Sans Sec560 Network Penetration Testing And Ethical

Hands-On Ethical Hacking and Network Defense
Offensive Countermeasures
Leveraging the Cyber Kill Chain for Practical Hacking and Its Detection Via Network Forensics
Learn Ethical Hacking from Scratch
Python Programming for Hackers and Reverse Engineers
Cybersecurity
Counter Hack Reloaded
The Hacker Playbook 2
Information Security Is Failing. Breaches Are Epidemic. How Can We Fix This Broken Industry?
Cybersecurity Career Master Plan
Python Programming for Hackers and Pentesters
Starting a Career as an Ethical Hacker
Practical Malware Analysis
Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition
Learning Python for Forensics
Hacking Kubernetes
Hacking Exposed Wireless
Investigate network attacks and find evidence using common network forensic tools
Upgrading, Deploying, Managing, and Securing Windows 7
Ethical Hacking 101
A Hacker's Guide to Online Intelligence Gathering Tools and Techniques
Hacking
Gray Hat Python
A Step-by-step Guide to Computer Attacks and Effective Defenses
A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
Violent Python
Advanced Penetration Testing
Network Forensics
Red Team Development and Operations
Hackers Beware
Black Hat Python
Your stepping stone to penetration testing
The Hands-On Guide to Dissecting Malicious Software
Penetration Testing: Procedures & Methodologies
Neurobiology For Dummies
Hacking the World's Most Secure Networks
Managing Systems, Conducting Testing, and Investigating Intrusions
Mastering Metasploit

HERRERA HEZEKIAH

Hands-On Ethical Hacking and Network Defense Syngress
Explains how and why hackers break into computers, steal information, and deny services to machines' legitimate users, and discusses strategies and tools used by hackers and how to defend against them.
Offensive Countermeasures Createspace Independent Publishing Platform
Get started with cybersecurity and progress with the help of expert tips to get certified, find a job, and more Key Features Learn how to follow your desired career path that results in a well-paid, rewarding job in cybersecurity Explore expert tips relating to career paths and certification options Access informative content from a panel of experienced cybersecurity experts Book Description Cybersecurity is an emerging career trend and will continue to become increasingly important. Despite the lucrative pay and significant career growth opportunities, many people are unsure of how to get started. This book is designed by leading industry experts to help you enter the world of cybersecurity with confidence, covering everything from gaining the right certification to tips and tools for finding your first job. The book starts by helping you gain a foundational understanding of cybersecurity, covering cyber law, cyber policy, and frameworks. Next, you'll focus on how to choose the career field best suited to you from options such as security operations, penetration testing, and risk analysis. The book also guides you through the different certification options as well as the pros and cons of a formal college education versus formal certificate courses. Later, you'll discover the importance of defining and understanding your brand. Finally, you'll get up to speed with different career paths and learning opportunities. By the end of this cyber book, you will have gained the knowledge you need to clearly define your career path and develop goals relating to career progression. What you will learn Gain an understanding of cybersecurity essentials, including the different frameworks and laws, and specialties Find out how to land your first job in the cybersecurity industry Understand the difference between college education and certificate courses Build goals and timelines to encourage a work/life balance while delivering value in your job Understand the different types of cybersecurity jobs available and what it means to be entry-level Build affordable, practical labs to develop your technical skills Discover how to set goals and maintain momentum after landing your first cybersecurity job Who this book is for This book is for college graduates, military veterans transitioning from active service, individuals looking to make a mid-career switch, and aspiring IT professionals. Anyone who considers cybersecurity as a potential career field but feels intimidated, overwhelmed, or unsure of where to get started will also find this book useful.
Leveraging the Cyber Kill Chain for Practical Hacking and Its Detection Via Network Forensics John Wiley & Sons
JUMPSTART YOUR NEW AND EXCITING CAREER AS A PENETRATION TESTER The Pentester BluePrint: Your Guide to Being a Pentester offers readers a chance to delve deeply into the world of the ethical, or "white-hat" hacker. Accomplished pentester and author Phillip L. Wylie and cybersecurity researcher Kim Crawley walk you through the basic and advanced topics necessary to understand how to make a career out of finding vulnerabilities in systems, networks, and applications. You'll learn about the role of a penetration tester, what a pentest involves, and the prerequisite knowledge you'll need to start the educational journey of becoming a pentester. Discover how to develop a plan by assessing your current skillset and finding a starting place to begin growing your knowledge and skills. Finally, find out how to become employed as a pentester by using social media, networking strategies, and community involvement. Perfect for IT workers and entry-level information security professionals, The Pentester BluePrint also belongs on the bookshelves of anyone seeking to transition to the exciting and in-demand field of penetration testing. Written in a highly approachable and accessible style, The Pentester BluePrint avoids unnecessarily technical lingo in favor of concrete advice and practical strategies to help you get your start in pentesting. This book will teach you: The foundations of pentesting, including basic IT skills like operating systems, networking, and security systems The development of hacking skills and a hacker mindset Where to find educational options, including college and university classes, security training providers, volunteer work, and self-study Which certifications and degrees are most useful for gaining employment as a pentester How to get experience in the pentesting field, including labs, CTFs, and bug bounties
Learn Ethical Hacking from Scratch Sams Publishing
Cutting-edge techniques for finding and fixing critical security flaws Fortify your network and avert digital catastrophe with proven strategies from a team of security experts. Completely updated and featuring 13 new chapters, Gray Hat Hacking, The Ethical Hacker’s Handbook, Fifth Edition explains the enemy’s current weapons, skills, and tactics and offers field-tested remedies, case studies, and ready-to-try testing labs. Find out how hackers gain access, overtake network devices, script and inject malicious code, and plunder Web applications and browsers. Android-based exploits, reverse engineering techniques, and cyber law are thoroughly covered in this state-of-the-art resource. And the new topic of exploiting the Internet of things is introduced in this edition. •Build and launch spoofing exploits with Ettercap •Induce error conditions and crash software using fuzzers •Use advanced reverse engineering to exploit Windows and Linux software •Bypass Windows Access Control and memory protection schemes •Exploit web applications with Padding Oracle Attacks •Learn the use-after-free technique used in recent zero days •Hijack web browsers with advanced XSS attacks •Understand ransomware and how it takes control of your desktop •Dissect Android malware with JEB and DAD decompilers •Find one-day vulnerabilities with binary diffing •Exploit wireless systems with Software Defined Radios (SDR) •Exploit Internet of things devices •Dissect and exploit embedded devices •Understand bug bounty programs •Deploy next-generation honeypots •Dissect ATM malware and analyze common ATM attacks •Learn the business side of ethical hacking
Python Programming for Hackers and Reverse Engineers John Wiley & Sons
Come hackeare professionalmente in meno di 21 giorni! Comprendere la mente dell’hacker, realizzare ricognizioni, scansioni ed enumerazione, effettuazione di exploit, come

