Netcat Power Tools

Coding for Penetration Testers discusses the use of various scripting languages in penetration testing. The book presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages. It also provides a primer on scripting including, but not limited to, Web scripting, scanner scripting, and exploitation scripting. It guides the student through specific examples of custom tool development that can be incorporated into a tester's toolkit as well as real-world scenarios where such tools might be used. This book is divided into 10 chapters that explores topics such as command shell scripting; Python, Perl, and Ruby; Web scripting with PHP; manipulating Windows with PowerShell; scanner scripting; information gathering; exploitation scripting; and post-exploitation scripting. This book will appeal to penetration testers, information security practitioners, and network and system administrators. Discusses the use of various scripting languages in penetration testing Presents step-by-step instructions on how to build customized penetration testing tools using Perl, Ruby, Python, and other languages Provides a primer on scripting including, but not limited to, Web scripting, scanner scripting, and exploitation scripting

Malware analysis is big business, and attacks can cost a company dearly. When malware breaches your defenses, you need to act quickly to cure current infections and prevent future ones from occurring. For those who want to stay ahead of the latest malware, Practical Malware Analysis will teach you the tools and techniques used by professional analysts. With this book as your guide, you'll be able to safely analyze, debug, and disassemble any malicious software that comes your way. You'll learn how to: – Set up a safe virtual environment to analyze malware – Quickly extract network signatures and host-based indicators – Use key analysis tools like IDA Pro, OllyDbg, and WinDbg – Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques – Use your newfound knowledge of Windows internals for malware analysis – Develop a methodology for unpacking malware and get practical experience with five of the most popular packers – Analyze special cases of malware with shellcode, C++, and 64-bit code Hands-on labs throughout the book challenge you to practice and synthesize your skills as you dissect real malware samples, and pages of detailed dissections offer an over-the-shoulder look at how the pros do it. You'll learn how to crack open malware to see how it really works, determine what damage it has done, thoroughly clean your network, and ensure that the malware never comes back. Malware analysis is a cat-and-mouse game with rules that are constantly changing, so make sure you have the fundamentals. Whether you're tasked with securing one network or a thousand networks, or you're making a living as a malware analyst, you'll find what you need to succeed in Practical Malware Analysis.

This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.

Graphite has become one of the most powerful monitoring tools available today, due to its ease of use, rapid graph prototyping abilities, and a friendly rendering API. With this practical guide, system administrators and engineers will learn how to use this open source tool to track operational data you need to monitor your systems, as well as application-level metrics for profiling your services. Author Jason Dixon, member of the Graphite project, provides a thorough introduction of Graphite from the basics to the skills and tools you need for troubleshooting and scaling out its software components. If you want to learn more about monitoring systems, services, or applications, this is the book you need. Get an introduction to monitoring, including important concepts and terminology Examine the features and functionality of key Graphite components, including Carbon and Whisper Learn the typical user workflow necessary to create a basic line chart Build complex charts with chained functions and multiple axes that interact directly with the rendering API Understand how to use the native Graphite dashboard, as well as the more popular third-party dashboards Master the art of scaling and troubleshooting high-performance or highly available Graphite clusters

Networking and Kubernetes
Monitoring with Graphite
Malware Forensics Field Guide for Windows Systems
Infrastructure and Application Performance Monitoring
Small, Sharp Software Tools
Building Situational Awareness
Python Programming for Hackers and Pentesters

Addressing general readers as well as software practitioners, "Software and Mind" discusses the fallacies of the mechanistic ideology and the degradation of minds caused by these fallacies. Mechanism holds that every aspect of the world can be represented as a simple hierarchical structure of entities. But, while useful in fields like mathematics and manufacturing, this idea is generally worthless, because most aspects of the world are too complex to be reduced to simple hierarchical structures. Our software-related affairs, in particular, cannot be represented in this fashion. And yet, all programming theories and development systems, and all software applications, attempt to reduce real-world problems to neat hierarchical structures of data, operations, and features. Using Karl Popper's famous principles of demarcation between science and pseudoscience, the book shows that the mechanistic ideology has turned most of our software-related activities into pseudoscientific pursuits. Using mechanism as warrant, the software elites are promoting invalid, even fraudulent, software notions. They force us to depend on generic, inferior systems, instead of allowing us to develop software skills and to create our own systems. Software mechanism emulates the methods of manufacturing, and thereby restricts us to high levels of abstraction and simple, isolated structures. The benefits of software, however, can be attained only if we start with low-level elements and learn to create complex, interacting structures. Software, the book argues, is a non-mechanistic phenomenon. So it is akin to language, not to physical objects. Like language, it permits us to mirror the world in our minds and to communicate with it. Moreover, we increasingly depend on software in everything we do, in the same way that we depend on language. Thus, being restricted to mechanistic software is like thinking and communicating while being restricted to some ready-made sentences supplied by an elite. Ultimately, by impoverishing software, our elites are achieving what the totalitarian elite described by George Orwell in "Nineteen Eighty-Four" achieves by impoverishing language: they are degrading our minds.

