The Art Of Computer Virus Research And Defense

031202889X

A comprehensive guide to Metasploit for beginners that will help you get started with the latest Metasploit 5.0 Framework for exploiting real-world vulnerabilities Key Features Perform pentesting in highly secured environments with Metasploit 5.0 Become well-versed with the latest features and improvements in the Metasploit Framework 5.0 Analyze, find, exploit, and gain access to different systems by bypassing various defenses Book Description Securing an IT environment can be challenging, however, effective penetration testing and threat identification can make all the difference. This book will help you learn how to use the Metasploit Framework optimally for comprehensive penetration testing. Complete with hands-on tutorials and case studies, this updated second edition will teach you the basics of the Metasploit Framework along with its functionalities. You'll learn how to set up and configure Metasploit on various platforms to create a virtual test environment. Next, you'll get hands-on with the essential tools. As you progress, you'll learn how to find weaknesses in the target system and hunt for vulnerabilities using Metasploit and its supporting tools and components. Later, you'll get to grips with web app security scanning, bypassing anti-virus, and post-compromise methods for clearing traces on the target system. The concluding chapters will take you through real-world case studies and scenarios that will help you apply the knowledge you've gained to ethically hack into target systems. You'll also discover the latest security techniques that can be directly applied to scan, test, ethically hack, and secure networks and systems with Metasploit. By the end of this book, you'll have learned how to use the Metasploit 5.0 Framework to exploit real-world vulnerabilities. What you will learn Set up the environment for Metasploit Understand how to gather sensitive information and exploit vulnerabilities Get up to speed with client-side attacks and web application scanning using Metasploit Leverage the latest features of Metasploit 5.0 to evade anti-virus Delve into cyber attack management using Armitage Understand exploit development and explore real-world case studies Who this book is for If you are a penetration tester, ethical hacker, or security consultant who wants to quickly get started with using the Metasploit Framework to carry out elementary penetration testing in highly secured environments, then this Metasploit book is for you. You will also find this book useful if you're interested in computer security, particularly in the areas of vulnerability assessment and pentesting, and want to develop practical skills when using the Metasploit Framework.

The world's most infamous hacker offers an insider's view of the low-tech threats to high-tech security Kevin Mitnick's exploits as a cyber-desperado and fugitive form one of the most exhaustive FBI manhunts in history and have spawned dozens of articles, books, films, and documentaries. Since his release from federal prison, in 1998, Mitnick has turned his life around and established himself as one of the most sought-after computer security experts worldwide. Now, in The Art of Deception, the world's most notorious hacker gives new meaning to the old adage, "It takes a thief to catch a thief." Focusing on the human factors involved with information security, Mitnick explains why all the firewalls and encryption protocols in the world will never be enough to stop a savvy grifter intent on rifling a corporate database or an irate employee determined to crash a system. With the help of many fascinating true stories of successful attacks on business and government, he illustrates just how susceptible even the most locked-down information systems are to a slick con artist impersonating an IRS agent. Narrating from the points of view of both the attacker and the victims, he explains why each attack was so successful and how it could have been prevented in an engaging and highly readable style reminiscent of a true-crime novel. And, perhaps most importantly, Mitnick offers

advice for preventing these types of social engineering hacks through security protocols, training programs, and manuals that address the human element of security.

Virus bioinformatics is evolving and succeeding as an area of research in its own right, representing the interface of virology and computer science. Bioinformatic approaches to investigate viral infections and outbreaks have become central to virology research, and have been successfully used to detect, control, and treat infections of humans and animals. As part of the Third Annual Meeting of the European Virus Bioinformatics Center (EVBC), we have published this Special Issue on Virus Bioinformatics.

“Why Understanding All The Ins And Outs Of Avoiding Viruses Is Crucial!” Computer viruses are unwanted computer programs that can invade your hard drive and cause many different types of damage. Usually viruses are created when someone writes a computer program and embeds harmful software within that program. As soon as other people begin downloading that infected program onto their computer...