scrivere una relazione professionale, e altro ancora! Contenuto: •La cerchia dell'hacking •Tipi di hacking, modalità e servizi opzionale •Riconoscimento passivo e attivo •Google hacking, WhoIs e nslookup •Footprinting con Maltego e Sam Spade •Metodi di scansione e stati della porta •Scansione con NMAP •Analisi della vulnerabilità con Nexpose e OpenVAS •Enumerazione di Netbios •Meccanismi di hacking •Metasploit Framework •Attacchi di chiave •Attacchi di malware •Attacchi DoS •Windows hacking con Kali Linux e Metasploit •Hacking Wireless con Aircrack-ng •Cattura di chiavi con sniffer di rete •Attacchi MITM con Ettercap e Wireshark •Ingegneria sociale con il SET Toolkit •Phishing e iniettando malware con SET •Hacking Metasploitable Linux con Armitage •Suggerimenti per scrivere una buona relazione di controllo •Certificazioni di sicurezza informatica e hacking pertinente

Cybersecurity No Starch Press

CompTIA Security+ Study Guide (Exam SY0-601) John Wiley & Sons

Gain basic skills in network forensics and learn how to apply them effectively Key Features Investigate network threats with ease Practice forensics tasks such as intrusion detection, network analysis, and scanning Learn forensics investigation at the network level Book Description Network forensics is a subset of digital forensics that deals with network attacks and their investigation. In the era of network attacks and malware threat, it’s now more important than ever to have skills to investigate network attacks and vulnerabilities. Hands-On Network Forensics starts with the core concepts within network forensics, including coding, networking, forensics tools, and methodologies for forensic investigations. You’ll then explore the tools used for network forensics, followed by understanding how to apply those tools to a PCAP file and write the accompanying report. In addition to this, you will understand how statistical flow analysis, network enumeration, tunneling and encryption, and malware detection can be used to investigate your network. Towards the end of this book, you will discover how network correlation works and how to bring all the information from different types of network devices together. By the end of this book, you will have gained hands-on experience of performing forensics analysis tasks. What you will learn Discover and interpret encrypted traffic Learn about various protocols Understand the malware language over wire Gain insights into the most widely used malware Correlate data collected from attacks Develop tools and custom scripts for network forensics automation Who this book is for The book targets incident responders, network engineers, analysts, forensic engineers and network administrators who want to extend their knowledge from the surface to the deep levels of understanding the science behind network protocols, critical indicators in an incident and conducting a forensic search over the wire.