Kubernetes has become an essential part of the daily work for most system, network, and cluster administrators today. But to work effectively together on a production-scale Kubernetes system, they must be able to speak the same language. This book provides a clear guide to the layers of complexity and abstraction that come with running a Kubernetes network. Authors James Strong and Vallery Lancey bring you up to speed on the intricacies that Kubernetes has to offer for large container deployments. If you're to be effective in troubleshooting and maintaining a production cluster, you need to be well versed in the abstraction provided at each layer. This practical book shows you how. Learn the Kubernetes networking model Choose the best interface for your clusters from the CNCF Container Network Interface project Explore the networking and Linux primitives that power Kubernetes Quickly troubleshoot networking issues and prevent downtime Examine cloud networking and Kubernetes using the three major providers: Amazon Web Services, Google Cloud, and Microsoft Azure Learn the pros and cons of various network tools--and how to select the best ones for your stack

Your one-stop guide to learning and implementing Red Team tactics effectively Key FeaturesTarget a complex enterprise environment in a Red Team activityDetect threats and respond to them with a real-world cyber-attack simulationExplore advanced penetration testing tools and techniquesBook Description Red Teaming is used to enhance security by performing simulated attacks on an organization in order to detect network and system vulnerabilities. Hands-On Red Team Tactics starts with an overview of pentesting and Red Teaming, before giving you an introduction to few of the latest pentesting tools. We will then move on to exploring Metasploit and getting to grips with Armitage. Once you have studied the fundamentals, you will learn how to use Cobalt Strike and how to set up its team server. The book introduces some common lesser known techniques for pivoting and how to pivot over SSH, before using Cobalt Strike to pivot. This comprehensive guide demonstrates advanced methods of post-exploitation using Cobalt Strike and introduces you to Command and Control (C2) servers and redirectors. All this will help you achieve persistence using beacons and data exfiltration, and will also give you the chance to run through the methodology to use Red Team activity tools such as Empire during a Red Team activity on Active Directory and Domain Controller. In addition to this, you will explore maintaining persistent access, staying untraceable, and getting reverse connections over different C2 covert channels. By the end of this book, you will have learned about advanced penetration testing tools, techniques to get reverse shells over encrypted channels, and processes for post-exploitation. What you will learnGet started with red team engagements using lesser-known methodsExplore intermediate and advanced levels of post-exploitation techniquesGet acquainted with all the tools and frameworks included in the Metasploit frameworkDiscover the art of getting stealthy access to systems via Red TeamingUnderstand the concept of redirectors to add further anonymity to your C2Get to grips with different uncommon techniques for data exfiltrationWho this book is for Hands-On Red Team Tactics is for you if you are an IT professional, pentester, security consultant, or ethical hacker interested in the IT security domain and wants to go beyond Penetration Testing. Prior knowledge of penetration testing is beneficial.

An Internet-connected Linux machine is in a high-risk situation. "Linux Firewalls, Third Edition" details security steps that any sized implementation--from home use to enterprise level--might take to protect itself from potential remote attackers. As with the first two editions, this book is especially useful for its explanations of iptables, packet filtering, and firewall optimization along with some advanced concepts including customizing the Linux kernel to enhance security.The third edition, while distribution neutral, has been updated for the current Linux Kernel and provides code examples for Red Hat, SUSE, and Debian implementations. Don't miss out on the third edition of the critically acclaimed "Linux Firewalls,"

Professional Penetration Testing
Linux Firewalls
Digital Forensics Field Guides
Penetration Testing
Using Wireshark and the Metasploit Framework
The Information Security Dictionary
The Definitive Guide

Something for Everyone If this book is to succeed and help readers, its cardinal virtue must be to provide a simple reference text. It should be an essential addition to an information security library. As such it should also serve the purpose of being a quick refresher for terms the reader has not seen since the days when one attended a computing science program, information security course or workshop. As a reference work, THE INFORMATION SECURITY DICTIONARY provides a relatively complete and easy-to-read explanation of common se- rity, malware, vulnerability and infrastructure protection terms, without causing much damage to the usually slim student pocketbook. This dictionary can help non-specialistreaders better understand the infor- tion security issues encountered in their work or studying for their certification examination or whilst doing a practical assignment as part of a workshop. This book is also essential to a reference collection for an organization’s system personnel. Special attention is paid to terms which most often prevent educated readers from understanding journal articles and books in cryptology, computing science, and information systems, in addition to applied fields that build on those disciplines, such as system design, security auditing, vulnera- lity testing, and role-based access management. The dictionary provides defi- tions that enable readers to get through a difficult article or passage. We do not, for the most part, directly explain how to conduct research or how to implement the terms briefly described.

Linux Server Security has been written for Sysadmins, DevOps engineers, developers and other technical professionals that wish to improve their hands-on knowledge of securing what is now the most popular Operating System on the planet. This detailed book walks steadily through challenging scenarios so that the reader may increase their knowledge of a number of diverse security areas which a technical professional faces. The reader is already familiar with Linux as a bedrock of stability but sometimes frustrated with certain software packages and the way that they integrate with the Operating System and indeed other packages. Looking closely at a considered selection of security topics empowers the reader to continue their learning and make full use of Linux's rocksteady foundation. In addition to each of the varied subjects covered such as sophisticated attacks, penetration testing, launching attacks and making a server invisible the book is brimming with invaluable insights gleaned from hard-won, professional experience. Applicable to almost all of the popular Linux flavours, such as Debian, Red Hat, Ubuntu, Linux Mint and CentOS, Linux Server Security can also be used to reference other Unix-type systems with little modification. The reader will improve their practical knowhow and background knowledge in order to increase their ability to troubleshoot and ultimately solve the daily security challenges encountered by Sysadmins and DevOps engineers. Whether the aim is to further a career or bring more enjoyment to a hobby the powerful, newfound knowledge gleaned from this book will help the reader add to their technical arsenal.