Viruses are the last frontier of undiscovered life on our planet. The most abundant type of organism on Earth, they infect all types of cellular life, and, as micro-organisms that cause disease in their hosts, they are highly opportunistic and relentlessly efficient. They exist at the vanguard of DNA variance, exhibiting more structural diversity than plants, animals, archaea, or even bacteria. This 21st-century guide offers an engaging introductory section explaining exactly what viruses are and how they operate, followed by individual profiles of 101 of the world's most notable examples, each with its own dazzling mugshot

This book provides key steps users should take to protect their systems from computer viruses. If a computer is infected with a virus, information on how to recover data is discussed. Also provides users with preventive care they should employ to reduce their risk to viruses in the future. This book also dissects a variety of viruses and presents famous viruses and how they spread.

The 1980's saw the advent of widespread (and potentially damaging) computer virus infection of both personal computer and mainframe systems. The computer security field has been comparatively slow to react to this emerging situation. It is only over the last two years that a significant body of knowledge on the operation, likely evolution and prevention of computer viruses has developed. A Pathology of Computer Viruses gives a detailed overview of the history of the computer virus and an in-depth technical review of the principles of computer virus and worm operation under DOS, Mac, UNIX and DEC operating systems. David Ferbrache considers the possible extension of the threat to the mainframe systems environment and suggests how the threat can be effectively combatted using an antiviral management plan. The author addresses the latest developments in "stealth" virus operations, specifically the trend for virus authors to adopt extensive camouflage and concealment techniques, which allow viruses to evade both existing anti-viral software and to avoid detection by direct observation of machine behaviour. A Pathology of Computer Viruses addresses a distinct need - that of the computer specialist and professional who needs a source reference work detailing all aspects of the computer virus threat.

Malware Data Science explains how to identify, analyze, and classify large-scale malware using machine learning and data visualization. Security has become a "big data" problem. The growth rate of malware has accelerated to tens of millions of new files per year while our networks generate an ever-larger flood of security-relevant data each day. In order to defend against these advanced attacks, you'll need to know how to think like a data scientist. In Malware Data Science, security data scientist Joshua Saxe introduces machine learning, statistics, social network analysis, and data visualization, and shows you how to apply these methods to malware detection and analysis. You'll learn how to: - Analyze malware using static analysis - Observe malware

behavior using dynamic analysis - Identify adversary groups through shared code analysis - Catch 0-day vulnerabilities by building your own machine learning detector - Measure malware detector accuracy - Identify malware campaigns, trends, and relationships through data visualization Whether you're a malware analyst looking to add skills to your existing arsenal, or a data scientist interested in attack detection and threat intelligence, Malware Data Science will help you stay ahead of the curve.

This open access book answers two central questions: firstly, is it at all possible to verify electronic equipment procured from untrusted vendors? Secondly, can I build trust into my products in such a way that I support verification by untrusting customers? In separate chapters the book takes readers through the state of the art in fields of computer science that can shed light on these questions. In a concluding chapter it discusses realistic ways forward. In discussions on cyber security, there is a tacit assumption that the manufacturer of equipment will collaborate with the user of the equipment to stop third-party wrongdoers. The Snowden files and recent deliberations on the use of Chinese equipment in the critical infrastructures of western countries have changed this. The discourse in both cases revolves around what malevolent manufacturers can do to harm their own customers, and the importance of the matter is on par with questions of national security. This book is of great interest to ICT and security professionals who need a clear understanding of the two questions posed in the subtitle, and to decision-makers in industry, national bodies and nation states.

