Learning Linux Binary Analysis

Ryan "elfmaster" O'Neill

Learning Linux Binary Analysis

Ryan "elfmaster" O'Neill

Learning Linux Binary Analysis Ryan "elfmaster" O'Neill

Key Features

- Grasp the intricacies of the ELF binary format of UNIX and Linux
- Design tools for reverse engineering and binary forensic analysis
- Insights into UNIX and Linux memory infections, ELF viruses, and binary protection schemes

Book Description

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.

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 learn

- Explore the internal workings of the ELF binary format
- Discover techniques for UNIX Virus infection and analysis
- Work with binary hardening and software anti-tamper methods
- Patch executables and process memory
- Bypass anti-debugging measures used in malware
- Perform advanced forensic analysis of binaries
- Design ELF-related tools in the C language
- Learn to operate on memory with ptrace

About the Author

Ryan "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 Contents

Download and Read Free Online Learning Linux Binary Analysis Ryan "elfmaster" O'Neill

---

From reader reviews:

Bobby Bagwell:

What do you ponder on book? It is just for students since they are still students or it for all people in the world, the particular best subject for that? Only you can be answered for that query above. Every person has distinct personality and hobby for every other. Don't to be pressured someone or something that they don't desire do that. You must know how great as well as important the book Learning Linux Binary Analysis. All type of book are you able to see on many resources. You can look for the internet sources or other social media.

Melissa Hopkins:

What do you regarding book? It is not important along with you? Or just adding material when you need something to explain what the one you have problem? How about your spare time? Or are you busy particular person? If you don't have spare time to try and do others business, it is make you feel bored faster. And you have free time? What did you do? Everyone has many questions above. They need to answer that question simply because just their can do that. It said that about publication. Book is familiar in each person. Yes, it is suitable. Because start from on jardín de infancia until university need this specific Learning Linux Binary Analysis to read.

Joyce Cassady:

Are you kind of occupied person, only have 10 as well as 15 minute in your day time to upgrading your mind talent or thinking skill actually analytical thinking? Then you are receiving problem with the book compared to can satisfy your limited time to read it because this time you only find e-book that need more time to be study. Learning Linux Binary Analysis can be your answer mainly because it can be read by you who have those short spare time problems.

Shari Villa:

As a student exactly feel bored for you to reading. If their teacher questioned them to go to the library or to make summary for some publication, they are complained. Just tiny students that has reading's heart and soul or real their passion. They just do what the educator want, like asked to go to the library. They go to presently there but nothing reading really. Any students feel that studying is not important, boring and can't see colorful photographs on there. Yeah, it is for being complicated. Book is very important for yourself. As we know that on this period of time, many ways to get whatever we really wish for. Likewise word says, ways to reach Chinese's country. Therefore , this Learning Linux Binary Analysis can make you sense more interested to read.

Read Learning Linux Binary Analysis by Ryan "elfmaster" O'Neill for online ebook

Learning Linux Binary Analysis by Ryan "elfmaster" O'Neill Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Learning Linux Binary Analysis by Ryan "elfmaster" O'Neill books to read online.

Online Learning Linux Binary Analysis by Ryan "elfmaster" O'Neill ebook PDF download

Learning Linux Binary Analysis by Ryan "elfmaster" O'Neill Doc

Learning Linux Binary Analysis by Ryan "elfmaster" O'Neill Mobipocket

Learning Linux Binary Analysis by Ryan "elfmaster" O'Neill EPub