Blue Team Field Manual Btfm Rtfm

A reference manual for Linux that has descriptions of core functions and and has command line tools, with popular applications such as docker and kubectl

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 how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the

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

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

Want Red Team offensive advice from the biggest cybersecurity names in the industry? Join our tribe. The Tribe of Hackers team is back with a new guide packed with insights from dozens of the world's leading Red Team security specialists. With their deep knowledge of system vulnerabilities and innovative solutions for correcting security flaws, Red Team hackers are in high demand. Tribe of Hackers Red Team: Tribal Knowledge from the Best in Offensive Cybersecurity takes the valuable lessons and popular interview format from the original Tribe of Hackers and dives deeper into the world of Red Team security with expert

perspectives on issues like penetration testing and ethical hacking. This unique guide includes inspiring interviews from influential security specialists, including David Kennedy, Rob Fuller, Jayson E. Street, and Georgia Weidman, who share their real-world learnings on everything from Red Team tools and tactics to careers and communication, presentation strategies, legal concerns, and more Learn what it takes to secure a Red Team job and to stand out from other candidates Discover how to hone your hacking skills while staying on the right side of the law Get tips for collaborating on documentation and reporting Explore ways to garner support from leadership on your security proposals Identify the most important control to prevent compromising your network Uncover the latest tools for Red Team offensive security Whether you're new to Red Team security, an experienced practitioner, or ready to lead your own team, Tribe of Hackers Red Team has the real-world advice and practical guidance you need to advance your information security career and ready yourself for the Red Team offensive.

Applied Incident Response

Best Practices for Securing Infrastructure

Red Team Development and Operations
Analyzing Computer Security
Infrastructure security with Red Team and Blue Team tactics
Learn C# in One Day and Learn It Well
A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers

The Red Team Field Manual (RTFM) is a no fluff, but thorough reference guide for serious Red Team members who routinely find themselves on a mission without Google or the time to scan through a man page. The RTFM contains the basic syntax for commonly used Linux and Windows command line tools, but it also encapsulates unique use cases for powerful tools such as Python and Windows PowerShell. The RTFM will repeatedly save you time looking up the hard to remember Windows nuances such as Windows wmic and dsquery command line tools, key registry values, scheduled tasks syntax, startup locations and Windows scripting. More importantly, it should teach you some new red team techniques.

Build a better defense against motivated, organized, professional attacks Advanced Penetration Testing: Hacking the World's Most Secure Networks takes hacking far beyond Kali linux and Metasploit to provide a more complex attack simulation. Featuring techniques not taught in any certification prep or covered by common defensive scanners, this book integrates social engineering, programming, and

vulnerability exploits into a multidisciplinary approach for targeting and compromising high security environments. From discovering and creating attack vectors, and moving unseen through a target enterprise, to establishing command and exfiltrating data—even from organizations without a direct Internet connection—this guide contains the crucial techniques that provide a more accurate picture of your system's defense. Custom coding examples use VBA, Windows Scripting Host, C, Java, JavaScript, Flash, and more, with coverage of standard library applications and the use of scanning tools to bypass common defensive measures. Typical penetration testing consists of low-level hackers attacking a system with a list of known vulnerabilities, and defenders preventing those hacks using an equally well-known list of defensive scans. The professional hackers and nation states on the forefront of today's threats operate at a much more complex level—and this book shows you how to defend your high security network. Use targeted social engineering pretexts to create the initial compromise Leave a command and control structure in place for long-term access Escalate privilege and breach networks, operating systems, and trust structures Infiltrate further using harvested credentials while expanding control Today's threats are organized, professionally-run, and very much for-profit. Financial institutions, health care organizations, law enforcement, government agencies, and other high-value targets need to harden their IT infrastructure and human capital against targeted advanced attacks from motivated professionals. Advanced Penetration Testing goes beyond Kali

linux and Metasploit and to provide you advanced pen testing for high security networks.

Analyzing how hacks are done, so as to stop them in thefuture Reverse engineering is the process of analyzing hardware orsoftware and understanding it, without having access to the sourcecode or design documents. Hackers are able to reverse engineersystems and exploit what they find with scary results. Now the goodguys can use the same tools to thwart these threats. PracticalReverse Engineering goes under the hood of reverse engineeringfor security analysts, security engineers, and system programmers,so they can learn how to use these same processes to stop hackersin their tracks. The book covers x86, x64, and ARM (the first book to cover allthree); Windows kernel-mode code rootkits and drivers; virtualmachine protection techniques; and much more. Best of all, itoffers a systematic approach to the material, with plenty ofhands-on exercises and real-world examples. Offers a systematic approach to understanding reverseengineering, with hands-on exercises and real-world examples Covers x86, x64, and advanced RISC machine (ARM) architecturesas well as deobfuscation and virtual machine protectiontechniques Provides special coverage of Windows kernel-mode code(rootkits/drivers), a topic not often covered elsewhere, andexplains how to analyze drivers step by step Demystifies topics that have a steep learning curve Includes a bonus chapter on reverse engineering tools Practical Reverse Engineering: Using x86, x64, ARM, WindowsKernel, and Reversing Tools provides

crucial, up-to-dateguidance for a broad range of IT professionals.

