
Linux Security Cookbook Pdf

Recognizing the mannerism ways to get this ebook **Linux Security Cookbook Pdf** is additionally useful. You have remained in right site to start getting this info. acquire the Linux Security Cookbook Pdf member that we manage to pay for here and check out the link.

You could purchase guide Linux Security Cookbook Pdf or acquire it as soon as feasible. You could quickly download this Linux Security Cookbook Pdf after getting deal. So, bearing in mind you require the ebook swiftly, you can straight acquire it. Its therefore extremely simple and as a result fats, isnt it? You have to favor to in this aerate

Linux Security Cookbook Pdf

Downloaded from ssm.nwherald.com by guest

BRADFORD HORTON

Kali Linux Cookbook "O'Reilly Media, Inc." Secure your Linux machines and keep them secured with the help of exciting recipes About This Book This book provides code-intensive discussions with detailed recipes that help you understand better and learn faster. More than 50 hands-on recipes to create and administer a secure Linux system locally as well as on a network Enhance file system security and local and remote user authentication by using various security tools and different versions of Linux for different tasks Who This Book Is For Practical Linux

Security Cookbook is intended for all those Linux users who already have knowledge of Linux File systems and administration. You should be familiar with basic Linux commands. Understanding Information security and its risks to a Linux system is also helpful in understanding the recipes more easily. However, even if you are unfamiliar with Information security, you will be able to easily follow and understand the recipes discussed. Since Linux Security Cookbook follows a practical approach, following the steps is very easy. What You Will Learn Learn about various vulnerabilities and exploits in relation to Linux systems Configure and build a secure kernel and test it Learn about file permissions and security and how to securely modify files Explore

various ways to authenticate local users while monitoring their activities. Authenticate users remotely and securely copy files on remote systems Review various network security methods including firewalls using iptables and TCP Wrapper Explore various security tools including Port Sentry, Squid Proxy, Shorewall, and many more Understand Bash vulnerability/security and patch management In Detail With the growing popularity of Linux, more and more administrators have started moving to the system to create networks or servers for any task. This also makes Linux the first choice for any attacker now. Due to the lack of information about security-related attacks, administrators now face issues in dealing with these attackers as quickly as

possible. Learning about the different types of Linux security will help create a more secure Linux system. Whether you are new to Linux administration or experienced, this book will provide you with the skills to make systems more secure. With lots of step-by-step recipes, the book starts by introducing you to various threats to Linux systems. You then get to walk through customizing the Linux kernel and securing local files. Next you will move on to manage user authentication locally and remotely and also mitigate network attacks. Finally, you will learn to patch bash vulnerability and monitor system logs for security. With several screenshots in each example, the book will supply a great learning experience and help you create more secure Linux systems. Style and approach An easy-to-follow cookbook with step-by-step practical recipes covering the various Linux security administration tasks. Each recipe has screenshots, wherever needed, to make understanding more easy. [Linux Security Cookbook](#) No Starch Press O'Reilly's Pocket Guides have earned a reputation as inexpensive, comprehensive, and compact guides that have the stuff

but not the fluff. Every page of Linux Pocket Guide lives up to this billing. It clearly explains how to get up to speed quickly on day-to-day Linux use. Once you're up and running, Linux Pocket Guide provides an easy-to-use reference that you can keep by your keyboard for those times when you want a fast, useful answer, not hours in the man pages. Linux Pocket Guide is organized the way you use Linux: by function, not just alphabetically. It's not the 'bible of Linux; it's a practical and concise guide to the options and commands you need most. It starts with general concepts like files and directories, the shell, and X windows, and then presents detailed overviews of the most essential commands, with clear examples. You'll learn each command's purpose, usage, options, location on disk, and even the RPM package that installed it. The Linux Pocket Guide is tailored to Fedora Linux--the latest spin-off of Red Hat Linux--but most of the information applies to any Linux system. Throw in a host of valuable power user tips and a friendly and accessible style, and you'll quickly find this practical, to-the-point book a small but mighty resource for Linux users.

