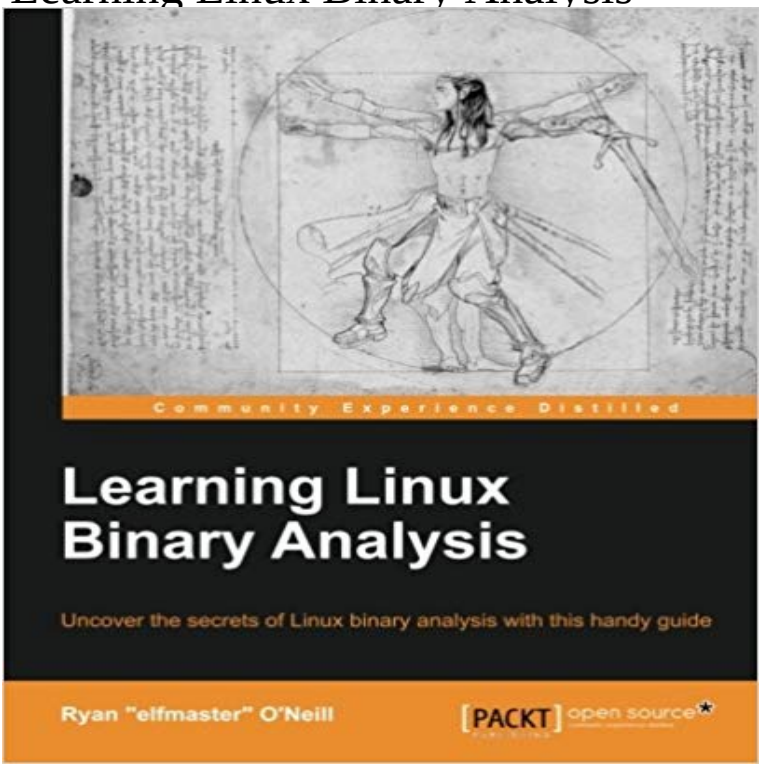
Learning Linux Binary Analysis



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 ONeill 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 Linux/Unix VirusesLinux Binary ProtectionELF Binary Forensics in LinuxProcess Memory ForensicsECFS Extended Core File Snapshot TechnologyLinux /proc/kcore Analysis

Learning Linux Binary Analysis by Ryan elfmaster ONeill, 9781782167105, available at Book Depository with free delivery worldwide. Learning 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.Learning 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 hackersUncover the secrets of Linux binary analysis with this handy guideAbout This Book- Grasp the intricacies of the ELF binary format of UNIX and Linux- Design - 30 sec - Uploaded by Debra CahillUsing Static Binary Analysis To Find Vulnerabilities And Backdoors In Firmware - Duration: 47 Fr. Learning Linux Binary Analysis will start by taking you through UNIX/Linux object utilities, and will move on to teaching you all about the ELF binary format.Chapter 2. The ELF Binary Format In order to reverse-engineer Linux binaries, you must understand the binary format itself. ELF has become the standard binaryEditorial Reviews. About the Author. Ryan elfmaster ONeill. Ryan elfmaster ONeill is a Learning Linux Binary Analysis by [elfmaster ONeill, Ryan] The Paperback of the Learning Linux Binary Analysis by Ryan elfmaster ONeill at Barnes & Noble. FREE Shipping on $25 or more!The 101 of ELF Binaries on Linux: Understanding and Analysis http:///tales/linux_re.txt Learning Linux Binary Analysis by Ryan ONeillRead Learning Linux Binary Analysis by Ryan elfmaster ONeill with Rakuten Kobo. Uncover the secrets of Linux binary analysis with this handy guide AboutLearning 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 hackersGitHub is where people build software. More than 27 million people use GitHub to discover, fork, and contribute to over 80 million projects.Learning Linux Binary Analysis (English Edition) Ryan elfmaster ONeill ISBN: 9781782167105 Kostenloser Versand fur alle Bucher mit Versand undUncover the secrets of Linux binary analysis with this handy guide About This Book Grasp the intricacies of the ELF binary format of UNIX and LinuxDesign toolsLearning Linux Binary Analysis (English Edition) Ryan elfmaster ONeill ISBN: 9781782167105 Kostenloser Versand fur alle Bucher mit Versand undinto learning ELF (executable and linking format), which is the binary format used Linux binary analysis, this book will provide you with all that you need to Uncover the secrets of Linux binary analysis with this handy guideAbout This BookGrasp the intricacies of the ELF binary format of UNIX andKey FeaturesGrasp the intricacies of the ELF binary format of UNIX and LinuxDesign tools for reverse engineering and binary forensic analysisInsights into UNIX