protect their networks, their computers and their data from cyber-attacks. Almost endless are the uses that a specific computer knowledge in this sector can do. The guide is designed to guide you through a step-by-step process, useful for learning the computer processes necessary to become an ethical hacker. IN THIS GUIDE YOU WILL LEARN: - What's a Hĸĸ? - WhCDoes a HĸĸHack? - The M▹U Common Targets - THE PRACTICAL GUIDE TO COMPUTER HACKING - HW YU CN PRTT! YURLF - THL! HACKER TRNNG - HOW HACKERS USE SOCIAL ENGINEERING TO GET INSIDE - Much more.

In this complete guide, you will find everything you need to become an ethical hacker. The information contained in it is of fundamental importance for having success in this field. Questions and answers: Q: Is the guide suitable for those starting from scratch? A: Yes, the guide explains the techniques used step by step, starting from the basics. Q: Will I need other guides to get started? A: The guide has all the notions useful to start in a short time. Q: Will I need to invest in expensive software? A: No, the guide teaches how to use many tools and tools easily available. Think of how many new perspectives will open once the skils in the guide are learned.You will be able to defend yourself and others against the most complex informatic attacks. What are you waiting for? Buy now the complete guide currently available on the market.

Hackers

This 25th anniversary edition of Steven Levy's classic book traces the exploits of the computer revolution's original hackers -- those brilliant and eccentric nerds from the late 1950s through the early '80s who took risks, bent the rules, and pushed the world in a radical new direction. With updated material from noteworthy hackers such as Bill Gates, Mark Zuckerberg, Richard Stallman, and Steve Wozniak, Hackers is a fascinating story that begins in early computer research labs and leads to the first home computers. Levy profiles the imaginative brainiacs who found clever and unorthodox solutions to computer engineering problems. They had a shared sense of values, known as "the hacker ethic," that still thrives today. Hackers captures a seminal period in recent history when underground activities blazed a trail for today's digital world, from MIT students finagling access to clunky computer-card machines to the DIY culture that spawned the Altair and the Apple II.

MORAL CODES

In today's rapidly evolving digital age, security isn't just about building walls; it's about understanding the labyrinthine corridors of the very systems these walls protect. "MORAL CODES: A COMPREHENSIVE GUIDE TO ETHICAL HACKING" serves as a beacon, guiding readers through the intricate pathways of the Cybersecurity realm while always upholding an unyielding commitment to ethics. At first glance, the juxtaposition of 'ethical' and 'hacking' may seem contradictory. Yet, within the covers of this volume, this book demystifies the confluence of morality and digital penetration, illustrating that ethical hacking is not an oxymoron but a necessity. This is not just another technical manual; it's a treatise on the moral imperatives that bind Cybersecurity professionals. Explore deep into the hacker's mindset, understanding not just the how, but more crucially, the why. Readers will be equipped with tools and techniques used by ethical hackers but, more importantly, the foundational knowledge to use them responsibly and beneficially. From penetration testing essentials to the latest in mobile and cloud security, this comprehensive guide leaves no stone unturned. Each chapter stands as a source of clarity, providing both novices and seasoned professionals with insights into the constantly evolving threats and the ethical countermeasures required.

Ethical Hacking

Do you know if you were hacked? Do you know if some personal information was stolen from your system or account? Have you always wanted to learn how to protect your system from such attacks? If you answered yes to all these questions, you've come to the right place. Unlike malicious hacking, ethical hacking is a legal way to test the vulnerabilities of a system. Many organizations are still wary of ethical hackers, and they have every right to be since some hackers lie for their own benefit. That being said, many organizations are now searching for ethical hackers because they want to identify a way to protect themselves and their customers and employees. Over the course of the book, you will learn more about what ethical hacking is and will begin to comprehend the different types of attacks that an ethical hacker can perform on a system. This book will talk about: What ethical hacking is and how it is different from malicious hacking Why it's important to hack a system What the different phases of ethical hacking are The steps that an ethical hacker must take to protect himself The different skills an ethical hacker must have The different tools that a hacker can utilize to test a system Different types of attacks that can be performed on a system How the hacker should protect a system from such attacks This book provides numerous examples of different attacks and also includes some exercises that you can follow when you're performing these attacks for the first time. It is important to remember that ethical hacking is becoming one of the most sought-after professions because every organization is looking for a way to protect their data. So, what are you waiting for - grab a copy of the book now!