Kali Linux Cookbook - Second Edition Packt Publishing Ltd

Discover network vulnerabilities and threats to design effective network security strategies Key Features Plunge into scanning techniques using the most popular tools Effective vulnerability assessment techniques to safeguard network infrastructure Explore the Nmap Scripting Engine (NSE) and the features used for port and vulnerability scanning Book Description Network scanning is a discipline of network security that identifies active hosts on networks and determining whether there are any vulnerabilities that could be exploited. Nessus and Nmap are among the top tools that enable you to scan your network for vulnerabilities and open ports, which can be used as back doors into a network. Network Scanning Cookbook contains recipes for configuring these tools in your infrastructure that get you started with scanning ports, services, and devices in your network. As you progress through the chapters, you will learn how to carry out various key scanning tasks, such as firewall detection, OS detection, and access management, and will look at

problems related to vulnerability scanning and exploitation in the network. The book also contains recipes for assessing remote services and the security risks that they bring to a network infrastructure. By the end of the book, you will be familiar with industry-grade tools for network scanning, and techniques for vulnerability scanning and network protection. What you will learn

Install and configure Nmap and Nessus in your network infrastructure

Perform host discovery to identify network devices

Explore best practices for vulnerability scanning and risk assessment

Understand network enumeration with Nessus and Nmap

Carry out configuration audit using Nessus for various platforms

Write custom Nessus and Nmap scripts on your own

Who this book is for

If you're a network engineer or information security professional wanting to protect your networks and perform advanced scanning and remediation for your network infrastructure, this book is for you.

Mobile Device Exploitation Cookbook

Createspace Independent Publishing Platform

This soup-to-nuts collection of recipes

covers everything you need to know to perform your job as a Linux network administrator, whether you're new to the job or have years of experience. With Linux Networking Cookbook, you'll dive straight into the gnarly hands-on work of building and maintaining a computer network. Running a network doesn't mean you have all the answers. Networking is a complex subject with reams of reference material that's difficult to keep straight, much less remember. If you want a book that lays out the steps for specific tasks, that clearly explains the commands and configurations, and does not tax your patience with endless ramblings and meanderings into theory and obscure RFCs, this is the book for you. You will find recipes for:

- Building a gateway, firewall, and wireless access point on a Linux network
- Building a VoIP server with Asterisk
- Secure remote administration with SSH
- Building secure VPNs with OpenVPN, and a Linux PPTP VPN server
- Single sign-on with Samba for mixed Linux/Windows LANs
- Centralized network directory with OpenLDAP
- Network monitoring with Nagios or MRTG
- Getting acquainted with IPv6
- Setting up hands-free

networks installations of new systems

Linux system administration via serial console

And a lot more. Each recipe includes a clear, hands-on solution with tested code, plus a discussion on why it works. When you need to solve a network problem without delay, and don't have the time or patience to comb through reference books or the Web for answers, Linux Networking Cookbook gives you exactly what you need.

Kali Linux Web Penetration Testing Cookbook

"O'Reilly Media, Inc."

Get hands-on experience in using Burp Suite to execute attacks and perform web assessments

Key Features

- Explore the tools in Burp Suite to meet your web infrastructure security demands
- Configure Burp to fine-tune the suite of tools specific to the target
- Use Burp extensions to assist with different technologies commonly found in application stacks

Book Description

Burp Suite is a Java-based platform for testing the security of your web applications, and has been adopted widely by professional enterprise testers. The Burp Suite Cookbook contains recipes to tackle challenges in determining and exploring vulnerabilities in web

applications. You will learn how to uncover security flaws with various test cases for complex environments. After you have configured Burp for your environment, you will use Burp tools such as Spider, Scanner, Intruder, Repeater, and Decoder, among others, to resolve specific problems faced by pentesters. You will also explore working with various modes of Burp and then perform operations on the web. Toward the end, you will cover recipes that target specific test scenarios and resolve them using best practices. By the end of the book, you will be up and running with deploying Burp for securing web applications. What you will learn

Configure Burp Suite for your web applications
 Perform authentication, authorization, business logic, and data validation testing
 Explore session management and client-side testing
 Understand unrestricted file uploads and server-side request forgery
 Execute XML external entity attacks with Burp
 Perform remote code execution with Burp
 Who this book is for
 If you are a security professional, web pentester, or software developer who wants to adopt Burp Suite for applications

security, this book is for you.