The shocking untold story of the elite secret society of hackers fighting to protect our privacy, our freedom -- even democracy itself Cult of the Dead Cow is the tale of the oldest, most respected, and most famous American hacking group of all time. Though until now it has remained mostly anonymous, its members invented the concept of hacktivism, released the top tool for testing password security, and created what was for years the best technique for controlling computers from afar, forcing giant companies to work harder to protect customers. They contributed to the development of Tor, the most important privacy tool on the net, and helped build cyberweapons that advanced US security without injuring anyone. With its origins in the earliest days of the Internet, the cDc is full of oddball characters -- activists, artists, even future politicians. Many of these hackers have become top executives and advisors walking the corridors of power in Washington and Silicon Valley. The most famous is former Texas Congressman and current presidential candidate Beto O'Rourke, whose time in the cDc set him up to found a tech business, launch an alternative publication in El Paso, and make long-shot bets on unconventional campaigns. Today, the group and its followers are battling electoral misinformation, making personal data safer, and battling to keep technology a force for good instead of for surveillance and oppression. Cult of the Dead Cow shows how governments, corporations, and criminals came to hold immense power over individuals and how we can fight back against them.

Practical Reverse Engineering
Tribe of Hackers Red Team
Red Team + OSINT + Blue Team Reference
The Complete Team Field Manual
A Condensed Guide for the Security Operations Team and Threat Hunter
UNIX and Linux System Administration Handbook
Nmap Network Scanning

The official guide to the Nmap Security Scanner, a free and open source utility used by millions of people, suits all levels of security and networking professionals.

The first book to reveal and dissect the technical aspect of many social engineering maneuvers From elicitation, pretexting, influence and manipulation all aspects of social engineering are picked apart, discussed and explained by using real world examples, personal experience and the science behind them to unraveled the mystery in social engineering. Kevin Mitnick—one of the most famous social engineers in the world—popularized the term "social engineering." He explained that it is much easier to trick someone into revealing a

password for a system than to exert the effort of hacking into the system. Mitnick claims that this social engineering tactic was the single-most effective method in his arsenal. This indispensable book examines a variety of maneuvers that are aimed at deceiving unsuspecting victims, while it also addresses ways to prevent social engineering threats. Examines social engineering, the science of influencing a target to perform a desired task or divulge information Arms you with invaluable information about the many methods of trickery that hackers use in order to gather information with the intent of executing identity theft, fraud, or gaining computer system access Reveals vital steps for preventing social engineering threats Social Engineering: The Art of Human Hacking does its part to prepare you against nefarious hackers—now you can do your part by putting to good use the critical information within its pages.

Just as a professional athlete doesn't show up without a solid game plan, ethical hackers, IT professionals, and security researchers should not be unprepared, either. The Hacker

Playbook provides them their own game plans. Written by a longtime security professional and CEO of Secure Planet, LLC, this step-by-step guide to the "game" of penetration hacking features hands-on examples and helpful advice from the top of the field. Through a series of football-style "plays," this straightforward guide gets to the root of many of the roadblocks people may face while penetration testing-including attacking different types of networks, pivoting through security controls, privilege escalation, and evading antivirus software. From "Pregame" research to "The Drive" and "The Lateral Pass," the practical plays listed can be read in order or referenced as needed. Either way, the valuable advice within will put you in the mindset of a penetration tester of a Fortune 500 company, regardless of your career or level of experience. This second version of The Hacker Playbook takes all the best "plays" from the original book and incorporates the latest attacks, tools, and lessons learned. Double the content compared to its predecessor, this guide further outlines building a lab, walks through test cases for attacks, and

provides more customized code. Whether you're downing energy drinks while desperately looking for an exploit, or preparing for an exciting new job in IT security, this guide is an essential part of any ethical hacker's library-so there's no reason not to get in the game.

A practical handbook to cybersecurity for both tech and non-tech professionals As reports of major data breaches fill the headlines, it has become impossible for any business, large or small, to ignore the importance of cybersecurity. Most books on the subject, however, are either too specialized for the non-technical professional or too general for positions in the IT trenches. Thanks to author Nadean Tanner's wide array of experience from teaching at a University to working for the Department of Defense, the Cybersecurity Blue Team Toolkit strikes the perfect balance of substantive and accessible, making it equally useful to those in IT or management positions across a variety of industries. This handy guide takes a simple and strategic look at best practices and tools available to both cybersecurity management and hands-on professionals,

whether they be new to the field or looking to expand their expertise. Tanner gives comprehensive coverage to such crucial topics as security assessment and configuration, strategies for protection and defense, offensive measures, and remediation while aligning the concept with the right tool using the CIS Controls version 7 as a guide. Readers will learn why and how to use fundamental open source and free tools such as ping, tracert, PuTTY, pathping, sysinternals, NMAP, OpenVAS, Nexpose Community, OSSEC, Hamachi, InSSIDer, Nexpose Community, Wireshark, Solarwinds Kiwi Syslog Server, Metasploit, Burp, Clonezilla and many more. Up-to-date and practical cybersecurity instruction, applicable to both management and technical positions • Straightforward explanations of the theory behind cybersecurity best practices • Designed to be an easily navigated tool for daily use • Includes training appendix on Linux, how to build a virtual lab and glossary of key terms The Cybersecurity Blue Team Toolkit is an excellent resource for anyone working in digital policy as well as IT security professionals, technical analysts, program

managers, and Chief Information and Technology Officers. This is one handbook that won't gather dust on the shelf, but remain a valuable reference at any career level, from student to executive.

