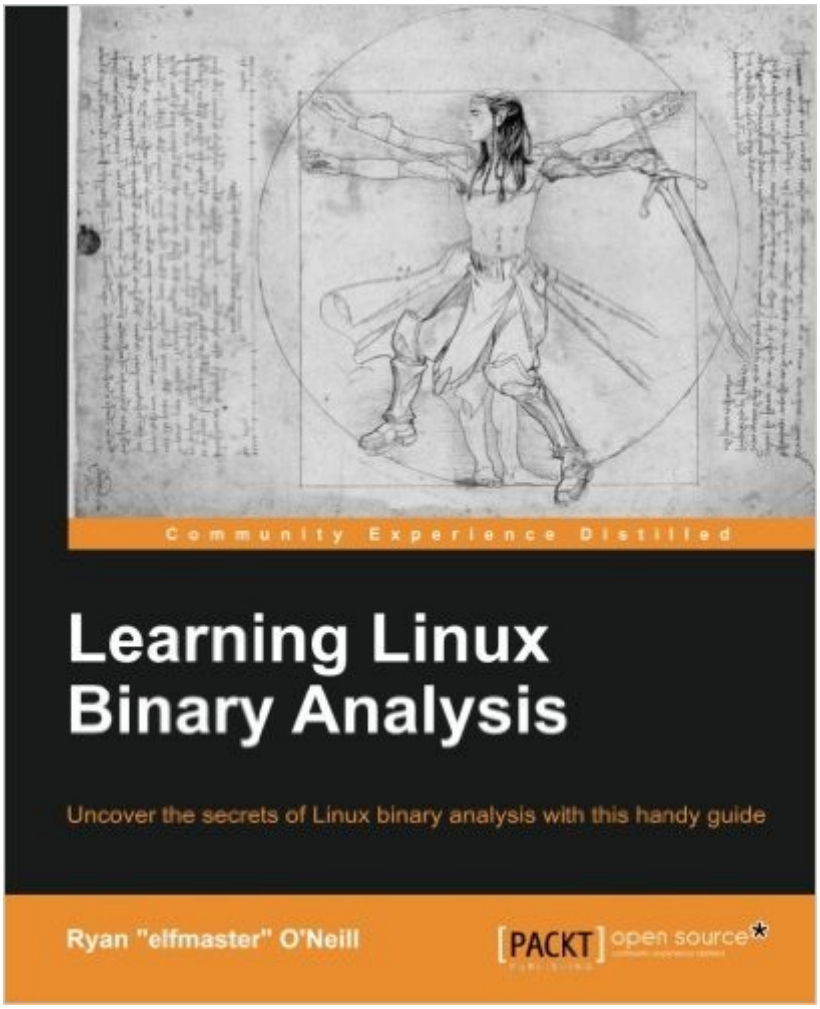
Learning Linux Binary Analysis



Synopsis

Key FeaturesGrasp the intricacies of the ELF binary format of UNIX and LinuxDesign tools for reverse engineering and binary forensic analysisInsights into UNIX and Linux memory infections, ELF viruses, and binary protection schemesBook DescriptionLearning Linux Binary Analysis is packed with knowledge and code that will teach you the inner workings of the ELF format, and the methods used by hackers and security analysts for virus analysis, binary patching, software protection and more.This book will start by taking you through UNIX/Linux object utilities, and will move on to teaching you all about the ELF specimen. You will learn about process tracing, and will explore the different types of Linux and UNIX viruses, and how you can make use of ELF Virus Technology to deal with them.The latter half of the book discusses the usage of Kprobe instrumentation for kernel hacking, code patching, and debugging. You will discover how to detect and disinfect kernel-mode rootkits, and move on to analyze static code. Finally, you will be walked through complex userspace memory infection analysis.This book will lead you into territory that is uncharted even by some experts; right into the world of the computer hacker.What you will learnExplore the internal workings of the ELF binary formatDiscover techniques for UNIX Virus infection and analysisWork with binary hardening and software anti-tamper methodsPatch executables and process memoryBypass anti-debugging measures used in malwarePerform advanced forensic analysis of binariesDesign ELF-related tools in the C languageLearn to operate on memory with ptraceAbout the AuthorRyan "elfmaster" O'Neill is a computer security researcher and software engineer with a background in reverse engineering, software exploitation, security defense, and forensics technologies. He grew up in the computer hacker subculture, the world of EFnet, BBS systems, and remote buffer overflows on systems with an executable stack. He was introduced to system security, exploitation, and virus writing at a young age. His great passion for computer hacking has evolved into a love for software development and professional security research. Ryan has spoken at various computer security conferences, including DEFCON and RuxCon, and also conducts a 2-day ELF binary hacking workshop.He has an extremely fulfilling career and has worked at great companies such as Pikewerks, Leviathan Security Group, and more recently Backtrace as a software engineer.Ryan has not published any other books, but he is well known for some of his papers published in online journals such as Phrack and VXHeaven. Many of his other publications can be found on his website at http://www.bitlackeys.org.Table of ContentsThe Linux Environment and Its ToolsThe ELF Binary FormatLinux Process TracingELF Virus Technology â " Linux/Unix VirusesLinux Binary ProtectionELF Binary Forensics in LinuxProcess Memory ForensicsECFS â " Extended Core File Snapshot TechnologyLinux