Ethical Hacking

If you wish to enter the world of ethical hacking, this book is for you. Ethical Hacking: A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking will walk you through the processes, skills, and tools you need to succeed. If you want to master ethical hacking, then this is the book you have been looking for. Inside you will learn the important lessons you need to master the basics of ethical hacking. No matter if you are a beginner or a knowledgeable IT professional, this book will enhance your skills and make you the best ethical hacker you can be. When it comes to honing your talents and seeking certification, this book provides you with the information you need to take the next step. This book covers everything you need to get started and move forward with ethical hacking.This book will prepare you to reach your goals in ethical hacking and will teach you the complex information behind packets, protocols, malware, and network infrastructure. Don't let this opportunity to enhance your skills pass. Stop wishing to know about ethical hacking, take the plunge, and purchase Ethical Hacking: A Comprehensive Guide to Learn and Master Hacking today!Inside you will find The knowledge of how to attack computer systems to find weaknesses Master what it means to be an ethical hacker Learn about the tools and terminology you need to get started Contemplate the difference between ethical hackers and system attackers Determine vulnerabilities, exploits, and weaknesses in computer systems Gain in-depth knowledge about the processes of enumeration, sniffing, port scanning, and network mapping Learn about malware and how to infect networks, servers, and computers with ease Everything you need to know to master evading intrusion detection systems Have fun with the techniques behind system hacking, social engineering, hacking the web, and the cloud Have fun with the techniques behind system hacking, social engineering, hacking the web, and the cloud And more . . .

Ethical Hacking and Penetration Testing Guide

Requiring no prior hacking experience, Ethical Hacking and Penetration Testing Guide supplies a complete introduction to the steps required to complete a penetration test, or ethical hack, from beginning to end. You will learn how to properly utilize and interpret the results of modern-day hacking tools, which are required to complete a penetration test. The book covers a wide range of tools, including Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. Supplying a simple and clean explanation of how to effectively utilize these tools, it details a four-step methodology for conducting an effective penetration test or hack.Providing an accessible introduction to penetration testing and hacking, the book supplies you with a fundamental understanding of offensive security. After completing the book you will be prepared to take on in-depth and advanced topics in hacking and penetration testing. The book walks you through each of the steps and tools in a structured, orderly manner allowing you to understand how the output from each tool can be fully utilized in the subsequent phases of the penetration test. This process will allow you to clearly see how the various tools and phases relate to each other. An ideal resource for those who want to learn about ethical hacking but dont know where to start, this book will help take your hacking skills to the next level. The topics described in this book comply with international standards and with what is being taught in international certifications.

Ethical Hacking

This book is for those of you looking to adding more skills to your arsenal. It touches upon all topics that an ethical hacker should know about and how to implement the skills of a professional hacker.The book will provide a brief history of ethical hacking.You will learn what ethical hacking means and how this term is different from general hacking. Hacking topics include physical threats as well as the non-physical threats in an organization that all skilled ethical hackers must understand.You'll be provided with the rules of ethical hacking that you must memorize in order to properly implement.An ethical hacker is nothing without tools; therefore, there is a compiled list of some of the most prominent tools that will help you manage your hacking plans. Some of the tools include Nmap, John the Ripper, IronWASP, Maltgeo, Wireshark, and Metasploit. Also included are tricks on how to use Python to hack passwords.As an ethical hacker, you'll learn how to beat the black hat hacker at his own game! Learn to recognize and counter social engineering attacks, trojan horses, malware and more.In this book you'll discover many unexpected computer vulnerabilities as we categorize the systems in terms of vulnerability. You may be surprised to learn that simple gaps under an office door can put your organization at risk for being hacked! In additional, you will learn in step by step detail how you can hack into a Windows operating system. Don't worry - you don't have to be an expert to be an ethical hacker. You just need an excellent guide, like this one. Click the Buy Now button to get started protecting yourself and your organization from unethical hackers.

Ethical Hacking

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 ambigue 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.