The Hacker Playbook 2

Violent Python

(Black & Blue)

Rtfm

Army Field Manual FM 22-100 (the U. S. Army Leadership Field Manual)

Incident Response Edition: a Condensed Field Guide for the Cyber Security Incident Responder

Password Cracking Manual

Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781119643371) was previously published as Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World (9781793464187). While this version features a new cover design and introduction, the remaining content is the same as the prior release and should not be considered a

new or updated product. Looking for real-world advice from leading cybersecurity experts? You've found your tribe. Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World is your guide to joining the ranks of hundreds of thousands of cybersecurity professionals around the world. Whether you're just joining the industry, climbing the corporate ladder, or considering consulting, Tribe of Hackers offers the practical know-how, industry perspectives, and technical insight you need to succeed in the rapidly growing information security market. This unique guide includes inspiring interviews from 70 security experts, including Lesley Carhart, Ming Chow, Bruce Potter, Robert M. Lee, and Jayson E. Street. Get the scoop on the biggest cybersecurity myths and misconceptions about security Learn what qualities and credentials you need to advance in the cybersecurity field Uncover which life hacks are worth your while Understand how social media and the Internet of Things has changed cybersecurity Discover what it takes to make the move from the corporate world to your

own cybersecurity venture Find your favorite hackers online and continue the conversation Tribe of Hackers is a must-have resource for security professionals who are looking to advance their careers, gain a fresh perspective, and get serious about cybersecurity with thought-provoking insights from the world's most noteworthy hackers and influential security specialists.

This edition of the US Army Leadership Field Manual (FM 22-100) establishes a unified leadership theory for all Army leaders based on the Army leadership framework and three leadership levels. Specifically, it-- * Defines and discusses Army values and leader attributes. * Discusses character-based leadership. * Establishes leader attributes as part of character. * Focuses on improving people and organizations for the long term. * Outlines three levels of leadership--direct, organizational, and strategic. * Identifies four skill domains that apply at all levels. * Specifies leadership actions for each level. The Army leadership framework brings together many existing

leadership concepts by establishing leadership dimensions and showing how they relate to each other. Solidly based on BE, KNOW, DO--that is character, competence, and action--the Army leadership framework provides a single instrument for leader development. Individuals can use it for self-development. Leaders can use it to develop subordinates. Commanders can use it to focus their programs. By establishing leadership dimensions grouped under the skill domains of values, attributes, skills, and actions, the Army leadership framework provides a simple way to think about and discuss leadership. The Army is a values-based institution. This field manual establishes and clarifies those values. Army leaders must set high standards, lead by example, do what is legally and morally right, and influence other people to do the same. They must establish and sustain a climate that ensures people are treated with dignity and respect and create an environment in which people are challenged and motivated to be all they can be. This field manual discusses these aspects of leadership and how they

contribute to developing leaders of character and competence.

A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker’s perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you’ll look for flaws and their known exploits—including tools developed by real-world government financed state-actors. • An introduction to the same hacking techniques that malicious hackers will use against an organization •

Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws • Based on the tried and tested material used to train hackers all over the world in the art of breaching networks • Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to

advanced techniques in a structured learning format. Master C# Programming with a unique Hands-On Project (Updated for VS Community 2017) Have you always wanted to learn computer programming but are afraid it'll be too difficult for you? Or perhaps you know other programming languages but are interested in learning the C# language fast? This book is for you. You no longer have to waste your time and money learning C# from boring books that are 600 pages long, expensive online courses or complicated C# tutorials that just leave you more confused. What this book offers... C# for Beginners Complex concepts are broken down into simple steps to ensure that you can easily master the C# language even if you have never coded before. Carefully Chosen C# Examples Examples are carefully chosen to illustrate all concepts. In addition, the output for all examples are provided immediately so you do not have to wait till you have access to your computer to test the examples. Careful selection of topics Topics are carefully selected to give you a broad exposure to C#, while not overwhelming you

with information overload. These topics include object-oriented programming concepts, error handling techniques, file handling techniques and more. Learn The C# Programming Language Fast Concepts are presented in a "to-the-point" style to cater to the busy individual. With this book, you can learn C# in just one day and start coding immediately. How is this book different... The best way to learn C# is by doing. At the end of the book, you'll be guided through a unique project that requires the application of all the concepts taught previously. Working through the project will not only help you see how it all ties together, it'll also give you an immense sense of achievement and the exhilaration of turning lines of code into a finished product that you can be proud of! Are you ready to dip your toes into the exciting world of C# coding? This book is for you. Click the "Add to Cart" button to buy it now. What you'll learn: Introduction to C#- What is C#? - How to install and run Visual Studio Community 2015? Data types and Operators - What are the common data types in C#? - What are

arrays and lists? - How to format C# strings - What is a value type vs reference type? - What are the common C# operators? Object Oriented Programming - What is object oriented programming? - How to write your own classes - What are fields, properties, methods and constructors? - What is encapsulation, inheritance and polymorphism? - What is an abstract class and interface? - What is an enum and struct? Controlling the Flow of a Program- What are condition statements? - How to use control flow statements in C# - What are jump statements? - How to handle errors and exceptions and Others...- How to accept user inputs and display outputs - How to use LINQ to save yourself from hours of work - How to work with external files ...and so much more.... Finally, you'll be guided through a hands-on project that requires the application of all the topics covered. Click the BUY button at the top of this page now to start learning C#. Learn it fast and learn it well.