Linux Networking Cookbook Packt Publishing Ltd

Over 100 recipes to get up and running with the modern Linux administration ecosystem
 Key Features
 Understand and implement the core system administration tasks in Linux
 Discover tools and techniques to troubleshoot your Linux system
 Maintain a healthy system with good security and backup practices
 Book Description
 Linux is one of the most widely used operating systems among system administrators, and even modern application and server development is heavily reliant on the Linux platform. The Linux Administration Cookbook is your go-to guide to get started on your Linux journey. It will help you understand what that strange little server is doing in the corner of your office, what the mysterious virtual machine languishing in Azure is crunching through, what that circuit-board-like thing is doing under your office TV, and why the LEDs on it are blinking rapidly. This book will get you started with administering Linux, giving you the knowledge and tools you need to troubleshoot day-to-day problems, ranging

from a Raspberry Pi to a server in Azure, while giving you a good understanding of the fundamentals of how GNU/Linux works. Through the course of the book, you'll install and configure a system, while the author regales you with errors and anecdotes from his vast experience as a data center hardware engineer, systems administrator, and DevOps consultant. By the end of the book, you will have gained practical knowledge of Linux, which will serve as a bedrock for learning Linux administration and aid you in your Linux journey. What you will learn

Install and manage a Linux server, both locally and in the cloud
 Understand how to perform administration across all Linux distros
 Work through evolving concepts such as IaaS versus PaaS, containers, and automation
 Explore security and configuration best practices
 Troubleshoot your system if something goes wrong
 Discover and mitigate hardware issues, such as faulty memory and failing drives
 Who this book is for
 If you are a system engineer or system administrator with basic experience of working with Linux, this book is for you.

Kali Linux - An Ethical Hacker's

Cookbook Packt Publishing Ltd

A guide to the most frequently used OpenSSL features and commands, written by Ivan Ristic. Comprehensive coverage of OpenSSL installation, configuration, and key and certificate management Includes SSL/TLS Deployment Best Practices, a design and deployment guide Written by a well-known practitioner in the field and the author of SSL Labs and the SSL/TLS configuration assessment tool Available in a variety of digital formats (PDF, EPUB, Mobi/Kindle); no DRM Continuously updated OpenSSL Cookbook is built around one chapter from Bulletproof SSL/TLS and PKI, a larger work that provides complete coverage of SSL/TLS and PKI topics. To download your free copy in various formats, visit

feistyduck.com/books/openssl-cookbook/
ASP.NET Core 5 Secure Coding Cookbook
Packt Publishing Ltd

Provides step-by-step instructions on how to use the computer operating system Linux.

Mastering Linux Security and Hardening Packt Publishing Ltd

To thoroughly understand what makes Linux tick and why it's so efficient, you

need to delve deep into the heart of the operating system--into the Linux kernel itself. The kernel is Linux--in the case of the Linux operating system, it's the only bit of software to which the term "Linux" applies. The kernel handles all the requests or completed I/O operations and determines which programs will share its processing time, and in what order. Responsible for the sophisticated memory management of the whole system, the Linux kernel is the force behind the legendary Linux efficiency. The new edition of Understanding the Linux Kernel takes you on a guided tour through the most significant data structures, many algorithms, and programming tricks used in the kernel. Probing beyond the superficial features, the authors offer valuable insights to people who want to know how things really work inside their machine. Relevant segments of code are dissected and discussed line by line. The book covers more than just the functioning of the code, it explains the theoretical underpinnings for why Linux does things the way it does. The new edition of the book has been updated to cover version 2.4 of the kernel, which is quite different

from version 2.2: the virtual memory system is entirely new, support for multiprocessor systems is improved, and whole new classes of hardware devices have been added. The authors explore each new feature in detail. Other topics in the book include: Memory management including file buffering, process swapping, and Direct memory Access (DMA) The Virtual Filesystem and the Second Extended Filesystem Process creation and scheduling Signals, interrupts, and the essential interfaces to device drivers Timing Synchronization in the kernel Interprocess Communication (IPC) Program execution Understanding the Linux Kernel, Second Edition will acquaint you with all the inner workings of Linux, but is more than just an academic exercise. You'll learn what conditions bring out Linux's best performance, and you'll see how it meets the challenge of providing good system response during process scheduling, file access, and memory management in a wide variety of environments. If knowledge is power, then this book will help you make the most of your Linux system.

[Web Security Testing Cookbook](#) Feisty

Duck
Android Security Cookbook' breaks down and enumerates the processes used to exploit and remediate Android app security vulnerabilities in the form of detailed recipes and walkthroughs. Android Security Cookbook is aimed at anyone who is curious about Android app security and wants to be able to take the necessary practical measures to protect themselves; this means that Android application developers, security researchers and analysts, penetration testers, and generally any CIO, CTO, or IT managers facing the impending onslaught of mobile devices in the business environment will benefit from reading this book.