Top cybersecurity journalist Kim Zetter tells the story behind the virus that sabotaged Iran’s nuclear efforts and shows how its existence has ushered in a new age of warfare—one in which a digital attack can have the same destructive capability as a megaton bomb. In January 2010, inspectors with the International Atomic Energy Agency noticed that centrifuges at an Iranian uranium enrichment plant were failing at an unprecedented rate. The cause was a complete mystery—apparently as much to the technicians replacing the centrifuges as to the inspectors observing them. Then, five months later, a seemingly unrelated event occurred: A computer security firm in Belarus was called in to troubleshoot some computers in Iran that were crashing and rebooting repeatedly. At first, the firm’s programmers believed the malicious code on the machines was a simple, routine piece of malware. But as they and other experts around the world investigated, they discovered a mysterious virus of unparalleled complexity. They had, they soon learned, stumbled upon the world’s first digital weapon. For Stuxnet, as it came to be known, was unlike any other virus or worm built before: Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to wreak actual, physical destruction on a nuclear facility. In these pages, Wired journalist Kim Zetter draws on her extensive sources and expertise to tell the story behind Stuxnet’s planning, execution, and discovery, covering its genesis in the corridors of Bush’s White House and its unleashing on systems in Iran—and telling the spectacular, unlikely tale of the security geeks who managed to unravel a sabotage campaign years in the making. But Countdown to Zero Day ranges far beyond Stuxnet itself. Here, Zetter shows us how digital warfare developed in the US. She takes us inside today’s flourishing zero-day “grey markets,” in which intelligence agencies and militaries pay huge sums for the malicious code they need to carry out infiltrations and attacks. She reveals just how vulnerable many of our own critical systems are to Stuxnet-like strikes, from nation-

state adversaries and anonymous hackers alike—and shows us just what might happen should our infrastructure be targeted by such an attack. Propelled by Zetter's unique knowledge and access, and filled with eye-opening explanations of the technologies involved, Countdown to Zero Day is a comprehensive and prescient portrait of a world at the edge of a new kind of war.
Hackers have uncovered the dark side of cryptography—thatdevice developed to defeat Trojan horses, viruses, password theft,and other cyber-crime. It's called cryptovirology, the art ofturning the very methods designed to protect your data into a meansof subverting it. In this fascinating, disturbing volume, theexperts who first identified cryptovirology show you exactly whatyou're up against and how to fight back. They will take you inside the brilliant and devious mind of ahacker—as much an addict as the vacant-eyed denizen of thecrackhouse—so you can feel the rush and recognize youropponent's power. Then, they will arm you for thecounterattack. This book reads like a futuristic fantasy, but be assured, thethreat is ominously real. Vigilance is essential, now. Understand the mechanics of computationally secure informationstealing Learn how non-zero sum Game Theory is used to developsurvivable malware Discover how hackers use public key cryptography to mountextortion attacks Recognize and combat the danger of kleptographic attacks onsmart-card devices Build a strong arsenal against a cryptovirology attack
While security is generally perceived to be a complicated and expensive process, Zen and the Art of Information Security makes security understandable to the average person in a completely non-technical, concise, and entertaining format. Through the use of analogies and just plain common sense, readers see through the hype and become comfortable taking very simple actions to secure themselves. Even highly technical people have misperceptions about security concerns and will also benefit from Ira Winkler's experiences making security understandable to the business world. Mr. Winkler is one of the most popular and highly rated speakers in the field of security, and lectures to tens of thousands of people a year. Zen and the Art of Information Security is based on one of his most well received international presentations. Written by an internationally renowned author of Spies Among Us who travels the world making security presentations to tens of thousands of people a year This short and concise book is specifically for the business, consumer, and technical user short on time but looking for the latest information along with reader friendly analogies Describes the REAL security threats that you have to worry about, and more importantly, what to do about them
An ex-hacker, a sexy college professor, stolen top secret hardware, a cover-up, a kidnapping, a government conspiracy, hacked defense computers, FBI, CIA, NSA, Armageddon. An excerpt from the actual deposition transcripts: "Let the record reflect that this deposition commenced at 9:15 am on December the 3rd, 2004 at the FBI offices in Atlanta, Georgia. Present for this recording are Special Agent Alvin Dirk, the Honorable Judge Ramiro Vasquez, and the witness, Robert O. Blain. This deposition is merely a recording of the events which transpired at Norwood University and is not now nor ever will be part of any trial or prosecution. Go ahead." "My name is Bobby Blain. Most people seem to think it all started when Dr. Jennings hired me, and all the computers started getting hacked. It was easy for people to think that, because I have a history and got myself in some trouble when I was younger. I hacked some computers and almost got the president impeached, but it really started before that, when I still worked for Dr. Karlyn." "Dr. Karlyn gave me a chance to redeem myself by allowing me to work on his computer for him. Then one day, this