Hacking the World's Most Secure Networks

Offensive Countermeasures

Operator Handbook
Tribal Knowledge from the Best in Offensive Cybersecurity
PTFM
The Art of Deception
Practical Binary Analysis

“ As an author, editor, and publisher, I never paid much attention to the competition—except in a few cases. This is one of those cases. The UNIX System Administration Handbook is one of the few books we ever measured ourselves against. ” —Tim O ’ Reilly, founder of O ’ Reilly Media “ This edition is for those whose systems live in the cloud or in virtualized data centers; those whose administrative work largely takes the form of automation and configuration source code; those who collaborate closely with developers, network engineers, compliance officers, and all the other worker bees who inhabit the modern hive. ” —Paul Vixie, Internet Hall of Fame-recognized innovator and founder of ISC and Farsight Security “ This book is fun and functional as a desktop reference. If you use UNIX and Linux systems, you need this book in your short-reach library. It covers a bit of the systems ’ history but doesn ’ t bloviate. It ’ s just straight-forward information delivered in a colorful and memorable fashion. ” —Jason A. Nunnelley UNIX® and Linux® System Administration Handbook, Fifth Edition, is today ’ s definitive guide to installing, configuring, and maintaining any UNIX or Linux system, including

systems that supply core Internet and cloud infrastructure. Updated for new distributions and cloud environments, this comprehensive guide covers best practices for every facet of system administration, including storage management, network design and administration, security, web hosting, automation, configuration management, performance analysis, virtualization, DNS, security, and the management of IT service organizations. The authors—world-class, hands-on technologists—offer indispensable new coverage of cloud platforms, the DevOps philosophy, continuous deployment, containerization, monitoring, and many other essential topics. Whatever your role in running systems and networks built on UNIX or Linux, this conversational, well-written ¿guide will improve your efficiency and help solve your knottiest problems.

Enhance your organization ' s secure posture by improving your attack and defense strategies Key Features Gain a clear understanding of the attack methods, and patterns to recognize abnormal behavior within your organization with Blue Team tactics. Learn to unique techniques to gather exploitation intelligence, identify risk and demonstrate impact with Red Team and Blue Team strategies. A practical guide that will give you hands-on experience to mitigate risks and prevent attackers from infiltrating your system. Book Description The book will start talking about the security posture before moving to Red Team tactics, where you will learn the basic syntax for the Windows and Linux tools that are commonly used to perform the

necessary operations. You will also gain hands-on experience of using new Red Team techniques with powerful tools such as python and PowerShell, which will enable you to discover vulnerabilities in your system and how to exploit them. Moving on, you will learn how a system is usually compromised by adversaries, and how they hack user's identity, and the various tools used by the Red Team to find vulnerabilities in a system. In the next section, you will learn about the defense strategies followed by the Blue Team to enhance the overall security of a system. You will also learn about an in-depth strategy to ensure that there are security controls in each network layer, and how you can carry out the recovery process of a compromised system. Finally, you will learn how to create a vulnerability management strategy and the different techniques for manual log analysis. By the end of this book, you will be well-versed with Red Team and Blue Team techniques and will have learned the techniques used nowadays to attack and defend systems. What you will learn Learn the importance of having a solid foundation for your security posture Understand the attack strategy using cyber security kill chain Learn how to enhance your defense strategy by improving your security policies, hardening your network, implementing active sensors, and leveraging threat intelligence Learn how to perform an incident investigation Get an in-depth understanding of the recovery process Understand continuous security monitoring and how to implement a vulnerability management strategy Learn how to perform log analysis to identify suspicious activities Who this

book is for This book aims at IT professional who want to venture the IT security domain. IT pentester, Security consultants, and ethical hackers will also find this course useful. Prior knowledge of penetration testing would be beneficial.

Blue Team Field Manual (BTFM) is a Cyber Security Incident Response Guide that aligns with the NIST Cybersecurity Framework consisting of the five core functions of Identify, Protect, Detect, Respond, and Recover by providing the tactical steps to follow and commands to use when preparing for, working through and recovering from a Cyber Security Incident.

Back for the third season, The Hacker Playbook 3 (THP3) takes your offensive game to the pro tier. With a combination of new strategies, attacks, exploits, tips and tricks, you will be able to put yourself in the center of the action toward victory. The main purpose of this book is to answer questions as to why things are still broken. For instance, with all the different security products, secure code reviews, defense in depth, and penetration testing requirements, how are we still seeing massive security breaches happening to major corporations and governments? The real question we need to ask ourselves is, are all the safeguards we are putting in place working? This is what The Hacker Playbook 3 - Red Team Edition is all about. By now, we are all familiar with penetration testing, but what exactly is a Red Team? Red Teams simulate real-world, advanced attacks to test how well your organization's defensive teams respond if you were breached. They find the answers to questions like: Do your

incident response teams have the right tools, skill sets, and people to detect and mitigate these attacks? How long would it take them to perform these tasks and is it adequate? This is where you, as a Red Teamer, come in to accurately test and validate the overall security program. THP3 will take your offensive hacking skills, thought processes, and attack paths to the next level. This book focuses on real-world campaigns and attacks, exposing you to different initial entry points, exploitation, custom malware, persistence, and lateral movement--all without getting caught! This heavily lab-based book will include multiple Virtual Machines, testing environments, and custom THP tools. So grab your helmet and let's go break things! For more information, visit http: //thehackerplaybook.com/about/.

A Practical Guide

Official Nmap Project Guide to Network Discovery and Security Scanning

The Pentester BluePrint

Red Team Field Manual

The Art of Human Hacking

Tribe of Hackers

Tribe of Hackers Blue Team

Red teams can show flaws that exist in your network before they are compromised by malicious actors and blue teams traditionally assess current security measures and identify

security flaws. The teams can provide valuable feedback to each other, but this is often overlooked, enter the purple team. The purple team allows for the integration of red team tactics and blue team security measures. The purple team field manual is a manual for all security professionals and integrates red and blue team methodologies.