Counter Hack Reloaded Beaver's Pond Press

Violent Python shows you how to move from a theoretical understanding of offensive computing concepts to a practical implementation. Instead of relying on another attacker’s tools, this book will teach you to forge your own weapons using the Python programming language. This book demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts. It also shows how to write code to intercept and analyze network traffic using Python, craft and spoof wireless frames to attack wireless and Bluetooth devices, and how to data-mine popular social media websites and evade modern anti-virus. Demonstrates how to write Python scripts to automate large-scale network attacks, extract metadata, and investigate forensic artifacts Write code to intercept and analyze network traffic using Python. Craft and spoof wireless frames to attack wireless and Bluetooth devices Data-mine popular social media websites and evade modern anti-virus

The Hacker Playbook 2 Packt Publishing Ltd

Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore. Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it. You'll learn how to: –Automate tedious reversing and security tasks –Design and program your own debugger –Learn how to fuzz Windows drivers and create powerful fuzzers from scratch –Have fun with code and library injection, soft and hard hooking techniques, and other software trickery –Sniff secure traffic out of an encrypted web browser session –Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more The world's best hackers are using Python to do their handiwork. Shouldn't you?

Information Security Is Failing. Breaches Are Epidemic. How Can We Fix This Broken Industry? Prentice Hall

Kali Linux is an open source Linux distribution for security, digital forensics, and penetration testing tools, and is now an operating system for Linux users. It is the successor to BackTrack, the world's most popular penetration testing distribution tool. In this age, where online information is at its most vulnerable, knowing how to execute penetration testing techniques such as wireless and password attacks, which hackers use to break into your system or network, help you plug loopholes before it's too late and can save you countless hours and money.Kali Linux Cookbook, Second Edition is an invaluable guide, teaching you how to install Kali Linux and set up a virtual environment to perform your tests. You will learn how to eavesdrop and intercept traffic on wireless networks, bypass intrusion detection systems, attack web applications, check for open ports, and perform data forensics.This book follows the logical approach of a penetration test from start to finish with many screenshots and illustrations that help to explain each tool in detail. This book serves as an excellent source of information for security professionals and novices alike.

Cybersecurity Career Master Plan Packt Publishing Ltd

The comprehensive A-to-Z guide on network security, fully revised and updated Network security is constantly evolving, and this comprehensive guide has been thoroughly updated to cover the newest developments. If you are responsible for network security, this is the reference you need at your side. Covering new techniques, technology, and methods for approaching security, it also examines new trends and best practices being used by many organizations. The revised Network Security Bible complements the Cisco Academy course instruction in networking security. Covers all core areas of network security and how they interrelate Fully revised to address new techniques, technology, and methods for securing an enterprise worldwide Examines new trends and best practices in use by organizations to secure their

enterprises Features additional chapters on areas related to data protection/correlation and forensics Includes cutting-edge topics such as integrated cybersecurity and sections on Security Landscape, with chapters on validating security, data protection, forensics, and attacks and threats If you need to get up to date or stay current on network security, Network Security Bible, 2nd Edition covers everything you need to know.

Python Programming for Hackers and Pentesters Applied Incident Response

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

Starting a Career as an Ethical Hacker Jones & Bartlett Learning

This is a perfect and magnificent lined journal for you to take to your meetings. A funny journal that will get you through them. Also would make a great gift for a co-worker. This is great as a journal or notebook perfect for you to write your own thoughts and everything in your mind, get a little creative with poetry or just writing down lists or ideas. It is a 100 pages blank ruled journal ready for you to fill with your own writing and get a little creative every now and then. DETAILS: 100 Pages Lined Sheets High Quality Paper 6" x 9" Paperback notebook, soft matte cover Perfect for gel pen, ink or pencils Perfet & great size to carry everywhere in your bag, for school, for high school, college... Great gift for any special occasion: Christmas, Secret Santa, Birthday, lovers...