Over the years, thousands of tools have been developed for debugging TCP/IP networks. They range from very specialized tools that do one particular task, to generalized suites that do just about everything except replace bad Ethernet cables. Even better, many of them are absolutely free. There's only one problem: who has time to track them all down, sort through them for the best ones for a particular purpose, or figure out how to use them?Network Troubleshooting Tools does the work for you--by describing the best of the freely available tools for debugging and troubleshooting. You can start with a lesser-known version of ping that diagnoses connectivity problems, or take on a much more comprehensive program like MRTG for graphing traffic through network interfaces. There's tkined for mapping and automatically monitoring networks, and Ethereal for capturing packets and debugging low-level problems.This book isn't just about the tools available for troubleshooting common network problems. It also outlines a systematic approach to network troubleshooting: how to document your network so you know how it behaves under normal conditions, and how to think about problems when they arise, so you can solve them more effectively.The topics covered in this book include: Understanding your network Connectivity testing Evaluating the path between two network nodes Tools for capturing packets Tools for network discovery and mapping Tools for working with SNMP Performance monitoring Testing application layer protocols Software sources If you're involved with network operations, this book will save you time, money, and needless experimentation.

The command-line interface is making a comeback. That's because developers know that all the best features of your operating system are hidden behind a user interface designed to help average people use the computer. But you're not the average user, and the CLI is the most efficient way to get work done fast. Turn tedious chores into quick tasks: read and write files, manage complex directory hierarchies, perform network diagnostics, download files, work with APIs, and combine individual programs to create your own workflows. Put down that mouse, open the CLI, and take control of your software development environment. No matter what language or platform you're using, you can use the CLI to create projects, run servers, and manage files. You can even create new tools that fit right in with grep, sed, awk, and xargs. You'll work with the Bash shell and the most common command-line utilities available on macOS, Windows 10, and many flavors of Linux. Create files without opening a text editor. Manage complex directory strutures and move around your entire file system without touching the mouse. Diagnose network issues and interact with APIs. Chain several commands together to transform data, and create your own scripts to automate repetitive tasks. Make things even faster by customizing your environment, creating shortcuts, and integrating other tools into your environment. Hands-on activities and exercises will cement your newfound knowledge and give you the confidence to use the CLI to its fullest potential. And if you're worried you'll wreck your system, this book walks you through creating an Ubuntu virtual machine so you can practice worry-free. Dive into the CLI and join the thousands of other devs who use it every day. What You Need: You'll need macOS, Windows 10, or a Linux distribution like Ubuntu, Fedora, CentOS, or Debian using the Bash shell.

Recovering Evidence, Personal Data, and Corporate Assets
Securing Data in Motion
Hacking and Penetration Testing Ultimate CD
Hacking- The art Of Exploitation
Eh
Security Testing, Penetration Testing, and Ethical Hacking
Learning Kali Linux

Summary Linux in Action is a task-based tutorial that will give you the skills and deep understanding you need to administer a Linux-based system. This hands-on book guides you through 12 real-world projects so you can practice as you learn. Each chapter ends with a review of best practices, new terms, and exercises. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the Technology You can't learn anything without getting your hands dirtyÃ¢â‚¬â€ including Linux. Skills like securing files, folders, and servers, safely installing patches and applications, and managing a network are required for any serious user, including developers, administrators, and DevOps professionals. With this hands-on tutorial, you'll roll up your sleeves and learn Linux project by project. About the Book Linux in Action guides you through 12 real-world projects, including automating a backup-and-restore system, setting up a private Dropbox-style file cloud, and building your own MediaWiki server. You'll try out interesting examples as you lock in core practices like virtualization, disaster recovery, security, backup, DevOps, and system troubleshooting. Each chapter ends with a review of best practices, new terms, and exercises. What's inside Setting up a safe Linux environment Managing secure remote connectivity Building a system recovery device Patching and upgrading your system About the Reader No prior Linux admin experience is required. About the Author David Clinton is a certified Linux Server Professional, seasoned instructor, and author of Manning's bestselling Learn Amazon Web Services in a Month of Lunches. Table of Contents Welcome to Linux Linux virtualization: Building a Linux working environment Remote connectivity: Safely accessing networked machines Archive management: Backing up or copying entire file systems Automated administration: Configuring automated offsite backups Emergency tools: Building a system recovery device Web servers: Building a MediaWiki server Networked file sharing: Building a Nextcloud file-sharing server Securing your web server Securing network connections: Creating a VPN or DMZ System monitoring: Working with log files Sharing data over a private network Troubleshooting system performance issues Troubleshooting network issues Troubleshooting peripheral devices DevOps tools: Deploying a scripted server environment using Ansible

With more than 600 security tools in its arsenal, the Kali Linux distribution can be overwhelming. Experienced and aspiring security professionals alike may find it challenging to select the most appropriate tool for conducting a given test. This practical book covers Kali’s expansive security capabilities and helps you identify the tools you need to conduct a wide range of security tests and penetration tests. You’ll also explore the vulnerabilities that make those tests necessary. Author Ric Messier takes you through the foundations of Kali Linux and explains methods for conducting tests on networks, web applications, wireless security, password vulnerability, and more. You’ll discover different techniques for extending Kali tools and creating your own toolset. Learn tools for stress testing network stacks and applications Perform network reconnaissance to determine what’s available to attackers Execute penetration tests using automated exploit tools such as Metasploit Use cracking tools to see if passwords meet complexity requirements Test wireless capabilities by injecting frames and cracking passwords Assess web application vulnerabilities with automated or proxy-based tools Create advanced attack techniques by extending Kali tools or developing your own Use Kali Linux to generate reports once testing is complete