/proc/kcore Analysis

Book Information

Paperback: 282 pages

Publisher: Packt Publishing - ebooks Account (February 29, 2016)

Language: English

ISBN-10: 1782167102

ISBN-13: 978-1782167105

Product Dimensions: 7.5 x 0.6 x 9.2 inches

Shipping Weight: 1.2 pounds (View shipping rates and policies)

Average Customer Review: 5.0 out of 5 starsÂ Â See all reviewsÂ (4 customer reviews)

Best Sellers Rank: #153,317 in Books (See Top 100 in Books) #41 inÂ Books > Computers & Technology > Operating Systems > Linux > Programming #47 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Administration > Linux & UNIX Administration #58 inÂ Books > Computers & Technology > Operating Systems > Linux > Networking & System Administration

Customer Reviews

The book contains information that cannot be found in any one place on the internet. It is a unique book in the sense that it covers information on the ELF binary format, Linux virus infection techniques, process memory forensics, kernel hacking, reverse engineering concepts, hot patching, binary encryption, and more. In some places the formatting of the code (As in tabs/indentation etc.) is not so great, but overall the book gives a very good presentation and summarizes knowledge that cannot be found from very many sources. The author is very experienced in his knowledge of ELF, security, virus design, forensics analysis and much more. It is great for a wide spectrum of people, from software engineers who are building ELF linkers, to security analysts who are designing Virus detection, and binary protection software. The author has also left a note on his web page describing some of the problems with the book: (...)

great introduction to ELF file format and linux malware techniques (there’s not too many books on the topic). Overall very good, useful and to the point book filled with practical code examples.

Chapter 2 is worth the price alone. Engaging discussion of a subject that can be difficult to make interesting.

Great book

Binary Options: Crash Course!: Learn How to Make Money with Binary Options Trading & Binary Options Signals - Start Investing & Wealth Building Today! Linux: Linux Command Line - A Complete Introduction To The Linux Operating System And Command Line (With Pics) (Unix, Linux kemel, Linux command line, ... CSS, C++, Java, PHP, Excel, code) (Volume 1) LINUX: Easy Linux For Beginners, Your Step-By-Step Guide To Learning The Linux Operating System And Command Line (Linux Series) Learning Linux Binary Analysis Binary Options: A Complete Guide On Binary Options Trading (stock market investing, passive income online, options trading) Make Money with Binary Options: The Calends Strategy (The Binary Options Speculator) (Volume 2) Binary Options: The Complete Guide To Trading Binary Options Linux For Beginners: The Ultimate Guide To The Linux Operating System & Linux Linux Administration: The Linux Operating System and Command Line Guide for Linux Administrators CompTIA Linux+ Powered by Linux Professional Institute Study Guide: Exam LX0-103 and Exam LX0-104 (Comptia Linux + Study Guide) Linux: For Beginners - Step By Step User Manual To Learning The Basics Of Linux Operating System Today! (Ubuntu, Operating System) Unsupervised Machine Learning in Python: Master Data Science and Machine Learning with Cluster Analysis, Gaussian Mixture Models, and Principal Components Analysis Analytics: Data Science, Data Analysis and Predictive Analytics for Business (Algorithms, Business Intelligence, Statistical Analysis, Decision Analysis, Business Analytics, Data Mining, Big Data) Subnetting For Beginners: How To Easily Master IP Subnetting And Binary Math To Pass Your CCNA (CCNA, Networking, IT Security, ITSM) Binary and Hexadecimal Workbook for GCSE Computer Science and Computing (Comp Sci Workbooks) (Volume 1) Binary Options Unmasked The Binary Options Book Of Knowledge: Everything I Wish I Had Known Before I Started Trading Binary Options Trading GURU: Learn How To Trade With Simple Strategies I Provide In This Book! Long Story Shortened Beat Binary Options: Winning Financial Betting Strategies for Today's Markets Options Trading: A CherryTree Style Trading Book(Options Trading,Options Trading for Beginners,options trading guide,options trading tips,binary options trading,trading options,option strategies)