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

From reader reviews:

Teddy Hathorn:

People live in this new moment of lifestyle always try to and must have the free time or they will get lots of stress from both everyday life and work. So , once we ask do people have extra time, we will say absolutely of course. People is human not just a robot. Then we request again, what kind of activity are there when the spare time coming to you of course your answer will probably unlimited right. Then do you ever try this one, reading publications. It can be your alternative within spending your spare time, typically the book you have read is usually Learning Linux Binary Analysis.

Leopoldo Gonzalez:

Playing with family within a park, coming to see the water world or hanging out with good friends is thing that usually you may have done when you have spare time, then why you don't try matter that really opposite from that. 1 activity that make you not sense tired but still relaxing, trilling like on roller coaster you already been ride on and with addition associated with. Even you love Learning Linux Binary Analysis, you may enjoy both. It is good combination right, you still want to miss it? What kind of hangout type is it? Oh can happen its mind hangout guys. What? Still don't get it, oh come on its referred to as reading friends.

Debra Weeks:

Are you kind of stressful person, only have 10 or maybe 15 minute in your time to upgrading your mind talent or thinking skill actually analytical thinking? Then you are receiving problem with the book when compared with can satisfy your short period of time to read it because this all time you only find e-book that need more time to be examine. Learning Linux Binary Analysis can be your answer given it can be read by you actually who have those short time problems.

Robert Burmeister:

As we know that book is significant thing to add our information for everything. By a book we can know everything we want. A book is a list of written, printed, illustrated or perhaps blank sheet. Every year seemed to be exactly added. This reserve Learning Linux Binary Analysis was filled concerning science. Spend your spare time to add your knowledge about your technology competence. Some people has several feel when they reading some sort of book. If you know how big advantage of a book, you can experience enjoy to read a book. In the modern era like at this point, many ways to get book that you just wanted.

Download and Read Online Learning Linux Binary Analysis Ryan

"elfmaster" O'Neill #P3GUEOLXDW0

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