When it comes to creating powerful and effective hacking tools, Python is the language of choice for most security analysts. But just how does the magic happen? In Black Hat Python, the latest from Justin Seitz (author of the best-selling Gray Hat Python), you’ll explore the darker side of Python’s capabilities—writing network sniffers, manipulating packets, infecting virtual machines, creating stealthy trojans, and more. You’ll learn how to: –Create a trojan command-and-control using GitHub –Detect sandboxing and automate common malware tasks, like keylogging and screenshotting –Escalate Windows privileges with creative process control –Use offensive memory forensics tricks to retrieve password hashes and inject shellcode into a virtual machine –Extend the popular Burp Suite web-hacking tool –Abuse Windows COM automation to perform a man-in-the-browser attack –Exfiltrate data from a network most sneakily Insider techniques and creative challenges throughout show you how to extend the hacks and how to write your own exploits. When it comes to offensive security, your ability to create powerful tools on the fly is indispensable. Learn how in Black Hat Python. Uses Python 2

Internet Infrastructure: Networking, Web Services, and Cloud Computing provides a comprehensive introduction to networks and the Internet from several perspectives: the underlying media, the protocols, the hardware, the servers, and their uses. The material in the text is divided into concept chapters that are followed up with case study chapters that examine how to install, configure, and secure a server that offers the given service discussed. The book covers in detail the Bind DNS name server, the Apache web server, and the Squid proxy server. It also provides background on those servers by discussing DNS, DHCP, HTTP, HTTPS, digital certificates and encryption, web caches, and the variety of protocols that support web caching. Introductory networking content, as well as advanced Internet content, is also included in chapters on networks, LANs and WANs, TCP/IP, TCP/IP tools, cloud computing, and an examination of the Amazon Cloud Service. Online resources include supplementary content that is available via the textbook’s companion website, as well useful resources for faculty and students alike, including: a complete lab manual; power point notes, for installing, configuring, securing and experimenting with many of the servers discussed in the text; power point notes; animation tutorials to illustrate some of the concepts; two appendices; and complete input/output listings for the example Amazon cloud operations covered in the book.

Coding for Penetration Testers
Techniques, Tactics and Tools for Security Practitioners
Secure web applications using Burp Suite, Nmap, Metasploit, and more
Linux Server Security
Linux in Action
Practical Malware Analysis

Professional Penetration Testing walks you through the entire process of setting up and running a pen test lab. Penetration testing—the act of testing a computer network to find security vulnerabilities before they are maliciously exploited—is a crucial component of information security in any organization. With this book, you will find out how to turn hacking skills into a professional career. Chapters cover planning, metrics, and methodologies; the details of running a pen test, including identifying and verifying vulnerabilities; and archiving, reporting and management practices. Author Thomas Wilhelm has delivered penetration testing training to countless security professionals, and now through the pages of this book you can benefit from his years of experience as a professional penetration tester and educator. After reading this book, you will be able to create a personal penetration test lab that can deal with real-world vulnerability scenarios. All disc-based content for this title is now available on the Web. Find out how to turn hacking and pen testing skills into a professional career Understand how to conduct controlled attacks on a network through real-world examples of vulnerable and exploitable servers Master project management skills necessary for running a formal penetration test and setting up a professional ethical hacking business Discover metrics and reporting methodologies that provide experience crucial to a professional penetration tester

The science of gathering and extracting information from data-intensive applications bring in the challenge of writing complex libraries and efficient programs using high level languages like Python, R, so on. This book aims to explore the power of "Unix-styled" scripting tools like awk, bash, grep and package them as highly efficient built-in ...

Hacking and Penetration Testing Ultimate CD contains six of our best-selling titles. This collection of ebooks provides the IT security professional with easy access to loads of information on a single CD. It contains over 2300 pages of techniques and tools. This features: *Long: "Google Hacking: Volume One," 9781931836364 *Jackson, et al.: "Asterisk Hacking," 9781597491518 *Haines, et al.: "Kismet Hacking," 9781597491174 *Kanclirz: "NetCat Power Tools," 9781597492577 *Beale, et al.: "Pentester's Open Source Toolkit," 9781597490214 *Orebaugh and Pinkard: "Nmap in the Enterprise," 9781597492416"

Nessus, Snort, and Ethereal Power Tools covers customizing Snort to perform intrusion detection and prevention; Nessus to analyze the network layer for vulnerabilities; and Ethereal to sniff their network for malicious or unusual traffic. The book contains an appendix detailing the best of the rest open source security tools. Each of these tools is intentionally designed to be highly customizable so that users can torque the programs to suit their particular needs. Users can code their own custom rules, plug-ins, and filters that are tailor-made to fit their own networks and the threats which they most commonly face. The book describes the most important concepts of coding and customizing tools, and then provides readers with invaluable working scripts that can either be used as is or further refined by using knowledge gained from the book. Snort, Nessus, and Ethereal are the three most popular open source security tools in the world Only book that teaches readers how to customize these tools for their specific needs by coding rules, plugins, and filters Companion Web site provides all working code and scripts from the book for download