Practical Linux Security Cookbook Packt Publishing Ltd

Discover over 90 practical and exciting recipes that leverage the power of OpenVPN 2.4 to help you obtain a reliable and secure VPN About This Book Master the skills of configuring, managing, and securing your VPN using the latest OpenVPN Gain expertise in establishing IPv6 connections and understand PolarSSL using the latest version of OpenVPN This

book contains enticing recipes about OpenVPN functionalities that cater to mission critical applications Who This Book Is For This book is for system administrators who have a basic knowledge of OpenVPN and are eagerly waiting to build, secure, and manage VPNs using the latest version. This book assumes some prior knowledge of TCP/IP networking and OpenVPN and you must have network administration skills to get the most out of this book. What You Will Learn Determine the best type of OpenVPN setup for your networking needs Get to grips with the encryption, authentication, and certifications features of OpenSSL. Integrate an OpenVPN server into the local IT infrastructure with the scripting features of OpenVPN Ease the integration of Windows clients into the VPN using Windows-specific client-side configuration Understand the authentication plugins for PAM and LDAP Get to know the difference between TUN-style and TAP-style networks and when to use what Troubleshoot your VPN setup Establish a connection via IPv6 along with demonstrations In Detail OpenVPN provides an extensible VPN framework

that has been designed to ease site-specific customization, such as providing the capability to distribute a customized installation package to clients, and supporting alternative authentication methods via OpenVPN's plugin module interface. This book provides you with many different recipes to help you set up, monitor, and troubleshoot an OpenVPN network. You will learn to configure a scalable, load-balanced VPN server farm that can handle thousands of dynamic connections from incoming VPN clients. You will also get to grips with the encryption, authentication, security, extensibility, and certifications features of OpenSSL. You will also get an understanding of IPv6 support and will get a demonstration of how to establish a connection via IPv6. This book will explore all the advanced features of OpenVPN and even some undocumented options, covering all the common network setups such as point-to-point networks and multi-client TUN-style and TAP-style networks. Finally, you will learn to manage, secure, and troubleshoot your virtual private networks using OpenVPN 2.4. Style and approach This practical,

recipe-based book covers the core functionalities of OpenVPN ending with troubleshooting, performance tuning and making the readers inquisitive about the advanced features.

Burp Suite Cookbook Packt Publishing Ltd

A comprehensive guide to mastering the art of preventing your Linux system from getting compromised. Key Features Leverage this guide to confidently deliver a system that reduces the risk of being hacked Perform a number of advanced Linux security techniques such as network service detection, user authentication, controlling special permissions, encrypting file systems, and much more Master the art of securing a Linux environment with this end-to-end practical guide Book Description This book has extensive coverage of techniques that will help prevent attackers from breaching your system, by building a much more secure Linux environment. You will learn various security techniques such as SSH hardening, network service detection, setting up firewalls, encrypting file systems, protecting user accounts, authentication processes, and so on. Moving forward, you will also develop

hands-on skills with advanced Linux permissions, access control, special modes, and more. Lastly, this book will also cover best practices and troubleshooting techniques to get your work done efficiently. By the end of this book, you will be confident in delivering a system that will be much harder to compromise. What you will learn Use various techniques to prevent intruders from accessing sensitive data Prevent intruders from planting malware, and detect whether malware has been planted Prevent insiders from accessing data that they aren't authorized to access Do quick checks to see whether a computer is running network services that it doesn't need to run Learn security techniques that are common to all Linux distros, and some that are distro-specific Who this book is for If you are a systems administrator or a network engineer interested in making your Linux environment more secure, then this book is for you. Security consultants wanting to enhance their Linux security skills will also benefit from this book. Prior knowledge of Linux is mandatory.

Network Scanning Cookbook Packt Publishing Ltd

Enhance file system security and learn about network attack, security tools and different versions of Linux build. Key Features Hands-on recipes to create and administer a secure Linux system Enhance file system security and local and remote user authentication Use various security tools and different versions of Linux for different tasks Book Description Over the last few years, system security has gained a lot of momentum and software professionals are focusing heavily on it. Linux is often treated as a highly secure operating system. However, the reality is that Linux has its share of security flaws, and these security flaws allow attackers to get into your system and modify or even destroy your important data. But there's no need to panic, since there are various mechanisms by which these flaws can be removed, and this book will help you learn about different types of Linux security to create a more secure Linux system. With a step-by-step recipe approach, the book starts by introducing you to various threats to Linux systems. Then, this book will walk you through customizing the Linux kernel and securing local files. Next, you will move on to managing user

authentication both locally and remotely and mitigating network attacks. Later, you will learn about application security and kernel vulnerabilities. You will also learn about patching Bash vulnerability, packet filtering, handling incidents, and monitoring system logs. Finally, you will learn about auditing using system services and performing vulnerability scanning on Linux. By the end of this book, you will be able to secure your Linux systems and create a robust environment. What you will learn