Python Ethical Hacking from Scratch

Explore the world of practical ethical hacking by developing custom network scanning and remote access tools that will help you test the system security of your organization Key Features Get hands-on with ethical hacking and learn to think like a real-life hacker Build practical ethical hacking tools from scratch with the help of real-world examples Leverage Python 3 to develop malware and modify its complexities Book DescriptionPenetration testing enables you to evaluate the security or strength of a computer system, network, or web application that an attacker can exploit. With this book, you'll understand why Python is one of the fastest-growing programming languages for penetration testing. You'll find out how to harness the power of Python and pentesting to enhance your system security. Developers working with Python will be able to put their knowledge and experience to work with this practical guide. Complete with step-by-step explanations of essential concepts and practical examples, this book takes a hands-on approach to help you build your own pentesting tools for testing the security level of systems and networks. You'll learn how to develop your own ethical hacking tools using Python and explore hacking techniques to exploit vulnerabilities in networks and systems. Finally, you'll be able to get remote access to target systems and networks using the tools you develop and modify as per your own requirements. By the end of this ethical hacking book, you'll have developed the skills needed for building cybersecurity tools and learned how to secure your systems by thinking like a hacker.What you will learn Understand the core concepts of ethical hacking Develop custom hacking tools from scratch to be used for ethical hacking purposes Discover ways to test the cybersecurity of an organization by bypassing protection schemes Develop attack vectors used in real cybersecurity tests Test the system security of an organization or subject by identifying and exploiting its weaknesses Gain and maintain remote access to target systems Find ways to stay undetected on target systems and local networks Who this book is forIf you want to learn ethical hacking by developing your own tools instead of just using the prebuilt tools, this book is for you. A solid understanding of fundamental Python concepts is expected. Some complex Python concepts are explained in the book, but the goal is to teach ethical hacking, not Python.

Ethical Hacking

Have you always wanted to understand what ethical hacking is? Did you ever want to learn more about how to perform an ethical hack to take care of the security vulnerabilities in a system? Do you want to learn how to secure your system? If you answered yes to these questions, then you have come to the right place. Ethical hacking is a profession that has gained popularity in the last few years. Network security and cybersecurity have become important aspects of every business. Hackers have always hacked the network or server of an organization to obtain personal information that can derail the company. It is for this reason that organizations have begun to hire the professionals to help them maintain this security. These professionals are ethical hackers. An ethical hacker will run numerous tests and hacks that another cracker may use to obtain sensitive information about the system. If you are looking to become an ethical hacker, you have come to the right place. Over the course of this book, you will gather information on: - What is hacking?- Differences between hacking and ethical hacking- Different terms used in ethical hacking- The ethical hacking commandments- The skills and tools required to become an ethical hacker- The process and phases of ethical hacking- Tools to perform ethical hacking- Different types of attacks to penetrate a network like penetration testing, ARP spoofing, DNS Spoofing, Password Hacking, Password Cracking, SQL injection, Sniffing, Fingerprinting, Enumeration, Exploitation and more- How to gain access to a system and much moreThis book also sheds some light on what the Kali Linux distribution is and how you can install this distribution on your system. This distribution is the best for any type of hacking. So, what are you waiting for? Grab a copy of this book now

Demystifying the World of Ethical Hacking

Demystifying the World of Ethical Hacking" presents an enlightening exploration into the realm of ethical hacking. This tome serves as a comprehensive guide for those seeking to comprehend the ethical, technical, and legal aspects of this often misunderstood field. It elucidates the role of ethical hackers, who employ their skills for the betterment of cyber security, contrasting them with malicious hackers. The book covers a wide array of topics, from the fundamentals of network security, vulnerabilities, and threat assessment, to advanced techniques in penetration testing and digital forensics. Readers will find detailed explanations of various hacking methodologies, tools, and strategies, accompanied by real-world scenarios and case studies. This not only imparts practical knowledge but also provides insights into the mindset and ethics governing this profession. Furthermore, the book delves into the legal framework surrounding ethical hacking, offering guidance on navigating the complex legalities and ethical dilemmas faced by professionals in this field. "Demystifying the World of Ethical Hacking" aims to educate its audience on the importance of ethical hacking in safeguarding cyberspace. It appeals to a broad audience, ranging from aspiring ethical hackers and IT professionals to business leaders and policymakers. With its blend of technical depth and accessible language, it demystifies the often opaque world of cyber security, making it an essential read for anyone intrigued by or involved in this critical domain.