A Hands-On Introduction to Hacking
Security Power Tools
Next Generation SSH2 Implementation
Prometheus: Up & Running
Hands-On Data Science with the Command Line

Kali Linux Penetration Testing Bible
Advanced Bash Scripting Guide

Master Wireshark to solve real-world security problems If you don’t already use Wireshark for a wide range of information security tasks, you will after this book. Mature and powerful, Wireshark is commonly used to find root cause of challenging network issues. This book extends that power to information security professionals, complete with a downloadable, virtual lab environment. Wireshark for Security Professionals covers both offensive and defensive concepts that can be applied to essentially any InfoSec role. Whether into network security, malware analysis, intrusion detection, or penetration testing, this book demonstrates Wireshark through relevant and useful examples. Master Wireshark through both lab scenarios and exercises. Early in the book, a virtual lab environment is provided for the purpose of getting hands-on experience with Wireshark. Wireshark is combined with two popular platforms: Kali, the security-focused Linux distribution, and the Metasploit Framework, the open-source framework for security testing. Lab-based virtual systems generate network traffic for analysis, investigation and demonstration. In addition to following along with the labs you will be challenged with end-of-chapter exercises to expand on covered material. Lastly, this book explores Wireshark with Lua, the light-weight programming language. Lua allows you to extend and customize Wireshark’s features for your needs as a security professional. Lua source code is available both in the book and online. Lua code and lab source code are available online through GitHub, which the book also introduces. The book’s final two chapters greatly draw on Lua and TShark, the command-line interface of Wireshark. By the end of the book you will gain the following: Master the basics of Wireshark Explore the virtual w4sp-lab environment that mimics a real-world network Gain experience using the Debian-based Kali OS among other systems Understand the technical details behind network attacks Execute exploitation and grasp offensive and defensive activities, exploring them through Wireshark Employ Lua to extend Wireshark features and create useful scripts To sum up, the book content, labs and online material, coupled with many referenced sources of PCAP traces, together present a dynamic and robust manual for information security professionals seeking to leverage Wireshark.

This is the only book to clearly demonstrate how to get big dollar security for your network using freely available tools. This is a must have book for any company or person with a limited budget. Network security is in a constant struggle for budget to get things done. Upper management wants thing to be secure but doesn’t want to pay for it. With this book as a guide, everyone can get what they want. The examples and information will be of immense value to every small business. It will explain security principles and then demonstrate how to achieve them using only freely available software. Teachers you how to implement best of breed security using tools for free Ideal for anyone recomending and implementing new technologies within the company

The first comprehensive guide to discovering and preventingattacks on the Android OS As the Android operating system continues to increase its shareof the smartphone market, smartphone hacking remains a growingthreat. Written by experts who rank among the world's foremostAndroid security researchers, this book presents vulnerabilitydiscovery, analysis, and exploitation tools for the good guys.Following a detailed explanation of how the Android OS works andits overall security architecture, the authors examine howvulnerabilities can be discovered and exploits developed forvarious system components, preparing you to defend againstthem. If you are a mobile device administrator, security researcher,Android app developer, or consultant responsible for evaluatingAndroid security, you will find this guide is essential to yourtoolbox. A crack team of leading Android security researchers explainAndroid security risks, security design and architecture, rooting,fuzz testing, and vulnerability analysis Covers Android application building blocks and security as wellas debugging and auditing Android apps Prepares mobile device administrators, security researchers,Android app developers, and security consultants to defend Androidsystems against attack Android Hacker's Handbook is the first comprehensiveresource for IT professionals charged with smartphonesecurity.

Netcat Power ToolsElsevier
Netcat Power Tools
IPhone Forensics
Instant Netcat Starter
Defining the Terms that Define Security for E-Business, Internet, Information and Wireless Technology
Harness the Combinatoric Power of Command-Line Tools and Utilities
The Hands-On Guide to Dissecting Malicious Software
Hack and Defend

Learn how to execute web application penetration testing end-to-end Key Features Build an end-to-end threat model landscape for web application security Learn both web application vulnerabilities and web intrusion testing Associate network vulnerabilities with a web application infrastructure Book Description Companies all over the world want to hire professionals dedicated to application security. Practical Web Penetration Testing focuses on this very trend, teaching you how to conduct application security testing using real-life scenarios. To start with, you’ll set up an environment to perform web application penetration testing. You will then explore different penetration testing concepts such as threat modeling, intrusion test, infrastructure security threat, and more, in combination with advanced concepts such as Python scripting for automation. Once you are done learning the basics, you will discover end-to-end implementation of tools such as Metasploit, Burp Suite, and Kali Linux. Many companies deliver projects into production by using either Agile or Waterfall methodology. This book shows you how to assist any company with their SDLC approach and helps you on your journey to becoming an application security specialist. By the end of this book, you will have hands-on knowledge of using different tools for penetration testing. What you will learn Learn how to use Burp Suite effectively Use Nmap, Metasploit, and more tools for network infrastructure tests Practice using all web application hacking tools for intrusion tests using Kali Linux Learn how to analyze a web application using application threat modeling Know how to conduct web intrusion tests Understand how to execute network infrastructure tests Master automation of penetration testing functions for maximum efficiency using Python Who this book is for Practical Web Penetration Testing is for you if you are a security professional, penetration tester, or stakeholder who wants to execute penetration testing using the latest and most popular tools. Basic knowledge of ethical hacking would be an added advantage.