Learn about vulnerabilities and exploits in relation to Linux systems
 Configure and build a secure kernel and test it
 Learn about file permissions and how to securely modify files
 Authenticate users remotely and securely copy files on remote systems
 Review different network security methods and tools
 Perform vulnerability scanning on Linux machines using tools
 Learn about malware scanning and read through logs
 Who this book is for
 This book is intended for all those Linux users who already have knowledge of Linux file systems and administration. You should be familiar with basic Linux commands. Understanding information security and its risks to a Linux system is

also helpful in understanding the recipes more easily.

Nagios Core Administration Cookbook
 Packt Publishing Ltd

Computer security is an ongoing process, a relentless contest between system administrators and intruders. A good administrator needs to stay one step ahead of any adversaries, which often involves a continuing process of education. If you're grounded in the basics of security, however, you won't necessarily want a complete treatise on the subject each time you pick up a book. Sometimes you want to get straight to the point. That's exactly what the new *Linux Security Cookbook* does. Rather than provide a total security solution for Linux computers, the authors present a series of easy-to-follow recipes--short, focused pieces of code that administrators can use to improve security and perform common tasks securely. The *Linux Security Cookbook* includes real solutions to a wide range of targeted problems, such as sending encrypted email within Emacs, restricting access to network services at particular times of day, firewalling a webserver, preventing IP spoofing, setting

up key-based SSH authentication, and much more. With over 150 ready-to-use scripts and configuration files, this unique book helps administrators secure their systems without having to look up specific syntax. The book begins with recipes devised to establish a secure system, then moves on to secure day-to-day practices, and concludes with techniques to help your system stay secure. Some of the "recipes" you'll find in this book are:

- Controlling access to your system from firewalls down to individual services, using iptables, ipchains, xinetd, inetd, and more
- Monitoring your network with tcpdump, dsniiff, netstat, and other tools
- Protecting network connections with Secure Shell (SSH) and stunnel
- Safeguarding email sessions with Secure Sockets Layer (SSL)
- Encrypting files and email messages with GnuPG
- Probing your own security with password crackers, nmap, and handy scripts

This cookbook's proven techniques are derived from hard-won experience. Whether you're responsible for security on a home Linux system or for a large corporation, or somewhere in between, you'll find valuable, to-the-point, practical recipes for dealing with everyday security

issues. This book is a system saver. [OpenVPN Cookbook](#) "O'Reilly Media, Inc." This unique and valuable collection of tips, tools, and scripts provides clear, concise, hands-on solutions that can be applied to the challenges facing anyone running a network of Linux servers from small networks to large data centers in the practical and popular problem-solution-discussion O'Reilly cookbook format. The Linux Cookbook covers everything you'd expect: backups, new users, and the like. But it also covers the non-obvious information that is often ignored in other books the time-sinks and headaches that are a real part of an administrator's job, such as: dealing with odd kinds of devices that Linux historically hasn't supported well, building multi-boot systems, and handling things like video and audio. The knowledge needed to install, deploy, and maintain Linux is not easily found, and no Linux distribution gets it just right. Scattered information can be found in a pile of man pages, texinfo files, and source code comments, but the best source of information is the experts themselves who built up a working knowledge of managing Linux systems. This cookbook's proven

techniques distill years of hard-won experience into practical cut-and-paste solutions to everyday Linux dilemmas. Use just one recipe from this varied collection of real-world solutions, and the hours of tedious trial-and-error saved will more than pay for the cost of the book. But those who prefer to learn hands-on will find that this cookbook not only solves immediate problems quickly, it also cuts right to the chase pointing out potential pitfalls and illustrating tested practices that can be applied to a myriad of other situations. Whether you're responsible for a small Linux system, a huge corporate system, or a mixed Linux/Windows/macOS network, you'll find valuable, to-the-point, practical recipes for dealing with Linux systems everyday. The Linux Cookbook is more than a time-saver; it's a sanity saver. **Android Internals - Volume I** "O'Reilly Media, Inc."