scientist I had never seen before comes and gives Dr. Karlyn a device. I was never told what he wanted, but I think he wanted Dr. Karlyn to help him reverse engineer it. I was only asked to build an interface to attach it to the computer. Dr. Karlyn did the rest. I think he figured out how to turn it on, but when he did, strange things started to happen." "We didn't know it then, but it turns out the device was stolen from a government facility. I don't know where they got it, that is more classified than this deposition. I can tell you with absolute certainty that they didn't make it themselves. I'd like to tell you more, but I don't think I'm allowed." "Anyway, someone at the university needed to get Dr. Karlyn out of the way and falsely accused him of inappropriate conduct with a student. He could have fought it, the dean believed him, but he decides to leave the school anyway. Before he goes, he gives his computer to Professor Jennings and he gives me a letter of recommendation, so after I help deliver and setup the computer, she agrees to hire me." "The first night it is up and running, at least two attempts are made to hack into the computer. I forgot to mention that even before I deliver the computer, this guy tries to break in and steal something from it, but I was there and he didn't get anything." "I can't divulge any secrets about Professor Jennings' project here, but my part is to prove that her process would work if she were given enough computer resources, so I re-write her process to work across a network and run on thousands of computers." "That's when things got really crazy. Someone keeps trying to hack into our computer; someone hacks the entire school and the phone company. Professor Jennings' secretary is kidnapped. The FBI gets involved, but they're chasing the wrong people for reasons only they can tell you." "Then someone plants a virus on our computer and the next thing we know, it's spread all over the internet, including some very sensitive government computers. Meanwhile, our project continues to gain speed and surpass anyone's expectations." "When the FBI come in and learn that the device that was given to Dr. Karlyn is actually some super cool futuristic computer that is able to grow and build more circuits for itself, they want to disconnect the computer and confiscate it." "That's when computers all over the world go out of control. The pentagon and all the armed forces are helpless. Air traffic is grounded. All the computer problems are traced back to the professor's computer. The FBI want it dismantled more than ever, but the academics involved want to get the device to relinquish control over the world before they do." "And, well, I guess that's all I'm allowed to say, thank you."

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: –Set up a safe virtual environment to analyze malware –Quickly extract network signatures and host-based indicators –Use key analysis tools like IDA Pro, OllyDbg, and WinDbg –Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques –Use your newfound knowledge of Windows internals for malware analysis –Develop a methodology for unpacking malware and get practical experience with five of the most popular packers –Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your

skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

This book discusses state of the art computer virus technology in 1996. It focuses on viruses working in the new 32-bit operating systems like Windows 95 & Windows NT, as well as internet-related threats. It includes detailed dissections & explanations of four complex computer viruses which attack the new PE-style executables, & a dissection & discussion of the Internet Worm. This is the most advanced book in the field, designed for the professional who must stay on top of the latest developments in computer security, or military personnel who require it to design advanced weapons systems. Also see, by the same author, THE GIANT BLACK BOOK OF COMPUTER VIRUSES (ISBN 0-929408-10-1, 662 pages, $39.95) & COMPUTER VIRUSES, ARTIFICIAL LIFE & EVOLUTION (ISBN 0-929408-07-1, 373 pages, $26.95). Order from American Eagle Publishing, P.O. Box 1507, Showlow, AZ 85901; 520-367-1621, 800-719-4957.

Zuto: The Adventures of a Computer Virus takes place inside a strange, little-known world: a personal computer, the perfect setting for a fast-paced, funny, one-minute-long story.Zuto, a smart, sneaky computer virus, leads a happy life in his secret hiding place: the Recycle Bin. There, among heaps of junk full of surprising treasures, he plans his tricks. Everything changes when a far more malicious program invades the computer . . . and threatens to end all life in it. Together with his Recycle Bin friends—outdated, buggy programs—Zuto sets off to save his world.Readers curious about the truth behind this rollicking adventure story will find it in the Zutopedia appendix, which explains concepts such as computer viruses, IP addresses, and binary numbers.Zuto was first published in Israel, where it was recommended by the Israeli Ministry of Education and voted in the top ten favorite books by children in grades 4-6 nationwide.

Describes the techniques of computer hacking, covering such topics as stack-based overflows, format string exploits, and shellcode.