Blue Team defensive advice from the biggest names in cybersecurity The Tribe of Hackers team is back. This new guide is packed with insights on blue team issues from the biggest names in cybersecurity. Inside, dozens of the world's leading Blue Team security specialists show you how to harden systems against real and simulated breaches and attacks. You'll discover the latest strategies for blocking even the most advanced red-team attacks and preventing costly losses. The experts share their hard-earned wisdom, revealing what works and what doesn't in the real world of cybersecurity. Tribe of Hackers Blue Team goes beyond the bestselling, original Tribe of Hackers book and delves into detail on defensive and preventative techniques. Learn how

to grapple with the issues that hands-on security experts and security managers are sure to build into their blue team exercises. Discover what it takes to get started building blue team skills Learn how you can defend against physical and technical penetration testing Understand the techniques that advanced red teamers use against high-value targets Identify the most important tools to master as a blue teamer Explore ways to harden systems against red team attacks Stand out from the competition as you work to advance your cybersecurity career Authored by leaders in cybersecurity attack and breach simulations, the Tribe of Hackers series is perfect for those new to blue team security, experienced practitioners, and cybersecurity team leaders. Tribe of Hackers Blue Team has the real-world advice and practical guidance you need to advance your information security career and ready yourself for the blue team defense.
Your ultimate guide to pentesting with Kali Linux Kali is a popular and powerful Linux distribution used by cybersecurity professionals around the world. Penetration

testers must master Kali's varied library of tools to be effective at their work. The Kali Linux Penetration Testing Bible is the hands-on and methodology guide for pentesting with Kali. You'll discover everything you need to know about the tools and techniques hackers use to gain access to systems like yours so you can erect reliable defenses for your virtual assets. Whether you're new to the field or an established pentester, you'll find what you need in this comprehensive guide. Build a modern dockerized environment Discover the fundamentals of the bash language in Linux Use a variety of effective techniques to find vulnerabilities (OSINT, Network Scan, and more) Analyze your findings and identify false positives and uncover advanced subjects, like buffer overflow, lateral movement, and privilege escalation Apply practical and efficient pentesting workflows Learn about Modern Web Application Security Secure SDLC Automate your penetration testing with Python

The Hash Crack: Password Cracking Manual v3 is an expanded reference guide for password recovery (cracking) methods,

tools, and analysis techniques. A compilation of basic and advanced techniques to assist penetration testers and network security professionals evaluate their organization's posture. The Hash Crack manual contains syntax and examples for the most popular cracking and analysis tools and will save you hours of research looking up tool usage. It also includes basic cracking knowledge and methodologies every security professional should know when dealing with password attack capabilities. Hash Crack contains all the tables, commands, online resources, and more to complete your cracking security kit. This version expands on techniques to extract hashes from a myriad of operating systems, devices, data, files, and images. Lastly, it contains updated tool usage and syntax for the most popular cracking tools.

Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1. 02)

Social Engineering

Lfm: Linux Field Manual

Investigating Windows Systems

Controlling the Human Element of Security

Hash Crack

Advanced Penetration Testing

The Red Team and the Blue Team are now obsolete. The only manual you need is this: "TCTFM" The Complete Team Field Manual is the most comprehensive cybersecurity manual around that includes all the different techniques and approaches of the blue and red teams. This book contains: the basic syntax for commonly used Linux and Windows command line tools unique use cases for powerful tools such as Python and Windows PowerShell five core functions of Identify, Protect, Detect, Respond, and Recover tactical steps and commands to use when preparing working through recovering commands after Cyber Security Incident more importantly, it should teach you some new secret techniques Scroll up and buy this manual. It will be the only book you will use!

Investigating Windows Systems helps readers discover the detailed tools they will need to perform research. It provides a walk-through of the analysis process, with descriptions of thought processes and an analysis of decisions made along the way. This must-have guide on the fields of digital forensic analysis and incident response doesn't simply put the pieces out to be analyzed and assembled. Instead, it presents a full understanding of what the final product is supposed to look like, providing a walk-through of the entire process, with descriptions of thought processes and an analysis and explanation of decisions made along the way. Provides the reader with a detailed walk-through of the analysis process, with decision points along the way, assisting the user in understanding the resulting data Coverage will include malware detection, user activity, and how to set up a testing environment Written at a beginner to intermediate level for anyone engaging in the field of digital forensic analysis and incident response

Tired of playing catchup with hackers? Does it ever seem they have all of the cool tools? Does it seem

like defending a network is just not fun? This books introduces new cyber-security defensive tactics to annoy attackers, gain attribution and insight on who and where they are. It discusses how to attack attackers in a way which is legal and incredibly useful.

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

Blue Team Handbook

Defensive Security Handbook

Hands on Hacking

Designing for Security

Threat Modeling

Blue Team Field Manual

Cult of the Dead Cow

Despite the increase of high-profile hacks, record-breaking data leaks, and

ransomware attacks, many organizations don't have the budget to establish or outsource an information security (InfoSec) program, forcing them to learn on the job. For companies obliged to improvise, this pragmatic guide provides a security-101 handbook with steps, tools, processes, and ideas to help you drive maximum-security improvement at little or no cost. Each chapter in this book provides step-by-step instructions for dealing with a specific issue, including breaches and disasters, compliance, network infrastructure and password management, vulnerability scanning, and penetration testing, among others. Network engineers, system administrators, and security professionals will learn tools and techniques to help improve security in sensible, manageable chunks. Learn fundamentals of starting or redesigning an InfoSec program Create a base set of policies, standards, and procedures Plan and design incident response, disaster recovery, compliance, and physical security Bolster Microsoft and Unix systems, network infrastructure, and password management Use segmentation practices and designs to compartmentalize your network Explore automated process and tools for vulnerability management Securely develop code to reduce exploitable errors Understand basic penetration testing concepts through purple teaming