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In Penetration Testing, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you’ll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you’ll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to: –Crack passwords and wireless network keys with brute-forcing and wordlists –Test web applications for vulnerabilities –Use the Metasploit Framework to launch exploits and write your own Metasploit modules –Automate social-engineering attacks –Bypass antivirus software –Turn access to one machine into total control of the enterprise in the post exploitation phase You’ll even explore writing your own exploits. Then it’s on to mobile hacking—Weidman’s particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, Penetration Testing is the introduction that every aspiring hacker needs.

Are you serious about network security? Then check out SSH, the Secure Shell, which provides key-based authentication and transparent encryption for your network connections. It's reliable, robust, and reasonably easy to use, and both free and commercial implementations are widely available for most operating systems. While it doesn't solve every privacy and security problem, SSH eliminates several of them very effectively. Everything you want to know about SSH is in our second edition of SSH, The Secure Shell: The Definitive Guide. This updated book thoroughly covers the latest SSH-2 protocol for system administrators and end users interested in using this increasingly popular TCP/IP-based solution. How does it work? Whenever data is sent to the network, SSH automatically encrypts it. When data reaches its intended recipient, SSH decrypts it. The result is "transparent" encryption-users can work normally, unaware that their communications are already encrypted. SSH supports secure file transfer between computers, secure remote logins, and a unique "tunneling" capability that adds encryption to otherwise insecure network applications. With SSH, users can freely navigate the Internet, and system administrators can secure their networks or perform remote administration. Written for a wide, technical audience, SSH, The Secure Shell: The Definitive Guide covers several implementations of SSH for different operating systems and computing environments. Whether you're an individual running Linux machines at home, a corporate network administrator with thousands of users, or a PC/Mac owner who just wants a secure way to telnet or transfer files between machines, our indispensable guide has you covered. It starts with simple installation and use of SSH, and works its way to in-depth case studies on large, sensitive computer networks. No matter where or how you're shipping information, SSH, The Secure Shell: The Definitive Guide will show you how to do it securely.

Cyber Warfare, Second Edition, takes a comprehensive look at how and why digital warfare is waged. The book explores the participants, battlefields, and the tools and techniques used in today's digital conflicts. The concepts discussed gives students of information security a better idea of how cyber conflicts are carried out now, how they will change in the future, and how to detect and defend against espionage, hacktivism, insider threats and non-state actors such as organized criminals and terrorists. This book provides concrete examples and real-world guidance on how to identify and defend a network against malicious attacks. It probes relevant technical and factual information from an insider's point of view, as well as the ethics, laws and consequences of cyber war and how computer criminal law may change as a result. Logical, physical, and psychological weapons used in cyber warfare are discussed. This text will appeal to information security practitioners, network security administrators, computer system administrators, and security analysts. Provides concrete examples and real-world guidance on how to identify and defend your network against malicious attacks Dives deeply into relevant technical and factual information from an insider's point of view Details the ethics, laws and consequences of cyber war and how computer criminal law may change as a result

Nessus, Snort, and Ethereal Power Tools
Practical Web Penetration Testing
Open Source Network Administration
Automate everyday data science tasks using command-line tools
Customizing Open Source Security Applications
The Mechanistic Myth and Its Consequences
Black Hat Python

"This book is a must for anyone attempting to examine the iPhone. The level of forensic detail is excellent. If only all guides to forensics were written with this clarity!"-Andrew Sheldon, Director of Evidence Talks, computer forensics experts With iPhone use increasing in business networks, IT and security professionals face a serious challenge: these devices store an enormous amount of information. If your staff conducts business with an iPhone, you need to know how to recover, analyze, and securely destroy sensitive data. iPhone Forensics supplies the knowledge necessary to conduct complete and highly specialized forensic analysis of the iPhone, iPhone 3G, and iPod Touch. This book helps you: Determine what type of data is stored on the device Break v1.x and v2.x passcode-protected iPhones to gain access to the device Build a custom recovery toolkit for the iPhone Interrupt iPhone 3G's "secure wipe" process Conduct data recovery of a v1.x and v2.x iPhone user disk partition, and preserve and recover the entire raw user disk partition Recover deleted voicemail, images, email, and other personal data, using data carving techniques Recover geotagged metadata from camera photos Discover Google map lookups, typing cache, and other data stored on the live file system Extract contact information from the iPhone's database Use different recovery strategies based on case needs And more. iPhone Forensics includes techniques used by more than 200 law enforcement agencies worldwide, and is a must-have for any corporate compliance and disaster recovery plan.

Get up to speed with Prometheus, the metrics-based monitoring system used by tens of thousands of organizations in production. This practical guide provides application developers, sysadmins, and DevOps practitioners with a hands-on introduction to the most important aspects of Prometheus, including dashboarding and alerting, direct code instrumentation, and metric collection from third-party systems with exporters. This open source system has gained popularity over the past few years for good reason. With its simple yet powerful data model and query language, Prometheus does one thing, and it does it well. Author and Prometheus developer Brian Brazil guides you through Prometheus setup, the Node exporter, and the Alertmanager, then demonstrates how to use them for application and infrastructure monitoring. Know where and how much to apply instrumentation to your application code Identify metrics with labels using unique key-value pairs Get an introduction to Grafana, a popular tool for building dashboards Learn how to use the Node Exporter to monitor your infrastructure Use service discovery to provide different views of your machines and services Use Prometheus with Kubernetes and examine exporters you can use with containers Convert data from other monitoring systems into the Prometheus format

Provides information on the X Window System, covering such topics as X.org configuration, the X Server, utility programs, remote access, VNC, and keyboard configuration.