Practical Malware Analysis Apress

Curious abot how to perform penetration testings? Have you always wanted to become an ethical hacker but haven't got the time or the money to take expensive workshops? Then this book is for you! With just 2 hours of daily dedication you could be able to start your practice as an ethical hacker, of course as long as you not only read the chapters but perform all the labs included with this book. Table of contents: - Chapter 1 - Introduction to Ethical Hacking - Chapter 2 - Reconnaissance or footprinting - Chapter 3 - Scanning - Chapter 4 - Enumeration - Chapter 5 - Exploitation or hacking - Chapter 6 - Writing the audit report without suffering a mental breakdown - Chapter 7 - Relevant international certifications - Final Recommendations - Please leave us a review - About the author - Glossary of technical terms - Apendix A: Tips for succesful labs - Notes and references Note: The labs are updated for Kali Linux 2!

Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition "O'Reilly Media, Inc."

The skills and tools for collecting, verifying and correlating information from different types of systems is an essential skill when tracking down hackers. This book explores Open Source Intelligence Gathering (OSINT) inside out from multiple perspectives, including those of hackers and seasoned intelligence experts. OSINT refers to the techniques and tools required to harvest publicly available data concerning a person or an organization. With several years of experience of tracking hackers with OSINT, the author whips up a classical plot-line involving a hunt for a threat actor. While taking the audience through the thrilling investigative drama, the author immerses the audience with in-depth knowledge of state-of-the-art OSINT tools and techniques. Technical users will want a basic understanding of the Linux command line in order to follow the examples. But a person with no Linux or programming experience can still gain a lot from this book through the commentaries. This book’s unique digital investigation proposition is a combination of story-telling, tutorials, and case studies. The book explores digital investigation from multiple angles: Through the eyes of the author who has several years of experience in the subject. Through the mind of the hacker who collects massive amounts of data from multiple online sources to identify targets as well as ways to hit the targets. Through the eyes of industry leaders. This book is ideal for: Investigation professionals, forensic analysts, and CISO/CIO and other executives wanting to understand the mindset of a hacker and how seemingly harmless information can be used to target their organization. Security analysts, forensic investigators, and SOC teams looking for new approaches on digital investigations from the perspective of collecting and parsing publicly available information. CISOs and defense teams will find this book useful because it takes the perspective of infiltrating an organization from the mindset of a hacker. The commentary provided by outside experts will also provide them with ideas to further protect their organization’s data.

Learning Python for Forensics John Wiley & Sons

Want to run your Kubernetes workloads safely and securely? This practical book provides a threat-based guide to Kubernetes security. Each chapter examines a particular component's architecture and potential default settings and then reviews existing high-profile attacks and historical Common Vulnerabilities and Exposures (CVEs). Authors Andrew Martin and Michael Hausenblas share best-practice configuration to help you harden clusters from possible angles of attack. This book begins with a vanilla Kubernetes installation with built-in defaults. You'll examine an abstract threat model of a distributed system running arbitrary workloads, and then progress to a detailed assessment of each component of a secure Kubernetes system. Understand where your Kubernetes system is vulnerable with threat modelling techniques Focus on pods, from configurations to attacks and defenses Secure your cluster and workload traffic Define and enforce policy with RBAC, OPA, and Kyverno Dive deep into sandboxing and isolation techniques Learn how to detect and mitigate supply chain attacks Explore filesystems, volumes, and sensitive information at rest Discover what can go wrong when running multitenant workloads in a cluster Learn what you can do if someone breaks in despite you having controls in place

Hacking Kubernetes McGraw Hill Professional

This guide empowers network and system administrators to defend their information and computing assets--whether or not

they have security experience. Skoudis presents comprehensive, insider's explanations of today's most destructive hacker tools and tactics, and specific, proven countermeasures for both UNIX and Windows environments.