Delve into IDS, IPS, SOC, logging, and monitoring
Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases provides the security practitioner with numerous field notes on building a security operations team and mining data sources to get the maximum amount of information out of them with a threat hunting approach. The author shares his fifteen years of experience with SIEMs and security operations after implementing five major platforms, integrating over one hundred data sources into various platforms, and running a MSSP practice.This book covers the topics below using a "zero fluff" approach as if you hired him as a security consultant and were sitting across the table with him (or her). Topics covered include: The book begins with a discussion for professionals to help them build a successful business case and a project plan, and deciding on SOC tier models. There is also a list of tough questions you need to consider when proposing a SOC, as well as a discussion of layered operating models. * It then goes through numerous data sources that feed a SOC and SIEM and provides specific guidance on how to use those data sources. Most of the examples presented were implemented in one organization or another. These uses cases explain how to use a SIEM and how to use the data coming into the platform, a question*

that is poorly answered by many vendors. An inventory of Security Operations Center (SOC) Services.* Several business concepts are also introduced, because they are often overlooked by IT: value chain, PESTL, and SWOT. * Metrics.* SOC staff onboarding, training topics, and desirable skills. Along these lines, there is a chapter on a day in the life of a SOC analyst. * Maturity analysis for the SOC and the log management program. * Applying a Threat Hunt mindset to the SOC. * A full use case template that was used within two major Fortune 500 companies, and is in active use by one major SIEM vendor, along with a complete example of how to build a SOC and SIEM focused use case. You can see the corresponding discussion on YouTube - search for the 2017 Security Onion conference. * Critical topics in deploying SIEM based on experience deploying five different technical platforms for nineteen different organizations in education, nonprofit, and commercial enterprises from 160 to 30,000 personnel. * Understanding why SIEM deployments fail with actionable compensators. * Real life experiences getting data into SIEM platforms and the considerations for the many different ways to provide data. * Issues relating to time, time management, and time zones. * Critical factors in log management, network security monitoring, continuous monitoring, and*

security architecture related directly to SOC and SIEM. A table of useful TCP and UDP port numbers.This is the second book in the Blue Team Handbook Series. Volume One, focused on incident response, has over 32,000 copies in print and has a 4.5/5.0 review rating!*

Incident response is critical for the active defense of any network, and incident responders need up-to-date, immediately applicable techniques with which to engage the adversary. Applied Incident Response details effective ways to respond to advanced attacks against local and remote network resources, providing proven response techniques and a framework through which to apply them. As a starting point for new incident handlers, or as a technical reference for hardened IR veterans, this book details the latest techniques for responding to threats against your network, including: Preparing your environment for effective incident response Leveraging MITRE ATT&CK and threat intelligence for active network defense Local and remote triage of systems using PowerShell, WMIC, and open-source tools Acquiring RAM and disk images locally and remotely Analyzing RAM with Volatility and Rekall Deep-dive forensic analysis of system drives using open-source or commercial tools Leveraging Security Onion and Elastic Stack for network security

monitoring Techniques for log analysis and aggregating high-value logs Static and dynamic analysis of malware with YARA rules, FLARE VM, and Cuckoo Sandbox Detecting and responding to lateral movement techniques, including pass-the-hash, pass-the-ticket, Kerberoasting, malicious use of PowerShell, and many more Effective threat hunting techniques Adversary emulation with Atomic Red Team Improving preventive and detective controls

Blue Team Planner is a must for network defenders, incident responders, and those who manage multiple breach events. Includes custom designed incident templates to help track indicators of compromise (IOC), forensic tool deployments, team member tasks, timelines, affected machines, and other vital data points essential to a successful breach event response. A freeform calendar helps users schedule effectively and contact sheets to record customer and team member points of contact. It also contains graph and bullet-note paper to allow users to add personal notes and expanded metrics tracking.A must have planner to help plan, track, and streamline your next red team engagement.Freeform scheduling calendar20 Incident Tracking TemplatesTrack tasks, tools, IOCs, timelines, and objectivesGraph paper & Bullet-note paperContacts section

Learn Ethical Hacking from Scratch
The Art of Active Defense
Practical Guide to Penetration Testing
Blue Team Planner
The Hacker Playbook 3
Cybersecurity ??? Attack and Defense Strategies
Tribal Knowledge from the Best in Defensive Cybersecurity
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. Stop manually analyzing binary! Practical Binary Analysis is the first book of its kind to present advanced binary analysis topics, such as binary instrumentation, dynamic taint analysis, and symbolic execution, in an accessible way. As malware increasingly obfuscates itself and applies anti-analysis techniques to thwart our analysis, we need more sophisticated methods that allow us to raise that dark curtain designed to keep us out--binary analysis can help. The goal of all binary analysis is to determine (and possibly modify) the true

properties of binary programs to understand what they really do, rather than what we think they should do. While reverse engineering and disassembly are critical first steps in many forms of binary analysis, there is much more to be learned. This hands-on guide teaches you how to tackle the fascinating but challenging topics of binary analysis and instrumentation and helps you become proficient in an area typically only mastered by a small group of expert hackers. It will take you from basic concepts to state-of-the-art methods as you dig into topics like code injection, disassembly, dynamic taint analysis, and binary instrumentation. Written for security engineers, hackers, and those with a basic working knowledge of C/C++ and x86-64, Practical Binary Analysis will teach you in-depth how binary programs work and help you acquire the tools and techniques needed to gain more control and insight into binary programs. Once you've completed an introduction to basic binary formats, you'll learn how to analyze binaries using techniques like the GNU/Linux binary analysis toolchain, disassembly, and code injection. You'll then go on to implement profiling tools with Pin and learn how to build your own dynamic taint analysis tools with libdft and symbolic execution tools