This book captures the state of the art research in the area of malicious code detection, prevention and mitigation. It contains cutting-edge behavior-based techniques to analyze and detect obfuscated malware. The book analyzes current trends in malware activity online, including botnets and malicious code for profit, and it proposes effective models for detection and prevention of attacks using. Furthermore, the book introduces novel techniques for creating services that protect their own integrity and safety, plus the data they manage.

Written by a pioneer in the field, this updated and expanded revision covers all aspects of computer viruses. New results include: analysis of the epidemiology of computer viruses, new forms of virus evolution that will render most current safeguards useless, strategy and tactics in virus defenses, assessment of synergistic effects in attack and defense. Features new chapters on LANs,

international and `good' viruses. Software includes a virus scanner, a password generator and checker, an `integrity' shell to test systems and much more. Packed with historical facts, anecdotes and authentic examples.

Our Internet-connected society increasingly relies on computers. As a result, attacks on computers from malicious software have never been a bigger concern. Computer Viruses and Malware draws together hundreds of sources to provide an unprecedented view of malicious software and its countermeasures. This book discusses both the technical and human factors involved in computer viruses, worms, and anti-virus software. It also looks at the application of malicious software to computer crime and information warfare. Computer Viruses and Malware is designed for a professional audience composed of researchers and practitioners in industry. This book is also suitable as a secondary text for advanced-level students in computer science.

Digital Contagions is the first book to offer a comprehensive and critical analysis of the culture and history of the computer virus phenomenon. The book maps the anomalies of network culture from the angles of security concerns, the biopolitics of digital systems, and the aspirations for artificial life in software. The genealogy of network culture is approached from the standpoint of accidents that are endemic to the digital media ecology. Viruses, worms, and other software objects are not, then, seen merely from the perspective of anti-virus research or practical security concerns, but as cultural and historical expressions that traverse a non-linear field from fiction to technical media, from net art to politics of software. Jussi Parikka mobilizes an extensive array of source materials and intertwines them with an inventive new materialist cultural analysis. Digital Contagions draws from the cultural theories of Gilles Deleuze and Félix Guattari, Friedrich Kittler, and Paul Virilio, among others, and offers novel insights into historical media analysis.

How viruses emerge to cause pandemics, how our immune system combats them, and how diagnostic tests, vaccines, and antiviral therapies work. Throughout history, humans have contended with pandemics. History is replete with references to plagues, pestilence, and contagion, but the devastation wrought by pandemics had been largely forgotten by the twenty-first century. Now, the enormous human and economic toll of the rapidly spreading COVID-19 disease offers a vivid reminder that infectious disease pandemics are one of the greatest existential threats to humanity. This book provides an accessible explanation of how viruses emerge to cause pandemics, how our immune system combats them, and how diagnostic tests, vaccines, and antiviral therapies work-- concepts that are a foundation for our public health policies.

Market_Desc: Primary audience: those working in IT with security responsibilities, incident responders, security administrators, forensic analysts, malware researchersSecondary audience: college and university students (majors: information security, information assurance, forensics, computer science, and computer engineering), hobbyists/hackers Special Features: · Authors are well-known malware experts with training, speaking, corporate blogging platforms· The DVD contains original, never-before-published custom programs demonstrating concepts in the recipes from the book, including files required to complete reverse-engineering challenges and files required for thwarting attacks.· Contains practical knowledge required to investigate and solve modern malware related computer crimes, along with unique and efficient techniques and tools for current security professionals

and anyone looking to become a security professional· The number of jobs requiring security skills is dramatically increasing. In September 2009, the Department of Homeland Security announced 1000 new job openings for computer security experts. About The Book: This book is a collection of problems, solutions, and practical examples designed to enhance the analytical capabilities of anyone who works with malware. Whether you're tracking a Trojan across networks, performing an in-depth binary analysis, or inspecting a machine for potential infections, the recipes in this book will help you achieve your goals more quickly and accurately. The book goes beyond how to tackle challenges using free or inexpensive tools. It also includes a generous amount of source code in C, Python, and Perl that show how to extend your favorite tools or build your own from scratch.The DVD contains original, never-before-published custom programs from the authors to demonstrate concepts in the recipes. This tool set includes files required to complete reverse-engineering challenges and files required for the reader to follow along with exhibits/figures in the book.

Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian). Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter"—a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases—a one-man sting operation that finally gained the attention of the CIA . . . and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

A precise and exhaustive description of different types of malware from three different points of view, namely the theoretical fundamentals of computer virology, algorithmic and practical aspects of viruses and their potential applications to various areas.

What is the coronavirus, and why is everyone talking about it? Engagingly illustrated by Axel Scheffler, this approachable and timely book helps answer these questions and many more, providing children aged 5-10 and their parents with clear and accessible explanations about the coronavirus and its effects - both from a health perspective and the impact it has on a family’s day-to-day life. With input from expert consultant Professor Graham Medley of the London School of Hygiene & Tropical Medicine, as well as advice from teachers and child psychologists, this is a practical and informative resource to help explain the changes we are currently all experiencing. The book is free to read and download, but Nosy Crow would like to encourage readers, should they feel in a position to, to make a donation to: https://www.nhscharitiestogether.co.uk/

Hack your antivirus software to stamp out future vulnerabilities The Antivirus Hacker's Handbook guides you through the process of reverse engineering antivirus software. You explore how to detect and exploit vulnerabilities that can be leveraged to improve future software design, protect your network, and anticipate attacks that may sneak through your antivirus' line of defense. You'll begin building your knowledge by diving into the reverse engineering process, which details how to start from a finished antivirus software program and work your way back through its development using the functions and other key elements of the software. Next, you leverage your new knowledge about software

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

The Art of Computer Virus Research and DefensePearson Education

Symantec's chief antivirus researcher has written the definitive guide to contemporary virus threats, defense techniques, and analysis tools. Unlike most books on computer viruses, The Art of Computer Virus Research and Defense is a reference written strictly for white hats: IT and security professionals responsible for protecting their organizations against malware. Peter Szor systematically covers everything you need to know, including virus behavior and classification, protection strategies, antivirus and worm-blocking techniques, and much more. Szor presents the state-of-the-art in both malware and protection, providing the full technical detail that professionals need to handle increasingly complex attacks. Along the way, he provides extensive information on code metamorphism and other emerging techniques, so you can anticipate and prepare for future threats. Szor also offers the most thorough and practical primer on virus analysis ever published—addressing everything from creating your own personal laboratory to automating the analysis process. This book's coverage includes Discovering how malicious code attacks on a variety of platforms Classifying malware strategies for infection, in-memory operation, self-protection, payload delivery, exploitation, and more Identifying and responding to code obfuscation threats: encrypted, polymorphic, and metamorphic Mastering empirical methods for analyzing malicious code—and what to do with what you learn Reverse-engineering malicious code with disassemblers, debuggers, emulators, and virtual machines Implementing technical defenses: scanning, code emulation, disinfection, inoculation, integrity checking, sandboxing, honeypots, behavior blocking, and much more Using worm blocking, host-based intrusion prevention, and network-level defense strategies

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

Including the technical description of four basic virus types found on IBM PCs and compatibles, along with programs to detect these viruses and programs to remove them, this book enables readers to learn how to protect a computer system against virus infections, how to detect viruses, and how to remove them once they are discovered.

Memory forensics provides cutting edge technology to help investigate digital attacks Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields. Beginning with introductory concepts and moving toward the advanced, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory

forensics and how to deploy such techniques properly. Discover memory forensics techniques: How volatile memory analysis improves digital investigations Proper investigative steps for detecting stealth malware and advanced threats How to use free, open source tools for conducting thorough memory forensics Ways to acquire memory from suspect systems in a forensically sound manner The next era of malware and security breaches are more sophisticated and targeted, and the volatile memory of a computer is often overlooked or destroyed as part of the incident response process. The Art of Memory Forensics explains the latest technological innovations in digital forensics to help bridge this gap. It covers the most popular and recently released versions of Windows, Linux, and Mac, including both the 32 and 64-bit editions.