New security risks, continuously evolving regulation and increasing security standards have created new and growing needs for secure internal information transfers, which SSH provides. This book addresses these new trends in depth, offering the most up-to-date information on the integration of SSH into a security environment. It covers the newest features and applications of SSH-2 (which received Proposed Standard status from the IETF in 2006). SSH2 is more secure than previous versions and has many expanded uses on a wider variety of computing platforms. Another particular note driving new SSH2 adoption are the requirements of recent legislation (PCI/HIPAA/SOX/FISMA). SSH 2 has become an even more valuable tool, as it provides communications security compliance with the latest standards. This book offers the most up-to-date information on SSH2 in a practical, hands-on, tutorial-style reference that goes well beyond UNIX implementation. It concentrates on the latest version of SSH 2 with all new information. * Discover why SSH2 offers more robust security than SSH1 and how to incorporate it into your network administration software toolbox.

Secure Your Network for Free
Network Security Through Data Analysis
Wireshark for Security Professionals
The Basics of Hacking and Penetration Testing
Creating and Learning in a Hacking Lab
Internet Infrastructure
Cyber Warfare

This book describes open source tools commonly used in network administration. Open source tools are a popular choice for network administration because they are a good fit for many organizations. This volume brings together a collection of these tools in a single reference for the networkadministrator.

Originally released in 1996, Netcat is a netowrking program designed to read and write data across both Transmission Control Protocol TCP and User Datagram Protocol (UDP) connections using the TCP/Internet Protocol (IP) protocol suite. Netcat is often referred to as a "Swiss Army knife" utility, and for good reason. Just like the multi-function usefullness of the venerable Swiss Army pocket knife, Netcat's functionality is helpful as both a standalone program and a backe-end tool in a wide range of applications. Some of the many uses of Netcat include port scanning, transferring files, grabbing banners, port listening and redirection, and more nefariously, a backdoor. This is the only book dedicated to comprehensive coverage of the tool's many features, and by the end of this book, you'll discover how Netcat can be one of the most valuable tools in your arsenal. * Get Up and Running with Netcat Simple yet powerful...Don't let the trouble-free installation and the easy command line belie the fact that Netcat is indeed a potent and powerful program. * Go PenTesting with Netcat Master Netcat's port scanning and service identification capabilities as well as obtaining Web server application information. Test and verify outbound firewall rules and avoid detection by using antivirus software and the Window Firewall. Also, create a backdoor using Netcat. * Conduct Enumeration and Scanning with Netcat, Nmap, and More! Netcat's not the only game in town...Learn the process of network of enumeration and scanning, and see how Netcat along with other tools such as Nmap and Scanrand can be used to thoroughly identify all of the assets on your network. * Banner Grabbing with Netcat Banner grabbing is a simple yet highly effective method of gathering information about a remote target, and can be performed with relative ease with the Netcat utility. * Explore the Dark Side of Netcat See the various ways Netcat has been used to provide malicious, unauthorized access to their targets. By walking through these methods used to set up backdoor access and circumvent protection mechanisms through the use of Netcat, we can understand how malicious hackers obtain and maintain illegal access. Embrace the dark side of Netcat, so that you may do good deeds later. * Transfer Files Using Netcat The flexability and simple operation allows Netcat to fill a niche when it comes to moving a file or files in a quick and easy fashion. Encryption is provided via several different avenues including integrated support on some of the more modern Netcat variants, tunneling via third-party tools, or operating system integrated IPsec policies. * Troubleshoot Your Network with Netcat Examine remote systems using Netat's scanning ability. Test open ports to see if they really are active and see what protocls are on those ports. Communicate with different applications to determine what problems might exist, and gain insight into how to solve these problems. * Sniff Traffic within a System Use Netcat as a sniffer within a system to collect incoming and outgoing data. Set up Netcat to listen at ports higher than 1023 (the well-known ports), so you can use Netcat even as a normal user. * Comprehensive introduction to the #4 most popular open source security tool available * Tips and tricks on the legitimate uses of Netcat * Detailed information on its nefarious purposes * Demystifies security issues surrounding Netcat * Case studies featuring dozens of ways to use Netcat in daily tasks

Dissecting the dark side of the Internet with its infectious worms, botnets, rootkits, and Trojan horse programs (known as malware) is a treaterous condition for any forensic investigator or analyst. Written by information security experts with real-world investigative experience, Malware Forensics Field Guide for Windows Systems is a "tool" with checklists for specific tasks, case studies of difficult situations, and expert analyst tips. *A condensed hand-held guide complete with on-the-job tasks and checklists *Specific for Windows-based systems, the largest running OS in the world *Authors are world-renowned leaders in investigating and analyzing malicious code

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

Ethical Hacking and Penetration Testing Made Easy
Android Hacker's Handbook
SSH, The Secure Shell
Software and Mind
A practical guide to mastering Red Team operations
Hands-On Red Team Tactics
Tracking Dynamic Host and Application Metrics at Scale