using Triton. You'll learn how to: - Parse ELF and PE binaries and build a binary loader with libbfd - Use data-flow analysis techniques like program tracing, slicing, and reaching definitions analysis to reason about runtime flow of your programs - Modify ELF binaries with techniques like parasitic code injection and hex editing - Build custom disassembly tools with Capstone - Use binary instrumentation to circumvent anti-analysis tricks commonly used by malware - Apply taint analysis to detect control hijacking and data leak attacks - Use symbolic execution to build automatic exploitation tools With exercises at the end of each chapter to help solidify your skills, you'll go from understanding basic assembly to performing some of the most sophisticated binary analysis and instrumentation. Practical Binary Analysis gives you what you need to work effectively with binary programs and transform your knowledge from basic understanding to expert-level proficiency.

The only security book to be chosen as a Dr. Dobbs Jolt Award Finalist since Bruce Schneier's Secrets and Lies and Applied Cryptography! Adam Shostack is responsible for security development lifecycle threat modeling at Microsoft and is one of a handful of threat

modeling experts in the world. Now, he is sharing his considerable expertise into this unique book. With pages of specific actionable advice, he details how to build better security into the design of systems, software, or services from the outset. You'll explore various threat modeling approaches, find out how to test your designs against threats, and learn effective ways to address threats that have been validated at Microsoft and other top companies. Systems security managers, you'll find tools and a framework for structured thinking about what can go wrong. Software developers, you'll appreciate the jargon-free and accessible introduction to this essential skill. Security professionals, you'll learn to discern changing threats and discover the easiest ways to adopt a structured approach to threat modeling. Provides a unique how-to for security and software developers who need to design secure products and systems and test their designs Explains how to threat model and explores various threat modeling approaches, such as asset-centric, attacker-centric and software-centric Provides effective approaches and techniques that have been proven at Microsoft and elsewhere Offers actionable how-to advice not tied to any specific software, operating system, or programming

language Authored by a Microsoft professional who is one of the most prominent threat modeling experts in the world As more software is delivered on the Internet or operates on Internet-connected devices, the design of secure software is absolutely critical. Make sure you're ready with Threat Modeling: Designing for Security.

In this book, the authors of the 20-year best-selling classic Security in Computing take a fresh, contemporary, and powerfully relevant new approach to introducing computer security. Organised around attacks and mitigations, the Pfleegers' new Analyzing Computer Security will attract students' attention by building on the high-profile security failures they may have already encountered in the popular media. Each section starts with an attack description. Next, the authors explain the vulnerabilities that have allowed this attack to occur. With this foundation in place, they systematically present today's most effective countermeasures for blocking or weakening the attack. One step at a time, students progress from attack/problem/harm to solution/protection/mitigation, building the powerful real-world problem solving skills they need to succeed as information security professionals. Analyzing Computer Security addresses crucial

contemporary computer security themes throughout, including effective security management and risk analysis; economics and quantitative study; privacy, ethics, and laws; and the use of overlapping controls. The authors also present significant new material on computer forensics, insiders, human factors, and trust.

Soc, Siem, and Threat Hunting Use Cases: A Condensed Field Guide for the Security Operations Team

Purple Team Field Manual

A Threat/vulnerability/countermeasure Approach

Cybersecurity Advice from the Best Hackers in the World

C# for Beginners with Hands-On Project

Your stepping stone to penetration testing

Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly

Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases is having an amazing impact on Security Operations worldwide. BTHb:SOCTH is the go to guiding book for new staff at a top 10 MSSP, integrated into University curriculum, and cited in top ten courses from a major information security training company. This listing is for V1.02.BTHb:SOCTH provides the security practitioner with numerous field notes on building a security operations team,

managing SIEM, and mining data sources to get the maximum amount of information out of them with a threat hunting approach. The author shares his fifteen years of experience with SIEMs and security operations is a no frills, just information format. Don Murdoch has implemented five major platforms, integrated over one hundred data sources into various platforms, and ran an MSSP practice for two years.This book covers the topics below using a "zero fluff" approach as if you hired him as a security consultant and were sitting across the table with him (or her).The book begins with a discussion for professionals to help them build a successful business case and a project plan, decide on SOC tier models, anticipate and answer tough questions you need to consider when proposing a SOC, and considerations in building a logging infrastructure. The book goes through numerous data sources that feed a SOC and SIEM and provides specific real world guidance on how to use those data sources to best possible effect. Most of the examples presented were implemented in one organization or another. These uses cases explain on what to monitor, how to use a SIEM and how to use the data coming into the platform, both questions that Don found is often answered poorly by many vendors. Several business concepts are also introduced, because they are often overlooked by IT: value chain, PESTL, and SWOT. Major sections include:An inventory of Security Operations Center (SOC) Services.Metrics, with a focus on objective measurements for the SOC, for analysts, and for SIEM's.SOC staff onboarding, training topics, and desirable skills. Along these lines, there is a chapter on a day in the life of a SOC analyst.Maturity analysis for the SOC and the log management program. Applying a Threat Hunt mindset to the SOC. A full use case template that was used within two major Fortune 500 companies, and is in active use by one major SIEM vendor, along with a complete example of how to build a SOC and SIEM