Ethical Hacking

There is a general belief that all hackers are the equivalent to cybercriminals. This belief is partly as a result of the growing rise in the damage that hackers are causing to computer systems and business organizations. However, this book aims to counter that belief. Hacking is a broad term that is used to describe the work of the ethical hacker and the black hat hacker.This book provides a comprehensive explanation of the work of an ethical hacker. It starts by explaining the term "hacking" and the different types of hacking. Ethical hacking is a type of hacking, and the ethical hacker is someone who is versatile in hacking but uses his or her knowledge for the benefit of the business organization or the individual.

Ethical hacking is observed from the three major aspects of hacking: The pre-attack stageAttack stagePenetration testingThe pre-attack stage involves footprinting, enumerations, and scanning, while the attack stage covers password cracking, keyloggers and spyware, threats and vulnerability scanning, and steganography. Penetration testing is a vital aspect of ethical hacking. During testing, the ethical hacker simulates the ways intruders gain access to a company's system. The book explains the different ways in which it is used and the countermeasures an ethical hacker can use to foil the work of the hacker. If you're interested in being an ethical hacker, or are just curious about the field of hacking, then this book is for you! Click the Buy Now button to get started.

Ethical Hacker

From the interesting and intriguing to the weird and wonderful Odd Jobs: Ethical Hacker is HIGH interest combined with a LOW level of complexity to help struggling readers along. The carefully written, considerate text will hold readers’ interest and allow for successful mastery, understanding, and enjoyment of reading about Ethic Hackers. Clear, full-color photographs with captions provide additional accessible information. A table of contents, glossary with simplified pronunciations, and index all enhance achievement and comprehension.

The Handbook of Information and Computer Ethics

This handbook provides an accessible overview of the most important issues in information and computer ethics. It covers: foundational issues and methodological frameworks; theoretical issues affecting property, privacy, anonymity, and security; professional issues and the information-related professions; responsibility issues and risk assessment; regulatory issues and challenges; access and equity issues. Each chapter explains and evaluates the central positions and arguments on the respective issues, and ends with a bibliography that identifies the most important supplements available on the topic.

Gender, Ethics and Information Technology

This book brings feminist philosophy, in the shape of feminist ethics, politics and legal theory, to an analysis of computer ethics problems including hacking, privacy, surveillance, cyberstalking and Internet dating. Adam claims that these issues cannot be properly understood unless we see them as problems relating to gender. For the first time, these issues are put under the feminist spotlight to show that traditional responses reproduce the public/private split which has so often reinforced the causes of women's oppression.

The Dark Side of Software Engineering

Betrayal! Corruption! Software engineering? Industry experts Johann Rost and Robert L. Glass explore the seamy underbelly of software engineering in this timely report on and analysis of the prevalance of subversion, lying, hacking, and espionage on every level of software project management. Based on the authors' original research and augmented by frank discussion and insights from other well-respected figures, The Dark Side of Software Engineering goes where other management studies fear to tread -- a corporate environment where schedules are fabricated, trust is betrayed, millions of dollars are lost, and there is a serious need for the kind of corrective action that this book ultimately proposes.

Internet Security

This collection of papers, articles, and monographs details the ethical landscape as it exists for the distinct areas of Internet and network security, including moral justification of hacker attacks, the ethics behind the freedom of information which contributes to hacking, and the role of the law in policing cyberspace.

Infinity Ethical Hacking

Ever wanted to learn computer security, but didn't know where to start? This book is for you. The author starts from scratch with the fundamental concepts of data networks and computer security, developing them during the first two chapters to build the knowledge bases. The second half of the book focuses on the work methodology of an ethical hacker, the management of various tools to perform vulnerability scanning and penetration testing, as well as the methods to perform attacks on data networks. The content presents the reader with a tutorial on the basic use of various tools through various laboratories that are easy to follow and reproduce in a virtual environment. Information technologies continue to evolve day by day, so this book represents a starting point for all those enthusiasts of the world of computer security. At the end, you will know the process to carry out ethical hacking through attack strategies in data networks and you will obtain knowledge about the methods of mitigation of computer threats, all this in a practical and simple way to learn.