Hacking Exposed Wireless No Starch Press

The Most Comprehensive Hacking Beginners Guide! Usually priced at $16.38, buy now to get a limited time discount and get it for only $13.38!! OFFER* Buy a paperback copy of this hacking book and receive the Kindle version for only .99 cents! Coming Soon - Other Books In This Series- Hacking: Cardinal Rules for Success. Don't miss out!! Have you watched the news lately? They can't stop talking about Hacking. It is portrayed in movies, shouted about in media headlines, and typically gets a lot of attention. In fact, in the run up to the 2016 US Presidential election, there were allegations made nearly everyday that the Russians were influencing the election by hacking into American databases and systems. And who can forget Julian Assange and his infamous WikiLeaks that successfully hacked into hundreds of thousands of emails and whose actions may have kept Hillary Clinton out of the White House. All this is commonly known as black hat hacking- where the hacker gets onto a network in the hopes of obtaining information that was not intended for his/ her use. However, there is another side of hacking- known as ethical hacking- that operates within the legal frameworks. In fact, many companies pay "ethical hackers" hefty salaries to keep their organization's information safe. After reading this book, there's no reason you can't become one of those individuals and dramatically increase your paycheck!! Of course, this book is a Beginners Guide so it is not all inclusive. We have more books on the way that will go into a more technical analysis of hacking, provide detailed tips and strategies, and a more advanced guide. Stay tuned and subscribe to our email list to get the best deals!! This extensive beginners guide will start you off on the right foot. We will go into details about hacking in all its various aspects. You will learn all the terminology you require, the differences between ethical and criminal hacking, and even some basic hacks that can be used, even when you're just protecting your own network. Here Is A Preview Of What You'll Discover... The basics of hacking including common terms and misconceptions How to hack passwords Ethical hacking versus criminal hacking Passive and active attacks Some practical uses for hacking How to map out your own hack to find vulnerabilities in the system Some simple spoofing and man in the middle attack techniques Popular tools and software you should use when starting out with hacking And More! Are You Ready To Begin Your Adventure To Becoming A Genius Hacker? Click The Buy Now With 1-Click Button Now And Enjoy This Book For A Limited Time Discount

Investigate network attacks and find evidence using common network forensic tools Pearson

Learn the art of designing, developing, and deploying innovative forensic solutions through Python About This Book This practical guide will help you solve forensic dilemmas through the development of Python scripts Analyze Python scripts to extract metadata and investigate forensic artifacts Master the skills of parsing complex data structures by taking advantage of Python libraries Who This Book Is For If you are a forensics student, hobbyist, or professional that is seeking to increase your understanding in forensics through the use of a programming language, then this book is for you. You are not required to have previous experience in programming to learn and master the content within this book. This material, created by forensic professionals, was written with a unique perspective and understanding of examiners who wish to learn programming What You Will Learn Discover how to perform Python script development Update yourself by learning the best practices in forensic programming Build scripts through an iterative design Explore the rapid development of specialized scripts Understand how to leverage forensic libraries developed by the community Design flexibly to accommodate present and future hurdles Conduct effective and efficient investigations through programmatic pre-analysis Discover how to transform raw data into customized reports and visualizations In Detail This book will illustrate how and why you should learn Python to strengthen your analysis skills and efficiency as you creatively solve real-world problems through instruction-based tutorials. The tutorials use an interactive design, giving you experience of the development process so you gain a better understanding of what it means to be a forensic developer. Each chapter walks you through a forensic artifact and one or more methods to analyze the evidence. It also provides reasons why one method may be advantageous over another. We cover common digital forensics and incident response scenarios, with scripts that can be used to tackle case work in the field. Using built-in and community-sourced libraries, you will improve your problem solving skills with the addition of the Python scripting language. In addition, we provide resources for further exploration of each script so you can understand what further purposes Python can serve. With this knowledge, you can rapidly develop and deploy solutions to identify critical information and fine-tune your skill set as an examiner. Style and approach The book begins by instructing you on the basics of Python, followed by chapters that include scripts targeted for forensic casework. Each script is described step by step at an introductory level, providing gradual growth to demonstrate the available functionalities of Python.

Upgrading, Deploying, Managing, and Securing Windows 7 Cengage Learning

A must-have, hands-on guide for working in the cybersecurityprofession Cybersecurity involves preventative methods to protectinformation from attacks. It requires a thorough understanding ofpotential threats, such as viruses and other malicious code, aswell as system vulnerability and security architecture. Thisessential book addresses cybersecurity strategies that includeidentity management, risk management, and incident management, andalso serves as a detailed guide for anyone looking to enter thesecurity profession. Doubling as the text for a cybersecuritycourse, it is also a useful reference for cybersecurity testing, ITtest/development, and system/network administration. Covers everything from basic network administration securityskills through advanced command line scripting, tool customization,and log analysis skills Dives deeper into such intense topics as wireshark/tcpdumpfiltering, Google hacks, Windows/Linux scripting, Metasploitcommand line, and tool customizations Delves into network administration for Windows, Linux, andVMware Examines penetration testing, cyber investigations, firewallconfiguration, and security tool customization Shares techniques for cybersecurity testing, planning, andreporting Cybersecurity: Managing Systems, Conducting Testing, andInvestigating Intrusions is a comprehensive and authoritativelook at the critical topic of cybersecurity from start tofinish.