focused use case. You can see the corresponding discussion of this chapter on YouTube. Just search for the 2017 Security Onion conference for the presentation.Critical topics in deploying SIEM based on experience deploying five different technical platforms for nineteen different organizations in education, nonprofit, and commercial enterprises from 160 to 30,000 personnel.Understanding why SIEM deployments fail with actionable compensators. Real life experiences getting data into SIEM platforms and the considerations for the many different ways to provide data. Issues relating to time, time management, and time zones.
Updated, Expanded, and released to print on 10/5/14! Complete details below! Two new sections, five protocol header illustrations, improved formatting, and other corrections. The Blue Team Handbook is a zero fluff reference guide for cyber security incident responders and InfoSec pros alike. The BTHb includes essential information in a condensed handbook format about the incident response process, how attackers work, common tools, a methodology for network analysis developed over 12 years, Windows and Linux analysis processes, tcpdump usage examples, Snort IDS usage, and numerous other topics. The book is peppered with practical real life techniques from the authors extensive career working in academia and a corporate setting. Whether you are writing up your cases notes, analyzing potentially suspicious traffic, or called in to look over a misbehaving server - this book should help you handle the case and teach you some new techniques along the way. Version 2.0 updates: - *** A new section on Database incident response was added. - *** A new section on Chain of Custody was added. - *** Matt Baxter's superbly formatted protocol headers were added! - Table headers bolded. - Table format slightly revised throughout book to improve left column readability. - Several sentences updated and expanded for readability and completeness. - A

few spelling errors were corrected. - Several sites added to the Web References section. - Illustrations reformatted for better fit on the page. - An index was added. - Attribution for some content made more clear (footnotes, expanded source citing) - Content expanded a total of 20 pages

This book is the culmination of years of experience in the information technology and cybersecurity field. Components of this book have existed as rough notes, ideas, informal and formal processes developed and adopted by the authors as they led and executed red team engagements over many years. The concepts described in this book have been used to successfully plan, deliver, and perform professional red team engagements of all sizes and complexities. Some of these concepts were loosely documented and integrated into red team management processes, and much was kept as tribal knowledge. One of the first formal attempts to capture this information was the SANS SEC564 Red Team Operation and Threat Emulation course. This first effort was an attempt to document these ideas in a format usable by others. The authors have moved beyond SANS training and use this book to detail red team operations in a practical guide. The authors' goal is to provide practical guidance to aid in the management and execution of professional red teams. The term 'Red Team' is often confused in the cybersecurity space. The terms roots are based on military concepts that have slowly made their way into the commercial space. Numerous interpretations directly affect the scope and quality of today's security engagements. This confusion has created unnecessary difficulty as organizations attempt to measure threats from the results of quality security assessments. You quickly understand the complexity of red teaming by performing a quick google search for the definition, or better yet, search through the numerous interpretations and opinions posted

by security professionals on Twitter. This book was written to provide a practical solution to address this confusion. The Red Team concept requires a unique approach different from other security tests. It relies heavily on well-defined TTPs critical to the successful simulation of realistic threat and adversary techniques. Proper Red Team results are much more than just a list of flaws identified during other security tests. They provide a deeper understanding of how an organization would perform against an actual threat and determine where a security operation's strengths and weaknesses exist.Whether you support a defensive or offensive role in security, understanding how Red Teams can be used to improve defenses is extremely valuable. Organizations spend a great deal of time and money on the security of their systems. It is critical to have professionals who understand the threat and can effectively and efficiently operate their tools and techniques safely and professionally. This book will provide you with the real-world guidance needed to manage and operate a professional Red Team, conduct quality engagements, understand the role a Red Team plays in security operations. You will explore Red Team concepts in-depth, gain an understanding of the fundamentals of threat emulation, and understand tools needed you reinforce your organization's security posture.

The Operator Handbook takes three disciplines (Red Team, OSINT, Blue Team) and combines them into one complete reference guide. The book contains 123 individual cheat sheet references for many of the most frequently used tools and techniques by practitioners. Over 400 pages of content to assist the most seasoned cybersecurity veteran or someone just getting started in the career field. The goal of combining all disciplines into one book was to remove the artificial barriers that only certain knowledge exists within a "Team". The reality is today's complex digital landscape demands some level of knowledge in all areas. The

"Operator" culture should mean a well-rounded team member no matter the "Team" you represent. All cybersecurity practitioners are Operators. The Blue Team should observe and understand Red Team tactics, Red Team should continually push collaboration with the Blue Team, and OSINT should continually work to peel back evidence of evil doers scattered across disparate data sources. In the spirit of having no separation, each reference is listed in alphabetical order. Not only does this remove those team separated notions, but it also aids in faster lookup. We've all had the same experience where we knew there was an "NMAP Cheat Sheet" but did it fall under Networking, Windows, or Tools? In the Operator Handbook it begins with "N" so flip to the N's section. Also almost every topic is covered in "How to exploit X" and "How to defend X" perspectives. Tools and topics covered: Cloud (AWS, Azure, GCP), Windows, macOS, Linux, Android, iOS, DevOps (Docker, Kubernetes), OSINT, Ports, Forensics, Malware Resources, Defender tools, Attacker tools, OSINT tools, and various other supporting tools (Vim, iptables, nftables, etc...). This handbook was truly meant to be a single source for the most common tool and techniques an Operator can encounter while on the job. Search Copy Paste L33t.

Starting a Career as an Ethical Hacker

x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation

How the Original Hacking Supergroup Might Just Save the World

Kali Linux Penetration Testing Bible

Cybersecurity Blue Team Toolkit