Master Wicket by example by implementing real-life solutions to every day tasks.

PfSense 2 Cookbook Packt Publishing Ltd 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.

[Linux Shell Scripting Cookbook](#) John Wiley & Sons

NGINX is one of the most widely used web servers available today, in part because of its capabilities as a load balancer and reverse proxy server for HTTP and other network protocols. This cookbook provides easy-to-follow examples to real-world problems in application delivery. The

practical recipes will help you set up and use either the open source or commercial offering to solve problems in various use cases. For professionals who understand modern web architectures, such as n-tier or microservice designs, and common web protocols including TCP and HTTP, these recipes provide proven solutions for security, software load balancing, and monitoring and maintaining NGINX's application delivery platform. You'll also explore advanced features of both NGINX and NGINX Plus, the free and licensed versions of this server. You'll find recipes for: High-performance load balancing with HTTP, TCP, and UDP Securing access through encrypted traffic, secure links, HTTP authentication subrequests, and more Deploying NGINX to Google Cloud, AWS, and Azure cloud computing services Setting up and configuring NGINX Controller Installing and configuring the NGINX Plus App Protect module Enabling WAF through Controller ADC [Understanding Linux Network Internals](#) Packt Publishing Ltd

A computer forensics "how-to" for fighting malicious code and analyzing incidents With our ever-increasing reliance on

computers comes an ever-growing risk of malware. Security professionals will find plenty of solutions in this book to the problems posed by viruses, Trojan horses, worms, spyware, rootkits, adware, and other invasive software. Written by well-known malware experts, this guide reveals solutions to numerous problems and includes a DVD of custom programs and tools that illustrate the concepts, enhancing your skills. Security professionals face a constant battle against malicious software; this practical manual will improve your analytical capabilities and provide dozens of valuable and innovative solutions. Covers classifying malware, packing and unpacking, dynamic malware analysis, decoding and decrypting, rootkit detection, memory forensics, open source malware research, and much more Includes generous amounts of source code in C, Python, and Perl to extend your favorite tools or build new ones, and custom programs on the DVD to demonstrate the solutions *Malware Analyst's Cookbook* is indispensable to IT security administrators, incident responders, forensic analysts, and malware

researchers.

Malware Analyst's Cookbook and DVD
Packt Publishing Ltd

Over 90 hands-on recipes that will employ Nagios Core as the anchor of monitoring on your network About This Book Master the advanced configuration techniques of Nagios Core to model your network better by improving hosts, services, and contacts Filter and improve the notifications that Nagios Core sends in response to failed checks, which can greatly assist you when diagnosing problems Pull Nagios Core's data into a database to write clever custom reports of your own devise Who This Book Is For If you are a network or system administrator and are looking for instructions and examples on working with Nagios Core, then this book is for you. Some basic shell command-line experience is required, and some knowledge of scripting would be helpful when we discuss how plugins work. What You Will Learn Manage the configuration of Nagios Core with advanced techniques to

achieve fine detail in your checks Find, install, and even write your own check plugins Filter notifications to send them to the right people or programs at the right time Work around difficult network accessibility issues and delegate checks to other machines Tweak a Nagios Core server to achieve both high performance and redundancy in case of disaster Process the results of checks performed by other machines to monitor backups and similar processes Extend Nagios Core to allow advanced scripting, reporting, and network visualization behavior In Detail Nagios Core is an open source monitoring framework suitable for any network that ensures both internal and customer-facing services are running correctly and manages notification and reporting behavior to diagnose and fix outages promptly. It allows very fine configuration of exactly when, where, what, and how to check network services to meet both the uptime goals of your network and systems team and the needs of your users. This

book shows system and network administrators how to use Nagios Core to its fullest as a monitoring framework for checks on any kind of network services, from the smallest home network to much larger production multi-site services. You will discover that Nagios Core is capable of doing much more than pinging a host or to see whether websites respond. The recipes in this book will demonstrate how to leverage Nagios Core's advanced configuration, scripting hooks, reports, data retrieval, and extensibility to integrate it with your existing systems, and to make it the rock-solid center of your network monitoring world. Style and approach Each chapter contains a set of step-by-step recipes to perform an example of a commonly performed task related to network administration. The book begins by focusing closely on the properties and configuration of Nagios Core itself, and gradually moves on to other pieces of software that can support, manage, and extend the system.