In this book you'll learn everything you wanted to know about computer viruses, ranging from the simplest 44-byte virus right on up to viruses for 32-bit Windows, Unix and the Internet. You'll learn how anti-virus programs stalk viruses and what viruses do to evade these digital policemen, including stealth techniques and poly-morphism. Next, you'll take a fascinating trip to the frontiers of science and learn about genetic viruses. Will such viruses take over the world, or will they become the tools of choice for the information warriors of the 21st century? Finally, you'll learn about payloads for viruses, not just destructive code, but also how to use a virus to compromise the security of a computer, and the possibility of beneficial viruses.

Master cutting-edge techniques and countermeasures to protect your organization from live hackers. Learn how to harness cyber deception in your operations to gain an edge over the competition. Key Features Gain an advantage against live hackers in a competition or real computing environment Understand advanced red team and blue team techniques with code examples Learn to battle in short-term memory, whether remaining unseen (red teams) or monitoring an attacker's traffic (blue teams) Book Description Little has been written about what to do when live hackers are on your system and running amok. Even experienced hackers tend to choke up when they realize the network defender has caught them and is zoning in on their implants in real time. This book will provide tips and tricks all along the kill chain of an attack, showing where hackers can have the upper hand in a live conflict and how defenders can outsmart them in this adversarial game of computer cat and mouse. This book contains two subsections in each chapter, specifically focusing on the offensive and defensive teams. It begins by introducing you to adversarial operations and principles of computer conflict where you will explore the core principles of deception, humanity, economy, and more about human-on-human conflicts. Additionally, you will understand everything from planning to setting up infrastructure and tooling that both sides should have in place. Throughout this book, you will learn how to gain an advantage over opponents by disappearing from what they can detect. You will further understand how to blend in, uncover other actors' motivations and means, and learn to tamper with them to hinder their ability to detect your presence. Finally, you will learn how to gain an advantage through advanced research and thoughtfully concluding an operation. By the end of this book, you will have achieved a solid understanding of cyberattacks from both an attacker's and a defender's perspective. What you will learn Understand how to implement process injection and how to detect it Turn the tables on the offense with active defense Disappear on the defender's system, by tampering with defensive sensors Upskill in using deception with your backdoors and countermeasures including

honeypots Kick someone else from a computer you are on and gain the upper hand Adopt a language agnostic approach to become familiar with techniques that can be applied to both the red and blue teams Prepare yourself for real-time cybersecurity conflict by using some of the best techniques currently in the industry Who this book is for Pentesters to red teamers, security operations center analysts to incident responders, attackers, defenders, general hackers, advanced computer users, and security engineers should gain a lot from this book. This book will also be beneficial to those getting into purple teaming or adversarial simulations, as it includes processes for gaining an advantage over the other team. Basic knowledge of Python programming, Go programming, Bash, PowerShell, and systems administration is desirable. Furthermore, knowledge of incident response and Linux is beneficial. Prior exposure to cybersecurity, penetration testing, and ethical hacking basics is desirable.

Computer viruses—just the thought of your trusty PC catchingone is probably enough to make you sick. Thanks to thecyber-sickies who persist in coming up with new strains,there's a major new cyberattack nearly every day. Virusessneak in, usually through e-mail. Fortunately, there are ways to inoculate and protect yourcomputer. Computer Viruses For Dummies helps you: Understand the risks and analyze your PC's currentcondition Select, install, and configure antivirus software Scan your computer and e-mail Rid your computer of viruses it's already caught Update antivirus software and install security patches Use firewalls and spyware blockers Protect handheld PDAs from viruses Adopt safe computing practices, especially with e-mail and whenyou're surfing the Net Written by Peter H. Gregory, coauthor of CISSP ForDummies and Security + For Dummies, Computer VirusesFor Dummies goes beyond viruses to explain other nasty computerinfections like Trojan horses, HiJackers, worms, phishing scams,spyware, and hoaxes. It also profiles major antivirus software tohelp you choose the best program(s) for your needs. Remember, if you don't protect your computer, not only doyou risk having your computer infiltrated and your datacontaminated, you risk unknowingly transmitting a virus, worm, orother foul computer germ to everybody in your address book! Thisguide will help you properly immunize your PC with antivirussoftware now and install updates and security patches that are likebooster shots to keep your software protected against newviruses.