A Hacker Manifesto

A double is haunting the world--the double of abstraction, the virtual reality of information, programming or poetry, math or music, curves or colorings upon which the fortunes of states and armies, companies and communities now depend. The bold aim of this book is to make manifest the origins, purpose, and interests of the emerging class responsible for making this new world--for producing the new concepts, new perceptions, and new sensations out of the stuff of raw data. "A Hacker Manifesto" deftly defines the fraught territory between the ever more strident demands by drug and media companies for protection of their patents and copyrights and the pervasive popular culture of file sharing and pirating. This vexed ground, the realm of so-called "intellectual property," gives rise to a whole new kind of class conflict, one that pits the creators of information--the hacker class of researchers and authors, artists and biologists, chemists and musicians, philosophers and programmers--against a possessing class who would monopolize what the hacker produces. Drawing in equal measure on Guy Debord and Gilles Deleuze, "A Hacker Manifesto" offers a systematic restatement of Marxist thought for the age of cyberspace and globalization. In the widespread revolt against commodified information, McKenzie Wark sees a utopian promise, beyond the property form, and a new progressive class, the hacker class, who voice a shared interest in a new information commons.

Ethical Hacking for Beginners and Dummies

The term hacking has been around for a long time now. The first recorded instance of hacking dates back to the early 1960s in MIT where both the terms, 'Hacking' and 'Hacker' were coined. Since then, hacking has evolved into a broadly followed discipline for the computing community. Understanding the reason why an individual may want to infiltrate or hack into a system is usually the most difficult task, the intention behind cyber-attacks usually allows room for prevention as the user may be able to defend against any possible system vulnerability. EH is used as a penetration testing tool in order to prevent breach of basic rights, privacy and free will. Ethical hackers are usually professionals or network penetration testers who use their hacking skills and toolsets for defensive and protective purposes. Then again there are three sorts of programmers: Black Hat, Grey Hat and White Hat as indicated by (Hoffman 2013). White Hats are usually software engineers that hack for good, and hack with respect to corporate/business networking structures. A Grey Hat hacker may do things imperfect in nature, however not to intentionally hurt people or damage systems, unless there is a genuine positive result. A Black Hat Hacker will maliciously misuse computers and networks with pernicious aim, with no legitimate reason. Hacking also means accessing a system that one is either not authorized to access, or who accesses a system at a level beyond their authorization, clearly abandoning the possibility of ethics being applied to it. The rise in cybercrime is a major breaching issue for organizations and it has been reported that over 30,000 SME websites are hacked daily. The need for advanced cyber security is a necessity to fight of Black Hat Hackers, and organizations all over the world need to start implementing such procedures to protect their businesses, but the costs related to EH make it impossible for smaller companies to cope. EH is gone beyond just professionals as universities all around the world have been offering courses to graduate and undergraduate students to increase their understanding on how to protect data and apply security procedures in an ethical way. Making it easier for organizations to employ talent rather than pay for services from external organizations, however teaching young students the profession of hacking without knowledge of their intent could be suicidal. EH can be applied to many circumstances however this paper will discuss the advantages and disadvantages of EH within three separate sectors, education, business and governmental to allow the reader to truly understand and grasp the importance of the subject at hand.

Ethical Hacking and Countermeasures: Web Applications and Data Servers

The EC-Council | Press Ethical Hacking and Countermeasures Series is comprised of five books covering a broad base of topics in offensive network security, ethical hacking, and network defense and countermeasures. The content of this series is designed to immerse the reader into an interactive environment where they will be shown how to scan, test, hack and secure information systems.

With the full series of books, the reader will gain in-depth knowledge and practical experience with essential security systems, and become prepared to succeed on the Certified Ethical Hacker, or C|EH, certification from EC-Council. This certification covers a plethora of offensive security topics ranging from how perimeter defenses work, to scanning and attacking simulated networks. A wide variety of tools, viruses, and malware is presented in this and the other four books, providing a complete understanding of the tactics and tools used by hackers. By gaining a thorough understanding of how hackers operate, an Ethical Hacker will be able to set up strong countermeasures and defensive systems to protect an organization's critical infrastructure and information. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.