What if you could sit down with some of the most talented security engineers in the world and ask any network security question you wanted? Security Power Tools lets you do exactly that! Members of Juniper Networks' Security Engineering team and a few guest experts reveal how to use, tweak, and push the most popular network security applications, utilities, and tools available using Windows, Linux, Mac OS X, and Unix platforms. Designed to be browsed, Security Power Tools offers you multiple approaches to network security via 23 cross-referenced chapters that review the best security tools on the planet for both black hat techniques and white hat defense tactics. It's a must-have reference for network administrators, engineers and consultants with tips, tricks, and how-to advice for an assortment of freeware and commercial tools, ranging from intermediate level command-line operations to advanced programming of self-hiding exploits. Security Power Tools details best practices for: Reconnaissance -- including tools for network scanning such as nmap; vulnerability scanning tools for Windows and Linux; LAN reconnaissance; tools to help with wireless reconnaissance; and custom packet generation Penetration -- such as the Metasploit framework for automated penetration of remote computers; tools to find wireless networks; exploitation framework applications; and tricks and tools to manipulate shellcodes Control -- including the configuration of several tools for use as backdoors; and a review of known rootkits for Windows and Linux Defense -- including host-based firewalls; host hardening for Windows and Linux networks; communication security with ssh; email security and anti-malware; and device security testing Monitoring -- such as tools to capture, and analyze packets; network monitoring with Honeyd and snort; and host monitoring of production servers for file changes Discovery -- including The Forensic Toolkit, SysInternals and other popular forensic tools; application fuzzer and fuzzing techniques; and the art of binary reverse engineering using tools like Interactive Disassembler and Ollydbg A practical and timely network security ethics chapter written by a Stanford University professor of law completes the suite of topics and makes this book a goldmine of security information. Save yourself a ton of headaches and be prepared for any network security dilemma with Security Power Tools.

Traditional intrusion detection and logfile analysis are no longer enough to protect today’s complex networks. In this practical guide, security researcher Michael Collins shows you several techniques and tools for collecting and analyzing network traffic datasets. You’ll understand how your network is used, and what actions are necessary to protect and improve it. Divided into three sections, this book examines the process of collecting and organizing data, various tools for analysis, and several different analytic scenarios and techniques. It’s ideal for network administrators and operational security analysts familiar with scripting. Explore network, host, and service sensors for capturing security data Store data traffic with relational databases, graph databases, Redis, and Hadoop Use SiLK, the R language, and other tools for analysis and visualization Detect unusual phenomena through Exploratory Data Analysis (EDA) Identify significant structures in networks with graph analysis Determine the traffic that's crossing service ports in a network Examine traffic volume and behavior to spot DDoS and database raids Get a step-by-step process for network mapping and inventory

Learn to harness the power and versatility of Netcat and understand why it remains an integral part of IT and security toolkits to this day Learn something new in an Instant! A short, fast, focused guide delivering immediate results. Downloading, compiling, and installing Netcat on Windows and

Linux platforms Establish a raw network connection so you can understand how Netcat processes information using a simplistic chat interface Establish and maintain a remote shell / back door on various operating systems In Detail As a featured networking utility, Netcat uses TCP/IP protocols to read and write data across network connections. Netcat is a feature rich backend network debugging and exploration tool with the ability to create almost any type of connection you would need. "Netcat Starter Guide" is a practical, hands-on guide that provides you with a simple and straightforward roadmap to proceed from newbie to seasoned professional with the Netcat utility. By progressing from simple to more complex uses, this book will inform and explain many of the primary use cases that are only limited by your imagination. This book explores the classic Netcat utility, and breaks down the common ways in which it can be utilized in the field. Beginning with compilation and installation, this book quickly has you utilizing the core features of the utility to perform file transfers regardless of commonly blocked firewall ports, perform real-world interrogation of services and listening ports to discover the true intention of an application or service, and tunnelling remotely into systems to produce remote command shells.

The Basics of Hacking and Penetration Testing, Second Edition, serves as an introduction to the steps required to complete a penetration test or perform an ethical hack from beginning to end. The book teaches students how to properly utilize and interpret the results of the modern-day hacking tools required to complete a penetration test. It provides a simple and clean explanation of how to effectively utilize these tools, along with a four-step methodology for conducting a penetration test or hack, thus equipping students with the know-how required to jump start their careers and gain a better understanding of offensive security. Each chapter contains hands-on examples and exercises that are designed to teach learners how to interpret results and utilize those results in later phases. Tool coverage includes: Backtrack Linux, Google reconnaissance, MetaGooFil, dig, Nmap, Nessus, Metasploit, Fast Track Autopwn, Netcat, and Hacker Defender rootkit. This is complemented by PowerPoint slides for use in class. This book is an ideal resource for security consultants, beginning InfoSec professionals, and students. Each chapter contains hands-on examples and exercises that are designed to teach you how to interpret the results and utilize those results in later phases. Written by an author who works in the field as a Penetration Tester and who teaches Offensive Security, Penetration Testing, and Ethical Hacking, and Exploitation classes at Dakota State University. Utilizes the Kali Linux distribution and focuses on the seminal tools required to complete a penetration test.

Help for Network Administrators

X Power Tools

Building Better Tools

Network Troubleshooting Tools

Networking, Web Services, and Cloud Computing