Have you always been interested and fascinated by the world of hacking? Do you want to know how to start hacking in a simple way? If you want to know more, this book will teach you how to start step by step. Keep reading... Hacking for anyone to understand! "Hacking for Beginners" will teach you the basics of hacking as well as the different types of hacking and how hackers think. By reading it, you will not only discover why they are attacking your computers, but you will also be able to understand how they can scan your system and gain access to your computer. It's important to know how hackers operate if you want to protect your computer from their attacks. You will learn the phases in preparation for an attack and the different ways to prevent it. The goal is to learn the techniques to gather as much information as possible about a potential target without interacting directly with the target system. You will learn: Google hacking and Web hacking Fingerprinting Security and wireless security Different types of attackers Defects in software Sniffing and Spoofing And more... The book is targeted towards beginners who have never hacked before and are not familiar with any of the terms in hacking but also for someone that is looking to learn tips and tricks regarding

hacking. Follow me, and let's dive into the world of hacking! Don't keep waiting to start your new journey as a hacker; get started now and order your copy today! Scroll up and select the Buy button!

A computer forensics "how-to" for fighting malicious code andanalyzing incidents With our ever-increasing reliance on computers comes anever-growing risk of malware. Security professionals will findplenty of solutions in this book to the problems posed by viruses,Trojan horses, worms, spyware, rootkits, adware, and other invasivesoftware. Written by well-known malware experts, this guide revealssolutions to numerous problems and includes a DVD of customprograms and tools that illustrate the concepts, enhancing yourskills. Security professionals face a constant battle against malicioussoftware; this practical manual will improve your analyticalcapabilities and provide dozens of valuable and innovativesolutions Covers classifying malware, packing and unpacking, dynamicmalware analysis, decoding and decrypting, rootkit detection,memory forensics, open source malware research, and much more Includes generous amounts of source code in C, Python, and Perlto extend your favorite tools or build new ones, and customprograms on the DVD to demonstrate the solutions Malware Analyst's Cookbook is indispensible to ITsecurity administrators, incident responders, forensic analysts,and malware researchers.

Most people who use the Internet at all and who browse online for any type of product or so-called "free" download are going to encounter a virus on their computer. It's practically inevitable that you will someday inadvertently download a virus. The real question is, "Are you going to download a virus without being aware of it?" or "Will you be equipped to tackle the virus before it lodges itself on your computer's hard drive?"One painful lesson to be learned online is that you should never follow the "directions" given to you by a website which is trying to "infect" your computer with an unwanted program or virus. A common tactic to infect your computer is for a website to post the following warning message: "You have downloaded a virus!" At that point, there will be an option for you to remove the infection by clicking on a particular button, such as "OK." Never, ever give in to the temptation to do so. It may take all of your will-power, but if you want to keep your computer's hard drive clean and running efficiently, do not succumb to the temptation to click that button. The makers of the website know how hard it is to resist the temptation. The moment we believe that our computer's health is at risk, we will gladly click on whatever button is available. Essentially, the trick is that the website owners and designers have played you into thinking that your own computer is delivering the message that it needs to rid your computer of a virus when, in fact, the website itself is prompting you with its own internal message.

Be The Master Hacker of The 21st Century A book that will teach you all you need to know! If you are aspiring to be a hacker, then you came to the right page! However, this book is for those who have good intentions, and who wants to learn the in's and out of hacking. Become The Ultimate Hacker - Computer Virus, Cracking, Malware, IT Security is now on its 2nd Edition! This book serves as a perfect tool for anyone who wants to learn and become more familiarized with how things are done. Especially that there are two sides to this piece of work, this book will surely turn you into the best white hacker that you can be. Here's what you'll find inside the book: - Cracking - An Act Different From Hacking - Malware: A Hacker's Henchman - Computer Virus: Most Common Malware - IT Security Why should you get this book? - It contains powerful information. - It will guide you to ethical

hacking. - Get to know different types of viruses and how to use them wisely. - Easy to read and straightforward guide. So what are you waiting for? Grab a copy of Become The Ultimate Hacker - Computer Virus, Cracking, Malware, IT Security - 2nd Edition TODAY and let's explore together! Have Fun!